Volume 6, No.1, January 2019

Journal of Global Research in Mathematical Archives

ISSN 2320 – 5822

UGC Approved Journal

RESEARCH PAPER

Available online at http://www.jgrma.info

IMPLEMENTING WIENER ATTACK WITH LATTICE REDUCTION

P. Anuradha Kameswari, S B T Sundari Katakam
Department of Mathematics, Andhra University,
Visakhapatnam - 530003, Andhra Pradesh, India.
panuradhakameswari@yahoo.in, sribalakatakam@gmail.com

Abstract:In this paper, approximation via lattice reduction is described and is adapted in implementing Wiener Attack on RSA cryptosystem with lattice reduction. The continued fraction based arguments of Wiener Attack are implemented with the Lattice based arguments and the LLL algorithm is used for reducing a basis of a lattice.

Key words :Lattice reduction, LLL algorithm, quadratic form, Wiener Attack.

1 INTRODUCTION

Wiener Attack on RSA cryptosystem for $N=pq$ is based on the idea that certain bound of the decryption exponent d allow the fraction $\frac{t}{d}$ to be a convergent of $\frac{e}{N}$ for e the encryption exponent and $t=\frac{ed-1}{\phi(N)}$.This search of the convergent $\frac{t}{d}$ is interpreted in this paper as finding a short vector of a positive definite quadratic form $q(x,y)$. This may be attained by applying LLL algorithm for the corresponding lattice of $q(x,y)$. In this context, we first describe approximation via lattice reduction and obtain the short vector, by applying LLL algorithm. Later, this idea is interpreted for Wiener Attack.

2 WIENER ATTACK ON RSA

The approximation of a real number α by a rational number $\frac{y}{x}$, as suggested by approximation theorem is obtained in the class of convergents of α[3].

Theorem 1 (**Approximation Theorem**): If α is a real number, and $\frac{y}{x}$ is a rational number with $|\alpha-\frac{y}{x}|\leq\frac{1}{2x^2}, x\geq 1$, then $\frac{y}{x}$ must be a convergent for α.

If $N=pq$, for $q<p<2q$ is the modulus for RSA, e is the public enciphering exponent and d is the deciphering exponent such that $ed-1=\phi(N)t$, the main idea of Wiener's attack is that certain restrictions on d allow the fraction $\frac{t}{d}$ to be a convergent of $\frac{e}{N}$, which may be proved from the estimation of $\phi(N)$ as, $N-3\sqrt{N}<\phi(N)<N$. Wiener Attack is based on the following theorem.

Theorem 2 Let (N,e) be the public key with $N=pq$ such that $q<p<2q$ and $d<\frac{N^{1/4}}{\sqrt{6}}$ then $|\frac{e}{N}-\frac{t}{d}|\leq\frac{1}{2d^2}$.

Proof. From the right inequality of the above result, we have

$$N-3\sqrt{N}<\frac{ed-1}{t}$$

$$t(N-3\sqrt{N})<ed-1$$

$$\frac{tN-3\sqrt{N}t}{dN}<\frac{ed-1}{dN}$$

$$\frac{t}{d}-\frac{e}{N}<\frac{3t}{d\sqrt{N}}-\frac{1}{dN} \qquad (1)$$

Also,

$$ed+1=\phi(N)t+2$$

$$<tN+3t\sqrt{N} \qquad as\ \ 2<3t\sqrt{N}$$

$$\frac{ed+1}{dN}<\frac{tN+3t\sqrt{N}}{dN}$$

$$\frac{1}{dN}-\frac{3t}{d\sqrt{N}}<\frac{t}{d}-\frac{e}{N}$$

$$-\left(\frac{3t}{d\sqrt{N}}-\frac{1}{dN}\right)<\frac{t}{d}-\frac{e}{N} \qquad (2)$$

From, (1) and (2) we have,

$$\left|\frac{e}{N}-\frac{t}{d}\right|<\frac{3t}{d\sqrt{N}}$$

which implies,

$$\left|\frac{e}{N}-\frac{t}{d}\right|<\frac{3}{\sqrt{N}} \qquad as\ \ t<d$$

$$\left|\frac{e}{N}-\frac{t}{d}\right|<\frac{1}{2d^2} \qquad as\ \ d<\frac{N^{1/4}}{\sqrt{6}}.$$

Hence by approximation theorem it follows that $\frac{t}{d}$ is a convergent of $\frac{e}{N}$. □

Wiener Attack on RSA basically searches the convergent $\frac{t}{d}$ from the class of convergents of $\frac{e}{N}$ that lead to (p,q,d).

Theorem 3 (**Wiener Attack**): Let $d\le\frac{N^{\frac{1}{4}}}{\sqrt{6}}$ and for any convergent $\frac{t'}{d'}$ of $\frac{e}{N}$, take $\phi'(N)=\frac{ed'-1}{t'}$, $x'=\frac{N-\phi'(N)+1}{2}$ and $y'=\sqrt{x'^2-N}$. If $x',y'\in N$, then the private key $(q,p,d)=(x'-y',x'+y',d')$.

Therefore, the search of $\frac{t}{d}$ leading to solution (p,q,d) may be obtained form the class of convergents of $\frac{e}{N}$. This search of integers y and x now can be interpreted as finding a short vector (x,y) of some quadratic form [11] in the following.

3 IMPLEMENTATION OF WIENER'S ATTACK IN TERMS OF LATTICE REDUCTION

Definition 1 A Lattice L is a discrete additive subgroup of $\mathbf{R}^m$, that is L is the $\mathbf{Z}$−span of a linearly independent subset of $\mathbf{R}^m$:

$$L=\mathbf{Z}b_1+\mathbf{Z}b_2+\ldots+\mathbf{Z}b_n$$

with the quadratic form $q(x)=<x,x>$, for $x\in L$. The vectors $b_1,b_2,\ldots,b_n$ are a basis for L, and $A=[<b_i,b_j>]_{1\le i,j\le n}$ is the corresponding Gram matrix also note $q(x)=x^TAx$.

Definition 2 The short vector in a lattice L is a nonzero vector $v\in L$ that minimizes the Euclidean norm $||v||$.

Definition 3 Let $\mathbf{B}=<b_1,b_2,\ldots,b_n>$ be a basis for a lattice L and let $\mathbf{B}^*=<b_1^*,b_2^*,\ldots,b_n^*>$ be the associated Gram - Schmidt orthogonal basis. The basis $\mathbf{B}$ is said to be *LLL* reduced if it satisfies the following two conditions:

1. $|\mu_{i,j}|=\frac{|b_i b_j^*|}{||b_j^*||^2}\le\frac{1}{2}$ for all $1\le j<i\le n$.

2. $||b_i^*||^2\ge(\frac{3}{4}-\mu_{i,i-1}^2)||v_{i-1}^*||^2$ for all $1<i\le n$.

Theorem 4 Let L be a lattice of dimension n. Any *LLL* reduced basis $<b_1',b_2',\ldots,b_n'>$ for L has the following two properties:

1. $\prod_{i=1}^{n}||v_i||\le 2^{n(n-1)/4}\det L$.

2. $\|v_j\| \leq 2^{(i-1)/2} \|v_i^*\|$ for all $1 \leq j \leq i \leq n$.

Remark 1 The *LLL* algorithm comes close to solve *SVP* in small dimensions, as the initial vector in an *LLL* reduced basis satisfies $\|v_1\| \leq 2^{n(n-1)/4} |\det L|^{1/n}$.

If $N=pq$, for $q<p<2q$ is the modulus for RSA, e is the public enciphering exponent and d is the deciphering exponent such that $ed-1=\phi(N)t$, we now implement the Wiener Attack via Lattice reduction. In this context we first note any short vector (x,y) of a quadratic form $q(x,y)=M(\bar{\alpha}x-y)^2+\frac{1}{M}x^2$ for $M=10^s$, is such that $\frac{y}{x}$ is a rational approximation of α.

Theorem 5 If α is a real number then for $M=10^s$, for some $s>0$, integer with $\bar{\alpha}$ a decimal approximation of α to precision $\frac{1}{M}$, any short vector (x,y) of the quadratic form $q(x,y)=M(\bar{\alpha}x-y)^2+\frac{1}{M}x^2$ is such that $\frac{y}{x}$ is a rational approximation of α.

Proof. For a given α choose M with $\bar{\alpha}$, a decimal approximation to $\frac{1}{M}$ and the quadratic form $q(x,y)=M(\bar{\alpha}x-y)^2+\frac{1}{M}x^2$. Now, we obtain the short vector (x,y) by reducing the lattice Z^2 equipped with quadratic form,

$$q(x,y)=M(\bar{\alpha}x-y)^2+\frac{1}{M}x^2$$

The 2-dimensional Gram-matrix associated with the quadratic form is given by a symmetric positive definite matrix,

$$A=\begin{bmatrix} \bar{\alpha}^2 M+\frac{1}{M} & -\bar{\alpha}M \\ -\bar{\alpha}M & M \end{bmatrix}$$

whose determinant is 1, and hence it corresponds to a lattice of determinant 1 .

The underlying lattice in the Euclidean space R^2 is given by the matrix B,

$$B=\begin{bmatrix} \frac{1}{\sqrt{M}} & 0 \\ \bar{\alpha}\sqrt{M} & -\sqrt{M} \end{bmatrix}$$

whose columns forms a basis for the lattice. Let $b_i's$ be the rows of B^T. Applying LLL algorithm to B^T, the resultant of LLL is then a reduced basis B' of the same lattice. As B and B'^T are the matrices whose columns represent basis of the same lattice,d B and B' are related by integer unimodular transformation matrix, U as $BU=B'^T$. Therefore, the matrix U, is obtained by $U=B^{-1}B'^T$,

$$U=\begin{bmatrix} ab \\ cd \end{bmatrix}$$

the vector(a,c) short vector (x,y). This short vector (x,y) is such that $\frac{y}{x}$ is a rational approximation of α.

By LLL for any short vector $(x_1,x_2,....,x_n)$ we have $q(x_1,...x_n) \leq 2^{\frac{n-1}{2}} \det q\, 1n$, Thus, we have for the 2-dimensional lattice L above $q(x,y) \leq \sqrt{2}$.

Therefore, we have

$$q(x,y) = M(\bar{\alpha}x-y)^2 + \frac{1}{M}x^2 \leq \sqrt{2}$$

$$M(\bar{\alpha}x-y)^2 \leq \sqrt{2} \text{ and } \frac{1}{M}x^2 \leq \sqrt{2}$$

$$(\bar{\alpha}x-y)^2 \leq \frac{\sqrt{2}}{M} \text{ and } x^2 \leq \sqrt{2}M$$

$$|\bar{\alpha}x-y|^2 \leq \frac{\sqrt{2}}{M} \text{ and } |x|^2 \leq \sqrt{2}M$$

Now, as $\bar{\alpha}$ is a decimal approximation of α to precision $\frac{1}{M}$, we have $|\alpha-\bar{\alpha}| \leq \frac{1}{M}$ and using the inequalities above, we get:

$$\begin{aligned}|\alpha x-y| &= |\alpha x-\bar{\alpha}x+\bar{\alpha}x-y| \\ &\leq |\alpha x-\bar{\alpha}x|+|\bar{\alpha}x-y| \\ &= |x(\alpha-\bar{\alpha})|+|\bar{\alpha}x-y| \\ &= |x||(\alpha-\bar{\alpha})|+|\bar{\alpha}x-y| \\ &\leq 2\cdot 14\sqrt{M}\frac{1}{M}+\frac{2\cdot 14}{\sqrt{M}} \\ &= 2.2\cdot 14.\frac{1}{\sqrt{M}} \\ &= 2.2\cdot 14.\frac{1}{\sqrt{M}} \\ &= 2\cdot 54.\frac{1}{\sqrt{M}}\end{aligned}$$

which implies, $|\alpha-\frac{y}{x}| = |\frac{\alpha x-y}{x}| \leq \frac{2\cdot 14}{\sqrt{M}x} \leq \frac{2\cdot 54}{x^2} = \frac{1}{kx^2}$, for $k = \frac{1}{2\cdot 54}$.

Therefore,as for all $k < \sqrt{5}$ by [6] we have $\frac{y}{x}$ is a rational approximation of α, $\frac{y}{x}$ is a rational approximation of α □

In the following theorem (d,t) is interpreted as a short vector.

Theorem 6 Let $N=pq$, for $q<p<2q$ be the modulus for RSA, e be the public enciphering exponent and d be the deciphering exponent. Then for t such that $ed-1=\phi(N)t$, (d,t) is a short vector of a lattice $\mathbf{Z^2}$ equipped with a quadratic form

$$q(d,t) = M(\bar{\frac{e}{N}}d-t)^2 + \frac{1}{M}d^2$$

for an appropriate M.

Proof. First note for each choice of $M=10^l$ for some l, and $\bar{\frac{e}{N}}$ decimal approximation of $\frac{e}{N}$ to the precision $\frac{1}{M}$ we reduce the lattice $\mathbf{Z}^2$ with a quadratic form $q(x,y)$ in the variables d,t given as

$$q(d,t) = M\left((\bar{\frac{e}{N}})d-t\right)^2 + \frac{1}{M}d^2,$$

and the 2-dimensional Gram-matrix for the above is given as

$$A = \begin{bmatrix} \left(\bar{\frac{e}{N}}\right)^2 M+\frac{1}{M} & -\left(\bar{\frac{e}{N}}\right)M \\ -\left(\bar{\frac{e}{N}}\right)M & M \end{bmatrix}$$

and note the corresponding lattice in R^2 is given by the basis as columns of matrix B given as

$$B=\begin{bmatrix} \frac{1}{\sqrt{M}} & 0 \\ \lceil \frac{e}{N} \rceil \sqrt{M} & -\sqrt{M} \end{bmatrix}$$

which may be deduced by the results in *Lattices and Quadratic Forms* of [4]. Now applying LLL algorithm to B^T, we get reduced basis matrix *B*' and repeating the arguments as above we have a integer umimodular transformation matrix *U*

$$U=\begin{bmatrix} ab \\ cd \end{bmatrix}$$

with (*a*,*c*) as short vector obtained for the choice of $M=10^l$

Now note for any (*v*,*u*) such that $\frac{u}{v}$ is an approximation of $\frac{e}{N}$, we have

$$q(v,u)=M(\lceil \frac{e}{N}v-u)^2+\frac{1}{M}v^2$$

$$=Mv(\lceil \frac{e}{N}-\frac{u}{v})^2+\frac{1}{M}v^2$$

$$=MvO(\frac{1}{v^4})+\frac{v^2}{M}$$

$$=O(\frac{M}{v^3})+O(\frac{v^2}{M})$$

$$=O(1)+O(\frac{v^2}{M})$$

$$\Rightarrow q(v,u)=O(1)+O(\frac{v^2}{M})$$

Therefore, for any short vector (*v*,*u*) as $q(u,v)=O(1)$, note for $M\approx d^2$ the above holds for $v,v\approx d$. Therefore by theorem 2 as the required t,d are such that $\frac{t}{d}$ is an approximation to $\frac{e}{N}$, (*d*,*t*) is a short vector for the given quadratic form $q(d,t)=M\left(\left(\frac{\bar{e}}{N}\right)d-t\right)^2+\frac{1}{M}d^2$, for $M\approx d^2$.

□

Note 1 The search of convergents $\frac{t}{d}$ leading to solution (*p*,*q*,*d*) may be obtained form the class of short vectors(*d*,*t*) for $q(d,t)=M(\lceil \frac{e}{N}d-t)^2+\frac{1}{M}d^2$ for an appropriate choice of *M*. In the following theorem it is proved that such *M* is possible under certain restrictions to *d*. This process can be interpreted as Wiener Attack via lattice reduction.

Theorem 7 (Wiener's attack via Lattice Reduction): Let $N=pq$, for $q<p<2q$ be the modulus for RSA, *e* be the public enciphering exponent and *d* be the deciphering exponent. If $d\leq \frac{N^{\frac{1}{4}}}{\sqrt{6}}$, then there is a *M* such that (*d*,*t*) is a short vector of the quadratic form, $q(d,t)=M\left(\left(\frac{\bar{e}}{N}\right)d-t\right)^2+\frac{1}{M}d^2$, where $\lceil \frac{e}{N} \rceil$ is a decimal approximation of $\frac{e}{N}$ to precision $\frac{1}{M}$.

Proof. By theorem 2 as the required *t*,*d*are such that $\frac{t}{d}$is an approximation to $\frac{e}{N}$, we have by above theorem that (*t*,*d*) is a short vector for a quadrtaic form

$$q(d,t)=M\left((\frac{\bar{e}}{N})d-t\right)^2+\frac{1}{M}d^2$$

for $M=10^l$ for some appropriate l, such that $d\approx\sqrt{M}$. Now to find (d,t) we search this appropriate M in the following: Let $d(N)$ be the number of digits in N and let

$$r=$$

[Sorry. Ignored \begin{cases} ... \end{cases}]

Note for $1\leq s\leq r$, we have $\sqrt{M_s}\leq N^{\frac{1}{4}}$ for $M_s=10^s$ and if $d\leq\frac{N^{\frac{1}{4}}}{\sqrt{6}}$ we have $d^2\leq 10^l$ for some l with $l\leq r$, therefore varying s in the range $1\leq s\leq r$, as s reaches l, we have $d^2\approx M_l$ and the corresponding short vector is the required (d,t). Further note for $d>\frac{N^{\frac{1}{4}}}{\sqrt{6}}$, $\frac{t}{d}$ need not be a convergent of $\frac{e}{N}$, that is $\frac{t}{d}$ need not be an approximation of $\frac{e}{N}$ to precision $1/M$ and $M=10^l$and hence (d,t) need not be obtained as a short vector of the quadratic form for some M,

□

After computing the short vector (d_s,t_s), the implementation of Wiener Attack is as follows:

Theorem 8 (**Implementation of Wiener's attack**): Let $d\leq\frac{N^{\frac{1}{4}}}{\sqrt{6}}$ and let$M=10^s$ for $1\leq s\leq r$, then for short vector (d_s,t_s) of the quadratic form,

$$q(d,t)=M\left((\frac{\bar{e}}{N})d-t\right)^2+\frac{1}{M}d^2$$

take $\phi'(N)=\frac{ed_s-1}{t_s}$,$x_s=\frac{N-\phi'(N)+1}{2}$ and $y_s=\sqrt{x_s^2-N}$. If $x_s,y_s\in N$, then the private key $(q,p,d)=(x_s-y_s,x_s+y_s,d_s)$.

Algorithm:

Step 1: Start

Step 2: Input e,N.

Step 3: Compute $\frac{e}{N}$ to r decimals, where

$$r=$$

[Sorry. Ignored \begin{cases} ... \end{cases}]

Step 4: Set i=1.

Step 5: Set $M=10^i$, $-\frac{e}{N}=\frac{e}{N}$ corrected to i decimal places.

Step 6: Set

$$B=\begin{bmatrix}\frac{1}{\sqrt{M}} & 0\\ (\frac{e}{N})\sqrt{M} & -\sqrt{M}\end{bmatrix}$$

Apply LLL algorithm to B^T and then obtain unimodular transformation matrix $U=B^{-1}(B')^T$, where B' is the resultant obtained using LLL

$$U=\begin{bmatrix}ab\\ cd\end{bmatrix}$$

Set $t=|c|,d=|a|$

Step 7: Compute $\phi(N)=\frac{ed-1}{t}$, $x=\frac{N-\phi(N)+1}{2}$,$y=\sqrt{x^2-N}$.

Step 8: If $\phi(N),x,y\in N$, then $(q,p,d)=(x-y,x+y,d)$, otherwise $i=i+1$ and go to step 5.

Example: Consider e=34595358402895546770510006990670130755550298 83 and N=722911237816849840536444728651897065509097364 87 public key for RSA.

We have $d(N)$=47 and r=24. Now, for $1\leq s\leq r$, we take $M=10^s$ and compute (d_s,t_s) the short vector of the quadratic form,

$$q(d,t)=M\left((\frac{\bar{e}}{N})d-t\right)^2+\frac{1}{M}d^2$$

,where $\bar{\frac{e}{N}}$ the decimal approximation of $\frac{e}{N}$ to precision $\frac{e}{N}$.

And $\frac{e}{N}$=0.047855610195480609486718232576811233202813560300492269 76..... . Now our aim is to find the private key $(q,p,d.)$.

Start Choosing $M=10^1$ and find the decimal expansion of $\frac{e}{N}$ to 1 corrected decimals. Construct matrix B and apply LLL algorithm to B^T and find the short vector, if this short vector is desired convergent. Then stop, otherwise update $M=10^2$ and repeat the procedure till we obtain a short vector which is desired convergent. In this case, we didn't get the required convergent till $M=10^{12}$ as none of the short vectors satisfy Wiener implementation theorem. Now, update $M=10^{13}$ and find the decimal expansion of $\frac{e}{N}$ to 13 corrected decimals. Then, , $\bar{\frac{e}{N}}$=0.0478556101955. Now construct the matrix B and apply LLL algorithm to B^T :

$$B^T=\begin{bmatrix}31239/98786391826 & 36625546597/242020\\ 0 & -289221914799/91460\end{bmatrix}$$

Now, the LLL matrix, B' is given by :

$$B'=\begin{bmatrix}-38566013733/98786391826 & -83777387/1106757460\\ -47941837281/98786391826 & 1365400829/553378730\end{bmatrix}$$

Now, B^{-1} is given by:

$$B^{-1}=\begin{bmatrix}98786391826/31239 & 0\\ 1654559689495598751542590 6/1093325760999085340 61 & -91460/289221914799\end{bmatrix}$$

Finally, the unimodular integral transformation matrix is given by:

$$U=\begin{bmatrix}-1234547 & -1534679\\ -59080 & -73443\end{bmatrix}$$

Now, required convergent is given by, $\frac{t}{d}=|\frac{-59080}{-1234547}|=\frac{59080}{1234547}$. Then, by Weiner implementation theorem,we get:

$\phi'(N)=\frac{ed-1}{t}$

$=\frac{(34595358402895546770510006990670130755550298 83)(1234547)-1}{59080}$

=722911237816849840536439025056039910525936946 00,

$x'=\frac{N-(N)+1}{2}$

$=\frac{722911237816849840536444728651897065509097364 87-722911237816849840536439025056039910525936946 00+1}{2}$

=285179792857749158020944

$y'=\sqrt{x'^2-N}$

=950599309525508419789 07.

Finally, the private key $(q,p,d)=(x'-y',x'+y',d)$=(190119861905198316042037,380239723810299999999851,1234547). The process of this example is given in the following table.

[Sorry. Ignored \begin{sidewaystable} ... \end{sidewaystable}]

[Sorry. Ignored \begin{section} ... \end{section}]

REFERENCES

[1] Tom M. Apostol, Introduction to Analytical Number Theory, Springer International student edition, Narosa Publishing House, ISBN: 81-85015-12-0.
[2] J. Buchmann, Introduction to cryptography , Springer-Verlag 2001.
[3] David M. Burton, Elementary Number Theory , Second Edition, Universal Book Stall, New Delhi.
[4] H.Cohen, A course in Computational Algebraic Number Theory, Graduate Texts in Math.138. Springer-1996, ISBN: 3-540-55640-0.
[5] S.C. Coutinho, The Mathematics of Ciphers, University Press, ISBN: 81 7371 442 8.
[6] H. Davenport, The Higher Arithmetic, Cambridge University Press, Eighth edition, 2008, ISBN: 978-1-107-68854-4.
[7] Jeffery Hoftstein, Jill Pipher, Joseph H. Silverman, An Introduction to Mathematical Cryptography, Springer, ISBN: 978-0-387-77993-5.
[8] P. Anuradha Kameswari, L. Jyotsna, Extending Wienerâ€™s Extension to RSA-Like Cryptosystems over Elliptic Curves, British Journal of Mathematics and Computer Science, 14(1): 1-8, 2016, Article no.BJMCS.23036, ISSN: 2231-0851, SCIENCEDOMAIN international.
[9] Neal Koblitz, A course in Number Theory and cryptography,Graduate Texts in Mathematics, second edition, Springer, ISBN 3-540-78071-8.
[10] A.K.Lenstra, H.W. Lenstra and L. Lovasz, Factoring Polynomials with Rational coefficients, Math.Ann.261, pg.no. 515-534, 1982, Springer - Verlag.
[11] Phong Q. Nguyen, Brigitte VallÃ©e (Eds.)The LLL Algorithm, Survey and Applications, Springer, ISBN: ISBN 978-3-642-02295-1.
[12] Nigel P.Smart, The Algorithmic Resolution of Diophantine Equations, London Mathematical Society, Student Texts 41, ISBN: 0 521 64633 2.
[13] Michael J.Wiener, Cryptanalysis of short RSA secret exponent, IEEE. Transaction on Information Theory, Vol.36, No.3, May 1990.

