

# Robust ID-based Threshold Signcryption Scheme From Pairings

Shanshan Duan  
Department of Computer  
Science and Engineering  
Shanghai Jiao Tong University  
1954 Huashang Road,  
Shanghai, P.R. China  
dss@sjtu.edu.cn

Zhenfu Cao  
Department of Computer  
Science and Engineering  
Shanghai Jiao Tong University  
1954 Huashang Road,  
Shanghai, P.R. China  
zfcaco@cs.sjtu.edu.cn

Rongxing Lu  
Department of Computer  
Science and Engineering  
Shanghai Jiao Tong University  
1954 Huashang Road,  
Shanghai, P.R. China  
rxlu@cs.sjtu.edu.cn

## ABSTRACT

Recently bilinear pairings on elliptic curves have raised great interest in cryptographic community. Based on their good properties, many excellent ID-based cryptographic schemes have been proposed. However, in these proposed schemes, the private key generator should be assumed trusted, while in real environment, this assumption does not always hold. To overcome this weakness, in this paper, we will use the threshold technology to devise a secure ID-based signcryption scheme. Since the threshold technology is adopted not only in the master key management but also in the group signature, our scheme can achieve high security and resist some malicious attacks under a certain threshold.

## Categories and Subject Descriptors

[Cryptography]

### General Terms

Security, Theory

### Keywords

Identity-based cryptography, Threshold scheme, Signcryption, Bilinear pairings

## 1. INTRODUCTION

Identity based cryptosystem was introduced by Shamir in 1984[1]. The main idea was to get rid of public key certificates by allowing the user's public key to be the binary sequence corresponding to some information identifying him, such as name, IP address and so on, while the private key is calculated by a trusted authority called private key generator(PKG). After the concept was proposed, several identity-based encryption and signature schemes were devised[2, 3, 4]. However, none of them are fully functioning until Boneh

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage, and that copies bear this notice and the full citation on the first page. To copy otherwise, or republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee.

*Proceedings of 2004 International Conference on Information Security, Shanghai, China*

Copyright 2004 ACM ISBN: 1-58113-955-1

and Franklin presented an identity-based encryption based on the Weil pairing over elliptic curves[5]. Since then, ID-based cryptography based on bilinear pairings has become an active area and many identity-based schemes using pairings have been put forward[6, 7, 8, 9].

A new type of cryptographic primitive called 'signcryption' which combines a function of digital signature scheme with encryption algorithm, was introduced by Zheng in [10]. Signcryption not only provides authenticity and confidentiality in a single step, but also gives more efficient computations than traditional sign-then-encrypt approach. So, it has caught many people's eye. Several efficient signcryption schemes have been proposed since 1997[10, 11, 12, 13] and the first identity-based signcryption scheme has also been published by B. Lynn in 2002[14].

In some scenarios, a communication is carried out between groups rather than individuals. To guarantee authenticity, the sender uses threshold signature scheme. If, at the same time, he hopes to ensure the confidentiality of the message, he has to perform encryption. Simply using the traditional sign-then-encrypt approach is not satisfying because of its high computational cost. To deal with such a situation, we drew inspiration from the mentioned above and proposed an efficient ID-based  $(k, n)$  threshold signcryption scheme, which can separate universal signature verification from designated message recovery. Such good properties make it useful in some particular applications. Furthermore, a distinguishing feature of our scheme is that it applies a  $(u, m)$  threshold scheme in the master key management, which makes the master key to be jointly generated by PKGs so that a single misfortune can no longer make the master key inaccessible. Another important aspect of our scheme is that robustness is our main concern. Especially, if a user is an organization entity, the private key is constructed and then distributed to all the members by a PKG private-key distributor called  $CLK_p$ . While in signing phase, the organization clerk  $CLK_s$  with the responsibility for signature shouldn't be able to recover the private key from what he gathered, say nothing of the master key. Under such condition, achieving robustness seems a little difficult. The following part will describe how we successfully settle it in detail.

The rest of the paper is organized as follows. Background

information is given in Section 2. Our proposed scheme is presented in Section 3. Security analysis is discussed in Section 4. Conclusions are drawn in Section 5.

## 2. BACKGROUND INFORMATION

### 2.1 Bilinear Maps and Related Mathematical Problems

We consider two groups  $G_1$  (additive) and  $G_2$  (multiplicative) of the same prime order  $q$ . We need bilinear maps  $\hat{e} : G_1 \times G_1 \rightarrow G_2$  satisfying the following properties:

1.  $\forall P, Q \in G_1, \forall a, b \in \mathbb{Z}_q^*$ , we have  $\hat{e}(aP, bQ) = \hat{e}(P, Q)^{ab}$ .
2. Non-degeneracy: for any point  $P \in G_1$ ,  $\hat{e}(P, Q) = 1$  for all  $Q \in G_1$  iff  $P = \mathcal{O}$ .
3. Computability: there exists an effective algorithm to compute  $\hat{e}(P, Q), \forall P, Q \in G_1$ .

$G_1$  is a cyclic additive group, we assume that multiplication and inversion in  $G_1$  can be computed in a unit time. At the same time, we are interested in the following mathematical problems. Let  $P, Q$  be elements of  $G_1$  and  $a, b, c$  be elements of  $\mathbb{Z}_q^*$ .

1. Discrete Logarithm(DL) problem: Given  $P, Q$ , find an integer  $n$  such that  $P = nQ$ , whenever such  $n$  exists.
2. Computation Diffie-Hellman Problem (CDHP): Given  $(P, aP, bP)$ , compute  $abP$ .
3. Decisional Diffie-Hellman Problem (DDHP): Given  $(P, aP, bP, cP)$ , decide whether  $c = ab$  in  $\mathbb{Z}_q^*$ .
4. Gap Diffie-Hellman Problem (GDHP): A class of problem where the CDH problem hard but DDH is easy.

We call  $G$  a GDH group if DDHP can be solved in polynomial time but no probabilistic algorithm can solve CDHP with non-negligible advantage within polynomial time. Such group can be found on super singular or hyper elliptic curves over finite field. The Weil pairing and the Tate pairing are admissible applications satisfying the properties mentioned above.

### 2.2 Threshold Cryptography Scheme

The idea behind the  $(k, n)$  threshold cryptography approach [15, 16, 17, 18] is to distribute secret information (i.e. a secret key) and computation (i.e. signature generation or decryption) between  $n$  parties in order to remove single point of failure. The goal is to allow any subset of not less than  $k$  parties to jointly reconstruct a secret and perform computation while preserving security even up to  $k - 1$  parties are corrupted. But in some scenarios, if we simply apply threshold scheme to share the secret, it is not robust. Because for the first time, the clerk can resume the private key by  $k$  sub-keys he collected, later he will not need  $k$  members present again.

In the following part, we use distinct secret sharing scheme from those mentioned above to make sure the robustness of our scheme in which threshold technology has been applied twice.

## 3. THE TWO THRESHOLDS SIGNCRYPTION SCHEME

### 3.1 Background of Our Proposed Scheme

Assume  $m$  PKGs ( $PKG_1, \dots, PKG_m$ ) are collectively in charge of the master key. When receiving a private key extraction request, only not less than  $u$  ( $2u \leq m - 1$ ) PKGs are involved, will the PKG clerk  $CLK_p$  return the just computed private key via secure channel.  $A$  is an organization entity composed of  $n$  members. If someone denoted by  $Bob$  asks  $A$  to sign a message, any  $k$  effective members can generate a valid signature on  $A$ 's behalf. Later, anyone can perform verification using  $A$ 's identity while only  $Bob$  can recover the message with his private key.

### 3.2 Notation

Let  $G_1$  and  $G_2$  be additive and multiplicative groups of the same large prime order  $q$ . Here  $q$  is a large prime. Assume  $G_1$  be a GDH group, and the bilinear map is given as  $\hat{e} : G_1 \times G_1 \rightarrow G_2$ . Let  $ID$  be a string denoting the identity of a user and  $H, H_1$  and  $H_2$  be public cryptographic hash functions. We require:  $H : G_2 \rightarrow \{0, 1\}^n$ ,  $H_1 : \{0, 1\}^* \rightarrow G_1$  and  $H_2 : \{0, 1\}^n \rightarrow G_1$ .

### 3.3 Description of the Scheme

Just like classical IBE system, our scheme is composed of four algorithms: Setup, Extract, Signcrypt, Verify and Decrypt.

#### Setup:

Let  $P$  be a generator of  $G_1$ . The PKG clerk  $CLK_p$  does the followings:

1. Chooses a random  $s \in \mathbb{Z}_q^*$  as the master key, sets  $P_{pub} = sP$  and makes  $P_{pub}$  publicly known.
2. Then he picks up some random coefficients  $a_i \in \mathbb{Z}_q^*$  for  $1 \leq i \leq u - 1$  and create a polynomial  $F(x) = s + a_1x + a_2x^2 + \dots + a_{u-1}x^{u-1}$  such that  $F(0) = s$ . Calculate  $F(i)$  ( $i = 1, 2, \dots, m$ ) and sent them secretly to the corresponding PKG  $PKG_i$ .
3. Each  $PKG_i$  computes  $F(i)P$  and sends it to  $CLK_p$  as a reply. To prevent attacks on the master key,  $CLK_p$  destroys  $s$  after all these have been done.

#### Extract:

Organization  $A$  sends its identity information  $IDA \in \{0, 1\}^*$  to at least  $u$  PKGs. Without loss of generality, assume  $PKG_1, \dots, PKG_u$  are gonging to jointly generate the private key. Each of them independently computes  $A$ 's public key as  $Q_{IDA} = H_1(IDA)$  and makes sub-private key  $\beta_i = F(i)Q_{IDA}$  for and then sends it to  $CLK_p$ .  $CLK_p$  can use the following equation to verify each sub-private key:

$$\hat{e}(F(i)Q_{IDA}, P) = \hat{e}(F(i)P, Q_{IDA})$$

If the equation does hold, the sub-private key can be accepted.

$CLK_p$  constructs  $A$ 's private key:

$$S_{IDA} = \sum_{i=1}^u \lambda_i \beta_i = \sum_{i=1}^u \lambda_i F(i) Q_{IDA} = s Q_{IDA}.$$

$$\text{where } \lambda_i = \frac{\prod_{i=1, j \neq i}^u (0-j)}{\prod_{i=1, j \neq i}^u (i-j)} \pmod{q}.$$

And then he performs steps as follows:

1. Randomly choose  $r \in Z_q^*$ , computes  $r^{-1}$  as the inverse of  $r$  in  $Z_q^*$ ,  $rsQ_{IDA}$ ,  $r^{-1}P$ ,  $r^{-1}P_{pub}$  and broadcast  $rsQ_{IDA}$ ,  $r^{-1}P$ ,  $r^{-1}P_{pub}$  in organization  $A$ .
2. Picks up a polynomial  $f(x)$  over  $Z_q^*$  of degree  $k-1$  randomly such that  $f(0) = r$ . Denote  $n$  members involved in organization  $A$ , each member  $m_i$  has his index  $i$  ( $i = 1, 2, \dots, n$ ). Compute  $f(i)$  ( $i = 1, \dots, n$ ) and send it secretly to the corresponding member  $m_i$ .

After all the steps above have been finished, the public key and the private key of  $A$  are  $Q_{IDA}$  and  $sQ_{IDA}$  respectively. The private share of each member  $m_i$  is  $f(i)$  and the corresponding public share is  $f(i)P$ .

### Signature and Message Encryption:

$Bob$  requests organization  $A$  to sign message  $M \in \{0, 1\}^*$ . The followings are carried out in sequence:

The clerk  $CLK_s$  with responsibility for signcryption performs the following steps:

1. Randomly choose  $t \in Z_q^*$  and compute  $t^{-1}$ , which is the inverse of  $t$  in  $Z_q^*$ .
2. Compute  $R = t^{-1}r^{-1}P$  and  $R_1 = t^{-1}r^{-1}P_{pub} = t^{-1}r^{-1}sP$ .
3. Broadcast  $R_1$  in the organization.

Assume members  $m_i$  ( $i = 1, 2, \dots, k$ ) are those who want to generate a signature collectively. Each of them makes his sub-signature like this:

1. Compute  $a = H(\hat{e}(Q_{IDB}, R_1)) \oplus M$  and  $B = H_2(a) \in G_1$ .
2. Sign the message with his sub-key:  $\delta_i = f(i)B$

Later, they submit  $\delta_i$  ( $i = 1, \dots, k$ ) to  $CLK_s$  who then performs the followings:

1. Verify each sub-signature by checking whether the equation holds or not.

$$\hat{e}(\delta_i, P) = \hat{e}(f(i)P, B) \quad (i = 1, \dots, k)$$

The sub-signature will be accepted if the equation is valid, and rejected otherwise.

2. Generate the whole signcryption with  $\delta_i$  ( $i = 1, 2, \dots, k$ ), compute  $b, C, D, E$  as

$$b = \sum_{i=1}^k \lambda_i \delta_i = \sum_{i=1}^k \lambda_i f(i)B = rB$$

$$\text{where } \lambda_i = \frac{\prod_{i=1, j \neq i}^k (0-j)}{\prod_{i=1, j \neq i}^k (i-j)} \pmod{q}$$

$$C = tb = trB$$

$$D = t(rsQ_{IDA})$$

$$E = C + D$$

3. Send  $(R, a, E)$  to  $Bob$ .

### Signature Verification & Message Decryption:

#### I. Signature Verification:

Anyone can verify  $A$ 's signature as follows:

1. Apply hash function  $H_2$  to produce  $H_2(a)$
2. Check whether  $\hat{e}(E, R) = \hat{e}(H_2(a), P)\hat{e}(Q_{IDA}, P_{pub})$  holds or not. If it does hold,  $(R, a, E)$  will be accepted. Since,

$$\hat{e}(E, R) = \hat{e}(C + D, R)$$

$$= \hat{e}(C, R)\hat{e}(D, R)$$

$$= \hat{e}(trB, t^{-1}r^{-1}P)\hat{e}(trsQ_{IDA}, t^{-1}r^{-1}P)$$

$$= \hat{e}(B, P)\hat{e}(sQ_{IDA}, P)$$

$$= \hat{e}(H_2(a), P)\hat{e}(Q_{IDA}, P_{pub})$$

#### II. Message Decryption:

Once  $(R, a, E)$  has been validated,  $Bob$  can use his private key  $S_{IDB}$  to recover the message:

$$a \oplus H(\hat{e}(S_{IDB}, R))$$

$$= H(\hat{e}(Q_{IDB}, R_1)) \oplus M \oplus H(\hat{e}(S_{IDB}, R))$$

$$= M$$

## 4. SECURITY ANALYSIS

### 4.1 Correctness of the Scheme

From the discussion in section 3, if  $A$  and  $Bob$  both follow the steps of the proposed scheme, anyone can verify the signature. At the same time,  $Bob$  can recover the message using his private key. Therefore, the scheme can be implemented correctly.

## 4.2 Security of the Scheme

Like the other signcryption schemes, our scheme is a good combination of digital signature and public-key encryption. But unlike them, our scheme can separate signature verification from message recovery. So, to prove its security, we only need to analyze each part respectively. Firstly, consider the signature part. Note that  $(R, a, E)$  is similar to Paterson's ID-based signature scheme whose security has been proved in the literature[8]. According to his work, we can conclude that the signature part of our scheme is also secure. Secondly, after the validation is finished, *Bob* can recover the message using his private key from  $(a, E)$ , which is actually an ID-based encryption proposed by Boneh and Franklin[5]. In the literature[5], their scheme has also been proved to be secure, then so is our encryption part. In sum, our signcryption scheme is secure.

Although our scheme can be viewed somewhat as a combination of Boneh and Franklin's ID-based encryption and Paterson's signature scheme, it does have its own unique secure properties. The most prominent one is that the master key is under the protection of a  $(u, m)$  threshold scheme. Firstly, according to Shamir's secret sharing technology, any  $(u - 1)$  members cannot reconstruct the master key  $s$  from their secret shares. Secondly, the master key is not exposed in users' private keys generation process. So, we can guarantee that the master key is secure.

Besides, the master key  $s$  can resist any cooperating attack of all members in one organization. Assume that organization  $A$  wants to attack PKG, all members' sub-private keys  $f(i)$  ( $1 \leq i \leq n$ ) are published. Then it is easy to compute  $r : r = \sum_{i=1}^k \lambda_i f(i)$  where  $\lambda_i = \frac{\prod_{i=1, j \neq i}^k (0-j)}{\prod_{i=1, j \neq i}^k (i-j)} \pmod{q}$ . However, even  $r$  is known, it is still impossible to get  $s$  from  $rsQ_{ID}$  since discrete logarithm problem is hard in  $G_1$ . Thus, from this point of view, the master key is also secure.

In previously proposed threshold signature schemes, if threshold technology is simply applied in sharing a secret, achieving robustness is rather difficult. When making the first signature, the clerk is able to recover the private key. Next time he will not again need  $k$  (i.e. threshold) sub keys. Better than them, in our  $(k, n)$  threshold signature scheme, computing a signature does not expose the private key.  $b = \sum_{i=1}^k \lambda_i \delta_i = rB$  ( $B \in G_1$ ) is the whole signature. Since the discrete logarithm problem in  $G_1$  is hard and  $r$  is chosen randomly in  $Z_q^*$ , it is difficult to get  $r$  from  $b = rB$ . Without  $r$ , the private key  $sQ_{ID}$  can't be deduced from  $rsQ_{ID}$ . Therefore, our scheme can guarantee robustness.

## 5. CONCLUSIONS

We have presented an identity-based threshold signcryption scheme whose prominent merit is robustness. The master key  $s$  is divided into  $m$  pieces. Even complete knowledge of  $u - 1$  ( $2u \leq m - 1$ ) pieces reveals absolutely no information about it. At the same time, an organization's private key is protected under our  $(k, n)$  threshold signature scheme. Even if  $k - 1$  dishonest members of an organization collude, the private key is still secure. Other than robustness, practicability is another merit. Our signcryption scheme can be divided into universal signature verification and designated

message recovery. So, it can be used in some particular scenarios.

## 6. ACKNOWLEDGMENTS

This research is supported by the National Natural Science Foundation of China for Distinguished Young Scholars under Grant No. 60225007, the National Research Fund for the Doctoral Program of Higher Education of China under Grant No. 20020248024, and the Science and Technology Research Project of Shanghai under Grant Nos. 04JC14055 and 046407067.

## 7. REFERENCES

- [1] A. Shamir. Identity-based cryptosystems and signature schemes. In *Advance in cryptology-crypto 84, LNCS 196*, pages 47–53. Springer-Verlag, 1984.
- [2] A. Fiat and A. Shamir. How to prove yourself: Practical solutions to identification and signature problems. In *Advance in cryptology-crypto 86, LNCS 0263*, pages 186–194. Springer, 1986.
- [3] L. Guillou and J.-J. Quisquater. A paradoxical identity-based signature scheme resulting from zero-knowledge. In *Advance in cryptology-crypto 88, LNCS 0403*, pages 216–231. Springer, 1988.
- [4] C.Cocks. An identity based encryption scheme based on quadratic residues. In *In cryptography and coding, LNCS 2260*, pages 360–363. Springer-Verlag, 2001.
- [5] D.Boneh and M.Franklin. Identity-based encryption from the weil pairing in advance. In *cryptology-crypto 2001, LNCS 2139*, pages 213–229. Springer-Verlag, 2001.
- [6] J.C.Cha and J.H.Cheon. An identity-based signature from gap diffe-hellman groups. In *to appear in proceedings of PKC 2003*. Springer-Verlag, 2003.
- [7] F.Hess. Efficient identity based signature schemes based on pairings. In *to appear in proceedings of SAC 2002*. Springer-Verlag, 2002.
- [8] K.G.Paterson. ID-based signatures from pairings on elliptic curves. *Cryptology eprint archive, Report 2002/004*, available at <http://eprint.iacr.org/>, 2002.
- [9] B. D.Boneh and H.Shancham. Short signatures from the weil pairing. In *Proceedings of Asiacrypt 2001, LNCS 2248*, pages 514–532. Springer-Verlag, 2001.
- [10] B. D.Boneh and H.Shancham. Digital signcryption or how to achieve  $\text{cost}(\text{signature} \& \text{encryption}) \ll \text{cost}(\text{signature}) + \text{cost}(\text{encryption})$ . In *Advance in Cryptology CCRTPTO97, LNCS 1294*, pages 165–179. Springer-Verlag, 1997.
- [11] B. D.Boneh and H.Shancham. Efficient signcryption scheme on elliptic curves. In *Proc. of IFIP/SEC98*. Chapman&Hall, 1998.
- [12] B. D.Boneh and H.Shancham. New signcryption schemes based on kcdsa. In *Proc. of ICISC01, LNCS 2288*, pages 305–317. Springer-Verlag, 2001.

- [13] Y. J.Back, R.Steinfeld. Formal proofs for the security of signcryption. In *Proc. of PKC02, LNCS 2274*, pages 81–98. Springer-Verlag, 2002.
- [14] J. Malone-Lee. Identity based signcryption. <http://eprint.iacr.org/2002/0798>.
- [15] S. Y.Desmedt and Y. Frankel. Shared generation of authentications and signatures(extended abstract). In *Advances in Cryptology CCRTPTO91 LNCS 576*, pages 457–469. Springer-Verlag, 1991.
- [16] H. K. R.Gennaro, S.Jarecki and T.Rabin. Robust threshold dss signatures. In *Advances in Cryptology CEUROCRYPT96, LNCS 1070*, pages 354–371. Springer-Verlag, 1996.
- [17] H. K. R.Gennaro, S.Jarecki and T.Rabin. Robust and efficient sharing of rsa functions. In *Advances in Cryptology CEUROCRYPT96, LNCS 1109*, pages 157–172. Springer-Verlag, 1996.
- [18] D. Stinson and R.Strobl. Provable secure distributed schnorr signatures and a (t,u) threshold scheme for implicit certificates. In *Information Security and Privacy (ACISP01), LNCS 2119*, pages 417–434. Springer-Verlag, 2001.