ELSEVIER

Information Processing Letters 70 (1999) 153–156

Information Processing Letters

www.elsevier.com/locate/ipl

Common modulus and chosen-message attacks on public-key schemes with linear recurrence relations ☆

Wen-Guey Tzeng [1]

Department of Computer and Information Science, National Chiao Tung University, Hsinchu City 30050, Taiwan

Received 1 September 1998; received in revised form 1 January 1999
Communicated by S.G. Akl

Abstract

We consider the linear recurrence relation $V_t(x) = \sum_{i=1}^{m}(a_i x + b_i)V_{t-i}(x) + cx + f$ where $m \geqslant 1$, a_i and b_i, $1 \leqslant i \leqslant m$, are integers. The RSA and LUC schemes can be defined by this relation. In this paper we show that if the linear recurrence relation has some properties, the public-key scheme based on it cannot withstand the common modulus and chosen-message attacks, no matter what the order m is and what the parameters for a_i and b_i, $1 \leqslant i \leqslant m$, are. This implies that the LUC cryptosystem cannot withstand the common modulus attack and the LUC digital signature scheme cannot withstand the chosen-message attack.

Keywords: Cryptanalysis; Chosen-message attack; Common modulus attack; Linear recurrence relation; Cryptography

1. Introduction

We consider the linear recurrence relation

$$V_t(x) = \sum_{i=1}^{m}(a_i x + b_i)V_{t-i}(x) + cx + f,$$

where a_i, b_i, c and f, $1 \leqslant i \leqslant m$, are integers. In the RSA scheme [13], the encryption, decryption, signing and verification operations are of the form

$$V_t(M) = M^t \bmod n.$$

We observe that this form can be expressed as the first-order ($m = 1$) linear recurrence relation with $a_1 = 1$, $b_1 = 0$, $c = 0$, $f = 0$ and the initial value $V_0(x) = 1$. Similarly, the LUC scheme [15,16] can be expressed as the second-order ($m = 2$) linear recurrence relation with $a_1 = 1$, $b_1 = 0$, $a_2 = 0$, $b_2 = -1$, $c = 0$, $f = 0$ and initial values $V_0(x) = -2$ and $V_1(x) = x$.

Two well-known attacks on the RSA scheme are the common modulus attack on the RSA cryptosystem [14] and the chosen-message attack on the RSA signature scheme [3]. It has been shown that the LUC cryptosystem cannot withstand the chosen-message attack [2]. Other the other hand, to our best knowledge there is no known common modulus attack on the LUC cryptosystem in the open literature. In this paper we show that the LUC cryptosystem cannot withstand the common modulus attack either.

It has been discussed that the exponentiation in the RSA scheme that preserves the "multiplicative" property makes the scheme vulnerable to the chosen-message attack [3,5,6]. Therefore, there are proposed public-key schemes based on permutation polynomials [10–12] and Lucas functions [15,16] in order

☆ Research supported in part by the National Science Council grant NSC 87-2213-E009-055, Taiwan.

[1] Email: tzeng@cis.nctu.edu.tw.

0020-0190/99/$ – see front matter
PII: S0020-0190(99)00055-1

to prevent the weakness. However, Bleichenbacher et al. [2] showed that this is not necessarily true by providing a chosen-message attack on the LUC signature scheme. One might naturally try to choose different parameters for a_i, b_i, c and f, $1 \leqslant i \leqslant m$, or use a higher-order linear relation so that the public-key scheme with the linear recurrence relation can withstand the attacks. In this paper we show that if the linear recurrence relation has some properties, which are usually required for the public-key scheme to function, the public-key scheme with the linear recurrence relation cannot withstand the chosen-message and common modulus attacks no matter what the order m is and what the parameters are. In particular, we provide a general chosen-message attack and a general common modulus attack on the public-key scheme with a linear recurrence relation. These results show that the design of public-key schemes along the direction of Lucas-like functions is not feasible if the chosen-message and common modulus attacks are considered as major threats.

The LUC scheme has been attacked in many directions [2,9]. Its claimed advantages over the RSA scheme seem not existent. However, it might have one merit. Our common modulus attack on the LUC cryptosystem uses three pairwise relatively prime exponents. From the structure, we observe that the attack with two relatively prime exponents might not exist. If a cryptographic protocol uses RSA-like functions and suffers from the two-exponent common-modulus attack, one might use Lucas-like functions as an alternative.

2. Preliminaries

We first assume that the public-key scheme is designed along the RSA-like direction. The scheme serves two purposes, cryptosystem and digital signature, simultaneously. The operations of the scheme are on $\mathbb{Z}_n$, i.e., "mod n" with few exclusions on finding multiplicative inverses. In Section 5, we consider the schemes with operations on other algebraic objects. The requirements (assumptions) for our attacks to succeed are:

R1 (*efficiency*). Given a and x, $a \geqslant 0$, $0 < x < n$, $V_a(x) \bmod n$ is polynomial-time computable in the size of a and n. We assume that $V_{ab}(x) = V_a(V_b(x))$.

R2 (*commutativity*). $V_a(V_b(x)) = V_b(V_a(x))$. For a public-key scheme to be used as both cryptosystem and digital signature, this property is almost necessary.

R3 (*identity*). One can find pairs (e, d) so that $V_{ed}(x) \equiv x \pmod n$ for any value $0 < x \leqslant n$. This is to make the scheme work. Therefore, the encryption/verification key is e and the decryption/signing key is d.

Note that $V_a(V_b(x)) \bmod n = V_a(V_b(x) \bmod n) \bmod n$. By the requirements R1–R3, the scheme looks like the following.

Let $0 < M < n$ be the message. Then, the encryption is $C = V_e(M) \bmod n$, the decryption is $V_d(C) \bmod n$, the signing is $S = V_d(M) \bmod n$, and the verification is to verify whether $V_e(S) \bmod n$ is equal to M.

The RSA and LUC schemes both fit into this classification. In the RSA scheme the identity is computed by $ed \equiv 1 \bmod (p-1)(q-1)$ and in the LUC scheme it is computed by $ed \equiv 1 \bmod (p^2-1) \cdot (q^2-1)$.

3. Common modulus attacks

In implementating a public-key cryptosystem as described in Section 2, the system may use the same modulus n for every user so that user i has the public key (e_i, n) and private key (d_i, n). We note that a user with some (e_i, d_i) pair can factor the moduli n. If a message M is encrypted and sent to every user, the adversary (not one of the users) can use the public keys (e_i, n) and the ciphertexts $V_{e_i}(M) \bmod n$ to compute the plaintext M. We show that the public-key cryptosystem with an order-m linear recurrence relation that satisfies the requirements R1–R3 cannot withstand the common modulus attack with $m+1$ pairwise relatively prime exponents.

Let e_i, $1 \leqslant i \leqslant m+1$, be pairwise relatively prime. Assume that $0 < M < n$ and $\gcd(M, n) = 1$. We consider the system of equations:

$$r_i e_i - r_{i+1} e_{i+1} = 1, \quad 1 \leqslant i \leqslant m.$$

The integer solutions for r_i, $1 \leqslant i \leqslant m+1$, exist and can be found by Euclid's algorithm.

Lemma 1. *If* e_i, $1 \leqslant i \leqslant m+1$, *are pairwise relatively prime, then the system of equations*: $r_i e_i - r_{i+1} e_{i+1} = 1$, $1 \leqslant i \leqslant m$, *has integer solutions for* r_i, $1 \leqslant i \leqslant m+1$.

Proof. We prove this theorem by induction on m. For the induction base $m = 1$, since e_1 and e_2 are relatively prime, we use Euclid's algorithm to find an integer solution (r'_1, r'_2) for $r_1 e_1 - r_2 e_2 = 1$. For the induction hypothesis $m = k$, we assume that $(r'_1, r'_2, \ldots, r'_{k+1})$ is an integer solution for $r_i e_i - r_{i+1} e_{i+1} = 1$, $1 \leqslant i \leqslant k$. Let E_i be $e_1 e_2 \cdots e_{i-1} e_{i+1} \cdots e_{k+1}$. We can see that $(r'_1 + tE_1, r'_2 + tE_2, \ldots, r'_{k+1} + tE_{k+1})$ is also an integer solution for an arbitrary integer t. We consider the case $m = k+1$ now. For the first k equations $r_i e_i - r_{i+1} e_{i+1} = 1$, $1 \leqslant i \leqslant k$, we find integer solutions $(r'_1 + tE_1, r'_2 + tE_2, \ldots, r'_{k+1} + tE_{k+1})$ for an arbitrary integer t by the hypothesis. We then substitute $r'_{k+1} + tE_{k+1}$ for r_{k+1} in the $(k+1)$th equation $r_{k+1} e_{k+1} - r_{k+2} e_{k+2} = 1$ to obtain $(r'_{k+1} + tE_{k+1}) e_{k+1} - r_{k+2} e_{k+2} = 1$, which is $te_1 e_2 \cdots e_{k+1} - r_{k+2} e_{k+2} = 1 - r'_{k+1} e_{k+1}$. Since $\gcd(e_1 e_2 \cdots e_{k+1}, e_{k+2}) = 1$, we use Euclid's algorithm to find an integer solution (t', r'_{k+2}) for (t, r_{k+2}). Therefore, $(r'_1 + t'E_1, r'_2 + t'E_2, \ldots, r'_{k+1} + t'E_{k+1}, r'_{k+2})$ is an integer solution for $r_i e_i - r_{i+1} e_{i+1} = 1$, $1 \leqslant i \leqslant k+1$. □

Theorem 2. *The public-key cryptosystem with an order-m linear recurrence relation that satisfies the requirements* R1–R3 *cannot withstand the common modulus attack with* $m+1$ *pairwise relatively prime exponents.*

Proof. In fact, $r_i e_i$, $1 \leqslant i \leqslant m+1$, are $m+1$ consecutive numbers. If the adversary obtains the ciphertexts $V_{e_i}(M) \bmod n$, $1 \leqslant i \leqslant m+1$, it can compute the values $V_{r_i e_i}(M) \bmod n$, $1 \leqslant i \leqslant m+1$, in polynomial time. Therefore, the adversary can solve the linear equation

$$V_{r_1 e_1}(M) \bmod n = \left(\sum_{i=2}^{m+1} (a_i M + b_i) V_{r_i e_i}(M) + cM + f \right) \bmod n.$$

to obtain the message M. □

4. Chosen-message attacks

In the chosen-message attack, the adversary can query a signer to sign some messages and then uses the signed messages to deduce the signature of some other message of its choice.

Theorem 3. *If the public-key signature scheme with an order-m linear recurrence that satisfies the requirements* R1–R3, *then it cannot withstand the chosen-message attack with m queries.*

Proof. Let (d, n) be the signing key of the signer and (e, n) be the verification key. The adversary chooses a message M, $0 < M < n$ and $\gcd(M, n) = 1$. The adversary computes the values $V_{e-i}(M) \bmod n$ for $1 \leqslant i \leqslant m$ and asks the signer to sign them. It then uses the query results $V_d(V_{e-i}(M) \bmod n) \bmod n$, $1 \leqslant i \leqslant m$, for the equation

$$\begin{aligned} M &= V_{ed}(M) \bmod n \\ &= V_e\big(V_d(M)\big) \bmod n \\ &= \left(\sum_{i=1}^{m} \big(a_i V_d(M) + b_i\big) V_{e-i}\big(V_d(M)\big) + cV_d(M) + f \right) \bmod n \\ &= \left(\sum_{i=1}^{m} \big(a_i V_d(M) \bmod n + b_i\big) V_d \times \big(V_{e-i}(M) \bmod n\big) + cV_d(M) + f \right) \bmod n \end{aligned}$$

to solve $V_d(M) \bmod n$, which is the signature of the message M. □

5. Computing on other algebraic objects

We have illustrated our attacks on the public-key scheme with a linear recurrence relation that satisfies the requirements R1–R3 and is of operations on $\mathbb{Z}_n$. It can be extended to other algebraic objects if the algebraic objects satisfy the following criteria.

(1) For efficiency, the general operations, such as addition, multiplication, additive inverse, multiplicative inverse, should be able to be computed efficiently.

(2) For the trapdoor property (security), the operations, such as factoring and discrete logarithm, should be polynomially infeasible to compute.

The finite fields F_{p^m} and elliptic curves over a finite field satisfy the above criteria.

6. Conclusion and open problems

We would like to ask whether the LUC cryptosystem can withstand the common modulus attack with only two relatively prime exponents. This can be generalized to ask whether the public-key cryptosystem with an order-m linear recurrence relation can be attacked with less than $m + 1$ pairwise relatively prime exponents. We note that there exist e_1 and e_2, for example, $e_1 = 3$ and $e_2 = 4$, such that $r_1 e_i$, $r_2 e_j$ and $r_3 e_k$, $i, j, k \in \{1, 2\}$, cannot be three consecutive numbers. Therefore, our common modulus attack on the LUC cryptosystem cannot succeed with only two relatively prime exponents.

The similar questions can be asked about the chosen-message attack. What is the minimum number of queries needed for a successful chosen-message attack?

References

[1] D. Bleichenbacher, On the security of the KMOV public key cryptosystem, in: Proceedings of Advances in Cryptology—Crypto 97, Springer, Berlin, 1997, pp. 235–248.

[2] D. Bleichenbacher, W. Bosma, A.K. Lenstra, Some remarks on Lucas-based cryptosystems, in: Proceedings of Advances in Cryptology—Crypto 95, Springer, Berlin, 1995, pp. 386–396.

[3] G.I. Davida, Chosen signature cryptanalysis of the RSA (MIT) public key cryptosystem, Technical Report TR-CS-82-2, Department of Electrical Engineering and Computer Science, University of Wisconsin, Milwaukee, 1982.

[4] J.M. DeLaurentis, A further weakness in the common modulus protocol for the RSA cryptoalgorithm, Cryptologia 8 (1984) 253–259.

[5] D.E. Denning, Digital signatures with RSA and other public-key cryptosystems, Comm. ACM 27 (4) (1984) 388–392.

[6] Y. Desmedt, A.M. Odlyzko, A chosen text attack on the RSA cryptosystem and some discrete logarithm problems, in: Proceedings of Advances in Cryptology—Crypto 85, Springer, Berlin, 1986, pp. 516–522.

[7] B. Kaliski, A chosen message attack on Demytko's elliptic curve crytosystem, J. Cryptology 10 (1997) 71–72.

[8] D. Kravitz, I. Reed, Extension of RSA cryptostructure: a Galois approach, Electron. Lett. 18 (6) (1982) 255–256.

[9] C.-S. Laih, F.-K. Tu, W.-C. Tai, On the security of the Lucas function, Inform. Process. Lett. 53 (1995) 243–247.

[10] R. Lidl, W.B. Muller, Permutation polynomials in RSA-cryptosystems, in: Proceedings of Advances in Cryptology—Crypto 83, Plenum Press, 1984, pp. 293–301.

[11] W.B. Muller, W. Nobauer, Some remarks on public-key cryptosystem, Studia Sci. Math. Hungar. 16 (1981) 71–76.

[12] W.B. Muller, W. Nobauer, Cryptanalysis of the Dickson scheme, in: Proceedings of Advances in Cryptology—Eurocrypt 85, Springer, Berlin, 1986, pp. 50–61.

[13] R. Rivest, A. Shamir, L. Adleman, A method for obtaining digital signatures and public-key cryptosystems, Comm. ACM 21 (2) (1978) 120–126.

[14] G.J. Simmons, A "weak" privacy protocol using the RSA crypto algorithm, Cryptologia 7 (1983) 180–182.

[15] P. Smith, LUC public-key encryption, Dr. Dobb's J. 18 (1) (1993) 44–49.

[16] P. Smith, M.J. Lennon, LUC: a new public key system, in: Proc. 9th IFIP International Conference on Computer Security, North-Holland, Amsterdam, 1993, pp. 103–117.

[17] P. Smith, C. Skinner, A public-key cryptosystem and a digital signature system based on the Lucas function analogue to discrete logarithms, in: Proceedings of Advances in Cryptology—Asiacrypt 94, Springer, Berlin, 1995, pp. 357–364.