

基于二元非对称多项式的公平秘密共享方案

杨文伟, 邢玉清

(信息工程大学, 河南 郑州 450001)

摘要: 在 Shamir 的 (t, n) 秘密共享方案中, 任何 $m(m \geq t)$ 个参与者可以重建秘密, 而任何少于 t 个的参与者无法得到秘密的任何信息。然而, 如果在秘密重建阶段有超过 t 个参与者进行重构时, Shamir 的秘密重建阶段不能阻止外部攻击者知道秘密, 而内部攻击者在秘密重构过程中可以提交虚假份额欺骗诚实参与者。提出一个基于非对称二元多项式的具有未知重构轮数的秘密共享方案, 并针对 4 种攻击模型(同步非合谋攻击、异步非合谋攻击、同步合谋攻击及异步合谋攻击)证明方案具有防范外部攻击者和内部攻击者的安全性与公平性。

关键词: 秘密共享; 非对称二元多项式; 公平性; 攻击模式

中图分类号: TP393

文献标识码: A

doi: 10.11959/j.issn.2096-109x.2019003

Fair secret sharing scheme using asymmetric bivariate polynomial

YANG Wenwei, XING Yuqing

Information Engineering University, Zhengzhou 450001, China

Abstract: In Shamir's (t, n) secret sharing scheme, any $m(m \geq t)$ participants can reconstruct the secret, and any less than t participants can't get any information about the secret. However, if there are more than t participants in the secret reconstruction phase, Shamir's secret reconstruction phase can not prevent external attackers from knowing the secret, while internal attackers can release a fake share to deceive honest participants during the secret reconstruction process. A rational threshold secret sharing scheme using asymmetric bivariate polynomial with unknown rounds is proposed. Then it shows its fairness and security against non-cooperative attack with synchronization, non-cooperative attack with a synchronization, cooperative attack with synchronization and cooperative attack with a synchronization.

Key words: threshold secret sharing, asymmetric bivariate polynomial, fairness, attack model

1 引言

Shamir^[1]和 Blakley^[2]于 1979 年分别提出了 (t, n) 门限秘密共享的概念, 其主要思想是秘密分发

者将一个秘密分成 n 份, 并通过安全通道发送给用户, t 个或更多的参与者可以使用他们的共享份额来重构秘密; 而任何少于 t 个的参与者则无法恢复秘密, 在完备情况下得不到任何关于秘密的信息。

收稿日期: 2018-12-14; 修回日期: 2019-01-04

通信作者: 杨文伟, 247218160@qq.com

基金项目: 国家重点研发计划基金资助项目 (No.2016YFB0801601, No.2016YFB0801505)

Foundation Item: The National Key R&D Plan Program of China (No.2016YFB0801601, No.2016YFB0801505)

论文引用格式: 杨文伟, 邢玉清. 基于二元非对称多项式的公平秘密共享方案[J]. 网络与信息安全学报, 2019, 5(1): 22-29.

YANG W W, XING Y Q. Fair secret sharing scheme using asymmetric bivariate polynomial[J]. Chinese Journal of Network and Information Security, 2019, 5(1): 22-29.

虽然 Shamir 方案的秘密重建阶段非常简单，但这一阶段对于参与者都是合法份额拥有者的假设并不总是正确的。特别是在有 $m(m > t)$ 个参与者合作恢复秘密时，一个并无有效份额的欺骗者（外部攻击者）可能获取其他参与者的至少 t 个有效份额，恢复出正确的秘密。另外，拥有有效份额的欺骗者（内部攻击者）在秘密重构过程中可能会提交虚假份额，即使这种攻击行为被检测到，但并不能阻止欺骗者获得其他诚实参与者提交的真实份额并恢复出正确的秘密，而诚实的参与者利用获得的虚假份额进行重构只能得到错误的秘密，欺骗者实现独占真实秘密的意图。

针对秘密共享方案中存在的欺骗问题，研究者提出了许多防范措施。Tomba 和 Woll^[3]于 1988 年最先提出公平秘密共享方案，其构造的方案通过将秘密隐藏在一个很难分辨的序列中，内部欺骗者要想独享秘密只有准确猜出真实秘密的位置，但该方案无法抵抗异步环境下的攻击。Tian 等^[4]于 2013 年构造了一种方案，该方案利用子秘密的一致性来检测是否存在欺骗者，同样将秘密隐藏在一个很难分辨的序列中，并基于 3 种攻击模型（非合谋攻击、同步合谋攻击、异步合谋攻击）证明方案的公平性。然而 Harn^[5]指出该方案对于外部攻击者，只能适应于同步环境，而不适应异步环境。2015 年，Harn 等^[6]提出一种公平秘密方案。该方案选择 k 个多项式，利用线性组合的方式将秘密隐藏在线性组合中，并将秘密隐藏在一个随机选择的秘密序列中，从而实现在异步环境下秘密重构的公平性。但是该方案在欺骗者存在的情况下只能终止协议。

遇到欺骗即终止协议的策略过于严厉，将终止协议作为对欺骗者的惩罚，但同时也使诚实参与者不能恢复秘密，这就提出了欺骗者检测识别的需求，研究者利用不同的数学工具提出了很多针对欺骗检测的方案。Rabin 等^[7]的方案中引入了

第一个作弊者检测识别方案，文献[8,9]方案基于线性纠错码和通用散列函数构造欺骗识别秘密共享方案，Roy 等^[10]的欺骗识别基于成对的共享认证密钥。大多数秘密共享方案的欺骗识别是基于 Shamir^[1]的工作，所有的份额由 $t-1$ 次多项式 $f(x)$ 生成。然而，二元多项式 $F(x, y)$ 也是构造功能性秘密共享方案的基本工具，但基于二元多项式的欺骗识别秘密共享方案很少。Liu 等^[11]提出了两种基于对称二元多项式的欺骗识别算法，欺骗识别仅基于二元多项式的对称性和插值多项式的线性。但该方案在异步环境下无法识别外部欺骗者，在同步环境中虽然可以识别出内部欺骗者，但无法阻止内部欺骗者独占真实秘密。

本文构造了基于非对称二元多项式的具有未知重构轮数的秘密共享方案，在该方案中，使用非对称多项式生成共享份额，利用非对称多项式次数比较高的变量构造多项式份额。多项式份额次数远高于 $t-1$ 且不需要被重构，可以随机选择高次多项式上的点生成秘密评估点，通过简单运算即可实现对攻击者的检测和识别。并且该方案在攻击者存在时并不是选择立即终止协议，在剔除识别出的欺骗者后，不少于 t 个诚实参与者依旧可以继续合作完成秘密重构，有效保证诚实者的权利。而且该方案可有效防范同步及异步环境下内部及外部攻击者的欺骗，有效保证了方案的安全性和公平性。

2 预备知识

本节简要介绍 Shamir 的 (t, n) 秘密共享方案（该方案也是基于二元多项式的 (t, n) 秘密共享方案的基础）以及对攻击者的定义分类及对秘密共享公平性的定义。

2.1 Shamir 的 (t, n) 秘密共享方案

Shamir 的 (t, n) 秘密共享方案利用拉格朗日插值公式构造，由两阶段组成：秘密分发阶段和秘密重构阶段。在秘密分发阶段，秘密分发者 D

分发秘密 s , 生成共享份额 $s_1, s_2, \dots, s_n$, 并将份额 s_i 发送给参与者 P_i ; 在秘密重构阶段, t 个及以上的参与者可以重建秘密, 具体算法如下。

1) 秘密分发阶段

秘密分发者 D 在 $GF(q)$ 中随机选择一个 $t-1$ 次多项式 $f(x)$, 使秘密 $s = f(0) \in GF(q)$ 。秘密分发者 D 生成 n 个秘密份额 $\{s_1, s_2, \dots, s_n\}$, 其中 $s_i = f(i), i=1, \dots, n$, 并将 s_i 发送给相应的参与者 P_i 。

2) 秘密重构阶段

任何 $m(\geq t)$ 个参与者 (不妨假设为 $P_1, P_2, \dots, P_m$) 发送他们的共享份额 $s_1, s_2, \dots, s_m$, 并使用拉格朗日插值公式计算秘密 $s = f(0) = \sum_{i=1}^m (s_i \prod_{j \neq i} \frac{-j}{i-j})$ 。

2.2 欺骗识别秘密共享方案

欺骗识别秘密共享方案的模型也包括两个阶段。

1) 秘密分发阶段

在这一阶段, 秘密分发者 D 将秘密 s 划分为 n 个共享份额 $s_1, s_2, \dots, s_n$, 并将每个共享发送给相应的用户 P_i 。

2) 秘密重构阶段

在该阶段, 至少有 $m(\geq t)$ 个用户提交自己的共享, 以重构秘密。但在这 m 个共享份额上设计欺骗识别算法来识别作弊者。令 L 为使用欺骗识别算法识别为欺骗者的用户集。如果 $(m - |L|) \geq t$, 则不在 L 中的用户继续使用共享份额重构秘密并输出 (s, L) 。如果 $(m - |L|) < t$, 则中止协议, 并输出 $(\perp, L)$ 。

2.3 公平秘密共享

秘密重构阶段的欺骗者可以分为两类: 外部攻击者和内部攻击者。

外部攻击者: 该类攻击者其实并没有从秘密分发者处获取到共享份额, 意图伪装成持有份额的参与者参与重构。

内部攻击者: 该类攻击者本身拥有真实的份额, 但会在重构的某个阶段选择发布虚假的份额,

内部攻击者不是完全诚实的参与者, 但也不是任意恶意的, 可能只是期望除了其本人外越少人知道秘密越好的理性攻击者。

定义 1 一个秘密共享方案称为公平的, 如果满足:

- 1) 无攻击者时, 所有参与者都能重构秘密;
- 2) 存在外部攻击者时, 诚实参与者能够重构秘密而外部攻击者无法重构秘密;
- 3) 存在内部攻击者时, 诚实参与者与内部攻击者要么都恢复秘密, 要么都无法恢复秘密, 即内部攻击者无法获得比诚实者多的优势。

3 基于二元非对称多项式的公平秘密共享方案

本节给出了基于二元非对称多项式的具有未知重构轮数的秘密共享方案, 首先给出针对外部攻击者的利用非对称二元多项式构建的方案 1, 该方案能有效防范外部攻击者, 但不能有效解决内部攻击者的问题。所以针对方案 1 进行改进, 构造具有未知轮数的方案 2, 同时解决外部及内部攻击者的问题。

给定一个安全参数 k , 假定协议使用有限域 $\mathbb{F} = GF(q)$ 中的值进行操作, 其中 $q = 2^k$, 即 $\mathbb{F}$ 的每个元素都可以用 k 个比特表示。

3.1 方案 1: 针对外部攻击者的方案

为了在参与者 $P = \{P_1, P_2, \dots, P_n\}$ 中共享秘密 s , 分发者 D 利用二元多项式 $F(x, y)$ 为每个参与者 P_i 生成共享份额, 其中变量 y 的次数为 $t-1$, 变量 x 的次数为 nk , 秘密 $s = F(0, 0)$, 对应的多项式份额 $f_i(x) = F(x, i)$, 容易看出 $\deg(f_i(x)) = nk \gg t-1$, 但这些多项式永远不需要被重构, 因此能够给每一方提供这些多项式上的数量足够多的计算点和相应值来作为秘密评估点。

1) 秘密分发阶段

输入: 秘密 s

Step1 秘密分发者 D 随机选择二元多项式

$F(x, y)$, 其中变量 x 的次数为 nk 次, 变量 y 的最高次数为 $t-1$ 次, 且满足 $F(0, 0) = s$ 。并计算 $f_i(x) = F(x, i), 1 \leq i \leq n$ 。

Step2 秘密分发者 D 随机选择域 $\mathbb{F}$ 上的 nk 次多项式 $r_i(x), 1 \leq i \leq n$, 以及 nk 个不同的随机非零值 $\alpha_{i,1}, \alpha_{i,2}, \dots, \alpha_{i,k}, 1 \leq i \leq n$ 。

Step3 秘密分发者 D 通过安全信道向 P_i 发送:

- ① 多项式份额 $f_i(x)$, 以及秘密共享份额 $s_i = f_i(0)$;
- ② 多项式 $r_i(x)$;
- ③ $\alpha_{i,l}, 1 \leq l \leq k$ 以及 $a_{j,i,l} = f_j(\alpha_{i,l}), b_{j,i,l} = r_j(\alpha_{i,l}), 1 \leq l \leq k, 1 \leq j \leq n$ 。

2) 秘密重构阶段

假设有 $m(m \geq t)$ 个参与者 (不失一般性, 记为 $P_1, P_2, \dots, P_m$) 参与重构阶段。欺骗者集合 $L = \emptyset$ 。

Step1 重构参与者 P_i 选择域 $\mathbb{F}$ 上的随机值 c_i , 并向其余重构参与者广播 c_i 以及多项式 $g_i(x) = f_i(x) + c_i r_i(x)$, 必须满足 $\deg(g_i(x)) = nk$ 。

所有重构参与者使用以下规则为彼此投票: 如果对于任意的 $l \in [1, k], a_{j,i,l} + c_j b_{j,i,l} = g_j(\alpha_{i,l})$ 都成立, 则 P_i 投票给 P_j , 否则 P_i 不给 P_j 投票。

如果每个参与重构者都得到 $m-1$ 票, 则转入 Step2; 否则转到 Step3 以识别攻击者。

Step2 所有参与重构者 P_i 广播多项式 $f_i(x)$, 并使用秘密评估点验证接收到的多项式, 若没有发现错误, 则提取份额 $s_j = f_j(0)$ 重构秘密 s , 输出 (s, L) ; 若发现错误则转入 Step4 以识别攻击者。

Step3 所有重构参与者 P_i 向未参与重构的 $n-m$ 个用户 $P_{m+1}, \dots, P_n$ 广播 c_i 以及多项式 $g_i(x) = f_i(x) + c_i r_i(x)$ 。

每个未参与重构的 $P_j, j \in [m+1, n]$ 给 $P_1, P_2, \dots, P_m$ 投票, 规则如下: 如果 $\forall l \in [1, k], a_{i,j,l} + c_i b_{i,j,l} = g_i(\alpha_{j,l})$ 都成立, 则 P_j 投票给 P_i , 其中 $j \in [m+1, n], i \in [1, m]$; 否则 P_j 不会投票给 P_i 。

设 V_i 为 P_i 在 Step1 和 Step3 中的票数之和。

如果 $V_i < T = \frac{n}{2}$, P_i 可被认为是一个攻击者, 并将 P_i 归入欺骗者集合 L , 给欺骗者投票的用户也归入欺骗者集合 L 。如果剩余的重构参与者数量大于 t , 则转入 Step2 继续完成秘密重构。否则中止协议并输出 $(\perp, L)$ 。

Step4 所有重构参与者 P_i 向未参与重构的且不包含在欺骗者集合 L 中的用户广播多项式 $f_i(x)$ 。

每个不包含在欺骗者集合 L 中的 P_i 给这些重构参与者投票, 规则如下: 如果 $\forall l \in [1, k], a_{i,j,l} = f_i(\alpha_{j,l})$ 都成立, 则 P_j 投票给 P_i ; 否则 P_j 不会投票给 P_i 。

设 V_i 为 P_i 的票数, 如果 $V_i < T = \frac{n}{2}$, P_i 可被认为是一个攻击者, 并将 P_i 归入欺骗者集合 L , 给欺骗者投票的用户也归入欺骗者集合 L 。如果剩余的重构参与者数量大于 t , 则转入 Step2 继续完成秘密重构, 否则中止协议并输出 $(\perp, L)$ 。

可以看出方案 1 是一个好的 (t, n) 秘密共享方案。令 $h_0(y) = F(0, y)$, $h_0(y)$ 是 $t-1$ 次多项式, 且秘密 $s = F(0, 0) = h_0(0)$ 。此外, 每个 P_i 都有一个秘密共享份额 $s_i = f_i(0) = F(0, i), i = 1, 2, \dots, n$ 。很容易看出, 秘密份额 s_i 可以看成是 $h_0(y)$ 产生的份额, 即 $s_i = F(0, i) = h_0(i)$, 这与 Shamir (t, n) 秘密共享方案一致。因此, 方案 1 是一个好的 (t, n) 秘密共享方案, 如果参与者都诚实地发布共享份额, 则可以成功地恢复秘密。

外部攻击者并没有从秘密分发者获取到共享份额, 所以在重构阶段只能猜测域 $\mathbb{F}$ 上的 nk 次共享多项式, 成功的概率远低于 $\frac{1}{q}$ 。但需要注意的是,

如果协议只执行一轮, 该方案不能阻止内部攻击者取得相对于诚实者的优势, 内部攻击者可以在重构的 Step1 中诚实发布多项式, 但在 Step2 时选择提交假的份额, 虽然该行为依然可以被诚实者发现, 但该攻击者已经获取到了足够的

份额以完成秘密重构。所以在该方案的基础上, 本文针对内部攻击者引入未知重构轮数的改进, 以同时防止外部和内部攻击者获得相对于诚实者的优势, 达到公平性。

3.2 方案 2: 针对外部和内部攻击者的方案

防止内部攻击者获得优势的基本思想是构造具有未知重构轮数的方案, 秘密发布方在最开始时通过选择随机数的方式确定正确的秘密在秘密序列中的位置, 从而将秘密 s 隐藏在一个长度为 k 的秘密序列 $\{v_1, v_2, \dots, v_{q-1}, v_q, v_{q+1}, \dots, v_k\}$ 中, 其中, v_{q+1} 用来指示真实秘密位置的“标志”。发布方为所有参与者选择 k 个秘密 (真实的和虚假的), 并按照方案 1 产生秘密共享份额。秘密重构参与者共同工作, 逐个完成秘密重构。如果过程中存在攻击者, 则对攻击者进行检测并剔除。直到在没有攻击者的情况下重构出标志 v_{q+1} 。当该标志被重构时, 所有的重构者都已经获得了真实的秘密, 秘密就是之前重构的 v_q 。

1) 秘密分发阶段

输入: 秘密 s

秘密发布方随机选择 $q \in [2, k-1]$ 以确定 s 在秘密序列中的位置, 并随机选择域 $\mathcal{M}$ 上的 k 个秘密 $v_1, v_2, \dots, v_k$, 满足 $v_1 > v_2 > \dots > v_{q-1} > v_q < v_{q+1}, s = v_q$ 。

对于每一个秘密 v_r , 秘密发布方利用方案 1 中的份额生成算法生成共享份额并发送给相应的参与者。

2) 秘密重构阶段

假设有 $m(m \geq t)$ 个参与者 (记为 $P_1, P_2, \dots, P_m$) 参与重构阶段。

重构参与者一起合作重构秘密 $\{v_1, v_2, \dots, v_k\}$, 按照 $v_1 \rightarrow v_2 \rightarrow \dots \rightarrow v_{q+1}$ 的顺序每次重建一个, 依次执行:

① 对于每一轮秘密 $v_r, 1 \leq r \leq q+1$, 重构参与者按照方案 1 秘密重构阶段的算法将其重构;

② 若成功重构秘密 $v_r, 2 \leq r \leq q+1$, 将 v_r 与 v_{r-1} 进行比较, 若 $v_r > v_{r-1}$, 则秘密 $s = v_r$, 并终止协议; 否则, 继续下一轮重构工作。

4 方案 2 的公平性与安全性分析

当所有的重构参与者每一轮都出示真实的秘密共享份额时, 即攻击者总数 $\gamma = 0$ 时, 由之前的分析可知方案 1 是一个好的 (t, n) 秘密共享方案, 即每一轮中任何少于 t 个秘密共享份额的集合不会泄露关于共享秘密的信息, 大于等于 t 个秘密共享份额的集合可以重构出共享秘密。那么在第 $q+1$ 轮重构完成后经检验发现 $v_{q+1} > v_q$, 从而确认秘密就在之前一轮, 得到秘密 $s = v_q$ 。

如果存在攻击者, 即攻击者总数 $\gamma \geq 1$ 时, 研究方案在同步非合谋攻击、异步非合谋攻击、同步合谋攻击及异步合谋攻击模型下的安全性与公平性。

引理 1 在方案 2 中任一重构参与者能正确猜出秘密在序列中的位置的概率是 $\frac{1}{k}$, 其中 k 是序列中的秘密数。

证明 在方案 2 中, 秘密 $s = v_q$ 在构建过程中被秘密分发者随机隐藏在序列 $\{v_1, \dots, v_{q-1}, v_q, v_{q+1}, \dots, v_k\}$ 中, 而重构参与者不知道 s 的确切位置, 只能通过猜测, 其成功的概率为 $\frac{1}{k}$ 。

定理 1 在同步非合谋攻击模型下, 方案是安全公平的。

证明 同步非合谋攻击模型假设所有重构参与者同时出示秘密共享份额且攻击者之间没有合作关系。

首先考虑外部攻击者, 假定其希望通过伪装成 P_l 参与到重构中, 下面考虑其通过伪造共享多项式 $\bar{g}_l$ 获得 P_j 投票的概率, 由投票规则可知其获得 P_j 投票的概率等于 $\Pr[a_{l,j,l} + c_l b_{l,j,l} = \bar{g}_l(\alpha_{j,l}), 1 \leq l \leq k]$ 。

$$\begin{aligned}
& \Pr[a_{l,j,l} + c_l b_{l,j,l} = \bar{g}_l(\alpha_{j,l}), 1 \leq l \leq k] = \\
& \Pr[a_{l,j,l} + c_l b_{l,j,l} = \bar{g}_l(\alpha_{j,l}), \\
& 1 \leq l \leq k | \bar{g}_l = g_l] \Pr[\bar{g}_l = g_l] + \\
& \Pr[a_{l,j,l} + c_l b_{l,j,l} = \bar{g}_l(\alpha_{j,l}), \\
& 1 \leq l \leq k | \bar{g}_l \neq g_l] \Pr[\bar{g}_l \neq g_l] < \\
& \Pr[\bar{g}_l \neq g_l] + \Pr[a_{l,j,l} + c_l b_{l,j,l} = \\
& \bar{g}_l(\alpha_{j,l}) | \bar{g}_l \neq g_l]
\end{aligned}$$

由同步条件可知, P_l 没有任何关于 g_l 的先验知识, 只能随意猜测一个域上的 nk 次多项式 $\bar{g}_l$, 其正好为 g_l 的概率远低于 $\frac{1}{q}$ 。而当 $\bar{g}_l \neq g_l$ 时, 多项式 $\bar{g}_l$ 与 g_l 最多有 nk 个点上重合, 其正好包含 $\alpha_{j,l}$ 的概率最多为 $\frac{C_{nk}^1}{C_q^1} = \frac{nk}{q}$ 。从而可得

$$\begin{aligned}
& \Pr[a_{l,j,l} + c_l b_{l,j,l} = \bar{g}_l(\alpha_{j,l}), 1 \leq l \leq k] < \\
& \frac{1}{q} + \frac{nk}{q} = \frac{nk+1}{2^k} \approx 2^{-\Omega(k)}
\end{aligned}$$

所以, 当安全参数足够大时, 攻击者伪装为 P_l 得到 P_j 投票的概率是可忽略的。又攻击者之间不存在同谋, 所以其得到别的攻击者投票的概率为 0。可知攻击者得到别人投票的概率是可忽略的, 该攻击者将被识别出来, 无法进入下一轮。

下面考虑内部攻击者的情况, 假设在第 i 轮内部攻击者 P_l 发送伪造的共享多项式 $\bar{g}_l^i \neq g_l^i$, 由上述分析可知, P_l 想要在投票阶段获得 P_j 投票的概率为 $\Pr[a_{l,j,l} + c_l^i b_{l,j,l}^i = \bar{g}_l^i(\alpha_{j,l}^i), 1 \leq l \leq k | \bar{g}_l^i \neq g_l^i] < \frac{nk}{q} \approx 2^{-\Omega(k)}$, 同理, 该攻击者将被识别出来, 无法进入下一轮。

假设在第 i 轮内部攻击者 P_l 发送真实的共享多项式 g_l^i 通过检测, 但在重构的步骤 2 中发送伪造 $\bar{f}_l^i \neq f_l^i$ 欺骗别的参与者, 希望能够获得独享重构秘密 s 的额外收益, 这要求其能够准确猜中秘密 $s = v_q$ 所在的轮数, 由引理 1 可知, 任一重构参与者能正确猜出秘密在序列中的位置的概率是

$\frac{1}{k}$, 当安全参数 k 足够大时, 可有效保证方案的安全公平。

综上所述, 在同步非合谋攻击模型下, 方案是安全公平的。

定理 2 在异步非合谋攻击模型下, 方案是安全公平的。

证明 异步非合谋攻击模型假设所有重构参与者和攻击者先后出示秘密共享份额且攻击者之间没有合作关系。对于攻击者而言, 最理想的攻击模式是最后出示信息, 以获得先前参与者出示的信息。

对于攻击者 P_l (外部和内部) 而言, 在重构过程的步骤 1 中, 与定理 1 中不同地方在于 P_l 可以选择最后发布信息, 从而获得之前所有参与者出示的多项式 $g_j(x), J \neq I$, 则 P_l 通过伪造共享多项式 $\bar{g}_l$ 获得 P_j 投票的概率可表述为 $\Pr[a_{l,j,l} + c_l b_{l,j,l} = \bar{g}_l(\alpha_{j,l}), 1 \leq l \leq k | g_{J \in [1,m], J \neq I}]$ 。但由于掩护多项式 $r_j(x), J \neq I$ 是随机选择的且相互独立的, 所以 $g_j(x), J \neq I$ 是相互独立的, 有

$$\begin{aligned}
& \Pr[a_{l,j,l} + c_l b_{l,j,l} = \bar{g}_l(\alpha_{j,l}), 1 \leq l \leq k | g_{J \in [1,m], J \neq I}] = \\
& \Pr[a_{l,j,l} + c_l b_{l,j,l} = \bar{g}_l(\alpha_{j,l}), 1 \leq l \leq k]
\end{aligned}$$

上式表明 $g_{J \in [1,m], J \neq I}$ 对 P_l 构造需要发送的多项式 $\bar{g}_l$ 并没有提供有用信息。如定理 1 证明所示, 攻击者将被识别出来, 无法进入下一轮。掩护多项式 $r_j(x), J \neq I$ 的随机选择, 同样使 P_l 无法从 $g_j, J \neq I$ 中还原出共享份额 $f_j, J \neq I$, 从而保证方案是安全公平的。

对于内部攻击者而言, 在第 i 轮重构的 Step2 中, 可以利用后发优势, 在获取到足够多的共享份额之后自行恢复本轮秘密 v_i , 并将其与上一轮秘密 v_{i-1} 进行比较, 若 $v_i < v_{i-1}$, 则发放真实的份额进入下一轮; 若 $v_i > v_{i-1}$, 则秘密 $s = v_{i-1}$, 其选择释放假的份额。但此时所有的诚实参与者都已经获得了这个秘密 s , 因为秘密在前一轮已经被重建, 也就是

说,对于内部攻击者而言其并没有能够获得独享秘密 s 的额外收益,但其一旦出示假的份额将被确认为攻击者。这就保证了方案是安全公平的。

综上所述,在异步非合谋攻击模型下,方案是安全公平的。

定理 3 在同步合谋攻击模型下,当 $\gamma < \min(t, \frac{n}{2})$ 时,方案是安全公平的。

证明: 同步合谋攻击模型假设此攻击模型假设所有参与者同时出示共享份额且有多攻击者合谋攻击方。

当内部攻击者数目 $\gamma \geq t$ 时,攻击者可以通过合作掌握超过 t 的共享份额,从而恢复秘密 s 。所以为保证方案的安全公平性,首先要求攻击者数目 $\gamma < t$ 。

假设合谋的攻击者(内部的或者外部的)为 $P_i, 1 \leq i \leq \gamma$,在重构开始前,攻击者至多知道多项式 $f_i(x), r_i(x), r+1 \leq i \leq n$ 上的 $k\gamma$ 个点。由于 $k\gamma$ 小于多项式 $f_i(x), r_i(x)$ 的次数 nk ,从而保证了 $f_i(x), r_i(x)$ 的安全性。攻击者没有办法搜集到足够的 $f_i(0)$ 完成秘密重构,只能出示多项式进入投票阶段。如同定理 1 证明所示,攻击者想要得到诚实者的投票的概率是可忽略的。所以投票阶段攻击者只能获得同谋者的 $\gamma-1$ 票,诚实者至少可以得到别的诚实者的 $n-\gamma-1$ 票,为将诚实者与攻击者区分开,只要保证 $\gamma-1 < n-\gamma-1$,即 $\gamma < \frac{n}{2}$,就可以保证没有外部攻击者能够进入重构阶段的 Step2。

同定理一证明类似,在重构阶段的 Step2 中,合谋攻击者只有在准确猜测到秘密 s 的位置,才可能达成独享恢复秘密 s 的目的。

综上所述,在同步合谋攻击模型下,当 $\gamma < \min(t, \frac{n}{2})$ 时,方案是安全公平的。

定理 4 在异步合谋攻击模型下,当 $\gamma < \min(t,$

$\frac{n}{2})$ 方案是安全公平的。

证明 异步合谋攻击模型假设此攻击模型假设所有参与者先后出示共享份额且有多攻击者合谋攻击方。对于攻击者而言,最理想的攻击模式是最后出示信息,他们可以获得先前诚实参与者出示的信息。

与定理 3 证明类似,在重构之前,外部攻击者无法伪造出合适的多项式以获得诚实者的投票。与定理 2 证明类似,在重构阶段的 Step1 中,即使攻击者掌握之前所有参与者出示的多项式,由于掩护多项式的存在,攻击既无法得到可以帮助构造多项式的有用信息,也无法从中推测出真实份额,从而阻止外部攻击者进入 Step2;在重构阶段的 Step2,尽管合谋的内部攻击者可以借助后发优势决定是否出示真实份额,但依然无法阻止诚实参与者获得秘密 s ,从而保证了方案的安全公平性。

5 方案对比

Liu 等^[11]提出了两种基于对称二元多项式的欺骗识别算法,该算法并不能完全抵抗异步攻击。例如,当 t 个或者更多个的诚实参与者先出示共享份额,外部攻击者选择之后出示份额,在出示之前他可以利用这 t 个真实共享份额进行拉格朗日插值计算得出正确的多项式,得到所有正确的共享份额,从而外部攻击者可以伪装成拥有真实份额的参与者通过检测,并成功得到秘密 s 。同时该方案也不能完全抵抗合谋同步攻击,合谋的内部攻击者在重构协议执行时出示错误的共享份额,即使攻击行为被检测到,但也不能阻止攻击者独享秘密 s 。本文的安全性与公平性证明了所提方案在 4 种攻击模式下的安全公平。

Harn 等^[6]提出了一个对抗内部和外部攻击者的秘密共享方案,但该方案能有效防范外部攻击者和内部攻击者,但该方案依赖于 Hash 函数是单

向碰撞稳固的这一密码学假设来保证每一轮恢复的正确性，在发现有攻击者时也无法对攻击者进行有效的检测确认，一旦有攻击者存在则协议中止。本文方案能够有效对攻击者进行检测确认，而且不依赖于任何的密码学假设。

还有些方案采用其他数学工具来构造欺骗识别方案，如表1所示。例如，文献[8]利用 Reed-Solomon 编码和正交测试法，可以识别 $\gamma \leq \frac{t-1}{3}$ 的欺骗者；文献[9]利用 Reed-Solomon 编码和强通用散列函数，可以识别 $\gamma \leq \frac{t-1}{2}$ 的欺骗者；文献[10]使用成对认证密钥来识别 $\gamma < \frac{t}{2}$ 的欺骗者，每一对用户之间需要一个安全的通信通道。所有这些方案[8,9,10]都能够识别 $m \geq t$ 用户参与秘密重建的情况。本文方案可以识别 $\gamma < \min(t, \frac{n}{2})$ 的欺骗者，具有更强的识别能力，并且采用的是非对称二元多项式及，计算简便。

表1 欺骗识别方案比较

方案	识别能力	采用的工具
文献[8]	$\gamma < \frac{t}{3}$	Reed-Solomon 编码和正交测试法
文献[9]	$\gamma < \frac{t}{2}$	Reed-Solomon 编码和强通用散列函数
文献[10]	$\gamma < \frac{t}{2}$	成对认证密钥
本文方案	$\gamma < \min(t, \frac{n}{2})$	非对称二元多项式

6 结束语

本文提出了基于非对称二元多项式的未知重构轮数的 (t, n) 理性秘密共享方案，该方案可对 $\gamma < \min(t, \frac{n}{2})$ 欺骗者进行有效识别。方案使用非对称多项式中生成多项式份额，利用多项式份额不需要被重构且次数较高的性质随机生成秘密评估点，不依赖于任何密码学假设，只需要简单验

算就可实现对欺骗者的检测与识别，并基于同步非合谋攻击、异步非合谋攻击、同步合谋攻击、异步合谋攻击证明了方案的安全公平。

参考文献：

- [1] SHAMIR A. How to share a secret [J]. Communications of the ACM, 1979, 22(11): 612-613.
- [2] BLAKLEY G R. Safeguarding cryptographic keys[C]//The National Computer Conference 1979. 1979: 313-317.
- [3] TOMPA M, WOLL H. How to share a secret with cheaters[J]. Journal of Cryptology, 1988, 1(3): 133-138.
- [4] TIAN Y L, MA J F, PENG C G, et al. Fair (t, n) threshold secret sharing scheme[J]. IET Information Security, 2013, 7(2): 106-112.
- [5] HARN L. Comments on fair (t, n) threshold secret sharing scheme[J]. IET Information Security, 2014, 8(6): 303-304.
- [6] HARN L, LIN C L, LI Y. Fair secret reconstruction in (t, n) secret sharing[J]. Journal of Information Security and Applications, 2015, 23: 1-7.
- [7] RABIN T, BEN-OR M. Verifiable secret sharing and multiparty protocols with honest majority[C]//ACM STOC 1989. 1989: 73-85.
- [8] KUROSAWA K, OBANA S, OGATA W. T-cheater identifiable (k, n) threshold secret sharing schemes[C]//International Cryptology Conference on Advances in Cryptology. 1995.
- [9] OBANA S. Almost optimum t -cheater identifiable secret sharing schemes[C]//International Conference on Theory & Applications of Cryptographic Techniques: Advances in Cryptology. 2011.
- [10] ROY P S, ADHIKARI A, XU R, et al. An efficient robust secret sharing scheme with optimal cheater resiliency[M]//Security, Privacy, and Applied Cryptography Engineering. 2014.
- [11] LIU Y X, YANG C N, WANG Y C, et al. Cheating identifiable secret sharing scheme using symmetric bivariate polynomial[J]. Information Sciences, 2018: 453.

[作者简介]



杨文伟（1985—），男，江苏盐城人，信息工程大学博士生，主要研究方向为网络安全、密码学、博弈论。



邢玉清（1981—），男，河南周口人，信息工程大学博士生，主要研究方向为网络安全、密码学、智能算法。