Efficiency Comparison of Various Important Identity-Based Digital Signature Schemes based on Bilinear Pairings

Subhas Chandra Sahana and Bubu Bhuyan

Abstract— **In identity-based cryptosystem (IBC), a user can use his/her unique identity as the public key, which simplifies the key management procedure compared to traditional public key infrastructure (PKI) based cryptosystem. Authentication is a desired property in cryptographic protocols. The signature scheme provides this property. Notion of pairing reduces the computation overheads and makes a cryptographic scheme simple and efficient. In this paper, we compare the efficiency of some important established identity (ID)-based signatures schemes based on bilinear pairings in terms of involved computational cost, communicational cost. We implement all the schemes using a tool called pairing based cryptography (PBC) and also compare all undertaken schemes in terms of consumed running time.**

Index Terms— **Bilinear pairings, Digital Signature, Identity (ID)-based signature, Pairing based cryptography**

I. INTRODUCTION

A simple digital signature which is the building block provides the authentication, integrity and non-repudiation security services. Improving the performance of digital signatures is therefore an essential goal. Generally, the time complexity is taken into account to measure the performance for a cryptographic scheme traditionally. It is to be noted that communication complexity is another measure which is becoming increasingly important.

In 1984, Shamir [1] proposed the idea of identity (ID)-based cryptosystem and signature scheme. The goal of Shamir's work was to simplify the key management procedures in certificate based public key setting and to achieve moderate security. They also proposed the first ID-based signature scheme. In such a scheme, the unique identity of each user is used as his/her public key. A private key generator (PKG) is supposed to provide the private key to the user for his/her identity. The main idea of ID-based cryptosystem is that the public key of a user can be calculated directly from his/her identity instead of being extracted from a certificate issued by a certificate authority. Therefore, the ID-based systems overcome and hence avoid the traditional PKI based systems. In an ID-based signature scheme, an unique identity of user (such as E-mail, IP address, etc.) is used as his/her public key for signing and verification algorithm. This scheme relaxes the public management procedure. It assumes that there exist a PKG to generate and provide the private key to each user according to their identity.

In recent years, a lot of research activities are going on cryptographic schemes based on bilinear pairing. Initially bilinear pairings, namely Weil pairing and Tate pairing of algebraic curves were used for cryptanalytic purpose such as MOV attack [10] to reduce the discrete logarithm problem on some elliptic or hyper elliptic curves to the discrete logarithm problem in a finite field. In 2001, Boneh and Franklin proposed a practical implementation of Identity-Based Encryption (IBE) [11] scheme based on bilinear pairing. After that, the bilinear pairings have been found positive application in cryptography to construct new cryptographic schemes. So, it is worth of giving a comparison study on the efficiency of identity-based signature schemes from bilinear pairings to judge the signature schemes such that we get efficient signature schemes in terms of involved computational cost and communication cost (keeping attention on the size of the generated signature) before deploying those schemes in the practical field.

The rest of this paper is organized as follows. In Section II, we briefly introduce some preliminary works. In section III, we review five important identity-based signature schemes. In section IV, the efficiency analysis has been done in terms of involved operation and consumed running time. Finally, in section V, we conclude our work.

The rest of this paper is organized as follows. In Section II, we briefly introduce some preliminary works. In section III, we review five important identity-based signature schemes. In section IV, the efficiency analysis has been done in terms of involved operation and consumed running time. Finally, in section V, we conclude our work.

II. MATHEMATICAL BACKGROUND

Bilinear pairings

Given two cyclic groups G_1 and G_2 of prime order q, a map $e: G_1 \times G_1 \rightarrow G_2$ satisfying the following properties are called bilinear pairing:

Manuscript received Sept, 2017.
***Subhas Chandra Sahana**, Department of Information Technology North Eastern Hill University, Shillong – 793022, INDIA Phone/ Mobile No9402135453.*
***Bubu Bhuyan**, Department of Information Technology North Eastern Hill University, Shillong – 793022, INDIA*

- Bilinearity: $e(aP, bQ) = e(P, Q)^{ab}$, for all $a, b \in Z_q^*$ and $P, Q \in G_1$.
- Non-degeneracy: There exists $P, Q \in G_1$, such that $e(P, Q) \neq 1$.
- Computability: There is an efficient algorithm to compute $e(P, Q)$, for all $P, Q \in G_1$.

Bilinear Diffie-Hellman Problem (BDHP)

Let G be a finite cyclic group of order n with a generator g, and let $a, b, c \in Z_q^*$. The BDHP is to compute the value of the bilinear pairing $e(g, g)^{abc}$, whenever g (generator of the group) g^a, g^b and g^c are given.

Decision Diffie-Hellman Problem (DDHP):

For $a, b, c \in Z_q^*$. If P, bP, cP is given to decide whether $c \equiv ab \bmod q$. Now due to bilinear pairing it is easy to solve this problem..

Computational Diffie-Hellman Problem (CDHP):

For $a, b, c \in Z_q^*$ given P, bP, cP to compute abP is known as Computational Difffie-Hellman Problem which is hard problem.

Gap Diffie-Hellman Groups (GDH) group:

A group G is called a Gap Diffie-Hellman (GDH) group if DDHP can be solved in polynomial time but no probabilistic algorithm can solved in CDHP with non-neglible advantage within polynomial time in G.

III. Brief Review of Undertaken Important Established ID-Based Signature Schemes

An ID-based signature scheme consists of the following four signature generation model:

- Key Generation: For the security parameter K, PKG generates the systems public parameters and the master key.
- Extraction: PKG runs this algorithm to extract the secret key SID for the user with identity ID.
- Signature: To produce a signature on a message m, a user with identity ID and secret key SID uses this algorithm with input (m, ID).
- Verification: This algorithm takes an input (m, ID). and verifies whether or not is a valid signature of the user with identity ID.

HESS'S SCHEME [5]

Hess et al. proposed an ID-based signature scheme using pairings and distribution of keys to multiple trust authorities. The signature scheme is as follows:

- *Key Generation*: Let G_1 and G_2 be two groups of prime order q, and let P be the generator of G_1. Define a bilinear map $e: G_1 \times G_1 \to G_2$. PKG selects $s \in Zq^*$ and set $P_{pub} = sP$. Define cryptographic hash functions $H_1: \{0,1\}^* \to G_1$ and $H_2: \{0,1\}^* \to Zq^*$. P_{pub} is the public key and s is the master key.
- *Extract:* For the given public identity $ID \in \{0,1\}^*$ of the user, PKG computes the user's public key $Q_{ID} = H_1(ID)$ and his secret key $S_{ID} = sQ_{ID}$.
- *Signing:* To sign a message $m \in \{0,1\}^*$ the signer having secret key SID, chooses arbitrary $P1 \in G_1^*$ and $k \in Zq^*$ and computes

$$r = e(P1, P)^k$$
$$v = H_2(m, r),$$
$$u = vSID + kP_1.$$

The signature is the pair $(u, v) \in (G_1, Zq^*)$.

- *Verification:* For the given public key $Q_{ID} \in G_1$, message $m \in \{0,1\}^*$ and the signature $(u, v) \in (G_1, Zq^*)$, the verifier computes $r = e(u, P)\, e(Q_{ID}, Ppub)^v$ and accepts the signature if and only *if* $v = H_2(m, r)$, rejects otherwise.

PATERSON'S SCHEME [3]

Paterson presented an ID based signature scheme from bilinear pairings, using the computational primitives and keys, almost the same as in Boneh and Franklin scheme. Their signature scheme consists of the following algorithms:

- *Key Generation*: Let G_1 and G_2 be two groups of prime order q, and let P be the generator of G_1. Define a bilinear map $e: G_1 \times G_1 \to G_2$. PKG selects $s \in Zq^*$ and set $Ppub = sP$. Define cryptographic hash functions $H_1: \{0,1\}^* \to G_1, H_2: \{0,1\}^* \to Zq^*$, and $H_3: G_1 \to Zq^*$. P_{pub} is the public key and s is the master key.
- *Extract:* For the given public identity $ID \in \{0,1\}^*$, of the user, PKG computes the users public key $Q_{ID} = H_1(ID)$ and his secret key $S_{ID} = sQ_{ID}$.
- *Signing:* To sign a message $M \in \{0,1\}^*$, the user first chooses a number $k_1 \in Zq^*$ and computes $S = k_1 (H_2(M)P + H_3(R)S_{ID})$, where $R = kP$, the signature on the message M is $(R, S) \in G_1 \times G_1$.
- *Verification:* To verify the signature (R, S) on M, verifier computes and accepts the signature, if and only if $e(R, S) = e(P, P)^{H_2(M)} e(Ppub, Q_{ID})^{H_3(R)}$.

SAKAI ET AL. SCHEME [8]

- *Key Generation:* The PKG chooses $s \in Zq^*$ as his master secret key and computes the global public key $P_{pub} = sP$. It then chooses a random Map-to-Point hash function $H_1: \{0,1\}^* \to G_1$. Parameter Generation: All the parameters are set $(G_1, G_2, e, s, P, P_{pub}, H_1)$.
- *Extract:* For the given public identity $ID \in \{0,1\}^*$, of the user, PKG computes the users public key $Q_{ID} = H_1(ID)$ and his secret key $S_{ID} = sQ_{ID}$.
- *Signing:* Given a private key S_{ID} and a message $m \in G_1$, choose a $r \in Zq^*$ and calculate:

$$S_1 = S_{ID} + rH_1(m)$$
$$S_2 = rP$$

Signature: $S = \{S_1, S_2\} \in G_1 \times G_1$.

- *Verification:* The signature $s = \{S_1, S_2\}$ of an identity ID on a message M is valid if the following equation holds.

$$e(Q_{ID}, P_{pub})e(m, S_2) = e(S_1, P)$$

CHA-CHEON'S SCHEME [6]

- *Key Generation:* The PKG chooses $s \in Zq^*$ as his master secret key and computes the global public key P_{pub} as sP. It then chooses a random Map-to-Point hash function $H_1: \{0,1\}^* \rightarrow G_1$ and another cryptographic hash function $H_2: \{0,1\}^* \times G_1 \rightarrow Zq^*$.
  Parameter Generation: All the parameters are set $(G_1, G_2, e, s, P, P_{pub}, H_1, H_2)$.
- *Extract:* For the given public identity $ID \in \{0,1\}^*$,of the user, PKG computes the users public key $Q_{ID} = H_1(ID)$ and his secret key $S_{ID} = sQ_{ID}$.
- *Signing:* Given a private key S_{ID} and a message $M \in \{0,1\}^*$, choose a $r \in Z^*q$ and calculate:

$$U = rQ_{ID}$$
$$h = H_2(m, U)$$
$$V = (r + h)S_{ID}$$

  Signature $S = \{U, V\} \in G_1 \times G_1$.
- *Verification:* The signature $s = \{U, V\}$ of an identity ID on a message M is valid if the following equation holds.

$$e(P, V) = e(P_{pub}, U + hQ_{ID})$$

Z. HUANG ET AL SCHEME [7]

- *Key Generation:* The PKG chooses $s \in (Z/q)$ as his master secret key and computes the global public key P_{pub} as sP. It then chooses a random Map-to-Point hash function $H_2: \{0,1\}^* \rightarrow G_1$ and another cryptographic hash function $H_1: \{0,1\}^* \times G_1 \rightarrow Zq^*$.
- Parameter Generation: All the parameters are set $(G_1, G_2, e, s, P, P_{pub}, H_1, H_2)$.
- *Extract:* For the given public identity $ID \in \{0,1\}$,of the user, PKG computes the users public key $Q_{ID} = H_2(ID)$ and his secret key $S_{ID} = sQ_{ID}$.
- *Signing:* The signer randomly chooses a $r \in Z_q^*$ and calculate:

$$R = e(P_{ID}, P_{pub})^r,$$
$$h = H_1(m, R)$$
$$V = (rh + 1)S_{ID}$$

  Signature $S = \{R, V\} \in G_2 \times G_1$.
- *Verification:* The signature s = {R, V} of an identity ID on a message m is valid if the following equation holds.

$$e(P, V) = R^h e(Q_{ID}, P_{pub})$$

IV. EFFICIENCY ANALYSIS

We compare all the undertaken ID-Based signature schemes. The implementation has been done on Linux systems with an Intel Core i3 CPU 2.13GHz and 6.00GB RAM. Pairing based cryptography (PBC) library [9] in C has been used for implementation. All schemes are different in the processes of user key generation, signature generation and the signature verification. So, it is worth of giving the efficiency comparison of all the undertaken schemes in terms of involved operations and time consumption in the phases of signature generation and the signature verification of the schemes. In some application

Table 1. Running time Comparison

Scheme	Sign	Verify	Signature Length
Paterson's scheme [3]	28.064	15.964	$\|G_1\| + \|G_1\|$
Hess' scheme [5]	25.798	3.799	$\|G_1\| + \|Z_q\|$
Sakai et al. Scheme [8]	19.533	22.530	$\|G_1\| + \|G_1\|$
Cha-Cheon's scheme [6]	19.919	16.400	$\|G_1\| + \|G_1\|$
Z Huang's scheme [7]	17.130	8.174	$\|G_2\| + \|G_1\|$

Communicational cost has same significant role as computation cost so, the table 1 depicts the signature length of each of the schemes with the consumed running time. The symbolic meaning of the operations has been given in the table 2. Table 3 depicts the involved operations only in the processes of signing and verification for each scheme as the private key generation process is almost same for all the schemes.

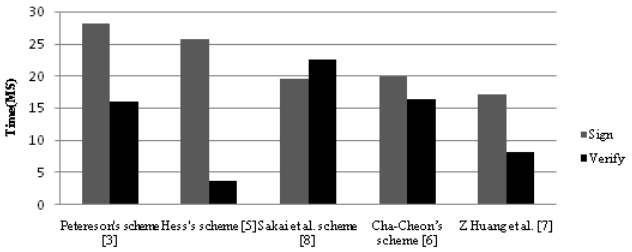

Fig. 1. Bar-chart for consumed running time

Table 2. Operation notation and its description

Notation	Description
τ_{po}	*Execution of a bilinear pairing operation*
τ_{inv}	*Execution of an inversion in* Z_n
τ_h	*Execution of a hash function*
τ_{p-add}	*Execution of an point addition in* G_1
τ_{squ}	*Execution of a square operation in* Z_n
τ_{cube}	*Execution of a cube operation in* Z_n
τ_{sm}	*Execution of scalar multiplication in* G_1
τ_{ec-add}	*Execution of a elliptic curve point addition* G_1
τ_{MTP}	*Execution of Map to point hash function*

Table3. Efficiency comparison in terms of involved operation

Algorithm	Hess's Scheme [5]	Paterson's Scheme[3]	Sakai et al. Scheme [8]	Cha-Cheon's Scheme [6]	Z Huang' Scheme[7]
Signing	$1\tau_h + 1\tau_{p-add} + 1\tau_{MTP} + 2\tau_{sm} + 1\tau_{squ} + 1\tau_{po}$	$2\tau_{sm} + 11\tau_{p-add} + 2\tau_{MTP} + 1\tau_{po} + 2\tau_h$	$1\tau_{p-add} + 2\tau_{sm}$	$1\tau_{MTP} + 2\tau_{sm} + 1\tau_{p-add}$	$1\tau_{po} + 2\tau_{sm} + 1\tau_{MTP} + 1\tau_{p-add}$
Verification	$1\tau_{sm} + 1\tau_{po} + 3\tau_{po}$	$2\tau_{MTP} + 3\tau_{sm} + 3\tau_{po}$	$1\tau_{sm} + 3\tau_{po}$	$1\tau_{MTP} + 1\tau_{p-add} + 1\tau_{sm} + 2\tau_{po}$	$1\tau_{po} + 1\tau_{sm} + 2\tau_{po}$

V. CONCLUSION

In our work, we have analysed all the undertaken established classical ID-Based signature schemes and observed that all the schemes are not efficient in terms of involved operations and consumed running time. All the schemes consumes same amount time/operations in the process of private key generation but totally different in the processes of signing and verification. So, it is always interesting to give a comparison study especially on signing and verification processes-which is done in the previous section. After analysing the generated signature length from different schemes, it is to be noted that except Z. Huang's scheme and Hess's scheme, all other schemes have same signature length. Hess's scheme produces a signature consisting of an element from the source group G_1 and another element from the set Z_q^* where the scheme proposed by Z. Huang et al. generates a signature consisting of two elements, one from the source group G_1 another from the target group G_2.

REFERENCES

[1] ANSI X9.62 and FIPS 186-2. Elliptic Curve Digital Signature Algorithm, 1998.
[2] Shamir A. Identity based cryptosystem and signature scheme. Lecture Notes in Computer Science, 1985, 196: 4753
[3] Paterson K G. ID-based signatures from pairings on elliptic curves. IEEE Electronic Letters, 2002, 38(18): 10251026.
[4] Boneh D, Franklin M. Identity based encryption from the Weil pairing. Lecture Notes in Computer Science, 2001, 2139: 213229
[5] Hess F. Efficient identity based signature scheme based on pairings. Lecture Notes in Computer Science, 2003, 2595: 310 324
[6] Cha J C, Cheon J H. An identity based signature from gap Diffie-Hellman groups. Lecture Notes in Computer Science, 2003, 2567: 1830
[7] Efficient Identity-Based Signatures and Blind Signatures Zhenjie Huang, Kefei Chen and Yumin Wang.
[8] R. Sakai, K. Ohgishi and M. Kasahara. Cryptosysytems based on pairing. In Proceedings of Symposium on Cryptography and Information Security, SCIS 2000, 2000.
[9] Lynn, Ben. "The pairing-based cryptography (PBC) library." (2010).
[10] Alfred J Menezes, Tatsuaki Okamoto, and Scott A Vanstone. Reducing elliptic curve logarithms to logarithms in a finite field. Information Theory, IEEE Transactions on, 39(5):1639–1646, 1993.
[11] Dan Boneh and Matt Franklin. Identity-based encryption from the weil pairing. In Advances in CryptologyCRYPTO 2001, pages 213–229. Springer, 2001.

Subhas Chandra Sahana was born at Bankura, India. He Received the B.Tech (bachelor degree) in Computer science and Engineering from Jalpaiguri Govt. Engineering College under West Bengal University of Technology. He got his M.Tech(IT) degree from Tezpur University , Assam. Currently He is Assistant Professor in the department of Information Technology.

Dr. Bubu Bhuyan was born in India. He received his M.Tech (IT) degree from Tezpur University , Assam. Currently he is Associate rofessor in the department of Information Technology.