ID-Based Distributed "Magic Ink" Signature

Yan Xie*, Fangguo Zhang*, Kwangjo Kim*

*Internatonal Research Center for Information Information Security(IRIS)

Information and Communications University(ICU)

Abstract

The advantage of ID-based(Identity-based) signature is the simplification of key distribution and certification management; a signer 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 certification from CA. Now a revocable blind ID-based signature is becoming more practical; because a complete anonymity is unreasonable 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 to share the commitment during the signature procedure to limit single signer's revocability, then only under the agreement and cooperation of a set of n singers, the user's identity can be discovered.

I. Introduction

In order to let the user get the signature of his message without revealing his message from signer, Chaum introduced a blind signature[5]. It can be used to protect the privacy of the user, but some malicious person can abuse such perfect anonymity provided by this scheme to commit perfect crime[12].

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 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 revoking a blind signature to investigate the abnormal activity, whilst keeps the legal action anonymous. The first ``magic ink'' signature[9] 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 public key cryptosystem, each participant should provide a digital certification 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[11], which directly utilizes user's identity as his public key. So this scheme could simplify the key distribution and certification management process.

Bilinear paring namely the Weil pairing and Tate pairing of algebraic curves was first used to analyze the discrete logarithm problem in cryptography, such as MOV attack[10] and FR attack[6]. Now a variety of cryptographic applications based on bilinear pairing[2, 3,] are proposed, it is also introduced to construct several ID-based signature schemes [4, 8,].

In this paper we provided an ID-based distributed ''magic ink'' signature scheme by combining a distributed ''magic ink'' signature with an ID-based signature. 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 singers, the original user can be found.

This paper is organized as follows: some properties of bilinear pairing is introduced in Section 2. Our main ID-based distributed ''magic ink'' is presented in Section 3. During Section 4 we analyzed the correctness, unforgeable security, robustness. Conclusion is given in Section 5.

II. Some Properties of Bilinear Pairing

If we assume G_1 and G_2 be two cyclic groups of order q for some large prime q, G_1 is an additive group and G_2 is a multiplicative group. A map $G_1 \times G_1 \rightarrow G_2$ 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: If there are $P, Q \in G$, $e(P, Q) \neq 1$.

3. Computability: If $P, Q \in G$, there exists an efficient algorithm to compute $e(P, Q)$.

There are some arithmetic hard problems based on bilinear pairing, as follows:

1. Discrete Logarithm Problem (**DLP**): It means that if there are two group 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**): Give P, aP, bP, cP, $a, b, c \in Z_q^*$, computer abP.

4. Gap Diffle-Hellman Problem (**GDHP**): We can call a group Gap Diffle-Hellman Group, if the **DDHP** is easy, but the **CDHP** is hard.

III. ID-Based Distributed ''Magic Ink'' Signature

ID-based ''magic ink'' signature can be thought as a combination of ID-based signature with a revocable blind signature. There are some definitions of security requirements and considerations related to ID-based ''magic ink'' signature. An ID-based ''magic ink'' signature scheme consists of three parties: Trust Authority(**TA**), signers and receiver, and five steps, which is described as below:

We set n signers to individually sign the message through using their own private key and send it to user through point-to-point communication with receiver, and a receiver combines those signatures to ID-based ''magic ink'' signature. The advantage of ID-based distributed ''magic ink'' signature is that it can blind the signature-view invariant to the signers least than n, 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, ramdomly 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: $\{q, P, P_{pub}, G_1, H, H_1\}$.

Extract:

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

Signature Session:

n sigers obtain an (n, n) secret sharing $(r_1, r_2 \ldots r_n)$ of a randomly chosen number $r \in Z_q^*$ by letting $r = \sum_{i=1}^{n} r_i$.

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 $C' = c/a \bmod q$ to each signer.

Each signer individually generates the signature $S'_i = c' S_{ID_i} + r_i P_{pub}$, and secretly sends it to receiver.

After receiveing all the signature S_i', a receiver combines those signatures to get blind signature S', where $S' = \sum_{i=1}^{n} S'_i = c' \sum_{i=1}^{n} S_{ID_i} + \sum_{i=1}^{n} r_i P_{pub}$, then the receiver unblinds the S_i' by computing $S = S'a$. so the (S, t, m) will be the valid ID-based distributed ''Magic Ink'' signature of message m.

Verification:

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

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

Signature-View Invariant:

Let $(c^{-1}S)$ identifies a valid signature (S, t, m), and (c', S') can be viewed by

signer during the signature session. In each signature, we have $C'^{-1}S'=C^{-1}S$, since: $C'^{-1}S'=a/c\times S/a=C^{-1}S$.

Tracing:

Since S' is blinded 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.

IV. Analysis of This Scheme

6.1 Correctness

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

$$\begin{aligned} e(S,F) &= e(aS',F) \\ &= e(ac'S_{ID}+arP_{pub},F) \\ &= e(cS_{ID},F)e(arP_{pub},F) \\ &= e(sQ_{ID},F)^{c}e(aP_{pub},rF) \\ &= e(Q_{ID},sF)^{c}t \\ &= e(Q_{ID},P_{pub})^{H(m,t)}t \end{aligned}$$

6.2 Blindness

This scheme is originally a blind signature, because the message sent to n singer will be blinded previously by a number $a \in Z_q^*$ randomly chosen by a receiver, so 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, the signer just has a probability of $1/q$ to correctly guess the unblinded signature, so we can say this scheme is blinded. 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 precompute 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 included. The tracing of distributed magic ink should be cooperated by n singers, because each signer can't get S' by himself, that controls revocability of n singers.

6.3 Unforgeable Security

This scheme can defend a forgeable attack. We assume the adversary can break $n-1$ signers and get their key pairs respectively:

$$(Q_{ID_1}, S_{ID_1}),(Q_{ID_2}, S_{ID_2}),$$
$$\ldots,(Q_{ID_{n-1}}, S_{ID_{n-1}}),$$

if the attacker wants to forge a valid signature, he must produce a valid ID-based distributed ''magic ink'' signature key pair (Q_{ID}, S_{ID}), in order to get this key pair, he should know the nth user's private key S_{ID_n}, so even he has $n-1$ user's key pairs, because of the CDHP in bilinear pairing, the difficulty to calculate the master key s equals to break TA to get to master key.

Because the master key s is chosen from Z_q randomly, so the probability for the forged signature to pass the verification is $1/q$.

6.4 Robustness

If the signature can't pass the verification, a receiver can trace the error.

Since each signer should send his partial signature S_i' to the user, user can check each signature by verifying whether $e(S_i, P) = e(Q_{ID_i}, P_{pub})^{H(m,t)}t$, where $S_i = aS_i'$. If one of the signatures doesn't pass, we can declare that this signer made some mistake or cheating.

V. Conclusion

ID-based distributed ''magic ink'' signature achieves revocable anonymity and revocability limitation by designing (n, n) threshold secret sharing, that means for each signer the valid signature is anonymous, even it is impossible for less than n signers work together to link the signed message to an original user. Only n singers working together can reach the revocability. This scheme can be used in a revocable e-cash system. Which requires revocability of tracing some illegal activities such as blackmailing, money laundering and so on. Further, we hope to find a (n, t) threshold to improve its robustness and availability, as well as making security proofs.

[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, pp. 354-368, Springer-Verlag, 2002.

[2] 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.

[3] D. Boneh, B. Lynn, and H. Shacham, ''Short signatures from the Weil pairing'', In C. Boyd, editor, Advances in Cryptology-Asiacrypt 2001, LNCS 2248, pp. 514-532, Springer-Verlag, 2001.

[4] 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/.

[5] D. Chaum, ''Blind signatures for untraceable payments'', Advanced in Cryptology Crypto'82, 1983, Plenum NY, pp. 199-203.

[6] G. Frey and H. Ruck, ''A remark concerning m-divisibility and the discrete logarithm in the divisor class group of curves'', Mathematics of Computation, 62, pp.865-874, 1994.

[7] S. D. Galbraith, K. Harrison, and D. Soldera, ''Implementing the Tate pairing'', In C. Fieker and D.R. Kohel (Eds.): ANTS 2002, LNCS 2369, pp. 324-337, Springer-Verlag, 2002.

[8] 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/.

[9] M. Jakobsson and M. Yung, ''Distributed magic ink signatures'', Advances in Cryptology-EUROCRYPT'97, LNCS 1233, PP.450-464, Spring-Velag, 1997.

[10] 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.

[11] A. Shamir, ''Identity-based cryptosystems and signature schemes'', Advances in Cryptology-Crypto'84, LNCS196, pp.47-53, Springer-Verlag, 1984.

[12] B.V. Solms and D. Naccache, ''On blind signatures and perfect crimes'', Computers and Security, 11(6):581-583, 1992.