抗合谋理性多秘密共享方案

张 恩 孙权党 刘亚鹏
(河南师范大学计算机与信息工程学院 新乡 453007)
("智慧商务与物联网技术"河南省工程实验室 新乡 453007)

摘 要 提出了一种可抗合谋的理性多秘密共享方案。分析了成员合谋行为及防范对策,设计了可计算防合谋均衡方法,构建了预防参与者合谋的博弈模型,使得参与者所采取的策略满足可计算防合谋均衡,合谋成员不清楚当前轮是真秘密所在轮,还是检验参与者诚实度的测试轮,参与者采取合谋策略的期望收益没有遵守算法的收益大,因此,理性的参与者没有动机合谋攻击。另外,在方案中分发者不用为参与者分配秘密份额,在秘密重构阶段,无需可信者参与,也没有利用安全多方计算。最终,每位参与者可以得到多个秘密。解决了参与者合谋问题及理性单秘密共享效率低下的问题。

关键词 理性秘密共享,博弈论,抗合谋,可证明安全
中图法分类号 TP309 **文献标识码** A **DOI** 10.11896/j.issn.1002-137X.2015.10.033

Collusion-free Rational Multi-secret Sharing Scheme

ZHANG En SUN Quan-dang LIU Ya-peng
(College of Computer and Information Engineering, Henan Normal University, Xinxiang 453007, China)
(Engineering Lab of Intelligence Business & Internet of Things of Henan Province, Xinxiang 453007, China)

Abstract A collusion-free scheme for rational multi-secret sharing was proposed. Collusive behavior and preventive measures were analyzed. The coalition-proof model and algorithm were developed to make the participants' strategies satisfy computational coalition-proof equilibrium. The participants do not know whether the current round is a test round. Rational players can not gain more by coalition, so rational players have no incentive to collude in the protocol. In addition, the dealer doesn't need to distribute a secret share among the participants, and the scheme assumes neither the availability of a trusted party nor multi-party computations in the secret reconstruction phase. Finally, every player can obtain multi-secret fairly. The scheme is collusion-free and avoids the inefficiency of the rational single secret sharing scheme.

Keywords Rational secret sharing, Game theory, Collusion-free, Provably secure

1 引言

秘密共享是信息安全研究的重要内容和密码协议设计的一个基本工具。经典的(m,n)门限秘密共享方案由 Shamir[1] 和 Blakeley[2] 于1979年分别提出。方案要求大于或等于 m 人方可重构出秘密,少于 m 人合作得不到秘密。之后,Chor 等人[3]和 Feldman 等人[4]提出可验证秘密共享方案。Hou 等人[5]和 Wu 等人[6]对可视秘密共享进行了研究,文献[7-10]对多秘密共享方案进行了研究,在每次秘密分发过程中,秘密分发者不必重新分配秘密份额,可以一次性重构 p ($p\geqslant 1$)个秘密。但受经典密码协议束缚,文献[1-8]存在参与者单独欺骗或者合谋欺骗的问题,例如,在重构过程中,一个参与者 A 没有广播他的子份额,而其他 $m-1$ 个人广播了各自的子份额,这样 A 可以独享秘密(尽管参与者的欺骗行为能被可验证的手段检验到,但为时已晚)。同样,参与者也可以通过合谋欺骗其他参与者,那么合谋集团则独得秘密。比如两个参与者合谋不广播或者广播错误的子份额,而其他 $m-2$ 个参与者广播正确的子份额,那么最终只有两个合谋成员能获得秘密;如果 $m-1$ 个成员合谋欺骗,则他们只需要再骗取1个子份额即可,可见传统的通过同时广播信道进行重构的协议不能防止参与者欺骗和合谋(即使仅有两个参与者合谋)。文献[9,10]在秘密重构阶段需要有可信的计算者参与,诚然,如果存在可信的计算者,那么由于秘密共享的性质,少于或等于 $m-1$ 个合谋者是不能独自得到结果的。然而网络环境下很难找到参与各方都信任的可信方,即使找到这样的可信者,其也可能成为网络资源的瓶颈,同时也会成为黑客集中攻击的对象。

博弈论又叫对策论,是一门以数学为基础,研究对抗冲突中最优解的学科,其在很多学科都有重要的应用。Halpern 和 Teague[11] 首次提出将博弈论引入秘密共享方案和安全多

到稿日期:2014-10-10 返修日期:2015-01-23 本文受国家自然科学基金资助项目(61170221),河南省教育厅科学技术重点研究项目(14A520032),河南省高等教育教学改革研究项目(2014SJGLX185)资助。

张 恩 博士,副教授,主要研究方向为信息安全、密码协议;孙权党 硕士,副教授,主要研究方向为计算机网络多媒体技术;刘亚鹏 硕士生,主要研究方向为信息安全。

方计算，从此开辟了一个新兴的密码学研究方向，即理性的密码协议。不同于传统方案中将参与者分为诚实者和恶意者，在理性密码协议中，所有的参与者都是理性的和自私的，所采取的任何策略都是为了使自身的利益最大化。为了使协议满足纳什均衡，Halpern 和 Teague 设计的方案采用了迭代删除弱优策略的方法，但他们的协议只能满足 $m\geqslant 3$ 的情形，并且分发者需要一直在线；另外，方案没有考虑博弈中的可计算问题和防合谋问题（其方案不能防止参与者分组执行协议时，组长之间的合谋攻击）。之后，文献[12-15] 对理性安全多方计算进行了研究。文献[16-25]对理性秘密共享进行了研究，G. Kol等人[16]采用有意义/无意义的加密和安全多方计算等工具，提出一种理性秘密共享方案，但参与者有可能在安全多方计算阶段合谋攻击。G. Kol 等人[17]采用一种信息论安全的方法设计了一种秘密共享方案，他们的方案中不需要可计算假设，但不能防止拥有短份额的人和拥有长份额的人合谋攻击。S. Maleka 和 S. Amjed[18]提出一种基于重复博弈的秘密共享方案，要求构造子秘密的任意两个多项式的次数最多相差为 1，参与者不知道其他参与者多项式的次数，但参与者在自己最后一轮可以通过欺骗，以较高的概率获得秘密，所以他们的方案对逆向归纳来说是敏感的；再有，他们的方案也不能防止参与者合谋攻击，例如如果有两个合谋者拥有的多项式的次数相差为 1，那么合谋者能合谋得到秘密，同时阻止其他参与者获得秘密。文献[19,20]提出的方案需要外部可信方在重构阶段参与。此后，文献[21-23]分别基于 RSA-OAEP、双线性对和扩展博弈各自提出一种理性秘密共享方案。Yu 等人[24]考虑了有恶意参与者的情况，Tian 等人[25]设计了一种公平的理性秘密共享方案。但以上理性秘密共享方案均为单秘密共享方案，在共享多个秘密时，需要多次调用协议，并且都没有对参与者的合谋动机、合谋收益以及防合谋均衡进行建模和分析。同时现有的理性秘密共享协议缺少严格和缜密的安全证明，不利于方案的推广和应用。如何利用可证明安全的理论对方案进行规约和证明，也是设计理性秘密共享方案亟需解决的重要问题。

本文的主要贡献是：提出了一种可抗合谋的理性多秘密共享方案，解决了理性单秘密共享效率低下以及参与者合谋的问题，同时利用规约证明的方法分析和证明了方案的安全性。在提出的方案中，参与者使用各自的私钥对每一轮数字的加密作为他们的秘密份额，秘密分发者只需计算一些公开信息，不需要进行秘密份额的分配，从而在很大程度上提高了秘密分发的效率。在重构阶段，所提方案没有采用文献[16]中所利用的安全多方计算工具，同时无需可信的计算者参与。在设计的方案中，每个参与者不清楚协议中当前轮是真秘密所在轮，还是检验参与者诚实度的测试轮，合谋成员偏离协议的期望收益没有遵守协议的收益大；另外，本文提出了可计算防合谋均衡的定义，建立了抗合谋的博弈模型，并且证明了当方案满足可计算防合谋均衡时，理性的参与者没有动机合谋，最终每个参与者能够公平地得到多个秘密。

2 预备知识

2.1 抗合谋博弈模型及其均衡

博弈论是研究在相互依存条件下如何进行理性决策的理论。博弈中的均衡是一种稳定的状态，但不是说任何博弈的结果都能成为均衡。如果所有博弈方都预测一个特定的博弈结果会出现，而且还预测到他们的对手也会预测到该结果，还可以预测他们的对手会预测自己会预测到该结果……，那么没有哪个博弈方有偏离这个结果的愿望，因此这个预测结果最终会成为博弈的结果。也就是说，各博弈方的实际行为选择与他们的预测一致。当用博弈论分析问题时，假设每个人都是理性的，即人人都会在一定的约束条件下最大化自身的利益，如果在协议中，人人都觉得在给定对方策略的情况下自己的利益已经最大化了，通俗地讲就是给定你的策略，我的策略是最好的策略，给定我的策略，你的策略也是你最好的策略，那么参与者在给定对方策略下，不愿意调整自己的策略，最好的策略是遵守协议。详细的博弈论知识请见文献[26,27]。

用 a_i 表示参与者 P_i 的策略，$a=(a_1,\cdots,a_n)$ 表示所有参与者的策略组合，a_{-i} 表示除 P_i 外其他人的策略，$(a_i',a_{-i})=(a_1,\cdots,a_{i-1},a_i',a_{i+1},\cdots,a_n)$ 表示参与者 P_i 的策略改为 a_i'，$u_i(a)$ 表示 P_i 在给定策略集 a 的条件下的收益。

在理性的秘密共享协议中，参与者的最大收益是了解秘密，其次是让尽可能少的其他人了解秘密，用 $u_i(o)$ 表示 P_i 关于结果 o 的效益函数，用 U^+,U,U^-,U^{--} 表示参与者在以下几种情况下的收益：(a)当 o 表示 P_i 了解秘密而其他参与者不了解秘密时，那么 $u_i(o)=U^+$；(b)当 o 表示 P_i 了解秘密而至少有一个其他参与者也了解秘密时，那么 $u_i(o)=U$；(c)当 o 表示 P_i 不了解秘密而其他参与者也不了解秘密时，那么 $u_i(o)=U^-$；(d)当 o 表示 P_i 不了解秘密而至少有一个其他参与者了解秘密时，$u_i(o)=U^{--}$。他们之间的关系是 $U^+>U>U^->U^{--}$。下面考虑只有两方参与者的情形，在秘密重构的过程中，每个参与者有两种策略：诚实地广播秘密（用 H 表示）或欺骗（用 D 表示）。该博弈如表 1 所列。

表 1 两方秘密共享策略博弈

	H	D
H	U,U	U^{--},U^+
D	U^+,U^{--}	U^-,U^-

从表 1 可以看出该博弈有唯一的纳什均衡：(D,D)。对于理性的参与者来说，在一次博弈中，最优的策略是采用欺骗的策略，如果大家都采用欺骗的策略，则秘密不可能在一次博弈中被重构出来。

引理 1 如果参与者知道博弈什么时候结束，那么他将没有合作的动机。

证明：如果参与者知道博弈在哪一轮结束，那么在这一轮欺骗者通过欺骗将独得秘密，因为他们不害怕有进一步的惩罚措施，所以就没有合作的动机。用逆向归纳法来分析：在每一轮，所有的参与者将保持沉默，秘密不会被重构。

定义 1 在博弈 $\Gamma=(\{A_i\}_{i=1}^n,\{u_i\}_{i=1}^n)$ 中，策略组合 $a=(a_1,\cdots,a_n)\in A$ 是一个纳什均衡，如果任一博弈方 i 的策略都是对其余博弈方策略的最佳对策，也就是说博弈保持

$$u_i(a_i',a_{-i})\leqslant u_i(a) \tag{1}$$

纳什均衡的价值主要在于它有一些非常重要的性质，“一致预测性”是其中最重要的性质之一。在纳什均衡下，任何理性的博弈方都不会单独改变策略，因为改变策略意味着自身利益的损失。

下面考虑多人合谋背离协议的情况。如果部分参与者通过合谋串通可能比不合谋时获得更大的利益，那么参与者就有很强的串通动机。通常的纳什均衡分析在这样的博弈问题中也会遇到问题。通过下面两个得益矩阵来进行分析，如表2、表3所列。

表2 多人博弈中的共谋情景1

		博弈方2	
		L	R
博弈方1	H	0,0,8	−3,−3,0
	M	−3,−3,0	2,2,−3

（博弈方3-U）

表3 多人博弈中的共谋情景2

		博弈方2	
		L	R
博弈方1	H	−2,−2,0	−3,−3,0
	M	−3,−3,0	−1,−1,3

（博弈方3-D）

在上面两个得益矩阵表示的博弈中，博弈方1的策略为H、M，博弈方2的策略为L、R，博弈方3的策略为U、D。表2为博弈方3选择U时，3个参与方的博弈；表3为博弈方3选择D时，3个参与方的博弈。容易发现，该博弈有两个纯策略纳什均衡(H,L,U)和(M,R,D)，前者帕累托效率(所有博弈方都偏好其中一个纳什均衡)优于后者，如果不考虑部分博弈方合谋，那么该博弈结果应为(H,L,U)。

但是，如果考虑到博弈方中间存在合谋的情况，那么情况会完全不一样。假设博弈方3选择U，如果博弈方1和博弈方2合谋采用M和R，那么他们可以获得2单位的收益，所以他们是有合谋的动机的。而防合谋的目标就是要排除部分博弈方合谋给博弈结果带来的不稳定性，使博弈分析的结论和预测更加可靠。策略组合(M,R,D)虽然在帕累托效率上明显不如(H,L,U)，但它却是防合谋均衡，因为无论是单人偏离，还是2人合谋偏离或3人联合偏离，都不能增加博弈方的利益。所以策略组合(M,R,D)具有更强的稳定性。

考虑到协议中参与者合谋的问题，协议所建立的抗合谋博弈模型应满足：(1)没有任何单个参与者的串通会改变博弈的结果，即单独改变策略无利可图(意味着该策略首先是一个纳什均衡)；(2)没有任何两个博弈方的串通会改变博弈的结果；(3)以此类推，直到所有博弈方都参加的串通也不会改变博弈的结果。其目标就是要排除由于多人博弈中可能存在部分博弈方结成小团体联合行动会给博弈结果带来的不稳定性等问题。

考虑到密码协议中一些密码原语的可计算安全性，提出可计算防合谋均衡的概念和设计方法。在满足该均衡的情况下，每一个博弈方在其余博弈方策略的基础上最大化了自己的利益，所以没有任何人会偏离纳什均衡策略，即合谋成员中任何偏离都不会为自己带来利益。所以理性的合谋成员不会选择合谋偏离协议。后面将证明本文设计的协议满足可计算防合谋均衡。

定义2 在博弈 $\Gamma=(\{A_i\}_{i=1}^n,\{u_i\}_{i=1}^n)$ 中，用 T 表示一个合谋集团，且 k 为密码协议的安全参数，假设对于每个合谋团体来说，不合谋的策略为 a_T，合谋的策略为 a_T'，非合谋团体的策略为 a_{-t}，称策略组合 $a=(a_1,\cdots,a_n)\in A$ 是一个可计算防合谋均衡，如果对于 $P_i\in T$，存在一个可忽略的函数 $\varepsilon(k)$，博弈能够保持

$$u_i(a_T'(k),a_{-T}(k))\leqslant u_i(a_T(k),a_{-T}(k))+\varepsilon(k) \tag{2}$$

2.2 双线性映射及困难问题

定义3 设 G_1 和 G_2 是2个阶为素数 p 的循环群，令 g 为 G_1 的生成元。如果 $e:G_1\times G_1\to G_2$ 满足

(1)双线性性：对任意的 $u,v\in G_1$ 和 $a,b\in Z_p^*$，有 $e(u^a,v^b)=e(u,v)^{ab}$。

(2)非退化性：$e(g,g)\neq 1$。

(3)可计算性：对任何 $u,v\in G_1$，都存在有效的算法来计算 $e(u,v)$。

则称 e 为双线性映射。双线性映射可以由 Weil 映射和 Tate 映射得到。

定义4(双线性 Diffie-Hellman 问题) 对于给定的 aP，bP，$cP\in G_1$，计算 $e(P,P)^{abc}$ 是非常困难的，这里 $a,b,c\in Z_n^*$ 是未知的整数，也称为 BDH 问题。

定义5(判定双线性 Diffie-Hellman 逆问题假设，Decisional Bilinear Diffie-Hellman Inversion Assumption) 具有多项式时间能力的敌对者不能以不可忽略的优势区分四元组 $(g,g^x,\cdots,g^{(x^q)},e(g,g)^{1/x})$ 和 $(g,g^x,\cdots,g^{(x^q)},\Gamma)$，$x\in Z_p^*$，$\Gamma\in G_2$。该假设也称为 q-DBDHI 问题。

2.3 可验证的随机函数

可验证随机函数(Verifiable Random Functions，VRF)的概念由 Micali，Rabin 和 Vadhan[28] 首先提出，其定义如下：设 G,F,V 都是多项式时间算法：G(函数生成单元)，输入是安全参数，输出 PK,SK。$F=(F_1,F_2)$(函数计算单元)是确定性算法，输入为 SK,x，输出 $v=F_1(Sk,x)$ 和相应的证据 $proof=F_2(SK,x)$。V(函数验证单元)是概率算法，输入为 PK,x,v 及 $proof$，输出为 YES 或 NO。文献[29]基于双线性对构造了一种高效的可验证随机函数，方案如下：

a)公私钥产生模块 $Gen(1^k)$：输入 1^k，输出 $SK=s,PK=g^s$。

b)加密模块 $F_{SK}(x)$：输入 SK,x，输出

$$y=F_{SK}(x)=e(g,g)^{1/(x+SK)} \tag{3}$$

c)证据模块 $\pi_{SK}(x)$：输入 SK,x，输出

$$\pi=\pi_{SK}(x)=g^{1/(x+SK)} \tag{4}$$

d)验证模块 $V_{PK}(x,y,\pi)$：判定 y 是否是与输入 x 对应的输出，输入(PK,x,y,π)，验证式(5)和式(6)是否成立。

$$e(g^x\cdot PK,\pi)=e(g,g) \tag{5}$$

$$y=e(g,\pi) \tag{6}$$

若两式都成立则输出1；否则输出0。

3 抗合谋理性多秘密共享方案

3.1 系统参数

令 $P=\{P_0,\cdots,P_n\}$ 表示 n 个参与者，用 $s_0,s_1,\cdots,s_{p-1}$ 表示 p 个秘密，$h:\{0,1\}^*\to Z_q^*$ 为防碰撞哈希函数，F_q 为包含 q 个元素的有限域，其中 q 为一个大素数。系统工作在 F_q 上，系统中所有的参数都是 F_q 中的元素。

3.2 秘密分享阶段

Setp1 分发者根据几何分布选择 $r^*\in Z^+$(Z^+ 为正整数集)，几何分布的参数为 λ(一次贝努利实验中秘密出现的概

率),λ的值取决于参与者的效益,例如,如果参与者的效益很大,则可将λ设小一点,增加协议的期望执行轮数以增大参与者背离协议的风险(所提协议的模型是建立在完全信息静态博弈下的,参与者对他人采取策略的收益是完全了解的,每个参与者都能通过计算获得λ的值,同时也都清楚分发者一定会采取这样的λ值来防范参与者背离协议,但参与者无法了解分发者选择的r^*值)。分发者使用$Gen(1^k)$模块产生$(pk_1, sk_1), \cdots, (pk_n, sk_n)$,其中$pk_n = g^{*_n}$。

Setp2 秘密分发者使用n个数值对$(h(ID_1 \| r^*), F_{*_1}(r^*)), \cdots, (h(ID_n \| r^*), F_{*_n}(r^*))$和$(0, s_0), (1, s_1), \cdots, (p-1, s_{p-1})$确定一个$n+p-1$次多项式,如式(7)。

$$G(x) = \sum_{i=1}^{n} F_{*_i}(r^*) \prod_{j=1, j\neq i}^{n} \frac{x - h(ID_j \| r^*)}{h(ID_i \| r^*) - h(ID_j \| r^*)} \prod_{j=0}^{p-1} \frac{x-j}{h(ID_i \| r^*) - j} + \sum_{i=0}^{p-1} s_i \prod_{j=0, j\neq i}^{p-1} \frac{x-j}{i-j} \prod_{j=1}^{n} \frac{x - h(ID_j \| r^*)}{i - h(ID_j \| r^*)} \bmod q$$
$$= a_0^{r^*} + a_1^{r^*} x + a_2^{r^*} x^2 + \cdots + a_{n+p-1}^{r^*} x^{n+p-1} \quad (7)$$

令

$$V_0^* = s_0 \oplus G(0), V_1^* = s_1 \oplus G(1), \cdots, V_{p-1}^* = s_{p-1} \oplus G(p-1)$$

Step3 为了防止与$h(ID_i \| r)$ $(i=1,2,\cdots,n; r=1,2,\cdots,r^*)$重复,分发者从$[p, q-1] - \{h(ID_i \| r) \mid i=1,2,\cdots,n; r=1,2,\cdots,r^*\}$中选取$n+p-t$个最小的整数$d_1, \cdots, d_{n+p-t}$。

Step4 将sk_i通过安全信道传给参与者i,同时公布如下数据:a)公钥$pk_i (i=1,2,\cdots,n)$;b)$n+p-t$个二元数组$(d_1, G(d_1)), \cdots, (d_{n+p-t}, G(d_{n+p-t}))$;c)$V_j^* = s_j \oplus G(j) (j=0,\cdots,p-1)$;d) $h(a_k^*) (k=0,\cdots,n+p-1)$,其中$a_k^*$为多项式$G(x)$的系数。

3.3 秘密重构阶段

在第$r (r=1,\cdots,r^*)$轮,参与者做以下工作:

Step1 参与者$i (i=1,2,\cdots,m)$同时广播发送$y_i^r = F_{*_i}(r) = e(g,g)^{1/(r+*_i)}$,$\pi_i^r = \pi_{*_i}(r) = g^{1/(r+*_i)}$给其他参与者。

Step2 参与者i收到$y_j^r, \pi_j^r (j=1,2,\cdots,i-1,i+1,\cdots,n)$,判断$e(g^r \cdot pk_j, \pi_j^r) = e(g,g)$与$y_j^r = e(g, \pi_j^r)$是否成立。若两式都成立,输出1,执行Step3;否则输出0(即出现欺骗行为),协议终止。

Step3 P_i利用参与者身份信息可以构造m个数值对$(h(ID_1 \| r), F_{*_1}(r)), \cdots, (h(ID_m \| r), F_{*_m}(r))$,结合$(d_1, G(d_1)), \cdots, (d_{n+p-m}, G(d_{n+p-m}))$共$n+p$个数值对可以确定一个$n+p-1$次多项式,如式(8):

$$P(x) = \sum_{u=1}^{m} F_{*_u}(r) \prod_{j=1, j\neq u}^{m} \frac{x - h(ID_j \| r)}{h(ID_u \| r) - h(ID_j \| r)} \prod_{k=1}^{n+p-m} \frac{x-d_k}{h(ID_u \| r) - d_k} + \sum_{i=1}^{n+p-m} G(d_i) \prod_{k=1, k\neq i}^{n+p-m} \frac{x-d_k}{d_i - d_k} \prod_{u=1}^{m} \frac{x - h(ID_u \| r)}{d_i - h(ID_u \| r)} \bmod q$$
$$= b_0^r + b_1^r x + b_2^r x^2 + \cdots + b_{n+p-1}^r x^{n+p-1} \quad (8)$$

Step4 如果$h(a_k^{r^*}) = h(b_k^r) (k=0,\cdots,n+p-1)$,那么这$p$个秘密为$s_i = P(i) \oplus V_i^* (i=0,1,\cdots,p-1)$,协议结束;否则,协议进行到下一轮。

4 方案分析

4.1 正确性分析

定理1 参与者能通过判断$e(g^r \cdot pk_j, \pi_j^r) = e(g,g)$与$y_j^r = e(g, \pi_j^r)$是否成立,来验证参与者发送份额的正确性。

证明:

$$e(g^r \cdot pk_j, \pi_j^r) = e(g^r \cdot g^{*_j}, g^{1/(r+*_j)}) = e(g^{r+*_j}, g^{1/(r+*_j)}) = e(g,g)^{(r+*_j)/(r+*_j)} = e(g,g)$$
$$y_j^r = e(g,g)^{1/(r+*_j)} = e(g, g^{1/(r+*_j)}) = e(g, \pi_j^r)$$

这样,每一位参与者都能确信他所获得的子份额是合法且有效的。

4.2 安全性分析

可证明安全性理论是一种公理化的研究方法,在计算复杂性理论的框架下,利用规约的方法将基础密码模块规约到对安全协议的攻击。假如存在一个攻击者能够对密码协议发动有效的攻击,那么就可以利用该攻击者构造一个算法用于求解困难问题(如大整数分解、二次剩余、离散对数、q-DBDHI等)或者破解基础密码模块。首先用可证明安全的理论方法证明攻击者不能获得和伪造信息,之后借助博弈论分析了理性参与者没有合谋攻击本文协议的动机。

引理2 如果具有多项式计算能力的攻击者A,能以ε优势突破本协议算法,构造出假的VRF输出值,那么可以构造一个模拟算法B以不可忽略的优势求解q-DBDHI困难问题。

证明:假设存在算法A能够以ε优势区分$y = F_{SK}(x) = e(g,g)^{1/(x+SK)}$和$G_2$中的一个随机元素,则能构造算法$B$利用算法$A$求解DBDHI问题的优势为$\varepsilon/2$。即给定$(g, g^a, \cdots, g^{(a^q)}, \Gamma)$,$\Gamma$或者为$e(g,g)^{1/a}$,或者是$G_2$中的一个随机元素,$B$试图以不可忽略的优势区分,如果$\Gamma$为$e(g,g)^{1/a}$就输出0,否则输出1。

首先挑战者设置群G_1和G_2,确定双线性变换e和生成元g。然后挑战者在在B视野外投币随机选择ξ,如果$\xi=0$,挑战者设置$\Gamma = e(g,g)^{1/a}$;如果$\xi=1$,设置Γ是G_2中的随机元素。

初始阶段:模拟算法B运行A,选择伪造某一个输入x_0的VRF值,令$\chi = \alpha - x_0$,定义一个函数$m(o) = \sum_{j=0}^{q-1} c_j o^j$,$m'(o) = \sum_{j=0}^{q-2} r_j o^j$,计算$n = g^{m(\chi)}$,得到$PK = n^\chi$和$SK = \chi$,并将公钥PK发送给攻击者$A$。

阶段1 攻击者询问$x_i (x_i \neq x_0)$的VRF值,预言机返回$\pi_{SK}(x_i) = n^{1/(x_i+\chi)}$,$F_{SK}(x_i) = e(n,n)^{1/(x_i+\chi)}$返回给$A$。

挑战阶段:A选择两个等长的值x_0, x_1发给B,B随机选择一个$\psi (\psi=0$或$1)$值后生成$\pi_\psi = \pi_{SK}(x_\psi) = n^{1/(x_\psi+\chi)}$,$y_\psi = F_{SK}(x_\psi) = e(n,n)^{1/(x_\psi+\chi)}$。

设$\Gamma^* = \Gamma^{(r^2)} \cdot e(g,g)^{(m(\chi)^2 - r^2)/a}$,如果$\Gamma = e(g,g)^{1/a}$,那么$\Gamma^* = (n,n)^{1/a}$。将$\pi_\psi, y_\psi, \Gamma^*$发给攻击者$A$,即当$\xi=0$时,$\Gamma = e(g,g)^{1/a}$,如果$\Gamma$是均匀分布,那么$\Gamma^* = (n,n)^{1/a}$也是均匀分布的;当$\xi=1$时,因为$\Gamma$为随机数,所以$\Gamma^*$也是随机信息。

阶段 2　算法重复阶段 1 过程。

猜测阶段：A 给出猜测的值 ψ'，如果 $\psi'=\psi$，则模拟算法 B 输出 $\xi'=0$；如果 $\psi'\neq\psi$，则算法 B 输出 $\xi'=1$。

下面分析 B 的优势：

当 $\xi=1$ 时，攻击者得到的是随机的信息，有 $\Pr[\psi'\neq\psi|\xi=1]=1/2$，算法 B 在 $\psi'\neq\psi$ 时猜测 $\xi'=1$，所以 $\Pr[\xi'=\xi|\xi=1]=1/2$。当 $\xi=0$ 时，攻击者得到的是有效的信息，此时攻击者的优势为 ε，所以有 $\Pr[\psi'=\psi|\xi=0]=1/2+\varepsilon$，算法 B 在 $\psi'=\psi$ 时猜测 $\xi'=0$，因此 $\Pr[\xi'=\xi|\xi=0]=1/2+\varepsilon$。那么算法 B 破解 q-DBDHI 中的优势为：

$$\begin{aligned}&\Pr[\xi'=\xi|\xi=1]+\Pr[\xi'=\xi|\xi=0]-1/2\\&=1/2(1/2+\varepsilon)+1/2*1/2-1/2\\&=\varepsilon/2\end{aligned}$$

定理得证。

引理 3　任何少于或等于 $m-1$ 个参与者合作不能获得关于 p 个秘密的信息。

证明：公开的信息 $(d_1,G(d_1)),\cdots,(d_{n+p-m},G(d_{n+p-m}))$ 总共 $n+p$ 个数值对，少于多项式 $G(x)$ 的次数，即使 P_i 利用 $m-1$ 个数值对 $(h(ID_1\|r-1),F_{*_1}(r-1)),\cdots,(h(ID_{m-1}\|r-1),F_{*_{m-1}}(r-1))$ 也不能确定一个如式(8)的 $n+p-1$ 次多项式。但是如果有 m 个参与者合作，结合公开信息则能够唯一确定一个如式(8)的 $n+p-1$ 次多项。

定理 2　在满足式(11)的条件下，本文设计的协议满足可计算防合谋均衡，理性的参与者有动机执行协议。

证明：在理性秘密共享方案秘密重构阶段，没有可信者存在，参与者根据自身效益来决定是否同时发送正确的子份额，这时就存在参与者合谋的问题，比如最简单的 2 个人合谋的情况，只要这 2 个人在发送子份额时发送错误的信息，而其他参与者发送正确的信息，那么这两个合谋成员将独得秘密，而其他成员则得不到正确的秘密，虽然事后这 2 个合谋成员的行为能被可验证的方法发现欺骗。通过引理 2 可知，攻击者不能伪造信息。通过引理 3 可知，任何少于 $m-1$ 个参与者合作，不能获得关于 p 个秘密的信息。在所提出的方案中，每一个合谋集团 $T\subset[n],|T|\leqslant m-1$ 中的合谋者不能通过合谋得知当前轮是否是 r^* 轮。如果合谋者在参与协议前想了解秘密，他们只能通过猜测秘密获得，猜对的概率为 β^T，合谋者 P_i 获得的效益为 U_i^+；如果猜错秘密，概率为 $1-\beta^T$，合谋者 P_i 获得的效益为 U_i^-。所以合谋者 P_i 的期望收益为

$$E(U_i^{T^{guess}})=\beta^T*U_i^++(1-\beta^T)*U_i^- \tag{9}$$

如果合谋成员参与协议时，恰好在 r^* 轮进行攻击，概率为 λ^C，那么合谋者 P_i 获得的效益为 U_i^+；否则合谋者 P_i 获得的效益为 $E(U_i^{T^{guess}})$。因此合谋者 P_i 的期望收益至多为

$$\lambda^T*U_i^++(1-\lambda^T)*E(U_i{}^{T^{guess}}) \tag{10}$$

如果合谋成员遵守协议，那么合谋者 P_i 获得的效益为 U_i，所以当满足式(11)时，合谋成员将没有偏离协议的动机。

$$U_i>\lambda^T*U_i^++(1-\lambda^T)*E(U_i{}^{T^{guess}}) \tag{11}$$

考虑到加密算法是可计算安全的，具有多项式计算能力的合谋成员能以 $\lambda^{T'}$ 的概率突破加密算法获得利益，则存在一个可忽略的 $\xi(k)$，满足：

$$\lambda^{T'}\leqslant\lambda^T+\xi(k) \tag{12}$$

否则，合谋成员能够以比较大的概率突破加密算法，计算哪一轮是真秘密所在轮，这对于计算能力有限的合谋者是不可能的。用 $U^{*'}$ 表示在计算安全情况下参与者的收益，那么：

$$\begin{aligned}U^{*'}&=\lambda^{T'}U^++(1-\lambda^{T'})*E(U_i^{T^{guess}})\\&=\lambda^{T'}(U^+-E(U_i^{T^{guess}}))+E(U_i^{T^{guess}})\\&\leqslant(\lambda^T+\xi(k))(U^+-E(U_i^{T^{guess}}))+E(U_i^{T^{guess}})\\&\leqslant\lambda^T*U_i^++(1-\lambda^T)*E(U_i^{T^{guess}})+\xi(k)(U^+-\\&\quad E(U_i^{T^{guess}}))\\&<U_i+\varepsilon(k)\end{aligned} \tag{13}$$

可见，当所提协议满足式(11)时，在每一轮中，所提协议都能满足合谋成员合谋背离协议获得的收益没有遵守协议的收益大，所以参与者没有合谋偏离协议的动机，参与者在协议执行过程中都会选择占优策略(遵守协议)，这样协议最终达到均衡，可证我们的协议满足可计算防合谋均衡，理性的参与者没有动机偏离协议。

4.3　性能分析

定理 3　当协议中几何分布的参数为 λ 时(一次贝努利实验中秘密出现的概率)，方案的期望迭代轮数为 $O(1/\lambda)$。

证明：假设 $r=k$ 时，真秘密出现，则根据几何分布的性质可得 $P(r=k)=(1-\lambda)^{k-1}\lambda$，可知

$$\begin{aligned}E(r)&=\lambda+2\lambda(1-\lambda)+3\lambda(1-\lambda)^2+\cdots+k\lambda(1-\lambda)^{k-1}+\cdots\\&=(1+2(1-\lambda)+3(1-\lambda)^2+\cdots+k(1-\lambda)^{k-1}+\cdots)\lambda\end{aligned} \tag{14}$$

令

$$S_k=1+2(1-\lambda)+3(1-\lambda)^2+\cdots+k(1-\lambda)^{k-1} \tag{15}$$

则

$$\begin{aligned}(1-\lambda)S_k=&(1-\lambda)+2(1-\lambda)^2+3(1-\lambda)^3+\cdots+\\&k(1-\lambda)^k\end{aligned} \tag{16}$$

式(15)和式(16)两式相减得

$$S_k=\frac{1-(1-\lambda)^k}{\lambda^2}-\frac{k(1-\lambda)^k}{\lambda} \tag{17}$$

又 $0<1-\lambda<1$，则 $\lim\limits_{k\to\infty}(1-\lambda)^k=0$，故 $\lim\limits_{k\to\infty}S_k=1/\lambda^2$，从而 $E(r)=1/\lambda$。

现有经典理性秘密共享方案中，文献[11]的期望迭代轮数为 $O(5/\alpha^3)$，文献[17]的期望迭代轮数为 $O(n/\beta)$，文献[18]的期望迭代轮数为 $O(n^2)$；而本文的期望迭代轮数为 $O(1/\lambda)$。另外，在本文设计的方案中，秘密分发者只需计算一些公开信息，不需要进行秘密份额的分配，方案可在一次重构过程中得到多个秘密，这在很大程度上提高了秘密分发和重构的效率。

结束语　理性密码协议是密码学的一个新兴的研究方向，本文基于博弈论，提出了可计算防合谋均衡的概念和设计方法，构建了秘密共享的防合谋博弈模型，最后设计了一种可抗合谋的理性多秘密共享方案，解决了单个理性秘密共享效率低下和参与者合谋的问题。在所设计的方案中，遵守协议是理性参与者的最优策略，参与者没有偏离协议的动机，直至每个参与者获得多个秘密。可证明安全的理论与方法分析和证明显示该方案是安全和实用的。

参 考 文 献

[1] Shamir A. How to share a secret [J]. Communications of the ACM, 1979, 22(11): 612-613

[2] Blakeley G R. Safeguarding Cryptographic Keys [C]// Proceedings of the National Computer Conference, 1979. New York: AFIPS Press, 1979: 313-317

[3] 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, 1985. Washington DC: IEEE Computer Society, 1985: 383-395

[4] 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

[5] Hou Y C, Quan Z Y, Tsai C F, et al. Block-based progressive visual secret sharing [J]. Information Sciences, 2013, 233(1): 290-304

[6] Wu X T, Sun W. Improving the visual quality of random grid-based visual secret sharing[J]. Signal Processing, 2013, 93(5): 988-955

[7] Chien H-Y, Jan J-K, Tseng Y-M. A practical (t, n) multi-secret sharing scheme[J]. IEICE Transactions on Fundamentals, 2000, E83-A (12): 2762-2765

[8] Yang Chou-chen, Chang Ting-yi, Huang Min-shang. A (t,n) multi-secret sharing scheme[J]. Applied Mathematics and Computation, 2004, 151(2): 483-490

[9] 庞辽军,裴庆祺,焦李成,等. 基于 ID 的门限多重秘密共享方案[J]. 软件学报,2008,19(10):2739-2745
Pang Liao-jun, Pei Qing-qi, Jiao Li-cheng, et al. An Identity(ID)-Based Threshold Multi-Secret Sharing Scheme [J]. Journal of Software, 2008, 19(10): 2739-2745

[10] 裴庆祺,马建峰,庞辽军,等. 基于身份自证实的秘密共享方案[J]. 计算机学报,2010,33(1):152-156
Pei Qing-qi, Ma Jian-feng, Pang Liao-jun, et al. An Identity(ID)-Based and Self-Certified Secret Sharing Scheme [J]. Chinese Journal of Computers, 2010, 33(1): 152-156

[11] Halpern J, Teague V. Rational Secret Sharing and Multiparty Computation[C]//Proceedings of the 36th Annual ACM Symposium on Theory of Computing(STOC), 2004. New York: ACM Press, 2004: 623-632

[12] Groce A, Katz J. Fair computation with rational players[C]// Advances in Cryptology Eurocrypt, 2012. UK, Springer, 2012: 81-98

[13] Garay J, Katz J, Maurer U. Rational protocol design: cryptography against incentive-driven adversaries[C]// Proc. 54th IEEE Symposium on Foundations of Computer Science, 2013. Berkeley: IEEE Computer Society, 2013: 648-657

[14] 张恩,蔡永泉. 理性的安全两方计算协议[J]. 计算机研究与发展,2013,50(7):1409-1417
Zhang En, Cai Yong-quan. Rational Secure Two-Party Computation Protocol[J]. Journal of Computer Research and Development, 2013, 50(7): 1409-1417

[15] Zhang En, Cai Yong-quan. Collusion-free Rational Secure Sum Protocol[J]. Chinese Journal of Electronics, 2013, 22(3): 563-566

[16] Kol G, Naor M. Cryptography and Game Theory: Designing Protocols for Exchanging Information[C]// The Proceedings of the 5th Theory of Cryptography Conference (TCC), 2008. Berlin: Springer, 2008: 317-336

[17] Kol G, Naor M. Games for exchanging information [C]// Proceedings of the 40th Annual ACM Symposium on Theory of Computing(STOC), 2008. New York: ACM Press, 2008: 423-432

[18] Maleka S, Amjed S, Rangan C P. The Deterministic Protocol for Rational Secret Sharing[C]// 22th IEEE International Parallel and Distributed Processing Symposium, 2008. New York: IEEE press, 2008: 1-7

[19] Izmalkov S, Lepinski M, Micali S. Veriably Secure Devices[C]// 5th Theory of Cryptography Conference (TCC 2008). LNCS 4948, Berlin: Springer, 2008: 273-301

[20] Micali S, Shelat A. Purely Rational Secret Sharing[C]// 6th Theory of Cryptography Conference(TCC 2009). LNCS 5444, Berlin: Springer, 2009: 54-71

[21] Isshiki T, Wada K, Tanaka K. A Rational Secret-Sharing Scheme Based on RSA-OAEP [J]. IEICE Transactions on Fundamentals, 2010, E93-A(1): 42-49

[22] 张恩,蔡永泉. 基于双线性对的可验证的理性秘密共享方案[J]. 电子学报,2012,40(5):1050-1054
Zhang En, Cai Yong-quan. A Verifiable Rational Secret Sharing Scheme Based on Bilinear Pairing[J]. Acta Electronica Sinica, 2012, 40(5): 1050-1054

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

[24] Yu Yang, Zhou Zhan-fei. An Efficient Rational Secret Sharing Protocol Resisting against Malicious Adversaries over Synchronous Channels [C] // Information Security Cryptology LNCS 7763. Berlin: Springer, 2013: 69-89

[25] Tian You-liang, Ma Jian-feng, Peng Chang-gen, et al. Fair (t, n) threshold secret sharing scheme[J]. IET Information Security, 2013, 7(2): 106-112

[26] 谢识予. 经济博弈论(第 2 版)[M]. 上海:复旦出版社,2002
Xie Shi-yu. Economic game theory(second edition)[M]. Shanghai: Fudan press, 2002

[27] Katz J. Bridging game theory and cryptography: Recent results and future directions[C]// 5th Theory of Cryptography Conference. LNCS 4984, Berlin: Springer, 2008: 251-272

[28] Micali S, Rabin M, Vadhan S. Verifiable random functions[C]// Proceedings of the 40th IEEE Symposium on Foundations of Computer Science. New York: IEEE press, 1999: 120-130

[29] Dodis Y, Yampolskiy A. A verifiable random function with short proof and keys[C] // PKC2005. LNCS 3386, Berlin: Springer, 2005: 416-431