DOI: 10.13656/j.cnki.gxkx.1999.04.007
广西科学 Guangxi Sciences 1999, 6 (4): 259~262

$P_n^{(r)}$ 公钥外部参数和嵌套函数的等概率*

Equiprobability of External Parameter and Inlaid Function in $P_n^{(r)}$ Public Key

彭宏祥 彭典祥** 李业清***
Peng Hongxiang Peng Dianxiang Li Yeqing

(广西农业科学院, 南宁市西乡塘路, 530007)
(Guangxi Academy of Agri. Sci., Xixiangtanglu, Nanning, Guangxi, 530007, China)

摘要 基于 PDX构造理论,证明了 $P_n^{(r)}$ 公钥外部参数和嵌套函数存在一种重要的等概率性,即构造与破译彼此概率相等.安全性分析证明 $P_n^{(r)}$ 公钥具有高强度安全性能.
关键词 $P_n^{(r)}$ 公钥 外部参数 嵌套函数 等概率
中图法分类号 TP 309.7

Abstract On the base of structural theorem of PDX system, this paper proves an important equiprobability of external parameter and inlaid function in $P_n^{(r)}$ public key. Corresponding probability from construction and decipher is equal. Safety analysis has proven that $P_n^{(r)}$ public key possesses high-strength secure function.
Key words $P_n^{(r)}$ public key, external parameter, inlaid function, equiprobability

以背包问题为基础的背包公钥结构简明,加解密容易,运算速度快,这些优点使之很快成为现代密码学研究的热点[1,2].但是,当今背包型公钥研究仍未能脱离超递增序列或纯素数序列构造方案,更未见有外部随机参数辅助输入实现一次一密的新型背包公钥研究方案出现.在传统密码学研究中,依靠增加多项式长度以加大密钥量,提高保密强度.多项式过长会减慢加解密速度,降低效率,纯素数构造方案亦未能解决多项式长度问题[3].本文基于 PDX体制的理论,进一步研究了该体制外部参数 $\{U_j^k\}$ 和嵌套函数的等概率性理论及其应用,且作了相应的扩展,旨在从根本上解决超递增序列或纯素数序列构造背包公钥的有限多项式易被破译问题.

1 $P_n^{(r)}$ 构造的数学模型

$P_n^{(r)}$ 加密变化过程如图 1所示.

众所周知,有限状态机存在周期性,为破译者提供了一种可以利用的条件.PDX 体制的随机参数序列 $\{U_j^k\}$ 是从有限机外部输入,可以消除有限状态机的周期状态.

1999-05-31收稿,1999-08-08修回.
* 广西自然科学基金资助项目(9811028).
** 广西武宣县六峰山林场,武宣县,545904(Liufeng Forest Farm, Wuxuan County, Guangxi, 545904).
*** 广西计算中心,南宁,530022(Compute Center of Guangxi, Nanning, Guangxi, 530022).

P 钥原型对 $\{U_j^k\}$ 表述:

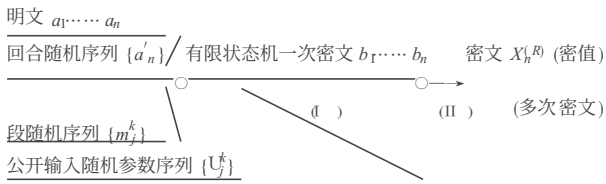

图 1 $P_n^{(r)}$ 加密流程示意
Fig. 1 Encipher process of $P_n^{(r)}$

$$f_m[d,(U_n^1 \cdots U_n^m)] = \begin{cases} d_1^{(m)} = (d_{11}^*, \cdots, d_{1k}, U_1^1 \cdots U_1^m) \\ \cdots\cdots \\ d_n^{(m)} = (d_{n1}, \cdots, d_{nf}^*, U_n^1 \cdots U_n^m) \end{cases}$$

或

$$f_m[d,(U_n^1 \cdots U_n^m)] = \begin{cases} d_1^{(m)} = ((d_{11}^*, \cdots, d_{1k})U_1^1 \cdots U_1^m) \\ \cdots\cdots \\ d_n^{(m)} = ((d_{n1}, \cdots, d_{nf}^*)U_n^1 \cdots U_n^m) \end{cases}$$

函数式包括 m_j^k (段参数)和 $\{U_j^k\}$ 的输入方式[4].

段参数 m_j^k 的选码关系表是公开的[5],加密者根据一段 (n回合) 信息序列进行相应分配选码加密.解密时必须完成全部一段解密后,通过选表、求解,最后才能解密另一 m_{ij} 信息数码,完成全解密过程.

2 $\{\beta_j^k\}$ 和嵌套函数的概率性

镜像变换性质 **1** 用相同若干层次、位数和进制

表示的二元数 $A=\{a_j^i\}$、$B=\{b_j^i\}$(a_j^i、$b_j^i\in[0,1]$),若 $\{a_j^i\}$ 的逻辑非运算等于 $\{b_j^i\}$,则 $\{a_j^i\}$ 是原型,$\{b_j^i\}$ 为镜像,存在一种数值互逆关系:$A\overset{非}{\longleftrightarrow}B$ 当 B 任取一种与原来相同层次、位数表示形式($B=\{c_j^i\}$)时,也存在另一种镜像关系 $\{a_j^i\}^*\overset{非}{\longleftrightarrow}\{c_j^i\}$,也可以推出 $\{a_j^i\}^*=A$.

镜像变换性质 **2** 镜像变换是一种数值倒置等距置换变换.

例 **1** 15取 2进制 3层 3位.

$$\begin{array}{cccccccccccc} & 111 & 000 & & & 011 & 100 & & & 010 & 101 & \\ 15 & 111 & \overset{非}{\longleftrightarrow} & 000 & = 6 \text{ 逆变 } 6 & 011 & \overset{非}{\longleftrightarrow} & 100 & = 15 \text{ 或} & 010 & \overset{非}{\longleftrightarrow} & 101 = 15 \\ & 001 & & 110 & & 000 & & 111 & & 010 & 101 & \end{array}$$

定理 **1** 在 Z^*(非零整数集)内,可以找到 $a,b,m,n(\in Z^*)$ 与一种适合的结合法 f 及 f'(逆)使 $f(n,b/a)\rightarrow m^{\#}$,$f'(m^{\#},a/b)\rightarrow n^{\#}$ 成立.$m^{\#}$、$n^{\#}$ 为变换过程 m、n 的不同精度的对应取值.

证明 设 $m^{\#}$ $n^{\#}$ 是非零整数,结合法 $f(n,b/a)\rightarrow m$,$f'(m,a/b)\rightarrow n$ 都是 Z^* 内子集间一一映射,不用输入精度参数 $\triangle m^{\#}$、$\triangle n^{\#}$(精度取 0).若 $m^{\#}$ $n^{\#}$ 是非零有理数,则结合法给 $m^{\#}$ 固定一个精度取法,并输入一个正参数 $\triangle m^{\#}$,可以建立 $m^{\#}\in Q^*$(非零有理集)$\rightarrow m$ 之间的一一映射关系,使 $f(n,b/a)\rightarrow m^{\#}\rightarrow m$.同理,对于 f',也为 $n^{\#}$ 建立一个精度取法,并输入一个负参数 $\triangle n^{\#}$,使 $f'(m^{\#},a/b)\rightarrow n^{\#}\rightarrow n$.证毕.

定理 1是对加密算子输入参数手段的说明,是加密算子的一种变换程序或一种函数映射方法,f 的精度与 f' 的精度是不同的.

推论 **1** $P_n^{(r)}$ 加密算子在结合的作用下,构造与破译具有等概率性.

设 A,B 分别是 $\{\cup_j\}$ 参与 $P_n^{(r)}$ 的构造集与破译集,破译集中包含了解译元素,其关系见图 2.

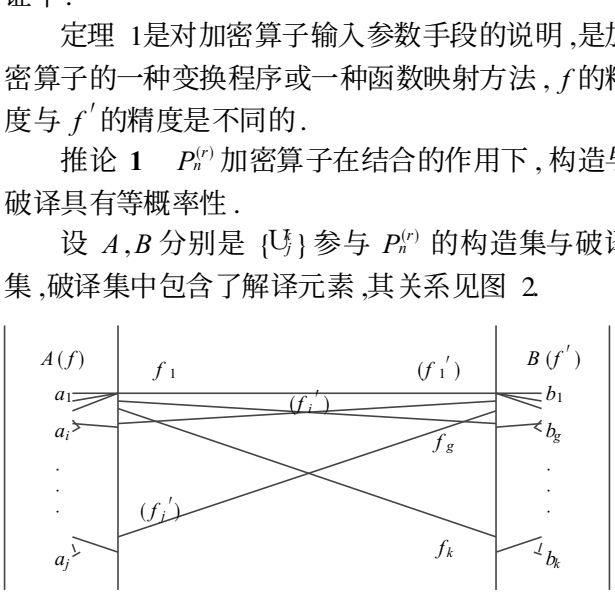

图 2 构造与破译集关系图

Fig. 2 Relationship of construction and decipher

f、f' 的指向是从 a_1 指向 $\{b_n\}$ 的 $f_1\cdots f_g\cdots f_k$ 全部是双向线"$\longleftrightarrow$",A 中其他 a_m 投映点情况相同.从 b_1 指向 $\{a_m\}$ 的除 $a_1\longleftrightarrow b_1$ 以外,$a_i\sim a_j$ 点全部是单向线"$\rightarrow$"理解为:从 A 中按 $f_1\cdots f_g\cdots f_K$ 程序,a_1 可以得到 $b_1\cdots b_g,\cdots b_k$;从 B 中用原 f 之逆 f_1',b_1 可以得到 a_1,用其他程序 $f_i'\cdots f_j'$ 不会得到 a_1 而得到其他 $a_i\cdots a_j$ 点,B 中其他点情况也是一样.$\{a_m\}$ 与 $\{b_n\}$ 密度一样,符合 Shannon的随机密码第一假设:密钥空间所有密钥均匀分布,每个密钥概率相等.不同的是假设中指传统密钥,本文的 $P_n^{(r)}$ 是公钥.背包公钥的超递增构造元素,不具备这种等概率性构造,因为它的 A集构造元素密度大于 B集的加密背包元素,由此产生了超递增型背包公钥一种周期,为破译者提供一种便利分析条件.

定理 **2** 在 Z^* 内,可以找到 a,b,m,n 与变元 $X_j(\in Z^*)$ 的一种适合结合法 f 及 f',使 $f(n\cdot x_j,b/a)\rightarrow m^{\#}$,$f'(m_j^{\#},a/b)\rightarrow n_j^{\#}x_j$.$m_j^*$、$n_j^{\#}$ 为运算过程 m、n 的概率选择还原法.

证明 设 $m_j^{\#}$,$n_j^{\#}\in Z^*$,结合法 $f(n\cdot x_j,b/a)\rightarrow m_j^{\#}$,$f'(m_j^{\#},a/b)\rightarrow n_j^{\#}x_j$ 都是 Z^* 内子集间的一一映射.精度全部是 0,概率选择为 1时,无需作概率选择.

由于 x_j 存在,若 $m_j^{\#}$,$n_j^{\#}(\in Q^*)$ 是有理无限数,必然各自产生一个精度取法下的元素集 $\{\triangle m_j^{\#}\}$,$\{\triangle n_j^{\#}\}$ 使得运算过程 $m^{\#}\cdot n_j^{\#}$ 转化为非零整数.因为 $P_n^{(r)}$ 是短序列,使得这种转化概率选择在多项式运算时间内得以实现.根据 $\{\triangle m_j^{\#}\}$ 和 $\{\triangle n_j^{\#}\}$ 取法全部取出运算结果 $\{m_j^{\#}\}$、$\{n_j^{\#}\}$ 之后,其中一种取法必然是正确的选择.这一正确结果会在 $P_n^{(r)}$ 的第二层次的平行逻辑判断还原系统中得到唯一证明解出.证毕.

结合法是多种简易算法的模函数(同余)、镜像函数(逻辑非)、有理函数(有理运算)的嵌套复合函数方法.秘密选择三种函数的排列组合及系列参数,对 $P_n^{(r)}$ 实施一定数量的连续变换得到 T 加密矩阵.

推论 **2** 在定理 1、2结论条件下,$P_n^{(r)}$ 密值构造具有等概率性.

定理 1、2分别描述证明单独加密算子与密钥的构造及可操作性,结合法的嵌套镜像函数、有理函数是严格的等概率变换函数.因为镜像函数是一种等距倒置变换函数,任何一个二元表示 K 进数,只需调节层数和位数就可以得到一个理想像值,由于 P钥结构特殊性,不同级别 I_i 算子可以用相同或不同层、位数构造,没有特别的数学统计特征.另外有理函数是内部的包含小数位加密算子的传导过程,逆解(或破译)也是一种包含小数的数值传导过程,而且最终是一种包含小数数值的逻辑选择行为,也无特别的数学统计特征.$\cup_j$ 为加密结束后任意加入的某区间内的随机数,是一种等概率选择数,解译过程,通过嵌套函数层次清除掉.

例 **2** a. 5的层、位数任选情况下,理想像值 2 1 57的情况是:

逻辑非	像值	进制
101~ 010	2	(1- 2- 4)
10~ 01	1	(1- 5- 25)
$\begin{bmatrix}010\\000\end{bmatrix}$ ~ $\begin{bmatrix}101\\111\end{bmatrix}$	57	(1- 5- 25)

b. 17. 63有理原型加密算子在有理函数参数作用下生成整数型加密算子 3 786,当 $x=$ 9时, 3 786$x=$ 34 074,该函数层次逆还原传导情况是(还原标准值为 17. 63× 9= 158. 67):

(误差区间) (符合误差)× 21/35 × 1617/2538 × 119/9768

[0,0. 01] 158. 68—— 264. 47—— (取 2位小数) 415. 1111 ←— 34074(正确)

158. 64—— 264. 4—— (取 1位小数) 415. 1 ←— 34074(偏差)
(误差 0. 03超出区间范围)

158. 683—— 264. 473—— (取 3位小数) 415. 111 ←— 34074(偏差)
(误差 0. 013超出区间范围)

要单独推出 17. 63,必需在连续还原过程加入系列 $\triangle n_{\#}$. 在整体解译运算过程中,则只需选对 2位小数还原精度,不用考虑加入 $\{\triangle n_{\#}\}$. $P_n^{(r)}$ 公钥这些等概率构造决定了复合函数整体操作运算的严格性.

3 加解密算法

把加密矩阵 T分成 T_1主加密矩阵、T_2辅助加密矩阵见表 1、2.

表 **1** T_1主加密矩阵 P^H

Table 1 Main encipher matrix at T_1

	I_1	I_2	…	I_n
0	$a_{1,1}$	$a_{1,2}$	…	$a_{1,n}$
1	$a_{2,1}$	$a_{2,2}$	…	$a_{2,n}$

表 **2** T_2辅加密矩阵

Table 2 Auxiliary encipher matrix at T_2

0000	$b_{1,1}$	$b_{1,2}$	…	$b_{1,k}$
0001	$b_{2,1}$	$b_{2,2}$	…	$b_{2,k}$
…	…	…	…	…
1111	$b_{16,1}$	$b_{16,2}$	…	$b_{16,k}$

$P_n^{(r)}$ 加密算法为:

(1) 任意规定一种 m_{ij}^k 选码对应关系表 T_3^* [5].这样由 T_1的信息码可以得 $m_1^1, m_2^1, \cdots, m_8^1 \cdots m_1^8, m_2^8 \cdots m_8^8$.

(2) 求 $P^H \cdot m_{ni}^* = A_d\ (d = 1, 2, \cdots, t) =>$ 一段密值 $A_1, A_2, \cdots, A_t$.

(3) 用信息码序列 $\{a_j\}$ 在 T_1对各回合加密.

$$\sum_{n=1(R=0\text{或}1)}^{4} I_n^R =>\ M_1, M_2, \cdots, M_t.$$

(4) 随机选择 $U_1, U_2, \cdots, U_t$等随机数 ($U_t \in [X, k]$ 自然数区间).

令 $U_1 = C_1, U_2 = C_2, \cdots, U_t = C_t$

设 $C_1, C_2, \cdots, C_{t-1}$的数值分别对应辅助算子的位置标号顺序是 $C_1 \rightarrow b_{n,a}$, $C_2 \rightarrow b_{l,g} \cdots C_{t-1} \rightarrow b_{a,r}\ (n, l, a \in [1, 16])$,首先任意设定一种置换规则: $b_{1,1} \longleftrightarrow b_{n,d}$ (若 $n = d = 1$,不置换),第一次置换结束得新辅助矩阵 T_2^1. 同理,又对 T_2^1作第二次置换 $b_{1,2} \longleftrightarrow b_{l,g}$ (若 $l = 1, g = 2$不置换),得 $T'^2_2 \cdots$,依次类推,做完一段置换得新辅助矩阵 $T_2^1, \cdots, T_2^{t-1}$.

根据环指码规则第 1至第 t回合分别在 T_2、$T_2^1 \cdots T_2^{t-1}$中选择

$$\sum_{n=1(f=1,2,\cdots,16\text{其中之一})}^{4} b_{f,n} =>\ N_1, N_2, \cdots, N_t.$$

一段加密值

$$X_1^{(1)} = A_1 + M_1 + U_1 + N_1, \cdots, X_1^{(t)} = A_t + M_t + U_t + N_t$$

密值为 4部分组成,U_k和 N_k是等概率构造层,其余是逻辑判断层. 在等概率构造层中,U_k是外部输入的有相同上下界值 $[X, k]$的随机因子,在区间内选取各数值的概率都等于 $1/k$. N_k同样具备构造等概率性: 设矩阵的元素序号区间是 $[1, t]$,则矩阵置换 $T_2 \rightarrow T_2^1 \cdots \rightarrow T_2^t$中,每一矩阵元素 $b_{k,n}$对各序号的置换概率为 $1/t - 1$.可见加密方法简易,为一次整体(段)置换选择环指码,t回合乘、加求和密值.

解密算法为:

设 f_1^i = 模函数, f_2^k = 镜像函数, f_3^m = 有理函数 (i、k、$m \in Z^+$),若构造

$$\{d_i\}(d_i \in Q\text{有理集}) \xrightarrow{\text{基码积}} P_n^{(r)} \rightarrow f_1^0(P_n^{(r)}) = P^1 \rightarrow f_3^0(P^1) = P^2 \rightarrow f_3^1(P^2) = P^3 \rightarrow f_2^0(P^3) = P^4 \rightarrow f_1^1(P^4) = P^5 \rightarrow f_3^2(P^5) = P^6(T_1, T_3, P^H \cdot m_{ij})$$

上述解密函数简单易操作,逆运算共 5次乘法、5次除法、1次逻辑非运算、4次平行逻辑二元判断完成全过程.由于序列短,串行时间开销少,解密速度比一般 120元以上背包密钥提高数倍以上.

4 安全性分析

分析密钥安全强度, $P_4^{(4)}$ 构造元素达 160种以上,强度高达 10^{272}以上[5],且有严格的等概率性能.只要嵌套函数选择错位或参数有微小差异,就会产生连续错误扩散,例 2的 b.还说明穷举参数独立破译加密算

(下转第 277页 Continue on page 277)

4 结语

本文考虑了一些自然系统中混沌同步的一种可能方式: 系统间连续不断地互相输入流,靠流的作用把不同的系统逐渐调整到相同的混沌态并在此后保持有相同的混沌轨道. 同步要求流的耦合对两系统必须是对称的,否则耦合后的两个系统完全不同,就无所谓同步. 我们还对三维系统的对应变量之差的收敛提出了新的判据. 在 Lorenz系统中进行了数值模拟,结果表明,全部分量上流的对称耦合在其强度较弱时就可同步,对于部分分量上流的对称耦合,由于存在耦合在各分量之间不对称的问题,强耦合才能使系统同步. 这种耦合同步方法对模拟生态系统等一些自然系统的混沌同步是一种尝试,也可用于一些人工系统.

参考文献

1 Henry, Abarbanel D I, Nikolai F. Phys Rev, 1996, E53: 4528.

2 Pecarev L, Parlitz U, Generalized synchronization, predictability and equivalence of unidirectionally coupled dynamical. Phys Rev Lett, 1996, 76: 1816.

3 Hayes S, Grebogi C, E Ott. Communicating with chaos. Phys Rev Lett, 1993, 70: 3031.

4 Perez G, Cerderra H A. Extracting messages masked by chaos. Phys Rev Lett, 1995, 74: 1970.

5 Kocarev L, Parlitz U. General approach for chaotic synchronization. with applications to communication. Phys Rev Lett, 1995, 74: 5028.

6 Pecora L M, Carroll T L. Synchronization in chaotic systems. Phys Rev Lett, 1990, 64: 821.

7 Pecora L M, Carroll T L. Driving systems with chaotic signals. Phys Rev, 1991, A44: 2374.

8 Pyrgas K. Predictable chaos in slightly perturbed unpredictable chaotic systems. Phys Lett, 1993, A181: 203.

9 Sugawarn T, Tachikawa M, Tsnkamoto T. Observation of synchronization in laser chaos. Phys Rev Lett, 1994, 72: 3502.

10 Jolly K John, Amritkar R E. Synchronization of unstable orbits using adaptive control. Phys Rev, 1994, E49: 4843.

(责任编辑: 黎贞崇)

(上接第 261页 Continue from page 261)

子是困难的. 现有各种破译方法对 $P_4^{(4)}$ 是无效的. 因此破译加密钥是不可能的.

分析密值抗破译强度, P^H 是已知的, 容易分解 $P^H \cdot m_{ij}$ 得到信息值 m_{ij}. 要保护 $P^H \cdot m_{ij}$, 取决于 T_2 元素的全部组合数量不被穷举. 由于 T_2 随机矩阵元素可以不断通过内部变换获得, 根据 $C_{200}^{25} = 2.5 \times 10^{30}$, 可使 T_2 元素达到 200个以上, 通过 (120回合以上) 环指方法, 每次选择 25个累加到密值中. 这一方案基本满足日常民用安全水平需要. 如果要求更高, 可以做到 C_{200}^{50} 要求或增加 T_2 元素.

5 结语

通过以上分析, 看到基于 PDX体制理论的 $P_n^{(r)}$ 公钥不但具有高抗击强度的多态变异功能系统, 而且还有独特的引入外部参数手段和优良的等概率构造性能, 为背包型公钥推向应用提供了新的方法.

参考文献

1 Chor B, Rivest R. A knapsack-type public key cryptosystem based on arithmetic in finite fields, IEEE Trans, Inform Theory, 1988, I T- 34, (5): 901~ 909.

2 邵祖华. 子集和组的求解与真分式背包体制的攻破: 密码学新进展, 北京: 科学出版社, 1994. 7~ 15.

3 Peter J, Smith, L U C. Public-key encryption-a secure alternative to RSA. Dr. Dobb's Journal, January 1993: 90 ~ 92.

4 彭宏祥等. P钥原型及抗击 SHORT V ECTOR破译算法研究. 广西大学学报 (自然科学版), 1996, 21 (3): 224 ~ 229.

5 彭典祥等. PDX有限机公钥密码体制. 广西大学学报 (自然科学版), 1995, 20 (3): 295~ 301.

(责任编辑: 黎贞崇)