The Cryptanalysis of a New Public-Key Cryptosystem based on Modular Knapsacks

Yeow Meng Chee
National Computer Systems
Center for Information Technology
73 Science Park Drive, S0511
REPUBLIC OF SINGAPORE
yeowmeng@itivax.bitnet

Antoine Joux
DMI-GRECC
45 rue d'Ulm
75230 Paris Cedex 05
FRANCE
joux@dmi.ens.fr

Jacques Stern
DMI-GRECC
45 rue d'Ulm
75230 Paris Cedex 05
FRANCE
stern@dmi.ens.fr

Abstract

At the 1990 EuroCrypt Conference, Niemi proposed a new public-key cryptosystem based on modular knapsacks. Y.M. Chee in Singapore, A. Joux and J. Stern in Paris independently found that this cryptosystem is insecure. Our two cryptanalytic methods are slightly different, but they are both based on the LLL algorithm. This is one more example of a cryptosystem that can be broken using this powerful algorithm.

1 Introduction

Let p be a prime and denote by $\mathbf{Z}/p\mathbf{Z}$ the field of integers modulo p. Unless otherwise stated, all vectors shall be assumed to be column vectors. The MODULAR KNAPSACK problem is defined as follows:

J. Feigenbaum (Ed.): Advances in Cryptology - CRYPTO '91, LNCS 576, pp. 204-212, 1992.

MODULAR KNAPSACKS
INSTANCE: A prime p, a matrix $E \in (\mathbf{Z}/p\mathbf{Z})^{n\times m}$ and a vector $c \in (\mathbf{Z}/p\mathbf{Z})^n$.
QUESTION: Is there a vector $x \in \{0,1\}^m$ such that $Ex = c$ over $\mathbf{Z}/p\mathbf{Z}$?
The MODULAR KNAPSACK problem is a decision problem that is NP-complete in the strong sense, even under the restriction $m = 2n$ [Nie91]. The related NP-hard algorithmic problem is considered here: Find a vector $x \in \{0,1\}^m$ that satisfies $Ex = c$ over $\mathbf{Z}/p\mathbf{Z}$ when one exists.

At the 1990 EuroCrypt Conference, Niemi proposed a new public-key cryptosystem based on this problem [Nie91]. Y.M. Chee in Singapore, A. Joux and J. Stern in Paris independently discovered that this cryptosystem is insecure. The purpose of this paper is to present our cryptanalysis on Niemi's cryptosystem. Our attacks are based on the LLL algorithm [LLL82]. This is one more example of a cryptosystem that can be broken using this powerful algorithm (see [Adl83, Ste87, ST91]).

2 The Proposed Cryptosystem

We briefly review Niemi's public-key cryptosystem in this section. The basic idea is a notion of absolute values in $\mathbf{Z}/p\mathbf{Z}$. The *absolute value* $|g|$ of $g \in \mathbf{Z}/p\mathbf{Z}$ is the minimum of the least non-negative residues modulo p of the two integers g and $-g$. We call g *k-small* if $|g| \leq k$ and g *k-large* if $|g| \geq \lceil p/2 \rceil - k$. We typically speak of *small* and *large* numbers, thus leaving k unfixed. The construction of the cryptosystem is as follows. Fix a prime p, and positive integers n and $k \ll p$. We randomly select matrices $C, D, S \in (\mathbf{Z}/p\mathbf{Z})^{n\times n}$ with k-small entries, a non-singular matrix $R \in (\mathbf{Z}/p\mathbf{Z})^{n\times n}$, and a diagonal matrix $\Delta \in (\mathbf{Z}/p\mathbf{Z})^{n\times n}$ with k-large entries. The public information is p and the $n \times 2n$ matrix $E = (\; A \quad B \;)$, where

$$A = R^{-1}(\Delta - SC), \tag{1}$$

$$B = -R^{-1}SD. \tag{2}$$

The private key is R. The matrices C, D, S, and Δ should also be kept secret but they are not needed after the initial construction. The message space is $\mathcal{M} = \{x \in \{0,1\}^{2n}\}$, and the ciphertext space is $\mathcal{C} = \{c \in (\mathbf{Z}/p\mathbf{Z})^n\}$. The encryption function is $\mathcal{E} : \mathcal{M} \to \mathcal{C}$ defined by $\mathcal{E}(x) = Ex$, arithmetic being done modulo p.

To decrypt a ciphertext c, we compute $l = Rc$. From (1) and (2) we can show that

$$(\Delta \quad 0)\, x = l + S\, (C \quad D)\, x.$$

Since the entries of C, D, and S are k-small and $x \in \{0,1\}^{2n}$, the entries of $S\,(C \quad D)\,x$ should be small as well. Hence, $\Delta_{i,i}x_i = l_i + \alpha_i$ for some small α_i, $1 \leq i \leq n$. It follows that our decryption rule is:

$$x_i = \begin{cases} 0, & \text{if } l_i \text{ is small;} \\ 1, & \text{if } l_i \text{ is large;} \end{cases}$$

for $1 \leq i \leq n$. The bits x_i, $n+1 \leq i \leq 2n$ can be obtained by solving the matrix equation

$$Bx^{(2)} = c - Ax^{(1)},$$

where $x^{(1)} = (x_1, \ldots, x_n)^T$ and $x^{(2)} = (x_{n+1}, \ldots, x_{2n})^T$. This can easily be done since we have n equations in n unknowns.

The decryption rule for x_i, $1 \leq i \leq n$, does not always yield the correct plain bits since its correctness depends on the size of the entries of $S\,(C \quad D)\,x$. Niemi restricts himself to the case $S = I$, where I denotes the identity matrix, and claims that in this case, the sufficient condition to ensure correct decryption is $p > 4kn$. Niemi also claims that $k = 1$ is a good choice.

In the sequel, we show how the plaintext can be recovered from the ciphertext without the knowledge of the secret key R.

3 The Cryptanalytic Principle

An *integer lattice* $\mathcal{L}$ of dimension m is an additive subgroup of $\mathbf{Z}^n$ that contains m linearly independent vectors over $\mathbf{R}^n$ (hence $m \leq n$). An *ordered basis* $(v_1, \ldots, v_m)$ of a lattice $\mathcal{L}$ of dimension m is a list of elements of $\mathcal{L}$ such that $\mathcal{L} = \mathbf{Z}v_1 \oplus \mathbf{Z}v_2 \oplus \cdots \oplus \mathbf{Z}v_m$. We represent an ordered basis of an m-dimensional lattice $\mathcal{L}$ by the $n \times m$ *basis matrix*

$$V = (\, v_1 \quad v_2 \quad \cdots \quad v_m\,),$$

whose columns are the basis vectors. A lattice with basis matrix V is simply denoted by $\mathcal{L}(V)$.

The main idea behind the attacks we are going to describe is the following. It is well-known that the LLL algorithm [LLL82] is a polynomial time algorithm designed to find a short (non-zero) vector in an integer lattice. More precisely, if the dimension of the lattice is n, then the LLL algorithm can find a vector in the lattice whose length is no more than $2^{(n-1)/2}$ times the length of the shortest vector in the lattice. In particular, if the length of the shortest vector in the lattice is $2^{(n-1)/2}$ times smaller than that of the other vectors, then the LLL algorithm will find the shortest vector. In practice, the LLL algorithm is much more effective and finds vectors whose lengths are much smaller than that gauranteed by the theoretical bound; and other algorithms exist, that are even more powerful [ScE91]. In our attacks, we transform the problem of finding the plaintext to that of finding short vectors in certain lattices. Then we show that the short vector is much shorter than the average short vectors. This gives heuristical evidence that the short vector can be found in polynomial time.

4 The Attack of Y.M. Chee

An observer of Niemi's cryptosystem who sees a ciphertext c, and has knowledge of public information p and E, can recover the corresponding plaintext by solving for a vector $x \in \{0,1\}^{2n}$ in the matrix equation $Ex = c$ over $\mathbf{Z}/p\mathbf{Z}$. The equivalent problem over $\mathbf{Z}$ is to find $x \in \{0,1\}^{2n}$ such that

$$\begin{pmatrix} E & -pI \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = c, \tag{3}$$

for some $y \in \mathbf{Z}^n$.

Lemma 4.1 *Let $\mathcal{L}$ be the lattice with basis matrix $V = \begin{pmatrix} I & 0 \\ M & -c \end{pmatrix}$. Then $Mu = \lambda c$ for some $\lambda \in \mathbf{Z}$ if and only if $\begin{pmatrix} u \\ 0 \end{pmatrix} \in \mathcal{L}$.*

Proof: The lattice $\mathcal{L}$ contains a vector $\begin{pmatrix} u \\ 0 \end{pmatrix}$ if and only if there exist some integer λ and integral vector v such that

$$\begin{pmatrix} u \\ 0 \end{pmatrix} = \begin{pmatrix} I & 0 \\ M & -c \end{pmatrix} \begin{pmatrix} v \\ \lambda \end{pmatrix} = \begin{pmatrix} v \\ Mv - \lambda c \end{pmatrix} \Longleftrightarrow Mu = \lambda c.$$

∎

It is easy to see that Lemma 4.1 implies that solving for $x \in \{0,1\}^n$ satisfying (3) for some $y \in Z^n$ is equivalent to finding a vector of the form $\begin{pmatrix} u \\ 0 \end{pmatrix}$, first $2n$ components of u being either 0 or 1, in the lattice $\mathcal{L}$ with basis matrix

$$\begin{pmatrix} \multicolumn{2}{c}{I} & 0 \\ E & pI & -c \end{pmatrix}$$

such that the first $2n$ components of u constitutes a $\{0,1\}$-vector x satisfying $Ex = c$. Since the first $2n$ components of u is either 0 or 1, $\begin{pmatrix} u \\ 0 \end{pmatrix}$ is a reasonably short vector in $\mathcal{L}$. Given an ordered basis of a lattice, the LLL algorithm computes another ordered basis, containing relatively short vectors, for the lattice. This new ordered basis is called a *reduced basis.* Our hope is that by running the LLL algorithm on the lattice $\mathcal{L}$, the vector $\begin{pmatrix} u \\ 0 \end{pmatrix}$ we are looking for appears in the reduced basis. Unfortunately, because the last n components of u may be large, such a vector is often too long to appear in any reduced bases. In order to remedy this situation, we adopt the following strategy.

Let

$$\epsilon_{i,j} = (\underbrace{0,\ldots,0}_{i-1}, -2^{j-1}p, 0, \ldots, 0)^T,$$

for $1 \leq i \leq n$. Then $x \in \{0,1\}^{2n}$ satisfies (3) for some $y \in Z^n$ if and only if x satisfies

$$\begin{pmatrix} E & \epsilon_{1,1} & \cdots & \epsilon_{1,j_1} & \epsilon_{2,1} & \cdots & \epsilon_{2,j_2} & \cdots & \epsilon_{n,1} & \cdots & \epsilon_{n,j_n} \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = c, \quad (4)$$

for some $y \in Z^{j_1+j_2+\cdots+j_n}$, where $j_i > 0$ for all $1 \leq i \leq n$. Let $s_i = \sum_{j=1}^{2n} E_{i,j}$ denote the sum of all entries in row i of E. It is easy to see that if we choose $j_i = \lceil \log_2(s_i/p) \rceil$, $1 \leq i \leq n$, then x satisfies (4) for some $y \in \{0, \pm 1\}^{j_1+j_2+\cdots+j_n}$.

We now consider a new lattice with the $(3n+\sum_{i=1}^{n} j_1) \times (2n+1+\sum_{i=1}^{n} j_i)$ basis matrix

$$G = \begin{pmatrix} \multicolumn{2}{c}{I} & 0 \\ E & E' & -c \end{pmatrix}$$

where $E' = \begin{pmatrix} \epsilon_{1,1} & \cdots & \epsilon_{1,j_1} & \epsilon_{2,1} & \cdots & \epsilon_{2,j_2} & \cdots & \epsilon_{n,1} & \cdots & \epsilon_{n,j_n} \end{pmatrix}$. It follows from previous discussions that we are looking for a vector $\begin{pmatrix} u \\ 0 \end{pmatrix} \in \mathcal{L}(G)$ such that its first n components consitutes a $\{0,1\}$-vector x satisfying $Ex = c$. There exists such a vector whose components are either 0, or ± 1. This short vector very often appears in the reduced basis of $\mathcal{L}(G)$.

5 The Attack of A. Joux and J. Stern

Given a ciphertext c and public information p and E, we choose a large scaling factor λ and define:

$$H = \begin{pmatrix} \lambda c & \lambda E & \lambda p I \\ \multicolumn{2}{c}{I} & 0 \end{pmatrix}$$

Lemma 5.1 *If $x \in \mathbf{Z}^{2n}$ satisfies (3) for some $y \in \mathbf{Z}^n$, then* $\begin{pmatrix} 0 \\ 1 \\ -x \end{pmatrix}$ *is a vector in the lattice $\mathcal{L}(H)$.*

Proof: The lattice $\mathcal{L}(H)$ contains the vector

$$\begin{pmatrix} \lambda c & \lambda E & \lambda p I \\ 1 & 0 & 0 \\ 0 & I & 0 \end{pmatrix} \begin{pmatrix} 1 \\ -x \\ y \end{pmatrix} = \begin{pmatrix} \lambda c - \lambda E x + \lambda p y \\ 1 \\ -x \end{pmatrix}.$$

By the hypothesis of the lemma, $c - Ex + py = 0$. Hence $\begin{pmatrix} 0 \\ 1 \\ -x \end{pmatrix}$ is a vector in $\mathcal{L}(H)$. ∎

As a consequence of Lemma 5.1, we see that if $x \in \{0,1\}^{2n}$ is the plaintext corresponding to a ciphertext c, then $v(x) = \begin{pmatrix} 0 \\ 1 \\ -x \end{pmatrix}$ is a short vector in the lattice $\mathcal{L}(H)$. In fact,

$$\|v(x)\|^2 = \|x\|^2 + 1 \leq 2n + 1.$$

Let us now discuss the other short vectors in $\mathcal{L}(H)$. Since λ is large, the first n components of the first vector of the reduced basis for $\mathcal{L}(H)$ will almost surely all be zero. A random vector of this form has average length $\sqrt{(2n+1)(p^2-1)/12}$. This shows that with $p = 4kn$, $v(x)$ is approximately $2kn/\sqrt{3}$ times shorter than an average vector with first n components all zero. This provides heuristical evidence that the vector $v(x)$ appears in the reduced basis for $\mathcal{L}(H)$ with high probability. It is also interesting to remark that there are other vectors which may provide a decryption of c, since they increase the probability of finding x. Let us explain informally what these vectors are, and why they are useful. First, we can say that summing up a few small numbers gives a small number (with a different constant k of course) and that summing up a few large numbers can give either a small number or a large number, depending on the parity of the number of numbers we sum up. Thus, if we obtain in the reduced basis a short vector of the form $\begin{pmatrix} 0 \\ \mu \\ -x' \end{pmatrix}$, where μ is a small odd number, we can write $E(\mu x - x') = 0$ and thus, if $\mu x - x'$ is small enough, we can infer that the first n components of this vector are all even, and therefore that the first n components of x and x' have the same parity.

6 Conclusion

The previous sections gave heuristical evidence that Niemi's proposed public-key cryptosystem is not secure. We would like to remark that it gets less and less secure. The reason for this is that a recent improvement of attacks against low-density knapsacks [CLJ91] can be used to improve the attacks described here. The idea is to replace the identity part of the basis matrices as described in [CLJ91]. We plan to carry out systematic experiments with this improved version.

Acknowledgement. The first named author would like to thank K. H. Lim for helpful discussions.

References

[Adl83] L. Adleman. *On Breaking the Iterated Merkle-Hellman Public Key Cryptosystem*, in: Advances in Cryptology, Proceedings of CRYPTO '82, Plenum Press, New York, 1983, 303–308.

[CLJ91] A. J. Coster, B. LaMacchia, A. Joux, A. Odlyzko, C. P. Schnorr and J. Stern. *Improved Low-Density Subset Sum Algorithms*, to appear.

[LLL82] A. K. Lenstra, H. W. Lenstra Jr. and L. Lovász. *Factoring Polynomials with Rational Coefficients*, Mathematische Annalen **261** (1982), 515–534.

[Nie91] V. Niemi. *A New Trapdoor in Knapsacks*, in: Advances in Cryptology, Proceedings of EUROCRYPT '90, Lecture Notes in Computer Science **473**, Springer-Verlag, Berlin, 1991, 405–411.

[ScE91] C. P. Schnorr, M. Euchner. *Lattice Basis Reduction: Improved Practical Algorithms and Solving Subset Sum Problems,* in: Proceedings of the FCT'91, Lecture Notes in Computer Science, Springer-Verlag, Berlin, to appear.

[Sha82] A. Shamir. *A Polynomial-Time Algorithm for Breaking the Basic Merkle-Hellman Cryptosystem*, in: Proceedings of the 23rd IEEE Symposium on Foundations of Computer Science, IEEE, New York, 1982, 145–152.

[Ste87] J. Stern. *Secret Linear Congruential Generators are Not Cryptographically Secure*, in: Proceedings of the 28th IEEE Symposium on Foundations of Computer Science, IEEE, New York, 1987, 421–426.

[ST91] J. Stern and P. Toffin. *Cryptanalysis of a Public-Key Cryptosystem Based on Approximations by Rational Numbers*, in: Advances in Cryptology, Proceedings of EUROCRYPT '90, Lecture Notes in Computer Science **473**, Springer-Verlag, Berlin, 1991, 313–317.