PROVABLE SECURE IDENTITY BASED SIGNCRYPTION SCHEMES WITHOUT RANDOM ORACLES

Prashant Kushwah[1] and Sunder Lal[2]

[1]Department of Mathematics and Statistics, Banasthali University, Rajasthan, India
pra.ibs@gmail.com
[2] Vice Chancellor, Veer Bahadur Singh Purvanchal University, Jaunpur (UP), India
sunder_lal2@rediffmail.com

ABSTRACT

Signcryption is a cryptographic primitive which performs encryption and signature in a single logical step with the cost lower than signature-then-encryption approach. Recently, Li et al. [35] proposed the first provable secure identity based signcryption without random oracles. In their scheme sender signs the ciphertext. However, in [11] Boyen showed that non-repudiation is easily achieved if the sender sign the plaintext rather than ciphertext. In this paper we proposed an identity based signcryption scheme without random oracles, which provides the non-repudiation with respect to plaintext. We also proposed an identity based public verifiable signcryption scheme with third party verification in the standard model.

KEYWORDS

Signcryption, identity based cryptography, provable security, standard model, public verifiable signcryption

1. INTRODUCTION

Confidentiality and authenticity of a message are achieved independently by public key encryption and digital signature respectively. There are scenarios where both confidentiality and authenticity are needed simultaneously (for example secure e-mailing). Earlier signature-then-encryption approach was followed to achieve both primitives. However, this approach has a high computational cost and communication overhead. In 1997, Zheng [1] proposed a novel cryptographic primitive "Signcryption" which achieves both confidentiality and authenticity in a single logical step with the cost significantly lower than 'signature-then-encryption' approach. Security notions for signcryption were first formalize by Beak et al. [2] i.e. semantic security against adaptive chosen cipher text attack and existential unforgeability against adaptive chosen message attack. Many public key signcryption schemes have been proposed after [1]. Some of them are [3-6].

In 1984, Shamir [7] introduced the concept of identity based cryptography. In the identity based cryptosystem public key of users are their identities (e.g. email address, PAN number etc.). Shamir gave an identity based signature (IBS) scheme in [7], but he cannot find any concrete scheme for identity based encryption (IBE). The first identity based encryption (IBE) scheme was given by Boneh and Franklin [8] in 2001. The first identity based signcryption (IBSC) scheme was proposed by Malone Lee [9] in 2002 along with a security model for signcryption in identity based setting. Since then, many IBSC schemes have been proposed in literature [10-16].

DOI : 10.5121/ijnsa.2012.4306

However, most IBSC schemes were proven secure in the random oracle model [17]. Although, in the random oracle model one can construct the efficient and provable secure schemes but a proof in the random oracle model only provides the heuristic security. Canetti et al. [18] showed that when random oracles are instantiated with concrete hash functions, the resulting scheme may not be secure. Many cryptographic schemes are proposed which are provably secure without random oracles (or in the standard model). Some of them are [19-27]. By combining Waters' [23] IBE scheme and Paterson and Schuldt's IBS scheme [22], Yu et al. [24] proposed an IBSC scheme in the standard model. Many authors proved that their scheme is not secure [21, 28-31]. Among them Zhang [30] and Jin et al. [21] gave improvement on Yu et al. scheme. However, Li, Liao and Qin [32] showed that Jin et al.'s [21] scheme in neither IND-CCA2 secure nor existential unforgeable and in [33], Li and Takagi showed that Zhang's [30] scheme does not possess IND-CPA security and proposed an improvement. In [34], Selvi et al. showed that Li and Takagi's [33] improvement is not IND-CCA2 secure.

Recently, Li et al. [35] proposed an efficient IBSC scheme without random oracle based on Kiltz and Vahlis's IBE scheme [36] and Paterson and Schuldt IBS scheme [22]. In their scheme, sender signs the ciphertext which provides existential ciphertext unforgeability i.e. non-repudiation for the ciphertext. In [11], Boyen noticed that this might difficult the task of receivers who want to convince a third party of the sender's authorship for an extracted plaintext. In this paper we first propose a provable secure IBSC scheme without random oracles which has existential signature unforgeability i.e. non-repudiation for the plaintext. Further, we also propose an identity based public verifiable signcryption (IBPSC) scheme with third party verification without random oracles. In the public verifiable signcryption scheme a third party who is unaware of the receiver's private key is able to verify whether a cipher text is valid or not and in third party verifiable signcryption schemes, a third party is able to verify the integrity and origin of the message using some additional information along with the signcryption provided by the receiver other than his/her private key. Signcryption schemes with these additional properties have applications in filtering out the spam in a secure email system and private contract signing [16].

This paper is organized as follows: In section 2, we give the formal definitions of IBSC schemes and their security model. Section 3 contains the preliminaries for the proposed schemes. In section 4, we propose the new IBSC without random oracle and prove its security. In section 5, we propose the identity based public verifiable signcryption scheme with third party verification without random oracles. We conclude this paper in section 6.

2. FORMAL MODEL OF IBSC SCHEME

An **identity based signcryption (IBSC) scheme** consists of the following four algorithms:

1. **Setup:** This algorithm takes input a security parameter *k* and outputs the system parameters **params** and a master secret key.
2. **Key Generation:** Given input params, master secret key and a user's identity ID_U, it outputs a partial private key D_U corresponding to ID_U.
3. **IBSC (signcryption):** To send a message m from a user A to B, this algorithm takes input (D_A, m, ID_A, ID_B) and outputs a $\sigma = IBSC(D_A, m, ID_A, ID_B)$.
4. **IBUSC (unsigncryption):** This algorithm takes input $(\sigma, D_B, ID_B, ID_A)$ and outputs m if σ is a valid signcryption of m done by *A* for *B*, otherwise outputs "invalid".

2.1. Security Model For IBSC Schemes

2.1.1. Message Confidentiality

The notion of security with respect to confidentiality is indistinguishability of encryptions under adaptive chosen cipher text attack (IND-CCA2). For IBSC this notion is captured by the following game played between challenger $\mathcal{C}$ and adversary $\mathcal{A}$.

GAME 1 (IND-CCA2):

Initialization: $\mathcal{C}$ runs the setup algorithm on input a security parameter *k*, gives public parameters params to the adversary $\mathcal{A}$. $\mathcal{C}$ keeps the master key secret.

Queries (Find Stage): The adversary $\mathcal{A}$ makes the following queries adaptively.

- **Key generation Queries:** $\mathcal{A}$ submits an identity ID_U and $\mathcal{C}$ computes the private key D_U corresponding to ID_U and returns to $\mathcal{A}$.
- **IBSC Queries:** $\mathcal{A}$ submits two identities ID_A, ID_B and a message *m*. Challenger $\mathcal{C}$ runs the IBSC algorithm with message *m* and identities ID_A and ID_B and returns the output σ to the adversary $\mathcal{A}$.
- **IBUSC Queries:** $\mathcal{A}$ submits two identities ID_A, ID_B along with σ to the challenger $\mathcal{C}$. $\mathcal{C}$ runs the IBUSC algorithm with input σ, ID_A and ID_B and returns the output *m* and ϕ if σ is a valid signcryption of m done by *A* for *B*, otherwise outputs "invalid".

  No queries with $ID_A = ID_B$ is allowed.

Challenge: At the end of the find stage, $\mathcal{A}$ submits two distinct messages m_0 and m_1 of equal length, a sender's identity ID_A^* and a receiver's identity ID_B^* on which $\mathcal{A}$ wishes to be challenged. The adversary $\mathcal{A}$ must have made no key generation query on ID_B^*. $\mathcal{C}$ picks randomly a bit $b \in \{0,1\}$, runs the IBSC algorithm with message m_b under ID_A^* and ID_B^* and returns the output σ^* to the adversary $\mathcal{A}$.

Queries (Guess stage): $\mathcal{A}$ queries adaptively again as in the find stage. It is not allowed to extract the private key corresponding to ID_B^* and also it is not allowed to make an IBUSC query on σ^* with sender ID_A^* and receiver ID_B^*.

Eventually, $\mathcal{A}$ outputs a bit b' and wins the game if $b = b'$.

$\mathcal{A}$'s advantage is defined as $Adv_{\mathcal{A}}^{IND-CCA2} = 2\Pr[b = b'] - 1$.

Definition 1: An IBSC scheme is said to IND-CCA2 secure if no polynomially bounded adversary $\mathcal{A}$ has non-negligible advantage of winning the above game.

Note that the confidentiality game described above deals with the insider security since the adversary is given access to the private key of the sender ID_A^* in the challenge phase.

2.2.1 Signature Unforgeability

The notion of security with respect to authenticity is existential unforgeability against chosen message attacks (EUF-CMA). For IBSC this notion is captured by the following game played between challenger $\mathcal{C}$ and adversary $\mathcal{A}$.

GAME 2 (EUF-CMA):

Initialization: Same as in GAME 1.

Queries: The adversary $\mathcal{A}$ asks a polynomially bounded number of queries adaptively as in GAME 1.

Forgery: Finally, $\mathcal{A}$ produces a triplet $(ID_A^*, ID_B^*, \sigma^*)$ that was not obtained from an IBSC query during the game and for which private key of ID_A^* was not exposed. The forger wins if σ^* is valid signcrypted text from ID_A^* to ID_B^*.

The adversary $\mathcal{A}$'s advantage is its probability of winning the above game.

Definition 3: An IBSC scheme is said to EUF-CMA secure if no polynomially bounded adversary $\mathcal{A}$ has non-negligible advantage of winning the above game.

Note that in the cipher text unforgeability game described above deals with the insider security since the adversary is given access to the private key of the receiver ID_B^* in the forgery.

3. PRELIMINARIES

Let $\mathbb{G}_1$ and $\mathbb{G}_2$ be multiplicative groups of the prime order p and g be a generator of $\mathbb{G}_1$. A function $e: \mathbb{G}_1 \times \mathbb{G}_1 \to \mathbb{G}_2$ is called a **bilinear pairing** if it satisfies the following properties:

1. Bilinearity: for all $a, b \in \mathbb{Z}_p, e(g^a, g^b) = e(g, g)^{ab}$
2. Non-degeneracy: $e(g, g) \neq 1_{\mathbb{G}_2}$
3. Computability: e is efficiently computable.

Given $g, g^a, g^b, g^c \in \mathbb{G}_1$ for some unknown $a, b, c \in \mathbb{Z}_p$ and an element $Z \in \mathbb{G}_2$, decide whether $Z = e(g, g)^{abc}$ or not is known as **Decisional Bilinear Diffie-Hellman (DBDH) Problem**.

Given $g, g^a, g^b \in \mathbb{G}_1$ for some unknown $a, b \in \mathbb{Z}_p$ to compute g^{ab} is known as **Computational Diffie-Hellman (CDH) Problem**.

4. PROPOSED IDENTITY BASED SIGNCRYPTION (IBSC) SCHEME WITHOUT RANDOM ORACLES

Setup: Choose two groups $\mathbb{G}_1$ and $\mathbb{G}_2$ of prime order p such that an admissible pairing $e: \mathbb{G}_1 \times \mathbb{G}_1 \to \mathbb{G}_2$ can be constructed and pick a generator g of $\mathbb{G}_1$.

Now pick a random secret $\alpha \in \mathbb{Z}_p$, compute $g_1 = g^\alpha$ and pick $g_2 \in_R \mathbb{G}_1$. Furthermore, pick elements $u', m' \in_R \mathbb{G}_1$ and vectors $\vec{\boldsymbol{u}} = (u_i)$, $\vec{\boldsymbol{m}} = (m_i)$ of length n_u and n_m, respectively, whose entries are random elements from $\mathbb{G}_1$. Here public parameters are params = $\langle \mathbb{G}_1, \mathbb{G}_2, e, g, g_1, g_2, u', \vec{\boldsymbol{u}}, m', \vec{\boldsymbol{m}}, H_1, H_2 \rangle$ and the master secret key is g_2^α. Cryptographic hash functions H_1 and H_2 are defined as $H_1 : \mathbb{G}_2 \to \{0,1\}^\ell$ and $H_2 : \{0,1\}^\ell \times \mathbb{G}_2 \times \mathbb{G}_1 \times \mathbb{G}_1 \to \{0,1\}^{n_m}$. Here ℓ is the length of the plaintext.

Key Generation: Let *u* be a bit string of length n_u representing an identity and let $u[i]$ be the *i*-th bit of *u*. Define $U' \subset \{1,...,n_u\}$ to be the set of indices *i* such that $u[i] = 1$.

To construct the private key d_u of the identity *u*, pick $r_u \in_R \mathbb{Z}_p^*$ and compute: $d_u = (g_2^\alpha (u' \prod_{j \in U'} u_j)^{r_u}, g^{r_u})$. Therefore, $d_A = (d_{A1}, d_{A2}) = (g_2^\alpha (u' \prod_{j \in U'_A} u_j)^{r_A}, g^{r_A})$ and $d_B = (d_{B1}, d_{B2}) = (g_2^\alpha (u' \prod_{j \in U'_B} u_j)^{r_B}, g^{r_B})$ are the private keys of the sender (Alice) with identity u_A and the receiver (Bob) with identity u_B respectively.

IBSC: To send a message $m \in \{0,1\}^\ell$ to Bob, Alice picks $r \in_R \mathbb{Z}_p$ randomly and computes $\omega = e(g_1, g_2)^r$, $\sigma_1 = m \oplus H_1(\omega)$, $\sigma_2 = g^r$, $\sigma_3 = (u' \prod_{j \in U'_B} u_j)^r$, $M = H_2(m, \omega, u' \prod_{j \in U'_A} u_j, d_{A2})$, $\sigma_4 = d_{A1}(m' \prod_{j \in M'} m_j)^r$ where $M' \subset \{1,...,n_m\}$ is the set of indices *j* such that $m[j] = 1$ ($m[j]$ is the *j*-th bit of *M*). Next Alice sets $\sigma_5 = d_{A2}$. The cipher text is $\sigma = (\sigma_1, \sigma_2, \sigma_3, \sigma_4, \sigma_5)$.

IBUSC: On receiving the cipher text $\sigma = (\sigma_1, \sigma_2, \sigma_3, \sigma_4, \sigma_5)$, Bob computes $\omega = e(d_{B2}, \sigma_3)^{-1} e(d_{B1}, \sigma_2)$, $m = \sigma_1 \oplus H_1(\omega)$, $\hat{M} = H_2(m, \omega, u' \prod_{j \in U'_A} u_j, \sigma_5)$. Bob generates the corresponding set $M' \subset \{1,...,n_m\}$ of indices *j* such that $m[j] = 1$, where $m[j]$ is the *j*-th bit of $\hat{M}$. Accept the message if and only if

$$e(\sigma_4, g) = e(g_1, g_2) e(u' \prod_{j \in U'_A} u_j, \sigma_5) e(m' \prod_{j \in M'} m_j, \sigma_2).$$

Consistency:

$$\omega = e(d_{B2}, \sigma_3)^{-1} e(d_{B1}, \sigma_2) = e(g^{r_B}, (u' \prod_{j \in U'_B} u_j)^r)^{-1} e(g_2^\alpha (u' \prod_{j \in U'_B} u_j)^{r_B}, g^r)$$

$$= e(g^r, (u' \prod_{j \in U'_B} u_j)^{r_B})^{-1} e(g_2^\alpha, g^r) e((u' \prod_{j \in U'_B} u_j)^{r_B}, g^r) = e(g_1, g_2)^r$$

and

$$e(\sigma_4, g) = e(d_{A1}(m' \prod_{j \in M'} m_j)^r, g)$$
$$= e(d_{A1}, g)e((m' \prod_{j \in M'} m_j)^r, g)$$
$$= e(g_2^{\alpha}(u' \prod_{j \in U'_A} u_j)^{r_A}, g)e((m' \prod_{j \in M'} m_j), g^r)$$
$$= e(g_1, g_2)e((u' \prod_{j \in U'_A} u_j), \sigma_5)e((m' \prod_{j \in M'} m_j), \sigma_2)$$

4.1. Security Analysis of proposed IBSC scheme

Our proofs of the security of the proposed IBSC scheme without random oracles depends on [22-24].

Theorem 1: (Message confidentiality) Assume that an IND-CCA2 adversary $\mathcal{A}$ has an advantage ε against the proposed IBSC scheme when running in time τ, asking at most q_e Key generation queries, q_s IBSC queries and q_u IBUSC queries respectively. Then there exists a distinguisher $\mathcal{B}$ that can solve an instance of the DBDH problem with probability

$$\varepsilon' \geq \frac{\varepsilon}{8q_s(q_e + q_s + q_u)(n_u + 1)(n_m + 1)}$$

within a time $\tau' < \tau + O((q_e + q_s + q_u)n_u\tau_{multi} + (q_e + q_s)\tau_{\exp} + q_u\tau_{\mathrm{p}})$ where $\tau_{\exp}$, τ_{multi} and τ_p are the time for an exponentiation, a multiplication in $\mathbb{G}_1$ and for a pairing computation respectively.

Proof: Let $\mathcal{A}$ be an IND-CCA2 adversary against the proposed IBSC scheme with advantage ε. Further assume that the distinguisher $\mathcal{B}$ receives a random DBDH problem instance $(g, A = g^a, B = g^b, C = g^c, Z \in \mathbb{G}_2)$, his goal is to decide whether $Z = e(g,g)^{abc}$ or not. $\mathcal{B}$ will run the adversary $\mathcal{A}$ as a subroutine and act as the $\mathcal{A}$'s challenger in the IND-CCA2 game.

Setup: The distinguisher $\mathcal{B}$ first sets $l_u = 2(q_e + q_s + q_u)$ and $l_m = 2q_s$, and chooses two integers k_u $(0 \leq k_u \leq n_u)$ and k_m $(0 \leq k_m \leq n_m)$ randomly. Then the distinguisher chooses randomly an integer $x' \in_R \mathbb{Z}_{l_u}$, an n_u-length vector $X = (x_i)$ where $(x_i \in_R \mathbb{Z}_{n_u})$, an integer $z' \in_R \mathbb{Z}_{n_m}$ and an n_m-length vector $Z = (z_i)$ where $(z_i \in_R \mathbb{Z}_{n_m})$. Additionally, the distinguisher $\mathcal{B}$ chooses randomly two integers $y', w' \in_R \mathbb{Z}_p$, an n_u-length vector $Y = (y_i)$ where $(y_i \in_R \mathbb{Z}_p)$ and an n_m-length vector $W = (w_i)$ where $(w_i \in_R \mathbb{Z}_p)$.

Let $U' \subset \{1, ..., n_u\}$ to be the set of indices *i* such that $u[i] = 1$ where $u[i]$ be the *i*-th bit of an identity *u* and $M' \subset \{1, ..., n_m\}$ is the set of indices *j* such that $m[j] = 1$ where $m[j]$ is the *j*-th bit of *M*. For ease of analysis, we define the functions for an identity *u* and a message *m* respectively as in [22, 24].

$$F(u) = -l_u k_u + x' + \sum_{i \in U'} x_i \text{ and } J(u) = y' + \sum_{i \in U'} y_i$$
$$K(M) = -l_m k_m + z' + \sum_{j \in M'} z_j \text{ and } L(M) = w' + \sum_{j \in M'} w_j$$

Then the challenger assigns a set of public parameters as follows

$$g_1 = g^a, \qquad g_2 = g^b$$
$$u' = g_2^{-l_u k_u + x'} g^{y'}, \; u_i = g_2^{x_i} g^{y_i} \; (1 \le i \le n_u)$$
$$m' = g_2^{-l_m k_m + z'} g^{w'}, m_j = g_2^{z_j} g^{w_j} \; (1 \le j \le n_m)$$

Note that these public parameters will have the same distribution as in the game between the challenger and the adversary $\mathcal{A}$. Furthermore, this assignment means that for an identity *u* and any bit string *M*, we have

$$U = u' \prod_{i \in U'} u_i = g_2^{F(u)J(u)} \text{ and } m' \prod_{j \in M'} m_j = g_2^{K(M)} g^{L(M)}.$$

Furthermore, the master secret key will be $g_2^{\alpha} = g_2^a = g^{ab}$.

Find Stage: $\mathcal{B}$ answers the $\mathcal{A}$'s queries as follows:

Key generation queries: Suppose the adversary $\mathcal{A}$ submits an identity *u*. If $F(u) = 0 \bmod p$, the distinguisher abort and randomly chooses its guess b' of the challengers value *b*. Otherwise the $\mathcal{B}$ chooses a random $r_u \in_R \mathbb{Z}_p$ and computes the private key corresponding to identity *u* as

$$d_u = (d_{u1}, d_{u2}) = (g_1^{-\frac{J(u)}{F(u)}} (u' \prod_{i \in U'} u_i)^{r_u}, \; g_1^{-\frac{1}{F(u)}} g^{r_u}).$$

The distinguisher $\mathcal{B}$ returns this private key to the adversary $\mathcal{A}$. As in the Waters' proof [23] and Paterson's proof [22], let $\bar{r}_u = r_u - \frac{a}{F(u)}$. Then we have

$$\begin{aligned} d_{u1} &= g_1^{-\frac{J(u)}{F(u)}} (u' \prod_{i \in U'} u_i)^{r_u} \\ &= g_1^{-\frac{J(u)}{F(u)}} (g_2^{F(u)} g^{J(u)})^{r_u} \\ &= g_2^a (g_2^{F(u)} g^{J(u)})^{-a/F(u)} (g_2^{F(u)} g^{J(u)})^{r_u} \\ &= g_2^a (g_2^{F(u)} g^{J(u)})^{r_u - (a/F(u))} \\ &= g_2^a (u' \prod_{i \in U'} u_i)^{\bar{r}_u} \end{aligned}$$

and

$$d_{u2} = g_1^{-\frac{1}{F(u)}} g^{r_u} = g^{r_u - \frac{a}{F(u)}} = g^{\bar{r}_u}.$$

The simulation is perfect if and only if $F(u) \neq 0 \bmod p$. For ease of analysis, assume $l_u(n_u+1) < p$ which implies $0 \le l_u k_u < p$ and $0 \le x' + \sum_{i \in U'} x_i < p$, also we have $F(u) = 0 \bmod p$ implies that $F(u) = 0 \bmod l_u$. Hence $F(u) \neq 0 \bmod l_u$ implies $F(u) \neq 0 \bmod p$, so the former condition will be sufficient to ensure that $\mathcal{B}$ will not abort in Key generation queries.

IBSC queries: The adversary submits a plaintext *m*, a sender's identity u_A and a receiver's identity u_B. If $F(u_A) \neq 0 \bmod l_u$, $\mathcal{B}$ first generates a private key for u_A as in Key generation queries described above, and then runs the IBSC algorithm with input *m*, d_{u_A} and u_B, to answer the adversary's query. Otherwise, if $F(u_A) = 0 \bmod l_u$, $\mathcal{B}$ will abort.

IBUSC queries: The adversary $\mathcal{A}$ submits a cipher text $\sigma = (\sigma_1, \sigma_2, \sigma_3, \sigma_4, \sigma_5)$, a sender's identity u_A and a receiver's identity u_B. If $F(u_B) \neq 0 \bmod l_u$ $\mathcal{B}$ first generates a private key for u_B as in Key generation queries described above, and then runs the IBUSC algorithm with input σ, u_A and d_{u_B}, to answer the adversary's query. Otherwise, if $F(u_B) = 0 \bmod l_u$ $\mathcal{B}$ will abort.

Challenge: After a polynomial bounded number of queries, adversary submits a sender's identity u_A^*, a receiver's identity u_B^* and two messages $m_0, m_1 \in \mathbb{G}_2$ on which she wants to be challenged. The distinguisher $\mathcal{B}$ will abort if $F(u_B^*) \neq 0 \bmod l_u$. Otherwise, we have $F(u_B^*) = 0 \bmod p$ and the distinguisher flips a fair coin, b, and computes $M_b^* = H_2(m_b, Z, g_2^{F(u_A^*)} g^{J(u_A^*)}, g^{-(1/F(u_A^*))} g^{r_A})$. If $K(M_b^*) \neq 0 \bmod p$ then $\mathcal{B}$ will abort, otherwise $\mathcal{B}$ sets the cipher text as

$$\sigma^* = (m_b \oplus H_1(Z), C, C^{J(u_B^*)}, g_1^{-(J(u_A^*)/F(u_A^*))} (g_2^{F(u_A^*)} g^{J(u_A^*)})^{r_A} C^{L(M_b^*)}, g^{-(1/F(u_A^*))} g^{r_A})$$

Guess stage: The adversary then performs a second series of queries which are treated in the same way as the find stage. It is not allowed to ask Key generation query for u_B^* and it is not allowed to ask an IBUSC query for σ^* under u_B^*. Finally, $\mathcal{A}$ outputs a guess b' of *b*. If $b' = b$, $\mathcal{B}$ answer's 1 indicating that $Z = e(g,g)^{abc}$; otherwise, $\mathcal{B}$ answers 0 to the DBDH problem.

Now we have to assess $\mathcal{B}$'s probability of success. For the simulation to complete without aborting, we require that all extraction queries on an identity *u* have $F(u) \neq 0 \bmod l_u$, that all IBSC queries with input (u_A, u_B, m) have $F(u_A) \neq 0 \bmod l_u$, that all IBUSC queries with input (σ, u_A, u_B) have $F(u_B) \neq 0 \bmod l_u$, in the challenge $F(u_A^*) \neq 0 \bmod l_u$ and $F(u_B^*) = 0 \bmod p$.

Let $u_1, u_2, ..., u_{q_I}$ be the identities appearing either in Key generation queries, in IBSC queries or in IBUSC queries not involving the challenge identity u_B^*. Clearly, we have $q_I \le q_e + q_s + q_u$. Define the events

$$A_i : F(u_i) \neq 0 \bmod l_u, \text{ where } i = 1, ..., q_I$$
$$A^* : F(u_B^*) = 0 \bmod p$$
$$B^* : K(M_b^*) = 0 \bmod p$$

The probability of $\mathcal{B}$ not aborting is $\Pr[\neg abort] \ge \Pr[\wedge_{i=1}^{q_I} A_i \wedge A^* \wedge B^*]$. Since the functions *F* and *K* are selected independently, therefore, the event $(\wedge_{i=1}^{q_I} A_i \wedge A^*)$ and B^* are independent. We have

$$\begin{aligned}\Pr[A^*] &= \Pr[F(u_B^*) = 0 \bmod p] \\ &= \Pr[F(u_B^*) = 0 \bmod p \wedge F(u_B^*) = 0 \bmod l_u] \\ &= \Pr[F(u_B^*) = 0 \bmod l_u] \Pr[F(u_B^*) = 0 \bmod p \mid F(u_B^*) = 0 \bmod l_u] \\ &= \frac{1}{l_u} \cdot \frac{1}{n_u + 1}\end{aligned}$$

In the same way we get

$$\Pr[B^*] = \frac{1}{l_m} \cdot \frac{1}{n_m + 1}$$

Also for two different identities u_1 and u_2, $F(u_1) = 0 \bmod l_u$ and $F(u_2) = 0 \bmod l_u$ will be independent. As a special case, for any *i*, the event A_i and A^* are independent. So we have

$$\begin{aligned}\Pr[\wedge_{i=1}^{q_I} A_i \wedge A^*] &= \Pr[A^*] \Pr[\wedge_{i=1}^{q_I} A_i \mid A^*] \\ &= \Pr[A^*] \left(1 - \Pr[\vee_{i=1}^{q_I} A_i \mid A^*]\right) \\ &\ge \Pr[A^*] \left(1 - \sum_{i=1}^{q_I} \Pr[\neg A_i \mid A^*]\right) \\ &= \frac{1}{l_u (n_u + 1)} \left(1 - \frac{q_I}{l_u}\right) \\ &\ge \frac{1}{2(q_e + q_s + q_u)(n_u + 1)} \left(1 - \frac{q_e + q_s + q_u}{2(q_e + q_s + q_u)}\right) \\ &\ge \frac{1}{4(q_e + q_s + q_u)(n_u + 1)}\end{aligned}$$

By combining above results and let $l_m = 2q_s$, we can get

$$\begin{aligned}\Pr[\neg abort] &\geq \Pr[\wedge_{i=1}^{q_I} A_i \wedge A^* \wedge B^*] \\ &= \Pr[\wedge_{i=1}^{q_I} A_i \wedge A^*]\Pr[B^*] \\ &= \frac{1}{8q_s(q_e+q_s+q_u)(n_u+1)(n_m+1)}\end{aligned}$$

Also the computation time bound of $\mathcal{B}$ can be derives from the fact that there are $O(n_u)$ multiplications in each Key generation query, IBSC query and IBUSC query. There are $O(1)$ exponentiations in each Key generation query and IBSC query. There are $O(1)$ pairing in each IBUSC query.

Theorem 2: (Signature unforgeability) Assume that an EUF-CMA adversary $\mathcal{A}$ has an advantage ε against the proposed IBSC scheme when running in time τ, asking at most q_e Key generation queries, q_s IBSC queries and q_u IBUSC queries respectively. Then there exists an algorithm $\mathcal{B}$ that can solve an instance of the Computational Diffie-Hellman problem with probability

$$\varepsilon' \geq \frac{\varepsilon}{8q_s(q_e+q_s+q_u)(n_u+1)(n_m+1)}$$

within a time $\tau' < \tau + O((q_e+q_s+q_u)n_u\tau_{multi} + (q_e+q_s)\tau_{\exp} + q_u\tau_p)$ where $\tau_{\exp}$, τ_{multi} and τ_p are the time for an exponentiation, a multiplication in $\mathbb{G}_1$ and for a pairing computation respectively.

Proof: Let $\mathcal{A}$ be an EUF-CMA adversary against the proposed IBSC scheme with advantage ε. Further assume that the $\mathcal{B}$ receives a random CDH problem instance $(g, A = g^a, B = g^b)$, his goal is to compute g^{ab}. $\mathcal{B}$ will run the adversary $\mathcal{A}$ as a subroutine and act as the $\mathcal{A}$'s challenger in the EUF-IBSC-CMA game. $\mathcal{B}$ first sets the public parameters $g_1 = g^a, g_2 = g^b, u', m', u_i, m_j$ and defines the functions $F(u), J(u), K(M)$ and $L(M)$ in the same way as described in the proof of Theorem 1. Now $\mathcal{A}$ asks Key generation queries, IBSC queries and IBUSC queries, which are answered in the same way as described in the proof of Theorem 1 by $\mathcal{B}$.

Finally, if $\mathcal{B}$ does not abort, the adversary $\mathcal{A}$ will return the forgery $\sigma^* = (\sigma_1^*, \sigma_2^*, \sigma_3^*, \sigma_4^*, \sigma_5^*)$ on the message m^* and two identities u_A^* and u_B^* such that σ^* is not the output of IBSC query with the sender's identity u_A^* and receiver's identity u_B^*. $\mathcal{B}$ unsigncrypts σ^* to obtain m^* and ω^*. $\mathcal{B}$ will abort if $F(u_A^*) \neq 0 \bmod p$, otherwise computes $M^* = H_2(m^*, \omega^*, g^{J(u_A^*)}, \sigma_5^*)$ and aborts if $K(M^*) \neq 0 \bmod p$. Thus $\mathcal{B}$ has $F(u_A^*) = 0 \bmod p$ and $K(M^*) = 0 \bmod p$. Now $\mathcal{B}$ computes and outputs

$$\frac{\sigma_4^*}{(\sigma_5^*)^{J(u_A^*)}(\sigma_2^*)^{L(M^*)}} = g_2^a = g^{ab}$$

as the solution to the given CDH problem. Now $\mathcal{B}$ advantage can be calculated similarly as in theorem 1.

5. PROPOSED IDENTITY BASED PUBLIC VERIFIABLE SIGNCRYPTION (IBPSC) SCHEME WITHOUT RANDOM ORACLES

Setup: Choose two groups $\mathbb{G}_1$ and $\mathbb{G}_2$ of prime order p such that an admissible pairing $e:\mathbb{G}_1\times\mathbb{G}_1\to\mathbb{G}_2$ can be constructed and pick a generator g of $\mathbb{G}_1$.

Now pick a random secret $\alpha\in_R\mathbb{Z}_p$, compute $g_1=g^\alpha$ and pick $g_2\in_R\mathbb{G}_1$. Furthermore, pick elements $u',m'\in_R\mathbb{G}_1$ and vectors $\vec{\boldsymbol{u}}=(u_i),\ \vec{\boldsymbol{m}}=(m_i)$ of length n_u and n_m, respectively, whose entries are random elements from $\mathbb{G}_1$. Here public parameters are params = $\left\langle \mathbb{G}_1,\mathbb{G}_2,e,g,g_1,g_2,u',\vec{\boldsymbol{u}},\ m',\ \vec{\boldsymbol{m}},H_1,H_2,\varphi,\varphi^{-1}\right\rangle$ and the master secret key is g_2^α. Cryptographic hash functions H_1 and H_2 are defined as $H_1:\{0,1\}^\ell\times\mathbb{G}_2\times\mathbb{G}_1^5\to\{0,1\}^k$ and $H_2:\mathbb{G}_2\to\{0,1\}^{n_m}$. $\varphi:\mathcal{R}\to\mathbb{G}_2$ is a bijection while φ^{-1} is its inverse, $\mathcal{R}$ is a subset of $\{0,1\}^{\ell+k}$ with *p* elements. Here ℓ is the length of the plaintext and k is the sufficiently large integer.

Key Generation: Similar to the previous scheme. Also for the convenience we denote $U_A=u'\prod_{j\in U'_A}u_j$ and $U_B=u'\prod_{j\in U'_B}u_j$.

IBSC: To send a message $m\in\{0,1\}^\ell$ to Bob, Alice randomly picks $r\in\mathbb{Z}_p$ and computes

$\sigma_2=g^r,\quad \sigma_3=(u'\prod_{j\in U'_B}u_j)^r,\quad \omega=e(g_1,g_2)^r,\quad R=H_1(m,\omega,\sigma_2,\sigma_3,d_{A2},U_A,U_B)$,

$\sigma_1=\omega\cdot\varphi(m\,||\,R)$, $M=H_2(\sigma_1)$, $\sigma_4=d_{A1}(m'\prod_{j\in M'}m_j)^r$ where $M'\subset\{1,...,n_m\}$ denotes the set of indices j such that $m[j]=1$ ($m[j]$ is the *j*-th bit of *M*). Next Alice sets $\sigma_5=d_{A2}$. The cipher text is $\sigma=(\sigma_1,\sigma_2,\sigma_3,\sigma_4,\sigma_5)$.

IBUSC: On receiving the cipher text $\sigma=(\sigma_1,\sigma_2,\sigma_3,\sigma_4,\sigma_5)$, Bob

1. computes $\hat{M}=H_2(\sigma_1)$
2. generates the corresponding set $M'\subset\{1,...,n_m\}$ of indices *j* such that $m[j]=1$, where $m[j]$ is the *j*-th bit of $\hat{M}$
3. if $e(\sigma_4,g)\neq e(g_1,g_2)e(u'\prod_{j\in U'_A}u_j,\sigma_5)e(m'\prod_{j\in M'}m_j,\sigma_2)$, returns invalid. Otherwise
4. computes $\omega=e(d_{B2},\sigma_3)^{-1}e(d_{B1},\sigma_2)$
5. computes $\varphi^{-1}(\sigma_1\cdot\omega^{-1})\to m\,||\,R$

6. computes $R' = H_1(m, \omega, \sigma_2, \sigma_3, \sigma_5, U_A, U_B)$
7. if $R' \neq R$ returns "invalid". Otherwise returns $\phi = (m, R', \omega, \sigma)$.

TP-Verify (Third party verification): On receiving $\phi = (m, R', \omega, \sigma)$, a sender's identity u_A and a receiver identity u_B. Trusted third party

1. computes $\hat{M} = H_2(\sigma_1)$
2. generates the corresponding set $M' \subset \{1, ..., n_m\}$ of indices j such that $m[j] = 1$, where $m[j]$ is the j-th bit of $\hat{M}$
3. if $e(\sigma_4, g) \neq e(g_1, g_2) e(u' \prod_{j \in U'_A} u_j, \sigma_5) e(m' \prod_{j \in M'} m_j, \sigma_2)$, returns invalid. Otherwise
4. computes $\varphi^{-1}(\sigma_1 \cdot \omega^{-1}) \rightarrow \hat{m} \,||\, \hat{R}$
5. accepts σ and output valid if $\hat{R} = H_1(\hat{m}, \omega, \sigma_2, \sigma_3, \sigma_5, U_A, U_B)$ and $\hat{R} = R'$.

It is easy to verify that the above scheme is consistent.

5.1 Security Analysis of proposed IBPSC scheme

Security analysis of the proposed IBPSC scheme is similar to the previous scheme. Due to space restriction we omit the proof.

6. CONCLUSION

In this paper, we proposed a new identity based signcryption scheme without random oracles which has existential signature unforgeability. In the proposed scheme non-repudiation is directly achieved for the plaintext which help the receiver to convince a third party for the sender's authorship on an extracted plaintext. Further, we also proposed an identity based public verifiable signcryption scheme with third party verification without random oracles.

REFERENCES

[1] Y. Zheng (1997) "Digital signcryption or how to achieve cost (Signature & Encryption) << Cost (Signature) + Cost (Encryption)", *CRYPTO'97*, LNCS # 1294, Springer-Verlag, pp. 165-179.

[2] J. Baek, R. Steinfeld & Y. Zheng (2002) "Formal proofs of security of signcryption", *PKC 02*, LNCS # 2274, pp. 81-98.

[3] F. Bao & R. H. Deng (1998) "A signcryption scheme with signature directly verifiable by public key", *Proceeding of PKC'98*, LNCS # 1431, Springer-Verlag pp. 55-59.

[4] R. Hwang, C. Lai & F. Su (2005) "An efficient signcryption scheme with forward secrecy based on elliptic curve", *Applied Mathematics and Commutation* 165, pp. 870-881.

[5] H. Y. Jung, K. S. Chang, D. H. Lee & J. I. Lim (2001) "Signcryption schemes with forward secrecy", *Proceeding of WISA 2*, pp. 403-233.

[6] Y. Zheng & H. Imai (1998) "How to construct efficient signcryption schemes on elliptic curves", *Information Proceeding Letters*, Vol. 68 No. 5, pp. 227-233.

[7] A. Shamir (1984) "Identity-based cryptosystems and signature schemes", *CRYPTO 84*, LNCS # 196, Springer-Verlag, pp 47-53.

[8] D. Boneh & M. Franklin (2001) "Identity–based encryption scheme from Weil pairing", *CRYPTO 2001*, LNCS # 2139, Springer-Verlag, pp. 213-229.

[9] J. Malone-Lee (2002) "Identity-based signcryption", *Cryptology ePrint Archive* Report 2002/098.

[10] P. S. L. M. Barreto, B. Libert, N. McCullagh & J. J. Quisquater "Efficient and provably-secure identity-based signatures and signcryption from bilinear maps", *ASICRYPT'05*, LNCS 3788, Springer-Verlag, pp. 515-532.

[11] X. Boyen (2003) "Multipurpose Identity based signcryption: A Swiss army knife for identity based cryptography", *CRYPTO 2003*, LNCS # 2729, Springer-Verlag, pp. 389-399.

[12] L. Chen & J. Malone-Lee (2005) "Improved identity-based signcryption", *PKC 2005*, LNCS # 3386, Springer-Verlag, pp. 362-379.

[13] S. S. M. Chow, S. M. Yiu, L. C. K. Hui & K. P. Chow (2003) "Efficient forward and provably secure ID based signcryption scheme with public verifiability and public cipher text authenticity", *ICISC'2003*, LNCS # 2971, Springer-Verlag, pp. 352-369.

[14] B. Libert & J. J. Quisquater (2003) "New identity based signcryption schemes from pairings", *IEEE Information Theory Workshop, Paris, France*, Avalable at *http://eprint.iacr.org/2003/023*, 2003.

[15] N. McCullagh & P.S.L.M. Baarreto (2004) "Efficient and forward secure identity based signcryption", *Cryptology ePrint Archive* Report 2004/117.

[16] S. S. D. Selvi, S. S. Vivek & C. P. Rangan (2010) "Identity based public verifiable signcryption scheme", *Proc. ProvSec 2010*, LNCS # 6402, Springer-Verlag, pp. 244-260.

[17] M. Bellare & P. Rogaway (1993) "Random oracles are practical: a paradigm for designing efficient protocols", *D. Denning et al. (Eds.), Proceedings of the First ACM Conference on Computer and Communications Security ACM Press*, pp. 62-73.

[18] R. Canetti, O. Goldreich & S. Halevi (2004) "The random oracle methodology revisited", *Journal of the ACM* 51 (4) pp. 557-594.

[19] D. Boneh & X. Boyen (2004) "Efficient selective-ID secure identity based encryption without random oracles", *In Eurocrypt'04*, LNCS # 3027, Springer, pp. 223-238.

[20] R. Canetti, S. Halevi & J. Katz (2003) "A forward secure public key encryption scheme. Advances in Cryptology", *EUROCRYPT 2003*, LNCS # 2656, Springer-Verlag, Berlin, pp. 225-271.

[21] Z. Jin, Q. Wen & H. Du (2010) "An improved semantically secure identity based signcryption scheme in the standard model", *Comput Electr Eng*.

[22] K. G. Paterson & J. C. Schuldt (2006) "Efficient identity based signatures secure in the standard model", *Proceedings of the 11th Australasian Conference Information Security and Privacy*, LNCS # 4058, Springer-Verlag, pp. 207-222.

[23] B. Waters (2005) "Efficient identity based encryption without random oracles. Advances in Cryptology", *EUROCRYPT 2005*, LNCS # 3494, Springer-Verlag, Berlin, pp. 114-127.

[24] Y. Yu, B. Yang, Y. Sun & S. L. Zhu (2009) "Identity based signcryption scheme without random oracles", *Computer Standard and Interfaces*, 31 (1) pp. 56-62.

[25] T. H. Yuen & V. K. Wei (2005) "Constant size hierarchical identity based signature/signcryption without random oracles", *Cryptology ePrint Archive*, http:eprint.iacr.org/2005/412.pdf.

[26] B. Zhang & Q. Xu (2010) "An ID-based anonymous signcryption scheme for multiple receivers", *International Journal of Advanced Science and Technology*, Vol. 20, pp. 9-24.

[27] B. Zhang & Q. Xu (2010) "Identity based multi-signcryption scheme without random oracles", *Chinese Journal of Computers*, Issue No. 1, pp. 103-110.

[28] X. Wang & H. Qian (2010) "Attacks against two identity based signcryption schemes", *2nd International Conference NSWCTC'2010*, Wuhan, Hubei, Vol. 1 pp. 24-27.

[29] Q. Xia & C. Xu (2009) "Cryptanalysis of identity based signcryption schemes". *8th IEEE International Conference, DASC'09*, pp. 292-294.

[30] B. Zhang (2010) "Cryptanalysis of an identity based signcryption scheme without random oracles", *Journal of Computational Information Systems* 6:6 (2010) pp. 1923-1931.

[31] M. Zhang, P. Li, B. Yang H. Wang & T. Takagi (2010) 'Towards confidentiality of ID-based signcryption scheme under without random oracle model", *PAISI'2010*, LNCS # 6122, Springer-Verlag, pp. 98-104.

[32] F. Li, Y. Liao & Z. Qin (2011) "Analysis of an identity based signcryption scheme in the standard model", *IEICE Transaction on Fundamentals of Electronics, Communications and Computer Science* E94-A (1), pp. 268-269.

[33] F. Li & T. Takagi (2011) "Secure identity based signcryption in the standard model", *Mathematical and Computer Modelling*, 2011.

[34] S. S. D. Selvi, S. S. Vivek, D. Vinayagamurthy & C. P. Rangan (2011) "On the security of ID based signcryption schemes", *Cryptology ePrint Archive* Report 2011/664.

[35] F. Li, F. B. Muhaya, M. Zhang & T. Takagi (2011) "Efficient identity based signcryption in the standard model", *In X. Boyen and X. Chen (Eds.) ProSec 2011*, LNCS # 6980, Springer-Verlag, pp. 120-137.

[36] E. Kiltz & Y. Vahlis (2008) "CCA2 Secure IBE: Standard model efficiency through authenticated symmetric encryption". *In: Malkin, T. (Ed.) CT-RSA 2008*, LNCS # 4964, Springer, Heidelberg, pp. 221-238.

BIOGRAPHY

Prashant Kushwah is an assistant professor in the department of Mathematics and Statistics at Banasthali University, Rajasthan, India. He obtained his M. Phil. degree from Dr. B. R. A. (Agra) University, India in 2007 and the candidate of Ph.D. from the same. His main research interest includes identity based cryptography mainly signcryption.

Sunder Lal is an ex-professor in the department of mathematics at Dr. B. R. A. (Agra) University in Agra, India. Now he is the Vice Chancellor of VBS Purvanchal University, Jaunpur, India. He obtained his Ph.D. degree in Mathematics from Meerut University in 1974. He is working in Cryptography past 20 years. His main research interest includes secret sharing, digital signature, access control, secret handshake, identity based cryptography.