# Small Secret Exponent Attacks on RSA with Unbalanced Prime Factors

Atsushi Takayasu
The University of Tokyo
National Institute of Advanced Industrial Science and Technology (AIST)
Tokyo, Japan
Email: a-takayasu@it.k.u-tokyo.ac.jp

Noboru Kunihiro
The University of Tokyo
Tokyo, Japan
Email: kunihiro@k.u-tokyo.ac.jp

***Abstract*—Boneh and Durfee (Eurocrypt 1999) proposed two polynomial time attacks on *small secret exponent RSA*. The first attack works when $d < N^{0.284}$ whereas the second attack works when $d < N^{0.292}$. Both attacks are based on lattice based Coppersmith's method to solve modular equations. Durfee and Nguyen (Asiacrypt 2000) extended the attack to a variant of RSA where prime factors are not the same sizes. However, the attack extended only the first attack of the Boneh-Durfee. Hence, an open problem remains, i.e., if the Boneh-Durfee second attack can be extended to unbalanced RSA.**

**In this paper, we propose a desired attack that extended the Boneh-Durfee second attack. Our proposed attack fully improves the Durfee-Nguyen attack for all size of prime factors. The improvement stems from our technical lattice construction. Although Durfee and Nguyen only analyzed lattices whose basis matrices are triangular, we analyze broader classes of lattices that contain non-triangular basis matrices. The analysis can be performed by using the unravelled linearization proposed by Herrmann and May (Asiacrypt 2009) and the transformation on the Boneh-Durfee lattices proposed by Takayasu and Kunihiro (PKC 2016). As a result, we can exploit useful algebraic structure compared with the Durfee-Nguyen.**

## I. Introduction

### A. Background

Since its invention, RSA [23] has been widely used and numerous papers have studied the security. Let $N = pq$ be a public RSA modulus where $p$ and $q$ are distinct prime factors. Basically, the prime factors are the same bit sizes. Let $e$ and $d$ be a public and a secret exponent, respectively where

$$ed = 1 + \ell(p-1)(q-1)$$

with some integer $\ell$. For decrypting a ciphertext $c$ or signing a signature for a message $m$, $c^d \mod N$ and $m^d \mod N$ should be computed, respectively where the computational cost is $O(\log d \log^2 N)$. A simple solution to reduce the computational cost is a small secret exponent RSA, however, Wiener [31] revealed that too small secret exponent, i.e., $d < N^{0.25}$, discloses the factorization of $N$.

Boneh and Durfee (Eurocrypt 1999) [4] revisited the attack by using lattice based Coppersmith's method [5], [12]. The method can solve a modular equation when the absolute value of the root is sufficiently small. To factorize the RSA modulus $N$, Boneh and Durfee solved the following modular equation:

$$1 + x(A + y) = 0 \pmod{e}$$

where $A = N + 1$ and the root is $(x, y) = (\ell, -(p+q))$. At first, they propose an attack that works when

$$d < N^{(7-2\sqrt{7})/6} = N^{0.284\cdots}$$

that improved Wiener's bound [31]. In the same work, they further improved the bound to

$$d < N^{1-1/\sqrt{2}} = N^{0.292\cdots}$$

by exploiting appropriate sublattices. Although they claimed that the bound may be improved to $d < N^{0.5}$, any subsequent works cannot obtain better bounds, e.g., [2], [17]. Moreover, Aono et al. [1] showed some evidence for the optimality of the Boneh-Durfee bound. Since the attack is one of the most famous attacks on RSA, numerous papers study variants of the attack, e.g., attacks on (Multi-Prime) RSA with partial information of prime factors [19], [27], [30], [32], attacks on RSA with a modulus $N = p^r q$ [13], [29], attacks on multi exponent pairs RSA [26], partial key exposure extensions [3], [9], [28], and some other generalizations [15], [16].

Durfee and Nguyen (Asiacrypt 2000) [8] studied a small secret exponent attack on RSA where the prime factors $p$ and $q$ are unbalanced. A straightforward extension of the Boneh-Durfee attack degrades for unbalanced prime factors since the absolute value of $y = -(p+q)$ become large. Then only smaller secret exponent can be captured by the attack. To factorize RSA modulus $N$, Durfee and Nguyen solved the following modular equation:

$$1 + x(A + y_1 + y_2) = 0 \pmod{e}$$

where the root is $(x, y_1, y_2) = (\ell, -p, -q)$. Although there are three variables, the equation is essentially a bivariate equation as the Boneh-Durfee since the relation $y_1 y_2 = N$, which is called the Durfee-Nguyen technique, can be used. The division of $p$ and $q$ to two variables offers useful information and the straightforward extension of Boneh-Durfee can be improved. Indeed, the attack breaks the small secret exponent

RSA design proposed by Sun et al. [24]. However, the Durfee-Nguyen attacks have an obvious drawback in the sense that the attack do not cover the Boneh-Durfee stronger bound, i.e., $d < N^{0.292}$. When the prime factors become balanced, the Durfee-Nguyen attack becomes the same as the Boneh-Durfee weaker bound, i.e., $d < N^{0.284}$. Hence, to improve the attack that covers the stronger bound remains as an interesting open problem.

### B. Our Contribution

In this paper, we propose an improved small secret exponent attack on RSA for unbalanced prime factors. Although we solve the same modular equation as the Durfee-Nguyen, our better lattice construction improves the attack. Our attack solves the above open problem; when the prime factors become balanced, our proposed attack becomes the same as the stronger bound, i.e., $d < N^{0.292}$. Moreover, our attack is better than the Durfee-Nugyen attack for arbitrary sizes of prime factors $p$ and $q$.

### C. Key Technique

The hardness to extend the stronger Boneh-Durfee attack stems from its involved proof. To obtain the stronger bound, we should bound a determinant of lattice where the basis matrix is not triangular. Since Durfee and Nguyen only analyzed triangular basis matrices, their attack only covered the weaker Boneh-Durfee bound. Our first key technique is the *unravelled linearization* proposed by Herrmann and May (Asiacrypt 2009) [10]. The technique transform non-triangular basis matrices to be triangular and offers simple analyses. Indeed, Herrmann and May (PKC 2010) [11] made use of the technique and gave an elementary proof of the Boneh-Durfee stronger attack.

Since Durfee and Nguyen solved a slightly different equation from Boneh and Durfee, it is not trivial to apply Herrmann and May's unravelled linearization to the equation. For the purpose, our second key technique is the Takayasu-Kunihiro transformation (PKC 2016) [29]. The paper studied the security of RSA with a modulus $N = p^r q$ and used the same modular equation as Durfee and Nguyen. Their transformation converted the Boneh-Durfee matrix to obtain the stronger bound to an analogous matrix for the Durfee-Nguyen equation. More concretely, they used unravelled linearization and transform the non-triangular basis matrix for the Durfee-Nguyen equation to triangular.

Although the Takayasu-Kunihiro transformation enables us to analyze the Durfee-Nguyen equation with non-triangular basis matrix, it is not straightforward to obtain the best result. The hardness stems from the unbalanced prime factors $p$ and $q$. Although Takayasu and Kunihiro analyzed the same equation with non-triangular basis matrices, they only focus on balanced prime factors. To maximize the solvable root bounds, we make use of the notion of *helpful polynomials*. The notion was defined by May [21]. Several subsequent works [19], [25], [28] made use of the notion and proposed improved attacks. In short, helpful polynomials tell us an appropriate lattice construction that take into account each root size. We also make use of the notion and show better lattice constructions.

TABLE I
COMPARISON FOR THE ATTACK CONDITIONS BETWEEN OUR PROPOSED ATTACK AND THE DURFEE-NGUYEN [8]

| $\gamma = \log_N p$ | Ours | [8] |
|---|---|---|
| 0.5 | 0.292 | 0.284 |
| 0.6 | 0.307 | 0.296 |
| 0.7 | 0.351 | 0.334 |
| 0.8 | 0.425 | 0.406 |
| 0.9 | 0.552 | 0.539 |

## II. PRELIMINARIES

In this section, we introduce the LLL lattice reduction algorithm and Howgrave-Graham's lemma where they are fundamental tools for lattice based Coppersmith's method.

### A. LLL Algorithm

Given linearly independent $m$-dimensional $n$ vectors $\boldsymbol{b}_1, \ldots, \boldsymbol{b}_n \in \mathbb{R}^m$, a lattice spanned by the basis vectors are defined as integer linear combinations of the vectors;

$$L(\boldsymbol{b}_1, \ldots, \boldsymbol{b}_n) := \left\{ \sum_{j=1}^{n} c_j \boldsymbol{b}_j \mid c_j \in \mathbb{Z} \text{ for all } j = 1, 2, \ldots, n \right\}.$$

Matrix representations of bases are also used where basis matrices of lattices are defined as $n \times m$ matrices each of whose rows consists of the basis vector $\boldsymbol{b}_1, \ldots, \boldsymbol{b}_n$. Lattices spanned by basis matrices $\boldsymbol{B}$ are denoted as $L(\boldsymbol{B})$. The values $n$ (resp. $m$) represent a rank (resp. a dimension) of a lattice. When $n = m$, we call lattices full-rank. A parallelepiped of a lattice is defined as

$$\mathcal{P}(\boldsymbol{B}) := \{\boldsymbol{c}\boldsymbol{B} : \boldsymbol{c} \in \mathbb{R}^n, 0 < c_j \leq 1 \text{ for all } j = 1, 2, \ldots, n\}.$$

The determinant of a lattice $\det(L(\boldsymbol{B}))$ is defined as the $n$-dimensional volume of the parallelepiped. In general, the determinant can be calculated as

$$\det(L(\boldsymbol{B})) = \sqrt{\det(\boldsymbol{B}\boldsymbol{B}^\mathsf{T})}$$

where $\boldsymbol{B}^\mathsf{T}$ represents a transpose of $\boldsymbol{B}$. For full-rank lattices, we can compute the determinant as

$$\det(L(\boldsymbol{B})) = |\det(\boldsymbol{B})|.$$

Lattices are used in many ways in the context of cryptanalysis. See [6], [7], [20], [21], [22] for detailed information. For the cryptanalyses, finding short lattice vectors is essential. In this paper, we introduce the celebrated LLL algorithm [18] as other previous works. In 1982, Lenstra, Lenstra, and Lovász proposed a lattice reduction algorithm that finds short lattice vectors in polynomial time.

*Propostition 1 (LLL algorithm [18]):* Given $m$-dimensional basis vectors $\boldsymbol{b}_1, \ldots, \boldsymbol{b}_n$, the LLL algorithm finds short lattice vectors $\boldsymbol{b}'_1$ and $\boldsymbol{b}'_2$ that satisfy

$$\|\boldsymbol{b}'_1\| \leq 2^{(n-1)/4}(\det(L(\boldsymbol{B})))^{1/n},$$

$$\|\boldsymbol{b}_2'\| \leq 2^{n/2}(\det(L(\boldsymbol{B})))^{1/(n-1)},$$

in polynomial time in $n, m$, and input length.

### B. Howgrave-Graham's Lemma

To solve modular equations $h(x,y) = 0 \mod e$ whose root is $(x,y) = (\tilde{x},\tilde{y})$ is difficult for the existence of the modulus $e$. Moreover, although the equation is bivariate, there is only one equation. However, Coppersmith (Eurocrypt 1996) [5] proposed a novel method to solve the equation. The method works when the absolute values of desired root is sufficiently small. In this paper, we introduce Howgrave-Graham's reformulation for the method. Let $\|h(x,y)\| := \sqrt{\sum h_{i,j}^2}$ be a norm of a bivariate polynomial $h(x,y) := \sum h_{i,j}x^iy^j$. Howgrave-Graham [12] revealed that if two small norm polynomials that have the same root as $h(x,y) \pmod e$ can be found, then the root can be recovered.

*Lemma 1 (Howgrave-Graham's Lemma [12]):* Given positive integers $X, Y$, and $m$, if a polynomial $h'(x,y)$ that has at most $n$ monomials satisfies following two conditions,
1. $h'(\tilde{x},\tilde{y}) = 0 \pmod{e^m}$ where $|\tilde{x}| < X$ and $|\tilde{y}| < Y$,
2. $\|h'(x,y)\| < e^m/\sqrt{n}$,

then $h'(\tilde{x},\tilde{y}) = 0$ holds over the integers.
Since polynomials that satisfy Howgrave-Graham's lemma share the common root over the integers, the root can be recovered by using standard operations, e.g., computing Gröbner bases or resultants. Hence, what we should do is finding low norm polynomials that share the same root modulo $e^m$. Coppersmith's method makes use of the LLL algorithm for the operation. More concretely, we construct a lattice whose basis vectors consist of coefficients of polynomials that share the same root modulo $e^m$. We apply the LLL algorithm to the lattice basis. If polynomials that are derived from LLL output vectors satisfy Howgrave-Graham's lemma, the root can be recovered.

We should note that the above method requires a heuristic argument since there are no assurance that the polynomials obtained by the LLL algorithm will be algebraically independent. In this paper, we assume the fact as previous works [4], [8] since there exist few negative reports of the assumption. Moreover, lattices that we use in this paper are sublattices of the lattices that have been previously used. Hence, validities of previous algorithms justify the validity of our algorithm.

## III. Proposed Attack for $N^{1/2} \leq p < N^{2/3}$

Let $\gamma$ denote the size of the prime factor such that $N^\gamma < p \leq 2N^\gamma$ and $q \leq 2N^{1-\gamma}$ for $1/2 \leq \gamma < 1$. Let $\alpha$ and $\beta$ denote the size of public/secret exponent such that $e = N^\alpha$ and $d = N^\beta$, respectively. As we discussed in Section I, to factorize the RSA modulus $N$, we solve the following modular equation:

$$f(x,y_1,y_2) = 1 + x(A + y_1 + y_2) \pmod e = 0$$

where $A = N + 1$. The polynomial $f(x,y_1,y_2)$ has a root $(x,y_1,y_2) = (\ell,-p,-q)$. The absolute values of the root is bounded above by $X := N^{\alpha+\beta-1}, Y_1 := N^\gamma, Y_2 := N^{1-\gamma}$, respectively within constant factors. Notice that we can use an algebraic information $y_1y_2 = N$.

To solve the modular equation $f(x,y_1,y_2) = 0$, we use the following shift-polynomials:

$$\begin{aligned} g^x_{[u,i,v]}(x,y_1,y_2) &= x^iy_2^vf^u(x,y_1,y_2)e^{m-u},\\ g^{y_1}_{[u,k_1]}(x,y_1,y_2) &= y_1^{k_1}f^u(x,y_1,y_2)e^{m-u},\\ g^{y_2}_{[u,k_2]}(x,y_1,y_2) &= y_2^{1+k_2}f^u(x,y_1,y_2)e^{m-u}, \end{aligned}$$

with a non-negative integer $m$. For non-negative integers $u, i, v, k_1$, and $k_2$, all these shift-polynomials modulo $e^m$ have the root $(x,y_1,y_2) = (\ell,-p,-q)$ that is the same as $f(x,y_1,y_2)$. The other shift-polynomial $g^x_{[u,i,v]}(x,y_1,y_2)$ is a base polynomial that was also used by Durfee and Nguyen. The shift-polynomials $g^{y_1}_{[u,k]}(x,y_1,y_2)$ and $g^{y_2}_{[u,k]}(x,y_1,y_2)$ are helper polynomials that maximize the solvable root bounds. These shift-polynomials were not used by Durfee-Nguyen and they enable us to obtain better results.

We define the following sets of indices:

$$\begin{aligned} &\mathcal{I}_x \Leftrightarrow u = 0,1,\ldots,m; i = 0,1,\ldots,m-u; v = 0,1,\\ &\mathcal{I}_{y_1} \Leftrightarrow u = 0,1,\ldots,m; k_1 = 1,2,\ldots,\lfloor\frac{1-\beta-\gamma}{\gamma}u\rfloor,\\ &\mathcal{I}_{y_2} \Leftrightarrow u = 0,1,\ldots,m;\\ &\qquad k_2 = 1,2,\ldots,\max\left\{\lfloor\frac{\gamma-\beta}{1-\gamma}u-1\rfloor, 0\right\}. \end{aligned}$$

Then we construct a basis matrix $\boldsymbol{B}$ whose rows consist of the coefficients of $g^x_{[u,i,v]}(xX,y_1Y_1,y_2Y_2), g^{y_1}_{[u,k]}(xX,y_1Y_1,y_2Y_2)$, and $g^{y_2}_{[u,k]}(xX,y_1Y_1,y_2Y_2)$ with indices in $\mathcal{I}_x, \mathcal{I}_{y_1}$, and $\mathcal{I}_{y_2}$, respectively. As the same way, all lattice points in $L(\boldsymbol{B})$ generate new polynomials that are integer linear combinations of these shift-polynomials. Since all these shift-polynomials modulo $e^m$ have the root $(x,y_1,y_2) = (\ell,-p,-q)$, polynomials that are generated by arbitrary points in $L(\boldsymbol{B})$ have the same root modulo $e^m$.

Our improvement stems from the above collection of helper polynomials $g^{y_1}_{[u,k_1]}(x,y_1,y_2)$ and $g^{y_2}_{[u,k_2]}(x,y_1,y_2)$. More concretely, in addition to base polynomials $g^x_{[u,i,0]}(x,y_1,y_2)$, Durfee-Nguyen collects some helper polynomials, however, these helper polynomials are not always helpful polynomials. However, in addition to the same base polynomials, we only collect helpful polynomials. To show the fact, we use unravelled linearization [10], [11] and the Takayasu-Kunihiro transformation [29]. By combining these techniques, the above basis matrix $\boldsymbol{B}$ becomes triangular with diagonals

- $X^{u+i}Y_1^ue^{m-u}$ for $g^x_{[u,i,0]}(x,y_1,y_2)$,
- $X^{u+i}Y_2^{1+u}e^{m-u}$ for $g^x_{[u,i,1]}(x,y_1,y_2)$,
- $X^uY_1^{u+k_1}e^{m-u}$ for $g^{y_1}_{[u,k_1]}(x,y_1,y_2)$,
- $X^uY_1^{1+u+k_2}e^{m-u}$ for $g^{y_2}_{[u,k_2]}(x,y_1,y_2)$.

Then the shift-polynomials $g^{y_1}_{[u,k_1]}(x,y_1,y_2)$ are helpful if

$$\begin{aligned} X^uY_1^{u+k_1}e^{m-u} \leq e^m &\Leftrightarrow \beta u + \gamma(u+k_1) \leq u\\ &\Leftrightarrow k_1 \leq \frac{1-\beta-\gamma}{\gamma}u \end{aligned}$$

whereas the shift-polynomials $g^{y_2}_{[u,k_2]}(x, y_1, y_2)$ are helpful if

$$X^u Y_2^{1+u+k_2} e^{m-u} \le e^m \Leftrightarrow \beta u + (1-\gamma)(1+u+k_2) \le u$$
$$\Leftrightarrow k_2 \le \frac{\gamma-\beta}{1-\gamma} u - 1.$$

Hence, we defined the above sets of indices $\mathcal{I}_x, \mathcal{I}_{y_1}$, and $\mathcal{I}_{y_2}$.

In this section, we focus on the case for small $\gamma$, i.e., $\gamma < 1-\beta$, since the set of indices $\mathcal{I}_{y_1}$ becomes empty otherwise. The dimension $n$ and the determinant of the lattice $\det(\boldsymbol{B}) = X^{s_X} Y_1^{s_{Y_1}} Y_2^{s_{Y_2}} e^{s_e}$ can be computed as the following:

$$\begin{aligned} n &= 2\sum_{u=0}^{m}\sum_{i=0}^{m-u} 1 + \sum_{u=0}^{m}\sum_{k_1=1}^{\lfloor \frac{1-\beta-\gamma}{\gamma} u\rfloor} 1 + \sum_{u=0}^{m}\sum_{k_2=1}^{\max\{\lfloor \frac{\gamma-\beta}{1-\gamma}u-1\rfloor, 0\}} 1 \\ &= \frac{1-\beta}{2\gamma(1-\gamma)} m^2 + o(m^2), \end{aligned}$$

$$\begin{aligned} s_X &= 2\sum_{u=0}^{m}\sum_{i=0}^{m-u}(u+i) + \sum_{u=0}^{m}\sum_{k_1=1}^{\lfloor \frac{1-\beta-\gamma}{\gamma} u\rfloor} u \\ &\quad + \sum_{u=0}^{m}\sum_{k_2=1}^{\max\{\lfloor \frac{\gamma-\beta}{1-\gamma}u-1\rfloor, 0\}} u = \frac{1-\beta}{3\gamma(1-\gamma)} m^3 + o(m^3), \end{aligned}$$

$$\begin{aligned} s_{Y_1} &= \sum_{u=0}^{m}\sum_{i=0}^{m-u} u + \sum_{u=0}^{m}\sum_{k_1=1}^{\lfloor \frac{1-\beta-\gamma}{\gamma} u\rfloor} (u+k_1) \\ &= \frac{(1-\beta)^2}{6\gamma^2} m^3 + o(m^3), \end{aligned}$$

$$\begin{aligned} s_{Y_2} &= \sum_{u=0}^{m}\sum_{i=0}^{m-u}(1+u) + \sum_{u=0}^{m}\sum_{k_2=1}^{\max\{\lfloor \frac{\gamma-\beta}{1-\gamma}u-1\rfloor, 0\}} (1+u+k_2) \\ &= \frac{(1-\beta)^2}{6(1-\gamma)^2} m^3 + o(m^3), \end{aligned}$$

$$\begin{aligned} s_e &= 2\sum_{u=0}^{m}\sum_{i=0}^{m-u}(m-u) + \sum_{u=0}^{m}\sum_{k_1=1}^{\lfloor \frac{1-\beta-\gamma}{\gamma} u\rfloor} (m-u) \\ &\quad + \sum_{u=0}^{m}\sum_{k_2=1}^{\max\{\lfloor \frac{\gamma-\beta}{1-\gamma}u-1\rfloor, 0\}} (m-u) \\ &= \left(\frac{1}{3} + \frac{1-\beta}{6\gamma(1-\gamma)}\right) m^3 + o(m^3). \end{aligned}$$

Ignoring low order terms of $m$, polynomials that are generated by the LLL output vectors satisfy Howgrave-Graham's lemma if $\det(\boldsymbol{B})^{1/n} < e^m$, i.e.,

$$\frac{\beta(1-\beta)}{3\gamma(1-\gamma)} + \frac{(1-\beta)^2}{6\gamma(1-\gamma)} + \frac{1}{3} - \frac{1-\beta}{3\gamma(1-\gamma)} < 0$$

where the inequality results in

$$\beta < 1 - \sqrt{2\gamma(1-\gamma)}.$$

When $\gamma = 1/2$, the bound corresponds to the stronger Boneh-Durfee bound, i.e., $\beta < 1 - 1/\sqrt{2}$.

As we claimed, the above analysis is valid only when

$$\gamma < 1 - \beta \Leftrightarrow \gamma < \frac{2}{3}.$$

## IV. Proposed Attack for $N^{2/3} \le p < N$

In this section, we analyze the other case; large $\gamma$ such that $\gamma \ge 1-\beta$. The set of indices $\mathcal{I}_{y_1}$ is empty. Hence, we construct a basis matrix $\boldsymbol{B}$ whose rows consist of the coefficients of $g^{x}_{[u,i,v]}(xX, y_1Y_1, y_2Y_2)$ and $g^{y_2}_{[u,k]}(xX, y_1Y_1, y_2Y_2)$ with indices in $\mathcal{I}_x$ and $\mathcal{I}_{y_2}$, respectively.

Then the dimension $n$ and the determinant of the lattice $\det(\boldsymbol{B}) = X^{s_X} Y_1^{s_{Y_1}} Y_2^{s_{Y_2}} e^{s_e}$ can be computed as the following:

$$\begin{aligned} n &= 2\sum_{u=0}^{m}\sum_{i=0}^{m-u} 1 + \sum_{u=0}^{m}\sum_{k_2=1}^{\max\{\lfloor \frac{\gamma-\beta}{1-\gamma}u-1\rfloor, 0\}} 1 \\ &= \left(\frac{1}{2} + \frac{1-\beta}{2(1-\gamma)}\right) m^2 + o(m^2), \end{aligned}$$

$$\begin{aligned} s_X &= 2\sum_{u=0}^{m}\sum_{i=0}^{m-u}(u+i) + \sum_{u=0}^{m}\sum_{k_2=1}^{\max\{\lfloor \frac{\gamma-\beta}{1-\gamma}u-1\rfloor, 0\}} u \\ &= \left(\frac{1}{3} + \frac{1-\beta}{3(1-\gamma)}\right) m^3 + o(m^3), \end{aligned}$$

$$s_{Y_1} = \sum_{u=0}^{m}\sum_{i=0}^{m-u} u = \frac{1}{6} m^3 + o(m^3),$$

$$\begin{aligned} s_{Y_2} &= \sum_{u=0}^{m}\sum_{i=0}^{m-u}(1+u) + \sum_{u=0}^{m}\sum_{k_2=1}^{\max\{\lfloor \frac{\gamma-\beta}{1-\gamma}u-1\rfloor, 0\}} (1+u+k_2) \\ &= \frac{(1-\beta)^2}{6(1-\gamma)^2} m^3 + o(m^3), \end{aligned}$$

$$\begin{aligned} s_e &= 2\sum_{u=0}^{m}\sum_{i=0}^{m-u}(m-u) + \sum_{u=0}^{m}\sum_{k_2=1}^{\max\{\lfloor \frac{\gamma-\beta}{1-\gamma}u-1\rfloor, 0\}} (m-u) \\ &= \left(\frac{1}{2} + \frac{1-\beta}{6(1-\gamma)}\right) m^3 + o(m^3). \end{aligned}$$

Ignoring low order terms of $m$, polynomials that are generated by the LLL output vectors satisfy Howgrave-Graham's lemma if $\det(\boldsymbol{B})^{1/n} < e^m$, i.e.,

$$\beta\left(\frac{1}{3} + \frac{1-\beta}{3(1-\gamma)}\right) + \frac{\gamma}{6} + \frac{(1-\beta)^2}{6(1-\gamma)} - \frac{1-\beta}{3(1-\gamma)} < 0$$

where the inequality results in

$$\beta < 2 - \gamma - \sqrt{3(1-\gamma)}.$$

## V. Conclusion

In this paper, we studied a small secret exponent attack on RSA where the prime factors of RSA modulus is unbalanced. As opposed to a previous attack proposed by Durfee and Nguyen [8], we successfully extended the stronger Boneh-Durfee attack [4] that captures a balanced RSA. As a result, our attack improves the Durfee-Nguyen attack.

## Acknowledgment

The first author is supported by a JSPS Fellowship for Young Scientists. This research was supported by CREST, JST, and JSPS KAKENHI Grant Number 14J08237, 16H02780, and 25280001.

## References


[1] Y. Aono, M. Agrawal, T. Satoh, and O. Watanabe, "On the optimality of lattices for the Coppersmith technique," Proc. ACISP 2012, LNCS 7372, pp. 376–389, 2012. IACR ePrint 2012/108, 2012.

[2] J. Blömer and A. May, "Low secret exponent RSA revisited," Proc. Crypto 2003, LNCS 2729, pp. 27–43, Springer, Heidelberg, 2003.

[3] J. Blömer and A. May, "New partial key exposure attacks on RSA," Proc. Crypto 2003, LNCS 2729, pp. 27–43, Springer, Heidelberg, 2003.

[4] D. Boneh and G. Durfee, "Cryptanalysis of RSA with private key $d$ less than $N^{0.292}$," IEEE Trans. Inf. Theory, vol. 46, no. 4, pp. 1339–1349, 2000. Firstly appeared in Eurocrypt 1999, volume 1592 of Lecture Notes in Computer Science, pp. 1–11, Springer, 1999.

[5] D. Coppersmith, "Finding a small root of a univariate modular equation," Proc. Eurocrypt 1996, LNCS 1070, pp. 155–165, Springer, Heidelberg, 1996.

[6] D. Coppersmith, "Small solutions to polynomial equations, and low exponent RSA vulnerabilities," J. Cryptology, vol. 10, no. 4, pp. 233–260, 1997.

[7] D. Coppersmith, "Finding small solutions to small degree polynomials," Proc. CaLC 2001, LNCS 2146, pp. 20–31, Springer, Heidelberg, 2001.

[8] G. Durfee and P. -Q. Nguyen, "Cryptanalysis of the RSA schemes with short secret exponent from Asiacrypt '99," Proc. Asiacrypt 2000, LNCS 1976, pp. 14–29, Springer, Heidelberg, 2000.

[9] M. Ernst, E. Jochemsz, A. May and B. Weger, "Partial key exposure attacks on RSA up to full size exponents," Proc. Eurocrypt 2005, LNCS 3494, pp. 371–386, Springer, Heidelberg, 2005.

[10] M. Herrmann and A. May, "Attacking power generators using unravelled linearization: When do we output too much?," Proc. Asiacrypt 2009, LNCS 5912, pp. 487–504, Springer, Heidelberg, 2009.

[11] M. Herrmann and A. May, "Maximizing small root bounds by linearization and applications to small secret exponent RSA," Proc. PKC 2010, LNCS 6056, pp. 53–69, Springer, Heidelberg, 2010.

[12] N. Howgrave-Graham, "Finding small roots of univariate modular equations revisited," Proc. Cryptography and Coding, LNCS 1355, pp. 1331–142, 1997.

[13] K. Itoh, N. Kunihiro and K. Kurosawa, "Small secret key attack on a variant of RSA (due to Takagi)," Proc. CT-RSA 2008, LNCS 4964, pp. 387–406, Springer, 2008. See also [14].

[14] K. Itoh, N. Kunihiro and K. Kurosawa, "Small secret key attack on a Takagi's variant of RSA," IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, vol. E92-A, No. 1, pp. 33–41, 2008.

[15] N. Kunihiro, "Solving generalized the small inverse problem," IEICE Transactions 94-A, no. 6, pp. 1274–1284, 2011.

[16] N. Kunihiro, "On optimal bounds of the small inverse problem and approximate gcd problems with higher degree," Proc. ISC 2012, LNCS 7483, pp. 55–69, Springer, 2012.

[17] N. Kunihiro, N. Shinohara and T. Izu, "A unified framework for small secret exponent attack on RSA," IEICE Trans. on Fundamentals of Electronics, Communications and Computer Sciences, vol. E97-A, No. 6, pp. 1285–1295, 2014. Firstly appeared in Proc. SAC 2011, LNCS 7118, pp. 260–277, Springer-Verlag, 2011.

[18] A. K. Lenstra, H. W. Lenstra Jr. and L. Lovász, "Factoring polynomials with rational coefficients," Mathematische Annalen 261, pp.515–534, 1982.

[19] Y. Lu, R. Zhang, L. Peng, and D. Lin, "Solving linear equations modulo unknown divisors: Revisited," Proc. Asiacrypt 2015, LNCS 9452, pp. 189–213, Springer, Heidelberg, 2015.

[20] A. May, "New RSA vulnerabilities using lattice reduction methods," PhD thesis, University of Paderborn, 2003.

[21] A. May, "Using LLL-reduction for solving RSA and factorization problems: A survey," Available from http://www.cits.rub.de/permonen/may.html, 2010.

[22] P. Q. Nguyen and J. Stern, "The two faces of lattices in cryptology," Proc. CaLC 2001, LNCS 2146, pp. 146–180, Springer, Heidelberg, 2001.

[23] R. L. Rivest, A. Shamir and L. M. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," Communications of the ACM, 21 (2), pp. 120–126, 1978.

[24] H. -M. Sun, W. -C. Yang, and C. -S. Laih, "On the design of RSA with short secret exponent," Proc. Asiacrypt 1999, volume 1716 of Lecture Notes in Computer Science, pp. 150–164, Springer, 1999.

[25] A. Takayasu and N. Kunihiro, "Better lattice constructions for solving multivariate linear equations modulo unknown divisors," IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, Vol. E97-A, No. 6, pp. 1259–1272, 2014. Firstly appeared in ACISP 2013, volume 7959 of Lecture Notes in Computer Science, pp. 118–135, Springer, 2013.

[26] A. Takayasu and N. Kunihiro, "Cryptanalysis of RSA with multiple small secret exponents," Proc. ACISP 2014, LNCS 8544, pp. 176–191, Springer, 2014.

[27] A. Takayasu and N. Kunihiro, "General bounds for small inverse problems and its applications to multi-prime RSA," Proc. ICISC 2014, LNCS 8949, pp. 3–17, Springer, 2014.

[28] A. Takayasu and N. Kunihiro, "Partial key exposure attacks on RSA: Achieving the Boneh-Durfee bound," Proc. SAC 2014, volume 8781 of Lecture Notes in Computer Science, Springer, 2014.

[29] A. Takayasu and N. Kunihiro, "How to generalize RSA cryptanalyses," Proc. PKC 2016, volume of Lecture Notes in Computer Science, Springer, 2016.

[30] B. de Weger, "Cryptanalysis of RSA with small prime difference, applicable algebra in engineering," Communication and Computing 13, pp. 17–28, 2002.

[31] M. J. Wiener, "Cryptanalysis of short RSA secret exponents," IEEE Trans. inf. theory, vol. 36, no. 3, pp. 553–558, 1990. Firstly appeared in Eurocrypt 1989, volume 434 of Lecture Notes in Computer Science, page 372, Springer, 1989.

[32] H. Zhang and T. Takagi, "Improved attacks on multi-prime RSA with small prime difference," IEICE Trans. VolE97-A, No.7, pp. 1533–1541, 2014.