

文章编号:1001-9081(2010)12-3334-03

## 参与者有权重的多重秘密共享方案

王伟<sup>1,2</sup>,周顺先<sup>1,3</sup>

(1. 广州番禺职业技术学院 信息工程学院, 广州 511483; 2. 暨南大学 管理学院, 广州 510632;

3. 湖南大学 软件学院, 长沙 410082)

(wvhhy0101@126.com)

**摘要:**考虑参与者权重不同,基于RSA密码体制和Hash函数的安全性,设计了一种参与者有权重的多重秘密共享方案。方案中,参与者只需维护一个秘密份额,可实现对多个秘密的共享。秘密份额由参与者确定和保管,秘密分发者也不知晓,秘密共享过程中,只需出示伪秘密份额。方案不需要安全信道,算法能够保证信息安全传送,以及验证参与者是否进行了欺骗。分析表明,方案具有更高的安全性和可行性。

**关键词:**秘密共享;门限方案;RSA密码体制;Hash函数

**中图分类号:** TP309 **文献标志码:** A

## Multi-secret sharing scheme among weighted participants

WANG Wei<sup>1,2</sup>, ZHOU Shun-xian<sup>1,3</sup>

(1. School of Information Engineering, Guangzhou Panyu Polytechnic, Guangzhou Guangdong 511483, China;

2. School of Management, Jinan University, Guangzhou Guangdong 510632, China;

3. School of Software, Hunan University, Changsha Hunan 410082, China)

**Abstract:** Based on the security of RSA (Rivest-Shamir-Adleman) cryptosystem and Hash function, a threshold multi-secret sharing scheme with different weights was proposed. In the scheme, each participant can share many secrets with other participants by holding only one secret shadow. Each participant's secret shadow is selected and saved by himself and even the secret dealer does not know anything about it. In the recovery phase, participant only needs to submit a pseudo-shadow instead of his secret shadow. The scheme does not require a secure channel between each participant and the dealer, and can guarantee secure delivery and verify authenticity of information. Analyses show that the scheme is more secure and feasible than the existing ones.

**Key words:** secret sharing; threshold scheme; Rivest-Shamir-Adleman (RSA) cryptosystem; Hash function

## 0 引言

1979年Shamir<sup>[1]</sup>基于Lagrange插值法、Blakley<sup>[2]</sup>基于射影几何理论分别独立提出了 $(t, n)$ 门限秘密共享方案。此后,秘密共享方案得到了进一步的发展<sup>[3-5]</sup>。 $(t, n)$ 秘密共享方案是指在 $n$ 个参与者中共享秘密,任意大于或等于 $t$ 个的参与者可联合重构共享秘密;而少于 $t$ 个的参与者联合不能得到共享秘密的任何信息。传统的门限秘密共享方案要求各参与者的秘密份额都由秘密分发者产生和分配;参与者的秘密份额只能使用一次,当进行新的秘密共享时,必须重新获得秘密份额;参与者权重相同;系统需要在秘密分发者和各参与者之间维护一条安全信道。这些都限制了门限方案在现实中的应用。

文献[6]中基于单向函数提出了一种多级秘密共享方案;文献[7]中基于Shamir的门限方案和RSA(Rivest-Shamir-Adleman)密码体制提出了一个新的门限秘密共享方案。上述方案中参与者只需保存一份秘密份额,便可共享多个秘密,但未涉及参与者权重不同的情况。

在现实中,参与者权重不尽相同。门限方案的核心是参与重构共享秘密的权值之和是否达到门限值,而不仅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[8]中提出了一种基于模运算的加权门限秘密共享方案,文献[9-10]中提出了基于中国剩余定理的参与者权

重不同的秘密共享方案。但上述方案中参与者的秘密份额都必须由秘密分发者产生和分配,同时需要维护一条安全信道。这样会使秘密分发者工作量增大,容易受到攻击,成为安全的瓶颈;且系统即使付出极高的代价,也未必能保证信道安全。

本文基于RSA密码体制和Hash函数构建了一种参与者有权重的多重秘密共享方案。方案中,参与者的权限可以不同,且同一个参与者共享不同秘密时,其权限也可根据实际需要而变动;参与者的秘密份额由自己选择和保存,不对外公开,即使秘密分发者也不知晓;参与者只需维护一个秘密份额,可实现对多个秘密的共享;方案不需要传递任何秘密信息,无需维护安全信道;方案具备防欺骗能力。以上特点能够降低方案实现的复杂度和减少系统付出的代价。

## 1 参与者有权重的多重秘密共享方案

假定 $A = \{a_1, a_2, \dots, a_n\}$ 为参与者集合, $W = \{W_1, W_2, \dots, W_n\}$ 为参与者对应的权值,要求为非负整数; $A$ 的门限值为 $t$ ,所要共享的秘密为 $s$ 。方案中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上发布、更新内容,其他人只能阅读或下载。

方案分为初始化、伪秘密份额的确定和秘密重构三个阶段。

收稿日期:2010-06-11;修回日期:2010-08-06。 基金项目:国家自然科学基金资助项目(60903168)。

作者简介:王伟(1972-),男,陕西三原人,讲师,博士研究生,主要研究方向:信息安全;周顺先(1968-),男,湖南新邵人,副教授,博士,主要研究方向:机器学习。

### 1.1 初始化阶段

在初始化阶段,秘密分发者根据 RSA 密码体制的要求生成自己公钥  $(N, e)$  和私钥  $d$ 。每个参与者确定自己的秘密份额。

1) 秘密分发者随机选取两个大素数  $p$  和  $q$  (均为超过 100 位的十进制数), 计算  $N = pq$ 。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  $ed \equiv 1 \pmod{(p-1)(q-1)}$ ,  $d$  和  $N$  也互素。

3) 秘密分发者确定一个强 Hash 函数  $h(x)$ , 要求  $h(x) \in [0, N]$ 。公开信息  $(N, e, h(x))$ 。

4) 参与者  $a_i$  随机地从  $[2, N]$  中选取一个整数  $Sa_i$  作为自己的秘密份额, 对外保密。

### 1.2 伪秘密份额的确定

参与者根据自己的秘密份额和公开信息计算伪秘密份额, 并发送给秘密分发者。

1) 秘密分发者计算  $S = s^e \pmod N$ , 公开  $S$ 。

2) 参与者  $a_i$  下载公告信息并计算伪秘密份额  $R_i = S^{Sa_i} \pmod N$ , 利用秘密分发者的公钥加密  $SR_i = R_i^e \pmod N$ ,  $a_i$  把  $\{ID_i, W_i, SR_i\}$  发送给秘密分发者,  $ID_i$  为参与者的身份标识。

3) 秘密分发者计算  $R_i = SR_i^d \pmod N$ , 必须确保对于任意两个不同的参与者  $a_i$  和  $a_j$ , 有  $R_i \neq R_j$  成立, 否则, 要求其重新选择秘密份额, 以确保参与者秘密份额的唯一性。同时在公告牌上公布  $\{(ID_i, W_i, h(R_i))\}, i = 1, 2, \dots, n$ 。

### 1.3 秘密的重构

不失一般性, 假设某个参与者集合  $A' = \{a_1, a_2, \dots, a_l\}$  合作准备重构共享秘密  $s$ 。秘密生成者为  $A'$  任意指定的一个参与者。重构过程如下。

1) 秘密生成者根据 RSA 密码体制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)  $A'$  中参与者  $a_i$  从公告牌下载公开信息  $(N_{DC}, e_{DC})$ , 计算  $R'_i = R_i^{e_{DC}} \pmod{N_{DC}}$  并将  $(ID_i, R'_i)$  发送给指定的秘密生成者。

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

4) 秘密生成者在收集到所有伪秘密份额  $\{R_1, R_2, \dots, R_l\}$  后, 查阅公告信息, 计算并判断  $\sum_{i=1}^l W_i \geq t$  是否成立, 若成立则将信息  $\{(ID_i, R_i), \dots, (ID_l, R_l)\}^e \pmod N$  发送给秘密分发者; 否则, 说明参与者集合  $A'$  没有资格重构共享秘密。

5) 秘密分发者解密收到的信息, 在确认参与者授权真实, 并判断  $\sum_{i=1}^l W_i \geq t$  成立的条件下, 计算  $y = (S^d / \prod_{i=1}^l R_i) \pmod N = (S^{d - \sum_{i=1}^l Sa_i}) \pmod N$ , 并将信息  $y^{e_{DC}} \pmod{N_{DC}}$  发送给秘密生成者; 否则发送警告信息。

6) 秘密生成者通过解密运算得到  $y$ , 计算  $y \times \prod_{i=1}^l R_i = y \times \prod_{i=1}^l S^{Sa_i} = S^{d - \sum_{i=1}^l Sa_i} \times \prod_{i=1}^l S^{Sa_i} = S^d \pmod N = s$ , 从而重构得到

共享秘密  $s$ 。

### 1.4 共享多个秘密

在  $n$  个参与者中共享  $r$  个秘密  $s_1, s_2, \dots, s_r$ 。利用本文所提出的方案, 在伪秘密份额确定过程中, 秘密分发者需要为每一个共享秘密  $s_i$  计算并公布对应的  $S_i = s_i^e \pmod N$ , 每一个参与者  $a_i$  只需维护一个秘密份额  $Sa_i$ , 伪秘密份额根据不同的  $S_i$  计算。合作重构共享秘密的参与者权重之和在  $\sum W_i \geq t$  成立的条件下, 可以恢复出任意一个对应的共享秘密, 并且每一个秘密的恢复不会影响其他未被恢复的密码的安全性。方案根据实际情况, 同一个参与者在共享不同秘密时可以有不同的权重值, 方案的灵活性更强, 适用范围更广。

## 2 方案分析

### 2.1 正确性分析

$(t, n)$  门限秘密共享方案的基本要求是: 合作的参与者少于  $t$  个不能重构秘密。本文针对参与者权重不同的情况, 要求其对应的权重之和不小于门限值  $t$ , 才能联合重构共享秘密。秘密分发者判断  $\sum W_i < t$ , 不会配合秘密生成者完成下一步工作, 秘密生成者无法得到恢复共享秘密所需的信息, 无法重构共享秘密。因此本文方案符合  $(t, n)$  门限方案规则。

多重秘密共享要求参与者只需保存一个秘密份额, 可在多个共享秘密中重复使用而不会影响系统的安全性。本文方案中, 参与者  $a_i$  只需维护一个秘密份额  $Sa_i$ , 变更的只是根据不同共享秘密计算的  $S_j = s_j^e \pmod N$ , 伪秘密份额  $R_{ij} = S_j^{Sa_i} \pmod N$  及其对应的  $\{h(R_{ij})\}$ , 根据 RSA 密码体制和强 Hash 函数的安全性, 秘密生成者可重构对应的共享秘密而不会威胁其他的共享秘密的安全性。即参与者的秘密份额  $Sa_i$  可重复使用而不会影响系统的安全性, 符合多重秘密共享方案的要求。

### 2.2 安全性分析

方案的安全性主要从抗假冒攻击、前向安全和抗被动攻击进行分析。

假冒攻击主要分析以下几种情况。

1) 参与者提供虚假的伪秘密份额。根据前文说明, 秘密生成者通过判断  $h(R_i^*) = h(R_i)$  是否成立, 可检验伪秘密份额的真实性。

2) 秘密生成者的欺骗。假设基于某种原因, 秘密生成者不想让授权子集中的某些参与者知道自己想要重构共享秘密, 或者授权子集中的某些参与者不支持其重构共享秘密。由于  $R_i$  只有对应的参与者  $a_i$  和秘密分发者知道, 秘密生成者无法获得足够的授权, 企图根据系统的公开信息来推导出  $R_i$ 。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, 以及  $h(R_i)$ 。基于 RSA 密码体制的安全性, 攻击者无法通过公钥来推导出私钥; 根据强 Hash 函数  $h(x)$  的抗冲突性, 秘密生成者既不可能根据  $h(R_i)$  来推导出  $R_i$ , 也不可能找到  $R_i$  的替代者, 因为寻找  $x \neq y, h(x) = h(y)$  在计算上是不可行的; 或许秘密生成者使用虚假的  $\{(ID_i, R_i), \dots, (ID_l, R_l)\}$  来欺骗秘密分发者, 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, 秘密分发者很容易识别伪秘密份额是否真实, 从而确定秘密生成者是否得到参与者的授权, 试图欺骗秘密分发者是行不通的。因此, 本文方案对于未得到足够授权的秘密生成者是安全的。

3) 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( $ID_{DC}, R_{DC}^e$ ), 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, 从而拒绝公布其公钥, 更不可能配合其提供  $y$  值, 冒充者无法重构出共享秘密。

2.2.1 前向安全性分析

在现实中, 某些已经重构的共享秘密对于非授权者也应该还是保密的。假设秘密生成者获得了足够的伪秘密份额  $\{R_{ij}\}$ ,  $i = 1, 2, \dots, l$ , 并重构了对应的共享秘密  $s_j$ , 秘密生成者企图利用得到的伪秘密份额去重构某些他无权知晓的秘密, 例如  $s_m$ 。根据方案要求, 必须得到对应共享秘密  $s_m$  的伪秘密份额  $\{R_{im}\}$ , 并且其对应的权值之和要不小于门限值。由于  $R_{ij} = S_j^{Sa_i} \bmod N, R_{im} = S_m^{Sa_i} \bmod N$ , 无法通过  $R_{ij}$  来获得  $R_{im}$  的信息。因此只有试图通过已知的  $R_{ij}$  来推导  $Sa_i$ , 进而得到  $R_{im}$ ; 或者根据  $SR_{im} = R_{im}^e \bmod N$  来推导  $R_{im}$ , 这都等价于破解了 RSA 密码体制, 或者说解决了大数分解的数学难题, 在计算上是不可行的。因此, 本文提出的门限共享方案具有前向安全性。

2.2.2 抗被动攻击安全分析

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来推导出共享秘密。基于安全分析中情况 2) 的分析, 攻击者无法根据公开信息获得重构共享秘密所需的有用信息; 而系统中传送的信息为  $SR_i = R_i^e \bmod N, R'_i = R_i^{eDC} \bmod N_{DC}$  和  $y^{eDC} \bmod N_{DC}$ , 其安全性等价于 RSA 密码体制的安全性。因此, 本方案可以抵抗被动攻击。

综上所述, 方案不需要传递任何秘密信息, 系统无需构建安全信道。

2.3 合作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, 需要选择秘密份额, 以及和秘密分发者进行一些信息交互; 当新成员参与重构共享秘密时, 按照算法要求, 需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, 只需向秘密分发者发送退出信息, 秘密分发者删除相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。

2.4 本文方案与文献中方案性能比较

表 1 中性能评价说明如下。

文献[1-4]: 系统需要构造专门的验证算法, 以检验参与者是否进行了欺骗。

文献[5]: 能够识别有欺诈者存在, 但不能确认欺诈者是哪一参与者。

文献[6]: 需要大量计算以预防欺诈, 当恢复最后一个秘密时, 秘密份额会暴露。

文献[7]: 可以验证参与者是否有欺骗行为, 方案针对不同秘密选择不同参数, 具有很强的前向安全性。但攻击者有可能获得  $t$  个伪秘密份额, 结合公开信息重构共享秘密。

文献[8]: 方案未分析秘密份额可否多次使用, 未涉及欺骗验证, 同时, 秘密重构时, 参与者要公布各自的秘密份额。

文献[9]: 可验证参与者是否有欺骗行为, 但伪秘密份额未保护, 攻击者可通过获得  $t$  个伪秘密份额来解密共享秘密。

文献[10]: 未涉及欺骗验证, 秘密重构时, 需要秘密份额参与运算, 安全性较低。

表 1 性能比较

方案	参与者权重	安全信道	秘密份额产生	秘密份额使用	防欺骗能力	前向安全	抗被动攻击
文献[1-4]	无权重	需要	秘密分发者	一次	弱	弱	弱
文献[5]	无权重	需要	秘密分发者	一次	较强	弱	弱
文献[6]	无权重	需要	秘密分发者	多次	一般	一般	一般
文献[7]	无权重	不需要	参与者	多次	强	强	一般
文献[8]	有权重	需要	秘密分发者	*	弱	*	*
文献[9]	有权重	需要	秘密分发者	多次	强	一般	一般
文献[10]	有权重	需要	秘密分发者	多次	弱	弱	弱
本文方案	有权重	不需要	参与者	多次	强	强	强

注: “\*”表示未分析

3 结语

本文基于 RSA 密码体制和 Hash 函数的安全性, 构建了一种参与者有权重的多重秘密共享方案。秘密份额由参与者选择和保存, 秘密共享过程中, 只出示伪秘密份额, 无需安全信道。方案降低了系统实现的复杂度和代价, 更符合现实环境。若参与者权重相同, 方案可退化为普通的门限共享方案。对于指定的组织必须参与秘密重构的需求, 如招投标活动中的招标方, 方案并未考虑, 这将在后续工作中作进一步研究。

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]// Proceedings of the 1979 AFIPS National Computer Conference Monval. New York: AFIPS Press, 1979: 313-317.  
[3] ASMUTH C, BLOOM J. A modular approach to key safeguarding

[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] 许春香, 陈凯, 肖国镇. 安全的矢量空间秘密共享方案[J]. 电子学报, 2002, 30(5): 715-718.  
[6] HARN L. Efficient sharing (broadcasting) of multiple secrets[J]. IEEE Proceedings—Computers and Digital Techniques, 1995, 142(3): 237-240.  
[7] 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.  
[8] 黄东平, 刘铎, 戴一奇. 加权门限秘密共享[J]. 计算机研究与发展, 2007, 44(8): 1378-1382.  
[9] 张艳颖, 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.  
[10] 张艳颖, 刘卓军. 有效的权重不同参与者之间门限多重秘密共享[J]. 计算机工程与设计, 2008, 29(4): 814-815.