基于单向函数的多级密钥共享方案 [1]

刘焕平　　杨义先　　杨放春 *

(北京邮电大学信息安全中心 126 信箱 北京 100876)
*(北京邮电大学程控交换技术与通信网国家重点实验室 北京 100876)

摘 要 本文在 Harn 于 1995 年指出的一个多级密钥 (t,n)-门限密钥共享方案的基础上，给出了两个新的多级密钥 (t,n)-门限密钥共享方案，该方案能够检测欺骗者.

关键词 数据安全，密码学，密钥共享

中图号 TN918.1

1 引 言

He 等在文献 [1] 中利用单向函数给出了一个基于计算安全的 (t,n)-门限多级密钥共享方案，该方案允许每个密钥共享者重复使用其子密钥，但在分享 k 个密钥时，须公开 kn 个信息. Harn 在 He 等的基础上给出了一个修改方案 [2]，只须公开 $k(n-t)$ 个信息. 但是这两个方案均不具有检测欺骗者的功能. 本文在 Harn 方案的基础上，给出了两个新的多级密钥 (t,n)-门限密钥共享方案，该方案能够检测欺骗者.

2 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 $f^0(x)=x$，$f^j(x)=f(f^{j-1}(x))$． $[a,b]$ 表示介于整数 a,b 之间的所有整数作成的集合，包括 a,b．

2.1 He 等所给方案 (记为 MSS1)

初始化 $\mathcal{D}$ 随机地选取 n 个不同的元素 x_i 作为 P_i $(i=1,\cdots,n)$ 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 $(i=1,\cdots,n)$ 的子密钥 (保密)．然后 $\mathcal{D}$ 执行如下过程:

(1) 对 $j=0,1,\cdots,k-1$，重复下述步骤:

(a) 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;

(b) 计算 $d_{ji}=h_j(x_i)-f^j(y_i)$ $(i=1,\cdots,n)$;

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

密钥按 $s_k,s_{k-1},\cdots,s_1$ 的顺序恢复. 任意 t 个子密钥持有者 (不妨设他们是 $P_1,P_2,\cdots,P_t$) 要恢复第 j 个密钥 s_j 时，只须每个 P_i 提供 $h_j(x_i)=d_{ji}+f^j(y_i)$ $(i=1,2,\cdots,t)$，就可由 t 个不同的点 $(x_1,\ h_j(x_1)),\cdots,\ (x_t,\ h_j(x_t))$ 恢复出 $(t-1)$ 次多项式 $h_j(x)$，进而得到 $s_j=h_j(0)$．

[1] 1998-02-27 收到， 1998-10-14 定稿
国家自然科学基金资助课题 (批准号: 69772035, 69896240, 69896243), 国家 "863" 项目

2.2 Harn 的方案 (记为 MSS2)

初始化 $\mathcal{D}$ 随机地选取 n 个不同的整数 $x_i \in [n-t+1,\ p-1]$ 作为 P_i $(i=1,\cdots,n)$ 的公开信息 (公开)，再任选 n 个整数 $y_i \in [1,\ p-1]$(可以相同) 作为 P_i $(i=1,\cdots,n)$ 的子密钥 (保密)。然后 $\mathcal{D}$ 执行如下过程:

(1) 对 $j=0,1,\cdots,k-1$，重复下述步骤:

(a) 计算 $f^j(y_i)$, $i=1,2,\cdots,n$；

(b) 利用 Lagrange 内插法 [3] 构造一个 $(n-1)$ 次多项式 $h_j(x)$, 使点 $(x_i,\ f^j(y_i))$ $(i=1,2,\cdots,n)$ 在 $h_j(x)$ 上，且 $h_j(0)=s_j$ 为第 j 个共享密钥;

(c) 计算 $h_j(m)$, $m=1,2,\cdots,n-t$；

(2) 将 y_i 秘密地送给 P_i，并公开 $h_j(m)$, $i=1,2,\cdots,n$; $j=0,1,\cdots,k-1$; $m=1,\cdots,n-t)$。

密钥按 $s_{k-1},\cdots,s_1,s_0$ 的顺序恢复。任意 t 个子密钥持有者 (不妨设他们是 $P_1,P_2,\cdots,P_t$) 要恢复第 j 个密钥 s_j 时，只须每个 P_i 提供 $f^j(y_i)$，于是得到 $h_j(x)$ 上的 n 个不同的点 $(x_1,\ f^j(y_1)),\cdots,\ (x_t,\ f^j(y_t)),(1,\ h_j(1)),\cdots,(n-t,\ h_j(n-t))$，从而可恢复出 $(n-1)$ 次多项式 $h_j(x)$，进而得到 $s_j=h_j(0)$。

2.3 对上述两方案的分析

我们认为这两个方案有一个共同的缺陷。事实上，由于每个 P_i 的子密钥 y_i 可以相同，因此当 (比如说) $y_1=y_2$ 时，就应有 $f^j(y_1)=f^j(y_2)$, $j=0,1,\cdots,k-1$。于是在恢复密钥 s_{k-1} 时，P_2 会发现 $f^{k-1}(y_1)=f^{k-1}(y_2)$，这样 P_2 就可以推断出 $f^{k-2}(y_1)=f^{k-2}(y_2)$，从而在恢复密钥 s_{k-2} 时，P_2 可以给出两个不同的点，其中在 MSS1 时给出 $h_{k-2}(x)$ 上的两个不同的点是: $(x_1,\ h_{k-2}(x_1))$ (因为 $h_{k-2}(x_1)=d_{k-2,1}+f^{k-2}(y_1)=d_{k-2,1}+f^{k-2}(y_2)$，而 $d_{k-2,1}$ 是公开的) 和 (x_2,h_{k-2})；而在 MSS2 时给出的两个不同的点是: $(x_1,\ f^{k-2}(y_1))$ 和 $(x_2,f^{k-2}(y_2))$，于是 $t-1$ 个成员 $P_2,P_3,\cdots,P_t$ 就能恢复出 s_{k-2}。即使将这两个方案中的 y_i 限制为彼此不同，上述缺陷仍无法克服！因为对不同的 y_1,y_2，很可能存在 j_0 使 $f^{j_0}(y_1)=y_2$，于是 $f^{j+j_0}(y_1)=f^j(y_2)$, $j=0,1,\cdots,k-j_0-1$。当恢复密钥 s_{k-1} 时，P_2 就会发现 $f^{k-1}(y_1)=f^{k-j_0-1}(y_2)$，这样 P_2 就可以推断出 $f^{k-2}(y_1)=f^{k-2-j_0}(y_2)$，从而在恢复密钥 s_{k-2} 时，P_2 可以给出 $h_{k-2}(x)$ 上两个不同的点，于是 $t-1$ 个成员 $P_2,P_3,\cdots,P_t$ 仍能恢复出 s_{k-2}。例如: 设 $p=29$，单向函数 $f(x)=2^x \pmod{29}$，$k=6,y_1=5,y_2=8$，则有 $f^2(y_1)=y_2=8,\cdots,f^5(y_1)=f^3(y_2)=23$。当恢复密钥 $s_{k-1}=s_5$ 时，就会发现 $f^5(y_1)=f^3(y_2)$，这样 P_2 就可以推断出 $f^4(y_1)=f^2(y_2)=20$，从而在恢复密钥 s_4 时，P_2 可以给出 $h_4(x)$ 上两个不同的点，即 P_2 一人可以起到 P_1、P_2 两个人的作用。

3 我们给出的修改方案及其安全分析

我们在文献 [2] 的基础上给出了如下修改方案，它能够检测欺骗者。

方案 1 设 GF(p) 是有限域，f_i :GF$(p)\to$GF(p) $(i=1,2,\cdots,n)$ 是 n 个不同的单向函数。

初始化 $\mathcal{D}$ 随机地选取 n 个不同的整数 $x_i \in [n-t+1,\ p-1]$ 作为 $P_i\ (i=1,\cdots,n)$ 的公开信息（公开），再任选 n 个整数 $y_i \in [1,\ p-1]$（可以相同）作为 $P_i\ (i=1,\cdots,n)$ 的子密钥（保密）。然后 $\mathcal{D}$ 执行如下过程：

(1) 对 $j=0,1,\cdots,k-1$，重复下述步骤：

(a) 计算 $f_i^j(y_i)$，$i=1,2,\cdots,n$；

(b) 利用 Lagrange 内插法构造一个 $(n-1)$ 次多项式 $h_j(x)$ 使点 $(x_i,\ f_i^j(y_i))$ $(i=1,2,\cdots,n)$ 在 $h_j(x)$ 上，且 $h_j(0)=s_j$ 为第 j 个共享密钥；

(c) 计算 $h_j(m)$，$m=1,2,\cdots,n-t$ 和 $v_i=f_i^k(y_i)$，$i=1,\cdots,n$；

(2) 将 y_i 秘密地送给 P_i，并公开 $h_j(m)$ 和 $f_i^k(y_i), i=1,2,\cdots,n;\ j=0,1,\cdots,k-1;\ m=1,\cdots,n-t$。

密钥按 $s_{k-1},\cdots,s_1,s_0$ 的顺序恢复。任意 t 个子密钥持有者（不妨设他们是 $P_1,P_2,\cdots,P_t$）要恢复第 j 个密钥 s_j 时 $(j=0,1,\cdots,k-1)$，只须每个 P_i 提供 $f_i^j(y_i)$，然后每个 P_i 验证等式 $v_i=f^{k-j}(f^j(y_i))$，$i=1,\cdots,t$，于是得到 $h_j(x)$ 上的 n 个不同的点 $(x_1,\ f_i^j(y_1)),\cdots,(x_t,\ f_i^j(y_t)),(1,\ h_j(1)),\cdots,(n-t,\ h_j(n-t))$，从而可恢复出 $(n-1)$ 次多项式 $h_j(x)$，进而得到 $s_j=h_j(0)$。

安全分析 由于 f_i 是单向函数，故由 $f_i^j(x)$ 得不到 $f_i^{j-1}(x)$ $(i=1,\cdots,n; j=1,\cdots,k)$，即由 P_i 公开的信息得不到 P_i 未公开的信息。另一方面，由于 $f_i\ (i=1,\cdots,n)$ 是互不相同的单向函数，于是任意一组成员（不包括 P_i）汇集他们自己的信息以及 P_i 公开的信息仍无法得到 P_i 未公开的信息。因此这一方案是安全的。

该方案实现的难易程度取决于 n 个不同的单向函数是否容易找到。当很 n 大时，不一定容易实现，为此给出下述方案。

方案 2 设 $GF(p)$ 是有限域，$f: GF(p) \to GF(p)$ 是单向函数。

初始化 $\mathcal{D}$ 随机地选取 n 个不同的整数 $x_i \in [n-t+1,\ p-1]$ 作为 $P_i\ (i=1,\cdots,n)$ 的公开信息（公开），再任选 n 个有序整数对 $(v_i,\ y_i) \in [1,\ p-1]^2$ 作为 $P_i\ (i=1,\cdots,n)$ 的子密钥（保密），要求 $v_i \neq v_j (i \neq j)$。然后 $\mathcal{D}$ 执行如下过程：

(1) 对 $j=0,1,\cdots,k-1$，重复下述步骤：

(a) 计算 $f^{v_i j}(y_i)$，$i=1,2,\cdots,n$；

(b) 利用 Lagrange 内插法构造一个 $(n-1)$ 次多项式 $h_j(x)$ 使点 $(x_i,\ f^{v_i j}(y_i))$ $(i=1,2,\cdots,n)$ 在 $h_j(x)$ 上，且 $h_j(0)=s_j$ 为第 j 个共享密钥；

(c) 计算 $h_j(m)$，$m=1,2,\cdots,n-t$；

(2) 将 $(v_i,\ y_i)$ 秘密地送给 P_i，并公开 $h_j(m)$，$i=1,2,\cdots,n;\ j=0,1,\cdots,k-1;\ m=1,\cdots,n-t$）。

密钥按 $s_{k-1},\cdots,s_1,s_0$ 的顺序恢复。任意 t 个子密钥持有者（不妨设他们是 $P_1,P_2,\cdots,P_t$）要恢复第 j 个密钥 s_j 时，只须每个 P_i 提供 $f^j(y_i)$，于是得到 $h_j(x)$ 上的 n 个不同的点 $(x_1,\ f^{v_1 j}(y_1)),\cdots,(x_t,\ f^{v_t j}(y_t)),(1,\ h_j(1)),\cdots,(n-t,\ h_j(n-t))$，从而可恢复出 $(n-1)$ 次多项式 $h_j(x)$，进而得到 $s_j=h_j(0)$。

安全分析 由于是 f 单向函数，故由 $f^{v_i j}(x)$ 得不到 $f^{v_i(j-1)}(x)$ $(i = 1, \cdots, n; j = 1, \cdots, k)$，即由 P_i 公开的信息得不到 P_i 未公开的信息．另一方面，由于 v_i 是互不相同的整数，于是由 $f^{v_i j}(y_i) = f^{v_t j'}(y_t)$ 得不到 $f^{v_i(j-1)}(y_i) = f^{v_t(j'-1)}(y_t)$，即其他人由自己的信息以及 P_i 公开的信息得不到 P_i 未公开的信息，因此这一方案克服了文献 [1,2] 所给方案的不足之处．

致谢 感谢北京商儒信息技术有限责任公司的大力支持．

参 考 文 献

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

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

[3] Shamir A. How to share a secret, Commun. ACM, 1979, 22(11): 612–613.

MULTISTAGE SECRET SHARING BASED ON ONE-WAY FUNCTION

Liu Huanping Yang Yixian Yang Fangchun

(*Dept. of Infor. Eng., Beijing University of Posts and Telecommunications, Beijing* 100876)

Abstract This paper points out the drawback of the secret sharing schemes proposed by J.He, *et al.* (1994) and L. Harn(1995). This paper also gives the secret sharing schemes, which overcome the above mentioned drawback.

Key words Data security, Crypotograph, Secret sharing scheme

刘焕平： 男，博士生．攻读密码学专业．

杨义先： 男， 1961 年生，教授，博士生导师，全国政协委员，主要从事密码、信号理论、纠错编码等领域的教学和研究工作．

杨放春： 男， 1958 年生，教授，博士生导师，从事通信技术的教学和研究工作．