

A rational threshold signature with hierarchical structure

Xiurong Li^{1*}, Yongquan Cai², Yali Liu³

^{1,2} College of Computer Science and Technology, Beijing University of Technology, Beijing 100124, China

³ School of Science and Technology, Beijing City University, Beijing, China

Received 10 September 2014, www.cmnt.lv

Abstract

Rational secret sharing module combines Game theory with cryptography by taking rational behavior into consideration thus has a wider range of application. We apply rational secret sharing into threshold signature so as to construct a hierarchical structure that is described by extended game. Dynamic game of complete information is applied into partial signature's distribution and reconstruction phase where a probable value is calculated that can maximize the payoff. In each round of the game, secret key is iteratively generated in a way that any forged secret key will be detected by PKG system. Mixed strategy model is adopted instead of pure strategy model to prevent deviation, which is proved to be Nash equilibrium. Correctness and anti-deceive feature is proved. The security is based on solving BDH problem in group so the scheme is high effective and chosen cipher text security.

Keywords: Threshold Signature; Hierarchical Structure; Mixed Strategy Model; Nash Equilibrium

1 Introduction

Traditional m-out-of-n secret sharing scheme was introduced independently by Shamir^[1] and Blakley^[2] in 1979. The idea is: a dealer divides a secret into "shares" s_1, s_2, \dots, s_n , which are distributed among n parties over a secret channel. The required properties are that at least m or more parties can reconstruct the secret s from their shares, but any set of fewer than m parties has no information about s . In the process of reconstruction, each party is supposed to broadcast its share to all others. However, the traditional scheme can't prevent the dealer's and players' cheating.

Chor B^[3] proposed the concept of verifiable secret sharing (VSS). Feldman^[4] and Pedersen^[5] respectively gave a VSS scheme based on Shamir's scheme which can effectively detect cheat of player and the dealer. But the VSS scheme can not take precautions against cheat. Lin^[6] propose a secret sharing protocol to solve the cheating problem without the simultaneous release constraint. But it fails in the last round in which the player who cheats will obtain the secret exclusively.

Recently, the cryptographic community rational secret sharing in game theoretic settings to overcome the problem, whereas we can't solve the program using traditional approach. A series of research works^[7-13] have focused on designing rational secret sharing protocols in a game light. Rational secret sharing was first introduced by Halpern and Teague^[7], whose protocols use the key idea that the only hope of getting a practical mechanism for secret sharing lies in using uncertainty about when the game will end to induce cooperation. Moreover, they think there is no practical mechanism for 2 out of 2 secret sharing. Whereas, we claim that it is possible there are protocols for 2 out of 2 secret sharing? Kol G^[8] proposed a rational secret sharing scheme protocol by some meaningful and meaningless encryptions and secure multiparty computation. However, the share distributed by the dealer

can't be identified by players. In addition, it is possible for rational player to cheat in the process of secure multiparty computation. The solution in reference^[9] does not rely on computational assumptions. Their scheme has information theoretic security. However, their scheme does not have resistance against coalitions. The solutions of [10, 11] constructs the secret sharing scheme based on repeated games, however, every player has high probability to obtain the secret in his last round. So, their solutions are susceptible to backward induction. The solutions of reference [12, 13] require the involvement of some (minimally trusted) external parties during the reconstruction phase, whereas it is very hard to find parties that all the players can trust.

In all traditional threshold signature schemes, signers are divided into two types-the honest one and the malicious one. Based on this, Shamir^[14] firstly raised the concept of ID-based signature which enables the signer generate verification information from identity. Therefore the security has been improved since the first threshold signature^[15] based on secret sharing^[1] in 1992. Paterson^[16] extended the ID-based signature to standard model. While the two types have many limitations, a new type is introduced called the rational one^[18] whose target is to maximize his utility. The player's strategy is influenced by rational thinking where he wants himself only to get the correct secret yet in a legal way. In the next papers^[17-19] more schemes had been raised in this frame.

We combine the secret sharing scheme with threshold signature so that the signers are described as rational. For example, a group of people share a bank account and they have to sign a document collectively to open the coffer. However, each one of them wants to obtain the final signed document to get access to the gold. So the bank has to make sure that they all obtained the gold at the same time. Constructing the signature scheme under rational module can solve the problem above without any deviation. We apply the ID-based hierarchical structure^[20] which is first

raised by Akl, S. G. and Taylor, P. D. [21] with rational secret sharing. In the scheme, players generate their personal secret key through hierarchical mechanism. Extended game model [22] is integrated with this structure to give the condition of Nash Equilibrium [23] of dynamic games of complete information [24]. Eventually, every signer gets the whole signature at the last round.

2 Background Knowledge

2.1 DYNAMIC GAME OF COMPLETE INFORMATION

In a dynamic game of complete information each player acts in a specified order. Former decision is fathomable by the latter one. According to the former player's strategy, the latter player makes his own.

Definition 1(The extended description of the dynamic game). A dynamic game of complete information is as follows:

1. Players set: $i \in \{1, 2, \dots, n\}$;
2. The order of moves: describe when does each player takes their action;
3. Players' action set: $\{s_1, s_2, \dots, s_n\}$;
4. Players' payoff function: $\{u_1, u_2, \dots, u_n\}$;

2.2 ADMISSIBLE PAIRINGS

A pairing is defined as an admissible pairing if it satisfies:

1. Bilinear: for all $P, Q \in G_1$.
2. Non-degeneration: If P is the generator of G_1 , then is the generator of G .
3. Computable: For any $P, Q \in G_1$, can be effectively computed.

2.3 BDH PROBLEM

Assume is a group. $P \in G_1$, aP , bP , are all randomly chosen from where a, b, c are randomly chosen from Z/qZ . The BDH problem is to compute $e(P, P)^{abc}$.

3 The New Scheme

We combine the hierarchical key tree structure with the extended description of the dynamic game, each key nodes is corresponded to a decision point in a dynamic game tree.

Let players' ID set be ID-tuple = $\{ID_1, ID_2, \dots, ID_i\}$. the order of the player in the scheme is randomly generated with the following function by trusted PKG:

$$O(h) = \text{Random}(ID, h), h \text{ is the arbitrary history.}$$

C_0 is the starting node of hierarchical key tree structure. Accordingly, C_1 to C_n are the decision point corresponding to players' ID (assume ID sequence is already corresponded). There exist majorized relations in the hierarchical key tree. That is if $C_i < C_j$ ($i < j$) means C_i majorizes C_j . In a direct majorized relation, the sub node's hierarchical key is computed by its father node.

3.1 INITIALIZATION

Let $e: G_1 \times G_1 \rightarrow G_2$ be a admissible pairing in which P is the generator of group G_1 , A_0 is the identity element. Randomly choose and secret random number s_0 ($s_0 \in Z_q^*$), let $Q_0 = s_0 P_0$. Choose three hash functions H_1, H_2 and H_3 as random oracle. So the system parameters are $(G_1, G_2, e, P_0, Q_0, H_1, H_2)$. PKG will keep H_3 secret to compute all the correlative value.

PKG chooses secret parameter in which to construct a polynomial $f(x) = \sum_{i=0}^q b_i x^i$. Let be the main secret key and $Q = sP_0$.

Compute every sub secret keys as $s_i = f(i)$ ($s_i \in Z_q^*$) to form the threshold secret sharing. Send the sub secret keys to the signers.

3.2 GENERATION OF THE HIERARCHICAL KEY

When all the signers obtain their sub secret key ($s_i \in Z_q^*$), PKG computes as well as the correlative value between two adjacent nodes. The hierarchical keys are generated as follows:

PKG computes $P_1 = H_1(s_0 || r_{0,1}) \in G_1$ to the first sub node, in which is the correlative value of root node and the first node.

Each father node computes $P_i = H_1(ID_{i-1} || r_{i-1,i}) \in G_1$, in which is the correlative value of father node and sub node.

Each father node computes ID_i 's hierarchical key A_i : $A_i = A_{i-1} + S_{i-1} P_i = \sum s_{k-1} P_k$.

Each father node computes ($1 \leq k \leq i-1$).

After the computation, father node will send A_i and all the to their sub node. The rule of communication will be given in the next section. Signing system PKG will verify the correctness of P_i in the generation phase after publishing all the common parameters.

3.3 THE GAME

The hierarchical key structure matches the extended description of dynamic game of complete information. In the game tree, each node stands for the decision point of each signer. There are two strategies for them so from the root node it is a binary tree. Once all the signers compute their partial signature, they will send the signature to others.

For each node, define the payoff of ID_i as follows:

- U_1 defines the payoff receiving the correct partial signature;
- U_2 defines the payoff receiving the forged partial signature;

Obviously $U_1 > U_2$. We assume in each transmission, signer's best interest is to obtain the correct partial signature; their ultimate goal is to obtain all the correct partial signatures.

In a synchronizing channel, every signer follows the rules of transmission in each round:

- (1) If signer ID_i has received the hierarchical secret key from father node, he verifies the secret key and

computes the partial signature. Then broadcasts the signature and computes the hierarchical secret key for his sub node.

- (2) If any broadcasted partial signatures or hierarchical secret key are not well received, the game stops.

Because in this game tree signers are absolutely aware of the information of the former decisions, they take their moves in a specified order, so the game is a dynamic game of complete information.

Consider the pure strategy model^[25]. Signer broadcasts with the probability of 0 or 1. If all the signers have sent their hierarchical secret keys, then the last signer will not broadcast his partial signature as he is the only one to get all the partial signatures. According to backward induction^[26], no one will send the hierarchical secret key. Then finally reach a Nash equilibrium that every one deviates.

So we consider the mixed strategy model^[27]. The rules are as follows:

- (1) Each node computes and sends the hierarchical secret key as defined, but broadcasts their partial signature in a way that the correct one is sent with probability α ($0 < \alpha < 1$) while the forged one is sent with probability $1 - \alpha$.
- (2) If any broadcasted partial signatures or hierarchical secret key are not well received, the game stops.
- (3) The last signer computes his partial signature and broadcasts as rule (1). All the signers compute the final signature and verify the correctness. If it's incorrect, replay the game.

4 Scheme Analysis

4. 1 CORRECTNESS OF THE SIGNATURE

- (1) correctness of partial signature

In our scheme, the correctness of the partial signature is verified by the following equation:

$$\begin{aligned} e(P_0, \sigma_i) &= e(P_0, A_i + s_i P_m) \\ &= e(P_0, A_i) e(P_0, s_i P_m) \\ &= e(P_0, s_0 P_1) \cdots e(P_0, s_{i-1} P_i) e(P_0, s_i P_m) \\ &= e(Q_0, P_1) e(Q_i, P_m) \prod_{j=2}^i e(Q_{j-1}, P_j) \end{aligned}$$

- (2) correctness of final signature

In our scheme, the correctness of the final signature is verified by the following equation:

$$\begin{aligned} e(P_0, \sigma) &= e(P_0, \sum_{i=1}^i A_i \eta_i + s P_m) \\ &= e(P_0, A_1 \eta_1) e(P_0, A_2 \eta_2) \cdots e(P_0, A_i \eta_i) e(Q, P_m) \\ &= e(Q_0, P_1)^{\sum \eta_1} e(Q_1, P_2)^{\sum \eta_2} \cdots e(Q_{i-1}, P_i)^{\sum \eta_i} e(Q, P_m) \\ &= e(Q_0, P_1)^{\sum \eta_1} e(Q, P_m) \prod_{j=2}^i [e(Q_{j-1}, P_j)]^{\sum \eta_j} \end{aligned}$$

3. 4 GENERATION OF THE THRESHOLD SIGNATURE

After each sub node has received the $A_i = \sum_{k=1}^i s_{k-1} P_k$ and

$Q_k = s_k P_0 (1 \leq k \leq i-1)$, he computes the partial signature as follows:

- (1) Let the message be M. Compute

$$P_m = H, (ID_{i-1} || M) \in G_1.$$

- (2) Compute partial signature $\sigma_i(ID_i, M) = A_i + s_i P_m$.

- (3) Through playing the game, signers exchange the partial signature $\sigma_i(ID_i, M)$ and hierarchical secret key $Q_k = s_k P_0 (1 \leq k \leq i-1)$. Use the following function to verify partial signature:

$$e(P_0, \sigma_i) = e(Q_0, P_1) e(Q_i, P_m) \prod_{j=2}^i e(Q_{j-1}, P_j)$$

$e(Q_0, P_1)$ can be computed in advance.

- (4) After collecting all the partial signatures. Signers compute the final signature:

$$\sigma(ID - tuple, M) = \sum_{i=1}^i \sigma_i \eta_i = \sum_{i=1}^i A_i \eta_i + s P_m$$

Signers use the following equation to verify the signature:

$$e(P_0, \sigma) = e(Q_0, P_1)^{\sum \eta_1} e(Q, P_m) \prod_{j=2}^i [e(Q_{j-1}, P_j)]^{\sum \eta_j}$$

4. 2 CORRECTNESS OF THE GAME

In the game, all the signers are not sure whether the partial signatures broadcasted are correct or whether they have obtained all the pieces. Before reconstruction, the potency of signature is not guaranteed. So the last signer will not deviate, according to backward induction, all signers will not deviate.

Signer ID_i 's expected payoff is:

$$\begin{aligned} U_i &= \alpha^t U_1 + (1-\alpha)^t U_2 + U_1 U_2 \sum_{j=1}^{t-1} \binom{t-1}{j} \alpha^j (1-\alpha)^{t-1-j} \\ &= \alpha^t U_1 + (1-\alpha)^t U_2 + U_1 U_2 \left[\sum_{j=1}^{t-1} \binom{t-1}{j} \alpha^j (1-\alpha)^{t-1-j} - (1-\alpha)^{t-1} \right] \\ &= \alpha^t U_1 + (1-\alpha)^t U_2 + U_1 U_2 \left[(\alpha + (1-\alpha))^{t-1} - (1-\alpha)^{t-1} \right] \\ &= \alpha^t U_1 + (1-\alpha)^t U_2 + U_1 U_2 - (1-\alpha)^{t-1} U_1 U_2 \end{aligned}$$

The derivation of this equation is:

$$\frac{\partial U_i}{\partial \alpha} = t\alpha^{t-1}U_1 - t(1-\alpha)^{t-1}U_2 + (t-1)(1-\alpha)^{t-2}U_1U_2$$

Let this equation equal to 0, we have the optimal probability α^* . So the signer sends the correct partial signature with probability α^* , he will have the best payoff. It is Nash equilibrium of dynamic game of complete information.

4. 3 SECURITY

Even the attacker has captured the partial signature $\sigma_i(ID-tuple, M)$, it's impossible to deduce the secret key from it. The security is based on solving BDH problem on group G_1 . In polynomial time, the BDH problem is intractable. So the scheme is secure.

Because the key is iteratively generated, even any attacker has captured any ciphered texts by enquiries and extractions he won't deduce any recursion formula from them. They can't possess any useful secret key to generate partial signature. The accuracy Rate of conjecture of the signature is negligible. So our scheme is chosen cipher text security.

4. 4 ANTI DECEIVE FEATURE

Hierarchical secret key

$A_i = A_{i-1} + s_{i-1} P_i$, in which $P_i = H_1(ID_{i-1} \| r_{i-1,i}) \in G_1$.

correlative value $r_{i-1,i} = h_3(C_i \| ID_i)$ is indispensable to compute P_i .

This correlative value is distributed by PKG at initialization phase. As H_3 is kept secret, so the attacker has to choose random number to forge the correlative value. However, A_i is iteratively generated, PKG can detect from the root node to any level of the tree. In the game, if any attacker send the forged partial signature with the probability of 1, then even though he gets all the partial

signatures, he still cannot tell whether they are correct. The reconstructed final signature is uncertain.

5 Conclusions

We combine the rational secret sharing with hierarchical key structure to raise a new rational threshold signature scheme. By implementing the hierarchical key with extended description of dynamic game, secret key is been transmitted in a certain probability so that rational signer has no idea that whether the partial signature is correct. Deviation has been successfully prevented so the game is Nash equilibrium according to the maximum utility function. Partial signature is computed by father node and broadcasted among all the signers, once if not been well transmitted, the game ceases. Based on the protocol analysis and security analysis, our scheme is high efficient, secure, robust. In the future, we will investigate the application of threshold signature in Internet of things.




Acknowledgements

This work was supported by National Fund Project of China, (No. NSC93-2218-E-150-013) and Beijing Natural Science Foundation Project of China(No. 4144074).

References

- [1] Shamir A. How to share a secret. Communications of the ACM. 1979, 22(11):612-613.
- [2] Blakeley G R. Safeguarding Cryptographic Keys[C] // Proceedings of the National Computer Conference. New York: AFIPS Press, 1979: 313-317.
- [3] Chor B, Goldwasser S, Micali S. Verifiable Secret Sharing and Achieving Simultaneity in the Presence of Faults[C] // Proceedings of the 26th Annual Symposium on Foundations of Computer Science. Washington, C: IEEE Computer Society, 1985:383-395.
- [4] Feldman P. A practical scheme for non-interactive verifiable secret sharing[C] // Proceedings of the 28th IEEE Symp. On Foundations of Comp. Science (FOCS'87). Los Angeles: IEEE Computer Society 1987:427-437.
- [5] Pedersen T P. Distributed Provers with Applications to Undeniable Signatures[C] // Proceedings of Eurocrypt'91, Lecture Notes in

- Computer Science, LNCS 547. Berlin: Springer-Verlag, 1991: 221-238.
- [6] Lin H Y, Harn L. Fair Reconstruction of a Secret[J]. Information Processing Letters, 1995, 55(1):45-47.
- [7] Halpern J, Teague, V. rational secret sharing and multiparty computation. Proc of STOC. New York ACM Press, 2004: 623-632.
- [8] Kol G, Naor M. Cryptography and Game Theory: Designing Protocols for Exchanging Information[c]//proceedings of the 5th Theory of Cryptography Conference(TCC). Berlin:Springer -Verlag, 2008:317-336.
- [9] Kol G, Naor M. Games for exchanging information[C] // Proceedings of the 40th Annual ACM Symposium on Theory of Computing(STCC). New York: ACM Press,2008:423-432.
- [10] Maleka S, Amjed S, Rangan C P. Rational Secret Sharing with Repeated Games[C] // In 4th Information Security Practice and Experience Conference, LNCS 4991. Berlin: Springer-Verlag, 2008:334-346.
- [11] Maleka S, Amjed S, Rangan C P. The Deterministic Protocol for Rational Secret Sharing[C] // In 22 th IEEE International Parallel and Distributed Processing Symposium, Miami, FL: IEEE Computer Society,2008:1-7.
- [12] Izmalkov S, Lepinski M, Micali S. Variably Secure Devices[C] // In 5th Theory of Cryptography Conference, LNCS 4948. Berlin:Springer-Verlag,2008:273-301.
- [13] Micali S, Shelat A. Purely Rational Secret Sharing[C] // In 6 th Theory of Cryptography Conference, LNCS 5444. Berlin: Springer-Verlag , 2009 : 54-71.
- [14] A Shamir. Identity-based cryptosystems and signature schemes[A]. Advances in Crypto' 84. 1984: 47-53.
- [15] Y. Desmedt, Y. Frankel, Shared generation of authenticators and signatures[A]. Advances in Cryptology - CRYPTO '91. Proceedings, 1992: 457-469.
- [16] Kenneth G Paterson, Jacob C N Schuldt. Efficient identity-based signatures secure in the standard model[A]. Information Security and Privacy. 11th Australasian Conference, ACISP 2006. Proceedings 2005: 207-222.
- [17] Gordon S D, Katz J. Rational secret sharing revisited[C], Proc of Security and Cryptography for Networks Conference Berlin Springer, 2006:229-241.
- [18] Abraham I, Dolev D, Gonen R, et al. Distributed computing meets game theory: robust mechanisms for rational secret sharing and multiparty computation[C], Proc of the 25th ACM Press, 2006:53-62.
- [19] Shaik Maleka. Rational secret sharing with repeated games[C]. Information Security Practice Experience. 4th International Conference, ISPEC 2008:334-346.
- [20] C Gentry. A Silverberg. Hierarchical ID-based cryptography[C]. Advances in Cryptology - ASIACRYPT 2002. 8th International Conference on the Theory and Application of Cryptology and Information Security , 2002: 548-66.
- [21] SG AKI, P D Taylor. Cryptographic solution to a problem of access control in a hierarchy[J]. ACM TRANS. Computer Systems, 1983, 1(3): 239-248.
- [22] Guangjiu Li. Game theory basis points short notes and exercises. Jiangsu : Jiangsu University press. 2008: 96-110.
- [23] J. F. Nash Jr. Equilibrium points in n-person games[C]. Proc. Nat. Acad. Sci. U. S. A. 1950(3): 48-49.
- [24] Guangmou Wu, Zhouyang Lv. Game theory and Application. Nanjing: Publishing House of Southeast University. 2009:60-74.
- [25] Von Neumann, J. Morgenstern, O. The theory of games and economic behavior. Chap. 3. Princeton University Press, Princeton, 1947.
- [26] R. J Aumann. Backward induction and common knowledge of rationality[J]. Games and Economic Behavior, 1995, 8 (1): 6-19.
- [27] J Katz. Bridging game theory and cryptography: Recent results and future directions. Theory of Cryptography. Fifth Theory of Cryptography Conference, 2008:251-272.

Authors	
	<p>Xiurong Li</p> <p>Current position, grades: Ph. D candidate of the College of Computer Science and Technology in Beijing University of Technology.</p> <p>University studies: M. S. degree in computer application from Beijing University of Technology in 2005</p> <p>Scientific interest: information security and computer network.</p>
	<p>Yong-quan Cai</p> <p>Current position, grades: professor and doctoral supervisor of College of Computer Science and Technology, Beijing University of Technology.</p> <p>University studies: M. S. degree in computer application from Northwest Polytechnic University in 1992 and Ph. D. degree in computer application from Beijing Agriculture Engineering in 1998.</p> <p>Scientific interest: information security, computer network, cryptographic protocols analysis and formal methods in cryptography</p>
	<p>Yali Liu</p> <p>Current position, grades: lecturer of School of Science and Technology, Beijing City University.</p> <p>University studies: M. S. degree in computer software and theory from Beijing University of Technology in 2002 and Ph. D. degree in computer architecture from University of Science and Technology Beijing in 2011.</p> <p>Scientific interest: high performance computing and software engineering.</p>