面向理性用户的秘密重构设计模型

刘海[1,2]，田有亮[3]，唐莹[4]，Jianbing Ni[5]，马建峰[3]

（1. 贵州财经大学信息学院，贵州 贵阳 550025；2. 中国科学院软件研究所可信计算与信息保障实验室，北京 100190；
3. 贵州大学公共大数据国家重点实验室，贵州 贵阳 550025；4. 贵州财经大学发展规划与学科建设办公室，贵州 贵阳 550025；
5. 女王大学电子与计算机学院，金斯顿 K7L 3N6）

摘 要：理性秘密重构是为了约束理性用户的自利性，在现实生活中确保所有参与用户均能获得共享秘密。然而，如果直接使用现有的理性秘密重构协议，不仅不能实现公平的秘密重构，甚至还会出现用户将虚假的秘密视为真实共享秘密的极端情形。导致上述现象的根本原因是缺乏参考模型，使协议设计者难以全面地考虑理性用户参与秘密重构时的自利行为。为解决该问题，通过形式化描述理性用户模型和理性秘密重构博弈模型来分析理性用户执行秘密重构协议时的先后顺序以及策略选择对公平秘密重构的影响，分别提出了面向纯理性用户环境、面向信誉环境和面向可信用户环境 3 种适用于不同场景的理性秘密重构协议设计模型。理论证明了所提模型能帮助协议设计者有效约束理性用户的自利性，设计了公平的理性秘密重构协议。此外，基于提出的设计模型，还构造了一个公平的理性秘密重构协议来证明所提模型的可用性。

关键词：秘密共享；理性用户；重构公平；设计模型；自利行为

中图分类号：TP391

文献标识码：A

DOI: 10.11959/j.issn.1000−436x.2021195

Design models of secret reconstruction towards rational users

LIU Hai[1,2], TIAN Youliang[3], TANG Ying[4], Jianbing Ni[5], MA Jianfeng[3]

1. School of Information, Guizhou University of Finance and Economics, Guiyang 550025, China
2. Laboratory of Trusted Computing and Information Assurance, Institute of Software, Chinese Academy of Sciences, Beijing 100190, China
3. State Key Laboratory of Public Big Data, Guizhou University, Guiyang 550025, China
4. Office of Development Planning and Academic Development, Guizhou University of Finance and Economics, Guiyang 550025, China
5. Department of Electrical and Computer Engineering, Queen's University, Kingston K7L 3N6, Canada

Abstract: Rational Secret Reconstruction is an intersection between traditional secret reconstruction and game theory, which aims to restrict the selfish behaviors of rational users, making both of them obtain the secret in real applications. However, when directly adopting the existing rational secret reconstruction protocols, it is infeasible to realize the fair secret reconstruction. More seriously, an extreme situation may rise, which is some users regard a fake secret as the real one. The crucial reason is that, due to lack of design models, the protocol designers cannot completely consider their selfish behaviors when rational users participate in secret reconstruction. To solve that problem, through the formalizations of rational users and rational secret reconstruction game, the influences of rational users' action order and their chosen strategies about the fair secret reconstruction were analyzed, and then, three design models for the different scenarios, including purely user rational scenario, reputation-based scenario and trusted user-based scenario, were proposed respectively. Theoretical analysis demonstrates that, the proposed models can help the designers restrict rational users' selfishness effectively, thereby guiding the designers to devise the fair rational secret reconstruction protocols. Additionally, under the guidance of the proposed models, a fair rational secret reconstruction protocol was devised, which indicated that the proposed models were usable.

Keywords: secret sharing, rational users, fair reconstruction, design models, selfish behaviors

收稿日期：2021−07−20；**修回日期**：2021−09−28

通信作者：唐莹，y.tang_coffty@hotmail.com

基金项目：国家自然科学基金资助项目（No.62062071）；贵州省科技计划基金资助项目（黔科合基础[2020]1Y265）

Foundation Items: The National Natural Science Foundation of China (No.62062071), The Science and Technology Program of Guizhou Province (No.[2020]1Y265)

1　引言

随着通信技术的不断发展，边缘计算[1]、雾计算[2]、云计算[3]等多方参与的互联网服务也在不断普及。为保护多方参与的互联网服务数据的安全性和用户的隐私性，作为分布式密码体制重要组成的秘密共享得到了广泛研究[4-8]。

理性秘密共享方案[9]是将博弈论中的自利用户与传统秘密共享相结合而提出的一种更适用于现实应用的秘密共享方案。其目的是解决传统秘密共享方案在现实应用中，由于受到“利益最大化”的驱使，导致理性用户选择自利的行动策略，从而无法实现公平的秘密重构（即不能确保所有用户均能重构出共享秘密）的问题。然而，若直接使用现有理性秘密共享方案[9-29]，会出现如下不公平的情形[30-32]。

1) 发送自己拥有的子秘密的用户无法恢复共享秘密，而未发送自己拥有的子秘密的用户却能恢复共享秘密，即仅有部分参与理性秘密共享的理性用户能恢复共享秘密。

2) 所有参与秘密共享的理性用户均未能恢复出真实的共享秘密，但是某些理性用户可通过欺骗行为，使其他发送自己拥有的子秘密的用户会重构出一个错误的共享秘密，并将该错误的共享秘密视为真实的共享秘密。

造成上述问题的根本原因是：在现有研究中，由于缺乏有效的秘密重构设计模型，方案设计者在设计理性秘密共享方案时（或更准确地说，设计理性秘密重构协议时），往往依赖个人经验，不能充分考虑理性用户在“利益最大化”驱使下的策略选择，从而难以实现公平的理性秘密重构。

为解决上述问题，本文首先通过构建理性秘密重构博弈模型，结合理性用户的自利性偏好，分析自利的理性用户执行秘密重构协议时追求“利益最大化”的策略选择，构造出 3 种不同应用场景下面向理性用户的秘密重构设计模型，并从理论上证明了所提设计模型的有效性。此外，为表明所提设计模型的实用性，本文还基于所提设计模型构造了一个公平的秘密重构协议。本文的主要贡献如下。

1) 提出面向纯理性用户环境的理性秘密重构设计模型，并证明该模型能帮助设计者综合考虑用户的自利行为，从而构造不依赖第三方且能确保公平性的理性秘密重构协议。

2) 构造面向信誉环境的理性秘密重构设计模型，并证明了该模型的有效性，能协助设计者构建基于信誉的理性秘密重构协议，实现公平的秘密重构。

3) 构造面向可信用户环境的理性秘密重构设计模型，并证明该模型可帮助设计者有效约束理性用户的自利性，从而设计适用于具有可信用户参与的理性秘密重构协议。

2　相关工作

根据约束理性用户在秘密重构阶段的自利行为的方法，现有理性秘密重构协议可大致分为：面向纯理性用户环境的理性秘密重构协议、面向信誉环境的理性秘密重构协议和面向可信用户环境的理性秘密重构协议。

2.1　面向纯理性用户环境的理性秘密重构协议

面向纯理性用户环境的理性秘密重构协议是指参与执行该类协议的用户均是理性用户，无可信用户参与且无信誉系统。该类理性秘密重构协议最早是由 Halpern 和 Teague[10]提出的，其基本思想是：每个理性用户在秘密重构阶段中发送包含大量虚假子秘密和真实子秘密的秘密集合给其余用户，使所有用户只有遵循协议的执行，才能分辨出真实的子秘密，从而共同恢复出共享秘密。在他们的方案中，每个理性用户采用“投硬币”的方式确定是否交互真实的子秘密。若有理性用户不发送子秘密，则终止交互。采用上述方法，所有理性用户只能遵循协议的执行，直至每个理性用户同时发送真实的子秘密给其余用户；否则，将没有任何用户能恢复出共享秘密。然而，该方案并不适用于 $t=n=2$ 的情形。其中，t 表示门限值，即表示可恢复共享秘密所需的最少子秘密数量；n 表示分发的子秘密的总数量。为解决该问题，Maleka 等[11-12]通过每多交互一轮将增加用户的通信开销从而降低用户的最终收益的方法，不断地调整理性用户选择遵循协议执行的概率，从而实现公平的理性秘密重构。

然而，上述重构协议仅适用于同步通信的情形。为解决该问题，Kol 和 Naor[13-14]通过让先发送子秘密的用户可获知交互真实子秘密，而后发送子秘密的用户不能获知交互真实子秘密的方法，设计了适用于异步通信的理性秘密重构协议。随后，Fuchsbauer 等[15]通过让理性用户在秘密重构阶段中随机验证其余理性用户发送子秘密正确性的方法，

降低理性用户执行秘密重构协议时的计算开销。Cai 和 Shi[16]让秘密分发者利用概率加密的方法对分发的子秘密进行加密，分别降低秘密分发者在秘密分发阶段和理性用户在秘密重构阶段的计算开销。Dani 等[17]通过让理性用户延迟收到其余用户发送的子秘密的方法来激励其遵循协议的执行，设计了一个仅需一轮交互的理性秘密重构协议。Kawachi 等[18]提出的理性秘密重构协议中，通过指定理性用户在秘密重构阶段中交互子秘密的先后顺序，使理性用户通过 3 轮交互就可恢复共享秘密。

此外，Zhang 和 Liu[19]对理性秘密重构协议的概率安全性进行研究；Zhang 等[20]、De 和 Ruj[21]分别提出了适用于通信资源受限场景的理性重构协议。田有亮等[22]探讨了理性用户的风险偏好函数对秘密重构博弈结果的影响。

2.2 面向信誉环境的理性秘密重构协议

面向信誉环境的理性秘密重构协议最早是由 Nojoumian 等[23]提出的，其基本思想是：将秘密重构视为一类特殊的社会活动，通过对理性用户的信誉（即其长期收益）的增减来约束他们在秘密重构中的自利性。因此，该类协议又称为社会理性秘密重构协议。随后，Nojoumian[24]采用数据拟合的方法，构造参与社会理性秘密重构的理性用户的收益函数。Wang 和 Xu[25]、Tian 等[26]分别结合贝叶斯博弈模型，分析了理性用户在执行社会理性秘密重构协议时的策略选择。Wang 和 Cai[27]指出理性用户可能会进行多次社会理性秘密重构活动。因此，他们结合重复博弈模型设计了一个适用于多秘密重构的社会理性秘密重构协议。Yu 和 Zhou[28]对执行社会理性秘密重构协议中的合谋行为进行研究，设计了概率安全的社会理性秘密共享协议。彭长根等[29]通过综合理性用户的长期收益和短期收益，设计了一个适用于无秘密分发者场景的分布式理性秘密重构协议。随后，Jin 等[33]研究发现当理性用户考虑自己的长期收益时，理性用户参与秘密重构的收益函数将发生改变。因此，他们对文献[24]构造的收益函数进行修改，给出理性用户的混合收益函数。此外，Nojoumian 等[34]还对社会理性秘密重构协议的无条件安全性进行研究。

2.3 面向可信用户环境的理性秘密重构协议

面向可信用户环境的理性秘密重构协议的基本是思想是：在秘密重构的过程中，由可信用户充当“仲裁者”来判断每个理性用户交互的子秘密的正确性，确保遵循协议执行的理性用户能恢复共享秘密；而偏离协议执行的理性用户不能恢复共享秘密。Gordon 和 Katz[35]通过让秘密分发者 Dealer 在重构协议执行过程中观察用户的行为，使只有当所有理性用户均发送自己的子秘密给其余用户时，他们才能进入真实子秘密的交互阶段。然而，Abraham 等[36]研究发现，在使用上述协议时，由于理性用户需经过多轮交互来不断提高自己选择“诚实地发送子秘密”的信念，故该协议的交互轮数较多，极大地增加了理性用户的通信负担。为减少交互轮数，降低理性用户的通信开销，Micali 和 Shelat[37]基于拍卖模型，通过让理性用户将自己拥有的子秘密发送给“拍卖官”，由其恢复共享秘密，并根据用户发送的子秘密正确性来确定哪些用户可获得共享秘密。Ong 等[38]通过将理性用户分成 2 个不同的群组，使每个不同的群组中均存在诚实的可信用户，由这些可信用户监测理性用户在秘密重构中所选择的策略，设计了一个仅需 2 轮交互的秘密重构协议。然而，Zhang 和 Liu[39]研究发现，当直接使用上述理性秘密重构协议时，会出现所有理性用户均不发送子秘密的特殊情形。因此，他们结合序贯纳什均衡设计了一个可避免上述“空威胁”情形的理性秘密重构协议。

但是，在设计上述理性秘密重构协议时，由于缺乏有效的参考模型，设计者只能根据自己的经验来设计理性秘密重构协议，未能有效地约束理性用户追求“利益最大化”的自利行为（面向可信用户环境的理性秘密共享协议除外）。这就导致如果直接使用上述理性秘密重构协议，就可能会出现如下不公平的情形：1) 正确发送子秘密的用户未能获得共享秘密，而未发送子秘密的用户却能获得共享秘密，即仅有部分理性用户能恢复共享秘密；2) 虽然所有参与秘密共享的理性用户均未能恢复真实的共享秘密，但是某些理性用户可通过欺骗行为，使其他发送自己拥有的子秘密的用户会重构出一个错误的共享秘密，并将该错误的共享秘密视为真实的共享秘密。

3 预备知识

3.1 秘密共享

(t,n) 门限秘密共享方案由秘密分发协议和秘密重构协议组成。其中，分发协议是由秘密分发者 Dealer 执行，其目的是将共享秘密 S 拆分成 n 份子

秘密 $s_1,s_2,\cdots,s_n$ 后，分别将子秘密 $s_i(1\leqslant i\leqslant n)$ 分发给用户 P_i；而秘密重构协议主要是由 n 个用户 $P_1,P_2,\cdots,P_n$ 共同执行，其目的是让每个用户 P_i 将秘密分发者 Dealer 分发的子秘密 s_i 交互给其余用户 $P_j(j\neq i)$，从而共同恢复共享秘密 S。为更好地分析用户执行秘密重构协议时的策略，下面给出门限秘密共享的形式化描述模型。

定义 1（门限秘密共享方案） 门限秘密共享方案 $\Gamma_{\mathrm{SS}}=\{\overline{P},\Pi_{\mathrm{Dis}},\Pi_{\mathrm{Res}}\}$ 是一个三元组，具体解释如下。

1) $\overline{P}=\{\mathrm{Dealer}\}\bigcup P$ 是用户集合。Dealer 表示秘密分发者；$P=\{P_1,P_2,\cdots,P_n\}$ 表示执行秘密重构协议的用户集合。$|P|=n$ 表示集合 P 中的元素个数。

2) $\Pi_{\mathrm{Dis}}=\Pi_{\mathrm{Dis}}(\overline{P},\mathrm{Dis}(\cdot),S,t)$ 是秘密分发协议。其中，Dis(·) 是拆分函数；S 是共享秘密；t 是门限值，表示可恢复共享秘密需要的最少的子秘密数量。它满足以下性质。

① 对于秘密分发者 Dealer 来说，在确定持有子秘密的用户以及门限值 t 后，可通过拆分函数 Dis(·) 将共享秘密 S 拆分成 n 份子秘密 $s_1,s_2,\cdots,s_n$。即

$$\mathrm{Dis}(S,t,n)=\{s_1,s_2,\cdots,s_n\}$$

② 对于用户 $P_i(1\leqslant i\leqslant n)$ 来说，当秘密分发者 Dealer 执行完成秘密分发协议 Π_{Dis} 后，其可获得子秘密 s_i。即

$$\Pi_{\mathrm{Dis}}(P_i,\mathrm{Dis}(\cdot),S,t)=s_i$$

3) $\Pi_{\mathrm{Res}}=\Pi_{\mathrm{Res}}(P,\mathrm{Res}(\cdot),s_1,s_2,\cdots,s_n)$ 是秘密重构协议。其中，Res(·) 是秘密重构函数，它满足以下性质。

① 对每个执行秘密重构协议的用户 $P_i(1\leqslant i\leqslant n)$ 来说，若将自己拥有的子秘密发送给其余用户，那么最终获得的子秘密数量应不少于 t 个；若不将自己拥有的子秘密发送给其余用户，则最终获得的子秘密数量应不多于 $t-1$ 个，即

$$\begin{cases}\Pi_{\mathrm{Res}}(P_i,s_i)=|s|\geqslant t,P_i\text{是诚实的}\\ \Pi_{\mathrm{Res}}(P_i,s_i)=|s|\leqslant t-1,P_i\text{是恶意的}\end{cases}$$

② 对每个执行秘密重构协议的用户 $P_i(1\leqslant i\leqslant n)$ 来说，如果其拥有的子秘密数量不少于 t 个，则通过秘密重构函数 Res(·) 就能正确地恢复共享秘密 S；否则，将不能得到关于共享秘密 S 的任何信息。即

$$\mathrm{Res}(|s|)=\begin{cases}S,|s|\geqslant t\\ \perp,|s|<t\end{cases}$$

其中，符号“⊥”表示空信息。

3.2 秘密重构中的理性用户

从秘密共享的形式化模型可以看出，当秘密分发者 Dealer 执行秘密分发协议 Π_{Dis} 后，每个用户 P_i 仅获得一个子秘密 s_i。为能恢复共享秘密 S，用户 P_i 在执行完秘密重构协议 Π_{Res} 时，至少要获得其他 $t-1$ 个用户拥有的子秘密。因此，用户 P_i 在执行秘密重构协议时所选择的行动策略将直接影响其最终拥有的子秘密数量。为更清晰地分析理性用户执行秘密重构协议时所选择的行动策略，本文首先给出理性用户的形式化模型。

定义 2（理性用户） 参与执行秘密重构协议的理性用户 $P_i=\{\theta_i,A_i,\omega_i,u_i\}$ 是一个四元组，具体解释如下。

1) θ_i 表示理性用户 P_i 执行秘密重构协议时的个人偏好。即自利的理性用户首先总是希望自己能获得共享秘密；其次，希望在自己获得共享秘密的同时让尽可能少的其余用户也获得共享秘密。若令 U_i^+ 表示理性用户 P_i 独自获得共享秘密时的收益；U_i 表示所有参与秘密重构的理性用户都获得共享秘密时理性用户 P_i 的收益；U_i^- 表示所有参与秘密重构的理性用户都未获得共享秘密时理性用户 P_i 的收益；U_i^{--} 表示其他参与秘密重构的理性用户 $P_j(j\neq i)$ 获得共享秘密，而自己却未获得共享秘密时的收益；U_i^f 表示所有参与秘密重构的理性用户都未获得共享秘密，但是有部分理性用户将重构出的错误秘密认为是真实共享秘密时理性用户 P_i 的收益，则 $\theta_i=$“$U_i^{--}\leqslant U_i^-\leqslant U_i\leqslant U_i^+,U_i^f<U_i$”。

2) $A_i=\{a_i^h,a_i^f\}$ 表示理性用户 P_i 执行秘密重构协议时的策略集合。其中，a_i^h 表示理性用户 P_i 将自己拥有的子秘密 s_i 正确地发送给其余用户；a_i^f 表示理性用户 P_i 未将自己拥有的子秘密 s_i 正确地发送给其余用户。本文把“理性用户 P_i 不发送任何子秘密给其余用户”、“理性用户 P_i 发送错误的子秘密 s_i' 给其余用户”均视为“理性用户 P_i 未将自己拥有的子秘密正确地发送给其余用户”的情况。

3) ω_i 表示理性用户 P_i 在执行秘密重构协议时所拥有的背景知识。显然，不同的理性用户所拥有

的背景知识是不同的。因此，$\forall 1 \leqslant i, j \leqslant n$ 且 $i \neq j$，有 $\omega_i \neq \omega_j$。

4) u_i 表示理性用户 P_i 执行完秘密重构协议时的收益函数。

在执行秘密重构协议时，理性用户 P_i 在其个人偏好 θ_i 的影响下，总在追求自身利益的最大化。因此，在执行秘密重构协议的过程中，理性用户 P_i 选择的行动策略 $a_i \in A_i$ 应遵循如下原则。

$$a_i = \arg\max\{u_i(a_i(\theta_i, \omega_i))\}$$

3.3 理性秘密重构博弈

当执行秘密重构协议时，自利的理性用户总是遵循“利益最大化”原则来选择自己的行动策略。从理性用户的形式化模型中可以发现，其自身利益最大化受 2 个因素的影响：1) 自己是否获得共享秘密；2) 其余用户是否获得共享秘密。因此，为更好地约束理性用户执行秘密重构协议的自利行为，本文形式化描述理性秘密重构博弈模型。

定义 3（理性秘密重构博弈） 理性秘密重构博弈 $G_{\text{Res}} = \{P, H, F, \boldsymbol{u}\}$ 是一个四元组，具体解释如下。

1) $P = \{P_1, P_2, \cdots, P_n\}$ 是参与理性秘密重构博弈 G_{Res} 的用户集合。其中，$P_i \in P$ 表示第 $i(1 \leqslant i \leqslant n)$ 个理性用户。

2) H 是秘密重构博弈过程的历史序列集合。$\forall \boldsymbol{h} = (a_l, a_m, \cdots, a_j) \in H$，其表示在某时刻已选择行动策略的理性用户 $P_l, P_m, \cdots, P_j$ 所选择的行动策略 $a_l, a_m, \cdots, a_j$ 组成的策略组合。在 $\boldsymbol{h}$ 之后的形成的所有行动策略组合记为 $A(\boldsymbol{h}) = \{\boldsymbol{a} \mid (\boldsymbol{h}, \boldsymbol{a}) \in H\}$。空字符 $\boldsymbol{\Phi} \in H$，表示理性秘密重构博弈 G_{Res} 的开始时刻。如果对于任意的历史 $\boldsymbol{h}' \in H$ 使 $A(\boldsymbol{h}') = \varnothing$，则称该历史 $\boldsymbol{h}'$ 是终止的，即表示理性秘密重构博弈 G_{Res} 结束。Z 表示由所有终止的历史组成的集合。其中，$P_l, P_m, \cdots, P_j \in P$；符号“$\varnothing$”表示空集。

3) $F: (H/Z) \to P$ 是参与理性秘密重构博弈 G_{Res} 的策略选择顺序函数。其含义是：为未终止的历史 $\boldsymbol{h} \in H/Z$ 指派下一个选择行动策略的理性用户 $P_i \in P$。若采用同步通信信道，即所有理性用户同时选择参与理性秘密重构博弈 G_{Res} 的行动策略时，$F(\boldsymbol{\Phi}) = P$。

4) $\boldsymbol{u} = (u_1, u_2, \cdots, u_n)$ 是理性秘密重构博弈结束时，每个理性用户 P_i 获得的最终收益 u_i 组成的收益组合。

下面，结合理性秘密重构博弈模型，给出理性秘密重构的公平性、安全性和正确性模型。

定义 4（理性秘密重构的公平性） 一个理性秘密重构博弈 G_{Res} 是公平的，若 $\forall P_i, P_j \in P$ 和 $\boldsymbol{a} \in Z$，有

$$u_i(\boldsymbol{a}) = U_i,\ u_j(\boldsymbol{a}) = U_j$$

$$\text{或} u_i(\boldsymbol{a}) = U_i^-,\ u_j(\boldsymbol{a}) = U_j^-$$

其中，$i \neq j$。

定义 5（理性秘密重构的安全性） 一个理性秘密重构博弈 G_{Res} 是安全的，若 $\forall P_i \in P$ 和 $\boldsymbol{a} = (a_{l_1}^h, \cdots, a_{l_k}^h, a_i, a_{m_1}, \cdots, a_{m_{k'}}) \in Z$，有

$$\text{Res}(|s| \,|\, \boldsymbol{a}) = \begin{cases} S, k \geqslant t-1 \\ \perp, k < t-1 \end{cases}$$

其中，$k + k' = n - 1$；$\text{Res}_i(\cdot)$ 是秘密重构函数；$|s| \,|\, \boldsymbol{a}$ 表示理性秘密重构博弈 G_{Res} 结束时，理性用户 P_i 在策略集合 $\boldsymbol{a}$ 情形下获得的真实子秘密的数量 $|s|$。

定义 6（理性秘密重构的正确性） 一个理性秘密重构博弈 G_{Res} 是正确的，若 $\forall P_i \in P$ 和 $\boldsymbol{a} \in Z$，有

$$\Pr_i[(a_{i,j} = a_j^h \mid a_j = a_j^f) \wedge (a_{i,j} = a_j^f \mid a_j = a_j^h)] = \varepsilon$$

其中，$\Pr_i[(a_{i,j} = a_j^h \mid a_j = a_j^f) \wedge (a_{i,j} = a_j^f \mid a_j = a_j^h)]$ 表示理性用户 P_i 错误地识别理性用户 P_j 所执行策略 a_j 的概率；$a_{i,j}$ 表示理性用户 P_i 识别理性用户 P_j 所选择的策略；$\varepsilon(\cdot)$ 是可忽略函数。

4 理性秘密重构设计模型与面向不同环境的设计模型

4.1 理性秘密重构设计模型

结合理性用户模型和理性秘密重构博弈模型，本文给出理性秘密重构设计模型，具体如下。

定义 7（理性秘密重构设计模型） 理性秘密重构设计模型 $M = \{F, \boldsymbol{u}, \boldsymbol{p}\}$ 是一个三元组，具体解释如下。

1) F 是执行理性秘密重构协议时，各理性用户 P_i 选择策略 a_i 的先后顺序。

2) $\boldsymbol{u} = (u_1, u_2, \cdots, u_n)$ 是理性秘密重构协议执行结束时，每个理性用户 P_i 选择策略 a_i 所获得的收益 u_i 组成的收益组合。

3) $\boldsymbol{p} = (p_1, p_2, \cdots, p_n)$ 是设计的理性秘密重构

协议根据理性用户 P_i 所选择的策略 a_i 返回给其的额外收益 p_i 所组成的组合。

简单来说，在上述理性秘密重构设计模型中，$\boldsymbol{p}=(p_1,p_2,\cdots,p_n)$ 是根据参与执行秘密重构协议的用户选择执行策略的先后顺序以及可能选择的策略，协议设计者需要设计的额外收益组合，从而通过该额外收益组合来约束理性用户的自利性。在该模型中，要求协议设计者结合用户选择策略的先后顺序 F 来设计额外收益组合 $\boldsymbol{p}$ 的原因如下。

以异步通信情形为例。在本文中，若理性用户能准确地知道共享秘密将在哪轮重构交互中被恢复，则称该重构轮为“已知最后重构轮”。

在异步通信情形下的理性秘密重构博弈中，由于后选择策略的理性用户可观察到在其之前已进行策略选择的理性用户选择的策略，故在已知最后重构轮中，当有 $t-1$ 个理性用户 P_i 选择策略 a_i^h 时（即将自己拥有的子秘密 s_i 正确地发送给其余用户），剩余的理性用户 $P_j(j\neq i)$ 由于其自利性，将选择策略 a_j^f，即不将自己拥有的子秘密正确地发送给其余用户。因此，对于所有选择策略 a_k^f 的理性用户 P_k 来说，此时他们的收益 $u_k=U_k^+$。然而，对于理性用户 P_i 来说，其收益为 $u_i=U_k^{--}$。

由此可知，若要设计出公平的理性秘密重构协议，协议设计者不仅要考虑参与执行秘密重构协议的理性用户可能选择的策略，更要根据这些理性用户在执行秘密重构协议时选择策略的先后顺序来设计额外收益组合。这样才能有效地约束理性用户的自利行为，确保所有理性用户均能重构出共享秘密。

为进一步证明所给出的理性秘密重构设计模型的有效性，本文针对面向纯理性用户环境、面向信誉环境以及面向可信用户环境分别给出适用于异步通信情形的理性秘密重构协议的设计模型。

4.2　面向纯理性用户环境的设计模型

当所有用户均是理性的，且无信誉系统时，可使用下述设计模型来构造公平的理性秘密重构协议。

定义 8（面向纯理性用户环境的设计模型）　面向纯理性用户环境的理性秘密重构设计模型 $M=\{F,\boldsymbol{u},\boldsymbol{p}\}$ 是一个三元组，具体解释如下。

1) F：若 $i<j$，则在执行理性秘密重构协议时理性用户 P_i 比理性用户 P_j 先进行策略选择。

2) $\boldsymbol{u}=(u_1,u_2,\cdots,u_n)$ 是执行完理性秘密重构协议后用户的收益组合。它满足

$$u_i\in\{U_i^{--},U_i^{-},U_i^{f},U_i,U_i^{+}\}$$

其中，$1\leqslant i\leqslant n$。

3) $\boldsymbol{p}=(p_1,p_2,\cdots,p_n)$ 是设计的理性秘密重构约束机制根据用户 P_i 选择的策略 a_i，返回给理性用户 P_i 的额外收益 $p_i(a_i)$ 所组成的额外收益组合。它满足

$$p_i(a_i)=\begin{cases}p_i^k=u_i(i\leftarrow i+0)=U_i^{-},a_i=a_i^{k-h}\\ p_i^k=u_i(i\leftarrow i\wedge k=1)=U_i^{-},a_i=a_i^{k-f}\end{cases}$$

其中，$u_i(i\leftarrow i+0)$ 表示理性用户 P_i 选择行动策略的顺序（无论是在该次重构博弈的第 $k+1$ 轮中，还是在新开设的重构博弈的第一轮中）保持不变时的收益；$u_i(i\leftarrow i\wedge k=1)$ 表示理性用户 P_i 在新开始的重构博弈的第一轮中率先选择行动策略时的收益。此时，原来的其余理性用户 $P_j(1\leqslant j\leqslant i-1)$ 选择策略的顺序分别向后顺延一位。此时，由于所有用户均未能重构出真实的共享秘密，故理性用户 P_i 选择的行动策略 a_i 时的额外收益均为 U_i^{-}。

值得注意的是，在使用上述模型时，需对秘密分发协议做相应的约束。具体约束如下。

在秘密分发协议执行之前，秘密分发者 Dealer 首先选择一个随机数 Round 作为执行该理性秘密重构协议时所需的最大交互轮数；然后在 $[1,\text{Round}-1]$ 中随机选择整数 K 作为能重构出真实共享秘密的重构轮数。此外，秘密分发者 Dealer 在理性用户 $P_1,P_2,\cdots,P_{t-1}$ 中任选 b 个理性用户 P_{i_m} 发送子秘密集合 $\{s_{i_m\_(1)},\cdots,s_{i_m\_(K)},s_{i_m\_(K+1)}\}$，给其余用户 $P_{\widetilde{i}}$ 发送子秘密集合 $\{s_{\widetilde{i}\_(1)},s_{\widetilde{i}\_(2)},\cdots,s_{\widetilde{i}\_(K+l)}\}$。其中，$1\leqslant i_m\leqslant t$；$1\leqslant m\leqslant b$；$\widetilde{i}\neq i_m$；$l$ 是正整数；$s_{i\_(k)}$ 是真实共享秘密 S 对应的子秘密，$1\leqslant j\leqslant n$。当 $j=i_m$ 时，$s_{j\_(K+1)}$ 为重构协议的执行终止符；而其余的子秘密均是错误的子秘密。此外，秘密分发者 Dealer 还需分发可验证所有子秘密正确性的验证信息。当所有理性收到执行终止符时，即可知道在第 K 轮中重构出真实的共享秘密 S。

本文将上述重构协议设计模型所对应的重构约束机制称为纯理性机制 $M_{\text{Res}}^{\text{PR}}$，下面证明该机制能帮助协议设计者有效约束理性用户的自利行为。

定理 1　在异步通信情形下的 (t,n) 理性秘密共

享重构博弈G_{Res}中，纯理性机制$M_{\mathrm{Res}}^{\mathrm{PR}}$能有效约束理性用户的自利行为。

证明 在纯理性机制$M_{\mathrm{Res}}^{\mathrm{PR}}$中，只有理性用户$P_{i_m}$知道何时能正确地重构出真实的共享秘密$S$。因此，本文首先证明理性用户$P_{i_m}$在纯理性机制$M_{\mathrm{Res}}^{\mathrm{PR}}$的约束下的策略选择。

由于理性用户P_{i_m}明确知道真实的共享秘密S是在已知重构轮——第k轮交互中才能恢复，因此在第k轮之前的交互轮k'中，其选择策略$a_{i_m}^{k'-h}$和$a_{i_m}^{k'-f}$的最终收益分别为

$$\begin{cases}\overline{u}_{i_m}(a_{i_m}^{k'-h})=u_{i_m}(a_{i_m}^{k'-h})+p_{i_m}^{k'}(a_{i_m}^{k'-h})=2U_{i_m}^{-}\\ \overline{u}_{i_m}(a_{i_m}^{k'-f})=u_{i_m}(a_{i_m}^{k'-f})+p_{i_m}^{k'}(a_{i_m}^{k'-f})=2U_{i_m}^{-}\end{cases}$$

其中，$1\leqslant k'<k$。

虽然$\overline{u}_{i_m}(a_{i_m}^{k'-h})=\overline{u}_{i_m}(a_{i_m}^{k'-f})$，但是在纯理性机制$M_{\mathrm{Res}}^{\mathrm{PR}}$的约束下，若理性用户$P_{i_m}$选择策略$a_{i_m}^{k'-f}$，则本次秘密重构结束，并且其会在重新开始的重构交互的第一轮中率先选择策略。

显然，这与理性用户P_{i_m}的个人偏好$\theta_{i_m}=\{U_{i_m}^{--}\leqslant U_{i_m}^{-}\leqslant U_{i_m}\leqslant U_{i_m}^{+}\}$相矛盾，故理性用户$P_{i_m}$在第$k'$轮交互中只会选择策略$a_{i_m}^{k'-h}$。

在已知最后重构轮——第k轮的交互过程中，由于$1\leqslant i_m\leqslant t-1$，若轮到理性用户$P_{i_m}$选择策略，则在理性用户$P_{i_m}$之前先选择策略的用户$P_1,P_2,\cdots,P_{i_m-1}$均发送自己拥有的子秘密给其余理性用户。否则，在纯理性机制$M_{\mathrm{Res}}^{\mathrm{PR}}$的约束下，本次秘密重构将结束，重新开始新的交互。此时，理性用户P_{i_m}选择策略$a_{i_m}^{k-h}$的收益为

$$u_{i_m}(a_{i_m}^{k-h}|a_1^{k-h},a_2^{k-h},\cdots,a_{i_m-1}^{k-h})=$$
$$\begin{cases}U_{i_m}+U_{i_m}^{-},\ \text{用户}P_{i_m+1},\cdots,P_t\text{正确发送子秘密}\\ 2U_{i_m}^{-},\ \text{用户}P_{i_m+1},\cdots,P_t\text{未正确发送子秘密}\end{cases}$$

而理性用户P_{i_m}选择策略$a_{i_m}^{k-f}$的收益为

$$u_{i_m}(a_{i_m}^{k-f}\,|\,a_1^{k-h},a_2^{k-h},\cdots,a_{i_m-1}^{k-h})=2U_{i_m}^{-}$$

因此，理性用户P_{i_m}在第k轮的交互过程中，选择策略$a_{i_m}^{k-h}$和$a_{i_m}^{k-f}$的最终收益为

$$\overline{u}_{i_m}(a_{i_m}^{k-h})=u_{i_m}(a_{i_m}^{k-h})+p_{i_m}^{k-h}(a_{i_m}^{k-h})\geqslant 2U_{i_m}^{-}=$$
$$u_{i_m}(a_{i_m}^{k-f})+p_{i_m}^{k-h}(a_{i_m}^{k-f})=\overline{u}_{i_m}(a_{i_m}^{k-f})$$

综上所述，根据其自利性，理性用户P_{i_m}在已知重构轮中只会选择策略$a_{i_m}^{k-h}$。

下面证明纯理性机制$M_{\mathrm{Res}}^{\mathrm{PR}}$也能有效约束理性用户$P_{\tilde{i}}$的自利性。对于理性用户$P_{\tilde{i}}$来说，其不知道真实的共享秘密在哪轮交互中可被恢复。此时，对于第$\tilde{k}$轮交互，理性用户$P_{\tilde{i}}$正确猜测$\tilde{k}=k$的概率$\Pr_{\tilde{i}}[\tilde{k}=k]$是可忽略的，即$\Pr_{\tilde{i}}[\tilde{k}=k]=\varepsilon$。

因此，理性用户$P_{\tilde{i}}$在第$\tilde{k}\neq k$轮交互中选择策略$a_{\tilde{i}}^{\tilde{k}-f}$和$a_{\tilde{i}}^{\tilde{k}-h}$的收益为

$$u_{\tilde{i}}(a_{\tilde{i}}^{\tilde{k}-f})=\Pr_{\tilde{i}}[\tilde{k}=k]u_{\tilde{i}}(a_{\tilde{i}}^{\tilde{k}-f})+\Pr_{\tilde{i}}[\tilde{k}\neq k]u_{\tilde{i}}(a_{\tilde{i}}^{\tilde{k}-f})=U_{\tilde{i}}^{-}$$
$$u_{\tilde{i}}(a_{\tilde{i}}^{\tilde{k}-h})=\Pr_{\tilde{i}}[\tilde{k}=k]u_{\tilde{i}}(a_{\tilde{i}}^{\tilde{k}-h})+\Pr_{\tilde{i}}[\tilde{k}\neq k]u_{\tilde{i}}(a_{\tilde{i}}^{\tilde{k}-h})=U_{\tilde{i}}^{-}$$

此时，在第$\tilde{k}\neq k$轮交互中选择策略$a_{\tilde{i}}^{\tilde{k}-f}$和$a_{\tilde{i}}^{\tilde{k}-h}$所获得最终收益为

$$\overline{u}_{\tilde{i}}(a_{\tilde{i}}^{\tilde{k}-f})=u_{\tilde{i}}(a_{\tilde{i}}^{\tilde{k}-f})+p_{\tilde{i}}^{\tilde{k}}(a_{\tilde{i}}^{\tilde{k}-f})=$$
$$u_{\tilde{i}}(a_{\tilde{i}}^{\tilde{k}-h})+p_{\tilde{i}}^{\tilde{k}}(a_{\tilde{i}}^{\tilde{k}-h})=\overline{u}_{\tilde{i}}(a_{\tilde{i}}^{\tilde{k}-h})$$

而在第$\tilde{k}=k$轮交互中选择策略$a_{\tilde{i}}^{k-f}$和$a_{\tilde{i}}^{k-h}$的收益分别为

$$u_{\tilde{i}}(a_{\tilde{i}}^{\tilde{k}-f})=\Pr_{\tilde{i}}[\tilde{k}=k]u_{\tilde{i}}(a_{\tilde{i}}^{\tilde{k}-f})+$$
$$\Pr_{\tilde{i}}[\tilde{k}\neq k]u_{\tilde{i}}(a_{\tilde{i}}^{\tilde{k}-f})=U_{\tilde{i}}^{-}$$

$$u_{\tilde{i}}(a_{\tilde{i}}^{\tilde{k}-h})=\Pr_{\tilde{i}}[\tilde{k}=k]u_{\tilde{i}}(a_{\tilde{i}}^{\tilde{k}-h})+$$
$$\Pr_{\tilde{i}}[\tilde{k}\neq k]u_{\tilde{i}}(a_{\tilde{i}}^{\tilde{k}-h})=U_{\tilde{i}}$$

此时，其最终收益满足

$$\overline{u}_{\tilde{i}}(a_{\tilde{i}}^{\tilde{k}-f})=u_{\tilde{i}}(a_{\tilde{i}}^{\tilde{k}-f})+p_{\tilde{i}}^{\tilde{k}}(a_{\tilde{i}}^{\tilde{k}-f})=$$
$$2U_{\tilde{i}}^{-}<U_{\tilde{i}}+U_{\tilde{i}}^{-}=u_{\tilde{i}}(a_{\tilde{i}}^{\tilde{k}-h})+p_{\tilde{i}}^{\tilde{k}}(a_{\tilde{i}}^{\tilde{k}-h})=\overline{u}_{\tilde{i}}(a_{\tilde{i}}^{\tilde{k}-h})$$

因此，对于理性用户$P_{\tilde{i}}$来说，在任意第$\tilde{k}$轮中选择策略$a_{\tilde{i}}^{\tilde{k}-f}$和$a_{\tilde{i}}^{\tilde{k}-h}$获得收益满足

$$\overline{u}_{\tilde{i}}(a_{\tilde{i}}^{\tilde{k}-f})\leqslant\overline{u}_{\tilde{i}}(a_{\tilde{i}}^{\tilde{k}-h})$$

故由于其自利性，理性用户$P_{\tilde{i}}$在纯理性机制$M_{\mathrm{Res}}^{\mathrm{PR}}$的约束下会选择策略$a_{\tilde{i}}^{\tilde{k}-h}$。

综上所述，本文给出的纯理性机制$M_{\mathrm{Res}}^{\mathrm{PR}}$有效约束理性的自利行为。

通过上述证明可以得出，本文给出的面向纯理性用户环境的设计模型能帮助协议设计者有效地约束理性用户的自利行为，使设计出的理性秘密重

构协议是公平的。

4.3　面向信誉环境的设计模型

在信誉环境中，假设每个理性用户 P_i 具有一个公开可见的信誉值 r_i，且 r_i 将会根据理性用户 P_i 在社会活动中的行为被其余用户进行提高或降低。令 $R=\{r_1,r_2,\cdots,r_n\}$ 为理性秘密重构博弈中理性用户的信誉值集合；并且在秘密分发阶段中，秘密分发者 Dealer 已分发相应的验证信息给理性用户，使他们可验证收到的子秘密和重构出的共享秘密的正确性。那么，面向信誉环境的理性秘密共享重构协议的设计参考模型如下。

定义 9（面向信誉环境的设计模型）　面向信誉环境的理性秘密重构设计模型 $M=\{F,\boldsymbol{u},\boldsymbol{p}\}$ 是一个三元组，具体解释如下。

1) F：若 $r_i \leqslant r_j$，则理性用户 P_i 在执行理性秘密重构协议时比理性用户 P_j 先进行策略的选择。

2) $\boldsymbol{u}=(u_1,u_2,\cdots,u_n)$ 是执行完理性秘密重构协议时用户的收益组合。它满足

$$u_i \in \{U_i^{--},U_i^{-},U_i^{f},U_i,U_i^{+}\}$$

其中，$1 \leqslant i \leqslant n$。

3) $\boldsymbol{p}=(p_1,p_2,\cdots,p_n)$ 是设计的理性秘密重构约束机制根据用户 P_i 选择的策略 a_i，返回给理性用户的额外收益 $p_i(a_i)$ 所组成的额外收益组合。它满足

$$p_i(a_i)=\begin{cases} p_i^h = r_{\min} > U_i^{+}-U_i^{--}, a_i=a_i^h \\ p_i^f = r_{\max} < U_i^{--}-U_i^{+}, a_i=a_i^f \end{cases}$$

其中，$r_{\min}=\min\{u_i(r_i \leftarrow r_i+n-1)\}$ 表示理性用户 P_i 的信誉值 r_i 提升 $n-1$ 时其获得的最小收益；$r_{\max}=\max\{u_i(r_i \leftarrow r_i-n+1)\}$ 表示理性用户 P_i 的信誉值 r_i 降低 $n-1$ 时的最大评估；“$\leftarrow$”表示赋值。

显然，通过不断调整用户信誉值提高和降低的额度，一定存在一个最小的 n' 使 $r_{\min}>U_i^{+}-U_i^{--}$ 和 $r_{\max}<U_i^{--}-U_i^{+}$ 成立。为便于描述，本文假设 $n'=n$。本文将上述设计参考模型所对应的重构约束机制称为信誉机制 $M_{\mathrm{Res}}^{\mathrm{R}}$。下面，将证明所提出的信誉机制 $M_{\mathrm{Res}}^{\mathrm{R}}$ 能帮助协议设计者有效地约束理性用户在理性秘密重构博弈 G_{Res} 的已知最后重构轮中的自利行为，实现公平的理性秘密重构。

定理 2　在异步通信情形下的 (t,n) 理性秘密共享重构博弈 G_{Res} 中，信誉机制 $M_{\mathrm{Res}}^{\mathrm{R}}$ 能有效约束理性的自利行为。

证明　1) 在已知最后重构轮中，当有 t 个理性用户 P_j 已选择行动策略 a_j^h 时，理性用户 P_i 选择行动策略 a_i^h 和 a_i^f 的收益为

$$u_i(a_i \mid a_{j_1}^h,a_{j_2}^h,\cdots,a_{j_t}^h)=\begin{cases} U_i, a_i=a_i^h \\ U_i, a_i=a_i^f \end{cases}$$

此时，他选择行动策略 a_i^h 和 a_i^f 使其自身信誉变化收益满足

$$p_i(a_i)=\begin{cases} p_i^h > U_i^{+}-U_i^{--}, a_i=a_i^h \\ p_i^f < U_i^{--}-U_i^{+}, a_i=a_i^f \end{cases}$$

因此，理性用户的最终收益满足

$$\overline{u}_i(a_i^h)=u_i(a_i^h)+p_i^h > u_i(a_i^f)+p_i^f=\overline{u}_i(a_i^f)$$

故自利的理性用户 P_i 不会选择行动策略 a_i^f。

2) 在已知最后重构轮中，有 $t-1$ 个理性用户 P_j 已选择行动策略 a_j^h。

①若 $t=n$，理性用户 P_i 是已知最后重构轮中最后选择行动策略的理性用户。那么，理性用户 P_i 选择行动策略 a_i^h 和 a_i^f 的收益为

$$u_i(a_i \mid a_{j_1}^h,a_{j_2}^h,\cdots,a_{j_t}^h)=\begin{cases} U_i, a_i=a_i^h \\ U_i^{+}, a_i=a_i^f \end{cases}$$

那么，理性用户 P_i 的最终收益为

$$\overline{u}_i(a_i)=\begin{cases} u_i(a_i^h)+p_i^h > U_i^{+}+U_i-U_i^{--}, a_i=a_i^h \\ u_i(a_i^f)+p_i^f < U_i^{--}, a_i=a_i^f \end{cases}$$

由于 $\overline{u}_i(a_i^h)>\overline{u}_i(a_i^f)$，故自利的理性用户 P_i 只会选择行动策略 a_i^h。

② 若 $t \neq n$，即理性用户 P_i 不是已知最后重构轮中最后选择行动策略的用户。那么，通过上述分析可知，理性用户 P_n 将会选择行动策略 a_n^h。此时，与有 t 个理性用户 P_j 已选择行动策略 a_j^h 的情形相同，故理性用户 P_i 不会选择行动策略 a_i^f。

3) 在已知最后重构轮中，有 $k(0 \leqslant k \leqslant t-1)$ 个理性用户 P_j 已选择策略 a_j^h。

① 如果 $k=t-2$，对于理性用户 P_i 来说，若 $i=n$，那么理性用户 P_i 在已知最后重构中选择行动策略 a_i^h 和 a_i^f 的收益为

$$u_i(a_i \mid a_{j_1}^h,a_{j_2}^h,\cdots,a_{j_k}^h)=\begin{cases} U_i^{-}, & a_i=a_i^h \\ U_i^{-}, & a_i=a_i^f \end{cases}$$

此时，理性用户 P_i 的最终收益为

$$\overline{u}_i(a_i)=\begin{cases}u_i(a_i^h)+p_i^h>U_i^+, & a_i=a_i^h\\ u_i(a_i^f)+p_i^f<2U_i^{--}-U_i^+, & a_i=a_i^f\end{cases}$$

显然，$\overline{u}_i(a_i^h)>\overline{u}_i(a_i^f)$。故自利的理性用户 P_i 只会选择行动策略 a_i^h。

② 若 $t\neq n$，$i=n-1$ 时，理性用户 P_i 的最终收益与“当有 $t-1$ 个理性用户 P_j 已选择行动策略 a_i^h”情形中 $i=n$ 的最终收益相同。此时，理性用户 P_i 不会选择行动策略 a_i^f。

那么，根据逆向归纳法可知，当 $k=0$ 且 $i=1$ 时，理性用户 P_i 仍只会选择行动策略 a_i^h。

综上所述，在本文给出的信誉重构机制 $M_{\text{Res}}^{\text{R}}$ 的约束下，所有的理性用户会将自己拥有的子秘密正确地发送给其余理性用户。此时，理性秘密重构博弈 G_{Res} 结束时形成的终止历史序列为 $\boldsymbol{h}'=(a_1^h,a_2^h,\cdots,a_n^h)$。因此，本文给出的面向信誉环境的设计模型能帮助协议设计者有效地约束理性用户的自利行为，使设计出的理性秘密重构协议是公平的。

4.4 面向可信用户环境的设计模型

当有可信用户参与理性秘密重构协议的执行时，可利用可信用户作为“仲裁者”来监督协议的执行过程。这不仅能降低执行理性秘密重构协议时理性用户的交互轮数，还能有效约束理性用户的自利性。假设在秘密分发阶段中，秘密分发者 Dealer 分发验证信息给所有的理性用户，使他们可验证收到的子秘密和重构出的共享秘密的正确性。那么，适用于具有可信用户环境的理性秘密重构协议设计参考模型如下所示。

定义 10（面向可信用户环境的设计模型） 面向可信用户环境的理性秘密重构设计模型 $M=\{F,\boldsymbol{u},\boldsymbol{p}\}$ 是一个三元组，具体解释如下。

1) F：若 $i<j$，则在执行理性秘密重构协议时理性用户 P_i 比理性用户 P_j 先进行策略的选择。

2) $\boldsymbol{u}=(u_1,u_2,\cdots,u_n)$ 是执行完理性秘密重构协议后用户的收益组合。它满足

$$u_i\in\{U_i^{--},U_i^-,U_i^f,U_i,U_i^+\}$$

且

$$u_i(a_i^h)=\begin{cases}u_i(a_i^h,a_{h,i}^h)\\ u_i(a_i^h,a_{h,i}^s)\end{cases},\quad u_i(a_i^f)=u_i(a_i^f,a_{h,i}^s)$$

其中，$1\leqslant i\leqslant n$；策略 $a_{h,i}^h$ 表示可信用户 P_h 将恢复出的共享秘密 S 发送给理性用户 $P_i(i\neq h,1\leqslant i\leqslant n)$；策略 $a_{h,i}^s$ 表示理性用户 P_i 未将正确的子秘密 s_i 发送给可信用户 P_h；策略 $a_{h,i}^{\text{slient}}$ 表示可信用户 P_h 保持沉默。

3) $\boldsymbol{p}=(p_1,p_2,\cdots,p_n)$ 是设计的理性秘密重构约束机制根据用户 P_i 选择的行动策略 a_i，返回给理性用户的额外收益 $p_i(a_i)$ 所组成的额外收益组合。它满足

$$p_i(a_i)=\begin{cases}0, & a_i=a_i^h\\ 0, & a_i=a_i^f\end{cases}$$

本文将上述重构协议设计模型所对应的重构约束机制称为可信机制 $M_{\text{Res}}^{\text{T}}$，下面证明该机制能帮助协议设计者有效约束理性用户的自利行为。

定理 3 在异步通信情形下的 (t,n) 理性秘密共享重构博弈 G_{Res} 中，可信机制 $M_{\text{Res}}^{\text{T}}$ 能有效约束理性的自利行为。

证明 由于验证信息的存在，使可信用户可验证理性用户发送的子秘密的正确性。因此，理性用户无法欺骗诚实用户。并且，由于可信用户将根据理性用户选择的行动策略决定是否将重构出的共享秘密 S 发送给理性用户。如果理性用户 P_i 选择策略 a_i^f，即不发送自己拥有的子秘密给诚实用户 P_h，其最终获得收益为

$$\overline{u}_i(a_i^f)=u_i(a_i^f,a_{h,i}^s)+p_i(a_i^f)=$$
$$\begin{cases}U_i^-,\text{至多有}t-2\text{个其余理性用户发送子秘密}\\ U_i^{--},\text{超过}t-1\text{个其余理性用户发送子秘密}\end{cases}$$

如果理性用户 P_i 选择策略 a_i^h，即发送自己拥有的子秘密给可信用户 P_h，其最终获得收益为

$$\overline{u}_i(a_i^h)=u_i(a_i^h)+p_i(a_i^h)=$$
$$\begin{cases}U_i,\text{超过}t-2\text{个其余理性用户发送子秘密}\\ U_i^-,\text{至多有}t-3\text{个其余理性用户发送子秘密}\end{cases}$$

显然，$\overline{u}_i(a_i^h)\geqslant\overline{u}_i(a_i^f)$。因此，由于自利性，理性用户 P_i 将不会选择行动策略 a_i^f。

综上所述，本文给出的可信机制 $M_{\text{Res}}^{\text{T}}$ 能有效帮助协议设计者有效约束理性用户的自利行为。因此，本文给出的面向可信用户环境的设计模型能帮助协议设计者有效地约束理性用户的自利行为，使设计的理性秘密重构协议具有公平性。

值得注意的是，在上述给出的面向纯理性用户环境、面向信誉环境和面向可信用户环境的理性秘密重构协议设计模型中，仅需将各设计模型中发送子秘密的顺序 F 调整为所有理性用户同时发送各自拥有的子秘密，就可用于同步通信情形下的理性秘密重构协议的设计。

5　设计实例

为表明所给出的设计模型具有可用性，本文将根据给出的面向信誉环境的设计模型来构造一个公平的理性秘密重构协议。

5.1　公平的理性秘密重构协议

假设在秘密分发阶段中，秘密分发者 Dealer 利用 Shamir 方案[40]中的方法将共享秘密 S 进行拆分；利用可公开验证秘密共享[41]的思想，选择单向承诺函数 $C(\cdot)$ 和承诺值 $C(s_i)$；最后，秘密分发者 Dealer 将子秘密 s_i 秘密地发送给理性用户 P_i，并广播发送 $C(\cdot)$ 和 $C(s_i)$。那么，本文所构造的理性秘密重构协议如下。

步骤 1　根据理性用户的信誉值的高低决定发送子秘密的先后顺序。即若 $r_i \leqslant r_j$，则理性用户 P_i 将先发送自己的子秘密 s_i。

步骤 2　P_i 发送自己的子秘密 s_i 给其余用户 $P_k(k \neq i)$；并等待接收其余理性用户 P_k 发送的消息 Info_k 并观察自己的信誉值 r_i。

1) 若 $\text{Info}_k =$ “OK”且理性用户 P_k 执行 $r_i \leftarrow r_i + 1$，then 进入步骤 3；

2) 否则，P_i 执行 $r_k \leftarrow r_k - 1$ 后进入步骤 3；

步骤 3　P_i 等待接收理性用户 P_j 发送的子秘密 s_j，并利用承诺函数验证其正确性。

1) 若 $C'(s_j) = C(s_j)$，P_i 发送 $\text{Info}_i =$ “OK”，并执行 $r_j \leftarrow r_j + 1$；

2) 否则，P_i 发送 $\text{Info}_i =$ “False”，并执行 $r_j \leftarrow r_j - 1$；

并且，P_i 始终观察 r_i, r_j 和 r_k。

1)当 $\text{Info}_i = \text{Info}_k =$ “OK”时，如果 P_k 正确地执行 $r_j \leftarrow r_j - 1$，则 P_i 执行 $r_k \leftarrow r_k - 1$；如果 P_j 执行 $r_k \leftarrow r_k - 1$，则 P_i 执行 $r_j \leftarrow r_j - 1$；

2) 当 $\text{Info}_i = \text{Info}_k =$ “False”时，如果 P_k 执行 $r_j \leftarrow r_j + 1$，则 P_i 执行 $r_k \leftarrow r_k - 1$；如果 P_j 执行 $r_k \leftarrow r_k + 1$，则 P_i 执行 $r_j \leftarrow r_j - 1$。

步骤 4　当理性用户 P_i 收到所有正确的子秘密后，利用拉格朗日插值法重构出共享秘密 S。

5.2　协议分析

1) 公平性

由定理 2 可知，在基于异步信道通信的 (t,n) 理性秘密共享重构博弈中，信誉机制 $M_{\text{Res}}^{\text{R}}$ 可有效地约束理性用户在已知最后重构轮中的自利行为。即 $\forall P_i, P_j \in P$，有

$$u_i(\boldsymbol{a}_{\text{Res}}^{\text{R}}) = U_i, u_j(\boldsymbol{a}_{\text{Res}}^{\text{R}}) = U_j$$

其中，$\boldsymbol{a}_{\text{Res}}^{\text{R}} \in Z$ 表示在信誉机制 $M_{\text{Res}}^{\text{R}}$ 约束下执行理性秘密重构博弈时形成的策略组合。因此，只要确保理性用户不恶意地执行信誉操作，那么本文提出理性秘密重构协议的公平性即可得到保证。

在提出的理性秘密重构协议中，当理性用户 P_i 恶意地改变理性用户 P_j 的信誉值 r_j 时，其余理性用户将会通过合理地降低理性用户 P_i 的信誉值 r_i 来提升自己的最终收益。因此，对于理性用户 P_i 来说，由于其自利性，他将不会对 r_j 进行恶意操作。因此，本文所提出的理性秘密共享协议的公平性将得以保证。

2) 正确性

由于承诺函数 $C(\cdot)$ 的存在，使理性用户可在秘密分发阶段中验证秘密分发者所分发的子秘密正确性。而在秘密重构阶段中，理性用户也可通过收到的承诺验证其余理性用户发送的子秘密的正确性。

因此，本文提出的协议可确保理性用户均接收到正确的子秘密，从而使协议执行完成时所有理性用户均可重构出正确的共享秘密。

3) 安全性

由于该协议是基于多项式函数对共享秘密进行拆分的，那么根据线性方程组解的性质可知，即使用户获得数量少于 t 个的子秘密也不能得到关于共享秘密 S 的任何信息。即

$$\forall P_i \in P \text{ 和 } \boldsymbol{a} = (a_{l_1}^h, \cdots, a_{l_k}^h, a_i, a_{m_1}, \cdots, a_{m_{k'}}) \in Z$$

有

$$\text{Res}(|s| \,|\, \boldsymbol{a}) = \begin{cases} S, k \geqslant t-1 \\ \perp, k < t-1 \end{cases}$$

因此，本文提出的基于信誉的理性秘密重构协议也是安全的。

6 结束语

由于缺少设计参考模型，导致协议设计者在设计理性秘密重构协议时往往依赖个人经验，难以充分考虑理性用户在“利益最大化”驱使下的策略选择。这就导致如果直接使用现有的理性秘密重构协议，不仅只有部分理性用户能恢复共享秘密，甚至还会出现部分理性用户将错误的秘密视为真实共享秘密的极端情形。为解决上述问题，本文基于理性用户的形式化模型，通过构建理性秘密重构博弈模型来分析自利的用户在执行秘密重构协议时追求“利益最大化”的策略选择，分别提出了适用于不同应用场景的理性秘密重构协议设计模型。理论证明和实例设计分别说明了本文给出的设计模型的有效性和实用性。

参考文献：

[1] KHAN W Z, AHMED E, HAKAK S, et al. Edge computing: a survey[J]. Future Generation Computer Systems, 2019, 97: 219-235.

[2] HABIBI P, FARHOUDI M, KAZEMIAN S, et al. Fog computing: a comprehensive architectural survey[J]. IEEE Access, 2020, 8: 69105-69133.

[3] GAI K K, GUO J N, ZHU L H, et al. Blockchain meets cloud computing: a survey[J]. IEEE Communications Surveys & Tutorials, 2020, 22(3): 2009-2030.

[4] 谭振华, 杨广明, 王兴伟, 等. 面向云存储的多维球面门限秘密共享方案[J]. 软件学报, 2016, 27(11): 2912-2928.
TAN Z H, YANG G M, WANG X W, et al. Threshold secret sharing scheme based on multidimensional sphere for cloud storage[J]. Journal of Software, 2016, 27(11): 2912-2928.

[5] ATTASENA V, DARMONT J, HARBI N. Secret sharing for cloud data security: a survey[J]. The VLDB Journal, 2017, 26(5): 657-681.

[6] 马利民, 王佳慧. 基于改进 FEMD 算法的可逆秘密图像共享方案[J]. 通信学报, 2019, 40(7): 48-56.
MA L M, WANG J H. Invertible secret image sharing scheme based on improved FEMD[J]. Journal on Communications, 2019, 40(7): 48-56.

[7] CAPUTO S, KORCHMÁROS G, SONNINO A. Multilevel secret sharing schemes arising from the normal rational curve[J]. Discrete Applied Mathematics, 2020, 284: 158-165.

[8] YANG J, FU F W. New dynamic and verifiable multi-secret sharing schemes based on LFSR public key cryptosystem[J]. IET Information Security, 2020, 14(6): 783-790.

[9] DESMEDT Y, SLINKO A. Realistic versus rational secret sharing[C]//Lecture Notes in Computer Science. Berlin: Springer, 2019: 152-163.

[10] HALPERN J, TEAGUE V. Rational secret sharing and multiparty computation: extended abstract[C]//Proceedings of the thirty-sixth annual ACM symposium on Theory of computing – STOC’04. New York: ACM Press, 2004: 623-632.

[11] MALEKA S, SHAREEF A, PANDU R C. The deterministic protocol for rational secret sharing[C]//Proceedings of 2008 IEEE International Symposium on Parallel and Distributed Processing. Piscataway: IEEE Press, 2008: 1-7.

[12] MALEKA S, SHAREEF A, RANGAN C P. Rational secret sharing with repeated games[C]//Information Security Practice and Experience. Berlin: Springer, 2008: 334-346.

[13] KOL G, NAOR M. Cryptography and game theory: designing protocols for exchanging information[C]//Theory of Cryptography. Berlin: Springer, 2008: 320-339.

[14] KOL G, NAOR M. Games for exchanging information[C]//Proceedings of the fortieth annual ACM symposium on Theory of computing. New York: ACM Press, 2008: 423-432.

[15] FUCHSBAUER G, KATZ J, NACCACHE D. Efficient rational secret sharing in standard communication networks[C]//Theory of Cryptography. Berlin: Springer, 2010: 419-436.

[16] CAI Y Q, SHI H L. Rational secret sharing scheme based on probability encryption without trusted center[J]. Journal of Networks, 2011, 6(6): 899-903.

[17] DANI V, MOVAHEDI M, SAIA J. Scalable mechanisms for rational secret sharing[J]. Distributed Computing, 2015, 28(3): 171-187.

[18] KAWACHI A, OKAMOTO Y, TANAKA K, et al. General constructions of rational secret sharing with expected constant-round reconstruction[J]. The Computer Journal, 2016, 60(5): 711-728.

[19] ZHANG Z F, LIU M L. Unconditionally secure rational secret sharing in standard communication networks[C]//Information Security and Cryptology - ICISC 2010. Berlin: Springer, 2011: 355-369.

[20] ZHANG E, YUAN P Y, DU J. Verifiable rational secret sharing scheme in mobile networks[J]. Mobile Information Systems, 2015, 2015: 1-7.

[21] DE S J, RUJ S. Failure tolerant rational secret sharing[C]//Proceedings of 2016 IEEE 30th International Conference on Advanced Information Networking and Applications (AINA). Piscataway: IEEE Press, 2016: 925-932.

[22] 田有亮, 王雪梅, 刘琳芳. 基于马尔可夫决策的理性秘密共享方案[J]. 通信学报, 2015, 36(9): 222-229.
TIAN Y L, WANG X M, LIU L F. Rational secret sharing scheme based on Markov decision[J]. Journal on Communications, 2015, 36(9): 222-229.

[23] NOJOUMIAN M, STINSON D R. Socio-rational secret sharing as a new direction in rational cryptography[C]//Lecture Notes in Computer Science. Berlin: Springer, 2012: 18-37.

[24] NOJOUMIAN M. Generalization of socio-rational secret sharing with a new utility function[C]//Proceedings of 2014 Twelfth Annual International Conference on Privacy, Security and Trust. Piscataway: IEEE Press, 2014: 338-341.

[25] WANG Y L, XU Q L. 2-out-of-2 rational secret sharing in extensive form[C]//Proceedings of 2011 Seventh International Conference on Computational Intelligence and Security. Piscataway: IEEE Press, 2011: 847-851.

[26] TIAN Y L, PENG C G, LIN D D, et al. Bayesian mechanism for rational secret sharing scheme[J]. Science China Information Sciences, 2015, 58(5): 1-13.

[27] WANG J, CAI Y Q. A rational secret sharing scheme based on repeated game[C]//Proceedings of 2011 Seventh International Conference on Computational Intelligence and Security. Piscataway: IEEE

Press, 2011: 615-619.
[28] YU Y, ZHOU Z F. An efficient rational secret sharing protocol resisting against malicious adversaries over synchronous channels[C]//Information Security and Cryptology. Berlin: Springer, 2013: 69-89.
[29] 彭长根, 刘海, 田有亮, 等. 混合偏好模型下的分布式理性秘密共享方案[J]. 计算机研究与发展, 2014, 51(7): 1476-1485.
PENG C G, LIU H, TIAN Y L, et al. A distributed rational secret sharing scheme with hybrid preference model[J]. Journal of Computer Research and Development, 2014, 51(7): 1476-1485.
[30] ASHAROV G, LINDELL Y. Utility dependence in correct and fair rational Secret Sharing[J]. Journal of Cryptology, 2011, 24(1): 157-202.
[31] DE S J, PAL A K. Achieving correctness in fair rational secret sharing[C]//Cryptology and Network Security. Cham: Springer International Publishing, 2013: 139-161.
[32] DE S J, RUJ S, PAL A K. Should silence be heard? fair rational secret sharing with silent and non-silent players[C]//Cryptology and Network Security. Cham: Springer International Publishing, 2014: 240-255.
[33] JIN J H, ZHOU X, MA C G, et al. A rational secret sharing relying on reputation[C]//Proceedings of 2016 International Conference on Intelligent Networking and Collaborative Systems (INCoS). Piscataway: IEEE Press, 2016: 384-387.
[34] NOJOUMIAN M, STINSON D R, GRAINGER M. Unconditionally secure social secret sharing scheme[J]. IET Information Security, 2010, 4(4): 202.
[35] GORDON S D, KATZ J. Rational secret sharing, revisited[C]//Lecture Notes in Computer Science. Berlin: Springer, 2006: 229-241.
[36] ABRAHAM I, DOLEV D, GONEN R, et al. Distributed computing meets game theory: robust mechanisms for rational secret sharing and multiparty computation[C]//Proceedings of the twenty-fifth annual ACM symposium on Principles of distributed computing. New York: ACM Press, 2006: 53-62.
[37] MICALI S, SHELAT A. Purely rational secret sharing (extended abstract)[C]//Theory of Cryptography. Berlin:Springer, 2009: 54-71.
[38] ONG S J, PARKES D C, ROSEN A, et al. Fairness with an honest minority and a rational majority[C]//Theory of Cryptography. Berlin: Springer, 2009: 36-53.
[39] ZHANG Z F, LIU M L. Rational secret sharing as extensive games[J]. Science China Information Sciences, 2013, 56(3): 1-13.
[40] SHAMIR A. How to share a secret[J]. Communications of the ACM, 1979, 22(11): 612-613.
[41] STADLER M. Publicly verifiable secret sharing[C]//Advances in Cryptology — EUROCRYPT'96. Berlin: Springer, 1996: 190-199.

[作者简介]

刘海（1984− ），男，河北献县人，博士，贵州财经大学副教授，主要研究方向为密码协议、大数据安全和隐私保护。

田有亮（1982− ），男，贵州盘县人，博士，贵州大学教授、博士生导师，主要研究方向为密码学与隐私计算等。

唐莹（1982− ），女，重庆人，贵州财经大学教师，主要研究方向为博弈论和数据安全。

Jianbing Ni（1988− ），男，博士，女王大学助理教授，主要研究方向为无线通信和网络安全、移动计算安全、机器学习安全和区块链技术。

马建峰（1963− ），男，陕西西安人，博士，西安电子科技大学教授、博士生导师，主要研究方向为应用密码学、无线网络安全、数据安全、移动智能系统安全等。