基于双线性对的可验证的理性秘密共享方案

张 恩[1,2],蔡永泉[1]
(1.北京工业大学计算机学院,北京 100124; 2.河南师范大学计算机与信息技术学院,河南新乡 453007)

摘 要: 针对传统秘密共享方案不能事先预防参与者欺骗的问题,本文结合博弈论,提出了一种理性秘密共享方案,该方案基于双线性对,是可验证的,能检验参与者的欺骗行为.秘密分发者不需要进行秘密份额的分配,因此很大程度上提高了秘密分发的效率.在密钥重构阶段,不需要可信者参与.参与者偏离协议没有遵守协议的收益大,理性的参与者有动机遵守协议,最终每位参与者公平的得到秘密.另外,所提方案可以防止至多 $m-1$ 成员合谋.经过分析它们是安全和有效的.

关键词: 理性秘密共享; 博弈论; 双线性对; 单向函数
中图分类号: TP309 **文献标识码:** A **文章编号:** 0372-2112 (2012) 05-1050-05
电子学报 URL: http://www.ejournal.org.cn **DOI:** 10.3969/j.issn.0372-2112.2012.05.031

A Verifiable Rational Secret Sharing Scheme Based on Bilinear Pairing

ZHANG En[1,2], CAI Yong-quan[1]
(1. *College of Computer Science and Technology, Beijing University of Technology, Beijing* 100124, *China*;
2. *College of Computer and Information Technology, Henan Normal University, Xinxiang, Henan* 453007, *China*)

Abstract: To correct the problem that traditional secret sharing scheme can not take precautions against cheat, in this paper, we propose a rational secret sharing scheme. The proposed scheme based on bilinear pairing is verifiable and the participants' cheat can not work. The dealer doesn't need a secret share distribution. Therefore, the scheme greatly improves the efficiency of secret distribution. In addition, the trusted party is eliminated in the secret reconstruction phase. The gain of following the protocol is more than the gain of deviating, so rational player has an incentive to abide by the protocol. Finally, every player can obtain the secret fairly. Moreover, the scheme can withstand the conspiracy attack with at most $m-1$ players. By analysis, we find the scheme is secure and effective.

Key words: rational secret sharing; game theory; bilinear pairing; one-way function

1 引言

秘密共享是现代密码学研究的重要内容,有着广泛和重要的应用.秘密共享方案最早是由 Shamir[1] 和 Blakeley[2] 于1979年分别基于多项式插值法和多维空间点的特性提出的.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.但方案存在分发者和参与者欺骗的问题.为了解决欺骗问题,Chor[3] 等人提出可验证的秘密共享(Verifiable Secret Sharing,简称VSS),Feldman[4] 和 Pedersen[5] 分别提出一种能检验分发者和参与者欺骗的可验证的秘密共享方案.但是VSS方案只能起到事后验证而不能起到事先预防的作用.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 则可以独享秘密,尽管他能被检验出存在欺骗行为.Lin 和 Harn[6] 提出一种方案来解决此类问题,但在该方案中,如果秘密在最后一轮,欺骗者通过欺骗将独得秘密,那么用逆向归纳法来分析,所有的参与者将保持沉默,秘密不会被重构.庞辽军[7] 等人提出一种门限多重秘密共享体制,通过一次秘密共享过程就可以实现多个秘密的共享,但文献[7]在重构的过程中需要将参与者子份额提交给可信的秘密计算者,如果没有可信的秘密计算者,理性的参与者必然会采取欺骗的策略,而在网络环境下,要找到大家都信任的秘密计算者是一件非常困难的事情.

理性的秘密共享的概念首先由 Halpern 和 Teague[8] 于2004年提出,他们将博弈论引入秘密共享方案和安全多方计算,用以弥补传统方案的缺陷,其方案认为所

收稿日期:2010-10-20;修回日期:2011-11-07
基金项目:国家自然科学基金(No.61170221);国家973重点基础研究发展规划(No.2007CB311106);北京市自然科学基金(No.1102003)

有的参与者都是自私的,都想使自己的效益最大化,参与者通过对自身的利益得失的判断来决定是否遵守或背离协议.他们认为所设计的理性方案必须满足让参与者不知道协议什么时候结束,从而才能使他们有合作的动机.但他们的协议不能工作在 2 out of 2 模式下,另外他们的协议在一定条件下需要重启,这样分发者需要重新分发秘密份额,相当于分发者需要一直在线.之后,一系列文献对理性秘密共享进行了研究,G. Kol 和 M. Naor[9]采用一种信息论安全的方法设计了一种秘密共享方案,在他们的方案中不需要可计算假设,但他们的方案中不能防止拥有短份额的人和拥有长份额人的合谋攻击.S. Maleka 和 S. Amjed[10]提出一种基于重复博弈的秘密共享方案,通过考虑所有阶段博弈得益的贴现值之和(加权平均值)来对秘密共享建立模型,使得参与者考虑当前行为对后续博弈的影响,最终选择对自己最有利的策略,但参与者在最后一圈可以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.S Micali,和 A Shelat[11]提出的方案需要外部可信方在重构阶段参与,然而现实很难找到参与各方都信任的可信方.

本文的主要贡献是,我们提出一种新的可验证的理性秘密共享方案,方案采用文献[12]构造的基于双线性对的随机函数,来检验参与者的欺骗行为,用椭圆曲线上双线性对实现的密码算法可以获得更好的安全性、达到特定的安全级别所需的密钥长度更短.在我们协议中,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,从而很大程度上提高了秘密分发的效率.在重构阶段,不需要可信者参与秘密重构过程,每个参与者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,偏离协议没有遵守协议的收益大,理性的参与者不可能偏离协议,分发者和参与者的任何欺骗行为都能被检测出,最终,每个参与者公平的得到秘密.

2　基础知识

2.1　双线性映射

定义 1　设 G_1, G_2 是 2 个阶为素数 p 的循环群,G_1 为加法循环群,G_2 为乘法循环群,g 为 G_1 的生成元.如果满足下列性质,则称映射 $e: G_1 \times G_1 \to G_2$ 是双线性映射:

(1)双线性性:①对任意的 $P_1, P_2, Q \in G_1$, $e(P_1 + P_2, Q) = e(P_1, Q) \cdot e(P_2, Q)$;②对任意的 $P, Q_1, Q_2 \in G_1$, $e(P, Q_1 + Q_2) = e(P, Q_1) \cdot e(P, Q_2)$.

(2)非退化性:存在 $P, Q \in G_1$,使得 $e(P, Q) \neq 1$.

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

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 2　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 $(g, g^x, \cdots, g^{(x^q)}, e(g,g)^{1/x})$ 和 $(g, g^x, \cdots, g^{(x^q)}, \Gamma)$, $x \in Z_p^*$, $\Gamma \in G_2$.该假设也称为 DBDHI 问题.

2.2　博弈论相关知识

博弈论又叫对策论,目前在许多学科中都有重要的应用.博弈论中,将所有的人视为理性的,自私的,都是从最大化自己的利益出发,具体在理性秘密共享协议中就是每个参与者首先需要了解秘密,其次希望越少的人知道秘密越好.如果它们偏离协议不能比其遵守协议获得利益多,那么他们将会遵守协议,这是设计安全、稳定的密码协议的基础.我们用 a_i 表示参与者 P_i 的策略,a_{-i} 表示除 P_i 外其他人的策略,$a = (a_1, \cdots, a_n)$ 表示所有参与者的策略组合,$(a_i', a_{-i}) = (a_1, \cdots, a_{i-1}, a_i', a_{i+1}, \cdots, a_n)$ 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.

定义 3　在博弈 $\Gamma = (\{A_i\}_{i=1}^n, \{u_i\}_{i=1}^n)$ 中,策略组合 $a = (a_1, \cdots, a_n) \in A$ 为 Γ 的一个纳什均衡,如果由各个博弈方的各一个策略组成的某个策略组合 $a = (a_1, \cdots, a_n) \in A$ 中,任一博弈方 i 的策略 a_i,都是对其余博弈方策略组合的最佳策略,也即

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

通俗的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.此时,双方在对方给定策略下不愿意调整自己的策略,最好按协议走.

定义 4　在博弈 $\Gamma = (\{A_i\}_{i=1}^n, \{u_i\}_{i=1}^n)$ 中. $1 \leqslant t < n$,策略组合 $a = (a_1, \cdots, a_n) \in A$ 是一个 t-弹性均衡,如果 $C \subset [n]$, $|C| \leqslant t$, $i \in C$,对任意的 $a'_C \in \Delta(A_C)$,博弈保持

$$u_i(a_C', a_{-C}) \leqslant u_i(a) \tag{2}$$

文献[13]首先提出弹性均衡的概念,该均衡可以用在有 t 方合谋的博弈中,因为每一个博弈方都在其余 $t-1$ 个博弈方策略基础上最大化了自己的得益,所以没有任何人会偏离纳什均衡策略,即合谋成员的任何偏离都不会为自己带来利益.

2.3　Dodis and Yampolskiy 方案简介

本节简单介绍 Dodis and Yampolskiy 构造的基于双线性对的可验证随机函数.具体细节可参考文献[12]:方案主要有四部份组成:(1)公私钥产生模块 $Gen(1^k)$:

输入 1^k,输出 $SK=s, PK=g^s$;(2)加密模块 $F_{SK}(x)$:输入 SK, x,输出 $y=F_{SK}(x)=e(g,g)^{1/(x+SK)}$;(3)证据模块 $\pi_{SK}(x)$:输入 SK, x,输出 $\pi=\pi_{SK}(x)=g^{1/(x+SK)}$;(4)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),判断 $e(g^x\cdot PK,\pi)=e(g,g)$ 与 $y=e(g,\pi)$是否成立.若两式都成立输出 1,否则输出 0.

3 基于双线性对的可验证理性秘密共享方案

3.1 系统参数

我们令 $P=\{P_1,P_2,\cdots,P_n\}$是 n 个参与者的集合,用 s 表示在参与者间分享的秘密,$h(\cdot)$为单向哈希函数,$f(\cdot)$为单向函数,$sk_1,sk_2,\cdots,sk_n$ 为分别为参与者 i $(i=1,2,\cdots,n)$的私钥,$pk_1,pk_2,\cdots,pk_n$ 为参与者 $i(i=1,2,\cdots,n)$的公钥.

3.2 秘密分享阶段

Setp 1 分发者根据几何分布选择一个整数 $r^*\in\mathbb{N}$,几何分布的参数为 β,β 的值取决于参与者的效益(本文在第 4 节给出了 β 是如何选取的).分发者使用 $Gen(1^k)$模块产生$(pk_1,sk_1),\cdots,(pk_n,sk_n)$,其中 $sk_n=s_n$,$pk_n=g^{s_n}$.

Setp 2 分发者使用 n 个数值对$(h(ID_1\|r^*),F_{sk_1}(r^*)),\cdots,(h(ID_n\|r^*),F_{sk_n}(r^*))$确定一个 $n-1$ 次多项式如式(3):

$$\begin{aligned}G(x)=&\sum_{i=1}^{n}F_{sk_i}(r^*)\\&\cdot\prod_{j=1,j\neq i}^{n}\frac{x-h(ID_j\|r^*)}{h(ID_i\|r^*)-h(ID_j\|r^*)}\bmod q\\=&c_0^{r^{real}}+c_1^{r^{real}}x+c_2^{r^{real}}x^2+\cdots+c_{n-1}^{r^{real}}x^{n-1}\end{aligned}\tag{3}$$

令

$$M^r=G(0)\tag{4}$$

$$value=s-M^r\tag{5}$$

Setp 3 从$[1,q-1]-\{h(ID_i\|r)\mid i=1,2,\cdots,n,r=1,2,\cdots,r^*\}$中选取 $n-t$ 个最小的整数 $d_1,\cdots,d_{n-t}$.

Step 4 将 sk_i 通过安全信道传给参与者 i,同时公布 pk_i,$(d_1,G(d_1)),\cdots,(d_{n-t},G(d_{n-t}))$,$value$ 和 $f(c_j^{r^{real}})(j=0,1,\cdots n-1)$的值.

3.3 秘密重构阶段

在第 $r(r=1,\cdots,)$轮,参与者做以下工作:

Step 1 参与者 $i(i=1,2,\cdots,t)$同时发送 $y_i^r=F_{sk_i}(r)=e(g,g)^{1/(r+sk_i)}$,$\pi_i^r=\pi_{sk_i}(r)=g^{1/(r+sk_i)}$给其他参与者.

Step 2 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,协议继续.否则输出 0,协议结束,欺骗者将永远失去得到秘密的机会.

Step 3 参与者 $i(i=1,2,\cdots,t)$利用参与者身份信息可以构造 t 个数值对$(h(ID_1\|r),F_{sk_1}(r)),\cdots,h(ID_t\|r),(F_{sk_t}(r))$,结合$(d_1,G(d_1)),\cdots,(d_{n-t},G(d_{n-t}))$共 n 个数值对可以确定一个 $n-1$ 次多项式如下式:

$$\begin{aligned}P(x)=&\sum_{i=1}^{t}F_{sk_i}(r)\prod_{j=1,j\neq i}^{t}\frac{x-h(ID_j\|r)}{h(ID_i\|r)-h(ID_j\|r)}\\&\cdot\prod_{j=1}^{n-t}\frac{x-d_i}{h(ID_i\|r)-d_i}+\sum_{i=1}^{n-t}G(d_i)\\&\cdot\prod_{j=1,j\neq i}^{n-t}\frac{x-d_j}{d_i-d_j}\prod_{j=1}^{t}\frac{x-h(ID_j\|r)}{d_i-h(ID_j\|r)}\bmod q\\=&a_0^r+a_1^rx+a_2^rx^2+\cdots+a_{n-1}^rx^{n-1}\end{aligned}\tag{6}$$

如果 $f(a_j^r)\neq f(c_j^{r^{real}})(j=0,1,\cdots,n-1)$,协议执行下一轮,否则 $M^r=P(0)$,$s=value+M^r$.协议结束.

4 方案分析

4.1 正确性分析

定理 1 如果 $f(a_j^r)=f(c_j^{r^{real}})(j=0,1,\cdots,n-1)$,则 $r=r^*$,最终参与者能够得到正确的秘密 $s=value+M^r$.

证明 参与者 i 在第 r 轮,构造 t 个数值对$(h(ID_1\|r),F_{sk_1}(r)),\cdots,(h(ID_t\|r),F_{sk_t}(r))$结合$(d_1,G(d_1)),\cdots,(d_{n-t},G(d_{n-t}))$共 n 个数值对可以确定一个 $n-1$ 次多项式如式(6).如果 $f(a_j^r)=f(c_j^{r^{real}})(j=0,1,\cdots,n-1)$则 $r=r^*$,$P(0)=M^r=G(0)=M^{r^*}$,又 $value=s-M^{r^*}$,即 $s=value+M^r$.

4.2 安全性分析

下面本文从所采用加密算法的安全性,以及从博弈的角度来分析理性参与者没有攻击本文协议的动机两个方面对本文方案安全性进行度量.

定理 2 具有多项式计算能力的攻击者,不能突破本文采用的加密算法,独自得到秘密.

证明 在协议中,如果攻击者可以选择利用算法从已知信息中,计算出其他成员的私钥.那么攻击者不再需要执行本文协议,就可以独自重构出秘密.下面分析攻击者能否采用算法 A 来获得其他成员的私钥.在本文协议中,攻击者 A 通过执行协议可以得到 $y_i^r=F_{sk_i}(r)=e(g,g)^{1/(r+sk_i)}$,$\pi_i^r=\pi_{sk_i}(r)=g^{1/(r+sk_i)}$,其中 $i\neq A$.假设攻击者采用算法 A 能够攻破加密算法,从 y_i^r,π_i^r 中计算获得 sk_i 的话,那么就可以构造一个模拟算法 B,利用算法 A 以不可忽略的优势解决离散对数难题和 DBDHI 难题,而这是不可能的,所以攻击者不能独自获得秘密.

定理 3 当本文协议满足式(9)时,理性的参与者

不会背离协议.

证明　在本文协议中,参与者不清楚当前圈是真秘密所在圈,还是没有任何有用信息的测试圈.如果有一位参与者偏离协议,那么其他参与者将终止协议.欺骗者将永远得不到秘密,对于理性参与者来说,他们只能恰在真秘密所在 r^* 轮,不发送子份额或者发送错误的子份额(尽管事后能被发现,但欺骗者已经能够重构出秘密),才能获得比其他成员更多的利益.在我们方案中,合谋集团 $C\subset[n],|C|\leqslant m-1$ 中的合谋者通过合谋不能获得当前轮是真秘密所在轮,还是测试轮.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,猜对的概率为 λ^C,合谋者 P_i 获得效益为 U_i^+.如果猜错秘密,概率为 $1-\lambda^C$,合谋者 P_i 获得效益为 U_i^-.所以合谋者 P_i 的期望收益为

$$E(U_i^{C^{guess}})=\lambda^C * U_i^+ +(1-\lambda^C) * U_i^- \tag{7}$$

如果合谋成员参与协议时,恰好在真秘密所在轮进行攻击,概率 β,那么合谋者 P_i 获得效益为 U_i^+,否则合谋者 P_i 获得效益为 $E(U_i^{C^{guess}})$.因此合谋者 P_i 的期望收益至多为

$$\beta * U_i^+ +(1-\beta) * E(U_i^{C^{guess}}) \tag{8}$$

如果合谋成员遵守协议,那么合谋者 P_i 获得效益为 U_i,所以当满足式(9)时,合谋成员偏离协议没有遵守协议的收益大.

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

当满足式(9)时,没有合谋成员能通过背离协议来获得更大的收益,在每一轮中,理性的参与者不得不遵守协议,最终,每一个参与者都获得秘密.

4.3　性能分析与比较

本节我们将所提方案与现有典型的理性方案性能做比较,在我们协议中,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,从而很大程度上提高了秘密分发的效率.我们协议的期望执行时间为 $O(1/\beta)$.另外,我们的协议满足弹性均衡,能防止至多 $m-1$ 个参与者合谋.而文献[8]在处理 $m\geqslant 3, n>3$ 这种情况时,要把参与者分成 3 个组,每个组都有一个组长,方案不能防止组长间合谋.并且他们的协议不能工作在 2 out of 2 模式下,他们协议的期望执行时间为 $O(5/\alpha^3)$,当 α 值和本文采用的 β 值相等时(α,β 都小于 1),本文的期望执行时间更短.文献[9]采用一种信息论安全的方法设计了一种秘密共享方案,但他们的方案中不能防止拥有短份额的人和拥有长份额人的合谋攻击,他们协议在同时广播信道下的期望执行时间为 $O(1/\beta^2)$.在文献[10]中,参与者在最后一轮通过欺骗会以较高的概率获得秘密,另外因为他们协议对参与者的子份额,用拉格朗日插值法进行进一步的分解,所以他们的协议执行效率非常的低,协议的期望执行时间为 $O(n^2)$.从以上分析比较可知,我们方案的性能更加高效.

5　结论

结合博弈论和密码学,基于双线性对提出了一种新的可验证的理性秘密共享方案,在我们方案中,理性的参与者偏离协议的收益没有遵守协议的收益大,所以他们没有偏离协议的动机,从而可以达到事先预防参与者欺骗的目的.通过分析,我们发现该方案是简单、公平和有效的.但是,当前我们协议中没有考虑恶意的参与者,恶意参与者的最大利益不是获得秘密,而是阻止他人获得秘密,今后,我们将进一步研究如何防止恶意参与者的解决方案.

参考文献

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

[2] G R Blakeley. Safeguarding cryptographic keys[A]. Proceedings of the National Computer Conference[C]. New York: AFIPS Press, 1979. 313 – 317.

[3] Chor B, S Goldwasser, S Micali. Verifiable secret sharing and achieving simultaneity in the presence of faults[A]. Proceedings of the 26th Annual Symposium on Foundations of Computer Science[C]. Washington, DC: IEEE Computer Society, 1985. 383 – 395.

[4] P Feldman. A practical scheme for non-interactive verifiable secret sharing[A]. Proceedings of the 28th IEEE Symp. On Foundations of Comp, Science(FOCS'87)[C]. Los Angeles: IEEE Computer Society, 1987. 427 – 437.

[5] T P Pedersen. Distributed provers with applications to undeniable signatures[A]. Proceedings of Eurocrypt'91, Lecture Notes in Computer Science, LNCS 547[C]. Berlin: Springer-Verlag, 1991. 221 – 238.

[6] H Y Lin, L Harn. Fair reconstruction of a secret[J]. Information Processing Letters, 1995, 55(1): 45 – 47.

[7] 庞辽军,柳毅,王育民.一个有效的(t,n)门限多重秘密共享体制[J].电子学报,2006,34(4):585 – 589.
Pang Liaojun, Liu Yi, Wang Yumin. An efficient (t, n) threshold multi-secret sharing scheme[J]. Acta Electroncia Sinica, 2006, 34(4): 585 – 589. (in Chinese)

[8] J Halpern, V Teague. Rational secret sharing and multiparty computation[A]. Proceedings of the 36th Annual ACM Symposium on Theory of Computing(STOC)[C]. New York: ACM Press, 2004. 623 – 632.

[9] G Kol, M Naor. Games for exchanging information[A]. Proceedings of the 40th Annual ACM Symposium on Theory of

Computing(STOC)[C]. New York: ACM Press, 2008. 423 – 432.

[10] S Maleka, S Amjed, C P Rangan. Rational secret sharing with repeated games[A]. 4th Information Security Practice and Experience Conference, LNCS 4991[C]. Berlin: Springer-Verlag, 2008. 334 – 346.

[11] S Micali, A Shelat. Purely rational secret sharing[A]. 6th Theory of Cryptography Conference, LNCS 5444[C]. Berlin: Springer-Verlag, 2009. 54 – 71.

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

[13] I Abraham, D Dolev, R Gonen, J Halpern, Distributed computing meets game theory: robust mechanisms for rational secret sharing and multiparty computation[A]. 25th ACM Symposium Annual on Principles of Distributed Computing[C]. New York: ACM Press, 2006. 53 – 62.

作者简介

张 恩 男,1974 年生于河南新乡,现为北京工业大学博士研究生,河南师范大学讲师,主要研究方向为信息安全、计算机网络.

E-mail: zhangenzdrj@163.com

蔡永泉 男,1956 年生于安徽,博士,北京工业大学教授,博士生导师,主要研究方向为信息安全、密码学理论与应用.

E-mail: cyq@bjut.edu.cn