Published in R. Whright and P. Neumann, Eds., *Network Threats*, DIMACS Series in Discrete Mathematics and Theoretical Computer Science, vol. 38, pp. 21–31, American Mathematical Society, 1998.

CRYPTANALYSIS OF RSA-TYPE CRYPTOSYSTEMS: A VISIT

MARC JOYE AND JEAN-JACQUES QUISQUATER

Abstract. This paper surveys RSA-type implementations based on Lucas sequences and on elliptic curves. The main focus is the way how some known attacks on RSA were extended to LUC, KMOV and Demytko's system. It also gives some directions for the choice of the most appropriate RSA-type system for a given application.

1. Introduction

In 1978, Rivest, Shamir and Adleman [63] introduced the so-called RSA cryptosystem. Its security mainly relies on the difficulty of factoring carefully chosen large integers.

After this breakthrough, other structures were proposed to produce analogues to RSA. So, Müller and Nöbauer [54, 55] presented a cryptosystem using Dickson polynomials. This system was afterwards slightly modified and rephrased in terms of Lucas sequences by Smith and Lennon [70, 72]. More recently, Koyama, Maurer, Okamoto and Vanstone [41] exhibited new one-way trapdoor functions similar to RSA on elliptic curves, the so-called KMOV cryptosystem. Later, Demytko [20] also pointed out a new one-way trapdoor function on elliptic curves to produce an analogue of RSA.

There are numerous mathematical attacks on RSA. They can basically be classified into three categories independently of the protocol in use for encryption or signature:

1. attacks exploiting the polynomial structure of RSA [11, 14, 25, 29, 47, 57];
2. attacks based on its homomorphic nature [2, 7, 15, 17, 19, 22, 21, 16, 26];
3. attacks resulting of a bad choice of parameters [74].

Most of known attacks on RSA can more or less successfully be extended to their Lucas and elliptic curves based analogues. Rather than reviewing in details all the attacks, we have chosen three representative attacks (one per category) and explain how there were extended. This enables the reader to evaluate the potential danger of a future attack on a RSA-type cryptosystem.

The first category of attacks relies on the polynomial structure of RSA. Since Lucas sequences can be expressed in terms of Dickson polynomials, all these attacks can almost straightforwardly be adapted. Using division polynomials, the same conclusion holds for elliptic curves based cryptosystems. The GCD attack [14] falls into this category.

The second type of attacks does not extend so easily to LUC or Demytko's system, because their non homomorphic nature. Therefore, they apparently seem to be resistant. However, multiplicative attacks can sometimes be rewritten in

1991 *Mathematics Subject Classification.* Primary 94A60, 11T71; Secondary 11B39, 14H52.

order to be applicable on these latter systems. We shall illustrate this topic with the common modulus attack [68].

The last category of attacks does not really result from a weakness of RSA but rather from a bad implementation. Parameters have to be carefully chosen. Unfortunately, there is no general recipe to extend this kind of attack. In some cases, attacks remain valid like for the low secret exponents attack [74].

The remaining of this paper is organized as follows. In Section 2, we review the Lucas-based cryptosystems, and the elliptic curves RSA cryptosystems in Section 3. Next, in Section 4, we present the GCD attack, the common modulus failure and the Wiener's attack. We also outline the way they were extended. Finally, we conclude in Section 5.

2. Lucas-based cryptosystems

We assume that the reader is familiar with the basic properties of RSA.

2.1. **Lucas sequences.**

Definition 2.1. Let P and Q be integers, and let α be a root of the polynomial $x^2 - Px + Q$ in the quadratic field $\mathbb{Q}(\sqrt{\Delta})$, where $\Delta = P^2 - 4Q$ is a non-square. Writing $\alpha = \frac{P+\sqrt{\Delta}}{2}$ and its conjugate $\beta = \frac{P-\sqrt{\Delta}}{2}$, the *Lucas sequences* $\{U_n\}_{n\geq 0}$ *and* $\{V_n\}_{n\geq o}$ are given by

$$U_n(P,Q) = \frac{\alpha^n - \beta^n}{\alpha - \beta} \quad \text{and} \quad V_n(P,Q) = \alpha^n + \beta^n. \tag{2.1}$$

In particular, $U_0 = 0$, $U_1 = 1$, $V_0 = 2$ and $V_1 = P$.

Proposition 2.2. *Let $U_i(P,Q)$ and $V_i(P,Q)$, the i^{th} terms of the Lucas sequences with parameters P, Q and $\Delta = P^2 - 4Q$. Then,*

$$V_k^2(P,Q) - \Delta U_k^2(P,Q) = 4Q^k, \tag{2.2}$$

$$U_{mk}(P,Q) = U_k(P,Q)U_m\left(V_k(P,Q), Q^k\right), \tag{2.3}$$

$$V_{mk}(P,Q) = V_m\left(V_k(P,Q), Q^k\right), \tag{2.4}$$

$$2U_{m+k}(P,Q) = U_m(P,Q)V_k(P,Q) + U_k(P,Q)V_m(P,Q), \tag{2.5}$$

$$2V_{m+k}(P,Q) = V_m(P,Q)V_k(P,Q) + \Delta U_m(P,Q)U_k(P,Q). \tag{2.6}$$

□

Proposition 2.3. *Let $\Psi(p) = p - (\Delta/p)$, where p is a prime that does not divide 2Δ. Then,*

$$U_{k\Psi(p)+1}(P,1) \equiv U_1(P,1) = 1 \pmod{p}, \tag{2.7}$$

$$V_{k\Psi(p)+1}(P,1) \equiv V_1(P,1) = P \pmod{p}. \tag{2.8}$$

□

Identity (2.8) enables to construct a RSA-like cryptosystem based on Lucas sequences with parameters P, $Q = 1$ and $\Delta = P^2 - 4$.

2.2. **LUC** [70, 72]**.** Each user chooses two large primes p and q, and publishes the product $n = pq$. Next, he chooses a public encryption key e that is relatively prime to $(p-1)$, $(p+1)$, $(q-1)$ and $(q+1)$. Finally, he computes the secret decryption key d according to

$$ed \equiv 1 \pmod{\Psi(n)}, \tag{2.9}$$

where $\Psi(n) = \ell\mathrm{cm}(p-(\Delta/p), q-(\Delta/q))$.

To send a message m to Bob, Alice looks to Bob's public key e and computes the ciphertext $c = V_e(m,1) \bmod n$. Next, to recover the plaintext m, Bob uses his secret decryption key d to obtain

$$m = V_d(c,1) \bmod n. \tag{2.10}$$

Proof. From Equation (2.4) and Proposition 2.3, we have

$$V_d(c,1) \equiv V_d\big(V_e(m,1),1\big) \equiv V_{de}(m,1) \equiv m \pmod{n}.$$

□

Apparently, the drawback in this method is that d depends on the message m because $\Delta = m^2 - 4$. In fact, according to the values of (Δ/p) and (Δ/q), there are four possibilities for d that satisfy relation (2.9). However, the decryption key corresponding to a given message can be determined *a priori* since

$$\begin{aligned}
\Psi(n) &= \ell\mathrm{cm}\big(p-(\Delta/p), q-(\Delta/q)\big) \\
&= \ell\mathrm{cm}\left(p-(\Delta U_e^2(m,1)/p), q-(\Delta U_e^2(m,1)/q)\right) \\
&= \ell\mathrm{cm}\left(p-\left(\frac{c^2-4}{p}\right), q-\left(\frac{c^2-4}{q}\right)\right), \text{ by Eq. (2.2).}
\end{aligned}$$

Remark 2.4. It is possible to construct a message independent cryptosystem, taking d such that $ed \equiv 1 \pmod{\ell\mathrm{cm}(p-1, p+1, q-1, q+1)}$. This method avoids the computation of the two Legendre symbols in the expression of $\Psi(n)$, but it doubles the length of the deciphering key, on average.

3. Elliptic curves RSA cryptosystems

3.1. **Basic facts.**

Definition 3.1. Let K be a field of characteristic $\neq 2, 3$, and let x^3+ax+b (where $a, b \in K$) be a cubic with no multiple roots. An *elliptic curve* $E(a,b)$ *over* K is the set of points $(x,y) \in K \times K$ satisfying the equation

$$y^2 = x^3 + ax + b \tag{3.1}$$

together with a single element denoted $\mathcal{O}$ and called the *point at infinity.*

Let $\mathbf{P}, \mathbf{Q} \in E(a,b)$, let ℓ be the line connecting $\mathbf{P}$ and $\mathbf{Q}$ (tangent line if $\mathbf{P} = \mathbf{Q}$), and let $\mathbf{T}$ be the third point of intersection of ℓ with $E(a,b)$. If ℓ' is the line connecting $\mathbf{T}$ and $\mathcal{O}$, then $\mathbf{P}+\mathbf{Q}$ is the point such that ℓ' intersects $E(a,b)$ at $\mathbf{T}, \mathcal{O}$ and $\mathbf{P}+\mathbf{Q}$.

Proposition 3.2. *The previous composition law makes* $E(a,b)$ *into an Abelian group with identity element* $\mathcal{O}$*.* □

Theorem 3.3 (Hasse)**.** *If K is the prime finite field $\mathbb{F}_p$, then the order m of the group $E_p(a,b)$ (i.e. the elliptic curve $E(a,b)$ over $\mathbb{F}_p$) is given by*

$$\#E_p(a,b) = p + 1 - a_p, \tag{3.2}$$

where $|a_p| \leq 2\sqrt{p}$. □

Definition 3.4. Let $E_p(a,b)$ be an elliptic curve over the prime field $\mathbb{F}_p$. The *complementary group* of $E_p(a,b)$ is the set of points satisfying relation (3.1) together with $\mathcal{O}$, where y is of the form $u\sqrt{v}$, and v is a fixed non-quadratic residue modulo p and $v \in \mathbb{F}_p$. The complementary group of $E_p(a,b)$ will be denoted $\overline{E_p(a,b)}$.

Corollary 3.5. *If $\#E_p(a,b) = 1 + p - a_p$, then $\#\overline{E_p(a,b)} = 1 + p + a_p$.* □

For some special cases, the order and the structure of an elliptic curve can easily be determined.

Lemma 3.6. *Let p be an odd prime congruent to* 2 mod 3*. Then the elliptic curve $E_p(0,b)$ is a cyclic group of order $p+1$.* □

Lemma 3.7. *Let p be a prime congruent to* 3 mod 4*. If a is a quadratic residue modulo p, then $E_p(a,0)$ is a cyclic group of order $p+1$. If a is a non quadratic residue modulo p, then $E_p(a,0)$ is a group isomorphic to $\mathbb{Z}_{(p+1)/2} \times \mathbb{Z}_2$ of order $p+1$.* □

3.2. **Elliptic curves over the ring $\mathbb{Z}_n$.** In this paragraph, n will denote the product of two large distinct primes p and q.

Definition 3.8. Like the definition over the field $\mathbb{F}_p$, an *elliptic curve $E_n(a,b)$ over the ring $\mathbb{Z}_n$* is the set of the points $(x,y) \in \mathbb{Z}_n \times \mathbb{Z}_n$ satisfying the equation

$$y^2 = x^3 + ax + b \pmod{n} \tag{3.3}$$

together with the point $\mathcal{O}$.

However, the resulting structure is not a group ; nevertheless a proposition similar to Lagrange's theorem holds.

Proposition 3.9. *Let $E_n(a,b)$ be an elliptic curve over $\mathbb{Z}_n$ such that* $\gcd(4a^3 + 27b^2, n) = 1$*. If $N_n = \ell\mathrm{cm}(\#E_p(a,b), \#E_q(a,b))$, then*

$$\forall \mathbf{P} \in E_n(a,b), \forall k \in \mathbb{Z} : (kN_n + 1)\mathbf{P} = \mathbf{P}. \tag{3.4}$$

□

It is possible (but very unlikely) that the addition of two points on $E_n(a,b)$ is undefined. In practice, this will cause no problem, because the probability of finding two points such that their sum is undefined is the same than finding the two prime factors of n.

Proposition 3.9 seems to establish a RSA-type cryptosystem. However, some problems occur. Suppose that Alice wants to send message m to Bob. Bob fixes an elliptic curve $E_n(a,b)$ over $\mathbb{Z}_n$ and computes $N_n = \ell\mathrm{cm}(\#E_p(a,b), \#E_q(a,b))$. He chooses a public key e that is relatively prime to N_n, and computes d such that $ed \equiv 1 \pmod{N_n}$. The values of e and n, and the elliptic curve $E_n(a,b)$ are public. To encode the message m, Alice represents it, in a publicly known way,

as a point $\mathbf{M}$ of the elliptic curve $E_n(a,b)$ (by adding redundancy, for example). Then she computes $\mathbf{C} = e\mathbf{M}$ and sends $\mathbf{C}$ to Bob. To recover the message m, Bob uses his secret key d to compute $d\mathbf{C} = de\mathbf{M} = \mathbf{M}$. This scheme is *not* correct because several messages may be represented by the same point $\mathbf{M}$. Therefore, Proposition 3.9 can only be used to construct a signature scheme. Another idea is to let Alice choosing the parameters a and b of the elliptic curve in order to uniquely represent m as a point of the curve. But in that case, N_n (which has to be re-computed by Bob) is not necessarily coprime to e. To overcome these drawbacks, new schemes were proposed.

3.3. **KMOV** [41]**.** The KMOV system relies on Lemma 3.6. Each user chooses two primes p and q both congruent to 2 modulo 3, and publishes their product $n = pq$. Next, he selects a public key e relatively prime to $N_n = \ell\mathrm{cm}(p+1, q+1)$ and computes the secret key d such to

$$ed \equiv 1 \pmod{N_n}. \tag{3.5}$$

To send a message $\mathbf{M} = (m_1, m_2)$ to Bob, Alice chooses the parameter b according to

$$b = m_2^2 - m_1^3 \bmod n. \tag{3.6}$$

Next, using Bob's public key e, she encrypts $\mathbf{M} \in E_n(0,b)$ as $\mathbf{C} = e\mathbf{M} = (c_1, c_2)$, and sends it to Bob. From $\mathbf{C}$, Bob computes the parameter $b = c_2^2 - c_1^3 \bmod n$. Then, he recovers the original message with its secret key d by computing $\mathbf{M} = d\mathbf{C}$ on the curve $E_n(0,b)$.

Remark 3.10. As mentioned in [41], from Lemma 3.7, it is also possible to work on a curve of the form $E_n(a,0)$ by choosing

$$a = \frac{m_2^2 - m_1^3}{m_1} \bmod n. \tag{3.7}$$

3.4. **Demytko** [20]**.** In this cryptosystem, each user chooses once for all the parameters a, b and e. Let m be the message to be encoded. The Demytko's system is based on the fact that if m (modulo p) is not the x-coordinate of a point on $E_p(a,b)$, it will be the x-coordinate of a point on the twisted curve $\overline{E_p(a,b)}$.

It is useful to introduce some notation. Since the computation of the y-coordinate can be avoided (by using the algorithm described in [8], for example), $k \star p_x$ will denote the x-coordinate of k times the point $\mathbf{P} = (p_x, p_y)$. To encrypt m, Alice computes $c = e \star m$. To decrypt the ciphertext c, Bob computes $d_i \star c = d_i e \star m = m$, where the decryption key is chosen according to

$$ed_i \equiv 1 \pmod{N_{n,i}} \quad (i = 1, \ldots, 4) \tag{3.8}$$

with

$$\begin{cases} N_{n,1} = \ell\mathrm{cm}(p+1-a_p, q+1-a_q) & \text{if } (w/p) = 1 \text{ and } (w/q) = 1 \\ N_{n,2} = \ell\mathrm{cm}(p+1-a_p, q+1+a_q) & \text{if } (w/p) = 1 \text{ and } (w/q) \neq 1 \\ N_{n,3} = \ell\mathrm{cm}(p+1+a_p, q+1-a_q) & \text{if } (w/p) \neq 1 \text{ and } (w/q) = 1 \\ N_{n,4} = \ell\mathrm{cm}(p+1+a_p, q+1+a_q) & \text{if } (w/p) \neq 1 \text{ and } (w/q) \neq 1 \end{cases}$$

and $w = c^3 + ac + b \pmod n$.

Remark 3.11. It is possible to construct a message independent cryptosystem by choosing p and q so that $a_p = a_q = 0$.

4. Attacks on RSA and its variations

4.1. **The GCD attack.** At the rump session of Crypto '95, Franklin and Reiter [25] identified a new attack against RSA with public exponent 3. Later, it was extended for exponents up to $\simeq 32$ bits by Patarin [57]. If two linearly dependent messages are encrypted with the same RSA cryptosystem, then it is possible to recover them as follows.

Let m_1 and $m_2 = m_1 + \Delta$ be the two messages, and let $c_1 = m_1^e \bmod n$ and $c_2 = m_2^e \bmod n$ be the corresponding ciphertexts. Then, let us form the polynomials $\mathcal{P}$ and $\mathcal{Q} \in \mathbb{Z}_n[x]$, defined by

$$\mathcal{P}(x) = x^e - c_1 \pmod{n} \quad \text{and} \quad \mathcal{Q}(x) = (x+\Delta)^e - c_2 \pmod{n}. \tag{4.1}$$

Since the message m_1 is a root of $\mathcal{P}$ and $\mathcal{Q}$, m_1 will be a root of $\gcd(\mathcal{P}, \mathcal{Q})$ which is, with a high probability, a polynomial of degree 1. Solving this polynomial in x gives the value of m_1, and $m_2 = m_1 + \Delta$. This attack was later generalized to any known polynomial relation between the messages and to any number of messages [14].

On the other hand, by expressing Lucas sequences as Dickson polynomials [49], Joye and Quisquater [34] proved the same result for LUC. Using division polynomials [66, Chap. 3, exercice 3.7], they also extended this attack to the KMOV and Demytko cryptosystems. Since the polynomial relation is of order e^2 for elliptic curves systems [34], the attack applies for public exponent up to $\simeq 16$ bits, instead of 32 bits as for RSA and LUC.

Furthermore, by lattice basis reduction techniques [48], Coppersmith [13] showed that if Δ (the difference between the two messages) is unknown, then m_1 and m_2 can sometimes be recovered. In fact, let $\varrho(\Delta)$ be the resultant in x of $\mathcal{P}$ and $\mathcal{Q}$, which is an univariate polynomial in Δ. It is possible to solve this polynomial ϱ if the solution Δ is smaller than $n^{1/k}$, where n is the public modulus and k is the degree of ϱ. Since $k = e^2$ for RSA and LUC, and $k = e^4$ for elliptic curves system, KMOV and Demytko's cryptosystems tolerate smaller random padding.

4.2. **The common modulus attack.** Since RSA is multiplicative, the knowledge of two ciphertexts $c_1 = m^{e_1} \bmod n$ and $c_2 = m^{e_2} \bmod n$ of the message m enables to recover message m, if the same modulus n is used and if the public encryption keys e_1 and e_2 are relatively prime. Indeed, since $\gcd(e_1, e_2) = 1$, by the extended Euclidean algorithm [38], there exists $r, s \in \mathbb{Z}$ such that

$$re_1 + se_2 = 1. \tag{4.2}$$

Consequently, we have

$$m = m^{re_1 + se_2} = c_1^r c_2^s \bmod n. \tag{4.3}$$

This was first noticed by Simmons [68].

KMOV is also homomorphic and is therefore susceptible to the same attack. This is not the case for LUC and Demytko's system. However, Bleichenbacher, Bosma and Lenstra [5] presented a signature forgery against LUC that requires two chosen

signatures. Kaliski [36] established the same result for the Demytko's system. In his PhD. thesis, Bleichenbacher [3] shows how to forge a LUC signature from only *one* other signature. This was later adapted to Demytko's system [6]. This enables to exhibit the common modulus protocol failure as follows. We shall only illustrate the attack on LUC and refer to [6] for the attack on Demytko's system.

Let (e_1, d_1) and (e_2, d_2) be two pairs of encryption/decryption keys and let n be the public modulus. Assuming e_1 relatively prime to e_2, let us use the extended Euclidean algorithm to find integers r and s such that $re_1 + se_2 = 1$. From the two ciphertexts $c_1 = V_{e_1}(m, 1) \bmod n$ and $c_2 = V_{e_2}(m, 1) \bmod n$, we find the message m by

$$m = \frac{1}{2} V_r(c_1, 1) V_s(c_2, 1) + \frac{c_1^2 - 4}{2} U_r(c_1, 1) U_s(c_2, 1) \frac{U_{e_2}(c_1, 1)}{U_{e_1}(c_2, 1)} \bmod n. \tag{4.4}$$

Proof. From (2.7) and (2.3), it follows

$$\begin{aligned} U_{e_2}(c_1, 1) &= U_{e_2 e_1 d_1}(c_1, 1) \equiv U_{e_2 d_1}(c_1, 1) U_{e_1}(V_{e_2 d_1}(c_1, 1), 1) \\ &\equiv U_{e_2 d_1}(c_1, 1) U_{e_1}(c_2, 1) \pmod{n}. \end{aligned}$$

Hence,

$$\begin{aligned} 2m &\equiv 2V_{d_1}(c_1, 1) \equiv 2V_{d_1(re_1 + se_2)}(c_1, 1) \equiv V_{r + d_1 s e_2}(c_1, 1) \\ &\equiv V_r(c_1, 1) V_{d_1 s e_2}(c_1, 1) + \Delta U_r(c_1, 1) U_{d_1 s e_2}(c_1, 1) \\ &\equiv V_r(c_1, 1) V_s(c_2, 1) + \Delta U_r(c_1, 1) U_{d_1 e_2}(c_1, 1) U_s(V_{d_1 e_2}(c_1, 1), 1) \\ &\equiv V_r(c_1, 1) V_s(c_2, 1) + (c_1^2 - 4) U_r(c_1, 1) U_{d_1 e_2}(c_1, 1) U_s(c_2, 1) \pmod{n}. \end{aligned}$$

□

4.3. **The Wiener's attack.** Wiener [74] pointed out that if the secret key d was chosen too small, then it might be recovered. He observed that when writing $ed = 1 + \frac{k}{g}(p-1)(q-1)$ with $\gcd(k, g) = 1$, we have

$$\frac{k}{dg} - \frac{e}{n} = \frac{k}{dg} \left(\frac{1}{p} + \frac{1}{q} - \frac{1}{n} \right) - \frac{1}{dn}. \tag{4.5}$$

Following the presentation of Pinch [58], the attack of Wiener can be illustrated as follows.

Theorem 4.1 ([28, p. 153])**.** *If $\left| \frac{a}{b} - x \right| < \frac{1}{2b^2}$, then $\frac{a}{b}$ is a continued fraction approximant for x.* □

So, if the condition of the previous theorem is fulfilled, then $k/(dg)$ is a continued approximant for e/n. Since e/n is public and since continued fractions can easily be computed, it is possible to find the secret exponent d under certain assumptions. More precisely, Wiener proved the following corollary.

Corollary 4.2 ([74])**.** *Assume that $p \sim q \sim \sqrt{n}$, that $g = 2$ and that $e \sim n$. Then, $k \sim dg$ and the continued fraction attack will succeed for secret exponents of order up to $n^{1/4}$.* □

Later, Pinch [58] proved the same result for the LUC and KMOV cryptosystems. He also extended this attack to Demytko's cryptosystem by using Theorem 3.3, and proved that the attack will succeed for secret exponents of order at most $n^{1/8}$.

5. Concluding remarks

The security of RSA-type systems are based on the difficulty of factoring the public modulus n. Against polynomial attacks, LUC presents no advantage comparatively to RSA because the degree of the polynomial is the same. This is not the case for elliptic curves RSA systems, where the degree is squared. Multiplicative-like attacks on LUC and KMOV/Demytko's system are not as general as for RSA, since the messages are precisely related. However, in some cases, they offer no advantage as in the common modulus failure, for example.

As mentioned in the introduction, the last type of attacks cannot really be considered as an attack. If the parameters are carefully chosen, RSA-type cryptosystems are considered to be secure.

Although Lucas based or elliptic curves based implementations are more time-consuming, they may offer some advantages in terms of security. Unfortunately, we cannot give a definitive answer to "What is the best RSA-type cryptosystem?". Given the state of the art, only the application will enable to choose the most adequate cryptosystem.

Acknowledgments

We are very grateful to Daniel Bleichenbacher for fruitful discussions. Michael Merritt was also helpful in encouraging us to write this paper.

References

[1] H. Aly and W. B. Müller, *Cryptosystems based on Dickson polynomials*, Presented at Pragocrypt '96, Prague, Czech Rep., 30 Sept-3 Oct. 1996.

[2] F. Bao, R. Deng, Y. Han, A. Jeng, A. D. Narasimhalu, and T.-H. Ngair, *Breaking public key cryptosystems on tamper resistant devices in the presence of transient faults*, Pre-proceedings of the 1997 Workshop on Security Protocols, Paris, France, 7-9th April 1997

[3] D. Bleichenbacher, *Efficiency and security analysis of cryptosystems based on number theory*, Ph.D. thesis, Swiss Federal Institute of Technology Zürich, 1996.

[4] ———, *On the security of the KMOV public key cryptosystem*, To appear in the proceedings of Crypto '97.

[5] D. Bleichenbacher, W. Bosma, and A. K. Lenstra, *Some remarks on Lucas-based cryptosystems*, Advances in Cryptology – Crypto '95 (D. Coppersmith, ed.), Lecture Notes in Computer Science, vol. 963, Springer-Verlag, 1995, pp. 386–396.

[6] D. Bleichenbacher, M. Joye, and J.-J. Quisquater, *A new and optimal chosen message attack on RSA-type cryptosystems*, Unpublished manuscript.

[7] D. Boneh, R. A. DeMillo, and R. J. Lipton, *On the importance of checking cryptographic protocols for faults*, Advances in Cryptology – Eurocrypt '97 (W. Fumy, ed.), Lecture Notes in Computer Science, vol. 1233, Springer-Verlag, 1997, pp. 37–51.

[8] D. M. Bressoud, *Factorization and primality testing*, Undergraduate Texts in Mathematics, Springer-Verlag, 1989.

[9] L. S. Charlap and D. P. Robbins, *An elementary introduction to elliptic curves*, CRD Expository Report No. 31, Institute for Defense Analysis, Princeton, December 1988.

[10] H. Cohen, *A course in computational algebraic number theory*, Graduate Texts in Mathematics, vol. 138, Springer-Verlag, 1993.

[11] D. Coppersmith, *Small solutions to polynomials equations, and low exponent RSA vulnerabilities*, Submitted to *Journal of Cryptology*.
[12] ———, *Finding a small root of a bivariate integer equation; factoring with high bits known*, Advances in Cryptology – Eurocrypt '96 (U. Maurer, ed.), Lecture Notes in Computer Science, vol. 1070, Springer-Verlag, 1996, pp. 178–189.
[13] ———, *Finding a small root of a univariate modular equation*, Advances in Cryptology – Eurocrypt '96 (U. Maurer, ed.), Lecture Notes in Computer Science, vol. 1070, Springer-Verlag, 1996, pp. 155–165.
[14] D. Coppersmith, M. Franklin, J. Patarin, and M. Reiter, *Low exponent RSA with related messages*, Advances in Cryptology – Eurocrypt '96 (U. Maurer, ed.), Lecture Notes in Computer Science, vol. 1070, Springer-Verlag, 1996, pp. 1–9.
[15] G. Davida, *Chosen signature cryptanalysis of the RSA (MIT) public key cryptosystem*, Tech. Report TR-CS-82-2, Dept. of Electrical Engineering and Computer Science, University of Wisconsin, Milwaukee, USA, October 1982.
[16] W. de Jonge and D. Chaum, *Attacks on some RSA signatures*, Advances in Cryptology – Crypto '85 (H. C. Williams, ed.), Lecture Notes in Computer Science, vol. 218, Springer-Verlag, 1986, pp. 18–27.
[17] J. M. DeLaurentis, *A further weakness in the common modulus protocol for the RSA cryptoalgorithm*, Cryptologia **8** (1984), no. 3, 253–259.
[18] R. DeMillo, N. A. Lynch, and M. J. Merritt, *Cryptographic protocols*, Proc. SIGACT Conf., 1982.
[19] R. A. Demillo and M. J. Merrit, *Chosen signatures cryptanalysis of public key cryptosystems*, Technical memorandum, School of Information and Computer Science, Georgia Institute of Technology, Atlanta, Georgia 30322, October 1982.
[20] N. Demytko, *A new elliptic curve based analogue of RSA*, Advances in Cryptology – Eurocrypt '93 (T. Helleseth, ed.), Lecture Notes in Computer Science, vol. 765, Springer-Verlag, 1994, pp. 40–49.
[21] D. E. Denning, *Digital signatures with RSA and other public-key cryptosystems*, Communications of the ACM **27** (1984), no. 4, 388–392.
[22] Y. Desmedt and A. M. Odlyzko, *A chosen text attack on the RSA cryptosystem and some discrete logarithms schemes*, Advances in Cryptology – Crypto '85 (H. C. Williams, ed.), Lecture Notes in Computer Science, vol. 218, Springer-Verlag, 1986, pp. 516–521.
[23] W. Diffie and M. E. Hellman, *New directions in cryptography*, IEEE Transactions on Information Theory **IT-26** (1976), no. 6, 644–654.
[24] T. ElGamal, *A public key cryptosystem and a signature scheme based on discrete logarithms*, IEEE Transactions on Information Theory **IT-31** (1985), no. 4, 469–472.
[25] M. K. Franklin and M. K. Reiter, *A linear protocol failure for RSA with exponent three*, Preliminary note for *Crypto '95* rump session.
[26] M. Girault and J.-F. Misarski, *Selective forgery of RSA signatures using redundancy*, Advances in Cryptology – Eurocrypt '97 (W. Fumy, ed.), Lecture Notes in Computer Science, vol. 1233, Springer-Verlag, 1997, pp. 493–507.
[27] L. C. Guillou, J.-J. Quisquater, M. Walker, P. Landrock, and C. Shaer, *Precautions taken against various potential attacks*, Advances in Cryptology – Eurocrypt '90 (I. B. Damgård, ed.), Lecture Notes in Computer Science, vol. 473, Springer-Verlag, 1991, pp. 465–473.
[28] G. H. Hardy and E. M. Wright, *An introduction to the theory of numbers*, 5th ed., Oxford University Press, 1979.
[29] J. Håstad, *On using RSA with low exponent in a public key network*, Advances in Cryptology – Crypto '85 (H. C. Williams, ed.), Lecture Notes in Computer Science, vol. 218, Springer-Verlag, 1986, pp. 404–408.
[30] ———, *Solving simultaneous modular equations of low degree*, SIAM J. Comput. **17** (1988), no. 2, 336–341.
[31] D. Husemöller, *Elliptic curves*, Graduate Texts in Mathematics, vol. 111, Springer-Verlag, 1987.
[32] M. Joye, A. K. Lenstra, and J.-J. Quisquater, *Chinese remaindering in the presence of faults*, Submitted to Journal of Cryptology.

[33] M. Joye and J.-J. Quisquater, *On the importance of securing your bins: The garbage-man-in-the-middle attack*, Proc. of the 4th ACM Conference on Computer and Communications Security (T. Matsumoto, ed.), ACM Press, 1997, pp. 135–141.
[34] ———, *Protocol failures for RSA-like functions using Lucas sequences and elliptic curves*, Security Protocols (M. Lomas, ed.), Lecture Notes in Computer Science, vol. 1189, Springer-Verlag, 1997, pp. 93–100.
[35] B. S. Kaliski Jr, *Elliptic curves and cryptography: A pseudorandom bit generator and other tools*, Ph.D. thesis, Massachusetts Institute of Technology, 1988.
[36] ———, *A chosen message attack on Demytko's elliptic curve cryptosystem*, Journal of Cryptology **10** (1997), no. 1, 71–72.
[37] A. Knapp, *Elliptic curves*, Mathematical Notes, Princeton University Press, 1992.
[38] D. E. Knuth, *The art of computer programming: Volume 2/seminumerical algorithms*, 2nd ed., Addison-Wesley Publishing Company, 1981.
[39] N. Koblitz, *Elliptic curve cryptosystems*, Mathematics of Computation **48** (1987), 203–209.
[40] ———, *A course in number theory and cryptography*, 2nd ed., Graduate Texts in Mathematics, vol. 114, Springer-Verlag, 1994.
[41] K. Koyama, U. M. Maurer, T. Okamoto, and S. A. Vanstone, *New public-key schemes based on elliptic curves over the ring $\mathbb{Z}_n$*, Advances in Cryptology – Crypto '91 (J. Feigenbaum, ed.), Lecture Notes in Computer Science, vol. 576, Springer-Verlag, 1991, pp. 252–266.
[42] K. Kurosawa, K. Okada, and S. Tsujii, *Low exponent attack against elliptic curve RSA*, Advances in Cryptology – Asiacrypt '94 (J. Pieprzyk and R. Safavi-Naini, eds.), Lecture Notes in Computer Science, vol. 917, Springer-Verlag, 1995, pp. 376–383.
[43] H. Kuwakado and K. Koyama, *Security of RSA-type cryptosystems over elliptic curves against Håstad attack*, Electronics Letters **30** (1994), no. 22, 123–124.
[44] C.-S. Laih, F.-K. Tu, and W.-C. Tai, *Remarks on LUC public key system*, Electronics Letters **30** (1994), no. 2, 123–124.
[45] C.-S. Laih, F.-K. Tu, and W.-C. Tai, *On the security of the Lucas functions*, Informations Processing Letters **53** (1995), 243–247.
[46] S. Lang, *Elliptic curves: Diophantine analysis*, Grundlehren der mathematischen Wissenschaften, vol. 231, Springer-Verlag, 1978.
[47] A. K. Lenstra, *Memo on RSA signature generation in the presence of faults*, September 1996.
[48] A. K. Lenstra, H. W. Lenstra Jr, and L. Lovasz, *Factoring polynomials with integer coefficients*, Matematische Annalen **261** (1982), 513–534.
[49] R. Lidl, G. L. Mullen, and G. Turnwald, *Dickson polynomials*, Longman Scientific & Technical, 1993.
[50] A. J. Menezes, *Elliptic curve public key cryptosystems*, Kluwer Academic Publishers, 1993.
[51] V. S. Miller, *Use of elliptic curves in cryptography*, Advances in Cryptology – Crypto '85 (H. C. Williams, ed.), Lecture Notes in Computer Science, vol. 218, Springer-Verlag, 1986, pp. 417–426.
[52] P. L. Montgomery, *Speeding the Pollard and elliptic curve methods of factorization*, Mathematics of Computation **48** (1987), no. 177, 243–264.
[53] J. H. Moore, *Protocol failures in cryptosystems*, Contemporary Cryptology (G. Simmons, ed.), IEEE Press, 1992, pp. 541–558.
[54] W. B. Müller and R. Nöbauer, *Some remarks on public-key cryptosystems*, Sci. Math. Hungar **16** (1981), 71–76.
[55] ———, *Cryptanalysis of the Dickson scheme*, Advances in Cryptology – Eurocrypt '85 (J. Pichler, ed.), Lecture Notes in Computer Science, vol. 219, Springer-Verlag, 1986, pp. 50–61.
[56] S. Murphy, *Remarks on the LUC public key system*, Electronics Letters **30** (1994), no. 7, 558–559.
[57] J. Patarin, *Some serious protocol failures for RSA with exponent e of less than $\simeq$ 32 bits*, Presented at the conference of cryptography, CIRM Luminy, France, September 1995.
[58] R. G. E. Pinch, *Extending the Håstad attack to LUC*, Electronics Letters **31** (1995), no. 21, 1827–1828.

[59] ———, *Extending the Wiener attack to RSA-type cryptosystems*, Electronics Letters **31** (1995), no. 20, 1736–1738.
[60] M. O. Rabin, *Digital signatures and public-key functions as intractable as factorization*, Tech. Report MIT/LCS/TR-212, MIT Laboratory for Computer Science, January 1979.
[61] P. Ribenboim, *The little book of big primes*, Springer-Verlag, 1991.
[62] H. Riesel, *Prime numbers and computer methods for factorization*, Progress in Mathematics, vol. 57, Birkhaüser, 1985.
[63] R. L. Rivest, A. Shamir, and L. Adleman, *A method for obtaining digital signatures and public-key cryptosystems*, Communications of the ACM **21** (1978), no. 2, 120–126.
[64] R. Schoof, *Elliptic curves over finite fields and the computation of square roots mod p*, Mathematics of Computation **44** (1985), no. 170, 483–494.
[65] A. Shamir, *A fast signature scheme*, Tech. Report MIT/LCS/TM-107, MIT Lab. for Computer Science, Cambridge, Mass., July 1978.
[66] J. H. Silverman, *The arithmetic of elliptic curves*, Graduate Texts in Mathematics, vol. 106, Springer-Verlag, 1986.
[67] J. H. Silverman and J. Tate, *Rational points on elliptic curves*, Undergraduate Texts in Mathematics, Springer-Verlag, 1992.
[68] G. J. Simmons, *A 'weak' privacy protocol using the RSA crypto algorithm*, Cryptologia **7** (1983), no. 2, 180–182.
[69] A. Smith and C. Boyd, *An elliptic curve analogue of McCurley's key agreement scheme*, Cryptography and Coding (C. Boyd, ed.), Lecture Notes in Computer Science, vol. 1025, Springer-Verlag, 1995, pp. 150–157.
[70] P. Smith, *LUC public-key encryption*, Dr. Dobb's Journal (1993), 44–49.
[71] P. Smith and C. Skinner, *A public-key cryptosystem and a digital signature based on the Lucas function analogue to discrete logarithms*, Advances in Cryptology – Asiacrypt '94 (J. Pieprzyk, ed.), Lecture Notes in Computer Science, vol. 917, Springer-Verlag, 1995, pp. 357–364.
[72] P. J. Smith and M. J. J. Lennon, *LUC: A new public key system*, Ninth IFIP Symposium on Computer Security (E. G. Douglas, ed.), Elsevier Science Publishers, 1993, pp. 103–117.
[73] T. Takagi and S. Naito, *The multi-variable modular polynomial and its applications to cryptography*, 7th International Symposium on Algorithm and Computation, ISAAC'96, Lecture Notes in Computer Science, vol. 1178, 1996, pp. 386–396.
[74] M. J. Wiener, *Cryptanalysis of short RSA secret exponents*, IEEE Transactions on Information Theory **36** (1990), no. 3, 553–558.
[75] H. C. Williams, *A modification of the RSA public-key encryption procedure*, IEEE Transactions on Information Theory **IT-26** (1980), no. 6, 726–729.

UCL Crypto Group, Dép. de Mathématique, Université catholique de Louvain, Chemin du Cyclotron 2, B-1348 Louvain-la-Neuve, Belgium
E-mail address: joye@agel.ucl.ac.be
URL: http://www.dice.ucl.ac.be/crypto/joye/

UCL Crypto Group, Lab. de Micro-électronique, Université catholique de Louvain, Place du Levant 3, B-1348 Louvain-la-Neuve, Belgium
E-mail address: jjq@dice.ucl.ac.be
URL: http://www.dice.ucl.ac.be/crypto/jjq.html