Published in M. Lomas, editor, "Security Protocols", vol. 1189 of Lecture Notes in Computer Science, pp. 93-100, Springer-Verlag, 1997.

Protocol Failures for RSA-like Functions using Lucas Sequences and Elliptic Curves

Marc Joye[1] and Jean-Jacques Quisquater[2]

[1] 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
[2] UCL Crypto Group, Dép. d'Électricité, Université de Louvain
Place du Levant, 3, B-1348 Louvain-la-Neuve (Belgium)
E-mail: jjq@dice.ucl.ac.be

URL: http://www.dice.ucl.ac.be/crypto/

Abstract. We show that the cryptosystems based on Lucas sequences and on elliptic curves over a ring are insecure when a linear relation is known between two plaintexts that are encrypted with a "small" public exponent. This attack is already known for the classical RSA system, but the proofs and the results here are different.

1 Introduction

In numerous situations, the difference between two plaintexts is known, as for example,

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

On the other hand, the security of public-key cryptosystems relies on trapdoor one-way functions. A trapdoor one-way function is a function easy to compute but infeasible to invert unless the trapdoor is known.

Many trapdoor one-way functions are using a polynomial in a given algebraic structure (think about RSA). Recently, some researchers [9, 25, 5, 6] were able to exploit such a structure to mount a new attack against well-known protocols. Here, we show that this attack is of very general nature and not specific to RSA.

The paper is organized as follows. First, we review the cryptosystems based on Lucas sequences and on elliptic curves over a ring. Next, we review the attack on the RSA. Finally, we show how to generalize it and give a short analysis.

2 RSA-like functions

Two years after the introduction of the concept of public-key cryptography [8], Rivest, Shamir and Adleman [29] presented the RSA cryptosystem. After this breakthrough, many generalizations were presented (e.g. using polynomials), and broken.

Recently, it has been adapted to work with other structures. In [16], Koyama, Maurer, Okamoto and Vanstone, and, later Demytko [7] pointed out the existence of new one-way trapdoor functions similar to the RSA on elliptic curves defined over a ring. In 1993, the system proposed by Müller and Nöbauer [22], in 1981, re-emerged to construct the LUC cryptosystem [32]. This latter system uses a special type of Lucas sequences, and is an alternative to the RSA.

In what follows, we shall describe the RSA-like functions used with Lucas sequences and on elliptic curves. The reader who is not familiar with these structures is invited to consult references [3, 27, 28] for Lucas sequences and [4, 11, 21, 30] for elliptic curves.

2.1 LUC function

Each user chooses two secret and "random" large primes p and q, and publishes their product $n = pq$. Next, he chooses a public encryption key e which is relatively prime to $(p-1)$, $(p+1)$, $(q-1)$ and $(q+1)$.

To send a message M to Bob, Alice looks to Bob's public key e, and using the Lucas sequence $\{V_i\}$, she forms the ciphertext $C = V_e(M,1) \bmod n$. Since Bob knows the factors p and q, he is able to compute the secret decryption key d according to $ed \equiv 1 \pmod{\Psi(n)}$, where $\Psi(n) = \mathrm{lcm}(p-(D/p), q-(D/q))$ and $D = M^2 - 4$.[⋆] Therefore, Bob can recover the message M by computing $V_d(V_e(M,1),1) \equiv V_{ed \bmod \Psi(n)}(M,1) \equiv V_1(M,1) \equiv M \pmod{n}$.

2.2 KMOV[⋆⋆]/Demytko's functions

Before presenting these systems, we show a naïve trapdoor one-way function using elliptic curves over a ring.

Similarly, each user chooses two large primes p and q. Moreover, he chooses two parameters a and b such that $\gcd(4a^3 + 27b^2, n) = 1$, where $n = pq$. Next, he computes the order of the elliptic curves $E_p(a,b)$ and $E_q(a,b)$. He chooses a public encryption key e relatively prime to $\#E_p(a,b)$ and $\#E_q(a,b)$, and computes the secret decryption key d such that $ed \equiv 1 \pmod{N_n}$, where $N_n = \mathrm{lcm}(\#E_p(a,b), \#E_q(a,b))$.

The public parameters are n, e, a and b. Before doing, the message $\widetilde{M}$ must be associated to a point $M = (m_x, m_y)$ on the curve $E_n(a,b)$. For this, in a publicly known way, redundancy is introduced to $\widetilde{M}$ so that $m_x^3 + am_x + b$ is a quadratic residue modulo n.

To sign the message $\widetilde{M}$ with her secret key d, Alice computes $C \in E_n(a,b)$ according to $C = dM$. To verify the signature, Bob checks that eC is equal to M.

[⋆] (D/p) denotes the Legendre symbol and is equal to 1 or -1 whether D is a quadratic residue modulo p or not.

[⋆⋆] From the last names of inventors Koyama, Maurer, Okamoto and Vanstone.

This function may only be used in a digital signature scheme, because the trapdoor is required to associate a point of $E_n(a,b)$ to M. Moreover, the signature is twice as long as the message $\widetilde{M}$. To overcome these shortcomings, new one-way trapdoors functions were proposed.

KMOV function In that system, the primes p and q are both congruent to 2 modulo 3, and the parameter a is equal to 0. In that case,

$$N_n = \operatorname{lcm}(\#E_p(0,b), \#E_q(0,b)) = \operatorname{lcm}(p+1, q+1).$$

Since N_n does not depend on b, the parameter b is chosen according to

$$b = m_y^2 - m_x^3 \bmod n.$$

Remarks. 1) The minimum possible value of the public key e is 5, because 6 divides N_n and e must be relatively prime to N_n.
2) It is also possible to work on the elliptic curve $E_n(a,0)$, if one chooses p and q congruent to 3 modulo 4.

Demytko's function The parameters n, a, b and e are chosen as before. To encrypt $M = (m_x, m_y)$, Alice computes $C = (c_x, c_y) = eM$. To decrypt the ciphertext C, Bob computes $d_i C = d_i e M = M$, where the decryption key is chosen so that

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

$$\text{with } \begin{cases} N_{n,1} = \operatorname{lcm}(\#E_p(a,b), \#E_q(a,b)) & \text{if } (w/p) = 1 \text{ and } (w/q) = 1 \\ N_{n,2} = \operatorname{lcm}(\#E_p(a,b), \#\overline{E_q(a,b)}) & \text{if } (w/p) = 1 \text{ and } (w/q) \neq 1 \\ N_{n,3} = \operatorname{lcm}(\#\overline{E_p(a,b)}, \#E_q(a,b)) & \text{if } (w/p) \neq 1 \text{ and } (w/q) = 1 \\ N_{n,4} = \operatorname{lcm}(\#\overline{E_p(a,b)}, \#\overline{E_q(a,b)}) & \text{if } (w/p) \neq 1 \text{ and } (w/q) \neq 1 \end{cases},$$

and $w = c_x^3 + ac_x + b \bmod n$.[***]

Remarks. 1) It is possible to construct a message independent cryptosystem by choosing p and q so that $\#E_p(a,b) = p + 1$ and $\#E_q(a,b) = q + 1$.
2) The computation of the second coordinate can be avoided if the algorithm described in [3] is used.

3 Description of the attack

At the rump session of Crypto '95, Franklin and Reiter [9] showed a protocol failure for RSA with a public encryption exponent equal to 3. This was later extended by Patarin [25, 6] for exponents up to $\simeq$ 32 bits. We shall generalize this kind of attack to protocols based on LUC and on elliptic curves over a ring.

[***] $\overline{E_p(a,b)}$ denotes the complementary group of $E_p(a,b)$.

3.1 Review of the attack

Suppose that two plaintexts M_1 and M_2 satisfy the known linear relation

$$M_2 = M_1 + \Delta,$$

and are encrypted with the same RSA function to produce the corresponding ciphertexts $C_1 = M_1^e \bmod n$ and $C_2 = M_2^e \bmod n$, respectively. An intruder can recover M_1 (and M_2) from C_1, C_2 and Δ as follows.

1. Let $\mathcal{P}$ and $\mathcal{Q}$ be the polynomials in the indeterminate x defined by
$$\mathcal{P}(x) = x^e - C_1 \quad \text{and} \quad \mathcal{Q}(x) = (x + \Delta)^e - C_2 \pmod{n}.$$
2. Since M_1 is a root of $\mathcal{P}$ and of $\mathcal{Q}$, the message M_1 will be a root of
$$\mathcal{R} = \gcd(\mathcal{P}, \mathcal{Q}).$$
Solving the polynomial $\mathcal{R}$, that is of degree 1 with a very high probability, will give the value of the plaintext M_1.

Example 1. 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 $M_2 = M_1 + \Delta$.

3.2 Extension to Lucas sequences

Let M_1 and $M_2 = M_1 + \Delta$ be two plaintexts encrypted by a LUC system to produce the ciphertexts $C_1 = V_e(M_1, 1) \bmod n$ and $C_2 = V_e(M_2, 1) \bmod n$, respectively.

Unlike RSA, the polynomial relation between the plaintext and the ciphertext is not explicitly given. We need the following proposition.

Proposition 1. *Let $\{V_k\}$ be the Lucas sequence with parameters P and $Q = 1$. Then*

$$V_k(P, 1) = P^k - \sum_{\substack{i=1 \\ i \text{ odd}}}^{k-2} \binom{k}{\frac{k-i}{2}} V_i(P, 1).$$

So, it is possible to express recursively $V_k(P, 1)$ as a polynomial of degree k in the indeterminate P. Consequently, the previous attack applies with $\mathcal{P}(x) = V_e(x, 1) - C_1$ and $\mathcal{Q}(x) = V_e(x + \Delta, 1) - C_2 \pmod{n}$.

Example 2. 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 $M_2 = M_1 + \Delta$.

3.3 Extension to elliptic curves

To extend the attack to elliptic curves, we need to introduce the division polynomials (see [30]). They allow to compute the multiple of a point in terms of the first coordinate.

Definition 2. The *division polynomials* $\Psi_m \in \mathbb{Z}[a, b, x, y]$, are inductively defined by

$$\begin{aligned}
\Psi_1 &= 1, \quad \Psi_2 = 2y, \quad \Psi_3 = 3x^4 + 6ax^2 + 12bx - a^2, \\
\Psi_4 &= 4y(x^6 + 5ax^4 + 20bx^3 - 5a^2x^2 - 4abx - 8b^2 - a^3), \\
\Psi_{2m+1} &= \Psi_{m+2}\Psi_m^3 - \Psi_{m-1}\Psi_{m+1}^2 \quad (m \geq 2), \\
2y\,\Psi_{2m} &= \Psi_m(\Psi_{m+2}\Psi_{m-1}^2 - \Psi_{m-2}\Psi_{m+1}^2) \quad (m \geq 2).
\end{aligned}$$

Proposition 3. *Let $E_n(a, b)$ be an elliptic curve over the ring $\mathbb{Z}_n$. Define the polynomials Φ_k and ω_k by*

$$\begin{aligned}
\Phi_k &= x\Psi_k^2 - \Psi_{k+1}\Psi_{k-1}, \\
4y\,\omega_k &= \Psi_{k+2}\Psi_{k-1}^2 - \Psi_{k-2}\Psi_{k+1}^2.
\end{aligned}$$

(a) Ψ_k, Φ_k, $y^{-1}\omega_k$ (for k odd) and $(2y)^{-1}\Psi_k$, Φ_k, ω_k (for k even) are polynomials in $\mathbb{Z}[a, b, x, y^2]$. Hence, by replacing y^2 by $x^3 + ax^2 + b$, they will be considered as polynomials in $\mathbb{Z}[a, b, x]$.

(b) As polynomials in x,

$$\begin{aligned}
\Phi_k(x) &= x^{k^2} + \textit{lower order terms}, \\
\Psi_k(x)^2 &= k^2 x^{k^2-1} + \textit{lower order terms}
\end{aligned}$$

are relatively prime polynomials.

(c) If $P \in E_n(a, b)$, then $kP = \left(\dfrac{\Phi_k(P)}{\Psi_k(P)^2}, \dfrac{\omega_k(P)}{\Psi_k(P)^3}\right) \pmod{n}$.

To illustrate the attack, we shall only focus on the first coordinate. Let $m_{1,x}$ and $m_{2,x} = m_{1,x} + \Delta$ be the first coordinates of two plaintexts M_1 and M_2, and let $c_{1,x}$ and $c_{2,x}$ be the first coordinates of the two corresponding ciphertexts $C_1 = eM_1$ and $C_2 = eM_2$, respectively.

By the previous proposition, we have

$$\Phi_e(m_{i,x}) - c_{i,x}\Psi_e(m_{i,x})^2 \equiv 0 \pmod{n} \qquad (i \in \{1, 2\}).$$

This relation allows to construct the following attack.

1. Let $\mathcal{P}$ and $\mathcal{Q}$ be the polynomials in the indeterminate x of degree e^2, defined by

   $\mathcal{P}(x) = \Phi_e(x) - c_{1,x}\Psi_e(x)^2$ and $\mathcal{Q}(x) = \Phi_e(x + \Delta) - c_{2,x}\Psi_e(x + \Delta)^2 \pmod{n}$.

2. We compute $\mathcal{R} = \gcd(\mathcal{P}, \mathcal{Q})$, which is with a very high probability, a polynomial of degree 1. Solving the polynomial $\mathcal{R}$ in x will give the value of $m_{1,x}$.

3.4 Analysis of the new attack

In [25], Patarin considered that, for the RSA, this attack applies with a public encryption exponent e up to typically 32 bits. From proposition 1, the same conclusion holds for LUC. However, this is not true for elliptic curves, 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 on elliptic curves will be as secure as a public exponent e of length 2ℓ for RSA or LUC.

On the other hand, from the polynomials $\mathcal{P}(x)$ and $\mathcal{Q}(x)$ defined as above, we can form the polynomial

$$\varrho(\varDelta) = \text{Resultant}_x(\mathcal{P}(x), \mathcal{Q}(x)) \pmod{n},$$

which is a univariate polynomial in $\varDelta$. As showed by Coppersmith in [5], if we call δ the degree of $\varrho(\varDelta)$, then it is possible to solve the polynomial ϱ as long as there is a solution less than about $n^{1/\delta}$. So, if the length of $\varDelta$ is less than $1/\delta$ times the length of the modulus n, then the technique of Coppersmith enables to recover M_1 (and M_2) even if the difference $\varDelta$ between the two plaintexts M_1 and M_2 is *unknown*. Since $\delta = e^2$ for the RSA and the LUC functions, and $\delta = e^4$ for the KMOV/Demytko's functions, the cryptosystems based on elliptic curves are more resistant against the attack of Coppersmith.

4 Conclusion

We have generalized a known attack for the RSA system, in the following way:

> *"If a cryptosystem enables to exhibit a non-trivial polynomial relationship, then we can form two polynomials from two related unknown messages to recover them."*

We have illustrated this attack on cryptosystems based on Lucas sequences and on elliptic curves over a ring.

Acknowledgments The authors are grateful to Daniel Bleichenbacher and to Richard Pinch for providing informations about the implementation and the security of the Lucas-based cryptosystems. Many thanks also to Don Coppersmith for showing how to solve a polynomial equation (modulo n).

References

1. Alfred V. Aho, John E. Hopcropft, and Jeffrey D. Ullman. *The design and analysis of computer programming.* Addison-Wesley, 1974.
2. Daniel Bleichenbacher, Wieb Bosma, and Arjen K. Lenstra. Some remarks on Lucas-based cryptosystems. In D. Coppersmith, editor, *Advances in Cryptology – CRYPTO '95*, vol. 963 of *Lecture Notes in Computer Science*, pp. 386–396, Springer-Verlag, 1995.

3. David M. Bressoud. *Factorization and primality testing.* Undergraduate Texts in Mathematics, Springer-Verlag, 1989.
4. Henri Cohen. *A course in computational algebraic number theory.* Number 138 in Graduate Texts in Mathematics. Springer-Verlag, 1993.
5. Don Coppersmith. Finding a small root of an univariate modular equation. *IBM Research Report*, RC 20223, Nov. 1995.
6. Don Coppersmith, Matthew Franklin, Jacques Patarin, and Michael Reiter. Low exponent RSA with related messages. To appear in EUROCRYPT '96.
7. N. Demytko. A new elliptic curve based analogue of RSA. In T. Helleseth, editor, *Advances in Cryptology – EUROCRYPT '95*, volume 765 of *Lecture Notes in Computer Science* pages 40–49. Springer-Verlag, 1993.
8. Whitfield Diffie, and Martin E. Hellman. New directions in Cryptography. *IEEE Trans. on Information Theory*, vol. IT-26, no. 6, pp. 644–654, Nov. 1976.
9. Matthew K. Franklin, and Michael K. Reiter. A linear protocol failure for RSA with exponent three. Preliminary note for *CRYPTO '95* rump session.
10. Johan Håstad. On using RSA with low exponent in a public key network. In H.C. Williams, editor, *Advances in Cryptology – CRYPTO '85*, vol. 218 of *Lecture Notes in Computer Science*, pp. 404–408, Springer-Verlag, 1986.
11. Dale Husemöller. *Elliptic curves.* Number 111 in Graduate Texts in Mathematics. Springer-Verlag, 1987.
12. Marc Joye, and Jean-Jacques Quisquater. Protocol failures for RSA-like functions using Lucas sequences and elliptic curves. *UCL Crypto Group Technical Report*, CG-1995/4, Dec. 1995.
13. Burton S. Kaliski, Jr. A chosen attack on Demytko's elliptic curve cryptosystem. To appear in Journal of Cryptology.
14. Donald E. Knuth. *The art of computer programming: Volume 2/Seminumerical algorithms.* 2nd ed., Reading, MA, Addison-Wesley Publishing Company, 1981.
15. Neal Koblitz. *A course in number theory and Cryptography.* Number 114 in Graduate Texts in Mathematics. Springer-Verlag, 2nd edition, 1994.
16. Kenji Koyama, Ueli M. Maurer, Tatsuaki Okamoto, and Scott 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.
17. H. Kuwakado, and K. Koyama. Security of RSA-type cryptosystems over elliptic curves against Håstad attack. *Electronics Letters*, vol. 30, no. 22, pp. 1843–1844, Oct. 1994.
18. C.-S. Laih, F-K. Tu, and W.-C. Tai. Remarks on LUC public key system. *Electronics Letters*, vol. 30, no. 2, pp. 123–124, Jan. 1994.
19. Chi-Sung Laih, Fu-Kuan Tu, and Wen-Chung Tai. On the security of the Lucas function. *Informations Processing Letters* 53, pp. 243–247, 1995.
20. Alfred Menezes, Minghua Qu, and Scott Vanstone. Standard for RSA, Diffie-Hellman and related public-key cryptography. Working draft of IEEE P1363 Standard, chapter 6, April 1995.
21. Alfred J. Menezes. *Elliptic curve public key Cryptosystems.* Kluwer Academic Publishers, 1993.
22. Winfried B. Müller, and Rupert Nöbauer. Some remarks on public-key cryptosystems. *Sci. Math. Hungar.*, vol. 16, pp. 71–76, 1981.
23. Winfried B. Müller, and Rupert Nöbauer. Cryptanalysis of the Dickson-scheme. In F. Pichler, editor, *Advances in Cryptology – EURORYPT '85*, vol. 219 of *Lecture Notes in Computer Science*, pp. 50–61, Springer-Verlag, 1986.

24. S. Murphy. Remarks on the LUC public key system. *Electronics Letters*, vol. 30, no, 7, pp. 558–559, March 1994.
25. Jacques Patarin. Some serious protocol failures for RSA with exponent e of less than $\simeq 32$ bits. Presented at the conference of cryptography, CIRM Luminy, France, 25–29 Sept. 1995.
26. R.G.E. Pinch. Extending the Håstad attack to LUC. *Electronics Letters*, vol. 31, no. 21, pp. 1827–1828, Oct. 1995.
27. Paulo Ribenboim. *The little book of big primes.* Springer-Verlag, 1991.
28. Hans Riesel. *Prime numbers and computers methods for factorization.* Progress in Mathematics, vol. 57, Birkhäuser, 1985.
29. R. L. Rivest, A. Shamir, and L. Adleman. A method for obtaining digital signatures and public-key cryptosystems. *Commun. ACM* 21, pp. 120–126, 1978.
30. Joseph H. Silverman. *The arithmetic of elliptic curves.* Number 106 in Graduate Texts in Mathematics. Springer-Verlag, 1986.
31. Peter J. Smith, and Michael J. J. Lennon. LUC: A new public key system. In E. G. Douglas, editor, *Ninth IFIP Symposium on Computer Security*, pp. 103–117, Elsevier Science Publishers, 1993.
32. Peter Smith. LUC public-key encryption. *Dr. Dobb's Journal*, pp. 44–49, Jan. 1993.

This article was processed using the LaTeX macro package with LLNCS style