Design of Threshold Blind Signature Scheme

Duc-Liem Vo and Kwangjo Kim

International Research center for Information Security (IRIS)

Information and Communications University (ICU), Korea

Abstract

Threshold signature and blind signature are playing important roles in cryptography as well as practical applications such as e-cash and e-voting systems. In this paper, we present a new threshold blind digital signature based on pairings without a trusted third party. Our scheme operates on Gap Diffie-Hellman group, where Computational Diffie-Hellman problems are hard but Decision Diffie-Hellman problems are easy. For example, we use pairings that could be built from Weil pairing or Tate pairing. To the best of our knowledge, we claim that our scheme is the first threshold blind signature using pairings with provable security in the random oracle model.

I. Introduction

Digital signature is an essential component in cryptography. Depending on its purpose, the digital signatures can provide the various setting.

A threshold signature scheme distributes the signing abilities to a group of signers such that a digital signature on a message cannot be produced by a predetermined number of signers. With this property, misbehavior caused by a single dishonest signer will be eliminated in many applications. A blind signature scheme, on the other hand, gives users ability to get a digital signature from a signer without revealing message content. This property is very important for implementing e-voting, e-commerce, and e-payment systems, etc.

A threshold blind signature combines a threshold signature and a blind one to exhibit both properties. Therefore, a threshold blind signature while giving user ability to get signature on a message without revealing its content, still maintains the shared secret key to be distributed among signers.

In this paper, we propose a new threshold blind signature scheme based on pairings. Working on an elliptic curve over a finite field, our proposed signature scheme has achieved efficiency in terms of the signature size compared to the previous schemes [14] and [15]. We also prove the security of our signature scheme in a formal way.

Organization: Some background on bilinear pairings and relevant tools are stated in Section II. In Section III, we describe our proposed threshold blind signature scheme. Section IV analyzes the security aspects of the proposed scheme. In Section V, we will evaluate performance of our scheme. Section VI is concluding remark.

II. Preliminaries

1. Concepts of bilinear pairings

We summarize some concepts of bilinear pairings using similar notations used by Zhang and Kim [23] which was used to design ID-based blind signature and ring signature based on pairings.

Let G_1 and G_2 be additive and multiplicative groups of the same prime order q, respectively. Let P is a generator of G_1. Assume that the discrete logarithm problems in both G_1 and G_2 are hard. Let $e:G_1 \times G_1 \rightarrow G_2$ be a pairing which satisfies the following properties:

1. *Bilinear*: $e(aP,bP') = e(P,P')^{ab}$ for all $P, P' \in G_1$ and all $a,b \in \mathbf{Z}$.

2. *Non-degenerate*: If $e(P,P') = 1$ for all $P' \in G_1$ then $P = O$.

3. *Computable*: There is an efficient algorithm such as [1] to compute $e(P,P')$ for any $P, P' \in G_1$.

Group G_1 is called Gap-Diffie-Hellman (GDH) group if in this group, Computational Diffie--Hellman (CDH) problems are hard but Decision Diffie-Hellman (DDH) problems are easy. Throughout this paper, G_1 is GDH group of the prime order q.

2. Blind signature scheme based on GDH problem

To propose the threshold blind signature scheme, we build a blind version of the signature scheme in [4] defined as follows:

Let P be a generator of G_1. Public information is $I=(q,P,H)$ where $H:\{0,1\}^* \rightarrow G_1$ is an one-way hash function. A new blind *GDH* signature scheme **BGS**=(*BK,BS,BV*), where *BK*, *BS*, and *BV* are key generation, blind signing and verification protocol, respectively, is defined as:

- *BK*(I): Pick randomly $s \in_R \mathbf{Z}_q$ and compute $Q=sP$. Return the public key pk and the secret key sk, where $pk=(q,P,H,Q)$, and $sk=s$.

- *BS*(I,sk,M): The user wants a message $M \in \{0,1\}^*$ to be signed blindly. He picks a random number $r \in_R \mathbf{Z}_q$ and computes a blind message M' of the message M, $M'=H(M)$. He sends M' to the signer. The signer signs on M', $\sigma'=sM'$ and sends back σ' to the user. Receiving σ', the user unblinds it and gets the signature of the message M, $\sigma = r^{-1}\sigma'$ and outputs (M,σ).

- *BV*(pk,M,σ): If $V_{DDH}(P,Q,H(M),\sigma)=1$ then return 1 else return 0, where $V_{DDH}()$ is an efficient algorithm which solves the DDH problem in G_1.

The security of the proposed blind signature will be discussed in Section 4.

III. Proposed Scheme

The threshold blind signature schemes TBS includes of three protocol: Key generation *TBK*, Signature generation *TBS*, and Signature verification *TBV* protocols.

1. Key generation *TBK*

Suppose that there are n players involved in the *TBK* protocol to make a (t,n)-threshold scheme DKG [9], where $n \geq 2t-1$.

Let P and P' (i.e., $P'=\beta P$ for some $\beta \in \mathbf{Z}_q$) be generators of G_1. Denote n players involving in *TBK* as $\{L_1, L_2,..., L_n\}$. The public key and the secret key of this group of players are Q and s, respectively. The public share of the player L_i is Q_i and the corresponding secret share is s_i, for $i=1, 2,..., n$.

Each player L_i behaves as the following to generate a shared secret.

G1. At first, L_i sends its information.

- Select randomly (uniformly distributed as in [18]) a_i and $b_i \in \mathbf{Z}_q$, keeps them secret.
- Pick up randomly two polynomials $f_i(x)$ and $f'_i(x)$ over $\mathbf{Z}_q$ of degree at most $t-1$ such that $f_i(0)=a_{i0}$ and $f'_i(0)=b_{i0}$. Let $f_i(x)=a_{i0} + a_{i1}x + ...+ a_{i,t-1}x^{t-1}$ and $f'_i(x)=b_{i0} + b_{i1}x +...+ b_{i,t-1}x^{t-1}$. These polynomials are kept secret by each player.
- Compute and broadcast $C_{ik}=a_{ik}P + b_{ik}P'$ for $k = 1, 2,..., t-1$; sends $f_i(j)$ and $f'_i(j)$ secretly to each player L_j for $j=1, 2,..., n$; $j \neq i$.

G2. L_i receives information from other players.

(a) After receiving $f_j(i)$ and $f'_j(i)$ from L_j for $j=1, 2,..., n$; $j \neq i$, the player L_i verifies $f_j(i)$ and $f'_j(i)$ by checking

$$f_j(i)P + f'_j(i)P = \sum_{k=0}^{t-1} i^k C_{jk} \qquad (1)$$

If Eq.(1) is verified to be false, L_i broadcasts a complaint against L_j.

(b) Each player L_j , who received a complaint from player L_i, broadcasts the values $f_j(i)$ and

$f'_j(i)$ satisfying Eq.(1).

(c) Each player marks as disqualified any player that either:

- received more than t-1 complaints at (a), or,
- answered to a complaint in (b) with values that make invalid Eq.(1).

G3. Build the set of non-disqualified players by denoting this by HP which means a set of honest players.

G4. Computes the secret share $s_i=\sum_{k\in HP} f_k(i)$.

G5. Each player $L_i \in HP$ broadcasts $a_{ik}P$ for k = $0, 1,..., t-1$.

- Player L_i verifies the value broadcast by other players in HP, for each $j \in HP$, verify:

$$f_j(i)P = \sum_{k=0}^{t-1} i^k a_{jk}P \qquad (2)$$

If the check fails for index j, play L_i sends complaint against L_j by broadcasting values $f_j(i)$ and $f'_j(i)$ which satisfies Eq.(1) but Eq.(2).

- For player L_j, who receives at least one valid complaint as above, the other players will use Pedersen's VSS to reconstruct value of a_{j0}, $f_j(x)$ and $a_{jk}P$ for k=0,1,...,t-1. Each player in HP sets public key of group as $Q = \sum_{i\in HP} a_{i0}P$. The corresponding secret key $s=\sum_{i\in HP} a_{i0}$ is distributed to n players but does not appear explicitly in the protocol. Each player has the secret share s_i and the public share $Q_i = s_iP$.

2. Signature Generation *TBS*

Suppose that a user A wants to get a signature on the message M blindly from t signers. Denote t signers as $S = \{L_i | 1 \le i \le t\}$.

S1. A chooses randomly (uniformly distributed) $r \in Z_q$ and blinds the message M by computing $M'=rH(M)$. A sends M' and $w_i = \prod_{j\in S, j\neq i} \frac{j}{j-i}$ to every signer L_i for i=1,2,...,t.

S2. Signer L_i, after receiving M', computes a partial signature σ_i and sends it back to the user, where $\sigma_i = s_i w_i M'$

S3. A, after receiving σ_i, verifies σ_i by:

$$e(\sigma_i,P) = e(w_iM',Q_i) \qquad (3)$$

If Eq.(3) does not hold, A sends M' again to get the correct σ_i. Otherwise, A computes the signature σ on M:

$$\sigma = r^{-1} \sum_{j\in S} \sigma_j, \qquad (4)$$

3. Verification *TBV*

The signature σ on a message M is accepted if and only if:

$$e(\sigma,P) = e(H(M),Q) \qquad (5)$$

4. Correctness

Firstly, the correctness of the signature scheme must involve the correctness of verification of Eq.(3) in *TBS* protocol. That means the partial signature σ_i is valid if the i-th signer is honest. We have:

$e(\sigma_i,P) = e(w_iM',Q_i) = e(w_iM',s_iP) = e(w_is_iM',P)$

Secondly, we verify the correctness of the threshold blind signature scheme. The scheme signature σ has a form:

$$\sigma = r^{-1} \sum_{j\in S} \sigma_i = r^{-1} \sum_{j\in S} s_i \prod_{j\in S, j\neq i} \frac{j}{j-i} \mathcal{M}(0)$$
$$= r^{-1} r s \mathcal{H}(\mathcal{M}) = s\mathcal{H}(\mathcal{M})$$

We can get above result by Lagrange interpolation.

The verification using Eq.(5) gives us:

$e(\sigma,P)=e(H(M),Q)=e(H(M),sP)= e(sH(M), P)$

Hence, if σ is the valid signature on M, the verification always holds.

IV. Security analysis

We analyze security of the proposed signature scheme in this session. First, we give definition of the security.

Definition 1. *Let* TBS=*(TBK, TBS, TBV) be the threshold blind signature scheme.* TBS *is secure threshold blind signature scheme if:*

1. Unforgeability. *No adversary who corrupts at most t-1 signers, with non-negligible probability, can do one-more forgery attack, that is an adversary cannot produce more than l signature after executing TBS protocol l times.*

2. Robustness. *Even there exists an adversary who can corrupt up to t-1 signers, the TBK and TBS protocols complete successfully.*

1. Blindness

First of all, we state that our proposed signature scheme has blind property. Since r is chosen randomly from Z_q, therefore $M' = rH(M)$ is also a random element in group G_1. Thus signers only receive the random information from the user and there is no way to know the original message.

2. Robustness

The robustness of the proposed signature scheme is shown by the following theorem:

Theorem 1. (Robustness) *The threshold blind signature scheme* TBS *is robust for an adversary who can corrupt t-1 signers among n signers such that* $n \geq 2t-1$ *signers.*

Proof. Even t-1 signers are corrupted, there always exists any subset of t signers can construct unique the secret key s uniformly distributed in Z_q. Thus *TBK* completes successfully. Similarly, in *TBS*, every partial signature is verified by Eq. (3), and so is the signature σ - Eq. (5). Hence, *TBS* completes successfully. ■

3. Unforgeability

To prove unforgeability of TBS scheme, first we have to prove that the underlying signature scheme BGS is unforgeable and then prove that TBS scheme is simulatable.

1) Unforgeability

Differ from the standard signatures, the notion of unforgeablity of the blind signatures is about *one-more-forgery* [19]. The proof of unforgeability of BGS based on "chosen-target CDH problem and assumption" given below:

Definition 2. (CT-CDH) *Let G_1 be GDH group of prime order q and P is a generator of G_1. Let s be a random element of Z_q and $Q=sP$. Let $H:\{0,1\}^* \rightarrow G_1$ be a random hash function. The adversary B is given input (q,P,Q,H) and has access to the target oracle T_{G1} that returns a random point U_i in G_1 and the helper oracle cdh-s(). Let q_T and q_H be the number of queries B made to the target oracle and the helper oracle, respectively. The advantage of the adversary attacking the chosen-target CDH problem $Adv^{ct\text{-}cdh}_{G1}(B)$ is defined as the probability of B to output a set of l pairs $((V_1,j_1), (V_2,j_2),...,(V_l,j_l))$, for all $i=1,2,..,l$ $\exists$ $j_i = 1,2,..,q_T$ such that $V_i=sU_{j_i}$ where all V_i are distinct and $q_H < q_T$.*

The chosen-target CDH assumption states that there is no polynomial-time adversary B with non-negligible $Adv^{ct\text{-}cdh}_{G1}(B)$.

We have the following theorem:

Theorem 2. *If the chosen-target CDH assumption is true in the group G_1 then the blind signature scheme* BGS *is secure against one-more-forgery under chosen message attack.*

Proof.(Sketch) If there is any polynomial-time adversary A attacking BGS against one-more forgery under chosen message attack, we always construct a polynomial-time adversary B who can solve CT-CDH problem such that $Adv^{blind}_{BGS}(A) = Adv^{ct\text{-}cdh}_{G1}(B)$. ■

2) Simulatable

The simulatable condition means that there exists simulators can simulate the view of an adversary on the execution of *TBK* and *TBS* protocols. Since *TBK* was based on DKG, we can have the same simulator as in [8]. For *TBS* protocol, we construct a simulator *SIM* which can simulate the view of an adversary A, whose view is $VIEW_A(TBS(s_1,s_2,...s_n,M,Q),\sigma)$, in the running of *TBS* protocol. A also can corrupts up to t-1 signers.

The input to *SIM* is a public key Q, a message M, a signature σ on M and secret shares $s_1, s_2,...,s_{t-1}$ of corrupted signers.

1. *SIM* chooses $r' \in Z_q$ randomly.
2. *SIM* computes partial signature:

   $\sigma_i = r' s_i \omega_i H(M)$ for $1 \leq i \leq t-1$.
3. For an uncorrupted signer, *SIM* computes partial signature as $\sigma_t = r\sigma - \sum_{i=1}^{t-1} \sigma_i$

Denote the information produced by the above simulator *SIM* as $SIM(M, Q, s_1, s_2,...,s_{t-1})$. The following theorem shows the simulatable condition of *TBS* scheme:

Theorem 3. $VIEW_A(TBS(s_1,s_2,...s_n,M,Q),\sigma)$ *and* $SIM(M, Q, s_1, s_2,...,s_{t-1})$ *have the same*

probability distribution.

Proof. (Sketch) By comparing the information produced by *SIM* and *TBS*, we can easily see that it is polynomially distinguishable the view of A and the output of *SIM*. ∎

Theorem 4. *The threshold blind signature scheme* TBS *is as secure as the blind signature scheme* BGS *against one-more-forgery under chosen message attack.*

Proof. This comes immediately from Theorems 2 and 3 ∎

By Theorems 1 and 4 we can state that TBS is secure and robust threshold blind signature scheme.

V. Performance

We compare the proposed signature scheme with the previous ones KKL01 [14], LJY99 [15].

Operation	KKL01	LJY99	Our scheme
A_m	2t+1	2t+1	0
M	t+5	2n-t+6	1
E	6	8	0
I	0	0	1
A	N/A	N/A	t-1
S	N/A	N/A	2

Table 1: Computation at a user's side

Operation	KKL01	LJY99	Our scheme
A_m	2	2(n-t+1)	0
M	5	2n-1	1
E	8	6	0
I	0	0	0
A	N/A	N/A	0
S	N/A	N/A	1

Table 2: Computation at a singer's side

In these tables, A_m, M, E and I mean modular addition, multiplication, exponentiation and inversion, respectively. A and S denote point addition and scalar multiplication on an elliptic curve over a finite field. N/A means Not Available.

Compare to previous schemes, our scheme is very efficient in term of the signature size, especially if the point compression technique is applied.

VI. Concluding remarks

We have proposed a secure and robust threshold blind signature scheme based on bilinear pairings. The scheme was proven as secure as the blind GDH signature scheme in the random oracle model. In addition, our scheme exhibits robustness. Even there exists an adversary who can corrupt up to t-1 signers among $n \geq 2t$-1 signers, the scheme still completes successfully. Moreover, our scheme achieves efficiency in a sense of the signature size.

Further more, we can add proactive property to our signature scheme using technique [11], [10]. This property makes the signature scheme more secure by coping with mobile adversary. Using DKG, we can achieve proactive property more secure, since original techniques used insecure distribution method as pointed out in [9].

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, pp. 354-369, 2002.

[2] M. Bellare, C. Namprempre, D. Pointcheval and M.Semanko, "The One-More-RSA-Inversion Problems and the Security of Chaum's Blind Signature Scheme," *Cryptology ePrint Archive* - 2001/02.

[3] D. Boneh and M. Franklin, "ID-based Encryption from the Weil-pairing," *Advances in Cryptology - Crypto'2001*, LNCS 2139, Springer-Verlag, pp. 213-229, 2001.

[4] D. Boneh, B. Lynn, and H. Shacham, "Short Signatures from the Weil-pairing," *Advances in Cryptology - Asiacrypt'2001*, LNCS 2248, Springer-Verlag, pp. 514-532, 2001.

[5] A. Boldyreva, "Threshold Signature, Multisignature and Blind Signature Schemes Based on the Gap-Diffie-Hellman-group Signature Scheme," *Public Key Cryptography - PKC 2003*, LNCS 2567, Springer-Verlag, pp. 31-46, 2003.

[6] D. Chaum, "Blind Signatures for Untraceable Payments," *Proc. of Crypto'82*, LNCS 1440, pp. 199-203, Springer-Verlag, 1983.

[7] Y. Desmedt and Y. Frankel, "Theshold

Cryptosystems," *Advances in Cryptology - Crypto'89*, LNCS 435, pp.307-315, Springer-Verlag, 1990.

[8] R. Gennaro, S. Jarecki, H. Krawczyk and T. Rabin, "Robust Threshold DDS Signatures," *Advances in Cryptology - Eurocrypt'96*, LNCS 1070, Springer-Verlag, pp. 354-371, 1996.

[9] R. Gennaro, S. Jarecki, H. Krawczyk and T. Rabin, "Secure Distributed Key Generation for Discrete-log Based Cryptosystems," *Advances in Cryptology - Eurocrypt'99*, LNCS 1592, Springer-Verlag, pp. 295-310, 1999.

[10] A. Herzberg, M. Jakobsson, S. Jarecki, H. Krawczyk, and M. Yung, "Proactive public key and signature systems," *ACM Conference on Computers and Communication Security - CCS'97*, ACM Press, pp. 100-110, 1997.

[11] A. Herzberg, S. Jarecki, H. Krawczyk, and M. Yung, "Proactive Secret Sharing Or: How to Cope With Perpetual Leakage," *Advances in Cryptology - Crypto'95*, LNCS 963, Springer-Verlag, pp. 339-352, 1999.

[12] F. Hess, G. Seroussi and N. Smart, "Two Topics in Hyperelliptic Cryptography," *SAC'2001*, LNCS 2259, Springer-Verlag, pp. 181-189, 2001.

[13] A. Joux and K. Nguyen, "Separating Decision Diffie-Hellman from Diffie-Hellman in Cryptographic Groups," *Cryptology ePrint Archive* - 2001/03.

[14] J. Kim, K. Kim and C. Lee, "An Efficient and Provably Secure Threshold Blind Signature," *International Conference on Information Security and Cryptology - ICISC'2001*, LNCS 2288, Springer-Verlag, pp. 318-327, 2002.

[15] C.L. Lei, W.S. Juang and P.L. Yu, "Provably Secure Blind Threshold Signatures Based on Discrete Logarithm," *National Computer Symposium 1999*, pp. C198-C205, 1999.

[16] M. Ohkubo, F. Miura, M Abe, A. Fujioka and T. Okamoto, "An Improvement on a Practical Secret Voting Scheme," *Information Security Workshop - ISW'99*, LNCS 1729, Springer-Verlag, pp. 225-234, 1999.

[17] T.P. Pedersen, "A Threshold Cryptosystem without a Trusted Party," *Advances in Cryptology - Eurocrypt'91*, LNCS 547, Springer-Verlag, pp. 522-526, 1991.

[18] T.P. Pedersen, "Non-interactive and Information-theoretic Secure Verifiable Secret Sharing," *Advances in Cryptology - Crypto'91*, LNCS 576, Springer-Verlag, pp. 129-140, 1991.

[19] D. Pointcheval and J. Stern, "Provably Secure Blind Signature Schemes," *Advances in Cryptology - Asiacrypt'96*, LNCS 1163, Springer-Verlag, pp. 252-265, 1996.

[20] D. Pointcheval and J. Stern, "Security Argument for Digital Signatures and Blind Signatures," *Journal of Cryptology*, Springer-Verlag, Vol.13 No.3, pp. 361-396, 2000.

[21] A. Shamir, "How to Share a Secret," *Commmunication of the ACM*, Vol.22, No.11, pp. 612-613, Nov.1979.

[22] V. Shoup, "Practical Threshold Signatures," *Advances in Cryptology - Eurocrypt'2000*, LNCS 1807, Springer-Verlag, pp. 207-220, 2000.

[23] F. Zhang and K. Kim, "ID-Based Blind Signature and Ring Signature from Pairings," *Advances in Cryptology - Asiacrypt'2002*, LNCS 2501, Springer--Verlag, pp. 533-547, 2002.