An efficient semantically secure elliptic curve cryptosystem based on KMOV

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

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. The 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 curve, KMOV scheme.

1 Introduction

In 1984, Goldwasser and Micali [9] defined a new security notion that any encryption scheme should satisfy, namely indistinguishability of encryptions or semantic security (IND-CPA), 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 length, to a passive polynomial-time attacker. Nowadays, it is generally recognized that the right notion of security for a cryptosystem is indistinguishability against chosen ciphertext attack (IND-CCA). Nevertheless, the few cryptosystems that are IND-CCA and practical in the standard model (cf. [5, 6]) come from previous existing IND-CPA schemes in the standard model. On the other hand, IND-CPA security is still considered to deal with homomorphic encryption.

Recently, some new IND-CPA cryptosystems in the standard model have been introduced by Paillier [13] in 1999 and by Catalano *et al.* [2] in 2001. Both schemes are defined over the ring $\mathbb{Z}_{n^2}$. Paillier's scheme is the first homomorphic IND-CPA 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 (the third proposal in [14]) and Galbraith [8]. But, these schemes are impractical since they have a high computational cost, not only in encryption and decryption, but also in key generation.

In this paper we propose a new IND-CPA elliptic curve scheme which is based on factoring and efficient. To our knowledge there is no previous such elliptic curve cryptosystem in the literature enjoying both properties. The efficiency of our scheme is similar to existing IND-CPA elliptic curve schemes in the literature. In particular, the encryption time of our scheme is similar to the well-known El Gamal scheme over elliptic curves with standard parameters.

The proposal is inspired by some techniques in [2] and uses as underlying primitive the KMOV scheme [10], that is an analogue of RSA in the elliptic curve setting. So, as in [2], the resulting scheme is not homomorphic anymore. It uses elliptic curves over the ring $\mathbb{Z}_{n^2}$, where n is an 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 [2] is based.

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. The computational cost of the new scheme is discussed in section 5. Finally, section 6 contains some considerations about further research.

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 an extensive treatment on elliptic curves we refer to [15], and for an overview on elliptic curve cryptosystems, see [12].

Elliptic curves can be also 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 [8], 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: $(x, y) = (x : y : 1) \in E_{n^2}(a, b)$.
- Semi-infinite points: $(x : y : z) \in E_{n^2}(a, b)$, with $\gcd(z, n) = p$ or q.

Since semi-infinite points give a factorization of n, they will not be considered. The usual tangent-and-chord formulas allow to perform addition of affine points on $E_{n^2}(a, b)$. To deal with points at infinity the following addition formulas are used:

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

Finally, 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: Let $y' = y + \gamma n \in \mathbb{Z}_{n^2}$, where $\gamma \in \mathbb{Z}_n$. Then, (x,y') belongs to $E_{n^2}(a,b)$ if and only if

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

■

3 Some previous schemes

In this section we briefly recall Paillier's scheme and some of its variants. The original Paillier's scheme [13] 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, where RSA$[n,e]$ denotes the RSA function with exponent e. 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* [13].

In order to increase the efficiency of Paillier scheme, Catalano *et al.* [2] 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* [2].

In [8], 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. 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 [10] 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 an IND-CPA 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 us consider the sets $\Omega = \{(x,y) \in \mathbb{Z}_{n^2} \times \mathbb{Z}_{n^2}^* \mid y^2 - x^3 \in \mathbb{Z}_{n^2}^*\}$ and $\Lambda = \{(x,y) \in \mathbb{Z}_n \times \mathbb{Z}_{n^2}^* \mid y^2 - x^3 \in \mathbb{Z}_{n^2}^*\}$ and 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 $0 \leq x < n$, then $x = \overline{x}$ and the point (x,y) is obtained by Property 2.

4.1 Semantic security

The scheme is semantically secure under the following assumption:
Decisional Small-x e-Multiples assumption (DSM assumption).
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 polynomially indistinguishable

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

From now on 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 $g(D_1) \approx g(D_2)$.

Proposition 4 *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

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

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

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

Note that the distribution on the left side is $D_{\text{e-multiple}}$. 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 [15] (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 DSM assumption 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. 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 [4]. This result ensures that one can efficiently compute (i.e. in polynomial time) all roots x_0 of a polynomial $p \in \mathbb{Z}_N[x]$ with degree d such that $|x_0| < N^{1/d}$. Up to now, no improvement on this bound has been made. The result by Coppersmith implies we cand find the roots $|x_0| < n^{2/e^2}$ of the polynomial $P_e(x)$. Taking into account that in our case $e \geq 5$, this does not affect the validity of the DSM assumption.

5 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 $\bmod n^2$, because modular inverses can be computed within a constant number of modular multiplications. The main cost in encryption is due to the computation of $e\#P \in E_{n^2}(0, b)$. 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.

Then, the computational cost of ψ_e (in terms of modular multiplications modulo n^2) is $(11 + c/2)\lfloor \log_2 e \rfloor + 5$. Practical implementations, suggests than the value $c = 8$ can be taken (see [1]), so our scheme has an encryption cost of $15\lfloor \log_2 e \rfloor + 5$.

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. If our scheme is implemented with the standard exponent $e = 17$, we deduce from the above computations that the number of multiplications modulo n^2 needed is bounded by 65, but using the special form of the exponent, this number is trivially reduced to 44 multiplications modulo n^2.

It is interesting to compare our scheme with existing semantically secure ECC in the standard model over finite fields. 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 170 bits long, and our scheme is performed over $\mathbb{Z}_{n^2}^*$, where n is 1024 bits long (cf. [11]). We will express both encryption costs in terms of multiplications modulo n^2.

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 which 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 $3 \cdot 170 \cdot 12$ 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^2 is $\frac{170^2}{(2 \cdot 1024)^2}$. It follows that the encryption time of El Gamal ECC would be equivalent to 42 multiplications modulo n^2.

6 Further research

Recently, Catalano, Nguyen and Stern [3], have showed that the one-wayness of Catalano *et al.* scheme is equivalent to the one-wayness of the RSA$[n, e]$ primitive. It remains an open problem to study if this result extend to our scheme.

Security against adaptive chosen ciphertext attack, IND-CCA for short, can be given in the random oracle model applying some generic construction like [7]. Since at the present there is no practical IND-CCA scheme from the RSA$[n, e]$ problem in the standard model, it is very interesting to provide IND-CCA security in the standard model to Catalano *et al.* scheme [2] as well as to ours. To achieve this goal, the recent work of Cramer and Shoup [6] 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] 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.Catalano, P.Q. Nguyen and J. Stern. The Hardness of Hensel Lifting: The Case of RSA and Discrete Logarithm. *To appear in Proceedings of ASIACRYPT'02.* (2002)

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

[5] R. Cramer and V. Shoup. A Practical Public Key Cryptosystem Provably Secure against Adaptive Chosen Ciphertext Attack. *CRYPTO' 98, LNCS* **1462** 13–25 (1998).

[6] R. Cramer and V. Shoup. Universal Hash Proofs and a Paradigm for Adaptive Chosen Ciphertext Secure Public-Key Encryption. *EUROCRYPT '2002, LNCS* **2332** 45–64 (2002).

[7] E. Fujisaki and T. Okamoto. Secure integration of asymmetric and symmetric encryption schemes. *CRYPTO'99* LNCS **1666** 53–68 (2000).

[8] S. Galbraith. Elliptic curve Paillier schemes. *Journal of Cryptology* **15** (2) 129–138 (2002).

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

[10] 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).

[11] A. K. Lenstra and E. R. Verheul. Selecting Cryptographyc Key Sizes. http://cryptosavvy.com/cryptosizes.pdf

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

[13] P. Paillier. Public-Key Cryptosystems Based on Composite Degree Residuosity Classes. *EUROCRYPT '99, LNCS* **1592** 223–238 (1999).

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

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