

An Improved Two-Step Attack on CRYSTALS-Kyber

Kai Wang
 Nanjing University
 School of Integrated Circuits
 Suzhou, China
 wang_kai@smail.nju.edu.cn

Dejun Xu
 Nanjing University
 School of Integrated Circuits
 Suzhou, China
 xudejun@smail.nju.edu.cn

Jing Tian*
 Nanjing University
 School of Integrated Circuits
 Suzhou, China
 tianjing@nju.edu.cn

ABSTRACT

After three rounds of post-quantum cryptography (PQC) strict evaluations conducted by the national institute of standards and technology (NIST), CRYSTALS-Kyber has successfully been selected and drafted for standardization from the mid of 2022. It becomes urgent to further evaluate Kyber's physical security for the upcoming deployment phase. In this paper, we present an improved two-step attack on Kyber to quickly recover the full secret key, s , by using much fewer energy traces and less time. In the first step, we use the correlation power analysis (CPA) attack to obtain a portion of guess values of s with a small number of energy traces. The CPA attack is enhanced by utilizing both the Pearson and Kendall's rank correlation coefficients and modifying the leakage model to improve the accuracy. In the second step, we adopt the lattice attack to recover s based on the results of CPA. The success rate is largely built up by constructing a trial-and-error method. We implement the proposed attack for the reference implementation of Kyber512 (4 128-value groups of s) on ARM Cortex-M4 and successfully recover a 128-value group of s in about 9 minutes using a 16-core machine. Additionally, in that case, we only cost at most 60 CPA guess values for a group and 15 power traces for a guess.

KEYWORDS

Lattice-based cryptography, CRYSTALS-Kyber, Side-channel attack, Power analysis

ACM Reference Format:

Kai Wang, Dejun Xu, and Jing Tian. 2024. An Improved Two-Step Attack on CRYSTALS-Kyber. In *Proceedings of 2024 ACM/IEEE International Conference on Computer-Aided Design (ICCAD 2024)*. ACM, New York, NY, USA, 9 pages. <https://doi.org/XXXXXX.XXXXXXX>

1 INTRODUCTION

Traditional public-key cryptography Rivest-Shamir-Adleman (RSA) algorithm [1] and elliptic-curve cryptography (ECC) [2] rely on the computational intractability of integer decomposition and discrete logarithm problems respectively. However, concerns have been raised with the emergence of quantum computing because they

*Corresponding author.

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for components of this work owned by others than the author(s) must be honored. Abstracting with credit is permitted. To copy otherwise, or republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee. Request permissions from permissions@acm.org.

ICCAD 2024, October 27–31, 2024, NEW JERSEY, USA

© 2024 Copyright held by the owner/author(s). Publication rights licensed to ACM.

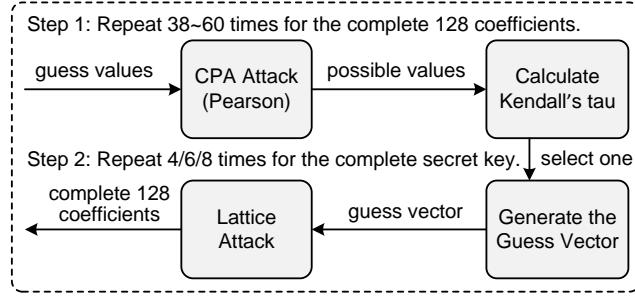
ACM ISBN 978-1-4503-XXXX-X/18/06...\$15.00

<https://doi.org/XXXXXX.XXXXXXX>

can be cracked in polynomial time by Shor's algorithm [3], and thereby revealing the security of existing cryptographic algorithms is insufficient. Recognizing this problem, the national institute of standards and technology (NIST) started the post-quantum cryptography (PQC) standardization process with the aim of standardizing quantum-resistant cryptographic algorithms in 2016 [4]. By July 2022, NIST released the post-quantum cryptographic standard candidates including three signatures and a key encapsulation mechanism (KEM) algorithm in the third round [5]. CRYSTALS-Kyber [6] is that only KEM.

Kyber is a lattice-based cryptographic algorithm constructed based on the module-learning with errors (M-LWE) problem. Even in quantum computing, the M-LWE problem is considered to be secure [7]. It should be noted that the mathematical security of Kyber has been widely recognized by the cryptography community. However, for the upcoming deployment phase, it becomes urgent to emphasize its physical security.

Kocher *et al.* first introduced side-channel attacks (SCAs) in 1996 by leveraging the data dependency on power consumption of cryptographic devices [8]. Generally, in the absence of any protective measures, devices running the cryptographic algorithms with long-term keys are susceptible to SCAs such as simple power analysis (SPA) attack, template attack (TA), and correlation power analysis (CPA) attack [7]. Different kinds of SCAs for Kyber have gradually emerged. In terms of SPA, Xu *et al.* successfully conducted such attack on the inverse number theoretic transform (INTT) of the reference implementation of Kyber512 and the pqm4 implementation by constructing specific ciphertext pairs, recovering a coefficient of a secret key costs $8 \sim 960$ power traces [9]. For TA, Works in [10–12] analyzed power traces collected from a large number of devices using belief propagation techniques to construct attack templates, enabling the recovery of keys from individual power traces. All of them require tremendous extra data to establish good templates. For CPA, most of previous works [13–15] are chosen-ciphertext attacks (CCAs). The latest work in [15] can significantly reduce the power traces compared to prior works by using an efficient two-step scheme to deal with the imperfect SCA oracles. However, since the NIST PQC KEMs are CCA secure, all of them need extra efforts such as plaintext checking to verify the final results. In [16], Yang *et al.* tried to carry out a random ciphertext CPA attack on the reference implementation of Kyber512, successfully recovering two coefficients of secret key using 20 or more power traces within a few minutes. Meanwhile, they have demonstrated that the chosen ciphertext CPA attack can improve the efficiency in some degree. Nevertheless, They adopted the original CPA method and the rest of coefficients of the secret key are needed to be recovered separately in the same way. In [17], Yen-Ting Kuo and Atsushi Takayasu recently presented a novel two-step attack on Kyber by integrating

**Figure 1: The flowchart of the proposed attack.**

the random ciphertext CPA attack with the lattice attack. They constructed a lower dimension of M-LWE problem in the NTT process based on the guess values of CPA and directly calculated the full key. Two hundreds simulated traces are used in their experiments to recover the secret key with about 20 minutes on a 16-core machine for Kyber512. However, they only conducted computer simulations. In this paper, we take the solution of [17] as the starting point and develop an improved two-step attack method on Kyber to further validate it in practical and improve the efficiency.

The proposed two steps can be overviewed as Fig. 1. In this first step, we apply an enhanced CPA attack to recover parts of coefficients of secret key by exploiting the combined correlation between the modified Hamming weight (HW) for some intermediate values and the power consumption of the decryption process in Kyber, specifically the point-wise multiplication covering a secret polynomial and a ciphertext. In this way, some of the secret coefficients can be recovered using a small amount of power traces in number theoretic transform (NTT) domain. In the second step, We take the points of the lattice attack used in [17] and construct a trail-and-error algorithm to recover the entire secret key. Our main contributions can be summarized as follows:

- We use both Pearson and Kendall’s rank correlation coefficients (Kendall’s tau) and modify the leakage model to improve the accuracy of CPA attacks.
- Based on lattice attack, we construct a trail-and-error algorithm to improve the success rate.
- We combine the two steps of attacks together and apply to Kyber512 on ARM Cortex-M4. Experimental results show that the proposed method only costs 38 ~ 60 CPA guess values and about 9 minutes on a 16-core machine to recover the 128 coefficients of a secret key s , much faster than the state-of-the-art.

The rest of this paper is structured as follows. Section 2 provides preliminary content. Section 3 presents the traditional attacks and our attack method. Experimental results are described in Section 4. Section 5 summarizes the paper.

2 PRELIMINARIES

In this section, we will introduce the notations, the principles of the LWE/M-LWE problem, NTT in Kyber, CPA Attack, and Kendall’s tau.

Table 1: Parameter in CRYSTALS-Kyber

	k	n	q	d_u	d_v	η_1	η_2
Kyber512	2	256	3329	10	4	3	2
Kyber768	3	256	3329	10	4	2	2
Kyber1024	4	256	3329	11	5	2	2

2.1 Notations

The ring of integers modulo the prime number q is denoted as \mathbb{Z}_q . Each polynomial ring $\mathcal{R}_q = \mathbb{Z}_q[x]/(x^n + 1)$ with moduli $x^n + 1$ and q has n coefficients. The Greek symbols β_η and \mathcal{U} denote the centered binomial distribution with parameter η and the uniform distribution, respectively. The vectors are represented by bold lowercase letters, such as \mathbf{a} , and the vectors in the NTT domain have a hat added to them, such as $\hat{\mathbf{a}}$. The matrices are represented by bold uppercase letters, such as \mathbf{A} .

2.2 LWE and M-LWE

Regev *et al.* introduced the LWE problem [18], which forms the basis for several NIST PQC candidates. As shown in (1), the LWE problem involves recovering the invariant secret vector s from m equations, where fixed $\mathbf{s} \leftarrow \beta_\eta(\mathbb{Z}_q^n)$.

$$(\mathbf{a}_i, b_i = \mathbf{a}_i^\top \mathbf{s} + e_i) \in \mathbb{Z}_q^n \times \mathbb{Z}_q, \quad (1)$$

where $\mathbf{a}_i \leftarrow \mathcal{U}(\mathbb{Z}_q^n)$ and the error vector $e_i \leftarrow \beta_\eta(\mathbb{Z}_q)$. The essence of the M-LWE problem lies in replacing the ring \mathbb{Z}_q in the above LWE problem with the polynomial ring \mathcal{R}_q , and the error distribution is $\beta_\eta(\mathcal{R}_q)$. Thus, an M-LWE sample $(\mathbf{a}_i, b_i) \leftarrow \mathcal{U}(\mathcal{R}_q^{k \times 1} \times \mathcal{R}_q)$ can be represented as:

$$(\mathbf{a}_i, b_i = \mathbf{a}_i^\top \mathbf{s} + e_i) \in \mathcal{R}_q^{k \times 1} \times \mathcal{R}_q, \quad (2)$$

where $\mathbf{a}_i \leftarrow \mathcal{U}(\mathcal{R}_q^{k \times 1})$ and the error vector $e_i \leftarrow \beta_\eta(\mathcal{R}_q)$. Thus, a set of m M-LWE samples can be integrated as:

$$(\mathbf{A}, \mathbf{b} = \mathbf{As} + \mathbf{e}) \in \mathcal{R}_q^{m \times k} \times \mathcal{R}_q^m. \quad (3)$$

2.3 NTT in CRYSTALS-Kyber

Kyber is the only standardized KEM of PQC algorithms established by NIST in the third round [19] and is built on the M-LWE problem. It offers three NIST security levels: Kyber512 corresponding to Level 1, Kyber768 to Level 3, and Kyber1024 to Level 5. The specific parameters are shown in Table 1.

The public-key encryption (PKE) scheme involved in KEM of Kyber consists of three stages: key generation, encryption, and decryption. In the key generation stage, the public key pk is constructed as $\mathbf{As} + \mathbf{e}$, where \mathbf{A} is the sampling polynomial matrix. \mathbf{s} and \mathbf{e} are the secret key and noise, respectively, both of which are polynomial vectors sampled from the β_{η_1} . During the encryption stage, the message m is encrypted into ciphertext c , where c is formed by compressing a polynomial vector u and an array v and concatenating them. In the decryption stage, the receiver extracts u and v from the ciphertext c , and then utilizes \mathbf{s} to perform corresponding operations to recover the message m . Algorithm 1 illustrates the decryption process of Kyber. The KEM protocol is an extension of the PKE protocol with re-encryption. The application

Algorithm 1 Kyber.CPAPKE.Dec(sk, c):decryption

Input: Secret key $sk \in \mathcal{B}^{12 \cdot k \cdot n/8}$
Input: Ciphertext $c = (u, v) \in \mathcal{B}^{d_u \cdot k \cdot n/8 + d_v \cdot n/8}$
Output: Message $m \in \mathcal{B}^{32}$

- 1: $u := \text{Decompress}_q(\text{Decode}_{d_u}(c), d_u)$
- 2: $v := \text{Decompress}_q(\text{Decode}_{d_v}(c + d_u \cdot k \cdot n/8), d_v)$
- 3: $\hat{s} := \text{Decode}_{12}(sk)$
- 4: $m := \text{Encode}_1(\text{Compress}_q(v - \text{INTT}(\hat{s}^T \circ \text{NTT}(u))), 1)$
- 5: **return** m

of the Fujisaki-Okamoto transformation [20] to an IND-CPA-secure PKE results in an IND-CCA2-secure KEM.

In Kyber, polynomial multiplication is a fundamental operation that is frequently used in the encryption and decryption processes. By performing multiplication calculations on the polynomial converted to the NTT domain, the polynomial multiplication on NTT can reduce the computational complexity from $O(N^2)$ to $O(N \log N)$, thus accelerating the speed of the entire encryption and decryption process. Note that for Kyber, here is only 256th primitive root of unity ξ instead of 512th. Therefore, the modulus $x^n + 1$ in Kyber can only be partially factored into $n/2$ quadratic polynomials, with odd and even coefficients calculated respectively. It is also considered that NTT is a linear transformation, the specific formula is described as follows:

$$\left\{ \begin{array}{l} \hat{f}_i = \sum_{j=0}^{127} f_{2j} \xi^{(2br(i)+1)j} \Rightarrow [\hat{f}_i]^T = M[f_{2i}]^T, \\ \hat{f}_{2i+1} = \sum_{j=0}^{127} f_{2j+1} \xi^{(2br(i)+1)j} \Rightarrow [\hat{f}_{2i+1}]^T = M[f_{2i+1}]^T, \end{array} \right. \quad (4)$$

where $br(i)$ represents a 7-bit bit-reversal of i and $M_{n \times n}$ is a reduced integer matrix. Similarly, INTT can be represented in the same way.

2.4 Correlation Power Analysis Attack

SCAs on cryptographic devices can be broadly categorized into invasive, non-invasive, and semi-invasive attacks. Non-invasive attacks, such as the CPA attack, can compromise secret keys without disrupting the operation of the cryptographic devices. In the following, we will delve into the principles and steps involved in CPA attack in summary.

In practical SCAs, physical phenomena such as the power consumption and the electromagnetic radiation are often observed [21]. The CPA attack is a widely used method in SCAs, which relies on the correlation between power models such as HW or Hamming distance (HD) and actual power consumption [22]. The higher the correlation guess, the greater the likelihood that the key with higher correlation guess is the correct one. A traditional CPA attack can generally be divided into four steps.

Firstly, select an intermediate value $f(d, k)$ computed by the device's encryption algorithm as the attack point, where d is a known partial ciphertext or message and k is a partial key. Secondly, measure the actual power consumption of the device. When the device encrypts or decrypts D different messages or ciphertexts, we record the actual power consumption $T_{D \times T}$, where T_{ij} denotes the power consumption of the i^{th} plaintext or ciphertext at time

j . Thirdly, calculate the hypothetical intermediate values and map them to the real power consumption. The hypothesis intermediate $V = [f(d_i, gk_j)]_{D \times K}$ is computed for all guess keys gk and mapped to the power consumption $H_{D \times K}$. Finally, calculate the Pearson correlation coefficient (PCC) between T and H to obtain the correlation coefficient matrix $P_{K \times T}$. According to the largest value in $|P|$, we determine the correct part of the private key k_c and time. The full secret key can be recovered by repeating the above procedure for each partial secret key.

2.5 Kendall's Rank Correlation Coefficient

The Kendall's tau is a non-parametric measure of the association between two random variables. It quantifies the degree of concordance in the rankings of two variables, *i.e.*, whether they are consistently ranked in terms of their values [23]. Kendall's tau τ ranges from -1 to 1 , where $\tau = 1$ indicates a perfect direct association, $\tau = -1$ indicates a perfect disassociation, and $\tau = 0$ indicates no agreement in rankings between the two variables.

$$\left\{ \begin{array}{l} \tau_a = \frac{c - d}{\frac{1}{2}n(n - 1)}, \\ \tau_b = \frac{c - d}{\sqrt{(c + d + t_x)(c + d + t_y)}}, \end{array} \right. \quad (5)$$

where c and d denote the numbers of concordant and discordant pairs, while t_x and t_y represent the counts of tied ranks in the x and y data sets, respectively.

Listing 1: Base multiplication in Kyber.

```

1 void basemul(int16_t r[2],
2               int16_t zeta,
3               const int16_t s[2],
4               const int16_t u[2])
5 {
6     r[0] = fqmul(s[1], u[1]);
7     r[0] = fqmul(r[0], zeta);
8     r[0] += fqmul(s[0], u[0]);
9     r[1] = fqmul(s[0], u[1]);
10    r[1] += fqmul(s[1], u[0]);
11 }
```

3 PROPOSED IMPROVED TWO-STEP ATTACK

It should be remarked that the proposed improved two-step attack is illustrated in Fig. 1. We will detail the basis of the attack analysis and our proposed three improvements in the following.

3.1 Basis of Attack Analysis

The goal of this paper is to explore the physical security of Kyber KEM under random-ciphertext CPA attack. The purpose of the attack is to obtain a long-term secret key. We assume that an attacker has access to a device which is running Kyber decryption and can enter arbitrary ciphertext into the device. In addition, they can also capture the electromagnetic radiation of the device to obtain the power traces.

In subsection 2.3, we have introduced NTT used in Kyber briefly, which only possesses n_{th} roots of unity because the modulus polynomial $(x^n + 1)$ can only be factored into $n/2$ linear polynomials. Consequently, multiplication involves the multiplication of linear polynomials rather than simple point-wise multiplication in the

NTT domain. Due to the properties of incomplete NTT in Kyber, the full secret key of Kyber can be divided into $2k$ ($k = 2, 3, 4$) groups.

The test vector leakage assessment (TVLA) methodology can be used to find side-channel leakage points and the t-test method is one of the commonly used methods in TVLA [24]. Several t-test results from previous works have indicated the potential leakage points during the decryption process in Kyber [16, 25]. One critical side-channel leakage occurs during the point-wise multiplication of $\hat{s} \circ \hat{u}$. Additionally, this operation takes place in the quotient ring $\mathbb{Z}_q[x]/(x^2 - \xi)$. In the clean implementation of pqm4 [26], polynomial multiplication employs 256 *basemuls* in Kyber512. Moreover, each calculation of *basemul* is independent from the others.

From Listing 1, we can observe that there are two steps related to the partial secret key coefficient s_0 and three steps related to the partial secret key coefficient s_1 . The inputs of a *basemul* are s_0 , s_1 , u_0 , and u_1 , and outputs are r_0 and r_1 . Five multiplications and two additions are involved in the listing. Obviously, the result is related to two secret key coefficients. All partial secret key coefficients range from (0, 3328) for Kyber. In a practical CPA attack, suppose that the attacker aims to recover the coefficient s_0 , r_0 can be selected as the intermediate value. Similarly, if the attacker aims to recover the coefficient s_1 , r_1 can be selected as the intermediate value. In addition, in order to recover the full secret key coefficients of a group, the attacker would need to perform 128 CPA attacks. Therefore, $128 \times 2k$ CPA attacks are required for the full secret key.

Listing 2: Modified HW in the CPA Attack.

```

1 def HW(r0):
2     if r0 < 0:
3         r0 = calculate_complement(r0, 16)
4         H_W = r0.count("1")
5     else:
6         H_W = bin(r0).count("1")
7     return H_W
8
9 def calculate_complement(r0, 16):

```

3.2 Modified Leakage Model for CPA

Modeling the power leakage is the basis for a CPA attack, and its accuracy directly determines the success rate of the attack. HW model counts the number of "1" in intermediate values, which is one of the most representative linear power models. Similarly, HD model records the amount of "1" → "0" or "0" → "1" transitions as power leakage. The difference of HW and HD model is given as:

$$HD(r_0, s_1) = HW(r_0 \oplus s_1). \quad (6)$$

Typically, when simulating the energy consumption of a microprocessor, the HW model is commonly employed [27], as is the case in this particular study.

The arithmetic logic units (ALUs) and multiplier units (MU) in ARM processors are often optimized for two's complement operations. Most arithmetic and logical instructions in the processor's instruction set are designed based on two's complement calculations. Therefore, we fine-tune the HW power leakage model according to this property to directly avoid the complementary false positive. We compute the HW of the complement of the intermediate instead of directly computing the HW of the intermediate, as shown in Listing 2, where the function *calculate_complement* computes the 16bit complement. The modified power leakage model can map

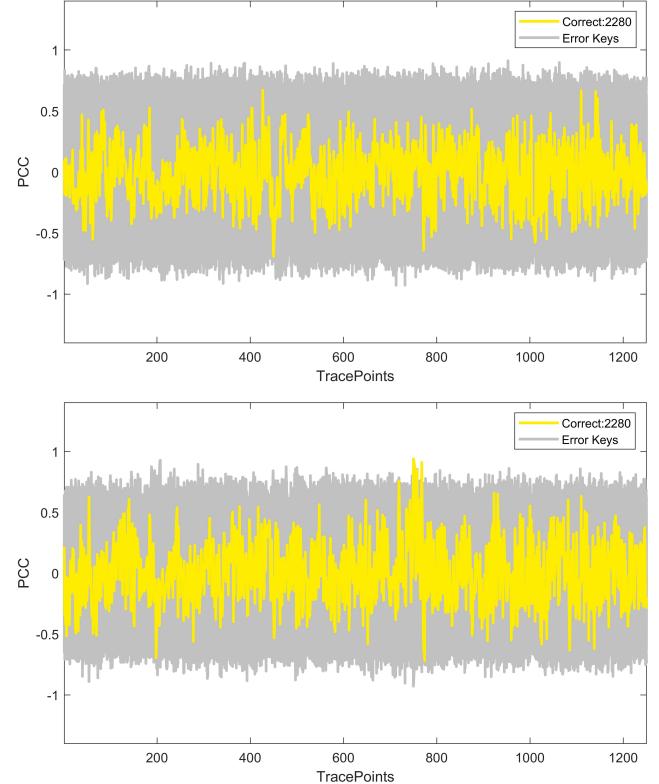


Figure 2: When $D = 15$ during a *basemul* call, PCC values for all guessed keys of the original HW model (top) and the modified HW model (bottom).

to the hypothetical power consumption values more accurately, thus reducing the number of power traces required for CPA attacks. As shown in Fig. 2, correct secret key coefficient in the original HW leakage model is drowned in all the guessed key coefficients, while the coefficient can be picked out in the modified model effectively by using a small number of 15 power traces.

3.3 Optional Kendall's tau for CPA

The goal of this improvement is to find the correct key coefficients using 15 or even fewer power traces while ensuring the efficiency and success rate of the attack. In scenarios where the number of power traces is limited, the calculated PCC value across all guessed keys tends to be exceptionally high. Consequently, it becomes challenging to accurately recover even a portion of the secret key coefficients using solely the traditional CPA attack, and attempting to reconstruct 128 or the entire set of secret key coefficients becomes even more daunting.

Our solution is as follows. After computing the PCC correlation matrix for each *basemul*, we set the threshold to 0.9 or even higher, adjusting it based on the values of P . For each *basemul*, if there are more than f correlations exceeding the threshold, we consider them as candidate coefficients $k_h = (k_{h_0}, \dots, k_{h_{f-1}})$. We then map the hypothetical intermediate values of the f candidate coefficients to candidate hypothetical power consumption value

matrix $\mathbf{H}'_{D \times f}$. Next, we calculate the Kendall's tau between the hypothetical power value matrix \mathbf{H}' and the actual power matrix \mathbf{T} . For each column of \mathbf{H}' , we compute the Kendall's tau with each column of the actual power matrix. Finally, we obtain a $f \times T$ Kendall coefficient matrix \mathbf{K}_d , from which we select the candidate key with the highest correlation coefficient as the correct key coefficient for that *basemul*. On the other hand, we skip the cases that have higher PCC correlations and smaller candidates.

PCC is used in the traditional CPA attack to calculate only the linear correlation between the actual power consumption and the hypothetical power consumption, which is not sufficient. With only a few power traces, it is possible to directly select some of the correct key coefficients even if only Kendall's tau is calculated, but the calculation time of Kendall's tau is $12\times$ longer than that of PCC. Therefore we combine Kendall's tau with PCC. After calculating PCC, the guessed keys coefficient exceeding a certain threshold is selected as the coefficients of candidate keys. Then, the Kendall's tau values of these coefficients of candidate keys are calculated so that the coefficient with the higher value is accepted. In this way, false positives can be quickly eliminated.

3.4 Trail-and-Error Lattice Attack after CPA

As mentioned earlier, each group of the secret key consists of 128 secret key coefficients including 128 even-index coefficients or 128 odd-index coefficients. As introduced in [17], suppose that an attacker wants to exploit the side-channel leakage point $\hat{\mathbf{s}} \circ \hat{\mathbf{u}}$ and has successfully recovered sr coefficients out of a group of 128 secret key coefficients $\hat{\mathbf{s}}_i$, while the remaining $128 - sr$ coefficients are unsuccessfully recovered.

Let $I_a = (a_0, \dots, a_{sr-1})$ denote the recovered coefficients indices, and $I_b = (b_0, \dots, b_{127-sr})$ represent the indices of coefficients that have failed to be recovered, i.e., the unknown coefficients. $\text{INTT}(\hat{\mathbf{s}}_i) = N\hat{\mathbf{s}}_i = \mathbf{s}_i \bmod q$ can be rewritten as $N_A \hat{\mathbf{s}}_{iA} + N_B \hat{\mathbf{s}}_{iB} = \mathbf{s}_i \bmod q$ [17], where matrix $N_A = [\mathbf{n}_{a_0}, \dots, \mathbf{n}_{a_{sr-1}}]$ consists of columns in matrix N corresponding to the indices I_c , while $\hat{\mathbf{s}}_{iA} = [\hat{s}_{a_0}, \dots, \hat{s}_{a_{sr-1}}]^\top$ represents the vector composed of successfully recovered coefficients. Similarly, $N_B = [\mathbf{n}_{b_0}, \dots, \mathbf{n}_{b_{127-sr}}]$, and $\hat{\mathbf{s}}_{iB} = [\hat{s}_{b_0}, \dots, \hat{s}_{b_{127-sr}}]^\top$.

In the above formulas, both N_A and $\hat{\mathbf{s}}_{iA}$ are known. Let $\mathbf{t} = N_A \hat{\mathbf{s}}_{iA}$, $\mathbf{A} = -N_B$, and $\mathbf{s}' = \hat{\mathbf{s}}_{iB}$. Then, we obtain $\mathbf{t} = \mathbf{A} \cdot \mathbf{s}' + \mathbf{s}_i \bmod q$. This conveniently forms a low-dimension LWE problem, which is simpler compared to the original problem in Kyber because the rank of \mathbf{A} is smaller. We firstly view it as a bounded distance decoding (BDD)/unique shortest vector problem (uSVP) lattice problem, and specific algorithm to solve the updated LWE problem is given by Algorithm 2 [28], where the matrixs \mathbf{BDD} and \mathbf{B}_{kan} are summarized as follows:

$$\mathbf{BDD} = \begin{bmatrix} I_{sr} & \mathbf{A}' \\ \mathbf{0} & qI_{n-sr} \end{bmatrix}, \quad (7)$$

$$\mathbf{B}_{kan} = \begin{bmatrix} I_{sr} & \mathbf{A}' & \mathbf{0} \\ \mathbf{0} & qI_{n-sr} & \mathbf{0} \\ \mathbf{t}^\top & \mathbf{0} & 1 \end{bmatrix}. \quad (8)$$

$[I_{sr} | \mathbf{A}']$ is a reduced row echelon matrix of \mathbf{A} transpose. This process yields the shortest vector containing the error vector \mathbf{s}_i^\top , denoted as $\mathbf{w} = [\mathbf{s}_i^\top | 1]$. Finally, We obtain the actual secret key with a length of 128 as shown in Step 3 of Algorithm 2.

Algorithm 2 Kannan's embedding technique.

Input: An LWE instance $\mathbf{t} = \mathbf{A}\mathbf{s} + \mathbf{s}_i \bmod q$
Output: the short error vector $\mathbf{s}_i \in \mathcal{R}_q^{128}$

- 1: Construct the lattice $\Lambda(\mathbf{BDD})$ generated by matrix \mathbf{BDD} ;
- 2: Reduce BDD to the SVP problem by rescaling \mathbf{BDD} to the basis matrix \mathbf{B}_{kan} ;
- 3: Use lattice algorithm (LLL or BKZ) to derive the short vector $\mathbf{w} = [\mathbf{s}_i^\top | 1]$ from \mathbf{B}_{kan} ;
- 4: **return** \mathbf{s}_i

But it is worth noting that the norm of vector \mathbf{w} is $\sqrt{\|\mathbf{s}_i\|^2 + 1} \approx \sqrt{n}\sigma_s$, which must be less than the norm of the shortest vector estimated by the Gaussian heuristic for the uSVP problem to be solved. For Kyber512, when $sr \geq 39$, it is possible to correctly recover the length of 128 odd/even index coefficients through lattice attack. For Kyber768/1024, when $sr \geq 38$, the corresponding coefficients can be correctly recovered. In other words, the lattice attack can tolerate at most 89/90 recovered incorrect secret key coefficients for Kyber512 and Kyber768/1024 respectively, where 38/39 of the coefficient are randomly selected from 128 recovery coefficients.

We elaborate on the theoretical principles of the lattice attack, which provides a fault-tolerant for recovering the full set of 128 keys. Leveraging this method, we propose a more flexible and versatile approach for its application. The proposed trail-and-error lattice attack is shown in Listing 3, where n represents the number of CPA attacks, and \mathbb{M} and $count$ denote the NTT linear matrix form of Kyber and the number of trails, respectively.

Listing 3: Trail-and-Error Lattice Attack.

```

1 index = [1, 2, ..., 37, 38]
2 other_index = [39, 40, ..., n-2, n-1]
3 guess_sk = [sk_bu0, ..., sk_bu38]
4 other_sk = [sk_bu39, ..., sk_bu(n-1)]
5 ken = [k_bu0, ..., k_bu38]
6 other_ken = [k_bu39, ..., k_bu(n-1)]
7
8 result = Lattice_attack(index, guess_sk)
9 result = ( $\mathbb{M}$  @ result)
10 if guess_sk == [result[j] for j in index]:
11     return result
12 else:
13     for i in count:
14         update_index(index)
15         update_sk(guess_sk)
16         result = Lattice_attack(index, guess_sk)
17         result = ( $\mathbb{M}$  @ result)
18         result_target = [result[j] for j in index]
19         if guess_sk == result_target:
20             return result
21             break
22
23 def Lattice_attack(a, b):
24     def update_index():
25         def update_sk():

```

One of the benefits of using the proposed method is that in order to recover a set of key coefficients, we can use a minimum of 38/39 CPA attacks instead of 128 CPA attacks. Certainly, the more CPA attacks are carried out, the higher the success rate of this method will be, but its efficiency will also slow down. The one with the smallest correlation among the 38/39 key coefficients is replaced by other key coefficients with higher correlation than it in a trail-and-error method. It is worth noting that it is necessary to set the



Figure 3: The experimental equipment.

appropriate parameters of lattice attack; otherwise, it may take too long in a trail and lead to the overall recovery inefficient.

For Kyber512, Kyber768, and Kyber1024, 4, 6, and 8 iterations are needed to recover the full secret key, respectively. Since even-indexed coefficients do not affect odd-indexed coefficients and coefficients within each group do not affect each other, the above method can be parallelized to compute the corresponding coefficients concurrently.

4 EXPERIMENTS

4.1 Experimental Setup

Our attacks are equally successful for different security levels of Kyber because they use the same *basemul*, whose algorithm is provided by Listing 1. For simplicity, we only take Kyber512 into consideration in the following. We run the reference implementation of Kyber512 from the pqm4 with -o compilation optimization on the STM32F407-DISCOVERY, an ARM Cortex-M4 microcontroller, at 48MHz. We capture the power traces using a Pico 3043D oscilloscope and a CYBERTEK EM5030-2 electromagnetic probe. The sampling rate is set to 500 MSa/s. The experimental equipment is shown in Fig. 3.

According to the introduction in Section 2.4 that the selection of the intermediate value of CPA attack should be related to the secret key, combined with the analysis mentioned in Section 3.1, we choose $f_{qmul}(k, u_1)$ as the intermediate value of our attack, and all the intermediate values in the following experiments are the same values.

4.2 Experiment Results

Step1: CPA Attack. As aforementioned, the CPA attack is divided into two stages: the capturing stage and the modeling computation stage. Our optimizations are mainly focus on the latter stage, including modifying the leakage model and adding an optional Kendall's tau computing following the PCC computing.

For the capturing stage, as introduced in Section 3.1, we carry out the CPA attack at the NTT operation which calls *basemul* functions 128 times. In our CPA experiments, we input random ciphertexts and capture tremendous electromagnetic radiations during those calls.

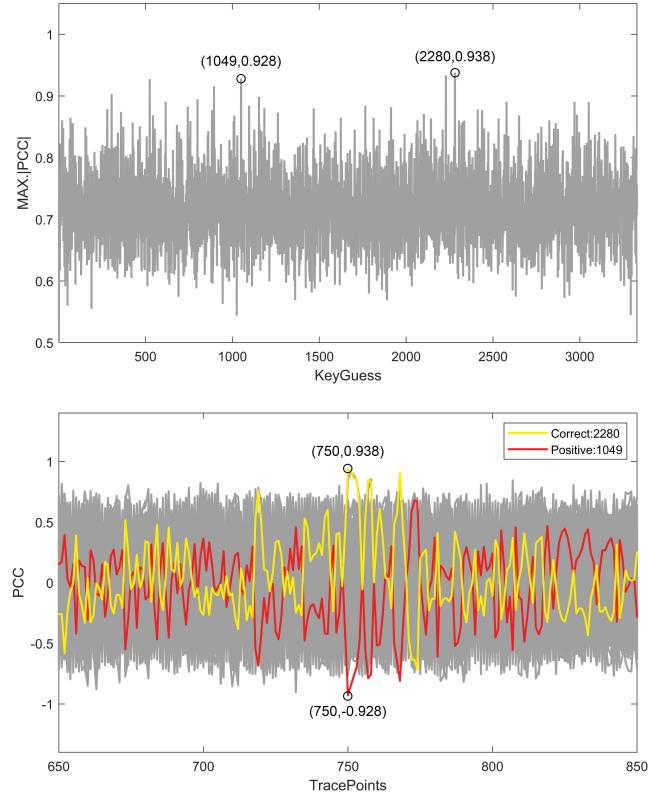


Figure 4: When $D = 15$, the PCC results during a certain *basemul* call.

To show the effectiveness of the modified leakage model in the modeling computation stage, we have implemented two experiments. The first one is shown in Fig. 2 of Section 3.2 and we can see that the new model can reinforce the PCC value of the correct key. The second one shown in the following is to demonstrate its superiority in identifying the complementary false positive.

When the number of random ciphertexts D is set to 15, the relationship of the maximum absolute values $|PCC|$ to the guess keys is shown in the above of Fig. 4. We can directly pick out the correct key 2280 and its complementary false positive 1049 (equal to $3329 - 2280$). This is a general phenomenon. As mentioned in [17], the attacker would run into some problems because the correct coefficient s_0 and its complementary value $q - s_0$ both would have high PCC values since $HW(s_0)$ and $HW(q - s_0)$ are highly correlated. So, we have modified the leakage model as described in Section 3.2 to escape such false positive. The relationship of the PCC values to the trace points is shown in the bottom of Fig. 4, where there are 3329 curves and the yellow and red curves present whose guess keys are 2280 and 1049, respectively. It can be seen that the maximum absolute value of PCC of the complementary false positive has a negative sign. We can only focus on the positive PCCs to avoid such false positive.

We briefly explain the reason of this phenomenon in the following. Let s_0 be the correct one. Then $s'_0 = 3329 - s_0$ represents the false positive. The f_{qmul} function in *basemul* is an operation

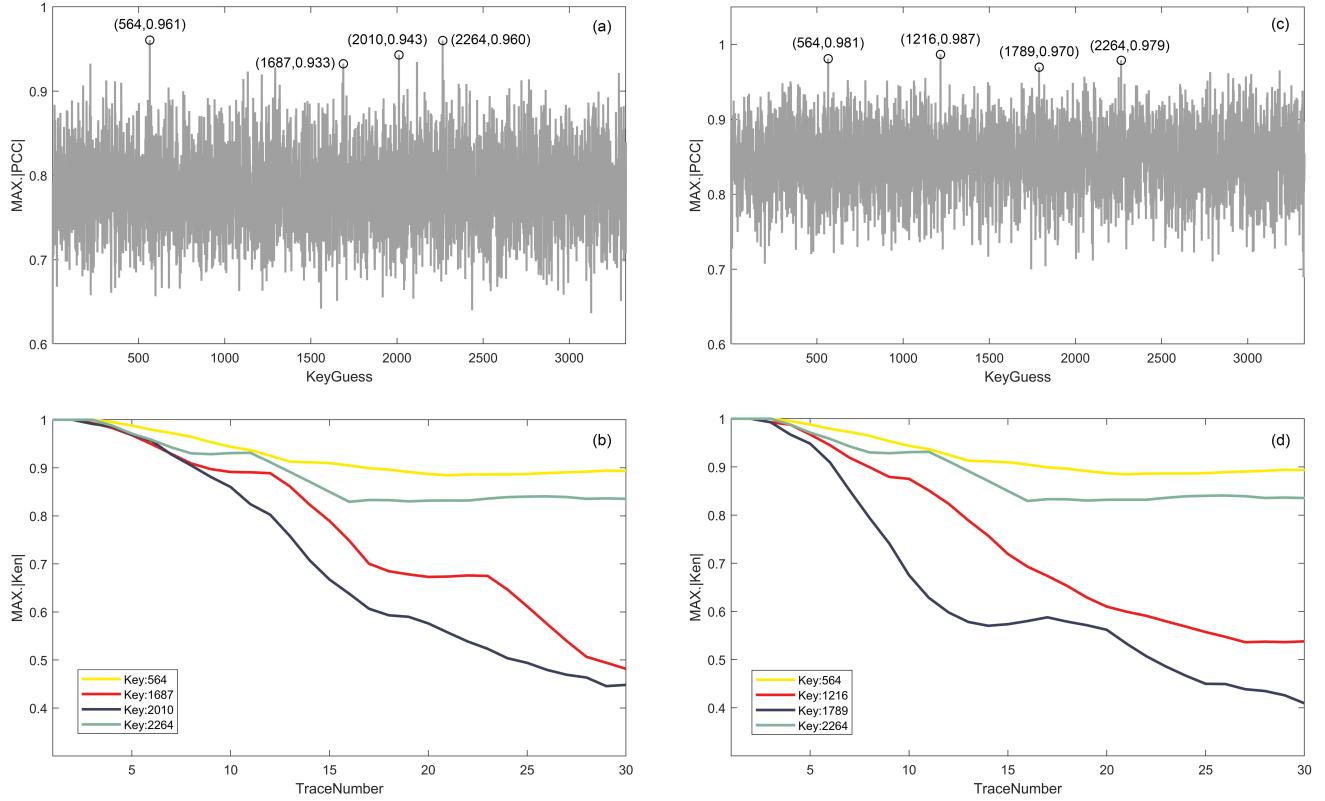


Figure 5: When $D = 15$, the PCC results (a) and Ken results (b) in a certain *basemul*. When $D = 11$, the PCC results (c) and Ken results (d) in the same *basemul*.

that multiplies two numbers and then is reduced by 3329 in Kyber. The intermediate values for the two guessed key coefficients are summarized as follows:

$$r_1 = \text{fmul}(s_0, u_1) = (s_0 \times u_1) \bmod q, \quad (9)$$

$$\begin{aligned} r'_1 &= \text{fmul}(s'_0, u_1) = ((3329 - s_0) \times u_1) \bmod q \\ &= -(s_0 \times u_1) \bmod q. \end{aligned} \quad (10)$$

Hypothetical power consumption values $MHW(r_1)$ and $MHW(r'_1)$ exhibit a negative correlation, while correct $MHW(r_1)$ will naturally exhibit a positive correlation. Obviously, we can figure them out by taking their signs into consideration.

To further improve the accuracy in the CPA step, we adopt the Kendall's tau to the picked candidates after the PCC process. Figure 5 (a) shows the points of the maximum absolute PCC results to the guess keys during another *basemul* call, where $D = 15$ and the number of candidates f after PCC is equal to 4. It can be seen that the correlations of four coefficients 564, 1687, 2010, and 2264 stand out from the crowd of guessed coefficients when setting the threshold to 0.930 and their correlation values are very close. Very close correlations can lead to an inability to distinguish the correct coefficient. This is an another kind of false positives. If the attacker just picks one of these four at random, the accuracy is only about 25%, which is still regarded as a failure. Therefore, we use the method mentioned in Section 3.3 to compensate for such case. First of all, we compute the Kendall coefficient matrix

of these four candidate coefficients. It should be noted that the time for this computation is negligible when comparing to the complete PCC computing. Figure 5 (b) shows the points of the four maximum absolute values $|Kendall's\ tau|$ to the numbers of power traces. It shows that Kendall's tau expands the differences between correct coefficient and false positives. As the number of power traces increases, the value of correct coefficient tends to be more stable while those of false positives decrease quickly. We can easily distinguish the correct key 564 when the number of power traces equals 15 and output it as the final result. In another word, an attacker can take the correct coefficient 564 for this *basemul* call using only 15 power traces. Similarly, we reduce the number of power traces to 11 step by step and implement the PCC and Kendall's tau computations. The corresponding results are shown in Fig. 5 (c) and (d). It can be seen that the correct key 564 can almost not be recognized. We can pick out the final correct candidate from those four candidates according to the results of the summations of their two kinds of corrections. Note that if we continue reducing the number of power traces, we cannot figure it out any more.

Step2: Trail-and-Error Lattice Attack. We conduct the trail-and-error lattice attack on a sixteen-thread server. The parameter of the *block size* in the BKZ reduction is set to 50 and the value of *max_loops* to 8. We collect the CPAs of the first sixty *basemuls* calls.

Figure 6 shows the relationships of the success rate and time to the number of power traces representing in the blue curve and groups of histograms, respectively. The success rate is evaluated by repeatedly conducting the proposed attack many times and counting the success times. It can be seen that when the number of power traces is no less than 15, all the experimental attacks are successful. Those cases with traces number smaller than 15 can be compensated to some degree by running more trials of the lattice attack. Meanwhile, according to the decomposed time histograms in Fig. 6, the time of the proposed lattice attack heavily relies on the number of power traces, while the CPA attack is almost unchanged although the traces number is doubled. The main reason could be the different utilization ratios of the multi-threading server. Note that the CPA computations are independently executed with the different power traces while the trail computations of the lattice attack are executed in serial.

Therefore, we can summarize that when the success rate is large enough (close to 1), we can only cost 15 power traces for a guess/call and about 9 minutes to recover the full key on Kyber512. So, the total number of required power traces is $15 \times 60 = 900$, much smaller than that of the state-of-the-art random ciphertext CPA [16] which requires $20 \times 128 = 2560$ power traces. If we slightly increasing the traces number of the guess, the required time can be reduced close to 5 minutes, much faster than the recorded 20 minutes reported in [17].

5 CONCLUSION

In this paper, we propose an efficient two-step attack including an enhanced CPA attack and a trail-and-error lattice attack for Kyber. In the CPA step, we modify the power leakage model to be more suitable for ARM Cortex-M4 architecture and further filter the candidate keys from the PCC results by using the Kendall's rank correlation coefficient. The accuracy of finding the correct key is significantly improved. In the lattice step, we construct a trail-and-error algorithm and dynamically compute the lattice attack to reduce the power traces and time. Experimental results show that our proposed attack can accurately recover the full secret key of Kyber512 in about 9 minutes with about 15 power traces of a guess on a machine with sixteen threads. Because the *basemul* function called by different security levels of Kyber is the same, our work can be directly applied to the other parameters. Moreover, the core idea of the proposed attack is a general methodology and can be easily extended to other lattice-based cryptography.

ACKNOWLEDGMENTS

This work was supported in part by the National Natural Science Foundation of China under Grant 62104097, in part by the Key Research Plan of Jiangsu Province of China under Grant BE2022098, and in part by the Young Elite Scientists Sponsorship Program by CAST under Grant 2023QNRC001.

REFERENCES

- [1] Ronald L Rivest, Adi Shamir, and Leonard Adleman. A Method for Obtaining Digital Signatures and Public-Key Cryptosystems. *Communications of the ACM*, 21(2):120–126, 1978.
- [2] Neal Koblitz. Elliptic Curve Cryptosystems. *Mathematics of computation*, 48(177):203–209, 1987.
- [3] Peter W Shor. Algorithms for Quantum Computation: Discrete Logarithms and Factoring. In *Proceedings 35th annual symposium on foundations of computer science*, pages 124–134. Ieee, 1994.
- [4] Roberto Avanzi, Joppe Bos, Léo Ducas, Eike Kiltz, Tancrède Lepoint, Vadim Lyubashevsky, John M Schanck, Peter Schwabe, Gregor Seiler, and Damien Stehlé. CRYSTALS-Kyber Algorithm Specifications And Supporting Documentation. 2017.
- [5] Gorjan Alagic, Gorjan Alagic, Daniel Apon, David Cooper, Quynh Dang, Thinh Dang, John Kelsey, Jacob Lichtinger, Yi-Kai Liu, Carl Miller, et al. Status Report on the Third Round of the NIST Post-Quantum Cryptography Standardization Process. 2022.
- [6] Joppe Bos, Léo Ducas, Eike Kiltz, Tancrède Lepoint, Vadim Lyubashevsky, John M Schanck, Peter Schwabe, Gregor Seiler, and Damien Stehlé. CRYSTALS-Kyber: A CCA-Secure Module-Lattice-Based KEM. In *2018 IEEE European Symposium on Security and Privacy (EuroS&P)*, pages 353–367. IEEE, 2018.
- [7] Roberto Avanzi, Joppe Bos, Léo Ducas, Eike Kiltz, Tancrède Lepoint, Vadim Lyubashevsky, John M Schanck, Peter Schwabe, Gregor Seiler, and Damien Stehlé. CRYSTALS-Kyber Algorithm Specifications And Supporting Documentation. *NIST PQC Round*, 2(4):1–43, 2019.
- [8] Paul C Kocher. Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS, and Other Systems. In *Advances in Cryptology—CRYPTO’96: 16th Annual International Cryptology Conference Santa Barbara, California, USA August 18–22, 1996 Proceedings 16*, pages 104–113. Springer, 1996.
- [9] Zhuang Xu, Owen Pemberton, Sujoy Sinha Roy, David Oswald, Wang Yao, and Zhiming Zheng. Magnifying Side-Channel Leakage of Lattice-Based Cryptosystems with Chosen Ciphertexts: The Case Study of Kyber. *IEEE Transactions on Computers*, 71(9):2163–2176, 2021.
- [10] Suresh Chari, Josyula R Rao, and Pankaj Rohatgi. Template Attacks. In *Cryptographic hardware and embedded systems—CHES 2002: 4th International Workshop Redwood Shores, CA, USA, August 13–15, 2002 Revised Selected Papers 4*, pages 13–28. Springer, 2003.
- [11] Omar Choudary and Markus G Kuhn. Efficient Template Attacks. In *Smart Card Research and Advanced Applications: 12th International Conference, CARDIS 2013, Berlin, Germany, November 27–29, 2013. Revised Selected Papers 12*, pages 253–270. Springer, 2014.
- [12] Jianan Mu, Yixuan Zhao, Zongyue Wang, Jing Ye, Junfeng Fan, Shuai Chen, Huawei Li, Xiaowei Li, and Yuan Cao. A Voltage Template Attack on the Modular Polynomial Subtraction in Kyber. In *2022 27th Asia and South Pacific Design Automation Conference (ASP-DAC)*, pages 672–677. IEEE, 2022.
- [13] Prasanna Ravi, Sujoy Sinha Roy, Anupam Chattopadhyay, and Shivam Bhasin. Generic Side-Channel Attacks on CCA-Secure Lattice-Based PKE and KEMs. *IACR transactions on cryptographic hardware and embedded systems*, pages 307–335, 2020.
- [14] Rei Ueno, Keita Xagawa, Yutaro Tanaka, Akira Ito, Junko Takahashi, and Naofumi Homma. Curse of Re-Encryption: A Generic Power/EM Analysis on Post-Quantum KEMs. *IACR Transactions on Cryptographic Hardware and Embedded Systems*, pages 296–322, 2022.
- [15] Muyan Shen, Chi Cheng, Xiaohan Zhang, Qian Guo, and Tao Jiang. Find the Bad Apples: An Efficient Method for Perfect Key Recovery under Imperfect SCA Oracles—A Case Study of Kyber. *IACR Transactions on Cryptographic Hardware and Embedded Systems*, pages 89–112, 2023.
- [16] Yipei Yang, Zongyue Wang, Jing Ye, Junfeng Fan, Shuai Chen, Huawei Li, Xiaowei Li, and Yuan Cao. Chosen Ciphertext Correlation Power Analysis on Kyber. *Integration*, 91:10–22, 2023.
- [17] Yen-Ting Kuo and Atsushi Takayasu. A Lattice Attack on CRYSTALS-Kyber with Correlation Power Analysis. In *International Conference on Information Security*

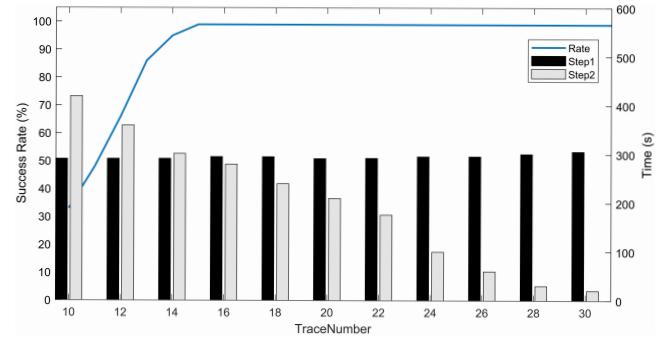


Figure 6: The success rate and efficiency of our attack in twenty experiments.

- and Cryptology}, pages 202–220. Springer, 2023.
- [18] Oded Regev. On Lattices, Learning with Errors, Random Linear Codes, and Cryptography. *Journal of the ACM (JACM)*, 56(6):1–40, 2009.
 - [19] Dustin Moody. Nist Status Update on the 3rd Round. *Cryptography Technology Group, National Institute of Standards and Technology*, 2021.
 - [20] Eiichiro Fujisaki and Tatsuaki Okamoto. How to Enhance the Security of Public-Key Encryption at Minimum Cost. In *International Workshop on Public Key Cryptography*, pages 53–68. Springer, 1999.
 - [21] Ingrid Verbauwhede. *Secure Integrated Circuits and Systems*. Springer, 2010.
 - [22] G Joy Persial, M Prabhu, and R Shanmugalakshmi. Side Channel Attack-Survey. *Int. J. Adv. Sci. Res. Rev.*, 1(4):54–57, 2011.
 - [23] Hervé Abdi. The Kendall Rank Correlation Coefficient. *Encyclopedia of measurement and statistics*, 2:508–510, 2007.
 - [24] Qianmei Wu, Wei Cheng, Sylvain Guilley, Fan Zhang, and Wei Fu. On Efficient and Secure Code-based Masking: A Pragmatic Evaluation. *IACR Transactions on Cryptographic Hardware and Embedded Systems*, pages 192–222, 2022.
 - [25] Daniel Heinz, Matthias J. Kannwischer, Georg Land, Thomas Pöppelmann, Peter Schwabe, and Amber Sprenkels. First-Order Masked Kyber on ARM Cortex-M4. *Cryptology ePrint Archive*, Paper 2022/058, 2022. <https://eprint.iacr.org/2022/058>.
 - [26] Matthias J Kannwischer, Joost Rijneveld, Peter Schwabe, and Ko Stoffelen. PQM4: Post-Quantum Crypto Library for the ARM Cortex-M4, 2019.
 - [27] Yiqiang Zhao, Shijian Pan, Haocheng Ma, Ya Gao, Xintong Song, Jiaji He, and Yier Jin. Side Channel Security Oriented Evaluation and Protection on Hardware Implementations of Kyber. *IEEE Transactions on Circuits and Systems I: Regular Papers*, 2023.
 - [28] Ravi Kannan. Minkowski’s Convex Body Theorem and Integer Programming. *Mathematics of operations research*, 12(3):415–440, 1987.