ID-Based Distributed "Magic Ink" Signature from Pairings

Yan Xie, Fangguo Zhang, Xiaofeng Chen, and Kwangjo Kim

International Research center for Information Security (IRIS)
Information and Communications University(ICU),
58-4 Hwaam-dong Yusong-ku, Taejon, 305-732 KOREA
{yanxie, zhfg, crazymount, kkj@icu.ac.kr}

Abstract. The advantage of ID-based system is the simplification of key distribution and certification management; a user can directly use his identity as his public key instead of an arbitrary number, thus at the same time he can prove his identity rather than providing a certificate from CA. Now a revocable blind signature is becoming more practical; because a complete anonymity can be abused in real world applications. For instance the perfect crime concern in e-cash system. The "magic ink" signature provides a revocable anonymity solution, which means that the signer has some capability to revoke a blind signature to investigate the original user in case of abnormal activity, while keeping the legal user's privacy anonymous. A single signer in "magic ink" signature can easily trace the original user of the message without any limitation; this scheme can't satisfy anonymity for a legal user, so we can use n signers to sign the message through a (n, n) threshold secret sharing to distribute the commitment during the signature procedure, single signer's revocability is limited, only under the agreement and cooperation of a set of n singers, the user's identity can be discovered. In this paper an ID-based (n, n) threshold "magic ink" signature is proposed along with its analysis and application.

1 Introduction

Blind signature introduced by Chaum [6] can be user to protect the privacy such as anonymity of user in the electronic cash system. However, unconditional anonymity facilitates some crimes such as perfect crime, illegal purchasing, *ect* [17]. In order to solve these problems, some technologies for anonymity revocation were proposed, such as "fair blind signature" [14], indirect discourse proofs [7], "magic ink" signature [1, 11], group signature [18, 21], and so on.

Physically "magic ink" signature can be described as follows: a user writes some message on an envelope using magic ink, simultaneously this message also is copied on a blank paper through carbon paper in this envelope, then the signer writes down his signature on the envelope, this signature also will appear on the inside paper, finally the signer and user keep the envelop and signed inside paper respectively. Normally the message is invisible on the envelop, but in some

case(criminal activity) signer can discover this invisible message. The "magic ink" signature provides a revocable anonymity solution, which means that the signer has some capability of revealing a blind signature to investigate the abnormal activity, whilst keeps the legal action anonymous. The first "magic ink" signature [11] is based on digital signature standard; this scheme approaches a revocable anonymity from a set of distributed servers through threshold cryptosystem instead of the enrollment of the trust third party in "fair blind signature". It achieves more security and availability.

In traditional CA-based public key cryptosystem, each participant should provide a digital certificate to prove the validity of his identity and public key; this procedure obviously exhausts huge system resource. In 1984, Shamir proposed an ID-based encryption and signature scheme [16], which directly utilizes user's identity as his public key. So this scheme could simplify the key distribution and certification management process.

Bilinear parings namely the Weil pairing and Tate pairing of algebraic curves were first used to analyze the discrete logarithm problem in cryptography, such as MOV attack [13] and FR attack [8]. Recently, the bilinear pairings have beeb found various applications in cryptography, more precisely, they can be need to constructed ID-based cryptographic schemes [3, 4, 12, 19, 5, 10, 15, 20].

In this paper we proposed an ID-based distributed "magic ink" signature scheme by combining a distributed "magic ink" signature with an ID-based signature from bilinear pairing. This scheme can be used in some revocable e-cash system or credential certificates applications. In case of a single signer can easily trace the original user of the message without any limitation; we can use a (n, n) threshold to share the commitment during the signature procedure. Only under the agreement and cooperation of n signers, the original user can be found.

This paper is organized as follows: some properties of bilinear pairing is introduced in Section 2. We then discuss the structure of this scheme in Section 3. In Section 4 we describe the basic idea of this signature. Our main ID-based distributed "magic ink" signature is presented in Section 5. During Section 6 we analyze the correctness, unforgeable security, robustness, efficiency and comparison of our scheme. We dedicate some application which can be established on this scheme in Section 7. Conclusion is given in Section 8.

2 Some Properties of Bilinear Pairing

We assume G_1 and G_2 are two cyclic groups of order q for a large prime q, G_1 is an additive group and G_2 is a multiplicative group, A map is a bilinear pairing, if it satisfies following properties:

1. Bilinear: $e(P_1+P_2, Q) = e(P_1, Q)e(P_2, Q)$ and $e(P, Q_1+Q_2) = e(P, Q_1)e(P, Q_2)$.
2. Non-degenerate: there exits $P, Q \in G_1$, $e(P, Q) \neq 1$.
3. Computability: If $P, Q \in G_1$, there exists an efficient algorithm to compute $e(P, Q)$.

There are some arithmetic hard problems in G_1 , as follows:

1. Discrete Logarithm Problem (**DLP**): It means that if there are two groups Q and P, it is difficult to find an integer n, which can satisfy $P = nQ$.

2. Decision Diffle-Hellman Problem (**DDHP**): Given P, aP, bP, cP, and $a, b, c \in Z_q^*$, determine whether $c \equiv ab \bmod q$.

3. Computational Diffle-Hellman Problem (**CDHP**): Given P,aP,bP,$a, b \in Z_q^*$, computes abP.

4. Gap Diffle-Hellman Problem(**GDHP**): A class of problems, when the **DDHP** is easy, but the **CDHP** is hard.

We let CDHP and DLP are intractable in this paper, that means there is no polynomial time algorithm to solve CDHP and DLP with nonnegligible probability. We call a group G a Gap Diffle-Hellman group, when the DDHP is easy and CDHP is hard on that group. Such group can be found on supersingular elliptic curves or hyperelliptic curves over finite field, and the bilinear pairing can be derived from the Weil or Tate pairing.

3 Structure

3.1 Computation and Communication

We assume: there are a set of n signers and k receivers, all of them are polynomial-time randomized Turing machines. In communication model, we also assume: any receiver can build point to point communication channel with each signer through a secure channel. An adversary can corrupt up to $n - 1$ among the n signers.

3.2 ID-based "Magic Ink" Signature

An ID-based "magic ink" signature scheme consists of three parties and five steps, which is described as follows:

- Three parties are Trust Authority(TA), n signers and receiver.
- **Setup** is a randomized algorithm, which generates system parameters and a master key by inputting a security parameter to TA.
- In **Extract** step, TA inputs system parameters, master key and an arbitrary $ID \in \{0, 1\}^*$, and outputs a private key S_{ID}. Here ID is the signer's identity, which is treated as the signer's public key.
- **Signature** is a signature generation protocol engaged by receiver and a set of n signers, signers output a blind signature, and receiver finally produces a valid or failed signature. Signers record a signature-view variant in their database to indicate each blind signature.

- **Verification** is a randomized algorithm that takes message m with its signature and signers' identities as an input, and outputs acceptation or rejection.
- **Tracing** occurs in case of illegal activities, signers will search their database of signature-view invariant to find a value, which can be linked to the valid signature. From this value, signers can find the original signature receiver.

4 Basic Idea of ID-Based "Magic Ink" Signature(Single Signer)

ID-based "magic ink" signature can be regarded as a combination of ID-based signature with a revocable blind signature. We will describe the basic idea of ID-based "magic ink" signature from a single signer. First set G_1 to be a cyclic additive group and G_2 to be a multiplicative group, both of groups have a same prime order q, our scheme is built on Gap Diffle-Hellman Group . We view the bilinear map as $e : G_1 \times G_1 \rightarrow G_2$.

At the beginning of this protocol, the **TA** operates Setup and Extract, during the generation of private key of the signer, we can use n **TA's** with a (n, n) threshold security sharing to share the master key, in order to control the power of **TA**.

Setup:

Let P be a generator of G_1, randomly choose a number $s \in Z_q^*$ as a master key of trust authority, set $P_{pub} = sP$. Construct two cryptographic hash functions $H : \{0,1\}^* \rightarrow Z_q$ and $H_1 : \{0,1\}^* \rightarrow G_1$. Then the system parameters are : $\{q, P, P_{pub}, G_1, G_2, e, H, H_1\}$.

Extract:

Assume that the signer's identity is his ID, we can calculate the public key as $Q_{ID} = H_1(ID)$, and the private key of signer is $S_{ID} = sQ_{ID}$.

Signature:

- The signer randomly chooses a number $r \in Z_q^*$, and computers $R = rP$, then sends R to the receiver.
- A number $a \in Z_q^*$ will be chosen randomly by receiver as a blind factor, then receiver computes $t = e(aP_{pub}, R)$ and $c = H(m, t)$ with his message m, sends blinded c by computing $c' = a^{-1}c \bmod q$ to signer.
- After receiving c', signer uses his private key S_{ID} to produce the blind signature by computing $S' = c'S_{ID} + rP_{pub}$, and sends the S' to the receiver.
- S' is unblinded by factor a, then the final signature of message m is (S, t, m), where $S = S'a$.

The protocol is showed in Fig.1.

Verification:

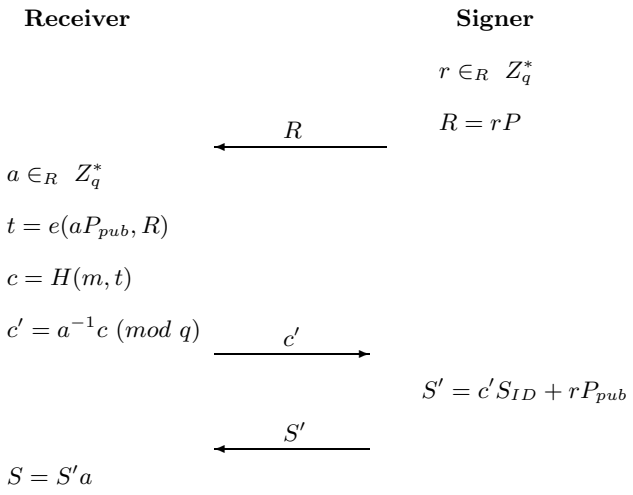

Fig. 1. ID-based "magic ink" signature protocol

Receiver can verify whether the signature is valid or not by using signer's public key to check:

$$e(S, P) = e(Q_{ID}, P_{pub})^{H(m,t)}t.$$

Receiver accepts the signature, if the above equation holds.

Tracing:

Let $(c^{-1}S)$ identifies a valid signature (m, t, S), and (c', S') can be viewed by the signer during the signature session. In each signature, we have $c'^{-1}S' = c^{-1}S$, since:

$$c'^{-1}S' = c^{-1}a \times Sa^{-1} = c^{-1}S.$$

From a valid signature (m, t, S), signer can easily calculate $c^{-1}S$, here $c = H(m, t)$. So if any illegal receiver needs to be discovered, signer can compare the value of $c^{-1}S$ with the database of signature-view invariant. If signer can find the same value in the database, the original receiver can be identified.

5 ID-Based Distributed "Magic Ink" Signature(Multiple Signers)

It is trivial that the case of single signer can't satisfy the privacy requirement because single signer can trace the user as his will. Therefore, we provide a (n, n) threshold scheme by modifying our previous construction in a single signer case, which means a signer will be replaced by n signers in a way that key generation

and signature generation require collaboration of at least n singers, whilst no subgroup of less than n participants can forge a signature.

We set n signers to individually sign the message through using their own private keys and send it to user through point-to-point communication with receiver, and receiver combines those signatures to an ID-based "magic ink" signature. The advantage of ID-Based distributed "magic ink" signature is that it can hide the signature-view invariant to each signer, also it satisfies the original ID-based blind signature requirement. So without the agreement and cooperation of n signers, the signature can't be revoked. The protocol of ID-based distributed "magic ink" signature is described as follow:

Set G_1 as a cyclic additive group and G_2 as a multiplicative group, both of groups have a same prime order q. We view the bilinear group as $e : G_1 \times G_1 \rightarrow G_2$.

Setup:

Let P be a generator of G_1, randomly choose a number $s \in Z_q^*$ as a master key of trust party, set $P_{pub} = sP$. Construct two cryptographic hash functions $H : \{0,1\}^* \rightarrow Z_q$ and $H_1 : \{0,1\}^* \rightarrow G_1$. Then the system parameters are : $\{q, P, P_{pub}, G_1, G_2, e, H, H_1\}$.

Extract:

Assume each signer's identity is ID_i. We can express the public key of each signer as: $Q_{IDi} = H_1(ID_i)$, and the private key of signer is $S_{IDi} = sQ_{IDi}$, so the public key of the scheme is $Q_{ID} = \sum_{i=1}^{n} Q_{IDi}, i = 1, 2...n$.

Signature Session:

- n signers obtain a (n, n) secret sharing $(r_1, r_2, \ldots r_n)$ of a randomly chosen number $r \in Z_q^*$ by letting $r = \sum_{i=1}^{n} r_i$, each signer computes $R_i = r_i P$, and sends R_i to receiver.
- Receiver computes $R = \sum_{i=1}^{n} R_i$, and randomly chooses a number $a \in Z_q^*$. Receiver computes $t = e(aP_{pub}, R)$ and $c = H(m, t)$ with the message m, and sends blinded c by computing $c' = a^{-1}c \bmod q$ to each signer.
- Each signer individually generates the signature $S_i' = c' S_{IDi} + r_i P_{pub}$, and secretly sends it to receiver.
- After receiving all the signature S_i', receiver computes $S' = \sum_{i=1}^{n} S_i' = c' \sum_{i=1}^{n} S_{IDi} + \sum_{i=1}^{n} r_i P_{pub}$. He then unblinds S' by computing $S = S'a$, and the (S, t, m) will be the valid ID-based distributed "magic ink" signature on message m.

  Fig.2 shows the protocol.

Verification:

The verification is similar to the previous single signer verification, receiver uses public key Q_{ID} to check whether it is a valid signature from equation:

$$e(S, P) = e(Q_{ID}, P_{pub})^{H(m,t)} t.$$

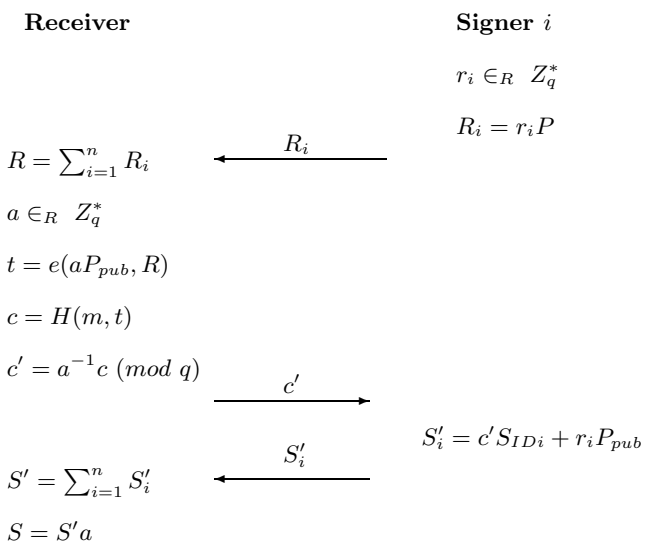

Fig. 2. ID-Based Distributed "Magic Ink" signature protocol

Tracing:

Since S' is blind to each signer, and each S_i' is secretly sent to receiver, so any signer can't know S' without cooperating with another $n-1$ signers. Only n signers work together to compute S' from $S' = \sum_{i=1}^{n} S_i'$, then the signature-view invariant will be revoked. Through this value signers can compare with the signature to trace the original signature receiver.

6 Analysis of ID-based distributed "magic ink" signature

6.1 Correctness

This scheme is a valid signature; the proof of verification equation is as follow:

$$\begin{aligned} e(S, P) &= e(S'a, P) = e(\sum_{i=1}^{n} S_i' a, P) \\ &= \prod_{i=1}^{n} e(ac' S_{IDi} + a r_i P_{pub}, P) \\ &= \prod_{i=1}^{n} e(c S_{IDi}, P) \prod_{i=1}^{n} e(a r_i P_{pub}, P) \\ &= e(S_{ID}, P)^c \prod_{i=1}^{n} e(a P_{pub}, P)^{r_i} \end{aligned}$$

$$
\begin{aligned}
&= e(sQ_{ID}, P)^c \prod_{i=1}^{n} e(aP_{pub}, r_i P) \\
&= e(sQ_{ID}, P)^c \prod_{i=1}^{n} e(aP_{pub}, R_i) \\
&= e(sQ_{ID}, P)^c e(aP_{pub}, R) = e(Q_{ID}, sP)^c t \\
&= e(Q_{ID}, P_{pub})^{H(m,t)} t
\end{aligned}
$$

6.2 Blindness

This scheme basically can achieve blindness requirement, because the message M sent to signer will be blinded previously by a randomly chosen integer $a \in Z_q^*$, and the signer just signs the blinded message c'. After receiving the blinded signature, the user can unblind this signature by using blind factor a and get the valid signature, but the signer can't find any relationship between S' and S, signer just has a probability of $1/q$ to correctly guess the unblinded signature, so we can say this scheme is blind.

6.3 Revocable Anonymity

A valid magic ink signature means that the scheme should be revocable anonymity; this scheme also supports such function. The signer receives c' and S' during each signature session, he can pre-compute the value of $c'^{-1}S'$ and store each value into a specific database. When he needs to trace the user, he can compute the value of $c^{-1}S$ from the signature (S, t, m). Since the signature view invariant, signature can search this value in database to find the original user. So the revocable property is maintained. The tracing mechanism of distributed magic ink should be cooperated by n signers, because each signer can't get S' by himself. The revocability of signers can be controlled

6.4 Unforgeable Security

We consider the following fame: assume that an adversary can cooperate $n-1$ signers without loss of generality. Let the identities of these $n-1$ signer are $Q_{ID_i}, i = 1, 2...n$. So adversary can get S_{ID_i} to compute S'_i. If he can compute S_{ID_n}, he can forge a valid ID-based distributed "magic ink" signature. However it is equivalent to solve CDHP in G_1 for computing $sH(ID_n)$ with sP and $H(ID_n)$.

6.5 Robustness

If the signature can't pass the verification, there exists some dishonest signers. Since each signer should send his partial signature S'_i to the receiver, receiver can

check each signature by verifying whether $e(S_i, P) = e(Q_{IDi}, P_{pub})^{H(m,t)} e(aP_{pub}, R_i)$, here $S_i = S_i' a$. If one of the signatures doesn't pass, we can declare that this signer made some mistake or cheating.

6.6 Comparison and Efficiency

Jakobsson first proposed a distributed "magic ink" signature [11] in 1997. The comparison with our proposed scheme is showed in Table 1 . We denote **DMIS**

	DMIS	IDDMIS
Number of costs(reciever)	$(2n+1)$**E**+ 4**m**+ 2**I**	1**e**+ 2**M**+ 1**D**+ $(2n-1)$**A**
Number of cost(each signer)	2**E**+ 3**m**	3**M**+ 1**A**
Private key size(bit)	160bit	161bit
Public key size(bit)	1024bit	161bit
Threshold	(n, t)	(n, n)
Based Problem	DLP	CDHP

Table 1. Comparison with Distributed "Magic Ink" Signature

the distributed "magic ink" signature [11], **IDDMIS** the ID-based distributed "magic ink" signature, **M** the cost of multiplication over G_2, **D** the cost of Division over a finite field, **A** the point addition over G_2, **e** the cost of weil pairing computation in G_1, **m** the cost of multiplication over a finite field, **E** the cost of exponent over a finite field, and **I** the cost of inverse over a finite field.

Compared with IDDMIS, The advantages of our protocol are described as follows:

- Due to the ID-based signature, n signers can directly use their identities such as an e-mail address related with their unique information instead of a certificate issued by Certification Authority. So it simplifies the key distribution and management in our scheme.
- We compare the computation costs of receiver's side between two schemes. we can find that if n, which denotes the number of distributed signers, is not less than 2, the computational costs in user side of our scheme is lower than previous scheme. If the system use a mount of distributed signers, our scheme will be more efficient as the number of n increases. For example, according to [2], on PIII 1 GHz one multiplication over a finite field costs 0.006 milliseconds, When n=20, in previous scheme each receiver takes 197 milliseconds, however our protocol for each receiver takes 25 milliseconds.

7 Application

Unconditional anonymity may facilitates perfect crimes such as money laundering, blackmailing, *etc.* So recently a revocable e-cash system is desirable in

practical use, that is the anonymity of the user is revocable in some urgent case. Our ID-based distributed "magic ink" signature scheme also can be used in a revocable e-cash system, we can treat bank as signers, and buyer as a receiver, during the withdrawal step, buyer first randomly chooses a message m as his e-coin, and gets the valid ID-based distributed "magic ink" signature to his coin from bank, bank assigns n different parties to sign this coin and as the same time stores each part of signature-view variant to their database. During payment step, vendor simply verifies whether the coin is valid or not by checking bank's signature. If the coin is valid, a vendor will deposit it to bank. When bank detects some illegal activities such as blackmail or money laundering, he can search the database of signature-view invariant to find the corresponding user. Also if bank cooperates with user, he can act coin tracing to calculate the final coin and signature. But because of the use of distributed signature, the revocability of bank is limited, Only under the cooperation of all n parties, bank can get the signature-view invariant. In some previous fair e-cash system scheme, a trust third party**(TTP)** was used to send the pseudonym in signature put by user during the signature procedure to bank, in order to help bank to make tracing, but our scheme doesn't need the enrollment of the TTP. It obviously reduces the protocol complexity and saves the system resource.

8 Conclusion

In this paper, we proposed an ID-based distributed "magic ink"s signature scheme. Our scheme combine the advantages of ID-based signature and traditional "magic ink" signature scheme, which can be used for designing revocable anonymity e-cash system without TTP. A disadvantage of our scheme is (n, n) threshold, so it lacks flexibility. Since it seems no (n, t) threshold ID-based signature until now, we will design a (n, t) threshold to improve the efficiency and availability in the future works.

References

1. F. Bao and R. Deng, *"A new type of "magic ink" signature towards transcript-irrelevant anonymity revocation"*, PKC'99, LNCS 1560, pp.1-11, Springer-Verlag, Berlin Heidelberg 1999.
2. 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, pp. 354-368, Springer-Verlag, 2002.
3. D. Boneh and M. Franklin, *"Identity-based encryption from the Weil Pairing"*, Advances in Cryptology-Crypto'2001, LNCS 2139, PP.213-29, Spring-Verlag, 2001.
4. D. Boneh, B. Lynn, and H. Shacham, *"Short signatures from the Weil pairing"*, Advances in Cryptology-Asiacrypt 2001, LNCS 2248, pp. 514-532, Springer-Verlag, 2001.

5. J.C. Cha and J.H. Cheon, *"An Identity-based signature from gap Diffie-Hellman groups"*, Cryptology ePrint Archive, Report 2002/018, available at http://eprint.iacr.org/2002/018/.
6. D. Chaum, *"Blind signatures for untraceable payments"*, Advanced in Cryptology-Crypto'82, 1983, Plenum NY, pp. 199-203.
7. Y. Frankel, Y. Tsiounis, M. Yung, *"Indirect discourse proofs: achieving efficient fair off-line e-cash"*, Advanced in Cryptology-Asiacrypt'96, LNCS 1163, pp. 286-300, Springer-verlag, 1996
8. G. Frey and H. Rück, *"A remark concerning m-divisibility and the discrete logarithm in the divisor class group of curves"*, Mathematics of Computation, 62, pp.865-874, 1994.
9. S. D. Galbraith, K. Harrison, and D. Soldera, *"Implementing the Tate pairing"*, ANTS 2002, LNCS 2369, pp. 324-337, Springer-Verlag, 2002.
10. F. Hess, *"Exponent group signature schemes and efficient identity based signature schemes based on pairings"*, Cryptology ePrint Archive, available at http://eprint.iacr.org/2002/012/.
11. M. Jakobsson and M. Yung, *"Distributed magic ink signatures"*, Advances in Cryptology-EUROCRYPT'97, LNCS 1233, PP.450-464, Spring-Velag, 1997.
12. A. Joux, *"The Weil and Tate Pairing as building blocks for Public Key Cryptosystem"*, ANTS 2002, LNCS 2369, PP.20-32, Springer-verlag, 2002.
13. A. Menezes, T. Okamoto, and S. Vanstone, *"Reducing elliptic curve logarithms to logarithms in a finite field"*, IEEE Transaction on Information Theory, 39: 1639-1646, 1993.
14. Y. Mu, K.Q. Nguyen, and V. Varadharajan, *"A fair electronic cash scheme"*, ISEC2001, LNCS 2040, pp. 20-32, Springer-verlag, 2001
15. K.G. Paterson, *"ID-based signatures from pairings on elliptic curves"*, Cryptology ePrint Archive, available at http://eprint.iacr.org/2002/004/.
16. A. Shamir, *"Identity-based cryptosystems and signature schemes"*, Advances in Cryptology-Crypto'84, LNCS196, pp.47-53, Springer-Verlag, 1984.
17. B.V. Solms and D. Naccache, *"On blind signatures and perfect crimes"*, Computers and security, 11(6):581-583, 1992.
18. J. Traor, *"Group signature and their relevance to privacy-protecting off-line electronic cash systems"*, Proc. of ASISP99, LNCS 1587, pp. 228-243, Springer-verlag, 1999.
19. F. Zhang, S. Liu and K. Kim, *"ID-Based one round authenticated tripartite key agreement protocol with pairings"*, Cryptology ePrint Archive, available at http://eprint.iacr.org/2002/122/.
20. F. Zhang and K. Kim, *"ID-Based blind signature and ring signature from pairings"*, Asiacrypt2002, New Zealand, LNCS 2501, pp.533-547, Springer-verlag, 2002.
21. F. Zhang, F.T. Zhang and Y. Wang, *"Fair electronic cash systems with multiple banks"*, SEC 2000, pp. 461-470, Kluwer, 2000.