Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 20 July 2018 doi:10.20944/preprints201807.0379.v1

Peer-reviewed version available at Cryptography 2018, 2, 36; doi:10.3390/cryptography2040036

An Attack Bound for Small Multiplicative Inverse of $\varphi(N) \bmod e$ with a Composed Prime Sum $p+q$ Using Sublattice Based Techniques

P. Anuradha Kameswari, L. Jyotsna

Department of Mathematics, Andhra University,
Visakhapatnam - 530003, Andhra Pradesh, India.
panuradhakameswari@yahoo.in, jyotsna.jahnavi@gmail.com

Abstract

In this paper, we gave an attack on RSA when $\varphi(N)$ has small multiplicative inverse modulo e and the prime sum $p+q$ is of the form $p+q = 2^n k_0 + k_1$ where n is a given positive integer and k_0 and k_1 are two suitably small unknown integers using sublattice reduction techniques and Coppersmith's methods for finding small roots of modular polynomial equations. When we compare this method with an approach using lattice based techniques, this procedure slightly improves the bound and reduces the lattice dimension.

Key words :RSA, Cryptanalysis, Lattices, LLL algorithm, Coppersmith's method.

2010 Mathematics Subject Classification: 11T71, 94A60.

1 Introduction

RSA Cryptosystem is the first public key cryptosystem invented by Ronald Rivest, Adi Shamir and Leonard Adalman in 1977 where the encryption and decryption are based on the fact that if $N = pq$, is the modulus for RSA, p, q distinct primes, if $1 \leq e \leq \varphi(N)$ with $(e, \varphi(N)) = 1$ and d, the multiplicative inverse of e modulo $\varphi(N)$, then $m^{ed} = m \bmod N$, for any message m, an integer in Z_N. The security of this system depends on the difficulty of finding factors of a composite positive integer, that is product of two large primes. In 1990, M.J.Wiener [20] was the first one to describe a cryptanalytic attack on the use of short RSA deciphering exponent d. This attack is based on continued fraction algorithm which finds the fraction $\frac{t}{d}$, where $t = \frac{ed-1}{\varphi(n)}$ in a polynomial time when d is less than $N^{0.25}$ for $N = pq$ and $q < p < 2q$. Using lattice reduction approach based on the Coppersmith techniques [7] for finding small solutions of modular bivariate integer polynomial equations, D. Boneh and G. Durfee [4] improved the wiener result from $N^{0.25}$ to $N^{0.292}$ in 2000 and J. Blömer and A. May [5] has given an RSA attack for d less than $N^{0.29}$ in 2001, that requires lattices of dimension smaller than the approach by Boneh and Durfee. In 2006, E. Jochemsz and A. May [10], described a strategy for finding small modular and integer roots of multivariate polynomial using lattice-based Coppersmith techniques and by implementing this strategy they gave a new attack on an RSA variant called common prime RSA.

In our paper [2], first we described an attack on RSA when $\varphi(N)$ has small multiplicative inverse k of modulo e, the public encryption exponent by using lattice and sublattice based techniques. Let $N = pq, q < p < 2q, p - q = N^{\beta}$ and $e = N^{\alpha} > p + q$. As $(e, \varphi(N)) = 1$, there exist unique r, s such that $(p-1)r \equiv 1 (\bmod\ e)$ and $(q-1)s \equiv 1 (\bmod\ e)$. For $k = rs (\bmod\ e)$, $k\varphi(N) \equiv 1 (\bmod\ e)$ and define $g(x, y) = x(y + B) - 1$ where $B = N + 1 - \lceil 2\sqrt{N} \rceil$. Then the pair $(x_0, y_0) = (k, -((p + q) - \lceil 2\sqrt{N} \rceil))$ is a solution for the modular polynomial equation $g(x, y) \equiv 0 (\bmod\ e)$. Now applying the lattice based techniques given by Boneh-Durfee in [4] using x, y shifts and using only x shifts to the above modular polynomial equation, we get the attack bounds for δ, $|k| \leq N^{\delta}$ are $\delta < \frac{3\alpha+\beta-2\sqrt{\beta(3\alpha+\beta)}}{3}$ and $\delta < \frac{\alpha-\beta}{2}$ respectively. Also we improved the bound for δ up to $\alpha - \sqrt{\alpha\beta}$ by implementing the sublattice based techniques given by Boneh and Durfee in [4] under the condition $\delta > \alpha - \beta(1 + \alpha)$ and improved the bound for δ up to $\delta < \frac{2\alpha-6\beta+2\sqrt{\alpha^2-\alpha\beta+4\beta^2}}{5}$ by implementing the sublattice based techniques with lower dimension given by J. Blömer and A. May in [5], this bound is slightly less than the above bound but this method requires lattices of smaller dimension than the above method. All these attack bounds are depending on the prime difference $p - q = N^{\beta}$ and $\alpha - \sqrt{\alpha\beta}$ is the maximum upper bound for δ.

© 2018 by the author(s). Distributed under a Creative Commons CC BY license.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 20 July 2018 doi:10.20944/preprints201807.0379.v1

Peer-reviewed version available at Cryptography 2018, 2, 36; doi:10.3390/cryptography2040036

Later we described that, for $\beta \approx 0.5$, the maximum bound for δ may be improved if the prime sum $p+q$ is in the form of the composed sum $p+q = 2^n k_0 + k_1$ where n is a given positive integer and k_0 and k_1 are two suitably small unknown integers. Define the polynomial congruence $f(x,y,z) \equiv 0 (\mathrm{mod} e)$ for $f(x,y,z) = \begin{cases} (N+1)x + xy + (2^n)xz - 1 \text{ if } |k_0| \leq |k_1| \\ 2^{n'}x(N+1) + xy + 2^{n'}xz - 2^{n'} \text{ if } |k_1| \leq |k_0| \end{cases}$ where $2^{n'}$ is an inverse of $2^n \bmod e$. By using lattice based techniques to the above polynomial congruence, the attack bound for δ is such that $\delta < \frac{1}{2}\alpha - \frac{1}{2}\gamma_1 + \frac{1}{16}\gamma_2 - \frac{1}{16}\sqrt{48(\alpha-\gamma_1)\gamma_2 + 33\gamma_2^2}$ where N^{γ_1}, N^{γ_2} are the upper bounds for $\max\{|k_0|, |k_1|\}$, $\min\{|k_0|, |k_1|\}$ respectively.

Now in this paper we slightly improved the above bound by using the sub-lattice based techniques given by J. Blömer, A. May in [5] to the above polynomial congruence and this method requires lattice of smaller dimension than the above method.

2 Preliminaries

In this section we state basic results on lattices, described briefly lattice basis reduction, Coppersmith's method and Howgrave-Graham theorem that are based on lattice reduction techniques are described.

Definition 1. Let $b_1, b_2, ..., b_n \in \mathbb{R}^m$ be a set of linearly independent vectors. The **lattice** L **generated** by $b_1, b_2, ..., b_n$ is the set of linear combinations of $b_1, b_2, ..., b_n$ with coefficients in $\mathbb{Z}$.

A **basis** for L is any set of independent vectors that generates L. The **dimension** of L is the number of vectors in a basis for L.

Remark 1. If L is a full rank lattice, means $n = m$ then the determinant of L is equal to the determinant of the $n \times n$ matrix whose rows are the basis vectors $b_1, b_2, ..., b_n$.

In 1982, A. K. Lenstra, H. W. Lenstra, Jr. and L. Lovasz [11] invented the LLL lattice based reduction algorithm to reduce a basis and to solve the shortest vector problem in polynomial time. The general result on the size of individual LLL-reduced basis vectors is given in the following Theorem.

Theorem 1. Let L be a lattice and $b_1, b_2, ..., b_n$ be an LLL-reduction basis of L. Then

$$\| b_1 \| \leq \| b_2 \| \leq ... \| b_i \| \leq 2^{\frac{n(n-1)}{4(n+1-i)}} \det(L)^{\frac{1}{n+1-i}}$$

for all $1 \leq i \leq n$ [12].

An important application of lattice reduction found by Coppersmith in 1996 [7] is finding small roots of low-degree polynomial equations. This includes modular univariate polynomial equations and bivariate integer equations. In 1997 Howgrave-Graham [8] reformulated Coppersmith's techniques and proposed a result which shows that if the coefficients of $h(x,y)$ are sufficiently small, then the equality $h(x_0, y_0) = 0$ holds not only modulo N, but also over integers. The generalization of Howgrave-Graham result in terms of the Euclidean norm of a polynomial $h(x_1, x_2, ..., x_n) = \sum a_{i_1 ... i_n} x_1^{i_1} ... x_n^{i_n}$ is defined by the Euclidean norm of its coefficient vector i.e., $||h(x_1, x_2, ..., x_n)|| = \sqrt{\sum a_{i_1 ... i_n}^2}$ given as follows:

Theorem 2. (Howgrave-Graham): Let $h(x_1, x_2, ..., x_n) \in \mathbb{Z}[x_1, x_2, ..., x_n]$ be an integer polynomial that consists of at most ω monomials. Suppose that

1. $h\left(x_1^{(0)}, x_2^{(0)}, ..., x_n^{(0)}\right) \equiv 0 \bmod e^m$ for some m where $|x_1^{(0)}| < X_1, |x_2^{(0)}| < X_2 \ldots |x_n^{(0)}| < X_n$, and
2. $||h(x_1 X_1, x_2 X_2, ..., x_n X_n)|| < \frac{e^m}{\sqrt{\omega}}$.

Then $h(x_1, x_2, ..., x_n) = 0$ holds over the integers.

Resultant of two polynomials:
The resultant of two polynomials $f(x_1, x_2, \ldots, x_n)$ and $g(x_1, x_2, \ldots, x_n)$ with respect to the variable x_i for some $1 \leq i \leq n$, is defined as the determinant of Sylvester matrix of $f(x_1, x_2, \ldots, x_n)$ and $g(x_1, x_2, \ldots, x_n)$ when considered as polynomials in the single indeterminate x_i, for some $1 \leq i \leq n$.

Remark 2. The resultant of two polynomials is non-zero if and only if the polynomials are algebraically independent .

Remark 3. If $\left(x_1^{(0)}, x_2^{(0)}, \ldots, x_n^{(0)}\right)$ is a common solution of algebraically independent polynomials $f_1, f_2, \ldots, f_m$ for $m \geq n$, then these polynomials yield $g_1, g_2, \ldots, g_{n-1}$ resultants in $n-1$ variables and continuing so on the resultants yield a polynomial $t(x_i)$ in one variable with $x_i = x_i^{(0)}$ for some i is a solution of $t(x_i)$. Note the polynomials considered to compute resultants are always assumed to be algebraically independent.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 20 July 2018 doi:10.20944/preprints201807.0379.v1

Peer-reviewed version available at Cryptography 2018, 2, 36; doi:10.3390/cryptography2040036

3 An Attack Bound Using Sublattice Reduction Techniques

In this section, an attack bound for a small multiplicative inverse k of $\varphi(N)$ modulo e when the prime sum $p+q$ is of the form $p+q=2^nk_0+k_1$, where n is a given positive integer and k_0 and k_1 are two suitably small unknown integers using sublattice reduction techniques is described.

In our paper [2], we proposed an attack on RSA when $\varphi(N)$ has small multiplicative inverse modulo e and the prime sum $p+q$ is of the form $p+q=2^nk_0+k_1$, where n is a given positive integer and k_0 and k_1 are two suitably small unknown integers using lattice reduction techniques.

For $2^{n'}$ is an inverse of 2^n mod e, define $f(x,y,z)=\begin{cases}(N+1)x+xy+(2^n)xz-1 \text{ if } |k_0|\leq|k_1|\\ 2^{n'}x(N+1)+xy+2^{n'}xz-2^{n'} \text{ if } |k_1|\leq|k_0|.\end{cases}$

If $|k_0|\leq|k_1|$, then $(k,-k_1,-k_0)$ is a solution and if $|k_1|\leq|k_0|$ then $(k,-k_0,-k_1)$ is a solution for the modular polynomial equation $f(x,y,z)\equiv 0(\text{mod } e)$.

Now define the set $M_k=\bigcup\limits_{0\leq j\leq t}\{x^{i_1}y^{i_2}z^{i_3+t}|x^{i_1}y^{i_2}z^{i_3}\text{is a monomial of } f^m \text{ and } \frac{x^{i_1}y^{i_2}z^{i_3}}{l^k}\text{is a monomial of } f^{m-k}\}$, where l is a leading monomial of f and define the shift polynomials as

$$g_{k,i_1,i_2,i_3}(x,y,z)=\frac{x^{i_1}y^{i_2}z^{i_3}}{l^k}(f'(x,y,z))^ke^{m-k},\ \text{for } k=0,...,m,\ x^{i_1}y^{i_2}z^{i_3}\in M_k\setminus M_{k+1}$$

and $f'=a_l^{-1}f \bmod e$ for the coefficient a_l of l. For $0\leq k\leq m$, divide the above shift polynomials according to $t=0$ and $t\geq 1$. Then for $t=0$, the shift polynomials $g(x,y,z)$ are

$$g(x,y,z)=\begin{cases}z^{i_3}(f(x,y,z))^ke^{m-k},\ \text{for } i_1=i_2=k,\ i_3=0\\ x^{i_1-k}z^{i_3}(f(x,y,z))^ke^{m-k},\ \text{for } k\leq m-1, i_1=k+1,...,m,\ i_2=k,\ i_3=0,...,(i_1-i_2).\end{cases}$$

and for $t\geq 1$, the shift polynomials $h(x,y,z)$ are

$$h(x,y,z)=\begin{cases}z^{i_3}(f(x,y,z))^ke^{m-k},\ \text{for } i_1=i_2=k,\ i_3=1,...,t\\ x^{i_1-k}z^{i_3}(f(x,y,z))^ke^{m-k},\ \text{for } k\leq m-1, i_1=k+1,...,m,\ i_2=k,\ i_3=(i_1-i_2)+1,...,(i_1-i_2)+t.\end{cases}$$

Let L be the lattice spanned by the coefficient vectors $g(xX,yY,zZ)$ and $h(xX,yY,zZ)$ shifts with dimension $(\frac{1}{6}m^3+m^2+\frac{11}{6}m+1)+\left(\frac{1}{2}(m^2+m)t+(m+1)t\right)$ [2]. Let M be the matrix of L with each row is the coefficients of the shift polynomial

$$g\text{-shifts}\begin{cases}e^m, xe^m, xze^m, x^2e^m, x^2ze^m, x^2z^2e^m, ..., x^me^m, x^mze^m, ..., x^mz^me^m,\\ fe^{m-1}, xfe^{m-1}, xzfe^{m-1}, ..., x^{m-1}fe^{m-1}, x^{m-1}zfe^{m-1}, ..., x^{m-1}z^{m-1}fe^{m-1},\\ \vdots\\ f^{m-1}e, xf^{m-1}e, xzf^{m-1}e,\\ f^m,\end{cases}$$

$$h\text{-shifts}\begin{cases}ze^m, ...z^te^m, xz^2e^m, ..., xz^{1+t}e^m, ..., x^mz^{m+1}e^m, ..., x^mz^{m+t}e^m,\\ zfe^{m-1}, ...z^tfe^{m-1}, xz^2fe^{m-1}, ..., xz^{1+t}fe^{m-1}, ..., x^{m-1}z^mfe^{m-1}, ..., x^{m-1}z^{(m-1)+t}fe^{m-1},\\ \vdots\\ zf^{m-1}e, ..., z^tf^{m-1}e, xz^2f^{m-1}e, ..., xz^{1+t}f^{m-1}e,\\ zf^m, ..., z^tf^m\end{cases}$$

and each column is the coefficients of each variable (in shift polynomials)

$$(\text{first } (\tfrac{1}{6}m^3+m^2+\tfrac{11}{6}m+1) \text{ columns})\begin{cases}1, x, xz, x^2, x^2z, x^2z^2, ..., x^m, x^mz, ..., x^mz^m,\\ xy, x^2y, x^2yz, x^3y, x^3yz, x^3yz^2, ..., x^my, x^myz, ..., x^myz^{m-1},\\ \vdots\\ x^{m-1}y^{m-1}, x^my^{m-1}, x^my^{m-1}z,\\ x^my^m,\end{cases}$$

$$(\text{remaining } \left(\tfrac{1}{2}(m^2+m)t+(m+1)t\right) \text{ columns})\begin{cases}z, ..., z^t, xz^2, ..., xz^{1+t}, ..., x^mz^{m+1}, ..., x^mz^{m+t},\\ xyz, ..., xyz^t, x^2yz^2, ..., x^2yz^{1+t}, ..., x^myz^m, ..., x^myz^{(m-1)+t},\\ \vdots\\ x^{m-1}y^{m-1}z, ..., x^{m-1}y^{m-1}z^t, x^my^{m-1}z^2, ..., x^my^{m-1}z^{1+t},\\ x^my^mz, ..., x^my^mz^t.\end{cases}$$

As xy is the leading monomial in $f(x,y,z)$ with coefficient 1, the diagonal elements in the matrix M are

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 20 July 2018 doi:10.20944/preprints201807.0379.v1

Peer-reviewed version available at Cryptography 2018, 2, 36; doi:10.3390/cryptography2040036

$$g\text{-shifts}\begin{cases} e^m, Xe^m, XZe^m, X^2e^m, X^2Ze^m, X^2Z^2e^m, ..., X^me^m, X^mZe^m, ..., X^mZ^me^m, \\ XYe^{m-1}, X^2Ye^{m-1}, X^2YZe^{m-1}, ..., X^mYe^{m-1}, X^mYZe^{m-1}, ..., X^mYZ^{m-1}e^{m-1}, \\ \vdots \\ X^{m-1}Y^{m-1}e, X^mY^{m-1}e, X^mY^{m-1}Ze, \\ X^mY^m, \end{cases}$$

$$h\text{-shifts}\begin{cases} Ze^m, ..., Z^te^m, XZ^2e^m, ..., XZ^{1+t}e^m, ..., X^mZ^{m+1}e^m, ..., X^mZ^{m+t}e^m, \\ XYZe^{m-1}, ..., XYZ^te^{m-1}, X^2YZ^2e^{m-1}, ..., X^2YZ^{1+t}e^{m-1}, ..., X^mYZ^me^{m-1}, ..., X^mYZ^{(m-1)+t}e^{m-1}, \\ \vdots \\ X^{m-1}Y^{m-1}Ze, ..., X^{m-1}Y^{m-1}Z^te, X^mY^{m-1}Z^2e, ..., X^mY^{m-1}Z^{1+t}e, \\ X^mY^mZ, ..., X^mY^mZ^t. \end{cases}$$

Note that the matrix M is lower triangular matrix. Therefore, the determinant is

$$\begin{aligned} det(L) &= e^{n(e)}X^{n(X)}Y^{n(Y)}Z^{n(Z)} \\ &= (((1/8)m^4 + (3/4)m^3 + (11/8)m^2 + (3/4)m) + ((1/6)(2m^3 + 3m^2 + m)t + (1/2)(m^2 + m)t))+ \\ &\quad (((1/8)m^4 + (3/4)m^3 + (11/8)m^2 + (3/4)m) + ((1/6)(2m^3 + 3m^2 + m)t + (1/2)(m^2 + m)t))+ \\ &\quad (((1/24)m^4 + (1/4)m^3 + (11/24)m^2 + (1/4)m) + ((1/6)(m^3 - m)t + (1/2)(m^2 + m)t))+ \\ &\quad (((1/24)m^4 + (1/4)m^3 + (11/24)m^2 + (1/4)m)+ \\ &\quad\quad ((1/4)(m^2 + m)t^2 + (1/2)(m + 1)t^2 + (1/12)(2m^3 + 9m^2 + 7m)t + (1/2)(m + 1)t)) \end{aligned}$$

where $n(e)$, $n(X)$, $n(Y)$ and $n(Z)$ are denotes the number of e's, X's, Y's and Z's in all diagonal elements respectively.
Let N^δ, N^{γ_1} and N^{γ_2} be the upper bounds for X, $\max\{k_0, k_1\}$ and $\min\{k_0, k_1\}$ respectively, then the bound for δ in which the generalized Howgrave-Graham result holds given in the following theorem.

Theorem 3. [2] Let $N = pq$ be an RSA modulus with $q < p < 2q$. Let $e = N^\alpha, X = N^\delta, Y = N^{\gamma_1}$, $Z = N^{\gamma_2}$ and k be the multiplicative inverse of $\varphi(N)$ modulo e. Suppose the prime sum $p + q$ is of the form $p + q = 2^n k_0 + k_1$, for a known positive integer n and for $|k| \leq X, \max\{|k_0|, |k_1|\} \leq Y$ and $\min\{|k_0|, |k_1|\} \leq Z$ one can factor N in polynomial time if

$$\delta < \frac{1}{2}\alpha - \frac{1}{2}\gamma_1 + \frac{1}{16}\gamma_2 - \frac{1}{16}\sqrt{48(\alpha - \gamma_1)\gamma_2 + 33\gamma_2^2}. \tag{1}$$

To improve this bound in a lower dimension than the above dimension, first we construct a sublattice S_L of L and after that we apply the sublattice based techniques to the lattice S_L given by J. Blömer, A. May in [5], and are described in the following sections.

3.1 Construction of a sublattice S_L of L

The construction of a sublattice S_L of L in order to improve the bound for δ is given in the following.

- First remove some rows in M corresponding to g-shifts, are such that
  $e^m, xe^m, xze^m, ..., x^{m-1}e^m, ..., x^{m-1}z^{m-1}e^m,$
  $fe^{m-1}, xfe^{m-1}, xzfe^{m-1}, ..., x^{m-2}fe^{m-1}, ..., x^{m-2}z^{m-2}fe^{m-1},$
  $\vdots$
  $f^{m-2}e^2, xf^{m-2}e^2, xzf^{m-2}e^2,$
  $f^{m-1}e.$

  Therefore the remaining rows in M corresponding to g-shifts are
  $x^me^m, x^mze^m, ..., x^mz^me^m,$
  $x^{m-1}fe^{m-1}, ..., x^{m-1}z^{m-1}fe^{m-1},$
  $\vdots$
  $xf^{m-1}e, xzf^{m-1}e,$
  $f^m,$
  and its corresponding g-shifts can be written as

$$g_s(x, y, z) = x^{l_1}z^{l_2}(f(x, y, z))^k e^{m-k} \text{ for } k = 0, ..., m, l_1 = m - k, l_2 = 0, ..., l_1.$$

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 20 July 2018 doi:10.20944/preprints201807.0379.v1

Peer-reviewed version available at Cryptography 2018, 2, 36; doi:10.3390/cryptography2040036

- Now remove some rows in M corresponding to h-shifts are
  $ze^m, ..., z^t e^m, ..., x^{m-1}z^m e^m, ..., x^{m-1}z^{(m-1)+t}e^m,$
  $zfe^{m-1}, ..., z^t fe^{m-1}, ..., x^{m-2}z^{m-1}fe^{m-1}, ..., x^{m-2}z^{(m-2)+t}fe^{m-1},$
  $\vdots$
  $zf^{m-2}e^2, ..., z^t f^{m-2}e^2, xz^2f^{m-2}e^2, ..., xz^{1+t}f^{m-2}e^2,$
  $zf^{m-1}e, ..., z^t f^{m-1}e.$
  Therefore the remaining rows in M corresponding to h-shifts are
  $x^m z^{m+1}e^m, ..., x^m z^{m+t}e^m,$
  $x^{m-1}z^m fe^{m-1}, ..., x^{m-1}z^{(m-1)+t}fe^{m-1},$
  $\vdots$
  $xz^2f^{m-1}e, ..., xz^{t+1}f^{m-1}e,$
  $zf^m, ..., z^t f^m$, and its corresponding h-shifts can be written as

$$h_s(x,y,z) = x^{l_1}z^{l_2}(f(x,y,z))^k e^{m-k} \text{ for } k = 0, ..., m, l_1 = m-k, l_2 = l_1+1, ..., l_1+t.$$

Now let S_L be the sub-lattice of L spanned by the coefficients of the vectors $g_s(xX, yY, zZ)$ and $h_s(xX, yY, zZ)$ shifts and M_s be the matrix of the lattice S_L.
Note that the matrix M_s is not square. So apply the sublattice based techniques to the basis of S_L or the rows of M_s to get a square matrix. Using that square matrix, the attack bound can be found and is given in the following section.

3.2 Applying sub-lattice based techniques to get an attack bound

In [5], J. Blomer, A. May proposed a method to find an attack bound for low deciphering exponent in a smaller dimension than the approach by Boneh and Durfee's attack in [4]. Apply their method based on sublattice reduction techniques to our lattice S_L to get an attack bound and is described in the following.

In order to apply the Howgrave-Graham's theorem by using Theorem 1, we need three short vectors in S_L as our polynomial consists three variables. But note that M_s is not a square matrix. So, first construct a square matrix M_{sl} by removing some columns in M_s, which are small linear combination of non-removing columns in M_s. Then the short vector in M_{sl} lead to short reconstruction vector in S_L.

Construction of a square sub-matrix M_{sl} of M_s.

Columns in M and M_s are same and each column in M is nothing but the coefficients of a variable, which is a leading monomial of the polynomial g or h-shifts. The first $(\frac{1}{6}m^3 + m^2 + \frac{11}{6}m + 1)$ and remaining $\left(\frac{1}{2}(m^2+m)t + (m+1)t\right)$ columns are corresponding to the leading monomial of the polynomials g and h-shifts respectively. Therefore,

1. the first $(\frac{1}{6}m^3+m^2+\frac{11}{6}m+1)$ columns are the coefficients of the each variable $x^{i_1}y^{i_2}z^{i_3}$ for $i_1 = i_2 = k, i_3 = 0$ and $i_1 = k+1, ..., m, i_2 = k, i_3 = 0, ..., (i_1 - i_2)$ and remaining $\left(\frac{1}{2}(m^2+m)t + (m+1)t\right)$ columns are the coefficients of the each variable $x^{i_1}y^{i_2}z^{i_3}$ for $i_1 = i_2 = k, i_3 = 1, ..., t$ and $i_1 = k+1, ..., m, i_2 = k, i_3 = (i_1-i_2)+1, ..., (i_1-i_2)+t$. So the variable $x^{i_1}y^{i_2}z^{i_3}$ corresponds a column in first $(\frac{1}{6}m^3+m^2+\frac{11}{6}m+1)$ columns if $i_1 \geq i_2 + i_3$ and corresponds a column in remaining $\left(\frac{1}{2}(m^2+m)t + (m+1)t\right)$ columns if $i_1 < i_2 + i_3$.

2. As $1, x, xy, xz$ are the monomials of f, the set of all monomials of f^m for $m \geq 0$ is $\{x^{i_1}y^{i_2}z^{i_3}; i_1 = 0, ..., m, i_2 = 0, ..., i_1, i_3 = 0, ..., i_1 - i_2\}$. Therefore, the coefficient of the variable $x^{i_1}y^{i_2}z^{i_3}$ in f^m is non-zero if and only if $i_3 \leq i_1 - i_2$, i.e., $i_1 \geq i_2 + i_3$.

Remove columns in M_s corresponding to the coefficients of the variable $x^a y^b z^c$ for all $0 \leq a \leq m-1$ and note that every such column is $\left(\frac{m-(a-b)}{(m-a)!b!}\right) \cdot \frac{1}{X^{m-a}Y^{m-a}}$ multiple of a non-removed column, corresponding to the coefficients of $x^m y^{m-(a-b)} z^c$ and is proved in the following theorem.

Theorem 4. Each column in M_s corresponding to the coefficients of the variable $x^a y^b z^c$, a leading monomial of the polynomial g or h-shifts, for all $0 \leq a \leq m-1$ is $\left(\frac{m-(a-b)}{(m-a)!b!}\right) \cdot \frac{1}{X^{m-a}Y^{m-a}}$ multiple of a non-removed column, represents the coefficients of the variable $x^m y^{m-(a-b)} z^c$.

Proof. For $n = 0, ..., m, k_1 = m-n, k_2 = 0, ..., k_1$, the g_s-shifts $x^{k_1}z^{k_2}f^n e^{k_1}$ corresponds first $(\frac{1}{6}m^3 + m^2 + \frac{11}{6}m+1)$ rows in M_s and for $n = 0, ..., m, k_1 = m-n, k_2 = k_1+1, ..., k_1+t$, the h_s-shifts $x^{k_1}z^{k_2}f^n e^{k_1}$ corresponds

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 20 July 2018 doi:10.20944/preprints201807.0379.v1

Peer-reviewed version available at Cryptography 2018, 2, 36; doi:10.3390/cryptography2040036

remaining rows in M_s. We prove this theorem in two cases.

Case(i): Any column in first $(\frac{1}{6}m^3 + m^2 + \frac{11}{6}m + 1)$ columns of M_s. i.e., a column corresponding coefficients of a variable $x^a y^b z^c$ with $a \geq b + c$, from the above analysis in (1).

Given that $0 \leq a \leq m-1$. From the above analysis in (1) and (2), the coefficient of $x^a y^b z^c$ is non-zero in g_s-shifts $x^{k_1} z^{k_2} f^n e^{k_1}$ if and only if $a \geq k_1, b \leq m - k_1, c \geq k_2$ and $a - k_1 \geq b + (c - k_2)$. As $k_1 \geq k_2$, $k_2 \geq 0$ and $a - k_1 \geq b + (c - k_2)$, $\max\{0, k_1 - (a - (b + c))\} \leq k_2 \leq \min\{k_1, c\}$ and also as $a - k_1 < b + (c - k_2)$ for $k_1 > a - b$, k_1 is such that $0 \leq k_1 \leq a - b$.

Therefore, the coefficient of $x^a y^b z^c$ is non-zero in g_s-shifts $x^{k_1} z^{k_2} f^n e^{k_1}$ if and only if $a \geq k_1, b \leq m - k_1, c \geq k_2$ and $k_1 = 0, ..., a - b, k_2 = \max\{0, k_1 - (a - (b + c))\}, ..., \min\{k_1, c\}$.

Similarly we can prove that, the coefficient of $x^a y^b z^c$ is non-zero in h_s-shifts $x^{k_1} z^{k_2} f^n e^{k_1}$ if and only if $a \geq k_1, b \leq m - k_1, c \geq k_2$ and $k_1 = 0, ..., c, k_2 = k_1 + 1, ..., \min\{c, k_1 + t\}$ using the inequalities $k_1 + 1 \leq k_2 \leq k_1 + t$, $a \geq b + c$ and analysis in (1) and (2), and say $\min\{c, k_1 + t\} = l_t$
The formula for finding a coefficient of a variable $x^{l_1} y^{l_2} z^{l_3} = (1)^{n-l_1} x^{l_1 - (l_2 + l_3)} (xz)^{l_3} (xy)^{l_2}$ for $l_1 \leq n - 1$ in f^n is

$$\frac{n!}{(n - l_1)!(l_1 - (l_2 + l_3))! l_2! l_3!)} (-1)^{n-l_1} (N + 1)^{l_1 - (l_2 + l_3)} (2^n)^{l_3}$$

and coefficient of $x^a y^b z^c$ in $x^{k_1} y^{k_2} f^n e^{k_1}$ is nothing but a coefficient of $x^{a-k_1} y^b z^{c-k_2}$ in f^n.

Note that a column corresponding to a variable $x^m y^{m-a} z^c$ is in the non-removing columns in M_s and coefficient of $x^m y^{m-a} z^c$ is zero for $k_1 > a - b$ in g_s-shifts , $k_1 > c$ in h_s-shifts. The columns corresponding to a variable $x^a y^b z^c$ and a variable $x^m y^{m-a} z^c$ only with non-zero terms is depicted in Table 1.
Therefore, from Table 1 the result holds in this case.

Case(ii): Any column in remaining $\left(\frac{1}{2}(m^2 + m)t + (m + 1)t\right)$ columns of M_s, i.e.,a column corresponding coefficients of a variable $x^a y^b z^c$ with $a < b + c$, from the above analysis in (1).

The coefficient of $x^a y^b z^c$ is non-zero in g_s-shifts $x^{k_1} z^{k_2} f^n e^{k_1}$ if and only if $a \geq k_1, b \leq m - k_1, c \geq k_2$, $a - k_1 \geq b + (c - k_2)$ and note for $a < b + c$, $a - k_1 < b + (c - k_2)$ as $k_1 \geq k_2$ in g_s-shifts. So the coefficient of $x^a y^b z^c$ is zero in all rows corresponding to g_s-shifts.

The coefficient of $x^a y^b z^c$ is non-zero in h_s-shifts $x^{k_1} z^{k_2} f^n e^{k_1}$ if and only if $a \geq k_1, b \leq m - k_1, c \geq k_2$ and $a - k_1 \geq b + (c - k_2)$. For $k_1 > a - b$, $a - k_1 < b + (c - k_2)$ and from the inequalities $k_1 + 1 \leq k_2 \leq k_1 + t$, $a - k_1 \geq b + (c - k_2)$, we have the coefficient of $x^a y^b z^c$ is non-zero in h_s-shifts $x^{k_1} z^{k_2} f^n e^{k_1}$ if and only if $a \geq k_1, b \leq m - k_1, c \geq k_2$ and $k_1 = 0, ..., a - b$, $k_2 = \max\{k_1 + 1, k_1 + (b + c) - a\}, ..., \min\{c, k_1 + t\}$. Take $l_t = \min\{c, k_1 + t\}$.

Note that coefficient of $x^m y^{m-a} z^c$ is zero in all g_s-shifts as $a > c$ and for $k_1 > a - b$ in h_s-shifts. The columns corresponding to a variable $x^a y^b z^c$ and a variable $x^m y^{m-a} z^c$ only with non-zero terms is depicted in Table 2. Therefore, from Table 2 the result holds in this case.

□

Rows corresponding to g and h shifts	Column corresponding to $x^a y^b z^c$	Column corresponding to $x^m y^{m-a} z^c$
$x^{a-b} z^c f^{m-(a-b)} e^{a-b}$	$\frac{(m-(a-b))!}{(m-a)!b!}(-1)^{m-a} X^a Y^b Z^c e^{a-b}$	$X^m Y^{m-(a-b)} Z^c e^{a-b}$
$x^{a-b-1} z^{c-1} f^{m-(a-b-1)} e^{a-b-1}$	$\frac{(m-(a-b)+1)!}{(m-a)!b!}(-1)^{m-a} 2^n X^a Y^b Z^c e^{a-b-1}$	$\frac{(m-(a-b)+1)!}{(m-(a-b))!} 2^n X^m Y^{m-(a-b)} Z^c e^{a-b-1}$
$x^{a-b-1} z^c f^{m-(a-b-1)} e^{a-b-1}$	$\frac{(m-(a-b)+1)!}{(m-a)!b!}(-1)^{m-a}(N+1) X^a Y^b Z^c e^{a-b-1}$	$\frac{(m-(a-b)+1)!}{(m-(a-b))!}(N+1) X^m Y^{m-(a-b)} Z^c e^{a-b-1}$
$\vdots$	$\vdots$	$\vdots$
$x^{a-b-(c-1)} z f^{m-((a-b)-(c-1))} e^{a-b-(c-1)}$	$\frac{(m-(a-b)+(c-1))!}{(m-a)!b!(c-1)!}(-1)^{m-a}(2^n)^{c-1} X^a Y^b Z^c e^{a-b-(c-1)}$	$\frac{(m-(a-b)+(c-1))!}{(m-(a-b))!(c-1)!}(2^n)^{c-1} X^m Y^{m-(a-b)} Z^c e^{a-b-(c-1)}$
$\vdots$	$\vdots$	$\vdots$
$x^{a-b-(c-1)} z^c f^{m-((a-b)-(c-1))} e^{a-b-(c-1)}$	$\frac{(m-(a-b)+(c-1))!}{(m-a)!b!(c-1)!}(-1)^{m-a}(N+1)^{c-1} X^a Y^b Z^c e^{a-b-(c-1)}$	$\frac{(m-(a-b)+(c-1))!}{(m-(a-b))!(c-1)!}(N+1)^{c-1} X^m Y^{m-(a-b)} Z^c e^{a-b-(c-1)}$
$x^{a-b-c} f^{m-(a-b)+c} e^{a-(b+c)}$	$\frac{(m-(a-b)+c)!}{(m-a)!b!c!}(-1)^{m-a}(2^n)^c X^a Y^b Z^c e^{a-b-c}$	$\frac{(m-(a-b)+c)!}{(m-(a-b))!c!}(2^n)^c X^m Y^{m-(a-b)} Z^c e^{a-b-c}$
$\vdots$	$\vdots$	$\vdots$
$x^{a-b-c} z^c f^{m-(a-b)+c} e^{a-(b+c)}$	$\frac{(m-(a-b)+c)!}{(m-a)!b!c!}(-1)^{m-a}(N+1)^c X^a Y^b Z^c e^{a-b-c}$	$\frac{(m-(a-b)+c)!}{(m-(a-b))!c!}(N+1)^c X^m Y^{m-(a-b)} Z^c e^{a-b-c}$
$\vdots$	$\vdots$	$\vdots$
f^m	$\frac{m!}{(m-a)!b!c!(a-(b+c))!}(-1)^{m-a}(N+1)^{(a-(b+c))}(2^n)^c X^a Y^b Z^c$	$\frac{m!}{(m-(a-b))!c!(a-(b+c))!}(N+1)^{a-(b+c)}(2^n)^c X^m Y^{m-(a-b)} Z^c$
$x^{c-1} z^c f^{m-(c-1)} e^{c-1}$	$\frac{(m-(c-1))!}{(m-a)!b!(a-(b+c)+1)!}(-1)^{m-a}(N+1)^{a-(b+c)+1} X^a Y^b Z^c e^{c-1}$	$\frac{(m-(c-1))!}{(m-(a-b))!(a-(b+c)+1)!}(N+1)^{a-(b+c)+1} X^m Y^{m-(a-b)} Z^c e^{c-1}$
$\vdots$	$\vdots$	$\vdots$
$xz^2 f^{m-1} e$	$\frac{(m-1)!}{(m-a)!b!(c-2)!(a-(b+c)+1)!}(-1)^{m-a}(N+1)^{a-(b+c)+1}(2^n)^{c-2} X^a Y^b Z^c e$	$\frac{(m-1)!}{(m-(a-b))!(c-2)!(a-(b+c)+1)!}(N+1)^{a-(b+c)+1}(2^n)^{c-2} X^m Y^{m-(a-b)} Z^c e$
$\vdots$	$\vdots$	$\vdots$
$xz^{l_t} f^{m-1} e$	$\frac{(m-1)!}{(m-a)!b!(c-l_t)!(a-(b+c)+l_t-1)!}(-1)^{m-a}(N+1)^{a-(b+c)+l_t-1}(2^n)^{c-l_t} X^a Y^b Z^c e$	$\frac{(m-1)!}{(m-(a-b))!(c-l_t)!(a-(b+c)+l_t-1)!}(N+1)^{a-(b+c)+l_t-1}(2^n)^{c-l_t} X^m Y^{m-(a-b)} Z^c e$
zf^m	$\frac{m!}{(m-a)!b!(c-1)!(a-(b+c)+1)!}(-1)^{m-a}(N+1)^{a-(b+c)+1}(2^n)^{c-1} X^a Y^b Z^c$	$\frac{m!}{(m-(a-b))!(c-1)!(a-(b+c)+1)!}(N+1)^{a-(b+c)+1}(2^n)^{c-1} X^m Y^{m-(a-b)} Z^c$
$\vdots$	$\vdots$	$\vdots$
$z^{l_t} f^m$	$\frac{m!}{(m-a)!b!(c-l_t)!(a-(b+c)+l_t)!}(-1)^{m-a}(N+1)^{a-(b+c)+l_t}(2^n)^{c-l_t} X^a Y^b Z^c$	$\frac{m!}{(m-(a-b))!(c-l_t)!(a-(b+c)+l_t)!}(-1)^{m-a}(N+1)^{a-(b+c)+l_t}(2^n)^{c-l_t} X^m Y^{m-(a-b)} Z^c$

Table 1: A column in first $(\frac{1}{6}m^3 + m^2 + \frac{11}{6}m + 1)$ columns of M_s and a column corresponding to coefficients of a variable $x^m y^{m-a} z^c$ only with non-zero terms.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 20 July 2018 doi:10.20944/preprints201807.0379.v1

Peer-reviewed version available at Cryptography 2018, 2, 36; doi:10.3390/cryptography2040036

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 20 July 2018 doi:10.20944/preprints201807.0379.v1

Peer-reviewed version available at *Cryptography* **2018**, *2*, 36; doi:10.3390/cryptography2040036

Rows corresponding to g and h shifts	Column corresponding to $x^a y^b z^c$	Column corresponding to $x^m y^{m-a} z^c$
$x^{a-b} z^c f^{m-(a-b)} e^{a-b}$	$\frac{(m-(a-b))!}{(m-a)!b!}(-1)^{m-a} X^a Y^b Z^c e^{a-b}$	$X^m Y^{m-(a-b)} Z^c e^{a-b}$
$\dots$	$\dots$	$\dots$
$x^2 z^{(b+c)-a+2} f^{m-2} e^2$	$\frac{(m-2)!}{(m-a)!b!((a-b)-2)!}(-1)^{m-a}(2^n)^{(a-b)-2} X^a Y^b Z^c e^2$	$\frac{(m-2)!}{(m-(a-b))!((a-b)-2)!}(2^n)^{(a-b)-2} X^m Y^{m-(a-b)} Z^c e^2$
$\dots$	$\dots$	$\dots$
$x^2 z^{l_t} f^{m-2} e^2$	$\frac{(m-2)!}{(m-a)!b!(c-l_t)!((b+c)-a+2)!}(-1)^{m-a}(N+1)^{l_t-((b+c)-a+2)}(2^n)^{c-l_t} X^a Y^b Z^c e^2$	$\frac{(m-2)!}{(m-(a-b))!(c-l_t)!(l_t-((b+c)-a+2))!}(N+1)^{l_t-((b+c)-a+2)}(2^n)^{c-l_t} X^m Y^{m-(a-b)} Z^c e^2$
$x z^{b+c-a+1} f^{m-1} e$	$\frac{(m-1)!}{(m-a)!b!((a-b)-1)!}(-1)^{m-a}(2^n)^{(a-b)-1} X^a Y^b Z^c e$	$\frac{(m-1)!}{(m-(a-b))!((a-b)-1)!}(2^n)^{(a-b)-1} X^m Y^{m-(a-b)} Z^c e$
$\dots$	$\dots$	$\dots$
$x z^{l_t} f^{m-1} e$	$\frac{(m-1)!}{(m-a)!b!(c-l_t)!((l_t-(b+c-a+1))!}(-1)^{m-a}(N+1)^{(l_t-(b+c-a+1))}(2^n)^{c-l_t} X^a Y^b Z^c e$	$\frac{(m-1)!}{(m-(a-b))!(c-l_t)!((l_t-(b+c-a+1))!}(N+1)^{(l_t-(b+c-a+1))}(2^n)^{c-l_t} X^m Y^{m-(a-b)} Z^c e$
$z^{b+c-a} f^m$	$\frac{m!}{(m-a)!b!(a-b)!}(-1)^{m-a}(2^n)^{a-b} X^a Y^b Z^c$	$\frac{m!}{(m-(a-b))!(a-b)!}(2^n)^{a-b} X^m Y^{m-(a-b)} Z^c$
$\dots$	$\dots$	$\dots$
$z^{l_t} f^m$	$\frac{m!}{(m-a)!b!(c-l_t)!(l_t-((b+c)-a))!}(-1)^{m-a}(N+1)^{l_t-((b+c)-a)}(2^n)^{c-l_t} X^a Y^b Z^c$	$\frac{m!}{(m-(a-b))!(c-l_t)!(l_t-((b+c)-a))!}(-1)^{m-a}(N+1)^{l_t-((b+c)-a)}(2^n)^{c-l_t} X^m Y^{m-(a-b)} Z^c$

Table 2: A column in the last $\left(\frac{1}{2}(m^2+m)t+(m+1)t\right)$ columns of M_s and a column corresponding to coefficients of a variable $x^m y^{m-a} z^c$ only with non-zero terms.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 20 July 2018 doi:10.20944/preprints201807.0379.v1

Peer-reviewed version available at Cryptography 2018, 2, 36; doi:10.3390/cryptography2040036

From the above theorem, all columns corresponding to a variable $x^a y^b z^c$ for all $0 \le a \le m-1$ are depending on a non-removed column, corresponding to a variable $x^m y^{m-(a-b)} z^c$ in M_s. Let M_{sl} be a matrix formed by removing all above columns from the matrix M_s and S_l be a lattice spanned by rows of M_{sl}. Then the short vector in S_l lead to short reconstruction vector in S_L, i.e., if $u = \sum_{b \in B} c_b b$ is a short vector in S_l then this lead to a short vector $\bar{u} = \sum_{b \in \bar{B}} c_b b$ (same coefficients c_b) in S_L where B and $\bar{B}$ are the basis for S_l and S_L respectively.

As we removed all depending columns in M_s to form a matrix M_{sl}, apply the lattice based techniques to S_l instead of S_L to get an attack bound and this lattice reduction techniques gives a required short vectors in S_L for a given bound.

The matrix M_{sl} is lower triangular with rows same as in M_s and each column corresponding to coefficients of one of the variables (leading monomials of g_s and h_s-shifts)

$$g_s\text{-shift}\begin{cases} x^m, x^m z, ..., x^m z^m, \\ x^m y, ..., x^m y z^{m-1}, \\ \vdots \\ x^m y^{m-1}, x^m y^{m-1} z, \\ x^m y^m, \end{cases}$$

$$h_s\text{-shift}\begin{cases} x^m z^{m+1}, ..., x^m z^{m+t}, \\ x^m y z^m, ..., x^m y z^{(m-1)+t}, \\ \vdots \\ x^m y^{m-1} z^2, ..., x^m y^{m-1} z^{1+t}, \\ x^m y^m z, .., x^m y^m z^t. \end{cases}$$

Therefore S_l is a lattice spanned by coefficient vectors of the shift polynomials $g_{sl}(xX, yY, zZ)$ and $h_{sl}(xX, yY, zZ)$ where

$$g_{sl}(x, y, z) = x^{l_1} z^{l_2} f^n e^{l_1} \text{ for } n = 0, ..., m, l_1 = m - n, l_2 = 0, ..., l_1 \text{ and}$$
$$h_{sl}(x, y, z) = x^{l_1} z^{l_2} f^n e^{l_1} \text{ for } n = 0, ..., m, l_1 = m - n, l_2 = l_1 + 1, ..., l_1 + t.$$

Since S_l is full-rank lattice, $\det S_l = \det M_{sl} = e^{n(e)} X^{n(X)} Y^{n(Y)} Z^{n(Z)}$ where $n(e), n(X), n(Y), n(Z)$ are denotes the number of $e's, X's, Y's, Z's$ in all the diagonal elements of M_{sl} respectively. As $x^n y^n$ is a leading monomial of f^n with coefficient 1, we have

$$\begin{aligned} n(e) &= \sum_{n=0}^{m} \sum_{l_1=m-n} \sum_{l_2=0}^{l_1} l_1 + \sum_{n=0}^{m} \sum_{l_1=m-n} \sum_{l_2=l_1+1}^{l_1+t} l_1 \\ &= (1/3)m^3 + m^2 + (1/2)(m^2+m)t + (2/3)m, \\ n(X) &= \sum_{n=0}^{m} \sum_{l_1=m-n} \sum_{l_2=0}^{l_1} n + l_1 + \sum_{n=0}^{m} \sum_{l_1=m-n} \sum_{l_2=l_1+1}^{l_1+t} n + l_1 \\ &= (1/2)m^3 + (3/2)m^2 + (m^2+m)t + m, \\ n(Y) &= \sum_{n=0}^{m} \sum_{l_1=m-n} \sum_{l_2=0}^{l_1} n + \sum_{n=0}^{m} \sum_{l_1=m-n} \sum_{l_2=l_1+1}^{l_1+t} n \\ &= (1/6)m^3 + (1/2)m^2 + (1/2)(m^2+m)t + (1/3)m, \\ n(Z) &= \sum_{n=0}^{m} \sum_{l_1=m-n} \sum_{l_2=0}^{l_1} l_2 + \sum_{n=0}^{m} \sum_{l_1=m-n} \sum_{l_2=l_1+1}^{l_1+t} l_2 \\ &= (1/6)m^3 + (1/2)(m+1)t^2 + (1/2)m^2 + (1/2)(m^2+2m+1)t + (1/3)m \\ \text{and } \dim(S_l) &= \omega = \sum_{n=0}^{m} \sum_{l_1=m-n} \sum_{l_2=0}^{l_1} 1 + \sum_{n=0}^{m} \sum_{l_1=m-n} \sum_{l_2=l_1+1}^{l_1+t} 1 \\ &= (1/2)m^2 + (m+1)t + (3/2)m + 1. \end{aligned}$$

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 20 July 2018 doi:10.20944/preprints201807.0379.v1

Peer-reviewed version available at Cryptography 2018, 2, 36; doi:10.3390/cryptography2040036

Take $t = \tau m$, then for sufficiently large m, the exponents $n(e), n(X), n(Y), n(Z)$ and the dimension ω reduce to

$$\begin{aligned}
\omega &= \left(\frac{1}{2} + \tau\right) m^2 + o(m),\\
n(e) &= \left(\frac{1}{3} + \frac{1}{2}\tau\right) m^3 + o(m^2),\\
n(X) &= \left(\frac{1}{2} + \tau\right) m^3 + o(m^2),\\
n(Y) &= \left(\frac{1}{6} + \frac{1}{2}\tau\right) m^3 + (m^2),\\
n(Z) &= \left(\frac{1}{6} + \frac{1}{2}\tau + \frac{1}{2}\tau^2\right) m^3 + o(m^2).
\end{aligned}$$

Applying the LLL algorithm to the basis vectors of the lattice S_l, i.e., coefficient vectors of the shift polynomials, we get a LLL-reduced basis say $\{v_1, v_2, ..., v_\omega\}$ and from the Theorem 1 we have

$$||v_1|| \leq ||v_2|| \leq ||v_3|| \leq 2^{\frac{\omega(\omega-1)}{4(\omega-2)}} \det(S_l)^{\frac{1}{\omega-2}}.$$

In order to apply the generalization of Howgrave-Graham result in Theorem 2, we need the following inequality

$$2^{\frac{\omega(\omega-1)}{4(\omega-2)}} \det(S_l)^{\frac{1}{\omega-2}} < \frac{e^m}{\sqrt{\omega}}.$$

from this, we deduce

$$\det(S_l) < \frac{1}{\left(2^{\frac{\omega(\omega-1)}{4(\omega-2)}}\sqrt{\omega}\right)^{\omega-2}} e^{m(\omega-2)} < \frac{1}{\left(2^{\frac{\omega(\omega-1)}{4(\omega-2)}}\sqrt{\omega}\right)^{\omega-2}} e^{m\omega}.$$

As the dimension ω is not depending on the public encryption exponent e, $\frac{1}{\left(2^{\frac{\omega(\omega-1)}{4(\omega-2)}}\sqrt{\omega}\right)^{\omega-2}}$ is a fixed constant, so we need the inequality $\det(S_l) < e^{m\omega}$, i.e., $e^{n(e)} X^{n(X)} Y^{n(Y)} Z^{n(Z)} < e^{m\omega}$.

Substitute all values and taking logarithms, neglecting the lower order terms and after simplifying by m^3 we get

$$(-1 - 3\tau)\alpha + (3 + 6\tau)\delta + (1 + 3\tau)\gamma_1 + (1 + 3\tau + 3\tau^2)\gamma_2 < 0.$$

The left hand side inequality is minimized at $\tau = \frac{\alpha - (2\delta + \gamma_1 + \gamma_2)}{2\gamma_2}$ and putting this value in the above inequality we get

$$\delta < \frac{1}{2}\alpha - \frac{1}{2}\gamma_1 - \frac{1}{6}\sqrt{6(\alpha - \gamma_1)\gamma_2 + 3\gamma_2^2}.$$

From the first three short vectors v_1, v_2 and v_3 in LLL reduced basis of a basis B in S_l we consider three polynomials $g_1(x, y, z), g_2(x, y, z)$ and $g_3(x, y, z)$ over $\mathbb{Z}$ such that $g_1(x_0, y_0, z_0) = g_2(x_0, y_0, z_0) = g_3(x_0, y_0, z_0) = 0$. These short vectors v_1, v_2 and v_3 lead to a short vector $\bar{v_1}, \bar{v_2}$ and $\bar{v_3}$ respectively and $\bar{g_1}(x, y, z), \bar{g_2}(x, y, z)$ and $\bar{g_3}(x, y, z)$ its corresponding polynomials. Apply the same analysis in paper [2] to the above polynomials to get the factors p and q of RSA modulus N.

Theorem 5. Let $N = pq$ be an RSA modulus with $q < p < 2q$. Let $e = N^\alpha, X = N^\delta, Y = N^{\gamma_1}, Z = N^{\gamma_2}$ and k be the multiplicative inverse of $\varphi(N)$ modulo e. Suppose the prime sum $p+q$ is of the form $p+q = 2^n k_0 + k_1$, for a known positive integer n and for $|k| \leq X, \max\{|k_0|, |k_1|\} \leq Y$ and $\min\{|k_0|, |k_1|\} \leq Z$ one can factor N in polynomial time if

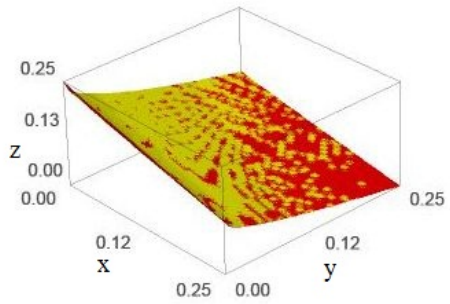
$$\delta < \frac{1}{2}\alpha - \frac{1}{2}\gamma_1 - \frac{1}{6}\sqrt{6(\alpha - \gamma_1)\gamma_2 + 3\gamma_2^2}. \tag{2}$$

Proof. Follows from the above argument and the LLL lattice basis reduction algorithm operates in polynomial time [11]. □

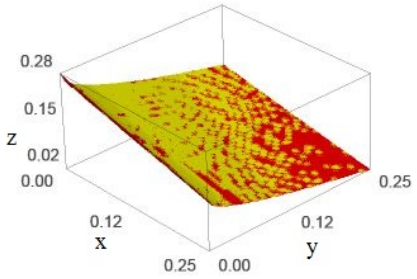
Note that for any given primes p and q with $q < p < 2q$, we can always find a positive integer n such that $p + q = 2^n k_0 + k_1$ where $0 \leq |k_0|, |k_1| \leq \approx 0.25$. A typical example is $2^n \approx \frac{3}{\sqrt{2}} N^{0.25}$ as $p + q < \frac{3}{\sqrt{2}} N^{0.5}$ [14]. So take γ_1 and γ_2 in the range (0,0.25).
Let δ_L and δ_{sl} be the bounds for δ in inequalities (1) and (2) respectively. Then note that δ_{sl} is slightly larger than δ_L and is depicted in Figure 1 for $\alpha = 0.51, 0.55, 0.750$ and 1.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 20 July 2018 doi:10.20944/preprints201807.0379.v1

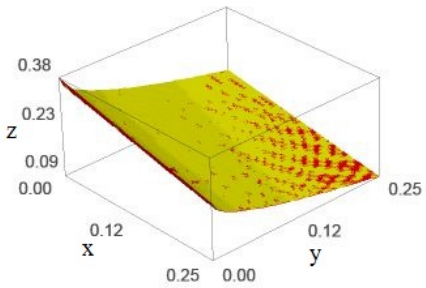
Peer-reviewed version available at Cryptography 2018, 2, 36; doi:10.3390/cryptography2040036



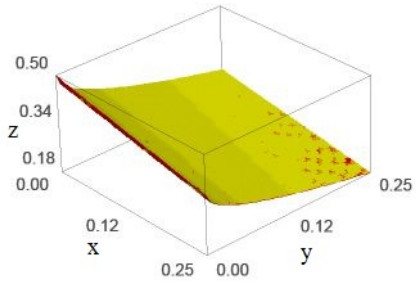
(a) $\alpha = 0.501$



(b) $\alpha = 0.55$



(c) $\alpha = 0.75$



(d) $\alpha = 1$

Figure 1: The region of δ_{sl} and δ_L for $\alpha = 0.501, 0.55, 0.75, 1$.

In the Figure 1, x, y, z-axis represents γ_1, γ_2, bound for δ respectively and yellow, red regions represents δ_{sl}, δ_L receptively. From this figure, it is noted that the yellow region is slightly above the red region, i.e., δ_{sl} is slightly grater than δ_L and this improvement increases when the values of α increases.

As the dimension of L is $(1/6)m^3 + (1/2)m^2(t+2) + (1/6)m(9t+11) + (t+1)$ for $t = \left(\frac{\alpha-(2\delta+\gamma_1+\gamma_2)}{3\gamma_2}\right) m$ [2] and S_l is $(1/2)m^2 + (m+1)t + (3/2)m + 1$ for $t = \left(\frac{\alpha-(2\delta+\gamma_1+\gamma_2)}{2\gamma_2}\right) m$, note the dimension of S_l is $(1/6)m^3 + (1/3)t(m^2-1) + (1/2)m^2 + (1/3)m$, for $t = \left(\frac{\alpha-(2\delta+\gamma_1+\gamma_2)}{2\gamma_2}\right)$ smaller than the dimension of L.

4 Conclusion

In this paper, an another attack bound for k, a small multiplicative inverse of $\varphi(N)$ modulo e is given when the prime sum $p+q$ is of the form $p+q = 2^n k_0 + k_1$ where n is a given positive integer and k_0 and k_1 are two suitably small unknown integers using sublattice reduction techniques and Coppersmith's methods for finding small roots of modular polynomial equations. This attack bound is slightly larger than the bound, in the approach using lattice based techniques and requires lattice of smaller dimension than the approach given by using lattice based techniques.

References

[1] P. Anuradha Kameswari and L. Jyotsna, *"Cryptanalysis of RSA with Small Multiplicative Inverse of $(p-1)$ or $(q-1)$ Modulo e"*, Journal of Global Research in Mathematical Archives, 5(5), May 2018, 72-81, ISSN: 2320-5822.

[2] P. Anuradha Kameswari and L. Jyotsna, *"Cryptanalysis of RSA with Small Multiplicative Inverse of $\varphi(N)$ Modulo e and with a Composed Prime Sum $p+q$"*, International Journal of Mathematics And its Applications 6(1-C)(May 2018), 515-526, ISSN: 2347-1557.

[3] Boneh, D. *"Twenty Years of Attacks on the RSA Cryptosystem"*, Notices Amer. Math. Soc. 46 (2), 203-213, (1999).

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 20 July 2018 doi:10.20944/preprints201807.0379.v1

Peer-reviewed version available at Cryptography 2018, 2, 36; doi:10.3390/cryptography2040036

[4] 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 Vol.1592, Springer-Verlag, pp. 111 (1999)).

[5] J. Blomer, A. May, *"Low Secret Exponent RSA Revisited"*, Cryptography and Lattice Conference (CaLC 2001), Lecture Notes in Computer Science Volume 2146, SpringerVerlag, pp. 419, 2001.

[6] D. Burton, *"Elementary Number Theory"*, Sixth edition, Mc Graw Hill, New York, 2007.

[7] Coppersmith, D. *"Small solutions to polynomial equations, and low exponent RSA vulnerabilities"*. Journal of Cryptology, 10(4), pp. 233260 (1997).

[8] Howgrave-Graham, N. *"Finding small roots of univariate modular equations revisited"*, In Cryptography and Coding, LNCS 1355, pp. 131142, Springer-Verlag (1997).

[9] PA Kameswari, L Jyotsna, *"Extending Wiener's Extension to RSA-Like Cryptosystems over Elliptic Curves"*, British Journal of Mathematics & Computer Science 14 (1), 1-8.

[10] Jochemsz, E., May, A. *"A strategy for finding roots of multivariate polynomials with new applications in attacking RSA variants"*, in: ASIACRYPT 2006, LNCS, vol. 4284, 2006, pp. 267-282, Springer-Verlag.

[11] Lenstra, A.K., Lenstra, H.W., Lovasz,L. *"Factoring polynomials with rational coefficients, Mathematische Annalen"*, Vol. 261, pp. 513534, 1982.

[12] May, A.: *"New RSA Vulnerabilities Using Lattice Reduction Methods"*,. PhD thesis, University of Paderborn (2003). Available at http://wwwcs.upb.de/cs/ag-bloemer/personen/alex/publikationen/

[13] Neal Kobliz, *"A Course in Number Theory and Cryprography"* ISBN 3-578071-8, SPIN 10893308.

[14] Nitaj, A.: *Another generalization of Wieners attack on RSA*, In: Vaudenay, S. (ed.) Africacrypt 2008. LNCS, vol. 5023, pp. 174190. Springer, Heidelberg (2008).

[15] K. H. Rosen, *" Elemetary Number Theory and Its Applications"*, Addison-Wesley, Reading Mass, 1984.

[16] Subhamoy Maitra and Santanu Sarkar, *" RSA Cryptanalysis with Increased Bounds on the Secret Exponent using Less Lattice Dimension"*,. Cryptology ePrint Archive: Report 2008/315, Available at http://eprint.iacr.org/2008/315.

[17] Subhamoy Maitra and Santanu Sarkar, *"Revivting Wiener's Attack - New Weak Keys in RSA"*, http://eprint.iacr.org/2005/228.pdf.

[18] H. -M. Sun, M. -E. Wu and Y. -H. Chen. *"Estimating the prime-factors of an RSA modulus and an extension of the Wiener attack"*. ACNS 2007, LNCS 4521, pp. 116128, 2007.

[19] B. de Weger, *" Cryptanalysis of RSA with Small Prime Difference"*, Applicable Algebra in Engineering, Communication and Computing, 13(1);17-28,2002.

[20] M. Wiener, *" Cryptanalysis of Short RSA Secret Exponents"*, IEEE Transactions on Information Theory, 36(3)-553-558, 1990.