Lattice Based Attack on Common Private Exponent RSA

R. Santosh Kumar[1], C. Narasimham[2] and S. Pallam Setty[3]

[1]Department of Information Technology ,MVGR College of Engg., Vizianagaram, India.

[2]Department of Information Technology ,VR Siddhartha Engineering College ,Vijayawada-7, India.

[3]Dept. of Computer Science & Systems Engineering, Andhra University, Vishakhapatnam, India.

Abstract

Lattice reduction is a powerful concept for solving diverse problems involving point lattices. Lattice reduction has been successfully utilizing in Number Theory, Linear algebra and Cryptology. Not only the existence of lattice based cryptosystems of hard in nature, but also has vulnerabilities by lattice reduction techniques. In this paper, we show that Wiener's small private exponent attack, when viewed as a heuristic lattice based attack, is extended to attack many instances of RSA when they have the same small private exponent.

Key words: Lattices, Lattice reduction, LLL, RSA.

1. Introduction

Lattices are periodic arrangements of discrete points. Apart from their wide-spread use in pure mathematics, lattices have found applications in numerous other fields as diverse as cryptography/cryptanalysis, the geometry of numbers, factorization of integer polynomials, subset sum and knapsack problems, integer relations and Diophantine approximations, coding theory.

Lattice reduction is concerned with finding improved representations of a given lattice using algorithms like LLL (Lenstra, Lenstra, Lov´asz) reduction . In section II, we introduce the some terminology about lattices, LLL algorithm. LLL algorithm is a lattice reduction algorithm, which takes arbitrary basis as input and output the basis in which vectors are nearly orthogonal.

2. Terminology

2.1 Lattices

A lattice is a discrete subgroup of $\mathbb{R}^n$. Equivalently, given $m \leq n$ linearly independent vectors $b_1, b_2, b_3, \ldots, b_n \in \mathbb{R}^n$, the set $\mathcal{L} = \mathcal{L}(b_1, b_2, b_3, \cdots, b_m) = \{\sum_{i=1}^{m} \alpha_i b_i \,|\alpha_i \in \mathbb{Z}\}$, is a lattice. The $b_i's$ are called basis vectors of $\mathcal{L}$ and $\mathcal{B} = \{b_1, b_2, \cdots, b_m\}$ is called a lattice basis for $\mathcal{L}$. Thus, the lattice generated by a basis $\mathcal{B}$ is the set of all integer linear combinations of the basis vectors in $\mathcal{B}$. The determinant of a lattice, denoted by $vol(\mathcal{L})$ is the square root of the gramian determinant $det_{1\leq i,j\leq m}\langle b_i, b_j\rangle$, which is independent of particular choice of basis. A general treatment of this topic see[1].

2.2 LLL reduced

Every lattice $\mathcal{L}$ with dimension $\dim(\mathcal{L}) \geq 2$ has infinite number of bases. Some bases however, are better than other bases. The definition of "better" depends on the particular application but, usually, we are interested in so-called reduced basis is simply a basis made up of short vectors. The following LLL reduced version given by Lenstra, Lenstra, Lovasz[1],[2],[3].

LLL reduced: A basis $b_1, b_2, b_3, \cdots, b_m$ of a lattice $\mathcal{L}$ is said to be Lovasz-reduced or LLL-reduced if

$|\mu_{i,j}| \leq \frac{1}{2}$ for $1 \leq j < i \leq n$

$|b_i^* + \mu_{i,i-1} b_{i-1}^*|^2 \geq \frac{3}{4}|b_{i-1}^*|^2$ for $1 < i \leq n$. where the b_i^* and $\mu_{i,j}$ are defined by the Gram-Schimdt orthogonalization process acting on the b_i. Above in place of ¾ one can replace any quantity $\frac{1}{4} < \delta < 1$.

2.3 LLL Algorithm

The Lenstra –Lenstra -Lov´asz (LLL) algorithm [1][2][3] is an iterative algorithm that transforms a given
lattice basis into an LLL-reduced one. Since the definition of LLL-reduced uses Gram-Schmidt process, the LLL algorithm performs the Gram-Schimdt method as subroutine.

LLL Algorithm with Euclidean norm:

Input: $b_1, b_2, b_3, \cdots, b_n \in \mathbb{Z}^m$
Output: LLL reduced basis $b_1, b_2, b_3, \cdots, b_n$
1: Compute the Gram-Schimdt basis $b_1^*, b_2^*, \cdots, b_n^*$ and coefficients $\mu_{i,j}$ for $1 \leq j < i < n$.
2: Compute $B_i = \langle b_i^*, b_i^* \rangle = \|b_i^*\|^2$ for $1 \leq i \leq n$
3: k=2
4: while $k \leq n$ do
5: for $j = k - 1$ downto 1 do
6: let $q_j = \mu_{k,j}$ and set $b_k = b_k - q_j b_j$
7: update the values $\mu_{k,j}$ for $1 \leq j < k$ and B_k
8: end for
9: if $B_k \geq (\frac{3}{4} - \mu_{k,k-1}^2) B_{k-1}$ then
10: $k = k + 1$
11: else
12: Swap b_k with b_{k+1}
13:Update the values $b_k^*, b_{k-1}^*, B_k, B_{k-1}, \mu_{k-1,j}$ and $\mu_{k,j}$ for $1 \leq j < k$ and $\mu_{i,k}$ and $\mu_{i,k-1}$ for $k < i \leq n$.
14: $k = \min\{2, k-1\}$
15: end if
16: end while

Let $b_1, b_2, b_3, \cdots, b_m$ be an LLL reduced basis of a lattice $\mathcal{L}$ and $b_1^*, b_2^*, \cdots, b_m^*$ be it s Gram-Schimdt orthogonalization. Then $|b_1| \leq 2^{\frac{m-1}{2}}$ for every $x \in \mathcal{L}$ and $x \neq 0$, It can be proven that the LLL algorithm terminates a finite number of iterations. Let $\mathcal{L} \subset \mathbb{Z}^n$ be a lattice with basis $\{b_1, b_2, b_3, \cdots, b_m\}$,and $C \in \mathbb{R}$, $C \geq 2$ be such that $\|b_i\| \leq \sqrt{C}$ for $i = 1,2, \cdots, n$. Then the number of arithmetic operations needed for the algorithm $O(n^4 \log C)$ on integers of size $O(n \log C)$ bits.

2.5 Assumption:

Let $\mathcal{B}$ be a basis for a lattice $\mathcal{L}$ and let $v \in \mathcal{L}$. If the vector v is smaller than all of the basis vectors in $\mathcal{B}$ and it satisfies Minkowsi's bound for the lattice $\mathcal{L}$, then $\pm v$ are the only smallest vectors in $\mathcal{L}$.

3 RSA Cryptosystem

The RSA cryptosystem was the first publicly known public key cryptosystem introduced by Rivest, Shamir, and Adleman.

The RSA cryptosystem: Let $N = pq$ be the product of two large primes p and q, let $\mathcal{P} = \mathcal{C} = \mathbb{Z}_N$ and define the key space as $\mathcal{K} = \{(N, p, q, e, d): ed \equiv 1(mod\ \varphi(N))\}$, where $\varphi(N) = (p-1)(q-1)$ is Euler's totient function. For each key $K \in \mathcal{K}$, given by $K = (N, p, q, e, d)$, the encryption rule $enc_K = Z_n \to Z_n$ is defined by $enc_K(x) = x^e mod\ N$, and the decryption rule $dec_k(y) = y^d mod\ N$, for any $x, y \in \mathbb{Z}_n$. The pair (e, N) is the RSA public key and the triple $(d, p, q)$is the RSA private key. Since the public and private exponents satisfy $ed \equiv 1(mod\ \varphi(N))$, it follows that $ed = 1 + k\varphi(N)$ for some integer k. This equation is called the RSA key equation, or simply the key equation. Sometimes we may encrypt the data with different encrypt values but all they can have same decryption exponent. If it is the case the following heuristic attack can retrieve the original data by using lattice reduction algorithms.

3.1 Attack

We assume that a single user has generated r instances of RSA that each has the same small private exponent d and a similarly sized modulus. Thus, there are r key equations

$$e_1 d = 1 + k_1 \varphi(N_1)$$
$$e_2 d = 1 + k_2 \varphi(N_2)$$
$$\vdots$$
$$e_r d = 1 + k_r \varphi(N_r)$$

Where $\varphi(N_r) = N_i - s_i$ and $k_i < d$ for each $i = 1,2, \cdots, r$. All of the moduli are assumed to be the same size and we arbitrarily label them so that they appear in increasing size. That is, we label them so that $N_1 < N_2 < \cdots < N_r < 2N_1$. Further, we assume all each modulus N_i is balanced so that $|s_i| < 3{N_I}^{1/2}$ for each $i = 1, 2, \cdots, r$.
Hinek introduced the following attack:
Attack: For any integer $r \geq 1$, let $N_1, N_2, \cdots, N_r$ be balanced RSA moduli satisfying $N_1, N_2, N_3, \cdots, N_r$ be balanced RSA moduli satisfying $N_1 < N_2 < \cdots < N_r < 2N_1$. Let $(e_1, N_1), \cdots, (e_r, N_r)$ be valid RSA public keys each with the same private exponent $d < {N_r}^{\delta_r}$. If $\delta_r < \frac{1}{2} - \frac{1}{2(r+1)} - log_{N_r}\delta_r(6)$, then all of the moduli can be factored in time polynomial in $\log(N_r)$ and r.

3.2 Justification:

Let $M = \lfloor {N_r}^{1/2} \rfloor$. Given the r public keys $(e_1, N_1), \cdots, (e_r, N_r)$, we begin by considering the r key equations $,e_i d = 1 + k_i(N_i, -s_i)$, along with the trivial equation $dM = dM$, written as

$$\begin{aligned} dM &= dM \\ e_1 d - N_1 k_1 &= 1 - k_1 s_1 \\ e_2 d - N_2 k_2 &= 1 - k_2 s_2 \\ &\vdots \\ e_r - N_r k_r &= 1 - k_r s_r, \end{aligned}$$

This system of $r + 1$ equations can be written as the vector-matrix equation $x_r \mathcal{B}_r = v_r$, where

$$x_r = (d, k_1, k_2, \cdots, k_r)$$

$$\mathcal{B}_r = \begin{bmatrix} M & e_1 & e_2 & & e_r \\ 0 & -N_1 & 0 & \cdots & 0 \\ 0 & 0 & -N_2 & & 0 \\ & \vdots & & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & -N_r \end{bmatrix}$$

$$v_r = (dM, 1 - k_1 s_1, \cdots, 1 - k_r s_r).$$

Observe that the target vector $v_r$is an integer linear combination of the rows in the matrix $\mathcal{B}_r$ and hence is a vector $\mathcal{L}_r$ generated by the rows in $\mathcal{B}_r$. Since $N_i \le N_r < 2N_1, k_i < d < {N_r}^{\delta_r}$ and $s_i < 3{N_r}^{1/2}$ for each $i = 1,2,\cdots,r$, it follows that the target vector satisfies$\|v_r\| < \sqrt{1 + 9r}{N_r}^{1/2+\delta_r}$. The volume of the lattice$\mathcal{L}_r$, given by $vol(\mathcal{L}) = |\det(\mathcal{B}_r)|$, satisfies $vol(\mathcal{L}) > \left({N_1}/{2}\right)^{r+1/2}$. From Minkowski's bound, a necessary condition for the target vector to be a smallest vector in $\mathcal{L}_r$(which has dimension $r + 1$) is given by $\|v_r\| < \sqrt{r+1}vol(\mathcal{L}_r)^{1/r+1}$. Using the bounds on the norm of the target vector and the volume of the lattice, a sufficient condition for this necessary condition to hold is given by $\sqrt{9r+1}{N_r}^{\delta+1/2} < \sqrt{r+1}\left(\frac{N_r}{2}\right)^{\frac{r+1/2}{r+1}}$ or more simply ${N_r}^{1/2+\delta_r} < c_r {N_r}^{\frac{(r+1/2)}{(r+1)}}$, where c_r is a constant depending on r but not N. For any $r \ge 1$, this constant satisfies $c_r = \sqrt{\frac{r+1}{9r+1}}\frac{1}{2^{\frac{r+1/2}{r+1}}} > \frac{1}{6}$. So a new sufficient condition is given by ${N_r}^{1/2+\delta_r} < {N_r}^{\frac{(r+1/2)}{(r+1)} - \log_N(6)}$. Solving for δ_r in the exponents, and we get $\delta_r < \frac{1}{2} - \frac{1}{2(r+2)} - log_{N_r}(6)$. When the private exponent is smaller than ${N_r}^{\delta_r}$, we know that the target vector v_r has satisfied the necessary condition, imposed by Minkowski's bound, to be a smallest vector in $\mathcal{L}_r$. In addition, the second condition is also satisfied. In particular, the size of the target vector v_r is smaller than the size of each of the basis vectors in $\mathcal{B}$, provided $\delta_r < {1}/{2}$. Therefore, when the private exponent is sufficiently small and assumption holds for the lattice $\mathcal{L}_r$, we can compute the target vector by solving the SVP for $\mathcal{L}_r$. Once the target vector is obtained we can easily factor all of the moduli. Since the target vector $v_r = (dM, 1 - k_1 s_1, \cdots, 1 - k_r s_r)$, exposes the private exponent d and each of the $(1 - k_i s_i)$, we can compute all of the k_i values. With $k_i$and d, this allows us to compute $\phi(N_i) = \frac{e_i d - 1}{k_i}$ which is then used to factor N_i, for each $i = 1,2,\cdots,r$. Since all computations can be done in log (N_r) and in r.

3.3 Example:

We illustrate the attack with the following example with three instances of RSA with the same small private exponent. We use NTL library to do the following experiment.

Consider the three RSA public keys, thought to have a common private exponent, given by

$$(e_1, N_1) = (587438623, 2915050561)$$
$$(e_2, N_2) = (2382816879, 3863354647)$$
$$(e_3, N_3) = (2401927159, 3943138939)$$

Letting $M = \left\lfloor {N_3}^{1/2} \right\rfloor = 62794$, we construct the basis matrix

$$\mathcal{B} = \begin{bmatrix} 62794 & 587438623 & 2382816879 & 2401927159 \\ 0 & -2915050561 & 0 & 0 \\ 0 & 0 & -3863354647 & 0 \\ 0 & 0 & 0 & -3943138939 \end{bmatrix}$$

Applying LLL algorithm, with $\mathcal{B}$ as input, we obtain a reduced basis whose smallest basis vector is $b = (-41130070, 14375987, 50221643, 50147516)$. If the attack is successful, we expect the first component of b, denoted by b_1, to satisfy $|b_1| = Md$. We have $\frac{|b_1|}{M} = 655$, which is, in fact, the common private exponent d. Also notice that the enabling condition for the attack, $\delta < \frac{1}{2} - \frac{1}{2(r+1)} - log_{N_3}(6) \approx 0.3189$, is satisfied since $log_{N_3}(d) \approx 0.2935$.

4. Conclusion:

In this paper, we attacked the RSA common private exponent. For this we have used the famous lattice reduction algorithm namely LLL. Lattice reduction algorithms play a very important role in cryptanalysis of RSA. Because using lattice reduction algorithm one can break several instances of RSA. This is another instance attacked by lattice reduction algorithm. So one should choose encryption components which have different decryption exponents so that to avoid this attack.

References:

1. H. Cohen, A Course in computational Algebraic Number Theory. Springer-Verlag, second edition, 1995.

2. A. J. Menezes, P.C.van Oorschot, and S.A.Vanstone. Hand book of Applied Cryptography. CRC Press, 1997.

3. A.K. Lenstra, H.W. Lenstra Jr., and L.Lovasz. Factoring polynomials with rational coefficients. Mathematische Annalen, volume 261(4): pages 515-534, 1982.

4. R.Kannan. Algorithmic geometry of numbers. Annual Review of Computer Science, (231-267), 1987.

5. Babai, L. On Lovasz lattice reduction and the nearest lattice point problem. Combinatorica, 6:1-13 (1986).

6. P. Schnorr and M. Euchner, Lattice basis reduction: Improved practical algorithms and solving subset sum problem, Math.Prog., 66: 181- 199,1994.

5. A. Shamir. A polynomial-time algorithm for breaking the basic Merkle-Hellman cryptosystem. IEEE Transactions on Information Theory, 1984.

6. R .C. Merkle and M.E. Hellman. Hiding information and signatures in trapdoor knapsacks. IEEE Transactions on Information Theory, IT-24(5):525-530, September 1978.

7. R.L.Rivest, A.Shamir and L.Adleman. A method for obtaining digital signatures and public key cryptosystems. Commun. of the ACM, 21: 120-126, 1978

8. D.Coppersmith. Finding a small root of a univaraite modular equation. Advances in Cryptology Proceedings of EUROCRYPT'96, VOLUME 1070 of Lecture Notes in Computer Science, pages 155-165. Springer-Verlag, 1996.

9. N.A. Howgrave - Graham. Finding small solutions of univaraite modular equations revisited. In Cryptography and Coding, volume 1355 of LNCS, pages131-142. Springer-Verlag, 1997.

10. Don Coppersmith, Matthew Franklin, Jacques Patarin, Michael Reitert. Low Exponenet RSA with related messages.

11. R.Kannan. Algorithmic geometry of numbers. Annual Review of Computer Science, (231-267), 1987.

12. Victor Shoup. NTL: A library for doing number theory. Website: http://www.shoup.net/ntl/

13. Nguyen, P.Q and Stern, J. The two faces of lattices in cryptology. In J.H.Silverman, editor, Cryptography and Lattices, Internatiional Conference (CaLc 2001), number 2146 in Lecture Notes in Computer Science, pages 146-180 (2001).

14. Regev O. On the complexity of lattice problems with polynomial approximation factors (2007). Survey paper prepared for the LLL+25 conference.