A New Rational Secret Sharing Scheme

ZHANG En[1,2], CAI Yongquan[1]
[1]College of Computer Science and Technology, Beijing University of Technology, Beijing, 100124, China
[2]College of Computer and Information Technology, Henan Normal University, Xinxiang, 453007, China

Abstract: In this paper, we propose a new approach for rational secret sharing in game theoretic settings. The trusted center is eliminated in the secret reconstruction phase. Every player doesn't know current round is real round or fake round. The gain of following the protocol is more than the gain of deviating, so rational player has an incentive to abide the protocol. Finally, every player can obtain the secret fairly. Our scheme is verifiable and any player's cheating can not work. Furthermore the proposed scheme is immune to backward induction and satisfies resilient equilibrium. No player of the coalition C can do better, even if the whole coalition C cheats. Our scheme can withstand the conspiracy attack with at most m-1 players.

Keywords: Secret Sharing; Game Theory; Verifiable Secret Sharing; Resilient Equilibrium

I. 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 s into "shares" $s_1, s_2, \cdots, s_n$, 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.

Reference [6] proposed the concept of verifiable secret sharing (VSS). Reference [7,8] respectively gave a VSS scheme based on Shamir's scheme which can effectively detect cheat of player and the dealer. However, the VSS scheme can not to take precautions against cheat. For example, assume that one party does not broadcast his share, he can still reconstruct the secret (e.g. exactly t-1 other players reveal their shares), however, prevents the others from learning the secret although his cheating can be detected by the VSS scheme. Reference[9] 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. Then, using a backward induction argument, all the players remain quiet and the secret will not be reconstructed. Recently, the cryptographic community has been significant interest in exploring protocols for rational secret sharing in game theoretic settings to overcome the problem which traditional approach can not solve. Recently, a series of works[3-5, 11-14] has focused on designing rational secret sharing protocols in a game light. Rational secret sharing was first introduced by Halpern and Teague[3]. Their 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. The solution in [4] proposes a rational secret sharing scheme to make rational player have an incentive to fulfill the protocol, by 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 [5] does not rely on computational assumptions. Their scheme has information theoretic security. However, their scheme does not have resistance against coalitions. The solutions of [11, 12] 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 [13, 14] 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.

The major contribution of our work is that we propose a new scheme for rational secret sharing and in our proposed scheme. We put the secret into a series of elements and distribute shares of these elements to players. And in the reconstruction stage, every player doesn't know current round is real round or fake round. So, rational players are unlikely deviating. Finally, every player can obtain the secret fairly, and our protocols can work for 2 out of 2 secret sharing. In addition, any fake shares whether they are sent by the dealer or other players can be verified by every player in our scheme. Moreover, our scheme can withstand the conspiracy attack with at most m-1 players.

The rest of this paper is organized as follows. In Section II, we introduce the preliminary of game theory and cryptography for rational secret sharing. In Section III, we introduce our scheme. In Section IV, we analyze the new scheme and in Section V, we conclude.

II. PRELIMINARY

A. Setting for Rational Secret Sharing

Game theory provides a efficient tool to study and analyze the situations in which decision-makers interact in a competitive manner. We begin by introducing some basic terminology of game theory.

We let a_i denote the strategy employed by playe P_i, $a=(a_1,\cdots, a_n)$ denote strategy profile of players, a_{-i} be a strategy profile of all players except for the playe P_i, $(a_i^{'}, a_{-i}) = (a_1,\cdots a_{i-1}, a_i^{'}, a_{i+1},\cdots, a_n)$ denote the strategy vector a wit P_i 's strategy changed to $a_i^{'}$, $u_i(a)$ which we assume that rational players wish to maximize denote utility o P_i under strategy vector a.

For any rational playe P_i, let $U+, U, U-, U--$ be the utilities obtained, below. (a) If o is an outcome in which P_i gets the secret and others do not get the secret, then $u_i(o) = U+$. (b) If o is an outcome in which P_i gets the secret and at least one other player does also, then $u_i(o) = U$. (c) If o is an outcome in which P_i does not get the secret and others does not either, then $u_i(o) = U-$. (d) If o is an outcome in which p_i does not get the secret, however, at least one other player does, then $u_i(o) = U--$. The relationship between them is $U+ > U > U- > U--$. For simplicity, we consider the situation of two players in which the playe P_i is denoted by the player 1 and the player P_{-i} is denoted by the player 2. In the reconstruction process, there are two strategies: honestly broadcasting his share (denoted by H) or deceive (denoted by D). The game can be showed by the Table 1.

Table 1 The Strategy Game

	H	D
H	U, U	$U--, U+$
D	$U+, U--$	$U-, U-$

From the Table 1, we can see, the game has a unique Nash Equilibrium: (D, D). Therefore, it is impossible for rational player to have an incentive to broadcast his share in the one-shot reconstruction. Further on, the rational player has no incentive to follow the protocol, if he knows when the game will end.

Definition 1 t-resilient equilibrium:

Let $\Gamma = (\{A_i\}_{i=1}^n, \{u_i\}_{i=1}^n)$. Then for $1 \leqslant t < n$ the strategy vector $a = (a_1,\cdots, a_n) \in A$ is a t-resilient equilibrium if for all $C \subset [n]$ with $|C| \leqslant t$, all $i \in C$, and any $a_C^{'} \in \Delta(A_C)$, it holds that

$$u_i(a_C^{'}, a_{-C}) \leqslant u_i(a) \tag{1}$$

This definition is taken from [10] which captures the facts that for every coalition C of size at most t, no member of the coalition improves its situation no matter how the members of C coordinate their actions.

B. Cryptographic TErminology

Cryptography can be viewed as the tool of any system that needs to withstand attack. Let's introduce several cryptographic terminologies.

Definition 2 Polynomial-Time Indistinguishability:

Two ensembles, $X \overset{def}{=} \{X_n\}_{n\in\mathbb{N}}$ and $Y \overset{def}{=} \{Y_n\}_{n\in\mathbb{N}}$, are indistinguishable in polynomial time if for every probabilistic polynomial-time algorithm D, every positive polynomial $p(\cdot)$, and all sufficiently large n's,

$$\left|\Pr[D(X_n,1^n)=1]-\Pr[D(Y_n,1^n)=1]\right|<\frac{1}{p(n)} \quad (2)$$

Definition 3 Pseudorandom Function Ensembles:

An $l-bit$ function ensemble $F=\{F_n\}_{n\in\mathbb{N}}$ is called pseudorandom if for every probabilistic polynomial-time oracle machine M, every polynomial $p(\cdot)$, and all sufficiently large n's,

$$\left|\Pr[M^{F_n}(1^n)=1]-\Pr[M^{H_n}(1^n)=1]\right|<\frac{1}{p(n)} \quad (3)$$

Where $H=\{H_n\}_{n\in\mathbb{N}}$ is the uniform $l-bit$ function ensemble.

Definition 4 Non-interactive zero-knowledge:

A non-interactive proof system (P,V) for a language L is zero-knowledge if there exists a polynomial p and a probabilistic polynomial-time algorithm M such that the ensembles $\{(x,U_{p(|x|)},P(x,U_{p(|x|)}))\}_{x\in L}$ and $\{M(x)\}_{x\in L}$ are computationally indistinguishable, where U_m is a random variable uniformly distributed over $\{0,1\}^m$.

These definitions are taken from reference [15].

III. THE RATIONAL SECRET SHARING SCHEME

A. Protocol for Sharing Phase

Step 1: The dealer chooses a series of elements, s^0, $s^1,\cdots,s^{w-1},s$ (let s denote the secret) from the domain of S. It suffices $s^0<s^1<\cdots<s^{w-1}<s$, Moreover, w depends on the players' utilities and it satisfies:

$$w>\frac{U_i^+-(q^{-1}*U_i^++(1-q^{-1})*U_i^-)}{U_i-(q^{-1}*U_i^++(1-q^{-1})*U_i^-)} \quad (4)$$

The dealer randomly chooses d^*, and replaces s^{d^*} with s if $0\leqslant d^*<w-1$. The dealer randomly chooses s^* from $s^{w-1}-s^0,s^{w-1}-s^1,\cdots,s^{w-1}-s^{w-2},s$, and replaces s^{d^*} with s^*, if d^* is $w-1$.

Step 2: The dealer chooses a prime q and constructs random polynomials $h_0,h_1,\cdots,h_{w-1}$ of degree $t-1$ for $s^0,s^1,\cdots,s^{w-1}$, where $0<P_0^m,P_1^m,P_2^m,\cdots,P_{t-1}^m<q$ $(m=0,1,\cdots,w-1)$, as equation (5).

$$h_m(x)=P_0^m+P_1^mx^1+\cdots+P_{t-1}^mx^{t-1}\bmod q \quad (5)$$

Step 3: Let $P_0^m=s^m(m=0,1,\cdots,w-1)$. For every element s^m, the dealer computes $S_i^m=h_m(i)\bmod q$ $(m=0,1,\cdots,w-1$ and $i=1,\cdots,n)$, and sends the set of $\{S_i^0,S_i^1,\cdots,S_i^m\}$ to player i, then publishes $\Re_j^m=g^{P_j^m}\bmod q$ $(j=0,1,\cdots,t-1$ and $m=1,\cdots,w-1)$.

B. Protocol for Reconstruction Phase

Step 1: Player i $(i=1,2,\cdots,n)$ can verify the validity of shares distributed by the dealer by equation (6). Proof can be found in section 4. If any fake share can be identified, the protocol stops. Otherwise the protocol continues.

$$g^{S_i^m}=\prod_{j=0}^{t-1}(\Re_j^m)^{i^j}\bmod q \quad (6)$$

Step 2: In each iteration $r=0,1,\cdots,w-1$ the player i does:

- The player i $(i=1,2,\cdots,n)$ broadcast the S_i^r. And then, the player i receives and identifies the validity of S_κ^r $(\kappa=1,2,\cdots,i-1,i+1,\cdots,n)$ by equation (6). If any fake share can be detected, the protocol stops. Otherwise the protocol continues.
- The player i $(i=1,2,\cdots,n)$ interpolates a degree $t-1$ polynomial $h_r(x)$ through t shares by (7). Finally, every player knows s^r.

$$h_r(x)=\sum_{i=1}^{t}S_i^r\prod_{1\leqslant j\atop t,j\neq i}\frac{x-x_j}{x_i-x_j} \quad (7)$$

- The player knows the secret is the s^{r-1} and the protocol aborts, if $r<w-1$ and the s^r is less than the s^{r-1}. Otherwise, the protocol continues. The player knows the secret s is the s^r, if $r=w-1$ and the s^r is more than the s^{r-1}. The protocol restarts if $r<w-1$ and the s^r is less than the s^{r-1}.

Step 3: Every player doesn't know whether the current round is the real round or a trap round, even under the $w-1$ round. If a player deviated in the trap round, the protocol will stop. The cheater will never

obtain the secret. So, all the players have to follow the protocol. Finally, every player knows the secret.

Ⅳ. SCHEME ANALYSIS

A. Security Analysis

Theorem 5: The scheme can verify the validity of shares distributed by the dealer or other players by equation (6).

Proof:

$$\begin{aligned}\prod_{j=0}^{t-1}(\Re_j^m)^{i^j} \bmod q &= (\Re_0^m)^{i^0}\times(\Re_1^m)^{i^1}\times\cdots\times(\Re_{t-1}^m)^{i^{t-1}}\\ &= g^{P_0^m}\times g^{P_1^m i^1}\times\cdots\times g^{P_{t-1}^m i^{t-1}}\\ &= g^{P_0^m+P_1^m i^1+\cdots+P_{t-1}^m i^{t-1}}\\ &= g^{S_i^m}\end{aligned}$$

Thus, every player can obtain very high confidence that he holds a valid share of the secret rather than a useless random number.

Theorem 6: The scheme has fairness property

Proof: In our proposed scheme, the players do not know whether this is supposed to be the real round, or whether this is just a test round in which no useful information can be revealed. If the player deviates from the protocol, other players will abort the protocol. Only in a real round, can the member of the coalition gain some advantages over the honest players by cheating. But our protocols do not leak any information about the secret and no information about the secret can be inferred in a fake round. If the members of coalition deviate in a trap round, they will pay the price. Rational party has to abide the protocol. Finally, all the players obtain the secret fairly.

Theorem 7: The scheme can withstand the conspiracy attack with at most m-1 players if it satisfies inequality (4).

Proof: In our scheme, every $C\subset[n]$ with $|C|\leqslant m-1$ doesn't know whether the current round is the meaningful round or a trap round. If members of the coalition C does not participate in the scheme, they can only guess the secret with probability β^C, The player i who is the member of the coalition C gets U_i^+. On the contrary, if they guess a wrong secret with probability $1-\beta^C$, the player i gets U_i^-. So, when the coalition C doesn't participate the protocols, the expected utility of player i is as equation (8)

$$E(U_i^{C^{guess}})=\beta^C*U_i^+ +(1-\beta^C)*U_i^- \tag{8}$$

When the coalition C participates the protocols, player i will get utility U_i^+, if the coalition C aborts in real round with probability λ^C. Otherwise, the player i 's utility is $E(U_i^{C^{guess}})$. Therefore, when the coalition C deviates, the expected utility of a player i is at most

$$\lambda^C*U_i^+ +\left(1-\lambda^C\right)*E(U_i^{C^{guess}}) \tag{9}$$

When the coalition C abides the protocol, the utility of the player i is U_i. So, rational coalition C has an inventive not to deviate from the protocol if the protocol satisfies

$$U_i > \lambda^C*U_i^+ +\left(1-\lambda^C\right)*E(U_i^{C^{guess}}) \tag{10}$$

In our protocol, it holds that

$$\beta^C=q^{-1} \tag{11}$$

and

$$\lambda^C=w^{-1} \tag{12}$$

Namely, no member of the coalition improves its situation no matter how the members of C coordinate their actions if the protocol holds that

$$\begin{aligned}U_i > {}& w^{-1}*U_i^+ +\\ & \left(1-w^{-1}\right)*(q^{-1}*U_i^+ +(1-q^{-1})*U_i^-)\end{aligned} \tag{13}$$

$$\Rightarrow w^{-1}<\frac{U_i-(q^{-1}*U_i^+ +(1-q^{-1})*U_i^-)}{U_i^+-(q^{-1}*U_i^+ +(1-q^{-1})*U_i^-)} \tag{14}$$

That is for every round and for all $C\subset[n]$ with $|C|\leqslant m-1$, all $i\in C$, and any $a_C^{'}\in\Delta(A_C)$, it holds that $u_i(a_C^{'},a_{-C})\leqslant u_i(a)$. So, the scheme can withstand the conspiracy attack.

B. Performance analysis

Generally speaking, the assumption on the existence of a trusted party is strong and the cost of multiparty computations is high. However, our scheme assumes neither the availability of a trusted party nor multiparty computations in the reconstruction phase. And the scheme is not susceptible to backward induction. In addition, our proposed scheme can work for 2 out 2 secret sharing.

V. CONCLUSIONS

We propose a new approach which combined cryptography with game theory for secret sharing to address the issues of traditional m-out-of-n secret sharing scheme. In our scheme rational players have to abide the protocols, and finally, every player can obtain the secret fairly. By analysis, we find that they are simple, fair and effective. However, we currently do not take into account the malicious players which may purse any goal and are not only interested in obtaining the secret. In the future, we will investigate how to prevent the malicious players from deviation.

Acknowledgements

This work was supported by the National Key Basic Research Program of China (NO. 2007CB311106), Beijing Municipal Natural Science Foundation.(No. 1102003) and Youth Science Foundation of Henan Normal University (No. 525198).

References

[1] Shamir A. How to share a secret[J]. Communications of the ACM, 1979, 22(1): 612-613.
[2] Blakeley G R. Safeguarding Cryptographic Keys[C] // Proceedings of the National Computer Conference. New York:AFIPS Press, 1979: 313-317.
[3] Halpern J, Teague V. Rational Secret Sharing and Multiparty Computation[C] // Proceedings of the 36th Annual ACM Symposium on Theory of Computing(STOC). New York: ACM Press, 2004: 623-632.
[4]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.
[5] Kol G, Naor M. Games for exchanging information[C]// Proceedings of the 40th Annual ACM Symposium on Theory of Computing(STOC). New York: ACM Press, 2008: 423-432.
[6] 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, DC: IEEE Computer Society, 1985: 383-395.
[7] 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.
[8] 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.
[9] Lin H Y, Harn L. Fair Reconstruction of a Secret[J]. Information Processing Letters, 1995, 55(1): 45-47.
[10]Katz J. Bridging game theory and cryptography: Recent results and future directions[C] // In 5th Theory of Cryptography Conference TCC 2008, LNCS 4984. Berlin:Springer-Verlag, 2008: 251-272.
[11] 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.
[12] 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.
[13] Izmalkov S, Lepinski M, Micali S. Veriably Secure Devices[C] // In 5th Theory of Cryptography Conference, LNCS 4948. Berlin:Springer-Verlag, 2008: 273-301.
[14] Micali S, Shelat A. Purely Rational Secret Sharing[C] // In 6th Theory of Cryptography Conference, LNCS 5444. Berlin: Springer-Verlag, 2009: 54-71.
[15] Goldreich O. Foundations of Cryptography: Basic Tools[M]. London: Cambridge University Press, 2001.

Biographies

ZHANG En received his M.S. degree in computer application from China University of Geosciences in 2006. He is currently a Ph.D candidate of the College of Computer Science and Technology in Beijing University of Technology. His current research interests include information security and computer networks. E-mail: zhangenzdrj@163.com.

CAI Yongquan received his 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. He is currently an professor and doctoral supervisor of College of Computer Science and Technology, Beijing University of Technology. His research interests include information security, computer network, cryptographic protocols analysis and formal methods in cryptography.