SCIENCE CHINA
Information Sciences

• HIGHLIGHT •

August 2017, Vol. 60 088101:1–088101:3
doi: 10.1007/s11432-015-9066-9

Reconstruction methodology for rational secret sharing based on mechanism design

Hai LIU[1,2,3], Xinghua LI[1,2,3*], Jianfeng MA[1,2,3], Mengfan XU[1,2,3] & Jingjing GUO[1,2,3]

[1] *State Key Laboratory of Integrated Service Networks, Xidian University, Xi'an* 710071*, China;*
[2] *Shaanxi Key Laboratory of Network and System Security, Xidian University, Xi'an* 710071*, China;*
[3] *School of Cyber Engineering, Xidian University, Xi'an* 710071*, China*

Received September 9, 2016; accepted March 16, 2017; published online June 12, 2017

Citation Liu H, Li X H, Ma J F, et al. Reconstruction methodology for rational secret sharing based on mechanism design. Sci China Inf Sci, 2017, 60(8): 088101, doi: 10.1007/s11432-015-9066-9

Rational secret sharing [1] is the intersection of game theory [2] and traditional secret sharing [3]. In rational secret sharing, the players are selfish and always behave in accordance with profit maximization. What this implies, primarily, is that rational players prefer obtaining the secret rather than not obtaining it and, secondarily, that players prefer as few other players as possible obtaining the secret. Motivated by selfishness, rational players either keep silent or send incorrect shares during the reconstruction phase, thereby the fairness and correctness of rational secret reconstruction become difficult to achieve. For the reasons mentioned above, existing investigations have focused on devising different reconstruction protocols, in order to restrict the selfishness of rational players and succeed in achieving fairness and correctness when reconstructing secrets. However, Game theory as well as existing investigations lacks a guideline reference model that is restrictive to the selfishness of rational players. Devising rational secret reconstruction protocols has always relied on the designers' experience. Although many interesting and ingenious rational secret reconstruction protocols have been presented in the absence of a reference model, some researchers [4–6] do point out that such protocols are likely to be inadequate in two different ways: (1) the terminal strategy profile is unfair; and (2) the obtained secret is incorrect.

To address the aforementioned problems, this article introduces mechanism design [7] from the field of microeconomics, and proposes a reference model for the purpose of devising rational secret reconstruction protocols. In the proposal, the rational secret reconstruction game is formalized; then, the expected goal of this game is discussed from the designer's perspective and with consideration to the security, correctness and fairness of rational secret sharing. Finally, the rational secret reconstruction design model is defined on the basis of mechanism design. Through this brief analysis, we indicate that the proposed model is able to assist the designer in achieving fairness and correctness, with regard to rational secret reconstruction.

Rational secret reconstruction game. In the extensive form game [2], each player considers his plan of action, at any point in time, when a decision needs to be made. Therefore, to cast the execution of rational secret reconstruction protocols, we formalize the rational secret reconstruction game based on the extensive form game.

Definition 1 (Rational secret reconstruction game). A rational secret reconstruction game is a tuple $G_{\mathrm{RS}} = (P, A, H, U, \Delta, \mathrm{Res})$.

- $P = \{P_1, \ldots, P_n\}$ is the set of rational players

[*] Corresponding author (email: xhli1@mail.xidian.edu.cn)
The authors declare that they have no conflict of interest.

in the reconstruction phase, and $P_i \in P$ is the i-th rational player.

- $A = \{A_1, \ldots, A_n\}$ is the set of rational players' strategies in the reconstruction phase, and $A_i = \{a_i^{(1)}, a_i^{(2)}\} \in A$ is the set of rational player P_i's strategies. In particular, the strategy $a_i^{(1)}$ denotes that rational player P_i sends his correct share to others, and the strategy $a_i^{(2)}$ denotes that rational player P_i does not send his correct share.
- H is the set of histories. A history $h \in H$ is the executed situation of the reconstruction game at the corresponding point in time, composed of strategies chosen by the players. For any $h \in H$, the set of strategy profiles available after h is denoted by $A(h) = \{a|(h, a) \in H\}$. A history h is called terminal if $A(h) = \emptyset$. The set of terminal histories is denoted by Z.
- $\Delta = \{\Delta_1, \ldots, \Delta_n\}$ is the set of rational players' private information with respect to the reconstruction game G_{RS}, and $\Delta_i \in \Delta$ is the set of rational player P_i's private information. For instance, $s_i \in \Delta_i$, where the share s_i is assigned by the dealer in the distribution phase.
- $U = \{u_1, \ldots, u_n\}$ is the set of rational players' utilities, and $u_i \in \{U^+, U, U^-, U^{--}, U^f\}$ is rational player P_i's utility. In particular, U^+ is the utility of rational player P_i when he obtains the correct secret solely; U is the utility of rational player P_i while all the rational players obtain the correct secret; U^- is the utility of rational player P_i when none of rational players obtains the correct secret; U^{--} is the utility of rational player P_i when this player does not obtain the correct secret while others do; U^f is the utility of rational player P_i when other players perceive a fake secret as the correct one. Furthermore, they satisfy that "$U^+ > U > U^- > U^{--}$" and "$U^f > U^-$".
- $\mathrm{Res}(\cdot)$ is the reconstruction function, which is rational players' common knowledge. It holds that:

$$\begin{cases} \mathrm{Res}(s_{i_1}, \ldots, s_{i_k}) = \perp, \ 1 \leqslant k \leqslant t-1, \\ \mathrm{Res}(s_{i_1}, \ldots, s_{i_k}) = S, \ t \leqslant k \leqslant n, \end{cases}$$

where S denotes the sharing secret, and the symbol "$\perp$" stands for "empty" information regarding the secret S.

Rational secret reconstruction design model. To establish an explicit design goal, with respect to the security, correctness and fairness of rational secret sharing [4,8], the following conclusion is taken into account:

(1) The security involved in rational secret sharing implies that no information about the secret S can be revealed with less than t shares. Therefore, the security of rational secret sharing relies only on the distribution function $\mathrm{Dis}(\cdot)$. However, there exist many ingenious secret sharing schemes, such as Lagrange [3] or Chinese remainder theorem [9] based schemes. The distribution functions used in these schemes can be adopted directly to achieve the secure rational secret sharing. Consequently, some attention has been brought to the need for devising rational secret reconstruction protocols.

(2) The correctness of rational secret sharing implies that at the end of the rational secret reconstruction game the output of each rational player is either the correct secret S or the "empty". This contains two meanings: (i) if rational players obtain more than t correct shares, they are able to reconstruct the secret correctly; and (ii) rational players can distinguish between the correct and fake shares. Obviously, when rational players have more than t correct shares, they can reconstruct the secret S correctly by using the function $\mathrm{Res}(\cdot)$, which is closely correlated to the distribution function $\mathrm{Dis}(\cdot)$. Furthermore, since the shares are distributed by the dealer, it suffices to prevent the dealer from cheating during the distribution phase, the same method can be adopted for the purpose of preventing rational players from sending incorrect shares during the reconstruction phase. It follows that the correctness of rational secret reconstruction is not the main concern of the designer.

By generalizing the above discussion, from the designer's perspective, the expected solution of the reconstruction game G_{RS} can be given as follows:

Definition 2 (Expected solution of the game G_{RS})**.** Given a terminal history $h \in Z$ is said to be a solution that is expected by the designer for the game G_{RS}, if this history h holds that $h = (a_1^{(1)}|_{\Delta_1}, \ldots, a_n^{(1)}|_{\Delta_n})$, where "$a_i^{(1)}|_{\Delta_i}$" means that rational player P_i chooses strategy $a_i^{(1)}$, based on his private information Δ_i in the reconstruction game G_{RS}.

The rational secret reconstruction design model is now proposed with the introduction of mechanism design [7] from the field of microeconomics.

Definition 3 (Rational secret reconstruction design model)**.** The rational secret reconstruction design model is a tuple $M_{\mathrm{RS}} = (Z, F, p, U, \mathrm{Soc})$.

- Z is the set of all the possible terminal histories at the end of the reconstruction game G_{RS}.
- $F : (H/Z) \to P$ is the function that assigns the "next" rational player to each $h \in H/Z$, thus implying the action order of rational players in the reconstruction game G_{RS}.
- $p = \{p_1, \ldots, p_n\}$ is the set of additional profits for rational players, obtained from the devised reconstruction protocols. According to the strategy $a_i \in A_i$ chosen by rational player P_i, the ad-

ditional profit of rational player P_i is denoted by $p_i : Z \rightarrow \mathbb{R}$, where $\mathbb{R}$ denotes the real number field.

- U is the set of rational players' utilities.
- Soc : $\Delta \times A \times F \times H/Z \rightarrow (a_1^{(1)}, \ldots, a_n^{(1)})$ is the designer's expected goal. The designer hopes that when the turn of rational player P_i comes for choosing the strategy at the corresponding history $h \in H/Z$, the player will choose strategy $a_i^{(1)}$, based on his private information Δ_i.

In our proposed reference model $M_{\rm RS}$, at the end of the reconstruction game $G_{\rm RS}$, the profit of rational player P_i is denoted by $\tilde{u}_i(h) = p_i(h) + u_i(h)$. Therefore, when the designer adopts the proposed model $M_{\rm RS}$ as a guideline, the fundamental design principle is $\max_{1\leqslant i\leqslant n}\{u_i + p_i\} \Leftrightarrow h = (a_1^{(1)}|_{\Delta_1}, \ldots, a_n^{(1)}|_{\Delta_n}) \in Z$. In other words, for each rational player P_i, the profit can be maximized if, and only if, the player sends the correct share to the other players.

Analysis. In the following, it is briefly explained that, under the instruction of our proposed reference model $M_{\rm RS}$, the terminal strategy profile is fair and that the obtained secret is correct when the devised rational secret reconstruction protocol is performed, therefore, the fairness and correctness of the rational secret reconstruction game are achieved.

(1) The terminal strategy profile is fair. The rational players's preference in being the only ones to obtain the secret causes the side effect of the terminal strategy profile to be potentially unfair in existing rational secret reconstruction protocols. However, by means of the presented model $M_{\rm RS}$, the designer computes rational players' utilities using different strategy profiles. According to the expected goal, it is easy for the designer to devise the payment function and motivate rational players to send correct shares during the execution of rational secret reconstruction protocols. As a result, the terminal strategy profile is fair and therefore overall fairness is achieved in rational secret reconstruction.

(2) The obtained secret is correct. While some rational players prefer that other players perceive a fake secret as the correct one, the correct secret may not be reconstructed in existing rational secret reconstruction protocols. Essentially, this happens because the designer does not have a clear idea of how selfish each rational player is. However, in our proposed reference model $M_{\rm RS}$, the set Z consists of all the possible terminal histories in the reconstruction game $G_{\rm RS}$. Additionally, the set U represents the utilities of rational players, with respect to the corresponding terminal history. Both of these two sets help the designer mull over all the possible results of the reconstruction game $G_{\rm RS}$, thereby circumventing the problem mentioned above. In this way, the correctness of the rational secret reconstruction is guaranteed.

Conclusion. Due to the lack of a guideline reference model, the designer always relies on his own experience when devising rational secret reconstruction protocols. This has a negative impact on the fairness and correctness of rational secret reconstruction. This article formalizes the rational secret reconstruction game, based on the extensive form game, and analyzes the expected solution with consideration to the security, correctness and fairness of rational secret sharing. Finally, by introducing the mechanism design from the field of microeconomics, a reference model for devising rational secret reconstruction protocols is proposed. The effectiveness of the proposed design model is indicated in brief.

Acknowledgements This work was supported by National Natural Science Foundation of China (Grant Nos. 61372075, U1405255, 61602360).

Supporting information Universality analysis of the proposed reference model. The supporting information is available online at info.scichina.com and link.springer.com. The supporting materials are published as submitted, without typesetting or editing. The responsibility for scientific accuracy and content remains entirely with the authors.

References

1 Halpern J, Teague V. Rational secret sharing and multiparty computation: extended abstract. In: Proceedings of the 36th Annual ACM Symposium on Theory of Computing, Chicago, 2004. 623–632

2 Osborn M J, Rubinstein A. A Course in Game Theory. Cambridge: MIT Press, 1994

3 Shamir A. How to share a secret. Commun ACM, 1979, 22: 612–613

4 Asharov G, Lindell Y. Utility dependence in correct and fair rational secret sharing. J Cryptol, 2011, 24: 157–202

5 Ong S J, Parkes D C, Rosen A, et al. Fairness with an honest minority and a rational majority. In: Proceedings of the 6th Theory of Cryptography Conference, San Francisco, 2009. 36–53

6 Sourya J D, Asim K P. Achieving correctness in fair rational secret sharing. In: Proceedings of the 12th International Conference on Cryptology and Network Security, Paraty, 2013. 139–161

7 Nisan N, Ronen A. Algorithmic mechanism design. Games Econ Behavior, 2001, 35: 166–196

8 Fuchsbauer G, Katz J, Naccache D. Efficient secret sharing in the standard communication model. In: Proceedings of the 7th Theory of Cryptography Conference, Zurich, 2010. 419–436

9 Asmuth C, Bloom J. A modular approach to key safeguarding. IEEE Trans Inf Theory, 1983, 29: 208–210