Cryptanalysis of a Cryptosystem due to Yoo, Hong, Lee, Lim, Yi and Sung

Simon R. Blackburn and Theodoulos Garefalakis
Department of Mathematics
Royal Holloway, University of London
Egham, Surrey TW20 0EX United Kingdom

April 20, 2001

Abstract

The paper shows that a public key cryptosystem due to Yoo, Hong, Lee, Lim, Yi and Sung is insecure, as it is susceptible to an attack based on the LLL algorithm.

Key words: Cryptography, lattice reduction, cryptanalysis

1 Introduction

This paper cryptanalyses a public key cryptosystem due to Yoo, Hong, Lee, Lim, Yi and Sung [8] (which we refer to as the YHLLYS cryptosystem). This scheme was inspired by a cryptosystem invented by Goldreich, Goldwasser and Helevi [1] and cryptanalysed by Nguyen [6]. The YHLLYS cryptosystem is an attempt to avoid the attacks of Nguyen by using modular arithmetic. However, we will show that the YHLLYS cryptosystem is open to an attack based on the LLL algorithm [4] for finding short vectors in a lattice.

We describe the YHLLYS cryptosystem in Section 2. Our cryptanalysis is contained in Section 3, and the results of practical experiments are given in Section 4.

2 The YHLLYS Cryptosystem

The YHLLYS cryptosystem is defined as follows. Let n be a small positive integer (the paper of Yoo *et al* [8] suggests that n should lie between 10 and 20). Let p and q be randomly chosen 512 bit primes, and let $N = pq$. Let m and e be random integers so that $m \approx q^{0.4}$ and $e \approx q^{0.2}$.

Let D, T, U and L be $n \times n$ integer matrices, chosen subject to the following conditions:

- D is diagonal, and the entries d_{ii} on the main diagonal of D have modulus between m and $q^{0.5}$.
- T is invertible, its entries are non-negative and its row sums are all at most $q^{0.2}$. (The non-negative condition is not explicitly stated in the paper of Yoo *et al* [8]. However something like this condition is needed for the decryption process to work correctly.)
- U is upper unitriangular, the entries off the main diagonal are multiples of q.
- L is lower unitriangular, the entries off the main diagonal are multiples of q.

Define $R = DT$. Note that the entries of R lie in the range $[-q^{0.7}, q^{0.7}]$. Define $B_q = R^{-1} \bmod q$ and define $B = B_q UL \bmod N$.

The public key consists of B, e, m and N. The secret key consists of the public key together with R, q and D.

Let M be a message, which is thought of as a length n (column) vector whose entries are integers between 0 and m. To encrypt M, a user randomly chooses a length n vector E whose entries are integers between 0 and e. The ciphertext C is

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

To decrypt, a user computes a length n vector X whose entries are integers between 0 and q by

$$X = RC \bmod q.$$

The ith entry of X is reduced modulo d_{ii} (the ith diagonal entry of D) to obtain the ith entry of M. To show that this decryption process works, see the paper of Yoo *et al* [8].

3 A Cryptanalysis

This section contains a cryptanalysis of the YHLLYS cryptosystem. We use the notation of the previous section throughout.

Yoo *et al* observe that their scheme is broken if q becomes known. But we will show that the public key contains sufficient information to enable N to be factorised, and so q is revealed.

We begin with a definition. The vector

$$\left(\frac{u_1}{u}, \frac{u_2}{u}, \ldots, \frac{u_\ell}{u}\right) \tag{1}$$

of rational numbers is an *unusually good simultaneous diophantine approximation* to the vector

$$\left(\frac{v_1}{v}, \frac{v_2}{v}, \ldots, \frac{v_\ell}{v}\right) \tag{2}$$

if $u < v$ and the following inequality holds

$$\left|u\frac{v_i}{v} - u_i\right| < v^{-\frac{1}{\ell}} \text{ for all } i \in \{1, 2, \ldots, \ell\}. \tag{3}$$

We will use the fact that if the vector (1) is an unusually good simultaneous diophantine approximation to the vector (2) then the integers u_i and the integer u may be found from the integers v_i and v by using the LLL Algorithm [4]. Lagarias [3] was the first to observe this; see Menezes, van Oorschot and Vanstone [5, Page 121]. Joux and Stern [2] give a useful survey of the uses of the LLL algorithm in cryptography. [The detail of the method is as follows. Let λ be an integer near to the expected upper bound for $\left|u\frac{v_i}{v} - u_i\right|$. Form the $(\ell + 1)$-dimensional integer lattice generated by λN times the first ℓ standard basis vectors together with the vector

$$(-\lambda v_1, -\lambda v_2, \ldots, -\lambda v_\ell, 1).$$

Apply the LLL algorithm to this lattice, to produce a reduced basis. Then the vector

$$(u_1, u_2, \ldots, u_\ell, u)$$

is usually one of the vectors in this basis.]

We now show how this technique may be used to break the YHLLYS scheme. Let S be defined by $S = B^{-1} \bmod N$. Note that S may be calculated from the public key. (It is highly unlikely that S fails to be invertible. In any case, if S is not invertible then the gcd of its determinant and N would be p and so N is factorised.) Now, since $U = L = I \bmod q$ the definition of B shows that $S = R \bmod q$. Since the entries of R lie in the range $[-q^{0.7}, q^{0.7}]$, we have that each entry s_{ij} of S is an integer such that s_{ij} mod $q \in [-q^{0.7}, q^{0.7}]$.

Let $v_1, v_2, \ldots, v_{n^2}$ be the entries of S listed in some order. Let ℓ be a small integer (we discuss the choice of ℓ below, but we must have $\ell \leq n^2$). We are only going to use ℓ of the entries v_i of S in our cryptanalysis. We may write $v_i = u_i q + r_i$ for some integers u_i and r_i such that $0 \leq u_i < p$ and $r_i \in [-q^{0.7}, q^{0.7}]$. We claim that the vector

$$\left(\frac{u_1}{p}, \frac{u_2}{p}, \ldots \frac{u_\ell}{p}\right) \tag{4}$$

is an unusually good simultaneous diophantine approximation to the vector

$$\left(\frac{v_1}{N}, \frac{v_2}{N}, \ldots \frac{v_\ell}{N}\right) \tag{5}$$

whenever $\ell \geq 7$. For we have that

$$\left|p\frac{v_i}{N} - u_i\right| = \frac{|r_i|}{q} < q^{-0.3},$$

where we have used the fact that $v_i = u_i q + r_i$ and the fact that $N = pq$. Since q is approximately $N^{0.5}$, we have that

$$\left|p\frac{v_i}{N} - u_i\right| \leq N^{-0.15}.$$

Now, $0.15 > \frac{1}{\ell}$ whenever $\ell \geq 7$, and so (4) is an unusually good simultaneous diophantine approximation to (5). Thus our claim follows.

Our cryptanalysis proceeds as follows. Let B and N be part of the public key. Assume that B is an $n \times n$ matrix, where $n \geq 3$ (as the suggested values for n range from 10 to 30, this is a reasonable assumption). Since $7 \leq 3^2 \leq n^2$, we may take $\ell = 7$ and the vector (5) may be efficiently computed from B and N (by inverting B modulo N to obtain the elements v_i). Since (4) is an unusually good simultaneous diophantine approximation to (5), we may use the LLL algorithm to compute p (and the integers u_i). But now we have obtained a factor of N, and so the YHLLYS cryptosystem is broken.

4 Experimental Verification

The above cryptanalysis relies on the heuristic simultaneous diophantine approximation techniques of Lagarias [3]. We have performed experiments to verify that these techniques work in practice, for the parameters we were considering. We picked two 512-bit pseudoprimes p and q at random, and multiplied them together to form N. We generated ℓ elements v_i modulo N of the form $v_i = u_i q + r_i$ where $0 \leq u_i < p$ and $r_i \in [-q^{0.7}, q^{0.7}]$ were chosen uniformly and independently at random.

Define an integer $\lambda = \lfloor N^{0.15} \rfloor$. We submitted the lattice generated by the rows of the following $(\ell + 1) \times (\ell + 1)$ matrix to the LLL algorithm:

$$\begin{pmatrix} \lambda N & 0 & 0 & \cdots & 0 & 0 & 0 \\ 0 & \lambda N & 0 & \cdots & 0 & 0 & 0 \\ 0 & 0 & \lambda N & \cdots & 0 & 0 & 0 \\ \vdots & & & \vdots & & & \vdots \\ 0 & 0 & 0 & \cdots & \lambda N & 0 & 0 \\ 0 & 0 & 0 & \cdots & 0 & \lambda N & 0 \\ -\lambda v_1 & -\lambda v_2 & -\lambda v_3 & \cdots & -\lambda v_{\ell-1} & -\lambda v_\ell & 1 \end{pmatrix}$$

In our experiments with $\ell = 7$, the reduced basis returned by the LLL algorithm always had p or $-p$ as its last entry and so we were able to factorise N. (Indeed, though not indicated by our theoretical analysis, this approach always factorised N when $\ell = 6$; but the method never succeeded if we chose $\ell = 5$.) We performed our experiemnts on a 700MHz Pentium 3 laptop running Lynux, using Victor Shoup's NTL library [7]. In every case, the LLL algorithm took under 3 minutes to return the reduced basis of the lattice. All these results were repeated for 712-bit primes p and q, with no change of outcome.

Acknowledgements Many thanks to Steven Galbraith, for carrying out some of the computations at an early stage of the paper.

References

[1] O. Goldreich, S. Goldwasser and S. Halevi, 'Public key cryptosystems from lattice reduction problems', in (B.S. Kaliski, Ed) *Advances in Cryp-*

tology — Proc. CRYPTO '97, Lecture Notes in Computer Science Vol. 1294, (Springer, Berlin, 1997), pp. 112-131.

[2] A. Joux and J. Stern, 'Lattice reduction: a toolbox for the cryptanalyst', *J. Cryptology*, Vol. 11 (1998), pp. 161-185.

[3] J.C. Lagarias, 'Knapsack public key cryptosystems and diophantine approximation', in (D. Chaum, Ed), *Advances in Cryptology — Proc. CRYPTO '83*, (Plenum Press, 1984), pp. 3-23.

[4] A.K. Lenstra, H.W. Lenstra and L. Lovász, 'Factoring polynomials with rational coefficients', *Mathematische Annalen*, Vol. 261 (1982), pp. 515-534.

[5] A.J. Menezes, P.C. van Oorschot and S.A. Vanstone, *Handbook of Applied Cryptography*, (CRC Press, Boca Raton, 1997).

[6] P. Nguyen, 'Cryptanalysis for the Goldreich–Goldwasser–Halevi cryptosystem from Crypto '97', in (M. Weiner, Ed) *Advances in Cryptology — Proc. CRYPTO '99*, Lecture Notes in Computer Science Vol. 1666, (Springer, Berlin, 1999), pp. 288-304.

[7] V. Shoup, *NTL: A Library for doing Number Theory*, available at `http://www.shoup.net/`.

[8] H. Yoo, S. Hong, S. Lee, J. Lim, O. Yi and M. Sung, 'A proposal for a new public key cryptosystem using matrices over a ring', in (E. Dawson, A. Clark, Eds) *ACISP 2000*, Lecture Notes in Computer Sience Vol. 1841, (Springer, Berlin, 2000), pp. 41-48.