鲁东大学学报(自然科学版)
Journal of Ludong University(Natural Science Edition) 2020,36(3):220—223

一种无可信中心的可验证秘密共享方案

黄科华[1],陈和风[2,3]

(1. 泉州幼儿师范高等专科学校 初等教育系,福建 泉州 362000; 2. 集美大学 计算机工程学院,福建 厦门 361021;
3. 虚拟现实与三维可视化福建省高校重点实验室,福建 厦门 361021)

摘要: 利用二元多项式和离散对数问题难解构造了一种秘密共享方案,该方案不需要可信中心进行参数和用户份额的生成,从而避免了可信中心的欺骗行为. 当秘密合成后,可以验证是否有用户从中作弊,并且可以证明该方案为一个完美的秘密共享方案.

关键词: 秘密共享; 无可信中心; 可验证
中图分类号: TP309 **文献标志码:** A **文章编号:** 1673-8020(2020)03-0220-04

秘密共享方案是密码学的重要研究方向,主要用于安全多方计算以及信息的加密、共享等方面. 一个秘密共享方案通常由以下几部分组成: 秘密分发者或者称之为可信中心 D,秘钥集合 S,秘钥份额所有者组成的集合 P,准入结构 Γ(由 P 的某些子集构成)、秘钥分配算法和份额合成算法.

如果 n 个用户中至少 t 个用户份额合作在一起才能合成秘钥,而少于 t 个用户合作无法得到秘钥任何信息,这种秘密共享方案称为 (t,n) 门限秘密共享方案. 这是一类最重要的秘密共享方案. Shamir[1] 和 Blakley[2] 于 1979 年分别独立提出了不同的 (t,n) 门限秘密共享方案,前者使用了拉格朗日插值公式,后者使用了线性集合投影方法. 此后,许多研究者利用不同的数学技术构造了相应的 (t,n) 门限秘密共享方案,如利用中国剩余定理[3—5]、格[6]、向量空间[7]、二元多项式[8—11] 等.

传统的 (t,n) 门限秘密共享方案存在一些不足之处,如果可信中心在分发秘密份额的过程中有人为介入,出现作弊行为,对整个方案是致命的,而且不容易验证. 基于此,研究者们提出了对应的改进方案,如无可信中心的 (t,n) 门限秘密共享方案[12—16]、可验证的 (t,n) 门限秘密共享方案[17—18] 等. 但是这些方案也并不完善,如使用了双线性对,增加了计算量,需要所有用户参与到验证过程中等. 为此,本文利用二元多项式,基于离散对数的安全性提出了一种无可信中心的可验证 (t,n) 门限秘密共享方案,摆脱了可信中心的控制,由用户自己生成秘钥份额,并且秘钥合成后可以验证用户是否作弊,提高了方案的安全性.

1 预备知识

1.1 离散对数

设 p 为一个大素数,a 是 p 的一个生成元,若 $i \equiv \log_a b \pmod p$,其中 $b \in \{1,2,\cdots,p-1\}$,则称 i 为模 p 下以 a 为底的 b 的离散对数.

所谓的离散对数问题难解是指,已知 a,p,i 计算 b 是容易的,但已知 a,p,b 计算 i 是困难的,在多项式时间内完成是不可行的.

收稿日期: 2019-09-01; 修回日期: 2020-05-12
基金项目: 福建省中青年教师教育科研项目(JAT190314); 虚拟现实与三维可视化福建省高校重点实验室开放课题(VRTY2019005); 泉州市高等学校中青年学科(专业)带头人培养计划(泉教高[2018]1 号)
第一作者简介: 黄科华(1983—),男,福建泉州人,副教授,硕士,研究方向为密码学、信息安全. E-mail: hkh_hkh@qq.com
通信作者简介: 陈和风(1982—),女,福建厦门人,讲师,博士,研究方向为密码学、信息隐藏. E-mail: chenhf@jmu.edu.cn

1.2　陷门单向函数

函数 $h(x)$ 称为陷门单向函数,如果其满足以下两个条件:

1) 给定 x,能够容易地计算 $y = h(x)$;

2) 给定 y,计算 $x = h^{-1}(y)$ 是困难的,但是如果知道陷门信息,可以容易地计算出 y.

陷门单向函数可以选择 RSA 函数等.

1.3　完美秘密共享方案

设 $P = \{P_1, P_2, \cdots, P_n\}$ 为合成秘钥的参与者集合; S 为秘钥; Γ 为准入结构; $S_1, S_2, \cdots, S_n$ 为用户 $P_1, P_2, \cdots, P_n$ 的份额,方案 $\Pi: S \to \{S_1, S_2, \cdots, S_n\}$ 满足:

$$H(S \mid \{S_i \in A\}) = \begin{cases} 0, A \in \Gamma, \\ H(S), A \notin \Gamma, \end{cases}$$

其中 H 表示熵,则称方案 Π 为完美秘密共享方案.

传统的 Shamir(t,n) 门限秘密共享方案[1] 为完美的秘密共享方案,因为其满足少于 t 个用户共谋无法得到秘密的任何信息,即 $H(S \mid$ 少于 t 个用户的集合$) = H(S)$.

2　一种无可信中心的可验证秘密共享方案

该方案定义在有限域 $GF(p)$ 上,其中大素数 p 的选取要满足离散对数问题难解的假定.

2.1　参数生成阶段

假设 n 个用户 $P_1, P_2, \cdots, P_n$ 合作,共同约定选择生成元 $a \in GF(p)$,然后每个用户 $P_i(i = 1, 2, \cdots, n)$ 进行如下操作:

1) 秘密选择并保存一个二元多项式

$$f_i(x,y) = a_{00}^i + a_{10}^i x + a_{20}^i x^2 + \cdots + a_{(t-1)0}^i x^{t-1} + a_{01}^i y + a_{11}^i xy + a_{21}^i x^2 y + \cdots + a_{(t-1)1}^i x^{(t-1)} y + \cdots + a_{(t-1)t}^i y^{(t-1)} + a_{1(t-1)}^i xy^{(t-1)} + a_{2(t-1)}^i x^2 y^{(t-1)} + \cdots + a_{(t-1)(t-1)}^i x^{(t-1)} y^{(t-1)}; \quad (1)$$

2) 选取并公布一个陷门单向函数 $h_i(x)$;

3) 对外公布自己的身份标识 $ID_i \in GF(p)$;

4) 计算并对外公布

$$A_i = a^{a_{00}^i} (\bmod p). \quad (2)$$

2.2　秘钥份额生成阶段

每个用户 $P_i(i = 1, 2, \cdots, n)$ 如下操作:

1) 针对第 j 个用户 P_j,利用陷门计算出 $f_i(ID_j, 0)$,其中 $j \in \{1, 2, \cdots, n\}, j \neq i$;

2) 针对第 j 个用户 P_j,计算 $h_j(f_i(ID_j, 0))$,并将其通过公开信道发送给用户 P_j,其中 $j \in \{1, 2, \cdots, n\}, j \neq i$;

3) 利用掌握的信息生成自己的份额

$$S_i = \sum_{j=1}^{n} f_j(ID_i, 0) (\bmod p). \quad (3)$$

2.3　秘钥合成阶段

假设 n 个用户中,任意 t 个用户 $P_{i_1}, P_{i_2}, \cdots, P_{i_t}$ 合作,他们可以通过手中的数对 (ID_{i_m}, S_{i_m}), $m = 1, 2, \cdots, t$, 合成多项式

$$G(x) = \sum_{m=1}^{t} S_{i_m} \prod_{r=1, r\neq m}^{t} \left(\frac{x - ID_{i_r}}{ID_{i_m} - ID_{i_r}}\right) (\bmod p). \tag{4}$$

从而，$G(0)$ 为所需合成的秘钥 S.

3 方案分析

3.1 正确性分析

任意一个用户 $P_i(i = 1,2,\cdots,n)$，手中的份额 $S_i = \sum_{j=1}^{n} f_j(ID_i,0) (\bmod p)$ 与用户标识 ID_i 组成的二元对 (ID_i, S_i)，均满足方程

$$G(x) = \sum_{i=1}^{t} S_i \prod_{j=1, j\neq i}^{t} \left(\frac{x - ID_j}{ID_i - ID_j}\right) (\bmod p). \tag{5}$$

而该方程为 $t-1$ 次一元多项式，根据朗格朗日插值定理，大于等于 t 个用户可以合成多项式，取得 $G(0)$，而少于 t 个用户合作得不到多项式 $G(x)$ 的任何信息.

3.2 可验证性分析

假设有 t 个用户 $P_{i_1}, P_{i_2}, \cdots, P_{i_t}$ 共谋，合成多项式 $G(x) = \sum_{m=1}^{t} S_{i_m} \prod_{r=1, r\neq m}^{t} \left(\frac{x - ID_{i_r}}{ID_{i_m} - ID_{i_r}}\right) (\bmod p)$，从而得到秘钥 S

$$S = G(0) = \sum_{m=1}^{t} \sum_{j=1}^{n} f_j(ID_{i_m},0) \prod_{r=1, r\neq m}^{t} \left(\frac{ID_{i_r}}{ID_{i_m} - ID_{i_r}}\right) =$$

$$\sum_{j=1}^{n} \sum_{m=1}^{t} f_j(ID_{i_m},0) \prod_{r=1, r\neq m}^{t} \left(\frac{ID_{i_r}}{ID_{i_m} - ID_{i_r}}\right) = \sum_{j=1}^{n} f_j(0,0) = \sum_{j=1}^{n} a_{00}^{j} (\bmod p). \tag{6}$$

该 t 个用户可以根据每个用户公布的 $A_i = a^{a_{00}^{i}} (\bmod p)$，计算 $\prod_{i=1}^{n} A_i$，若 $a^{G(0)} \neq \prod_{i=1}^{n} A_i (\bmod p)$，则说明至少有一个用户作弊，没有提供正确的参数.

在验证过程中，由于离散对数问题难解的困难假设，所以用户手中的 a_{00}^{i} 是安全的.

3.3 方案更新

如果有新用户 P_v 想加入系统，只需要公布自己的陷门单向函数 $h_v(x)$，向系统其它用户 P_j 发送 $h_j(f_v(ID_j,0))$，并接收对方发送的 $h_v(f_j(ID_v,0))$ 即可.

当再次合成秘钥时，只需每个用户更新 a_{00}^{i} 即可.

3.4 本方案为完美的秘密共享方案

本方案的准入结构 Γ 定义为大于 t 个用户所组成的集合. 由于在秘钥合成的过程中，采用拉格朗日插值公式，根据多项式性质，少于 t 用户合作将无法得到秘钥的任何信息. 此外，根据离散对数问题难解的困难假设，用户也得不到其他人手中的二元多项式常数项的秘密信息. 即，如果用户集合 $A \notin \Gamma$，则 $H(S|\{S_i \in A\}) = H(S)$. 综上所述，该方案为完美的秘密共享方案.

3.5 与其他方案的比较

在现有的利用二元多项式构造秘密共享方案[8—11]的设计中，均需要由可信中心 D 进行参数的生成和份额的分发工作. 本文提供了一个无可信中心的秘密共享方案，摆脱了对可信中心的依赖性，增强了

系统的安全性.

与现有的无可信中心的秘密共享方案[12—15]对比,这些方案均需要使用双线性对支持无可信中心的功能,其中,张文芳等[16]的方案在合成秘钥过程中,需要全体用户联合合成; 而本方案大部分都是进行多项式运算,且秘钥合成不需要所有用户的联合,故而在效率上更加高效.

4　结语

本文基于离散对数问题难解的困难假设,利用二元多项式构造秘密共享方案,该方案不需要可信中心进行参数和用户份额的生成,并且当秘钥合成后,可以验证是否有用户作弊. 今后可以进一步研究多秘密共享方案或可变门限共享方案.

参考文献:

[1] SHAMIR A. How to share a secret [J]. Communications of the ACM,1979(11):612 - 613.

[2] BLAKLEY G R. Safeguarding cryptographic keys [C]// AFIPS 1979 National Computer Conference,1979,48:313 - 317.

[3] IFTENE S. General secret sharing based on the Chinese remainder theorem with applications in E - voting [J]. Electronic Notes in Theoretical Computer Science,2007,186:67 - 84.

[4] GUO C,CHANG C C. An authenticated group key distribution protocol based on the generalized Chinese remainder theorem [J]. International Journal of Communication Systems,2014,27(1):126 - 134.

[5] CHEN H F,CHANG C C. A novel (t,n) secret sharing scheme based upon Euler's theorem [J]. Security and Communication Networks,2019,6:1 - 7.

[6] 张红军,刘珂,牟占生. 基于格的门限秘密共享算法 [J]. 计算机工程,2016,42(6):139 - 143.

[7] 李滨. 基于向量空间不同访问群体的门限方案 [J]. 通信学报,2015,36(11):67 - 72.

[8] 黄科华,热娜·艾合买提,张瑛瑛. 基于单向函数与二元多项式的秘密分享方案 [J]. 鲁东大学学报(自然科学版),2014,30(3):223 - 226.

[9] 黄科华. 基于二元多项式与中国剩余定理的多秘密分享方案 [J]. 长沙大学学报,2015,29(2):8 - 10.

[10] 顾为玉,苗付友,何晓婷. 基于二元对称多项式的公平秘密共享方案 [J]. 计算机工程与应用,2016,52(13):38 - 42.

[11] 杨文伟,邢玉清. 基于二元非对称多项式的公平秘密共享方案 [J]. 网络与信息安全学报,2019,5(1):22 - 29.

[12] 杨阳,朱晓玲,丁凉. 基于中国剩余定理的无可信中心可验证秘密共享研究 [J]. 计算机工程,2015,41(2):122 - 128.

[13] 于佳,陈养奎,郝蓉,等. 无可信中心的可公开验证多秘密共享 [J]. 计算机学报,2014,37(5):1030 - 1038.

[14] 王俞力,杜伟章. 向量空间上无可信中心的动态多秘密共享方案 [J]. 计算机工程,2017,43(7):163 - 169.

[15] 谷婷,杜伟章. 无可信中心的可动态更新多秘密共享方案 [J]. 计算机工程,2016,42(3):148 - 155.

[16] 张文芳,王小敏,何大可. 一个无可信中心(t,n)门限签名方案的安全缺陷及其改进 [J]. 铁道学报,2008(3):40 - 45.

[17] PATRA A,CHOUDHARY A,PANDU R C. Simple and efficient asynchronous byzantine agreement with optimal resilience [C]// The 28th ACM Symposium on Principles of Distributed Computing,2009:92 - 101.

[18] CAFARO M,PELLE P. Space - efficient verifiable secret sharing using polynomial interpolation [J]. IEEE Transactions on Cloud Computing,2018,6:453 - 463.

(下转第 264 页)

Soil Soluble Salts and Nutrient Profile Analysis of *Tamarix chinensis*-*Suaeda glauca* Community in the Yellow River Delta Wetland

LIU Xiaoxia[1], ZHANG Tao[2], TAN Xiaoli[1], MING Liping[3], WANG Weili[3]

(1. Zibo Linzi District Environmental Monitoring Station, Zibo 255400, China;
2. Environmental Monitoring Station of Zibo National High-tech Industrial Development Zone, Zibo 255400, China;
3. School of Chemistry and Material Science, Ludong University, Yantai 264039, China)

Abstract: *Tamarix chinensis*-*Suaeda glauca* community is the representative vegetation in the Yellow River Delta, and is mostly used to improve the saline soil by the local people. In the current study, the distribution characteristics of soluble salt ions and nutrients of the soil profile of *Tamarix chinensis*-*Suaeda glauca* community in the Yellow River Delta wetland were studied, and the soil condition of this community in this region was fully investigated. The research results show that chloride ion is one of the main soluble salt ions in this area, and the land is potassium-rich soil. The contents of soluble salt ions and various nutrients have obvious gradation, which are mainly distributed on the surface layer of the soil. This study provides the scientific basis for protecting the soil and decreasing the salinization of soil in this area.

Keywords: Yellow River Delta; soil soluble salts; soil nutrient; *Tamarix chinensis*-*Suaeda glauca* community; distribution characteristics of profile

(责任编辑 李维卫)

(上接第223页)

Abstract ID: 1673-8020(2020)03-0220-EA

Verifiable Secret Sharing Scheme Without Trusted Authority

HUANG Kehua[1], CHEN Hefeng[2,3]

(1. Department of Primary Education, Quanzhou Preschool Education College, Quanzhou 362000, China;
2. Computer Engineering College, Jimei University, Xiamen 361021, China;
3. Key Laboratory of Fujian Universities for Virtual Reality and 3D Visualization, Xiamen 361021, China)

Abstract: A secret sharing scheme was constructed by using binary polynomial and discrete logarithms. The scheme does not need the trusted authority to generate parameters and user shares, thus avoiding the cheating of the trusted authority. After secret synthesis, it can be verified whether a user is cheating, and it can be proved that the scheme is a perfect secret sharing scheme.

Keywords: secret sharing scheme; without trusted authority; verifiable

(责任编辑 李秀芳)