第38卷 第18期
Vol.38 No.18

计 算 机 工 程
Computer Engineering

2012年9月
September 2012

• 安全技术 •

文章编号：1000—3428(2012)18—0120—03 文献标识码：A 中图分类号：TP309

基于重复博弈参与者有权重的秘密共享方案

蔡永泉，孙 科

(北京工业大学计算机学院，北京 100124)

摘 要：在大多数参与者有权重的秘密共享方案中，各参与者子秘密份额数量的不同会导致秘密重构阶段产生不公平问题。为此，提出一个基于重复博弈的理性秘密共享方案。在参与者原有份额的基础上，为其构造数量差不超过1的有效子秘密份额，利用重复博弈使每个参与者可以获得其他参与者的全部份额，进而重构出秘密。分析结果表明，该方案可以使理性参与者始终遵守协议，完成秘密重构，且具有较高的安全性和良好的可扩展性。

关键词：秘密共享；博弈论；子秘密份额；中国剩余定理；重复博弈；公平性

Secret Sharing Scheme with Weighted Participants Based on Repeated Games

CAI Yong-quan, SUN Ke

(College of Computer Science, Beijing University of Technology, Beijing 100124, China)

【Abstract】In most secret sharing schemes with weighted participants, different amount of players' secret subshares can cause unfairness problem in the secret reconstruction phase. This paper proposes a rational secret sharing scheme based on repeated games. On the basis of original subshares, it constructs new subshares for each player, making sure that each two amount of subshares differ by a value at most 1. Through repeated games, every player can get all of other players' subshares and then reconstruct the secret. Analysis result shows that the scheme can make every rational player follow the secret reconstruction protocol all the time and be able to reconstruct the secret. And it has high security and expandability.

【Key words】secret sharing; game theory; secret subshare; Chinese remainder theorem; repeated games; fairness

DOI: 10.3969/j.issn.1000-3428.2012.18.032

1 概述

文献[1-2]分别基于 Lagrange 插值多项式和几何方法提出(t,n)门限秘密共享方案。在现实生活中，参与者往往具有不同的权重。文献[3]基于中国剩余定理，提出一个参与者具有权重的秘密共享方案，只有当参与者的权重之和达到门限值时，才能重构出秘密，而与参与者的数量无关。

目前绝大多数参与者有权重的方案[4-5]都是基于中国剩余定理的，参与者的权重越大，秘密分发阶段获得的子份额数量就越多。在秘密重构时，由于参与者发送份额的速度、网络等一系列因素，很难保证参与者同时接收完其他参与者发送的份额，而权重较大的参与者仅需少量的份额便可以重构出秘密，因此权重较大的参与者往往能够率先接收完重构秘密所需的全部份额。考虑参与者是理性的情形，他们一方面希望获得秘密，另一方面又希望尽可能少的其他人获得秘密，所以一旦自己已经获得了足够的份额，而自己手中的份额尚未发送完毕时，就可以选择停止发送自己的份额，并自行重构出秘密，从而获得最大利益。对于诚实执行协议的权重小的参与者来说，由于没有接收到权重大的参与者手中的全部份额，因此无法重构出秘密，显然这是不公平的。这种由于参与者手中子秘密份额数量的不同造成的不公平问题，传统的秘密共享方案是很难解决的。文献[6]将博弈论的思想引入到秘密共享方案中，解决了理性参与者条件下秘密重构过程无法顺利进行的问题。文献[7-8]利用重复博弈提出了新的理性秘密共享协议，使得参与者放弃短期利益而遵守协议。本文在文献[3]的基础上，基于重复博弈，通过为参与者构造数量差不超过1的有效子秘密份额，提出了一个参与者有权重的理性秘密共享方案，使得理性参与者为了长远利益必须自始至终遵守协议，因此，所有的参与者最终都可以重构出秘密，解决了由于参与者手中份额数量不均所导致的不公平问题。本文方案不需要秘密分发者的频繁参与，还可以检测参与者的欺骗行为，因此，具有良好的安全性和扩展性。

2 参与者有权重的(t,n)门限秘密共享

定义1 参与者有权重的(t,n)门限秘密共享[4]

令$\{P_1,P_2,\cdots,P_n\}$为参与者集合，参与者的权重分别为$weight(P_i)=w_i, i=1,2,\cdots,n$。现假设参与者$P_1,P_2,\cdots,P_r(r\leqslant n)$参与秘密重构，当且仅当$\sum_{i=i}^{r} weight(P_i)\geqslant t$时，才可以重构出

基金项目：国家自然科学基金资助项目(61170221)；北京市自然科学基金资助项目(1102003)

作者简介：蔡永泉(1956－)，男，教授、博士生导师，主研方向：密码学，网络安全；孙 科，硕士研究生

收稿日期：2011-12-16 **修回日期：**2012-02-10 **E-mail：**sunke0517@163.com

秘密，否则，参与者无法获得秘密的任何信息。

3 参与者有权重的理性秘密共享方案

3.1 理性假设

博弈论认为参与者是理性的，他们选择策略的依据就是最大化自己的收益。如果参与者偏好某种策略，那是因为这种策略所带来的结果能够增加他们的收益。本文假设理性参与者都想要得到秘密，同时希望尽可能少的其他参与者得到秘密。如果用 $u_i(o)$ 表示 P_i 关于结果 o 的效用函数，在秘密恢复的过程中可能出现以下结果：参与者 P_i 自己获得秘密，而其他参与者均没有获得秘密，记 $u_i(o)=U^+$；所有参与者都获得秘密，记 $u_i(o)=U$ ；所有参与者都没有获得秘密，记 $u_i(o)=U^-$。根据上述假设，可得：

$$U^+ > U > U^-$$

本文将秘密重构过程建模成重复博弈。

定义 2 重复博弈[9]

对于策略式博弈 $G=\{N,S,u\}$，其中，$N=\{1,2,\cdots,n\}$ 为参与者集合；$S=\{S_1,S_2\cdots,S_n\}$ 为所有参与者的策略空间；$u=\{u_1,u_2,\cdots u_n\}$ 为所有参与者的收益函数，如果 G 不断重复，并且在下一次博弈 G 开始前，所有以前博弈的历史都被观察到，那么它构成的动态博弈就称为重复博弈。

3.2 方案描述

3.2.1 参数假设

设 $\{P_1,P_2\cdots,P_n\}$ 为参与者集合，参与者 P_i 的权重为 $weight(P_i)=w_i, i=1,2,\cdots,n$。$t$ 为门限值，且 $t<n$。设 p 是一个大素数，Z_p 为相应的有限域，g 为 Z_p 上的生成元。$H(r,s)$ 为一个二元单向函数，在公告栏上公开 $g,p,H(r,s)$，所有参与者可以从公告栏上下载信息，但是只有分发者有权发布、更改公告栏信息。K 为待分享秘密。

3.2.2 秘密分发阶段

秘密分发过程如下：

步骤 1 分发者随机选取 $r\in Z_p$ 并在公告栏上公开，参与者 P_i 自行选取 $s_j\in Z_p$，计算 $I_i=H(s_i,r), i=1,2,\cdots,n$，并将 I_i 发送给秘密分发者。秘密分发者在收到 I_i 后必须确保 I_i 互不相同，否则，通知相应的参与者令其重新选取 s_i。参与者公开 I_i 并将其作为参与者 P_i 的身份。

步骤 2 分发者在 Z_p 中随机选取 $b_i\in Z_p$，$i=1,2,\cdots,t-1$，构成多项式：$f(x)=K+b_1x+b_2x^2+\cdots+b_{t-1}x^{t-1}$。然后计算：$y_i(x)=f(x)\bmod(x-I_i)^{w_i}$，$i=1,2,\cdots,n$。不妨假设：$y_i(x)=a_0^i+a_1^ix+a_2^ix^2+\cdots+a_{w_i-1}^ix^{w_i-1}$，$i=1,2,\cdots,n$

步骤 3 分发者利用多项式 $y_i(x)$，$i=1,2,\cdots,n$ 随机选取 $a_{w_i}^i,\cdots,a_{D_i}^i\in Z_p$，其中，$D_i>\max\{w_1,w_2\cdots,w_n\}$，且 $|D_i-D_j|\leqslant 1$，$i,j=1,2,\cdots,n$，$i\neq j$，构造 n 个次数为 D_i 的多项式：

$$y_i'(x)=a_0^i+a_1^ix+a_2^ix^2+\cdots+a_{w_i-1}^ix^{w_i-1}+a_{w_i}^ix^{w_i}+\cdots+a_{D_i}^ix^{D_i}$$

步骤 4 分发者计算 $m_{ij}=y'_i(j)$，$j=1,2,\cdots,D_i+1$，并将 (j,m_{ij}) 发送给参与者 P_i。同时公布：

$$g^{a_0^i},g^{a_1^i},\cdots,g^{a_{D_i}^i}\bmod p,\ i=1,2,\cdots,n$$

3.2.3 秘密重构阶段

假设参与者 $P_1,P_2,\cdots,P_q$ 参与秘密恢复，不妨设：

$$\sum_{i=1}^{q}weight(P_i)=t$$

秘密重构过程如下：

步骤 1 每个参与者手中拥有 D_i+1，$i=1,2,\cdots,q$ 个子份额，通过重复博弈与其他参与者交换各自的子份额。以 P_i 和 P_j 相互交换子份额为例，在第 1 轮，P_i 和 P_j 发送 m_{i1} 和 m_{j1} 给对方；在第 r 轮 P_i 和 P_j 发送 m_{ir} 和 m_{jr} 给对方，如果其中一个参与者(假设为 P_j)在本轮没有收到对方发来的子份额，则在以后的各轮中 P_j 均不再发送自己的子份额给 P_i，协议终止。同时，对于参与者 P_i 发送来的子份额 m_{ir}，P_j 可以通过下式验证其真伪：

$$g^{m_{ir}}=\prod_{k=0}^{D_i}(g^{a_k^i})^{r^k}\bmod p,\ i=1,2,\cdots,n$$

一旦发现参与者有欺骗行为，则停止发送自己的子秘密份额，协议终止。

步骤 2 参与者获得其他人发送来的子份额以后，通过下式计算出多项式 $y_i'(x)$，$i=1,2,\cdots,q$：

$$y_i'(x)=\sum_{i=1}^{D_i+1}m_{ij}\prod_{j=1,j\neq i}^{D_i+1}\frac{x-j}{i-j}\bmod p=$$
$$a_0+a_1x+a_2x^2+\cdots+a_{w_i-1}x^{w_i-1}+a_{iw_i}x^{w_i}+\cdots+a_{iD_i}x^{D_i}$$

根据参与者的权重值 w_i，取 $y_i'(x)$ 的前 w_i 项，即可得到多项式 $y_i(x)$：

$$y_i(x)=a_0+a_1x+a_2x^2+\cdots+a_{w_i-1}x^{w_i-1},\ i=1,2,\cdots,n$$

步骤 3 根据中国剩余定理，当 $\sum_{i=1}^{q}weight(P_i)\geqslant t$ 时，下式可以唯一确定一个次小于 $\sum_{i=1}^{q}weight(P_i)$ 的多项式 $f'(x)$：

$$\begin{cases}f(x)\equiv y_1(x)\bmod(x-I_1)^{w_1}\\ f(x)\equiv y_2(x)\bmod(x-I_2)^{w_2}\\ \cdots\\ f(x)\equiv y_q(x)\bmod(x-I_q)^{w_q}\end{cases}$$

由于：

$$degree(f(x))=t-1<\sum_{i=1}^{q}weight(P_i)$$

因此 $f(x)=f'(x)$。

求解方法基于中国剩余定理，过程如下[3]：

(1)计算：$M=(x-I_i)^{w_1}(x-I_2)^{w_2}\cdots(x-I_q)^{w_q}$。

(2)计算：$M_i=M/(x-I_i)^{w_i}$。

(3)使用欧几里得扩展算法计算出 s_i、t_i，使得：

$$s_iM_i+t_i(x-I_i)^{w_i}=1$$

(4)计算：$c_i=y_i(x)\cdot s_i$。

(5)计算：$f(x)=\sum_{i=0}^{q}c_i\cdot M_i$。

(6)计算 $K=f(0)$ 即可获得共享的秘密。在 P_i 和 P_j 交换子份额的过程中，通过步骤(1)中的重复博弈，双方均可以获得对方的全部份额。P_i 和 P_j 分别具有 $d_i=D_i+1$ 和 $d_j=D_j+1$ 个子份额。由于：

$|D_i - D_j| \leqslant 1,\ i,j = 1,2,\cdots,n,\ i \neq j$

因此任意 2 个参与者之间的子份额数量差不超过 1，在 P_i 和 P_j 相互交换各自份额的过程中，存在如下情况：

(1) P_i 的子份额数比 P_j 少 1。在第 r 轮，每位参与者为了获得第 r+1 轮的子份额，会诚实地发送本轮的份额，否则会因无法获得下一轮子份额而无法重构出秘密。由于 P_i 的子份额数少，因此 P_i 率先发送完自己的份额，此后不再发送份额。而 P_j 不知道 P_i 已经发送完毕，为了获得 P_i 的全部份额，在接下来的一轮中继续发送自己的份额。这样 P_i、P_j 均可获得对方的全部份额。至此，交换过程结束。

(2) P_i 的子份额数与 P_j 相等。双方在同一轮发送完自己的份额，由于在接下来的各轮中再没有收到对方的份额，双方都可以知道已经获得对方的全部份额，因此交换过程结束。

(3) P_i 的子份额数比 P_j 多 1。这与情形(1)类似，在此不在赘述。

4 方案性能分析

本文参与者有权重的秘密共享方案具有以下特点：

(1)本文方案可以使参与者自始至终遵守协议，从而保证所有参与者都可以顺利重构出秘密，有效解决了传统方案中的不公平问题。

本文方案基于参与者原有的份额，为参与者构造了相互间数量差不超过 1 的有效子份额。在秘密重构过程中，参与者为了获得对方全部的子份额，必须诚实地在每一轮发送自己的份额。因为一旦在某一轮选择欺骗，其他参与者在以后的各轮中均不会再发送自己的子份额，这样，参与者就永远无法重构出秘密，无疑这种代价太大，所以为了长远利益，每个参与者会将自己的份额全部发送出去，最终每个参与者都可以获得秘密。由于各个参与者的子份额数量并非完全相同，因此参与者无法预测重复博弈在哪一阶段结束，从而有效防止了逆向归纳法的攻击。综上，本文方案可以避免传统方案中由于参与者手中子秘密份额数量不均造成的权重小的参与者无法获得秘密的问题。

(2)本文方案可以检测参与者提交份额的真实性。

在秘密重构阶段，参与者可能选择发送伪份额的策略。参与者在相互交换子份额的过程中，可以通过下式检验其他参与者所提交份额的真实性：

$$g^{m_{ir}} = \prod_{k=0}^{D_i} (g^{a_k^i})^{r^k} \bmod p,\ i = 1,2,\cdots,n,\ r = 1,2,\cdots,D_i + 1$$

证明：

$$\prod_{k=0}^{D_i} (g^{a_k^i})^{r^k} = g^{a_0^i \cdot r^0} \cdot g^{a_1^i \cdot r^1} \cdots\cdots g^{a_{D_i}^i \cdot r^{D_i}} =$$

$$g^{a_0^i \cdot r^0 + a_1^i \cdot r^1 + \cdots + a_{D_i}^i \cdot r^{D_i}} = g^{f_i(r)} = g^{m_{ir}} \bmod p$$

一旦检测出参与者有欺骗行为，参与者便选择终止协议。对每个参与者来说，一旦选择发送伪份额的策略，便永远无法重构出秘密。因此，理性参与者不会选择欺骗。

(3)本文方案可以动态地添加新成员。

当需要添加一个新成员 P_l 时，假设其权重为：

$weight(P_l) = w_l$

并且存在参与者 P_i，有 $weight(P_i) > weight(P_l)$，此时只需令新成员 P_l 自行选取 $s_l \in Z_p$，然后计算 $I_l = H(s_l, r)$，并将 I_l 发送给秘密分发者。秘密分发首先确保 I_l 不与现有的 $I_j,\ j = 1,2,\cdots,n$ 相同，否则通知新成员 P_l，令其重新选取 s_l。将 I_l 作为新成员 P_l 的身份。然后为新成员 P_l 分配相应的子秘密份额，公布相应的参数。这样，新成员便可以按照前面秘密重构协议与其他参与者重构秘密。

(4)本文方案可以动态地删除成员。

当删除某位参与者时，只要其余参与者的权重之和大于门限值，根据中国剩余定理，他们依然可以利用他们的多项式重构出秘密分发者所选择的多项式。进而获得秘密。参与者手中的份额不会因为被删除的成员而受到影响，也不会因为删除某位参与者而无法重构出秘密。

5 结束语

在传统参与者有权重的方案中，由于参与者手中子秘密份额数量的不同，因此会造成不公平问题。对此，本文结合博弈论，提出一个新的理性秘密共享方案。通过为参与者构造数量差不超过 1 的有效子秘密份额，并利用重复博弈，使每个参与者都可以获得其他参与者的全部份额，进而重构出秘密。本文方案满足参与者有权重的秘密共享体制的完备性，同时还可以检测秘密重构阶段参与者所提交份额的真实性，因此，具有较高的安全性。分析结果表明，本文方案可以方便地添加和删除成员，并且不影响参与者手中的现有份额，具有良好的实用性、扩展性。

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]//Proc. of National Computer Conference. New York, USA: [s. n.], 1979.

[3] 王明生, 刘卓军, 张艳硕. 权重不同参与者之间的秘密共享[J]. 北京电子科技学院学报, 2005, 13(2): 1-8.

[4] 张艳硕, 刘卓军, 柴凤娟. 参与者权重不同的防欺诈的动态秘密共享方案[J]. 计算机工程与应用, 2007, 43(29): 8-10.

[5] 兰建青, 张建中. 参与者有权重的动态多重秘密共享方案[J]. 计算机工程与应用, 2009, 45(33): 81-82.

[6] Halpern J, Teague V. Rational Secret Sharing and Multiparty Computation[C]//Proc. of the 36th Annual Symposium on Theory of Computing. Crete, Greece: ACM Press, 2001.

[7] Maleka S, Shareef A, Rangan C P. The Deterministic Protocol for Rational Secret Sharing[C]//Proc. of the 4th IEEE International Workshop on Security in Systems and Networks. [S. l.]: IEEE Press, 2008.

[8] Maleka S, Shareef A, Rangan C P. Rational Secret Sharing with Repeated Games[C]//Proc. of the 4th Information Security Practice and Experience Conference. Sydney, Australia: [s. n.], 2008.

[9] 姚国庆. 博弈论[M]. 北京: 高等教育出版社, 2007.

编辑 张 帆