第 30 卷第 12 期　　电 子 与 信 息 学 报　　Vol.30No.12
2008 年 12 月　　Journal of Electronics & Information Technology　　Dec. 2008

一个基于内插多项式的广播加密方案

王尚平　解康乐　王晓峰　丁如意
(西安理工大学理学院　西安　710054)

摘　要：该文提出了一种基于内插多项式的广播加密方案，消息发布者通过管理中心指定多个信息接收者，管理中心生成一个内插多项式，并公布相关的信息，合法用户根据自己的秘密信息和中心公布的消息，通过计算线段的中点来得到内插多项式，达到安全广播加密的目的。

关键词：广播加密；内插多项式；安全广播
中图分类号：TP309　　**文献标识码**：A　　**文章编号**：1009-5896(2008)12-2996-03

A Broadcast Encryption Scheme Based on the Interpolating Polynomial

Wang Shang-ping　Xie Kang-le　Wang Xiao-feng　Ding Ru-yi

Abstract: A broadcast encryption scheme based on the interpolating polynomial is proposed. It allows the sender to designate multi-receivers to the Authority Center (AC). The interpolating polynomial is constructed and the related information is proclaimed by AC. The interpolating polynomial can be reconstructed by computing the central point of line segment to achieve the purpose of broadcasting safely by the legal users using their secret information and the public information published by AC.

Key words: Broadcast encryption; Interpolating polynomial; Broadcast safely

1　引言

广播加密是由 Fiat 等人[1]首先提出来的，与基于点对点的通信方式不同，广播加密将视频、音频、软件程序等数字加密之后的内容连续的传送到 PC，机顶盒或手提设备上，只有合法的用户才可以解密。其共同特点是，前向信道数据率高，反向信道不存在，或者数据率很低，只有授权用户才可以解密信息[2]。随着计算机网络的不断发展，广播加密近几年得到了广泛的研究[3,4]。Chang[5]等人提出了使用内插多项式构建广播加密的方案，但是用户的计算量比较大。Wang [6]等人提出的基于三角形的快速定位方法，中心公布的消息过多，增加了中心的存贮负担。陈昭智、郑建德[7]等人提出的分层结构的广播加密方案，减少中心持有密钥的同时，增加了用户的持有密钥量。谭作文[8]等人提出的方案，实现起来计算量非常大。

本文利用内插多项式构建了一个新的广播加密方案，算法的特点是：(1)中心公布的参数很少，只有 2 个；(2)中心持有 n 个参数，用户持有一个秘密参数，可以减少用户的存贮量；(3)本方案的改进方案可以抵御 Lin 等人提出的方案之中的攻击方式；(4)本方案相对于文献[3]中的方案，中心公布的公开信息的个数会有很大的减少；(5)本方案不需要提供公钥证书查询，相对减少了中心的负担。

2007-06-04 收到, 2007-12-24 改回
国家自然科学基金(60273089), 陕西教育厅专项科研计划项目(06JK211), 陕西省自然科学基础研究计划项目(2006F37), 和教育部科学技术研究重点项目(208139)资助课题

2　预备知识

2.1 内插多项式的构建方法

选择一个大素数 P，随机选择多项式环 $Z_p[x]$ 中的 $k-1$ 次的多项式 $F(x)=a_0+a_1x+\cdots+a_{k-1}x^{k-1}$，$x$ 的取值是 $x\in Z_p$，系数 $a_i\in Z_p, i=0,1,\cdots,k-1$ 是随机选择的。在模 P 运算下，在多项式上任意选择 k 个互不相同的坐标点 $(x_i,y_i), i=0,1,\cdots,k-1$，即这些坐标点满足：$F(x_i)=y_i(\bmod P)$，则可以由这 k 个坐标点来恢复出 $F(x)$ (即恢复出多项式的系数)[10]，但是任意 $k-1$ 个坐标点不能恢复出原来的 $F(x)$。

2.2 中国剩余定理

设 $P_0,P_1,\cdots,P_k$ 是 $k+1$ 个两两互素的正整数，则对任意的整数 $b_0,b_1,\cdots,b_k$，同余式组

$$\begin{cases} x\equiv b_0(\bmod P_0)\\ x\equiv b_1(\bmod P_1)\\ \quad\vdots\\ x\equiv b_k(\bmod P_k)\end{cases}$$ 的解是 $$x=M_0'M_0b_0+M_1'M_1b_1+\cdots+M_k'M_kb_k(\bmod m)$$

其中 $m=P_0P_1\cdots P_k$，$m=P_iM_i$，$M_i'M_i\equiv 1(\bmod P_i), i=0,1,2,\cdots,k$。

2.3 广播模型

广播加密类似于一般的加密，分为 5 个过程。

(1)系统建立　由 AC 选择安全参数 k，满足系统的安全性。

(2)用户私钥初始化　由 AC 给每个用户初始化私钥，私

钥通过安全信道传送。

(3)发送者请求 AC　在预定的一段时间里，消息发送者请求 AC 要于其它人进行通信， AC 选择一个多项式 $F(x)\in Z_p[x]$，并公布部分公开信息。

(4)加密　消息发送者通过公开信息与他的私钥，构造多项式 $F(x)$，选择一个 t 计算 $\text{Key}\leftarrow F(t)\bmod P$ 作为本次会话的会话密钥。并使用一个公开的对称加密算法对明文 m 进行加密。

(5)解密　合法用户输入通过自己的密钥，重构多项式，来解密出明文 m。

3　基于内插多项式的广播加密方案

3.1 系统的建立

选择大素数 P，$n+1$ 个用户 $U_0,U_1,\cdots,U_n$ 都在中心 AC 处注册，中心 AC 通过安全信道秘密地给每个用户 $U_i,i=0,1,\cdots,n$ 分发一对秘密参数 $H_i=(H_{ix},H_{iy})$ 和素数 P_i，其中 P_i，H_{ix}，$H_{iy}\in Z_p$ 对外保密，且满足 $P_0P_1\cdots P_n<P$。把 (H_{ix},H_{iy}) 所标记的二维坐标点记做点 H_i。

3.2 广播加密

(1)假设发送者 U_0 通知中心 AC 他需要给 $k\le n$ 个用户，不妨设为 $U_1,U_2,\cdots,U_k,k\le n$ 发送消息。

(2) AC 在二维坐标系中任意选择 $k+1$ 个异于点 $H_i,i=0,1,\cdots,k$ 的坐标点 $W_i=(W_{ix},W_{iy}),i=0,1,\cdots,k$，连接线段 $\overline{H_iW_i},i=0,1,\cdots,k$，计算线段 $\overline{H_iW_i}$ 的中点为 $S_i=(S_{ix},S_{iy}),i=0,1,\cdots,k$，其中线段中点的坐标是在模 P 下计算的，即 $S_{ix}=(H_{ix}+W_{ix})/2(\bmod P),S_{iy}=(H_{iy}+W_{iy})/2(\bmod P)$。利用内插多项式的构建方法[10]，做一条经过 $S_i,i=0,1,\cdots,k$ 的 k 次多项式 $F(x)\in Z_p[x]$。 AC 再在此 k 次多项 $F(x)$ 上任意选择 k 个异于点 $S_i,i=0,1,\cdots,k$ 并且异于 $H_i,i=0,1,\cdots,n$ 的坐标点 $O_i=(O_{ix},O_{iy}),i=1,\cdots,k$，并公布这 k 个坐标点。 AC 根据刚才选择的 $k+1$ 个坐标点 $W_i=(W_{ix},W_{iy}),i=0,1,\cdots,k$，利用中国剩余定理，计算得到 (C_x,C_y) 如下：

$$\begin{cases}C_x\equiv W_{0x}\bmod P_0\\ C_x\equiv W_{1x}\bmod P_1\\ \quad\vdots\\ C_x\equiv W_{kx}\bmod P_k\end{cases}\text{和}\begin{cases}C_y\equiv W_{0y}\bmod P_0\\ C_y\equiv W_{1y}\bmod P_1\\ \quad\vdots\\ C_y\equiv W_{ky}\bmod P_k\end{cases}$$

AC 并公布 (C_x,C_y) 及本次会话的发送者 U_0 和指定的合法接收者 $U_1,U_2,\cdots,U_k,k\le n$。

(3)发送者 U_0 通过 AC 公开的 (C_x,C_y) 以及通信接收方 $U_1,U_2,\cdots,U_k,k\le n$，计算出点 W_0 的坐标为：$(W_{0x},W_{0y})=(C_x\bmod P_0,C_y\bmod P_0)$。使用自己的秘密信息 $H_0=(H_{0x},H_{0y})$，计算出线段 $\overline{W_0H_0}$ 的中点坐标点 $S_0((H_{0x}+W_{0x})/2(\bmod P),(H_{0y}+W_{0y})/2(\bmod P))$。再通过公开的坐标点 $O_i=(O_{ix},O_{iy}),i=1,\cdots,k$ 和已经计算出来的坐标点 S_0，通过构建内插多项式[10]，可以得到原来的 k 次多项式 $F(x)$。任意选择一个整数 $t\in[0,P)$，计算 $\text{Key}\leftarrow F(t)\bmod P$ 作为本次会话的会话密钥。发布 $(t,\text{SEnc}(\text{Key},m))$，其中 m 是 U_0 发送的消息， $\text{SEnc}(\cdot,\cdot)$ 和 $\text{SDec}(\cdot,\cdot)$ 分别是安全的对称加密算法和解密算法，例如 AES 或者其他安全分组密码算法。

3.3 用户端解密

对于合法用户 $U_j,j\le k$，U_j 根据公开信息 (C_x,C_y)，计算坐标点 W_j 的坐标为：$(W_{jx},W_{jy})=(C_x\bmod P_j,C_y\bmod P_j)$ 再使用自己的秘密信息坐标点 H_j，计算出线段 $\overline{H_iW_i}$ 的中点坐标点 S_j=$((H_{jx}+W_{jx})/2(\bmod P),(H_{jy}+W_{jy})/2(\bmod P))$。通过公开的坐标点 $O_i=(O_{ix},O_{iy}),i=1,\cdots,k$ 和已经计算出来的坐标点 S_j，通过构建内插多项式[10]，可以得到原来的 k 次多项式 $F(x)$。根据 U_0 发布的消息 $(t,\text{SEnc}(\text{Key},m))$，可以得到 t，计算出 $\text{Key}\leftarrow F(t)\bmod P$，作为本次会话的会话密钥，解密 $\text{SDec}(\text{Key},\text{SEnc}(\text{Key},m))$，得到消息 m。

4　方案讨论

4.1 方案的正确性

对于合法的用户 $U_1,U_2,\cdots,U_k,k\le n$，按照解密算法，根据内插多项式性质，可以证明方案是正确的。

4.2 方案的安全性分析

(1)对于任意一个不合法用户，例如 U_{k+1}，他要构造出正确的 k 次多项式 $F(x)\in Z_p[x]$，利用公开信息，可以知道 k 个作标点 $O_i=(O_{ix},O_{iy}),i=1,\cdots,k$，但还需要知道 k 次多项式 $F(x)$ 上的一个异于 $O_i=(O_{ix},O_{iy}),i=1,\cdots,k$ 的坐标点 $Q=(Q_x,Q_y)$。则可以归结为如下的问题：

假设 $F(x)=a_0+a_1x+a_2x^2+\cdots+a_kx^k\in Z_P[x]$，已知 $F(O_{ix})=O_{iy},i=1,2,\cdots,k$，求点 $Q=(Q_x,Q_y),Q_x\ne O_{ix},i=1,2,\cdots,k$ 满足 $F(Q_x)=Q_y$。则有如下方程：

$$\begin{bmatrix}1&O_{1x}&O_{1x}^2&\cdots&O_{1x}^k\\1&O_{2x}&O_{2x}^2&\cdots&O_{2x}^k\\\vdots&\vdots&\vdots&\vdots&\vdots\\1&O_{kx}&O_{kx}^2&\cdots&O_{kx}^k\\1&Q_x&Q_x^2&\cdots&Q_x^k\end{bmatrix}\begin{bmatrix}a_0\\a_1\\\vdots\\a_k\end{bmatrix}=\begin{bmatrix}O_{1y}\\O_{2y}\\\vdots\\O_{ky}\\Q_y\end{bmatrix}\begin{bmatrix}1&O_{1x}&O_{1x}^2&\cdots&O_{1x}^k\\1&O_{2x}&O_{2x}^2&\cdots&O_{2x}^k\\\vdots&\vdots&\vdots&\vdots&\vdots\\1&O_{kx}&O_{kx}^2&\cdots&O_{kx}^k\\1&Q_x&Q_x^2&\cdots&Q_x^k\end{bmatrix}$$

是一个范得蒙行列式，故有逆，因而

$$\begin{bmatrix}a_0\\a_1\\\vdots\\a_k\end{bmatrix}=\begin{bmatrix}1&O_{1x}&O_{1x}^2&\cdots&O_{1x}^k\\1&O_{2x}&O_{2x}^2&\cdots&O_{2x}^k\\\vdots&\vdots&\vdots&\vdots&\vdots\\1&O_{kx}&O_{kx}^2&\cdots&O_{kx}^k\\1&Q_x&Q_x^2&\cdots&Q_x^k\end{bmatrix}^{-1}\begin{bmatrix}O_{1y}\\O_{2y}\\\vdots\\O_{ky}\\Q_y\end{bmatrix}$$

上式表明，当不合法用户 U_{k+1} 任意确定一个异于 $O_{ix},i=1,\cdots,k$ 的值 Q_x 后，由于 $a_0,a_1,\cdots,a_k$ 是确定的，满足上式的解 $Q_y\in Z_P$ 是唯一的。对于不合法用户 U_{k+1}，要计算出来未知数 $a_0,a_1,\cdots,a_k$，他需要知道 $Q_y\in Z_P$，在模大素数 P 下，U_{k+1} 猜对 Q_y 的概率是 $1/P$。因而当 P 充分大时，系统是安全的。

(2)对于不合法用户 U_{k+1} 来说，他也可能是以前好几次会话的合法接收者，这样，他就可能通过以前的一些信息

W_i，来构造一个圆方程，这样该方案就会受到文献[9]所提出的方法的攻击。因此，本文提出一个改进方案，在进行一段时间的使用之后，将用户的 H_i 进行更换，计算 $H_i^{'} = (H_i + s_i)(\mathrm{mod}\, P)$，其中 s_i 是 AC 选择的随机正整数，且 $s_i < P$ 。$H_i^{'}$ 的更换可在 AC 于原用户的网络设备上自动更换，这样就可以完成秘密信息的更换。

(3)对于系统内部的不合法用户的联合攻击来说，由于 AC 随机选择的坐标点 $S_i = (S_{ix}, S_{iy}), i = 0,1,\cdots,k$ 与非法用户的秘密信息没有关系，因而非法用户即使合谋，也没有办法破解出多项式 $F(x)$，原因如(1)。

4.3 效率分析

在秘密信息分发阶段，中心需要给每个用户分发 1 对秘密信息，中心需要存贮 n 个用户私钥，每个用户的存贮量是 1。本方案与文献[6,7]中方案的效率分析比较如表 1 所示。

表 1 本方案与文献[6,7]效率分析对比表

	基于 RSA 的方案[7]	方案[6]	本方案
秘钥分发中心	需要提供证书/公钥查询服务	不需要提供证书查询服务，需要发布 $(k+1)$ 对公开信息	不需要提供证书查询服务，发布 1 对公开信息
消息发布者	需要查询证书或者公钥	不需要	不需要
用户	需要存贮 $\log N$ 个用户私钥	存贮 1 个秘密信息	存贮 2 个秘密信息

用户的秘密信息分配之后，不需要再改变。由于在广播加密系统中，参加的用户会改变，在每次用户改变之后，发送者需要更改多项式，这就需要每个用户重新构造新的多项式。依据拉格朗日多项式公式，每个用户不用构造多项式，也可以计算出信息，方法如下。

设 $F(x)$ 是所要构造的多项式，给定函数 $F(x)$ 在 k 个不同点 x_i 处的值 $y_i, i = 1,2,\cdots,n$。记 $l_j(x) = \prod_{\substack{i=1 \\ i \neq j}}^{k} \left(\frac{x - x_j}{x_i - x_j} \right)$，那么

$$F(x_r) = \sum_{j=1}^{k} l_j(x_r) \cdot y_i = \sum_{j=1}^{k} \left[\prod_{\substack{i=1 \\ i \neq j}}^{k} \left(\frac{x_r - x_j}{x_i - x_j} \right) \right] \cdot y_i \text{。}$$

4.4 用户的增加和删除管理

可以方便地增加或者撤销用户。如果有新用户加入，只要 AC 给新用户分配一对秘密参数，就可以加入系统。如果要撤销用户 U_j，则 AC 只需任意选取一个坐标点代替 H_j，即可排除用户 U_j。

5 结束语

本文在内插多项式的基础上，构造了一个新的广播加密方案。随着广播消息的时间、发起者的变化，AC 可以任意选择构造内插多项式，使得攻击者破解秘密更加困难，符合密码系统的简单原理、分析复杂的要求。该方案对系统的存贮要求低，可以应用于存贮量较小的应用中。该方案可以解决一些实际中的问题，如电子会议、版权认证等。另外，广播加密中关于不可否认性、高效的密钥分发等问题还需要进一步的研究。

参 考 文 献

[1] Fiat A and Naor M. Broadcase Encryption. Stinson DR. Advances in Cryptology Crypto 93, Springer-Verlag, 1993: 480–491.

[2] 屈劲, 葛建华, 蒋铭. 加密广播的密钥分发. 西安电子科技大学学报, 2002, 29(3): 310–323.

[3] Boneh Dan and Gentry Craig. Collusion resistant broadcast encryption with short ciphertexts and private keys. Lecture notes in computer science, Springer, 2005: 258–275.

[4] Attrapadung Nuttapong, Furukawa Jun, and Imai Hideki. Forward-secure and searchable broadcast encryption with short ciphertexts and private keys. ASIACRYPT2006. LNCS , 2006, Vol. 4284: 161–177.

[5] Chang C C and Wu T C. Broadcast cryptosystem in computer networks using interpolating polynomials. *Computer System Science & Enginnering*, 1991, 6(3): 185–188.

[6] Wang Xu-zheng and Lin Ya-qi. A Scheme of Fast Key Recovery on Broadcast Network upon on the Three-center-location of a Triangle. Proceedings of 2000 Workshop on internet & Distributed Systems at MCKU, 2000. 10.

[7] 陈昭智, 郑建德. 一种基于身份分层结构加密算法的广播加密方案. 厦门大学学报, 2006, 45(3): 342–346.

[8] 谭作文, 刘卓军, 肖红光. 一个安全公钥广播加密方案. 软件学报, 2005, 16(7): 1333–1343.

[9] Lin J F and Chen S J. Comment on broadcasting cryptosystem in computer networks using interpolating polynomials. *Computer Systems Science & Engineering*, 1996, 11(5): 315–317.

[10] Shamir A. How to share a secret. *Communications of the ACM*, 1979, 22(4): 612–613.

王尚平： 男，1963 年生，教授，博士，研究方向为密码理论与网络安全.

解康乐： 男，1982 年生，硕士生，研究方向为密码理论与网络安全.

王晓峰： 女，1966 年生，副教授，博士，研究方向为密码理论与网络安全.

丁如意： 男，1983 年生，硕士生，研究方向为密码理论与网络安全.