INTL JOURNAL OF ELECTRONICS AND TELECOMMUNICATIONS, 2022, VOL. 68, NO. 3, PP. 469-473
Manuscript received January 31, 2022; revised August, 2022. DOI: 10.24425/ijet.2022.141262

Secure And Efficient Encryption Scheme Based on Bilinear Mapping

Vandani Verma, and Pragya Mishra

***Abstract*—With the increasing uses of internet technologies in daily life, vulnerability of personal data/information is also increasing. Performing secure communication over the channel which is insecure has always been a problem because of speedy development of various technologies. Encryption scheme provides secrecy to data by enabling only authorized user to access it. In the proposed paper, we present an encryption algorithm designed for data security based on bilinear mapping and prove it secure by providing its security theoretical proof against adaptive chosen cipher-text attack. With the help of a lemma, we have shown that no polynomially bounded adversary has non-negligible advantage in the challenging game. We also give the comparative analysis of the proposed scheme in terms of security and performance with Deng et al., 2020 and Jiang et al., 2021 schemes and prove that proposed algorithm is more efficient and secure than others existing in literature against adaptive chosen cipher-text attack.**

***Keywords*—Bilinear mapping; encryption; KGC; ID-OWE; Discrete Log Problem**

I. Introduction

PASSING secret messages via insecure channels have been important concerns amongst the communication techniques. Disguising such secret message is solution to such problem. Encryption is a method to encode the words or messages such that the message is readable only to the authorized receiver. To encrypt the desired message, an encryption scheme uses an encryption algorithm that produces cipher text which is decrypted by the authorized recipient only. In early symmetric key cryptography, sender of the message used to share a private key in advance with the intended recipient so that only this intended recipient (to whom sender has shared private key) can read the message by decrypting the cipher text using the key. In this way, an encryption algorithm with symmetric key makes possible for two users to share their messages securely over an insecure channel. Though, in public key cryptography or symmetric key cryptography it is not necessary to share a key beforehand between the sender and authorized recipient for a secure communication. Sender or originator of the message uses his public key for encryption of the message and the intended recipient uses his private/secret key for decryption of the message. To unburden the load of public key certificates management in traditional public key encryption, in 1984, Shamir firstly proposed the idea of ID based public key cryptography. The ID based public key systems allows some public information of the user such as name, address etc. to be used as his/her public key. The private key of the user is calculated by a trusted party called key generating center (KGC) after user authentication and sent to the user via a secure channel. The use of this trusted third party makes easy for the user to authenticate other parties existing on the communicating network. This type of encryption scheme holds primary innovation as it uses user's identity attributes, such as email addresses or phone numbers. This selective feature significantly reduces the complexity of a cryptography system by eliminating the need for generating and managing users' certificates. It also makes much easier to provide cryptography to unprepared users, since messages may be encrypted for users before they interact with any system components. Onwards 1984, many schemes were proposed to realize identity-based encryption schemes (Craig, 2006; Matthew and Susan, 2007; SK Hafizul, 2014). However, Boneh and Franklin (2001) and Cocks (2001) proposed the first identity-based encryption schemes which was provenly secure in random oracle model. Cocks's scheme is based on the "Quadratic Residuosity Problem," and encryption and decryption are comparatively fast in respect of speed of RSA scheme [10]. The ID based encryption is a public key encryption. This facility of public key encryption without using certificates allows it to cater many practical applications.

II. Background Concepts

A. Bilinear pairing

In 1993, Menezes et al (1993) had firstly introduced the concept of Bilinear pairings [9]. They proposed the reduction of elliptic curve logarithmic problem to logarithmic problem in the multiplicative group of an extension of the underlying finite field. pairing can be used to take the discrete log problem on a certain class of elliptic curves over finite field to the discrete log problem on a smaller finite field. Bilinear pairing is defined as: A mapping e: $G_1 \times G_1 \rightarrow G_2$ where, G_1 is a cyclic additive group and G_2 is a cyclic multiplicative group with the same order q of G_1 and P is generator. A mapping is bilinear if it holds the following properties:

Bilinearity: $e(aP, bQ) = e(P,Q)^{ab}$ for all $P,Q \in G_1$ and $a, b \in Z_q^*$

Non-Degeneracy: $e(P,P)$ is the generator of G_1 only if P is a generator of G_2.

Computability: If $P, Q \in G_1$ then $e(P,Q)$ is easily computable

B. Some Difficult Problems in Cryptography:

1) Discrete log Problem:

For a given $Z \in G_1$, where $Z = aP$, to compute a is a discrete

Vandani Verma is with Amity Institute of Applied Sciences, Amity University, Noida-125 (Uttar Pradesh), India (email: vandaniverma@yahoo.com).

Pragya Mishra is with Amity Institute of Applied Sciences, Amity University, Noida-125 (Uttar Pradesh), India (e-mail: pragya.login@gmail.com).

logarithm problem.

2) *Decisional Diffie-Hellman Problem and Bilinear Diffie-Hellman problem:*
For unknown $a, b, c \in Z_q^*$ and given P, aP, bP, cP to decide whether $c = ab \bmod q$ is a decisional Diffie-Hellman problem and to compute $e(P, P)^{abc}$ is called bilinear Diffie-Hellman problem.

III. PROPOSED ALGORITHM

In this section, identity-based encryption algorithm is proposed, which will act as the BasicIdent in the proposed security proof.

A. *Setup:*

In this phase, the public parameters params is generated by Key Generation Center KGC. Using the system parameter $U \in N$ as input, it outputs master public-private key pair (*mpk*, *msk*), $e: G_1 \times G_1 \to G_2$ is a bilinear map, where $\langle G_1, + \rangle$is a cyclic additive group with generator p, $\langle G_2, . \rangle$ is a cyclic multiplicative group. The public key is calculated as $P_{Pub} = sP$, where s denotes the master secret/private key (*msk*). The hash functions used are:
$H_0: \{0,1\}^* \to G_1,\ H_1: G_2 \to \{0,1\}^*,\ H_2: \{0,1\}^* \times \{0,1\}^* \to Z_p^*$.
The message space is $M = \{0,1\}^*$. The cipher text space is calculated as $c = Z_p \times \{0,1\}^* \times \{0,1\}^*$. The hash functions and the definition of the groups that are used in the scheme fix the parameter params $\langle G_1, G_2, mpk, e, p, H_0, H_1, H_2 \rangle$.

B. *Key Generation:*

The key generation activity is performed by Key Generation Centre once in a year for their registered users. It takes as input the identity ID_U of the corresponding user U and his/her master secret key s and computes secret/ private key S_{IDU} for user U such as-
Step 1: $Q_{IDU} = H_0(ID_U) \in G_1$,
Step 2: $S_{IDU} = sQ_{IDU}$
where the string $ID \in \{0,1\}^*$

C. *Encryption:*

For a given plain text $M \in M$, a private key S_{IDU}, a public key Q_{IDU} and system parameters,
Step 1: Choose a random $\sigma \in \{0,1\}^n$
Step 2: Compute $r = H_2(\sigma, M)$
Step 3: $g = e(Q_{IDU,} P_{pub})$
Step 4: $T_1 = rP, T_2 = \sigma \oplus H_1(g^r), T_3 = M \oplus H_1(g^r)$
Then the cipher text $c = \langle T_1, T_2, T_3 \rangle$

D. *Decryption:*

For a given cipher text $c = \langle T_1, T_2, T_3 \rangle$, system parameters and a public key Q_{IDU}, the message can be decrypted by the authorized user if and only if $g' = e(S_{IDU}, T_1)$ holds,
i.e. $g' = e(S_{IDU}, T_1)$
$= e(sQ_{IDU}, rP)$
$= e(Q_{IDU}, srP)$
$= e(Q_{IDU}, sP)^r$
$= e(Q_{IDU}, P_{pub})^r$
$= g^r$
Step 1: Compute $\sigma' = T_2 \oplus H_1(g^r)$
Step 2: $M' = T_3 \oplus H_1(g^r)$
Step 3: $r' = H_2(\sigma', M')$
If $T_1 = r'P$, then scheme is consistent.

IV. SECURITY ANALYSIS

In public key encryption scheme, standard concept of security of a scheme is that no adversary should be able to get any piece of information about a ciphertext even he is provided the decryption of any other ciphertext as per the choice made by him. But we have allowed here the adversary to get the knowledge of private key corresponding to some IDs of his interest excluding the one on which he would be tried. But the system is kept secure in this setting also against such type of attack. This is the notion of semantic security against adaptive chosen cipher-text attack for an identity-based encryption scheme (IND-ID-CCA).

A. *BasicPub:*

1) *Key Gen:*
In the setup stage, the algorithm is arranged in the same way as in BasicIdent. The two cyclic groups G_1 and G_2 of same prime order and a bilinear map $e: G_1 X G_1 \to G_2$ are generated in the same way. KGC computes a pair of public key P_{pub} and private key s similarly as BasicIdent. The message space $M = \{0,1\}^*$and the cipher text space $c = Z_p \times \{0,1\}^* \times \{0,1\}^*$ and the hash function $H_2: \{0,1\}^* X \{0,1\}^* \to Z_p^*$ are selected in the same way. Now, the algorithm picks a random point Q_{IDU} in group G_1. The public key is < G_1, G_2, e, n, p, P, P_{pub}, Q_{IDU}, H_2 > and the private key is $S_{IDU=}$ $sQ_{IDU.}$

2) *Encryption:*
This is same as BasicIdent. For encryption of message $m \in \{0,1\}^*$, the algorithm chooses randomly $\sigma \in \{0,1\}^*$ and computes- $r = H_2(\sigma, M)$, cipher text $c =< T_1, T_2, T_3 >$ such that $T_1 = rP, T_2 = \sigma \oplus H_1(g^r), T_3 = M \oplus H_1(g^r)$Where, $g = e(Q_{ID}, P_{pub})$

3) *Decryption:*
For a given cipher text $c = \langle T_1, T_2, T_3 \rangle$, the message can be decrypted by using < G_1, G_2, e, n, p, P, P_{pub}, Q_{IDU}, H_2 > and the private key S_{IDU} as input. The message can be decrypted by authorized user only if $g' = e(S_{IDU,} T_1)$ holds
i.e.$g' = e(S_{IDU}, T_1)$
$= e(Q_{IDU}, srP)$
$= e(Q_{IDU}, P_{pub})^r$
$= g^r$
The algorithm computes-
$\sigma' = T_2 \oplus H_1(g^r)$
$M' = T_3 \oplus H_1(g^r)$
$r' = H_2(\sigma', M')$
If $T_1 = r'P$, then scheme is consistent.

B. *One-Way Encryption (OWE):*

To prove that an identity-based encryption scheme is IND-ID-CCA, security notion of One-way Encryption (OWE) has been recognized as follows:

For a public key encryption scheme, if an adversary is given a random public key P_{pub} and ciphertext C against the random plaintext M, the objective of adversary is to retrieve the original plaintext M. In other words, a public key encryption scheme would be OWE scheme if there is no polynomially bounded adversary which have a non-negligible probability of retrieving the plain text while attacking the scheme. If an adversary is allowed to obtain some private keys too, then concept of One-

Way Identity based Encryption (ID-OWE) can be defined using the following game:

1) *Setup:*

Using the security parameter λ, the challenger runs the Setup algorithm. The challenger preserves the master secret key with himself and returns the public parameters to adversary.

2) *Phase 1:*

In this phase, adversary raises private key extraction queries $ID_1, ID_2 \ldots\ldots ID_m$. The challenger runs the Extract algorithm to produce the private key d_i corresponding to the public key ID_i and responds to adversary by sending it.

3) *Challenge:*

The adversary challenges by giving output of a public key ID different from $ID_1, ID_2 \ldots\ldots ID_m$. The challenger encrypts randomly chosen plain text $M \in M$ by using ID as public key. He sends this encrypted text to the adversary.

4) *Phase 2:*

The adversary raises some more private key extraction queries $ID_{m+1}, ID_{m+2} \ldots ID_n$ other than ID. The challenger replies in same manner as given in Phase 1.

5) *Guess 1:*

The guess produced by adversary is $M' \in M$. It wins if $M' = M$. Here, the advantage gained by adversary (ID-OWE attacker) against the scheme is $Pr[M' = M]$ where, the probability is computed over random picks made by the adversary and the challenger. We say that an identity-based encryption scheme is ID-OWE scheme if no polynomially bounded adversary (in λ) has non-negligible advantage (in λ) in the above game against the challenger. We here provide security analysis of proposed identity-based encryption scheme (BasicIdent). We will prove here that an ID-OWE attack on BasicIdent scheme can be transformed on OWE attack on its BasicPub scheme. It shows that extraction of private key queries does not help the adversary. To prove this, we will use the following lemma:

C. Lemma

Let $H_0: \{0,1\}^* \rightarrow G_1{}^*$ be a random oracle. Let U be an ID-OWE adversary with advantage ε against BasicIdent and creates private key extraction queries at most $q_E > 0$. Let V be an OWE adversary with advantage at least $\frac{\varepsilon}{\varepsilon(1+qE)}$ against BasicPub. The running time of V is $O(time(A))$.

Proof of Lemma: A public key $N_{pub} = \langle G_1, G_2, e, P, Q_{ID}, H_1, P_{pub}, n, p \rangle$ and a private key $S_{ID} = sQ_{ID}$, is generated by the challenger using the algorithm Setup of BasicPub. The challenger using the Encrypt Algorithm and the public key N_{pub} also encrypts a random plaintext M and provides the ciphertext $c = \langle T_1, T_2, T_3 \rangle$ to V, where $T_1 = rP$, $T_2 = \sigma \oplus H_1(g^r)$ and $T_3 = M \oplus H_1(g^r)$. After this V computes some speculations for M on interfacing with U in following manner:

1) *Setup:*

V outputs the algorithm U, the BasicIdent parameters $\langle G_1, G_2, e, P, H_0, H_1, P_{pub}, n, p \rangle$, where all elements of tuple excluding H_0 are taken from N_{pub}. H_0 is a random oracle governed by V.

2) *H_1-queries:*

V maintains a list of tuples $\langle ID_i, Q_i, x_i, y_i \rangle$ which holds the information of all the previous queries raised to oracle H_0. We call initially empty list of such queries as H_0^{list1}. V responds to queries of U in following ways: It returns Q_j if the query ID_j is already present in H_0^{list1} in a tuple $\langle ID_j, Q_j, x_j, y_j \rangle$. Otherwise, V generates a random *card* $\in \{0,1\}$ so that P(card = 0) = ω where $\boldsymbol{\omega = 1 - \frac{1}{(1+qE)}}$. V selects a random $a \in Z_p^*$. If *card* = 1, compute $Q_j = aQ_{ID} \in G_1$. If *card* = 0, compute $Q_j = bP \in G_1$. The tuple $\langle ID_j, Q_j, a, card_j \rangle$ is added to H_0^{list1} and returns Q_j to *U*. Here, in both the situations, Q_j is uniformly distributed in G_1^* and is independent of *U*'s understanding.

3) *Private Key Extraction Queries:*

The private key extraction ID_j issued by *U* are responded by *V* as follows: If U had issued the query ID_j to oracle H_0 previously then find the tuple $\langle ID_j, Q_j, a, card_j \rangle$ in the H_0^{list1}. On the contrary, by following the former procedure, it creates a tuple and connect it to H_0^{list1}. If $card_j = 1$, therefore, V reports failure and collapses. This symbolizes the foul up of the attack on BasicPub. Otherwise, if $card_j = 0$, so $Q_j = a_j P$. Return $S_j = a_j P_{pub} \in G_1^*$ to *U*. On the contrary, S_j is the private key related to ID_j since $S_j = a_j P_{pub} = a_j sP = sQ_j$.

4) *Challenge:*

When *U* wishes to be challenged against ID for which V responds as follows: If *U* issues a query ID to oracle H_1 previously then find the tuple $\langle ID, Q, a, card \rangle$ in the H_0^{list1}. Otherwise, create a tuple by using the said procedure and connect it to H_0^{list1}.

- If *card* = 0 then *V* submits failure and terminates. This symbolizes the failure of the attack on BasicPub.
- If *card* = 1, then $Q = aQ_{ID}$. Let the challenged ciphertext be $c = \langle T_1, T_2, T_3 \rangle$ where, $T_1 = rP$, $T_2 = \sigma \oplus H_1(g^r)$ and $T_3 = M \oplus H_1(g^r)$ given to algorithm U. Return $c' = \langle a^{-1}T_1, T_2, T_3 \rangle$ where a^{-1} is inverse of a *mod* p. For the public key *ID*, the BasicIdent encryption of message *M* is c' since T_2 and T_3 is exclusive-or of σ and message M respectively with the hash of $e(Q_{ID}, P_{pub})^r$. Since,

$$\begin{aligned} e(S_{ID}{}', a^{-1}T_1) &= e(sQ, a^{-1}rP) \\ &= e(saQ_{ID}, a^{-1}rP) \\ &= e(Q_{ID}, sP)^{raa^{-1}} \\ &= e(Q_{ID}, P_{pub})^r \\ &= g^r \end{aligned}$$

Therefore, the decryption of c' using $S_{ID}{}'$ is synonymous to the decryption of C using S_{ID}.

D. Guess 2:

Algorithm U gives its guess M' and V returns M' as its guess i.e. the decryption of C.

1) Claim.

If V doesn't terminate during the simulation, algorithm U's view is identical to its view in actual attack. In addition, if V doesn't terminate, then $P(M = M') \geq \varepsilon$, where the probability is computed for the random bits consumed by the challenger, U and V.

2) Proof of the Claim:

All the replies return to the private key extraction queries are valid until V doesn't get abort. The responses which oracle H_1 gives are independently and uniformly distributed in G_1^*. And the encryption of plaintext $M \in M$ is the challenged ciphertext C'. Thus, view of U is identical to its view in the actual attack. In addition, BasicIdent encryption of M against the public key ID which U selects is the challenged ciphertext C'. Hence, by considering the definition of U, the probability of making correct guess by U is at least ε. The calculation left over is probability computation during the simulation when V doesn't get abort. If U raises q_E private key extraction queries, then the probability of V for not aborting while handling one of these queries is ω^{qE}. The probability for V to not get abort during the challenge step is $(1-\omega)$. Therefore, the probability of V for not getting abort during the simulation is given by $\omega^{qE}(1-\omega)$. We chose $\boldsymbol{\omega} = \mathbf{1} - \frac{\mathbf{1}}{(\mathbf{1}+\boldsymbol{qE})}$ to maximize this function. We can learn that the probability of V doesn't get abort is at least $\frac{\mathbf{1}}{\boldsymbol{\varepsilon}(\mathbf{1}+\boldsymbol{qE})}$. The analysis carried out for proof of the Lemma is based on Coron's analysis [4] of the Full signature scheme.

V. Performance Analysis

In this section, we compare the proposed scheme on the basic of pairing, multiplication, hash, exponential and inverse required for the encryption and decryption with the schemes proposed by (Deng et al., 2020 and Jiang et al., 2021)

TABLE I
PERFORMANCE ANALYSIS

Operations → / Scheme ↓	Bilinear Pairing	Multiplication in G_1 and Z_q	Hash	Exponential	Inverse in Z_q	Secure against adaptive chosen cipher-text attack
Proposed Algorithm	2	6	1	1	0	Yes
Deng et al 2020	5	5	2	7	2	No
Jiang et al 2021	10	6	2	9	0	No

TABLE II
COMPUTATIONAL TIME FOR EACH SCHEME

Scheme	Proposed Algorithm	Deng et al 2020	Jiang et al 2021
Total Bilinear Pairing	2	5	10
Computational time (3.21m. sec for one pairing)	6.42	16.05	32.1

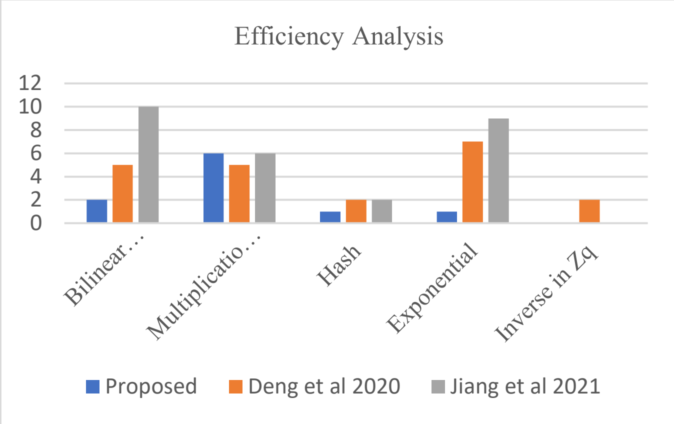

Fig.1. Efficiency Analysis

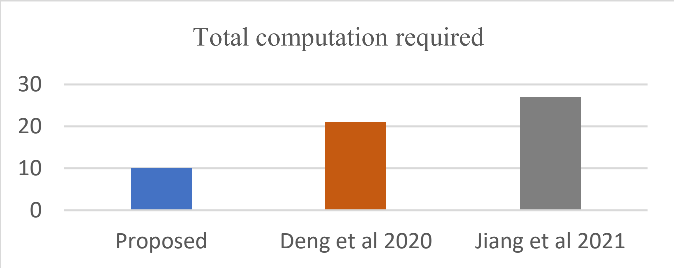

Fig.2. Required computations

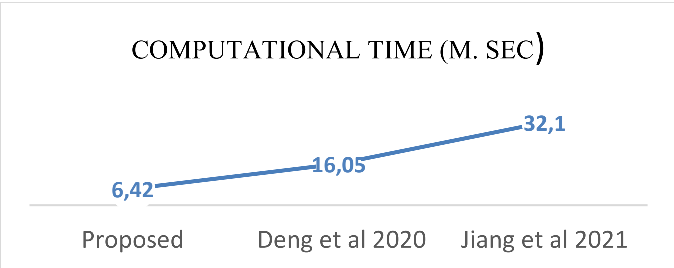

Fig.3. Efficiency Analysis

From the above facts and figures, we can conclude that our proposed scheme is more secure and efficient as compared to Jianting Ning et al 2020 and Hua Deng et al 2020 schemes.

VI. Conclusion

The paper proposed an identity-based encryption scheme based on bilinear maps and provides notion of semantic security against adaptive chosen cipher-text. The proposed scheme has been analyzed keeping security aspects by giving theoretical proof of the lemma and results that if a user is confirmed to create at most $q_E > 0$ private key extraction queries then OWE adversary has at least $\frac{\boldsymbol{\varepsilon}}{\boldsymbol{\varepsilon}(\mathbf{1}+\boldsymbol{qE})}$ advantage against BasicPub with the running time $O(time(A))$ of V, where A is the algorithm. In other words, no polynomially bounded adversary has non-negligible advantage in the challenging game. So, our scheme is secure against adaptive chosen cipher-text. We also checked the performance of the proposed scheme and showed our scheme is more efficient and secure than Jianting Ning et al 2018 and Hua Deng et al 2020.

REFERENCES

[1] C. Gentry, "Practical identity-based encryption without random oracles," in *Advances in Cryptology-EUROCRYPT*, ed: Springer 445-464, 2006. https://doi.org/10.1007/11761679_27

[2] M. Green, and S. H. Berger, "Blind Identity based encryption and simulatable oblivious transfer," *Cryptography eprint Archive,* Report 2007/235, 2007, available at https://eprint.iacr.org/2007/235

[3] S. K. H. Islam, "Identity-based encryption and digital signature scheme using extended chaotic maps", *IACR Cryptology ePrint Archive*, Volume 2014/ 275, 2014

[4] D. Boneh, and M. Franklin, "Identity based encryption from the Weil pairing", *In Advances in Cryptology*, Crypto 01, 2139:213-229, 2001. https://doi.org/10.1007/3-540-44647-8_13

[5] C. Cocks, "An identity-based encryption scheme based on quadratic residues," *Proceedings of the 8th IMA International Conference on Cryptography and Coding*, Lecture Notes in Computer Science, 2260, 2001. https://doi.org/10.1007/3-540-45325-3_32

[6] R. L. Rivest, A. Shamir, and L. M. Adleman, "A Method for Obtaining Digital Signatures and Public Key Cryptosystems", *ACM*, vol. 21 no. 2, pp. 120-126, 1978.

[7] A. Menezes, T. Okamoto, and S. Vanstone,. "Reducing elliptic curve logarithms to logarithms in a finite field," *IEEE Transactions on Information Theory* 39(5): 1639-1646, 1993. https://doi.org/10.1109/18.259647

[8] A. Shamir, "Identity based cryptosystems and signature schemes," in *Proceedings of Crypto*'1984, LNCS 196, Springer Verlag, p. 47-53, 1984. https://doi.org/10.1007/3-540-39568-7_5

[9] J. S. Coron, "On the exact security of full domain hash," In Bellare M. (eds), *Advances in Cryptology-Crypto* 2000. LNCS, Vol 1880, Springer Verlag, Berlin, 2000. https://doi.org/10.1007/3-540-44598-6_14

[10] V. Verma, and D. Gupta, "An efficient signcryption algorithm using bilinear mapping," in *Proceedings of 3rd International Conference on Computing for Sustainable Global Development* (INDIACom) 2016, 16-18 March 2016, IEEE Xplore Digital Library, pp. 988-990, 2016.

[11] H. Deng, Z. Qin, Q. Wu, Z. Guan, R. H. Deng, Y. Wang, & Y. Zhou, "Identity-Based Encryption Transformation for Flexible Sharing of Encrypted Data in Public Cloud," IEEE Transactions on Information Forensics and Security, 15(April), 3168–3180, 2000. https://doi.org/10.1109/TIFS.2020.2985532

[12] P. Jiang, J Ning, K. Liang, C. Dong, J. Chen, & Z. Cao, "Encryption Switching Service: Securely Switch Your Encrypted Data to Another Format," IEEE Transactions on Services Computing, 14(5), 1357–1369, 2021. https://doi.org/10.1109/TSC.2018.2876849

[13] M. Gagne, "Applications of Bilinear Maps," in *Cryptography*, Waterloo, Ontario, Canada, 2002.

[14] D. Galindo, and I. Hasuo,."Security notions for identity-based encryption," *Cryptology eprint Archive*, Report 2005/253, 2005 http://eprint.iacr.org/