基于椭圆曲线同源的公钥密码机制

胡 进，何德彪，陈建华，黄 尹
（武汉大学 数学与统计学院，武汉 430072）

摘 要：针对 RSA 公钥密码系统和椭圆曲线密码系统基于的数学难题均不能抵抗量子计算机攻击问题，提出了一种能构造公钥密码系统的数学难题——椭圆曲线同源星上的计算问题. 解决该数学难题的时间复杂度为指数级，该数学难题能抵抗量子计算机攻击. 在此数学难题基础上构造了一个公钥密码机制 ECIIES（elliptic curve isogenies integrated encryption scheme），ECIIES 是在基本 Elgamal 机制基础上，通过对中间变量和密文作校验来抵抗自主消息攻击. 在随机模型下证明了 ECIIES 在自主选择消息攻击下是不可区分安全的.

关键词：公钥密码系统；量子计算机；同源；椭圆曲线；自主选择消息攻击；随机模型
中图分类号：TN 918 **文献标志码**：A **文章编号**：0254－0037(2011)06－0916－05

目前，主流的公钥密码技术为 RSA 和椭圆曲线密码. RSA 密码的安全性基于大整数分解，椭圆曲线密码的安全性基于椭圆曲线群上的离散对数问题. 但是量子计算机的相关研究表明，根据以量子计算机为核心的 Shor 算法[1]，量子计算机能在多项式时间内解决上述两大难题. 数学难题是公钥密码学的基石，一旦相应的数学难题被攻破，则 RSA 和椭圆曲线密码的安全性也将不存在.

为了弥补以量子计算机为核心的 Shor 算法带来的安全漏洞，一种办法是使用现在不太常用的密码系统，这些密码系统还没有相应的量子攻击算法，如 NTRU 公钥密码系统[2-4]、McEliece 加密系统[5]、HFE（hidden field equations）签名系统[6]和基于辫群[7]的公钥密码系统等；另一种办法就是寻找新的能抵抗量子计算机攻击的数学难题，在此难题上构造新的公钥密码系统. 最近，一种新的数学难题——阿贝尔群范畴上的态射计算问题引起了密码学界的广泛兴趣. 该数学难题被认为能抵挡量子计算机攻击，也适用于构造公钥密码系统[8]. 特别是基于有限域上椭圆曲线之间的同源计算问题，使用多条椭圆曲线来代替单条椭圆曲线，可以提供更高的安全性，极具研究价值和应用潜力.

作者介绍了一种能抵抗量子计算机攻击的数学难题：椭圆曲线同源星上的计算问题，并分析了该数学难题的安全性，并在此数学难题的基础上，构造了一个基于椭圆曲线同源的公钥密码机制 ECIIES（elliptic curve isogenies integrated encryption scheme）. 在随机模型下，证明了公钥密码机制 ECIIES 在自主选择消息攻击下是不可区分安全的.

1 同源星及其安全性

1.1 同源星

设 $E: y^2 = x^3 + ax + b, a, b \in F_p$ 是定义在有限域 F_p 上的椭圆曲线，D_π 为其 Frobenius 方程的判别式. 设 $U = \{E_i(F_p)\}$ 为所有定义在 F_p 上有相同阶的椭圆曲线集合，U 中的每个元由它的 j－不变量唯一确定，U 中的元都是两两互为同源[9]，并且 $\#U = h_{D_\pi}$，h_{D_π} 为 $Q(\sqrt{D_\pi})$ 上 Hilbert 类多项式一次因子的个数.

根据椭圆曲线同源的性质，U 中的任意 2 条曲线之间的同源映射由次数为素数的同源映射复合而成，对于给定的椭圆曲线 E，其 j－不变量为 j，则定义在复数域上的 l－同源的椭圆曲线的 j－不变量满足经典

收稿日期：2009-04-24.
基金项目：国家“八六三”计划资助项目（2001AA141010）.
作者简介：胡 进（1979—），男，湖北襄樊人，博士生.

的模多项式方程

$$\phi_l(X,j) = \prod_{i=1}^{\psi(l)} (X - j(\alpha_i\tau))$$

在上述曲线中间，定义在 F_p 上的 l -同源的曲线个数由参考文献[9]给出.

如果挑选 D_π 和素数 l 满足 $\left(\frac{D_\pi}{l}\right) = 1$，则 U 中的任意一条曲线存在 2 条 l -同源的椭圆曲线[9]，这样 U 中的 l -同源就形成了圈. 进一步，如果 $\#U$ 为素数则可以证明 U 中的 l -同源形成了单同源圈(single isogeny cycle). 如果挑选另外的 $l_1 \neq l$ 并且 $\left(\frac{D_\pi}{l_1}\right) = 1$，则又可以形成另外的 l_1 -单同源圈，这一过程可以一直继续下去，U 中的同源形成了次数不同的单同源圈.

定义 1　由 U 中的元(顶点)和满足 $\left(\frac{D_\pi}{l_i}\right) = 1$ 的 l_i -单同源圈形成的图称为同源星(isogeny star).

如果 U 中的元足够多，l_i -单同源圈也足够多，则可以形成非常复杂的同源星. 在此基础上，定义同源星中边的方向[10]和路径，就可以构造公钥密码系统.

设 S 为同源星，$L = \{l_i\}$ 为同源星中 Elkies 数的集合，$F = \{\pi_i\}$ 是 Frobenius 映射对每个 $l_i \in L$ 在 Z/l_iZ 中的指定同源正方向的特征值集合.

定义 2　集合 $R = \{r_i\}$，这里 r_i 表示沿着 l_i -单同源圈的正方向 π_i 前进的步数，定义为同源星中的一条路径.

设路径 $A = \{a_i\}$，$B = \{b_i\}$，定义路径的复合运算为 $AB = \{a_i + b_i\}$，显然有 $AB = BA$.

1.2　安全性

目前已知的搜索计算椭圆曲线之间的同源映射的方法有:

1) 暴力破解，时间复杂度 $O(n)$.

2) 中间碰撞法，时间复杂度 $O(\sqrt{n})$.

3) 文献[11]给出的攻击方法，时间复杂度 $O(\sqrt[4]{p})$.

同源星上的同源搜索计算问题可以抵抗量子计算机的攻击. 具体描述如下: 对于有限域上椭圆曲线之间的同源，每个同源的计算需要解方程 $\phi_l(X,j) = 0$. 为了计算 q 个同源映射组成的同源链，其过程为

$$E_1 \to \phi_{l_1}(X, j_{E_1}) = 0 \to j_{E_2} \to E_2 \to \phi_{l_2}(X, j_{E_2}) = 0 \to j_{E_3} \to \cdots$$

由于方程 $\phi_l(X,j) = 0$ 中 j 值随着曲线和 l 的不同而不断变化，并且数据有前后的依赖关系，所以在量子计算机上，这一计算过程并不能被并行化，这意味着量子计算机的随机并行优势在解决搜索椭圆曲线之间同源映射方面得不到发挥.

综上所述，有限域 F_p 上的椭圆曲线同源搜索计算问题时间复杂度 $O(\sqrt{n}) \approx O(\sqrt[4]{p})$，是输入规模 $\log p$ 的指数级.

2　基于同源星的公钥密码机制 ECIIES

2.1　系统参数

系统公共参数包括: 有限域 F_p; 初始椭圆曲线 $E_{\text{init}}: y^2 = x^3 + a_{\text{init}}x + b_{\text{init}}$，$a_{\text{init}}, b_{\text{init}} \in F_p$; 单同源圈的个数 d; Elkies 数的集合 $L = \{l_i\}$，$1 \leqslant i \leqslant d$; Frobenius 映射对每个 $l_i \in L$ 指定同源正方向的特征值集合 $F = \{\pi_i\}$，$1 \leqslant i \leqslant d$; 路径中沿着单同源正方向圈前进的步数的上限值 k，即对任意路径 $\{r_i\}$，$-k \leqslant r_i \leqslant k$; 密钥派生函数 KDF: ANSI-X9.63-KDF; 消息验证码函数 MAC: HMAC-SHA-1.

密钥生成包括:

1) 用户私钥路径 R_{priv}.

2) 用户公钥椭圆曲线 $E_{\text{pub}} = R_{\text{priv}}(E_{\text{init}})$，该椭圆曲线由$(a_{\text{pub}}, b_{\text{pub}})$给定.

2.2 加密

设需要发送的消息为比特串 m，s 为 m 的比特长度，则

1) 随机选择路径 R_{enc}，如果 $R_{\text{enc}} = \{0, 0, \ldots, 0\}$，则重新选择路径 R_{enc};
2) 计算 $E_{\text{enc}} = R_{\text{enc}}(E_{\text{pub}})$;
3) 计算 $C_1 = R_{\text{enc}}(E_{\text{init}})$;
4) 计算 $t = \text{KDF}(j_{\text{enc}}, s)$，若 t 为全零，则返回步骤 1);
5) $C_2 = m \oplus t$;
6) $C_3 = \text{MAC}(C_1, C_2, j_{\text{enc}})$;
7) 输出密文 $C = (C_1, C_2, C_3)$.

2.3 解密

设 s 为密文中 C_2 的比特长度，则

1) 从密文 C 中取出比特串 C_1，计算 $E'_{\text{enc}} = R_{\text{priv}}(C_1)$;
2) 判断 $C_3 = \text{MAC}(C_1, C_2, j'_{\text{enc}})$ 是否成立，若否，则报错并退出;
3) 计算 $t' = \text{KDF}(j'_{\text{enc}}, s)$，若 t' 全为零，则报错并退出;
4) 输出明文 $m = C_2 \oplus t'$.

3 安全性证明

对于公钥加密机制的安全性要求一般是针对密文的特性而言，即指密文应满足的某种安全特性. 目前，被国际密码学界所广泛接受的密文安全性要求主要有 3 种: 单向性(one-wayness，OW)、不可区分性(indistinguishability，IND)和不可延展性(non-malleability，NM). 对于公钥密码机制的攻击行为包括选择明文攻击(chosen plaintext attack，CPA)、选择密文攻击(chosen cipher attack，CCA1)和自主选择密文攻击(adaptive chosen cipher attack，CCA2). CCA2 是从网络上对于公钥加密机制的攻击行为中抽象出的一种最强攻击行为模型. 将攻击方法和安全性要求相结合，就可得到公钥加密机制的安全性定义. 目前，IND-CCA2 已成为目前国际密码学界衡量一个公钥加密机制安全性的最重要指标，一个公钥加密机制只有被严格证明是 IND-CCA2 安全的才能被大家认可和采纳.

引理 1 公钥加密机制 ECIIES 存在一个成功概率为 $1 - (1/2^{\lambda} + q_E\delta + 1/2^{s})$ 的明文提取(knowledge extractor，KE)算法，其运行时间为 $q_F t$. 其中，q_E、q_F 为访问加密机和随机源 F 的次数; t 为椭圆曲线之间同源计算的时间复杂度; δ 为解决有限域 F_{p} 上的椭圆曲线同源搜索问题的概率; λ、s 分别为消息验证码(message authentication code，MAC)和密钥派生函数(key derivation function，KDF)的输出位长.

证明: 设 B 为加密机制 ECIIES 的一个攻击者，它可以访问随机源 KDF、MAC 和加密机 ENC(encryptor). 设访问次数分别为 q_K、q_H 和 q_E 次. 令 τ_K、τ_H 分别表示攻击者 B 访问随机源 KDF、MAC 的记录

$$\tau_K = \{(k_1, K_1), (k_2, K_2), \cdots (k_{q_K}, K_{q_K})\}$$
$$\tau_H = \{(h_1, H_1), (h_2, H_2), \cdots (h_{q_H}, H_{q_H})\}$$

η 为攻击者 B 访问加密机 ENC 的记录，其中 k_i 为 $R_i(E_{\text{pub}})$ 的 j-不变量. 记 B 所产生的挑战密文为 $C = (C_1, C_2, C_3)$. KE[12] 算法构造如下.

输入: $\tau_K, \tau_H, \eta, C, E_{\text{init}}$

输出: 明文 m 或者空字符串 ε

算法:

For i from 1 to q_K

If $j_{C_1} = j_{R_i(E_{\text{init}})}$

For l from 1 to q_H

If $C_1 \parallel C_2 \parallel k_i = h_l$ and $C_3 = H_l$

Then $m = C_2 \oplus K_i$ and break;

else $m \leftarrow \varepsilon$

else $m \leftarrow \varepsilon$

return m

考虑 KE 算法的成功概率，令 Fail 为事件 KE 算法的输出不真，即 $m \neq D_{sk}(C)$.

令 R 为椭圆曲线 E_{init} 到椭圆曲线 C_1 的路径，$j = j_{R(E_{\text{pub}})}$，$m' = C_2 \oplus \text{KDF}(j)$，$h = C_1 \parallel C_2 \parallel j$.

令 W 为攻击者 B 向随机源 KDF 访问了 j 的事件，令 U 为攻击者 B 向随机源 MAC 访问了 h 的事件.

假设攻击者 B 没有访问 h，则由 KE 算法的构造知 KE 输出为空字符串 ε，如果 KE 输出不真，那么 C 一定是合法密文，即有 $C_3 = \text{MAC}(h)$. 如果在 η 中存在密文 C'，与挑战密文的 C_3 相等，则由随机模型的定义知 $C = C' \in \eta$. 攻击者还可能从记录 τ_H 获得 $\text{MAC}(h)$ 的信息，但是因为 h 没有被访问，故 $\text{MAC}(h)$ 是其值域上的随机数，从而 $\Pr[\text{MAC}(h) = C_3] = 1/2^{\lambda}$.

攻击者 B 从 η 中伪造 h 即获得 j 的信息，这即为解决素域 F_p 上的椭圆曲线同源搜索问题，攻击者伪造成功的概率为 $q_E\delta$（δ 为解决素域 F_p 上的椭圆曲线同源搜索问题的概率，可忽略）.

假设攻击者访问了 h 但没有访问 j，则 KE 输出为空字符串 ε，如果 KE 的输出不真，那么 C 一定是合法密文. 如果攻击者从 η 中获得 $\text{KDF}(j)$ 的信息，则攻击者必须从 η 中伪造 h，攻击者伪造成功的概率为 $q_E\delta$；否则攻击者只能从 τ_K 处获得 $\text{KDF}(j)$ 的信息，但因为 j 没有被访问，故 $\text{KDF}(j)$ 是其值域上的随机数，从而密文 C 为合法密文的概率为 $1/2^s$.

显然，当 W 和 U 事件都发生时，由 KE 算法构造知 KE 输出一定为真，则

$$\Pr[\text{Fail}] = \Pr[\text{Fail} \mid \overline{U}]\Pr[\overline{U}] + \Pr[\text{Fail} \mid \overline{W} \wedge U]\Pr[\overline{W} \wedge U] + \Pr[\text{Fail} \mid W \wedge U]\Pr[W \wedge U] \leqslant 1/2^{\lambda} + q_E\delta + 1/2^s$$

由 KE 算法的执行过程知 KE 的时间复杂度为 $q_K t$.

引理 2　公钥加密机制 ECIIES 是 IND-CPA 安全的.

证明： 攻击者在 CPA 攻击下不能访问解密机，此时攻击者攻击 ECIES，就是攻击基本的 Elgamal 机制，而 Elgamal 机制已被证明是 IND-CPA 安全的[13].

定理 1　随机模型下，公钥加密机制 ECIIES 是明文知晓的，从而是 IND-CCA2 安全的.

证明： 由引理 1 和引理 2 可知 ECIIES 是明文知晓的，从而根据定理[14]知是 IND-CCA2 安全的.

4　结束语

作者对能抵抗量子计算机的数学问题和密码系统进行了研究，提出了椭圆曲线同源星上的搜索计算问题. 基于此数学问题设计了一个公钥密码机制 ECIIES，并在随机模型下证明了 ECIIES 是 IND-CCA2 安全的. 本文的构造方法和安全性证明方法同样可以在基于其他数学难题的密码机制构造和安全性证明中发挥很大的作用.

参考文献：

[1] BONEH D, LIPTON R. Quantum cryptanalysis of hidden linear functions [C] // Proceedings of the 15th Annual International Cryptology Conference on Advances in Cryptology (LNCS 963). London: Springer-Verlag, 1995: 424-437.

[2] JEFF J, JILL P, SILVERMAN J H. NTRU: a new high speed public key cryptosystem [C] // Proc of ANTS III. Berlin: Springer-Verlag, 1998: 267-288.

[3] NICK H. A hybrid lattice-reduction and meet-in-the-middle attack against ntru [C] // Advances in Cryptology-CRYPTO2007

(LNCS 4622). Berlin: Springer-Verlag, 2007: 150-169.

[4] JEFF J, NICK H, JILL P, et al. Practical lattice-based cryptography: ntruencrypt and ntrusign [EB/OL]. [2007-07-01]. http://www.ntru.com/cryptolab/pdf/lll25.pdf.

[5] MENEZES A J, VANSTONE S A, van OORSCHOT P C. Handbook of applied cryptography [M]. [S.l.]: CRC Press, 1996: 298-299.

[6] PATARIN J. Asymmetric cryptography with a hidden monomial [C] //Proceedings of the 16th Annual International Cryptology Conference on Advances in Cryptology (LNCS 1109). London: Springer-Verlag, 1996: 45-60.

[7] KASSEL C, TURAEV V. Braid groups [M]. [S.l.]: Springer, 2008: 1-40.

[8] ROSTOVTSEV A, STOLBUNOV A. Public-key cryptosystem based on isogenies [EB/OL]. [2006-05-29]. http://eprint.iacr.org/.

[9] KOHEL D. Endomorphism rings of elliptic curves over finite fields [D]. Berkeley: University of California, 1996: 2-3.

[10] COUVEIGNES J M, DEWAGHE L, MORAIN F. Isogeny cycles and the schoof-elkies-atkin algorithm [EB/OL]. [1996-04-26]. http://www.lix.polytechnique.fr/Labo/Francois.Morain/.

[11] GALBRAITH S. Constructing isogenies between elliptic curves over finite fields [J]. Journal of Computational Mathematics, 1999, 2: 118-138.

[12] FUJISAKI E, OKAMOTO T. How to enhance the security of public-key encryption at minimum cost [C] //Public Key Cryptography - PKC 1999 (LNCS 1560). Berlin: Springer-Verlag, 1999: 53-68.

[13] TSIOUNIS Y, YUNG M. On the security of ElGamal based encryption [C] // PKC'98 (LNCS 1431). Berlin: Springer-Verlag, 1998: 117-134.

[14] BELLARE M, DESAI A, POINTCHEVAL D, et al. Relations among notions of security for public-key encryption schemes [C] //Advances in Cryptology-CRYPTO'98 (LNCS 1462). Berlin: Springer-Verlag, 1998: 26-45.

Public-key Cryptosystem Based on Elliptic Curve Isogenies

HU Jin, HE De-biao, CHEN Jian-hua, HUANG Yin

(School of Mathematics and Statistics, Wuhan University, Wuhan 430072, China)

Abstract: To the question of the mathematical problems of RSA public-key cryptosystem and elliptic curve cryptosystem can't be against quantum computer, a mathematical problem, suitable for constructing public-key cryptosystem, is proposed: computing an isogeny between the given elliptic curves. The computational complexity for solving this problem is exponential. The problem is hard for solving with a quantum computer. A public-key cryptosystem scheme named ECIIES is proposed for an isogeny crypto system. ECIIES which based on the basic Elgamal scheme, can be against chosen ciphertext attacks by using a MAC function about intermediate variables and ciphertext. At last, the scheme ECIIES is proved to be IND-CCA2 security in the random oracle model.

Key words: public-key cryptosystem; quantum computer; isogeny; elliptic curve; chosen ciphertext attack; random oracle

(责任编辑 梁 洁)