

文章编号:1001-9081(2016)04-0952-04

DOI:10.11772/j.issn.1001-9081.2016.04.0952

## 基于 Birkhoff 插值的可验证多等级秘密共享算法

许晓洁<sup>1,2\*</sup>, 王力生<sup>1</sup>

(1. 同济大学 电子与信息工程学院, 上海 201804; 2. 上海师范大学 天华学院, 上海 201815)

(\*通信作者电子邮箱 [lilili\\_124@163.com](mailto:lilili_124@163.com))

**摘要:**分布式密钥生成(DKG)协议是分布式加密系统的重要组成部分,其允许一群参与者共同产生私钥和公钥,但只有授权的参与者子集才能重构私钥。然而,现有的基于 DKG 协议均是假定参与者等级相同。为此,提出基于 Birkhoff 插值的可验证多等级秘密共享 BI-VHTSS 算法。BI-VHTSS 算法考虑了 DKG 问题,并由等级门限访问结构定义授权子集。利用 Birkhoff 插值和离散对数问题,验证了 BI-VHTSS 算法的正确性和安全性。

**关键词:**可验证; 多等级; Birkhoff 插值; 门限秘密共享

**中图分类号:**TP393    **文献标志码:**A

### Birkhoff interpolation-based verifiable hierarchical threshold secret sharing algorithm

XU Xiaojie<sup>1,2\*</sup>, WANG Lisheng<sup>1</sup>

(1. College of Electronics and Information Engineering, Tongji University, Shanghai 201804, China;

2. Tianhua College, Shanghai Normal University, Shanghai 201815, China)

**Abstract:** A Distributed Key Generation (DKG) protocol is a central component in distributed cryptosystems, it allows a group of participants to jointly generate private key and public key, but only authorised subgroups of participants are able to reconstruct private key. However, the existing literatures based on DKG protocol assume equal authority for participants. Therefore, Birkhoff Interpolation-based Verifiable Hierarchical Threshold Secret Sharing (BI-VHTSS) algorithm was proposed. Considering the problem of DKG, authorized subsets were defined by a hierarchical threshold access structure in BI-VHTSS algorithm. On the basis of intractability of the Discrete Logarithm Problem (DLP) and Birkhoff interpolation, the correctness and security of the proposed algorithm were also proved.

**Key words:** verifiable; hierarchical; Birkhoff interpolation; threshold secret sharing

## 0 引言

分布式密钥生成(Distributed Key Generation, DKG)协议是分布式加密系统的重要组成部分,与密码系统的安全性息息相关。在 DKG 协议中,多个参与者依据预先设定的加密系统,共同合作生成公钥和私钥,并且无需任何可信任体。生成的公钥以公开的形式输出,而私钥被参与者按照某一秘密分享方案所分享<sup>[1]</sup>。这一被分享的私钥以后可用于面向群体的密码系统,如群体签名或群体解密等。

所谓秘密共享就是秘密分发者 Dealer 把一个秘密  $s$  分割成  $s_1, s_2, \dots, s_n$ , 形成  $n$  份, 每一份称为份额; 然后, 再秘密地给每一个参与者分发一份份额。授权子集中的所有参与者分享自己所接到的份额,再合作恢复秘密  $s$ 。文献[1–2]提出基于门限秘密共享方案。在  $(t, n)$  门限方案中,任意  $t$  个或以上的参与者合作可恢复秘密<sup>[3]</sup>。

文献[2]提出了基于可验证门限秘密共享(Verifiable Threshold Secret Sharing, VTSS)的 DKG 协议,记为  $(t, n)$ -TDKG(Threshold-DKG),其基本思想就是并行执行  $n$  次 VTSS 协议。文献[4–10]对  $(t, n)$ -TDKG 协议进行了修改,但是这些修改协议并未保证产生的公钥均匀分布。

目前,DKG 协议的主要问题在于假定所有参与者的等级相同。然而,这个假设存在欠缺。在特定情况下,参与者有不同的等级。例如,某公司的管理层,有 12 位管理人员,将他们分为三个等级:3 位最高级,3 人中级,余下的 6 人第三级。基于这个等级划分,使用普通的门限签名方案,并给所有管理者在签署文件时相同的权限是不明智的,应该是不同等级的管理人员具有不同的签署文件权。

显然, $(t, n)$  门限秘密共享中,所有的参与者权限相同,无等级区分。而实现生活中,参与者可能因权利、级别等不同,参与者通常是不对等,并且具有等级划分。通常依据权限的不同,将参与者划分为不同等级的参与者集合。为此,研究人员提出了多等级门限秘密共享策略,其旨在解决具有多等级访问结构的秘密共享问题<sup>[3]</sup>。

Simmons<sup>[11]</sup> 和 Birckell<sup>[12]</sup> 均提出了或结构的多等级门限秘密共享策略。在或结构中,等级高的参与者可以完全被等级低的用户代替,即:在只有等级低的参与者参与的情况下,只要等级低的参与者足够多,就可以恢复秘密。此外 Ghodosi 等<sup>[13]</sup> 提出了基于门限秘密共享扩展的理想的或结构  $(t, n)$  策略。

或结构的门限策略对访问结构的构成要求较低。相比之

收稿日期:2015-09-02;修回日期:2015-10-30。

基金项目:国家 863 计划项目(2013AA040302);上海经信委重大技术装备研制专项(ZB-ZBYZ-03-12-1067-1,沪 CXY-2014-006)。

作者简介:许晓洁(1982—),男,讲师,博士,主要研究方向:计算机体系结构、嵌入式系统、信息安全、可信计算; 王力生(1957—),男,教授,博士生导师,主要研究方向:计算机体系结构、嵌入式系统、可信计算、多线程并行计算。

下,与结构的门限策略对访问结构的成员构成要求更苛刻<sup>[10]</sup>。在或结构中,参与者集合只要满足所有门限要求中的某一条要求,该子集就是合格子集;而与结构中,参与者集合必须满足所有门限要求,才能成为合格子集。Tassa 等<sup>[14]</sup>提出了与结构的多等级门限秘密共享策略,利用对多项式的求导,获取不同等级参与者的秘密份额;Basu 等<sup>[7]</sup>提出了一种安全多等级门限秘密策略;Tentu 等<sup>[8]</sup>提出了基于最大距离可分码的多等级门限秘密共享策略,然而,这些方案均假设参与者是可信的、诚实的。

在现实生活中,某些参与者可能篡改自己的份额,对系统发起攻击,或者不合作。使得系统无法恢复秘密。为此,本文结合多等级门限秘密共享策略,提出基于 Birkhoff 插值的可验证的多等级门限秘密共享(Birkhoff Interpolation-based Verifiable Hierarchical Threshold Secret Sharing, BI-VHTSS)算法。BI-VHTSS 算法引用了与结构,提高进入授权子集要求;同时,给参与者设定不同等级划分,不同等级的参与者具有不同的门限值。最后,利用离散对数的困难性,保证了 BI-VHTSS 算法的正确性和安全性。

## 1 预备知识

假定  $U = \{P_1, P_2, \dots, P_n\}$  是  $n$  个参与者的子集,这些参与者被划分为  $m$  等级  $U_1, U_2, \dots, U_m$ 。假定处于  $U_1$  级内的参与者表示为  $P_1, P_2, \dots, P_{|U_1|}$ ;相应地,处于  $U_2$  级内的参与者表示为  $P_{|U_1|+1}, \dots, P_{|U_1|+|U_2|}$ 。其中:  $|U_i|$  表示  $U_i$  等级内参与者的个数。

假定门限值要求的序列  $1 < t_1 < \dots < t_m$  决定等级门限访问结构。 $p, q$  为两个大素数,且  $q/(p-1)$  为素数。 $G = \langle g \rangle$  是  $\mathbf{Z}_p^*$  域内  $q$  阶元素的子群。为了满足插值问题的适定性,素数  $q$  也必须满足式(1)<sup>[15]</sup>:

$$q > 2^{-t+2} \cdot (t-1)^{(t-2)/2} \cdot (t-1)! \cdot n^{(t-1)(t-2)/2} \quad (1)$$

此外,令  $h$  是  $G$  内元素,致使计算以  $g$  为底的离散对数是不可行的。

**定义 1 访问结构<sup>[3]</sup>。**

$U = \{P_1, P_2, \dots, P_n\}$  是  $n$  个参与者的集合,  $\Gamma \subseteq 2^U$  表示由参与者集合  $U$  的非空子集构成的集合。若  $\Gamma$  由所有可以恢复秘密的参与者子集组成,则  $\Gamma$  被称为集合  $U$  上的访问结构。其中  $\Gamma$  中的子集称为授权子集(或合格子集)。

**定义 2 与结构的  $(t, n)$  多等级门限访问结构<sup>[3]</sup>。**

$U = \{P_1, P_2, \dots, P_n\}$  是  $n$  个参与者的集合,且有  $m$  个等级构成。若  $1 \leq i \leq j \leq m$  时,  $U = \bigcup_{i=1}^m U_i$ ,  $U_i \cap U_j = \emptyset$ , 门限序列为  $1 < t_1 < \dots < t_m$ 。如果满足下列条件,则  $\Gamma$  称为与结构的  $(t, n)$  多等级门限访问结构:

$$\Gamma = \left\{ V \subset U : \left| V \cap \left( \bigcup_{j=1}^i U_j \right) \right| \geq t_i; \forall i \in \{1, 2, \dots, m\} \right\}$$

## 2 Birkhoff 插值法

由于在 BI-VHTSS 算法的秘密重构以及证明完备性过程中需要使用 Birkhoff 插值,为此本章简要描述 Birkhoff 插值的基础知识<sup>[7]</sup>。首先定义一个三元组  $\langle X, E, C \rangle$ ,其中  $X, E, C$  定义如下:

$X = \{x_1, x_2, \dots, x_k\}$  是实数域  $\mathbf{R}$  内的一组给定数,且  $x_1 <$

$x_2 < \dots < x_k$ 。

$E = (e_{i,j})_{1 \leq i \leq k, 0 \leq j \leq l}$  为二进制插值矩阵,  $I(E) = \{(i, j) : e_{i,j} = 1\}$ , 并且令  $N = |I(E)|$  (假定矩阵  $E$  中最右列是非零的)。

$C = \{c_{i,j} : (i, j) \in I(E)\}$  为  $N$  个实数构成的集合。

对于特定的三元组  $\langle X, E, C \rangle$ , Birkhoff 插值问题就是寻找一个多项式  $P(x) \in R_{N-1}[x]$ , 其满足式(2) 所示的  $N$  个等式:

$$P^{(j)}(x_i) = c_{i,j}; \quad (i, j) \in I(E) \quad (2)$$

其中:  $P^{(j)}(\cdot)$  是  $P(x)$  的  $j$  阶导数,  $R_{N-1}[x]$  是不大于  $N-1$  阶的所有可能多项式集合。

接下来,论述 Birkhoff 插值的具体细节。

设定  $\varphi = \{g_0, g_1, \dots, g_{N-1}\}$  为一个线性独立系统。 $I'(E) = \{\alpha_i : i = 1, 2, \dots, N\}$  由  $I(E)$  按降序排序的矢量。 $\alpha_i(1)$  和  $\alpha_i(2)$  分别表示  $\alpha_i \in I'(E)$  中的第一个、二个元素。此外,定义矢量  $C' = \{c'_i : i = 1, 2, \dots, N\}$ 。

利用  $E, X, \varphi$  能够解决 Birkhoff 插值问题:

$$P(x) = \sum_{j=0}^{N-1} \frac{|A(E, X, \varphi_j)|}{|A(E, X, \varphi)|} g_j(x) \quad (3)$$

其中:  $|\cdot|$  为行列式运算。

$$A(E, X, \varphi) = \begin{bmatrix} g_0^{(\alpha_1(2))}(x_{\alpha_1(1)}) & g_1^{(\alpha_1(2))}(x_{\alpha_1(1)}) & \dots & g_{N-1}^{(\alpha_1(2))}(x_{\alpha_1(1)}) \\ g_0^{(\alpha_2(2))}(x_{\alpha_2(1)}) & g_1^{(\alpha_2(2))}(x_{\alpha_2(1)}) & \dots & g_{N-1}^{(\alpha_2(2))}(x_{\alpha_2(1)}) \\ \vdots & \vdots & \ddots & \vdots \\ g_0^{(\alpha_N(2))}(x_{\alpha_N(1)}) & g_1^{(\alpha_N(2))}(x_{\alpha_N(1)}) & \dots & g_{N-1}^{(\alpha_N(2))}(x_{\alpha_N(1)}) \end{bmatrix} \quad (4)$$

对式(3) 进行变换,可得:

$$P(x) = \sum_{j=0}^{N-1} \sum_{i=0}^{N-1} (-1)^{(i+j)} c'_{i+1} \frac{|A_i(E, X, \varphi_j)|}{|A(E, X, \varphi)|} g_j(x) \quad (5)$$

其中: 删除  $A(E, X, \varphi)$  第  $(i+1)$  行和第  $(j+1)$  列便可得到  $A_i(E, X, \varphi_j)$ 。依据式(5) 可知:

$$P(0) = \sum_{j=0}^{N-1} \sum_{i=0}^{N-1} (-1)^{(i+j)} c'_{i+1} \frac{|A_i(E, X, \varphi_j)|}{|A(E, X, \varphi)|} g_j(0) \quad (6)$$

令  $\varphi = \{g_0(x) = 1, g_1(x) = x, \dots, g_{N-1}(x) = x^{N-1}\}$ , 则  $g_0(0) = 1, g_j(0) = 0, 1 \leq j \leq N-1$ 。据此,便可计算  $P(0)$ :

$$P(0) = \sum_{j=0}^{N-1} (-1)^{(i)} c'_{i+1} \frac{|A_i(E, X, \varphi_0)|}{|A(E, X, \varphi)|} = \sum_{i=0}^{N-1} c'_{i+1} \left[ (-1)^{(i)} \frac{|A_i(E, X, \varphi_0)|}{|A(E, X, \varphi)|} \right] \quad (7)$$

## 3 BI-VHTSS 算法

### 3.1 系统建立

分发者选择  $p, q$  两个大素数,  $g$  为  $\mathbf{Z}_p^*$  中一个  $q$  阶元,且在  $\mathbf{Z}_p^*$  内计算以  $g$  为底的离散对数是不可能的;分发者公布参数  $p, q, g$ 。

### 3.2 私钥产生

步骤 1 每个参与者  $P_i \in U$  随机选择系数  $\{a_{ij}\}_{j=0}^{t-1}$  和  $\{b_{ij}\}_{j=0}^{t-1}$ , 并构建两个多项式:

$$f_i(x) = a_{i0} + a_{i1}x + \dots + a_{i(t-1)}x \pmod{q} \quad (8)$$

$$f'_i(x) = b_{i0} + b_{i1}x + \dots + b_{i(t-1)}x \pmod{q} \quad (9)$$

步骤 2 广播  $\{C_{ij} = g^{a_{ij}} h^{b_{ij}} \pmod{p}\}_{j=0}^{t-1}$ 。

步骤 3 参与者  $P_i \in U$  为每个参与者  $P_j \in U$  计算份额:  $(sh_{i-j} = f_i^{(t_k-1)}(j), sh'_{i-j} = f'_i^{(t_k-1)}(j))$

步骤 4 参与者  $P_i \in U$  给每个参与者传输  $P_j \in U$  份额。由于提出的 BI-VHTSS 方案具有可验证性, 若在传输份额中出现错误, 那错误的份额将无法通过验证, 因此可认为传输通道是安全的。

### 3.3 份额验证

为了保证收到的份额的有效性, 参与者  $P_j \in U$  对所接收的份额进行验证。

步骤 1 参与者  $P_i \in U$  检测自己的份额是否满足式(10):

$$g^{sh_{i-j}} h^{sh'_{i-j}} = \prod_{l=0}^{t-1} C_l^{e^{(t_k-1)(j)}} \pmod{p} \quad (10)$$

其中:  $g_i^{(t_k-1)}(j)$  是  $g_i(x) = x^i$  在  $x = j$  的  $t_{k-1}$  阶导数。

步骤 2 如果不满足式(10), 参与者  $P_j$  就向  $P_i$  投诉。

步骤 3 一旦收到投诉,  $P_i$  就广播满足式(10)的  $(sh_{i-j}, sh'_{i-j})$ 。

步骤 4 如果以下任何一种情况发生,  $P_i$  就标记不合格:

1) 接收了  $t$  个或以上的投诉; 2) 应答投诉时, 广播的  $(sh_{i-j}, sh'_{i-j})$  仍不满足式(11)。

步骤 5 每个参与者建立自己的合格子集 QUPS (Qualified Participants Set)。

步骤 6 参与者  $P_i$  计算自己的份额:  $sh_i = \sum_{j \in QUPS} sh_{j-i} \pmod{q}$ ,  $sh'_i = \sum_{j \in QUPS} sh'_{j-i} \pmod{q}$ , 则分布式私钥  $x = \sum_{i \in QUPS} x_i \pmod{q}$ 。

### 3.4 公钥提取

步骤 1 每个参与者  $P_i (i \in QUPS)$  广播参数  $\{A_{il} = g^{a_{il}} (b \pmod{p})\}_{l=0}^{t-1}$ 。

步骤 2 其余的参与者  $P_j (j \in QUPS)$  验证广播参数:

$$g^{sh_{j-i}} = \prod_{l=0}^{t-1} (A_{jl})^{e^{(t_k-1)(i)}} \pmod{p} \quad (11)$$

步骤 3 如果验证失败, 就通过广播满足式(10)但不满足式(11)的  $(sh_{i-j}, sh'_{i-j})$  来投诉  $P_i$ 。

步骤 4 对于在式(10)中受到合法投诉的  $P_i$ , 其他合法参与者计算  $f_i(x)$  和  $\{A_{ik}\}_{k=0}^{t-1}$ 。

步骤 5 QUPS 内的所有参与者子集  $\{y_i = A_{i0} = g^{x_i} \pmod{p}\}_{i \in QUPS}$ , 提取公钥:

$$y = \prod_{i \in QUPS} y_i \pmod{p}$$

随后, 利用 Birkhoff 插值可重构秘密, 此部分见第 3 章描述。为了更充分地理解算法, 举例说明。假定某科技公司要恢复某重要文件的密码(秘密), 规定至少需要 3 个参与者, 其中至少有一个参与者是经理, 且至少有两个参与者是科研部。为此, 假定参与重构此文件秘密的参与者有 5 人, 分别为  $P_1, P_2, P_3, P_4, P_5$ , 他们的职位、部门以及自选的份额如表 1 所示。

因此, 在这个案例中能够重构秘密的最小授权子集分别为  $\{P_1, P_2, P_3\}$ 、 $\{P_1, P_2, P_4\}$ 、 $\{P_1, P_3, P_4\}$  以及  $\{P_2, P_3, P_4\}$ 。假定文件密码  $S = 15$ , 两个子秘密  $S_1 = 1, S_2 = 2$ 。接下来, 分发者建立两个多项式:  $f_1(x) = 1 + x + 2x \pmod{83}$ ,  $f_2(x) = 2 + 2x + x^2 \pmod{97}$ 。

在本案例中: 按职位属性划分时将经理职员的参与者为

第一等级; 而按部门划分时, 将科研部的参与者为第一等级。因此, 这 5 个人参与者的计算各自份额信息, 如表 2 所示。

表 1 参与者的属性

参与者	部门	职位	自选份额
$P_1$	科研部	总经理	1
$P_2$	销售部	总经理	2
$P_3$	科研部	科员	3
$P_4$	科研部	科员	4
$P_5$	销售部	销售人员	5

表 2 5 个参与者的份额

参与者	$sh_i$	$sh'_i$
$P_1$	4	5
$P_2$	11	2
$P_3$	13	17
$P_4$	17	26
$P_5$	21	2

每个最小授权子集利用自己选择的数, 并结合表 2 便能恢复由分发者建立的两个多项式。例如对于  $\{P_1, P_2, P_3\}$  子集, 它们自选的份额分别为 1, 2, 3。建立的两个方程:

$$\begin{cases} a_1 + b_1 + c_1 = 4 \pmod{83} \\ a_1 + 2b_1 + 4c_1 = 11 \pmod{83} \end{cases} \quad (12)$$

$$\begin{cases} b_1 + 6c_1 = 13 \pmod{83} \\ a_2 + b_2 + c_2 = 4 \pmod{83} \end{cases} \quad (13)$$

$$\begin{cases} 2c_2 = 2 \pmod{83} \\ a_2 + 3b_2 + 9c_2 = 17 \pmod{83} \end{cases}$$

通过分别求解这两个方程组, 可解得:  $a_1 = 1, b_1 = 1, c_1 = 2, a_2 = b_2 = c_2 = 2$ 。因此, 各参与者能够重构现多项式  $f_1(x) = 1 + x + 2x \pmod{83}$ ,  $f_2(x) = 2 + 2x + x^2 \pmod{97}$ 。两个多项式的常数项为子秘密, 可得子秘密  $S_1 = 1, S_2 = 2$ 。

## 4 性能分析

### 4.1 安全性能

#### 4.1.1 正确性

命题 1 在提出的 BI-VHTSS 协议中, 所有被授权的参与者的份额能够恢复相同的且唯一的秘密  $x$ 。

证明 若  $j \in QUPS$ , 分发者  $P_j$  就能成功地共享份额  $x_j$ 。接下来, 定义  $AS = \{P_{a_1}, P_{a_2}, \dots, P_{a_t}\}$  为任意一个授权的参与者子集, 相应地, 它们份额分别为  $\{sh_{a_1}, sh_{a_2}, \dots, sh_{a_t}\}$ , 且  $a_i < a_j, i < j$ 。那么, 子集  $AS$  内的参与者, 结合它们的份额, 并利用 Birkhoff 插值恢复秘密  $x$ :

$$\begin{aligned} x &= \sum_{i=1}^t \left[ (-1)^{(i-1)} sh_i \frac{|A_{i-1}(E, X, \varphi_0)|}{|A(E, X, \varphi)|} \right] = \\ &= \sum_{i=1}^t \left[ (-1)^{(i-1)} \left( \sum_{j \in QUPS} sh_{j-i} \right) \frac{|A_{i-1}(E, X, \varphi_0)|}{|A(E, X, \varphi)|} \right] = \\ &= \sum_{j \in QUPS} \left[ \sum_{i=1}^t \left[ sh_{j-i} (-1)^{(i-1)} \frac{|A_{i-1}(E, X, \varphi_0)|}{|A(E, X, \varphi)|} \right] \right] = \\ &= \sum_{j \in QUPS} x_j \end{aligned} \quad (14)$$

命题 2 在提出的 BI-VHTSS 协议中, 所有授权的参与者能够提取相同的且唯一的公钥  $y = g^x \pmod{p}$ 。

证明 计算公钥  $y = \prod_{i \in QUPS} y_i$ , 对于  $i \in QUPS$ ,  $y_i = g^{x_i}$ 。

因此可得:

$$y = \prod_{i \in QUPS} y_i = \prod_{i \in QUPS} g^{x_i} = g^{\sum_{i \in QUPS} x_i} = g^x \quad (15)$$

对于每个广播了一个有效投诉的参与者  $P_i (i \in QUPS)$  (见3.3节步骤3),  $x_i$  将进行重构, 并且设定  $y_i = g^{x_i} (\bmod p)$ 。

对于没有广播投诉的参与者  $P_i (i \in QUPS)$  而言,  $y_i = A_{i,0}$ 。由  $P_i$  广播的  $A_{ik} (k = 0, 1, \dots, t)$  定义了  $t - 1$  阶的多项式  $\hat{f}_i(x)$ 。由于假定不存在无效的投诉, 所有诚实的参与者均满足式(12)~(13)。另外, 由于至少存在一个授权子集  $AS \subset QUPS$ ,  $\hat{f}_i(x)$  和  $f_i(x)$  是等价的, 即  $A_{i0} = g^{\hat{f}_i(0)} = g^{x_i}$ 。

#### 4.1.2 安全性

**命题3** 基于离散对数问题 (Discrete Logarithm Problem, DLP), 除了  $y = g^x (\bmod p)$  蕴含秘密  $x$  外, 攻击者无法获取  $x$  信息。

**证明** 为了证明 BI-VHTSS 协议的安全性, 假定一个模拟者  $S$  防御攻击者。针对 DLP, 其输入为  $(g, y)$ , DLP 的解就是秘密  $x$ 。首先作以下设定:

1) 腐化的参与者子集  $B = \{P_{\beta_1}, P_{\beta_2}, \dots, P_{\beta_l}\}$ , 未腐化参与者子集  $G = \{P_{\beta_{l+1}}, P_{\beta_{l+2}}, \dots, P_{\beta_n}\}$ 。

2) 考虑最糟糕的情况,  $B$  中存在被授权的参与者。

3)  $B'$  是  $B$  的一个子集, 致使  $|B'| = t - 1$ , 并且  $B' \cup \{P_0\}$  为一个授权的子集, 其中  $P_0$  表示  $U_0$  内的任意的某一参与者。

4)  $B'$  中的参与者分别表示为  $P_{\beta_1}, P_{\beta_2}, \dots, P_{\beta_{t-1}}$ 。

第1步 执行 BI-VHTSS 算法的密钥生成阶段, 包括从不诚实的到诚实的参与者接收、处理信息, 均满足下列条件:

1) 确定了  $QUPS, G \subseteq QUPS$  以及多项式  $f_i(z), f'_i(z)$ , 且  $P_i \in G$ 。

2) 对于参与者  $P_i \in B, P_j \in G$  接收了各自的份额  $(sh_{j-i}, sh'_{j-i}) = (f_j^{(t_k-1)}(i), f'_j^{(t_k-1)}(i))$  以及公共参数  $C_{jl}, l = 0, 1, \dots, t - 1$ 。

3)  $S$  知道所有多项式  $f_i(z), f'_i(z) (i \in QUPS)$ , 并且具有所有份  $(sh_{j-i}, sh'_{j-i})$  和公共参数  $C_{jl}$  值。

第2步 执行以下计算:

1) 计算  $A_{il} = g^{a_{il}}, i \in QUPS \setminus \{\beta_n\}, l = 0, 1, \dots, t - 1$ 。

2) 设定  $A_{\beta_{l0}}^* = y \cdot \prod_{i \in (QUPS) \setminus \{\beta_n\}} A_{i0}^{-1} (\bmod p)$ ;

3) 计算  $A_{\beta_{nl}}^* = (A_{\beta_{l0}}^*)^{\lambda_{l0}} \cdot \prod_{i=1}^{t-1} (g^{sh_{n \rightarrow \beta_i}})^{\lambda_{li}}$ , 其中  $\lambda_{li}$  为适宜的 Birkhoff 插值系数。

4) 广播  $A_{il}$  和  $A_{\beta_{nl}}^*$ , 其中:  $i \in G \setminus \{\beta_n\}; l = 0, \dots, t - 1$ 。

5) 每个参与者  $P_i \in B$ , 利用式(3) 验证  $A_{ik}$ 。如果验证未通过, 就投诉。

6) 接下来以未腐化的参与者计算  $x_i$ 。

$x_i$  是 DLP 的唯一解。这就表明广播的参数没有泄露关于秘密的任何信, 即提出的 BI-VHTSS 算法是安全的。

#### 4.2 计算复杂度及完备性

首先给出完备性的定义。

**定义3** 秘密共享方案的完备性<sup>[3]</sup>

$U = \{P_1, P_2, \dots, P_n\}$  是  $n$  个参与者的集合,  $\Gamma \subseteq 2^U$  为参与者集合的访问结构(见定义2)。令  $\{u_1, u_2, \dots, u_n\}$  表示各个参与者拥有的份额, 且它们共享的秘密为  $S$ 。若满足下列两个

条件, 则该方案称为完备的。

1) 正确性: 对于任何一个最小的授权子集  $A \in \Gamma$ , 则满足  $H(S \mid u_i \mid u_i \in A) = 0$ 。

2) 安全性: 对于任何一个最小的授权子集  $A \notin \Gamma$ , 则满足  $0 < H(S \mid u_i \mid u_i \in A) \leq H(S)$ 。

其中,  $H(\cdot)$  表示信息熵。在秘密共享方案中,  $H(S)$  可理解为秘密  $S$  的字节长度。3.1节分别证明了 BI-VHTSS 算法的正确性和安全性。因此 BI-VHTSS 算法具有完备性。

为考察本文 BI-VHTSS 算法的计算复杂度、访问结构以及安全性能的完备性, 将本文算法与文献[1~2]分别提出的两种基于 DKG 的算法进行对比。本文将这两种算法分别称为 TDKG-G 算法和 TDKG-P 算法。实验结果如表3所示。

从表3可知, 提出的 BI-VHTSS 算法与 TDKG-G 相同, 计算复杂度均为  $O(2nt + 2n + t - 3)$ ; 而 TDKG-P 算法的计算复杂度降低约一半, 从计算复杂度角度, TDKG-P 算法更有效。此外, BI-VHTSS 和 TDKG-G 算法的安全性能高于 TDKG-P 算法, 具有完备安全性能。原因在于 TDKG-P 算法并不满足公钥的均匀分布。与 TDKG-G 算法不同, BI-VHTSS 算法属于多等级门限访问结构, 而 TDKG-P、TDKG-G 算法没有考虑参与者的等级问题, 限制了它们的应用。

表3 几种同类算法的性能比较

算法	计算复杂度	访问结构	完备安全
TKDG-G <sup>[1]</sup>	$O(2nt + 2n + t - 3)$	门限访问结构	有
TKDG-P <sup>[2]</sup>	$O(nt + n - 1)$	门限访问结构	否
BI-VHTSS	$O(2nt + 2n + t - 3)$	等级访问结构	有

注:  $n$  为总的参与者个数,  $t$  为授权参与者子集的尺寸。

#### 5 结语

本文基于秘密共享策略提出了一个可验证的安全的多等级秘密共享算法, 解决了参与者的不同等级问题; 同时, 利用 Birkhoff 插值法、离散对数问题, 证明了 BI-VHTSS 算法的安全性。此外, BI-VHTSS 算法能够应用于分布式加密系统, 可产生多等级门限签名或加密系统。

#### 参考文献:

- [1] GENNARO R, JARECKI S, KRAWCZYK H, et al. Secure distributed key generation for discrete-log based cryptosystems[J]. Journal of Cryptology, 2007, 20(1): 51~83.
- [2] PEDERSEN T. A threshold cryptosystem without a trusted party [C]// EUROCRYPT 1991: Proceedings of the 1991 Workshop on the Theory and Application of Cryptographic Techniques. Berlin: Springer, 1991: 522~526.
- [3] 焦栋. 门限秘密共享策略及其应用研究[D]. 大连: 大连理工大学, 2014: 21~36. (JIAO D. Research on threshold secret sharing scheme and its applications [D]. Dalian: Dalian University of Technology, 2014: 21~36.)
- [4] YUAN H, ZHANG F, HUANG X, et al. Certificateless threshold signature scheme from bilinear maps[J]. Information Sciences, 2010, 180(23): 4714~4728.
- [5] HERRANZ J, RUIZ A, SÁEZ G. Signcryption schemes with threshold unsigncryption, and applications[J]. Designs, Codes and Cryptology, 2014, 70(3): 1~23.

(下转第 972 页)

- [18] CHEN J, ZHU Z, FU C, et al. Reusing the permutation matrix dynamically for efficient image cryptographic algorithm [J]. *Signal Processing*, 2015, 111(5): 294 – 307.
- [19] 江帆, 吴小天, 孙伟. 基于稀疏矩阵的 Arnold 数字图像加密算法[J]. *计算机应用*, 2015, 35(3): 726 – 731, 745. (JIANG F, WU X T, SUN W. Arnold digital image encryption algorithm based on sparse matrix [J]. *Journal of Computer Applications*, 2015, 35(3): 726 – 731, 745.)
- [20] LIU H, KADIR A, NIU Y. Chaos-based color image block encryption scheme using S-box [J]. *AEU — international Journal of Electronics and Communications*, 2014, 68(7): 676 – 686.
- [21] MURILLO-ESCOBAR M A, CRUZ-HERNANDEZ C, ABUNDIZ-PEREZ F, et al. A RGB image encryption algorithm based on total plain image characteristics and chaos [J]. *Signal Processing*, 2015, 109(6): 119 – 131.
- [22] 刘国宏, 郭文明. 改进的中值滤波去噪算法应用分析[J]. *计算机工程与应用*, 2010, 46(10): 187 – 189. (LIU G H, GUO W M. Application of improved arithmetic of median filtering denoising [J]. *Computer Engineering and Applications*, 2010, 46(10): 187 – 189.)
- [23] 金建国, 陈晨, 魏明军, 等. 基于混沌调制 DFRFT 旋转因子的语音加密[J]. *计算机工程*, 2012, 6(12): 95 – 98. (JIN J G, CHEN C, WEI M J, et al. Audio encryption based on chaotic modulation DFRFT rotation factor [J]. *Computer Engineering*, 2012, 6(12): 95 – 98.)
- [24] 金建国, 王乐, 魏明军, 等. 混沌密钥调制 DFRFT 旋转因子的视频加密研究[J]. *中国图象图形学报*, 2013, 18(12): 1567 – 1573. (JIN J G, WANG L, WEI M J, et al. Video encryption based on chaotic key modulating DFRFT rotation factor [J]. *Journal of Image and Graphics*, 2013, 18(12): 1567 – 1573.)
- [25] PEI S C, YEH M H, TSENG C C. Discrete fractional Fourier transform based on orthogonal projections [J]. *IEEE Transactions on Signal Processing*, 1999, 47(5): 1335 – 1348.
- [26] 文昌辞, 王沁, 刘向宏, 等. 基于仿射和复合混沌的图像加密新算法[J]. *计算机研究与发展*, 2013, 50(2): 319 – 324. (WEN C C, WANG Q, LIU X H, et al. An encryption algorithm for image based on affine and composed chaos [J]. *Journal of Computer Research and Development*, 2013, 50(2): 319 – 324.)
- [27] 王静, 蒋国平. 一种超混沌图像加密算法的安全性分析及其改进[J]. *物理学报*, 2011, 60(6): 83 – 93. (WANG J, JIANG G P. Cryptanalysis of a hyper-chaotic image encryption algorithm and its improved version [J]. *Acta Physica Sinica*, 2011, 60(6): 83 – 93.)
- [28] SUI L, DUAN K, LIANG J, et al. Asymmetric multiple-image encryption based on coupled logistic maps in fractional Fourier transform domain [J]. *Optics and Lasers in Engineering*, 2014, 62(5): 139 – 152.

#### Background

This work is partially supported by the Natural Science Foundation of Hebei Province (F201409108).

**JIN Jianguo**, born in 1956, M. S., professor. His research interests include information security, chaotic encryption.

**XIAO Ying**, born in 1990, M. S. candidate. Her research interests include information security, chaotic encryption.

**DI Zhigang**, born in 1975, Ph. D., lecturer. His research interests include opto-electronic technology, fiber sensor, information security, chaotic encryption.

(上接第 955 页)

- [6] BUDURUSHI J, NEUMANN S, OLEMBO M, et al. Pretty understandable democracy — a secure and understandable Internet voting scheme[C]// Proceedings of the 2013 Eighth IEEE International Conference on Availability, Reliability and Security. Piscataway, NJ: IEEE, 2013: 198 – 207.
- [7] BASU A, SENGUPTA I, SING J K. Secured hierarchical secret sharing using ECC based signcryption [J]. *Security Communication Networks*, 2012, 5(7): 752 – 763.
- [8] TENTU A N, PAUL P, VENKAIAH V C. Ideal and perfect hierarchical secret sharing schemes[J]. *IACR Cryptology Eprint Archive*, 2013, 3(4): 23 – 32.
- [9] FARRAS O, PADRO C. Ideal hierarchical secret sharing schemes [J]. *IEEE Transactions on Information Theory*, 2012, 58(5): 3273 – 3286.
- [10] 焦栋, 李明楚, 郭成, 等. 可重用多属性多等级门限秘密共享 [J]. *计算机工程与应用*, 2014, 50(10): 7 – 12. (JIAO D, LI M C, GUO C, et al. Reusable multi-attributes hierarchical threshold scheme[J]. *Computer Engineering and Applications*, 2014, 50(10): 7 – 10.)
- [11] SIMMONS G J. How to (really) share a secret[C]// Proceedings of CRYPTO 1988, LNCS 403. Berlin: Springer, 1990: 390 – 448.
- [12] BRICKELL E F. Some ideal secret sharing schemes[C]// EUROCRYPT 1989: Proceedings of the 1989 Workshop on the Theory

and Application of Cryptographic Techniques, LNCS 434. Berlin: Springer, 1990: 468 – 475.

[13] GHODOSI H, PIEPRZYK J, SAFAVI-NAINI R. Secret sharing in multilevel and compartmented groups[C]// ACISP 1998: Proceedings of the 3rd Australasian Conference on Information Security and Privacy, LNCS 1438. Berlin: Springer, 1998: 367 – 378.

[14] TASSA T. Hierarchical threshold secret sharing [J]. *Journal of Cryptology*, 2007, 20(2): 237 – 264.

[15] PAKNIAT H, NOROOZI M, ESLAMI Z. Distributed key generation protocol with hierarchical threshold access structure[J]. *IET Information Security*, 2015, 9(4): 248 – 255.

#### Background

This work is partially supported by the National High Technology Research and Development Program (863 Program) of China (2013AA040302), 2014 Shanghai Economic and Information Commission Project (ZB-ZBYZ-03-12-1067-1).

**XU Xiaojie**, born in 1982, Ph. D., lecturer. His research interests include computer architecture, embedded system, information security, trusted computing.

**WANG Lisheng**, born in 1957, professor. His research interests include computer architecture, embedded system, trusted computing, multi-threaded parallel computing.