Trapdooring Discrete Logarithms on Elliptic Curves over Rings

Pascal Paillier

Cryptography and Security Group, Gemplus Card International
34 rue Guynemer, F-92447 Issy-Les-Moulineaux
pascal.paillier@gemplus.com

Abstract. This paper introduces three new probabilistic encryption schemes using elliptic curves over rings. The cryptosystems are based on three specific trapdoor mechanisms allowing the recipient to recover discrete logarithms on different types of curves. The first scheme is an embodiment of Naccache and Stern's cryptosystem and realizes a discrete log encryption as originally wanted in [23] by Vanstone and Zuccherato. Our second scheme provides an elliptic curve version of Okamoto and Uchiyama's probabilistic encryption, thus answering a question left open in [10] by the same authors. Finally, we introduce a Paillier-like encryption scheme based on the use of twists of anomalous curves. Our contributions provide probabilistic, homomorphic and semantically secure cryptosystems that concretize all previous research works on discrete log encryption in the elliptic curve setting.

Keywords. Elliptic Curve Cryptosystems, Discrete Logarithm Encryption, Homomorphic Encryption, Naccache-Stern, Okamoto-Uchiyama, Paillier.

1 Introduction

At the present time, one of the most challenging open problems in cryptography is certainly the realization of a trapdoor in the discrete logarithm problem. A discrete-log (DL) encryption scheme over a group G intends to encrypt a plaintext m by simply raising some base element $g \in \mathrm{G}$ to the power m, while decryption recovers m up to a public bound[1]. Motivations for this may be diverse. The main advantage in comparison to other public-key techniques such as RSA or El-Gamal comes from the *additive* homomorphic property of ciphertexts (the group product of encryptions of m_1 and m_2 yields an encryption of $m_1 + m_2$). This property constitutes the necessary condition for many cryptographic protocols to exist in fields like electronic voting [4], key escrow [13] or group signatures, to quote a few. Clearly, discovering novel discrete-log encryption techniques has a crucial positive impact on these research domains. In contrast, direct applications of these for simple encryption purposes may be of more moderate interest

[1] the decryption is only expected to retrieve m modulo the given bound, *i.e.* the trapdoor is partial.

T. Okamoto (Ed.): ASIACRYPT 2000, LNCS 1976, pp. 573–584, 2000.

as malleability destroys chosen-ciphertext security anyway[2]. Without considering all potential applications, this paper focuses on providing and analyzing new discrete log trapdoors and comparing their properties with the ones recently discovered in [8,9,11].

High degree residuosity was introduced by Benaloh [1] as an algebraic framework extending the properties of quadratic residuosity to prime degrees greater than two. Since then, successive works have considerably improved the efficiency of residuosity-based encryption. Naccache and Stern [8], utilizing a smooth degree modulo $n = pq$, increased Benaloh's encryption rate up to $\approx 1/5$. More recently, Okamoto and Uchiyama [9] and Paillier [11] came up with modulus-independent encryption rates of $1/3$ and $1/2$ respectively, basing trapdoorness on a joint use of Fermat quotients and clever parameter choices. Interestingly, these three cryptosystems only stand in the multiplicative groups $\mathbb{Z}_n^*$ where $n = pq$, p^2q or p^2q^2 and p, q are large prime numbers.

There have been several attempts, in the meantime, to realize discrete-log encryption over elliptic curves instead of standard groups. This was motivated by the fact that no subexponential time algorithm for extracting discrete logarithms is known so far, at least for most elliptic curves[3]. As a matter of fact, all such design proposals have revealed themselves unsuccessful. Vanstone and Zuccherato [23] proposed a deterministic DL encryption scheme that was shown to be insecure a few months later by McKee and Pinch [6] and Coppersmith [2]. Independently, Okamoto and Uchiyama failed in attempting to design DL encryption over composite anomalous curves [10].

This paper introduces cryptosystems successfully answering the quests of [23] and [10] respectively, with guaranteed semantic security relatively to well identified computational problems. The first scheme is an embodiment of Naccache and Stern's cryptosystem on curves defined over $\mathbb{Z}_n$ ($n = pq$) which realizes a discrete-log encryption as originally imagined by Vanstone and Zuccherato. Probabilistic, the scheme is also provably semantically secure relatively to the so-called high-degree residuosity problem. Our second cryptosystem relates to the p-residuosity of a well-chosen curve over the ring $\mathbb{Z}_{p^2q}$, that is, provides an elliptic curve instance of Okamoto and Uchiyama's encryption scheme. Finally, we show how to extend the same design framework to Paillier encryption [11], while preserving all security and efficiency properties inherent to the original cryptosystem. All three schemes are reasonably efficient, simple to understand, additively homomorphic, probabilistic and provably secure against chosen plaintext attacks (IND-CPA) in the standard model. We believe our cryptosystems to be the only ones that verify these properties.

Due to space limitations, we do not recall here the basics of high-degree residuosity (neither do we give the description of the encryption schemes we

[2] like for other cryptosystems however, security improvements are possible to reach resistance against active adversaries, see [12].

[3] it is known that there exist subexponential algorithms for curves of trace zero over $\mathbb{F}_p$ for p prime. The discrete-log problem happens to be trivially polynomial in the case of trace one, see [20].

work with), referring the reader to the bibliography for further information when needed.

2 Elliptic Curve Naccache-Stern Encryption

The first encryption scheme that we describe here is a variant of Naccache and Stern's encryption scheme [8] where the working group is an elliptic curve over the ring $\mathbb{Z}_n$. The construction of such a curve is similar in spirit to the work of Koyama, Maurer, Okamoto and Vanstone [5] that allowed to export factoring-based cryptosystems like RSA [15] and Rabin [14] on a particular family of curves over the ring $\mathbb{Z}_n$ (KMOV). We now describe briefly their construction.

In the sequel, p and q denote distinct large primes of product n. Recall that for any integer k, $E_k(a,b)$ is defined as the set of points $(x,y) \in \mathbb{Z}_k \times \mathbb{Z}_k$ such that

$$y^2 = x^3 + ax + b \mod k \ ,$$

together with a special element $\mathcal{O}_k$ called the point at infinity. It is known that given a composite integer k, a curve $E_k(a,b)$ defined over the ring $\mathbb{Z}_k$ has no reason to be a group. This problem, however, does not have real consequences in practice when $k = n$ because exhibiting a litigious addition leads to factor n and this event remains of negligible probability. Furthermore, projections of $E_n(a,b)$ over $\mathbb{F}_p$ and $\mathbb{F}_q$ (namely, $E_p(a,b)$ and $E_q(a,b)$) being finite abelian groups, the Chinese remainder theorem easily conducts to the following statement:

Lemma 1 (Koyama *et al.* **[5]).** *Let $E_n(a,b)$ be an elliptic curve where $n = pq$ is the product of two primes such that $\gcd(4a^3 + 27b^2, n) = 1$. Let us define the order of $E_n(a,b)$ as*

$$|E_n(a,b)| = \operatorname{lcm}(|E_p(a,b)|, |E_q(a,b)|) \ .$$

Then, for any point $P \in E_n(a,b)$,

$$|E_n(a,b)| \cdot P = \mathcal{O}_n$$

where $\mathcal{O}_n$ denotes the point at infinity of $E_n(a,b)$.

Although not being a group in a strict sense, the structure of the curve $E_n(a,b)$ complies to Lagrange's theorem and, from this standpoint, can be used as a group. Koyama *et al.* take advantage of this feature by focusing on curves of the following specific form:

$$E_n(0,b) \ : \ y^2 = x^3 + b \mod n \quad \text{for } b \in \mathbb{Z}_n^* \ ,$$

with $p \equiv q \equiv 2 \pmod 3$. This is motivated by the fact that the projected curves $E_p(0,b)$ and $E_q(0,b)$ happen to be of trace of Frobenius equal to zero. More specifically,

Lemma 2. *Let p be an odd prime satisfying $p \equiv 2 \pmod 3$. Then, for all $b \in [1, p-1]$, $E_p(0,b)$ is a cyclic group of order*

$$|E_p(0,b)| = p + 1 \ .$$

Subsequently, the problem of recovering $|E_n(0,b)| = \operatorname{lcm}(p+1, q+1)$ from n is equivalent to factoring n when $p \equiv q \equiv 2 \pmod 3$. Note that another possible choice of parameters are curves $E_n(a,0)$ for $a \in \mathbb{Z}_n^*$ and $p \equiv q \equiv 3 \pmod 4$. We refer the reader to [5] for further details.

2.1 Our Setting

Just as above, for some $b \in \mathbb{Z}_n^*$, we will be considering the curve $E_n(0,b)$ as a finite abelian group of order

$$\mu = |E_n(0,b)| = \operatorname{lcm}(p+1, q+1) \ .$$

In our setting, the prime factors p and q are both chosen congruent to 2 modulo 3 so that, by virtue of lemma 2, the two curves $E_p(0,b)$ and $E_q(0,b)$ are cyclic groups of respective orders $p+1$ and $q+1$. We also impose

$$p + 1 = 6 \cdot u \cdot p' \quad \text{where} \quad u = \prod p_i^{\delta_i} \quad \text{and} \tag{1}$$

$$q + 1 = 6 \cdot v \cdot q' \quad \text{where} \quad v = \prod p_j^{\delta_j} \ , \tag{2}$$

for some B-smooth integers u and v of (roughly) equal bitsize such that

$$\gcd(6, u, v, p', q') = 1$$

and $B = O(\log n)$. Integers p' and q' are taken prime. The whole construction is closely related to Naccache and Stern's encryption scheme [8]. In our case, we focus on base points of $E_n(0,b)$ of order a multiple of $\sigma = uv$. If G is such a point, then one could envision to encrypt some plaintext $m \in \mathbb{Z}_\sigma$ by

$$m \longmapsto m \cdot G + \sigma \cdot R \qquad \text{where} \quad R \in_R E_n(0,b) \ , \tag{3}$$

and decrypt by computing the residuosity class with respect to G. Because σ was chosen to be smooth, computing discrete logarithms for a base of degree σ can be efficiently done using the baby-step giant-step algorithm combined with Pohlig and Hellman's method. Thus, one can compute residuosity classes on $E_n(0,b)$ in polynomial time provided that μ is known, *i.e.* knowing the factors of n. There still remains the problem of randomly choosing an element $R \in_R E_n(0,b)$ during encryption: the spontaneous creation of an arbitrary point seems to require either the computation of a quadratic root of $R_x^3 + b$ with $R_x \in_R \mathbb{Z}_n$ (equivalent to the knowledge of the factors), or the computation of $\sqrt[3]{R_y^2 - b}$ with $R_y \in_R \mathbb{Z}_n$

(equivalent to RSA on $\mathbb{Z}_n^*$ with $e = 3$). An elegant solution[4] consists in modifying the encryption function so that $m \in \mathbb{Z}_\sigma$ is now encrypted as

$$m \longmapsto C = (m + \sigma r) \cdot G \qquad \text{with} \quad r \in_R \mathbb{Z}_n \, ,$$

and decryption necessitates to compute the discrete logarithm of $(\mu/\sigma) \cdot C$ with respect to the base $G' = (\mu/\sigma) \cdot G$, which is done as previously discussed since G' is of smooth order σ. The so-obtained probabilistic encryption scheme is described more precisely hereafter.

Our parameter generation process is very similar to Naccache and Stern's. One chooses two B-smooth integers u and v of product σ such that $\log \sigma = O(\log^\varepsilon n)$ with $\varepsilon > 0$. For practical use, one sets as in [8] $\lceil \log_2 \sigma \rceil = 160$ and $B \approx 2^{10}$. Prime numbers p and q are then generated according to equations 1 and 2. The choice of b is arbitrary in $\mathbb{Z}_n^*$: we recommend a small constant value such as $b = 1$ which renders point additions easier. The base point G can be chosen of maximal order $\mu = \text{lcm}(p + 1, q + 1)$, computed separately mod p and mod q, and recombined at the very end by Chinese remaindering.

Public key n, b, σ, G.

Private key (p, q) or $\mu = \text{lcm}(p + 1, q + 1)$.

Encryption plaintext $m \in \mathbb{Z}_\sigma$,
pick a random $r < n$,
ciphertext $C = (m + \sigma r) \cdot G$.

Decryption compute $u = (\mu/\sigma) \cdot C = m \cdot G'$.
Use Pohlig-Hellman and baby-step giant-step
to compute the discrete log of u in base G'.

Decryption can also be performed over $E_p(0, b)$ and $E_q(0, b)$: in this case, one separately computes $m \mod u$ and $m \mod v$. The plaintext m is then recovered modulo σ by Chinese remaindering.

2.2 Security Analysis

Clearly, inverting the encryption function of our scheme is equivalent to computing residuosity classes on $E_n(0, b)$, and the semantic security is equivalent to the decisional version of the same problem. By analogy with [8], we conjecture that these two problems are actually intractable.

Note also that the scheme can be made deterministic by setting $r = 0$ in the encryption function. We therefore have $C = m \cdot G$ like in Vanstone and Zuccherato's cryptosystem [23]. This variant is of moderate interest as it looses semantic security.

[4] alternatively, one can pick random coordinates for R and then select the coefficient b as $b = R_y^2 - R_x^3 \mod n$. During decryption, b is recovered by $b = C_y^2 - C_x^3$. In this event, the scheme relies on a *family* of curves, see [5].

2.3 Implementation Aspects

We analyze briefly the performances of our encryption scheme. Note first that since $E_p(0,b)$ and $E_q(0,b)$ are cyclic and G chosen of maximal order, the ciphertext space is $E_n(0,b)$ itself. The expansion rate is therefore $\rho = 2\lceil \log_2 n \rceil / \lceil \log_2 \sigma \rceil$ *i.e.* twice the one of Naccache and Stern's cryptosystem. This is due to the fact that the ciphertext has two coordinates modulo n. For instance, we have $\rho \approx 10$ when $\lceil \log_2 n \rceil = 768$ and $\lceil \log_2 \sigma \rceil = 160$. One way to increase the encryption bandwidth is to transmit only one ciphertext coordinate. Transmitting C_y, C_x is recovered before decryption by extracting the cubic root of $C_y^2 - b \mod n$. Transmitting C_x, decryption leads to exactly four message solutions: necessarily, 2 redundant bits have then to be included in the plaintext to eradicate any decryption ambiguity. This is similar to Rabin encryption [14].

3 Elliptic Curve Okamoto-Uchiyama Encryption

In this section, we show how to extend the setting defined in [9] to the one of elliptic curves. In particular, the technique we suggest addresses an open question described in [10].

It is known that curves $E_p(\overline{a},\overline{b})$ over $\mathbb{F}_p$ which have trace of Frobenius one (they are said to be anomalous) present the property that computing discrete logarithms on them is *very easy.* To be more precise, such an extraction requires a linear number of field operations over $\mathbb{F}_p$, *i.e.* $O(\log^3 p)$ bit operations. This was studied by several authors [20,19,22]. Okamoto *et al.* [10] attempted to take advantage of this feature to design an identity-based cryptosystem, but due to $|E_p(\overline{a},\overline{b})| = p$, we believe that this property can hardly be captured so directly into a properly secure encryption scheme. Instead, we extend the discrete logarithm recoverability property to a p-subgroup of $E_{p^2}(a,b)$ so that the projection onto $\mathbb{F}_p$ gives the *twist* of an anomalous curve. This is done as follows. We begin by stating a few useful facts that derive from Hasse's theorem.

Lemma 3. *Let* $E_p(\overline{a},\overline{b}) \ :\ y^2 = x^3 + \overline{a}x + \overline{b} \mod p$ *be an elliptic curve of order* $|E_p(\overline{a},\overline{b})| = p + 1 - t$ *where* $|t| \leq 2\sqrt{p}$. *Then for any integers* a, b *such that* $a = \overline{a} \mod p$ *and* $b = \overline{b} \mod p$, *we have*

$$|E_{p^2}(a,b)| = (p+1-t)(p+1+t) \ .$$

The curve $E_{p^2}(a,b)$ is usually said to be a lift of $E_p(\overline{a},\overline{b})$ to $\mathbb{F}_{p^2}$. One consequence of lemma 3 is that if $E_p(\overline{a},\overline{b})$ has $p+2$ points, then any lift $E_{p^2}(a,b)$ must be of order $p(p+2)$.

Lemma 4. *Let* $E_p(\overline{a},\overline{b})$ *be an elliptic curve over* $\mathbb{F}_p$ *of order* $p+2$. *Provided that* $p \equiv 2 \pmod 3$, *any lift* $E_{p^2}(a,b)$ *of* $E_p(\overline{a},\overline{b})$ *to* $\mathbb{F}_{p^2}$ *is cyclic.*

Proof. Let $E_{p^2}(a,b)$ be a non-cyclic lift of $E_p(\overline{a},\overline{b})$. From Rück's theorem [17], we know that $E_{p^2}(a,b) = \mathbb{Z}_{d_1} \times \mathbb{Z}_{d_2}$ with $d_1|d_2$, $d_1 > 1$ and $d_1|p^2-1$. By virtue of lemma 3, we must have $d_1 d_2 = p(p+2)$. Therefore, d_1 divides

$$\gcd(p+2, p^2-1) = \gcd(p+2, p-1) = \gcd(3, p-1) ,$$

which implies $d_1 = 3$ or 1. Since $d_1 \neq 1$ and $p = 2 + 3\eta$ for some integer η, we get the contradiction $3|(1+3\eta)$. Hence $E_{p^2}(a,b)$ must be cyclic. □

In what follows, p denotes a large prime verifying $p \equiv 2 \pmod 3$, $E_p(\overline{a},\overline{b})$ stands for a curve of order $p+2$ and $E_{p^2}(a,b)$ is some lift of $E_p(\overline{a},\overline{b})$ to $\mathbb{F}_{p^2}$. We note

$$E[p] = (p+2) \cdot E_{p^2}(a,b)$$

the (cyclic) p-torsion subgroup formed by the points of order dividing p, *i.e.* points of order p together with the point at infinity $\mathcal{O}_{p^2}$ of $E_{p^2}(a,b)$. We state:

Theorem 1. *There exist a polynomial time algorithm that computes discrete logarithms on $E[p]$ with complexity at most $O(\log^3 p)$.*

Proof. Since $E[p]$ is the group of p-torsion points of $E_{p^2}(a,b)$, we could apply Semaev's algorithm [20] *stricto sensu*. We rather rely on a (simpler) elliptic-log-based approach similar to Smart's [22] as follows. Observe that any point P belongs to $E[p]$ if (and only if) it is a lift of $\mathcal{O}_p \in E_p(\overline{a},\overline{b})$, wherefrom $E[p]$ is the kernel of the reduction map $P \mapsto P \mod p$. Hence the p-adic elliptic logarithm (see [21, p. 175])

$$\psi_p(x,y) = -\frac{x}{y} \mod p^2$$

is well-defined and can be applied on any point of $E[p]$. ψ_p being actually a morphism, if $P = m \cdot G$ stands for any arbitrary points $P, G \in E[p]$, we have

$$m = \frac{\psi_p(P)}{\psi_p(G)} \mod p ,$$

provided that $G \neq \mathcal{O}_{p^2}$. The main computational workload stands in the modular divisions which require at most $O(\log^3 p)$ bit operations. □

Note that other approaches such as Satoh and Araki's [19] or Rück [16], in application to our case, would have led to somehow equivalent computation methods.

3.1 Description

This section shows how to realize an analogue of Okamoto and Uchiyama's encryption scheme [9] on elliptic curves, in the sense wanted by the same authors in [10]. We make use of our previous results as follows.

One first chooses two large primes p (with $p \equiv 2 \pmod 3$) and q of bitsize k, and sets $n = p^2 q$. The user then picks integers $\overline{a_p}, \overline{b_p} \in \mathbb{F}_p$ such that $E_p(\overline{a_p}, \overline{b_p})$ is of order $p+2$, using techniques such as [7]. He then chooses some lift $E_{p^2}(a_p, b_p)$ of $E_p(\overline{a_p}, \overline{b_p})$ to $\mathbb{F}_{p^2}$, as well as a random curve $E_q(\overline{a_q}, \overline{b_q})$ defined over $\mathbb{F}_q$. Using Chinese remaindering, the user combines $E_{p^2}(a_p, b_p)$ and $E_q(\overline{a_q}, \overline{b_q})$ to get the curve $E_n = E_n(a, b)$ where $a, b \in \mathbb{Z}_n$. Finally, the user picks a point $G \in E_n$ of maximal order $\operatorname{lcm}(|E_{p^2}|, |E_q|)$ and sets $H = n \cdot G$. Our cryptosystem is as depicted below.

Public key $n = p^2 q$, E_n, G of maximal order, $H = n \cdot G$.

Private key p.

Encryption plaintext $m < 2^{k-1}$,
pick a random $r < 2^{2k}$,
ciphertext $C = m \cdot G + r \cdot H$

Decryption compute $m = \dfrac{\psi_p((p+2) \cdot C)}{\psi_p((p+2) \cdot G)} \mod p$.

Our system is very similar in spirit to Okamoto and Uchiyama's encryption as originally discovered. For this reason, most properties of their scheme still apply to ours: in particular, chosen ciphertext security can be easily shown equivalent to factoring $n = p^2 q$. The proof of this fact is a straightforward adaptation of Okamoto and Uchiyama's, see [9]. Besides, one-wayness and semantic security remain effective, except that they rely on problems related to high (p-degreed) residuosity on E_n instead of $\mathbb{Z}_n^*$. The scheme also features additive homomorphic properties for short messages.

4 Elliptic Curve Paillier Encryption

In this section, we refine the previous encryption technique to meet more advanced security requirements: we show how to construct an efficient yet natural embodiment of Paillier's cryptosystem [11] on elliptic curves. We first extend the setting of section 3 to curves defined over $\mathbb{Z}_{n^2}$ where $n = pq$. Suppose $E_{p^2}(a_p, b_p)$ (*resp.* $E_{q^2}(a_q, b_q)$) is some lift of a curve of trace $p+2$ (*resp.* $q+2$) defined over $\mathbb{F}_p$ (*resp.* $\mathbb{F}_q$). Considering $E_{n^2}(a, b)$ as the Chinese remaindering of $E_{p^2}(a_p, b_p)$ and $E_{q^2}(a_q, b_q)$ (hence it is defined over the ring $\mathbb{Z}_{n^2}$), it is easily seen that $E_{n^2}(a, b)$ is of order $n\mu$ where

$$\mu = \mu(n) = \operatorname{lcm}(p+2, q+2) .$$

We extend theorem 1 up to the present setting as follows. Noting

$$E[n] = \mu \cdot E_{n^2}(a, b) ,$$

we state:

Corollary 1 (of theorem 1). *There exist a polynomial time algorithm that computes discrete logarithms on $E[n]$ with complexity $O(\log^3 n)$.*

Proof. This is easily proven, either by applying theorem 1 twice on curves $E[p] \simeq E[n] \mod p^2$ and $E[q] \simeq E[n] \mod q^2$ and then by Chinese remaindering local logarithms, or more compactly by defining over $E[n]$ an n-adic elliptic logarithm

$$\psi_n(x, y) = -\frac{x}{y} \mod n^2 .$$

Provided that $P = m \cdot G$ for $P, G \in E[n]$ and $G \neq \mathcal{O}_{n^2}$, we retrieve m by computing

$$m = \frac{\psi_n(P)}{\psi_n(G)} \mod n .$$

□

Here is how the cryptosystem is initialized: the user chooses two large primes p and q (with $p \equiv q \equiv 2 \pmod 3$) and sets $n = pq$. He then picks up integers $\overline{a_p}$, $\overline{b_p} \in \mathbb{F}_p$ and $\overline{a_q}$, $\overline{b_q} \in \mathbb{F}_q$ such that $E_p(\overline{a_p}, \overline{b_p})$ is of order $p + 2$ and $E_q(\overline{a_q}, \overline{b_q})$ is of order $q + 2$. Lifted curves $E_{p^2}(a_p, b_p)$ and $E_{q^2}(a_q, b_q)$ are chosen and combined to get $E_{n^2} = E_{n^2}(a, b)$. Finally, a base point $G \in E_{n^2}$ is chosen of order divisible by n, possibly of maximal order $n\mu$.

Public key $n = pq$, E_{n^2}, G.

Private key $\mu = \mathrm{lcm}(p + 2, q + 2)$ or equivalently (p, q).

Encryption plaintext $m \in \mathbb{Z}_n$,
pick a random $r < n$,
ciphertext $C = (m + nr) \cdot G$

Decryption compute $m = \dfrac{\psi_n(\mu \cdot C)}{\psi_n(\mu \cdot G)} \mod n$.

Note that, due to lemma 4, the ciphertext space covers the entire curve E_{n^2} *i.e.* , any point of E_{n^2} is the image of some plaintext. We therefore have a maximal encryption bandwidth. This is obtained thanks to the fact that all curves we work with are cyclic.

4.1 Security Analysis

Here again, the very high resemblance of our encryption scheme with [11] implies that most cryptographic features happen to be identical in the two cases. The one-wayness of our scheme is equivalent to the problem of computing residuosity classes over E_{n^2} which, provided that n is hard to factor, we conjecture to be intractable[5]. Similarly, semantic security relates to the indistinguishability of n-residues of E_{n^2}, *i.e.* points belonging to $E[\mu] = n \cdot E_{n^2}$, from other points of the curve. We conjecture this problem to be intractable as well.

Our scheme is clearly malleable, and as such, does not resist adaptive chosen-ciphertext attacks. We believe, however, that security enhancement techniques such as [12] could be applied *mutatis mutandis* to meet provable security at the strongest level NM-CCA2.

[5] this is similar to the Composite Residuosity Assumption over $\mathbb{Z}^*_{n^2}$, see [11,12].

4.2 Implementation Aspects

Slight modifications of our encryption scheme may allow significant cost savings: a typical implementation speed-up is obtained by choosing a base point G of order $n\alpha$ with $\alpha = \alpha_p \alpha_q$, where

$$\alpha_p | \, p+2, \quad \alpha_p \not| \, q+2, \quad \alpha_q | \, q+2, \quad \alpha_q \not| \, p+2 \, ,$$

and $\lceil \log_2 \alpha \rceil$ is fixed to 160 for practical use. The decryption process is then advantageously replaced by

$$m = \frac{\psi_n(\alpha \cdot C)}{\psi_n(\alpha \cdot G)} \mod n$$

where the main computational workload is now a single scalar multiplication[6] by a short 160-bit constant. Chinese remaindering can also be used during decryption.

4.3 Homomorphic Properties

Our encryption scheme is $(+,+)$-homomorphic, *i.e.* an elliptic curve addition of two or several ciphertexts induces the implicit modular addition of the corresponding plaintexts. It also allows self-blinding, that is, provides the ability to publicly randomize a given ciphertext while conserving the correspondence with the initial plaintext. Finally, just like other known one-way trapdoor morphisms, the scheme provides random self-reducible encryption [3,18].

5 Conclusions

This paper introduced three new probabilistic encryption schemes on elliptic curves over rings. The cryptosystems are based on three specific trapdoor mechanisms allowing the recipient to recover discrete logarithms on different types of curves. More specifically, we showed how to design embodiments of Naccache-Stern, Okamoto-Uchiyama and Paillier discrete-log encryption schemes. Each provided cryptosystem is probabilistic and semantically secure relatively to the high residuosity problem associated with its curve type. We believe our work positively concretizes all previous research works on discrete log encryption in the elliptic curve setting.

6 Acknowledgements

The author is very grateful to Marc Joye who guided much of this research and to Moti Yung for various thoughts and discussions. I also thank the anonymous referees for their helpful and detailed comments.

[6] the value of $\psi_p(\alpha \cdot G)^{-1} \mod n$ can be pre-computed and stored before decryption takes place.

References

1. J. C. Benaloh. *Verifiable Secret-Ballot Elections.* PhD Thesis, Yale University, 1988.

2. D. Coppersmith. *Specialized Integer Factorization.* In Advances in Cryptology, Proceedings of Eurocrypt'98, LNCS 1403, Springer-Verlag, pp. 542–545, 1992.

3. J. Feigenbaum, S. Kannan and N. Nisan. *Lower Bounds on Random-Self-Reducibility.* In Proceedings of Structures 1990, 1990.

4. P-A. Fouque, G. Poupard, and J. Stern. *Sharing Decryption in the Context of Voting or Lotteries.* In Proceedings of Financial Cryptography '00, LNCS, Springer-Verlag, 2000.

5. K. Koyama, U. Maurer, T. Okamoto and S. Vanstone. *New Public-Key Schemes based on Elliptic Curves over the ring $\mathbb{Z}_n$.* In Advances in Cryptology, Proceedings of Crypto'91, LNCS 576, Springer-Verlag, pp. 252–266, 1992.

6. J. McKee and R. Pinch. *On a Cryptosystem of Vanstone and Zuccherato.* Preprint, 1998.

7. A. Miyaji. *Elliptic Curves over $\mathbb{F}_p$ Suitable for Cryptosystems.* In Advances in Cryptology, Proceedings of Auscrypt'92, LNCS 718, Springer-Verlag, pp. 479–491, 1993.

8. D. Naccache and J. Stern. *A New Cryptosystem based on Higher Residues.* In Proceedings of the 5th CCCS, ACM Press, pp. 59–66, 1998.

9. T. Okamoto and S. Uchiyama. *A New Public Key Cryptosystem as Secure as Factoring.* In Advances in Cryptology, Proceedings of Eurocrypt '98, LNCS 1403, Springer Verlag, pp. 308–318, 1998.

10. T. Okamoto and S. Uchiyama. *Security of an Identity-Based Cryptosystem and the Related Reductions.* In Advances in Cryptology, Eurocrypt'98, LNCS 1403, pp. 546–560, Springer Verlag, 1998.

11. P. Paillier. *Public-Key Cryptosystems Based on Composite-Degree Residuosity Classes.* In Advances in Cryptology, Eurocrypt'99, LNCS 1592, pp. 223–238, Springer Verlag, 1999.

12. P. Paillier and D. Pointcheval. *Efficient Public-Key Cryptosystems Provably Secure Against Active Adversaries.* In Advances in Cryptology, Asiacrypt'99, LNCS 1716, pp. 165–179, Springer Verlag, 1999.

13. G. Poupard and J. Stern. *Fair Encryption of RSA Keys.* In Advances in Cryptology, Eurocrypt'00, LNCS 1807, Springer Verlag, 2000.

14. M. O. Rabin. *Digital Signatures and Public-Key Encryptions as Intractable as Factorization.* MIT Technical Report No 212, 1979.

15. R. Rivest, A. Shamir, and L. Adleman. *A Method for Obtaining Digital Signatures and Public Key Cryptosystems.* Communications of the ACM, vol. 21, no. 2, pp. 120–126, 1978.

16. H.-G. Rück. *On the Discrete Logarithm in the Divisor Class Group of Curves.* Math. Comp, vol. 68, no. 226, pp. 805–806, 1999.

17. H.-G. Rück. *A Note on Eliiptic Curves over Finite Fields*. Math. Comp, vol. 49, no. 179, pp. 301–304, 1987.

18. T. Sander, A. Young and M. Yung. *Non-Interactive CryptoComputing for NC^1*. IEEE FOCS'99, 1999.

19. T. Satoh and K. Araki. *Fermat Quotient and the Polynomial Time Discrete Log Algorithm for Anomalous Elliptic Curves*. Preprint, 1997.

20. I. A. Semaev. *Evaluation of Discrete Logarithms in a Group of p-Torsion Points of an Elliptic Curve in Characteristic p*. Math. Comp., vol. 67, pp. 353-356, 1998.

21. J. H. Silverman. *The Arithmetic of Elliptic Curves*. Springer-Verlag, GTM 106, 1986.

22. N. Smart. *The Discrete Logarithm Problem on Elliptic Curves of Trace One*. Journal of Cryptology, vol. 12, no. 3, pp. 193–196, 1999.

23. S. Vanstone and R. Zuccherato. *Elliptic Curve Cryptosystem Using Curves of Smooth Order Over the Ring Z_n*. In IEEE Trans. Inf. Theory, vol. 43, no. 4, 1997.