Estimating the Effectiveness of Lattice Attacks

Kotaro Abe[1] and Makoto Ikeda[1]

School of Engineering, The University of Tokyo, Tokyo, Japan
[kabe,ikeda]@silicon.t.u-tokyo.ac.jp

Abstract. Lattice attacks are threats to (EC)DSA and have been used in cryptanalysis. In lattice attacks, a few bits of nonce leaks in multiple signatures are sufficient to recover the secret key. Currently, the BKZ algorithm is frequently used as a lattice reduction algorithm for lattice attacks, and there are many reports on the conditions for successful attacks. However, experimental attacks using the BKZ algorithm have only shown results for specific key lengths, and it is not clear how the conditions change as the key length changes.
In this study, we conducted some experiments to simulate lattice attacks on P256, P384, and P521 and confirmed that attacks on P256 with 3 bits nonce leak, P384 with 4 bits nonce leak, and P521 with 5 bits nonce leak are feasible. The result for P521 is a new record. We also investigated in detail the reasons for the failure of the attacks and proposed a model to estimate the feasibility of lattice attacks using the BKZ algorithm. We believe that this model can be used to estimate the effectiveness of lattice attacks when the key length is changed.

Keywords: Lattice Attacks · ECDSA · Hidden Number Problem · BKZ

1 Introduction

Side-channel attacks extract information related to the secret key or the key itself from cryptographic devices. If a cryptographic device is vulnerable to side-channel attacks, the secret key can be easily recovered by cryptanalysis. Thus, cryptographic devices are required to be tolerant of side-channel attacks. To implement secure cryptographic devices, it is necessary to clarify the side-channel attacks that can be achieved. In particular, for devices that generate signatures, such as DSA and ECDSA, lattice attacks[14, 25, 26] and Bleichenbacher's attack[5, 6, 23, 31] are quite effective cryptanalytic techniques. In such attacks, only a few bits of the nonce are required to recover the secret key. These attacks are based on the hidden number problem (HNP), which was introduced by D. Boneh and R. Venkatesan[10].

To recover the secret key of the (EC)DSA, the attacker must perform two attacks. In the first attack, the attacker conducts side-channel attacks to obtain information about some bits of the nonce for multiple signatures. In the second attack, lattice attacks or Bleichenbacher's attack are used to recover the secret key. For the attack to work, the following two conditions must be satisfied:

1. Side-channel attacks can leak some bits of the nonce for multiple signatures.
2. The leaked information via side-channel attacks is sufficient to recover the secret key.

For condition 1 to hold, it is necessary to consider whether there exists a vulnerability to side-channel attacks that can obtain information about the nonce. For example, [22] attacked via timing analysis and [21] attacked via template attacks. Although it is often

difficult for an attacker to leak a large number of nonce bits in many signatures, we assume that the attacker can obtain an arbitrary amount of leakage via side-channel attacks because our goal is to investigate condition 2 in this work.

For condition 2, two types of attacks are possible: lattice attacks and Bleichenbacher's attack. The attacker constructs an HNP from the information obtained via side-channel attacks and uses either type of attack to solve the HNP. Because it is more convenient for the attacker to reduce the amount of leakage in condition 1, the minimum amount of leakage to recover the correct secret key has been investigated (summarized in the next subsection).

The Bleichenbacher attack is based on a Fourier analysis. It can attack with a very small nonce leak, such as only one bit, and it can handle errors, but it requires a large number of signatures. However, lattice attacks require a smaller number of signatures. However, lattice attacks require a certain amount of leakage, and it is difficult to recover the key when errors are included. Lattice attacks are based on the closest vector problem (CVP). In practice, CVP is solved via the nearest plane[7] or Kannan's embedding method[17] and lattice reduction algorithms such as BKZ[29], but it cannot always be solved. If the amount of nonce leak is too small, lattice attacks cannot solve the HNP owing to a lack of constraints.

1.1 Related Works

Many previous studies have attacked (EC)DSA via HNP. To solve HNP, [2, 9, 14, 22] used lattice attacks, and [5, 6, 23, 31] used Bleichenbacher's attack.

To construct an HNP, we need to obtain nonce leakage in multiple signatures, and the leakage positions are assumed to be the most significant bits, the least significant bits, and bits in the middle. In previous studies, nonce leakage of most significant bits or least significant bits was used in lattice attacks, but as mentioned in [25], HNP can be constructed with any position of nonce leakage. According to [25], the number of leaked bits required for a successful attack is one bit more for the most significant bits than for the least significant bits, and twice as much for bits in the middle for the least significant bits.

For lattice attacks on 160-bit DSA, [20] succeeded with 2 bits nonce leakage. For 256-bit (EC)DSA, [22, 27] succeeded with 4 bits nonce leakage, [4, 13] succeeded with three or more bit nonce leakages, and [19] succeeded with 3 bits nonce leakage. For 384-bit ECDSA, [3] succeeded with 4 bits nonce leakage. Recently, [2] proposed a new method based on sieving and enumeration with predicates and showed that 160, 192, 256, 384, and 521-bit ECDSA can be attacked with 2, 2, 3, 4, and 6 bits nonce leakage, respectively. More recently, [30] estimated some bits of nonce or the secret key and attacked 160,256,384-bit ECDSA with 2,3,4 bit nonce leakage using a large number of signatures.

Lattice attacks usually require less than or around 100 signatures, whereas Bleichenbacher's attack requires a large number of them. [6] broke 163-bit ECDSA with 1 bit nonce leakage for about 2^{23} signatures and 192-bit ECDSA with 1 bit nonce leakage for about 2^{29} signatures via Bleichenbacher's attack. For a longer key length, [31] broke a 256-bit ECDSA with 2 bits nonce leak for approximately 2^{26} signatures.

1.2 Contributions

To confirm the effectiveness of lattice attacks experimentally, we conducted lattice attacks against 256, 384, and 521-bit ECDSA with a wide range of nonce leakage bits. As a result, we confirmed that attacks on P256 with 3 bits nonce leakage, P384 with 4 bits nonce leakage, and P521 with 5 bits nonce leakage were feasible. Attacks against P521 with five bits are a new record in lattice attacks.

To estimate the effectiveness of lattice attacks theoretically, we developed a model of lattice attacks based on the experimental results. According to the model, attacks on P256 with less than 3.29 bits nonce leakage, P384 with less than 4.4 bits nonce leakage, and P521 with less than 5.59 bits nonce leakage are difficult or infeasible.

2 Preliminaries

2.1 Lattices

The lattice in $\mathbb{R}^n$ is a subgroup of $\mathbb{R}^n$. Let $\boldsymbol{b}_1, \cdots, \boldsymbol{b}_n$ be basis of $\mathbb{R}^n$. A lattice Λ is generated by linear combinations with integer coefficients of the basis $\boldsymbol{b_1}, \cdots, \boldsymbol{b_n}$.

$$\Lambda = \left\{ \sum_{i=1}^{n} c_i \boldsymbol{b}_i \mid c_i \in \mathbb{Z} \right\} \tag{1}$$

We denote the norm of the shortest vector in Λ as $\lambda_1(\Lambda)$ and the minimum radius r such that a ball with radius r contains i linearly independent vectors as $\lambda_i(\Lambda)$. In this work, we consider only regular matrices as basis matrices $\boldsymbol{B}$, so $\mathrm{vol}(L) = |\det(B)|$.

The shortest vector problem (SVP) and the closest vector problem (CVP) are basic lattice problems. Given the basis of a lattice Λ in $\mathbb{R}^n$, SVP is used to find the shortest nonzero vector in Λ. CVP is related to SVP: given a basis of a lattice Λ in $\mathbb{R}^n$ and a target point $\boldsymbol{v} \in \mathbb{R}^n$, find a vector in Λ closest to $\boldsymbol{v}$. When the shortest distance between the target and the vectors in the lattice is limited to a small value, CVP is called bounded distance decoding (BDD), which can be solved by the nearest plane[7], but in practice, Kannan's embedding method[17] is often used to solve CVP. This technique heuristically reduces CVP into SVP and is said to outperform the nearest plane in [15, 30]. As another lattice problem, unique SVP is also widely known: given a lattice Λ in $\mathbb{R}^n$ such that $\lambda_2(\Lambda)/\lambda_1(\Lambda) > \gamma$, find a non-zero shortest vector in Λ.

According to Gaussian Heuristic, $\lambda_1(\Lambda)$ is expected as

$$\lambda_1(\Lambda) \approx \sqrt{\frac{n}{2\pi e}} \cdot \mathrm{vol}(\Lambda)^{1/n} \tag{2}$$

2.2 Lattice Reduction

Lattice reduction methods such as LLL[18], BKZ[29], and G6K[1] can be used to solve SVP or CVP. In particular, the BKZ algorithm is widely used in cryptoanalysis.

The BKZ algorithm is an extension of the LLL algorithm, which achieves lattice reduction in polynomial time. The BKZ is executed with a block size β. BKZ proceeds by focusing on the Euclidean norm of the basis and the shortest basis's norm of $\Lambda \in \mathbb{R}^n$ is expected to be $\delta_\beta^{n-1}\mathrm{vol}(\Lambda)^{1/n}$ using δ_β, which depends on β. Some improved versions have also been introduced, such as BKZ2.0[11].

When a large block size is used as the input, the output basis is expected to be short, but the execution time increases significantly. The behavior of BKZ (and other lattice reduction algorithms), including running time, was examined in [12].

In previous studies, BKZ was used to attack (EC)DSA with partially leaked nonce bits. In those works, the block size β was set to approximately 30, for example, 30 in [13] and 25 in [27].

2.3 DSA/ECDSA

DSA is a Federal Information Processing Standard[24].

Let p and q be large prime numbers. $p-1$ must be a multiple of q.

Let $h \in [2, p-2]$ be a random integer and compute $g \equiv h^{(p-1)/q} \bmod p$ (if $g = 1$, a different h is selected).

p,q ,and g are the domain parameters for DSA. The secret key d is selected from $[1, q-1]$, and the public key is $y = g^x \bmod p$. To sign a message, the signer selects a random integer $k \in [1, q-1]$, called the nonce. The signatures r and s for message m are generated as follows:

$$r \equiv (g^k \bmod p) \bmod q \tag{3}$$
$$s \equiv k^{-1}(\mathrm{HASH}(m) + rd) \bmod q \tag{4}$$

If the value is 0, start again from the selection of k.

ECDSA[16, 24] is a variant of DSA that uses elliptic curve cryptography. The domain parameters for ECDSA are the elliptic curve E and the base point G on E of order n. The secret key d is selected from $[1, n-1]$, and the public key is $Q = dG$. The signer selects the nonce $k \in [1, n-1]$, and the signatures r and s for message m are generated as follows:

$$r \equiv x_1 \bmod n, kG = (x_1, y_1) \tag{5}$$
$$s \equiv k^{-1}(\mathrm{HASH}(m) + rd) \bmod n \tag{6}$$

If the value is 0, start again from the selection of k.

In both DSA and ECDSA, k must have a different value for each signature, and the value must be kept secret. If the value of k is known to the attacker, the secret key d can be calculated by solving the equation for generating signature s. Furthermore, even if a few bits of k are known, the secret key can be recovered via the HNP, as described in the next subsection.

2.4 Hidden Number Problem

The HNP was introduced by D. Boneh and R. Venkatesan[10] and has been used in attacks against (EC)DSA[14, 25, 26]. The HNP recovers the secret $\alpha \in [1, n-1]$ when some of the most significant bits of $t_i\alpha \bmod n$ are known for all random integers t_i and a modulus n.

To apply HNP to DSA/ECDSA, the attacker uses the equation for signature s. From here, the prime number q in DSA is rewritten as n in accordance with the notation in the ECDSA. Let n be an N-bit prime number. From the equation generating s, we have:

$$k - s^{-1}rd - s^{-1}\mathrm{HASH}(m) \equiv 0 \bmod n \tag{7}$$

When the signatures are generated K times, we have K equations as follows:

$$k_i - s_i^{-1}r_i d - s_i^{-1}\mathrm{HASH}(m_i) \equiv 0 \bmod n \quad (i = 1, \cdots, K) \tag{8}$$

Assuming that the attacker learns the l most significant bits of the nonce k_i (via side-channel attacks) for all K signatures, k_i can be expressed as $k_i = z_i + a_i$, where a_i is a known integer and $z_i (0 \le z_i < 2^{N-l})$ is an unknown integer. Then, Equation (8) becomes

$$z_i + a_i - s_i^{-1}r_i d - s_i^{-1}\mathrm{HASH}(m_i) \equiv 0 \bmod n \quad (i = 1, \cdots, K) \tag{9}$$

Because the message m_i can be selected by the attacker, the value of $\mathrm{HASH}(m_i)$ can be calculated. In addition, because a_i is a known value, the values of $u_i = -s_i^{-1}r_i$ and $v_i = a_i - s_i^{-1}\mathrm{HASH}(m_i)$ can be calculated by the attacker. Using u_i and v_i, we obtain

$$z_i + u_i d + v_i \equiv 0 \bmod n \quad (i = 1, \cdots, K) \tag{10}$$

Recalling that $0 \leq z_i < 2^{N-l}$, we have $-(u_i d + v_i) \bmod n < 2^{N-l}$. Therefore, the secret key d can be calculated using HNP. To tighten this constraint, Equation (10) is rearranged as follows: This technique is known as recentering.

$$(z_i - 2^{N-l-1}) + u_i d + v_i + 2^{N-l-1} \equiv 0 \bmod n \quad (i = 1, \cdots, K) \tag{11}$$

In this case, we have $|u_i d + v_i + 2^{N-l-1}|_n \leq 2^{N-l-1}$.

HNP is solved by lattice attacks that calculate the secret key via CVP or Bleichenbacher's attack, which is based on Fourier analysis.

Lattice attacks use lattice basis reduction algorithms, such as BKZ. These attacks can successfully recover the secret key with a relatively small number of signatures (K) when sufficient bits (l) of the nonce are known to the attacker, but are vulnerable to error information of the nonce[6].

2.5 Side-channel Attacks

In this work, we assume nonce leaks, but in practice, the attacker must obtain information about nonce via side-channel attacks.

For example, in [22], 40,000 signatures were generated to construct an HNP. Another example is [8], which did not attack ECDSA via HNP but aimed to leak all bits of the nonce. In the attack, it is theoretically possible to leak all the bits of nonce in a single signature, but owing to the buffer limit of the oscilloscope, only a few bits are actually acquired.

As in the example above, it can be difficult to obtain enough leaked information for HNP, so it is important for the attacker to minimize the number of leaked bits l and the number of signatures K.

3 Lattice Attacks

3.1 Details of the attack

For lattice construction, we follow [9, 25]. This work assumes that the most significant bits of nonce k are leaked by side-channel attacks. As discussed in Section 2.4, we assume the leakage of l most significant bits of nonce k, and we have

$$(z_i - 2^{N-l-1}) + u_i d + v_i + 2^{N-l-1} \equiv 0 \bmod n \quad (i = 1, \cdots, K) \tag{12}$$

with the constraints $|u_i d + v_i + 2^{N-l-1}|_n \leq 2^{N-l-1}$. Now, let $Z = 2^{l+1}$ and $v'_i = v_i + 2^{N-l-1}$ and construct the following matrix:

$$A = \begin{pmatrix} Zn & & & & \\ & Zn & & & \\ & & \ddots & & \\ & & & Zn & \\ Zu_1 & Zu_2 & \cdots & Zu_K & 1 \end{pmatrix} \tag{13}$$

Now, considering the lattice $\Lambda = \{\boldsymbol{x}A | \boldsymbol{x} \in \boldsymbol{Z}^{K+1}\}$ generated by the matrix A and the target point $\boldsymbol{v} = (Zv'_1, \cdots, Zv'_K, 0)$, the lattice A contains a vector $\boldsymbol{x}$ that satisfies

$$\boldsymbol{w_0} = \boldsymbol{x}A + \boldsymbol{v} = (-Z(z_1 - 2^{N-l-1}), \cdots, -Z(z_K - 2^{N-l-1}), d) \tag{14}$$

or

$$\boldsymbol{w_1} = \boldsymbol{x}A + \boldsymbol{v} = (-Z(z_1 - 2^{N-l-1}), \cdots, -Z(z_K - 2^{N-l-1}), d - n) \tag{15}$$

Because $\boldsymbol{w_0}$ and $\boldsymbol{w_1}$ are related to d, finding $\boldsymbol{w_0}$ or $\boldsymbol{w_1}$ leads to the recovery of the secret key. Because of the constraints on the value of $z_i - 2^{N-l-1}$, the norm of $\boldsymbol{w_0}$ or $\boldsymbol{w_1}$ is very short, so it is possible to find $\boldsymbol{w_0}$ or $\boldsymbol{w_1}$ by using the approach to solve the CVP.

To solve this CVP, we used the Kannan's embedding method. This heuristic method reduces the CVP into SVP. Here, matrix A is embedded into a larger matrix A'.

$$A' = \begin{pmatrix} A & \mathbf{0} \\ \boldsymbol{v} & n \end{pmatrix} \tag{16}$$

$$= \begin{pmatrix} Zn & & & & & \\ & Zn & & & & \\ & & \ddots & & & \\ & & & Zn & & \\ Zu_1 & Zu_2 & \cdots & Zu_K & 1 & 0 \\ Zv'_1 & Zv'_2 & \cdots & Zv'_K & 0 & n \end{pmatrix} \tag{17}$$

The vectors

$$\boldsymbol{w'_0} = (-Z(z_1 - 2^{N-l-1}), \cdots, -Z(z_K - 2^{N-l-1}), d, n) \tag{18}$$

$$\boldsymbol{w'_1} = (-Z(z_1 - 2^{N-l-1}), \cdots, -Z(z_K - 2^{N-l-1}), d-n, n) \tag{19}$$

and $-\boldsymbol{w'_0}$ and $-\boldsymbol{w'_1}$ are vectors whose norm is particularly small among the vectors in the lattice, so they are expected to be found by the SVP approach. However, there is another short vector, $(0, \cdots, 0, \pm n, 0)$, and this vector is the shortest vector of the lattice generated by A', so we are looking for the second shortest vector. Therefore, we apply the BKZ algorithm to the matrix A' to reduce the basis and look for a basis whose last element is $\pm n$ to find the target vector $\pm\boldsymbol{w'_0}$ or $\pm\boldsymbol{w'_1}$. The $K+1$ th element of the basis is the secret key $d \bmod n$.

To avoid appearing $(0, \cdots, 0, \pm n, 0)$ on the first basis, [2, 30] uses a technique to remove $(0, \cdots, 0, \pm n, 0)$ from the lattice. With this technique, the target vector is expected to appear on the first basis. [2] mentioned, however, that this technique "would not be expected to make a significant difference in the feasibility of the algorithm", so we do not apply the technique to this work.

3.2 Theoretical success probability

In this section, we discuss the theoretical attack success rates. A similar discussion that depends on the Gaussian heuristic and unique SVP is found in [30], but it cannot be applied to our attack scenario because the shortest basis is expected to be $(0, \cdots, 0, \pm n, 0)$, and the target vector is expected to be located on the second basis in our attack.

Thus, we assume the existence of a CVP oracle for the infinity norm (CVP_∞ oracle) to estimate the success rates. Considering the constraints of $z_i - 2^{N-l-1}$ in equations (14) and (15), the CVP_∞ oracle is more suitable than the CVP oracle for the Euclidean norm. However, the CVP_∞ oracle is an NP-hard problem [25], so it cannot always be feasible to solve a practical problem.

We now calculate the success rate of the attack based on the assumptions described in Section 3.1. This discussion is based on [10]. Consider the difference $\boldsymbol{a} = \boldsymbol{x}A + \boldsymbol{v}$ between a vector $\boldsymbol{x}A$ in lattice L and vector $-\boldsymbol{v}$. Let $\boldsymbol{x} = (x_1, \cdots, x_K, a)$, and we have that

$$\boldsymbol{a} = (aZu_1 + x_1 Zn + Zv'_1, \cdots, aZu_K + x_K Zn + Zv'_K, a) \tag{20}$$

The target vectors satisfy $a \bmod n = d$ and are expressed as follows:

$$\boldsymbol{w_0} = \big(-Z(z_1 - 2^{N-l-1}), \cdots, -Z(z_K - 2^{N-l-1}), d\big) \tag{21}$$

$$\boldsymbol{w_1} = \big(-Z(z_1 - 2^{N-l-1}), \cdots, -Z(z_K - 2^{N-l-1}), d-n\big) \tag{22}$$

When $d < \frac{n}{2}$, $\boldsymbol{w_0}$ has a smaller infinity norm than $\boldsymbol{w_1}$. Otherwise, $\boldsymbol{w_1}$ has a smaller infinity norm. In either case, let the vector with a smaller infinity norm be $\boldsymbol{w}$. Its infinity norm is

$$||\boldsymbol{w}||_\infty = \max\left\{\left|Z(z_1 - 2^{N-l-1})\right|, \ldots, \left|Z(z_K - 2^{N-l-1})\right|, \min\{d, n-d\}\right\} \leq 2^N. \quad (23)$$

On the other hand, let the vector with a smaller infinity norm be $\boldsymbol{a}_a$ under the condition that $a \bmod n \neq d$. Its infinity norm is

$$\begin{aligned} ||\boldsymbol{a}_a||_\infty &= \max\left\{\left|aZu_1 + Zv_1')\right|_{Zn}, \cdots, \left|aZu_K + Zv_K'\right|_{Zn}, |a|_{Zn}\right\} & (24)\\ &= \max\left\{Z\left|au_1 + v_1'\right|_n, \cdots, Z\left|au_K + v_K'\right|_n, |a|_{Zn}\right\} & (25)\end{aligned}$$

If $||\boldsymbol{a}_a||_\infty$ is greater than 2^N, then there is no vector whose infinity norm is smaller than $\boldsymbol{w}$. The probability of this is

$$\begin{aligned} \Pr\left(||\boldsymbol{a}_a||_\infty > 2^N\right) &\geq \Pr\left(^\exists i : Z\left|au_i + v_i'\right|_n > 2^N\right) \\ &= \Pr\left(^\exists i : \left|au_i + v_i'\right|_n > 2^{N-l-1}\right) \quad (26)\end{aligned}$$

Since $|du_i + v_i'|_n \leq 2^{N-l-1}$,

$$\begin{aligned} &\left|au_i - du_i\right|_n > 2^{N-l} \\ \Leftrightarrow &\left|au_i + v_i' - (du_i + v_i')\right|_n > 2^{N-l} \\ \Rightarrow &\left|au_i + v_i'\right|_n > 2^{N-l-1} \quad (27)\end{aligned}$$

Thus,

$$\begin{aligned} \Pr\left(||\boldsymbol{a}_a||_\infty > 2^N\right) &\geq \Pr\left(^\exists i : \left|au_i - du_i\right|_n > 2^{N-l}\right) \\ &= 1 - \left(\frac{2^{N-l+1}}{n-1}\right)^K \quad (28)\end{aligned}$$

Because $a \bmod n$ can take any $n-1$ values except d among $0, \cdots, n-1$, the probability $\overline{P}$ that there exists a vector with a smaller infinity norm than $\boldsymbol{w}$ when all values of a are considered is

$$\overline{P} \leq (n-1)\left(\frac{2^{N-l+1}}{n-1}\right)^K \quad (29)$$

Therefore, the probability P that there is no vector with a smaller infinity norm than $\boldsymbol{w}$, that is, the probability P that the secret key recovery is possible with a CVP oracle for the infinity norm is

$$P \geq 1 - (n-1)\left(\frac{2^{N-l+1}}{n-1}\right)^K \quad (30)$$

Table 1-3 shows the minimum conditions under which the success rate of the attack P exceeds 0.99, as a result of using the parameters of P256, P384, and P521 recommended in NIST[24], which are the target elliptic curves in this work.

Table 1: Required K to attack P256 with CVP_∞ oracle

Leaked bits l	8	7	6	5	4	3	2
Signatures K	38	44	53	66	88	132	263

Table 2: Required K to attack P384 with CVP_∞ oracle

Leaked bits l	8	7	6	5	4	3	2
Signatures K	56	66	79	98	131	196	391

Table 3: Required K to attack P521 with CVP_∞ oracle

Leaked bits l	8	7	6	5	4	3	2
Signatures K	76	88	106	132	176	264	528

4 Experimental Results

4.1 Settings

To investigate the conditions under which lattice attacks are possible in terms of the key length, the number of leaked nonce bits, and the number of signatures, we randomly generated the matrix represented by Equation (17), recovered the secret key using BKZ reduction, and confirmed that the attack recovers the correct secret key. In this experiment, u_i and v_i are not calculated from the actual signatures but are randomly generated to satisfy Equation (10). When actual signatures are used, the distributions of u_i and v_i are not necessarily uniform because the relationship between nonce k and signature r is not a one-to-one correspondence, and the hash value $\mathrm{HASH}(m_i)$ may not be uniformly distributed under modulus n. Therefore, when the results obtained from this experiment are applied to actual signatures using actual signatures, they can be affected by distribution bias. Specifically, if (ui, vi) has the same value in multiple signatures, duplicated signatures do not add significant constraints to Equation (10). If the distribution is biased, the probability of having the same value increases, so the number of signatures required may increase slightly. However, because the distribution of (ui, vi) is also affected by the attacker's message selection and n is a very large number, we assume that the difference between this attack and the actual signature is negligible.

We ran the attack described previously on the library Sage 9.1[28]. We used the parameters of P256, P384, and P521 recommended in [24] as the target of the attack, and measured the total execution time required to finish the BKZ algorithm, to find the target vector w, and to recover the secret key candidate. This experiment was conducted on an AMD Ryzen Threadripper 3990X as a single thread.

4.2 Results

The number of trials is 100 times. Because the running time of the BKZ algorithm becomes very long when the dimension of the lattice becomes large, the number of trials under such conditions is small. In such cases, the number of trials is specified.

Figure 1-3 shows the results of attacks on P256, P384, and P521. If a certain number of leaks can be obtained, as shown in the figures, the attack can easily succeed. The conditions for this are 4 bits for P256, 5 bits for P384, and 7 bits for P521.

For the experiment targeting P256, P384, and P521, the minimum number of signatures K that correctly recovered the secret key in all trials are shown in Table 4-6 respectively. These numbers are smaller than those in Table 1-3. This is probably because the discussion in Section 3.2 restricts the probability to be calculated with inequalities. When such many leaks can be obtained, the lattice attacks can be said to perform like a CVP oracle for the infinity norm.

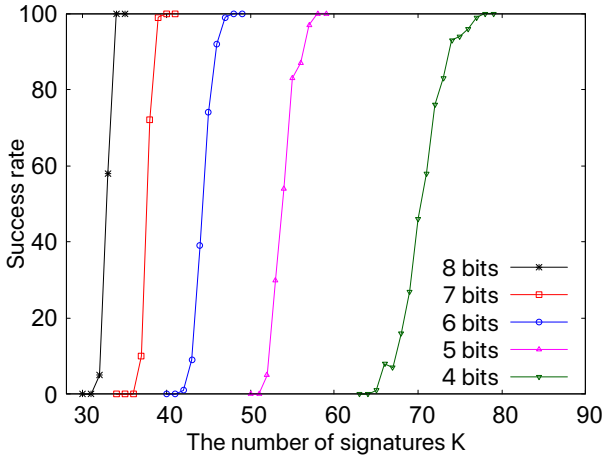

Figure 1: Attacks against P256

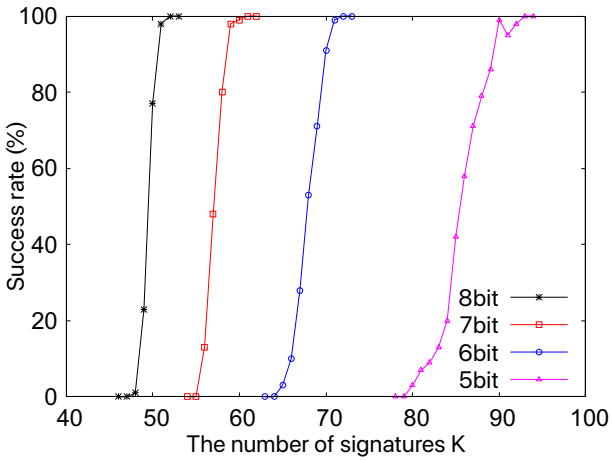

Figure 2: Attacks against P384

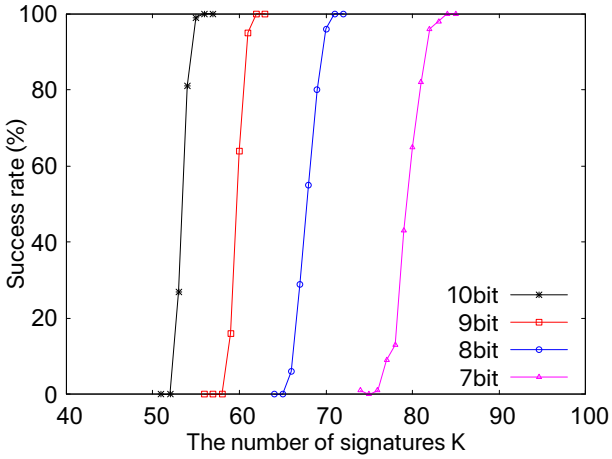

Figure 3: Attacks against P521

Table 4: Required K to attack P256

Leaked bits l	8	7	6	5	4
Signatures K	34	40	48	58	78

Table 5: Required K to attack P384

Leaked bits l	8	7	6	5
Signatures K	52	61	72	93

Table 6: Required K to attack P521

Leaked bits l	10	9	8	7
Signatures K	56	63	71	84

Table 7 shows the attack results for less nonce leakage. Owing to the long execution time, we were not able to run many experiments with different numbers of signatures K, but we ran the experiments with the number of signatures derived in Table 1-3.

Table 7: Attacks with less leaks

Target	Leaked bits l	Signatures K	Success rate
P256	3	132	43/100
P384	4	131	136/200
P521	6	106	100/100
P521	5	132	64/100

For P521, attacks with 6 bits leakage are feasible. However, the success rates of attacks with 3 bits leakage for P256, 4 bits leakage for P384, and 5 bits leakage for P521 are not 100%. Nonetheless, these attacks are still feasible because the success rates are approximately 50%.

4.3 Detailed investigation

We conducted more detailed experiments on attacks with few leaks in which the attack could fail. Attacks on P256 with a 3bits nonce leak were conducted, and the results are shown in Table 8. Owing to the long running time, the number of trials in $K \geq 150$ is limited to only 10.

Table 8: Attacks on P256 with 3bits nonce leak

Signatures K	132	140	150	160	170	180	190	200	210	220	230	240
Success	43	52	5	4	3	7	9	6	2	8	4	2
All	100	100	10	10	10	10	10	10	10	10	10	10

The results seem to have a large variance because of the small number of trials. However, we found that there was no significant improvement in the success rate of the attacks,

even if the number of signatures was increased beyond 140. This may be due to the fact that the reduction in HNP is sufficient. A possible reason is that the target could not be found because of insufficient lattice basis reduction of BKZ.

We conducted a detailed study in 100 samples for P256 and 100 samples for P384 to evaluate the performance of BKZ in this attack. In particular, we further investigated the case in which the number of signatures was 132, 131 for P256, P384 respectively. Here we denote a vector whose last element is $\pm n$ as candidate vector and the vector in Equation (18) or (19) as the target vector. By outputting the target vector and all the bases after lattice basis reduction, we found the following:

- Regardless of success or failure, the shortest basis was $(0, \cdots, 0, n, 0)$.
- In case of success, BKZ succeeded in finding the target vector. The target vector was the second shortest basis.
- In case of failure, BKZ failed in finding the target vector. The second shortest basis was a candidate vector that are not the target vector, an irrelevant vector in the lattice, or Zn, that is, a basis in which only one element was Zn and the others were 0.
- (P256) The norm of the target vector was $6.718n$ on average.
  (P384) The norm of the target vector was $6.689n$ on average.
- (P256) 8 samples in which the norm of the target vector $< 6.351n$ succeeded.
  (P384) 19 samples in which the norm of the target vector $< 6.479n$ succeeded.
- (P256) 12 samples in which the norm of the target vector $> 7.027n$ failed.
  (P384) 9 samples in which the norm of the target vector $> 7.086n$ failed.
- (P256) In 80 samples in which $6.351n <$ the norm of the target vector $< 7.027n$, success and failure are mixed.
  (P384) In 72 samples in which $6.479n <$ the norm of the target vector $< 7.086n$, success and failure are mixed.

From the first result, we can say that we succeeded in finding the shortest basis. The second and third results show that when the attack fails, the basis whose norm is larger than the norm of the target vector is output as the second shortest basis. On the other hand, the target vector always appears on the second basis when the attack succeeds.

The 4-7th results show the norm of the target vector. From these results, it appears that it is difficult for lattice attacks to find the target vector when the norm of the target vector reaches approximately $7n$.

4.4 Running time

Figure 4 shows the running time. The running time does not depend significantly on the key length but depends on the size of the input matrix. The running time increases exponentially, and the difficulty of the attack increases under the condition that there are few leaks in terms of execution time.

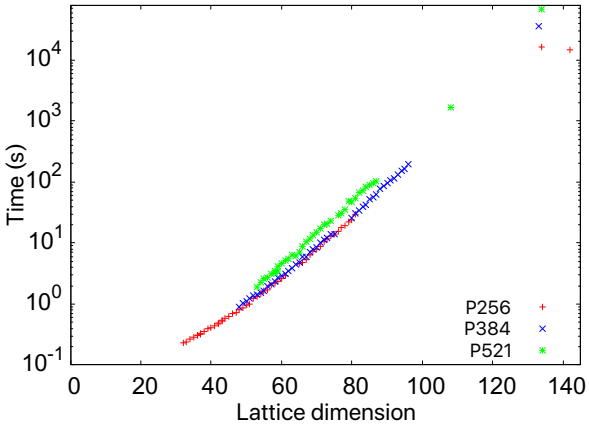

Figure 4: Running time of BKZ

5 Effectiveness of lattice attacks

Based on the results in the previous section, we discuss the conditions under which the secret key can be recovered by the method employed in this work after making some assumptions for a simplified discussion.

To evaluate the success or failure of lattice attacks, we consider modeling lattice attacks by focusing on the norm of the target vector. Intuitively, we consider that BKZ can find the target vector if its norm is significantly small.

In our experiments, we found that the norm of the shortest basis is always n, and we assume that the BKZ can find this vector as the shortest basis. Therefore, we discuss the ratio R of the smallest norm n to the norm of the target vector. If the ratio is sufficiently small, the BKZ will find the target, and if it is large, the target will be concealed by other bases.

The experimental results in Section 4.3 show that the ratio R is approximately 6 to 7 in the attacks on P256 with 3 bits leakage and P384 with 4 bits leakage, so we can suspect that when R is approximately 6 to 7, lattice attacks sometimes fail to recover the secret key. Intuitively, the smaller R is, the easier it is to recover the key.

We calculated the expected value of the norm for the target vector. The target vector is the shortest vector of the

$$\boldsymbol{w}'_{\mathbf{0}} = (-Z(z_1 - 2^{N-l-1}), \cdots, -Z(z_K - 2^{N-l-1}), d, n) \tag{31}$$

$$\boldsymbol{w}'_{\mathbf{1}} = (-Z(z_1 - 2^{N-l-1}), \cdots, -Z(z_K - 2^{N-l-1}), d-n, n) \tag{32}$$

and $-\boldsymbol{w}'_{\mathbf{0}}$,$-\boldsymbol{w}'_{\mathbf{1}}$. Here, we denote the target vector as $\boldsymbol{w}'$, and its expected square of the norm is

$$E(||\boldsymbol{w}'||^2) = E\left(\sum_{i=1}^{K} Z^2(z_i - 2^{N-l-1})^2 + \min\{d^2, (d-n)^2\} + n^2\right) \tag{33}$$

Here, we assume that z_i independently and randomly takes a value from 0 to 2^{N-l-1}. Because d is determined independently of z_i, we have

$$E(||\boldsymbol{w}'||^2) = E\left(\sum_{i=1}^{K} Z^2(z_i - 2^{N-l-1})^2\right) + E\left(\min\{d^2, (d-n)^2\}\right) + n^2 \tag{34}$$

Since $0 \leq z_i < 2^{N-l}$,

$$E(Z^2(z_i - 2^{N-l-1})^2) = Z^2 \frac{\sum_{i=0}^{2^{N-l}-1} (i - 2^{N-l-1})^2}{2^{N-l}} \tag{35}$$

$$= Z^2 \frac{(2^{N-l-1})^2 + 2 \cdot \sum_{i=1}^{2^{N-l-1}-1} i^2}{2^{N-l}} \tag{36}$$

$$= Z^2 \frac{(2^{N-l-1})^2 + \frac{(2^{N-l-1}-1)2^{N-l-1}(2\times 2^{N-l-1}-1)}{3}}{2^{N-l}} \tag{37}$$

$$= \frac{1}{3}(2^{2N} + 2^{2l+1}) \tag{38}$$

Next, for $E\left(\min\{d^2, (d-n)^2\}\right)$, n is a prime number, and thus an odd number. Therefore

$$E\left(\min\{d^2, (d-n)^2\}\right) = \frac{2 \cdot \sum_{i=1}^{\frac{n-1}{2}} i^2}{n-1} \tag{39}$$

$$= \frac{n(n+1)}{12} \tag{40}$$

Therefore,

$$E(||\boldsymbol{w}'||^2) = K \cdot \frac{1}{3}(2^{2N} + 2^{2l+1}) + \frac{n(n+1)}{12} + n^2 \tag{41}$$

Originally, we would like to find $E(||\boldsymbol{w}'||)$, but this is difficult, so we proceed with the discussion around the expectation value of the square. In this case, we have the relation $E(X^2) \geq (E(X))^2$, which means that we use a value larger than the original $E(||\boldsymbol{w}'||)$. We denote the estimated value (not the expected value) of the target norm as:

$$\sqrt{K \cdot \frac{1}{3}(2^{2N} + 2^{2l+1}) + \frac{n(n+1)}{12} + n^2} \tag{42}$$

and consider the ratio R to norm of the shortest basis

$$R = \frac{\sqrt{K \cdot \frac{1}{3}(2^{2N} + 2^{2l+1}) + \frac{n(n+1)}{12} + n^2}}{n} \tag{43}$$

Figure 5 plots the R for attacks with 3, 4, and 5 bits against P256, P384, and P521, where the success rate dropped in 4.2.

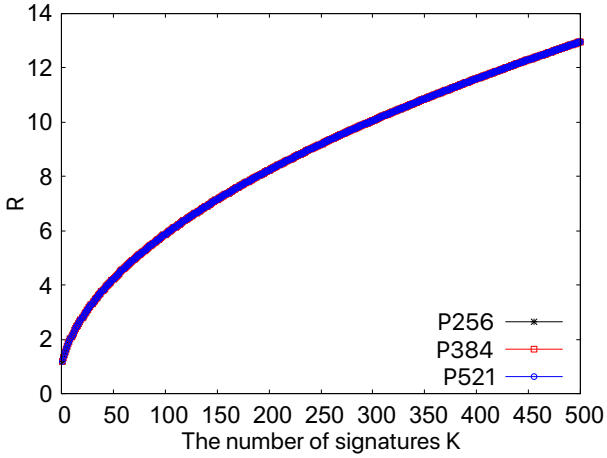

Figure 5: Estimated R

The estimated R in Figure 5 for the 132, 131 signatures where we performed the attack on P256, P384 is 6.7144 and 6.6895 respectively, which is consistent with the experimental results (6.718 and 6.689 on average). Depending on this model, we consider the execution of an attack when the leakage is less than that. The value of R is not significantly affected by l because $2^{2N} >> 2^{2l+1}$ when the value of l is small. Thus, we approximate R as follows:

$$R \approx \frac{\sqrt{K \cdot \frac{2^{2N}}{3} + \frac{n(n+1)}{12} + n^2}}{n} \tag{44}$$

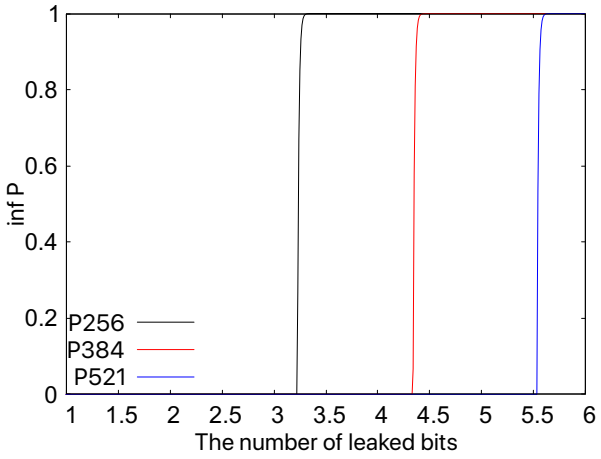

Figure 6: Inf P in Equation (30) (K=115)

The 5th result in Section 4.3 suggests that lattice attacks easily succeed when R is less than 6.3. In Equation (44), we calculated that the condition on K to satisfy $R < 6.3$ using parameters P256, P384, and P521. In each case, $K < 116$ was required. This result and Table 1-3 show that attacks against P256 with 3 bits, P384 with 4 bits, and P521 with 5 bits are difficult, as shown in the experimental results in Section 4.2. Furthermore, the value of the right side of Equation (30) when $K = 115$ is shown in Figure 6. From

Figure 6, we can infer attacks against P256 with about 3.29 bits, P384 with about 4.4 bits and P521 with about 5.59 bits are easily succeed.

Based on this model, it is necessary to use a lattice reduction algorithm that can handle a larger R to improve lattice attacks. Recalling equations (30) and (5), when a larger R is allowed, a larger K and, thus, a smaller l is allowed.

Acknowledgement

We would like to thank Editage (www.editage.com) for English language editing.

References

[1] M. R. Albrecht, L. Ducas, G. Herold, E. Kirshanova, E. W. Postlethwaite, and M. Stevens, “The General Sieve Kernel and New Records in Lattice Reduction," EUROCRYPT 2019, Lecture Notes in Computer Science, Y. Ishai and V. Rijmen eds., vol. 11477, pp. 717-746, Springer, Cham, 2019.

[2] Martin R. Albrecht and Nadia Heninger, “On Bounded Distance Decoding with Predicate: Breaking the "Lattice Barrier" for the Hidden Number Problem," EUROCRYPT 2021, Lecture Notes in Computer Science, A. Canteaut and FX. Standaert eds., vol. 12696, pp. 528-558, Springer, Cham, 2021.

[3] A. C. Aldaya, B. B. Brumley, S. ul Hassan, C. Pereida García and N. Tuveri, “Port Contention for Fun and Profit," 2019 IEEE Symposium on Security and Privacy (SP), pp. 870-887, 2019.

[4] A. Cabrera Aldaya, C. Pereida García, and B. B. Brumley, “From A to Z: Projective coordinates leakage in the wild," IACR Transactions on Cryptographic Hardware and Embedded Systems, vol. 2020, no. 3, pp. 428-453, 2020.

[5] D. F. Aranha, P. A. Fouque, B. Gérard, J. G. Kammerer, M. Tibouchi, and J. C. Zapalowicz, “GLV/GLS Decomposition, Power Analysis, and Attacks on ECDSA Signatures with Single-Bit Nonce Bias," Advances in Cryptology – ASIACRYPT 2014, Lecture Notes in Computer Science, P. Sarkar and T. Iwata eds., vol. 8873, pp. 262–281, Springer, Berlin, Heidelberg, 2014.

[6] Diego F. Aranha, Felipe Rodrigues Novaes, Akira Takahashi, Mehdi Tibouchi, and Yuval Yarom, “LadderLeak: Breaking ECDSA With Less Than One Bit Of Nonce Leakage," Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security, pp.225-242, 2020.

[7] L. Babai, “On Lovász ’ lattice reduction and the nearest lattice point problem," Combinatorica, 6(1), pp. 1–13, 1986.

[8] L. Batina, Ł. Chmielewski, L. Papachristodoulou, P. Schwabe, and M. Tunstall, “Online Template Attacks," Journal of Cryptographic Engineering, 9(1), pp. 21-36, 2019.

[9] N. Benger, J. van de Pol, N. P. Smart and Y. Yarom, ““Ooh Aah... Just a Little Bit" : A Small Amount of Side Channel Can Go a Long Way," International Workshop on Cryptographic Hardware and Embedded Systems, L. Batina and M. Robshaw eds., Lecture Notes in Computer Science, vol. 8731, pp. 75-92, Springer, Berlin, Heidelberg, 2014.

[10] D. Boneh and R. Venkatesan, “Hardness of Computing the Most Significant Bits of Secret Keys in Diffie-Hellman and Related Schemes," Advances in Cryptology - CRYPTO ’96, Lecture Notes in Computer Science, N. Koblitz ed., vol. 1109, pp. 129-142, Springer, Berlin, Heidelberg, 1996.

[11] Yuanmi Chen and Phong Q. Nguyen. “BKZ 2.0: Better Lattice Security Estimates," Advances in Cryptology – ASIACRYPT 2011, Lecture Notes in Computer Science, D. H. Lee and X. Wang eds., vol. 7073, pp. 1–20, Springer, Berlin, Heidelberg, 2011.

[12] N. Gama and P. Q. Nguyen, “Predicting Lattice Reduction," Advances in Cryptology – EUROCRYPT 2008, Lecture Notes in Computer Science, N. Smart ed., vol. 4965, pp. 31-51, Springer, Berlin, Heidelberg, 2008.

[13] Cesar Pereida García and Billy Bob Brumley, “Constant-Time Callees with Variable-Time Callers," 26th USENIX Security Symposium, pp. 83-98, 2017.

[14] N. A. Howgrave-Graham and N. P. Smart ,“Lattice Attacks on Digital Signature Schemes," Designs, Codes and Cryptography, vol. 23, pp.283–290, 2001.

[15] J. Jancar, V. Sedlacek, P. Svenda, and M. Sys, “Minerva: The curse of ECDSA nonces," IACR Transactions on Cryptographic Hardware and Embedded Systems, 2020(4), pp. 281–308, 2020.

[16] D. Johnson, A. Menezes and S. Vanstone, “The Elliptic Curve Digital Signature Algorithm (ECDSA)," International Journal of Information Security, vol. 1, pp. 36–63, 2001.

[17] Ravi Kannan, “Minkowski ’s Convex Body Theorem and Integer Programming," Mathematics of Operations Research, 12(3), pp. 415–440, 1987.

[18] A. K. Lenstra, H. W. Lenstra and L. Lovász, “Factoring polynomials with rational coefficients," Mathematische annalen, vol. 261, pp. 515-534, 1982.

[19] Mingjie Liu, Jiazhe Chen, and Hexin Li, “Partially Known Nonces and Fault Injection Attacks on SM2 Signature Algorithm," International Conference on Information Security and Cryptology, D. Lin, S. Xu, and M. Yung eds., Lecture Notes in Computer Science, vol. 8567, pp. 343-358, Springer, Cham, 2013.

[20] M. Liu and P. Q. Nguyen, “Solving BDD by Enumeration: An Update," CT-RSA 2013, Lecture Notes in Computer Science, E. Dawson, ed., vol. 7779, pp. 293–309, Springer, Berlin, Heidelberg, 2013.

[21] M. Medwed and E. Oswald, “Template Attacks on ECDSA," International Workshop on Information Security Applications, KI. Chung, K. Sohn, and M. Yung eds., Lecture Notes in Computer Science, vol. 5379, pp. 14-27, Springer, Berlin, Heidelberg, 2009.

[22] Daniel Moghimi, Berk Sunar, Thomas Eisenbarth, and Nadia Heninger, “TPM-FAIL: TPM meets Timing and Lattice Attacks," 29th USENIX Security Symposium, pp. 2057-2073, 2020.

[23] E. De Mulder, M. Hutter, M. E. Marson, and P. Pearson, “Using Bleichenbacher ”s Solution to the Hidden Number Problem to Attack Nonce Leaks in 384-Bit ECDSA," CHES 2013, Lecture Notes in Computer Science, G. Bertoni and J. S. Coron eds., vol. 8086, pp. 435–452. Springer, Berlin Heidelberg 2013.

[24] National Institute of Standards and Technology, “FIPS PUB 186-4 Digital Signature Standard (DSS)," 2013.

[25] P. Q. Nguyen and I. E. Shparlinski, “The Insecurity of the Digital Signature Algorithm with Partially Known Nonces," Journal of Cryptology, vol.15, pp. 151-176, 2002.

[26] P. Q. Nguyen and I. E. Shparlinski, “The Insecurity of the Elliptic Curve Digital Signature Algorithm with Partially Known Nonces," Designs, Codes and Cryptography, vol. 30, pp. 201-217, 2003.

[27] Keegan Ryan, “Return of the Hidden Number Problem," IACR Transactions on Cryptographic Hardware and Embedded Systems, 2019(1), pp. 146–168, 2018.

[28] SageMath(Version 9.1). https://www.sagemath.org

[29] C. P. Schnorr and M. Euchner, “Lattice basis reduction: Improved practical algorithms and solving subset sum problems," Mathematical Programming, vol. 66, pp. 181-199, 1994.

[30] C. Sun, T. Espitau, M. Tibouchi, and M. Abe, “Guessing Bits: Improved Lattice Attacks on (EC)DSA with Nonce Leakage," Cryptology ePrint archive, Report 2021/455, 2021. https://eprint.iacr.org/2021/455

[31] A. Takahashi, M. Tibouchi, and M. Abe, “New Bleichenbacher Records: Fault Attacks on qDSA Signatures," IACR Transactions on Cryptographic Hardware and Embedded Systems, 2018(3), pp. 331–371, 2018.