International Journal of Cryptology Research 1(2): 179-189 (2009)

GCD Attack on the LUC_4 Cryptosystem

[1]Wong Tze Jin, [2]Mohamad Rushdan Md. Said, [3]Mohamed Othman and [4]Kamel Ariffin Mohd. Atan

[1, 2, 4] *Institute for Mathematical Research, Universiti Putra Malaysia, 43400 UPM Serdang, Selangor, Malaysia.*

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

E-mail: [1]tjwong1979@gmail.com, [2]rushdan@math.upm.edu.my

ABSTRACT

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. This paper reports an investigation into the GCD attack on the LUC_4 cryptosystem and GCD attack is one of the polynomial attacks on LUC_4 cryptosystem. The GCD attack can succeed if two messages differ only from a known fixed value Δ and are RSA-encrypted under same RSA-modulus n.

INTRODUCTION

In 1978 Rivest, Shamir, and Adleman discovered the first practical public-key encryption and signature scheme, now referred to as RSA. The RSA scheme is based on another hard mathematical problem, the intractability of factoring large integers. This application of a hard mathematical problem to cryptography revitalized efforts to find more efficient methods to factor. The 1980s saw major advances in this area but none, which rendered the RSA system insecure. These are based on the discrete logarithm problem.

As we have known, the security is the crucial part of the cryptosystem. If we do not want to lose any investment or do not want to disclose any information which may be hacked by hacker, we require an extensively safe and secure cryptosystem. LUC_4 cryptosystem is a public key cryptosystem derived from the fourth order linear recurrence relation and analogue to the RSA and LUC cryptosystems. The aim of this research is to analyze and implement this system. 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 that goal. Thus, we will decrease the risk of losing our investment or secret information.

LUC_4 cryptosystem is analog to the RSA, LUC and LUC_3 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. As we know, the security aspect is a 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. The GCD attack is one of the polynomial attacks. The aim of this research is to analyze and implement LUC_4 cryptosystem. If two messages differ only from a known fixed value Δ and are RSA-encrypted under 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 different addressees;
- retransmission of a message with a new ID number due to an error…

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. 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,

$$x^4 - Px^3 + Qx^2 - Rx + S = 0. \tag{1}$$

Therefore, the quartic recurrence sequence define as

$$V_n(P, Q, R, S) = PV_{n-1} - QV_{n-2} + RV_{n-3} - SV_{n-4}, \quad \text{for } n > 4 \tag{2}$$

with initial values $V_0(P,Q,R,S) = 4$, $V_1(P,Q,R,S) = P$, $V_2(P,Q,R,S) = P^2 - 2Q$, and $V_3(P,Q,R,S) = P^3 - 3PQ + 3R$.

In LUC_4 cryptosystem, the sixth order of Lucas sequence is necessary to calculate the second plaintext. Therefore, we consider the sextic polynomial

$$x^6 - b_1x^5 + b_2x^4 - b_3x^3 + b_4x^2 - b_5x + b_6 = 0, \tag{3}$$

which help us to define the sixth order of Lucas sequence. Thus, the sextic recurrence sequence define as

$$V_n(b_1,b_2,b_3,b_4,b_5,b_6) = b_1V_{n-1} - b_2V_{n-2} + b_3V_{n-3} - b_4V_{n-4} + b_5V_{n-5} - b_6V_{n-6},$$
for $n > 6$, (4)

with initial values $V_0 = 6$, $V_1 = b_1$, $V_2 = b_1{}^2 - 2b_2$, $V_3 = b_1{}^3 - 3b_1b_2 + 3b_3$, $V_4 = b_1{}^4 - 4b_1{}^2b_2 + 2b_2{}^2 + 4b_1b_3 - 4b_4$, and $V_5 = b_1{}^5 - 5b_1{}^3b_2 + 5b_1b_2{}^2 + 5b_1{}^2b_3 - 5b_2b_3 - 5b_1b_4 + 5b_5$.

Now, the encryption function is defined by

$$\begin{aligned} &E(P,Q,R) \\ &= (V_e(P,Q,R,1), V_e(Q, PR-1, P^2+R^2-2Q, PR-1, Q, 1), V_e(R,Q,P,1)) \\ &\equiv (C_1, C_2, C_3) \bmod N, \end{aligned} \tag{5}$$

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

$$
\begin{aligned}
&D(C_1, C_2, C_3) \\
&= (V_d(C_1, C_2, C_3, 1), V_d(C_2, C_1C_3 - 1, C_1^{\ 2} + C_3^{\ 2} - 2C_2, C_1C_3 - 1, C_2, 1), \\
&\quad V_d(C_3, C_2, C_1, 1)) \\
&\equiv (P, Q, R) \bmod N,
\end{aligned} \tag{6}
$$

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.

GCD ATTACK

To succeed in the GCD attack, we need two plaintexts, which M_1 be the first plaintext and $M_2 = M_1 + \Delta$ be the second plaintext. Let the $C_1 = E(M_1)$ and $C_2 = E(M_2)$ be the corresponding ciphertexts. Then, the polynomial X and $Y \in Z_n[x]$ defined as

$$X(x) = E(x) - C_1 \text{ and } Y(x) = E(x + \Delta) - C_2 \tag{7}$$

Because of M_1 is the root of polynomial $X(x)$ and $Y(x)$, we will get the polynomial

$$W(x) = \gcd(X(x), Y(x)) = x - M_1. \tag{8}$$

Finally, solving the polynomial $W(x)$ will give the plaintexts M_1 and $M_2 = M_1 + \Delta$.

Now, let us use this idea to attack the LUC_4 cryptosystem. First, we choose (P_1, Q_1, R_1) to be the first set of the plaintext and $(P_2, Q_2, R_2) = (P_1 + \Delta, Q_1, +\Delta, R_1 + \Delta)$ be the second set of the plaintext and let $(C_{1,1}, Q_{1,2}, R_{1,3}) = E(P_1 + Q_1, +R_1) \bmod n$ and $(C_{2,1}, Q_{2,2}, R_{2,3}) = E(P_2 + Q_2, +R_2) \bmod n$ be the corresponding ciphertexts, where $E(P_i + Q_i, +R_i) \bmod n$ is the encryption function, which was defined previously and the encryption key e is relatively prime to n. Then, by the Dickson polynomial, the polynomial X_i and $Y_i \in Z_n[x_1, x_2, x_3]$ can be defined as

$$
\begin{aligned}
&X_1(x_1,x_2,x_3)\\
&\equiv V_e(x_1,x_2,x_3,1)-C_{1,1} \mod n\\
&\equiv V_e(x_1,x_2,x_3,1)-V_e(P_1,Q_1,R_1,1) \mod n\\
&\equiv \sum_{i=0}^{\lfloor \frac{e}{2}\rfloor}\sum_{j=0}^{\lfloor \frac{e}{2}\rfloor}\sum_{k=0}^{\lfloor \frac{e}{2}\rfloor}\left(\frac{e(-1)^{i+k}}{e-i-2j-3k}\right)\binom{e-i-2j-3k}{i+j+k}\binom{i+j+k}{i+j}\binom{i+j}{i}\\
&\quad \times x_1^{e-2i-3j-4k}x_2^{\,i}x_3^{\,j}\\
&\quad -\sum_{i=0}^{\lfloor \frac{e}{2}\rfloor}\sum_{j=0}^{\lfloor \frac{e}{2}\rfloor}\sum_{k=0}^{\lfloor \frac{e}{2}\rfloor}\left(\frac{e(-1)^{i+k}}{e-i-2j-3k}\right)\binom{e-i-2j-3k}{i+j+k}\binom{i+j+k}{i+j}\binom{i+j}{i}\\
&\quad \times P_1^{e-2i-3j-4k}Q_1^{\,i}R_1^{\,j} \mod n\\
&\equiv \sum_{i=0}^{\lfloor \frac{e}{2}\rfloor}\sum_{j=0}^{\lfloor \frac{e}{2}\rfloor}\sum_{k=0}^{\lfloor \frac{e}{2}\rfloor}\left(\frac{e(-1)^{i+k}}{e-i-2j-3k}\right)\binom{e-i-2j-3k}{i+j+k}\binom{i+j+k}{i+j}\binom{i+j}{i}\\
&\quad \times x_1^{e-2i-3j-4k}x_2^{\,i}x_3^{\,j}-P_1^{e-2i-3j-4k}Q_1^{\,i}R_1^{\,j} \mod n, \qquad (9)
\end{aligned}
$$

where $2i-3j-4k \le e.$

$$
\begin{aligned}
&X_3(x_1,x_2,x_3)\\
&\equiv V_e(x_3,x_2,x_1,1)-C_{1,3} \mod n\\
&\equiv V_e(x_3,x_2,x_1,1)-V_e(R_1,Q_1,P_1,1) \mod n\\
&\equiv \sum_{i=0}^{\lfloor \frac{e}{2}\rfloor}\sum_{j=0}^{\lfloor \frac{e}{2}\rfloor}\sum_{k=0}^{\lfloor \frac{e}{2}\rfloor}\left(\frac{e(-1)^{i+k}}{e-i-2j-3k}\right)\binom{e-i-2j-3k}{i+j+k}\binom{i+j+k}{i+j}\binom{i+j}{i}\\
&\quad \times x_3^{e-2i-3j-4k}x_2^{\,i}x_1^{\,j}\\
&\quad -\sum_{i=0}^{\lfloor \frac{e}{2}\rfloor}\sum_{j=0}^{\lfloor \frac{e}{2}\rfloor}\sum_{k=0}^{\lfloor \frac{e}{2}\rfloor}\left(\frac{e(-1)^{i+k}}{e-i-2j-3k}\right)\binom{e-i-2j-3k}{i+j+k}\binom{i+j+k}{i+j}\binom{i+j}{i}\\
&\quad \times R_1^{e-2i-3j-4k}Q_1^{\,i}P_1^{\,j} \mod n\\
&\equiv \sum_{i=0}^{\lfloor \frac{e}{2}\rfloor}\sum_{j=0}^{\lfloor \frac{e}{2}\rfloor}\sum_{k=0}^{\lfloor \frac{e}{2}\rfloor}\left(\frac{e(-1)^{i+k}}{e-i-2j-3k}\right)\binom{e-i-2j-3k}{i+j+k}\binom{i+j+k}{i+j}\binom{i+j}{i}
\end{aligned}
$$

$$\times\ x_3^{\ e-2i-3j-4k} x_2^{\ i} x_1^{\ j} - R_1^{\ e-2i-3j-4k} Q_1^{\ i} P_1^{\ j} \mod n, \tag{10}$$

where $2i-3j-4k \le e.$

$$\begin{aligned}
&Y_1(x_1, x_2, x_3)\\
&\equiv V_e(x_1+\Delta, x_2+\Delta, x_3+\Delta, 1) - C_{2,1} \mod n\\
&\equiv V_e(x_1+\Delta, x_2+\Delta, x_3+\Delta, 1) - V_e(P_1+\Delta, Q_1+\Delta, R_1+\Delta, 1) \mod n\\
&\equiv \sum_{i=0}^{\lfloor \frac{e}{2} \rfloor}\sum_{j=0}^{\lfloor \frac{e}{2} \rfloor}\sum_{k=0}^{\lfloor \frac{e}{2} \rfloor}\left(\frac{e(-1)^{i+k}}{e-i-2j-3k}\right)\binom{e-i-2j-3k}{i+j+k}\binom{i+j+k}{i+j}\binom{i+j}{i}\\
&\quad \times\ (x_1+\Delta)^{e-2i-3j-4k}(x_2+\Delta)^i(x_3+\Delta)^j\\
&\quad -\sum_{i=0}^{\lfloor \frac{e}{2} \rfloor}\sum_{j=0}^{\lfloor \frac{e}{2} \rfloor}\sum_{k=0}^{\lfloor \frac{e}{2} \rfloor}\left(\frac{e(-1)^{i+k}}{e-i-2j-3k}\right)\binom{e-i-2j-3k}{i+j+k}\binom{i+j+k}{i+j}\binom{i+j}{i}\\
&\quad \times\ (P_1+\Delta)^{e-2i-3j-4k}(Q_1+\Delta)^i(R_1+\Delta)^j \mod n\\
&\equiv \sum_{i=0}^{\lfloor \frac{e}{2} \rfloor}\sum_{j=0}^{\lfloor \frac{e}{2} \rfloor}\sum_{k=0}^{\lfloor \frac{e}{2} \rfloor}\left(\frac{e(-1)^{i+k}}{e-i-2j-3k}\right)\binom{e-i-2j-3k}{i+j+k}\binom{i+j+k}{i+j}\binom{i+j}{i}\\
&\quad \times\ [(x_1+\Delta)^{e-2i-3j-4k}(x_2+\Delta)^i(x_3+\Delta)^j\\
&\quad -(P_1+\Delta)^{e-2i-3j-4k}(Q_1+\Delta)^i(R_1+\Delta)^j] \mod n, \quad (11)
\end{aligned}$$

where $2i-3j-4k \le e.$

$$\begin{aligned}
&Y_3(x_1, x_2, x_3)\\
&\equiv V_e(x_3+\Delta, x_2+\Delta, x_1+\Delta, 1) - C_{2,3} \mod n\\
&\equiv V_e(x_3+\Delta, x_2+\Delta, x_1+\Delta, 1) - V_e(R_1+\Delta, Q_1+\Delta, P_1+\Delta, 1) \mod n\\
&\equiv \sum_{i=0}^{\lfloor \frac{e}{2} \rfloor}\sum_{j=0}^{\lfloor \frac{e}{2} \rfloor}\sum_{k=0}^{\lfloor \frac{e}{2} \rfloor}\left(\frac{e(-1)^{i+k}}{e-i-2j-3k}\right)\binom{e-i-2j-3k}{i+j+k}\binom{i+j+k}{i+j}\binom{i+j}{i}\\
&\quad \times\ (x_3+\Delta)^{e-2i-3j-4k}(x_2+\Delta)^i(x_1+\Delta)^j\\
&\quad -\sum_{i=0}^{\lfloor \frac{e}{2} \rfloor}\sum_{j=0}^{\lfloor \frac{e}{2} \rfloor}\sum_{k=0}^{\lfloor \frac{e}{2} \rfloor}\left(\frac{e(-1)^{i+k}}{e-i-2j-3k}\right)\binom{e-i-2j-3k}{i+j+k}\binom{i+j+k}{i+j}\binom{i+j}{i}
\end{aligned}$$

$$
\begin{aligned}
&\times (R_1+\Delta)^{e-2i-3j-4k}(Q_1+\Delta)^i(P_1+\Delta)^j \bmod n \\
&\equiv \sum_{i=0}^{\lfloor \frac{e}{2} \rfloor}\sum_{j=0}^{\lfloor \frac{e}{2} \rfloor}\sum_{k=0}^{\lfloor \frac{e}{2} \rfloor}\left(\frac{e(-1)^{i+k}}{e-i-2j-3k}\right)\binom{e-i-2j-3k}{i+j+k}\binom{i+j+k}{i+j}\binom{i+j}{i} \\
&\times [(x_3+\Delta)^{e-2i-3j-4k}(x_2+\Delta)^i(x_1+\Delta)^j \\
&-(R_1+\Delta)^{e-2i-3j-4k}(Q_1+\Delta)^i(P_1+\Delta)^j] \bmod n, \qquad (12)
\end{aligned}
$$

where $2i-3j-4k \le e.$

$$
\begin{aligned}
&X_2(x_1,x_2,x_3) \\
&\equiv V_e(x_2, x_1x_3-1, x_1^2+x_3^2-2x_2, x_1x_3-1, x_2, 1) - C_{1,2} \bmod n \\
&\equiv V_e(x_2, x_1x_3-1, x_1^2+x_3^2-2x_2, x_1x_3-1, x_2, 1) \\
&-V_e(Q_1, P_1R_1-1, P_1^2+R_1^2-2Q_1, P_1R_1-1, Q_1, 1) \bmod n \\
&\equiv \sum_{i_1=0}^{\lfloor \frac{e}{2} \rfloor}\sum_{i_2=0}^{\lfloor \frac{e}{3} \rfloor}\sum_{i_3=0}^{\lfloor \frac{e}{4} \rfloor}\sum_{i_4=0}^{\lfloor \frac{e}{5} \rfloor}\sum_{i_5=0}^{\lfloor \frac{e}{6} \rfloor}\left(\frac{e(-1)^{i_1+i_3+i_5}}{e-i_1-2i_2-3i_3-4i_4-5i_5}\right) \\
&\times \binom{e-i_1-2i_2-3i_3-4i_4-5i_5}{i_1+i_2+i_3+i_4+i_5}\binom{i_1+i_2+i_3+i_4+i_5}{i_1+i_2+i_3+i_4} \\
&\times \binom{i_1+i_2+i_3+i_4}{i_1+i_2+i_3}\binom{i_1+i_2+i_3}{i_1+i_2}\binom{i_1+i_2}{i_1}(x_2)^{e-i_1-2i_2-3i_3-4i_4-5i_5} \\
&\times (x_1x_3-1)^{i_1+i_3}(x_1^2+x_3^2-2x_2)^{i_2} \\
&-\sum_{i_1=0}^{\lfloor \frac{e}{2} \rfloor}\sum_{i_2=0}^{\lfloor \frac{e}{3} \rfloor}\sum_{i_3=0}^{\lfloor \frac{e}{4} \rfloor}\sum_{i_4=0}^{\lfloor \frac{e}{5} \rfloor}\sum_{i_5=0}^{\lfloor \frac{e}{6} \rfloor}\left(\frac{e(-1)^{i_1+i_3+i_5}}{e-i_1-2i_2-3i_3-4i_4-5i_5}\right) \\
&\times \binom{e-i_1-2i_2-3i_3-4i_4-5i_5}{i_1+i_2+i_3+i_4+i_5}\binom{i_1+i_2+i_3+i_4+i_5}{i_1+i_2+i_3+i_4} \\
&\times \binom{i_1+i_2+i_3+i_4}{i_1+i_2+i_3}\binom{i_1+i_2+i_3}{i_1+i_2}\binom{i_1+i_2}{i_1}(Q_1)^{e-i_1-2i_2-3i_3-4i_4-5i_5} \\
&\times (P_1R_1-1)^{i_1+i_3}(P_1^2+R_1^2-2Q_1)^{i_2} \bmod n
\end{aligned}
$$

$$\equiv \sum_{i_1=0}^{\lfloor \frac{e}{2} \rfloor} \sum_{i_2=0}^{\lfloor \frac{e}{3} \rfloor} \sum_{i_3=0}^{\lfloor \frac{e}{4} \rfloor} \sum_{i_4=0}^{\lfloor \frac{e}{5} \rfloor} \sum_{i_5=0}^{\lfloor \frac{e}{6} \rfloor} \left(\frac{e(-1)^{i_1+i_3+i_5}}{e-i_1-2i_2-3i_3-4i_4-5i_5} \right)$$
$$\times \binom{e-i_1-2i_2-3i_3-4i_4-5i_5}{i_1+i_2+i_3+i_4+i_5} \binom{i_1+i_2+i_3+i_4+i_5}{i_1+i_2+i_3+i_4}$$
$$\times \binom{i_1+i_2+i_3+i_4}{i_1+i_2+i_3} \binom{i_1+i_2+i_3}{i_1+i_2} \binom{i_1+i_2}{i_1}$$
$$\times [(x_2)^{e-i_1-2i_2-3i_3-4i_4-5i_5} (x_1x_3-1)^{i_1+i_3} ({x_1}^2+{x_3}^2-2x_2)^{i_2}$$
$$-(Q_1)^{e-i_1-2i_2-3i_3-4i_4-5i_5} (P_1R_1-1)^{i_1+i_3} (P_1^2+{R_1}^2-2Q_1)^{i_2}] \bmod n, \tag{13}$$

where $2i_1-3i_2-4i_3-5i_4-6i_5 \le e.$

$$Y_2(x_1,x_2,x_3)$$
$$\equiv V_e(x_2+\Delta,(x_1+\Delta)(x_3+\Delta)-1,(x_1+\Delta)^2+(x_3+\Delta)^2-2(x_2+\Delta),$$
$$(x_1+\Delta)(x_3+\Delta)-1,x_2+\Delta,1)-C_{1,2} \bmod n$$
$$\equiv V_e(x_2+\Delta,(x_1+\Delta)(x_3+\Delta)-1,(x_1+\Delta)^2+(x_3+\Delta)^2-2(x_2+\Delta),$$
$$(x_1+\Delta)(x_3+\Delta)-1,x_2+\Delta,1)$$
$$-V_e((Q_1+\Delta),(P_1+\Delta)(R_1+\Delta)-1,(P_1+\Delta)^2+(R_1+\Delta)^2-2(Q_1+\Delta),$$
$$(P_1+\Delta)(R_1+\Delta)-1,(Q_1+\Delta),1) \bmod n$$
$$\equiv \sum_{i_1=0}^{\lfloor \frac{e}{2} \rfloor} \sum_{i_2=0}^{\lfloor \frac{e}{3} \rfloor} \sum_{i_3=0}^{\lfloor \frac{e}{4} \rfloor} \sum_{i_4=0}^{\lfloor \frac{e}{5} \rfloor} \sum_{i_5=0}^{\lfloor \frac{e}{6} \rfloor} \left(\frac{e(-1)^{i_1+i_3+i_5}}{e-i_1-2i_2-3i_3-4i_4-5i_5} \right)$$
$$\times \binom{e-i_1-2i_2-3i_3-4i_4-5i_5}{i_1+i_2+i_3+i_4+i_5} \binom{i_1+i_2+i_3+i_4+i_5}{i_1+i_2+i_3+i_4}$$
$$\times \binom{i_1+i_2+i_3+i_4}{i_1+i_2+i_3} \binom{i_1+i_2+i_3}{i_1+i_2} \binom{i_1+i_2}{i_1} (x_2+\Delta)^{e-i_1-2i_2-3i_3-4i_4-5i_5}$$
$$\times ((x_1+\Delta)(x_3+\Delta)-1)^{i_1+i_3} ((x_1+\Delta)^2+(x_3+\Delta)^2-2(x_2+\Delta))^{i_2}$$

$$-\sum_{i_1=0}^{\lfloor\frac{e}{2}\rfloor}\sum_{i_2=0}^{\lfloor\frac{e}{3}\rfloor}\sum_{i_3=0}^{\lfloor\frac{e}{4}\rfloor}\sum_{i_4=0}^{\lfloor\frac{e}{5}\rfloor}\sum_{i_5=0}^{\lfloor\frac{e}{6}\rfloor}\left(\frac{e(-1)^{i_1+i_3+i_5}}{e-i_1-2i_2-3i_3-4i_4-5i_5}\right)$$
$$\times\binom{e-i_1-2i_2-3i_3-4i_4-5i_5}{i_1+i_2+i_3+i_4+i_5}\binom{i_1+i_2+i_3+i_4+i_5}{i_1+i_2+i_3+i_4}$$
$$\times\binom{i_1+i_2+i_3+i_4}{i_1+i_2+i_3}\binom{i_1+i_2+i_3}{i_1+i_2}\binom{i_1+i_2}{i_1}(Q_1+\Delta)^{e-i_1-2i_2-3i_3-4i_4-5i_5}$$
$$\times((P_1+\Delta)(R_1+\Delta)-1)^{i_1+i_3}$$
$$\times((P_1+\Delta)^2+(R_1+\Delta)^2-2(Q_1+\Delta))^{i_2} \bmod n$$
$$\equiv\sum_{i_1=0}^{\lfloor\frac{e}{2}\rfloor}\sum_{i_2=0}^{\lfloor\frac{e}{3}\rfloor}\sum_{i_3=0}^{\lfloor\frac{e}{4}\rfloor}\sum_{i_4=0}^{\lfloor\frac{e}{5}\rfloor}\sum_{i_5=0}^{\lfloor\frac{e}{6}\rfloor}\left(\frac{e(-1)^{i_1+i_3+i_5}}{e-i_1-2i_2-3i_3-4i_4-5i_5}\right)$$
$$\times\binom{e-i_1-2i_2-3i_3-4i_4-5i_5}{i_1+i_2+i_3+i_4+i_5}\binom{i_1+i_2+i_3+i_4+i_5}{i_1+i_2+i_3+i_4}$$
$$\times\binom{i_1+i_2+i_3+i_4}{i_1+i_2+i_3}\binom{i_1+i_2+i_3}{i_1+i_2}\binom{i_1+i_2}{i_1}$$
$$\times[(x_2+\Delta)^{e-i_1-2i_2-3i_3-4i_4-5i_5}((x_1+\Delta)(x_3+\Delta)-1)^{i_1+i_3}$$
$$\times((x_1+\Delta)^2+(x_3+\Delta)^2-2(x_2+\Delta))^{i_2}$$
$$-(Q_1+\Delta)^{e-i_1-2i_2-3i_3-4i_4-5i_5}((P_1+\Delta)(R_1+\Delta)-1)^{i_1+i_3}$$
$$((P_1+\Delta)^2+(R_1+\Delta)^2-2(Q_1+\Delta))^{i_2}] \bmod n, \tag{14}$$

where $2i_1-3i_2-4i_3-5i_4-6i_5\le e.$

Since the equations (9), (10), (11), (12), (13), and (14) do not have linear factor, then

$$\begin{aligned}W_i &= \gcd(X_i(x_1,x_2,x_3),\ Y_1(x_1,x_2,x_3)),\ \text{for } i=1,2,3\\ &\neq x_i-M_i,\end{aligned} \tag{15}$$

where $M_1 = P_1$, $M_2 = Q_1$, and $M_3 = R_1$. Thus, GCD attack cannot succeed on LUC_4 cryptosystem.

DISCUSSION AND FURTHER RESEARCH

In this respect, we are able to make a conclusion, which is the security of LUC_4 cryptosystems is good enough to protect our information. This is because it does not allow the cryptanalyst to hack our information by GCD attack. Therefore, the cryptanalyst cannot get any information from this attack if we are using the LUC4 cryptosystem to encrypt our information.

For further research, 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 their financial support.

REFERENCES

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

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

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.

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.

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

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.

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

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.*