基于ElGamal密码体制的可验证秘密共享方案

柳 毅[1] 郝彦军[1] 庞辽军[2]
(广东工业大学计算机学院 广州 510006)[1]
(西安电子科技大学综合业务网国家重点实验室 西安 710071)[2]

摘 要 基于ElGamal密码体制,提出了一个新的可验证秘密共享方案。方案中,秘密份额由各个参与者自己选择,秘密分发者不知道各个参与者所持有的份额,而且秘密份额长度与共享秘密长度相同。重构秘密时,任一参与者只需计算一次即可确认参与者中是否存在欺诈者,欺诈成功的概率可忽略不计。若存在欺诈者,则可通过秘密分发者来确定欺诈者身份。该方案具有充分的秘密信息利用率和较少的验证计算量。当共享秘密更换时,参与者不必更换自己的秘密份额。并且,每个参与者只需维护一个秘密份额,就可以实现对多个秘密的共享。方案的安全性是基于ElGamal密码体制和Shamir门限方案的安全性。

关键词 ElGamal密码体制,可验证秘密共享,Shamir门限方案
中图法分类号 TN918.4 **文献标识码** A

Verifiable Secret Sharing Scheme Based on ElGamal Cryptosystem

LIU Yi[1] HAO Yan-jun[1] PANG Liao-jun[2]
(Faculty of Computer, Guangdong University of Technology, Guangzhou 510006, China)[1]
(National Key Laboratory on Integrated Services Networks, Xidian University, Xi'an 710071, China)[2]

Abstract Based on ElGamal cryptosystem, a new verifiable secret sharing scheme was proposed. In this scheme, each participant's secret shadow is selected by the participant himself and even the secret dealer does not know anything about his secret shadow. All these shadows are as short as the secret to be shared. In the recovery phase, any participant computes only one time in order to detect if cheats exist and the probability of successfully cheating can be ignored. The secret dealer can point out the identity of cheats if they exist. For this scheme, the secret information is fully used and the computation complexity of verifying can be reduced largely. The shadows do not need to be changed when the shared secret is renewed. Moreover, each participant can share many secrets with other participants by holding only one shadow. The security of this scheme is the same as that of the ElGamal cryptosystem and Shamir's (t,n) threshold secret sharing scheme.

Keywords ElGamal scheme, Verifiable secret sharing, Shamir's threshold scheme

1 引言

秘密共享机制是现代密码学领域中一个非常重要的分支,也是信息安全方向一个重要的研究内容。

第一个(t,n)门限秘密共享方案是1979年分别由Shamir[1]和Blakley[2]基于Lagrange插值法和多维空间点的性质提出的。一个秘密被n个参与者所共享,只有t个或t个以上的参与者联合才可以重构该秘密;而$(t-1)$个或更少的参与者不能得到该秘密的任何信息。实现(t,n)门限秘密共享方案的方法除了Shamir和Blakey的方案外,还有基于中国剩余定理的Asmuth-Bloom法[3]、使用矩阵乘法的Karnin-Greene-Hellman方法[4]等等。

关于可验证秘密共享,已有许多不同方案提了出来,如文献[5-8]。对于如何发现欺诈者,解决的方法主要有两种:一种情况是需要利用验证公式对每一个参与者提供的子秘密进行检查,存在欺诈者时,能够发现哪个参与者是欺诈者。但当没有欺诈者存在时,验证所需计算量并没有减少。针对这种情况,目前已有文献能够达到的信息率为1,即各个参与者所持有秘密份额长度与共享秘密长度相同,如文献[7,8]。另一种情况是在重构共享秘密阶段,计算一次即可确认参与者中是否存在欺诈者,若存在欺诈者,则再对每个参与者出示的子秘密进行逐个检查以确定欺诈者的具体身份。这种情况的优点是当不存在欺诈者时,验证所需的计算量大大减少。但是目前的方案秘密信息利用率只能达到1/2[9],即各个参与者所持有秘密份额长度是共享秘密长度的两倍,秘密信息利用率不高。

到稿日期:2009-09-18 返修日期:2009-12-07 本文受国家自然科学基金(60803151),广东联合基金重点项目(U0835004),广东工业大学博士启动基金(073036)资助。

柳 毅(1976-),男,博士后,副教授,CCF会员,主要研究方向为网络与信息安全,E-mail:liuyi_xd@126.com;郝彦军(1974-),男,博士,讲师,主要研究方向为密码学与信息安全;庞辽军(1977-),男,博士后,副教授,主要研究方向为密码学与信息安全。

在欺诈者较少的情况下(如参与者的范围相对较小或者对欺诈者的惩罚力度加大),以上两种解决方法或者验证所需计算量较大,或者秘密信息利用率较低,都不能充分发挥系统性能。本文基于 ElGamal 密码体制提出一个有效的、计算上安全的可验证秘密共享方案。该方案信息率为 1,而且重构秘密时,任一参与者只需计算一次即可确认参与者中是否存在欺诈者,欺诈成功的概率可忽略不计。若存在欺诈者,则可进一步通过秘密分发者确定欺诈者身份。因此,方案特别适合欺诈者出现机会较少的情况。另外,参与者和秘密分发者之间不需要传递任何秘密信息,因此不需要维护安全信道。当共享秘密更换时,参与者也不必更换自己的秘密份额。并且,每个参与者只需维护一个秘密份额,就可以实现对多个秘密的共享。

2 方案描述

设 d 为秘密分发者(dealer),$P=\{P_1,P_2,\cdots,P_n\}$ 是 n 个参与者的集合。该方案需要一个公告牌(noticeboard),只有秘密分发者 d 可以修改、更新公告牌上的内容,其他人只能阅读或下载。方案由系统初始化、秘密分发以及秘密重构三部分构成。

2.1 系统初始化

首先,秘密分发者 d 选取安全系统参数 p,q,g。其中 p,q 是大素数,使得在 Z_p 上求解离散对数为困难问题,q 是 $p-1$ 的一个因子(q 需要大于所要共享的秘密);g 是 Z_p^* 中的一个 q 阶生成元。d 在公告牌上公布参数信息$\{p,q,g\}$。

然后,每个参与者 P_i 随机选取一个整数 $r_i(r_i\in Z_q)$,计算 $R_i=g^{r_i} \bmod p$。P_i 将 R_i 发送给秘密分发者 d,而将 r_i 保密。秘密分发者 d 需确保对于不同的参与者,$R_i\neq R_j,i\neq j$。否则,秘密分发者必须要求这些参与者重新选取秘密份额,直到所有的参与者都有不同的份额为止。

最后,秘密分发者 d 为每个参与者 P_i 随机选取一个惟一的整数 $ID_i(n+2-t\leqslant ID_i<p)$作为其身份标识,用来标识该参与者。并在公告牌上公开每个参与者 P_i 的信息$\{R_i,ID_i\}$。

2.2 秘密分发

在 n 个参与者 $P_1,P_2,\cdots,P_n$ 中共享秘密 $s(s\in Z_q)$,使得至少有 t 个参与者合作才能重构该秘密。秘密分发者 d 进行如下过程:

(1)计算 $R_s=g^s \bmod p$;

(2)在公告牌上公布关于共享秘密 s 的公开值 R_s;

(3)通过 $n+1$ 个点:$(0,s)$,$(ID_1,R_1^s \bmod p)$,$(ID_2,R_2^s \bmod p)$,$\cdots$,$(ID_n,R_n^s \bmod p)$,利用 Lagrange 插值法构造 n 次多项式 $f(x)$:$f(x)=s\times\prod_{k=1}^{n}\frac{(x-ID_k)}{-ID_k}+\sum_{l=1}^{n}[(R_l^s \bmod p)\times(\frac{x}{ID_l})\times\prod_{k=1,k\neq l}^{n}\frac{(x-ID_k)}{ID_l-ID_k}] \bmod q$

(4)计算并在公告牌上公布 $f(1),f(2),\cdots,f(n+1-t)$。

2.3 秘密重构

不失一般性,设参与者集合 $\Gamma=\{P_1,P_2,\cdots,P_t\}$ 合作重构秘密,重构过程如下:

(1)Γ 中每个参与者 P_i 在公告牌上查看有关秘密 s 的公开信息 R_s。

(2)Γ 中每个参与者 P_i 利用自己的秘密份额 r_i,计算 $s_i=R_s^{r_i} \bmod p$,并将 s_i 发给指定的秘密生成者。

(3)秘密生成者在公告牌上查看公共信息 $f(1),f(2),\cdots,f(n+1-t)$,利用这 $n+1$ 个点:$(1,f(1)),(2,f(2)),\cdots,(n+1-t,f(n+1-t)),(ID_1,s_1),(ID_2,s_2),\cdots,(ID_t,s_t)$,通过 Lagrange 插值法重构 n 次多项式 $\tilde{f}(x)$。为简单起见,这里用$(x_i,y_i),i=1,2,\cdots,n+1$ 来表示$(n+1)$个数值对,则:

$$\tilde{f}(x)=\sum_{i=1}^{n}y_i\prod_{j=1,j\neq i}^{n+1}\frac{x-x_j}{x_i-x_j} \bmod q$$

(4)恢复共享秘密 $\tilde{s}=\tilde{f}(0) \bmod q$。

(5)判断是否存在欺诈者。首先给出以下定理。

定理 1 在秘密重构阶段第(2)步,集合 Γ 中参与者传送给秘密生成者共有 t 个 $s_i(i=1,2,\cdots,t)$。从其中任意选取一个,若验证等式(1)不成立,则必定存在欺诈者;若验证等式(1)成立,则欺诈成功的概率不超过 $\frac{1}{q}$。

$$s_i=(R_i)^{\tilde{s}} \bmod p \tag{1}$$

证明:(a)等式(1)不成立,则必定存在欺诈者。

用反证法。如果集合 Γ 中的所有参与者都是诚实的,秘密生成者通过 Lagrange 插值构造的 n 次多项式 $\tilde{f}(x)$,必然有 $\tilde{f}(x)=f(x)$,进一步得到 $\tilde{s}=s$,所以

$$s_i=(R_s)^{r_i} \bmod p=(g^s)^{r_i} \bmod p=g^{s\cdot r_i} \bmod q=(g^{r_i})^s \bmod p=(R_i)^s \bmod q=(R_i)^{\tilde{s}} \bmod p$$

因此,若等式(1)不成立,则一定存在欺诈者。

(b)若等式(1)成立,则欺诈成功的概率不超过 $\frac{1}{q}$。

假设集合 Γ 中存在 $m(1\leqslant m\leqslant t)$个欺诈者,不妨设欺诈者为$\{P_1,P_2,\cdots,P_m\}$,而$\{P_{m+1},P_{m+2},\cdots,P_t\}$为诚实的参与者。则在秘密重构阶段第(2)步,欺诈者提供给秘密生成者的 s_k 为:

$s_k=(R_s)^{\tilde{r}_k} \bmod p$,其中 $\tilde{r}_k\neq r_k \bmod q,k=1,2,\cdots,m$

这样,通过 Lagrange 插值构造的 n 次多项式 $\tilde{f}(x)$,必有 $\tilde{f}(x)\neq f(x)$,下面分两种情况讨论。

b1. 当 $\tilde{f}(0)=f(0) \bmod q$,即 $\tilde{s}=s$ 时。

因为 $s\in Z_q$,所以当 $\tilde{f}(x)\neq f(x)$,而 $\tilde{f}(0)=f(0) \bmod q$,即 $\tilde{s}=s$ 时的概率为 $\frac{1}{q}$。

当选取 $s_k,k=1,2,\cdots,m$ 时,$s_k=(R_s)^{\tilde{r}_k} \bmod p=g^{s\cdot\tilde{r}_k} \bmod p$,而$(R_i)^{s^*} \bmod p=g^{s\cdot r_k} \bmod p$。由于 $\tilde{r}_k\neq r_k \bmod q$,即 $s\cdot\tilde{r}_k \bmod p\neq s\cdot r_k \bmod q$,因此等式(1)不成立。

当选取 $s_l,l=m+1,m+2,\cdots,t$ 时,$s_l=(R_s)^{r_l} \bmod p=g^{s\cdot r_l} \bmod p=(R_l)^s \bmod p=(R_l)^{\tilde{s}} \bmod p$,等式(1)成立。

因此,在情况 b1 时,等式(1)成立,即欺诈成功的概率为 $\frac{t-m}{t}\times\frac{1}{q}$。

b2. 当 $\tilde{f}(0)\neq f(0) \bmod q$,即 $\tilde{s}\neq s$ 时。

因为 $s\in Z_p$,所以当 $\tilde{f}(x)\neq f(x)$,$\tilde{f}(0)\neq f(0) \bmod q$,即 $\tilde{s}\neq s$ 时的概率为 $1-\frac{1}{q}$。

当选取 $s_k,k=1,2,\cdots,m$ 时,$s_k=(R_s)^{\tilde{r}_k} \bmod p=g^{s\cdot\tilde{r}_k} \bmod p$,而$(R_i)^{\tilde{s}} \bmod p=g^{\tilde{s}\cdot r_k} \bmod p$。若要等式(1)成立,必须有 $s\cdot\tilde{r}_k=\tilde{s}\cdot r_k \bmod q$,即欺诈者需要能够提供满足条件 $\tilde{r}_k=r_k\cdot(\tilde{s}\cdot s^{-1}) \bmod q$ 的 $\tilde{r}_k$。由于参与者 P_k 不知道$(\tilde{s}\cdot s^{-1})$

mod q，因此他找到满足条件的$\tilde{r_k}$($\tilde{r_k}\in Z_q$)的概率为$\frac{1}{q}$。

当选取 s_l，$l=m+1,m+2,\cdots,t$ 时，$s_l=(R_s)^{r_l} \bmod p=g^{s\cdot r_l} \bmod p\neq g^{s\cdot \tilde{r}_l} \bmod p=(R_l)^s \bmod p$，等式(1)不成立。

因此，在情况 b2 时，等式(1)成立，即欺诈成功的概率为$\frac{m}{t}\times\frac{1}{q}\times(1-\frac{1}{q})$。

综合 b1、b2 两种情况，欺诈者成功欺诈的概率为：

$$\frac{t-m}{t}\times\frac{1}{q}+\frac{m}{t}\times\frac{1}{q}\times(1-\frac{1}{q})<\frac{t-m}{t}\times\frac{1}{q}+\frac{m}{t}\times\frac{1}{q}=\frac{1}{q}$$

根据定理 1，秘密生成者只需从 t 个 $s_i(i=1,2,\cdots,t)$ 中任意选取一个，验证等式(1)是否成立，只需计算一次即可以很高的概率发现系统中是否存在欺诈者，欺诈成功的概率不超过$\frac{1}{q}$。

若等式(1)不成立，为了进一步确定欺诈者的身份，秘密生成者通知秘密分发者 d 利用秘密 s 来对 t 个 $s_i(i=1,2,\cdots,t)$ 逐个进行验证，看是否有下式成立：

$$s_i=(R_i)^s \bmod p \tag{2}$$

若式(2)成立，P_i 为诚实参与者；反之，P_i 为欺诈者。因为当 P_i 为诚实参与者时，有：

$$s_i=(R_s)^{r_i} \bmod p=(g^s)^{r_i} \bmod p=g^{s\cdot r_i} \bmod p=(g^{r_i})^s \bmod p=(R_i)^s \bmod p$$

而当 P_i 为欺诈者时，由于$\tilde{r_k}\neq r_k \bmod q$，因此 $s\cdot\tilde{r_k}\neq s\cdot r_k \bmod q$，进一步有：

$$s_i=g^{s\cdot\tilde{r_i}} \bmod p\neq g^{s\cdot r_i} \bmod p=(R_i)^s \bmod p$$

3 方案分析与讨论

3.1 安全性分析

方案的安全性是基于有限域上求解离散对数的困难性和 Shamir 门限方案的安全性。

重构 n 阶多项式 $f(x)$需要知道$(n+1)$个满足 $y_i=f(x_i)$ 的点(x_i,y_i)。而$(t-1)$个或更少的参与者的合作不可能得到这样的$(n+1)$个点。利用 n 个或更少的点重构 n 阶多项式 $f(x)$等价于破解 Shamir 的(t,n)门限体制。因此，$(t-1)$个或更少的参与者合作不能正确重构 n 阶多项式 $f(x)$，也就不能恢复共享秘密 s。

方案中，每个参与者 P_i 只需维护一个可以重复使用的秘密份额 r_i，即使共享秘密 s 更换，秘密份额的重复使用也不会影响系统的安全性。这是因为，在系统初始化和秘密重构时，参与者 P_i 都不需要直接给出他的秘密份额 r_i，而只提供通过 r_i 计算得到的 $R_i=g^{r_i} \bmod p$ 和 $s_i=R_i^{r_i} \bmod p$。任何攻击者想要从 R_i 和 s_i 中推导出 r_i，其困难性都相当于求解有限域 Z_p 上的离散对数问题，这在计算上是不可行的。因此在共享秘密更换时，参与者仍然可以重复使用自己的秘密份额。

除了重构 n 阶多项式 $f(x)$，没有其他方法能够得到共享秘密 s，因为在系统中，攻击者能够得到的有关共享秘密的信息为 $R_s=g^s \bmod p$ 和 $s_i=R_i^{r_i} \bmod p=(R_i)^s \bmod p$。若要从 R_s 和 s_i 中推导出 s，其困难性都相当于求解有限域 Z_p 上的离散对数问题，在计算上是不可行的。

3.2 性能分析

方案中主要的运算为多项式插值和模指数运算。针对这两种运算已有不少文献进行了研究，如文献[7]中给出了计算多项式插值的有效方法，其计算复杂度为 $O(n\log^2 n)$；另外，文献[7,10]中也分别给出了若干计算快速模指数的方法。这些都使得本文的方案可以有效地快速实现。

3.2 共享多个秘密

本文提出的方案同样可以在 n 个参与者中共享 $m(m>1)$个秘密 $S_1,S_2,\cdots,S_m$，使得至少有 t 个参与者合作才可以恢复出其中任意一个秘密。这里每个参与者 P_i 仍只需维护一个秘密份额 r_i。在秘密分发过程中，对不同的共享秘密 S_i，分发者需要计算并公布 $R_{S_i}=g^{S_i} \bmod p$，并且还需要计算和公布秘密 S_i 相应的公开信息 $f_i(1),f_i(2),\cdots,f_i(n+1-t)$。这样，任何 t 个或 t 个以上的合作者可以执行秘密重构算法恢复任一个秘密。由于参与者的秘密份额不会被泄漏，因此一个秘密的恢复不会影响其他未被恢复的秘密的安全性。

结束语 基于 ElGamal 密码体制和 Shamir 门限方案，本文提出了一个有效的可验证秘密共享方案。方案具有充分的秘密信息利用率和较少的验证计算量，特别适合欺诈者出现机会较少的情形。方案具有以下性质：1)秘密份额由参与者自己选择，任何人无法得知；2)秘密份额的长度与共享秘密长度相同，即秘密信息率为 1；3)只需计算一次即可以很高的概率发现参与者中是否存在欺诈者，欺诈成功的概率不超过 $1/q$，若存在欺诈者，可以进一步确认其身份；4)方案可以共享多个秘密，一个秘密的恢复不会影响其他未被恢复的秘密的安全性；5)系统各个实体之间不需要维护安全信道；6)方案安全性依赖于有限域上求解离散对数的困难性和 Shamir 门限方案的安全性。

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. Safeguarding cryptographic keys[A]// Proc. AFIPS 1979 National Computer Conference[C]. New York: AFIPS Press, 1979: 313-317

[3] Asmuth C, Bloom J. A modular approach to key safegrarding [J]. IEEE Transactions on Information Theory, 1983, 29(2): 208-210

[4] Karnin E D, Green J W, Hellman M E. On sharing secret system [J]. IEEE Transactions on Information Theory, 1983, 29(1): 35-41

[5] Chien H Y, Jan J K, Tseng Y M. A practical (t,n) multi-secret sharing scheme [J]. IEICE Transactions on Fundamentals, 2000, 83 (12): 2762-2765

[6] Yang C C, Chang T Y, Hwang M S. A (t,n) multi-secret sharing scheme[J]. Applied Mathematics and Computation, 2004, 151(2): 483-490

[7] Hwang R J, Chang C C. An on-line secret sharing scheme for multi-secrets[J]. Computer Communications, 1998, 21(13): 1170-1176

[8] 庞辽军，王育民. 基于 RSA 密码体制(t,n)门限秘密共享方案[J]. 通信学报，2005，26(6)：70-73

[9] 许春香. 安全秘密共享及其应用研究[D]. 西安：西安电子科技大学，2003

[10] Chang C C, Horug H J, Buehrer D J. A cascade exponentiation evaluation scheme based on the Lempel-Ziv-Welch compression algorithm[J]. Journal of Information Science and Engineering, 1995, 11(3): 417-431