A Provably Secure ID-Based Signcryption Protocol for Secure and Authentic Energy Efficient Communication

Sunil Kumar
DRDO: Defence Research and Development Organisation
Pratik Gupta
Mandsaur University
Dharminder Dharminder (c_dharminder@ch.amrita.edu)
Amrita Vishwa Vidyapeetham

Research Article

Keywords: Signcryption, Confidentiality, Authenticity, Provable Security, Cryptography

Posted Date: April 19th, 2021

DOI: https://doi.org/10.21203/rs.3.rs-399509/v1

Noname manuscript No.
(will be inserted by the editor)

A Provably Secure ID-Based Signcryption Protocol for Secure and Authentic Energy Efficient Communication

Sunil Kumar · Pratik Gupta · Dharminder Dharminder*

Received: date / Accepted: date

Abstract Singcryption was first proposed by Yuliang Zheng in 1997, based on the construction of a shortened ElGamal-based signature scheme in parallel to *authenticated encryption* in a symmetric environment. Signcryption is a cryptographic primitive that enables the conventional two-step method of secure and authenticated message transmission or storage (sign-then-encrypt or encrypt-then-sign) to be done in a single step at a much lower computational cost than the traditional two-step approach. This article concentrates on designing a provably secure identity-based signcryption (IBSC) scheme. The user performs pairing-free computation during encryption in the proposed scheme, making it user-side effective. In addition, the IBSC structure is shown to be secure when dealing with modified bilinear Diffie-Hellman inversion (MBDHI) and modified bilinear strong Diffie-Hellman (MBSDH) problems. The proposed framework supports efficient communication, protection against chosen cipher attack, and existential unforgeability against chosen message attack, according to the performance review of IBSC with related schemes.

Keywords Signcryption · Confidentiality · Authenticity · Provable Security · Cryptography

Dharminder Dharminder*
Amrita School of Engineering*
Amrita Vishwa Vidyapeetham, Chennai, India

1 Introduction

Achieving secure and authenticated message transmission or storage has been one of the major interests of computer and communication fortified research. Between the beginning of public key infrastructure (PKI) and 1997, the standard notion for obtaining this objective had been to adopt the two-step approach namely signature then encryption or encryption then signature under a randomly chosen key. Then in 1997 presence of a redundant (in the sense not explicitly contained in a signature) parameter in a shortened ElGamal based signature scheme motivates Zheng [1] to introduce a new cryptographic primitive so-called "*signcryption*", for the authentic message delivery or storage. The main aim of signcryption is to provide authentication and non-repudiation of signature and confidentiality of message in a single step with less computation cost, compared to the traditional two-step approach. This makes the scheme more useful in numerous real-time applications such as communication between unmanned vehicles, secure e-mailing, broadcast communication with multiple recipients, and electronic commerce. In addition, Steinfeld et al. [2] and Malone-Lee et al. [3] introduced efficient signcryption scheme using the factorization problem and RSA trapdoor one-way function, respectively.

In 1984, Shamir introduced the concept of *identity-based cryptography* (IBC). The main motivation behind IBC was to simplify many practical problems regarding certificate management system in public key infrastructure like verification of the authenticity of receiver's public key, revocation of certificates by the *Certifying Authority* (CA) and user credential management (before the existence of SSL and TLS protocols).The idea behind an IBC is that the public key can be any string $\in \{0,1\}^*$ such as an e-mail address or phone number, without the need for a CA. In order to work such a system, a trusted authority known as *Private Key Generator* (PKG) generates a private key using the user's identity and own master key, and then sends it to the user through a secure channel. In such a system sender can impose a set of rules for the receiver before the transfer of the receiver's secure key by the PKG. Thus, in an IBC, PKG works as a policy enforcer and this mitigates, a lot of practical problems inherent with the CA system. In 2001, Boneh et al. [5] introduced the first ID-based cryptographic primitive. Since then numerous identity-based cryptosystems using viewpoint of [5] have been designed [6–9].

In 2002, Malone-Lee [10] proposed the first ID-based signcryption scheme. Libert et al. [11], found that this scheme is not secure against semantic attack and introduced a new three IBSC scheme, capturing the insider security model, with public verifiability. Since then numerous efficient IBSC schemes [12–16] have been proposed. All of the above schemes' security proofs have been formulated (or rely upon) using Bellare and Rogaway's random Oracle model [17]. Even though the model is useful but it has been criticized [18] as proofs in random Oracle model only establish working correctness of the scheme as real-world hash functions and random oracles are not at all the same things. Canettie et al. [19] and Bellare et al. [20] also have shown various security threats of using random oracle model. So designing identity-based signcryption without a random oracle model has been an important and interesting work for the researcher. In 2009 using concept of Paterson et al. scheme [21] and Waters' IBE scheme [22], Yu et al. [18] introduced the initial IBSC in standard (ST) model. But in the subsequent years (2010) their scheme was shown insecure under CPA in [23–25]. Meantime Ren et al. [26] proposed an IBSC scheme based on Gentry's [27] approach. Wang et el. [28] identified the weakness in [26] against confidentiality and existential unforgeability. Then, based on Waters IBE, Jin et al. [29] provided an improved semantically secure scheme, but it was not resistant to the IND-CCA2 property and the EUF-CMA property, as discussed in [30]. Another new scheme was proposed by Zhang [25]. But we find that [25] is not IND-CCA2 secure as in challenged ciphertext σ^* an adversary can guess in advance that it is encryption of m_0. Then the adversary can check the validity of signature equation by computing $\hat{R}$= $\sigma_1^*.m_0^{-1}$, $\hat{t} = H_1(m_0||\hat{R})$ and $\hat{\hat{m}} = H_2(g^{\hat{t}}h^{\sigma_6^*})$, and can conclude whether m_0 or m_1 is a plaintext corresponding to the challenged ciphertext [31]. Thereafter in 2016, Ming and Wang [32] demonstrated that the scheme proposed by Li et al. [33] is insecure under the IND-CCA2 property using concrete attacks. In 2020 Dharminder et al. [34] proposed a new scheme, but here also the scheme is not secure against IND-CCA2 property. Thus in conclusion to the best of our knowledge, the majority of ID-based signcryptions proposed thus far are not provably secure. This motivates us to create a new signcryption that can be proven to be provably secure.

1.1 Our contribution

We have proposed a provably secure identity-based signcryption without the use of a random oracle model in this article. Our scheme alleviates the problem of IND-CCA2 (indistinguishable against chosen cipher attack) property. Apart from this, our scheme is computationally efficient due to pairing-free computation on the user side and the use of symmetric key encryption. The proposed work presents that the implementation of the scheme can ensure the confidentiality and authenticity of the data transmitted.

1.2 Paper Organisation:

Section 2 of the remaining paper deals with preliminary work. In section 3, we introduced a formal IBSC model, and in section 4, we define the scheme. Section 5 introduces the most critical work of security-proof. Section 6 compares the performance of the signcryption to that of other similar ones, followed by a discussion in section 7.

2 Preliminaries

This section covers the fundamental tools and definitions of bilinear pairings, as well as some computationally hard problems, which we used to construct our scheme. [5, 11, 12, 16, 21, 22].

2.1 Bilinear Pairings

Let $\mathcal{G}_1$ and $\mathcal{G}_2$ be two well known groups under multiplicative of prime order q and a map $\Phi : \mathcal{G}_1 \times \mathcal{G}_1 \rightarrow \mathcal{G}_2$. Then we say Φ is bilinear pairing under following three properties.

1. Bilinearity:
   - $\Phi(xy, z) = \Phi(x, z) \cdot \Phi(y, z)$
   - $\Phi(x, yz) = \Phi(x, y) \cdot \Phi(x, z)$

   Where $x, y, z \in \mathcal{G}_1$
2. Non-Degeneracy: $\Phi(\hat{x}, \hat{x}) \neq I_{\mathcal{G}_2}$, where $I_{\mathcal{G}_2}$ is the identity of group $\mathcal{G}_2$ and $\hat{x}$ is a generator of $\mathcal{G}_1$
3. Computability: $\forall x, y \in \mathcal{G}_1$, $\Phi(x, y)$ is efficiently computable.

2.2 Hard Assumption

In this subsection, we will describe some hard problems admissible to the proposed scheme.

Definition 1 Bilinear Diffie-Hellman Problem (BDHP): For given a bilinear map $\Phi : \mathcal{G}_1 \times \mathcal{G}_1 \rightarrow \mathcal{G}_2$, and a generator $\hat{x}$ of $\mathcal{G}_1$, the task of BDHP is to compute $\Phi(\hat{x}, \hat{x})^{\alpha\beta\gamma}$ provided polynomial time adversary ($\mathcal{A}$) is aware of $(\hat{x},\ \hat{x}^{\alpha},\ \hat{x}^{\beta},\ \hat{x}^{\gamma})$, where $\alpha,\ \beta,\ \gamma\ \in\ Z_q^*$; i.e., multiplicative group of order $p-1$.

Definition 2 Decision Bilinear Diffie-Hellman Problem (DBDHP): Given a generator $\hat{x}$ of $\mathcal{G}_1$ and a bilinear map $\Phi : \mathcal{G}_1 \times \mathcal{G}_1 \rightarrow \mathcal{G}_2$, the task of DBDHP is to differentiate between $\Phi(\hat{x}, \hat{x})^{\alpha\beta\gamma}$ and $\Phi(\hat{x}, \hat{x})^{h}$ provided $\mathcal{A}$ is aware of $(\hat{x},\ \hat{x}^{\alpha},\ \hat{x}^{\beta},\ \hat{x}^{\gamma})$ and $h \in Z_q^*$ is random.

Definition 3 q-Modified Bilinear Diffie-Hellman Inversion (q-MBDHI) Problem: Given a generator $\hat{x}$ of $\mathcal{G}_1$ and a bilinear map $\Phi : \mathcal{G}_1 \times \mathcal{G}_1 \rightarrow \mathcal{G}_2$, the task of q-MBDHI is to compute $\Phi(\hat{x}, \hat{x})^{\frac{1}{\alpha^2}}$ with given $< \hat{x}, \hat{x}^{\alpha}, \hat{x}^{\alpha^2}, \cdots, \hat{x}^{\alpha^{q-1}} >$ by submitting polynomial queries, where $\alpha \in Z_q^*$ is a random number.

Definition 4 q-Modified Bilinear Strong Diffie-Hellman (q-MBSDH) Problem: Given a generator $\hat{x}$ of $\mathcal{G}_1$ and a bilinear map $\Phi : \mathcal{G}_1 \times \mathcal{G}_1 \rightarrow \mathcal{G}_2$, the task of q-MBSDH is to compute $\Phi(\hat{x}, \hat{x})^{\frac{\beta(\alpha+\gamma)}{\alpha+\delta}}$ with given $< \hat{x}, \hat{x}^{\alpha}, \hat{x}^{\alpha^2}, \cdots, \hat{x}^{\alpha^{q-1}} >$ by submitting polynomial queries, where $\alpha, \beta, \gamma, \delta \in Z_q^*$ are random numbers.

3 Formal Model of IBSC

This section is pertaining to the basic definition and security notion for our proposed IBSC scheme.

3.1 Generic model

An IBSC essentially is consisting of the four algorithms.

- **Setup:**The private key generator (PKG) executes the setup algorithm and produces the system's public parameters *paramts* and a master key *MK* under security parameter 1^k. The PKG then publishes the *paramts* and stores *MK* in a secure location.
- **Extract:** In this phase PKG runs key generation algorithm using his master key *MK* and identity $ID_A \in \{0,1\}^*$ of user A, and creates private key SK_A corresponding to ID_A

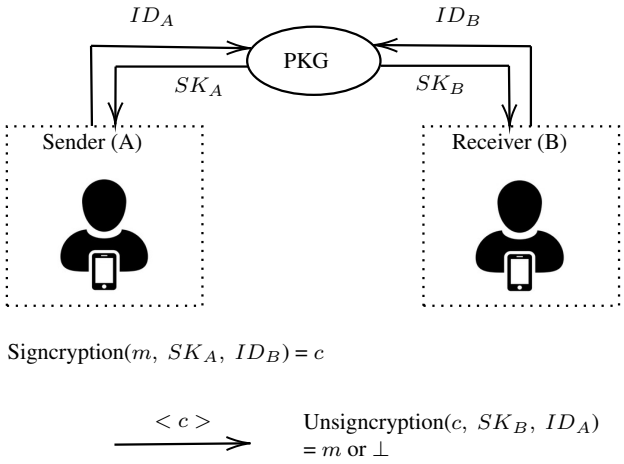

Fig. 1: Illustration of ID-based signcryption communication

– **Signcryption:** In this phase sender A takes his identity ID_A, message m and compute ciphertext $c =$ Signcryption(m, SK_A, ID_B), where ID_B is identity of receiver B.
– **Unsigncryption:** Receiver B computes Unsigncryption (c, SK_B, ID_A) after receiving ciphertext c, to get the message m or the symbol $\perp$ stating that c is a invalid ciphertext.

The schematic representation of an IBSC model is illustrated in Figure 1.

3.2 Security Notions

Our proposed scheme satisfies two main IBSC security concepts.

1. Indistinguishable under adaptive chosen ciphertext attack (IND-CCA2).
2. Existential unforgeable against adaptive chosen message attack (EUF-CMA)] [8, 18, 22].

Definition 5 An IBSC possesses IND-CCA2 property if in the game played between a challenger($\mathcal{C}$) and an adversary ($\mathcal{A}$), an adversary ($\mathcal{A}$) gains a non-negligible advantage.

Initial: $\mathcal{C}$ executes the setup phase under security parameter 1^k and obtains *paramts* and a master key *MK*. He sends *paramts* to $\mathcal{A}$ and keep *MK* secretly with himself.
Phase-1: A polynomial bounded queries are executed between $\mathcal{A}$ and $\mathcal{C}$. In fact these queries are performed by $\mathcal{A}$ and may be made adaptively as follows.

1. Key-generation: $\mathcal{A}$ chooses ID_A and submits to $\mathcal{C}$, then $\mathcal{C}$ computes $SK_A = Extract(ID_A)$ and sends SK_A to $\mathcal{A}$.
2. Signcryption: $\mathcal{A}$ chooses ID_A and ID_B, as well as a message m. Then $\mathcal{C}$ computes $SK_A = Extract(ID_A)$ and $c =$ Signcryption(m, SK_A, ID_B) and sends c to $\mathcal{A}$.
3. Unsigncryption: $\mathcal{A}$ gets ID_A and ID_B, and a cipher c, then $\mathcal{C}$ generates $SK_B = Extract(ID_B)$ and forwards the result Unsigncryption(c, ID_B, SK_A) to $\mathcal{A}$.

Challenge: Finally, after completing phase-1 (as determined by $\mathcal{A}$), $\mathcal{A}$ chooses $m_0, m_1 \in \{0,1\}^k$ and two identities, ID_A^* and ID_B^*, for which it wishes to receive a challenge, and sends them to C. In this case, $\mathcal{A}$ should not have asked SK_B^* in phase-1. $\mathcal{C}$ selects a random bit $b \in \{0,1\}$ and executes c^* = Signcryption(m_b, SK_A^*, ID_B^*). Now, as a challenge, $\mathcal{C}$ now sends c^* to $\mathcal{A}$.
Phase-2: $\mathcal{A}$ receives cipher c^*, and as in phase-1, adaptively performs polynomial bounded queries. But now he is not allowed to ask for SK_B^* and Unsigncryption(c^*, ID_A^*, SK_B^*).
Guess: $\mathcal{A}$ guesses a bit b' at the end of phase-2 and wins the game if $b' = b$.

Definition 6 In the EUF-CMA phase defined below, an IBSC is EUF-CMA if adversary $\mathcal{A}$ gains a non-negligible advantage.

EUF-CMA-phase: The game is played in the same way as in phase-1, $\mathcal{C}$ runs setup(1^k) and generates parameters, which he sends to A, who then executes queries in the same way as in phase-1. At last, $\mathcal{A}$ produces a triplet (c', ID'_A, ID'_B) as a forgery, where private key i.e. SK'_A never extracted during the process

of attack. If Unsigncryption($c^{'},\ ID_A,\ SK_B$) returns a value other than the $\perp$ symbol, $\mathcal{A}$ wins the game.

4 Proposed provable secure signcryption scheme

We have described the signcryption in the four phases namely, (1) setup, (2) key-extraction, (3) signcryption, and (4) unsigncryption. The setup is responsible to generate the essential parameter for the corresponding PKG. And private key of the corresponding user or receiver is generated by key extraction. The scheme possesses the architecture as

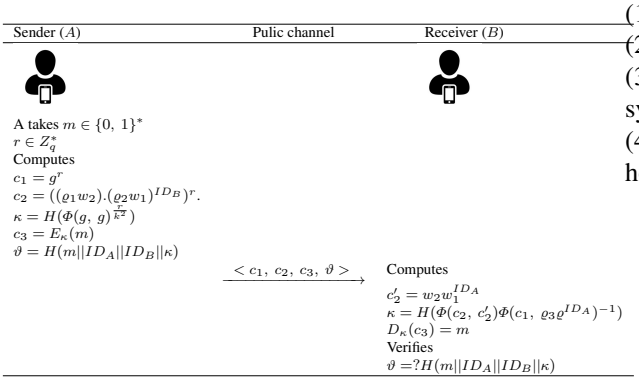

Fig. 2: Registration phase executed via secure channel

Setup (1^κ)**:** $\mathcal{PKG}$ executes the setup algorithm under security parameter κ, and generates two groups $(\mathcal{G}_1,\ \mathcal{G}_2)$ of order "q", where q is an arbitrary large prime number, $g \in \mathcal{G}_1$ is a generator of the group, $\Phi : \mathcal{G}_1 \times \mathcal{G}_1 \rightarrow \mathcal{G}_2$ is a bilinear map, $E,\ D$ symmetric encryption, decryption and $H : \{0,1\}^* \rightarrow Z_q^*$ is a collision resistant hash function. Now, it chooses arbitrary random $g,\ \varrho \in \mathcal{G}_1$ and $s,\ k \in Z_q^*$ and computes necessarily the values $\varrho_1 = \varrho^{ks},\ \varrho_2 = \varrho^k,\ \varrho_3 = \varrho^s,\ Z = \Phi(g,\ g)^{\frac{1}{k^2}}$. These values $paramts = (g,\ \varrho,\ \varrho_1,\ \varrho_2,\ \varrho_3,\ Z,\ \Phi,\ H,\ E,\ D)$ are published in public and master key $MK = (s,\ k)$ is kept secret.

Extraction ($paramts,\ MK,\ ID_A$)**:** $\mathcal{PKG}$ obtains MK, ID_A and computes private key for ID_A as, $w_1 = g^{\frac{1}{k(s+ID_A)}}$, $w_2 = w_1^s$, sends $SK_A = (w_1,\ w_2)$ to the ID_A under secure communication.

Signcryption ($m,\ paramts,\ ID_A,\ SK_A,\ ID_B$)**:** The sender A takes an arbitrary message $m \in \{0,\ 1\}^*$ along with public parameters, then he chooses an arbitrary $r \in Z_q^*$ and executes as :

(1) Calculates $c_1 = g^r$.
(2) Calculates $c_2 = ((\varrho_1 w_2).(\varrho_2 w_1)^{ID_B})^r$.
(3) Calculates $\kappa = H(\Phi(g,\ g)^{\frac{r}{k^2}})$, where "$\kappa$" is fixed length key for AES or DES algorithms. (4) Calculates $c_3 = E_\kappa(m)$, where "E" stands for symmetric encryption algorithm.
(4) Calculates $\vartheta = H(m||ID_A||ID_B||\kappa)$.
(5) Finally, the output $c = (c_1,\ c_2,\ c_3,\ \vartheta)$ is sent to the corresponding receiver (B).

Unsigncryption ($c,\ paramts,\ ID_B,\ SK_B,\ ID_A$)**:** The receiver "B" obtains the encrypted text $c = (c_1,\ c_2,\ c_3,\ \vartheta)$, and follows the decryption of "c" as follows:
(1) Calculate $c_2' = w_2 w_1^{ID_A}$.
(2) Calculate $\kappa = H(\Phi(c_2,\ c_2')\Phi(c_1,\ \varrho_3 \varrho^{ID_A})^{-1})$.
(3) Calculate $D_\kappa(c_3) = m$, where "D" stands for symmetric decryption algorithm.
(4) Message is autnentic if $\vartheta =?H(m||ID_A||ID_B||\kappa)$ holds.

5 Security and correctness analysis

We have analyzed the signcryption under the MBDHI and MBSDH assumptions, where $\mathcal{C}$ and $\mathcal{A}$ play a game. $\mathcal{C}$ uses $\mathcal{A}$ as a subroutine to break down security and, under hard assumptions, solves an arbitrary instance of the given problem. However, theorem (4.1) ensures the correctness of the scheme, theorem (4.2) and theorem (4.3) ensures confidentiality and unforgeability of the scheme respectively.

Theorem 4.1. Proposed signcryption follows the mathematical correctness i.e. if sender "A" follows the given signcryption algorithm, the message is always recovered correctly by receiver "B" with the correct secret key.

Proof. The receiver "B" gets $SK_B = (w_1,\ w_2)$, where $w_1 = g^{\frac{1}{k(s+ID_B)}}$, $w_2 = w_1^s$, and computes "c_2'" as

$$w_2.w_1^{ID_A} = g^{\frac{s+ID_A}{k(s+ID_B)}} \tag{1}$$

Now, "B" uses the equation (1) and computes

$$d = \Phi(c_2,\ c_2')\Phi(c_3, \varrho_3 \varrho^{ID_A})^{-b} \quad (2)$$

$$= \frac{\Phi(\varrho^{rk(s+ID_B)},\ g^{\frac{s+ID_A}{k(s+ID_B)}}).\Phi(g,\ g)^{\frac{r(s+ID_B)}{k(s+ID_A)}\frac{(s+ID_A)}{k(s+ID_B)}}}{\Phi(g^r,\ \varrho^{s+ID_A})} \quad (3)$$

$$= \frac{\Phi(g,\ \varrho)^{r(s+ID_A)}\Phi(g,\ g)^{\frac{r}{k^2}}}{\Phi(g,\ \varrho)^{r(s+ID_A)}} \quad (4)$$

$$= \Phi(g,\ g)^{\frac{r}{k^2}} \quad (5)$$

Therefore, "B" uses the equation (2) and computes $m' = d^{-1}.c_3$ and gets the correct message. Now, "B" confirms the verification with the help of the equations (1) and (2) as $\vartheta? = H(m'||ID_A||ID_B||d)$.

Theorem 4.2. Under the q-MBDHI assumption, If $\mathcal{A}$ can distinguishes two ciphers in IND-CCA2 phase defined in definitions (5) and (6) with an arbitrarily however small advantage ϵ via executing polynomial times private key extractions at most q_e in time t, where q_1 and q_2 are signcryption unsigncryption queries. Then, one can design a subroutine or distinguisher $\mathcal{B}$ who can solve a problem instance in time $t + O((6q_e + 5q_1 + 4q_2)T_e + q_1T_p)$, where T_e exponentiation time, T_p pairing time respectively.

Proof. If $\mathcal{A}$ breaks down the security of proposed scheme, then one can easily model a subroutine algorithm $\mathcal{B}$, who solves decision version of the q-MBDHI assumption by using subroutine $\mathcal{A}$. In general, $\mathcal{B}$ has to distinguish $\Phi(g,g)^{\frac{1}{x^2}}$ from an arbitrary instance $\Phi(g,g)^z$, where $< g,\ g^x,\ g^{x^2},\ \ldots,\ g^{x^q} >$ given and $x \leftarrow Z_q^*$ is a random number respectively. For simplicity, one can assume that $I_i = g^{x_i}$, where $i \in Z_q$. Now, a challenger in the game $\mathcal{C}$ chooses a random $b \in \{0,1\}$ and if $b = 0$, then sets $Z' = \Phi(g,\ g)^{\frac{1}{x^2}}$, otherwise sets $Z' = \Phi(g,g)^z$, where $z \leftarrow Z_q^*$ is random and it sends $(Z',\ T,\ H)$ to $\mathcal{B}$.

Setup-phase : In setup, $\mathcal{B}$ chooses $P(y) = \pi_{i=0}^{q-2}(y + ID_i) = \Sigma_{i=0}^{q-2}(\alpha_i y^i)$ and an arbitrary random $\beta \leftarrow Z_q^*$ respectively. Now, $\mathcal{B}$ computes $g' = g^\beta$ and $\varrho_3' = \prod_{i=0}^{q-2}(I_{i+1})^{\alpha_i} = g^{xp(x)}$, $\varrho' = g^{p(x)}$, $\varrho_2' = (\varrho_3')^\beta$ and $\varrho_1' = (\prod_{i=0}^{q-2}(I_{i+2})^{\alpha_i})^\beta = g^{x^2\beta p(x)}$, then sends $paramts = (g',\ \varrho',\ \varrho_1',\ \varrho_2',\ \varrho_3',\ E,\ D,\ \Phi,\ Z',\ H)$ to $\mathcal{A}$ and keeps master key $MK = \beta$ secret.

Phase 1: $\mathcal{A}$ asks polynomial times any of the query "q_i" as discussed above.

Extraction Queries: If $\mathcal{A}$ submits a query on secret key related to an identity ID_i, then $\mathcal{B}$ chooses polynomials of $(q-4)$ degree as

$$F_{\omega_1,ID_i}(y) = \frac{P(y)+1}{y(y+ID_i)} + \mu_0 = \sum_{j=0}^{q-2}\mu_j y^j$$

$$F_{\omega_2,ID_i}(y) = \frac{P(y)+y}{y(y+ID_i)} + \mu_0' = \sum_{j=0}^{q-2}\mu_j' y^j$$

$$F_{ID_i}(y) = \frac{P(y)}{y(y+ID_i)} + \delta_0 = \sum_{j=0}^{q-2}\delta_j y^j$$

$\mathcal{B}$ computes w_1' and w_2' as $w_1' = \prod_{i=0}^{q-2}\frac{(I_i)^{\mu_i}}{\varrho'^{\mu_0}} = (\varrho')^{\frac{1}{x(x+ID_i)}} g^{\frac{1}{x(x+ID_i)}}$, $w_2' = \prod_{i=0}^{q-2}\frac{(I_i)^{\mu_i'}}{\varrho'^{\mu_0'}} = (\varrho')^{\frac{1}{x(x+ID_i)}} g^{\frac{x}{x(x+ID_i)}}$, and $w = \prod_{i=0}^{q-2}\frac{(I_i)^{\delta_i}}{\varrho'^{\delta_0}} = (\varrho')^{\frac{1}{x(x+ID_i)}}$.

Therefore, $\mathcal{B}$ can generate $w_1 = \frac{w_1'}{w} = g^{\frac{1}{x(x+ID_i)}}$, $w_2 = \frac{w_2'}{w} = g^{\frac{1}{(x+ID_i)}}$ and sends back $sk_i = (w_1,\ w_2)$ as a reply to $\mathcal{A}$ related to the query of ID_i.

Signcryption Queries: If $\mathcal{A}$ submits a polynomial times queries for $(m_i,\ {ID_A}^i,\ {ID_B}^i)$, and then $\mathcal{B}$ generates corresponding to the secret key SK_B under extraction phase and returns $c_i = Signcryption(m_i,\ {Sk_A}^i,\ {ID_A}^i,\ {ID_B}^i)$ to $\mathcal{A}$.

Unsigncryption Queries: If $\mathcal{A}$ submits $(c_i,\ {ID_A}^i,\ {ID_B}^i)$, then $\mathcal{B}$ generates corresponding to the secret key SK_B by executing the extraction queries, and then returns $Unsigncryption(c_i,\ ID_A, paramts,\ ID_B,\ SK_B)$ to $\mathcal{A}$.

Challenge: If $\mathcal{A}$ queries $(m_0,\ m_1,\ ID_A^*,\ ID_B^*)$, then $\mathcal{B}$ chooses an arbitrary $b \in \{0,\ 1\}$ and generates signcryptext $c^* = (c_1^*,\ c_2^*,\ c_3^*,\ \vartheta^*)$ as :

(1) $\mathcal{B}$ chooses an arbitrary $r \leftarrow Z_q^*$ and computes $c_1^* = g^r$.
(2) $\mathcal{B}$ computes $SK_A^* = (w_1,\ w_2)$ using extraction-phase.
(3) $\mathcal{B}$ computes ${c_2}^* = ((\varrho_1' w_2).(\varrho_2' w_1)^{ID_B^*})^r$, then $\vartheta^* = H((m_b||ID_A^*||ID_B^*||\Phi(g,\ g)^{\frac{r}{k^2}})$, $\kappa = H(\Phi(g,\ g)^{\frac{r}{k^2}}))$ and then computes $c_3^* = E_\kappa(m_b)$.

Now, $\mathcal{B}$ sends a challenge c^* to $\mathcal{A}$, under the assumption $k = x\beta$, $\varrho_1' = {\varrho'}^{kx}, \varrho_2' = {\varrho'}^k, \varrho_3' = {\varrho'}^x$, $\kappa' = H(\Phi(g',\ g')^{\frac{1}{k^2}})$, $w_1 = {g'}^{\frac{1}{k(x+ID_i)}}$ and $w_2 = {g'}^{\frac{x}{k(x+ID_i)}}$, where all the distributions are

uniform for $\mathcal{A}$.

Phase 2: $\mathcal{A}$ submits adaptive queries to $\mathcal{B}$ following the phase (1), except an extraction queries on ID_B^* and $Unsigncryption(c^*,\ ID_A^*,\ ID_B^*)$.

Guess: At last,
$mathcal A$ guesses a bit $b' \in \{0,1\}$ and wins the game if $b' = b$.

Probability : If $\xi = 0$, then $\mathcal{A}$ answers m_b, where $b \leftarrow \{0,\ 1\}$ with advantage ϵ, it has $pr[\xi = 0|b' = b] = \frac{1}{4} + \epsilon$ and if $\mathcal{B}$ guesses $\xi' = 0$ under $b' = b$, so one gets $pr[\xi' = \xi|\xi = 0] = \frac{1}{4} + \epsilon$. Now, if $\xi = 1$, then $\mathcal{A}$ cannot recover correct "b" and estimated probability is given $Pr[\xi = 1|c \neq c'] = \frac{1}{4}$. If $\mathcal{B}$ answers correct $\xi' = 1$ when $b' \neq b$, then $Pr[\xi' = \xi|\xi = 1] = \frac{1}{4}$. Therefore, $\mathcal{B}$ gains an advantage in decision version of q-MBDHI game as

$$\epsilon' = \tfrac{1}{2}Pr[\xi' = \xi|\xi = 0] + \tfrac{1}{2}[\xi' = \xi|\xi = 1] - \tfrac{1}{2} = \tfrac{1}{2}(\tfrac{1}{4} + \epsilon) + \tfrac{1}{2}(\tfrac{1}{4}) - \tfrac{1}{2} = \tfrac{1}{2}(\epsilon - \tfrac{1}{2})$$

Time analysis: In extractions, signcryptions and unsigncryptions phases, Oracle requires $3q_eT_e$, $5q_1T_e$ and $(5T_e + T_p)q_2$ operations respectively. Therefore, $\mathcal{B}$ costs $t' = t + O(6q_e + 5q_1 + 4q_2)T_e + q_1T_p$ to be successful in the game.

Theorem 4.3. Our signcryption is $(t,\ q_e,\ q_1,\ q_2,\ \epsilon)$ existential unforgeable under chosen message (EUF-CMA) with $(t',\ q,\ \epsilon')$ q-MBSDH assumption, where $\epsilon' = \epsilon$ and $t' = t + O((2q_e + 5q_1 + 4q_2)T_e + q_2T_p)$, where q_e extractions, q_1 signcryptions and q_2 unsigncryptions queries in polynomial time "t", T_e exponentiation-time, T_p pairing-time respectively.

Proof. If $\mathcal{A}$ can break down the security of the proposed signcryption, then one can develop an algorithm $\mathcal{B}$ under q-MBSDH problem using subroutine $\mathcal{A}$. Let $T =< g,\ g^x,\ g^{x^2},\ \ldots,\ g^{x^q} >$ for an arbitrary random $x \leftarrow Z_q^*$ be a random instance sent by challenger $\mathcal{C}$. Now, $\mathcal{B}$ tries to estimate correct $\rho = \Phi(g,\ g)^{\frac{k_1+x}{k_2+x}}$ for some arbitrary random $k_1,\ k_2 \leftarrow Z_q^*$. Now, $\mathcal{C}$ publishes all parameters $(p,\ \mathcal{G}_1,\ \mathcal{G}_2,\ \Phi,\ T,\ H)$ same as in theorem (2), and $I_i = g^{x_i}$, where $i \in Z_q$.

Setup: $\mathcal{B}$ uses the setup phase as in theorem (2), and publishes the values $paramts = (g',\ \varrho',\ \varrho_1',\ \varrho_2',\ \varrho_3',\ \Phi,\ Z,\ H)$, where master key is secret $MK = \beta$.

Now, $\mathcal{A}$ will ask at most q_s queries, but one at a time to $\mathcal{C}$ respectively.

Extraction queries: $\mathcal{B}$ follows the theorem (2), and generates w_1 and w_2 as $w_1 = \frac{w_1'}{w} = g^{\frac{1}{x(x+ID_i)}}$ and $w_2 = \frac{w_2'}{w} = g^{\frac{1}{(x+ID_i)}}$, then it will return $Sk_i = (w_1,\ w_2)$ to $\mathcal{A}$ relative to ID_i respectively.

Signcryption queries: If $\mathcal{A}$ sends query $(m_i,\ {ID_A}^i,\ {ID_B}^i)$, then $\mathcal{B}$ chooses an arbitrary random $r \leftarrow Z_q^*$ and calculates $c_1^i = (g')^r$. Now, $\mathcal{B}$ sets $k = x\beta$, then it computes $w_1 = \frac{w_1'}{w} = {g'}^{\frac{1}{k(x+ID_A)}}$ and $w_2 = \frac{w_2'}{w} = {g'}^{\frac{x}{k(x+ID_A)}}$. Furthers $\mathcal{B}$ computes $c_2^i = ((\varrho_1' w_2).(\varrho_2' w_1)^{ID_B})^r$ and $\vartheta_i = H(m||ID_B^*||ID_A^*||\Phi(g,\ g)^{\frac{r}{k^2}})$ and returns $c^i = (c_1^i,\ c_2^i,\ c_3^i,\ \vartheta)$ to $\mathcal{A}$.

Unsigncryption queries: If $\mathcal{A}$ submits a query related to $(c,\ ID_A^i,\ ID_B^i)$, then $\mathcal{B}$ calls extraction-phase to construct SK_B, and then it generates $Unsigncryption(c^i,\ paramts,\ ID_A,\ ID_B,\ SK_B)$ sends to $\mathcal{A}$.

Forgery: After submitting polynomial times queries, $\mathcal{A}$ guesses $(m^*,\ c^*,\ ID_A^*,\ ID_B^*)$, where $(m^*,\ ID_A^*,\ ID_B^*)$ has never been queried to $\mathcal{B}$. However, $c^* = (c_1^*,\ c_2^*,\ c_3^*,\ \vartheta^*)$ claims a correct signcryption, so $\mathcal{B}$ confirms that c^* is correct generated by $\mathcal{A}$. Now, $\mathcal{B}$ views $c_2^* = (\rho_2')^{r^*(x+ID_B^*)}.(g')^{\frac{r^*(x+ID_B^*)}{k(x+ID_A^*)}}$, where $r^* \leftarrow Z_q^*$ randomly chosen by $\mathcal{A}$. Now, $\mathcal{B}$ sets a polynomial as $\psi(y) = y.(y + ID_B^*)P(y) + \delta_0 = \sum_{i=0}^{q} \delta_i y^i$, where $\delta_0,\ \delta_i,\ \ldots,\ \delta_q \in Z_q^*$.

Now, $\mathcal{B}$ computes $d = (\prod_{i=0}^{q} I_i^{\delta_i})^{\beta}(g^{\beta\delta_0})^{-1} = (g^{x\beta(x+ID_B^*)P(x)}.g^{\beta\delta_0}.g^{-\beta\delta_0} = (\rho_2')^{(x+ID_B^*)}$. Furthers $\mathcal{B}$ computes $\tilde{\rho} = \Phi(c_2^*,\ g)(\Phi(c_1^*,\ d^{\frac{1}{\beta}}))^{-1} = \Phi(d^{r^*}.(g')^{\frac{r^*(x+ID_B^*)}{k(x+ID_A^*)}},\ g)(\Phi(c_1^*,\ d^{\frac{1}{\beta}}))^{-1} = \Phi(d^{r^*},\ g).\Phi((g')^{\frac{r^*(x+ID_B^*)}{k(x+ID_A^*)}},\ g).(\Phi(c_1^*,\ d^{\frac{1}{\beta}}))^{-1} = \Phi(d,\ g)^{r^*}.\Phi(g,\ g)^{\frac{\beta r^*(x+ID_B^*)}{k(x+ID_A^*)}}.(\Phi(c_1^*,\ d^{\frac{1}{\beta}}))^{-1} = \Phi(g,g)^{\frac{\beta r^*(x+ID_B^*)}{k(x+ID_A^*)}}$.

Finally, $\mathcal{B}$ claims a q-MBSDH solution relative to the challenge $((c_1^*)^{\frac{1}{\beta}},\ T)$ as $\rho = \tilde{\rho}^{\frac{k}{\beta}} = \Phi(g,\ g)^{\frac{r^*(x+ID_B^*)}{(x+ID_A^*)}}$. In order to output a correct signcryptext corresponding to the challenge $(m^*,\ c^*,\ ID_A^*,\ ID_B^*)$, $\mathcal{B}$ requires $3q_eT_e,\ 5q_1T_e$ and $(4T_e + T_p)q_2$ times queries during signcryption and unsigncryption respectively. Therefore, $\mathcal{B}$ takes time $t' = t + O((2q_e + 4q_1 + 4q_2)T_e + q_2T_p)$ to breach q-

MBSDH assumption, which is not possible, hence no such $\mathcal{B}$ exists.

6 Performance analysis

This scheme uses the public parameters as groups $\mathcal{G}_1$ and $\mathcal{G}_2$, a bilinear map Φ and a collision resistant hashing, where the scheme is being efficient due to pairing-free computation on sender-side during signcryption. The signcryptext c is 3-tuple with size in terms of group elements is $|c| = 2|\mathcal{G}_1| + 1|AES| + 1|Hash|$ where hashing-160 bits, Z_q^*-1024 bits, E_{sym}-128 bits, message m-128 bits, $\mathcal{G}_2$-1024 bits and $\mathcal{G}_1$-160 bits, where total cost of [18, 29, 33, 34, 36, 37] is given in Figure 4.

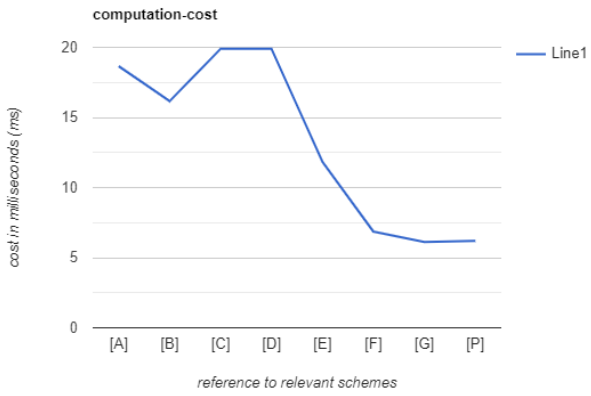

Fig. 4: Computation analysis with existing relevant schemes

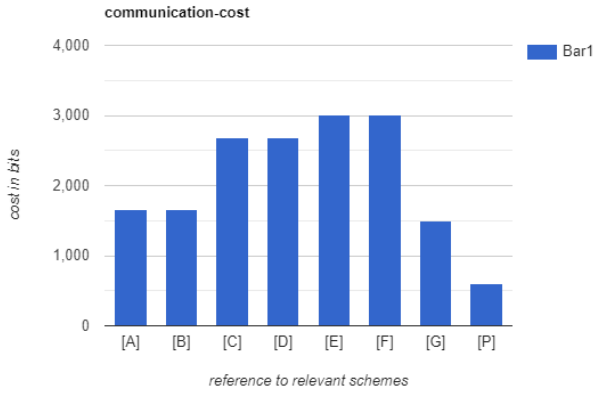

Fig. 3: Communication in terms of bits with existing relevant schemes

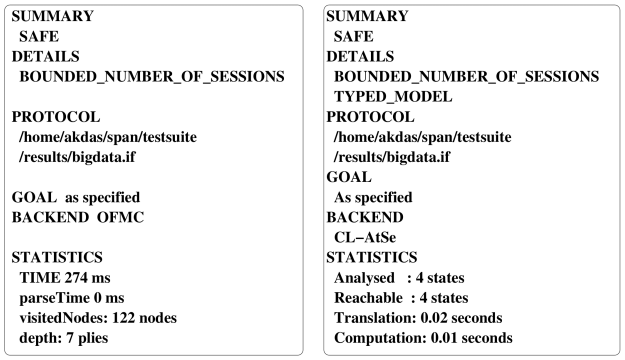

Fig. 5: Analysis under CL-AtSe and OFMC backends

Moreover, various cryptographic operations [34] such as, bilinear costs $t_p \approx 2.485$ ms, one exponentiation costs $t_e \approx 0.311$ ms in $\mathcal{G}_1$, 0.058 ms in $\mathcal{G}_2$ point-add arithmetic $t_a \approx 0.001$ ms, point-mul $t_m \approx 0.317$ ms for multiplications, inversion group costs $t_i \approx 0.009$ ms, symmetric-encryption costs $t_{sym} \approx 0.0817$ ms and hashing $t_h \approx 0.004$ ms in the proposed scheme, where cryptographic operations costs taken via experiment $Sony - i_5$- personal computer with processor i5-2310M CPU@2.10 GHzs and 2-GB-RAM on 14.04 Ubuntu.

Moreover, Table 1 shows a relevant comparison between the signcryptions based on the indepedent operations run in signcryption-phase, unsigncryption-phase in the proposed scheme. Moreover, various relevant schemes [18] takes $4t_e + t_p$ in signcryption and $6t_p+1t_i$ costs in unsigncryption, [29] costs $4t_e$ in signcryption and costs in unsigncryption $6t_p + 1t_i$, [35] costs in signcryption $6t_e + t_p$ and costs in unsigncryption $2t_e + 6t_p + 1t_i$, [33] costs in signcryption and costs in unsigncryption $6t_e + t_p$, [36] costs in signcryption $6t_e$ and costs in unsigncryption $4t_p+1t_i$, [37] costs during signcryption $4t_e + t_h$ and costs during unsigncryption $2t_e + 2t_p + 2t_i + t_h$, [34] costs during signcryption $3t_e + t_h$ and costs during unsigncryption $1t_e + 2t_p + 1t_i + t_h$ and proposed scheme costs $3t_e + t_h + t_{sym}$ in signcryption and $1t_e + 2t_p + 1t_i + t_h + t_{sym}$ in unsigncryption, where total cost is $4t_e + 2t_p + 1t_i + 2t_h + 2t_{sym}$ respectively.

Therefore, various discussed schemes [18] costs $7t_p + 1t_i + 4t_e \approx 18.648$ ms, [29] costs $6t_p + 4t_e + 1t_i \approx 16.163$ ms, [35] costs $7t_p + 8t_e + 1t_i \approx 19.892$ ms, [33] costs $7t_p + 8t_e + t_i \approx 19.892$ ms, [36]

Schemes	Signcryption-side	Unsigncryption-side	Total number of operations	Communication cost
$[A]$ Yu et al. [18]	$4t_e + t_p$	$6t_p + 1t_i$	$7t_p + 1t_i + 4t_e$	$4\|\mathcal{G}_1\| + \|\mathcal{G}_2\|$
$[B]$ Jin et al. [29]	$4t_e$	$6t_p + 1t_i$	$6t_p + 4t_e + 1t_i$	$4\|\mathcal{G}_1\| + \|\mathcal{G}_2\|$
$[C]$ Selvi et al. [35]	$6t_e + t_p$	$2t_e + 6t_p + 1t_i$	$7t_p + 8t_e + 1t_i$	$4\|\mathcal{G}_1\| + 4\|Z_q^*\|$
$[D]$ Li et al. [33]	$6t_e + t_p$	$2t_e + 6t_p + t_i$	$7t_p + 8t_e + t_i$	$4\|\mathcal{G}_1\| + \|\mathcal{G}_2\| + \|Z_q^*\|$
$[E]$ Wei et al. [36]	$6t_e$	$4t_p + 1t_i$	$6t_e + 4t_p + 1t_i$	$6\|\mathcal{G}_1\| + \|\mathcal{G}_2\| + \|Z_q^*\|$
$[F]$ Karati et al. [37]	$4t_e + t_h$	$2t_e + 2t_p + 2t_i + t_h$	$6t_e + 2t_p + 2t_i + t_h$	$3\|\mathcal{G}_1\| + 1\|\mathcal{G}_2\| + \|m\|$
$[G]$ Dharminder et al. [34]	$3t_e + t_h$	$1t_e + 2t_p + 1t_i + t_h$	$4t_e + 2t_p + 1t_i + 1t_h$	$3\|\mathcal{G}_1\| + Z_q^*$
$[P]$ Proposed	$3t_e + t_h + t_{sym}$	$1t_e + 2t_p + 1t_i + t_h + t_{sym}$	$4t_e + 2t_p + 1t_i + 2t_h + 2t_{sym}$	$2\|\mathcal{G}_1\| + 2\|AES\| + 2\|Hash\|$

Table 1: Performance analysis and comparison with existing schemes.

costs $6t_e + 4t_p + 1t_i \approx 11.735$ ms, [37] scheme costs $6t_e + 2t_p + 2t_i + t_h \approx 6.858$ ms, [34] costs $4t_e + 2t_p + 1t_i + 1t_h \approx 6.127$ ms and proposed scheme costs $4t_e + 2t_p + 1t_i + 2t_h + 2t_{sym} \approx 6.289$ms (see 4) respectively.

We used AVISPA, an excellent verification tool, to demonstrate the resistance against replay and man-in-the-middle attacks. The "On-the-fly Model-Checker (OFMC)", "Constraint Logic-based Attack Searcher (CL-AtSe)", "SATbased Model-Checker (SATMC)", and "Tree Automata based on Automated Approximations for the Study of Security Protocols (TA4SP)" are the four backends that make up AVISPA.

7 Conclusion

This article demonstrates an efficient and secure signcryption technique based on MBDHI and MBSDH hard problems.This scheme ensures that confidentiality is indistinguishable from the chosen cipher, and that authenticity is existentially unforgeable from the chosen message. This scheme attains efficiency on the user end as it is being paired free. In terms of computing and communication costs, the proposed scheme has been compared to other similar schemes. Therefore, it becomes very useful where both confidentiality and authenticity required in one step. In the future, it can be used in E-mails, e-transactions, and e-commerce respectively.

8 Declaration

The authors have no conflicts of interest/Competing interests. We have not received any funding for this article. Availability of data and material is supported on request only. We have not used any special code required for the study of article.

References

1. Yuliang Zheng. Digital signcryption or how to achieve cost (signature & encryption) $\ll$ cost (signature)+ cost (encryption). In *Annual international cryptology conference*, pages 165–179. Springer, 1997.
2. Ron Steinfeld and Yuliang Zheng. A signcryption scheme based on integer factorization. In *International Workshop on Information Security*, pages 308–322. Springer, 2003.
3. John Malone-Lee and Wenbo Mao. Two birds one stone: signcryption using rsa. In *Cryptographers Track at the RSA Conference*, pages 211–226. Springer, 2003.
4. Adi Shamir. Identity-based cryptosystems and signature schemes. In *Workshop on the theory and application of cryptographic techniques*, pages 47–53. Springer, 1984.
5. Dan Boneh and Matt Franklin. Identity-based encryption from the weil pairing. In *Annual international cryptology conference*, pages 213–229. Springer, 2001.
6. Jae Choon Cha and Jung Hee Cheon. An identity-based signature from gap diffie-hellman groups. Cryptology ePrint Archive, Report 2002/018, 2002. https://eprint.iacr.org/2002/018.
7. Florian Hess. Efficient identity based signature schemes based on pairings. In *Selected Areas in Cryptography*, pages 310–324. Springer Berlin Heidelberg, 2003.
8. Kenneth G. Paterson. Id-based signatures from pairings on elliptic curves. Cryptology ePrint Archive, Report 2002/004, 2002. https://eprint.iacr.org/2002/004.
9. N.P. Smart. Identity-based authenticated key agreement protocol based on weil pairing. *Electronics Letters*, 38(13):630, 2002.
10. John Malone-Lee. Identity-based signcryption. *IACR Cryptology ePrint Archive*, 2002:98, 2002.
11. Benoit Libert and Jean-Jacques Quisquater. A new identity based signcryption scheme from pairings. In *Information Theory Workshop, 2003. Proceedings. 2003 IEEE*, pages 155–158. IEEE, 2003.
12. Paulo S. L. M. Barreto, Benoît Libert, Noel McCullagh, and Jean-Jacques Quisquater. Efficient and provably-secure identity-based signatures and signcryption from bilinear maps. In *Lecture Notes in Computer Science*, pages 515–532. Springer Berlin Heidelberg, 2005.
13. Xavier Boyen. Multipurpose identity-based signcryption. In *Advances in Cryptology - CRYPTO 2003*, pages 383–399. Springer Berlin Heidelberg, 2003.
14. Liqun Chen and John Malone-Lee. Improved identity-based signcryption. In *International Workshop on Public Key Cryptography*, pages 362–379. Springer, 2005.
15. Benoît Libert and Jean-Jacques Quisquater. Efficient signcryption with key privacy from gap diffie-hellman groups. In *Public Key Cryptography – PKC 2004*, pages 187–200. Springer Berlin Heidelberg, 2004.

16. S S M Chow, S M Yiu, L C K Hui, and K P Chow. Efficient forward and provably secure id-based signcryption scheme with public verifiability and public ciphertext authenticity. In *Information Security and Cryptology- ICISC 2003*, pages 352–369. Springer-Verlag, 2004.
17. Mihir Bellare and Phillip Rogaway. Random oracles are practical: A paradigm for designing efficient protocols. In *Proceedings of the 1st ACM conference on Computer and communications security*, pages 62–73, 1993.
18. Yong Yu, Bo Yang, Ying Sun, and Sheng-lin Zhu. Identity based signcryption scheme without random oracles. *Computer Standards & Interfaces*, 31(1):56–62, 2009.
19. Ran Canetti, Oded Goldreich, and Shai Halevi. The random oracle methodology, revisited. *Journal of the ACM (JACM)*, 51(4):557–594, 2004.
20. Mihir Bellare, Alexandra Boldyreva, and Adriana Palacio. An uninstantiable random-oracle-model scheme for a hybrid-encryption problem. In *Advances in Cryptology - EUROCRYPT 2004*, pages 171–188. Springer Berlin Heidelberg, 2004.
21. Kenneth G. Paterson and Jacob C. N. Schuldt. Efficient identity-based signatures secure in the standard model. In *Information Security and Privacy*, pages 207–222. Springer Berlin Heidelberg, 2006.
22. Brent Waters. Efficient identity-based encryption without random oracles. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pages 114–127. Springer, 2005.
23. Xing Wang and Hai feng Qian. Attacks against two identity-based signcryption schemes. In *2010 Second International Conference on Networks Security, Wireless Communications and Trusted Computing*. IEEE, 2010.
24. Mingwu Zhang, Pengcheng Li, Bo Yang, Hao Wang, and Tsuyoshi Takagi. Towards confidentiality of id-based signcryption schemes under without random oracle model. In *Pacific-Asia Workshop on Intelligence and Security Informatics*, pages 98–104. Springer, 2010.
25. Bo Zhang. Cryptanalysis of an identity based signcryption scheme without random oracles. *Journal of Computational Information Systems*, 6(6):1923–1931, 2010.
26. Ren Yanli and Gu Dawu. Efficient identity based signature/signcryption scheme in the standard model. In *Data, Privacy, and E-Commerce, 2007. ISDPE 2007. The First International Symposium on*, pages 133–137. IEEE, 2007.
27. Craig Gentry. Practical identity-based encryption without random oracles. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pages 445–464. Springer, 2006.
28. Xu An Wang, Weidong Zhong, and Haining Luo. Cryptanalysis of efficient identity based signature/signcryption schemes in the standard model. In *Intelligence Information Processing and Trusted Computing (IPTC), 2010 International Symposium on*, pages 622–625. IEEE, 2010.
29. Zhengping Jin, Qiaoyan Wen, and Hongzhen Du. An improved semantically-secure identity-based signcryption scheme in the standard model. *Computers & Electrical Engineering*, 36(3):545–552, 2010.
30. Fagen Li, Yongjian Liao, and Zhiguang Qin. Analysis of an identity-based signcryption scheme in the standard model. *IEICE transactions on fundamentals of electronics, communications and computer sciences*, 94(1):268–269, 2011.
31. Fagen Li, Fahad Bin Muhaya, Mingwu Zhang, and Tsuyoshi Takagi. Efficient identity-based signcryption in the standard model. In *Provable Security*, pages 120–137. Springer Berlin Heidelberg, 2011.
32. Yang Ming and Yumin Wang. Cryptanalysis of an identity based signcryption scheme in the standard model. *IJ Network Security*, 18(1):165–171, 2016.
33. Fagen Li and Tsuyoshi Takagi. Secure identity-based signcryption in the standard model. *Mathematical and Computer Modelling*, 57(11-12):2685–2694, 2013.
34. Dharminder Dharminder, Dheerendra Mishra, Joel JPC Rodrigues, Ricardo de AL Rabelo, and Kashif Saleem. Psscc: Provably secure communication framework for crowdsourced industrial internet of things environments. *Software: Practice and Experience*, 2020.
35. S Sharmila Deva Selvi, S Sree Vivek, Dhinakaran Vinayagamurthy, and C Pandu Rangan. Id based signcryption scheme in standard model. In *International Conference on Provable Security*, pages 35–52. Springer, 2012.
36. Guiyi Wei, Jun Shao, Yang Xiang, Pingping Zhu, and Rongxing Lu. Obtain confidentiality or/and authenticity in big data by id-based generalized signcryption. *Information Sciences*, 318:111–122, 2015.
37. Arijit Karati, SK Hafizul Islam, GP Biswas, Md Zakirul Alam Bhuiyan, Pandi Vijayakumar, and Marimuthu Karuppiah. Provably secure identity-based signcryption scheme for crowdsourced industrial internet of things environments. *IEEE Internet of Things Journal*, 5(4):2904–2914, 2018.

Figures

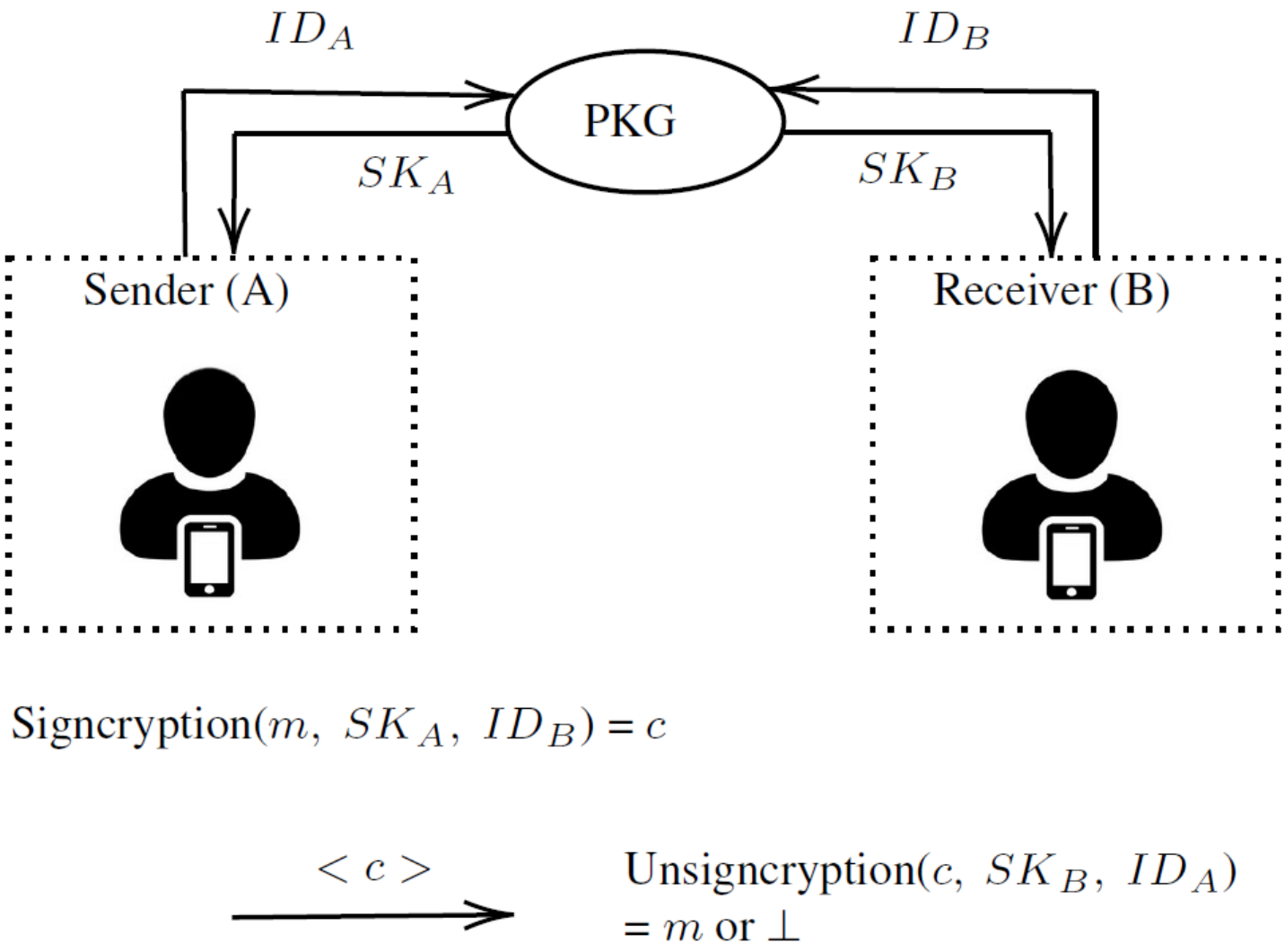

Figure 1

Illustration of ID-based signcryption communication

Sender (A)	Pulic channel	Receiver (B)
		
A takes $m \in \{0,\ 1\}^*$ $r \in Z_q^*$ Computes $c_1 = g^r$ $c_2 = ((\varrho_1 w_2).(\varrho_2 w_1)^{ID_B})^r.$ $\kappa = H(\Phi(g,\ g)^{\frac{r}{k^2}})$ $c_3 = E_\kappa(m)$ $\vartheta = H(m\|\|ID_A\|\|ID_B\|\|\kappa)$	$\xrightarrow{< c_1,\ c_2,\ c_3,\ \vartheta >}$	Computes $c_2' = w_2 w_1^{ID_A}$ $\kappa = H(\Phi(c_2,\ c_2')\Phi(c_1,\ \varrho_3 \varrho^{ID_A})^{-1})$ $D_\kappa(c_3) = m$ Verifies $\vartheta =? H(m\|\|ID_A\|\|ID_B\|\|\kappa)$

Figure 2

Registration phase executed via secure channel

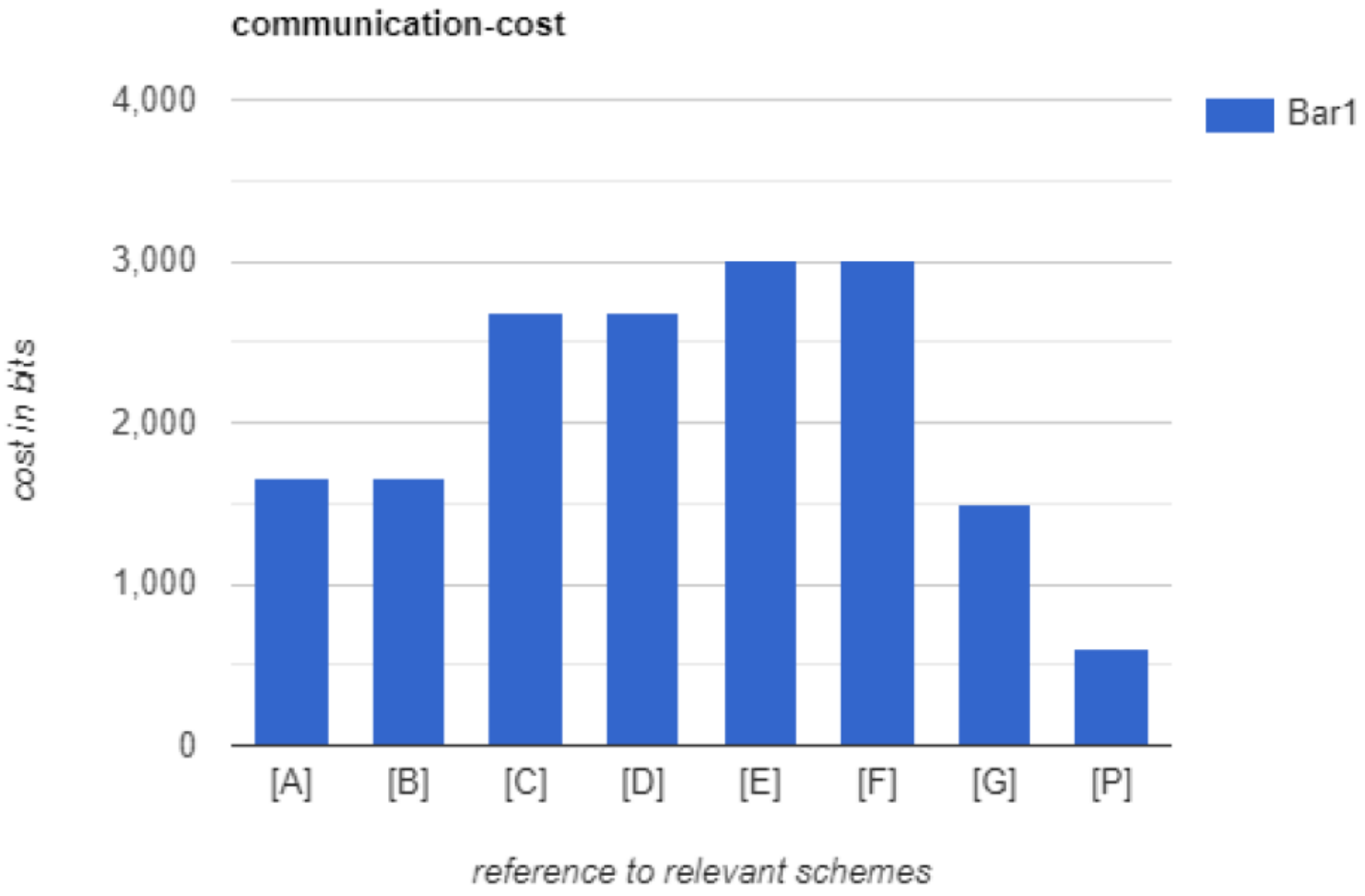

Figure 3

Communication in terms of bits with existing relevant schemes

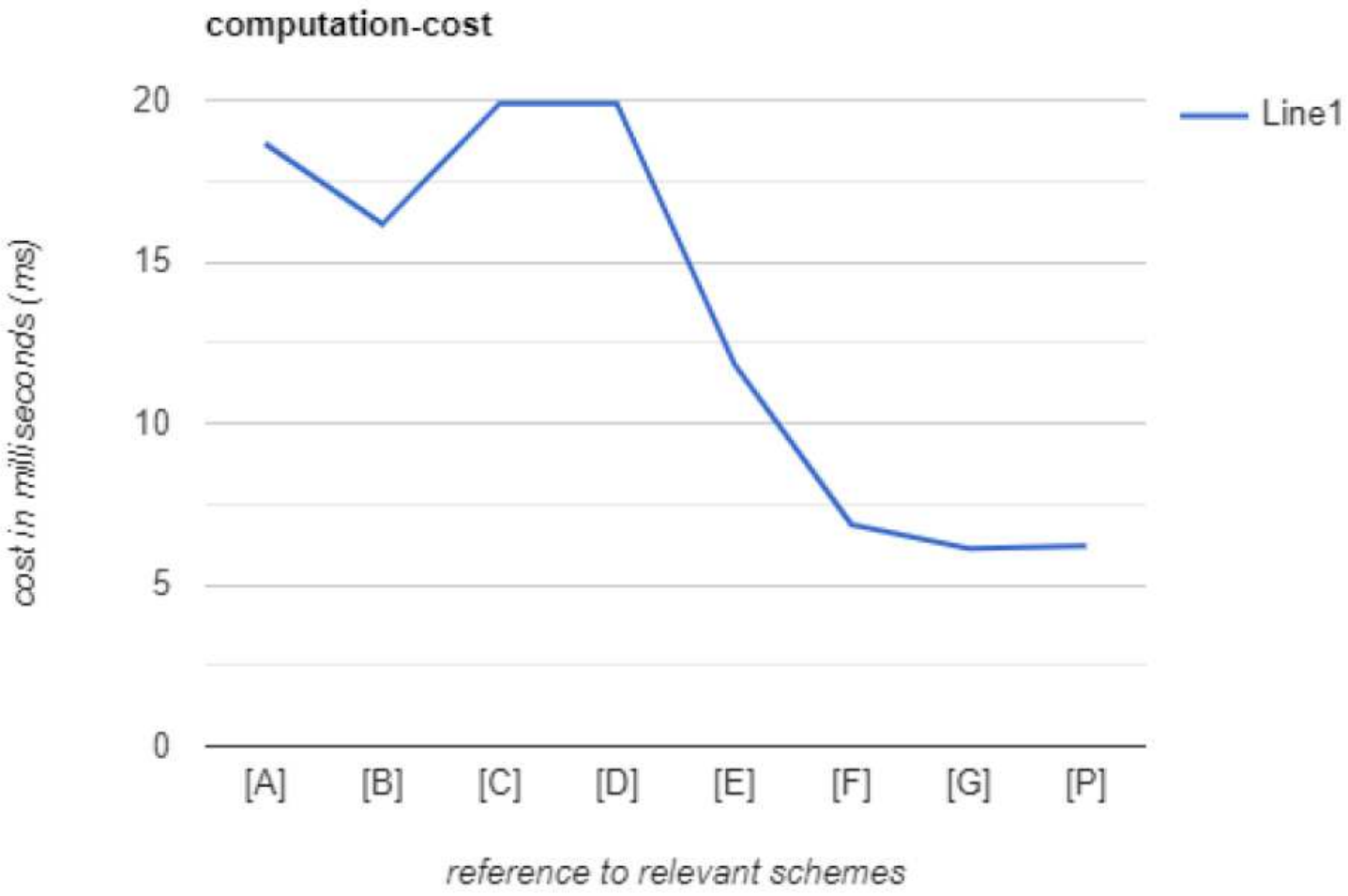

Figure 4

Computation analysis with existing relevant schemes

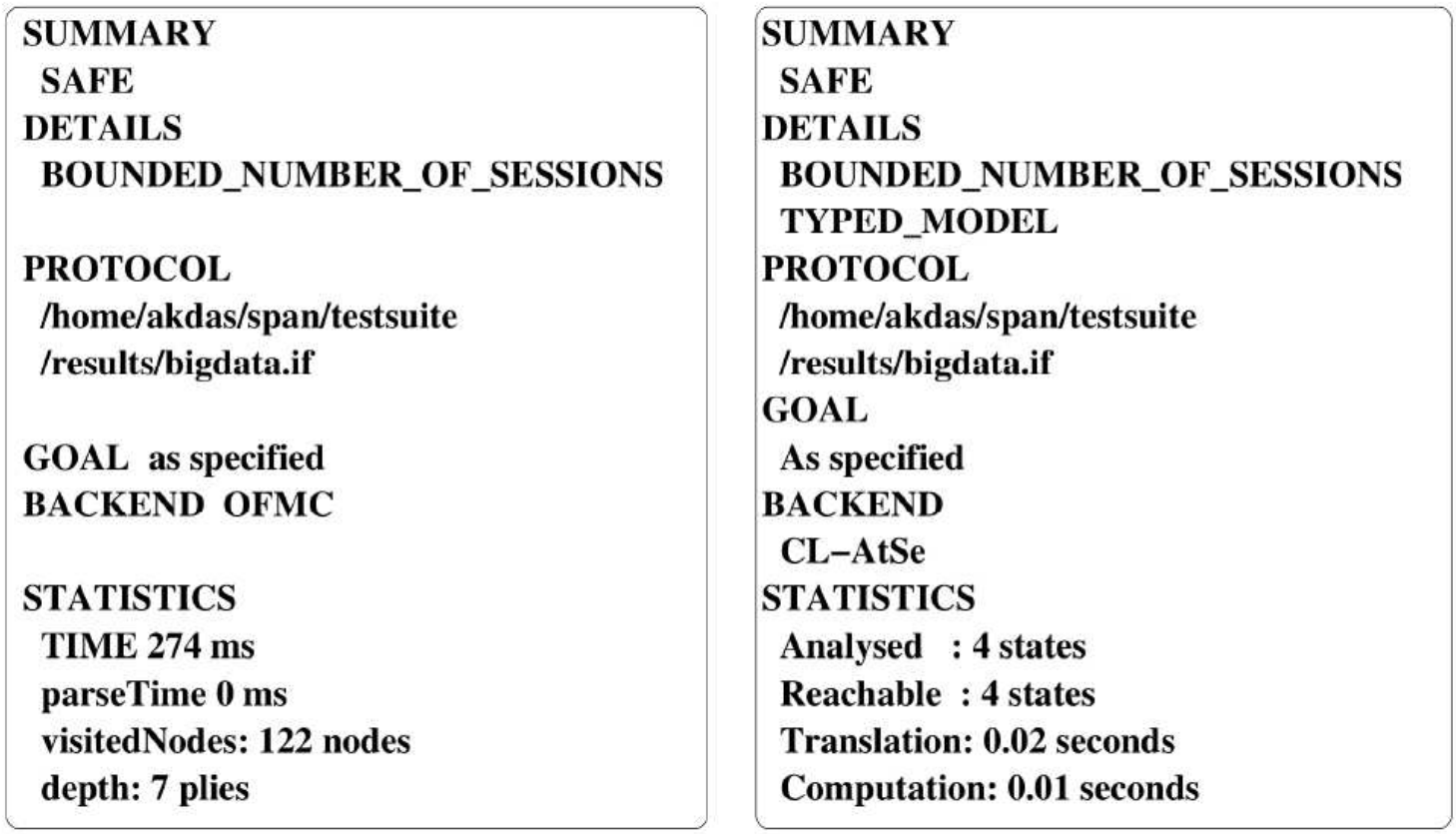

Figure 5

Analysis under CL-AtSe and OFMC backends