Appendix A — Universality Analysis of the Proposed Reference Model

According to the methods that the designer restricts the selfishness of rational players, existing rational secret reconstruction protocols can be labeled as two types: the uncertain number of reconstruction rounds [1-7], and the existence of trusted players [8, 9]. For simplicity, these two methods are called "the uncertain rounds mechanism" and "the trusted player mechanism", respectively.

In order to validate the proposed reference model M_{RS}, we employ it to analyze the idea that such mechanisms restrict the selfishness of rational players.

(1) The uncertain rounds mechanism

The uncertain rounds mechanism implies that rational players continuously reconstruct a huge number of secrets, and they cannot distinguish between the correct secret and fake secrets until the rational secret reconstruction game is complete. Therefore, rational users always send their correct shares to others, thereby achieving the fairness and correctness of rational secret reconstruction.

Without loss of generality, in any k-th round of the reconstruction game G_{RS}, suppose the strategy $a_i^{k\_(1)}$ denotes that rational player P_i sends his correct share $s_{i\_(k)}$ to others. In particular, the share $s_{i\_(k)}$ is assigned by the dealer in the distribution phase; S_k is the secret reconstructed in this round; S is the real secret. Let ε be the probability that rational players guess $S = S_k$ correctly, then $\varepsilon = \Pr[S = S_k]$ is negligible. Furthermore, to prevent the dealer from cheating, the dealer distributes the authentication information to all the rational players in the distribution phase. Therefore, they can verify the correctness of the shares received from the others.

In any k-th reconstruction round, the additional profit provided from the uncertain rounds mechanism satisfies that:

$$\begin{cases} p_i^k(a_i) = 0, & a_i = a_i^{k\_(1)} \\ p_i^k(a_i) = 0, & a_i = a_i^{k\_(2)} \end{cases}.$$

Additionally, since $\varepsilon = \Pr[S = S_k]$ is negligible, the utility of rational player P_i with choosing the strategy $a_i^{k\_(1)}$ or $a_i^{k\_(2)}$ holds that:

$$\begin{cases} u_i^k(a_i) = U^-, & a_i = a_i^{k\_(1)} \\ u_i^k(a_i) = U^-, & a_i = a_i^{k\_(2)} \end{cases}.$$

Therefore, the profit of rational player P_i is

$$\tilde{u}_i^k = p_i^k(a_i) + u_i^k(a_i) = \begin{cases} U^- & a_i = a_i^{k\_(1)} \\ U^- & a_i = a_i^{k\_(2)} \end{cases}.$$

However, if rational player P_i chooses the strategy $a_i^{k\_(2)}$ in the k-th round, the reconstruction game will be aborted. In this situation, rational player P_i cannot obtain the real secret, which is contradictory with his selfishness. It follows that rational player chooses the strategy $a_i^{k\_(1)}$, thereby achieving the fairness and correctness of rational secret reconstruction.

We stress that the discussion mentioned above is the basis of the uncertain rounds mechanism. For this kind of reconstruction protocols, there exist some differences. For instance, the communication channel is either simultaneous or non-simultaneous, and the dealer remains online or offline in the reconstruction phase.

(2) The trusted player mechanism

The trusted player mechanism means that the trusted player observes the execution of the reconstruction game, and according to the strategies chosen by rational players, he can determine whether to reconstruct the real secret.

Without loss of generality, in the reconstruction game G_{RS}, suppose that the player $P_h \in P$ is honest and the rest players are rational. Let $a_{i,h}^{(1)}$ be the strategy that rational player P_i sends his correct share to the player P_h, and let $a_{i,h}^{(2)}$ be the strategy that rational player P_i does not send his correct share to the player P_h. Similarly, the strategy $a_{h,i}^{(1)}$ denotes that honest player P_h sends the reconstructed secret to rational player P_i, and the strategy $a_{h,i}^{(2)}$ denotes that honest player P_h remains silent. Additionally, we suppose that the dealer distributes the authentication information to the honest player, therefore, he can verify the correctness of the shares received from the other rational players.

The additional profit provided from the trusted player mechanism satisfies that:

$$p_i(a_i) = \begin{cases} 0 & a_i = a_{i,h}^{(1)} \\ 0 & a_i = a_{i,h}^{(2)} \end{cases}.$$

Furthermore, the utility of rational player P_i with choosing the strategy $a_{i,h}^{(1)}$ or $a_{i,h}^{(2)}$ holds that:

$$u_i(a_{i,h}^{(1)}) = \begin{cases} u_i(a_{i,h}^{(1)}, a_{h,i}^{(1)}) & a_h = a_{h,i}^{(1)} \\ u_i(a_{i,h}^{(1)}, a_{h,i}^{(2)}) & a_h = a_{h,i}^{(2)} \end{cases}, \quad u_i(a_{i,h}^{(2)}) = u_i(a_{i,h}^{(2)}, a_{h,i}^{(2)}) \in \{U_i^-, U_i^{--}\}.$$

Obviously, $u_i(a_{i,h}^{(2)}) \le \max\{u_i(a_{i,h}^{(2)})\} = U_i^- = \min\{u_i(a_{i,h}^{(1)})\} \le u_i(a_{i,h}^{(1)})$. Therefore, the profit of rational player P_i holds that

$$\widetilde{u}_i^k(a_{i,h}^{(2)}) \le \widetilde{u}_i^k(a_{i,h}^{(1)}).$$

This indicates that, under the restriction of the trusted player mechanism, rational players will send their correct shares to others, thereby achieving the fairness and correctness of rational secret reconstruction game.

We stress again that the analysis mentioned above is the basis of the trusted player mechanism. In this kind of the reconstruction protocol, there exist some differences, such as the number of trusted players and reconstruction rounds.

By generalizing the above discussions, we can conclude that the proposed reference model is compatible with the publicly-published protocols [1-9], which illustrate its effectiveness.

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] Gordon S D, Katz J. Rational secret sharing, revisited. In: Proceedings of the 5th International Conference on Security and Cryptography for Networks. Maiori, 2006. 18-37

[3] Maleka S, Amjed S, Rangan C P. Rational secret sharing with repeated games. In: Proceedings of the 4th International Conference on Information Security Practice and Experience. Sydney, 2008. 334-346

[4] Kol G, Naor M. Games for exchanging information. In: Proceedings of the 40 Annual ACM Symposium on Theory of computing. Victoria, 2008. 423-432G.

[5] Fuchsbauer, J. Katz, D. Naccache. Efficient secret sharing in the standard communication model. In: Proceedings of the 7th International Conference on Theory of Cryptography. Berlin: Springer, 2010, pp.419-436.

[6] Asharov G, Lindell Y. Utility dependence in correct and fair rational secret sharing. Journal of Cryptology, 2011. 24(1): 157-202

[7] Zhang Z F, Liu M L. Rational secret sharing as extensive game. Science China Information Sciences, 2013. 56(3): 1-13

[8] Micali S, Shelat A. Purely rational secret sharing (extend abstract). In: Proceedings of the 6th Theory of Cryptography Conference. San Francisco, 2009. 54-71

[9] 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