第37卷 第14期 计 算 机 工 程 2011年7月
Vol.37 No.14 Computer Engineering July 2011

• 安全技术 • 文章编号：1000—3428(2011)14—0109—03 文献标识码：A 中图分类号：TP309

参与者有权重的特殊门限秘密共享方案

王 伟[1,2]，周顺先[2,3]

(1. 暨南大学管理学院，广州 510632；
2. 广州番禺职业技术学院信息工程学院，广州 511483；
3. 湖南大学软件学院，长沙 410082)

摘 要：基于Shamir门限方案、RSA密码体制和哈希函数的安全性构建一种参与者有权重的特殊门限秘密共享方案。秘密份额由参与者选择和保存，每个参与者只需维护一个秘密份额即可共享多个秘密。在信息交互过程中不需要传递任何秘密信息，系统无需维持专门的安全信道。理论分析结果表明，该方案安全有效，易于实现。

关键词：秘密共享；特殊门限方案；RSA密码体制；哈希函数

Special Threshold Secret Sharing Scheme Among Weighted Participants

WANG Wei[1,2], ZHOU Shun-xian[2,3]

(1. Management School, Jinan University, Guangzhou 510632, China;
2. School of Information Engineering, Guangzhou Panyu Polytechnic, Guangzhou 511483, China;
3. Software School, Hunan University, Changsha 410082, China)

【Abstract】This paper proposes a special threshold secret sharing scheme among weighted participants which is based on the security of Rivest Shamir Adleman(RSA) cryptosystem, Shamir threshold secret sharing scheme and hash function. Each participant's secret shadow is selected and saved by the participant himself, and he can share many secrets with other participants by holding only one secret shadow. In the process of information exchange, it is not necessary to pass any confidential information and the scheme does not need a secure channel between each participant and the dealer. Theoretical analysis shows that the scheme is secure, effective and easy to implement.

【Key words】secret sharing; special threshold scheme; Rivest Shamir Adleman(RSA) cryptosystem; hash function

DOI: 10.3969/j.issn.1000-3428.2011.14.035

1 概述

(t, n)秘密共享方案于1979年由Shamir A[1]和Blakley G[2]分别提出。在方案中，若参与者数量大于或等于门限值，则可合作重构共享秘密，否则不能得到共享秘密的任何信息。除此之外，还有一些比较有影响力的秘密共享方案，如利用中国剩余定理构造的Asmuth-Bloom法、使用矩阵乘法的Karnin-Greene-Hellman法等。这些方案都较简单，有一些共同的局限性：

(1)参与者的秘密份额由秘密分发者产生和分配；

(2)秘密份额只能使用一次；

(3)缺乏简单有效的检验算法以验证参与者信息的真实性；

(4)参与者的权限无差异；

(5)系统需要维护一条安全信道。

这些都制约了秘密共享方案在现实中的应用，尤其是安全信道，系统即使付出极大的代价，也未必能保证信息安全传送。

对于多重秘密共享的研究，文献[3]基于Shamir门限方案提出在一般访问结构上的秘密共享方案。文献[4]基于大整数分解和离散对数问题的难解性给出一种公开可验证的门限多重秘密共享方案。在上述方案中参与者只需要保存一份秘密份额，可共享多个秘密，但并没有涉及参与者权重不同的情况。

门限方案的核心是参与重构共享秘密的权重值之和是否达到门限值，而不仅在于参与者的数量，因此，参与者有权重的秘密共享研究更有意义。文献[5]利用差分方程给出具有特殊权限的$(m+n,t+1)$门限秘密共享方案。文献[6]基于中国剩余定理给出权重不同参与者之间的$(m+n_1+n_2+\mathrm{L}+n_l,$ $t+t_1+t_2+\mathrm{L}+t_l)$门限方案。但是，上述方案参与者的秘密份额必须由秘密分发者产生和分配，需要系统维护一条安全信道。

在某些情况下，参与共享的利益方有特殊要求，不仅参与者的权重之和要达到对应的门限值，而且要求某些指定的利益方必须参与。对应此类问题，本文基于Shamir门限方案、RSA(Rivest Shamir Adleman)密码体制和哈希函数的特性构建一种参与者有权重的特殊$(n_1+n_2+\mathrm{L}+n_m,t_1+t_2+\mathrm{L}+t_m,l,t)$门限秘密共享方案。

在方案中，秘密份额由参与者自己产生和保管，不对外公开，即使秘密分发者也不知晓；参与者的权限有所不同，

基金项目：国家自然科学基金资助项目(51074097)

作者简介：王 伟(1972－)，男，讲师、博士研究生，主研方向：密码学，信息安全；周顺先，副教授、博士

收稿日期：2011-02-15 **E-mail：**wangw@gzpyp.edu.cn

且同一个参与者共享不同秘密时，其权限也不尽相同；参与者只需维护一个秘密份额就可实现对多个秘密的共享。

2 特殊门限秘密共享方案定义

以现实中招投标为例，企业参与投标需得到董事会的授权，股东权重是有差异的；同时《招标投标法》规定，至少 3 家企业以及招标方、公证方等共同参与方可进行招投标活动；招标方、公证方为指定的参与者，且需要得到本单位授权。基于此类需求，本文定义一种参与者有权重的特殊 $(n_1+n_2+\mathrm{L}+n_m,t_1+t_2+\mathrm{L}+t_m,l,t)$ 门限秘密共享方案。

定义 设共享方案中参与者由 m 个集合组成，$A=\{A_1,A_2,\mathrm{L},A_m\}$，要求 $A_1\mathrm{I}A_2\mathrm{I}\mathrm{L}\mathrm{I}A_m=\Phi$。$t_i$ 为 A_i 的门限值，t 为 A 的门限值，要求都为正整数。参与者拥有一份秘密份额 Sa_{ij}。对于任一集合 A_i，参与者权重之和大于或等于对应的门限值 t_i 时，集合 A_i 获得授权参与重构共享秘密。在合作重构共享秘密的集合数不小于门限值 t，且指定的 l 个集合全部参与时，授权集合的参与者在一起可以重构共享秘密；若指定的 l 个集合中有一个未参与重构，则不论参与重构的集合数是否大于等于 t，参与者在一起都不能得到共享秘密的任何信息，称这种方案为参与者有权重的特殊 $(n_1+n_2+\mathrm{L}+n_m,t_1+t_2+\mathrm{L}+t_m,l,t)$ 门限秘密共享方案。

3 特殊门限秘密共享方案构成

假定方案中参与者的集合为 $A=\{A_1,A_2,\mathrm{L},A_m\}$，参与者数量为 $n=n_1+n_2+\mathrm{L}+n_m$，其中，$A_i=\{a_{i1},a_{i2},\mathrm{L},a_{in_i}\},i=1,2,\mathrm{L},m$；参与者权值为 $W_i=\{w_{i1},w_{i2},\mathrm{L},w_{in_i}\}$，要求为非负整数；$t_i$ 为 A_i 的门限值，大小由 A_i 决定，t 为参与者集合 A 的门限值；指定必须参与重构的集合数为 l，为方便描述，指定为 $\{A_1,A_2,\mathrm{L},A_l\}$，显然 $l<t\leqslant m$；所要共享的秘密为 s。方案有一个可信任的秘密分发者和一个公告牌，秘密分发者可以在公告牌发布、更新信息，其他参与者只能阅读或下载。方案分为初始化、秘密分发和秘密重构 3 个阶段。

3.1 初始化阶段

在初始化阶段，秘密分发者根据 RSA 密码体系的要求生成自己的公钥 (N,e) 和私钥 d。每个参与者确定自己的秘密份额。具体过程如下：

(1)秘密分发者随机选取 2 个大素数 p 和 q，计算 $N=pq$。随机选取加密密钥 e，要求 e 和 $(p-1)(q-1)$ 互素。

(2)秘密分发者利用欧几里德扩展算法计算解密密钥 d，要求 $ed\equiv1\bmod(p-1)(q-1)$，d 和 N 也互素。

(3)秘密分发者随机选取一个大素数 Q（$Q>\max(N,s)$），确定一个强 hash 函数 $h(x)$，要求 $h(x)$ 的值域为 $[0,Q]$，以及从 $[\sqrt{N},N]$ 中随机选取一个整数 g。公开信息 $(Q,N,e,h(x),g)$。

(4)参与者 a_{ij} 随机地从 $[2,N]$ 中选取一个整数 Sa_{ij} 作为自己的秘密份额，对外保密。

3.2 秘密分发

在 n 个参与者中共享秘密，获得授权的集合数目不小于 t，且指定的 l 个集合参与的条件下，参与者在一起可以合作重构共享秘密。秘密分发过程如下：

(1)秘密分发者对应于 m 个集合，在区间 $[\sqrt{N},N]$ 中随机选取整数值 $\{ls_1,ls_2,\mathrm{L},ls_m\}$ 作为中间秘密，要求 $ls_i\neq g,i=1,2,\mathrm{L},m$。计算 $S_i=ls_i^e\bmod N$，并将 $\{S_i\}$ 公开。

(2)参与者 a_{ij} 下载公告信息并计算伪秘密份额 $R_{ij}=S_i^{Sa_{ij}}\cdot\bmod N$，利用秘密分发者的公钥计算 $SR_{ij}=R_{ij}^e\bmod N$，a_{ij} 将 (ID_{ij},SR_{ij}) 发送给秘密分发者，ID_{ij} 为参与者的身份标识。

(3)秘密分发者计算 $R_{ij}=SR_{ij}^d\bmod N$，必须确定对于任意 2 个不同的参与者 a_{ij} 和 a_{kl}，有 $R_{ij}\neq R_{kl}$ 成立，否则要求其重新选择秘密份额，以保证参与者秘密份额的唯一性。同时公布 $\{(ID_{ij},w_{ij},h(R_{ij})),i=1,2,\mathrm{L},m,j=1,2,\mathrm{L},n_i\}$。

(4)秘密分发者计算 $h(ls_i)$ 并构造一个 l 次多项式 $f(x)=s+a_1x+a_2x+\mathrm{L}+a_lx^l\bmod Q$。其中，$a_1,a_2,\mathrm{L},a_l$ 均随机从 $GF(Q)$ 选取，且 $a_l\neq0$，s 为共享秘密。计算并公布 $y_i=f(h(ls_i)),i=1,2,\mathrm{L},l$。

(5)秘密分发者计算 $y_g=f(g)$ 并构造一个 $(t-l-1)$ 次多项式 $g(x)=y_g+b_1x+b_2x+\mathrm{L}+b_{t-l-1}x^{t-l-1}\bmod Q$。其中，$b_1,b_2,\mathrm{L},b_{t-l-1}$ 均随机从 $GF(Q)$ 选取，且 $b_{t-l-1}\neq0$，计算并公布：

$$y_i=g(h(ls_i)),i=l+1,l+2,\mathrm{L},m$$

3.3 秘密重构

不失一般性，假设某个参与者集合 $A'=\{A_1',A_2',\mathrm{L},A_t'\}$ 合作准备重构秘密 s，$A_i'\subseteq A_i$。A' 任意秘密指定一个参与者作为秘密生成者。为方便描述，定义如下：若 $a_{ij}\in A'$，则 $a_{ij}'=a_{ij}$、$w_{ij}'=w_{ij}$、$R_{ij}'=R_{ij}$，否则，$w_{ij}'=0$，a_{ij}' 命名为合作者。重构过程如下：

(1)秘密生成者根据 RSA 密码体系的要求生成自己的公钥 (N_{DC},e_{DC}) 和私钥 d_{DC}，将公钥 (N_{DC},e_{DC}) 和 (ID_{DC},R_{DC}^e) 发送给秘密分发者，秘密分发者确认秘密生成者的身份后将其公钥公布在公告牌上。要求 (N_{DC},e_{DC},d_{DC}) 和 (N,e,d) 无关联。

(2)合作者 a_{ij}' 从公告牌下载公开信息 (N_{DC},e_{DC})，计算 $R_{ij}^*=R_{ij}'^{e_{DC}}=R_{ij}^{e_{DC}}\bmod N_{DC}$。并将 (ID_{ij},R_{ij}^*) 发送给指定的秘密生成者。

(3)秘密生成者计算 $\overline{R}_{ij}=R_{ij}^{*d_{DC}}\bmod N_{DC}$ 和 $h(\overline{R}_{ij})$，并和公开信息比对，若 $h(\overline{R}_{ij})=h(R_{ij})$，则可以判断 a_{ij}' 没有撒谎，否则向其发送警告信息，并让其重新发送 R_{ij}^*。

(4)对应于集合 A_i'，秘密生成者解密得到 $\{R_{ij}'\},j=1,2,\mathrm{L},n_i$。查阅公告信息，计算并判断 $\sum_{j=1}^{n_i}w_{ij}'\geqslant t_i$ 是否成立，若成立，则将 $\{R_{ij}'\}^e\bmod N$ 发送给秘密分发者；否则，说明集合 A_i' 没有资格参与重构共享秘密。

(5)秘密分发者解密收到的信息 $\{R_{ij}'\}$，在确认合作者授权真实，并判断 $\sum_{j=1}^{n_i}w_{ij}'\geqslant t_i$ 成立的条件下，计算 $y_i=(S_i^d/\prod_{j=1}^{n_i}R_{ij}')\bmod N=(S_i^{d-\sum_{j=1}^{n_i}Sa_{ij}})\bmod N$，并将信息 $\{y_i\}^{e_{DC}}\bmod N_{DC}$ 发送给秘密生成者；否则发送警告信息。

(6)秘密生成者解密得到 $\{y_i\}$，计算 $y_i\times\prod_{j=1}^{n_i}R_{ij}'=y\times\prod_{j=1}^{n_i}S_i^{Sa_{ij}}=S_i^{d-\sum_{j=1}^{n_i}Sa_{ij}}\times S_i^{\sum_{j=1}^{n_i}Sa_{ij}}=S_i^d\bmod N=ls_i$，从而得到参与重构集合的全部中间秘密 $\{ls_1,ls_2,\mathrm{L},ls_t\}$。

(7)秘密生成者计算 $h(ls_i)$，查阅公告信息得到 $(t-l)$ 个点 $\{(h(ls_i),y_i)\},i=l+1,l+2,\mathrm{L},t$，利用 Lagrange 插值法重构一个

$(t-l-1)$ 阶多项式，表示如下：

$$g(x)=\sum_{i=l+1}^{t} y_i \prod_{j=l+1,j\neq i}^{t} \frac{x-h(ls_j)}{h(ls_i)-h(ls_j)}=$$
$$y_g+b_1x+b_2x^2+\mathrm{L}+b_{t-l-1}x^{t-l-1} \bmod Q$$

计算得到 $y_g=g(0) \bmod Q$。

(8)秘密生成者根据 $(l+1)$ 个点及 (g,y_g) 和 $\{(h(ls_i),y_i)\}$，$i=1,2,\mathrm{L},l$，利用 Lagrange 插值法重构一个 l 阶多项式，表示如下：

$$f(x)=\sum_{i=1}^{l} y_i\Big(\prod_{j=1,j\neq i}^{l} \frac{x-h(ls_j)}{h(ls_i)-h(ls_j)}\Big)\times\frac{x-h(ls_j)}{g-h(ls_j)}+y_g\prod_{j=1}^{l}\frac{x-h(ls_j)}{g-h(ls_j)}=$$
$$s+a_1x+a_2x^2+\mathrm{L}+a_lx^l \bmod Q$$

计算得到共享秘密 $s=f(0) \bmod Q$。

3.4 多个秘密共享

在 n 个参与者中共享 r 个秘密 $\{s_1,s_2,\mathrm{L},s_r\}$，利用本文方案，秘密分发者需要为每一个共享秘密 s_1,s_2,L,s_r 随机选定不同的中间秘密 $\{ls_{j1},ls_{j2},\mathrm{L},ls_{jm}\}, j=1,2,\mathrm{L},r$；对应不同的共享秘密，计算 $S_{ji}=ls_{ji}^{\ e} \bmod N, i=1,2,\mathrm{L},m$；根据指定必须参与的集合个数构造 l 及 $(t-l-1)$ 次多项式，公布 $y_i=f(h(ls_i)),i=1,2,\mathrm{L},l$ 和 $y_i=g(h(ls_i)),i=l+1,l+2,\mathrm{L},m$。

每一个参与者 a_{ij} 只需维护一个秘密份额 Sa_{ij}，在合作重构共享秘密的参与者权重之和 $\sum_{j=1}^{n_i} w'_{ij}\geqslant t_i, i=1,2,\mathrm{L},t$ 成立，且指定集合参与的条件下，秘密生成者根据重构算法可以恢复出任意一个对应的共享秘密。根据实际情况，同一个参与者在共享不同秘密时可以具有不同的权重值，方案的灵活性更强，适用范围更广。

4 本文方案分析

4.1 安全性分析

本文方案的安全性主要从以下 4 个方面进行分析：

(1)授权不足的秘密生成者的欺骗。授权不足的秘密生成者或许使用虚假的伪秘密份额欺骗秘密分发者。由于每一个参与者在秘密分发者处存有伪秘密份额的备份，秘密分发者很容易确定合作者的授权是否真实；或许秘密生成者企图利用少于 $(t-l)$ 个满足多项式 $g(x)$ 的点重构 $(t-l-1)$ 阶多项式，或少于 $(l+1)$ 个满足多项式 $f(x)$ 的点重构 l 阶多项式，这等价于破解了 Shamir 的 (t,n) 门限体制，在计算上是不可行的。因此，本文提出的门限共享方案对于未得到足够授权的秘密生成者是安全的。

(2)参与者冒充秘密生成者。根据方案要求，冒充者需要向秘密分发者发送信息 (ID_{DC},R^e_{DC})，由于 R_{DC} 对于其他参与者是保密的，秘密分发者通过解密计算可以识别秘密生成者身份的真伪，从而拒绝配合冒充者完成下一步工作，冒充者无法恢复共享秘密。

(3)秘密份额的重复使用不会影响系统的安全性。假设秘密生成者获得足够的伪秘密份额，并重构了对应的共享秘密 s_u，秘密生成者企图利用得到的信息去重构某些他无权知晓的秘密，如 s_v。根据方案要求，秘密生成者必须拥有对应共享秘密 s_k 的伪秘密份额信息，并且其对应的权值之和不小于于门限值。由于伪秘密份额在产生、传送中都采用加密方式：$R_{uij}=S_{ui}^{\ Sa_{ij}} \bmod N$，$R_{vij}=S_{vi}^{\ Sa_{ij}} \bmod N$，$SR_{vij}=R^e_{vij} \bmod N$，$R^*_{vij}=R_{vij}^{\ e_{DC}} \bmod N$，因此秘密生成者只有试图通过已知的信息推导 R_{vij} 或 Sa_{ij}，这等价于攻破了 RSA 密码体制，在计算上是不可行的，同理，也无法根据 $\{y_i\}$ 推导出有关 d 和 Sa_{ij} 的信息。因此，秘密份额的重复使用不会影响系统的安全性。

(4)抗被动攻击。抗被动攻击要求攻击者无法根据公开信息以及系统中交互的信息推导出共享秘密。本文方案中的公开信息主要为秘密分发者和秘密生成者的公钥信息和 $h(R_{ij})$，交互信息全部采用加密方式。根据 RSA 密码体系的安全性，攻击者无法通过公钥信息推导私钥，也无法通过密文推导加密信息；强哈希函数的性质保证了攻击者既无法通过 $h(R_{ij})$ 推导 R_{ij}，也无法找到伪秘密份额的替代者，因为寻找 $x\neq y$, $h(x)=h(y)$ 在计算上不可行，所以本方案可以抵抗被动攻击。同理，由于算法本身具有的安全性，因此在秘密分发者、参与者和秘密生成者之间无需构建安全信道。

4.2 参与者的动态加入和退出

根据方案的要求，当有新的成员参与共享秘密时，他需要选择自己的秘密份额以及和秘密分发者进行一些信息交互；当新成员参与合作重构共享秘密时，需要将其伪秘密份额加密发送给秘密生成者；当参与者退出共享秘密时，他只需要向秘密生成者发送退出信息，秘密生成者删除对应的伪秘密份额备份即可。因此，本文方案对于参与者的动态加入和退出非常灵活，不需要对方案做任何更改。

5 结束语

本文基于 Shamir 门限方案、RSA 密码体制和哈希函数的特性构建一种参与者有权重的特殊 $(n_1+n_2+\mathrm{L}+n_m,t_1+t_2+\mathrm{L}+t_m,l,t)$ 动态多重秘密共享方案。该方案解决了现实中参与者有权重，重构共享秘密时指定的利益方必须参与的难题，秘密份额选取更方便、安全，且系统无需维持安全信道，更适于现实应用。

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[C]//Proc. of National Computer Conference. New York, USA: AFIPS Press, 1979: 313-3l7.

[3] 庞辽军, 李慧贤, 王育民. 一个安全高效的访问结构上的秘密共享方案[J]. 电子科技大学学报, 2007, 36(5): 827-829.

[4] 刘 佳, 韩文报. 一种安全的公开可验证门限多秘密共享方案[J]. 计算机工程, 2009, 35(1): 24-26.

[5] 李 滨. 基于特殊访问权限的差分秘密共享方案[J]. 四川大学学报: 自然科学版, 2006, 43(1): 78-83.

[6] 张艳硕, 刘卓君, 杜耀刚. 特殊权限下权重不同参与者的广义门限方案[J]. 计算机工程与应用, 2007, 43(17): 15-17.

编辑 陆燕菲