International Journal of Soft Computing and Engineering (IJSCE)
ISSN: 2231-2307, Volume-3, Issue-2, May 2013

Small Secret Exponent Attack on Multiprime RSA

Santosh Kumar R, Narasimham Ch, Pallam Setty S

Abstract- Lattice reduction is a powerful algorithm for cryptanalyzing public key cryptosystems, especially RSA. There exist several attacks on RSA by using the lattice reduction techniques. In this paper, we attack on the version of RSA, called Multiprime RSA, by using the lattice reduction techniques.

Index Terms- Lattice reduction, Multiprime RSA, Unravelled linearization.

I. INTRODUCTION

Multiprime RSA is a version of original RSA. In Multiprime RSA, the modulus is a product of three or more primes. The encryption process is similar to the original RSA. The decryption and signature schemes can be done by Chinese Remainder Theorem. As in original RSA, there exists lattice based attacks for this version too. In this paper, we present an attack on multiprime RSA by using unravelled linearization .

II. MATHEMATICAL PRELIMANRAIES

A. Lattices

Let $B = \{b_1, b_2, \cdots, b_n\}$ be set of n linearly independent vectors in $\mathbb{R}^m$. The lattice generated by B is the set $\mathcal{L}(B) = \{\sum_{i=1}^{n} x_i . b_i : x_i \in \mathbb{Z}\}$. That is, the set of all integer linear combinations of the basis vectors. The set B is called basis and we can compactly represent it as an $m * n$ matrix each column of whose is a basis vector: $B = [b_1, b_2, \cdots, b_n]$. The rank of the lattice is defined as $rank(\mathcal{L}) = n$ while its dimension is defined as $\dim(\mathcal{L}) = m$. For good introduction of lattices and their applications refer [1][2].

B. Lattice reduction

Lattice reduction is a problem to find the reduced basis of the given lattice. Reduced basis is the basis of the lattice such that the vectors are near orthogonal. So many versions exist to find reduced basis, but the one given by Lenstra, Lovasz, Lovasz is a special one, called LLL reduced. Because there exist a polynomial time algorithm for this reduction called LLL algorithm. This problem not only solves the reduced problem, it also solves SVP problem in some extent.

C. LLL Algorithm

Let $\mathcal{L}$ be a lattice spanned by linearly independent vectors $b_1, b_2, \cdots, b_n$, where $b_1, b_2, \cdots, b_n \in \mathbb{R}^n$. By $b_1^*, b_2^*, \cdots, b_n^*$, we denote the vectors obtained by applying the Gram-Schimdt process to the vectors $b_1, b_2, \cdots, b_n$. It is known that given basis $b_1, b_2, \cdots, b_n$ of lattice $\mathcal{L}$, LLL algorithm can find a new basis $b_1, b_2, \cdots, b_n$ of $\mathcal{L}$ with the following properties:

1) $\|b_i^*\|^2 \leq 2\|b_{i+1}^*\|^2$

2.For all i, if $b_i = b_i^* + \sum_{j=1}^{i-1} \mu_{i,j} b_j^*$, then $|\mu_{i,j}| \leq \frac{1}{2}$ for all j.

3.$\|b_1\| \leq 2^{\frac{n}{2}} \det(L)^{\frac{1}{n}}$, $\|b_2\| \leq 2^{\frac{n}{2}} \det(L)^{\frac{1}{n-1}}$.

The determinant of $\mathcal{L}$ is defined as $\det(\mathcal{L}) = \prod_{i=1}^{w} \|b_i^*\|$, where $\|.\|$ denotes the Euclidean norm on vectors.[1][2]

D. Unravelled linearization

Unravelled linearization is a clever technique of linearization introduced by Hermann and May[14], and it proceeds in three steps: linearization, basis construction, unravellization . In the cryptanalysis of RSA literature, the existing work proceeded in two steps, basis construction, identifying special structure (called sub lattice) in a basis to compute determinant easily.

E. Multiprime RSA

The public and private exponents are defined as inverses modulo $\varphi(N)$, so that $ed \equiv 1 mod \varphi(N)$. So, the key equation is $ed = 1 + k\varphi(N)$, where k is a some positive integer. We can replace $\varphi(N)$ with $N - s$. So s can be written as $s = N - \varphi(N)$. Since, we have assumed the primes are balanced, we have the upper bound for $|s| < (2r-1)N^{1-\frac{1}{r}}$. Ciet et.al[12] provided the bound for the secret exponent as $\delta < \frac{r-\sqrt{r(r-1)}}{r}$. They have used the technique called "Geometrical progressive matrices" introduced by Boneh-Durfee. In this paper, we use another technique called "Unravelled linearization" which is introduced by Hermann and May. The advantage of this method is simplified analysis.

F . *Exitsing small private exponent attacks on Multi Prime RSA:*

Several attacks have been existed in the literature of RSA, which can be extended easily to Multiprime RSA. We listed the results below.

Wiener's attack[12]: Let N be an r-prime RSA modulus with balanced primes, let e be a valid public exponent, and d be its corresponding private exponent. Given the public key, if the private exponent satisfies $d < \frac{N^{\frac{1}{r}}}{2k(2r-1)}$, then the modulus can be (probabilistically) factored in time polynomial in $\log(N)$.

Boneh-Durfee's attack[12]: Let N be an n-bit r-prime RSA modulus with balanced primes, let $e = N^{\alpha}$ be a valid public exponent and let $d = N^{\delta}$ be its corresponding private exponent. Given the public key(N, e), if the private exponent satisfies $\delta \leq \frac{1}{3r}(4r - 1 - 2\sqrt{(r-1)(r-1+3\alpha r)})$, then the modulus can be factored in time polynomial in n.

Blomer-May's attack[12]: Let Nbe an n-bit r-prime RSA modulus with balanced primes, and let $e = N^{\alpha}$ be a valid public exponent and let $d = N^{\delta}$ be its corresponding private exponent. Given the public key

Manuscript received on May, 2013.

Santosh kumar ravva, Depart,ent of IT, MVGR college of engineering, Vizianagaram, INDIA.

Narasimham Ch, Department of CSE, Amrita institute of Science and Technilogy,Vijayaeada, India.

Pallam setty, Department of CS&SE , Andhra Univesity, Vishakapatnam, India.

(N, e), if the private exponent satisfies $\delta \le \frac{1}{5r}(6 - r - 3\alpha r + 2\sqrt{\alpha^2 r^2 - \alpha r(r-1) + 4(r-1)^2}$, then the modulus can be probabilistically factored in time polynomial in n.

Ciet's attack[12]: Let N be an n-bit r-prime RSA modulus with balanced primes, let $e = N^{\alpha}$ be a valid public exponent and $d = N^{\delta}$ be its corresponding private key. Given the public key (N, e), the private exponent satisfies $\delta < \frac{r - \sqrt{\alpha r(r-1)}}{r}$, then the modulus can be factored in time polynomial in n.

Ciet's attack is the best among all the attacks listed above. But for this attack they have used complicated concept called geometrical progressive matrices. This concept is difficult to understand. Here, we use another technique called unravelled linearization, to achieve the same bound as Ciet.

III. ATTACK ON MULTIPRIME RSA

A Attack

Let N be an n-bit r-prime RSA modulus with balanced primes, let e be a valid public exponent with a same size as modulus and $d = N^{\delta}$ be its corresponding private key. Given the public key (N, e), the private exponent satisfies $\delta < \frac{r - \sqrt{r(r-1)}}{r}$, then the modulus can be factored in n.

B Justification

We follow the analysis of ciet. The key equation is same as the original RSA. The underlying polynomial $f(x, y) = 1 + x(A + y) \bmod e$ used by Boneh-Durfee. Here, we introduced the variable u_1 for the monomial $1 + xy$, u_2 for x and u_3 for y. Then the new polynomial is $F(u_1, u_2) = u_1 + Au_2 (\bmod e)$ with the relation $u_2 u_3 = u_1 - 1$. Now, construct the polynomials for the basis, as introduced by Jochemsz and May[18] with leading monomial $\lambda = u_1$. $G_{i,k} = u_2^i F^k e^{m-k}$ for $k = 0, 1, 2, \cdots, m$ and $i = 0, 1, 2, \cdots, m - k$. For extra shifts, use the variable u_3 and introduced as in the Boneh-Durfee paper. $H_{j,k} = u_3^j F^k e^{m-k}$ for $j = 1, 2, \cdots, t$ and $k = \left\lfloor \frac{m}{t} \right\rfloor j, \cdots, m$. It is also noted that $t \le m$. For $m = 2$ and $t = 2$ refer the matrix in fig(1).

	1	U_2	U_1	U_2^2	U_1U_2	U_1^2	U_1U_3	$U_1^2U_3$	$U_1^2U_3^2$
e^2	e^2								
U_2e^2		$e^2u_2U_2$							
fe		eAu_2U_2	eu_1U_1						
$U_2^2e^2$				$e^2u_2^2U_2^2$					
U_2fe				$eAu_2^2U_2^2$	$eu_1U_1u_2U_2$				
f^2				$A^2u_2^2U_2^2$	$2Au_1U_1u_2U_2$	$u_1^2U_1^2$			
U_3fe	$-eA$		eAu_1U_1				$u_1U_1u_3U_3$		
U_3f^2		$-A^2u_2U_2$	$-2Au_1U_1$		$A^2u_1U_1u_2U_2$	$2Au_1^2U_1^2$		$u_1^2U_1^2u_3U_3$	
$U_3^2f^2$	A^2		$-2A^2u_1U_1$			$A^2u_1^2U_1^2$	$-2Au_1U_1u_3U_3$	$2Au_1^2U_1^2u_3U_3$	$u_1^2U_1^2u_3^2U_3^2$

Fig 1: Lattice matrix for the parameters m=2, t=2.

Now one can show that the above construction yields that, every new row introduced only one new monomial. For the sake of completeness we present the details here[13]. For this, observe the factor $u_3^i F^l$ by the binomial theorem $u_1^l u_3^i + \binom{l}{1} A u_1^{l-1} u_2 u_3^i + \cdots + \binom{l}{l} A^l u_2^l u_3^i$. The first term introduces a new monomial $u_1^l u_3^i$. If we substitute the value of $u_2 u_3$ in the second term, we have $u_1^{l-1} u_2 u_3^i = u_1^l u_3^{i-1} - u_1^{l-1} u_3^{i-1}$. Observe that these monomials appear in $u_3^{i-1} F^l$ and $u_3^{i-1} F^{l-1}$, respectively. In general, the $(j+1)^{th}$ term of the binomial expansion contains monomials that appear in $u_3^{i-j} F^{l-k}$ for $k = 0, 1, \cdots, j$. Thus, the shift $u_3^i F^l$ introduces exactly one new monomial $u_1^l u_3^i$ if all shifts $u_3^{i-j} F^{l-k}$ for $j = 1, 2, \cdots, i-1$ and $k = 0, 1, \cdots, j$ were used in the construction of lattice basis. It remains to show that the chosen u_3- shifts $H_{j,k}$ satisfies the requirement, i.e we show that if $u_3^i F^l$ is a u_3 -shift, then all of $u_3^{i-j} F^{l-k}$ for $j = 1, 2, \cdots, i-1$ and $k = 0, 1, 2, \cdots, j$ are also used as shifts. Refer the fig1 for the example. Notice that it is sufficient to show $u_3^{i-j} F^{l-j}$ is used as a shift. Since $u_3^i F^l$ is in the set of u_3 shifts, we know that $l \in \left\{ \left\lfloor \frac{m}{t} \right\rfloor i, \cdots, m \right\}$ and therefore $l - j \in \left\{ \left\lfloor \frac{m}{t} \right\rfloor i - j, \cdots, m - j \right\}$. For $u_3^{i-j} F^{l-j}$, we have $l - j \in \left\{ \left\lfloor \frac{m}{t} \right\rfloor (i - j), \cdots, m \right\}$. Our requirement is thus fulfilled if the condition $\left\lfloor \frac{m}{t} \right\rfloor (i - j) \le \left\lfloor \frac{m}{t} \right\rfloor i - j$ holds. From this, we have $m \ge t$. Since the basis matrix is by construction triangular, we can easily compute the determinant as the product of the diagonal entries. Note that each shift polynomial $G_{i,k}$ introduces a diagonal term $u_1^k u_2^i e^{m-k}$ and each extra shift $H_{i,k}$ contributes a diagonal term $u_1^k u_3^i e^{m-k}$. Let $\tau = tm$ and the bounds of u_1, u_2, u_3 are U_1, U_2, U_3 respectively. we compute the determinant of the lattice as $U_1^{S_1} U_2^{S_2} U_3^{S_3} e^{S_e}$ for values

$$s_1 = \sum_{k=0}^{m} \sum_{i=0}^{m-k} k + \sum_{i=1}^{\tau m} \sum_{k=\frac{1}{\tau} i}^{m} k = \left(\frac{1}{6} + \frac{\tau}{3}\right) m^3 + o(m^3)$$

$$s_2 = \sum_{k=0}^{m} \sum_{i=0}^{m-k} i = \frac{1}{6} m^3 + o(m^3)$$

$$s_3 = \sum_{i=1}^{\tau m} \sum_{k=\frac{1}{\tau} i}^{m} i = \frac{\tau^2}{6} m^3 + o(m^3)$$

$$s_e = \sum_{k=0}^{m} \sum_{i=0}^{m-k} (m - k) + \sum_{i=1}^{\tau m} \sum_{k=\frac{1}{\tau} i}^{m} (m - k) = \left(\frac{1}{3} + \frac{\tau}{6}\right) m^3 + o(m^3).$$

Also we have $\dim(\mathcal{L}) = \sum_{k=0}^{m} \sum_{i=0}^{m-k} 1 + \sum_{i=1}^{\tau m} \sum_{k=\frac{1}{\tau} i}^{m} 1 = \left(\frac{1}{2} + \frac{\tau}{2}\right) m^2 + o(m^2)$. Note that determinant of the lattice is bounded by $e^{\dim(\mathcal{L}).m}$. Substitute all these values, we get the inequality

$$U_1^{\left(\frac{1}{6} + \frac{\tau}{3}\right) m^3 + o(m^3)} U_2^{\frac{1}{6} m^3 + o(m^3)} U_3^{\frac{\tau^2}{6} m^3 + o(m^3)} e^{\left(\frac{1}{3} + \frac{\tau}{6}\right) m^3} \le e^{\left(\frac{1}{2} + \frac{\tau}{2}\right) m^3 + o(m^3)}$$

Also observe that the upper bounds of U_1, U_2, U_3 respectively $e^{\delta + 1 - \frac{1}{r}}, e^{\delta}, e^{1 - \frac{1}{r}}$. Substitute above upper bounds into above inequality, we have $\frac{\tau^2}{6}\left\{1 - \frac{1}{r}\right\} + \tau\left\{\frac{\delta}{3} - \frac{1}{3r}\right\} + \left\{\frac{\delta}{3} - \frac{1}{6r}\right\} \le 0$. Above inequality is minimized when $\tau = \frac{1 - r\delta}{r - 1}$. Substitute τ value into above inequality, we have $\left(\frac{1 - r\delta}{r - 1}\right)^2 \left\{\frac{r - 1}{r}\right\} + \frac{1 - r\delta}{3(r-1)} \left\{\frac{r\delta - 1}{r}\right\} + \left\{\frac{\delta}{3} - \frac{1}{6r}\right\} \le 0$. After simplification, we have $\delta < 1 - \frac{\sqrt{r(r-1)}}{r}$. For $r = 2$, it reduces to Boneh-Durfee's bound.

IV. EXPERIMENTS

We have done the experiments for the values $\alpha = 1$ and $r = 3$. Each prime is 512 bits.

The first prime number is
11653782858684191308687738875839248426691497564407763301840258422857937840961702781154595808289802909292323320910007888619334322530205520118809692679380997

The second prime number is
13182622932956540343624877951220351472265526833181272216094982197833709213750435524604923597808142054681653877151436527754516 6

0074592112796916136004758857 3
The third prime numbers is
1112543441320575632691810722578273779893794748233640502894573577804799965450692232933967564853191617976515333350453026476634239608440390342052433 2784224827.

We construct the matrix as above and we apply LLL algorithm for this matrix. We use NTL library[14] for all these calculations. We apply grobner basis technique for first two rows to get a common solution.

V. CONCLUSION

In this paper, we present the attack on multiprime RSA. So many attacks have been provided for this version, but the one presented in this paper is easy to understand. We did not get the better bound but analysis is simple.

REFERENCES

[1] H. Cohen, A Course in computational Algebraic NumberTheory. Springer-Verlag, second edition, 1995
[2] A.Lenstra, H.Lenstra, L.Lovasz ," Factoring Polynomials with Rational Coeffiecients", Mathematiche Annalen 261, pp.515-534, 1982
[3] Boneh, D., Durfee, G.: Cryptanalysis of RSA with Private Key d Less than N0:292. Advances in Cryptology - Proceedings of Eurocrypt '99, Lecture Notes in Computer Science 1952 (1999) 1-11.
[4] De Weger, B.: Cryptanalysis of RSA with small prime difference, Applicable Algebra in Engineering,Communication and Computing, Vol 13(1), 17-28, 2002
[5] Boneh, D., Durfee, G.: Cryptanalysis of RSA with Private Key d Less than N^292. IEEE Transactions on Information Theory 46:4 (2000),1339-1349
[6] Boneh, D.: Twenty Years of Attacks on the RSA Cryptosystem. Notices of the American Mathematical Society 46:2 (1999) 203-213.
[7] Boneh, D. and Durfee, G. and Howgrave-Graham, N.: Factoring N =prq for Large r. Advances in Cryptology, Proceedings of CRYPTO 1999, Lecture Notes in Computer Science 1666 (1999) 326-337
[8] Coppersmith, D.: Small Solutions to Polynomial Equations, and Low Exponent RSA Vulnerabilities. Journal of Cryptology 10:4 (1997) 233-260.
[9] Durfee, G., Nguyen, P. Q.: Cryptanalysis of RSA Schemes with Short secret Exponent from Asiacrypt '99. Advances in Cryptology – Proceedings of Asiacrypt '00, Lecture Notes in Computer Science 1976 (2000).
[10] M.J.Hinek. Small private exponent partial key-exposure attacks on multiprime RSA. CACR Technical Report CACR 2005-16, Centre for Applied Cryptographic Research, University of Waterloo, 2005
[11] M.J.Hinek, M.K.Low, and E.Teske. On some attacks on multiprime RSA. In K.Nyberg and H.M.Heys, editors, Selected areas in Cryptography, volume 2595 of Lecture Notes in Computer Science, pages 385-404. Springer, 2002.
[12] M.Ciet, F. Koeune, F. Laguillaumie, Jean-Jacues Quisuater. Short private exponent attacks on fast variants of RSA. UCL Technical report CG-2003\2004.
[13] Hermann, M., May, A.,: Maximizing Small Root Bounds by Linearization and Applications to Small Secret Exponent RSA, In Practice and Theory in Public Key Cryptography (PKC 2010), Lecture Notes in Computer Science 6056, Berlin: Springer-Verlag 2010, pp.53-69.
[14] R. Santosh kumar, C. Narasimham, S. Pallam setty, "Lattice based tools for cryptanalysis in various applications", springer-LNICST, 84:530-537, 2012.
[15] R.Santosh kumar, C.Narasimham, S.Pallam setty," Lattice bases attacks on short secret exponent RSA: A Survey", International Journal of Computer Applications (0975 – 8887) Volume 49– No.19, July 2012.
[16] Victor Shoup. NTL: A library for doing number theory. Website: http://www.shoup.net/ntl/.
[17] Wiener, M.: Cryptanalysis of short RSA secret exponents, IEEE Transactions on Information Theory 36, 553-558 (1990).
[18] M.Ernst, E. Jochemsz, A.May, B.de Weger," Partial Key Exposure Attacks on RSA up to Full Size Exponents", Advanced in Cryptology-EUROCRYPT'05, Springer-Verlag pp 1-11, 2000
[19] R.Santosh Kumar, C.Narasimham, S.Pallam Setty," Cryptanalysis of RSA with Small Prime Difference using Unravelled Linearization, International Journal of Computer Applications (0975 – 8887) Volume 61– No.3, January 2013.