应用 n-adic 展开的快速 Harn 体制*)

张京良[1,2]　王育民[1]

(西安电子科技大学综合业务网国家重点实验室　西安 710071)[1]　(中国海洋大学数学系　青岛 266071)[2]

摘　要　应用 n-adic 展开方法给出了 Harn 密码体制的改进体制，其安全性与原体制的相同。在加密 t 块消息时，实行一次加密；解密时仅用一次 RSA 和 ElGamal 解密以及求解一个模 n 的线性方程组。而在原体制中，加密时需重复应用 t 次 RSA 与 ElGamal 加密；解密时需重复应用 t 次 RSA 与 ElGamal 解密。由于解线性方程组的速度较快，故当消息分块 t 较大时，无论在加密阶段还是在解密阶段，改进后的体制具有更好的运行效率。

关键词　公钥体制，n-adic，整数分解，离散对数

Fast Harn Cryptosystem Using N-adic Expansion

ZHANG Jing-Liang[1,2]　WANG Yu-Min[1]

(State Key Lab. of Integrated Service Networks, Xidian Univ., Xi'an 710071)[1]

(Department of Mathematics, Ocean Univ. of China, Qingdao 266071)[2]

Abstract　An improved Harn cryptosystem that has the same security as the original one is proposed using n-adic expansion. The proposed cryptosystem only needs one time encryption and decryption as well as solving a system of linear equations modulo n when a large message with t blocks is encrypted, while the originalcryptosystem needs t times RSA and ElGamal encryption and decryption repeatedly, so the proposed cryptosystem has more efficiency when the number of message blocks t is large.

Keywords　Public-key cryptosystem, N-adic, Integer factorization, Discrete logarithm

1　引言

1994 年，Harn [1]提出了一个基于双重困难问题即整数分解与离散对数问题的公钥体制，称为 Harn 体制。在该体制中所取参数为 $p=2p'q'+1, n=p-1$，其中 p, p', q' 皆为大素数。如此攻破此体制需能解子群 Z_p^* 中的离散对数问题及分解 $\frac{n}{2}$。由于 p 与 $\frac{n}{2}$ 的长度相当，从而使得这两个困难问题的困难程度相当，这比 McCurley [3]的体制的实现效率要高。但在加密有 t 个分块的大消息时，该体制的加密过程仅是重复应用 t 次 RSA 加密与 ElGamal 加密，解密时也是如此，因而运行效率较低。

为此，我们用 Takagi [2]的 n-adic 展开方法对该体制进行了改进，改进后的体制在加密 t 块消息时仅需一次模 n^t 的 RSA 加密和一次 ElGamal 加密，解密时仅需一次 RSA 和 ElGamal 加密及求解一个模 n 的线性方程组，由于解线性方程组速度较快，从而我们所提体制比原体制在运行效率上要高。

2　Harn 体制的 n-adic 改进

设大素数 $p=2p'q'+1, p'=2p''+1, q'=2q''+1, p', q', p'', q''$ 也为大素数。Z_p 的本原元是 g。假定用户 B 给用户 A 发送消息 m。A 任取 $x\in Z_p$，计算 $y=g^x \bmod p$，记 $n=\frac{p-1}{2}=p'q'$。再选取整数 e 使得 $\gcd(e,n)=1$，并求 d 使得 $ed=1 \bmod \Phi(p-1)$，则 A 的公钥为 (p,g,y,e)，私钥为 (p',q',x,d)。

阶段 1：公钥分配

B 得到 A 的公钥 (p,g,y,e)，并随机选择 $k\in[1,p-1]$，计算 $K_{AB}=y^k \bmod p$，k 是 B 的秘密会话钥，K_{AB} 是 AB 的公共会话钥。B 计算 $z=g^k \bmod p, v=z^e \bmod (p-1)$，将 v 送给 A。

阶段 2：加密

B 将 m 分成 t 块，设为 $m_0, m_1, \cdots, m_{t-1}$，且 $m_0\in Z_n^*, m_i\in Z_n, i=1,2,\cdots,t-1$。计算

$$C'=(m_0+nm_1+\cdots+n^{t-1}m_{t-1})^e \bmod n^t \tag{1}$$

$$C=K_{AB}C' \bmod p$$

阶段 3：解密

A 收到 v 后，计算

$$Z=v^d \bmod (p-1), K_{AB}=z^x \bmod p$$

$$C'=CK_{AB}^{-1} \bmod p, m_0=C'^d \bmod n$$

其余各块解模 n 的线性方程组，具体如下：

假设已经如上，由原 RSA 体制的解密方法得到了 m_0，下面介绍得到 $m_1, \cdots, m_{t-1}$ 的过程。将加密函数(1)按多项式定理展开得：

$$\sum_{\substack{0\leqslant s_0,s_1,\cdots,s_{t-1}\leqslant e\\ s_0+s_1+\cdots+s_{t-1}=e}} \frac{e!}{s_0!\ s_1!\ \cdots s_{t-1}!} m_0^{s_0}(nm_1)^{s_1}\cdots(n^{t-1}m_{t-1})^{s_{t-1}}$$

令 $\Gamma_i=\{(s_0,s_1,\cdots,s_i)\mid s_1+2s_2+\cdots is_i=i, s_0+s_1+\cdots+s_i=e, 0\leqslant s_0,s_1,\cdots,s_i\leqslant e\}, 0\leqslant i\leqslant t-1$。

令 $D_i(m_0,m_1,\cdots,m_i)$ 是 n^i 的系数 $(0\leqslant i\leqslant t-1)$，对 $i=0,1,\cdots,t-1$，$D_i(m_0,m_1,m_i)$ 可如下计算

*)基金项目：国家自然科学基金(60473072)。张京良　博士生，讲师，主要研究方向为信息安全；王育民　教授，博士生导师，主要研究方向为信息论、密码、编码。

$$D_i(m_0,m_1,\cdots,m_i)=\sum_{(s_0,s_1,\cdots,s_i)\in\Gamma_i}\frac{e!}{s_0!\ s_1!\ \cdots s_i!}m_0^{s_0}m_1^{s_1}\cdots m_i^{s_i} \quad (2)$$

这里，将较小 i 时的 D_i 写出如下：

$D_0=(m_0)=m_0^e$

$D_1(m_0,m_1)=em_0^{e-1}m_1$

$D_2(m_0,m_1,m_2)=C_e^2m_0^{e-2}m_1^2+em_0^{e-1}m_2$

$D_3(m_0,m_1,m_2,m_3)=C_e^3m_0^{e-3}m_1^3+2C_e^2m^{e-2}m_1m_2+em_0^{e-1}m_3$

$D_4(m_0,m_1,m_2,m_3,m_4)=C_e^4m_0^{e-4}m_1^4+3C_e^3m_0^{e-3}m_1^2m_2+C_e^2m_0^{e-2}m_2^2+em_0^{e-1}m_4$

$D_5(m_0,m_1,\cdots,m_5)=C_e^5m_0^{e-5}m_1^5+4C_e^4m_0^{e-4}m_1^3m_2+3C_e^3m_0^{e-3}m_1m_2^2+2C_e^2m_0^{e-2}m_2m_3+2C_e^2m_0^{e-2}m_1m_4+em_0^{e-1}m_5$

……

……

$D_{t-1}(m_0,m_1,\cdots,m_{t-1})=\{m_0,m_1,\cdots\cdots,m_{t-1}$的多项式$\}$

注意到，含 m_i 的项在 $D_j(j<i)$ 中不出现且 D_i 中含 m_i 的项仅为 $em_0^{e-1}m_i$，$i=0,1,\cdots,t-1$。

定义 $D'_i(m_0,m_1,\cdots,m_{i-1})=D_i(m_0,m_1,\cdots,m_i)-em_0^{e-1}m_i$，从而 D_0,D_1,D_{i-1},D'_i 都是 $m_0,m_1,\cdots,m_{i-1}$ 的多项式$(0\leqslant i\leqslant t-1)$。

$m_1,m_2,\cdots,m_{t-1}$ 可按下述方法递推计算：

取 $i=1$，$D'_1(m_0)=0$，$D_0(m_0)=m_0^e$，解线性方程

$em_0^{e-1}x\equiv B_1\pmod n$，$B_1=E_1/n$，$E_1\equiv C'-D_0(m_0)\pmod{n^2}$

解便是 m_1。因为已知条件中要求 $\gcd(e,n)=1$，$m_0\in Z_n^*$，所以上述方程有唯一解。

假设解密得到了 $m_1,m_2,\cdots,m_{i-1}$，用同样方法，通过解下述线性方程可得 m_i：

$$em_0^{e-1}x\equiv B_i\pmod n,$$

$$B_i=E_i/n^i\quad E_i\equiv C'-\sum_{j=0}^{i-1}n^jD_j(m_0,m_1,\cdots,m_j)-n^iD'_i(m_0,m_1,\cdots,m_{i-1})\pmod{n^{i+1}}$$

递推地，可解密得所有明文 $m_1,m_2,\cdots,m_{t-1}$

解密过程可用下述程序表示：$[x]_N$ 表示 x 模 N

```
Procedure DECRYPTION
INPUT: d, n, C'(:=[(m0+nm1+…+n^(t-1)m(t-1))^e]n')
OUTPUT: m0, m1, …, m(t-1)
(1)C0 := [C']n
   m0 := [C0^d]n
(2)D0 := [m0^e]n^2
   E1 := [C'-D0]n^2
   B1 := E1/n in Z
   A := [(eC0)^-1 m0]n
   m1 := [A B1]n
(3)FOR i=2to (t-1)do
     begin
     SUM := 0
     FOR j=0 to (i-1) do
     begin
     Dj := [Dj(m0,m1,…,mj)]n^(i+1)
     SUM := [SUM+n^d Dj]n^(i+1)
     end
   D'i := [D'i(m0,m1,…,m(i-1))]n^(i+1)
   Ei := [C-SUM-n^i D'i]n^(i+1)
   Bi := Ei/n^i in Z
  mi := [A Bi]n
  end
```

3 讨论

(1)安全性。由于 Takagi[2] 证明了 n-adic 型 RSA 体制与原 RSA 体制的安全性相同，从而我们的体制与 Harn 体制的安全性相同。

(2)性能比较。两个体制的密钥分配阶段是一样的；在加密阶段，Harn 体制需 $2t$ 个模指数运算与 $2t$ 个乘法，而我们的体制仅需一个模 n^t 的指数运算和一个乘法，当然为了使 mod n^t 的指数运算尽可能地快，可选取较小的公钥 e；在解密阶段 Harn 体制需 $3t+2$ 个模指数运算与 t 个乘法，而我们的体制需 2 个模指数运算与解一个模 n 的线性方程组，由于解线性方程组速度较快，因此我们的体制在运行效率上的优势十分明显。

结论 我们用 Takagi[2] 的 n-adic 展开方法给出了 Harn[1] 体制的一个改进体制，所给出的体制与原体制的安全性相同，但运行效率比原体制要高得多。

参考文献

1 Harn L. Public-key Cryptosystem Design Based on Factoring and Discrete Logrithms. IEE Proc. Comput. Digit. Tech., 1994, 14 (3): 193～195

2 Takagi T. Fast RSA-Type Cryptosystems Using N-Adic Expansion, Advances in Cryptology—CRYPT'97. In: B. S. Kaliski Jr, ed. Springer-Verlag Berlin Heidelberg, LNCS 1294, 1997. 372～384

3 McCurley K S. A Key Distribution System Equivalent to Factoring. J. Cryptology, 1988, 1(2): 95～106

4 Lim S, Kim S, Yie I, Lee H. A Generalized Takagi-Cryptosystem with a Modulus of the Form p^rq^s. In: B. Roy, E. Okamoto, eds. INDOCRYPT 2000, LNCS, 1977. 283～294, Springer-Verlag, Berlin, Heidelberg, 2000

5 Hinek M J, Low M K, Teske E. On Some Attacks on Multi-prime RSA. In: K. Nyberg, H. Heys, eds. SAC2002, LNCS 2595, Springer-Verlag, Berlin, Heidelberg, 2003. 385～404

(上接第 35 页)

3 Felegyhazi M, Buttyan L, Hubaux J-P. Cooperative Packet Forwarding in Multi-Domain Sensor Networks. In: Proc. of IEEE PerSeNS 2005, Hawaii, Mar. 2005

4 Marbach P, Qiu Y. Cooperation in Wireless Ad Hoc Networks: A Market-Based Approach. IEEE/ACM Transactions on Networking, 2005, 13 (6): 1325～1338

5 Buttýan L, Hubaux J. -P. Stimulating Cooperation in Self-Organizing Mobile Ad Hoc Networks. ACM/Kluwer Mobile Networks and Applications (MONET)Special Issue on Mobile Ad Hoc Networks, 2003, 8 (5): 579～592

6 Zhong S, Chen J, Yang Y R. Sprite: A Simple, Cheat-proof, Credit-based System for Mobile Ad hoc Networks. In Proceeding of IEEE IOFOCOM'03, 2003(3): 1987～1997

7 Ileri O, Mau S-C, Mandayam N B. Pricing for Enabling Forwarding in Self-Configuring Ad Hoc Networks. IEEE J. Select. Areas commun, 2005, 23(1)

8 Altman E, Kherani A A, Michiardi P, Molva R. Non-cooperative Forwarding in Ad-hoc Networks. Technical Report INRIA Report No. RR-5116, 2004

9 Felegyhazi M, Hubaux J P, Buttyan L. Nash Equilibria of Packet Forwarding Strategies in Wireless Ad Hoc Networks. IEEE Transactions on Mobile Computing, 2005, 5: 463～476

10 Osborne M J, Rubinstein A. A course in Game Theory, MIT press, 1994

11 MacKenzie A B, Wicker S B. Game Theory and the Design of Self-configuring, Adaptive Wireless Networks. IEEE Communications Magazine, 2001, 39 (11): 126～131

12 Axelrod R. The Evolution of Cooperation, Basic Books, New York, 1984

13 Nash J. Equilibrium Points in N-person Games. Proceedings of the National Academy of Sciences, 1950, 36: 48～49

14 Fudenburg D, Tirole J. Game Theory, Cambridge, MA: MIT Press, 1991

15 Bertsekas D P, Tsitsiklis J N. Neuro-Dynamic Programming, Athena Scientific, Belmant, 1996.