Selected Areas in Cryptography '98
(August 17–18, 1998, Kingston, Ontario, Canada)
S. Tavares (Ed.), vol. ???? of Lecture Notes in Computer Science, pages ???–???

Cryptanalysis of a Fast Public Key Cryptosystem Presented at SAC '97

Phong Nguyen and Jacques Stern

École Normale Supérieure
Laboratoire d'Informatique
45, rue d'Ulm
F – 75230 Paris Cedex 05
{Phong.Nguyen,Jacques.Stern}@ens.fr
http://www.dmi.ens.fr/~{pnguyen,stern}/

Abstract. At SAC '97, Itoh, Okamoto and Mambo presented a fast public key cryptosystem. After analyzing several attacks including lattice-reduction attacks, they claimed that its security was high, although the cryptosystem had some resemblances with the former knapsack cryptosystems, since decryption could be viewed as a multiplicative knapsack problem. In this paper, we show how to recover the private key from a fraction of the public key in less than 10 minutes for the suggested choice of parameters. The attack is based on a systematic use of the notion of the orthogonal lattice which we introduced as a cryptographic tool at Crypto '97. This notion allows us to attack the linearity hidden in the scheme.

1 Introduction

Two decades after the discovery of public key cryptography, only a few asymmetric encryption schemes exist, and the most practical public key schemes are still very slow compared to conventional secret key schemes. Extensive research has been conducted on public-key cryptography based on the knapsack problem. Knapsack-like cryptosystems are quite interesting: they are easy to implement, can attain very high encrypt/decrypt rates, and do not require expensive operations. Unfortunately, all the cryptosystems based on the additive knapsack problem have been broken, mainly by means of lattice-reduction techniques. Linearity is probably the biggest weakness of these schemes.

To overcome this problem, multiplicative knapsacks have been proposed as an alternative. The idea of multiplicative knapsack is roughly 20 years old and was first proposed in the open literature by Merkle and Hellman [3] in their original paper. Merkle-Hellman's knapsack was (partially) cryptanalyzed by Odlyzko [8], partly because only decryption was actually multiplicative, while encryption was additive.

Recently, two new public-key cryptosystems based on the multiplicative knapsack problem have been proposed: the Naccache-Stern cryptosystem [4] presented at Eurocrypt '97, and the Itoh-Okamoto-Mambo cryptosystem [1] presented at

SAC '97. In the latter one, both encryption and decryption were relatively fast. After analyzing several attacks including lattice-reduction attacks, Itoh, Okamoto and Mambo claimed that the security of their cryptosystem was high.

We present a very effective attack against this cryptosystem. In practice, one can recover the private key from the public key in less than 10 minutes for the suggested choice of parameters. The attack is based on a systematic use of the notion of the orthogonal lattice which we introduced as a cryptographic tool at Crypto '97 [5]. As in [5, 7, 6], this technique enables us to attack the linearity hidden in the keys generation process.

2 Description of the Cryptosystem

The message space is $\mathbb{Z}_M$, the ring of integers modulo an integer M. Let N be a product of two large primes P and Q. Let l and n be integers such that $l \leq n$. Select positive integers $q_1, \ldots, q_n$ less than $P^{1/l}$ and distinct primes $q'_1, \ldots, q'_n$ such that:

- For all i, q'_i divides q_i.
- For all $i \neq j$, q'_j does not divide q_i/q'_i.

Choose an integer t in $\mathbb{Z}_N$ coprime with P, and integers $k_1, \ldots, k_n$ in $\mathbb{Z}_N$ satisfying the following congruence:

$$k_i \equiv tq_i \pmod{P}.$$

Finally, select random elements $e_1, \ldots, e_n$ in $\mathbb{Z}_M$.

The public key consists of: the (e_i, k_i)'s, M, N, n and l.

The secret key consists of: P, Q, t, the q_i's and the q'_i's.

2.1 Encryption

Let $s \in \mathbb{Z}_M$ be the plaintext. Alice chooses l integers $i_1, \ldots, i_l$ (not necessarily distinct) in $\{1, \ldots n\}$. The ciphertext is $(m, r) \in \mathbb{Z}_M \times \mathbb{Z}_N$ defined by:

$$\begin{aligned} m &\equiv s + e_{i_1} + e_{i_2} + \cdots + e_{i_l} \pmod{M} \\ r &\equiv k_{i_1} k_{i_2} \ldots k_{i_l} \pmod{N} \end{aligned}$$

2.2 Decryption

Let (m, r) be the ciphertext. First, Bob computes $r' \equiv (t^l)^{-1} r \pmod{P}$, We have:

$$r' \equiv q_{i_1} q_{i_2} \ldots q_{i_l} \pmod{P}.$$

Since each q_i^l is strictly less than P, we actually have:

$$r' = q_{i_1} q_{i_2} \ldots q_{i_l}.$$

Eventually, Bob recovers s as follows:

1. Let $i = 1$.
2. If q'_i divides r', let $m := m - e_i \pmod{M}$ and $r' = r'/q_i$.
3. If $r' = 1$, Bob gets m as a plaintext. Otherwise, increment i and start again at Step 2.

2.3 Parameters

In their paper [1], Itoh, Okamoto and Mambo analyzed several possible attacks, including a lattice-reduction attack. They concluded that their cryptosystem was secure for the following choice of parameters:

- $N = 1024$ bits, $P = 768$ bits and $Q = 256$ bits.
- $n = 180$ and $l = 17$.
- $q_{max} = 2^{45}$ (6 bytes) and $q'_{max} = 2^{32}$ (4 bytes).

In this example, the public key takes 45 Kbytes and the private key takes 1.8 Kbytes. Compared to RSA-1024 with small exponent, encryption speed is similar, but decryption is about 50 times faster.

3 The Orthogonal Lattice

We recall a few useful facts about the notion of an orthogonal lattice, which was introduced in [5] as a cryptographic tool. Let L be a lattice in $\mathbb{Z}^n$ where n is any integer. The orthogonal lattice $L^\perp$ is defined as the set of elements in $\mathbb{Z}^n$ which are orthogonal to all the lattice points of L, with respect to the usual dot product. We define the lattice $\bar{L} = (L^\perp)^\perp$ which contains L and whose determinant divides the one of L. The results of [5] which are of interest to us are the following two theorems:

Theorem 1. *If L is a lattice in $\mathbb{Z}^n$, then* $\dim(L) + \dim(L^\perp) = n$ *and:*

$$\det(L^\perp) = \det(\bar{L}).$$

Thus, $\det(L^\perp)$ divides $\det(L)$. This implies that if L is a low-dimensional lattice in $\mathbb{Z}^n$, then a reduced basis of $L^\perp$ will consist of very short vectors compared to a reduced basis of L. In practice, most of the vectors of any reduced basis of $L^\perp$ are quite short, with norm around $\det(\bar{L})^{1/(n-\dim L)}$.

Theorem 2. *There exists an algorithm which, given as input a basis $(\mathbf{b}_1, \ldots, \mathbf{b}_d)$ of a lattice L in $\mathbb{Z}^n$, outputs an LLL-reduced basis of the orthogonal lattice $L^\perp$, and whose running time is polynomial with respect to n, d and any upper bound of the bit-length of the $\|\mathbf{b}_j\|$'s.*

In practice, one obtains a simple and very effective algorithm (which consists of a single lattice reduction, described in [5]) to compute a reduced basis of the orthogonal lattice, thanks to the celebrated LLL algorithm [2]. This means that, given a low-dimensional L in $\mathbb{Z}^n$, one can easily compute many short and linearly independent vectors in $L^\perp$.

4 Attacking the Scheme by Orthogonal Lattices

Let m be an integer less than n. Define the following vectors in $\mathbb{Z}^m$:

$$\mathbf{k} = (k_1, k_2, \ldots, k_m)$$
$$\mathbf{q} = (q_1, q_2, \ldots, q_m)$$

Note that an attacker knows $\mathbf{k}$, but not $\mathbf{q}$. By construction of the keys, we have the following congruence:

$$\mathbf{k} \equiv t\mathbf{q} \pmod{P}.$$

This leads to a simple remark:

Lemma 3. *Let $\mathbf{u} \in \mathbb{Z}^m$. If $\mathbf{u} \perp \mathbf{k}$ then $\mathbf{u} \perp \mathbf{q}$ or $\|\mathbf{u}\| \geq P/\|\mathbf{q}\|$.*

Proof. We have: $t\mathbf{q}.\mathbf{u} \equiv 0 \pmod{P}$. Therefore $\mathbf{q}.\mathbf{u} \equiv 0 \pmod{P}$, and the result follows by Cauchy-Schwarz. □

This remark is interesting because $\|\mathbf{q}\|$ is much smaller than P. Indeed, since each $q_i < P^{1/l}$, we have:

$$\|\mathbf{q}\| < \sqrt{m} P^{1/l}.$$

Therefore, if $\mathbf{u} \in \mathbb{Z}^m$ is orthogonal to $\mathbf{k}$ then it is also orthogonal to $\mathbf{q}$ or satisfies

$$\|\mathbf{u}\| \geq \frac{P^{(l-1)/l}}{\sqrt{m}} \tag{1}$$

which implies that $\mathbf{u}$ is quite long.

Furthermore, from the previous section, one can expect to find many vectors orthogonal to $\mathbf{k}$, with norm around

$$\|\mathbf{k}\|^{1/(m-1)} \leq (P\sqrt{m})^{1/(m-1)}.$$

This quantity is much smaller than the right quantity of (1) when m is large enough, so that we make the following assumption:

Assumption 4. *Let $(\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_{m-1})$ be a reduced basis of $\mathbf{k}^\perp$. Then the first $m-2$ vectors $\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_{m-2}$ are orthogonal to $\mathbf{q}$.*

Actually, one can prove that the first vector of an LLL-reduced basis satisfies the assumption, but this is not enough.

Now assume that the hypothesis holds. Then $\mathbf{q}$ belongs to the 2-dimensional lattice $L = (\mathbf{b}_1, \ldots, \mathbf{b}_{m-2})^\perp$. One expects the vectors $\mathbf{b}_1, \ldots, \mathbf{b}_{m-2}$ to have norm around $\|\mathbf{k}\|^{1/(m-1)}$. Therefore, the determinant of L should be around

$$\|\mathbf{k}\|^{(m-2)/(m-1)} \approx \|\mathbf{k}\|.$$

But $\mathbf{q}$ belongs to L and its norm is much smaller than $\|\mathbf{k}\|^{1/2}$. This leads to a more general assumption which is as follows:

Assumption 5. *Let* $(\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_{m-1})$ *be a reduced basis of* $\mathbf{k}^\perp$*. Then* $\mathbf{q}$ *is a shortest vector of the 2-dimensional lattice* $(\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_{m-2})^\perp$*.*

If this hypothesis holds, one can use the Gaussian algorithm for lattice reduction (which has worst-case polynomial time and average-case constant time) to recover $\pm\mathbf{q}$.

Next, we easily recover the secret factorization $P \times Q$ using the so-called differential attack described in [1]. More precisely, there exist integers $p_1, \ldots, p_n$ such that:

$$k_i \equiv p_i P + t q_i \pmod{N}.$$

Therefore, we have for all $i \neq j$:

$$q_j k_i - q_i k_j \equiv (p_i q_j - p_j q_i) P \pmod{N}.$$

It is likely that $gcd(q_j k_i - q_i k_j, N)$ is equal to P. And if it is not, we can try again with a different (i, j).

To sum up, the attack is the following:

1. Select an integer $m \leq n$.
2. Compute a reduced basis $(\mathbf{b}_1, \ldots, \mathbf{b}_{m-1})$ of the lattice $\mathbf{k}^\perp$.
3. Compute a reduced basis $(\mathbf{a}_1, \mathbf{a}_2)$ of the lattice $(\mathbf{b}_1, \ldots, \mathbf{b}_{m-2})^\perp$.
4. Compute a shortest vector $\mathbf{s}$ of the previous lattice.
5. Select integers $i \neq j$ in $\{1, \ldots, n\}$ and denote the coordinates of $\mathbf{s}$ by s_i.
6. If $gcd(s_j k_i - s_i k_j, N)$ is not a proper factor of N, restart at previous step.

In practice, we perform Steps 3 and 4 by a single LLL-reduction and take $\mathbf{a}_1$ as $\mathbf{s}$. Only Steps 2 and 3 take a little time. Note that we do not need to compute a complete reduced basis in Step 2 since the last vector is useless.

Once $\mathbf{q}$ and the secret factorization of N are found, it is not a problem to recover the rest of the secret key:

- t modulo P is given by $k_i \equiv t q_i \pmod{P}$.
- The q_i''s (or something equivalent) are revealed by the factors of the q_i's.

5 Experiments

We implemented the attack using the NTL package [9] which includes efficient lattice-reduction algorithms. We used the LLL floating point version with extended exponent to compute orthogonal lattices, since the entries of $\mathbf{k}$ were too large (about the size of N) for the usual floating point version.

In practice, the attack reveals the secret factorization as soon as $m \geq 4$ for the suggested choice of parameters. When $m \leq 20$, the total computation time is less than 10 minutes on a UltraSparc-I clocked at 167 MHz.

6 Conclusion

We showed that the cryptosystem presented by Itoh, Okamoto and Mambo at SAC '97 is not secure. The core of our attack is the notion of the orthogonal lattice which we introduced at Crypto '97, in order to cryptanalyze a knapsack-like cryptosystem proposed by Qu and Vanstone. The attack is very similar to the attack we devised against the so-called Merkle-Hellman transformations. This is because the congruence $\mathbf{k} \equiv t\mathbf{q} \pmod{P}$, which is used in the keys generation process, looks like a Merkle-Hellman transformation: in a Merkle-Hellman equation, we have an equality instead of a congruence.

We suggest that the design of multiplicative knapsack cryptosystems should avoid any kind of linearity. But this might be at the expense of efficiency.

References

1. K. Itoh, E. Okamoto, and M. Mambo. Proposal of a fast public key cryptosystem. In *Proc. of SAC '97*, 1997. Available at `http://adonis.ee.queensu.ca:8000/sac/sac97/papers/paper10.ps`.
2. A. K. Lenstra, H. W. Lenstra, and L. Lovász. Factoring polynomials with rational coefficients. *Math. Ann.*, 261:515–534, 1982.
3. R. Merkle and M. Hellman. Hiding information and signatures in trapdoor knapsacks. *IEEE Trans. Inform. Theory*, IT-24:525–530, September 1978.
4. D. Naccache and J. Stern. A new public-key cryptosystem. In *Proc. of Eurocrypt '97*, volume 1233 of *LNCS*, pages 27–36. Springer-Verlag, 1997.
5. P. Nguyen and J. Stern. Merkle-Hellman revisited: a cryptanalysis of the Qu-Vanstone cryptosystem based on group factorizations. In *Proc. of Crypto '97*, volume 1294 of *LNCS*, pages 198–212. Springer-Verlag, 1997.
6. P. Nguyen and J. Stern. The Béguin-Quisquater server-aided RSA protocol from Crypto '95 is not secure. In *Proc. of Asiacrypt '98*, LNCS. Springer-Verlag, 1998.
7. P. Nguyen and J. Stern. Cryptanalysis of the Ajtai-Dwork cryptosystem. In *Proc. of Crypto '98*, volume 1462 of *LNCS*, pages 223–242. Springer-Verlag, 1998.
8. A. Odlyzko. Cryptanalytic attacks on the multiplicative knapsack cryptosystem and on Shamir's fast signature scheme. *IEEE Trans. Inform. Theory*, IT-30:594–601, 1984.
9. V. Shoup. NTL computer package version 2.0. Can be obtained at `http://www.cs.wisc.edu/~shoup/ntl`.