A semantically secure elliptic curve RSA scheme with small expansion factor

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

June 27, 2002

Abstract

We propose an elliptic curve scheme over the ring $\mathbb{Z}_{n^2}$, which is efficient and semantically secure in the standard model, and it has expansion factor 2 (previous schemes with similar features present expansion factors greater or equal than 4). Demytko's RSA type 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 Root Assumption. Confidence on this assumption is also discussed.

Keywords: public-key cryptography, semantic security, expansion factor, elliptic curves, Demytko's 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, and they proposed a scheme with this property. This notion informally says that a ciphertext does not leak any useful information about the plaintext, except its lenght, to a polynomial-time attacker. This security notion becomes a standard requirement for the design of new cryptosystems. Stronger security notions introduced later (e.g. non-malleability, plaintext awareness) can not be considered as general requirements since they preclude homomorphic encryption.

A relevant parameter for encryption schemes is the *expansion factor*, that is, the ratio between the lengths of the ciphertext and the plaintext. The use of large expansion factors leads to decreasing the effective bandwith in secure communications. Some of the known semantically secure cryptosystems achieve expansion factor 2, that is optimal when the encryption uses as much randomness as the message length. Nevertheless, all semantically secure elliptic curve cryptosystems in the literature have expansion factor greater or equal than 4.

In this paper we propose an efficient and semantically secure elliptic curve cryptosystem with expansion factor 2. To our knowledge there is no previous elliptic curve cryptosystem based on factoring enjoying these properties. The design of our scheme is based on [8] but using as underlying primitive the Demytko's scheme [6], instead of [10]. This enables to use elliptic curves with arbitrary parameters to design the scheme, in contrast with [8], where only supersingular curves were possible.

The new proposed cryptosystem 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 Root Assumption. In some sense, this assumption is analogous to the one on which Catalano et al. scheme [3] is based.

In terms of efficiency, our proposal is efficient, specially in ciphering. Although it is slower than Catalano et al. cryptosystem [3], ours is much faster than the existing elliptic curve semantically secure schemes, such as [7, 13].

The rest of the paper is organised as follows. Section 2 briefly recalls Demytko's scheme. In section 3, 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 4. Finally, section 5 contains the conclusions.

For a brief description of the results about elliptic curves over the ring $\mathbb{Z}_{n^2}$ used in this paper see [8].

2 Demytko's scheme revisited

Demytko proposed in [6] an elliptic curve RSA based scheme. He uses a fixed randomly chosen elliptic curve $E_n(a, b)$ over the ring $\mathbb{Z}_n$, where $n = pq$ is an RSA modulus. Let $t_p = p+1-|E_p(a, b)|$, $t_q = q+1-|E_q(a, b)|$ and e an (small) integer such that

$$\gcd(e, p+1 \pm t_p) = \gcd(e, q+1 \pm t_q) = 1\ . \tag{1}$$

Let

$$\Lambda_{a,b} = \{x \in \mathbb{Z}_n^* \mid x^3 + ax + b \in \mathbb{Z}_n^*\}.$$

Demytko considered a set $\mathcal{E}$ of four elliptic curves related to $E_n(a, b)$, including itself. These curves are usually referred as the *quadratic twists of* $E_n(a, b)$, and their number of points have the form $(p+1 \pm t_p)(q+1 \pm t_q)$. The main feature is that for all $m \in \Lambda_{a,b}$ there exists a unique curve in $\mathcal{E}$ with exactly four points

with x-coordinate m, i.e of the form (m, y), with $y \in \mathbb{Z}_n^*$. Moreover, the x-coordinate of the multiple $e\#(m, y)$, computed on the corresponding curve, is the same for the four values of y and can be computed without knowing any of them. We will hereafter denote by $e \star m$ the x-coordinate of multiple $e\#(m, y)$ for any of the four possible values of y.
It can be proved that the map

$$\begin{array}{rccc} \mathcal{D}_e : & \Lambda_{a,b} & \longrightarrow & \Lambda_{a,b} \\ & m & \longmapsto & e \star m \end{array}$$

is well defined and bijective, since an e satisfying (1) is coprime with the number of points of any of the four curves in $\mathcal{E}$.

In Demytko's scheme, the ciphertext c for a message $m \in \Lambda_{a,b}$ is $c = e \star m$. The ciphertext c can be efficiently computed, for almost all $m \in \Lambda_{a,b}$, as $c = \Phi_e(m) \bmod n$, where the rational function Φ_e is recursively defined as:

$$\Phi_1 = x$$

$$\Phi_{2k} = \frac{(\Phi_k^2 - a)^2 - 8b\Phi_k}{4(\Phi_k^3 + a\Phi_k + b)}$$

$$\Phi_{2k+1} = \frac{2(a - \Phi_k\Phi_{k+1})(\Phi_k + \Phi_{k+1}) + 4b}{(\Phi_{k+1} - \Phi_k)^2} - x$$

The above formulae can only fail for x corresponding to points (x, y) with order less or equal than e, that are a negligible subset of $\Lambda_{a,b}$, when e is small. Besides, such points can be totally supressed by taking $E_n(a, b)$ such that $p + 1 \pm t_p$ and $q + 1 \pm t_q$ have no divisor between 3 and e (e.g. $t_p = t_q = 0$, $p = 2p' - 1$, $q = 2q' - 1$ and p', q' primes).

In [6] it is conjectured that Φ_e is a one-way trapdoor permutation with trapdoor p, q and the four inverses of e modulo $\mathrm{lcm}(p + 1 \pm t_p, q + 1 \pm t_q)$.

To decrypt the ciphertext $c \in \Lambda_{a,b}$, it suffices to compute $m = d \star c$, where d is one of the four inverses of e. The Jacobi symbols $(c^3 + ac + b/p)$ and $(c^3 + ac + b/q)$ easily determine which inverse must be used.

If we restrict the above scheme to supersingular curves (i.e. $t_p = t_q = 0$), there is only one value of d involved and no Jacobi symbol computation is needed in the decryption process, and therefore the values of p and q are not explicitly used in decryption (except for improving speed by using the Chinese Remainder Theorem).

3 The new scheme

Applying the ideas in [8], one can add semantic security to Demytko's scheme without loosing efficiency and achieving the same expansion factor as in Paillier or OAEP-RSA schemes [12, 1] .

Let

$$\Omega_{a,b} = \{x \in \mathbb{Z}^*_{n^2} \mid x^3 + ax + b \in \mathbb{Z}^*_{n^2}\}$$

Notice that $\Omega_{a,b} = \{z + mn \mid z \in \Lambda_{a,b},\ m \in \mathbb{Z}_n\}$. Let us consider the function

$$\begin{array}{rcl} \Theta_e : \Lambda_{a,b} \times \mathbb{Z}_n & \longrightarrow & \Omega_{a,b} \\ (r, m) & \longrightarrow & \Phi_e(r) + mn \bmod n^2 \end{array}$$

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

Proof: Θ_e is well defined since $\Theta_e(r, m) \equiv \mathcal{D}_e(r) \bmod n$, and $\mathrm{Im}(\mathcal{D}_e) = \Lambda_{a,b}$. Also, due to the bijectivity of $\mathcal{D}_e$, $\Theta_e(r_1, m_1) = \Theta_e(r_2, m_2)$ implies that $r_1 \equiv r_2 \bmod n$, that is $r_1 = r_2$. Therefore $m_1 = m_2$. ∎

In the sequel we describe the proposed new scheme:

Key generation. Given a security parameter ℓ, choose at random two different primes p and q with ℓ bits, a random elliptic curve $E_{n^2}(a, b)$, where $n = pq$, and an integer e such that $\gcd(e, pq) = \gcd(e, p + 1 \pm t_p) = \gcd(e, q + 1 \pm t_q) = 1$, where $t_p = p + 1 - |E_p(a, b)|$ and $t_q = q + 1 - |E_q(a, b)|$.
Then the public key is $\mathrm{PK} = (n, e, a, b)$, and the secret key is

$$\mathrm{SK} = (p, q, d_1, d_2, d_3, d_4),$$

where $d_i = e^{-1} \bmod \mathrm{lcm}(p + 1 \pm t_p, q + 1 \pm t_q)$.

Encryption. To encrypt a message $m \in \mathbb{Z}_n$ we compute $c = \Theta_e(r, m)$, where r is uniformly chosen in $\Lambda_{a,b}$.

Decryption. To recover the message m from $c = \Phi_e(r) + mn$, notice that $c \equiv \mathcal{D}_e(r) \bmod n$, and r is obtained from $c \bmod n$ as in Demytko's scheme. Now, m is easily obtained from $mn = c - \Phi_e(r) \bmod n^2$.

As a particular case, the size of private key as well as decryption complexity can be reduced if supersingular curves are used. Then, $t_p = t_q = 0$ and only one value of d is needed to recover r from $c \bmod n$.

3.1 Semantic security

Probabilistic notation.
If A is a non-empty set, then $x \in_{\mathrm{R}} A$ denotes that x has been uniformly chosen in A. If D_1 and D_2 are two probability distributions, then the notation $D_1 \approx D_2$ means that D_1 and D_2 are polinomally indistinguishable. Notice that if g is a bijection such that g and g^{-1} can be computed in probabilistic polynomial time,

then $D_1 \approx D_2$ is equivalent to $g(D_1) \approx g(D_2)$.

Our scheme is semantically secure under the following assumption:

Decisional Small Root Assumption (DSRA).
Let p, q be randomly chosen ℓ-bit long different primes, $n = pq$, $E_{n^2}(a, b)$ a randomly chosen elliptic curve and e an integer such that $\gcd(e, n) = \gcd(e, p+1\pm t_p) = \gcd(e, q+1\pm t_q) = 1$, *where* $t_p = p+1-|E_p(a, b)|$, $t_q = q+1-|E_q(a, b)|$.
The following probability distributions are polinomially indistinguishable

$$\begin{aligned} D_{\mathrm{small-x}} &= (n, a, b, \Phi_e(x) \bmod n^2) \quad \text{where } x \in_{\mathrm{R}} \Lambda_{a,b} \\ D_{\mathrm{random}} &= (n, a, b, x') \qquad \text{where } x' \in_{\mathrm{R}} \Omega_{a,b}. \end{aligned}$$

Proposition 2 *The proposed scheme is semantically secure if and only if DSRA 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

$$\begin{aligned} D_0 &= (n, a, b, \Phi_e(x) + m_0 n \bmod n^2) \quad \text{where } x \in_{\mathrm{R}} \Lambda_{a,b}\,, \quad \text{and} \\ D &= (n, a, b, \Phi_e(x) + mn \bmod n^2) \quad \text{where } x \in_{\mathrm{R}} \Lambda_{a,b},\ m \in_{\mathrm{R}} \mathbb{Z}_n, \end{aligned}$$

are polynomially indistinguishable, which is equivalent to

$$(n, a, b, \Phi_e(x) \bmod n^2) \approx (n, a, b, \Phi_e(x){+}m'n \bmod n^2), \quad \text{with } x \in_{\mathrm{R}} \Lambda_{a,b},\ m' \in_{\mathrm{R}} \mathbb{Z}_n\,.$$

Note that the distribution on the left side is $D_{\mathrm{small-x}}$.
Besides, since $\Phi_e(x) + m'n \bmod n^2 = \Theta_e(x, m')$, and Θ_e is a bijection, then D and D_{random} are identically distributed. ■

3.2 Hardness of the Small Root Problems

In this subsection we argue why one should be confident on the hardness of the new decisional problem presented in this paper. From [15] (Section 3, ex. 3.7) one proves that

$$\Phi_e(x) = \frac{\nu_e(x)}{\eta_e(x)}$$

where $\nu_e(x)$ and $\eta_e(x)$ are relatively prime polynomials such that,

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

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

Thus, given $t = \Phi_e(x_0) \bmod n^2$, x_0 is a root of the polynomial $\nu_e(x) - t\eta_e(x) \in \mathbb{Z}_{n^2}[x]$, whose degree is e^2. Then, DSRA is equivalent to the assumption that it is infeasible deciding if the polynomial $\nu_e(x) - t\eta_e(x) \in \mathbb{Z}_{n^2}[x]$, with $t \in_{\mathrm{R}} \mathbb{Z}_{n^2}$, has a root smaller than n, for random n, a and b.

Similarly, the semantic security of Catalano et al. scheme is related to the difficulty of deciding if the polynomial $x^e - t \in \mathbb{Z}_{n^2}[x]$, with $t \in_{\mathrm{R}} \mathbb{Z}_{n^2}$, has a root smaller than n. After Coppersmith's result [4], it makes sense to use the degree of the polynomial as a security parameter to compare both schemes. Therefore, our scheme with parameter e could achieve the same security level than Catalano et al. scheme with exponent e^2.

4 Efficiency analysis

In this section, we compare the computational encryption cost of our scheme and the efficient Catalano et al. scheme, at the same security level (i.e. the same degree of the polynomials involved in the security assumptions).

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. Then, we compare the computational costs of evaluating $\Phi_e(r) \bmod n^2$ and $r^{e^2} \bmod n^2$.

It is not possible to use the same addition chains in both computations. We will suppose that the *binary algorithm* is used to evaluate $r^{e^2} \bmod n^2$. Then, $2\lfloor \log_2 e \rfloor$ modular squares and 2 modular multiplications modulo n^2 are needed in the best case (i.e. $e = 2^s + 1$).

In the same case, $e = 2^s + 1$, the computation of $\Phi_e(r) \bmod n^2$ requires $\lfloor \log_2 e \rfloor$ evaluations of the formula for Φ_{2k+1} and $\lfloor \log_2 e \rfloor - 1$ evaluations of the formula for Φ_{2k}. Both rules involve the computation of one inverse modulo n^2. 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 $\bmod n^2$ 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, our encrypting function requires about $(12 + c/2)\lfloor \log_2 e \rfloor$ multiplications modulo n^2 compared to $2\lfloor \log_2 e \rfloor$ required by Catalano et al. encrypting function in the best case. Practical implementations suggest that the value $c = 8$ can be taken (see [2]), so our scheme is about 8 times slower compared with the best case for Catalano et al. scheme at the same security level. This is a low computational cost if we compare it with previous semantically secure elliptic curve cryptosystems based on factoring [13, 7].

5 Conclusions and further research

In this paper we have presented a new elliptic curve based scheme over the ring $\mathbb{Z}_{n^2}$, with n an RSA modulus. We prove that the scheme is semantically secure under a new decisional assumption. The new scheme has been designed applying to Demytko's scheme techniques that are similar to those applied by Catalano et al. [3] to RSA scheme. One of the advantages is that the scheme can be performed on arbitrary elliptic curves. As far as we know, this is the first proven semantically secure elliptic curve cryptosystem based on factoring that is efficient, both in key generation (if supersingular curves are used) as well as in encryption/decryption procedures, with expansion factor 2. A lower encryption cost can be achieved if the scheme is designed over a *Montgomery form* elliptic curve (see [11]), and we estimate that the computational cost is reduced in a 50% approximately.

Security against adaptive chosen ciphertext attack, IND-CCA for short, can be given in the random oracle model applying the technique introduced by Pointcheval in [14]. It would be interesting to provide IND-CCA security in the standard model to Catalano et al. scheme as well as to ours. To achieve this goal, the recent work of Cramer and Shoup [5] could provide useful ideas.

Since the publication of Paillier's crytosystem [12], several new decisional assumptions have been formulated (e.g in [3],[7],[8]). There is little knowledge about the validity of these assumptions, and a careful study of it would be worthwhile.

References

[1] M. Bellare and P. Rogaway. Optimal asymmetric encryption. *EUROCRYPT '94, LNCS* **950** 92–111 (1995).

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

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

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

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

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

[8] D. Galindo, S. Martín, P. Morillo and J. L. Villar. An efficient semantically secure elliptic curve cryptosystem based on KMOV scheme. Cryptology ePrint Archive, Report 2002/037. http://eprint.iacr.org/.

[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] Montgomery, P.L. Speeding the Pollard and Elliptic Curve Methods of Factorizations. *Math. Comp.* **48** 243–264 (1987).

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

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

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

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