Cryptanalysis of ElGamal type encryption schemes based on conic curves

Zong-Duo Dai, Ding-Feng Ye, Ding-Yi Pei and
Jun-Hui Yang

It is shown that the security of the ElGamal type encryption scheme based on a conic over $GF(p)$ is not stronger than that based on $GF(p^2)^*$.

Introduction: Both the ElGamal encryption scheme [1, 2] and the Diffie-Hellman key agreement protocol [2 – 4], and those of the same type, can be carried out in any finite group in which both the discrete logarithm problem (DLP) is hard and the group operation is relatively efficient. The most common examples of such groups used in practice are the multiplicative group $GF(q)^*$ of the finite field $GF(q)$ ($q = p^m$ and p is a prime) and the elliptic curve group (ECG) over a finite field. Along this line, a conic curve group (CCG) over the finite field $GF(p)$, $p > 2$, is suggested [5] to make both a new ElGamal type encryption scheme and a new Diffie-Hellman type key agreement protocol. We notice that the operation of a CCG is simpler than that of an ECG, and that it appears that the general techniques, such as the index calculus algorithm for solving the DLP of a finite field, could not be applied in solving the DLP of a CCG (where it is hard to define a 'factor base'). If the DLP of a CCG was as hard as that of a ECG, the conic curves would be the better candidates for cryptographic applications. Unfortunately, as demonstrated in this Letter, any conic curve group over $GF(p)$ ($p > 2$) is isomorphic to the subgroup of $GF(p^2)^*$ of order $p - 1$ or $p + 1$ and the isomorphism is given by an explicit simple formula. Consequently, the security of both the ElGamal type encryption scheme and the Diffie-Hellman type key agreement protocol based on a conic over $GF(p)$ [5] is not stronger than that based on $GF(p^2)^*$.

Conic curve groups: The conic curve $C(a, b)$ [6] over $GF(p)$ is the solution set in the affine space $GF(p)^2$ of the equation $y^2 = ax^2 - bx$, where a and b are elements in $GF(p)$ and $ab \neq 0$. It is known that

$$C(a,b) = \left\{P(t) = \left(\frac{b}{a-t^2}, \frac{bt}{a-t^2}\right) \mid t \in GF(p), t^2 \neq a\right\} \cup \{P(\infty) = (0,0)\}$$

One may identify the point $P(t)$ to t, and $P(\infty)$ to 0. The conic $C(a, b)$ becomes an abelian group under the operation $\oplus$ as below:

$$t_1 \oplus t_2 = \begin{cases} \frac{t_1 t_2 + a}{t_1 + t_2} & t_1 + t_2 \neq 0 \\ O & t_1 + t_2 = 0 \end{cases}$$

$$O \oplus O = O \qquad O \oplus t = t \oplus O = t \quad \forall t \in C(a,b)$$

Theorem (i): For any given conic curve $C(a, b)$ over $GF(p)$ ($p > 2$), let $\theta \in GF(p^2)$ be a given root of $x^2 - a = 0$ and set

$$\phi(O) = 1 \qquad \phi(t) = \frac{t+\theta}{t-\theta} \quad \forall t \in C(a,b) - \{O\}$$

Then ϕ is a group isomorphism from $C(a, b)$ onto G_ε, where $\varepsilon = -1$ if a is a square element in $GF(p)$, and $\varepsilon = 1$ otherwise; G_ε is the subgroup of $GF(q^2)^*$ of order $q + \varepsilon$.

Proof of theorem (i): By definition, $t \in C(a, b)\backslash\{O\}$ implies $t \neq \theta$. So the map ϕ is well defined. For any $t_1, t_2 \in C(a, b)\backslash\{O\}$, we have

$$\phi(t_1)\phi(t_2) = \frac{(t_1+\theta)(t_2+\theta)}{(t_1-\theta)(t_2-\theta)} = \frac{t_1 t_2 + (t_1+t_2)\theta + a}{t_1 t_2 - (t_1+t_2)\theta + a}$$
$$= \begin{cases} \frac{t_1 \oplus t_2 + \theta}{t_1 \oplus t_2 - \theta} & \text{if } t_1 + t_2 \neq 0 \\ 1 & \text{if } t_1 + t_2 = 0 \end{cases} = \phi(t_1 \oplus t_2)$$

which shows that ϕ is a group homomorphism. Since

$$\phi(t) = \frac{t+\theta}{t-\phi} \neq 1 \quad \forall t \in C(a,b) - \{O\}$$

we can conclude that ϕ is an isomorphism. Note that $|C(a, b)| = q + \varepsilon$, so the image of $C(a, b)$ under ϕ is G_ε.

Conclusion: By Theorem (i), we know that the DLP in the $C(a, b)$ over $GF(p)$ ($p > 2$) can be reduced to the DLP of $GF(p)^*$ or $GF(p^2)^*$ easily. As a consequence, the security of both the ElGamal type encryption scheme and the Diffie-Hellman type key agreement protocol based on a conic over $GF(p)$ is not stronger than that based on the multiplicative group $GF(p^2)^*$.

12 December 2000
Electronics Letters Online No: 20010272
DOI: 10.1049/el:20010272

Zong-Duo Dai, Ding-Feng Ye and Ding-Yi Pei (*State Key Laboratory of Information Security, Department of Mathematics, Graduate School, University of Science and Technology of China, 100039-08, Beijing, People's Republic of China*)

E-mail: yangdai@mimi.cnc.ac.cn

Jun-Hui Yang (*Institute of Software, Academia Sinica, 100080, Beijing, People's Republic of China*)

References

1 ELGAMAL, T.: 'A public key cryptosystem and a signature scheme based on discrete logarithms', *IEEE Trans. Inf. Theory*, 1985, **31**, pp. 469–472

2 MENEZES, A.J., VAN OORSCHOT, P.C., and VANSTONE, S.A.: 'Handbook of applied cryptography' (CRC Press, 1996)

3 DIFFIE, W., and HELLMAN, M.E.: 'Multiuser cryptographic techniques'. Proc. AFIPS National Computer Conf., 1976, pp. 109–112

4 DIFFIE, W., and HELLMAN, M.E.: 'New directions in cryptography', *IEEE Trans. Inf. Theory*, 1976, **22**, pp. 644–654

5 CHAO ZHENG FU: 'A public key cryptosystem based on conic curves over finite field F_p'. ChinaCrypt'1998, Science Press, pp. 45–49

6 ZHANG MING ZHI: 'Factoring integers with conics', *J. Sichuan Univ. (Natural Science Edition)*, 1996, **33**, (4), pp. 356–359