An efficient semantically secure elliptic curve cryptosystem based on KMOV scheme

David Galindo, Sebastià Martín, Paz Morillo and Jorge L. Villar

Dep. Matemàtica Aplicada IV. Universitat Politècnica de Catalunya
Campus Nord, c/Jordi Girona, 1-3, 08034 Barcelona
e-mail: {dgalindo,sebasm,paz,jvillar}@mat.upc.es

March 26, 2002

Abstract

We propose an elliptic curve scheme over the ring $\mathbb{Z}_{n^2}$, which is efficient and semantically secure in the standard model. There appears to be no previous elliptic curve cryptosystem based on factoring that enjoys both of these properties. KMOV scheme has been used as an underlying primitive to obtain efficiency and probabilistic encryption. Semantic security of the scheme is based on a new decisional assumption, namely, the Decisional Small-x e-Multiples Assumption. Confidence on this assumption is also discussed.

Keywords: public-key cryptography, semantic security, elliptic curves, KMOV scheme.

1 Introduction

In 1984, Goldwasser and Micali [13] defined a new security notion that any encryption scheme should satisfy, namely indistinguishability of encryptions or semantic security, and they proposed a scheme with this property. This notion informally says that a ciphertext does not leak any useful information about the plaintext, except its lenght, to a polynomial-time attacker. This security notion becomes a standard requirement for the design of new cryptosystems. Stronger security notions introduced later (e.g. non-malleability, plaintext awareness) can not be considered as general requirements since they preclude homomorphic encryption.

Recently, some new semantically secure cryptosystems have been introduced by Paillier [22] in 1999 and by Catalano et al. [6] in 2001. Both schemes are defined over the ring $\mathbb{Z}_{n^2}$. Paillier's scheme is the first homomorphic and semantically secure cryptosystem based on a trapdoor permutation. It has attracted

the attention of the cryptographic community and several works have generalised and applied Paillier's result. In this way, Catalano et al. cryptosystem is a variant of Paillier's, with far improved efficiency. Besides, Catalano et al. encryption can be seen as a probabilistic encryption obtained from RSA.

Elliptic curves have been broadly used in the design of cryptosystems. Nevertheless, as far as we know, the only semantically secure elliptic curve cryptosystems based on factoring are those presented by Paillier [23] and Galbraith [12]. But, these schemes have a high computational cost, not only in encryption and decryption, but also in key generation.

In this paper we propose an efficient and semantically secure elliptic curve cryptosystem based on factoring. To our knowledge there is no previous such elliptic curve cryptosystem in the literature enjoying both properties. The design of our scheme is inspired by some techniques in [6] and uses as underlying primitive the KMOV scheme [18], that is an analogue of RSA in the elliptic curve setting.

The new proposed cryptosystem uses elliptic curves over the ring $\mathbb{Z}_{n^2}$, where n is a RSA modulus. Its semantic security is based on a new decisional assumption, namely the decisional small- x e-multiples assumption. In some sense, this assumption is analogous to the one on which Catalano et al. scheme is based.

In terms of efficiency, our proposal is only 3.75 times slower than Catalano et al. cryptosystem, at the same security level. This result is beyond the hopes for an elliptic curve cryptosystem.

The rest of the paper is organised as follows. Section 2 is devoted to introduce the definition and some results about elliptic curves. Section 3 briefly recalls the schemes our cryptosystem is related to. In section 4, we describe the new scheme and prove it is semantically secure under a new assumption. Then, we argue why one should be confident on this new assumption. In section 5, we propose a variant of the scheme. The computational cost of the new scheme is discussed in section 6. Finally, section 7 contains the conclusions.

2 Some results about elliptic curves

In this section, we are going to summarize the definition and some results about elliptic curves defined over the finite field $\mathbb{Z}_p$, and over the rings $\mathbb{Z}_{p^2}$ and $\mathbb{Z}_{n^2}$, where n is an RSA modulus.

Definition 1 *Let $p > 3$ be a prime. An elliptic curve over the finite field $\mathbb{Z}_p$, denoted by $E_p(a, b)$, where $a, b \in \mathbb{Z}_p$, and $\gcd(4a^3 + 27b^2, p) = 1$, is the set of points $(x, y) \in \mathbb{Z}_p \times \mathbb{Z}_p$ such that $y^2 = x^3 + ax + b \bmod p$, together with a point $\mathcal{O}$, called the point at infinity.*

The set $E_p(a, b)$ is a group, with the usual tangent-and-chord operation. For a brief account on elliptic curves we refer to [17], for a more extensive treatment, see [27], and for an overview on elliptic curve cryptosystems, see [3, 5, 20].

Elliptic curves can be also defined on the projective plane $\mathbb{P}^2(\mathbb{Z}_p)$ as the set of points $(x : y : z) \in \mathbb{P}^2(\mathbb{Z}_p)$ satisfying $y^2z = x^3 + axz^2 + bz^3 \bmod p$, and $\gcd(x, y, z, p) = 1$. In particular, the point $(0 : 1 : 0)$ corresponds to the point at infinity $\mathcal{O}$. According to [12], this definition can be extended to the ring $\mathbb{Z}_{p^2}$. The natural map

$$\pi_p : E_{p^2}(a, b) \to E_p(a, b)$$

is a surjective group morphism whose kernel is the set $\{O_k = (kp : 1 : 0), k \in \mathbb{Z}_p\}$, called the set of points at infinity. $E_{n^2}(a, b)$ can be defined from the natural surjective maps from $E_{n^2}(a, b)$ to $E_{p^2}(a, b)$ and $E_{q^2}(a, b)$. Via the Chinese Remainder Theorem $E_{n^2}(a, b)$ can be seen as a group isomorphic to $E_{p^2}(a, b) \times E_{q^2}(a, b)$. Points on curves $E_{n^2}(a, b)$ can be classified in three types:

- Points at infinity: $O_k = (kn : 1 : 0), k \in \mathbb{Z}_n$,
- Affine points: $(x : y : 1) \in E_{n^2}(a, b)$.
- Semi-infinite points: $(x : y : z) \in E_{n^2}(a, b)$, with $\gcd(z, n) = p$ or q.

The usual tangent-and-chord formulas do not always allow to perform addition of affine points on $E_{n^2}(a, b)$, since computation of inverses modulo n^2 is required. In practice, though, those formulas can be used, because the probability of finding a non-invertible element is negligible. Otherwise, we would have a probabilistic polynomial time algorithm that would factor n with non negligible probability, which is assumed to be infeasible. From this discusion it follows that semi-infinite points will appear with negligible probability and therefore, in practice, we can just consider affine points and points at infinity.
Next, we state a property we will use later on:

Property 2 *let $P = (x, y) \in E_n(a, b)$, with $y \in \mathbb{Z}_n^*$. Then, there exists a unique $(x, y') \in E_{n^2}(a, b)$ such that $y' \equiv y \bmod n$.*

Proof: We have $y' = y + \gamma n \in \mathbb{Z}_{n^2}$, for $\gamma \in \mathbb{Z}_n$. If we assume that (x, y') belongs to $E_{n^2}(a, b)$, we obtain a unique value for γ, namely

$$\gamma = \frac{x^3 - y^2 + ax + b}{n}(2y)^{-1} \bmod n.$$

■

Finally, let us see some addition formulas for points on $E_{n^2}(a, b)$, that will be useful later. Let $P = (x, y) \in E_{n^2}(a, b)$ be an affine point, and $O_m, O_{m'} \in E_{n^2}(a, b)$ points at infinity. Then,

$$\boxed{\begin{array}{l} O_m + O_{m'} = O_{m+m'}. \\ P + O_m = (x - 2ymn, y - (3x^2 + a)mn). \end{array}}$$

3 Some previous schemes

In this section we briefly recall Paillier's scheme and some of its variants.
The original Paillier's scheme [22] is performed on the multiplicative group $\mathbb{Z}_{n^2}^*$. Paillier considers the following function:

$$\begin{array}{rcl} \mathcal{F}_g : \mathbb{Z}_n^* \times \mathbb{Z}_n & \longrightarrow & \mathbb{Z}_{n^2}^* \\ (r, m) & \longmapsto & r^n g^m \bmod n^2 \end{array}$$

where n is an RSA modulus, and g is an element of $\mathbb{Z}_{n^2}^*$ with order multiple of n. The function $\mathcal{F}_g$ is a trapdoor permutation assuming that inverting RSA$[n, n]$ is hard. To encrypt a message $m \in \mathbb{Z}_n$ with randomness $r \in \mathbb{Z}_n^*$, one computes $\mathcal{F}_g(r, m)$. The scheme is semantically secure under the *decisional n-residuosity assumption* [22].

In order to increase the efficiency of Paillier scheme, Catalano et al. [6] use a slightly different trapdoor permutation:

$$\begin{array}{rcl} \mathcal{E}_e : \mathbb{Z}_n^* \times \mathbb{Z}_n & \longrightarrow & \mathbb{Z}_{n^2}^* \\ (r, m) & \longmapsto & r^e (1 + mn) \bmod n^2 \end{array}$$

for a *small* value of e, namely $e \in \mathbb{Z}_n$ such that $\gcd(e, \lambda(n^2)) = 1$, where λ denotes Carmichael's function. The encryption scheme $\mathcal{E}_e(r, m)$ with randomness $r \in \mathbb{Z}_n^*$ is semantically secure under the *decisional small e-residues assumption* [6].

In [12], Galbraith proposes an elliptic curve Paillier scheme based on the one-way trapdoor function

$$\begin{array}{rcl} \mathcal{X}_Q : \mathbb{Z}_n \times \mathbb{Z}_n & \longrightarrow & E_{n^2}(a, b) \\ (r, m) & \longmapsto & r\#Q + O_m \end{array}$$

where $Q \in E_{n^2}(a, b)$ is a fixed point whose order is a big-enough factor of $|E_n(a, b)|$. The semantic security of the scheme $C = \mathcal{X}_Q(r, m)$ is related to the following decisional problem: given a point $Q \in E_{n^2}(a, b)$ whose order is a divisor of $|E_n(a, b)|$, and a random point $S \in E_{n^2}(a, b)$, determine whether S lies on the subgroup generated by Q. The scheme has a high computational cost, both in key generation and decryption. There exists a polynomial time algorithm ([26]) that computes this number, but it is impractical for huge n (see [14] for a more recent discussion on implementation). Moreover, Galbraith's scheme involves the computation of the multiple $r\#Q$, where r has roughly the same length as n.

Koyama et al. propose in [18] an elliptic curve RSA based scheme. They use supersingular elliptic curves of type $E_n(0, b)$, and thus avoid the problem of computing $|E_n(a, b)|$, because $|E_n(a, b)| = (p+1)(q+1)$ when $p \equiv q \equiv 2 \bmod 3$. To encrypt a message $m = (x, y) \in \mathbb{Z}_n \times \mathbb{Z}_n$, the following trapdoor one-way

function is used:

$$\begin{aligned} \mathrm{KMOV}[n,e] : \mathbb{Z}_n \times \mathbb{Z}_n &\longrightarrow \mathbb{Z}_n \times \mathbb{Z}_n \\ (x,y) &\longmapsto e\#(x,y). \end{aligned}$$

The e-multiple is computed on the elliptic curve $E_n(0,b)$, where $b = y^2 - x^3 \bmod n$. Let us observe that the elliptic curve used to perform computation is determined by the message point. We also point out that $b \notin \mathbb{Z}_n^*$ with negligible probability. The trapdoor is

$$d = e^{-1} \bmod \mathrm{lcm}(p+1, q+1),$$

since $d\#(e\#(x,y)) = (x,y)$ on $E_n(0,b)$.

In the same way as RSA$[n,e]$ with small exponent e is more efficient than Paillier's scheme, KMOV$[n,e]$ for small values of e is significantly more efficient than Galbraith's scheme. Nevertheless, RSA and KMOV schemes are not semantically secure. Our aim is to design a semantically secure elliptic curve cryptosystem that makes use of the efficiency of KMOV cryptosystem.

4 The new scheme

In this section we present a KMOV-type scheme over the ring $\mathbb{Z}_{n^2}$ which is semantically secure under a new decisional assumption, and significantly preserves the efficiency of the original scheme.

Let

$$\Omega = \{(x,y) \in \mathbb{Z}_{n^2} \times \mathbb{Z}_{n^2}^* \mid y^2 - x^3 \in \mathbb{Z}_{n^2}^*\} \quad \text{and}$$
$$\Lambda = \{(x,y) \in \mathbb{Z}_n \times \mathbb{Z}_{n^2}^* \mid y^2 - x^3 \in \mathbb{Z}_{n^2}^*\}.$$

Let us consider the function

$$\begin{aligned} \psi_e : \Lambda \times \mathbb{Z}_n &\longrightarrow \Omega \\ (x,y,m) &\longrightarrow e\#P + O_m \end{aligned}$$

where $P = (x,y)$, and the e-multiple as well as the addition are performed on $E_{n^2}(0,b)$, with $b = y^2 - x^3 \bmod n^2$.

Lemma 3 *For all e such that $\gcd(e, n(p+1)(q+1)) = 1$, ψ_e is well defined and bijective.*

The proof of this lemma is postponed to the appendix.
In the sequel we describe the proposed new scheme:

Key generation. Given $e \equiv 1, 5 \bmod 6$, (so $e \geq 5$) and a security parameter ℓ, choose at random two primes p and q with ℓ bits such that $p \equiv q \equiv 2 \bmod 3$ and

$\gcd(e, pq(p+1)(q+1)) = 1$. Then the public key is PK=(n, e), where $n = pq$, and the private key is SK=(p, q, d), where $d = e^{-1} \bmod \mathrm{lcm}(p+1, q+1)$.

Encryption. To encrypt a message $m \in \mathbb{Z}_n$ we compute $C = \psi_e(x, y, m)$, where (x, y) is randomly chosen in Λ.

Decryption. To recover the message m from

$$C = (c_x, c_y) = e\#(x, y) + O_m,$$

the randomness (x, y) is computed firstly and, afterwards, m is easily obtained from

$$O_m = C - e\#(x, y),$$

where the operations take place on the curve $E_{n^2}(0, b)$, with $b = (c_y^2 - c_x^3) \bmod n^2$. Let us see how to compute (x, y) from C. Notice that $\overline{C} = \mathrm{KMOV}[n, e](\overline{x}, \overline{y})$, where overline stands for reduction modulo n. Now, $(\overline{x}, \overline{y}) = d\#\overline{C}$ on $E_n(0, b)$, because d is the trapdoor of KMOV$[n, e]$. Since $0 \leq x < n$ and $y \in \mathbb{Z}_{n^2}^*$ we have $x = \overline{x}$ and $y = \overline{y} + kn$. Using the fact that $(x, y) \in E_{n^2}(0, b)$, we obtain $2k\overline{y}n = x^3 - \overline{y}^2 + b \bmod n^2$, and therefore

$$k = \frac{x^3 - \overline{y}^2 + b}{n}(2\overline{y})^{-1} \bmod n.$$

4.1 Semantic security

The scheme is semantically secure under the following assumption:

Decisional Small-x e-Multiples Assumption (DSMA).
Let p, q be randomly chosen ℓ-bit long primes, with $p, q \equiv 2 \bmod 3$, $n = pq$, and let e be an integer such that

$$\gcd(e, n(p+1)(q+1)) = 1.$$

The following probability distributions are polinomially indistinguishable

$$\begin{aligned} D_{\mathrm{e-multiple}} &= (n, e\#(x, y)) \quad \textit{where } (x, y) \in_{\mathrm{R}} \Lambda \\ D_{\mathrm{random}} &= (n, (x', y')) \quad \textit{where } (x', y') \in_{\mathrm{R}} \Omega. \end{aligned}$$

From now on we will be denoted by $D_1 \approx D_2$ the fact that two probability distributions D_1 and D_2 are polinomally indistinguishable.

Notice that if g is a bijection such that g and g^{-1} can be computed in probabilistic polynomial time, then $D_1 \approx D_2$ is equivalent to $g(D_1) \approx g(D_2)$.

Proposition 4 *The proposed scheme is semantically secure if and only if DSMA holds.*

Proof: Semantic security is equivalent to indistinguishability of encryptions, so we have to prove that for all $m_0 \in \mathbb{Z}_n$, the distributions

$$\begin{aligned} D_0 &= (n, e\#(x,y) + O_{m_0}) \quad \text{where } (x,y) \in_{\mathrm{R}} \Lambda\,, \quad \text{and} \\ D &= (n, e\#(x,y) + O_m) \quad \text{where } (x,y) \in_{\mathrm{R}} \Lambda,\ m \in_{\mathrm{R}} \mathbb{Z}_n. \end{aligned}$$

are polynomially indistinguishable. From the definition of sum of an affine point and a point at infinity given at the end of section 2, it is easy to see that the map

$$\begin{aligned} \Omega &\longrightarrow \Omega \\ P &\longmapsto P - O_{m_0} \end{aligned}$$

is a polynomial time bijection. Then, $D_0 \approx D$ is equivalent to

$$(n, e\#(x,y)) \approx (n, e\#(x,y) + O_{m'}), \quad \text{with } (x,y) \in_{\mathrm{R}} \Lambda,\ m' \in_{\mathrm{R}} \mathbb{Z}_n\,.$$

Note that the distribution on the left side is $D_{\mathrm{e-multiple}}$.
Besides, since $e\#(x,y) + O_{m'} = \psi_e(x,y,m')$, and ψ_e is a bijection, then D and D_{random} are identically distributed. ∎

4.2 Hardness of the Small-x e-Multiple Problems

In this subsection we argue why one should be confident on the hardness of the new decisional problem presented in this paper. In [27] (Section 3, ex. 3.7) one proves that given $Q = (x,y) \in E_p(a,b)$ and e odd, then

$$e\#Q = \left(\frac{\phi_e(x)}{\eta_e(x)^2}, \frac{\omega_e(x)}{\eta_e(x)^3} y \right) \tag{1}$$

where $\phi_e(x), \eta_e(x)$ and $\omega_e(x) \in \mathbb{Z}_p[x]$, whenever $e\#Q$ is defined. Moreover,

$$\phi_e(x) = x^{e^2} + \textit{lower order terms},$$

$$\eta_e(x)^2 = e^2 x^{e^2-1} + \textit{lower order terms},$$

and they are relatively prime polynomials in $\mathbb{Z}_p[x]$.

Thus, given $(t_1, t_2) = e\#(x_0, y_0)$, x_0 is a root of the univariate polynomial $P_e(x) = \phi_e(x) - t_1 \eta_e(x)^2 \in \mathbb{Z}_{n^2}[x]$ whose degree is e^2. Then, the DSMA is related to the difficulty of deciding if the polynomial $\phi_e(x) - t\eta_e(x)^2$, with $t \in_{\mathrm{R}} \mathbb{Z}_{n^2}$, has a root smaller than n.

Similarly, the semantic security of Catalano et al. scheme is related to the difficulty of deciding if the polynomial $x^e - t$, with $t \in_{\mathrm{R}} \mathbb{Z}_{n^2}$, has a root smaller than n. After Coppersmith's result [7], it makes sense to use the degree of the polynomial as a security parameter to compare both schemes. Therefore, our scheme with parameter e could achieve the same security level than Catalano et al. scheme with exponent e^2.

5 A variant of the proposed scheme

In this section we propose a variant of our scheme that enables to use the value $e = 3$.

Instead of working with supersingular curves of type $E_{n^2}(0, b)$, we can use the family of supersingular curves $E_{n^2}(a, 0)$ with $p \equiv q \equiv 3 \bmod 4$. If primes p, q satisfy $p, q \not\equiv -1 \bmod 12$, then 3 is a correct value for the parameter e in function

$$\begin{aligned} \psi'_e : \Lambda' \times \mathbb{Z}_n &\longrightarrow \Omega' \\ (x, y, m) &\longrightarrow e\#P + O_m \end{aligned}$$

where now

$$\Omega' = \{(x, y) \in \mathbb{Z}_{n^2}^* \times \mathbb{Z}_{n^2}^* \mid y^2 - x^3 \in \mathbb{Z}_{n^2}^*\},$$
$$\Lambda' = \{(x, y) \in \mathbb{Z}_n^* \times \mathbb{Z}_{n^2}^* \mid y^2 - x^3 \in \mathbb{Z}_{n^2}^*\}$$

and the computations take place on the curve $E_{n^2}(a, 0)$, with $a = (y^2 - x^3)x^{-1} \bmod n^2$. With this definition, the alternative scheme is defined in a completely similar way as the initial proposal, and the same results hold.

6 Efficiency analysis

We have argued it makes sense to use the degree of the polynomials $x^e - t$ and $P_e(x)$ as a security parameter to compare Catalano et al. scheme with ours. Since the degree of $P_e(x)$ is e^2, we will study the computational encryption cost of both schemes, first for the same security level e^2, and next for the same exponent e in $\mathcal{E}_e$ and ψ_e.

Since operations modulo a large number are involved, we neglect the cost of performing additions, multiplications and divisions by small integers. We will express the cost in terms of multiplications $\bmod n^2$, because modular inverses can be computed within a constant number of modular multiplications. The main cost in encryption is due to the computation of $r^e \bmod n^2$ and $e\#P \in E_{n^2}(0, b)$ respectively, and the amount of operations depends on the addition chain used. We will suppose these addition chains are obtained by using the *binary algorithm*. Doubles and addition of points on $E_{n^2}(0, b)$ are performed with the usual tangent-and-chord formulas.

We point out that $a^{-1} \bmod n^2$ can be obtained by computing $a^{-1} \bmod n$ and then performing two multiplications modulo n^2. Let c be the number of multiplications modulo n needed to compute $a^{-1} \bmod n$. Since the cost of multiplying two numbers mod n^2 is roughly the cost of 4 multiplications modulo n, we deduce that $a^{-1} \bmod n^2$ can be computed in $2 + c/4$ multiplications modulo n^2. In the table below we show bounds on the number of modular multiplications

needed to compute $\mathcal{E}_e$ and ψ_e as well as the number of products needed to reach the same security level e^2 in both encryption functions.

	Security level	Number of products in $\mathbb{Z}_{n^2}$	Exponent	Number of products in $\mathbb{Z}_{n^2}$
Catalano et al.	e^2	$4\lfloor \log_2 e \rfloor + 2$	e	$2\lfloor \log_2 e \rfloor + 2$
Our scheme	e^2	$(11 + c/2)\lfloor \log_2 e \rfloor + 5$	e	$(11 + c/2)\lfloor \log_2 e \rfloor + 5$

From the above comparison, we deduce that for the same security level, our scheme is roughly $\frac{11}{4} + \frac{c}{8}$ times slower than Catalano et al. cryptosystem. Practical implementations, suggests than the value $c = 8$ can be taken (see [4]), so our scheme would be only 3,75 times slower than Catalano et al. scheme at the same security level.

Next, we compare the computational cost of our schemes with the original Paillier's cryptosystem in the case $g = 1 + n$, which leads to the ciphertext $c = r^n(1 + mn) \bmod n^2$ for message m. The choice of g is made in order to achieve the minimal computational cost. In our scheme, we will chose the value $e = 2^8 + 1$, since it roughly leads to the high security level proposed by Catalano et al. in their paper [6]. In this case, the number of products needed to encrypt a message with our scheme is 108. Then, if we take a 1024 bits long RSA modulus n, our scheme is 17 times faster, on average, than Paillier's. However, we point out Paillier's cryptosystem has the homomorphic property, whereas ours does not.

Since our cryptosystem can be viewed as an improvement of KMOV scheme, let us briefly comment why the most known attacks on KMOV do not apply to our new scheme. In most cases these attacks extend previous successful attacks on RSA (see [2] for a recent overview). The attacks on KMOV described in [19, 1, 15] do not apply to our scheme, at least in their actual formulation, because they take advantage of KMOV scheme not being probabilistic. These attacks, to name a few, use the fact that the message and the ciphertext are points on the same curve (see [19, 1]), or use homomorphic properties when a sender encrypts the same message with different keys (as the common attack modulus in [15]).

7 Conclusions and further research

In this paper we have presented a new elliptic curve based scheme over the ring $\mathbb{Z}_{n^2}$, with n an RSA modulus. We prove that the scheme is semantically secure under a new decisional assumption. The new scheme has been designed applying to KMOV scheme techniques that are similar to those applied by Catalano et al. [6] to RSA scheme. As far as we know, this is the first proven semantically secure elliptic curve cryptosystem based on factoring that is efficient, both in key generation and in encryption/decryption procedures. Security against adaptive

chosen ciphertext attack, IND-CCA for short, can be given in the random oracle model applying the technique introduced by Pointcheval in [24]. It would be interesting to provide IND-CCA security in the standard model to Catalano et al. scheme as well as to ours. To achieve this goal, the recent work of Cramer and Shoup [8] could provide useful ideas.

Appendix: proof of Lemma 3

The following function is well defined and bijective:

$$\begin{aligned} \psi_e : \Lambda \times \mathbb{Z}_n &\longrightarrow \Omega \\ (x, y, m) &\longrightarrow e\#P + O_m \,. \end{aligned}$$

- ψ_e is well-defined.

  From the addition formula for an affine point and a point at infinity (at the very end of section 2), we deduce

  $$\psi_e(x, y, m) \in \Omega \Longleftrightarrow e\#(x, y) \in \Omega.$$

  Therefore, it suffices to prove that, if $y \in \mathbb{Z}_{n^2}^*$, then $e\#(x, y) = (x_e, y_e)$, with $y_e \in \mathbb{Z}_{n^2}^*$. For the sake of contradiction, suppose $y_e \equiv 0 \bmod p$ for a prime factor p of n. Then, the point (x_e, y_e) has order 2 on the curve $E_p(0, b)$. Since $\gcd(e, |E_p(0, b)|) = 1$, also the point (x, y) has order 2 on $E_p(0, b)$, contradicting the assumption $y \in \mathbb{Z}_{n^2}^*$.

- ψ_e is injective.

  Let us suppose $\psi_e(x, y, m) = \psi_e(x', y', m')$. Reducing this equality modulo n, we obtain $e\#(x, y) = e\#(x', y')$ on $E_n(0, b)$. Since $\gcd(e, |E_p(0, b)|) = 1$, we have the equality $(x, y) = (x', y')$ on $E_n(0, b)$. Now, taking into account that (x, y), (x', y') belong to the same curve $E_{n^2}(0, b)$, and that $0 \leq x, x' < n$, we use Property 2 to deduce $(x, y) = (x', y')$ on $E_{n^2}(0, b)$. Finally, it is easy to see that $O_m = O_{m'}$, and it follows that $m = m'$.

- ψ_e is surjective.

  Let $Q \in \Omega$, $d = e^{-1} \bmod \operatorname{lcm}(p + 1, q + 1)$, and $P = d\#Q = (x, y)$ on the curve $E_n(0, b)$. Let $P' = (x, y')$ be the point on $E_{n^2}(0, b)$ given in Property 2. Then, $e\#P' - Q$ is a point at infinity, O_m. Therefore, $Q = \psi_e(x, y', m)$.

■

References

[1] D. Bleichenbacher. On the security of the KMOV public key cryptosystems. *CRYPTO '97, LNCS* **1294** 235–248 (1997)

[2] D. Boneh. Twenty years of attacks on the RSA cryptosystem. *Notices of the AMS* **46** (2) 203–213 (1999).

[3] J. Borst. Public Key Cryptosistems using Elliptic Curves. *Master's Thesis. Technische Universiteit en Informatica* 24–26 (1997).

[4] R. P. Brent. Some Integer Factorization Algorithms using Elliptic Curves. *Australian Computer Science Comunications* 24–26 (1986) (Republished 1998).

[5] I. Blake, G. Seroussi and N. Smart. Elliptic curves in cryptography. *London Mathematical Society LNS* **265** (1999)

[6] D. Catalano, R. Gennaro, N. Howgrave-Graham and P. Q. Nguyen. Paillier's Cryptosystem Revisited.*ACM CCS '2001 ACM Press* (2001).

[7] D. Coppersmith. Finding a small root of a univariate modular equation. *EUROCRYPT '96, LNCS* **1070** 155–165 (1996).

[8] R. Cramer and V. Shoup. Universal Hash Proofs and a Paradigm for Adaptive Chosen Ciphertex Secure Public-Key Encryption. *Paper accepted at EUROCRYPT '2002.*

[9] N. Demytko. A new elliptic curve based analogue of RSA. *EUROCRYPT '93, LNCS* **765** 40–49 (1993).

[10] W. Diffie and M. E. Hellman. New directions in cryptography. *IEEE Trans. on Inf. Theory* **22** 644–654 (1976).

[11] T. ElGamal. A public key cryptosystem and a signature scheme based on discrete logarithms. *IEEE Trans. on Inf. Theory* **31** 469–472 (1985).

[12] S. Galbraith. Elliptic curve Paillier schemes. To appear in *Journal of Cryptology.*

[13] S. Golwasser and S. Micali. Probabilistic encryption. *Journal of Computer and System Sciences* **28** 270–299 (1984).

[14] T. Izu, J. Kogure, M. Noro and K. Yokoyama. Efficient Implementation of Schoof's Algorithm. *ASYACRIPT '98, LNCS* **1519** 66–79 (1998).

[15] M. Joye and J. J. Quisquater. Cryptanalysis of RSA-type cryptosystems: a visit. *Network Threats, DIMACS Series in Discr. Math. ant Th. Comp. Sci., AMS* 21–31 (1998).

[16] N. Koblitz. Elliptic Curve Cryptosystems. *Math. of Comp.* **48** 203–209 (1987).

[17] N. Koblitz. Algebraic aspects of Cryptography. *Springer, Algorithms and computations in mathematics* **3** (1998)

[18] K. Koyama, U.M. Maurer, T. Okamoto and S.A. Vanstone. New Public-Key Schemes Based on Elliptic Curves over the Ring $\mathbb{Z}_n$. *CRYPTO '91, LNCS* **576** 252–266 (1991).

[19] K. Kurosawa, K. Okada and S. Tsujii. Low exponent attack against elliptic curve RSA. *ASIACRYPT '94, LNCS* **917** 376–383 (1995).

[20] A. Menezes. Elliptic Curve Public-Key Cryptosystems. *Kluwer Academic SECS* **234** (1993)

[21] V. Miller. Use of elliptic curves in cryptography. *CRYPTO '85, LNCS* **218** 417–426 (1985).

[22] P. Paillier. Public-Key Cryptosystems Based on Composite Degree Residuosity Classes. *Advances in Cryptology-EUROCRYPT '99, Lectures Notes in Computer Science* **1592** 223–238 (1999).

[23] P. Paillier. Trapdooring discrete logarithms on elliptic curves over rings. *ASIACRYPT '00, LNCS* **1976** 573–584 (2000).

[24] D. Pointcheval. Chosen-Ciphertext Security for any One-Way Cryptosystem. *Proc. PKC '2000 LNCS* **1751** 129–146 (2000).

[25] R. Rivest, A. Shamir and L. Adleman. A method for obtaining digital signatures public-key cryptosystems. *Comm. of ACM* **21** (2) 120–126 (1978).

[26] R. Schoof. Elliptic curves over finite fields and the computation of square root mod p. *Math. of Computation* **44** (170) 483-494 (1985).

[27] J.H. Silverman. The arithmetic of elliptic curves. *Springer GTM* **106** (1986).