2015

Pairing-free identity-based cryptography

Ibrahim Elashry
University of Wollongong

Pairing-Free Identity-Based Cryptography

Ibrahim Elashry

This thesis is presented as part of the requirements for the conferral of the degree:

Doctor of Philosophy

The University of Wollongong
School of Computing and Information Technology

April 27, 2015

When one door closes, another opens; but we often look so long and so regretfully upon the closed door that we do not see the one that has opened for us.

Dedicated to The Memory of My Beloved Father

1943 – 2012

Declaration

I, Ibrahim Elashry, declare that this thesis submitted in partial fulfilment of the requirements for the conferral of the degree Doctor of Philosophy, from the University of Wollongong, is wholly my own work unless otherwise referenced or acknowledged. This document has not been submitted for qualifications at any other academic institution.

Ibrahim Elashry
April 27, 2015

Abstract

Identity-based cryptography (IBC) is considered nowadays as the evolution of public key cryptography because it completely eliminates the use of digital certificates by representing the public key of a user as his identity. Although the first IBC proposed by Adi Shamir [Sha84] was based on RSA, most of the proposed IBC systems are based on bilinear pairings. This limits the use of IBC in the real world because of several reasons. First, a bilinear pairing is time- and power-inefficient and it takes around 2.5 times an RSA modular exponentiation based on MIRACL benchmarks. Second, these systems are incompatible with the most widely used public key cryptosystem (RSA) which makes them non-commercially appealing. Thus, it is useful to think outside the box and try to use different tools to construct IBC systems. These constructions may have unique security properties that do not exist in current IBC systems. We worked on constructing IBC systems based on RSA settings. We have improved the performance of identity-based encryption (IBE) systems, cryptanalysed IBE systems, implemented variants of IBE systems such as mediated encryption and attribute-based signcryption, and presented an identity-based authenticated key exchange (IBAKE) with some novel security features.

In this thesis, we first present some background about IBC and the motivation for solving the problems associated with pairing-based IBC. Then we give solutions to these problems along with the thesis structure. Then, we give a literature review about IBC, including identity-based encryption (IBE) and key exchange (KE) with focusing on pairing-free constructions. We also review some applications of IBC such as mediated cryptography and attribute-based cryptography. In addition, we review the definitions and preliminaries related to the contents of the thesis, including definitions of security models, hard problems, and some mathematical tools. Then, we review identity-based mediated RSA encryption and signature systems (IB-mRSA) presented by Boneh, Ding and Tsudik [BDT02]. We show that IB-mRSA is not secure and we present a secure modified version of it which is as efficient as the original system. We also propose a generic mediated encryption (GME) that transforms any IBE to a mediated version of this IBE. We also present two implementations of GME based on Boneh-Franklin FullIdent [BF01] which is a pairing-based IBE and Boneh, Gentry and Hamburg (BGH) AnonIBE [BGH07] which is a pairing-free IBE. After that, we present two efficient variants of (BGH) systems (BasicIBE, AnonIBE) [BGH07] in terms of ciphertext length and encryption/decryption speed. The ciphertext is as short as the BGH systems, but with more time-efficient algorithms.

We prove that these variants are as secure as the BGH systems. Then, we review an efficient variant of Boneh, Gentry and Hamburg BasicIBE presented by Jhanwar and Barua [JB08]. We prove that this IBE is not secure against an indistinguishable chosen plaintext attack (IND-ID-CPA) adversary and present a solution to the security flaw of this IBE. After that, we present two ciphertext-policy attribute-based signcryption (CP-ABSC) systems. One of our proposed ABSC is anonymous i.e., an adversary cannot determine for which attributes or policies the message has been signcrypted. These systems are time-efficient and fully secure under the quadratic residuosity (QR) assumption and provide a constant ciphertext size regardless of the number of attributes associated with the access structure. Then, we present a new security notion for key exchange (KE) protocols called Resiliency. That is, if a shared secret between designated parties is compromised or leaked, they can generate another completely new shared secret without the need to setup a new key exchange session. We present an identity-based authenticated key exchange protocol (IBAKE) that satisfies the resiliency security property. Finally, we present the conclusion of the thesis.

Acknowledgments

First and foremost, all praises and thanks to Allah for giving me the opportunity to pursue my PhD studies until the end.

After that, I would like to express my special appreciation and thanks to my supervisors Prof. Yi Mu and Prof. Willy Susilo. You have been tremendous mentors for me. I would like to thank you for encouraging my research and for allowing me to grow as a research scientist. Your advice on both research as well as on my career has been priceless. I also want to thank you for your continuous encouragement, support, patience, discussions, valuable comments, and excellent suggestions to improve the quality of this work. I would especially like to express my gratitude to all my friends in the centre for computer and information security research lab (CCISR). All of you have been there to support me when I was pursuing my PhD studies.

A special thanks to my family. Words cannot express how grateful I am to my mother, my brother, and my sisters for all the sacrifices that you have made on my behalf. Your prayers for me were what sustained me thus far. I would also like to thank all of my friends who supported me in my studies and encouraged me to strive towards my goal. Finally, I would like to express my appreciation to my beloved father. Thank you for all what you have done for me. May Allah give you peace.

[This page is intentionally left blank]

Publications

My thesis is related to the following publications/manuscripts.

1. Ibrahim F. Elashry, Yi Mu, and Willy Susilo. *Generic Mediated Encryption. In Security and Privacy in Communication Networks - 9th International ICST Conference, SecureComm 2013, Sydney, NSW, Australia, September 25-28, 2013, Revised Selected Papers, pages 154-168*, 2013.

2. Ibrahim F. Elashry, Yi Mu, and Willy Susilo. *Identity-based Mediated RSA Revisited. In 12th IEEE International Conference on Trust, Security and Privacy in Computing and Communications, TrustCom 2013, Melbourne, Australia, July 16-18, 2013, pages 728-735*, 2013.

3. Ibrahim F. Elashry, Yi Mu, and Willy Susilo. *Jhanwar-barua's Identity-based Encryption Revisited. In Network and System Security - 8th International Conference, NSS 2014, Xi'an, China, October 15-17, 2014, Proceedings, pages 271-284*, 2014.

4. Ibrahim F. Elashry, Yi Mu, and Willy Susilo. *Efficient Variant of Boneh-Gentry-Hamburg's Identity-based Encryption Without Pairing. In The 15th International Workshop on Information Security Applications (WISA 2014), Lecture Notes in Computer Science, Springer- Verlag, pages 257-268*, 2014.

5. Ibrahim F. Elashry, Yi Mu, and Willy Susilo. *Mediated Encryption: Analysis and Design. The Journal of Security and Safety*, 3:e2 (2015).

6. Ibrahim F. Elashry, Yi Mu, and Willy Susilo. *A Resilient Identity- based Authenticated Key Exchange Protocol, Security and Communication Networks (to appear), 2015.*

Contents

List of Tables

List of Figures

[This page is intentionally left blank]

Chapter 1

Introduction

1.1 Background

During the last decade, the use of computer networks has grown spectacularly, and this growth continues unabated. Almost all networks are being installed, interconnected, and connected to the Internet. The growing use of Internet applications gives rise to the problem of managing digital identities and preserving their privacy. In an open large-scale domain such as the Internet, preserving user privacy is not a straightforward task. Identity theft, which occurs when an impostor uses a legitimate user's identifying information without his consent, is becoming one of the biggest security concerns both for users and for organisations offering services on the Internet. Several cryptography techniques have been employed to protect the digital data from illegal tampering or stealing. These techniques are symmetric (private) key cryptography, that uses the same key for encryption/encryption, such as the advanced encryption standard (AES) [DR00] and asymmetric (public) key cryptography, that uses different keys for encryption/verify and decryption/sign, such as RSA [RSA83], named after its inventors, Rivest, Shamir, and Adleman.

For a long time, the symmetric key cryptography was believed to be the only way to secure communications, but it faced the problem of key distribution. Besides, the number of keys to maintain this system is very large, if there are n users that need secure communications between them, a number of $\frac{n(n-1)}{2}$ keys is required to maintain this system, and every user needs to maintain $n-1$ of secret keys. As said, necessity is the mother of invention, so the cryptography community had to invent a cryptographic technique that uses different keys for encryption and decryption. Asymmetric cryptography solves the problem of key distribution because the key used for encryption can be made public without any security problems. Besides, compared with the previous secure communication model, only a number of n public keys are required. Diffie and Hellman were the first to publish a paper about public key cryptography systems [DH76]. After that, scholars such as Taher ElGamal [Gam84], Goldwasser and Micali [GM84], and Rivest, Shamir, and Adleman [RSA83] proposed different asymmetric key cryptography systems.

The idea behind identity-based cryptography (IBC) was first proposed by [Sha84], in which Shamir asked the cryptography community to design a public key encryption with public keys that could be any arbitrary string. This gives the opportunity

to make the public key any string that is related to the identity of a user, such as his e-mail address or phone number. This is why this type of cryptography is called identity-based cryptography. This gives the advantage of simplifying the management of public keys since it greatly decreases the need for and reliance on public key certificates. In his paper, he successfully achieved his goal to design an identity-based signature based on RSA, but he could not achieve that for encryption because sharing a common modulus between different users makes RSA insecure. Sixteen years later, Sakai *et al.* proposed the first identity-based encryption (IBE) [SK03], while Boneh and Franklin proposed [BF01] the first reliable and provable IBE, which is based on Weil pairings over elliptic curves. After the presentation of Boneh-Franklin IBE, many IBE systems based on bilinear pairings were presented in the literature [BB04b, Gen06, Wat05].

IBE is not perfect and has some drawbacks. For instance, IBE does not support an access control structure for an encrypted data, a user can only decrypt the message if and only if he posses the secret key associated with the public key by which the message is encrypted.

Attribute-based encryption (ABE) was first introduced by Sahai and Waters [SW05] as a variant of IBE [Sha84]. Attribute-based cryptography (ABC) was presented to give an access structure to the encrypted data stored on a public cloud. It allows the users to encrypt or sign messages based on their attributes instead of their individual identities as in IBC. These attributes are, for example, the place where they live or the company in which they work. ABC can be classified as a key-policy ABC (KP-ABC) and a ciphertext-policy ABC (CP-ABE). A policy is a rule that determines which attributes should decrypt or verify the message. In a KP-ABC, the policy is inserted in the key while the message is encrypted or signed using the attributes. In a CP-ABC, the policy is inserted in the ciphertext while the key represents the attributes. CP-ABE is more suitable in access control applications compared with KP-ABE because it lets the sender to choose the access structure which determines who can decrypt the message [GMS+14].

Another problem that faces IBC is the key revocation problem. This problem exists in public key cryptography but became more severe in IBC. Assume that there is a user A who works in a company XYZ and his public key B needs to be revoked for some reason (for example, his secret key is leaked). In public key cryptography, the certificate associated with this public key must be revoked and a new public key along with a new certificate must be generated and this certificate must be available to all users who might communicate with this user. Sharing a great deal of fresh certificates periodically leads to the key revocation problem which consumes large amount of computation power and bandwidth. This is considered a hindrance to global application of public-key cryptography. The most widely-known and a

very ineffective way to solve the key revocation problem is the certificate revocation list (CRL) [CSF+08, HPFS02] which is a list that contains revoked certificates. The certificate authority (CA) produces this list periodically with its signature. Because the CA will probably revoke many of its certificates -say 10 %- if they are produced for a validity time of one year [Gen03, Mic02], the CRL will be too lengthy if the CA has many clients. Moreover, the complete CRL must be sent to any party that needs to carry out a certificate status check. There are improvements to this approach such as delta CRLs [HPFS02] which list only those certificates revoked since the CA's last update. But the consumed transmission bandwidth and computation costs of the transmission of these lists are still very high. Another method of solving the key revocation problem is the online certificate status protocol (OCSP) [MAM+99]. If a client wants to check the status of a certificate, he sends to the CA a certificate status query. The CA replies to this query by producing a fresh signature on the certificate's current status. This omits the need to send a list of all revoked certificates and reduces the transmission costs to a single signature per query but it significantly increases computation costs. It also negatively affects security. If the CA is centralised, the system will have a single point of failure and will become highly vulnerable to denial-of-service (DoS) attacks [Gen03, Mic02].

As we mentioned before, the key revocation problem becomes more severe in IBC because it is not possible to change the public key (identity) of a user. This problem can be solved using certificateless encryption [Gen03] and mediated encryption [BDTW01].

Gentry presented the notion of certificate-based encryption (CBE) [Gen03]. This system combines public-key encryption (PKE) and IBE while keeping most of the advantages of each. Using PKE, each client creates his own public-key/secret-key pair and asks for a certificate from the CA. The CA uses an IBE to create the certificate. This certificate has all of the functionality of a conventional PKI certificate as well as a decryption key. This double encryption gives us implicit certification. If T wants to encrypt a message, he double encrypts it using PKI and IBE and then the decryptor uses both his secret key and an up-to-date certificate from his CA to decrypt the message. CBE has no escrow (since the CA does not know the user's secret key) and it does not have a secret key distribution problem because the CA's certificate does not have to be secret. The disadvantage of CBE is that it uses certificates. It is preferable to completely eliminate the use of certificates to preserve the infrastructure costs.

Boneh, Ding, Tsudik and Wong were the first to introduce the notion of mediated cryptosystems [BDTW01]. They designed a variant of RSA that allows an immediate revocation of, for instance, an employee's key by an employer for any reason (mRSA). mRSA is the first secure variant of RSA that shares a common

modulus between different users. It is based on the so-called security mediator (SEM) architecture in which the SEM is a semi-trusted server. To maintain its security, it is assumed that throughout the life of the system, neither any user nor the SEM can obtain a complete public key/secret key pair. If an employee wants to decrypt/sign a message, he must co-operate with the SEM to do so. The idea behind mRSA is splitting the secret key of an employee between the employee himself and the SEM. Hence, without the SEM cooperation, the employee cannot sign or encrypt messages. This is also helpful to monitor the security of sent/received secure messages in the company. Later on, Ding and Tsudik presented an identity-based mediated RSA (IB-mRSA) along with its security proof [DT03]. In particular, they stated that 'IB-mRSA/OAEP encryption offers equivalent the semantic security to RSA/OAEP against adaptive chosen ciphertext attacks in the random oracle model if the key generation function is division intractable'. To make the key generation function division intractable, Ding and Tsudik used a division intractable hash function to generate division intractable public keys. The SEM architecture was proven useful [BDTW01] to simplify signature validation and enable key revocation in legacy systems. Although IB-mRSA does not require a CA to create a certificate or send certificate status information and the computation and transmission costs are kept to minimum, it has a major security concern. Since the SEM is centralised, it represents a single point of failure for the system and hence it is vulnerable to DOS attacks. In addition, a hacked SEM can be a major threat to the system security because the SEM is a semi-trusted server.

The main problem that faced the cryptography community to develop an IBE since Adi Shamir presented the idea in 1985 until the existence of the first provable secure IBE by Boneh and Franklin in 2001 is that the main two public key cryptography systems (RSA and ElGamal) and their variants are not compatible with IBE. For RSA, if a modulus is shared among multiple users with a complete public key /secret key pair for each user, any user can use his key pair to factorise the modulus and hence, he can find the secret key of any other user and break the system. For ElGamal-like systems, the usual method to generate a public key / secret key pair is as follows. The user first generates a random value α as the secret key, and then generates the public key as g^{α} for a generator g. Obtaining the secret key from the public key represents the discrete log (DL) hard problem. But in IBE, the public key (identity) of a user is given, and the secret key associated with the identity is required, which is a DL hard problem.

There were several attempts to construct IBE systems without bilinear pairings. Cocks [Coc01] was the first to present an IBE that does not depend on bilinear pairings. Although Cock's IBE is time-efficient, it produces a long ciphertext of 2 elements in $\mathbb{Z}_{\mathbb{N}}$ for each bit in the message. The size of an element in $\mathbb{Z}_{\mathbb{N}}$ is as large as

the modulus N. Boneh, Gentry and Hamburg (BGH) presented space-efficient IBE systems without bilinear pairings [BGH07]. The ciphertext size is smaller compared to Cock's IBE but on the other hand, it requires two prime search operations to encrypt each bit. In addition, the private key length is one element in $\mathbb{Z}_{\mathbb{N}}$ for each bit in the message. Jhanwar and Barua [JB08] made some significant observations on BGH systems and proposed a trade-off system that reduces the private key length but increases the ciphertext length. Only $2\sqrt{l}$ inversions in $\mathbb{Z}_{\mathbb{N}}$ are required to encrypt the whole message where l is the message length. This increases the encryption/decryption speed dramatically. The private key is only one element in $\mathbb{Z}_{\mathbb{N}}$. However, this system produces a large ciphertext of $2\sqrt{l}$ elements in $\mathbb{Z}_{\mathbb{N}}$.

Another way to implement IBE systems without pairing is from trapdoor discrete logarithm groups [PS09, Pat08]. This system uses a special RSA modulus to build groups in which knowledge of trapdoor information makes it easier to solve the DL problem to generate secret keys from the identity of the user. Although the solution of the DL problem is much easier with the trapdoor information, it is still completely inefficient compared to pairing-based systems.

Gentry, Peikert and Vaikuntanathan presented a lattice-based IBE [GPV07, Pat08]. This system is based on hardness of learning with error (LWE) problem in random modular lattices. This system has a long private key. It is also difficult to specify secure choice of parameters for new lattice-based systems.

1.2 Problems and Motivation

In general, IBC systems based on bilinear pairings have few major drawbacks. First, bilinear pairings are time- and power-inefficient mathematical tools. According to MIRACL benchmarks, a bilinear pairing takes approximately 2.5 times a modular exponentiation in RSA. Second, the incompatibility of these systems with the well-established public key cryptography systems such as RSA prevents them from being widely used in the real world. Third, the security of these systems are based on relatively untested computational problems compared to RSA or ElGamal. Fourth, the implementation of these systems can be complex with many choices of parameters, families of curves and implementation tricks. The current IBE systems without pairings are not practical and cannot compete with pairing-based IBE systems. That motivates us to find alternative constructions that achieve the following.

1. Time- and power-efficient IBE systems that make them suitable for mobile devices with limited power capabilities such as lightweight devices.

2. The compatibility of these systems with RSA by using an RSA modulus $N = pq$ where p and q are primes.

3. The construction of these systems must be simple and easy to implement.

4. The availability of other security features that make them more appealing.

1.3 Solutions

We investigated the above problems using the following techniques.

1. We first reviewed the current IBE systems in the literature without pairings in RSA settings (IB-mRSA, BGH IBE systems and Jhanwar-Barua IBE).

2. We investigated if these systems can be improved to become time- and power-efficient compared to pairing-based IBE systems.

3. We checked if these systems can be adopted to solve IBE problems like attribute-based encryption and key revocation problem.

4. We checked if these systems can be adapted to achieve security properties that make them more appealing than the current IBC systems.

After following the above methodology, we achieved the following results.

1. We find that IB-mRSA and Jhanwar-Barua IBE are insecure and we present solutions to the security flaws in these systems.

2. We present a generic mediated encryption technique that can transform any IBE to one that supports key revocation.

3. We present variants of BGH IBE systems that are time- and power-efficient compared to pairing-based IBE systems without affecting their security.

4. We present two ciphertext-policy attribute-based signcryption (CP-ABSC) systems that are efficient and fully secure compared to other pairing-based ABCS. One of these systems is anonymous. i.e., an adversary cannot determine for which attributes or policies the message has been signcrypted. As far as we know, there is no anonymous CP-ABSC in the literature.

5. We present a new security notion for key exchange protocols called Resiliency. In resilient KE protocols, if a shared secret between different parties is leaked, these parties can generate a new secret without the need to exchange new information or establish a new session.

1.4 Thesis Structure

The thesis is structured as follows.

In Chapter 1, we present some background about IBC and the motivation for solving the problems associated with pairing-free IBC. Then we give the solutions to these problems along with the thesis structure.

In Chapter 2, we give a literature review about IBC, including IBE and identity-based key exchange (IBKE) with focusing on pairing-free IBC. We also review some applications of IBC such as mediated cryptography and attribute-based cryptography. We also review the definitions and preliminaries related to the contents of the thesis, including definitions of security models, hard problems, and some mathematical tools.

In Chapter 3, we review a paper by Boneh, Ding and Tsudik in which they presented identity-based mediated RSA encryption and signature systems (IB-mRSA). In these systems, the users are not allowed to decrypt/sign messages without the authorisation of a security mediator. We show that IB-mRSA is insecure and we present a secure modified version of it which is as efficient as the original system. We also propose a generic mediated encryption (GME) that converts any IBE to a mediated version of this IBE. It envelops an IBE encrypted message using a user's identity into an IBE envelope using the identity of the SEM. We present two security models based on the role of the adversary whether it is a revoked user or a hacked SEM. We prove that GME is as secure as the SEM's IBE against a revoked user and as secure as the user's IBE against a hacked SEM. We also present two implementations of GME based on Boneh-Franklin FullIdent which is a pairing-based IBE and a BGH AnonIBE which is a pairing-free IBE.

In Chapter 4, we review two IBE systems presented by Boneh, Gentry and Hamburg (BasicIBE and AnonIBE). These systems have short ciphertext of $\log_2 N$ plus $2l$ bits for BasicIBE and $\log_2 N$ plus $l + 1$ bits for AnonIBE. But this comes at the cost of less time-efficient algorithms in which their processing time increases drastically with the message length. In addition, the private key of these systems has l elements in $\mathbb{Z}_{\mathbb{N}}$. In this chapter, we optimise these systems in two steps. First, we decrease the private key length from l elements in $\mathbb{Z}_{\mathbb{N}}$ to only one element. Second, we present two efficient variants of the these systems in terms of ciphertext length and encryption/decryption speed. The ciphertext is as short as the original systems, but with more time-efficient algorithms which do not depend on the message length. We prove that these variants are secure as the original ones.

In Chapter 5, we review an efficient variant of Boneh, Gentry Hamburg BasicIBE presented by Jhanwar and Barua (JB IBE). We prove that this IBE is not IND-ID-CPA secure and present a solution to the security flaw of this IBE. We also point

out a flaw in the security proof of JB IBE and propose a security proof for the fixed IBE. We prove that it has the same security as the original BasicIBE.

In Chapter 6, we present two ciphertext-policy attribute-based signcryption (CP-ABSC) systems which are efficient and fully secure. In addition to providing confidentiality, unforgeability and access control to the signcrypted data, one of the proposed ABSC systems is anonymous, i.e., an adversary cannot determine for which attributes or policies the message has been signcrypted. This feature is very useful especially when the signcrypted data are stored on a public cloud. As far as we know, this is the first CP-ABSC that has such a property. Our proposed ABSC systems are also time- and power-efficient because they do not depend on expensive pairing operations which make them suitable for mobile and lightweight devices. Our systems are fully secure under the quadratic residuosity (QR) assumption and provide a constant ciphertext size regardless of the number of attributes associated with the access structure.

In Chapter 7, we present a new security notion for key exchange (KE) protocols called Resiliency. That is, if a shared secret between designated parties is compromised or leaked, they can generate another completely new shared secret without the need to setup a new key exchange session. We present an identity-based authenticated key exchange protocol (IBAKE) that satisfies the resiliency security property. We prove that, if a shared secret SSK between two parties P_1 and P_2 is leaked, then they can safely generate another shared secret SSK_1 without the need to establish a new session. We adjust the unauthenticated adversarial model (UM) of the CK model to meet this security property and prove the security of the proposed protocol using the CK model based on the quadratic residuosity (QR) assumption.

Finally, we conclude the thesis in Chapter 8.

Chapter 2

Literature Review

2.1 Identity-Based Encryption

The notion of identity-based cryptography presented by Shamir [Sha84] is a type of public key cryptography in which the user's identity represents his public key and consequently, no public key certificate is required. Identity-based cryptography offers the advantage of simplifying public key management as it eliminates the need for public key certificates. In Shamir's seminal paper, he successfully designed an identity-based signature based on RSA, but he could not construct an identity-based encryption (IBE) using a similar approach since sharing a common modulus between different users makes RSA insecure. Designing an IBE was an open problem until Boneh and Franklin [BF01] proposed the first reliable and provable IBE, which is based on Weil pairings over elliptic curves. Cocks [Coc01] presented an IBE that is based on the factorisation of a composite integer. These cryptosystems opened a new era in cryptography.

Any IBE consists of four algorithms. *Setup*, *Extract*, *Encrypt*, and *Decrypt*.

- $(params, MS) \leftarrow Setup(k)$. A private key generator (PKG) takes a security parameter k and returns $params$, which are the system parameters of the IBE. The system parameters contain all the information to encrypt/decrypt a message for any user, such as the message space M and the ciphertext space C. The system parameters are made public. The PKG also generates a master secret (MS) that can be considered as a master key for the whole system and keeps it secret.

- $(d) \leftarrow Extract(params, MS, ID)$. The PKG takes the system parameters $params$, the master secret MS, and the identity of a user ID and produces a private key d for that user.

- $(C) \leftarrow Encrypt(params, ID, m)$. If Alice wants to encrypt a message to Bob, she uses Bob's ID and the system parameters $params$ to encrypt a message m. The resulted ciphertext C is sent to Bob.

- $(m) \leftarrow Decrypt(params, d, C)$. Bob uses his private key d and the system parameters $params$ to obtain the message m from the ciphertext C.

The security of IBE is based on hard problems. Hard problems are mathematical problems that are hard to solve, (i.e. it needs huge amounts of computation resources

and time to solve these problems). A famous example of these problems is integer factorisation: having a large composite integer N which equals to the product of two large primes of the same size p, q, (i.e. $N = pq$), it is hard to find the values of p and q. Other examples of these problems are the RSA problem [RSA83] and the quadratic residuosity (QR) problem [Coc01]. There are also problems that are based on Diffie-Hellman assumptions such as the Discrete Log (DL) problem, the Computational Diffie-Hellman (CDH) problem, the Decisional Diffie-Hellman (DDH) problem, and the Bilinear Diffie-Hellman (BDH) problem [Kat13].

To prove the security of an IBE, a game is played between an challenger $\mathcal{B}$, who wants to solve the hard problem and an adversary $\mathcal{A}$, who is challenged by $\mathcal{B}$ to break the IBE. This game between the challenger and the adversary is called security model. If $\mathcal{B}$ can simulate key and decryption queries (in the case of chosen-ciphertext attack (CCA)) successfully and $\mathcal{A}$ could break the IBE, then $\mathcal{B}$ can solve the hard problem. Because $\mathcal{B}$ cannot solve the hard problem, then $\mathcal{A}$ can not break the IBE. This way of proving the security of an IBE is called "reduction to contradiction". This game between the challenger and the adversary defines the resources available to the adversary to break the IBE, and what is the required task from the adversary to break the IBE. Next, we present an example of a security model called indistinguishability adaptive chosen-ciphertext attack (IND-ID-CCA2).

- *Setup.* The challenger $\mathcal{B}$ runs $Setup(k)$ for a security parameter k and gives the adversary $\mathcal{A}$ the resulting system parameters $params$. It keeps MS to itself. It sets the challenge ID ($ID^* \leftarrow \perp$) and challenge ciphertext ($C^* \leftarrow \perp$).

- *Query Phase* 1. The adversary $\mathcal{A}$ issues adaptive queries $q_1, q_2, ..., q(k)$ where q_i is one of,

  - *Private key query* (ID_i) where $ID_i \neq ID^*$. $\mathcal{B}$ responds by running *Extract* $(params, MS, ID_i)$ and sending the corresponding private key (d_i) to the adversary $\mathcal{A}$.
  - *Decryption query* (ID_i, C_i) where $(ID_i, C_i) \neq (ID^*, C^*)$. $\mathcal{B}$ responds by first running *Extract* $(params, MS, ID_i)$ to get d_i, and then running *Decrypt* $(params, d_i, C_i)$ and sending the corresponding plaintext (m_i) to the adversary $\mathcal{A}$.

- When the adversary $\mathcal{A}$ is satisfied with his queries, he sends two equal length messages m_0, m_1 to the challenger $\mathcal{B}$, then $\mathcal{B}$ tosses a fair coin $b \in \{0, 1\}$ and sets,

$$C^* = Encrypt(params, ID^*, m_b^*),$$

  and sends C^* to $\mathcal{A}$.

- *Query Phase* 2. After receiving C^*, the adversary $\mathcal{A}$ makes another adaptive queries like before.

- *Guess*. Eventually, the adversary $\mathcal{A}$ outputs a guess $\overline{b} \in \{0, 1\}$. $\mathcal{A}$ wins if $b = \overline{b}$. We define $A's$ advantage in breaking an IBE ξ as,

$$IBEadv_{A,\xi} = |\Pr[b = \overline{b}] - \tfrac{1}{2}|.$$

If $\mathcal{A}$ submits two pairs of (ID_0, m_0) and (ID_1, m_1) in the challenge phase and $\mathcal{A}$ must correctly guess ID^* and m^*, then this game is called anonymous indistinguishability adaptive chosen-ciphertext attack (ANON-IND-ID-CCA2) security model. The advantage of the adversary winning this game is the same as above. Any security model defines two properties of the adversary.

- The attack model, which defines the resources available for the adversary to break the IBE. If the adversary has no decryption service, this game is chosen plaintext attack (CPA). If the adversary has decryption service only before receiving the challenge ciphertext, this game is chosen ciphertext attack (CCA or CCA1), and if the adversary has decryption service before and after receiving the challenge ciphertext like the previously mentioned security model, this adversary is adaptive chosen ciphertext attack (CCA2) [Kat13]. Obviously, the more resources are available to the adversary, the more secure the IBE is.

- Security goals, which define the objective of the adversary to break the IBE. There are four essential security goals which are,

  - One-wayness (OW). Given the challenge ciphertext, the adversary is required to find the message [GM84]. This notion of security is considered the weakest security notion.
  - Semantic Security (SS). Given the challenge ciphertext, the adversary is required to find any priori information about the plaintext. This notion of security was proposed by Goldwasser and Micali in [GM84]. Any probabilistic encryption is semantically secure with respect to a passive attacker.
  - Non-malleability (NM). Given the challenge ciphertext, the adversary is required to alter this ciphertext to another one. The new ciphertext when decrypted gives another message designed by the adversary [DDN91]. For example, a ciphertext of a malleable IBE can be altered from being the encryption of "please send one thousand dollars to Bob" to become the encryption of "please send one million dollars to Bob"!!.
  - indistinguishability (IND). Given two different messages m_0 and m_1, the challenger chooses one of them randomly and sends the challenge ciphertext to the

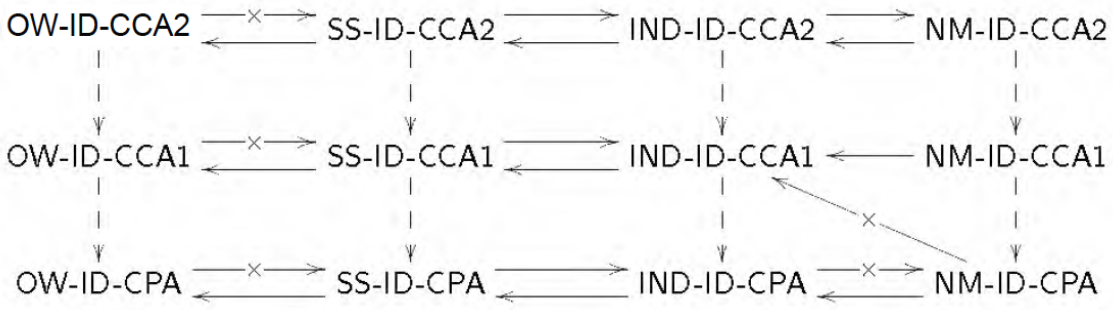

Figure 2.1: The Relations Between Security Notions for IBE

adversary, the adversary is required to guess which message is the origin of the challenge ciphertext [ACG+06].

The relations between security notions for IBE is shown in Figure 2.1. The arrows in Figure 2.1 in the form of $A \rightarrow B$ indicate that if the system is secure based on the security notion A, then it is also secure based on the the security notion B. Identity-based encryption can be classified based on its structure to pairing-based identity-based encryption and pairing-free identity-based encryption.

2.1.1 Identity-Based Encryption Based on Pairings

A symmetric pairing is a bilinear map $\hat{e} : \mathbb{G}_1 \times \mathbb{G}_1 \rightarrow \mathbb{G}_2$ where $\mathbb{G}_1$ is an additive cyclic group and $\mathbb{G}_2$ is a multiplicative cyclic group. All these groups are of prime order p. Let $P, Q \in \mathbb{G}_1$ be generators of $\mathbb{G}_1$. $\hat{e}$ is called an admissible pairing if $\hat{e} : \mathbb{G}_1 \times \mathbb{G}_1 \rightarrow \mathbb{G}_2$ is a map with the following properties.

- Bilinear. $\hat{e}(aP, bQ)=\hat{e}(P, Q)^{ab}$ for all $P, Q \in \mathbb{G}_1$ and all $a, b \in \mathbb{Z}$.
- Non-degenerate. $\hat{e}(P, Q) \neq 1$ for all $P, Q \in \mathbb{G}_1$.
- Computable. There is an efficient algorithm to compute $\hat{e}(P, Q)$ for any $P, Q \in \mathbb{G}_1$.
- Symmetric. $\hat{e}(P, Q) = \hat{e}(P, Q)$ for any $P, Q \in \mathbb{G}_1$.

Examples of these bilinear pairings are Weil and Tate pairings [Kat13]. In the following, we review some IBE systems based on pairing.

Boneh and Franklin [BF01] proposed the first reliable IBE systems based on pairings. In their paper, they proposed two IBE systems, BasicIdent which is IND-ID-CPA secure under the BDH assumption and FullIdent which is IND-ID-CCA2 secure under the same assumption. Both IBE systems are secure in the random oracle model, in which the used hash functions are assumed to be completely randomising functions (i.e. the relation between the input and output cannot be obtained). The ciphertext size of FullIdent is $2k + 2l$, where k is the size of the prime

defining the underlying elliptic curve, and l is the message length. FullIdent uses one pairing operation and two group exponentiations in $\mathbb{G}_1$ during encryption and one pairing operation and one group exponentiation in $\mathbb{G}_1$ during decryption. The security of Boneh-Franklin IBE systems are based on the Bilinear Diffie-Hellman (BDH) assumption which is based on the following definitions.

Definition 2.1. *Bilinear Diffie-Hellman (BDH) Parameter Generator. A randomised algorithm $\mathcal{IG}$ is a BDH parameter generator if $\mathcal{IG}$ takes a security parameter $k > 0$, runs in time polynomial in k and outputs the description of two groups $\mathbb{G}_1$ and $\mathbb{G}_2$ of the same prime order q and the description of an admissible pairing $\hat{e} : \mathbb{G}_1 \times \mathbb{G}_1 \to \mathbb{G}_2$.*

Definition 2.2. *BDH Problem. Given a randomly chosen $P \in \mathbb{G}_1$ as well as aP, bP and cP (for unknown randomly chosen $a, b, c \in \mathbb{Z}_q$), compute $\hat{e}(P, P)^{abc}$.*

For the BDH problem to be hard, $\mathbb{G}_1$ and $\mathbb{G}_2$ must be chosen so that there is no known algorithm for efficiently solving the Diffie-Hellman problem in either $\mathbb{G}_1$ or $\mathbb{G}_2$.

Definition 2.3. *BDH Assumption. If $\mathcal{IG}$ is a BDH parameter generator, the advantage $Adv_{\mathcal{G}}(B)$ of algorithm B in solving the BDH problem is defined to be the probability that the algorithm B outputs $\hat{e}(P, P)^{abc}$ when the inputs to the algorithm are $\mathbb{G}_1$, $\mathbb{G}_2$, $\hat{e}$, aP, bP and cP where $\mathbb{G}_1$, $\mathbb{G}_2$ and $\hat{e}$ are $\mathcal{IG}$'s output for large enough security parameter k, P is a random generator of $\mathbb{G}_1$ and a, b, c are random elements of $\mathbb{Z}_q$. The BDH assumption is that $Adv_{\mathcal{IG}}(B)$ is negligible for all efficient algorithms B.*

The structure of BF FullIdent is as follows.

- $(params) \leftarrow Setup(k)$. The public key generator (PKG) runs $\mathcal{IG}$ on input k to generate groups $\mathbb{G}_1$, $\mathbb{G}_2$ of some prime order q and an admissible pairing $\hat{e} : \mathbb{G}_1 \times \mathbb{G}_1 \to \mathbb{G}_2$. It picks an arbitrary generator $P \in \mathbb{G}_1$ and a master secret $s \in \mathbb{Z}_q$ and sets $P_{pup} = sP$ and chooses cryptographic hash functions $H_1\{0,1\}^* \to \mathbb{G}_1$, $H_2 : \mathbb{G}_1 \to \{0,1\}^n$, $H_3 : \{0,1\}^n \times \{0,1\}^n \to \mathbb{Z}_q$ and a hash function $H_4 : \{0,1\}^n \to \{0,1\}^n$ for some n. The system parameters are $params = (\mathbb{G}_1, \mathbb{G}_2, \hat{e}, Q, H_1, H_2, H_3, H_4)$. The message space is $\mathcal{M} = \{0,1\}^n$. The master secret is $s \in \mathbb{Z}_q$.

- $(d) \leftarrow Extract(ID, s)$. For a given string $ID \in \{0,1\}^*$, the PKG computes $Q = H_1(ID)$ and sets the private key $d = sQ$.

- $(C) \leftarrow Encrypt(params, ID, m)$. To encrypt a message m for a user with an identity ID, compute $Q = H_1(ID)$ and choose a random $\sigma \in \{0,1\}^n$ and set

$r = H_3(\sigma, m)$. The ciphertext C is,

$$C = \langle rP, \sigma \oplus H_2(g^r), m \oplus H_4(\sigma))\rangle,$$

where $g = \hat{e}(Q, P_{pub})$.

- $(C) \leftarrow Decrypt(params, ID, C)$. To decrypt $C = \langle U, V, W\rangle$ for a user with identity ID, the user computes $V \oplus H_2(\hat{e}(d, U)) = \sigma$ and $W \oplus H_4(\sigma) = m$ and sets $r = H_3(\sigma, m)$. He outputs m as a decryption of C if $U = rP$.

A symmetric encryption E can be used instead of Xor to encrypt the message m [BF01].

Galindo found a flaw in the security proof of Boneh-Franklin IBE systems [Gal05]. He observed that the original argument does not take into account the fact that the decryption algorithm performs a ciphertext integrity check before returning the message. In the same paper, he suggested a suitable modification of the simulation to fix this flaw.

Boneh and Franklin used Fujisaki-Okamoto generic transformation [FO13] to build FullIdent. This transformation is used to convert weak encryption IBE systems to strong IND-ID-CCA2 secure IBE systems. The security of this transformation is based on the random oracle model. This transformation based on the idea of hybrid encryption, i.e. it is based on symmetric and asymmetric encryption. The formula of this transformation can be expressed as,

$$\xi_{pk}^{hyp} = \xi_{pk}^{asym}(\sigma; H(\sigma, m)) \| \xi_{G(\sigma)}^{sym}(m),$$

where,

1. ξ_{pk}^{hyp}. An IND-ID-CCA2 secure hybrid encryption.
2. σ. A random integer chosen from a suitable domain.
3. ξ_{pk}^{asym}. A weak asymmetric encryption.
4. $\xi_{G(\sigma)}^{sym}$. A symmetric encryption.
5. G, H. Hash functions.

Jean-Sebastien Coron presented a variant of Boneh-Franklin IBE with a tight security reduction in the random oracle model [Cor09]. The security proof was based on D-Square-BDH assumption [Cor09]. Although the security reduction is tight, it is less efficient than Boneh-Franklin IBE. The ciphertext size is $3k + 2l$ bits, and it requires one pairing operation and three group exponentiations in $\mathbb{G}$ during encryption/decryption.

All the previously mentioned IBE systems are secure under the random oracle model. Brent Waters [Wat05] proposed an IBE that is CPA secure without the random oracle model. This IBE is secure under the decisional BDH assumption. The ciphertext size is $2k + l$ bits. It requires four group exponentiations in $\mathbb{G}$ to encrypt a message and two pairing operations to decrypt it. This IBE has a drawback of not having a tight security reduction.

Another IBE that is secure without the random oracle model is the one proposed by Gentry [Gen06]. This IBE is secure under decisional augmented bilinear Diffie-Hellman exponent assumption (decisional ABDHE), which is not a standard assumption. Although it is IND-ID-CCA2 secure with a tight security reduction, it is less efficient than the previous IBE systems. The ciphertext size is $5k + l$ bits. It requires six group exponentiations in $\mathbb{G}$ to encrypt a message and three group exponentiations in $\mathbb{G}$ and two pairing operations to decrypt it.

2.1.2 Identity-Based Encryption Without Pairings

Although most of the work done in IBE is based on pairings, there are papers that proposed IBE systems based on number theory. These IBE systems are simpler than the ones based on pairings. But on the other hand, the ciphertext size is space-inefficient. We believe that this topic needs a lot of research and that is why we decided to work on this area.

Next, we present some definitions related to IBE systems without pairings, then we review some of these systems.

Definition 2.4. *Legendare Symbol. For any integer a and any prime p, the Legendre symbol is defined as:*

$$\left(\frac{a}{p}\right) = a^{(\frac{p-1}{2})} \pmod{p},$$

where,

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & \text{if } a \equiv 0 \pmod{p} \\ 1 & \text{if } x^2 \equiv a \pmod{p} \text{ has a solution} \\ -1 & \text{if there is no such } x. \end{cases}$$

Definition 2.5. *Jacobi Symbol. For any integer a and any positive odd integer $N = pq$ where p, q are primes, the Jacobi symbol is defined as the product of the Legendre symbols of a w.r.t. $p, q,$. i.e.*

$$\left(\frac{a}{N}\right) = \left(\frac{a}{p}\right)\left(\frac{a}{q}\right).$$

Definition 2.6. *Quadratic Residue. For a positive integer N, define the following set.*

$$J(N) = [a \in \mathbb{Z}_{\mathbb{N}} : \left(\frac{a}{N}\right) = 1],$$

where $\left(\frac{a}{N}\right)$ *is the Jacobi symbol of a w.r.t N [Coc01]. The quadratic residue set* $QR(N)$ *is defined as follows,*

$$QR(N) = [a \in \mathbb{Z}_{\mathbb{N}} : gcd(a, N) = 1 \wedge x^2 \equiv a \pmod{N} \text{ has a solution}].$$

Definition 2.7. *Quadratic Residuosity Assumption. Let RSAgen(*λ*) be a probabilistic polynomial time (PPT) algorithm. This algorithm generates two equal size primes* p, q*. The QR assumption holds for RSAgen if it cannot distinguish between the following two distributions for all PPT algorithms* $\mathcal{A}$*.*

$$P_{QR}(\lambda) : (N, V)(p, q) \leftarrow RSAgen(\lambda), N = pq, V \in_R QR(N),$$
$$P_{NQR}(\lambda) : (N, V)(p, q) \leftarrow RSAgen(\lambda), N = pq, V \in_R J(N) \setminus QR(N).$$

In other words, the advantage of $\mathcal{A}$ *against QR assumption* $QRAdv_{\mathcal{A},RSAgen(\lambda)} =$

$$|\Pr[(N, V) \leftarrow P_{QR}(\lambda) : \mathcal{A}(N, V) = 1]| - |\Pr[(N, V) \leftarrow P_{NQR}(\lambda) : \mathcal{A}(N, V) = 1]|$$

is negligible. i.e. $\mathcal{A}$ *cannot distinguish between elements in* $J(N) \setminus QR(N)$ *and elements in* $QR(N)$*.*

Definition 2.8. *Interactive Quadratic Residuosity Assumption. Let H be a collision free hash function such that* $H : [0, 1]^* \rightarrow J(N)$*. Let* $\mathcal{O}$ *be a square root oracle that picks* $u_N \leftarrow J(N) \setminus QR(N)$ *and maps input pair* (N, x) *to one of* $H_N(x)^{\frac{1}{2}}$ *or* $(u_N H_N(x))^{\frac{1}{2}}$ *in* $\mathbb{Z}_{\mathbb{N}}$ *based on which value is quadratic residue. The interactive quadratic residue (IQR) assumption holds for the pair* $(RSAgen, H)$ *if for all PPT algorithms* $\mathcal{A}$*, the function* $IQRAdv_{\mathcal{A},(RSAgen(\lambda),H)} =$

$$|\Pr[(N, V) \leftarrow P_{QR}(\lambda) : \mathcal{A}^{\mathcal{O}}(N, V) = 1]| - |\Pr[(N, V) \leftarrow P_{NQR}(\lambda) : \mathcal{A}^{\mathcal{O}}(N, V) = 1]|$$

is negligible. $IQRAdv_{\mathcal{A},(RSAgen(\lambda),H)}$ *is the IQR advantage of* $\mathcal{A}$ *against* $(RSAgen, H)$*.*

In 2001, Clifford Cocks [Coc01] presented the first IBE based on quadratic residue [Coc01, BGH07]. The structure of Cock's IBE is as follows.

- $(N, u, MS) \leftarrow Setup(k)$. A private key generator (PKG) takes a security parameter k and returns $N = pq$, where p and q are primes. It also generates a random variable $u \in J(N) \backslash QR(N)$ and a hash function H that maps an identity to a number in $J(N)$. The master secret MS parameters are p and q.

- $(d) \leftarrow Extract(N, u, MS, ID)$. To generate the private key d for a user with identity ID, the PKG calculates $R = H(ID)$ and uses its master secret (p, q) to determine if R is quadratic residue modulo N or not. If $R \in QR(N)$, then it sets $d^2 = R$. If $R \in J(N) \backslash QR(N)$, then it sets $d^2 = uR$.

- $(C, \overline{C}) \leftarrow Encrypt(N, u, ID, m)$. To encrypt a message $m \in \{-1, +1\}^l$ for Bob's identity ID, Alice computes $R = H(ID)$ and chooses uniformly at random two independent values $\{t_1, t_2\} \in \mathbb{Z}_{\mathbb{N}}$ such that $\left(\frac{t_1}{N}\right) = \left(\frac{t_2}{N}\right) = m$ and then computes,

$$(c, \overline{c}) = (t_1 + \frac{R}{t_1} \pmod N, t_2 - \frac{R}{t_2} \pmod N).$$

  Because Alice cannot determine if R is quadratic residue modulo N or not, she sends both $(c, \overline{c})$ to Bob. She repeats this process for encrypting the whole message. The ciphertext is $(C, \overline{C})$ where $C = \{c_0, c_1, ..., c_{l-1}\}$ and $\overline{C} = \{\overline{c}_0, \overline{c}_1, ..., \overline{c}_{l-1}\}$ where l is the message length.

- $m \leftarrow Decrypt(N, u, d, C, \overline{C})$. For Bob to decrypt a ciphertext $(c, \overline{c}) \in \mathbb{Z}_{\mathbb{N}}$ sent by Alice, he uses his private key d to check if R is quadratic residue modulo N or not. If $d^2 = R \in QR(N)$, he sets $s = c$ and $\overline{c}$ is discarded, and if $d^2 = uR \in QR(N)$, he sets $s = \overline{c}$ and c is discarded. Then he calculates $m \in \{-1, +1\}$ as follows.

$$m = \left(\frac{s + 2d}{N}\right).$$

Bob repeats this process until the whole message is recovered. To prove the correctness of Cock's IBE, let $s = c$, then,

$$\left(\frac{s + 2d}{N}\right) = \left(\frac{t_1 + \frac{R}{t_1} + 2d}{N}\right) = \left(\frac{t_1}{N}\right)\left(\frac{1 + \frac{d^2}{t_1^2} + \frac{2d}{t_1}}{N}\right),$$
$$= \left(\frac{t_1}{N}\right)\left(\frac{(1 + \frac{d}{t_1})^2}{N}\right) = \left(\frac{t_1}{N}\right) = m.$$

Although Cock's IBE is very efficient in terms of speed, it is very expensive w.r.t ciphertext size. For each $m \in \{1, -1\}$, Alice sends two elements in $\mathbb{Z}_{\mathbb{N}}$. For a message of l bits, Alice sends $2l \log(N)$ bits of ciphertext. Cock's IBE is IND-ID-CPA secure under the random oracle model.

The concept of key-privacy or anonymity in PKC was first presented by Bellare *et al.* [BBDP01]. It requires that the adversary in possession of a ciphertext not to find the public key for which the ciphertext is encrypted. Boyen and Waters [BW06] proposed a hierarchical IBE that features fully anonymous ciphertexts. It is secure in the standard model based on the mild decision linear complexity assumption. Ateniese and Gasti proposed an IBE that is universally anonymous variant of Cock's IBE [AG09]. The idea of universally anonymous cryptosystems was firstly proposed by Hayashi and Tanaka [HT05] in which any one can hide the identity of the sender if required without affecting the decryption process. This is useful

in some applications, for example, in a company in which it may be required for the internal emails not to be anonymous, but when the emails are routed outside the company, a router can make it anonymous. To make the IBE IND-ID-CCA2 secure under the random oracle model, the authors consider the hybrid encryption proposed by Cramer and Shoup in [CS98, CS03] and Shoup [Sho01]. The hybrid encryption proposed by Cramer and Shoup consists of two parts, key encapsulation mechanism (KEM) used to encrypt the key of the symmetric encryption, and data encapsulation mechanism (DEM) used to encrypt the data using the symmetric encryption. In [CS03], Cramer and Shoup proved that this hybrid encryption is secure if the KEM component is IND-ID-CCA2 secure and the DEM component is IND-ID-CCA2-secure one-time symmetric encryption. Later, Desmedt *et al.* proved that the KEM component doesn't have to be IND-ID-CCA2 secure [DGKS10]. So, their construction can be used efficiently to convert an IND-ID-CPA IBE like Cock's to an IND-ID-CCA2 secure IBE. The efficiency of Ateniese and Gasti IBE is comparable to Cock's IBE, so it is not efficient in terms of ciphertext size.

Boneh, Gentry and Hamburg (BGH) proposed space-efficient IBE systems without pairings [BGH07]. They proposed two IBE systems in this paper, an abstract IBE (BasicIBE) and an anonymous IBE (AnonIBE).

These systems depend mainly on solving equations in the form $Rx^2 + Sy^2 \equiv 1 \pmod{N}$. Next, we discuss how Boneh *et al.* [BGH07] employed a lattice based algorithm of Cremona-Rusin [CR03] to solve such equations, then we explain the full structure of BGH systems. First we describe a little about finding rational solutions to rational conics.
Consider the following equation,

$$aX^2 + bY^2 + cZ^2 = 0, \tag{2.1}$$

where a, b, c are non-zero integers. We discuss a method to find rational solution to equation 2.1.

Definition 2.9. *Solubility Certificate. A triple $(k_1, k_2, k_3) \in \mathbb{Z}^3$ is called a solubility certificate for equation 2.1 if it is a solution to the following congruences,*

$$X_1^2 \equiv bc \pmod{a} \quad X_2^2 \equiv ca \pmod{b} \quad X_3^2 \equiv ab \pmod{c}. \tag{2.2}$$

Theorem 2.1. *Let a, b and c be nonzero integers with abc square-free, not all of the same sign. Then equation 2.1 has a rational solution iff a solubility certificate exists.*

If a, b and c are pairwise co-prime (but not necessarily square-free), then the existence of a solubility certificate is sufficient, but no longer necessary, for the

existence of a rational solution to equation 2.1. So given a solubility certificate, theorem 2.1 confirms the existence of a rational solution to equation 2.1 . What about an integer solution? The following important theorem due to Holzer [JB08] says that:

Assuming equation 2.1 is soluble, there exists an integral solution (x, y, z) with,

$$\max(|a|x^2, |b|y^2, |c|z^2) \leq |abc| \tag{2.3}$$

Cremona-Rusin [CR03] gave an efficient lattice-based algorithm to find integer solution to equation 2.1. They associated to the triple of coefficients (a, b, c) and the solubility certificate (k_1, k_2, k_3) a 3-dimensional sub-lattice $\mathfrak{L} = \mathfrak{L}(a, b, c; k_1, k_2, k_3)$ of $\mathbb{Z}^3$. They show that for $(x, y, z) \in \mathfrak{L}, ax^2 + by^2 + cz^2 \equiv 0 \pmod{2abc}$ and apply a theorem of Gauss [BJ10] to assert the existence of a point $(x, y, z) \in \mathfrak{L}$ with $|ax^2 + by^2 + cz^2| < 2|abc|$. This gives a integer solution to equation 2.1. Now to find $(x, y, z) \in \mathfrak{L}$ which satisfies $|ax^2 + by^2 + cz^2| < 2|abc|$, Cremona-Rusin applies an LLL algorithm.

Now, consider the following ternary quadratic equation,

$$\hat{R}x^2 + \hat{S}y^2 - z^2 = 0, \tag{2.4}$$

where $\hat{R}, \hat{S}, x, y, z \in \mathbb{Z}$ and $\hat{R} \equiv R \pmod N, \hat{S} \equiv S \pmod N$. Clearly a solution to equation 2.4 in $\mathbb{Z}$ gives a solution to $Rx^2 + Sy^2 \equiv 1 \pmod N$ in $\mathbb{Z}_N$. So we can call Cremona-Rusin algorithm to solve equation 2.4. We can provide a solubility certificate for equation 2.4 by looking at equation 2.2. We can see that this is amount to solving the following,

$$r^2 \equiv \hat{R} \pmod{\hat{S}} \quad \text{and} \quad s^2 \equiv \hat{S} \pmod{\hat{R}}. \tag{2.5}$$

To solve this we need to generate $\hat{R}$ and $\hat{S}$ in the arithmetic progressions $\hat{R} \equiv R \pmod N, \hat{S} \equiv S \pmod N$ as primes. There lies the reason behind the slower encryption algorithm.

After reviewing how to solve equations in the form $Rx^2 + Sy^2 \equiv 1 \pmod N$, BasicIBE is explained as follows. It encrypts an l-bit message $m \in \{1, -1\}^l$ using a square $S \equiv s^2 \pmod N$ where $s \in_R \mathbb{Z}_{\mathbb{N}}$, the user's identity ID and a pair of Jacobi symbols for each bit. It first hashes ID to different values $H(ID, i) = u^a R_i = r_i^2$ where $a \in \{0, 1\}$, $u \in J(N) \setminus QR(N)$ and i is the bit index. Then it solves the equations $R_i x_i^2 + Sy_i^2 \equiv 1 \pmod N$ and $uR_i\overline{x}_i^2 + S\overline{y}_i^2 \equiv 1 \pmod N$ to get $(x_i, y_i, \overline{x}_i, \overline{y}_i)$. The ciphertext C is $(S, c, \overline{c})$ where $c \leftarrow [c_0, c_1, c_2, ..., c_{l-1}]$, $c_i = m_i \cdot \left(\frac{2+2y_i s}{N}\right)$ and $\overline{c} \leftarrow [\overline{c}_0, \overline{c}_1, \overline{c}_2, ..., \overline{c}_{l-1}]$, $\overline{c}_i = m_i \cdot \left(\frac{2+2\overline{y}_i s}{N}\right)$ where $(c_i, m_i) \in \{1, -1\}$. To decrypt, one needs to know the square-root of R_i or uR_i. If $R_i = r_i^2$, the message

is $m_i = c_i \cdot \left(\frac{1+x_i r_i}{N}\right)$ and if $uR_i = r_i^2$, the message is $m_i = \overline{c}_i \cdot \left(\frac{1+\overline{x}_i r_i}{N}\right)$. The full structure of BasicIBE is explained as follows,

- $(params) \leftarrow Setup(\lambda)$. Using RSAgen($\lambda$), generate ($p$, q), calculate the modulus $N \leftarrow pq$, choose $u \in J(N) \setminus QR(N)$, and choose a hash function $H : ID \rightarrow J(N)$. The public parameters $params$ are $[N, u, H]$. The master secret MS parameters are p, q and a secret key K for a pseudorandom function (PRF) $F_K : ID \rightarrow [0, 1, 2, 3]$.

- $(r_i) \leftarrow Extract(MS, ID, l)$. Calculate $R_i \leftarrow H(ID, i) \in J(N)$ for each bit i and $w \leftarrow F_K(ID) \in \{0, 1, 2, 3\}$. Choose $a \in \{0, 1\}$ such that $u^a R_i \in QR(N)$. Let $[z_0, z_1, z_2, z_3]$ be the four square roots of $u^a R_i \in \mathbb{Z}_{\mathbb{N}}$, then $r_i \leftarrow z_w$.

- $(C) \leftarrow Encrypt(params, ID, m)$. To encrypt a message $m \in \{-1, 1\}^l$, calculate $R_i \leftarrow H(ID, i) \in J(N)$ for each bit i and choose a random value $s \in_R \mathbb{Z}_{\mathbb{N}}$ and calculate $S = s^2$. Then calculate $[x_i, y_i, \overline{x}_i, \overline{y}_i]$, $i \in [0, l-1]$ that satisfy the following equations.

$$[x_i, y_i] \leftarrow R_i x_i^2 + S y_i^2 \equiv 1 \pmod{N}\ ,\ [\overline{x}_i, \overline{y}_i] \leftarrow u R_i \overline{x}_i^2 + S \overline{y}_i^2 \equiv 1 \pmod{N}.$$

  The message $m \leftarrow [m_0, m_1, ..., m_{l-1}]$ is encrypted using the following equation.

$$c_i \leftarrow m_i \cdot \left(\frac{2y_i s + 2}{N}\right)\ ,\ \overline{c}_i \leftarrow m_i \cdot \left(\frac{2\overline{y}_i s + 2}{N}\right).$$

  The ciphertext is $C = (S, c, \overline{c})$ where $c = \{c_0, c_1, ..., c_{l-1}\}$ and $\overline{c} = \{\overline{c}_0, \overline{c}_1, ..., \overline{c}_{l-1}\}$.

- $(m) \leftarrow Decrypt(params, ID, C)$. To decrypt a ciphertext $C = (S, c, \overline{c})$ for a user with an identity ID, the user calculates $m_i \in \{1, -1\}$ as follows.

$$m_i \leftarrow c_i \cdot \left(\frac{x_i r_i + 1}{N}\right) \quad \text{if } r_i^2 = R_i\ ,\ m_i \leftarrow \overline{c}_i \cdot \left(\frac{\overline{x}_i r_i + 1}{N}\right) \quad \text{if } r_i^2 = uR_i.$$

AnonIBE is similar to BasicIBE. The only difference is in the equations needed to encrypt or decrypt messages. Instead of encrypting/decrypting messages by solving $2l$ equations in the form $u^a R_i x_i^2 + S y_i^2 \equiv 1 \pmod{N}$, AnonIBE solves l equations in the form $R_i x_i^2 + S y_i^2 \equiv 1 \pmod{N}$ and an equation in the form $u\alpha^2 + S\beta^2 \equiv 1 \pmod{N}$. That is why the ciphertext length of AnonIBE is smaller than BasicIBE by $l-1$ bits. The ciphertext is (S, T, c) where $c \leftarrow [c_0, c_1, c_2, ..., c_{l-1}]$, $c_i = m_i \cdot \left(\frac{2+2y_i s}{N}\right)$ and $T = \left(\frac{1+\beta s}{N}\right)$. To decrypt, if $R_i = r_i^2$, the message is $m_i = c_i \cdot \left(\frac{1+x_i r_i}{N}\right)$ and if $uR_i = r_i^2$, the message is $m_i = c_i \cdot \left(\frac{1+\alpha x_i r_i + S y_i \beta}{N}\right) \cdot T$. The structure of AnonIBE is as follows.

- The *Setup* and *Extract* algorithms are the same as BasicIBE.
- $(C) \leftarrow Encrypt(params, ID, m)$. To encrypt a message $m \in \{-1, 1\}^l$, calculate $R_i \leftarrow H(ID, i) \in J(N)$ for each bit i and choose a random value $s \in_R \mathbb{Z}_{\mathbb{N}}$ and calculate $S = s^2$. Then calculate $[x_i, y_i, \alpha, \beta]$, $i \in [0, l-1]$ that satisfy the following equations.

$$[x_i, y_i] \leftarrow R_i x_i^2 + S y_i^2 \equiv 1 \pmod{N}\ ,\ [\alpha, \beta] \leftarrow u\alpha^2 + S\beta^2 \equiv 1 \pmod{N}.$$

  The message $m \leftarrow [m_0, m_1, ..., m_{l-1}]$ is encrypted using the following equation.

$$c_i \leftarrow m_i \cdot \left(\frac{2y_i s + 2}{N}\right)$$

  The ciphertext C is (S, T, c) where $T = \left(\frac{\beta s+1}{N}\right)$ and $c = [c_0, c_1, ..., c_{l-1}]$.
- $(m) \leftarrow Decrypt(params, ID, C)$. To decrypt a ciphertext $C = (S, T, c)$ for a user with identity ID, calculate m_i as follows.

$$m_i \leftarrow c_i \cdot \left(\frac{x_i r_i + 1}{N}\right) \text{ if } r_i^2 = R_i\ ,\ m_i \leftarrow c_i \cdot \left(\frac{1 + S y_i \beta + \alpha x_i r_i}{N}\right) \cdot T \text{ if } r_i^2 = uR_i.$$

- **Remarks**. BasicIBE has to solve $2l$ equations in the form $R_i x^2 + S y^2 \equiv 1 \pmod{N}$ to encrypt/decrypt a message m of length l by computing pairs (x_i, y_i), $(\overline{x}_i, \overline{y}_i) \in \mathbb{Z}_{\mathbb{N}}{}^2$. Boneh, Gentry and Hamburg presented a product formula which only solves $l + 1$ equations to encrypt/decrypt a message [BGH07].

  Lemma 2.1. *For $i = 1, 2$ let (x_i, y_i) be a solution to $R_i x^2 + S y^2 \equiv 1 \pmod{N}$. Then (x_3, y_3) is a solution to*

$$R_1 R_2 x^2 + S y^2 \equiv 1 \pmod{N},$$

  where $x_3 = \frac{x_1 x_2}{S y_1 y_2 + 1}$ and $y_3 = \frac{y_1 + y_2}{S y_1 y_2 + 1}$.

  During encryption/decryption, BasicIBE solves the following equations.

$$R_i x_i^2 + S y_i^2 \equiv 1 \pmod{N} \text{ and } ux^2 + Sy^2 \equiv 1 \pmod{N},$$

  and then uses Lemma 2.1 to find solutions to $uR_i \overline{x}_i^2 + S\overline{y}_i^2 \equiv 1 \pmod{N}$.
- The equation $Rx^2 + Sy^2 \equiv 1 \pmod{N}$ has $N - 1$ solutions if $R, S \in QR(N)$ [BJ10]. A BGH IBE must generate (x_i, y_i) such that $x_i \neq x_j$ and $y_i \neq y_j$ for $i \neq j$ to avoid using the same key for encryption/decryption. If $x_i = x_j$ or $y_i = y_j$ for $i \neq j$, this IBE must search for another solution to avoid this equality.

Table 2.1: Comparison Between Different IBE Systems

Systems	Pairings	Assumption	IND-ID-X	ROM	Ciphertext Size	Complex Operations
BF [BF01]	Yes	BDH	CCA	Yes	$2k + 2l$	1P+2E
JSC [Cor09]	Yes	D-Square-BDH	CCA	Yes	$3k + 2l$	1P+3E
Waters[Wat05]	Yes	DBDH	CPA	No	$2k + l$	0P+4E
Gentry[Gen06]	Yes	q_e-ABDHE	CCA	No	$5k + l$	0P+6E
Cocks[Coc01]	No	QR	CPA	Yes	$2l(\log N)$	0
BasicIBE [BGH07]	No	QR	CPA	Yes	$\log N + 2l$	$(l + 1)eq$
AnonIBE [BGH07]	No	QR	CPA	Yes	$\log N + l + 1$	$(2l + 1)eq$
JB [JB08]	No	QR	CPA	Yes	$2\sqrt{l} \log N + 2l$	0

- The secret key r is chosen randomly from the four square roots of $u^a R$ for $a \in \{0, 1\}$ using a deterministic function F to assure that the same key is sent to the sender for each key query. If a PKG sends randomly selected (not deterministic) square roots r_w, $w \in \{0, 1, 2, 3\}$ for each key query, the sender, with high probability, will receive the four square roots of $u^a R$ for $a \in \{0, 1\}$ and he will be able to factor N.

- AnonIBE can be proven secure in the random oracle model model based on the QR assumption or in the standard model based on the IQR assumption.

BGH IBE systems are IND-ID-CPA secure under the quadratic residuary assumption. The ciphertext size of BasicIBE is $\log(N) + 2l$ while AnonIBE has a ciphertext size of $\log(N) + l + 1$. Although BGH IBE systems are space-efficient compared to Cock's IBE, it is time-inefficient. Besides, the decryption key of the BGH IBE systems is l elements in $\mathbb{Z}_{\mathbb{N}}$.

A variant of BasicIBE was proposed by Jhanwar and Barua [JB08]. Jhanwar and Barua made some significant observations on the BGH IBE systems (for solving equations in the form $Rx^2 + Sy^2 \equiv 1 \pmod N$) and proposed a trade-off IBE that reduces the private key length but increases the ciphertext length [JB08]. They found that by knowing the value of $S \pmod N$, one can find a random solution to the equation $Rx^2 + Sy^2 \equiv 1 \pmod N$ using only one inversion in $\mathbb{Z}_{\mathbb{N}}$. The sender solves only $2\sqrt{l}$ equations in the form $Rx^2 + Sy^2 \equiv 1 \pmod N$ using only $2\sqrt{l}$ inversions in $\mathbb{Z}_{\mathbb{N}}$ and thus, no prime generation is required. This increases the encryption/decryption speed dramatically. The private key is only one element in $\mathbb{Z}_{\mathbb{N}}$. However, this IBE produces a large ciphertext of $2\sqrt{l}$ elements in $\mathbb{Z}_{\mathbb{N}}$.

Table 2.1 compares between the security and the performance of various IBE systems presented in this chapter. P denotes a pairing operation, and E a group exponentiation in G or G_1. k denotes the bit-size of p, l denotes the bit-size of the message space. Here p is the prime modulus used to define the underlying elliptic-curve. An element of G requires k bits (using point compression), whereas an element of G_1 requires $2k$ bits. eq denotes the number of solved equations in the form $Rx^2 + Sy^2 \equiv 1 \pmod N$.

2.2 Key Exchange Protocols

Another interesting cryptography application is key exchange (also called key agreement) protocol. Key exchange (KE) protocols are cryptographic tools that allow two or more parties to securely share a common secret via insecure or public networks such as the Internet. They are considered the cornerstones of establishing any secure communication channel. In the last four decades, KE protocols have been significantly designed and analysed for different network settings. Diffie-Hellman key exchange protocol (DH, for short) is the first and best-known key agreement protocol [DH76]. Suppose that Alice wants to share a symmetric encryption key with Bob using the DH protocol.

- Alice chooses a random value a and computes g^a, where g is a generator of a cyclic group $\mathbb{G}$, and sends g^a to Bob.
- Bob chooses a random value b and computes g^b, and sends it to Alice.
- Alice and Bob get the key by calculating $(g^b)^a = (g^a)^b = g^{ab}$.

The security of this protocol relies on the fact that, knowing any of g^a or g^b, no third party can get a or b (Discrete Log problem). Also, a third party cannot get g^{ab} from g^a and g^b (computational Diffie-Hellman problem). Later, this protocol was proven insecure because the links between the parties are not authenticated, and a man-in the-middle attack can be launched against the DH protocol.

A tripartite version of Diffie-Hellman key exchange protocol was proposed by Joux [Jou04]. His protocol is based on pairing. Suppose that three persons, Alice, Bob, and Eve, want to share a key.

- Each user of Alice, Bob, and Eve chooses a random value x_i, and calculates $X_i = P^{x_i}$ for a generator P and sends X_i to the other two.
- Each user calculates their shared key $\hat{e}(P,P)^{x_1x_2x_3} = \hat{e}(X_1,X_2)^{x_3} = \hat{e}(X_3,X_2)^{x_1} = \hat{e}(X_1,X_3)^{x_2}$

The security of Joux protocol is based on Bilinear Diffie-Hellman (BDH) assumption. Given $X_i = P^{x_i}, i = 1,2,3$, it is hard to calculate $\hat{e}(P,P)^{x_1x_2x_3}$.

The first identity-based key agreement protocol was proposed by Sakai and Kasahara [SK03]. Scott [Sco02] presented an ID-based key agreement protocol in which each party chooses his own personal identity number (PIN) and a reliable PKG gives each party a specific secret related to the identity of the corresponding party. A value is calculated from the secret and PIN and inserted into a hardware token. The party's secret can be calculated from their PIN, identity and token.

Authenticated key exchange (AKE) protocols permit a group of parties within a huge and fully insecure public network to form a shared secret key and guarantees each party that no other party apart from these parties can get a particular secret key. Over the past two decades, some security properties have been seen to be important in key agreement protocols and different protocols have been implemented in the literature. Examples of these protocols are [ABB+04, BPR00, BR93, BR95, BCNP08, CK01, ISO09a, Oka07, YDW+11, YWWD08]. A comprehensive survey of KE protocols is presented in [DB05].

The concept of identity-based encryption was extended to AKE protocols to generate identity-based authenticated key exchange protocols (IBAKE). Smart [Sma01] presented a two-pass IBAKE based on Weil pairings and merges the ideas of Boneh and Franklin IBE [BF01] with tripartite DH protocol of Joux [Jou04]. The protocol obliges all parties involved in the key agreement to be members of the same PKG. The protocol permits efficient ID-based escrow ability for sessions that allow low enforcement agencies to decrypt messages encrypted with the session keys after obtaining the necessary licenses. Chen and Kudla [CK02] proposed an ID-based authenticated key agreement protocol, which is more efficient than Smart's protocol [Sma01]. They presented a technique to disable escrow, which is also applicable to Smart's protocol. The escrow-free setting may be necessary for private communications in which the parties request to retain the confidentiality of the messages even from the PKG. Chen and Kudla also presented an adjustment that permits key agreement between parties under different PKGs. Another efficient ID-based authenticated key agreement protocol was proposed by McCullagh and Barreto [MB05]. This protocol can be adjusted to work in either escrow or escrow-free mode. They also presented a key agreement protocol between clients of different PKGs. The protocol is twice as efficient as the protocol in [CK02] without pre-computation. None of the two-party key agreement protocols by Scott [Sco02], Smart [Sma01], Chen and Kudla [CK02] and McCullagh and Barreto [MB05] were broken, although heuristic arguments are assumed to prove their security against active adversary.

An authenticated multiple key exchange protocol is an AKE protocol in which multiple keys can be shared in each session. Harn and Lin [HL01] presented an authentication key exchange protocol in which two parties produce four shared keys each session, but only three keys can guarantee perfect forward secrecy. Afterwards, Hwang *et al.* [HSL03] presented an efficient authenticated multiple key exchange protocol. However, this protocol was proven insecure by Lee and Wu [LW04]. Lee *et al.* [LWW08] presented two multiple key exchange protocols in which one depends on elliptic curve cryptography (ECC) and the other is based on bilinear pairings. Nevertheless, Vo *et al.* [VLYK10] presented an impersonation attack on Lee *et al.*'s bilinear pairing-based authenticated multiple key exchange protocol and proposed

a simple modification to the protocol to withstand their attack.

Bellare and Rogaway were the first to propose a formal security model for AKE [BR93]. The Bellare-Rogaway (BR) model and its variants are considered nowadays the standard for the analysis of an AKE protocol security. One of the most used formal security model is the Canetti-Krawczyk (CK) model [CK01]. It combines between the BR model and the Bellare-Canetti-Krawczyk (BCK) model [BCK98]. In their security model, they use generic authenticators to transform any key exchange protocol vulnerable to a man-in-the-middle attack such as the DH protocol [DH76] to an AKE protocol secure against such attacks. Many practical AKE protocols, such as the internet key exchange (SIGMA) protocol [Kra03] were proven secure using the CK model. Yang *et al.* [YDW+11] proposed a variant of the CK model that takes into account AKE under bad randomness. Some generic protocols were also proposed for improving the security of current AKE protocols.

The CK model is defined based on the adversary. The adversary in this model can be classified as authenticated adversarial model (AM) and unauthenticated adversarial model (UM) [CK01].

2.2.1 The Unauthenticated Adversarial Model (UM)

In this model, the adversarial capabilities and possible attacks are defined as follows.

Basic attacker capabilities. We assume that a probabilistic polynomial-time (PPT) attacker has dominated the communications links. It can eavesdrop to all the transferred information and choose what messages will reach their target and when to replace these messages or insert its own messages. The formalism characterises this capability of the attacker by permitting it to be the one responsible for passing messages from one party to another. The attacker is also in charge of the arrangement of all protocol events such as the initiation of protocols and message transmission.

Acquiring secret information. Besides the above basic adversarial capabilities, we permit the attacker to get secret information saved in the party's memories through explicit attacks. We believe that all the secret information stored at a user's memory is possibly susceptible to any form of leakages. Yet, it is important when defining the security of a protocol to assure that the leakage of some form of secret information has the slightest possible outcome on the security of other secrets. For instance, we guarantee that the leakage of information particular to one session (like a session key or an ephemeral state information) will not affect the security of other sessions, or even revealing critical long-term secrets (such as private keys) that are used along various sessions will not essentially reveal secret information from all previous sessions. In order to distinguish between various vulnerabilities and guarantee

as much security as possible, we categorise attacks into three categories based on the type of information accessed by the adversary.

Party corruption. The attacker can infiltrate at any time the internal memory of a party and learn all secret information including long-term secrets (e.g. long-term private keys) and session-specific secret information such as the internal state of incomplete sessions and the session-keys of completed sessions. Because the attacker now has access to the party's long-term secret, this party is considered under full control of the attacker since the time of corruption.

Session-key query. The attacker gives a party's name and a session identifier of a completed session at that party and receives the session-key generated from that session. This attack models the information leakage of session-keys due to hacking the party's memory, cryptanalysis, eavesdropping, careless disposal of keys, etc.

Session-state reveal. The attacker gives the name of a party and a session identifier of an incomplete session at that party and receives the internal state of that session. The information included in the local state of each session is identified by each KE protocol.

Session expiration. It is a protocol action that erases the named session key (and any related session state) from that party's memory when activated. An expired session key cannot be found using the three above attacks. That is useful in simulating the good security practice of limiting the life-time of a session key and modelling the notion of perfect forward secrecy.

We note here that the sessions attacked by any of the first three queries are locally exposed. If these sessions and their matching sessions (a matching session is the session established with the other party) are locally exposed, then they both are exposed sessions.

A game between a distinguisher $\mathcal{D}$ and a UM adversary $\mathcal{U}$ to break a KE protocol is played as follows.

Participants. Parties $P_1, ..., P_n$ operating an n-party protocol π on inputs $X_1, ..., X_n$ respectively, and an adversary $\mathcal{U}$.

Initialisation. First, choose a random value d, then each party P_i invokes π on inputs X_i, security parameter k and random inputs. After that, P_i gets an initialisation function $I(d,k)_i$ and $I(d,k)_0$.

Activation. When $\mathcal{U}$ activates P_i, it runs its program and hands $\mathcal{U}$ the resulting outgoing messages and action requests. Local outputs resulted from the protocol are known to $\mathcal{U}$ except for those labeled 'secret'. $\mathcal{U}$ may corrupt a party P_i. After corruption, $\mathcal{U}$ gets the current internal state of P_i and a special message is impeded to P_i's local output. From this point on, P_i can not be activated and does not produce further local outputs. $\mathcal{U}$ may make a session-state reveal query for a specified session within some party P_i. $\mathcal{U}$ gets the current local state of the specified session within

P_i. This event is recorded through a special note in P_i's local output. $\mathcal{U}$ may make a session-output query for a specified session within some party P_i. $\mathcal{U}$ gets any output from the specified session that was identified as secret. This event is recorded through a special note in P_i's local output. The global output of the execution is the concatenation of the outputs of $\mathcal{U}$ and $P_1, ..., P_n$.

Test-session. When $\mathcal{U}$ is satisfied with the above queries, it sends a test-session query of a specific session to $\mathcal{D}$. $\mathcal{D}$ tosses a fair coin $b \in \{0, 1\}$. If $b = 0$, it sends the challenge session key SSK^* to $\mathcal{U}$ otherwise, it sends a random value to $\mathcal{U}$.

$\mathcal{U}$ continues to issue session-state reveal, session-key and corruption queries and in the end, it outputs $\overline{b}$. It wins the game if $\overline{b} = b$.

Remark. After each corruption query, the corrupted party issues a corruption notice and stops issuing any future sessions. That is because $\mathcal{U}$ has got the long-term secret of party P_i and consequently, it will be able to completely impersonate that party in future sessions. $\mathcal{U}$ is not allowed to corrupt a party involved in the test session or issue any other exposure command against that session while unexpired.

2.2.2 The Authenticated Adversarial Model (AM) and Authenticators

The AM adversary $\mathcal{A}$ is an adversary that is similar to $\mathcal{U}$ except that $\mathcal{A}$ is obliged to honestly deliver messages sent between the corresponding parties during the protocol execution. This is helpful in simplifying the security analysis of KE protocols. If a KE protocol is proven secure against $\mathcal{A}$, it can be automatically compiled to a version secure against $\mathcal{U}$ using authenticators. Authenticators are cryptographic tools (such as signatures and Mac) that can transform any protocol secure in the AM model to become secure in the UM model. These authenticators, firstly presented in [BR93] and then adopted in [CK01], are generic and independent from the main KE protocol. It is somewhat similar to the Fujisaki-Okamoto transformation [FO13] that transforms IND-ID-CPA secure encryption to IND-ID-CCA2 secure encryption.

2.3 Key Revocation

For the last few years, the key revocation problem has received the attention of the cryptography community because the user's public key cannot be used if the corresponding private key is compromised. This problem occurs in public key cryptography because it depends on digital certificates which are signatures issued by a trusted certificate authority (CA) that securely ties together a number of quantities. Typically, these quantities contain at least the ID of a user (U) and its public key (PK).

The most widely-known and a very ineffective way to solve the key revocation problem is the certificate revocation list (CRL) [CSF+08, HPFS02] which is a list that contains revoked certificates. The CA produces this list periodically with its signature. Because the CA will probably revoke many of its certificates -say 10 %- if they are produced for a validity time of one year [Gen03, Mic02], the CRL will be too lengthy if the CA has many clients. Moreover, the complete CRL must be sent to any party that needs to carry out a certificate status check. There are improvements to this approach such as delta CRLs [BDT04] which list only those certificates revoked since the CA's last update. But the consumed transmission bandwidth and computation costs of these lists are still very high. Another method of solving the key revocation problem is the online certificate status protocol (OCSP) [MAM+99]. If a client wants to check a certificate status, he sends to the CA a certificate status query. The CA replies to this query by producing a fresh signature on the certificate's current status. This omits the need to send a list of all revoked certificates and reduces the transmission costs to a single signature per query but it significantly increases computation costs. It also negatively affects security. If the CA is centralised, the system will have a single point of failure and consequently will become highly vulnerable to denial-of-service (DoS) attacks [Gen03, Mic02].

Kocher [Koc98] suggested an improved version of OCSP called certificate revocation trees (CRTs). The CA can be considered as a global service provider and must be replicated using many servers in order to stand the entire load of certificate validation requests. The CA's signing key must be distributed securely over many servers. This process is expensive and insecure. A solution to this problem is that a highly secure root CA sends a signed CRL-like data structure to other less-secure servers and then clients can query these servers for their certificate validation requests. The data structure is like a tree where the leaves are the revoked certificates and the root is a signature of the highly secure root CA. If a user wants to check the validity of a certificate, he sends a request to the nearest less-secure CA server.

A disadvantage of the current CRT structure is that the whole CRT must be recalculated and sent to all servers if a new certificate is revoked. This problem can be solved if the CRT can be updated without the need to recalculate it. 2-3 trees proposed by Naor and Nissim [NN98], Aiello, Lodha and Ostrovsky [ALO98] and skip-lists proposed by Goodrich *et al.* [GTS01] are proposed solutions to this problem.

Micali [Mic96, Mic02] proposed an efficient algorithm to solve this problem called Novomodo. Similar to previous PKI proposals, Micali's Novomodo system includes a CA, one or more directories (to distribute the certification information) and the users. Despite this similarity, it is more efficient than CRLs and OCSP without sacrificing security.

The basic idea behind Novomodo is as follows. For each client, the CA first picks a random 160-bit value X_0 and applies a public one-way hash function (SHA1, for instance) to it n times to get a 160-bit value X_n, where $X_i = H(X_{i-1})$. The CA contains X_n in the client's certificate. If the user's certificate is still valid on the ith day after release, the CA sends the value of X_{n-i} to the directories. Otherwise, it does not. In the former case, third party T can verify that the user's certificate is still active by querying a directory and then checking that $H^i(X_{n-i})$ (i times) equals X_n, the value embedded in the user's certificate.

The advantage of Novomodo over a CRL-based system is that a directory's reply to a certificate status query is brief, only 160 bits per query. On the other hand, the length of a CRL increases with the number of certificates that have been revoked (i.e. number of clients). Novomodo has several advantages over OCSP. First, Novomodo depends on hashing while OCSP depends on signing. Because hashing has lower computation costs than signing, the CA's computational costs in Novomodo are typically much lower. Second, the directories in Novomodo do not have to be trusted unlike the distributed components of an OCSP CA. Instead of issuing signatures depending on third parties, the directories publish only hashed pre-images sent by the CA (which cannot be produced by Novomodo directories). Third, the directories do not perform any online computation and make Novomodo less vulnerable to DoS attacks. Finally, although OCSP does not consume too much bandwidth, Novomodo's bandwidth consumption is typically even lower since public-key signatures are typically longer than 160 bits (length of X_{n-i} sent per query).

A disadvantage of all the above techniques is relaying on third-party queries [Gen03]. It is preferable to eliminate third-party queries for several reasons. First, since anyone can ask for third-party queries, each certificate server must be able to get the certificate status of every client in the system. The situation is much simpler if third-party queries are eliminated. Each server is only required to have certification proofs for the clients that it works for. In addition, multi-cast can be used to push certificate proofs to clients to reduce the transmission costs. Second, third-party queries multiply the query computation costs of the CA and/or its servers. For example, if each client queries the certificate status of X clients per day, the system must process XN queries (where N is the number of clients). Third, from a business model perspective, non-client queries are not recommended. If T is not a client of the CA, he will not be motivated to deliver T fresh certificate status information. Finally, since the CA must reply to queries from non-clients, it becomes more vulnerable to DoS attacks and this is a security concern. In summary, removing third-party queries leads to a reduction in infrastructure costs, simplifies the business model and increases security. We can completely remove third-party

queries by using an implicit certification such as IBE or certificate-based encryption (CBE).

Gentry presented the notion of certificate-based encryption (CBE) [Gen03]. This system combines public-key encryption (PKE) and IBE while keeping most of the advantages of each. Using PKE, each client creates its own public-key/secret-key pair and asks for a certificate from the CA. The CA uses an IBE to create the certificate. This certificate has all of the functionality of a conventional PKI certificate as well as also being able to be used as a decryption key. This double encryption gives us implicit certification. If T wants to encrypt a message to a user, it double encrypts the message using PKI and IBE, and then the user uses both his secret key and an up-to-date certificate from his CA to decrypt the message. CBE has no escrow (since the CA does not know the user's secret key), and it does not have secret key distribution problem since the CA's certificate needs not be kept secret. Although CBE consumes less computation and transmission costs than Novomodo, it is preferable to completely eliminate the use of certificates to preserve the infrastructure costs.

As a special type of public-key cryptography (PKC), IBC also suffers from the key revocation problem. The strategy to face this problem in IBC is quiet different than PKC because first, there is no certificate in IBC to revoke. Second, the public key of IBC is hard to replace since it represents the identity of the user. Next, we represent mediated cryptosystems which solve the key revocation problem in IBC.

Boneh, Ding, Tsudik and Wong were the first to introduce the notion of mediated cryptosystems [BDTW01]. They designed a variant of RSA that allows an immediate revocation of, for instance, an employee's key by an employer for any reason (m-RSA). m-RSA is the first secure variant of RSA that shares a common modulus between different users. It is based on the so-called security mediator (SEM) architecture in which the SEM is a semi-trusted server. If an employee wants to decrypt/sign a message, he must co-operate with the SEM to do so. The idea behind m-RSA is splitting the secret key of an employee between the employee himself and the SEM. Hence, without the SEM cooperation, the employee cannot sign or encrypt messages. This is also helpful to monitor the security of sent/received secure messages in the company. Later on, Ding and Tsudik presented an identity-based mediated RSA (IB-mRSA) along with a security proof [DT03]. In particular, they stated that "IB-mRSA/OAEP encryption offers equivalent the semantic security to RSA/OAEP against adaptive chosen ciphertext attacks in the random oracle model if the key generation function is division intractable". To make the key generation function division intractable, Ding and Tsudik used a division intractable hash function to generate division intractable public keys.

The SEM architecture was proven useful to simplify signature validation and

enable key revocation in legacy systems [BDTW01]. Although this system does not require a CA to create a certificate or send certificate status information and the computation and transmission costs are kept to minimum, it has few major security concerns. First, since SEM is centralised, it represents a single point of failure for the system and hence it is vulnerable to DOS attacks. Second, a hacked SEM can be a major threat to the system security because the SEM is a semi-trusted server.

2.4 Attribute-Based Cryptography

Attribute-based cryptography (ABC) was presented to give an access structure to the encrypted data stored on a public cloud. It allows the users to encrypt or sign messages based on their attributes instead of their individual identities as in the identity-based cryptography (IBC) [Sha84]. These attributes are, for example, the place where they live or the company in which they work. ABC can be classified as a key-policy ABC (KP-ABC) and ciphertext-policy ABC (CP-ABC). A policy is a rule that determines which attributes should decrypt or verify the message. In a key-policy ABC, the policy is inserted in the key while the ciphertext is encrypted or signed using the attributes. In a ciphertext-policy ABC, the policy is inserted in the ciphertext while the key represents the attributes.

Attribute-based encryption (ABE) was first introduced by Sahai and Waters [SW05] as a variant of identity-based encryption (IBE) [Sha84]. ABE systems can be classified into a key-policy attribute-based encryption (KP-ABE) and ciphertext policy attribute-based encryption (CP-ABE). Examples of KP-ABE and CP-ABE systems are [ALdP11, GPSW06] and [EMN$^+$09, GMS$^+$14, Wat11] respectively. CP-ABE is more suitable in access control applications compared with KP-ABE because it lets the sender to choose the access structure which determines who can decrypt the message [GMS$^+$14].

Bethencourt, Sahai and Waters [BSW07] were the first to present a valid construction of a CP-ABE. Cheung and Newport [CN07] presented a CP-ABE with AND-gate access structure. Their system is chosen plaintext (CPA) secure under the decisional bilinear Diffie-Hellman (DBDH) assumption. Guo, Mu and Susilo presented a CP-ABE with a constant key size, which is suitable for lightweight devices [GMS$^+$14].

CP-ABE can be categorised based on their access structure including threshold access structure [OSW07] and AND-gate access structure [CN07, GMS$^+$14]. Monotone access structure [BSW07] supports threshold, AND and OR gates. A linear secret sharing scheme (LSSS) [Wat11] can formulate any monotonic boolean equation. Sahai and Waters [GGH$^+$13] proposed the first ABE scheme for general circuit.

Most CP-ABE systems in the literature are provably secure in the selective secu-

rity model [GMS+14]. The first to present a fully secure CP-ABE using composite-order pairing was Lewko *et al.* [LOS+10]. A fully secure CP-ABE with constant-size ciphertext was presented by Chen *et al.* [CCL+13]. Okamoto and Takashima [OT12] presented a fully-secure unbounded CP-ABE. Nieto *et al.* [NMS12] presented a predicate encryption in which they combined an ABE with key revocation support. The ciphertext can be successfully decrypted if the decryption policy is fulfilled by the receiver's private keys and they were not revoked by the time the ciphertext were created.

Signature systems were firstly adopted to the attribute based settings by Maji *et al.* [MPR08] by presenting an attribute-based signature. Li *et al.* constructed two efficient attribute-based signature systems that support flexible threshold [LAS+10]. Recently, an attribute-based signature from RSA was presented by Herranz [Her14]. This system is efficient because it does not depend on pairings. Li and Kim presented a hidden attribute-based signatures without anonymity revocation from pairings [LK10].

The first to propose a signcryption cryptosystem was Zheng [Zhe97] with the goal of producing a cryptosystem that provides both confidentiality and unforgettability efficiently compared to using two encryption and signature systems simultaneously. Libert and Quisquater [LQ04] proposed a public key authenticated signcryption based on the Diffie-Hellman problem. Xavier Boyen [Boy03] was the first to present a security model for identity-based signcryption (IBSC). He also presented an IBSC based on pairings that is secure in this model.

The first to propose an attribute-based signcryption (ABSC) was Gagne, Narayan, and Safavi-Naini with threshold structure [GNS10]. Later, Wang *et al.* [WHLL13] proved that the ABSC presented by Gange *et al.* is not secure and launched a forgery attack against it. Han *et al.* [HLY13] presented an attribute-based signcryption with non-monotonic access structure. Guo *et al.* [GLF13] presented a fully secure attribute-based ring signcryption. Meng *et al.* presented a privacy-preserving decentralised KP-ABS in cloud computing environments [MCM14]. Next, we present some definitions related to ABSC including the definitions of the attributes and AND-gate access structure, the structure of CP-ABSC and its security notions.

2.4.1 Attributes and Access Structure

Let A be an attribute and let $\{A_1, A_2, ..., A_n\}$ be all possible attributes. The attributes belonging to a user is denoted by $\mathbb{A}$. The attribute set $\mathbb{A}$ is defined as an n-bit string $\{a_1, a_2, ..., a_n\}$ where $a_i = 1$ if $A_i \in \mathbb{A}$ and $a_i = 0$ otherwise. $\mathbb{P}$ represents the AND-gate access structure that defines which attributes can signcrypt/unsigncrypt the message. Similar to $\mathbb{A}$, $\mathbb{P}$ is defined as an n-bit string

$\{b_1, b_2, ..., b_n\}$ where $b_i = 1$ if $A_i \in \mathbb{P}$ and $b_i = 0$ otherwise.

Definition 2.10. *We say that an attribute set of a user* $\mathbb{A} = \{a_1, a_2, ..., a_n\}$ *fulfils the access structure* $\mathbb{P} = \{b_1, b_2, ..., b_n\}$ *iff* $a_i \geq b_i \forall i \in \{1, n\}$. *We write* $\mathbb{P} \subseteq \mathbb{A}$ *as a shorthand of* $\mathbb{A}$ *fulfils* $\mathbb{P}$. *In other words,* $\mathbb{A}$ *fulfils* $\mathbb{P}$ *if* $\mathbb{P}$ *is a subset of* $\mathbb{A}$.

2.4.2 Construction

An ABSC comprises the following algorithms [GNS10].

- $(params, MS) \leftarrow Setup(\lambda)$. Taking the security parameter λ, a private key generator (PKG) executes this algorithm to generate the system's public parameters ($params$) and a master secret (MS).

- $(r_{i,\sigma}, r_{i,\eta}) \leftarrow KeyGeneration(MS, params, A_{i,\sigma}, A_{i,\eta})$. First, the PKG assigns two values to each attribute $A_{i,\sigma}$, $A_{i,\eta}$. $A_{i,\sigma}$ is the signature value and $A_{i,\eta}$ is the encryption value. Then the key generation runs two sub-algorithms.

  - $(r_{i,\sigma}) \leftarrow sExtract(MS, params, A_{i,\sigma})$. Given the master secret MS and the public parameters $params$, the PKG generates the secret key $r_{i,\sigma}$ corresponding to each signature attribute $A_{i,\sigma}$.

  - $(r_{i,\eta}) \leftarrow uExtract(MS, params, A_{i,\eta})$. Given the master secret MS and the public parameters $params$, the PKG generates the secret key $r_{i,\eta}$ corresponding to each encryption attribute $A_{i,\eta}$.

- $(C) \leftarrow Signcrypt(m, params, \mathbb{A}_\sigma, \mathbb{P}_\sigma, \mathbb{P}_\eta, r_{i,\sigma})$. Given the message m, the public parameters $params$, and the structure of the signature attributes $\mathbb{P}_\sigma$ along with the signature attribute set $\mathbb{A}_\sigma$, the sender encrypts the message based on the receiver's access structure $\mathbb{P}_\eta$ and signs the message using his signing key $r_{i,\sigma}$.

- $(m) \leftarrow Unsigncrypt(C, params, \mathbb{A}_\eta, \mathbb{P}_\sigma, \mathbb{P}_\eta, r_{i,\eta})$. Given the ciphertext C, the public parameters $params$, the access structure of the sender's signature attributes $\mathbb{P}_\sigma$, and the access structure of the encryption attributes $\mathbb{P}_\eta$ along with his encryption attribute set $\mathbb{A}_\eta$, the receiver will be able to decrypt and verify the ciphertext iff $\mathbb{A}_\eta$ fulfils $\mathbb{P}_\eta$. If $\mathbb{A}_\eta$ fulfils $\mathbb{P}_\eta$, the receiver decrypts the message and verify the signature of the sender using his decryption key $r_{i,\eta}$.

- **Remark**. The subscript σ represents a signature (or sender) variable because the signature part is done by the sender while the subscript η represents an encryption (or receiver) variable because the sender is encrypting the message based on the receiver's attributes.

2.4.3 Security Notions

An ABSC must maintain two security notions, message confidentiality and ciphertext unforgeability.

2.4.3.1 Message Confidentiality

This security notion models an adversary who tries to distinguish the ciphertext from a random value under a chosen-plaintext attack. The message confidentiality under the chosen plaintext attack is described as a game between an adversary $\mathcal{A}$ and a challenger $\mathcal{C}$ [GNS10]. This game is as follows.

- *Setup*(λ). $\mathcal{C}$ generates the public parameters (*params*) and sends them to $\mathcal{A}$, and keeps the master secret (MS) to himself.

- *Query Phase* 1. In this phase, $\mathcal{A}$ can query any signature attribute $A_{i,\sigma}$ or encryption attribute $A_{i,\eta}$ of his choice. The challenger then runs $sExtract$ and $uExtract$ to get $r_{i,\sigma}$ and $r_{i,\eta}$. The adversary $\mathcal{A}$ can also make a signcryption query for a message m, an encryption attribute set $\mathbb{A}_\eta$ based on an access structure $\mathbb{P}_\eta$ and a signature attribute set $\mathbb{A}_\sigma$ based on an access structure $\mathbb{P}_\sigma$. The challenger $\mathcal{C}$ replies by running $sExtract$ to get the secret key $r_{i,\sigma}$ and then signcrypts the message by running the *Signcrypt* algorithm.

- *Challenge*. $\mathcal{A}$ sends to $\mathcal{C}$ two messages m_1 and m_2 for a challenge encryption attribute set $\mathbb{A}^*_\eta$ based on an access structure $\mathbb{P}^*_\eta$ and a signature attribute set $\mathbb{A}^*_\sigma$ based on an access structure $\mathbb{P}^*_\sigma$. $\mathcal{C}$ tosses a fair coin $b \in \{0,1\}$ and encrypts m_b using the encryption access structure $\mathbb{P}^*_\eta$ and signs it using the secret key $r^*_{i,\sigma}$ of a challenge signature attribute set $\mathbb{A}^*_\sigma$ associated to an access structure $\mathbb{P}^*_\sigma$. Note here that the challenged attributes must not be queried in the query phase.

- *Query Phase* 2. The adversary is allowed to make adaptive queries as in phase 1 but the challenged attributes.

- *Guess*. $\mathcal{A}$ outputs $\overline{b} \in \{0,1\}$. $\mathcal{A}$ wins the game if $b = \overline{b}$.

The advantage of $\mathcal{A}$ to attack a system ξ and win this game is,

$$ABSCAdv_{\mathcal{A},\xi}(\lambda) = |\Pr[\overline{b} = b] - \tfrac{1}{2}|.$$

Definition 2.11. *An attribute-based signcryption is indistinguishable against adaptive chosen plaintext attack (IND-ABSC-CPA), if the advantage of any polynomially bounded adversary $\mathcal{A}$ in the above game is negligible.*

If $\mathcal{A}$ submits two pairs of $(\mathbb{A}^*_{0,\eta}, m_0)$ and $(\mathbb{A}^*_{1,\eta}, m_1)$ in the challenge phase, then this game is called anonymous adaptive chosen plaintext attack (Anon-IND-ABSC-CPA) security model. The advantage of the adversary winning this game is the same as above.

2.4.3.2 Ciphertext Unforgeability

This security notion models existentially unforgeable security against chosen-message attack. It is described as a game between an adversary $\mathcal{A}$ and a challenger $\mathcal{C}$ [GNS10]. This game is as follows.

- *Setup*(λ). $\mathcal{C}$ generates the public parameters (*params*) and sends them to $\mathcal{A}$, and keeps the master secret (MS) to himself.
- *Query Phase* 1. In this phase, $\mathcal{A}$ can query any signature attribute $A_{i,\sigma}$ or encryption attribute $A_{i,\eta}$ of his choice. The challenger then runs $sExtract$ and $uExtract$ to get $r_{i,\sigma}$ and $r_{i,\eta}$. The adversary $\mathcal{A}$ can also make a signcryption query for a message m, an encryption attribute set $\mathbb{A}_\eta$ based on an access structure $\mathbb{P}_\eta$ and a signature attribute set $\mathbb{A}_\sigma$ based on an access structure $\mathbb{P}_\sigma$. The challenger $\mathcal{C}$ replies by running $sExtract$ to get the secret key $r_{i,\sigma}$ and then signcrypts the message by running the $Signcrypt$ algorithm.
- *Forgery Phase*. $\mathcal{A}$ sends to $\mathcal{C}$ a ciphertext C^* for a challenge encryption attribute set $\mathbb{A}^*_\eta$ based on an access structure $\mathbb{P}^*_\eta$ and a signature attribute set $\mathbb{A}^*_\sigma$ based on an access structure $\mathbb{P}^*_\sigma$. $\mathcal{A}$ wins the game if C^* is a valid ciphertext which was not obtained by running the $Signcrypt$ query. That is satisfied if $Unsigncrypt$ (C^*, $params, \mathbb{A}^*_\eta$, $\mathbb{P}^*_\sigma, \mathbb{P}^*_\eta, r^*_{i,\eta}$) $= m^*$ and $r^*_{i,\eta} = uExtract(A^*_{i,\eta})$ and $\mathcal{A}$ did not issue a query $Signcrypt(m^*, params, \mathbb{A}^*_\sigma, \mathbb{P}^*_\sigma, \mathbb{P}^*_\eta, r^*_{i,\sigma})$.

The advantage of $\mathcal{A}$ to attack a system ξ and win this game is,

$$ABSCAdv_{\mathcal{A},\xi}(\lambda) = |\Pr[\overline{b} = b] - \tfrac{1}{2}|.$$

Definition 2.12. *An attribute-based signcryption is existentially unforgeable against a chosen-message attack (EUF-ABSC-SMA), if the advantage of any polynomially bounded adversary $\mathcal{A}$ in the above game is negligible.*

Chapter 3

Mediated Encryption: Analysis and Design

Boneh, Ding and Tsudik presented identity-based mediated RSA encryption and signature systems (IB-mRSA) in which the users are not allowed to decrypt/sign messages without the authorisation of a security mediator. We show that IB-mRSA is not secure. We present a secure modified version which is as efficient as the original system. We also propose a generic mediated encryption (GME) that converts any identity based encryption to a mediated version of this IBE. It envelops an IBE encrypted message using a user's identity into an IBE envelope using the identity of the SEM. We present two security models based on the role of the adversary whether it is a revoked user or a hacked SEM. We prove that GME is as secure as the SEM's IBE against a revoked user and as secure as the user's IBE against a hacked SEM. We also present two implementations of GME based on Boneh-Franklin FullIdent which is a pairing-based IBE and Boneh, Gentry and Hamburg (BGH) AnonIBE which is a pairing-free IBE.

3.1 Introduction

For the last few years, the key revocation problem has received the attention of the cryptography community because the user's public key cannot be used if the corresponding private key is compromised. This problem occurs in public key cryptography because it depends on digital certificates. Digital certificates are signatures issued by a trusted certificate authority (CA) that securely ties together a number of quantities. Typically, these quantities contain at least the ID of a user (U) and its public key (PK). Frequently, the CA comprises a serial number (SN) for managing certificates. The CA also binds the certificates to an issue date D_1 and an expiration date D_2. By issuing the signature of $SigCA(U, PK, SN, D_1, D_2)$, the CA provides PK between the current date D_1 and the future date D_2.

A user's public key may have to be revoked before its expiration date D_2 if a user's secret key is accidentally leaked or an attacker successfully compromises it. A new key pair should be generated and the corresponding certificate should be issued. If the CA can revoke a certificate, then third parties cannot depend on this certificate unless the CA shares certificate status information indicating whether this certificate is still valid. This certificate status information has to be

recently generated and must be widely distributed. Sharing a great deal of fresh certificates periodically leads to the key revocation problem which consumes large amount of computation power and bandwidth. This is considered a hindrance to global application of public-key cryptography.

As a special type of public-key cryptography (PKC), IBC also suffers from the key revocation problem. The strategy to face this problem in IBC is quiet different than PKC because first, there is no certificate in IBC to revoke. Second, the public key of IBC is hard to replace since it represents the identity of the user. Boneh, Ding, Tsudik and Wong were the first to introduce the notion of mediated cryptosystems [BDTW01]. They designed a variant of RSA that allows an immediate revocation of, for instance, an employee's key by an employer for any reason. Their system is the first secure RSA variant that shares a common modulus between different users. It is based on the so-called security mediator (SEM) architecture in which the SEM is a semi-trusted server. If an employee wants to decrypt/sign a message, he must co-operate with the SEM to do so. The idea behind their system is splitting the secret key of an employee between the employee himself and the SEM. Hence, without the SEM cooperation, the employee cannot sign or encrypt messages. This is also helpful to monitor the security of sent/received secure messages in the company. Later on, Ding and Tsudik presented an identity based mediated RSA (IB-mRSA) along with a security proof [DT03]. In particular, they stated that "IB-mRSA/OAEP encryption offers equivalent the semantic security to RSA/OAEP against adaptive chosen ciphertext attacks in the random oracle model if the key generation function is division intractable". To make the key generation function division intractable, Ding and Tsudik used a division intractable hash function to generate division intractable public keys.

3.1.1 Our Contribution

First, we investigate the security of IB-mRSA [BDTW01, DT03]. We show that hashing users' identities using a division intractable hash function does not necessarily generate division intractable public keys. We show that an inside attacker can breach IB-mRSA even if the hash function used is division intractable. We present two solutions that make the key generation function division intractable and hence, IB-mRSA is secure. Second, we take the idea of [BDTW01] one step further and present a generic mediation system that is capable of making any IBE support key revocation. This idea is based on a letter-envelope technique. If U_A wants to encrypt a message to U_B, he first encrypts it normally using U_B's identity (letter) then he encrypts the letter again using the identity of the SEM (envelope) and sends the resulted ciphertext to U_B. To decrypt the ciphertext, U_B sends the message to the

SEM. If U_B is revoked, the SEM will not open the envelope for him. If U_B is not revoked, the SEM will open the envelope and send the letter to U_B who decrypts the message using his private key. The structure of GME combines the advantages of both Gentry [Gen03] and Boneh *et al.* [BDTW01] systems. It completely eliminates the use of certificates. In addition, the SEM in GME is not a single point of failure. If the SEM is compromised, the system can continue working using the user's IBE. In addition, all messages sent to the SEM before or after an attack are safe and secure. Through the chapter, U represents a user and S represents the SEM.

The rest of the chapter is organised as follows. Section 3.2 discusses IB-mRSA encryption/signature systems and their implementations. Section 3.3 discusses the security flaw of IB-mRSA. Section 3.4 proposes two solutions to overcome IB-mRSA security flaw. The effect of using these solutions on IB-mRSA are discussed in Section 3.5. Section 3.6 presents the generic mediated encryption (GME) and its security proof. Section 3.7 presents two implementations of GME, the first one is based on BF FullIdent [BF01] which is a pairing-based system and the second one is based on the BGH AnonIBE [BGH07] which is not a pairing-based IBE. The last section presents the conclusions of the chapter.

3.2 IB-mRSA

We review the structure of IB-mRSA as follows. In the setup phase, a PKG produces two safe primes p, q with a length of a security parameter k then computes $N = pq$. He preserves p, q as the secret system parameters while makes the modulus N public. Next, the PKG produces the private key for U_A by hashing his identity to a value $KG()$ and padding $KG()$ with one to get an odd public key for U_A. After that, he makes the corresponding full RSA private key for U_A and splits it between U_A and the SEM. U_B encrypts message m to U_A normally using the public key of U_A. After getting the encrypted message C from U_B, U_A directs it to the SEM to partially decrypt it. If U_A is revoked, the SEM declines to decrypt the message and returns 'error'. Otherwise, the SEM partially decrypts the message to get PD_S and sends it to U_A. After receiving the partially decrypted message PD_S from the SEM, U_A computes his own partially decrypted version of the message PD_U and then combines it with PD_S to get his fully decrypted message. The algorithms of *Extract*, *Encrypt* and *Decrypt* are shown below. The signature system has the same *Extract* algorithm as the encryption system. When U_A signs a message to U_B, he sends it to the SEM to partially sign the message for him if he is not revoked. U_A combines the partially signed message of the SEM with his partially signed version of the message to get his own signature. U_B can verify the signature of U_A normally as RSA.

Extract.
Input: two safe primes p and q
Output: r_U, r_S
$N = pq$
for U **do**
  $s = k - |KG()| - 1$, $e = 0^s||KG()||1$
  $r = \frac{1}{e} \pmod{\varphi(N)}$
  $r_U \overset{R}{\leftarrow} Z_N - [0]$, $r_S = (r - r_U) \pmod{\varphi(N)}$

Encrypt.
Input: $N, k, KG()$
Output: C
$s = k - |KG()| - 1$, $e = 0^s||KG()||1$
$C =$ Encrypt the message using RSA/OAEP

Decrypt.
Input: C, r_U, r_S
Output: m
for S **do**
  if *U is Revoked* **then**
    return (ERROR) and Exit
  $PD_S = C^{r_S} \pmod{N}$
for U **do**
  $PD_U = C^{r_U} \pmod{N}$, $M = (PD_S \times PD_U) \pmod{N}$
$m =$ OAEP Decoding of M

Figure 3.1: The Structure of IB-mRSA Encryption System

Sign.
Input: m, r_U, r_S
Output: h, S
$h = H(m)$
for S **do**
  if *U is revoked* **then**
    return (ERROR) and Exit
  $PD_S = h^{r_S} \pmod{N}$
for U **do**
  $PD_U = c^{r_U} \pmod{N}$, $S = (PD_S \times PD_U) \pmod{N}$
Verify. Input: $h, S, N, k, KG()$
Output: $\overline{h}$
$s = k - |KG()| - 1$, $e = 0^s||KG()||1$
$\overline{h} = S^e \pmod{N}$
if $h \neq \overline{h}$ **then**
  return (ERROR)

Figure 3.2: The Structure of IB-mRSA Signature System

3.3 IB-mRSA Security

IB-mRSA is assumed to be secure in the random oracle model based on [BDTW01] and [DT03]. However, there is a special attack that an insider can initiate. He can modify the encrypted message so that it can be decrypted using his private key by finding a mapping function $f(C_A) = C_B$.

Lemma 3.1. *Assume that there are two users U_A and U_B, U_B is able to obtain a mapping function $f(C_A) = C_B$ and decrypt/forge the encrypted message/signed message of U_A iff $e_a|e_b$.*

Lemma 3.1 and its proof are presented in [DT03]. If $e_a|e_b$ i.e. $e_b = \sigma \times e_a$, we can build a mapping function f such that $f(a) = a^\sigma \pmod N$. To protect the system against this attack, the user's public key cannot be a factor of the product of the other users' public keys. To ensure that, Ding and Tsudik used a division intractable hash function to map a user's identity to his public key ($KG()$). This notion of division intractable hash functions was presented by Gennaro *et al.* [GHR99]. A hash function $H()$ is division intractable if it is unfeasible to find a set of values $(X_1, X_2, ..., X_n, Y)$ such that $H(Y)|\prod_i(H(X_i))$.

In this section, we prove that IB-mRSA is still vulnerable to this attack. A division intractable hash function does not necessarily produce division intractable public keys because the output of the hash function $KG()$ is padded with a 'one'. The public key is $e = KG()\|1$ [DT03] or $e = KG()\|00000001$ [BDT02]. This means that $e = 2KG() + 1$ or $e = 8KG() + 1$. This multiplication and addition completely change the property of the public key and it is likely to no more becoming division intractable. For example, if $|KG(ID_1)| = 6$ and $|KG(ID_2)| = 19$, these two values are division intractable. But if we calculate $e_1 = 2|KG(ID_1)| + 1 = 2 \times 6 + 1 = 13$ and $e_2 = 2|KG(ID_2)| + 1 = 2 \times 19 + 1 = 39$, we can see that e_1 and e_2 are no longer division intractable ($e_2 = 3e_1$) and consequently, Lemma 3.1 can be used to attack IB-mRSA even though the hash function is division intractable. Real life values that represent the same idea are shown in Table 3.1. These numbers are in hexadecimal. We now demonstrate how an inside one-wayness adversary takes advantage of this simple notice to initiate two different attacks against IB-mRSA. The first attack is a direct application of Lemma 3.1. The second attack is a common modulus attack against IB-mRSA. For the signature system, we prove that if such a mapping function exists, an inside attacker can forge the signature of another user without knowing his private key.

Table 3.1: Example of An Attack on IB-mRSA in The Real World

Variables	Value
$\|KG(ID_1)\|$	$A07B0C7AFE0A33D7A270D8A35B995B3546D77D6E$
$\|KG(ID_2)\|$	$808288FE7D6E2B83AD145D7AD059CE09A9BA8F717C$
e_1	$140F618F5FC1467AF44E1B146B732B66A8DAEFADD$
e_2	$1010511FCFADC57075A28BAF5A0B39C1353751EE2F9$
e_2/e_1	CD

3.3.1 Attacks on IB-mRSA Encryption System

The first attack holds when the effect of using an intractable hash function is canceled by padding the output with one and the resulting public keys are in the form of $(e_B = \sigma \times e_A)$. Under these conditions, U_B can obtain the message of U_A using the following formula.

$$C_B = C_A^{e_B/e_A} \pmod{N},$$

and then decrypt this message using his private key. This attack is executed as follows.

- The attacker U_B chooses an identity ID_B such that $e_B = \sigma \times e_A$ where σ is an integer.
- At the challenge phase, U_B sends to the challenger any two messages m_0 and m_1 and the identity ID_A.
- The challenger tosses a fair coin $b \in \{0, 1\}$ and sends $C_A \leftarrow Encrypt(m_b)$ to U_B.
- U_B calculates $C_B = C_A^{e_B/e_A} \pmod{N}$.
- U_B sends C_B to the SEM for decryption.
- After decryption, U_B can successfully find $b' = b$.

The gravity of this attack is that it makes IB-mRSA exposed against a one-wayness adversary; not only U_B can distinguish between two messages m_0 and m_1, he can decrypt it as a message of his own.

The second attack can be applied if the same message was sent to two users, U_A and U_B, U_C with public key satisfies $gcd(e_A, e_B)|e_C$ can launch an attack to decrypt this message as follows.

- Assuming that $g = gcd(e_A, e_B)|e_C$, U_C finds the values of a and b such that $a \times e_A + b \times e_B = g$ using the extended euclidian algorithm.

- After obtaining a and b, U_C calculates $C_g = C_A^a \times C_B^b \pmod N = m^{ae_A+be_B} \pmod N = m^g \pmod N$
- From C_g, U_C obtains his version of m as follows.

$$C_c = C_g^{e_c/g} \pmod N = m^{ge_c/g} \pmod N = m^{e_c} \pmod N,$$

and then he can decrypt it using his private key.

3.3.2 The Attack on IB-mRSA Signature System

In this subsection, we demonstrate an attack on IB-mRSA signature system even with a division intractable hash function. We assume that there are two users, U_A and U_B and show that U_B can forge the signature of U_A without knowing his private key using the following steps, as long as a mapping function between their public keys exists.

- U_B signs the message m with the SEM using his private key.
- After obtaining his signed message (m_B), U_B calculates the forged signature of U_A.

$$\overline{m}_A = m_B^\sigma \pmod N, \text{ where } \sigma = e_B/e_A.$$

- $\overline{m}_A$ can be verified using the public key of U_A.

The proof of the correctness of this attack is described as follows.

$$e^b h_b = ke^a h_b = e^a(kh_b) = e^a \overline{h}_a = 1 \pmod{\varphi(N)}.$$

3.4 IB-mRSA-V2

After showing the security flaw of IB-mRSA encryption/signature systems, we present two solutions that correctly make IB-mRSA secure against these types of attacks. We denote IB-mRSA with these solutions as IB-mRSA-V2. Any solution to these attacks must satisfy the following conditions.

- There is a deterministic one-to-one mapping function that maps the identities of the users to their public keys.
- This function must be division intractable.
- The produced public keys must be co-prime with $\varphi(N)$.

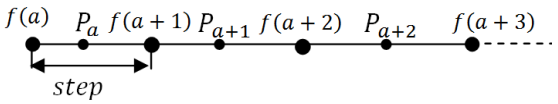

Figure 3.4: The Distribution of Primes

The first proposed solution satisfying the above conditions ensures that the maximum value of a public key is less than three times the smallest public key value, i.e. $e_M < 3e_m$. The subscript M denotes maximum while the subscript m denotes minimum. One can see that this completely eliminates the problem. The relation between the hash function of the maximum and minimum public keys values must be,

$$\begin{aligned} e_M &< 3e_m, \\ 2|KG_M| + 1 &< 3(2|KG_m| + 1) < 6|KG_m| + 3, \\ 2|KG_M| &< 6|KG_m| + 2, \\ |KG_M| &< 3|KG_m| + 1. \end{aligned}$$

If the inequality $|KG_M| < 3|KG_M| + 1$ holds, then all public keys are division intractable. The disadvantage of this solution is that it limits the space of the hash function. The other solution to fix this security flaw is mapping the users' identities to public keys that are primes. To generate primes from identities, we first calculate $a = H(ID)$ and then apply the following function.

$$f(a) = (a - 1) \times \text{step} + 1.$$

where *step* is a value used to generate unique primes. After that, we find the next smallest prime larger than $f(a)$. The algorithm is shown in Figure 3.3.

```
1 a = H(ID)
2 f(a) = (a − 1) × step + 1
3 if f(a) is not prime then
4     f(a) =NxPrime(f(a))
5 return (f(a))
```

Figure 3.3: The Mapping Function

Where $NxPrime(x)$ is a subfunction that finds the smallest prime larger than x. This function must satisfy the following conditions.

- The hash function must be collision resistant i.e. it is unfeasible to find two different values X, Y such that $a = H(Y) = H(X)$. This guarantees that each identity is mapped to a unique public key.

- *step* is chosen carefully such that $f(a) < P_a < f(a+1)$ for any value a. This will guarantee that each identity will be mapped to a unique prime. Figure 3.4 shows this idea. *step* can be determined by finding a value greater than the maximal prime gap which is the gap larger than the gaps of smaller primes.

- If the mapping function satisfies the above conditions, it will overcome the first attack to the encryption system because primes satisfy the division intractable property. However, it cannot withstand the second attack because the greatest common divisor between primes is one. The only solution for this attack is not to use the same OAEP padding when encrypting the same message to multiple users. For the signature system, there is no mapping function exists between primes and consequently, it will be safe from such attacks. After fixing these drawbacks, IB-mRSA-V2 can be proven CCA2 secure in the random oracle model using the same methodology explained in [DT03, BDTW01].

3.5 Implementation

IB-mRSA-V2 was programmed using MIRACL software C library and its performance was compared with IB-mRSA and RSA. The PC used to run these tests has a processor Intel(R) Core(TM) i5-2410M CPU @ 2.30GHz (4 CPUs) and 4096MB RAM. Table 3.2 shows the test results. The results are in ms.

From these results, we can see that.

- IB-mRSA-V2 has the same performance of the original IB-mRSA.

- The time required for RSA to generate a private key is larger than those of IB-mRSA and IB-mRSA-V2 because the key generation of IB-mRSA and IB-mRSA-V2 is for each user and it does not involve the prime key generation that exists in RSA key generation.

- The encryption time increases slightly with the key length. This can be seen also in the encryption times of IB-mRSA and IB-mRSA-V2.

- The decryption times are longer than the encryption times in all systems. This drawback is actually comes originally from RSA because the decryption keys are extremely large (of the length of N).

- The time consumed by all these systems are proportional to the modulus size.

Table 3.2: The Time Performance of RSA, IB-mRSA and IB-mRSA-V2

The Process	Modulus	Key Size	RSA	IB-mRSA	IB-mRSA-V2
Key Generation	1024 Bits	16 Bits	17.19	0.13	0.11
		128 Bits	22.04	0.13	0.13
		160 Bits	19.8	0.14	0.14
	2048 Bits	16 Bits	128.26	0.17	0.16
		128 Bits	130.26	0.14	0.14
		160 Bits	127.86	0.16	0.16
Encryption / Verify	1024 Bits	16 Bits	0.03	0.06	0.05
		128 Bits	0.03	0.03	0.05
		160 Bits	0.03	0.05	0.03
	2048 Bits	16 Bits	0.03	0.06	0.06
		128 Bits	0.01	0.06	0.05
		160 Bits	0.03	0.06	0.06
Decryption / Sign	1024 Bits	16 Bits	0.14	0.12	0.14
		128 Bits	0.13	0.13	0.14
		160 Bits	0.14	0.13	0.13
	2048 Bits	16 Bits	0.22	0.22	0.22
		128 Bits	0.23	0.23	0.23
		160 Bits	0.22	0.22	0.22

3.6 Generic Mediated Encryption (GME)

In this section, we take the idea of IB-mRSA one step ahead. Assume that there is a company XYZ and the security manager of this company wants to upgrade the currently-used IBE to one that supports key revocation. The security manager has two options. He can install a CBE system [Gen03] but he has to uninstall the currently-used IBE and install a PKE. PKE certificates will lead to more computation and transmission costs. The other option is using mediated cryptosystem such as IB-mRSA [BDTW01, DT03]. The security manager also has to uninstall the current IBE and install IB-mRSA. The process of uninstalling the currently-used IBE and installing a new one is time-consuming and expensive. It is like having a safe with a one-key lock and you want to replace it with a two-key lock, you will have to completely remove the old lock and install the new one. The question we address here is "Is there a way to make any IBE support key revocation without having to uninstall it?". We take the idea of IB-mRSA and present a generic mediated encryp-

tion (GME) that converts any IBE to a version that supports key revocation. In the following section, we explain the construction of GME followed by the security model and the security proof of these systems.

3.6.1 GME Construction

Definition 3.1. *A Generic Mediated Encryption is a 6- tuple of algorithms. These algorithms are (Gen_S, KG_S, Gen_U, KG_U, Enc, Dec_S, Dec_U) such that.*

- $(MS_S, P_S) \leftarrow Gen_S(k_1)$. *The private key generator (PKG) runs the probabilistic IBE key generation algorithm Gen_S which takes as input a security parameter k_1. It returns MS_S (the first PKG master secret) and public parameters P_S.*

- $(MS_U, P_U) \leftarrow Gen_U(k_2)$. *The PKG runs the probabilistic IBE key generation algorithm Gen_U which takes as input a security parameter k_2. It returns MS_U (the second PKG master secret) and public parameters P_U.*

- $(r_S) \leftarrow KG_S(MS_S, P_S, ID_S)$. *This algorithm generates the secret key r_S for a SEM with identity ID_S using P_S and MS_S.*

- $(r_U) \leftarrow KG_U(MS_U, P_U, ID_U)$. *This algorithm generates the secret key r_U for a user with identity ID_U using P_U and MS_U.*

- $(C) \leftarrow Enc(P_S, P_U, ID_U, ID_S, m)$. *The probabilistic algorithm Enc takes P_S, P_U, ID_U, ID_S, m. It returns a ciphertext C.*

- $(C_U) \leftarrow Dec_S(P_S, r_S, C)$. *The deterministic decryption algorithm Dec_S takes (P_S, r_S, C) as input along with the user revocation status. If the user is revoked, Dec_S returns $\perp$. Otherwise it returns C_U.*

- $(m) \leftarrow Dec_U(P_U, r_U, C_U)$. *The deterministic decryption algorithm Dec_U takes (P_U, r_U, C_U) as input and returns m.*

3.6.2 Security

Our main concern is the GME security against two different types of attacks: 1) by a revoked user or 2) by a hacked SEM. GME must be secure against each of these adversaries considering that each obtains 'half' of the information needed to decrypt. Correspondingly, we define IND-CCA2 security using two different games. The adversary selects the game to play. In the first game, Type 1, the adversary plays the role of a revoked user. After demonstrating knowledge of the private key related to his identity, the revoked user can make Dec_S queries. In the second game, Type 2, the adversary plays the role of a compromised SEM. After demonstrating

knowledge of the private key related to his identity, a compromised SEM can make Dec_U queries. We can say that GME is secure if no adversary can win either Type 1 or Type 2.

Type 1. The challenger runs $Gen_S(k_1)$ and $Gen_U(k_2)$ and gives P_S and P_U to the adversary. The adversary then interleaves key extraction quires and decryption queries with a single challenge query. These queries are answered as follows.

- On key extraction queries $(MS_U, P_U, ID_U,\ MS_S, P_S, ID_S)$, the challenger runs KG_U, KG_S and outputs r_U and r_S corresponding to the identities ID_U and ID_S.
- On decryption queries $(P_S, P_U, ID_U, ID_S, r_U, C)$, the challenger checks that r_U is the private key related to ID_U. If so, it generates r_S and outputs $Dec_U(Dec_S(C))$.
- On challenge query $(P_S, P_U, ID_S^*, ID_U^*, m_0, m_1)$, the challenger checks that r_U^* is the private key related to ID_U^*. Then, upon receiving two messages m_0 and m_1 from the adversary, the challenger chooses a random bit $b \in \{0, 1\}$ and returns $Enc(m_b)$ to the adversary. The adversary is allowed to make key extraction and decryption queries after submitting the challenge.

In the end, the adversary outputs a guess $b' \in \{0, 1\}$. The adversary wins the game if $b' = b$ and ID_S^* and r_S^* were not subject to valid key extraction and decryption queries. The adversary's advantage is defined to be the absolute value of the difference between $1/2$ and its probability of winning.

Type 2. The challenger runs $Gen_S(k_1)$ and $Gen_U(k_2)$ and gives P_S and P_U to the adversary. The adversary then interleaves key extraction and decryption queries with a single challenge query. These queries are answered as follows.

- On key extraction queries $(MS_U, P_U, ID_U,\ MS_S, P_S, ID_S)$, the challenger runs KG_U, KG_S and outputs r_U and r_S corresponding to the identities ID_U and ID_S.
- On decryption queries $(P_S, P_U, ID_U, ID_S, r_S, C)$, the challenger checks that r_S is the private key related to ID_S. If so, it generates r_U and outputs $Dec_U(Dec_S(C))$.
- On challenge query $(P_S, P_U, ID_U^*, ID_S^*, m_0, m_1)$, the challenger checks that r_S^* is the private key related to ID_S^*. Then, upon receiving two messages m_0 and m_1 from the adversary, the challenger chooses a random bit $b \in \{0, 1\}$ and returns $Enc(m_b)$ to the adversary. The adversary is allowed to make key extraction and decryption queries after submitting the challenge.

In the end, the adversary outputs a guess $b' \in \{0, 1\}$. The adversary wins the game if $b' = b$ and ID_U^* and r_U^* were not subject of valid key extraction and decryption queries. The adversary's advantage is defined to be the absolute value of the difference between $1/2$ and its probability of winning.

Definition 3.2. *A generic mediated encryption is secure against adaptive chosen ciphertext attack (IND-GME-CCA2) if no PPT adversary has non-negligible advantage in either Type 1 or Type 2.*

Remark. Type 1 and Type 2 are IND-GME-CCA2 secure if both IBE_S and IBE_U are IND-ID-CCA2 secure. If IBE_S and IBE_U are IND-ID-CPA secure, then Type 1 and Type 2 are modified by eliminating the decryption queries to get IND-GME-CPA security.

3.6.3 Security Proof

The security proof of GME is defined by the following two theorems.

Theorem 3.1. *If an adversary $\mathcal{A}$ who plays the role of a revoked user has an advantage ϵ against GME, then this adversary has the same advantage against IBE_S.*

Theorem 3.2. *If an adversary $\mathcal{A}$ who plays the role of a hacked SEM has an advantage ϵ against GME, then this adversary has the same advantage against IBE_U.*

Proof. Theorem 3.1 stats that the game between an adversary $\mathcal{A}$ who plays the role of a revoked user with a challenger B against GME (Type 1) is identical to the game between the same adversary $\mathcal{A}$ and the challenger B against IBE_S. To prove that, we rewrite Type 1 as follows.

Type 1'.

- The Setup phase is the same as Type 1.
- Key extraction queries are the same as Type 1.
- Decryption queries are the same as Type 1.
- On challenge query $(P_S, P_U, ID_S^*, ID_U^*, m_0, m_1)$, the challenger checks that r_U^* is the private key related to ID_U^*. Then, upon receiving two messages m_0 and m_1 from the adversary, the challenger chooses a random bit $b \in \{0, 1\}$ and returns $Enc(m_b)$ to the adversary. Since the revoked user has r_U, he can partially decrypt the message to get C_S=$Enc_S(m)$ where Enc_S is the SEM's IBE encryption algorithm.

In the end, the adversary outputs a guess $b' \in \{0, 1\}$. The adversary wins the game if $b' = b$ and ID_S^* and r_S^* were not subject of valid key extraction and decryption queries. The adversary's advantage is defined to be the absolute value of the difference between 1/2 and its probability of winning. This concludes Type 1'.

- **Remarks.** Type 1' represents a game against IBE_S because in the challenge phase the adversary $\mathcal{A}$ has to attack $C_S = Enc_S(m)$ to get the message m.
- The only difference between a game against GME (in the case of a revoked user) and IBE_S is the excess information of P_U which does not give the adversary any excessive information to identify m.

This concludes the proof of Theorem 3.1. The proof of Theorem 3.2 is similar.

3.7 Implementation of GME

Generally speaking, a GME is produced by the combination of two IBE systems. To prove that GME is generic, we present GME in two different instantiations. The first one is based on BF FullIdent [BF01] which is a pairing-based IBE. The other instantiation is based on BGH AnonIBE [BGH07] which is not a pairing-based IBE. We note here that the proposed GME systems use the same setup and key generation algorithms for both the users and SEM.

3.7.1 GME_{BF}

Let k be the security parameter given to the setup algorithm and let $\mathcal{IG}$ be a BDH parameter generator.

- $(params) \leftarrow Setup(k)$. The public key generator (PKG) runs $\mathcal{IG}$ on input k to generate groups $\mathbb{G}_1$, $\mathbb{G}_2$ of some prime order q and an admissible pairing $\hat{e} : \mathbb{G}_1 \times \mathbb{G}_1 \rightarrow \mathbb{G}_2$. It picks an arbitrary generator $P \in \mathbb{G}_1$ and a master secret $s \in \mathbb{Z}_q$ and sets $P_{pup} = sP$ and chooses cryptographic hash functions $H_1\{0,1\}^* \rightarrow \mathbb{G}_1$, $H_2 : \mathbb{G}_1 \rightarrow \{0,1\}^n$, $H_3 : \{0,1\}^n \times \{0,1\}^n \rightarrow \mathbb{Z}_q$ and a hash function $H_4 : \{0,1\}^n \rightarrow \{0,1\}^n$ for some n. The system parameters are $params = (\mathbb{G}_1, \mathbb{G}_2, \hat{e}, P_{pup}, H_1, H_2, H_3, H_4)$. The message space is $\mathcal{M} = \{0,1\}^n$. The master secret is $s \in \mathbb{Z}_q$.
- $(r_S, r_U) \leftarrow KG(ID_U, ID_S, s)$. For given strings $ID_U, ID_S \in \{0,1\}^*$, the PKG computes $Q_S = H_1(ID_S)$ and $Q_U = H_1(ID_U)$ and sets the private key $r_S = sQ_S$ and $r_U = sQ_U$.
- $(C) \leftarrow Enc(params, ID_U, ID_S, m)$. To encrypt a message m for a user with identity ID_U, compute $Q_S = H_1(ID_S)$ and $Q_U = H_1(ID_U)$. After that, choose a random $\sigma \in \{0,1\}^n$ and set $r = H_3(\sigma, m)$. The ciphertext C is

$$C = \langle rp, \sigma \oplus H_2(g_U^r) \oplus H_2(g_S^r), m \oplus H_4(\sigma)) \rangle,$$

where $g_U = \hat{e}(Q_U, P_{pub})$ and $g_S = \hat{e}(Q_S, P_{pub})$.

- $(C_U) \leftarrow Dec_S(params, ID_S, C)$. To partially decrypt $C = \langle U, V, W \rangle$ for a SEM with identity ID_S, the user sends C to the SEM. If the user is revoked, the SEM returns $\perp$. If the user is not revoked, the SEM calculates

$$C_U = \langle U, V \oplus H_2(\hat{e}(r_S, U)), W \rangle,$$

  and returns C_U to the user.

- $(m) \leftarrow Dec_U(params, ID_U, C_U)$. After receiving $C_U = \langle U, V_U, W \rangle$, the user computes $V_U \oplus H_2(\hat{e}(r_U, U)) = \sigma$ and $W \oplus H_4(\sigma) = m$ and sets $r = H_3(\sigma, m)$. He outputs m as a decryption of C if $U = rp$. This concludes GME_{BF}.

3.7.2 Security Proof

Theorem 3.3. *Let $\mathcal{A}$ be an IND-GME-CCA2 adversary that has advantage ϵ against GME_{BF}. This adversary $\mathcal{A}$ can be a revoked user or a hacked SEM. Then, there is an IND-ID-CCA2 adversary B with the same probability ϵ against BF FullIdent.*

Proof. If an adversary $\mathcal{A}$ simulates the role of a revoked user, then he plays Type 1 with the challenger. The ciphertext sent to the adversary is $C = \langle rp, m \oplus H_2(g_U^r) \oplus H_2(g_S^r), m \oplus H_4(\sigma) \rangle$. The adversary then partially decrypts it using his secret key r_U to get $C_S = \langle rp, m \oplus H_2(g_S^r), m \oplus H_4(\sigma) \rangle$ which is the message m encrypted by FullIdent using the SEM's ID. This also can be applied for a hacked SEM.

3.7.3 GME_{BGH}

Boneh, Gentry and Hamburg presented an anonymous IND-ID-CPA secure IBE (AnonIBE) [BGH07]. Unlike Boneh-Franklin FullIdent, AnonIBE is CPA secure based on the interactive quadratic residuosity (IQR) assumption. In the following, we present GME based on AnonIBE.

- $(params) \leftarrow Setup(\lambda)$. Using RSAgen($\lambda$), generate ($p$, q), calculate the modulus $N \leftarrow pq$, choose $u \in J(N) \setminus QR(N)$, and choose a hash function $H : ID \rightarrow J(N)$. The public parameters $params$ are $[N, u, H]$. The master secret MS parameters are p, q and a secret key K for a pseudorandom function (PRF) $F_K : ID \rightarrow [0, 1, 2, 3]$.

- $(r_i) \leftarrow KeyGen(MS, ID, l)$. Calculate $R_i \leftarrow H(ID, i) \in J(N)$ for each bit i and $w \leftarrow F_K(ID) \in \{0, 1, 2, 3\}$. Choose $a \in \{0, 1\}$ such that $u^a R_i \in QR(N)$. Let $[z_0, z_1, z_2, z_3]$ be the four square roots of $u^a R_i \in \mathbb{Z}_N$, then $r_i \leftarrow z_w$.

- $(C) \leftarrow Enc(params, R_{U,i}, R_{S,i}, m)$. To encrypt a message $m \in \{-1,1\}^l$, choose a random value $s \in \mathbb{Z}_{\mathbb{N}}$ and calculate $S = s^2$. Then calculate $[x_{U,i}, y_{U,i}, x_{S,i}, y_{S,i}, \alpha, \beta]$, $i \in [0, l-1]$ that satisfy the following equations.

$$\begin{aligned}[x_{U,i}, y_{U,i}] \leftarrow R_{U,i}x_{U,i}^2 + Sy_{U,i}^2 \equiv 1 \pmod N,\\ [x_{S,i}, y_{S,i}] \leftarrow R_{S,i}x_{S,i}^2 + Sy_{S,i}^2 \equiv 1 \pmod N,\\ [\alpha, \beta] \leftarrow u\alpha^2 + S\beta^2 \equiv 1 \pmod N,\end{aligned}$$

  These equations are solved as shown in [BGH07].

  The message $m \leftarrow [m_0, m_1, ..., m_{l-1}]$ is encrypted using the following equation.

$$c_i \leftarrow m_i \cdot \left(\frac{2y_{U,i}s + 2}{N}\right) \cdot \left(\frac{2y_{S,i}s + 2}{N}\right).$$

  The ciphertext is (S, T, c) where $T = \left(\frac{\beta s+1}{N}\right)$ and $c = [c_0, c_1, ..., c_{l-1}]$.

- $(C_U) \leftarrow Dec_S(params, ID_S, C)$. To decrypt a ciphertext $C = (S, T, c)$ for a user with public key ID_U, he sends C to the SEM. The SEM then does the following.

- if U is revoked, the SEM returns $\perp$.

- if U is not revoked, the SEM calculates $c_{U,i}$ as follows.

$$c_{U,i} \leftarrow c_i \cdot \left(\frac{x_{S,i}r_{S,i} + 1}{N}\right) \quad \text{if } r_{S,i}^2 = R_{S,i}.$$

$$c_{U,i} \leftarrow c_i \cdot \left(\frac{1 + Sy_{S,i}\beta + \alpha x_{S,i}r_{S,i}}{N}\right) \cdot T \quad \text{if } r_{S,i}^2 = uR_{S,i}.$$

  and returns $C_U = [c_{U,1}, c_{U,2}, ..., c_{U,l}]$ to the user along with T and S. Then the user decrypts C_U similar to the SEM to get the message m. This concludes GME_{BGH}.

3.7.4 Security Proof

Theorem 3.4. *Let $\mathcal{A}$ be an Anon-IND-GME-CPA adversary that has advantage ϵ against GME_{BGH}. This adversary $\mathcal{A}$ can be a revoked user or hacked SEM. Then, there is an Anon-IND-ID-CPA adversary B with the same probability ϵ against AnonIBE.*

Proof. If an adversary $\mathcal{A}$ simulates the role of a revoked user, then he plays Type 1 with the challenger. The ciphertext sent to the adversary is $c_i \leftarrow m_i \cdot \left(\frac{2y_{U,i}s+2}{N}\right) \cdot \left(\frac{2y_{S,i}s+2}{N}\right)$. The adversary then partially decrypts it using his secret key

r_U to get $c_{S,i} \leftarrow m_i \cdot \left(\frac{2y_{S,i}s+2}{N}\right)$ which is the message m encrypted by AnonIBE using SEM's ID. This also can be applied for a hacked SEM.

3.8 Conclusion

In this chapter, we investigate the mediated structure of IB-mRSA which is a solution to the key revocation problem in the identity-based settings. We showed that using a division intractable hash function does not necessarily guarantee that the generated public keys are also division intractable. Consequently, the system may not be secure even if the hash function used is division intractable. We proposed two solutions to overcome this drawback. After applying these modifications, IB-mRSA is secure in the random oracle model if the mapping function parameters have been chosen correctly. After that, we extended the idea of IB-mRSA to be generic by presenting a generic mediated encryption (GME) system that converts any IBE to a mediated system. Although it is based on double encryption, GME is efficient. The ciphertext size is the same as a single IBE. It combines the advantage of CBE and SEM structures. GME is more efficient than CBE because it does not depend on certificates and it is more secure than [BDTW01] and [Gen06] because the SEM in GME is not a single point of failure and can be untrusted. We prove that GME is as secure as the IBE used in the case of a revoked user or a hacked SEM.

Chapter 4

Efficient Pairing-Free IBE Systems Based on The Quadratic Residuosity Assumption

Most identity-based encryption (IBE) systems are constructed using bilinear maps on elliptic curves (pairings). Two elegant exceptions are due to Cocks [Coc01] and Boneh, Gentry and Hamburg [BGH07]. Cocks' IBE is based on the quadratic residuosity (QR) assumption. It is time-efficient compared to pairing-based IBE systems but produces a long ciphertext of $2l(\log_2 N)$ bits for an l-bit message where N is an RSA composite. Boneh, Gentry and Hamburg presented two IBE systems known as BasicIBE and AnonIBE. These IBE systems have short ciphertext of $\log_2 N$ plus $2l$ bits for BasicIBE and $\log_2 N$ plus $l+1$ bits for AnonIBE but this comes at the cost of less time-efficient algorithms in which their processing time increases drastically with the message length. In addition, the private key of these IBE systems is l elements in $\mathbb{Z}_{\mathbb{N}}$. In this chapter, we optimise these IBE systems in two steps. First, we decrease the private key length from l elements in $\mathbb{Z}_{\mathbb{N}}$ to only one element. Second, we present two efficient variants of Boneh, Gentry and Hamburg (BGH) IBE systems in terms of ciphertext length and encryption/decryption speed. The ciphertext is as short as BGH systems, but with more time-efficient algorithms which do not depend on the message length. We prove that these variants are as secure as the BGH systems.

4.1 Introduction

In 1985, Shamir [Sha84] presented the notion of identity-based encryption (IBE) in which the user's identity represents his public key and consequently, no public key certificate is required. Shamir successfully managed to design an identity-based signature based on the RSA algorithm but he was unable to design an IBE because sharing an RSA modulus between different users makes RSA insecure [Sha84]. The design of a provable secure IBE remained an open problem for sixteen years until Boneh and Franklin [BF01] proposed a provably secure IBE in the random oracle model based on bilinear maps. Subsequently, there has been a rapid development in IBE based on bilinear maps, such as [BB04a, BB04b, Gen06, Wat05]. Another approach to design IBE systems is based on the quadratic residuosity (QR) assump-

tion. The first IBE based on this approach is due to Cocks [Coc01]. This IBE is IND-ID-CPA secure in the random oracle model. It is time-efficient compared to pairing-based IBE systems, but it produces a long ciphertext of two elements in $\mathbb{Z}_{\mathbb{N}}$ for every bit in the message.

The design of efficient IBE systems without pairings was an open problem until Boneh, Gentry and Hamburg [BGH07] presented two space-efficient IBE systems (BasicIBE and AnonIBE). Although the concrete instantiation of BGH systems is highly space-efficient, this comes at the cost of less time-efficient encryption/decryption algorithms. To encrypt an l-bit message, these systems solves $l+1$ equations in the form $Rx^2 + Sy^2 \equiv 1 \pmod{N}$ for known values of R, S and N [BGH07]. Solving such an equation requires a 'solubility certificate' and obtaining these certificates requires the generation of primes [Coc01, CR03, Kel08]. The obtained certificates can be used to solve $Rx^2 + Sy^2 \equiv 1 \pmod{N}$ efficiently using the Cremona-Rusin algorithm [CR03]. The prime generation is a time-consuming process and it is the bottleneck in BGH systems. In addition, the decryption key is l elements in $\mathbb{Z}_{\mathbb{N}}$ because the identity ID is hashed to a different value to encrypt each bit. BasicIBE is IND-ID-CPA secure in the random oracle model under the quadratic residuosity (QR) assumption while AnonIBE is Anon-IND-ID-CPA secure in the standard model under the interactive quadratic residuosity (IQR) assumption [BGH07].

Our Contribution. In this chapter, we first prove that hashing the identity ID to a different value to encrypt each bit is as secure as hashing the identity once to encrypt the whole message and therefore, the private key length is reduced to one element in $\mathbb{Z}_{\mathbb{N}}$. Then, we present two variants of BasicIBE and AnonIBE (V-BasicIBE, V-AnonIBE) which are both time- and space-efficient. We prove that these variants are as secure as the original BGH systems. Although the proposed variants are space-efficient as BGH systems, they only solve two equations in the form $Rx^2 + Sy^2 \equiv 1 \pmod{N}$ regardless of the message length. We also present other versions of these variants with a time-space trade-off. For V-BasicIBE, with only the cost of one more element in $\mathbb{Z}_{\mathbb{N}}$, the sender can find a solution to $Rx^2 + Sy^2 \equiv 1 \pmod{N}$ using only one inversion in $\mathbb{Z}_{\mathbb{N}}$ and the receiver does not have to solve any of these equations. This time-space trade-off is applied for V-AnonIBE at the cost of four more elements in $\mathbb{Z}_{\mathbb{N}}$. Table 4.1 compares all IBE systems in this chapter, where V2-BasicIBE and V2-AnonIBE are the proposed IBE systems with the trade-off applied.

Table 4.1: Comparison Between all IBE Systems in This Chapter

	Ciphertext size	Number of equations	Private key length
Cock's	$2l(\log_2 N)$	0	$\log_2 N$
BasicIBE	$\log_2 N + 2l$	$l+1$	$l(\log_2 N)$
AnonIBE	$\log_2 N + l + 1$	$l+1$	$l(\log_2 N)$
Jhanwar-Barua	$2\sqrt{l}\log_2 N + 2l$	$\sqrt{l}$	$\log_2 N$
V-BasicIBE	$\log_2 N + 2l$	2	$\log_2 N$
V-AnonIBE	$\log_2 N + 2l$	2	$\log_2 N$
V2-BasicIBE	$2\log_2 N + 2l$	0	$\log_2 N$
V2-AnonIBE	$5\log_2 N + 2l$	0	$\log_2 N$

4.2 Optimisation of BGH Systems

4.2.1 Optimisation of The Private Key Length

Both BGH systems hash the identity ID to different values $H(ID, i) = u^a R_i = r_i^2, a \in \{0, 1\}$. This has negative impacts on these systems. First, the private key length is larger than the message by a factor of an element in $\mathbb{Z}_{\mathbb{N}}$ which consumes bandwidth and memory. Second, the PKG must generate n private keys of l elements in $\mathbb{Z}_{\mathbb{N}}$ where n is the number of users in the whole system. This overloads the PKG. Third, this not suitable for encrypting variable message lengths.

In this section, we prove that hashing the identity ID to different values $R_i = H(ID, i)$ does not have a positive impact on the security of BasicIBE or AnonIBE. Solving the equations $Rx_i^2 + Sy_i^2 \equiv 1 \pmod N$ is exactly equivalent to solving the equations $R_i x_i^2 + Sy_i^2 \equiv 1 \pmod N$. Consequently, there is no need for generating a long private key of l elements in $\mathbb{Z}_{\mathbb{N}}$.

Theorem 4.1. *Hashing the identity ID to a different value to encrypt each bit is as secure as hashing the identity once to encrypt the whole message.*

Proof. Jhanwar and Barua [JB08] showed that there are $N - 1$ solutions for the equation $Rx^2 + Sy^2 \equiv 1 \pmod N$ if $S, R \in QR(N)$. The solution (x, y) for that equation is in the form.

$$\left(\frac{-2st}{R + St^2}, \frac{R - St^2}{s(R + St^2)}\right),$$

for some random value $t \in \mathbb{Z}_{\mathbb{N}}^*$ such that $R + St^2 \in \mathbb{Z}_{\mathbb{N}}^*$.

$$Rx_i^2 + Sy_i^2 = R\left(\frac{-2st}{R + St^2}\right)^2 + Sy_i^2 = \left(\frac{4SR}{(R + St^2)^2}\right)t^2 + Sy_i^2 = R_i\overline{x}_i^2 + Sy_i^2,$$

$$\textit{where } R_i = t^2 \textit{ and } \overline{x}_i = \frac{-2sr}{R + St^2}.$$

Since t is random in $\mathbb{Z}_{\mathbb{N}}^*$, R looks mathematically random exactly as $R_i = H(ID, i)$. □ □

This does not improve the performance of BGH systems though. These systems still require solving $l + 1$ equations in the form $Rx_i^2 + Sy_i^2 \equiv 1 \pmod N$. This requires generating new primes for each bit like the original BGH systems (low time-efficiency), or generating random solutions to these equations and sending them along with the ciphertext like Jhanwar-Barua IBE (low space-efficiency) [JB08].

4.3 V-BasicIBE

In this section, we explain how to implement a variant of BasicIBE (V-BasicIBE) that is both time- and space-efficient. Like any other IBE, V-BasicIBE consists of four algorithms: Setup, Extract, Encrypt and Decrypt.

- $(params) \leftarrow Setup(\lambda)$. Using RSAgen($\lambda$), generate (p, q), calculate the modulus $N \leftarrow pq$, choose $u \in J(N) \setminus QR(N)$, and choose a hash function $H : ID \rightarrow J(N)$. The public parameters $params$ are $[N, u, H]$. The master secret MS parameters are p, q and a secret key K for a pseudorandom function (PRF) $F_K : ID \rightarrow [0, 1, 2, 3]$.

- $(r) \leftarrow Extract(MS, ID)$. Calculate $R \leftarrow H(ID) \in J(N)$ and $w \leftarrow F_K(ID) \in \{0, 1, 2, 3\}$. Choose $a \in \{0, 1\}$ such that $u^a R \in QR(N)$. Let $[z_0, z_1, z_2, z_3]$ be the four square roots of $u^a R \in \mathbb{Z}_{\mathbb{N}}$, then $r \leftarrow z_w$.

- $(C) \leftarrow Encrypt(params, ID, m)$. To encrypt a message $m \in \{-1, 1\}^l$, V-BasicIBE calculates $[x_i, y_i, \overline{x}_i, \overline{y}_i]$, $i \in [0, l-1]$ that satisfy the following equations.

$$[x_i, y_i] \leftarrow Rx_i^2 + S^j y_i^2 \equiv 1 \pmod N, [\overline{x}_i, \overline{y}_i] \leftarrow uR\overline{x}_i^2 + S^j \overline{y}_i^2 \equiv 1 \pmod N \quad (4.1)$$

  for an odd number $j = 2i + 1$. To solve these equations, we review a product formula presented by Jhanwar and Barua [JB08] in which they presented a variant of Lemma 2.1 to implement their IBE. This lemma states that,

  Lemma 4.1. *For $i = 1, 2$ let (x_i, y_i) be a solution to $Rx^2 + S_i y^2 \equiv 1 \pmod N$. Then (x_3, y_3) is a solution to*

$$Rx^2 + S_1 S_2 y^2 \equiv 1 \pmod N,$$

  where $x_3 = \frac{x_1 + x_2}{Rx_1x_2+1}$ and $y_3 = \frac{y_1 y_2}{Rx_1x_2+1}$

  Proof. Same as Lemma 2.1. □

V-BasicIBE calculates $[x_0, y_0]$ and then uses Lemma 4.1 to find $[x_i, y_i]$ as follows.

$$\hat{x} = \frac{2x_0}{Rx_0^2 + 1} \ \ and \ \ \hat{y} = \frac{y_0^2}{Rx_0^2 + 1},$$
$$x_i = \frac{\hat{x} + x_{i-1}}{R\hat{x}x_{i-1} + 1} \ \ and \ \ y_i = \frac{\hat{y}y_{i-1}}{R\hat{x}x_{i-1} + 1},$$

where $[\hat{x}, \hat{y}]$ is a solution to $R\hat{x}^2 + S^2\hat{y}^2 \equiv 1 \pmod N$. Similarly, $[\overline{x}_i, \overline{y}_i]$ are generated as shown above.

The message $m \leftarrow [m_0, m_1, ..., m_{l-1}]$ is encrypted using the following formula.

$$c_i \leftarrow m_i \cdot \left(\frac{2y_i s^j + 2}{N}\right) \ \ and \ \ \overline{c}_i \leftarrow m_i \cdot \left(\frac{2\overline{y}_i s^j + 2}{N}\right).$$

The ciphertext is $C \leftarrow (S, c, \overline{c})$.

- $(m) \leftarrow Decrypt(C, r)$. The message can be retrieved from the ciphertext as follows.

$$m_i \leftarrow c_i \cdot \left(\frac{x_i r + 1}{N}\right) \quad \text{if } r^2 = R \ , \ m_i \leftarrow \overline{c}_i \cdot \left(\frac{\overline{x}_i r + 1}{N}\right) \quad \text{if } r^2 = uR.$$

Correctness. As in [BGH07], it is easy to prove that.

$$\begin{aligned}(x_i r + 1) \cdot (2y_i s^j + 2) &= 2x_i r y_i s^j + 2x_i r + 2y_i s^j + 2 + (Rx_i^2 + S^j y_i^2 - 1) \\ &= (x_i r + y_i s^j + 1)^2, \\ \left(\frac{x_i r + 1}{N}\right) \cdot \left(\frac{2y_i s^j + 2}{N}\right) &= 1 \\ \left(\frac{x_i r + 1}{N}\right) &= \left(\frac{2y_i s^j + 2}{N}\right).\end{aligned}$$

- **Remarks**. $\hat{y}, \hat{x}$ cannot be used to encrypt or decrypt messages. That is because the encryption key for $\hat{y}$ is the Jacobi symbol $\left(\frac{2\hat{y}s^2+2}{N}\right) = \left(\frac{2\hat{y}S+2}{N}\right)$ which can be easily calculated. The variables $\hat{y}, \hat{x}$ are only used to generate x_i, y_i. The variable j in the equation $Rx^2 + S^j y^2 \equiv 1 \pmod N$ must be odd for the same reason.

- The variables $[\overline{x}_i, \overline{y}_i]$ can be generated in another way as follows. V-BasicIBE first generates $[x_i, y_i]$ and $[\alpha_i, \beta_i]$ such that $[x_i, y_i] \leftarrow Rx_i^2 + S^j y_i^2 \equiv 1 \pmod N$ and $[\alpha_i, \beta_i] \leftarrow u\alpha_i^2 + S^j \beta_i^2 \equiv 1 \pmod N$ using Lemma 4.1 as shown above. After that, it uses $[x_i, y_i]$ and $[\alpha_i, \beta_i]$ to generate $[\overline{x}_i, \overline{y}_i]$ using Lemma 2.1.

4.3.1 V-BasicIBE Security

Theorem 4.2. *Suppose the quadratic residuosity assumption holds for RSAgen and F is a secure PRF. Then the proposed V-BasicIBE is IND-ID-CPA secure based on the QR assumption when H is modelled as a random oracle. In particular, suppose $\mathcal{A}$ is an efficient IND-ID-CPA adversary, then there exist efficient algorithms B_1, B_2 whose running time is the same as that of $\mathcal{A}$ such that,*

$$IBEAdv_{\mathcal{A},V-BasicIBE}(\lambda) \leq 2QRAdv_{B_2,RSAgen}(\lambda) + PRFAdv_{B_1,F}(\lambda).$$

Proof. We first introduce Lemma 4.2.

Lemma 4.2. *Let $N = pq$ be an RSA modulus, $S, R \in J(N)$. Then*

- *1-When $R \in J(N) \setminus QR(N)$, $S \in QR(N)$, the Jacobi symbols $\left(\frac{g(y_i,s)}{N}\right)$ are uniformly distributed in $\{\pm 1\}$ for any function g, where s is a random variable uniformly chosen among the four square roots of S modulo N and $g(y_i, s)g(y_i, -s)R \in QR(N)$ for all the four values of s.*
- *2-When $S \in J(N) \setminus QR(N)$, $R \in QR(N)$, the Jacobi symbols $\left(\frac{f(x_i,r)}{N}\right)$ are uniformly distributed in $\{\pm 1\}$ for any function f, where r is a random variable uniformly chosen among the four square roots of R modulo N and $f(x_i, r)f(x_i, -r)S \in QR(N)$ for all the four values of r.*
- *3-When $S, R \in QR(N)$, the Jacobi symbols $\left(\frac{g(y_i,s)}{N}\right)$ and $\left(\frac{f(x_i,r)}{N}\right)$ are constant, i.e. the same for all four values of r and s .*

Proof. Let $s, \overline{s}$ be the four square roots of $S \in QR(N)$ such that $\overline{s} = s \pmod p$ and $\overline{s} = -s \pmod q$, then the four square roots of S are $\{\pm\overline{s}, \pm s\}$. We can assume the same for $R \in QR(N)$ and the four square roots are $\{\pm\overline{r}, \pm r\}$, where $\overline{r} = r \pmod p$ and $\overline{r} = -r \pmod q$. We prove the three cases of Lemma 4.2 as follows.

Case 1

Since $g(y_i, s)g(y_i, -s)R \in QR(N)$

$$\left(\frac{g(y_i, s)g(y_i, -s)R}{N}\right) = \left(\frac{g(y_i, s)g(y_i, -s)R}{p}\right) = \left(\frac{g(y_i, s)g(y_i, -s)R}{q}\right) = 1.$$

Since $R \in J(N) \setminus QR(N)$

$$\left(\frac{R}{p}\right) = \left(\frac{R}{q}\right) = -1,$$

$$\left(\frac{g(y_i,s)g(y_i,-s)}{p}\right)=\left(\frac{g(y_i,s)g(y_i,-s)}{q}\right)=-1,$$
$$\left(\frac{g(y_i,s)}{p}\right)=-\left(\frac{g(y_i,-s)}{p}\right) \quad and \quad \left(\frac{g(y_i,s)}{q}\right)=-\left(\frac{g(y_i,-s)}{q}\right),$$
$$\left(\frac{g(y_i,s)}{N}\right)=\left(\frac{g(y_i,-s)}{N}\right).$$

Since $\overline{s}=s \pmod p$,

$$g(y_i,\overline{s})=g(y_i,s) \pmod p,$$
$$\left(\frac{g(y_i,\overline{s})}{p}\right)=\left(\frac{g(y_i,s)}{p}\right).$$

Since $\overline{s}=-s \pmod q$,

$$g(y_i,\overline{s})=g(y_i,-s) \pmod q,$$
$$\left(\frac{g(y_i,\overline{s})}{q}\right)=\left(\frac{g(y_i,-s)}{q}\right)=-\left(\frac{g(y_i,s)}{q}\right),$$
$$\left(\frac{g(y_i,\overline{s})}{p}\right)\left(\frac{g(y_i,\overline{s})}{q}\right)=-\left(\frac{g(y_i,s)}{p}\right)\left(\frac{g(y_i,s)}{q}\right),$$
$$\left(\frac{g(y_i,\overline{s})}{N}\right)=-\left(\frac{g(y_i,s)}{N}\right),$$
$$\left(\frac{g(y_i,\overline{s})}{N}\right)=\left(\frac{g(y_i,-\overline{s})}{N}\right)=-\left(\frac{g(y_i,s)}{N}\right)=-\left(\frac{g(y_i,-s)}{N}\right).$$

This means that among the four Jacobi symbols $\left(\frac{g(y_i,\overline{s})}{N}\right), \left(\frac{g(y_i,-\overline{s})}{N}\right), \left(\frac{g(y_i,s)}{N}\right), \left(\frac{g(y_i,-s)}{N}\right)$ two are $+1$ and two are -1. □

Case 2

Since $f(x_i,r)f(x_i,-r)S \in QR(N)$,

$$\left(\frac{f(x_i,r)f(x_i,-r)S}{N}\right)=\left(\frac{f(x_i,r)f(x_i,-r)S}{p}\right)=\left(\frac{f(x_i,r)f(x_i,-r)S}{q}\right)=1.$$

Since $S \in J(N) \setminus QR(N)$,

$$\left(\frac{S}{p}\right)=\left(\frac{S}{q}\right)=-1,$$
$$\left(\frac{f(x_i,r)f(x_i,-r)}{p}\right)=\left(\frac{f(x_i,r)f(x_i,-r)}{q}\right)=-1,$$
$$\left(\frac{f(x_i,r)}{p}\right)=-\left(\frac{f(x_i,-r)}{p}\right) \quad and \quad \left(\frac{f(x_i,r)}{q}\right)=-\left(\frac{f(x_i,-r)}{q}\right),$$
$$\left(\frac{f(x_i,r)}{N}\right)=\left(\frac{f(x_i,-r)}{N}\right).$$

Since $\overline{r}=r \pmod p$,

$$f(x_i,\overline{r})=f(x_i,r) \pmod p,$$

$$\left(\frac{f(x_i,\overline{r})}{p}\right)=\left(\frac{f(x_i,r)}{p}\right),$$

Since $\overline{r}=-r \pmod q$.

$f(x_i,\overline{r})=f(x_i,-r) \pmod q$,

$$\left(\frac{f(x_i,\overline{r})}{q}\right)=\left(\frac{f(x_i,-r)}{q}\right)=-\left(\frac{f(x_i,r)}{q}\right),$$

$$\left(\frac{f(x_i,\overline{r})}{p}\right)\left(\frac{f(x_i,\overline{r})}{q}\right)=-\left(\frac{f(x_i,r)}{p}\right)\left(\frac{f(x_i,r)}{q}\right),$$

$$\left(\frac{f(x_i,\overline{r})}{N}\right)=-\left(\frac{f(x_i,r)}{N}\right),$$

$$\left(\frac{f(x_i,\overline{r})}{N}\right)=\left(\frac{f(x_i,-\overline{r})}{N}\right)=-\left(\frac{f(x_i,r)}{N}\right)=-\left(\frac{f(x_i,-r)}{N}\right).$$

This means that among the four Jacobi symbols $\left(\frac{f(x_i,\overline{r})}{N}\right),\left(\frac{f(x_i,-\overline{r})}{N}\right),\left(\frac{f(x_i,r)}{N}\right),\left(\frac{f(x_i,-r)}{N}\right)$ two are $+1$ and two are -1. □

Case 3

Since $S,R\in QR(N)$,

Since $f(x_i,r)f(x_i,-r)S, g(y_i,s)g(y_i,-s)R\in QR(N)$,

$f(x_i,r)f(x_i,-r), g(y_i,s)g(y_i,-s)\in QR(N)$,

$$\left(\frac{f(x_i,r)f(x_i,-r)}{p}\right)=\left(\frac{f(x_i,r)f(x_i,-r)}{q}\right)=$$

$$\left(\frac{g(y_i,s)g(y_i,-s)}{p}\right)=\left(\frac{g(y_i,s)g(y_i,-s)}{q}\right)=1,$$

$$\left(\frac{f(x_i,r)}{p}\right)=\left(\frac{f(x_i,-r)}{p}\right)\ \ and\ \ \left(\frac{f(x_i,r)}{q}\right)=\left(\frac{f(x_i,-r)}{q}\right),$$

$$\left(\frac{g(y_i,s)}{p}\right)=\left(\frac{g(y_i,-s)}{p}\right)\ \ and\ \ \left(\frac{g(y_i,s)}{q}\right)=\left(\frac{g(y_i,-s)}{q}\right).$$

Since $\overline{r}=r \pmod p$, $\overline{r}=-r \pmod q$

$\overline{s}=s \pmod p$ *and* $\overline{s}=-s \pmod q$,

$$\left(\frac{f(x_i,\overline{r})}{p}\right)=\left(\frac{f(x_i,r)}{p}\right)\ \ and\ \ \left(\frac{f(x_i,\overline{r})}{q}\right)=\left(\frac{f(x_i,-r)}{q}\right),$$

$$\left(\frac{g(y_i,\overline{s})}{p}\right)=\left(\frac{g(y_i,s)}{p}\right)\ \ and\ \ \left(\frac{g(y_i,\overline{s})}{q}\right)=\left(\frac{g(y_i,-s)}{q}\right),$$

$$\left(\frac{f(x_i,\overline{r})}{p}\right)=\left(\frac{f(x_i,r)}{p}\right)=\left(\frac{f(x_i,-\overline{r})}{p}\right)=\left(\frac{f(x_i,-r)}{p}\right),$$

$$\left(\frac{f(x_i,\overline{r})}{q}\right)=\left(\frac{f(x_i,r)}{q}\right)=\left(\frac{f(x_i,-\overline{r})}{q}\right)=\left(\frac{f(x_i,-r)}{q}\right),$$

$$\left(\frac{g(y_i,\overline{s})}{p}\right)=\left(\frac{g(y_i,s)}{p}\right)=\left(\frac{g(y_i,-\overline{s})}{p}\right)=\left(\frac{g(y_i,-s)}{p}\right)$$
$$\left(\frac{g(y_i,\overline{s})}{q}\right)=\left(\frac{g(y_i,s)}{q}\right)=\left(\frac{g(y_i,-\overline{s})}{q}\right)=\left(\frac{g(y_i,-s)}{q}\right),$$
$$\left(\frac{f(x_i,\overline{r})}{N}\right)=\left(\frac{f(x_i,r)}{N}\right)=\left(\frac{f(x_i,-\overline{r})}{N}\right)=\left(\frac{f(x_i,-r)}{N}\right).$$
$$\left(\frac{g(y_i,\overline{s})}{N}\right)=\left(\frac{g(y_i,s)}{N}\right)=\left(\frac{g(y_i,-\overline{s})}{N}\right)=\left(\frac{g(y_i,-s)}{N}\right)\square.$$

- **Security Proof.** We define two sequences of games and let W_i represents the winning of the i_{th} game and $\overline{W}_i$ represents the winning of the $\overline{i}_{th}$ game by the adversary $\mathcal{A}$. The security proof can be proved in two ways, Proof 1 and Proof 2. Both proofs have in common the games from **Game-0** to **Game-3**. **Game-4** to **Game-7** belongs to Proof 1 and **Game-**$\overline{4}$ to **Game-**$\overline{7}$ belongs to Proof 2. Any of these proofs can prove the security of the V-BasicIBE. These games are defined as follows.

  - **Game-0**. This game is the usual adversarial game.
  - **Game-1**. This game replaces the PRF F with a truly random function.
  - **Game-2**. This game explains how to simulate the hash function H.
  - **Game-3**. This game sets $u \in QR(N)$.
  - **Game-4**. This game explains how to respond to a challenge query from $\mathcal{A}$.
  - **Game-**$\overline{4}$. This game explains how to respond to a challenge query using the *Decrypt* algorithm.
  - **Game-5**. This game sets $R \in J(N) \setminus QR(N)$.
  - **Game-**$\overline{5}$. This game sets $S^j \in J(N) \setminus QR(N)$.
  - **Game-6**. This game sets $S_i = s_i^2$ for each bit.
  - **Game-**$\overline{6}$. This game sets $R_i = H(ID, i)$ for each bit.
  - **Game-7** and **Game-**$\overline{7}$ replace the message m with a random number z.

- Game-0. This is the usual adversarial game for defining the IND-ID-CPA security of IBE protocols. The challenger picks the random oracle $H : ID \rightarrow J(N)$ at random from the set of all such functions in the *Setup* algorithm and allows $\mathcal{A}$ to query H at arbitrary points. Thus, we have,

$$|\Pr[W_0] - \frac{1}{2}| = IBEAdv_{\mathcal{A},V-BasicIBE}(\lambda).$$

- Game-1. This is the same as Game-0, with the following change. In the *Setup* algorithm, instead of using a PRF F to respond to $\mathcal{A}$'s private key queries, we

use a truly random function $f : ID \rightarrow \{0, 1, 2, 3\}$. If F is a secure PRF, $\mathcal{A}$ will not notice the difference between Game-0 and Game-1. In particular, there exists an algorithm B_1 (whose running time is about the same as that of $\mathcal{A}$) such that,

$$|\Pr[W_1] - \Pr[W_0]| = PRFAdv_{B_1,F}(\lambda).$$

- Game-2. (N, u, H) are the public parameters $params$ given to $\mathcal{A}$ in the previous game where u is uniform in $J(N) \setminus QR(N)$ and the random oracle H is a random function $H : ID \rightarrow J(N)$. We make the following change in the random oracle H in this game. The challenger responds to a query to $H(ID)$ by picking $a \in_R \{0, 1\}$ and $v \in_R \mathbb{Z}_{\mathbb{N}}$ and setting $H(ID) = u^a v^2$. Thus the challenger implements a random function $H : ID \rightarrow J(N)$ as in the previous game. The challenger responds to a private key query as follows.

  Suppose $R = H(ID) = u^a v^2$ for some $a \in_R \{0, 1\}$ and $v \in_R \mathbb{Z}_{\mathbb{N}}$. The challenger responds to a private key query for ID by setting either $R^{\frac{1}{2}} = v$ (when $a = 0$) or $(uR)^{\frac{1}{2}} = uv$ (when $a = 1$). Since v is uniform in $\mathbb{Z}_{\mathbb{N}}$, this will produce a square root of R or uR which is also uniform among the four square roots, as in the previous game. Thus, $\mathcal{A}$'s views in Game-1 and Game-2 are identical and therefore,

  $$|\Pr[W_2] = \Pr[W_1]|.$$

- Game-3. In this game, the challenger chooses u uniformly in $QR(N)$ instead of $J(N) \setminus QR(N)$. Since this is the only change between Game-2 and Game-3, $\mathcal{A}$ will not notice the difference assuming that the QR assumption holds for RSAgen. In particular, there exists an algorithm B_2 (whose running time is about the same as that of $\mathcal{A}$) such that,

  $$|\Pr[W_3] - \Pr[W_2]| = QRAdv_{B_2,RSAgen}(\lambda).$$

- Game-4. We describe below in detail how, in this game, the challenger responds to a challenge query from $\mathcal{A}$.

  - He chooses $uR, R \in QR(N)$. (*)
  - He chooses $s \in_R \mathbb{Z}_{\mathbb{N}}$ and computes $S^j = s^{2j}$ for an odd value j.
  - Upon receiving two messages m_0, m_1 from the adversary, the challenger tosses a fair coin $b \in \{0, 1\}$ and sets $(C) \leftarrow Encrypt(params, ID, m_b)$.
  - He sends $C = (S, c, \overline{c})$ to $\mathcal{A}$.

Since this game is the same as Game-3, thus,

$$|\Pr[W_4] = \Pr[W_3]|.$$

- Game-$\overline{4}$. This game is the same as Game-3 except that the challenger handles a challenge query from $\mathcal{A}$ differently. To encrypt a message m for an identity ID, the challenger does the following.
  - He chooses $uR, R \in QR(N)$.
  - He chooses $s \in_R \mathbb{Z}_{\mathbb{N}}$ and computes $S^j = s^{2j}$ for an odd value j. (*)
  - Upon receiving two messages m_0, m_1 from the adversary, the challenger tosses a fair coin $b \in \{0, 1\}$ and sets $(C) \leftarrow Decrypt(r, params, (S, m_b))$.
  - He sends $C = (S, c, \overline{c})$ to $\mathcal{A}$.

  $(c, \overline{c})$ are calculated as $c_i \leftarrow m_i \cdot \left(\frac{x_i r+1}{N}\right)$ and $\overline{c}_i \leftarrow m_i \cdot \left(\frac{\overline{x}_i r+1}{N}\right)$. It is easy to see that C is a unique encryption of m. Since this game is the same as Game-3, thus,

$$|\Pr[\overline{W}_4] = \Pr[W_3]|.$$

- Game-5. In this game, we make a change in the challenge phase. We replace the line (*) in Game-4 with the following.
  - He chooses $uR, R \in J(N) \setminus QR(N)$.

  Since the only difference between Game-5 and Game-4 is that $uR, R \in J(N) \setminus QR(N)$ in Game-5 instead of $uR, R \in QR(N)$ in Game-4, $\mathcal{A}$ will not notice the difference assuming that the QR assumption holds for RSAgen. In particular, there exists an algorithm B_2 (whose running time is about the same as that of $\mathcal{A}$) such that,

$$|\Pr[W_5] - \Pr[W_4]| = QRAdv_{B_2, RSAgen}(\lambda).$$

- Game-$\overline{5}$. This game is similar to Game-5. We replace the line (*) in Game-$\overline{4}$ with the following:
  - He chooses $S^j \in J(N) \setminus QR(N)$.

  The only difference between Game-$\overline{5}$ and Game-$\overline{4}$ is that $S^j \in J(N) \setminus QR(N)$ in Game-$\overline{5}$ instead of $S^j \in QR(N)$ in Game-$\overline{4}$ so $\mathcal{A}$ will not notice the difference assuming that the QR assumption holds for RSAgen. In particular, there exists an algorithm B_2 (whose running time is about the same as that of $\mathcal{A}$) such that,

$$|\Pr[\overline{W}_5] - \Pr[\overline{W}_4]| = QRAdv_{B_2, RSAgen}(\lambda).$$

- Game-6. In this game, we encrypt the message by choosing $S_i \in \mathbb{Z}_{\mathbb{N}}$ independently and randomly for each bit. In other words, we replace the Jacobi symbols $\left(\frac{2y_i s^j+2}{N}\right)$ and $\left(\frac{2\overline{y}_i s^j+2}{N}\right)$ with the Jacobi symbols $\left(\frac{2y_i s_i+2}{N}\right)$ and $\left(\frac{2\overline{y}_i s_i+2}{N}\right)$ respectively i.e $c_i = m_i \cdot \left(\frac{2y_i s_i+2}{N}\right)$ and $\overline{c}_i = m_i \cdot \left(\frac{2\overline{y}_i s_i+2}{N}\right)$. To prove that Game-6 is indistinguishable from Game-5, we present the following Lemma.

Lemma 4.3. *The distribution of the Jacobi symbols* $\left(\frac{2y_i s^j+2}{N}\right)$ *is indistinguishable from the distribution the Jacobi symbols* $\left(\frac{2y_i s_i+2}{N}\right)$.

The proof of this Lemma 4.3 is based on the work of Damgard [Dam88]. He proved that the Jacobi sequences are indistinguishable from random. i.e. if an adversary knows the value of $\left(\frac{a}{N}\right)$, it is a hard problem to find $\left(\frac{a+1}{N}\right)$ for an unknown value a. Although the values of a and $a+1$ are highly correlated and dependent, that does not mean that their Jacobi symbols are correlated. We now present a formal proof for Lemma 4.3.

Proof. Damgard proved that the following is a hard problem [Dam88].

Theorem 4.3. *Let J be the Jacobi sequence modulo N with a starting point a and length P(k), for a security parameter k and polynomial P. Given J, find* $\left(\frac{a+P(k)+1}{N}\right)$.

This means that, knowing $\left(\frac{a}{N}\right), \left(\frac{a+1}{N}\right), \left(\frac{a+2}{N}\right), ..., \left(\frac{a+a_1}{N}\right), ..., \left(\frac{a+a_2}{N}\right), ..., \left(\frac{a+P}{N}\right)$, it is a hard problem to find $\left(\frac{a+P+1}{N}\right)$.

We first choose a and P such that $a + P + 1 = 2y_i s^j + 2$, then we can write the above sequence in two different forms.

$$\left(\frac{a}{N}\right), \left(\frac{a+1}{N}\right), \left(\frac{a+2}{N}\right), ..., \left(\frac{2y_{i_1} s^{j_1}+2}{N}\right), ..., \left(\frac{2y_{i_2} s^{j_2}+2}{N}\right), ..., \left(\frac{a+P}{N}\right)$$

where $a_1 = 2y_{i_1} s^{j_1} + 2 - a,\ a_2 = 2y_{i_2} s^{j_2} + 2 - a,$ and $j_1 < j_2 < j$.

$$\left(\frac{a}{N}\right), \left(\frac{a+1}{N}\right), \left(\frac{a+2}{N}\right), ..., \left(\frac{2y_{i_1} s_{j_1}+2}{N}\right), ..., \left(\frac{2y_{i_2} s_{j_2}+2}{N}\right), ..., \left(\frac{a+P}{N}\right)$$

where $a_1 = 2y_{i_1} s_{j_1} + 2 - a,\ a_2 = 2y_{i_2} s_{j_2} + 2 - a.$

Since $\mathbb{Z}_{\mathbb{N}}$ is an additive group, the values of a_1, a_2 and P exist in both sequences for any value y or s which means that both sequences represent the Damgard hard problem. Moreover, guessing the Jacobi symbol $\left(\frac{2y_i s^j+2}{N}\right)$ from the sequence $\left(\frac{2y_i s+2}{N}\right)$, $\left(\frac{2y_i s^2+2}{N}\right)$, ..., $\left(\frac{2y_i s^{j-1}+2}{N}\right)$ is as hard as guessing the same Jacobi symbol from the sequence $\left(\frac{2y_i s_1+2}{N}\right)$, $\left(\frac{2y_i s_2+2}{N}\right)$, ..., $\left(\frac{2y_i s_j+2}{N}\right)$. The same holds for $\left(\frac{2\overline{y}_i s^j+2}{N}\right)$ and $\left(\frac{2\overline{y}_i s_i+2}{N}\right)$. □

Based on Lemma 4.3, $\mathcal{A}$ will not be able to distinguish between Game-5 and Game-6. i.e.

$$|\Pr[W_6] = \Pr[W_5]|.$$

- Game-$\overline{6}$. In this game, we hash the identity ID to a different value $H(ID, i) = u^a R_i = r_i^2$ for each bit such as the original BGH systems. In other words, we replace the Jacobi symbols $\left(\frac{x_i r+1}{N}\right)$ and $\left(\frac{\overline{x}_i r+1}{N}\right)$ with $\left(\frac{x_i r_i+1}{N}\right)$ and $\left(\frac{\overline{x}_i r_i+1}{N}\right)$. i.e. $c_i = m_i \cdot \left(\frac{x_i r_i+1}{N}\right)$ and $\overline{c}_i = m_i \cdot \left(\frac{\overline{x}_i r_i+1}{N}\right)$.

  To prove that Game-$\overline{6}$ is equivalent to Game-$\overline{5}$, we recall Theorem 4.1 which stats that hashing the identity to encrypt each bit does not have a positive impact on the security of the IBE. Thus,

$$|\Pr[\overline{W}_6] = \Pr[\overline{W}_5]|.$$

- Game-7. In this game, we replace the message $m_{(b)}$ by a random string $z \in_R \{-1, 1\}^l$ i.e., $c_i = z_i \cdot \left(\frac{2y_i s_i+2}{N}\right)$ and $\overline{c}_i = z_i \cdot \left(\frac{2\overline{y}_i s_i+2}{N}\right)$. We first prove that $(2y_i s_i + 2)(-2y_i s_i + 2)R \in QR(N)$.

  Proof. Let $g(y_i, s_i) = (2y_i s_i + 2)$, then we have,

$$\begin{aligned} g(y_i, s_i)g(y_i, -s_i)R &= 4(y_i s_i + 1)(-y_i s_i + 1)R, \\ g(y_i, s_i)g(y_i, -s_i)R &= 4(1 - (y_i s_i)^2)R, \\ g(y_i, s_i)g(y_i, -s_i)R &= 4(Rx_i^2)R = (2Rx_i)^2 \in QR(N). \end{aligned}$$

  Similarly, we can prove that $(2\overline{y}_i s_i + 2)(-2\overline{y}_i s_i + 2)uR \in QR(N)$.
  Since $S_i \in QR(N)$, $uR, R \in J(N) \setminus QR(N)$, $(2y_i s_i + 2)(-2y_i s_i + 2)R \in QR(N)$ and $(2\overline{y}_i s_i + 2)(-2\overline{y}_i s_i + 2)uR \in QR(N)$ then Case 1 in Lemma 4.2 can be applied and the distribution of the Jacobi symbols $\left(\frac{2y_i s_i+2}{N}\right)$ and $\left(\frac{2\overline{y}_i s_i+2}{N}\right)$ are random in $\{\pm 1\}$. Thus, $\mathcal{A}$ will not be able to distinguish between Game-6 and Game-7. i.e.

$$|\Pr[W_7] = \Pr[W_6]|.$$

- Game-$\overline{7}$. In this game, we replace the message $m_{(b)}$ by a random string $z \in_R \{-1, 1\}^l$ i.e., $c_i = z_i \cdot \left(\frac{x_i r_i+1}{N}\right)$ and $\overline{c}_i = z_i \cdot \left(\frac{\overline{x}_i r_i+1}{N}\right)$. We first prove that $(x_i r_i + 1)(-x_i r_i + 1)S^j \in QR(N)$.

Proof. Let $f(x_i, r_i) = (x_i r_i + 1)$, then we have

$$f(x_i, r_i)f(x_i, -r_i)S^j = (x_i r_i + 1)(-x_i r_i + 1)S^j,$$
$$f(x_i, r_i)f(x_i, -r_i)S^j = (1 - (x_i r_i)^2)S^j = (1 - x_i^2 R_i)S^j,$$
$$f(x_i, r_i)f(x_i, -r_i)S^j = (S^j y_i^2)S^j = (S^j y_i)^2 \in QR(N).$$

Similarly, we can prove that $(\overline{x}_i r_i + 1)(-\overline{x}_i r_i + 1)S^j \in QR(N)$.
Since $uR_i, R_i \in QR(N)$, $S^j \in J(N) \setminus QR(N)$, $(x_i r_i + 1)(-x_i r_i + 1)S^j \in QR(N)$ and $(\overline{x}_i r_i + 1)(-\overline{x}_i r_i + 1)S^j \in QR(N)$ then Case 2 in Lemma 4.2 can be applied and the distribution of the Jacobi symbols $\left(\frac{x_i r_i + 1}{N}\right)$ and $\left(\frac{\overline{x}_i r_i + 1}{N}\right)$ are random in $\{\pm 1\}$. Thus, $\mathcal{A}$ will not be able to distinguish between Game-$\overline{7}$ and Game-$\overline{6}$. i.e.

$$|\Pr[\overline{W}_7] = \Pr[\overline{W}_6]|.$$

- Clearly in Game-7 and Game-$\overline{7}$ we have,

$$|\Pr[W_7] = \Pr[\overline{W}_7] = \frac{1}{2}|.$$

Combining all the previous equations proves Theorem 4.2.

4.4 V-AnonIBE

V-AnonIBE follows the same concept of V-BasicIBE. The *Setup* and *Extract* algorithms are identical to the ones in V-BasicIBE. To encrypt a message $m \in \{-1, 1\}^l$, V-AnonIBE calculates $[x_i, y_i, \alpha_i, \beta_i]$, $i \in [0, l-1]$ that satisfy the following equations.

$$[x_i, y_i] \leftarrow Rx_i^2 + S^j y_i^2 \equiv 1 \pmod{N} \text{ and } [\alpha_i, \beta_i] \leftarrow u\alpha_i^2 + S^j \beta_i^2 \equiv 1 \pmod{N},$$

for an odd number j. V-AnonIBE solves the equations $Rx_i^2 + S^j y_i^2 \equiv 1 \pmod{N}$ exactly as V-BasicIBE. The variables α_i, β_i are calculated using Lemma 4.1 as follows.

$$\hat{\alpha} = \frac{2\alpha_0}{u\alpha_0^2 + 1} \text{ and } \hat{\beta} = \frac{\beta_0^2}{u\alpha_0^2 + 1},$$
$$\alpha_i = \frac{\alpha_{i-1} + \hat{\alpha}}{u\alpha_{i-1}\hat{\alpha} + 1} \text{ and } \beta_i = \frac{\beta_{i-1}\hat{\beta}}{u\alpha_{i-1}\hat{\alpha} + 1},$$

where $[\alpha_0, \beta_0]$ are a valid solution to $u\alpha_0^2 + S\beta_0^2 \equiv 1 \pmod{N}$ and $[\hat{\alpha}, \hat{\beta}]$ are a valid solution to $u\hat{\alpha}^2 + S^2\hat{\beta}^2 \equiv 1 \pmod{N}$.

The message $m \leftarrow [m_0, m_1, ..., m_{l-1}]$ is encrypted using the following equation.

$$c_i \leftarrow m_i \cdot \left(\frac{2y_i s^j + 2}{N}\right).$$

The main difference between V-AnonIBE and AnonIBE is that S^j is not constant and $k_i \leftarrow \left(\frac{1+\beta_i s^j}{N}\right)$ must be calculated and sent along with the ciphertext. That is why V-AnonIBE is longer than AnonIBE by $l-1$. The ciphertext is (S, k, c) where $c \leftarrow [c_0, ..., c_{l-1}]$, $k \leftarrow [k_0, ..., k_{l-1}]$.

For decryption, the message can be retrieved as follows.

$$m_i \leftarrow c_i \cdot \left(\frac{x_i r + 1}{N}\right) \quad \text{if } r^2 = R.$$

$$m_i \leftarrow c_i \cdot \left(\frac{1 + S^j y_i \beta_i + \alpha_i x_i r}{N}\right) \cdot k_i \quad \text{if } r^2 = uR.$$

For $i \in [0, l-1]$ and j is odd.

Correctness: If $r^2 = R$, the correctness of AnonIBE is exactly the same as that of BasicIBE. If $r^2 = uR$,

$$\begin{aligned}(1 + S^j y_i \beta_i + \alpha_i x_i r)(2y_i s^j + 2)(1 + \beta_i s^j) = \\ &= 2(1 + S^j y_i \beta_i + \alpha_i x_i r)(1 + S^j y_i \beta_i + y_i s^j + \beta_i s^j) \\ &= 2(1 + \frac{\alpha_i x_i r}{1 + S^j y_i \beta_i})(1 + \frac{s^j(\beta_i + y_i)}{1 + S^j y_i \beta_i})(1 + S^j y_i \beta_i)^2 \\ &= 2(1 + \overline{x}_i r)(1 + \overline{y} s^j)(1 + S^j y_i \beta_i)^2\end{aligned}$$

where $\overline{x}_i = \dfrac{\alpha_i x_i r}{1 + S^j y_i \beta_i}$ and $\overline{y} = \dfrac{\beta_i + y_i}{1 + S^j y_i \beta_i}$.

From Lemma 2.1, $[\overline{x}_i, \overline{y}_i]$ is a valid solution to $uR\overline{x}_i^2 + S^j \overline{y}_i^2 \equiv 1 \pmod N$.

$(1 + \overline{x}_i r)(2 + 2\overline{y} s^j) \in QR(N)$,

$$\left(\frac{(1 + S^j y_i \beta_i + \alpha_i x_i r)(2y_i s^j + 2)(1 + \beta_i s^j)}{N}\right) = 1,$$

$$\left(\frac{2y_i s^j + 2}{N}\right) = \left(\frac{1 + S^j y_i \beta_i + \alpha_i x_i r}{N}\right) \cdot k_i.$$

4.4.1 V-AnonIBE Security

Theorem 4.4. *Suppose the interactive quadratic residuosity assumption holds for RSAgen and F is a secure PRF. Then the proposed V-AnonIBE is Anon-IND-ID-CPA secure in the standard model based on the IQR assumption. In particular, suppose $\mathcal{A}$ is an efficient Anon-IND-ID-CPA adversary, then there exist efficient algorithms B_1, B_2 whose running time is the same as that of $\mathcal{A}$ such that,*

$$IBEAdv_{\mathcal{A}, V-AnonIBE}(\lambda) \leq IQRAdv_{B_2, RSAgen}(\lambda) + PRFAdv_{B_1, F}(\lambda).$$

- **Proof**. Similar to V-BasicIBE security proof, we define two sequences of games and let W_i represents the winning of the i_{th} game and $\overline{W}_i$ represents the winning of the $\bar{i}_{th}$ game by the adversary $\mathcal{A}$. Any of these sequences proves the security of V-AnonIBE.

  These games are defined as follows.

  - **Game-0**. This game is the usual adversarial game.
  - **Game-1**. This game replaces the PRF F with a truly random function.
  - **Game-2**. This game explains how to simulate private key queries using a square root oracle $\mathcal{O}$.
  - **Game-3**. This game explains how to respond to a challenge query from $\mathcal{A}$.
  - **Game-$\overline{3}$**. This game explains how to respond to a challenge query using the *Decrypt* algorithm.
  - **Game-4**. This game sets $R \in J(N) \setminus QR(N)$.
  - **Game-$\overline{4}$**. This game sets $S^j \in J(N) \setminus QR(N)$.
  - **Game-5**. This game sets $S_i = s_i^2$ for each bit.
  - **Game-$\overline{5}$**. This game sets $R_i = H(ID, i)$ for each bit.
  - **Game-6** and **Game-$\overline{6}$** replace the message m with a random number z.

- Game-0. This is the usual adversarial game for defining Anon-IND-ID-CPA security of IBE protocols. The challenger picks the random oracle $H : ID \rightarrow J(N)$ at random from the set of all such functions in the *Setup* algorithm and allows $\mathcal{A}$ to query H at arbitrary points. Thus, we have,

$$|\Pr[W_0] - \frac{1}{2}| = IBEAdv_{\mathcal{A},V-AnonIBE}(\lambda).$$

- Game-1. This is the same as Game-0, with the following change. In the *Setup* algorithm, instead of using a PRF F to respond to $\mathcal{A}$'s private key queries, we use a truly random function $f : ID \rightarrow \{0, 1, 2, 3\}$. If F is a secure PRF, $\mathcal{A}$ will not notice the difference between Game-0 and Game-1. In particular, there exists an algorithm B_1 (whose running time is about the same as that of $\mathcal{A}$) such that,

$$|\Pr[W_1] - \Pr[W_0]| = PRFAdv_{B_1,F}(\lambda).$$

- Game-2. In this game, we modify the challenger so that it does not need the factorisation of N. We will work in the setting of the IQR assumption, so we assume a randomly chosen square root oracle $\mathcal{O}$ with its associated quadratic non-residue u as in [BGH07]. As before, the challenger chooses $p, q \leftarrow RSAgen(\lambda)$ and

$N = pq$, but now it does not need the factorisation during the game. (N, u, H) are the public parameters $params$ given to $\mathcal{A}$ in the previous game where u is uniform in $J(N) \setminus QR(N)$. The challenger responds to private key queries using the oracle $\mathcal{O}$. Given a private key query for ID the challenger must return $r \in \mathbb{Z}_{\mathbb{N}}$ where $r^2 = u^a H(ID)$ for some $a \in \{0, 1\}$. This is precisely what the oracle does, enabling the challenger to respond to private key queries. Because the square root oracle is chosen at random (replacing the random function f), the distributions of query responses are identical to those in Game-1. Therefore,

$$|\Pr[W_2] = \Pr[W_1]|.$$

- Game-3. We explain, in this game, how the challenger answers a challenge query from $\mathcal{A}$ for an identity ID and a message m.
  - He constructs the private key r and $u^a R \in QR(N)$ for ID using the oracle $\mathcal{O}$. (*)
  - He chooses $s \in_R \mathbb{Z}_{\mathbb{N}}$ and computes $S^j = s^{2j}$ for an odd value j.
  - He chooses $k_i \in_R \{\pm 1\}$.
  - Upon receiving two messages m_0, m_1 and two identities ID_0, ID_1 from the adversary, the challenger tosses two fair coins $(b, \bar{b}) \in \{0, 1\}^2$ and sets $(c, k) \leftarrow Encrypt(params, ID_{\bar{b}}, m_b)$.
  - He sends (S, k, c) to $\mathcal{A}$.

  We prove that this game has the same distribution for (S, k, c) as the real $Encrypt$ of Game-2.

  We first prove that $\left(\frac{1+\beta_i s^j}{N}\right)\left(\frac{1-\beta_i s^j}{N}\right) u \in QR(N)$.

  Proof. Let $g(\beta_i, s^j) = (1 + \beta_i s^j)$, then we have,

$$\begin{aligned} g(\beta_i, s^j) g(\beta_i, -s^j) u &= (\beta_i s^j + 1)(1 - \beta_i s^j) u, \\ g(\beta_i, s^j) g(\beta_i, -s^j) u &= (1 - (\beta_i s^j)^2) u, \\ g(\beta_i, s^j) g(\beta_i, -s^j) u &= (u\alpha_i^2) u = (u\alpha_i)^2 \in QR(N). \end{aligned}$$

  Since $S^j \in QR(N)$ and $u \in J(N) \setminus QR(N)$ then Case 1 in Lemma 4.2 can be applied and the distribution of the Jacobi symbols $k_i = \left(\frac{1+\beta_i s^j}{N}\right)$ are random in $\{\pm 1\}$. Thus,

$$|\Pr[W_3] = \Pr[W_2]|.$$

- Game-$\overline{3}$. This game is the same in Game-2 except that a challenge query is processed differently. To encrypt a message m to a particular ID, the challenger does the following.

  – He constructs the private key r and $u^a R \in QR(N)$ for ID using the oracle $\mathcal{O}$.

  – He chooses $s \in_R \mathbb{Z}_{\mathbb{N}}$ and computes $S^j = s^{2j}$ for an odd value j. (*)

  – He chooses $k_i \in_R \{\pm 1\}$.

  – Upon receiving two messages m_0, m_1 and two identities ID_0, ID_1 from the adversary, the challenger tosses two fair coins $b, \overline{b} \in \{0,1\}^2$ and sets $(c,k) = Decrypt(r, params, (S, k, ID_{\overline{b}}, m_b))$.

  – He sends (S, k, c) to $\mathcal{A}$.

  We prove in Game-3 that k_i has a random distribution in $\{\pm 1\}$. In addition, It is easy to see that (S, k, c) is the unique encryption of m. Therefore, (S, k, c) of Game-$\overline{3}$ is the same as in Game-2. Thus,

$$|\Pr[\overline{W}_3] = \Pr[W_2]|.$$

- Game-4. In this game, we make a change in the challenge phase. We replace the line (*) in Game-3 with the following.

  – He constructs $u^a R \in J(N) \setminus QR(N)$ for ID using the oracle $\mathcal{O}$.

  Since the only difference between Game-4 and Game-3 is that $u^a R \in J(N) \setminus QR(N)$ in Game-4 instead of $u^a R \in QR(N)$ in Game-3, $\mathcal{A}$ will not notice the difference assuming that the IQR assumption holds for RSAgen. In particular, there exists an algorithm B_2 (whose running time is about the same as that of $\mathcal{A}$) such that,

$$|\Pr[W_4] - \Pr[W_3]| = IQRAdv_{B_2, RSAgen}(\lambda).$$

- Game-$\overline{4}$. We replace the line (*) in Game-$\overline{3}$ with the following.

  – He chooses $S^j \in J(N) \setminus QR(N)$.

  Since the only difference between Game-$\overline{4}$ and Game-$\overline{3}$ is that $S^j \in J(N) \setminus QR(N)$ in Game-$\overline{4}$ instead of $S^j \in QR(N)$ in Game-$\overline{3}$, $\mathcal{A}$ will not notice the difference assuming that the IQR assumption holds for RSAgen. In particular, there exists an algorithm B_2 (whose running time is about the same as that of $\mathcal{A}$) such that,

$$|\Pr[\overline{W}_4] - \Pr[\overline{W}_3]| = IQRAdv_{B_2, RSAgen}(\lambda).$$

- Game-5. In this game, we replace S^j with randomly independent values $S_i = s_i^2$, $s_i \in_R \mathbb{Z}_{\mathbb{N}}$ for each bit. i.e. $c_i = m_i \cdot \left(\frac{2y_i s_i + 2}{N}\right)$. As we proved in Game-6 in V-BasicIBE, the sequence $\left(\frac{2y_i s^j + 2}{N}\right)$ represents the Damgard hard problem and the adversary $\mathcal{A}$ cannot distinguish between Game-5 and Game-4. Thus.

$$|\Pr[W_5] = \Pr[W_4]|.$$

- Game-$\overline{5}$. In this game, we hash the identity ID to a different value $H(ID, i) = u^a R_i = r_i^2$ for each bit such as the original BGH systems. i.e. $c_i = m_i \cdot \left(\frac{x_i r_i + 1}{N}\right)$ if $r_i^2 = R_i$ and $\overline{c}_i = m_i \cdot \left(\frac{1 + S^j y_i \beta_i + \alpha_i x_i r_i}{N}\right) \cdot k_i$ if $r_i^2 = uR_i$. Similar to Game-$\overline{6}$ in V-BasicIBE, we recall Theorem 4.1 to prove that Game-$\overline{5}$ is indistinguishable from Game-$\overline{4}$. Thus,

$$|\Pr[\overline{W}_5] = \Pr[\overline{W}_4]|.$$

- Game-6. In this game, we replace the message $m_{(b)}$ by a random string $z \in_R \{-1, 1\}^l$ i.e., $c_i = z_i \cdot \left(\frac{2y_i s_i + 2}{N}\right)$. Since $S_i \in QR(N)$, $R \in J(N) \setminus QR(N)$ and $(2y_i s_i + 2)(-2y_i s_i + 2)R \in QR(N)$ then Case 1 in Lemma 4.2 can be applied and the distribution of the Jacobi symbols $\left(\frac{2y_i s_i + 2}{N}\right)$ are random in $\{\pm 1\}$. Thus, $\mathcal{A}$ will not be able to distinguish between Game-6 and Game-5. i.e.

$$|\Pr[W_6] = \Pr[W_5]|.$$

- Game-$\overline{6}$. In this game, we replace the message $m_{(b)}$ by a random string $z \in_R \{-1, 1\}^l$ i.e., $c_i = z_i \cdot \left(\frac{x_i r_i + 1}{N}\right)$ if $r_i^2 = R_i$ and $\overline{c}_i = z_i \cdot \left(\frac{1 + S^j y_i \beta_i + \alpha_i x_i r_i}{N}\right) \cdot k_i$ if $r_i^2 = uR_i$. In Game-$\overline{7}$ of BasicIBE we prove that $(x_i r_i + 1)(-x_i r_i + 1)S^j \in QR(N)$. We now prove that $(1 + S^j y_i \beta_i + \alpha_i x_i r_i)(1 + S^j y_i \beta_i - \alpha_i x_i r_i)S^j \in QR(N)$.

  Proof. Let $f(x_i, r_i) = (1 + S^j y_i \beta_i + \alpha_i x_i r_i)$, then we have,

$$\begin{aligned} f(x_i, r_i) f(x_i, -r_i) S^j &= (1 + S^j y_i \beta_i + \alpha_i x_i r_i)(1 + S^j y_i \beta_i - \alpha_i x_i r_i) S^j \\ &= (1 + \frac{\alpha_i x_i r_i}{1 + S^j y_i \beta_i})(1 - \frac{\alpha_i x_i r_i}{1 + S^j y_i \beta_i})(1 + S^j y_i \beta_i)^2 S^j \\ &= (\overline{x} r_i + 1)(-\overline{x} r_i + 1)(1 + S^j y_i \beta_i)^2 S^j \in QR(N), \end{aligned}$$

  where $\overline{x}_i = \dfrac{\alpha_i x_i r_i}{1 + S^j y_i \beta_i}$.

  Similar to BasicIBE, it is easy to prove that $(\overline{x} r_i + 1)(-\overline{x} r_i + 1)S^j \in QR(N)$. □

  Since $u^a R_i \in QR(N)$, $S^j \in J(N) \setminus QR(N)$ and $f(x_i, r_i) f(x_i, -r_i) S^j \in QR(N)$ where $f(x_i, r_i) = (x_i r_i + 1)$ if $R_i = r_i^2$ and $f(x_i, r_i) = (1 + S^j y_i \beta_i + \alpha_i x_i r_i)$ if

$uR_i = r_i^2$ then Case 2 in Lemma 4.2 can be applied and the distribution of the Jacobi symbols $\left(\frac{x_i r_i + 1}{N}\right)$ and $\left(\frac{1+S^j y_i \beta_i + \alpha_i x_i r_i}{N}\right) \cdot k_i$ are random in $\{\pm 1\}$. Thus, $\mathcal{A}$ will not be able to distinguish between Game-$\overline{6}$ and Game-$\overline{5}$. i.e.

$$|\Pr[\overline{W}_6] = \Pr[\overline{W}_5]|.$$

- End. Clearly in Game-6 and Game-$\overline{6}$ we have,

$$|\Pr[\overline{W}_6] = \Pr[W_6] = \frac{1}{2}|.$$

Combining all the previous equations proves Theorem 4.4.

4.5 Space-Time Tradeoff

In this section, we present a trade-off between the time and the ciphertext length of the proposed IBE systems. For V-BasicIBE, instead of sending S along with c and $\overline{c}$ as the full ciphertext C, the sender obtains a random solution to the equation $Rx^2 + Sy^2 \equiv 1 \pmod N$ using only one inversion in $\mathbb{Z}_{\mathbb{N}}$ [JB08] and sends $C = (x_0, \overline{x}_0, c, \overline{c})$. This results in high encryption speed. In the decryption, the receiver does not have to solve any equations and he can generate x_i or $\overline{x}_i$ (based on if $r^2 = R$ or uR) using Lemma 4.1. This, of course, comes at the cost of sending one more element in $\mathbb{Z}_{\mathbb{N}}$. This time-space trade-off applies for V-AnonIBE where the ciphertext is $C = (S, x_0, y_0, \alpha_0, \beta_0, c, \overline{c})$.

4.6 Conclusion

This chapter proposed two variants of BGH systems. The proposed variants are more efficient (in terms of computation time) than the original IBE systems. We also proved that these IBE systems have the same security level as BGH systems. In addition, the proposed IBE systems have only one element in the $\mathbb{Z}_{\mathbb{N}}$ private key instead of l elements in $\mathbb{Z}_{\mathbb{N}}$ as in BGH systems. We also produced time-space trade-off variants that are both fast and efficient.

Chapter 5

Jhanwar-Barua's Identity-based Encryption Revisited

In FOCS'07, Boneh, Gentry and Hamburg presented an identity-based encryption (IBE) (BasicIBE) based on the quadratic residuosity (QR) assumption. A BasicIBE encryption of an l-bit message has a short ciphertext of $\log_2 N + 2l$ bits where N is an RSA modulus. However, it is not time-efficient due to solving $l + 1$ equations in the form $Rx^2 + Sy^2 \equiv 1 \pmod{N}$. Jhanwar and Barua presented a variant of BasicIBE in which the sender only solves $2\sqrt{l}$ such equations. The receiver decrypts the message without solving any such equations. In addition, the decryption key is decreased to only one element in $\mathbb{Z}_{\mathbb{N}}$. However, the ciphertext size increases from a single element to $2\sqrt{l}$ elements in $\mathbb{Z}_{\mathbb{N}}$. In this chapter, we revisit the Jhanwar-Barua (JB) IBE and review its security. We prove that this IBE is not IND-ID-CPA secure and present a solution to the security flaw of this IBE. We also point out a flaw in the security proof of JB IBE and propose a security proof for the fixed IBE. We prove that it has the same security as the original BasicIBE.

5.1 Introduction

Most IBE systems presented in the literature are based on pairing operations. According to MIRACL benchmarks, a 512-bit Tate pairing takes 20 ms while a 1024-bit prime modular exponentiation takes 8.80 ms. The pairing computations are expensive compared to normal operations. This limits IBE from being used in real life, specially when time and power consumptions are a major concern such as in limited wireless sensor networks. Hence, seeking for an IBE that does not rely on pairings is desirable.

Another approach to design IBE systems is based on the quadratic residuosity (QR) assumption. The first IBE based on this approach is due to Cocks [Coc01]. It is time-efficient compared to pairing-based IBE systems, but it produces a long ciphertext of two elements in $\mathbb{Z}_{\mathbb{N}}$ for every bit in the message. Boneh, Gentry and Hamburg [BGH07] presented two space-efficient IBE systems (BasicIBE and AnonIBE) in which the ciphertext is reduced from $2l$ elements to only one element in $\mathbb{Z}_{\mathbb{N}}$. As in Cocks' IBE, the security of BasicIBE is based on the QR assumption in the random oracle model. Although the concrete instantiation of BasicIBE is highly space-efficient, this comes at the cost of less time-efficient encryption/decryption

Table 5.1: Comparison Between Various IBE Systems and JB IBE

	Expensive Mathematical Operations	Ciphertext Length
Cock's	0	$2l(\log N)$
BasicIBE	$(l+1)p$	$\log N + 2l$
AnonIBE	$(2l+1)p$	$\log N + l + 1$
Jhanwar-Barua	0	$2\sqrt{l}\log N + 2l$
Boneh-Boyen	e+3m	G_T+2G
BRS	m+(x)e	G+(x)G_T

algorithms. To encrypt an l-bit message, BasicIBE solves $l+1$ equations in the form $Rx^2 + Sy^2 \equiv 1 \pmod N$ for known values of R, S and N [BGH07]. Solving such an equation requires a 'solubility certificate' and obtaining these certificates requires the generation of primes [CR03, Kel08]. The prime generation is a time-consuming process and it is the bottleneck in the BGH systems. Moreover, the decryption key is l elements in $\mathbb{Z}_{\mathbb{N}}$ because the identity ID is hashed to a different value to encrypt each bit.

Jhanwar and Barua [JB08] made some significant observations on the BGH systems (for solving equations in the form $Rx^2 + Sy^2 \equiv 1 \pmod N$) and proposed a trade-off IBE that reduces the private key length but increases the ciphertext length. They found that by knowing the value of $S \pmod N$, one can find a random solution to the equation $Rx^2 + Sy^2 \equiv 1 \pmod N$ using only one inversion in $\mathbb{Z}_{\mathbb{N}}$. The sender solves only $2\sqrt{l}$ equations in the form $Rx^2 + Sy^2 \equiv 1 \pmod N$ using only $2\sqrt{l}$ inversions in $\mathbb{Z}_{\mathbb{N}}$ and thus, no prime generation is required. This increases the encryption/decryption speed dramatically. The private key is only one element in $\mathbb{Z}_{\mathbb{N}}$. However, this IBE produces a large ciphertext of $2\sqrt{l}$ elements in $\mathbb{Z}_{\mathbb{N}}$.

The most interesting part of Jhanwar and Barua IBE [JB08] is its time- and power-efficiency. It avoids the expensive prime generation and replaces it with only one inversion in $\mathbb{Z}_{\mathbb{N}}$. Moreover, there is no expensive computational operations such as pairing or even modular exponentiation. We compare between JB IBE and some other efficient IBE systems such as Boneh-Boyen IBE [BB04a] and IBE systems with more powerful adversary such as Boneh, Raghunathan, Segev (BRS) IBE [BRS13]. We also compare it to other pairing-free IBE such as Cock's IBE [Coc01] and BGH systems [BGH07]. In Table 5.1, the symbol m represents prime modular exponentiation while e and p represents pairing operation and prime generation respectively. l represents the message length. The symbol x in the table represents a parameter in BRS IBE which is function of the security parameter, the length of the identity and a prime p [BRS13]. The symbols G and G_T represents an element in two groups G and G_T such that $e : G \times G \to G_T$.

Our Contributions. We revisit JB IBE and identify some security issues with it.

We prove that an IND-ID-CPA adversary can attack this IBE and hence it is not IND-ID-CPA secure. The attack comes from mistakenly reusing the same key to encrypt multiple bits and hence, these bits are encrypted using the same key. We also present a solution to the security flaw of this IBE. We also point to a flaw of the security proof of JB IBE and present a security proof for the fixed IBE. We prove that it is as secure as BasicIBE.

5.2 The IBE Structure

JB IBE is explained as follows.

- $(params) \leftarrow Setup(\lambda)$. Using RSAgen($\lambda$), generate (p, q). Calculate the modulus $N \leftarrow pq$. Choose a random $u \in J(N) \setminus QR(N)$ and choose a hash function $H : ID \rightarrow J(N)$. The public parameters $params$ are $[N, u, H]$. The master secret MS parameters are p, q and a secret key K for a pseudorandom function (PRF) $F_K : ID \rightarrow \{0, 1, 2, 3\}$.

- $(r) \leftarrow Extract(MS, ID, l)$. Calculate $R \leftarrow H(ID) \in J(N)$ and $w \leftarrow F_K(ID) \in \{0, 1, 2, 3\}$. Choose $a \in \{0, 1\}$ such that $u^a R \in QR(N)$. Let $[z_0, z_1, z_2, z_3]$ be the four square roots of $u^a R \in \mathbb{Z}_{\mathbb{N}}$, then $r \leftarrow z_w$.

- $(C) \leftarrow Encrypt(params, ID, m)$. To encrypt a message $m \in \{-1, 1\}^l$, JB IBE calculates $[x_i, y_i, \overline{x}_i, \overline{y}_i]$, $i \in [0, l-1]$ that satisfy the following equations.

  $$[x_i, y_i] \leftarrow Rx_i^2 + S_i y_i^2 \equiv 1 \pmod N \text{ and } [\overline{x}_i, \overline{y}_i] \leftarrow uR\overline{x}_i^2 + S_i \overline{y}_i^2 \equiv 1 \pmod N,$$

  for the first $k = \sqrt{l}$ bits. After that, it calculates $y_i, i > k-1$ from $y_{j_1}, y_{j_2}, x_{j_1}, x_{j_2}$ such that $(j_1, j_2) \leftarrow i = k \cdot j_1 + j_2$ using Lemma 4.1. After that, the message is encrypted exactly as BasicIBE. The full structure of JB IBE encryption algorithm is shown in Figure 5.1. The ciphertext is $C \leftarrow (c, \overline{c}, x, \overline{x})$.

$k \leftarrow \sqrt{l}$, $R \leftarrow H(ID) \in J(N)$
foreach $i \in [0, l-1]$ **do**
  if $i \leq k-1$ **then**
    $s_i \in_R \mathbb{Z}_{\mathbb{N}}$, $s_i^2 \equiv S_i \pmod N$, $[x_i, y_i] \leftarrow Rx_i^2 + S_i y_i^2 \equiv 1 \pmod N$
    $[\overline{x}_i, \overline{y}_i] \leftarrow uR\overline{x}_i^2 + S_i\overline{y}_i^2 \equiv 1 \pmod N$
    $c_i \leftarrow m_i \cdot \left(\frac{2y_i s_i + 2}{N}\right)$, $\overline{c}_i \leftarrow m_i \cdot \left(\frac{2\overline{y}_i s_i + 2}{N}\right)$
  else
    $(j_1, j_2) \leftarrow i = k \cdot j_1 + j_2$, $y_{j_1,j_2} \leftarrow \frac{y_{j_1} y_{j_2}}{Rx_{j_1} x_{j_2}+1}$, $\overline{y}_{j_1,j_2} \leftarrow \frac{\overline{y}_{j_1}\overline{y}_{j_2}}{uR\overline{x}_{j_1}\overline{x}_{j_2}+1}$
    $c_i \leftarrow m_i \cdot \left(\frac{2y_{j_1,j_2} s_{j_1} s_{j_2} + 2}{N}\right)$, $\overline{c}_i \leftarrow m_i \cdot \left(\frac{2\overline{y}_{j_1,j_2} s_{j_1} s_{j_2} + 2}{N}\right)$
  end
  $c \leftarrow [c_0, ..., c_{l-1}], \overline{c} \leftarrow [\overline{c}_0, ..., \overline{c}_{l-1}], x \leftarrow [x_1, ..., x_k]$ and $\overline{x} \leftarrow [\overline{x}_1, ..., \overline{x}_k]$
end

Figure 5.1: The Structure of JB IBE Encryption Algorithm

- $(m) \leftarrow Decrypt(C, r)$. The receiver decrypts the message based on if $R \in QR(N)$ or not. If $R \in QR(N)$, the receiver discards $\overline{c}, \overline{x}$ and decrypts the message $m_i \leftarrow c_i \cdot \left(\frac{x_i r + 1}{N}\right)$. Otherwise the receiver discards c, x and decrypts the message $m_i \leftarrow \overline{c}_i \cdot \left(\frac{\overline{x}_i r + 1}{N}\right)$. The full structure of JB IBE decryption algorithm is shown in Figure 5.2.

foreach $i \in [0, l-1]$ **do**
  if $r^2 = R$ **then**
    if $i > k-1$ **then**
      $(j_1, j_2) \leftarrow i = k \cdot j_1 + j_2$, $x_i \leftarrow \frac{x_{j_1} + x_{j_2}}{Rx_{j_1} x_{j_2}+1}$
    end
    $m_i \leftarrow c_i \cdot \left(\frac{x_i r + 1}{N}\right)$
  end
  if $r_i^2 = uR$ **then**
    if $i > k-1$ **then**
      $(j_1, j_2) \leftarrow i = k \cdot j_1 + j_2$, $\overline{x}_i \leftarrow \frac{\overline{x}_{j_1} + \overline{x}_{j_2}}{uR\overline{x}_{j_1}\overline{x}_{j_2+1}}$
    end
    $m_i \leftarrow \overline{c}_i \cdot \left(\frac{\overline{x}_i r + 1}{N}\right)$
  end
end

Figure 5.2: The Structure of JB IBE Decryption Algorithm

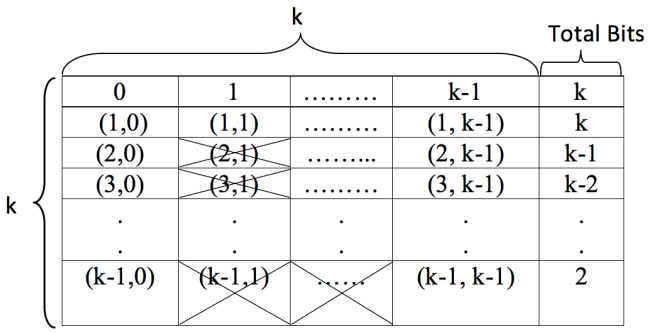

Figure 5.3: The Maximum Number of bits Encrypted by k Elements of y_{j_1,j_2}

5.3 The Security Flaw of JB IBE

The idea behind JB IBE is based on a time-space trade-off of BasicIBE [BGH07]. To decrease the number of $y, \overline{y}$ elements, JB IBE solves only two sets of $k = \sqrt{l}$ equations. Each set is used to generate c and $\overline{c}$ respectively. A bit $m_{i \leq k-1}$ is encrypted with $y_i, \overline{y}_i$ while a bit $m_{i>k-1}$ is encrypted with $(y_{j_1,j_2}) \leftarrow f(y_{j_1}, y_{j_2})$ where $i = k \cdot j_1 + j_2$. Assume that there are two bits m_{i_1}, m_{i_2} where $i_1 = k \cdot j_1 + j_2$ and $i_2 = k \cdot j_2 + j_1$, then $x_{j_1,j_2} = x_{j_2,j_1} = \frac{x_{j_1}+x_{j_2}}{Rx_{j_1}x_{j_2}+1}$ and $y_{j_1,j_2} = y_{j_2,j_1} = \frac{y_{j_1}y_{j_2}}{Rx_{j_1}x_{j_2}+1}$. Consequently, bits m_{i_1}, m_{i_2} are encrypted/decrypted using the same key. The same idea goes for $\overline{x}_{j_1,j_2}, \overline{y}_{j_1,j_2}$. Based on this security flaw, an IND-ID-CPA adversary can win an IND-ID-CPA game against this IBE as follows.

- An adversary $\mathcal{A}$ chooses $i_1, i_2 > k-1$ such that $i_1 = k \cdot j_1 + j_2$ and $i_2 = k \cdot j_2 + j_1$.
- In the challenge phase, $\mathcal{A}$ sends to the challenger $\mathcal{C}$ two messages $m, \overline{m}$. These messages are chosen at random with $m_{i_1} = m_{i_2}$ and $\overline{m}_{i_1} \neq \overline{m}_{i_2}$.
- In the guess phase, the adversary $\mathcal{A}$ checks the bits c_{i_1}, c_{i_2}. If $c_{i_1} = c_{i_2}$ then $b = 0$ and if $c_{i_1} \neq c_{i_2}$ then $b = 1$.

To overcome this security flaw, j_1 must not be equal to j_2 for all values of j_1 and j_2. i.e., $j_1 \neq j_2$ for all $[j_1, j_2] \in [0, k-1]$. This means that the number of k equations (i.e. the number of y elements) required to encrypt a message with length l is more than $\sqrt{l}$. Next, we deduce the relation between k and l in order to make JB IBE secure. Figure 5.3 represents a message m as a table. Each row is encrypted using k elements of y_i. The first row is encrypted by the first k elements of y_i. The second row is encrypted by the combination of y_1 and all values of $y_0, ..., y_{k-1}$. The third row is encrypted by the combination of y_2 and all values of $y_0, ..., y_{k-1}$ and so on. In the third row, the value $y_{2,1}$ is eliminated because it is equal to $y_{1,2}$. In the fourth row, the values of $y_{3,1}$ and $y_{3,2}$ are eliminated because they are equal to $y_{1,3}$ and $y_{2,3}$ respectively. Similarly, one can find the number of eliminated bits in each row

until the last row, where only $y_{k-1,0}, y_{k-1,k-1}$ are used. The maximum number of bits that can be encrypted using k values of y is,

$$l \leq k + \sum_{i=2}^{k} i \leq \frac{k^2 + 3k - 2}{2}.$$

For example, if the message length is 100 bits, then the minimum number of solved equations must be $200 \leq k^2 + 3k - 2$, $k \geq 13$, which is larger than $\sqrt{l} = \sqrt{100} = 10$.

5.4 JB IBE Security Proof

In this section, we first point out a flaw in the security proof presented in [JB08] for JB IBE, then we present a security proof for the fixed IBE. In JB IBE security proof, the authors assumed that, if an adversary $\mathcal{A}$ guessed the first k Jacobi symbols on the form $\left(\frac{2y_{j_1}s_{j_1}+2}{N}\right)$ and $\left(\frac{2y_{j_2}s_{j_2}+2}{N}\right)$, he will be able to guess the distribution of the rest $l-k$ Jacobi symbols $\left(\frac{2y_{j_1,j_2}s_{j_1}s_{j_2}+2}{N}\right)$. That is obviously because $y_{j_1,j_2}, s_{j_1}, s_{j_2}$ depends on $y_{j_1}s_{j_1}$ and $y_{j_2}s_{j_2}$ and consequently, the IBE security is reduced by a factor of $\frac{1}{2^k}$. We prove that this claim needs revision. In fact, we prove that guessing the Jacobi symbols $\left(\frac{2y_{j_1,j_2}s_{j_1}s_{j_2}+2}{N}\right)$ from $\left(\frac{2y_{j_1}s_{j_1}+2}{N}\right)$ and $\left(\frac{2y_{j_2}s_{j_2}+2}{N}\right)$ is as hard as guessing them from other independent Jacobi symbols $\left(\frac{2y_js_j+2}{N}\right)$ and $\left(\frac{2y_is_i+2}{N}\right)$. That is because Damgard [Dam88] showed that the distribution of Jacobi symbols sequences is random. If an adversary knows $\left(\frac{a}{N}\right)$, it is a hard problem for him to find $\left(\frac{a+1}{N}\right)$ for an unknown value a. Although a and $a+1$ are highly related, the Jacobi symbols $\left(\frac{a}{N}\right)$ and $\left(\frac{a+1}{N}\right)$ look random and indistinguishable from the adversary point of view. Based on the above, we present the following Lemma.

Lemma 5.1. *The distribution of the last $l-k$ bits of JB IBE encryption key in the form of $\left(\frac{2y_{j_1,j_2}s_{j_1}s_{j_2}+2}{N}\right)$ does not depend on the distribution of the first k bits in the form $\left(\frac{2y_{j_1}s_{j_1}+2}{N}\right)$ and $\left(\frac{2y_{j_2}s_{j_2}+2}{N}\right)$.*

Proof. As shown in Theorem 4.3, knowing $\left(\frac{a}{N}\right), \left(\frac{a+1}{N}\right), \left(\frac{a+2}{N}\right), ..., \left(\frac{a+a_1}{N}\right), ..., \left(\frac{a+a_2}{N}\right), ..., \left(\frac{a+P}{N}\right)$, it is a hard problem to find $\left(\frac{a+P+1}{N}\right)$.

We first choose a and P such that $a + P + 1 = 2y_{j_1,j_2}s_{j_1}s_{j_2} + 2$, then we can

write the above sequence in two different forms.

$$\left(\frac{a}{N}\right), \left(\frac{a+1}{N}\right), \left(\frac{a+2}{N}\right), ..., \left(\frac{2y_{j_1}s_{j_1}+2}{N}\right), ..., \left(\frac{2y_{j_2}s_{j_2}+2}{N}\right), ..., \left(\frac{a+P}{N}\right)$$

where $a_1 = 2y_{j_1}s_{j_1} + 2 - a,\ a_2 = 2y_{j_2}s_{j_2} + 2 - a.$

$$\left(\frac{a}{N}\right), \left(\frac{a+1}{N}\right), \left(\frac{a+2}{N}\right), ..., \left(\frac{2y_{j}s_{j}+2}{N}\right), ..., \left(\frac{2y_{i}s_{i}+2}{N}\right), ..., \left(\frac{a+P}{N}\right)$$

where $a_1 = 2y_{j}s_{j} + 2 - a,\ a_2 = 2y_{i}s_{i} + 2 - a.$

Since $\mathbb{Z}_{\mathbb{N}}$ is an additive group, the values of a_1, a_2 and P exist in both sequences for any value y or s. From the above equations, guessing the Jacobi symbol $\left(\frac{2y_{i}s_{j_1}s_{j_2}+2}{N}\right)$ from $\left(\frac{2y_{j_1}s_{j_1}+2}{N}\right)$ and $\left(\frac{2y_{j_2}s_{j_2}+2}{N}\right)$ is as hard as guessing them from independent Jacobi symbols. □

We note here that in JB IBE, it is much harder to guess the Jacobi symbols $\left(\frac{2y_{j_1,j_2}s_{j_1}s_{j_2}+2}{N}\right)$ than the Damgard problem because the only available Jacobi symbols in the whole sequence are $\left(\frac{2y_{j_1}s_{j_1}+2}{N}\right)$ and $\left(\frac{2y_{j_2}s_{j_2}+2}{N}\right)$.

We now present the security proof for the fixed JB IBE.

Theorem 5.1. *Suppose the QR assumption holds for RSAgen and F is a secure PRF. Then the proposed JB IBE is IND-ID-CPA secure based on the QR assumption when H is modelled as a random oracle. In particular, suppose $\mathcal{A}$ is an efficient IND-ID-CPA adversary, then there exist efficient algorithms B_1, B_2 whose running time is the same as that of $\mathcal{A}$ such that,*

$$IBEAdv_{\mathcal{A},JB}(\lambda) \leq 2QRAdv_{B_2,RSAgen}(\lambda) + PRFAdv_{B_1,F}(\lambda).$$

We define a sequence of games and let W_i represents the winning of the i_{th} game by the adversary $\mathcal{A}$. These games are defined as follows.

- **Game-0**. This game is the usual adversarial game.
- **Game-1**. This game replaces the PRF F with a truly random function.
- **Game-2**. This game explains how to simulate the hash function H.
- **Game-3**. This game sets $u \in QR(N)$.
- **Game-4**. This game explains how to respond to a challenge query from $\mathcal{A}$.
- **Game-5**. This game sets $R \in J(N) \setminus QR(N)$.
- **Game-6** replaces the message m with a random number z.

The details of the proof are as follows.

- Game-0. This is the usual adversarial game for defining the IND-ID-CPA security of IBE protocols. The challenger picks the random oracle $H : ID \to J(N)$ at random from the set of all such functions in the *Setup* algorithm and allows $\mathcal{A}$ to query H at arbitrary points. Thus,

$$|\Pr[W_0] - \frac{1}{2}| = IBEAdv_{\mathcal{A},JB}(\lambda).$$

- Game-1. This is the same as Game-0, with the following change. In the *Setup* algorithm, instead of using a PRF F to respond to $\mathcal{A}$'s private key queries, we use a truly random function $f : ID \to \{0, 1, 2, 3\}$. If F is a secure PRF, $\mathcal{A}$ will not notice the difference between Game-0 and Game-1. In particular, there exists an algorithm B_1 (whose running time is about the same as that of $\mathcal{A}$) such that,

$$|\Pr[W_1] - \Pr[W_0]| = PRFAdv_{B_1,F}(\lambda).$$

- Game-2. (N, u, H) are the public parameters *params* given to $\mathcal{A}$ in the previous game where u is uniform in $J(N) \setminus QR(N)$ and the random oracle H is a random function $H : ID \to J(N)$. We make the following change in the random oracle H in this game. The challenger responds to a query to $H(ID)$ by picking $a \in_R \{0, 1\}$ and $v \in_R \mathbb{Z}_{\mathbb{N}}$ and setting $H(ID) = u^a v^2$. Thus the challenger implements a random function $H : ID \to J(N)$ as in the previous game. The challenger responds to a private key query as follows.

  Suppose $R = H(ID) = u^a v^2$ for some $a \in_R \{0, 1\}$ and $v \in_R \mathbb{Z}_{\mathbb{N}}$. The challenger responds to a private key query for ID by setting either $R^{\frac{1}{2}} = v$ (when $a = 0$) or $(uR)^{\frac{1}{2}} = uv$ (when $a = 1$). Since v is uniform in $\mathbb{Z}_{\mathbb{N}}$, this will produce a square root of R or uR which is also uniform among the four square roots, as in the previous game. Thus, $\mathcal{A}$'s views in Game-1 and Game-2 are identical and therefore,

$$|\Pr[W_2] = \Pr[W_1]|.$$

- Game-3. In this game, the challenger chooses u uniformly in $QR(N)$ instead of $J(N) \setminus QR(N)$. Since this is the only change between Game-2 and Game-3, $\mathcal{A}$ will not notice the difference assuming that the QR assumption holds for RSAgen. In particular, there exists an algorithm B_2 (whose running time is about the same as that of $\mathcal{A}$) such that

$$|\Pr[W_3] - \Pr[W_2]| = QRAdv_{B_2,RSAgen}(\lambda).$$

- Game-4. We describe below in detail how, in this game, the challenger responds to a challenge query from $\mathcal{A}$.
  - He chooses $uR, R \in QR(N)$ and sets $H(ID) = R$. (*)
  - He chooses $s \in_R \mathbb{Z}_{\mathbb{N}}$ and computes $S_i = s_i^2$.
  - Upon receiving two messages m_0, m_1 from the adversary, the challenger tosses a fair coin $b \in \{0, 1\}$ and sets $(c, \overline{c}) \leftarrow Encrypt(params, ID, m_b)$.
  - He sends $(S, c, \overline{c})$ to $\mathcal{A}$.

  Since this game is the same as Game-3, thus,

$$|\Pr[W_4] = \Pr[W_3]|.$$

- Game-5. In this game, we make a change in the challenge phase. We replace the line (*) in Game-4 with the following.
  - He chooses $uR, R \in J(N) \setminus QR(N)$ and sets $H(ID) = R$.

  Since the only difference between Game-5 and Game-4 is that $uR, R \in J(N) \setminus QR(N)$ in Game-5 instead of $uR, R \in QR(N)$ in Game-4, $\mathcal{A}$ will not notice the difference assuming that the QR assumption holds for RSAgen. In particular, there exists an algorithm B_2 (whose running time is about the same as that of $\mathcal{A}$) such that

$$|\Pr[W_5] - \Pr[W_4]| = QRAdv_{B_2,RSAgen}(\lambda).$$

- Game-6: In this game, we replace the message $m_{(b)}$ by a random string $z \in_R \{-1, 1\}^l$ i.e., $c_i = z_i \cdot \left(\frac{2y_i s_i + 2}{N}\right)$ and $\overline{c}_i = z_i \cdot \left(\frac{2\overline{y}_i s_i + 2}{N}\right)$ where $y_i = y_{j_1,j_2}$ and $s_i = s_{j_1} s_{j_2}$, $i = k \cdot j_1 + j_2$ for the last $l - k$ bits. We first prove that $(2y_i s_i + 2)(-2y_i s_i + 2)R \in QR(N)$.

  Proof. Let $g(s_i) = (2y_i s_i + 2)$, then we have,

$$\begin{aligned} g(s_i)g(-s_i)R &= 4(y_i s_i + 1)(-y_i s_i + 1)R, \\ g(s_i)g(-s_i)R &= 4(1 - (y_i s_i)^2)R, \\ g(s_i)g(-s_i)R &= 4(Rx_i^2)R = (2Rx_i)^2 \in QR(N). \end{aligned}$$

  Similarly, we can prove that $(2\overline{y}_i s_i + 2)(-2\overline{y}_i s_i + 2)uR \in QR(N)$.
  Since $S_i \in QR(N)$, $uR, R \in J(N) \setminus QR(N)$, $(2y_i s_i + 2)(-2y_i s_i + 2)R \in QR(N)$ and $(2\overline{y}_i s_i + 2)(-2\overline{y}_i s_i + 2)uR \in QR(N)$ and based on Lemma 5.1, Case 1 in Lemma 4.2 can be applied and the distribution of the Jacobi symbols $\left(\frac{2y_i s_i + 2}{N}\right)$ and $\left(\frac{2\overline{y}_i s_i + 2}{N}\right)$

are random in $\{\pm 1\}$. Thus, $\mathcal{A}$ will not be able to distinguish between Game-5 and Game-6. i.e.

$$|\Pr[W_6] = \Pr[W_5]|.$$

- Clearly in Game-6 we have

$$|\Pr[W_6] = \Pr[\overline{W}_6] = \frac{1}{2}|.$$

Combining all the previous equations proves Theorem 5.1.

5.5 Conclusion

In this chapter, we reviewed the security of JB IBE. We showed that this IBE is not IND-ID-CPA secure. We also presented a solution to overcome this security flaw. We also pointed out a flaw of the security proof of JB IBE and presented a security proof that shows that the fixed JB IBE is as secure as the original BasicIBE.

Chapter 6

Efficient Attribute-based Signcryption Systems

In this chapter, we present two ciphertext-policy attribute-based signcryption (CP-ABSC) which are efficient and fully secure. These systems are BasicABSC and AnonABSC. In addition to providing confidentiality, unforgeability and access control to the signcrypted data, our proposed AnonABSC is anonymous. i.e. an adversary can not determine for which attributes or policies the message is signcrypted. This is very useful especially when the signcrypted data are stored on a public cloud such as the Internet. As far as we know, this is the first CP-ABSC that achieves such property. In addition, our proposed systems are time- and power-efficient and they do not depend on expensive paring operations which make them suitable for mobile and lightweight devices. Our systems are fully secure under the quadratic residuosity (QR) assumption and provide a constant ciphertext size regardless of the number of attributes associated with the access structure.

6.1 Introduction

Nowadays, most sensitive data for individuals and organisations alike are stored in a public cloud such as the Internet to provide an access on demand to their data in multiple devices anywhere anytime. This sensitive information may be, for instance, an email address and it's password. To safely store this information on a public cloud, this information must be in an encrypted format with some sort of access control. Public key cryptography (PKC) does not support an access control structure for encrypted data; a user can only decrypt the message if and only if he posses the secret key associated with the public key by which the message is encrypted.

Attribute-based cryptography (ABC) was presented to give an access structure to encrypted data stored on a public cloud. It allows users to encrypt or sign messages based on their attributes instead of their individual identities as in the identity-based cryptography (IBC) [Sha84]. These attributes are, for example, the place where they live or the company in which they work. ABC can be classified as key-policy ABC and ciphertext-policy ABC. A policy is a rule that determines which attributes should decrypt or verify the message. In a key-policy ABC, the policy is inserted in the key while the ciphertext is encrypted or signed using the

Table 6.1: Comparison Between Different ABC Systems

Systems	KP/CP-ABC	Access Structure	Security Model	Decryption Key Size	Ciphertext Size
SW [SW05]	KP-ABE	Threshold	Selective Security	$n\mathbb{G}$	$n\mathbb{G} + \mathbb{G}_T$
OSW [OSW07]	KP-ABE	Tree	Selective Security	$\lvert\mathbb{A}\rvert\mathbb{G}$	$\lvert\mathbb{P}\rvert\mathbb{G} + \mathbb{G}_T$
BSW [BSW07]	CP-ABE	Tree	Selective Security	$(2\lvert\mathbb{A}\rvert + 1)\mathbb{G}$	$(2\lvert\mathbb{P}\rvert + 1)\mathbb{G} + \mathbb{G}_T$
Waters [Wat11]	CP-ABE	LSSS	Selective Security	$(\lvert\mathbb{A}\rvert + 2)\mathbb{G}$	$(2\lvert\mathbb{P}\rvert + 1)\mathbb{G} + \mathbb{G}_T$
FYW [GMS+14]	CP-ABE	AND gates	Selective Security	$2\mathbb{G}$	(n-$\lvert\mathbb{P}\rvert$ + 2)$\mathbb{G}$+$\mathbb{G}_T$
YWX [HLY13]	CP-ABSC	Non monotonic	Full Security	$(n+1)\mathbb{G}$	$5\mathbb{G} + l$
Proposed system	CP-ABSC	AND gates	Full Security	$n\mathbb{Z}_{\mathbb{N}}$	$\mathbb{Z}_{\mathbb{N}} + 2l$

attributes. In a ciphertext-policy ABC, the policy is inserted in the ciphertext while the key represents the attributes.

In this chapter, we present two ciphertext-policy attribute-based signcryption (CP-ABSC) systems in which the confidentiality and unforgeability of the data is guaranteed in a more efficient way than using an encryption and signature systems individually. These systems are BasicABSC and AnonABSC. AnonABSC is anonymous to preserve the privacy of the attributes of the signcrypted data. The access structure of these systems is AND gate. They are efficient compared to other pairing-based cryptosystems and hence, they are more suitable for mobile and lightweight devices. They are fully secure in the random oracle model based on the quadratic residuosity (QR) assumption. The ciphertext size is constant regardless of the size of the access structure.

A comparison of some ABC systems is presented in Table 6.1 where n represents the number of available attributes, $\mathbb{G}$ and $\mathbb{G}_T$ are two groups defined over a bilinear pairing $\hat{e} : \mathbb{G} \times \mathbb{G} \rightarrow \mathbb{G}_T$. $|\mathbb{A}|$ represents the size of an attribute set and $|\mathbb{P}|$ is the size of the access structure. l is the message size and $\mathbb{Z}_{\mathbb{N}}$ represents an element of the same size as the modulus N.

Contribution. Our systems have the following advantages.

Anonymity. The anonymity of any cryptography system is an important security property especially for information with public access. If an adversary obtained an access to the signcrypted data, he will not be able to get the attributes for which the message is signcrypted (the receiver's attributes). As far as we know, there is no attribute-based signcryption with anonymity in the literature.

Time-efficiency. All the proposed ABSC systems in the literature are constructed using pairing. A pairing operation is an expensive and time-consuming process. It takes approximately 2.5 times an RSA modular exponentiation based on MIRACL benchmarks. Our proposed systems require only two prime search operations which take around 11ms each for a modulus size of 1024 bits [JB08] with a large message space of $2^{|N|}$ bits where $|N|$ is the modulus size. In addition, our proposed systems can be constructed using a trade-off approach to further boost the performance of the proposed CP-ABSC systems.

Security. Our proposed systems are fully secure in both message confidentiality

and ciphertext unforgeability based on the quadratic residuosity (QR) assumption in the random oracle model. In addition, the signcryption process can only be done with the secret keys associated with the attributes of the sender (and that where the signature part comes from), so these systems can be transformed to become secure against adaptive chosen ciphertext attack (IND-CCA2) using the Fujisaki-Okamoto transformation [FO13] without affecting the signature process.

Fixed ciphertext size. The ciphertext of the proposed systems are fixed at $|N|+2l$ bits regardless of the access structure of the receiver (which defines who can decrypt the message) or the sender (which defines who can sign the message).

In the rest of chapter, we present the structure of the proposed systems along with their security proofs. After that, we present a trade-off construction for these systems and then conclude the chapter. Through the rest of the chapter, η is a subscript that defines a receiver (encryption) variable, σ is a subscript that defines a sender (signature) variable, A is an attribute, $\mathbb{A}$ is a set of all user's attributes, $\mathbb{P}$ is the access structure, n is the number of all possible attributes, i is an attribute index and j is a bit index.

6.2 BasicABSC

In this section, we explain how to implement BasicABSC which is time-efficient and fully secure ABSC system. BasicABSC consists of four algorithms: Setup, KeyGeneration, Signcrypt and Unsigncrypt. We note here that the attributes in our proposed systems are mapped to the same values for both encryption and signature i.e. $A_{i,\sigma} = A_{i,\eta}$, $r_{i,\sigma} = r_{i,\eta}$ and uExtract and sExtract are the same. From now on, we refer to the key extraction algorithm as KeyGeneration. The construction of BasicABSC is as follows.

- $(params, MS) \leftarrow Setup(\lambda)$. Using RSAgen($\lambda$), generate (p, q), calculate the modulus $N = pq$, choose $u \in J(N) \setminus QR(N)$, and choose a hash function $H : A_i \rightarrow J(N)$. The public parameters $params$ are $[N, u, H]$. The master secret MS parameters are p, q and a secret key K for a pseudorandom function (PRF) $F_K : A_i \rightarrow [0, 1, 2, 3]$.

- $(r_i) \leftarrow KeyGeneration(MS, params, A_i)$. Calculate $H(A_i) \in J(N)$ and $w_i = F_K(A_i) \in \{0, 1, 2, 3\}$. Choose $a \in \{0, 1\}$ such that $u^a A_i \in QR(N)$. Let $[z_0, z_1, z_2, z_3]$ be the four square roots of $u^a A_i \in \mathbb{Z}_{\mathbb{N}}$, then $r_i = z_w$. Repeat this process for all n attributes in the system.

- $(C) \leftarrow Signcrypt(m, params, \mathbb{A}_\sigma, \mathbb{P}_\sigma, \mathbb{P}_\eta, r_{i,\sigma})$. To signcrypt a message $m \in \{-1, 1\}^l$ where l is the message length, the sender checks based on his access structure $\mathbb{P}_\sigma$

which attributes are quadratic residue and which are not. Let t_σ be the number of the sender's (signature) attributes that are non quadratic residue and $|\mathbb{P}_\sigma| - t_\sigma$ be the number of the sender's attributes (signature) that are quadratic residue. Choose two random even values d_1, d_2 and a random value s. Calculate $S = s^{d_2}$, $U = u^{d_1}$ and $D = USu^{t_\sigma} = s^{d_2}u^{d_1+t_\sigma}$. Calculate $[x_j, y_j, \overline{x}_j, \overline{y}_j]$, $j \in [0, l-1]$ such that these variables satisfy the following equations.

$$[x_j, y_j] = Rx_j^2 + T_j y_j^2 \equiv 1 \pmod{N} \tag{6.1}$$

$$[\overline{x}_j, \overline{y}_j] = u^{-1}Rx_j^2 + T_j y_j^2 \equiv 1 \pmod{N} \tag{6.2}$$

$$\text{Where } R = u^{|\mathbb{P}_\eta|}\prod_{i=1}^{n} b_{i,\eta}A_i, \text{ and } T_j = T^{2j+1} = D^{2j+1}\prod_{i=1}^{n} b_{i,\sigma}A_i^{2j+1}$$

$b_i = 1$ iff $A_i \subset \mathbb{P}$ and $b_i = 0$ otherwise.

The message $m = [m_0, m_1, ..., m_{l-1}]$ is signcrypted using the following formula.

$$c_j = m_j \cdot \left(\frac{2y_j t_j + 2}{N}\right) \text{ and } \overline{c}_j = m_j \cdot \left(\frac{2\overline{y}_j t_j + 2}{N}\right)$$

$$\text{Where } t_j = \sqrt{T_j} = (US)^{\frac{2j+1}{2}}\prod_{i=1}^{n} b_{i,\sigma}r_{i,\sigma}^{2j+1}$$

The ciphertext is $C = (D, c, \overline{c})$, where $c = [c_0, c_1, ..., c_{l-1}]$ and $\overline{c} = [\overline{c}_0, \overline{c}_1, ..., \overline{c}_{l-1}]$.

- $(m) \leftarrow Unsigncrypt(C, params, \mathbb{A}_\eta, \mathbb{P}_\sigma, \mathbb{P}_\eta, r_{i,\eta})$. First, the receiver checks that $\mathbb{P}_\eta \subseteq \mathbb{A}_\eta$. If $\mathbb{P}_\eta \subseteq \mathbb{A}_\eta$, then he finds t_η in a way similar to the sender based on his attribute set $\mathbb{A}_\eta$. Then he solves either Equation 6.1 or 6.2 and unsigncrypts the message based on if $|\mathbb{P}_\eta| - t_\eta$ is even or odd. If $|\mathbb{P}_\eta| - t_\eta$ is even, then the receiver solves Equation 6.1 to get x_j and y_j otherwise he solves Equation 6.2 to get $\overline{x}_j$ and $\overline{y}_j$. He calculates m as follows.

$$m_j = c_j \cdot \left(\frac{x_j r + 1}{N}\right), \text{ If } |\mathbb{P}_\eta| - t_\eta \text{ is even.}$$

$$m_j = \overline{c}_j \cdot \left(\frac{\overline{x}_j r + 1}{N}\right), \text{ If } |\mathbb{P}_\eta| - t_\eta \text{ is odd.}$$

$$\text{Where } r = \sqrt{R} = u^{\frac{|\mathbb{P}_\eta| - t_\eta}{2}}\prod_{i=1}^{n} b_{i,\eta}r_{i,\eta}, \text{ If } |\mathbb{P}_\eta| - t_\eta \text{ is even.}$$

$$r = \sqrt{R} = u^{\frac{|\mathbb{P}_\eta| - t_\eta - 1}{2}}\prod_{i=1}^{n} b_{i,\eta}r_{i,\eta}, \text{ If } |\mathbb{P}_\eta| - t_\eta \text{ is odd.}$$

The Unsigncrypt process is illustrated in Figure 6.1.

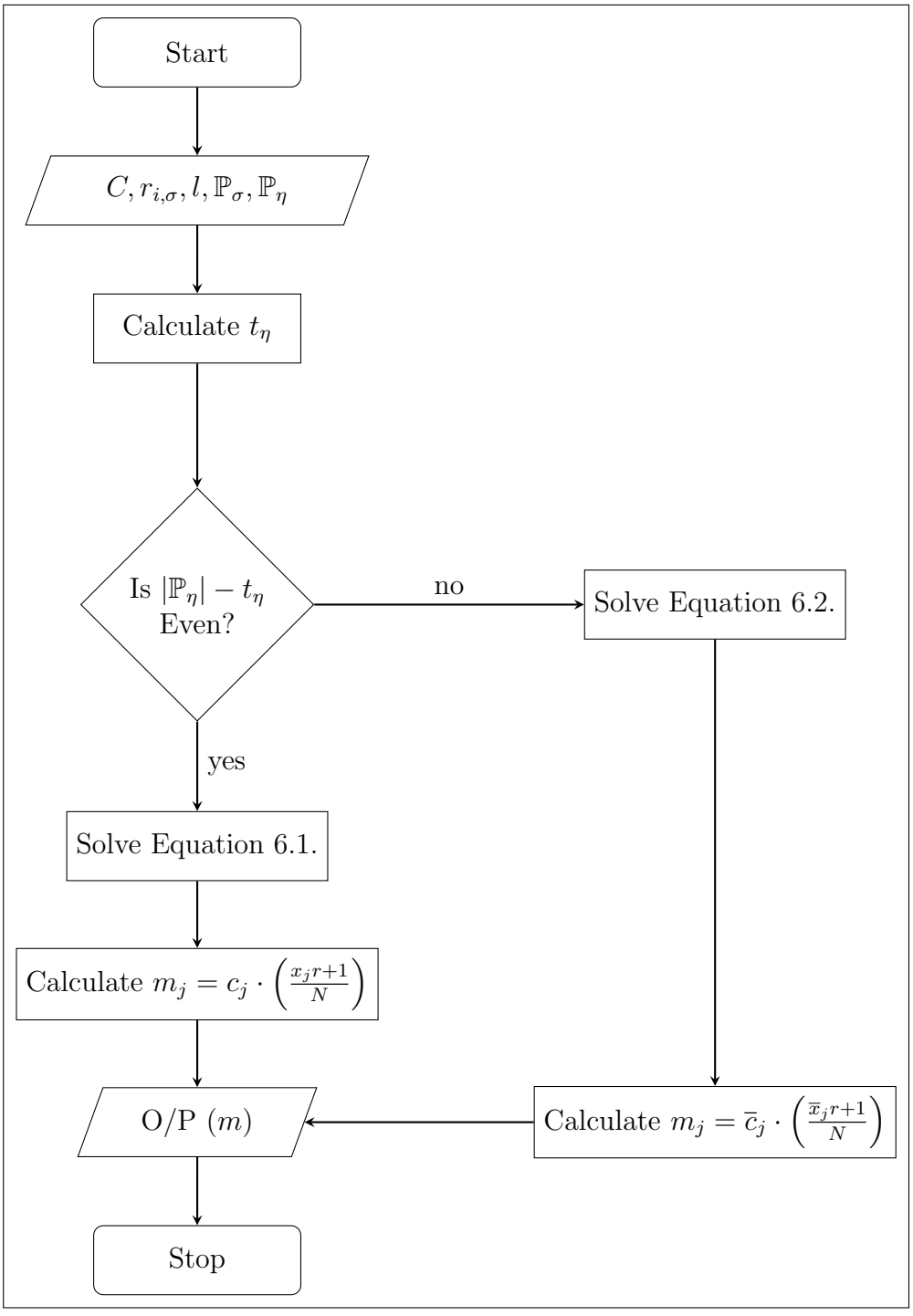

Figure 6.1: Flaw Chart of The Unsigncrypt Process of BasicABSC

6.2.1 Soundness

In this section, we explain the soundness of the proposed BasicABSC. Assume two random variables $R = r^2$ and $T = t^2$ such that $r, t \in \mathbb{Z}_{\mathbb{N}}$. R represents the public key (attributes) of the receiver and r represents his secret key and T represents the public key (attributes) of the sender and t represents his secret key. The equation $Rx^2 + Ty^2 = 1 \pmod N$ can be solved to obtain x, y [BGH07]. After obtaining x, y, the following equality holds.

$$\left(\frac{xr+1}{N}\right) = \left(\frac{2yt+2}{N}\right).$$

if the sender wants to encrypt the message $m \in \{-1, 1\}$, he uses his secret key t to encrypt the message as follows.

$$c = m \cdot \left(\frac{2yt+2}{N}\right)$$

And the receiver can decrypt the message as follows.

$$c \cdot \left(\frac{xr+1}{N}\right) = m \cdot \left(\frac{2yt+2}{N}\right) \cdot \left(\frac{xr+1}{N}\right) = m.$$

One issue that faces the sender during the signcryption process is that he can not determine if R is quadratic residue or not, so he has to solve Equations 6.1 and 6.2 for each bit and sends c and $\overline{c}$ [BGH07].

Another issue that faces the sender during the signcryption process is that while he generates S^{2j+1}, U^{2j+1}, he must do it in a way that makes $T^{2j+1} \in QR(N)$ without revealing t_σ to the receiver because t_σ will give information about the quadratic residuosity of the sender's attributes. We insure that by generating $S = s^{d_2}$ and $U = u^{d_1}$ as shown above. d_1, d_2 and s conceal t_σ while maintaining $T^{2j+1} = D^{2j+1} \prod_{i=1}^{n} b_{i,\sigma} A_i^{2j+1} \in QR(N)$.

The signature part comes from the fact that, the sender will not be able to encrypt the message unless he has the secret keys $r_{i,\sigma}$ which are related to his access structure $\mathbb{P}_\sigma$. If he uses another secret keys $\overline{r}_{i,\sigma}$ to encrypt the message, the receiver will not be able to decrypt the ciphertext. In other words, if the receiver successfully decrypts the messages, that gives an implicit verification of the signature of the sender.

– **Remark.** In a multi-user environment, the sender must be the only one who can sign his messages regardless of the attributes because many users may have

the same attributes. For instance, two users may have the same position a company. To insure that, the sender create a secret key s and sends $S = s^{d_2}$ to the receiver. If the receiver correctly decrypts the message using S, this means that the correct value of s was used to encrypt the message.

6.2.2 BasicABSC Security

We show that the proposed BasicABSC is secure by proving the following theorems.

Theorem 6.1. *Suppose the quadratic residuosity assumption holds for RSAgen and F is a secure PRF. Then the proposed BasicABSC is indistinguishably secure against adaptive chosen plaintext attack (IND-ABSC-CPA) based on the QR assumption when H is modelled as a random oracle. In particular, suppose $\mathcal{A}$ is an efficient IND-ABSC-CPA adversary, then there exist efficient algorithms B_1, B_2 whose running time is the same as that of $\mathcal{A}$ such that,*

$$ABSCAdv_{\mathcal{A},BasicABSC}(\lambda) \leq 2QRAdv_{B_2,RSAgen}(\lambda) + PRFAdv_{B_1,F}(\lambda).$$

Theorem 6.2. *Suppose the quadratic residuosity assumption holds for RSAgen and F is a secure PRF. Then the proposed BasicABSC is existentially unforgeable against chosen-message attack (EUF-ABSC-SMA) based on the QR assumption when H is modelled as a random oracle. In particular, suppose $\mathcal{A}$ is an efficient EUF-ABSC-SMA adversary, then there exist efficient algorithms B_1, B_2 whose running time is the same as that of $\mathcal{A}$ such that,*

$$ABSCAdv_{\mathcal{A},BasicABSC}(\lambda) \leq 2QRAdv_{B_2,RSAgen}(\lambda) + PRFAdv_{B_1,F}(\lambda).$$

We note here that in BasicABSC, a forgery attack is similar to a message confidentiality attack. That is because the equation $Rx^2+Ty^2 \equiv 1 \pmod N$ is symmetric and the secret keys $\left(\frac{2yt+2}{N}\right) = \left(\frac{xr+1}{N}\right)$ can be both used in Signcrypt and Unsigncrypt. In addition, if an adversary was able to generate a valid encryption $\left(\frac{2yt+2}{N}\right)$ without running the Signcrypt algorithm (i.e. without knowing the secret key t) then this very adversary can decrypt the message by calculating $m = c \cdot \left(\frac{2yt+2}{N}\right)$.

- **Security Proof for Message Confidentiality**
  We define a sequence of games and let W_i represents the winning of the i_{th} game by the adversary $\mathcal{A}$. These games are defined as follows.
  - **Game-0**. This game is the usual adversarial game.
  - **Game-1**. This game replaces the PRF F with a truly random function.
  - **Game-2**. This game explains how to simulate the hash function H.

- **Game-3**. This game explains how to respond to a signcryption query from $\mathcal{A}$.
- **Game-4**. This game sets $u \in QR(N)$.
- **Game-5**. This game sets $u^{-1}R, R \in J(N) \setminus QR(N)$ in the challenge phase.
- **Game-6**. This game sets T_j randomly for each bit.
- **Game-7** replaces the message m with a random number z.

- Game-0. This is the usual adversarial game for defining the IND-ABSC-CPA security of ABSC protocols. The challenger picks the random oracle $H : A_i \rightarrow J(N)$ at random from the set of all such functions in the *Setup* algorithm and allows $\mathcal{A}$ to query H at arbitrary points. Thus,

$$|\Pr[W_0] - \frac{1}{2}| = ABSCAdv_{\mathcal{A},BasicABSC}(\lambda).$$

- Game-1. This is the same as Game-0, with the following change. In the *Setup* algorithm, instead of using a PRF F to respond to $\mathcal{A}$'s private key queries, we use a truly random function $f : A_i \rightarrow \{0, 1, 2, 3\}$. If F is a secure PRF, $\mathcal{A}$ will not notice the difference between Game-0 and Game-1. In particular, there exists an algorithm B_1 (whose running time is about the same as that of $\mathcal{A}$) such that,

$$|\Pr[W_1] - \Pr[W_0]| = PRFAdv_{B_1,F}(\lambda).$$

- Game-2. (N, u, H) are the public parameters *params* given to $\mathcal{A}$ in the previous game where u is uniform in $J(N) \setminus QR(N)$ and the random oracle H is a random function $H : A_i \rightarrow J(N)$. We make the following change in the random oracle H in this game. The challenger responds to a query to $H(A_i)$ by picking $a \in_R \{0, 1\}$ and $v \in_R \mathbb{Z}_{\mathbb{N}}$ and setting $H(A_i) = u^a v^2$. Thus the challenger implements a random function $H : A_i \rightarrow J(N)$ as in the previous game. The challenger responds to a private key query as follows.

  Suppose $H(A_i) = u^a v^2$ for some $a \in_R \{0, 1\}$ and $v \in_R \mathbb{Z}_{\mathbb{N}}$. The challenger responds to a private key query for A_i by setting either $H(A_i)^{\frac{1}{2}} = v$ (when $a = 0$) or $(uH(A_i))^{\frac{1}{2}} = uv$ (when $a = 1$). Since v is uniform in $\mathbb{Z}_{\mathbb{N}}$, this will produce a square root of $H(A_i)$ or $uH(A_i)$ which is also uniform among the four square roots, as in the previous game. Thus, $\mathcal{A}$'s views in Game-1 and Game-2 are identical and therefore,

$$|\Pr[W_2] = \Pr[W_1]|.$$

- Game-3. We describe below how the challenger responds to a signcryption query from $\mathcal{A}$ for a given message m.

– He sets $u^{t_\eta}\prod_{i=1}^{n} b_{i,\eta}A_i \in QR(N)$. (*)

– He chooses two random even values d_1, d_2 and a random value s and calculates $D = u^{d_1+t_\sigma}s^{d_2}$ as in Signcrypt.

– He sets $(C) = Signcrypt(m, params, \mathbb{A}_\sigma, \mathbb{P}_\sigma, \mathbb{P}_\eta, r_{i,\sigma})$.

– He sends $C = (D, c, \overline{c})$ to $\mathcal{A}$.

Since this game is the same as Game-2, thus,

$$|\Pr[W_3] = \Pr[W_2]|.$$

- Game-4. In this game, the challenger chooses u uniformly in $QR(N)$ instead of $J(N)\backslash QR(N)$ and consequently, $u^{-1}R, R \in QR(N)$. Since this is the only change between Game-4 and Game-3, $\mathcal{A}$ will not notice the difference assuming that the QR assumption holds for RSAgen. In particular, there exists an algorithm B_2 (whose running time is about the same as that of $\mathcal{A}$) such that,

$$|\Pr[W_4] - \Pr[W_3]| = QRAdv_{B_2,RSAgen}(\lambda).$$

- Game-5. In this game, we show how to simulate the challenge phase. Upon receiving two different messages m_0, m_1, the challenge signature attribute set $\mathbb{A}^*_\sigma$, the encryption attribute set $\mathbb{A}^*_\eta$ and the challenge access structures for both sender and receiver $\mathbb{P}^*_\sigma, \mathbb{P}^*_\eta$, the challenger tosses a fair coin $b \in \{0, 1\}$ and calculates $C^* = Signcrypt(m^*_b, params, \mathbb{A}^*_\sigma, \mathbb{P}^*_\sigma, \mathbb{P}^*_\eta, r^*_{i,\sigma})$ but with exception of replacing the line (*) in Game-4 with the following.

– He sets $u^{t_\eta}\prod_{i=1}^{n} b_{i,\eta}A_i \in J(N) \setminus QR(N)$. (*)

i.e. $u^{-1}R, R \in J(N) \setminus QR(N)$. Since the only difference between Game-5 and Game-4 is that $u^{-1}R, R \in J(N) \setminus QR(N)$ instead of $u^{-1}R, R \in QR(N)$, $\mathcal{A}$ will not notice the difference assuming that the QR assumption holds for RSAgen. In particular, there exists an algorithm B_2 (whose running time is about the same as that of $\mathcal{A}$) such that,

$$|\Pr[W_5] - \Pr[W_4]| = QRAdv_{B_2,RSAgen}(\lambda).$$

- Game-6. In this game, we encrypt the message by choosing U_j and S_j such that $T_j = t_j^2 \in \mathbb{Z}_\mathbb{N}$ is independent and random for each bit. i.e. $c_j = m_j \cdot \left(\frac{2+2y_j t_j}{N}\right)$ where

$t_j = U_j S_j \prod_{i=1}^{n} b_{i,\sigma} r_{i,j,\sigma}$. To prove that Game-6 is indistinguishable from Game-5, we present Lemma 6.1.

Lemma 6.1. *The distribution of the Jacobi symbols* $\left(\frac{2y_j t^{2j+1}+2}{N}\right)$ *is indistinguishable from the distribution the Jacobi symbols* $\left(\frac{2y_j t_j+2}{N}\right)$.

The proof of Lemma 6.1 is similar to Lemma 4.3 and $\mathcal{A}$ will not be able to distinguish between Game-5 and Game-6. i.e.

$$|\Pr[W_6] = \Pr[W_5]|.$$

- Game-7. In this game, we replace the message $m_{(b)}$ by a random string $z \in_R \{-1, 1\}^l$ i.e., $c_j = z_j \cdot \left(\frac{2y_j t_j+2}{N}\right)$ and $\overline{c}_j = z_j \cdot \left(\frac{2\overline{y}_j t_j+2}{N}\right)$. We first prove that $(2y_j t_j + 2)(-2y_j t_j + 2)R \in QR(N)$.
  Proof. Let $g(y_j, t_j) = (2y_j t_j + 2)$, then we have,

$$\begin{aligned} g(y_j, t_j)g(y_j, -t_j)R &= 4(y_j t_j + 1)(-y_j t_j + 1)R, \\ g(y_j, t_j)g(y_j, -t_j)R &= 4(1 - (y_j t_j)^2)R, \\ g(y_j, t_j)g(y_j, -t_j)R &= 4(Rx_j^2)R = (2Rx_j)^2 \in QR(N). \end{aligned}$$

  Similarly, we can prove that $(2\overline{y}_j t_j + 2)(-2\overline{y}_j t_j + 2)u^{-1}R \in QR(N)$.
  Since $T_j \in QR(N)$, $u^{-1}R, R \in J(N) \setminus QR(N)$, $(2y_j t_j + 2)(-2y_j t_j + 2)R \in QR(N)$ and $(2\overline{y}_j t_j + 2)(-2\overline{y}_j t_j + 2)u^{-1}R \in QR(N)$ then Case 1 in Lemma 4.2 can be applied and the distribution of the Jacobi symbols $\left(\frac{2y_j t_j+2}{N}\right)$ and $\left(\frac{2\overline{y}_j t_j+2}{N}\right)$ are random in $\{\pm 1\}$. Thus, $\mathcal{A}$ will not be able to distinguish between Game-6 and Game-7. i.e.

$$|\Pr[W_7] = \Pr[W_6]|.$$

- Clearly in Game-7 we have

$$|\Pr[W_7] = \frac{1}{2}|.$$

  Combining all the previous equations proves Theorem 6.1.

- **Security Proof for Ciphertext Unforgeability**
  We define a sequence of games and let W_i represents the winning of the i_{th} game by the adversary $\mathcal{A}$. These games are defined as follows.

  – **Game-0**. This game is the usual adversarial game.

  – **Game-1**. This game replaces the PRF F with a truly random function.

  – **Game-2**. This game explains how to simulate the hash function H.

- **Game-3**. This game explains how to respond to a signcrypt query using the Unsigncrypt algorithm.
- **Game-4**. This game sets $u \in QR(N)$.
- **Game-5**. This game sets $T_j \in J(N) \setminus QR(N)$.
- **Game-6**. This game sets a value A_i for each attribute for each bit.
- **Game-7** replaces the message m with a random number z.

- Game-0. This is the usual adversarial game for defining the EUF-ABSC-SMA security of ABSC protocols. The challenger picks the random oracle $H : A_i \rightarrow J(N)$ at random from the set of all such functions in the *Setup* algorithm and allows $\mathcal{A}$ to query H at arbitrary points. Thus, we have,

$$|\Pr[W_0] - \frac{1}{2}| = ABSCAdv_{\mathcal{A},BasicABSC}(\lambda).$$

- Game-1. This is the same as Game-0, with the following change. In the *Setup* algorithm, instead of using a PRF F to respond to $\mathcal{A}$'s private key queries, we use a truly random function $f : A_i \rightarrow \{0, 1, 2, 3\}$. If F is a secure PRF, $\mathcal{A}$ will not notice the difference between Game-0 and Game-1. In particular, there exists an algorithm B_1 (whose running time is about the same as that of $\mathcal{A}$) such that,

$$|\Pr[W_1] - \Pr[W_0]| = PRFAdv_{B_1,F}(\lambda).$$

- Game-2. (N, u, H) are the public parameters *params* given to $\mathcal{A}$ in the previous game where u is uniform in $J(N) \setminus QR(N)$ and the random oracle H is a random function $H : A_i \rightarrow J(N)$. We make the following change in the random oracle H in this game. The challenger responds to a query to $H(A_i)$ by picking $a \in_R \{0, 1\}$ and $v \in_R \mathbb{Z}_{\mathbb{N}}$ and setting $H(A_i) = u^a v^2$. Thus the challenger implements a random function $H : A_i \rightarrow J(N)$ as in the previous game. The challenger responds to a private key query as follows.

  Suppose $H(A_i) = u^a v^2$ for some $a \in_R \{0, 1\}$ and $v \in_R \mathbb{Z}_{\mathbb{N}}$. The challenger responds to a private key query for A_i by setting either $H(A_i)^{\frac{1}{2}} = v$ (when $a = 0$) or $(uH(A_i))^{\frac{1}{2}} = uv$ (when $a = 1$). Since v is uniform in $\mathbb{Z}_{\mathbb{N}}$, this will produce a square root of $H(A_i)$ or $uH(A_i)$ which is also uniform among the four square roots, as in the previous game. Thus, $\mathcal{A}$'s views in Game-1 and Game-2 are identical and therefore,

$$|\Pr[W_2] = \Pr[W_1]|.$$

- Game-3. We describe below how the challenger simulates a Signcrypt query from $\mathcal{A}$ for a given encryption attribute set $\mathbb{A}_\eta$, the message m, the access structures

for both sender and receiver $\mathbb{P}_\sigma, \mathbb{P}_\eta$.

- He sets $u^{t_\eta}\prod_{i=1}^{n} b_{i,\eta}A_i \in QR(N)$.
- He chooses two random even values d_1, d_2 and a random value s and calculates $D = u^{d_1+t_\sigma}s^{d_2}$ as in Signcrypt.(*)
- He sets C= Unsigncrypt$((D, m), params, \mathbb{A}_\eta, \mathbb{P}_\eta, \mathbb{P}_\sigma)$. As follows

$$c_j = m_j \cdot \left(\frac{rx_j + 1}{N}\right) \quad \text{and} \quad \overline{c}_j = m_j \cdot \left(\frac{r\overline{x}_j + 1}{N}\right)$$

- He sends $C = (D, c, \overline{c})$ to $\mathcal{A}$.

It is clear that C is simulated perfectly as the usual Signcrypt process. Since this game is the same as Game-2, thus,

$$|\Pr[W_3] = \Pr[W_2]|.$$

- Game-4. In this game, the challenger chooses u uniformly in $QR(N)$ instead of $J(N) \setminus QR(N)$. i.e. $u^{-1}R, R \in QR(N)$. Since this is the only change between Game-4 and Game-3, $\mathcal{A}$ will not notice the difference assuming that the QR assumption holds for RSAgen. In particular, there exists an algorithm B_2 (whose running time is about the same as that of $\mathcal{A}$) such that,

$$|\Pr[W_4] - \Pr[W_3]| = QRAdv_{B_2,RSAgen}(\lambda).$$

- Game-5. In this game, we replace the line (*) in Game-4 with the following.
  - He chooses a random value D such that $T_j \in J(N) \setminus QR(N)$.(*)

  Since the only difference between Game-5 and Game-4 is that $T_j \in J(N) \setminus QR(N)$ instead of $T_j \in QR(N)$, $\mathcal{A}$ will not notice the difference assuming that the QR assumption holds for RSAgen. In particular, there exists an algorithm B_2 (whose running time is about the same as that of $\mathcal{A}$) such that,

$$|\Pr[W_5] - \Pr[W_4]| = QRAdv_{B_2,RSAgen}(\lambda).$$

- Game-6, In this game, we hash the attributes A_i to a different value $H(A_i, j) = u^a A_{i,j} = r_{i,j}^2$ for each bit so that each bit is signcrypted using different key r_j for each bit. To prove that Game-6 is indistinguishable to Game-5, we present Lemma 6.2.

Lemma 6.2. *Hashing the attributes A_i to different values to signcrypt each bit is as secure as hashing the attribute to a single value to signcrypt the whole message.*

Proof. Jhanwar and Barua [BJ10] showed that there are $N-1$ solutions to the equation $Rx^2 + Ty^2 \equiv 1 \pmod N$ if $T, R \in QR(N)$. The solution (x, y) for that equation is in the form,

$$\left(\frac{-2zt}{R+Tz^2}, \frac{R-Tz^2}{t(R+Tz^2)}\right)$$

for some $z \in \mathbb{Z}_{\mathbb{N}}^*$ such that $R + Tz^2 \in \mathbb{Z}_{\mathbb{N}}^*$.

$$Rx_j^2 + Ty_j^2 = R\left(\frac{-2zt}{R+Tz^2}\right)^2 + Ty_j^2 = \left(\frac{4SR}{(R+Tz^2)^2}\right)t^2 + Ty_j^2 = R\overline{x}_i^2 + Ty_j^2.$$
$$\textit{where } R = z^2 \textit{ and } \overline{x}_i = \frac{-2tr}{R+Tz^2}.$$

Since z is random in $\mathbb{Z}_{\mathbb{N}}^*$, $R = u^{\frac{|\mathbb{P}_\eta|-t_\eta}{2}} \prod_{i=1}^{n} b_{i,\eta} r_{i,\eta}$ and $u^{-1}R$ look mathematically random and hence $H(A_i) = u^a A_i = \prod_{i=1}^{n} b_{i,\eta} r_{i,\eta}^2$ looks also completely random in $\mathbb{Z}_{\mathbb{N}}^*$ for each bit. Thus,

$$|\Pr[W_6] = \Pr[W_5]|.$$

- Game-7, In this game, we replace the message $m_{(b)}$ by a random string $z \in_R \{-1, 1\}^l$ i.e., $c_j = z_j \cdot \left(\frac{r_j x_j + 1}{N}\right)$ and $\overline{c}_j = z_j \cdot \left(\frac{\overline{x}_j r_j + 1}{N}\right)$.
  We first prove that $(x_j r_j + 1)(-x_j r_j + 1)T_j \in QR(N)$.
  Proof. Let $f(x_j, r_j) = (x_j r_j + 1)$, then we have,

$$f(x_j, r_j)f(x_j, -r_j)T_j = (x_j r_j + 1)(-x_j r_j + 1)T_j,$$
$$f(x_j, r_j)f(x_j, -r_j)T_j = (1 - (x_j r_j)^2)T_j = (1 - x_j^2 R_j)T_j,$$
$$f(x_j, r_j)f(x_j, -r_j)T_j = (T_j y_i^2)T_j = (T_j y_j)^2 \in QR(N).$$

  Similarly, we can prove that $(\overline{x}_j r_j + 1)(-\overline{x}_j r_j + 1)T_j \in QR(N)$.
  Since $u^{-1}R_j, R_j \in QR(N)$, $T_j \in J(N) \setminus QR(N)$, $(x_j r_j + 1)(-x_j r_j + 1)T_j \in QR(N)$ and $(\overline{x}_j r_j + 1)(-\overline{x}_j r_j + 1)T_j \in QR(N)$ then Case 2 in Lemma 4.2 can be applied and the distribution of the Jacobi symbols $\left(\frac{x_j r_j + 1}{N}\right)$ and $\left(\frac{\overline{x}_j r_j + 1}{N}\right)$ are random in $\{\pm 1\}$. Thus, $\mathcal{A}$ will not be able to distinguish between Game-7 and Game-6. i.e.

$$|\Pr[W_7] = \Pr[W_6]|.$$

- Clearly in Game-7 we have,

$$|\Pr[W_7] = \Pr[W_7] = \frac{1}{2}|.$$

Combining all the previous equations proves Theorem 6.2.

6.3 AnonABSC

In this section, we explain how to implement an anonymous CP-ABSC (Anon-ABSC) which consists of four algorithms: Setup, KeyGeneration, Signcrypt and Unsigncrypt.

- The *Setup* and *KeyGeneration* algorithms are the same as BasicABSC.

- $(C) \leftarrow Signcrypt(m, params, \mathbb{A}_\sigma, \mathbb{P}_\sigma, \mathbb{P}_\eta, r_{i,\sigma})$. To signcrypt a message $m \in \{-1, 1\}^l$ where l is the message length, the sender checks based on his signature attribute set $\mathbb{A}_\sigma$ and the access structure of his signature $\mathbb{P}_\sigma$ which attributes are quadratic residue and which are not. Let t_σ be the number of attributes that are non-quadratic residue. Choose two random even values d_1, d_2 and a random value s. Calculate $S = s^{d_2}$, $U = u^{d_1}$ and $D = USu^{t_\sigma}$ and calculate $x_j, y_j, \alpha_j, \beta_j$, $j \in [0, l-1]$ such that these variables satisfy the following equations.

$$[x_j, y_j] = Rx_j^2 + T_j y_j^2 \equiv 1 \pmod{N}, \tag{6.3}$$

$$[\alpha_j, \beta_j] = u^{-1}\alpha_j^2 + T_j \beta_j^2 \equiv 1 \pmod{N}. \tag{6.4}$$

$$\text{Where } R = u^{|\mathbb{P}_\eta|} \prod_{i=1}^{n} b_{i,\eta} A_i,\ T_j = T^{2j+1} = D^{2j+1} \prod_{i=1}^{n} b_{i,\sigma} A_i^{2j+1}$$

The message $m = [m_0, m_1, ..., m_{l-1}]$ is signcrypted using the following formula.

$$c_j = m_j \cdot \left(\frac{2 + 2y_j t_j}{N}\right),\ k_j = \left(\frac{1 + \beta_j t_j}{N}.\right)$$

$$\text{Where } t_j = t^{2j+1} = (US)^{\frac{2j+1}{2}} \prod_{i=1}^{n} b_{i,\sigma} r_{i,\sigma}^{2j+1}$$

The ciphertext is $C = (D, k, c)$ where $c = [c_0, c_1, ..., c_{l-1}]$ and $k = [k_0, k_1, ..., k_{l-1}]$.

- $(m) \leftarrow Unsigncrypt(C, params, \mathbb{A}_\eta, \mathbb{P}_\sigma, \mathbb{P}_\eta, r_{i,\eta})$. First, the receiver checks that $\mathbb{P}_\eta \subseteq \mathbb{A}_\eta$. If $\mathbb{P}_\eta \subseteq \mathbb{A}_\eta$, then he finds t_η based on his access structure $\mathbb{P}_\eta$. Then he solves Equations 6.3 and 6.4 to get $x_j, y_j, \alpha_j, \beta_j$ and unsigncrypts the message as

follows.

$$m_j = c_j \cdot \left(\frac{x_j r + 1}{N}\right) \quad \text{if} \quad |\mathbb{P}_\eta| - t_\eta \text{ is even.}$$
$$m_j = c_j \cdot \left(\frac{\overline{r}_j + 1}{N}\right) \cdot k_j \quad \text{if} \quad |\mathbb{P}_\eta| - t_\eta \text{ is odd.}$$
$$r = u^{\frac{|\mathbb{P}_\eta|-t_\eta}{2}} \prod_{i=1}^{n} b_{i,\eta} r_{i,\eta}, \quad \overline{r}_j = u^{\frac{|\mathbb{P}_\eta|-t_\eta-1}{2}} x_j \alpha_j \prod_{i=1}^{n} b_{i,\eta} r_{i,\eta} + \beta_j y_j T_j$$

The Unsigncrypt process is illustrated in Figure 6.2.

6.3.1 Soundness

If $|\mathbb{P}_\eta| - t_\eta$ is even, the correctness of this system is exactly the same as that of BasicABSC. If $|\mathbb{P}_\eta| - t_\eta$ is odd then,

$$(\overline{r}_j + 1) \cdot (1 + \beta_j t_j) \cdot (2 y_j t_j + 2) = 2(\overline{r}_j + 1) \cdot (1 + \beta_j t_j + y_j t_j + \beta_j y_j T_j)$$
$$= 2 \left(1 + \frac{u^{\frac{|\mathbb{P}_\eta|-t_\eta-1}{2}} x_j \alpha_j \prod_{i=1}^{n} b_{i,\eta} r_{i,\eta}}{\beta_j y_j T_j + 1} \right) \cdot \left(1 + \frac{t_j(\beta_j + y_j)}{\beta_j y_j T_j + 1}\right) \cdot (\beta_j y_j T_j + 1)^2$$
$$= 2(1 + \overline{x}_j u^{\frac{|\mathbb{P}_\eta|-t_\eta-1}{2}} \prod_{i=1}^{n} b_{i,\eta} r_{i,\eta})(1 + \overline{y}_j t_j) \cdot (\beta_j y_j T_j + 1)^2$$

where $\overline{x}_j = \dfrac{\alpha_j x_j}{\beta_j y_j T_j + 1}, \quad \overline{y}_j = \dfrac{\beta_j + y_j}{\beta_j y_j T_j + 1}.$

Based on Lemma 2.1, we can see that $[\overline{x}_j, \overline{y}_j]$ is a valid solution to

$u^{-1} R \overline{x}_j^2 + T_j \overline{y}_j^2 \equiv 1 \pmod{N}$.

$$2(1 + \overline{x}_j u^{\frac{|\mathbb{P}_\eta|-t_\eta-1}{2}} \prod_{i=1}^{n} b_{i,\eta} r_{i,\eta})(1 + \overline{y}_j t_j) \cdot (\beta_j y_j T_j + 1)^2 \in QR(N),$$

$$\left(\frac{1 + \overline{x}_j u^{\frac{|\mathbb{P}_\eta|-t_\eta-1}{2}} \prod_{i=1}^{n} b_{i,\eta} r_{i,\eta}}{N} \right) \cdot \left(\frac{2 + 2\overline{y}_j t_j}{N}\right) = 1.$$

6.3.2 AnonABSC Security

The security of AnonABSC is based on the proof of the following two theorems.

Theorem 6.3. *Suppose the quadratic residuosity assumption holds for RSAgen and F is a secure PRF. Then the proposed AnonABSC is anonymous indistinguishable against adaptive chosen plaintext attack (Anon-IND-ABSC-CPA) in the random*

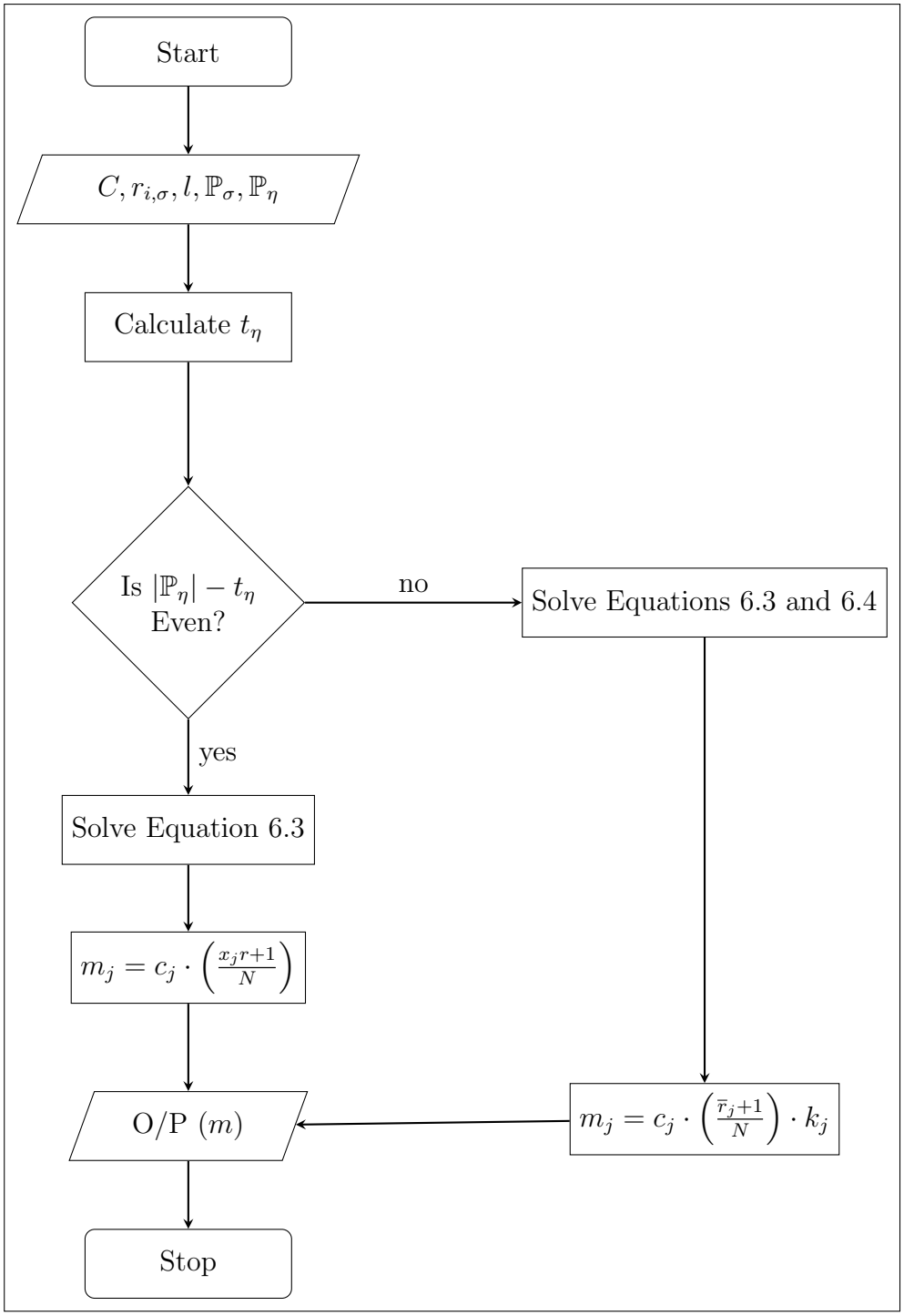

Figure 6.2: Flaw Chart of The Unsigncrypt Process of AnonABSC

oracle model based on the QR assumption. In particular, suppose $\mathcal{A}$ is an efficient Anon-IND-ABSC-CPA adversary, then there exist efficient algorithms B_1, B_2 whose running time is the same as that of $\mathcal{A}$ such that,

$$ABSCAdv_{\mathcal{A},AnonABSC}(\lambda) \leq 2QRAdv_{B_2,RSAgen}(\lambda) + PRFAdv_{B_1,F}(\lambda).$$

Theorem 6.4. *Suppose the quadratic residuosity assumption holds for RSAgen and F is a secure PRF. Then the proposed AnonABSC is existentially unforgeable against chosen-message attack (EUF-ABSC-SMA) in the random oracle model based on the QR assumption. In particular, suppose $\mathcal{A}$ is an efficient EUF-ABSC-SMA adversary, then there exist efficient algorithms B_1, B_2 whose running time is the same as that of $\mathcal{A}$ such that,*

$$ABSCAdv_{\mathcal{A},AnonABSC}(\lambda) \leq 2QRAdv_{B_2,RSAgen}(\lambda) + PRFAdv_{B_1,F}(\lambda).$$

Theorem 6.3 proves the security of AnonABSC for message confidentiality and Theorem 6.4 proves the security of AnonABSC for ciphertext unforgeability.

- **Security Proof for Message Confidentiality**
  We define a sequence of games and let W_i represents the winning of the i_{th} game by the adversary $\mathcal{A}$. These games are defined as follows.

  Game-0.This game is the usual adversarial game.
  Game-1.This game replaces the PRF F with a truly random function.
  Game-2.This game explains how to simulate the hash function H.
  Game-3.This game explains how to respond to a Signcrypt query from $\mathcal{A}$.
  Game-4.This game sets $u \in QR(N)$.
  Game-5.This game sets $u^{-1}R, R \in J(N) \setminus QR(N)$ in the challenge phase.
  Game-6.This game sets T_j randomly for each bit.
  Game-7 replaces the message m with a random number z.

- Game-0. This is the usual adversarial game for defining the Anon-IND-ABSC-CPA security of ABSC protocols. The challenger picks the random oracle $H : A_i \rightarrow J(N)$ at random from the set of all such functions in the *Setup* algorithm and allows $\mathcal{A}$ to query H at arbitrary points. Thus, we have,

$$|\Pr[W_0] - \frac{1}{2}| = ABSCAdv_{\mathcal{A},AnonABSC}(\lambda).$$

- Game-1. This is the same as Game-0, with the following change. In the *Setup* algorithm, instead of using a PRF F to respond to $\mathcal{A}$'s private key queries, we use a truly random function $f : A_i \rightarrow \{0, 1, 2, 3\}$. If F is a secure PRF, $\mathcal{A}$ will not

notice the difference between Game-0 and Game-1. In particular, there exists an algorithm B_1 (whose running time is about the same as that of $\mathcal{A}$) such that,

$$|\Pr[W_1] - \Pr[W_0]| = PRFAdv_{B_1,F}(\lambda).$$

- Game-2. (N, u, H) are the public parameters *params* given to $\mathcal{A}$ in the previous game where u is uniform in $J(N) \setminus QR(N)$ and the random oracle H is a random function $H : A_i \to J(N)$. We make the following change in the random oracle H in this game. The challenger responds to a query to $H(A_i)$ by picking $a \in_R \{0, 1\}$ and $v \in_R \mathbb{Z}_{\mathbb{N}}$ and setting $H(A_i) = u^a v^2$. Thus the challenger implements a random function $H : A_i \to J(N)$ as in the previous game. The challenger responds to a private key query as follows.

  Suppose $H(A_i) = u^a v^2$ for some $a \in_R \{0, 1\}$ and $v \in_R \mathbb{Z}_{\mathbb{N}}$. The challenger responds to a private key query for A_i by setting either $H(A_i)^{\frac{1}{2}} = v$ (when $a = 0$) or $(uH(A_i))^{\frac{1}{2}} = uv$ (when $a = 1$). Since v is uniform in $\mathbb{Z}_{\mathbb{N}}$, this will produce a square root of $H(A_i)$ or $uH(A_i)$ which is also uniform among the four square roots, as in the previous game. Thus, $\mathcal{A}$'s views in Game-1 and Game-2 are identical and therefore,

  $$|\Pr[W_2] = \Pr[W_1]|.$$

- Game-3. We explain, in this game, how the challenger answers a Signcrypt query from $\mathcal{A}$ for a given message m, the attribute sets of both signature and encryption $\mathbb{A}_\sigma, \mathbb{A}_\eta$ and the access structures for both sender and receiver $\mathbb{P}_\sigma, \mathbb{P}_\eta$.

  - He sets $u^{t_\eta} \prod_{i=1}^{n} b_{i,\eta} A_i \in QR(N)$. (*)
  - He chooses two random even values d_1, d_2 and a random value s and calculates $D = u^{d_1 + t_\sigma} s^{d_2}$ as in Signcrypt.
  - He chooses $k_j \in_R \{\pm 1\}$.
  - He sets $C = Signcrypt(m, params, \mathbb{A}_\sigma, \mathbb{P}_\sigma, \mathbb{P}_\eta, r_{i,\sigma})$.
  - He sends (D, k, c) to $\mathcal{A}$.

  We prove that this game has the same distribution for (D, k, c) as the real *Signcrypt* of Game-2.

  We first prove that $(1 + \beta_j t_j) \cdot (1 - \beta_j t_j) u^{-1} \in QR(N)$.

Proof. Let $g(\beta_j, t_j) = k_j$, then we have,

$$g(\beta_j, t_j)g(\beta_j, -t_j)u^{-1} = (1 + \beta_j t_j)(1 - \beta_j t_j)u^{-1},$$
$$g(\beta_j, t_j)g(\beta_j, -t_j)u^{-1} = (1 - (\beta_j t_j)^2)u^{-1},$$
$$g(\beta_j, t_j)g(\beta_j, -t_j)u^{-1} = (u^{-1}\alpha_j)^2 \in QR(N).$$

Since $T_j = t_j^2 = D^{2j+1}\prod_{i=1}^{n} b_{i,\sigma}A_i^{2j+1} \in QR(N)$ and $u^{-1} \in J(N) \setminus QR(N)$ then Case 1 in Lemma 4.2 can be applied and the distribution of the Jacobi symbols k_j are random in $\{\pm 1\}$. Thus,

$$|\Pr[W_3] = \Pr[W_2]|.$$

- Game-4. In this game, the challenger chooses u uniformly in $QR(N)$ instead of $J(N) \setminus QR(N)$ i.e. $u^{-1}R, R \in QR(N)$. Since this is the only change between Game-4 and Game-3, $\mathcal{A}$ will not notice the difference assuming that the QR assumption holds for RSAgen. In particular, there exists an algorithm B_2 (whose running time is about the same as that of $\mathcal{A}$) such that,

$$|\Pr[W_4] - \Pr[W_3]| = QRAdv_{B_2,RSAgen}(\lambda).$$

- Game-5. In this game, we show how to simulate the challenge phase. Upon receiving two different messages m_0, m_1, two different encryption attribute sets $\mathbb{A}^*_{1,\eta}$, $\mathbb{A}^*_{2,\eta}$, a signature attribute set $\mathbb{A}^*_\sigma$ and two challenge access structures for both sender and receiver $\mathbb{P}^*_\sigma, \mathbb{P}^*_\eta$, the challenger tosses two fair coins $(b, \bar{b}) \in \{0,1\}^2$ and calculates $C^* = Signcrypt(m^*_b, params, \mathbb{A}^*_{\bar{b},\eta}, \mathbb{A}^*_\sigma, \mathbb{P}^*_\sigma, \mathbb{P}^*_\eta)$. But with exception of replacing the line (*) in Game-3 with the following.

  – He sets $u^{t_\eta}\prod_{i=1}^{n} b_{i,\eta}A_i \in J(N) \setminus QR(N)$. (*)

  i.e. $u^{-1}R, R \in J(N) \setminus QR(N)$. Since the only difference between Game-5 and Game-4 is that $u^{-1}R, R \in J(N) \setminus QR(N)$ instead of $u^{-1}R, R \in QR(N)$, $\mathcal{A}$ will not notice the difference assuming that the QR assumption holds for RSAgen. In particular, there exists an algorithm B_2 (whose running time is about the same as that of $\mathcal{A}$) such that,

$$|\Pr[W_5] - \Pr[W_4]| = QRAdv_{B_2,RSAgen}(\lambda).$$

- Game-6. In this game, we replace $T_j = t^{2j+1}$ with randomly independent values of $T_j = t_j^2$, $t_j \in_R \mathbb{Z}_\mathbb{N}$ by generating U_j, S_j and $r_{i,j,\sigma}$ for each bit. i.e. $c_j = m_j \cdot \left(\frac{2+2y_j t_j}{N}\right)$

where $t_j = U_j S_j \prod_{i=1}^{n} b_{i,\sigma} r_{i,j,\sigma}$. Based on Lemma 6.1, $\mathcal{A}$ will not be able to distinguish between Game-6 and Game-5. i.e.

$$|\Pr[W_6] = \Pr[W_5]|.$$

- Game-7. In this game, we replace the message $m_{(b)}$ by a random string $z \in_R \{-1, 1\}^l$ i.e., $c_j = z_j \cdot \left(\frac{2+2y_j t_j}{N}\right)$. Since $T_j \in QR(N)$, $u^{-1}R, R \in J(N) \setminus QR(N)$ and $(2y_j t_j + 2)(-2y_j t_j + 2)u^a R \in QR(N)$ (which can be proven similar to Game-3) then Case 1 in Lemma 4.2 can be applied and the distribution of the Jacobi symbols $\left(\frac{2y_j t_j + 2}{N}\right)$ are random in $\{\pm 1\}$. Thus, $\mathcal{A}$ will not be able to distinguish between Game-7 and Game-6. i.e.

$$|\Pr[W_7] = \Pr[W_6]|.$$

- End. Clearly in Game-7 we have,

$$\Pr[W_7] = \frac{1}{2}|.$$

Combining all the previous equations proves Theorem 6.3.

- **Security Proof for Ciphertext Unforgeability**
We define a sequence of games and let W_i represents the winning of the i_{th} game by the adversary $\mathcal{A}$. These games are defined as follows.

Game-0.This game is the usual adversarial game.
Game-1.This game replaces the PRF F with a truly random function.
Game-2.This game explains how to simulate the hash function H.
Game-3.This game explains how to respond to a signcrypt query from $\mathcal{A}$ using Unsigncrypt algorithm.
Game-4.This game sets $u \in QR(N)$.
Game-5.This game sets $T_j \in J(N) \setminus QR(N)$.
Game-6.This game sets $H(A_i)$ for each bit.
Game-7 replaces the message m with a random number z.

- Game-0. This is the usual adversarial game for defining the EUF-ABSC-SMA security of ABSC protocols. The challenger picks the random oracle $H : A_i \rightarrow J(N)$ at random from the set of all such functions in the *Setup* algorithm and allows $\mathcal{A}$ to query H at arbitrary points. Thus, we have,

$$|\Pr[W_0] - \frac{1}{2}| = ABSCAdv_{\mathcal{A},AnonABSC}(\lambda).$$

- Game-1. This is the same as Game-0, with the following change. In the *Setup* algorithm, instead of using a PRF F to respond to $\mathcal{A}$'s private key queries, we use a truly random function $f : A_i \to \{0, 1, 2, 3\}$. If F is a secure PRF, $\mathcal{A}$ will not notice the difference between Game-0 and Game-1. In particular, there exists an algorithm B_1 (whose running time is about the same as that of $\mathcal{A}$) such that,

$$|\Pr[W_1] - \Pr[W_0]| = PRFAdv_{B_1,F}(\lambda).$$

- Game-2. (N, u, H) are the public parameters *params* given to $\mathcal{A}$ in the previous game where u is uniform in $J(N) \setminus QR(N)$ and the random oracle H is a random function $H : A_i \to J(N)$. We make the following change in the random oracle H in this game. The challenger responds to a query to $H(A_i)$ by picking $a \in_R \{0, 1\}$ and $v \in_R \mathbb{Z}_{\mathbb{N}}$ and setting $H(A_i) = u^a v^2$. Thus the challenger implements a random function $H : A_i \to J(N)$ as in the previous game. The challenger responds to a private key query as follows.

  Suppose $H(A_i) = u^a v^2$ for some $a \in_R \{0, 1\}$ and $v \in_R \mathbb{Z}_{\mathbb{N}}$. The challenger responds to a private key query for A_i by setting either $H(A_i)^{\frac{1}{2}} = v$ (when $a = 0$) or $(uH(A_i))^{\frac{1}{2}} = uv$ (when $a = 1$). Since v is uniform in $\mathbb{Z}_{\mathbb{N}}$, this will produce a square root of $H(A_i)$ or $uH(A_i)$ which is also uniform among the four square roots, as in the previous game. Thus, $\mathcal{A}$'s views in Game-1 and Game-2 are identical and therefore,

$$|\Pr[W_2] = \Pr[W_1]|.$$

- Game-3. We explain, in this game, how the challenger answers a Signcrypt query from $\mathcal{A}$ for a given message m.
  - He sets $u^{t_\eta} \prod_{i=1}^{n} b_{i,\eta} A_i \in QR(N)$.
  - He chooses two random even values d_1, d_2 and a random value s and calculates $D = u^{d_1 + t_\sigma} s^{d_2}$ as in Signcrypt. (*)
  - He chooses $k_j \in_R \{\pm 1\}$.
  - He sets (C)= Unsigncrypt$((D, k_j, m), params, \mathbb{A}_\eta, \mathbb{P}_\eta, \mathbb{P}_\sigma)$.
  - He sends (D, k, c) to $\mathcal{A}$.

  We prove in Game-3 of the message confidentiality security proof that k_j has a random distribution in $\{\pm 1\}$. In addition, It is easy to see that (D, k, c) is the unique signcryption of m. Therefore, (D, k, c) of Game-3 is the same as in Game-2. Thus,

$$|\Pr[W_3] = \Pr[W_2]|.$$

- Game-4. In this game, the challenger chooses u uniformly in $QR(N)$ instead of $J(N) \setminus QR(N)$. i.e. $u^{-1}R, R \in QR(N)$. Since this is the only change between Game-4 and Game-3, $\mathcal{A}$ will not notice the difference assuming that the QR assumption holds for RSAgen. In particular, there exists an algorithm B_2 (whose running time is about the same as that of $\mathcal{A}$) such that,

$$|\Pr[W_4] - \Pr[W_3]| = QRAdv_{B_2,RSAgen}(\lambda).$$

- Game-5. In this game, we replace the line (*) in Game-4 with the following.

  – He chooses a random value D such that $T_j \in J(N) \setminus QR(N)$.(*)

  Since the only difference between Game-5 and Game-4 is that $T_j \in J(N) \setminus QR(N)$ instead of $T_j \in QR(N)$, $\mathcal{A}$ will not notice the difference assuming that the QR assumption holds for RSAgen. In particular, there exists an algorithm B_2 (whose running time is about the same as that of $\mathcal{A}$) such that,

$$|\Pr[W_5] - \Pr[W_4]| = QRAdv_{B_2,RSAgen}(\lambda).$$

- Game-6. In this game, we hash the attributes A_i to a different value $H(A_i, j) = u^a A_{i,j}$ for each bit so that $r_j, \overline{r}_j$ are random for each bit. This game can be proven as Game-6 of the Ciphertext Unforgeability of BaiscABSC. Thus,

$$|\Pr[W_6] = \Pr[W_5]|.$$

- Game-7. In this game, we replace the message $m_{(b)}$ by a random string $z \in_R \{-1, 1\}^l$ i.e.,

$$c_j = z_j \cdot \left(\frac{r_j x_j + 1}{N}\right) \quad \text{if } |\mathbb{P}_\eta| - t_\eta \text{ is even}$$
$$c_j = z_j \cdot \left(\frac{\overline{r}_j + 1}{N}\right) \cdot k_j \quad \text{if } |\mathbb{P}_\eta| - t_\eta \text{ is odd.}$$

  We can see that $(x_j r_j + 1)(-x_j r_j + 1)T_j \in QR(N)$ if $|\mathbb{P}_\eta| - t_\eta$ is even. We now

prove that, $(\overline{r}_j + 1)(-\overline{r}_j + 1)T_j \in QR(N)$ if $|\mathbb{P}_\eta| - t_\eta$ is odd.

Proof. Let $\overline{f}(x_j, r_j) = \overline{r}_j + 1 = (u^{\frac{|\mathbb{P}_\eta|-t_\eta-1}{2}} x_j \alpha_j \prod_{i=1}^{n} b_{i,\eta} r_{i,\eta} + \beta_j y_j T_j + 1)$.

$\overline{f}(x_j, r_j)\overline{f}(x_j, -r_j)T_j = (\overline{r}_j + 1)(-\overline{r}_j + 1)T_j =$

$(u^{\frac{|\mathbb{P}_\eta|-t_\eta-1}{2}} x_j \alpha_j \prod_{i=1}^{n} b_{i,\eta} r_{i,\eta} + \beta_j y_j T_j + 1)(-u^{\frac{|\mathbb{P}_\eta|-t_\eta-1}{2}} x_j \alpha_j \prod_{i=1}^{n} b_{i,\eta} r_{i,\eta} + \beta_j y_j T_j + 1)T_j,$

$= (\overline{x}_j r_j + 1)(-\overline{x}_j r_j + 1)(1 + T_j y_j \beta_j)^2 T_j,$

where $\overline{x}_j = \dfrac{\alpha_j x_j}{1 + T_j y_j \beta_j}$.

We can see that $(\overline{x}_j r_j + 1)(-\overline{x}_j r_j + 1)T_j \in QR(N)$ if $|\mathbb{P}_\eta| - t_\eta$ is odd.

Since $u^{-1}R, R \in QR(N)$, $T_j \in J(N) \setminus QR(N)$ and $f(x_j, r_j)f(x_j, -r_j)T_j \in QR(N)$ if $|\mathbb{P}_\eta| - t_\eta$ is even and $\overline{f}(x_j, r_j)\overline{f}(x_j, -r_j)T_j \in QR(N)$ if $|\mathbb{P}_\eta| - t_\eta$ is odd. Then Case 2 in Lemma 4.2 can be applied and the distribution of both Jacobi symbols $\left(\frac{x_j r_j + 1}{N}\right)$ and $\left(\frac{\overline{r}_j + 1}{N}\right)$ are random in $\{\pm 1\}$. Thus, $\mathcal{A}$ will not be able to distinguish between Game-7 and Game-6. i.e.

$$|\Pr[W_7] = \Pr[W_6]|.$$

- End. Clearly in Game-7 we have,

$$\Pr[W_7] = \frac{1}{2}|.$$

Combining all the previous equations proves Theorem 6.4.

6.4 Space-Time Tradeoff

In this section, we present a trade-off between the time and the ciphertext length of the proposed systems. For AnonABSC, instead of sending D along with c and k as the full ciphertext C, the sender sends $C = (D, x_0, y_0, \alpha_0, \beta_0, c, k)$. Thus, he can solve equations on the form $Rx^2 + Ty^2 \equiv 1 \pmod{N}$ using only one inversion in $\mathbb{Z}_\mathbb{N}$. This results in high signcryption speed. In the unsigncryption process, the receiver does not have to solve any equations and he can generate $x_j, y_j, \alpha_j, \beta_j$ using Lemma 2.1. This, of course, comes at the cost of sending four more element in $\mathbb{Z}_\mathbb{N}$. The same concept can be applied with BasicABSC with the cost of only one element in $\mathbb{Z}_\mathbb{N}$ by sending $C = (x_0, \overline{x}_0, c, \overline{c})$ as the ciphertext.

6.5 Conclusion

This chapter presents two ciphertext-policy attribute-based signcryption systems (CP-ABSC) that signcrypts data in a more efficient way than individually encrypting and signing data. In addition, the proposed AnonABSC system preserves the privacy of the encryption attributes (i.e. anonymous). We construct these systems without pairing and hence, it is time- and power-efficient. They are full secure in the random oracle model based on the QR assumption. The proposed systems have a constant ciphertext size regardless of the size of the access structure.

Chapter 7

A Resilient Identity-based Authenticated Key Exchange

7.1 Introduction

Key exchange (KE) protocols are cryptographic tools that allow two or more parties to securely share a common secret via insecure or public networks such as the Internet. They are considered the cornerstones of establishing any secure communication channels. In the last three decades, KE protocols have been significantly designed and analysed for different network settings. Diffie-Hellman key exchange protocol (DH, for short) is the first and best-known key agreement protocol [DH76]. The security of this protocol is based on the computational Diffie-Hellman assumption. Unfortunately, this protocol was breakable because the links between the parties are not authenticated, and a man-in the-middle attack can be launched against the DH protocol.

Authenticated key exchange (AKE) protocols permit a group of parties within a huge and fully insecure public network to form a shared secret key and guarantees each party that no other party apart from these parties can get that key. Moreover, AKE protocols are made to ensure that the designated parties are sharing this secret key with each other. This security property is called explicit key authentication and the protocol is said to be authenticated key agreement with key confirmation (AKC) protocol. Over the past few years, some security properties have been seen to be important in key agreement protocols and different protocols have been implemented to solve the problem. Examples of these protocols are [ABB+04, BPR00, BR93, BR95, BCNP08, CK01, ISO09a, Oka07, YDW+11, YWWD08]. A comprehensive survey of KE protocols is presented in [DB05].

The concept of identity-based encryption was extended to AKE protocols to generate identity-based authenticated key exchange protocols (IBAKE). Smart [Sma01] presented a two-pass IBAKE based on Weil pairings and merges the ideas of Boneh and Franklin [BF01] with the tripartite DH protocol of Joux [Jou04]. McCullagh and Barreto [MB05] presented an IBAKE that is inspired on an identity-based key pair derivation algorithm first proposed by Sakai and Kasahara [SK03]. Their protocol has the advantage of running on escrow or escrowless mode, and is also based on pairings operations.

In this chapter, we present a security notion of KE protocols called resiliency. It

measures the ability of a KE protocol to maintain the security of its session even if an adversary was able to obtain the shared secret during this session. A KE protocol can withstand such devastating attack if it can generate a new shared secret between the respective parties without the need to setup a new session between these parties. Until now, there is no KE protocol that can withstand such attack. We present the first IBAKE that securely share a multiple shared secrets between two parties P_1, P_2 instead of only generating a shared secret. This has two useful applications. First, If a session key between two parties P_1 and P_2 is exposed, they can generate another shared secret without the need to establish a new session. Second. It allows multi-key generation of arbitrary different lengths for different purposes (email and credit cards, for instance) in one session. The proposed KE protocol is also time- and power-efficient compared to other AKE protocols. It does not use expensive-computational operations such as pairing like [VLYK10] or even a prime modular exponentiation such as the ISO/IEC 11770-3 standard [ISO09b].

- **Remarks.** We note here that the notion of resiliency in KE protocols should not be confused with leakage-resilient key exchange [YMSW13]. The notion of leakage resilience defines the KE security in the case of leaked information of the private key or ephemeral key, while the notion of resiliency in KE protocols defines the ability of a session to maintain its security even if the shared secret during this session is completely leaked.

- On the first glance, a resilient KE can be considered as a multiple key exchange [HL01] in terms of that both protocols can share multiple keys within a session. But the major difference between the two is that, if any shared secret in multiple key exchange protocol session is compromised, the other keys will be no longer secure, while resilient KE must maintain its security even if a shared secret key is leaked.

The rest of the chapter is organised as follows. Section. 7.2 explains the resiliency property and redefines the CK model to achieve this security property. Section. 7.3 explains the construction of the proposed IBAKE. Section. 7.4 presents the security proof of the proposed IBAKE. Then, we present an efficiency evaluation of the proposed IBAKE in Section. 7.5. Then we conclude the chapter in Section. 7.6.

7.2 Resiliency

Let π be a KE protocol that shares a secret SSK_w between parties $P_1, ..., P_n$ where n is the number of parties and w is the number of previously shared secrets within

a session between these parties. If this secret is compromised by an adversary $\mathcal{U}$, the corresponding parties can safely generate another secret SSK_{w+1} without the need to exchange information or establish a new session. Based on the above, the CK-Security with resiliency can be defined as follows.

Definition 7.1. *CK-Security with resiliency. A KE protocol π is CK-secure with resiliency against a UM adversary if the following properties hold.*

- *If the protocol π is executed correctly, all parties participating in this protocol must share the same secret key SSK, and they can generate other secret keys SSK_w without the need to share any other information or establish a new session.*
- *The probability that the adversary $\mathcal{U}$ successfully distinguishes between a shared secret SSK_w from a random value is no more than 1/2 plus a negligible fraction in the security parameter even it was given the previously shared secrets $SSK_1, ..., SSK_{w-1}$.*

This can be simulated by $\mathcal{U}$ obtaining shared secrets $SSK_1, ..., SSK_{w-1}$ stored in the memory of any of the corresponding parties. The leakage of these shared secrets can be in the form of cryptanalysis, unauthorised access to a party's memory, careless storage of the shared secret, etc. As far as we know, no KE can achieve such property because the main focus in the literature is to share a secret without investigating how KE protocols can adapt if the shared secret is compromised.

We now modify the UM adversary so that it can capture the resiliency property as follows.

Resiliency query. Upon request, the adversary $\mathcal{U}$ gets the session key of a complete unexpired session of a party P. P outputs to the other parties that this session-key is exposed.

Test-session*. We modify the test session of the U adversary in [CK01]. $\mathcal{D}$ chooses a random number w. He generates $SSK_0, ..., SSK_{w-1}$ and sends it to the adversary. After that it tosses a fair coin $b \in \{0, 1\}$ and sends SSK_w to $\mathcal{U}$ if $b = 1$ and sends a random number if $b = 0$.

7.3 The Proposed IBAKE

The proposed IBAKE operates as follows.

- $(params) \leftarrow Setup(\lambda)$. Using RSAgen($\lambda$), generate ($p$, q), calculate the modulus $N \leftarrow pq$, choose $u \in J(N) \setminus QR(N)$, and choose a hash function $H : ID \rightarrow J(N)$. The public parameters $params$ are $[N, u, H]$. The master secret MS parameters are p, q and a secret key K for a pseudorandom function (PRF) $F_K : ID \rightarrow [0, 1, 2, 3]$.

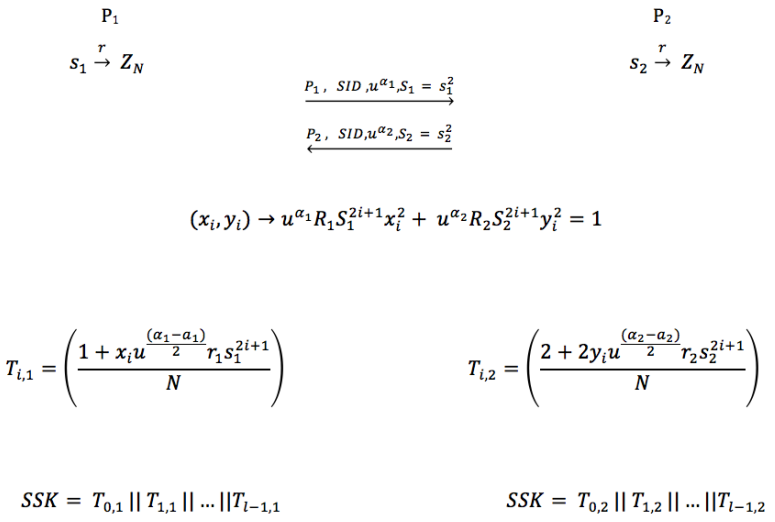

Figure 7.1: IBAKE Interaction

- $(r) \leftarrow Extract(MS, ID)$. Calculate $R \leftarrow H(ID) \in J(N)$ and $w \leftarrow F_K(ID) \in \{0, 1, 2, 3\}$. Choose $a \in \{0, 1\}$ such that $u^a R \in QR(N)$. Let $[z_0, z_1, z_2, z_3]$ be the four square roots of $u^a R \in \mathbb{Z}_{\mathbb{N}}$, then $r \leftarrow z_w$.

- $(SSK) \leftarrow KeyExchange(ID_1, ID_2, SID)$. First, the initiator P_1 on input of his identity ID_1, the other party's identity ID_2 and a session identifier SID chooses two random values $s_1, \alpha_1 \in \mathbb{Z}_{\mathbb{N}}$ such that $u^{\alpha_1} R_1 \in QR(N)$ and sends $(ID_1, SID, u^{\alpha_1}, S_1 = s_1^2)$ to P_2. Upon receipt of $(ID_1, SID, u^{\alpha_1}, S_1 = s_1^2)$ from P_1, P_2 chooses two random value $s_2, \alpha_2 \in \mathbb{Z}_{\mathbb{N}}$ such that $u^{\alpha_2} R_2 \in QR(N)$ and sends $(ID_2, SID, u^{\alpha_2}, S_2 = s_2^2)$ to P_1. After that, P_1 and P_2 solve the following equations.

$$(x_i, y_i) \leftarrow u^{\alpha_1} R_1 S_1^{2i+1} x_i^2 + u^{\alpha_2} R_2 S_2^{2i+1} y_i^2 \equiv 1 \pmod{N}, \tag{7.1}$$

  where i is the bit index. Equation 7.1 can be solved as explained in [BGH07]. After that, P_1 and P_2 calculate $T_i = \left(\frac{1+u^{\frac{\alpha_1 - a_1}{2}} x_i r_1 s_1^{2i+1}}{N} \right) = \left(\frac{2+2u^{\frac{\alpha_2 - a_2}{2}} y_i r_2 s_2^{2i+1}}{N} \right)$ respectively. P_1 and P_2 can now generate $SSK = T_0 \| T_1 \| ... \| T_{l-1}$. After successfully sharing SSK between P_1 and P_2, they can now generate multiple session keys SSK_w with arbitrary different lengths. The interaction between the P_1 and P_2 is shown in Figure 7.1.

7.3.1 IBAKE Product Formula

Each user has to solve l equations in the form of $Ax_i^2 + By_i^2 \equiv 1 \pmod{N}$ to share a secret SSK of length l by computing $x_i, y_i, \in \mathbb{Z}_{\mathbb{N}}$.

We present a variant of Lemma 2.1 suitable for solving the IBAKE equations.

Lemma 7.1. *For $i = 1, 2$ let (x_i, y_i) be a solution to $A_i x^2 + B_1 y^2 \equiv 1 \pmod N$. Then (x_3, y_3) is a solution to*

$$A_1 A_2 x^2 + B_1 B_2^j y^2 \equiv 1 \pmod N, \tag{7.2}$$

where $x_3 = \frac{x_1 x_2}{B_1 y_1 y_2 + 1}$ and $y_3 = \frac{y_1 + y_2}{B_2^{j/2}(B_1 y_1 y_2 + 1)}$.

Proof. Rewrite Equation 7.2 to be $A_1 A_2 x^2 + B_1 (B_2^{j/2} y)^2 \equiv 1 \pmod N$ and apply Lemma 2.1 to get x_3, y_3.

P solves the equations $u^{\alpha_1} R_1 S_1^{2i+1} x_i^2 + u^{\alpha_2} R_2 S_2^{2i+1} y_i^2 \equiv 1 \pmod N$ as follows. First, it solves the equations $u^{a_1} R_1 S_1 x_0^2 + u^{\alpha_2} R_2 S_2 y_0^2 \equiv 1 \pmod N$ and $S_1^2 x^2 + u^{\alpha_2} R_2 S_2 y^2 \equiv 1 \pmod N$ to get x_0, y_0, x, y respectively. Then, it applies Lemma 7.1 to solve $u^{a_1} R_1 S_1^3 x_1^2 + u^{\alpha_2} R_2 S_2^3 y_1^2 \equiv 1 \pmod N$ to get x_1, y_1. It solves the rest of the equations $u^{a_1} R_1 S_1^{2i+1} x_i^2 + R_2 S_2^{2i+1} y_i^2 \equiv 1 \pmod N$ to get (x_i, y_i) by using (x_{i-1}, y_{i-1}, x, y).

7.4 The Proposed IBAKE Security

The first property is the correctness of IBAKE which is proven as follows.

Correctness. As in [BGH07], it is easy to prove that.

$$\begin{aligned}
&(u^{\frac{\alpha_1 - a_1}{2}} r_1 s_1^{2i+1} x_i + 1) \cdot (2u^{\frac{\alpha_2 - a_2}{2}} r_2 s_2^{2i+1} y_i + 2) = 2u^{\frac{\alpha_1 - a_1}{2}} r_1 u^{\frac{\alpha_2 - a_2}{2}} r_2 s_1^{2i+1} s_2^{2i+1} x_i y_i \\
&+ 2u^{\frac{\alpha_1 - a_1}{2}} r_1 s_1^{2i+1} x_i + 2u^{\frac{\alpha_2 - a_2}{2}} r_2 s_2^{2i+1} y_i + 2 + (u^{\alpha_1} R_1 S_1^{2i+1} x_i^2 + u^{\alpha_2} R_2 S_2^{2i+1} y_i^2 - 1) \\
&= (u^{\frac{\alpha_1 - a_1}{2}} r_1 s_1^{2i+1} x_i + u^{\frac{\alpha_2 - a_2}{2}} r_2 s_2^{2i+1} y_i + 1)^2, \\
&\left(\frac{u^{\frac{\alpha_1 - a_1}{2}} r_1 s_1^{2i+1} x_i + 1}{N}\right) \cdot \left(\frac{2u^{\frac{\alpha_2 - a_2}{2}} r_2 s_2^{2i+1} y_i + 2}{N}\right) = 1, \\
&\left(\frac{u^{\frac{\alpha_1 - a_1}{2}} r_1 s_1^{2i+1} x_i + 1}{N}\right) = \left(\frac{2u^{\frac{\alpha_2 - a_2}{2}} r_2 s_2^{2i+1} y_i + 2}{N}\right).
\end{aligned}$$

We now present Theorem 7.1 to prove that the second property of CK-Security holds for IBAKE.

Theorem 7.1. *Suppose the quadratic residuosity assumption holds for RSAgen and F is a secure PRF. Then the proposed IBAKE protocol is CK-secure with resiliency under the unauthenticated-links adversarial model (UM) if H is modelled as a random oracle. In particular, suppose $\mathcal{U}$ is an efficient UM adversary, then there exist efficient algorithms Q_1, Q_2 whose running time is the same as that of $\mathcal{U}$ such that,*

$$SKAdv_{\mathcal{U},IBAKE}(\lambda) \leq 2QRAdv_{Q_2,RSAgen}(\lambda) + PRFAdv_{Q_1,F}(\lambda). \tag{7.3}$$

Security Proof. We first prove the CK-security with resiliency against an AM adversary $\mathcal{A}$, then we make it secure against a UM adversary using authenticators. Assume to the contrary that there is an AM adversary $\mathcal{A}$ against the IBAKE protocol that has non-negligible advantage in guessing correctly whether the response to a test-query is real or random. We construct out of this attacker an algorithm $\mathcal{D}$ that distinguishes between the two sets QR(N) and $J(N) \setminus QR(N)$ with non-negligible probability, reaching a contradiction with the quadratic residuosity problem. The input to $\mathcal{D}$ is denoted by $(P_1, ..., P_n, H, N, u, u^{\alpha_1^*}, u^{\alpha_2^*}, S_1^*, S_2^*, SSK_w^*)$. Let l be an upper bound on the number of sessions invoked by $\mathcal{A}$ in any interaction. $\mathcal{D}$ plays an adversarial game with $\mathcal{A}$ to solve the quadratic residuosity problem. We defines two sequences of games and let W_i represents the winning of the i_{th} game and $\overline{W}_i$ represents the winning of the $\bar{i}_{th}$ game by the adversary $\mathcal{A}$. The security proof can be proved in two ways, Proof 1 and Proof 2. Both proofs have in common the games from **Game-0** to **Game-5** and **Game-9**. **Game-6** to **Game-8** belongs to Proof 1 and **Game-**$\overline{6}$ to **Game-**$\overline{8}$ belongs to Proof 2. Any of these proofs can prove the security of the proposed IBAKE. The structure of these proofs is illustrated in Figure 7.2.

These games are defined as follows.

- **Game-0** is the usual adversarial game.
- **Game-1** replaces the PRF F with a truly random function.
- **Game-2** explains how to simulate the hash function H.
- **Game-3** shows how $\mathcal{A}$ interacts with IBAKE and how to answer corruption, state-reveal, session-output and resiliency queries.
- **Game-4** sets $u \in QR(N)$.
- **Game-5** explains how to respond to the test-session query from $\mathcal{A}$.
- **Game-6** sets $S_2 \in J(N) \setminus QR(N)$.
- **Game-**$\overline{6}$ sets $S_1 \in J(N) \setminus QR(N)$.
- **Game-7** and **Game-**$\overline{7}$ prove that the proposed IBAKE is resilient if $\mathcal{A}$ attacked P_1 or P_2 respectively.
- **Game-8** and **Game-**$\overline{8}$ show that the shared secret is indistinguishable from random if $\mathcal{A}$ attacked P_1 or P_2 respectively.
- **Game-9** explains what happens if the test-session query is different that the input of $\mathcal{D}$. We now present the security proof.

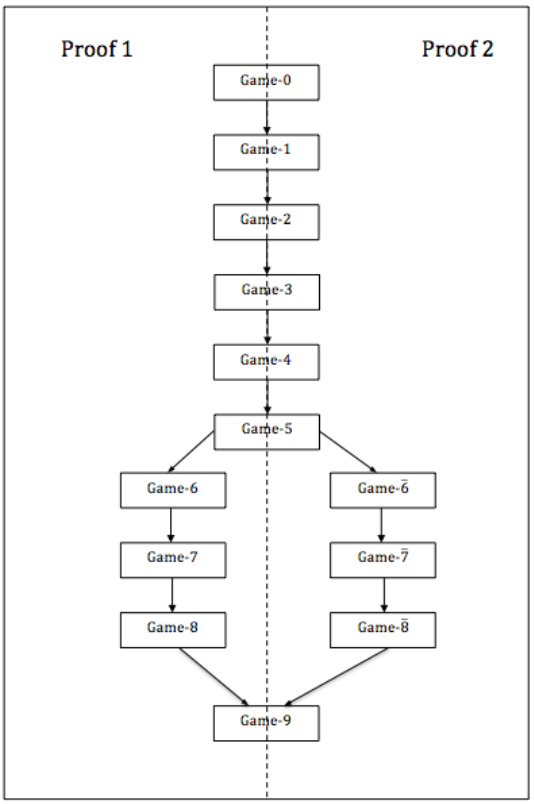

Figure 7.2: IBAKE Security Proof

Game-0. Choose in random a value $1 < d < l$. Run $\mathcal{A}$ on a simulated interaction in the AM model with $P_1, .., P_n$ running IBAKE. Give the adversary $\mathcal{A}$ the public parameters H, u, N as a result of executing the *Setup* algorithm of IBAKE. Since this game is the same as running IBAKE, we have,

$$|\Pr[W_0] - \frac{1}{2}| = IBEAdv_{\mathcal{A},IBAKE}(\lambda).$$

Game-1. This is the same as Game-0, with the following change. In the *Setup* algorithm, instead of using a PRF to generate the private keys of a party P, we use a truly random function $f : ID \rightarrow \{0, 1, 2, 3\}$. If F is a secure PRF, $\mathcal{A}$ will not notice the difference between Game-0 and Game-1. In particular, there exists an algorithm Q_1 (whose running time is about the same as that of $\mathcal{A}$) such that,

$$|\Pr[W_1] - \Pr[W_0]| = PRFAdv_{Q_1,F}(\lambda).$$

Game-2. (N, u, H) are the public parameters *params* given to $\mathcal{A}$ in the previous game where u is uniform in $J(N) \setminus QR(N)$ and the random oracle H is a random function $H : ID \rightarrow J(N)$. We make the following change in the random oracle H in this game. $\mathcal{D}$ responds to a query to $H(ID)$ by picking $a \in_R \{0, 1\}$ and $v \in_R \mathbb{Z}_{\mathbb{N}}$ and setting $H(ID) = u^a v^2$. Thus $\mathcal{D}$ implements a random function $H : ID \rightarrow J(N)$ as

in the previous game. $\mathcal{D}$ generates the private key of a party P as follows. Suppose $R = H(ID) = u^a v^2$ for some $a \in_R \{0,1\}$ and $v \in_R \mathbb{Z}_{\mathbb{N}}$. $\mathcal{D}$ generates the private key for ID by setting either $R^{\frac{1}{2}} = v$ (when $a = 0$) or $(uR)^{\frac{1}{2}} = uv$ (when $a = 1$). Since v is uniform in $\mathbb{Z}_{\mathbb{N}}$, this will produce a square root of R or uR which is also uniform among the four square roots, as in the previous game. Thus, $\mathcal{A}$'s views in Game-1 and Game-2 are identical and therefore,

$$|\Pr[W_2] = \Pr[W_1]|.$$

Game-3. When $\mathcal{A}$ triggers a party to start a new session (except for the d session) or retrieve a message, follow the instructions of IBAKE on behalf of that party. When a session is expired at a party, delete the corresponding session key from that party's memory. When a party is corrupted, give the adversary the long-term key r_i of that party along with the current internal state s_i of that party. If $\mathcal{A}$ makes a session-state reveal query for a specified session within a party, it gets the current local state s_i of the specified session within that party. If $\mathcal{A}$ makes a session-output query for a specified session within a party, it gets SSK_w. If $\mathcal{A}$ issues a resiliency query for an unexpired session, it gets the shared secret SSK of that session. Since this game is the same as the previous game, we have,

$$|\Pr[W_3] = \Pr[W_2]|.$$

Game-4. In this game, $\mathcal{D}$ chooses u uniformly in $QR(N)$ instead of $J(N) \setminus QR(N)$. Since this is the only change between Game-3 and Game-4, $\mathcal{A}$ will not notice the difference assuming that the QR assumption holds for RSAgen. In particular, there exists an algorithm Q_2 (whose running time is about the same as that of $\mathcal{A}$) such that,

$$|\Pr[W_4] - \Pr[W_3]| = QRAdv_{Q_2,RSAgen}(\lambda).$$

Game-5. We now explain how $\mathcal{D}$ answers the test-session query from $\mathcal{A}$. When the d-th session (P_1, P_2, SID^*) starts, P_1 initiates the session with P_2 and sends $(P_1, SID^*, u^{\alpha_1^*}, S_1^*)$ to P_2. When P_2 receives the message $(P_1, SID^*, u^{\alpha_1^*}, S_1^*)$ from P_1, it sends back the message $(P_2, SID^*, u^{\alpha_2^*}, S_2^*)$. If $\mathcal{A}$ chooses (P_1, P_2, SID^*) as the test-session, then give $\mathcal{A}$ the values of $SSK_1, ..., SSK_{w-1}$ and toss a fair coin $b \in \{0,1\}$. If $b = 1$ then give the adversary the challenge shared secret SSK_w^* otherwise give a random number to $\mathcal{A}$ as the answer to this query. Since this game is the same as Game-4, thus,

$$|\Pr[W_5] = \Pr[W_4]|.$$

Game-6. In this game, we make a change in the test-session. Instead of sending

$S_2^* \in QR(N)$ to P_1, P_2 sends $S_2^* \in J(N) \setminus QR(N)$. Since the only difference between Game-6 and Game-5 is that $S_2^* \in J(N) \setminus QR(N)$ in Game-6 instead of $S_2^* \in QR(N)$ in Game-5, $\mathcal{A}$ will not notice the difference assuming that the QR assumption holds for RSAgen. In particular, there exists an algorithm Q_2 (whose running time is about the same as that of $\mathcal{A}$) such that,

$$|\Pr[W_6] - \Pr[W_5]| = QRAdv_{Q_2,RSAgen}(\lambda).$$

Game-$\overline{6}$. In this game, we make a change in the test-session. Instead of sending $S_1^* \in QR(N)$ to P_2, P_1 sends $S_1^* \in J(N) \setminus QR(N)$. Since the only difference between Game-$\overline{6}$ and Game-5 is that $S_1 \in J(N) \setminus QR(N)$ in Game-$\overline{6}$ instead of $S_1 \in QR(N)$ in Game-5 , $\mathcal{A}$ will not notice the difference assuming that the QR assumption holds for RSAgen. In particular, there exists an algorithm Q_2 (whose running time is about the same as that of $\mathcal{A}$) such that,

$$|\Pr[\overline{W}_6] - \Pr[W_5]| = QRAdv_{Q_2,RSAgen}(\lambda).$$

Game-7. This game shows that the proposed IBAKE protocol is resilient if the adversary attacks P_1. To prove this, we need to show that the Jacobi symbols $\left(\frac{x_i u^{\frac{\alpha_1-a_1}{2}} r_1 s_1^{2i+1}+1}{N}\right) = \left(\frac{x_i \gamma S_1^i+1}{N}\right)$ where $\gamma = u^{\frac{\alpha_1-a_1}{2}} r_1 s_1$ are independent from one another, so if the adversary gets in the test session the shared secrets $SSK_1, SSK_2, ..., SSK_{w-1}$ that will not provide him any information about the challenge shared secret SSK_w^*. The proof of this claim depends on the following Lemma.

Lemma 7.2. *It is a hard problem to find the Jacobi symbol* $\left(\frac{P(k)a+1}{N}\right)$ *for a security parameter* k *from a sequence of* $\left(\frac{a+1}{N}\right)$, $\left(\frac{2a+1}{N}\right)$, $\left(\frac{3a+1}{N}\right)$, ..., $\left(\frac{P(k)a+1}{N}\right)$ *if* $GCD(a, N) = 1$.

Proof. Damgard [Dam88] presented Theorem 4.3 which stats that the Jacobi symbols of $(a+1, a+2, ..., a+P(k))$ is indistinguishable from random. The difference between the Jacobi sequence $\left(\frac{a+1}{N}\right)$, $\left(\frac{a+2}{N}\right)$, $\left(\frac{a+3}{N}\right)$, ..., $\left(\frac{a+P(k)+1}{N}\right)$ and the Jacobi sequence $\left(\frac{a+1}{N}\right)$, $\left(\frac{2a+1}{N}\right)$, $\left(\frac{3a+1}{N}\right)$, ..., $\left(\frac{P(k)a+1}{N}\right)$ is that the first is incremented by 1 and the other is incremented by a. Since $GCD(a, N) = 1$ i.e. a is relatively prime to N, a is a generator for the additive cyclic group $\mathbb{Z}_{\mathbb{N}}$ and the two sequences are exactly the same but generated in different order and consequently Lemma 7.2 holds.

The sequence $\left(\frac{x_i \gamma S_1^i+1}{N}\right)$ can be expressed as $\left(\frac{c_i a+1}{N}\right)$ where $c_i = x_i S_1^i$ and $a = \gamma$. If c_i does not repeat i.e. there is no $c_i = c_j$ for $i \neq j$ and $GCD(\gamma, N) = 1$, then the sequence $\left(\frac{x_i \gamma S_1^i+1}{N}\right)$ imitates the sequence $\left(\frac{a+1}{N}\right)$, $\left(\frac{2a+1}{N}\right)$, $\left(\frac{3a+1}{N}\right)$, ..., $\left(\frac{(P(k)a+1}{N}\right)$ and we can say that guessing the Jacobi symbol $\left(\frac{x_{l,1} \gamma S_1^l+1}{N}\right)$ from the sequence of Jacobi

symbols $\left(\frac{x_i\gamma S_1^i+1}{N}\right)$, $0 < i < l-1$ is a hard problem, where l is the number total shared bits between P_1 and P_2. Thus,

$$|\Pr[W_7] = \Pr[W_6]|.$$

Game-$\overline{7}$. This game shows in the same way as Game-7 that the proposed IBAKE protocol is resilient if the adversary attacks P_2 by proving that the Jacobi sequence $\left(\frac{2y_i u^{\frac{\alpha_2-a_2}{2}} r_2 s_2^{2i+1}+2}{N}\right) = \left(\frac{2y_i\beta S_2^i+2}{N}\right)$ where $\beta = u^{\frac{\alpha_2-a_2}{2}} r_2 s_2$ are independent from one another. Thus,

$$|\Pr[\overline{W}_7] = \Pr[\overline{W}_6]|.$$

Game-8. In this game, we replace the shared secret SSK_w^* by a random string $z \in_R \{-1,1\}^l$. We first prove that $(x_i\gamma S_1^i+1)(-x_i\gamma S_1^i+1)u^{\alpha_2}R_2S_2^{2i+1} \in QR(N)$.

Proof. Let $f(x_i,\gamma) = (x_i\gamma S_1^i+1)$, then we have,

$$\begin{aligned} &f(x_i,\gamma)f(x_i,-\gamma)u^{\alpha_2}R_2S_2^{2i+1} = (x_i\gamma S_1^i+1)\cdot(-x_i\gamma S_1^i+1)u^{\alpha_2}R_2S_2^{2i+1} \\ &= (1-u^{\alpha_1}R_1S_1^{2i+1}x_i^2)u^{\alpha_2}R_2S_2^{2i+1} = (u^{\alpha_2}R_2S_2^{2i+1}y_i^2)u^{\alpha_2}R_2S_2^{2i+1} \\ &= (u^{\alpha_2}R_2S_2^{2i+1}y_i)^2 \in QR(N). \end{aligned}$$

Since $u, R_1, R_2, S_1 \in QR(N)$, $S_2 \in J(N) \setminus QR(N)$, $(x_i\gamma S_1^i+1)(-x_i\gamma S_1^i+1)R_2S_2^{2i+1} \in QR(N)$, then Case 2 in Lemma 4.2 can be applied and the distribution of the Jacobi symbols $\left(\frac{x_i\gamma S_1^i+1}{N}\right)$ are random in $\{\pm 1\}$. Thus, $\mathcal{A}$ will not be able to distinguish between Game-6 and Game-7. i.e.

$$|\Pr[W_8] = \Pr[W_7]|.$$

Game-$\overline{8}$. In this game, we replace the shared secret SSK_w^* by a random string $z \in_R \{-1,1\}^l$. We first prove that $(2y_i\beta S_2^i+2)(-2y_i\beta S_2^i+2)u^{\alpha_1}R_1S_1^{2i+1} \in QR(N)$.

Proof. Let $g(y_i,\beta) = 2(y_i\beta S_2^i+1)$, then we have,

$$\begin{aligned} &g(y_i,\beta)g(y_i,-\beta)u^{\alpha_1}R_1S_1^{2i+1} = 4(y_i\beta S_2^i+1)\cdot(-y_i\beta S_2^i+1)u^{\alpha_1}R_1S_1^{2i+1} \\ &= 4(1-u^{\alpha_2}R_2S_2^{2i+1}y_i^2)u^{\alpha_1}R_1S_1^{2i+1} = 4(u^{\alpha_1}R_1S_1^{2i+1}x_i^2)u^{\alpha_1}R_1S_1^{2i+1} \\ &= (2u^{\alpha_1}R_1S_1^{2i+1}x_i)^2 \in QR(N). \end{aligned}$$

Since $u, R_1, R_2, S_2 \in QR(N)$, $S_1 \in J(N) \setminus QR(N)$, $(2y_i\beta S_2^i+2)(-2y_i\beta S_2^i+2)R_1S_1^{2i+1} \in QR(N)$, then Case 1 in Lemma 4.2 can be applied and the distribution of the Jacobi symbols $\left(\frac{2y_i\beta S_2^i+2}{N}\right)$ are random in $\{\pm 1\}$. Thus, $\mathcal{A}$ will not be able to

distinguish between Game-$\overline{6}$ and Game-$\overline{7}$. i.e.

$$|\Pr[\overline{W}_8] = \Pr[\overline{W}_7]|.$$

Game-9. If the d-th session (P_1, P_2, SID^*) is ever exposed, or if chooses a session different than the d-th session, or if $\mathcal{A}$ halts without choosing a test-session then $\mathcal{D}$ outputs a random value $\overline{b} \in \{0, 1\}$ and halts. If $\mathcal{A}$ halts and outputs $\overline{b}$, then $\mathcal{D}$ halts and outputs $\overline{b}$ too.

Clearly in **Game-8**, **Game-**$\overline{8}$ and **Game-9** we have,

$$|\Pr[W_8] = \Pr[\overline{W}_8] = \Pr[W_9] = \frac{1}{2}|.$$

Combining all the previous equations proves the security of the proposed IBAKE against an AM adversary.

We note here that the proposed IBAKE protocol (in its current state) is not secure against UM adversary. If an adversary $\mathcal{U}$ can manipulate the values S_1 and S_2 exchanged between parties P_1, P_2 he can break the protocol as follows. $\mathcal{U}$ chooses a random value $\alpha \in \mathbb{Z}_{\mathbb{N}}$ and calculates $S_1 = \alpha^2 R^{-1}$ and sends S_1 to P_2.

$\mathcal{U}$ will be able to completely break the protocol and exchange a session key with P_2 on behalf of P_1 even though $\mathcal{U}$ did not know the long-term secret key r_1 or s_1 because every generated bit is function in the secret $r_1 s_1 = \alpha_1$ which is known by $\mathcal{U}$. We can use authenticators presented in [BR93, CK01] to convert the IBAKE protocol to be secure against $\mathcal{U}$.

Based on the above, we can say that the proposed IBAKE is resilient and is CK-secure against the UM adversary. This concludes the proof of Theorem 7.1.

7.5 Efficiency

In this section, we present an efficiency comparison between our proposed IBAKE, the multiple key exchange protocol of Lee *et al.* [LWW08, VLYK10] which is based on parings and the ISO/IEC 11770-3 standard [ISO09b]. We compare between them in terms of number of keys that can be shared per session, the number of expensive operations per session and the required bandwidth (BW) to establish each session. Table 7.1 compares between these three protocols. The symbol p presents a prime search, $\hat{e}$ presents a pairing operation, m presents a prime modular exponentiation. N is the modulus and l is the shared secret length. The symbols G presents an element in in a group G such that $e : G \times G \rightarrow G_T$. From Table 7.1, we can see that.

- The proposed IBAKE can work as an excellent multiple key exchange protocol

Table 7.1: Comparison Between Some KE Protocols and The Proposed IBAKE

	N. of shared keys	Expensive Operations	BW
IBAKE	$\frac{N}{l}$	$2p$	$\mathbb{Z}_{\mathbb{N}}$
Lee *et al.*	4	$4\hat{e}$	$4G$
standard	1	$3m$	$\mathbb{Z}_{\mathbb{N}}$

with the possibility to generate $\frac{N}{l}$ keys.

- The proposed IBAKE requires only two prime search operations to solve the equations $u^{\alpha_1} R_1 S_1 x_0^2 + u^{\alpha_2} R_2 S_2 y_0^2 \equiv 1 \pmod{N}$ and $S_1^2 x^2 + u^{\alpha_2} R_2 S_2 y^2 \equiv 1 \pmod{N}$ to generate the whole set of $\frac{N}{l}$ keys. Moreover, because of the resiliency property, if a shared key SSK is leaked, we can generate another key SSK_i without the need to solve any such equations, while the other two protocols must establish a new session.

- Both parties need to share only one element in $\mathbb{Z}_{\mathbb{N}}$ to establish the session, and if a new shared key is required it can be generated without exchange any further information.

7.6 Conclusion

We presented a new notion of security called resiliency which presents the ability of a KE protocol to securely generate another session key if the previous session key is leaked without the need to setup a new session. We modify the CK-model to meet the resiliency security requirement. We then present an IBAKE that can generate multiple, independent and secure shared secrets between two parties within the same session. We proved that the proposed IBAKE protocol is secure against a UM adversary with resiliency. We also showed that the proposed IBAKE is efficient and practical compared to other KE protocols.

Chapter 8

Conclusion And Future Work

8.1 Conclusion

Identity-based cryptography (IBC) is considered as the next generation of public key cryptography because it completely eliminates the use of certificates. Most IBC systems, especially identity-based encryption (IBE) systems, are constructed using bilinear pairings. IBC systems based on pairings have few major drawbacks. First, bilinear pairings are time- and power-inefficient mathematical tools. According to MIRACL benchmarks, a bilinear pairing takes approximately 2.5 times a modular exponentiation in RSA. Second, the incompatibility of these systems with the well-established public key cryptography such as RSA prevents them from being widely used in the real world. Third, the security of these systems are based on relatively untested computational problems compared to RSA or ElGamal. Fourth, the implementation of these systems can be complex with many choices of parameters, families of curves and implementation tricks. The current IBE systems without pairings are not practical and cannot compete with IBE based on bilinear pairings.

To overcome the above mentioned drawbacks, we investigated in this thesis identity-based variants of RSA and we also investigated the current pairing-free IBE systems based on RSA settings such as Cock's IBE [Coc01], Boneh, Gentry and Hamburg (BGH) IBE [BGH07] and Jhanwar and Barua (JB) IBE [JB08] and we got the following results.

In Chapter 3, we investigated the mediated structure of IB-mRSA which is a solution to the key revocation problem in the identity-based settings. We showed that IB-mRSA may not be secure and proposed two solutions to overcome the security flaw of IB-mRSA. After that, we presented a generic mediated encryption (GME) that converts any IBE to an identity-based mediated IBE. Although it is based on double encryption, our proposed system is efficient. The ciphertext size is the same as a single IBE. It combines the advantage of CBE and SEM structures. Our system is more efficient than CBE because it does not depend on certificates and it is more secure than [BDTW01] and [Gen06] because the SEM in GME is not a single point of failure and can not be fully trusted. We prove that GME is as secure as the IBE used in the case of a revoked user or a hacked SEM.

In Chapter 4, we investigated two BGH IBE systems presented in [BGH07] and proposed two variants of these systems. The proposed variants are more time-efficient than BGH systems without negatively effecting the security of BGH IBE

systems. We also presented a time-space trade-off variants that are both time- and power-efficient.

In Chapter 5, we investigated the security of JB IBE. We showed that this IBE is not IND-ID-CPA secure and presented a solution to overcome this security flaw. We also pointed out a flaw of the security proof of JB IBE and presented a security proof that shows that the fixed JB IBE is as secure as the original BasicIBE of Boneh, Gentry and Hamburg.

In Chapter 6, we presented two ciphertext-policy attribute-based signcryption systems (CP-ABSC) that signcrypts data in away more efficient than individually encrypting and signing data. In addition, one of the proposed ABSC systems (Anon-ABSC) preserves the privacy of the encryption attributes (i.e. anonymous). They are full secure in the random oracle model based on the QR assumption. The proposed systems have a constant ciphertext size regardless of the size of the access structure.

In Chapter 7, we proposed a new notion of security of key exchange (KE) protocols called resiliency. The concept of resiliency presents the ability of a KE protocol to securely generate another session key between the designated parties if the previous session key is leaked without the need to setup a new session. We modify the CK-model to meet the resiliency security requirement. We then present an IBAKE that can generate multiple, independent and secure shared secrets between two parties within the same session. We proved that the proposed IBAKE protocol is secure against a UM adversary with resiliency. We also showed that the proposed IBAKE is efficient and practical compared to other KE protocols.

8.2 Future Work

Tradeoffs between security and performance exist in the proposed pairing-free identity-based cryptography systems. Although these systems are highly time-efficient, they are space-inefficient compared to pairing-based identity-based cryptography systems. In addition, pairing-based systems are applied in many applications such as hierarchical encryption and certificateless cryptography. In our future work, we would investigate new techniques to construct IBE systems that are both time- and space-efficient, improve the security of these systems by presenting efficient CCA secure systems without random oracle, and design efficient systems that can be adopted to the security applications of our digital world.

Bibliography

[ABB+04] William Aiello, Steven M. Bellovin, Matt Blaze, Ran Canetti, John Ioannidis, Angelos D. Keromytis, and Omer Reingold. Just fast keying: Key agreement in a hostile internet. *ACM Trans. Inf. Syst. Secur.*, 7(2):242–273, 2004.

[ACG+06] Nuttapong Attrapadung, Yang Cui, David Galindo, Goichiro Hanaoka, Ichiro Hasuo, Hideki Imai, Kanta Matsuura, Peng Yang, and Rui Zhang. Relations among notions of security for identity based encryption schemes. In *LATIN 2006: Theoretical Informatics, 7th Latin American Symposium, Valdivia, Chile, March 20-24, 2006, Proceedings*, pages 130–141, 2006.

[AG09] Giuseppe Ateniese and Paolo Gasti. Universally anonymous IBE based on the quadratic residuosity assumption. In *Topics in Cryptology - CT-RSA 2009, The Cryptographers' Track at the RSA Conference 2009, San Francisco, CA, USA, April 20-24, 2009. Proceedings*, pages 32–47, 2009.

[ALdP11] Nuttapong Attrapadung, Benoît Libert, and Elie de Panafieu. Expressive key-policy attribute-based encryption with constant-size ciphertexts. In *Public Key Cryptography - PKC 2011 - 14th International Conference on Practice and Theory in Public Key Cryptography, Taormina, Italy, March 6-9, 2011. Proceedings*, pages 90–108, 2011.

[ALO98] William Aiello, Sachin Lodha, and Rafail Ostrovsky. Fast digital identity revocation (extended abstract). In *Advances in Cryptology - CRYPTO '98, 18th Annual International Cryptology Conference, Santa Barbara, California, USA, August 23-27, 1998, Proceedings*, pages 137–152, 1998.

[BB04a] Dan Boneh and Xavier Boyen. Efficient selective-ID secure identity-based encryption without random oracles. In *Advances in Cryptology - EUROCRYPT 2004, International Conference on the Theory and Applications of Cryptographic Techniques, Interlaken, Switzerland, May 2-6, 2004, Proceedings*, pages 223–238, 2004.

[BB04b] Dan Boneh and Xavier Boyen. Secure identity based encryption without random oracles. In *Advances in Cryptology - CRYPTO 2004, 24th Annual International CryptologyConference, Santa Barbara, California, USA, August 15-19, 2004, Proceedings*, pages 443–459, 2004.

[BBDP01] Mihir Bellare, Alexandra Boldyreva, Anand Desai, and David Pointcheval. Key-privacy in public-key encryption. In *Advances in Cryptology - ASIACRYPT 2001, 7th International Conference on the Theory and Application of Cryptology and Information Security, Gold Coast, Australia, December 9-13, 2001, Proceedings*, pages 566–582, 2001.

[BCK98] Mihir Bellare, Ran Canetti, and Hugo Krawczyk. A modular approach to the design and analysis of authentication and key exchange protocols (extended abstract). In *Proceedings of the Thirtieth Annual ACM Symposium on the Theory of Computing, Dallas, Texas, USA, May 23-26, 1998*, pages 419–428, 1998.

[BCNP08] Colin Boyd, Yvonne Cliff, Juan Manuel González Nieto, and Kenneth G. Paterson. Efficient one-round key exchange in the standard model. In *Information Security and Privacy, 13th Australasian Conference, ACISP 2008, Wollongong, Australia, July 7-9, 2008, Proceedings*, pages 69–83, 2008.

[BDT02] Dan Boneh, Xuhua Ding, and Gene Tsudik. Identity-based mediated RSA. In *The Proceedings of the 3rd International Workshop on Information Security Applications(WISA'02) (Jeju Island, Korea)*, 2002.

[BDT04] Dan Boneh, Xuhua Ding, and Gene Tsudik. Fine-grained control of security capabilities. *ACM Trans. Internet Techn.*, 4(1):60–82, 2004.

[BDTW01] Dan Boneh, Xuhua Ding, Gene Tsudik, and Chi-Ming Wong. A method for fast revocation of public key certificates and security capabilities. In *10th USENIX Security Symposium, August 13-17, 2001, Washington, D.C., USA*, 2001.

[BF01] Dan Boneh and Matthew K. Franklin. Identity-based encryption from the weil pairing. In *Advances in Cryptology - CRYPTO 2001, 21st Annual International Cryptology Conference, Santa Barbara, California, USA, August 19-23, 2001, Proceedings*, pages 213–229, 2001.

[BGH07] Dan Boneh, Craig Gentry, and Michael Hamburg. Space-efficient identity based encryption without pairings. In *48th Annual IEEE Sym-*

posium on Foundations of Computer Science (FOCS 2007), October 20-23, 2007, Providence, RI, USA, Proceedings, pages 647–657, 2007.

[BJ10] Rana Barua and Mahabir Jhanwar. On the number of solutions of the equation $Rx^2+Sy^2 = 1 \pmod N$. *Sankhya A - Mathematical Statistics and Probability*, 72:226–236, 2010. 10.1007/s13171-010-0010-9.

[Boy03] Xavier Boyen. Multipurpose identity-based signcryption (A swiss army knife for identity-based cryptography). In *Advances in Cryptology - CRYPTO 2003, 23rd Annual International Cryptology Conference, Santa Barbara, California, USA, August 17-21, 2003, Proceedings*, pages 383–399, 2003.

[BPR00] Mihir Bellare, David Pointcheval, and Phillip Rogaway. Authenticated key exchange secure against dictionary attacks. In *Advances in Cryptology - EUROCRYPT 2000, International Conference on the Theory and Application of Cryptographic Techniques, Bruges, Belgium, May 14-18, 2000, Proceeding*, pages 139–155, 2000.

[BR93] Mihir Bellare and Phillip Rogaway. Entity authentication and key distribution. In *Advances in Cryptology - CRYPTO '93, 13th Annual International Cryptology Conference, Santa Barbara, California, USA, August 22-26, 1993, Proceedings*, pages 232–249, 1993.

[BR95] Mihir Bellare and Phillip Rogaway. Provably secure session key distribution: the three party case. In *Proceedings of the Twenty-Seventh Annual ACM Symposium on Theory of Computing, 29 May-1 June 1995, Las Vegas, Nevada, USA*, pages 57–66, 1995.

[BRS13] Dan Boneh, Ananth Raghunathan, and Gil Segev. Function-private identity-based encryption: Hiding the function in functional encryption. In *Advances in Cryptology - CRYPTO 2013 - 33rd Annual Cryptology Conference, Santa Barbara, CA, USA, August 18-22, 2013. Proceedings, Part II*, pages 461–478, 2013.

[BSW07] John Bethencourt, Amit Sahai, and Brent Waters. Ciphertext-policy attribute-based encryption. In *2007 IEEE Symposium on Security and Privacy (S&P 2007), 20-23 May 2007, Oakland, California, USA*, pages 321–334, 2007.

[BW06] Xavier Boyen and Brent Waters. Anonymous hierarchical identity-based encryption (without random oracles). *IACR Cryptology ePrint Archive*, 2006:85, 2006.

[CCL+13] Cheng Chen, Jie Chen, Hoon Wei Lim, Zhenfeng Zhang, Dengguo Feng, San Ling, and Huaxiong Wang. Fully secure attribute-based systems with short ciphertexts/signatures and threshold access structures. In *Topics in Cryptology - CT-RSA 2013 - The Cryptographers' Track at the RSA Conference 2013, San Francisco,CA, USA, February 25-March 1, 2013. Proceedings*, pages 50–67, 2013.

[CK01] Ran Canetti and Hugo Krawczyk. Analysis of key-exchange protocols and their use for building secure channels. In *Advances in Cryptology - EUROCRYPT 2001, International Conference on the Theory and Application of Cryptographic Techniques, Innsbruck, Austria, May 6-10, 2001, Proceeding*, pages 453–474, 2001.

[CK02] Liqun Chen and Caroline Kudla. Identity based authenticated key agreement protocols from pairings. *IACR Cryptology ePrint Archive*, Report 2002/184, 2002.

[CN07] Ling Cheung and Calvin C. Newport. Provably secure ciphertext policy ABE. In *Proceedings of the 2007 ACM Conference on Computer and Communications Security, CCS 2007, Alexandria, Virginia, USA, October 28-31, 2007*, pages 456–465, 2007.

[Coc01] Clifford Cocks. An identity based encryption scheme based on quadratic residues. In *Cryptography and Coding, 8th IMA International Conference, Cirencester, UK, December 17-19, 2001, Proceedings*, pages 360–363, 2001.

[Cor09] Jean-Sébastien Coron. A variant of boneh-franklin IBE with a tight reduction in the random oracle model. *Des. Codes Cryptography*, 50(1):115–133, 2009.

[CR03] J. E. Cremona and D. Rusin. Efficient solution of rational conics. *Math. Comput.*, 72(243):1417–1441, 2003.

[CS98] Ronald Cramer and Victor Shoup. A practical public key cryptosystem provably secure against adaptive chosen ciphertext attack. In *Advances in Cryptology - CRYPTO '98, 18th Annual International Cryptology Conference, Santa Barbara, California, USA, August 23-27, 1998, Proceedings*, pages 13–25, 1998.

[CS03] Ronald Cramer and Victor Shoup. Design and analysis of practical public-key encryption schemes secure against adaptive chosen ciphertext attack. *SIAM J. Comput.*, 33(1):167–226, 2003.

[CSF+08] D. Cooper, S. Santesson, S. Farrell, S. Boeyen, R. Housley, and W. Polk. RFC5280: Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, May 2008.

[Dam88] Ivan Damgård. On the randomness of legendre and jacobi sequences. In *Advances in Cryptology - CRYPTO '88, 8th Annual International Cryptology Conference, Santa Barbara, California, USA, August 21-25, 1988, Proceedings*, pages 163–172, 1988.

[DB05] Ratna Dutta and Rana Barua. Overview of key agreement protocols. *IACR Cryptology ePrint Archive*, Report 2005/289, 2005.

[DDN91] Danny Dolev, Cynthia Dwork, and Moni Naor. Non-malleable cryptography (extended abstract). In *Proceedings of the 23rd Annual ACM Symposium on Theory of Computing, May 5-8, 1991, New Orleans, Louisiana, USA*, pages 542–552, 1991.

[DGKS10] Yvo Desmedt, Rosario Gennaro, Kaoru Kurosawa, and Victor Shoup. A new and improved paradigm for hybrid encryption secure against chosen-ciphertext attack. *J. Cryptology*, 23(1):91–120, 2010.

[DH76] Whitfield Diffie and Martin E. Hellman. New directions in cryptography. *IEEE Transactions on Information Theory*, 22(6):644–654, 1976.

[DR00] Joan Daemen and Vincent Rijmen. Rijndael for AES. In *AES Candidate Conference*, pages 343–348, 2000.

[DT03] Xuhua Ding and Gene Tsudik. Simple identity-based cryptography with mediated RSA. In *Topics in Cryptology - CT-RSA 2003, The Cryptographers' Track at the RSA Conference 2003, San Francisco, CA, USA, April 13-17, 2003, Proceedings*, pages 193–210, 2003.

[EMN+09] Keita Emura, Atsuko Miyaji, Akito Nomura, Kazumasa Omote, and Masakazu Soshi. A ciphertext-policy attribute-based encryption scheme with constant ciphertext length. In *Information Security Practice and Experience, 5th International Conference, ISPEC 2009, Xi'an, China, April 13-15, 2009, Proceedings*, pages 13–23, 2009.

[FO13] Eiichiro Fujisaki and Tatsuaki Okamoto. Secure integration of asymmetric and symmetric encryption schemes. *J. Cryptology*, 26(1):80–101, 2013.

[Gal05] David Galindo. Boneh-franklin identity based encryption revisited. In *Automata, Languages and Programming, 32nd International Colloquium, ICALP 2005, Lisbon, Portugal, July 11-15, 2005, Proceedings*, pages 791–802, 2005.

[Gam84] Taher El Gamal. A public key cryptosystem and a signature scheme based on discrete logarithms. In *Advances in Cryptology, Proceedings of CRYPTO '84, Santa Barbara, California, USA, August 19-22, 1984, Proceedings*, pages 10–18, 1984.

[Gen03] Craig Gentry. Certificate-based encryption and the certificate revocation problem. In *Advances in Cryptology - EUROCRYPT 2003, International Conference on the Theory and Applications of Cryptographic Techniques, Warsaw, Poland, May 4-8, 2003, Proceedings*, pages 272–293, 2003.

[Gen06] Craig Gentry. Practical identity-based encryption without random oracles. In *Advances in Cryptology - EUROCRYPT 2006, 25th Annual International Conference on the Theory and Applications of Cryptographic Techniques, St. Petersburg, Russia, May 28 - June 1, 2006, Proceedings*, pages 445–464, 2006.

[GGH+13] Sanjam Garg, Craig Gentry, Shai Halevi, Amit Sahai, and Brent Waters. Attribute-based encryption for circuits from multilinear maps. In *Advances in Cryptology - CRYPTO 2013 - 33rd Annual Cryptology Conference, Santa Barbara, CA, USA, August 18-22, 2013. Proceedings, Part II*, pages 479–499, 2013.

[GHR99] Rosario Gennaro, Shai Halevi, and Tal Rabin. Secure hash-and-sign signatures without the random oracle. In *Advances in Cryptology - EUROCRYPT '99, International Conference on the Theory and Application of Cryptographic Techniques, Prague, Czech Republic, May 2-6, 1999, Proceeding*, pages 123–139, 1999.

[GLF13] Zhenzhou Guo, Mingchu Li, and Xinxin Fan. Attribute-based ring signcryption scheme. *Security and Communication Networks*, 6(6):790–796, 2013.

[GM84] Shafi Goldwasser and Silvio Micali. Probabilistic encryption. *J. Comput. Syst. Sci.*, 28(2):270–299, 1984.

[GMS+14] Fuchun Guo, Yi Mu, Willy Susilo, Duncan S. Wong, and Vijay Varadharajan. CP-ABE with constant-size keys for lightweight devices.

IEEE Transactions on Information Forensics and Security, 9(5):763–771, 2014.

[GNS10] Martin Gagné, Shivaramakrishnan Narayan, and Reihaneh Safavi-Naini. Threshold attribute-based signcryption. In *Security and Cryptography for Networks, 7th International Conference, SCN 2010, Amalfi, Italy, September 13-15, 2010. Proceedings*, pages 154–171, 2010.

[GPSW06] Vipul Goyal, Omkant Pandey, Amit Sahai, and Brent Waters. Attribute-based encryption for fine-grained access control of encrypted data. In *Proceedings of the 13th ACM Conference on Computer and Communications Security, CCS 2006, Alexandria, VA, USA, Ioctober 30 - November 3, 2006*, pages 89–98, 2006.

[GPV07] Craig Gentry, Chris Peikert, and Vinod Vaikuntanathan. Trapdoors for hard lattices and new cryptographic constructions. *Electronic Colloquium on Computational Complexity (ECCC)*, 14(133), 2007.

[GTS01] M. T. Goodrich, R. Tamassia, and A. Schwerin. Implementation of an Authenticated Dictionary with Skip Lists and Commutative Hashing. *DARPA Information Survivability Conference and Exposition*, 2:1068, 2001.

[Her14] Javier Herranz. Attribute-based signatures from RSA. *Theor. Comput. Sci.*, 527:73–82, 2014.

[HL01] L. Harn and H-Y Lin. Authenticated key agreement without using one-way hash functions. *Electronics Letters*, 37(10):629–630, May 2001.

[HLY13] Yiliang Han, Wanyi Lu, and Xiaoyuan Yang. Attribute-based signcryption scheme with non-monotonic access structure. In *2013 5th International Conference on Intelligent Networking and Collaborative Systems, Xi'an city, Shaanxi province, China, September 9-11, 2013*, pages 796–802, 2013.

[HPFS02] R. Housley, W. Polk, W. Ford, and D. Solo. RFC3280: Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, April 2002.

[HSL03] Ren-Junn Hwang, Sheng-Hua Shiau, and Chih-Hua Lai. An enhanced authentication key exchange protocol. In *17th International Conference on Advanced Information Networking and Applications (AINA'03), March 27-29, 2003, Xi'an, China*, pages 202–205, 2003.

[HT05] Ryotaro Hayashi and Keisuke Tanaka. Universally anonymizable public-key encryption. In *Advances in Cryptology - ASIACRYPT 2005, 11th International Conference on the Theory and Application of Cryptology and Information Security, Chennai, India, December 4-8, 2005, Proceedings*, pages 293–312, 2005.

[ISO09a] ISO/IEC 9798-3:1998. Information technology – Security techniques – Entity authentication – Part 3: Mechanisms using digital signature techniques, International Organization for Standardization, Geneva, Switzerland., 2009.

[ISO09b] ISO/IEC 9798-3:1998. Information technology – Security techniques – Key management – Part 3: Mechanisms using asymmetric techniques, International Organization for Standardization, Geneva, Switzerland., 2009.

[JB08] Mahabir Prasad Jhanwar and Rana Barua. A variant of boneh-gentry-hamburg's pairing-free identity based encryption scheme. In *Information Security and Cryptology, 4th International Conference, Inscrypt 2008, Beijing, China, December 14-17, 2008, Revised Selected Papers*, pages 314–331, 2008.

[Jou04] Antoine Joux. A one round protocol for tripartite Diffie-Hellman. *J. Cryptology*, 17(4):263–276, 2004.

[Kat13] Jon Katz. Review of identity-based encryption by Sanjit Chattarjee and Palash Sarkar. *SIGACT News*, 44(4):29–31, 2013.

[Kel08] Timothy Kelley. Review of"A Course in Computational Algebraic Number Theory by Henri Cohen, " springer, 2000. *SIGACT News*, 39(2):36–39, 2008.

[Koc98] Paul C. Kocher. On certificate revocation and validation. In *Financial Cryptography, Second International Conference, FC'98, Anguilla, British West Indies, February 23-25, 1998, Proceedings*, pages 172–177, 1998.

[Kra03] Hugo Krawczyk. SIGMA: the 'sign-and-mac' approach to authenticated Diffie-Hellman and its use in the ike-protocols. In *Advances in Cryptology - CRYPTO 2003, 23rd Annual International Cryptology Conference, Santa Barbara, California, USA, August 17-21, 2003, Proceedings*, pages 400–425, 2003.

[LAS+10] Jin Li, Man Ho Au, Willy Susilo, Dongqing Xie, and Kui Ren. Attribute-based signature and its applications. In *Proceedings of the 5th ACM Symposium on Information, Computer and Communications Security, ASIACCS 2010, Beijing, China, April 13-16, 2010*, pages 60–69, 2010.

[LK10] Jin Li and Kwangjo Kim. Hidden attribute-based signatures without anonymity revocation. *Inf. Sci.*, 180(9):1681–1689, 2010.

[LOS+10] Allison B. Lewko, Tatsuaki Okamoto, Amit Sahai, Katsuyuki Takashima, and Brent Waters. Fully secure functional encryption: Attribute-based encryption and (hierarchical) inner product encryption. In *Advances in Cryptology - EUROCRYPT 2010, 29th Annual International Conference on the Theory and Applications of Cryptographic Techniques, French Riviera, May 30 - June 3, 2010. Proceedings*, pages 62–91, 2010.

[LQ04] Benoît Libert and Jean-Jacques Quisquater. Efficient signcryption with key privacy from gap diffie-hellman groups. In *Public Key Cryptography - PKC 2004, 7th International Workshop on Theory and Practice in Public Key Cryptography, Singapore, March 1-4, 2004*, pages 187–200, 2004.

[LW04] Narn-Yih Lee and Chien-Nan Wu. Improved authentication key exchange protocol without using one-way hash function. *Operating Systems Review*, 38(2):85–92, 2004.

[LWW08] Narn-Yih Lee, Chien-Nan Wu, and Chien-Chih Wang. Authenticated multiple key exchange protocols based on elliptic curves and bilinear pairings. *Computers & Electrical Engineering*, 34(1):12–20, 2008.

[MAM+99] M. Myers, R. Ankney, A. Malpani, S. Galperin, and C. Adams. "RFC 2560:X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP", June 1999.

[MB05] Noel McCullagh and Paulo S. L. M. Barreto. A new two-party identity-based authenticated key agreement. In *Topics in Cryptology - CT-RSA 2005, The Cryptographers' Track at the RSA Conference 2005, San Francisco, CA, USA, February 14-18, 2005, Proceedings*, pages 262–274, 2005.

[MCM14] Xian Yong Meng, Zhong Chen, and Xiang Yu Meng. Privacy-Preserving Decentralized Key-Policy Attribute-Based Signcryption in Cloud Com-

puting Environments. *Applied Mechanics and Materials*, 475:1144–1149, 2014.

[Mic96] S. Micali. Efficient Certificate Revocation. Technical report tm-542b, MIT Laboratory for Computer Science, Cambridge, MA, USA, March 22 1996.

[Mic02] S. Micali. Novomodo: Scalable Certificate Validation and Simplified PKI Management. In *1st Annual PKI Research Workshop, Gaithersburg, Maryland, USA*, pages 15–25, 2002.

[MPR08] Hemanta K. Maji, Manoj Prabhakaran, and Mike Rosulek. Attribute-based signatures: Achieving attribute-privacy and collusion-resistance. *IACR Cryptology ePrint Archive*, Report 2008/328, 2008.

[NMS12] Juan Manuel González Nieto, Mark Manulis, and Dongdong Sun. Fully private revocable predicate encryption. In *Information Security and Privacy - 17th Australasian Conference, ACISP 2012, Wollongong, NSW, Australia, July 9-11, 2012. Proceedings*, pages 350–363, 2012.

[NN98] Kobbi Nissim and Moni Naor. Certificate revocation and certificate update. In *Proceedings of the 7th USENIX Security Symposium, San Antonio, TX, USA, January 26-29, 1998*, 1998.

[Oka07] Tatsuaki Okamoto. Authenticated key exchange and key encapsulation in the standard model. In *Advances in Cryptology - ASIACRYPT 2007, 13th International Conference on the Theory and Application of Cryptology and Information Security, Kuching, Malaysia, December 2-6, 2007, Proceedings*, pages 474–484, 2007.

[OSW07] Rafail Ostrovsky, Amit Sahai, and Brent Waters. Attribute-based encryption with non-monotonic access structures. In *Proceedings of the 2007 ACM Conference on Computer and Communications Security, CCS 2007, Alexandria, Virginia, USA, October 28-31, 2007*, pages 195–203, 2007.

[OT12] Tatsuaki Okamoto and Katsuyuki Takashima. Fully secure unbounded inner-product and attribute-based encryption. In *Advances in Cryptology - ASIACRYPT 2012 - 18th International Conference on the Theory and Application of Cryptology and Information Security, Beijing, China, December 2-6, 2012. Proceedings*, pages 349–366, 2012.

[Pat08] Kenny Paterson. Recent advances in identity-based encryption. In *Fields Institute Workshop on New Directions in Cryptography*. University of Ottawa, June 2008.

[PS09] Kenneth G. Paterson and Sriramkrishnan Srinivasan. On the relations between non-interactive key distribution, identity-based encryption and trapdoor discrete log groups. *Des. Codes Cryptography*, 52(2):219–241, 2009.

[RSA83] Ronald L. Rivest, Adi Shamir, and Leonard M. Adleman. A method for obtaining digital signatures and public-key cryptosystems (reprint). *Commun. ACM*, 26(1):96–99, 1983.

[Sco02] Mike Scott. Authenticated id-based key exchange and remote log-in with simple token and PIN number. *IACR Cryptology ePrint Archive*, Report 2002/164, 2002.

[Sha84] Adi Shamir. Identity-based cryptosystems and signature schemes. In *Advances in Cryptology, Proceedings of CRYPTO '84, Santa Barbara, California, USA, August 19-22, 1984, Proceedings*, pages 47–53, 1984.

[Sho01] Victor Shoup. A proposal for an ISO standard for public key encryption. *IACR Cryptology ePrint Archive*, Report 2001/112, 2001.

[SK03] Ryuichi Sakai and Masao Kasahara. ID based cryptosystems with pairing on elliptic curve. *IACR Cryptology ePrint Archive*, Report 2003/54, 2003.

[Sma01] Nigel P. Smart. An identity based authenticated key agreement protocol based on the weil pairing. *IACR Cryptology ePrint Archive*, Report 2001/111, 2001.

[SW05] Amit Sahai and Brent Waters. Fuzzy identity-based encryption. In *Advances in Cryptology - EUROCRYPT 2005, 24th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Aarhus, Denmark, May 22-26, 2005, Proceedings*, pages 457–473, 2005.

[VLYK10] Duc-Liem Vo, Hyunrok Lee, Chan Yeob Yeun, and Kwangjo Kim. Enhancements of authenticated multiple key exchange protocol based on bilinear pairings. *Computers & Electrical Engineering*, 36(1):155–159, 2010.

[Wat05] Brent Waters. Efficient identity-based encryption without random oracles. In *Advances in Cryptology - EUROCRYPT 2005, 24th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Aarhus, Denmark, May 22-26, 2005, Proceedings*, pages 114–127, 2005.

[Wat11] Brent Waters. Ciphertext-policy attribute-based encryption: An expressive, efficient, and provably secure realization. In *Public Key Cryptography - PKC 2011 - 14th International Conference on Practice and Theory in Public Key Cryptography, Taormina, Italy, March 6-9, 2011. Proceedings*, pages 53–70, 2011.

[WHLL13] Chang-Ji Wang, Jia-Sen Huang, Wen-Long Lin, and Hai-Tao Lin. Security analysis of gagne et al.'s threshold attribute-based signcryption scheme. In *2013 5th International Conference on Intelligent Networking and Collaborative Systems, Xi'an city, Shaanxi province, China, September 9-11, 2013*, pages 103–108, 2013.

[YDW+11] Guomin Yang, Shanshan Duan, Duncan S. Wong, Chik How Tan, and Huaxiong Wang. Authenticated key exchange under bad randomness. In *Financial Cryptography and Data Security - 15th International Conference, FC 2011, Gros Islet, St. Lucia, February 28 - March 4, 2011, Revised Selected Papers*, pages 113–126, 2011.

[YMSW13] Guomin Yang, Yi Mu, Willy Susilo, and Duncan S. Wong. Leakage resilient authenticated key exchange secure in the auxiliary input model. In *Information Security Practice and Experience - 9th International Conference, ISPEC 2013, Lanzhou, China, May 12-14, 2013. Proceedings*, pages 204–217, 2013.

[YWWD08] Guomin Yang, Duncan S. Wong, Huaxiong Wang, and Xiaotie Deng. Two-factor mutual authentication based on smart cards and passwords. *J. Comput. Syst. Sci.*, 74(7):1160–1172, 2008.

[Zhe97] Yuliang Zheng. Digital signcryption or how to achieve cost(signature & encryption) << cost(signature) + cost(encryption). In *Advances in Cryptology - CRYPTO '97, 17th Annual International Cryptology Conference, Santa Barbara, California, USA, August 17-21, 1997, Proceedings*, pages 165–179, 1997.