On Newly Partial Key Exposure Attack Using Near-square RSA Primes

Wan Nur Aqlili Ruzai, *Member, IAENG,* Amir Hamzah Abd Ghafar*, Muhammad Rezal Kamel Ariffin, and Muhammad Asyraf Asbullah

***Abstract*—Asymmetric key cryptography is crucial for securing digital communications by encrypting data and ensuring information integrity. The Rivest-Shamir-Adleman (RSA) cryptosystem is widely used, with its security primarily relying on the complexity of the integer factorization problem, particularly the modulus $N = pq$. Adversaries attempting to factor the prime factors p and q have made specific assumptions, such as targeting scenarios where p and q exhibit vulnerabilities like those in Pollard's weak prime structures or when partial knowledge about the least significant bits (LSBs) of these primes is available. These weaknesses allow adversaries to efficiently factor the modulus N in polynomial time, compromising RSA encryption security. This paper broadens the understanding of such vulnerabilities by introducing three additional forms of near-square primes. These new forms express N as $p \times q$ in the following ways: $(a^m - r_a)(b^m - r_b)$ and $(a^m \pm r_a)(b^m \mp r_b)$, where a and b are positive integers, and m is a positive even number. It is assumed that r_a and r_b, corresponding to the LSBs of p and q, are known to the attacker. This study demonstrates the efficient factorization of N under these assumptions and quantifies the impact of this attack on the number of primes. These findings highlight a significant risk to RSA users and emphasize the need for countermeasures to mitigate this attack's potential impact.**

***Index Terms*—asymmetric key cryptography, partial key exposure attack, RSA cryptanalysis, RSA primes.**

I. Introduction

INFORMATION Technology serves as the cornerstone of contemporary society, permeating nearly every facet of daily life. The rapid expansion of today's technological landscape generates an ever-increasing volume of data. As this digital universe continues to expand, the imperative to safeguard and preserve data privacy intensifies, a concern shared by both individuals and organizations alike. Security has long been a paramount issue within the realm of computing, particularly concerning the secure transmission of information and data across the Internet. Across various channels, whether via the Internet or through smart devices, reports of data thefts and breaches have shown a consistent upward trend [1]. In response to these challenges, researchers and cryptographers tirelessly endeavor to innovate novel cryptographic models and enhance existing cryptographic algorithms. These advancements are geared towards practical implementation in real-world applications, with the ultimate aim of enhancing user privacy, fortifying data security, strengthening authentication mechanisms, and addressing a multitude of related features [2].

In the field of cryptographic algorithms, the RSA public key cryptographic algorithm is notable for being one of the earliest and most widely used asymmetric cryptosystem [3]. Asymmetric cryptography is typically employed when advanced security is prioritized over speed. It is commonly used in digital signatures, blockchain technology, and public key infrastructure (PKI) [4]. The contemporary applications of the traditional RSA algorithm encompass activities such as key exchanges [5], digital signatures [6], the functioning of web browsers, chat applications, email services, VPNs, and other communication methods that require the secure transmission of data between two parties [7].

The security of RSA relies on the significant difficulty of factoring the product of two large prime numbers, known as the integer factorization problem (IFP). Before continuing into further details, it is crucial to understand the parameters of the RSA cryptosystem. One key parameter is the RSA modulus, denoted by N, which is obtained by multiplying two large, randomly selected prime numbers, p and q. Additionally, we compute $\phi(N)$, the product of $(p-1)$ and $(q-1)$, representing Euler's totient function for N. To enhance security and prevent factorization through trial division, we carefully select p and q such that $q < p < 2q$. Once $\phi(N)$ is determined, we choose a random integer e, ensuring that e is less than $\phi(N)$ and coprime to it. We then compute the private key component d, which satisfies the congruence equation $ed \equiv 1 (\mathrm{mod} \phi(N))$. As the outputs of RSA key generation, N and e form the public key, while d and $\phi(N)$ are kept as the private key.

Earlier attempts to compromise RSA security, particularly Pollard's work in 1974 [8], identified vulnerabilities in certain prime structures that can be factored within polynomial time—a task that modern computers can accomplish with ease. Previous research has shown that primes with specific traits, such as small factors in $p-1$ and $q-1$, render the product $p \cdot q$ vulnerable to polynomial-time factorization, especially using Pollard's $p-1$ algorithm [8]. This algorithm is highly efficient when the prime factors of both $p-1$ and $q-1$ are small.

Another strategy to exploit RSA involves the assumption that an attacker has partial knowledge of p and q. This knowledge diminishes the difficulty of factoring N. Boneh et al. [9] demonstrated that knowing the least significant bits

Manuscript received February 21, 2024; revised November 12, 2024.

This work was supported by Universiti Putra Malaysia under Putra Initiative Grant with Vot No. 9779100.

W.N.A. Ruzai is a university lecturer at the School of Distance Education, Universiti Sains Malaysia, 11800 USM, Penang, Malaysia. (email: aqliliruzai@usm.my)

A.H.A. Ghafar is a senior lecturer at the Department of Mathematics and Statistics, Faculty of Science, Universiti Putra Malaysia, 43400 UPM Serdang, Selangor, Malaysia. (Corresponding author e-mail: amir_hamzah@upm.edu.my).

M.R.K. Ariffin is a professor at the Department of Mathematics and Statistics, Faculty of Science, Universiti Putra Malaysia, 43400 UPM Serdang, Selangor, Malaysia. (e-mail: rezal@upm.edu.my).

M.A. Asbullah is a senior lecturer at the Centre for Foundation Studies in Science, Universiti Putra Malaysia, 43400 Serdang, Selangor, Malaysia. (email: ma_asyraf@upm.edu.my)

(LSBs) of the RSA primes, particularly the lower half, is sufficient for polynomial-time factorization of N. Heninger and Shacham's random reconstruction algorithm further underscores this efficiency, especially when approximately 57% of the random bits for p and q are known [10]. Maitra et al. [11] subsequently introduced a combinatorial model inspired by Heninger's approach, successfully reconstructing the LSBs of RSA primes through a refined brute-force attack.

In a different case, Abd Ghafar et al. [12] introduced a specific attack strategy targeting the RSA modulus N. This strategy is applied to instances where N is the product of two prime numbers, p and q, with p structured as $p = a^m + r_p$ and q as $q = b^m + r_q$. In this context, r_p and r_q are the least significant bits (LSBs) of the primes p and q. Their method can operate efficiently within polynomial time, assuming the LSBs of these prime numbers are known and fulfill certain conditions. It is important to note that these LSBs, often targeted in RSA attacks, are typically obtained through side-channel attacks. Such methods remain a key approach for extracting information during computation [13]. Side-channel attacks exploit various characteristics, including computational time and power consumption during decryption [14], [15], heat emissions, electromagnetic radiation from devices [16], cache behaviour [17], and even acoustic emissions produced by the processor during computations [18].

A. Contribution of This Paper

The authors of [19] have effectively demonstrated the vulnerabilities associated with using near-square primes in generating the RSA modulus $N = pq$. However, near-square primes can inadvertently be used during the random prime generation process for p and q. Note that this type of N structure might unknowingly be widespread in real-world applications today, as no existing cryptographic implementation prevents its generation. Our research has shown that the use of such primes can critically compromise RSA security. Specifically, we present three scenarios where near-square primes serve as factors in RSA. These scenarios are configured as follows:

1) Case I: $p = a^m - r_a$ and $q = b^m - r_b$;
2) Case II: $p = a^m + r_a$ and $q = b^m - r_b$; and
3) Case III: $p = a^m - r_a$ and $q = b^m + r_b$

In this study, we assume that an adversary has knowledge of certain LSBs of RSA primes with near-square primes structured. More precisely, if the attacker gains access to the bits corresponding to r_a and r_b of RSA primes p and q, then we can efficiently factor N without the need to reconstruct the remaining bits of the primes. Our results indicate that our attack can efficiently factor N within a polynomial time frame, needing only a limited number of LSBs, under the condition that RSA primes conform to these specific structures. Additionally, we highlight the common occurrence of primes that fit these structural criteria and the absence of sufficient protections in standard RSA libraries to avoid using such primes. This underscores the inherent weaknesses in the existing RSA key generation process, which could lead to RSA modulus that are susceptible to our attack.

B. Organization of the Paper

The following sections of this paper are structured as follows. Section II provides a crucial background overview, detailing previous research that inspired and guided our study. In Section III, we present the core of our work, including the proof of our main attacks and numerical examples to illustrate our findings. Next, Section IV quantifies the number of vulnerable prime numbers affected by our attacks. This is followed by a comparison of our results with existing attacks that utilize known bits of primes in Section V. Finally, Section VI concludes the paper by summarizing the key takeaways and our conclusions.

II. Background Overview

In this section, we revisit several lemmas and definitions that are pivotal for the success of our attack. To begin, we must establish the equivalence between $(a^m - r)^{\frac{1}{2}}$ in its integer and decimal forms, as detailed in Lemma 1.

Lemma 1. Let a and r be positive integers, and consider a power of 2, denoted as $m \geq 2$. If $(a^m - r)^{\frac{1}{2}}$ is expressed as $a^{\frac{m}{2}} - \epsilon$, then it follows that ϵ is bounded by $\epsilon < \frac{r}{2}a^{-\frac{m}{2}}$.

Proof: Let us consider the assumption that $(a^m - r)^{\frac{1}{2}} \in \mathbb{Z}$, where $a \in \mathbb{Z}^+$. We can then establish the following inequality:

$$\begin{aligned}(a^m - r)^{\frac{1}{2}} &< \left(a^m + \frac{r^2}{4a^m} - r\right)^{\frac{1}{2}} \\ &= \left(\left(a^{\frac{m}{2}} - \frac{r}{2}a^{-\frac{m}{2}}\right)^2\right)^{\frac{1}{2}} \\ &= a^{\frac{m}{2}} - \frac{r}{2}a^{-\frac{m}{2}}.\end{aligned}$$

Given our assumption that $(a^m - r)^{\frac{1}{2}} = a^{\frac{m}{2}} - \epsilon$, it follows that $\epsilon < \frac{r}{2}a^{-\frac{m}{2}}$. ■

Expanding upon the conditions outlined in Lemma 1, we further define the upper limit and lower limit of $(ab)^{\frac{m}{2}} - N^{\frac{1}{2}}$ in the subsequent Lemma 2.

Lemma 2. Consider positive integers a, b, r_a, and r_b and let $m \geq 2$. Suppose $a < b < (2a^m + 1)^{\frac{1}{m}}$, and define $N = (a^m - r_a)(b^m - r_b)$, where the maximum of r_a and r_b is denoted as N^γ. We also impose the conditions that $r_a < 2a^{\frac{m}{2}}$ and $r_b < 2b^{\frac{m}{2}}$. Under these conditions, we establish the following inequalities:

$$(r_a r_b)^{\frac{1}{2}} < (ab)^{\frac{m}{2}} - N^{\frac{1}{2}} < 2^{\frac{m}{2}-1}r_a + \frac{r_b}{2} - 1.$$

Proof: In order to establish the lower limit of $(ab)^{\frac{m}{2}} - N^{\frac{1}{2}}$, our objective is to demonstrate the following inequality:

$$a^m r_b + b^m r_a > 2(ab)^{\frac{m}{2}}(r_a r_b)^{\frac{1}{2}},$$

which implies

$$-(a^m r_b + b^m r_a) < -2(ab)^{\frac{m}{2}}(r_a r_b)^{\frac{1}{2}}.$$

We can observe that:

$$\left(a^{\frac{m}{2}} r_b^{\frac{1}{2}} - b^{\frac{m}{2}} r_a^{\frac{1}{2}}\right)^2 = a^m r_b + b^m r_a - 2(ab)^{\frac{m}{2}}(r_a r_b)^{\frac{1}{2}}.$$

Since $\left(a^{\frac{m}{2}} r_b^{\frac{1}{2}} - b^{\frac{m}{2}} r_a^{\frac{1}{2}}\right)^2$ is always positive, it follows that:

$$a^m r_b + b^m r_a > 2(ab)^{\frac{m}{2}}(r_a r_b)^{\frac{1}{2}}.$$

Now, we proceed as follows:

$$\begin{aligned}((a^m - r_a)(b^m - r_b))^{\frac{1}{2}} &= ((ab)^m + r_a r_b - (a^m r_b + b^m r_a))^{\frac{1}{2}} \\ &< \left((ab)^m + r_a r_b - 2(ab)^{\frac{m}{2}}(r_a r_b)^{\frac{1}{2}}\right)^{\frac{1}{2}} \\ &= \left([(ab)^{\frac{m}{2}} - (r_a r_b)^{\frac{1}{2}}]^2\right)^{\frac{1}{2}} \\ &= (ab)^{\frac{m}{2}} - (r_a r_b)^{\frac{1}{2}}. \end{aligned} \quad (1)$$

Consequently, we have shown that from (1), we can write

$$[(a^m - r_a)(b^m - r_b)]^{\frac{1}{2}} - (ab)^{\frac{m}{2}} = N^{\frac{1}{2}} - (ab)^{\frac{m}{2}} < -(r_a r_b)^{\frac{1}{2}},$$

which can also be expressed as $(ab)^{\frac{m}{2}} - N^{\frac{1}{2}} > (r_a r_b)^{\frac{1}{2}}$.

Now, we shift our focus to establish the upper limit. It is worth noting that $(a^m - r_a)^{\frac{1}{2}} = a^{\frac{m}{2}} - \epsilon_1$ and $(b^m - r_b)^{\frac{1}{2}} = b^{\frac{m}{2}} - \epsilon_2$. Utilizing Lemma 1, we can deduce the following:

$$\begin{aligned} N^{\frac{1}{2}} &= [(a^m - r_a)(b^m - r_b)]^{\frac{1}{2}} \\ &= (a^m - r_a)^{\frac{1}{2}}(b^m - r_b)^{\frac{1}{2}} \\ &= (a^{\frac{m}{2}} - \epsilon_1)(b^{\frac{m}{2}} - \epsilon_2) \\ &= (ab)^{\frac{m}{2}} - a^{\frac{m}{2}}\epsilon_2 - b^{\frac{m}{2}}\epsilon_1 + \epsilon_1\epsilon_2 \\ &> (ab)^{\frac{m}{2}} - \left(a^{\frac{m}{2}}\frac{r_b}{2b^{\frac{m}{2}}} + b^{\frac{m}{2}}\frac{r_a}{2a^{\frac{m}{2}}}\right) + \frac{r_a}{2a^{\frac{m}{2}}}\frac{r_b}{2b^{\frac{m}{2}}}. \end{aligned} \quad (2)$$

If $r_a < 2a^{\frac{m}{2}}$ and $r_b < 2b^{\frac{m}{2}}$, we have:

$$\frac{r_a}{2a^{\frac{m}{2}}} \cdot \frac{r_b}{2b^{\frac{m}{2}}} = \frac{r_a r_b}{4(ab)^{\frac{m}{2}}} < \frac{4(ab)^{\frac{m}{2}}}{4(ab)^{\frac{m}{2}}} = 1. \quad (3)$$

For $a < b < (2a^m + 1)^{\frac{1}{m}}$, we can rewrite (2) as:

$$\begin{aligned} N^{1/2} - (ab)^{\frac{m}{2}} &> -\left(a^{\frac{m}{2}}\frac{r_b}{2b^{\frac{m}{2}}} + b^{\frac{m}{2}}\frac{r_a}{2a^{\frac{m}{2}}}\right) + 1 \\ &= -\left(\left(\frac{a}{b}\right)^{\frac{m}{2}}\frac{r_b}{2} + \left(\frac{b}{a}\right)^{\frac{m}{2}}\frac{r_a}{2}\right) + 1 \\ &> -\left((1)^{\frac{m}{2}}\frac{r_b}{2} + (2)^{\frac{m}{2}}\frac{r_a}{2}\right) + 1 \\ &= -\frac{r_b}{2} - 2^{\frac{m}{2}-1}r_a + 1. \end{aligned}$$

This can be rewritten as $(ab)^{\frac{m}{2}} - N^{\frac{1}{2}} < 2^{\frac{m}{2}-1}r_a + \frac{r_b}{2} - 1$.

In conclusion, the bounds can be expressed as $(r_a r_b)^{\frac{1}{2}} < (ab)^{\frac{m}{2}} - N^{\frac{1}{2}} < 2^{\frac{m}{2}-1}r_a + \frac{r_b}{2} - 1$. This concludes the proof. ■

Furthermore, we introduce a revised version of Lemma 3 to support the subsequent attack. This lemma will not only be applied in the second LSB attack but will also play a crucial role in LSB Attack Case III.

Lemma 3. Let a and b be positive integers, along with r_a and r_b. Consider a power of 2, denoted as $m \geq 2$, with the condition that a is less than b and both are less than $(2a^m + 1)^{\frac{1}{m}}$. If r_a is significantly smaller than $2a^{\frac{m}{2}}$ and r_b is considerably less than $2b^{\frac{m}{2}}$, we establish that:

$$a^m r_b + 2(ab)^{\frac{m}{2}}(r_a r_b)^{\frac{1}{2}} > b^m r_a.$$

Proof: Kindly refer to the proof of Lemma 5 in [19]. ■

Building upon the findings of Lemma 3, we further define the upper limit and lower limit of $N^{\frac{1}{2}} - (ab)^{\frac{m}{2}}$ in cases where the prime factors are represented as $p = a^m + r_a$ and $q = b^m - r_b$, as elucidated in Lemma 4.

Lemma 4. Consider positive integers a, b, r_a, r_b, and let $m \geq 2$, subject to the condition that a and b satisfy $a < b < (2a^m + r_a)^{\frac{1}{m}}$. Define N as $N = (a^m + r_a)(b^m - r_b)$. Given the additional assumptions that r_a is significantly smaller than $2a^{\frac{m}{2}}$ and r_b is considerably less than $2b^{\frac{m}{2}}$, we can establish the following limits:

$$\frac{1}{2}(r_a - r_b) - 1 < N^{\frac{1}{2}} - (ab)^{\frac{m}{2}} < (r_a r_b)^{\frac{1}{2}}.$$

Proof: Kindly refer to the proof of Lemma 6 in [19]. ■

Conversely, expanding upon the results derived from Lemma 3, we now turn our attention to establishing the lower limit and upper limit of $N^{\frac{1}{2}} - (ab)^{\frac{m}{2}}$ when the primes of modulus N are expressed as $p = a^m - r_a$ and $q = b^m + r_b$, as outlined below.

Lemma 5. Consider positive integers a, b, r_a, and r_b where m is a power of 2 with $m \geq 2$. It is essential that these integers adhere to the condition $a < b < (2a^m - r_a)^{\frac{1}{m}}$. We define N as $N = (a^m - r_a)(b^m + r_b)$. Provided that r_a is significantly smaller than $2a^{\frac{m}{2}}$ and r_b is notably less than $2b^{\frac{m}{2}}$, we can establish the following limits:

$$-(1 + \sqrt{2})(r_a r_b)^{\frac{1}{2}} < N^{\frac{1}{2}} - (ab)^{\frac{m}{2}} < \frac{(r_b - r_a)}{2}.$$

Proof: Kindly refer to the proof of Lemma 7 in [19]. ■

Before proceeding on the new attacks, we revisit and clarify key definitions, specifically the terms "near-square primes" and "sufficiently small." These definitions were initially introduced in the earlier works by Abd Ghafar et al. [12] and Ruzai et al. [19], and they play a pivotal role in justifying our cryptanalytic approaches. In the context of this research, the term "near-square prime" is coined to characterize a specific type of prime number.

Definition 1. A prime p qualifies as a near-square prime if it adheres to the following criteria:

- p can be expressed as $p = a^m \pm r_a$.
- In this context, a represents any integer, while m stands as a power of 2.
- Crucially, r_a is a finite integer, and for the purpose of practical consideration, it typically falls below a threshold, such as $r_a < 100$.

It's worth noting that while the notion of near-square primes was previously addressed from a theoretical perspective in the context of sieve approaches [20], this research underscores its relevance and implications within cryptographic settings. Prior works [21], [12], [22] and [19] from our team have unveiled the vulnerabilities posed by such primes in the RSA cryptosystem. This particular definition is integral to all of the attack strategies detailed in this work and serves as the foundation for our cryptanalytic approach to near-square primes used in the RSA cryptosystem.

Definition 2. Consider an integer a and a power of 2 denoted as m. If a prime number p can be expressed as $p = a^m \pm r_a$, where r_a is an integer deemed 'sufficiently small,' we classify such a prime p as an r_a-near square prime.

In real-world situations, the expression "sufficiently small," as defined in Definition 2, refers to integer sizes that are practical for exhaustive searching within a foreseeable time frame. To determine precise criteria for what qualifies as "sufficiently small" in modern cryptographic contexts, we suggest consulting the most up-to-date key size guidelines provided by NIST (the National Institute of Standards and Technology) [23].

III. New LSB Attacks Using Near-Square RSA Primes

By establishing the lower and upper limits of $(ab)^{\frac{m}{2}} - N^{\frac{1}{2}}$ as described in Lemma 2, and the bounds of $N^{\frac{1}{2}} - (ab)^{\frac{m}{2}}$ as detailed in Lemma 4 and Lemma 5, we have obtained significant results that will be employed in our subsequent attacks. This study focuses on the RSA near-square primes p and q represented in the following cases:

1) Case I: $p = a^m - r_a$ and $q = b^m - r_b$
2) Case II: $p = a^m + r_a$ and $q = b^m - r_b$
3) Case III: $p = a^m - r_a$ and $q = b^m + r_b$

Consequently, we introduce the concept of Least Significant Bits (LSBs) in the subsequent definition, based on the representations provided for each of these cases.

Definition 3. (LSBs for Near-Square Primes). Let l_1, l_2, m be positive integers. Suppose we have RSA primes p and q structured as $p = a^m \pm r_a$ and $q = b^m \pm r_b$. Assume there exist unknown values a_0 and b_0 such that:

$$p = (2^{l_1} \cdot a_0)^m \pm r_a, \tag{4}$$

and

$$q = (2^{l_2} \cdot b_0)^m \pm r_b. \tag{5}$$

We define r_a and r_b as the k-least significant bits of p and q, respectively. The value k must satisfy $k \leq l_1 m, l_2 m$ and adhere to the following conditions:

$$r_a \equiv \pm p \pmod{2^{l_1 m}}, \tag{6}$$

and

$$r_b \equiv \pm q \pmod{2^{l_2 m}}. \tag{7}$$

To identify prime numbers that meet the criteria outlined in Equations (4) and (5), we examine the binary representations of a^m and b_m. To satisfy the conditions for $p = a^m \pm r_a$ and $q = b^m \pm r_b$, the least significant bits (LSBs) of both a^m and b_m must form a sequence of k consecutive zeros. Let us denote the binary representation of a as r_{a_i} and that of b as r_{b_i}. In this context, i ranges from 1 to n. This concept can be expressed as follows:

$$a^m = \underbrace{r_{a_1} r_{a_2} r_{a_3} \cdots r_{a_{(n-k)}}}_{\substack{n-k \text{ many bits} \\ \text{of 1 and 0's}}} \quad \underbrace{r_{a_{(n-k+1)}} \cdots r_{a_n}}_{\substack{k \text{ many bits} \\ \text{of 0's}}} \tag{8}$$

$$b^m = \underbrace{r_{b_1} r_{b_2} r_{b_3} \cdots r_{b_{(n-k)}}}_{\substack{n-k \text{ many bits} \\ \text{of 1 and 0's}}} \quad \underbrace{r_{b_{(n-k+1)}} \cdots r_{b_n}}_{\substack{k \text{ many bits} \\ \text{of 0's}}} \tag{9}$$

Efficient algorithms, such as the random reconstruction algorithm, which has been further enhanced by other researchers, can be employed to determine the values of r_a and r_b that satisfy the conditions in Equations (6) and (7). In various contexts, including cryptography and digital signal processing, the LSBs of numbers are of interest because they can contain information or patterns that, if known or manipulated, might have significant implications. For instance, in cryptography, knowledge of the LSBs of certain numbers may be exploited in side-channel attacks to gain insights into cryptographic keys or operations.

A. New LSB Attack Case I

Theorem 1 shows that an RSA modulus can be factorized in polynomial time if an adversary knows specific LSBs of the RSA primes, particularly when the primes are nearly square as described in Case I with $p = a^m - r_a$ and $q = b^m - r_b$.

In detail, if the attacker has access to the k-bits corresponding to r_a and r_b of the RSA primes p and q, they can exploit this information. It is important to note that r_a and r_b are odd integers, as the rightmost bit of an odd prime is always 1.

Theorem 1. Consider positive integers a and b, where m is a power of 2 with a less than b but still within the range of $(2a^m + 1)^{\frac{1}{m}}$. Let N be defined as the product of $(a^m - r_a)$ and $(b^m - r_b)$, forming a valid RSA modulus. Assume that $r_a \equiv -p \pmod{2^m}$ and $r_b \equiv -q \pmod{2^m}$ such that $r_a < 2a^{\frac{m}{2}}$ and $r_b < 2b^{\frac{m}{2}}$. Additionally, the maximum value between r_a and r_b is less than 2^k. If we have knowledge of k-least significant bits (LSBs) of both p and q, and $2^{k-1}\left(2^{\frac{m}{2}} + 1\right)$ is sufficiently small, then it is feasible to factor N in polynomial time.

Proof: We begin by considering Lemma 2, which provides the following inequality:

$$(r_a r_b)^{\frac{1}{2}} < (ab)^{\frac{m}{2}} - N^{\frac{1}{2}} < 2^{\frac{m}{2}-1} r_a + \frac{r_b}{2} - 1. \tag{10}$$

We can rewrite Equation (10) as:

$$N^{\frac{1}{2}} + (r_a r_b)^{\frac{1}{2}} < (ab)^{\frac{m}{2}} < N^{\frac{1}{2}} + 2^{\frac{m}{2}-1} r_a + \frac{r_b}{2} - 1. \tag{11}$$

Given that we know r_a and r_b as the least significant bits (LSBs) of the primes p and q respectively, and assuming these LSBs can be obtained through side-channel attacks, we consider the maximum of $r_a, r_b \approx 2^k$ to be adequately small. We then calculate the difference between the lower and upper limits in Equation (11) as follows:

$$\begin{aligned} & N^{\frac{1}{2}} + 2^{\frac{m}{2}-1} r_a + \frac{r_b}{2} - 1 - N^{1/2} - (r_a r_b)^{\frac{1}{2}} \\ & < 2^k\left(2^{\frac{m}{2}-1} + \frac{1}{2}\right) - [(\min\{r_a, r_b\})^2]^{\frac{1}{2}} - 1 \\ & = 2^k\left(\frac{2^{\frac{m}{2}}+1}{2}\right) - \min\{r_a, r_b\} - 1 \\ & = 2^{k-1}\left(2^{\frac{m}{2}} + 1\right) - \min\{r_a, r_b\} - 1. \end{aligned} \tag{12}$$

This calculation shows the upper limit on the number of integers necessary to compute $(ab)^{\frac{m}{2}}$. The task of computing $(ab)^{\frac{m}{2}}$ can be achieved in polynomial time when $2^{k-1}\left(2^{\frac{m}{2}} + 1\right)$ is sufficiently small.

It is important to highlight that we can obtain $(ab)^m$ by simply squaring $\left((ab)^{\frac{m}{2}}\right)$. Thus, we observe the following:

$$\begin{aligned} r_a r_b - N &\equiv r_a r_b - [(a^m - r_a)(b^m - r_b)] \\ &\equiv r_a r_b - r_a r_b - (ab)^m + a^m r_b + b^m r_a \\ &\equiv -(ab)^m + a^m r_b + b^m r_a \\ &\equiv a^m r_b + b^m r_a \pmod{(ab)^m}. \end{aligned}$$

Note that, $-(ab)^m \pmod{(ab)^m} \equiv 0$. Given that $r_a < 2a^{\frac{m}{2}}$ and $r_b < 2b^{\frac{m}{2}}$, we can establish that:

$$a^m r_b + b^m r_a < (ab)^m.$$

Thus, the computation of $(a^m r_b + b^m r_a)$ can be accomplished without modular reduction. Since we already know the values of $a^m r_b + b^m r_a, r_a, r_b$, and $(ab)^m$, we can determine p and q by solving the quadratic equation as follows:

$$Z^2 + (a^m r_b + b^m r_a)Z + ((ab)^m r_a r_b).$$

Solving this, we find two solutions which are $Z_1 = -a^m r_b$ and $Z_2 = -b^m r_a$. Given the knowledge of r_a and r_b, we can compute

$$a^m = -\frac{Z_1}{r_b} \quad \text{and} \quad b^m = -\frac{Z_2}{r_a}.$$

Consequently, we conclude the proof by calculating the modulus N:

$$\frac{N}{b^m - r_b} = a^m - r_a.$$

■

The process for factorizing $N = pq$ using Theorem 1 is detailed in Algorithm 1. Below is the revised algorithm:

Algorithm 1 Factorization of $N = pq = (a^m - r_a)(b^m - r_b)$ using Theorem 1

Require: The integers N, m, r_a, r_b
Ensure: The primes p and q
1: Initialize $i = \lceil (r_a r_b)^{1/2} \rceil$.
2: **while** $i < \left\lfloor 2^{\frac{m}{2}-1} r_a + \frac{r_b}{2} - 1 \right\rfloor$ **do**
3: Compute $\sigma = \left(\left\lfloor \sqrt{N} \right\rfloor + i \right)^2$
4: Determine $x \equiv r_a r_b - N \pmod{\sigma}$
5: Solve the quadratic equation $Z^2 + xZ + \sigma r_a r_b = 0$
6: Let $z_1 = Z_1$ and $z_2 = Z_2$
7: **if** $\frac{N}{\frac{z_1}{r_b} - r_a}$ or $\frac{N}{\frac{z_2}{r_a} - r_b} \neq$ integer **then**
8: $i++$
9: **else**
10: **end if**
11: **end while**
12: **Output** $p = z_1$ and $q = z_2$

B. New LSB Attack Case II

In Theorem 2, we present a method for efficiently factoring an RSA modulus when an attacker has knowledge of specific least significant bits (LSBs) of the RSA prime numbers. This method is particularly effective when the prime numbers follow a near-square prime structure as described in Case II, where p is represented as $a^m + r_a$ and q as $b^m - r_b$. Specifically, the adversary gains access to the k-bit values corresponding to r_a and r_b of the RSA primes p and q. We introduce Theorem 2 to illustrate that with the bounds of $N^{\frac{1}{2}} - (ab)^{\frac{m}{2}}$ derived in Lemma 4, it is possible to factorize the modulus $N = pq$ in polynomial time.

Theorem 2. Consider positive integers a and b, where m is a power of 2. We have $a < b$, and they both lie within the range of $(2a^m + 1)^{\frac{1}{m}}$. Let N be defined as the product of $(a^m + r_a)$ and $(b^m - r_b)$, forming a valid RSA modulus. Assume that $r_a \equiv p \pmod{2^m}$ and $r_b \equiv -q \pmod{2^m}$ such that $r_a < 2a^{\frac{m}{2}}$ and $r_b < 2b^{\frac{m}{2}}$. Additionally, the larger of the two values, r_a and r_b, is less than 2^k. If k least significant bits (LSBs) of both p and q are known, and $2^k\left(2^{\frac{m}{2}} + 1\right)$ is sufficiently small, then it becomes feasible to factor the modulus N efficiently within a polynomial time frame.

Proof: We start with the inequality provided in Lemma 4:

$$\frac{1}{2}(r_a - r_b) - 1 < N^{\frac{1}{2}} - (ab)^{\frac{m}{2}} < (r_a r_b)^{\frac{1}{2}}. \tag{13}$$

We can rewrite Equation (13) as:

$$N^{\frac{1}{2}} - (r_a r_b)^{\frac{1}{2}} < (ab)^{\frac{m}{2}} < N^{\frac{1}{2}} + \frac{1}{2}(r_a - r_b) + 1. \tag{14}$$

Suppose we have the least significant bits (LSBs) of primes p and q denoted as r_a and r_b, respectively. These LSBs might be obtained through side-channel attacks. Given that the $\max\{r_a, r_b\} \approx 2^k$ falls within the range of being suitably small, we can calculate the difference between the lower and upper bounds of Equation (14) as follows:

$$\begin{aligned} &N^{\frac{1}{2}} + \frac{1}{2}(r_a - r_b) + 1 - N^{\frac{1}{2}} + (r_a r_b)^{\frac{1}{2}} \\ &= \frac{1}{2}(r_a - r_b) + (r_a r_b)^{\frac{1}{2}} + 1 \\ &< 2^{k+1}\left(2^{\frac{m}{2}-1} + \frac{1}{2}\right) - [(\min\{r_a, r_b\})^2]^{\frac{1}{2}} + 1 \\ &= 2^{k+1}\left(\frac{2^{\frac{m}{2}} + 1}{2}\right) - \min\{r_a, r_b\} + 1 \\ &= 2^k\left(2^{\frac{m}{2}} + 1\right) - \min\{r_a, r_b\} + 1. \end{aligned} \tag{15}$$

This calculation shows the upper bound on the number of integers needed to compute $(ab)^{\frac{m}{2}}$. The computation of $(ab)^{\frac{m}{2}}$ can be done in polynomial time if $2^k\left(2^{\frac{m}{2}} + 1\right)$ is sufficiently small.
Note that $(ab)^m$ can be obtained by squaring $\left((ab)^{\frac{m}{2}}\right)$. Therefore, we have:

$$\begin{aligned} N + r_a r_b &\equiv (a^m + r_a)(b^m - r_b) + r_a r_b \\ &\equiv (ab)^m - a^m r_b + b^m r_a - r_a r_b + r_a r_b \\ &\equiv (ab)^m - a^m r_b + b^m r_a \\ &\quad \text{since } (ab)^m \pmod{(ab)^m} \equiv 0 \\ &\equiv (b^m r_a - a^m r_b) \pmod{(ab)^m}. \end{aligned}$$

Since r_a and r_b are much smaller than $2a^{\frac{m}{2}}$ and $2b^{\frac{m}{2}}$ respectively, it follows that:

$$b^m r_a - a^m r_b < (ab)^m.$$

Thus, the computation of $b^m r_a - a^m r_b$ can be performed without modular reduction. Given that we already know the values of $b^m r_a - a^m r_b, r_a, r_b$, and $(ab)^m$,we can solve for p and q by solving the quadratic equation:

$$Z^2 + (b^m r_a - a^m r_b)Z - ((ab)^m r_a r_b).$$

Solving this equation, we identify two solutions: $Z_1 = a^m r_b$ and $Z_2 = -b^m r_a$. Knowing r_a and r_b, we can determine:

$$a^m = \frac{Z_1}{r_b} \quad \text{and} \quad b^m = -\frac{Z_2}{r_a}.$$

Finally, we conclude the proof by computing the modulus N:

$$\frac{N}{b^m - r_b} = a^m + r_a.$$

This completes the proof. ∎

We now describe the factorization of $N = pq$ as outlined in Theorem 2, which is implemented in Algorithm 2.

Algorithm 2 Factorization of $N = pq = (a^m + r_a)(b^m - r_b)$ using Theorem 2

Require: The integers N, m, r_a, r_b
Ensure: The primes p and q
1: Initialize $i = \lceil (r_a r_b)^{1/2} \rceil$.
2: **while** $i < (r_a r_b)^{1/2}$ **do**
3: Compute $\sigma = \left(\left\lfloor \sqrt{N} \right\rfloor + i \right)^2$
4: Determine $x \equiv N + r_a r_b \pmod{\sigma}$
5: Solve the quadratic equation $Z^2 + xZ - \sigma r_a r_b = 0$
6: Let $z_1 = Z_1$ and $z_2 = Z_2$
7: **if** $\frac{N}{\frac{z_1}{r_b} + r_a}$ or $\frac{N}{\frac{z_2}{r_a} - r_b} \neq$ integer **then**
8: $i++$
9: **else**
10: **end if**
11: **end while**
12: **Output** $p = z_1$ and $q = z_2$

C. New LSB Attack Case III

In Theorem 3, we present an approach to efficiently factorize an RSA modulus when the attacker knows certain least significant bits (LSBs) of the RSA prime factors. This technique proves particularly effective when the primes exhibit a near-square structure as detailed in Case III, where $p = a^m - r_a$ and $q = b^m + r_b$. In particular, the attacker has access to the k-bit values representing r_a and r_b for the primes p and q. We introduce Theorem 3 to demonstrate that, under the constraints specified by $N^{\frac{1}{2}} - (ab)^{\frac{m}{2}}$ as outlined in Lemma 5, the RSA modulus $N = pq$ can be efficiently factorized.

Theorem 3. Let a and b be positive integers with m being a power of 2, and let a be less than b but still within the range of $(2a^m + 1)^{\frac{1}{m}}$. Define N as the product of $(a^m - r_a)$ and $(b^m + r_b)$. Assume that $r_a \equiv -p \pmod{2^m}$ and $r_b \equiv q \pmod{2^m}$ with $r_a < 2a^{\frac{m}{2}}$ and $r_b < 2b^{\frac{m}{2}}$. Additionally, if the maximum value between r_a and r_b is less than 2^k, and we know the k least significant bits of both p and q, and $2^k \left(2^{\frac{m}{2}} + 1\right)$ is sufficiently small, then N can be factorized within polynomial time.

Proof: Referring to Lemma 5, we derive the following inequality:

$$-(1+\sqrt{2})(r_a r_b)^{\frac{1}{2}} < N^{\frac{1}{2}} - (ab)^{\frac{m}{2}} < \frac{1}{2}(r_b - r_a). \quad (16)$$

We can rewrite Equation (16) as:

$$N^{\frac{1}{2}} + \frac{1}{2}(r_b - r_a) < (ab)^{\frac{m}{2}} < N^{\frac{1}{2}} + (1+\sqrt{2})(r_a r_b)^{\frac{1}{2}}. \quad (17)$$

Given the knowledge of the least significant bits (LSBs), denoted as r_a for p and r_b for q, which can be obtained through side-channel attacks, and considering the maximum of these LSBs is $\max(r_a, r_b) \approx 2^k$ and is relatively small, we can calculate the difference between the upper and lower bounds of Equation (17) as follows:

$$\begin{aligned}
&\left(N^{\frac{1}{2}} + (1+\sqrt{2})(r_a r_b)^{\frac{1}{2}}\right) - \left(N^{\frac{1}{2}} + \frac{1}{2}(r_b - r_a)\right) \\
&= (1+\sqrt{2})(r_a r_b)^{1/2} - \frac{1}{2}(r_b - r_a) \\
&< 2^{k+1}\left(2^{\frac{m}{2}-1} + \frac{1}{2}\right) - [(\min\{r_a, r_b\})^2]^{\frac{1}{2}} \\
&= 2^{k+1}\left(\frac{2^{\frac{m}{2}}+1}{2}\right) - \min\{r_a, r_b\} \\
&= 2^k\left(2^{\frac{m}{2}} + 1\right) - \min\{r_a, r_b\}. \quad (18)
\end{aligned}$$

This calculation shows the maximum number of integers required to determine $(ab)^{\frac{m}{2}}$. If $2^k \left(2^{\frac{m}{2}} + 1\right)$ is sufficiently small, this process can be completed in polynomial time.

As previously discussed, determining $(ab)^m$ involves squaring $\left((ab)^{\frac{m}{2}}\right)^2$. Now, consider the following expressions:

$$\begin{aligned}
N + r_a r_b &\equiv (a^m - r_a)(b^m + r_b) + r_a r_b \\
&\equiv (ab)^m + r_a r_b + a^m r_b - b^m r_a - r_a r_b \\
&\equiv (ab)^m + a^m r_b - b^m r_a \\
&\equiv (a^m r_b - b^m r_a) \pmod{(ab)^m}.
\end{aligned}$$

Given that $r_a \ll 2a^{\frac{m}{2}}$ and $r_b \ll 2b^{\frac{m}{2}}$, it is clear that:

$$a^m r_b - b^m r_a < (ab)^m.$$

Thus, we can compute $(a^m r_b - b^m r_a)$ without modular reduction. With the known values of r_a, r_b, $(ab)^m$, and $(a^m r_b - b^m r_a)$, we can compute the primes p and q by solving the following quadratic equation:

$$Z^2 + (a^m r_b - b^m r_a)Z - ((ab)^m r_a r_b).$$

From this equation, we identify $Z_1 = -a^m r_b$ and $Z_2 = b^m r_a$. With the known values of r_a and r_b, we can calculate:

$$a^m = -\frac{Z_1}{r_b} \quad \text{and} \quad b^m = \frac{Z_2}{r_a}.$$

Finally, we can factor the modulus N by performing the following calculation:

$$\frac{N}{b^m + r_b} = a^m - r_a.$$

This concludes the proof. ∎

Next, we outline the steps to factorize $N = pq$ according to Theorem 3, as illustrated in Algorithm 3. The updated algorithm is presented below:

Algorithm 3 Factorization of $N = pq = (a^m - r_a)(b^m + r_b)$ using Theorem 3

Require: The integers N, m, r_a, r_b
Ensure: The primes p and q
Initialize $i = \left\lceil -(1+\sqrt{2})(r_a r_b)^{\frac{1}{2}} \right\rceil$.
while $i < \frac{1}{2}(r_b - r_a)$ **do**
  Compute $\sigma = \left(\left\lceil \sqrt{N} \right\rceil + i\right)^2$
  Determine $x \equiv N + r_a r_b \pmod{\sigma}$
  Solve the quadratic equation $Z^2 + xZ - \sigma r_a r_b = 0$
  Let $z_1 = -Z_1$ and $z_2 = Z_2$
  if $\frac{N}{\frac{z_1}{r_b} - r_a}$ or $\frac{N}{\frac{z_2}{r_a} + r_b} \neq$ integer **then**
    $i++$
  else
  end if
end while
Output $p = z_1$ and $q = z_2$

IV. Counting Number of Vulnerable Near-Square Primes

Upon examining Equations (8) and (9), it becomes clear that r_{a_1} through $r_{a_{(n-k)}}$ represent the binary representations of squared numbers, and the same applies to r_{b_1} through $r_{b_{(n-k)}}$. In the following theorem, our goal is to identify the squared numbers with $n-k$ bits.

Theorem 4. For a large positive integer n and a small positive integer k, there are at least $\left\lfloor \frac{2-\sqrt{2}}{2}(2^{n-k})^{\frac{1}{2}} \right\rfloor$ number of square primes within the range $\left(2^{n-k-1}, 2^{n-k} - 1\right)$.

Proof: Let us define the set $X = \{x_i^2\}$, where i ranges over the positive integers. This set consists of all squared numbers falling between $\left(2^{n-k-1}, 2^{n-k} - 1\right)$. Specifically,

$$2^{n-k-1} < x_i^2 < 2^{n-k} - 1.$$

This can be rewritten as:

$$(2^{n-k-1})^{\frac{1}{2}} < x_i < \left(2^{n-k} - 1\right)^{\frac{1}{2}},$$

which implies

$$(2^{n-k-1})^{\frac{1}{2}} < x_i < \left(\left((2^{n-k})^{\frac{1}{2}} - 1\right)\left((2^{n-k})^{\frac{1}{2}} + 1\right)\right)^{\frac{1}{2}}.$$

To determine the smallest number of squared values within the interval from 2^{n-k-1} and $2^{n-k}-1$, we need to calculate the integer difference between the upper and lower bounds as shown in Equation (19). This is computed as follows:

$$\left\lfloor \left(\left((2^{n-k})^{\frac{1}{2}} - 1\right)\left((2^{n-k})^{\frac{1}{2}} + 1\right)\right)^{\frac{1}{2}} - (2^{n-k-1})^{\frac{1}{2}} \right\rfloor. \tag{19}$$

Now, let us simplify (19) further:

$$\begin{aligned} &> \left\lfloor \left(\left((2^{n-k})^{\frac{1}{2}} - 1\right)\left((2^{n-k})^{\frac{1}{2}} - 1\right)\right)^{\frac{1}{2}} - (2^{n-k-1})^{\frac{1}{2}} \right\rfloor \\ &= \left\lfloor \left(\left((2^{n-k})^{\frac{1}{2}} - 1\right)^2\right)^{\frac{1}{2}} - (2^{n-k-1})^{\frac{1}{2}} \right\rfloor \\ &= \left\lfloor (2^{n-k})^{\frac{1}{2}} - 1 - (2^{n-k-1})^{\frac{1}{2}} \right\rfloor \\ &= \left\lfloor \frac{2-\sqrt{2}}{2}(2^{n-k})^{\frac{1}{2}} - 1 \right\rfloor. \end{aligned} \tag{20}$$

In the context of a sufficiently large positive integer n and a relatively small positive integer k, we can approximate the expression in the last line (Equation 20) as:

$$\left\lfloor \frac{2-\sqrt{2}}{2}(2^{n-k})^{\frac{1}{2}} - 1 \right\rfloor \approx \left\lfloor \frac{2-\sqrt{2}}{2}(2^{n-k})^{\frac{1}{2}} \right\rfloor.$$

This concludes the proof. ■

Theorem 5. Consider positive integers a and b, where $m \geq 2$, and a and b satisfy the condition $a < b < (2a^m + 1)^{\frac{1}{m}}$. Let $N = pq = (a^m \pm r_a)(b^m \mp r_b)$ be a valid RSA modulus, where $r_a \equiv p \pmod{2^m}$ and $r_b \equiv q \pmod{2^m}$. It is further given that $r_a < 2a^{m/2}$ and $r_b < 2b^{m/2}$, and $\max\{r_a, r_b\} < 2^k$. Let $x > 0$ be an integer such that x^2 represents the smallest squared number with an n-bit size. Under the condition that $2^k\left(2^{\frac{m}{2}} + 1\right)$ is sufficiently small and we have knowledge of k LSBs of both p and q, there are at most

$$\left\lfloor \frac{2-\sqrt{2}}{2}(2^{n-k})^{\frac{1}{2}} \right\rfloor \left(\frac{2^k}{\log(x)^2} + \frac{2^k}{\log\left(\left\lfloor \frac{2-\sqrt{2}}{2}(2^{n-k})^{\frac{1}{2}} \right\rfloor + x\right)^2} \right)$$

potential candidates for p and q such that $p = a^m \pm r_a$ and $q = b^m \mp r_b$, each having a size of n bits.

Proof: Let's consider the situation where x^2 is the smallest perfect square number with $n-k$ bits. We introduce the prime-counting function $\pi(x)$, which counts prime numbers between x^2 and the larger of $\max\{r_a, r_b\} + x^2$, defined as follows (Equation 21):

$$\pi_1^*(x) = \frac{\max\{r_a, r_b\} + x^2}{\log\left(\max\{r_a, r_b\}\right) + x^2} - \frac{x^2}{\log x^2}. \tag{21}$$

We can make an approximation of (21) as follows:

$$\begin{aligned} &\approx \frac{\max\{r_a, r_b\} + x^2}{\log x^2} - \frac{x^2}{\log x^2} \\ &= \frac{\max\{r_a, r_b\} + x^2 - x^2}{\log x^2} = \frac{\max\{r_a, r_b\}}{\log x^2} \\ &< \frac{2^k}{\log x^2}. \end{aligned}$$

Now, referring to Theorem 4, we know that there are approximately $\left\lfloor \frac{2-\sqrt{2}}{2}(2^{n-k})^{\frac{1}{2}} \right\rfloor$ squared numbers with $n-k$-bit sizes. In this context, $\pi_1^*(x)$ for consecutive squared numbers can be represented as follows:

$$\begin{aligned} \pi_1^*(x) &< \frac{2^k}{\log(x)^2} \\ \pi_1^*(1+x) &< \frac{2^k}{\log(1+x)^2} \\ \pi_1^*(2+x) &< \frac{2^k}{\log(2+x)^2} \\ &\vdots \\ &\vdots \\ \pi_1^*\left(\left\lfloor \frac{2-\sqrt{2}}{2}(2^{n-k})^{\frac{1}{2}} \right\rfloor + x\right) &< \frac{2^k}{\log\left(\left\lfloor \frac{2-\sqrt{2}}{2}(2^{n-k})^{\frac{1}{2}} \right\rfloor + x\right)^2}. \end{aligned} \tag{22}$$

We can represent the summation given in Equation (22) by applying the formula for the sum of an arithmetic progression. This formula involves multiplying the number of terms

indicated by i by the average of the first and last terms in the progression, and then dividing the result by 2. In other words, π_2^* can be expressed as

$$\begin{aligned} &= \sum_{i=0}^{\left\lfloor \frac{2-\sqrt{2}}{2}(2^{n-k})^{\frac{1}{2}} \right\rfloor} \frac{2^k}{\log(i+x)^2} \\ &< \left\lfloor \frac{2-\sqrt{2}}{2}(2^{n-k})^{\frac{1}{2}} \right\rfloor \left(\pi_1^*(x) + \pi_1^* \left(\left\lfloor \frac{2-\sqrt{2}}{2}(2^{n-k})^{\frac{1}{2}} \right\rfloor + x \right) \right) \\ &< \left\lfloor \frac{2-\sqrt{2}}{2}(2^{n-k})^{\frac{1}{2}} \right\rfloor \left(\frac{2^k}{\log(x)^2} + \frac{2^k}{\log\left(\left\lfloor \frac{2-\sqrt{2}}{2}(2^{n-k})^{\frac{1}{2}} \right\rfloor + x \right)^2} \right) \end{aligned}$$

This concludes the proof. ■

The outcome derived from Theorem 5 demonstrates the existence of a notable quantity of prime numbers that meet the conditions outlined in the attacks presented in Section III.

V. Comparing Results

In this section, we compare our findings with existing attacks that involve known bits of primes. Table I compiles a summary of all these attacks.

TABLE I: COMPARISON OF OUR METHOD AGAINST EXISTING ATTACKS WITH KNOWN BITS OF PRIMES

Cryptanalysis	Position of known bits	Conditions for bits of primes	Benefits/ Drawbacks
[24]	LSBs or MSBs	0.5 of the bits of p or q	**Benefits:** Fast speed **Drawbacks:** Requires lot of known bits
[25]	Any position (in blocks)	$\log_e(2) \approx 0.7$ of the bits of p or q	
[10]	Any position	$r_p = N^{\delta_1}$, $r_q = N^{\delta_2}$, $\delta_1 + \delta_2 \geq 0.57$ of the bits of p or q	
[11]	LSBs	$r_p = N^{\delta_1}$, $r_q = N^{\delta_2}$, $\delta_1 + \delta_2 \geq 0.5$ of the bits of p or q	
[12]	LSBs	$r_p, r_q < 2^k$ where 2^k is sufficiently small with $r_p, r_q < N^{\frac{k}{\log_2 N}}$	**Benefits:** Fast speed, requires less of known bits **Drawbacks:** Requires specific hardware to conduct side-channel attack
New LSB Attacks (Theorem 1 - Theorem 3)	LSBs	$r_a < 2a^{m/2}$, $r_b < 2b^{m/2}$, $\max\{r_a, r_b\} \approx 2^k$ where $2^{k-1}\left(2^{\frac{m}{2}}+1\right)$ is sufficiently small with $r_a, r_b < N^{\frac{k}{\log_2 N}}$	

VI. Conclusion

In conclusion, this study significantly extends our previous research by highlighting a critical vulnerability inherent in the structure of RSA primes. We have shown the risks associated with using near-square primes in the generation of the RSA modulus $N = pq$. It is crucial to acknowledge that during the random generation of primes p and q, the accidental selection of near-square primes is a real possibility. This structural characteristic of N might unknowingly be present in current cryptographic applications, as no existing cryptographic implementations actively prevent the generation of such primes. Our research reveals the potential risks of using these primes, which can severely compromise RSA security. Specifically, we present three scenarios where near-square primes are key components of RSA factors, configured as follows:

1) Case I: $p = a^m - r_a$ and $q = b^m - r_b$;
2) Case II: $p = a^m + r_a$ and $q = b^m - r_b$;
3) Case III: $p = a^m - r_a$ and $q = b^m + r_b$.

In our study, we assume that potential adversaries may have knowledge of specific least significant bits (LSBs) within RSA primes that feature these near-square prime structures. Specifically, the attacker gains access to the bits corresponding to r_a and r_b within the RSA primes p and q. Our findings show that our attack can factor N in polynomial time with only a small number of LSBs, as long as the RSA primes exhibit the defined structural characteristics.

References

[1] Abderrahmane Nitaj, Muhammad Rezal Kamel Ariffin, Nurul Nur Hanisah Adenan, Terry Shue Chien Lau and Jiahu Chen, "Security issues of novel RSA variant," *IEEE Access*, vol. 10, pp53788-53796, 2022.

[2] Wan Nur Aqlili Wan Mohd Ruzai, Abderrahmane Nitaj, Muhammad Rezal Kamel Ariffin, Zahari Mahad and Muhammad Asyraf Asbullah, "Increment of insecure RSA private exponent bound through perfect square RSA Diophantine parameters cryptanalysis," *Comput. Stand. Interfaces*, vol. 80, no. 1, pp103584, 2022.

[3] Ron Rivest, Adi Shamir and Leonard Adleman, "A method for obtaining digital signatures and public-key cryptosystems," *Commun. ACM*, vol. 21, no. 2, pp120-126, 1978.

[4] Anthony Adam Pranajaya and Iwan Sugiarto, "Simulation and Analysis on Cryptography by Maclaurin Series and Laplace Transform," IAENG International Journal of Applied Mathematics, vol. 52, no. 2, pp441-449, 2022.

[5] Jackson J and Perumal R, "Another Cryptanalysis of a Tropical Key Exchange Protocol," IAENG International Journal of Computer Science, vol. 50, no. 4, pp1330-1336, 2023.

[6] Abdullah M. Jaafar and Azman Samsudin, "Visual Digital Signature Scheme: A New Approach," IAENG International Journal of Computer Science, vol. 37, no. 4, pp350-358, 2010.

[7] Gabriela Mogos, "Ciphertext-policy Attribute-based Encryption Using Quantum Multilevel Secret Sharing Scheme," IAENG International Journal of Computer Science, vol. 45, no. 4, pp500-504, 2018.

[8] J. M. Pollard, "Theorems on factorization and primality testing," in *Math. Proc. Camb. Philos. Soc. 1974*, pp521-528.

[9] Dan Boneh, Glenn Durfee, and Yair Frankel, "An Attack on RSA Given a Small Fraction of the Private Key Bits," Lecture Notes in Computer Science: International Conference on the Theory and Application of Cryptology and Information Security 1998, 18-22 October, 1998, Beijing, China, pp25-34.

[10] Nadia Heninger and Hovav Shacham, "Reconstructing RSA Private Keys From Random Key Bits," Lecture Notes in Computer Science: Annual International Cryptology Conference 2009, 16-20 August, 2009, Santa Barbara, CA, USA, pp1-17.

[11] Subhamoy Maitra, Santanu Sarkar, and Sourav Sen Gupta, "Factoring RSA Modulus Using Prime Reconstruction From Random Known Bits," Lecture Notes in Computer Science: International Conference on Cryptology in Africa 2010, 3-6 May, 2010, Stellenbosch, South Africa, pp82-99.

[12] Amir Hamzah Abd Ghafar, Muhammad Rezal Kamel Ariffin, and Muhammad Asyraf Asbullah, "A new LSB attack on special-structured RSA primes," *Symmetry*, vol. 12, no. 5, pp838, 2020.

[13] Paul Kocher, Joshua Jaffe, Benjamin Jun, and Pankaj Rohatgi, "Introduction to differential power analysis," *J. Cryptogr. Eng.*, vol. 1, no. 1, pp5-27, 2011.

[14] Paul C. Kocher, "Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS, and Other Systems," Lecture Notes in Computer Science: Annual International Cryptology Conference 1996, 18-22 August, 1996, Santa Barbara, CA, USA, pp104-113.

[15] Paul Kocher, Joshua Jaffe, and Benjamin Jun, "Differential Power Analysis," Lecture Notes in Computer Science: Annual International Cryptology Conference 1999, 15-19 August, 1999, Santa Barbara, CA, USA, pp388–397.

[16] Zdenek Martinasek, Vaclav Zeman, and Krisztina Trasy, "Simple electromagnetic analysis in cryptography," *Int. J. Adv. Telecommun. Electrotech. Signals Syst.*, vol. 1, no. 1, pp5-27, 2012.

[17] Jonghyeon Cho, Taehun Kim, Soojin Kim, and Miok Im, Taehyun Kim, and Youngjo Shin, "Real-time detection for cache side channel attack using performance counter monitor," *Appl. Sci.*, vol. 10, no. 3, pp984, 2020.

[18] Daniel Genkin, Adi Shamir, and Eran Tromer, "RSA Key Extraction Via Low-Bandwidth Acoustic Cryptanalysis," Lecture Notes in Computer Science: Annual International Cryptology Conference 2014, 17-21 August, 2014, Santa Barbara, CA, USA, pp444–461.

[19] Wan Nur Aqlili Wan Mohd Ruzai, Amir Hamzah Abd Ghafar, Nur Raidah Salim and Muhammad Rezal Kamel Ariffin, "On (unknowingly) using near-square RSA primes," *Symmetry*, vol. 14, no. 9, pp1898, 2022.

[20] Daniel Shanks, "A sieve method for factoring numbers of the form $n^2 + 1$," *Math. Comput.*, vol. 13, no. 66, pp78-86, 1959.

[21] Amir Hamzah Abd Ghafar, Muhammad Rezal Kamel Ariffin, and Muhammad Asyraf Asbullah, "A new attack on special-structured RSA primes," *Malays. J. Math. Sci.*, vol. 12, no. S, pp111-125, 2019.

[22] Wan Nur Aqlili Wan Mohd Ruzai, Nurul Nur Hanisah Adenan, Muhammad Rezal Kamel Ariffin, Amir Hamzah Abd Ghafar, and Mohamat Aidil Mohamat Johari, "An attack on $N = p^2q$ with partially known bits on the multiple of the prime factors," *Malays. J. Math. Sci.*, vol. 15, no. S, pp63-75, 2021.

[23] Elaine Barker and Allen Roginsky, "Transitioning the Use of Cryptographic Algorithms and Key Lengths: NIST Special Publication," in *National Institute of Standards and Technology*, Revision 2, vol. 800-131A.

[24] Don Coppersmith, "Finding a Small Root of a Bivariate Integer Equation: Factoring with High Bits Known," Lecture Notes in Computer Science: International Conference on the Theory and Applications of Cryptographic Techniques 1996, 12-16 May, 1996, Saragossa, Spain, pp178-189.

[25] Mathias Herrmann and Alexander May, "Solving Linear Equations Modulo Divisors: On Factoring Given Any Bits," Lecture Notes in Computer Science: International Conference on the Theory and Application of Cryptology and Information Security 2008, 7-11 December, 2008, Melbourne, Australia, pp406-424.