Université catholique de Louvain
Faculté des Sciences Appliquées

Security Analysis of RSA-type Cryptosystems

Marc Joye

Submitted for the degree of Doctor of Philosophy in Applied Sciences

Jury: P. Sobieski, UCL (Chairman)
F. Borceux, UCL
J.-M. Couveignes, U. Bordeaux
A. Magnus, UCL
D. Naccache, Gemplus
J.-J. Quisquater, UCL (Thesis supervisor)
J. Stern, ENS

October 1997

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

ABSTRACT. In 1978, Rivest, Shamir and Adleman introduced the public-key cryptosystem RSA. Thereafter, it was extended to Lucas sequences and elliptic curves. This thesis analyses the security of these cryptosystems in given contexts. In particular, all known major attacks against RSA-type systems (including some attacks due to the author) are reviewed. We also see how these attacks can be avoided.

RÉSUMÉ. En 1978, Rivest, Shamir et Adleman introduisaient le cryptosystème à clé publique RSA. Par après, ce dernier a été étendu aux suites de Lucas et aux courbes elliptiques. Cette thèse analyse la sécurité de ces cryptosystèmes dans des contextes donnés. En particulier, toutes les principales attaques connues contre les systèmes du type RSA (dont certaines sont dues à l'auteur) sont revues. Nous voyons également comment éviter ces attaques.

Author address:

UCL CRYPTO GROUP, UNIVERSITÉ CATHOLIQUE DE LOUVAIN
PLACE DU LEVANT 3, B-1348 LOUVAIN-LA-NEUVE, BELGIUM

E-mail address: `joye@dice.ucl.ac.be`
URL: `http://www.dice.ucl.ac.be/crypto/joye/`

To my two favorite persons,
Anne-Marie and Hung-Mei.

Toutes les guerres ayant leur caractère propre et présentant dans leur évolution un grand nombre de caractères particuliers, chacune d'elle peut être considérée comme une mer inconnue du général en chef.

— Clausewitz (cited in the biography of de Gaulle by Lacouture)

Acknowledgements

I am most grateful to my advisor Jean-Jacques Quisquater for guiding me all along my research. I am also grateful to Francis Borceux, Jean-Marc Couveignes and Alphonse Magnus who served me on committee thesis. In particular, I want to thank Jean-Marc Couveignes for patiently answering many questions on the theory of elliptic curves. Thanks to David Naccache and Jacques Stern for accepting to be co-referees of this thesis. Thanks also to Feng Bao, Daniel Bleichenbacher, Robert Deng, Arjen Lenstra and Tsuyoshi Takagi for giving me the opportunity to write joint papers. Other researchers were of some utility for sending preprints of their work or for providing some fruitful comments; in alphabetical order, they are Dan Boneh, Seng-Kiat Chua, George Davida, Marc Girault, Burt Kaliski, David Kohel, Kenji Koyama, Masahiro Mambo, Alfred Menezes, Michael Merritt, Victor Miller, Peter Montgomery, François Morain, Willi More, Volker Müller, Richard Pinch, Mike Rosing, Joe Silverman, Scott Vanstone and Moti Yung. Thanks also to all my colleagues and friends of the UCL Crypto Group* for many discussions on cryptography.

Most importantly, I want to thank my friend Hung-Mei for her patience during the writing of this thesis and my family for their encouragements.

Part of this work was supported by the European project *ACCOPI* (Prof. B. Macq and Prof. J.-J. Quisquater), the *Action Concertée*, the *Communauté Française* and the *Fonds National de la Recherche Scientifique* (F.N.R.S.). I have also benefited from teaching assistantships of the department of Mathematics of UCL.

✎ Marc Joye

*See `<http://www.dice.ucl.ac.be/crypto/>`.

Contents

List of Figures

Preface

Cryptology, from the Greek *kruptos* (hidden) and *logos* (science), is the science of secure information. In particular, this science studies how two people, Alice and Bob, can exchange secret messages over an insecure channel. This can been achieved thanks to secret-key or public-key cryptography.

In *secret-key cryptography*, Alice and Bob have to share a common secret key k. Then, to send a message m to Bob, Alice forms the ciphertext $c = E_k(M)$ where $E_k(\cdot)$ is the encryption function. To recover the plaintext m from the ciphertext c, Bob computes $D_k(c) = D_k(E_k(m)) = m$, where $D_k(\cdot)$ is the decryption function. Example of such cryptosystems is DES [**1**], developed by IBM and later adopted by the US government as standard for unclassified data.

One drawback of secret-key systems is that they require the prior exchange of the secret key k. This assumes the existence of a secure channel. In 1976, Diffie and Hellman [**97**] overcomed this limitation by introducing *public-key cryptography*. This one enables Alice and Bob to derive a secret key over an insecure channel. The idea behind public-key cryptography is concept of *one-way* function. A function f is one-way if given x, one can easily compute $f(x)$; but given $f(x)$, it is *infeasible* to derive x. By infeasible, we mean computationally impossible.

In 1978, Rivest, Shamir and Adleman realized the first public-key cryptosystem, the so-called RSA [**292**]. This system is based on the difficulty of factoring large integers. It can briefly be described as follows. Suppose that Alice wants to send a message m to Bob. To setup the system, Bob carefully selects two large primes p and q, computes $n_B = pq$ and $\phi(n_B) = (p-1)(q-1)$, chooses an encryption key e_B relatively prime to $\phi(n_B)$, and computes the decryption key $d_B = e_B^{-1} \bmod \phi(n_B)$. The public key of Bob is the pair (n_B, e_B) and his secret key is d_B. To send m to Bob, Alice forms the ciphertext $c = m^{e_B} \bmod n_B$ and sends it to Bob. Then, Bob recovers the plaintext by computing $m = c^{d_B} \bmod n_B$ with his secret key d_B.

However, the design of strong cryptoalgorithms is not sufficient to guarantee the security of information. We also have to deal with the *soundness* of the protocols using these algorithms. In some situations, a protocol may be completely subverted without compromising the security of the underpinning cryptoalgorithm. Such situations are called *protocol failures* [**246**]. Suppose that a pirate, say Carol, wants to recover the RSA-encrypted message m. She can proceed as follows. Carol chooses a random number k, intercepts the ciphertext c, replaces it by $c' = ck^{e_B} \bmod n_B$, and sends c' to Bob. Now, when Bob deciphers c', he obtains $m' \equiv (c')^{d_B} \equiv mk \pmod{n_B}$. Since m' is meaningless, Bob discards it. If Carol can get access to this discard, she finds $m = m'k^{-1} \bmod n_B$. This failure was first pointed out by Davida [**83**].

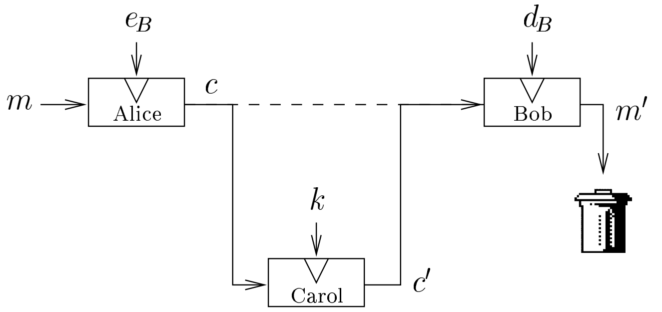

Figure 0.1: Davida's attack

Avoiding this attack is easy, users have to really destroy the discards, or in other words to protect their bins. The lesson of this failure is that the protocol designer has to pay attention to what is generally accepted but not explicitly stated.

The decryption process for RSA can be speeded up by the Chinese Remainder Theorem (CRT). From the secret factors p and q, Bob computes $m_p = c^{d_B \bmod (p-1)} \bmod p$ and $m_q = c^{d_B \bmod (q-1)} \bmod q$, and finally finds $m = \mathrm{CRT}(m_p, m_q)$ [**283**]. Suppose that Carol induces an external constraint on the deciphering device of Bob (e.g., ionizing or microwave radiation) so that the computation of m_p is correctly performed but not computation of m_q. So, Bob gets $m' = \mathrm{CRT}(m_p, m'_q)$ instead of m. If Bob discards m' and if Carol can get access to m', then she finds the secret factor p by computing $\gcd\big((m')^{e_B} - c \bmod n_B, n_B\big)$. Hence, $q = n_B/p$ and Carol can compute the secret decryption key d_B [**205, 156**]. This second attack is more dangerous because it completely breaks the system. This shows clearly the importance of checking cryptographic protocols for faults [**40**]. Note also that if Bob protects his bin, the attack does not remain applicable.

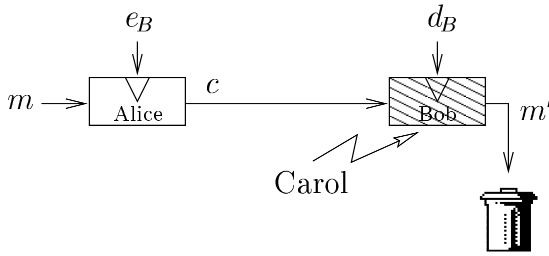

Figure 0.2: Lenstra's attack

The two previous attacks show that it is extremely difficult for a protocol designer to determine whether his protocol is sound, even for very simple protocols. Some researchers proposed formal techniques for analyzing the soundness of protocols, such as the BAN logic [**52**] or the three systems presented in [**173**]. Another approach for the protocol designer is to try to find flaws in his protocol with all his experience of good and bad practice. In [**2**], Abadi and Needham give general rules helping protocol designers to avoid many of the pitfalls (see also [**15**]). In this thesis, we review for the first time all known attacks against RSA-type cryptosystems. We also present new failures. This may serve as guidelines to construct secure RSA-based protocols.

On the other hand, RSA was extended to other structures, including Lucas sequences and elliptic curves. A few authors have studied the underlying systems. These systems are sometimes claimed more resistant in some given contexts. My main contribution to this subject is to show that this is not always justified (see Table 4.1). Indeed, we will see that all major attacks against RSA can more or less successfully be extended to its analogues.

This thesis presumes almost no background in number theory or algebra. The relevant mathematics are introduced in Chapter 1. Chapter 2 reviews the RSA and its analogues based on Lucas sequences and elliptic curves. Chapter 3 is the main part of this thesis. We present attacks on RSA-type systems. These attacks are classified into three categories: polynomial attacks, homomorphic attacks and attacks resulting from a bad implementation. Finally, in Chapter 4, we compare the RSA-type systems in terms of security. This can help to choose the most adequate system for a given application.

References

[1] NBS FIPS 46, *Data Encryption Standard*, National Bureau of Standards, U.S. Department of Commerce, January 1977.

[2] M. Abadi and R. Needham, *Prudent engineering practice for cryptographic protocols*, 1994 IEEE Symposium on Security and Privacy, IEEE Press, 1994, pp. 122–136.

[15] R. J. Anderson and R. Needham, *Robustness principles for public key protocols*, Advances in Cryptology – Crypto '95 (D. Coppersmith, ed.), Lecture Notes in Computer Science, vol. 963, Springer-Verlag, 1995, pp. 236–247.

[40] 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.

[52] M. Burrows, M. Abadi, and R. Needham, *A logic of authentication*, ACM Trans. on Computer Systems **8** (1990), no. 1, 18–36.

[83] 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.

[97] W. Diffie and M. E. Hellman, *New directions in cryptography*, IEEE Transactions on Information Theory **IT-26** (1976), no. 6, 644–654.

[156] M. Joye, A. K. Lenstra, and J.-J. Quisquater, *Chinese remaindering in the presence of faults*, Submitted to Journal of Cryptology.

[173] R. Kemmerer, C. Meadows, and J. Millen, *Three systems for cryptographic protocol analysis*, Journal of Cryptology **7** (1994), no. 2, 79–130.

[205] A. K. Lenstra, *Memo on RSA signature generation in the presence of faults*, September 1996.

[246] J. H. Moore, *Protocol failures in cryptosystems*, Contemporary Cryptology (G. Simmons, ed.), IEEE Press, 1992, pp. 541–558.

[283] J.-J. Quisquater and C. Couvreur, *Fast decipherment algorithm for RSA public-key cryptosystem*, Electronics Letters **18** (1982), no. 21, 905–907.

[292] 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.

CHAPTER 1

Mathematical Background

There are numerous books devoted to the theory of numbers, good references are [**137, 147, 182, 260, 295**]. Computational aspects are treated in [**67, 175**].

For the Lucas sequences, we refer to [**286, 287**]. Also, the book of Lidl *et al.* [**214**] is an invaluable source on Dickson polynomials.

The classical reference for elliptic curves is [**316**] (see also [**145, 174**]). More accessible textbooks are [**231, 317**]. In [**201**], Lang gives a good introduction to division polynomials. Another introduction to division polynomials may be found in [**59**].

A lattice basis reduction algorithm was developed by Lenstra, Lenstra and Lovász [**206**]. The underlying mathematics are introduced in [**55**].

1. Basic facts

In this Section, we give some well-known results on number theory. All the proofs were omitted since they may be found in most textbooks on number theory (see [**137**] for example).

THEOREM 1.1 (Lagrange's Theorem). *If a is an element of a (multiplicatively written) finite group G of order n, then $a^n = 1$.* □

This beautiful theorem is a generalization of two theorems due to Fermat and Euler.

THEOREM 1.2 (Fermat's Little Theorem). *If p is a prime and $p \nmid a$, then*

$$a^{p-1} \equiv 1 \pmod{p}. \tag{1.1}$$

□

DEFINITION 1.3. The *Euler's totient function* $\phi(n)$ denotes the number of positive integers not greater than and relatively prime to n.

PROPOSITION 1.4. *Let $n = \prod_{i=1}^{r} p_i^{e_i}$ be the prime factorization of n. Then,*

$$\phi(n) = p_1^{e_1}(1 - \frac{1}{p_1})\, p_2^{e_2}(1 - \frac{1}{p_2}) \cdots p_r^{e_r}(1 - \frac{1}{p_r}) = n \prod_{p|n}(1 - \frac{1}{p}). \tag{1.2}$$

□

THEOREM 1.5 (Euler's Theorem). *If $\gcd(a, n) = 1$, then*

$$a^{\phi(n)} \equiv 1 \pmod{n}. \tag{1.3}$$

□

DEFINITION 1.6. Let a be an integer and let p be an odd prime. The *Legendre symbol* (a/p) is defined by

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & \text{if } p \mid a, \\ 1 & \text{if } a \text{ is a quadratic residue modulo } p, \\ -1 & \text{if } a \text{ is a quadratic non-residue modulo } p. \end{cases}$$

PROPOSITION 1.7. *For any odd prime p,*

$$\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \pmod{p}. \tag{1.4}$$

□

We usually do not use Eq. (1.4) to compute Legendre symbols. This can efficiently be achieved thanks to the next corollary and the *Law of Quadratic Reciprocity*, also known as the Gauss' Theorem.

COROLLARY 1.8. *The Legendre symbol satisfies the following properties:*

(i) $(a/p) = (a \bmod p/p)$,
(ii) $(ab/p) = (a/p)(b/p)$,
(iii) *for b prime to a*, $(ab^2/p) = (a/p)$,
(iv) $(1/p) = 1$ *and* $(-1/p) = (-1)^{\frac{p-1}{2}}$.

□

THEOREM 1.9 (Gauss' Theorem). *If p and q are two odd primes, then*

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}, \tag{1.5}$$

$$\left(\frac{q}{p}\right) = (-1)^{\left(\frac{p-1}{2}\right)\left(\frac{q-1}{2}\right)} \left(\frac{p}{q}\right). \tag{1.6}$$

□

One difficulty with this method of computing Legendre symbols is that it requires the factorization of the number on top. However, if we generalize Legendre symbols to Jacobi symbols, the Law of Quadratic Reciprocity remains valid for any two positive odd integers.

DEFINITION 1.10. Let n be a positive odd integer. If $n = \prod_{i=1}^{r} p_i^{e_i}$ is the prime factorization of n, then the *Jacobi symbol* (a/n) is given by

$$\left(\frac{a}{n}\right) = \prod_{i=1}^{r} \left(\frac{a}{p_i}\right)^{e_i}$$

where (a/p_i) is the Legendre symbol of a modulo p_i.

PROPOSITION 1.11. *If m and n are two positive odd integers, then*

$$\left(\frac{2}{n}\right) = (-1)^{\frac{n^2-1}{8}}, \tag{1.7}$$

$$\left(\frac{n}{m}\right) = (-1)^{\left(\frac{m-1}{2}\right)\left(\frac{n-1}{2}\right)} \left(\frac{m}{n}\right). \tag{1.8}$$

□

Another result that will be useful is the following:

THEOREM 1.12 (Chinese Remainder Theorem). *Consider a system of r congruences*

$$x \equiv a_i \pmod{n_i} \quad (1 \le i \le r). \tag{1.9}$$

Let $N = \prod_{i=1}^{r} n_i$. If $\gcd(n_i, n_j) = 1$ for all $i \ne j$, then there exists a unique solution modulo N given by

$$x = \sum_{i=1}^{r} a_i u_i \bmod N, \tag{1.10}$$

with $u_j := \frac{N}{n_j}\left(\frac{n_j}{N} \bmod n_j\right) \bmod N \equiv \delta_{ij} \pmod{n_i}$ where δ_{ij} is the Kronecker's delta, i.e. $\delta_{ij} = 1$ if $i = j$ and $\delta_{ij} = 0$ otherwise. □

2. Eisenstein and Gaussian integers

The Legendre symbol tells whether a number is a square modulo a prime p. The purpose of this Section is to extend this notion to higher powers. This was first studied by Gauss and later by Eisenstein. We will restrict our study to the third, fourth and sixth power residue symbols.

From Proposition 1.7, we know that, if $p \nmid a$, there exists a unique integer j (modulo 2) such that $a^{(p-1)/2} \equiv (-1)^j \pmod{p}$. To obtain the analogue to a higher power d, we have to extend our integers so that they include the d^{th} root of unity, namely $e^{2i\pi/d}$. The case $d = 3$ defines the Eisenstein integers, and the case $d = 4$ the Gaussian integers. It is well known that, for these choices of d, these integers form unique factorization domains. So, we will analyze the units (*i.e.* invertible elements) and the primes for these new integers. We will also give the analogue of Fermat's Little Theorem.

2.1. The ring $\mathbb{Z}[\omega]$.

DEFINITION 1.13. Let $\omega = e^{2i\pi/3} = \frac{1}{2}(-1+\sqrt{-3})$. The *ring* $\mathbb{Z}[w]$ *of Eisenstein integers* is the set of all numbers of the form $\alpha = a + b\omega$ where a and b are rational integers.

Now, we study the units and the primes in $\mathbb{Z}[\omega]$.

LEMMA 1.14. *The units in* $\mathbb{Z}[\omega]$ *are* ± 1, $\pm\omega$ *and* $\pm\omega^2$.

PROOF. Let $\alpha = a + b\omega = \frac{1}{2}\big((2a-b)+b\sqrt{-3}\big) \in \mathbb{Z}[\omega]$, then $\mathrm{N}(\alpha) = \alpha\overline{\alpha} = \frac{1}{4}\big((2a-b)^2+3b^2\big) \geq 0$. If α is a unit, there exists $\beta \in \mathbb{Z}[\omega]$ such that $\alpha\beta = 1$. Hence, $\mathrm{N}(\alpha)\,\mathrm{N}(\beta) = 1$ and $\mathrm{N}(\alpha) = 1$ since $\mathrm{N}(\alpha)$ and $\mathrm{N}(\beta)$ are positive integers. Therefore $(2a-b)^2 + 3b^2 = 4$. So, either $2a - b = \pm 2$ and $b = 0$ or $2a - b = \pm 1$ and $b = \pm 1$. This implies $\alpha = \pm 1, \pm\omega$ or $\pm(1+\omega) = \mp\omega^2$. $\square$

It is important to note that the primes in $\mathbb{Z}$ are not necessarily prime in $\mathbb{Z}[\omega]$. For example, $7 = (3+\omega)(2-\omega)$. The two following propositions tell more about the primes in $\mathbb{Z}[\omega]$.

PROPOSITION 1.15. *If* $p \equiv 2 \pmod 3$ *is a rational prime, then* p *is prime as an element of* $\mathbb{Z}[\omega]$.

PROOF. Suppose that p is not prime in $\mathbb{Z}[\omega]$, then $p = \pi\gamma$ for some non-units $\pi, \gamma \in \mathbb{Z}[\omega]$. Therefore, $\mathrm{N}(\pi)\,\mathrm{N}(\gamma) = p^2$ and $\mathrm{N}(\pi) = p$. Writing $\pi = a + b\omega$, we have $p \equiv \mathrm{N}(\pi) \equiv 4\,\mathrm{N}(\pi) \equiv (2a-b)^2 \equiv 0, 1 \pmod 3$, which is contrary to the hypothesis. $\square$

PROPOSITION 1.16. *If* $p \equiv 1 \pmod 3$ *is a rational prime, then* $p = \pi\overline{\pi}$ *where* π *is a prime in* $\mathbb{Z}[\omega]$.

PROOF. By Corollary 1.8 and Theorem 1.9,

$$\left(\frac{-3}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{3}{p}\right) = (-1)^{(p-1)/2}\left(\frac{p}{3}\right)(-1)^{(p-1)/2} = \left(\frac{1}{3}\right) = 1.$$

So, there exists $x \in \mathbb{Z}$ such that $x^2 \equiv -3 \pmod p \iff x^2 \equiv (2\omega+1)^2 \pmod p$. Suppose p prime in $\mathbb{Z}[\omega]$, then $p \mid (x+1+2\omega)$ or $p \mid (x-1-2\omega)$. This implies $bp = \pm 2$ for some $b \in \mathbb{Z}$, and thus $p = 2$. But $p \equiv 1$

(mod 3), so p is not prime in $\mathbb{Z}[\omega]$ and $p = \pi\gamma$ where π and γ are non-units in $\mathbb{Z}[\omega]$. Taking the norm, we obtain $p^2 = \mathrm{N}(\pi)\,\mathrm{N}(\gamma)$ and thus $p = \mathrm{N}(\pi) = \pi\overline{\pi}$. It remains to prove that π is prime. If π was not prime, then $\pi = \rho\theta$ for some non-units ρ and θ. So, $p = \mathrm{N}(\rho)\,\mathrm{N}(\theta)$ which cannot be true since p is prime. $\square$

Therefore, if $\pi \in \mathbb{Z}[\omega]$ is prime, then $\mathrm{N}(\pi) = p^2$ or p for some rational prime p. The first case corresponds to Proposition 1.15 and the second one to Proposition 1.16. The next proposition deals with the remaining case $p \equiv 0 \pmod 3$.

PROPOSITION 1.17. *$(1-\omega)$ is prime in $\mathbb{Z}[\omega]$.*

PROOF. Suppose that $1 - \omega = \pi\gamma$ for non-units $\pi, \gamma \in \mathbb{Z}[\omega]$. Taking the norm, we get $3 = \mathrm{N}(\pi)\,\mathrm{N}(\gamma)$. This cannot be true since 3 is prime in $\mathbb{Z}$. $\square$

The primes in $\mathbb{Z}[\omega]$ are given up to multiplication by $\pm 1, \pm\omega$ or $\pm\omega^2$. The notion of *primary* prime enables to distinguish among these primes.

DEFINITION 1.18. Two integers $\alpha, \beta \in \mathbb{Z}[\omega]$ are called *associates* if $\alpha = \beta\upsilon$ for some unit $\upsilon \in \mathbb{Z}[\omega]$.

DEFINITION 1.19. Let $\alpha \in \mathbb{Z}[\omega]$. If $\alpha \equiv 2 \pmod 3$, then α is said *primary.*

PROPOSITION 1.20. *Let a prime $\pi \in \mathbb{Z}[\omega]$. If $\mathrm{N}(\pi) \equiv 1 \pmod 3$, then among the associates of π, exactly one is primary.*

PROOF. Let $\pi = a + b\omega$, then $\mathrm{N}(\pi) = a^2 - ab + b^2$. The associates of π are

(1) $\pi = a + b\omega$;
(2) $-\pi = -a - b\omega$;
(3) $\omega\pi = -b + (a - b)\omega$;
(4) $-\omega\pi = b + (b - a)\omega$;
(5) $\omega^2\pi = (b - a) - a\omega$;
(6) $-\omega^2\pi = (a - b) + a\omega$.

Suppose first $a \equiv 0 \pmod 3$. Hence, $a^2 - ab + b^2 \equiv b^2 \equiv 1 \pmod 3$. So b mod 3 is either equal to 1 or to 2. If $b \equiv 1 \pmod 3$, then $\pm(a-b) \equiv \mp 1 \pmod 3$ and (6) is primary. If $b \equiv 2 \pmod 3$, then $\pm(a - b) \equiv \pm 1 \pmod 3$ and (5) is primary. The remaining cases ($a \equiv 1, 2 \pmod 3$) are treated in a similar way. $\square$

Putting all together, we have:

THEOREM 1.21. *The primes in $\mathbb{Z}[\omega]$ (up to multiplication by ± 1, $\pm\omega$ or $\pm\omega^2$) are the rational primes congruent to* 2 mod 3, $(1 - \omega)$, *and the* *integers of the form* $\pi = a + b\omega$ *and* $\overline{\pi} = a + b\omega^2$ *such that* $a^2 - ab + b^2$ *is a rational prime congruent to* $1 \bmod 3$*. In the latter case, if* $\mathrm{N}(\pi) \equiv 1 \pmod 3$*, then among the primes* $\pm\pi, \pm\omega\pi$ *and* $\pm\omega^2\pi$*, exactly one is congruent to* $2 \bmod 3$*.* □

The theorem of Fermat (Theorem 1.2) in $\mathbb{Z}[\omega]$ becomes:

THEOREM 1.22. *If* π *is a prime in* $\mathbb{Z}[\omega]$ *and if* $\pi \nmid \alpha$*, then*

$$\alpha^{\mathrm{N}(\pi)-1} \equiv 1 \pmod{\pi}. \tag{1.11}$$

PROOF. By Proposition 9.2.1 in [**147**, p. 111], $K = \mathbb{Z}[\omega]/(\pi\,\mathbb{Z}[\omega])$ is a finite field with $\mathrm{N}(\pi)$ elements. Thus the multiplicative group of K has order $\mathrm{N}(\pi) - 1$. Using Theorem 1.1, this concludes the proof. □

Finally, by analogy with the Legendre symbol, the cubic and sixtic residue symbols are defined as follows.

DEFINITION 1.23. Let π be a prime in $\mathbb{Z}[\omega]$ with $\mathrm{N}(\pi) \neq 3$. If $\pi \nmid \alpha$, then the *cubic residue symbol* $(\alpha/\pi)_3$ is defined to be ω^j where j is the unique integer (modulo 3) satisfying

$$\alpha^{(\mathrm{N}(\pi)-1)/3} \equiv \omega^j \pmod{\pi}, \tag{1.12}$$

and the *sixtic residue symbol* $(\alpha/\pi)_6$ is defined to be $(-\omega)^j$ where j is the unique integer (modulo 6) satisfying

$$\alpha^{(\mathrm{N}(\pi)-1)/6} \equiv (-\omega)^j \pmod{\pi}. \tag{1.13}$$

If $\pi \mid \alpha$, then $(\alpha/\pi)_3 = (\alpha/\pi)_6 = 0$.

REMARK 1.24. Note that $\{\pm 1, \pm\omega, \pm\omega^2\}$ is a cyclic group of order 6. So by Theorem 1.1, $6 \mid (\mathrm{N}(\pi) - 1)$.

2.2. The ring $\mathbb{Z}[i]$. The Gaussian integers are constructed by adding $i = e^{2i\pi/4}$ to the rational integers. We can now mimic the presentation of Eisenstein integers.

DEFINITION 1.25. Let $i = \sqrt{-1}$. The *ring* $\mathbb{Z}[i]$ *of Gaussian integers* is the set of all numbers of the form $\alpha = a + bi$ where a and b are rational integers.

LEMMA 1.26. *The units in* $\mathbb{Z}[i]$ *are* ± 1 *and* $\pm i$*.*

PROOF. Suppose that $\alpha = a + bi$ is a unit, then $\mathrm{N}(\alpha) = a^2 + b^2 = 1$. So, either $a = \pm 1$ and $b = 0$ or $a = 0$ and $b = \pm 1$. It follows $\alpha = \pm 1$ or $\alpha = \pm i$. □

PROPOSITION 1.27. *If $p \equiv 3 \pmod 4$ is a rational prime, then p is prime as an element of $\mathbb{Z}[i]$.*

PROOF. Suppose that p is not prime in $\mathbb{Z}[i]$, then $p = \pi\gamma$ with $\mathrm{N}(\pi) = \mathrm{N}(\gamma) = p$. Writing $\pi = a + bi$, we have $p \equiv \mathrm{N}(\pi) \equiv a^2 + b^2 \equiv 0, 1, 2 \pmod 4$, which is contrary to the hypothesis. □

PROPOSITION 1.28. *If $p \equiv 1 \pmod 4$ is a rational prime, then $p = \pi\overline{\pi}$ where π is a prime in $\mathbb{Z}[i]$.*

PROOF. Since $p \equiv 1 \pmod 4$, $(-1/p) = 1$. So, $x^2 \equiv -1 \pmod p$ for some $x \in \mathbb{Z}$. If p was prime in $\mathbb{Z}[i]$, then $p \mid (x + i)$ or $p \mid (x - i)$, which implies $bp = \pm 1$ for some $b \in \mathbb{Z}$. Therefore, $p = \pi\gamma$ with $\mathrm{N}(\pi) = \mathrm{N}(\gamma) = p$ and $p = \mathrm{N}(\pi) = \pi\overline{\pi}$. Furthermore, since $\mathrm{N}(\pi)$ is prime, it follows that π is prime in $\mathbb{Z}[i]$. □

PROPOSITION 1.29. *$(1 + i)$ is prime in $\mathbb{Z}[i]$.*

PROOF. Suppose that $(1 + i) = \pi\gamma$ for some non-units $\pi, \gamma \in \mathbb{Z}[i]$. This implies $2 = \mathrm{N}(\pi)\,\mathrm{N}(\gamma)$, which is impossible. □

DEFINITION 1.30. A non-unit $\alpha \in \mathbb{Z}[i]$ is said *primary* if $\alpha \equiv 1 \pmod{2 + 2i}$.

LEMMA 1.31. *A non-unit $\alpha = a + bi$ is primary if and only if either $a \equiv 1 \pmod 4$ and $b \equiv 0 \pmod 4$ or $a \equiv 3 \pmod 4$ and $b \equiv 2 \pmod 4$.*

PROOF. Obvious, since $a + bi \equiv 1 \pmod{2 + 2i}$ implies that $a = 2k + 1$ and $b = 2k$ for some $k \in \mathbb{Z}$. □

PROPOSITION 1.32. *Let a prime $\pi \in \mathbb{Z}[i]$. If $\mathrm{N}(\pi) \equiv 1 \pmod 4$, then among the associates $\{\pm\pi, \pm i\pi\}$ of π, exactly one is primary.*

PROOF. Let $\pi = a + bi$ with $a^2 + b^2 \equiv 1 \pmod 4$. Its associates are

(1) $\pi = a + bi$;
(2) $-\pi = -a - bi$;
(3) $i\pi = -b + ai$;
(4) $-i\pi = b - ai$.

If $a \equiv 0 \pmod 4$, then either $b \equiv 1 \pmod 4$ and (4) is primary, or $b \equiv 3 \pmod 4$ and (3) is primary. The remaining cases are proceeded in a similar way. □

More succinctly, we have shown:

THEOREM 1.33. *The primes in $\mathbb{Z}[i]$ (up to multiplication by ± 1 or $\pm i$) are the rational primes congruent to* 3 mod 4, $(1+i)$, *and the integers of the form $\pi = a+bi$ and $\overline{\pi} = a-bi$ such that a^2+b^2 is a rational prime* *congruent to* 1 mod 4. *In the latter case, if* $\mathrm{N}(\pi) \equiv 1 \pmod 4$, *then among the primes* $\pm\pi$ *and* $\pm i\pi$, *exactly one is congruent to* 1 mod $2 + 2i$. □

THEOREM 1.34. *If* π *is a prime in* $\mathbb{Z}[i]$ *and if* $\pi \nmid \alpha$, *then*

$$\alpha^{\mathrm{N}(\pi)-1} \equiv 1 \pmod{\pi}. \tag{1.14}$$

PROOF. The proof is identical to that of Theorem 1.22 because $\mathbb{Z}[i]/(\pi\,\mathbb{Z}[i])$ is a finite field with $\mathrm{N}(\pi)$ elements from Proposition 9.8.1 in [**147**, p. 121]. □

DEFINITION 1.35. Let π be a prime in $\mathbb{Z}[i]$ with $\mathrm{N}(\pi) \neq 2$. If $\pi \nmid \alpha$, then the *quartic residue symbol* $(\alpha/\pi)_4$ is defined to i^j where j is the unique integer (modulo 4) satisfying

$$\alpha^{(\mathrm{N}(\pi)-1)/4} \equiv i^j \pmod{\pi}. \tag{1.15}$$

If $\pi \mid \alpha$, then $(\alpha/\pi)_4 = 0$.

3. Lucas sequences

Lucas sequences have numerous applications in mathematics. For example, they can be used to construct compositeness and primality tests. They also play a role in the construction of irreducibles and optimal normal bases. Lucas sequences can be used to evaluate the determinants of certain circulant matrices. They allow to identify some properties of Kloosterman and Brewer character sums. The construction of sets of $q-1$ pairwise Latin squares of order q can be achieved thanks to Lucas sequences. We refer to [**214**, Chapter 6] for a description of these applications. Note that these applications are described in terms of Dickson polynomials; but, as we will see, this formulation is equivalent. Moreover, using Weil's Theorem, Lucas sequences enable to efficiently compute the number of points on a elliptic curve over $GF(2^m)$ [**159**]. Finally, Lucas sequences play a role in the design of cryptosystems [**330, 331**].

In this Section, we give the definition of Lucas sequences and derive some properties that will be useful later. We also show the connection between Lucas sequences and Dickson polynomials.

3.1. Definition and properties.

DEFINITION 1.36. Let P, Q be rational integers and let $\Delta = P^2 - 4Q$ be a non-square. If $\alpha = \frac{P+\sqrt{\Delta}}{2}$ and $\beta = \overline{\alpha} = \frac{P-\sqrt{\Delta}}{2}$ are the roots of

$x^2-Px+Q=0$ in the quadratic field $\mathbb{Q}(\sqrt{\Delta})$, then the *Lucas sequences* $\{U_k\}_{k\geq 0}$ *and* $\{V_k\}_{k\geq 0}$ are the rational integers satisfying

$$V_i + U_i\sqrt{\Delta} = 2\alpha^i. \tag{1.16}$$

NOTATION. The k^{th} terms of the Lucas sequences $\{U_i\}_{i\geq 0}$ and $\{V_i\}_{i\geq 0}$ with parameters P and Q will respectively be denoted by $U_k(P,Q)$ and $V_k(P,Q)$.

Remark that since $\alpha \in \mathbb{Q}(\sqrt{\Delta})$ is a root of $x^2-Px+Q=0$, α is an element of $\mathfrak{O}_{\sqrt{\Delta}}$, the ring of integers of the field $\mathbb{Q}(\sqrt{\Delta})$.

From Eq. (1.16) and since $V_i - U_i\sqrt{\Delta} = 2\beta^i$, it follows that

$$U_i = \frac{\alpha^i - \beta^i}{\alpha-\beta} \quad \text{and} \quad V_i = \alpha^i + \beta^i. \tag{1.17}$$

This relation is sometimes used as an alternative definition of Lucas sequences. This second definition enables to efficiently compute the Lucas sequences. We have

$$\begin{aligned} U_{k+m} &= \frac{\alpha^{k+m}-\beta^{k+m}}{\alpha-\beta} \\ &= \frac{(\alpha^k-\beta^k)(\alpha^m+\beta^m)}{\alpha-\beta} - \frac{\alpha^m\beta^m(\alpha^{k-m}-\beta^{k-m})}{\alpha-\beta} \\ &= U_kV_m - Q^mU_{k-m}, \end{aligned} \tag{1.18}$$

and

$$\begin{aligned} V_{k+m} &= \alpha^{k+m}+\beta^{k+m} \\ &= (\alpha^k+\beta^k)(\alpha^m+\beta^m) - \alpha^m\beta^m(\alpha^{k-m}+\beta^{k-m}) \\ &= V_kV_m - Q^mV_{k-m}. \end{aligned} \tag{1.19}$$

In particular, taking $m=1$, we obtain

$$U_{k+1} = PU_k - QU_{k-1} \quad \text{and} \quad V_{k+1} = PV_k - QV_{k-1}.$$

So, using matrix notations, we finally get

$$\begin{aligned} \begin{pmatrix} U_{k+1} & V_{k+1} \\ U_k & V_k \end{pmatrix} &= \begin{pmatrix} P & -Q \\ 1 & 0 \end{pmatrix} \begin{pmatrix} U_k & V_k \\ U_{k-1} & V_{k-1} \end{pmatrix} \\ &= \begin{pmatrix} P & -Q \\ 1 & 0 \end{pmatrix}^k \begin{pmatrix} U_1 & V_1 \\ U_0 & V_0 \end{pmatrix}. \end{aligned} \tag{1.20}$$

LEMMA 1.37. *Any pair (U_i, V_i) with parameters P and Q satisfies*

$$V_i^2 - \Delta U_i^2 = 4Q^i. \tag{1.21}$$

Proof. By definition,

$$V_i^2 - \Delta U_i^2 = (V_i + U_i\sqrt{\Delta})(V_i - U_i\sqrt{\Delta}) = 2\alpha^i 2\overline{\alpha^i} = 4(\alpha\overline{\alpha})^i = 4Q^i.$$

□

Proposition 1.38. *Let $U_i(P,Q)$ and $V_i(P,Q)$ be the i^{th} terms of the Lucas sequences with parameters P, Q and $\Delta = P^2 - 4Q$. Then,*

$$U_{km}(P,Q) = U_k(P,Q)U_m\big(V_k(P,Q),Q^k\big), \tag{1.22}$$

$$V_{km}(P,Q) = V_m\big(V_k(P,Q),Q^k\big), \tag{1.23}$$

$$2U_{k+m}(P,Q) = U_k(P,Q)V_m(P,Q) + U_m(P,Q)V_k(P,Q), \tag{1.24}$$

$$2V_{k+m}(P,Q) = V_k(P,Q)V_m(P,Q) + \Delta U_k(P,Q)U_m(P,Q), \tag{1.25}$$

$$V_{-k}(P,Q) = Q^{-k}V_k(P,Q), \tag{1.26}$$

$$U_{-k}(P,Q) = -Q^{-k}U_k(P,Q). \tag{1.27}$$

Proof. By Lemma 1.37 and letting $P' = V_k(P,Q)$ and $Q' = Q^k$, we have $\Delta' := P'^2 - 4Q' = \Delta U_k^2(P,Q)$. Hence,

$$\begin{aligned}
2\alpha^{km} &= 2^{1-m}\big(2\alpha^k\big)^m = 2^{1-m}\big(V_k(P,Q) + U_k(P,Q)\sqrt{\Delta}\big)^m \\
&= 2^{1-m}(P' + \sqrt{\Delta'})^m = 2\alpha'^m = V_m(P',Q') + U_m(P',Q')\sqrt{\Delta'} \\
&= V_m\big(V_k(P,Q),Q^k\big) + U_m\big(V_k(P,Q),Q^k\big)U_k(P,Q)\sqrt{\Delta},
\end{aligned}$$

which proves Eqs (1.22) and (1.23) by comparison with the coefficients of $2\alpha^{km} = V_{km}(P,Q) + U_{km}(P,Q)\sqrt{\Delta}$. The two next equations are proved in a similar way,

$$\begin{aligned}
4\alpha^{k+m} &= 2\alpha^k\, 2\alpha^m \\
&= \big(V_k(P,Q) + U_k(P,Q)\sqrt{\Delta}\big)\big(V_m(P,Q) + U_m(P,Q)\sqrt{\Delta}\big) \\
&= V_k(P,Q)V_m(P,Q) + U_k(P,Q)U_m(P,Q)\Delta \\
&\qquad + \big(U_k(P,Q)V_m(P,Q) + U_m(P,Q)V_k(P,Q)\big)\sqrt{\Delta}.
\end{aligned}$$

Finally, from $\alpha\overline{\alpha} = Q$, we have

$$\begin{aligned}
V_{-k}(P,Q) + U_{-k}(P,Q)\sqrt{\Delta} = 2\alpha^{-k} &= \frac{2\overline{\alpha}^k}{Q^k} \\
&= \frac{V_k(P,Q)}{Q^k} - \frac{U_k(P,Q)\sqrt{\Delta}}{Q^k}.
\end{aligned}$$

□

THEOREM 1.39. *For any* $\alpha \in \mathfrak{O}_{\sqrt{\Delta}}$,

$$\alpha^p \bmod p = \begin{cases} \alpha & \text{if } (\Delta/p) = 1, \\ \overline{\alpha} & \text{if } (\Delta/p) = -1, \end{cases} \tag{1.28}$$

where (Δ/p) *denotes the Legendre symbol.*

PROOF. From Proposition 1.7, $\Delta^{\frac{p-1}{2}} \equiv (\Delta/p) \pmod p$. Therefore,

$$\begin{aligned} \alpha^p &\equiv \frac{(P+\sqrt{\Delta})^p}{2^p} \equiv \frac{1}{2}\sum_{i=0}^{p}\binom{p}{i}P^i(\sqrt{\Delta})^{p-i} \\ &\equiv \frac{P^p+(\sqrt{\Delta})^p}{2} \equiv \frac{P+(\Delta/p)\sqrt{\Delta}}{2} \pmod p. \end{aligned}$$

□

COROLLARY 1.40. *If p is an odd prime that does divide Δ, then*

$$\begin{cases} U_{p-(\Delta/p)}(P,1) \equiv 0 \pmod p, \\ V_{p-(\Delta/p)}(P,1) \equiv 2 \pmod p. \end{cases} \tag{1.29}$$

PROOF. Let α be a non-zero integer of $\mathfrak{O}_{\sqrt{\Delta}}$. From Theorem 1.39 follows $\alpha^{p-1} \equiv 1 \pmod p$ if $(\Delta/p) = 1$ and $\alpha^{p+1} \equiv \alpha\overline{\alpha} \equiv Q \equiv 1$ if $(\Delta/p) = -1$. Hence, by Eq. (1.16), $V_{p-(\Delta/p)}(P,1) + U_{p-(\Delta/p)}(P,1)\sqrt{\Delta} \equiv 2 \pmod p$. □

3.2. Dickson polynomials. These polynomials were introduced by Dickson in [**96**]. They enable to consider Lucas sequences as polynomials.

DEFINITION 1.41. The *Dickson polynomials of the first kind, denoted by* $D_n(x,a)$, are given by

$$D_n(x,a) = \sum_{i=0}^{\lfloor n/2 \rfloor} \frac{n}{n-i}\binom{n-i}{i}(-a)^i x^{n-2i}. \tag{1.30}$$

The *Dickson polynomials of the second kind* $E_n(x,a)$ are given by

$$E_n(x,a) = \sum_{i=0}^{\lfloor n/2 \rfloor} \binom{n-i}{i}(-a)^i x^{n-2i}. \tag{1.31}$$

The next proposition shows that Lucas sequences and Dickson polynomials are essentially the same functions.

PROPOSITION 1.42. *The Dickson polynomials and the Lucas sequences are connected by the following relations*

$$D_n(x,a) = V_n(x,a) \quad \text{and} \quad E_n(x,a) = U_{n+1}(x,a). \tag{1.32}$$

PROOF. We shall only prove the first equality. Using the same notations as in Definition 1.36, we have $V_n(P,Q) = \alpha^n + \beta^n$. By Waring's formula [**216**, p. 30], we obtain

$$\begin{aligned}
\alpha^n + \beta^n &= \sum_{i_1+2i_2=n} (-1)^{i_2} \frac{(i_1+i_2-1)!\,n}{i_1!\,i_2!} (\alpha+\beta)^{i_1}(\alpha\beta)^{i_2} \\
&= \sum_{i_1+2i_2=n} \frac{(i_1+i_2-1)!\,n}{i_1!\,i_2!} P^{i_1}(-Q)^{i_2} \\
&= \sum_{i_2=0}^{\lfloor n/2 \rfloor} \frac{n}{n-i_2} \binom{n-i_2}{i_2} P^{n-2i_2}(-Q)^{i_2} = D_n(P,Q).
\end{aligned}$$

□

4. Elliptic curves

Elliptic curves is one of the oldest and most fascinating branch in mathematics. They recently gained more interest thanks to cryptography. All began when Lenstra discovered a factorization algorithm over these structures [**209**]. Thereafter, Koblitz [**177**] and Miller [**240**] independently proposed to adapt existing cryptographic protocols on elliptic curves.

The theory of elliptic curves is quite difficult; we will only introduce the rudiments that will be useful for our purposes. The interested reader may for example consult [**316**] for further study. In this Section, we recall the definition of an elliptic curve over a field and over a ring. We also give some basic properties. Finally, we introduce the division polynomials.

4.1. Elliptic curves over a field.

DEFINITION 1.43. 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 Weierstraß equation

$$y^2 = x^3 + ax + b \tag{1.33}$$

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

REMARK 1.44. If K is the prime field $\mathbb{F}_p$, then the equation $x^3 + ax + b$ has no multiple roots if and only if $\gcd(4a^3 + 27b^2, p) = 1$.

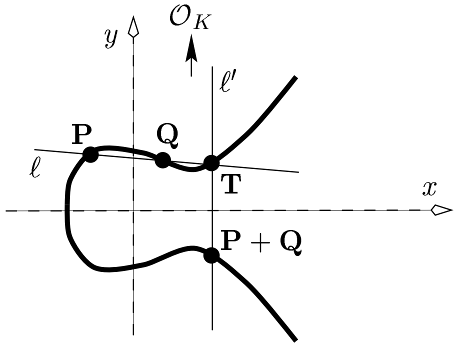

Figure 1.1: Group law on $E(a,b)$

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 $\mathcal{O}_K$, then $\mathbf{P} + \mathbf{Q}$ is the point such that ℓ' intersects $E(a,b)$ at $\mathbf{T}, \mathcal{O}_K$ and $\mathbf{P} + \mathbf{Q}$.

PROPOSITION 1.45. *The previous composition law makes $E(a,b)$ into an Abelian group with identity element $\mathcal{O}_K$.*

PROOF. Elementary proofs of this proposition are quite long (see [**152**] for example). However this proposition can also be seen as a consequence of Abel's Theorem [**221, 9**]. □

Algebraically, we have

(i) $\mathcal{O}_K$ is the identity element, i.e. $\forall \mathbf{P} \in E(a,b)$, $\mathbf{P} + \mathcal{O}_K = \mathbf{P}$.
(ii) The inverse of $\mathbf{P} = (x_1, y_1)$ is $-\mathbf{P} = (x_1, -y_1)$.
(iii) Let $\mathbf{P} = (x_1, y_1)$ and $\mathbf{Q} = (x_2, y_2) \in E(a,b)$ with $\mathbf{P} \neq -\mathbf{Q}$. Then $\mathbf{P} + \mathbf{Q} = (x_3, y_3)$ where

$$x_3 = \lambda^2 - x_1 - x_2 \tag{1.34}$$

$$y_3 = \lambda(x_1 - x_3) - y_1 \tag{1.35}$$

and $\lambda = \begin{cases} \dfrac{3x_1^2 + a}{2y_1} & \text{if } x_1 = x_2, \\ \dfrac{y_1 - y_2}{x_1 - x_2} & \text{otherwise.} \end{cases}$

Note that if $\mathbf{P} = (x_1, 0) \in E(a,b)$, then $[2]\mathbf{P} = \mathcal{O}_K$.

In the sequel, we will see some properties of the order and the structure of elliptic curves over finite prime fields.

THEOREM 1.46 (Hasse). *If K is the finite prime field $\mathbb{F}_p$, then the order of the group $E_p(a,b)$ (i.e. the elliptic curve $E(a,b)$ over $\mathbb{F}_p$) is given by*

$$\#E_p(a,b) = p + 1 - a_p \tag{1.36}$$

where $|a_p| \leq 2\sqrt{p}$.

PROOF. See [**316**, p. 131], Theorem 1.1. □

THEOREM 1.47. *The group $E_p(a,b)$ is either cyclic or isomorphic to a product of two cyclic groups. Furthermore, we can write $E_p(a,b) \cong \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2}$ with $n_2 \mid n_1$ and $n_2 \mid p-1$.*

PROOF. The proof involves higher mathematics. The required material can be found in [**56**]. □

COROLLARY 1.48. *In $E_p(a,b)$, the number of points of order dividing j is equal to*

$$\gcd(j, n_1)\, \gcd(j, n_2). \tag{1.37}$$

PROOF. From Theorem 1.47, we can write

$$E_p(a,b) = \{\mathbf{P} = [u]\mathbf{R} + [v]\mathbf{S} \mid 0 \leq u < n_1 \text{ and } 0 \leq n_2 < v\}.$$

Hence $[j]\mathbf{P} = [ju]\mathbf{R} + [jv]\mathbf{S} = \mathcal{O}_p$ if and only if $ju \equiv 0 \pmod{n_1}$ and $jv \equiv 0 \pmod{n_2}$. There are thus $\gcd(j,n_1)\gcd(j,n_2)$ points of order dividing j. □

DEFINITION 1.49. Let $E_p(a,b)$ be an elliptic curve over the prime field $\mathbb{F}_p$. Let D_p be a quadratic non-residue modulo p. The *complementary group of $E_p(a,b)$*, denoted by $\overline{E_p(a,b)}$, is the elliptic curve given by the (extended) Weierstraß equation

$$D_p y^2 = x^3 + ax + b \tag{1.38}$$

together with the point at infinity $\mathcal{O}_p$. The sum of two points (that are not inverse of each other) $(x_1, y_1) + (x_2, y_2) = (x_3, y_3)$ can be computed by

$$x_3 = \lambda^2 D_p - x_1 - x_2$$
$$y_3 = \lambda(x_1 - x_3) - y_1$$

and $\lambda = \begin{cases} \dfrac{3x_1^2 + a}{2D_p y_1} & \text{if } x_1 = x_2, \\ \dfrac{y_1 - y_2}{x_1 - x_2} & \text{otherwise.} \end{cases}$

COROLLARY 1.50. *If* $\#E_p(a,b) = p + 1 - a_p$, *then* $\#\overline{E_p(a,b)} = p + 1 + a_p$.

PROOF. Letting $a_p = -\sum_{x \in \mathbb{F}_p} \big(1 + (x^3 + ax + b/p)\big)$ and counting the point at infinity, we have

$$\#E_p(a,b) = 1 + \sum_{x \in \mathbb{F}_p} \left(1 + \left(\frac{x^3 + ax + b}{p}\right)\right) = 1 + p - a_p.$$

Hence,

$$\#\overline{E_p(a,b)} = 1 + \sum_{x \in \mathbb{F}_p} \left(1 - \left(\frac{x^3 + ax + b}{p}\right)\right) = 1 + p + a_p.$$

□

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

LEMMA 1.51. *Let p be an odd prime congruent to* $2 \bmod 3$. *Then the elliptic curve $E_p(0,b)$ is a cyclic group of order $p+1$.*

PROOF. Since $p \equiv 2 \pmod 3$, cube roots exist and are unique. Consequently, there are $p+1$ points on $E_p(0,b)$, namely p points of the form $(\sqrt[3]{y^2 - b}, y)$ with $y \in \mathbb{F}_p$ and the point at infinity.

By Theorem 1.47, $E_p(0,b) \cong \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2}$ with $n_2 \mid n_1$ and $n_2 \mid p-1$. Since $n_1 n_2 = p+1$, n_2 is equal to 1 or to 2. But n_2 cannot be 2 because $E_p(0,b)$ has only 2 points of order dividing 2, namely $(\sqrt[3]{-b}, 0)$ and $\mathcal{O}_p$. Therefore, by Corollary 1.48, $n_2 = 1$ and $E_p(0,b)$ is cyclic. □

LEMMA 1.52. *Let p be a prime congruent to* $3 \bmod 4$. *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 quadratic non-residue modulo p, then $E_p(a,0)$ is a group isomorphic to $\mathbb{Z}_{(p+1)/2} \times \mathbb{Z}_2$ of order $p+1$.*

PROOF. Since $p \equiv 3 \pmod 4$, $(-1/p) = -1$ and

$$\left(\frac{(-x)^3 + a(-x)}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{x^3 + ax}{p}\right) = -\left(\frac{x^3 + ax}{p}\right).$$

So, $\sum_{x \in \mathbb{F}_p} (x^3 + ax/p) = 0$ because the term for x and the term for $-x$ cancel in the sum. Therefore, $a_p = 0$ and $\#E(a,0) = p+1$.

As in the proof of Lemma 1.51, $E_p(a,0) \cong \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2}$ with $n_2 = 1$ or 2. If $(a/p) = 1$, then the equation $x^3 + ax \equiv 0 \pmod{p}$ has only the solution $x = 0$ because $p \equiv 3 \pmod{4}$ implies $(-a/p) = -1$. Therefore, $E_p(a,0)$ has only two points of order dividing 2, namely $(0,0)$ and $\mathcal{O}_p$, and $E_p(a,0)$ is cyclic. Otherwise, if $(a/p) = -1$, the equation $x^3+ax \equiv 0 \pmod{p}$ has 3 solutions, namely $x = 0$ and $x = \pm\sqrt{a}$. Hence, $E_p(a,0)$ has 4 points of order dividing 2, namely $(0,0)$, $(\pm\sqrt{a}, 0)$ and $\mathcal{O}_p$, and $n_2 = 2$ by Corollary 1.48. □

LEMMA 1.53. *Let p be a prime congruent to 1 modulo 3. If $p = \pi_p\overline{\pi_p}$ with $\pi_p \in \mathbb{Z}[w]$ and $\pi_p \equiv 2 \pmod{3}$, then*

$$\#E_p(0,b) = p + 1 + \overline{\left(\frac{4b}{\pi_p}\right)_6}\pi_p + \left(\frac{4b}{\pi_p}\right)_6\overline{\pi_p}. \tag{1.39}$$

PROOF. See [**147**, p. 305], Theorem 4. □

LEMMA 1.54. *Let p be prime congruent to 1 modulo 4. If $p = \pi_p\overline{\pi_p}$ with $\pi_p \in \mathbb{Z}[i]$ and $\pi_p \equiv 1 \pmod{2+2i}$, then*

$$\#E_p(a,0) = p + 1 - \overline{\left(\frac{-a}{\pi_p}\right)_4}\pi_p - \left(\frac{-a}{\pi_p}\right)_4\overline{\pi_p}. \tag{1.40}$$

PROOF. See [**147**, p. 307], Theorem 5. □

4.2. Elliptic curves over a ring. Elliptic curves over rings are defined similarly as over the field $\mathbb{F}_p$. The main difference is that they do not define an Abelian group.

DEFINITION 1.55. Let n be the product of two primes p and q, and let a, b such that $\gcd(4a^3 + 27b^2, n) = 1$. 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

$$y^2 = x^3 + ax + b \tag{1.41}$$

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

Consider the group $\widetilde{E}_n(a,b)$ given by the direct product

$$\widetilde{E}_n(a,b) = E_p(a,b) \times E_q(a,b). \tag{1.42}$$

By Theorem 1.12, there exists a unique point $\mathbf{P} = (x_1, y_1) \in E_n(a,b)$ for every pair of points $\mathbf{P}_p = (x_{1p}, y_{1p}) \in E_p(a,b) \setminus \{\mathcal{O}_p\}$ and $\mathbf{P}_q = (x_{1q}, y_{1q}) \in E_q(a,b) \setminus \{\mathcal{O}_q\}$ such that $x_1 \bmod p = x_{1p}$, $x_1 \bmod q = x_{1q}$, $y_1 \bmod p = y_{1p}$ and $y_1 \bmod q = y_{1q}$. This equivalence will be denoted by $\mathbf{P} = [\mathbf{P}_p, \mathbf{P}_q]$. Since $\mathcal{O}_n = [\mathcal{O}_p, \mathcal{O}_q]$, the group $\widetilde{E}_n(a,b)$ consists of all the points of $E_n(a,b)$ together with a number of points of the form $[\mathbf{P}_p, \mathcal{O}_q]$ or $[\mathcal{O}_p, \mathbf{P}_q]$.

LEMMA 1.56. *The tangent-and-chord addition on $E_n(a,b)$, whenever it is defined, coincides with the group operation on $\widetilde{E}_n(a,b)$.*

PROOF. Let $\mathbf{P}$ and $\mathbf{Q} \in E_n(a,b)$. Assume $\mathbf{P}+\mathbf{Q}$ is well-defined by the tangent-and-chord rule. Therefore $\mathbf{P}+\mathbf{Q} = [(\mathbf{P}+\mathbf{Q})_p, (\mathbf{P}+\mathbf{Q})_q] = [\mathbf{P}_p+\mathbf{Q}_p, \mathbf{P}_q+\mathbf{Q}_q]$. □

If n is the product of two large primes, it is extremely unlikely that the "addition" is not defined on $E_n(a,b)$. Consequently, computations in $\widetilde{E}_n(a,b)$ can be performed without knowing the two prime factors of n.

Although $E_n(a,b)$ is not a group, a proposition similar to Lagrange's Theorem holds.

PROPOSITION 1.57. *Let $n = pq$ and let $E_n(a,b)$ be an elliptic curve over $\mathbb{Z}_n$. If $N_n = \operatorname{lcm}(\#E_p(a,b), \#E_q(a,b))$, then*

$$\forall \mathbf{P} \in E_n(a,b), \forall k \in \mathbb{Z} : [kN_n+1]\mathbf{P} = \mathbf{P}, \tag{1.43}$$

with the overwhelming probability for large p and q.

PROOF. Since $[kN_n+1]\mathbf{P}_p = \mathbf{P}_p$ and $[kN_n+1]\mathbf{P}_q = \mathbf{P}_q$, $[kN_n+1]\mathbf{P} = \mathbf{P}$ by Lemma 1.56.

Multiple of points can be computed in polynomial time (see for example [**249**]). Therefore, there exists a polynomial chain of intermediate points $\mathbf{P_j} := [j]\mathbf{P}$ from which we can compute $[kN_n+1]\mathbf{P}$. The computation of $[kN_n+1]\mathbf{P}$ cannot be achieved if one of the points $\mathbf{P_j}$ is of the form $[\mathcal{O}_p, \mathbf{P_j}_q]$ or $[\mathbf{P_j}_p, \mathcal{O}_q]$. Let us analyze the probability that some $\mathbf{P_j}_p$ is equal to $\mathcal{O}_p$. From Theorem 1.47, we can write

$$E_p(a,b) = \{\mathbf{P}_p = [u]\mathbf{R} + [v]\mathbf{S} \mid 0 \le u < n_1 \text{ and } 0 \le v < n_2\}.$$

Hence, from Corollary 1.48 and assuming that $\mathbf{P}_p \neq \mathcal{O}_p$, the probability that $\mathbf{P_j}_p = \mathcal{O}_p$ is equal to

$$\frac{\gcd(n_1,j) \times \gcd(n_2,j) - 1}{n_1 n_2 - 1}.$$

So, since the chain of intermediate points is polynomial while the number of "bad" points $\mathbf{P_j}$ in this chain is exponentially small, the probability that $[kN_n+1]\mathbf{P}$ cannot be computed is negligible. □

4.3. Division polynomials. Division polynomials play the same role as Dickson polynomials for Lucas sequences. They enable to express multiples of points in terms of polynomials.

DEFINITION 1.58. Let $E_n(a,b)$ be an elliptic curve over the ring $\mathbb{Z}_n$. Consider the polynomials $\mathcal{P}_i \in \mathbb{Z}_n[a,b,x]$ defined by

(i) $\mathcal{P}_0 = 0$,
(ii) $\mathcal{P}_1 = 1$,
(iii) $\mathcal{P}_2 = 1$,
(iv) $\mathcal{P}_3 = 3x^4 + 6ax^2 + 12bx - a^2$,
(v) $\mathcal{P}_4 = 2(x^6 + 5ax^4 + 20bx^3 - 5a^2x^2 - 4abx - 8b^2 - a^3)$,
(vi) for $i > 2$,

$$\mathcal{P}_{2i} = \mathcal{P}_i(\mathcal{P}_{i+2}\mathcal{P}_{i-1}^2 - \mathcal{P}_{i-2}\mathcal{P}_{i+1}^2),$$

and for $i \geq 2$,

$$\mathcal{P}_{2i+1} = \begin{cases} \mathcal{P}_{i+2}\mathcal{P}_i^3 - \mathcal{P}_{i+1}^3\mathcal{P}_{i-1}16(x^3+ax+b)^2 & \text{if } i \text{ is odd,} \\ 16(x^3+ax+b)^2\,\mathcal{P}_{i+2}\mathcal{P}_i^3 - \mathcal{P}_{i+1}^3\mathcal{P}_{i-1} & \text{if } i \text{ is even.} \end{cases}$$

Letting $\Psi_i(x,y) = \begin{cases} \mathcal{P}_i(x) & \text{if } i \text{ is odd} \\ 2y\,\mathcal{P}_i(x) & \text{if } i \text{ is even} \end{cases}$, define the polynomials Φ_i and $\omega_i \in \mathbb{Z}_n[a,b,x,y]$ by

$$\Phi_i = x\Psi_i^2 - \Psi_{i+1}\Psi_{i-1},$$
$$4y\,\omega_i = \Psi_{i+2}\Psi_{i-1}^2 - \Psi_{i-2}\Psi_{i+1}^2.$$

One of the most important results about division polynomials is given in the next proposition.

PROPOSITION 1.59. *Let $E_n(a,b)$ be an elliptic curve over $\mathbb{Z}_n$.*

(a) Ψ_i, Φ_i, $y^{-1}\omega_i$ *(for i odd) and* $y^{-1}\Psi_i$, Φ_i, ω_i *(for i even) are polynomials in $\mathbb{Z}_n[a,b,x,y^2]$. Hence, by replacing y^2 by x^3+ax+b, they will be considered as polynomials in $\mathbb{Z}_n[a,b,x]$.*
(b) *As polynomials in x,*

$$\Phi_k(x) = x^{k^2} + \textit{lower order terms}, \tag{1.44}$$

$$\Psi_k(x)^2 = k^2x^{k^2-1} + \textit{lower order terms}. \tag{1.45}$$

(c) *If $\mathbf{P} \in E_n(a,b)$, then*

$$\mathbf{Q} = [k]\mathbf{P} = \left(\frac{\Phi_k(\mathbf{P})}{\Psi_k(\mathbf{P})^2}, \frac{\omega_k(\mathbf{P})}{\Psi_k(\mathbf{P})^3}\right) \pmod{n}. \tag{1.46}$$

PROOF. See [**201**, p. 38], Theorem 2.1. ☐

COROLLARY 1.60. *Let $\mathcal{F}_i, \mathcal{G}_i$ and $\mathcal{H}_i$ be the rational functions defined by*

(i) $\mathcal{F}_1(x) = 1$ *and* $\mathcal{G}_1(x) = x \bmod n$,
(ii) *for* $i \geq 2$,

$$\mathcal{F}_i(x) = \begin{cases} \dfrac{\mathcal{P}_{i+2}(x)\mathcal{P}_{i-1}(x)^2 - \mathcal{P}_{i-2}(x)\mathcal{P}_{i+1}(x)^2}{\mathcal{P}_i(x)^3} \bmod n & \textit{for } i \textit{ odd} \\ \dfrac{\mathcal{P}_{i+2}(x)\mathcal{P}_{i-1}(x)^2 - \mathcal{P}_{i-2}(x)\mathcal{P}_{i+1}(x)^2}{16(x^3+ax+b)^2\,\mathcal{P}_i(x)^3} \bmod n & \textit{for } i \textit{ even} \end{cases}$$

$$\mathcal{G}_i(x) = \begin{cases} x - 4(x^3+ax+b)\,\dfrac{\mathcal{P}_{i+1}(x)\mathcal{P}_{i-1}(x)}{\mathcal{P}_i(x)^2} \bmod n & \textit{for } i \textit{ odd} \\ x - \dfrac{1}{4(x^3+ax+b)}\dfrac{\mathcal{P}_{i+1}(x)\mathcal{P}_{i-1}(x)}{\mathcal{P}_i(x)^2} \bmod n & \textit{for } i \textit{ even} \end{cases}$$

$\mathcal{H}_i(x,y) = y\,\mathcal{F}_i(x) \bmod n.$

If $\mathbf{P} = (p_1, p_2)$ *and* $\mathbf{Q} = [k]\mathbf{P} = (q_1, q_2)$, *then*

$$q_1 = \mathcal{G}_k(p_1) \quad \textit{and} \quad q_2 = p_2\,\mathcal{F}_k(p_1) = \mathcal{H}_k(p_1, p_2). \tag{1.47}$$

PROOF. If k (≥ 3) is odd, then

$$\begin{aligned} \Phi_k(p_1,p_2) &= p_1\Psi_k(p_1,p_2)^2 - \Psi_{k+1}(p_1,p_2)\Psi_{k-1}(p_1,p_2) \\ &= p_1\mathcal{P}_k(p_1)^2 - 4(p_1^3 + ap_1 + b)\,\mathcal{P}_{k+1}(p_1)\mathcal{P}_{k-1}(p_1), \end{aligned}$$

and $\Psi_k(p_1,p_2)^2 = \mathcal{P}_k(p_1)^2$. Hence, $q_1 = \Phi_k(p_1,p_2)/\Psi_k(p_1,p_2)^2 = \mathcal{G}_k(p_1)$. Note that if $k = 1$, then $q_1 = p_1 = \mathcal{G}_1(p_1)$. Moreover,

$$\begin{aligned} \omega_k(p_1,p_2) &= \frac{1}{4p_2}\big(\Psi_{k+2}(p_1,p_2)\Psi_{k-1}(p_1,p_2)^2 \\ &\qquad -\Psi_{k-2}(p_1,p_2)\Psi_{k+1}(p_1,p_2)^2\big) \\ &= p_2\left(\mathcal{P}_{k+2}(p_1)\mathcal{P}_{k-1}(p_1)^2 - \mathcal{P}_{k-2}(p_1)\mathcal{P}_{k+1}(p_1)^2\right), \end{aligned}$$

and $\Psi_k(p_1,p_2)^3 = \mathcal{P}_k(p_1)^3$. Therefore, $q_2 = \omega_k(p_1,p_2)/\Psi_k(p_1,p_2)^3 = p_2\,\mathcal{F}_k(p_1) = \mathcal{H}_k(p_1,p_2)$. Note also that if $k = 1$, then $q_2 = p_2 = \mathcal{H}_1(p_1,p_2)$.

The case k even is treated in a similar way. □

PROPOSITION 1.61. *Functions $\mathcal{G}_i$ and $\mathcal{F}_i$ satisfy*

$$\mathcal{G}_{km}(x) = \mathcal{G}_m\big(\mathcal{G}_k(x)\big), \tag{1.48}$$

$$\mathcal{F}_{km}(x) = \mathcal{F}_k(x)\mathcal{F}_m\big(\mathcal{G}_k(x)\big), \tag{1.49}$$

if $k \neq m$, then

(1.50)
$$\mathcal{G}_{k+m}(x) = -\mathcal{G}_k(x) - \mathcal{G}_m(x) + (x^3 + ax + b)\left(\frac{\mathcal{F}_k(x) - \mathcal{F}_m(x)}{\mathcal{G}_k(x) - \mathcal{G}_m(x)}\right)^2$$

and

(1.51)
$$\mathcal{F}_{k+m}(x) = -\mathcal{F}_k(x) + \frac{\mathcal{F}_k(x) - \mathcal{F}_m(x)}{\mathcal{G}_k(x) - \mathcal{G}_m(x)}\big(\mathcal{G}_k(x) - \mathcal{G}_{k+m}(x)\big),$$

$$\mathcal{G}_{-k}(x) = \mathcal{G}_k(x), \tag{1.52}$$

$$\mathcal{F}_{-k}(x) = -\mathcal{F}_k(x). \tag{1.53}$$

Proof. Let $\mathbf{P} = (x, y)$ be a generic point on $E_n(a, b)$. Then,

$$\mathcal{G}_{km}(x) = \mathrm{x}([km]\mathbf{P}) = \mathrm{x}\big([m]([k]\mathbf{P})\big) = \mathcal{G}_m\big(\mathrm{x}([k]\mathbf{P})\big) = \mathcal{G}_m\big(\mathcal{G}_k(x)\big)$$

and

$$\mathcal{F}_{km}(x) = \frac{\mathrm{y}([km]\mathbf{P})}{\mathrm{y}(\mathbf{P})} = \frac{\mathrm{y}\big([m]([k]\mathbf{P})\big)}{\mathrm{y}([k]\mathbf{P})}\,\frac{\mathrm{y}([k]\mathbf{P})}{\mathrm{y}(\mathbf{P})} = \mathcal{F}_m\big(\mathcal{G}_k(x)\big)\mathcal{F}_k(x),$$

which proves Eqs (1.48) and (1.49). Eqs (1.50) and (1.51) are an application of addition formulae on elliptic curves. Finally, since $[-k]\mathbf{P} = [k](-\mathbf{P}) = [k](x, -y)$, we have Eqs (1.52) and (1.53). □

Remark 1.62. Note the great similarity of this proposition with Proposition 1.38 on Lucas sequences. Indeed, using the alternative definition in terms of Dickson polynomials (see Proposition 1.42), we have

$$\begin{aligned}
D_{km}(x, 1) &= D_m\big(D_k(x, 1), 1\big),\\
E_{km}(x, 1) &= E_k(x, 1)E_m\big(D_k(x, 1), 1\big),\\
D_{-k}(x, 1) &= D_k(x, 1),\\
E_{-k}(x, 1) &= (-1)^k E_k(x, 1).
\end{aligned}$$

This has to be compared to Eqs (1.48), (1.49), (1.52) and (1.53), respectively.

5. Lattice basis reduction

The theory of lattice reduction was introduced by Lagrange in order to define a reduced form associated to a quadratic form. This notion was later reconsidered by several mathematicians, including Hermite, Korkine, Zolotarev, Gauss and Minkowski. The theory of lattice reduction re-emerged in 1982 when Lenstra, Lenstra and Lovász [**206**] proposed a polynomial time algorithm, the so-called LLL algorithm, that transforms a basis of a lattice into a reduced basis in the sense of Lovász. Although the resulting basis is not always optimal, this technique revealed itself to be a powerful tool to mount successful attacks on knapsack based cryptosystems [**150**] or to find roots of polynomial equations [**70, 68, 69**].

DEFINITION 1.63. A subset L of the vector space $\mathbb{R}^n$ is called a *lattice* if there exists n linearly independent vectors $\vec{b_i} \in \mathbb{R}^n$ such that

$$L = \left\{ \sum_{i=1}^{n} r_i \, \vec{b_i} \mid r_i \in \mathbb{Z} \right\}.$$

The set $\{\vec{b_1}, \ldots, \vec{b_n}\}$ is called a *basis of* L and n is its *rank*. The *determinant of* L is the quantity $\Delta(L) = |\det(\vec{b_1}, \ldots, \vec{b_n})|$, where the $\vec{b_i}$ are written as column vectors.

PROPOSITION 1.64. $\Delta(L)$ *is a positive quantity that does not depend on the choice of the basis.*

PROOF. See [**55**, p. 10], Section I.2. □

DEFINITION 1.65. The k^{th} *minimum of a lattice* L is the smallest positive real number $\Lambda_k(L)$ such that there exists k linearly independent vectors $\vec{v_1}, \ldots, \vec{v_k} \in L$ satisfying $\|\vec{v_i}\|^2 \leq \Lambda_k(L)$, for $i = 1, \ldots, k$.

In dimension 2, a basis is called *reduced* if it realizes the minima $\Lambda_1(L)$ and $\Lambda_2(L)$. This can be achieved by the Gaussian algorithm.

ALGORITHM 1.66 (Gauss).

<u>`Input:`</u> $\{\vec{b_1}, \vec{b_2}\}$ `basis with` $\|\vec{b_1}\| \geq \|\vec{b_2}\|$

    `do`

        $\lambda := \left\lfloor \frac{\langle \vec{b_1}, \vec{b_2} \rangle}{\langle \vec{b_2}, \vec{b_2} \rangle} \right\rceil$

        $\vec{b_1} := \vec{b_1} - \lambda \vec{b_2}$

        `exchange` $\vec{b_1}$ `and` $\vec{b_2}$

    `until` $\|\vec{b_1}\| \leq \|\vec{b_2}\|$

<u>`Output:`</u> $\{\vec{b_1}, \vec{b_2}\}$ `reduced basis`

In higher dimension, a reduced basis cannot be defined as the set of vectors realizing the minima $\Lambda_i(L)$ because this set of vectors does not necessarily exist.

Until 1982, there was no general definition for lattice reduction. The LLL reduction [**206**] relies on the Gram-Schmidt orthogonalization process.

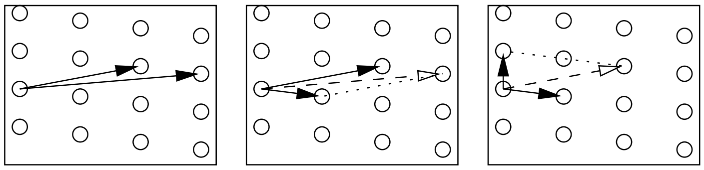

Figure 1.2: Gauss' reduction algorithm

Algorithm 1.67 (Gram-Schmidt).

<u>`Input:`</u> $\{\vec{b_1}\dots,\vec{b_n}\}$ `a basis of` $\mathbb{R}^n$

`for` $i := 1$ `to` n `do`

  $\vec{b_i^*} := \vec{b_i}$

  `for` $j := 1$ `to` $i-1$ `do`

    $\mu_{i,j} := \frac{\langle \vec{b_i}, \vec{b_j^*}\rangle}{\langle \vec{b_j^*}, \vec{b_j^*}\rangle}$

    $\vec{b_i^*} := \vec{b_i^*} - \mu_{i,j}\vec{b_j^*}$

  `od`

`od`

<u>`Output:`</u> $\{\vec{b_1^*},\dots,\vec{b_n^*}\}$ `an orthogonal basis`

Remark 1.68. At step i, the vector $\vec{b_i^*}$ is not only orthogonal to all the $\vec{b_\ell^*}$ $(\ell < i)$, but also to all the $\vec{b_\ell}$ since $\sum_j \mathbb{R}\vec{b_j} = \sum_j \mathbb{R}\vec{b_j^*}$.

Definition 1.69. The basis $\{\vec{b_1}\dots,\vec{b_n}\}$ of a lattice L is called *LLL-reduced* if

$$|\mu_{i,j}| \leq 1/2 \quad \text{for } 1 \leq j < i \leq n \quad \text{[size reduction]}, \tag{1.54}$$

and for $1/4 \leq t \leq 1$

$$\|\vec{b_i^*} + \mu_{i,i-1}\vec{b_{i-1}^*}\|^2 \geq t\,\|\vec{b_{i-1}^*}\|^2 \quad \text{for } 1 < i \leq n \tag{1.55}$$

[Lovász condition].

The LLL algorithm is a combination of Gauss and Gram-Schmidt. We shall describe it in its simplest form. Suppose that the vectors $\{\vec{b_1},\dots\vec{b_{k-1}}\}$ are already reduced. The next vector to be reduced is $\vec{b_k}$. We first have to satisfy the size reduction, *i.e.* $|\mu_{k,j}| \leq 1/2$ for $1 \leq j < k$.

ALGORITHM 1.70 (Size Reduction).

```
Input: {b_1 ..., b_{k-1}} a set of LLL-reduced vectors
    for j := k-1 downto 1 do
        q := ⌊μ_{k,j}⌉   (= ⌊<b_k, b_j^*> / <b_j^*, b_j^*>⌉)
        if q > 1/2 then
            b_k := b_k - q b_j
            update μ_{k,ℓ} for ℓ = 1, ..., j
        fi
    od
Output: {b_1 ..., b_{k-1}, b_k} a set of size-reduced vectors
```

Suppose that $q > 1/2$ at step j, then $|\mu_{k,j}^{(\text{updated})}| = |\mu_{k,j} - q| \leq 1/2$. Furthermore, the values of $\mu_{k,\ell}$ are not affected by the updating for $\ell > j$:

$$\mu_{k,\ell}^{(\text{updated})} = \mu_{k,\ell} - q\frac{\langle \vec{b_j}, \vec{b_\ell^*}\rangle}{\langle \vec{b_\ell^*}, \vec{b_\ell^*}\rangle} = \mu_{k,\ell}$$

because $\vec{b_\ell^*}$ is orthogonal to $\vec{b_j}$ if $j < \ell$ (see Remark 1.68).

Now, we have to fulfill the Lovász condition. If

$$\|\vec{b_k^*} + \mu_{k,k-1}\vec{b_{k-1}^*}\|^2 \geq t\,\|\vec{b_{k-1}^*}\|^2,$$

we are done and $\{\vec{b_1}, \ldots, \vec{b_k}\}$ are LLL-reduced. Otherwise, we exchange the vectors $\vec{b_{k-1}}$ and $\vec{b_k}$. We then reiterate the same process with input $\{\vec{b_1}, \ldots, \vec{b_{k-2}}\}$ are LLL-reduced vectors.

Lenstra, Lenstra and Lovász proved that their algorithm terminates. It runs in polynomial time at most $O(n^6 \log^3 B)$ where $B = \max_i \|\vec{b_i}\|$. However, in practice, this bound is quite pessimistic. Efficient implementations of this algorithm are presented in [**305**].

Once a basis is LLL-reduced, it fulfills the following useful properties.

THEOREM 1.71. *Let $\{\vec{b_1}, \ldots, \vec{b_n}\}$ be a LLL-reduced basis of a lattice L. Then,*

$$\Delta(L) \leq \prod_{i=1}^{n} \|\vec{b_i}\| \leq 2^{n(n-1)/4}\Delta(L), \tag{1.56}$$

$$\|\vec{b_j}\| \leq 2^{(i-1)/2}\|\vec{b_i^*}\| \quad \text{for } 1 \leq j \leq i \leq n, \tag{1.57}$$

$$\|\vec{b_1}\| \leq 2^{(n-1)/4}\Delta(L)^{1/n}, \tag{1.58}$$

$$\|\vec{b_1}\| \leq 2^{(n-1)/2}\|\vec{x}\| \quad \forall \vec{x}(\neq \vec{0}) \in L. \tag{1.59}$$

Furthermore, for any linearly independent vectors $\vec{x_1}, \vec{x_2}, \ldots, \vec{x_t} \in L$,

$$\|\vec{b_j}\| \le 2^{(n-1)/2} \max(\|\vec{x_1}\|, \|\vec{x_2}\|, \ldots, \|\vec{x_t}\|) \quad \text{for } 1 \le j \le t. \tag{1.60}$$

PROOF. See [**67**, p. 84], Theorem 2.6.2. □

References

[9] N. I. Akhiezer, *Elements of the theory of elliptic functions*, 2nd ed., Nauka, Moscow, 1970, (in Russian). Translations of Math. Monographs, vol. 79, American Mathematical Society, 1990.

[55] J. W. S. Cassels, *An introduction to the geometry of numbers*, Grundlehren der mathematischen Wissenschaften, vol. 99, Springer-Verlag, 1959.

[56] ———, *Diophantine equations with special references to elliptic curves*, J. of the London Math. Soc. **41** (1966), 193–291.

[59] 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.

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

[68] D. Coppersmith, *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.

[69] ———, *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.

[70] ———, *Small solutions to polynomials equations, and low exponent RSA vulnerabilities*, Journal of Cryptology **10** (1997), no. 4, 233–260.

[96] L. E. Dickson, *The analytic representation of substitutions on a power of a prime number of letters with a discussion of the linear group*, Annals of Mathematics **11** (1896/97), 65–120,161–183.

[137] G. H. Hardy and E. M. Wright, *An introduction to the theory of numbers*, 5th ed., Oxford University Press, 1979.

[145] D. Husemöller, *Elliptic curves*, Graduate Texts in Mathematics, vol. 111, Springer-Verlag, 1987.

[147] K. Ireland and M. Rosen, *A classical introduction to modern number theory*, Graduate Texts in Mathematics, vol. 84, Springer-Verlag, 1982.

[150] A. Joux and J. Stern, *Lattice reduction: a toolbox for the cryptanalyst*, Submitted to Journal of Cryptology.

[152] M. Joye, *Introduction à la théorie des courbes elliptiques*, Mémoire de DEA en mathématiques, Université catholique de Louvain, June 1995.

[159] M. Joye and J.-J. Quisquater, *Efficient computation of full Lucas sequences*, Electronics Letters **32** (1996), no. 6, 537–538.

[174] A. Knapp, *Elliptic curves*, Mathematical Notes, vol. 40, Princeton University Press, 1992.

[175] D. E. Knuth, *The art of computer programming: Volume 2/seminumerical algorithms*, 2nd ed., Addison-Wesley, 1981.

[177] N. Koblitz, *Elliptic curve cryptosystems*, Math. of Comp. **48** (1987), no. 177, 203–209.

[182] ———, *A course in number theory and cryptography*, 2nd ed., Graduate Texts in Mathematics, vol. 114, Springer-Verlag, 1994.

[201] S. Lang, *Elliptic curves: Diophantine analysis*, Grundlehren der mathematischen Wissenschaften, vol. 231, Springer-Verlag, 1978.

[206] A. K. Lenstra, H. W. Lenstra Jr, and L. Lovász, *Factoring polynomials with integer coefficients*, Mathematische Annalen **261** (1982), 513–534.

[209] H. W. Lenstra Jr, *Factoring integers with elliptic curves*, Annals of Mathematics **126** (1987), 649–673.

[214] R. Lidl, G. L. Mullen, and G. Turnwald, *Dickson polynomials*, Longman Scientific & Technical, 1993.

[216] R. Lidl and H. Niederreiter, *Finite fields*, Encyclopedia of Mathematics and its Applications, vol. 20, Addison-Wesley, 1983.

[221] A. Magnus, Personal communication.

[231] A. J. Menezes, *Elliptic curve public key cryptosystems*, Kluwer Academic Publishers, 1993.

[240] 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.

[249] F. Morain and J. Olivos, *Speeding up the computations on an elliptic curve using addition-substraction chains*, Theoretical Informatics and Applications, vol. 24, 1990, pp. 531–543.

[260] I. M. Niven and H. S. Zuckerman, *An introduction to the theory of numbers*, 4th ed., John Wiley & Sons, 1980.

[286] P. Ribenboim, *The little book of big primes*, Springer-Verlag, 1991.

[287] H. Riesel, *Prime numbers and computer methods for factorization*, 2nd ed., Progress in Mathematics, vol. 126, Birkhaüser, 1994.

[295] K. H. Rosen, *Elementary number theory and its applications*, 3rd ed., Addison-Wesley, 1992.

[305] C. P. Schnorr and M. Euchner, *Lattice basis reduction: Improved practical algorithms and solving subset sum problems*, Proc. of Fundamentals of Computation Theory (FCT '91) (L. Budach, ed.), Lecture Notes in Computer Science, vol. 529, Springer-Verlag, 1991, pp. 68–85.

[316] J. H. Silverman, *The arithmetic of elliptic curves*, Graduate Texts in Mathematics, vol. 106, Springer-Verlag, 1986.

[317] J. H. Silverman and J. Tate, *Rational points on elliptic curves*, Undergraduate Texts in Mathematics, Springer-Verlag, 1992.

[330] 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.

[331] P. J. 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 and R. Safavi-Naini, eds.), Lecture Notes in Computer Science, vol. 917, Springer-Verlag, 1995, pp. 357–364.

CHAPTER 2

RSA-type Cryptosystems

In 1978, Rivest, Shamir and Adleman [**292**] introduced the so-called RSA cryptosystem. Its security mainly relies on the intractability of factoring large numbers, or more precisely on the RSA hypothesis.

DEFINITION 2.1. Given a positive integer n that is the product of two odd primes p and q, a positive integer e relatively prime to $(p-1)(q-1)$ and an integer c, the *RSA problem* is: "Find an integer m such that $m^e \equiv c \pmod{n}$".

CONJECTURE 2.2 (RSA hypothesis). *The RSA problem and the integer factorization problem are computationally equivalent.*

In Section 1, we will show that if the factors of n are known, then solving the RSA problem is obvious. However, it has never been proved (although widely believed) that the knowledge of the factors of n is the only way to solve the RSA problem.

Later, other structures were envisaged to implement analogues of RSA. So, in 1981, a cryptosystem based on Dickson polynomials was proposed by Müller and Nöbauer [**251**] and analyzed in [**252**]. This system re-emerged later in terms of Lucas sequences to produce LUC [**328, 330**].

In 1985, Koblitz [**177**] and Miller [**240**] independently suggested the use of elliptic curves in cryptography. Afterwards, Koyama, Maurer, Okamoto and Vanstone [**187**] and later Demytko [**89**] exhibited new one-way trapdoor functions on elliptic curves over the ring $\mathbb{Z}_n$ (see also [**169**]). The resulting cryptosystems are respectively called KMOV (from the last names of their inventors) and Demytko's system.

1. RSA

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 $(p-1)$ and $(q-1)$. Finally, he computes the secret decryption key d according to

$$ed \equiv 1 \pmod{\operatorname{lcm}(p-1, q-1)}. \tag{2.1}$$

To send a message $m \in \mathbb{Z}_n$ to Bob, Alice looks to Bob's public key e and forms the ciphertext $c = m^e \bmod n$. Next, to recover the plaintext m, Bob uses his secret decryption key d to obtain

$$m = c^d \bmod n. \tag{2.2}$$

PROOF. Since $ed \equiv 1 \pmod{\operatorname{lcm}(p-1, q-1)}$, $ed \equiv 1 \pmod{(p-1)}$ and $ed \equiv 1 \pmod{(q-1)}$. By Theorem 1.2, if $p \nmid m$, then $c^d \equiv m^{ed} \equiv m \pmod{p}$. Otherwise, without loss of generality, we may assume $\gcd(m, p) = p$. Then $c \equiv 0 \pmod{p}$ and we still have $c^d \equiv m \pmod{p}$. Similarly, $c^d \equiv m \pmod{q}$. Hence, by Theorem 1.12, $c^d \equiv m \pmod{n}$. □

This encryption scheme can be converted into a signature scheme. If Bob wants to sign a message m, he uses his secret key d to compute the signature $s = m^d \bmod n$. Next, he sends m and s to Alice. Then Alice can verify that s is the Bob's signature of message m by checking whether $s^e \equiv m \pmod{n}$ where e is the public key of Bob.

2. LUC

To setup the system, each user proceeds in a similar way as for RSA. The public parameters are the RSA-modulus $n = pq$ that is the product of two large primes, and the encryption key e that is relatively prime to $(p-1)$, $(p+1)$, $(q-1)$ and $(q+1)$. The secret decryption key d is computed according to

$$ed \equiv 1 \pmod{\Psi(n)}, \tag{2.3}$$

where $\Psi(n) = \operatorname{lcm}(p - (\Delta/p), q - (\Delta/q))$.

To send a message m to Bob, Alice uses Bob's public key e to compute the ciphertext $c = V_e(m, 1) \bmod n$. Then, Bob recovers the plaintext m with his secret key d by computing

$$m = V_d(c, 1) \bmod n. \tag{2.4}$$

PROOF. From Eq. (1.23) and Corollary 1.40, it follows

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

□

Apparently, the drawback in this method is that d depends on 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 Eq. (2.3). However, the decryption key corresponding to a given message can be determined *a priori* since

$$\begin{aligned}\Psi(n) &= \operatorname{lcm}\bigl(p-(\Delta/p), q-(\Delta/q)\bigr)\\ &= \operatorname{lcm}\left(p-(\Delta U_e^2(m,1)/p), q-(\Delta U_e^2(m,1)/q)\right)\\ &= \operatorname{lcm}\left(p-\left(\frac{c^2-4}{p}\right), q-\left(\frac{c^2-4}{q}\right)\right) \quad \text{by Eq. (1.21).}\end{aligned}$$

REMARK 2.3. It is also possible to construct a message-independent cryptosystem, taking d such that $ed \equiv 1 \pmod{\operatorname{lcm}(p-1, p+1, q-1, q+1)}$. 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 curve systems

Proposition 1.57 seems to establish a RSA-type system. However, some problems occur. Suppose that Alice wants to send a message m to Bob. Bob fixes an elliptic curve $E_n(a,b)$ over $\mathbb{Z}_n$ and computes $N_n = \operatorname{lcm}(\#E_p(a,b), \#E_q(a,b))$. 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 $E_n(a,b)$. 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 algorithms known for imbedding a message as a point of a given elliptic curve $E_n(a,b)$ require the knowledge of the factors p and q. For example, Koblitz proposes the following probabilistic method [**182**, pp. 179–180]. Given a security parameter κ, a message $m < \lfloor n/\kappa \rfloor$ is represented by $x_j = m\kappa + j$, where $1 \le j \le \kappa$ is chosen so that we can find some y_j satisfying $y_j^2 = x_j^3 + ax_j + b$. In this case, we take $\mathbf{M} = (x_j, y_j) \in E_n(a,b)$. From $\mathbf{M}$, message m is recovered as $m = \lfloor (x_j - 1)/\kappa \rfloor$. However, the evaluation of y_j cannot be achieved without knowing p and q. Therefore, this method can only be used to a construct signature schemes. To construct encryption schemes, other solutions were proposed.

3.1. KMOV.

3.1.1. *Basic scheme.* KMOV system relies on Lemma 1.51. 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 $N_n = \operatorname{lcm}(p+1, q+1)$ and computes the secret key d so that

$$ed \equiv 1 \pmod{N_n}. \tag{2.5}$$

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

$$b = m_2^2 - m_1^3 \bmod n. \tag{2.6}$$

Next, using Bob's public key e, she encrypts $\mathbf{M} \in E_n(0, b)$ as

$$\mathbf{C} = [e]\mathbf{M} = (c_1, c_2), \tag{2.7}$$

and sends it to Bob. From $\mathbf{C}$, Bob computes the parameter b as $b = c_2^2 - c_1^3 \bmod n$. Then, he recovers the original message with his secret key d by computing

$$\mathbf{M} = [d]\mathbf{C} \tag{2.8}$$

on the curve $E_n(0, b)$.

PROOF. Obvious by Proposition 1.57. □

Note that, from the addition formulae on elliptic curves (see Eqs (1.34) and (1.35)), the knowledge of parameter b is not really required in the decryption process.

REMARK 2.4. The minimum value of e is 5 because $6 \mid N_n$.

REMARK 2.5. As mentioned in [**187**], from Lemma 1.52, it is also possible to work on a curve of the form $E_n(a, 0)$ by choosing a as

$$a = \frac{m_2^2 - m_1^3}{m_1} \bmod n. \tag{2.9}$$

In this case, the minimum value of e is 3 because $4 \mid N_n$.

3.1.2. *Kuwakado/Koyama's extension.* KMOV system was extended to form-free primes by Kuwakado and Koyama [**191**]. Their extension is based on Lemmas 1.53 and 1.54.

Let the elliptic curve

$$E_n(0, b) : y^2 \equiv x^3 + b \pmod{n}. \tag{2.10}$$

To setup the system, each user chooses two large primes p and q and publishes $n = pq$. Suppose $p \equiv 1 \pmod 3$. By Lemma 1.53, $\#E_p(0, b) = p + 1 + \overline{(4b/\pi_p)_6}\pi_p + (4b/\pi_p)_6\overline{\pi_p}$ where $\pi_p = r + s\omega$ is a prime in $\mathbb{Z}[\omega]$

such that $\pi_p\overline{\pi_p} = p$ and $\pi_p \equiv 2 \pmod 3$. So, depending on the values of the sixtic symbols, we have

$$\#E_p(0,b) = \begin{cases} N_{p,1} = p+1+2r-s & \text{if } (4b/\pi_p)_6 = 1, \\ N_{p,2} = p+1-2r+s & \text{if } (4b/\pi_p)_6 = -1, \\ N_{p,3} = p+1-r+2s & \text{if } (4b/\pi_p)_6 = \omega, \\ N_{p,4} = p+1+r-2s & \text{if } (4b/\pi_p)_6 = -\omega, \\ N_{p,5} = p+1-r-s & \text{if } (4b/\pi_p)_6 = \omega^2, \\ N_{p,6} = p+1+r+s & \text{if } (4b/\pi_p)_6 = -\omega^2. \end{cases}$$

If $q \equiv 1 \bmod 3$, then the user similarly computes $\#E_q(0,b) = N_{q,i}$ $(1 \le i \le 6)$. Next, he computes $N_{n,i,j} = \operatorname{lcm}(N_{p,i}, N_{q,j})$ for $1 \le i,j \le 6$ and chooses a public encryption key e such that $\gcd(e, N_{n,i,j}) = 1$ for $1 \le i,j \le 6$. The decryption keys $d_{i,j}$ are computed so that

$$ed_{i,j} \equiv 1 \pmod{N_{n,i,j}} \quad (i,j = 1,\dots,6). \tag{2.11}$$

If $q \equiv 2 \pmod 3$, then $\#E_q(0,b) = q+1$. So, the user computes $N_{n,i} = \operatorname{lcm}(N_{p,i}, q+1)$ for $1 \le i \le 6$ and chooses e relatively prime to $N_{n,i}$ for $1 \le i \le 6$. In this case, the decryption keys d_i are computed according to

$$ed_i \equiv 1 \pmod{N_{n,i}} \quad (i = 1,\dots,6). \tag{2.12}$$

For both cases, the encryption process is the same as for KMOV. To decrypt a ciphertext, Bob has to use the corresponding decryption key $d_{i,j}$ according to the values of $(4b/\pi_p)_6$ and of $(4b/\pi_q)_6$ if $q \equiv 1 \pmod 3$. If $q \equiv 2 \pmod 3$, then Bob chooses the decryption key d_i according to the value of $(4b/\pi_p)_6$.

REMARK 2.6. A similar system can be constructed from Lemma 1.54 instead of Lemma 1.53.

Another cryptosystem based on elliptic curves was later proposed by Demytko.

3.2. Demytko's system. Each user chooses two large primes p and q and makes $n = pq$ public. He also chooses once for all the parameters a, b. Next, he computes

$$\begin{aligned} N_{n,1} &= \operatorname{lcm}(p+1-a_p, q+1-a_q), \\ N_{n,2} &= \operatorname{lcm}(p+1-a_p, q+1+a_q), \\ N_{n,3} &= \operatorname{lcm}(p+1+a_p, q+1-a_q), \\ N_{n,4} &= \operatorname{lcm}(p+1+a_p, q+1+a_q), \end{aligned}$$

where $a_p = p + 1 - \#E_p(a,b)$ and $a_q = q + 1 - \#E_q(a,b)$. He chooses a public encryption key e that is relatively prime to $N_{n,i}$ $(1 \le i \le 4)$ and computes the secret decryption keys d_i so that

$$ed_i \equiv 1 \pmod{N_{n,i}} \quad (i = 1, \dots, 4). \tag{2.13}$$

Let m be the message being encoded. 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 (see Corollary 1.60 and the resulting algorithm described in [**48**, p. 214], for example), $[k]_x\, p_1$ will denote the x-coordinate of k times the point $\mathbf{P} = (p_1, p_2)$, *i.e.* $[k]_x\, p_1 = \mathcal{G}_k(p_1) = \mathrm{x}([k]\mathbf{P})$. To encrypt m, Alice computes

$$c = [e]_x\, m. \tag{2.14}$$

To decrypt the ciphertext c, Bob computes

$$[d_i]_x\, c = [d_i e]_x\, m = m, \tag{2.15}$$

where the decryption key is

$$\begin{cases} d_1 & \text{if } (w/p) = 1 \text{ and } (w/q) = 1, \\ d_2 & \text{if } (w/p) = 1 \text{ and } (w/q) \neq 1, \\ d_3 & \text{if } (w/p) \neq 1 \text{ and } (w/q) = 1, \\ d_4 & \text{if } (w/p) \neq 1 \text{ and } (w/q) \neq 1, \end{cases}$$

with $w = c^3 + ac + b \bmod n$.

PROOF. Suppose, for example, $(w/p) = 1$ and $(w/q) = -1$. Then $(c, \cdot) \in E_p(a,b)$ and $(c, \cdot) \in \overline{E_q(a,b)}$. So, $[d_2]_x\, c = [ed_2]_x\, m = m$ by Proposition 1.57, which concludes the proof. □

REMARK 2.7. It is also possible to construct a message-independent cryptosystem by choosing d according to

$$ed \equiv 1 \pmod{\operatorname{lcm}(N_{n,1}, N_{n,2}, N_{n,3}, N_{n,4})}.$$

REMARK 2.8. In all RSA-type systems, the decryption process can be speeded up by using the Chinese Remainder Theorem (Theorem 1.12). This was first pointed out by Quisquater and Couvreur [**283**].

References

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

[89] 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.

[169] B. S. Kaliski Jr, *One-way permutations on elliptic curves*, Journal of Cryptology **3** (1991), no. 3, 187–199.

[177] N. Koblitz, *Elliptic curve cryptosystems*, Math. of Comp. **48** (1987), no. 177, 203–209.

[182] ———, *A course in number theory and cryptography*, 2nd ed., Graduate Texts in Mathematics, vol. 114, Springer-Verlag, 1994.

[187] 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, 1992, pp. 252–266.

[191] H. Kuwakado and K. Koyama, *Efficient cryptosystems over elliptic curves based on a product of form-free primes*, IEICE Trans. Fundamentals **E77-A** (1994), no. 8, 1309–1318.

[240] 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.

[251] W. B. Müller and R. Nöbauer, *Some remarks on public-key cryptosystems*, Sci. Math. Hungar **16** (1981), 71–76.

[252] ———, *Cryptanalysis of the Dickson scheme*, Advances in Cryptology – Eurocrypt '85 (F. Pichler, ed.), Lecture Notes in Computer Science, vol. 219, Springer-Verlag, 1986, pp. 50–61.

[283] J.-J. Quisquater and C. Couvreur, *Fast decipherment algorithm for RSA public-key cryptosystem*, Electronics Letters **18** (1982), no. 21, 905–907.

[292] 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.

[328] P. Smith, *LUC public-key encryption*, Dr. Dobb's Journal (1993), no. 1, 44–49.

[330] 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.

CHAPTER 3

Security Analysis

Due to its popularity, the original RSA was subject to an extensive cryptanalysis. The attacks 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;
2. attacks based on its homomorphic nature;
3. attacks resulting from a bad choice of parameters.

Most of these attacks can more or less successfully be extended to their Lucas-based and elliptic curve analogues.

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 on LUC. Using division polynomials, the same conclusion holds for elliptic curve cryptosystems.

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

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 attacks.

1. Polynomial attacks

1.1. Håstad's attack.

1.1.1. *Basic attack.* Extending a simple attack of Blum and Davida, Håstad showed that sending linearly related messages over a large network using RSA with low public exponent is insecure [**139, 140**]. To mount his attack, Håstad developed a technique to solve a system of univariate modular equations. This technique was later generalized to the multivariate case by Takagi and Naito [**340**] and improved in [**155**].

On the other hand, Coppersmith [**70**] recently proposed a new method for finding a (small) root of a modular equation, which turned out to be a better way to mount a successful attack [**314, 34**].

We will first review the original attack of Håstad and then we will discuss the Coppersmith based variation.

THEOREM 3.1. *Consider a system of k modular polynomial equations of degree $\leq \delta$ with l variables given by*

$$\sum_{j_1,j_2,\dots,j_l=0}^{j_1+j_2+\cdots+j_l\leq\delta} a_{i,j_1,j_2,\dots,j_l}\, x_1^{j_1} x_2^{j_2}\dots x_l^{j_l} \equiv 0 \pmod{n_i} \tag{3.1}$$

for $i = 1,\dots,k$, and where $x_1,\dots,x_l < n$ and $n = \min_{1\leq i\leq k} n_i$.

Let

$$N = \prod_{i=1}^{k} n_i, \quad f = \sum_{m=1}^{\delta} m\binom{m+l-1}{m} \quad \text{and} \quad g = \sum_{m=0}^{\delta}\binom{l+m-1}{m}. \tag{3.2}$$

If the moduli n_i are coprime, if $\gcd(\langle a_{i,j_1,j_2,\dots,j_l}\rangle_{j_1,j_2,\dots,j_l=0}^{j_1+j_2+\cdots+j_l\leq\delta}, n_i) = 1$ for $i = 1,\dots,k$ and if $N > 2^{\frac{g(g+1)}{4}} g^g n^f$, then we can get in polynomial time a real-valued equation which is equivalent to Eq. (3.1).

PROOF. Consider a lattice L whose basis is given by

$$\begin{array}{ll}
\vec{b_1} &= (\mu_{0,\dots,0}, n\mu_{0,\dots,0,1}, n\mu_{0,\dots,0,1,0}, \dots, n^{j_1+\cdots+j_l}\mu_{j_1,\dots,j_l}, \dots, n^{\delta}\mu_{\delta,0,\dots,0}, \tfrac{1}{g}),\\
\vec{b_2} &= (N, 0, 0, \dots, 0, \dots, 0, 0),\\
\vec{b_3} &= (0, nN, 0, \dots, 0, \dots, 0, 0),\\
\vec{b_4} &= (0, 0, nN, \dots, 0, \dots, 0, 0),\\
&\vdots\\
\vec{b_{i+1}} &= (0, 0, 0, \dots, n^{j_1+\cdots+j_l}N, \dots, 0, 0),\\
&\vdots\\
\vec{b_{g+1}} &= (0, 0, 0, \dots, 0, \dots, n^{\delta}N, 0).
\end{array}$$

A vector of this lattice is of the form $\vec{V} = S\vec{b_1} + \sum_{i=1}^{g} s_i\vec{b_{i+1}}$. Its i^{th} coordinate (apart from the last one) is given by

$$V_i = n^{j_1+\cdots+j_l}(S\mu_{j_1,\dots,j_l} + s_iN).$$

Suppose that we can find a vector $\vec{V}(\neq \vec{0}) \in L$ such $\|\vec{V}\| < N/g$, then $|V_i| < N/g$. So,

$$(*)\qquad \begin{aligned} \left|\frac{V_i}{n^{j_1+\cdots+j_l}}\right| &= \left|\frac{V_i}{n^{j_1+\cdots+j_l}} \bmod_{\pm} N\right| = |S\mu_{j_1,\dots,j_l} \bmod_{\pm} N| \\ &< \frac{N}{g\, n^{j_1+\cdots+j_l}}, \end{aligned}$$

for all $j_1, \dots, j_l$.

Let $u_j \equiv \delta_{ij} \pmod{n_i}$ where δ_{ij} is Kronecker's delta. Using Theorem 1.12, we get

$$\begin{aligned} 0 &\equiv \sum_{j_1,j_2,\dots,j_l=0}^{j_1+j_2+\cdots+j_l\leq\delta} \underbrace{\left(\sum_{i=1}^{k} a_{i,j_1,j_2,\dots,j_l} u_i\right)}_{:=\mu_{j_1,j_2,\dots,j_l}} x_1^{j_1} x_2^{j_2} \dots x_l^{j_l} \\ (**)\qquad &\equiv \sum_{j_1,j_2,\dots,j_l=0}^{j_1+j_2+\cdots+j_l\leq\delta} S\mu_{j_1,j_2,\dots,j_l}\, x_1^{j_1} x_2^{j_2} \dots x_l^{j_l} \pmod{N}, \end{aligned}$$

From Eq. (*), for any $x_1, x_2, \dots, x_l < n$, we have

$$\begin{aligned} &\left|\sum_{j_1,j_2,\dots,j_l=0}^{j_1+j_2+\cdots+j_l\leq\delta} (S\mu_{j_1,j_2,\dots,j_l} \bmod_{\pm} N)\, x_1^{j_1} x_2^{j_2} \dots x_l^{j_l}\right| \\ &\qquad < \sum_{j_1,j_2,\dots,j_l=0}^{j_1+j_2+\cdots+j_l\leq\delta} |S\mu_{j_1,j_2,\dots,j_l} \bmod_{\pm} N|\, n^{j_1+j_2+\cdots+j_l} \\ &\qquad < \sum_{j_1,j_2,\dots,j_l=0}^{j_1+j_2+\cdots+j_l\leq\delta} \frac{N}{g} = N. \end{aligned}$$

We can thus consider Eq. (**) as a real-valued equation. If nontrivial (*i.e.* there is at least one nonzero coefficient), this equation is equivalent to Eq. (3.1). Note that the last coefficient of $\vec{V}$ is equal to S/g, and therefore $|S| < N$ since $\|\vec{V}\| < N/g$. Note also that $S \neq 0$ because all nonzero vectors $\vec{V}$ with $S = 0$ are of length at least N. So, $0 < |S| < N$ whence $S \not\equiv 0 \pmod{N}$, and thus $S \not\equiv 0 \pmod{n_i}$ for some n_i. Furthermore, since $\mu_{j_1,j_2,\dots,j_l} \equiv a_{i,j_1,j_2,\dots,j_l} \pmod{n_i}$ and $\gcd(\langle a_{i,j_1,j_2,\dots,j_l}\rangle_{j_1,j_2,\dots,j_l=0}^{j_1+j_2+\cdots+j_l\leq\delta}, n_i) = 1$, there exists at least one $\mu_{j_1,j_2,\dots,j_l} \not\equiv 0 \pmod{n_i}$. Consequently, Eq. (**) is nontrivial.

It remains to prove how to find a vector $\vec{V}$ such that $\|\vec{V}\| < N/g$. From Theorem 1.71, the LLL algorithm can find a vector $\vec{V}$ such that

$$\|\vec{V}\| \leq 2^{g/4}\Delta(L)^{1/(g+1)}$$

within polynomial time. Therefore, this algorithm will provide the required vector $\vec{V}$ if $2^{g/4}\left(N^g n^f/g\right)^{1/(g+1)} < N/g \iff 2^{g(g+1)/4}g^g n^f < N$. $\square$

COROLLARY 3.2 (Håstad's Theorem). *Let $N = \prod_{i=1}^{k} n_i$ and let $n = \min n_i$. Given a set of k equations $\sum_{j=0}^{\delta} a_{i,j}x^j \equiv 0 \pmod{n_i}$ where the moduli n_i are pairwise relatively prime and $\gcd(\langle a_{i,j}\rangle_{j=0}^{\delta}, n_i) = 1$ for all i. Then it is possible to find $x < n$ in polynomial time if $N > 2^{(\delta+1)(\delta+2)/4}(\delta+1)^{\delta+1}n^{\delta(\delta+1)/2}$.*

PROOF. In the univariate case, we have $f = \sum_{m=1}^{\delta} m\binom{m}{m} = \delta(\delta+1)/2$ and $g = \sum_{m=0}^{\delta}\binom{m}{m} = \delta+1$. $\square$

If the public encryption exponents are small, the encryption process is fast. However, such a choice can be dangerous. We will illustrate the failure with a exponent $e = 3$. Suppose that the same message m has to be sent to three different users. The corresponding ciphertexts are $c_1 = m^3 \bmod n_1$, $c_2 = m^3 \bmod n_2$ and $c_3 = m^3 \bmod n_3$. If n_1, n_2 and n_3 are not relatively prime, then we find the secret factors of some n_i and thus recover the message m. Otherwise, by Theorem 1.12,

$$m^3 \equiv c_1u_1 + c_2u_2 + c_3u_3 \pmod{n_1n_2n_3},$$

where $u_j \equiv \delta_{ij} \pmod{n_i}$. But, since $m^3 < n_1n_2n_3$, it can be recovered.

To foil this attack, we can use larger exponents or send not exactly the same message by adding a time-stamp, for example. This latter solution does not always prevent the recovery of messages. Suppose that the messages are linearly related

$$m_i = \alpha_i m + \beta_i \bmod n_i \quad (1 \leq i \leq k),$$

where α_i and β_i are known constants. The corresponding ciphertexts are $c_i = m_i^{e_i} \bmod n_i$. In this case, we have:

COROLLARY 3.3. *In the RSA cryptosystem, a set of k linearly related messages encrypted with public encryption keys e_i and RSA-moduli n_i can be recovered if*

$$k > e(e+1)/2 \quad \textit{and} \quad n_i > 2^{(e+1)(e+2)/4}(e+1)^{e+1}, \tag{3.3}$$

where $e = \max e_i$.

PROOF. We have just to verify that the conditions of Corollary 3.2 are fulfilled. From the k ciphertexts, we have k equations $\mathcal{P}_i(m) = (\alpha_i m + \beta_i)^{e_i} - c_i \equiv 0 \pmod{n_i}$. We can suppose that the moduli n_i are pairwise coprime and also that the coefficients of polynomial $\mathcal{P}_i$ are relatively prime to n_i; otherwise we recover the message by factoring n_i. Since $k > e(e+1)/2$ and $n_i > 2^{(e+1)(e+2)/4}(e+1)^{e+1}$, it follows

$$N = \prod_{i=1}^{k} n_i \geq n_1 \prod_{i=2}^{e(e+1)/2+1} n_i > 2^{(e+1)(e+2)/4}(e+1)^{e+1} n^{e(e+1)/2},$$

where $n = \min n_i$. □

Describing Lucas sequences in terms of quadratic rings [**254**], Pinch showed the previous corollary remains valid for the LUC cryptosystem [**276**]. This can also be proved thanks to the Dickson polynomials. Indeed, from Proposition 1.42, we can consider $c_i = V_{e_i}(\alpha_i m + \beta_i, 1) \bmod n_i$ as polynomials in m of degree e_i.

Kuwakado and Koyama [**192**] obtained a similar result for elliptic curve cryptosystems by using division polynomials (see also [**190**]).

COROLLARY 3.4. *In the KMOV or Demytko's cryptosystems, a set of k linearly related messages encrypted with public encryption keys e_i and RSA-moduli n_i can be recovered if*

$$k > e^2(e^2+1)/2 \quad \textit{and} \quad n_i > 2^{(e^2+1)(e^2+2)/4}(e^2+1)^{e^2+1}, \tag{3.4}$$

where $e = \max e_i$.

PROOF. We only focus on the x-coordinate. Let k plaintexts $m_i = \alpha_i m + \beta_i \bmod n_i$ and the corresponding ciphertexts $c_i = [e_i]_x\, m_i$. From Proposition 1.59, we obtain k modular equations of degree at most e^2

$$c_i \Psi_{e_i}(\alpha_i m + \beta_i)^2 - \Phi_{e_i}(\alpha_i m + \beta_i) \equiv 0 \pmod{n_i} \quad (1 \leq i \leq k).$$

By Corollary 3.2, this set of equations can be solved if $k > e^2(e^2+1)/2$ and $n_i > 2^{(e^2+1)(e^2+2)/4}(e^2+1)^{e^2+1}$. □

1.1.2. *Coppersmith based variation.* The previous approach is not optimal [**314, 34**]. The amount of messages can significantly be reduced if we use a powerful technique due to Coppersmith.

THEOREM 3.5 (Coppersmith's Theorem). *Let a monic integer polynomial $\mathcal{P}(x)$ of degree δ and a positive integer N of unknown factorization. In time polynomial in $\log N$ and δ, we can find all integer solutions x_0 to $\mathcal{P}(x_0) \equiv 0 \pmod{N}$ with $|x_0| < N^{1/\delta}$.*

PROOF. See [**69**, p. 159], Corollary 2. □

COROLLARY 3.6. *Let a positive integer e. Sending more than e linearly related messages that are encrypted via RSA or LUC with public exponents $e_i \leq e$ and RSA-moduli n_i is dangerous.*

PROOF. Let $m_i = \alpha_i m + \beta_i \bmod n_i$ $(1 \leq i \leq k)$ be k linearly related plaintexts and let $N = \prod_{i=1}^{k} n_i$. We can assume that the RSA-moduli n_i are pairwise coprime; otherwise the messages are recovered by factoring n_i. Let $e = \max e_i$. From the ciphertexts c_i, we can derive k monic polynomial equations of degree e given by

$$\begin{aligned}\mathcal{P}_i(m) &\equiv (\alpha_i m + \beta_i)^{e_i} - c_i \equiv (m + \alpha_i^{-1}\beta_i)^{e_i} - \alpha_i^{-e_i} c_i \\ &\equiv m^{e-e_i}[(m + \alpha_i^{-1}\beta_i)^{e_i} - \alpha_i^{-e_i} c_i] \equiv 0 \pmod{n_i},\end{aligned}$$

if the RSA cryptosystem is used. Combining these equations by Chinese remaindering (Theorem 1.12), we get a monic polynomial (modulo N) in m of degree e. By Theorem 3.5, we can recover m since $m < \min n_i \leq N^{1/k} \leq N^{1/e}$ if $k \geq e$.

If the LUC cryptosystem is used, we express the ciphertexts in terms of Dickson polynomials and compute $\mathcal{P}_i(m) \equiv m^{e-e_i}\alpha_i^{-e_i}[D_{e_i}(\alpha_i m + \beta_i, 1) - c_i] \equiv 0 \pmod{n_i}$ which are monic polynomial equations of degree e. We combine them by Chinese remaindering. The resulting polynomial can then be solved thanks to Theorem 3.5 if $k \geq e$. □

COROLLARY 3.7. *Let a positive integer e. Sending more than e^2 linearly related messages that are encrypted via Demytko's cryptosystem with public exponents $e_i \leq e$ and RSA-moduli n_i is dangerous.*

PROOF. As before, from the ciphertexts $c_i = [e_i]_x(\alpha_i m + \beta_i)$, we compute

$$\mathcal{P}_i(m) \equiv m^{e^2-e_i^2}\alpha_i^{-e_i^2}[\Phi_{e_i}(\alpha_i m + \beta_i) - c_i\Psi_{e_i}(\alpha_i m + \beta_i)^2] \equiv 0 \pmod{n_i},$$

which are monic and of degree e^2 by Proposition 1.59. We conclude the proof in a similar way as for Corollary 3.6. □

Bleichenbacher [**36**] also improves Håstad's attack against KMOV. Its improvement relies on another result of Coppersmith.

PROPOSITION 3.8. *Let $\mathcal{P}(x_1, \ldots, x_m) \pmod N$ be a polynomial of total degree δ. If there exists a solution $x_i = y_i$ with $|y_i| < N^{\alpha_i}$, then we can find this solution as long as $\sum_{i=1}^{m} \alpha_i < (1/\delta) - \varepsilon$ for some $\varepsilon > 0$.*

PROOF. See [**69**, p. 160], Section 3. □

Let k linearly related messages $\mathbf{M_i} = (\alpha_{1i}m_1 + \beta_{1i}, \alpha_{2i}m_2 + \beta_{2i})$. Since each message respectively belongs to the elliptic curve $E_{n_i}(0, b_i)$:

$y^2 = x^3 + b_i$, we have

$$(\alpha_{2i} m_2 + \beta_{2i})^2 \equiv (\alpha_{1i} m_1 + \beta_{1i})^3 + b_i \pmod{n_i},$$

for $i = 1, \ldots, k$. If we combine these k equations by Chinese remaindering, we obtain a bivariate modular polynomial

$$\begin{aligned}\mathcal{P}(m_1, m_2) \equiv \left(\textstyle\sum_{i=1}^k \alpha_{1i}^3 u_i\right) m_1^3 + 3\left(\textstyle\sum_{i=1}^k \alpha_{1i}^2 \beta_{1i} u_i\right) m_1^2 \\ + 3\left(\textstyle\sum_{i=1}^k \alpha_{1i} \beta_{1i}^2 u_i\right) m_1 - \left(\textstyle\sum_{i=1}^k \alpha_{2i}^2 u_i\right) m_2^2 - 2\left(\textstyle\sum_{i=1}^k \alpha_{2i} \beta_{2i}\right) m_2 \\ + \textstyle\sum_{i=1}^k (\beta_{1i}^3 + b_i - \beta_{2i}^2) u_i \equiv 0 \pmod{N},\end{aligned}$$

where $u_j \equiv \delta_{ij} \pmod{n_i}$ and $N = \prod_{i=1}^k n_i$. Let $n = \min n_i$. We know that m_1 and m_2 lie in the interval $[0, n)$. Therefore,

$$|m_1 \bmod_{\pm} n| \text{ and } |m_2 \bmod_{\pm} n| \le \lfloor n/2 \rfloor < \frac{N^{1/k}}{2} = N^{\frac{1}{k} - \frac{1}{\log_2 N}}.$$

By Proposition 3.8, we can solve the polynomial $\mathcal{P}(m_1, m_2)$ if

$$\frac{2}{k} - \frac{2}{\log_2 N} < \frac{1}{3} - \varepsilon.$$

This inequality can already be satisfied for $k = 6$. This means that sending more than 6 linearly related messages with KMOV cryptosystem is dangerous. Note that the amount of messages does not depend on the public encryption exponents.

1.1.3. *Summary.* The following tables summarizes the number of messages required to mount a successful Håstad's attack.

e	2	3	4	5	7	33
RSA	–	7	–	16	29	562
LUC	–	7	–	16	29	562
KMOV	–	–	–	326	*	*
Demytko	11	46	137	326	*	*

Table 3.1: Basic Håstad's attack

	# of messages
RSA	e
LUC	e
KMOV	6
Demytko	e^2

Table 3.2: Coppersmith based variation

Table 3.1 was constructed for 512-bit RSA-moduli n_i. The '$-$' means that the system is not defined for this value of e and the '$*$' means that the attack is not applicable. We can see that the attack fails for elliptic curve systems if public encryption keys e are greater than 7; while for RSA and LUC, if only 29 linearly related messages are sent then they can be recovered.

The Coppersmith based variation is more powerful, it works whatever the size of the RSA moduli n_i. In particular, only 6 linearly related KMOV-encrypted messages can be sufficient to mount a successful attack. We also see that Demytko's system is more resistant.

Bleichenbacher [**36**] implemented this attack against KMOV on an Ultra Sparc. He was able to recover the plaintexts from the ciphertexts of 9 linearly related messages in a few minutes, and from the ciphertexts of 8 linearly related messages in about 2 weeks. The theoretical lower bound of 6 messages seemed to be computationally unreachable.

1.2. GCD attack. At the rump session of Crypto '95, Franklin and Reiter identified a new attack against RSA with public exponent 3 [**108**]. Later, it was extended for exponents up to $\simeq$ 32 bits by Patarin [**273**] and generalized to other RSA-type cryptosystems [**164**]. If two messages differ only from a known fixed value Δ and are RSA-encrypted under the *same* RSA-modulus n, then it is possible to recover both of them. This situation occurs quite often, as for example,

- texts differing only from their date of compilation;
- letters sent to different addressees;
- retransmission of a message with a new ID number due to an error ...

1.2.1. *Review of the attack.* 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, form the polynomials $\mathcal{P}$ and $\mathcal{Q} \in \mathbb{Z}_n[x]$, defined by

$$\mathcal{P}(x) = x^e - c_1 \bmod n \quad \text{and} \quad \mathcal{Q}(x) = (x+\Delta)^e - c_2 \bmod n. \tag{3.5}$$

Since the message m_1 is a root of $\mathcal{P}$ and $\mathcal{Q}$, m_1 will be a root of

$$\mathcal{R} = \gcd(\mathcal{P}, \mathcal{Q}) \tag{3.6}$$

which is, with a high probability, a polynomial of degree 1. Solving polynomial $\mathcal{R}$ in x gives the value of m_1, and $m_2 = m_1 + \Delta$.

EXAMPLE 3.9. With exponent $e = 3$, the plaintext m_1 is given by

$$m_1 = \frac{\Delta(2c_1 + c_2 - \Delta^3)}{-c_1 + c_2 + 2\Delta^3} \bmod n,$$

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 [**71**]. Suppose that two messages satisfy a known polynomial relation of the form $m_1 \equiv P(m_2) \pmod{n}$. So, from the corresponding ciphertexts c_1 and c_2, we construct

$$\mathcal{P}(x) = x^e - c_1 \bmod n \quad \text{and} \quad \mathcal{Q}(x) = P(x)^e - c_2 \bmod n, \tag{3.7}$$

for which m_1 is a root. Therefore, we can obtain m_1 by computing $\mathcal{R} = \gcd(\mathcal{P}, \mathcal{Q})$.

Suppose now that m_1 and m_2 satisfy an implicit polynomial relation given by $P(m_1, m_2) \equiv 0 \pmod{n}$. In this case, from $P(x, y)$ and $\mathcal{Q}(y) = y^e - c_2$ considered as univariate polynomials in $\mathbb{Z}_n[y]$, we compute their resultant $\varrho \in \mathbb{Z}_n[x]$ (see [**42**], pp. 415-419)

$$\varrho(x) = \text{Resultant}_y(P(x, y), \mathcal{Q}(y)), \tag{3.8}$$

for which m_1 is a root. Then, from $\mathcal{P}(x) = x^e - c_1 \bmod n$, we compute $\mathcal{R} = \gcd(\mathcal{P}, \varrho)$ that will give the value of m_1.

If there are several polynomial related messages, the same technique enables to recover all of them. Let k messages m_i satisfying $P(m_1, \dots, m_k) \equiv 0 \pmod{n}$ and let $c_i = m_i^e \bmod n$ the corresponding ciphertexts. We construct the k polynomials $\mathcal{P}_i(x_i) = x_i^e - c_i \bmod n$ and we let $\varrho_0(x_1, \dots, x_k) = P(x_1, \dots, x_k) \bmod n$. Next, we iteratively compute

$$\varrho_i(x_1, \dots, x_{k-i}) = \text{Resultant}_{x_{k-i+1}}(\mathcal{P}_{k-i+1}, \varrho_{i-1})$$

until we obtain $\varrho_{k-1}(x_1)$ for which m_1 is a root. Consequently, we find m_1 by computing $\gcd(\mathcal{P}_1, \varrho_{k-1})$. To recover the other messages m_i ($i = 2, \dots, k$), we first construct

$$\mathcal{Q}_i(m_1, \dots, m_{i-1}, x_i) = \varrho_{k-i}(m_1, \dots, m_{i-1}, x_i),$$

and then we solve

$$\mathcal{R}_i = \gcd(\mathcal{P}_i, \mathcal{Q}_i). \tag{3.9}$$

1.2.2. *Extension to LUC.* Let m_1 and $m_2 = m_1 + \Delta$ be two plaintexts encrypted by LUC to produce the corresponding ciphertexts $c_1 = V_e(m_1, 1) \bmod n$ and $c_2 = V_e(m_2, 1) \bmod n$.

Unlike RSA, the polynomial relation between the plaintext and the ciphertext is not explicitly given. However, by Proposition 1.42, Lucas sequences can be rephrased in terms of Dickson polynomials:

$$\begin{aligned} c_1 &\equiv V_e(m_1, 1) \equiv D_e(m_1, 1) \\ &\equiv \sum_{i=0}^{\lfloor e/2 \rfloor} \frac{e}{e-i} \binom{e-i}{i} (-1)^i m_1^{e-2i} \pmod{n}. \end{aligned}$$

Consequently, the previous attack applies with $\mathcal{P}(x) = D_e(x, 1) - c_1 \bmod n$ and $\mathcal{Q}(x) = D_e(x + \Delta, 1) - c_2 \bmod n$ [**164**].

EXAMPLE 3.10. With a public encryption exponent $e = 3$, the plaintext m_1 can be recovered from c_1, c_2 and Δ by

$$m_1 = \frac{\Delta(2c_1 + c_2 - \Delta^3 + 3\Delta)}{-c_1 + c_2 + 2\Delta^3 - 6\Delta} \bmod n,$$

and $m_2 = m_1 + \Delta$.

1.2.3. *Extension to Demytko's system.* Demytko's system makes only use of the first coordinate of points of elliptic curves. Let m_1 and $m_2 = m_1 + \Delta$ be two plaintexts, and let $c_1 = [e]_x\, m_1$ and $c_2 = [e]_x\, m_2$ be the corresponding ciphertexts. We will exhibit the polynomial dependence thanks to Proposition 1.59 [**164**]:

$$c_1 \Psi_e(m_1)^2 \equiv \Phi_e(m_1) \pmod{n},$$

where Ψ and Φ are considered as univariate polynomials. So, we construct polynomials $\mathcal{P}$ and $\mathcal{Q} \in \mathbb{Z}_n[x]$ as

$$\begin{aligned} \mathcal{P}(x) &= c_1 \Psi_e(x)^2 - \Phi_e(x) \bmod n \quad \text{and} \\ \mathcal{Q}(x) &= c_2 \Psi_e(x + \Delta)^2 - \Phi_e(x + \Delta) \bmod n. \end{aligned} \tag{3.10}$$

Therefore, $\mathcal{R} = \gcd(\mathcal{P}, \mathcal{Q})$ will give the desired value of m_1 and $m_2 = m_1 + \Delta$.

1.2.4. *Extension to KMOV.* Let two plaintexts $\mathbf{M_1} = (m_{1,1}, m_{1,2})$ and $\mathbf{M_2} = (m_{2,1}, m_{2,2})$ related by

$$m_{2,1} = m_{1,1} + \Delta_1 \quad \text{and} \quad m_{2,2} = m_{1,2} + \Delta_2.$$

These messages are encrypted as $\mathbf{C_1} = [e]\mathbf{M_1} = (c_{1,1}, c_{1,2})$ and $\mathbf{C_2} = [e]\mathbf{M_2} = (c_{2,1}, c_{2,2})$ on the elliptic curves $E_n(0, b_1)$ and $E_n(0, b_2)$, respectively.

Bleichenbacher [**36**] showed that we can recover the messages independently of the size of the public encryption key e as follows. First, we construct polynomials $\mathcal{P}$ and $\mathcal{Q} \in \mathbb{Z}_n[x, y]$ as

$$\mathcal{P}(x, y) = x^3 - y^2 + b_1 \bmod n \quad \text{and} \qquad \mathcal{Q}(x, y) = (x + \Delta_1)^3 - (y + \Delta_2)^2 + b_2 \bmod n,$$

where b_i $(i = 1, 2)$ is derived from the ciphertexts, *i.e.* $b_i = c_{i,2}^2 - c_{i,1}^3 \bmod n$. Note that $\mathcal{P}(m_{1,1}, m_{1,2}) = \mathcal{Q}(m_{1,1}, m_{1,2}) = 0$. Next, we compute

$$\begin{aligned} \varrho(x) &= \mathrm{Resultant}_y(\mathcal{P}, \mathcal{Q}) \\ &= 9\Delta_1^2 x^4 + \left(18\Delta_1^3 - 4\Delta_2^2\right) x^3 \\ &\quad + \left(15\Delta_1^4 - 6\Delta_1(\Delta_2^2 + b_1 - b_2)\right) x^2 \\ &\quad + 6\Delta_1^2(\Delta_1^3 - \Delta_2^2 - b_1 + b_2)x \\ &\quad + \Delta_1^3\left(\Delta_1^3 - 2(\Delta_2^2 + b_1 - b_2)\right) \\ &\quad + (\Delta_2^2 - b_1 - b_2)^2 - 4b_1b_2, \end{aligned} \tag{3.11}$$

for which $m_{1,1}$ is a root. Finally, we compute

$$\mathcal{C}(x) = c_{1,1}\Psi_e(x)^2 - \Phi_e(x) \bmod (n, \varrho(x)) \tag{3.12}$$

over $\mathbb{Z}_n[x]/(\varrho(x))$. Since $c_{1,1} = [e]_x\, m_{1,1}$, $m_{1,1}$ is a root of $\mathcal{C}$. Consequently, $m_{1,1}$ can be recovered by computing $\mathcal{R} = \gcd(\varrho, \mathcal{C})$. The second part of $\mathbf{M_1}$, *i.e.* $m_{1,2}$, is recovered thanks to Corollary 1.60, $m_{1,2} = c_{1,2}/\mathcal{F}_e(m_{1,1}) \bmod n$. Then, $m_{2,1} = m_{1,1} + \Delta_1$ and $m_{2,2} = m_{1,2} + \Delta_2$.

1.2.5. *Analysis.* In [**273**], Patarin estimated that, for RSA, this attack applies with a public encryption exponent e up to typically 32 bits. From Proposition 1.42, the same conclusion holds for LUC. However, this is not true for Demytko's system, since the polynomial relation $\mathcal{P}(x)$ is of order e^2 instead of e. It means that for the same modulus n, a public exponent e of length ℓ for Demytko's system will be as secure as a public exponent e of length 2ℓ for RSA or LUC. Putting all this information together, we get the following table.

RSA	32 bits
LUC	32 bits
Demytko	16 bits
KMOV	∞

Table 3.3: Maximum size of the public exponent e

Furthermore, from Theorem 3.5, Coppersmith [**69**] showed that even if Δ (the difference between the two messages) is unknown, then m_1 and m_2 can sometimes be recovered. In particular, this means that adding a random padding to the messages being encrypted does not always prevent the recovery of messages.

Let $\vartheta(\Delta)$ be the resultant in x of polynomials $\mathcal{P}$ and $\mathcal{Q}$ (previously defined), which is an univariate polynomial in Δ. It is possible to solve this polynomial ϑ if the solution Δ is smaller than $n^{1/k}$, where n is the public modulus and k is the degree of ϑ. For RSA and LUC, we have $k = e^2$; for the elliptic curve systems, we have $k = e^4$. So, we obtain:

e	2		3		5		7	
	512	1024	512	1024	512	1024	512	1024
RSA	–	–	56	113	20	40	10	20
LUC	–	–	56	113	20	40	10	20
KMOV	–	–	–	–	*	1	*	*
Demytko	31	63	6	12	*	1	*	*

Table 3.4: Random padding Δ (in bits) tolerated for a 512/1024-bit modulus n

Note that, with a 512-bit modulus n, the attack only applies on RSA and LUC with a public exponent e equal to 3, because in this case the maximum size of the random padding Δ is of $\frac{512}{3^2} \approx 56$ bits. In the other cases, the tolerated random padding becomes too small and that would be better treated by exhaustion.

1.3. Garbage-man-in-the-middle attack. The basic idea of this attack relies on the possibility to get access to the “bin” of the recipient. In fact, if the cryptanalyst intercepts, transforms and re-sends a ciphertext, then the corresponding plaintext will be meaningless when the authorized receiver (say, Bob) will decrypt it. So, Bob will discard it. If the cryptanalyst can get access to this discard, he will be able to recover the original plaintext if the transformation is done in a clever way. Such an attack was already been mounted against RSA by Davida [**83**]. In many situations, we can get access to the discards, as for example,

- bad implementation of softwares or bad architectures;
- negligent secretaries;
- recovering of a previously deleted message, by a tool like the `<undelete>` command with MS-DOS ...

Another scenario is to ask the victim to sign the forged messages. The working hypothesis are thus not unrealistic.

1.3.1. *Davida's attack.* Suppose Alice wants to send a message m to Bob. Using Bob's public encryption key e, she computes $c = m^e \bmod n$, and sends it to Bob. Then, because only Bob knows the secret decryption key d, he can recover the message $m = c^d \bmod n$.

However, a cryptanalyst (Carol) can also recover the message as follows. She intercepts the ciphertext c, and replaces it by $c' = ck^e \bmod n$ where k is a random number. Then, when Bob will decrypt c', he will compute $m' = {c'}^d \bmod n$. Since the message m' is meaningless, he will discard it. Consequently, if Carol can get access to m', she recovers the original message m by computing

$$m'k^{-1} \equiv {c'}^d k^{-1} \equiv c^d \equiv m \pmod{n}. \tag{3.13}$$

This attack relies on the homomorphic nature of RSA. Thus, it can easily be extended to other systems which have the same property [**90**]. For example, KMOV is also susceptible to this attack. Let $\mathbf{M}$ the message being encrypted. Carol intercepts the corresponding ciphertext $\mathbf{C} = [e]\mathbf{M}$ and transforms it into $\mathbf{C}' = \mathbf{C} + [ek]\mathbf{C}$ where k is randomly chosen. Then, Bob deciphers $\mathbf{C}'$ and obtains $\mathbf{M}' = \mathbf{M} + [k]\mathbf{C}$. Therefore, Carol recovers $\mathbf{M} = \mathbf{M}' - [k]\mathbf{C}$.

1.3.2. *Generalization.* Non-homomorphic cryptosystems seem to be resistant to the Davida's attack. However, thanks to Theorem 1.1, a similar result can be found [**163**].

Let $E_e(\cdot)$, $D_d(\cdot)$ and $T_k(\cdot)$ be respectively the public encryption function, the corresponding secret decryption function and the cryptanalytic transformation function.

Now, imagine Alice wants to send a message m to Bob. She first computes the ciphertext $c = E_e(m)$, and sends it to Bob. Suppose that the cryptanalyst, Carol, intercepts the ciphertext c, and modifies it into $c' = T_k(c)$ according to Lagrange's Theorem. Next, Bob decrypts c', and

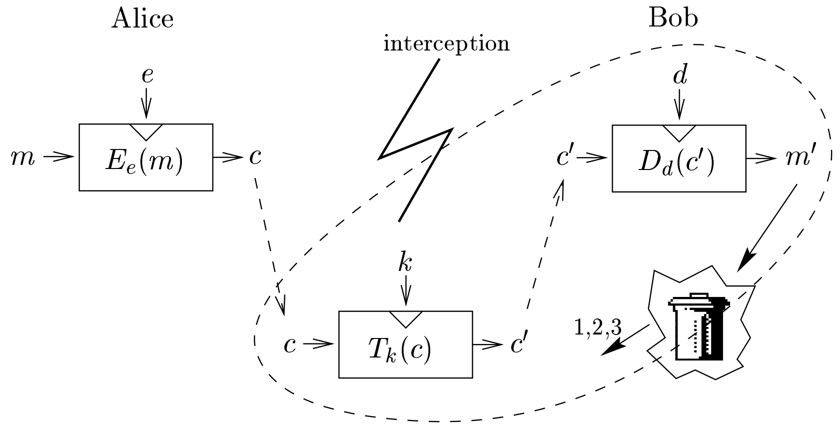

Figure 3.5: Garbage-man-in-the-middle attack

gets $m' = D_d(c')$. Since the message m' has no meaning, Bob discards it. Finally, if Carol can get access to m', then she recovers the message m from c, k, c' and m' from a non-trivial relation.

1.3.3. *Illustrations.*

1) Attacking LUC. For LUC cryptosystem, the enciphering function and the deciphering function are respectively defined by

$$c = E_e(m) := V_e(m, 1) \bmod n \tag{3.14}$$

and

$$m' = D_d(c') := V_d(c', 1) \bmod n. \tag{3.15}$$

In order to modify the ciphertext c into c', the cryptanalyst uses the transformation function

$$c' = T_k(c) := V_k(c, 1) \bmod n. \tag{3.16}$$

The non-trivial relation enabling the attack comes from Proposition 1.42. It is possible to express $V_k(x, 1)$ as a polynomial of degree k in the indeterminate x. Consequently, to recover the message m, the cryptanalyst, Carol, does the following.

[Lagrange's modification]: Carol intercepts $c = V_e(m, 1) \bmod n$ and replaces it by $c' = V_k(c, 1) \bmod n$, where k is relatively prime to e.

[Recovery of m']: Next, she gets from Bob the value of m', the plaintext corresponding to c':

$$m' \equiv V_d(c', 1) \equiv V_{dk}(c, 1) \equiv V_{dke}(m, 1) \equiv V_k(m, 1) \pmod{n}.$$

[Non-trivial relation]: She constructs the polynomials $\mathcal{P}, \mathcal{Q} \in \mathbb{Z}_n[x]$ given by

$$\mathcal{P}(x) = D_e(x, 1) - c \bmod n \tag{3.17}$$

and

$$\mathcal{Q}(x) = D_k(x, 1) - m' \bmod n, \tag{3.18}$$

for which m is a root. Then, she computes

$$\mathcal{R} = \gcd(\mathcal{P}, \mathcal{Q}),$$

that is with a very high probability a polynomial of degree 1. So, Carol obtains the value of m by solving $\mathcal{R}$ in x.

2) Attacking Demytko's system. To illustrate the attack against Demytko's system, we shall use division polynomials. Let m be the message to be encrypted. Then, the cryptanalyst proceeds in a similar way as for LUC to recover the message.

[Lagrange's modification]: Carol intercepts $c = [e]_x\, m$ and replaces it by $c' = [k]_x\, c$, where k is relatively prime to e.

[Recovery of m']: Next, she gets from Bob the value of m', the plaintext corresponding to c':

$$m' = [d]_x\, c' = [dke]_x\, m = [k]_x\, m.$$

[Non-trivial relation]: She constructs the polynomials $\mathcal{P}, \mathcal{Q} \in \mathbb{Z}_n[x]$

$$\mathcal{P}(x) = \Phi_e(x) - c\Psi_e(x)^2 \bmod n \tag{3.19}$$

and

$$\mathcal{Q}(x) = \Phi_k(x) - m'\Psi_k(x)^2 \bmod n, \tag{3.20}$$

for which m is a root. Finally, she recovers m by computing $\mathcal{R} = \gcd(\mathcal{P}, \mathcal{Q})$.

1.3.4. *Analysis.* The computation of a GCD may be done as long as the degree of the polynomials is less than 32-bit long [**273**]. So, unlike the basic attack of Davida against RSA, from Eqs (3.17) and (3.18), this attack applies on LUC only if the public encryption exponent e has length less than 32 bits. Moreover, when Alice encrypts a message with Demytko's system with a public exponent e, the polynomial relations (3.19) and (3.20) are of order e^2 instead of e as in LUC. Therefore, this attack is useless against Demytko's system if the encryption exponent e has length greater than 16 bits.

To overcome this drawback, the cryptanalyst (Carol) has to apply the attack twice. We shall illustrate the technique on Demytko's system.

Let m be the message to be encrypted. Then, the attack goes as follows. Carol intercepts $c = [e]_x\, m$, and replaces it by $c'_1 = [k_1]_x\, c$. Next, Bob computes

$$m'_1 = [d]_x\, c'_1 = [dk_1e]_x\, m = [k_1]_x\, m. \tag{3.21}$$

Carol chooses k_2 (relatively prime to k_1), and sends $c'_2 = [k_2]_x\, c$ to Bob. Then, Bob computes

$$m'_2 = [d]_x\, c'_2 = [dk_2e]_x\, m = [k_2]_x\, m. \tag{3.22}$$

Therefore, from relations (3.21) and (3.22), Carol forms the polynomials $\mathcal{P}$ and $\mathcal{Q} \in \mathbb{Z}_n[x]$ given by

$$\mathcal{P}(x) = \Phi_{k_1}(x) - m'_1\Psi_{k_1}(x)^2$$

and

$$\mathcal{Q}(x) = \Phi_{k_2}(x) - m'_2\Psi_{k_2}(x)^2,$$

for which m is a root. So, if k_1 and k_2 are "small" (typically less than 16-bit long), then by solving the polynomial $\mathcal{R} = \gcd(\mathcal{P}, \mathcal{Q})$, Carol obtains the message m.

1.3.5. *Further results.*

1) Substituting the authority. Imagine that we deal with a key distribution scheme. If the cryptanalyst intercepts the encrypted key c sent by the authority to Bob, and modifies it into c', then Bob will discover that the key is corrupted when he will decrypt it. Therefore, he will ask to the authority to re-send the key. If now, the cryptanalyst plays the role of the authority, *i.e.* if he sends the encrypted key c, then the authority will never know that a pirate knows the secret key of Bob. The cryptanalyst behaves thus transparently for the authority.

2) Concealing the cryptanalyst. The aim of the cryptanalyst is to modify the ciphertext c in such a way that Bob is not able to make the difference between his modification and noise (error of transmission) on the public channel. Consequently, he has to modify c in an apparently random way. So, he has to use "large" exponents for the transformation or to use the basic attack of Davida (when applicable).

We shall illustrate this topic on LUC. Imagine that the cryptanalyst, Carol, chooses a small exponent k in order to speed up the computation of the GCD. Then, Bob can "prove" that somebody (namely Carol) modified the ciphertext c into c' by recovering k. He has just to compare (modulo n) $V_j(m,1)$ with m', for $j = 2, 3, \dots, k$. To prevent this, Carol has to choose a relatively large exponent k. However, in order to recover the plaintext, she has to get access two or three times to the bin.

Let m be the message that Alice wants to send to Bob, and let $c = V_e(m,1) \bmod n$ be the corresponding ciphertext, where e is the public key of Bob. Then, the attack is the following.

Carol intercepts c, and replaces it by $c'_1 = V_{k_1}(c,1) \bmod n$. Bob receives c'_1, and decrypts it as $m'_1 = V_d(c'_1, 1) \bmod n$ with his secret key d. Bob asks Alice to re-send c, and Carol sends $c'_2 = V_{k_2}(c,1) \bmod n$. When Bob computes $m'_2 = V_d(c'_2, 1) \bmod n$, he finds a meaningless message. So, he asks to Alice to send a third time the ciphertext c. Next, Carol sends $c'_3 = V_{k_3}(c,1) \bmod n$. Bob decrypts c'_3 to $m'_3 = V_d(c'_3, 1) \bmod n, \dots$

Now, from the discards m'_i $(i = 1, 2(, 3))$, Carol can recover the original message m if k_1, k_2 and k_3 and correctly chosen. This can for instance be done by selecting

$$k_1 = rst, k_2 = ru \text{ and } k_3 = sv,$$

where r and s are small, and $\gcd(st, u) = \gcd(rt, v) = 1$. Note that t, u and v must be sufficiently large to disable Bob to distinguish noise with piracy on the public channel.

From our choices on the transformation keys k_i, Carol obtains

$$\begin{aligned}
m'_1 &\equiv V_{rst}(m,1) \equiv V_{st}\big(V_r(m,1),1\big) \equiv V_{rt}\big(V_s(m,1),1\big) \pmod{n},\\
m'_2 &\equiv V_{ru}(m,1) \equiv V_u\big(V_r(m,1),1\big) \pmod{n},\\
m'_3 &\equiv V_{sv}(m,1) \equiv V_v\big(V_s(m,1),1\big) \pmod{n}.
\end{aligned}$$

Next, she forms the polynomials $\mathcal{Q}_{1_r}, \mathcal{Q}_2 \in \mathbb{Z}_n[y]$ given by

$$\mathcal{Q}_{1_r}(y) = V_{st}(y,1) - m'_1 \quad \text{and} \quad \mathcal{Q}_2(y) = V_u(y,1) - m'_2,$$

for which $V_r(m,1)$ is a root.
Hence, by computing $\mathcal{R} = \gcd(\mathcal{Q}_{1_r}, \mathcal{Q}_2)$, she gets (with a high probability) a polynomial of degree 1, for which $m_r = V_r(m,1) \bmod n$ is the root.

Now, if e is small, Carol recovers the original message m by constructing $\mathcal{P}, \mathcal{R} \in \mathbb{Z}_n[x]$ given by

$$\mathcal{P}(x) = V_e(x,1) - c \quad \text{and} \quad \mathcal{R}(x) = V_r(x,1) - m_r,$$

and by computing $\gcd(\mathcal{P}, \mathcal{R})$, she recovers the original message m as explained before.

Otherwise, she constructs the polynomials $\mathcal{Q}_{1_s}, \mathcal{Q}_3 \in \mathbb{Z}_n[z]$ as

$$\mathcal{Q}_{1_s}(z) = V_{rt}(z,1) - m'_1 \quad \text{and} \quad \mathcal{Q}_3(z) = V_v(z,1) - m'_3,$$

for which $V_s(m,1)$ is a root.
Hence, by computing $\mathcal{S} = \gcd(\mathcal{Q}_{1_s}, \mathcal{Q}_3)$, she gets (with a high probability) a polynomial of degree 1, for which $m_s = V_s(m,1) \bmod n$ is the root. Next, from polynomials $\mathcal{R}, \mathcal{S} \in \mathbb{Z}_n[x]$ given by $\mathcal{R}(x) = V_r(x,1) - m_r$ and $\mathcal{S}(x) = V_s(x,1) - m_s$, she computes $\gcd(\mathcal{R}, \mathcal{S})$ and recovers the message m.

REMARK 3.11. It is possible to speed up the computation by using the ideas developed in [**37**] (see [**171**] for Demytko's system).

3) Combinations/Broadcast encryption. There are basically three ways for a cryptanalyst to recover a message

1. to force the retransmission;
2. to have a look in the bin;
3. to ask a signature.

Therefore, by combining these methods, it is possible to recover the message.

Furthermore, if the same message is broadcasted to several people, the security is compromised if only two or three persons are negligent (*i.e.* they do not protect their bins).

REMARK 3.12. The previous attack was later improved (see Subsection 2.2) against LUC and Demytko's system. However, we have presented it because of its very general nature.

2. Homomorphic attacks

The inherent homomorphic structure of RSA enables to mount some attacks. One example is the Davida's attack (see § 1.3.1). Naturally, all known homomorphic attacks also apply to KMOV since $[k](\mathbf{P} + \mathbf{Q}) = [k]\mathbf{P} + [k]\mathbf{Q}$. This seems not to be the case for LUC and for Demytko's system. However, the existence of a chosen-message forgery against LUC that needs two messages has been described in [**37**]. Kaliski found a similar attack on Demytko's system [**171**].

In this Section, we describe a new chosen-message attack which needs only one message. This new attack shows that RSA-type cryptosystems are even closer related to RSA, *i.e.* several attacks based on the multiplicative nature of the original RSA can straightforwardly be adapted to any RSA-type cryptosystem. We shall illustrate this with the common modulus failure. We also revisit the garbage-man-in-the-middle attack.

2.1. Chosen-message attack.

2.1.1. *Sketch of the attack.* Suppose that a cryptanalyst (say Carol) wants to make Alice to sign message m without her consent. Carol can proceed as follows. She chooses a random number k and asks Alice to sign (or to decrypt) $m' = mk^e \bmod n$. Carol gets then $s' \equiv m^d (k^e)^d \equiv m^d k \pmod n$ and therefore the signature s of message m as $s = s'k^{-1} \bmod n$.

Consequently, chosen-message attacks against RSA seem quite naturally to be a consequence of its multiplicative structure. By reformulating this attack with the extended Euclidean algorithm, it appears that non-homomorphic cryptosystems are also susceptible to a chosen-message attack [**38**]. Applying on RSA, the attack goes as follows.

[Input]: A message m and the public key n, e of Alice.
[Step 1]: Carol chooses an integer k relatively prime to e. Then by the extended Euclidean algorithm, she finds $u, v \in \mathbb{Z}$ such that $ku + ev = 1$.
[Step 2]: Carol computes $m' = m^k \bmod n$.
[Step 3]: Next, she asks Alice to sign m' and gets therefore

$$s' = {m'}^d \bmod n.$$

[Step 4]: Consequently, Carol can compute the signature s of m by

$$s = {s'}^u m^v \bmod n. \tag{3.23}$$

[Output]: The signature s of message m.

Proof. Since $ku + ev = 1$, $d = d(ku + ev) \equiv dku + v \pmod{\operatorname{lcm}(p-1, q-1)}$. Hence, $s \equiv m^d \equiv m^{dku} m^v \equiv \left(m^{dk}\right)^u m^v \equiv {s'}^u m^v \pmod n$. □

2.1.2. *Attacking LUC.* The cryptanalyst Carol can try to get a signature s on a message m in the following way [**35**].

[Input]: A message m and the public key n, e of Alice.
[Step 1]: Carol chooses an integer k relatively prime to e. Then she uses extended Euclidean algorithm to find $u, v \in \mathbb{Z}$ such that $ku + ev = 1$.
[Step 2]: Next she computes $m' = V_k(m, 1) \bmod n$.
[Step 3]: Now she asks Alice to sign m'. If Alice does so then Carol knows s' given by

$$s' = V_d(m', 1) \bmod n.$$

[Step 4]: Finally Carol computes

$$V_{ukd}(m,1) = V_u(s',1) \bmod n, \tag{3.24}$$

$$U_{ukd}(m,1) = \frac{U_k(m,1)U_u(s',1)}{U_e(s',1)} \bmod n, \tag{3.25}$$

and finds the signature s of m

$$\begin{aligned} s &\equiv V_d(m,1) \\ &\equiv \frac{V_{ukd}(m,1)V_v(m,1)}{2} + \frac{\Delta\, U_{ukd}(m,1)U_v(m,1)}{2} \pmod n \end{aligned} \tag{3.26}$$

where $\Delta = m^2 - 4$.

[Output]: The signature s of message m.

PROOF. Eq. (3.24) follows from Eq. (1.23) since

$$V_u(s',1) \equiv V_u\big(V_{kd}(m,1),1\big) \equiv V_{ukd}(m,1) \pmod n.$$

Eq. (3.25) is a consequence of Eq. (1.22) and

$$\begin{aligned} U_{ukd}(m,1)U_e(s',1) &\equiv U_u\big(V_{kd}(m,1),1\big)U_{kd}(m,1)U_e\big(V_{kd}(m,1),1\big) \\ &\equiv U_u\big(V_{kd}(m,1),1\big)U_{kde}(m,1) \\ &\equiv U_u\big(V_{kd}(m,1),1\big)U_k(m,1) \pmod n. \end{aligned}$$

Moreover, $ku+ev = 1$ implies $V_d(m,1) = V_{ukd+dev}(m,1) \equiv V_{ukd+v}(m,1) \pmod n$. Hence Eq. (3.26) is an application of Eq. (1.25). □

2.1.3. *Attacking Demytko's system.* Demytko's system is also vulnerable thanks to Corollary 1.60. The cryptanalyst proceeds similarly as for LUC.

[Input]: A message m and the public key n, e of Alice.

[Step 1]: The cryptanalyst Carol chooses a random number k relatively prime to e. Then she uses extended Euclidean algorithm to find $u, v \in \mathbb{Z}$ such that $ku + ev = 1$.

[Step 2]: Carol computes $m' = [k]_x\, m$. Next, she asks Alice to sign m'. So, Carol obtains the signature

$$s' = [d]_x\, m'.$$

[Step 3]: Finally, Carol finds the signature $s = [d]_x\, m$ of message m as follows.

[Step 3a]: If $[u]_x\, s' \neq [v]_x\, m$ then, by Corollary 1.60, Carol can compute

$$\mathcal{F}_k(m), \mathcal{F}_u(s'), \mathcal{F}_e(s') \text{ and } \mathcal{F}_v(m), \tag{3.27}$$

and

$$s = (m^3 + am + b)\left(\frac{\mathcal{F}_k(m)\mathcal{F}_u(s')/\mathcal{F}_e(s') - \mathcal{F}_v(m)}{[u]_x\, s' - [v]_x\, m}\right)^2 - [u]_x\, s' - [v]_x\, m \bmod n. \tag{3.28}$$

[Step 3b]: Otherwise, the signature is given by

$$s = \frac{\big(3([u]_x\, s')^2 + a\big)^2}{4\big(([u]_x\, s')^3 + a[u]_x\, s' + b\big)} - 2[u]_x\, s' \bmod n. \tag{3.29}$$

[Output]: The signature s of message m.

PROOF. $ku+ev = 1$ implies that $d = kud+evd \equiv kud+v \pmod{N_n}$. Consequently,

$$s = [d]_x\, m = [kud + v]_x\, m = [u]_x\, s' + [v]_x\, m.$$

Let $\mathbf{M}$ and $\mathbf{S}'$ respectively be the points corresponding to m and s', *i.e.* $\mathbf{M} = (m, \cdot)$ and $\mathbf{S}' = (s', \cdot)$.

a) If $[u]_x\, s' \neq [v]_x\, m$, then

$$\begin{aligned}
\mathrm{x}([u]\mathbf{S}' + [v]\mathbf{M}) &\equiv \left(\frac{\mathrm{y}([u]\mathbf{S}') - \mathrm{y}([v]\mathbf{M})}{\mathrm{x}([u]\mathbf{S}') - \mathrm{x}([v]\mathbf{M})}\right)^2 - \mathrm{x}([u]\mathbf{S}') - \mathrm{x}([v]\mathbf{M}) \\
&\equiv \mathrm{y}(\mathbf{M})^2 \left[\frac{\frac{\mathrm{y}([k]\mathbf{M})}{\mathrm{y}(\mathbf{M})}\frac{\mathrm{y}([u]\mathbf{S}')}{\mathrm{y}(\mathbf{S}')}\frac{\mathrm{y}(\mathbf{S}')}{\mathrm{y}([e]\mathbf{S}')} - \frac{\mathrm{y}([v]\mathbf{M})}{\mathrm{y}(\mathbf{M})}}{\mathrm{x}([u]\mathbf{S}') - \mathrm{x}([v]\mathbf{M})}\right]^2 \\
&\qquad - \mathrm{x}([u]\mathbf{S}') - \mathrm{x}([v]\mathbf{M}) \pmod{n}
\end{aligned}$$

since

$$\frac{\mathrm{y}([u]\mathbf{S}')}{\mathrm{y}(\mathbf{M})} = \frac{\mathrm{y}([u]\mathbf{S}')}{\mathrm{y}(\mathbf{S}')}\frac{\mathrm{y}(\mathbf{S}')}{\mathrm{y}([k]\mathbf{M})}\frac{\mathrm{y}([k]\mathbf{M})}{\mathrm{y}(\mathbf{M})}$$

and $\mathrm{y}([k]\mathbf{M}) = \mathrm{y}([edk]\mathbf{M}) = \mathrm{y}([e]\mathbf{S}')$.

b) Otherwise, since $\gcd(d, N_n) = 1$, it follows that $[u]\mathbf{S}' \neq -[v]\mathbf{M}$ and therefore

$$\mathrm{x}([u]\mathbf{S}' + [v]\mathbf{M}) = \left(\frac{3\,\mathrm{x}([u]\mathbf{S}')^2 + a}{2\,\mathrm{y}([u]\mathbf{S}')}\right)^2 - \mathrm{x}([u]\mathbf{S}') - \mathrm{x}([v]\mathbf{M}) \bmod n.$$

$\square$

2.2. Garbage-man-in-the-middle attack (II). A *one*-chosen-message attack straightforwardly extends to the garbage-man-in-the-middle attack. In Subsection 1.3, one, two or three accesses to the bin were required for LUC or for Demytko's system. By the previous chosen-message attack, only one access to the bin is necessary to recover the message m.

Using the same notations as in Subsection 1.3, the garbage-man-in-the-middle attack on LUC and Demytko's system becomes:

1) Attacking LUC.

[Lagrange's modification]: Carol intercepts $c = V_e(m, 1) \bmod n$ and replaces it by $c' = V_k(c, 1) \bmod n$, where k is relatively prime to e.

[Recovery of m']: Next, she gets from Bob the value of m', the plaintext corresponding to c':

$$m' \equiv V_d(c', 1) \equiv V_{dk}(c, 1) \pmod{n}.$$

[Non-trivial relation]: By the extended Euclidean algorithm, Carol computes $u, v \in \mathbb{Z}$ such that $ku + ev = 1$. Then, she computes

$$V_{ukd}(c, 1) = V_u(m', 1) \bmod n,$$
$$U_{ukd}(c, 1) = \frac{U_k(c, 1)U_u(m', 1)}{U_e(m', 1)} \bmod n,$$

and finally recovers m as

$$m = \frac{V_{ukd}(c, 1)V_v(c, 1)}{2} + \frac{\Delta\, U_{ukd}(c, 1)U_v(c, 1)}{2} \bmod n \tag{3.30}$$

where $\Delta = c^2 - 4$.

2) Attacking Demytko's system.

[Lagrange's modification]: Carol intercepts $c = [e]_x\, m$ and replaces it by $c' = [k]_x\, c$, where k is relatively prime to e.

[Recovery of m']: Next, she gets from Bob the value of m', the plaintext corresponding to c':

$$m' = [d]_x\, c' = [dk]_x\, c.$$

[Non-trivial relation]: By the extended Euclidean algorithm, Carol computes $u, v \in \mathbb{Z}$ such that $ku + ev = 1$. If $[u]_x\, m' \neq [v]_x\, c$, then Carol computes $\mathcal{F}_k(c), \mathcal{F}_u(m'), \mathcal{F}_e(m')$ and $\mathcal{F}_v(c)$, and finally recovers the message m as

$$m = (c^3 + ac + b)\left(\frac{\mathcal{F}_k(c)\mathcal{F}_u(m')/\mathcal{F}_e(m') - \mathcal{F}_v(c)}{[u]_x\, m' - [v]_x\, c}\right)^2 - [u]_x\, m' - [v]_x\, c \bmod n; \tag{3.31}$$

otherwise, the message m is given by

$$m = \frac{\big(3([u]_x\, m')^2 + a\big)^2}{4\big(([u]_x\, m')^3 + a[u]_x\, m' + b\big)} - 2[u]_x\, m' \bmod n. \tag{3.32}$$

2.3. Common modulus attack. Simmons pointed out in [**320**] that the use of a common RSA modulus is dangerous. Indeed, if a message m is sent to two users that have coprime public encryption keys, then the message can be recovered. Suppose that the ciphertexts corresponding to message m are given by $c_1 = m^{e_1} \bmod n$ and $c_2 = m^{e_2} \bmod n$, with $\gcd(e_1, e_2) = 1$. Then the cryptanalyst uses the extended Euclidean algorithm to find $u, v \in \mathbb{Z}$ such that $ue_1 + ve_2 = 1$. Therefore, the message m is recovered as

$$m = m^{ue_1+ve_2} \equiv c_1^u c_2^v \pmod{n}. \tag{3.33}$$

The same attack applies on KMOV. From the ciphertexts $\mathbf{C_1} = [e_1]\mathbf{M}$ and $\mathbf{C_2} = [e_2]\mathbf{M}$, the cryptanalyst computes $u, v \in \mathbb{Z}$ such that $ue_1 + ve_2 = 1$ and finds

$$\mathbf{M} = [u]\mathbf{C_1} + [v]\mathbf{C_2}, \tag{3.34}$$

if $\gcd(e_1, e_2) = 1$.

Because the previous chosen-message attack (Subsection 2.1) requires only one message, Lucas-based systems and Demytko's elliptic curve system are vulnerable to the common modulus attack [**153, 38**].

2.3.1. *Extension to LUC and Demytko's system.* Let (e_1, d_1) and (e_2, d_2) be two pairs of encryption/decryption keys and let m be the message being encrypted. Assuming e_1 and e_2 are relatively prime, the cryptanalyst Carol use the extended Euclidean algorithm to find integers u and v such that $ue_1 + ve_2 = 1$.

If m is encrypted as $c_1 = V_{e_1}(m, 1) \bmod n$ and $c_2 = V_{e_2}(m, 1) \bmod n$ by LUC, then Carol recovers it by computing

$$m = \frac{V_u(c_1, 1)V_v(c_2, 1)}{2} + \frac{(c_2^2 - 4)}{2}\,\frac{U_u(c_1, 1)U_{e_1}(c_2, 1)U_v(c_2, 1)}{U_{e_2}(c_1, 1)} \bmod n. \tag{3.35}$$

PROOF. By Proposition 1.38 and since $ue_1 + ve_2 = 1$, we have

$$\begin{aligned}2m &\equiv 2V_{d_2}(c_2,1) \equiv 2V_{d_2(ue_1+ve_2)}(c_2,1) \equiv 2V_{d_2ue_1+v}(c_2,1)\\ &\equiv V_{d_2ue_1}(c_2,1)V_v(c_2,1) + (c_2^2-4)\,U_{d_2ue_1}(c_2,1)U_v(c_2,1)\\ &\equiv V_{ue_1}(m,1)V_v(c_2,1) +\\ &\qquad\qquad (c_2^2-4)\,U_{d_2e_1}(c_2,1)U_u\big(V_{d_2e_1}(c_2,1),1\big)U_v(c_2,1)\\ &\equiv V_u(c_1,1)V_v(c_2,1) +\\ &\qquad\qquad (c_2^2-4)\,U_{d_2e_1}(c_2,1)U_u(c_1,1)U_v(c_2,1) \pmod{n}.\end{aligned}$$

Hence, since

$$\begin{aligned}U_{e_1}(c_2,1) &\equiv U_{e_1e_2d_2}(c_2,1) \equiv U_{d_2e_1}(c_2,1)U_{e_2}\big(V_{d_2e_1}(c_2,1),1\big)\\ &\equiv U_{d_2e_1}(c_2,1)U_{e_2}(c_1,1) \pmod{n},\end{aligned}$$

the proof is complete. □

Suppose now that Demytko's system is used for encryption. Then, Carol can recover $m = [ue_1 + ve_2]_x\, m$ from the ciphertexts $c_1 = [e_1]_x\, m$ and $c_2 = [e_2]_x\, m$ as follows. If $[u]_x\, c_1 \neq [v]_x\, c_2$, then

$$m = (c_2^3 + ac_2 + b)\left[\frac{\mathcal{F}_{e_1}(c_2)\mathcal{F}_u(c_1)/\mathcal{F}_{e_2}(c_1) - \mathcal{F}_v(c_2)}{[u]_x\, c_1 - [v]_x\, c_2}\right]^2 - [u]_x\, c_1 - [v]_x\, c_2 \bmod n; \tag{3.36}$$

otherwise

$$m = \frac{\big(3([u]_x\, c_1)^2 + a\big)^2}{4\big(([u]_x\, c_1)^3 + a[u]_x\, c_1 + b\big)} - 2[u]_x\, c_1 \bmod n. \tag{3.37}$$

PROOF. Let $\mathbf{C_1}$ and $\mathbf{C_2}$ be the points respectively corresponding to ciphertexts c_1 and c_2, *i.e.* $\mathbf{C_1} = (c_1, \cdot)$ and $\mathbf{C_2} = (c_2, \cdot)$. Since $ue_1 + ve_2 = 1$, it follows that

$$m = [d_1]_x\, c_1 = [d_1(ue_1 + ve_2)]_x\, c_1 = \mathrm{x}([u]\mathbf{C_1} + [v]\mathbf{C_2}).$$

Noting that $\mathrm{y}([e_2]\mathbf{C_1}) = \mathrm{y}([e_1]\mathbf{C_2})$, Eqs (3.36) and (3.37) are simply an application of addition formulae on elliptic curves. □

2.3.2. *Faulty encryption.* We will suppose that an error occurs during the computation of the ciphertext. More precisely, if $e = \sum_{i=0}^{t-1} e_i 2^i$ (with $e_{t-1} = 1$) denotes the binary decomposition of the public exponent e, we will suppose that the j^{th} bit of e flips to its complementary value.

For example, if RSA is used, the ciphertext corresponding to message m will be $\hat{c} = m^{\hat{e}} \bmod n$ instead of $c = m^e \bmod n$, where

$$\hat{e} = \begin{cases} e + 2^j & \text{if } e_j = 0, \\ e - 2^j & \text{if } e_j = 1. \end{cases} \tag{3.38}$$

Let $\delta = \gcd(\hat{e}, e)$. Since $\delta = \gcd(e \pm 2^j, e)$, δ divides 2^j. This implies $\delta = 1$ because e is odd for RSA.

Therefore, a cryptanalyst can recover m from c and $\hat{c}$ by the common modulus attack described in Subsection 2.3 [**162**]. This attack also applies to LUC and KMOV since the encryption exponent must be odd for these systems. This is not always the case for Demytko's system.

When several bits of the encryption exponent flip, the attack may still apply or not depending on the value of $\gcd(\hat{e}, e)$. Note also that using prime public encryption exponents is dangerous because, in this case, the attack is always applicable.

3. Other attacks

This last section will address attacks resulting from bad implementations or from the presence of faults.

If the secret prime factors p and q of the RSA-moduli are improperly chosen, then factoring attacks [**278, 352**] can recover the secret keys. Note also that p and q must carefully be generated [**282**]. Factoring attacks were recently reconsidered by Silverman and Rivest [**318, 293**]. Furthermore, if a portion of the bits of p (or q) is known, then the RSA-moduli can be factorized [**291, 68**]. Although dangerous, we will not discuss this kind of attacks because there apply identically to any RSA-type system. There are also attacks depending on specific software implementations, such as the timing attacks [**183**] or the cycling attacks against defective hardware [**115**]. Other attacks were mounted against some standards using the RSA cryptosystem (see for example the attacks of Girault and Misarsky [**118, 242**]). On the other hand, the RSA cryptosystem was sometimes modified for efficiency or security purposes. A good example is the Shamir's unbalanced RSA [**313**] which use extremely large moduli. However, unless carefully implemented and used, this version can be completely broken [**113**]. The range of attacks resulting from bad implementations is quite large. So we will only explain how to choose the secret (decryption or signature) exponent d.

The second kind of attacks that we will analyze relies on the presence of faults during the computations. If no precaution is taken, we will see that this can give some information on the secret parameters.

Faults based attacks are quite old [**255**]. In his book "Seizing the Enigma", Kahn reported that, before sending a ciphertext, the operators of Enigma (used by the Germans during the World War II) encrypted a given message twice and compared the resulting ciphertexts. They already knew that Enigma could be attacked if an error occurred during the computation of a ciphertext. We will here study the consequences of faults in the RSA-type cryptosystems (see also § 2.3.2).

3.1. Wiener's attack. Wiener [**350**] showed that if the secret key d is chosen too small, then it can be recovered. In the RSA cryptosystem, the public key e and the secret key d are related by

$$ed \equiv 1 \pmod{\operatorname{lcm}(p-1, q-1)}.$$

So, $\exists k, h \in \mathbb{Z}$ with $\gcd(k, h) = 1$ such that

$$ed = 1 + \frac{k}{h}(p-1)(q-1) = 1 + \frac{k}{h}(n - p - q + 1).$$

Therefore, dividing both sides by dn yields

$$\frac{k}{hd} - \frac{e}{n} = \frac{k}{hd}\left(\frac{1}{p} + \frac{1}{q} - \frac{1}{n}\right) - \frac{1}{dn}. \tag{3.39}$$

Following the presentation of Pinch [**277**], the attack of Wiener can be explained by the following theorem.

THEOREM 3.13. *If* $\left|\frac{a}{b} - x\right| < \frac{1}{2b^2}$, *then* $\frac{a}{b}$ *is a continued fraction approximant for* x.

PROOF. See [**137**, p. 153], Theorem 184. □

So, if the condition of the previous theorem is fulfilled, then $k/(hd)$ 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 3.14. *Assume that* $p \sim q \sim \sqrt{n}$, *that* $h < d$ *and that* $e \sim n$. *Then,* $k \sim hd$ *and the continued fraction attack will succeed for secret exponents of order up to* $n^{1/4}$.

The assumption $h < d$ comes from the fact that the RSA-modulus n is generally chosen as a *rigid* integer, *i.e.* n is the product of two primes of the form $p = 2p' + 1$ and $q = 2q' + 1$ where p' and q' are prime (in this case, $h = 2$). Indeed, if $p - 1$ or $q - 1$ does not contain large prime factors then the Pollard's $p - 1$ method [**278**] enables to factorize n.

PROOF (OF COROLLARY 3.14). If $e \sim n$, then $k \sim hd$ since the right side of Eq. (3.39) tends to zero. We now have to verify the condition of Theorem 3.13:

$$\left|\frac{k}{hd} - \frac{e}{n}\right| \leq \frac{k+h}{hdn} + \frac{k}{hd}\left(\frac{1}{p} + \frac{1}{q}\right) \sim \frac{1}{n} + \frac{1}{\sqrt{n}} \sim \frac{1}{\sqrt{n}}.$$

So $\left|\frac{k}{hd} - \frac{e}{n}\right| < \frac{1}{2h^2d^2} \sim \frac{1}{d^2}$ if d is of order at most $n^{1/4}$. □

For LUC, the public and the secret keys are chosen according to $ed \equiv 1 \pmod{\operatorname{lcm}(p - (\Delta/p), q - (\Delta/q))}$. Hence, fixing the sign of the two Legendre symbols, we can write [**277**]

$$\frac{k}{hd} - \frac{e}{n} = \frac{k}{hd}\left(\pm\frac{1}{p} \pm \frac{1}{q} \pm \frac{1}{n}\right) - \frac{1}{dn}, \tag{3.40}$$

for some k and h such that $\gcd(k, h) = 1$. From this equation, we can prove that Corollary 3.14 remains valid.

PROOF. Straightforward since

$$\left|\frac{k}{hd} - \frac{e}{n}\right| \leq \frac{k+h}{hdn} + \frac{k}{hd}\left(\frac{1}{p} + \frac{1}{q}\right) \sim \frac{1}{\sqrt{n}}.$$

So the condition of Theorem 3.13 is fulfilled if d is of order at most $n^{1/4}$. □

This attack also applies to KMOV under the same assumptions. In KMOV, we have $ed \equiv 1 \pmod{\operatorname{lcm}(p+1, q+1)}$. So this can be seen as a special case of LUC where $(\Delta/p) = (\Delta/q) = -1$.

Pinch [**277**] also extended the previous attack to Demytko's cryptosystem by using the Hasse's Theorem.

COROLLARY 3.15. *Assume that $p \sim q \sim \sqrt{n}$, that $h < d$ and that $e \sim n$. Then, $k \sim hd$ and the continued fraction attack will succeed for secret exponents of order up to $n^{1/8}$.*

PROOF. For Demytko's system, the secret and public keys are related by $ed \equiv 1 \pmod{\operatorname{lcm}(p + 1 \pm a_p, q + 1 \pm a_q)}$. So if h is the highest common factor of $p + 1 \pm a_p$ and $q + 1 \pm a_q$, then

$$ed = 1 + \frac{k}{h}(p + 1 \pm a_p)(q + 1 \pm a_q),$$

for some integer k so that

$$\frac{k}{hd} - \frac{e}{n} = \frac{k}{hd}\left(\frac{\pm a_p - 1}{p} + \frac{\pm a_q - 1}{q} + \frac{\pm a_p \pm a_q \pm a_p a_q - 1}{n}\right) - \frac{1}{dn}$$

$$(*) \qquad \sim \frac{k}{hd}\left(\pm\frac{a_p}{p} \pm \frac{a_q}{q} \pm \frac{a_p a_q}{n}\right) - \frac{1}{dn}.$$

By Theorem 1.46, $|a_p| \leq 2\sqrt{p}$ and $|a_q| \leq 2\sqrt{q}$. Hence, $k \sim hd$ since $e \sim n$ and (*) tends to zero. Furthermore, this implies that

$$\left|\frac{k}{hd} - \frac{e}{n}\right| \lesssim \frac{k}{hd}\left(\frac{2}{\sqrt{p}} + \frac{2}{\sqrt{q}} + \frac{4}{\sqrt{n}}\right) + \frac{1}{dn} \sim \frac{1}{n^{1/4}}.$$

Therefore, from Theorem 3.13, $k/(hd)$ will be a continued approximant for e/n as long as d has order at most $n^{1/8}$. □

The choice of short secret exponents may be attractive in order to quickly perform decryptions or to efficiently sign messages. However, some precautions must be taken. Table 3.6 summarizes the minimum key length for the secret exponent to avoid the Wiener's attack.

n	512	1024
RSA	~ 128	~ 256
LUC	~ 128	~ 256
KMOV	~ 128	~ 256
Demytko	~ 64	~ 128

Table 3.6: Order (in bits) of a secure secret key d for a 512/1024-bit modulus n

3.2. Lenstra's attack. In September 1996, Boneh, DeMillo and Lipton from Bellcore identified a new attack against RSA when performed with Chinese remaindering. This attack was reported in a Bellcore press release, but no technical details were provided. Thereafter and independently, Lenstra wrote a short memo [**205**] that after the publication of the Bellcore researchers [**40**] appeared as a more realistic attack. In case of computation error, the Bellcore researchers showed how to recover the secret factors p and q of the public modulus n from two signatures of the same message: a correct one and a faulty one; Lenstra showed that actually only the faulty signature is required.

We will show that Lenstra's attack is of very general nature and applies on all Chinese remaindering based cryptosystems [**156**].

3.2.1. *Review of Lenstra's attack.* Let p and q be two primes and let $n = pq$. Imagine that a message m is signed with the secret exponent d using RSA: $s = m^d \bmod n$. Using Theorem 1.12, the value of s can be computed more efficiently [**283**] from

$$s_p = m_p^{d_p} \bmod p \quad \text{and} \quad s_q = m_q^{d_q} \bmod q, \tag{3.41}$$

with $m_p = m \bmod p$, $m_q = m \bmod q$, $d_p = d \bmod (p-1)$ and $d_q = d \bmod (q-1)$.

Suppose that an error occurs during the computation of s_p (we note $\hat{s}_p$ the faulty value), but not during the computation of s_q. Applying Chinese remaindering on $\hat{s}_p$ ($\neq s_p$) and s_q will give the faulty signature $\hat{s}$ for message m. Then, the computation of

$$\gcd(\hat{s}^e - m \bmod n, n) \tag{3.42}$$

will give the secret factor q, where e is the public exponent.

Proof. This is a special case of Proposition 3.17. □

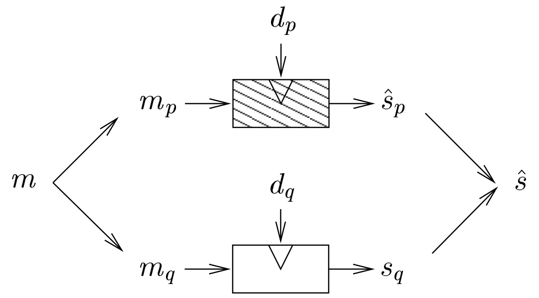

Figure 3.7: Lenstra's attack

Remark 3.16. The same attack applies to decryption process, if the attacker has access to the faulty decryption (see pp. 2–3).

3.2.2. *Generalization.* In this Paragraph, $n = pq$ denotes the RSA-modulus, and e and d are respectively the public and the secret exponents. The message to be signed is m, and the corresponding signature is s. Let

$$\mathcal{S} : \mathbb{Z}_n \to \mathbb{Z}_n, m \mapsto s = \mathcal{S}(m)$$

be an RSA-type signature function. If the signature s of message m is performed with the Chinese Remainder Theorem, then the previous attack still applies. More explicitly, we have:

PROPOSITION 3.17. *Let two primes p and q whose product is n. Suppose that $s = \mathcal{S}(m)$ is the signature of a message m and that $\hat{s}$ is a faulty signature. If $\hat{s} \not\equiv s \pmod{p}$ but $\hat{s} \equiv s \pmod{q}$, then*

$$\gcd(\mathcal{S}^{-1}(\hat{s}) - m \bmod n, n) \tag{3.43}$$

will give the secret factor q.

PROOF. Since $\hat{s} \equiv s \pmod{q}$ and $\hat{s} \not\equiv s \pmod{p}$,

$$\mathcal{S}^{-1}(\hat{s}) \equiv \mathcal{S}^{-1}(s) \equiv m \pmod{q}$$

and $\mathcal{S}^{-1}(\hat{s}) \not\equiv m \pmod{p}$. Hence, $\mathcal{S}^{-1}(\hat{s}) - m \pmod{n}$ is divisible by q and not by p. □

Consequently, the attack of Lenstra works with all RSA-type cryptosystems. With LUC, the signature function is defined as $\mathcal{S}(m) := V_d(m, 1) \bmod n$, and the verification function is defined as $\mathcal{S}^{-1}(s) := V_e(s, 1) \bmod n$. If $\hat{s} \not\equiv s \pmod{p}$ but $\hat{s} \equiv s \pmod{q}$, then

$$\gcd(V_e(\hat{s}, 1) - m \bmod n, n) \tag{3.44}$$

will give q.

Demytko's cryptosystem uses the x-coordinate of points on elliptic curves over the ring $\mathbb{Z}_n$. The x-coordinate of the multiple of a point can be computed thanks to division polynomials (see Proposition 1.59) considered as univariate polynomials. The signature function is defined as $\mathcal{S}(m) := \Phi_d(m)/\Psi_d(m)^2 \bmod n$, and the verification function as $\mathcal{S}^{-1}(s) := \Phi_e(s)/\Psi_e(s)^2 \bmod n$. If $\hat{s} \not\equiv s \pmod{p}$ but $\hat{s} \equiv s \pmod{q}$, then

$$\gcd\left(\frac{\Phi_e(\hat{s})}{\Psi_e(\hat{s})^2} - m \bmod n, n\right) \tag{3.45}$$

will give q. For KMOV, the two coordinates of the points are used. Let $\mathbf{S} = (s_1, s_2) = [d]\mathbf{M}$ be the KMOV-signature of message $\mathbf{M} = (m_1, m_2)$. Suppose that the computation of the x-coordinate of $\mathbf{S}$ is faulty. More precisely, if $\widehat{s_1} \not\equiv s_1 \pmod{p}$ and $\widehat{s_1} \equiv s_1 \pmod{q}$, then, as for Demytko's system, q can be recovered by computing $\gcd(\Phi_e(\widehat{s_1})/\Psi_e(\widehat{s_1})^2 - m_1 \bmod n, n)$. If only the computation of the y-coordinate of $\mathbf{S}$ is faulty, *i.e.* $\widehat{s_2} \not\equiv s_2 \pmod{p}$ and $\widehat{s_2} \equiv s_2 \pmod{q}$, then, thanks to Proposition 1.59, q can be found by computing

$$\gcd\left(\frac{\omega_e(s_1,\widehat{s_2})}{\Psi_e(s_1,\widehat{s_2})^3} - m_2 \bmod n, n\right). \tag{3.46}$$

3.2.3. *Countermeasure.* Shamir [**309**] presented a simple solution to prevent the previous attack. We shall illustrate his technique for RSA, but it remains valid for the other RSA-type systems. The signer first chooses a (small) random number r relatively prime to n. Then he computes $s_{rp} = m^{d \bmod \phi(rp)} \bmod rp$ and $s_{rq} = m^{d \bmod \phi(rq)} \bmod rq$. If $s_{rp} \equiv s_{rq} \pmod{r}$, then the computations are assumed correct, and s is computed by applying Chinese remaindering on $(s_{rp} \bmod p)$ and $(s_{rq} \bmod q)$.

3.2.4. *Further results.* Imagine that someone finds a lost smart card. The card performs RSA signatures (using Chinese remaindering), but does not mention any information about its owner. The attacker is thus in a situation where he does not possess *any* information about the parameters, even not the public ones. Even in such a challenging situation, it is possible to recover much sensitive information if the public exponent is known. Since the public exponent is often a standard value (for example, $e = 3, 5$ or $2^{16} + 1$), identical for each card of a given organization, this hypothesis is not so unlikely [**154**].

As before, suppose that the computation modulo p is faulty. From two faulty signatures $\hat{s}_1$ and $\hat{s}_2$ of messages m_1 and m_2 respectively, we compute $g = \gcd(\hat{s}_1^e - m_1, \hat{s}_2^e - m_2)$ over the rational integers. Removing the small factors of g gives the secret value of q. Moreover, once q is known, we can compute $d_q = e^{-1} \bmod q - 1$.

Furthermore, from the knowledge of two (valid) signatures s_3 and s_4 of messages m_3 and m_4, we can find p by computing $\gcd((s_3^e - m_3)/q, (s_4^e - m_4)/q)$. Of course, these results straightforwardly extend to any Chinese remaindering based cryptosystem, including LUC, KMOV and Demytko's system.

3.3. (Transient) faults based attack. At the last Workshop on Security Protocols, some researchers from the University of Singapore exhibited new attacks against several cryptosystems [**17**]. Their attacks exploit the presence of transient faults. By exposing a device to external constraints, one can induce some faults with a non-negligible probability [**14**]. We will show that their attacks are of very general nature [**165**]. Moreover, we will focus on signatures generation, reducing the number of required signatures for a successful attack to one.

In the sequel, $n = pq$ will denote the RSA-modulus, and e and d will respectively denote the public verification key and the secret signature key. Let $d = \sum_{i=0}^{t-1} d_i 2^i$ be the binary expansion of d. We assume that one bit of d flips to its complementary value when the signature is performed. This corrupted signature key will be denoted $\hat{d}$. So, if bit j of d flips, then

$$\hat{d} = \begin{cases} d + 2^j & \text{if } d_j = 0, \\ d - 2^j & \text{id } d_j = 1. \end{cases} \tag{3.47}$$

3.3.1. *Attacking RSA.* Let $s = m^d \bmod n$ and $\hat{s} = m^{\hat{d}} \bmod n$ be the correct and the faulty signatures corresponding to message m, respectively. Mimicking the attack in [**17**], we find the flipped bit of d by computing

$$\frac{\hat{s}}{s} \equiv m^{\hat{d}-d} \equiv \begin{cases} m^{2^j} \pmod{n} & \text{if } d_j = 0, \\ \frac{1}{m^{2^j}} \pmod{n} & \text{if } d_j = 1. \end{cases} \tag{3.48}$$

However, this formulation is not optimal in signature context. If we put Eq. (3.48) to the e, we obtain

$$\frac{\hat{s}^e}{m} \equiv \begin{cases} (m^e)^{2^j} \pmod{n} & \text{if } d_j = 0, \\ \frac{1}{(m^e)^{2^j}} \pmod{n} & \text{if } d_j = 1. \end{cases} \tag{3.49}$$

So only the faulty signature $\hat{s}$ is required to recover the flipped bit. The attack can thus be summarized as follows. The attacker randomly chooses a message m. He computes $F = m^e \bmod n$ and $\alpha_j = F^{2^j} \bmod n$. Then, inducing a physical effort, he asks the device to sign message m. If one bit of d has flipped, he easily recovers it by comparing $\hat{s}^e/m$ to α_j and $1/\alpha_j$.

3.3.2. *Attacking LUC.* The attack on LUC works similarly. The attacker chooses a random message m. He computes $F = V_e(m, 1) \bmod n$ and $G = (m^2 - 4)\, U_e(m, 1) \bmod n$. He also computes $\alpha_j = V_{2^j}(F, 1) \bmod n$ and $\beta_j = U_{2^j}(F, 1) \bmod n$. Now, inducing a external effort to the signing device, he gets the faulty signature of message m,

$$\hat{s} = V_{\hat{d}}(m, 1) \bmod n.$$

Finally, he finds the flipped bit of d as

$$2V_e(\hat{s}, 1) \equiv \begin{cases} \alpha_j m + \beta_j G \pmod{n} & \text{if } d_j = 0, \\ \alpha_j m - \beta_j G \pmod{n} & \text{if } d_j = 1. \end{cases} \tag{3.50}$$

Proof. From the properties of Lucas sequences (see Proposition 1.38), it follows that

$$\begin{aligned}
2V_e(\hat{s},1) &\equiv 2V_e\big(V_{\hat{d}}(m,1),1\big) \equiv V_{e(\hat{d}-d+d)}(m,1) \equiv 2V_{e(\hat{d}-d)+1}(m,1)\\
&\equiv V_{e(\hat{d}-d)}(m,1)V_1(m,1) + \Delta U_{e(\hat{d}-d)}(m,1)U_1(m,1)\\
&\equiv V_{\hat{d}-d}\big(V_e(m,1),1\big)m + (m^2-4)\,U_e(m,1)U_{\hat{d}-d}\big(V_e(m,1),1\big)\\
&\equiv V_{\hat{d}-d}(F,1)m + U_{\hat{d}-d}(F,1)G \pmod{n}.
\end{aligned}$$

Moreover, since $V_{-k}(P,1) = V_k(P,1)$ and $U_{-k}(P,1) = -U_k(P,1)$, we have the required result. □

Note that the computation of α_j and β_j is not expensive. Taking $m = k$ in Eqs (1.19) and (1.18) yields $V_{2k}(P,1) = V_k^2(P,1) - 2$ and $U_{2k}(P,1) = U_k(P,1)V_k(P,1)$. Therefore, α_j and β_j can recursively be evaluated by

$$\begin{cases}\alpha_0 = F\\ \alpha_j = \alpha_{j-1}^2 - 2 \bmod n\end{cases} \quad\text{and}\quad \begin{cases}\beta_0 = 1\\ \beta_j = \alpha_{j-1}\beta_{j-1} \bmod n\end{cases}. \tag{3.51}$$

3.3.3. *Attacking KMOV.* In KMOV, messages are represented as points of elliptic curves. Let $\mathbf{M} = (m_1, m_2)$ be the message being signed, and let $\mathbf{S} = [d]\mathbf{M}$ and $\hat{\mathbf{S}} = [\hat{d}]\mathbf{M}$ respectively be the correct and the faulty signatures. We still assume that bit j of d has flipped during the computation of the signature, *i.e.* $\hat{d} = d \pm 2^j$.

To recover this flipped bit, the attacker has just to compare $[e]\hat{\mathbf{S}} - \mathbf{M}$ to $[\hat{d}-d]\,([e]\mathbf{M})$. More precisely,

$$[e]\hat{\mathbf{S}} - \mathbf{M} = \begin{cases}[2^j](F_1,F_2) & \text{if } s_j = 0\\ [2^j](F_1,-F_2) & \text{if } s_j = 1\end{cases}, \tag{3.52}$$

where $(F_1, F_2) = [e]\mathbf{M}$.

Proof. Obvious since

$$\begin{aligned}
[e]\hat{\mathbf{S}} &= [e\hat{d}]\mathbf{M} = [e(\hat{d}-d+d)]\mathbf{M} = [e(\hat{d}-d)]\mathbf{M} + \mathbf{M}\\
&= [\hat{d}-d]\,([e]\mathbf{M}) + \mathbf{M}.
\end{aligned}$$

Moreover, if $\mathbf{P} = (P_1, P_2)$ is a point on an elliptic curve, then its inverse is given by $-\mathbf{P} = (P_1, -P_2)$. □

3.3.4. *Attacking Demytko's system.* Demytko's system only uses the x-coordinate of points on elliptic curves. Let m the message to be signed. This message is represented as a point $\mathbf{M} = (m, \cdot)$, or equivalently $m = \mathrm{x}(\mathbf{M})$. As before, we suppose that one bit of d has flipped during the computation of the signature. So, the resulting signature is $\hat{s}$.

The attack relies on Corollary 1.60. To recover the flipped bit of d, the attacker computes $F = \mathrm{x}([e]\mathbf{M}) = \mathcal{G}_e(m)$, $G = \mathrm{y}([e]\mathbf{M})/\,\mathrm{y}(\mathbf{M}) = \mathcal{F}_e(m)$, $H = m^3 + am + b \bmod n$, $\alpha_j = \mathcal{G}_{2^j}(F)$ and $\beta_j = \mathcal{F}_{2^j}(F)$. Then,

$$[e]_x\,\hat{s} + m \equiv \begin{cases} \frac{(\beta_j G-1)^2 H}{(\alpha_j - M)^2} - \alpha_j \pmod{n} & \text{if } s_j = 0, \\ \frac{(\beta_j G+1)^2 H}{(\alpha_j - M)^2} - \alpha_j \pmod{n} & \text{if } s_j = 1. \end{cases} \tag{3.53}$$

PROOF. The chord-and-tangent addition on elliptic curves yields

$$\begin{aligned}
[e]_x\,\hat{s} &\equiv \mathcal{G}_e(\hat{s}) \equiv \mathrm{x}([\hat{d}e]\mathbf{M}) \equiv \mathrm{x}\big([(\hat{d}-d)e]\mathbf{M} + \mathbf{M}\big) \\
&\equiv \left[\frac{\mathrm{y}([(\hat{d}-d)e]\mathbf{M}) - \mathrm{y}(\mathbf{M})}{\mathrm{x}([(\hat{d}-d)e]\mathbf{M}) - \mathrm{x}(\mathbf{M})}\right]^2 - \mathrm{x}([e(\hat{d}-d)]\mathbf{M}) - \mathrm{x}(\mathbf{M}) \\
&\equiv \frac{m^3+am+b}{\Big(\mathrm{x}\big([\hat{d}-d]([e]\mathbf{M})\big) - m\Big)^2}\left[\frac{\mathrm{y}\Big([\hat{d}-d]([e]\mathbf{M})\Big)}{\mathrm{y}(\mathbf{M})} - 1\right]^2 \\
&\quad - \mathrm{x}\big([\hat{d}-d]([e]\mathbf{M})\big) - m \\
&\equiv \frac{H\left[\frac{\mathrm{y}\left([\hat{d}-d]([e]\mathbf{M})\right)}{\mathrm{y}([e]\mathbf{M})}\,\frac{\mathrm{y}([e]\mathbf{M})}{\mathrm{y}(\mathbf{M})} - 1\right]^2}{(\mathcal{G}_{\hat{d}-d}(F) - m)^2} - \mathcal{G}_{\hat{d}-d}(F) - m \\
&\equiv \frac{H\big(\mathcal{F}_{\hat{d}-d}(F)\,G - 1\big)^2}{\big(\mathcal{G}_{\hat{d}-d}(F) - m\big)^2} - \mathcal{G}_{\hat{d}-d}(F) - m \pmod{n}.
\end{aligned}$$

Hence, since $\mathcal{G}_{-k}(x) = \mathcal{G}_k(x)$ and $\mathcal{F}_{-k}(x) = -\mathcal{F}_k(x)$, the proof is complete. $\square$

3.3.5. *Further results.*

Generalizing the number of faulty bits. Assume that two bits of d are faulty when performing the signature of a message m with the RSA. Then, the signature is $\hat{s} = m^{\hat{d}} \bmod n$, where

$$\hat{d} = d \pm 2^j \pm 2^k. \tag{3.54}$$

As before, the attacker computes $F = m^e \bmod n$, $\alpha_j = F^{2^j} \bmod n$, and compares $\hat{s}^e/m$ to $(\alpha_j)^{\pm 1}(\alpha_k)^{\pm 1}$ until a match is found. In this case, he finds two bits of the secret key d. This method naturally extends to multiple faulty bits and to Lucas-based and elliptic curve systems.

Davida's attack. This attack also applies for encryption process. This can been considered as a special case of the Davida's attack (see § 1.3.1). We shall illustrate this attack on RSA, but it remains valid for Lucas-based and elliptic curve systems.

Let e and d be the pair of public encryption key and secret decryption key of Bob. The attacker chooses a random message m, computes the ciphertext $c = m^e \bmod n$ with the public key e of Bob. Then, inducing a external constraint, he asks Bob to decipher c. If Bob does so, he obtains $\hat{m} = c^{\hat{d}} \bmod n$. Since $\hat{m}$ is meaningless, Bob will discard it. Suppose that the attacker can get access to this discard and that only one bit of d is faulty, i.e. $\hat{d} = d \pm 2^j$. Then,

$$\frac{\hat{m}^e}{c} \equiv \begin{cases} (c^e)^{2^j} \pmod{n} & \text{if } d_j = 0, \\ \frac{1}{(c^e)^{2^j}} \pmod{n} & \text{if } d_j = 1. \end{cases} \tag{3.55}$$

References

[14] R. J. Anderson and M. Kuhn, *Tamper resistance – a cautionary note*, Proceedings of the Second USENIX Workshop on Electronic Commerce, USENIX Association, 1996, pp. 1–11.

[17] 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.

[34] D. Bleichenbacher, Personal communication.

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

[36] ———, *On the security of the KMOV public key cryptosystem*, Advances in Cryptology – Crypto '97 (B. S. Kaliski Jr, ed.), Lecture Notes in Computer Science, vol. 1294, Springer-Verlag, 1997, pp. 235–248.

[37] 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.

[38] D. Bleichenbacher, M. Joye, and J.-J. Quisquater, *A new and optimal chosen-message attack on RSA-type cryptosystems*, Information and Communications Security (Y. Han, T. Okamoto, and S. Qing, eds.), Lecture Notes in Computer Science, vol. 1334, Springer-Verlag, 1997, pp. 302–313.

[40] 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.

[42] F. Borceux, *Invitation à la géométrie*, Ciaco, Louvain-la-Neuve, 1986.

[68] D. Coppersmith, *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.

[69] ———, *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.

[70] ———, *Small solutions to polynomials equations, and low exponent RSA vulnerabilities*, Journal of Cryptology **10** (1997), no. 4, 233–260.

[71] 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.

[83] 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.

[90] D. E. Denning, *Digital signatures with RSA and other public-key cryptosystems*, Communications of the ACM **27** (1984), no. 4, 388–392.

[108] M. K. Franklin and M. K. Reiter, *A linear protocol failure for RSA with exponent three*, Preliminary note for Crypto '95 rump session.

[113] H. Gilbert, D. Gupta, A. M. Odlyzko, and J.-J. Quisquater, *Attacks on Shamir's 'RSA for paranoids'*, Preprint.

[115] A. Gillet, M. Joye, and J.-J. Quisquater, *Cautionary note for protocols designers: Security proof is not enough*, Proc. of the DIMACS Workshop on Design and Formal Verification of Security Protocols (H. Orman and C. Meadows, eds.), (CDROM), 1997.

[118] M. Girault and J.-F. Misarsky, *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.

[137] G. H. Hardy and E. M. Wright, *An introduction to the theory of numbers*, 5th ed., Oxford University Press, 1979.

[139] 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.

[140] ———, *Solving simultaneous modular equations of low degree*, SIAM Journal on Computing **17** (1988), no. 2, 336–341.

[153] M. Joye, *Common modulus attack against Lucas-based systems*, Tech. Report CG-1996/10, UCL Crypto Group, Louvain-la-Neuve, December 1996.

[154] M. Joye, F. Koeune, and J.-J. Quisquater, *Further results on Chinese remaindering*, Tech. Report CG-1997/1, UCL Crypto Group, Louvain-la-Neuve, January 1997, Presented at the rump session of Eurocrypt '97.

[155] ———, *Takagi/Naito's algorithm revisited*, Tech. Report CG-1997/3, UCL Crypto Group, Louvain-la-Neuve, March 1997.

[156] M. Joye, A. K. Lenstra, and J.-J. Quisquater, *Chinese remaindering in the presence of faults*, Submitted to Journal of Cryptology.

[162] M. Joye and J.-J. Quisquater, *Faulty RSA-type encryption*, Tech. Report CG-1997/8, UCL Crypto Group, Louvain-la-Neuve, July 1997.

[163] ———, *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.

[164] ———, *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.

[165] M. Joye, J.-J. Quisquater, F. Bao, and R. H. Deng, *RSA-type signatures in the presence of transient faults*, To appear in the proceedings of the *Sixth IMA International Conference on Cryptography and Coding*, Cirencester, U.K., 17-19th December 1997.

[171] B. S. Kaliski Jr, *A chosen message attack on Demytko's elliptic curve cryptosystem*, Journal of Cryptology **10** (1997), no. 1, 71–72.

[183] P. C. Kocher, *Timing attacks on implementations of Diffie-Hellman, RSA, DSS, and other systems*, Advances in Cryptology – Crypto '96 (N. Koblitz, ed.), Lecture Notes in Computer Science, vol. 1109, Springer-Verlag, 1996, pp. 104–113.

[190] 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.

[192] H. Kuwakado and K. Koyama, *Security of RSA-type cryptosystems over elliptic curves against Håstad attack*, Electronics Letters **30** (1994), no. 22, 1843–1844.

[205] A. K. Lenstra, *Memo on RSA signature generation in the presence of faults*, September 1996.

[242] J.-F. Misarsky, *A multiplicative attack using LLL algorithm on RSA signatures with redundancy*, Advances in Cryptology – Crypto '97 (B. S. Kaliski Jr, ed.), Lecture Notes in Computer Science, vol. 1294, Springer-Verlag, 1997, pp. 221–234.

[254] S. Murphy, *Remarks on the LUC public key system*, Electronics Letters **30** (1994), no. 7, 558–559.

[255] D. Naccache, Personal communication.

[273] J. Patarin, *Some serious protocol failures for RSA with exponent e of less than ≃ 32 bits*, Presented at the conference of cryptography, CIRM Luminy, France, September 1995.

[276] R. G. E. Pinch, *Extending the Håstad attack to LUC*, Electronics Letters **31** (1995), no. 21, 1827–1828.

[277] ———, *Extending the Wiener attack to RSA-type cryptosystems*, Electronics Letters **31** (1995), no. 20, 1736–1738.

[278] J. M. Pollard, *Theorems on factorization and primality testing*, Proc. Cambridge Philos. Soc. **76** (1974), 521–528.

[282] J.-J. Quisquater, *How to avoid a successful cryptanalysis of your random prime generator (abstract)*, Presented at the conference of cryptography, CIRM Luminy, France, September 1995.

[283] J.-J. Quisquater and C. Couvreur, *Fast decipherment algorithm for RSA public-key cryptosystem*, Electronics Letters **18** (1982), no. 21, 905–907.

[291] R. L. Rivest and A. Shamir, *Efficient factoring based on partial information*, Advances in Cryptology – Eurocrypt '85 (F. Pichler, ed.), Lecture Notes in Computer Science, vol. 219, Springer-Verlag, 1986, pp. 31–34.

[293] R. L. Rivest and R. D. Silverman, *Are 'strong' primes needed for RSA*, The 1997 RSA Laboratories Seminar Series, Seminars Proceedings, 1997.

[309] A. Shamir, *How to check modular exponentiation*, Presented at the rump session of Eurocrypt '97.

[313] ———, *RSA for paranoids*, CryptoBytes **1** (1995), no. 3, 1–4.

[314] H. Shimizu, *On the improvement of the Håstad bound*, Proc. of the 1996 IEICE Fall Conference, vol. A-162, 1996, (in Japanese).

[318] R. D. Silverman, *Fast generation of random, strong RSA primes*, CryptoBytes **3** (1997), no. 1, 9–13.

[320] G. J. Simmons, *A 'weak' privacy protocol using the RSA cryptoalgorithm*, Cryptologia **7** (1983), no. 2, 180–182.

[340] T. Takagi and S. Naito, *The multi-variable modular polynomial and its applications to cryptography*, 7th International Symposium on Algorithm and Computation, Lecture Notes in Computer Science, vol. 1178, 1996, pp. 386–396.

[350] M. J. Wiener, *Cryptanalysis of short RSA secret exponents*, IEEE Transactions on Information Theory **IT-36** (1990), no. 3, 553–558.

[352] H. C. Williams, *A $p+1$ method of factoring*, Math. of Comp. **39** (1982), no. 159, 225–234.

CHAPTER 4

Summary and Conclusions

The following table summarizes the vulnerability of the RSA-type cryptosystems against a collection of attacks.

attacks	RSA 512	RSA 1024	LUC 512	LUC 1024	KMOV 512	KMOV 1024	Demytko 512	Demytko 1024
Håstad (1.1)								
# of messages	e	e	e	e	6	6	e^2	e^2
GCD (1.2)								
max. size of e (bits)	32	32	32	32	∞	∞	16	16
random padding (bits)								
for $e = 3$	56	113	56	113	–	–	6	12
for $e = 5$	20	40	20	40	*	*	*	*
Garbage-man (1.3)								
# access to the bin	1	1	1	1	1	1	1	1
Chosen-message (2.1)								
# of messages	1	1	1	1	1	1	1	1
Common modulus (2.3)								
applicable	yes	yes	yes	yes	yes	yes	yes	yes
Faulty encryption (2.3.2)								
susceptible	often	often	often	often	often	often	some-times	some-times
Wiener (3.1)								
max. size of d (bits)	128	256	128	256	128	256	64	128
Lenstra (3.2)								
applicable	yes	yes	yes	yes	yes	yes	yes	yes
Transient faults (3.3)								
susceptible	yes	yes	yes	yes	yes	yes	yes	yes

Table 4.1: Attacks against 512- and 1024-bit RSA-type systems

The security of all these systems is based on the difficulty of factoring the public modulus n. We can see that LUC presents no advantage comparatively to RSA. Moreover, since the computation of Lucas sequences is more expensive, there is practically no reason to use LUC instead of RSA for security purposes. For elliptic curve RSA, addition of points on elliptic curves consumes also more time than exponentiation. Table 4.1 shows that the security of KMOV is comparable to that of RSA, except against polynomial attacks for which KMOV is less resistant. It also shows that Demytko's system generally is more resistant. So, in my own opinion, original RSA system provides the best ratio between security and efficiency. Since the size of the secret prime factors for systems based on the factorization problem is independent of the underlying structure, devising a competitive RSA-type cryptosystem seems quite difficult. This does not mean that elliptic curve-based implementations must be discarded. Elliptic curves still present some advantages, especially for systems based on the discrete logarithm problem [**177, 240**]. It is believed (except in few cases [**230, 326**]) that computing of a discrete logarithm is harder over an elliptic curve than in a finite field of the same size.

Can we still trust RSA-type cryptosystems? The answer is yes. As we will see, there is always a practical and efficient countermeasure. A first weakness of these systems is their polynomial structure. This can enable an attacker to find some secret information. However, two polynomial relations are generally required to mount a successful attack. So there is already a lesson we can learn, sending related messages is dangerous. This also clearly shows a potential weakness of KMOV over the other systems; because with KMOV, the x- and y-coordinates of messages are already related as points on elliptic curves. This weakness has for example been exploited by Bleichenbacher to reduce the number of messages to 6 for a successful Håstad's attack (see p. 44).

The second type of attacks against RSA relies on its multiplicative nature. As shown before, non-homomorphic systems can also be subject to this kind of attacks. The remedy is simple, the attacker should never be able to obtain the raw decryption (or signature) of an arbitrary value. For example, users may be very careful about meaningless messages and have to really destroy them (see the Garbage-man-in-the-middle-attack, Subsection 1.3). Another lesson is that the use of the same cryptoalgorithm for encryption and signature is definitively not a good practice. It is better to have two pairs of public/secret keys, one for encryption and the other one for signature.

The last type of attacks is rather the domain of the mathematician or the cryptographer than the one of the protocol designer. So Wiener pointed out that, even if attractive, the use of short secret exponents is insecure (see Subsection 3.1). Therefore, the protocol designer has to pay much attention for the choice of good and bad parameters for the underpinning cryptoalgorithm that he makes use. He has also to be careful about the implementation (hardware and software) of protocols. In particular, good protocols must be faults resistant, or at least must provide for how to correctly react in the case of faults. The correctness verification cannot always be achieved by doing calculations twice. This must be done by another (proved) secure way (see for example Shamir's countermeasure against Lenstra's attack, § 3.2.3).

The previous discussion shows that no implementation of RSA-type based protocols can be considered fully secure unless all security issues are considered. However, we can be quite confident in these systems if they are carefully and properly used.

References

[177] N. Koblitz, *Elliptic curve cryptosystems*, Math. of Comp. **48** (1987), no. 177, 203–209.

[230] A. Menezes, T. Okamoto, and S. Vanstone, *Reducing elliptic curve logarithms to logarithms in a finite field*, IEEE Transactions on Information Theory **IT-39** (1993), 1639–1646.

[240] 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.

[326] N. Smart, *Elliptic curve discrete logarithms*, Posted in `sci.crypt.research`, 30 September 1997.

Bibliography

1. NBS FIPS 46, *Data Encryption Standard*, National Bureau of Standards, U.S. Department of Commerce, January 1977.
2. M. Abadi and R. Needham, *Prudent engineering practice for cryptographic protocols*, 1994 IEEE Symposium on Security and Privacy, IEEE Press, 1994, pp. 122–136.
3. H. Abelson and B. LaMacchia, *A simple variant of RSA based on* 2×2 *matrices*, Unpublished manuscript, July 1993.
4. L. M. Adleman and J. DeMarrais, *A subexponential algorithm for discrete logarithms over all finite fields*, Advances in Cryptology – Crypto '93 (D. R. Douglas, ed.), Lecture Notes in Computer Science, vol. 773, Springer-Verlag, 1994, pp. 147–158.
5. L. M. Adleman, J. DeMarrais, and M.-D. Huang, *A subexponential algorithm for discrete logarithms over the rational subgroup of the Jacobians of large genus hyperelliptic curves over finite fields*, Algorithmic Number Theory – ANTS-I (L. M. Adleman and M.-D. Huang, eds.), Lecture Notes in Computer Science, vol. 877, Springer-Verlag, 1994, pp. 28–40.
6. G. B. Agnew, T. Beth, R. C . Mullin, and S. A. Vanstone, *Arithmetic operations in* $GF(2^m)$, Journal of Cryptology **6** (1993), no. 1, 3–13.
7. G. B. Agnew, R. C. Mullin, I. M. Onyszchuk, and S. A. Vanstone, *An implementation for a fast public-key cryptosystem*, Journal of Cryptology **3** (1991), no. 2, 63–79.
8. A. V. Aho, J. E. Hopcroft, and J. D. Ullman, *The design and analysis of computer algorithms*, Addison-Wesley, 1974.
9. N. I. Akhiezer, *Elements of the theory of elliptic functions*, 2nd ed., Nauka, Moscow, 1970, (in Russian). Translations of Math. Monographs, vol. 79, American Mathematical Society, 1990.
10. W. Alexi, B. Chor, O. Goldreich, and C. P. Schnorr, *RSA and Rabin functions: certain parts are as hard as the whole*, SIAM Journal on Computing **17** (1988), no. 2, 194–209.
11. H. Aly and W. B. Müller, *Cryptosystems based on Dickson polynomials*, Presented at Pragocrypt '96, Prague, Czech Rep., 30 Sept-3 Oct. 1996.
12. R. J. Anderson, *Practical RSA trapdoor*, Electronics Letters **29** (1993), no. 11, 995.
13. ———, *Why cryptosystems fail*, 1st ACM Conference on Computer and Communications Security, ACM Press, 1993, pp. 215–227.
14. R. J. Anderson and M. Kuhn, *Tamper resistance – a cautionary note*, Proceedings of the Second USENIX Workshop on Electronic Commerce, USENIX Association, 1996, pp. 1–11.

15. R. J. Anderson and R. Needham, *Robustness principles for public key protocols*, Advances in Cryptology – Crypto '95 (D. Coppersmith, ed.), Lecture Notes in Computer Science, vol. 963, Springer-Verlag, 1995, pp. 236–247.
16. A. O. L. Atkin and F. Morain, *Elliptic curves and primality proving*, Math. of Comp. **61** (1993), no. 203, 29–68.
17. 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.
18. P. Barrett, *Communications authentication and security using public key encryption - A design for implementation*, Master's thesis, Oxford University, 1984.
19. ———, *Implementing the Rivest, Shamir and Adleman public key encryption algorithm on a standard digital signal processor*, Advances in Cryptology – Crypto '86 (A. M. Odlyzko, ed.), Lecture Notes in Computer Science, vol. 263, Springer-Verlag, 1987, pp. 311–323.
20. C. Batut, D. Bernardi, H. Cohen, and M. Olivier, *Users's guide to PARI-GP*, January 1995, Available via anonymous ftp at `megrez.math.u-bordeaux.fr`.
21. T. Becker and V. Weispfenning, *Gröbner bases*, Graduate Texts in Mathematics, vol. 141, Springer-Verlag, 1993.
22. M. Bellare and P. Rogaway, *Optimal asymmetric encryption*, Advances in Cryptology – Eurocrypt '94 (A. De Santis, ed.), Lecture Notes in Computer Science, vol. 950, Springer-Verlag, 1995, pp. 92–111.
23. ———, *The exact security of digital signatures – How to sign with RSA and Rabin*, Advances in Cryptology – Eurocrypt '96 (U. Maurer, ed.), Lecture Notes in Computer Science, vol. 1070, Springer-Verlag, 1996, pp. 399–416.
24. J. Benaloh and M. de Mare, *One-way accumulators: A decentralized alternative to digital signatures*, Advances in Cryptology – Eurocrypt '93 (T. Helleseth, ed.), Lecture Notes in Computer Science, vol. 765, Springer-Verlag, 1994, pp. 274–285.
25. S. Berkovits, *Factoring via superencryption*, Cryptologia **6** (1982), no. 3, 229–237.
26. T. Beth, M. Frish, and G. J. Simmons (eds.), *Public-key cryptography: State of the art and future directions*, Lecture Notes in Computer Science, vol. 578, Springer-Verlag, 1992.
27. T. Beth and F. Schaefer, *Non supersingular elliptic curves for public key cryptosystems*, Advances in Cryptology – Eurocrypt '91 (D. W. Davies, ed.), Lecture Notes in Computer Science, vol. 547, Springer-Verlag, 1991, pp. 316–327.
28. I. Biehl, J. Buchmann, and C. Thiel, *Cryptographic protocols based on discrete logarithms in real-quadratic orders*, Advances in Cryptology – Crypto '94 (Y. Desmedt, ed.), Lecture Notes in Computer Science, vol. 839, Springer-Verlag, 1994, pp. 56–60.
29. R. Bird, I. Gopal, A. Herzberg, P. Janson, S. Kutten, R. Molva, and M. Yung, *Systematic design of a family of attack-resistant protocols*, IEEE Journal on Selected Areas in Communication **11** (1993), no. 5, 679–693.
30. B. Blakey and G. R. Blakley, *Security of number theoretic public key cryptosystems against random attack I*, Cryptologia **2** (1978), no. 4, 305–321.
31. ———, *Security of number theoretic public key cryptosystems against random attack II*, Cryptologia **3** (1979), no. 1, 29–42.

32. ———, *Security of number theoretic public key cryptosystems against random attack III*, Cryptologia **3** (1979), no. 2, 105–118.
33. G. R. Blakey and I. Borosh, *Rivest-Shamir-Adleman public key cryptosystems do not always conceal messages*, Comp & Maths. with Appls. **5** (1979), 169–178.
34. D. Bleichenbacher, Personal communication.
35. ———, *Efficiency and security analysis of cryptosystems based on number theory*, Ph.D. thesis, Swiss Federal Institute of Technology Zürich, 1996.
36. ———, *On the security of the KMOV public key cryptosystem*, Advances in Cryptology – Crypto '97 (B. S. Kaliski Jr, ed.), Lecture Notes in Computer Science, vol. 1294, Springer-Verlag, 1997, pp. 235–248.
37. 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.
38. D. Bleichenbacher, M. Joye, and J.-J. Quisquater, *A new and optimal chosen-message attack on RSA-type cryptosystems*, Information and Communications Security (Y. Han, T. Okamoto, and S. Qing, eds.), Lecture Notes in Computer Science, vol. 1334, Springer-Verlag, 1997, pp. 302–313.
39. M. Blum and S. Goldwasser, *An efficient probabilistic public key encryption which hides all partial information*, Advances in Cryptology – Crypto '84 (G. R. Blakley and D. Chaum, eds.), Lecture Notes in Computer Science, vol. 196, Springer-Verlag, 1986, pp. 289–299.
40. 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.
41. D. Boneh, A. Shamir, and S. Vanstone, *Fault attacks on RSA and ElGamal moduli*, Unpublished manuscript, 1997.
42. F. Borceux, *Invitation à la géométrie*, Ciaco, Louvain-la-Neuve, 1986.
43. F. Borceux and J.-J. Quisquater, *Number theory and cryptology*, To appear.
44. W. Bosma, *Primality testing using elliptic curves*, Tech. Report 85-12, Mathematisch Instituut, Universiteit van Amsterdam, July 1985.
45. C. Boyd and W. Mao, *On a limitation of BAN logic*, Advances in Cryptology – Eurocrypt '93 (T. Helleseth, ed.), Lecture Notes in Computer Science, vol. 765, Springer-Verlag, 1994, pp. 240–247.
46. H. Brandstrom, *A public-key cryptosystem based upon equations over a finite field*, Cryptologia **7** (1983), no. 4, 347–358.
47. G. Brassard, *Modern cryptology: A tutorial*, Lecture Notes in Computer Science, vol. 325, Springer-Verlag, 1988.
48. D. M. Bressoud, *Factorization and primality testing*, Undergraduate Texts in Mathematics, Springer-Verlag, 1989.
49. E. F. Brickell and K. S. McCurley, *An interactive identification scheme based on discrete logarithms and factoring*, Journal of Cryptology **5** (1992), no. 1, 29–39.
50. E. F. Brickell and A. M. Odlyzko, *Cryptanalysis: A survey of recent results*, Contemporary Cryptology (G. Simmons, ed.), IEEE Press, 1992, pp. 541–558.
51. M. Burmester and Y. Desmedt, *Remarks on soundness of proofs*, Electronics Letters **25** (1989), no. 22, 1509–1511.
52. M. Burrows, M. Abadi, and R. Needham, *A logic of authentication*, ACM Trans. on Computer Systems **8** (1990), no. 1, 18–36.

53. D. Cantor, *On the analogue of the division polynomials for hyperelliptic curves*, J. reine angew. Math. **447** (1994), 91–145.
54. R. D. Carmichael, *Introduction to the theory of groups of finite order*, Dover Publications, Inc., 1956.
55. J. W. S. Cassels, *An introduction to the geometry of numbers*, Grundlehren der mathematischen Wissenschaften, vol. 99, Springer-Verlag, 1959.
56. ———, *Diophantine equations with special references to elliptic curves*, J. of the London Math. Soc. **41** (1966), 193–291.
57. ———, *Lectures on elliptic curves*, London Mathematical Society Students Texts, vol. 24, Cambridge University Press, 1991.
58. L. S. Charlap and R. Coley, *An elementary introduction to elliptic curves II*, CRD Expository Report No. 34, Institute for Defense Analysis, Princeton, July 1990.
59. 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.
60. D. Chaum, *Blind signatures for untraceable payments*, Advances in Cryptology – Crypto 82 (D. Chaum, R. L. Rivest, and A. T. Sherman, eds.), Plenum Press, 1983, pp. 199–203.
61. ———, *Blinding for unanticipated signatures*, Advances in Cryptology – Eurocrypt '87 (D. Chaum and W. L. Lynch, eds.), Lecture Notes in Computer Science, vol. 304, Springer-Verlag, 1988, pp. 227–233.
62. M. Chen and E. Hughes, *Protocol failures related to order of encryption and signature: computation of discrete logarithms in RSA groups*, Draft for P1363 standard, April 1997.
63. B. Chor and O. Goldreich, *RSA/Rabin least significant bits are* $\frac{1}{2}+\frac{1}{poly(\log N)}$ *secure*, Advances in Cryptology – Crypto '84 (G. R. Blakley and D. Chaum, eds.), Lecture Notes in Computer Science, vol. 196, Springer-Verlag, 1986, pp. 303–313.
64. S.-K. Chua and S. Ling, *A Rabin-type scheme on* $y^2 \equiv x^3 + bx^2 \bmod n$, Third Annual International Computing and Combinatorics Conference (COCOON '97) (T. Jiang and D. T. Lee, eds.), Lecture Notes in Computer Science, vol. 1276, Springer-Verlag, To appear.
65. C. C. Chuang and J. G. Dunham, *Matrix extensions of the RSA algorithm*, Advances in Cryptology – Crypto '90 (A. J. Menezes and S. A. Vanstone, eds.), Lecture Notes in Computer Science, vol. 537, Springer-Verlag, 1991, pp. 140–155.
66. D. V. Chudnovsky and G. V. Chudnovsky, *Sequences of numbers generated by addition in formal groups and new primality and factorization tests*, Research Report RC 11262 (#50739), IBM Thomas J. Watson Research Center, November 1985.
67. H. Cohen, *A course in computational algebraic number theory*, Graduate Texts in Mathematics, vol. 138, Springer-Verlag, 1993.
68. D. Coppersmith, *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.

69. ———, *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.
70. ———, *Small solutions to polynomials equations, and low exponent RSA vulnerabilities*, Journal of Cryptology **10** (1997), no. 4, 233–260.
71. 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.
72. D. Coppersmith, J. Stern, and S. Vaudenay, *The security of the birational permutation signature schemes*, Journal of Cryptology **10** (1997), no. 3, 207–221.
73. T. H. Cormen, C. E. Leiserson, and R. L. Rivest, *Introduction to algorithms*, MIT Press, 1990.
74. J.-M. Couveignes and F. Morain, *Théorie algorithmique des nombres*, Notes de cours.
75. ———, *Schoof's algorithm and isogeny cycles*, Algorithmic Number Theory – ANTS-I (L. M. Adleman and M.-D. Huang, eds.), Lecture Notes in Computer Science, vol. 877, Springer-Verlag, 1994, pp. 43–58.
76. C. Couvreur and J.-J. Quisquater, *An introduction to fast generation of large prime numbers*, Philips J. Res. **37** (1982), no. 5/6, 231–264.
77. D. Cox, J. Little, and D. O'Shea, *Ideals, varieties and algorithms*, Undergraduate Texts in Mathematics, Springer-Verlag, 1992.
78. J. E. Cremona, *Algorithms for modular elliptic curves*, Cambridge University Press, 1992.
79. I. B. Damgård, *Collision free hash functions and public key signatures schemes*, Advances in Cryptology – Eurocrypt '87 (D. Chaum and W. L. Lynch, eds.), Lecture Notes in Computer Science, vol. 304, Springer-Verlag, 1988, pp. 203–216.
80. ———, *Towards practical public key systems secure against chosen ciphertext attacks*, Advances in Cryptology – Crypto '91 (J. Feigenbaum, ed.), Lecture Notes in Computer Science, vol. 576, Springer-Verlag, 1992, pp. 445–456.
81. I. B. Damgård and P. Landrock, *The RSA system and its theoretical background*, Unpublished manuscript, October 1996.
82. H. Daudé, P. Flajolet, and B. Vallée, *An analysis of the Gaussian algorithm for lattice reduction*, Algorithmic Number Theory – ANTS-I (L. M. Adleman and M.-D. Huang, eds.), Lecture Notes in Computer Science, vol. 877, Springer-Verlag, 1994, pp. 144–158.
83. 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.
84. 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.
85. ———, *Some variations on RSA signatures & their security*, Advances in Cryptology – Crypto '86 (A. M. Odlyzko, ed.), Lecture Notes in Computer Science, vol. 263, Springer-Verlag, 1987, pp. 49–59.
86. J. M. DeLaurentis, *A further weakness in the common modulus protocol for the RSA cryptoalgorithm*, Cryptologia **8** (1984), no. 3, 253–259.

87. R. A. DeMillo, N. A. Lynch, and M. J. Merritt, *Cryptographic protocols*, Proc. SIGACT Conf., 1982.
88. 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.
89. 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.
90. D. E. Denning, *Digital signatures with RSA and other public-key cryptosystems*, Communications of the ACM **27** (1984), no. 4, 388–392.
91. T. Denny, B. Dodson, A. K. Lenstra, and M. S. Manasse, *On the factorization of RSA-120*, Advances in Cryptology – Crypto '93 (D. R. Douglas, ed.), Lecture Notes in Computer Science, vol. 773, Springer-Verlag, 1994, pp. 166–174.
92. M. A. F. Derôme, *Generating RSA keys without the Euclid algorithm*, Electronics Letters **29** (1993), no. 1, 19–21.
93. 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.
94. Y. Desmedt and J.-J. Quisquater, *Public-key systems based on the difficulty of tmapering (Is there a difference between DES and RSA?)*, Advances in Cryptology – Crypto '86 (A. M. Odlyzko, ed.), Lecture Notes in Computer Science, vol. 263, Springer-Verlag, 1987, pp. 111–117.
95. D. de Waleffe and J.-J. Quisquater, *CORSAIR: a smart card for public key cryptosystems*, Advances in Cryptology – Crypto '90 (A. J. Menezes and S. A. Vanstone, eds.), Lecture Notes in Computer Science, vol. 537, Springer-Verlag, 1991, pp. 502–513.
96. L. E. Dickson, *The analytic representation of substitutions on a power of a prime number of letters with a discussion of the linear group*, Annals of Mathematics **11** (1896/97), 65–120,161–183.
97. W. Diffie and M. E. Hellman, *New directions in cryptography*, IEEE Transactions on Information Theory **IT-26** (1976), no. 6, 644–654.
98. A. Di Porto, *A note on the Dickson public-key cryptosystem*, La Comunicazione (Note Recensioni Notizie) **43** (1994), 59–62.
99. A. Di Porto and P. Filipponi, *A probabilistic test based on the properties of certain generalized Lucas numbers*, Advances in Cryptology – Eurocrypt '88 (C. G. Günther, ed.), Lecture Notes in Computer Science, vol. 330, Springer-Verlag, 1988, pp. 211–223.
100. 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.
101. ———, *A subexponential-time algorithm for computing discrete logarithms over* GF(p^2), IEEE Transactions on Information Theory **IT-31** (1985), no. 4, 473–481.
102. S. Even, O. Goldreich, and A. Shamir, *On the security of ping-pong protocols when implemented using the RSA*, Advances in Cryptology – Crypto '85 (H. C. Williams, ed.), Lecture Notes in Computer Science, vol. 218, Springer-Verlag, 1986, pp. 58–72.

103. J.-H. Evertse and E. van Heyst, *Which new RSA signatures can be computed from some given RSA signatures?*, Advances in Cryptology – Eurocrypt '90 (I. B. Damgård, ed.), Lecture Notes in Computer Science, vol. 473, Springer-Verlag, 1991, pp. 83–97.
104. ———, *Which new RSA-signatures can be computed from certain given RSA-signatures*, Journal of Cryptology **5** (1992), no. 1, 41–52.
105. C.-I. Fan and C.-L. Lei, *Efficient blind signature scheme based on quadratic residues*, Electronics Letters **32** (1996), no. 9, 811–813.
106. H. Fell and W. Diffie, *Analysis of public-key approach based on polynomial substitution*, Advances in Cryptology – Crypto '85 (H. C. Williams, ed.), Lecture Notes in Computer Science, vol. 218, Springer-Verlag, 1986, pp. 340–349.
107. A. Fiat, *Batch RSA*, Journal of Cryptology **10** (1997), no. 2, 75–88.
108. M. K. Franklin and M. K. Reiter, *A linear protocol failure for RSA with exponent three*, Preliminary note for Crypto '95 rump session.
109. ———, *Verifiable signature sharing*, Advances in Cryptology – Eurocrypt '95 (L. C. Guillou and J.-J. Quisquater, eds.), Lecture Notes in Computer Science, no. 921, Springer-Verlag, 1995, pp. 50–63.
110. A. M. Frieze, J. Håstad, R. Kannan, J. C. Lagarias, and A. Shamir, *Reconstructing truncated integer variables satisfying linear congruences*, SIAM Journal on Computing **17** (1988), no. 2, 262–280.
111. W. Fulton, *Algebraic curves*, W. A. Benjamin, Inc., 1969.
112. M. J. Ganley, *Note on the generation of p_0 for RSA keysets*, Electronics Letters **26** (1990), no. 6, 369.
113. H. Gilbert, D. Gupta, A. M. Odlyzko, and J.-J. Quisquater, *Attacks on Shamir's 'RSA for paranoids'*, Preprint.
114. A. Gillet, *Fragilisation du cryptosystème RSA en présence de fautes*, Master's thesis, Université catholique de Louvain, June 1997.
115. A. Gillet, M. Joye, and J.-J. Quisquater, *Cautionary note for protocols designers: Security proof is not enough*, Proc. of the DIMACS Workshop on Design and Formal Verification of Security Protocols (H. Orman and C. Meadows, eds.), (CDROM), 1997.
116. M. Girault, *Hash-functions using modulo-N operations*, Advances in Cryptology – Eurocrypt '87 (D. Chaum and W. L. Lynch, eds.), Lecture Notes in Computer Science, vol. 304, Springer-Verlag, 1988, pp. 217–226.
117. ———, *An identity-based identification scheme based on discrete logarithms modulo a composite number*, Advances in Cryptology – Eurocrypt '90 (I. B. Damgård, ed.), Lecture Notes in Computer Science, vol. 473, Springer-Verlag, 1991, pp. 481–486.
118. M. Girault and J.-F. Misarsky, *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.
119. M. Girault, P. Toffin, and B. Vallée, *Computation of approximate l-th root modulo n and application to cryptography*, Advances in Cryptology – Crypto '88 (S. Goldwasser, ed.), Lecture Notes in Computer Science, vol. 403, Springer-Verlag, 1990, pp. 100–117.
120. V. Gligor, R. Kailar, S. Stubblebine, and L. Gong, *Logics for cryptographic protocols – virtues and limitations*, Computer Security Fondations Workshop IV, IEEE Press, 1991, pp. 219–226.

121. R. Godement, *Cours d'algèbre*, 3rd ed., Hermann, 1966.
122. S. Goldwasser and S. Micali, *Probabilistic encryption*, Journal of Computer and Systems Science **28** (1984), no. 2, 270–299.
123. S. Goldwasser, S. Micali, and R. L. Rivest, *A digital signature scheme secure against adaptative chosen-message attacks*, SIAM Journal on Computing **17** (1988), no. 2, 281–307.
124. Li Gong and D. J. Wheeler, *A matrix key-distribution scheme*, Journal of Cryptology **2** (1990), no. 1, 51–59.
125. D. M. Gordon, *On the number of elliptic pseudoprimes*, Math. of Comp. **52** (1989), no. 185, 231–245.
126. ———, *Discrete logarithms in* GF(p) *using the number field sieve*, SIAM J. Discr. Math. **6** (1993), no. 1, 124–138.
127. J. Gordon, *Strong RSA keys*, Electronics Letters **20** (1984), no. 12, 514–516.
128. ———, *How to forge RSA keys certificates*, Electronics Letters **21** (1985), no. 9, 377–379.
129. ———, *Strong primes are easy to find*, Advances in Cryptology – Eurocrypt '84 (T. Beth, N. Cot, and I. Ingemarsson, eds.), Lecture Notes in Computer Science, vol. 209, Springer-Verlag, 1986, pp. 216–223.
130. R. Graham, D. Knuth, and O. Patashnik, *Concrete mathematics*, 2nd ed., Addison-Wesley, 1994.
131. J. Grantham, *Frobenius pseudoprimes*, Preprint, May 1996.
132. J. Guajardo and C. Paar, *Efficient algorithms for elliptic curve cryptosystems*, Advances in Cryptology – Crypto '97 (B. S. Kaliski Jr, ed.), Lecture Notes in Computer Science, vol. 1294, Springer-Verlag, 1997, pp. 342–356.
133. L. C. Guillou and J.-J. Quisquater, *Efficient public-key signatures with shadow*, Advances in Cryptology – Crypto '87 (C. Pomerance, ed.), Lecture Notes in Computer Science, vol. 293, Springer-Verlag, 1988, p. 283.
134. ———, *A practical zero-knowledge protocol fitted to security processor minimizing both transmission and memory*, Advances in Cryptology – Eurocrypt '88 (C. G. Günther, ed.), Lecture Notes in Computer Science, vol. 330, Springer-Verlag, 1988, pp. 123–128.
135. ———, *A "paradoxical" identity-based signature scheme resulting from zero-knowledge*, Advances in Cryptology – Crypto '88 (S. Goldwasser, ed.), Lecture Notes in Computer Science, vol. 403, Springer-Verlag, 1990, pp. 216–231.
136. L. C. Guillou, J.-J. Quisquater, M. Walker, P. Landrock, and C. Shaer, *Precautions taken against various potential attacks in ISO/IEC DIS9796*, Advances in Cryptology – Eurocrypt '90 (I. B. Damgård, ed.), Lecture Notes in Computer Science, vol. 473, Springer-Verlag, 1991, pp. 465–473.
137. G. H. Hardy and E. M. Wright, *An introduction to the theory of numbers*, 5th ed., Oxford University Press, 1979.
138. L. Harn, *Public-key cryptosystem design based on factoring and discrete logarithms*, IEE Proc.-Comput. Digit. Tech. **141** (1994), no. 3, 193–195.
139. 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.
140. ———, *Solving simultaneous modular equations of low degree*, SIAM Journal on Computing **17** (1988), no. 2, 336–341.

141. T. Herlestam, *Critical remarks on some public-key cryptosystems*, BIT **17** (1978), 493–496.
142. P. Horster, M. Michels, and H. Petersen, *Digital signature schemes based on Lucas functions*, Proc. of Communication and Multimedia Security, Chapman & Hall, 1995, pp. 178–190.
143. K. Huber, *Some considerations concerning the selection of RSA moduli*, Advances in Cryptology – Eurocrypt '91 (D. W. Davies, ed.), Lecture Notes in Computer Science, vol. 547, Springer-Verlag, 1991, pp. 294–301.
144. L. C. K. Hui and K.-Y. Lam, *Fast square-and-multiply exponentiation for RSA*, Electronics Letters **30** (1994), no. 17, 1396–1397.
145. D. Husemöller, *Elliptic curves*, Graduate Texts in Mathematics, vol. 111, Springer-Verlag, 1987.
146. S.-J. Hwang, C.-C. Chang, and W.-P. Yang, *Some active attacks on fast server-aided secret computation protocols for modular exponentiation*, Cryptography: Policy and algorithms (E. Dawson and J. Golić, eds.), Lecture Notes in Computer Science, vol. 1029, Springer-Verlag, 1996, pp. 215–227.
147. K. Ireland and M. Rosen, *A classical introduction to modern number theory*, Graduate Texts in Mathematics, vol. 84, Springer-Verlag, 1982.
148. W. E. Jenner, *Rudiments of algebraic geometry*, Oxford University Press, 1963.
149. A. Joux, *La réduction des réseaux en cryptographie*, Ph.D. thesis, École Polytechnique, April 1993.
150. A. Joux and J. Stern, *Lattice reduction: a toolbox for the cryptanalyst*, Submitted to Journal of Cryptology.
151. M. Joye, *Arithmétique algorithmique : application au crypto-système à clé publique RSA*, Master's thesis, Université catholique de Louvain, 1994.
152. ———, *Introduction à la théorie des courbes elliptiques*, Mémoire de DEA en mathématiques, Université catholique de Louvain, June 1995.
153. ———, *Common modulus attack against Lucas-based systems*, Tech. Report CG-1996/10, UCL Crypto Group, Louvain-la-Neuve, December 1996.
154. M. Joye, F. Koeune, and J.-J. Quisquater, *Further results on Chinese remaindering*, Tech. Report CG-1997/1, UCL Crypto Group, Louvain-la-Neuve, January 1997, Presented at the rump session of Eurocrypt '97.
155. ———, *Takagi/Naito's algorithm revisited*, Tech. Report CG-1997/3, UCL Crypto Group, Louvain-la-Neuve, March 1997.
156. M. Joye, A. K. Lenstra, and J.-J. Quisquater, *Chinese remaindering in the presence of faults*, Submitted to Journal of Cryptology.
157. M. Joye and J.-J. Quisquater, *Cryptanalysis of RSA-type cryptosystems: A visit*, Presented at the DIMACS Workshop on Network Threats, New-York, USA., 4-6th December 1996. To appear in a volume of the American Mathematical Society.
158. ———, *Reducing the elliptic curve cryptosystem of Meyer-Müller to the cryptosystem of Rabin-Williams*, Presented to the rump session of Eurocrypt '96, Zaragoza, Spain, 12-16th May 1996. To appear in Designs, Codes and Cryptography.
159. ———, *Efficient computation of full Lucas sequences*, Electronics Letters **32** (1996), no. 6, 537–538.
160. ———, *Note on the preliminary version of the Meyer-Müller cryptosystem*, Tech. Report CG-1996/2, UCL Crypto Group, Louvain-la-Neuve, January 1996.

161. ______, *Cryptosystem of Chua and Ling*, Electronics Letters **33** (1997), no. 23, 1938.
162. ______, *Faulty RSA-type encryption*, Tech. Report CG-1997/8, UCL Crypto Group, Louvain-la-Neuve, July 1997.
163. ______, *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.
164. ______, *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.
165. M. Joye, J.-J. Quisquater, F. Bao, and R. H. Deng, *RSA-type signatures in the presence of transient faults*, To appear in the proceedings of the *Sixth IMA International Conference on Cryptography and Coding*, Cirencester, U.K., 17-19th December 1997.
166. A. Jurišić and A. J. Menezes, *Elliptic curves and cryptography*, Dr. Dobb's Journal (1997), no. 4, 26–36.
167. B. S. Kaliski Jr, *A pseudo-random bit generator based on elliptic logarithms*, Advances in Cryptology – Crypto '86 (A. M. Odlyzko, ed.), Lecture Notes in Computer Science, vol. 263, Springer-Verlag, 1987, pp. 84–103.
168. ______, *Elliptic curves and cryptography: A pseudorandom bit generator and other tools*, Ph.D. thesis, Massachusetts Institute of Technology, 1988.
169. ______, *One-way permutations on elliptic curves*, Journal of Cryptology **3** (1991), no. 3, 187–199.
170. ______, *Anderson's RSA trapdoor can be broken*, Electronics Letters **29** (1993), no. 15, 1387–1388.
171. ______, *A chosen message attack on Demytko's elliptic curve cryptosystem*, Journal of Cryptology **10** (1997), no. 1, 71–72.
172. B. S. Kaliski Jr and M. Robshaw, *The secure use of RSA*, CryptoBytes **1** (1995), no. 3, 7–12.
173. R. Kemmerer, C. Meadows, and J. Millen, *Three systems for cryptographic protocol analysis*, Journal of Cryptology **7** (1994), no. 2, 79–130.
174. A. Knapp, *Elliptic curves*, Mathematical Notes, vol. 40, Princeton University Press, 1992.
175. D. E. Knuth, *The art of computer programming: Volume 2/seminumerical algorithms*, 2nd ed., Addison-Wesley, 1981.
176. N. Koblitz, *Introduction to elliptic curves and modular forms*, Graduate Texts in Mathematics, vol. 97, Springer-Verlag, 1984.
177. ______, *Elliptic curve cryptosystems*, Math. of Comp. **48** (1987), no. 177, 203–209.
178. ______, *Primality of the number of points on an elliptic curve over a finite field*, Pacific J. Math **131** (1988), no. 1, 157–165.
179. ______, *Hyperelliptic cryptosystems*, Journal of Cryptology **1** (1989), no. 3, 139–150.
180. ______, *Elliptic curve implementation of zero-knowledge blobs*, Journal of Cryptology **4** (1991), no. 3, 207–213.
181. ______, *CM-curves with good cryptographic protocols*, Advances in Cryptology – Crypto '91 (J. Feigenbaum, ed.), Lecture Notes in Computer Science, vol. 576, Springer-Verlag, 1992, pp. 279–287.

182. ______, *A course in number theory and cryptography*, 2nd ed., Graduate Texts in Mathematics, vol. 114, Springer-Verlag, 1994.

183. P. C. Kocher, *Timing attacks on implementations of Diffie-Hellman, RSA, DSS, and other systems*, Advances in Cryptology – Crypto '96 (N. Koblitz, ed.), Lecture Notes in Computer Science, vol. 1109, Springer-Verlag, 1996, pp. 104–113.

184. D. Kohel, *Endomorphism rings of elliptic curves over finite fields*, Ph.D. thesis, University of California, Berkeley, 1996.

185. A. G. Konheim, *Cryptography: A primer*, John Wiley & Sons, 1981.

186. K. Koyama, *Fast RSA-type schemes based on singular cubic curves* $y^2 + axy \equiv x^3 \pmod{n}$, Advances in Cryptology – Eurocrypt '95 (L. C. Guillou and J.-J. Quisquater, eds.), Lecture Notes in Computer Science, no. 921, Springer-Verlag, 1995, pp. 329–340.

187. 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, 1992, pp. 252–266.

188. K. Koyama and Y. Tsuruoka, *Speeding up elliptic cryptosystems by using a signed binary window method*, Advances in Cryptology – Crypto '92 (E. F. Brickell, ed.), Lecture Notes in Computer Science, vol. 740, Springer-Verlag, 1993, pp. 345–358.

189. E. Kranakis, *Primality and cryptography*, John Wiley & Sons, 1986.

190. 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.

191. H. Kuwakado and K. Koyama, *Efficient cryptosystems over elliptic curves based on a product of form-free primes*, IEICE Trans. Fundamentals **E77-A** (1994), no. 8, 1309–1318.

192. ______, *Security of RSA-type cryptosystems over elliptic curves against Håstad attack*, Electronics Letters **30** (1994), no. 22, 1843–1844.

193. ______, *A uniquely decipherable Rabin-type scheme over elliptic curves*, Tech. Report ISEC95-33, IEICE, December 1995, (in Japanese).

194. C.-S. Laih and W.-C. Kuo, *Cryptanalysis of the enhanced ElGamal's signature scheme*, Cryptography: Policy and algorithms (E. Dawson and J. Golić, eds.), Lecture Notes in Computer Science, vol. 1029, Springer-Verlag, 1996, pp. 228–231.

195. C.-S. Laih, F.-K. Tu, and W.-C. Tai, *Remarks on LUC public key system*, Electronics Letters **30** (1994), no. 2, 123–124.

196. ______, *On the security of the Lucas functions*, Informations Processing Letters **53** (1995), 243–247.

197. C.-S. Laih, W.-C. Yang, and C.-H. Chen, *Efficient method for generating strong primes with constraint of bit length*, Electronics Letters **27** (1991), no. 20, 1807–1808.

198. K.-Y. Lam, S. Ling, and L. C.-K. Hui, *Efficient generation of elliptic cryptosystems*, Computing and Combinatorics (COCOON '96) (J.-Y. Hai and C. K. Wong, eds.), Lecture Notes in Computer Science, vol. 1090, Springer-Verlag, 1996, pp. 411–416.

199. S. Lang, *Elliptic functions*, Addison-Wesley, 1973.

200. ______, *Structures algébriques*, InterEditions, Paris, 1976.
201. ______, *Elliptic curves: Diophantine analysis*, Grundlehren der mathematischen Wissenschaften, vol. 231, Springer-Verlag, 1978.
202. ______, *Algebraic number theory*, 2nd ed., Graduate Texts in Mathematics, vol. 110, Springer-Verlag, 1994.
203. G.-J. Lay and H. G. Zimmer, *Constructing elliptic curves with given group order over large finite fields*, Algorithmic Number Theory – ANTS-I (L. M. Adleman and M.-D. Huang, eds.), Lecture Notes in Computer Science, vol. 877, Springer-Verlag, 1994, pp. 250–263.
204. F. Lehmann, M. Maurer, V. Müller, and V. Shoup, *Counting the number of points on elliptic curves over finite fields of characteristic greater than three*, Algorithmic Number Theory – ANTS-I (L. M. Adleman and M.-D. Huang, eds.), Lecture Notes in Computer Science, vol. 877, Springer-Verlag, 1994, pp. 60–70.
205. A. K. Lenstra, *Memo on RSA signature generation in the presence of faults*, September 1996.
206. A. K. Lenstra, H. W. Lenstra Jr, and L. Lovász, *Factoring polynomials with integer coefficients*, Mathematische Annalen **261** (1982), 513–534.
207. A. K. Lenstra and M. S. Manasse, *Factoring with two large primes*, Advances in Cryptology – Eurocrypt '90 (I. B. Damgård, ed.), Lecture Notes in Computer Science, vol. 473, Springer-Verlag, 1991, pp. 72–82.
208. ______, *Factoring with two primes*, Math. of Comp. **63** (1994), no. 208, 785–798.
209. H. W. Lenstra Jr, *Factoring integers with elliptic curves*, Annals of Mathematics **126** (1987), 649–673.
210. R. Lercier, *Reducing the cost of exponentiation in the $P-1$ type factorization algorithms*, Unpublished manuscript, January 1995.
211. ______, *Algorithmique des courbes elliptiques dans les corps finis*, Ph.D. thesis, École Polytechnique, May 1997.
212. ______, *Finding good random elliptic curves for cryptosystems defined over $\mathbb{F}_{2^n}$*, Advances in Cryptology – Eurocrypt '97 (W. Fumy, ed.), Lecture Notes in Computer Science, vol. 1233, Springer-Verlag, 1997, pp. 379–392.
213. R. Lercier and F. Morain, *Counting the number of points on elliptic curves over finite fields: strategies and performances*, Advances in Cryptology – Eurocrypt '95 (L. C. Guillou and J.-J. Quisquater, eds.), Lecture Notes in Computer Science, no. 921, Springer-Verlag, 1995, pp. 79–94.
214. R. Lidl, G. L. Mullen, and G. Turnwald, *Dickson polynomials*, Longman Scientific & Technical, 1993.
215. R. Lidl and W. B. Müller, *Permutation polynomials in RSA-cryptosystems*, Advances in Cryptology – Crypto '83, Plenum Press, 1984, pp. 293–301.
216. R. Lidl and H. Niederreiter, *Finite fields*, Encyclopedia of Mathematics and its Applications, vol. 20, Addison-Wesley, 1983.
217. ______, *Introduction to finite fields and their applications*, 2nd ed., Cambridge University Press, 1994.
218. C. H. Lim and P. J. Lee, *Another method for attaining security against adaptively chosen ciphertext attacks*, Advances in Cryptology – Crypto '93 (D. R. Douglas, ed.), Lecture Notes in Computer Science, vol. 773, Springer-Verlag, 1994, pp. 420–434.
219. J. H. Loxton (ed.), *Number theory and cryptography*, London Mathematical Society Lecture Note Series, vol. 154, Cambridge University Press, 1990.

220. J. H. Loxton, D. S. P. Khoo, G. J. Bird, and J. Seberry, *A cubic RSA code equivalent to factorization*, Journal of Cryptology **5** (1992), no. 2, 139–150.
221. A. Magnus, Personal communication.
222. T. Matsumoto and H. Imai, *Public quadratic polynomial-tuples for efficient signature-verification and message-encryption*, Advances in Cryptology – Eurocrypt '88 (C. G. Günther, ed.), Lecture Notes in Computer Science, vol. 330, Springer-Verlag, 1988, pp. 419–453.
223. U. M. Maurer, *Fast generation of secure RSA-moduli with almost maximal diversity*, Advances in Cryptology – Eurocrypt '89 (J.-J. Quisquater and J. Vandewalle, eds.), Lecture Notes in Computer Science, vol. 434, Springer-Verlag, 1990, pp. 636–647.
224. ———, *Fast generation of prime numbers and secure public-key cryptographic parameters*, Journal of Cryptology **8** (1995), no. 3, 123–155.
225. U. M. Maurer and Y. Yacobi, *A non-interactive public-key distribution system*, To appear in Designs, Codes and Cryptography.
226. K. S. McCurley, *A key distribution scheme equivalent to factoring*, Journal of Cryptology **1** (1988), no. 2, 95–105.
227. R. J. McEliece, *Finite fields for computer scientists and engineers*, Kluwer international series in engineering and computer science, no. 23, Kluwer Academic Publishers, 1987.
228. C. Meadows, *A system for the specification and verification of key management protocols*, 1991 IEEE Symposium on Security and Privacy, IEEE Press, 1991, pp. 182–195.
229. W. Meier and O. Staffelbach, *Efficient multiplication on certain nonsupersingular elliptic curves*, Advances in Cryptology – Crypto '92 (E. F. Brickell, ed.), Lecture Notes in Computer Science, vol. 740, Springer-Verlag, 1993, pp. 333–344.
230. A. Menezes, T. Okamoto, and S. Vanstone, *Reducing elliptic curve logarithms to logarithms in a finite field*, IEEE Transactions on Information Theory **IT-39** (1993), 1639–1646.
231. A. J. Menezes, *Elliptic curve public key cryptosystems*, Kluwer Academic Publishers, 1993.
232. ———, *Elliptic curve cryptosystems*, CryptoBytes **1** (1995), no. 2, 1–4.
233. A. J. Menezes, I. Blake, X. Gao, R. Mullin, S. Vanstone, and T. Yaghoobian, *Applications of finite fields*, Kluwer Academic Publishers, 1993.
234. A. J. Menezes, P. C. van Oorschot, and S. A. Vanstone, *Handbook of applied cryptography*, CRC Press, 1997.
235. A. J. Menezes and S. A. Vanstone, *The implementation of elliptic curves*, Advances in Cryptology – Auscrypt '90 (J. Seberry and J. Pieprzyk, eds.), Lecture Notes in Computer Science, vol. 453, Springer-Verlag, 1990, pp. 2–13.
236. ———, *Elliptic curve cryptosystems and their implementation*, Journal of Cryptology **6** (1993), no. 4, 209–224.
237. A. J. Menezes, Y.-H. Wu, and R. J. Zuccherato, *An elementary introduction to hyperelliptic curves*, Tech. Report CORR 96-19, Dept of C&O, University of Waterloo, Ontario, Canada, November 1996.

238. B. Meyer and V. Müller, *A public key cryptosystem based on elliptic curves over $\mathbb{Z}/n\mathbb{Z}$ equivalent to factoring*, Advances in Cryptology – Eurocrypt '96 (U. Maurer, ed.), Lecture Notes in Computer Science, vol. 1070, Springer-Verlag, 1996, pp. 49–59.
239. M. Mignotte, *Mathématiques pour le calcul formel*, Presses Universitaires de France, 1989.
240. 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.
241. J.-F. Misarsky, *Analyse et programmation de méthodes permettant de forger des signatures RSA*, Mémoire de DEA, Université de Limoges, 1996.
242. ———, *A multiplicative attack using LLL algorithm on RSA signatures with redundancy*, Advances in Cryptology – Crypto '97 (B. S. Kaliski Jr, ed.), Lecture Notes in Computer Science, vol. 1294, Springer-Verlag, 1997, pp. 221–234.
243. A. Miyaji, *On ordinary elliptic curve cryptosystems*, Advances in Cryptology – Asiacrypt '91 (H. Imai, R. L. Rivest, and T. Matsumoto, eds.), Lecture Notes in Computer Science, vol. 739, Springer-Verlag, 1993, pp. 460–469.
244. P. L. Montgomery, *Evaluating recurrences of form $X_{m+n} = f(X_m, X_n, X_{m-n})$ via Lucas chains*, To appear in Fibonacci Quaterly.
245. ———, *Speeding the Pollard and elliptic curve methods of factorization*, Math. of Comp. **48** (1987), no. 177, 243–264.
246. J. H. Moore, *Protocol failures in cryptosystems*, Contemporary Cryptology (G. Simmons, ed.), IEEE Press, 1992, pp. 541–558.
247. F. Morain, *Courbes elliptiques et tests de primalité*, Ph.D. thesis, Université Claude Bernard - Lyon I, September 1990.
248. ———, *Building cyclic elliptic curves modulo large primes*, Advances in Cryptology – Eurocrypt '91 (D. W. Davies, ed.), Lecture Notes in Computer Science, vol. 547, Springer-Verlag, 1991, pp. 328–336.
249. F. Morain and J. Olivos, *Speeding up the computations on an elliptic curve using addition-substraction chains*, Theoretical Informatics and Applications, vol. 24, 1990, pp. 531–543.
250. C. J. Moreno, *Algebraic curves over finite fields*, Cambridge Tracts in Mathematics, vol. 97, Cambridge University Press, 1991.
251. W. B. Müller and R. Nöbauer, *Some remarks on public-key cryptosystems*, Sci. Math. Hungar **16** (1981), 71–76.
252. ———, *Cryptanalysis of the Dickson scheme*, Advances in Cryptology – Eurocrypt '85 (F. Pichler, ed.), Lecture Notes in Computer Science, vol. 219, Springer-Verlag, 1986, pp. 50–61.
253. W. B. Müller and A. Oswald, *Dickson pseudoprimes and primality testing*, Advances in Cryptology – Eurocrypt '91 (D. W. Davies, ed.), Lecture Notes in Computer Science, vol. 547, Springer-Verlag, 1991, pp. 512–516.
254. S. Murphy, *Remarks on the LUC public key system*, Electronics Letters **30** (1994), no. 7, 558–559.
255. D. Naccache, Personal communication.
256. J. Nechvatal, *Public key cryptography*, Contemporary Cryptology (G. Simmons, ed.), IEEE Press, 1992, pp. 541–558.
257. H. Niederreiter, *Factoring polynomials over finite fields using differential equations and normal bases*, Math. of Comp. **62** (1994), no. 206, 819–830.

258. ______, *New deterministic factorization algorithms for polynomials over finite fields*, Contemporary Mathematics **168** (1994), 251–268.

259. H. Niederreiter and R. Göttfert, *On a new factorization algorithm for polynomials over finite fields*, Math. of Comp. **64** (1995), no. 209, 347–353.

260. I. M. Niven and H. S. Zuckerman, *An introduction to the theory of numbers*, 4th ed., John Wiley & Sons, 1980.

261. K. Nyberg and R. A. Rueppel, *Weakness in some recent key agreement protocols*, Electronics Letters **30** (1994), no. 1, 26–27.

262. A. M. Odlyzko, *Discrete logarithms and their cryptographic significance*, Advances in Cryptology – Eurocrypt '84 (T. Beth, N. Cot, and I. Ingemarsson, eds.), Lecture Notes in Computer Science, vol. 209, Springer-Verlag, 1986, pp. 224–314.

263. ______, *The future of integer factorization*, CryptoBytes **1** (1995), no. 2, 5–12.

264. ______, *RSA for selfish paranoids*, Unpublished manuscript, May 1996.

265. R. W. K. Odoni, V. Varadharajan, and P. W. Sanders, *Public key distribution in matrix rings*, Electronics Letters **20** (1984), no. 9, 386–387.

266. T. Okamoto, A. Fujioka, and E. Fujisaki, *An efficient digital signature scheme based on an elliptic curve over the ring* $\mathbb{Z}_n$, Advances in Cryptology – Crypto '92 (E. F. Brickell, ed.), Lecture Notes in Computer Science, vol. 740, Springer-Verlag, 1993, pp. 54–65.

267. T. Okamoto and K. Sakurai, *Efficient algorithms for the construction of hyperelliptic cryptosystems*, Advances in Cryptology – Crypto '91 (J. Feigenbaum, ed.), Lecture Notes in Computer Science, vol. 576, Springer-Verlag, 1992, pp. 267–278.

268. H. Ong, C. P. Schnorr, and A. Shamir, *A fast signature scheme based on quadratic equations*, Proc. of the 16th Annual ACM Symposium on Theory of Computing, 1984, pp. 208–216.

269. T. Ono, *An introduction to algebraic number theory*, The University series in mathematics, Plenum Press, 1990.

270. H. Orup, E. Svendsen, and E. Andreasen, *VICTOR: an efficient RSA hardware implementation*, Advances in Cryptology – Eurocrypt '90 (I. B. Damgård, ed.), Lecture Notes in Computer Science, vol. 473, Springer-Verlag, 1991, pp. 245–252.

271. C. Park, K. Kurosawa, T. Okamoto, and S. Tsuji, *On key distribution and authentication in mobile radio networks*, Advances in Cryptology – Eurocrypt '93 (T. Helleseth, ed.), Lecture Notes in Computer Science, vol. 765, Springer-Verlag, 1994, pp. 461–465.

272. J. Patarin, *Cryptanalysis of the Matsumoto and Imai public scheme of Eurocrypt '88*, Advances in Cryptology – Crypto '95 (D. Coppersmith, ed.), Lecture Notes in Computer Science, vol. 963, Springer-Verlag, 1995, pp. 248–261.

273. ______, *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.

274. A. Pfister, *Quadratic forms with applications to algebraic geometry and topology*, London Mathematical Society Lecture Note Series, vol. 217, Cambridge University Press, 1995.

275. J. Pieprzyk, *On public-key cryptosystems built using polynomial rings*, Advances in Cryptology – Eurocrypt '85 (F. Pichler, ed.), Lecture Notes in Computer Science, vol. 219, Springer-Verlag, 1986, pp. 73–78.
276. R. G. E. Pinch, *Extending the Håstad attack to LUC*, Electronics Letters **31** (1995), no. 21, 1827–1828.
277. ______, *Extending the Wiener attack to RSA-type cryptosystems*, Electronics Letters **31** (1995), no. 20, 1736–1738.
278. J. M. Pollard, *Theorems on factorization and primality testing*, Proc. Cambridge Philos. Soc. **76** (1974), 521–528.
279. J. M. Pollard and C. P. Schnorr, *An efficient solution to the congruence* $x^2 + ky^2 = m \pmod{n}$, IEEE Transactions on Information Theory **IT-33** (1987), no. 5, 702–709.
280. C. Pomerance, J. L. Selfridge, and S. S. Wagstaff Jr, *The pseudoprimes to* $25{\cdot}10^9$, Math. of Comp. **35** (1980), no. 151, 1003–1026.
281. Minghua Qu and S.A. Vanstone, *Factorizations in the elementary Abelian p-group and their cryptographic significance*, Journal of Cryptology **7** (1994), no. 4, 201–212.
282. J.-J. Quisquater, *How to avoid a successful cryptanalysis of your random prime generator (abstract)*, Presented at the conference of cryptography, CIRM Luminy, France, September 1995.
283. J.-J. Quisquater and C. Couvreur, *Fast decipherment algorithm for RSA public-key cryptosystem*, Electronics Letters **18** (1982), no. 21, 905–907.
284. 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.
285. P. Ribenboim, *L'arithmétique des corps*, Collection Méthodes, Hermann, 1972.
286. ______, *The little book of big primes*, Springer-Verlag, 1991.
287. H. Riesel, *Prime numbers and computer methods for factorization*, 2nd ed., Progress in Mathematics, vol. 126, Birkhaüser, 1994.
288. R. L. Rivest, *Remarks on a proposed cryptanalytic attack on the M.I.T. public-key cryptosystem*, Cryptologia **2** (1978), no. 1, 62–65.
289. ______, *Critical remarks on "Critical remarks on some public-key cryptosystems" by T. Herlestam*, BIT **19** (1979), 274–275.
290. R. L. Rivest and A. Shamir, *How to expose an eavesdropper*, Communications of the ACM **27** (1984), no. 4, 393–395.
291. ______, *Efficient factoring based on partial information*, Advances in Cryptology – Eurocrypt '85 (F. Pichler, ed.), Lecture Notes in Computer Science, vol. 219, Springer-Verlag, 1986, pp. 31–34.
292. 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.
293. R. L. Rivest and R. D. Silverman, *Are 'strong' primes needed for RSA*, The 1997 RSA Laboratories Seminar Series, Seminars Proceedings, 1997.
294. D. J. R. Robinson, *A course in the theory of groups*, 2nd ed., Graduate Texts in Mathematics, vol. 80, Springer-Verlag, 1996.
295. K. H. Rosen, *Elementary number theory and its applications*, 3rd ed., Addison-Wesley, 1992.

296. H.-G. Rück, *A note on elliptic curves over finite fields*, Math. of Comp. **49** (1987), no. 179, 301–304.
297. A. Salomaa, *Public-key cryptography*, 2nd ed., Springer, 1996.
298. P. Samuel, *Théorie algébrique des nombres*, Collection Méthodes, Hermann, 1967.
299. R. Scheidler, J. A. Buchmann, and H. C. Williams, *Implementation of a key exchange protocol using real quadratic fields*, Advances in Cryptology – Eurocrypt '90 (I. B. Damgård, ed.), Lecture Notes in Computer Science, vol. 473, Springer-Verlag, 1991, pp. 98–109.
300. R. Scheidler, A. Stein, and H. C. Williams, *Key-exchange in real quadratic congruence function fields*, Designs, Codes and Cryptography **7** (1996), 153–174.
301. B. Schneier, *Applied cryptography: protocols, algorithms, and source code in C*, 2nd ed., John Wiley & Sons, 1996.
302. C. P. Schnorr, *Efficient signature generation by smart cards*, Journal of Cryptology **4** (1991), no. 3, 161–173.
303. ______, *Factoring integers and computing discrete logarithms via Diophantine approximation*, Advances in Cryptology – Eurocrypt '91 (D. W. Davies, ed.), Lecture Notes in Computer Science, vol. 547, Springer-Verlag, 1991, pp. 281–293.
304. C. P. Schnorr and W. Alexi, *RSA-bits are* $0.5+\varepsilon$ *secure*, Advances in Cryptology – Eurocrypt '84 (T. Beth, N. Cot, and I. Ingemarsson, eds.), Lecture Notes in Computer Science, vol. 209, Springer-Verlag, 1986, pp. 113–126.
305. C. P. Schnorr and M. Euchner, *Lattice basis reduction: Improved practical algorithms and solving subset sum problems*, Proc. of Fundamentals of Computation Theory (FCT '91) (L. Budach, ed.), Lecture Notes in Computer Science, vol. 529, Springer-Verlag, 1991, pp. 68–85.
306. R. Schoof, *Elliptic curves over finite fields and the computation of square roots mod* p, Math. of Comp. **44** (1985), no. 170, 483–494.
307. ______, *Counting points on elliptic curves over finite fields*, Preliminary version, March 1994.
308. F. Schwenk and J. Eisfeld, *Public key encryption and signature schemes based on polynomials over* $\mathbb{Z}_n$, Advances in Cryptology – Eurocrypt '96 (U. Maurer, ed.), Lecture Notes in Computer Science, vol. 1070, Springer-Verlag, 1996, pp. 60–71.
309. A. Shamir, *How to check modular exponentiation*, Presented at the rump session of Eurocrypt '97.
310. ______, *A fast signature scheme*, Tech. Report MIT/LCS/TM-107, MIT Lab. for Computer Science, Cambridge, Mass., July 1978.
311. ______, *How to share a secret*, Communications of the ACM **22** (1979), no. 11, 120–126.
312. ______, *Efficient signature schemes based on birational permutations*, Advances in Cryptology – Crypto '93 (D. R. Douglas, ed.), Lecture Notes in Computer Science, vol. 773, Springer-Verlag, 1994, pp. 1–12.
313. ______, *RSA for paranoids*, CryptoBytes **1** (1995), no. 3, 1–4.
314. H. Shimizu, *On the improvement of the Håstad bound*, Proc. of the 1996 IEICE Fall Conference, vol. A-162, 1996, (in Japanese).
315. H. Shizuya, T. Itoh, and K. Sakurai, *On the complexity of hyperelliptic discrete logarithm problem*, Advances in Cryptology – Eurocrypt '91 (D. W. Davies, ed.),

Lecture Notes in Computer Science, vol. 547, Springer-Verlag, 1991, pp. 337–351.

316. J. H. Silverman, *The arithmetic of elliptic curves*, Graduate Texts in Mathematics, vol. 106, Springer-Verlag, 1986.
317. J. H. Silverman and J. Tate, *Rational points on elliptic curves*, Undergraduate Texts in Mathematics, Springer-Verlag, 1992.
318. R. D. Silverman, *Fast generation of random, strong RSA primes*, CryptoBytes **3** (1997), no. 1, 9–13.
319. R. D. Silverman and S. S. Wagstaff Jr, *A practical analysis of the elliptic curve factoring algorithm*, Math. of Comp. **61** (1993), no. 203, 445–462.
320. G. J. Simmons, *A 'weak' privacy protocol using the RSA cryptoalgorithm*, Cryptologia **7** (1983), no. 2, 180–182.
321. ———, *A secure subliminal channel (?)*, Advances in Cryptology – Crypto '85 (H. C. Williams, ed.), Lecture Notes in Computer Science, vol. 218, Springer-Verlag, 1986, pp. 33–41.
322. G. J. Simmons (ed.), *Contemporary cryptology: The science of information integrity*, IEEE Press, 1992.
323. ———, *Cryptanalysis and protocol failure*, 1st ACM Conference on Computer and Communications Security, ACM Press, 1993, pp. 213–214.
324. ———, *Proof of soundness (integrity) of cryptographic protocols*, Journal of Cryptology **7** (1994), no. 2, 69–77.
325. G. J. Simmons and M. J. Norris, *Preliminary comment on the M.I.T. public-key cryptosystem*, Cryptologia **1** (1977), 406–414.
326. N. Smart, *Elliptic curve discrete logarithms*, Posted in `sci.crypt.research`, 30 September 1997.
327. 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.
328. P. Smith, *LUC public-key encryption*, Dr. Dobb's Journal (1993), no. 1, 44–49.
329. ———, *Cryptography without exponentiation*, Dr. Dobb's Journal (1994), no. 4, 26–30.
330. 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.
331. P. J. 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 and R. Safavi-Naini, eds.), Lecture Notes in Computer Science, vol. 917, Springer-Verlag, 1995, pp. 357–364.
332. J. A. Solinas, *An improved algorithm for arithmetic on a family of elliptic curves*, Advances in Cryptology – Crypto '97 (B. S. Kaliski Jr, ed.), Lecture Notes in Computer Science, vol. 1294, Springer-Verlag, 1997, pp. 357–371.
333. M. Stadler, J.-M. Piveteau, and J. Camenisch, *Fair blind signatures*, Advances in Cryptology – Eurocrypt '95 (L. C. Guillou and J.-J. Quisquater, eds.), Lecture Notes in Computer Science, no. 921, Springer-Verlag, 1995, pp. 209–219.
334. N. M. Stephens, *Lenstra's factorization method based on elliptic curves*, Advances in Cryptology – Crypto '85 (H. C. Williams, ed.), Lecture Notes in Computer Science, vol. 218, Springer-Verlag, 1986, pp. 409–416.

335. J. Stern and P. Toffin, *Cryptanalysis of a public-key cryptosystem based on approximations by rational numbers*, Advances in Cryptology – Eurocrypt '90 (I. B. Damgård, ed.), Lecture Notes in Computer Science, vol. 473, Springer-Verlag, 1991, pp. 313–317.
336. D. R. Stinson, *Cryptography: Theory and practice*, CRC Press, Inc., 1995.
337. J. Stiwell, *Elements of algebra*, Undergraduate Texts in Mathematics, Springer-Verlag, 1994.
338. P. Syverson, *Limitations on design principles for public key protocols*, 1996 IEEE Symposium on Security and Privacy, IEEE Press, 1996, pp. 62–72.
339. T. Takagi, *Fast RSA-type cryptosystems using n-adic expansion*, Advances in Cryptology – Crypto '97 (B. S. Kaliski Jr, ed.), Lecture Notes in Computer Science, vol. 1294, Springer-Verlag, 1997, pp. 372–384.
340. 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.
341. ———, *Extension of Rabin cryptosystem to Eisenstein and Gauss fields*, IEICE Trans. Fundamentals **E80-A** (1997), no. 4, 753–760.
342. P. C. van Oorschot, *A comparison of practical public key cryptosystems based on integer factorization and discrete logarithms*, Advances in Cryptology – Crypto '90 (A. J. Menezes and S. A. Vanstone, eds.), Lecture Notes in Computer Science, vol. 537, Springer-Verlag, 1991, pp. 576–581.
343. ———, *A comparison of practical public key cryptosystems based on integer factorization and discrete logarithms*, Contemporary Cryptology (G. Simmons, ed.), IEEE Press, 1992, pp. 289–322.
344. ———, *An alternate explanation of two BAN-logic "failures"*, Advances in Cryptology – Eurocrypt '93 (T. Helleseth, ed.), Lecture Notes in Computer Science, vol. 765, Springer-Verlag, 1994, pp. 443–447.
345. S. A. Vanstone and R. J. Zuccherato, *Elliptic curve cryptosystems using curves of smooth order over the ring $\mathbb{Z}_n$*, To appear in IEEE Transactions on Information Theory.
346. ———, *Short RSA keys and their generation*, Journal of Cryptology **8** (1995), no. 2, 101–114.
347. V. Varadharajan, *Trapdoor rings and their use in cryptography*, Advances in Cryptology – Crypto '85 (H. C. Williams, ed.), Lecture Notes in Computer Science, vol. 218, Springer-Verlag, 1986, pp. 369–395.
348. V. Varadharajan and R. Odoni, *Extension of RSA cryptosystems to marix rings*, Cryptologia **9** (1985), no. 2, 140–153.
349. R. J. Walker, *Algebraic curves*, Springer-Verlag, 1950.
350. M. J. Wiener, *Cryptanalysis of short RSA secret exponents*, IEEE Transactions on Information Theory **IT-36** (1990), no. 3, 553–558.
351. H. C. Williams, *A modification of the RSA public-key encryption procedure*, IEEE Transactions on Information Theory **IT-26** (1980), no. 6, 726–729.
352. ———, *A $p+1$ method of factoring*, Math. of Comp. **39** (1982), no. 159, 225–234.
353. ———, *Some public-key crypto-functions as intractable as factorization*, Cryptologia **9** (1985), no. 3, 223–237.

354. ______, *An M^3 public key encryption scheme*, Advances in Cryptology – Crypto '85 (H. C. Williams, ed.), Lecture Notes in Computer Science, vol. 218, Springer-Verlag, 1986, pp. 358–368.
355. ______, *Some public-key crypto-functions as intractable as factorization*, Advances in Cryptology – Crypto '84 (G. R. Blakley and D. Chaum, eds.), Lecture Notes in Computer Science, vol. 196, Springer-Verlag, 1986, pp. 66–70.
356. H. C. Williams and B. Schmid, *Some remarks concerned the M.I.T public-key cryptosystem*, BIT **19** (1979), 525–538.
357. T.-C. Wu and Y.-S. Chang, *Improved generalisation common-multiplicand multiplications algorithm of Yen and Laih*, Electronics Letters **31** (1995), no. 20, 1738–1739.
358. S.-M. Yen and C.-S. Laih, *Common-multiplicand multiplication and its applications to public key cryptography*, Electronics Letters **29** (1993), no. 17, 1583–1584.
359. ______, *Fast algorithms for LUC digital signature computation*, IEE Proc.-Comput. Digit. Tech. **142** (1995), no. 2, 165–169.
360. A. Young and M. Yung, *Kleptography: Using cryptography against cryptography*, Advances in Cryptology – Eurocrypt '97 (W. Fumy, ed.), Lecture Notes in Computer Science, vol. 1233, Springer-Verlag, 1997, pp. 62–74.
361. Y. Zheng and T. Matsumoto, *Breaking smart card implementations of ElGamal signature and its variants*, Presented at the rump session of Asiacrypt '96.
362. R. Zuccherato, *New applications of elliptic curves and function fields in cryptography*, Ph.D. thesis, University of Waterloo, 1997.

APPENDIX A

Index to Notations

1. General

Formal symbolism	Meaning
G	group
$\#G$	order of the (finite) group G
R	ring
R^*	group of units of the ring R
K	field
$\mathfrak{O}_{\sqrt{\Delta}}$	ring of integers of the quadratic field $\mathbb{Q}(\sqrt{\Delta})$
$\mathbb{F}_p$	finite prime field
$\mathbb{Z}_n$	ring of integers modulo n
$\mathbb{Z}[i]$	ring of Gaussian integers
$\mathbb{Z}[\omega]$	ring of Eisenstein integers
$\phi(n)$	Euler's totient function
$\mathrm{Resultant}_x(\mathcal{P}, \mathcal{Q})$	resultant in x of $\mathcal{P}$ and $\mathcal{Q} \in R[x]$
$\lfloor a \rfloor$	largest integer $\leq a$
$\lceil a \rceil$	least integer $\geq a$
$\lfloor a \rceil$	nearest integer to a
$\overline{\alpha}$	conjugate of the quadratic integer α
$\mathrm{N}(\alpha)$	norm of α, *i.e.* $\mathrm{N}(\alpha) = \alpha\overline{\alpha}$
(a/p)	Legendre symbol of a modulo p
$(\alpha/\pi)_3$	cubic residue symbol of α modulo π
$(\alpha/\pi)_4$	quartic residue symbol of α modulo π
$(\alpha/\pi)_6$	sixtic residue symbol of α modulo π
(a/n)	Jacobi symbol of a modulo n
$n!$	n factorial
$\binom{n}{k}$	binomial coefficient
$\gcd(a, b)$	greatest common divisor of a and b
$\gcd(\langle a_i \rangle_{i=1}^k, b)$	$\gcd(a_1, a_2, \dots, a_k, b)$

Formal symbolism	Meaning
$\mathrm{lcm}(a,b)$	least common multiple of a and b
$a \mid b$	a divides b
$a \nmid b$	a does not divide b
$a \equiv b \pmod{n}$	a is congruent to b modulo n
$a = b \bmod n$	$a \equiv b \pmod{n}$ and $a \in [0, n-1]$
$a = b \bmod_{\pm} n$	$a \equiv b \pmod{n}$ and $a \in [-\lceil n/2 \rceil + 1, \lfloor n/2 \rfloor]$
$\mathrm{lsb}(a)$	least significant bit of a
δ_{ij}	Kronecker's delta

2. Lucas sequences

Formal symbolism	Meaning
$U_k(P,Q)$	'sister' Lucas sequence with parameters P and Q
$V_k(P,Q)$	Lucas sequence with parameters P and Q
$D_n(x,a)$	Dickson polynomials of the first kind
$E_n(x,a)$	Dickson polynomials of the second kind

3. Elliptic curves

Formal symbolism	Meaning
$E(a,b)$	elliptic curve
$E_p(a,b)$	elliptic curve over the prime field $\mathbb{F}_p$
$\#E_p(a,b)$	order of the elliptic curve $E_p(a,b)$
a_p	$p+1-\#E_p(a,b)$
$\overline{E_p(a,b)}$	complementary group of $E_p(a,b)$
$E_n(a,b)$	elliptic curve over the ring $\mathbb{Z}_n$ $(n = pq)$
$\mathcal{O}$	point at infinity of an elliptic curve
$\mathrm{x}(\mathbf{P})$	x-coordinate of point $\mathbf{P} \in E(a,b)$
$\mathrm{y}(\mathbf{P})$	y-coordinate of point $\mathbf{P} \in E(a,b)$
$[k]\mathbf{P}$	$\mathbf{P} + \mathbf{P} + \cdots + \mathbf{P}$ (k times) on $E(a,b)$
$[k]_x\, p_1$	x-coordinatewise multiplication

Formal symbolism	Meaning
$\Psi_k(x, y)$	division polynomials
$\mathcal{G}_k(x)$	$\mathrm{x}([k]\mathbf{P})$ where $\mathbf{P} = (x, y)$
$\mathcal{F}_k(x)$	$\mathrm{y}([k]\mathbf{P})/\,\mathrm{y}(\mathbf{P})$ where $\mathbf{P} = (x, y)$

4. Lattices

Formal symbolism	Meaning
L	lattice
$\Delta(L)$	determinant of the lattice L
$\Lambda_k(L)$	k^{th} minimum of lattice L
$\Vert\vec{v}\Vert$	Euclidean length of the vector $\vec{v}$
$\langle\vec{u}, \vec{v}\rangle$	usual inner product of the vectors $\vec{u}$ and $\vec{v}$

APPENDIX B

Biography and Publications

1. Biographical sketch

Marc Joye was born in Mouscron (Belgium) on December 27th, 1969. He graduated as engineer in applied mathematics at the University of Louvain (January 1994) and received a degree in mathematics at the same university (June 1995). He participated to the European project ACCOPI (Acces Control and COpyright Protection for Images): study of access control in a multimedia environment in April-August 1994. He was teaching assistant in mathematics from Sept. 1994 till Sept. 1997. He has been member of the International Association of Cryptologic Research (IACR) since 1995. He is also editor of the technical reports of the UCL Crypto Group.

2. Publications and communications

1. Marc Joye and Jean-Jacques Quisquater. Protocol failures for RSA-type cryptosystems using Lucas sequences and elliptic curves. In M. Lomas, ed., *Security Protocols*, volume 1189 of *Lectures Notes in Computer Science*, pages 93–100. Springer-Verlag, 1997.

2. Marc Joye and Jean-Jacques Quisquater. Note on the preliminary version of Meyer-Müller cryptosystem. Tech. Report CG-1996/2, UCL Crypto Group, Louvain-la-Neuve, January 1996.

3. Marc Joye and Jean-Jacques Quisquater. Efficient computation of full Lucas sequences. *Electronics Letters*, 32(6):537–538, March 1996.

4. Marc Joye and Jean-Jacques Quisquater. Reducing the elliptic curve cryptosystem of Meyer-Müller to the cryptosystem of Rabin-Williams. *Designs, Codes and Cryptography*. To appear.

5. Marc Joye and Jean-Jacques Quisquater. Cryptanalysis of RSA-type cryptosystems: a visit. In *Network Threats*, DIMACS Series in Dicrete Mathematics and Theoretical Computer Science. American Mathematical Society. To appear.

6. Jean-Jacques Quisquater, Benoît Macq, Marc Joye, Nicolas Degand, and Alexis Bernard. Practical solution to authentication of images with a secure camera. In

I. K. Sethi and R. C. Jain, eds, *Storage and Retrieval for Image and Video Databases V*, volume 3022, pages 290–297. SPIE, 1997.

7. Marc Joye and Jean-Jacques Quisquater. On the importance of securing your bins: The garbage-man-in-the-middle attack. In T. Matsumoto, ed., *4th ACM Conference on Computer and Communications Security*, pages 135–141. ACM Press, 1997.

8. Marc Joye. Common modulus attack against Lucas-based cryptosystems. Tech. Report CG-1996/10, UCL Crypto Group, Louvain-la-Neuve, December 1996.

9. Marc Joye, Arjen K. Lenstra, and Jean-Jacques Quisquater. Chinese remaindering cryptosystems in the presence of faults. Submitted to *Journal of Cryptology.*

10. Marc Joye, François Koeune, and Jean-Jacques Quisquater. Further results on Chinese remaindering. Tech. Report CG-1997/1, UCL Crypto Group, Louvain-la-Neuve, March 1997. Presented at the rump session of Eurocrypt '97.

11. Marc Joye and Jean-Jacques Quisquater. Authentication of sequences with the SL_2 hash function : Application to video sequences. *Journal of Computer Security.* To appear.

12. Marc Joye, François Koeune, and Jean-Jacques Quisquater. Takagi/Naito's algorithm revisited. Tech. Report CG-1997/3, UCL Crypto Group, Louvain-la-Neuve, March 1997.

13. Daniel Bleichenbacher, Marc Joye, and Jean-Jacques Quisquater. A new and optimal chosen-message attack on RSA-type cryptosystems. In Y. Han *et al.*, eds, *Information and Communications Security*, volume 1334 of *Lectures Notes in Computer Science*, pages 302–313. Springer-Verlag, 1997.

14. Marc Joye and Jean-Jacques Quisquater. Cryptosystem of Chua and Ling. *Electronics Letters*, 33(23):1938, November 1997.

15. Aurore Gillet, Marc Joye, and Jean-Jacques Quisquater. Cautionary note for protocols designers: Security proof is not enough. In H. Orman and C. Meadows, eds, *Proc. of the DIMACS Workshop on Design and Formal Verification of Security Protocols.* (CDROM), 1997.

16. Marc Joye, Jean-Jacques Quisquater, Feng Bao, and Robert H. Deng. RSA-type signatures in the presence of transient faults. In M. Darnell, ed., *Cryptography and Coding*, Lectures Notes in Computer Science. Springer-Verlag. To appear.

17. Jean-François Dhem, Marc Joye, and Jean-Jacques Quisquater. Normalisation in diminished-radix modulus transformation. *Electronics Letters*, 33(23):1931, November 1997.

18. Marc Joye and Jean-Jacques Quisquater. Faulty RSA encryption. Tech. Report CG-1997/8, UCL Crypto Group, Louvain-la-Neuve, July 1997.

19. Marc Joye, Jean-Jacques Quisquater, and Tsuyoshi Takagi. How to choose secret parameters for RSA-type cryptosystems over elliptic curves. In preparation.

Index