Discrete Applied Mathematics 203 (2016) 127–133

Contents lists available at ScienceDirect

Discrete Applied Mathematics

journal homepage: www.elsevier.com/locate/dam

Revisiting Prime Power RSA

Santanu Sarkar

Department of Mathematics, Indian Institute of Technology Madras, Sardar Patel Road, Chennai 600 036, India

ARTICLE INFO

Article history:
Received 2 April 2014
Received in revised form 27 August 2015
Accepted 1 October 2015
Available online 27 October 2015

Keywords:
Partial key exposure
Lattice
Prime Power RSA
Small decryption exponent

ABSTRACT

Recently Sarkar (DCC 2014) has proposed a new attack on small decryption exponent when RSA Modulus is of the form $N = p^r q$ for $r \geq 2$. This variant is known as Prime Power RSA. The work of Sarkar improves the result of May (PKC 2004) when $r \leq 5$. In this paper, we improve the work of Sarkar when $2 < r \leq 8$.

We also study partial key exposure attack on Prime Power RSA. Our result improves the works of May (PKC 2004) when $r \leq 8$ and the decryption exponent $d < N^{\frac{1}{r+1}+\frac{3r-2\sqrt{3r+3}+3}{3(r+1)}}$.

1. Introduction

In the domain of public key cryptography, RSA has been the most popular cipher since its inception in 1978 by Rivest, Shamir and Adleman. Wiener [22] presented an important result on RSA by showing that one can factor N in polynomial time if the decryption exponent $d < \frac{1}{3}N^{\frac{1}{4}}$. Later using the idea of Coppersmith [6], Boneh and Durfee [3] improved this bound up to $d < N^{0.292}$.

There are several RSA variants proposed in the literature for efficiency and security point of view. In this paper, we consider Prime Power RSA, where RSA modulus N is of the form $N = p^r q$ where $r \geq 2$. The modulus $N = p^2 q$ was first used by Fujioka et al. in Eurocrypt 1991 [9]. In Eurocrypt 1998, Okamoto et al. [19] also used $N = p^2 q$ to design a public key crypto system.

There are two variants of Prime Power RSA. In the first variant $ed \equiv 1 \bmod p^{r-1}(p-1)(q-1)$, where as in the second variant $ed \equiv 1 \bmod (p-1)(q-1)$. In [11], authors proved that polynomial time factorization is possible for the second variant if $d < N^{\frac{2-\sqrt{2}}{r+1}}$.

For the first variant, Takagi in Crypto 1998 [21] proved that when $d \leq N^{\frac{1}{2(r+1)}}$, one can factor N in polynomial time. Later in PKC 2004, May [18] improved this bound up to $d < N^{\max\left\{\frac{r}{(r+1)^2}, (\frac{r-1}{r+1})^2\right\}}$. Recently, Lu et al. [16,17] have shown that one can factor N when $d < N^{\frac{r(r-1)}{(r+1)^2}}$, which improves the work of [18].

Sarkar [20] has considered the polynomial $f_e(x, y, z) = 1 + x(N - y^r - y^{r-1}z + y^{r-1})$ over $\mathbb{Z}_e$ whose root is $(x_0, y_0, z_0) = (b, p, q)$, where $ed = 1 + b\phi(N)$ to analyze the RSA modulus $N = p^r q$. In this paper we consider the same polynomial. But our lattice construction to solve this polynomial is different from [20]. As a result, we improve the existing works of [18,20,16] when $r = 3, 4$.

Partial exposure on d. In Crypto 1996, Kocher [12] first proposed a novel attack which is known as partial key exposure attack. He showed that an attacker can get a few bits of d by timing characteristic of an RSA implementing device. Fault

E-mail address: sarkar.santanu.bir@gmail.com.

http://dx.doi.org/10.1016/j.dam.2015.10.003
0166-218X/

attacks [2] and power analysis [13] are other important side channel attacks in this direction. Boneh, Durfee and Frankel [4] first proposed polynomial time algorithms when the attacker knows a few bits of the decryption exponent. The approach of [4] works only when the upper bound on e is $\sqrt{N}$. Later this constraint was removed by Blömer et al. in Crypto 2003 [1] and Ernst et al. in Eurocrypt 2005 [8].

May in PKC 2004 [18] studied partial key exposure attack on Prime Power RSA. He showed that one can factor N in polynomial time from the knowledge of d_0 where $|d - d_0| < N^{\max\left\{\frac{r}{(r+1)^2}, (\frac{r-1}{r+1})^2\right\}}$ when RSA modulus $N = p^r q$. Lu et al. [16] improve the work of [18] and show that factorization of N can be possible when $|d - d_0| < N^{\frac{r(r-1)}{(r+1)^2}}$. So in particular, when $r = 2$, approach of [16] works when $|d - d_0| < N^{0.22}$. We have improved this bound up to $N^{0.33}$. Unfortunately, our method works only when $d < N^{0.67}$.

2. Useful lemmas and preliminaries

Consider w many linearly independent vectors $b_1, \ldots, b_w \in \mathbb{R}^n$. The set

$$L = \left\{ \boldsymbol{b} : \boldsymbol{b} = \sum_{i=1}^{w} c_i b_i, \;\; c_1, \ldots, c_w \in \mathbb{Z} \right\}$$

is called an w dimensional lattice with basis $B = \{b_1, \ldots, b_w\}$. A lattice is of full rank when $w = n$ and in this paper we only use such lattices. The determinant of L is defined as $\det(L) = \det(M)$, where the rows of M are the vectors from B. When $b_1, \ldots, b_w \in \mathbb{Z}^n$, the lattice L is called an integer lattice.

In 1982, Lenstra, Lenstra and Lovász [15] proposed a polynomial time algorithm (known as LLL algorithm) to obtain another basis with some useful properties: given a basis $b_1, \ldots, b_w$ of a lattice L, LLL algorithm gives a (reduced) basis $u_1, \ldots, u_w$ with

$$\|u_1\| \leq \|u_2\| \leq \|u_3\| \leq 2^{\frac{w(w-1)}{4(w-2)}} \det(L)^{\frac{1}{w-2}}. \tag{1}$$

In [6], Coppersmith formulated seminal ideas to find small roots of modular polynomials in single variable and also of polynomials in two variables over the integers. These deterministic techniques have many important consequences in cryptography. The idea of [6] can also be extended to more than two variables, but the method becomes a heuristic in that case. The following result due to Howgrave-Graham [10] gives a sufficient condition under which modular roots become the roots over integers for polynomials in three variables.

Theorem 1. *Let $g(x, y, z)$ be a polynomial with integer coefficients which is a sum of w many monomials. Suppose that*
1. *$g(x_0, y_0, z_0) \equiv 0 \bmod e^m$ for positive integers e, m and $|x_0| < X$, $|y_0| < Y$, $|z_0| < Z$.*
2. *$\|g(xX, yY, zZ)\| < \frac{e^m}{\sqrt{w}}$,*

Then $g(x_0, y_0, z_0) = 0$ holds over integers.

Suppose we have w polynomials $b_1, \ldots, b_w$ in the variables x, y, z such that $b_1(x_0, y_0, z_0) = \cdots = b_w(x_0, y_0, z_0) = 0 \bmod e^m$ with $|x_0| < X$, $|y_0| < Y$ and $|z_0| < Z$. Now we construct a lattice L with the coefficient vectors of $b_1(xX, yY, zZ), \ldots, b_w(xX, yY, zZ)$. Since lattice reduction is a series of elementary row operations, after reduction, we get three polynomials $u_1(x, y, z)$, $u_2(x, y, z)$ and $u_3(x, y, z)$ such that

$$u_1(x_0, y_0, z_0) = u_2(x_0, y_0, z_0) = u_3(x_0, y_0, z_0) = 0 \bmod e^m$$

which correspond to first three vectors of the reduced basis. Also by the property of LLL algorithm, we have

$$\|u_1(xX, yY, zZ)\| \leq \|u_2(xX, yY, zZ)\| \leq \|u_3(xX, yY, zZ)\| \leq 2^{\frac{w(w-1)}{4(w-2)}} \det(L)^{\frac{1}{w-2}}.$$

Hence by Theorem 1, if

$$2^{\frac{w(w-1)}{4(w-2)}} \det(L)^{\frac{1}{w-2}} < \frac{e^m}{\sqrt{w}},$$

then we have $u_1(x_0, y_0, z_0) = u_2(x_0, y_0, z_0) = u_3(x_0, y_0, z_0) = 0$. The required condition can be taken as $\det(L)^{\frac{1}{w-2}} < e^m$ by neglecting the terms $2^{\frac{w(w-1)}{4(w-2)}}$ and $\frac{1}{\sqrt{w}}$. Again if $w \gg 2$, we can simplify the condition as $(\det(L))^{\frac{1}{w}} < e^m$.

Thus if $\det(L) < e^{mw}$, after lattice reduction we will get three polynomials $u_1(x_0, y_0, z_0) = u_2(x_0, y_0, z_0) = u_3(x_0, y_0, z_0) = 0$. We want to find x_0, y_0, z_0 from u_1, u_2, u_3. Although our technique works in practice as noted from the experiments we perform, we need the following heuristic assumption for theoretical results.

Assumption 1. Our lattice-based construction yields algebraically independent polynomials. The common roots of these polynomials can be efficiently computed by using techniques like calculation of the resultants or finding a Gröbner basis.

It is important to fix the degrees of the polynomials, since time complexity of the Gröbner basis computation is in general double-exponential in the degrees of the polynomials [7]. For this reason, the dimension of the lattice that we construct should not be large.