mathematics

MDPI

Article

Partial Key Attack Given MSBs of CRT-RSA Private Keys

Amir Hamzah Abd Ghafar [1,2], **Muhammad Rezal Kamel Ariffin** [1,2,*], **Sharifah Md Yasin** [1,3] **and Siti Hasana Sapar** [1,2]

[1] Institute for Mathematical Research, Universiti Putra Malaysia (UPM), Serdang 43400, Selangor Darul Ehsan, Malaysia; amir_hamzah@upm.edu.my (A.H.A.G.); ifah@upm.edu.my (S.M.Y.); sitihas@upm.edu.my (S.H.S.)

[2] Department of Mathematics, Faculty of Science, Universiti Putra Malaysia (UPM), Serdang 43400, Selangor Darul Ehsan, Malaysia

[3] Department of Computer Science, Faculty of Computer Science and Information Technology, Universiti Putra Malaysia (UPM), Serdang 43400, Selangor Darul Ehsan, Malaysia

* Correspondence: rezal@upm.edu.my

Received: 27 October 2020; Accepted: 22 November 2020; Published: 9 December 2020

check for updates

Abstract: The CRT-RSA cryptosystem is the most widely adopted RSA variant in digital applications. It exploits the properties of the Chinese remainder theorem (CRT) to elegantly reduce the size of the private keys. This significantly increases the efficiency of the RSA decryption algorithm. Nevertheless, an attack on RSA may also be applied to this RSA variant. One of the attacks is called partially known private key attack, that relies on the assumption that the adversary has knowledge of partial bits regarding RSA private keys. In this paper, we mount this type of attack on CRT-RSA. By using partial most significant bits (MSBs) of one of the RSA primes, p or q and its corresponding private exponent, d, we obtain an RSA intermediate. The intermediate is derived from $p-1$ and RSA public key, e. The analytical and novel reason on the success of our attack is that once the adversary has obtained the parameters: approximation of private exponent $\tilde{d}_p$, approximation of p, $\tilde{p}$ and the public exponent e where $\tilde{d}_p, \tilde{p}, e = N^{\alpha/2}$ where $0 < \alpha \leq 1/4$ such that $|d_p - \tilde{d}_p|, |p - \tilde{p}| < N^{\frac{1-\alpha}{2}}$ and has determined the largest prime of $\left\lfloor \frac{p-1}{e} \right\rfloor$, it will enable the adversary to factor the RSA modulus $N = pq$. Although the parameter space to find the prime factor is large, we show that one can adjust its "success appetite" by applying prime-counting function properties. By comparing our method with contemporary partial key attacks on CRT-RSA, upon determining a suitable predetermined "success appetite" value, we found out that our method required fewer bits of the private keys in order to factor N.

Keywords: CRT-RSA cryptosystem; cryptanalysis; partial-key exposure attack; prime counting function; Dickman's function

1. Introduction

RSA algorithm is known as one of the earliest public-key cryptosystems, introduced in 1977 [1]. However, its practical applications multiply in numbers with the coming of the digital age that requires swift key transportation mechanism to establish secure communication, either by encrypting a key or verifying a digital certificate. To ensure the encryption (or signing) and decryption (or verification) of RSA works, an RSA modulus $N = pq$ is introduced where $p \neq q$ and $p < q < 2p$. To encrypt or sign, an RSA public exponent, e is required such that it satisfies $\gcd(e, \phi(N)) = 1$ where $\phi(N)$ is Euler's totient function. To decrypt or verify, an RSA private exponent, d is required such that it satisfies the RSA key equation,

$$ed \equiv 1 \pmod{\phi(N)}.$$

One of the hard mathematical problems that become the sources of security for RSA is embedded in N and called an integer factorization problem. Since p and q are very large n-bit primes (typically $n = 1024$), the best current algorithm to factor N is still running in sub-exponential times using a method called general number field sieve [2]. Therefore, no modern computers yet can threaten the security of RSA.

As RSA algorithms need to be flexible and meet the demands of their applications, a lot of RSA variants have been introduced over the years. In this paper, we focus on a variant of RSA called Chinese remainder theorem (CRT) RSA cryptosystem [3]. This variant applies the result from the Chinese remainder theorem by utilizing two private exponents, d_p and d_q, instead of a single private exponent in standard RSA. These private exponents are derived from the original d with respect to its corresponding RSA primes, p and q. The addition in numbers of private exponents in CRT-RSA may require additional modular exponentiations, but the computations in CRT-RSA are significantly faster compared to the computations in standard RSA, since d_p and d_q are significantly smaller in size compared to the original d [4]. Due to this speed up, CRT-RSA is ubiquitous in many cryptographic implementations today.

For the past attacks on RSA and its variants to be successful, an adversary needs to gain certain advantages. One of the advantages is that the adversary knows partial bits of RSA private parameters, d and p and/or q. The bits may be derived from their most significant bits (MSBs) or least significant bits (LSBs). This assumption is realistic since there is a method called side-channel attacks that is helpful to retrieve certain bits of parameters from cryptographic devices [5].

Using the partially known bits, an adversary can conduct an attack called partial key exposure attack. This kind of attack initially was executed on a standard RSA cryptosystem by [6], where they showed that $2/3$ bits of p or q are required to factor N using an integer programming technique. Then, Ref. [7] reduced the required value of bits to $1/2$ using the LLL algorithm. This method utilizes a lattice-based approach to find the small solution of polynomials modulo N that consequently results in the factorization of N. It then proliferated other partial key exposure attacks on standard RSA cryptosystem [8–10]. For the collection of this type of attack on standard RSA cryptosystem, refer to [11].

In 2003, Ref. [12] showed that partial key exposure attack can also be conducted on CRT-RSA. Given an approximation d_p, called $\tilde{d_p}$, that has half of the MSBs of d_p, they showed that factorization of N can be solved easily. Particularly, d_p satisfies $ed_p \equiv 1 \pmod{p-1}$ within the CRT-RSA key equation, and given $\tilde{d_p}$ such that $|d_p - \tilde{d_p}| < N^{1/4-\alpha}$ for some α that satisfy $e = N^{\alpha} < N^{1/4}$ where e is the public exponent of CRT-RSA, then N can be factored in polynomial time. It then can be generalized to $|d_p - \tilde{d_p}| < N^{1/4}$ if e is very small, which occurs greatly in most implementations. This result utilized an approach using lattice-based approximation which has been extended in [13–15].

Another method of attacking CRT-RSA is using a key reconstruction algorithm by [16]. The method is motivated by the capability of a newly introduced side-channel attack called cold boot attacks [17]. It systematically constructs bits of RSA private keys namely RSA private exponent and RSA primes from any random bit positions as its initial point. The method only requires at least 0.27 bits from any bit position of p, q, d, d_p, d_q. If this condition is fulfilled, then the adversary can solve the factorization of N in polynomial time using the lattice-based method. In more recent work, Ref. [18] proposed an improvement of past attacks by showing an attack that requires less amount of leaked MSBs for all $e < N^{0.375}$. The attack can be conducted by selecting better lattice constructions of the underlying polynomials created from the obtained partial information.

Our contribution. We take a novel approach in conducting partial key exposure attack on CRT-RSA by proving that by knowing the largest prime factor of $\left\lfloor \frac{p-1}{e} \right\rfloor$ called a_1, N can be factored in polynomial time if the conditions on the approximations of d_p and p are satisfied. We also extend this result by showing the difficulties of finding a_1 can be reduced by having sufficient combinations of computing power and success appetites.

Organization of the article. In Section 2, we show the CRT-RSA key generation algorithm in its full form. We also introduce a certain theorem, definition and lemmas that will be utilized in our attack. In Section 3, we introduce our attack by parts. First, we show the conditions required to conduct our attack. Then, we proceed with the attack by proving that by knowing the largest prime factor of $\left\lfloor \frac{p-1}{e} \right\rfloor$ called a_1, our attack can factor N in polynomial time using conditions from the first part of the attack. In Section 4, we estimate the number of primes that can be the candidates for the largest prime factor of $\left\lfloor \frac{p-1}{e} \right\rfloor$ using a theorem provided before. Then, in Section 5, we estimate the number of primes that can be the candidates for the largest prime factor of $\left\lfloor \frac{p-1}{e} \right\rfloor$ if based on various success appetites which have been pre-defined. By using this estimation, we discuss our method compared to other methods that attacked CRT-RSA in Section 6 before we finally conclude our paper in Section 7.

2. Preliminaries

One of the earliest variations of the RSA cryptosystem is to decrypt the plaintext using Chinese remainder theorem or CRT (more on CRT can be read here [19]). This variant, called CRT-RSA, is proposed by the creators of RSA in their patent application [3]. The rationale of using the concept is to utilize much smaller parameter size in the decryption algorithm specifically during computing the modular exponentiation computation. As we shall see, in Algorithm 1, the key generation algorithm of CRT-RSA employs almost similar computations compared to the standard process. However, the difference lies in additional computations of

$$d_p \equiv e^{-1} \pmod{p-1}$$

and

$$d_q \equiv e^{-1} \pmod{q-1}$$

which we called **CRT exponents** as in Algorithm 1 (line 5 and line 6). The CRT-RSA key generation algorithm is as follows:

Algorithm 1 Chinese remainder theorem (CRT)-RSA Key Generation Algorithm

```
Input: Security parameter, $n$
Output: RSA public keys $(N, e)$, and RSA private keys $(p, q, \phi(N), d_p, d_q)$
1: Generate randomly two distinct of $n$-bit primes $p$ and $q$, where $p < q < 2p$.
2: Compute $N = pq$.
3: Compute $\phi(N) = (p-1)(q-1)$.
4: Choose $e$ such that $e < \phi(N)$ and $\gcd(e, \phi(N)) = 1$.
5: Compute $d_p$ such that $ed_p \equiv 1 \pmod{p-1}$.
6: Compute $d_q$ such that $ed_q \equiv 1 \pmod{q-1}$.
7: Output $(N, e)$ as RSA public keys and $(p, q, \phi(N), d_p, d_q)$ as RSA private keys.
```

In this paper, supposing $e = N^{\frac{\alpha}{2}}$, we assume that the adversary is given a fraction α of the MSBs of d_p and p (or q). We shall see that by having this information, the adversary can derive an important intermediate that allows us to find d in polynomial time, thus factoring N in polynomial time. However, to find the greatest prime factor of the intermediate that can enable our attack, we need to count the number of primes that can be the suitable candidates for our greatest prime factor. To achieve that, we need to utilize the prime counting function as follows: (See [20], (Theorem 6.9)).

Theorem 1. *Let $\pi(X)$ be a function estimating number of primes $\leq X$. Then*

$$\pi(X) \leq \frac{X}{\ln X}\left(1 + \frac{1}{\ln X} + \frac{2.334}{\ln^2 X}\right)$$

for $X \geq 2953652287$.

After the adversary can count the number of primes that can be the suitable candidates for our greatest prime factor, the adversary need to know the probability of finding the prime in a known parameter space. This probability will help the adversary to adjust the success appetite of the attack and consequently determine whether the attack is feasible, based on the computational ability of the adversary. To estimate the probability, we require an application of the prime number theorem called Dickman's function. Given a real number value, this function computes the probability of the greatest prime factor of an integer to be less than the given value. We call this function a Dickman's function [21,22] and it is defined as below:

Definition 1 (Dickman's function)**.** *The probability function that a random integer between 1 and N will have its greatest prime factor less than* N^{ζ} *is defined through the integral equation*

$$F(\zeta) = \int_0^{\zeta} F(t/(1-t))\frac{dt}{t}$$

for $0 \leq \zeta \leq 1$.

Dickman's function is defined in a form of cumulative distribution function. It is important to determine the distribution of the greatest prime factor of a given value. For example, let $\zeta = 1/2$ then

$$\begin{aligned} F(1/2) &= \textstyle\int_0^{1/2} F(t/(1-t))\frac{dt}{t} = 1 - \int_{1/2}^{1} F(t/(1-t))\frac{dt}{t} \\ &= 1 - \textstyle\int_{1/2}^{1} \frac{dt}{t} = 1 + \ln(1/2) = 0.3068. \end{aligned} \tag{1}$$

This means that for any random integer N, there is a probability of 0.3068 that its greatest prime factor is less than $N^{1/2}$. Next, we require these two lemmas to help us in the attack.

Lemma 1. *Let* $u, v, w \in \mathbb{Z}$ *where* $v < u < v + w$. *If* $\lfloor \frac{u}{w} \rfloor = \frac{u}{w} - \epsilon_1$ *and* $\lfloor \frac{v}{w} \rfloor = \frac{v}{w} - \epsilon_2$ *such that* $\epsilon_2 - \epsilon_1 < 0$, *then* $\lfloor \frac{u}{w} \rfloor = \lfloor \frac{v}{w} \rfloor$.

Proof. Observe that

$$0 < u - v < w \quad \Rightarrow \quad 0 < \frac{u}{w} - \frac{v}{w} < 1.$$

Since

$$0 < \frac{u}{w} \quad \Rightarrow \quad 0 \leq \left\lfloor \frac{u}{w} \right\rfloor < \frac{u}{w} \tag{2}$$

and

$$0 < \frac{v}{w} \quad \Rightarrow \quad 0 \leq \left\lfloor \frac{v}{w} \right\rfloor < \frac{v}{w}. \tag{3}$$

If $\lfloor \frac{u}{w} \rfloor = \frac{u}{w} - \epsilon_1$ and $\lfloor \frac{v}{w} \rfloor = \frac{v}{w} - \epsilon_2$ for $\epsilon_2 - \epsilon_1 < 0$, computing (2) and (3) will get

$$\begin{aligned} 0 \leq \left\lfloor \frac{u}{w} \right\rfloor - \left\lfloor \frac{v}{w} \right\rfloor &= \left(\frac{u}{w} - \epsilon_1\right) - \left(\frac{v}{w} - \epsilon_2\right) \\ &= \left(\frac{u}{w} - \frac{v}{w}\right) + (\epsilon_2 - \epsilon_1) \\ &< 1 + (\epsilon_2 - \epsilon_1) < 1 + 0 = 1 \end{aligned} \tag{4}$$

Since $\lfloor \frac{u}{w} \rfloor$ and $\lfloor \frac{v}{w} \rfloor$ are integers, $\lfloor \frac{u}{w} \rfloor - \lfloor \frac{v}{w} \rfloor = 0 \Rightarrow \lfloor \frac{u}{w} \rfloor = \lfloor \frac{v}{w} \rfloor$. □

This result will help us to enable the attack later presented in Theorem 2.

Lemma 2. *If an integer H divides* $\lfloor \frac{rs}{t} \rfloor$ *then* $\lfloor \frac{rs}{t} \rfloor \cdot \frac{1}{H} = \lfloor \frac{rs}{tH} \rfloor$.

Proof. Let $\frac{rs}{t} = z_1 + \frac{r'}{t}$ for some integer z_1 and r' where $r' < t$. Then

$$\begin{aligned}\left\lfloor \frac{rs}{t} \right\rfloor \cdot \frac{1}{H} &= \left\lfloor z_1 + \frac{r'}{t} \right\rfloor \cdot \frac{1}{H} \\ &= \lfloor z_1 \rfloor \cdot \frac{1}{H} \\ &= \frac{z_1}{H}\end{aligned}$$

If H divides $\left\lfloor \frac{rs}{t} \right\rfloor$ then H will also divides z_1. Hence $\frac{z_1}{H} = z_2$ for some integer $z_2 \in \mathbb{Z}$. That is,

$$\left\lfloor \frac{rs}{t} \right\rfloor \cdot \frac{1}{H} = z_2. \tag{5}$$

Then

$$\begin{aligned}\left\lfloor \frac{rs}{tH} \right\rfloor &= \left\lfloor \frac{z_1}{H} + \frac{r'}{tH} \right\rfloor \\ &= \left\lfloor \frac{z_1}{H} \right\rfloor \\ &= \lfloor z_2 \rfloor \\ &= z_2.\end{aligned} \tag{6}$$

Comparing (5) and (6), This completes the proof. □

The above results will help us to enable the attack later presented in Theorem 2.

3. The Attack

The initial strategy in our attack is to find the conditions on the approximations of d_p and p to enable our attack. By using these conditions, we shall prove mathematically that there exists an unknown intermediate that will help us to find the factorization of N in polynomial time.

First, to find the conditions on the approximations of d_p and p, we need the following lemma regarding an approximation of p.

Lemma 3. *Let $N = pq$ with $p < q < 2p$. If there exists $\tilde{p}$ where $|p - \tilde{p}| < p^{1-\alpha}$ then $(p-1)\tilde{p} > \frac{1}{8}N$.*

Proof. From $p < q < 2p$ we know

$$p^2 < pq < 2p^2 \Rightarrow p < N^{1/2} < \sqrt{2}p \tag{7}$$

and

$$pq < q^2 < 2pq \Rightarrow N^{1/2} < q < 2N^{1/2} \tag{8}$$

Combining (7) and (8), we get $p < N^{1/2} < q$. Since p and q are of the same bit length, observe

$$p > p - 1 > \frac{q}{2} > \frac{N^{1/2}}{2}. \tag{9}$$

Suppose $|p - \tilde{p}| < p^{1-\alpha}$. This implies $\tilde{p}$ shares the same a fraction α of the MSBs with p and subsequently $\tilde{p} > \frac{p}{2}$. Thus

$$\begin{aligned}(p-1)\tilde{p} &> \frac{N^{1/2}}{2}\tilde{p} > \frac{N^{1/2}}{2}\frac{p}{2} > \frac{N^{1/2}}{2}\frac{N^{1/2}}{4} \\ &= \frac{1}{8}N.\end{aligned}$$

This completes the proof. □

The next lemma assumes that $p < q < 2p$, then we show that, by having a fraction α of the MSBs of p and q of CRT-RSA modulus, we can get an approximation of p to a certain bound.

Lemma 4. *Let $N = pq$ be an CRT-RSA modulus with $p < q < 2p$. If a fraction α of the MSBs of p or q are known then we can find $\tilde{p}$ such that $|p - \tilde{p}| < N^{\frac{1-\alpha}{2}}$.*

Proof. We know that if $p < q < 2p$ then $p^2 < N < 2p^2$. Observe $p < N^{1/2} < \sqrt{2}p$. If a fraction α of the MSBs of p are known then we can find $\tilde{p}$ which consists of a fraction α of the MSBs of p such that

$$|p - \tilde{p}| < p^{1-\alpha} < N^{\frac{1-\alpha}{2}}.$$

On the side of q, since $N^{1/2} < q^2 < 2pq \Rightarrow N^{1/2} < q < (2N)^{1/2}$, if a fraction α of the MSBs of q are known, then

$$|q - \tilde{q}| < q^{1-\alpha} < (2N)^{\frac{1-\alpha}{2}}.$$

Since q and $\tilde{q}$ shares the same a fraction α of the MSBs, then $\tilde{q} < (2N)^{1/2}$. Given $\tilde{q}$, we can compute $\tilde{p} = \frac{N}{\tilde{q}}$ which satisfies

$$|p - \tilde{p}| = \left|\frac{N}{q} - \frac{N}{\tilde{q}}\right| = \left|\frac{N(\tilde{q} - q)}{q\tilde{q}}\right| < \frac{N((2N)^{\frac{1-\alpha}{2}})}{2N} < N^{\frac{1-\alpha}{2}}.$$

This completes the proof. □

From Lemma 4, we know that by having a fraction α of MSBs of p or q, we can obtain an approximation of p called $\tilde{p}$ where $|p - \tilde{p}| < N^{\frac{1-\alpha}{2}}$. This approximation of p will enable the next lemma to find k_p given a fraction α of the MSBs of d_p and $\tilde{p}$ where $ed_p = 1 + k_p(p-1)$ and $|p - \tilde{p}| < N^{\frac{1}{2}-\alpha}$.

Lemma 5. *Let $N = pq$ be an CRT-RSA modulus with $p < q < 2p$. Suppose $e = N^{\frac{\alpha}{2}}$ be a valid public exponent with $0 < \alpha \leq 1/4$ and d_p be its corresponding private exponent which satisfies CRT-RSA key equation $ed_p = 1 + k_p(p-1)$. If a fraction α of the MSBs of d_p and p (or q) are known, then the constant k_p in the key equation can be determined, up to a small constant additive error, in time polynomial in $\log(N)$.*

Proof. Recall that one of the private exponent of CRT-RSA satisfies $ed_p = 1 + k_p(p-1)$. So, we can write

$$k_p = \frac{ed_p - 1}{p - 1} \tag{10}$$

If a fraction α of the MSBs of d_p are known, then we have $\tilde{d_p}$ such that $|d_p - \tilde{d_p}| < d_p^{1-\alpha} < N^{\frac{1}{2}(1-\alpha)}$. From Lemma 4, if we have a fraction α of the MSBs of p (or q) are known then we have $\tilde{p}$ such that $|p - \tilde{p}| < p^{1-\alpha} < N^{\frac{1}{2}(1-\alpha)}$. $\tilde{k}_p$ is given by

$$\tilde{k}_p = \left\lceil \frac{e\tilde{d_p} - 1}{\tilde{p}} \right\rfloor = \frac{e\tilde{d_p} - 1}{\tilde{p}} + \epsilon,$$

for some $|\epsilon| \leq 1/2$, reveals some of the most significant bits of k_p. In particular, notice that

$$\begin{aligned}
|k_p - \tilde{k}_p| &= \left| \frac{ed_p - 1}{p-1} - \left\lceil \frac{e\tilde{d_p} - 1}{\tilde{p}} \right\rfloor \right| = \left| \frac{ed_p - 1}{p-1} - \frac{e\tilde{d_p} - 1}{\tilde{p}} + \epsilon \right| \\
&= \left| \frac{\tilde{p}(ed_p - 1)}{(p-1)\tilde{p}} - \frac{(p-1)(e\tilde{d_p} - 1)}{(p-1)\tilde{p}} + \epsilon \right| \\
&= \left| \frac{\tilde{p}ed_p - \tilde{p} - pe\tilde{d_p} + p + e\tilde{d_p} - 1}{(p-1)\tilde{p}} + \epsilon \right| \\
&= \left| \frac{\tilde{p}ed_p - \tilde{p} - \tilde{p}e\tilde{d_p} + \tilde{p}e\tilde{d_p} - pe\tilde{d_p} + p + e\tilde{d_p} - 1}{(p-1)\tilde{p}} + \epsilon \right| \\
&< \left| \frac{\tilde{p}e(d_p - \tilde{d_p})}{(p-1)\tilde{p}} + \frac{(\tilde{p} - p)(e\tilde{d_p} - 1)}{(p-1)\tilde{p}} + \epsilon \right| \\
&< \left| \frac{e(d_p - \tilde{d_p})}{(p-1)} + \frac{(\tilde{p} - p)(e\tilde{d_p})}{(p-1)\tilde{p}} + \epsilon \right|.
\end{aligned} \tag{11}$$

If $(p-1)\tilde{p} > \frac{1}{8}N$ as in Lemma 3, then (11) will be

$$|k_p - \tilde{k}_p| < \left| N^{\frac{\alpha}{2} + \frac{1}{2}(1-\alpha) - \frac{1}{2}} + 8N^{\frac{1}{2}(1-\alpha) + \frac{\alpha}{2} + \frac{1}{2} - 1} + \epsilon \right| < 10$$

for large N. Hence, the constant k_p will be in the range $\{\tilde{k}_p - 10, \tilde{k}_p + 10\}$. Since k_p can be computed in time polynomial in $\log(N)$. This completes the proof. □

Lemma 5 shows the significance of knowing a fraction α of the MSBs of d and p, in order to find k_p. It also shows that the conditions presented in Lemma 5 must be carried throughout the attack since it enables the attack. The value of k_p obtained in Lemma 5 is utilized in the next proposition.

Proposition 1. *Let $N = pq$ be an CRT-RSA modulus with $p < q < 2p$ and $|p - \tilde{p}| < N^{\frac{1}{2}-\alpha}$. Suppose $e = N^{\frac{\alpha}{2}}$ be a valid public exponent with $0 < \alpha \leq 1/4$ and d_p be its corresponding private exponent, which satisfies $ed_p = 1 + k_p(p-1)$. Let $ed'_p = 1 \pmod{k_p}$ for some $d'_p \in \mathbb{Z}$ then $d_p = k_p \left\lfloor \frac{(p-1)}{e} \right\rfloor + d'_p$.*

Proof. Observe that

$$\begin{aligned}
ed_p &= 1 + k_p(p-1) && (12) \\
ed'_p &= 1 + k'_p k_p. && (13)
\end{aligned}$$

for some $k'_p \in \mathbb{Z}$. Substitute value of e in (12) into (13), we obtain

$$\begin{aligned}
\left(\frac{1 + k_p(p-1)}{d_p} \right) d'_p &= 1 + k'_p k_p \\
d'_p + d'_p k_p(p-1) &= d_p + d_p k'_p k_p
\end{aligned} \tag{14}$$

Rearranging (14), we have

$$\begin{aligned}
d_p &= d'_p k_p(p-1) - d_p k'_p k_p + d'_p \\
&= k_p(d'_p(p-1) - d_p k'_p) + d'_p.
\end{aligned} \tag{15}$$

The term $d'_p(p-1) - dk'_p$ can become

$$\begin{aligned}
d'_p(p-1) - d_pk'_p &= \frac{1+k'_pk}{e}(p-1) - d_p\frac{d'_pe-1}{k_p} \\
&= \frac{(p-1)k_p(1+k'_pk_p) - ed_p(d'_pe-1)}{k_pe} \\
&= \frac{(p-1)k_p(1+k'_pk_p) - ((p-1)k_p+1)(d'_pe-1)}{k_pe} \\
&= \frac{(p-1)k_p(1+k'_pk_p) - ((p-1)k_p)(d'_pe-1)+1}{k_pe} - \frac{d'_p}{k_p} \\
&= \frac{(p-1)k_p(1+k'_pk_p) - ((p-1)k_p)(d'_pe-1)}{k_pe} + \frac{1-ed'_p}{k_pe} \\
&= \frac{(p-1)k_p(1+k'_pk_p) - ((p-1)k_p)(d'_pe-1)}{k_pe} - \frac{k'_pk_p}{k_pe} \\
&= \frac{(p-1)k_p(1+k'_pk_p) - ((p-1)k_p)(d'_pe-1)}{k_pe} - \frac{k'_p}{e} \\
&> \left(\frac{(p-1)}{e}\left(k'_pk_p - d'_pe + 2\right)\right) - 1
\end{aligned} \tag{16}$$

since $\frac{k'_p}{e} < 1$. If $ed'_p = 1 + k'_pk_p$ then $k'_pk_p - d'_pe = -1$. Thus, (16) become

$$\begin{aligned}
d'_p(p-1) - d_pk'_p &> \left(\frac{(p-1)}{e}(-1+2)\right) - 1 \\
&= \frac{(p-1)}{e} - 1.
\end{aligned} \tag{17}$$

This implies that $\frac{(p-1)}{e} - (d'_p(p-1) - d_pk'_p) < 1$. Since $d'_p(p-1) - d_pk'_p$ is always an integer, $d'_p(p-1) - d_pk'_p = \left\lfloor \frac{(p-1)}{e} \right\rfloor$. Now, we can see that

$$d_p = k_p\left\lfloor \frac{(p-1)}{e} \right\rfloor + d'_p. \tag{18}$$

This completes the proof. □

Remark 1. *Equation (18) shows that under assumption of Proposition 1, which values d'_p and k'_p are known, it is crucial that $\left\lfloor \frac{(p-1)}{e} \right\rfloor$ is kept secret.*

The next theorem shows the implication of the results from Proposition 1 in our aim to factor CRT-RSA modulus in polynomial time.

Theorem 2. *Let $N = pq$ be a CRT-RSA modulus with $p < q < 2p$. Suppose $e = N^{\frac{\alpha}{2}}$ be a valid public exponent with $0 < \alpha \leq 1/4$ and d_p be its corresponding private exponent which satisfies $ed_p = 1 + k_p(p-1)$. Let $ed'_p = 1 + k'_pk_p$ for some $k_p, k'_p, d'_p \in \mathbb{Z}$. Let a_1 be one of the prime factor of $\left\lfloor \frac{(p-1)}{e} \right\rfloor = a_1^{b_1} \cdot a_2^{b_2} \cdot \ldots \cdot a_n^{b_n} = \prod_{i=1}^{n} a_i^{b_i}$ such that $|(p-1) - \tilde{p}| < ea_1$. Suppose $\left\lfloor \frac{\tilde{p}}{ea_1} \right\rfloor = \frac{\tilde{p}}{ea_1} - \epsilon_1$ and $\left\lfloor \frac{p-1}{ea_1} \right\rfloor = \frac{p-1}{ea_1} - \epsilon_2$ such that $\epsilon_2 - \epsilon_1 < 0$. If a_1 and a fraction α of the MSBs of d_p and p (or q) are known then N can be factored in polynomial time.*

Proof. If a_1 satisfies $|(p-1)-\tilde{p}| < ea_1$, and $\left\lfloor \frac{\tilde{p}}{ea_1} \right\rfloor = \frac{\tilde{p}}{ea_1} - \epsilon_1$ and $\left\lfloor \frac{p-1}{ea_1} \right\rfloor = \frac{p-1}{ea_1} - \epsilon_2$ such that $\epsilon_2 - \epsilon_1 < 0$, from Lemma 1, we obtain

$$\left\lfloor \frac{\tilde{p}}{ea_1} \right\rfloor = \left\lfloor \frac{(p-1)}{ea_1} \right\rfloor \tag{19}$$

Lemma 2 implies if a_1 divides $\left\lfloor \frac{(p-1)}{e} \right\rfloor$ then $\left\lfloor \frac{(p-1)}{e} \right\rfloor \cdot \frac{1}{a_1} = \left\lfloor \frac{(p-1)}{e \cdot a_1} \right\rfloor$. This also implies

$$\left\lfloor \frac{(p-1)}{e} \right\rfloor \cdot \frac{a_1}{a_1} = \left\lfloor \frac{(p-1)}{e \cdot a_1} \right\rfloor a_1 \tag{20}$$

From Proposition 1,

$$\begin{aligned} d_p &= k_p \left\lfloor \frac{(p-1)}{e} \right\rfloor + d_p' \\ &= k_p \frac{a_1}{a_1} \left\lfloor \frac{(p-1)}{e} \right\rfloor + d_p' \\ &= k_p a_1 \left\lfloor \frac{(p-1)}{ea_1} \right\rfloor + d_p' \\ &= k_p a_1 \left\lfloor \frac{\tilde{p}}{ea_1} \right\rfloor + d_p'. \end{aligned} \tag{21}$$

If $\tilde{p}$ and a fraction α of the MSBs of d_p are known, based on Lemma 5, we can find k_p in polynomial time. Then, we can compute d_p' as $d_p' \equiv 1/e \pmod{k_p}$. If a_1 is known, we can compute d_p in (21). Using the value of d_p, we can obtain p by computing $p = \frac{ed_p - 1}{k_p} + 1$ and factorizes N. This completes the proof. □

Remark 2. *We have shown that given α most significant bits of d_p and p, the complexity of factoring N depends on knowing the factor of $\left\lfloor \frac{(p-1)}{ea_1} \right\rfloor$. This demonstrates that we have reduced one of the hard problems of RSA from factoring N to factoring $\left\lfloor \frac{(p-1)}{ea_1} \right\rfloor$. However, the complexity of factorization is still sub-exponential according to the current factorization technique.*

We construct an algorithm based on our attack. The parameters used in the algorithm are described in Table 1:

Table 1. List of Parameters Used in the Attack.

Parameters known before the attack:	• RSA public keys, (N, e) • approximation of d, $\tilde{d}_p$ • approximation of p, $\tilde{p}$ • a prime factor of $\left\lfloor \frac{(p-1)}{e} \right\rfloor$, a_1
Parameters known during the attack:	• Constant from CRT-RSA key Equation (10), k_p • Intermediate of (13), $\tilde{k}_p$ • Intermediate of (13), d_p'
Parameters known after the attack:	• CRT-RSA private exponent, d_p • CRT-RSA private key, p • CRT-RSA private key, q

The algorithm takes the input of RSA public keys (N, e) and a prime factor of $\left\lfloor \frac{(p-1)}{e} \right\rfloor$, a_1 that satisfies $|(p-1)-\tilde{p}| < ea_1$, given a fraction α of the MSBs of d_p and $\tilde{p}$. The algorithm is as follows:

Remark 3. *Since we assume that the value of a_1 is already known in Algorithm 2, the algorithm runs in polynomial time.*

The following is an example to illustrate Algorithm 2.

Algorithm 2 Factoring N of CRT-RSA via Theorem 2

```
Input: CRT-RSA public keys $(N, e)$, $\tilde{d}_p, \tilde{p}$ and prime factor of $\left\lfloor \frac{(p-1)}{e} \right\rfloor$, $a_1$
Output: $p, q$
 1: Compute $\tilde{k}_p = \left\lceil \frac{e\tilde{d}_p - 1}{\tilde{p}} \right\rceil$.
 2: Set $k_p \in \{\tilde{k}_p - 10, \tilde{k}_p + 10\}$.        ▷ Step 1 until 2 are based on Lemma 5
 3: for each $k_p$ do
 4:     Compute $d'_p \equiv e^{-1} \pmod{k_p}$
 5:     Compute $d_p = k_p \cdot a_1 \cdot \left\lfloor \frac{\tilde{p}}{ea_1} \right\rceil + d'_p$.
 6:     Compute $p' = \frac{ed_p - 1}{k_p} + 1$.
 7:     if $p' \in \mathbb{Z}$ then
 8:         Compute $q' = N/p'$.
 9:         if $q' \in \mathbb{Z}$ then
10:             Set $q = q'$.
11:         end if
12:         Set $p = p'$.
13:     end if
14: end for
15: Output $p$ and $q$
```

Example 1. *We use RSA-2048 in this example. Specifically, we are given*

$$
\begin{aligned}
N \quad = \quad & 268540419852383752124757781646760115726806634309406581074841646 78 \\
& 818810094752469751648037573551844196485950558863751590032474784 39 \\
& 921437412557306326108278884401657509117670049123360590970470225653 \\
& 673701911936889363297131638788931985028007516345491386397309288 12 \\
& 401425058761393220630657089767369455446755632318574748297537573 64 \\
& 894611626926354574456629455105347452788310043288302994462775661 22 \\
& 876871690049262391946504470641295926369660224645723012456372347 70 \\
& 502946474809229685432563429452630363461587950458888108014233919 16 \\
& 977362834773650286859490282783251469037487901444550330085321164 17 \\
& 8989582093892246325688605122444 1
\end{aligned}
$$

and $e = 2588040962967479019863275440499$ *which is about* $N^{0.05}$*. Let*

$$
\begin{aligned}
\tilde{d}_p \quad = \quad & 360556072312027752830808020096526196788485792026768353595223372 32 \\
& 453046482103828822629034801599272511981342175383384176100106636 88 \\
& 390778357971320439782824120168506888845409074208686481856096377 54 \\
& 110635060134491294562654457439311279810441309784833614308576930 84 \\
& 40916227786667499669328426663847808738852591212
\end{aligned}
$$

where a fraction α of the MSBs of d_p are given such that $|d_p - \tilde{d_p}| < d_p^{1-\alpha}$. In this case, $\alpha = 0.1$ or about 10% (103-bits) bits of its original, d_p. Then, let

$$\begin{aligned}\tilde{p} \quad = \quad & 14367613307214246903591926069142770099295123891127829274068843132\\ & 84507873128193703874025274483229621351740372731847216208987451381\\ & 22600446098472260720529957802520996016314325569094216775717168908\\ & 41782721517081770370921396206536643264683692385497895745823983436\\ & 077015609406740888486197789102004162673736698020 4\end{aligned}$$

where a fraction α of the MSBs of p (or q) are also given, such that $|p - \tilde{p}| < p^{1-\alpha}$. From Lemma 5, given $\tilde{d_p}$ and $\tilde{p}$, we obtain $\tilde{k}_p$ and proceed to recover $k_p = 6494703501810202246856940 2425$ in polynomial time. Then, we compute

$$\begin{aligned} d'_p \quad & \equiv \quad e^{-1} \pmod{k_p}\\ & \equiv \quad 1429183232878563009651447 1874 \pmod{6494703501810202246856940 2425}\end{aligned}$$

Given that we also know one of the prime factor of $\lfloor \frac{p}{e} \rfloor$,

$$\begin{aligned} a_1 \quad = \quad & 43185843225970563415154944273587881760667418641821175935878843801\\ & 62779147404915309140284507695180396733831689901698607027115346112\\ & 71569728695701943263595028176276635021689474779238127599104918615\\ & 72151376677546400416324969826940325349800202462521919212154035625\\ & 31983030526947\end{aligned}$$

such that $|\tilde{p} - p| < ea_1$. Then

$$\begin{aligned} d_p \quad & = \quad k_p \cdot a_1 \cdot \left\lfloor \frac{\tilde{p}}{ea_1} \right\rfloor + d'_p\\ & = \quad 36055607231202775283080802009649108834176664752875840471779128853\\ & \qquad 65479408662427699263008533084770049815277792852591783505517277427\\ & \qquad 76754417366858919379167907800491269897943246773311982875789843868\\ & \qquad 49579557361199476994871376824209224903108180826295016253816460096\\ & \qquad 0201663771475059064946051225399729968771990 7999.\end{aligned}$$

By knowing d_p, we can get

$$\begin{aligned} p \quad & = \quad \frac{ed_p - 1}{k_p} + 1\\ & = \quad 14367613307214246903591926069142452203848898341656376495846139272\\ & \qquad 96888354084505142420920972987941360124023642545598929784435347521\\ & \qquad 29827893551421260667238347559758806433514905636985352008519026850\\ & \qquad 47195482010956044783038279094608638461799318081089013845804738749\\ & \qquad 489723986572380341329335562143499823477229124398 1.\end{aligned}$$

and

$$\begin{aligned} q &= N/p \\ &= 18690677018537559979968031085225887816085307412051352387412281562 \\ &\quad 63664879599722127409077204025890837680223683840960510872264130729 \\ &\quad 19499428723542093381211298664979433605748124826497957558030353615 \\ &\quad 18738757121243839997910925158423130594718234233298178099345593794 \\ &\quad 914232287044653237871292153157051592537039121366 1. \end{aligned}$$

N has been successfully factored.

Figure 1 shows the flowchart based on Algorithm 2:

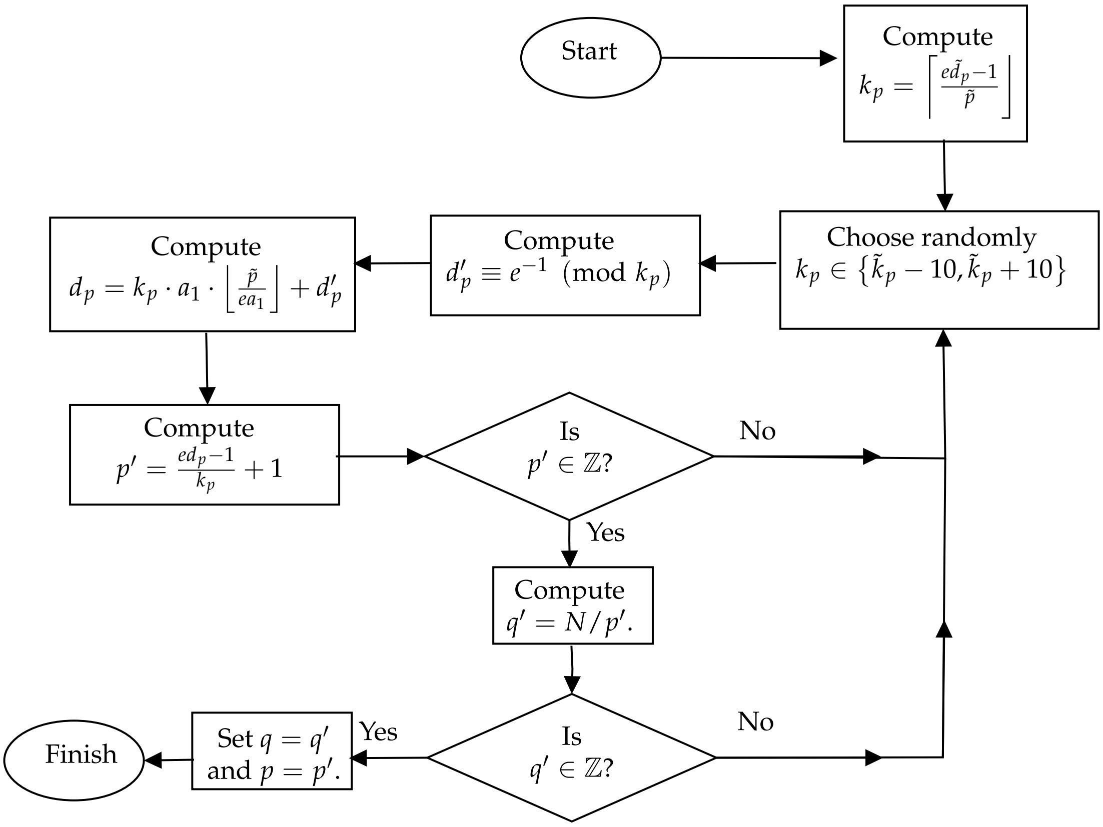
Start
Compute $k_p = \left\lceil \frac{e\tilde{d}_p - 1}{\tilde{p}} \right\rceil$
Choose randomly $k_p \in \{\tilde{k}_p - 10, \tilde{k}_p + 10\}$
Compute $d'_p \equiv e^{-1} \pmod{k_p}$
Compute $d_p = k_p \cdot a_1 \cdot \left\lfloor \frac{\tilde{p}}{ea_1} \right\rfloor + d'_p$
Compute $p' = \frac{ed_p - 1}{k_p} + 1$
Is $p' \in \mathbb{Z}$?
No
Yes
Compute $q' = N/p'$.
Is $q' \in \mathbb{Z}$?
No
Yes
Set $q = q'$ and $p = p'$.
Finish

Figure 1. Flowchart of Algorithm 2.

Our Attack in RSA Implementation

In most RSA implementations, RSA public exponent e is a small integer. The reason for this choice is to optimize the computing time of the RSA encryption algorithm. In this part, we investigate the implication of the size of e in our attack. Typically, $e = 2^{16} + 1$. Since we set $e = N^{\frac{\alpha}{2}}$ in our attack, observe that

$$\alpha = 2 \log_N e \approx 2 \log_{2^{2048}} 2^{16} + 1 \approx 0.01562$$

in the implementation of RSA-2048.

This implicates that our attack requires $0.01562 \cdot 2048 = 31.98976$ or about 32 bits of d_p and p to be exposed since $|d_p - \tilde{d}_p| < N^{1-\alpha}$ and $|p - \tilde{p}| < p^{1-\alpha}$. The exposed bits may come from the side-channel attack or a brute-force method, since the number of bits that are required are quite small. The number of exposed bits that are required can be reduced, if the size of N or e is smaller.

4. Estimating Number of Candidates for a_1

To find an a_1 that satisfy $|(p-1)-\tilde{p}| < ea_1$ posed in Theorem 2, we can anticipate that a_1 to be the largest prime factor of $\left\lfloor \frac{(p-1)}{e} \right\rfloor$. We need to estimate the number of primes that are eligible to be a_1. However, first, the next lemma modifies the result by [20] and applies it to show an estimation of the number of primes between two bounds.

Lemma 6. *Let N^{ζ} and N^{θ} respectively be the upper and lower bounds of a_1 where $0 < \theta < \zeta < 1$. Then, the number of primes between N^{ζ} and N^{θ} will be less than $N^{\zeta}\left(\frac{1}{\ln N^{\zeta}}\right)\left(1+\frac{1}{\ln N^{\theta}}+\frac{2.334}{\ln^2 N^{\theta}}\right)$.*

Proof. Let F be the number of primes less than the upper bound of a_1 and G be the number of primes less than the lower bound of a_1. Then, according to Theorem 1,

$$F = \frac{N^{\zeta}}{\ln N^{\zeta}}\left(1+\frac{1}{\ln N^{\zeta}}+\frac{2.334}{\ln^2 N^{\zeta}}\right)$$

and

$$G = \frac{N^{\theta}}{\ln N^{\theta}}\left(1+\frac{1}{\ln N^{\theta}}+\frac{2.334}{\ln^2 N^{\theta}}\right).$$

To estimate the number of candidates of a_1, we need to calculate

$$\begin{aligned} F-G &= \frac{N^{\zeta}}{\ln N^{\zeta}}\left(1+\frac{1}{\ln N^{\zeta}}+\frac{2.334}{\ln^2 N^{\zeta}}\right)-\frac{N^{\theta}}{\ln N^{\theta}}\left(1+\frac{1}{\ln N^{\theta}}+\frac{2.334}{\ln^2 N^{\theta}}\right) \\ &< \frac{N^{\zeta}}{\ln N^{\zeta}}\left(1+\frac{1}{\ln N^{\theta}}+\frac{2.334}{\ln^2 N^{\theta}}\right)-\frac{N^{\theta}}{\ln N^{\theta}}\left(1+\frac{1}{\ln N^{\theta}}+\frac{2.334}{\ln^2 N^{\theta}}\right) \\ &= \left(\frac{N^{\zeta}}{\ln N^{\zeta}}-\frac{N^{\theta}}{\ln N^{\theta}}\right)\left(1+\frac{1}{\ln N^{\theta}}+\frac{2.334}{\ln^2 N^{\theta}}\right) \\ &< \left(\frac{N^{\zeta}}{\ln N^{\zeta}}\right)\left(1+\frac{1}{\ln N^{\theta}}+\frac{2.334}{\ln^2 N^{\theta}}\right) \\ &= N^{\zeta}\left(\frac{1}{\ln N^{\zeta}}\right)\left(1+\frac{1}{\ln N^{\theta}}+\frac{2.334}{\ln^2 N^{\theta}}\right) \end{aligned} \tag{22}$$

as $N^{\theta} < N^{\zeta}$. This completes the proof. □

Then, we need to find the upper and lower bounds of a_1 that satisfy the condition posed in Theorem 2.

Proposition 2. *Let $N = pq$ be a CRT-RSA modulus with $p < q < 2p$. Suppose $e = N^{\frac{\alpha}{2}}$ is a valid public exponent with $0 < \alpha \leq 1/4$ and d_p be its corresponding private exponent which satisfies $ed_p = 1 + k_p(p-1)$. Let $ed'_p = 1 + k'_p k_p$ for some $k_p, k'_p, d'_p \in \mathbb{Z}$. Let a fraction α of the MSBs of d_p and p (or q) are known. If a_1 be one of the prime factor of $\left\lfloor \frac{(p-1)}{e} \right\rfloor = a_1^{b_1} \cdot a_2^{b_2} \cdot \ldots \cdot a_n^{b_n} = \prod_{i=1}^{n} a_i^{b_i}$ such that $|(p-1) - \tilde{p}| < ea_1$ then a_1 will be bounded as $N^{\frac{1-3\alpha}{2}} < a_1 < N^{\frac{1-\alpha}{2}}$.*

Proof. We know that $|(p-1) - \tilde{p}| < ea_1$ where $|p - \tilde{p}| < N^{\frac{1}{2}-\alpha}$. Then

$$\begin{aligned} a_1 &> \frac{|(p-1) - \tilde{p}|}{e} \\ &\approx \frac{N^{\frac{1}{2}-\alpha}}{N^{\frac{\alpha}{2}}} \\ &= N^{\frac{1}{2}-\alpha-\frac{\alpha}{2}} = N^{\frac{1-3\alpha}{2}}. \end{aligned}$$

Thus, $N^{\frac{1-3\alpha}{2}}$ is the lower bound for a_1. For the upper bound, we know that $a_1 < \left\lfloor \frac{(p-1)}{e} \right\rfloor$ as a_1 is a factor of $\left\lfloor \frac{(p-1)}{e} \right\rfloor$. Then

$$\begin{aligned} a_1 &< \left\lfloor \frac{(p-1)}{e} \right\rfloor \\ &< \frac{N^{\frac{1}{2}}}{N^{\frac{\alpha}{2}}} \\ &= N^{\frac{1-\alpha}{2}} \end{aligned}$$

Thus, $a_1 < N^{\frac{1-\alpha}{2}}$. This follows the result. □

After we know the upper and lower bounds of a_1, we can estimate the number of primes between the bounds. To achieve that, we use the estimation in Lemma 6. The estimation is as follows in the next proposition.

Proposition 3. *Let $N = pq$ be an CRT-RSA modulus with $p < q < 2p$. Suppose $e = N^{\frac{\alpha}{2}}$ be a valid public exponent with $0 < \alpha \leq 1/4$ and d_p be its corresponding private exponent which satisfies $ed_p = 1 + k_p(p-1)$. Let $ed'_p = 1 + k'_p k_p$ for some $k_p, k'_p, d'_p \in \mathbb{Z}$. Let a fraction α of the MSBs of d_p and p (or q) are known. If a_1 be one of the prime factor of $\left\lfloor \frac{(p-1)}{e} \right\rfloor = a_1^{b_1} \cdot a_2^{b_2} \cdot \ldots \cdot a_n^{b_n} = \prod_{i=1}^{n} a_i^{b_i}$ such that $|(p-1) - \tilde{p}| < ea_1$ then the number of candidates of a_1 that satisfies Theorem 2. will be less than*

$$\frac{N^{\frac{1-\alpha}{2}}\left(\ln^2(N^{\frac{1-3\alpha}{2}}) + \ln(N^{\frac{1-3\alpha}{2}}) + 2.334\right)}{\ln(N^{\frac{1-\alpha}{2}})\ln^2(N^{\frac{1-3\alpha}{2}})}.$$

Proof. We use results from Lemma 6 to count the sum of primes that satisfy Theorem 2. Thus, we changes H_1 and H_2 in Lemma 6 to $N^{\frac{1-\alpha}{2}}$ and $N^{\frac{1-3\alpha}{2}}$ respectively based on the bounds in Proposition 2. Equation (22) will become

$$\begin{aligned}
&\frac{N^{\frac{1-\alpha}{2}}}{\ln N^{\frac{1-\alpha}{2}}}\left(1+\frac{1}{(\frac{1-3\alpha}{2})\ln N}+\frac{2.334}{(\frac{1-3\alpha}{2})^2\ln^2 N}\right)\\
&=\frac{N^{\frac{1-\alpha}{2}}}{\ln(N^{\frac{1-\alpha}{2}})}+\frac{N^{\frac{1-\alpha}{2}}}{\ln(N^{\frac{1-\alpha}{2}})\ln(N^{\frac{1-3\alpha}{2}})}+\frac{N^{\frac{1-\alpha}{2}}(2.334)}{\ln(N^{\frac{1-\alpha}{2}})\ln^2(N^{\frac{1-3\alpha}{2}})}\\
&=\frac{N^{\frac{1-\alpha}{2}}\left(\ln^2(N^{\frac{1-3\alpha}{2}})+\ln(N^{\frac{1-3\alpha}{2}})+2.334\right)}{\ln(N^{\frac{1-\alpha}{2}})\ln^2(N^{\frac{1-3\alpha}{2}})}.
\end{aligned} \tag{23}$$

This completes the proof. □

The following is an example to illustrate the result from Proposition 3.

Example 2. *In this example, we try to illustrate the number of primes that are eligible to be the candidates of a_1.To do that, we set $\alpha = \frac{1}{4}$ to imitate the lowest possible estimation of the number of primes. We also substitute the value of N from Example 1 into (23) which approximates to*

$$2.736665 \times 10^{228} \approx N^{0.3705816}.$$

This is the approximation of the amount of primes that are eligible to be the candidates of a_1.

5. Estimating the Number of Candidates for a_1 with Various Success Appetite

To reduce the number of the candidates of a_1 to be manipulated by an adversary, we define the "success appetite" terminology to best describe our findings.

Definition 2. ***CRT-RSA Success Appetite**, $G(\delta_h)$ is the conditional probability of successfully finding the largest prime factor of $\lfloor \frac{p}{e} \rfloor$, a_1; where a_1 is less than N^{y_1}, given that a_1 is greater than N^{y_2} where $N = pq$ and $y_1 > y_2$ for suitable $y_1, y_2 \in (0,1)$.*

Remark 4. *Success appetite as described in this paper relates to the success probability of the adversary to find the actual value of a_1 from a certain set of primes. The adversary can choose his success appetite, depending on computing resources available to the adversary. The probability of success for the adversary depends on the size of the set of prime candidates where a_1 resides. As such, success appetite and probability of success are two different concepts.*

Since further experiment and analysis must be completed to be corroborated with the independent nature of Dickman's function and randomized values of $\left\lfloor \frac{p_i}{e_i} \right\rfloor$, we put forward the next conjecture that defines CRT-RSA success appetite quantitatively.

Conjecture 1. *Given i different RSA moduli, $N_i = p_i q_i$ that are randomly generated in RSA key generation algorithm, then the largest number of RSA moduli of which the greatest prime factor of $\left\lfloor \frac{p_i}{e_i} \right\rfloor$ is between its intended success-dependent upper and lower bound is $G(\delta_h) \cdot i$.*

By having the CRT-RSA success appetite, an adversary can evaluate it using the next corollary.

Proposition 4. *Let $N = pq$ be an RSA modulus. Let $e = N^{\frac{\alpha}{2}}$ be an RSA public exponent and d be an RSA private exponent where $0 < \alpha \leq 1/4$. Let a_1 be one of the prime factors of $\lfloor \frac{p}{e} \rfloor = a_1^{b_1} \cdot a_2^{b_2} \cdot \ldots \cdot a_n^{b_n} = \prod_{i=1}^{n} a_i^{b_i}$. Suppose B is a known integer larger than $\rho\phi(N)$ and $B - \rho\phi(N) < ea_1$. Let $F_X(y)$ be the Dickman's function. If δ_h is the CRT-RSA success appetite, then the number of candidates of a_1 that satisfies Theorem 2 will be less than*

$$\frac{N^{\frac{1-\alpha}{2}} \left(\ln^2(N^{\frac{1-3\alpha}{2}}) + \ln(N^{\frac{1-3\alpha}{2}}) + 2.334 \right)}{\ln(N^{\frac{1-\alpha}{2}}) \ln^2(N^{\frac{1-3\alpha}{2}})}.$$

where $y_1 = F^{-1}\left(\delta_h \cdot F_X(\overline{\frac{1-3\alpha}{2}}) + F_X(\frac{1-3\alpha}{2}) \right)$.

Proof. Let $F_X(y)$ or $F(y)$ be the probability function for a random integer between 1 and X to have the greatest prime factor less than X^y as defined in Definition 1 (Dickman's function). Let X^{y_1} be the upper bound of a_1 and X^{y_2} to be the lower bound of a_1, then (23) can also be written as

$$\frac{N^{y_1} \left(\ln^2(N^{y_2}) + \ln(N^{y_2}) + 2.334 \right)}{\ln(N^{y_1}) \ln^2(N^{y_2})} \tag{24}$$

Next, we define

(a) $F(y_1)$ to be the probability of X having its greatest prime factor less than X^{y_1};
(b) $F(y_2)$ to be the probability of X having its greatest prime factor less than X^{y_2}; and
(c) $F(\overline{y_2})$ to be the probability of X not having its greatest prime factor less than X^{y_2}.

Let δ_h be the success appetite as defined in Definition 2, we can rewrite δ_h as the probability of $\left\lfloor \frac{p-1}{e} \right\rfloor$ having its largest prime factor less than N^{y_1}, given that it has no largest prime factor less than N^{y_2}. Using the definition of conditional probability, observe that

$$\begin{aligned} \delta_h = F(y_1 \mid \overline{y_2}) &= \frac{F(y_1 \cap \overline{y_2})}{F(\overline{y_2})} \\ &= \frac{F(y_1) - F(y_2)}{F(\overline{y_2})}. \end{aligned} \tag{25}$$

From (25),

$$\begin{aligned} F(y_1) - F(y_2) &= \delta_h \cdot F(\overline{y_2}) \\ F(y_1) &= \delta_h \cdot F(\overline{y_2}) + F(y_2) \\ y_1 &= F^{-1}\left(\delta_h \cdot F(\overline{y_2}) + F(y_2) \right). \end{aligned}$$

According to Proposition 2, $y_2 = \frac{1-3\alpha}{2}$. Substitute values of y_1 and y_2 into (24), we obtain

$$\frac{N^{y_1} \left(\ln^2(N^{\frac{1-3\alpha}{2}}) + \ln(N^{\frac{1-3\alpha}{2}}) + 2.334 \right)}{\ln(N^{y_1}) \ln^2(N^{\frac{1-3\alpha}{2}})}. \tag{26}$$

where $y_1 = F^{-1}\left(\delta_h \cdot F(\overline{\frac{1-3\alpha}{2}}) + F(\frac{1-3\alpha}{2}) \right)$ □

Proposition 4 shows that an adversary can adjust the upper bound of a_1 according to the success appetite preferred by the adversary. In the next section, we can see how this adjustment can reduce the number of primes eligible to be the significant candidates of a_1.

6. Comparative Analysis

In this section, we show two comparisons. In the first comparison, we compare the changes of the number of candidates of a_1, $\pi(a_1)$ in terms of β (where $\pi(a_1) = N^{\beta}$) when the success appetite, δ_h changes. We also set $\alpha = 0.05, 0.1, 0.15, 0.2$ and 0.25 to see the changes in $\pi(a_1)$. The full details of the values are shown in Table 2.

Table 2. Comparison in Number of Candidates of a_1 In Terms of Logarithm to Base N with Respect to δ_h and α.

Intended Success Probability, δ_h	**β, $\pi(a_1) = N^{\beta}$**				
	$\alpha = 0.05$	**$\alpha = 0.1$**	**$\alpha = 0.15$**	**$\alpha = 0.2$**	**$\alpha = 0.25$**
0.01	0.4208	0.3464	0.2719	0.1973	0.1250
0.25	0.4324	0.3682	0.3023	0.2337	0.1796
0.50	0.4448	0.3925	0.3375	0.2785	0.2289
0.75	0.4575	0.4182	0.3768	0.3318	0.2913
1.00	0.4706	0.4457	0.4205	0.3952	0.3704

Based on Table 2, when δ_h progressively reduces from 1 to 0.01, for $\alpha = 0.05$, the number of candidates also slowly reduces from $N^{0.4706}$ to $N^{0.4208}$, $N^{0.4457}$ to $N^{0.3464}$ for $\alpha = 0.1$, $N^{0.4205}$ to $N^{0.2719}$ for $\alpha = 0.15$, $N^{0.3952}$ to $N^{0.1973}$ for $\alpha = 0.2$ and $N^{0.3704}$ to $N^{0.125}$ for $\alpha = 0.25$. In general, the number of candidates decreases as the values of the success appetites decrease. A similar pattern occurs when the values of α increases. This means that the best situation for an adversary to conduct an attack against CRT-RSA using our method is when 0.25 MSBs of d and p (or q) are known with a consideration of a success appetite that is as small as possible.

In the second comparison, we intend to compare our attack with results from [12–16]. All of these results require some bits of d_p to be known beforehand. In [15], Takayatsu et al. provided a result which includes bits of d_q. A comparison with our results is shown in Table 3.

Based on Table 3, Ref. [16] requires at least 0.27 random bits of all p, q, d, d_p, d_q. The attack also used random reconstruction algorithm. On another hand, attack by [12] requires an approximation of d_p called $\tilde{d}_p$ to be given, such that $|d_p - \tilde{d}_p| < N^{\frac{1}{4}-\alpha}$ where $e = N^{\alpha}$. The suitable size of e used in the attack is $1 < e < N^{1/4}$. The methodology used in [12] can also be applied in many conditions, since we can see that the extension of the results in [13–15] are also using the similar lattice-based approach.

Meanwhile, our attack requires an approximation of d_p and p called $\tilde{d}_p$ and $\tilde{p}$ to be given, such that $|d_p - \tilde{d}_p|, |p - \tilde{p}| < N^{\frac{1-\alpha}{2}}$. As $0 < \alpha \leq 1/4$, this means that the suitable range for e in our case is $0 < e < N^{1/8}$. based on Table 3, Ref. [12] needs the approximation of d_p to be between 0 and $< N^{1/4}$ from the actual d_p. Meanwhile, in our case, we need the approximation of d_p and p to be between $N^{3/8}$ and $N^{1/2}$ from the actual values of d_p and p. This means that our attack is less stringent and requires less MSBs of private keys to be known than [12] (although our attack needs two approximations of private keys). In addition, our method takes a different approach compared to other results, since we detach our method from the common approach of partial key attack on CRT-RSA by using the lattice-based method to finding the largest prime factor of $\left\lfloor \frac{p-1}{e} \right\rfloor$ with versatile success appetites.

Table 3. Comparison of Our Method Against Existing Methods to Conduct Partial-Key Exposure Attack Against CRT-RSA.

Attacks	**Exposed Information about Private Keys for the Attack to be Successful**	**Methodology**
Heninger and Shacham (2009)	Given 0.27 of the bits of p, q, d, d_p, d_q	Using random reconstruction algorithm
Blömer and May (2003)	Given $\tilde{d_p}, e = N^{\alpha}$ such that $\lvert d_p - \tilde{d_p} \rvert < N^{\frac{1}{4}-\alpha}$ where $0 < \alpha \leq 1/4$	Using lattice-based method
Lu et al. (2014)	Given $\tilde{d_p} \approx N^{\gamma}, e \approx N^{\alpha}$ where $\lvert d_p - \tilde{d_p} \rvert < N^{\gamma_1}$ such that γ, γ_1, α satisfy conditions in Theorem 6 of [13]	
Sarkar and Venkateswarlu (2014)	Given $e \approx N^{\alpha}$ and bits of d_p except for n many blocks with sizes $\gamma_i \log N$ bits for $1 \leq i \leq n$, such that γ, γ_1, α satisfy inequality in Theorem 1 of [14]	
Takayatsu and Kunihiro (2015)	Given $\tilde{d_p} \approx N^{\gamma}, e \approx N^{\alpha}$ where $d_p \approx N^{\gamma_1}$ such that α, γ, γ_1 satisfy conditions in Theorem 6 of [15]	
Our method	Given $\tilde{d_p}, \tilde{p}, e = N^{\alpha/2}$ where $0 < \alpha \leq 1/4$ such that $\lvert d_p - \tilde{d_p} \rvert, \lvert p - \tilde{p} \rvert < N^{\frac{1-\alpha}{2}}$	Need to determine the largest prime factor of $\left\lfloor \frac{p-1}{e} \right\rfloor$

7. Conclusions

We have successfully factored the modulus of CRT-RSA in polynomial time using our new method under specific conditions. Given $e = N^{\frac{\alpha}{2}}$, where $0 < \alpha \leq 1/4$, the method requires an approximation of private exponent called $\tilde{d_p}$ and approximation of p called $\tilde{p}$ to be known, such that $|d_p - \tilde{d_p}|, |p - \tilde{p}| < N^{\frac{1-\alpha}{2}}$. Our attack also requires the largest prime factor of $\left\lfloor \frac{p-1}{e} \right\rfloor$. By utilizing Dickman's theorem, we showed a practical approach to identify the prime from a set of primes that the factor most likely resides in. The approach manipulates a versatile self-defined value known as the success appetite value that can be referred to by the adversary based on the computational power at hand. This makes our attack less stringent and requires fewer MSBs of private keys to be known than existing attacks. For a future extension of this work, one may develop a new method to find a_1 from a smaller set of primes. The method should include a marked up algorithm that identifies a_1, where its respective success appetite is compared with the number of candidates of a_1 in terms of the logarithm to base N, as shown in Table 2. Another interesting future approach to tackle the problem of finding a_1 is by using synchronized machine learning with the aid of cloud systems for its storage space, as shown in [23].

Author Contributions: Conceptualization, A.H.A.G. and M.R.K.A.; methodology, formal analysis, investigation, writing—original draft preparation, A.H.A.G.; writing—review and editing, A.H.A.G., M.R.K.A., S.M.Y. and S.H.S.; supervision and funding acquisition, M.R.K.A. All authors have read and agreed to the published version of the manuscript.

Funding: The research was supported by Ministry of Higher Education of Malaysia with Fundamental Research Grant Scheme (FRGS/1/2019/STG06/UPM/02/8).

Acknowledgments: The research was supported by Ministry of Higher Education of Malaysia with Fundamental Research Grant Scheme (FRGS/1/2019/STG06/UPM/02/8).

Conflicts of Interest: The authors declare no conflict of interest.

Abbreviations

The following abbreviations are used in this manuscript:

LSB	Least significant bits
MSB	Most significant bits
RSA	Rivest–Shamir–Adleman

References

1. Rivest, R.L.; Shamir, A.; Adleman, L. A method for obtaining digital signatures and public-key cryptosystems. *Commun. ACM* **1978**, *21*, 120–126. [CrossRef]
2. Buhler, J.P.; Lenstra, H.W.; Pomerance, C. Factoring integers with the number field sieve. In *The Development of the Number Field Sieve*; Springer: Berlin/Heidelberg, Germany, 1993; pp. 50–94.
3. Rivest, R.L.; Shamir, A.; Adleman, L.M. Cryptographic Communications System and Method. U.S. Patent 4,405,829, 20 September 1983.
4. Hinek, M.J. *Cryptanalysis of RSA and Its Variants*; CRC Press: Boca Raton, FL, USA, 2009.
5. Kocher, P.; Jaffe, J.; Jun, B.; Rohatgi, P. Introduction to differential power analysis. *J. Cryptogr. Eng.* **2011**, *1*, 5–27. [CrossRef]
6. Rivest, R.L.; Shamir, A. Efficient factoring based on partial information. In *Workshop on the Theory and Application of of Cryptographic Techniques*; Springer: Berlin/Heidelberg, Germany, 1985; pp. 31–34.
7. Coppersmith, D. Finding a small root of a bivariate integer equation; factoring with high bits known. In *International Conference on the Theory and Applications of Cryptographic Techniques*; Springer: Berlin/Heidelberg, Germany, 1996; pp. 178–189.
8. Boneh, D.; Durfee, G.; Frankel, Y. Exposing an RSA private key given a small fraction of its bits. *Full Version Work. Asiacrypt* **1998**, *98*, 25-34.
9. Ernst, M.; Jochemsz, E.; May, A.; De Weger, B. Partial key exposure attacks on RSA up to full size exponents. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*; Springer: Berlin/Heidelberg, Germany, 2005; pp. 371–386.
10. Sarkar, S.; Maitra, S.; Sarkar, S. RSA Cryptanalysis with Increased Bounds on the Secret Exponent using Less Lattice Dimension. *IACR Cryptol. ePrint Arch.* **2008**, *2008*, 315.
11. Abd Ghafar, A.H.; Ariffin, M.R.K.; Johari, M.A.M.; Asbullah, M.A. A Survey of Partial Key Exposure Attacks on RSA Cryptosystem. *Embrac. Math. Divers.* **2019**, *1*, 24.
12. Blömer, J.; May, A. New partial key exposure attacks on RSA. In *Annual International Cryptology Conference*; Springer: Berlin/Heidelberg, Germany, 2003; pp. 27–43.
13. Lu, Y.; Zhang, R.; Lin, D. New partial key exposure attacks on CRT-RSA with large public exponents. In *International Conference on Applied Cryptography and Network Security*; Springer: Cham, Switzerland, 2014; pp. 151–162.
14. Sarkar, S.; Venkateswarlu, A. Partial key exposure attack on CRT-RSA. In *International Conference on Cryptology in India*; Springer: Berlin/Heidelberg, Germany, 2014; pp. 255–264.
15. Takayasu, A.; Kunihiro, N. Partial key exposure attacks on CRT-RSA: Better cryptanalysis to full size encryption exponents. In *International Conference on Applied Cryptography and Network Security*; Springer: Cham, Switzerland, 2015; pp. 518–537.
16. Heninger, N.; Shacham, H. Reconstructing RSA private keys from random key bits. In *Advances in Cryptology-CRYPTO 2009*; Springer: Berlin/Heidelberg, Germany, 2009; pp. 1–17.
17. Halderman, J.A.; Schoen, S.D.; Heninger, N.; Clarkson, W.; Paul, W.; Calandrino, J.A.; Feldman, A.J.; Appelbaum, J.; Felten, E.W. Lest we remember: Cold-boot attacks on encryption keys. *Commun. ACM* **2009**, *52*, 91–98. [CrossRef]

18. Takayasu, A.; Kunihiro, N. Partial key exposure attacks on CRT-RSA: General improvement for the exposed least significant bits. In *International Conference on Information Security*; Springer: Berlin/Heidelberg, Germany, 2016; pp. 35–47.
19. Ireland, K.; Rosen, M. *A Classical Introduction to Modern Number Theory*; Springer Science & Business Media: Berlin/Heidelberg, Germany, 2013; Volume 84.
20. Dusart, P. Estimates of some functions over primes without RH. *arXiv* **2010**, arXiv:1002.0442.
21. Dickman, K. On the frequency of numbers containing prime factors of a certain relative magnitude. *ARkiv Mat. Astron. Och Fys.* **1930**, *22*, 1–14.
22. Donald, E.K. *The Art of Computer Programming, Vol. 2: Seminumerical Algorithms*; Addison-Wesley: Boston, MA, USA, 1981.
23. Çatak, F.Ö.; Mustacoglu, A.F. CPP-ELM: Cryptographically privacy-preserving extreme learning machine for cloud systems. *Int. J. Comput. Intell. Syst.* **2018**, *11*, 33–44. [CrossRef]

Publisher's Note: MDPI stays neutral with regard to jurisdictional claims in published maps and institutional affiliations.