Certificateless Designated Verifier Signature Schemes

Xinyi Huang  
*University of Wollongong*

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

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

Futai Zhang  
*Nanjing Normal University*

---

Publication Details

This article was originally published as: Huang, X, Susilo, W, Mu, Y & Zhang, F, Certificateless Designated Verifier Signature Schemes, 20th International Conference on Advanced Information Networking and Applications (AINA 2006), 18-20 April 2006, 2, 15-19. Copyright IEEE 2006.
Certificateless Designated Verifier Signature Schemes

Abstract
Designated verifier signature schemes allow a signer to convince a designated verifier, in such a way that only the designated verifier will believe with the authenticity of such a signature. The previous constructions of designated verifier signature rely on the underlying Public Key Infrastructure, that requires both signer and verifier to verify the authenticity of the public keys, and hence, the certificates are required. In contrast to the previous constructions, in this paper, we propose the first notion and construction of the certificateless designated verifier signature scheme. In our new notion, the necessity of certificates are eliminated. We show that our scheme satisfies all the requirements of the designated verifier signature schemes in the certificateless system. We also provide complete security proofs for our scheme and prove that our scheme is unforgeable under the assumption of the Gap Bilinear Diffie-Hellman Problem in the random oracle model.

Disciplines
Physical Sciences and Mathematics

Publication Details
This article was originally published as: Huang, X, Susilo, W, Mu, Y & Zhang, F, Certificateless Designated Verifier Signature Schemes, 20th International Conference on Advanced Information Networking and Applications (AINA 2006), 18-20 April 2006, 2, 15-19. Copyright IEEE 2006.

This conference paper is available at Research Online: http://ro.uow.edu.au/infopapers/462
Certificateless Designated Verifier Signature Schemes

Xinyi Huang\textsuperscript{1}, Willy Susilo\textsuperscript{1}, Yi Mu\textsuperscript{1} and Futai Zhang\textsuperscript{2}

\textsuperscript{1}School of Information Technology and Computer Science
University of Wollongong, Australia
\textsuperscript{2}College of Mathematics and Computer Science
Nanjing Normal University, P.R. China

Email: xinyinjnu@126.com, wsusilo@uow.edu.au,
ymu@uow.edu.au, zhangfutai@njnu.edu.cn

Abstract: Designated verifier signature schemes allow a signer to convince a designated verifier, in such a way that only the designated verifier will believe with the authenticity of such a signature. The previous constructions of designated verifier signature rely on the underlying Public Key Infrastructure, that requires both signer and verifier to verify the authenticity of the public keys, and hence, the certificates are required. In contrast to the previous constructions, in this paper, we propose the first notion and construction of the certificateless designated verifier signature scheme. In our new notion, the necessity of certificates are eliminated. We show that our scheme satisfies all the requirements of the designated verifier signature schemes in the certificateless system. We also provide complete security proofs for our scheme and prove that our scheme is unforgeable under the assumption of the Gap Bilinear Diffie-Hellman Problem in the random oracle model.

KeyWord: Certificateless Cryptography, Designated Verifier, Gap Bilinear Diffie-Hellman Problem

I. INTRODUCTION

In a designated verifier signature scheme, the signature provides authentication of a message without providing a non-repudiation property of traditional signatures. A designated verifier scheme can be used to convince a single party, i.e., the designated verifier, and only this designated verifier who can be convinced about its validity or invalidity of the signatures, due to the fact that the designated verifier can always construct a signature intended for himself that is indistinguishable from an original signature. This kind of signature has numerous applications, for example, call for tenders, electronic voting, electronic auction, and distributed contract signing. Some recent works about the designated verifier signature are given in [5]–[10]. The first construction of the identity-based designated verifier signature scheme was proposed in [12]. In the identity-based setting, the public key is the identity of the participants themselves. However, in the latter setting, the trusted authority, known as the Private Key Generator (PKG), can always impersonate any user, and hence, the problem of key escrow is inherent in this setting.

Certificateless Cryptography was first proposed by Al-Riyami and Paterson [1] in Asiacrypt 2003. In contrast to the traditional cryptography, this notion does not require the use of any certificate to ensure the authenticity of public keys. Instead, certificateless cryptography relies on the existence of a trusted third party KGC who has the master key. In this sense, it is similar to identity-based cryptography [11]. Nevertheless, certificateless cryptography does not suffer from the key escrow property that seems to be inherent in identity-based cryptography. In the certificateless system, KGC only knows the partial private key of the user and the user must use the secret value, which is chosen by the user himself, to obtain the full private key. For more about the certificateless system, one can refer the paper [1]. Some recent works about the certificateless system are given in [2]–[4], [13], [14].

Our Contribution In this paper, we propose the first notion and construction of the certificateless designated verifier (or CLDVS for short) signature scheme. We also provide a formal definition of the certificateless designated verifier signature. Our scheme is very efficient. Nevertheless, as we shall show in this paper, our scheme achieves all the required properties of the certificateless designated verifier signature. We provide security proofs for our scheme based on the random oracle model.

Roadmap In the next section, we will review some preliminaries required throughout the paper. In Section III, we describe our certificateless designated verifier signature. The security analysis is also given in the Section IV. At last, Section V concludes the paper.

II. PRELIMINARIES

A. Bilinear Pairing

Let \( G_1 \) denote an additive group of prime order \( q \) and \( G_2 \) be a multiplicative group of the same order. Let \( P \) denote a generator in \( G_1 \). Let \( e : G_1 \times G_1 \rightarrow G_2 \) be a bilinear mapping defined in [1].

Definition 1: Bilinear Diffie-Hellman (BDH) Problem.

Given a randomly chosen \( P \in G_1 \), as well as \( aP, bP, cP \) (for unknown randomly chosen \( a, b, c \in \mathbb{Z}_q^* \)), compute \( e(P, P)^{abc} \).

This work is supported by ARC Discovery Grant DP0557493, Ministry of Education of Jiangsu Province Grant 03KJA520066 and Xidian University’s Open Grant of Key Laboratory on Computer Network and Information Security of Ministry of Education of China.
Type I Adversary: This type of adversary $A_I$ has access to the master-key but cannot perform public keys replacement. Given the public keys of the signer (and the receiver), system parameter and the system’s master-key, a type II adaptively chosen-message attacker $A_{II}$ can ask the sign oracle and verify the oracle in the polynomial time adaptively. At last $A_{II}$ outputs a message-signature pair. $A_{II}$ is successful if the message has not been submitted to the sign oracle and the message-signature pair is valid.

Definition 4: A certificateless designated verifier signature scheme is existential unforgeable against adaptively chosen-message attacks iff it is secure against both types of adversaries.

III. OUR SCHEME

In this section, we will propose our certificateless designated verifier signature scheme (CLDVS). We regard it as the main result of this paper. There are two parties in our scheme, the sender $A$ and the designated verifier $B$, all the algorithms are described as follows.

• Setup: This algorithm runs as follows.
  1) Run $\mathcal{G}$ on input $\ell$ to generate $(G_1, G_2, e)$ where $G_1$ and $G_2$ are groups of some prime order $q$ and $e: G_1 \times G_1 \rightarrow G_2$ is a bilinear pairing.
  2) Select a random generator $P \in G_1$.
  3) Select a master-key $s$ randomly from $Z_q^*$ and set $P_0 = sp$.
  4) Select cryptographic hash functions $H_1: \{0, 1\}^* \rightarrow G_1^*$ and $H_2: \{0, 1\}^* \times G_2 \rightarrow Z_q$.

• Partial-Private-Key-Extract: This algorithm accepts an identity $ID_i \in \{0, 1\}^*$, $i \in \{A, B\}$ and constructs the partial private key for the user as follows.
  1) Compute $Q_i = H_i(ID_i)$.
  2) Output the partial private key $D_i = sQ_i$.

• Set-Secret-Value: This algorithm takes as inputs param and the user’s identity $ID_i$, and selects a random $x_i \in Z_q^*$ and outputs $x_i, i \in \{A, B\}$ as the user’s secret value. That is the sender $A$ randomly chooses $x_A \in Z_q^*$ and the designated verifier $B$ randomly chooses $x_B \in Z_q^*$.

• Set-Private-Key: This algorithm accepts param, a user’s partial private key $D_i$ and the user’s secret value $x_i \in Z_q^*$ to transform the partial private key $D_i$ to a full private key $S_i$ by computing $S_i = x_iD_i = x_isQ_i$ and output $S_i, i \in \{A, B\}$.

Proceedings of the 20th International Conference on Advanced Information Networking and Applications (AINA’06) 1550-445X/06 © 2006 IEEE
$S_B = x_B s_B$ and public key $P_B = (X_B, Y_B) = (x_B P, x_B P_0)$.

- Sign: To sign a message $m \in M$ for $B$, the signer $A$ computes the signature $\sigma = H_2(m)[e(S_A, x_A^3 Q_B + X_B)]$.
- Verify: To verify a signature $\sigma$ on a message $m \in M$ from an identity $ID_A$ and public key $(X_A, Y_A)$, $B$ performs the following steps.
  1. Verify whether $e(X_A, P_0) = e(Y_A, P)$ holds with equality. If not, then output $\bot$ and abort.
  2. Verify whether $\sigma = H_2(m)[e(Q_A, D_B + x_B Y_A)]$ holds with equality. If it does, output true. Otherwise, output $\bot$.

- Transcript-Simulation: $B$ can produce the signature $\hat{\sigma}$ intended for himself, by computing $\hat{\sigma} = H_2(m)[e(Q_A, D_B + \sigma)(x_B Q_A, Y_A)]$.

IV. SECURITY ANALYSIS

**Theorem 1:** Our CLDVS scheme is a designated verifier signature scheme.

**Proof:** We note that the verification algorithm requires $D_B, x_B$, where $D_B$ is the partial private key of the designated verifier $B$ and $x_B$ is the secret value of $B$. Hence, $B$ can always “simulate” a valid signature by producing a valid signature himself. This is achieved by constructing a signature $\hat{\sigma} = H_2(m)[e(Q_A, D_B + x_B Y_A)]$. Note that the signature produced by $B$ is indistinguishable from the one that was produced by the sender $A$. Hence, no third party can be convinced with the validity or invalidity of this signature other than the designated verifier himself. If the designated verifier has not generated such a signature, then he will believe that the signature was indeed generated by the signer $A$.

**Theorem 2:** Let $A_j$ be an active adaptive chosen-message attacker against our CLDVS with success probability greater than $Succ_{CLDVS}(s, A_j)$ after asking $q_B$ queries to the hash function $H_2$, $q_B$ queries to the sign algorithm and $q_V$ queries to the verify algorithm, then there exists an algorithm $B$ who can use $A_j$ to solve a random instance of the GBDH problem with the probability $Succ_{CLDVS}(s, A_j) \geq (1 - \frac{q_B}{q_V}) Succ_{CLDVS}(s, A_j)$, $\ell$ is the security parameter for our CLDVS scheme.

**Proof:** Given a random instance $(P, P_1 = a P, P_2 = b P, P_3 = e P)$ of the Gap Bilinear Diffie-Hellman (GBDH) problem, we will show how $B$ can use $A_j$ to obtain the value of $e(P, P)^{abc}$ with the help of the Decisional Bilinear Diffie-Hellman (DBDH) Oracle. In the proof, we regard the hash function $H_2$ as the random oracle. We assume $A_j$ is well-behaved in the sense that $A_j$ doesn’t repeat any two identical queries.

- Setup: In this game, $B$ will set the system parameters. There are two parts in the proof, the sender $A$ and the designated verifier $B$. $B$ starts by set $Q_A = P_1, Q_B = P_2$ and $P_0 = P_3$ where $(P_1, P_2, P_3)$ is the instance of the Gap Bilinear Diffie-Hellman problem given to $B$. Then the algorithm $B$ also randomly chooses $x_A, x_B \in \mathbb{Z}_q^*$ and sets $P_A = (X_A, Y_A) = (x_A P, x_A P_0)$, $P_B = (X_B, Y_B) = (x_B P, x_B P_0)$. $B$ will return all the parameters to $A_j$.

- Hash Queries: In this game, $B$ will simulate the hash function $H_2$. At any time algorithm $A_j$ can query the random oracle. To respond to these queries algorithm, $B$ maintains a list $H$-list which consists of the tuples $(m_i, r_i, \sigma_i, X_i^A, Y_i^A)$ as described below. The list is initially empty. When $A_j$ queries the oracle $H$ with the request $(m_i, r_i)$, algorithm $B$ checks the $H$-list:
  1. If there is no item $(m_i, \cdot, \cdot, \cdot, \cdot)$ in $H$-list, $B$ will choose a random $\sigma_i \in \mathbb{Z}_q$ such that there is no item $(\cdot, \cdot, \cdot, \cdot, \cdot)$ in the $H$-list. Then $B$ adds $(m_i, r_i, \sigma_i, \bot, \bot)$ into the $H$-list and returns $\sigma_i$ to $A_j$ as the answer. Here the notation $\bot$ means $B$ doesn’t know the corresponding value.
  2. Else, there is an item $(m_i, \cdot, \cdot, \cdot, \cdot)$ in the $H$-list such that $m_i = m_i$.
    a) This item has the form $(m_i, r_j, \cdot, \cdot, \cdot, \cdot)$ such that $r_i \neq r_j$.

  If this case happens, $B$ will choose a random $\sigma_i \in \mathbb{Z}_q$ such that there is no item $(\cdot, \cdot, \cdot, \cdot, \cdot)$ in the H-list. Then $B$ adds $(m_i, r_i, \sigma_i, \bot, \bot)$ into the $H$-list and returns $\sigma_i$ to $A_j$ as the answer.

  b) Otherwise, this item must have the form $(m_i, \bot, \cdot, \cdot, \cdot, \cdot)$ which can only be added into the $H$-list during the Sign Queries.

   i) If $r_i/e(Q_A, x_B Y_A) = e(P, P)^{abc}$, which means $r_i = e(Q_A, D_B + x_B Y_A)$, $B$ rewrites this form as $(m_i, r_i, \sigma_i, X_i^A, Y_i^A)$.

   ii) Else $r_i/e(Q_A, x_B Y_A) \neq e(P, P)^{abc}$, $B$ will choose a random $\sigma_i \in \mathbb{Z}_q$ such that there is no item $(\cdot, \cdot, \cdot, \cdot, \cdot)$ in the $H$-list. Then $B$ adds $(m_i, r_i, \sigma_i, \bot, \bot)$ into the $H$-list and returns $\sigma_i$ to $A_j$ as the answer.

Note that either way $\sigma_i$ is uniform in $\mathbb{Z}_q$ and is independent of $A_j$’s current view as required, so $B$ simulates the hash function perfectly.

- Sign Queries: In this game, $B$ will simulate the sign algorithm. At any time algorithm $A_j$ can query the sign algorithm and $B$ will answer $A_j$’s queries. Since $A_j$ is the type I adversary, $A_j$ can choose the public key $(X_i^A, Y_i^A)$ for the sender $A$. After receiving $A_j$’s choice of the message $m_i$ and the public key $(X_i^A, Y_i^A)$, $B$ checks whether $e(X_i^A, P_0) = e(Y_i^A, P)$. If the equation does not hold, $B$ terminates this query and asks $A_j$ to choose a valid public key. Otherwise, $B$ checks the $H$-list:
  1. If there is no item $(m_j, \cdot, \cdot, \cdot, \cdot, \cdot)$ in $H$-list, $B$ will choose a random $\sigma_i \in \mathbb{Z}_q$ such that there is no item $(\cdot, \cdot, \cdot, \cdot, \cdot)$ in the $H$-list. Then $B$ adds $(m_j, \bot, \sigma_i, X_i^A, Y_i^A)$ into the $H$-list and returns $\sigma_i$ to $A_j$ as the answer.

  2. Else there is an item $(m_j, \cdot, \cdot, \cdot, \cdot, \cdot)$ in the $H$-list such that $m_j = m_i$.
    a) This item has the form $(m_j, \bot, \sigma_i, X_i^A, Y_i^A)$
such that $X_A^j \neq X_A^i$.

If this case happens, $B$ will choose a random $\sigma_i \in Z_q$ such that there is no item $(\cdot, \cdot, \cdot, \cdot)$ in the H-list. Then $B$ adds $(m_i, \bot, \sigma_i, X_A^i, Y_A^i)$ into the H-list and returns $\sigma_i$ to $A_I$ as the answer.

b) Otherwise, this item must have the form $(m_j, r_j, \sigma_j, \bot, \bot)$ which can only be added into the H-list during the Hash Queries.

If this case happens, $B$ will submit $(P, P_s, P_{s'}, r_j/e(A, x_s Y_A^j))$ to the DBDH oracle and the DBDH oracle will tell $B$ whether $r_j/e(A, x_s Y_A^j) = (P, P_s)^{abc}$. $B$ rewrites this form as $(m_j, r_j, \sigma_j, X_A^i, Y_A^i)$. Then $B$ returns $\sigma_j$ as the answer to $A_I$.

ii) Else $r_j/e(A, x_s Y_A^j) \neq (P, P_s)^{abc}$. $B$ will choose a random $\sigma_j \in Z_q$ such that there is no item $(\cdot, \cdot, \cdot, \cdot)$ in the H-list. Then $B$ adds $(m_j, \bot, \sigma_j, X_A^i, Y_A^i)$ into the H-list and returns $\sigma_j$ to $A_I$ as the answer.

- Verify Queries: In this game, $B$ will simulate the verify algorithm. At any time algorithm $A_I$ can query the verify algorithm and $B$ will answer $A_I$'s queries. After receiving $A_I$'s request $(m, \sigma)$ and the sender $A'$'s public key $(X_A^i, Y_A^j)$ chosen by $A_I$, $B$ checks the H-list:

1) If there is no item $(\cdot, \cdot, \cdot, \cdot)$ in the H-list, $B$ rejects $(m, \sigma)$ as an invalid signature.

2) Else, there is an item $(\cdot, \cdot, \cdot, \cdot)$ in the H-list:

a) If this item has the form of $(m_1, \bot, \sigma_1, X_A^1, Y_A^1)$ or $(m_1, r_1, \sigma_1, X_A^1, Y_A^1)$, $B$ will accept it as a valid signature.

b) Else if this item has the form of $(m_i, r_i, \sigma_i, \bot, \bot)$, $B$ will submit $(P, P_s, P_{s'}, r_i/e(A, x_s Y_A^1))$ to the DBDH oracle and the DBDH oracle will tell $B$ whether $r_i/e(A, x_s Y_A^1) = (P, P_s)^{abc}$.

i) If $r_i/e(A, x_s Y_A^1) = (P, P_s)^{abc}$, $B$ will accept it as a valid signature.

ii) Else $r_i/e(A, x_s Y_A^1) \neq (P, P_s)^{abc}$, $B$ rejects it as an invalid signature.

c) Otherwise, $B$ rejects it as an invalid signature.

This simulation works well except that $(m_1, \sigma_1)$ is a valid signature, while $\sigma_1$ is not queried from the random oracle $H$. Since, $H$ is uniformly distributed, this case happens with probability less than $\frac{q_v}{2^w - q_v - q_s}$.

If $B$ doesn’t fail during all the queries, $A_I$ can output a valid message-signature pair $(m^*, \sigma^*)$ under the sender $A'$'s public key $(X_A^i, Y_A^j)$ with probability greater than $\frac{q_v}{2^w - q_v - q_s}$.

Since $(m^*, \sigma^*)$ is a valid message-signature pair, which means there is an item $(\cdot, \cdot, \cdot, \cdot)$ in the H-list. By the definition of the adversary model, $m^*$ can not be queried to the signer oracle, so $\sigma^*$ is returned as the hash value of $A_I$'s query $(m^*, r^*)$. That is to say there is an item $(m^*, r^*, \sigma^*, \bot, \bot)$ in the H-list and $r^*/e(A, x_s Y_A^1) = (P, P_s)^{abc}$. Since $Q_A, x_s Y_A^1, r^*$ are all known to $B$, $B$ can successfully solve this instance of the GBDH problem.

However, the probability $B$ doesn’t fail is greater than $1 - \frac{q_v}{2^w - q_v - q_s}$. Therefore, $B$ can solve this instance of the GBDH problem with the probability: $\frac{q_v}{2^w - q_v - q_s} \cdot \frac{q_v}{2^w - q_v - q_s} \geq (1 - \frac{q_v}{2^w - q_v - q_s}) \cdot \frac{q_v}{2^w - q_v - q_s}$

Theorem 3: Let $A_{II}$ be an type II adaptively chosen-message attacker against our CLDVS with success probability greater than $\frac{q_v}{2^w - q_v - q_s}$, then asking $q_H$ queries to the hash function $h_{2q}$, $q_H$ queries to the sign algorithm and $q_H$ queries to the verify algorithm, then there exists an algorithm $B$ can use $A_{II}$ to solve a random instance of the GBDH problem with the probability $\frac{q_v}{2^w - q_v - q_s} \cdot \frac{q_v}{2^w - q_v - q_s} \geq (1 - \frac{q_v}{2^w - q_v - q_s}) \cdot \frac{q_v}{2^w - q_v - q_s}$.

Proof: Given a random instance $(m, r, s) = (P, P_s, P_{s'}, P)$ of the Gap Bilinear Diffie-Hellman (GBDH) problem, we will show how $B$ can use $A_{II}$ to obtain the value of $e(P, P)^{abc}$ with the help of the Decisional Bilinear Diffie-Hellman (DBDH) Oracle. In the proof, we regard the hash function as the random oracle. We assume $A_{II}$ is well-behaved in the sense that $A_{II}$ doesn’t repeat any two identical queries.

- Setup: In this game, $B$ will set the system parameters. There are two parts in the proof, the sender $A$ and the designated verifier $B$. $B$ starts by set $X_A = P_1, X_B = P_2$ and $Q_A = Q_B$ where $(P_1, P_2, P_3)$ is the instance of the Gap Bilinear Diffie-Hellman problem given to $B$. Then the algorithm $B$ also randomly chooses $s \in Z_q, Q_B \in G_1$ and sets $P_0 = s P, P_1 = (X_A, Y_A) = (P_1, sP), P_2 = (X_B, Y_B) = (P_2, sP)$, $B$ will return all the parameters to $A_I$. Since $A_{II}$ is the type II adversary, $B$ will also send the master-key $s$ to $A_{II}$.

- Hash Queries: In this game, $B$ will simulate the hash function. At any time algorithm $A_{II}$ can query the random oracle $H$. To respond to these queries algorithm $B$ maintains a list $H$-list which consists of the tuples $(m_i, r_i, \sigma_i, a_i)$ as described below. The list is initially empty. When $A_{II}$ queries the oracle $H$ with the request $(m_i, r_i)$, algorithm $B$ submits $(P, P_s, P_{s'}, (r_i)^{a_i}/e(A, Q_B))$ to the DBDH oracle and DBDH oracle will tell $B$ whether $(r_i)^{a_i}/e(A, Q_B) = (P, P_s)^{abc}$:

1) $(r_i)^{a_i}/e(A, Q_B) = (P, P_s)^{abc}$, which means $r_i = e(A, Q_B)e(P, P)^{abc} = e(Q_A, D_B + x_B Y_A)$.

a) If there is no item $(\cdot, \cdot, \cdot, \cdot)$ in the H-list, $B$ will set $c_i = 1$ and choose a random $\sigma_i \in Z_q$ such that there is no item $(\cdot, \cdot, \cdot, \cdot)$ in the H-list.

Then $B$ adds $(m_i, r_i, \sigma_i, 1)$ into the H-list and returns $\sigma_i$ to $A_{II}$ as the answer.

b) Else, there is an item $(m_{j'}, r_{j'}, \cdot, \cdot)$ in the H-list such that $m_i = m_{j'}$. If this item has the form $(m_{j'}, r_{j'}, \cdot, \cdot, \cdot)$ such that $m_i = m_{j'}$, $r_i \neq r_{j'}$, $B$ will set $c_i = 1$ and choose a random $\sigma_i \in Z_q$ such that there is no item $(\cdot, \cdot, \cdot, \cdot)$ in the H-list.

Then $B$ adds $(m_i, r_i, \sigma_i, 1)$ into the H-list and returns $\sigma_i$ to $A_{II}$ as the answer.
c) Otherwise, as described below, this item must have the form \( (m_i, \perp, \sigma_i, 1) \) (item of this form only can be added into the H-list during the Sign Queries). Then \( B \) returns \( \sigma_i \) to \( A_{II} \) as the answer.

2) Otherwise \((v_r)_{i=1}^{q} \neq e(Q_A, Q_B) \neq e(P, P)^{abc} \) \( B \) sets \( c_i = 0 \) and chooses \( \sigma_i \in \mathbb{Z}_q^* \) such that there is no item \((\cdot, \cdot, \cdot, \cdot)\) in the H-list. Then \( B \) adds \((m_i, \perp, \sigma_i, 0)\) into the H-list and returns \( \sigma_i \) to \( A_{II} \) as the answer.

Sign Queries: In this game, \( B \) will simulate the sign algorithm. At any time algorithm \( A_{II} \) can query the sign algorithm and \( B \) will answer \( A_{II}'s \) queries. After receiving \( A_{II}'s \) choice of the message \( m_i \), \( B \) checks the H-list:

1) If \( m_i \) has never been submitted to the hash oracle, \( B \) will set \( c_i = 1 \) and choose \( \sigma_i \in \mathbb{Z}_q^* \) such that there is no item \((\cdot, \cdot, \cdot, \cdot)\) in the H-list. Then \( B \) adds \((m_i, \perp, \sigma_i, 1)\) into the H-list and returns \( \sigma_i \) to \( A_{II} \) as the answer.

2) Else, \( m_i \) has been submitted to the hash oracle. There must be an item \((m_j, r_j, \sigma_j, c_j)\) in the H-list such that \( m_i = m_j \):

a) If \( c_j = 1 \), which means \( r_j = e(Q_A, s_B) (e(P, P)^{abc} = e(Q_A, D_B + x_B Y_A) \), \( B \) returns \( \sigma_i \) to \( A_{II} \) as the answer.

b) Otherwise, \( B \) will set \( c_i = 1 \) and choose a random \( \sigma_i \in \mathbb{Z}_q^* \) such that there is no item \((\cdot, \cdot, \cdot, \cdot)\) in the H-list. Then \( B \) adds \((m_i, \perp, \sigma_i, 1)\) into the H-list and returns \( \sigma_i \) to \( A_{II} \) as the answer.

Verify Queries: In this game, \( B \) will simulate the verify algorithm. At any time algorithm \( A_{II} \) can query the verifying algorithm and \( B \) will answer \( A_{II}'s \) queries. After receiving \( A_{II}'s \) request \((m_i, \sigma_i)\), \( B \) checks the H-list:

1) If there is no item \((\cdot, \cdot, \cdot, \cdot)\) in the H-list, \( B \) rejects \((m_i, \sigma_i)\) as an invalid signature.

2) Else, there is an item \((\cdot, \cdot, \cdot, \cdot)\) in the H-list:

a) If this item has the form \((m_i, \perp, \cdot, 1)\) or \((m_i, r_i, \sigma_i, 1)\), \( B \) will accept it as a valid signature.

b) Otherwise, \( B \) rejects it as an invalid signature.

This simulation works well except that \((m_i, \sigma_i)\) is a valid message-signature pair, while \( \sigma_i \) is not queried from the random oracle \( H \). Since \( H \) is uniformly distributed, this case happens with probability less than \( \frac{q}{2^{\sqrt{2q} - q}} \).

If \( B \) doesn’t fail during all the queries, \( A_{II} \) can output a valid message-signature pair \((m^{*}, \sigma^{*})\) with probability greater than \( Succ_{\text{CLDV\,S,\,A_{II}}}^{\text{CMA}} \). Since \((m^{*}, \sigma^{*})\) is a valid message-signature pair, which means there is an item \((\cdot, \cdot, \cdot, \cdot)\) in the H-list. By the definition of the adversary model, \( m^{*} \) cannot be queried to the sign oracle, so \( \sigma^{*} \) is returned as the hash value of \( A_{II}'s \) query \((m^{*}, r^{*})\). That is to say there is an item \((m^{*}, r^{*}, \sigma^{*}, 1)\) in the H-list and \((r^{*})^{(\cdot, \cdot, \cdot, \cdot)} = e(Q_A, Q_B) = e(P, P)^{abc} \). So if \( B \) doesn’t fail, \( B \) can successfully solves this instance of the GBDH problem with same probability \( Succ_{\text{CLDV\,S,\,A_{II}}}^{\text{CMA}} \).

However, the probability \( B \) doesn’t fail is greater than \( 1 - \frac{q}{2^{\sqrt{2q} - q}} \). Therefore, \( B \) can solve this instance of the GBDH problem with probability \( Succ_{\text{GBDH},\,B}^{\text{CMA}} \geq 1 - \frac{q}{2^{\sqrt{2q} - q}} \).

V. CONCLUSION

In this paper, we proposed the notion of certificateless designated verifier signature scheme and the first construction of the certificateless designated verifier signature scheme. We showed that our scheme satisfies all the requirements of the designated verifier signature schemes. We also provided security proofs for our scheme in the random oracle model and proved that our scheme is unforgeable to both types of adversaries in certificateless model under the assumption of the Gap Bilinear Diffie-Hellman Problem.

Acknowledgement.

The authors would like to express their gratitude thanks to the anonymous referees of the Second International Workshop on Security in Networks and Distributed Systems (SNDS-06) for the suggestions to improve this paper.

REFERENCES


