计算机科学 2006Vol. 33№. 8

基于埃尔米特插值的秘密分割门限方案的构造*)

杜伟章[1]　陈克非[2]

(烟台大学计算机学院　烟台 264005)[1]　(上海交通大学计算机科学与工程系　上海 200030)[2]

摘　要　该文在 Shamir 门限方案的基础上，利用埃尔米特插值构造了一个秘密分割门限方案，证明了方案构造的可行性，并对它的安全性进行了讨论。

关键词　埃尔米特插值，秘密分割，门限方案

Construction of Threshold Scheme on Share of Secret Based on the Problem of Hermite Interpolation

DU Wei-Zhang[1]　CHEN Ke-Fei[2]

(School of Computer Science & Technology, Yantai University, Yantai 264005)[1]

(Department of Computer Science & Engineering, Shanghai Jiaotong University, Shanghai 200030)

Abstract　Based on the threshold scheme of Shamir and the problem of Hermite interpolation, a new threshold scheme on share of secret is constructed in this paper. Feasibility of the scheme is proved. Besides, Security on the scheme is discussed also.

Keywords　Hermite interpolation, Share of secret, Threshold scheme

1　引言

在导弹控制发射、重要场所的通行检验等情况下，通常必须由两人或多人同时参与才能生效，这时需要将秘密分给多人掌管，并且必须有一定人数的掌管秘密的人同时到场才能恢复这一秘密。由此，需引入门限方案这一概念。设秘密 s 被分成 n 个部分信息，每一部分信息称为一个子密钥或影子，由一个参与者持有，使得由 k 个或多于 k 个参与者所持有的部分信息可重构 s，而由少于 k 个参与者所持有的部分信息则无法重构 s，则称这种方案为 (k,n)-秘密分割门限方案。Shamir 在文[1]中基于多项式的 Lagrange 插值公式构造了 Shamir 门限方案。本文在此方案的基础上，利用埃尔米特插值构造一个新的秘密分割门限方案，对方案构造的可行性进行了证明，并对所构造的方案的安全性进行了讨论。

2　方案的构造

设 $f(x)$ 为 $GF(q)$ 上的一个 $2k-1$ 次多项式，密钥 s 取作 $f'(0)$，n 个子密钥取作 $(f(x_i),f'(x_i))(i=1,2,\cdots,n)$，它们满足当 $i\neq j$ 时，$x_i\neq x_j$，且 $x_i\neq 0(1\leqslant i\leqslant n)$，那么利用其中的任意 k 个子密钥可重构 $f(x)$，从而可得密钥 s，而显然当密钥个数少于 k 个时无法重构 $f(x)$，也无法重构 $f'(x)$，因而无法得出密钥 s。这样我们构造出的方案为一 (k,n)-秘密分割门限方案。方案的可行性可由如下定理证明。

定理 1　设 $f(x)$ 为 $GF(q)$ 上的一个 $2k-1$ 次多项式，若已知 $f(x_j)$ 和 $f'(x_j)(1\leqslant i_1\leqslant j\leqslant i_k\leqslant n)$，它们满足当 $i\neq j$ 时，$x_i\neq x_j$，且 $x_j\neq 0(1\leqslant i_1\leqslant j\leqslant i_k\leqslant n)$，则由它们可确定出 $f(x)$，而当给出的 $f(x)$ 和 $f'(x_j)$ 的对数少于 k 个时，无法确定出 $f(x)$。并且 $f(x)$ 由这些 $(f(x_j),f'(x_j))(1\leqslant i_1\leqslant j\leqslant i_k\leqslant n)$ 唯一确定。

证明：设 $f(x)=a_0+a_1x+a_2x^2+\cdots+a_{2k-1}x^{2k-1}$，则确定 $f(x)$ 需要 $2k$ 个条件，所以当给出的 $f(x_j)$ 和 $f'(x_j)$ 的对数少于 k 个时，无法确定出 $f(x)$。

记 $f(x_i)=y_i$，$f'(x_i)=y'_i(1\leqslant i\leqslant n)$，则可由插值基函数的方法构造出 $f(x)$。

事实上，设

$$f(x)=y_{i_1}\varphi_{i_1}(x)+y_{i_2}\varphi_{i_2}(x)+\cdots+y_{i_k}\varphi_{i_k}+y'_{i_1}\psi_{i_1}(x)+y'_{i_2}\psi_{i_2}(x)+\cdots+y'_{i_k}\psi_{i_k}(x),$$

其中 $\varphi_{i_j}(x)$ 满足

$$\varphi_{i_j}(x_{i_j})=1,\varphi_{i_j}(x_{i_j})=0,(\text{当 } l\neq j \text{ 时})\text{和 } \varphi'_{i_j}(x_{i_j})=0(1\leqslant l\leqslant k)。$$

而 $\psi_{i_j}(x)$ 满足

$$\psi_{i_j}(x_{i_j})=0(1\leqslant l\leqslant k),\psi'_{i_j}(x_{i_j})=1,\psi'_{i_j}(x_{i_j})=0(\text{当 } l\neq j \text{ 时})。$$

首先证明 $\varphi_{i_j}(x)$ 的存在性。

由 $\varphi_{i_j}(x)$ 满足

$$\varphi_{i_j}(x_{i_j})=1,\varphi_{i_j}(x_{i_j})=0(\text{当 } l\neq j \text{ 时})\text{和 } \varphi'_{i_j}(x_{i_j})=0(1\leqslant l\leqslant k)$$

可知

$x_{i_j}(1\leqslant l\leqslant k,l\neq j)$ 为 $\varphi_{i_j}(x)$ 的二重零点，故可设

$$\varphi_{i_j}(x)=(ax+b)(x-x_{i_j})^2(x-x_{i_2})^2\cdots(x-x_{i_{j-1}})^2(x-x_{i_{j+1}})^2\cdots(x-x_{i_k})^2,$$

由此可得

$$\varphi'_{i_j}(x)=a(x-x_{i_1})^2(x-x_{i_2})^2\cdots(x-x_{i_{j-1}})^2(x-x_{i_{j-1}})^2\cdots(x-x_{i_k})^2+(ax+b)[(x-x_{i_1})^2(x-x_{i_2})^2\cdots(x-x_{i_{j-1}})^2(x-x_{i_{j+1}})^2\cdots(x-x_{i_k})^2]',$$

由 $\varphi_{i_j}(x_{i_j})=1$ 和 $\varphi'_{i_j}(x_{i_j})=0$ 可得

*)基金项目：国家自然科学基金重大研究计划项目资金资助(编号：90104005)。杜伟章　博士，副教授，研究方向为纠错编码理论与密码学。陈克非　博士生导师，教授，主要研究方向为密码理论与技术，网络与信息安全。

$$\begin{cases}(ax_{i_j}+b)(xi-x_{i_1})^2(x_{i_j}-x_{i_2})^2\cdots(x_{i_j}-x_{i_{j-1}})^2\\ \quad(x_{i_j}-x_{i_{j+1}})^2\cdots(x_{i_j}-x_{i_k})^2=1\\ a(x_{i_j}-x_{i_1})^2(x_{i_j}-x_{j_2})^2\cdots(x_{i_j}-x_{i_{j-1}})^2(x_{i_j}-x_{i_{j+1}})^2\cdots\\ \quad(x_{i_j}-x_{i_k})^2+(ax_{i_j}+b)\cdot[(x-x_{i_1})^2(x-x_{i_2})^2\cdots\\ \quad(x-x_{i_{j-1}})^2(x-x_{i_{j+1}})^2\cdots(x-x_{i_k})^2]'|x\\ \quad=x_{i_j}=0\end{cases}$$

令 $c=[(x-x_{i_1})^2(x-x_{i_2})^2\cdots(x-x_{i_{j-1}})^2(x-x_{i_{j+1}})^2\cdots(x-x_{i_k})^2]'|x=x_{i_j}$，得

$$\begin{cases}ax_{i_j}\prod\limits_{\substack{l=1\\l\neq j}}^{k}(x_{i_j}-x_{i_l})^2+b\prod\limits_{\substack{l=1\\l\neq j}}^{k}(x_{i_j}-x_{i_l})^2=1\\ a[\prod\limits_{\substack{l=1\\l\neq j}}^{k}(x_{i_j}-x_{i_l})^2+x_{i_j}c]+bc=0\end{cases},$$

由此方程组可得

$$a=\frac{\begin{vmatrix}1 & \prod\limits_{\substack{l=1\\l\neq j}}^{k}(x_{i_j}-x_{i_l})^2\\ 0 & c\end{vmatrix}}{\begin{vmatrix}x_{i_j}\prod\limits_{\substack{l=1\\l\neq j}}^{k}(x_{i_j}-x_{i_l})^2 & \prod\limits_{\substack{l=1\\l\neq j}}^{k}(x_{i_j}-x_{i_l})^2\\ \prod\limits_{\substack{l=1\\l\neq j}}^{k}(x_{i_j}-x_{i_l})^2+x_{i_j}c & c\end{vmatrix}}$$

$$=\frac{c}{[\prod\limits_{\substack{l=1\\l\neq j}}^{k}(x_{i_j}-x_{i_l})^2]^2}$$

$$b=\frac{\begin{vmatrix}x_{i_j}\prod\limits_{\substack{l=1\\l\neq j}}^{k}(x_{i_j}-x_{i_l})^2 & 1\\ \prod\limits_{\substack{l=1\\l\neq j}}^{k}(x_{i_j}-x_{i_l})^2+x_{i_j}c & 0\end{vmatrix}}{\begin{vmatrix}x_{i_j}\prod\limits_{\substack{l=1\\l\neq j}}^{k}(x_{i_j}-x_{i_l})^2 & \prod\limits_{\substack{l=1\\l\neq j}}^{k}(x_{i_j}-x_{i_l})^2\\ \prod\limits_{\substack{l=1\\l\neq j}}^{k}(x_{i_j}-x_{i_l})^2+x_{i_j}c & c\end{vmatrix}}$$

$$=\frac{x_{i_j}c+\prod\limits_{\substack{l=1\\l\neq j}}^{k}(x_{i_j}-x_{i_l})^2}{[\prod\limits_{\substack{l=1\\l\neq j}}^{k}(x_{i_j}-x_{i_l})^2]^2}$$

由此

$$\varphi_{ij}(x)=\left[-\frac{c}{[\prod\limits_{\substack{l=1\\l\neq j}}^{k}(x_{i_j}-x_{i_l})^2]^2}+\frac{x_{i_j}c+\prod\limits_{\substack{l=1\\l\neq j}}^{k}(x_{i_j}-x_{i_l})^2}{[\prod\limits_{\substack{l=1\\l\neq j}}^{k}(x_{i_j}-x_{i_l})^2]^2}\right]\prod_{\substack{l=1\\l\neq j}}^{k}(x_{i_j}-x_{i_l})^2,$$

由 $\psi_{i_j}(x)$满足

$\psi_{i_j}(x_{i_j})=0(1\leqslant l\leqslant k)$，$\psi'_{i_j}(x_{i_j})=1$，$\psi'_{i_j}(x_{i_j})=0$(当 $l\neq j$ 时)可知 x_{i_j} 为 $\psi_{i_j}(x)$的一重零点，而 x_{i_j} $(1\leqslant l\leqslant k, l\neq j)$为 $\psi_{i_j}(x)$的二重零点，故可设 $\psi_{i_j}(x)=a(x-x_{i_j})(x-x_{i_1})^2(x-x_{i_2})^2\cdots(x-x_{i_{j-1}})^2(x-x_{i_{j+1}})^2\cdots(x-x_{i_k})^2$，

由此可得

$$\psi'_{i_j}(x)=a(x-x_{i_1})(x-x_{i_2})^2\cdots(x-x_{i_{j-1}})^2(x-x_{i_{j+1}})^2\cdots(x-x_{i_k})^2+a(x-x_{i_j})[(x-x_{i_1})^2(x-x_{i_2})^2\cdots(x-x_{i_{j-1}})^2(x-x_{i_{j+1}})^2\cdots(x-x_{i_k})^2]'$$

故 $\psi'_{i_j}(x_{i_j})=a\prod\limits_{\substack{l=1\\l\neq j}}^{k}(x_{i_j}-x_{i_l})^2$，

由 $\psi'_{i_j}(x_{i_j})=1$ 得，$a=\dfrac{1}{\prod\limits_{\substack{l=1\\l\neq j}}^{k}(x_{i_j}-x_{i_l})^2}$，

这样 $\psi'_{i_j}(x)=\dfrac{1}{\prod\limits_{\substack{l=1\\l\neq j}}^{k}(x_{i_j}-x_{i_l})^2}(x-x_{i_j})\prod\limits_{\substack{l=1\\l\neq j}}^{k}(x_{i_j}-x_{i_l})^2$，

由 $\varphi_{i_j}(x)$和 $\psi_{i_j}(x)$的存在性和唯一性，可知由已知条件可唯一地决定 $f(x)$。证毕。

显然，当$(f(x_{i_j}), f'(x_{i_j}))$多于 k 个时，由已知条件可决定出 $f(x)$，而当给定$(f(x_{i_j}), f'(x_{i_j}))(j<k)$时，可得 $f(x)$满足的至多 $2(k-1)$个条件，而要确定 $f(x)$需 $2k$ 个条件，要确定 $f'(x)$需 $2k-1$ 个条件，这样由这些已知条件无法确定 $f(x)$，也无法确定 $f'(x)$，从而无法构造出秘密 $f'(0)$，故我们给出的方案为一(k,n)-秘密分割门限方案。

结束语 本文在 Shamir 门限方案的基础上，利用埃尔米特插值构造了一个新的秘密分割门限方案，并对方案的可行性进行了讨论和证明。但我们所给出的方案是基于埃尔米特插值的一种特殊情况，如何利用一般的埃尔米特插值构造秘密分割门限方案，还需进一步研究。

参 考 文 献

1 Shamir A. How to share a secret. Communications of the ACM, 1979,24(11):612～613

2 王能超编著. 数值分析简明教程(第二版). 高等教育出版社，2004，5

(上接第 120 页)

4 Matsushita T. A flexibly revocable key-distribution scheme for efficient black-box tracing. In: ICICS 2002[C], LNCS. Springer-Verlag, 2002,2513:97～208

5 Pfitzmann B. Trials of traced traitors. In: Information Hiding'96 [C], LNCS. Springer-Verlag, 1996,1174:49～64

6 Kurosawa K, Desmedt Y. Optimum traitor tracing and asymmetric schemes. In: Proc. of Eurocrypt98[C], LNCS. Springer-Verlag, 1998,1403:145～157

7 Watanabe Y, Hanaoka G, Imai H. Efficient asymmetric public key traitor tracing without trusted agents. In: CT-RSA2001 [C], LNCS. Springer-Verlag, 2001,2020:392～407

8 Kiayias A, Yung M. Breaking and repairing asymmetric public-key traitor tracing. In: ACM Workshop on DRM2002 [C], LNCS, Springer-Verlag, 2003, 2696:32～50

9 李勇，杨波. 一种高效非对称的动态公钥叛逆者追踪方案[J]. 西安电子科技大学学报(自然科学版)，2003，30(3):394～398

10 Lyuu Y, Wu M. A fully public-key traitor tracing scheme. WSEAS Transactions on Circuits[J], 2002, 1(1):88～93

11 Mu Y, Varadharajan V. Robust and secure broadcasting. In: Indocryt 2001[C], LNCS. Springer-Verlag, 2001,2247:223～231

12 Kiayias A, Yung M. Traitor tracing with constant transmission rate. In: Euocrypt 2002 [C], LNCS. Springer-Verlag, 2002, 2332:450～465

13 Wagstaff S. Cryptanalysis of number theoretic cipher[M]. Boca Raton, Florida: CRC Press, 2002. 144～153