

## 动态安全的多级门限多秘密共享方案

邹 惠,王建东

(石家庄经济学院 信息工程学院,石家庄 050031)

(zhfirst11@163.com)

**摘 要:**在已有的多秘密共享方案中,存在只能在同一级门限下共享秘密的限制。基于离散对数问题的难解性,利用二元多项式,给出一种多级门限多秘密共享方案。二元多项式能在不同级门限共享中退化为不同的低阶的二元多项式,实现多级多秘密共享。该方案具有如下特点:在多级门限下共享秘密,在同级门限下可共享任意多个秘密;具有动态安全性,能定时更新成员的子秘密。

**关键词:**多级门限;多秘密共享;离散对数;动态安全

**中图分类号:** TP309.7 **文献标志码:** A

## Multi-level threshold multi-secret sharing scheme with proactive security

ZOU Hui, WANG Jian-dong

(School of Information Engineering, Shijiazhuang University of Economics, Shijiazhuang Hebei 050031, China)

**Abstract:** In multi-secret sharing schemes, the secrets can only be shared in the same level threshold. A multi-level threshold multi-secret sharing scheme based on bivariate polynomial and the intractability of the discrete logarithm was proposed. A bivariate polynomial can degenerate to different lower-order bivariate polynomial according to different thresholds. The scheme has the following characteristics: the secrets can be shared in the multiple level threshold; the multiple secrets can be shared in the same level threshold; the scheme is proactive secure, and the shadow of every participant can be renewed periodically.

**Key words:** multi-level threshold; multi-secret sharing; discrete logarithm; proactive security

### 0 引言

自 1979 年 Shamir 及 Blakley 分别提出门限秘密共享方案后,秘密共享得到了大量的研究。

针对传统方案存在参与者的子秘密只能使用一次的问题,文献[1-4]提出了相关的解决方案,即所谓的多秘密共享方案。这些方案实现了子秘密的反复使用,但只能在同一级门限下共享秘密。文献[5]提出了多级门限多秘密共享方案,此方案基于离散对数和大数分解的困难性,能在多级门限下共享秘密,但该方案却存在子秘密的生命期较长的问题。

利用文献[5]的思想,本文给出一种动态安全的多级门限多秘密共享方案,该方案利用二元多项式,基于离散对数问题的难解性,能在多级门限下共享任意多个秘密;通过子秘密的定时更新,缩短子秘密的生命期,实现动态安全。

### 1 理论基础

**引理 1** 若  $p$  为素数,  $d \mid (p-1)$ , 则阶为  $d$  的最小剩余  $(\text{mod } p)$  的个数为  $\varphi(d)$ 。

**引理 2** 若  $(a, m) = 1, a^n \equiv 1 (\text{mod } m), n > 0$ , 且  $a$  的阶  $(\text{mod } m)$  为  $t$ , 则  $t \mid n$ 。

**定理 1** 若存在  $n$  个不同的大素数  $P_0, P_1, \dots, P_{n-1}$ , 对所有  $i$ , 有  $p_i = (P_i - 1)/2$  也是大素数, 则存在一整数  $g$ , 满足  $g$

模  $N_i$  的阶为  $n_i$ , 其中  $N_i = \prod_{j=0}^i P_j, n_i = \prod_{j=0}^i p_j$ 。

由引理 1 可以看出, 存在整数  $g_i$ , 使得  $g_i$  模  $P_i$  的阶为  $p_i$ ,

$i = 1, 2, \dots, n-1$ 。根据中国剩余定理, 一定存在整数  $g$ , 满足  $g \equiv g_i \text{ mod } P_i$ 。下面证明  $g$  模  $N_i$  的阶为  $n_i$ , 其中  $N_i = \prod_{j=0}^i P_j$ ,

$$n_i = \prod_{j=0}^i p_j。$$

首先证明  $g^{n_i} \equiv 1 \text{ mod } N_i$ , 用数学归纳法。

1) 当  $i = 0$  时,  $n_i = p_0, N_i = P_0, g^{n_i} = g^{p_0} \equiv g_0^{p_0} \equiv 1 \text{ mod } P_0 \circ g^{n_i} \equiv 1 \text{ mod } N_i$  成立。

2) 设当  $i = k$  时,  $g^{n_k} \equiv 1 \text{ mod } N_k$ , 其中  $0 \leq k \leq n-2$ 。

3) 证明当  $i = k+1$  时等式成立。

$$g^{n_{k+1}} - 1 = g^{n_k p_{k+1}} - 1 = (g^{n_k})^{p_{k+1}} - 1 = (t_1 N_k + 1)^{p_{k+1}} - 1 \quad (1)$$

$$g^{n_{k+1}} - 1 = g^{n_k p_{k+1}} - 1 = (g^{p_{k+1}})^{n_k} - 1 = (t_2 P_{k+1} + 1)^{n_k} - 1 \quad (2)$$

由式(1)(2)可看出,  $g^{n_{k+1}} - 1$  分别能被  $N_k$  和  $P_{k+1}$  整除。因为  $N_k$  与  $P_{k+1}$  互素, 故  $g^{n_{k+1}} - 1$  能被  $N_k P_{k+1} = N_{k+1}$  整除。即:

$$g^{n_{k+1}} \equiv 1 \text{ mod } N_{k+1} \quad (3)$$

由 1)~3) 得出, 当  $0 \leq i \leq n-1$  时,  $g^{n_i} \equiv 1 \text{ mod } N_i$  成立。

利用引理 2, 采用数学归纳法, 可进一步证出  $n_i$  是  $g$  模  $N_i$  的阶。

### 2 方案构成

#### 2.1 系统建立

设  $U = \{U_1, U_2, \dots, U_n\}$  是  $n$  个参与者的集合, Dealer 负

负责秘密的分发及更新。方案中有  $l$  级门限,分别为  $t_1, t_2, \dots, t_l$ 。

Dealer 进行如下工作:

1) 选定  $l+1$  个不同的大素数  $P_0, P_1, \dots, P_l$ , 对所有  $i$ , 有  $p_i = (P_i - 1)/2$  也是大素数。令  $N_i = \prod_{j=0}^i P_j, n_i = \prod_{j=0}^i p_j (i = 1, 2, \dots, l)$ 。选取一整数  $g$ , 使得  $g$  模  $N_i$  的阶为  $n_i$ 。

2) 随机选取  $m$  个正整数  $c_{0j} (0 \leq j \leq m-1)$ , 满足  $c_{0j} \bmod n_i \neq 0 (i = 1, 2, \dots, l)$ 。

3) 随机选择  $t_1 \times m$  个正整数  $c_{ij}^{(0)} \in Z_{n_i} (0 \leq r \leq t_1 - 1, 0 \leq j \leq m-1)$ , 对  $i = 1, 2, \dots, l-1, j = 0, 1, \dots, m-1$ , 按如下方式选择  $c_{i,j}^{(0)}, c_{i+1,j}^{(0)}, \dots, c_{i+1-1,j}^{(0)}$ :

$$c_{ij}^{(0)} \equiv b_{ij}^{(0)} \times n_i \bmod n_i \quad (4)$$

其中  $b_{ij}^{(0)}$  为任意整数,  $r = t_i, t_i + 1, \dots, t_{i+1} - 1$ 。

4) 定义二元多项式:

$$f^{(0)}(x, y) = \sum_{i=0, j=0}^{i=t_l-1, j=m-1} c_{ij}^{(0)} x^i y^j \quad (5)$$

计算并公布  $C_{ij}^{(0)} (i = 0, 1, \dots, t_l - 1, j = 0, 1, \dots, m-1)$ , 其中:

$$C_{ij}^{(0)} = g^{c_{ij}^{(0)}} \bmod N_i \quad (6)$$

5) 计算:

$$\alpha_r^{(0)}(y) = f^{(0)}(ID_r, y) = \sum_{j=0}^{m-1} d_{ij}^{(0)} y^j \bmod n_i \quad (7)$$

其中  $d_{ij}^{(0)} = \sum_{i=0}^{t_l-1} c_{ij}^{(0)} (ID_r)^i$ 。

将  $\alpha_r^{(0)}(y)$  秘密地发送给每个参与者  $U_r$ 。每个参与者  $U_r$  收到子秘密后,通过下式验证收到子秘密的正确性。

$$g^{d_{ij}^{(0)}} = \prod_{i=0}^{t_l-1} C_{ij}^{(0)} (ID_r)^i; j = 0, 1, 2, \dots, m-1 \quad (8)$$

## 2.2 子秘密的定期更新

在时间标志  $\beta = 1, 2, 3, \dots$ , Dealer 做如下工作:

1) 随机选择  $t_1 \times m$  个正整数  $\Delta c_{ij}^{(\beta)} \in Z_{n_i} (0 \leq r \leq t_1 - 1, 0 \leq j \leq m-1)$ , 对  $i = 1, 2, \dots, l-1, j = 0, 1, \dots, m-1$ , 按如下方式选择  $\Delta c_{i,j}^{(\beta)}, \Delta c_{i+1,j}^{(\beta)}, \dots, \Delta c_{i+1-1,j}^{(\beta)}$ :

$$\Delta c_{ij}^{(\beta)} \equiv \Delta b_{ij}^{(\beta)} \times n_i \bmod n_i \quad (9)$$

其中  $\Delta b_{ij}^{(\beta)}$  为任意整数,  $r = t_i, t_i + 1, \dots, t_{i+1} - 1$ 。

2) 定义二元多项式:

$$\Delta f^{(\beta)}(x, y) = \sum_{i=0, j=0}^{i=t_l-1, j=m-1} \Delta c_{ij}^{(\beta)} x^i y^j \quad (10)$$

计算  $C_{ij}^{(\beta)} (i = 1, 2, \dots, t_l - 1, j = 0, 1, \dots, m-1)$  和  $\Delta \alpha_r^{(\beta)}(y)$ :

$$C_{ij}^{(\beta)} = C_{ij}^{(\beta-1)} g^{\Delta c_{ij}^{(\beta)}} \bmod N_i \quad (11)$$

$$\Delta \alpha_r^{(\beta)}(y) = \Delta f^{(\beta)}(ID_r, y) = \sum_{j=0}^{m-1} \Delta d_{ij}^{(\beta)} y^j \bmod n_i \quad (12)$$

其中  $\Delta d_{ij}^{(\beta)} = \sum_{i=0}^{t_l-1} \Delta c_{ij}^{(\beta)} (ID_r)^i$ 。

3) 将  $\Delta \alpha_r^{(\beta)}(y)$  秘密地发送给每个参与者  $U_r$ 。公布  $C_{ij}^{(\beta)} (i = 1, 2, \dots, t_l - 1, j = 0, 1, \dots, m-1)$ , 删除  $C_{ij}^{(\beta-1)} (i = 1, 2, \dots, t_l - 1, j = 0, 1, \dots, m-1)$ , 每个参与者  $U_r$  收到子秘密后,验证收到子秘密的正确性。按照下式更新子秘密并销毁  $\alpha_r^{(\beta-1)}$ :

$$\alpha_r^{(\beta)} = \alpha_r^{(\beta-1)} + \Delta \alpha_r^{(\beta)} \quad (13)$$

## 2.3 秘密的共享

设要共享的秘密集合为  $\{k_{t_1,1}, k_{t_1,2}, \dots, k_{t_i,j}, \dots, k_{t_l,s}\}$ 。  $\xi (\xi = 0, 1, 2, \dots)$  次定期更新后, Dealer 任意选择一整数  $e$ , 计算:

$$T_{t_i,j} = k_{t_i,j} - f^{(\beta)}(0, e); \quad i = 1, 2, \dots, l, j = 1, 2, \dots, s \quad (14)$$

并公布  $e$  和  $T_{t_i,j}$ 。

## 2.4 秘密的恢复

1)  $\xi (\xi = 0, 1, 2, \dots)$  次定期更新后, 设要恢复门限为  $t_i$  的共享秘密, 每个参与者计算并出示  $A_{r,t_i}^{(\xi)} = \alpha_r^{(\xi)}(e) \bmod n_i$ 。

2) 其他参与者通过下式验证  $P_i$  提供子秘密的正确性:

$$g^{A_{r,t_i}^{(\xi)}} \equiv \prod_{i=0, j=0}^{i=t_l-1, j=m-1} C_{ij}^{(\xi)} (ID_r)^{i \otimes j} \bmod N_i \quad (15)$$

3) 通过下式恢复共享秘密:

$$k_{t_i,j} = T_{t_i,j} + \sum_{r=0}^{t_i-1} A_{r,t_i}^{(\xi)} h_r \bmod n_i \quad (16)$$

其中  $h_r = \prod_{j=1, j \neq r}^{t_i} \frac{(-ID_j)}{ID_r - ID_j}$ 。

## 3 性能分析

### 3.1 正确性分析

定理2  $\xi$  次定期更新后, 参与者出示的信息  $A_{r,t_i}^{(\xi)}$  是由正确子秘密计算所得的必要条件为公式  $g^{A_{r,t_i}^{(\xi)}} \equiv \prod_{i=0, j=0}^{i=t_l-1, j=m-1} C_{ij}^{(\xi)} (ID_r)^{i \otimes j} \bmod N_i$  成立。

证明 因为参与者出示的信息  $A_{r,t_i}^{(\xi)}$  是由正确子秘密计算所得, 所以:

$$\alpha_r^{(\xi)}(e) = f^{(\xi)}(ID_r, e) = \sum_{j=0}^{m-1} d_{ij}^{(\xi)} e^j \bmod n_i \quad (17)$$

又因为  $n_i \mid n_i$ , 故  $\alpha_r^{(\xi)}(e) \bmod n_i = \sum_{j=0}^{m-1} d_{ij}^{(\xi)} e^j \bmod n_i$ 。

$$g^{A_{r,t_i}^{(\xi)}} = g^{\alpha_r^{(\xi)}(e) \bmod n_i} = g^{\sum_{j=0}^{m-1} d_{ij}^{(\xi)} e^j \bmod n_i} = \sum_{i=0, j=0}^{i=t_l-1, j=m-1} c_{ij}^{(\xi)} (ID_r)^{i \otimes j} \bmod n_i \quad (18)$$

$$\prod_{i=0, j=0}^{i=t_l-1, j=m-1} C_{ij}^{(\xi)} (ID_r)^{i \otimes j} = \prod_{i=0, j=0}^{i=t_l-1, j=m-1} g^{c_{ij}^{(\xi)} (ID_r)^{i \otimes j}} = \sum_{i=0, j=0}^{i=t_l-1, j=m-1} c_{ij}^{(\xi)} (ID_r)^{i \otimes j} \bmod N_i \quad (19)$$

$$g^{A_{r,t_i}^{(\xi)}} \equiv \prod_{i=0, j=0}^{i=t_l-1, j=m-1} C_{ij}^{(\xi)} (ID_r)^{i \otimes j} \bmod N_i$$

定理3  $\beta$  时刻, 在保证各参与者提供正确子秘密参数信息  $A_{r,t_i}^{(\xi)}$  的情况下, 汇集  $t_i$  个参数  $A_{r,t_i}^{(\xi)}$ , 即可恢复共享秘密  $k_{t_i,j}$ 。

证明 设  $h_r = \prod_{j=1, j \neq r}^{t_i} \frac{(-ID_j)}{ID_r - ID_j}$ , 则:

$$\sum_{r=0}^{t_i-1} A_{r,t_i}^{(\xi)} h_r = \sum_{r=0}^{t_i-1} f^{(\xi)}(ID_r, e) h_r \bmod n_i \quad (20)$$

根据多项式  $f^{(\xi)}(x, y)$  系数特点, 可得:

$$\sum_{r=0}^{t_i-1} f^{(\xi)}(ID_r, e) h_r \bmod n_i = f^{(\xi)}(0, e) \quad (21)$$

$t_i$  个参数  $A_{r,t_i}^{(\xi)}$ , 即可恢复共享秘密  $k_{t_i,j}$ , 具体过程如下:

$$k_{t_i,j} = T_{t_i,j} + \sum_{r=0}^{t_i-1} A_{r,t_i}^{(\xi)} h_r \bmod n_i \quad (22)$$

(下转第 2232 页)

带参数的 URL 定义为变量 myurl), `<a href = "{mySec;secURL(vurl,request)}">`(注:使用 myurl)。

标签化和 3.1 节所述普通的部署方式是等效的,代码更规范简洁。

### 3.3 权限管理

权限管理的扩展很简单。按照 RBAC 的方式,细化到按钮进行权限配置,并记录在数据库里。实际的权限控制,仍然是改动 URL。

非权限控制点的 URL 可以忽略,需要进行权限控制的点,URL 里加入“&ACT = xxx”,其中 ACT 是验证过滤器检测权限的保留字,xxx 为某种权限,按图 3 的算法对用户、基址和权限进行审核。如“`<a href = "{mySec;secURL('a.jsp?ID=1',request)}">`编辑`</a>`”变成权限控制点后,将改写为“`<a href = "{mySec;secURL('a.jsp?ID=1&ACT=edit',request)}">`编辑`</a>`”。如果运行时用户没有此权限,“编辑”将成为一个空链接。

### 3.4 运行结果

在实际运用中,采用 64 位鉴别码,为方便使用,鉴别码在 URL 内作为 auth 参数的值,原始目标链接为“set\_sta.jsp?ID=102”时,生成的安全链接为:“set\_sta.jsp?ID=102&auth=45c83a25b6dbb7f23016e10aba05bed051dbaf29b938557aa02feaff0234eb788e62d”。

经测试,安全链接对于 struts 框架的页面定向(mapping.findForward),JSP 的服务器端重定向(jsp:forward)、服务器端包含(jsp:include)均完全支持,这些 URL 无需更改。

### 3.5 AJAX 兼容

有些 AJAX 代码在客户端运行,只有运行时才能确定 URL,这会被视为“篡改”,为了兼容这一点,验证算法略作调整,以 auth 名值对为界,将安全链接分为定址和变址两部分,定址参与鉴别码生成,变址部分不参与,从而允许客户端脚本

临时修改和使用。如“view\_sta.jsp?ID=102&auth=45c...34b86220&page=1&style=2”中,“page=1&style=2”为客户端脚本生成的变址,为了系统的安全,将不太重要的参数放在变址里。

## 4 结语

安全链接方法的算法代码集中,可以独立为一个生成类(class)和一个验证过滤器(filter),实际应用只需要按照规则改写需要进行安全控制的 URL,并非常便利地结合权限管理,这在开发过程中可以逐步完成,因而对于软件工程来说是实用的。在部署后,白名单之外的所有 URL 都被嵌入了鉴别码,此鉴别码无法伪造,有效防止了 URL 的篡改,从而能阻止 SQL 注入和部分 XSS 攻击,尤其是难以防范的语义 URL 攻击,极大地提高了软件系统的安全。同时,无需额外的代码,就能够提高权限管理的粒度,统一规范的接口和流程,提高了大型管理系统的开发效率。

### 参考文献:

- [1] 刘繁艳,姜瑜. SQL 注入攻击研究[J]. 中国科技信息, 2005(17): 89.
- [2] 古开元,周安民. 跨站脚本攻击原理与防范[J]. 网络安全技术与应用, 2005(12): 19-21.
- [3] 林晶,黄青松,张晶. 基于改进 MD5 算法的数据篡改检测方法[J]. 计算机工程与应用, 2008, 44(33): 148-150.
- [4] 黄箐,马德山,项链. 基于角色的安全登录框架设计与实现[J]. 西北民族大学学报: 自然科学版, 2008, 29(1): 33-39.
- [5] 芦斌,罗向阳,刘粉林. 一种基于混沌的软件水印算法框架及实现[J]. 软件学报, 2007, 18(2): 351-360.
- [6] 徐兵,谢仕义. Web 应用程序会话安全模块的设计[J]. 计算机工程, 2008, 34(19): 176-178.
- [7] 曹勇刚,金茂忠,刘超. CMS 中 RBAC 模型的改造和应用[J]. 北京航空航天大学学报, 2005, 31(10): 1153-1158.

(上接第 2219 页)

### 3.2 安全性分析

1) 在子秘密的分发和更新过程中,公布了消息  $C_y^{(\xi)}$  ( $\xi = 0, 1, 2, \dots$ ), 其中  $C_y^{(\xi)} = g_y^{c^{(\xi)}} \bmod N_l$ , 基于求解有限域上的离散对数问题的难解性,由公开信息不可能求出  $c_y^{(\xi)}$ 。

2) 参与者收到子秘密及更新信息后,将分别通过公式验证子秘密和更新信息的正确性,防止了 Dealer 欺诈;各参与者示包含子秘密的参数信息  $A_{r,t_i}^{(\xi)}$  时,也通过公式验证出示参数的正确性,有效防止了参与者之间的欺诈。

3) 子秘密的定期更新解决了子秘密的生命期较长的问题。攻击者必须在子秘密的更新周期内获得  $t$  个或  $t$  个以上的子秘密,这势必增加攻击的难度,实现了动态安全。

4) 基于 Shamir 方案的安全性,在秘密恢复前的子秘密验证过程中,由公开信息  $A_{r,t_i}^{(\xi)}$ , 不能求出用户子秘密的相关信息;通过已恢复的秘密不能得到另一个秘密,即由  $f^{(\beta)}(0, e)$ , 不可能求出  $f^{(\beta)}(0, e')$ , 其中  $e \neq e'$ 。

## 4 结语

本文给出了动态安全的多级门限多秘密共享方案。方案的安全性依赖离散对数问题的难解性,能实现对不同门限值的多个秘密的共享,有效防止 Dealer 欺诈及参与者之间的欺诈。通过定期更新子秘密,实现了动态安全,增强了系统的安

全性。

### 参考文献:

- [1] HARN L. Efficient sharing (Broadcasting) of mutiple secrets[J]. IEE Proceedings - Computers Digital Techniques, 1995, 142(3): 237-240.
- [2] CHEN L, COLLMANN D, MITCHELL C J, et al. Secret sharing with reusable polynomials [C]// The Second Australasian Conference on Information Security and Privacy: ACISP' 97. Berlin: Springer-Verlag, 1997: 183-192.
- [3] 许春香,肖国镇. 门限多重秘密共享方案[J]. 电子学报, 2004, 32(10): 1688-1689.
- [4] 吴开贵,刘东,冯永. 基于椭圆曲线的门限多重秘密共享方案[J]. 计算机科学, 2006, 33(3): 97-98.
- [5] 黄东平,刘铎,戴一齐. 安全的多级门限多秘密共享[J]. 清华大学学报, 2007, 47(4): 592-594.
- [6] CHANG T Y, HWANG M S, YANG W P. An improvement on the Lin-Wu(t, n) threshold verifiable multi-secret sharing scheme [J]. Applied Mathematics and Computation, 2005, 166(1): 1-14.
- [7] 康斌,余昭平. 一个基于椭圆曲线的多重秘密共享体制[J]. 计算机工程, 2007, 33(13): 176-178.
- [8] 张燕燕. 一种动态安全的多重密钥门限共享方案[J]. 计算机工程与应用, 2007, 43(34): 156-158.