有限域F_P上的DFT在秘密共享中的应用

范安东[1,3]，孙 琦[1,2]

(1. 四川大学数学学院 成都 610064；2. 现代通信国家重点实验室 成都 610041；3. 成都理工大学信息管理学院 成都 610059)

【摘要】为了提高Shamir (m,n) 门限方案中的 n 个共享的生成速度和 m 个共享者恢复密钥的运算速度，将Shamir (m,n) 门限方案中采用拉格朗日插值法生成 n 个共享和 m 个共享者恢复密钥的方法，改为利用有限域上的离散傅里叶变换(DFT)来实现。由于有限域上的DFT也具循环卷积性和类似复数域上FFT的快速算法，从而可以提高 n 个共享的生成速度。当 $m>[n/2]$ 时，能够提高可信中心构作 n 个共享的运算速度，特别当门限数 m 与共享数 n 相等且为2的方幂时，还能够提高共享者恢复密钥的运算速度。

关 键 词 离散傅里叶变换； 有限域； 拉格朗日插值； 秘密共享； Shamir门限方案

中图分类号 TP393 **文献标识码** A

Application of DFT Over Finite Field F_P in the Secret Sharing Scheme

FAN An-dong[1,3] and SUN Qi[1,2]

(1. College of Mathematics, Sichuan University Chengdu 610064; 2. National Laboratory for Modern Communications Chengdu 610041; 3. Information Management College, Chengdu University of Technology Chengdu 610059)

Abstract In order to increase the calculation speed of the n sharing's generation and the m partners to recover the secret in Shamir(m,n) threshold scheme, the discrete Fourier transform (DFT) over finite field is adopted other than the classical Lagrange interpolation. Because the DFT over finite field has some similar properties of the DFT over complex, such as the cycling convolution and the FFT algorithm, this method can improve the efficient of Shamir(m,n) threshold scheme. If $m>[n/2]$, it can increase the calculation speed of the trust center to divide the key to n sharing components. Moreover, if $m=n$ and it is the power of 2, this scheme can increase the calculation speed of the partners to recover the secret key.

Key words discrete Fourier transform; finite field; Lagrange interpolation; secret sharing; Shamir threshold scheme

秘密共享的 (m,n) 门限方案的基本思想是把一个秘密数据 k (例如密钥)分成n个共享：$k_1,k_2,\cdots,k_n$，使得已知其中任意m个 $(2\leqslant m\leqslant n)$ 共享个数 k_i 均容易计算出 k (即恢复密钥 k)，而当已知共享小于m时，则无法恢复 k。这种思想是由文献[1]和文献[2]分别提出来的。秘密共享门限方案是应用密码学中一种重要的基本协议，介绍密码学的文献[3, 4-8]都有论及。

Shamir (m,n) 门限方案是利用基于 F_p 上多项式的拉格朗日插值多项式构建的[9]。它需要产生 F_p 上的一个次数为 $m-1$ 的多项式 $f(x)$，其系数是秘密的，其中常数项 $f(0)=k$。通过 F_p 中的 n 个不同的非零元 x_j 来决定 n 个共享 $k_j=f(x_j)$，其中 x_j 是公开的，k_j 是秘密的，$j=1,2,\cdots,n$。若已知任意m个 $(2\leqslant m\leqslant n)$ 共享 k_i，则可用 F_p 上的拉格朗日插值公式重构 $f(x)$ 即可恢复密钥 k $(k=f(0))$。

本文把 F_p 上的DFT应用到秘密共享的Shamir (m,n) 门限方案中，当 $m>[n/2]$ (符号[x]表示不超过实数x的最大整数)时，能够提高可信中心构建n个共享的运算速度。特别当门限数m与共享数n相等且为2的方幂时，还能够提高共享者恢复密钥的运算速度。

1 秘密共享的Shamir(m,n)门限方案简介

设p是一个素数，密钥 $k\in F_p$，可信中心给 n $(n<p)$ 个秘密共享者 A_i $(i=0,1,\cdots,n-1)$，分配共

收稿日期：2007－12－27; 修回日期：2008－03－25

基金项目：四川省教育厅自然科学项目青年基金(2006B057)

作者简介：范安东(1970－)，男，博士生，副教授，主要从事信息隐藏和应用数论方向的理论和应用方面的研究；孙 琦(1973－)，男，教授，博士生导师，主要从事数论及其在密码算法和数字信号处理中的应用研究.

享的过程如下：

(1) 可信中心随机选取一个 F_p 上的 $m-1$ 次多项式：$f(x)=c_{m-1}x^{m-1}+c_{m-2}x^{m-2}+\cdots+c_1x+c_0$，$c_i\in F_p$，$c_{m-1}\neq 0$，显然，$F_p$ 中的元在需要时也可取为整数，故不妨设 $0\leqslant c_i<p\ (i=0,1,\cdots,m-1)$，其中 c_0(即 $f(0)$)常取为密钥 k。

(2) 可信中心在 F_p 中取 n 个不同的非零元 a_i，即可取 n 个不同的整数值 a_i 满足，$0<a_i<p\ (i=0,1,\cdots,n-1)$，并计算：

$$b_i=f(a_i)\qquad i=0,1,\cdots,n-1 \tag{1}$$

其中 F_p 上的运算是整数模 p 的运算，计算结果 b_i 可取 $0\leqslant b_i<p\ (i=0,1,\cdots,n-1)$。

(3) 可信中心公开 p 和 $a_i\ (i=0,1,\cdots,n-1)$，对每一个 i 把 b_i 秘密传给共享者 A_i，称 b_i 是 A_i 的共享(也称 A_i 的子密钥)。对于门限数m，若已知任意m个共享，不妨设为 $b_0,b_1,\cdots,b_{m-1}$，它们分别是 $a_0,a_1,\cdots,a_{m-1}$ 通过 $f(x)$ 的取值，则可由 F_p 上的拉格朗日插值公式重构 F_p 的m–1次多项式 $f(x)$ (唯一决定)：

$$\begin{aligned}f(x)=&b_0\frac{(x-a_1)\cdots(x-a_{m-1})}{(a_0-a_1)\cdots(a_0-a_{m-1})}+\\&b_1\frac{(x-a_0)(x-a_2)\cdots(x-a_{m-1})}{(a_1-a_0)(a_1-a_2)\cdots(a_1-a_{m-1})}+\cdots+\\&b_{m-1}\frac{(x-a_0)\cdots(x-a_{m-2})}{(a_{m-1}-a_0)\cdots(a_{m-1}-a_{m-2})}\end{aligned}$$

于是密钥 k 得以恢复：

$$\begin{aligned}k=f(0)=&\\(-1)^{m-1}\Bigg[&\frac{b_0a_1\cdots a_{m-1}}{(a_0-a_1)\cdots(a_0-a_{m-1})}+\\&\frac{b_1a_0a_2\cdots a_{m-1}}{(a_1-a_0)\cdots(a_1-a_{m-1})}+\cdots+\\&\frac{b_{m-1}a_0\cdots a_{m-2}}{(a_{m-1}-a_0)\cdots(a_{m-1}-a_{m-2})}\Bigg]\end{aligned} \tag{2}$$

如果已知的共享小于 m，则不能算出密钥 k。

注意：$f(x)$ 的使用是一次性的，当分发完 n 个共享后，立即毁掉；如需第二次分发 n 个共享时，可信中心再随机选取新的 $f(x)$。

2 F_p上的DFT在Shamir(m,n)门限方案中的应用

设 p 是一个奇素数，F_p 上一个 N 点序列 $x_i(i=0,1,\cdots,N-1)$ 的DFT是指：

$$X_k=\sum_{n=0}^{N-1}x_n\alpha^{nk}\qquad k=0,1,\cdots,N-1 \tag{3}$$

式中 α 模 p 的次数是 N (整数次数的定义参阅文献[10])。

和复数域上的DFT类似，F_p 上的DFT仍具有循环卷积性质，且当 $N=2^t$ 时，可用快速傅里叶变换(FFT)计算式(3)，其乘、加法运算次数均为 $O(N\log_2 N)$，而直接计算式(3)所需乘、加法次数均为 $O(N^2)$，两者相比，可见用FFT计算式(3)可以大大提高了运算速度。与复数域上FFT不同的是，F_p 上的FFT在计算时不需要存储三角函数，只需给定 F_p 上的一个生成元 α，且不存在计算误差，当 $\alpha=2$ 时(大多数情况下 α 都可取为2)，模指数运算 α^{nk} 可以通过简单的移位运算来完成，从而可以大大提高运算速度。关于 F_p 上的DFT更多的性质可参阅文献[11]。显然，式(3)的逆变换(IDFT)为：

$$x_n=N^{-1}\sum_{k=0}^{N-1}X_k\alpha^{-nk}\qquad n=0,1,\cdots,N-1 \tag{4}$$

式中 N^{-1} 为N在 F_p 中的逆，即 $NN^{-1}\equiv 1(\mathrm{mod}\ p)$。

式(3) 和式(4)均可写成矩阵形式，分别为：

$$\begin{pmatrix}X_0\\X_1\\\vdots\\X_{N-1}\end{pmatrix}=\boldsymbol{T}\begin{pmatrix}x_0\\x_1\\\vdots\\x_{N-1}\end{pmatrix} \tag{5}$$

和

$$\begin{pmatrix}x_0\\x_1\\\vdots\\x_{N-1}\end{pmatrix}=\boldsymbol{U}\begin{pmatrix}X_0\\X_1\\\vdots\\X_{N-1}\end{pmatrix} \tag{6}$$

这里

$$\boldsymbol{T}=\begin{pmatrix}1&1&\cdots&1\\1&\alpha&\cdots&\alpha^{N-1}\\1&\alpha^2&\cdots&\alpha^{2(N-1)}\\\vdots&\vdots&\vdots&\vdots\\1&\alpha^{N-1}&\cdots&\alpha^{(N-1)^2}\end{pmatrix}$$

$$\boldsymbol{U}=\frac{1}{N}\begin{pmatrix}1&1&\cdots&1\\1&\alpha^{-1}&\cdots&\alpha^{-(N-1)}\\1&\alpha^{-2}&\cdots&\alpha^{-2(N-1)}\\\vdots&\vdots&\vdots&\vdots\\1&\alpha^{-(N-1)}&\cdots&\alpha^{-(N-1)^2}\end{pmatrix}$$

在Shamir (m,n) 门限方案中，如果 $[n/2]<m\leqslant n\leqslant N=2^t$，$N$ 是所有大于或等于 n 的2的方幂中最小者。取素数 $p>N$，且 $2^t\,|\,(p-1)$，设 g 是 F_p 的一个生成元(即 g 是模 p 的一个原根)，此时 $\alpha=g^{\frac{p-1}{N}}$ 模 p 的次数为 N，于是，式(3)是 F_p 上的一个DFT。现在，可信中心可用式(3)来计算 n 个共享。取 n 个点 $1,\alpha,\cdots,\alpha^{n-1}$，记 $a_i=\alpha^i$，计算 $b_i=f(a_i)$ $(i=0,1,\cdots,n-1)$ 即可得到 n 个共享，这里 $f(x)$ 的次数是 $m-1$ ($m\leqslant n\leqslant N$)。为了使用 F_p 上的DFT(式(3))来得到 n 个共享，采取添零的方法，把 $f(x)$ 的系数 $c_0,c_1,\cdots,c_{m-1}$ 延拓成 $c_0,\cdots,c_{m-1},c_m,\cdots,c_{N-1}$，这里 $c_j=0$ $(j=m,m+1,\cdots,N-1)$。于是 F_p 上的 N 点序列 $c_0,c_1,\cdots,c_{N-1}$ 经 F_p 上长为 N 的DFT(即矩阵式(5))变换成 $b_0,b_1,\cdots,b_{N-1}$，即：

$$\begin{pmatrix} b_0\\ b_1\\ \vdots\\ b_{m-1}\\ \vdots\\ b_{n-1}\\ \vdots\\ b_{N-1}\end{pmatrix}=\boldsymbol{T}\begin{pmatrix} c_0\\ c_1\\ \vdots\\ c_{m-1}\\ \vdots\\ 0\\ \vdots\\ 0\end{pmatrix}\tag{7}$$

式中 $b_j=f(\alpha^j)$，$j=0,1,\cdots,m-1,m,\cdots,n-1,n,\cdots,N-1$，这就计算出了 n 个共享 $b_j=f(\alpha^j)$，$j=0,1\cdots,n-1$。证明如下：

由$\boldsymbol{T}$的构造易知：

$$b_j=(1\quad \alpha^j\quad \cdots\quad \alpha^{j(N-1)})\begin{pmatrix} c_0\\ c_1\\ \vdots\\ c_{m-1}\\ \vdots\\ 0\\ \vdots\\ 0\end{pmatrix}=$$

$$c_0+c_1\alpha^j+\cdots+c_{m-1}\alpha^{j(m-1)}=f(\alpha^j)$$

由于 $N=2^t$，用FFT计算式(7)，其乘、加法运算次数均为 $O(N\log_2 N)$。如果由式(1)直接计算 n 个共享，其乘、加法次数均为 $O(mn)$。当 $m\geqslant[n/2]+1$ 时，由于 $N=2^t\geqslant n>2^{t-1}=N/2$，故有：

$$mn>n^2/2\geqslant(N/2)^2/2=N\cdot N/8$$

而当 $N\geqslant 64$ 时，$N/8>\log_2 N$，即有：

$$N\log_2 N<mn$$

所以当n较大(不小于32)以及 $m>[n/2]$ 时，用 F_p 上的DFT计算n个共享，可提高运算速度；反之，当 $m<[n/2]$ 或n不超过32时，可直接计算 $b_i=f(a_i)$，而不宜采用FFT方法。

特别当 $m=n=N=2^t$ 时，式(7)的逆变换为：

$$\begin{pmatrix} c_0\\ c_1\\ \vdots\\ c_{N-1}\end{pmatrix}=\boldsymbol{U}\begin{pmatrix} b_0\\ b_1\\ \vdots\\ b_{N-1}\end{pmatrix}\tag{8}$$

用FFT计算式(8)，即可重构 $f(x)$，恢复密钥 $k=f(0)$，其乘、加法运算次数均为 $O(N\log_2 N)$；如果用 F_P 上的多项式的拉格朗日插植公式去重构 $f(x)$，恢复密钥 $k=f(0)$，其乘、加法运算次数均为 $O(N^2)$，因此用 F_P 上的DFT可大大提高重构 $f(x)$ 的运算速度。

3　结　论

本文把 F_p 上的DFT(或称 F_p 上的数论变换)应用到秘密共享的Shamir$(m,\ n)$门限方案中，当 $m>[n/2]$ 时，能够提高可信中心构作n个共享的运算速度；特别当门限数m与共享数 n 相等且为2的方幂时，还能够提高共享者恢复密钥的运算速度。由于 $f(x)$ 的使用为一次性的，需要更换新的 $f(x)$，计算n个新的共享，所以运用 F_p 上的DFT来提高运算速度是有意义的。对于条件 $m>[n/2]$，就是常用的选举投票原则——票数过半有效，因而也是合理的。至于找大素数 p 和 p 的原根，可分别用素数判定的方法和计算原根的算法预先计算，部分算法可参阅文献[6]。

参　考　文　献

[1] SHAMIR A. How to share a secret[J]. Communication of ACM, 1979, 24(11): 612-613.

[2] BLAKLEY G R. Safeguarding cryptographic keys[C]// Proceedings of the National computer conference. New York: AFIPS Press, 1979.

[3] 冯克勤. 数论与密码[M]. 北京: 科学出版社, 2007.
FENG Ke-qin. Number Theory and Cryptography[M]. Beijing: Science Press, 2007.

(下转第741页)

Science and Technology of China, 2008, 6(1): 47-51.
[4] IMAI A. Multi-objective simultaneous stowage and load planning for a container ship with container rehandle in yard stacks[J]. European Journal of Operational Research, 2006, 171(2) : 373-389.
[5] 许光泞, 俞金寿. 改进遗传算法求解三维集装箱装载问题[J]. 华东理工大学学报, 2007, 33(3): 425-428.
XU Guang-ning, YU Jin-shou. An improved genetic algorithm for three-dimension container loading problem[J]. Journal of East China University of Science and Technology, 2007, 33(3): 425-428.
[6] HUANG H Z, BO R F, CHEN W. An integrated computational intelligence approach to product concept generation and evaluation[J]. Mechanism and Machine Theory, 2006, 41(5): 567-583.
[7] 杨 军, 张 兢, 王当利, 等. 基于效用矩阵的货物配载调整算法研究[J]. 交通与计算机, 2005, 23(2): 76-79.
YANG Jun, ZHANG Jing, WANG Dang-li, et al. Research on adjusting algorithm of cargo stowage based on efficiency matrix[J]. Computer and Communications, 2005, 23(2): 76-79.
[8] IMO. Chapter XII-additional safety measures for bulk carriers amendments to the international convention for the safety of life at sea 1974[S]. MSC68, 1997.
[9] 李贵成. 船舶装运散装谷物的稳性要求[J]. 航海技术, 2007, 10(6): 23-27.
LI Gui-cheng. Stability requirements for the carriage of grain in bulk[J]. Marine Technology, 2007, 10(6): 23-27.
[10] IMO. International code for the safe carriage of grain in bulk[S]. London, UK: IMO, 1996.
[11] 孔月萍. 人工智能及其应用[M]. 北京: 电子工业出版社, 2008.
KONG Yue-ping. Artificial intelligence: priciples and applications[M]. Beijing: Publishing House of Electronics Industry, 2008.
[12] 杨思春. 一种改进的句子相似度计算模型[J]. 电子科技大学学报, 2006, 35(6): 956-959.
YANG Si-chun. An improved model for sentence similarity computing[J]. Journal of University of Electronic Science and Technology of China, 2006, 35(6): 956-959.
[13] KOOMEN P, PUNYAKANOK V, Roth D, et al. Generalized Inference wiht multiple semantic role labeling systems[C]//In: Proceedings of the Ninth Conference on Computational Natural Language Learning (CoNLL-2005). Ann Arbor: Michigan: Association for Computational Linguistics, 2005.
[14] 江铭虎. 自然语言处理[M]. 北京: 高等教育出版社, 2006.
JIANG Ming-hu. Natural language processing[M]. Beijing: Higher Education Press, 2006.

编 辑 熊思亮

(上接第711页)

[4] 鲁荣波, 何大可, 王常吉. 一种门限代理签名方案的分析与改进[J]. 电子学报, 2007, 35(1): 145-149.
LU Rong-bo, HE Da-ke, WANG Chang-ji. Cryptanalysis and improvement of a threshold proxy signature scheme from bilinear pairings[J]. Acta Electronica Sinica, 2007, 35(1): 145-149.
[5] 庞辽军, 李慧贤, 王育民. 基于LUC密码体制防欺诈的秘密共享方案[J]. 电子科技大学学报, 2007, 36(1): 108-111.
PANG Liao-jun, LI Hui-xian, WANG Yu-min. A secret sharing scheme with ability to identify cheaters based on LUC cryptosystem[J]. Journal of University of Electronic Science and Technology of China，2007, 36(1): 108-111.
[6] ZHANG Xian-feng, ZHANG Feng, QIN Zhi-guang, et al. ECC based threshold decryption scheme and its application in Web security[J]. JESTC, 2004, 2(4): 41-46.
[7] XIN Xiang-jun, WANG Mei-zhi, XIAO Guo-zhen. A (k, n) threshold nominative proxy signature scheme for electronic commerce[J]. Journal of China University of Mining and Technology, 2006, 16(4): 470-474.
[8] YU Yong, YANG Bo, SUN Ying. Identity-based threshold signature and mediated proxy signature schemes[J]. The Journal of China Universities of Posts and Telecommunications, 2007, 14(2): 69-74.
[9] 杜伟章, 陈克非. 基于埃尔米特插值的秘密分割门限方案的构造. 计算机科学, 2006, 33(8): 126-127.
DU Wei-zhang, CHEN Ke-fei. Construction of threshold scheme on share of secret based on the problem of hermite interpolation[J]. Computer Science, 2006, 33(8): 126-127.
[10] 柯 召, 孙 琦. 数论讲义(上册)[M]. 第2版. 北京: 高等教育出版, 2001.
KE Zhao, SUN Qi. Lectures (On List)[M]. 2nd Ed. Beijing: Higher Education Press, 2001.
[11] 刘向丽, 党岚君, 寇卫东, 等. 一种基于二维DFT的一对多非对称数字水印算法[J]. 四川大学学报(工程科学版), 2007, 39(5): 133-136.
LIU Xiang-li, DANG Lan-jun, KOU Wei-dong, et al. An asymmetric digital watermarking algorithm based on 2D-DFT[J]. Journal of Sichuan University (Engineering Science Edition), 2007, 39(5): 133-136.

编 辑 张 俊