第 37 卷 第 14 期
Vol.37 No.14

计 算 机 工 程
Computer Engineering

2011 年 7 月
July 2011

• 安全技术 •

文章编号：1000—3428(2011)14—0118—02 文献标识码：A 中图分类号：TP918

基于 RSA 密码体制的公平秘密共享新方案

柳 毅[1,2]，郝彦军[1]，庞辽军[3]

(1. 广东工业大学计算机学院，广州 510006；2. 南京大学计算机软件新技术国家重点实验室，南京 210093；
3. 西安电子科技大学综合业务网国家重点实验室，西安 710071)

摘 要：基于 RSA 密码体制，提出一个新的(*v*, *t*, *n*)公平秘密共享方案。在该方案中，秘密份额由各参与者自己选择，其他人均不知道该份额。在重构秘密时，即使存在 *v*(*v*<*t*/2)个欺诈者，所有参与者仍有相同的概率恢复出共享秘密，且每个参与者只需维护一个秘密份额即可共享多个秘密。该方案的安全性基于 RSA 密码体制和 Shamir 门限方案的安全性。

关键词：RSA 密码体制；公平秘密共享；多秘密共享；Shamir 门限方案；欺诈者

Fair Secret Sharing Scheme Based on RSA Cryptosystem

LIU Yi[1,2], HAO Yan-jun[1], PANG Liao-jun[3]

(1. Faculty of Computer, Guangdong University of Technology, Guangzhou 510006, China; 2. State Key Laboratory for Novel Software Technology, Nanjing University, Nanjing 210093, China; 3. National Key Laboratory on Integrated Services Networks, Xidian University, Xi'an 710071, China)

【Abstract】Based on RSA cryptosystem, this paper proposes a new (*v*, *t*, *n*) fairness secret sharing scheme. In the scheme, each participant's secret shadow is selected by the participant himself and others do not know anything about his secret shadow. Even if *v*(*v*<*t*/2) cheaters exist among the *n* participants, all participants have equal probability to recover the shared secret. Each participant can share many secrets with other participants fairly by holding only one shadow. The security of the scheme is based on that of RSA cryptosystem and Shamir's (*t*, *n*) threshold secret sharing scheme.

【Key words】RSA cryptosystem; fair secret sharing; multi-secret sharing; Shamir's threshold scheme; cheater

DOI: 10.3969/j.issn.1000-3428.2011.14.038

1 概述

目前绝大多数秘密共享方案[1-4]在涉及欺诈者方面都是讨论如何发现欺诈者，而对于发现欺诈者后的情况讨论较少，欺诈者往往仍能恢复共享秘密，而诚实的参与者却不能。针对存在欺诈者的情况，文献[5]提出了一个(*v*, *t*, *n*)公平秘密共享方案，用以保证诚实参与者也能公平地恢复出共享秘密。系统中一个秘密被 *n* 个参与者共享，只有 *t* 个或 *t* 个以上的诚实参与者联合才能重构出该秘密。假设存在 *v* 个欺诈者，其中，*v*<*t*/2，该方案使得所有参与者(包括诚实者和欺诈者)有同样的概率恢复共享秘密。为了实现这样的公平性，每个参与者都必须持有分发者分发的 3 个秘密份额。随后，文献[6]对此进行了改进，使得每个参与者只需持有 2 个秘密份额即可实现诚实者与欺诈者在恢复共享秘密上的公平性。

本文基于 RSA 密码体制提出了一个新的(*v*, *t*, *n*)公平秘密共享方案。方案中参与者的秘密份额不需要由分发者分发，而是由各个参与者自己选择，其他人均不知道该份额。每个参与者只需保存一个秘密份额就可以实现公平的秘密共享，并且当共享秘密更换时，参与者不必更换自己的秘密份额却仍能保证整个系统安全有效。

2 新的秘密共享方案描述

设 *d* 为秘密分发者，$P=\{P_1,P_2,\mathrm{L}\ ,P_n\}$ 是 *n* 个参与者的集合，*s* 为共享秘密。假设系统中存在 *v* 个欺诈者，其中，*v*<*t*/2，并且需要一个公告牌，只有 *d* 可以修改。方案包括初始化阶段、秘密分发阶段和秘密重构阶段。

2.1 初始化

初始化过程如下：

(1)*d* 根据 RSA 密码体制的安全性要求选取系统参数 *p*、*q*，*p*、*q* 均是大素数。令 *N* 表示 *p* 与 *q* 的乘积。

(2)*d* 从 $[N^{\frac{1}{2}},N]$ 中随机选取 2 个不相等的整数 g_1、g_2，要求：$g_1\neq p$，$g_1\neq q$，$g_2\neq p$，$g_2\neq q$。

(3)*d* 随机选取一个大于 *N* 的素数 *Q*(要求 *Q* 大于共享秘密 *s*)，在公告牌上公布参数信息 $\{N,g_1,g_2,Q\}$。

(4)每个参与者 $P_i(i=1,2,\mathrm{L}\ ,n)$ 随机从 $[2,N]$ 中选取一个整数 S_i，计算 $R_{1i}=(g_1)^{S_i}\bmod N, R_{2i}=(g_2)^{S_i}\bmod N$。$P_i$ 保密 S_i，将 R_{1i}、R_{2i} 发送给 *d*，*d* 需要确保 $R_{1i}\neq R_{1j}$、$R_{2i}\neq R_{2j}(i\neq j)$，否则，*d* 必须要求参与者 P_i、P_j 重新选取他们的秘密份额，直到所有参与者都有不同的份额为止。

(5)*d* 随机地从 $[n+2-t,N]$ 中为每个参与者 P_i 选取一个唯一的整数 ID_i 作为其身份标识。*d* 在公告牌上公布每个参与者 P_i 的公开信息 $\{R_{1i},R_{2i},ID_i\}$。

2.2 秘密分发

在 *n* 个参与者 $P_1,P_2,\mathrm{L}\ ,P_n$ 中共享秘密 $s(s\in Z_Q)$，使得至少 *t* 个参与者合作才能重构该秘密。过程如下：

(1) *d* 随机选取 $a(a\in Z_Q,a\neq s)$，计算 $b=a\oplus s$，其中，$\oplus$ 为异或运算。

(2)*d* 从 $[2,N]$ 中随机选取一个整数 S_0，要求 S_0 与 $(p-1)$、

基金项目：国家自然科学基金资助项目(60803151)；NSFC-广东联合基金资助重点项目(U0835004)；计算机软件新技术国家重点实验室开放基金资助项目(2010B13)

作者简介：柳 毅(1976－)，男，副教授、博士，主研方向：网络与信息安全；郝彦军，讲师、博士；庞辽军，副教授、博士

收稿日期：2010-12-22 **E-mail：**liuyi_xd@126.com

$(q-1)$互素。计算：$R_{10}=(g_1)^{S_0} \bmod N$，$R_{20}=(g_2)^{S_0} \bmod N$。

(3)d计算整数h，要求满足$S_0 \times h=1 \bmod \phi(N)$，其中，$\phi(N)$为欧拉函数。$d$在公告牌上公布$\{R_{10},R_{20},h\}$。

(4)d通过$n+1$个点：$(0,a)$，$(ID_1,R_{11}{}^{S_0} \bmod p)$，$(ID_2,R_{12}{}^{S_0} \bmod p),\cdots,(ID_n,R_{1n}{}^{S_0} \bmod p)$，利用Lagrange插值法构造$n$次多项式$f_1(x)$：

$$f_1(x)=a\times\prod_{k=1}^{n}\frac{(x-ID_k)}{-ID_k}+\sum_{l=1}^{n}\left[(R_{1l}{}^{S_0} \bmod N)\times(\frac{x}{ID_l})\times\prod_{k=1,k\neq l}^{n}\frac{(x-ID_k)}{ID_l-ID_k}\right]\bmod Q$$

计算并在公告牌上公布$f_1(1),f_1(2),\text{L},f_1(n+1-t)$。

(5)d通过$n+1$个点：$(0,b)$，$(ID_1,R_{21}{}^{S_0} \bmod p)$，$(ID_2,R_{22}{}^{S_0} \bmod p),\text{L},(ID_n,R_{2n}{}^{S_0} \bmod p)$，利用Lagrange插值法构造$n$次多项式$f_2(x)$：

$$f_2(x)=b\times\prod_{k=1}^{n}\frac{(x-ID_k)}{-ID_k}+\sum_{l=1}^{n}\left[(R_{2l}{}^{S_0} \bmod N)\times(\frac{x}{ID_l})\times\prod_{k=1,k\neq l}^{n}\frac{(x-ID_k)}{ID_l-ID_k}\right]\bmod Q$$

计算并在公告牌上公布$f_2(1),f_2(2),\text{L},f_2(n+1-(t-v))$。

2.3 秘密重构

不失一般性，设参与者集合$\Gamma=\{P_1,P_2,\text{L},P_t\}$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$\{R_{10},R_{20},h,N\}$。

(2)Γ中每个参与者$P_i(i=1,2,\text{L},t)$利用秘密份额S_i计算并公开自己的第1个份额$S_{1i}=R_{10}{}^{S_i} \bmod N$。

(3)任何人都可以验证参与者P_i是否提供了诚实的子秘密。因为：

$$(S_{1i})^h \bmod N=(R_{10}{}^{S_i})^h \bmod N=((g_1{}^{S_0})^{S_i})^h \bmod N=g_1{}^{S_0\times h\times S_i} \bmod N=g_1{}^{S_i} \bmod N=R_{1i}$$

所以验证者可以验证是否有$R_{1i}=(S_{1i})^h \bmod N$成立，若等式成立，说明参与者$P_i$是诚实的。如果验证得到所有$t$个参与者均是诚实的，则继续下一步；否则，终止秘密重构。

(4)利用公告牌上的公共信息$f_1(1),f_1(2),\text{L},f_1(n+1-t)$，通过以下$n+1$个点：$(1,f_1(1)),(2,f_1(2)),\text{L},(n+1-t,f_1(n+1-t)),(ID_1,S_{11}),(ID_2,S_{12}),\text{L},(ID_t,S_{1t})$，采用Lagrange插值法重构$n$次多项式$f_1(x)$。为简单起见，这里用$(x_i,y_i),i=1,2,\text{L},n+1$表示$n+1$个数值对，则：

$$f_1(x)=\sum_{i=1}^{n}y_i\prod_{j=1,j\neq i}^{n+1}\frac{x-x_j}{x_i-x_j}\bmod Q$$

(5)Γ中每个参与者$P_i(i=1,2,\text{L},t)$提供自己的第2个份额$S_{2i}=R_{20}{}^{S_i} \bmod N$。

(6)任何人都可以验证参与者P_i是否提供了诚实的子秘密。因为：

$$(S_{2i})^h \bmod N=(R_{20}{}^{S_i})^h \bmod N=((g_2{}^{S_0})^{S_i})^h \bmod N=g_2{}^{S_0\times h\times S_i} \bmod N=g_2{}^{S_i} \bmod N=R_{2i}$$

所以验证者可以验证是否有$R_{2i}=(S_{2i})^h \bmod N$成立，若等式成立，说明参与者$P_i$是诚实的。

(7)因为假设系统中欺诈者的数目v小于$t/2$，所以当验证得到$t-v$个参与者为诚实者后(不妨假设这$t-v$个诚实者为P_i $(i=1,2,\text{L},t-v)$)，可利用公告牌上的信息$f_2(1),f_2(2),\text{L},f_2(n+1-(t-v))$，通过以下$n+1$个点：$(1,f_2(1)),(2,f_2(2)),\text{L},(n+1-(t-v)),f_2(n+1-(t-v)),(ID_1,S_{21}),(ID_2,S_{22}),\text{L},(ID_{t-v},S_{2(t-v)})$采用Lagrange插值法重构$n$次多项式$f_2(x)$。为简单起见，这里用$(x_i,y_i),i=1,2,\text{L},n+1$表示$n+1$个数值对，则：

$$f_2(x)=\sum_{i=1}^{n}y_i\prod_{j=1,j\neq i}^{n+1}\frac{x-x_j}{x_i-x_j}\bmod Q$$

(8)重构秘密$s=f_1(0)\oplus f_2(0)$。

3 方案可行性分析

下面分3种情况讨论方案的可行性。

情形1：所有t个参与者都诚实公布自己第1和第2份额，那么他们都能重构得到多项式$f_1(x)$、$f_2(x)$，进而通过等式$s=f_1(0)\oplus f_2(0)$求得共享秘密s。

情形2：在公布第1份额时存在v个欺诈者，那么诚实的参与者不能重构$f_1(x)$，也就不能得到$f_1(0)$，而欺诈者可以利用诚实参与者公布的信息重构得到$f_1(x)$。但诚实参与者通过验证公式发现存在欺诈者后，就不会继续发送自己的第2份额，这样，$v(v<t/2)$个欺诈者只能提供v个第2份额，而重构$f_2(x)$需要至少$t-v$个第2份额。由于$v<t-v$，因此欺诈者无法重构$f_2(x)$，也就不能得到共享秘密s。最终，欺诈者和诚实者都不能得到共享秘密s。

情形3：所有t个参与者都公布了正确的第1份额，但在公布第2份额时存在v个欺诈者。在这种情况下，显然所有t个参与者都能重构得到$f_1(0)$，v个欺诈者可以利用其他诚实参与者公布的第2份额重构得到$f_2(0)$。然而，通过$t-v$个正确的第2份额，$t-v$个诚实的参与者仍能重构多项式$f_2(x)$。最终，欺诈者和诚实者都能得到共享秘密s。

综合以上3种情形可以得出，本文方案能够实现诚实参与者和欺诈者在恢复共享秘密上的公平性，即所有参与者(包括诚实者和欺诈者)具有相同的概率恢复出共享秘密。

4 方案安全性分析

方案的安全性是基于RSA密码体制和Shamir门限方案的安全性。

根据Shamir门限方案，重构n阶多项式$f_1(x)$、$f_2(x)$需要分别知道$n+1$个点。由于$t-1$个或更少的参与者合作不可能得到满足$y_i=f_1(y_i)$的$n+1$个点(x_i,y_i)，因此$t-1$个或更少的参与者合作不能正确重构多项式$f_1(x)$。同样，$t-v-1$个或更少的参与者合作不可能得到满足$y_i'=f_2(x_i')$的$n+1$个点(x_i',y_i')，因此，$t-v-1$个或更少的参与者合作不能正确地重构多项式$f_2(x)$。

在本文的方案中，每个参与者P_i只需维护一个秘密份额S_i，并不会影响系统的安全性。一方面，在秘密重构过程中，每个参与者P_i只公开由S_i计算出的2个份额S_{1i}、S_{2i}，而无需直接给出S_i。P_i计算S_{1i}、S_{2i}的公式为：$S_{1i}=R_{10}{}^{S_i} \bmod N$和$S_{2i}=R_{20}{}^{S_i} \bmod N$，这可以看作是$P_i$执行了RSA算法的解密算法：$N$为模数，$S_i$为私钥，$R_{10}$、$R_{20}$为密文，$S_{1i}$、$S_{2i}$为明文。攻击者想要从$S_{1i}$、$S_{2i}$推导出$S_i$，其难度相当于解出RSA体制中的用户私钥，在计算上是不可行的。另一方面，攻击者可以设法由公告牌上的信息$\{R_{1i},R_{2i}\}$推导出S_i。但由于

(下转第122页)