A Short Identity-based Signcryption Scheme in the Multi-PKG over the VANETs

Jianhong Zhang, Yuanbo Cui and Xiuna Su
1College of Sciences, North China University of Technology, Beijing, China
2Institution of Imagine Process and Pattern Recognition, North China University of Technology, Beijing, 100144, China

Abstract: Signcryption is a novel cryptographic primitive that simultaneously provides the authentication and encryption in a single logic step. In this study, by combining two ID-based signature schemes with a signcryption scheme, we build a security model of ID-based signcryption in the multi-PKG and have proposed an ID-based signcryption scheme in the multi-PKG based on the bilinear pairings to adapt to the different graphical system setting. We prove that our proposed scheme is secure and satisfies the confidentiality and unforgeability. The fixed verification computation is needed in our proposed signcryption, thus, it is very efficient.

Key words: Signcryption, ID-based cryptography, security proof, the CDH problem

INTRODUCTION

A Vehicular Ad-Hoc Network (VANET), is a technology that uses moving cars as nodes in a network to create a mobile network. VANET turns every participating car into a wireless router or node, allowing cars approximately 100 to 300 m of each other to connect and in turn, create a network with a wide range. As cars fall out of the signal range and drop out of the network, other cars can join in, connecting vehicles to one another so that a mobile Internet is created. It is estimated that the first systems that will integrate this technology are police and fire vehicles to communicate with each other for safety purposes.

The attractive features of VANETs inevitably incur higher risks if such networks do not take security into account prior to deployment. For instance, if the safety messages are modified, discarded, or delayed either intentionally or due to hardware malfunctioning, serious consequences such as injuries and even deaths may occur. Unlike traditionally wired networks are protected by several lines of defense such as firewalls and gateways, security attacks on such wireless networks may come from any direction and target all nodes. Therefore, VANETs are susceptible to intruders ranging from passive eavesdropping to active spamming, tampering and interfering due to the absence of basic infrastructure and centralized administration. Moreover, the main challenge facing vehicular ad hoc networks is user privacy. Whenever vehicular nodes attempt to access some services from roadside infrastructure nodes, they want to maintain the necessary privacy without being tracked down for whoever they are, wherever they are and whatever they are doing. It is considered as one of the important security requirements that should be paid more attention for secure VANET schemes, especially in privacy-vital environment. Thus, we adopt signcryption to realize security authentication and secret transmission.

Message security and the sender's identity authentication for communication in the open channel is a basic and important technology of internet. For keeping message confidential and unforgeable, the sender can use a digital signature algorithm with his private key to sign the message, then encrypts the message and its signature by a symmetric encryption algorithm with secret key. The sender encrypts this secret key with using the recipient's public key. The process is a sign-then-encrypt way to realize authentication and encryption. But computational costs and communication overheads are large in this way. Zheng (1997) first proposed a new cryptographic primitive: signcryption, which can perform digital signature and public key encryption in a logic step, at lower computational costs and communication overheads than the above sign-then-encrypt way. Since then, there are many signcryption schemes proposed.

It is only recently that a formal security proof model (Baek et al., 2002) is formalized providing security proof for Zheng (1997) in the random oracle model. By combining ID-based cryptography and signcryption, Malone-Lee (2002) proposed a first ID-based signcryption scheme. But Libert and Quisquater (2003) pointed out that Malone-Lee's scheme (Malone-Lee, 2002) is not...
semantically secure, since the signature of the message is visible in the signrypted message. Chow et al. (2004) proposed an ID-based signryption scheme that can provide both public verifiability and forward security. In Boyen (2003) proposed a secure identity-based signcryption scheme with ciphertext anonymity and provable secure in the random oracle model.

Their security proof model is slightly different from that of (Baek et al., 2002) which includes the ciphertext anonymity. In Libert and Quisquater (2004) modified Boyen’s security proof model to non-dentity based signcryption scheme and proposed a signcryption scheme. They proved that their signcryption scheme is secure in the random oracle model with the following properties: semantically security against adaptive chosen ciphertext attacks, ciphertext anonymity and key invisibility. Unfortunately, Tan showed that the scheme did not satisfy the above properties in Tan (2005). Up to now, the most efficient ID-based signcryption scheme (Barreto et al., 2005) was proposed by Barreto et al. (2005) and the security of the scheme was based on recently studied computational assumptions: the q-Bilinear Diffie-Hellman Inversion problem.

In the cloud computing, grid computing, trust management is a crucial approach to authenticate user and protect resource. Trust between two unknown parties in different autonomous domain is established based on the party’s properties, by which are proven their qualifications through the disclosure of appropriate credentials. Assertion, described as well-defined uniformly semantic structure entities such as credentials, policies and requests, is encrypted by issuer or authorities public key. In order to protect the security of assertion for decentralized autonomous environments, Zhang et al. (2008) proposed an efficient assertion security protect model based on signcryption scheme for multiple autonomous domain managers and Privacy Key Generators (PKGs). Unfortunately, Wang and Qian (2010) shown that their extensions were incorrect, i.e., Zhang et al. (2008) scheme is not suitable for multi-PKG scenario, it can reach consistency when only one PKG exists in the system. In this work, by combining two ID-based signature schemes with a signcryption scheme, we build security model of ID-based signcryption in the multi-PKG and have proposed an ID-based signcryption scheme in the multi-PKG based on the bilinear pairings to adapt to the different cryptographical system setting. We prove that our proposed scheme is secure and satisfies the confidentiality and unforgeability.

**PRELIMINARIES**

Here, we briefly review the basic definition and properties of the bilinear pairings.

Let $G_1$ be a cyclic additive group generated by the generator $P$, whose order is a prime $q$ and $G_2$ be a cyclic multiplicative group of the same prime order $q$.

We assume that the Discrete Logarithm Problem (DLP) in both $G_1$ and $G_2$ are hard. An admissible pairing $e: G_1 \times G_1 \rightarrow G_2$, which satisfies the following three properties:

- **Bilinear:** If $P, Q \in G_1$ and $a, b \in \mathbb{Z}_q$, then $e(aP, bP) = e(P, P)^{ab}$
- **Non-degenerate:** There exists a $P \in G_1$ such that $e(P, P) \neq 1$
- **Computable:** If $P, Q \in G_1$, one can compute $e(P, Q) \in G_2$ in the polynomial time

We note the modified Weil and Tate pairings associated with supersingular elliptic curves are examples of such admissible pairings. The security of the ID-based signcryption scheme discussed in this paper is based on the following security assumption.

**Definition 1:** Given two group $G_1$ and $G_2$ of the same prime order $q$, a bilinear map $e: G_1 \times G_1 \rightarrow G_2$ and a generator $P$ of $G_1$, the Decisional Bilinear Diffie-Hellman problem (DBHP) in $(G_1, G_2, e)$ is to decide whether $h = e(P, P)^{aP}$ given $(P, aP, bP, cP)$ and an element $h \in G_2$. We define the advantage of a distinguisher against the DBDH as follows:

$$Adv_{\text{DBDH}}(t) = \Pr[A(q, G_1, xP, yP) = xyP | (q, G_1), x, y \leftarrow \mathbb{Z}_q]$$

**Definition 2:** (CDH Assumption). Let $\text{gen}$ be a CDH parameter generator. We say algorithm $A$ has advantage $\text{Adv}_{\text{CDH}}(t)$ when solving the CDH problem for $\text{gen}$ if for a sufficiently large key

$$Adv_{\text{CDH}}(t) = \Pr[A(q, G_1, xP, yP) = xyP | (q, G_1), x, y \leftarrow \mathbb{Z}_q]$$

We say that $\text{gen}$ satisfies the CDH assumption if for any randomized polynomial time in $t$, algorithm $A$ we have the $\text{Adv}_{\text{CDH}}(t)$ is negligible function.

**DEFINITION AND SECURITY MODEL OF ID-BASED SIGNCRYPTION IN THE MULTI-PKG**

An ID-based signcryption scheme in the multi-PKG consists of the algorithms $<$System Setup, PKG setup, Key Extract, Signcrypt, Unsigncrypt$>$. Malone-Lee (2002) define the security requirements for ID-based signcryption schemes. These security requirements include indistinguishable against adaptive chosen ciphertext attacks and unforgeability against adaptive chosen message attacks. In the following, we modify the

definitions to adapt for our ID-based signcryption scheme in the multi-PKG.

**System parameter setup:** It takes a security parameter $k$ as input and returns system parameters Params. PKG-Setup: Each autonomous domain manager PKGi takes the $\text{Params}$ input and returns his public/private key pair $(P^1_{pub}, s_i)$ where he only publishes his public key to group members.

**Key extract:** This algorithm is to produce a secret key SID of the user with identity ID, the method is the same as the ordinary ID-based key extract algorithm (Libert and Quisquater, 2003; Malone-Lee, 2000), where the difference is that a user should register in and extract from his autonomous domain manager PKGi in multiple autonomous trust domain environments.

**Signcrypt:** To send an assertion $a$ to Bob identified by ID$_b$, the sender Alice produces the ciphertext by this algorithm on input of $(a, S_{as}, ID_{as}, P^1_{pub}, P^2_{pub})$.

**Designcrypt:** The recipient Bob with secret key $S_B$ under the different domain uses this algorithm to decrypt the ciphertext and verify the validation of the signature.

**Definition 3:** (Confidentiality) An ID-based signcryption scheme in the multi-PKG is indistinguishable against adaptive chosen ciphertext attacks property (IND-IDSCMP-CCA2) if no polynomial bounded adversary has a non-negligible advantage in the following game.

**Setup:** The challenger $C$ runs Setup algorithm and Issuer-Setup algorithm with a security parameter $k$ and sends the system parameters to the adversary $A$.

**Phase 1:** A performs a series of queries in an adaptive fashion. The following queries are allowed:

**Key extraction queries:** A chooses an identity ID. $C$ computes private key $s_{ID}, ID_{ID}, P^1_{pub}, P^2_{pub}$ to response $A$.

**Signcryption queries:** A inputs the sender’s identity ID$_{as}$ and the recipient’s identity ID$_b$ and a signcryption-ed message $m$, $C$ computes $\delta = \text{signcryption} (m, s_{ID_{as}}, ID_{ID}, \delta^1_{pub}, P^2_{pub})$ and sends it to $A$.

**Unsigncryption queries:** Given a ciphertext $\delta$, the challenger $C$ runs Unsigncrypt algorithm on input $(\delta, s_{ID_{as}}, ID_{ID}, \delta^1_{pub}, P^2_{pub})$ and returns its output to $A$.

**Selection:** At the end of phase $1$, $A$ generates two equal length plaintext $m_0$ and $m_1$ and a sender’s identity $ID_{as}$ and the recipient $ID_b$ on which he wants to be challenged. He cannot have query the private key of $ID_b$ as the first phase.

**Challenge:** The challenge flips $b \in \{0, 1\}$ then computes $\delta = \text{signcryption} (s_{ID_{as}}, ID_{ID}, \delta^1_{pub}, P^2_{pub})$ to return it to the adversary $A$.

**Phase 2:** A can ask a polynomial bounded number of queries adaptively again as in the first phase. But he cannot make a key extraction query on $ID_b$ and cannot make an unsigncryption query on $\delta'$.

**Output:** $A$ outputs a bit $b'$ and wins the game if $b' = b$.

The advantage of $A$ is defined as $\text{Adv}_A = |2P(b' = b)-1|$, where $P(b' = b)$ denotes the probability that $b' = b$.

**Definition 4:** Unforgeability: A signcryption scheme based on multiple PKGs is existentially unforgeable against chosen-message insider attack (EUF-IDSCMP-CMA2) if no PPT forger $F$ has a non-negligible advantage in the following game:

- Challenger runs System. setup and Issuer. setup just like in IDASC game
- Forger $F$ adaptively performs a number of queries just like in IDASC game
- $F$ produces a ciphertext $(\delta, ID_{as}, ID_b)$ in the sense that the key is the range of key extract algorithm and wins the game if: (a) Designcrypt $(\delta, ID_{as}, ID_b) \neq \perp$; (b) $\delta$ is not produced by Signcryption oracle

**OUR SCHEME**

In this section, we give a novel ID-based signcryption scheme which is suitable to the multi-PKG. The details of our scheme are described as follows:

**Setup:** Given a security parameter $k$, select two bilinear map groups $(G_1, G_2)$ of prime order $q > 2^k$, $e: G_1 \times G_2 \rightarrow G_3$, and a generator $P_{G_1}$. Define three hash functions $H_j: \{0, 1\}^l \rightarrow G_j, H_j: G_1 \rightarrow G_2$, and $H_2: G_1 \rightarrow \{0, 1\}^l$, where $l$ denotes the length of assertion $a$. Publish the system parameters $(G_1, G_2, q, e, P, H_1, H_2, H_3)$. For each PKG$_i$, it randomly chooses $s_i \in Z_q$ to compute $P^1_{pub} = s_iP$ as his public key and secretly keeps $s_i$ as his master key.

**Key extraction:** When a user registers his identity ID to PKG$_a$, the PKG$_i$ computes $S_{ID} - s_iQ_{ID}$ as the corresponding
secret key of the user ID where, \( Q_a = H_i(ID) \). Finally, PKG \(_i\) sends the secret key \( S_{in} \) to the user via a secure channel.

**Signcryption:** Given a message \( m \), a recipient Bob’s identity \( ID_b \), which secret key is issued by PKG \(_b\), the sender Alice’s secret key is issued by PKG \(_i\). Note that the sender and recipient are the two users of different domains. Alice computes as follows:

- First, Alice sends an assertion \( a \) to Bob with identity \( ID_b \) in trust domain PKG \(_b\).
- Then, it randomly chooses \( r \in \mathbb{Z}_q \) to compute \( U = rP \).
- Compute \( h = H_i(U[a|m]) \) and \( V = rP_{pub} + hS_a \).
- Compute \( t = e(rP_{pub}, Q_b) \) and \( W = H_j(t \oplus (V|Q_a|a|m)) \).
- Finally, the resultant ciphertext is \( C = (U, W) \).

**De-signcryption:** Upon receiving a ciphertext \( C = (U, W) \) the recipient Bob does as follows:

- Firstly, the recipient Bob checks whether \( U \) belongs to group \( G_1 \), if it holds, then Bob computes \( t = e(U, S_a) \).
- Then recover \( (V|Q_a|a|m) = W \oplus H_j(t) \) and compute \( h = H_i(U[a|m]) \).
- If \( Q_a \in G_2 \) or \( V \notin G_1 \), then abort it. Otherwise, accept the assertion \( a \) and return TRUE if and only if the following equation holds

\[
\sigma(P, V) = \sigma(P, rP_{pub} + hS_a) \equiv \sigma(P_{pub}, U + hQ_a)
\]

If so, output valid; if not, output invalid.

**SECURITY ANALYSIS**

**Theorem 1:** (Confidentiality) Assume that an IND-IBSC-CCA adversary \( A \) has an advantage \( \varepsilon \) against our proposed scheme when running in time \( t \), asking \( q_a \) queries to random oracles \( H_i (i = 1, 2, 3) \), \( q_s \) signcryption queries, and \( q_s \) queries to the unsigncryption oracle. Then there is an algorithm \( B \) to solve the DBDH problem with non-negligible probability.

**Proof:** Given a random instance \( (P, aP, bP, cP, h) \) of the Decisional Bilinear Diffie-Hellman problem, where \( h \in G_1 \), we are going to construct a probabilistic polynomial time Turing machine \( D \) which use the attacker \( A \) as a subroutine in order to distinguish whether \( h = \sigma(P, P)^{bc} \) holds or not. In the whole game, \( A \) will consult \( D \) for answers to the random oracles \( H_i, H_2, \) and \( H_3 \). And \( D \) needs to maintain hash lists \( L_1, L_2 \) and \( L_3 \) that are initially empty and are used to keep track of answers to queries asked by \( A \) to oracle \( H_1, H_2, \) and \( H_3 \).

We suppose that the following assumption are made:

- A asks for \( H_i(ID) \) before ID is used in any key extraction query, signcryption query, and unsigncryption query.
- Ciphertext returned from a signcryption query will not be used by A in an unsigncryption query.

At the beginning of the game, \( D \) randomly chooses \( s, e \in \mathbb{Z}_q \) to compute \( P_{pub} = sP \) as the public key of PKG \(_i\) and sets the public key of PKG \(_b\) with \( P_{pub} = aP \) and sends \( (P_{pub}, P_{pub}) \) to the adversary \( A \). (Note that \( a \) is unknown to \( D \) and plays the roles of PKG \(_i\)’s master key in the game.) The identities of \( n \) signers are denoted by \( ID_{s1}, ID_{s2}, \ldots, ID_{sn} \). \( D \) chooses a random number \( i \in \{1, 2, \ldots, q_b\} \) as challenged identity index.

**Phase 1:** A performs a first series of queries of the following kinds that are handled by \( D \) as explained below:

- **H-Oracles:** When \( A \) asks \( H_i \) queries with \( ID_b \), \( D \) responds as follows:
  - If \( j \neq i \), then \( D \) answers by \( H_i(ID_j) = bP \).
  - If \( j = i \), then \( D \) randomly chooses \( b, e \in \mathbb{Z}_q \) to set \( H_i(ID_i) = bP \) and records the pair \( (ID_i, b) \) in the list \( L_1 \).

- **H-Oracles:** When \( A \) makes queries on \( H_2 \)-oracle with \( w_p \), \( D \) searches the pair \( (w_p, t) \) in the list \( L_2 \) if such a pair exists, then \( D \) returns \( t \) to \( A \), otherwise, \( D \) randomly chooses \( t \in \mathbb{Z}_q \), answers \( A \) and records this pair \( (w_p, t) \) in the list \( L_2 \).

- **H-Oracles:** When \( A \) makes queries on \( H_3 \)-oracle with \( t_p \), \( D \) searches the pair \( (a, t) \) in the list \( L_3 \) if such a pair exists, then \( D \) returns \( a \) to \( A \), otherwise, \( D \) randomly chooses \( a \in \mathbb{Z}_q \) to answer \( A \) and records this pair \( (a, t) \) in the list \( L_3 \).

**Key extract oracle:** When \( A \) makes a key extract query with \( ID_b \) to PKG \(_b\), if \( j = i \), then \( D \) and \( A \) aborts it. Otherwise, \( D \) first searches \( ID_b \) in the list \( L_1 \). If the pair \( (ID_p, b) \) exists, then \( D \) responds \( S_{ID_b} = bP_{pub} \) as the private key, otherwise, \( D \) randomly selects \( b \in \mathbb{Z}_q \) to answer the private key \( S_{ID_b} = bP_{pub} \) and records \( (ID_p, b) \) in the list \( L_1 \).

When the adversary \( A \) makes a key extract query with \( ID_b \) to PKG \(_b\), \( D \) can use the master secret key \( s \) of PKG \(_b\) to compute the secret key \( S = sQ_a \) where \( Q_a = H_i(ID_i) \) since it has PKG \(_i\)’s master secret key.

**Signcryption oracle:** When an adversary makes a signcryption query with the message \( (ID_s, ID_b, M) \), \( D \) responds as follows:

For \( ID_a \in \{0, 1\} \), which belongs to the domain of PKG \(_i\), \( D \) has the master secret key of PKG \(_b\) so that \( D \) can compute the secret key of the user with identity \( ID_a \).
means that D can use the secret key of IDₐ to compute a
ciphertext on message M.

**Unsignryption oracle:** When A makes a unsignryption
query for δ = (Uᵣ, Uₒ, W) from IDₐ to IDₜ. We consider the
following cases:

- If IDₜ = IDₐ, D always answer A the δ is a valid
ciphertext
- If IDₜ ∈ IDₐ, D can query key extract oracle with IDₜ,
  thus, it can compute the secret key of the user with
  identity IDₜ to recover the message m. Finally, D can
  recover V to check whether the following equation
  holds or not

\[ e(P, V) = e(P_{pub}, Uᵣ + hQ₁) \]

**Challenge:** Finally, A outputs two equal length plaintexts
mᵣ and m₁, together with the receiver’s secret key sₒD, on
which he wishes to be challenged. D randomly chooses
b ∈ {0, 1} and signcrypt mᵣ as follows:

- Set Uᵣ = cP
- Compute hᵣ = H₄(t), where t is among the DBDH
  problem
- Compute h₁ = H(Uᵣ||Q₁||a||m₁)

Finally, D sends the ciphertext δ' = (Uᵣ, W') to A.

**Phase 2:** A performs new queries which are treated in the
same way of Phase 1. At the end of the simulation, it
produces a bit b' for its guess. If b ≠ b', then it denotes
that D can output

\[ t = e(Uᵣ, sₒD) = e(cP, aD) = e(P, P) \]

as a solution of distinguish DBDH problem, otherwise D
outputs “failure”.

**Theorem 2:** Suppose that there exists an adaptively
chosen message and identity attack F making qᵢ₀ queries
to random oracles Hᵢ (i = 1, 2, 3), qᵢ queries to key extract
oracle and qᵢ queries to the signryption oracle. If the
adversary F can produce a forgery with non-negligible
probability, then, there exists an algorithm B which is able
to solve the CDH problem.

**Proof:** Suppose that F is a forger which is able to break
our proposed ID-based signryption scheme. Given a
CDH instance \((P, XP, yP, \alpha, y, eG₃)\), we will construct an
algorithm B to compute the CDH solution \(xyP \) in \(G₁ \) by

using the algorithm F as subroutine. To do so, algorithm
B performs the following simulation by interacting with
the forger F.

**Setup:** Algorithm B sets the system-wide PKGᵢ’s public
key as \(P_{pub} = xP \) and randomly chooses \(sᵢ \in Zₚ \) to compute
\(P_{pub} = sᵢP\) as the public key of PKGᵢ. Finally, B sends them
to the adversary F.

At any time, algorithm A can query the random
oracles Hᵢ, H₁, H₀, Extract oracle and Signryption Oracle.
To answer these queries, B executes the following
response.

**H₁-queries:** To respond to H₁-queries, the algorithm B
maintains a list of tuples \((ID, w, b, c)\) as explained belows.
We refer to this list as \(L₁\)-list which is initially empty.
When F makes a H₁-query with ID, the algorithm B
responds as follows:

- If the query ID already appear on the \(L₁\)-list in a tuple
  \((ID, b, c)\), then it responds with \(H₁(ID) = \omega\)
- Otherwise, B chooses a random coin \(c \in \{0, 1\}\) with
  \(Pr[c = 0] = \frac{1}{qᵢ + 1}\)

If \(c = 0\), then B randomly picks \(b ∈ Zₚ\) to compute
\(w = byP\). If \(c = 1\), then B randomly picks \(b ∈ Zₚ\) to compute
\(w = byP\).

Finally, B records the tuple \((ID, w, b, c)\) in the \(L₁\)-list
and responds to F with \(w = H₁(ID)\).

**Hᵢ-queries:** When F makes hash queries on Hᵢ-oracle with
\((Uᵣ, a, m)\) B searches the pair \((\omega, Uᵣ, a, m)\) in the list \(L₂\)
which maintains the tuples \((\omega, Uᵣ, a, m)\), if such a pair
exists, then B responds \(\omega\) to F, otherwise, B randomly
chooses \(\omega ∈ Zₚ\) to answer F and records this pair \((\omega, Uᵣ, a, m)\)
in the list \(L₂\).

**H₀-queries:** When F makes queries on H₀-oracle with \(t, b\)
searches the pair \((a, t)\) in the list \(L₀\) which maintains the
tuples \((a, t)\), if such a pair exists, B responds \(a\) to F.
Otherwise, B randomly chooses \(b ∈ G₃\) to answer F and
records this pair \((a, t)\) in the list \(L₀\).

**Extract queries:** When F queries the private key
concerning to ID, B searches the corresponding tuple
\((ID, w, b, c)\) in the \(L₁\)-list.

- If \(c = 0\), then B fails and aborts it
- Otherwise, B computes \(sᵢ = byP_{pub}\) and responds to F
  with \(sᵢ\) as a private key of ID
Signcryption Query: When $F$ makes a signcryption query on message $m$ with $L = (\text{ID}_a, \text{ID}_b)$, $B$ searches the corresponding tuples $(\text{ID}_a, w_a, b_a, c_a)$ in the $L$-list:

- If $\text{ID}_a$ exists in the $L$-list, it means that was previously queried. Thus, $B$ is able to compute signcryption of message $m$ by using the above signcryption algorithm.
- Otherwise, $B$ fails and aborts it.

If $B$ does abort as a result of $F$'s Extract queries and Signcryption queries, then $F$'s view is identical to its view in the real attack.

Output: Eventually, $A$ outputs a forgery $\delta' = (U', W')$ on a message $m'$. By adopting the forking lemma, we use the same tape, then we will obtain the other pair signature $\delta'' = (U'', W'')$ on the same message $m'$. By previous assumption, $\text{ID}'_a$ and message $m'$ must be queried to $H_1$-oracle. If the coin flipped by $B$ for the query with the identity, which did not show $0$ then $B$ declares "failure". Otherwise, if the coin flipped $c_n'=1$ by $B$ for message $m'$, then $B$ aborts it, if $c_n'=0$ (it means that $H_1(m') = b_n'P$) and $B$ has the master secret key of PKG, it means that $B$ has the secret key of the recipient, he can respond as follows:

Without loss of generality, $\text{ID}'_a$ is the honest signer, then $1'.1$. We have:

$$V = rP + hS_a$$
$$V'' = rP + hS_a$$

It means that $B$ is able to the instance of the CDH problem:

$$xyP = \frac{1}{h-h'}(V-V'')$$

CONCLUSION

Signcryption is a relatively new cryptographic technique that is supposed to fulfill the functionalities of digital signature and encryption in a single logical step and can effectively decrease the computational costs and communication overheads in comparison with the traditional signature-then-encryption schemes. By combining two ID-based signature schemes with ID-based signcryption scheme, we build security model of signcryption in the multi-PKG and based on the bilinear pairings to adapt to multi-PKG cryptographical system setting. The scheme can be applied in multiple autonomous domain environments such as decentralized self-organization network, autonomous P2P and large scale distributed trust management environment etc. At the same time, we also prove that our proposed scheme is secure and satisfies the confidentiality and unforgeability. It remains an open problem to design identity-based signcryption scheme that is secure in the standard model.

ACKNOWLEDGMENTS

I thank the anonymous referees for their very valuable comments on this study. This work is supported by, the New Star Plan Project of Beijing Science and Technology (No: 2007B-001) and and The Beijing Natural Science Foundation Program and Scientific Research Key Program of Beijing Municipal Commission of Education (No: KZ200810009005).

REFERENCES


2103

