

Efficient Identity-Based Parallel Key-Insulated Signature Scheme using Pairings over Elliptic Curves

R B Amarapu^{1*} and P V Reddy²

¹Department of Engineering Mathematics, ANITS (A), Sangivalasa, Visakhapatnam, AP, India

²Department of Engineering Mathematics, AUCE (A), Andhra University, Visakhapatnam, AP, India

Received 22 November 2016; revised 22 August 2017; accepted 03 November 2017

Many cryptographic schemes were designed under the assumption that the private keys involved in the system are perfectly secure. If the private key of a signer is exposed then security of the system is totally lost. Key-insulation mechanism minimizes the damage caused by the exposure of private keys in cryptographic schemes. To deal with the key-exposure problem in ID-based schemes, private keys have to be updated at very short intervals; but it will increase the risk of helper key exposure. In order to improve the security and efficiency of key insulation mechanism in ID-based signatures, in this paper, we proposed an ID-based parallel key insulated signature scheme. This scheme uses the bilinear pairings over elliptic curves and is provably secure in the ROM model with the assumption that the CDH problem is intractable. This scheme is strong key-insulated and allows frequent key updates without increasing the risk of helper key exposure and hence improve the security of the system. Also our IDPKIS Scheme reduces the computational, communicational complexity and hence the scheme can be deployed on inexpensive, lightweight and mobile devices.

Keywords: Signature Schemes, Key exposure Problem, Key-Insulation, Elliptic Curves, CDH Problem

Introduction

Motivated by the concept of the IBC, many ID-based schemes were designed under the assumption that the private keys involved in the system are perfectly secure. In a signature scheme, if the private key of a signer is exposed then security of the system is totally lost. To deal with this key-exposure problem, in 2002, Dodis *et al.*¹ developed the concept of key-insulated mechanism with an idea by dividing the total life span of the master private key into discrete time periods and user updates their temporary key to encrypt some message in a time period. In 2003, Dodis *et al.*² proposed key-insulated signature scheme and then many efforts have been devoted to development of new the key-insulated schemes both in PKI and ID-based settings³⁻⁸. In 2006, Hanaoka *et al.*⁹ and proposed a parallel key-insulated encryption (IDPKIE) scheme with two distinct helpers which are alternately used to update the secret keys. In the same year 2006, Weng *et al.*¹⁰ proposed an IDPKIE and signature schemes (IDPKIS). In 2008, Weng *et al.*¹¹ proposed IDPKIS scheme using pairings over elliptic curves. In order to reduce the computational and communicational complexity in key insulated schemes, in this paper, we

proposed an ID-based parallel key-insulated signature scheme (IDPKIS). We prove the security of our scheme under random oracle paradigm without using the Forking lemma and hence the security is tightly connected to the CDH problem¹². We compare our scheme with Zhou *et al.* scheme³ and Weng *et al.* scheme¹¹.

Preliminaries

In this section we briefly review bilinear parings and computational Diffie-Hellman problem which will be used for the construction and security analysis of our scheme.

Bilinear Map

Let $(G_a, +)$ and $(G_m, \cdot)$ are two cyclic groups of same prime order q with P as a generator in G_a . A bilinear pairing is a map $\hat{e} : G_a \times G_a \rightarrow G_m$ which satisfy the following.

- *Bilinear:* $\forall P, Q \in G_a$ and $\forall x, y \in \mathbb{Z}_q^*$, $\hat{e}(xP, yQ) = \hat{e}(P, Q)^{xy}$
- *Non-Degeneracy:* $\exists P \in G_a, \exists \hat{e}(P, P) \neq 1$.
- *Computable:* $\forall P, Q \in G_a, \hat{e}(P, Q)$ can be calculable using an efficient algorithm.

Upon making suitable variations in the Weil or Tate pairing one can obtain such maps on elliptic curves that are defined on a finite field^{13, 14}.

*Author for Correspondence
E-mail: rameshamarapu.maths@anits.edu.in

Computational Diffie-Hellman (CDH) Problem

For a given tuple $(P, xP, yP) \in G_a^3$ and anonymous $x, y \in Z_q^*$ the CDH problem in G_a is to compute $xyP \in G_a$. The advantage of a Probabilistic Polynomial Time (PPT) algorithm $\mathcal{A}$ in obtaining the solution of the CDH problem in G_a is $Adv_A^{CDH} = \Pr[A(P, xP, yP) = xyP/x, y \in Z_q^*]$. The CDH assumption assures that for any PPT algorithm $\mathcal{A}$ Adv_A^{CDH} is negligible.

Syntax of IDPKIS scheme

In this section we present the syntax of our IDPKIS scheme. The lifetime of IDPKIS systems is divided into discrete time periods. The public key of a user is his/her identity and is fixed for all the lifetime, while his secret key is updated in every time period. Every user ID has two helpers which store hsk_1, hsk_0 . The two helper keys are alternately used to update user's secret/private keys i.e. hsk_1 is used in odd time periods while hsk_0 is used for even time periods. At time period t , user ID obtains an update key $HSK_{ID,t}$ from the j^{th} helper (here $j \equiv t(mod 2)$). Combining $HSK_{ID,t}$ with the private key $d_{ID,t-1}$ for the previous time period; he can derive the private key $d_{ID,t}$ for the current time period and $d_{ID,t}$ is used to sign a message during the corresponding time period without further access to the helpers. Moreover, due to the fact that hsk_1 and hsk_0 are alternately used, the risk of key exposure for hsk_1 or hsk_0 will not be increased, even if this user's key-updates frequency is doubled. Concretely, an IDPKIS scheme consists of the following five polynomial-time algorithms.

- **System Setup:** This algorithm run by the PKG by taking input a security parameters k and (possibly) a total number of time periods N , outputs a public parameter $params$ and a master key msk .
- **Extract/Initial Private Key Generation:** This algorithm run by the PKG by taking input msk , $params$ and a user's identity $ID \in \{0, 1\}^*$ outputs an initial private key $d_{ID,0}$ and two helper keys hsk_1, hsk_0 .
- **Key Update:** This consists of two deterministic algorithms. One is run by user helpers, the other is run by user.

Helper key update: This algorithm run by the user's helpers by taking as input a time period index t , a user's Identity ID and the j^{th} helper key with $j \equiv t(mod 2)$, returns an update key $HSK_{ID,t}$.

User key update: This algorithm run by the user by taking input a time period index t , a user's identity

ID , a private key $d_{ID,t-1}$ and an update key $HSK_{ID,t}$ returns a private key $d_{ID,t}$.

- **Signature Generation:** The signing algorithm takes input a time period index t , a message m and a private key $d_{ID,t}$; outputs $\sigma = (U, V, t)$ composed of the time period t and a signature σ .
- **Signature Verification:** The verification algorithm, on input a candidate signature (t, σ) on m and the user's identity ID outputs 1 if (t, σ) is a valid signature, and 0 otherwise.

Proposed IDPKIS scheme

The proposed IDPKIS scheme consists of five polynomial time algorithms and the detailed functionalities of these algorithms are presented as follows.

- **System Setup:** This algorithm run by the PKG takes a security parameter $l \in Z^+$ and proceed as follows:

Generate two cyclic groups G_a under addition and G_m under multiplication respectively of same prime order $q \geq 2^l$, with P as a generator of G_a . Generate a Bilinear map $\hat{e}: G_a \times G_a \rightarrow G_m$. Picks cryptographic hash functions $H_1, H_2: \{0,1\}^* \rightarrow G_a$, $H_3: \{0,1\}^* \times G_m \rightarrow Z_q^*$. Picks random integers and computes $P_{pub} = sP$, $P_{hlp_1} = hsk_1P$, $P_{hlp_0} = hsk_0P$. Also computes $g = \hat{e}(P_{pub}, P)$. Here P_{pub} is the system overall public key, P_{hlp_0} and P_{hlp_1} are public keys of the helpers 0 and 1 respectively.

Publishes the system parameters as $PP = \langle G_a, G_m, q, P, \hat{e}, H_1, H_2, H_3, P_{pub}, P_{hlp_1}, P_{hlp_0}, g \rangle$ and keeps the system's master private key s , the helpers private keys hsk_1, hsk_0 with itself securely.

- **Initial Private key Generation:** Upon receiving user's identity $ID \in \{0, 1\}^*$, the PKG computes $d_{ID,0}$ as

$$d_{ID,0} = sH_1(ID) + hsk_j H_2(ID, -1) + hsk_j H_2(ID, 0) \dots (1)$$

PKG sends $d_{ID,0}$ as the initial private key for the user ID .

- **Key Update:** This algorithm consists of two deterministic algorithms.

Helper key update: Given an identity $ID \in \{0, 1\}^*$ and a time period index t , the j^{th} (here $j \equiv t(mod 2)$) helper computes $HSK_{ID,j} = hsk_j[H_2(ID, t) - H_2(ID, t-2)]$ and sends to user ID .

User key update: Given an identity $ID \in \{0, 1\}^*$ a time period index t , an update key $HSK_{ID,t}$ and the

private key $d_{ID,t-1}$ for the previous time period, user ID computes $d_{ID,t} = d_{ID,t-1} + HSK_{ID,t}$ as the private key for time period t . Finally the user erases two values $d_{ID,t-1}$ and $HSK_{ID,t}$. Note that the $j \equiv t(mod 2), j' \equiv (t-1)(mod 2)$ then the following equality always holds

$$d_{ID,t} = sH_1(ID) + hsk_j \cdot H_2(ID, t-1) + hsk_j H_2(ID, t) \quad \dots (2)$$

- **Signature Generation:** In time period t , for a given message M and the private key $d_{ID,t}$, the user ID chooses $r \in Z_q^*$ and computes $U = g^r, h = H_3(ID, M, U, t), V = hd_{ID,t} + rP_{pub}$. The signature on M in time period t generated by ID is $\sigma = (U, V, t)$.
- **Signature Verification:** Given a signature σ on a message M and identity ID , any one can verify this signature as follows: Let $j \equiv t(mod 2), j' \equiv (t-1)(mod 2)$: Compute $h = H_3(ID, M, U, t)$; return 1 if the following equality (3) holds; otherwise it returns 0.

$$\hat{e}(P, V) = \hat{e}(P_{pub}, hH_1(ID)) \hat{e}(P_{hsk_j}, hH_2(ID, t-1)) \hat{e}(hsk_j, hH_2(ID, t))U \quad \dots (3)$$

Analysis of the proposed idpkis scheme

Proof of correctness

Theorem 1

The proposed IDPKIS scheme satisfies the proof of correctness

Proof: The proof of correctness of the scheme is justified by verifying the validity of the equation (3).

$$\begin{aligned} \hat{e}(P, V) &= \hat{e}(P, hd_{ID,t} + rP_{pub}) \\ &= \hat{e}(P_{pub}, hH_2(ID)) \hat{e}(P_{hsk_j}, hH_2(ID, t-1)) \hat{e}(P_{hsk_j}, hH_2(ID, t))U \end{aligned}$$

Security Analysis

Theorem 2

In the random oracle model, the proposed IDPKIS scheme is strong key-insulated and is existential unforgeable against adaptive chosen message and identity attacks on the feasibility assumption of the CDH problem.

Proof: We will show how to construct an algorithm $\mathcal{B}$ against the CDH assumption in group G_a . Suppose $\mathcal{B}$ is given a CDH instance $(P, aP, bP) \in G_m^3$. $\mathcal{B}$'s goal is to derive abP with the help of adversary $\mathcal{A}$. $\mathcal{B}$ plays the role of $\mathcal{A}$'s challenger and works by interacting with $\mathcal{A}$ in a unforgeable under adaptively chosen message and ID- attack game as follows:

Setup: Algorithm $\mathcal{B}$ sets $P_{pub} = aP$ and gives the public parameters PP to $\mathcal{A}$. Note that the master key is implicitly assigned to be on $msk = a$ which is unknown to $\mathcal{B}$.

Queries: Algorithm $\mathcal{B}$ responds to a series of queries made by $\mathcal{A}$ adaptively as follows.

H_1 - queries: When $\mathcal{A}$ Queries the H_1 oracle at a point $ID \in \{0, 1\}^*$ algorithm $\mathcal{B}$ maintains a H_1 - list of tuples (ID, x, y, v) and responds to $\mathcal{A}$ as given below.

- If the queried ID already appears on the H_1 -list in a tuple (ID, x, y, v) then $\mathcal{B}$ responds with previously defined value as $H_1(ID) = v \in G_a$.
- Otherwise, $\mathcal{B}$ picks $y \in \{0, 1\}^*$, that yields 0 with probability μ and 1 with probability $1 - \mu$.
- If $y = 0$ then $\mathcal{B}$ picks a random value $x \in Z_q^*$ and computes $H_1(ID) = v = x(bP)$, else $H_1(ID) = v = xP$.

$\mathcal{B}$ adds the tuple (ID, x, y, v) to the H_1 -list and responds to $\mathcal{A}$ with $H_1(ID) = v \in G_a$.

H_2 - queries: $\mathcal{B}$ maintains a H_2 -list which is initially empty. When $\mathcal{A}$ queries the tuple (ID, t) , $\mathcal{B}$ first checks whether H_2 -list contains a tuple for this input. If it does, the previously defined value is returned. Otherwise, $\mathcal{B}$ chooses a random integer $w \in Z_q^*$ and computes the hash value $H_2(ID, t) = wP \in G_a$ and then stores the tuple (ID, t, w, wP) in the H_2 -list.

H_3 - queries: : At any time $\mathcal{A}$ queries the oracle H_3 at (ID, M, U, t) . $\mathcal{B}$ maintains a list referred as H_3 - list of tuples (ID, M, U, t, v') and responds to $\mathcal{A}$ as given below. If the queried tuple (ID, M, U, t) already appears in the H_3 - list in a tuple (ID, M, U, t, v') then $\mathcal{B}$ responds with $H_3(ID, M, U, t) = v' \in Z_q^*$. Otherwise, $\mathcal{B}$ picks a random $v' \in Z_q^*$ and adds the tuple (ID, M, U, t, v') in the H_3 - list and responds to $\mathcal{A}$ with $H_3(ID, M, U, t) = v' \in Z_q^*$.

Signature queries: When $\mathcal{A}$ queries a signature on a message M for an identity ID of a user in a time period t , $\mathcal{B}$ does the following.

- Chooses a random integer $k \in Z_q^*$ and computes $U = g^k$.
- If the tuple (ID, M, U, t, v') in the H_3 – list, $\mathcal{B}$ chooses $v'' \in Z_q^*$ and tries again. Otherwise, $\mathcal{B}$ computes $V = v'(xP_{pub} + w_1P_{hl} + w_0P_{hlp}) + kP_{pub}$ and stores in the H_3 – list and responds to a with $\sigma = (U, V)$ as the Queried signature. All responds to sign Queries are valid; indeed, the output (U, V) is a valid signature on M under ID .

Forgery: Finally, $\mathcal{A}$ output a forgeable signature (U^*, V^*) on a message M^* for an identity ID^* of a user in a time period t^* . $\mathcal{B}$ finds the tuple (ID, x^*, y^*, v^*) from the H_1 –list and proceeds only if $y^* = 0$; since $y = 0$, it follows that $H_1(ID) = x^*(bp)$. If succeeds in this game, then we have the following.

$$\hat{e}(P, V^*) = \hat{e}\left(P, v^* x^*(abP)\right) + w_j^* P_{hlp_1} + w_j^* P_{hl_0} + k^* P_{pub}$$

From this, $\mathcal{B}$ can derive abP as $(x^*)^{-1} (v^*)^{-1} [V^* - w_j^* P_{hlp_1} - w_j^* P_{hl_0} - k^* P_{pub}]$ and solve the CDH instance successfully. But the CDHP is computationally infeasible by any polynomial-time bounded algorithm. Therefore, based on the intractability of CDHP, our scheme is provable secure and strong key insulated secure in the random oracle model against the adaptive chosen message and identity attacks.

Efficiency analysis

We present the efficiency analysis of our scheme by comparing it with the related and existing IDPKIS scheme in terms of computation and communicational point of view. For comparison, we consider point addition in G_a as AD , scalar multiplication in G_a as SM , exponentiation in G_m as EX , hash functions as H and computation of bilinear pairing (BP). The following Table 1 gives the comparison of our scheme with Weng *et al.* scheme¹¹. In the pairing-based signature schemes, the pairing operation is the most time-consuming compared with the other operations

Table1 — Comparison with Weng *et. al* scheme

Scheme	Computational cost for Signature Generation	Computational cost for Signature verification.	Communication cost (Signature Size)
Weng. <i>et.al</i> [11]	1 EX + 2 SM + 1 H + 1 AD	4 H + 5 BP	$ 4G_a $
Ours	1 EX + 2 SM + 1 H + 1 AD	3 SM + 4 H + 4 BP	$ 2G_a $

like addition and hash functions etc. Despite a number of attempts to reduce the complexity in evaluation of pairing operation, still the operation is very costly^{13, 14}. From the Table 1, it is clear that our scheme requires 4 pairing operations whereas Weng *et al.* scheme¹¹ requires 5 Pairing operations which means that the computational complexity of our scheme is less than Weng *et al.* scheme¹¹. Also, the proposed scheme has $2|G_a|$ as signature length whereas Weng *et al.*¹¹ scheme has $4|G_a|$ as signature length and hence the communicational efficiency is improved greatly than Weng *et al.* scheme¹¹.

Conclusions

In this paper, we presented a new IDPKIS scheme to deal with key exposure problem in ID-based signatures. The proposed scheme is provable secure and strong key insulated. Also this scheme allows frequent key-updates without increasing the risk of helper key-exposure, hence enhances the security of the system. The proposed scheme requires less number of pairing operations and has the signature size is less than the existing schemes. Thus the proposed IDPKIS scheme is efficient in terms of computation and communication point of view. The security of our scheme is proved under random oracle paradigm without using the Forking lemma and hence the security of the scheme is tightly connected to the CDH problem. Further, as a future work, we extend our scheme to construct a PKIS scheme with multiple helper keys to increase simultaneously the security of both helper keys and user's without significant loss of efficiency.

References

- 1 Dodis Y, Katz J, Xu S & Yung M, Key-insulated public key cryptosystems, *Advances in Cryptology*, EUROCRYPT'03, LNCS, **2332**(2002), 65-82.
- 2 Dodis Y, Katz J & Xu S and Yung M, Strong key-insulated signature schemes, LNCS, **2567**(2003), 130-144.
- 3 Zhou Y, Cao Z, & Chai Z, ID- based key-insulated signature, in *Proc ISPEC 2006*, LNCS, **3903** (2006), 226-234.
- 4 Tsu-yang Wu, Yuh-Min Tseng & Ching-Wen Yu, ID-based key-insulated signature scheme with batch verifications and its novel application, *Int J Inno, Comp, Inf and Con*, **87**(2012), 4797-4810.
- 5 Zhao H, Duan S, Cheng X, & Hhao R, Key-insulated aggregate signature, *Front Cmput Sci*, **8(5)** (2014), 837–846.
- 6 Gopal P V S S N & V Reddy P, Efficient ID-based key-insulated signature scheme with batch verifications using bilinear pairings over elliptic curves, *J Discrete Math Sci and Cryp*, T & F, **18(4)** (2015), 385-402.
- 7 Li J, Du H & Zhang Y, Certificate-based key-insulated signature in the standard model, *Security in Comp Sys and Net, Com J*, **2**(2016), 1-12.

- 8 Rao Y S & Dutta R, Attribute-based key-insulated signature for boolean formula, *Int J Comp Math*, T & F, **93(6)** (2016), 864–888.
- 9 Hanaoka G, Hanaoka & Imai H, Parallel key-insulated public key encryption, *Proc PKC 06*, LNCS **3958** (2006), 105-122.
- 10 Weng J, Liu S, Chen K & MA C, Identity based parallel key-insulated encryption without random oracles security notions and construction, *Proc INDOCRYPT 06*, LNCS, **4329** (2006), 409-423.
- 11 Weng J, Liu S & Chen K., Identity based parallel key-insulated signature: Frame work and Construction, *J Res and Pract in Info Tech*, **40(1)** (2008), 55-68.
- 12 Hofheinz D & Jager T. Tightly secure signatures and PKE, *J Designs, Codes and cryptography*, **80(1)** (2016), 29-61.
- 13 IEEE Standard for identity-based Cryptographic techniques using pairing. IEEE Std:1363.3-2013 (2013), 1-151.
- 14 Enge A & Milan A, Implementing cryptographic pairings at Standard Security levels, *SPACE-2014*, LNCS, **8804** (2014), 28-46.