ID-SS: A New Identity-Based Short Signature Scheme

Mehbub Alam, Subhas Chandra Sahana

Department of Computer Science and Engineering, Indian Institute of Information Technology, Guwahati
Department of Computer Science & Engineering, National Institute of Technology, Durgapur, India

Abstract: The conventional public-key cryptography (PKC) has to take the burden of certificate management; identity-based cryptography (IBC) eliminates the need for any certificate management activity as it deprives the usage of certificates completely. The user's publicly available unique entities such as a phone number, email-id, IP-address are considered as the public keys in identity-based cryptography. Apart from all the security services the digital signatures provide, the short signature is more popular because this scheme can generate a shorter signature differentiating other conventional digital signature schemes. The research community very rarely emphasises identity-based short signature schemes. However, adopting IBC for short signature strengthen the security paradigm is a worthy choice. We propose *ID-SS*, a short signature scheme based on identity-based cryptography. Assuming the Computational Diffie-Hellman Problem (CDHP) is an ungovernable problem, we claim our proposed scheme is secure. Experimental results and comparison with related work reflect the satisfactory performance of the proposed scheme.

Index Terms: Identity-Based Signature, Short Signature, Bilinear Pairing, CDHP, Key Generation Center.

1. Introduction

A digital signature is a crucial cryptographic primitive that provides data security to the users, which ensure the following: message authentication, message integrity and non-repudiation. The short signature scheme in identity-based cryptography is an interesting research topic as it merges the advantages of identity-based cryptography with short signature. Short signatures have many practical applications. The signature of a message needs to be transmitted over a channel with low bandwidth communication capability or stored in storage constraint devices. The association of public-key with the owner is carried out by issuing and signing the certificates by a trusted Certification Authority (CA) for authentication purposes in the traditional public-key cryptography. Consequently, managing all these generated certificates is really inefficient concerning the cost incurred in the computation and storage. The IBC removes the need for certificates to overcome the drawback of certificate generation and certificate management in public-key cryptography. The public-key is acquired from a user's distinctive identity parameters; thus, there is no need for a certificate to get a verified public key.

To overcome the difficulties faced by the traditional public-key cryptography, Shamir *et al.* [1] proposed a conventional scheme. This scheme brings the concept of acquiring user's verified public-key from their unique identification parameters. Resulting to the new feature, this new model omitted the burden of managing certificates as well as the use of CA, which was bound to take care of things such as certificate management and revocation. Until 2001, identity-based cryptography was a theoretical concept as there was not a practical implementation of it. With the use of bilinear pairing, Boneh *et al.* proposed an identity-based signature scheme [2] and implemented the scheme in 2001. Moreover, BLS signature was proposed by Boneh *et al.* [3]. The short

signature scheme in [3], is built based on the traditional public-key cryptography. Due to its various advantages, in recent years, several identity-based signature schemes [4], [5], [6], [1], [7] are proposed and widely investigated.

Proposing a short signature scheme in the identity-based cryptography is really a challenge for the researchers as the signature is triplet $< m, ID, \sigma_m, ID >$ here σ indicates the signature on the message m for the unique identification ID but in conventional PKI based system it is $< m, \sigma_m >$. After the pioneering work done by Boneh, several short signature schemes [8], [9], [10] fitted in the traditional PKI based system have been proposed. The generated signature from the BLS has half of the digital signature algorithm (320 bits) with alike security power. However, the proposed signatures in [11], [12], [13], [14], [15], [16] have approximately 320-bit size with the elliptic curve over the field F^{397}. Based on pairing, Du *et al.* [17] proposed an identity-based short signature scheme [17]. In this work, we also design an identity-based short signature scheme that is more computationally efficient in comparison to the existing scheme [17]. The rest of the paper is organized into six sections. In Section 2, we discuss essential preliminaries required. We explain the syntax of the signature generation model for the IBC in Section 3. In Section 4, we present our proposed *ID-SS* scheme. The efficiency analysis of the proposed scheme is presented in Section 5. Lastly, we conclude our work in Section 6.

2. Preliminaries

2.1. Bilinear Map and Related Complexity Assumption

- **Bilinear Map:** Let Gr_2 be a multiplicative group and Gr_1 be an additive group. Both the groups are of prime order p. Let P denote a generator of Gr_1 and e is computable map $e : Gr_1 \times Gr_1 \rightarrow Gr_2$ with the following properties:
  - Bilinear : $e(aP, bQ) = e(P, Q)^{ab}$ for all $P, Q \in Gr_1$; $a, b \in p$.
  - Non-degenerate: $e(P, P) \neq 1$.
  - The map e is efficiently computable.
- **Bilinear Diffie-Hellman Problem (BDHP):** For $a, b, c \in R, q$, given (P, aP, bP, cP), to compute $e(P, P)^{abc}$ is known as Bilinear Diffie-Hellman Problem.
- **Discrete Logarithm Problem (DLP):** For given $y, g \in =< p^*, >$, where g is the generator of the group . If $y = gx$ mod p then compute x for given prime p.
- **Decisional Diffie-Hellman Problem (DDHP):** For $a, b, c \in R, q^*$ given P, aP, bP, cP the problem is to decide whether $c = ab$ mod q. Using pairings, we can solve DDHP problem by a simple algorithm where bit operation complexity is polynomial.
- **Computational Diffie-Hellman problem (CDHP):** For $a, b \in R, q^*$, given P, aP, bP to compute abP is known as Computational Diffie-Hellman Problem.

3. Syntax of Signature Generation Model for Identity-Based signature Scheme

To create an identity-based signature scheme, it has included Signer, KGC, and Verifier.

1) **Signer:** It is involved in the process of signing the message.
2) **Private Key Generator (PKG):** the PKG generates the private key in the process. PKG is considered as the trusted authority that is responsible for authenticating the user's ID.
3) **Verifier:** It is responsible for verifying a message and taking the accept/reject decision.

In the creation of an identity-based signature scheme, the following four algorithms are associated: ***Setup, Extract, Signature Generation, and Signature Verification.*** In the following, a brief explanation of those components are discussed.

1) **Setup:** The PKG runs the setup algorithm to initial frame up an ID-Based system. We consider k as a security parameter; the algorithm returns the master secret key (MSK)

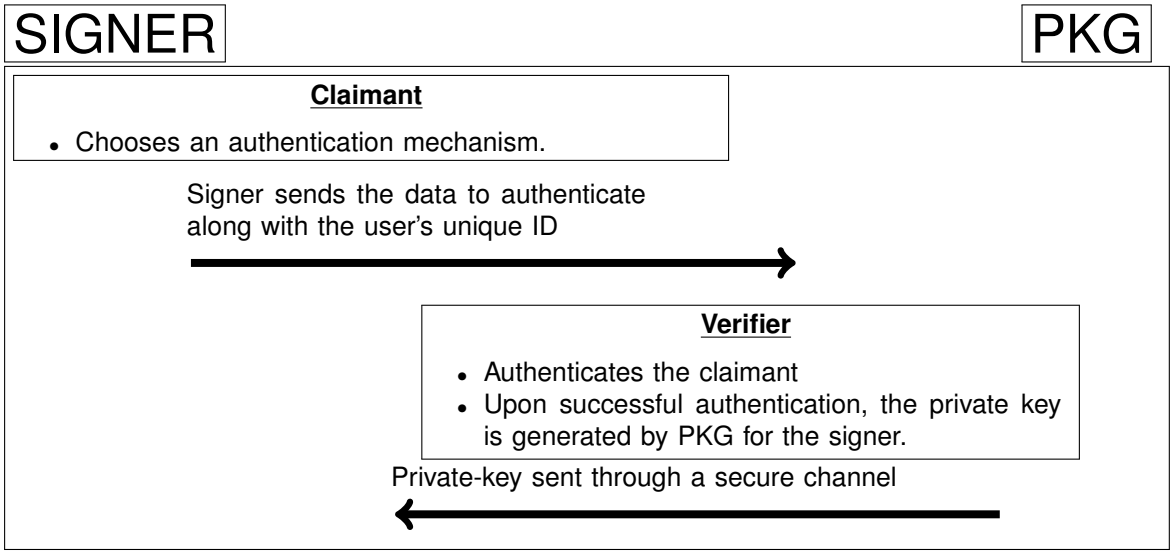

Fig. 1. Private key generation process for a signer in identity-based signature scheme

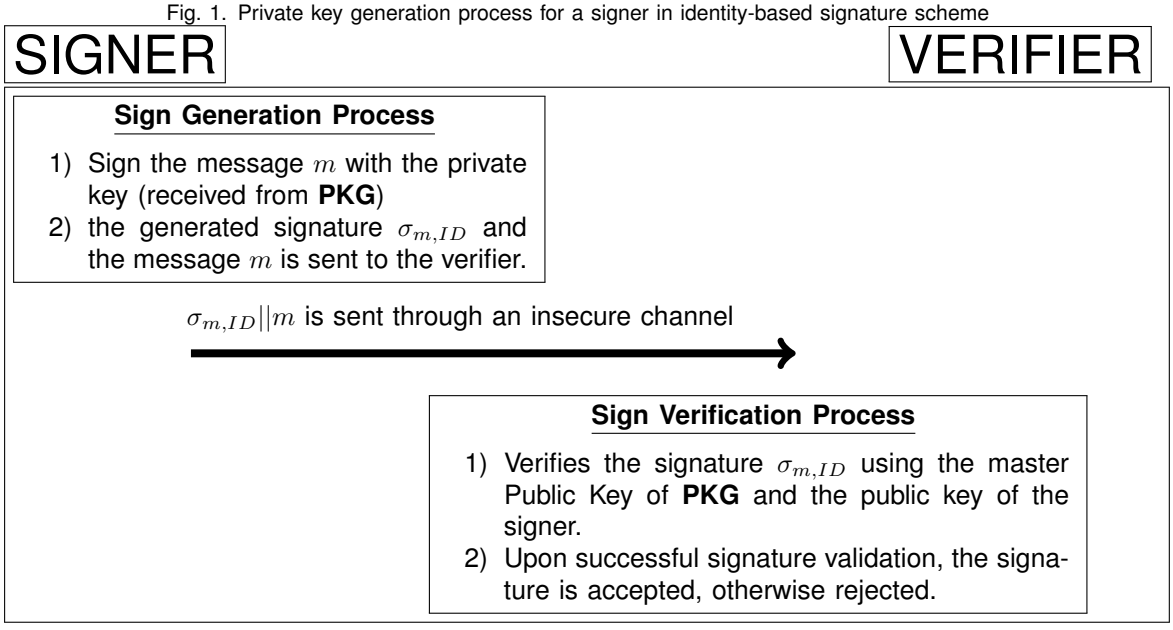

Fig. 2. Signing and verification of signature in IBS

and $params$. The $params$ are shared with the users, and the MSK is kept secret.

2) **Extract:** Upon receiving the user's identity parameter, the PKG executes the Extract algorithm. The PKG sent back the private keys. We showed the detailed process in Figure 1.
3) **Signature Generation:** In this algorithm, the signer who has received the private key from PKG signs the message m. The generated signature is expressed as $< \sigma_m, ID >$, where σ_m is the signature on the message m and ID is the user's identity parameter. The process is presented in Figure 2.
4) **Signature Verification:** In this process, the signature $< \sigma_m, ID >$ is verified by the verifier who holds the public ID of the user and the master public key from KGC (refer to Figure 2).

4. Proposed Identity-Based Short Signature Scheme: *ID-SS*

We present a novel identity-based short signature scheme in this section. The following four algorithms are the fundamentals of the *ID-SS* scheme.

1) **Setup:** We assume k as security parameter , the the key generation party PKG chooses Gr_1 and Gr_2, two groups belongs to the same prime order q. Moreover, it selects $e : Gr_1 \times Gr_1 \rightarrow Gr_2$, i.e, a Modified Weil Pairing Map. We represent P as a generator of the group Gr_1. Let $g = e(P, P)$, then the PKG chooses cryptographic hash functions H_1, and H_2, where $H_1 : \{0,1\}^* \rightarrow Z_p^*$ and $H_2 : \{0,1\}^* \times Gr_1 \rightarrow Z_p^*$.
   A master secret key (msk) is chosen randomly by the PKG and accordingly computes the master public key as $P_{pub} = y.P \in Gr_1$.

   (Gr_1's generator is P). **PKG** publishes $(Gr_1, Gr_2, e, Hsh_1, Hsh_2, P, g, P_{pub},)$ while y is stored secret.
2) **Extract:** Assuming an identity $ID \in (0,1)^*$ and master secret key $msk = y$, PKG computes the following.
   a) $PK_{ID} = Hsh_1(ID)$, here PK_{ID} is the public key belongs the user.
   b) The user's private key $SK_{ID} = (\frac{1}{(y+PK_{ID})}).P$
   c) A public parameter $E_{ID} = P_{pub} + PK_{ID}.P$
   PKG finishes the calculation of 1), 2) and 3), following by generating a private key as SK_{ID}. Then the SK_{ID} along with the public ID is sent through a secure channel.
3) **Signature Generation:** For the signature generation, the signer of the message m selects a random number r and computes the public parameter W as follows:

$$W = r.Q = r(P_{pub} + PK_{ID}.P), r \in Z_q^*$$

   W is broadcast to all the users and r is kept secret. The signer of the message generates a signature σ_m on the message m for an identity ID by performing the following calculations:
   a) Calculates $h = H_2(m, E_{ID})$
   b) Signature
   $\sigma = e(\frac{1}{r.h(y+PK_{ID})})P$
   and $QID = Hsh_2(ID)$

   After generating the signature, $< m, ID, \sigma >$ is the signature tuple sent to the verifier.
4) **Signature Verification:** Now the verifier receives a signature σ that is signed on the message m on the public ID of a user. The verifier verifies the received signature. The verifier checks the equation $e(\sigma, h, W) = e(P, P)$ holds or not.
5) **Correctness:** The verification algorithm checks the correctness of the algorithm as computed below:
   $e(\sigma, h.W)$
   $= e(\frac{1}{r.h(y+PK_{ID})}.P, h.W)$
   $= e(\frac{1}{r.h(y+PK_{ID})}.P, h.r(P_{pub} + PK_{ID}.P))$
   $= e(\frac{1}{r.h(y+PK_{ID})}.P, h.r(y.P + PK_{ID}.P))$
   $= e(\frac{1}{r.h(y+PK_{ID})}.P, h.rP(y + PK_{ID}))$
   $= e(P, P)$

5. Efficiency Comparison

In this section, we provide the efficiency analysis with the only existing similar scheme [17].

Both the schemes are similar in Setup and Extract algorithms. However, they are totally different in the SignGen (signature generation) algorithm as well as SignVeri (signature verification) algorithm. We provide the comparative efficiency analysis in the Signature Generation and Signature

TABLE I
NOTATION TABLE

Notation	Description
S_M	Scalar multiplication operation
H	Cryptographic Hash function operation such as MD5 or SHA-1
INV	Inverse operation in Z_q^*.
P_{ADD}	Point addition
PO	Pairing
$\|G_1\|$	Size of an element in the source group G_1 used in pairing operation
ADD	Addition operation between two elements in the set Z_q^*
MUL	Multiplication operation between two elements in the set Z_q^*

TABLE II
EFFICIENCY COMPARISON OF *ID-SS* WITH AN EXISTING ESTABLISHED SCHEME

Scheme	**Du et al.** [17]	**Proposed *ID-SS* Scheme**
Sign	$1H + 1INV + 1SM + 1ADD$	$1H + 1INV + 1SM + 1MUL$
Verify	$1H + 1PO + 1SM + 1P_{ADD}$	$1H + 1PO + 1SM$
Signature Size	$\|G_1\|$	$\|G_1\|$

Verification processes of both the schemes. The different notations used for efficiency analysis are given in Table I. The efficiency comparison of both the schemes in terms of involved operations in the process of SignGen and SignVeri are shown in Table II. From Table II, we draw the conclusion that our proposed scheme and the compared scheme both generates the same size of the signature. This represents that the size of a single element from the source group Gr_1. Moreover, in these schemes, the involved operations in the SignGen process are common except that the short signature scheme in the compared scheme and our proposed *ID-SS* scheme appends one addition operation in the set Z_q^* and one multiplication operation in the set Z_q^* respectively. It is also observed that our scheme is more computationally efficient in the SignVeri process as the compared scheme needs one extra addition operation in the group Gr_1. If we take the elliptic curve group for implementation of the Gr_1 group, then one extra point addition operation is needed.

We implement the proposed *ID-SS* scheme and the compared scheme on a Linux system with

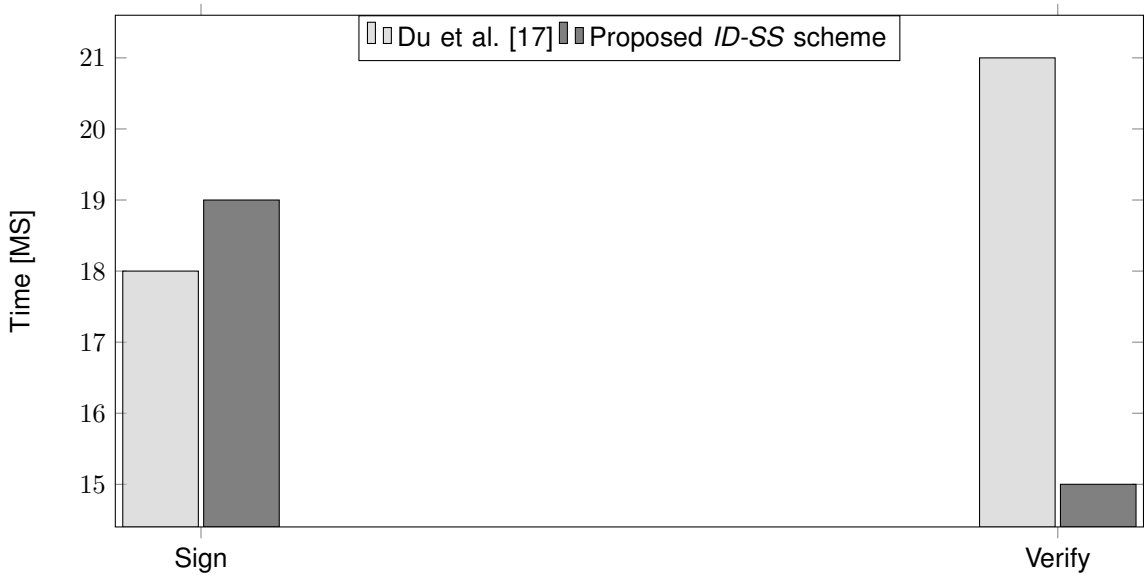

Fig. 3. Comparison of the running time in Sign and Verify

TABLE III
EXECUTION TIME EFFICIENCY OF *ID-SS* SCHEME WITH DU ET AL. [17]

Scheme	Du et al. [17]	Proposed *ID-SS* scheme
Signing	18 ns	19 ns
Verifying	21 ns	15 ns

system configuration with Intel Core i3 CPU, 2.30GHz with 4 GB RAM using PBC (Pairing Based Cryptography) library package installed in the Linux machine. We used C language to implement the short signature schemes. Moreover, we have compared the *ID-SS* scheme with Du et al. [17] in terms of running time taken in SignGen and SignVeri processes. It can be observed from Table III that the verification process of our proposed scheme takes less operational time in comparison to the other scheme. The graphical representation from the achieved results has been shown in Figure 3.

6. Conclusion

In this paper, we proposed *ID-SS*, a digital signature scheme that is shorter in size and holds identity-based characteristics. However, short signatures upholding the identity-based cryptosystem concept is very rare in the literature. Under the assumption of CDHP that it is an ungovernable problem, the proposed signature scheme is secure. The signature length of the generated short signature by our proposed scheme is the length of one element of the source group used in the pairing operation. We addressed the efficiency comparison of the proposed scheme with a comparable exiting scheme, and, remarkably, our scheme is computationally more efficient in the signature verification process, unlike in compared scheme takes additional point addition operation is involved in the process.

References

[1] A. Shamir, "Identity-based cryptosystems and signature schemes," in *Workshop on the theory and application of cryptographic techniques*. Springer, 1984, pp. 47–53.

[2] D. Boneh, C. Gentry, B. Lynn, and H. Shacham, "Aggregate and verifiably encrypted signatures from bilinear maps," in *International conference on the theory and applications of cryptographic techniques*. Springer, 2003, pp. 416–432.

[3] D. Boneh, B. Lynn, and H. Shacham, "Short signatures from the weil pairing," *Journal of cryptology*, vol. 17, no. 4, pp. 297–319, 2004.

[4] F. Zhang, R. Safavi-Naini, and W. Susilo, "An efficient signature scheme from bilinear pairings and its applications," in *International Workshop on Public Key Cryptography*. Springer, 2004, pp. 277–290.

[5] Y. Gao, P. Zeng, K.-K. R. Choo, and F. Song, "An improved online/offline identity-based signature scheme for wsns." *Int. J. Netw. Secur.*, vol. 18, no. 6, pp. 1143–1151, 2016.

[6] M. Dugardin, A. Facon, S. Guilley, X.-T. Ngo, and K. Lorvellec, "A new fair identity based encryption scheme," in *2019 3rd International Conference on Recent Advances in Signal Processing, Telecommunications & Computing (SigTelCom)*. IEEE, 2019, pp. 85–89.

[7] J. Chen, J. Ling, J. Ning, and J. Ding, "Identity-based signature schemes for multivariate public key cryptosystems," *The Computer Journal*, vol. 62, no. 8, pp. 1132–1147, 2019.

[8] R. Yaduvanshi and S. Mishra, "An efficient and secure pairing free short id-based signature scheme over elliptic curve," in *Proceedings of 2nd International Conference on Advanced Computing and Software Engineering (ICACSE)*, 2019.

[9] P. S. Barreto, B. Libert, N. McCullagh, and J.-J. Quisquater, "Efficient and provably-secure identity-based signatures and signcryption from bilinear maps," in *International conference on the theory and application of cryptology and information security*. Springer, 2005, pp. 515–532.

[10] R. A. Sahu and S. Padhye, "Provable secure identity-based multi-proxy signature scheme," *International Journal of Communication Systems*, vol. 28, no. 3, pp. 497–512, 2015.

[11] J. C. Choon and J. H. Cheon, "An identity-based signature from gap diffie-hellman groups," in *International workshop on public key cryptography*. Springer, 2003, pp. 18–30.

[12] K. G. Paterson, "Id-based signatures from pairings on elliptic curves," *Electronics Letters*, vol. 38, no. 18, pp. 1025–1026, 2002.

[13] K. G. Paterson and J. C. Schuldt, "Efficient identity-based signatures secure in the standard model," in *Australasian conference on information security and privacy*. Springer, 2006, pp. 207–222.

[14] J.-L. Tsai, "A new efficient certificateless short signature scheme using bilinear pairings," *IEEE Systems Journal*, vol. 11, no. 4, pp. 2395–2402, 2015.

[15] D. Boneh and M. Franklin, “Identity-based encryption from the weil pairing,” *SIAM journal on computing*, vol. 32, no. 3, pp. 586–615, 2003.
[16] X. Chen, F. Zhang, and K. Kim, “A new id-based group signature scheme from bilinear pairings.” *IACR Cryptol. ePrint Arch.*, vol. 2003, p. 116, 2003.
[17] H. Du and Q. Wen, “An efficient identity-based short signature scheme from bilinear pairings,” in *2007 International Conference on Computational Intelligence and Security (CIS 2007)*. IEEE, 2007, pp. 725–729.