对一种基于椭圆曲线加密体制的安全性分析*)

姜正涛　郝艳华　王育民
(西安电子科技大学 综合业务网国家重点实验室　西安 710071)

摘　要　本文对一种椭圆曲线环上的陷门离散对数加密体制的安全性进行分析，指出它存在的安全缺陷，攻击者通过选择适当的明文加密，在得到相应的解密明文后，能够分解模数，从而成功地攻击此加密体制，因此该体制不能抵抗选择密文攻击。

关键词　椭圆曲线加密体制，安全性分析，选择密文攻击，分解模数

Security Analysis of an Elliptic-Curve Based Encryption Scheme

JIANG Zheng-Tao　HAO Yan-Hua　WANG Yu-Min
(National Key Lab. of Integrated Service Networks, Xidian Univ., Xi'an 710071)

Abstract　We provide security analysis of a trapdoor discrete logarithm encryption scheme in elliptic curve ring proposed by Paillier, and point out the security flaws of it. The attacker can choose a proper plaintext to be encrypted, after getting the decrypted plaintext, he can factorize the modulus, and attack the encryption scheme successively, so this encryption scheme can not withstand chosen ciphertext attack.

Keywords　Elliptic curve cryptographic scheme, Security analysis, Chosen ciphertext attack, Modulus factorization

1　引言

自从 Diffie 和 Hellman 提出公钥密码体制以来，研究者对公钥密码学这一领域进行了广泛深入的研究[1,2]，不断提出基于新的困难问题的密码体制以满足不尽相同的应用需求[3,4]。密码分析的主要目的是对已提出的密码体制的安全性进行分析，一方面指出密码体制(在实际应用中应当避免)的安全缺陷，另一方面通过对密码体制的分析，也证明了密码体制的安全性[5]。

2000 年，Pascal Paillier 在亚洲密码会议上提出了一种椭圆曲线密码体制的变形(P-EC)，基于新的困难问题，该体制具有单向性和语意安全性等特性[6]。本文对该体制的安全性进行分析，指出该体制不能抵抗选择密文攻击，攻击者的一次选择密文攻击就可以求得模数的一个素因子，从而分解模数，成功地攻击该加密体制。类似地，该选择密文攻击方法同样适于对 Okamoto-Uchiyama 密码体制的分析[7]。

2　P-EC 的描述

首先解密者(或可信第三方)选取长度为 k 的两个大素数 $p(p\equiv 2(\bmod 3))$ 和 q，计算 $n=pq$；并选取两个整数 $\overline{a_p},\overline{b_p}\in F_p$，满足 $E_p(\bar{a},\bar{b})$ 的阶为 $p+2$。随机选取定义在 F_q 上的椭圆曲线 $E_q(\overline{a_q},\overline{b_q})$[6]。

令 $E_{p^2}(a_p,b_p)$ 是 $E_p(\bar{a},\bar{b})$ 到 F_{p^2} 上的一个提升，由中国剩余定理，解密者由 $E_{P^2}(a_p,b_p)$ 和 $E_q(\overline{a_q},\overline{b_q})$ 可以得到椭圆曲线 $E_n(a,b)$，其中 $a,b\in Z_n^*$[6]。

最后，解密者选取 $E_n(a,b)$ 上阶为 $lcm(|E_{p^2}|,|E_q|)$ 的点 G，并计算 $H=nG$。

该密码体制的描述如下：

公开参数　n,G,H；

秘密参数　p；

加密　明文 $m<2^{k-1}$，随机选取 $r<2^{2k}$，密文 $C=mG+rH$；

解密　$m=\dfrac{\phi_p((p+2)C)}{\phi_p((p+2)G)} \bmod p$。

其中 ϕ_p 是定义在 $E_{p^2}(a_p,b_p)$ 中的 p-挠点组成的群 $E[p]$ 到 F_p 的一个影射[7~9]，满足对任意的 $P,G\in E[p]$，如果 $G=mP$ $(m<p)$，则有

$$m=\frac{\phi_p(P)}{\phi_p(G)} \bmod p。$$

3　安全性分析

引理 1[6]　设 $E_p(\bar{a},\bar{b}):y^2=x^3+\bar{a}x+\bar{b} \bmod p$ 的阶为 $|E_p(\bar{a},\bar{b})|=p+1-t$，其中 $|t|\leqslant 2\sqrt{p}$，则对任意满足 $a\equiv\bar{a} \bmod p$ 和 $b\equiv\bar{b} \bmod p$ 的整数 a,b，均有

$$|E_{p^2}(a,b)|=(p+1-t)(p+1+t)$$

引理 2[6]　设 $E_p(\bar{a},\bar{b})$ 是 F_p 上阶为 $p+2$ 的椭圆曲线，如果 $p\equiv 2(\bmod 3)$，则 $E_p(\bar{a},\bar{b})$ 到 F_{p^2} 的任意提升 $E_{p^2}(a,b)$ 均为循环群。

定理 1　攻击者选取适当的消息 $m(m>2^k)$，并对 m 加密得密文 $C=mG+rH$，在得到"正确的"解密明文 m_1 后，可以分解模数 $n=p^2q$。

证明：由参数的选择，$E_p(\bar{a},\bar{b})$ 的阶为 $p+2$，再由引理 1 和引理 2，$E_p(\bar{a},\bar{b})$ 的提升 $E_{p^2}(a,b)$ 的阶为 $p(p+2)$ 且为循环群。

*)国家自然科学重点基金资助项目(69931010)；国家"863"基金资助项目(2002AA143021)；国家通信保密基金项目(J 6410130)。**姜正涛**　博士研究生，研究方向为密码算法理论的研究与分析，数论及其应用，通信网的安全等。**郝艳华**　博士研究生，研究方向为椭圆密码体制的研究与分析。**王育民**　教授，博士生导师，主要从事编码理论、密码学、信息安全等领域的科研与教学工作。

由于攻击者所选取的加密明文 $m>p$，则 $m=lp+m_i$，其中 l 为正整数。于是，密文

$$C=mG+rH=m_1G+lpG+rnG$$

因此，解密用户在 $E[P]$ 中执行的解密算法得到

$$\frac{\phi_p((p+2)C)}{\phi_p((p+2+G)} \bmod p=$$

$$\frac{\phi_p((p+2)m_1G+l(p+2)pG+r(p+2)nG)}{\phi_p((p+2)G)} \bmod p \qquad (1)$$

因为 $E_p(\bar{a},\bar{b})$ 的阶为 $p(p+2)$，于是在 $E_{p^2}(a,b)$ 中有

$$(p+2)m_1G+l(p+2)pG+r(p+2)nG$$
$$=(p+2)m_1G+O_{p^2}$$

这里的 O_{p^2} 是 $E_{p^2}(a,b)$ 中的单位元。所以

$$\frac{\phi_p((p+2)C)}{\phi_p((p+2)G)} \bmod p=\frac{\phi_p((p+2)m_1G+O_{p^2})}{\phi_p((p+2)G)} \bmod$$
$$p=m_1 \qquad (2)$$

由于 $p|m-m_q$，当攻击者得到解密明文 m_1 后，可以计算 $p=\gcd(m-m_1,n)$

攻击者求得素因子 p 后，能够完全分解模数 n。这样，攻击者可以运用第 2 节中的解密算法，计算

$$m=\frac{\phi_p((p+2)C)}{\phi_p((p\div2)G)} \bmod p$$

对所有的密文解密，从而成功攻击此加密体制。

结束语 本文对 Paillier 提出的基于椭圆曲线陷门离散对数加密体制的安全性进行了简单的分析，指出它存在的安全缺陷，不能抵抗选择密文攻击，在使用该加密体制时应当特别注意这一点。

为了避免这种不安全性，在实际应用中，不能向攻击者出示解密后的明文，然而，攻击者可以从解密结果的有效性得知他所选择的明文与素因子 p 的大小关系，这也为分解模数提供了重要的信息。

参 考 文 献

1 Diffie W, Hellman M. New directions in cryptography[J]. IEEE Transactions on Information Theory, 1976, 22(6): 644～654

2 Rivest R, Shamir A, Adleman L. A method for obtaining digital signatures and public-key cryptosystems[A]. CACM, 1978, 21(2): 120～126

3 Koyama K, Maurer U, Okamoto T, Vanstone S. New Public-Key Schemes based on Elliptic Curves over the ring Z_n[A]. In: Advances in Cryptology, Proc. of Crypto'91, LNCS 576[C], Springer-Verlag, 1992. 252～266

4 Pallier P. Public-Key Cryptosystems Based on Composite Degree Residuosity Classes[A]. Advances in Cryptology-EUROCRYPT'99, LNCS 1592[C], Springer-Verlag, 1999. 223～238

5 Catalano D, Gennaro R, Graham N H. The bit security of Paillier's encryption scheme and its applications[A]. Advances in Cryptology- EUROCRYPTO'01, LNCS 2045[C], Springer-Verlag, 2001. 229～243

6 Paillier P. Trapdooring Discrete Logarithms on Elliptic Curves over Rings[A]. Advances in Cryptology- ASIACRYPT 2000, LNCS 1976[C], Springer-Verlag, 2000. 573～584

7 Okamoto T, Uchiyama S. A new public key cryptosystem as secure as factoring[A]. Advances in Cryptology-EUROCRYPTO'98[C], LNCS 1043, 1998. 309～318

8 Semaev I A. Evaluation of Discrete Logarithms in a Group of p-Torsion Points of an Elliptic Curve in Characteristic p[J]. Math. Comp., 1998, 67: 353～356

9 Silverman J H. The Arithmetic of Elliptic Curves[M]. Springer-Verlag, GTM 106, 1986

(上接第 67 页)

既然 I-型序列的 0-1 分布不均，不妨假设 1 的个数比 0 多 $2^{\frac{n-1}{2}}$ 个，我们试图将 $2^{\frac{n-1}{2}}$ 个 1 改为 0，使得 0-1 分布均匀，而不改变该序列的周期和线性复杂度。下面提出三种方案。

方案一：1. 置 $a_v=a_{\frac{v}{2}}+1$；2. 随机改变除 a_v，$a_{\frac{v}{2}}$ 外的其它元素，使得 0-1 分布平衡。

方案二：1. 置 $a_v=a_{\frac{v}{2}}+1$；2. 随机改变除 a_v，$a_{\frac{v}{2}}$ 外的元素对 $\binom{a_i}{b_i}=\binom{1}{1}$ 为 $\binom{0}{0}$，使得 0-1 分布平衡。

方案三：1. 令 $S'_0=S_0\oplus S_1$，取 $S=(S'_0,S_1)^T$；2. 在 S'_0 中如果 $a_v=a_{\frac{v}{2}}$，则 a_1 与 a_v 对调。

方案一和方案二的(1)及方案三的(2)是为了保证修改后的 S 的周期仍为 2^{n+1}，可从定理 2 的证明看出。从而 S 的线性复杂度的界不变。方案三注意到 iP 与 $(v-i)P$ 互为反点，从而 $a_i=a_{v-i}$，$b_i=b_{v-i}+1$，于是 $\begin{pmatrix}a_i & a_{v-i}\\ b_i & b_{v-i}\end{pmatrix}=\begin{pmatrix}1 & 1\\ z & z+1\end{pmatrix}$ 或 $\begin{pmatrix}0 & 0\\ z & z+1\end{pmatrix}$，$z=0$ 或 1，那么把第二行加到第一行，得 $\begin{pmatrix}1+z & z\\ z & z+1\end{pmatrix}$ 或 $\begin{pmatrix}z & z+1\\ z & z+1\end{pmatrix}$，上下两行的 0、1 个数相同，从而使得 0-1 分布平衡。特别是方案三，在软件和硬件上都易实现。

例 3 条件同例 2，应用方案三，

$S'_0=S_0\oplus S_1=(01000111011010001110100100011101)$，那么

$S=(S'_0,S_1)^T=(00110100011010110110110110010100111010011000011000010110111000011)$，$S$ 的极小多项式为 $m(x)=(1+x)^{61}$。

参 考 文 献

1 Koblitz N. Elliptic curve cryptosystems[J]. Math. Comp., 1987, 48: 203～209

2 Miller V. Uses of elliptic curves in cryptography[A]. Advances in Cryptology-CRYPTO'85[C]. LNCS 218. Berlin: Spring-Verlag, 1986. 417～426

3 Kaliski B. A pseudorandom bit generator based on elliptic logarithms[A]. Advances in Cryptology-CRYPTO'86[C]. LNCS 263. Berlin: Spring-Verlag, 1986. 84～103

4 Gong G, Berson T, Stinson D. Elliptic curve pseudorandom sequence generator[A]. In: Proc. of the sixth annual workshop on selected areas in Cryptography, LNCS 1758, Berlin: Spring-Verlag, (Extended http://www.cacr.math.uwaterloo.ca:[Technical Reports, CORR1998-53]. 1998. 34～48

5 Gong G, Lam C. Linear recursive sequences over elliptic curves [A]. In: Proc. of Sequences and Their Applications-SETA'01 [C]. DMTCS series. Berlin: Spring-Verlag, 2001. 182～196

6 Lam C Y, Gong G. Randomness of elliptic curve sequences[R]. http://www.cacr.math.Uwaterloo.ca: [Technical Reports, CORR2002-18]. 2002

7 Beelen P H T, Doumen J M. Pseudorandom sequences from elliptic curves[A]. Finite Fields with Applications to Coding Theory, Cryptography and Related Areas [C]. Berlin: Spring-Verlag, 2002. 37～52

8 Enge A. Elliptic curves and their applications to cryptography: an introduction[M]. Kluwer Academic Publishers, Dordrecht, 1999

9 丁存生，肖国镇. 流密码及其应用[M]. 北京：国防工业出版社，1994