基于单向函数的动态密钥分存方案*

刘焕平[1,2], 胡铭曾[2], 方滨兴[2], 杨义先[3]

[1](哈尔滨师范大学 信息科学系,黑龙江 哈尔滨 150080);
[2](哈尔滨工业大学 计算机科学与技术学院,黑龙江 哈尔滨 150001);
[3](北京邮电大学 信息安全中心,北京 100876)
E-mail: hpliu@0451.com
http://www.hrbnu.edu.cn

摘要: 给出了一个基于单向函数的动态(t,n)-门限方案,它具有下述特点:(1) 系统在更新系统密钥时,无须更改每个成员的子密钥;(2) 当某个成员的子密钥泄密时,系统只需为该成员重新分配子密钥而不必更改其他成员的子密钥;(3) 当有新成员加入时,系统只需为新成员分配一个子密钥,而其他成员不受任何影响;(4) 子密钥可无限制地多次使用;(5) 只需公开 n+1 个信息(在需要确认欺骗者时需公开 2n+1 个);(6) 恢复系统密钥时,采用并行过程.

关键词: 数据安全;密码学;密钥分存方案;单向函数
中图法分类号: TP393 文献标识码: A

在保密通信中,为了实现信息的安全保密,人们主要采用密钥加密信息,从而使不拥有密钥的非法用户无法窃获信息.这使得信息的安全保密主要维系于密钥的安全,从而如何有效地管理密钥就成为密码学中十分重要的课题.1979 年,Shamir[1]和 Blakley[2]独立地提出了密钥分散管理的概念,实现这一思想的机制称为(t,n)-门限方案.该方案是将一个密钥(称为系统密钥)分成 n 个部分(称为 n 个子密钥),分别交给 n 个人保管,使得对确定的整数 t(t<n)满足:(1) 在这 n 个人中,任意 r(r≥t)个人协作都能恢复出系统密钥;(2) 任意 r(r<t)个人协作对恢复系统密钥没有任何帮助.这种密钥分散管理的思想使密钥管理更加安全灵活.目前,这一思想除用于密钥管理之外,在密码学的其他领域(如组签名和组认证等方面)也有诸多应用.

在(t,n)-门限思想提出以后,很多学者对其进行了研究,并提出了许多方案[1~10]来实现它.在早期提出的(t,n)-门限方案[1~3]中大都存在下述几方面的不足:(1) 当要更新系统密钥(比如原密钥已恢复或由于某种原因而需要更换原密钥)时,系统必须为每个成员重新分配子密钥(尽管这些子密钥可能还从未被用过),即每个子密钥至多只能使用一次;(2) 当某个成员的子密钥泄密时,系统不能做到只为该成员重新分配子密钥而不影响其他成员的子密钥;(3) 当有新成员加入时,系统也必须重新为每个成员分配子密钥.为了克服上述不足,人们又提出了许多能够重复使用子密钥的(t,n)-门限方案[4~6],但是这些子密钥只能保存或恢复系统预先确定的一个密钥集合中的密钥,而要保存一个新的密钥(确定密钥集合之外的密钥),系统则必须更新每个成员的子密钥.

文献[7,8]在 t=n 的情形下,分别给出了一个可无限制地多次使用子密钥来恢复系统密钥的(n,n)-门限方案,但在恢复系统密钥时,所有成员必须根据一个强制性序列(即一个串行过程)$m_1,m_2,\ldots,m_n$ 来恢复系统密钥,这样,在恢复密钥时势必要造成一个较大的时间开销.

* 收稿日期: 2000-04-18; 修改日期:2001-04-27
基金项目: 黑龙江省科委基金资助项目(G99A10-3);哈尔滨师范大学杰出青年基金资助项目

作者简介: 刘焕平(1965－),男,山东安丘人,博士,副教授,主要研究领域为密码学,互联网络结构分析,应用数学;胡铭曾(1935－),男,江苏江阴人,教授,博士生导师,主要研究领域为高性能计算机系统结构,并行处理技术,信息安全;方滨兴(1960－),男,江西万年人,博士,教授,博士生导师,主要研究领域为网络安全,网络技术,并行处理技术,计算机体系结构;杨义先(1961－),男,四川绵阳人,博士,教授,博士生导师,主要研究领域为信息安全,现代密码学,电子商务系统,信号理论,编码理论.

文献[9]给出了一个一般访问结构的在线多密钥分存方案,该方案为每个极小合法成员组发布一组公开信息.我们认为,该方案对许多情形来说过于复杂,如对经常使用的(t,n)-门限,利用该方案需计算$O(C_n^t)$个公开信息(因为此种情形下共有C_n^t个极小合法成员组),这样的计算量是指数级的,所公开的信息量也是指数级的.

本文在文献[4]的基础上,给出了一个基于单向函数的动态(t,n)-门限方案,它具有下述特点:(1) 系统在更新系统密钥时,无须更改每个成员的子密钥;(2) 当某个成员的子密钥泄密时,系统只需为该成员重新分配子密钥而不必更改其他成员的子密钥;(3) 当有新成员加入时,系统只需为新成员分配一个子密钥,而其他成员不受任何影响;(4) 子密钥可无限制地多次使用;(5) 只需公开$O(n)$(而非$O(C_n^t)$个信息);(6) 恢复系统密钥时,采用并行过程.

1 原始方案

设$GF(p)$是有限域,$f:GF(p)\to GF(p)$是单向函数(即:由$y=f(x)$求x在计算上是不可能的),对$x\in GF(p)$,定义$f^0(x)=x$, $f^j(x)=f(f^{j-1}(x))$.$P_1,P_2,\ldots,P_n$是系统中的n个成员.$[a,b]$表示介于整数a,b之间的所有整数作成的集合,包括a,b.

He等人在文献[4]中给出的基于单向函数的多级(t,n)-门限方案如下:

初始化:系统D随机地选取n个不同的元素x_i作为$P_i(i=1,\ldots,n)$的公开信息(公开),再任选n个元素$y_i\in[1,p-1]$(可以相同)作为$P_i(i=1,\ldots,n)$的子密钥(保密).然后系统D执行如下过程:

(1) 对$j=0,1,\ldots,k-1$,重复下述步骤:

(i) 任选一个$(t-1)$次多项式$h_j(x)$且$h_j(0)=s_j$为第j个共享密钥;

(ii) 计算$d_{ji}=h_j(x_i)-f^j(y_i)(i=1,\ldots,n)$.

(2) 将y_i秘密地送给P_i,并公开$d_{ji}(i=1,2,\ldots,n;j=0,1,\ldots,k-1;i=1,\ldots,n)$.

密钥按$S_k,S_{k-i},\ldots,S_l$的顺序恢复.任意t个子密钥持有者(不妨设他们是$P_1,P_2,\ldots,P_t$)要恢复第j个密钥S_j时,只需每个P_i提供$h_j(x_i)=d_{ji}+f^j(y_i)(i=1,2,\ldots,t)$,就可由$t$个不同的点$(x_1,h_j(x_1)),\ldots,(x_t,h_j(x_t))$恢复出$(t-1)$次多项式$h_j(x)$,进而得到$S_j=h_j(0)$.

经分析可知,在上述方案中,要保存的系统密钥应预先确定好,并且一旦这些系统密钥被确定好之后,每个成员的子密钥就只能用来保存和恢复这些被确定好的系统密钥,而要保存这些密钥之外的系统密钥,就需要更新每个成员的子密钥.也就是说,在该方案中,子密钥的多次使用是受限制的.

2 我们给出的方案

我们在文献[4]的基础上给出了如下无限制的多次使用子密钥的(t,n)-门限方案.

2.1 系统初始化

设$GF(p)$是有限域,$f:GF(p)\to GF(p)$是一个无碰撞的单向函数,公开f.

(1) 系统D随机地选取n个不同的元素$s_1,s_2,\ldots,s_n\in GF(p)$,并将$s_i$通过安全信道秘密地递给$P_i(i=1,\ldots,n)$;

(2) 系统D随机地选取一个元素$\alpha\in GP(p)$,一个$(t-1)$次多项式$h(x)$,满足$h(0)=K$为要保存的系统密钥.之后计算:

$$y_i=h(f(\alpha+s_i)),\ \text{for } i=1,2,\ldots,n;$$

(3) 系统D在公告牌上公开α及有序数组$(y_1,y_2,\ldots,y_n)$.

2.2 密钥恢复

当任意t个子密钥持有者(不妨设他们是$P_1,P_2,\ldots,P_t$)要恢复系统密钥时,每个成员P_i只需在公告牌上查到α和y_i后,计算$x_i=f(\alpha+s_i)$,并提交x_i(x_i称为P_i的屏蔽子密钥).在汇总所有的$(x_i,y_i),i=1,2,\ldots,t$之后,利用Lagrange内插法恢复出$h(x)$,进而可恢复出系统密钥$K=h(0)$.

3 性能分析

(1) 可行性:由 $x_i = f(\alpha + s_i)$ 及 $y_i = h(f(\alpha + s_i))$ 可知,(x_i,y_i)是 $h(x)$上的一个点.再注意到 $f(x)$是无碰撞的单向函数及 $s_i \neq s_j (i \neq j)$,故有 $x_i \neq x_j (i \neq j)$.于是在恢复密钥时,t 个成员 $P_1,P_2,\ldots,P_t$ 恰好可以给出 $h(x)$上的 t 个不同的点$(x_i,y_i)(i=1,\ldots,t)$,而 $h(x)$是 $t-1$ 次多项式,故可由这 t 个点确定出来,进而可将系统密钥 $K=h(0)$恢复出来.因此上述方案可行.

(2) 安全性:本方案的安全性基于单向函数不可求逆这一特性.第 1,在恢复密钥时,每个成员提交的是其屏蔽子密钥 $x_i = f(\alpha + s_i)$,由于 f 是单向函数,故其他成员无法通过α及 x_i 求出 P_i 的子密钥 s_i.即每个成员的子密钥并没有因为系统密钥的恢复而被公开,从而可继续使用;第 2,同样由于 f 是单向函数,任何成员无法通过系统公开的信息α及有序数组$(y_1,y_2,\ldots,y_n)$来获取其他成员的子密钥及其屏蔽子密钥.

(3) 系统更新:

(a) 原系统密钥 K 尚未被恢复,只是出于某种原因而需要更换系统密钥.此时,系统只需重新选择一个 $t-1$ 次多项式 $h'(x)$,满足 $h'(0)=K'$为新的系统密钥.然后利用新的 $t-1$ 次多项式 $h'(x)$更新公告牌上的有序数组$(y_1,y_2,\ldots,y_n)$即可.

(b) 原系统密钥 K 已被恢复,现在要保存新的系统密钥 K'.此时,系统选择一个新的本原元 $\alpha'(\alpha' \neq \alpha)$ 及 $t-1$ 次多项式 $h'(x)$,满足 $h'(0)=K'$为新的系统密钥.然后利用新的 α' 及 $h'(x)$更新公告牌上的α及有序数组$(y_1,y_2,\ldots,y_n)$即可.

由于α是 $GF(p)$的任意元素,故每个成员的子密钥可以无限制地被多次使用.

(4) 确认欺骗者:该方案可以很容易修改为一个可确认欺骗者的动态(t,n)-门限方案.此时,系统只需为每个成员 P_i 公开一个检测信息:$v_i=f(x_i)$,其中 $x_i = f(\alpha + s_i)$.在恢复密钥时,其他成员可以通过检验等式 $v_i=f(x_i)$(此处 x_i 是 P_i 的屏蔽子密钥)是否成立来确认成员 P_i 是否欺骗者.注意,由于 $f(x)$是单向函数,故任何成员无法通过系统公开的信息α, y_i 及 v_i 来获取成员 P_i 的子密钥和屏蔽子密钥.

(5) 当有新成员 P_{n+1} 加入时,系统只需为新成员 P_{n+1} 随机地生成一个子密钥 s_{n+1},并在公告牌上的有序数组$(y_1,y_2,\ldots,y_n)$中增加一个元素 y_{n+1},其中 $y_{n+1} = f(\alpha + s_{n+1})$ 即可;当要删除某个成员 P_i 时,系统只需重新选择一个 $t-1$ 次多项式 $h'(x)$,满足 $h'(0)=K$ 为系统密钥,然后利用新的 $t-1$ 次多项式 $h'(x)$更新公告牌上的有序数组$(y_1,y_2,\ldots,y_n)$,此时无须计算 y_i(可令 y_i 仍为原值或置 y_i 项为空),那么 P_i 原有的子密钥 s_i 即可无效.

(6) 当某个成员 P_i 的子密钥泄密时,系统只需为该成员重新分配子密钥 s'_i,之后重新选择一个 $t-1$ 次多项式 $h'(x)$,满足 $h'(0)=K$ 为系统密钥,并利用新的 s_i 和 $h'(x)$更新公告牌上的有序数组$(y_1,y_2,\ldots,y_n)$,而不必更改其他成员的子密钥.

致谢 感谢哈尔滨工业大学计算机科学与技术系体系结构教研室的全体老师所给予的支持与帮助.

References:

[1] Shamir, A. How to share a secret. Communications of the ACM,1979,22(11):612~613.

[2] Blackley, G.R. Safeguarding cryptographic keys. In: Proceedings of the National Computer Conference of AFIPS. 1979. 313~317. http://citeseer.nj.nec.com/contest/7527/0

[3] Tompa, M., Woll, H. How to share a secret with cheater. Journal of Crypto, 1988,1(2):133~138.

[4] He, J., Dawson, E. Multistage secret sharing based on one-way function. Electronics Letters, 1994,30(19):1591~1592.

[5] Harn, L. Comment: multistage secret sharing based on one-way function. Electronics Letters, 1995,31,(4):262~263.

[6] Liu, Huan-ping, Yang, Yi-xian, Yang, Fang-chun. Multistage secret sharing schemes based on one-way function. Journal of Electronics, 1999,21(4):561~564 (in Chinese).

[7] Pinch, R.G.E. Online multiple secret sharing. Electronics Letters,1996,32(12):1087~1088.

[8] Tan, Kai-jun, Chu, Hong-wen. Dynamic sharing based on one-way function. Journal of China Institute of Communications, 1999, 20(7):81~84 (in Chinese).

[9] Sun, H.M. On-Line multiple sharing based on one-way function. Computer Communications, 1999,22(8):745~747.

[10] Liu, Huan-ping, Yang, Yi-xian. A generalized (*k*,*n*)-threshold secret sharing scheme. Journal of China Institute of Communications, 1998,19(8):72~75 (in Chinese).

附中文参考文献:

[6] 刘焕平,杨义先,杨放春.基于单向函数的多级密钥共享方案.电子科学学刊,1999,21(4):561~564.

[8] 谭凯军,诸鸿文.基于单向函数的动态秘密分享机制.通信学报,1999,20(7):81~84.

[10] 刘焕平,杨义先.广义(*k*,*n*)-门限方案.通信学报,1998,20(8):72~75.

A Dynamic Secret Sharing Scheme Based on One-Way Function*

LIU Huan-ping[1,2], HU Ming-zeng[2], FANG Bin-xing[2], YANG Yi-xian[3]

[1](*Department of Information Science*, *Harbin Normal University*, *Harbin* 150080, *China*);

[2](*College of Computer Science and Technology*, *Harbin Institute of Technology*, *Harbin* 150001, *China*);

[3](*Center of Information Security*, *Beijing University of Posts and Telecommunications*, *Beijing* 100876, *China*)

E-mail: hpliu@0451.com

http://www.hrbnu.edu.cn

Abstract: A dynamic (*t*,*n*)-threshold secret sharing scheme based on one-way function is proposed in this paper. It has the following properties: (1) The dealer can renew system secrets without renewing the shadows of the participants; (2) When some participants' shadows are revealed, they can be renewed without any effect on the others; (3) A new shadow can be generated for a new participant without any effect on the others; (4) The shadows can be reused for many times; (5) Only *n*+1 parameters should be public (When a cheater could be checked out, it should be opened 2*n*+1 parameters.); (6) The system secret can be recovered with a parallel process.

Key words: data security; cryptography; secret sharing scheme; one-way function

* Received April 18, 2000; accepted April 27, 2001

Supported by the Science and Technology Foundation of Heilongjiang Province of China under Grant No.G99A10-3; the Outstanding Youth Foundation of Harbin Normal University of China