

# 一种动态的多秘密共享方案

柳 烨, 李志慧, 郭 瑞

(陕西师范大学数学与信息科学学院, 西安 710062)

**摘 要:** 基于 Shamir 的秘密共享体制和 RSA 加密算法的安全性, 提出一种动态的门限秘密共享方案。在该方案中可以动态添加或删除参与者以及更新多重秘密, 无需重新分发子秘密, 参与者的秘密份额由每个参与者自己选取, 其秘密份额的信息可以通过公开的信道发送给秘密分发者, 在秘密恢复过程中, 每个参与者能够验证其他参与者是否进行了欺骗。

**关键词:** 门限方案; 动态; 多秘密共享

## Dynamic Multi-secret Sharing Scheme

LIU Ye, LI Zhi-hui, GUO Rui

(College of Mathematics & Information Science, Shaanxi Normal University, Xi'an 710062)

**【Abstract】** This paper proposes a dynamic multi-secret sharing scheme based on the safety of Shamir secret sharing scheme and RSA encryption algorithm. The participants can be dynamically joined or deleted and multi-secrets are dynamically renewed without re-distributing the sub-secrets. The sub-secrets of participants are chosen by himself or herself and are submitted to secret dealer by using public channel. In the recovering phase, each participant is allowed to check whether another participant provides the true information.

**【Key words】** threshold scheme; dynamic; multi-secret sharing

### 1 概述

秘密共享<sup>[1]</sup>在现代密码中有非常重要的作用, 它是在一组参与者中共享秘密, 主要用于保护重要信息以防丢失、破坏、篡改或落入坏人手里。1979年, Shamir 和 Blakley 分别基于 Lagrange 插值多项式和射影几何提出了  $(t, n)$  门限秘密共享方案。在  $(t, n)$  门限方案中, 一个秘密被分成  $n$  份, 分别分发给  $n$  个参与者,  $n$  个参与者中的任意  $t$  个合作能恢复共享的秘密, 少于  $t$  个则得不到关于秘密的任何信息。但这 2 个方案都只适用于单秘密共享, 同时要求参与者和分发者是诚实的, 这在现实生活中是不可能的。随后, 多秘密共享方案和可验证的秘密共享方案被提出。大多数方案在设计时都基于 2 个假设: (1) 在秘密被重构之前所有的参与者和秘密都不改变。(2) 秘密分发者和各参与者之间需要建立一条安全信道。但这 2 个假设会影响秘密共享方案的实际应用。文献[2-3]分别提出了在线的秘密共享方案, 但是要求秘密分发者必须安全存储各参与者的份额, 存储负担过重。文献[4]提出的方案尽管能够有效解决秘密份额分发问题, 但效率较低。文献[5]提出了一个动态的秘密共享方案, 在该方案中使用了 RSA 密码体制, 这使得方案不需要建立安全信道并且秘密和参与者都可以动态地发生变化, 但它只适用于单秘密共享, 存在一定的局限性。本文基于 Shamir 的秘密共享体制和 RSA 密码体制, 提出了一个动态的  $(t, n)$  门限多秘密共享方案。

### 2 方案构成

#### 2.1 初始化过程

令  $P = \{P_1, P_2, \dots, P_n\}$  是  $n$  个参与者的集合,  $S = \{S_1, S_2, \dots, S_m\}$  为群组密钥的集合。该方案需要一个公告牌<sup>[2]</sup>。首先, 秘密分发者随机选取 2 个安全素数  $p$  和  $q$ , 满足  $p = 2p' + 1$ ,  $q = 2q' + 1$ ,  $p', q'$  也是素数。计算  $N = pq$  和  $R = p'q'$ 。在  $Z_N^*$

中选择一个阶为  $R$  的元素  $g$ , 然后选择公钥和私钥对  $(e, d)$ , 满足  $ed = 1 \bmod \phi(N)$ 。在公告牌上公布系统信息  $(g, N, e)$  并将  $(R, d)$  保密。

在秘密分发者公开  $(g, N, e)$  之后, 每个参与者  $P_i$  随机地从  $[2, N]$  中选取一个整数  $s_i$ , 并计算  $R_i = g^{s_i} \bmod N$ 。参与者保密  $s_i$ , 并将  $R_i$  发送给秘密分发者。秘密分发者确保  $R_i \neq R_j$  ( $i \neq j$ ), 否则, 要求参与者重新选择, 直到对于所有的  $1 \leq i \neq j \leq n$  都有  $R_i \neq R_j$  为止。

秘密分发者随机地从  $[1, n]$  中为每个参与者  $P_i$  选取一个唯一的整数  $ID_i$  作为其身份标识, 并在公告牌上公开每一个参与者  $P_i$  的信息  $(R_i, ID_i)$ 。

#### 2.2 秘密分发算法

秘密分发者可以执行以下步骤完成秘密的分发:

(1) 计算  $R_0 = g^d \bmod N$ 。

(2) 随机地构造一个  $(t-1)$  次多项式  $f(x) = (a_0 + a_1x + a_2x^2 + \dots + a_{t-1}x^{t-1}) \bmod R$ , 其中,  $a_k \in Z_R$  且  $a_{t-1} \neq 0$ 。计算信息:  $MSG = (R_0, e, f(ID_1) \oplus R_1^d \bmod N, f(ID_2) \oplus R_2^d \bmod N, \dots, f(ID_n) \oplus R_n^d \bmod N)$ , 并将其公布在公告牌上。

(3) 计算  $S'_i = a_0 \oplus S_i$  ( $i = 1, 2, \dots, m$ ) 并将其公布在公告牌上。

#### 2.3 秘密重构算法

本文在  $P$  中选取  $t$  个参与者的集合  $A = (P_1, P_2, \dots, P_t)$  作为

**基金项目:** 国家自然科学基金资助项目(60873119); 陕西省自然科学基金基础研究计划基金资助项目(2007A06)

**作者简介:** 柳 烨(1982—), 女, 硕士研究生, 主研方向: 有限域, 密码学; 李志慧, 副教授、博士; 郭 瑞, 硕士研究生

**收稿日期:** 2009-03-10 **E-mail:** liuye7699824@163.com

例子来说明秘密重构过程。

$A$  中每个参与者  $P_i$  从公告牌上下载有关  $a_0$  的公开信息  $(g, N, e)$  和  $MSG$ 。每个  $P_i$  利用其秘密份额  $s_i$  计算子秘密  $R_0^{s_i} \bmod N$ ，并将结果送给指定的秘密生成者 DC(Designated Combiner)。当然要求 DC 是诚实的。

DC 在收到各参与者的子秘密后，从公告牌上下载关于  $a_0$  的公共信息  $(g, N, e)$  和  $MSG$  以及  $A$  中每个  $P_i$  的信息  $(R_i, ID_i)$ ，并通过等式  $(R_0^{s_i})^e = R_i \bmod N$  来验证每个  $P_i$  是否进行了欺骗。

对于每个  $i = 1, 2, \dots, t$ ，DC 计算  $f(ID_i) \oplus R_i^d \oplus R_0^{s_i} = f(ID_i) \oplus g^{ds_i} \oplus g^{ds_i} = f(ID_i)$ ，利用参与者公开的身份信息  $ID_i$  和计算得到的  $t$  个  $f(ID_i)$  可以构成  $t$  个点： $(ID_1, f(ID_1)), (ID_2, f(ID_2)), \dots, (ID_t, f(ID_t))$ 。利用 Lagrange 插值法重构  $(t-1)$  次多项式  $f(x)$ ，最终可以恢复出  $a_0 = f(0)$ 。

DC 从公告牌上下载公开信息  $S_i'$ ，计算出共享的秘密  $S_i = a_0 \oplus S_i' (i = 1, 2, \dots, m)$ 。

### 3 分析与讨论

#### 3.1 安全性分析

方案的安全性可以通过以下 3 种攻击进行分析：

攻击 1：  $(t-1)$  个或更少的参与者试图合作恢复共享的秘密。 $(t, n)$  门限秘密共享方案最基本的要求就是少于  $t$  个参与者的合作不能恢复共享的秘密。由于重构  $(t-1)$  次多项式  $f(x)$  需要知道  $t$  个满足  $y_i = f(x_i)$  的点  $(x_i, y_i)$ ，而  $(t-1)$  个或更少的参与者的合作不可能得到这样的  $t$  个点，因此利用  $(t-1)$  个或更少的点来重构  $(t-1)$  次多项式  $f(x)$  等价于成功攻破 Shamir 的  $(t, n)$  门限体制，这是不可行的。

攻击 2：攻击者可能设法从公开的信息  $R_i = g^{s_i} \bmod N$  中推导出  $s_i$  从而进行攻击，显然，该等式利用了  $Z_N$  上离散对数的难解性，因此，公开  $R_i$  并不会暴露秘密份额  $s_i$ 。

攻击 3：攻击者试图从  $P_i$  的子秘密  $R_0^{s_i} \bmod N$  推导其秘密份额  $s_i$  从而进行攻击，与攻击 2 一样，这显然也是不可能的。

#### 3.2 动态性分析

(1) 当共享秘密  $S = \{S_1, S_2, \dots, S_m\}$  需要更新即删除或添加某个  $S_i$  时，各参与者的秘密份额不需要改变，秘密分发者只需更新公告牌上公布的信息  $S_i$  即可。

(2) 当需要删除某个成员  $P_i$  时，只需从公告牌上删除此成

员的信息  $(R_i, ID_i)$ ，然后在公开的信息  $MSG$  序列中删除  $f(ID_i) \oplus R_i^d \bmod N$  即可。当需要添加参与者  $P_{n+1}$  时，只需要计算参与者的个人信息  $(R_{n+1}, ID_{n+1})$ ，在公告牌上将其公布，然后计算  $f(ID_{n+1}) \oplus R_{n+1}^d \bmod N$ ，并放入  $MSG$  中进行公开。

#### 3.3 性能分析

通过以上的分析发现，本文提出的动态多秘密共享体制具有以下的特点：

(1) 是一个多秘密共享体制，每个参与者的秘密份额可以用于多次秘密共享过程。

(2) 参与者的秘密份额由自己选取，可防止秘密分发者的欺骗行为。

(3) 参与者秘密份额的提交可以经过公开的信道进行，无须事先建立安全信道。

(4) 能够防止外部的攻击，是一个可验证的秘密共享体制。

(5) 可以动态地更新秘密或动态地变动参与者，而参与者的秘密份额无须更改。

### 4 结束语

本文基于 Shamir 的门限方案和 RSA 密码体制，提出了一个动态的多秘密共享方案。该方案的参与者自行选取秘密份额，并且支持参与者的动态加入或退出以及秘密的动态更新。该方案还支持对参与者身份合法性的验证功能，并且不需要安全通道，更为实用。

### 参考文献

- [1] Chien H Y, Jan J K, Tseng Y M. A Practical  $(t, n)$  Multi-secret Sharing Scheme[J]. IEICE Transaction on Fundamentals, 2000, 83(12): 2762-2765.
- [2] Cachin C. On-line Secret Sharing[C]//Proc. of the 5th IMA Conf. on Cryptography and Coding. Berlin, Germany: Springer-Verlag, 1994.
- [3] Pinch R. On-line Multiple Secret Sharing[J]. Electronics Letters, 1996, 32(12): 1087-1088.
- [4] Hwang R J, Chang Chin-Chen. An On-line Secret Sharing Scheme for Multi-secrets[J]. Computer Communication, 1998, 21(13): 1170-1176.
- [5] 庞辽军, 李慧贤. 动态门限多重秘密共享方案[J]. 计算机工程, 2008, 34(15): 164-165.

编辑 张帆

(上接第 117 页)

### 5 结束语

本文对 FTP 服务的压力进行仿真，通过增加其他应用服务器，并参照目标网络环境中用户的网络访问行为对不同客户端配置不同的分布定义，可对更广泛的网络压力(如汇聚层交换机的处理能力、网络负载、特定服务器的服务响应时间等)进行仿真。对于网络规划和网络改造而言，如能在实施前获得关于网络压力的相关性能参数，无疑对网络的优化实施有很大的帮助。需要说明的是，当仿真环境中网络负荷较重或网络规模较大时，需要为仿真服务器配置较大的内存，建

议仿真机器的内存大于 1 GB。

### 参考文献

- [1] 徐磊, 李晓辉, 方红雨. 基于 OPNET 的 Ad Hoc 网络建模与仿真[J]. 计算机工程, 2009, 35(1): 123-125.
- [2] 伍俊洪, 杨洋, 李惠杰, 等. 网络仿真方法和 OPNET 仿真技术[J]. 计算机工程, 2004, 30(5): 106-108.
- [3] 李略. 基于 OPNET 的校园网优化设计与仿真[D]. 武汉: 华中科技大学.

编辑 任吉慧