Cryptanalysis of Multi-Prime Φ-Hiding Assumption

Jun Xu[1,2], Lei Hu[1,2], Santanu Sarkar[3], Xiaona Zhang[1,2], Zhangjie Huang[1,2] and Liqiang Peng[1,2]

[1] State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences, Beijing 100093, China
[2] Data Assurance and Communications Security Research Center, Chinese Academy of Sciences, Beijing 100093, China
[3] Indian Institute of Technology, Sardar Patel Road, Chennai 600 036, India
{xujun,hulei,zhangxiaona,huangzhangjie,pengliqiang}@iie.ac.cn,sarkar.santanu.bir@gmail.com

Abstract. In Crypto 2010, Kiltz, O'Neill and Smith used m-prime RSA modulus N with $m \geq 3$ for constructing lossy RSA. The security of the proposal is based on the Multi-Prime Φ-Hiding Assumption. In this paper, we propose a heuristic algorithm based on the Herrmann-May lattice method (Asiacrypt 2008) to solve the Multi-Prime Φ-Hiding Problem when prime $e > N^{\frac{2}{3m}}$. Further, by combining with mixed lattice techniques, we give an improved heuristic algorithm to solve this problem when prime $e > N^{\frac{2}{3m} - \frac{1}{4m^2}}$. These two results are verified by our experiments. Our bounds are better than the existing works.

Keywords: Multi-Prime Φ-Hiding Assumption, Multi-Prime Φ-Hiding Problem, lattice, LLL algorithm, Coppersmith's technique, Gauss algorithm

1 Introduction

1.1 Background

The Φ-Hiding Assumption [1] firstly introduced by Cachin, Micali and Stadler in Eurocrypt 1999 was used for building a practical private information retrieval scheme. Based on this assumption, many cryptographic schemes have been designed, such as [3, 4, 6, 12]. This assumption is roughly stated as follows:

> "For a given integer N with unknown factorization, it is hard to decide whether a given prime e divides $\Phi(N)$, where Φ is the Euler function."

Obviously, the Φ-Hiding Assumption holds with some requirements on the size of e since it is not true for $e \geq N$. The Φ-Hiding Assumption with RSA modulus $N = pq^{2k}$ has been analyzed in Asiacrypt 2008 [16]. The corresponding result is that a case of this variant fails with a good probability for any prime e.

For cryptographic applications, one would like e to be as large as possible, but from a security point of view, if e divides $\Phi(N)$ and is sufficiently large, then one can recover the factorization of N by using the idea of Coppersmith [2, 9, 14]. Thus, it is interesting to know the minimal size of e that allows for efficient factoring attacks.

It is well known that one can utilize Coppersmith's method to factorize the balanced RSA modulus $N = pq$ when prime $e > N^{\frac{1}{4}}$ divides $\Phi(N) = (p-1)(q-1)$. In Asiacrypt 2012, Kakvi, Kiltz and May proposed a lattice algorithm for obtaining a non-trivial factor of general N under the above condition [10].

In Crypto 2010, Kiltz *et al.* [12] showed that the RSA function $f : x \to x^e \bmod N$ is a $\log e$ lossy trapdoor permutation (LTDP) under the Φ-Hiding Assumption with $N = pq$. They also showed that the RSA-OAEP is indistinguishable against chosen plaintext attack (IND-CPA) in the standard model under this assumption, which is a long time open problem. Furthermore, they generalized this assumption to the multi-prime situation in order to obtain a more efficient LTDP such that RSA-OAEP can securely encrypt longer plaintext. To be specific, this multi-prime situation is described as follows:

> "For a given RSA modulus $N = p_1 \cdots p_m$ where bit-length of the p_i are equal for all $1 \leq i \leq m$, it is hard to decide whether a given prime e divides $p_i - 1$ for all p_i except one prime factor of N."

The condition that e divides $p_i - 1$ for all p_i except one prime factor of N implies that e^{m-1} divides $\Phi(N) = (p_1 - 1) \cdots (p_m - 1)$. So, this is a special case of e divides $\Phi(N)$. Therefore, it is a variant of the Φ-Hiding Assumption. For the sake of terminology, it is called as the Multi-Prime Φ-Hiding Assumption.

Now when $e|(p_i - 1)$ for $i \in [1, m-1]$, there are integers x_i such that $ex_i = p_i - 1$. So if one obtains the integer root x_i of equation $ex_i = p_i - 1$ for any $i \in [1, m-1]$, factorization of N is easily possible as $\gcd(ex_i + 1, N) = p_i$. Lattice method like Coppersmith's technique can be used to find x_i in polynomial time. So the research goal is to maximize the bound up to which x_i can be computed efficiently. Since the prime p_i are of the same bit-length, one fully breaks the Multi-Prime Φ-Hiding Assumption when the bound of x_i reaches $N^{\frac{1}{m}}$.

Originally, the bound $N^{\frac{1}{m^2}}$ of x_i was received by the Howgrave-Graham method in [9]. Later, this bound was improved up to $N^{O(\frac{1}{m^c})}$ for some $1 < c \leq 2$ in [12, 7]. Eventually, the bounds $N^{O(\frac{1}{m \log m})}$ were acquired in [19, 15, 18]. However, it is open whether a bound $N^{O(\frac{1}{m})}$, i.e., the exponent being linear in $\frac{1}{m}$, could be achieved.

1.2 Previous Works

In this subsection, we recall some known attacks on the Multi-Prime Φ-Hiding Problem. Note that if e divides $p_i - 1$ for all $1 \leq i \leq m$, then $N \equiv 1 \bmod e$. It gives a polynomial time distinguisher. To decide if e is Multi-Prime Φ-Hidden in N, consider the system of equations

$$ex_1 + 1 \equiv 0 \bmod p_1, \quad ex_2 + 1 \equiv 0 \bmod p_2, \quad \ldots, \quad ex_{m-1} + 1 \equiv 0 \bmod p_{m-1}.$$

Let $x_1 = N^\delta$. Here all p_i are of sizes of the same magnitude for $1 \leq i \leq m-1$. Usually we have

$$x_2 \approx \cdots \approx x_{m-1} \approx N^\delta.$$

The Howgrave-Graham method [9] can be used to find the desired small solutions of a modular linear equation

$$ex_i + 1 = 0 \bmod p_i \text{ for some } i \in \{1, \cdots, m-1\}.$$

Using Howgrave-Graham's method, one can solve the Multi-Prime Φ-Hiding Problem by finding the root of the equation $ex_i + 1 = 0 \mod p_i$ for some $i \in [1, m-1]$ in polynomial time if

$$\delta < \frac{1}{m^2}.$$

In Crypto 2010, Kiltz et al. [12] constructed a polynomial equation

$$e^{m-1}\left(\prod_{i=1}^{m-1} x_i\right) + \cdots + e\left(\sum_{i=1}^{m-1} x_i\right) + 1 \equiv 0 \bmod \prod_{i=1}^{m-1} p_i$$

by multiplying all given equations. Then they linearized the polynomial and solved it by the Herrmann-May theorem [8]. They showed that one can solve the Multi-Prime Φ-Hiding Problem in polynomial time if[4]

$$\delta < \frac{2}{m}\left(\frac{1}{m}\right)^{\frac{m}{m-1}}.$$

Later in Africacrypt 2011, Herrmann [7] improved the work of Kiltz et al. He used the Herrmann-May theorem to find the desired root (x, y) in equation

$$e^2 x + ey + 1 = 0 \bmod \prod_{i=1}^{m-1} p_i,$$

where $x = e^{m-3}\prod_{i=1}^{m-1} x_i + \cdots + \sum x_i x_j, y = \sum_{i=1}^{m-1} x_i$. He solved the Multi-Prime Φ-Hiding Problem in polynomial time if

$$\delta < \frac{2}{3}\left(\frac{1}{m}\right)^{\frac{3}{2}}.$$

In ACISP 2012, Tosu and Kunihiro [19] generalized the method of Herrmann. Instead of taking two variables, they considered linear polynomials of k variables

[4] There is a minor mistake in proceedings version of Crypto 2010 as reported in [7, Page 97].

for $k \in [1, m-1]$. They proved that one can solve the Multi-Prime Φ-Hiding Problem in polynomial time if

$$\delta < \max_{1 \le k \le m-1} \left\{ \frac{2}{k+1} \left(\frac{1}{m} \right)^{\frac{k+1}{k}} \right\}.$$

For large m, Tosu and Kunihiro further optimized k and got

$$\delta < \frac{2}{em(\ln m + 1)}$$

where e is the base of the natural logarithm. Thus, asymptotically bound of δ is

$$\frac{2}{em \ln m} = O(\frac{1}{m \log m}).$$

In SPACE 2012, Sarkar [15] observed that the sizes of two components of the desired root (x, y) in the analysis of Herrmann are not balanced. Based on this observation, he obtained better bound on δ than the work of Herrmann.

Takayasu and Kunihiro generalized the work of Herrmann and May [8] in [17, 18]. Their bounds are better when components of the desired root are of different size. Since there is a big difference between the sizes of x and y in Φ-Hiding Polynomial of [7], one can get a better bound on δ than the work of Herrmann. The bound of δ in the work of [17] is very close to [15], however, the work of [17] is more flexible and it can deal with modular equations with more variables than [15].

1.3 Our Contribution

In this paper, we show that the Multi-Prime Φ-Hiding Assumption does not hold when $\delta < \frac{1}{3m}$. For the first time, we obtain such a bound of δ which is linear in $\frac{1}{m}$. Thus we can solve the Multi-Prime Φ-Hiding Problem in polynomial time if

$$e > N^{\frac{1}{m} - \frac{1}{3m}} = N^{\frac{2}{3m}}.$$

Further, we improve the bound of δ up to $\frac{1}{3m} + \frac{1}{4m^2}$. This improvement is enormous for small values of m. Hence Multi-Prime Φ-Hiding Problem can be solved in polynomial time if

$$e > N^{\frac{1}{m} - (\frac{1}{3m} + \frac{1}{4m^2})} = N^{\frac{2}{3m} - \frac{1}{4m^2}}.$$

1.4 Organization of the Paper

We organize our paper as follow. In Section 2, we recall some preliminaries. In Section 3, we propose an algorithm using lattice technique. We give an improved algorithm using mixed lattice methods in Section 4. In Section 5, we give the comparison of our work with the existing results. We present our experiment results in Section 6. Section 7 concludes the paper.

2 Preliminaries

2.1 Lattice

An integer lattice $\mathcal{L}$ is a discrete subgroup of $\mathbb{Z}^n$. An alternative equivalent definition of an integer lattice can be given using a basis.

Let $\mathbf{b_1}, \cdots, \mathbf{b_m}$ be linear independent row vectors in $\mathbb{Z}^n$, a lattice $\mathcal{L}$ spanned by them is

$$\mathcal{L} = \left\{ \sum_{i=1}^{m} k_i \mathbf{b_i} \mid k_i \in \mathbb{Z} \right\}.$$

The set $\{\mathbf{b_1}, \cdots, \mathbf{b_m}\}$ is called a basis of $\mathcal{L}$ and $B = [\mathbf{b_1}^T, \cdots, \mathbf{b_m}^T]^T$ is the corresponding basis matrix. The dimension and determinant of $\mathcal{L}$ are respectively

$$\dim(\mathcal{L}) = m, \det(\mathcal{L}) = \sqrt{\det(BB^T)}.$$

When $m = n$, lattice is called full rank. In case of a full rank lattice, $\det(\mathcal{L}) = |\det(B)|$. From Hadamard's inequality, it is known that $\det(B) \leq \prod_{i=1}^{n} \|\mathbf{b_i}\|$, where $\|\mathbf{b}\|$ denotes Euclidean ℓ_2 norm of a vector $\mathbf{b}$.

For any two-dimensional lattice $\mathcal{L}$, the Gauss algorithm can find out the reduced basis vectors $\mathbf{v_1}$ and $\mathbf{v_2}$ satisfying

$$\|\mathbf{v_1}\| \leq \|\mathbf{v_2}\| \leq \|\mathbf{v_1} \pm \mathbf{v_2}\|$$

in time $O\left(\log^2(\max\{\|\mathbf{v_1}\|, \mathbf{v_2}\|\})\right)$. Here $\mathbf{v_1}$ is the shortest nonzero vector in $\mathcal{L}$ and $\mathbf{v_2}$ is the shortest vector in $\mathcal{L} \setminus \{k\mathbf{v_1} \mid k \in \mathbb{Z}\}$. A shortest vector $\mathbf{v}$ of an n dimensional lattice satisfies the Minkowski bound $\|\mathbf{v}\| \leq \sqrt{n}(\det(\mathcal{L}))^{\frac{1}{n}}$. The following result will be used in Section 4.

Lemma 1 (See, e.g., [5]). *Let $\mathbf{v_1}$ and $\mathbf{v_2}$ be the reduced basis vectors of $\mathcal{L}$ by the Gauss algorithm and $\mathbf{x} \in \mathcal{L}$. For the unique pair of integers (α, β) that satisfies $\mathbf{x} = \alpha\mathbf{v_1} + \beta\mathbf{v_2}$, we have*

$$\|\alpha\mathbf{v_1}\| \leq \frac{2}{\sqrt{3}}\|\mathbf{x}\|, \ \|\beta\mathbf{v_2}\| \leq \frac{2}{\sqrt{3}}\|\mathbf{x}\|.$$

2.2 Finding Small Roots

Coppersmith gave rigorous methods for extracting small roots of modular univariate polynomials and bivariate integer polynomials. These methods can extend to multivariate cases under the following assumption.

Assumption 1. *Let $h_1, \cdots, h_n \in \mathbb{Z}[x_1, \cdots, x_n]$ be the polynomials that are found by Coppersmith's algorithm. Then the ideal generated by the polynomial equations $h_1(x_1, \cdots, x_n) = 0$, $\cdots$, $h_n(x_1, \cdots, x_n) = 0$ has dimension zero.*

Herrmann and May used the idea of Coppersmith's technique to analyze modular linear polynomials and got the following result for bivariate linear polynomials.

Theorem 1 ([8]). *Let $\epsilon > 0$ and N be a large integer with a divisor $p \geq N^{\beta}$. Let $f(x_1, x_2) \in \mathbb{Z}[x_1, x_2]$ be a linear polynomial. Under Assumption 1, one can find all solutions (x_1, x_2) of the equation $f(x_1, x_2) = 0 \mod p$ with $|x_1| \leq N^{\gamma_1}, |x_2| \leq N^{\gamma_2}$ in polynomial time if*

$$\gamma_1 + \gamma_2 \leq 3\beta - 2 + 2(1-\beta)^{\frac{3}{2}} - \epsilon.$$

In our analyses, we consider the asymptotic case and ignore the low order term.

2.3 Multi-Prime Φ-Hiding Assumption

We briefly introduce the Multi-Prime Φ-Hiding Assumption and the corresponding problem. Please refer to [12, 7, 19, 15] for more details.

Definition 1 (Multi-Prime Φ-Hiding Problem). *Let $N = p_1 \cdots p_m$ be a Multi-Prime RSA modulus where the p_i are of the same bit length for $1 \leq i \leq m$. Let e be a given prime of the size $N^{\frac{1}{m}-\delta}$. Problem is to decide whether*

$$e \mid (p_1 - 1), \cdots, e \mid (p_{m-1} - 1), e \nmid (p_m - 1).$$

Definition 2 (Multi-Prime Φ-Hiding Assumption). *There is no polynomial time algorithm that solves the Multi-Prime Φ-Hiding Problem with a non-negligible probability of success.*

3 Algorithm Using Lattice Technique

In this section we give an algorithm for solving the Multi-Prime Φ-Hiding Problem. Our algorithm can be derived from the following theorem.

Theorem 2. *Let $N = p_1 \cdots p_m$ be a Multi-Prime RSA modulus where the p_i are of same bit length for $1 \leq i \leq m$. Let e be a prime of the size $N^{\frac{1}{m}-\delta}$. Under Assumption 1, we can solve the Multi-Prime Φ-Hiding Problem in polynomial time when*

$$\delta < \frac{1}{3m}.$$

Proof. Let $r = N \bmod e$ and $s = (\frac{N-r}{e}) \bmod e$. If $e \mid (p_1 - 1), \cdots, e \mid (p_{m-1} - 1)$ and $e \nmid (p_m - 1)$, there exist unknown integers $x_1, \cdots, x_{m-1}$ such that

$$ex_1 + 1 = p_1, \cdots, ex_{m-1} + 1 = p_{m-1}.$$

Since $N = p_1 \cdots p_m$, we have $(ex_1 + 1) \cdots (ex_{m-1} + 1) \cdot p_m = N$. Then taking modulo e on both sides we get

$$p_m \bmod e = N \bmod e = r.$$

Thus, there is an equation $ex_m + r = p_m$ with unknown x_m. We multiply all equations together to get $(ex_1 + 1) \cdots (ex_{m-1} + 1)(ex_m + r) = N$. So we have

$$\begin{aligned}
&(e^{m-1} \prod_{i=1}^{m-1} x_i + \cdots + e^2 \sum_{1 \le i < j \le m-1} x_i x_j + e \sum_{1 \le i \le m-1} x_i + 1) \\
&(ex_m + r) = N \Rightarrow (e \sum_{1 \le i \le m-1} x_i + 1)(ex_m + r) \equiv N \bmod e^2 \\
&\qquad \Rightarrow ex_m + er \sum_{1 \le i \le m-1} x_i + r \equiv N \bmod e^2 \\
&\qquad \Rightarrow ex_m + er \sum_{1 \le i \le m-1} x_i \equiv es \bmod e^2 \\
&\qquad \Rightarrow x_m + r \sum_{1 \le i \le m-1} x_i - s \equiv 0 \bmod e
\end{aligned}$$

Let $y_1 = x_m$, $y_2 = x_1 + \cdots + x_{m-1}$. Consider the bivariate modular linear equation

$$f(y_1, y_2) = y_1 + r y_2 - s. \tag{1}$$

The equation (1) has root $\mathbf{y} := (x_m, x_1 + \cdots + x_{m-1})$ in $\mathbb{Z}_e$ as $f(y_1, y_2) \equiv 0 \bmod e$.

First, let us bound the size of $\mathbf{y}$. Since $0 < x_i = \frac{p_i - 1}{e} < \frac{N^{\frac{1}{m}}}{N^{\frac{1}{m} - \delta}} = N^{\delta}$ for $i = 1, \ldots, m$, we have

$$0 < x_1 + \cdots + x_{m-1} < (m-1)N^{\delta} = e^{\log_e (m-1) + \frac{\delta}{\frac{1}{m} - \delta}}.$$

Next, we use Theorem 1 for solving equation (1). Since modulus e is known, we take $\beta = 1$. Here $\gamma_1 = \frac{\delta}{\frac{1}{m} - \delta}$ and $\gamma_2 = \log_e (m-1) + \frac{\delta}{\frac{1}{m} - \delta}$. Under Assumption 1, we can find all solution (y_1, y_2) in polynomial time when

$$\gamma_1 + \gamma_2 = \frac{2\delta}{\frac{1}{m} - \delta} + \log_e (m-1) \le 1 - \epsilon.$$

Considering the asymptotic case and ignoring the lower order terms, the above condition is simplified to

$$\delta < \frac{1}{3m}.$$

Further, we check whether $\gcd(ey_1 + r, N)$ gives a nontrivial factor of N for every candidate. Thus, we can find out the desired root $\mathbf{y}$ and recover p_m. Conversely, if we cannot get a non-trivial factor of N under Assumption 1, then relation $e \mid (p_1 - 1), \cdots, e \mid (p_{m-1} - 1), e \nmid (p_m - 1)$ in the Multi-Prime Φ-Hiding Problem does not hold. □

Based on the Theorem 2, we have the Algorithm 1 to solve the Multi-Prime Φ-Hiding Problem.

Algorithm 1 Solving Multi-Prime Φ-Hiding Problem

Input: Public key (N, e) and m is the number of prime factors of N.
Output: Decide whether $e \mid (p_1 - 1), \cdots, e \mid (p_{m-1} - 1), e \nmid (p_m - 1)$.

1: Compute $r = N \bmod e$ and $s = (\frac{N-r}{e}) \bmod e$.
2: Solve equation $y_1 + ry_2 - s \equiv 0 \bmod e$ using Theorem 1.
3: If $\gcd(ey_1 + r, N)$ for all solutions (y_1, y_2) are trivial factors of N, output no. Else, output yes.

4 Improved Algorithm Using Mixed Lattice Methods

In this section we present an improved algorithm in order to improve the bound $\delta < \frac{1}{3m}$. This algorithm is obtained by dealing with equation (1) with mixed lattice methods in the following theorem.

Theorem 3. *Let $N = p_1 \cdots p_m$ be a Multi-Prime RSA modulus where the p_i are of same bit length for $1 \leq i \leq m$. Let e be a prime of the size $N^{\frac{1}{m}-\delta}$. Under Assumption 1, we can solve the Multi-Prime Φ-Hiding Problem in polynomial time when*

$$\delta < \frac{4}{3m} - \frac{2}{3} + \frac{2}{3}\left(1 - \frac{1}{m}\right)^{3/2}.$$

Proof. If $e \mid (p_1 - 1), \cdots, e \mid (p_{m-1} - 1)$ and $e \nmid (p_m - 1)$, we know

$$y_1 + ry_2 \equiv s \bmod e \tag{2}$$

has integer root $\mathbf{y} := (x_m, x_1 + \cdots + x_{m-1})$, where

$$\|\mathbf{y}\| = \sqrt{(x_1 + \cdots + x_{m-1})^2 + x_m^2} < m \cdot N^{\delta}.$$

The set of solutions

$$\mathcal{L} = \left\{(y_1, y_2) \in \mathbb{Z}^2 \mid y_1 + ry_2 \equiv 0 \bmod e\right\}$$

forms an additive discrete subgroup of $\mathbb{Z}^2$. Thus, $\mathcal{L}$ is a 2-dimensional integer lattice. Lattice $\mathcal{L}$ is spanned by the row vectors of the basis matrix

$$B = \begin{bmatrix} -r & 1 \\ e & 0 \end{bmatrix}.$$

Let us briefly check integer span of B, denoted by $\mathrm{span}(B)$ is indeed equal to $\mathcal{L}$. First both $(-r, 1)$ and $(e, 0)$ are solutions of $y_1 + ry_2 \equiv 0 \bmod e$. Thus $\mathrm{span}(B) \subseteq \mathcal{L}$. Conversely, let $(y_1, y_2) \in \mathcal{L}$. So we have $y_1 + ry_2 = ke$ for some $k \in \mathbb{Z}$. Then $(y_2, k)B = (y_1, y_2) \in \mathrm{span}(B)$. Thus $\mathcal{L} \subseteq \mathrm{span}(B)$.

Consider the set

$$\mathcal{L}' = \left\{(s + y_1, y_2) \mid (y_1, y_2) \in \mathcal{L}\right\}.$$

It is clear that for any $(x, y) \in \mathcal{L}'$, (x, y) will satisfy the equation (2).

Let $\mathbf{u} := (u_1, u_2)$ be the smallest length vector in $\mathcal{L}'$, which can be obtained by the closest vector algorithm on the lattice $\mathcal{L}$ from the point $(-s, 0)$ in polynomial time (see, e.g., [11]). Obviously, $\|\mathbf{u}\| \leq \|\mathbf{y}\| < m \cdot N^{\delta}$.

Let $\mathbf{v_1} := (v_{11}, v_{12}), \mathbf{v_2} := (v_{21}, v_{22})$ be Gauss-reduced basis vectors of $\mathcal{L}$. Since $\mathbf{y} - \mathbf{u}$ belongs to $\mathcal{L}$, there exist integer coefficients α_1, α_2 such that

$$\mathbf{y} - \mathbf{u} = \alpha_1 \mathbf{v_1} + \alpha_2 \mathbf{v_2}. \tag{3}$$

Observing that the first component of $\mathbf{y}$ is equal to $\frac{p_m - r}{e}$ and rearranging equation (3), we get $ev_{11}\alpha_1 + ev_{21}\alpha_2 + eu_1 + r = p_m$. In Appendix A, we prove that $|v_{11}| \leq \sqrt{2e}$ and $v_{11} \neq 0$. Thus, the bivariate modular linear equation

$$(ev_{11})x_1 + (ev_{21})x_2 + (eu_1 + r) \equiv 0 \bmod p_m \tag{4}$$

has an integer root (α_1, α_2).

First, let us bound the sizes of unknown α_1 and α_2. From (3), according to Lemma 1, we obtain

$$|\alpha_1| \leq \frac{2\|\mathbf{y} - \mathbf{u}\|}{\sqrt{3}\|\mathbf{v_1}\|} \leq \frac{2(\|\mathbf{y}\| + |\mathbf{u}\|)}{\sqrt{3}\|\mathbf{v_1}\|} < \frac{4mN^{\delta}}{\sqrt{3}\|\mathbf{v_1}\|},$$
$$|\alpha_2| \leq \frac{2\|\mathbf{y} - \mathbf{u}\|}{\sqrt{3}\|\mathbf{v_2}\|} \leq \frac{2(\|\mathbf{y}\| + |\mathbf{u}\|)}{\sqrt{3}\|\mathbf{v_2}\|} < \frac{4mN^{\delta}}{\sqrt{3}\|\mathbf{v_2}\|}.$$

So $|\alpha_1\alpha_2| < \frac{16m^2N^{2\delta}}{3\|\mathbf{v_1}\|\|\mathbf{v_2}\|}$. Notice that $e = \det(\mathcal{L}) \leq \|\mathbf{v_1}\|\|\mathbf{v_2}\|$. Thus we have

$$|\alpha_1\alpha_2| < \frac{16m^2N^{2\delta}}{3\|\mathbf{v_1}\|\|\mathbf{v_2}\|} = N^{3\delta - \frac{1}{m} + \log_N \frac{16m^2}{3}}, \text{ as } e = N^{\frac{1}{m} - \delta}.$$

Next, we use Theorem 1 to solve the equation (4), where the size of unknown modulus p_m is $N^{\frac{1}{m}}$. So we take $\beta = \frac{1}{m}$. Under Assumption 1, we can find all roots (x_1, x_2) of the equation (4) in polynomial time when

$$3\delta - \frac{1}{m} + \log_N \frac{16m^2}{3} \leq \frac{3}{m} - 2 + 2\left(1 - \frac{1}{m}\right)^{\frac{3}{2}} - \epsilon.$$

Ignoring the term $\log_N \frac{16m^2}{3}$ as $m \ll N$, we get

$$\delta < \frac{4}{3m} - \frac{2}{3} + \frac{2}{3}\left(1 - \frac{1}{m}\right)^{3/2}.$$

Furthermore, we check whether $\gcd(ev_{11}x_1 + ev_{21}x_2 + eu_1 + r, N)$ gives a nontrivial factor of N for every candidate. Thus, we can obtain the desired root (α_1, α_2) and recover the factor p_m of N. □

Since $(1 - \frac{1}{m})^{\frac{3}{2}} = 1 - \frac{3}{2m} + \frac{3}{8m^2} + o(\frac{1}{m^2})$, we have $\frac{4}{3m} - \frac{2}{3} + \frac{2}{3}\left(1 - \frac{1}{m}\right)^{3/2} \approx \frac{1}{3m} + \frac{1}{4m^2}$. Thus the simplified condition is

$$\delta < \frac{1}{3m} + \frac{1}{4m^2}.$$

Algorithm 2 Further Solving Multi-Prime Φ-Hiding Problem

Input: Public key (N, e) and m is the number of prime factors of N.
Output: Decide whether $e \mid (p_1 - 1), \cdots, e \mid (p_{m-1} - 1), e \nmid (p_m - 1)$.

1: Compute $r = N \bmod e$ and $s = (\frac{N-r}{e}) \bmod e$.
2: Find the smallest Euclidean length root (u_1, u_2) of equation $y_1 + ry_2 \equiv s \bmod e$ using the closest vector algorithm.
3: Generate lattice $\mathcal{L}$ spanned by the row vectors of the matrix

$$\begin{bmatrix} -r & 1 \\ e & 0 \end{bmatrix}.$$

4: Compute Gauss-reduced basis vectors (v_{11}, v_{12}) and (v_{21}, v_{22}) of lattice $\mathcal{L}$.
5: Solve equation $(ev_{11})x_1 + (ev_{21})x_2 + (eu_1 + r) \equiv 0 \bmod p_m$ using Theorem 1.
6: If $\gcd(ev_{11}x_1 + ev_{21}x_2 + eu_1 + r, N)$ for all solutions (x_1, x_2) are trivial factors of N, output no. Else, output yes.

So when $e > N^{\frac{1}{m} - \frac{1}{3m} - \frac{1}{4m^2}} = N^{\frac{2m}{3} - \frac{1}{4m^2}}$, one can solve Multi-Prime Φ-Hiding Problem in polynomial time.

Since $\frac{4}{3m} - \frac{2}{3} + \frac{2}{3}\left(1 - \frac{1}{m}\right)^{3/2} > \frac{1}{3m}$, bound of δ in Theorem 3 is better than that of Theorem 2. In Figure 1, we present the two bounds pictorially.

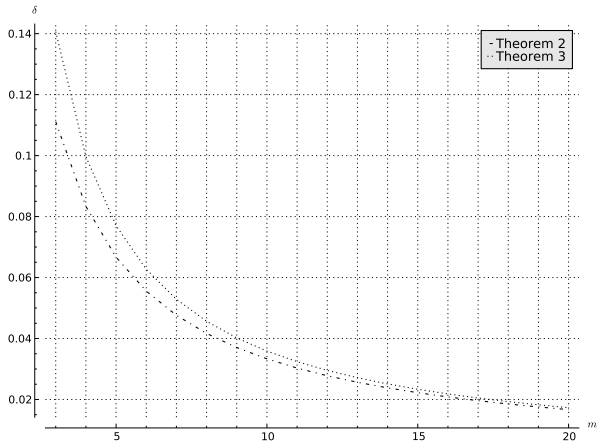

Fig. 1. Comparison between the bounds δ for Theorem 2 and Theorem 3 when $3 \leq m \leq 20$.

Based on the Theorem 3, we have the Algorithm 2 to solve the Multi-Prime Φ-Hiding Problem.

5 Comparison with the existing works

In this section, we compare our results with previous works.

In Figure 2, we compare our results with the existing works pictorially. We observe that the curve of [18] is almost identical with that of [15]. So we do not plot it explicitly. It is clear from the figure that our bound is much better than the existing bounds. Thus our new attack solves the Multi-Prime Φ-Hiding Problem for more values of e than the existing works. One can see that existing curves [7, 19, 15] are very close to each other. On the other hand, we are achieving much improved curve. More importantly, for small values of m, these differences are more prominent. For example when $m = 4$, new bound of δ becomes 0.09968 whereas existing was 0.08358 in [18]. Thus the improvement is significant for small values of m. Also m cannot be large as in that case Elliptic Curve Factorization [13] will be efficient.

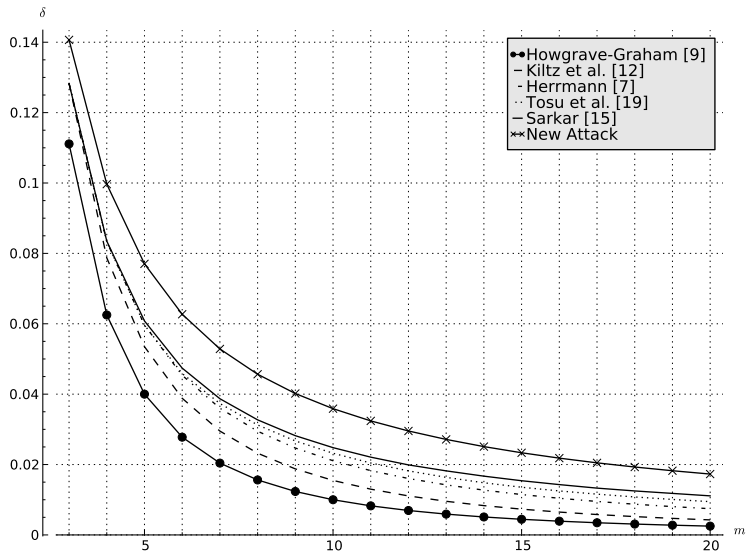

Fig. 2. Comparison of our bound $\delta < \frac{4}{3m} - \frac{2}{3} + \frac{2}{3}\left(1 - \frac{1}{m}\right)^{3/2}$ with the existing works for $3 \leq m \leq 20$.

In Table 1, we present the minimum bit lengths of e for which Φ-Hidding Problem is polynomial time solvable for different values of m. Here we take 2048-bit N. From the table, it is clear that all existing bounds are almost same for $m = 3$. Though early works improve the work of [12] for values $m > 3$, this work improves the bound on δ for $m > 3$ as well as $m = 3$. So one can solve Φ-Hidding Problem in polynomial time for much smaller values of e.

Table 1. Comparison of bit lengths of the minimum e with 2048-bit N

Results \ m	3	4	5	6	7	8	9	10
Kiltz *et al.* [12]	420	351	301	262	233	209	190	174
Herrmann [7]	420	342	288	249	219	196	177	162
Tosu *et al.* [19]	420	342	288	248	217	192	173	158
Sarkar [15]	420	341	286	245	214	190	170	155
Takayasu *et al.* [18]	421	341	286	245	214	190	170	154
$(\frac{1}{m} - \frac{1}{3m}) \cdot 2048$	456	342	274	228	196	171	152	137
$\left(\frac{1}{m} - (\frac{4}{3m} - \frac{2}{3} + \frac{2}{3}(1 - \frac{1}{m})^{3/2})\right) \cdot 2048$	395	308	252	213	185	163	146	132

6 Experiment Results

We implement the above attacks with LLL algorithm in Magma on a PC with Intel(R) Core(TM) Quad CPU (2.83GHz, 3.25GB RAM, Windows XP). In our experiments, Assumption 1 is always verified. We present our experimental results in Table 2. As we can see that the experimental results and theoretical upper bounds on δ are perfectly match.

For Theorem 2, we take $3 \leq m \leq 10$. We use Theorem 1 to solve equation $y_1 + ry_2 - s = 0 \bmod e$. For a positive integer t, we generate polynomials

$$g_{k,i}(y_1, y_2) := y_2^i (y_1 + ry_2 - s)^k e^{t-k}$$

which share the common root $\mathbf{y}$ modulo e^t, where $k = 0, \cdots, t$; $i = 0, \ldots, t-k$. In our experiments, we choose $t = 8$. The dimensions of the involved lattices are $\frac{1}{2}(t^2 + 3t + 2) = 45$. Then the desired root can be obtained by lattice reduction. Hence the factor p_m of the modulus N can be recovered when e is Multi-Prime Φ-Hidden in N and the corresponding δ satisfies the experimental value.

For Theorem 3, we present the situations of $3 \leq m \leq 5$. We neglect running times of the closest vector algorithm and the Gauss algorithm as they are negligible since the corresponding lattices are only two-dimensional. In order to use Theorem 1, we first multiply the equation $(ev_{11})x_1 + (ev_{21})x_2 + (eu_1 + r) \equiv 0 \bmod p_m$ by $(ev_{11})^{-1}$ modulo N and get a monic equation $f(x_1, x_2) \equiv 0 \bmod p_m$. Then, we collect the polynomials which share a common root (α_1, α_2) modulo N^l

$$h_{k,i}(x_1, x_2) := x_2^i f^k(x_1, x_2) N^{\max\{l-k,0\}}$$

for $k = 0, \cdots, t; i = 0, \ldots, t-k$ and $l = \left\lfloor \left(1 - \sqrt{\frac{m-1}{m}}\right) t \right\rfloor$. In our experiments, we take $t = 12$. The dimensions of the corresponding lattices are $\frac{1}{2}(t^2 + 3t + 2) = 91$. Finally, we obtain the desired (α_1, α_2).

7 Conclusion

In this paper, we have reduced the Multi-Prime Φ-Hiding Problem to the problem of finding small root of a bivariate modular linear equation. Based on this, we

Table 2. Experiment results for different values of m with 2048 bit N

Analyses	m	δ (theoretical)	δ (experimental)	LLL (seconds)	Gröbner (seconds)
Theorem 2	3	0.1111	0.1100	60.497	0.842
	4	0.0833	0.0820	32.854	0.484
	5	0.0667	0.0657	19.859	0.421
	6	0.0556	0.0548	15.241	0.296
	7	0.0476	0.0469	11.778	0.287
	8	0.0417	0.0409	8.299	0.187
	9	0.0370	0.0355	6.349	0.125
	10	0.0333	0.0315	5.444	0.078
Theorem 3	3	0.1407	0.1320	3975.826	1120.540
	4	0.0997	0.0891	2059.156	121.734
	5	0.0770	0.0683	1866.188	109.938

have proposed two algorithms using lattice techniques to solve the problem. We have obtained better bounds than the existing works.

References

1. Cachin, C., Micali, S., Stadler, M.: Computationally private information retrieval with polylogarithmic communication. In Stern, J., ed.: Advances in Cryptology EUROCRYPT 99. Volume 1592 of Lecture Notes in Computer Science. Springer Berlin Heidelberg (1999) 402–414
2. Coppersmith, D.: Small solutions to polynomial equations, and low exponent RSA vulnerabilities. Journal of Cryptology **10**(4) (1997) 233–260
3. Gentry, C., Mackenzie, P., Ramzan, Z.: Password authenticated key exchange using hidden smooth subgroups. In: Proceedings of the 12th ACM Conference on Computer and Communications Security. CCS 2005, New York, NY, USA, ACM (2005) 299–309
4. Gentry, C., Ramzan, Z.: Single-database private information retrieval with constant communication rate. In Caires, L., Italiano, G., Monteiro, L., Palamidessi, C., Yung, M., eds.: Automata, Languages and Programming. Volume 3580 of Lecture Notes in Computer Science. Springer Berlin Heidelberg (2005) 803–815
5. Gomez, D., Gutierrez, J., Ibeas, A.: Attacking the Pollard generator. Information Theory, IEEE Transactions on **52**(12) (Dec 2006) 5518–5523
6. Hemenway, B., Ostrovsky, R.: Public-key locally-decodable codes. In Wagner, D., ed.: Advances in Cryptology – CRYPTO 2008. Volume 5157 of Lecture Notes in Computer Science. Springer Berlin Heidelberg (2008) 126–143
7. Herrmann, M.: Improved cryptanalysis of the multi-prime ϕ-hiding Assumption. In Nitaj, A., Pointcheval, D., eds.: Progress in Cryptology – AFRICACRYPT 2011. Volume 6737 of Lecture Notes in Computer Science. Springer Berlin Heidelberg (2011) 92–99
8. Herrmann, M., May, A.: Solving linear equations modulo divisors: On factoring given any bits. In Pieprzyk, J., ed.: Advances in Cryptology - ASIACRYPT 2008. Volume 5350 of Lecture Notes in Computer Science. Springer Berlin Heidelberg (2008) 406–424

9. Howgrave-Graham, N.: Approximate integer common divisors. In Silverman, J., ed.: Cryptography and Lattices. Volume 2146 of Lecture Notes in Computer Science. Springer Berlin Heidelberg (2001) 51–66
10. Kakvi, S.A., Kiltz, E., May, A.: Certifying RSA. In Wang, X., Sako, K., eds.: Advances in Cryptology – ASIACRYPT 2012. Volume 7658 of Lecture Notes in Computer Science. Springer Berlin Heidelberg (2012) 404–414
11. Kannan, R.: Minkowski's convex body theorem and integer programming. Mathematics of Operations Research **12**(3) (1987) 415–440
12. Kiltz, E., ONeill, A., Smith, A.: Instantiability of RSA-OAEP under chosen-plaintext attack. In Rabin, T., ed.: Advances in Cryptology - CRYPTO 2010. Volume 6223 of Lecture Notes in Computer Science. Springer Berlin Heidelberg (2010) 295–313
13. Lenstra, Jr., H.W.: Factoring integers with elliptic curves. Annals of Mathematics **126** (1987) 649–673
14. May, A.: Using LLL-reduction for solving RSA and factorization problems. In Nguyen, P.Q., Valle, B., eds.: The LLL Algorithm. Information Security and Cryptography. Springer Berlin Heidelberg (2010) 315–348
15. Sarkar, S.: Reduction in lossiness of RSA trapdoor permutation. In Bogdanov, A., Sanadhya, S., eds.: Security, Privacy, and Applied Cryptography Engineering. Volume 7644 of Lecture Notes in Computer Science. Springer Berlin Heidelberg (2012) 144–152
16. Schridde, C., Freisleben, B.: On the validity of the ϕ-hiding assumption in cryptographic protocols. In Pieprzyk, J., ed.: Advances in Cryptology - ASIACRYPT 2008. Volume 5350 of Lecture Notes in Computer Science. Springer Berlin Heidelberg (2008) 344–354
17. Takayasu, A., Kunihiro, N.: Better lattice constructions for solving multivariate linear equations modulo unknown divisors. In Boyd, C., Simpson, L., eds.: Information Security and Privacy - ACISP 2013. Volume 7959 of Lecture Notes in Computer Science. Springer Berlin Heidelberg (2013) 118–135
18. Takayasu, A., Kunihiro, N.: Better lattice constructions for solving multivariate linear equations modulo unknown divisors. IEICE Transactions **97-A**(6) (2014) 1259–1272
19. Tosu, K., Kunihiro, N.: Optimal bounds for multi-prime ϕ-hiding assumption. In Susilo, W., Mu, Y., Seberry, J., eds.: Information Security and Privacy. Volume 7372 of Lecture Notes in Computer Science. Springer Berlin Heidelberg (2012) 1–14

A Proof on $|v_{11}| \leq \sqrt{2e}$ and $v_{11} \neq 0$

Proof. Note that $\mathbf{v_1} = (v_{11}, v_{12})$ is the shortest nonzero vector in lattice $\mathcal{L}$. According to Minkowski bound, we know that

$$\|\mathbf{v_1}\| \leq \sqrt{2\det(\mathcal{L})} = \sqrt{2e}.$$

Since v_{11} is a component of $\mathbf{v_1}$, we have $|v_{11}| \leq \sqrt{2e}$. Now, we prove that $v_{11} \neq 0$. Since $v_1 \in \mathcal{L}$, there exists some integer c_1 such that

$$v_{11} + rv_{12} = c_1 e.$$

If $v_{11} = 0$, we get $rv_{12} = c_1 e$. Since e is a prime and $0 < r < e$, e divides v_{12}. Thus e divides $\|\mathbf{v_1}\|$. So $\|\mathbf{v_1}\| \geq e$. However, it is impossible since $\|\mathbf{v_1}\| \leq \sqrt{2e}$. Therefore, $v_{11} \neq 0$.

□