·密码学·

一种新的可实现安全公钥密码体制
—— 4次同余方程的应用

王泽辉[1]，张治国[2]

(1. 中山大学科学计算与计算机应用系 广州 510275; 2. 中山大学计算机科学系 广州 510275)

【摘要】提出了一种新的、可实现安全的公钥密码体制，在采用原有的公钥、私钥的基础上，增加数量庞大、开销极低的公开参数集合；在每加密一批数据时选择一组新的不重复公开参数。提出了判断4次同余方程解结构及其求解的线性时间快速算法，以实现公开参数集合的操作。该安全方案可以主动抵御选择明文攻击与各种选择密文攻击，包括IND-CCA2，并且可以达到类似一次一密的安全效果。对于大批量数据的加密解密，计算和存储开销集中于第一个数据，自第二个之后只需要简单的异或操作；可应用于如RFID标签的低端产品或如无线网络等计算、存储、带宽等资源受到极大限制的设备中。

关 键 词 选择密文攻击; 信息安全; 一次一密; 4次同余方程; 快速算法
中图分类号 TP309 文献标识码 A

A Novel Security-Ensured Public Key Cryptosystem
——A Quartic Congruential Equation Approach

WANG Ze-hui[1]，ZHANG Zhi-guo[2]

(1. Department of Scientific Computation and Computer Applications, Sun Yat-sen University Guangzhou 510275;
2. Department of Computer Science, Sun Yat-sen University Guangzhou 510275)

Abstract For improving the efficiency and the potential for actively protecting against attacks, a novel security-ensured public key cryptosystem is proposed. The idea is that a large set of published parameters, which are generated with almost no more overheads, is taken into account in addition to the original public and private keys. A new set of published parameters will be chosen when a group of data to be encrypted each time. The linear time quick algorithms for deciding the solution structure and computing the solution of the quartic congruential equations are proposed for implementing the operations on the published parameters. This cryptosystem can actively protect against the chosen plaintext and the various chosen ciphertext attacks including IND-CCA2 attacks. It achieves the same security like One-Time-Pad. For the repeated encryption/decryption for a set of data the requirements for computation and memory size are deeply decreased because only a series of XOR operations are needed after first data item has been encrypted/decrypted. Due to this reason, this cryptosystem may be used in very low-end devices, such as RFID tags, sensor networks, where the computation, memory and bandwidth are very limited.

Key words chosen ciphertext attack; information security; one-time-pad; quartic congruential equation; quick algorithm

到目前为止，成熟的公钥密码体制主要基于两类著名的数学难题：大整数分解的困难性及求解各种离散对数困难性，由此诞生了RSA、ECC、XTR等公钥密码体制[1-3]。同时也开展了对基于其他困难问题的公钥体制的研究，如基于格上难题的NTRU体制。但底层的数学难题并不能保证密码体制的绝对安全性，反而增加了生成密钥的开销，因此无论RSA还是ECC，其密钥总是少而精。公钥密码体制的重要发展方向是构造可证明安全的密码体制[4-5]，要求包括抗不可区分适应性选择密文攻击的安全性

收稿时间：2007– 07– 21
基金项目：广东省自然科学基金(7003624)
作者简介：王泽辉(1963 –)，男，副教授，主要从事数论快速算法、新型密码与信息安全技术等方面的研究；张治国(1962 –)，男，副教授，主要从事系统描述与验证、计算理论、网络与系统安全等方面的研究.

(IND-CCA2安全)。这种安全定义给予攻击者最大的权限，攻击者可以收集足够多的明文-密文对。如果分析得到的密钥信息或密文信息几乎可以忽略，那么密码体制就是安全的。因此在这种安全定义下，密码体制的密钥一成不变，加密者是“被动挨打”的。由此安全带来的代价是同样的明文，加密成的密文(组)比原来更加膨胀，在实现中需要消耗更多的资源。在诸如RFID标签、无线网络等低成本设备中，由于计算、存储、带宽等资源受到极大的限制，这种公钥密码体制的实现变得非常困难[6-7]。

基于以上分析，本文提出公钥密码体制安全性的新观点，公钥密码安全可以主动抵御攻击。只要能满足以下条件：保证加密解密协议在各种密码分析攻击手段下，泄漏的密钥信息或明文信息几乎可忽略，其极端情况是一次一密。但完全意义的一次一密的密钥信息量应不低于明文的信息量，必须解决加密解密参数的开销问题，只有在新增开销几乎可以忽略时才能效仿一次一密方式。

本文提出建立公钥密码体制以满足安全性要求的思路如下：在采用原有的公钥、私钥的基础上(其比特数可保证在现有计算机资源下不被破译)，增加数量庞大的公开参数集合——造成的新开销几乎可以忽略。类似一次一密的做法，每一次加密(解密)变换需要采用固定的公钥(私钥)，且需要选择一组新的公开参数(保证不重复)；当公开参数集合元素使用到达一半时，更换公钥、私钥，生成对应的公开参数集合。

采用上述思路建立的公钥密码体制可以主动抵御攻击，数学难题保证了私钥的不可破译性，且攻击者即使收集足够多的明文-密文对，分析成功也只是已经公开的参数。只要公开参数的集合足够大，预测下一个公开参数的有效性几乎为零，因此各种选择明文、选择密文攻击手段对于一批挑战密文的有效性几乎为零。另外，本文构造特殊的加密解密变换，使对于诸如RFID标签、无线网络等低成本，且计算、存储、带宽等资源受到极大的限制的设备，能节省大量的计算和存储开销。

本文假定n为正整数时，F_n为模n的剩余类、$X(\mathrm{mod}\ n)$作为取值符号表示时，当X为整数时值取模n的非负最小剩余，即在$\{0,1,\cdots,n-1\}$中取值；当X为多项式时，系数值取模n的非负最小剩余。$F_n[x]$为系数在F_n的多项式环。

1 保证公钥体制安全性的新方案

本文设p、q为接近1 024 b的安全素数，$n=pq$为2 048 b，那么以现有计算机资源为基础，近期内无法由n分解出p、q。公布n为公钥，p、q为私钥，利用n值随机选取F_n新增加的开销几乎为零。

一个安全哈希函数为$H:\{0,1\}^{2\,048}\rightarrow\{0,1\}^{512}$，由$H(\alpha)$求512 b的$\alpha$几乎不可能。设$F_4(x)=x^4-\theta_1x^3+\theta_2x^2-\theta_3x+\theta_4$，考虑4次同余方程为：

$$F_4(x)\equiv 0(\mathrm{mod}\ n) \tag{1}$$

式中 $\theta_i\in F_n$，$i=1,2,3,4$；$\theta_4\neq 0$。取$(\theta_1,\theta_2,\theta_3,\theta_4)$为公开参数，则其全集元素数为$n^3(n-1)$，$n^3(n-1)/2$的比特数接近8 000。考虑到对称密码体制AES的安全密钥仅为256 b及解4次同余方程的相应计算量，当已经公布的公开参数总数低于$n^3(n-1)/2$时，预测下一组将使用的$(\theta_1,\theta_2,\theta_3,\theta_4)$有效性几乎为零。当公开参数列表数目高于$n^3(n-1)/2$时更换$n$值，密码体制对应于新的$n$即使取同一组$(\theta_1,\theta_2,\theta_3,\theta_4)$，意义完全不同。

同Rabin密码体制的分析一样，当已知私钥p、q时，由解$F_4(x)\equiv 0(\mathrm{mod}\ p)$与$F_4(x)\equiv 0(\mathrm{mod}\ q)$可得到式(1)的解；而不知道私钥$p$、$q$时，求解式(1)的困难性等同于由$n$分解出$p$、$q$，几乎不可能。

1.1 任意第三方的加密方案

设已公布n为公钥，已经使用的公开参数列表为$\{(\theta_1^*,\theta_2^*,\theta_3^*,\theta_4^*)\}$，总数量低于$n^3(n-1)/2$。任意第三方将一批明文分为每512 b一组，设为$\{m_1, m_2,\cdots\}$。其中，一批的含义是加密者确信其中的明文都是自己想加密的而未含异己的(对于最高安全数据，每一批明文只有一组)。任意第三方加密前选择F_n中的4个不同随机数$\alpha_i\in F_n\backslash\{0\}$, $i=1,2,3,4$，计算可得：

$$\begin{cases}\theta_1=\alpha_1+\alpha_2+\alpha_3+\alpha_4(\mathrm{mod}\,n)\\ \theta_2=\alpha_1(\alpha_2+\alpha_3+\alpha_4)+\alpha_2(\alpha_3+\alpha_4)+\alpha_3\alpha_4(\mathrm{mod}\,n)\\ \theta_3=\alpha_1\alpha_2(\alpha_3+\alpha_4)+(\alpha_1+\alpha_2)\alpha_3\alpha_4(\mathrm{mod}\,n)\\ \theta_4=\alpha_1\alpha_2\alpha_3\alpha_4(\mathrm{mod}\,n)\end{cases} \tag{2}$$

式中 $\theta_i\in F_n$。如果生成的$(\theta_1,\theta_2,\theta_3,\theta_4)$在列表中，则重新选择$\{\alpha_i\}$，按式(2)重计$\{\theta_i\}$直到不在列表中为止。由韦达定理和中国剩余定理可知，式(1)在F_n中的解包含α_i，用4比特数ε表示按从小到大排序α_1的顺序(α_1排在第$\varepsilon+1$个)。利用前述函数H计算$H(\alpha_1)$，加密变换为：

$$c_i=E_k(m_i)=m_i\oplus H(\alpha_1)\qquad i=1,2,\cdots \tag{3}$$

式中 $\oplus$为按比特逻辑异或，本批次的明文组$\{m_1,m_2,\cdots\}$对应的密文组为$\{\theta_1,\theta_2,\theta_3,\theta_4,\ \varepsilon,\ c_1,c_2,\cdots\}$。

解密时，解$F_4(x)\equiv 0(\mathrm{mod}\ p)$与$F_4(x)\equiv 0(\mathrm{mod}\ q)$，采用中国剩余定理得到式(1)在$F_n$中的全部解，排序后用$\varepsilon$可从中确定出$\alpha_1$。计算$H(\alpha_1)$后，解密变换为：

$$m_i=D_k(c_i)=c_i\oplus H(\alpha_1)\quad i=1,2,\cdots \tag{4}$$

1.2　己方(获悉私钥方)的加密方案

加密前选择F_n中的2个不同随机数$\alpha_i\in F_n\backslash\{0\}$, i=1,2；选择随机数u、v，使$(u^2-4v)^{(p-1)/2}(\mathrm{mod}\ p)=1$，$(u^2-4v)^{(q-1)/2}(\mathrm{mod}\ q)=1$，即$x^2-ux+v$为$F_p[x]$与$F_q[x]$中不可约多项式，计算$(x-\alpha_1)(x-\alpha_2)(x^2-ux+v)(\mathrm{mod}n)=x^4-\theta_1x^3+\theta_2x^2-\theta_3x+\theta_4$，则$\theta_i\in F_n$。如果生成的$(\theta_1,\theta_2,\theta_3,\theta_4)$在列表中，则重新选择$\{\alpha_1,\ \alpha_2,\ u,\ v\}$，重计$\{\theta_i\}$直到不在列表中为止。由式(1)可知，在$F_n$中的解包含$\alpha_i$，用4比特数$\varepsilon$表示$\alpha_1$的顺序。其余的加密、解密过程同任意第三方的方案，本文不赘述。

1.3　安全性与效率分析

由于同一批明文不含异己，即使破译者挑选的明文也只存在于自己所属的一批，得到是不同于其他批的参数。由式(3)可知，要破译其他批密文必须知道$H(\alpha_1)$，但$H(\alpha_1)$是一个安全散列函数的值，近乎随机值。如果不清楚α_1，只能靠穷举。在现有计算机资源下，512 b的散列函数穷举是无效的，α_1只能靠求解$F_4(x)\equiv0(\mathrm{mod}\ p)$与$F_4(x)\equiv0(\mathrm{mod}\ q)$，难度相当于从$n$解出$p$、$q$。根据文献，分解2 048 b的模$n$在现有计算机资源下是无效的。采取选择明文与选择密文的攻击，即使是不可区分适应性选择密文攻击，无法分解出p、q，至多可以得到公开参数表$\{(\theta_1^*,\theta_2^*,\theta_3^*,\theta_4^*,)\}$不含挑战密文所用的全部元素。要预测一批挑战密文所用的或下一个将使用的$(\theta_1,\theta_2,\theta_3,\theta_4)$，有效性几乎为零(对一批数据仅一组的加密方案结论更明显)。无法预测就解不出新的α_1，也得不到$H(\alpha_1)$，因此有以下定理：

定理 **1**　采用任意第三方与己方方案，可保证密文不被破译，各种选择明文与选择密文的攻击包括IND-CCA2，对一批挑战密文所得到的有用信息量几乎可忽略，即密码体制是可实现安全的。

从效率上看，在使用了公钥n的基础上，生成$(\theta_1,\ \theta_2,\ \theta_3,\ \theta_4)$新增的计算机开销几乎为零。而每传输一批数据，密文组只增加公开参数$\{\theta_1,\ \theta_2,\ \theta_3,\ \theta_4,\ \varepsilon\}$至多是4×2 048+4=8 192 b。对于每批的L×512 b明文而言(L是大整数)，密文相对于明文几乎没有膨胀；一对密钥$(n,\ p,\ q)$只有参数集使用近半才更换，可节省密钥资源，提高效率。

2　4次同余方程F_n中根的求解

考虑3次同余方程为：

$$f(x)=x^3+b_1x^2+b_2x+b_3\equiv0(\mathrm{mod}\ p) \tag{5}$$

式中　p为奇素数；$b_3\equiv0(\mathrm{mod}\ p)$不成立($b_3\equiv0(\mathrm{mod}\ p)$退化为2次或1次同余方程更易解)。设$x_1$、$x_2$、$x_3$为$f(x)$在其分裂域$E_f$中的根，定义$E_f$中根的判别式为(可称为同余方程(5)根的判别式)：

$$\Delta_3=\prod\nolimits_{1\le i<j\le3}(x_i-x_j)^2 \tag{6}$$

式(6)的运算按F_p中运算进行。由文献[8]可以得到以下引理：

引理 **1**　$\Delta_3\in F_p$，且可表示为：

$$\Delta_3=\Delta_3(b_1,b_2,b_3)=(b_1b_2)^2-4b_1^3b_3-4b_2^3-27b_3^2+18b_1b_2b_3 \tag{7}$$

引理 **2**　设p为奇素数，$b_3\equiv0(\mathrm{mod}\ p)$不成立，则对3次同余方程(5)解的结构或者$f(x)$的结构，只能发生下列情况，且存在以下判断：

(1) 式(5)在F_p中有3个不同余的解，或者$f(x)$在$F_p[x]$可分解为1次多项式的乘积，且无重因式。该情况发生当且仅当：

$$(\Delta_3/p)=1\qquad x^{p-1}\equiv1(\mathrm{mod}\ f(x))$$

(2) 式(5)在F_p中有3个解，且至少有2个同余；或者$f(x)$在$F_p[x]$可分解为1次多项式的乘积，且有重因式。该情况发生当且仅当：

$$(\Delta_3/p)==0$$

(3) 式(1)在F_p中有唯一解，或者$f(x)$在$F_p[x]$可分解为1次多项式与一个2次不可约多项式$g_2(x)$的乘积，且无重因式。该情况发生当且仅当：

$$(\Delta_3/p)=-1$$

(4) 式(5)在F_p中没有解，或者$f(x)$是$F_p[x]$中的3次不可约多项式。该情况发生当且仅当$(\Delta_3/p)=1$，且$x^{p-1}\equiv1(\mathrm{mod}\ f(x))$不成立。做出判断只需耗费$O((\log_2\{p\})^3)$比特时间。

文献[9]提出当3次同余方程(5)在F_p有解时，求出方程(5)在F_p的解的算法，且有以下引理：

引理 **3**　当式(5)在F_p有解时，求式(5)在F_p的解，只需耗费$O(\log_2p)$次模p乘法或$O((\log_2\{p\})^3)$b时间。

设$F_4(x)=x^4-\theta_1x^3+\theta_2x^2-\theta_3x+\theta_4$，考虑4次同余方程可得：

$$F_4(x)\equiv0(\mathrm{mod}\ \ p) \tag{8}$$

式中　$\theta_i\in F_n$, i=1,2,3,4；$\theta_4\ne0$；p>4。设$F_4(x)$在其分裂域E_{F_4}中的4个解为α_i，i=1,2,3,4。当$\alpha_i\in F_p$时，α_i为同余方程(4)在F_p的解。定义E_{F_4}中根的判别式(或式(8)根的判别式)为$\Delta_4=\prod\nolimits_{1\le i<j\le4}(\alpha_i-\alpha_j)^2$，由韦达定理可得：

$$\begin{cases}\alpha_1+\alpha_2+\alpha_3+\alpha_4\equiv\theta_1(\mathrm{mod}\ p)\\ \alpha_1\alpha_2\alpha_3\alpha_4\equiv\theta_4(\mathrm{mod}\ p)\end{cases} \tag{9}$$

令：

$$\begin{cases}\beta_1=\alpha_1\alpha_2+\alpha_3\alpha_4 (\mathrm{mod}\ p)\\ \beta_2=\alpha_1\alpha_3+\alpha_2\alpha_4 (\mathrm{mod}\ p)\\ \beta_3=\alpha_1\alpha_4+\alpha_2\alpha_3 (\mathrm{mod}\ p)\end{cases} \tag{10}$$

利用韦达定理容易验证β_j (j=1,2,3)是$F_3(x)$在其分裂域 E_{F_3} 中的3个解，且$F_3(x)=x^3-\theta_2x^2+(\theta_1\theta_3-4\theta_4)x-\theta_4(\theta_1^2-4\theta_2)-\theta_3^2$。当$\beta_j\in F_p$时，有：

$$F_3(x)\equiv 0(\mathrm{mod}\ p) \tag{11}$$

β_j即为式(11)在F_p的解。令$b_1=-\theta_2$，$b_2=\theta_1\theta_3-4\theta_4$，$b_3=-\theta_4(\theta_1^2-4\theta_2)-\theta_3^2$，则式(11)化为式(5)。计算 E_{F_3} 中根的判别式为$\Delta_3(b_1,b_2,b_3)=(\theta_2(\theta_1\theta_3-4\theta_4))^2-4\theta_2^3(\theta_4(\theta_1^2-4\theta_2)+\theta_3^2)-4(\theta_1\theta_3-4\theta_4)^3-27b_3^2+18\theta_2(\theta_1\theta_3-4\theta_4)\times(\theta_4(\theta_1^2-4\theta_2)+\theta_3^2)$，化简后记为$\Delta_3(\theta_1,\theta_2,\theta_3,\theta_4)$。

命题 1　E_{F_3} 中根$\{\beta_j\}$的判别式$\Delta_3(\theta_1,\theta_2,\theta_3,\theta_4)$也是 E_{F_4} 中根$\{\alpha_i\}$的判别式 $\Delta_4=\prod_{1\le i<j\le 3}(\alpha_i-\alpha_j)^2$，即$\Delta_4\in F_p$，且可由$(\theta_1,\theta_2,\theta_3,\theta_4)$表示。

证明　$\Delta_3(\theta_1,\theta_2,\theta_3)=\prod_{1\le i<j\le 3}(\beta_i-\beta_j)^2$，可由式(10)得$\prod_{1\le i<j\le 3}(\beta_i-\beta_j)^2=\prod_{1\le i<j\le 4}(\alpha_i-\alpha_j)^2$。

定理 **2**　设Δ_4为式(8)根的判别式，则有：

1) $(\Delta_4/p)=0$，当且仅当$F_4(x)$在$F_p[x]$有重因式。

2) $(\Delta_4/p)=1$，当且仅当：(1) 式(8)在F_p有4个不同单重根；(2) 式(8)在F_p仅有1个单重根α_1，且$f(x)=(x-\alpha_1)f_3(x)$，$f_3(x)$是$F_p[x]$中3次不可约多项式；(3) 式(8)在F_p无解，且$f(x)=f_{21}(x)f_{22}(x)$，$f_{21}(x)$与$f_{22}(x)$是$F_p[x]$中不同2次不可约多项式。

3) $(\Delta_4/p)=-1$，当且仅当：(1) 式(8)在F_p仅2个不同单重根α_1、α_2，且$f(x)=(x-x_1)(x-x_2)f_2(x)$，$f_2(x)$是$F_p[x]$中2次不可约多项式；(2) 式(8)在$F_p$无解，且$f(x)$是$F_p[x]$中4次不可约多项式。

证明　简记 $\Delta_4=\prod_{1\le i<j\le 4}(\alpha_i-\alpha_j)^2=\Delta$，设 $\delta=\prod_{1\le i<j\le 4}(\alpha_i-\alpha_j)$，则 $\Delta_4=\Delta=\delta^2$。

1) $(\Delta/p)=0$，当且仅当$p|\Delta$或者$\Delta=0$。当根α_i在F_p时不可能有$p|\Delta$，只能$\Delta=0$，即有重1次因式；α_i不在F_p时是不可约因式，不可能有$p|\Delta$，只能$\Delta=0$，即有重2次以上因式。故$(\Delta/p)\ne 0$，当且仅当$F_4(x)$在$F_p[x]$全为单因式。

2) (1) 当$F_4(x)$在F_p有4个不同单重根$\{\alpha_i\}$时，由费马定理可得$(\alpha_i)^p\equiv\alpha_i$, i=1,2,3,4；由欧拉定理可以得到 $(\Delta/p)\equiv\Delta^{(p-1)/2}$，而 $\delta^p\equiv\prod_{1\le i<j\le 4}(\alpha_i-\alpha_j)^p\equiv\prod_{1\le i<j\le 4}(\alpha_i-\alpha_j)=\delta$，$\Delta\equiv 0$不成立，所以$1\equiv\Delta^{p-1}=(\Delta^2)^{(p-1)/2}=\Delta^{(p-1)/2}\equiv(\Delta/p)$。

(2) 设ξ, ξ^p, ξ^{p^2}为3次不可约多项式，$f_3(x)$在F_p的3次扩域 F_p^3 的根、$F_4(x)$在F_p的根是α_1。由3次扩域 F_p^3 性质可得$\xi^{p^3}=\xi$，因$\Delta=(\alpha_1-\xi)(\alpha_1-\xi^p)\times(\alpha_1-\xi^{p^2})(\xi-\xi^p)(\xi-\xi^{p^2})(\xi^p-\xi^{p^2})$，所以$\Delta^p\equiv((\alpha_1)^p-\xi^p)(\alpha_1)^p-\xi^{p^2})((\alpha_1)^p-\xi^{p^3})$ $(\xi^p-\xi^{p^2})(\xi^p-\xi^{p^3})$ $(\xi^{p^2}-\xi^{p^3})=(\alpha_1-\xi)(\alpha_1-\xi^p)(\alpha_1-\xi^{p^2})(\xi^p-\xi^{p^2})(-1)(\xi-\xi^p)(-1)(\xi-\xi^{p^2})=\Delta$。类似于(1)可得$1\equiv\Delta^{p-1}=\Delta^{(p-1)/2}\equiv(\Delta/p)$。同上可以证明，当定理2的2)中的(1)～(3)发生时，均有$(\Delta/p)=1$(必要性可以得证)。

同理可以证明当定理2的3)中的(1)～(2)发生时，均有$(\Delta/p)=-1$(必要性得证)。但$F_4(x)$在$F_p[x]$全为单因式，只能发生定理2的2)中的(1)～(3)和3)中的(1)～(2)等5种情况[10]。用反证法可得$(\Delta/p)=1$只能是定理2的2)中的(1)～(3)，而$(\Delta/p)=-1$只能是定理3的3)中的(1)～(2)，充分性得证。

利用文献[9]的方法，当式(11)在F_p有解时，可求出其在式(11)的解$\beta_j(\mathrm{mod}\ p)$, $j\in\{1,2,3\}$。同样为了简洁证明，设$p\equiv 7(\mathrm{mod}12)$, 而$p\equiv 1(\mathrm{mod}\ 9)$不成立，则$4|(p-3)$, $3|(p-1)$。

当$(\Delta_4/p)=-1$时，设式(11)在F_p的唯一解为β_1，$\beta_1=\alpha_1\alpha_2+\alpha_3\alpha_4(\mathrm{mod}\ p)$，有：

$$t^2-\beta_1t+\theta_4\equiv 0(\mathrm{mod}\ p) \tag{12}$$

由韦达定理可得$\alpha_1\alpha_2$与$\alpha_3\alpha_4$分别是式(12)的2个根。式(12)可变为$4t^2-4\beta_1t+\beta_1^2\equiv\beta_1^2-4\theta_4$，$2t-\beta_1\equiv\pm[\beta_1^2-4\theta_4]^{(p+1)/4}$。$t=2^{-1}(\beta_1\pm[\beta_1^2-4\theta_4]^{(p+1)/4})$ $(\mathrm{mod}\ p)$为式(12)在F_p的2个解，即$\alpha_1\alpha_2$与$\alpha_3\alpha_4$。取±中的+记为t_1，另一个为t_2。

解同余方程为：

$$\gamma_1^2\equiv\theta_1^2-4\theta_2+4\beta_1(\mathrm{mod}\ p) \tag{13}$$

式中　$\gamma_1=\pm(\theta_1^2-4\theta_2+4\beta_1)^{(p+1)/4}(\mathrm{mod}\ p)$为式(13)在$F_p$的2个解。容易验证$\gamma_1\equiv\pm(2(\alpha_1+\alpha_2)-\theta_1)\equiv\pm((\alpha_1+\alpha_2)-(\alpha_3+\alpha_4))(\mathrm{mod}\ p)$，取±中的+记为$\gamma_1^*$，$(\gamma_1^*+\theta_1)(\mathrm{mod}\ p)$值为$2(\alpha_1+\alpha_2)\mathrm{mod}\ p$与$2(\alpha_3+\alpha_4)\ \mathrm{mod}\ p$其中的一个。

求解方案 1　分别求解2次同余方程为：

$$y^2-2^{-1}(\theta_1+r_1^*)(\mathrm{mod}\ p)y+t_1\equiv 0(\mathrm{mod}\ p) \tag{14}$$

$$y^2-2^{-1}(\theta_1-r_1^*)(\mathrm{mod}\ p)y+t_2\equiv 0(\mathrm{mod}\ p) \tag{15}$$

如果由式(14)或式(15)能得到F_p中的2个解(记为α_1、α_2)，且代入式(8)成立，则输出返回；否则分别求解2次同余方程为：

$$y^2-2^{-1}(\theta_1+r_1^*)(\mathrm{mod}\ p)y+t_2\equiv 0(\mathrm{mod}\ p) \tag{16}$$

$$y^2-2^{-1}(\theta_1-r_1^*)(\mathrm{mod}\ p)y+t_1\equiv 0(\mathrm{mod}\ p) \tag{17}$$

如果由式(10)或式(11)得到F_p中的2个解(记为α_1、α_2)，且代入式(4)成立，则输出返回；否则输出“$F_4(x)$为$F_p[x]$中不可约多项式”判断后返回。

定理 **3**　按照方案1，当$(\Delta_4/p)=-1$时，耗费

$O((\log_2\{p\})^3)$比特时间，可以输出4次同余方程在F_p中的2个解，或者输出“$F_4(x)$为$F_p[x]$中4次不可约多项式”的判断。

当$(\Delta_4/p)=1$，且式(11)在F_p有解时，设式(11)在F_p的3个解为β_j, $j=1,2,3$；任取其中一个解记为β_1，$\beta_1=\alpha_1\alpha_2+\alpha_3\alpha_4 (\mathrm{mod}\ p)$；那么上述关于式(12)与式(13)的判断以及$t_1,t_2, r_1^*$的记号依然有效。

求解方案 2　分别求解2次同余方程(14)、(15)，如果由同余方程(14)或(15)能分别得到F_p中的两组解(记为α_1、α_2与α_3、α_4)，且代入式(8)成立，则输出返回；否则分别求解2次同余方程(16)、(17)。如果由同余方程(16)、(17)能分别得到F_p中的两组解(记为α_1、α_2与α_3、α_4)，且代入式(8)成立，则输出返回；否则输出“$F_4(x)$在$F_p[x]$中可分解为2个不同2次不可约多项式乘积”的判断。

定理 **4**　按照方案2，当$(\Delta_4/p)=1$，且式(11)在F_p有解时，耗费$O((\log_2\{p\})^3)$比特时间，可以输出4次同余方程在F_p中的两组解；或者输出“$F_4(x)$为$F_p[x]$中2个不同2次不可约多项式乘积”的判断。

加密方案生成的$(\theta_1,\theta_2,\theta_3,\theta_4)$或式(8)，对应于定理2的2)中的(1)与3)中的(1)，分别对应于$(\Delta_4/p)=1$与$(\Delta_4/p)=-1$，而一定不会出现其他判断。可以由计算方案1、2求出$F_4(x)\equiv 0 (\mathrm{mod}\ p)$与$F_4(x)\equiv 0 (\mathrm{mod}\ q)$在$F_p$或$F_q$中的2个解与4个解，用中国剩余定理得到式(1)在$F_n$中的$2^2$个解与$2^4$个解，用大小顺序$\varepsilon$求出$\alpha_1$值。

定理 **5**　采用计算方案1与2，耗费$O((\log_2\{n\})^3)$比特时间，可以由密文组中的$\{\theta_1,\theta_2,\theta_3,\theta_4,\varepsilon\}$求解$\alpha_1$，从而得到$H(\alpha_1)$。

由于目前未出现求解高于4次同余方程的算法，因此选择4次同余方程在可解范围能得到最大的参数集合$(F_n\backslash\{0\})^4=\{(\theta_1,\theta_2,\theta_3,\theta_4)|\theta_i\in F_n\backslash\{0\}\}$，而几乎未增加新的开销。方案1、2保证了参数的同一性。

3　结 束 语

本文提出了一种新的公钥密码安全方案，有别于现有的建立可证明安全密码体制的思路，在采用原有的公钥、私钥的基础上增加数量庞大、开销甚少的公开参数集合，每加密一批由加密者挑选、其他方无从猜测的明文数据，选择一组不重复的新公开参数。该方案可以主动抵御各种选择明文与选择密文的攻击包括IND-CCA2。

实现该方案的途径是使用4次同余方程，本文对于一般的模数是n的4次同余方程，分析了解的结构，提出了判断解结构及求F_n中解的快速算法。新方案在保证信息安全条件下，可充分利用现有密钥资源，而加密解密变换主体时间是$O((\log_2\{n\})^3)$比特时间，相当于线性时间的模乘法，属于高效算法。

参 考 文 献

[1] 陈　原, 王育民, 肖国镇. 公钥密码体制与选择密文安全性[J]. 西安电子科技大学学报(自然科学版), 2004, 31(1): 135-139.

[2] 王泽辉. 一类椭圆曲线求阶的$O((\log_2 p)^3)$时间算法及应用[C]//密码学进展—CHINACRYPT'2006. 北京: 中国科学技术出版社, 2006: 67-74.

[3] WANG Ze-hui, ZHANG Zhi-guo. XTR+: A provable secure public key cryptosystem[C]//Proc of the 2006 International Conference on CIS. Berlin: Springer-Verlag, 2007, LNAI 4456: 534-544.

[4] CRAMER R, SHOUP V. Design and analysis of practical public-key encryption schemes secure against adaptive chosen ciphertext attack[J]. SIAM Journal of Computing, 2003, 33: 167-226.

[5] 冯登国. 可证明安全性理论与方法研究[J]. 软件学报, 2005, 16(10): 1743-1756.

[6] JUELS A. RFID security and privacy: a research survey[J]. IEEE Journal on Selected Areas in Communications, 2006, 24(2): 381-394.

[7] BONO S, GREEN M, STUBBLEFIELD A, et al. Security analysis of a cryptographically-enabled RFID device[C]//In Proc 14th USENIX Security Symp. Baltimore: USENIX Association, 2005: 1-16.

[8] 王泽辉, 方小洵. 增加多媒体隐藏信息量的高效算法[J]. 哈尔滨工业大学学报, 2006, 38(增刊): 710-714.

[9] 王泽辉. 基于3次同余方程的概率公钥密码体制[J]. 通信学报, 2006, 27(12A): 61-65.

[10] 冯克勤, 余红兵. 整数与多项式[M]. 北京: 高等教育出版社, 1999.

[11] 秦志光, 张险峰, 周世杰, 等. 基于ECC的门限数字签名方案及其安全性[J]. 电子科技大学学报, 2005, 34(1): 109-112.

[12] 周世杰, 秦志光, 张　峰, 等. 基于多Agent的入侵快速响应系统[J]. 电子科技大学学报, 2004, 33(4): 419-422.

编　辑　黄　莘