J. Cryptology (2002) 15: 129–138
DOI: 10.1007/s00145-001-0015-6

Journal of
CRYPTOLOGY

Elliptic Curve Paillier Schemes

Steven D. Galbraith*
Computer Science Department,
University of Bristol, Merchant Venturers Building,
Woodland Road, Bristol BS8 1UB, England
steven@cs.bris.ac.uk

Communicated by Johannes Buchmann

Received January 2001 and revised June 2001
Online publication 23 November 2001

Abstract. This paper is concerned with generalisations of Paillier's probabilistic encryption scheme from the integers modulo a square to elliptic curves over rings. Paillier himself described two public key encryption schemes based on anomalous elliptic curves over rings. It is argued that these schemes are not secure. A more natural generalisation of Paillier's scheme to elliptic curves is given.

Key words. Public key cryptography, Cryptanalysis, Elliptic curves, Factoring.

1. Introduction

Paillier [9] developed a probabilistic, homomorphic public key encryption scheme based on arithmetic in the ring of integers modulo N^2 where N is a product of two large primes. This scheme has found many applications in cryptography (such as [4]). In [11] Paillier tried to generalise this scheme to the elliptic curve setting by using anomalous elliptic curves over rings. In Section 6 we show that the scheme of Section 4 of [11] is not secure, as the private key can be easily recovered from the public data. In Section 7 we argue that the scheme of Section 3 of [11] cannot be securely implemented.

The idea of using anomalous elliptic curves over rings for public key cryptosystems first appeared in Okamoto and Uchiyama [8]. Their goal was to "trapdoor" the elliptic curve discrete logarithm problem on an elliptic curve over a ring $\mathbb{Z}/N\mathbb{Z}$ where N is a product pq of primes, by using the fact that it is easy to solve the elliptic curve discrete logarithm problem on an anomalous curve over a prime field $\mathbb{F}_p$ using the methods of [12], [13] and [15]. However, Okamoto and Uchiyama realised that their attempts to build such a system were unsuccessful, in that it was possible to derive the factorisation

[*] The author thanks Hewlett-Packard Laboratories Bristol for support.

of N from the public information of their system. In general, it seems unlikely that cryptosystems based on anomalous elliptic curves over rings can be secure.

In Section 9 we describe a more natural generalisation of the original Paillier scheme to elliptic curves. The motivation behind this work is to enable elliptic curve variants of the interesting new protocols developed using Paillier's idea. Of course, the performance of cryptosystems based on elliptic curves modulo large numbers is much worse than non-elliptic curve versions of these schemes. Hence the scheme in Section 9 is mainly of theoretical interest.

2. Elliptic Curves over Rings

We recall some facts about elliptic curves over rings.

Let R be a commutative ring (with 1) and denote by R^* the set of invertible elements of R. A pair $a, b \in R$ such that $6(4a^3 + 27b^2) \in R^*$ defines an *elliptic curve* $y^2z = x^3 + axz^2 + bz^3$. The set of R-valued points of the elliptic curve is denoted by $E(R)$ and is defined (see [7]) to be the set of equivalence classes of points $(x : y : z)$ such that $x, y, z \in R$, $y^2z = x^3 + axz^2 + bz^3$ and such that the ideal generated by x, y, z is R (and where the equivalence relation is $(x : y : z) \sim (x' : y' : z')$ if and only if there exists $\lambda \in R^*$ such that $\lambda x = x'$, $\lambda y = y'$ and $\lambda z = z'$).

Suppose R satisfies the further condition that every projective R-module of rank one is free (see Section 3 of [7]). Then the usual chord and tangent operation on the set $E(R)$ provides a group law with identity element $(0 : 1 : 0)$.

Let p and q be distinct primes (this notation applies to the whole paper) and let R be a ring isomorphic to $\mathbb{F}_p \times \mathbb{F}_q$ (for instance, by the Chinese remainder theorem we can take $R = \mathbb{Z}/pq\mathbb{Z}$). Suppose that E is an elliptic curve over R. Then there are natural reduction maps from $E(R)$ to $E(\mathbb{F}_p)$ and $E(\mathbb{F}_q)$ and it follows that $E(R) \cong E(\mathbb{F}_p) \times E(\mathbb{F}_q)$.

More generally, the "Chinese remainder" (see Section II.2 of [5]) of two finite fields $\mathbb{F}_{p^n}, \mathbb{F}_{q^m}$ is a ring R which is isomorphic to $\mathbb{F}_{p^n} \times \mathbb{F}_{q^m}$. For such a ring there are natural reduction maps from $E(R)$ to $E(\mathbb{F}_{p^n})$ and $E(\mathbb{F}_{q^m})$ and we find $E(R) \cong E(\mathbb{F}_{p^n}) \times E(\mathbb{F}_{q^m})$.

Let E be the elliptic curve $y^2z = x^3 + axz^2 + bz^3$ over a ring R. For any $d \in R$ define the *quadratic twist* $E^{(d)} : y^2z = x^3 + (d^2a)xz^2 + (d^3b)z^3$.

To add points $(x_1 : y_1 : z_1)$ and $(x_2 : y_2 : z_2)$ on an elliptic curve over a ring R one can use the usual formulae when $z_1, z_2 \in R^*$. In our setting it will often happen that one of z_1 or z_2 is not invertible. One way to avoid these problems (which applies when both $y_1, y_2 \in R^*$) is to make the curves affine using the (x, z)-plane by imposing the condition $y = 1$ rather than the more usual (x, y)-plane. The elliptic curve becomes $z = x^3 + axz^2 + bz^3$ and a point $(x : y : z)$ becomes the point $(x/y, z/y)$. Points for which y is not invertible do not lie in this affine space. The identity element for the group law is now $(0, 0)$ and the inverse of a point (x_1, z_1) is $(-x_1, -z_1)$.

Explicit group formulae can easily be given. The sum of (x_1, z_1) and (x_2, z_2) when $x_1 \neq x_2$ is given by (x_3, z_3) where

$$\begin{aligned} \lambda &= (z_1 - z_2)/(x_1 - x_2), \\ x_3 &= x_1 + x_2 + (z_1 - \lambda x_1)(2a\lambda + 3b\lambda^2)/(1 + a\lambda^2 + b\lambda^3), \\ z_3 &= \lambda(x_3 + x_1) - z_1. \end{aligned}$$

To double (x_1, z_1) we obtain

$$\begin{aligned} \lambda &= (3x_1^2 + az_1^2)/(1 - 3bz_1^2 - 2ax_1z_1), \\ x_3 &= 2x_1 + (z_1 - \lambda z_1)(2a\lambda + 3b\lambda^2)/(1 + a\lambda^2 + b\lambda^3), \\ z_3 &= \lambda(x_3 + x_1) - z_1. \end{aligned}$$

These formulae are valid whenever the divisions are possible in the ring.

3. Elliptic Curves modulo N^2

We recall some fragments of the p-adic theory of elliptic curves (for further details see [14]). Let p be a prime, n a positive integer, and E an elliptic curve over $\mathbb{Z}/p\mathbb{Z}$. Define

$$E_1(\mathbb{Z}/p^n\mathbb{Z}) := \{P \in E(\mathbb{Z}/p^n\mathbb{Z})\colon\ P \text{ reduces to } (0:1:0) \text{ in } E(\mathbb{Z}/p\mathbb{Z})\}.$$

Obviously, an element $(x : y : z) \in E_1(\mathbb{Z}/p^n\mathbb{Z})$ has $p|x$, $p|z$ and $p \not| y$.

The theory of formal groups (see [14], especially Proposition VII.2.2) gives rise to a mapping $\psi\colon\ p(\mathbb{Z}/p^n\mathbb{Z}) \longrightarrow E_1(\mathbb{Z}/p^n\mathbb{Z})$ which is of the form $\psi\colon\ x \longmapsto (x : 1 : w(x))$ where

$$w(x) = x^3 + ax^7 + bx^9 + 2a^2x^{11} + 5abx^{13} + (5a^3 + 3b^2)x^{15} + 21a^2bx^{17} + \cdots.$$

The image of $p^j(\mathbb{Z}/p^n\mathbb{Z})$ under ψ is the subgroup of $E_1(\mathbb{Z}/p^n\mathbb{Z})$ given by

$$E_j(\mathbb{Z}/p^n\mathbb{Z}) = \{(x : 1 : z) \in E_1(\mathbb{Z}/p^n\mathbb{Z})\colon\ p^j|x \text{ and } p^{3j}|z\}.$$

More importantly, the map ψ has certain homomorphic properties. In fact Proposition IV.3.2 of [14] implies that the map induced by ψ is a group isomorphism from $p^j(\mathbb{Z}/p^n\mathbb{Z})/p^{j+1}(\mathbb{Z}/p^n\mathbb{Z})$ to $E_j(\mathbb{Z}/p^n\mathbb{Z})/E_{j+1}(\mathbb{Z}/p^n\mathbb{Z})$.

The group operation is not entirely as one might expect (and this is why it does not extend to the whole of $p(\mathbb{Z}/p^n\mathbb{Z})$). The sum of the points $(x_1 : 1 : w(x_1))$ and $(x_2 : 1 : w(x_2))$ is the point $(x_3 : 1 : w(x_3))$ where

$$\begin{aligned} x_3 &= (x_1 + x_2) + a(-2x_1x_2^4 - 4x_1^2x_2^3 - 4x_1^3x_2^2 - 2x_1^4x_2) \\ &\quad + b(-3x_1x_2^6 - 9x_1^2x_2^5 - 15x_1^3x_2^4 - 15x_1^4x_2^3 - 9x_1^5x_2^2 - 3x_1^6x_2) \\ &\quad + a^2(-2x_1x_2^8 + 8x_1^3x_2^6 + 16x_1^4x_2^5 + 16x_1^5x_2^4 + 8x_1^6x_2^3 - 2x_1^8x_2) + \cdots. \end{aligned} \tag{1}$$

As usual, when $N = pq$ then one can apply the Chinese remainder theorem to these results and therefore deduce that $\#E(\mathbb{Z}/N^n\mathbb{Z}) = MN^{n-1}$ where $M = \#E(\mathbb{Z}/N\mathbb{Z})$. We emphasise here that $E(\mathbb{Z}/N^n\mathbb{Z})$ is a group.

One important family of points on $E(\mathbb{Z}/N^2\mathbb{Z})$ are $P_i = (Ni : 1 : 0)$. It is not possible to use the group law formula from Section 2 to compute mP_i since the divisions are not defined. Instead, one must use (1), from which it follows that $mP_i = P_{mi}$.

Similarly, when working in $E(\mathbb{Z}/N^n\mathbb{Z})$ one has the point $P_1 = (N : 1 : w(N) = N^3 + aN^7 + \cdots)$. To compute mP_1 it is necessary to use (1), for instance $2P_1 = (2N - 12aN^5 - 54bN^7 + \cdots : 1 : (2N)^3 + \cdots)$. One can show that $N^{n-1}P_1 = (0 : 1 : 0)$.

4. Anomalous Elliptic Curves

In this section we recall the definition of an anomalous elliptic curve. In the next section we explain why it is easy to factor $N = pq$ when given an elliptic curve E over $\mathbb{Z}/N\mathbb{Z}$ which is anomalous modulo p and q.

An elliptic curve $E\colon\ y^2z = x^3 + axz^2 + bz^3$ over a field $\mathbb{F}_p$ is called *anomalous* if $\#E(\mathbb{F}_p) = p$.

Let E be an anomalous elliptic curve over $\mathbb{F}_p$ and let d be a non-square modulo p. Then the quadratic twist $E^{(d)}$ satisfies $\#E^{(d)}(\mathbb{F}_p) = p + 2$ and $\#E(\mathbb{F}_{p^2}) = \#E^{(d)}(\mathbb{F}_{p^2}) = p(p+2)$.

We now explain how to construct an elliptic curve E and primes p and q, such that E is an anomalous elliptic curve over both $\mathbb{F}_p$ and $\mathbb{F}_q$. The first step is to choose a discriminant $D < 0$, $D \equiv 1 \pmod 4$ of an imaginary quadratic field of small class number (taking class number one allows E to be written with coefficients in $\mathbb{Z}$, with higher class numbers we would only store the j-invariant modulo p and q). The next step is to find suitably large primes $p = (1 - k^2D)/4$ and $q = (1 - k'^2D)/4$ where k and k' are large positive integers. The CM method [1] constructs the j-invariant (usually just modulo p and q) of an elliptic curve E whose endomorphism ring has discriminant D. Since

$$p = \frac{(1 + k\sqrt{D})}{2}\frac{(1 - k\sqrt{D})}{2}$$

it follows that the elliptic curve over $\mathbb{F}_p$ has trace $t = \pm 1$ (and similarly for q). Taking an appropriate quadratic twist (determined by trial and error) gives an elliptic curve which is anomalous over $\mathbb{F}_p$ and $\mathbb{F}_q$.

Let $N = pq$ and suppose E is an elliptic curve over $\mathbb{Z}/N\mathbb{Z}$ which is anomalous modulo p and q. Let d be an integer so that $(\frac{d}{p}) = (\frac{d}{q}) = -1$. Then $E^{(d)}(\mathbb{Z}/N\mathbb{Z}) = (p+2)(q+2)$. Taking d' such that, say, $(\frac{d'}{p}) = -(\frac{d'}{q}) = 1$ yields $E^{(d')}(\mathbb{Z}/N\mathbb{Z}) = p(q+2)$.

5. Factoring Using Elliptic Curves

Let $N = pq$ and suppose that E is an elliptic curve over $\mathbb{Z}/N\mathbb{Z}$. Let $P = (x : y : z)$ be a point of $E(\mathbb{Z}/N\mathbb{Z})$ and suppose m is a multiple of the order of P in $E(\mathbb{F}_p)$. Then $mP = (x' : y' : z') \in E(\mathbb{Z}/N\mathbb{Z})$ reduces to the point at infinity in $E(\mathbb{F}_p)$ and so $p|x'$ and $\gcd(x', N)$ yields a factorisation of N. This is the key to Lenstra's elliptic curve factoring method [6].

Consider now the case where $\#E(\mathbb{Z}/pq\mathbb{Z}) = p(q+2)$ and $N = pq$. If we take a random point $P = (x : y : z)$ on $E(\mathbb{Z}/N\mathbb{Z})$, then, with probability at least $(1 - 1/p)$, P will have order divisible by p (and not divisible by q) and so NP will yield a factorisation of N using the method shown above.

In practice one cannot find a random point P on $E(\mathbb{Z}/N\mathbb{Z})$ without knowing the factorisation of N (since if one chooses x at random one cannot take square roots and compute the corresponding y). This difficulty is solved by using addition formulae which do not require y-coordinates (see [6] or [8] for a statement of these formulae and for more discussion about factoring N in this way). Similarly one cannot check that a given value corresponds to the x-coordinate of a point on $E(\mathbb{F}_p)$, but this will be true with probability roughly 1/2.

More generally, if E is an elliptic curve over $\mathbb{Z}/N\mathbb{Z}$, then knowledge of $\#E(\mathbb{Z}/N\mathbb{Z})$ is polynomial-time equivalent to knowledge of the factorisation of N.

6. Paillier's Third Encryption Scheme

The third scheme of Paillier (Section 4 of [11]) concerns an elliptic curve E over $\mathbb{Z}/pq\mathbb{Z}$ which is the quadratic twist of an anomalous curve over $\mathbb{F}_p$ and $\mathbb{F}_q$. Thus, writing $N = pq$, $\#E(\mathbb{Z}/N\mathbb{Z}) = (p+2)(q+2)$.

Paillier claims that $\#E(R) = (p+2)(q+2)pq$ where $R = \mathbb{Z}/N^2\mathbb{Z}$. This is true, due to the p-adic theory discussed in Section 3. The argument given by Paillier relies on Hasse's theorem, but this would apply only if the ring R were taken to be isomorphic to $\mathbb{F}_{p^2} \times \mathbb{F}_{q^2}$. One construction for such a ring which does not seem to leak the factorisation of N is to take an integer d such that $(\frac{d}{p}) = (\frac{d}{q}) = -1$ and define $R = (\mathbb{Z}/N\mathbb{Z})[t]/(t^2 - d)$.

In either case there is a natural inclusion from $\mathbb{Z}/N\mathbb{Z}$ to R and, since E is defined over $\mathbb{Z}/N\mathbb{Z}$, so $E(\mathbb{Z}/N\mathbb{Z})$ can be viewed as a subgroup of $E(R)$.

For this scheme the public data is the modulus N and the coefficients a and b of the elliptic curve E over $\mathbb{Z}/N\mathbb{Z}$. The public data also includes a point $G \in E(R)$ which has order divisible by N. The cryptosystem is based on the fact that the owner of the secret key $\{p, q\}$ knows the group order and thus can map elliptic curve points into the N-torsion subgroup. The discrete logarithm problem is then easily solved using the anomalous curve methods.

It is possible to recover the factorisation of N efficiently from the public data using the same technique as that used by Okamoto and Uchiyama [8, Section 4]. We give a sketch of the method (see Section 5 for details): Take random quadratic twists $E^{(d_j)}$ of E and random values $x_i \in \mathbb{Z}/N\mathbb{Z}$. With probability approximately $1/2$ the curve $E^{(d_j)}$ is anomalous modulo one of the primes (say p_j) and not anomalous modulo the other, and with probability approximately $1/2$ the value x_i is an x-coordinate of a point on $E^{(d_j)}(\mathbb{F}_{p_j})$. One then simply pretends that there is a point $P_i = (x_i : \star : 1)$ in $E^{(d_j)}(\mathbb{Z}/N\mathbb{Z})$ and computes NP_i using the addition formulae which only require x-coordinates. In the good case (which occurs with probability approximately $1/4$) the addition algorithm produces an x-coordinate which has a non-trivial and proper common divisor with N.

7. Paillier's Second Encryption Scheme

The scheme of Section 3 of [11] concerns an elliptic curve E over $\mathbb{Z}/pq\mathbb{Z}$ which is the twist of an anomalous curve over $\mathbb{F}_p$. Paillier selects the other prime q randomly (so E is just a "random" elliptic curve over $\mathbb{F}_q$ and is assumed to have no special properties) and defines $N = p^2q$. The public key includes the elliptic curve E and the integer N. Paillier claims that $\#E(R) = (p+2)p\#E(\mathbb{F}_q)$ where $R = \mathbb{Z}/p^2q\mathbb{Z}$. This is true, but again the fact follows from p-adic theory rather than from Hasse's theorem. Taking a quadratic twist where $(\frac{d}{p}) = -1$ yields $\#E^{(d)}(\mathbb{Z}/p^2q\mathbb{Z}) = p^2\#E^{(d)}(\mathbb{Z}/q\mathbb{Z})$ and so $E^{(d)}$ can be used to factor N.

This attack could be avoided by using a ring R which is isomorphic to $\mathbb{F}_{p^2} \times \mathbb{F}_q$. However, I do not know of any description of such a ring which does not leak the factorisation of $N = p^2q$.

Suppose instead that one takes $R = \mathbb{Z}/(pq)^2\mathbb{Z}$ or R isomorphic to $\mathbb{F}_{p^2} \times \mathbb{F}_{q^2}$ (one can use the construction for R given in the previous section). One then has $\#E(R) = (p+2)pM$ (where M is $\#E(\mathbb{Z}/q^2\mathbb{Z})$ or $\#E(\mathbb{F}_{q^2})$ depending on the definition of R) and Paillier's protocol can be applied in this setting. However, it is still possible to factor $N = pq$ by working with random quadratic twists of E over $\mathbb{Z}/N\mathbb{Z}$ as discussed above.

8. Generalisations

The attack used in Section 6 relies on the fact that the elliptic curve E is defined over the subring $\mathbb{Z}/N\mathbb{Z}$ of $R = (\mathbb{Z}/N\mathbb{Z})[t]/(t^2-d)$ and so we can consider the group $E(\mathbb{Z}/N\mathbb{Z})$. If E could be taken so that it is always defined over the full ring R (i.e., so that $j(E) \in R$ and $j(E) \notin \mathbb{Z}/N\mathbb{Z}$), then the attack would fail.

However, the following lemma shows that the attack described in this paper cannot be avoided in this manner.

Lemma 1. *Let E be an elliptic curve over $\mathbb{F}_{p^2}$ such that $\#E(\mathbb{F}_{p^2}) = p(p+2)$. Then $j(E) \in \mathbb{F}_p$.*

Proof. The trace of Frobenius for $E(\mathbb{F}_{p^2})$ is $t = 1-2p$. Write $\Delta = t^2 - 4p^2 = 1-4p$, $K = \mathbb{Q}(\sqrt{\Delta})$, $\pi = (1+\sqrt{\Delta})/2$, and suppose $\mathcal{O}_K$ is the maximal order of K. The endomorphism ring of E is isomorphic to some order $\mathcal{O}$ such that $\mathbb{Z}[\pi] \subseteq \mathcal{O} \subseteq \mathcal{O}_K$.

The prime ideal (p) splits in $\mathcal{O}$ as $(p) = (\pi)(\bar{\pi})$ and the order $\mathbb{Z}[\pi]$ has conductor coprime to p. Since (π) is a principal ideal, it follows from the theory of complex multiplication (see Theorem 3, Chapter 13 of [2]) that the Frobenius automorphism fixes the j-invariant of E. In other words, $j \in \mathbb{F}_p$. □

We remark that the above result is not necessarily valid for other elliptic curves such that $\#E(\mathbb{F}_{p^2}) = (p+1-t)(p+1+t)$ when $t \neq \pm 1$.

9. The Elliptic-Curve-Based Paillier Scheme

In this section we give a very natural generalisation of the probabilistic, homomorphic public key encryption scheme of [9] to elliptic curves over rings.

Each user chooses a modulus $N = pq$ as a product of two odd primes (of course, multiprime variants are also possible). Users then choose a random elliptic curve $E\colon y^2z = x^3 + axz^2 + bz^3$ over $\mathbb{Z}/N\mathbb{Z}$ (i.e., $\gcd(N, 6(4a^3+27b^2)) = 1$).

Let $M = \operatorname{lcm}(\#E(\mathbb{F}_p), \#E(\mathbb{F}_q))$. This number can be computed in polynomial time using the Schoof–Atkin–Elkies algorithm when p and q are known. As mentioned in Section 5, knowledge of M is polynomial-time equivalent to knowledge of the factorisation of $N = pq$.

Another approach would be to construct E, p and q together, using the CM method [1]. This would involve choosing the primes p and q to have a certain form (and care would have to be taken that the system is still secure).

The user also requires a point $Q = (x : y : z)$ which has order dividing M in $E(\mathbb{Z}/N^2\mathbb{Z})$. This point can be found by taking a random point $Q' = (x' : y' : z')$ and setting $Q = NQ'$.

The public information for a user is the number N, the coefficients (a, b) of the elliptic curve, and the point Q. The secret key is the order M of the group $E(\mathbb{Z}/N\mathbb{Z})$.

To encrypt a message one first obtains certified copies of the public parameters of the recipient. Assume there is a standard way to interpret the message as an element $m \in \mathbb{Z}/N\mathbb{Z}$. The encryption algorithm is to choose a random integer $1 \leq r < N$, compute the point

$$S = rQ + P_m$$

and send it to the desired recipient. Recall that $P_m = (mN : 1 : 0)$.

To decrypt the message the owner of the secret key M computes $MS = r(MQ) + MP_m = P_{mM} = (mMN : 1 : 0)$. Given the x-coordinate one can divide by N and multiply by the inverse of M modulo N to recover $m \in \mathbb{Z}/N\mathbb{Z}$.

The security analysis of the elliptic curve scheme is very similar to that in [9]. This is discussed further in Section 11. A significant difference between our scheme and those of [11] is that the elliptic curve E is chosen completely at random and so the elliptic curve itself does not give any extra information to an adversary which would help to factorise N.

One of the most useful properties of this scheme (and that of [9]) is the homomorphic property: if S_1 is an encryption of m_1 and S_2 is an encryption of m_2, then $(S_1 + S_2)$ is an encryption of $(m_1 + m_2)$.

10. Example

Let E: $y^2z = x^3 + xz^2 - 6z^3$ be an elliptic curve over $\mathbb{Q}$. Write $N = 17 \cdot 19 = 323$. Then $\#E(\mathbb{F}_{17}) = 20$ and $\#E(\mathbb{F}_{19}) = 22$ so $M = 220$. Consider the point $Q' = (2 : 2 : 1) = (1 : 1 : 52165) \in E(\mathbb{Z}/N^2\mathbb{Z})$. The public key also comprises the point $Q = NQ' = (54136 : 1 : 5949)$.

To encrypt the message $m = 23$ we take a random number r (in this case, $r = 57$) and compute

$$S = rQ + P_{23} = (18358 : 1 : 8804) + (23N : 1 : 0) = (61963 : 1 : 72758).$$

To decrypt the ciphertext S, the owner of the secret key $M = 220$ computes MS which is equal to $(215N : 1 : 0)$. The message is recovered by computing $215M^{-1} \equiv 23 \pmod{N}$.

11. Security

The semantic security of the elliptic curve Paillier scheme (in the case of passive adversaries) depends on the hardness of the following problem: given a point $Q \in E(\mathbb{Z}/N^2\mathbb{Z})$

of order dividing $\#E(\mathbb{Z}/N\mathbb{Z})$ and given a random point $S \in E(\mathbb{Z}/N^2\mathbb{Z})$ determine whether S lies in the subgroup generated by Q.

If the group order is known (equivalently, if the factorisation of N is known), then one can check whether MS is zero or not. This gives a method to solve the problem in the case that there is no large prime dividing the order of Q whose square divides the order of the group $E(\mathbb{Z}/N^2\mathbb{Z})$.

There does not seem to be any other obvious approach to solving this problem for general E and N. However, we do not have any argument that breaking the cryptosystem is as hard as factoring (such a statement is not known for the original Paillier scheme [9] either).

It is often possible for the user to construct the point Q to have rather small order, in which case the scheme would not have good security. For some applications it may be desirable for users to prove that their public parameters have been chosen at random.

One could make the security rely on a slightly more general problem by changing the cryptosystem as follows. Instead of the point Q being part of the public key one could demand that the encryptor choose some point $Q' \in E(\mathbb{Z}/N^2\mathbb{Z})$ at random and then compute $Q = NQ'$ as part of the encryption process. There are various problems with this approach. The main problem is that it is impossible to find a point Q' without knowledge of the factorisation of N as one must solve polynomial equations. This problem can be avoided by using addition formulae which only require x-coordinates (see Section 5 for more details). Another problem is that the encryption operation would be less efficient. In any case, if the elliptic curve E is chosen randomly, then the group $E(\mathbb{Z}/N\mathbb{Z})$ is likely to be cyclic (at least, apart from some small primes) and so the “more general problem” is actually not so different to the one we stated above.

There are standard methods to obtain more robust security properties (such as semantic security against an adaptive chosen ciphertext attack) from a semantically secure encryption scheme. See [10] for further details in this context.

It is trivial to show that the powerful bit security results of Catalano et al. [3] apply to the elliptic curve setting.

12. Generalisations

Damgård and Jurik [4] have given a generalisation of Paillier’s original scheme which uses higher powers of N. There are certain advantages to this approach and it is natural to give a similar generalisation in the elliptic curve case.

The basic process is the same: one considers elliptic curves over $\mathbb{Z}/N^n\mathbb{Z}$ with $n \geq 3$. However, the generalisation is not entirely trivial due to subtleties relating to the formal group.

The special point P_1 is now of the form $(N : 1 : N^3 + aN^7 + \cdots)$ where we take terms in the z-coordinate until the degree is greater than n. The encryption and decryption processes are a little more subtle in this case since there is not an isomorphism between $E_1(\mathbb{Z}/N^n\mathbb{Z})$ and $\mathbb{Z}/N^{n-1}\mathbb{Z}$. For encryption (i.e., to compute mP_1) one must use the formal group law (see (1)).

For decryption it is necessary to recover the message m gradually in terms of its base-N representation. This can be done iteratively as follows: Given a point $(x : y : z) = mP_1$

one can determine the value of m modulo N as $m_0 = (x/N) \pmod{N}$. One can then subtract $m_0 P_1$ (again, using (1) to compute this) to obtain a new point $(x : y : z)$. From this we can recover $m_1 = (x/N^2) \pmod{N}$ and the process is iterated.

13. Example

We give an example of the generalised method. We use the same parameters (e.g., $N = 323$ and $(a, b) = (1, -6)$) used in the original example except this time we work modulo N^8.

The point $(1 : 1 : 52165)$ lifts to $Q' = (1 : 1 : 59236608128974169041)$ in $E(\mathbb{Z}/N^8\mathbb{Z})$. This gives

$$Q = N^7 Q' = (18303714591156039953 : 1 : 55196583021208274577).$$

The public key also includes the point $P_1 = (N : 1 : N^3 + N^7)$.

To encrypt the message $m = 23 + 2N + 3N^2 + 5N^3 + 7N^4 + 5N^5 + 3N^6 = 737004660916410454 \in \mathbb{Z}/N^7\mathbb{Z}$ one must compute mP_1 using (1). This gives $mP_1 = (44828281409610407073 : 1 : 110845145481572967958)$. We now construct the ciphertext (with random value $r = 57$ again)

$$S = 57Q + mP_1 = (23604029167550350628 : 1 : 44212819685579361133).$$

To decrypt we multiply by $M = 220$ to get

$$S' = 220S = (37521586473075957168 : 1 : 36700387693963393941).$$

It follows that $S' = 220mP_1$. Multiplying by 95031991650760699, which is $220^{-1} \pmod{N^7}$, gives

$$S'' = (220^{-1})S = (44828281409610407073 : 1 : 110845145481572967958).$$

The first part of the message may now be read directly from the x-coordinate

$$44828281409610407073/N = 23 + 2N + 3N^2 + 5N^3 + 12750860N^4$$

but we cannot recover the whole message due to the form of the map ψ of Section 3. Instead, we may subtract $(23 + 2N + 3N^2 + 5N^3)P_1$ from S'' to obtain the point $(11060729055798888387 : 1 : 0)$ where the x-coordinate in this case is $N^5(7 + 5N + 3N^2)$. Hence the full message has been recovered.

Acknowledgments

I thank Florian Hess and the anonymous referee for their thorough and careful reading of the paper. I also thank Ivan Damgård for very helpful comments about the elliptic curve scheme.

References

[1] A. O. L. Atkin and F. Morain, Elliptic curves and primality proving, *Math. Comp.*, **61** (1993), 29–67.

[2] J. W. S. Cassels and A. Frölich, *Algebraic Number Theory*, Proceedings of the Brighton Conference, Academic Press, New York, 1967.

[3] D. Catalano, R. Gennaro and N. Howgrave-Graham, The bit security of Paillier's encryption scheme and its applications, in B. Pfitzmann (ed.), *Eurocrypt* 2001, LNCS 2045, Springer-Verlag, Berlin, 2001, pp. 229–243.

[4] I. B. Damgård and M. J. Jurik, A generalisation, a simplification and some applications of Paillier's probabilistic public-key system, in K. Kim (ed.), *Proc. of Public Key Cryptography* 2001, LNCS 1992, Springer-Verlag, Berlin, 2001.

[5] S. Lang, *Algebra*, 3rd edition, Addison-Wesley, Reading, MA, 1993.

[6] H. W. Lenstra, Jr., Factoring integers with elliptic curves, *Ann. of Math.*, **126** (1987), 649–673.

[7] H. W. Lenstra, Jr., Elliptic curves and number theoretic algorithms, *Proc. International Congr. Math.*, Berkeley, CA, 1986, AMS, Providence, RI, 1988, pp. 99–120.

[8] T. Okamoto and S. Uchiyama, Security of an identity-based cryptosystem and the related reductions, In K. Nyberg (ed.), *Eurocrypt* '98, LNCS 1403, Springer-Verlag, Berlin, 1998, pp. 546–560.

[9] P. Paillier, Public-key cryptosystems based on composite degree residuosity classes, in J. Stern (ed.), *Eurocrypt* 1999, LNCS 1592, Springer-Verlag, Berlin, 1999, pp. 223–238.

[10] P. Paillier and D. Pointcheval, Efficient public-key cryptosystems provably secure against active adversaries, in K. Y. Lam et al. (eds.), *Asiacrypt* '99, LNCS 1716, Springer-Verlag, Berlin, 1999, pp. 165–179.

[11] P. Paillier, Trapdooring discrete logarithms on elliptic curves over rings, in T. Okamoto (ed.), *Asiacrypt* 2000, LNCS 1976, Springer-Verlag, Berlin, 2000, pp. 573–584.

[12] T. Satoh and K. Araki, Fermat quotients and the polynomial time discrete logarithm algorithm for anomalous elliptic curves, *Comment. Math.*, **47**(1) (1998), 81–92.

[13] I. Semaev, Evaluation of discrete logarithms in a group of p-torsion points of an elliptic curve in characteristic p, *Math. Comp.*, **67** (1998), 353–356.

[14] J H. Silverman, *The Arithmetic of Elliptic Curves*, GTM 106, Springer-Verlag, New York, 1986.

[15] N. P. Smart, The discrete logarithm problem on elliptic curves of trace one, *J. Cryptology*, **12**(3) (1999), 193–196.