A Rational Secret Sharing Scheme Against Coalition Based on Nash Equilibrium and Neighbor’s Strategy*

CAI Cheng¹, WANG Bojun¹, Ditta Allah² and YANG Yi²

(1. School of Electronic and Computer Engineering, Shenzhen Graduate School, Peking University, Shenzhen 518055, China)
(2. College of Computer Science and Technology, Beijing University of Technology, Beijing 100124, China)

Abstract — In order to prevent any arbitrary subsets of coalition in rational secret sharing, we propose a new one-way information transmission mechanism, every player in a rational secret sharing protocol only interacts with his around two players, which means his decision is strictly based on previous neighboring player’s strategy. Combined with the punishment strategy of Maleka’s scheme and payoff distribution principle in Game Theory, our scheme is capable of achieving Nash equilibrium and has the feature of anti-coalition. For the conspirators, getting the secret at the same time or in less than necessary iteration rounds is almost impossible. Without repeated involvement of the dealer, our scheme has the features of verifiability, anti-coalition, and more meaningfully, superiority of approaching reality model by taking rational behavior into consideration.

Key words — Secret sharing, Game theory, Anti-coalition, Nash equilibrium, One-way transmission.

I. Introduction

Shamir¹ first proposed the \((k,n)\) threshold secret sharing scheme in his paper “how to share a secret”. After then, the first Verifiable secret sharing (VSS) scheme² was raised by Chor B, as well as the first Publicly verifiable secret sharing (PVSS) scheme³ was raised by M. Stadler. In order to adapt secret sharing to reality Applications and build interactive model with practical value, J. Halpern, Teague⁴ proposed the concept of rational secret sharing in 2004. To be rational means the players’ decision is constrained by subjective benefit factor and other players’ strategy. The rational thinking means each player is selfish, just enough to take his own interests into consideration so that he wants himself to be and only be the person who obtains the secret. Besides, if he failed to get the secret then the less other people who get it the better. Under such circumstances, they raised a \(t \geq 3, n \geq 3\) protocol that was proved to be Nash equilibrium after repeated elimination of weakly dominated strategy. However, the protocol has strict implementation constraints and many limitations on the player and the dealer.

An improvement was made by D. Gordon and J. Katz⁵ who extend the protocol to \(t \geq 2, n > 2\) condition without the repeated involvement of the dealer. Furthermore, schemes were introduced by Cai Y. Q. [6,7] which can efficiently prevent cheating. However, all above have not discussed the coalition problem in rational secret sharing. Abraham⁸ did this work by giving k-resilient equilibrium. He proposed a scheme concerning coordinated behavior and rational multiparty computation. Shareef Anjed⁹ indicated that G. Kol, M. Naor’s scheme¹⁰ cannot prevent coalition and gave an improvement under the condition of \(n \geq 2m - 1\). What is more, both Ishihiki, Toshiyuki¹¹ and G. Fuchsbauer¹² designed some schemes that can break the coalition of \(m - 1\) players. Without necessary research into multi subset of coalition, all these schemes proceed at the cost of strict channel condition or some extra protocol limitations.

Most scholars adopt non-cooperative game theory in rational secret sharing scheme while cooperative game already has a certain degree of application¹³. Based on cooperative game, we introduce a new rational secret sharing scheme that prevents beneficial deviation of multi subset of coalition without any constraints on \(m, n\) and communication channel. Through second-time secret segmentation and one-way transmission mechanism¹⁴, we build protocol framework on punishment strategy to finish the reconstruction of the secret. By detailed analysis, it was proved that protocol cost is limited, and the dealer only has to intervene in the initialization phase without a trusted third party.

II. Related Notion

1. Related knowledge of rational secret sharing

Let \(\Gamma(N, S, U)\) represents a \(n\) players game, where \(N\) is a

*Manuscript Received Dec. 2013; Accepted Jan. 2014. This work is supported by the National Natural Science Foundation of China (No.61170221).
finite players set \( \{p_1, p_2, \ldots, p_n\} \), \( S = \{S_1, \ldots, S_n\} \) is a set of corresponding strategies for each \( p_i, i \in \{1, \ldots, n\} \) and \( U = \{u_1, \ldots, u_n\} \) is the utility function. Each \( p_i \) chooses a strategy \( \alpha_i \in S_i \), forming a strategy profile \( \alpha = \{\alpha_1, \ldots, \alpha_n\} \) thus obtains an utility of \( u_i(\alpha_i) \).

**Definition 1 (Strict domination)** Let \( \alpha_i \) represents the strategy profile of all players except \( p_i \). Player \( p_i \)'s strategy \( \alpha_i \in S_i \) is strictly dominate \( \alpha'_i \in S_i \) if for all other \( \alpha_{-i} \in S_{-i} \), we have \( u_i(\alpha_i, \alpha_{-i}) > u_i(\alpha'_i, \alpha_{-i}) \).

**Definition 2 (Nash equilibrium)** If any player’s deviation from the protocol will not bring him any extra utility, i.e. \( \forall i, u_i(\alpha_i, \alpha_{-i}) \geq u_i(\alpha_i, \alpha_{-i}\cdot) \) then strategy profile \( \alpha \in S \) is a Nash equilibrium.

2. **Punishment strategy**[15]

Maleka designed his scheme in a repeated game model so that players can share multi secrets. He assumed that the protocol is strictly proceeded in synchronous channel, and players interact in sequential round \( (I_1, I_2, \ldots) \). As analyzed above, players want their utility to be maximized, thus there exists a discount factor \( \delta \in (0, 1) \) so that the final utility function of \( p_i \) is \( u_i = u_i + \delta^1 u_i + \delta^2 u_i + \delta^3 u_i + \cdots \).

**Definition 3 (Feasible payoff)** If there exists a positive value \( a_\alpha \) so that for all \( p_i \), we have \( y_i = \sum_{\alpha \in S} a_\alpha u_i(\alpha) \) where \( y_i \) represents \( p_i \)'s payoff and \( \sum_{\alpha \in S} a_\alpha = 1 \), then payoff profile \( y \) is feasible.

**Definition 4 (Friedman theorem)** Define \( \Gamma \) as a game in which each player has finite strategies, \( \{y_1, y_2, \ldots, y_n\} \) is \( \Gamma \)'s feasible profile and \( (e_1, e_2, \ldots, e_n) \) is its payoff from some Nash equilibrium. If for all player we have \( y_i > e_i \) and \( \delta \) is close to one, then there exists a Nash equilibrium of infinite repeated game that has \( \{y_1, y_2, \ldots, y_n\} \) as its payoff.

For player \( p_i \), his strategy profile is a pure strategy profile \( (A, B) \) with \( A \) denotes sending the secret, \( B \) denotes not sending it.

The punishment strategy indicates player \( p_i \) chooses \( A \) if other players choose \( A \) while if any other player chooses \( B \) then will choose \( B \) in all next rounds. That is to say, the action of \( p_i \) is strictly influenced by other players. Once anyone deviated, he has to choose the risk of getting the secret in the following procedure, i.e. loss outperforming benefits.

For arbitrary \( p_i \), denotes \( w_1, w_2, w_3, w_4 \) as follows:

- \( w_1 : p_i \) gets the secret while others do not get it.
- \( w_2 \): both \( p_i \) and other players get the secret.
- \( w_3 \): neither of \( p_i \) and other players get the secret.
- \( w_4 \): others get the secret while \( p_i \) does not get it.

We assume that the strategy profile of player \( p_i \) is \( (A, A, \cdots) \) if no one deviated. Denominate above implies \( u_i(A) = w_2 \) so that \( p_i \)'s total payoff function is

\[
\sum_{j=0}^{\infty} \delta^j u_i(I_j) = w_2 + \frac{\delta w_2}{1-\delta} + \frac{\delta^2 w_2}{1-\delta^2} + \cdots + \frac{\delta^j w_2}{1-\delta^j} \\
\delta^j w_1 + \delta^{j+1} w_3 + \delta^{j+2} w_3 + \cdots = w_2 (1 + \delta + \delta^2 + \cdots + \delta^j) + \delta^j w_1 + \delta^{j+1} w_3 (1 + \delta + \cdots) = \frac{w_2(1 - \delta^j)}{1-\delta} + \frac{w_2 \delta^j w_3}{1-\delta} 
\]

If \( \delta \) is close to one and \( w_2(1 - \delta^j) + \delta^j w_1 + \frac{w_2 \delta^j w_3}{1-\delta} < w_2 \) then each player will choose \((A, A, \cdots)\).

**Proof** if a player sends his secret share other \( m-1 \) players, \( (w_2, w_2, \cdots) \) will be his payoff. That means strategy profile \( (A, A, \cdots) \) is a feasible payoff strategy. Due to the desirability of reaping long term payoff, for players as long as they are willing to play, along with \( \delta \) closing to one and \( w_2 \) is greater than the min-max value and \( w_2(u_i(A) > u_i(B)) \).

According to Definition 4, strategy profile \( (A, A, \cdots) \) is a Nash equilibrium of an infinite repeated game \( \Gamma(n, m) \), in which \( A \) is the best strategy. The punishment strategy plays a crucial part in prevention deviation. Ref.[16] analyzed Maleka’s scheme and pointed out that the expected execution time is \( O(n^2) \).

III. **A New Rational Secret Sharing Scheme Against Coalition**

In this section, we introduce a new rational secret sharing scheme that can efficiently prevent coalition among players. We assume our scheme is based on synchronous communication and one-way transmission. In each round, one player can only communicate with two other neighboring players in sequential information transmission chain i.e. transmission is unidirectional (this unidirectional transmission is not necessarily rely on a physical unidirectional channel, in other words, it is also guaranteed in a duplex channel if player follow the protocol. We will prove this in the following context). In initialization phase the dealer distributes all the shadow secrets to players in a way that they cannot reconstruct the secret until the last round. It is demonstrated that our protocol is a Nash equilibrium of static games of complete information.

1. **Protocol initialization**

The dealer holds the original secret \( S \), and let \( N = \{p_1, p_2, \ldots, p_n\} \) be the players’ set with the threshold of \( m \). After generating subshare \( s_i(i = 1, \ldots, n) \) according to Shamir’s[3] secret sharing scheme, the dealer conducts a second-time secret segmentation of the subshare. He chooses a random integer \( t(l > m) \) to construct a random polynomial \( f_i(x) = a_{i,0} + a_{i,1} x + a_{i,2} x^2 + \cdots + a_{i,t-1} x^{t-1} \) in which \( s_i = a_{i,0} \). At the same time he signs every polynomial to make sure the secret is traceable. Then he chooses another random integer \( k(k \geq t) \) to send all shadow shares \( s_{i,j}(i = 1, \ldots, n, j = 1, \ldots, k) \) to \( p_i \) combining the Feldman’s[17] verifiable secret sharing scheme to ensure no cheating or forge. Ref.[17] indicates that there exists a multi party rational exchange protocol without a trusted third party. Also, in our protocol, the dealer only has to get involved at the beginning.

2. **The model of the protocol**

Information one-way transmission model: In our scheme, we assume there are \( m \) players who strictly follow the one transmission mechanism in an order of \( p_{i-1} \rightarrow p_i \rightarrow p_{i+1} \) and \( p_m \rightarrow p_1 \) so that it forms a circular transmission. The order is randomly set by the dealer in initialization phase as portrayed in Fig.1:

\( p_i \) has a pure strategy profile of \((A, B)\) as follows:

\[
(A, B) = \begin{cases} 
A, \text{ denotes sending the secret} \\
B, \text{ denotes sending the secret} 
\end{cases}
\]
Transmission rule: whether or not to send the secret share for player $p_i$ in round $r$ strictly depends on whether $p_{i-1}$ had sent the share in round $r-1$. In each round, player $p_i$ is supposed to send all his shadow secret along with the pieces he has received last round, meanwhile sending the verification message.

To simplify our protocol, we discuss details in a three players game. Let $p_1, p_2, p_3$ be the three players.

**Step 1** In the first round, $p_1$ sends secret share $s_{1,1}$ to $p_2$, say it is $s_{1,1}$; at the same time, he receives a secret share $s_{3,1}$ from $p_3$. We believe that in this one-way interaction, $p_2$ has no intention to send his secret share back to $p_1$ because this would only unilaterally enlarge $p_i$'s quantity of information except himself. This analysis matches the description of rational thinking according to H-J. Therefore this one-way transmission does not necessarily rely on a physical unidirectional channel.

**Step 2** In the second round, $p_1$ sends her secret share $s_{1,2}$ along with $s_{3,1}$ received in round 1 to $p_2$. He receives $s_{3,2}$ from $p_3$ as well as $s_{2,1}$ that $p_1$ received in round 1.

**Step 3** accordingly, in round $r$, $p_1$ sends secret share $s_{1,r}$ and $s_{3,r-1}$ to $p_2$, receives $s_{3,r}$ and $s_{2,r-1}$ from $p_3$. Not until the last round can all the players reconstruct the original secret. They can detect if they received the right shadow secrets and detect forge pieces through verification.

According to the reasoning, this protocol can be extended to a range of $m$ players within which they all have incentive to follow the protocol. Thus in a $(m, n)$ situation, protocol is also feasible.

**3. Punishment strategy**

Define punishment strategy as follows:

Any arbitrary player $p_i$ in round $r$ has two options:

- choose strategy $A$ if $p_{i-1}$ chose $A$ in round $r - 1$.
- choose strategy $B$ in all sequential rounds if $p_{i-1}$ choose $B$ in round $r - 1$.

For the utility of each player, we define punishment strategy matrix as Table 1:

<table>
<thead>
<tr>
<th>$p_i$'s amount of information increases</th>
<th>Other players' amount of information increase</th>
<th>Other players' amount of information does not increase</th>
</tr>
</thead>
<tbody>
<tr>
<td>$w_2$</td>
<td>$w_1$</td>
<td>$w_3$</td>
</tr>
<tr>
<td>$w_4$</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Apparently we have $w_1 > w_2 > w_3 > w_4$.

We assume that there exists a parameter $\delta \in (0, 1)$ so that the utility function of $p_i$ is:

$$k-1 \sum_{j=0}^{k-1} \delta^j u_i(\Gamma_j) = w_2 + \delta^1 w_2 + \cdots + \delta^{k-1} w_2 = w_2 \frac{1 - \delta^k}{1 - \delta}.$$ 

hypothetically if $p_i$ deviates in round $r$, then $p_{i+1}$ will deviate too in round $r + 1$ on the basis of punishment strategy, the rest can be deduced by analogy, that is in round $r + m - 1$, $p_{i-1}$ also deviates. At this point no one could ever receive any secret.

The utility function of arbitrary $p_i$ is:

$$\sum_{j=0}^{k-1} \delta^j u_i(\Gamma_j) = w_2 + \delta^1 w_2 + \cdots + \delta^{r-1} w_2 + \delta^{r-1} w_1 = w_2 \frac{1 - \delta^{r-1}}{1 - \delta} + w_1 \delta^{r-1} \frac{1 - \delta^{m+1}}{1 - \delta} + w_3 \delta^{r-1} \frac{1 - \delta^{k-r-m}}{1 - \delta}.$$ 

If $\delta \in (0, 1)$ is reasonably chosen then

$$\frac{w_2(1 - \delta^{r-1})}{1 - \delta} + \frac{w_1 \delta^{r-1} (1 - \delta^{m+1})}{1 - \delta} + \frac{w_3 \delta^{r-1} (1 - \delta^{k-r-m})}{1 - \delta} < \frac{w_2(1 - \delta^k)}{1 - \delta},$$

in this case there is no reason for $p_i$ to deviate.

**4. Prove**

In the initialization phase the dealer segment the subsahre with a threshold of $t(t > m)$. Then he distributes $k$ pieces of secret to every player. Due to $k \geq t$ and the randomness of $k$, none of the player shaves any idea of the threshold value, so they are not aware of the last round. Because of the one-way transmission, $p_{i-1}$ is the only information source of $p_i$, but the other way round $p_i$ hardly has any influence on $p_i$’s decision making. For long-term interest and the drive to obtain the secret, $p_i$ will choose the strategy profile $(A, A, \cdots)$, because deviation will not bring him any extra profits. With $\delta$ being chosen appropriately under certain condition, all players will follow the protocol till the end. Hence according to Definition 2, our protocol has a Nash equilibrium with the feature of unidirectionality, security, robust, verifiability. The Expected execution time is $O(n^2)$. In the following section, we will discuss the anti-coalition feature.

**5. Capability of coalition-proof**

In our protocol, we assume that conspirators have already share all their secret share through some subliminal channel\cite{18}. However, they still implement the game as the honest player. They try to obtain the all secret share in less than $k$ round. But we use one theorem\cite{19} in cooperative game to prevent this. That is, cooperative game mainly focuses on how to allocate payoffs among players according to collective rationality of cooperative game: efficient, fair and equitable. Personal strategy is limited by the group’s expected payoff, if uneven distribution of income is detected, then players would deviate.

(1) suppose in $m$ players set $M = \{p_1, p_2, \cdots, p_m\}$
there exists a coalition of an arbitrary nonvoid subset \( S = \{p_i, p_{i+1}, \ldots, p_r\} \) where \( r > i \), \( S \subseteq M \). Conspirator \( p_i \)'s contribution to the coalition is \( v_i(S) = v(S) - v(S - \{i\}) \), \( p_i \)'s extra expected payoff would be
\[
   u_i(S) = \frac{v_i(S)}{\sum_{S \subseteq N, i \in S} v_i(S)} (U(S) - \sum_{i \in S, 0 \leq j \leq k} \delta^j u_i(I_j))
\]
Where \( U(S) \) is the total expected payoff for join the coalition, \( \sum_{i \in S, 0 \leq j \leq k} \delta^j u_i(I_j) \) is the total payoff for not join the coalition.

During the protocol, \( p_i \) will be the only source of information for the coalition while \( p_j \) is the only outflow of information. By detailed analyze we found that in round \( k + m - s - 1 \), \( p_i \) will obtain all the secret share first. Yet according to rational thinking of H–J, he will not transmit the secret to \( p_{i+1} \), that is
\[
   v_i(S) = v_{i+1}(S), \quad u_i(S) > u_{i+1}(S)
\]
So in the coalition, there is an unreasonable distribution of payoff, the coalition will collapse.

(2) Our scheme is also capable of prevent multi subset of coalition. To simplify analysis, suppose player \( p_{i-1} \) and \( p_{i+1} \) are two hypothetical subset of coalition of \( M = \{p_1, p_2, \ldots, p_m\} \). At the beginning, they have shared their secret. During the protocol, even if they have a larger amount of information than the others, but they cannot obtain the last piece of secret share any round prior to the others. So
\[
   U(S) = \sum_{i \in S, 0 \leq j \leq k} \delta^j u_i(I_j)
\]
That means, there is no incentive for \( p_{i-1} \) and \( p_{i+1} \) to conspire. If extend \( p_{i-1} \) and \( p_{i+1} \) as any arbitrary discontinuous subset of coalition in the information chain, it can be deduced true in any case.

Some other schemes were introduced in Refs.[20,21].

### IV. Conclusion

We raise a new type of rational secret sharing scheme that uses Nash equilibrium theory to reconstruct the secret. Without dividing player into groups and choosing the leader, we could effectively avoid any player’s deviation if he has too much power. We prevent any possible cheating by adding verifiable information in secret exchange. We combine Maleka’s punishment strategy to define the utility function and the necessary condition for player not to deviate. Besides, due to the second-segmentation, our protocol can be proceeded without repeated involvement of the dealer. One-way transmission mechanism is of crucial use in guaranteeing anti-coalition. We prove that our protocol is a simple, high-efficiency rational secret scheme against any subset of coalition combining the theory of cooperative game.

References

CAI Cheng was born in 1989, from Beijing, China. He is currently a graduate student of School of Electronic and Computer Engineering, Peking University. His research interests include Cryptography Protocol, Information Security and Network Security. (Email: frankgt40@gmail.com)

WANG Bojun was born in 1990, from Jiangsu province of China. She is currently a graduate student of School of Electronic and Computer Engineering, Peking University. Her research interests include Information Security and its applications, secret sharing and game theory. (Email: bojunchang@hotmail.com)

Ditta Allah was born in 1988, from Islamic Republic of Pakistan. He is currently a Ph.D. of the College of Computer Science and Technology in Beijing University of Technology. His research interests include Cryptograph Protocol and Network Security. (Email: dittaallah@bjut.edu.cn)

YANG Yi was born in 1987, from Hubei province of China. She is a graduate student of the College of Computer Science and Technology in Beijing University of Technology. Her research interests include cryptography protocol, information security and digital signature. (Email: chelsealove@126.com)