New Results on the ϕ-Hiding Assumption and Factoring Related RSA Moduli

Jun Xu, Jun Song, Lei Hu
Institute of Information Engineering, Chinese Academy of Sciences

August 18, 2025

Outline

The ϕ-Hiding Assumption

- At Eurocrypt 1999, Cachin, Micali, and Stadler first introduced the ϕ-hiding assumption
  - in order to construct an efficient private information retrieval scheme
- The ϕ-hiding assumption is related to many cryptographic schemes
  - private information retrieval schemes
  - lossy trapdoor permutation
  - certified trapdoor permutations
  - laconic private set intersection
  - non-committing encryption
  - factoring-based signature schemes

Definition

Definition (ϕ-Hiding Assumption)

Given an integer N with unknown factorization, it is computationally hard to decide whether a prime e with $2 < e \ll N^{\frac{1}{4}}$ divides $\phi(N)$ or not.

- For a standard RSA modulus $N = PQ$ (P, Q have the same bit length), if a given prime $e > N^{\frac{1}{4}}$, then N can be decomposed in the polynomial time by the univariate Coppersmith theorem. Once N is decomposed, the ϕ-Hiding Assumption is decided.
- At Asiacrypt 2008, Schridde and Freisleben analyzed a case of $N = PQ^r$ with even r
  - There exists a polynomial-time algorithm that, with high probability, determines whether a given prime $e \mid (P-1)$ (a special case of $e \mid \phi(N)$).

The integer e in the ϕ-hiding assumption

- In the Journal of Cryptology published in 2019, Abdalla et al. pointed out that:
  - *More precisely, we need e in the ϕ-hiding assumption to be chosen as a power of a small prime number ... But to our knowledge, this new variant of the ϕ-hiding assumption has not been analyzed and might actually not hold.*
- This means that the e involved in ϕ-hiding assumption can be non prime numbers.

The ϕ-hiding assumption and factoring

- The ϕ-hiding assumption shows a connection between known factors of $\phi(N)$ and decomposing the modulus N.
- Some cryptographic schemes that rely on RSA modulus N also embed information about known factors of $\phi(N)$.
- Given a positive integer N, finding positive integers r and s such that $N = rs^2$, where r is squarefree, is a classic problem in algorithmic number theory.
    - polynomial-time equivalence to the problem of determining the ring of integers of a number field

Outline

Case 1: e is a prime number

Theorem

Let $N = PQ^r$ be a given integer with unknown factorization, where P, Q are different primes, $r \geq 1$ is a given integer, and $Q \geq N^{\beta}$ for $0 < \beta < \frac{1}{r}$. Let e be a given prime satisfying $e \mid \phi(N)$. For any fixed $\varepsilon > 0$, we can factorize N in time polynomial of ε^{-1} and $\log N$, when one of the following two conditions is met:

$$\begin{cases} e \geq N^{\frac{1}{4r}+\varepsilon} & (\beta \text{ is unknown}) \quad (1) \\ e \geq N^{\beta - r\beta^2 + \varepsilon} & (\beta \text{ is known}) \quad (2) \end{cases}$$

- Bound (2) equals bound (1), when $\beta = \frac{1}{2r}$ $(\beta - r\beta^2 = \frac{1}{4r})$.
- Bound (2) is better, when $\beta \neq \frac{1}{2r}$ $(\beta - r\beta^2 < \frac{1}{4r})$.

Case 2: e is a square-free composite number

Theorem

Define N as above. Let e be a given square-free composite number with known factorization satisfying $e \mid \phi(N)$, *where the number of prime factors of e is* $O(\log\log N)$. *For any fixed* $\varepsilon > 0$, *we can factorize N in time polynomial of* ε^{-1} *and* $\log N$ *for any integer constant r, when one of conditions (1) and (2) is satisfied.*

- The hypothesis on the number of prime factors of e is reasonable
  - The average number of prime factors of a random integer is $O(\log\log N)$.

Case 3: e is a general composite number

Theorem

Define N as above, where unknown prime factors P, Q satisfy $\gcd(P-1, Q-1) = 2$. Let e be a given integer with known factorization such that $e \mid \phi(N)$, where the number of prime factors of e is $O(\log\log N)$. For any fixed $\varepsilon > 0$, we can factorize N in time polynomial of ε^{-1} and $\log N$ for any integer constant r, when one of conditions (1) and (2) holds.

- For random primes P and Q, the condition that $\gcd(P-1, Q-1) = 2$ holds with a probability of $\frac{6}{\pi^2} \approx 61\%$.

Outline

1. The ϕ-Hiding Assumption
2. Our Main Results
3. Technical Overview
4. Partial Applications

Core idea

- The GOAL: The relation $e \mid \phi(N) \Rightarrow e \mid (Q - u)$, where $N = PQ^r$.
- Once u is obtained, then $ex + u \equiv 0 \mod Q$
  - Here $Q \mid N$ and $Q \geq N^\beta$
- Then factorize N via two univariate Coppersmith algorithms, based on whether β is unknown or not.
  - For known β, the univariate Coppersmith algorithm is well-known.
  - For unknown β, we develop the corresponding univariate Coppersmith algorithm.
- Our results are rigorous.
  - Due to the lack of heuristics in univariate Coppersmith algorithms.

Case 1: e is a prime number

- From $N = PQ^r$, the relation $e \mid \phi(N) \Leftrightarrow e \mid (P-1)(Q-1)$.
  - We can assume $\gcd(e, N) = 1$. Otherwise, N is factorized easily.
- From prime $e \mid (P-1)(Q-1)$, we have $e \mid (Q-1)$ or $e \mid (P-1)$.
- We can write $e \mid (Q-u)$, where $0 < u < e$
  - If $e \mid (Q-1)$, then $u = 1$.
  - If $e \mid (P-1)$, then $u^r \equiv N \mod e$.
    - The u can be computed by the Adleman–Manders–Miller (AMM) algorithm.

Case 2: e is a square-free composite number

- From $e \mid (P-1)(Q-1)$, there must be two factors of e, E_1 and E_2, satisfying $e = E_1E_2$ such that $E_1 \mid (P-1)$ and $E_2 \mid (Q-1)$.
- In order for such tuple (E_1, E_2) to be enumerated in polynomial time,
    - we limit the number of prime factors of e to $O(\log\log N)$
- When such tuple (E_1, E_2) is found, we obtain $P = E_1k_1 + 1$ and $Q = E_2k_2 + 1$.
    - k_1, k_2 are unknown integers
    - $\gcd(E_1, E_2) = 1$ because e is square-free

Case 2: e is a square-free composite number

- From $P = E_1 k_1 + 1$ and $Q = E_2 k_2 + 1$, we derive $P = e x_0 + s$
  - x_0 is unknown, and s is known, with $0 < s < e$ and $\gcd(e, s) = 1$
- According to division with remainder, we write $Q = e y_0 + u$, where $0 < u < e$.
  - y_0, u are both unknown.
- From $N = PQ^r$, we get $u^r \equiv b \mod e$,
  - b can be calculated publicly.
- The current task is how to calculate u.
  - If $r = 1$, then u can be easily calculated.

Case 2: e is a square-free composite number

- For $r > 1$, u can be calculated via AMM+CRT.
  - We write $e = e_1 e_2 \cdots e_n$
    - e_i's are prime factors and n is the number of prime factors.
  - Then $u^r \equiv b \mod e_i$ for all $1 \leq i \leq n$.
  - Use the AMM algorithm to compute the root for $x^r \equiv b \mod e_i$.
  - Utilize the CRT algorithm to obtain u for $x^r \equiv b \mod e$.

Case 3: e is a general composite number

- Similar to Case 2, except for calculating $u^r \equiv b \mod e$ when $r > 1$.
- We use AMM+CRT+Hensel to obtain the u.
    - In addition to AMM and CRT, we also need Hensel lifting.

Outline

Application to the ϕ-Hiding Assumption

Corollary

Let $N = PQ^r$ be a given integer with unknown factorization, where primes P, Q have the same bit-length, and $r \geq 1$. For any fixed $\varepsilon > 0$, let

$$e \geq N^{\frac{1}{(r+1)^2}+\varepsilon}$$

be a given prime. Then we can decide whether e divides $\phi(N)$ or not in polynomial time.

- For a standard RSA modulus $N = PQ$ ($r = 1$), the bound $e > N^{\frac{1}{4}}$ is the same as previous results.
  - But our results can generalize the prime number e to the case of related composite numbers.
- For $r > 1$, our results have more advantages.

Application to the ϕ-Hiding Assumption

Table 2. Experimental results comparing with prior works. For integer $N = PQ^r$, primes P and Q have the same bit-length, and $e = N^\gamma$ is prime. The bounds in [39] are derived under the condition that e is expressed as $e = rk + 1$ with $r \geq 1$, which implies $\gcd(r, e-1) = r$. Define "Bound" and "Dim." as in Table 1.

	k, l_b, B_Q, B_P	Bound ([22], [26], [39], Ours)	r	γ	Dim.
Theorem 1	20,20,300,300	(0.250, 0.250, 0.250, 0.250)	1	0.267	174
Theorem 1	20,20,300,300	(0.250, 0.250, 0.222, 0.111)	2	0.133	121
Theorem 1	20,20,300,300	(0.250, 0.250, 0.188, 0.062)	3	0.082	171
Theorem 1	20,20,300,300	(0.250, 0.250, 0.160, 0.040)	4	0.061	149

- For a standard RSA modulus $N = PQ$ ($r = 1$), the bound $e > N^{\frac{1}{4}}$ is the same as previous results.
- For $r > 1$, our results are significantly better than those in [22,26,39].

Application to factoring RSA moduli

Corollary

Let $N = PQ$ be a given semi-smooth RSA subgroup modulus. For any fixed $\varepsilon > 0$, let

$$e \geq N^{\frac{1}{4}+\varepsilon}$$

be a given integer with a known factorization such that $e \mid \phi(N)$, where the number of prime factors of e is $O(\log \log N)$. We can factorize N in time polynomial of $\log N$.

- For the first time, a rigorous proof for the Naccache-Stern bound is presented.

Thank you for your attention