Cryptanalysis of RSA with Small Prime Difference using Unravelled Linearization

Santosh Kumar. R
Department Of IT
Mvgr College Of Engg
Vizianagaram
Andhra Pradesh

Narasimham. C
Department Of CSE
AIST
Vijayawada
Andhra Pradesh

Pallam Setty. S
Department Of CS & SE
Andhra University
Vishakapatnam
Andhra Pradesh

ABSTRACT

In 2002, de Weger showed that choosing an RSA modulus with a small difference of primes improves the attack given by Boneh-Durfee. For this attack, de Weger used the complicated geometrical progressive matrices, introduced by Boneh-Durfee. In this paper, we analyzed by using another technique called unravelled linearization.

Keywords:

Lattice reduction, RSA, Cryptanalysis, Unravelled linearization.

1. Introduction

The RSA cryptosystem[1] is the most widely used public key cryptosystem. The modulo N of RSA cryptosystem is the product two large prime numbers p, q. The public exponent e and private exponent d satisfy the equation $ed \equiv 1(mod\ \varphi(N))$, where $\varphi(N) = (p-1)(q-1)$ is Euler's totient function. In a typical RSA cryptosystem p and q are balanced. In some practical applications, to speed up the decryption process, one might be tempted to use small secret exponent. But in 1990, Wiener[2] showed that if the secret exponent $d < N^{0.25}$, then the factorization of N can be found in polynomial time. To achieve this bound, Wiener used the continued fraction technique. Later, Boneh-Durfee[3] improved this attack by using powerful lattice reduction technique and they improved the bound up to 0.292. For this they have used Coppersmith's theorem of univariate modular equation (modified by Howgrave-Graham)[4], which has been solved by using lattice reduction techniques. In addition to this, Boneh-Durfee used the geometrical progressive matrices to improve their bound to 0.292. Later Blomer-May[5] used the different technique, but they achieved the bound up to 0.280. de Weger[6] also applied the same techniques, which were introduced by Boneh-Durfee to the problem of RSA with small prime difference. De Weger did not properly analyzed in his attack. In this paper we use another technique, called unravelled linearization, which is introduced by Hermann and May[7]. The importance of this attack is simplified analysis. Rest of the paper organized as follows. In section 2, we introduce Mathematical preliminaries. In next section, we present the attacks given by Wiener, Boneh-Durfee and others. In section 4, we introduce our attack and details of the proof.

2. Mathematical Prelimanaries

Lattices: Lattice is a discrete subset of $\mathbb{R}^m$. That is, lattice contains all integer linear combinations of the vectors in $\mathbb{R}^m$. The set of vectors is called a basis of lattice. A given lattice may have several basis. Among all these, there exists a basis which contains small norm vectors and nearly orthogonal. Process of converting the given lattice into a basis with these characteristics is called lattice reduction. There are several versions of reduction strategies, but all they lead to exponential time algorithms. The one is given by Lenstra, Lenstra, Lovasz [8] has polynomial time algorithm called (LLL) algorithm. The output of the algorithm is the reduced basis. Also the first vector in the reduced basis is also nearer to the smallest vector in the lattice. Lattice reduction algorithms play important role in cryptology [9], especially for RSA cryptanalysis. For survey on this refer[10].

3. De Weger's attack on RSA small prime difference:

De Weger studied this problem initially[6]. For the sake of completeness, we provide the details here. The RSA cryptosystem is widely used in public key cryptography. The modulus N is a product of two large primesp, q. The exponent e is relatively prime to $(p-1) * (q-1)$. The (N, e) constitutes the public key. The private key should satisfy the equation$ed = 1\ mod\ \varphi(n)$. In this paper we assume the primes are balanced, that is they are equal sized and satisfied the inequality$4 < \frac{1}{2}N^{\frac{1}{2}} < p < N^{\frac{1}{2}} < q < 2N^{\frac{1}{2}}$. From this we get, $|N - \varphi(N)| < 3N^{\frac{1}{2}}$. That's why, Boneh-Durfee used $\varphi(N)$ as the approximation to N, with an error term $p + q$. De Weger used the expression $n + 1 - \left\lceil 2n^{\frac{1}{2}} \right\rceil$ for his attack. de Weger proved the following attack: Let p, q be large primes of same size, and let $n = pq$. Let $\Delta = |p - q|$. Let e, d be integers > 1 and $< \varphi(n)$, satisfying $ed \equiv 1(\ mod\ \varphi(n))$. Put $\Delta = n^{\beta}$ and $d = n^{\delta}$. Given only n, e, the factors p, q of n and the number d can be recovered efficiently whenever $2 - 4\beta < \delta < 1 - \sqrt{2\beta - \frac{1}{2}}$ or $\delta < \frac{1}{6}(4\beta + 5) - \frac{1}{3}\sqrt{(4\beta + 5)(4\beta - 1)}$.

4. Unravelled linearization:

Unravelled linearization is a clever technique of linearization introduced by Hermann and May[7], 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. There are several techniques in the existing work, for example Boneh-Durfee, May.

5. Attack on RSA small prime difference:

De Weger used efficient lattice reduction technique and the special structure of matrix, called geometrical progressive matrices to obtain above bound. But understanding the structure of geometrical progressive matrix is so hard. De Weger also not properly analyzed in his attack. One can use unravelled linearization to obtain above method. The advantage of this method over de Weger's method is easy to understand and analyze. In this section we introduce the attack on RSA with small prime difference by using unravelled linearization.

	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.

The underlying polynomial $f(x,y) = 1 + x(A+y) mod\ e$ 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 $F(u_1,u_2) = u_1 + Au_2 (mod\ e)$ with the relation $u_2u_3 = u_1 - 1$. Now, construct the polynomials for the basis, as introduced by Jochemsz and May with leading monomial $\lambda = u_1$. $G_{i,k} = u_1^i F^k e^{m-k}$ 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 $t \le m$. Otherwise, we get a non triangular matrix and it leads to getting a sublattice structure from a given lattice. Hermann[7] showed that, each polynomial row generates exactly one new polynomial and leads to triangular matrix. 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_2u_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 $l - j \in \{\left\lfloor\frac{m}{t}\right\rfloor (i-j),\cdots,m\}$. 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

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

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

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

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

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

$U_1^{\left(\frac{1}{6}+\frac{\tau}{3}\right)m^3+o(m^3)} U_2^{\frac{1}{6}m^3+o(m^3)} U_3^{\frac{\tau^2}{6}m^3+o(m^3)} e^{(\frac{1}{3}+\frac{\tau}{6})m^3} \le e^{\left(\frac{1}{2}+\frac{\tau}{2}\right)m^3+o(m^3)}$. Also note that the upper bounds of the values

U_1, U_2, U_3 are $N^{\delta+2\beta-\frac{1}{2}}, N^{\delta}, N^{2\beta-\frac{1}{2}}$. Plug into above inequality, we get $\left(\delta+2\beta-\frac{1}{2}\right)\left(\frac{1}{6}+\frac{\tau}{3}\right)m^3+\frac{\delta}{6}m^3+\left(2\beta-\frac{1}{2}\right)\left(\frac{\tau^2}{6}\right)m^3+(\frac{1}{3}+\frac{\tau}{6}-\frac{1}{2}-\frac{\tau}{2})\leq 0.$ The left side is minimal for $\tau=\frac{3-2\delta-4\beta}{4\beta-1}$. If we substitute this value into above inequality we have $\delta=1-\sqrt{2\beta-\frac{1}{2}}$, which is equal to the de Weger's original attack. Also observe that de Weger used the technique of geometrical progressive matrices and the technique is only valid for $\delta \leq 0.5$. Our technique also has the restriction that $\tau \leq 1$, which is satisfied for the values $\delta \leq 0.5$. We implement this attack by using NTL library[11], which is freely available. We assume that public exponent is same size as modulus size.

6. Conclusion:

We showed that RSA with small prime difference is insecure. This problem was studied by de Weger, and used the technique called geometrical progressive matrices technique. Here we provide the same bound, by using another technique, unravelled linearization.

7. References:

[1] R.Rivest, A.Shamir and L. Adleman," A Method for Obtaining Digital Signatures and Public-Key Cryptosystems", Communications of the ACM, vol.21, No.2, pp.120-126,1978.

[2] Wiener, M.: Cryptanalysis of short RSA secret exponents, IEEE Transactions on Information Theory 36, 553-558 (1990).

[3] Boneh, D., Durfee, G.: Cryptanalysis of RSA with Private Key d Less Than $N^{0.292}$, Advances in Cryptology-EUROCRYPT99, Lecture Notes in Computer Science 1592, Berlin: Springer 1999,pp.1-11.

[4] Nick Howgrave-Graham, N.: Finding small roots of univariate modular equations revisited, In Cryptology and Coding, Lecture Notes in Computer Science 1335, Berlin: Springer-Verlag 1997, pp. 131-142.

[5] J.Blomer and A.May. Low secret exponent RSA revisited. In J.H.Silverman, editor,CaLC, volume 2146 of Lecture Notes in COMPUTER Science, pages 4-19. Springer, 2001.

[6] De Weger, B.: Cryptanalysis of RSA with small prime difference, Applicable Algebra in Engineering, Communication and Computing, Vol 13(1), 17-28 (2002).

[7] 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.

[8] A.Lenstra, H.Lenstra, L.Lovasz ," Factoring Polynomials with Rational Coeffiecients", Mathematiche Annalen 261, pp.515-534, 1982.

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

[10] R.Santosh kumar, C.Narasimham, S.Pallam settee," Lattice bases attacks on short secret exponent RSA: A Survey", International Journal of Computer Applications (0975 – 8887) Volume 49– No.19, July 2012.

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