General Bounds for Small Inverse Problems and Its Applications to Multi-Prime RSA*

†Atsushi Takayasu and ‡Noboru Kunihiro

April 4, 2016

Abstract

In 1999, Boneh and Durfee introduced the *small inverse problem*, which solves the bivariate modular equation $x(N+y) \equiv 1 \pmod{e}$. Absolute values of solutions for x and y are bounded above by $X = N^{\delta}$ and $Y = N^{\beta}$, respectively. They solved the problem for $\beta = 1/2$ in the context of small secret exponent attacks on RSA and proposed a polynomial time algorithm that works when $\delta < \left(7 - 2\sqrt{7}\right)/6 \approx 0.284$. In the same work, the bound was further improved to $\delta < 1 - 1/\sqrt{2} \approx 0.292$. Thus far, the small inverse problem has also been analyzed for an arbitrary β. Generalizations of Boneh and Durfee's lattices to obtain the stronger bound yielded the bound $\delta < 1 - \sqrt{\beta}$. However, the algorithm works only when $\beta \geq 1/4$. When $0 < \beta < 1/4$, there have been several works where the authors claimed their results are the best.

In this paper, we revisit the problem for an arbitrary β. At first, we summarize the previous results for $0 < \beta < 1/4$. We reveal that there are some results that are not valid and show that Weger's algorithms provide the best bounds. Next, we propose an improved algorithm to solve the problem for $0 < \beta < 1/4$. Our algorithm works when $\delta < 1 - 2\left(\sqrt{\beta(3+4\beta)} - \beta\right)/3$. Our algorithm construction is based on the combinations of Boneh and Durfee's two forms of lattices and it is more natural compared with previous works. For the cryptographic application, we introduce small secret exponent attacks on Multi-Prime RSA with small prime differences.

1 Introduction

The Small Inverse Problem. In [BD00], Boneh and Durfee introduced the *small inverse problem* (SIP). Given two distinct large integers N and e, the goal of the problems is to find $\tilde{x}$ and $\tilde{y}$ such that $\tilde{x}$ is an inverse of $N + \tilde{y} \mod e$ where $\tilde{x}$ and $\tilde{y}$ are small, i.e., absolute values of $\tilde{x}$ and $\tilde{y}$ are bounded by $X := N^{\delta}$ and $Y := N^{\beta}$, respectively. The SIP can be formulated as the following modular equation,

$$x(N+y) \equiv 1 \pmod{e}$$

*This paper is the full version of [TK14b]. This research was supported by CREST, JST, and JSPS KAKENHI Grant Number 26·8237 and 25280001.

†The University of Tokyo. The author is supported by a JSPS Fellowship for Young Scientists. e-mail: a-takayasu@it.k.u-tokyo.ac.jp

‡The University of Tokyo. e-mail: kunihiro@k.u-tokyo.ac.jp

whose solution is $(x, y) = (\tilde{x}, \tilde{y})$. In this paper, we call the problem the (δ, β)-SIP.

One of the typical cryptographic applications of the SIP is the small secret exponent attack on RSA. Recall RSA key generation $ed \equiv 1 \pmod{\phi(N)}$ where $\phi(N) = (p-1)(q-1) = N-(p+q)+1$. We can rewrite the equation as $ed+\ell(N-(p+q)+1) = 1$ with some integer $\ell < N^{\delta}$. If we can solve the $(\delta, 1/2)$-SIP, i.e., $x(N+y) \equiv 1 \pmod{e}$, whose solution is $(x, y) = (\ell, -(p+q)+1)$, we can factor the RSA modulus N. When public exponents e are full size, the size of the secret exponent d is $\approx \ell < N^{\delta}$. Boneh and Durfee [BD00] proposed lattice-based polynomial time algorithms to solve the $(\delta, 1/2)$-SIP. At first, they proposed an algorithm that works when $\delta < \left(7 - 2\sqrt{7}\right)/6 = 0.28474\cdots$. This result improved the previous bound $\delta < 1/4 = 0.25$ proposed by Wiener [Wie90]. In the same work, Boneh and Durfee further improved the bound to $\delta < 1 - 1/\sqrt{2} = 0.29289\cdots$. To obtain the stronger bound, they extracted sublattices from the previous lattices that provided the weaker bound. However, the analysis to compute the determinant of the sublattice is involved since the basis matrix is not triangular.

Boneh and Durfee [BD00] claimed that their bound may not be optimal. They estimated that the bound should be improved to $\delta < 1/2$. Although several papers [BM01, HM10, KSI11] have followed the work, no results that improved the Boneh-Durfee bound have been reported and Aono et al. [AASW12] showed some evidence of the optimality of the attack. Blömer and May [BM01] considered different lattice constructions to solve the $(\delta, 1/2)$-SIP. Their algorithm works when $\delta < \left(\sqrt{6} - 1\right)/5 = 0.28989\cdots$. Although the bound is inferior to the Boneh-Durfee stronger bound, it is superior to the weaker bound. Moreover, dimensions of the Blömer-May lattices are smaller than those of the Boneh-Durfee lattices. However, the analysis to compute the determinant of the lattice is also involved since the basis matrix is not triangular.

Herrmann and May [HM10] revisited the Boneh-Durfee algorithms [BD00]. They used a technique called unravelled linearization [HM09] and analyzed the determinant of the lattice to obtain the stronger bound. They used linearization $z = -1 + xy$ and transformed the basis matrices that were not triangular to be triangular. The proof is very simple compared with Boneh and Durfee's original proof [BD00]. Kunihiro, Shinohara, and Izu [KSI11] followed the work and provided a simpler proof for the Blömer-May algorithm [BM01] by using unravelled linearization. Hence, unravelled linearization is a key technique to maximize solvable root bounds of the SIP.

General Bounds for the Small Inverse Problem. The SIP is an important problem in the context of RSA cryptanalysis and has been analyzed in a number of papers. Several variants of the problem have been considered, small secret exponent attacks on variants of RSA [DN00, IKK08b], partial key exposure attacks [BM03, EJMW05, Aon09, SGM10, TK14a], and more. To analyze the problem in detail, mathematical generalizations of the SIP [Kun11, Kun12] have also been considered. One of the well considered generalizations is the (δ, β)-SIP for an arbitrary $0 < \beta < 1$, not only $\beta = 1/2$. For the attack, generalizations of lattices for the $(\delta, 1/2)$-SIP [BD00, BM01] have been analyzed.

Weger [Weg02] studied small secret exponent attacks on RSA for a small difference of prime factors, e.g., $|p - q| < N^{\gamma}$ with $\gamma \leq 1/2$. In this case, they revealed that the RSA modulus can be factored when we solve the $(\delta, 2\gamma - 1/2)$-SIP. They extended the Boneh-Durfee lattice constructions and constructed algorithms to solve the (δ, β)-SIP for an arbitrary β. Their algorithms solve the

(δ, β)-SIP when

$$\delta < 1 - \sqrt{\beta} \quad \text{for } \frac{1}{4} \leq \beta < 1, \tag{1}$$

$$\delta < 1 - \frac{1}{3}\left(2\sqrt{\beta(\beta+3)} - \beta\right). \tag{2}$$

The first (resp. the second) bound can be obtained by lattice constructions to obtain the Boneh-Durfee stronger (resp. weaker) bound. Weger [Weg02] also extended Wiener's algorithm [Wie90] for the attack. The algorithm works when

$$\delta < \frac{3}{4} - \beta. \tag{3}$$

Although the bound (1) is the best among the three bounds, the algorithm works only when $1/4 \leq \beta < 1$. The bound (2) (resp. (3)) is the better when $0 < \beta < 1/8$ (resp. $1/8 \leq \beta < 1/4$).

Sarkar et al. [SMS08] studied small secret exponent attacks on RSA for the case when attackers know the most significant bits of a prime factor p. They solved the (δ, β)-SIP for an arbitrary β for the attack. In addition to Weger's results [Weg02], Sarkar et al. extended the Blömer-May lattice constructions. Their algorithm solves the (δ, β)-SIP when

$$\delta < \frac{2}{5}\left(\sqrt{4\beta^2 - \beta + 1} - 3\beta + 1\right). \tag{4}$$

The bound is superior to Weger's bound (2) and (3) when $3/35 \leq \beta < 1/4$.

Kunihiro, Shinohara, and Izu [KSI11] considered a broader class of lattices and not just generalizations of lattices for the $(\delta, 1/2)$-SIP [BD00, BM01]. To solve the (δ, β)-SIP for an arbitrary β, Kunihiro et al. analyzed hybrid lattice constructions that included the Boneh-Durfee lattices for the stronger bound [BD00, Weg02] and the Blömer-May lattices [BM01, SMS08]. To be precise, Kunihiro et al. considered a broader class of lattices, and the previous two lattices [SMS08, Weg02] were special cases of the class. Therefore, there may be chances to improve the previous result by making use of the structures of two lattices, simultaneously. However, their result becomes the same as Weger's bound (1) for $1/4 \leq \beta < 1$ and Sarkar et al.'s bound (4) for $0 < \beta < 1/4$.

Small Secret Exponent Attacks on Multi-Prime RSA with Small Prime Differences. Multi-Prime RSA is a variant of RSA whose public modulus $N = \prod_{j=1}^{k} p_j$ is a product of k distinct primes $p_1, p_2, \ldots, p_k$. The bit length of all prime factors are the same. Key generations of Multi-Prime RSA are the same as that of standard RSA, $ed = 1 \pmod{\phi(N)}$ where $\phi(N) = \prod_{j=1}^{k}(p_j - 1)$.

Multi-Prime RSA becomes efficient for its low cost decryption of a large k since the main computation costs are modular exponentiations with $\log N/k$ bits moduli when Chinese Remaindering is used. Moreover, most algebraic attacks become less efficient for a larger k such as small secret exponent attacks [Wie90, BD00] and partial key exposure attacks [BM03, EJMW05, TK14a]. As the standard RSA, Multi-Prime RSA becomes insecure when extremely small secret exponents $d < N^{\delta}$ are used. Ciet et al. [CKL+02] extended Wiener's [Wie90] and Boneh and Durfee's attacks [BD00]. Extensions of Wiener's attacks work when $\delta < 1/2k$. To extend Boneh and Durfee's attacks, they solved the $(\delta, 1 - 1/k)$-SIP. The algorithms work when $\delta < 1 - \sqrt{1 - 1/k}$. Both bounds become the same as the previous results [Wie90, BD00] for $k = 2$.

Zhang and Takagi [ZT13] analyzed small secret exponent attacks on Multi-Prime RSA with small prime differences[1]. Assume $p_1 > p_2 > \cdots > p_k$ without loss of generality. Zhang and Takagi analyzed the case when $|p_1 - p_k| < N^\gamma, 0 < \gamma \leq 1/k$ and revealed that Multi-Prime RSA becomes insecure when we can solve the $(\delta, \gamma + 1 - 2/k)$-SIP. After that the same authors [ZT14] gave an improved analysis. Multi-Prime RSA becomes insecure when we can solve the $(\delta, 2\gamma + 1 - 3/k)$-SIP. When $\gamma = 1/k$, the results [ZT13, ZT14] becomes the same as that of Ciet et al.'s results [CKL+02] that solves the $(\delta, 1 - 1/k)$-SIP. In addition, the improved result [ZT14] becomes the same as Weger [Weg02] that solves the $(\delta, 2\gamma - 1/2)$-SIP for $k = 2$.

Our Contributions. In this paper, we study the (δ, β)-SIP for an arbitrary β. At first, we summarize previous lattice constructions [BD00, BM01, Weg02, SMS08, KSI11] to obtain the bounds (1) to (4). We reveal that a generalization of the Blömer-May lattices to obtain the bound (4) is not valid for $\beta < 1/4$. Therefore, although Sarkar et al. [SMS08] and Kunihiro et al. [KSI11] claimed that the bound (4) is the best when $3/35 < \beta < 1/4$, the results are incorrect. Among previous results, Weger's bound (2) (resp. (3)) is the best for $0 < \beta \leq 1/8$ (resp. $1/8 < \beta < 1/4$).

Next, we propose an improved algorithm to solve the (δ, β)-SIP for arbitrary β. We consider a broader class of lattices that include Weger's three lattices to obtain the bounds (1)-(3) [Weg02] for special cases. Therefore, there may be chances to improve the previous results by making use of the structures of previous lattices, simultaneously. Indeed, when $0 < \beta < 1/4$, our algorithm works when

$$\delta < 1 - \frac{2}{3}\left(\sqrt{\beta(3 + 4\beta)} - \beta\right) \tag{5}$$

and the bound is superior to the previous bounds. This means that our lattice constructions make better use of algebraic structures of polynomials than previous analyses to solve the (δ, β)-SIP [Weg02]. As several previous works [HM10, KSI11, ZT14], we analyze the determinant of lattices using unravelled linearization. Therefore, the proof is rather simple.

Figure 1 compares recoverable sizes of δ for our algorithm and previous ones [Weg02, SMS08] to solve the (δ, β)-SIP for $0 \leq \beta \leq 1/4$. Table 1 shows the numerical data. When $\beta = 1/4$ and $\beta = 0$, our bound becomes the same as Weger's result $\delta < 0.5$ and $\delta < 1$, respectively. However, our algorithm is better than the two results for $0 < \beta < 1/4$.

As an application of our algorithm, we analyze small secret exponent attacks on Multi-Prime RSA with small prime differences. It is clear that we can improve previous results since our algorithm to solve the (δ, β)-SIP is better than that which was used in [ZT14].

Organizations. In Section 2, we introduce lattice-baesd Coppersmith's method to solve modular equations [Cop96, How97]. In Section 3, we define the (δ, β)-SIP and recall previous lattice constructions to solve the (δ, β)-SIP. In Section 4, we propose our lattice constructions to solve the (δ, β)-SIP for an arbitrary β. In Section 5, we analyze small secret exponent attacks on Multi-Prime RSA with small prime differences.

[1] See also Bahig et al.'s work [BBN12]. They extended Weger's attacks that are based on Wiener's work [Wie90]. The attacks work when $\delta < 1/k - \gamma/2$.

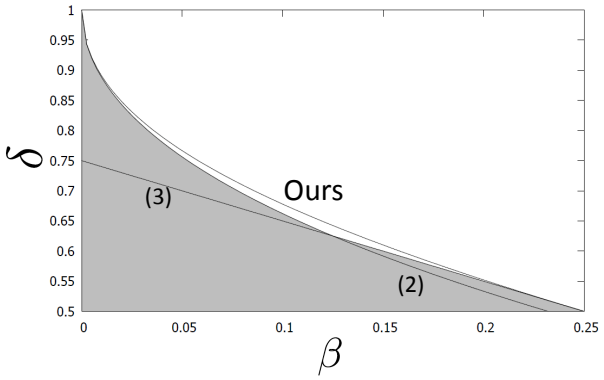

Figure 1: The comparison of the recoverable sizes of δ for $0 \leq \beta \leq 1/4$. Our algorithm works in the left below of the solid line.

2 Preliminaries

In this section, we briefly explain Coppersmith's method to solve modular equations [Cop96]. We introduce the simpler modification of the method proposed by Howgrave-Graham [How97].

The 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,

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

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. Parallelepiped of a lattice is defined by $\mathcal{P}(\boldsymbol{B}) := \{\boldsymbol{cB} : \boldsymbol{c} \in \mathbb{R}^n, 0 < c_j \leq 1 \text{ for all } j = 1, 2, \ldots, n\}$. 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 [Cop97, Cop01, May10, NS01] for detailed information. One of the cryptanalytic applications that use lattices is Coppersmith's method to solve modular equations [Cop96]. To use the method, finding short lattice vectors is essential. In this paper, we introduce the celebrated LLL algorithm [LLL82] 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 [LLL82])**.** *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*

$$\|\boldsymbol{b}'_1\| \leq 2^{(n-1)/4} (\det(L(\boldsymbol{B})))^{1/n} \quad \textit{and} \quad \|\boldsymbol{b}'_2\| \leq 2^{n/2} (\det(L(\boldsymbol{B})))^{1/(n-1)},$$

Table 1: Numerical data of solvable δ for the (δ, β)-SIP.

β	Ours	(3) of [Weg02]	(2) of [Weg02]
$1/4 = 0.25$	0.5	0.5	0.482408121
0.225	0.5255002	0.525	0.507109165
0.2	0.552146808	0.55	0.533333333
0.175	0.580217435	0.575	0.561398283
0.15	0.610102051	0.6	0.591742431
$1/8 = 0.125$	0.642374781	0.625	0.625
0.1	0.67793654	0.65	0.662149042
0.075	0.718337521	0.675	0.704843788
0.05	0.766666667	0.7	0.756325011
0.025	0.831074521	0.725	0.825
0	1	0.75	1

in polynomial time in input length and n, m.

Howgrave-Graham's Lemma. To solve modular equations $h(x, y) = 0 \mod e$ whose roots are $(x, y) = (\tilde{x}, \tilde{y})$ is difficult for the existence of the modulus e. Howgrave-Graham [How97] revealed that we can find polynomials $h'_1(x, y)$ and $h'_2(x, y)$ that have the same roots as $h(x, y) \pmod e$ over the integers. For bivariate polynomials $h(x, y) := \sum h_{i,j} x^i y^j$, we define norms of polynomials as $\|h(x, y)\| := \sqrt{\sum h_{i,j}^2}$. Howgrave-Graham showed the following lemma that implies that norms of polynomials $h'_1(x, y)$ and $h'_2(x, y)$ should be low.

Lemma 1 (Howgrave-Graham's Lemma [How97])**.** *Given integers X, Y, and t, if a polynomial $h'(x, y)$ that has at most n monomials satisfies following two conditions,*
1. $h'(\tilde{x}, \tilde{y}) = 0 \pmod{e^t}$ where $|\tilde{x}| < X$ and $|\tilde{y}| < Y$,
2. $\|h'(x, y)\| < e^t/\sqrt{n}$,
then $h'(\tilde{x}, \tilde{y}) = 0$ holds over the integers.

For solving the modular equation $h(x, y) = 0 \pmod e$, we can find such low norm polynomials $h'_1(x, y)$ and $h'_2(x, y)$ by using the LLL algorithm. We construct n polynomials $h_1(x, y), \ldots, h_n(x, y)$ that have roots $(x, y) = (\tilde{x}, \tilde{y})$ modulo e^t, and construct a basis matrix $\boldsymbol{B}$ where each basis vector $\boldsymbol{b}_1, \ldots, \boldsymbol{b}_n$ consists of coefficients of a polynomial $h_1(xX, yY), \ldots, h_n(xX, yY)$. By the definitions of $h_1(x, y), \ldots, h_n(x, y)$ and lattices, all polynomials modulo e^t whose coefficients correspond to lattice vectors in $L(\boldsymbol{B})$ have the roots $(x, y) = (\tilde{x}, \tilde{y})$. Therefore, we can find low norm polynomials $h'_1(x, y)$ and $h'_2(x, y)$ whose roots modulo e^t are the same as the original solutions by using the LLL algorithm. If the polynomials $h'_1(x, y)$ and $h'_2(x, y)$ satisfy Howgrave-Graham's Lemma, we can find the roots by finding the roots of the polynomials over the integers. The operation is easy by computing Gröbner bases or resultants of $h'_1(x, y)$ and $h'_2(x, y)$. In this paper, we focus on the lattice constructions to solve modular equations as in previous works [BD00, BM01, SMS08, HM10].

To solve modular bivariate equations, a heuristic argument is required since there are no assurance that the polynomials $h'_1(x,y)$ and $h'_2(x,y)$ will be algebraically independent. In this paper, we assume the fact as previous works [BD00, HM10, KSI11, SMS08, Weg02] since there exist few negative reports of the assumption. See [BJ07, BCC+13] for more information. 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.

3 Previous Lattice Constructions to Solve the (δ, β)-SIP

In this section, we formally define the (δ, β)-SIP.

Definition 1 (The (δ, β)-SIP)**.** *Given two distinct integers N and e with the same bit size and real numbers $\delta, \beta \in (0,1)$, the goal of the the (δ, β)-SIP is to find integers $\tilde{x}$ and $\tilde{y}$ that satisfy $|\tilde{x}| < N^{\delta}$ and $|\tilde{y}| < N^{\beta}$, and*

$$x(N+y) \equiv 1 \pmod{e}.$$

In this paper, we also use $X := N^{\delta}$ and $Y := N^{\beta}$ that denote upper bounds of the absolute values of the solutions. Although we only consider the case when two integers N and e are the same bit sizes, it is easy to extend to more general cases.

To solve the modular equation

$$f(x,y) = -1 + x(N+y) = 0 \pmod{e},$$

Boneh and Durfee [BD00] used two forms of shift-polynomials,

$$g^x_{[i,u]}(x,y) := x^{i-u} f(x,y)^u e^{t-u} \quad \text{and} \quad g^y_{[u,j]}(x,y) := y^j f(x,y)^u e^{t-u}.$$

Each polynomial $g^x_{[i,u]}(x,y)$ (resp. $g^y_{[u,j]}(x,y)$) is called x-shifts (resp. y-shifts). When all indices i, u, and j are non-negative integers, both polynomials modulo e^t have roots $(\tilde{x}, \tilde{y})$, e.g., $g^x_{[i,u]}(\tilde{x}, \tilde{y}) = 0 \pmod{e^t}$ and $g^y_{[u,j]}(\tilde{x}, \tilde{y}) = 0 \pmod{e^t}$. Let $\mathcal{S}_x$ and $\mathcal{S}_y$ denote sets of indices and $\boldsymbol{B}$ be the basis matrices that consist of coefficients of shift-polynomials $g^x_{[i,u]}(x,y)$ with indices in $\mathcal{S}_x$ and $g^y_{[u,j]}(x,y)$ with indices in $\mathcal{S}_y$. The selection of shift-polynomials $\mathcal{S}_x$ and $\mathcal{S}_y$ is essential to maximize the solvable root bounds X and Y. In the rest of this section, we summarize previous lattice constructions [BD00, BM01, Weg02, SMS08, HM10, KSI11] to solve the problem.

Weaker Boneh-Durfee Lattices. We introduce the Boneh-Durfee lattices [BD00] to obtain the weaker bound $\delta < (7 - 2\sqrt{7})/6$ and its generalization by Weger [Weg02] to obtain the bound (2), $\delta < \frac{1}{3}(\beta + 3 - 2\sqrt{\beta(\beta+3)})$. Boneh and Durfee defined sets of indices,

$$\mathcal{S}^{wBD}_x := \{(i,u) | i = 0,1,\ldots,t; u = 0,1,\ldots,i\} \quad \text{and} \quad \mathcal{S}^{wBD}_y := \{(u,j) | u = 0,1,\ldots,t; j = 1,2,\ldots,\lfloor \eta t \rfloor\}$$

with a parameter $\eta \geq 0$. They constructed basis matrices $\boldsymbol{B}$ that consist of coefficients of $g^x_{[i,u]}(x,y)$ with indices in $\mathcal{S}^{wBD}_x$ and $g^y_{[u,j]}(x,y)$ with indices in $\mathcal{S}^{wBD}_y$. The matrices become triangular with diagonals $X^i Y^u e^{t-u}$ for $g^x_{[i,u]}(x,y)$ and $X^u Y^{u+j} e^{t-u}$ for $g^y_{[u,j]}(x,y)$. Ignoring low order terms of t,

the dimension and the determinant of the lattices are computed as $n = (\frac{1}{2} + \eta)t^2$ and $\det(\boldsymbol{B}) = X^{(\frac{1}{3}+\frac{\eta}{2})t^3} Y^{(\frac{1}{6}+\frac{\eta(1+\eta)}{2})t^3} e^{(\frac{1}{3}+\frac{\eta}{2})t^3}$, respectively. The conditions for the (δ, β)-SIP to be solved, i.e., $(\det(B))^{1/n} < e^t$, become

$$\delta\left(\frac{1}{3}+\frac{\eta}{2}\right) + \beta\left(\frac{1}{6}+\frac{\eta(1+\eta)}{2}\right) + \left(\frac{1}{3}+\frac{\eta}{2}\right) < \frac{1}{2}+\eta,$$

$$\delta < \frac{1-\beta+3(1-\beta)\eta-3\beta\eta^2}{2+3\eta}.$$

To maximize the right hand side of the inequality, we set the parameter $\eta = \left(-2\beta + \sqrt{\beta(\beta+3)}\right)/3\beta$ and the condition becomes

$$\delta < \frac{1}{3}\left(\beta + 3 - 2\sqrt{\beta(\beta+3)}\right).$$

Stronger Boneh-Durfee Lattices. To improve the bound, Boneh and Durfee [BD00] extracted sublattices from the previous weaker Boneh-Durfee lattices and constructed an algorithm that solves the $(\delta, 1/2)$-SIP when $\delta < 1 - 1/\sqrt{2}$. Weger [Weg02] generalized the lattice constructions and constructed an algorithm that solves the (δ, β)-SIP when the condition (1) $\delta < 1 - \sqrt{\beta}$ holds.

Boneh and Durfee redefined sets of indices,

$$\mathcal{S}_x^{sBD} := \{(i,u) | i = 0, 1, \ldots, t; u = 0, 1, \ldots, i\} \quad \text{and} \quad \mathcal{S}_y^{sBD} := \{(u,j) | u = 0, 1, \ldots, t; j = 1, 2, \ldots, \lfloor \tau u \rfloor\}$$

with a parameter $0 \leq \tau \leq 1$. They selected shift-polynomials $g^x_{[i,u]}(x,y)$ with indices in $\mathcal{S}_x^{sBD}$ and $g^y_{[u,j]}(x,y)$ with indices in $\mathcal{S}_y^{sBD}$. Although the basis matrices generated by the polynomial selections are not triangular, Herrmann and May [HM10] showed that the matrices can be transformed into triangular with a linearization $z = -1 + xy$. As the Boneh-Durfee weaker lattice, polynomials in $\mathcal{S}_x^{sBD}$ generate a triangular matrix with diagonals $X^i Y^u e^{t-u}$. When the linearization $z = -1 + xy$ is applied to the polynomials, the matrix is still triangular with diagonals $X^{i-u} Z^u e^{t-u}$. Although the matrix with extra polynomials in $\mathcal{S}_y^{sBD}$ becomes non-triangular, the linearization preserves the matrix to be triangular with diagonals $Y^j Z^u e^{t-u}$. In short, existences of monomials $X^{i-u}Z^u$ for $i = 0, 1, \ldots, t, u = 0, 1, \ldots, i$ (that are equivalent to $X^i Y^u$ for the same set of indices) enable the transformation. Notice that the analysis requires a restriction $\tau \leq 1$. See [HM10] for the detailed analysis.

Ignoring low order terms of t, the dimension and the determinant of the lattices are computed as $n = (\frac{1}{2} + \frac{\tau}{2})t^2$ and $\det(\boldsymbol{B}) = X^{\frac{1}{6}t^3} Y^{\frac{\tau^2}{6}t^3} Z^{(\frac{1}{6}+\frac{\tau}{3})t^3} e^{(\frac{1}{3}+\frac{\tau}{6})t^3}$, respectively. The conditions for the (δ, β)-SIP to be solved, i.e., $(\det(\boldsymbol{B}))^{1/n} < e^t$, becomes

$$\delta \cdot \frac{1}{6} + \beta \cdot \frac{\tau^2}{6} + (\delta+\beta)\left(\frac{1}{6}+\frac{\tau}{3}\right) + \left(\frac{1}{3}+\frac{\tau}{6}\right) < \frac{1}{2}+\frac{\tau}{2},$$

$$\delta < \frac{1-\beta+2(1-\beta)\tau-\beta\tau^2}{2+2\tau}.$$

To maximize the right hand side of the inequality, we set the parameter $\tau = \sqrt{1/\beta} - 1$ and the condition becomes

$$\delta < 1 - \sqrt{\beta}.$$

Although the bound is the best, the algorithm does not work for an arbitrary $0 < \beta < 1$. Since the restriction $0 \leq \tau = \sqrt{1/\beta} - 1 \leq 1$, the algorithm works only when $1/4 \leq \beta \leq 1$.

Wiener Lattices. Weger [Weg02] also considered the generalization of Wiener's algorithm [Wie90] and obtained the bound (3).[2] The bound can be obtained by the special case of the Boneh-Durfee lattice. We fix the parameter $\tau = 1$ and obtain the condition (3),

$$\delta < \frac{3}{4} - \beta.$$

By the definition, the Wiener lattice is the special case of the stronger Boneh-Durfee lattices.

Blömer-May Lattices. Blömer and May [BM01] extracted other sublattices from the weaker Boneh-Durfee lattices and constructed an algorithm that solves the $(\delta, 1/2)$-SIP when $\delta < (\sqrt{6} - 1)/5$. Sarkar et al. [SMS08] generalized the lattice constructions and constructed an algorithm that solves the (δ, β)-SIP when the condition (4) $\delta < \frac{2}{5}\left(\sqrt{4\beta^2 - \beta + 1} - 3\beta + 1\right)$ holds.

Blömer and May defined sets of indices,

$$\mathcal{S}_x^{BM} := \{(i,u) | i = \lfloor (1-\mu)t \rfloor, \lfloor (1-\mu)t \rfloor + 1, \ldots, t; u = 0, 1, \ldots, i\} \quad \text{and}$$
$$\mathcal{S}_y^{BM} := \{(u,j) | u = \lfloor (1-\mu)t \rfloor, \lfloor (1-\mu)t \rfloor + 1, \ldots, t; j = 1, 2, \ldots, \lfloor u - (1-\mu)t \rfloor\}$$

with a parameter $0 \leq \mu < 1$. As the Boneh-Durfee lattices, the basis matrices generated by the polynomial selections are not triangular. Following the work of Herrmann and May [HM10], Kunihiro et al. [KSI11] used the same linearization $z = -1 + xy$ and transformed the basis matrices to be triangular. Applying the linearization appropriately and the basis matrices become triangular with diagonals $X^{i-u}Z^u e^{t-u}$ for $g^x_{[i,u]}(x,y)$ and $Z^u Y^j e^{t-u}$ for $g^y_{[u,j]}(x,y)$. See [KSI11] for the detailed analysis. Ignoring low order terms of t, the dimension and the determinant of the lattices are computed as $n = \mu t^2$ and $\det(B) = X^{\frac{3\mu - 3\mu^2 + \mu^3}{6} t^3} Y^{\frac{\mu^3}{6} t^3} Z^{\frac{\mu}{2} t^3} e^{\frac{\mu}{2} t^3}$, respectively. The conditions for the (δ, β)-SIP to be solved, i.e., $(\det(B))^{1/n} < e^t$, become

$$\delta \cdot \frac{3\mu - 3\mu^2 + \mu^3}{6} + \beta \cdot \frac{\mu^3}{6} + (\delta + \beta) \cdot \frac{\mu}{2} + \frac{\mu}{2} < \mu,$$

$$\delta < \frac{3 - 3\beta - \beta\mu^2}{6 - 3\mu + \mu^2}.$$

To maximize the right hand side of the inequality, we set the parameter $\mu = \left(1 + \beta - \sqrt{4\beta^2 - \beta + 1}\right)/\beta$ and the condition becomes

$$\delta < \frac{2}{5}\left(\sqrt{4\beta^2 - \beta + 1} - 3\beta + 1\right).$$

[2] In Boneh and Durfee's work [BD00], they obtain the Wiener's bound $\delta < 1/4$ for the $(\delta, 1/2)$-SIP [Wie90]. The bound can be obtained by the special case of the Boneh-Durfee lattice with the fixed parameter $\tau = 0$.

Although Sarkar et al. [SMS08] claimed the bound is the best when $3/35 \leq \beta < 1/4$ for the (δ, β)-SIP, it is incorrect. Since the restriction of the parameter $0 \leq \mu = \left(1 + \beta - \sqrt{4\beta^2 - \beta + 1}\right)/\beta < 1$, the algorithm works only when $1/4 < \beta \leq 1$. In this range, the bound (4) is weaker than the generalization of the Boneh-Durfee stronger bound (1).

Kunihiro-Shinohara-Izu Lattices. Kunihiro et al. [KSI11] considered a broader class of lattices for the (δ, β)-SIP. They defined sets of indices,

$$\mathcal{S}_x^{KSI} := \{(i,u) | i = \lfloor (1-\mu)t \rfloor, \lfloor (1-\mu)t \rfloor + 1, \ldots, t; u = 0, 1, \ldots, i\} \quad \text{and}$$
$$\mathcal{S}_y^{KSI} := \{(u,j) | u = \lfloor (1-\mu)t \rfloor, \lfloor (1-\mu)t \rfloor + 1, \ldots, t; j = 1, 2, \ldots, \lfloor \tau(u - (1-\mu)t) \rfloor\},$$

with two parameters $0 \leq \tau \leq 1$ and $0 \leq \mu < 1$. The sets are hybrid sets consisting of the stronger Boneh-Durfee lattices and the Blömer-May lattices. More concretely, the previous two lattices are the special cases of the Kunihiro-Shinohara-Izu lattices; when $\tau = 1$ (resp. $\mu = 1$), the sets $\mathcal{S}_x^{KSI}$ and $\mathcal{S}_y^{KSI}$ become the same as the sets $\mathcal{S}_x^{sBD}$ and $\mathcal{S}_y^{sBD}$ (resp. $\mathcal{S}_x^{BM}$ and $\mathcal{S}_y^{BM}$).

As the stronger Boneh-Durfee lattices and the Blömer-May lattices, the basis matrices generated by the polynomial selections are not triangular. Kunihiro et al. [KSI11] used a linearization $z = -1 + xy$ and transformed the basis matrices to be triangular. Applying the linearization appropriately and the basis matrices become triangular with diagonals $X^{i-u}Z^u e^{t-u}$ for $g^x_{[i,u]}(x,y)$ and $Z^u Y^j e^{t-u}$ for $g^y_{[u,j]}(x,y)$. See [KSI11] for the detailed analysis. Ignoring low order terms of t, the dimension and the determinant of the lattices are computed as $n = \frac{(2\mu-\mu^2)+\mu^2\tau}{2}t^2$ and $\det(B) = X^{\frac{3\mu-3\mu^2+\mu^3}{6}t^3} Y^{\frac{\mu^3\tau^2}{6}t^3} Z^{\frac{(3\mu-3\mu^2+\mu^3)+(3\mu^2-\mu^3)\tau}{6}t^3} e^{\frac{(3\mu-\mu^3)+\mu^3\tau}{6}t^3}$, respectively. The conditions for the (δ, β)-SIP to be solved, i.e., $(\det(\boldsymbol{B}))^{1/n} < e^t$, become

$$\delta \cdot \frac{3\mu - 3\mu^2 + \mu^3}{6} + \beta \cdot \frac{\mu^3\tau^2}{6} + (\delta + \beta) \cdot \frac{(3\mu - 3\mu^2 + \mu^3) + (3\mu^2 - \mu^3)\tau}{6} + \frac{(3\mu - \mu^3) + \mu^3\tau}{6}$$
$$< \frac{(2\mu - \mu^2) + \mu^2\tau}{2},$$

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

When $1/4 \leq \beta < 1$, we set the parameter $\mu = 1, \tau = \sqrt{1/\beta} - 1$, and obtain the bound $\delta < 1 - \sqrt{\beta}$ that is the same as the stronger Boneh-Durfee lattices. When $0 < \beta < 1/4$, we set the parameter $\mu = 1, \tau = 1$, and obtain the bound $\delta < 3/4 - \beta$ that is the same as Wiener's Lattice.[3]

4 New Lattice Constructions to Solve the (δ, β)-SIP

In this section, we propose an improved algorithm to solve the (δ, β)-SIP. Inspired by the work of [KSI11], we consider a broader class of lattices that contains the weaker and stronger Boneh-Durfee lattices, and the Wiener lattices for special cases. The three lattices provide the best results among

[3] Although Kunihiro et al. [KSI11] claimed the lattices yield the bound (4) when $0 < \beta < 1/4$, the result is not correct as noted above.

previous results [Weg02, SMS08, KSI11]. When $1/4 \leq \beta < 1$, our hybrid lattices become the same as the stronger Boneh-Durfee lattices and yield the bound (1). When $0 < \beta < 1/4$, our lattices make use of the properties of the three lattices, i.e., the weaker and stronger Boneh-Durfee lattices, and the Wiener lattices, simultaneously and obtain the following improved result.

Theorem 1. *We can solve the (δ, β)-SIP when*

$$\delta < 1 - \sqrt{\beta} \quad \textit{for} \;\; 1/4 \leq \beta < 1,$$
$$\delta < 1 - \frac{2}{3}\left(\sqrt{(3+4\beta)\beta} - \beta\right) \quad \textit{for} \;\; 0 < \beta < \frac{1}{4},$$

in polynomial time.

4.1 The Lattice Construction

To solve the SIP, we define sets of indices

$$\mathcal{S}_x := \{(i,u) | i = 0, 1, \ldots, t; u = 0, 1, \ldots, i\} \quad \text{and} \quad \mathcal{S}_y := \{(u,j) | u = 0, 1, \ldots, t; j = 1, 2, \ldots, \lfloor \eta t + \tau u \rfloor\}$$

with two parameters $\eta \geq 0$ and $0 \leq \tau \leq 1$. The sets are hybrid sets with the weaker and stronger Boneh-Durfee lattices, and the Wiener lattices. More concretely, the previous three lattices are the special cases of our lattices; when $\tau = 0$ (resp. $\eta = 0$), the sets $\mathcal{S}_x$ and $\mathcal{S}_y$ become the same as the sets $\mathcal{S}_x^{wBD}$ and $\mathcal{S}_y^{wBD}$ (resp. $\mathcal{S}_x^{sBD}$ and $\mathcal{S}_y^{sBD}$). Since the Wiener lattice is the special case of the stronger Boneh-Durfee lattices, the Wiener lattice is the special case of our lattices.

Our selections of polynomials generate basis matrices $\boldsymbol{B}$ that are not triangular. However, as Herrmann and May's analysis, we use a linearization $z = -1 + xy$ and the matrices can be transformed into triangular with diagonals $X^{i-u}Z^u e^{t-u}$ for $g^x_{[i,u]}(x,y)$ and $Z^u Y^j e^{t-u}$ for $g^y_{[u,j]}(x,y)$. The analysis is almost trivial from the previous analyses. At first, as the case of the weaker Boneh-Durfee lattice, polynomials in $\mathcal{S}_x$ and $\mathcal{S}_y$ for $j = 1, 2, \ldots, \lfloor \eta t \rfloor$ generate a triangular matrix with diagonals $X^i Y^u e^{t-u}$ for $\mathcal{S}_x$ and $X^u Y^{u+j} e^{t-u}$ for $\mathcal{S}_y$ and $j = 1, 2, \ldots, \lfloor \eta t \rfloor$. When the linearization $z = -1 + xy$ is applied to the polynomials, the matrix is still triangular with diagonals $X^{i-u}Z^u e^{t-u}$ for $g^x_{[i,u]}(x,y)$ and $Z^u Y^j e^{t-u}$ for $g^y_{[u,j]}(x,y)$. Hence, what we have to show is that the matrix is still triangular when we use extra polynomials in $\mathcal{S}_y$ for $u = 0, 1, \ldots, t, j = \lfloor \eta t \rfloor + 1, \lfloor \eta t \rfloor + 2, \ldots, \lfloor \eta t + \tau u \rfloor$. Notice that there are monomials $X^i Y^u$ for $i = 0, 1, \ldots, t, u = \lfloor \eta t \rfloor, \lfloor \eta t \rfloor + 1, \ldots, \lfloor \eta t \rfloor + i$ that correspond to diagonals for $\mathcal{S}_x$ and for $\mathcal{S}_y$ and $j = 1, 2, \ldots, \lfloor \eta t \rfloor$. The extra polynomials $g^y_{[u,j]}(x,y)$ for $u = 0, 1, \ldots, t, j = \lfloor \eta t \rfloor + 1, \lfloor \eta t \rfloor + 2, \ldots, \lfloor \eta t + \tau u \rfloor$ are (almost) equivalent to $y^{\lfloor \eta t \rfloor}$ times $g^y_{[u,j]}(x,y)$ with indices in $\mathcal{S}_y^{sBD}$. Therefore, as the Boneh-Durfee stronger lattice, the existences of the monomials $X^i Y^u$ for $i = 0, 1, \ldots, t, u = \lfloor \eta t \rfloor, \lfloor \eta t \rfloor + 1, \ldots, \lfloor \eta t \rfloor + i$ preserve the matrix with the extra polynomials to be triangular by using the linearization $z = -1 + xy$. The diagonals for the extra polynomials are $Z^u Y^j e^{t-u}$.

The dimension and the determinant of the lattices $\det(\boldsymbol{B}) = X^{s_X} Y^{s_Y} Z^{s_Z} e^{s_e}$ are computed by

$$n = \sum_{i=0}^{t} \sum_{u=0}^{i} 1 + \sum_{u=0}^{t} \sum_{j=1}^{\lfloor \eta t + \tau u \rfloor} 1 = \left(\frac{1}{2} + \eta + \frac{\tau}{2}\right) t^2 + o(t^2),$$

$$s_X + s_Z = \sum_{i=0}^{t}\sum_{u=0}^{i} i + \sum_{u=0}^{t}\sum_{j=1}^{\lfloor \eta t+\tau u\rfloor} u = \left(\frac{1}{3}+\frac{\eta}{2}+\frac{\tau}{3}\right)t^3 + o(t^3),$$

$$s_Y + s_Z = \sum_{i=0}^{t}\sum_{u=0}^{i} u + \sum_{u=0}^{t}\sum_{j=1}^{\lfloor \eta t+\tau u\rfloor} (u+j) = \left(\frac{1}{6}+\frac{\eta}{2}+\frac{\tau}{3}+\frac{\eta^2}{2}+\frac{\tau\eta}{2}+\frac{\tau^2}{6}\right)t^3 + o(t^3),$$

$$s_e = \sum_{i=0}^{t}\sum_{u=0}^{i} (m-u) + \sum_{u=0}^{t}\sum_{j=1}^{\lfloor \eta t+\tau u\rfloor} (t-u) = \left(\frac{1}{3}+\frac{\eta}{2}+\frac{\tau}{6}\right)t^3 + o(t^3).$$

Ignoring low order terms of t, the conditions for the (δ,β)-SIP to be solved, i.e., $(\det(\boldsymbol{B}))^{1/n} < e^t$, become

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

When $1/4 \le \beta < 1$, to maximize the right hand side of the inequality, we set the parameter $\eta = 0$ and $\tau = \sqrt{1/\beta}-1$, and obtain the bound

$$\delta < 1-\sqrt{\beta}$$

that is the same as the bound (1).

When $0 < \beta < 1/4$, we set the parameter

$$\eta = \frac{-4\beta+\sqrt{\beta(3+4\beta)}}{3\beta} \quad \text{and} \quad \tau = 1,$$

and obtain the bound

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

This bound is the best among all known results [Weg02, SMS08, KSI11] when $0 < \beta < 1/4$.

4.2 An Observation of the Lattice

Although the lattice construction is obtained by a simple combination of the previous three lattices, i.e., the weaker and the stronger Boneh-Durfee lattice and the Wiener lattice, the construction should be appropriate. To show the fact, we introduce *helpful polynomials*. The notion was introduced by May [May10] and Takayasu and Kunihiro [TK13] made use of the notion and proposed improved lattice constructions. In lattice constructions to solve modular equations, we call polynomials helpful if the absolute values of the diagonals are smaller than the modulus in triangular basis matrices. Helpful polynomials enable us to solve modular equations for larger solutions since the polynomials reduce the norm of vectors output by the LLL algorithm. Takayasu and Kunihiro suggested that as many helpful polynomials as possible should be selected in lattice constructions as long as the basis matrices are triangular.

To solve the (δ,β)-SIP for $1/4 \le \beta < 1$ and $\delta < 1-\sqrt{\beta}$, the above lattice (that is equivalent to the stronger Boneh-Durfee lattice) contains as many helpful polynomials as possible. That means all

$g^y_{[u,j]}(x,y)$ in the lattice basis are helpful polynomials and other $g^y_{[u,j]}(x,y)$ are not helpful since the diagonals $Z^uY^je^{t-u}$ for the polynomials $g^y_{[u,j]}(x,y)$ with indices in $u=0,1,\ldots,t, j \le \left(\sqrt{1/\beta}-1\right)u$ are always equivalent to or smaller than the modulus e^t and and those for the polynomial with indices in $j > \left(\sqrt{1/\beta}-1\right)u$ are larger than e^t:

$$Z^uY^je^{t-u} \le e^t \Leftrightarrow \left(1-\sqrt{\beta}+\beta\right)u + \beta j \le u \Leftrightarrow j \le \left(\sqrt{1/\beta}-1\right)u.$$

Although not all $g^x_{[i,u]}(x,y)$ in lattice basis are helpful, they contribute the basis matrices to be triangular.

As we explained, the lattice construction is valid only when $\sqrt{1/\beta}-1 \le 1$, i.e., $\beta \ge 1/4$, since the unravelled linearization does not work well otherwise. Then we consider to solve the (δ,β)-SIP for $0<\beta<1/4$ and $\delta < 1-\frac{2}{3}\left(\sqrt{(3+4\beta)\beta}-\beta\right)$. In this case, not all $g^y_{[u,j]}(x,y)$ in the lattice basis are helpful and not all helpful $g^y_{[u,j]}(x,y)$ are in the lattice basis. However, our lattice construction is the best possible. For the series of $g^y_{[u,j]}(x,y)$ for $u=0,1,\ldots,t, j=\eta t+u$ with some η, the corresponding diagonals in the lattice basis are

$$Z^uY^{\eta t+u}e^{t-u} = N^{(\beta+\delta)u+\beta(\eta t+u)+t-u} \le N^{-\frac{2}{3}\left(\sqrt{(3+4\beta)\beta}-4\beta\right)u+(1+\eta\beta)t}.$$

Since $\beta < 1/4$, $\sqrt{(3+4\beta)\beta}-4\beta > 0$ and the diagonals become smaller for larger u. Hence, if possible, we want to select only $g^y_{[u,j]}(x,y)$ for larger u in the lattice basis, however, unravelled linearization does not work well without $g^y_{[u,j]}(x,y)$ for smaller u. Therefore, the best possible lattice construction is collecting as many helpful series of $g^y_{[u,j]}(x,y)$ for $u=0,1,\ldots,t, j=\eta t+u$ as possible. The helpful series of $g^y_{[u,j]}(x,y)$ for $u=0,1,\ldots,t, j=\eta t+u$ means the geometric mean of all the diagonals is smaller than the modulus e^t. The geometric mean is calculated as

$$\left(\prod_{u=0}^{t} Z^uY^{\eta t+u}e^{t-u}\right)^{1/(t+1)} \le N^{-\frac{1}{3}\left(\sqrt{(3+4\beta)\beta}-4\beta\right)t+(1+\eta\beta)t} = N^{\left(1-\frac{1}{3}\left(\sqrt{(3+4\beta)\beta}-(4+3\eta)\beta\right)\right)t}.$$

Hence, the series of $g^y_{[u,j]}(x,y)$ becomes helpful when the geometric mean is smaller than $e^t \approx N^t$, that is,

$$\sqrt{(3+4\beta)\beta}-(4+3\eta)\beta \ge 0 \Leftrightarrow \eta \le \frac{-4\beta+\sqrt{\beta(3+4\beta)}}{3\beta}.$$

The analysis suggests that our lattice contains all helpful series of $g^y_{[u,j]}(x,y)$ for $u=0,1,\ldots,t, j=\eta t+u$.

5 On the Security of Multi-Prime RSA

In this section, we consider the security of Multi-Prime RSA for small differences of the prime factors of the Multi-Prime RSA modulus. We write the Multi-Prime RSA modulus as $N=p_1p_2\cdots p_k$

and assume the following two conditions $p_1 > p_2 > \cdots > p_k$ without loss of generality, and $|p_1 - p_k| < N^\gamma$. Define $p'_j = N/p_j$ and

$$\Delta_k = \sum_{j=1}^{k} p'_j - k \left(\prod_{j=1}^{k} p'_j \right)^{1/k}.$$

By definition, $p'_1 < p'_2 < \cdots < p'_k$ and $k \left(\prod_{j=1}^{k} p'_j \right)^{1/k} = kN^{(k-1)/k}$ holds.

In [ZT13, ZT14], Zhang and Takagi analyzed the security. They revealed that Multi-Prime RSA becomes insecure if we can solve the (δ, β)-SIP.

Lemma 2 (Proposition 1 and Theorem 2 of [ZT13])**.** *Let $N = p_1 p_2 \cdots p_k$ with $p_1 > p_2 > \cdots > p_k$ be a Multi-Prime RSA modulus. All prime factors of N are the same bit size and $p_1 - p_k < N^\gamma$, $0 < \gamma < 1/k$. Let e be a full size public exponent whose corresponding secret exponent d is smaller than N^δ. When $\Delta_k = \sum_{j=1}^{k} p'_j - k \left(\prod_{j=1}^{k} p'_j \right)^{1/k}$ is smaller than N^β, if we can solve the (δ, β)-SIP, we can factor the Multi-Prime RSA modulus N.*

For the attack, bounding the size of Δ_k is crucial. Although Zhang and Takagi [ZT14] obtained a similar bound, i.e., $0 < \Delta_k < poly(k) \cdot N^{2\gamma+1-3/k}$ from Proposition 1 of [ZT14], we show a slightly better bound.

Lemma 3. *Let $N = p_1 p_2 \cdots p_k$ be composite integers and Δ_k be defined as in Lemma 2, then*

$$0 < \Delta_k < 2(k-1) \cdot N^{2\gamma+1-3/k}.$$

We prove the lemma in A although the bound is almost the same as that of [ZT14] and the improvement is not very important.

Since we proposed an improved algorithm for the (δ, β)-SIP, i.e., Theorem 1, we can improve the cryptanalysis of Multi-Prime RSA. Combining Lemma 2, Lemma 3, and Theorem 1, we obtain the following result.

Theorem 2. *Let the Multi-Prime RSA modulus N, public (resp. secret) exponent e (resp. d) as in Lemma 2. We can factor the Multi-Prime RSA modulus N when*

$$\delta < 1 - \sqrt{1 + 2\gamma - 3/k} \qquad \text{for } \frac{3}{2}\left(\frac{1}{k} - \frac{1}{4}\right) \le \gamma < \frac{1}{k},$$

$$\delta < 1 - \frac{2}{3}\left(\sqrt{(7 + 8\gamma - 12/k)(1 + 2\gamma - 3/k)} - 1 - 2\gamma + 3/k\right) \quad \text{for } 0 < \gamma < \frac{3}{2}\left(\frac{1}{k} - \frac{1}{4}\right).$$

6 Conclusion

In this paper, we studied the (δ, β)-SIP for an arbitrary β that relates to the security of Multi-Prime RSA. Unlike the results of the $(\delta, 1/2)$-SIP [BD00, BM01, HM10], the results for the general

(δ, β)-SIP are not widely known. Indeed, some previous results reconstruct the algorithm to solve the problem, which had already been proved, and did not refer to the previous works. Therefore, one of the contributions of this paper is to summarize the previous results [BD00, BM01, Weg02, SMS08, HM10, KSI11]. Moreover, we revealed that the bound (4) proposed by previous works [SMS08, KSI11] is not valid.

The main contribution of the paper was to provide the improved lattice construction for the (δ, β)-SIP. Our lattice covers a broader class and previous results [BD00, Weg02] that provide the best bounds among previous works are special cases of our lattice. The lattice makes better use of the algebraic structures of modular polynomials and we improved the previous bound.

Based on the improvement, we also showed the improved analysis for the security of Multi-Prime RSA. Our result showed that Multi-Prime RSA is vulnerable than expected when differences of prime factors are small.

Acknowledgement. We would like to thank members of the study group "Shin-Akarui-Angou-Benkyou-Kai" for their helpful comments.

References

[Aon09] Y. Aono, "A new lattice construction for partial key exposure attack for RSA," Proc. PKC 2009, LNCS 5443, pp. 34–53, Springer, 2009.

[AASW12] 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.

[BBN12] H. M. Bahig, A. Bhery and D. I. Nassr, "Cryptanalysis of multi-prime RSA with small prime difference," Proc. ICICS 2012, LNCS 7618, pp. 33–44, Springer, 2012.

[BJ07] A. Bauer and A. Joux, "Toward a rigorous variation of Coppersmiths algorithm on three variables," Proc. Eurocrypt 2007, LNCS 4514, pp. 361–378, Springer, 2007.

[BCC+13] D. J. Bernstein, Y. Chang, C. -M. Cheng, L. -P. Chou, N. Heninger, T. Lange, and N. van Someren, "Factoring RSA keys from certified smart cards: Coppersmith in the wild," Proc. Asiacrypt 2013, LNCS 8270, pp. 341–360, Springer, 2013.

[BM01] J. Blömer and A. May, "Low secret exponent RSA revisited," Proc. CaLC 2001, LNCS 2146, pp. 4–19, Springer, 2001.

[BM03] J. Blömer and A. May, "New partial key exposure attacks on RSA," Proc. Crypto 2003, LNCS 2729, pp. 27–43, Springer, 2003.

[BD00] 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.

[CKL+02] M. Ciet, F. Koeune, F. Laguillaumie and J. -J. Quisquater, "Short private exponent attacks on fast variants of RSA," UCL Crypto Group Technical Report Series CG-2002/4, University Catholique de Louvain, 2002.

[Cop96] D. Coppersmith, "Finding a small root of a univariate modular equation," Proc. Eurocrypt 1996, LNCS 1070, pp. 155–165, Springer, 1996.

[Cop97] D. Coppersmith, "Small solutions to polynomial equations, and low exponent RSA vulnerabilities," J. Cryptology, vol. 10, no. 4, pp. 233–260, 1997.

[Cop01] D. Coppersmith, "Finding small solutions to small degree polynomials," Proc. CaLC 2001, LNCS 2146, pp. 20–31, Springer, 2001.

[DN00] 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, 2000.

[EJMW05] 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, 2005.

[HM09] 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, 2009.

[HM10] 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, 2010.

[How97] N. Howgrave-Graham, "Finding small roots of univariate modular equations revisited," Proc. Cryptography and Coding, LNCS 1355, pp. 1331–142, 1997.

[IKK08a] 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 [IKK08b].

[IKK08b] 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.

[Kun11] N. Kunihiro, "Solving generalized the small inverse problem," IEICE Transactions 94-A, no. 6, pp. 1274–1284, 2011.

[Kun12] 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.

[KSI11] 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.

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

[May03] A. May, "New RSA vulnerabilities using lattice reduction methods," PhD thesis, University of Paderborn, 2003.

[May10] A. May, "Using lll-reduction for solving RSA and factorization problems: A survey," Available from http://www.cits.rub.de/permonen/may.html, 2010.

[NS01] P. Q. Nguyen and J. Stern, "The two faces of lattices in cryptology," Proc. CaLC 2001, LNCS 2146, pp. 146–180, Springer, 2001.

[SGM10] S. Sarkar, S. Sen Gupta and S. Maitra, "Partial key exposure attack on RSA - Improvements for limited lattice dimensions," Proc. Indocrypt 2010, LNCS 6498 , pp. 2–16, Springer, 2010.

[SMS08] S. Sarkar, S. Maitra and S. Sarkar, "RSA cryptanalysis with increased bounds on the secret exponent using less lattice dimension," IACR ePrint Archive: Report 2008/315, 2008.

[TK13] A. Takayasu and N. Kunihiro, "Better lattice constructions for solving multivariate linear equations modulo unknown divisors," Proc. ACISP 2013, LNCS 7959, pp. 118–135, Springer, 2013.

[TK14a] A. Takayasu and N. Kunihiro, "Partial key exposure attacks on RSA: Achieving the Boneh-Durfee bound," Proc. SAC 2014, LNCS 87871, pp.345–362, Springer, 2014.

[TK14b] 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.

[Weg02] B. de Weger, "Cryptanalysis of RSA with small prime difference, applicable algebra in engineering," Communication and Computing 13, pp. 17–28, 2002.

[Wie90] M. J. Wiener, "Cryptanalysis of short RSA secret exponents," IEEE Trans. inf. theory, vol. 36, (3), pp. 553–558, 1990.

[ZT13] H. Zhang and T. Takagi, "Attacks on multi-prime RSA with small prime difference," Proc. ACISP 2013, LNCS 7959, pp. 41–56, Springer, 2013.

[ZT14] 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.

A Proof of Lemma 3

Zhang and Takagi [ZT14] used Newton's Generalized Binomial Theorem to bound the size of Δ_k. See [ZT14] for detailed information. Since small $k = 3, 4, 5$ are used in standard settings of Multi-Prime RSA, the term $poly(k)$ can be assumed to be much smaller than N. Therefore, Zhang and Takagi did not analyze the term in detail.

We give an alternative proof for Lemma 3 that does not use Newton's Generalized Binomial Theorem. Moreover, our proof shows $poly(k) = 2(k-1)$. Hence, our result justifies the assumption, e.g., the term $poly(k)$ is much smaller than N. To prove it, we use the following Lemma 4 and Lemma 5. In all following equations, if all indices j for p_j in summations are larger than k, let j be $j - k$.

Lemma 4. *Let $N = p_1 p_2 \cdots p_k$ be composite integers and Δ_k be defined as in Lemma 2, then*

$$\Delta_k = \frac{1}{2} \sum_{u=0}^{k-2} \sum_{j=1}^{k} \sum_{l=0}^{k-u-2} \mathcal{P}_{u,j}^{1/k} p_j'^{(k-u-l-2)/k} p_{j+u+1}'^{l/k} \left(p_j'^{1/k} - p_{j+u+1}'^{1/k} \right)^2,$$

where

$$\mathcal{P}_{u,j} = \begin{cases} 1 & \text{for } u = 0, \\ p'_{j+1} p'_{j+2} \cdots p'_{j+u} & \text{for } u = 1, 2, \ldots, k-2. \end{cases}$$

The proof of Lemma 4 is written at the end of this section.

Lemma 5. *Let $N = p_1 p_2 \cdots p_k$ be composite integers, then*

$$\left| p_i'^{1/k} - p_j'^{1/k} \right| \leq \frac{2^{(k+1)/k}}{k} \cdot N^{\gamma - 1/k^2},$$

for all $i, j = 1, 2, \ldots, k, i \neq j$.

Proof. By definition,

$$\left| p_i'^{1/k} - p_j'^{1/k} \right| = \left| \frac{1}{p_i^{1/k}} - \frac{1}{p_j^{1/k}} \right| \cdot N^{1/k} = \left| \frac{p_j^{1/k} - p_i^{1/k}}{p_i^{1/k} p_j^{1/k}} \right| \cdot N^{1/k}.$$

By definition, since $p_1 > p_2 > \cdots > p_k$,

$$< \frac{p_1^{1/k} - p_k^{1/k}}{p_k^{2/k}} \cdot N^{1/k} = \frac{p_1 - p_k}{p_k^{2/k} \sum_{l=0}^{k-1} p_1^{(k-l-1)/k} p_k^{l/k}} \cdot N^{1/k} < \frac{p_1 - p_k}{p_k^{2/k} \sum_{l=0}^{k-1} p_k^{(k-1)/k}} \cdot N^{1/k}$$
$$= \frac{p_1 - p_k}{k p_k^{(k+1)/k}} \cdot N^{1/k}.$$

By definition, all prime factors $p_1, p_2, \cdots, p_k$ are the same bit size. Hence, $p_k > \frac{1}{2} N^{1/k}$ holds, and

$$< \frac{N^{\gamma}}{k \left(\frac{1}{2} N^{1/k} \right)^{(k+1)/k}} \cdot N^{1/k} = \frac{2^{(k+1)/k}}{k} \cdot N^{\gamma - 1/k^2}$$

as required. □

Combining Lemma 4 and Lemma 5, we can prove Lemma 3 as follows.

Proof. From Lemma 4,

$$\Delta_k = \frac{1}{2}\sum_{u=0}^{k-2}\sum_{j=1}^{k}\sum_{l=0}^{k-u-2} \mathcal{P}_{u,j}^{1/k} p_j'^{(k-u-l-2)/k} p_{j+u+1}'^{l/k} \left(p_j'^{1/k} - p_{j+u+1}'^{1/k}\right)^2.$$

By splitting the summation into two parts with respect to $u = 0$ and $u = 1, 2, \ldots, k$,

$$\begin{aligned}
=&\frac{1}{2}\sum_{j=1}^{k}\sum_{l=0}^{k-2} p_j'^{(k-l-2)/k} p_{j+1}'^{l/k} \left(p_j'^{1/k} - p_{j+1}'^{1/k}\right)^2 \\
&+ \frac{1}{2}\sum_{u=1}^{k-2}\sum_{j=1}^{k}\sum_{l=0}^{k-u-2} \left(p'_{j+1}p'_{j+2}\cdots p'_{j+u}\right)^{1/k} \cdot p_j'^{(k-u-l-2)/k} p_{j+u+1}'^{l/k} \left(p_j'^{1/k} - p_{j+u+1}'^{1/k}\right)^2. \qquad (6)
\end{aligned}$$

By definition, since $p'_1 < p'_2 < \cdots < p'_k$, we bound the first summation of equation (6) as

$$\begin{aligned}
\frac{1}{2}\sum_{j=1}^{k}\sum_{l=0}^{k-2} p_j'^{(k-l-2)/k} p_{j+1}'^{l/k} \left(p_j'^{1/k} - p_{j+1}'^{1/k}\right)^2 <& \frac{1}{2}\sum_{j=1}^{k}\sum_{l=0}^{k-2} p_k'^{(k-2)/k} \left(p_k'^{1/k} - p_1'^{1/k}\right)^2 \\
=& \frac{1}{2}k(k-1)p_k'^{(k-2)/k} \left(p_k'^{1/k} - p_1'^{1/k}\right)^2.
\end{aligned}$$

As the proof of Lemma 5, since $p_k > \frac{1}{2}N^{1/k}$, $p'_k = N/p_k < 2N^{(k-1)/k}$ holds, then

$$< \frac{1}{2}k(k-1)\left(2N^{(k-1)/k}\right)^{(k-2)/k} \cdot \left(p_k'^{1/k} - p_1'^{1/k}\right)^2 = \frac{1}{2^{2/k}}k(k-1)N^{(k-1)(k-2)/k^2} \cdot \left(p_k'^{1/k} - p_1'^{1/k}\right)^2.$$

By Lemma 5,

$$< \frac{1}{2^{2/k}}k(k-1)N^{(k-1)(k-2)/k^2} \cdot \left(\frac{2^{(k+1)/k}}{k}N^{\gamma-1/k^2}\right)^2 = \frac{4(k-1)}{k}N^{2\gamma+1-3/k}.$$

Next, we bound the second summation of equation (6). By definition, since $p'_1 < p'_2 < \cdots < p'_k$,

$$\begin{aligned}
&\frac{1}{2}\sum_{u=1}^{k-2}\sum_{j=1}^{k}\sum_{l=0}^{k-u-2} \left(p'_{j+1}p'_{j+2}\cdots p'_{j+u}\right)^{1/k} \cdot p_j'^{(k-u-l-2)/k} p_{j+u+1}'^{l/k} \left(p_j'^{1/k} - p_{j+u+1}'^{1/k}\right)^2 \\
<&\frac{1}{2}\sum_{u=1}^{k-2}\sum_{j=1}^{k}\sum_{l=0}^{k-u-2} p_k'^{(k-2)/k} \left(p_k'^{1/k} - p_1'^{1/k}\right)^2 = \frac{(k-2)(k-1)k}{4} \cdot p_k'^{(k-2)/k} \left(p_k'^{1/k} - p_1'^{1/k}\right)^2.
\end{aligned}$$

Since $p'_k < 2N^{(k-1)/k}$,

$$\begin{aligned}
&< \frac{(k-2)(k-1)k}{4} \cdot \left(2N^{(k-1)/k}\right)^{(k-2)/k} \cdot \left(p_k'^{1/k} - p_1'^{1/k}\right)^2 \\
&= \frac{(k-2)(k-1)k}{2^{(k+2)/k}} \cdot N^{(k-1)(k-2)/k^2} \cdot \left(p_k'^{1/k} - p_1'^{1/k}\right)^2.
\end{aligned}$$

By Lemma 5,

$$< \frac{(k-2)(k-1)k}{2^{(k+2)/k}} \cdot N^{(k-1)(k-2)/k^2} \cdot \left(\frac{2^{(k+1)/k}}{k} N^{\gamma - 1/k^2} \right)^2 = \frac{2(k-2)(k-1)}{k} N^{2\gamma+1-3/k}.$$

Therefore, Δ_k is bounded above by

$$\Delta_k < \frac{4(k-1)}{k} N^{2\gamma+1-3/k} + \frac{2(k-2)(k-1)}{k} N^{2\gamma+1-3/k} = 2(k-1)N^{2\gamma+1-3/k}$$

as required. □

In the rest of the paper, we prove Lemma 4.

Proof. We show the following equation

$$\begin{aligned}\sum_{j=1}^{k} p'_j =& \frac{1}{2} \sum_{j=1}^{k} \sum_{l=0}^{k-2} \left(p_j'^{1/k} - p_{j+1}'^{1/k} \right)^2 p_j'^{(k-l-2)/k} p_{j+1}'^{l/k} + k \left(\prod_{j=1}^{k} p'_j \right)^{1/k} \\ &+ \frac{1}{2} \sum_{u=1}^{k-2} \sum_{j=1}^{k} \sum_{l=0}^{k-u-2} \left(p'_{j+1} p'_{j+2} \cdots p'_{j+u} \right)^{1/k} \cdot p_j'^{(k-u-l-2)/k} p_{j+u+1}'^{l/k} \left(p_j'^{1/k} - p_{j+u+1}'^{1/k} \right)^2\end{aligned}$$

that is equivalent to the equation of Lemma 4.

For all $u = 2, 3, \cdots, k$,

$$\begin{aligned}\left(p_i'^{1/k} - p_j'^{1/k} \right)^2 \sum_{l=0}^{u-2} p_i'^{(u-l-2)/k} p_j'^{l/k} &= \left(p_i'^{1/k} - p_j'^{1/k} \right) \left(p_i'^{(u-1)/k} - p_j'^{(u-1)/k} \right) \\ &= p_i'^{u/k} + p_j'^{u/k} - p_i'^{1/k} p_j'^{(u-1)/k} - p_i'^{(u-1)/k} p_j'^{1/k}.\end{aligned}$$

Hence,

$$p_i'^{u/k} + p_j'^{u/k} = \left(p_i'^{1/k} - p_j'^{1/k} \right)^2 \sum_{l=0}^{u-2} p_i'^{(u-l-2)/k} p_j'^{l/k} + p_i'^{1/k} p_j'^{(u-1)/k} + p_i'^{(u-1)/k} p_j'^{1/k}. \tag{7}$$

Next, by the equation (7),

$$\begin{aligned}&\sum_{j=1}^{k} \left(p'_{j+1} p'_{j+2} \cdots p'_{j+u} \right)^{1/k} \left(p_j'^{(k-u)/k} + p_{j+u+1}'^{(k-u)/k} \right) \\ =& \sum_{j=1}^{k} \left(p'_{j+1} p'_{j+2} \cdots p'_{j+u} \right)^{1/k} \\ &\cdot \left(\left(p_j'^{1/k} - p_{j+u+1}'^{1/k} \right)^2 \sum_{l=0}^{k-u-2} p_j'^{(k-u-l-2)/k} p_{j+u+1}'^{l/k} + p_j'^{1/k} p_{j+u+1}'^{(k-u-1)/k} + p_j'^{(k-u-1)/k} p_{j+u+1}'^{1/k} \right)\end{aligned}$$

$$
\begin{aligned}
=&\sum_{j=1}^{k}\sum_{l=0}^{k-u-2}\left(p'_{j+1}p'_{j+2}\cdots p'_{j+u}\right)^{1/k}\cdot\left(p_j'^{1/k}-p_{j+u+1}'^{1/k}\right)^2 p_j'^{(k-u-l-2)/k}p_{j+u+1}'^{l/k}\\
&+\sum_{j=1}^{k}\left(p'_{j+1}p'_{j+2}\cdots p'_{j+u}\right)^{1/k}\cdot\left(p_j'^{1/k}p_{j+u+1}'^{(k-u-1)/k}+p_j'^{(k-u-1)/k}p_{j+u+1}'^{1/k}\right).
\end{aligned}
$$

From the standard calculation, we slide the indices of the second term as

$$
\begin{aligned}
=&\sum_{j=1}^{k}\sum_{l=0}^{k-u-2}\left(p'_{j+1}p'_{j+2}\cdots p'_{j+u}\right)^{1/k}\cdot\left(p_j'^{1/k}-p_{j+u+1}'^{1/k}\right)^2 p_j'^{(k-u-l-2)/k}p_{j+u+1}'^{l/k}\\
&+\sum_{j=1}^{k}\left(\left(p'_jp'_{j+1}\cdots p'_{j+u}\right)^{1/k}\cdot p_{j+u+1}'^{(k-u-1)/k}+\left(p'_{j+1}p'_{j+2}\cdots p'_{j+u+1}\right)^{1/k}p_j'^{(k-u-1)/k}\right)\\
=&\sum_{j=1}^{k}\sum_{l=0}^{k-u-2}\left(p'_{j+1}p'_{j+2}\cdots p'_{j+u}\right)^{1/k}\cdot\left(p_j'^{1/k}-p_{j+u+1}'^{1/k}\right)^2 p_j'^{(k-u-l-2)/k}p_{j+u+1}'^{l/k}\\
&+\sum_{j=1}^{k}\left(p'_{j+1}p'_{j+2}\cdots p'_{j+u+1}\right)^{1/k}\left(p_j'^{(k-u-1)/k}+p_{j+u+2}'^{(k-u-1)/k}\right). \qquad (8)
\end{aligned}
$$

Again, by the equation (7) for $u=k$,

$$
\begin{aligned}
\sum_{j=1}^{k}p'_j=&\frac{1}{2}\sum_{j=1}^{k}\left(p'_j+p'_{j+1}\right)\\
=&\frac{1}{2}\sum_{j=1}^{k}\sum_{l=0}^{k-2}\left(p_j'^{1/k}-p_{j+1}'^{1/k}\right)^2 p_j'^{(k-l-2)/k}p_{j+1}'^{l/k}+\frac{1}{2}\sum_{j=1}^{k}\left(p_j'^{1/k}p_{j+1}'^{(k-1)/k}+p_j'^{(k-1)/k}p_{j+1}'^{1/k}\right).
\end{aligned}
$$

From the standard calculation, we slide the indices of the second term as

$$
\begin{aligned}
=&\frac{1}{2}\sum_{j=1}^{k}\sum_{l=0}^{k-2}\left(p_j'^{1/k}-p_{j+1}'^{1/k}\right)^2 p_j'^{(k-l-2)/k}p_{j+1}'^{l/k}+\frac{1}{2}\sum_{j=1}^{k}\left(p_{j+1}'^{1/k}p_{j+2}'^{(k-1)/k}+p_j'^{(k-1)/k}p_{j+1}'^{1/k}\right)\\
=&\frac{1}{2}\sum_{j=1}^{k}\sum_{l=0}^{k-2}\left(p_j'^{1/k}-p_{j+1}'^{1/k}\right)^2 p_j'^{(k-l-2)/k}p_{j+1}'^{l/k}+\frac{1}{2}\sum_{j=1}^{k}p_{j+1}'^{1/k}\left(p_j'^{(k-1)/k}+p_{j+2}'^{(k-1)/k}\right).
\end{aligned}
$$

For the second term, we recursively apply the transformation of the equation (8) for $u=1,2,\ldots,k-1$ and obtain

$$
\begin{aligned}
=&\frac{1}{2}\sum_{j=1}^{k}\sum_{l=0}^{k-2}\left(p_j'^{1/k}-p_{j+1}'^{1/k}\right)^2 p_j'^{(k-l-2)/k}p_{j+1}'^{l/k}+\sum_{j=1}^{k}\left(p'_{j+1}p'_{j+2}\cdots p'_{j+k-2}\right)^{1/k}p_j'^{1/k}p_{j+k-1}'^{1/k}\\
&+\frac{1}{2}\sum_{u=1}^{k-2}\sum_{j=1}^{k}\sum_{l=0}^{k-u-2}\left(p'_{j+1}p'_{j+2}\cdots p'_{j+u}\right)^{1/k}\cdot p_j'^{(k-u-l-2)/k}p_{j+u+1}'^{l/k}\left(p_j'^{1/k}-p_{j+u+1}'^{1/k}\right)^2.
\end{aligned}
$$

From the fact that $\left(p'_{j+1}p'_{j+2}\cdots p'_{j+k-2}\right)^{1/k} p_j'^{1/k} p_{j+k-1}'^{1/k} = \left(\prod_{j=1}^{k} p'_j\right)^{1/k}$ for all $j = 1, 2, \ldots, k$,

$$
\begin{aligned}
=&\frac{1}{2}\sum_{j=1}^{k}\sum_{l=0}^{k-2}\left(p_j'^{1/k} - p_{j+1}'^{1/k}\right)^2 p_j'^{(k-l-2)/k} p_{j+1}'^{l/k} + k\left(\prod_{j=1}^{k} p'_j\right)^{1/k} \\
&+\frac{1}{2}\sum_{u=1}^{k-2}\sum_{j=1}^{k}\sum_{l=0}^{k-u-2}\left(p'_{j+1}p'_{j+2}\cdots p'_{j+u}\right)^{1/k}\cdot p_j'^{(k-u-l-2)/k} p_{j+u+1}'^{l/k}\left(p_j'^{1/k} - p_{j+u+1}'^{1/k}\right)^2
\end{aligned}
$$

as required. □