文章编号:1001 - 9081(2007)09 - 2187 - 02

可选子密钥的门限多秘密共享方案

殷凤梅,侯整风
(合肥工业大学 计算机与信息学院, 合肥 230009)
(yinfm@163.com)

摘 要:现有的门限多秘密共享方案中,成员的子密钥是由庄家分发的,可能会导致庄家分发时的主动欺骗或无意欺骗,并且子密钥只能使用一次。针对这两个问题,基于离散对数求解的困难性提出了一个新的门限多秘密共享方案。该方案允许成员自主选择子密钥,子密钥可以重复使用,且不需要执行交互协议就能检测出庄家和参与者的欺诈。与现有方案相比,该方案的可行性更强、成员自主权更大,数据利用率更高。

关键词:多秘密共享;(t,n)门限方案;Lagrange 插值
中图分类号: TP309.7 **文献标志码**:A

Self-selecting share threshold multi-secret sharing scheme

YIN Feng-mei, HOU Zheng-feng
(*School of Computer and Information, Hefei University of Technology, Hefei Anhui* 230009, *China*)

Abstract: In the present threshold multi-secret sharing schemes, the dealer distributes share to every shareholder, which could lead to the dealer's intentional or unintentional cheating in shadow distribution, and the shareholder can only use share once. To solve these two problems, a new multi-secret sharing scheme based on the intractability of the discrete logarithm was presented. In this scheme, every shareholder's share is selected by himself (or herself), and the share can be reused, in addition, the cheating of the dealer and the cheating between shareholders can be detected without using interactive protocol. Compared with the existing schemes, the proposed scheme is more feasible, and the shareholders take more initiatives. Besides, the utilization ratio of the data is higher.

Key words: multi-secret sharing; (t, n) threshold scheme; Lagrange interpolation

0 引言

文献[1,2]分别基于 Lagrange 插值多项式和射影几何理论提出 (t,n) 门限的秘密共享方案,其含义是指由一个称为庄家(秘密分发者) 的人将一个秘密分发给 n 个成员(秘密分享者) 保存,其中至少 t 个合格成员共同合作便可恢复出原秘密。由此可知,每个成员的子密钥是由庄家产生的,成员自身无权选择,这就可能导致庄家在分发子密钥时的主动欺骗或无意欺骗,给实际应用带来诸多不便。

文献[3]首次提出了一个可以由成员自主选择子密钥的动态 (t,n) 门限方案(Hwang-Chwang 方案),该方案需要公开一个系统信息和为每位成员公开两个信息,这样一来要分存一个系统密钥就需要公开 $2n+1$ 个信息。在 Hwang-Chwang 方案的基础上,文献[4]提出了一个新的可自选子密钥的动态 (t,n) 门限方案,该方案在保持 Hwang-Chwang 方案优点的基础上,只需为每位成员公开一个信息,从而降低了存储开销。

在传统的秘密共享方案中,当秘密已被恢复,庄家必须为每个成员分发新的子密钥,在此过程中,每个成员的子密钥至多只能使用一次,数据的利用率非常低。为了让成员能重复使用子密钥,许多多秘密共享方案[5-9]应运而生。其中文献[6]首次提出一个能同时防止庄家与成员欺骗的多秘密共享方案。

本文在 Shamir 的 Lagrange 插值多项式的基础上,提出了一种可选子密钥的门限多秘密共享方案,其安全性依赖于离散对数求解的困难性。该方案具有以下特点:成员的子密钥不用庄家产生,而由成员自主选择,这给实际应用带来很多方便;每个成员的子密钥可以重复使用,以共享多个秘密,与文献[4]相比,数据的利用率明显提高;该方案能有效预防庄家欺诈及成员之间的欺骗,并且在检测欺诈过程中,不需要执行交互协议,与文献[6]相比,该方案更加切实可行。

1 可选子密钥的门限多秘密共享方案

本方案中有一个庄家(秘密分发者) 和 n 个成员(秘密分享者) 以及共享的 m 个秘密,其中每个秘密至少需要 t 个合格成员合作才能恢复。m 个秘密记为 $k_i(i=1,\cdots,m)$,n 个成员记为 $H_i(i=1,\cdots,n)$。

1.1 初始化

庄家选择大素数 p 和 q,且满足 $q \mid p-1$ 和 $q^2 \nmid p-1$;在 $GF(p)$ 中选择 m 个阶为 q 的生成元 $g_i(i=1,\cdots,m)$,以及另一生成元 g,并公布 g_i 和 g 的值。对于 m 个秘密 k_i,相应的有:

$$k_i = g_i^{a_0} \bmod p; i = 1,\cdots,m \quad (1)$$

选择单向函数 $H(\cdot)$,使其值域 $H(\cdot) \in [p^{\delta_1}]$,其中 $0 \leqslant \delta_1 \leqslant 1$ 为安全参数[10];选择一个 $t-1$ 次多项式:

收稿日期:2007 - 03 - 23;**修回日期**:2007 - 06 - 01。

作者简介:殷凤梅(1981 -),女,安徽肥东人,硕士研究生,主要研究方向:计算机网络、信息安全; 侯整风(1958 -),男,安徽和县人,教授,主要研究方向:网络安全、数据库。

$$f(x) = a_0 + a_1x + \cdots + a_{t-1}x^{t-1} \bmod q$$

计算并公布检测向量 $V = (v_0, v_1, \cdots, v_{t-1})$

其中：

$$v_k = g^{a_k} \bmod p; k = 0,1, \cdots, t-1 \quad (2)$$

1.2 子密钥的选取

每个成员 $H_i(i = 1, \cdots, n)$ 随机地选择一个 $s_i \in GF(p)$ 作为其子密钥，然后按照式(3)计算

$$p_i = g^{s_i} \bmod p \quad (3)$$

并将 p_i 发送给庄家(此处要求 s_i 各不相同)。收到以上 p_i 后，庄家随机选取一个元素 r，要求 r 与 $p-1$ 互素，并且 $r \neq s_i$，按照式(4)～(7)计算 y_i, c_i, R 和 Y_i，并把 y_i 发送给相应成员，公布 Y_i, c_i 和 R。

$$y_i = f(p_i{}^r) \bmod q \quad (4)$$

$$c_i = g^{p_i{}^r} \bmod p \quad (5)$$

$$R = g^r \bmod p \quad (6)$$

$$Y_i = g^{y_i} \bmod p \quad (7)$$

成员可以通过式(8)验证 y_i 的正确性。若式(8)成立，则成员 H_i 接受 y_i，否则拒绝 y_i。

$$Y_i = g^{y_i} \bmod p = \prod_{k=0}^{t-1} v_k{}^{x_i{}^k} \bmod p \quad (8)$$

1.3 秘密的恢复

任意 t 个合格成员若想恢复秘密 k_i，成员 $H_j(j = 1, \cdots, t)$ 按照式(9)、(10)计算并公布秘密份额 k_{ij} 和屏蔽子密钥 x_j：

$$k_{ij} = g_i{}^{y_j} \bmod p \quad (9)$$

$$x_j = R^{s_j} \bmod p \quad (10)$$

每个成员 H_j 选取 $c_{ij} \in [p^{1+\delta_1+\delta_2}]$，其中 δ_1, δ_2 为安全参数，且 $0 \leqslant \delta_1, \delta_2 \leqslant 1$[10]，计算：

$$w = g^{c_{ij}}$$

$$m = g_i{}^{c_{ij}}$$

$$b_{ij} = H(g, g_i, k_{ij}, Y_j, w, m)$$

并在整数环 Z 上计算 $y_{ij} = c_{ij} + b_{ij}y_j$，公布验证值：$\{y_{ij}, b_{ij}\}$；其他成员可以检测成员 H_j 提供的 k_{ij} 和 x_j 是否正确。若式(11)成立，则 H_j 提供的 k_{ij} 是正确的，若通过式(12)计算的 c_j' 满足 $c_j' = c_j$，则 H_j 提供的 x_j 是正确的；

$$b_{ij} = H(g, g_i, k_{ij}, Y_j, g^{y_{ij}}Y_j{}^{-b_{ij}}, g_i{}^{y_{ij}}k_{ij}{}^{-b_{ij}}) \quad (11)$$

$$c_j' = g^{x_j} \bmod p \quad (12)$$

那么秘密 k_i 可由式(13)恢复。

$$k_i = k_{i1}{}^{w(1)}k_{i2}{}^{w(2)}\cdots k_{it}{}^{w(t)} \bmod p \quad (13)$$

式中：

$$w(s) = \prod_{\substack{j=1 \\ j \neq s}}^{t} \frac{-x_j}{x_s - x_j} \bmod q \quad (14)$$

式(13)的正确性证明：

引理[6] $g_i{}^{t \bmod q} \bmod p = g_i{}^t \bmod p$

$$\because f(0) = \sum_{s=1}^{t} y_s w(s) \bmod q$$

$$\therefore k_i = g_i{}^{a_0} \bmod p =$$

$$g_i{}^{f(0)} \bmod p = g_{is}{}^{\sum_{s=1}^{t} y_s w(s) \bmod q} \bmod p =$$

$$g_i{}^{y_1 w(1) \bmod q} g_i{}^{y_2 w(2) \bmod q} \cdots g_i{}^{y_t w(t) \bmod q} \bmod p =$$

$$k_{i1}{}^{w(1)}k_{i2}{}^{w(2)}\cdots k_{it}{}^{w(t)} \bmod p$$

2 欺诈检测

在子密钥选取阶段，由于计算错误或分发错误，用户可能会从庄家那里得到不正确的数据 y_i；同样，在秘密恢复阶段，某成员 H_j 为了不让其他成员恢复出正确的秘密，可能会提供假的数据 k_{ij} 和 x_j。总之，无论是庄家的无意还是成员的有心，都将会造成原秘密最终无法恢复，因而，欺诈的检测非常重要。我们可以通过下面3个定理来检测欺诈，以保证秘密能正确恢复。

定理1 成员可以通过式(8)检测庄家发来的 y_i 的有效性。

证明

$$\because y_i = f(x_i) = a_0 + a_1x_i + \cdots + a_{t-1}x_i{}^{t-1} \bmod q$$

$$\therefore Y_i = g^{y_i} \bmod p = g^{a_0 + a_1x_i + \cdots + a_{t-1}x_i{}^{t-1} \bmod q} \bmod p =$$

$$\prod_{k=0}^{t-1} g^{a_k x_i{}^k} \bmod p = \prod_{k=0}^{t-1} v_k{}^{x_i{}^k} \bmod p$$

定理2 若由式(12)计算出的 c_j' 满足 $c_j' = c_j$，则成员 H_j 提供的 x_j 是正确的。

证明

由式(10)、(6)和(3)可知：

$$x_j = R^{s_j} \bmod p = (g^r)^{s_j} \bmod p = (g^{s_j})^r \bmod p = p_j{}^r \bmod p$$

$$c_j' = g^{x_j} \bmod p = g^{p_j{}^r} \bmod p = c_j$$

定理3 其他成员可以通过式(12)检测成员 H_j 提供的 k_{ij} 是否正确。

证明

$$\because g_i{}^{y_{ij}}k_{ij}{}^{-b_{ij}} = g_i{}^{y_{ij}}g_i{}^{-b_{ij}p_j} = g_i{}^{y_{ij}-b_{ij}p_j} = g_i{}^{c_{ij}} = m$$

$$g^{y_{ij}}Y_j{}^{-b_{ij}} = g^{y_{ij}}g^{-b_{ij}p_j} = g^{y_{ij}-b_{ij}p_j} = g^{c_{ij}} = w$$

$$\therefore H(g, g_i, k_{ij}, Y_j, g^{y_{ij}}Y_j{}^{-b_{ij}}, g_i{}^{y_{ij}}k_{ij}{}^{-b_{ij}}) =$$

$$H(g, g_i, k_{ij}, Y_j, w, m) = b_{ij}$$

3 方案分析

3.1 可行性

由定理2的证明可知 $x_i = p_i{}^r \bmod p$，又由式(4)可知：(x_i, y_i) 是 $t-1$ 次多项式 $f(x)$ 上的一个点。因为 $s_i \neq s_j (i \neq j)$(这是可以做到的。因为在实际应用中，p 远大于成员数 n，可以很容易地从 $GF(p)$ 中随机地选取 n 个不同的元素。如果某次选取出现碰撞(发生这种碰撞的概率非常小，几乎为零，并且不会连续发生)，庄家可以由收到的 p_i 检测出碰撞发生，于是要求每个成员重新选取子密钥)，由式(10)可知 $x_i \neq x_j$，即 t 个不同的成员可以恰好给出 $f(x)$ 上的 t 个不同的点，利用 Lagrange 插值算法可以恢复出 $t-1$ 次多项式，进而恢复出秘密 k_i。

3.2 安全性

本方案的安全性基于对离散对数问题的求解，而求解离散对数问题是非常困难的。

1) 当恢复出某一秘密 k_i 时，攻击者若试图通过式(1)获得 a_0，则必须求解离散对数问题，而离散对数的求解是非常困难的，因此 a_0 是安全的；

2) 同理，任何成员发送 p_i 给庄家，庄家不能通过式(3)获得 s_i，任何成员提交 x_i，其他成员不能通过式(10)获得 s_i，即

(下转第2199页)

连接至 GPRS 或 CDMA 移动网络,再插入智能卡,通过 VPNManager 连接至 VPN 服务器,随后通过 VPN 访问 Web 服务器。在 WLAN 的移动网络环境中,3 台 Pocket PC 先通过 AP 连接至互联网,再插入智能卡,通过 VPNManager 连接至 VPN 服务器,随后通过 VPN 访问 Web 服务器。

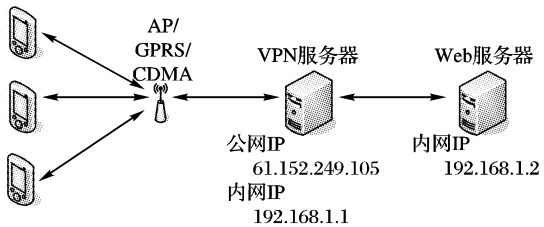

图 5　测试环境网络拓扑图

表 1　性能测试结果(s)

测试操作	VPN 建立连接	状态查询	VPN 断开连接	Web 服务访问
GRPS	8.2	0.6	0.8	4.2
CDMA	6.8	0.6	0.8	3.8
WLAN	3.3	0.6	0.8	1.3

表 2　安全性测试结果

测试操作	系统安全性表现
Pocket PC 插入智能卡后 PIN 码输入不正确	PIN 码输入不正确,不能进行 VPN 连接。三次输入 PIN 码不正确,系统自动锁死此智能卡
用过期或伪造证书进行 VPN 连接	不能进行 VPN 连接,并且系统会自动锁死此智能卡
使用不同用户的证书进行 VPN 连接,并访问 Web 服务器	SIS 的用户管理模块根据用户的访问控制列表进行权限控制,不同权限的用户具有不同的访问级别
嗅探、截获 MSS 传输过程中的数据包	用 Ethereal 查看了 VPN 传输的数据包,确认了 MMS 传输的数据包均用 ESP 封装加密
伪造 MSS 传输过程中的数据包	用流光等黑客工具伪造数据包攻击 SIS,SIS 自动断开连接,并自动过滤这个 IP 的数据包 3 h

测试中,3 台 Pocket PC 在三种移动网络环境下先分别进行 VPN 连接,VPN 连接状态查询和断开 VPN 连接等操作,一旦 VPN 连接成功,则每台 Pocket PC 被分配一个与 Web 服务器具有相同网段的 IP。然后分别测试了三种操作在三种移动网络环境下的系统响应时间,其中 VPN 建立连接时间包含移动网络连接的建立时间。最后测试了 Pocket PC 访问 Web 服务器的响应时间。每项操作均测试了 20 次,测试结果为平均值,测试结果如表 1 所示。

通过多种方式测试了 MSS 的安全性,测试结果如表 2 所示。

由上述安全性测试结果可以看出,MSS 有效保证了移动网络和固定网络之间信息交换的安全性,使得固网信息能够安全无缝地移动扩展。

4　结语

IPSec 在 IP 层上提供了安全服务,对高层协议透明,本文设计并实现了一套完整的基于 IPSec VPN 的移动安全系统 MSS。它有助于将基于固网的信息系统和数据服务安全无缝地移动扩展,凡是覆盖移动通讯网络(GPRS/CDMA/3G/WLAN)的地方,MSS 能够很好满足公安、政务、国防、航运、物流等国家关键业务系统工作中具有的移动性、突发性和紧急性的特点。

参考文献:

[1] STALLINGS W. Cryptography and network security: principles and practice [M]. 4th ed. New Jersey: Prentice Hall, 2006.

[2] TANENBAUM A S. Computer networks [M]. 4th ed. [S. l.]: Pearson education, 2004.

[3] NASH A. PKI implementing and managing e-security [M]. [S. l.]: McGraw-Hill, 2004.

[4] RFC 2764, A framework for IP based virtual private networks[S].

[5] RFC 2409, The Internet key exchange[S].

[6] RFC 2459, Internet X.509 public key infrastructure certificate and CRL profile[S].

(上接第 2188 页)

每个成员的子密钥 s_i 并不会因为任一秘密的恢复而公开;

3) 当已恢复出某一秘密 k_i 时,若内部成员企图通过收集到的 t 个 k_{ij} 和 $x_j(j=1,\cdots,t)$ 恢复另一秘密 k_u,根据离散对数的难解性,其无法通过式(9)得到 $y_j(j=1,\cdots,t)$,因而无法得到 $k_{uj}(j=1,\cdots,t)$,继而不能恢复出秘密 k_u。

4　结语

本文提出的门限多秘密共享方案,允许成员自主选择子密钥,并且子密钥可以重复使用以共享多个秘密,同时本方案在检测欺诈过程中,不需要执行交互协议,从而能有效预防庄家和成员的欺诈。与已有的方案相比,本方案的可行性更强,成员的自主权更大,数据的利用率更高。在保密通信,数据库安全以及电子商务等众多领域本方案有广阔的应用前景。

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 R. Safeguarding cryptographic keys[C]// Proceedings AFIPS 1979 National Computer Conference. New York: AFIPS, 1979: 313 - 317.

[3] HWANG S J, CHANG C C, YANG W P. An efficient dynamic threshold scheme[J]. IEICE Transactions on Information and Systems, 1996, E79-D(7): 936 - 942.

[4] 申一頔, 刘焕平. 可选子密钥的秘密共享方案[J]. 哈尔滨师范大学自然科学学报, 2006, 22(1): 54 - 57.

[5] CHIEN H Y, JAN J K, TSENG Y M. A practical(t, n) multi-secret sharing scheme [J]. IEICE Transaction on Fundamentals, 2000, E83-A(12): 2762 - 2765.

[6] HARN L. Efficient sharing (broadcasting) of multiple secrets [J]. IEE Computers and Digital Techniques, 1995, 142(3): 237 - 240.

[7] YANG C C, CHANG T Y, HWANG M S. A (t, n) multisecret sharing scheme[J]. Applied Mathematics and Computation, 2004, 151(2): 483 - 490.

[8] HE W H, WU T S. Comment on Lin-wu (t, n) threshold verifiable multisecret sharing scheme[J]. IEE Computers and Digital Techniques, 2001, 148(3): 139 - 141.

[9] 许春香, 肖国镇. 门限多重秘密共享方案[J]. 电子学报, 2004, 32(10): 1687 - 1689.

[10] GENNARO R, JARECKI S, KRAWCZYK H. *et al.* Robust and efficient sharing of RSA functions [C]//Advanced in Cryptology-CRYPTO' 96 Proceedings. Berlin: Springer-Verlag, 1996: 157 - 172.