International Journal of Cryptology Research 1 (1): 33-41 (2009)

Garbage-Man-In-The-Middle Attack on the Luc_4 Cryptosystem

[1]Wong Tze Jin, [1]Mohamad Rushdan Md. Said, [2]Mohamed Othman, [1]Kamel Ariffin Mohd. Atan

[1]Institute for Mathematical Research, Universiti Putra Malaysia, 43400 Serdang, Selangor, Malaysia

[2]Faculty of Computer Science and Information Technology, Universiti Putra Malaysia, 43400 Serdang, Selangor, Malaysia

Email: tjwong1979@gmail.com

ABSTRACT

This paper reports an investigation into an attack on the LUC_4 cryptosystem. LUC_4 cryptosystem is derived from a fourth order linear recurrence relation and is based on the Lucas function. This cryptosystem is analogous to the RSA, LUC and LUC_3 cryptosystems. Therefore, the security for this cryptosystem is similar to the RSA cryptosystem because they are depend on the intractability of factorization. There are numerous mathematical attacks on RSA-type cryptosystem, one of them is polynomial attacks. The Garbage-man-in-the-middle attack is one of the polynomial attacks on LUC_4 cryptosystem. This type of attacks is exploiting the polynomial structure of RSA. Based on the analysis and implementations, the security aspects will be looked into and appear to depend on the intractability of factorization.

INTRODUCTION

LUC_4 cryptosystem [9] is analog to the RSA [7], LUC [6] and LUC_3 [5] cryptosystems, which is derived from a fourth order linear recurrence relation and based on the Lucas function. Therefore, the security of this cryptosystem is similar to the RSA cryptosystem because they are depend on the intractability of factorization. As we known, the security aspect is crucial part in the public key cryptosystem. There are numerous mathematical attacks on RSA-type cryptosystem, one of them is polynomial attacks. The polynomial attacks are exploiting the polynomial structure of RSA. And, the garbage-man-in-the-middle attack is one of the polynomial attacks. The aim of this research is to analyze and implement LUC_4 cryptosystem. Based on the analysis and implementations, the security aspects will be looked into and appear to depend on the intractability of factorization. There is a possibility that our research will accomplish the goal, which is decreasing the risk of losing our investment or secret information.

The basic idea of Garbage-man-in-the-middle 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 decrypt it. So, the receiver will discard it. If the cryptanalyst can get access

to this discard, the cryptanalyst 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 [2]. In many situations, we can get access to the discards, as for example,

- bad implementation of software or bad architectures;
- negligent secretaries;
- recovering of a previously deleted message, by a tool like the <undeleted> command with MS-DOS…

Suppose Alice wants to send a message m to Bob. Using Bob's public encryption key e, she computes $c \equiv E_e(m) \bmod n$, and sends it to Bob. Then, because only Bob knows the secret decryption key d, he can recover the message $m \equiv D_d(c) \bmod n$. However, a cryptanalyst (Carol) can also recover the message as follows. She intercepts the ciphertext c, and replaces it by $c' \equiv T_k(c) \bmod n$ where k is a random number. Then, when Bob will decrypt c', he will compute $m' = D_d(c') \bmod n$. Since the message m' is meaningless, he will discard it. Consequently, if carol can get access to m', she recovers the original message by computing $T_{k^{-1}}(m') \equiv D_d(c) \equiv m \bmod n$.

LUC$_4$ CRYPTOSYSTEM

As in the RSA, LUC and LUC$_3$ cryptosystem, the strength of the system to be constructed depends on the difficulty of factoring large number. Thus, it is necessary to pick two large secret primes p and q, the product of N which is part of the encryption key. Currently, the length of the keys is 2048-bits. The encryption key is (e, N) which is made public. Note that, e must be chosen so that it is relatively prime to the function $\Phi(N) = \overline{pq}$ because it is necessary to solve the congruence $ed \equiv 1 \bmod \Phi(N)$ to find the decoding key d. In practice, since $\Phi(N)$ depends on the type of an auxiliary polynomial, we choose e prime to $p-1$, $q-1$, $p+1$, $q+1$, p^2-1, q^2-1, p^3-1, q^3-1, p^3+p^2+p+1, q^3+q^2+q+1 to cover all possible cases.

With these preliminary observations, a public-key cryptosystem will be set out based on the quartic recurrence sequence V_n derived from the quartic polynomial,

$$x^4 - Px^3 + Qx^2 - Rx + S = 0 . \qquad (1)$$

The encryption function is defined by

$$\begin{aligned} E(P,Q,R) &= (V_e(P,Q,R,1), V_e(Q,PR-1,P^2+R^2-2Q,PR-1,Q,1), V_e(R,Q,P,1)) \\ &\equiv (C_1, C_2, C_3) \bmod N, \end{aligned} \tag{2}$$

where $N = pq$ as above, (P,Q,R) constitutes the message and the encryption key, (e,N). $V_e(P,Q,R,1)$ and $V_e(R,Q,P,1)$ are the e-th term of the quartic recurrence and $V_e(Q,PR-1,P^2+R^2-2Q,PR-1,Q,1)$ is e-th term of the sextic recurrence defined earlier.

The decryption key is (d,N) where d is the inverse of e modulo $\Phi(N)$. To decipher the message, the receiver must know or be able to compute $\Phi(N)$ and then calculate

$$\begin{aligned} &D(C_1, C_2, C_3) \\ &= (V_d(C_1, C_2, C_3, 1), V_d(C_2, C_1C_3-1, C_1^2+C_3^2-2C_2, C_1C_3-1, C_2, 1), V_d(C_3, C_2, C_1, 1)) \\ &\equiv (P,Q,R) \bmod N, \end{aligned} \tag{3}$$

which recovers the original message (P,Q,R).

In decryption, $g(x) = x^4 - C_1x^3 + C_2x^2 - C_3x + 1,$ is given but not $f(x) = x^4 - Px^3 + Qx^2 - Rx + 1$ and so we have to deduce the type of f in order to apply the algorithm correctly.

Example

The following example is an illustration that describe the details required in the computations to show how the system works.

Let $p = 23$ and $q = 29$ be two primes and thus, $N = 667$. Assume that the plaintext messages are $P = 17, Q = 7, R = 21$. The function f is given by $f(x) = x^4 - 17x^3 + 7x^2 - 21x + 1.$ If the encryption key is $e = 41$, then the sender calculates

$$\begin{aligned} C_1 &= V_e(P,Q,R,1) \\ &\equiv V_{41}(17,7,21,1) \bmod 667 \\ &\equiv 108 \bmod 667; \end{aligned}$$

$$\begin{aligned} C_2 &= V_e(Q, PR-1, P^2+R^2-2Q, PR-1, Q, 1) \\ &= V_{41}(7, 356, 716, 356, 7, 1) \bmod 667 \\ &\equiv 558 \bmod 667; \\ C_3 &= V_e(R, Q, P, 1) \\ &\equiv V_{41}(21, 7, 17, 1) \bmod 667 \\ &\equiv 249 \bmod 667; \end{aligned} \tag{4}$$

$$\begin{aligned} E(P,Q,R) &\equiv (C_1, C_2, C_3) \bmod N \\ &\equiv (108, 558, 249) \bmod 667. \end{aligned} \tag{5}$$

The receiver thus constructs the function $g(x) = x^4 - 108x^3 + 558x^2 - 249x + 1$. In order to determine the decryption key d, the owner of the encryption key $(41, 667)$ has to determine the function $\Phi(N)$ and, to this end, must deduce the type of the function f with respect to the primes p and q.

For prime $p = 23$, discriminant of g is $D \equiv 9 \bmod 23$, which is non-zero and this implies that f is of the same type as g, namely $t[1,1,1,1]$, since the function

$$\begin{aligned} g(x) &= x^4 - 108x^3 + 558x^2 - 249x + 1 \\ &\equiv x^4 + 7x^3 + 6x^2 + 4x + 1 \bmod 23 \\ &\equiv (x+13)(x+9)(x+6)(x+2) \bmod 23. \end{aligned} \tag{7}$$

(In fact,

$$\begin{aligned} f(x) &= x^4 - 17x^3 + 7x^2 - 21x + 1 \\ &\equiv x^4 + 6x^3 + 7x^2 + 2x + 1 \bmod 23 \\ &\equiv (x+13)(x+9)(x+4)(x+3) \bmod 23.) \end{aligned} \tag{8}$$

In case of the primes $q = 29$, discriminant of g is $D \equiv 28 \bmod 29$ which is non-zero and this implies that f is of the same type as g, namely $t[1,1,1,1]$, since the function

$$\begin{aligned} g(x) &= x^4 - 108x^3 + 558x^2 - 249x + 1 \\ &\equiv x^4 + 8x^3 + 7x^2 + 12x + 1 \bmod 29 \\ &\equiv (x+28)(x+19)(x+10)(x+9) \bmod 29. \end{aligned} \tag{9}$$

(In fact,

$$\begin{aligned} f(x) &= x^4 - 17x^3 + 7x^2 - 21x + 1 \\ &\equiv x^4 + 12x^3 + 7x^2 + 8x + 1 \bmod 29 \\ &\equiv (x+28)(x+26)(x+13)(x+3) \bmod 29.) \end{aligned} \tag{10}$$

Therefore,

$$\Phi(N) = \Phi(23 \bullet 29) = (23-1)(29-1) = 616, \tag{11}$$

and, the decryption key

$$\begin{aligned} ed &\equiv 1 \bmod \Phi(N) \\ 41d &\equiv 1 \bmod 616 \\ d &\equiv 41^{-1} \bmod 616 \\ &\equiv 601 \bmod 616 \end{aligned} \tag{12}$$

Now, the receiver can readily decrypt by computing

$$\begin{aligned} P &\equiv V_d(C_1, C_2, C_3, 1) \bmod N \\ &\equiv V_{601}(108, 558, 149, 1) \bmod 667 \\ &\equiv 17 \bmod 667; \\ Q &\equiv V_d(C_2, C_1C_3 - 1, C_1^{\,2} + C_3^{\,2} - 2C_2, C_1C_3 - 1, C_2, 1) \bmod N \\ &\equiv V_{601}(558, 211, 513, 211, 558, 1) \bmod 667 \\ &\equiv 7 \bmod 667; \\ R &\equiv V_d(C_3, C_2, C_1, 1) \bmod N \\ &\equiv V_{601}(149, 558, 108, 1) \bmod 667 \\ &\equiv 21 \bmod 667; \end{aligned} \tag{13}$$

$$\begin{aligned} D(C_1, C_2, C_3) &\equiv (17, 7, 21) \bmod 667 \\ &\equiv (P, Q, R) \bmod N. \end{aligned} \tag{14}$$

GARBAGE-MAN-IN-THE-MIDDLE ATTACK

Let the encryption and decryption functions are respectively defined by

$$\begin{aligned}(c_1, c_2, c_3) &= E(m_1, m_2, m_3) \\ &\equiv (V_e(m_1, m_2, m_3, 1), V_e(m_2, m_1 m_3 - 1, m_1^2 + m_3^2 - 2m_2, m_1 m_3 - 1, m_2, 1), \\ &\quad V_e(m_3, m_2, m_1, 1)) \bmod N,\end{aligned} \tag{15}$$

and

$$\begin{aligned}(m_1', m_2', m_3') &= D(c_1', c_2', c_3') \\ &\equiv (V_d(c_1', c_2', c_3', 1), V_d(c_2', c_1' c_3' - 1, c_1'^2 + c_3'^2 - 2c_2', c_1' c_3' - 1, c_2', 1), \\ &\quad V_d(c_3', c_2', c_1', 1)) \bmod N.\end{aligned} \tag{16}$$

In order to modify the ciphertext (c_1, c_2, c_3) into (c_1', c_2', c_3'), the cryptanalyst uses the transformation function

$$\begin{aligned}(c_1', c_2', c_3') &= T_k(c_1, c_2, c_3) \\ &\equiv (V_k(c_1, c_2, c_3, 1), V_k(c_2, c_1 c_3 - 1, c_1^2 + c_3^2 - 2c_2, c_1 c_3 - 1, c_2, 1), \\ &\quad V_k(c_3, c_2, c_1, 1)) \bmod N,\end{aligned} \tag{17}$$

where k is relatively prime to e and $\Phi(N)$. It is possible to express $V_k(x_1, x_2, x_3, 1)$, $V_k(x_3, x_2, x_1, 1)$, $V_k(x_2, x_1 x_3 - 1, x_1^2 + x_3^2 - 2x_2, x_1 x_3 - 1, x_2, 1)$. Consequently, to recover the messages (m_1, m_2, m_3), the cryptanalyst does the following.

Step 1:
Cryptanalyst intercepts (c_1, c_2, c_3) and replaces it by (c_1', c_2', c_3').

Step 2:
Next, cryptanalyst get from receiver the value of (m_1', m_2', m_3'), the plaintext corresponding to (c_1', c_2', c_3').

$$
\begin{aligned}
(m_1', m_2', m_3') &\equiv (V_d(c_1', c_2', c_3', 1), V_d(c_2', c_1'c_3' - 1, c_1'^2 + c_3'^2 - 2c_2', c_1'c_3' - 1, c_2', 1), \\
&\quad V_d(c_3', c_2', c_1', 1)) \bmod N \\
&\equiv (V_{dk}(c_1, c_2, c_3, 1), V_{dk}(c_2, c_1c_3 - 1, c_1^2 + c_3^2 - 2c_2, c_1c_3 - 1, c_2, 1), \\
&\quad V_{dk}(c_3, c_2, c_1, 1)) \bmod N \\
&\equiv (V_{dke}(m_1, m_2, m_3, 1), V_{dke}(m_2, m_1m_3 - 1, m_1^2 + m_3^2 - 2m_2, m_1m_3 - 1, m_2, 1), \\
&\quad V_{dke}(m_3, m_2, m_1, 1)) \bmod N \\
&\equiv (V_k(m_1, m_2, m_3, 1), V_k(m_2, m_1m_3 - 1, m_1^2 + \\
&\quad m_3^2 - 2m_2, m_1m_3 - 1, m_2, 1),\ V_k(m_3, m_2, m_1, 1)) \bmod N. \qquad (18)
\end{aligned}
$$

Step 3:
Cryptanalyst recover the original message (m_1, m_2, m_3) by

$$
\begin{aligned}
&D_{k^{-1}}(m_1', m_2', m_3') \\
&\equiv (V_{k^{-1}}(m_1', m_2', m_3', 1), V_{k^{-1}}(m_2', m_1'm_3' - 1, m_1'^2 + m_3'^2 - 2m_2', m_1'm_3' - 1, m_2', 1), \\
&\quad V_{k^{-1}}(m_3', m_2', m_1', 1)) \bmod N \\
&\equiv (V_{k^{-1}d}(c_1', c_2', c_3', 1), V_{k^{-1}d}(c_2', c_1'c_3' - 1, c_1'^2 + c_3'^2 - 2c_2', c_1'c_3' - 1, c_2', 1), \\
&\quad V_{k^{-1}d}(c_3', c_2', c_1', 1)) \bmod N \\
&\equiv (V_{k^{-1}kd}(c_1, c_2, c_3, 1), V_{k^{-1}kd}(c_2, c_1c_3 - 1, c_1^2 + c_3^2 - 2c_2, c_1c_3 - 1, c_2, 1), \\
&\quad V_{k^{-1}kd}(c_3, c_2, c_1, 1)) \bmod N \\
&\equiv (V_{k^{-1}kde}(m_1, m_2, m_3, 1), V_{k^{-1}kde}(m_2, m_1m_3 - 1, m_1^2 + m_3^2 - 2m_2, m_1m_3 - 1, m_2, 1), \\
&\quad V_{k^{-1}kde}(m_3, m_2, m_1, 1)) \bmod N \\
&\equiv (V_1(m_1, m_2, m_3, 1), V_1(m_2, m_1m_3 - 1, m_1^2 + m_3^2 - 2m_2, m_1m_3 - 1, m_2, 1), \\
&\quad V_1(m_3, m_2, m_1, 1)) \bmod N \\
&\equiv (m_1, m_2, m_3) \bmod N. \qquad (19)
\end{aligned}
$$

where k^{-1} is inverse of $k \bmod \Phi(N)$.

DISCUSSION AND FURTHER RESEARCH

The functions in garbage-man-in-the-middle attack on LUC_4 cryptosystem are more complexity, if we compare to RSA and LUC cryptosystems. This is because LUC_4 cryptosystem has three variables, but RSA and LUC cryptosystems have a variable only. The calculations to break the LUC_4 cryptosystem is more complicated than RSA and LUC cryptosystems.

For further research, we will be trying to find the data to prove that the LUC_4 cryptosystem is comparable to the RSA and LUC cryptosystems.

Beside that, we will be using other mathematical attacks to analyze the security of LUC_4 cryptosystem. We will propose how they were extended and will propose ways to minimize their effects and thus enables the user to evaluate the potential danger of a future attack on the LUC_4 cryptosystem.

ACKNOWLEDGEMENTS

I would like to thank National Science Fellowship (NSF) from Ministry of Science, Technology and Innovation (MOSTI) for they financial support.

REFERENCES

[1] Diffie, W. and Hellman, M. 1976. New directions in cryptography. *IEEE Trans. Inform. Theory*, IT-22(6), 644-654.

[2] G, Davida. 1982. Chosen signature cryptanalysis of the RSA (MIT) public key cryptosystem. *Tech. report TR-CS82-2*, Dept. of Electical Engineering and Computer Science, University of Wisconsin, Milwaukee, USA.

[3] Joye, M. and Quisquater, J. J. 1998. Cryptanalysis of RSA-type cryptosystems: a visit. *Network Threats, DIMACS Series in Discr. Math. ant Th. Comp. Sci., AMS*, 21-31.

[4] Joye, M. 1997. Security Analysis of RSA-type Cryptosystems. *PhD thesis, Universite Catholique de Louvain*, *Belgium.*

[5] Said, M. R. M and Loxton, J. 2003. A cubic analogue of the RSA cryptosystem. *Bulletin of the Australia Mathematical Society* 68, 21-38.

[6] Smith, P. J. and Lennon, M. J. J. 1993. LUC: A new public key system. *Proceedings of the ninth IFIP international Symposium on Computer Security*, 103-117.

[7] Rivest, R. , Shamir, A. and Adleman, L. 1978. A method for obtaining digital signatures and public key cryptosystems. *Comm. of the ACM* 21, 120-126.

[8] Williams, H. C. 1972. On a generalization of the Lucas functions. *Acta Arithmetica,* 20, 33-51.

[9] Wong, T. J. and Said, M. R. M. 2006. The fourth order linear recurrence sequence for RSA-type cryptosystem. *Master Thesis, Universiti Putra Malaysia, Malaysia.*