A Provably Secure Elliptic Curve Scheme with Fast Encryption

David Galindo[1], Sebastià Martín[1], Tsuyoshi Takagi[2] and Jorge L. Villar[1]

[1] Dep. Matemàtica Aplicada IV. Universitat Politècnica de Catalunya. Campus Nord, c/Jordi Girona, 1-3, 08034 Barcelona. {dgalindo,sebasm,jvillar}@mat.upc.es
[2] Technical Universität Darmstadt, Fachbereich Informatik, Alexanderstr.10, D-64283 Darmstadt, Germany. ttakagi@cdc.informatik.tu-darmstadt.de

Abstract. We present a new elliptic curve cryptosystem with fast encryption and key generation, which is provably secure in the standard model. The scheme uses arithmetic modulo n^2, where n is an RSA modulus, and merges ideas from Paillier and Rabin related schemes. Despite the typical bit length of n, our encryption algorithm is faster than El Gamal elliptic curve cryptosystems. The one-wayness of the new cryptosystem is as hard as factoring n while the semantic security is proved under a reasonable decisional assumption.
Two new length-preserving trapdoor permutations equivalent to factoring are also described.

Keywords: public-key cryptography, provable security, elliptic curves, fast encryption, point doubling.

1 Introduction

Several elliptic curve based cryptosystems have been proposed during the last decades. On the one hand, cryptosystems related to the elliptic curve discrete logarithm problem (such as elliptic curve versions of El Gamal) have the feature of having small keysizes, at the cost of moderate encryption/decryption times. On the other hand, cryptosystems based on elliptic curves over the ring $\mathbb{Z}_n$ have security related to the hardness of factoring $n = pq$. Therefore, their keysizes are the same as in RSA schemes while encryption/decryption times are greater. In both cases, messages are hidden by means of computing multiples of points. Thus, the computational cost depends on the size of the multiplier.

In this paper, a minimal encryption-time cryptosystem based on elliptic curves is proposed. The encryption function is related to the computation of doubles of points on elliptic curves over $\mathbb{Z}_{n^2}$, and is reminiscent of the Blum-Williams trapdoor permutation. Despite the typical size of n, the encryption algorithm is faster than in elliptic curve versions of El Gamal. Furthermore, if the encryption efficiency is measured in terms of encryption time per plaintext bit, the difference is even greater.

As done in [8], the new cryptosystem works on a family of supersingular elliptic curves. Since doubling points on elliptic curves over $\mathbb{Z}_n$ is not a bijection, the set of allowed points must be restricted to the subset D_n of doubles of points. We show that if $p \equiv q \equiv 5 \bmod 12$ then doubling points in D_n is a trapdoor permutation whose one-wayness is equivalent to factoring n.

Now, by following the ideas in [2], this bijection is lifted to $\mathbb{Z}_{n^2}$ and the definition of the new cryptosystem arises. Its semantic security is proven equivalent to a new decisional problem, that is in turn related to the existence of small roots of some polynomials. Since the best result in this area (namely [3]) does not apply to our case, the new problem is supposed to be intractable.

By taking profit of some interesting techniques, the one-wayness of the proposed cryptosystem is proved to be equivalent to factoring n.

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 propose new trapdoor permutations equivalent to factoring. In section 5, we describe the new scheme and prove that its one-wayness is based on the hardness of factoring the modulus. We also prove that the proposed scheme is semantically secure under a new assumption. Then, we argue why one should be confident on this new assumption. Finally, the computational cost of the new scheme is discussed in section 6.

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 $y^2 = x^3 + ax + b \bmod p$, 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. We will denote by $|E_p(a, b)|$ the number of elements of the group $E_p(a, b)$ and by $r\#P$ the p-th multiple of a point $P \in E_p(a, b)$. For an extensive treatment on elliptic curves we refer to [11], and for an overview on elliptic curve cryptosystems, see [10].

Elliptic curves can also be defined on the projective plane $\mathbb{P}^2(\mathbb{Z}_p)$ as the set of points $(x : y : z)$ 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 $\mathcal{O}$. Following [4], this definition can be extended to the ring $\mathbb{Z}_{p^2}$. The natural map $\pi_p : E_{p^2}(a, b) \rightarrow E_p(a, b)$ that reduces coordinates modulo p, is a surjective group morphism whose kernel is the set $\{O_m = (mp : 1 : 0) \mid m \in \mathbb{Z}_p\}$, 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 $E_{p^2}(a, b) \times E_{q^2}(a, b)$. The natural group morphism from $E_{n^2}(a,b)$ to $E_n(a,b)$ will be denoted as π_n. Points on curves $E_{n^2}(a,b)$ can be classified in three types:

- Points at infinity: $O_m = (mn : 1 : 0)$, $m \in \mathbb{Z}_n$, (the kernel of π_n)
- Affine points: $(x,y) = (x : y : 1) \in E_{n^2}(a,b)$.
- 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 allow to perform addition of affine points on $E_{n^2}(a,b)$, without knowledge of the factorisation of n. In particular, the formula to double an affine point is the following:

$$\boxed{2\#(x,y) = (\lambda^2 - 2x, -\lambda^3 + 3x\lambda - y), \text{ where } \lambda = (3x^2+a)(2y)^{-1}.}$$

To deal with points at infinity the following addition formulas are used:

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

3 Some Previous Elliptic Curve Based Schemes

In [4], Galbraith proposes an elliptic curve scheme based on the one-way trapdoor function

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

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 an RSA modulus n, an elliptic curve $E_{n^2}(a,b)$, 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. 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 [8] a (deterministic) elliptic curve RSA based scheme. They use supersingular elliptic curves of type $E_n(0,b)$, $b \in \mathbb{Z}_n^*$, and thus avoid the problem of computing $|E_n(a,b)|$, because $|E_n(0,b)| = (p+1)(q+1)$ 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:

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

where $e\#(x,y)$ stands for the e-multiple of (x,y) 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 the computation is determined by the message point. Although it is required that $b \in \mathbb{Z}_n^*$ in order to be able to perform the computation, this condition is fulfilled with overwhelming probability. For e such that $\gcd(e,(p+1)(q+1))=1$, the trapdoor is $d=e^{-1} \bmod \operatorname{lcm}(p+1,q+1)$, since $d\#(e\#(x,y))=(x,y)$ on $E_n(0,b)$.

A probabilistic version of KMOV scheme has been proposed in [6]. Basically, this scheme is a lifted version of KMOV that works on supersingular elliptic curves over $\mathbb{Z}_{n^2}$. For small values of e, KMOV$[n,e]$ as well as its lifted version are significantly more efficient than Galbraith's scheme, as shown in [6].

The optimal efficiency would be achieved using $e=2$, but in this case the map KMOV$[n,2]$ is not bijective (some points have 4 pre-images, others have none). We will overcome this inconvenience by restricting the set of points on the elliptic curves used, and using an RSA modulus $n=pq$ such that $p\equiv q\equiv 5 \bmod 12$. We will obtain a new trapdoor permutation equivalent to factoring.

4 New Trapdoor Permutations

In this section, the well-known Blum-Williams trapdoor permutation is adapted to the elliptic curve setting.

4.1 Blum-Williams Function

Let $n=pq$ be an RSA modulus with $p\equiv q\equiv 3 \bmod 4$, and let Q_n be the set of quadratic residues modulo n. The squaring function restricted to Q_n, i.e.

$$\begin{aligned}\mathcal{G}_n : Q_n &\longrightarrow Q_n\\ x &\longmapsto x^2 \bmod n\end{aligned}$$

is a trapdoor one-way permutation if factoring large numbers is unfeasible (see page 34 in [7]). Let us briefly recall how to invert $\mathcal{G}_n$, provided the factorisation of n (see [12] for a nice account on this). We first compute the numbers $f=c^{\frac{p+1}{4}} \bmod p$ and $g=c^{\frac{q+1}{4}} \bmod q$, which are the square roots of c modulo p and modulo q that are quadratic residues to their respective modulus. Then, by using the Chinese Remainder Theorem, we obtain an $s\in Q_n$ such that $s^2=c \bmod n$.

4.2 Point-Doubling Trapdoor Permutation

As in KMOV scheme, only supersingular curves $E_n(0,b)$, $b\in\mathbb{Z}_n^*$, will be considered. Thus, $p\equiv q\equiv 2 \bmod 3$. A new restriction on the prime factors of n must be introduced, in order to avoid the existence of points of order 4.

Observation 1. *If $p\equiv 5 \bmod 12$, then $|E_p(0,b)|\equiv 2 \bmod 4$, and consequently there are no points of order 4 on $E_p(0,b)$. Also, there is a unique point of order 2, namely $(\eta,0)$, where η is the unique cubic root of $-b$. This implies that given a point $P\in E_p(0,b)$, the equation $2\#\bar{P}=2\#P$ has exactly two solutions: $\bar{P}=P$ and $\bar{P}=P+(\eta,0)$, since the order of the point $\bar{P}-P$ divides 2.*

Now, the elliptic analogous to the set of quadratic residues is defined.

Definition 2. *For $n = pq$, and $p \equiv q \equiv 5 \bmod 12$, let*

$$D_n = \{2\#(x,y) \in \mathbb{Z}_n \times \mathbb{Z}_n \mid x \in \mathbb{Z}_n,\ y \in \mathbb{Z}_n^*,\ y^2 - x^3 \in \mathbb{Z}_n^*\},$$

where the double $2\#(x,y)$ is computed on the curve $E_n(0,b)$, with $b = y^2 - x^3$.

We say that $(x,y) \in \mathbb{Z}_n \times \mathbb{Z}_n^*$ is a *double* if it is in D_n. We will also consider the sets D_p and D_q defined in the same way as D_n, but using modulo p and q instead of n. From the Chinese Remainder Theorem, it is clear that $D_n = D_p \times D_q$.

Lemma 1. *If $(u,v) \in D_n$, then $v \in \mathbb{Z}_n^*$.*

Proof. Let $Q = (u,v) \in D_n$. Then, there exists a point $P = (x,y)$ on the same curve such that $Q = 2\#P$ and $y \in \mathbb{Z}_n^*$. Let us suppose that $v = 0 \bmod p$. This implies that $2\#\pi_p(Q) = O$ and then $4\#\pi_p(P) = O$. Since there are no points of order 4 on $E_p(0,b)$, we can assure that $2\#\pi_p(P) = O$. So, $y \equiv 0 \bmod p$, which is a contradiction. □

Lemma 2. $|D_p| = \frac{(p-1)^2}{2}$ *and* $|D_n| = \frac{(p-1)^2(q-1)^2}{4}$.

Proof. Let $Q \in E_p(0,b) \cap D_p$ where $b \in \mathbb{Z}_p^*$. From observation 1 it is clear that the equation $2\#P = Q$ has exactly two solution $P, \bar{P} \in E_p(0,b)$. Since there are $p-1$ affine points $P = (x,y)$ on $E_p(0,b)$ with $y \in \mathbb{Z}_p^*$, then $|E_p(0,b) \cap D_p| = \frac{p-1}{2}$. By considering the $p-1$ possible values for b, we obtain the claimed result $|D_p| = \frac{(p-1)^2}{2}$. Finally, $|D_n| = \frac{(p-1)^2(q-1)^2}{4}$ comes from $D_n = D_p \times D_q$. □

Proposition 1. *Let $n = pq$, with $p \equiv q \equiv 5 \bmod 12$. Then, the following map is a bijection:*

$$\begin{aligned} \varDelta_n : D_n &\longrightarrow D_n \\ (x,y) &\longmapsto 2\#(x,y) \end{aligned}$$

Proof. $\varDelta_n$ is well-defined by the definition of D_n and lemma 1. In order to prove that $\varDelta_n$ is injective, let us consider Q_1 and Q_2 in D_n such that $2\#Q_1 = 2\#Q_2$. This implies, on the one hand, that there exist P_1 and P_2 such that $Q_1 = 2\#P_1$ and $Q_2 = 2\#P_2$. On the other hand, P_1, P_2, Q_1 and Q_2 lie on the same curve and $2\#(Q_2 - Q_1) = O$. Thus, $4\#(P_2 - P_1) = O$ which implies $2\#P_2 = 2\#P_1$, since there are no points of order 4 in $E_n(0,b)$. Therefore, $Q_2 = Q_1$. Finally, by a simple counting argument, $\varDelta_n$ must be surjective. □

We point out that $\varDelta_n$ is an elliptic analogous of Blum-Williams function.

Proposition 2. *If $p \equiv q \equiv 5 \bmod 12$, then $\varDelta_n$ is a trapdoor permutation equivalent to factoring n.*

Proof. Let us see, given the trapdoor information, p and q, how to invert $\varDelta_n$ efficiently on a point $Q \in D_n$. Since $\varDelta_n$ is a bijection, there exist a point $P \in D_n$ such that $Q = 2\#P$, but there also exists another point $R \in D_n$ such that $P = 2\#R$, that is $Q = 4\#R$. Let us consider the points $T_p = \frac{p+3}{4}\#\pi_p(Q)$

and $T_q = \frac{q+3}{4}\#\pi_q(Q)$. Then, $T_p = (p+3)\#\pi_p(R) = 2\#\pi_p(R) = \pi_p(P)$ and $T_q = (q+3)\#\pi_q(R) = 2\#\pi_q(R) = \pi_q(P)$. Thus, the preimage P of Q can be easily computed from T_p and T_q by the Chinese Reminder Theorem. In fact, a point-halving procedure that works in a more general case can be found in [8].

Now, to conclude the proof, it suffices to show a reduction from the one-wayness of Δ_n to the problem of factoring n. To do this, take a random pair $\bar{P} = (\bar{x}, \bar{y}) \in \mathbb{Z}_n \times \mathbb{Z}_n^*$ and compute $Q = 2\#\bar{P}$, that is uniformly distributed in D_n. Observe that $\pi_q(\bar{P}) \in D_q$ but $\pi_p(\bar{P}) \notin D_p$ with probability 1/4. Let us consider we are in this case. Since $Q \in D_n$, there exists a point $P = (x, y) \in D_n$ such that $Q = 2\#P$. Let us consider an algorithm $\mathcal{A}$ such that on input (n, Q) returns P with probability ϵ. If $\mathcal{A}$ succeeds then $2\#\bar{P} = 2\#P$. We can assure now that $\pi_q(\bar{P}) = \pi_q(P)$ and $\bar{x} \neq x \bmod p$ (note that, if $\bar{x} = x \bmod p$, then $\pi_p(\bar{P}) = \pm\pi_p(P)$ and $\pi_p(\bar{P}) \in D_p$, which is a contradiction). Finally, $\gcd(\bar{x}-x, n) = p$. By considering also the case $\pi_p(\bar{P}) \in D_p$ and $\pi_q(\bar{P}) \notin D_q$, it is straightforward to show that this procedure gives a nontrivial factor of n with probability $\epsilon/2$. □

4.3 Lifted Trapdoor Bijection

Next, a lifted version of the map Δ_n is presented. The technique used here is somewhat related to the one used in [5]. The following useful property allows to lift a point $P_0 \in E_n(0, b_0)$ to a special point P on each curve $E_{n^2}(0, b)$ such that $b \equiv b_0 \bmod n$.

Property 1. Let $b \in \mathbb{Z}_{n^2}^*$ and $P = (x_0, y_0) \in E_n(0, b \bmod n)$, with $y_0 \in \mathbb{Z}_n^*$. Then, there exists a unique point $(x_0, y) \in E_{n^2}(0, b)$ such that $y \equiv y_0 \bmod n$.

Proof. Let $y = y_0 + \gamma n \in \mathbb{Z}_{n^2}^*$, where $\gamma \in \mathbb{Z}_n$. Then, (x_0, y) belongs to $E_{n^2}(0, b)$ if and only if

$$\gamma = \frac{x_0^3 - y_0^2 + b}{n}(2y_0)^{-1} \bmod n.$$

□

Let $n = pq$, with $p \equiv q \equiv 5 \bmod 12$, and let us consider the following sets:

$$\Omega_n = \{(x, y) \in \mathbb{Z}_{n^2} \times \mathbb{Z}_{n^2}^* \mid \pi_n(x, y) \in D_n\},\ \omega_n = \{(x, y) \in \Omega_n \mid x < n\}.$$

and the function

$$\begin{aligned} \psi_n : \omega_n \times \mathbb{Z}_n &\longrightarrow \Omega_n \\ (x, y, m) &\longrightarrow 2\#P + O_m \end{aligned}$$

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

Lemma 3. *If $p \equiv q \equiv 5 \bmod 12$, then the map ψ_n is well defined and bijective.*

Proof. The map ψ_n is well-defined since $\psi_n(x, y, m)$ is always in Ω_n. This comes from the definition of Ω_n, since $\psi_n(x, y, m) \in \Omega_n$ if and only if $\pi_n(\psi_n(x, y, m)) \in D_n$. As $(x, y) \in \omega_m$, $\pi_n(x, y) \in D_n$ and then $\pi_n(\psi_n(x, y, m)) = \pi_n(2\#(x, y)) = 2\#\pi_n(x, y) \in D_n$.

In order to show that ψ_n is injective, let us suppose $\psi_n(x, y, m) = \psi_n(x', y', m')$ for some $(x, y), (x', y') \in \omega_n$ and $m, m' \in \mathbb{Z}_n$. Reducing this equality modulo n, we obtain $2\#\pi_n(x, y) = 2\#\pi_n(x', y')$. By the injectivity of Δ_n and from the fact that $\pi_n(x, y)$ and $\pi_n(x, y)$ are points in D_n we deduce $\pi_n(x, y) = \pi_n(x', y')$.

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 1 to deduce $(x, y) = (x', y')$. From this, it is easy to see that $O_m = O_{m'}$, so $m = m'$.

Finally, let us show that ψ_n is surjective. Let $C = (u, v) \in \Omega_n$ and $b = v^2 - u^3 \bmod n^2$. Then there exists $P_0 = (x_0, y_0) \in D_n$ such that $\pi_n(u, v) = 2\#P_0$. Let $P = (x_0, y)$ be the point on $E_{n^2}(0, b)$ given in Property 1. Clearly, $P \in \omega_n$ and $2\#P - C$ is a point at infinity, say O_m. Then, $C = \psi_n(x_0, y, m)$. □

Proposition 3. *If $p \equiv q \equiv 5 \bmod 12$, then ψ_n is a trapdoor bijection equivalent to factoring n.*

Proof. Let us see, given the trapdoor information, p and q, how to invert ψ_n efficiently on a point $C = (u, v) \in \Omega_n$. Let $b = v^2 - u^3 \bmod n^2$. Compute $Q_0 = \pi_n(C)$ that is a point in D_n and let $P_0 \in D_n$ such that $Q_0 = 2\#P_0$. The point P_0 can be efficiently computed by using the procedure for inverting Δ_n described in the proof of proposition 2. Then, let $P = (x, y) \in E_{n^2}(0, b)$ the point given in property 1 computed from P_0. Clearly, $P \in \omega_n$ and $C - 2\#P$ is a point at infinity, say O_m. Then, $C = \psi_n(x, y, m)$.

To conclude the proof, it suffices to show a reduction from the one-wayness of ψ_n to the problem of factoring n. As in the proof of proposition 2, take a random pair $(\bar{x}, \bar{y}) \in \mathbb{Z}_n \times \mathbb{Z}_n^*$ and compute $Q_0 = (u_0, v_0) = 2\#(\bar{x}, \bar{y})$. Now randomly lift Q_0 obtaining $C = (u_0 + \mu n, v_0 + \nu n)$, where μ and ν are randomly selected in $\mathbb{Z}_n$. Note that C is uniformly distributed on Ω_n. Let us consider an algorithm $\mathcal{A}$ such that on input (n, C) returns $P = (x, y) \in \omega_n$ and $m \in \mathbb{Z}_n$ such that $C = \psi_n(x, y, m)$, with probability ϵ. If $\mathcal{A}$ succeeds, then $\Delta_n(\pi_n(x, y)) = 2\#\pi_n(x, y) = \pi_n(C) = Q_0$. So, by following the same steps as in the proof of proposition 2, a nontrivial factor of n is found with probability $\epsilon/2$. □

5 The New Scheme

Based on the previous trapdoor bijection, in this section we present an elliptic curve cryptosystem (ECC) over the ring $\mathbb{Z}_{n^2}$ which is semantically secure under a new decisional assumption and has the fastest encryption and the highest one-way security among the known ECC, in the standard model.

Key generation. Given a security parameter ℓ, choose at random two primes p and q with ℓ bits such that $p \equiv q \equiv 5 \bmod 12$. Then the public key is PK=$\{n\}$, $n = pq$, and the private key is SK=$\{p, q\}$.

Encryption. To encrypt a message $m \in \mathbb{Z}_n$ we choose at random $z \in \mathbb{Z}_n$ and $t \in \mathbb{Z}_n^*$ such that $b_0 = t^2 - z^3 \in \mathbb{Z}_n^*$. This choice determines an elliptic curve $E_n(0, b_0)$ and a point $R = (z, t)$ on it. Let $P_0 = (x_0, y_0) = 2\#R$ and γ chosen at random in $\mathbb{Z}_n$, and compute $y = y_0 + \gamma n$. Then $P = (x_0, y)$ is a random point in ω_n. The encryption of the message $m \in \mathbb{Z}_n$ is $C = \psi_n(x_0, y, m)$.

Decryption. To recover the message m from the ciphertext $C = (u, v) = \psi_n(x, y, m)$, the randomness $(x, y) \in \omega_n$ is computed firstly and, afterwards, m is easily obtained from $O_m = C - 2\#(x, y)$. This is just the procedure detailed in the proofs of propositions 2 and 3. We recall the steps to obtain (x, y) from C. Firstly, compute $\pi_n(x, y)$ by inverting Δ_n on $\pi_n(C)$ (using the Chinese Reminder Theorem). Next, compute $(x, y) \in E_{n^2}(0, b)$, where $b = v^2 - u^3 \bmod n^2$, by using property 1.

In the following, the security of this scheme is analyzed. Let us introduce some convenient notations. If A is a finite set, $x \leftarrow A$ will denote that x is randomly selected with uniform distribution in A. We will denote by $D_1 \approx D_2$ the fact that two probability distributions D_1 and D_2 are polynomially 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 $g(D_1) \approx g(D_2)$.

M_ℓ will denote the set of integers $n = pq$ such that p and q are two primes with ℓ bits, and $p \equiv q \equiv 5 \bmod 12$.

5.1 One-Wayness

The following lemma allows to compute, with overwhelming probability, a rational function of the coordinates of a point $P_0 \in D_n$, given two special lifted points Q_1 and Q_2 such that $\pi_n(Q_1) = \pi_n(Q_2) = 2\#P_0$.

Lemma 4. *Let $Q_1 = (u_1, v_1) = 2\#P_1$ and $Q_2 = (u_2, v_2) = 2\#P_2$ where P_1 and P_2 are different points in ω_n such that $\pi_n(P_1) = \pi_n(P_2)$. Let $b_1 = v_1^2 - u_1^3 \bmod n^2$ and $b_2 = v_2^2 - u_2^3 \bmod n^2$. Let $(x_0, y_0) = \pi_n(P_1)$. Then*

$$9\alpha \left(\frac{x_0}{y_0} \right)^4 = -4\beta \bmod n,$$

where $\alpha = (b_2 - b_1)/n$ and $\beta = (u_2 - u_1)/n$.

Proof. Since $P_1, P_2 \in \omega_n$ we can write $P_1 = (x_0, y_1)$ and $P_2 = (x_0, y_2)$, where $y_1 \equiv y_2 \equiv y_0 \bmod n$ and $x_0 < n$. Observe that both points lie in different curves. Indeed, Q_1 and P_1 are in $E_n(0, b_1)$ while Q_2 and P_2 are in $E_n(0, b_2)$. Since $b_1 \equiv b_2 \bmod n$, $\alpha = (b_2 - b_1)/n$ is well defined.

By using the doubling formula, we obtain

$$u_1 = \left(\frac{3x_0^2}{2y_1} \right)^2 - 2x_0 = \frac{9x_0^4}{4(x_0^3 + b_1)} - 2x_0 \bmod n^2$$
$$u_2 = \left(\frac{3x_0^2}{2y_2} \right)^2 - 2x_0 = \frac{9x_0^4}{4(x_0^3 + b_2)} - 2x_0 \bmod n^2$$

and then,

$$u_2 - u_1 = \frac{9x_0^4}{4(x_0^3 + b_2)} - \frac{9x_0^4}{4(x_0^3 + b_1)} = \frac{9x_0^4(b_1 - b_2)}{4(x_0^3 + b_1)(x_0^3 + b_2)} = -\frac{9}{4}\frac{x_0^4}{y_1^2 y_2^2}\alpha n \bmod n^2.$$

Therefore

$$\beta = \frac{u_2 - u_1}{n} = -\frac{9}{4}\left(\frac{x_0}{y_0}\right)^4 \alpha \bmod n.$$

□

Note that if Q_1 and Q_2 are chosen at random (but fulfilling the conditions in lemma 4) then $\alpha \in \mathbb{Z}_n^*$ with overwhelming probability.

From this lemma, given a random modulus n, we can exploit an adversary $\mathcal{A}$ against the one-wayness of the proposed scheme to build such two points Q_1 and Q_2, and efficiently derive a nontrivial factor of n.

Proposition 4. *The one-wayness of the proposed scheme is equivalent to the unfeasability of factoring the modulus.*

Proof. Let $\mathcal{A}$ be an adversary trying to break the one-wayness of the proposed cryptosystem. Let us consider the following probability

$$\mathsf{Succ}_{\mathcal{A}}^{\mathsf{OW}}(\ell) = \mathsf{Prob}\left[\mathcal{A}(n, \psi_n(x, y, m)) = m \mid n \leftarrow M_\ell;\ (x, y) \leftarrow \omega_n;\ m \leftarrow \mathbb{Z}_n\right].$$

The following algorithm $\mathcal{B}$ can be used to obtain a nontrivial factor of $n \leftarrow M_\ell$.

```
$\mathcal{B}(n)$
1   $\bar{x}_0 \leftarrow \mathbb{Z}_n;\ \bar{y}_0 \leftarrow \mathbb{Z}_n;\ b_0 = \bar{y}_0^2 - \bar{x}_0^3 \bmod n$
2       if $\gcd(\bar{y}_0, n) \neq 1$ return $\gcd(\bar{y}_0, n)$
3       if $\gcd(b_0, n) \neq 1$ return $\gcd(b_0, n)$
4   $(u_0, v_0) = 2\#(\bar{x}_0, \bar{y}_0)$, computed in $E_n(0, b_0)$
5   $\gamma_1 \leftarrow \mathbb{Z}_n;\ \delta_1 \leftarrow \mathbb{Z}_n;\ C_1 = (u_0 + \gamma_1 n, v_0 + \delta_1 n)$
6   $m_1 = \mathcal{A}(n, C_1);\ (u_1, v_1) = C_1 - O_{m_1}$
7   $\gamma_2 \leftarrow \mathbb{Z}_n;\ \delta_2 \leftarrow \mathbb{Z}_n;\ C_2 = (u_0 + \gamma_2 n, v_0 + \delta_2 n)$
8   $m_2 = \mathcal{A}(n, C_2);\ (u_2, v_2) = C_2 - O_{m_2}$
9   $\alpha = (v_2^2 - u_2^3 - v_1^2 + u_1^3)/n$
10      if $\gcd(\alpha, n) \neq 1$ return $\gcd(\alpha, n)$
11  $\beta = (u_2 - u_1)/n$
12  return $\gcd\left(\frac{\bar{x}_0^4}{\bar{y}_0^4} + \frac{4\beta}{9\alpha}, n\right)$
```

At steps 1 to 4 of the algorithm, a random point $Q_0 = (u_0, v_0) \in D_n$ is built. Next, points $Q_1 = (u_1, v_1)$ and $Q_2 = (u_2, v_2)$ are built by calling $\mathcal{A}$ twice using two randomly lifted points C_1 and C_2 coming from the same point Q_0.

If $\mathcal{A}$ succeeds in the first call, at step 6, then Q_1 can be written as $Q_1 = 2\#P_1$ where $P_1 \in \omega_n$. This is a consequence of the bijectivity of ψ_n, since $C_1 \in \Omega_n$, and then there exists a unique $P_1 \in \omega_n$ and a unique $m_1 \in \mathbb{Z}_n$ such that

$C_1 = \psi_n(P_1, m_1)$. The same occurs with $Q_2 = 2\#P_2$, if $\mathcal{A}$ succeeds in the second call.

Let us consider the case that $\mathcal{A}$ succeeds in both calls. Note that $Q_0 = \pi_n(C_1) = \pi_n(C_2)$ and $Q_0 = 2\#\pi_n(P_1) = 2\#\pi_n(P_2)$. But there is only one point in D_n whose double is Q_0. Thus, $\pi_n(P_1) = \pi_n(P_2)$. Let $P_0 = (x_0, y_0) = \pi_n(P_1) = \pi_n(P_2)$. Since Q_1 and Q_2 fulfil the conditions in the previous lemma, then

$$\left(\frac{x_0}{y_0}\right)^4 = -\frac{4\beta}{9\alpha} \bmod n$$

if $\alpha \in \mathbb{Z}_n^*$.

On the other hand, $Q_0 = 2\#(\bar{x}_0, \bar{y}_0) = 2\#P_0$. Observe that $P_0 \in D_n$ but $\bar{P}_0 = (\bar{x}_0, \bar{y}_0)$ is chosen at random. By using the Chinese Reminder Theorem, $\pi_p(\bar{P}_0) = \pi_p(P_0)$ with probability $1/2$, and independently $\pi_q(\bar{P}_0) = \pi_q(P_0)$ with probability $1/2$. So, with probability $1/4$, $\pi_q(\bar{P}_0) = \pi_q(P_0)$ but $\pi_p(\bar{P}_0) \neq \pi_p(P_0)$. The last expression implies $\bar{x}_0 \neq x_0 \bmod p$. To see this, let us suppose $\bar{x}_0 = x_0 \bmod p$. Then, $\pi_p(\bar{P}_0) = -\pi_p(P_0)$. From $2\#\bar{P}_0 = 2\#P_0$ we deduce $4\#\pi_p(\bar{P}_0) = O$. Since there are no points with order 4 on $E_p(0, b_0 \bmod p)$ then $2\#\pi_p(\bar{P}_0) = O$ and consequently $\bar{y}_0 \equiv 0 \bmod p$. But, this is not possible due to step 2 in the algorithm.

Except for a negligible fraction of the values of $(\bar{x}_0, \bar{y}_0)$, it can be also shown that[1]

$$\left(\frac{\bar{x}_0}{\bar{y}_0}\right)^4 \neq \left(\frac{x_0}{y_0}\right)^4 \bmod p.$$

Then, by using lemma 4,

$$\gcd\left(\frac{\bar{x}_0^4}{\bar{y}_0^4} + \frac{4\beta}{9\alpha}, n\right) = p.$$

By considering the other case, $\pi_p(\bar{P}_0) = \pi_p(P_0)$ but $\pi_q(\bar{P}_0) \neq \pi_q(P_0)$, the previous gcd expression leads to the other nontrivial factor of n.

Finally, except for a negligible function of ℓ (due to the technical steps 2, 3 and 10, and the anomalous values of $(\bar{x}_0, \bar{y}_0)$) the success probability

$$\mathsf{Succ}_{\mathcal{B}}^{\mathsf{FACT}}(\ell) = \mathsf{Prob}\left[\mathcal{B}(n) \in \{p, q\} \mid n \leftarrow M_\ell\right]$$

is one half the probability that $\mathcal{A}$ is successful in both calls. Notice that this two calls are not independent, since they share the same values of n and Q_0. However, by using lemma 5 (given in appendix A) with algorithm $\mathcal{A}$, predicate $P =$ "$\mathcal{A}$ succeeds" and map $f(n, C) = (n, \pi_n(C))$, the following inequality is obtained:

$$\mathsf{Succ}_{\mathcal{B}}^{\mathsf{FACT}}(\ell) \geq \frac{1}{2}\left(\mathsf{Succ}_{\mathcal{A}}^{\mathsf{OW}}(\ell)\right)^2.$$

□

[1] The exception are points $(\bar{x}_0, \bar{y}_0)$ such that $\bar{x}_0 \bmod p$ is a root of a certain polynomial of degree 8. However, by making some cumbersome calculations, it can be shown that if $p \equiv 1 \bmod 8$ then there are no exceptional points, otherwise, i.e. $p \equiv 5 \bmod 8$, there are only $p - 1$ exceptional points (modulo p), that is, only a fraction $1/p$. (See appendix B for details.)

5.2 Semantic Security

The scheme is semantically secure under the following assumption:

Assumption 1 (Decisional Small-x Double (DSD) Assumption). *The following probability distributions are polynomially indistinguishable*

$$\begin{aligned} D_{\text{double}} &= (n, 2\#(x,y)) \quad \text{where } n \leftarrow M_\ell,\ (x,y) \leftarrow \omega_n \\ D_{\text{random}} &= (n, (x',y')) \qquad \text{where } n \leftarrow M_\ell,\ (x',y') \leftarrow \Omega_n . \end{aligned}$$

Proposition 5. *The proposed scheme is semantically secure if and only if the DSM assumption 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

$$\begin{aligned} D_0 &= (n, \psi_n(x,y,m_0)) \quad \text{where } n \leftarrow M_\ell,\ (x,y) \leftarrow \omega_n \,, \quad \text{and} \\ D &= (n, \psi_n(x,y,m)) \quad \text{where } n \leftarrow M_\ell,\ (x,y) \leftarrow \omega_n,\ m \leftarrow \mathbb{Z}_n . \end{aligned}$$

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

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

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

$$(n, 2\#(x,y)) \approx (n, 2\#(x,y) + O_{m'}), \quad \text{with } (x,y) \leftarrow \omega_n,\ m' \leftarrow \mathbb{Z}_n \,.$$

Note that the distribution on the left side is D_{double}. Besides, since $2\#(x,y) + O_{m'} = \psi_n(x,y,m')$, and ψ_n is a bijection, then D and D_{random} are identical distributions. □

Finally, we argue why one should be confident about the hardness of the new decisional problem presented in this paper.

According to the formula for computing the double of a point on an elliptic curve $E_{n^2}(0,b)$ (see end of Section 2), given $(u,v) = 2\#(x_1,y_1)$, x_1 is a root of the univariate polynomial $R(x) = x^4 + 4x^3u - 8bx + 4bu \in \mathbb{Z}_{n^2}[x]$. Then, DSD assumption is related to the difficulty of deciding if the polynomial $R(x)$ has a root smaller than n.

Similarly, the semantic security of other related cryptosystems (such as [2]) is related to the difficulty of deciding if a certain polynomial has a root smaller than n. The best known way to attack the above decisional problems is to solve their computational versions. The problem of finding small roots of polynomials modulo a large integer with unknown factorisation has been directly studied in the literature. The most powerful result in this area was obtained by Coppersmith in [3]. This result ensures that one can efficiently compute (i.e. in polynomial time) all roots x_1 of a polynomial $P(x) \in \mathbb{Z}_K[x]$ with degree d such that $|x_1| < K^{1/d}$. Up to now, no improvement on this bound has been made. The result by Coppersmith implies we can only find the roots $|x_1| < (n^2)^{1/4} = n^{1/2}$ of the polynomial $R(x)$, which does not affect the validity of DSD assumption.

We point out that if we construct a similar encryption scheme over $\mathbb{Z}_{n^2}$, that is $f(m,r) = r^2 + mn \bmod n^2$ (the scheme in [5] using $e = 1$), then the resulting scheme is not semantically secure anymore. This is due to the fact that the related decisional problem is trivially solved. In order to see if c is an encryption of m it suffices to check if $c - mn \bmod n^2$ is a square over the integers. This is why we are interested in constructing a Rabin-based scheme using elliptic curves over $\mathbb{Z}_{n^2}$.

6 Efficiency Analysis

Now we study the encryption cost of our scheme. 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 $\bmod n$, because modular inverses can be computed within a constant number of modular multiplications.

Generating $(x, y) \in \omega_n$*:* 5 multiplications modulo n, 1 inverse modulo n, and 1 n-length integer multiplication.

Computing $2\#(x, y)$*:* 5 multiplications modulo n^2, 1 inverse modulo n^2.

Adding O_m*:* 3 multiplications modulo n, 2 n-length integer multiplication.

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 $8 + c$ multiplications modulo n. Practical implementations, suggests than the value $c = 8$ can be taken (see [1]).

Then, since the n-length integer multiplication cost is bounded by the cost of a multiplication modulo n, the encryption cost of our scheme is 55 multiplications modulo n. Thus we have proved that our scheme is drastically more efficient than the previous semantically secure elliptic curve cryptosystems (ECC) in the standard model based on factoring.

Next, we will compare the efficiency of our scheme with the well-known El Gamal ECC scheme. We assume that El Gamal ECC is performed over $\mathbb{Z}_p^*$, where p is 160 bits long, and our scheme is performed over $\mathbb{Z}_{n^2}^*$, where n is 1024 bits long (cf. [9]). We will express both encryption costs in terms of multiplications modulo n.

In El Gamal ECC the most time consuming operation is the computation of two multiples $r\#P$ and $ra\#P$, where r is a random integer whose size is roughly the same as the modulus p, and a is a fixed integer. Then, using the *double and* *add* algorithm, the computation of these two multiples requires on average k additions of points and $2k$ doublings, where k is the bit length of r. Assuming that a point addition or doubling requires about 12 modular multiplications, then El Gamal ECC would take approximately $3 \cdot 160 \cdot 12$ multiplications modulo p. Since the time needed to perform a modular multiplication is quadratic in the size of the modulus, the ratio between the time of a multiplication modulo p and a multiplication modulo n is $\frac{160^2}{1024^2}$. It follows that the encryption time of El Gamal ECC would be equivalent to 159 multiplications modulo n, which is almost three times the encryption cost of our scheme. If the efficiency is measured in terms of encryption-time per plaintext bit, this ratio must be multiplied by the ratio of the message lengths. Therefore, our cryptosystem is 18 times faster than El Gamal ECC in encryption-time per bit.

Thus, our cryptosystem is the provably secure IND-CPA elliptic curve cryptosystem in the standard model with the fastest encryption algorithm to the best of our knowledge.

The key generation of the proposed cryptosystem is faster than generating an RSA key, since only the modulus is needed. Regarding decryption, the main cost is due to the computation of $\frac{p+3}{4}\#P \in E_p(0,b)$, and $\frac{q+3}{4}\#P \in E_q(0,b)$, from $P \in E_n(0,b)$ which is almost the same as in the other existing ECC over $\mathbb{Z}_{n^2}$. Nevertheless, from a global point of view, it is unlikely that our scheme could compete with El Gamal ECC, due to its decryption cost.

References

1. R. P. Brent. Some Integer Factorization Algorithms using Elliptic Curves. *Australian Computer Science Comunications* 24–26 (1986) (Republished 1998).
2. D. Catalano, R. Gennaro, N. Howgrave-Graham and P. Q. Nguyen. Paillier's Cryptosystem Revisited.*ACM CCS '2001 ACM Press* (2001).
3. D. Coppersmith. Finding a small root of a univariate modular equation. *EUROCRYPT '96, LNCS* **1070** 155–165 (1996).
4. S. Galbraith. Elliptic curve Paillier schemes. *Journal of Cryptology* **15** (2) 129–138 (2002).
5. D. Galindo, S. Martín, P. Morillo and J. L. Villar. A Practical Public Key Cryptosystem from Paillier and Rabin Schemes. *PKC'03* LNCS **2567** 279–291 (2002).
6. D. Galindo, S. Martín, P. Morillo and J. L. Villar. An efficient semantically secure elliptic curve cryptosystem based on KMOV. *Proceedings of International Workshop on Coding and Cryptography (WCC'03)*, (2003).
7. S. Goldwasser and M. Bellare. Lecture Notes on Cryptography. `http://www-cse.ucsd.edu/users/mihir`
8. 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).
9. A. K. Lenstra and E. R. Verheul. Selecting Cryptographyc Key Sizes. http://cryptosavvy.com/cryptosizes.pdf
10. A. Menezes. Elliptic Curve Public-Key Cryptosystems. *Kluwer Academic SECS* **234** (1993)
11. J.H. Silverman. The arithmetic of elliptic curves. *Springer GTM* **106** (1986).

12. H.C.A. van Tilborg. A Professional Reference and Interactive Tutorial. *Kluwer Academic Publishers SECS* **528** (1999).

A Technical Lemma

This technical lemma is useful when dealing with two non-independent calls to a probabilistic algorithm.

Lemma 5. *Consider a probabilistic algorithm $\mathcal{A}$ with input $x \in X$, a (surjective) map $f : X \to Y$, and a predicate P on the input and the output of $\mathcal{A}$ (e.g. $P(n, \mathcal{A}(n))$ true if $\mathcal{A}(n)$ is a nontrivial factor of n).*

Let $\epsilon = \mathsf{Prob}\,[P(x, \mathcal{A}(x)) \mid x \leftarrow X]$. Then,

$$\mathsf{Prob}\left[P(x_1, \mathcal{A}(x_1)) \wedge P(x_2, \mathcal{A}(x_2)) \mid x_1 \leftarrow X;\ x_2 \leftarrow f^{-1}(f(x_1))\right] \geq \epsilon^2,$$

where the internal random coins used by $\mathcal{A}$ in the two calls are independent.

Proof. For any $y \in Y$, let us define

$$\begin{aligned} w_y &= \mathsf{Prob}\,[f(x) = y \mid x \leftarrow X] \quad \text{and} \\ \epsilon_y &= \mathsf{Prob}\left[P(x, \mathcal{A}(x)) \mid x \leftarrow f^{-1}(y)\right]. \end{aligned}$$

Then $\sum_{y \in Y} w_y = 1$ and $\sum_{y \in Y} w_y \epsilon_y = \epsilon$. Given the following experiment $x_1 \leftarrow X;\ x_2 \leftarrow f^{-1}(f(x_1))$, then,

$$\begin{aligned} &\mathsf{Prob}\,[P(x_1, \mathcal{A}(x_1)) \wedge P(x_2, \mathcal{A}(x_2))] = \\ &\quad = \sum_{y \in Y} \mathsf{Prob}\,[P(x_1, \mathcal{A}(x_1)) \wedge P(x_2, \mathcal{A}(x_2)) \wedge f(x_1) = y] = \\ &\quad = \sum_{y \in Y} \mathsf{Prob}\,[P(x_1, \mathcal{A}(x_1)) \wedge P(x_2, \mathcal{A}(x_2)) \mid f(x_1) = y]\, \mathsf{Prob}\,[f(x_1) = y]\,. \end{aligned}$$

But the condition $f(x_1) = y$ is equivalent to modifying the experiment into $x_1 \leftarrow f^{-1}(y);\ x_2 \leftarrow f^{-1}(y)$. So, in this new probability space, x_1 and x_2 are identically distributed independent random variables, and

$$\begin{aligned} &\mathsf{Prob}\,[P(x_1, \mathcal{A}(x_1)) \wedge P(x_2, \mathcal{A}(x_2)) \mid f(x_1) = y] = \\ &\quad = (\mathsf{Prob}\,[P(x_1, \mathcal{A}(x_1)) \mid f(x_1) = y])^2 = \epsilon_y^2. \end{aligned}$$

By using for instance the Cauchy-Schwartz inequality for a suitable weighted inner product (i.e. $\mathbf{a} \cdot \mathbf{b} = \sum_{y \in Y} w_y a_y b_y$), it is straightforward to see that $\sum_{y \in Y} w_y \epsilon_y^2 \geq \epsilon^2$. □

Observe that, although the two calls to $\mathcal{A}$ are not independent, they share part of the input. So, there can be a positive correlation (due to the map f) between their outputs. This is the reason (and not the independence) why the success probability of the two calls can be bounded by the square of the success probability of a single call. Typically, the image of f is a part of the input of $\mathcal{A}$, e.g. when the same RSA modulus is used in both calls to $\mathcal{A}$.

This lemma applies to almost all security proofs in the literature related to an RSA modulus, where more than one call to an adversary is made.

B Computing the Number of Exceptional Points

In this appendix, we compute the number of points $(\bar{x}, \bar{y}) \in \mathbb{Z}_p \times \mathbb{Z}_p^*$ such that $\bar{x} \neq x$ and $\left(\frac{\bar{x}}{\bar{y}}\right)^4 = \left(\frac{x}{y}\right)^4$, where $(x, y) \in D_p$ is the unique point such that $2\#(x, y) = 2\#(\bar{x}, \bar{y})$. From observation 1, $(\bar{x}, \bar{y}) = (x, y) + (\eta, 0)$. Thus

$$\bar{x} = \left(\frac{y}{x-\eta}\right)^2 - x - \eta = \frac{x^3 - \eta^3}{(x-\eta)^2} - x - \eta = \frac{x^2 + \eta x + \eta^2}{x - \eta} - x - \eta = \eta \frac{x + 2\eta}{x - \eta}$$

and

$$\bar{y} = \frac{y}{x-\eta}(\eta - \bar{x}) = \frac{\eta y}{x - \eta}\left(1 - \frac{x + 2\eta}{x - \eta}\right) = -\frac{3\eta^2 y}{(x-\eta)^2}.$$

Dividing both equations

$$\frac{\bar{x}}{\bar{y}} = -\frac{(x + 2\eta)(x - \eta)}{3\eta y}.$$

On the other hand, $\frac{\bar{x}}{\bar{y}} = \rho \frac{x}{y}$, where ρ is a fourth root of unity. This equation is equivalent to $(x + 2\eta)(x - \eta) = -3\rho\eta x$, that means x is a root of the polynomial equation $(x + 2\eta)^4(x - \eta)^4 = 81\eta^4 x^4$. So, there are at most 8 different values of x, given η. Moreover, there are at most 16 points $(\bar{x}, \bar{y})$ in each curve $E_p(0, b)$ satisfying the conditions at the beginning of this appendix. Finally, the probability that one of these points is guessed at random is at most $16/p$.

A tighter bound for this probability can be obtained if the quadratic equation $(x+2\eta)(x-\eta) = -3\rho\eta x$ is discussed for each value of ρ. Let $t = x/\eta$. The equation can be rewritten as $(t + 2)(t - 1) = -3\rho t$, and also as $t^2 + (1 + 3\rho)t - 2 = 0$. The discriminant of the equation is $\varDelta = (1 + 3\rho)^2 + 8 = 9\rho^2 + 6\rho + 9$.

Since $p \equiv 1 \bmod 4$, then $\left(\frac{-1}{p}\right) = 1$ and there are 4 different values of ρ: 1, -1 and the two square roots of -1. Moreover, since $p \equiv 5 \bmod 12$, then $\left(\frac{3}{p}\right) = -1$, and $\left(\frac{2}{p}\right) = 1$ if and only if $p \equiv 1 \bmod 8$.

Taking this into account, if $\rho = 1$, then $\varDelta = 24$, that is a quadratic residue only if $p \equiv 5 \bmod 8$. If $\rho = -1$, then $\varDelta = 12$ that is not a quadratic residue. Finally, if $\rho^2 = -1$, then $\varDelta = 6\rho$. But

$$\left(\frac{\rho}{p}\right) = \rho^{\frac{p-1}{2}} = (-1)^{\frac{p-1}{4}} \bmod p$$

that is equal to 1 if and only if $p \equiv 1 \bmod 8$. This implies that 2ρ is always a quadratic residue, so 6ρ never is.

Summing up the above information, the only values of t come up when $p \equiv 5 \bmod 8$ and $\rho = 1$. This two values are $t = -(2 \pm \sqrt{6})$. Now, $x = \eta t$ and $y^2 = x^3 - \eta^3 = \eta^3(t^3 - 1)$. From that, for each value of t, only $\frac{p-1}{2}$ values of η lead to existing values of y. It is easy to see that there are exactly $2(p-1)$ points (x, y), but only $p - 1$ are in D_p.

This last step follows from a symmetry argument. In all equations, (x, y) and $(\bar{x}, \bar{y})$ play a symmetric role, since $(\bar{x}, \bar{y}) = (x, y) + (\eta, 0)$ is equivalent to $(x, y) = (\bar{x}, \bar{y}) + (\eta, 0)$. But $(x, y) \in D_p$ and $(\bar{x}, \bar{y}) \notin D_p$. Thus, only half of the solutions found correspond to values of (x, y), and the other half correspond to values of $(\bar{x}, \bar{y})$.