INFORMATICA, 2017, Vol. 28, No. 3, 471–484
© 2017 *Vilnius University*
DOI: http://dx.doi.org/10.15388/Informatica.2017.139

An IND-ID-CPA Secure ID-Based Cryptographic Protocol using GDLP and IFP

Chandrashekhar MESHRAM[1,2], Yuh-Min TSENG[3], Cheng-Chi LEE[4,5]*, Sarita Gajbhiye MESHRAM[6]

[1]*Department of Mathematics and Computer Science, R D University, Jabalpur (M.P.), India*
[2]*Department of Mathematics, RTM Nagpur University, Nagpur, India*
[3]*Department of Mathematics, National Changhua University of Education*
Chang-Hua 500, Taiwan, R.O.C.
[4]*Department of Library and Information Science, Fu Jen Catholic University*
New Taipei 24205, Taiwan, R.O.C.
[5]*Department of Photonics and Communication Engineering, Asia University*
Wufeng Shiang, Taichung 413, Taiwan, R.O.C.
[6]*Department of Water Resources Development & Management, Indian Institute of Technology Roorkee (Uttrakhand), India*
e-mail: cs_meshram@rediffmail.com, ymtseng@cc.ncue.edu.tw, cclee@mail.fju.edu.tw, gajbhiyesarita@gmail.com

Received: September 2016; accepted: January 2017

Abstract. ID-based cryptographic protocol is an extremely valuable apparatus in the field of cryptography and has numerous latent applications. The safety of conventional ID-based cryptographic protocol is entirely contingent in light of the safety of private keys. Revelation of private keys needs reissuing all beforehand doled out encryptions. This confinement turns out to be clearer today as key presentation is more regular with expanding utilization of unprotected gadgets and mobile technology. In this context, relieving the loss of key disclosure in ID-based cryptographic protocol is a critical issue. To manage this issue, we present to include onward security into ID-based cryptographic protocol. Besides, we propose another development of indistinguishability-ID-based cryptographic protocol using Integer Factorization Problem (IFP) and Generalized Discrete Logarithm Problem (GDLP) which is semantically protected against Chosen Plaintext Attack (CPA) in random oracle. We show that our presented protocol beats the other standing protocol as far as security, the length of public key and computational cost are concerned. We shed light on some applications and future scope.

Key words: cryptography, ID-based cryptographic, IFP, GDLP, random oracle.

1. Introduction

An ID-based cryptography gives a helpful approach to do public key cryptography deprived of the problem of issuing public keys. The sender's message can encrypt utilizing the identity of the recipient as the public key in an ID-based cryptographic protocol. In

*Corresponding author.

this way, there is no requirement for the recipient to demonstrate his/her public key certificate to the correspondent. Cryptosystem is especially valuable in applications anywhere message recipients are not generally accessible to contemporary public key certificates.

Shamir (1984) developed the model of an ID-based cryptographic protocol to streamline the key administration issue in 1984. It is very clear that identity of a user, for example, government managed savings number, e-mail address etc. are utilized as people in public key, while the secret key connected through that identity is registered and allotted subtly to the user by Private Key Generator (PKG), which is a trusted third party in an ID-based cryptographic protocol. In such type of settings, the main thing that ought to be certificated is general public parameters of the PKG. Hence, an identity-based cryptographic protocol definitely decreases the need for certificates. It was not until 2001 that Cocks (2001) and Boneh and Franklin (2001) presented two identity-based encryption protocol. Boneh and Franklin (2003) utilized a grouping of bilinear maps as starting point of their development (Boneh and Boyen, 2004a, 2004b; Waters, 2005).

Despite the fact that there have been numeral well-organized ID-based cryptographic protocols, these protocols are still considerably slower than general public key cryptosystems. For instance, Boneh-Franklin protocol is slower than ElGamal protocol 400 times in terms of encryption process (Galindo, 2004). In exercise, quick encryption and decryption operations are required in many applications. Thus, the time execution costs of present ID-based cryptographic protocols cannot address the issue of practice. Many ID-based cryptographic protocols (Boneh and Franklin, 2003; Boneh *et al.*, 2003; Gangishetti *et al.*, 2007; Kiltz and Vahlis, 2008; Lee and Liao, 2004; Meshram *et al.*, 2012; Meshram and Meshram, 2013; Sun *et al.*, 2010) have been proposed in the reported literature after 2003. However, in these ID-based cryptographic protocols, the public key of every user is an identity as well as some arbitrary number chosen either by the user or by the trusted parties. This marks the ID-based cryptography area an attractive exploration field in the current century.

Boneh and Franklin presented primary provably secure ID-based cryptographic protocol in Boneh and Franklin (2001, 2003). The recent methodology they utilized depends on a category of bilinear maps. Subsequent to their work, lots of ID-based cryptographic protocols based on bilinear maps were presented. For instance, Boneh and Boyen (2004a) introduced a safe ID-based cryptographic protocol lacking random oracles; Waters (2005) designed a well-organized ID-based cryptographic protocol lacking random oracles; in Boneh and Boyen (2004b) Boneh and Boyen developed additional ID-based cryptographic protocol lacking random oracles, which is safe in the specific model. However, as pointed out in Galindo (2004), even the well-organized protocols such as Boneh and Franklin (2001, 2003) are considerably slower than ElGamal cryptosystem. In this way, the present ID-based cryptographic protocol is just about as quick as the ElGamal cryptographic protocol in both decryption and encryption stages. Heng and Kurosawa utilized a polynomial using way to deal with building up an ID-based cryptographic protocol that does not require random oracles in Han *et al.* (2004, 2006). Their protocol is semantically secure under the IFP and GDLP supposition. But their protocol is considerably dawdling compared to ElGamal, too.

As shown in the above, unfortunately we initiated that standing ID-based cryptographic protocol using IFP and discrete logarithm problem (DLP), respectively, can't be viewed as secure. Along these lines, our principle commitment in this paper is to plug this crevice by presenting effective provably secure ID-construct cryptographic protocol using IFP and GDLP. The time execution costs of decryption and encryption stages in presented ID-based cryptographic protocol are those of ElGamal. All further unequivocally, with the exception of the principal of encryption process for separate identity, all decryption and encryption processes have the same time expense as the resultant processes of ElGamal. We likewise give a proper safety evidence to semantically protect against chosen plaintext attack (CPA) under the IFP and GDLP hypothesis in the random oracle utilizing the reversing procedure presented by Boneh and Franklin (2001).

The rest of this paper is composed as follows: The required mathematical background is presented in Section 2. Our proposed IND-ID-CPA secure ID-based cryptographic protocol is displayed in Section 3. The security examination and security evidence of the protocol are exhibited in Section 4. The performance comparison with other protocols is talked about in Section 5. Some applications and future scope are talked about in Section 6. At last, Section 7 finishes up the paper.

2. Mathematical Background

In this area, we portray some foundation knowledge utilized as a part of this paper, containing IFP and DLP (Meshram *et al.*, 2012).

2.1. *Related Definitions*

Definition 1 (IFP). For a given positive an integer N find its prime factorization; to be precise, as $N = p_1^{e_1}.p_2^{e_2}.p_3^{e_3}.p_4^{e_4}\ldots\ldots\ldots p_t^{e_t}$ where the p_i are pairwise discrete primes and each $e_i \geqslant 1$.

Definition 2 (GDLP over Z_N^*). Let an integer $N = p * q$ and e be a primitive root for both Z_p^* and Z_q^*, where q and p are arbitrary safe primes. Given $y = e^x\ (mod\ N)$, it is computationally intractable to derive x.

2.2. *Complexity Statement*

The security of presented protocol depends on a regular complexity-hypothetical supposition, viz. GDLP and IFP supposition. We survey it as follows.

2.2.1. *GDLP and IFP Supposition*

Let e be a generator of a multiple group Z_N^*. The challenger randomly chooses $u, v, z \in Z_p^*$ and a bit $\xi \in \{0, 1\}$, consistently and autonomously. If $\xi = 1$ he/she yields the tuple $(e, e^u(mod\ N), e^v(mod\ N), e^{uv}(mod\ N))$, else, he/she yields the tuple $(e, e^u(mod\ N),$

$e^v(mod\ N), e^z(mod\ N))$, where $N = p * q$. Then the adversary yields a guess ξ' of ξ. An adversary has an ϵ advantage if

$$\left|\Pr[\xi = \xi'] - \frac{1}{2}\right| = \epsilon.$$

Definition 3. The decisional ϵ-GDLP and IFP hypothesis holds in G if not any PPT foe has no less than ϵ advantage in resolving the game, which is mentioned in Meshram (2015).

3. The Proposed Scheme

We present an ID-based cryptographic protocol using IFP and GDLP. It consists of four sub-algorithms. These four sub-algorithms are developed as the following:

3.1. *Setup*

This algorithm will be done by PKG by taking in security parameter as follows:

1. Select an integer $N = p * q$, where q and p are safe prime numbers and compute Euler-phi function $\varphi(N) = (p - 1)(q - 1)$;
2. Choose arbitrary integer e and unique integer d, such that $1 \leqslant e, d \leqslant \varphi(N)$, $gcd(e, \varphi(N)) = 1$, and $ed \equiv 1\ (mod\ \varphi(N))$ (Rivest *et al.*, 1978);
3. Generate k dimensional secret vectors $A = (a_1, a_2, a_3, \dots, a_k)$, where a_i is arbitrary selected from $Z^*_{\varphi(N)}$;
4. Generate the corresponding k dimensional public vectors $B = (b_1, b_2, b_3, \dots, b_k)$, where $b_i = e^{a_i}\ (mod\ N)$ and $i \in (1, k)$;
5. Construct cryptographic hash function $H : \{0,\ 1\}^* \to \{0,\ 1\}^k$.

The master key and public parameter of PKG are given by $mk = \{p, q, d, A\}$ and $pm = \{N, e, B, H\}$. For the notational accommodation, we mean the bit length n by $|N| = n$.

The algorithm for a particular $ID \in \{0, 1\}^*$ implements the following:

1. Compute $H(ID) \to (h_1, h_2, h_3, h_4, \dots, h_k)$ and suppose that h_i is the ith bit of $H(ID)$, where $i \in (1, k)$;
2. Calculate the secret key as follows:

$$a_{ID} = \sum_{i=1}^{k} h_i a_i\ (mod\ N);$$

3. Calculate the resultant public key as follows:

$$b_{ID} = \prod_{i=1}^{k} (b_i)^{h_i}\ (mod\ N) = \prod_{i=1}^{k} (e_i)^{h_i a_i}\ (mod\ N) = e^{a_{ID}}\ (mod\ N).$$

3.2. *Encryption*

A message $M \in \{0,1\}^*$ is encrypted for *ID* as follows:

1. Compute $C_1 = M^{b_{ID}}\ (mod\ N\ ) = M^{e^{a_{ID}}}\ (mod\ N\ )$;
2. Compute the ciphertext $C = C_1^e\ (mod\ N\ )$.

3.3. *Decryption*

To decrypt the ciphertext C under identity *ID* of entity:

1. Compute $\delta = C^d (mod\ N)$;
2. A user can decrypt C utilizing his/her secret key a_{ID} as $\delta^{d^{a_{ID}}} = M\ (mod\ N)$.

3.4. *Correctness*

$$\begin{aligned}\delta^{d^{a_{ID}}} &= {C_1}^{d^{a_{ID}}}(mod\ N) = \left(M^{e^{a_{ID}}}\right)^{d^{a_{ID}}}(mod\ N) = M^{(ed)^{a_{ID}}}(mod\ N)\\ &= M\ (mod\ N).\end{aligned}$$

4. Security Analysis

In this area, we demonstrate the security of ID-based cryptographic protocol using the complexity of GDLP and IFP. We demonstrate that ID-based cryptographic protocol is semantically protected against CPA in the random oracle, which has been developed by Boneh and Franklin (2001).

Definition 4. An ID-based cryptographic protocol is $(t, \epsilon(t))$-semantically protected against an adaptive CPA, if all Probabilistic Polynomial Time (PPT) foes creating at the most t secret key inquiries have at the most an $\epsilon(t)$ advantage in breaking the scheme.

Theorem 1. *Suppose that H the cryptographic hash function, be a random oracle, then an ID-based cryptographic protocol using GDLP and IFP is* $(t, \epsilon(t))$*-semantically protected under the decisional* $\epsilon(t)(1 - \frac{1}{\alpha} - \frac{1}{2^{t-k}})/2$*-GDLP and IFP assumption in the random oracle.*

Proof. Let $\mathfrak{F}$ be an IND-ID-CPA foe that has advantage $\epsilon(t)$ against ID-based cryptographic scheme using GDLP and IFP. It means the foe $\mathfrak{F}$ makes at most t queries and gets at least $\epsilon(t)$ advantage in the IND-ID-CPA game.

We created a simulator $\mathcal{S}$ as PPT to perform the IFP and GDLP game, which is cited in Meshram (2015). Simulator $\mathcal{S}$ proceeds the task $(e, A = e^u(mod\ N), B = e^v(mod\ N), Z)$ as response and guess an output ξ' of ξ, where $\xi', \xi \in \{0,1\}$. To locate a decent guess ξ', simulator $\mathcal{S}$ performs an IND-ID-CPA game with the foe $\mathfrak{F}$ in the accompanying steps:

Setup: The simulator $\mathcal{S}$ arbitrarily chooses uniformly and independently, tm-dimensional binary vector $V_i = (h_{1i}, h_{2i}, h_{3i}, \dots, h_{mi})^T$, where $1 \leqslant i \leqslant t$. Simulator $\mathcal{S}$ also selects $x_1, x_2, x_3, \dots, x_m \in Z^*_{\varphi(N)}$ consistently and individually at random. Then simulator $\mathcal{S}$ chooses $y_1, y_2, y_3, \dots, y_m \in Z^*_{\varphi(N)}$ that fulfills the accompanying system:

$$\begin{aligned}&\begin{bmatrix} y_1, y_2, y_3, \dots, y_m \end{bmatrix} \begin{bmatrix} h_{11} & h_{12} & h_{13} & \dots & h_{1t} \\ h_{21} & h_{22} & h_{23} & \dots & h_{2t} \\ \vdots & \vdots & \vdots & \dots & \vdots \\ h_{m1} & h_{m2} & h_{m3} & \dots & h_{mt} \end{bmatrix} (\text{mod N}) \\ &\quad = [0, \dots 0] \ (\text{mod } N) = 0. \end{aligned} \tag{1}$$

It may be noted that there exist many tuples $y_1, y_2, y_3, \dots, y_k \in Z^*_N$ that satisfy the Eq. (1). Simulator $\mathcal{S}$ arbitrarily selects any one of them.

The simulator $\mathcal{S}$ arranges the public parameter B as follows:

$$B = \left(A^{y_1} e^{x_1},\ A^{y_2} e^{x_2},\ A^{y_3} e^{x_3}, \dots, A^{y_m} e^{x_m}\right)(mod\ N).$$

Obviously, the analogous master secret key is given by

$$A = (a_1, a_2, a_3, a_4, \dots, a_k) = (uy_1 + x_1, uy_2 + x_2, uy_3 + x_3, \dots, uy_k + x_k).$$

Note that u is independent of B. Simulator $\mathcal{S}$ provides the public parameters (N, e, k, B) to the foe $\mathfrak{F}$.

Random oracle queries: In the following stages, the foe $\mathfrak{F}$ requires to mark inquiries to the random oracle H, when he/she requires to acquire hash values. Note the contrast among these random oracle inquiries and the inquiries in the IND-ID-CPA game. The simulator $\mathcal{S}$ replies random oracle inquiries in the rest of the stages as explained as follows.

H-queries: Let q_H be a polynomial upper bound of the quantity of random oracle inquiries. That is, foe $\mathfrak{F}$ creates at most q_H inquiries to the random oracle H. Simulator $\mathcal{S}$ arbitrarily selects $\delta \subseteq (1, 2, \dots, q_H)$ such that $|\delta| = t$. To reply the random oracle inquiries, the simulator $\mathcal{S}$ keeps up a list of tuples $\langle ID_i, H(ID_i), \gamma_i \rangle$, where $\gamma_i \in \{0, 1\}$ is allotted when simulator $\mathcal{S}$ reacts to the query and ID_i is an identity that has showed up in the before random oracle inquiries. Let $\mathcal{L}_H$ signify this list of tuples; toward the starting, $\mathcal{L}_H$ is vacant. Once there is a random oracle inquiry ID_i, $\mathcal{S}$ reacts as follows.

1. Simulator $\mathcal{S}$ answers with the noted hash value $H(ID_i)$, if ID_i is already in the list $\mathcal{L}_H$;
2. Simulator $\mathcal{S}$ registers the tuple $\langle ID_i,\ H(ID_i),\ \gamma_i \rangle \in \mathcal{L}_H$, in both cases: (a) In the event that ID_i is the ith new inquiry to the random oracle and $i' \in \delta$, suppose that i' is the ith smallest component in δ, then $\mathcal{S}$ arrangements $H(ID_i) = (h_{1i"}, h_{2i"}, h_{3i"}, \dots, h_{ki"})$ and $\gamma_i = 1$, something else, (b) $\mathcal{S}$ arbitrarily selects a binary string $h_{1j}, h_{2j}, h_{3j}, \dots, h_{kj} \in \{0, 1\}^k$ that is not in $\mathcal{L}_H$, sets $H(ID_i) = h_{1j}, h_{2j}, h_{3j}, \dots, h_{kj}$ and $\gamma_i = 0$, and answers with $H(ID_i)$.

Given the above technique for noting random oracle inquiries, we can now portray in what manner the simulator $\mathcal{S}$ functions in the rest of the stages of the IND-ID-CPA game.

Stage 1: For each secrete key extraction query ID_i allotted through the foe $\mathfrak{F}$, simulator $\mathcal{S}$ replies as follows:

1. Simulator $\mathcal{S}$ takes up the IND-ID-CPA game, if ID_i appears in $\mathcal{L}_H$ and $\gamma_i \neq 1$, or ID_i does not show up in $\mathcal{L}_H$ and all the V_j produced in the *Setup stage* have been utilized in responding the earlier inquiries. Specifically, $\mathcal{S}$ requires to re-pick $\delta \subseteq (1, 2, \ldots, q_H)$ in the saved game. Note that simulator $\mathcal{S}$ can start over the IND-ID-CPA game at the most $(\binom{q_H}{t} - 1)$ times. In the event that the time of resuming the IND-ID-CPA game surpasses this numeral, then $\mathcal{S}$ aborts, yielding a consistently arbitrary bit as ξ';
2. Simulator $\mathcal{S}$ computes $a_{ID_i} = \sum_{s=1}^{k} h'_{si}\ x_s\ (mod\ N)$, if ID_i appears in $\mathcal{L}_H$ and $\gamma_i = 1$, and replies with a_{ID_i}, where h'_{si} is the sth bit of noted value $H(ID_i)$;
3. If ID_i does not show up in $\mathcal{L}_H$ and there exists V_j created in the *Setup* stage that was never utilized as a part of reacting to the past inquiries, simulator $\mathcal{S}$ selects such a never utilized V_j, arrangements $H(ID_i) = h_{1j}, h_{2j}, h_{3j}, \ldots, h_{kj}$ and $\gamma_i = 1$, answers the query using $a_{ID_i} = \sum_{s=1}^{k} h_{si}\ x_s\ (mod\ N)$, and archives the tuple $\langle ID_i,\ H(ID_i),\ \gamma_i\rangle \in \mathcal{L}_H$.

Note that

$$\begin{aligned} a_{ID_i} &= \sum_{s=1}^{k} h_{si}\ a_s\ (mod\ N) \\ &= \sum_{s=1}^{k} h_{si}\ (uy_s + x_s)\ (mod\ N) \\ &= u\sum_{s=1}^{k} h_{si}\ y_s\ (mod\ N) + \sum_{s=1}^{k} h_{si}\ x_s\ (mod\ N) \\ &= \sum_{s=1}^{k} h_{si}\ x_s\ (mod\ N) \end{aligned}$$

where the last equity is because of Eq. (1). So the above task of a_{ID_i} is valid.

Challenge: Formerly the foe $\mathfrak{F}$ decides that Stage 1 is finished, then he/she submits two plaintexts M_0 and M_1 from {0, 1}* and an identity $ID_0 \neq ID_i$ shows up in the secret key extraction inquiries. Simulator $\mathcal{S}$ arbitrary selects a binary string $h_{10}, h_{20}, h_{30}, \ldots, h_{k0} \in$ {0, 1}^{k}. If the binary vector $V_0 = (h_{10}, h_{20}, h_{30}, \ldots, h_{k0})^T$ is a linear combination of V_i, $(1 \leqslant i \leqslant t)$, then simulator $\mathcal{S}$ aborts, yielding a consistently random bit as ξ' generally, simulator $\mathcal{S}$ calculates $y = \sum_{i=1}^{k} h_{i0}\ y_i\ (mod\ N)$, $x = \sum_{i=1}^{k} h_{i0}\ x_i\ (mod\ N)$, and $z_{ID_0} = A^y e^x\ (mod\ N) = e^{uy+x}\ (mod\ N)$. Simulator $\mathcal{S}$

archives the tuple $\langle ID_0, h_{10}, h_{20}, h_{30}, \dots, h_{k0}, 0\rangle \in \mathcal{L}_H$. Next, simulator $\mathcal{S}$ selects β consistently at arbitrary from $\{0, 1\}$ and utilizes the ciphertext

$$C = \left(M_{\beta}^{e^{uy+x}}\right)(mod\ N)$$

as the challenge to the foe $\mathfrak{F}$.

Stage 2: The foe $\mathfrak{F}$ issues secret key extraction queries $ID_0 \neq ID_{s+1}, \dots, ID_t$, and simulator replies in the similar methodology such as in Stage 1.

Guess: Finally foe $\mathfrak{F}$ outputs a guess ξ' of ξ. Simulator $\mathcal{S}$ outputs a guess ξ' of ξ using the output β' of the foe $\mathfrak{F}$ such as follows: if $\beta' = \beta$, then $\xi' = 1$; else, $\xi' = 0$.

To lower bound the upside of simulator $\mathcal{S}$ which is mentioned above, we first examine a few occasions and dissect their probabilities. Assume that abort is the event that simulator $\mathcal{S}$ aborts in the IND-ID-CPA game. We watch that there are two conceivable reasons that simulator $\mathcal{S}$ aborts: (1) In Stage 1 or Stage 2, a secret key extraction inquiry prompts take up of the IND-ID-CPA game, yet the quantity of restarting the IND-ID-CPA game surpasses $(\binom{q_H}{t} - 1)$, (2) In the Challenge stage, the binary vector $V_0 = (h_{10}, h_{20}, h_{30}, \dots, h_{k0})^T$ is a linear combination of V_i $(1 \leqslant i \leqslant t)$.

Claim 1. *The probability is at the most $\frac{1}{\alpha}$, if the simulator $\mathcal{S}$ aborts for goal* (1).

Proof. By one decision of δ, the probability that there is a secret key extraction question prompting to pick up of the IND-ID-CPA game is at the most $(1 - \frac{1}{\binom{q_H}{t}})$. Let $\omega = \binom{q_H}{t}$, then, the probability that ω decisions of δ all lead to pick up of the IND-ID-CPA game are at the most $(1 - \frac{1}{\omega})^{\omega} \approx \frac{1}{\alpha}$. It means, the probability is at the most $\frac{1}{\alpha}$ if simulator $\mathcal{S}$ aborts for the first goal. □

Claim 2. *The probability is at the most $\frac{1}{2^{t-k}}$ if the simulator $\mathcal{S}$ aborts for goal* (2).

Proof. We consider the condition that the binary vector $V' = (h'_1, h'_2, \dots, h'_k)^T$ is a linear combination of V_j $(1 \leqslant j \leqslant t)$. Let the matrix $M_{t(k+1)} = (V_1, V_2, V_3, \dots, V_t, V')$, where $(k+1) < t$. By observing that, the matrix is a linear combination of above condition. Assume the rank of matrix $M_{t(k+1)}$ is t', where $t' \leqslant k$. That is, there exist t' rows of the matrix $M_{t(k+1)}$ that are linearly independent. Without loss of all-inclusive statement, expect that the main t' rows of $M_{k(t+1)}$ are linearly independent. Let $M_{t't'}$ indicate the t'-dimensional vector comprising of the linearly independent elements of V_j $(1 \leqslant j \leqslant t)$. So we observe that $|M_{t't'}| \leqslant 2^{t'} \leqslant 2^k$. But there are totally $2^t t$-dimensional binary vectors, the probability that the simulator $\mathcal{S}$ aborts for V' is linear combination of V_j $(1 \leqslant j \leqslant t)$ is $\frac{1}{2^{t-k}}$ $(k < t)$.

Combining Claims 1 and 2, we have the probability that simulator $\mathcal{S}$ aborts at the most $(\frac{1}{\alpha} + \frac{1}{2^{t-k}})$. Therefore, the probability that simulator $\mathcal{S}$ does not abort is at least $(1 - \frac{1}{\alpha} - \frac{1}{2^{t-k}})$. The provisional probability that $\xi = \xi'$ on condition that simulator $\mathcal{S}$ does not abort is $|\Pr[\xi = \xi' \mid \overline{abort}] - \frac{1}{2}| \geqslant \epsilon(t)$. To prove Theorem 4.1, we obtain the advantage of the simulator $\mathcal{S}$ by above claim $Pr[\xi = \xi'] = Pr[\xi = \xi' \mid \overline{abort}]\Pr[\overline{abort}] \geqslant \frac{\epsilon(t)}{2}(1 - \frac{1}{\alpha} - \frac{1}{2^{t-k}})$. This finishes the proof of Theorem 4.1. □

5. Execution Comparison with Other Protocols

In this area, we have discussed eight record widely-used ID-based cryptographic protocols and analysed their execution. These eight ID-based cryptographic protocols are: Boneh and Franklin's protocol (Boneh and Franklin, 2001), Cocks's protocol (Cocks, 2001), Lynn's protocol (Lynn, 2002), Boneh and Boyen's protocol (Boneh and Boyen, 2004b), Gentry and Silverberg's protocol (Gentry and Silverberg, 2002), Water's protocol (Waters, 2005), Meshram et al.'s protocol (Meshram *et al.*, 2012), Meshram's protocol (Meshram, 2015), and our proposed protocol based on IFP and GDLP. These ID-based cryptographic protocols have diverse execution on server for assessing encryption process execution, decryption process execution, and computational cost.

Notations utilized as a part of this calculation are as follows:

T_P – the time of acting a pairing operation.

T_M – the time of acting a modular multiplication.

T_e – the time of acting a modular exponentiation in group.

T_m – the time of acting a scalar or point multiplication in group.

T_x – the time of acting an XOR operation.

T_H – the time of acting a map to point hash function.

T_h – the time of acting a one way hash function.

T_a – the time of acting a modular addition operation.

T_i – the time of acting a modular inverses operation.

T_j – the time of acting a Jacobi symbol operation.

As we as a whole know, the time of implementing a pairing operation T_P is additional time overriding new operations. Some execution simulation results (Boneh and Franklin, 2001; Cui *et al.*, 2006) demonstrate that T_a and T_h are insignificant in examination with T_e, T_M, T_x, T_H, T_i, and T_j.

It is to be noted that encryption algorithmic phase and decryption algorithmic phase are the dominating process in terms of computation cost compared to setup and extract phases as they are executed only once. Thus, we consider only the encryption and decryption phase and accordingly compare the proposed ID-based cryptographic schemes with Cocks (2001), Boneh and Franklin (2001), Boneh and Boyen (2004b), Waters (2005), Meshram *et al.* (2012), Meshram (2015), Lynn (2002), Gentry and Silverberg (2002). We demonstrate the comparative result in Table 1 in terms of computational cost and security properties.

F_1: *Computational cost for encryption phase*; F_2: *Computational cost for decryption phase*; F_3: *Overall computational cost for encryption and decryption phases*; F_4: *Provides provable security in random oracle model*; F_5: *Provides security in standard model*; F_6: *Provides security in CPA*; F_7: *Provides security in CCA*.

It may be noted that the presented ID-based cryptographic protocol using IFP and GDLP designed in this paper bears lower computational cost than (Cocks, 2001; Boneh

Table 1
Comparisons among our presented protocol and former protocols.

ID-based cryptographic schemes	F_1	F_2	F_3	F_4	F_5	F_6	F_7
Boneh and Franklin's scheme (Boneh and Franklin, 2001)	$T_P + T_H + T_h + T_e + T_m + T_x$	$T_P + T_h + T_x$	$2T_P + T + T + T_e + T_m + 2T_x$	Yes	No	Yes	Yes
Cocks's scheme (Cocks, 2001)	$T_J + 2T_a + 2T_M + 2T_i$	$T_J + T_a$	$2T_j + 3T_a + 2T_M + 2T_i$	No	No	No	No
Lynn's scheme (Lynn, 2002)	$T_P + T_H + 3T_h + T_x$	$T_P + T_H + 3T_h + T_x$	$2T_P + 2T_H + 6T_h + 2T_x$	Yes	No	No	Yes
Boneh and Boyen's scheme (Boneh and Boyen, 2004b)	$T_P + 4T_e + 2T_M$	$T_P + T_e + T_M + T_i$	$2T_P + 5T_e + 3T_M + T_i$	No	No	Yes	No
Gentry et al.'s scheme (Gentry and Silverberg, 2002)	$T_P + T_H + T_h + T_e + T_m + T_x$	$T_P + T_h + T_x$	$2T_P + T_H + 2T_h + T_e + T_m + 2T_x$	Yes	No	No	Yes
Water's scheme (Waters, 2005)	$2T_P + 3T_m$	$2T_P + T_m + T_i$	$4T_P + 4T_m + T_i$	No	No	No	No
Meshram et al.'s scheme (Meshram *et al.*, 2012)	$4T_e + T_m$	$3T_e$	$7T_e + T_m$	No	No	No	No
Meshram's scheme (Meshram, 2015)	$2T_e + T_m$	$T_e + T_m + T_i$	$3T_e + 2T_m + T_i$	Yes	No	Yes	No
Our scheme	$2T_e$	$2T_e + T_m$	$4T_e + T_m$	Yes	No	Yes	No

and Franklin, 2001; Boneh and Boyen, 2004b; Waters, 2005; Meshram *et al.*, 2012; Meshram, 2015; Lynn, 2002; Gentry and Silverberg, 2002) and is more provably secure in random oracle than (Cocks, 2001; Boneh and Boyen, 2004b; Waters, 2005; Meshram *et al.*, 2012).

6. Applications and Future Scope

Various analysts have as of late begun considering the utilization of ID-based cryptographic protocol in grid security. Our proposed ID-based cryptographic protocol has been designed using IFP and GDLP. By using our technique, we will develop an ID-based encryption model based on lightweight public key management techniques. It has small sizes key pair's private and public keys as contrasted to other ID-based cryptographic protocols available in literature. It is more benefited in grid security architecture. The grid environment may have a huge amount of members that join and leave after some time and that certificates are utilized widely for each employment accommodation. This would definitely muddle key administration and intensification of the bandwidth necessity of a grid system. It was likewise noticed that these issues could be rearranged by utilizing certificate-free ID-based cryptographic protocol. Moreover, in the ID-based cryptographic setting, a user's public key can be made and utilized promptly without the requirement for a public key certificate to be sent to the expected beneficiary (ordinarily via a Transport Layer Security (TLS) handshake). Be that as it may, as far as anyone knows, the dynamic utilization of ID-based keys was ruined by some conventional impediments of ID-based cryptographic protocol, for example, key escrow and the need to circulate private keys through secure channels. All the more critically, a portion of the fundamental security prerequisites wanted in the Globus Toolkit (GT) requires utilizing proxy qualifications for single sign-on and delegation, but our developed ID-based schemes are free from certificate and key escrow problems.

Pay-TV system broadcasts signals of TV channels to a great number of consumers. To enjoy these TV programs, each customer needs only a television, a set-top box and a smart card (conceivably connected to the decoder box). Since there is just a restricted correspondence channel from the administration supplier to the customer, it is necessary to find ways to make sure that only those consumers who fulfill the payment criteria are able to recover the TV signals. Likewise the service provider needs to make it difficult to duplicate the decoder box and make it easy to trace out the traitors if there are any pirate decoder boxes. We notice that pay-TV system is an application just identical to broadcast encryption.

Pay-TV system is an application identical to broadcast encryption on that just supporters who have satisfied the payment criteria are skilled to decrypt the encrypted TV signals. Any broadcast encryption scheme that is collusion resistant and with revocation ability can be used to construct a pay-TV system. A trivial way for constructing a broadcast encryption scheme (pay-TV system) is encrypting TV programs separately for each subscriber using our ID-based cryptographic protocol using IFP and GDLP. It will be a waste of bandwidth, so we improve the scheme by using the subset-cover framework. We evaluated our broadcast encryption scheme in terms of transmission cost (message header), storage (number of secret keys per user and public key size), as well as computational complexity (encryption and decryption cost) per user. The efficiency of our scheme is comparable to the symmetric Subset Difference (SD) scheme and the asymmetric (public key) SD scheme. The difference is that our scheme relies on tamper resistant smart card to achieve an efficient ID-based cryptographic protocol, so it is applicable to applications where smart cards are preferred. For instance, when subscribing for pay-TV service, what people need is a smart card issued by the providers, while they can buy all kinds of favourite set-top boxes from the market.

6.1. *Proposed Chosen Ciphertext Attack (CCA)-Secure ID-Based Scheme Based on IFP and GDLP*

New proposed Chosen Ciphertext Attack (CCA)-secure ID-based scheme based on IFP and GDLP is described in four sub-algorithms such as Setup, Extraction, Encryption and Decryption, which are shown as follows.

Setup: The *Setup* algorithm is same as only steps 1–5 in Section 3 of the present paper. The different steps from scheme are as follows:

1. Construct Hash functions H_1: $\{0,1\}^* \to \{0,1\}^k$, H_2: $Z_q^* \to \{0,1\}^t$, H_3: $Z_q^* \times \{0,1\}^t \to Z_N^*$.

The master key of PKG is set to be $mk = \{p, q, d, A\}$ and the public parameters of PKG are $pp = \{N, e, B, H_1, H_2, H_3\}$.

Extract: The *Extract* algorithm is same as only steps 1–2 in Section 3 of the present paper. The different steps from scheme are as follows:

1. Calculate the analogous public key as follows:

$$b_{ID} = \prod_{i=1}^{K} (b_i)^{h_i} = \prod_{i=1}^{k} (e_i)^{h_i a_i} = e^{a_{ID}} (mod\ N).$$

Encryption: A message $M \in \{0, 1\}^m$ is encrypted for *ID* as follows:

1. Pick random value $r \in Z_q$ and compute

$$C_1 = r{b_{ID}}^{H_3(r,M)}.$$

2. Compute $C_2 = d^{H_3(r,M)}$ and $C_3 = M \bigoplus H_2(r)$.

The cipertext is given by $C = (C_1, C_2, C_3)$.

Decryption: To decrypt $C = (C_1, C_2, C_3)$ under entities identity *ID*, the user can decrypt C utilizing his a_{ID} as follows:

$$C_3 \bigoplus H_2\big(C_1 * C_2^{a_{ID}}\big).$$

7. Conclusion

In the present study, we deal with innovative development model for ID-based cryptographic protocol, its unforgeability can be lessened to the complexity of the IFP and GDLP. IFP and GDLP are major obstinate issues in cryptography. The time execution costs of our presented ID-based cryptographic protocol are nearly as low as the ElGamal cryptosystem using ID-based cryptographic protocol. Moreover, it has a very low computational cost. It is anything but difficult to observe that proposed ID-based cryptographic protocol requires that $t < k$, i.e. that the general number of secret key extraction inquiries ought to be not as much as k. The remarkable open problem is whether we can develop an ID-based cryptographic protocol that has comparable efficiency, however does not require $t < k$.

Acknowledgement. The author would like to thank both anonymous reviewers for their helpful advice. This work was supported by Dr. D.S. Kothari fellowship awarded by University Grants Commission, New Delhi, India.

References

Boneh, D., Boyen, X. (2004a). Secure identity based encryption without random oracles. *Lecture Notes in Computer Science*, 3152, 443–459.

Boneh, D., Boyen, X. (2004b). Efficient selective-id secure identity based encryption without random oracles. *Lecture Notes in Computer Science*, 3027, 223–238.

Boneh, D., Franklin, M.K. (2001). Identity-based encryption from the weil pairing. *Lecture Notes in Computer Science* , 2193, 213–229.

Boneh, D., Franklin, M.K. (2003). Identity based encryption from the weil pairing. *SIAM Journal on Computing*, 32(3), 586–615.

Boneh, D., Canetti, R., Halevi, S., Katz, J. (2003). Chosen-ciphertext security from identity-based encryption. *SIAM Journal on Computing*, 36(5), 1301–1328.

Cocks, C. (2001). An identity based encryption scheme based on quadratic residues. *Lecture Notes in Computer Science*, 2260, 360–363.

Cui, S., Duan, P., Chan, C.W. (2006). An efficient identity-based signature scheme with batch verifications. In: *Proceedings of the 1st ACM International Conference on Scalable Information Systems*, Hong Kong, pp. 22.

Galindo, D. (2004). The exact security of pairing based encryption and signature schemes. *Working Draft*. Available at http://www.cs.ru.nl/ dgalindo/galindoEcrypt.pdf.

Gangishetti, R., Gorantla, M.C., Das, M.L., Saxena, A. (2007). Threshold key issuing in identity-based cryptosystems. *Computer Standards & Interfaces*, 29, 260–264.

Gentry, C., Silverberg, A. (2002). Hierarchical ID-based cryptography. *Lecture Notes in Computer Science*, 2501, 548–566.

Heng, S., Kurosawa, K. (2004). k-Resilient identity-based encryption in the standard model. *Lecture Notes in Computer Science*, 2964, 67–80.

Heng, S., Kurosawa, K. (2006). k-Resilient identity-based encryption in the standard model. *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, E89CA(1), 39–46.

Kiltz, E., Vahlis, Y. (2008). CCA2 secure IBE: standard model efficiency through authenticated symmetric encryption. *Lecture Notes in Computer Science*, 4964, 221–239.

Lee, W.C., Liao, K.C. (2004). Constructing identity-based cryptosystems for discrete logarithm based cryptosystems. *Journal of Network and Computer Applications*, 22, 191–199.

Lynn, B. (2002). Authenticated ID-based encryption. *Crypt., ePrint Archive*, Report 2002/072.
http://eprint.iacr.org/2002/072.

Meshram, C. (2015). An efficient ID-based cryptographic encryption based on discrete logarithm problem and integer factorization problem. *Information Processing Letters*, 115(2), 351–358.

Meshram, C., Meshram, S. (2013). An identity-based cryptographic model for discrete logarithm and integer factoring based cryptosystem. *Information Processing Letters*, 113(10–11), 375–380.

Meshram, C., Meshram, S., Zhang, M. (2012). An ID-based cryptographic mechanisms based on GDLP and IFP. *Information Processing Letters*, 112(19), 753–758.

Rivest, R., Shamir, A., Adelman, L. (1978). A method for obtaining digital signature and public key cryptosystems. *Communications of the ACM*, 21, 120–126.

Shamir, A. (1984). Identity-based cryptosystems and signature schemes. *Lecture Notes in Computer Science*, 196, 47–53.

Sun, J., Zhang, C., Zhang, Y., Fang, Y. (2010) An identity-based security system for user privacy in vehicular ad hoc networks. *IEEE Transactions on Power Systems*, 27(9), 1227–1239.

Waters, B. (2005). Efficient identity-based encryption without random oracles. *Lecture Notes in Computer Science*, 3494, 114–127.

C. Meshram received the PhD from R.T.M. Nagpur University, Nagpur (MS) India. Presently he is post-doctoral fellow under Dr. DS Kothari postdoctoral fellow New Delhi, India. He is interested in the field of cryptography and its application, statistics, raga (music and statistics), neural network, ad hoc network, number theory, time series analysis and climate change, mathematical modelling and chaos theory. He is a member of International Association of Engineers (IAENG), Hong Kong, World Academy of Science, Engineering and Technology (WASET), New Zealand, Computer Science Teachers Association (CSTA), USA, Association for Computing Machinery (ACM), USA, International Association of Computer Science and Information Technology (IACSIT), Singapore, European Association for Theoretical Computer Science (EATCS), Greece, International

Association of Railway Operations Research (IAROR), Netherlands, International Association for Pattern Recognition (IAPR), New York, International Federation for Information Processing (IFIP), Austria, Association for the Advancement of Computing in Education (AACE), USA, International Mathematical Union (IMU), Berlin, Germany, European Alliance for Innovation (EAI), International Linear Algebra Society (ILAS), Haifa, Israel, Science and Engineering Institute (SCIEI), Machine Intelligence Research Labs (MIR Labs), USA, Society: Intelligent Systems, KES International Association, United Kingdom, Universal Association of Computer and Electronics Engineers (UACEE), The Society of Digital Information and Wireless Communications (SDIWC) and life-time member of Internet Society (ISOC), USA, Indian Mathematical Society, Cryptology Research Society of India and Ramanujan Mathematical Society of India (RMS). He is regular reviewer of sixty international journals and international conferences.

Y.-M. Tseng is currently a professor in the Department of Mathematics, National Changhua University of Education, Taiwan. He is a member of IEEE Computer Society, IEEE Communications Society and the Chinese Cryptology and Information Security Association (CCISA). In 2006, his paper received the Wilkes Award from The British Computer Society. He has published over one hundred scientific journals and conference papers on various research areas of cryptography, security and computer network. His research interests include cryptography, network security, computer network and mobile communications. He serves as an editor of several international journals.

C.-C. Lee received the PhD degree in Computer Science from National Chung Hsing University (NCHU), Taiwan, in 2007. He is currently a professor with the Department of Library and Information Science at Fu Jen Catholic University. Dr. Lee is currently an editorial board member of International Journal of Network Security, Journal of Computer Science, Cryptography, and International Journal of Internet Technology and Secured Transactions, and The Open Automation and Control Systems Journal. He also served as a reviewer in many SCI-index journals, other journals, other conferences. His current research interests include data security, cryptography, network security, mobile communications and computing, wireless communications.

S.-G. Meshram received M. Tech degree in Soil and Water Engineering in 2009 with gold medal from College of Agricultural Engineering, Jawaharlal Nehru Krishi Vishwa Vidhyalaya, Jabalpur (M.P.); and PhD Degree in Water Resource Development and Management from IIT Roorkee (U.K.) India in 2015. She is currently Dr. D.S. Kothari postdoctoral fellow in the Department of Mathematics and Computer Sciences, Rani Durgawati University, Jabalpur, India. Her current research interests include geographical information systems, rainfall-runoff sediment yield modelling, SCS-CN. She is carrying out her research work in the field of rainfall-runoff, sediment yield, water quality, application of RS and GIS water network and cryptographic protocol. She has published more than 50 research papers in refereed journals, conference and workshop proceedings, and books. She is a member of an international society and reviewer of a reputed journal.