Electronics and Communications in Japan, Part 3, Vol. 77, No. 12, 1994
Translated from Denshi Joho Tsushin Gakkai Ronbunshi, Vol. 77-A, No. 3, March 1994, pp. 471-475

A New Method for Breaking the Lu-Lee Cryptosystem

Akira Hayashi and Hideo Shimizu, *Members*

Kanazawa Institute of Technology, Ishikawa, Japan 921

SUMMARY

The authors present a method to break the Lu-Lee (LL) cryptosystem, whose security is based on the difficulty of factoring the product of large primes. Previously, other methods of attacking the LL cryptosystem have been proposed, but the new method proposed here is different from them. In the present method, the computation required is polynomial-time and computer experiments make it clear that all the cipher text can be broken with high speed. In this method, the authors construct simultaneous congruences from the encryption congruence and then transform these into simultaneous equations, whose solution gives the original plain text. The authors do require a condition for the transformation into equations, but it is satisfied in almost all cases; so the probability of success of the attack can be considered to be high.

Key words: Cryptosystems; public-key cryptosystems; cryptologic attacks; Lu-Lee cryptosystem.

1. Introduction

Since the general idea of public-key cryptosystems was proposed by Diffie and Hellman [1], the Lu-Lee cryptosystem [2] is one of the fastest cryptosystems which has been designed. Other cryptosystems which have been proposed include the RSA cryptosystem [3], Merkle-Hellman cryptosystem [4], and McEliece cryptosystem [5]. The bases for the security of these differ, and each has some sort of disadvantage.

First, an effective attack on the RSA cryptosystem has not yet been discovered but there is only circumstantial evidence for its security. Overall, it is regarded as one of the public-key cryptosystems having the best prospects. However, its encryption and decryption require the operation of modular exponentiation; hence, a lot of computation, so its slowness is the fly in the ointment. Research into speeding up the operation has been stimulated vigorously in various places, but the problems cannot yet be said to have been overcome.

Data expansion is a problem for the Merkle-Hellman cryptosystem; that is, the problem of relatively low efficiency, whether encryption and decryption can be performed at high speed. However, Shamir [6] gave a method for attacking this cryptosystem. Finally, it is not known whether the decryption method utilized by the McEliece cryptosystem, used for none of the other types of systems, is efficient for general linear codes. The complexity of encryption and decryption is the disadvantage of this system.

The cryptosystem proposed by Lu and Lee utilizes the Chinese Remainder Theorem and, as mentioned above, its security is based on the difficulty of factoring large composite numbers. That is, in the Lu-Lee (LL) cryptosystem encryption and decryption can easily be

ISSN1042-0967/94/0012-0050

implemented at high speed, and it has a comparatively small data expansion.

However, methods for breaking the LL cryptosystem have been proposed, among which are those of Adelman and Rivest [7], Goethals and Couvreur [8], and Kochanski [9]. In the method of Goethals and Couvreur [8], the decryption key is determined utilizing the fact that the public key relative to the secret moduli have small remainders. The original references [7, 9] for the other two methods do not provide details, but in these methods, the plain text seems to be determined from the cipher text without determination of the decryption key.

The proposers of the LL cryptosystem did not prove its security under attack. In this paper, in addition to the three above-mentioned methods, we offer another breaking method. This method differs from the method of Goethals and Couvreur and also from the method of Adleman and Rivest and the method of Kochanski, so seems to be new. Although the insecurity of the cryptosystem has already been shown, the presentation of another attacking method may be useful in the design of new cryptosystems and in research on other cryptographic attacks and countermeasures against this attack may be useful. It is significant in exactly the same way as the existence of various proofs of a theorem in mathematics; the significance of this paper should be considered in this way. Note that in our method the conversion of the encryption congruence into simultaneous equations was suggested by Theorem 2.1 of Frieze et al. [10].

The organization of this paper is as follows. In section 2, the LL cryptosystem is explained; and the breaking method is proposed in section 3. A numerical example of the attack and experimental results with computers are described in section 4. In section 5, we study the amount of computation for the proposed method and a condition for its validity.

2. The Lu-Lee Cryptosystem

Following [2], we briefly sketch the Lu-Lee cryptosystem.

Secret key: Two large primes p_1 and p_2 and comparatively small positive integers a_{11}, a_{12}, a_{21}, and a_{22}, such that $a_{11}a_{22} \neq a_{12}a_{21}$.

Public key: Positive integers a_1, a_2, n, M_1, and M_2. Here, $n = p_1p_2$, $a_1 < n$ and $a_2 < n$ are positive integers satisfying

$$\begin{cases} a_i \equiv a_{1i} \pmod{p_1} \\ a_i \equiv a_{2i} \pmod{p_2}, \quad i=1, 2 \end{cases}$$

and

$$M_i = \left\lfloor \frac{1}{2} \min\left\{ \frac{p}{a_{1i}}, \frac{p}{a_{2i}} \right\} \right\rfloor, \quad i=1, 2 \tag{1}$$

where $p = \min\{p_1, p_2\}$.

Plaintext space: The plaintext space $\mathcal{M}$ is the set of integers given by

$$\mathcal{M} = \{(m_1, m_2) | 0 \leq m_1 \leq M_1, 0 \leq m_2 \leq M_2\}$$

Encryption: Encryption is a mapping E from $\mathcal{M}$ to $\mathbf{Z}_n = \{0, 1, \cdots, n-1\}$ for which the cipher text c is given by

$$c = E((m_1, m_2)) = a_1m_1 + a_2m_2 \bmod n \tag{2}$$

Note that E is an injection.

Decryption: First compute

$$c_i = c \bmod p_i, \quad i=1, 2$$

then solve the simultaneous equations

$$\begin{cases} a_{11}x_1 + a_{12}x_2 = c_1 \\ a_{21}x_1 + a_{22}x_2 = c_2 \end{cases} \tag{3}$$

The solutions x_1 and x_2 are the plaintext (m_1, m_2): $x_1 = m_1$ and $x_2 = m_2$.

Note that the a_{ij} of the Lu-Lee system are designed to be fairly small compared to p_1 and p_2. From Eq. (1) we see that, as the a_{ij} becomes large, M_1 and M_2 become small, the plaintext space narrows and, hence, data expansion becomes large. The attack of Goethals and Couvreur [8], as sketched briefly above, utilizes the fact that the a_{ij} are comparatively small.

Also from Eqs. (2) and (3), we know that the encryption and decryption operations of the LL cryptosystem can be performed very much faster than those of the RSA cryptosystem.

3. The Breaking Method

In our breaking method, the secret key of the cryptosystem is not revealed; instead, for a received

cipher text, the corresponding plaintext (m_1, m_2) is discovered. That is accomplished by the algorithm **BrkLL**, which accepts as input the public keys a_1, a_2, and n and the cipher text c and outputs either the correct plaintext or "FAILURE."

Algorithm **BrkLL**.

① Transform the encryption congruence (4) into the simultaneous congruences (8).

② Transform the simultaneous congruences (8) into the simultaneous two-variable equations (15).

③ Solve the simultaneous equations (15). If the solution belongs to $\mathcal{M}$, output that solution as plaintext, otherwise output "FAILURE."

Note that it is unnecessary, in steps ① and ②, to compute the matrices A and B for each ciphertext; instead the computations are performed only once for a fixed cryptosystem. Below we describe the details of the algorithm.

3.1. Transformation into simultaneous congruences

We first consider how to find the plaintext (m_1, m_2) in the solution set $\mathcal{X}$ of the congruence

$$a_1x_1 + a_2x_2 \equiv c \pmod{n} \tag{4}$$

In fact, we cannot specify the correct plaintext (m_1, m_2) in $\mathcal{X}$ with only Eq. (4). As information supplementary to Eq. (4), we utilize the following fact:

- As solution of Eq. (4), we need to consider only positive integers (x_1, x_2).

This information seems to be unnecessary, but it is not since it is not clearly expressed in Eq. (4) that both x_1 and x_2 are integers.

Necessary and sufficient conditions that the solutions are integers are given by

$$nx_1 \equiv 0 \pmod{n} \tag{5}$$

and

$$nx_2 \equiv 0 \pmod{n} \tag{6}$$

Reorganizing the above, the three congruences (4), (5), and (6) hold simultaneously.

From the above three simultaneous congruences, an equivalent set of two congruences can be derived since both sides of Eq. (4) can be multiplied by the multiplicative inverse a_2^{-1} of a_2 mod n, transforming Eq. (4) into

$$a_0x_1 + x_2 \equiv c' \pmod{n} \tag{7}$$

where

$$a_0 = a_2^{-1}a_1 \bmod n$$

and

$$c' = a_2^{-1}c \bmod n$$

Note that a_2^{-1} mode n exists since $(a_2, n) = 1$.

By the above transformation, we can replace the simultaneous congruences (4), (5), and (6) by the simultaneous congruences (7) and (5); that is, (6) is unnecessary. Thus, if x_1 is an integer, then it follows from Eq. (7) that x_2 is also an integer. By the above, we need only find $x = (x_1, x_2)$, which satisfies the simultaneous congruences

$$Ax^T \equiv \begin{pmatrix} c' \\ 0 \end{pmatrix} \pmod{n}, \tag{8}$$

where

$$A = \begin{pmatrix} a_0 & 1 \\ n & 0 \end{pmatrix}. \tag{9}$$

3.2. Transformation into simultaneous equations

Next, we find a solution which exists for the maximum M_1 and M_2, then use it to transform the simultaneous congruences (8) into simultaneous equations. The coefficients of (8) must thereby be transformed into small quantities. That is, by means of a unimodular matrix Q, we transform A into B (for example, see [11, chapter 5] and [12, chapter 2]):

$$B = Q^TA, \tag{10}$$

where

$$Q = \begin{pmatrix} p & q \\ r & s \end{pmatrix}$$

By a unimodular matrix, we mean a matrix whose determinant has absolute value 1.

We are looking for B, whose two rows, the vectors $\boldsymbol{b}_1$ and $\boldsymbol{b}_2$, are short in the Euclidean norm $\|\cdot\|$. In particular, we choose $\boldsymbol{b}_1$ and $\boldsymbol{b}_2$ to be the shortest basis vectors for the lattice $L(A)$ spanned by the two rows of A. Thus, we can either choose a "small B" or find Q as described next.

The square $f(t, u)$ of the Euclidean norm of a linear combination of the two row vectors $(a_0, 1)$ and $(n, 0)$ of A is

$$\begin{aligned} f(t, u) &= (a_0 t + nu)^2 + t^2 \\ &= \alpha t^2 + \beta tu + \gamma u^2 \end{aligned} \tag{11}$$

where

$$\alpha = a_0^2 + 1, \quad \beta = 2a_0 n, \quad \gamma = n^2 \tag{12}$$

Denote f by (α, β, γ). Or we could put $\boldsymbol{u} = (t, u)$; then, since

$$AA^T = \begin{pmatrix} \alpha & \beta/2 \\ \beta/2 & \gamma \end{pmatrix}$$

we can write

$$f(\boldsymbol{u}) = \boldsymbol{u} A A^T \boldsymbol{u}^T$$

The quadratic form $f(\boldsymbol{u})$ is positive definite, so since $\boldsymbol{u} \neq \boldsymbol{0}$, we have $f(\boldsymbol{u}) > 0$. Thus, because $\alpha > 0$, the discriminant D is negative since

$$D = \beta^2 - 4\alpha\gamma = -4n^2 < 0$$

We say that a quadratic form is *reduced* in the case that one or the other of

(1) $-\alpha < \beta \leqq \alpha < \gamma$

or

(2) $0 \leqq \beta \leqq \alpha = \gamma$

holds.

If the positive definite quadratic form $g(t, u) = \alpha t^2 + \beta tu + \gamma u^2$ is a reduced quadratic form, then the two smallest nonzero values it assumes are $g(1, 0) = \alpha$ and $g(0, 1) = \gamma$. Therefore, we infer that the smallest B is found by reducing the quadratic form (11).

Below, we present a reduction algorithm **Red** [13] which for a quadratic form $f = (\alpha, \beta, \gamma)$ successively applies either the unimodular transformation

$$Q_1 = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$$

or the unimodular transformation

$$Q_2 = \begin{pmatrix} 1 & -k \\ 0 & 1 \end{pmatrix}$$

to produce a reduced quadratic form g. Since the product of unimodular matrices is again unimodular, any such transformation Q is unimodular.

Reduction algorithm **Red**.

① Apply the transformation Q_2, replacing (α, β, γ) by $(\alpha, \beta - 2k\alpha, \gamma + k^2\alpha - k\beta)$, where $k \in \boldsymbol{Z}$ is an integer and $-\alpha < \beta - 2k\alpha \leqq \alpha$.

② If (α, β, γ) is reduced, STOP; otherwise, apply the transformation Q_1, replacing (α, β, γ) with $(\gamma, -\beta, \alpha)$, and return to **1**.

The values assumed by the reduced quadratic form g obtained from the above procedure are the same as those of the original quadratic form f:

$$g(\boldsymbol{u}') = \boldsymbol{u}' B B^T \boldsymbol{u}'^T = \boldsymbol{u}' Q^T A A^T Q \boldsymbol{u}'^T = f(\boldsymbol{u})$$

where

$$\boldsymbol{u} = \boldsymbol{u}' Q^T$$

The two smallest values of g are taken on at $\boldsymbol{u}' = (1, 0)$ and $\boldsymbol{u}' = (0, 1)$ which correspond in the original $\boldsymbol{u}$ to $\boldsymbol{u}_1 = (1, 0)Q^T = (p, r)$ and $\boldsymbol{u}_2 = (0, 1)Q^T = (q, s)$.

By the above, we obtain

$$B = \begin{pmatrix} pa_0 + rn & p \\ qa_0 + sn & q \end{pmatrix}$$

Transforming the right side of the congruence (8) also by means of Q,

$$\mathbf{c} = (c_1, c_2) = (pc', qc')$$

In this way the congruence (8) is transformed into

$$B\mathbf{x}^T \equiv \mathbf{c}^T \pmod{n} \tag{13}$$

Here, the two row vectors $\boldsymbol{b}_1$ and $\boldsymbol{b}_2$ of B are of sufficiently small length so that

$$\|\boldsymbol{b}_i\|\,\|\boldsymbol{x}\| < n/2, \quad i=1, 2 \tag{14}$$

hold. Then, if we assume that the absolute value of the least residue (pc', qc') is in the interval $(-n/2, n/2)$, then the congruence (13) becomes an equation

$$B\boldsymbol{x}^T = \boldsymbol{c}^T \tag{15}$$

4. A Numerical Example and Some Computer Experiments

In this section, we illustrate applications of our method proposed in section 3 by a numerical example, then use some computer experiments to describe the probability of success of the attack.

4.1. A numerical example

We consider the application of the proposed method to the example of Lu and Lee [2].

Secret key: $p_1 = 97$, $p_2 = 103$, $a_{11} = 3$, $a_{12} = 2$, $a_{21} = 5$, $a_{22} = 4$.

Public key: $n = 9991$, $a_1 = 3301$, $a_2 = 3300$, $M_1 = 9$, $M_2 = 12$.

Encryption: When $m_1 = 7$ and $m_2 = 5$, we get $c = 9634$.

Attack: Solve $3301x_1 + 3300x_2 \equiv 9634 \pmod{9991}$ as follows. For

$$A' = \begin{pmatrix} a_1 & a_2 \\ n & 0 \\ 0 & n \end{pmatrix}$$

$a_2^{-1} \bmod n = 3300^{-1} \bmod 9991 = 2086$ and $a_0 = a_2^{-1}a_1 \bmod n = 2086 \times 3301 \bmod 9991 = 2087$. Therefore, we obtain

$$A = \begin{bmatrix} 2087 & 1 \\ 9991 & 0 \end{bmatrix}$$

Also transform the cipher text $c = 9634$ into

$$c' = a_2^{-1}c \bmod n = 2086 \times 9634 \bmod 9991 = 4623$$

Reduce the quadratic form $f(\boldsymbol{u}) = \boldsymbol{u}AA^T\boldsymbol{u}^T$ by finding the unimodular matrix

$$Q = \begin{bmatrix} p & q \\ r & s \end{bmatrix} = \begin{bmatrix} 67 & 91 \\ -14 & -19 \end{bmatrix}$$

Hence,

$$B = Q^TA = \begin{bmatrix} 67 & -14 \\ 91 & -19 \end{bmatrix}\begin{bmatrix} 2087 & 1 \\ 9991 & 0 \end{bmatrix} = \begin{bmatrix} -45 & 67 \\ 88 & 91 \end{bmatrix}$$

and

$$\boldsymbol{c}^T = \begin{bmatrix} pc' \\ qc' \end{bmatrix} = \begin{bmatrix} 67 \times 4623 \\ 91 \times 4623 \end{bmatrix} \equiv \begin{bmatrix} 20 \\ 1071 \end{bmatrix} \pmod{9991}$$

Thus, we obtain the equations

$$\begin{pmatrix} -45 & 67 \\ 88 & 91 \end{pmatrix}\begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} 20 \\ 1071 \end{pmatrix}$$

which we must solve. Their unique solution is

$$x_1 = 7, \quad x_2 = 5,$$

in agreement with the original plaintext (m_1, m_2).

4.2. Computer experiments

Experiment 1. For the numerical example of [2] treated in the preceding section, we tried our method of attack when the plaintext space to be enciphered is $\mathcal{M} = \{(m_1, m_2) \mid 0 \leq m_1 \leq 9,\ 0 \leq m_2 \leq 12\}$. The result was that, from each of the 130 cipher texts, the correct plaintext could be recovered.

Experiment 2. For a larger example, let $p_1 = 104{,}729$, $p_2 = 104{,}759$, and $n = 10{,}971{,}305{,}311$. Also choose the a_{ij} to be of the order of 100: $a_{11} = 123$, $a_{12} = 91$, $a_{21} = 73$, and $a_{22} = 153$; thus, $a_1 = 7{,}314{,}378{,}212$, $a_2 = 10{,}239{,}668{,}608$, $M_1 = 425$, and $M_2 = 342$.

As in Experiment 1, we encrypted all the plaintexts in the plaintext space and tried this attack. We succeeded on all 146,118 cipher texts.

Experiment 3. We did an experiment using the sizes actually recommended for values of the parameters in the Lu-Lee system. We chose the 100-digit primes $p_1 = 10^{99} + 289$ and $p_2 = 10^{99} + 303$, and let a_{ij} be of the order of 100. The attack could break all the cipher texts of 1000 randomly chosen plaintexts.

5. Investigations

We do not know whether the validity of condition (14) is sufficient for the transform of the simultaneous congruences (13) to the simultaneous equations (15). Also, we should consider if this is a necessary condition.

First, we investigate the size of the determined solution $\boldsymbol{x}$. Since $\boldsymbol{x} \in \mathcal{M}$, we have $\|\boldsymbol{x}\| \leq \sqrt{M_1^2 + M_2^2}$. In addition, from Eq. (1), M_1 and M_2 satisfy the inequalities

$$0 < M_1, M_2 < \mu\sqrt{n}, \quad \mu < 1/2$$

Therefore, $\|\boldsymbol{x}\| \leq \mu\sqrt{2n}$.

Next, we consider the lengths of the vectors $\boldsymbol{b}_1$ and $\boldsymbol{b}_2$. According to the theory of quadratic forms [12],

$$\|\mathbf{b}_1\| \leq \left(\frac{|D|}{3}\right)^{\frac{1}{4}} = \left(\frac{4}{3}\right)^{\frac{1}{4}} \sqrt{n}$$

and

$$\|\boldsymbol{b}_1\| \, \|\boldsymbol{b}_2\| \leq \sqrt{\frac{|D|}{3}} = \sqrt{\frac{4}{3}}\, n$$

Using the above inequalities we cannot bound $|\boldsymbol{b}_2|$ from above.

We investigate $\|\boldsymbol{b}_2\| = \varepsilon\sqrt{n}$ with computer experiments. With the same p_1 and p_2 as in experiment 2 of section 4.2, and in the case that 1000 sets of a_{ij} are chosen randomly in [100, 1000), 77 percent of the time $1 \leq \varepsilon < 2$, and the largest ε which occurred was $\varepsilon < 64$. On the other hand, we can suppose that, since $a_{ij} \geq 100$, $\mu = 1/200$, so $\|\boldsymbol{x}\| < \sqrt{2n}/200$. Therefore, the right-side of Eq. (15) is $< 64\sqrt{n}\sqrt{2n}/200 < n/2$, so the assumption (14) for the transformation of the congruences into the equations is valid.

If the amount of computation of the attack were not polynomial-time, then this method could not be said to be effective. This is dominated by the amount of computation in the proposed algorithm **BrkLL** and in the quadratic-form-reduction algorithm **Red**. Applying a result of [14], the number of steps in our case is $O(\log n)$; that is, the number of steps is bounded by the number of digits in the modulus of the cryptosystem. In addition, recall that the preliminary computations are performed only once. Obviously, the operations performed on each cipher text can be performed at high speed.

6. Conclusions

We have given a new breaking method for the cryptosystem proposed by Lu and Lee. We obtain simultaneous equations from the published encryption congruence, then find the plain text by solving them. The amount of computation in the attack is polynomial-time, and the effectiveness of the attacking method has been verified by computer experiments. The same technique may be applied to other cryptosystems. Also, we hope that this method of attack may provide a suggestion for the construction of a secure linear cryptosystem.

Acknowledgement. Part of this research was carried out with aid from the Kanazawa Technology Research Center and from the Toshiba Corporation, to whom we express our thanks.

REFERENCES

1. W. Diffie and M. E. Hellman. New directions in cryptography. IEEE Trans. Info. Theory., **IT-22**, 6, pp. 644-654 (Nov. 1976).
2. S. C. Lu and L. N. Lee. A simple and effective public-key cryptosystem. COMSAT Tech. Rev., **9**, pp. 15-24 (1979).
3. R. L. Rivest, A. Shamir, and L. Adleman. A method of obtaining digital signatures and public key cryptosystems. Comm. of ACM, **21**, 2, pp. 120-126 (Feb. 1978).
4. R. C. Merkle and M. E. Hellman. Hiding information and signatures in trapdoor knapsacks. IEEE Trans. Inf. Theory, **IT-24**, 5, pp. 525-530 (Sept. 1978).
5. R. J. McEliece. A public-key cryptosystem based on algebraic coding theory. DSN Progress Rep., pp. 42-44. Jet Propulsion Lab. (Jan.-Feb. 1978).
6. A. Shamir. A polynomial time algorithm for breaking the basic Merkle-Hellman cryptosystem. IEEE Trans. Inf. Theory, **IT-30**, 5, pp. 699-704 (1984).

7. L. M. Adleman and R. L. Rivest. How to break the Lu-Lee (COMSAT) public-key cryptosystem. MIT Laboratory for Computer Science (July 1979).
8. J. M. Goethals and C. Couvreur. A cryptoanalytic attack on the Lu-Lee public-key cryposystem. Phillips J. Res., **35**, pp. 301-306 (1980).
9. M. J. Kochanski. Remarks on Lu and Lee's Proposals. Cryptologia, **4**, 4, pp. 204-207 (1980).
10. A. M. Frieze, J. Hastad, R. Kannan, J. C. Lagarias, and A. Shamir. Reconstructing truncated integer variables satisfying linear congruences. SIAM J. Comput., **17**, 2, pp. 262-280 (April 1988).
11. A. Baker. A concise introduction to the theory of numbers. Cambridge University Press (1984).
12. J. W. S. Cassels. An introduction to the geometry of numbers. Springer-Verlag (1971).
13. A. K. Lenstra and H. W. Lenstra, Jr. Algorithms in Number Theory. In: Handbook of Theoretical Computer Science, Vol. A, Algorithms and Complexity, Chapter 12, pp. 673-715 (Ed. J. Van Leeuwen). The MIT Press/Elsevier (1990).
14. J. C. Lagarias. Worst-case complexity bounds for algorithms in the theory of integral quadratic forms. J. Algorithms, **1**, pp. 142-186 (1980).

AUTHORS (from left to right)

Akira Hayashi graduated from Kanazawa University in Electronics Engineering in 1964. In 1973, he completed his M.A. at the University of Minnesota, and in 1976, a Ph.D. at the University of Hawaii. He joined Toshiba Research in 1964; and then, in 1970, he became a Lecturer at Kanazawa University where, since 1977, he has been a Professor in the Department of Information Engineering. He has interest in acoustic engineering, communications theory, information theory, and coding theory. He is a member of the Information Processing Institute, the Institute for Information Theory and its Applications, and the IEEE.

Hideo Shimizu graduated from Kanazawa University in Information Engineering in 1988 and, in 1990, completed his M.A. at the same university, where he is currently enrolled in the Ph.D. program. His area of research is computer science, particularly information security.