Cryptanalysis of a Public Key Cryptosystem Proposed at ACISP 2000

Amr Youssef[1] and Guang Gong[2]

[1] Center for Applied Cryptographic Research
Department of Combinatorics & Optimization
[2] Department of Electrical and Computer Engineering
University of Waterloo
Waterloo, Ontario N2L 3G1, CANADA
{a2youssef,ggong}@cacr.math.uwaterloo.ca

Abstract. At ACISP 2000, Yoo *et al* proposed a fast public key cryptosystem using matrices over a ring. The authors claim that the security of their system is based on the RSA problem. In this paper we present a heuristic attack that enables us to recover the private key from the public key. In particular, we show that breaking the system can be reduced to finding a short vector in a lattice which can be achieved using the L^3-lattice reduction algorithm.

Key words: public key cryptography, cryptanalysis, L^3-algorithm

1 Introduction

Most practical public key schemes are very slow compared to symmetric key schemes. This motivates extensive research for faster public key schemes. Several lattice-based systems such as [1], [2] are among these schemes. Both of these schemes, which are based on the closest vector problem and the shortest vector problem [6] [7] are broken using the L^3 lattice reduction algorithm. In fact, the L^3 algorithm was successfully used to attack many similar public key systems [5]. Yoo *et al* [11] proposed a fast public key cryptosystem similar to the system proposed in [2]. However, they claim that since the security of their scheme is based on the RSA problem and not the lattice problems, their scheme is secure against these lattice basis reduction attacks. In this paper we show that breaking this system is equivalent to the problem of finding a short vector in a lattice which can be solved using the L^3-lattice reduction algorithm [4]. In particular, our heuristic attack enables us to recover the private key from the public key and hence represent a total break for the proposed system.
The paper is organized as follows. In section 2 we give a description for the system proposed in [11]. In section 3, we describe our attack. Finally we give a numerical example using the same parameters of the encryption-decryption example in [11].

V. Varadharajan and Y. Mu (Eds.): ACISP 2001, LNCS 2119, pp. 15–20, 2001.

2 Description of the Proposed Scheme

In this section we review the proposed public key scheme. Further details and justification for the bounds on the parameters can be found in [11].
Let n be the dimension of a lattice. The basic steps to choose the parameters are as follows:
1 Choose positive integers $\hat{m}, \hat{e}, d_{ii},\ 1 \leq i \leq n$, primes p, q and a matrix $D \in Mat_n(\mathbb{Z})$ with the following conditions:
1.1 $N = pq$.
1.2 $\hat{m}, \hat{e}$: random integers such that $\hat{m} \approx q^{0.4}, \hat{e} \approx q^{0.3}$, where $\hat{m}$ and $\hat{e}$ are upper bounds of messages and error vectors respectively.
1.3 D : diagonal matrix such that $\hat{m} < |d_{ii}| < q^{0.5}$, where $d_{ii}, 1 \leq i \leq n$ are diagonal entries of D.
2 Choose an invertible matrix $T = (t_{ij})_{1 \leq i,j \leq n} \in Mat_n(\mathbb{Z})$ such that $\sum_{j=1}^{n} t_{ij} < q^{0.2}$.
3 Form the matrices $R = DT$ and $B = B_q UL \bmod N$ where $B_q = R^{-1} \bmod q$, L (respectively U) are uni-modular lower (respectively upper) triangular matrix whose all entries except the diagonal entries are multiples of q.

$B, \hat{e}, \hat{m}$ and N are public information. R, q and T are kept secret.

Encryption: Let $M = (m_1, \cdots, m_n)^t, 0 \leq m_i < \hat{m}$ be a message vector and $E = (e_1, \cdots e_n)^t, 0 \leq e_i < \hat{e}$ be an arbitrary error vector. Then the ciphertext is

$$C = (BM + E) \bmod N.$$

Decryption: At first compute $X = (x_1, \cdots, x_n)^t$:

$$C_q = C \bmod q,$$

$$X = RC_q \bmod q.$$

Then $m_i = x_i (\bmod\ d_{ii})_{1 \leq i \leq n}$.

3 Attacking the Scheme

In this section we will present a heuristic attack that enables us to recover the private key from the public key. In particular, this attack enables us to factor N using the matrix B only. As mentioned in [11], once q is revealed, one can find B_q and D and the system is totally broken. Recall that

$$B^{-1} \bmod q = R.$$

The following lemma follows by noting that for $N = pq$ and for any integer a we have

$$a \bmod q = (a \bmod N) \bmod q.$$

Let $V = B^{-1} \bmod N$. Then we have

Lemma 1.

$$V\ mod\ q = (B^{-1}\ mod\ N)\ mod\ q = (B^{-1}\ mod\ q) = R.$$

Let r_{max} denote $\max_{\{i,j\}} |r_{ij}|$. Then from Section 3 in [11] we have

$$r_{max} < \frac{q-\hat{m}}{n\hat{e}} \approx \frac{q-q^{0.4}}{nq^{0.3}} < q^{0.7}.$$

Thus every element of the matrix V can be represented as

$$v_{ij} = a_{ij}q + r_{ij},$$

where $0 \le a_{ij} < p, r_{ij} < r_{max}, 1 \le i,j \le n$.

The basic steps in the attack are as follows:

1. Calculate the matrix $V = B^{-1}$ mod N.

2. Pick an $m, m \le n^2$, elements from the set $\{v_{ij}\}_{\{1 \le i,j \le n\}}$. Let $S = \{s_i\}_{\{1 \le i \le m\}}$ denote the set formed from the elements above.

3. Use the L^3 algorithm to find a reduced basis B for the $(m+1)$-dimensional lattice L which is generated by the rows of the matrix

$$\begin{bmatrix} N & 0 & 0 & \cdots & 0 & 0 \\ 0 & N & 0 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & N & 0 \\ -s_1 & -s_2 & -s_3 & \cdots & -s_m & 1 \end{bmatrix}.$$

4. For each row $l = (l_1, l_2, \cdots, l_m, l_{m+1})$ in B such that $l_{m+1} \ne N$ do the following:

- Evaluate $gcd(N, l_{m+1})$.
- If $gcd(N, l_{m+1}) \ne 1$, return $p = gcd(N, l_{m+1})$.

5. Return (Failure).

The following lemma is used to justify the success of the attack.

Lemma 2. *The vector*

$$x = ((a_1N - ps_1), (a_2N - ps_2), \cdots, (a_mN - ps_m), p) = (-p\delta_1, -p\delta_2, \cdots, -p\delta_m, p)$$

is in L and has length less than approximately $(\sqrt{m+1}\ pq^{0.7})$.

Proof. The first part follows by noting that x is a linear combination of the rows of L. The second part follows by noting that each of the elements s_i can be represented as $s_i = a_iq + \delta_i$ where $\delta_i < q^{0.7}$.

Note that our lattice has dimension $(m+1)$ and volume N^m. From the lemma above, x is short compared to the $(m+1)^{th}$ root of the volume of the lattice. Hence, there is a good possibility that the L^3 algorithm will produce a reduced basis which include the vector x. If no solution exists then we can try another subset of elements $\{v_{ij}\}$. Our experimental results show that the L^3 algorithm finds p with high probability.

Let $\{b_1, b_2, \cdots, b_{m+1}\}$ denote the basis of the lattice L above. Let $C \in \mathbb{R}$ be such that $|b_i|^2 \leq C$ for $i = 1, 2, \cdots m+1$ and $|b_i|$ denote the length of the basis b_i. From [4], the number of arithmetic operations needed by the L^3 algorithm is $O((m+1)^4 logC)$, on integers of size $O((m+1)logC)$.

Remark 1. The lattice used in step 3 is the standard lattice used in the Simultaneous Diophantine Approximation (SDA) [4]. I.e., our problem can also be formulated in terms of SDA. It was noted by Nguyen and Shparlinski [9] that this formulation leads to unconditional provable attack provided that p and q are much unbalanced ($q > p^{10/3}$) because we would have an unusually good SDA (See Fact 3.107 in [4]). In fact, in this case, we can easily solve the problem using the continuous fraction approximation [3]. It was also noted in [9] that while the attack in [8] can be applied to this cryptosystem, it is not an improvement of our attack and our attack is much simpler in this case.

4 Numerical Example

In order to illustrate the steps in our cryptanalysis, we will use the same numerical example given in [11]. Let $q = 10570841$ and $p = 10570837$. Then $N = 111742637163917$. Let

$$D = \begin{bmatrix} 612 & 0 & 0 & 0 \\ 0 & 681 & 0 & 0 \\ 0 & 0 & 697 & 0 \\ 0 & 0 & 0 & 601 \end{bmatrix},$$

and

$$T = \begin{bmatrix} 5 & 2 & 3 & 7 \\ 4 & 3 & 1 & 2 \\ 4 & 7 & 1 & 3 \\ 2 & 3 & 4 & 9 \end{bmatrix}.$$

Then

$$R = \begin{bmatrix} 3060 & 1224 & 1836 & 4284 \\ 2724 & 2043 & 681 & 1362 \\ 2788 & 4879 & 697 & 2091 \\ 1202 & 1803 & 2404 & 5409 \end{bmatrix}.$$

Choose

$$U = \begin{bmatrix} 1 & -10570841 & 10570841 & -10570841 \\ 0 & 1 & 10570841 & -10570841 \\ 0 & 0 & 1 & 10570841 \\ 0 & 0 & 0 & 1 \end{bmatrix},$$

$$L = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 10570841 & 1 & 0 & 0 \\ 10570841 & -10570841 & 1 & 0 \\ -10570841 & 10570841 & 10570841 & 1 \end{bmatrix}.$$

Then we have

$$B = \begin{bmatrix} 85902782524529 & 7783949494261 & 108645955098741 & 62082137341722 \\ 37207086894442 & 97811933363455 & 31492859166426 & 47829503460547 \\ 43940929239657 & 99629428908384 & 64015171957907 & 95852228892018 \\ 100737337377789 & 6871742549039 & 58298211039553 & 15913440226477 \end{bmatrix}.$$

Since B and N are public information, we can calculate

$$V = B^{-1} \text{mod } N =$$

$$\begin{bmatrix} 72960716256453 & 4761772750607 & 47819503708674 & 64505037116731 \\ 18354764339802 & 34264334590284 & 25746128923461 & 46666277809305 \\ 28770435964827 & 105706232411633 & 39730135919762 & 9119580812042 \\ 89276407646137 & 79398453561765 & 94718657144415 & 99534468035995 \end{bmatrix}$$

Then we arbitrarily select the set

$$S = \{v_{11}, v_{12}, v_{13}, v_{14}\} =$$

$$\{72960716256453, 4761772750607, 47819503708674, 64505037116731\}.$$

Using the L^3 algorithm (See algorithm 3.101 in [4], [10]), the basis to be reduced is:

$$\begin{bmatrix} 111742637163917 & 0 & 0 & 0 & 0 \\ 0 & 111742637163917 & 0 & 0 & 0 \\ 0 & 0 & 111742637163917 & 0 & 0 \\ 0 & 0 & 0 & 111742637163917 & 0 \\ -72960716256453 & -4761772750607 & -47819503708674 & -64505037116731 & 1 \end{bmatrix}.$$

The L^3-reduced basis is:

$$\begin{bmatrix} -32346761220 & -12938704488 & -19408056732 & -45285465708 & \mathbf{10570837} \\ -87078711029 & 39709857984 & 7883945327 & 11690435622 & 4385339758 \\ -12420733475 & -4968293390 & -7452440085 & -17389026865 & 182590067501 \\ -102740951106 & -253999460687 & 146924464771 & 79909317394 & 26579009212 \\ 1917450399 & -58848334744 & -420915726704 & 231779925047 & 78377734153 \end{bmatrix}.$$

Hence we get $\mathbf{p} = \mathbf{10570837}$. Once p is revealed we calculate $q = N/p$. Then we get $R = V^{-1}$ mod q. After this we calculate $d_{ii} = gcd(r_{i1}, r_{i2}, \cdots r_{in}), 1 \leq i \leq n$.

It is worth noting that it only took us 91, 520 and 4802 seconds to break the algorithm for the size of N = 256, 512 and 1024 bits respectively. We set $m = 10$ through step 2 of the attack. We performed our experiments with Maple V Release 5.1 running on a SUN ULTRA-80 workstation.

References

1. *M. Ajtai and C. Dwork, A public key cryptosystem with worst-case/average case equivalence*, Proc. of the twenty ninth annual ACM symposium on theory of computing, pp. 284-293, 1997.
2. O. Goldreich, S. Goldwasser and S. Halevi, *Public key cryptosystems from lattice reduction problems*, Advances in Cryptology, Pro. of CRYPTO' 97, Springer-Verlag, LNCS 1294, pp. 112-131.
3. G. H. Hardy and E. M. Wright, *An introduction to the theory of numbers,* 5^{th} *edition*, Oxford University Press, 1979.
4. A J. Menezes, P. C. van Oorschot and S A. Vanstone, *Handbook of Applied Cryptographic Research*, CRC Press, 1996.
5. P. Nguyen and J. Stern, *Lattice reduction in cryptology : An update*, Algorithmic Number Theory, Proc. of ANTS-IV, Springer-Verlag, LNCS 1838.
6. P. Nguyen, *Cryptanalysis of the Goldreich-Goldwasser-Halevi Cryptosystem from Crypto '97*, Advances in Cryptology, Pro. of CRYPTO'99, Springer-Verlag, LNCS 1666, pp. 288-304.
7. P. Nguyen and J. Stern, *Cryptanalysis of the Ajtai-Dwork Cryptosystem*, Advances in Cryptology, Pro. of CRYPTO' 98, Springer-Verlag, LNCS 1462, pp. 223-242.
8. P. Nguyen, J. Stern: Cryptanalysis of a Fast Public Key Cryptosystem Presented at SAC '97. Selected Areas in Cryptography 1998, Springer-Verlag, LNCS 1556, pp. 213-218.
9. P. Nguyen and I. Shparlinkski, Private communications, Jan 24, 2001.
10. Pate Williams, *Algorithms from Handbook of Applied Cryptography* , C code available at `http://www.mindspring.com/~pate/crypto/chap03.html.`
11. H. Yoo, S. Hong, S. Lee, O. Yi and M. Sung, *A Proposal of a New Public Key Cryptosystem using Matrices Over a Ring*, Fifth Australian Conference on Information Security and Privacy (ACISP 2000), Springer-Verlag, LNCS 1841, 2000, pp. 41-48.