Published in Y. Han, T. Okamoto, and S. Qing, eds, *Information and Communications Security (ICICS '97)*, vol. 1334 of *Lecture Notes in Computer Science*, pp. 302-313, Springer-Verlag, 1997.

A New and Optimal Chosen-message Attack on RSA-type Cryptosystems

Daniel Bleichenbacher[1], Marc Joye[2] and Jean-Jacques Quisquater[3]

[1] Bell Laboratories
700 Mountain Av. , Murray Hill, NJ 07974, U.S.A.
E-mail: bleichen@research.bell-labs.com
[2] UCL Crypto Group, Dép. de Mathématique, Université de Louvain
Chemin du Cyclotron 2, B-1348 Louvain-la-Neuve, Belgium
E-mail: joye@agel.ucl.ac.be
[3] UCL Crypto Group, Lab. de Microélectronique, Université de Louvain
Place du Levant 3, B-1348 Louvain-la-Neuve, Belgium
E-mail: jjq@dice.ucl.ac.be

Abstract. Chosen-message attack on RSA is usually considered as an inherent property of its homomorphic structure. In this paper, we show that non-homomorphic RSA-type cryptosystems are also susceptible to a chosen-message attack. In particular, we prove that only *one* message is needed to mount a successful chosen-message attack against the Lucas-based systems and Demytko's elliptic curve system.

Keywords. Chosen-message attack, signature forgery, RSA, Lucas-based systems, Demytko's elliptic curve system.

1 Introduction

The most used public-key cryptosystem is certainly the RSA [12]. Due to its popularity, the RSA was subject to an extensive cryptanalysis. Many attacks are based on the multiplicative nature of RSA [5]. To overcome this vulnerability, numerous generalizations of the original RSA were proposed and broken.

Later, other structures were envisaged to implement analogues of RSA. This seemed to be the right way to foil the homomorphic attacks. So, a cryptosystem based on Lucas sequences was proposed in [10] and analyzed in [11] by Müller and Nöbauer. The authors use Dickson polynomials to describe their scheme; however, Dickson polynomials can be rephrased in terms of Lucas sequences [2, 14]. The Lucas sequences play the same role in this scheme as exponentiations in RSA.

In 1985, Koblitz and Miller independently suggested the use of elliptic curves in cryptography [7, 9]. Afterwards, Koyama *et al.* [8] and Demytko [4] exhibited new one-way trapdoor functions on elliptic curves in order to produce analogues of RSA. Demytko's system has the particularity to only use the first coordinate and is therefore not subject to the chosen-message attack described in [8].

The Lucas-based cryptosystems and Demytko's elliptic curve cryptosystem seem to be resistant against homomorphic attack. However, the existence of a chosen-message

forgery that needs two messages has been described in [1]. Kaliski found a similar attack on Demytko's system [6].

In this paper, we describe a new chosen-message attack which needs only one message. This new attack shows that the RSA-type cryptosystems are even closer related to RSA, i.e. it shows that all the attacks based on the multiplicative nature of the original RSA can straightforward be adapted to any RSA-type cryptosystem. We illustrate this topic with the common modulus failure [13].

The remainder of this paper is organized as follows. In Section 2, we review the Lucas-based and Demytko's elliptic curve cryptosystems. The reader who is not not familiar with these systems may first read the appendix. We present our attack in Section 3 and apply it in Section 4. In Section 5, we revisit the common modulus failure. Finally, we conclude in Section 6.

2 RSA-type cryptosystems

In this section, we present cryptosystems based on Lucas sequences [10, 11, 14] and on elliptic curves [4]. We only outline the systems, for a detailed description we refer to the original papers.

2.1 Lucas-based RSA

The Lucas-based scheme can briefly be described as follows. Each user A chooses two large primes p and q and an exponent e that is relatively prime to $(p^2-1)(q^2-1)$, computes $n = pq$, and publishes n and e as his public key. The corresponding $d \equiv e^{-1} \pmod{\operatorname{lcm}(p-1, p+1, q-1, q+1)}$ is kept secret.

A's public parameters: n and e.
A's secret parameters: p, q and d.

A message m is encrypted by computing $c \equiv v_e(m,1) \pmod{n}$. It is decrypted using the secret key d by $m \equiv v_d(c,1) \pmod{n}$. The correctness of this system is based on Proposition 3 (in appendix) as $v_d\big(v_e(m,1),1\big) \equiv v_{de}(m,1) \equiv v_1(m,1) \equiv m \pmod{n}$. Signatures are generated accordingly by exchanging the roles of the public and secret parameters e and d.

2.2 Demytko's system

Similarly to RSA, to setup Demytko's system, each user A chooses two large primes p and q, and publishes their product $n = pq$. He publicly selects integers a and b such that $\gcd(4a^3 + 27b^2, n) = 1$. Then once and for all, he computes

$$N_n = \operatorname{lcm}\left(\#E_p(a,b), \#E_q(a,b), \#\overline{E_p(a,b)}, \#\overline{E_q(a,b)}\right). \tag{1}$$

He randomly chooses the public encryption key e such that $\gcd(e, N_n) = 1$, and computes the secret decryption key d according to $ed \equiv 1 \bmod N_n$.

A's public parameters: n, a, b and e.
A's secret parameters: p, q, N_n and d.

It is useful to introduce some notation. The $x-$ and the $y-$coordinates of a point $\mathbf{P}$ will respectively be denoted by $x(\mathbf{P})$ and $y(\mathbf{P})$. To send a message m to Alice, Bob uses Alice's public key e and computes the corresponding ciphertext $c \equiv x(e\mathbf{M}) \pmod{n}$ where $\mathbf{M}$ is a point having its $x-$coordinate equal to m. Note that, from Proposition 1, the computation of $c \equiv x(e\mathbf{M}) \pmod{n}$ does not require the knowledge of $y(\mathbf{M})$.

Using her secret key d, Alice can recover the plaintext m by computing $m \equiv x(d\mathbf{C}) \pmod{n}$ where $\mathbf{C}$ is a point having its $x-$coordinate equal to c. Note also that Alice has not to know $y(\mathbf{C})$.

Remark 1. To speed up the computations, Alice can choose $p, q \equiv 2 \bmod 3$ and $a = 0$. In that case, $N_n = \operatorname{lcm}(p+1, q+1)$. The same conclusion holds by choosing $p, q \equiv 3 \bmod 4$ and $b = 0$ (see [8]).

Remark 2. For efficiency reasons, it is also possible to define a message-dependent system (see [4]).

3 Sketch of the new attack

Let $n = pq$ be a RSA modulus. Let e and d be respectively the public key and the secret key of Alice, according to $ed \equiv 1 \pmod{\Phi(n)}$. The public key e is used to encrypt messages and verify signatures; the secret key d is used to decrypt ciphertexts and to sign messages.

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

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. Applying to 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 she uses the extended Euclidean algorithm to find $r, s \in \mathbb{Z}$ such that $kr + es = 1$.
Step 2: Carol computes $m' \equiv m^k \pmod{n}$.
Step 3: Next, she asks Alice to sign m' and gets therefore

$$c' \equiv m'^d \pmod{n}.$$

Step 4: Consequently, Carol can compute the signature c of m by

$$c \equiv c'^r m^s \pmod{n}. \tag{2}$$

Output: The signature c of message m.

Proof. From $kr + es = 1$, it follows $d = d(kr + es) \equiv dkr + s \pmod{\Phi(n)}$. Hence, $c \equiv m^d \equiv m^{dkr} m^s \equiv \left(m^{dk}\right)^r m^s \equiv c'^r m^s \pmod{n}$. □

Remark 3. This attack can also be considered as a generalization of the Davida's attack [3].

4 Applications

The previous attack applies also to non-homomorphic cryptosystems. In this section, we show how it works against Lucas-based systems and Demytko's system.

4.1 Attacking Lucas-based systems

The cryptanalyst Carol can try to get a signature c on a message m in the following way.

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 $r, s \in \mathbb{Z}$ such that $kr + es = 1$.
Step 2: Next she computes $m' \equiv v_k(m, 1) \pmod{n}$.
Step 3: Now she asks Alice to sign m'. If Alice does so then Carol knows c' such that

$$c' \equiv v_d(m', 1) \pmod{n}.$$

Step 4: Finally Carol computes the signature c of m as follows

$$v_{rkd}(m, 1) \equiv v_r(c', 1) \pmod{n}, \tag{3}$$

$$u_{rkd}(m, 1) \equiv \frac{u_k(m, 1)u_r(c', 1)}{u_e(c', 1)} \pmod{n}, \tag{4}$$

$$c = v_d(m, 1) \equiv \frac{v_{rkd}(m, 1)v_s(m, 1)}{2} + \frac{\Delta\, u_{rkd}(m, 1)u_s(m, 1)}{2} \pmod{n} \tag{5}$$

where $\Delta = m^2 - 4$.
Output: The signature c of message m.

Proof. Equation (3) follows from (13)[1] since

$$v_r(c', 1) \equiv v_r\left(v_{kd}(m, 1), 1\right) \equiv v_{rkd}(m, 1) \pmod{n}.$$

[1] (9) to (22) refer to equations in the appendix.

Equation (4) is a consequence of (14) and

$$\begin{aligned} u_{rkd}(m,1)u_e(c',1) &\equiv u_r\big(v_{kd}(m,1),1\big)u_{kd}(m,1)u_e\big(v_{kd}(m,1),1\big) \\ &\equiv u_r\big(v_{kd}(m,1),1\big)u_{kde}(m,1) \\ &\equiv u_r\big(v_{kd}(m,1),1\big)u_k(m,1) \pmod{n}. \end{aligned}$$

Moreover, $kr + es = 1$ implies $v_d(m,1) = v_{rkd+des}(m,1) = v_{rkd+s}(m,1)$. Hence Equation (5) is an application of (15). □

Remark 4. This attack is the analogue to the chosen-message attack on RSA presented in Section 3, by using algebraic numbers (replace m by $\alpha = (m + \sqrt{\Delta})/2$ and use Equation (9)). The only additional step to be proved is that $u_{kd}(m,1)$ is computable from m and $v_{kd}(m,1)$. This can be shown by using (14) and noting that

$$u_k(m,1) \equiv u_{kde}(m,1) \equiv u_{kd}(m,1)u_e\big(v_{kd}(m,1),1\big) \pmod{n}.$$

If $\alpha = m/2 + \sqrt{\Delta}/2$ then the signature $v_{kd}(m,1)$ on the message $v_k(m,1)$ can be used to compute

$$\alpha^{kd} \equiv v_{kd}(m,1)/2 + u_{kd}(m,1)\sqrt{\Delta}/2.$$

Once α^{kd} is known, $\alpha^d = v_d(m,1)/2 + u_d(m,1)\sqrt{\Delta}/2$ can be computed from

$$\alpha^d \equiv \alpha^{(kr+es)d} \equiv \left(\alpha^{kd}\right)^r \alpha^s \pmod{n}.$$

Hence (3) and (4) correspond to the computation of c'^r and (5) corresponds to the multiplication of c'^r by m^s in (2).

4.2 Attacking Demytko's system

Before showing that a similar attack applies to Demytko's system, we need to prove the following proposition.

Proposition 1. *Let p be a prime greater than 3, and let $E_p(a,b)$ be an elliptic curve over $\mathbb{Z}_p$. If $\mathbf{P} \in E_p(a,b)$ or if $\mathbf{P} \in \overline{E_p(a,b)}$, then the computations of $x(k\mathbf{P})$ and $\dfrac{y(k\mathbf{P})}{y(\mathbf{P})}$ depend only on $x(\mathbf{P})$.*

Proof. Letting $X_j := x(j\mathbf{P})$ and $Y_j := \frac{y(j\mathbf{P})}{y(\mathbf{P})}$, the tangent-and-chord composition rule on elliptic curves gives the following formulas

$$\begin{aligned} X_{2j} = x(j\mathbf{P} + j\mathbf{P}) &= \begin{cases} \left(\frac{3\,x(j\mathbf{P})^2+a}{2\,y(j\mathbf{P})}\right)^2 - 2\,x(j\mathbf{P}) & \text{if } \mathbf{P} \in E_p(a,b) \\ \left(\frac{3\,x(j\mathbf{P})^2+a}{2D_p\,y(j\mathbf{P})}\right)^2 D_p - 2\,x(j\mathbf{P}) & \text{if } \mathbf{P} \in \overline{E_p(a,b)} \end{cases} \\ &= \frac{1}{X_1^3+aX_1+b}\left(\frac{3X_j^2+a}{2Y_j}\right)^2 - 2X_j, \end{aligned}$$

$$Y_{2j} = \frac{y(j\mathbf{P}+j\mathbf{P})}{y(\mathbf{P})} = \begin{cases} \frac{\left(\frac{3\,x(j\mathbf{P})^2+a}{2\,y(j\mathbf{P})}\right)\left(x(j\mathbf{P})-x(2j\mathbf{P})\right)-y(j\mathbf{P})}{y(\mathbf{P})} & \text{if } \mathbf{P} \in E_p(a,b) \\ \frac{\left(\frac{3\,x(j\mathbf{P})^2+a}{2D_p\,y(j\mathbf{P})}\right)\left(x(j\mathbf{P})-x(2j\mathbf{P})\right)-y(j\mathbf{P})}{y(\mathbf{P})} & \text{if } \mathbf{P} \in \overline{E_p(a,b)} \end{cases}$$

$$= \frac{1}{X_1^3+aX_1+b}\left(\frac{3X_j^2+a}{2Y_j}\right)(X_j - X_{2j}) - Y_j,$$

$$X_{2j+1} = x\big(j\mathbf{P} + (j+1)\mathbf{P}\big)$$

$$= \begin{cases} \left(\frac{y(j\mathbf{P})-y((j+1)\mathbf{P})}{x(j\mathbf{P})-x((j+1)\mathbf{P})}\right)^2 - x(j\mathbf{P}) - x\big((j+1)\mathbf{P}\big) & \text{if } \mathbf{P} \in E_p(a,b) \\ \left(\frac{y(j\mathbf{P})-y((j+1)\mathbf{P})}{x(j\mathbf{P})-x((j+1)\mathbf{P})}\right)^2 D_p - x(j\mathbf{P}) - x\big((j+1)\mathbf{P}\big) & \text{if } \mathbf{P} \in \overline{E_p(a,b)} \end{cases}$$

$$= (X_1^3 + aX_1 + b)\left(\frac{Y_j - Y_{j+1}}{X_j - X_{j+1}}\right)^2 - X_j - X_{j+1},$$

$$Y_{2j+1} = \frac{y\big(j\mathbf{P}+(j+1)\mathbf{P}\big)}{y(\mathbf{P})}$$

$$= \frac{\left(\frac{y(j\mathbf{P})-y((j+1)\mathbf{P})}{x(j\mathbf{P})-x((j+1)\mathbf{P})}\right)\left(x(j\mathbf{P})-x((2j+1)\mathbf{P})\right)-y(j\mathbf{P})}{y(\mathbf{P})} \quad \text{if } \mathbf{P} \in E_p(a,b) \text{ or } \overline{E_p(a,b)}$$

$$= \frac{Y_j - Y_{j+1}}{X_j - X_{j+1}}(X_j - X_{2j+1}) - Y_j.$$

So X_k and Y_k can be computed from $X_1 = x(\mathbf{P})$ and $Y_1 = 1$ by using the binary method. □

Then, the message forgery goes as follows.

Input: A message m and the public key n, e of Alice.
Note that m is the $x-$coordinate of a point $\mathbf{M}$, i.e. $m = x(\mathbf{M})$.

Step 1: The cryptanalyst Carol chooses a random k relatively prime to e. Then she uses extended Euclidean algorithm to find $r, s \in \mathbb{Z}$ such that $kr + es = 1$.

Step 2: From $x(\mathbf{M})$, Carol computes $m' = x(\mathbf{M}') \equiv x(k\mathbf{M}) \pmod{n}$. Next, she asks Alice to sign m'. So, Carol obtains the signature

$$c' = x(\mathbf{C}') \equiv x(d\mathbf{M}') \pmod{n}.$$

Step 3: Finally, Carol finds the signature $c = x(\mathbf{C}) \equiv x(d\mathbf{M}) \pmod{n}$ of message m as follows.

3a) If $x(r\mathbf{C}') \not\equiv x(s\mathbf{M}) \pmod{n}$ then, using Proposition 1, Carol can compute

$$\frac{y(k\mathbf{M})}{y(\mathbf{M})}, \frac{y(r\mathbf{C}')}{y(\mathbf{C}')} \text{ and } \frac{y(e\mathbf{C}')}{y(\mathbf{C}')} \tag{6}$$

and

$$c \equiv (m^3 + am + b)\left[\frac{\frac{y(k\mathbf{M})}{y(\mathbf{M})}\frac{y(r\mathbf{C}')}{y(\mathbf{C}')}\left(\frac{y(e\mathbf{C}')}{y(\mathbf{C}')}\right)^{-1} - \frac{y(s\mathbf{M})}{y(\mathbf{M})}}{x(r\mathbf{C}') - x(s\mathbf{M})}\right]^2 - x(r\mathbf{C}') - x(s\mathbf{M}) \pmod{n}. \tag{7}$$

3b) Otherwise, the signature is given by

$$c \equiv \frac{\left[3\,x(r\mathbf{C}')^2 + a\right]^2}{4\left[x(r\mathbf{C}')^3 + a\,x(r\mathbf{C}') + b\right]} - 2\,x(r\mathbf{C}') \pmod{n}. \qquad (8)$$

Output: The signature c of message m.

Proof. Since $kr + es = 1$, $d \equiv krd + esd \equiv krd + s \pmod{N_n}$. So,

$$x(\mathbf{C}) \equiv x(d\mathbf{M}) \equiv x\big([krd + s]\mathbf{M}\big) \equiv x(r\mathbf{C}' + s\mathbf{M}) \pmod{n}.$$

a) If $x(r\mathbf{C}') \not\equiv x(s\mathbf{M}) \pmod{n}$, then

$$\begin{aligned} &x(r\mathbf{C}' + s\mathbf{M}) \\ &\quad\equiv \left(\frac{y(r\mathbf{C}') - y(s\mathbf{M})}{x(r\mathbf{C}') - x(s\mathbf{M})}\right)^2 - x(r\mathbf{C}') - x(s\mathbf{M}) \\ &\quad\equiv y(\mathbf{M})^2 \left[\frac{\frac{y(k\mathbf{M})}{y(\mathbf{M})}\frac{y(r\mathbf{C}')}{y(\mathbf{C}')}\frac{y(\mathbf{C}')}{y(e\mathbf{C}')} - \frac{y(s\mathbf{M})}{y(\mathbf{M})}}{x(r\mathbf{C}') - x(s\mathbf{M})}\right]^2 - x(r\mathbf{C}') - x(s\mathbf{M}) \pmod{n} \end{aligned}$$

since

$$\frac{y(r\mathbf{C}')}{y(\mathbf{M})} = \frac{y(r\mathbf{C}')}{y(\mathbf{C}')}\frac{y(\mathbf{C}')}{y(k\mathbf{M})}\frac{y(k\mathbf{M})}{y(\mathbf{M})}$$

and $y(k\mathbf{M}) \equiv y(edk\mathbf{M}) \equiv y(e\mathbf{C}') \pmod{n}$.

b) Otherwise, since $\gcd(d, N_n) = 1$ it follows that $r\mathbf{C}' \not\equiv -s\mathbf{M} \pmod{n}$ and therefore

$$x(r\mathbf{C}' + s\mathbf{M}) \equiv \left(\frac{3\,x(rC')^2 + a}{2\,y(r\mathbf{C}')}\right)^2 - x(r\mathbf{C}') - x(s\mathbf{M}) \pmod{n}.$$

□

5 Common modulus attack

Simmons pointed out in [13] that the use of a common RSA modulus is dangerous. Indeed, if a message is sent to two users that have coprime public encryption keys, then the message can be recovered.

Because our chosen-message attack requires only one message, the Lucas-based systems and Demytko's elliptic curve system are vulnerable to the common modulus attack. We shall illustrate this topic on Demyko's system.

Let (e_1, d_1) and (e_2, d_2) be two pairs of encryption/decryption keys and let $m = x(\mathbf{M})$ be the message being encrypted. Assuming e_1 and e_2 are relatively prime, the cryptanalyst Carol can recover m from the ciphertexts $c_1 = x(\mathbf{C_1}) \equiv x(e_1\mathbf{M}) \pmod{n}$ and $c_2 = x(\mathbf{C_2}) \equiv x(e_2\mathbf{M}) \pmod{n}$ as follows.

Carol uses the extended Euclidean algorithm to find integers r and s such that $re_1 + se_2 = 1$. Then, she computes $x(\mathbf{M}) = x((re_1 + se_2)\mathbf{M}) \equiv x(r\mathbf{C_1} + s\mathbf{C_2}) \pmod{n}$ as follows. If $x(r\mathbf{C_1}) \not\equiv x(s\mathbf{C_2}) \pmod{n}$, then

$$m \equiv (c_1^3 + ac_1 + b) \left[\frac{\frac{y(r\mathbf{C_1})}{y(\mathbf{C_1})} - \frac{y(e_2\mathbf{C_1})}{y(\mathbf{C_1})} \frac{y(s\mathbf{C_2})}{y(\mathbf{C_2})} \left(\frac{y(e_1\mathbf{C_2})}{y(\mathbf{C_2})} \right)^{-1}}{x(r\mathbf{C_1}) - x(s\mathbf{C_2})} \right]^2 - x(r\mathbf{C_1}) - x(s\mathbf{C_2}) \pmod{n}$$

otherwise

$$m \equiv \frac{\left[3\,x(r\mathbf{C_1})^2 + a\right]^2}{4\left[x(r\mathbf{C_1})^3 + a\,x(r\mathbf{C_1}) + b\right]} - 2\,x(r\mathbf{C_1}) \pmod{n}.$$

Proof. Straightforward since $y(e_2\mathbf{C_1}) \equiv y(e_1\mathbf{C_2}) \pmod{n}$. □

6 Conclusion

We have presented a new type of chosen-message attack. Our formulation has permitted to mount a successful chosen-message attack with only one message against Lucas-based systems and Demytko's system. This also proved that the use of non-homomorphic systems is not necessarily the best way to foil chosen-message attacks.

Acknowledgments The second author is grateful to Victor Miller for providing some useful comments to enhance the presentation of the paper.

References

1. D. Bleichenbacher, W. Bosma, and A. K. Lenstra. Some remarks on Lucas-based cryptosystems. In D. Coppersmith, editor, *Advances in Cryptology – CRYPTO '95*, volume 963 of *Lecture Notes in Computer Science*, pages 386–396. Springer-Verlag, 1995.
2. D. M. Bressoud. *Factorization and primality testing*. Undergraduate Texts in Mathematics. Springer-Verlag, 1989.
3. G. Davida. Chosen signature cryptanalysis of the RSA (MIT) public key cryptosystem. Technical Report TR-CS-82-2, Dept. of Electrical Engineering and Computer Science, University of Wisconsin, Milwaukee, USA, October 1982.
4. N. Demytko. A new elliptic curve based analogue of RSA. In T. Helleseth, editor, *Advances in Cryptology – EUROCRYPT '93*, volume 765 of *Lecture Notes in Computer Science*, pages 40–49. Springer-Verlag, 1994.
5. D. E. Denning. Digital signatures with RSA and other public-key cryptosystems. *Communications of the ACM*, 27(4):388–392, April 1984.
6. B. S. Kaliski Jr. A chosen message attack on Demytko's elliptic curve cryptosystem. *Journal of Cryptology*, 10(1):71–72, 1997.
7. N. Koblitz. Elliptic curve cryptosystems. *Mathematics of Computation*, 48:203–209, 1987.
8. K. Koyama, U. M. Maurer, T. Okamoto, and S. A. Vanstone. New public-key schemes based on elliptic curves over the ring $\mathbb{Z}_n$. In J. Feigenbaum, editor, *Advances in Cryptology – CRYPTO '91*, volume 576 of *Lecture Notes in Computer Science*, pages 252–266. Springer-Verlag, 1991.

9. V. S. Miller. Use of elliptic curves in cryptography. In H. C. Williams, editor, *Advances in Cryptology – CRYPTO '85*, volume 218 of *Lecture Notes in Computer Science*, pages 417–426. Springer-Verlag, 1986.
10. W. B. Müller and R. Nöbauer. Some remarks on public-key cryptosystems. *Sci. Math. Hungar*, 16:71–76, 1981.
11. W. B. Müller and R. Nöbauer. Cryptanalysis of the Dickson scheme. In J. Pichler, editor, *Advances in Cryptology – EUROCRYPT '85*, volume 219 of *Lecture Notes in Computer Science*, pages 50–61. Springer-Verlag, 1986.
12. R. L. Rivest, A. Shamir, and L. Adleman. A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*, 21(2):120–126, February 1978.
13. G. J. Simmons. A weak privacy protocol using the RSA cryptoalgorithm. *Cryptologia*, 7:180–182, 1983.
14. P. J. Smith and M. J. J. Lennon. LUC: A new public key system. In E. G. Douglas, editor, *Ninth IFIP Symposium on Computer Security*, pages 103–117. Elsevier Science Publishers, 1993.

A Basic facts

A.1 Lucas sequences

Let P, Q be integers, $\Delta = P^2 - 4Q$ be a non-square, $\alpha = \frac{P+\sqrt{\Delta}}{2}$ and $\beta = \overline{\alpha} = \frac{P-\sqrt{\Delta}}{2}$ be the roots of $x^2 - Px + Q = 0$ in the quadratic field $\mathbb{Q}(\sqrt{\Delta})$. The Lucas sequences $v_k(P,Q)$ and $u_k(P,Q)$ for $k \in \mathbb{Z}$ are then defined as the integers satisfying

$$\alpha^k := \frac{v_k(P,Q)}{2} + \frac{u_k(P,Q)\sqrt{\Delta}}{2}. \tag{9}$$

From $\alpha^2 = P\alpha - Q$ follows $\alpha^k = P\alpha^{k-1} - Q\alpha^{k-2}$. Hence the Lucas sequences satisfy the following recurrence relation

$$\begin{aligned} &v_0(P,Q) = 2; \quad v_1(P,Q) = P; \quad v_k(P,Q) = Pv_{k-1}(P,Q) - Qv_{k-2}(P,Q), \\ &u_0(P,Q) = 0; \quad u_1(P,Q) = 1; \quad u_k(P,Q) = Pu_{k-1}(P,Q) - Qu_{k-2}(P,Q). \end{aligned}$$

This recurrence relation is sometimes used as an alternative definition of Lucas sequences. Since conjugation and exponentiation are exchangeable it follows

$$\beta^k = \overline{\alpha^k} = \frac{v_k(P,Q)}{2} - \frac{u_k(P,Q)\sqrt{\Delta}}{2}.$$

From this equation and from (9) it follows that

$$v_k(P,Q) = \alpha^k + \beta^k, \tag{10}$$

$$\text{and } u_k(P,Q) = \frac{\alpha^k - \beta^k}{\alpha - \beta}. \tag{11}$$

The next proposition states some well-known properties of Lucas sequences.

Proposition 2.

$$4Q^k = v_k(P,Q)^2 - \Delta u_k(P,Q)^2 \tag{12}$$
$$v_{km}(P,Q) = v_k\big(v_m(P,Q), Q^m\big) \tag{13}$$
$$u_{km}(P,Q) = u_m(P,Q)u_k\big(v_m(P,Q), Q^m\big) \tag{14}$$
$$v_{k+m}(P,Q) = \frac{v_k(P,Q)v_m(P,Q)}{2} + \frac{\Delta u_k(P,Q)u_m(P,Q)}{2} \tag{15}$$
$$u_{k+m}(P,Q) = \frac{u_k(P,Q)v_m(P,Q)}{2} + \frac{v_k(P,Q)u_m(P,Q)}{2} \tag{16}$$

Proof. Equation (12) can be proved as follows.

$$\begin{aligned} 4Q^k &= 4(\alpha\overline{\alpha})^k = 2\alpha^k 2\overline{\alpha^k} \\ &= (v_k(P,Q) + u_k(P,Q)\sqrt{\Delta})(v_k(P,Q) - u_k(P,Q)\sqrt{\Delta}) \\ &= v_k(P,Q)^2 - \Delta u_k(P,Q)^2. \end{aligned}$$

Equation (12) now implies that

$$\begin{aligned} \alpha^k &= \frac{v_k(P,Q)}{2} + \frac{u_k(P,Q)\sqrt{\Delta}}{2} = \frac{v_k(P,Q)}{2} + \frac{\sqrt{u_k(P,Q)^2\Delta}}{2} \\ &= \frac{v_k(P,Q)}{2} + \frac{\sqrt{v_k(P,Q)^2 - 4Q^k}}{2} \end{aligned}$$

and hence $\alpha^k = P'/2 + \sqrt{P'^2 - 4Q'}/2$ with $P' = v_k(P,Q)$ and $Q' = Q^k$. Thus we have

$$\begin{aligned} (\alpha^k)^m &= \frac{v_m(P',Q')}{2} + \frac{u_m(P',Q')\sqrt{P'^2 - 4Q'}}{2} \\ &= \frac{v_m(P',Q')}{2} + \frac{u_m(P',Q')u_k(P,Q)\sqrt{\Delta}}{2}. \end{aligned}$$

Comparing the coefficients of this equation with

$$\alpha^{km} = v_{km}(P,Q)/2 + u_{km}(P,Q)\sqrt{\Delta}/2$$

proves (13) and (14). Writing $\alpha^{k+m} = \alpha^k\alpha^m$ as sums of Lucas sequences and comparing the coefficients shows (15) and (16). □

Proposition 3. *Let p be an odd prime, $Q = 1$ and $\gcd(\Delta, p) = 1$. Then the sequence $v_k(P,1) \bmod p$ is periodic and the length of the period divides $p - \left(\frac{\Delta}{p}\right)$.*

Proof. α and therefore also α^p are algebraic integers in $\mathbb{Q}(\sqrt{\Delta})$. Thus we have $\alpha^p = (P/2 + \sqrt{\Delta}/2)^p \equiv P/2 + (\sqrt{\Delta})^p/2 \equiv P/2 + \Delta^{(p-1)/2}\sqrt{\Delta}/2 \equiv P/2 + \left(\frac{\Delta}{p}\right)\sqrt{\Delta}/2 \pmod p$. Thus if $\left(\frac{\Delta}{p}\right) = 1$ then $\alpha^{p-1} \equiv 1 \pmod p$ and if $\left(\frac{\Delta}{p}\right) = -1$ then $\alpha^{p+1} \equiv 1 \pmod p$. It follows that the sequence α^k (and therefore also $v_k(P,1)$) is periodic with a period that divides $p - \left(\frac{\Delta}{p}\right)$. □

A.2 Elliptic curves

Elliptic curves over $\mathbb{Z}_p$ Let p be a prime greater than 3, and let a and b be two integers such that $4a^3 + 27b^2 \neq 0 \pmod{p}$. An *elliptic curve $E_p(a,b)$ over the prime field $\mathbb{Z}_p$* is the set of points $(x,y) \in \mathbb{Z}_p \times \mathbb{Z}_p$ satisfying the Weierstraß equation

$$y^2 = x^3 + ax + b \pmod{p} \tag{17}$$

together with the point at infinity $\mathcal{O}_p$. The points of the elliptic curve $E_p(a,b)$ form an Abelian group under the tangent-and-chord law defined as follows.

(i) $\mathcal{O}_p$ is the identity element, i.e. $\forall \mathbf{P} \in E_p(a,b)$, $\mathbf{P} + \mathcal{O}_p = \mathbf{P}$.
(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 $\mathbf{Q} = (x_2, y_2) \in E_p(a,b)$ with $\mathbf{P} \neq -\mathbf{Q}$. Then $\mathbf{P} + \mathbf{Q} = (x_3, y_3)$ where

$$x_3 = \lambda^2 - x_1 - x_2, \tag{18}$$
$$y_3 = \lambda(x_1 - x_3) - y_1, \tag{19}$$

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 $\mathbf{P} = (x_1, 0) \in E_p(a,b)$, then $2\mathbf{P} = \mathcal{O}_p$.

Theorem 1 (Hasse). *Let $\#E_p(a,b) = p + 1 - a_p$ denote the number of points in $E_p(a,b)$. Then $|a_p| \leq 2\sqrt{p}$.* □

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

$$D_p y^2 = x^3 + ax + b \tag{20}$$

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

Proposition 4. *If $\#E_p(a,b) = p + 1 - a_p$, then $\#\overline{E_p(a,b)} = p + 1 + a_p$.*

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

Elliptic curves over $\mathbb{Z}_n$ Let $n = pq$ with p and q two primes greater than 3, and let a and b be two integers 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 points $(x, y) \in \mathbb{Z}_n \times \mathbb{Z}_n$ satisfying the Weierstraß equation

$$y^2 = x^3 + ax + b \pmod{n} \tag{21}$$

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

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

$$\widetilde{E}_n(a, b) = E_p(a, b) \times E_q(a, b). \tag{22}$$

By the Chinese remainder theorem 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. *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.