Cryptanalysis of RSA with Multiple Small Secret Exponents

Atsushi Takayasu and Noboru Kunihiro

The University of Tokyo, Japan
{a-takayasu@it.,kunihiro@}k.u-tokyo.ac.jp

Abstract. In this paper, we study the security of RSA when there are multiple public/secret exponents $(e_1, d_1), \ldots, (e_n, d_n)$ with the same public modulus N. We assume that all secret exponents are smaller than N^β. When $n = 1$, Boneh and Durfee proposed a polynomial time algorithm to factor the public modulus N. The algorithm works provided that $\beta < 1 - 1/\sqrt{2}$. So far, several generalizations of the attacks for arbitrary n have been proposed. However, these attacks do not achieve Boneh and Durfee's bound for $n = 1$. In this paper, we propose an algorithm which is the exact generalization of Boneh and Durfee's algorithm. Our algorithm works when $\beta < 1 - \sqrt{2/(3n+1)}$. Our bound is better than all previous results for all $n \geq 2$. We construct the lattices by collecting as many helpful polynomials as possible. The collections reduce the volume of the lattices and enable us to improve the bound.

Keywords: Cryptanalysis, RSA, Lattices, Coppersmith's method.

1 Introduction

1.1 Background

Small Secret Exponent RSA. Small secret exponent RSA is efficient for its low cost decryption and signature generation, but is known to be insecure. We assume that decryption exponent is smaller than N^β. Wiener [Wie90] proposed the polynomial time algorithm to factor public modulus N. The algorithm works when $\beta < 0.25$. The algorithm is constructed by computing the diophantine approximation of rational number.

Boneh and Durfee [BD00] revisited the Wiener's attack. They constucted improved algorithm by using lattice based method to solve modular equations proposed by Coppersmith [Cop96a]. At first, they constructed the lattices which provide Wiener's bound, $\beta < 0.25$. They improved the bound to $\beta < (7 - 2\sqrt{7})/6 = 0.28474\cdots$ by adding some extra polynomials in the lattice bases. Finally, they achieved the stronger bound $\beta < 1 - 1/\sqrt{2} = 0.29289\cdots$ by extracting sublattices from the previous lattices. Though several papers revisited the work [BM01, HM10, Kun11, KSI11, Kun12], none of them improved Boneh and Durfee's stronger bound. Boneh and Durfee's attack has also been applied to the variants of RSA [DN00, IKK08a, May04].

W. Susilo and Y. Mu (Eds.): ACISP 2014, LNCS 8544, pp. 176–191, 2014.

Multiple Small Secret Exponents RSA. Generalizations of small secret exponent attack on RSA have also been considered when there are multiple public/secret key pairs $(e_1, d_1), \ldots, (e_n, d_n)$ for the same public modulus N. All secret keys $d_1, \ldots, d_n$ are smaller than N^β. Howgrave-Graham and Seifert [HS99] generalized Wiener's attack and achieved the bound

$$\beta < \frac{(2n+1)\cdot 2^n - (2n+1)\binom{n}{n/2}}{(2n-2)\cdot 2^n + (4n+2)\binom{n}{n/2}} \text{ when } n \text{ is even,}$$
$$\beta < \frac{(2n+1)\cdot 2^n - 4n\binom{n-1}{(n-1)/2}}{(2n-2)\cdot 2^n + 8n\binom{n-1}{(n-1)/2}} \text{ when } n \text{ is odd.}$$

The bound converges to full size secret exponents, $\beta = 1$.

Sarkar and Maitra [SM10b] used the Coppersmith's method to find small roots of polynomials over the integers [Cop96b] and improved the bound. They constructed the lattices based on Jochemsz and May's strategy [JM06]. The algorithm works when

$$\beta < \frac{3}{4} - \frac{1}{n+1}.$$

The algorithm improved Howgrave-Graham and Seifert's bound for $2 \leq n \leq 42$. In the same work [SM10b], Sarkar and Maitra achieved ad-hoc improvement, $\beta < 0.422$ for $n = 2$. See also [SM10a].

Aono [Aon13] used the Coppersmith's method to solve modular equations [Cop96a] and improved the bound. Aono's algorithm works when

$$\beta < \frac{3}{4} - \frac{2}{3n+1}.$$

The algorithm improved Sarkar and Maitra's algorithm. The bound is better than Howgrave-Graham and Seifert's bound for $2 \leq n \leq 46$. In the same work [Aon13], Aono heurisically considered ad-hoc improvement for $n \geq 3$, though no exact conditions are given.

All these algorithms run in polynomial time in $\log N$ and exponential in n. It is clear that these algorithms have the room to be improved. All algorithms only achieve Winer's bound [Wie90] for $n = 1$. In addition, we should consider the case when there are infinitely many public/secret key pairs. In this case, Aono [Aon13] counted the number of solutions and claimed that public modulus N can be factored with full size secret exponents. Howgrave-Graham and Seifert's bound [HS99] converges to $\beta < 1$. However, Sarkar and Maitra's bound [SM10b] and Aono's bound [Aon13] converge to $\beta < 3/4$. Therefore, we should construct the algorithm which achieves Boneh and Durfee's bound [BD00] and converges to $\beta < 1$.

Lattice Constructions for the Coppersmith's Methods. At Eurocrypt 1996, Coppersmith introduced celebrated lattice based methods. One method is to solve modular univariate equations which have small solutions [Cop96a].

The other method is to find small roots of bivariate polynomials over the integers [Cop96b]. Both methods can be heuristically generalized to more multivariate cases with reasonable assumption. The former method was reformulated by Howgrave-Graham [How97], and the latter method was reformulated by Coron [Cor04, Cor07]. The Coppersmith's methods have been used to reveal the vulnerabilites of several cryptosystems, especially RSA cryptosystem [Cop97, Cop01, NS01, May10].

The Coppersmith's methods have improved several algorithms which compute diophantine approximation of rational numbers. Boneh and Durfee [BD00] improved Winer's small secret exponent attack on RSA [Wie90]. Howgrave-Graham [How01] considered approximate common divisor problems and constructed two types of algorithms. The first algorithm computes diophantine approximation. The second algorithm uses the Coppersmith's method. Since the second algorithm is better than the first algorithm, Howgrave-Graham's results imply that the Coppersmith's method is superior to the other method. Therefore, Howgrave-Graham and Seifert's result [HS99] is expected to be improved by using the Coppersmith's method.

To maximize the solvable root bounds using the Coppersmith's methods, we should select appropriate lattice bases which reduce the volume. At Asiacrypt 2006, Jochemsz and May [JM06] proposed the strategy for lattice constructions. The strategy can automatically decide the selections of lattice bases. The strategy covers several former results [BD00, Weg02, May04, EJMW05], and later some algorithms [JM07] have been proposed based on the strategy including Sarkar and Maitra's work [SM10a, SM10b]. However, it is widely known that Jochemsz and May's strategy does not always select the appropriate lattice bases. In fact, for small secret exponent attacks on RSA, we only obtain Boneh and Durfee's weaker bound $\beta < (7 - 2\sqrt{7})/6$ based on the strategy. The strategy cannot tell us the selections of lattice bases which provide Boneh and Durfee's stronger bound [BD00]. Therefore, Sarkar and Maitra's results [SM10a, SM10b] are expected to be improved by selecting appropriate lattice bases.

For $n \geq 2$, Aono solved simultaneous modular equations. Each single equation is the same one which Boneh and Durfee [BD00] solve. Aono combined Boneh and Durfee's n lattices based on Minkowski sum. However, Aono used Boneh and Durfee's lattices which only achieve Wiener's bound $\beta < 0.25$. Therefore, it is clear that the algorithm cannot achieve Boneh and Durfee's stronger bound for $n = 1$ and is expected to be improved.

What makes the problems difficult is that we should change the selections of lattice bases with respect to the sizes of root bounds. Sarkar and Maitra's ad-hoc improvement [SM10b] for $n = 2$ is achieved based on the condition $\beta < 1/2$. They selected extra polynomials in the lattice bases to reduce the volume. Boneh and Durfee's improvement [BD00] from the Wiener's bound [Wie90] is also based on the condition $\beta < 1/2$ by adding extra polynomials. Conversely, though heuristic, Aono's ad-hoc improvement [Aon13] for $n \geq 3$ is based on the fact that $\beta > 1/2$. Aono claimed that some polynomials in the lattice bases should be eliminated to

reduce the volume. Therefore, we should work out the selections of lattice bases which take into account the sizes of root bounds in general.

Collecting Helpful Polynomials. Recently, Takayasu and Kunihiro [TK13] proposed simple and useful strategy for lattice constructions. In their strategy, the notion of *helpful polynomials* is essential. The notion was firstly noted by May [May10]. Helpful polynomials can reduce the volume of the lattices and contribute to the conditions for modular equations to be solved. If each polynomial is helpful or not is decided by comparing the sizes of diagonals and the size of modulus. Takayasu and Kunihiro claimed that as many helpful polynomials as possible should be selected, and as few unhelpful polynomials as possible should be selected in the lattice bases. Based on the strategy, they improved the algorithms to solve two forms of modular multivariate linear equations [HM08, CH12] when each root bound becomes extremely large or small.

1.2 Our Results

In this paper, we solve the same simultaneous modular equations as Aono [Aon13]. However, we change the selections of lattice bases and improve the previous bounds. Based on Takayasu and Kunihiro's strategy for lattice constructions [TK13], we reveal that there are some helpful polynomials which were not selected or there are some unhelpful polynomials which were selected in Aono's lattice bases. This analysis enables us to select as many helpful polynomials as possible and as few unhelpful polynomials as possible. Our algorithm works provided that

$$\beta < 1 - \sqrt{\frac{2}{3n+1}}.$$

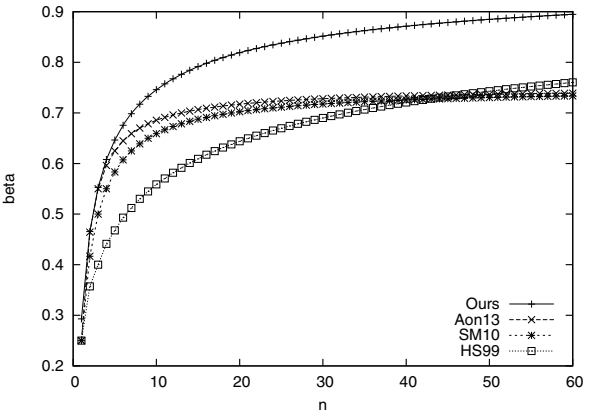

Fig. 1. The comparison of the recoverable sizes of secret exponents

Table 1. Numerical data for the recoverable sizes of secret exponents

n	Ours	[Aon13]	[SM10b]	[HS99]
1	0.292893219	0.25	0.25	0.25
2	0.465477516	0.464285714	0.416666667	0.357142857
3	0.552786405	0.55	0.5	0.4
4	0.60776773	0.596153846	0.55	0.441176471
5	0.646446609	0.625	0.583333333	0.467741935
6	0.675557158	0.644736842	0.607142857	0.493103448
7	0.698488655	0.659090909	0.625	0.512048193
8	0.717157288	0.67	0.638888889	0.530181087
9	0.732738758	0.678571429	0.65	0.544740024
10	0.745999746	0.685483871	0.659090909	0.55872622
⋮	⋮	⋮	⋮	⋮
101	0.918889289	0.743421053	0.740196078	0.805167829
102	0.919286569	0.743485342	0.740291262	0.80595288
103	0.919678067	0.743548387	0.740384615	0.806723605
104	0.920063923	0.743610224	0.74047619	0.807488696
105	0.920444272	0.743670886	0.740566038	0.808240085
106	0.920819242	0.743730408	0.740654206	0.808986071
107	0.921188959	0.74378882	0.740740741	0.809718942
108	0.921553546	0.743846154	0.740825688	0.810446627
109	0.921913119	0.743902439	0.740909091	0.811161748
110	0.922267793	0.743957704	0.740990991	0.811871889

Our algorithm achieves Boneh and Durfee's bound $\beta < 1 - 1/\sqrt{2}$ for $n = 1$, and converges to $\beta < 1$ with infinitely many exponents. The bound[1] is better than all known algorithms [HS99, SM10a, SM10b, Aon13].

Figure 1 compares the recoverable sizes of secret exponents for $n = 1, 2, \ldots, 60$. For smaller n, our algorithm is slightly better than Aono's algorithm [Aon13]. However, for larger n, our algorithm is much better than all other algorithms [HS99, SM10b, Aon13].

Table 1 represents the numerical data for the recoverable sizes of secret exponents for $n = 1, 2, \ldots, 10$, and $n = 101, 102, \ldots, 110$. For smaller n, though our algorithm and Aono's algorithm [Aon13] achieve almost the same bound, our algorithm is always better. For larger n, our algorithm is still much better than Howgrave-Graham and Seifert's algorithm [HS99].

[1] It is not obvious that our bound is better than Howgrave-Graham and Seifert's bound [HS99]. For large n, we approximate binomial coefficients as $\binom{n}{n/2} \approx \sqrt{\frac{2}{\pi n}} 2^n$ (see [OLBC10] in detail). The approximation suggests that our bound is better than the previous bound. The detailed analysis is written in the full version.

1.3 Organizations

In Section 2, we introduce the lattice based Coppersmith's method to solve modular equations [Cop96a], and the lattice construction strategy proposed by Takayasu and Kunihiro [TK13]. In Section 3, we recall the Boneh and Durfee's algorithm [BD00] and Aono's algorithm [Aon13]. In Section 4, we analyze the previous lattice constructions [BD00, Aon13] based on Takayasu and Kunihiro's strategy [TK13]. In Section 5, we propose our improved algorithm. In Section 6, we discuss the security of multiple exponents RSA in partial key exposure situations.

2 Preliminaries

In this section, we introduce the Coppersmith's method to solve modular equations which have small solutions [Cop96a]. First, we explain Howgrave-Graham's reformulation of the method [How97], and the LLL algorithm [LLL82]. After that, we introduce the strategy for lattice constructions proposed by Takayasu and Kunihiro [TK13].

Consider the modular equations, $h(x_1, \ldots, x_n) = 0 \pmod{W}$. All sizes of the solutions $(\tilde{x}_1, \ldots, \tilde{x}_n)$ are bounded by $X_1, \ldots, X_n$. When $\prod_{j=1}^{n} X_j$ is much smaller than W, the Coppersmith's method can find all the solutions in polynomial time. We write the norm of polynomials as $\|h(x_1, \ldots, x_n)\|$, which represents the Euclidean norm of the coefficeint vector. The following Howgrave-Graham's Lemma reduces the modular equations into integer equations.

Lemma 1 (Howgrave-Graham's Lemma [How97]). *Let $\tilde{h}(x_1, \ldots, x_n) \in \mathbb{Z}[x_1, \ldots, x_n]$ be a polynomial with at most w monomials. Let $m, W, X_1, \ldots, X_n$ be positive integers. Consider the case when*
1. $\tilde{h}(\tilde{x}_1, \ldots, \tilde{x}_n) = 0 \pmod{W^m}$, where $|\tilde{x}_1| < X_1, \ldots, |\tilde{x}_n| < X_n$,
2. $\|\tilde{h}(x_1 X_1, \ldots, x_n X_n)\| < W^m/\sqrt{w}$.
Then $\tilde{h}(\tilde{x}_1, \ldots, \tilde{x}_n) = 0$ holds over the integers.

To solve n-variate modular equations $h(x_1, \ldots, x_n) = 0 \pmod{W}$, it is suffice to find n new polynomials $\tilde{h}_1(x_1, \ldots, x_n), \ldots, \tilde{h}_n(x_1, \ldots, x_n)$ whose roots are the same as the solutions $(\tilde{x}_1, \ldots, \tilde{x}_n)$ and whose norms are small enough to satisfy Hograve-Graham's Lemma.

To find such polynomials from the original polynomial $h(x_1, \ldots, x_n)$, lattices and the LLL algorithm are often used. Lattices represent the integer linear combinations of the basis vectors. All vectors are row representation. For the basis vectors $\mathbf{b}_1, \ldots, \mathbf{b}_w$, which are all v dimensional vectors in $\mathbb{R}^v$, the lattice spanned by these vectors is defined as

$$L(\mathbf{b}_1, \ldots, \mathbf{b}_w) := \{\sum_{j=1}^{w} c_j \mathbf{b}_j : c_j \in \mathbb{Z} \text{ for all } j = 1, \ldots, w\}.$$

We also use the matrix representation for the basis. We define the basis matrix B as $w \times v$ matrix which has the basis vectors $\mathbf{b}_1, \ldots, \mathbf{b}_w$ in each row. In the same

way, the lattice can be rewritten as $L(B)$. We call the lattice full-rank when $w = v$. The volume of the lattice $\mathrm{vol}(L(B))$ is defined as the w-dimensional volume of the parallelpiped $\mathcal{P}(B) := \{xB : x \in \mathbb{R}^w, 0 \leq x_j < 1, \text{for all } j = 1, \ldots, w\}$. The volume can be computed as $\mathrm{vol}(L(B)) = \sqrt{\det(BB^T)}$. It is clear that the volume of full-rank lattice can be computed as $\mathrm{vol}(L(B)) = |\det(B)|$.

Lattice is used in many places in cryptography. See [NS01, nv10] in detail. In cryptanalysis, it is very important to find non-zero short lattice vectors. In this paper, we introduce the LLL algorithm [LLL82] which outputs non-zero short lattice vectors in polynomial time.

Proposition 1 (LLL algorithm [LLL82]). *Given basis vectors* $\mathbf{b}_1, \ldots, \mathbf{b}_w$ *in* $\mathbb{R}^k$*, the LLL algorithm finds LLL-reduced bases* $\tilde{\mathbf{b}}_1, \ldots, \tilde{\mathbf{b}}_w$ *that satisfy*

$$\|\tilde{\mathbf{b}}_n\| \leq 2^{w(w-1)/4(w-n+1)}(\mathrm{vol}(L(B)))^{1/(w-n+1)} \quad \textit{for } 1 \leq n \leq w,$$

in polynomial time in w, v*, and the maximum input length.*

Again, we consider how to solve modular equations $h(x_1, \ldots, x_n) = 0 \pmod{W}$. First, we construct w polynomials $h_1(x_1, \ldots, x_n), \ldots, h_w(x_1, \ldots, x_n)$, which have the roots $(\tilde{x}_1, \ldots, \tilde{x}_n)$ modulo W^m with positive integer m. We convert these polynomials to the vectors $\mathbf{b}_1, \ldots, \mathbf{b}_w$ in $\mathbb{Z}^v$, and construct the matrix B. The elements of each vector $\mathbf{b}_j$ are the same as the coefficients of $h_j(x_1X_1, \ldots, x_nX_n)$. All i-th elements of the vectors $\mathbf{b}_1, \ldots, \mathbf{b}_w$ are the coefficients of the same variables $x_1^{i_1} \cdots x_n^{i_n}$ for all $1 \leq i \leq k$. The vectors can be converted to the polynomials in the opposite way. We span the lattice $L(B)$. Since all the lattice vectors are the integer linear combinations of the basis vectors, the polynomials which are conversions of the lattice vectors have the roots $(\tilde{x}_1, \ldots, \tilde{x}_n)$ modulo W^m. We apply the LLL algorithm to the lattice bases and obtain n LLL-reduced bases $\tilde{\mathbf{b}}_1, \ldots, \tilde{\mathbf{b}}_n$. Finally, we can get the polynomials $\tilde{h}_1(x_1, \ldots, x_n), \ldots, \tilde{h}_n(x_1, \ldots, x_n)$ by converting the LLL-reduced bases. The norm of these polynomials are small. These polynomials satisfy Howgrave-Graham's Lemma provided that

$$(\mathrm{vol}(L(B)))^{1/w} < W^m.$$

We omit the small terms.

When we obtain the polynomials $\tilde{h}_1(x_1, \ldots, x_n), \ldots, \tilde{h}_n(x_1, \ldots, x_n)$, it is easy to solve the modular equation $h(x_1, \ldots, x_n) = 0 \pmod{W}$. What we should do is to find the roots of the polynomials over the integers by computing resultant or Gröbner basis. We should note that the method needs heuristic argument if we consider multivariate problems. Since the polynomials $\tilde{h}_1(x_1, \ldots, x_n), \ldots, \tilde{h}_n(x_1, \ldots, x_n)$ have no assurance of algebraic independency. In this paper, we assume that the polynomials are algebraic independence as the previous works [BD00, SM10a, SM10b, Aon13]. In fact, there are few negative cases reported.

The solvable sizes of small solutions depend on the lattice constructions. To maximize the sizes, we should select appropriate lattice bases which reduce the volume. Recently, Takayasu and Kunihiro [TK13] proposed the strategy for the

selections. To construct the triangular basis matrix, we define helpful polynomials whose diagonals are smaller than the modulus W^m. Since helpful polynomials contribute to the conditions for modular equations to be solved, we should select as many helpful polynomials as possible in the lattice bases. Conversely, unhelpful polynomials whose diagonals are larger than the modulus do not contribute to the conditions. We should select as few unhelpful polynomials as possible. The selections should be done with the constraint for the basis matrix to be triangular. The strategy clarifies which polynomials to be selected and which polynomials not to be selected in the lattice bases. To improve the previous bounds, we should add helpful polynomials or eliminate unhelpful polynomials in the lattice bases. When we counstruct the basis matrix which is not triangular, we should transform the basis matrix to be triangular by using unravelled linearization [HM09].

3 Previous Works

In this section, we introduce the lattice constructions in previous works [BD00, Aon13], which used the Coppersmith's method to solve modular equations [Cop96a, How97].

3.1 Boneh and Durfee's Lattice Construction

We recall the RSA key generation,

$$ed = 1 + k\phi(N), \text{ where } \phi(N) = (p-1)(q-1).$$

Boneh and Durfee [BD00] considered the modular polynomial

$$f(x,y) = 1 + x(N+y) \pmod{e}.$$

The polynomial has the roots $(x,y) = (k, 1-p-q)$. The sizes of the roots are bounded by $X := N^{\beta}, Y := 3N^{1/2}$. If we can find the roots, we can easily factor RSA modulus N.

To solve the modular equation $f(x,y) = 0$, Boneh and Durfee constructed the basis matrix with polynomials which have the roots $(x,y) = (k, 1-p-q)$ modulo e^m. At first, Boneh and Durfee used the shift-polynomials,

$$x^i f(x,y)^j e^{m-j}, \text{ with } j = 0, 1, \ldots, m, i = 0, 1, \ldots, m-j,$$

in the lattice bases. The shift-polynomials modulo e^m have the roots $(x,y) = (k, 1-p-q)$. The shift-polynomials generate the triangular basis matrix with diagonals $X^{i+j}Y^j e^{m-j}$ for all i, j. Ignoring low order terms of m, we can compute the dimension $w = \frac{1}{2}m^2$ and the volume of the lattice $\mathrm{vol}(L(B)) = X^{\frac{1}{3}m^3} Y^{\frac{1}{6}m^3} e^{\frac{1}{3}m^3}$. The lattice provides Wiener's bound $\beta < 0.25$.

To improve the bound, Boneh and Durfee added extra shifts,

$$y^l f(x,y)^u e^{m-u}, \text{ with } u = 0, 1, \ldots, m, l = 1, \ldots, t,$$

in the lattice bases. The shift-polynomials modulo e^m have the roots $(x, y) = (k, 1-p-q)$. We should optimize the parameter $\tau := t/u$. Though the extra shifts do not generate the tirangular basis matrix, we can transform it to be triangular using unravelled linearization [HM09]. The detailed analysis is written in [HM10]. After the transformation, the sizes of the diagonals become $X^u Y^{u+l} e^{m-u}$. Ignoring low order terms of m, we can compute the dimension $w = (\frac{1}{2} + \frac{\tau}{2})m^2$ and the volume of the lattice $\mathrm{vol}(L(B)) = X^{(\frac{1}{3}+\frac{\tau}{3})m^3} Y^{(\frac{1}{6}+\frac{\tau}{3}+\frac{\tau^2}{6})m^3} e^{(\frac{1}{3}+\frac{\tau}{6})m^3}$. We can solve the modular equation $f(x, y) = 0$ provided that $(\mathrm{vol}(L(B)))^{1/w} < e^m$, that is,

$$\beta(\frac{1}{3} + \frac{\tau}{3}) + \frac{1}{2}(\frac{1}{6} + \frac{\tau}{3} + \frac{\tau^2}{6}) + \frac{1}{3} + \frac{\tau}{6} < \frac{1}{2} + \frac{\tau}{2}.$$

To maximize the solvable bound β, we optimize $\tau = 1 - 2\beta$ and obtain the stronger bound $\beta < 1 - 1/\sqrt{2}$.

3.2 Aono's Lattice Construction

For the multiple key setting, the attackers have multiple public exponents $e_1, \ldots, e_n$ that satisfy

$$e_j d_j = 1 + k_j \phi(N), \text{ for } j = 1, 2, \ldots, n.$$

Aono [Aon13] considered n modular polynomials

$$f_j(x_j, y) = 1 + x_j(N + y) \pmod{e_j}, \text{ for } j = 1, 2, \ldots, n.$$

The polynomials have the roots $(x_1, \ldots, x_n, y) = (k_1, \ldots, k_n, 1-p-q)$. The sizes of the roots are bounded by $X_j := N^\beta$ for $j = 1, 2, \ldots, n$, $Y := 3N^{1/2}$. We also write $X := N^\beta$ for simplicity. If we can find the roots, we can easily factor RSA modulus N.

To solve simultaneous modular equations $f_j(x_j, y) = 0$ for $j = 1, 2, \ldots, n$, Aono constructed the basis matrix with polynomials which have the same roots as the solutions of the modular equation modulo $(e_1 \cdots e_n)^m$. Aono combined n lattices, each of which is the lattice to solve a single equation. To solve each single equation, Aono selected the shift-polynoials

$$x_j^{i_j} f_j(x_j, y)^{u_j} e_j^{m-u_j}, \quad \text{with } u_j = 0, 1, \ldots, m, i_j = 0, 1, \ldots, m - u_j, \text{ for } j = 1, 2, \ldots, n.$$

The selection for each single equation generates the triangular basis matrix. Aono combined the n lattices based on Minkowski sum. Aono proved that the combined lattices based on Minkowski sum are also triangular, if each basis matrix is triangular. The combined basis matrix has diagonals $X_1^{i'_1} \cdots X_n^{i'_n} Y^{u'} e_1^{m-\min\{i'_1, u'\}} \cdots e_n^{m-\min\{i'_n, u'\}}$, for $0 \le u' \le \sum_{j=1}^n i'_j$, $0 \le i'_j \le m$ for $j = 1, 2, \ldots, n$. Each polynomial of the row is the integer linear combination of shift-polynomials that have the corresponding diagonals. This operation reduce the powers of $e_1, \ldots, e_n$. The detailed discussion is written in [Aon13].

Ignoring low order terms of m, we can compute the dimension $w = \frac{n}{2}m^{n+1}$, and the volume of the lattice $\mathrm{vol}(L(B)) = X_1^{s_{X_1}} \cdots X_n^{s_{X_n}} Y^{s_Y} e_1^{s_{e_1}} \cdots e_n^{s_{e_n}}$, where $s_{X_j} = (\frac{n}{4} + \frac{1}{12})m^{n+2}, s_Y = (\frac{n^2}{8} + \frac{n}{24})m^{n+2}, s_{e_j} = (\frac{n}{4} + \frac{1}{12})m^{n+2}$, for $j = 1, 2, \ldots, n$. The lattice provides the bound

$$\beta < \frac{3}{4} - \frac{2}{3n+1}.$$

4 Another Look at Previous Lattice Constructions

In this section, we analyze the previous lattice constructions [BD00, Aon13] based on Takayasu and Kunihiro's strategy [TK13]. What we should mention is that if there are as many helpful polynomials as possible or as few unhelpful polynomials as possible in the lattice bases.

4.1 The Analysis of Boneh and Durfee's Lattices

We can rewrite the sizes of diagonals in Boneh and Durfee's basis matrix as $X^{i'}Y^{u'}e^{m-\min\{i',u'\}}$ for $0 \le u' \le 2(1-\beta)i'$, $0 \le i' \le m$. We consider the shift-polynomials for $i' < u' \le 2(1-\beta)i'$, $0 \le i' \le m$. To examine if the shift-polynomials are helpful or not, we compare the sizes of diagonals and the size of the modulus e^m. For easy comparison, we rewrite the sizes as the powers of N. The sizes of diagonals are $N^{\beta i' + \frac{1}{2}u' + m - i'}$, and the size of the modulus is N^m. The shift-polynomials are helpful when $\beta i' + \frac{1}{2}u' + m - i' \le m$, that is, $u' \le 2(1-\beta)i'$. Therefore, the shift-polynomials which Boneh and Dufee selected for $i' < u'$ are all helpful polynomials. Moreover, the condition is tight. That means when $2(1-\beta)i' < u'$, all shift-polynomials are unhelpful. For the basis matrix to be triangular, we have to select the shift-polynomials for $0 \le u' \le i', 0 \le i' \le m$. This analysis implies that Boneh and Durfee selected as many helpful polynomials as possible and as few unhelpful polynomials as possible.

4.2 The Analysis of Aono's Lattices

Next, we consider the Aono's lattices. We can rewrite the sizes of diagonals in Aono's basis matrix as $X_1^{i'_1} \cdots X_n^{i'_n} Y^{u'} e_1^{m-\min\{i'_1,u'\}} \cdots e_n^{m-\min\{i'_n,u'\}}$ for $0 \le u' \le \sum_{j=1}^n i'_j$, and $0 \le i'_j \le m$ for $j = 1, 2, \ldots, n$. We show that Aono selected unhelpful polynomials or the selections are not tight. To examine if the shift-polynomials are helpful or not, we compare the sizes of diagonals and the size of the modulus $(e_1 \cdots e_n)^m$. We consider the diagonal $X_1^m \cdots X_n^m Y^{nm}$, which is the case $i'_1 = \cdots = i'_n = m, u' = nm$. The size of the diagonal is $(XY)^{nm}$. For easy comparison, we rewrite the sizes as the powers of N. The sizes of the diagonal is $N^{nm\beta + \frac{nm}{2}}$, and the size of the modulus is N^{nm}. The shift-polynomial is helpful when $nm\beta + \frac{nm}{2} \le nm$, that is, $\beta \le \frac{1}{2}$. We recall that Aono's lattice provides the bound $\beta < \frac{3}{4} - \frac{2}{3n+1}$. Therefore, Aono selected unhelpful polynomials for $n \ge 3$, and the selections are not tight for $n = 1, 2$.

Aono also pointed out the issue in his paper [Aon13]. They proposed the heuristic improvement in appendix of their paper. They claimed that to improve the bound, some polynomials with highr powers of Y should be omit for $n \geq 3$. However, no exact conditions are given in the paper.

5 Our Improvements

In this section, we show the improved lattice constructions. To improve the bound, we select as many helpful polynomials as possible and as few unhelpful polynomials as possible in the lattice bases. We consider the same simultaneous modular equations as Aono [Aon13], $f_j(x_j, y) = 1 + x_j(N + y) \pmod{e_j} = 0$, for $j = 1, 2, \ldots, n$. We use shift-polynomials $x_j^{i_j} f_j(x_j, y)^{u_j} e_j^{m-u_j}, y^{l_j} f_j(x_j, y)^{u_j} e_j^{m-u_j}$ for $j = 1, 2, \ldots, n$. Aono's analysis suggests that we can construct the triangular basis matrix[2] with diagonals $X_1^{i'_1} \cdots X_n^{i'_n} Y^{u'} e_1^{m-\min\{i'_1, u'\}} \cdots e_n^{m-\min\{i'_n, u'\}}$. We reveal the condition when each lattice basis becomes helpful. We consider the polynomials with $\max\{i'_1, \ldots, i'_n\} \leq u'$. To examine if the shift-polynomials are helpful or not, we compare the sizes of diagonals and the size of modulus $(e_1 \cdots e_n)^m$. The polynomials have the diagonals $X_1^{i'_1} \cdots X_n^{i'_n} Y^{u'} e_1^{m-i'_1} \cdots e_n^{m-i'_n}$. For easy comparison, we rewrite the sizes as the powers of N. The sizes of the diagonals are $N^{\beta \sum_{j=1}^n i'_j + \frac{u'}{2} + nm - \sum_{j=1}^n i'_j}$, and the size of the modulus is N^{nm}. The shift-polynomials are helpful when

$$\beta \sum_{j=1}^{n} i'_j + \frac{u'}{2} + nm - \sum_{j=1}^{n} i'_j \leq nm,$$

that is,

$$u' \leq 2(1-\beta) \sum_{j=1}^{n} i'_j.$$

Therefore, we select the shift-polynomials $x_j^{i_j} f_j(x_j, y)^{u_j} e_j^{m-u_j}, y^{l_j} f_j(x_j, y)^{u_j} e_j^{m-u_j}$ for $j = 1, 2, \ldots, n$, which generate the diagonals $X_1^{i'_1} \cdots X_n^{i'_n} Y^{u'} e_1^{m-\min\{i'_1, u'\}} \cdots e_n^{m-\min\{i'_n, u'\}}$ for $0 \leq u' \leq 2(1-\beta) \sum_{j=1}^n i'_j$, $0 \leq i'_j \leq m$ for $j = 1, 2, \ldots, n$. It is clear that our selection becomes identical to Boneh and Durfee's selection for $n = 1$. The selection provides the better bound than previous works including Aono's heuristically improved lattices[3].

[2] For $n = 1, 2$ we should use unravelled linearization and transform the basis matrix which is not triangular to be triangular. See [HM10] for $n = 1$ and the full version of this paper for $n = 2$ in detail.

[3] Compared with Aono's heuristically improved lattice bases [Aon13], there are less unhelpful polynomials and as many helpful polynomials in our lattice bases. See the full version of this paper in detail.

Ignoring low order terms of m, we can compute the dimension

$$w = \sum_{i'_n=0}^{m} \cdots \sum_{i'_1=0}^{m} \sum_{u'=0}^{\lfloor 2(1-\beta)(i'_1+\cdots+i'_n)\rfloor} 1 = n(1-\beta)m^{n+1},$$

and the volume of the lattice $\mathrm{vol}(L(B)) = X_1^{s_{X_1}} \cdots X_n^{s_{X_n}} Y^{s_Y} e_1^{s_{e_1}} \cdots e_n^{s_{e_n}}$, where

$$s_{X_j} = \sum_{i'_n=0}^{m} \cdots \sum_{i'_1=0}^{m} \sum_{u'=0}^{\lfloor 2(1-\beta)(i'_1+\cdots+i'_n)\rfloor} i'_j = \frac{(3n+1)(1-\beta)}{6} m^{n+2},$$

$$s_Y = \sum_{i'_n=0}^{m} \cdots \sum_{i'_1=0}^{m} \sum_{u'=0}^{\lfloor 2(1-\beta)(i'_1+\cdots+i'_n)\rfloor} u' = \frac{n(3n+1)}{6}(1-\beta)^2 m^{n+2},$$

$$s_{e_j} = \sum_{i'_n=0}^{m} \cdots \sum_{i'_1=0}^{m} \sum_{u'=0}^{\lfloor 2(1-\beta)(i'_1+\cdots+i'_n)\rfloor} (m - \min\{u', i'_j\}) = \frac{1+(3n-1)(1-\beta)}{6} m^{n+2}.$$

We can solve the simultaneous modular equations $f_j(x_j, y) = 1 + x_j(N+y) \pmod{e_j} = 0$, for $j = 1, 2, \ldots, n$, when $(\mathrm{vol}(L(B)))^{1/w} < (e_1 \cdots e_n)^m$,

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

$$(3n+1)\beta^2 - 2(3n+1)\beta + 3n - 1 > 0,$$

that is,

$$\beta < 1 - \sqrt{\frac{2}{3n+1}}.$$

The bound is superior to all known algorithms [HS99, SM10a, SM10b, Aon13].

6 Partial Key Exposure Attacks on RSA

In the context of the security evaluations of RSA, partial key exposure attacks [BDF98, BM03, EJMW05, Aon09, SGM10] have been considered. In the partial key exposure situaion, the attackers know the partial information of secret exponent d. In the work [Aon13], Aono also considered partial key exposure attacks on RSA with multiple key settings. In this case, the attackers know public modulus N and multiple public exponents $e_1, \ldots, e_n$, whose corresponding secret exponents $d_1, \ldots, d_n$ are smaller than N^β, and the least significant $\delta \log N$ bits of secret exponents, $\tilde{d_1}, \ldots, \tilde{d_n}$. Aono proposed the algorithm with Minkowski sum based lattices, which works provided that

$$\beta < \frac{\delta}{2} + \frac{3}{4} - \frac{2}{3n+1}.$$

Based on Takayasu and Kunihiro's strategy [TK13], we propose the improved algorithm for partial key exposure attacks on RSA. Our algorithm works provided that

$$\beta < 1 - \sqrt{\frac{2(1-2\delta)}{3n+1}}, \delta < \frac{1}{2} - \frac{4}{3n+1}.$$

Our algorithm is the same as Aono's algorithm for $n = 1, 2$, and is superior to Aono's algorithm for $n \geq 3$. The detailed analysis is written in the full version of the paper.

7 Concluding Remarks

In this paper, we analyzed the security of RSA when the attackers have multiple public exponents $e_1, \ldots, e_n$ for the same public modulus N. We proposed improved algorithm for small secret exponent attacks. All secret exponents $d_1, \ldots, d_n$ are smaller than N^β. Our algorithm factors public modulus N provided that $\beta < 1 - \sqrt{2/(3n+1)}$. To the best of our knowledge, this is the first result that covers Boneh and Durfee's bound $\beta < 1 - 1/\sqrt{2}$ for $n = 1$, and converge to $\beta < 1$ for infinitely large n, simultaneously. Our bound is better than all known previous ones [HS99, SM10a, SM10b, Aon13].

Our lattice construction is based on Takayasu and Kunihiro's strategy [TK13] to collect helpful polynomials. The strategy enables us to determine the selections of polynomials in the lattice bases while taking into account the sizes of root bounds. That is the main difficulty in previous works [SM10b, Aon13].

Acknowledgement. This work was supported by JSPS KAKENHI Grant Number 25280001.

References

[Aon09] Aono, Y.: A new lattice construction for partial key exposure attack for RSA. In: Jarecki, S., Tsudik, G. (eds.) PKC 2009. LNCS, vol. 5443, pp. 34–53. Springer, Heidelberg (2009)

[Aon13] Aono, Y.: Minkowski Sum Based Lattice Construction for Multivariate Simultaneous Coppersmith's Technique and Applications to RSA. In: Boyd, C., Simpson, L. (eds.) ACISP. LNCS, vol. 7959, pp. 88–103. Springer, Heidelberg (2013), http://eprint.iacr.org/2012/675

[BM01] Blömer, J., May, A.: Low secret exponent RSA revisited. In: Silverman, J.H. (ed.) CaLC 2001. LNCS, vol. 2146, pp. 4–19. Springer, Heidelberg (2001)

[BM03] Blömer, J., May, A.: New partial key exposure attacks on RSA. In: Boneh, D. (ed.) CRYPTO 2003. LNCS, vol. 2729, pp. 27–43. Springer, Heidelberg (2003)

[BD00] Boneh, D., Durfee, G.: Cryptanalysis of RSA with private key d less than $N^{0.292}$. In: Stern, J. (ed.) EUROCRYPT 1999. LNCS, vol. 1592, pp. 1–11. Springer, Heidelberg (1999)

[BDF98] Boneh, D., Durfee, G., Frankel, Y.: Exposing an RSA private key given a small fraction of its bits. In: ASIACRYPT 1998. LNCS, vol. 1514, pp. 25–34. Springer, Heidelberg (1998)

[CH12] Cohn, H., Heninger, N.: Approximate common divisors via lattices. In: 10th Algorithmic Number Theory Symposium ANTS-X, 2012. Longer version available as IACR Cryptology ePrint Archive, Report 2011/437 (2011), http://eprint.iacr.org/2011/437

[Cop96a] Coppersmith, D.: Finding a Small Root of a univariate modular Equation. In: Maurer, U.M. (ed.) Advances in Cryptology - EUROCRYPT 1996. LNCS, vol. 1070, pp. 155–165. Springer, Heidelberg (1996)

[Cop96b] Coppersmith, D.: Finding a Small Root of a Bivariate Integer Equation; Factoring with High Bits Known. In: Maurer, U. (ed.) Advances in Cryptology - EUROCRYPT 1996. LNCS, vol. 1070, pp. 178–189. Springer, Heidelberg (1996)

[Cop97] Coppersmith, D.: Small solutions to polynomial equations, and low exponent RSA vulnerabilities. Journal of Cryptology 10(4), 233–260 (1997)

[Cop01] Coppersmith, D.: Finding small solutions to small degree polynomials. In: Silverman, J.H. (ed.) CaLC 2001. LNCS, vol. 2146, pp. 20–31. Springer, Heidelberg (2001)

[Cor04] Coron, J.-S.: Finding Small Roots of Bivariate Integer Equations Revisited. In: Cachin, C., Camenisch, J.L. (eds.) EUROCRYPT 2004. LNCS, vol. 3027, pp. 492–505. Springer, Heidelberg (2004)

[Cor07] Coron, J.-S.: Finding Small Roots of Bivariate Integer Equations: A Direct Approach. In: Menezes, A. (ed.) CRYPTO 2007. LNCS, vol. 4622, pp. 379–394. Springer, Heidelberg (2007)

[DN00] Durfee, G., Nguyên, P.Q.: Cryptanalysis of the RSA Schemes with Short Secret Exponent from Asiacrypt '99. In: Okamoto, T. (ed.) ASIACRYPT 2000. LNCS, vol. 1976, pp. 14–29. Springer, Heidelberg (2000)

[EJMW05] Ernst, M., Jochemsz, E., May, A., de Weger, B.: Partial key exposure attacks on RSA up to full size exponents. In: Cramer, R. (ed.) EUROCRYPT 2005. LNCS, vol. 3494, pp. 371–386. Springer, Heidelberg (2005)

[HM08] Herrmann, M., May, A.: Solving Linear Equations modulo Divisors: On factoring given any bits. In: Pieprzyk, J. (ed.) ASIACRYPT 2008. LNCS, vol. 5350, pp. 406–424. Springer, Heidelberg (2008)

[HM09] Herrmann, M., May, A.: Attacking power generators using unravelled linearization: When do we output too much? In: Matsui, M. (ed.) ASIACRYPT 2009. LNCS, vol. 5912, pp. 487–504. Springer, Heidelberg (2009)

[HM10] Herrmann, M., May, A.: Maximizing Small Root Bounds by Linearization and Applications to Small Secret Exponent RSA. In: Nguyen, P.Q., Pointcheval, D. (eds.) PKC 2010. LNCS, vol. 6056, pp. 53–69. Springer, Heidelberg (2010)

[How97] Howgrave-Graham, N.: Finding small roots of univariate modular equations revisited. In: Darnell, M. (ed.) Cryptography and Coding 1997. LNCS, vol. 1355, pp. 131–142. Springer, Heidelberg (1997)

[How01] Howgrave-Graham, N.: Approximate integer common divisors. In: Silverman, J.H. (ed.) CaLC 2001. LNCS, vol. 2146, pp. 51–66. Springer, Heidelberg (2001)

[HS99] Howgrave-Graham, N., Seifert, J.-P.: Extending Wiener's attack in the presence of many decrypting exponents. In: Baumgart, R. (ed.) CQRE 1999. LNCS, vol. 1740, pp. 153–166. Springer, Heidelberg (1999)

[IKK08a] Itoh, K., Kunihiro, N., Kurosawa, K.: Small Secret Key Attack on a Variant of RSA (due to Takagi). In: Malkin, T. (ed.) CT-RSA 2008. LNCS, vol. 4964, pp. 387–406. Springer, Heidelberg (2008)

[IKK08b] Itoh, K., Kunihiro, N., Kurosawa, K.: Small Secret Key Attack on a Takagi's Variant of RSA. IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sceiences E92-A(1), 33–41 (2008)

[JM06] Jochemsz, E., May, A.: A Strategy for Finding Roots of Multivariate Polynomials. In: Lai, X., Chen, K. (eds.) ASIACRYPT 2006. LNCS, vol. 4284, pp. 267–282. Springer, Heidelberg (2006)

[JM07] Jochemsz, E., May, A.: A Polynomial Time Attack on RSA with Private CRT-Exponents Smaller Than $N^{0.073}$. In: Menezes, A. (ed.) CRYPTO 2007. LNCS, vol. 4622, pp. 395–411. Springer, Heidelberg (2007)

[Kun11] Kunihiro, N.: Solving Generalized Small Inverse Problems. In: Steinfeld, R., Hawkes, P. (eds.) ACISP 2010. LNCS, vol. 6168, pp. 248–263. Springer, Heidelberg (2010)

[Kun12] Kunihiro, N.: On Optimal Bounds of Small Inverse Problems and Approximate GCD Problems with Higher Degree. In: Gollmann, D., Freiling, F.C. (eds.) ISC 2012. LNCS, vol. 7483, pp. 55–69. Springer, Heidelberg (2012)

[KSI11] Kunihiro, N., Shinohara, N., Izu, T.: A Unified Framework for Small Secret Exponent Attack on RSA. In: Miri, A., Vaudenay, S. (eds.) SAC 2011. LNCS, vol. 7118, pp. 260–277. Springer, Heidelberg (2012)

[LLL82] Lenstra, A.K., Lenstra Jr., H.W., Lovász, L.: Factoring polynomials with rational coefficients. Mathematische Annalen 261, 515–534 (1982)

[May04] May, A.: Secret Exponent Attacks on RSA-type Schemes with Moduli $N = p^r q$. In: Bao, F., Deng, R., Zhou, J. (eds.) PKC 2004. LNCS, vol. 2947, pp. 218–230. Springer, Heidelberg (2004)

[May10] May, A.: Using LLL-reduction for solving RSA and factorization problems: A survey. In: NV10 (2007), `http://www.cits.rub.de/permonen/may.html`

[MR09] May, A., Ritzenhofen, M.: Implicit Factoring: On Polynomial Time Factoring Given Only an Implicit Hint. In: Jarecki, S., Tsudik, G. (eds.) PKC 2009. LNCS, vol. 5443, pp. 1–14. Springer, Heidelberg (2009)

[NS01] Nguyên, P.Q., Stern, J.: The Two Faces of Lattices in Cryptology. In: Silverman, J.H. (ed.) CaLC 2001. LNCS, vol. 2146, pp. 146–180. Springer, Heidelberg (2001)

[nv10] Nguyen, P.Q., Vallée, B. (eds.): The LLL Algorithm: Survey and Applications. Information Security and Cryptography. Springer, Heidelberg (2007)

[OLBC10] Olver, F.W.J., Lozier, D.W., Boisvert, R.F., Clark, C.W.: NIST handbook of mathematical functions. Cambridge University Press, Cambridge (2010)

[SGM10] Sarkar, S., Sen Gupta, S., Maitra, S.: Partial Key Exposure Attack on RSA - Improvements for Limited Lattice Dimensions. In: Gong, G., Gupta, K.C. (eds.) INDOCRYPT 2010. LNCS, vol. 6498, pp. 2–16. Springer, Heidelberg (2010)

[SM10a] Sarkar, S., Maitra, S.: Cryptanalysis of RSA with two decryption exponents. Information Processing Letter 110, 178–181 (2010)

[SM10b] Sarkar, S., Maitra, S.: Cryptanalysis of RSA with more than one decryption exponents. Information Processing Letter 110, 336–340 (2010)

[TK13] Takayasu, A., Kunihiro, N.: Better Lattice Constructions for Solving Multivariate Linear Equations Modulo Unknown Divisors. In: Boyd, C., Simpson, L. (eds.) ACISP. LNCS, vol. 7959, pp. 118–135. Springer, Heidelberg (2013)

[Weg02] de Weger, B.: Cryptanalysis of RSA with Small Prime Difference, Applicable Algebra in Engineering. Communication and Computing 13, 17–28 (2002)

[Wie90] Wiener, M.J.: Cryptanalysis of Short RSA Secret Exponents. IEEE Transactions on Information Theory 36(3), 553–558 (1990); Firstly appeared In: Quisquater, J.-J., Vandewalle, J. (eds.) EUROCRYPT 1989. LNCS, vol. 434, p. 372. Springer, Heidelberg (1990)