Lattice based Attacks on Small Private Exponent RSA: A Survey

R. Santosh Kumar
Department of IT
MVGR College of Eng., INDIA

C.Narasimam
Department of CSE
V.R.SIDDARTHA ENGG COLLEGE, INDIA

S.Pallam Setty
Department of CS&SE
ANDHRA UNIVERSITY
INDIA

ABSTRACT

Lattice basis reduction algorithms have contributed a lot to cryptanalysis of RSA crypto system. With coppersmith's theory of polynomials, these algorithms are searching for the weak instances of Number-theoretic cryptography, mainly RSA. In this paper we present several lattice based attacks on low private exponent of RSA.

Keywords: Lattices, Lattice basis reduction, RSA, Cryptanalysis.

1. INTRODUCTION

A normal RSA decryption/signature requires time O(log d log^2N). Selecting a small value for the secret exponent d can significantly increase the speed for the normal RSA decryption process/signature process. However, recent attacks show small private exponents should be handled with care as they may be threaten RSA's security. In this paper we present some lattice based attacks mounted against RSA instances with small secret exponent d. Firstly we present the wiener attack in terms of lattices. The original paper of wiener used continuous fractions to derive the bound 0.25. Next, Boneh improved this bound to 0.292. Initially they solved the problem to 0.284. Later they improved the bound to 0.292, but used complicated techniques called geometrical progressive matrices. Later May used simplified analysis, but they got the bound 0.290, which is worse than the Boneh method, but the analysis is much simpler.

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 $b_i$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][3].

2.2 Lattice reduction

Lattice reduction is a old problem in number theory. Lattice reduction reduced the given lattice into "short" basis. Here "short" in the sense that Euclidean distance. In the literature, so many lattice reduction algorithms exist but the one given by Lenstra, Lenstra, Lovasz is a famous one. Because there exists polynomial time algorithm for this reduction and it solves SVP problem of lattices in some sense.

2.3 LLL reduced

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 $\frac{1}{4} < \delta < 1$. 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. 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. The other properties can be found in [3].

2.4 RSA Cryptosystem:

The well known RSA cryptosystem was the first publicly known public key cryptosystem introduced by Rivest, Shamir, Adleman [5]. In this paper, we consider only instances of RSA with balanced primes. Balanced primes are the primes which have the same size. Also we assume that $4 < \frac{1}{2} N^{1/2} < p < N^{1/2} < q < 2N^{1/2}$. So, if p, q are balanced primes then the following inequality hold: $|N - \varphi(N)| < 3N^{1/2}$.

2.5 Resultant of two bivaraite polynomials:

The resultant of two polynomials $f(x,y)$ and $g(x,y)$with respect to the variable y, is defined as the determinant of Sylvester matrix of $f(x,y)$ and $g(x,y)$ when considered as polynomials in the single indeterminate y. The resultant is non-zero if and only if the two polynomials are algebraically independent . When the polynomials are algebraically independent, the resultant yields a new polynomial $h(x)$ such that if (x_0, y_0) is a root of both $f(x,y)$ and $g(x,y)$ then $h(x_0) = 0$.

Assumption: We assume that the two polynomials return by LLL algorithm are algebraically independent. There is no theoretical proof for this one, but in practice most of the times achieved.

2.6 Howgrave-Graham for Bivariate Integer Polynomials:

Let $h(x,y) \in \mathbb{Z}[x,y]$ be a polynomial in 2 variables with at most w monomials and let m be a positive integer. Suppose in addition that

1) h$(x_0, y_0) \equiv 0(mod\ e^m)$ where $|x_0| < X$ and $|y_0| < Y$, and

2) $\|h(xX, yY)\| \leq \frac{e^m}{\sqrt{w}}$,

then $h(x_0, y_0) = 0$ holds over the integers.

3. WIENER'S ATTACK WITH LATTICES

Wiener proposed the attack [7] on short secret exponent attack using continuous fractions. Later May introduced the same attack using lattice reduction techniques. We present their attack here. Let $N = pq$ be an RSA modulus with balanced primes satisfying$p + q < \frac{3}{\sqrt{2}} N^{\frac{1}{2}}$. Let (e, N) be a valid public key and let d be its corresponding exponent defined modulo $\emptyset(N)$. If the private exponent satisfies $d < \frac{1}{3} N^{\frac{1}{4}}$ then the modulus can be factored in time polynomial in $\log(N)$.

For the derivation of this attack May used the Coppersmith techniques. Consider the key equation modulo N gives $ed + ks - 1 \equiv 0(mod\ N)$, and so $(x_0, y_0) = (d, ks - 1)$ is a root of polynomial $f(x,y) = ex + y$, modulo N. In order to break the instance of RSA we only need to find the small roots of this polynomial modulo N. Typically, this would involve using the heuristic extensions of Coppersmith's methods. That is, using lattice reduction to find two small normed bivariate polynomials that have the root (x_0, y_0) over the integers. We use LLL algorithm to find lattice reduction for the lattice, constructed from the coefficient vectors of $f(xX, yY)$ and $g(xX, yY)$ where $g(x,y) = Nx$. The basis matrix for the lattice is given by $\mathfrak{B} =$. Using the conditions given in the theorem, it follows that

$$|x_0| = d < \frac{1}{3} N^{\frac{1}{4}}$$

$$|y_0| = |ks - 1| < ds < d(p + q) < \frac{1}{\sqrt{2}} N^{3/4},$$

And so the bounds can be defined as $X = \frac{1}{3} N^{\frac{1}{4}}$ and $Y = \frac{1}{\sqrt{2}} N^{\frac{3}{4}}$. All the vectors in the above lattice correspond that have root (x_0, y_0) modulo N. Thus, if two small vectors can be found whose norm satisfies Howgrave-Graham's condition, then these vectors correspond to the coefficient vectors of polynomials with root (x_0, y_0) over the integers. Thus, the private exponent is revealed once a smallest vector is found. If d known, $ed - 1 = k\ \emptyset(N)$ gives a multiple of $\emptyset(N)$, which can be used to factor the modulus.

4. BONEH AND DURFEE SMALL INVERSE ATTACK

Boneh and durfee attack [8] can recover the primes p, q in polynomial time provided that $d \leq N^{0.292}$. Their result is heuristic since it is based on coppersmith's technique for finding small solutions to bivariate modular polynomial equations. However this attack seems to work very well in practice. We sketch the main idea of their attack.

Consider the normal RSA scheme where p, q are balanced and defining equation of the RSA:

$$ed + k(N + 1 - (p + q)) = 1$$

Writing s=-(p+q) and $A = N + 1$, above equation can be simplified to $k(A + s) \equiv 1(mod\ e)$. Also assume $e = N^{\alpha}$ for some α.

Small Inverse Problem: Given a polynomial $f(x,y) \equiv x(A + y) - 1$, find (x_0, y_o) satisfying $f(x_0, y_0) \equiv 0(mod\ e)$ where $|x_0| < e^{\delta}$and $|y_0| < e^{0.5}$. So. if we solve the SIP for this instance, we will get $s = -(p + q)$ and consequently the factorization N. The goal is to recover the values of δ for which the roots (x_0, y_0) with $|x_0| < e^{\delta}$, $|y_0| < e^{0.5}$ can be recovered in polynomial time. The main idea is, first transform the modular equation into an equation over the integers using Howgrave-Graham's lemma for the bivariate case.

For a positive integer m define the polynomials

$$g_{i,k}(x,y) = x^i\ f^k(x,y)e^{m-k}$$

$$h_{j,k}(x,y) = y^j f^k(x,y)e^{m-k} \ .$$

In order to apply Howgrave-Graham's lemma, consider the lattice spanned by the coefficient vectors of the polynomials $g_{i,k}(x,y), h_{j,k}(x,y)$ for certain parameters i, j and k. For each $k = 0,1,2, \cdots, m$ use $g_{i,k}(xX, yY)$ for

$i = 0,1,\cdots,m-k,$ and $h_{j,k}(xX,yY)$ for $j = 0,1,\cdots,t$ for some parameter t to be optimized later. For example see fig 1.

Example for $m = 2$ and $t = 1$:

	1	X	Xy	x^2	x^2y	x^2y^2	y	xy^2	x^2y^3
e^2	e^2								
xe^2		e^2X							
xe	-e	eAX	exy						
x^2e^2				e^2X^2					
xfe		-eX		eAX^2	eX^2Y				
f^2	1	-2AX	-2XY	A^2X^2	2AX^2Y	X^2Y^2			
ye^2							e^2Y		
xfe			eAXY				-eY	eXY^2	
yf^2			-2AXY		A^2X^2Y	2AX^2Y^2	Y	-2XY^2	X^2Y^3

Fig1. Boneh and durfee lattice for $m = 2$ and $t = 1$. (Empty places are filled with zeros)

Let $\mathcal{L}_{BD}$ denote the lattice and $\mathcal{B}_{BD}$ be the corresponding basis. Running LLL algorithm we can obtain two short vectors b_1, b_2 which by inequality, we have $\|b_1\|, \|b_2\| \leq 2^{\frac{w}{2}}\det(\mathcal{L}_{BD})^{\frac{1}{w-1}}$ where w is the dimension of the lattice. Now in order to apply Howgrave-Graham's lemma, we should have

$$2^{\frac{w}{2}}\det(\mathcal{L}_{BD})^{\frac{1}{w-1}} \leq \frac{e^m}{\sqrt{w}}.$$

The determinant and the dimension of the lattice $\mathcal{L}_{BD}$ have the following rules respectively $\det(\mathcal{L}_{BD}) = e^{\frac{5+4\delta}{12}m^3+\frac{3+2\delta}{4}tm^2+\frac{mt^2}{4}+o(m^3)}$

$w = \frac{m^2}{2} + tm + o(m^2)$. Optimizing with respect to t and ignoring low degree terms gives the condition -12$-12\delta^2 + 28\delta - 7 < 0 \Longrightarrow \delta < \frac{7}{6} - \frac{1}{3}\sqrt{7} \approx 0.284$. This means that if $\delta < 0.284$ or, equivalently if $d < N^{0.284}$, one can find in time polynomial in $\log N$ the factorization of N and consequently break RSA.

Improved Bounds: The results in last section show that the small inverse problem can be solved when $\delta <$ 0.284. The bound is derived from the determinant of the lattice L, which gives an upper bound on the lengths of the shortest vectors of the lattice. In the last section, we compute the determinant of a lattice L generated by shifts and powers of f. Since L is full rank and corresponding matrix is triangular, the determinant is just the product of the entries on the diagonal-carefully balanced so that this product is less than 1. Once $\delta > 0.284$ the approach no longer works, as the product exceeds 1 for every choice of m. But if the some of the larger terms of this product were removed, we might be able to find greater values of δ. This suggests that one can ignore some rows which have large diagonal values. But unfortunately the resulting lattice is not full rank, and computing its determinant is not so easy. Boneh-Durfee used the strategy called "Geometric progressive matrices" to improve the bound to 0.292. For full details refer[8].

5. BLOMER AND MAY'S ATTACK

Blomer and May revisited the above attack. They come up with the bound 0.290. Even though it is worse than Boneh and Durfee's bound, analysis is much simpler than Boneh and Durfee. They begin their analysis by choosing parameters m, t and then construct exactly the same lattice as Boneh and Durfee, before removal the rows with corresponding basis of B_{BD}. Next they remove certain rows of B_{BD} to take an intermediate matrix $\bar{B}$. Let $\bar{\mathcal{L}}$ be the lattice spanned by $\bar{B}$. Unlike Boneh-Durfee, they go on removing an equal number of columns in order to obtain a square matrix. As an example, the following matrix corresponds to matrix after removal of certain rows and columns. We denote the final matrix constructed by Blomer and May as B_{BM} and the corresponding lattice $\mathcal{L}_{BM}$. The row vectors of the matrix B_{BM} are no longer the coefficient vectors of the polynomials $g_{i,k}(xX,yY)$ and $h_{j,k}(xX,yY)$ since they have removed some columns from the initial basis matrix B_{BD}. For example of a basis see fig 2. Notice that the basis constructed by Boneh and Durfee does not suffer from the same drawback since they have only removed rows but not columns. In order to apply Howgrave's theorem, it is necessary to ensure that the linear combination of bivaraite polynomials evaluates to zero modulo e^m. Blomer and May show how associate the rows of B_{BM} matrix with the polynomials $g_{i,k}$ and $h_{j,k}$. This means that they show how to reconstruct a vector $\bar{u} \in \bar{\mathcal{L}}$ by a vector $u \in \mathcal{L}_{BM}$. More significantly, they prove that short vectors $u \in \mathcal{L}_{BM}$ lead to short reconstruction vector $\bar{u} \in \bar{\mathcal{L}}$. Expressed in a different way, the size of small vectors found in the eliminated lattice $\mathcal{L}_{BM}$ by LLL is the same size as those found in the original lattice $\bar{\mathcal{L}}$ up to a small correction term. For full details of this adjustment refer[12].

Example of a Blomer and May lattice for $m = 2$ and $t = 1$:

	X	Xy	x^2	x^2y	x^2y^2	x^2y^3
xe^2	e^2X					
Xe	eAX	Exy				
x^2e^2			e^2X^2			
xfe	-ex		eaX^2	eX^2Y		
f^2	-2AX	-2XY	A^2X^2	2AX^2Y	X^2Y^2	
yf^2		-2AXY		A^2X^2Y	2AX^2Y^2	X^2Y^3

Fig 1: Blomer –May lattice for m=2 and t=1

Although it yields a weaker bound than Boneh and Durfee method, the new approach followed by Blomer and May has some advantages. They are a) It leads to simple proofs since one deals with square matrices which significantly simplifies determinant calculations. b) It reduces the lattice dimension as a function of m and t which implies that one can get closer to the theoretical bound. c) It makes use of structural properties of the underlying polynomials which makes possible extension to other lattice constructions using these polynomials.

6. CONCLUSION

In this paper we investigate main techniques to derive bound for the secret exponent RSA. Wiener provided the bound 0.25 initially. But later Boneh improved the bound upto 0.292. May proposed another technique which is easy to analysis, but the bound they achieved is 0.290. It is an open problem for RSA, if secret exponent is greater than 0.292 without having the partial knowledge of any parameter. If secret exponent is greater than 0.292, then there is no any current knowledge for RSA security if there is no any partial information about the parameters of RSA cryptosystem.

7. REFERENCES

[1] Cohen, H. 1995. A Course in Computational Algebraic Number Theory. Springer-Verlag. Second edition.

[2] Menezes, A.J, Van Oorschot P.C, and Vanstone. 1997. Hand book of Applied Cryptography. CRC Press.

[3] Lenstra A.K, Lenstra Jr. H.W, Lovasz L. 1982. “Factoring polynomials with rational coefficients”. Mathematische A1nnalen, volume 261(4): pages 515-534.

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

[5] Coppersmith D. 1997. “Small solution to polynomial equations, and low exponent RSA vulnerabilities. Journal of Cryptology”, 10(4):233-260.

[6] Howgrave-Graham N. 1997. Finding small roots of univariate modular equations revisited. Proceedings of Cryptography and Coding, Springer-LNCS, vol. 1355, Springer-Verlag, pp.13-142.

[7] Wiener M.J. 1990. Cryptanalysis of short RSA secret exponents. IEEE Trans. In formation Theory, 36(3):553:559.

[8] Boneh.D, and Durfee,G. 2000. Cryptanalysis of RSA with private key d less than N^0.292.IEEE Transactions on information Theory, 46(4):1339-1349.

[9] D.Boneh, G.Durfee,Y.Frankel. 1998 An attack on RSA given fraction of the private key bits. Proceeding of Asiacypt’98. Springer-Verlag, LNCS 1514:25-34.

[10] M. Ernst, E. Jochemsz, A,May, and D.Weger 2005. Partial key exposure attacks on RSA upto full size exponents. Advances in Cryptology –Eurocrypt 2005. Springer-Verlag, LNCS 3494:371-386.

[11] P. Schnorr and M. Euchner. 1994. Lattice basis reduction: Improved practical algorithms and solving subset sum problems Math.Prog. 66: 181-199.

[12] Blomer, May. 2001. Low Secret Exponent RSA Revisited. Cryptography and Lattice Conference (CaLC 2001). Springer Lecture Notes in Computer Science Volume 2146 **.**

[13] Santosh kumar R, Narasimham C, Pallam setty S.2012 Lattice based tools for cryptanalysis in various applications. Springer-LNICST, 84:530-537.

[14] Boneh.,D. 1999. Twenty Years of Attacks on the RSA Cryptosystem. Notices the AMS 46(2), 203-213.

[15] Durfee, G, Nguyen, P.Q.2000. Crtptanalysis of the RSA schemes with short exponent from Asiacrypt ’99. Proceedings of cryptography-ASIACRYPT, LNCS 1976, Springer-Verlag, pp 1-11.

[16] H.M. Sun, W.C Yang, C.S. Laih.1999. On the design of RSA with short secret exponent. Proceedings of Cryptology – ASIACRYPT’99,LNCS 1716, Springer-Verlag, pp.120-126,1978.

[17] Verhaul, E., van Tilborg.1997. “Cryptanalysis of less short RSA secret exponents”. Applicable Algebra of Engineering, Communication and Computing, Vol.8, Springer-Verlag, pp.425-435.

[18] Aono,Y. 2009. Simplification of the lattice based attack of Boneh and Durfee for RSA cryptoanalysis. Proceedings of joint conference of ASCM and MACS.

[19] Victor Shoup. NTL: A library for doing Number Theory, online available at http://shoup.net/ntl.