

# An Efficient ID- based Directed Signature Scheme from Bilinear Pairings

<sup>1</sup>B. Umapasada Rao,

<sup>1</sup>P. Vasudeva Reddy,

<sup>2</sup>T. Gowri

1. *Department of Engineering Mathematics, Andhra University, Visakhapatnam, A.P, India.*
  2. *Department of Electronics and communication Engineering, ASCET, Gudur, A.P, India.*
- 

## Abstract:

A directed signature scheme allows a designated verifier to directly verify a signature issued to him, and a third party to check the signature validity with the help of the signer or the designated verifier as well. Directed signatures are applicable where the signed message is sensitive to the signature receiver. Due to its merits, directed signature schemes are suitable for applications such as bill of tax and bill of health. In this paper, we proposed efficient identity based directed signature scheme from bilinear pairings. Our scheme is efficient than the existing directed signature schemes. In the random oracle model, our scheme is unforgeable under the Computational Diffie-Hellman (CDH) assumption, and invisible under the Decisional Bilinear Diffie-Hellman (DBDH).

## Keywords:

Directed signature, ID-based cryptography, CDH problem, DBDH problem.

## Introduction:

Digital signature is one of the most important techniques in the modern information security system for its functionality of providing data integrity and authentication. In ordinary digital signature schemes, any one can verify the validity of a signature with signer's public key. However, in some scenarios, it is not necessary for any one to be convinced a validity of signer's confidential message, since the signed

message may contain a confidential agreement or a private information between the signer and the recipient. For example, signatures on medical records, tax information and most business transactions. To address this problem, Chaum and Van Antwerpen [6] introduced the concept of undeniable signatures. In an undeniable signature scheme, one party can verify a signature only by interaction with the legitimate signer through a conformation protocol. Therefore the signer can control when and by whom his signatures can be verified. Because undeniable signatures have various applications in the security of e-commerce, such as licensing software, auction and electronic voting, many variants of undeniable signature appear, such as FDH undeniable signature [6] and threshold undeniable signatures[17,18] are only verified with the cooperation of the signer. It is very inconvenient and impractical in real life. As an alternative approach to undeniable signatures, designated confirmer signatures [5] was proposed by Chaum in 1994. In this scheme a designated confirmer signatures allows certain designated parties to confirm the authenticity of a document with out the need for the signer's input. At the same time many signature types with controlled verifiability are proposed, such as limited verifier signature, designated verifier signature [10]. These schemes mainly focus on the ability of verification which is limited. However we may meet the following situation [23].

A hospital *A* has issued a hospital record to the patient, Bob, in the form of hospital *A*'s digital signature. Bob then wants to exclusively verify these signatures with others knowing nothing about his state of illness. Otherwise, his state of illness is exposed. After a period time, he also needs to prove validity of his hospital record to other hospitals for cure. At the same time, hospital *A* also shares the ability and

responsibility to acknowledge this hospital records when Bob may not be convenient to do so.

The aforementioned signature schemes with verifiability restriction seem to not be suitable for the above situation, as the verifier cannot prove validity of a signature to the others in a designated verifier signature and only the recipient can acknowledge a signature to a third party in a limited verifier signature. In [15], to solve the above problem, Lim and Lee proposed a new type of signature: directed signature, based on Guillou-Quisquater signature scheme [9].

In 2004, Lal and Kumar [13] suggested another scheme based on Schnorr's signature. However, no formal model was present in [15] and [13]. In 2005, Laguillaumie et al. [12] studied the universally convertible directed signatures and presented a concrete scheme which is provably secure in the random oracle model [3]. In 2006, Lu and Cao [16] independently presented a formal model for directed signatures, and proposed such a scheme based on the RSA assumption. In 2007, Lu et al. [17] studied the notion of threshold directed signatures, and presented a  $(t, n)$  threshold directed signature scheme from bilinear pairings, in which they proved that their scheme is existentially unforgeable based on the computational Diffie-Hellman (CDH) assumption.

All the above directed signature schemes work in the Public-Key Infrastructure (PKI) based setting, where the public-key is usually a "random" string that is unrelated to the user's identity. To bind the public-key to its legitimate owner, a certificate authority (CA) needs to digitally sign a certificate claiming this relationship between the public-key and the user. As a result, any verifier must obtain the valid certificate before performing signature verification. Nowadays, certificate management (including

revocation, storage and distribution) and the computational cost of certificate verification incur the main complaint against traditional public-key cryptosystems.

To eliminate the burden of certificate management, Shamir introduced the notion of identity-based cryptography [19]. In an identity-based cryptosystem, a user's public-key is just his publicly available identity (e.g. real name, email address, or IP address), hence no extra effort is necessary for ensuring the authenticity of a public-key, the complexity of the certificate management is released. ID-based cryptography is supposed to provide a more convenient alternative to conventional public key infrastructure. However, the study of directed signatures in the identity-based setting is far from satisfactory. In 2005, an ID-based signature scheme was proposed by Wang [21]. However, there is neither a formal model nor rigorous security proof in [21]. Besides, it also does not support public verification.

Recently, in 2008, Xun Sun et al. [20], proposed an ID-based directed signature scheme from bilinear pairings. The scheme is based on modified SOK identity based signature scheme due to Bellare et al. [2]. Also, based on the work of Libert and Quisquarter [14], they proved that their scheme is existentially unforgeable and invisible in the random oracle model based on CDH and DBDH assumptions respectively.

In 2009, Jianhong Zhang et al. [23] proposed an ID-based directed signature scheme using Water's signature scheme [22]. They proved that their scheme is secure against existential unforgeability and invisibility in the standard model.

In this paper, we propose an efficient ID based directed signature from bilinear pairings. This scheme uses the Hess signature scheme [11] as the base scheme. The proposed scheme is efficient than the X.Sun et al. Scheme [20] and Jianhong Zhang et al.

scheme [23]. The proposed scheme is unforgeable and invisible in the random oracle model under the CDH and DBDH assumptions respectively.

The rest of the paper is organized as follows: Section 2 briefly describes the necessary background concepts; Section 3 presents syntax and security model of ID-based directed signature scheme in the random oracle; Our ID-based directed signature scheme is proposed in Section 4; Security proof and efficiency analysis of the proposed scheme are given in Section 5. Finally, we conclude our work in Section 6.

## 2. Preliminaries

In this section, we will briefly review the basic concepts on bilinear pairings and some related mathematical problems.

### 2.1 Bilinear Pairings

Let  $G_1$  be a additive cyclic group generated by  $p$ , whose order is a prime  $q$ , and  $G_2$  be a multiplicative cyclic group of the same order  $q$ . A bilinear pairing is a map  $e : G_1 \times G_1 \rightarrow G_2$  with the following properties:

1. Bilinear:  $e(aP, bQ) = e(P, Q)^{ab}$ , for all  $P, Q \in G_1$  and all  $a, b \in \mathbb{Z}_q^*$ .
2. Non –degenerate: There exists  $P, Q \in G_1$  such that  $e(P, Q) \neq 1$ .
3. Computable: There is an efficient algorithm to compute  $e(P, Q)$  for all  $P, Q \in G_1$ .

### 2.2 Computational problems

Now, we give some computational problems, which will form the basis of security for our scheme.

**Discrete Logarithm Problem (DLP):** Given two group elements  $P$  and  $Q$ , find an integer  $n$  such that  $Q = nP$  whenever such an integer exists.

**Decisional Diffie-Hellman Problem (DDHP):** For  $a, b, c \in_R Z_q^*$ , given  $P, aP, bP, cP$  decide whether  $c \equiv ab \pmod q$ .

**Computational Diffie-Hellman Problem (CDHP):** For  $a, b, c \in_R Z_q^*$ , given  $P, aP, bP$ , Compute  $abP$ .

### 2.3 Hess-ID- based signature scheme

To prepare for the proposed scheme, we first give a review of the ID-based signature scheme [11] given by Hess as follows.

**Setup:** The Private Key Generator (PKG) chooses  $s \in_R Z_q^*$  as his master secret key and computes the global public key  $P_{pub} = sP$ . The PKG also selects a map-to-point hash function  $H_1 : \{0,1\}^* \rightarrow G_1^*$  and another cryptographic hash function  $h : \{0,1\}^* \times G_2 \rightarrow Z_q^*$ . PKG publishes system parameters  $params \langle G_1, G_2, e, P, P_{pub}, H_1, h \rangle$  and the master key  $\langle s \rangle$  is kept secret.

**Extract:** Given the public identity information on ID compute the secret key for the identity as  $d_{ID} = sQ_{ID}$ . The component  $Q_{ID} = H_1(ID)$  plays the role of the corresponding public-key.

**Signature:** To sign a message  $M \in \{0,1\}^*$ , using the secret key  $d_{ID}$ , the signer chooses an arbitrary  $P_1 \in G_1^*$  picks a random integer  $k \in Z_q^*$ .

Then signer computes

$$\begin{aligned} R &= e(P_1, P)^k, \\ V &= h(M, R), \\ U &= Vd_{ID} + kP_1. \end{aligned}$$

The signature on message M is  $\sigma = (U, V) \in G_1 \times Z_q^*$ .

**Verification:** To verify the signature  $\sigma = (U, V)$  of an identity  $ID$  on a message  $M$ , the verifier computes  $R = e(U, P)e(Q_{ID}, -P_{pub})^V$ . He accepts the signature if and only if  $V = h(M, R)$ .

### 3. Syntax and Security model for Identity-Based Directed Signature Scheme

An ID-based directed signature scheme (ID-DS) in the random model consists of the algorithms  $\langle \text{Setup}, \text{Extract}, \text{Sign}, \text{DVerify}, \text{PVerify} \rangle$ . In the following, we give the detail definitions of their algorithms:

- **System initialization (Setup):** The Private Key Generator (PKG) generates the system parameters  $params$  and the master key  $x$ ,  $params$  are made public, while  $x$  is kept secret.  $Params$  are implicit input to all the following algorithms.

- **Key extraction (Extract):** Given an identity  $ID$  and the master key  $x$ , the PKG computes the private key  $d_{ID}$  and sends it to the corresponding user through a secret channel.

- **Signature generation (Sign):** On input signer's identity  $ID_s$ , the verifier's identity  $ID_v$ , a message  $M$  and the private key  $d_{ID_s}$ , the signer  $ID_s$  generates his signature  $\sigma$  on  $M$  designated to  $ID_v$ .

- **Direct verification (DVerify):** Given signer's identity  $ID_s$ , verifier's identity  $ID_v$  and the corresponding private key  $d_{ID_v}$ , a message  $M$  and a signature  $\sigma$ , this algorithm checks the validity of  $\sigma$  to output 1 (valid) or 0 (invalid).

- **Public verification (PVerify):** On input signer's identity  $ID_s$ , verifier's identity  $ID_v$ , a message  $M$ , and a purported signature  $\sigma$ , a third party  $T$ , with an *Aid* provided by  $ID_s$  or  $ID_v$ , outputs 1 if  $\sigma$  is valid, and 0 otherwise.

### 3.1 Security Notions

The security of identity based directed signature scheme in the random oracle modal consists of two properties: unforgeability and invisibility.

**Unforgeability:** The standard security notion for digital signature schemes is existential unforgeability against adaptively chosen message attack [8]. Cha and Cheon generalized this notion to identity-based signature schemes [4]. [11] and [17] independently formalized this notion for directed signatures under their respective settings. Developed in the same line with [4, 8, 16], Xun Sun et al.[20] defined the following game between a challenger and a PPT attacker  $A$  for existential unforgeability of ID-DS schemes.

**Setup:** The challenger  $C$  runs the private key generation algorithm of ID-DS algorithm, it gives  $A$  the resulting system parameters and master secret to itself.

**Oracle queries:**  $A$  adaptively makes a number of different queries to the challenger  $C$ . Each query can one of the following.

**Extract query:**  $A$  requests the private key of any identity  $ID$ . The challenger runs the extract algorithm on  $ID$  and forwards the output  $d_{ID}$  to  $A$ .

**Signing query:**  $A$  request a signature of a signer  $IDs$  to a designated verifier  $IDv$  on message  $M$ . The challenger runs the extract algorithm to obtain a private key  $d_{IDs}$  of  $IDs$ , then runs the signature generation algorithm on  $IDs$ ,  $IDv$ ,  $M$  and  $d_{IDs}$  to obtain a signature  $\sigma$ , which is forwarded to  $A$ .

**Direct verify query:**  $A$  submits  $(IDs, IDv, M, \sigma)$  to the challenger. The challenger first extracts  $IDv$ 's private key  $d_{IDv}$  then uses  $d_{IDv}$  to verify the signature. If the signature is valid, the challenger returns 1(valid) to  $A$ , otherwise it returns 0(invalid).

**Public verify query:**  $A$  submits  $(IDs, IDv, M, \sigma)$  to  $C$  the challenger. The challenger returns  $\perp$  to  $A$ , if  $\sigma$  turns out to be invalid with respect to  $(IDs, IDv, M)$ . Otherwise, the challenger produce an *Aid* on behalf of the signers  $IDs$  or the designated verifier  $IDv$ , then forwards *Aid* to  $A$ .

**Hash query:** When the involved hash functions are modeled by random oracles,  $A$  also performs adaptive queries to the hash functions. The challenger usually responds by randomly picking an element from the output space of the hash function.

**Forgery:**  $A$  outputs signer's identity  $IDs^*$ , a verifier identity  $IDv^*$ , a message  $M^*$ , and a signature  $\sigma^*$ .  $A$  succeeds if the following situation holds:

1.  $\sigma^*$  is valid (as verified by  $IDv^*$ ) with respect to  $IDs^*$ ,  $IDv^*$  and  $M^*$ .
2.  $A$  has not made extract query on  $IDs^*$ .
3.  $\sigma^*$  was not returned by a previous sign query on  $(IDs^*, IDv^*, M^*)$ .

$A$ 's advantage in the above game is defined as  $Adv_A = \Pr[A \text{ succeeds}]$ . Where the probability is taken over all coin tosses made by the challenger and  $A$ .

**Definition1(Unforgeability):** *An ID-based directed signature scheme is  $(\epsilon, t, qE, qS, qDv, qPv, qH)$ - unforgeable, if there is no adversary who runs in time at most  $t$ , makes at most  $qE$  Extract oracle queries,  $qS$  Sign oracle queries,  $qDv$  DVerify oracle queries,  $qPv$  PVerify oracle queries, and  $qH$  Hash oracle queries, and has advantage at least  $\epsilon$  in the above game.*

**Invisibility:** The invisibility property requires that it should be (computationally) infeasible for any third party to decide whether a signature was indeed produced by a signer  $IDs$ , designated to  $IDv$ , on message  $M$ . To precisely define this property, we

consider the following game between a PPT distinguisher  $D$  and a challenger as described in [20].

**Setup:** The challenger runs the Setup algorithm of the ID-DS scheme to obtain the public parameters  $params$  and the master secret. It then gives  $params$  to  $D$  and keeps the master secret to itself.

**Phase1:**  $D$  adaptively makes a number of different queries to the challenger. Each query can be either an Extract query, a Sign query, a DVerify query, a PVerify query or a Hash query. The challenger responds to these queries in the same way as in the unforgeability game.

**Challenge:** Once  $D$  decides that Phase1 is over, it outputs a signer identity  $IDS^*$ , a verifier identity  $IDV^*$ , and a message  $M^*$ , and submits them to the challenger. The constraint is that  $IDV^*$  must have not been submitted for the Extract oracle. The challenger then generates a random bit  $b \in \{0,1\}$ , if  $b=1$ , the challenger produces a signature  $\sigma^*$  on  $(IDS^*, IDV^*, M^*)$  in the same way as the Sign query. Otherwise, it picks a random  $\sigma^*$  from the signature space. In both cases  $\sigma^*$  is forwarded to  $D$ .

**Phase2:**  $D$  again adaptively performs several oracle queries as it did in Phase 1, subjected to the following restrictions.

- $D$  cannot make an Extract query on  $IDV^*$ .
- $D$  cannot make a DVerify or a PVerify query on  $(IDS^*, IDV^*, M^*, \sigma^*)$ .

**Guess:** Finally  $D$  outputs a bit  $b' \in \{0,1\}$ .  $D$  succeeds if  $b = b'$ .

$D$ 's advantage in the above game is defined as  $Adv_D = \Pr[D \text{ succeeds}] - \frac{1}{2}$ .

Where the probability is taken over all coin tosses made by the challenger and  $D$ .

**Definition2(Invisibility):** An ID-DS scheme is  $(\epsilon, t, qE, qS, qDv, qPv, qH)$ -invisible, if there is no adversary who runs in time at most  $t$ , makes at most  $qE$  Extract oracle queries,  $qS$  Sign oracle queries,  $qDv$  DVerify oracle queries,  $qPv$  PVerify oracle queries, and  $qH$  Hash oracle queries, and has advantage at least  $\epsilon$  in the above game.

#### 4. Proposed ID-Based Directed Signature Scheme (ID-DS)

In this section, we give our proposed ID- based directed signature (ID-DS) scheme from bilinear pairings in the random oracle model. Our scheme is based on the Hess ID-based signature scheme. The proposed scheme is described as follows:

**Setup:** The PKG chooses  $x \in_R Z_q^*$  as his master secret key and computes the global public-key  $P_{pub}$  as  $xP$ . The PKG also selects a hash functions  $H_1, H_2 : \{0,1\}^* \rightarrow G_1^*$  and another cryptographic hash function  $h : \{0,1\}^* \times G_2 \rightarrow Z_q^*$ ,  $e : G_1 \times G_1 \rightarrow G_2$  where  $G_1$  and  $G_2$  be additive and multiplicative group of prime order  $q$ , let  $P$  be a generator of  $G_1$ .

Params  $\langle G_1, G_2, e, P, P_{pub}, H_1, H_2, h \rangle$ ,

Master key  $\langle x \rangle$ .

**Extract:** Given an identity  $ID \in \{0,1\}^*$ . The PKG computes  $Q_{ID} = H_1(ID) \in G_1$  then computes the user private key  $d_{ID} = xQ_{ID} \in G_1$ .

**Signature:** To sign a message  $M \in \{0,1\}^*$  to a designated verifier  $IDv$ , the signature with identity  $IDs$  and private key  $d_{ID_s}$  perform the signature.

1. The signer chooses an arbitrary  $P_1 \in G_1^*$  and picks a random integers

$$r_1, k \in Z_q^*.$$

2. Compute  $U = e(P_1, P)^k$ ,  $L = r_1 Q_{ID_s}$ .

3. Compute  $V = h(H, U)$  where  $H = H_2(ID_s, ID_v, M, U, e(d_{ID_s}, r_1 Q_{ID_v}))$ .

4. Compute  $W = V d_{ID_s} + k P_1$ .

The signature is  $\sigma = (V, W, L)$ .

**DVerify:** Given a purported signature  $\sigma = (V, W, L)$  on signature  $ID_s$ , verifier  $ID_v$  and message  $M$ ,  $ID_v$  verifies it with his private key  $d_{ID_v}$  as follows.

1. Compute  $U = e(W, P) \cdot e(Q_{ID_s}, -P_{pub})^V$ .

2. Compute  $H = H_2(ID_s, ID_v, M, U, e(d_{ID_v}, L))$ .

Accept the signature if  $V = h(H, U)$ . Reject it otherwise.

**P Verify:** Given a purported signature  $\sigma = (V, W, L)$  on signature  $ID_s$ , verifier  $ID_v$  and message  $M$ , to enable third party  $T$  to verify it either  $ID_s$  or  $ID_v$  computes  $Aid = e(d_{ID_v}, L) = e(d_{ID_s}, r_1 Q_{ID_v})$  and send it to  $T$ .

Now  $T$  computes  $U = e(W, P) \cdot e(Q_{ID_s}, -P_{pub})^V$  and  $H = H_2(ID_s, ID_v, M, U, Aid)$ .

Accept the signature if  $V = h(H, U)$ . Reject it otherwise.

## 5. Security and Efficiency Analysis

We will prove that our proposed scheme is existentially unforgeable and invisible under CDH and BDH assumptions respectively in the random oracle model.

## 5.1 Proof of correctness

To show correctness of our scheme, we show that the **DVerify** algorithm is consistent with the signature algorithm because

$$\begin{aligned}
& e(W, P).e(Q_{ID_s}, -P_{pub})^V \\
&= e(Vd_{ID_s} + KP_1, P).e(Q_{ID_s}, -P_{pub})^V \\
&= e(Vd_{ID_s}, P).e(KP_1, P).e(Q_{ID_s}, -P_{pub})^V \\
&= e(d_{ID_s}, P)^V.e(P_1, P)^K.e(Q_{ID_s}, -P_{pub})^V \\
&= e(Q_{ID_s}, P_{pub}).e(P_1, P)^K.e(Q_{ID_s}, -P_{pub})^V \\
&= U
\end{aligned}$$

Correctness of **PVerify** algorithm is straightforward.

## 5.2 Security Analysis

In the following, we will show that our scheme satisfies the existential unforgeability and invisibility. Their proofs are same as given in the [20] based on the work of [14].

**Theorem 1 (Unforgeability):** *If a PPT forger  $A$  has an advantage  $\varepsilon$  in forging a signature of ID-based directed signature when running in time  $t$  and asking  $qH_i$  queries to random oracles  $H_i (i=1,2)$ ,  $qE$  queries to the Extract oracle,  $qS$  queries to sign oracle,  $qDv$  queries to the Dveirfy oracle and  $qPv$  queries to the Pverify oracle, then the  $(\varepsilon', t')$ -CDH problem can be solved with probability  $\varepsilon'$ .*

**Theorem 2 (Invisibility):** *If a PPT distinguisher  $D$  has an advantage  $\varepsilon$  in breaking the invisibility of our ID-based directed signature when running in time  $t$  and asking  $qH_i$  queries to random oracles  $H_i (i=1,2)$ ,  $qE$ ,  $qS$ ,  $qDv$ ,  $qPv$  queries to the Extract oracle, queries to sign oracle, quires to the Dveirfy oracle and quires to the Pverify oracle, respectively, then the  $(\varepsilon', t')$ -BDH problem can be solved with probability  $\varepsilon'$ .*

### 5.3 Efficiency Analysis

We now analyze the efficiency of our proposed scheme and compare it with the related schemes including the Xun Sun et al. ID-DS scheme [20] and Jianhong Zhang et al. ID-DS scheme [23]. The comparison is summarized in table1. We consider only computations of pairings, we don't consider hash function evaluation, point addition in  $G_1$  and multiplication in  $G_2$  as they are much cheaper than the computation of pairing. We note that the computation of pairing is the most time consuming. Although there has been many papers discuss the complexity of pairings and how to speedup the pairing computation [1, 7], the computation of pairing is still time consuming. Let  $C_p$  be the computational cost to perform one pairing operation.

When compared with Xun Sun et al. ID-DS scheme [20], our scheme is efficient in signing and verifications due to the fact that the schemes required one more pairing computation for verifications and in signature generation process, our scheme requires one more pairing computations.

When compared with Jianhong Zhang et al. ID-DS scheme [23], our scheme is efficient in signing and verifications due to the fact that the schemes require two more pairing computation for verifications and in signature generation process our scheme requires one more pairing computations.

Scheme	Signature size	Signing cost	D Verify	PVerify
SOK-IBS	$3 G_1 $	1 pairing ( $1 C_p$ )	4 pairings ( $4 C_p$ )	3 pairings ( $3 C_p$ )
Zhang & yang	$4 G_1 $	1pairing( $1 C_p$ )	5 pairings ( $5 C_p$ )	5pairings ( $5 C_p$ )
Our Scheme	$2 G_1  +  Z_q^* $	2pairings ( $2 C_p$ )	3 pairings ( $3 C_p$ )	2pairings ( $2 C_p$ )

**Table 1.** Comparison of our scheme with previous schemes

## 6. Conclusions

The directed signature, due to its unforgeability and verifiable directedness properties, is very useful in some practical applications, where a signed message is personally or commercially sensitive. In this paper, we proposed efficient identity based directed signature scheme from bilinear pairings. The number of pairing operations involved in the verification process of our scheme is less than the previous identity based directed signature schemes, so our scheme is efficient than the existing directed signature schemes. In the random oracle model, our scheme is unforgeable under the Computational Diffie-Hellman (CDH) assumption, and invisible under the Decisional Bilinear Diffie-Hellman (DBDH) assumption.

## References

- [1] P.S.L.M.Barreto, H.Y.Kim, B.Lynn and M.Scott, Efficient algorithms for pairing-based cryptosystems, *Advances in Cryptology-Crypto 2002*, LNCS 2442, Springer-Verlag, 2002, pp.354-368.
- [2] M.Bellare, C.Namprempre, G.Neven, Security proofs for identity-based identification and signature schemes, *Advances in Cryptology - EUROCRYPT'04*, LNCS 3027, Springer-Verlag, 2004, pp.268-286.
- [3] M.Bellare, P.Rogaway, Random oracles are practical: a paradigm for designing efficient protocols, *Proceedings of the First Annual Conference on Computer and Communications Security*, ACM Press, 1993, pp.62-73.
- [4] J.C. Cha, J.H.Cheon, An identity-based signature from gap Diffie-Hellman groups, *Public Key Cryptography - PKC'03*, LNCS 2567, Springer-Verlag, 2003, pp.18-30.

- [5] D.Chaum Designated Confirmer Signatures. In: De Santis, A. (ed.) EUROCRYPT 1994, Springer, Heidelberg, LNCS 950, 1995, pp.86–91.
- [6] D.Chaum, H.van Antwerpen, Undeniable Signatures. In: Brassard, G. (ed.) CRYPTO 1989, Springer, Heidelberg, LNCS 435,1990, pp. 212–216.
- [7] S.D.Galbraith, K. Harrison, and D.Soldera, Implementing the Tate pairing, ANTS 2002, LNCS 2369, Springer-Verlag, 2002, pp.324-337.
- [8] S.Goldwasser, S.Micali, R.L.Rivest, A digital signature scheme secure against adaptive chosen-message attacks, SIAM Journal on Computing 17(2), 1988, pp.281–308.
- [9] L.C.Guillou and J.J. Quisquater, A practical zero-knowledge protocol fitted to security microprocessors minimizing both transmission and memory. *Advances in Cryptology,Eurocrypt-88*, LNCS 330, 1988, pp.123 - 128.
- [10] M.Jakobsson, K.Sako, R.Impagliazzo, Designated Verifier Proofs and Their Applications, In: Maurer, U.M. (ed.) EUROCRYPT 1996, Springer, Heidelberg, 1996, LNCS 1070, pp.143–154.
- [11] F.Hess, Efficient identity based signature schemes based on pairings, Selected Areas in cryptography, SAC 2002, Springer-Verlag, 2003, pp.310-324.
- [12] F.Laguillaumie, P.Paillier, D.Vergnaud, Universally convertible directed signatures, *Advances in Cryptology - ASIACRYPT'05*, LNCS 3788, Springer-Verlag, 2005, pp. 682–701.
- [13] S.Lal, M.Kumar, A directed signature scheme and its applications, see: *arXiv: cs/0409036*, 2004.
- [14] B.Libert, J.J.Quisquater, The exact security of an Identity based signature and its applications, <http://eprint.iacr.org/2004/102>.

- [15] C.H.Lim, P.J.Lee, Modified Maurer-Yacobi's scheme and its applications, *Advances in Cryptology - AUSCRYPT'92*, LNCS 718, Springer-Verlag, 1992, pp.308–323.
- [16] R. Lu, Z. Cao, A directed signature scheme based on RSA assumption, *International Journal of Network Security* 2 (3), 2006, pp.182–421.
- [17] R. Lu, X. Lin, Z. Cao, J. Shao, X. Liang, New  $(t, n)$  threshold directed signature scheme with provable security, *Information Sciences* 178 (3), 2008, pp.756–765.
- [18] R. Lu, Zhen.F, Zhou.Y, Threshold undeniable signature scheme based on conic. *Applied mathematics and computation* 162, 2005, pp.165–177.
- [19] A. Shamir, Identity based cryptosystems and signature schemes, *Advances in Cryptology - CRYPTO'84*, LNCS 196, Springer-Verlag, 1984, pp.47–53.
- [20] X. Sun, Jian-hua Li, Gong-liang Chen, and Shu-tang Yung, Identity-Based Directed Signature Scheme from Bilinear Pairings, *eprint.iacr.org/2008/305.pdf*.
- [21] Y. Wang, Directed signature based on identity, *Journal of Yulin College* 15 (5), 2005, pp.1–3.
- [22] B.Waters, Efficient Identity-based encryption without random oracles, in: Cramer, R. (ed.) *EUROCRYPT 2005*, LNCS 3494, Springer, Heidelberg 2005, pp.114–127.
- [23] J.Zhang, Y.Yang and Xinxin Niu, Efficient Provable Secure ID-Based Directed Signature Scheme without Random Oracle, *Proceedings of the 6th International Symposium on Neural Networks: Advances in Neural Networks*, LNCS, Vol. 5553,2009, Springer-Verlag, pp.318-327.