2005

Identity-based partial message recovery signatures (or how to shorten ID-based signatures)

Fangguo Zhang
Sun Yat-Sen University

Willy Susilo
University of Wollongong, wsusilo@uow.edu.au

Yi Mu
University of Wollongong, ymu@uow.edu.au

Identity-based partial message recovery signatures (or how to shorten ID-based signatures)

Abstract

We propose a new notion of short identity-based signature scheme. We argue that the identity-based environment is essential in some scenarios. The notion of short identity-based signature schemes can be viewed as identity-based (partial) message recovery signatures. Signature schemes with message recovery has been extensively studied in the literature. This problem is somewhat related to the problem of signing short messages using a scheme that minimizes the total length of the original message and the appended signature. In this paper, firstly, we revisit this notion and propose an identity-based message recovery signature scheme. Our scheme can be regarded as the identity based version of Abe-Okamoto's scheme [1]. Then, we extend our scheme to achieve an identity-based partial message recovery signature scheme. In this scheme, the signature is appended to a truncated message and the discarded bytes are recovered by the verification algorithm. This is to answer the limitation of signature schemes with message recovery that usually deal with messages of fixed length. This paper opens a new research area, namely how to shorten identity based signatures, in contrast to proposing a short signature scheme. We present this novel notion together with two concrete schemes based on bilinear pairings.

Disciplines

Physical Sciences and Mathematics

Publication Details

Susilo, W., Mu, Y. & Zhang, F. (2005). Identity-based partial message recovery signatures (or how to shorten ID-based signatures). In A. Patrick & M. Yung (Eds.), Financial Cryptography and Data Security International Conference (pp. 45-56). Germany: Springer.

Identity-based Partial Message Recovery Signatures (or How to Shorten ID-based Signatures) *

Fangguo Zhang[1] **, Willy Susilo[2], and Yi Mu[2]

[1]Department of Electronics and Communication Engineering
Sun Yat-sen University, Guangzhou 510275, P.R. China
Email: isdzhfg@zsu.edu.cn
[2]School of Information Technology and Computer Science
University of Wollongong, Australia
Email: {wsusilo, ymu}@uow.edu.au

Abstract. We firstly proposed a new notion of short identity-based signature scheme. We argue that the identity-based environment is essential in some scenarios. The notion of short identity-based signature schemes can be viewed as identity-based (partial) message recovery signatures. Signature schemes with message recovery has been extensively studied in the literature. This problem is somewhat related to the problem of signing short messages using a scheme that minimizes the total length of the original message and the appended signature. In this paper, firstly, we revisit this notion and propose an identity-based message recovery signature scheme. Our scheme can be regarded as the identity based version of Abe-Okamoto's scheme [1]. Then, we extend our scheme to achieve an identity-based partial message recovery signature scheme. In this scheme, the signature is appended to a truncated message and the discarded bytes are recovered by the verification algorithm. This is to answer the limitation of signature schemes with message recovery that usually deal with messages of fixed length. This paper opens a new research era, namely how to shorten identity based signatures, in contrast to proposing a short signature scheme. We note that for the first time, we present this novel notion together with two concrete schemes based on bilinear pairing.

1 Introduction

Even in a small organization, it is desirable to authenticate all messages sent from one employee to the others. One way to authenticate an email is by incorporating a method such as PGP. However, the length of the signature itself is quite long. This drawback has certainly played a great influence in an organization where bandwidth is one of the main concern. Therefore, the invention of a short

* This work is supported by ARC Discovery Grant DP0557493
** This work is supported by the National Natural Science Foundation of China (No. 60403007).

signature scheme applicable to email is essential. This problem can be viewed as how to construct an identity based (or ID-based, for short) short signature scheme. The ID-based scenario is required to avoid the necessity to employ a certification system.

Several signature schemes have been proposed in the last decade by the research community. It is known that a signature scheme that produces signatures of length ℓ can have some security level of at most 2^ℓ, which means that given the public key, it is possible to forge a signature on any message in $\mathcal{O}(2^\ell)$. A natural question that arises is how we can concretely construct a signature scheme that can produce shorter signature length whilst maintaining an existential forgery with the same security level.

It was noted in [7] that in some situations, it is desirable to use very short signatures, for instance when one needs to sign a postcard. In this situation, it is desirable to minimize the total length of the original message and the appended signature. In the early days, research in this area has been mainly focusing on how to minimize the total length of the message and the appended signature [7, 1]. The idea that was used was originated from the message recovery schemes, for example [8]. For example, the work proposed in [7] has shortened DSS signatures to provide security level $\mathcal{O}(2^\ell)$ with signature length of about 3.5ℓ bits (in contrast to 4ℓ bits in the original DSS scheme).

A totally new approach was taken by Boneh, Lynn and Shacham by proposing a short digital signature scheme, where signatures are about half the size of DSA signatures with the same level of security [5]. The resulting signature scheme, referred to as the BLS signature scheme, is based on the Computational Diffie-Hellman (CDH) assumption on certain elliptic curves. The approach that was taken in this scheme is totally different from its predecessor, i.e. directly minimizing the signature without providing a partial message to the receiver, with the intention that on the receiver's side, the complete message can be recovered (eg. [7, 1]). In BLS signature scheme, with a signature length $\ell = 160$ bits (which is approximately half the size of DSS signatures with the same security level), it provides a security level of approximately $\mathcal{O}(2^{80})$ in the random oracle model. This signature scheme has attracted a lot of attention in the research community and has been used to construct several other new schemes (eg. [4, 12]). The main drawback of the BLS scheme is its dependency on a special hash function, i.e. an admissible encoding function, which is still probabilistic.

In [13], a more efficient approach to produce a signature of the same length of BLS was proposed. However, its security is based on a stronger assumption. The same assumption has been used in [2] to produce a short signature scheme *without* random oracles.

Our Contribution

In this paper, we revisit the notion of shortening message and the appended signature as described in [7] in an ID-based scenario. We provide two formal model and schemes, namely an ID-based message recovery signature scheme and an ID-based partial message recovery signature scheme. Our ID-based message recovery signature scheme can be regarded as the ID-based version of [1]. Although

message recovery techniques seem to solve the signature size problem, they still suffer from several drawbacks. They usually deal with messages of fixed length and it is unclear how to extend them when the message exceeds some given size. For example, the Nyberg-Rueppel scheme applied to redundant messages of twenty bytes. This presumably means ten bytes for the message and ten for the redundancy but what if the message happens to be fourteen bytes long. In our ID-based partial message recovery signature scheme, we answer this question affirmatively, by providing an ID-based scheme that can cope with arbitrarily length messages.

The rest of this paper is organized as follows. In section 2, we review some preliminaries used throughout this paper. In section 3, we propose a notion of ID-based message recovery signature scheme and present a concrete scheme based on bilinear pairing. In section 4, we extend this notion to an ID-based partial message recovery signature scheme that can handle an arbitrarily length of message. Finally, section 5 concludes the paper.

2 Preliminaries

2.1 Bilinear Pairings

Let $\mathbb{G}_1, \mathbb{G}_1'$ be cyclic additive groups generated by P_1, P_1', respectively, whose order are a prime q. Let $\mathbb{G}_2$ be a cyclic multiplicative group with the same order q. We assume there is an isomorphism $\psi : \mathbb{G}_1' \to \mathbb{G}_1$ such that $\psi(P_1') = P_1$. Let $\hat{e} : \mathbb{G}_1 \times \mathbb{G}_1' \to \mathbb{G}_2$ be a bilinear mapping with the following properties:

1. *Bilinearity*: $\hat{e}(aP, bQ) = \hat{e}(P, Q)^{ab}$ for all $P \in \mathbb{G}_1, Q \in \mathbb{G}_1', a, b, \in \mathbb{Z}_q$.
2. *Non-degeneracy*: There exists $P \in \mathbb{G}_1, Q \in \mathbb{G}_1'$ such that $\hat{e}(P, Q) \neq 1$.
3. *Computability*: There exists an efficient algorithm to compute $\hat{e}(P, Q)$ for all $P \in \mathbb{G}_1, Q \in \mathbb{G}_1'$.

For simplicity, hereafter, we set $\mathbb{G}_1 = \mathbb{G}_1'$ and $P_1 = P_1'$. We note that our scheme can be easily modified for a general case, when $\mathbb{G}_1 \neq \mathbb{G}_1'$.

Bilinear pairing instance generator is defined as a probabilistic polynomial time algorithm $\mathcal{IG}$ that takes as input a security parameter ℓ and returns a uniformly random tuple $param = (p, \mathbb{G}_1, \mathbb{G}_2, \hat{e}, P)$ of bilinear parameters, including a prime number p of size ℓ, a cyclic additive group $\mathbb{G}_1$ of order q, a multiplicative group $\mathbb{G}_2$ of order q, a bilinear map $\hat{e} : \mathbb{G}_1 \times \mathbb{G}_1 \to \mathbb{G}_2$ and a generator P of $\mathbb{G}_1$. For a group $\mathbb{G}$ of prime order, we denote the set $\mathbb{G}^* = \mathbb{G} \setminus \{\mathcal{O}\}$ where $\mathcal{O}$ is the identity element of the group.

Complexity Assumption

Definition 1. (Computational Diffie-Hellman (CDH) Problem). *Let $\mathbb{G}_1$ and $\mathbb{G}_2$ be two groups of order the same prime order q. Let P be a generator of $\mathbb{G}_1$. Suppose there exists a bilinear map $\hat{e} : \mathbb{G}_1 \times \mathbb{G}_1 \to \mathbb{G}_2$. Let $\mathcal{A}$ be an attacker. $\mathcal{A}$ tries to solve the following problem:* Given (P, aP, bP) for some unknown $a, b \in \mathbb{Z}_q^*$, compute abP.

The success probability of $\mathcal{A}$, which is polynomially bounded with a security parameter ℓ, is defined as

$$\mathtt{Succ}^{CDH}_{\mathbb{G}_1,\mathcal{A}}(\ell) = Pr[\mathcal{A}(P, aP, bP, abP) = 1; a, b \in \mathbb{Z}^*_q].$$

The CDH problem is said to be intractable, if for every probabilistic polynomial time, 0/1-valued algorithm $\mathcal{A}$, $\mathtt{Succ}^{CDH}_{\mathbb{G}_1,\mathcal{A}}(\ell)$ is negligible.

2.2 Identity-based Cryptography

The idea of ID-based system was proposed by Shamir in [11]. In this system, the public key is the identity information of each user. In other words, the user's public key can be calculated directly from his/her identity rather than being extracted from a certificate issued by a certificate authority (CA). ID-based public key setting can be a good alternative for certificate-based public key setting, especially when efficient key management and moderate security are required. The construction of identity based signature scheme was also proposed in [11], but the first efficient construction of ID-based encryption scheme was proposed in [3] that was developed using bilinear pairings.

2.3 Notations

Throughout this paper, we will use the following notations. Let $|q|$ denote the length of q in bits. Let $[m]^{k_1}$ denote the most significant k_1 bits of m and $[m]_{k_2}$ denote the least significant k_2 bits of m.

3 Identity-based Message Recovery Signatures

3.1 Model

There exists a trusted Private Key Generator (PKG) in the system. An ID-based message recovery signature scheme consists of four algorithms.

- Setup: A deterministic algorithm that is on input a PKG's secret key, s_{PKG}, outputs the PKG's public key, P_{pub}, together with the system parameters, `param`.
- Extract: A deterministic algorithm that is on input an identity of a user, ID, outputs a user's secret key, $\mathcal{S}_{\mathsf{ID}}$.
- Sign: A probabilistic algorithm that accepts a message m, an identity ID and his/her secret key $\mathcal{S}_{\mathsf{ID}}$, outputs a signature σ on m.
- Verify: A deterministic algorithm that accepts an identity of the sender, ID and a signature σ, outputs either `true` or $\perp$ to indicate whether the verification is successful or not. When the output is `true`, the original message m can be reconstructed.

Consistency
For consistency of the scheme, we require

$$Pr\left(\begin{array}{l}(\mathtt{true}, m) \leftarrow \mathsf{Verify}(\sigma, \mathsf{ID});\\ \sigma \leftarrow \mathsf{Sign}(\mathsf{ID}, \mathcal{S}_{\mathsf{ID}}, m);\\ \mathcal{S}_{\mathsf{ID}} \leftarrow \mathsf{Extract}(\mathsf{ID})\end{array}\right) = 1$$

holds with an overwhelming probability.

3.2 Formal Security Notion

We provide a formal definition of existential unforgeability of an ID-based message recovery signature scheme under a chosen message attack. To do this, we extend the definition of existential unforgeability against a chosen message attack of [6]. Our extension is strong enough to capture an adversary who can simulate and observe the scheme. It is defined using the following game between an adversary $\mathcal{A}$ and a challenger $\mathcal{C}$.

- Setup: $\mathcal{C}$ runs Setup for a given security parameter ℓ to obtain description of $\mathcal{U} = \{\mathsf{ID}_1, \mathsf{ID}_2, \cdots, \mathsf{ID}_{2^\ell}\}$ and the parameter setup `param`. The public key of the PKG, P_{pub}, is also obtained. The associated PKG's secret key is kept by $\mathcal{C}$.
- Extract Queries: $\mathcal{A}$ can request the private key corresponding to any identity, $\mathsf{ID}_i \in \mathcal{U}$. In response, $\mathcal{C}$ outputs the associated secret key $\mathcal{S}_{\mathsf{ID}_i}$.
- Sign Queries: $\mathcal{A}$ can request a signature on a message m for an identity $\mathsf{ID}_i \in \mathcal{U}$. In responds, $\mathcal{C}$ outputs a signature σ for the message m.
- Verify Queries: Answers to these queries are not provided by $\mathcal{C}$ since $\mathcal{A}$ can compute them for himself using the Verify algorithm.
- Output: Finally, $\mathcal{A}$ outputs a signature σ (for a message m), along with a valid identity $\mathsf{ID}_i \in \mathcal{U}$, which was supposed to be the signer. $\mathcal{A}$ wins the game if $\mathsf{Verify}(\mathsf{ID}_i, \sigma) \stackrel{?}{=} \mathtt{true}$ holds, and no Sign Queries have been asked on the message m, for the identity ID_i and no Extract Queries have been asked on the identity ID_i.

The success probability of an adversary to win the game is defined by

$$\mathtt{Succ}_{\mathcal{A}}^{UF-IDMRSS-CMA}(\ell).$$

Definition 2. *We say that an ID-based message recovery signature scheme is existentially unforgeable under a chosen message attack if the probability of success of any polynomially bounded adversary in the above game is negligible. In other words,*

$$\mathtt{Succ}_{\mathcal{A}}^{UF-IDMRSS-CMA}(\ell) \leq \epsilon$$

3.3 A Concrete Scheme from Bilinear Pairing

In this section, we present a concrete ID-based message recovery signature scheme from bilinear pairing. Our scheme can be regarded as the ID-based version of Abe-Okamoto's scheme [1]. The scheme is illustrated as follows.

- Setup: PKG chooses a random number $s \in \mathbb{Z}_q^*$ and sets $P_{pub} = sP$. PKG also publishes system parameters $\{\mathbb{G}_1, \mathbb{G}_2, \hat{e}, q, \lambda, P, H_0, H_1, F_1, F_2, k_1, k_2\}$, and keeps s as the *master-key*, which is known only by itself. Here $|q| = k_1 + k_2$, $H_1 : \{0,1\}^* \to \mathbb{Z}_q^*$, $H_0 : \{0,1\}^* \to \mathbb{G}_1^*$, $F_1 : \{0,1\}^{k_2} \to \{0,1\}^{k_1}$ and $F_2 : \{0,1\}^{k_1} \to \{0,1\}^{k_2}$ are four cryptographic hash functions.
- Extract: A user submits his/her identity information ID to PKG. PKG computes the user's public key as $\mathsf{Q_{ID}} = H_2(\mathsf{ID})$, and returns $\mathcal{S}_{\mathsf{ID}} = s\mathsf{Q_{ID}}$ to the user as his/her private key.
- Sign: Let the message be $m \in \{0,1\}^{k_2}$.
  S1 Compute $v = e(P,P)^k$, where $k \in_R \mathbb{Z}_q^*$
  S3 $f = F_1(m)||(F_2(F_1(m)) \oplus m)$
  S3 $r = H_1(v) + f \pmod q$
  S4 $U = kP - r\mathcal{S}_{\mathsf{ID}_A}$.
  The signature is (r, U). We note the length of the signature is $|r + U| = |q| + |\mathbb{G}_1|$. This signature can be used to recover the message m, where $|m| = k_2$.
- Verification: Given ID_A, a message m, and a signature (r, U), compute

$$r - H_1(\hat{e}(U, P)\hat{e}(\mathsf{Q}_{\mathsf{ID}_A}, P_{pub})^r) = f,$$

  and

$$m = [f]_{k_2} \oplus F_2([f]^{k_1}).$$

  Check whether $[f]^{k_1} = F_1(m)$ holds. If it is correct, then accept this signature and output `true`. Otherwise, output $\perp$.

3.4 Security Analysis

Theorem 1. *Our ID-based message recovery signature scheme is correct and sound.*

Proof. The correctness of the scheme is justified as follows.

$$\begin{aligned}
\hat{e}(U, P)\hat{e}(\mathsf{Q}_{\mathsf{ID}_A}, P_{pub})^r &= \hat{e}(kP - r\mathcal{S}_{\mathsf{ID}_A}, P)\hat{e}(\mathsf{Q}_{\mathsf{ID}_A}, P_{pub})^r \\
&= \hat{e}(kP - r\mathcal{S}_{\mathsf{ID}_A}, P)\hat{e}(s\mathsf{Q}_{\mathsf{ID}_A}, P)^r \\
&= \hat{e}(kP - r\mathcal{S}_{\mathsf{ID}_A}, P)\hat{e}(r\mathcal{S}_{\mathsf{ID}_A}, P) \\
&= \hat{e}(kP, P) \\
&= \hat{e}(P, P)^k
\end{aligned}$$

Hence, we obtain

$$\begin{aligned} r - H_1(\hat{e}(U,P)\hat{e}(\mathsf{Q}_{\mathsf{ID}_A}, P_{pub})^r) &= r - H_1(\hat{e}(P,P)^k) \\ &= r - H_1(v) \\ &= f \end{aligned}$$

Since f is computed from $f = F_1(m)||(F_2(F_1(m)) \oplus m)$, therefore testing whether

$$\begin{aligned} [r - H_1(\hat{e}(U,P)\hat{e}(\mathsf{Q}_{\mathsf{ID}_A}, P_{pub})^r)]^{k_1} &= [f]^{k_1} \\ &= F_1(m) \end{aligned}$$

should hold with equality. This way, we obtain $[f]^{k_1} = F_1(m)$. Finally, to recover the message from the signature, we can compute

$$\begin{aligned} m &= [f]_{k_2} \oplus F_2([f]^{k_1}) \\ &= [(F_1(m)||(F_2(F_1(m)) \oplus m))]_{k_2} \oplus F_2([f]^{k_1}) \\ &= F_2(F_1(m)) \oplus m \oplus F_2([f]^{k_1}) \\ &= F_2(F_1(m)) \oplus m \oplus F_2(F_1(m)) \\ &= m \end{aligned}$$

□

Theorem 2. *Our ID-based message recovery signature scheme is existentially unforgeable under a chosen message attack in the random oracle model, assuming the hardness of Computational Diffie-Hellman problem.*

Proof. See Appendix.

3.5 Efficiency and Limitation

The length of the signature produced by our scheme is $|r + U| = |q| + |\mathbb{G}_1|$. This signature can be used to sign (and recover) the message m, where $|m| = k_2$. Using any of the families of curves described in [5], one can select p to be a 170-bit prime and use a group $\mathbb{G}_1$ where each element is 171 bits. Hence, the total signature length is 341 bits or 43 bytes. With these parameters, security is approximately the same as a standard 1024-bit RSA signature, which is 128 bytes. This signature scheme can be used to recover a message m where $|m| = k_2$ and $|q| = k_1 + k_2$. The overhead of this scheme is $|q| + |\mathbb{G}_1| - k_2 = |\mathbb{G}_1| + k_1$. To obtain a 2^{-80} probability of the verification condition holding for an attempted forgery generated by an adversary, we need to have $k_1 \leq 80$ bits. Hence, if $|\mathbb{G}_1|$ is chosen to be 171 bits, we obtain the signature overhead as 251 bits. We note that the previous pairing ID-based signature schemes normally requires two elements of $\mathbb{G}_1$, which is approximately 340 bits. The only limitation in this scheme is the message size $|m|$ is limited to be k_2. In the next section, we will eliminate this problem by proposing an ID-based partial message recovery signature scheme.

4 Identity-based Partial Message Recovery Signatures

4.1 Model

There exists a trusted PKG in the system. An ID-based message recovery signature scheme consists of four algorithms.

- Setup: A deterministic algorithm that is on input a PKG's secret key, s_{PKG}, outputs the PKG's public key, P_{pub}, together with the system parameters, `param`.
- Extract: A deterministic algorithm that is on input an identity of a user, ID, outputs a user's secret key, $\mathcal{S}_{\mathsf{ID}}$.
- Sign: A probabilistic algorithm that accepts a message m, an identity ID and his/her secret key $\mathcal{S}_{\mathsf{ID}}$, outputs a signature σ on m and a partial message m_1.
- Verify: A deterministic algorithm that accepts an identity of the sender, ID, a partial message m_1 and a signature σ, outputs either `true` or $\perp$ to indicate whether the verification is successful or not. If the output is `true`, outputs the complete message m.

Consistency
For consistency of the scheme, we require

$$Pr\left(\begin{array}{l}(\mathtt{true}, m) \leftarrow \mathsf{Verify}(m_1, \sigma, \mathsf{ID});\\ (\sigma, m_1) \leftarrow \mathsf{Sign}(\mathsf{ID}, \mathcal{S}_{\mathsf{ID}}, m);\\ \mathcal{S}_{\mathsf{ID}} \leftarrow \mathsf{Extract}(\mathsf{ID})\end{array}\right) = 1$$

holds with an overwhelming probability.

4.2 Formal Security Notion

In this section, we provide a formal security notion for an ID-based partial message recovery scheme. We provide a formal definition of existential unforgeability of an ID-based partial message recovery signature scheme under a chosen message attack, which is similar to the notion of existential unforgeability of an ID-based message recovery signature. It is defined using the following game between an adversary $\mathcal{A}$ and a challenger $\mathcal{C}$.

- Setup: $\mathcal{C}$ runs Setup for a given security parameter ℓ to obtain description of $\mathcal{U} = \{\mathsf{ID}_1, \mathsf{ID}_2, \cdots, \mathsf{ID}_{2^\ell}\}$ and the parameter setup `param`. The public key of the PKG, P_{pub}, is also obtained. The associated PKG's secret key is kept by $\mathcal{C}$.
- Extract Queries: $\mathcal{A}$ can request the private key corresponding to any identity, $\mathsf{ID}_i \in \mathcal{U}$. In response, $\mathcal{C}$ outputs the associated secret key $\mathcal{S}_{\mathsf{ID}_i}$.
- Sign Queries: $\mathcal{A}$ can request a signature on a message m for an identity $\mathsf{ID}_i \in \mathcal{U}$. In responds, $\mathcal{C}$ outputs a signature σ and a partial message m_1.
- Verify Queries: Answers to these queries are not provided by $\mathcal{C}$ since $\mathcal{A}$ can compute them for himself using the Verify algorithm.

– Output: Finally, $\mathcal{A}$ outputs a signature σ (for a message m) and a partial message m_1, along with a valid identity $\mathsf{ID}_i \in \mathcal{U}$, which was supposed to be the signer. $\mathcal{A}$ wins the game if $\mathsf{Verify}(m_1, \sigma, \mathsf{ID}_i) \stackrel{?}{=} \mathtt{true}$ holds, and no Sign Queries have been asked on the message m, for the identity ID_i and no Extract Queries have been asked on the identity ID_i.

The success probability of an adversary to win the game is defined by

$$\mathtt{Succ}_{\mathcal{A}}^{UF-IDPMRSS-CMA}(\ell).$$

Definition 3. *We say that an ID-based partial message recovery signature scheme is existentially unforgeable under a chosen message attack if the probability of success of any polynomially bounded adversary in the above game is negligible. In other words,*

$$\mathtt{Succ}_{\mathcal{A}}^{UF-IDPMRSS-CMA}(\ell) \leq \epsilon$$

4.3 A Concrete Scheme from Bilinear Pairing

– Setup: PKG chooses a random number $s \in Z_q^*$ and sets $P_{pub} = sP$. PKG also publishes system parameters $\{\mathbb{G}_1, \mathbb{G}_2, \hat{e}, q, \lambda, P, H_0, H_1, F_1, F_2, k_1, k_2\}$, and keeps s as the *master-key*, which is known only by itself. Here $|q| = k_1 + k_2$, $H_1 : \{0,1\}^* \to Z_q^*$, $H_0 : \{0,1\}^* \to \mathbb{G}_1^*$, $F_1 : \{0,1\}^{k_2} \to \{0,1\}^{k_1}$ and $F_2 : \{0,1\}^{k_1} \to \{0,1\}^{k_2}$ are four cryptographic hash functions.
– Extract: A user submits his/her identity information ID to PKG. PKG computes the user's public key as $\mathsf{Q}_{\mathsf{ID}} = H_2(\mathsf{ID})$, and returns $\mathcal{S}_{\mathsf{ID}} = s\mathsf{Q}_{\mathsf{ID}}$ to the user as his/her private key.
– Sign: Let the message be $m = m_2 \parallel m_1$, here $m_2 \in \{0,1\}^{k_2}$.
S1 Compute $v = e(P,P)^k$, where $k \in_R Z_q^*$
S3 $f = F_1(m_2)||(F_2(F_1(m_2)) \oplus m_2)$
S3 $r = H_1(v) + f \pmod q$
S4 $c = H_1(m_1 \parallel r)$
S5 $U = kP - c\mathcal{S}_{\mathsf{ID}_A}$.
The signature is (m_1, r, U). We note that the size of the message-signature pair is $|m_1 + r + U|$, which is $|m_1| + |q| + |\mathbb{G}_1|$.
– Verify: Given ID_A, a partial message m_1, and a signature (r, U), compute

$$r - H_1(\hat{e}(U,P)e(\mathsf{Q}_{\mathsf{ID}_A}, P_{pub})^{H_1(m_1\|r)}) = f.$$

and

$$m_2 = [f]_{k_2} \oplus F_2([f]^{k_1}).$$

Check whether $[f]^{k_1} \stackrel{?}{=} F_1(m_2)$ holds. If it holds with an equality, then accept this signature and output $\mathtt{true}$ and output the complete message $m = m_1 \parallel m_2$. Otherwise, output $\perp$.

4.4 Security Analysis

Theorem 3. *Our ID-based partial message recovery scheme is complete and sound.*

Proof. The correctness of the scheme is justified as follows.

$$\begin{aligned}
\hat{e}(U,P)\hat{e}(\mathsf{Q}_{\mathsf{ID}_A}, P_{pub})^{H_1(m_1\|r)} &= \hat{e}(kP - c\mathcal{S}_{\mathsf{ID}_A}, P)\hat{e}(\mathsf{Q}_{\mathsf{ID}_A}, sP)^{H_1(m_1\|r)} \\
&= \hat{e}(kP - c\mathcal{S}_{\mathsf{ID}_A}, P)\hat{e}(\mathsf{Q}_{\mathsf{ID}_A}, sP)^{c} \\
&= \hat{e}(kP - c\mathcal{S}_{\mathsf{ID}_A}, P)\hat{e}(cs\mathsf{Q}_{\mathsf{ID}_A}, P) \\
&= \hat{e}(kP - c\mathcal{S}_{\mathsf{ID}_A}, P)\hat{e}(c\mathcal{S}_{\mathsf{ID}_A}, P) \\
&= \hat{e}(kP, P) \\
&= \hat{e}(P,P)^k
\end{aligned}$$

Obtaining this value, we can compute

$$\begin{aligned}
r - H_1(\hat{e}(U,P)e(\mathsf{Q}_{\mathsf{ID}_A}, P_{pub})^{H_1(m_1\|r)}) &= r - H_1(\hat{e}(P,P)^k) \\
&= r - H_1(v) \\
&= f
\end{aligned}$$

Since $f = F_1(m_2)||(F_2(F_1(m_2)) \oplus m_2)$, then testing $[f]^{k_1} \stackrel{?}{=} F_1(m_2)$ must hold with equality. Therefore, we obtain $F_2([f]^{k_1}) = F_2(F_1(m_2))$. Hence, to recover the message, we can compute

$$\begin{aligned}
m_2 &= [f]_{k_2} \oplus F_2([f]^{k_1}) \\
&= [f]_{k_2} \oplus F_2(F_1(m_2)) \\
&= [F_1(m_2)||(F_2(F_1(m_2)) \oplus m_2)]_{k_2} \oplus F_2(F_1(m_2)) \\
&= (F_2(F_1(m_2)) \oplus m_2) \oplus F_2(F_1(m_2)) \\
&= m_2
\end{aligned}$$

The complete message is recovered as $m = m_1 \parallel m_2$. □

Theorem 4. *Our ID-based message recovery signature scheme is existentially unforgeable under a chosen message attack in the random oracle model, assuming the hardness of Computational Diffie-Hellman problem.*

Proof. The proof is similar to the proof of Theorem 2 and therefore it is omitted. □

4.5 Efficiency

The length of the signature of the scheme presented in this section is $|m_1 + r + U|$, which equal to $|m_1| + |q| + |\mathbb{G}_1|$. The scheme can be used to recover a message m of arbitrary length, where m is represented as $m = m_1||m_2$. Using any of the families of curves described in [5], one can select p to be a 170-bit prime

and use a group $\mathbb{G}_1$ where each element is 171 bits. Hence, the total signature length is $|m_1| + 341$ bits or $\frac{|m_1|}{8} + 43$ bytes. With these parameters, security is approximately the same as a standard 1024-bit RSA signature, which is 128 bytes. We note that the overhead of our second scheme is identical to our first scheme.

5 Conclusion

In this paper, we presented the first ID-based short signature schemes. Our schemes are essentially ID-based message recovery signature schemes and ID-based partial message recovery signature schemes. The construction has opened a new area of research, namely how to shorten ID-based signature schemes. Unlike the previous contributions in constructing short signature schemes, our schemes *are ID-based*. We presented concrete schemes for ID-based message recovery signature scheme and ID-based partial message recovery signature scheme. The efficiency of both algorithms are as follows.

	Scheme 1	*Scheme 2*
Total Length	$\|q\| + \|\mathbb{G}_1\|$	$\|m_1\| + \|q\| + \|\mathbb{G}_1\|$
Signature Length in Practice	341 bits	$\|m_1\| + 341$ bits
Maximum size of m	k_2	arbitrary length

Acknowledgement. The authors would like to thank the anonymous referees of Financial Cryptography & Data Security 2005 for the suggestions to improve this paper.

References

1. M. Abe and T. Okamoto. A Signature Scheme with Message Recovery as Secure as Discrete Logarithm. *Advances in Cryptology - Asiacrypt 1999, Lecture Notes in Computer Science 1716*, pages 378 – 389, Springer-Verlag, Berlin, 1999.
2. D. Boneh and X. Boyen. Short Signatures Without Random Oracles. *Advances in Cryptology - Eurocrypt 2004, Lecture Notes in Computer Science 3027*, pages 56–73, Springer-Verlag, Berlin, 2004.
3. D. Boneh and M. Franklin. Identity-based encryption from the Weil pairing. *Lecture Notes in Computer Science 2139*, pages 213+, Springer-Verlag, Berlin, 2001.
4. D. Boneh, C. Gentry, B. Lynn, and H. Shacham. Aggregate and Verifiable Encrypted Signatures from Bilinear Maps. *Proceedings of Eurocrypt 2003, Lecture Notes in Computer Science 2656*, pages 416 – 432, Springer-Verlag, Berlin, 2003.
5. D. Boneh, B. Lynn, and H. Shacham. Short signatures from the weil pairing. *Asiacrypt 2000, Lecture Notes in Computer Science*, pages 514–532, Springer-Verlag, Berlin, 2001.
6. S. Goldwasser, S. Micali, and R. L. Rivest. A digital signature scheme secure against adaptive chosen-message attacks. *SIAM Journal of Computing*, 17/2:281–308, 1988.

7. D. Naccache and J. Stern. Signing on a Postcard. *Financial Cryptography (FC2000), Lecture Notes in Computer Science 1962*, pages 121 – 135, Springer-Verlag, Berlin, 2000.
8. K. Nyberg and R. Rueppel. A New Signature Scheme based on the DSA, Giving Message Recovery. *Proceedings of the 1st ACM conference on communications and computer security*, pages 58 – 61, 1993.
9. D. Pointcheval and J. Stern. Security Proofs for Signature Schemes. *Advanced in Cryptology - Eurocrypt 1996, Lecture Notes in Computer Science 1070*, pages 387 – 398, Springer-Verlag, Berlin, 1996.
10. D. Pointcheval and J. Stern. Security arguments for digital signatures and blind signatures. *Journal of Cryptology*, 13(3):361–396, 2000.
11. A. Shamir. Identity-based cryptosystems and signature schemes. *Advances in Cryptology - Crypto '84, Lecture Notes in Computer Science 196*, pages 47–53, Springer-Verlag, Berlin, 1985.
12. R. Steinfeld, L. Bull, H. Wang, and J. Pieprzyk. Universal designated-verifier signatures. *Proceedings of Asiacrypt 2003, Lecture Notes in Computer Science 2894*, pages 523 – 543, Springer-Verlag, Berlin, 2003.
13. F. Zhang, R. Safavi-Naini, and W. Susilo. An Efficient Signature Scheme from Bilinear Pairings and Its Applications. *Public Key Cryptography (PKC) 2004, Lecture Notes in Computer Science 2947*, pages 277 – 290, Springer-Verlag, Berlin, 2004.

Appendix

Proof of Theorem 2. We will incorporate the idea of the proof of unforgeability of Schnorr signature scheme by Pointcheval and Stern [10], and use of the forking lemma [10, 9]. The forking lemma states that if E is a polynomial time Turing machine with input only public data, which produces, in time τ and with probability $\eta \geq 10(\mu_s+1)(\mu_s+\mu)/2^\ell$ where ℓ is a security parameter, μ is the number of hash queries and μ_s is the number of signature queries, then there exists an algorithm A which controls E and replaces E's interaction with the signer and produces two valid signatures in expected time at most $\tau' = 120686\mu_s\tau/\eta$.

We will show that our scheme is existentially unforgeable under a chosen message attack in the random oracle model by simulating the interaction of the adversary $\mathcal{A}$ with an algorithm $\mathcal{B}$. We will show how to build an algorithm $\mathcal{B}$ that uses $\mathcal{A}$ to solve an instance of CDH problem. $\mathcal{B}$ simulates the random oracles and the challenger $\mathcal{C}$ in the game with $\mathcal{A}$. $\mathcal{B}$'s goal is to compute abP given aP and bP. In the sense of the simulation below, $\mathcal{B}$'s goal is to compute the secret key of ID_x, namely $\mathcal{S}_{\mathsf{ID}_x}$, where $\mathcal{S}_{\mathsf{ID}_x} = s\mathsf{Q}_{\mathsf{ID}_x}$. Let $\mathsf{Q}_{\mathsf{ID}_x}$ denote aP and $P_{pub} = sP$ denote bP. Then, the purpose is to compute $\mathcal{S}_{\mathsf{ID}_x} = s\mathsf{Q}_{\mathsf{ID}_x} = abP$ in polynomial time by using $\mathcal{A}$.

Simulation: $\mathcal{B}$ provides the required parameters `param` to $\mathcal{A}$. $\mathcal{B}$ generates a set of participants $\mathcal{U}$, where $|\mathcal{U}| = \rho(\ell)$ and ρ is a polynomial function of the security parameter ℓ. Each participant has his/her own identity, $\mathsf{ID}_i \in \mathcal{U}$, as his/her public key, and the associated secret key $\mathcal{S}_{\mathsf{ID}_i} = sP$, kept by $\mathcal{B}$. $\mathcal{B}$ guesses that $\mathcal{A}$ will select ID_α in the position of ID_x, and hence, $\mathcal{B}$ sets $\mathsf{ID}_\alpha = \mathsf{ID}_x$, or $\mathsf{ID}_\alpha = \mathsf{ID}$ for short. $\mathcal{A}$ is given all the public parameters together with all the identities of

the participants. Now, $\mathcal{B}$ simulates the challenger by simulating all the oracles which $\mathcal{A}$ can query as follows.

- F_1 **Queries:** $\mathcal{A}$ can query the random oracle F_1 at any time. $\mathcal{B}$ simulates the random oracle by keeping a list of tuples (M_i, r_i) which is called the $F_1 - list$. When the oracle is queried with an input M_i, $\mathcal{B}$ responds as follows.
  1. If the query M_i is already on the $F_1 - list$, then $\mathcal{B}$ retrieves (M_i, r_i) and outputs r_i.
  2. Otherwise, $\mathcal{B}$ selects a random $r \in \{0,1\}^{k_1}$, outputs r and records (M_i, r) to the $F_1 - list$.
- F_2 **Queries:** $\mathcal{A}$ can query the random oracle F_2 at any time. $\mathcal{B}$ simulates the oracle F_2 in the same way as the F_1 oracle, keeping an $F_2 - list$ of tuples.
- H_0 **and** H_1 **Queries:** $\mathcal{A}$ can query the random oracles H_0 and H_1 at any time. $\mathcal{B}$ simulates the oracles H_0 and H_1 in the same way as the F_1 oracle, keeping an $H_0 - list$ and $H_1 - list$ of tuples.
- **Extract Queries:** $\mathcal{A}$ can request the private key for any identity $\mathsf{ID}_i \in \mathcal{U}$. If $\mathsf{ID}_i = \mathsf{ID}_\alpha$, then $\mathcal{B}$ terminates the simulation with $\mathcal{A}$ having failed to guess the correct challenge identity. The probability of this failure is $\frac{1}{\rho(\ell)}$. Otherwise, $\mathcal{B}$ returns the appropriate private key $\mathcal{S}_{\mathsf{ID}_i} = s\mathsf{Q}_{\mathsf{ID}_i}$.
- **Sign Queries:** $\mathcal{B}$ simulates the signing oracle by accepting signature queries of the form (m, ID_i). If $\mathsf{ID}_i \neq \mathsf{ID}_\alpha$, then $\mathcal{B}$ computes the signature as normal, i.e. by executing $\mathsf{Sign}(m, \mathsf{ID}_i)$ to produce a signature σ. Otherwise, $\mathcal{B}$ terminates the simulation with $\mathcal{A}$ having failed to guess the correct challenge identity. The probability of this failure is $\frac{1}{\rho(\ell)}$.
- **Output:** Finally, with a non-negligible probability, $\mathcal{A}$ outputs a signature σ for the message m and ID_α, where this signature has never been queried before.

Then, $\mathcal{B}$ restarts all his list and run the above game for the second time. With a non-negligible probability, $\mathcal{B}$ will obtain two different signatures for the same message and ID_α. When this case happens, $\mathcal{B}$ obtains (U, r) and (U', r') that both pass the verification test. Hence,

$$\begin{aligned}
\hat{e}(U, P)\hat{e}(\mathsf{Q}_{\mathsf{ID}_\alpha}, P_{pub})^r &= \hat{e}(U', P)\hat{e}(\mathsf{Q}_{\mathsf{ID}_\alpha}, P_{pub})^{r'} \\
\hat{e}(U, P)\hat{e}(s\mathsf{Q}_{\mathsf{ID}_\alpha}, P)^r &= \hat{e}(U', P)\hat{e}(s\mathsf{Q}_{\mathsf{ID}_\alpha}, P_{pub})^{r'} \\
\hat{e}(U + r\mathcal{S}_{\mathsf{ID}_\alpha}, P) &= \hat{e}(U' + r'\mathcal{S}_{\mathsf{ID}_\alpha}, P)
\end{aligned}$$

From the above equation, we obtain

$$\begin{aligned}
U + r\mathcal{S}_{\mathsf{ID}_\alpha} &= U' + r'\mathcal{S}_{\mathsf{ID}_\alpha} \\
(r - r')\mathcal{S}_{\mathsf{ID}_\alpha} &= (U' - U) \\
\mathcal{S}_{\mathsf{ID}_\alpha} &= (r - r')^{-1}(U' - U)
\end{aligned}$$

which is the solution of the CDH problem. Here, $\mathcal{S}_{\mathsf{ID}_\alpha}$ is $\mathcal{S}_{\mathsf{ID}_x}$, i.e. the CDH problem that $\mathcal{B}$ would like to solve. The probability of the simulation fails is upper bounded by $\frac{2}{\rho(\ell)}$ which is negligible. Hence, we obtain the contradiction. □