

An Efficient Multi-sender Identity Based Threshold Signcryption with Public Verifiability

Wen Chen and Feiyu Lei

Department of Communications and Electronic Engineering
School of Information Science and Technology, Donghua University
1882 Yanan Road, Shanghai, China, 200051
wen.chenwen@gmail.com

Abstract

In this paper, we propose a new multi-sender(t, n) identity based signcryption scheme with public verifiability using pairings, and give a security proof about the original scheme in the random oracle model.

1. Introduction

The paper presents a Multi-sender (t, n) identity based threshold signcryption with public verifiability, which contains three important primitives: *threshold cryptography, signcryption, identity based systems*. Threshold cryptography [1] provides for increased security of the distributed platform by distributing protocols among a number of participants. In 1997, Zheng [2] proposed a new primitive called signcryption, which is more efficient than the conventional 'sign-then-encrypt' approach. In 1984, Shamir [3] put forward the idea of identity based cryptosystem. Until 2002, Libert and Quisquater [4] (LQ for short) proposed a new scheme with public verifiability, which was more efficient and produced shorter ciphertext.

In this paper, we use pairing as our maths basis [4]. And the common idea to prove threshold security [5] is that the adversary \mathcal{A} 's view in the threshold setting can be simulated by a simulator θ that runs in the original scheme.

2. Multi-sender Threshold Signcryption Model and Security Requirements

2.1. System Model

Communication Model. We consider a set of n senders $\{P_1, \dots, P_n\}$, indexed $1, \dots, n$, and a recipient *Bob*, and a static adversary \mathcal{A} who can corrupt the set of n senders.

Assumed that the network provides services such as undeniable, point-to-point connections. In addition, the players have access to a dedicated broadcast channel.

System Parameters. Initially, given security parameters k , the Trusted Key Generator (TKG) chooses a groups G_1 of prime order q , a generator P of q , and chooses F_q^* as G_2 , a bilinear map $e : G_1 \times G_1 \rightarrow G_2$, four hash functions $H_1 : \{0, 1\}^* \rightarrow G_1$, $H_2 : G_2 \rightarrow \{0, 1\}^n$, $H_3 : \{0, 1\}^n \times \{0, 1\}^n \rightarrow F_q^*$, and $G : G_2 \rightarrow \{0, 1\}^n$. Then TKG chooses a master key $c \in F_q^*$ and computes $P_{pub} = cP$. The algorithm pair (E, D) is secure symmetric encryption and decryption algorithms respectively. The system's public parameters are: $K = (G_1, G_2, n, e, P, P_{pub}, H_1, H_2, H_3, G)$, where n denotes the size of ciphertext. Given an identity ID , TKG computes the public key $Q_{ID} = H_1(ID) \in G_1$, then sets $d_{ID} = cQ_{ID}$ to be the private key. Alice's key pair is (Q_{ID_A}, d_{ID_A}) . Bob's key pair is (Q_{ID_B}, d_{ID_B}) . Note that we choose the same system parameters as in the LQ scheme [4].

3. The Proposed Threshold Signcryption

We have a set of n senders $\{P_1, \dots, P_n\}$, $t-1$ is the number of corrupted players, such as $n \geq 2t + 1$. Distributed Key Generation and Joint Pedersen Verifiable Secret Sharing in [5] are easily extended to that in the identity based setting. We make use of Distributed Key Generation to generate key pairs d_{ID_A}, Q_{ID_A} and d_{ID_B}, Q_{ID_B} in the identity based setting. Joint Pedersen Verifiable Secret Sharing in the Identity Based setting is used to distribute the randomness x . Finally, each sender P_i obtains the information $(d_{ID_{A_i}}, Q_{ID_{A_i}}, x_i)$. Let *Interpolate* denote the standard Lagrange polynomial interpolation. Then it is possible to compute $v = \text{Interpolate}(v_1, \dots, v_t) = e(Q_{ID_B}, P_{pub})^x$ where $v_i = e(Q_{ID_{A_i}}, P_{pub})^{x_i}$.

We show the threshold signcryption and unsigncryption in the following.

Table 1. Comparison with previous solutions

	Communication Costs	Computational cost
<i>OldScheme</i>	$ H + 2n p + 2n q $	$7nExp.$
<i>OurScheme</i>	$n m + n H + n q $	$nExp.andAnMul.$

Signcryption of m by P_i the Sender:

$$v_i = e(Q_{ID_B}, P_{pub})^{x_i}$$

$$w_i = G(G(v_i))$$

$$t_i = H_2(v_i)$$

$$C_i = E_{t_i}(m)$$

$$R_i = H_3(C_i, w_i, G(m))$$

$$S_i = x_i P_{pub} - R_i d_{ID_{A_i}}$$

Unsigncryption of (C_i, R_i, S_i) by Bob the Recipient:

$$v_i = e(S_i, Q_{ID_B}) \times e(Q_{ID_{A_i}}, d_{ID_B})^{R_i}$$

$$t_i = H_2(v_i)$$

$$\text{decrypts } m = D_{t_i}(C_i)$$

$$w_i = G(G(v_i))$$

$$\text{Accepts } m \text{ only if } R_i = H_3(C_i, w_i, G(m))$$

After collects the t signcryptions (C_i, R_i, S_i) , Bob does as follows:

computes t valid v_i respectively.

$$v = \text{Interpolate}(v_1, \dots, v_t).$$

$$w = G(G(v))$$

$$C = E_{H_2(v)}(m)$$

$$r = H_2(C, w)$$

$$S = \text{Interpolate}(S_1, \dots, S_t)$$

$$R = r \cdot Q_{ID_A}$$

Then he gets the original signcryption (C, R, S) .

4. Efficiency Analysis

We consider that the most expensive operations are paring in G_1 , exponentiation in G_2 (short for Exp.), and multiplication in G_1 (short for Mul.). The multiplications in G_2 are omitted. $|x|$ denotes the number of bits in x . We may see the computation cost $Exp. \simeq Mul.$. **Table 1** shows that our scheme is more efficient than old scheme (a threshold scheme based on traditional Schnorr signature and ElGamal encryption [6]), although with small information expansion.

5. Security Proofs

Confidentiality: We can get the results in the random oracle model through simulation, if an adversary \mathcal{A} has a non-negligible advantage ϵ against the IND-IDSC-CCA security of the proposed scheme TSC when running in a time t and performing q_{SC} **Signcrypt** queries, q_U **Unsigncrypt** queries and q_{H_i} queries to oracles H_i (for $i = 1, 2, 3$), then

there exists an algorithm \mathcal{B} that can solve the DBDH problem in the group \mathbb{G}_1 with a probability $\epsilon' \geq \epsilon - q_U/2^k$ in a time $t' < t + (8q_{SC}q_{H_3} + 4q_U)te$, where te denotes the time required for one pairing evaluation.

Unforgeability: The Unforgeability against an existential forgery for adaptive chosen messages attacks (**EF-IDSC-ACMA**) derives from Hess's identity signature scheme [4]. It is obvious that the adversary doesn't know more information about signature than that in LQ scheme. Under the BDH assumption, the unforgeability of our scheme is as secure as that of LQ scheme.

Public Verifiability: If Alice denies her signcryption, Bob computes and forwards $(C, R, G(v), G(m))$ to a TTP (or anybody). TTP computes $w = G(G(v))$, then verifies $R = H_3(C, w, G(m))$. If the equation holds, TTP says that Alice tells a lie. Therefore, it is computationally feasible for any TTP to settle a dispute between Alice and Bob without divulging Bob's private key and the plain message to anyone besides TTP.

Robustness. In this paper, Bob receives the (C_i, R_i, S_i) only when the verification holds: Accept m only if $R_i = H_3(C_i, w_i)$. The verification detects the corrupted party easily, so that the threshold scheme provides the robustness.

6 Conclusion

Identity based threshold cryptosystem is a useful practical tool to protect system security in the open network, and signcryption is a new primitive to achieve the efficient communication and computation. In this paper, we present a new a multi-sender (t, n) identity based threshold signcryption with public verifiability using pairings. The scheme is secure and efficient.

References

- [1] H. K. Author. Jointly unsigncryptable signcryption scheme. *International Workshop on Information Security Application - WISA 2001*, 2:397–407, 2001.
- [2] L. B. Author. New identity based signcryption based on parings. *Cryptology ePrint Archive, Report 2003/023*, <http://eprint.iacer.org>, February 2003.
- [3] R. Author. Adaptive security for threshold cryptosystems. *Advances in Cryptology-Crypto'99*, Lecture Notes in Computer Science 1666:98–115, 1999.
- [4] S. A. Author. Identity based cryptosystems and signature schemes. *Advances in Cryptology -Crypto'84*, Lecture Notes in Computer Science 0196:47–53, 1984.
- [5] Y. Author. Threshold cryptography. *European Transactions on Telecommunications*, 5(4):449–457, July 1994.
- [6] Y. Z. Author. Digital signcryption or how to achieve cost (signature & encryption) \ll cost(signature) + cost(encryption). *Advances in Cryptology - Crypto'97*, Lecture Notes in Computer Science 1294:165 – 179, 1997.