# 一种抗共谋的非对称公钥叛逆者追踪方案*)

张学军　周利华　王育民

(西安电子科技大学计算机网络与信息安全教育部重点实验室　西安 710071)

**摘　要**　将会话密钥 S 分解成 $S_1$ 与 $S_2$ 之和。在大整数分解困难问题的条件下，构造特殊多项式函数来解密 $S_1$(方案 1)。在离散对数困难问题的条件下，利用中国剩余定理来解密 $S_2$(方案 2)。在两种方案组合的基础上形成一种新的叛逆者追踪方案。新方案兼有前两种方案的共同优点，同时弥补了它们各自的不足。新方案具有抗共谋性、非对称性、用户密钥的耐用性、黑盒子追踪等优越特性。

**关键词**　抗共谋，非对称，用户密钥的耐用性，黑盒子追踪

## A Collusion-resistant Asymmetric Public-key Traitor Tracing Scheme

ZHANG Xue-Jun　ZHOU Li-Hua　WANG Yu-Min

(The Ministry of Edu. Key Lab. of Computer Network and Info. Security, Xidian Univ., Xi'an 710071)

**Abstract**　The session key S is divided into a sum of $S_1$ and $S_2$. Under the condition of large integer factoring problem, $S_1$ is decrypted by constructing a special polynomial function(scheme 1). Under the condition of discrete logarithm problem, $S_2$ is decrypted by Chinese Remainder Theorem(scheme 2). On the basis of a combination of the scheme 1 and scheme 2, a new traitor tracing scheme is formed, which has both advantages of them, meanwhile overcomes their disadvantages. It has many advantages such as collusion-resistance, asymmetry, long-lived subscriber's key, and black-box tracing.

**Keywords**　Collusion-resistance, Asymmetric, Long-lived subscriber's key, Black-box tracing

## 1　引言

加密数据(如付费电视、广播加密、在线数据库)的安全分发是现代信息社会的一个重要问题。数据提供商 DS 通过广播信道向授权用户提供加密信息。授权用户用自己的密钥先将加密数据包头中的会话密钥解密，然后用得到的会话密钥解密加密数据。如果恶意的授权用户将自己的密钥泄露给别的非法用户使用，或者某些授权用户先共谋制造出密钥然后让非法用户使用，那么这些恶意的授权用户就称为叛逆者，非法用户称为盗版者，通过盗版者的解码器分析出叛逆者的工作则称为叛逆者追踪。在这种应用场合，叛逆者追踪作为保障数据安全分发并保护数据提供商合法权益的手段，成为当前的研究热点。

叛逆者追踪的概念首先由 Chor, Fiat, Naor 提出[1]，此后各种叛逆者追踪方案相继被提出来[2~10]。其中文[1～4]中的方案都是对称方案，不具有不可否认性。Pfitzmann 在文[5]中首先提出的非对称叛逆者追踪方案解决了对称方案中存在的问题，即只有授权用户自己知道自己的密钥，数据提供商无法陷害因而叛逆者无法抵赖，但其方案效率不高，无法实际应用。另外，这些方案[2~10]都不能阻止共谋的发生。文[11]提出了一种付费电视方案，但其方案也是对称方案，并且还属于私钥方案(加密数据包头的加密钥保密，只有特定的人才能发送加密数据)。文[10]提出了一种完全的非对称公钥叛逆者追踪方案，当增加用户或者撤消用户时，无需改变现有用户的秘密钥，但是其方案不能抵抗共谋攻击。因此，本文提出了一种抗共谋攻击的非对称公钥叛逆者追踪方案，其主要思想是将会话密钥 S 分解成 $S_1$ 与 $S_2$ 之和。在大整数分解困难问题的条件下，构造特殊多项式函数来解密 $S_1$(方案 1)。在离散对数困难问题的条件下，利用中国剩余定理来解密 $S_2$(方案 2)。在两种方案组合的基础上形成一种新的叛逆者追踪方案。新方案兼有前两种方案的共同优点，同时弥补了它们各自的不足。新方案具有抗共谋性、非对称性、用户密钥的耐用性、黑盒子追踪等优越特性。

## 2　方案 1 简介

该方案是文[11]中方案的修改方案，原方案和本文修改后的方案的比较见表 1。

表 1　方案[11]和本文修改后的方案的比较

| | 算法类型 | 抗共谋攻击 | 增加/撤消用户 | 用户密钥耐用性 |
|---|---|---|---|---|
| 方案[11] | 私钥算法 | 不支持 | 支持 | 部分支持 |
| 修改后的方案 | 公钥算法 | 支持 | 支持 | 部分支持 |

假定系统有 3 个实体：系统管理员(System Manager, SM)、数据提供商(Data Supplier, DS)和用户。SM 负责建立系统参数、公钥、主密钥并公布公钥等，查获盗版解码器后追踪叛逆者，DS 加密数据并发送加密数据给用户。

### 2.1　系统设置

系统管理员 SM 首先选择大整数 $N=pq$，其中 $p=2p'+1, q'=2q'+1$，且 $p,q,p',q'$，均为大素数，$\phi(N)=(p-1)(q-1)$。随机选取 $0<x_i<\phi(N), i=0,1,2,\cdots,n$，则次数为 $n$ 的

*)国家自然科学基金重大计划项目(90204012)、国家"863"计划项目(2002AA143021)。张学军　副教授，博士生，研究方向：信息安全、叛逆者追踪；周利华　教授，博士生导师；王育民　教授，博士生导师。

多项式函数 $f(x)$构造如下：

$$f(x)=\prod_{i=1}^{n}(x-x_i)\equiv\sum_{i=0}^{n}a_i x^i \pmod q$$

其中系数$\{a_i\}$为：$a_0=\prod_{j=1}^{n}(-x_j)$，$a_1=\sum_{i=1}^{n}\prod_{i\neq j}^{n}(-x_j)$，…，$a_{n-2}=\sum_{i\neq j}^{n}(-x_i)(-x_j)$，$a_{n-1}=\sum_{i=1}^{n}(-x_j)$，$a_n=1$，注意到$\sum_{i=0}^{n}a_i x_j^i$。有了$\{a_i\}$就可构造相应的指数形式，随机选取 $0<g<N$，$\{g^{a0},g^{a1},\cdots,g^{an}\equiv\{g_0,g_1,\cdots,g_n\}$所有元素都是在模下运算的。为了方便，以下叙述中忽略模。注意到$\prod_{i=0}^{n}g_i^{r_j^i}=1$。

假设 $n$ 为最大用户数的上限，实际用户数为 $m$，$0<m\leqslant n$，$n-m$ 提供新用户加入系统时用。以下步骤将构造加密公钥和用户解密密钥：

Step1：选择 $n$ 个不同的随机数 $0<x_i<\phi(N)$，$i=1,2,\cdots,n$，形成集合 $\chi_n$，子集 $\chi_m\subset\chi_n$。

Step2：计算 $A=\prod_j^n=1(\prod_{i=0}^{n-1}g_i^{r_j^i})$ mod $N$。

*Step*3：计算 $\bar{x}_i=\sum_{k=1,k\neq i}^{n}x_k^n \ mod\ \phi(N)$。

*Step*4：计算 $\hat{x}_i=bx_i^n \ mod\ \phi(N)$，$i=1,2,\cdots,n$，随机数 $0<b<\phi(N)$。

*SM* 的主密钥 SK 为 f(x)和 p,q,$\phi$(N)，公钥 PK=(N,g,$g^b$,$A^b$)。

### 2.2 用户注册

用户 $i$ 注册时，系统管理员 SM 将$(\bar{x}_i,\hat{x}_i)$发送给 $i$ 作为其密钥，相应的定购单为 $text=i\parallel\bar{x}_i\parallel\hat{x}_i\parallel(g^{br_i}\parallel g^{x_i})$ mod $N$。

### 2.3 加密算法

DS 选 $0<\bar{s}<N$ 作为加密消息时使用的会话密钥，随机数 $0<r<\phi(N)$，计算 $\bar{g}=g^r$，$\hat{g}=g^{br}$，$c=\bar{s}A^{br}$，广播三元组密文$(\bar{g},\hat{g},c)$。

### 2.4 解密算法

用户 $i$ 收到三元组密文$(\bar{g},\hat{g},c)$后利用自己的密钥$(\bar{x}_i,\hat{x}_i)$计算出 $\bar{s}$：

$$c.\hat{g}^{\bar{x}_i}\bar{g}^{\hat{x}_i}=\bar{s}$$

**定理 2.1**(正确性)　经过注册的合法用户能够按照上述的解密算法正确解密。

证明：合法用户 $i$ 利用自己的解密钥$(\bar{x}_i,\hat{x}_i)$进行如下计算：

$$c.\hat{g}^{\bar{x}_i}\bar{g}^{\hat{x}_i}=\bar{s}A^{br}g^{br\sum_{k=1,k\neq i}^{n}x_k^n}g^{r\hat{x}_i}=\bar{s}A^{br}g^{br\sum_{k=1}^{n}x_k^n}$$

$$=\bar{s}(\prod_{j=1}^{n}\prod_{i=0}^{n}g_i^{r_j^i})^{br}=\bar{s}$$

上式中最后一个等式基于$\prod_{j=1}^{n}\prod_{i=0}^{n}g_i^{r_j^i}=1$。

**定理 2.2**(安全性)　假设在大整数分解困难问题的情况下，上述方案被动攻击者能解密的概率为 $n/N^2$，其中 $n$ 表示最大用户数的上限，$N=pq$ 表示大整数。

证明：如果被动攻击者在没有合法密钥的情况下，能从密文$(\bar{g},\hat{g},c)$解密获得 $\bar{s}$(mod $N$)，假定被动攻击者选取的密钥为$(s_1,s_2)$，则被动攻击者正确选对 $s_1$ 的概率为 $n/N$(因为在小于的值中只有 $n$ 个值是合法用户的值)。假设 $s_1$ 已经正确选择，那么选对 $s_2$ 的概率为 $1/N$。所以正确选对 $s_1,s_2$ 从而能正确解密的概率为$(n/N)\times(1/N)=n/N^2$。为 $n<<N$，从而 $n<<N^2$，这说明被动攻击者能正确解密的概率是可以忽略的。

**定理 2.3**(抗共谋性)　若用户共谋上限为 $k(k<n)$，则此方案共谋成功计算上不可行。

证明：不失一般性，先假设有两个合法用户 $i$ 和 $j$，其解密钥分别为$(\bar{x}_i,\hat{x}_i)$和$(\bar{x}_j,\hat{x}_j)$。若这两个用户共谋，则有两种形式的共谋密钥，下面予以详细讨论。

第一种情况，其密钥形式为$(\theta\bar{x}_i+(1-\theta)\bar{x}_j,\theta\hat{x}_i+(1-\theta)\hat{x}_j)$，其中 $0<\theta,(1-\theta)<\phi(N)$，且$-\theta$ 为 $\theta$ 关于 $\phi(N)$的加法逆元。首先，若先求出 $\phi(N)$，然后求出 $\theta$ 关于 $\phi(N)$的加法逆元$-\theta$。这种情况显然不可能，因为这等价于大整数分解困难问题。其次，若不知道 $\phi(N)$而直接由计算 $\theta$ 出$-\theta$。此时 $\theta+(-\theta)=\phi(N)$，由此等式可解出 $\phi(N)$，从而攻破大整数分解困难问题，导致矛盾。

第二种情况，其密钥形式为$(\theta_i\bar{x}_i+\theta_j\bar{x}_j+\theta_i\hat{x}_i+\theta_j\hat{x}_j)$，另外还需再附加$(\theta_i+\theta_j)^{-1}$，其中 $0<\theta_i,\theta_j<\phi(N)$，$(\theta_i+\theta_j)^{-1}$为$(\theta_i+\theta_j)$关于 $\phi(N)$的乘法逆元。首先，若先求出 $\phi(N)$，然后求出$(\theta+\theta$ 关于 $\phi(N)$的乘法逆元$(\theta_i+\theta_j)^{-}1$。这种情况显然不可能，因为这等价于大整数分解困难问题。其次，若不知道 $\phi(N)$而直接由$(\theta_i+\theta_j)$计算出$(\theta_i+\theta_j)^{-1}$，此时$(\theta_i+\theta_j)\cdot(\theta_i+\theta_j)^{-1}=k\phi(N)+1$，其中 $0\leqslant k<\phi(N)$。“有一半的整数是偶数，大约 92%的大奇数有一个小于 $10^6$ 的素数因子，大约 96%的大整数有一个小于 $10^6$ 的素数因子”[13]。我们来分析分解 $k$ 从而求出 $\phi(N)$的概率，考虑 $N$ 为 1024 位二进制长度的情况，此时 $N\approx10^{308}$，因此 $k<10^{308}$，$k<k_1k_2\cdots k_{52}$，其中每个 $k_i<10^6$。根据文[13]的结果可知能分解 k 的概率不低于$(96\%)^{52}\approx12\%$，这意味着能以不可忽略的概率(>12%)计算出 $\phi(N)$从而攻破大整数分解困难问题，导致矛盾。

综合两种情况，对于任意两个共谋用户，上述方案共谋成功在计算上是不可行的。

对于用户共谋数量为 $c(2<c<n)$的情况也有类似的结论。

## 3 方案 2

该方案是文[10]提出的方案。

设 $m$ 是实际用户数，选择素数 $p_i=2q_i+1$，其中 $q_i$ 是奇素数。为方便，假设 $p_1<p_2\cdots<p_m$。上述素数的选择要使得 $q_1^{1/2}$ 足够大。令 $M=\prod_{i=1}^{m}p_i$。设 $\hat{g}$ 是模每一个 $p_i$ 的公共素根，由中国剩余定理可知这样的 $\hat{g}$ 是存在的。

### 3.1 密钥和公钥的建立

首先，用户 $i$ 随机选择密钥 $d_i\in Z_{p_i}^*$，发送$(\beta_i,p_i)$给 SM，其中 $\beta_i=\hat{g}^{d_i} \bmod p_i$。其次，SM 计算 $\beta=\sum_{i=1}^{m}\beta_iM_iy_i \bmod M$，其中 $M_i=M/p_i$，$M_iy_i\equiv1 \pmod{p_i}$，$1\leqslant i\leqslant m$。不难发现 $\beta\equiv\beta_i \pmod{p_i}$。三元组$(\beta,\hat{g},M)$就是公钥。

### 3.2 加密

令明文 $x\in Z_{p1}$。DS 从中选择 $r\in_R\{0,1,\cdots,p_1-1\}$并计算 $z_1=\hat{g}^r \bmod M$，$z_2=x\beta \bmod M$。密文为 $C=(z_1,z_2)$。

### 3.3 解密

$$x=z_2(z_1^{d_i})^{-1} \bmod p_i$$

**定理 3.1**[10]　方案 2 对被动的攻击者是语义上安全的。

## 4 新方案

除非另作说明，以下的符号含义同第 2、3 小节中的说明。

SM 的主密钥 *SK* 为 $f(x)$和 $p,q,\phi(N)$，公钥为 $PK=(N,g,g^b,A^b)\parallel(\beta,\hat{g},M)$。

### 4.1 用户注册

用户 $i$ 注册时，产生的密钥为：$(\bar{x}_i,\hat{x}_i)\parallel d_i$，相应的定购单为：

$$text=i\parallel\bar{x}_i\parallel\hat{x}_j\parallel(g^{br_i}\parallel g^{x_i}) \bmod N\parallel\hat{g}^{d_i} \bmod p_i$$

### 4.2 加密算法

DS 随机选 $0<\bar{s}<N$ 作为加密消息时使用的对称密钥，不妨设 $p_1<p_2<\cdots p_m<N$。令 $\bar{s}=\bar{s}_1+\bar{s}_2$，其中 $\bar{s}_1<N$，$\bar{s}_2<$

$p_1$，选择 $r\in_R Z_{p_1}$。DS发送的五元组密文头为：

$((\bar{g},\hat{g},c) \bmod N, z_1, z_2)=((g^r, g^{hr}, \bar{s}_1, A^{hr}) \bmod N, \hat{g}^r \bmod M, \bar{s}_2\beta \bmod M)$

### 4.3 解密算法

用户 $i$ 收到密文头后利用自己的频道解密钥 $(\bar{x}_i,\hat{x}_i)\|d_i$，按以下步骤获得明文：

Step1：利用第2.5小节解密算法可得到 $\bar{s}_1 \bmod N$。

Step2：利用第3.3小节解密方法可得到 $\bar{s}_2 \bmod p_i$。

Step3：$\bar{s}_1 \bmod N+\bar{s}_2 \bmod p_i=(\bar{s}_1+\bar{s}_2) \bmod N=\bar{s} \bmod N=\bar{s}$。

说明：因为 $\bar{s}_2<p_1$，$p_1<p_2<\cdots<p_m<N$ 所以有 $\bar{s}_2 \bmod p_i=\bar{s}_2 \bmod N$。

### 4.5 追踪算法

当SM得到一个密钥为 $(\alpha_1,\alpha_2)\|d_i$ 的盗版解码器后，任选2个线性无关的向量 $\bar{Z}_j=(z_{j1},z_{j2})0<z_{j1}<z_{j2}<\phi(N)$，$j=1,2$，(如向量(3,3)，(4,3)就是2个线性无关的向量)，构造2个非法密文头(盗版解码器不能识别合法密文头与非法密文头[2])：

$$C_j=((g^{hz_{j1}}, g^{z_{j2}}, W) \bmod N, g^r \bmod M, \bar{s}_2\cdot\beta^r \bmod M)$$
$$=((h_1^{z_{j1}}, h_2^{z_{j2}}, W) \bmod N, g^r \bmod M, \bar{s}_2\beta^r \bmod M)$$

当输入一个非法密文头 $C_j$ 给解码器时，解码器按照正常的解密算法输出一个值 $R_j$。通过输入2个非法密文头 $C_j$，$j=1,2$，得到2个不同的输出

$$R_j=(Wh_{j1}^{z_{j1}a_1}h_{j2}^{z_{j2}a_2})+\bar{s}_2 (\bmod N) \quad (1)$$

由(1)式联立可解出 $h_1^{a_1}$，$h_2^{a_2}$，也就是 $g^{ha_1}$，$g^{a_2}$。通过比较确定出与 $g^{ha_1}$，$g^{a_2}$ 相对应的定购单 $text=i\|\bar{x}_i\|\hat{x}_j\|(g^{\bar{x}_i}\|g^{\hat{x}_i}) \bmod N\|\hat{g}^{d_i} \bmod p_i$，即用户 $i$ 为叛逆者。因为具有非对称性，所以SM可以向第三方提供不可否认证据，即用户不能抵赖其叛逆行为。

### 4.6 用户密钥的耐用性

用户密钥的耐用性是指当增加用户或者撤消用户时无需改变现有用户的密钥，而只需改变公钥 $PK=(N,g,g^b,A^b)\|(\beta,\hat{g},M)$ 即可。

假设用户 $\gamma$ 已被撤消(用户 $\gamma$ 是叛逆者或者自愿离开系统)，则SM进行如下操作：

第一步，计算新的 $A$。$A'=(\prod_{j=1,j\neq\gamma}^{n}(\prod_{i=0}^{n-1}g_i^{x_j^i}))g^{-x_\gamma^n}$ 注意到如果所有数据在系统设置阶段已经存贮的话，那么只需从原来的 $A$ 中去掉与用户 $\gamma$ 相应的部分即可得到 $A'$。

第二步，计算新的 $M$。$M'=Mp_\gamma^{-1}$。

第三步，公布新的公钥 $PK$。

$$PK=(N,g,g^b,A'^b)\|(\beta',\hat{g},M')=(N,g,g^b,A'^b)\|(\beta \bmod M',\hat{g},M')$$

这样一来，用户 $\gamma$ 由于不能正确解密 $\bar{s}_1$，$\bar{s}_2$，进而也不能解密 $\bar{s}$，从而其密钥就失效了，但是现有用户的密钥此时无需改变。

假设一个新用户 $m+1$ 加入这个系统，那么SM只需重新计算 $PK$ 中的 $(\beta,\bar{g},M)$：

$(\hat{\beta},\hat{g},\hat{M})=(\beta p_{m+1}v+\beta_{m+1}Mw \bmod Mp_{m+1},\hat{g},Mp_{m+1})$，其中 $p_{m+1}$ 是新的素数且不同于 $p_1,p_2,\cdots,p_m$，$p_mv\equiv1(\bmod M)$，$Mw\equiv1(\bmod p_{m+1})$。SM公布新的 $PK$ 为：

$$PK=(N,g,g^b,A^b)\|(\hat{\beta},\hat{g},\hat{M})$$

这样一来，合法的新用户 $m+1$ 虽然能解密加入系统前的 $\bar{s}_1$，但是不能解密加入系统前的 $\bar{s}_2$，进而也不能解密加入系统前的 $\bar{s}$，现有用户的密钥此时也无需改变。

### 4.7 安全性分析

(1)新方案对被动攻击者来说能成功解密的概率可以忽略。

由定理2.2可知，假设大整数分解问题困难的情况下，方案1中被动攻击者能成功解密 $\bar{s}_1$ 的概率不超过 $n/N^2$，可以忽略，其中 $n$ 表示用户总数，$M=pq$ 表示大整数。由定理3.1可知，方案2对被动攻击者是语义上安全的，成功解密 $\bar{s}_2$ 的概率可以忽略。因此新方案对被动攻击者来说能成功解密 $\bar{s}=\bar{s}_1+\bar{s}_2$ 的概率可以忽略。

(2)如果用户共谋数量的上限为 $k(k<n)$，则新方案共谋成功在计算上不可行。

由定理2.3可知，若用户共谋数量上限为 $k$，则方案1共谋成功在计算上不可行，即共谋解密出 $\bar{s}_1$ 在计算上不可行。方案2不能抵抗共谋，即共谋可解密出 $\bar{s}_2$。新方案中要共谋计算出 $\bar{s}=\bar{s}_1+\bar{s}_2$ 才算共谋成功。但是新方案中，由于共谋解密出 $\bar{s}_1$ 在计算上不可行，因此即使共谋计算出其中的 $\bar{s}_2$，仍不能成功计算出 $\bar{s}$。所以，如果用户共谋数量的上限为 $k(k<n)$，则新方案共谋成功在计算上不可行。

(3)新方案具有前向安全性和后向安全性。

由第4.6节的分析可知，用户被撤消后，公钥已经改变，公钥中与被撤消用户相关部分的信息已经被去掉，因此被撤消用户不能再解密未来的加密信息，所以新方案具有前向安全性。另一方面，增加新用户后，新方案中对应于方案2中的公钥部分已经改变，虽然新方案中对应于方案1中的公钥部分没有改变，即可解密出 $\bar{s}_1$。但是新方案中需要计算出 $\bar{s}=\bar{s}_1+\bar{s}_2$，由于新增加的用户不能计算出 $\bar{s}_2$，因此也不能计算出 $\bar{s}$，所以新方案具有后向安全性。

### 4.8 同其它有关方案的性能比较

表2 本文方案同其它有关方案的性能比较

| | 文[2] | 文[10] | 文[11] | 文[12] | 本文方案 |
|---|---|---|---|---|---|
| 算法类型 | 公钥 | 公钥 | 私钥 | 公钥 | 公钥 |
| 非对称性 | 不支持 | 支持 | 不支持 | 不支持 | 支持 |
| 抗共谋攻击 | 不支持 | 不支持 | 不支持 | 不支持 | 支持 |
| 增加/撤消用户 | 不支持 | 支持 | 支持 | 不支持 | 支持 |
| 用户钥耐用性 | 不支持 | 支持 | 部分支持 | 不支持 | 支持 |
| 黑盒追踪 | 低效 | 较高效 | 不支持 | 高效 | 高效 |

**结束语** 本文提出了一种抗共谋的非对称公钥叛逆者追踪方案，具有如下优越特性：

(1)抗共谋，能阻止叛逆者共谋的发生；

(2)非对称，DS可以向第三方提供不可否认证据，即用户不能抵赖其叛逆行为；

(3)用户密钥的耐用性，当增加用户或者撤消用户时无需改变现有用户的密钥；

(4)黑盒子追踪，不用打开盗版者的解码器，只通过请求/应答的方式追踪叛逆者。

## 参 考 文 献


1 Chor B, Fiat A, Naor M. Tracing traitors. In: Advances in Cryptology-CRYPT'94[C], LNCS. Springer-Verlag, 1994, 839: 257～270

2 Boneh D, Franklin F. An efficient public key traitor tracing scheme. In: Proc. of CRYPTO'99[C], LNCS. Springer-Verlag, 1999, 1666: 338～353

3 Tzeng, Wen-Guey, Tzeng Zhi-Jia. A public-key traitor tracing scheme with revocation using Dynamic shares. In: PKC 2001[C]. LNCS. Springer-Verlag, 2001, 1992: 207～224


(下转第127页)

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

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