Concrete Analysis of Schnorr-type Signatures with Aborts

Theo Fanuela Prabowo[1] and Chik How Tan[1]

[1*]Temasek Laboratories, National University of Singapore, 5A Engineering Drive 1, #09-02, Singapore, 117411, Singapore.

Contributing authors: tsltfp@nus.edu.sg; tsltch@nus.edu.sg;

Abstract

Lyubashevsky's signature [1, 2] can be viewed as a lattice-based adapation of the Schnorr signature [3], with the core difference being the use of aborts during signature generation process. Since the proposal of Lyubashevsky's signature, a number of other variants of Schnorr-type signatures with aborts have been proposed, both in lattice-based and code-based setting. In this paper, we examine the security of Schnorr-type signature schemes with aborts. We give a detailed analysis of when the expected value of the signature is correlated to the secret key, and when it is not. Our analysis shows that even when abort condition is employed, it is crucial to set the parameters carefully in order to defend against statistical attack. In particular, we recommend to set $\boldsymbol{\delta} \geq \boldsymbol{\beta}$ (where $\boldsymbol{\delta}, \boldsymbol{\beta}$ are public parameters) as in this case we prove that the signature does not reveal any information about the secret key. On the other hand, if this condition is not satisfied, then some information about the secret key are leaked, making the scheme susceptible to statistical attacks. For completeness, we also analyze the security of Schnorr-type signatures without aborts. In particular, we present a detailed key recovery attack via statistical method on the EagleSign signature [4], which is one of the submission to the NIST call for Additional PQC Signature. Moreover, we give a formula for determining the number of required signatures to successfully launch the statistical attack.

Keywords: statistical attack, key recovery attack, Lyubashevsky's signature, Schnorr-type signatures, signature with aborts

MSC Classification: 94A60

[0] This paper was submitted to a journal in November 2023 and is currently under review.

1 Introduction

Schnorr's signature scheme is a signature scheme proposed by Schnorr in [3]. It is constructed by first constructing an identification scheme, which is then transformed into a signature scheme via the Fiat-Shamir transformation [5]. However, the security of the original Schnorr's signature scheme relies on the discrete logarithm problem. As such, it is no longer secure in the presence of quantum adversaries.

Lyubashevsky [1, 2] adapts Schnorr's approach in order to construct lattice-based signatures. Adapting Schnorr's signature to lattice-based setting is not trivial due to the different underlying structures for lattices. A trivial adaptation will not be secure as in this case, the signature will reveal information about the secret key. Thus, secret key recovery can be done via statistical attack. Lyubashevsky overcame this issue by introducing the use of aborts during signature generation. The idea is to abort/discard a signature if it is deemed to leak information about the secret key. The signer then repeats the signature generation process until it produces a desired signature. This approach of constructing signatures is sometimes also called the Fiat-Shamir with aborts paradigm.

Ever since the proposal of the Lyubashevsky's signature, many lattice-based signature schemes were proposed based on the Lyubashevsky's signature scheme, for example, qTESLA [6] and Dilithium [7], which are some of the submissions in the NIST call for Post-Quantum Cryptography (PQC) standardization. In fact, Dilithium has been selected as one of the NIST PQC standardized signature schemes. Furthermore, Lyubashevsky's signature has been adapted to construct code-based signature schemes as well. For example, the SHMWW signature scheme [8] which is a Hamming-metric code-based signature, and the RankSign signature [9] which is a rank-metric code-based signature. Unfortunately, both of these signatures have been attacked. The papers [10] and [11] successfully recover the secret key of the SHMWW signature in polynomial time. The paper [12] also gives a polynomial-time key recovery attack on the RankSign signature.

In this paper, we further analyze the security of Schnorr-type signature schemes with aborts over $\mathbb{Z}_q$ in either lattice-based or code-based settings. We will give a detailed analysis of when the expected value of the signature will be correlated to the secret key, and when the signature does not reveal any information about the secret key.

For completeness, we also analyze the security of Schnorr-type signature schemes without aborts. In particular, we present a detailed key recovery attack on the EagleSign signature, which is a lattice-based signature scheme submitted to the NIST call for Additional PQC Signature. The rest of the paper is organized as follows. In Section 2, we introduce some notations and give a brief review on some results in probability theory. We then analyze the security of Schnorr-type signature schemes without aborts in Section 3. A detailed analysis of the Schnorr-type signatures with aborts is given in Section 4. We further show information-theoretically that the signature does not reveal any information about the secret key if certain condition is satisfied in Section 5. Finally, the paper is concluded in Section 6.

2 Preliminaries

2.1 Notations

Let n be a power of 2 or a prime and q be an odd prime; and we set $q_1 := \frac{q-1}{2}$ throughout this paper.

Rings. Let $\mathbb{Z}_q = \mathbb{Z}/q\mathbb{Z}$ denote the quotient ring of integers modulo q, and let $\mathcal{R}$, $\mathcal{R}_q$ denote the rings $\mathbb{Z}[x]/(x^n+1)$ and $\mathbb{Z}_q[x]/(x^n+1)$ respectively. Denote $\mathcal{R}_q^* = \{a(x) \in \mathcal{R}_q \mid a(x) \text{ is invertible}\}$.

For a polynomial $\bar{\mathbf{a}}(x) = \bar{a}_0 + \bar{a}_1 x + \ldots + \bar{a}_{n-1}x^{n-1} \in \mathcal{R}$, define $\mathbf{a}(x) = \sum_{i=0}^{n-1} a_i x^i$ where $a_i = \bar{a}_i \bmod q = \begin{cases} a_i & \text{if } a_i \leq q_1, \\ a_i - q & \text{otherwise} \end{cases}$. So, $a_i \in [-q_1, q_1]$. We denote its vector form as $\mathbf{a} = (a_0, a_1, \ldots, a_{n-1})$. We also denote the vector form of $a(x)b(x) \in \mathcal{R}_q$ as $\mathbf{ab}$. We sometimes abuse the notation by interchanging $\mathbf{a}$ with $a \in \mathcal{R}_q$.

Euclidean and Infinity Norm. Given $\mathbf{a}(x) = a_0 + a_1 x + \ldots + a_{n-1}x^{n-1} \in \mathcal{R}$, define its Euclidean norm as $\|\mathbf{a}\| := \sqrt{\sum_{i=0}^{n-1} a_i^2}$ and its infinity norm as $\|\mathbf{a}\|_\infty := \max_i\{|a_i|\}$. The length of $\mathbf{a}$ is defined as its Euclidean norm $\|\mathbf{a}\|$.

Distribution. Let $b < q_1$ and $t < n$ be positive integers.

(1) Distribution X_t on $\{-1, 0, 1\}$, defined by $\Pr[X_t = 1] = \Pr[X_t = -1] = \frac{t}{2n}$, and $\Pr[X_t = 0] = \frac{n-t}{n}$.
(2) Distribution $Y_{t,b}$ on $[-b, b] \cap \mathbb{Z}$, defined by $\Pr[Y_{t,b} = 0] = \frac{n-t}{n}$ and $\Pr[Y_{t,b} = i] = \frac{t}{2bn}$ for any $i \in \{\pm 1, \pm 2, \ldots, \pm b\}$.
Note that $X_t = Y_{t,1}$.
(3) Uniform Distribution on $[-b, b] \cap \mathbb{Z}$: We denote it by $\mathcal{U}_b$.
(4) Normal Distribution: We denote by $\mathcal{N}(0, \sigma^2)$ the normal distribution with mean 0 and standard deviation σ.

The following results are well known.

Lemma 1. *Let U, V be independent random variables with mean $\mathbb{E}(U), \mathbb{E}(V)$ and variance $\mathbb{V}(U), \mathbb{V}(V)$. Then,*

(a) $\mathbb{E}(U \pm V) = \mathbb{E}(U) \pm \mathbb{E}(V)$ *and* $\mathbb{V}(U \pm V) = \mathbb{V}(U) + \mathbb{V}(V)$,
(b) $\mathbb{E}(UV) = \mathbb{E}(U)\mathbb{E}(V)$ *and* $\mathbb{V}(UV) = (\mathbb{V}(U) + \mathbb{E}(U)^2) \times (\mathbb{V}(V) + \mathbb{E}(V)^2) - \mathbb{E}(U)^2\mathbb{E}(V)^2$.

Lemma 2. *Let $\mathcal{U}_b$ be the uniform distribution on $[-b, b] \cap \mathbb{Z}$. Then, the mean and the variance of this distribution are 0 and $\frac{b(b+1)}{3}$ respectively.*

Lemma 3. *Let $n > t, b \geq 1$ and. Then the mean and variance of $Y_{t,b}$ are 0 and $\frac{t(b+1)(2b+1)}{6n}$ respectively. In particular, the mean and variance of X_t is 0 and $\frac{t}{n}$.*

Proof. Note that

$$\mathbb{E}[Y_{t,b}] = \sum_{i=-b}^{b} i \Pr[Y_{t,b} = i] = \sum_{i=-b}^{-1} i \cdot \frac{t}{2bn} + \sum_{i=1}^{b} i \cdot \frac{t}{2bn} = 0.$$

Moreover,

$$\begin{aligned}
\mathbb{V}[Y_{t,b}] &= \mathbb{E}[Y_{t,b}^2] - \mathbb{E}[Y_{t,b}]^2 = \mathbb{E}[Y_{t,b}^2] \\
&= \sum_{i=-b}^{b} i^2 \Pr[Y_{t,b} = i] \\
&= \sum_{i=-b}^{-1} i^2 \cdot \frac{t}{2bn} + \sum_{i=1}^{b} i^2 \cdot \frac{t}{2bn} \\
&= 2 \left(\sum_{i=1}^{b} i^2 \right) \cdot \frac{t}{2bn} \\
&= \frac{t(b+1)(2b+1)}{6n}.
\end{aligned}$$

□

Now, consider the normal distribution $\mathcal{N}(0, \sigma^2)$ with mean 0 and standard deviation σ. The probability density function of $\mathcal{N}(0, \sigma^2)$ is $\rho_\sigma(t) := \left(\frac{1}{\sqrt{2\pi\sigma^2}}\right) e^{-\frac{t^2}{2\sigma^2}}$ for $t \in \mathbb{R}$.

Theorem 1 ([13, Theorem 2.23] (Central Limit Theorem)). *Let $X_1, X_2, \ldots, X_n$ be independent and identically distributed random variables such that $\mathbb{E}(X_i) = \mu$ and $\mathbb{V}(X_i) = \sigma^2$. Let $\overline{X} = \frac{1}{n}\sum_{i=1}^{n} X_i$. Then $\overline{X} - \mu$ approximates to the normal distribution $\mathcal{N}(0, \sigma^2/n)$ with mean 0 and standard deviation $\frac{\sigma}{\sqrt{n}}$. That is,*

$$\lim_{n\to\infty} \Pr\left(\frac{\overline{X} - \mu}{\sigma/\sqrt{n}} \leq Z\right) = \Phi(Z), \quad \text{where} \quad \Phi(Z) := \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{Z} e^{-t^2/2} \mathrm{d}t.$$

Lemma 4. *For any $Z \geq 0$, we have $\Phi(-Z) = 1 - \Phi(Z)$. Furthermore, we have the following approximations [14, page 932].*

(i) $\Phi(Z) \approx 1 - (0.4361836 t_Z - 0.1201676 t_Z^2 + 0.937298 t_Z^3) \cdot \frac{\exp(-Z^2/2)}{\sqrt{2\pi}}$ *if $Z \geq 0$; and*

(ii) $\Phi(Z) \approx (0.4361836 t_Z - 0.1201676 t_Z^2 + 0.937298 t_Z^3) \cdot \frac{\exp(-Z^2/2)}{\sqrt{2\pi}}$ *if $Z < 0$;*
where $t_Z := 1/(1 + 0.33267|Z|)$.

Definition 1. (Circulant Matrix) *Let $\mathbf{v} = (v_0, \ldots, v_{n-1}) \in \mathcal{V}$, a circulant matrix defined by $\mathbf{v}$ is*

$$V := \begin{bmatrix} v_0 & v_1 & \cdots & v_{n-1} \\ -v_{n-1} & v_0 & \cdots & v_{n-2} \\ \vdots & \vdots & \ddots & \vdots \\ -v_1 & -v_2 & \cdots & v_0 \end{bmatrix} \in \mathbb{Z}_q^{n \times n}.$$

For $\mathbf{u}, \mathbf{v} \in \mathcal{R}$, the product $\mathbf{w} = \mathbf{uv}$ can be computed as $\mathbf{w} = \mathbf{u}V = \mathbf{v}U$, and $\mathbf{w} = (w_0, \ldots, w_{n-1})$. Then, for $l = 0, \ldots, n-1$,

$$w_l = \sum_{i+j=l \bmod n} \epsilon_{i,j} u_i v_j,$$

where

$$\epsilon_{i,j} := \begin{cases} 1 & \text{if } i+j < n \\ -1 & \text{if } i+j \geq n. \end{cases}$$

Lemma 5. *Let $\mathbf{u}, \mathbf{v} \in \mathcal{R}_q$ and suppose each coordinates u_i, v_i of $\mathbf{u}$ and $\mathbf{v}$ are independently distributed random variables with mean 0 and variance $\sigma_{\mathbf{u}}^2$ and $\sigma_{\mathbf{v}}^2$ respectively. Then, each coordinate of $\mathbf{uv}$ approximates to $\mathcal{N}(0, n\sigma_{\mathbf{u}}^2\sigma_{\mathbf{v}}^2)$.*

Proof. Let $\mathbf{uv} = (w_0, \ldots, w_{n-1})$, then $w_t = \sum_{i=0}^{n-1} \pm u_i v_{(t-i) \bmod n}$. By Lemma 1(b), each $\pm u_i v_j$ follows a random variable with mean 0 and variance $\sigma_{\mathbf{u}}^2\sigma_{\mathbf{v}}^2$. By the Central Limit Theorem, each w_t approximates to $\mathcal{N}(0, n\sigma_{\mathbf{u}}^2\sigma_{\mathbf{v}}^2)$. □

3 Schnorr-type Signatures without Aborts

Let n be a power of 2 or a prime and q be an odd prime. We set $q_1 := \frac{q-1}{2}$ Let $\mathcal{R} := \mathbb{Z}[x]/(x^n + 1)$ and $\mathcal{R}_q := \mathbb{Z}_q[x]/(x^n + 1)$. For $b > 0$, denote $S_b := \{\mathbf{a} \in \mathcal{R} \mid \|\mathbf{a}\|_\infty \leq b\}$. For positive integer τ, b, denote $B_\tau := \{\mathbf{a} \in \{0, 1, -1\}^n \mid \mathrm{wt}_H(\mathbf{a}) = \tau\}$ and $B_{\tau,b} := \{\mathbf{a} \in \{0, \pm 1, \ldots, \pm b\}^n \mid \mathrm{wt}_H(\boldsymbol{a}) = \tau\}$.

We shall consider the following setting of Schnorr-type signature. The signature typically gives information of the form

$$\mathbf{s} = \mathbf{u} + \mathbf{ce} \in \mathcal{R}_q,$$

where $\mathbf{e} \in S_\eta$ is a (fixed) secret key, $\mathbf{u}$ is chosen randomly from S_γ, $\mathbf{c} := \mathcal{H}(\text{message } \mathbf{m} \| pk) \in B_\tau$, and $\|\mathbf{s}\|_\infty < q_1$. Here, η, γ, τ are integers which are public parameters satisfying $\gamma \gg \eta$. We set $\beta := \eta \cdot \tau$. Given a signature of a message $\mathbf{m}$, the public information include $\mathbf{s}, \mathbf{c}$, and $\mathbf{m}$; while $\mathbf{u}$ and $\mathbf{e}$ are secret.

Recall that $\mathbf{s} = \mathbf{u} + \mathbf{ce}$, where $\mathbf{ce}$ can be computed as

$$(c_0, \ldots, c_{n-1}) \begin{bmatrix} e_0 & e_1 & \ldots & e_{n-1} \\ -e_{n-1} & e_0 & \ldots & e_{n-2} \\ \vdots & \vdots & \ddots & \vdots \\ -e_1 & -e_2 & \ldots & e_0 \end{bmatrix}.$$

Fix $0 \leq i \leq n-1$. Suppose $c_l \neq 0$. Considering the $(l+i)$-th coordinate of $\mathbf{s} = \mathbf{u} + \mathbf{ce}$, we have

$$s_{l+i} = u_{l+i} + (ce)_{l+i}$$

$$\begin{aligned}
&= u_{l+i} + \sum_{j=0}^{n-1} \epsilon_{j,l+i-j} c_j e_{l+i-j} \\
&= u_{l+i} + \epsilon_{l,i} c_l e_i + \sum_{\substack{0 \le j \le n-1 \\ j \ne l}} \epsilon_{j,l+i-j} c_j e_{l+i-j} \\
&= u_{l+i} + \epsilon_{l,i} c_l e_i + w_{l+i} \qquad (1)
\end{aligned}$$

where

$$w_{l+i} := \sum_{\substack{0 \le j \le n-1 \\ j \ne l}} \epsilon_{j,l+i-j} c_j e_{l+i-j} \qquad (2)$$

and all indices are considered modulo n.

3.1 Computing $\mathbb{E}[s_{l+i}]$

In this section, we shall compute the expected value of s_{l+i}, denoted as $\mathbb{E}[s_{l+i}]$. We start by considering $\mathbb{E}[w_{l+i}]$.

Lemma 6. *We have $|w_{l+i}| \le \beta - \eta$.*

Proof. Note that

$$\begin{aligned}
|w_{l+i}| &= \left| \sum_{\substack{0 \le j \le n-1 \\ j \ne l}} \epsilon_{j,l+i-j} c_j e_{l+i-j} \right| \\
&\le \sum_{\substack{0 \le j \le n-1 \\ j \ne l}} |c_j| \cdot |e_{l+i-j}| \\
&\le \sum_{\substack{0 \le j \le n-1 \\ j \ne l}} |c_j| \cdot \eta \qquad (\text{as } \mathbf{e} \in S_\eta) \\
&= (\tau - 1) \cdot \eta \qquad (\text{as } \mathbf{c} \in B_\tau \text{ and } c_l \ne 0) \\
&= \beta - \eta.
\end{aligned}$$

□

For $k \in \mathbb{Z}$, we define

$$\overline{p_k} := \Pr[w_{l+i} = k].$$

Remark 1.*(i) By Lemma 6, we have $\overline{p_k} = 0$ if $|k| > \beta - \eta$.*

(ii) So, $\displaystyle\sum_{k=-(\beta-\eta)}^{\beta-\eta} \overline{p_k} = 1$.

(iii) We shall assume that $\overline{p_k} = \overline{p_{-k}}$ for any $k \in \mathbb{Z}$.

(iv) As a consequence of (iii), we have $\mathbb{E}[w_{l+i}] = \displaystyle\sum_{k=-(\beta-\eta)}^{\beta-\eta} k\overline{p_k} = 0$.

Since $\mathbf{u}$ is chosen randomly from S_γ, we observe that

$$\Pr[u_{l+i} = k] = \begin{cases} \frac{1}{2\gamma+1} & \text{if } |k| \leq \gamma, \\ 0 & \text{otherwise.} \end{cases}$$

Consequently, $\mathbb{E}[u_{l+i}] = 0$.

In this case when there is no aborts in the Schnorr-type lattice-based signature, we then have

$$\mathbb{E}[s_{l+i}] = \mathbb{E}[u_{l+i}] + \epsilon_{l,i} c_l e_i + \mathbb{E}[w_{l+i}] = \epsilon_{l,i} c_l e_i,$$

or equivalently (since $\epsilon_{l,i} c_l \in \{1, -1\}$),

$$e_i = \epsilon_{l,i} c_l \mathbb{E}[s_{l+i}]. \tag{3}$$

3.2 Recovering the Secret e

Equation (3) can be used to recover e_i from a number of signatures. Suppose we have collected a number of samples $s_{l+i}^{(1)}, s_{l+i}^{(2)}, \ldots, s_{l+i}^{(\hat{N})}$ from some known signatures. Then $\mathbb{E}[s_{l+i}]$ can be estimated as $\mathbb{E}[s_{l+i}] \approx \sum_{k=1}^{\hat{N}} s_{l+i}^{(k)} / \hat{N}$. This allows us to recover e_i for any $0 \leq i \leq n-1$ (and hence the whole secret key $\mathbf{e} = (e_0, e_1, \ldots, e_{n-1})$) as given in the following Algorithm 1.

Algorithm 1: Recovering $\mathbf{e} = (e_0, e_1, \ldots, e_{n-1}) \in \mathcal{R}_q = \mathbb{Z}_q[x]/(x^n + 1)$

```
Collect $N$ signatures $(\mathbf{s}^{(k)})_{k=1}^{N}$ for messages $(\mathbf{m}^{(k)})_{k=1}^{N}$
 Set $\Sigma = (\Sigma_0, \Sigma_1, \ldots, \Sigma_{n-1}) := (0, 0, \ldots, 0)$ and $\hat{N} := 0$
 for $1 \le k \le N$ do
    Compute $\mathbf{c}^{(k)} := \mathcal{H}(\mathbf{m}^{(k)} \| pk)$
    for $0 \le l \le n-1$ do
        if $c_l^{(k)} = 1$ then
            $\hat{N} := \hat{N} + 1$
            for $0 \le i \le n-1$ do
                $p := (l + i) \bmod n$
                if $l + i \ge n$ then
                    $\Sigma_i := \Sigma_i - s_p^{(k)}$
                else
                    $\Sigma_i := \Sigma_i + s_p^{(k)}$
                end if
            end for
        end if
        if $c_l^{(k)} = -1$ then
            $\hat{N} := \hat{N} + 1$
            for $0 \le i \le n-1$ do
                $p := (l + i) \bmod n$
                if $l + i \ge n$ then
                    $\Sigma_i := \Sigma_i + s_p^{(k)}$
                else
                    $\Sigma_i := \Sigma_i - s_p^{(k)}$
                end if
            end for
        end if
    end for
end for
for $0 \le i \le n-1$ do
    $e_i := \lfloor \Sigma_i / \hat{N} \rceil$
end for
```

Remark 2. *In Algorithm 1, the notation $\lfloor \Sigma_i / \hat{N} \rceil$ denotes the value of $\Sigma_i / \hat{N}$ rounded to the nearest integer. Observe that $\Sigma_i / \hat{N} \approx \epsilon_{l,i} c_l \mathbb{E}[s_{l+i}] = e_i$. The algorithm will recover e_i correctly if $|\frac{\Sigma_i}{\hat{N}} - e_i| < 0.5$.*

3.3 The Number of Required Signatures

In this section, we estimate the number N of signatures required for the statistical attack described in Algorithm 1 above.

Since $\mathbf{u} \in S_\gamma$, it follows that each coordinate u_j of $\mathbf{u}$ follows the uniform distribution $\mathcal{U}_\gamma$ on $[-\gamma, \gamma] \cap \mathbb{Z}$. Recall that the mean and standard deviation of $\mathcal{U}_\gamma$ is 0 and $\sqrt{\gamma(\gamma+1)/3}$ respectively.

Similarly, each coordinate e_j of $\mathbf{e}$ follows the uniform distribution $\mathcal{U}_\eta$ with mean 0 and standard deviation $\sqrt{\eta(\eta+1)/3}$. On the other hand, as $\mathbf{c} \in B_\tau$, we may treat each coordinate c_j of $\mathbf{c}$ as following the distribution X_τ. This distribution has mean and standard deviation of 0 and $\sqrt{\tau/n}$ respectively. Thus, letting $(w_0, w_1, \ldots, w_{n-1}) := \mathbf{ce}$, then by Lemma 5 each w_j approximates to the normal distribution $\mathcal{N}(0, n \cdot \frac{\eta(\eta+1)}{3} \cdot \frac{\tau}{n}) = \mathcal{N}(0, \tau\eta(\eta+1)/3)$.

Therefore, by Lemma 1(a), each $(u_j^{(k)} + w_j^{(k)})$ follows a probability distribution with mean 0 and standard deviation

$$\sigma := \sqrt{\frac{\gamma(\gamma+1) + \tau\eta(\eta+1)}{3}}.$$

Moreover, $\frac{1}{\hat{N}} \sum_{k=1}^{\hat{N}} [u_j^{(k)} + w_j^{(k)}]$ approximates to the normal distribution $\mathcal{N}(0, \frac{\sigma^2}{\hat{N}}) = \mathcal{N}\left(0, \frac{\gamma(\gamma+1)+\tau\eta(\eta+1)}{3\hat{N}}\right)$.

Theorem 2. *Let $U_1, U_2, \ldots, U_{\hat{N}}$ be independent and identically distributed probability distributions with mean μ and standard deviation σ. Let $\hat{U} := \frac{1}{\hat{N}} \sum_{i=1}^{\hat{N}} U_i$. Then, $\hat{U} - \mu \sim \mathcal{N}\left(0, \sigma^2/\hat{N}\right)$. Moreover, the required number $\hat{N}$ of samples such that $|\hat{U} - \mu| \leq d$ with probability $\Phi(Z) - \Phi(-Z)$ is $\hat{N} = \left(\frac{Z\sigma}{d}\right)^2$.*

Proof. By the Central Limit Theorem (Theorem 1), we have $\hat{U} - \mu = \frac{1}{\hat{N}} \sum_{i=1}^{\hat{N}} U_i - \mu \sim \mathcal{N}\left(0, \sigma^2/\hat{N}\right)$ and $\lim_{\hat{N} \to \infty} \Pr\left(\frac{\hat{U}-\mu}{\sigma/\sqrt{\hat{N}}} \leq Z\right) = \Phi(Z)$. It then follows that $\lim_{\hat{N} \to \infty} \Pr\left(\left|\frac{\hat{U}-\mu}{\sigma/\sqrt{\hat{N}}}\right| \leq Z\right) = \Phi(Z) - \Phi(-Z)$.

For large enough $\hat{N}$, we have $\Pr\left(\left|\frac{\hat{U}-\mu}{\sigma/\sqrt{\hat{N}}}\right| \leq Z\right) = \Phi(Z) - \Phi(-Z)$. Equivalently, $\Pr\left(|\hat{U} - \mu| \leq \frac{Z\sigma}{\sqrt{\hat{N}}}\right) = \Phi(Z) - \Phi(-Z)$ Then, we may set $\frac{Z\sigma}{\sqrt{\hat{N}}} = d$. Consequently,

$$\hat{N} = \left(\frac{Z\sigma}{d}\right)^2.$$

□

In Algorithm 1, we need to ensure that $|\Sigma_i/\hat{N} - \mathbb{E}[\epsilon_{l,i} c_l s_{l+i}]| < 0.5$. As such, we may take $d = 0.49$ and apply Theorem 2 to estimate the number of samples needed as

$$\hat{N} = (Z\sigma/0.49)^2.$$

Since $\mathbf{c} \in B_\tau$, the number of nonzero element in $\mathbf{c}$ is $\mathrm{wt}_H(\mathbf{c}) = \tau$. Thus, the number of required signatures is

$$N = \frac{\hat{N}}{\tau} = \left(\frac{Z\sigma}{0.49}\right)^2 / \tau. \tag{4}$$

We list some values of Z with the corresponding probability $(\Phi(Z) - \Phi(-Z))$ in the following Table 1.

Table 1 Some Values of Z with Their Corresponding Probabilities

Z	1.96	2.326	2.576	2.807	3.090	3.2905	3.8905	4.4171
Prob.	0.95	0.98	0.99	0.995	0.998	0.999	0.9999	0.99999

We end this section by giving the following remark.

Remark 3. *Note that in the case when there is no aborts in the signature generation process, we have*

$$\begin{aligned}\Pr[(w_{l+i} = k) \quad \wedge \quad (u_{l+i} = t)] &= \Pr[w_{l+i} = k] \cdot \Pr[u_{l+i} = t] \\ &= \begin{cases} \overline{p_k}/(2\gamma + 1) & \text{if } |t| \le \gamma, \\ 0 & \text{otherwise.} \end{cases}\end{aligned}$$

3.4 Key Recovery Attack on EagleSign [4]

EagleSign [4] is a lattice-based signature submitted to the NIST Call for PQC Additional Signature. It is a Schnorr-type signature without aborts. In this section, we apply the statistical attack technique given in Section 3.2 on EagleSign 2. We briefly describe certain important part of the EagleSign 2 signature which is sufficient to launch the statistical attack. For more details on the EagleSign signature, please refer to [4].

In this section, we use the same notation as in [4]. In the EagleSign 2 signature, we have

$$\mathbf{z} = \mathbf{Gu}, \qquad \mathbf{u} = \mathbf{y}_1 + \mathbf{c}, \qquad \mathbf{w} = \mathbf{y}_2 - \mathbf{Du},$$

where $\mathbf{G}$ and $\mathbf{D}$ are secret key uniformly chosen from $S_1^{l\times l}$ and $S_1^{k\times l}$ respectively, $\mathbf{y}_1 \in B^l_{t,\eta_{y_1}}$, $\mathbf{y}_2 \in B^k_{t,\eta_{y_2}}$ and $\mathbf{c} \in B^l_\tau$ is an output of a hash function depending on the message and some other inputs. Therefore,

$$\mathbf{z} = \mathbf{Gy}_1 + \mathbf{Gc}, \qquad \mathbf{w} = \mathbf{y}_2 - \mathbf{Dy}_1 - \mathbf{Dc}.$$

The above signature $\mathbf{z}$ and $\mathbf{w}$ are without aborts. Hence, the secret key $\mathbf{G}$ and $\mathbf{D}$ can be recovered by applying the technique given in Section 3.2. After recovering $\mathbf{G}$ and $\mathbf{D}$, one can easily recover another secret key $\mathbf{A}$ from the public key $\mathbf{E}$ as $\mathbf{A} = \mathbf{EG} - \mathbf{D}$. The EagleSign signature uses $n = 1024$ and $q = 12289$. The simulation results on the following parameters are given as follows.

Table 2 Timing results of our proof-of-concept Sagemath implementation of the attack on EagleSign

Level	k	l	τ	t	η_{y_1}	η_{y_2}	σ_z	σ_w	N	N_{exp}	Time
3	1	1	38	140	1	64	10.8934	17.5991	663	665	104.67 sec
5	1	2	18	86	1	32	11.7756	12.9881	762	765	151.63 sec

Note:

(1) σ_z is the standard deviation of $\mathbf{z}$ and is equal to $\sqrt{\frac{2}{3}(\tau+t)l}$.

(2) σ_w is the standard deviation of $\mathbf{w}$ and is equal to $\sqrt{\frac{2}{3}(\tau+t)l+\frac{t(\eta_{y_2}+1)(2\eta_{y_2}+1)}{6n}}$.

(3) N is the number of required signatures, which is computed using Equation (4) as $N=\left\lceil\left(\frac{Z\cdot\sigma_w}{0.49}\right)^2/\tau\right\rceil$, where $Z=4.4171$.

(4) N_{exp} is the number of signatures used in our proof-of-concept experiment.

(5) Time is the time taken to recover the secret key of $\mathbf{G},\mathbf{D}$ in the experiment.

4 Schnorr-type Signatures with Aborts

Let $\beta=\eta\tau$, γ and δ be positive integers and $0<\beta\ll B=\gamma-\delta<q_1$. We shall consider the following setting of Schnorr-type lattice-based signature with aborts as $\mathbf{s}=\mathbf{u}+\mathbf{ce}\in\mathcal{R}_q$, where $\mathbf{e}\in S_\eta$ is a (long-term) secret key, $\mathbf{u}$ is chosen randomly from S_γ, $\mathbf{c}\in B_\tau$ is an output of a hash function depending on the message and some other inputs, and we impose the condition that $\|\mathbf{s}\|_\infty\le B=\gamma-\delta$ (i.e. if $\|\mathbf{s}\|_\infty>B=\gamma-\delta$, then the signature is aborted and the signer repeats the signature generation process). The idea of introducing aborts in the signature is to avoid the statistical attack described in the previous section. In this section, we analyze the expected value of $\mathbf{s}$. This will show whether it will hide or reveal the secret key $\mathbf{e}$.

In this case (where the signature is only outputted if $\|s\|_\infty\le B=\gamma-\delta$), we note that $\Pr[(w_{l+i}=k)\quad\wedge\quad(u_{l+i}=t)]$ is proportionate to $\overline{p_k}/(2\gamma+1)$ if $|t|\le\gamma$ and $|s_{l+i}|=|w_{l+i}+u_{l+i}+\epsilon_{l,i}c_le_i|\le B$; the probability is equal to 0 otherwise. As $(2\gamma+1)$ is a constant, then we may take $\Pr[(w_{l+i}=k)\quad\wedge\quad(u_{l+i}=t)]$ to be proportionate to $\overline{p_k}$ if $|t|\le\gamma$ and $|s_{l+i}|=|w_{l+i}+u_{l+i}+\epsilon_{l,i}c_le_i|\le B$. Thus,

$$\Pr[(w_{l+i}=k)\quad\wedge\quad(u_{l+i}=t)]=\begin{cases}\overline{p_k}/\mathsf{N} & \text{if } |t|\le\gamma \text{ and } |s_{l+i}|\le B,\\ 0 & \text{otherwise,}\end{cases}$$

where N is a fixed normalization factor that makes the sum of all probabilities equals to 1.

4.1 General Formula for $\mathbb{E}[s_{l+i}]$

In this section, we shall give a general formula for computing $\mathbb{E}[s_{l+i}]$ when $c_l=1$. However, due to the abort condition in the signing process, u_{l+i} and w_{l+i} are now dependent, so we may **not** have $\mathbb{E}[s_{l+i}]=\mathbb{E}[u_{l+i}]+\epsilon_{l,i}e_i+\mathbb{E}[w_{l+i}]$ anymore. We now compute $\mathbb{E}[s_{l+i}]$ as

$$\mathbb{E}[s_{l+i}] = \sum_{j=-B}^{B} j \Pr[s_{l+i} = j].$$

As $|w_{l+i}| \leq \beta - \eta$ by Lemma 6 and $s_{l+i} = w_{l+i} + u_{l+i} + \epsilon_{l,i}e_i$, we then have for any $-B \leq j \leq B$,

$$\begin{aligned}\Pr[s_{l+i} = j] &= \sum_{t'=-(\beta-\eta)}^{\beta-\eta} \Pr[(w_{l+i} = t') \quad \wedge \quad (u_{l+i} + \epsilon_{l,i}e_i = j - t')] \\ &= \sum_{t=j-\beta+\eta}^{j+\beta-\eta} \Pr[(w_{l+i} = j - t) \quad \wedge \quad (u_{l+i} + \epsilon_{l,i}e_i = t)],\end{aligned}$$

and

$$\begin{aligned}\Pr[(w_{l+i} = j - t) \quad \wedge \quad (u_{l+i} + \epsilon_{l,i}e_i = t)] &= \begin{cases} \overline{p_{j-t}}/\mathsf{N} & \text{if } |t - \epsilon_{l,i}e_i| \leq \gamma, \\ 0 & \text{otherwise,} \end{cases} \\ &= \begin{cases} \overline{p_{j-t}}/\mathsf{N} & \text{if } \epsilon_{l,i}e_i - \gamma \leq t \leq \epsilon_{l,i}e_i + \gamma, \\ 0 & \text{otherwise.} \end{cases}\end{aligned}$$

Thus,

$$\mathbb{E}[s_{l+i}] = \sum_{j=-B}^{B} j \Pr[s_{l+i} = j] = \sum_{j=-B}^{B} \left(j \sum_{t=\max\{j-\beta+\eta,\ \epsilon_{l,i}e_i-\gamma\}}^{\min\{j+\beta-\eta,\ \epsilon_{l,i}e_i+\gamma\}} \overline{p_{j-t}} \right) /\mathsf{N}. \tag{5}$$

Since $\gamma = B + \delta$, by Equation (5), we have

$$\begin{aligned}\mathbb{E}[s_{l+i}] &= \sum_{j=-B}^{B} \left(j \sum_{t=\max\{\epsilon_{l,i}e_i-B-\delta,\ j-\beta+\eta\}}^{\min\{\epsilon_{l,i}e_i+B+\delta,\ j+\beta-\eta\}} \overline{p_{j-t}} \right) /\mathsf{N} \\ &= \sum_{j=-B}^{B} \sum_{t=\max\{\epsilon_{l,i}e_i-B-\delta,\ -B-\beta+\eta\}}^{\min\{\epsilon_{l,i}e_i+B+\delta,\ B+\beta-\eta\}} j\overline{p_{j-t}}/\mathsf{N} \\ &\qquad \text{(as } \overline{p_k} = 0 \text{ if } |k| > \beta - \eta \text{ by Remark 1(i))} \\ &= \sum_{t=\max\{\epsilon_{l,i}e_i-B-\delta,\ -B-\beta+\eta\}}^{\min\{\epsilon_{l,i}e_i+B+\delta,\ B+\beta-\eta\}} \sum_{j=-B}^{B} j\overline{p_{j-t}}/\mathsf{N} \\ &= \sum_{t=\max\{\epsilon_{l,i}e_i-B-\delta,\ -B-\beta+\eta\}}^{\min\{\epsilon_{l,i}e_i+B+\delta,\ B+\beta-\eta\}} f(t)/\mathsf{N},\end{aligned}$$

where $f(t) := \sum_{j=-B}^{B} j\overline{p_{j-t}}$.

We now compute the normalization factor N as follows:

$$\begin{aligned}
\mathsf{N} &= \sum_{j=-B}^{B} \sum_{t=\max\{\epsilon_{l,i}e_i-B-\delta,\ j-\beta+\eta\}}^{\min\{\epsilon_{l,i}e_i+B+\delta,\ j+\beta-\eta\}} \overline{p_{j-t}} \\
&= \sum_{j=-B}^{B} \sum_{t=\max\{\epsilon_{l,i}e_i-B-\delta,\ -B-\beta+\eta\}}^{\min\{\epsilon_{l,i}e_i+B+\delta,\ B+\beta-\eta\}} \overline{p_{j-t}} \\
&= \sum_{t=\max\{\epsilon_{l,i}e_i-B-\delta,\ -B-\beta+\eta\}}^{\min\{\epsilon_{l,i}e_i+B+\delta,\ B+\beta-\eta\}} \sum_{j=-B}^{B} \overline{p_{j-t}} \\
&= \sum_{t=\max\{\epsilon_{l,i}e_i-B-\delta,\ -B-\beta+\eta\}}^{\min\{\epsilon_{l,i}e_i+B+\delta,\ B+\beta-\eta\}} \sum_{j=-B-t}^{B-t} \overline{p_j} \\
&= \sum_{t=\max\{\epsilon_{l,i}e_i-B-\delta,\ -B-\beta+\eta\}}^{\min\{\epsilon_{l,i}e_i+B+\delta,\ B+\beta-\eta\}} g(t),
\end{aligned}$$

where

$$g(t) := \sum_{j=-B-t}^{B-t} \overline{p_j}.$$

We have thus shown the following result.

Proposition 1. *Suppose $B = \gamma - \delta$ for some $\delta > 0$. Then*

$$\mathbb{E}[s_{l+i}] = \left(\sum_{t=\max\{\epsilon_{l,i}e_i-B-\delta,\ -B-\beta+\eta\}}^{\min\{\epsilon_{l,i}e_i+B+\delta,\ B+\beta-\eta\}} f(t) \right) \Big/ \left(\sum_{t=\max\{\epsilon_{l,i}e_i-B-\delta,\ -B-\beta+\eta\}}^{\min\{\epsilon_{l,i}e_i+B+\delta,\ B+\beta-\eta\}} g(t) \right),$$

where $f(t) := \sum_{j=-B}^{B} j\overline{p_{j-t}}$ and $g(t) := \sum_{j=-B-t}^{B-t} \overline{p_j}$ for any $t \in \mathbb{Z}$.

Remark 4. *We have*

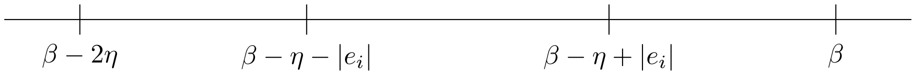
(i) $\min\{\epsilon_{l,i}e_i + B + \delta,\ B + \beta - \eta\} = B + \beta - \eta$ *if and only if* $\delta \geq \beta - \eta - \epsilon_{l,i}e_i$.

(ii) $\min\{\epsilon_{l,i}e_i + B + \delta,\ B + \beta - \eta\} = \epsilon_{l,i}e_i + B + \delta$ *if and only if* $\delta \leq \beta - \eta - \epsilon_{l,i}e_i$.

(iii) $\max\{\epsilon_{l,i}e_i - B - \delta,\ -B - \beta - \eta\} = -B - \beta + \eta$ *if and only if* $\delta \geq \beta - \eta + \epsilon_{l,i}e_i$.

(iv) $\max\{\epsilon_{l,i}e_i - B - \delta,\ -B - \beta - \eta\} = \epsilon_{l,i}e_i - B - \delta$ *if and only if* $\delta \leq \beta - \eta + \epsilon_{l,i}e_i$.

We now divide into a few cases depending on the value of δ.



4.2 Case 1: $\delta \geq \beta - \eta + |e_i|$ (including $\delta \geq \beta$)

In this section, we consider the case when $B = \gamma - \delta$ for some $\delta \geq \beta - \eta + |e_i|$. Note that as $\mathbf{e} \in S_\eta$, we have $\beta \geq \beta - \eta + |e_i|$. So, this case includes in particular the situation when $\delta \geq \beta$. We shall show that $\mathbb{E}[s_{l+i}] = 0$ in this case. We start by proving the following properties of $f(t)$.

Lemma 7. *For $t \in \mathbb{Z}$, define $f(t) := \sum_{j=-B}^{B} j\overline{p_{j-t}}$. Then*

(a) $f(0) = 0$*;*

(b) $f(-t) = -f(t)$ *for any* $t \in \mathbb{Z}$*.*

Proof. For (a), note that since $\overline{p_{-j}} = \overline{p_j}$ for any j, then we have

$$\begin{aligned} f(0) &= \sum_{j=-B}^{B} j\overline{p_j} = \sum_{j=-B}^{-1} j\overline{p_j} + 0 + \sum_{j=1}^{B} j\overline{p_j} \\ &= \sum_{j=1}^{B} (-j)\overline{p_{-j}} + \sum_{j=1}^{B} j\overline{p_j} \\ &= -\sum_{j=1}^{B} j\overline{p_j} + \sum_{j=1}^{B} j\overline{p_j} \qquad (\text{since } \overline{p_{-j}} = \overline{p_j}) \\ &= 0. \end{aligned}$$

As for (b),

$$\begin{aligned} f(-t) &= \sum_{j=-B}^{B} j\overline{p_{j+t}} = \sum_{j=-B}^{B} (-j)\overline{p_{-j+t}} = -\sum_{j=-B}^{B} j\overline{p_{-(j-t)}} \\ &= -\sum_{j=-B}^{B} j\overline{p_{j-t}} \qquad (\text{since } \overline{p_{-(j-t)}} = \overline{p_{j-t}}) \\ &= -f(t). \end{aligned}$$

□

Theorem 3. *If $\delta \geq \beta - \eta + |e_i|$, then $\mathbb{E}[s_{l+i}] = 0$. In particular, $\mathbb{E}[s_{l+i}] = 0$ if $\delta \geq \beta$.*

Proof. As $\delta \geq \beta - \eta + |e_i| \geq \beta - \eta - |e_i|$, therefore, by Proposition 1 and Remark 4(i), (iii), we have

$$\begin{aligned} \mathbb{E}[s_{l+i}] &= \left(\sum_{t=\max\{\epsilon_{l,i}e_i - B - \delta,\ -B-\beta+\eta\}}^{\min\{\epsilon_{l,i}e_i + B + \delta,\ B+\beta-\eta\}} f(t) \right) / \mathsf{N} \\ &= \sum_{t=-(B+\beta-\eta)}^{B+\beta-\eta} f(t) / \mathsf{N} \\ &= \left(\sum_{t=-(B+\beta-\eta)}^{-1} f(t) + f(0) + \sum_{t=1}^{B+\beta-\eta} f(t) \right) / \mathsf{N} \end{aligned}$$

$$
\begin{aligned}
&= \left(\sum_{t=1}^{B+\beta-\eta} f(-t) + f(0) + \sum_{t=1}^{B+\beta-\eta} f(t) \right) / \mathsf{N} \\
&= \left(- \sum_{t=1}^{B+\beta-\eta} f(t) + 0 + \sum_{t=1}^{B+\beta-\eta} f(t) \right) / \mathsf{N} \qquad \text{(by Lemma 7)} \\
&= 0.
\end{aligned}
$$

□

Note that if $\delta \geq \beta$, then by Theorem 3, we have $\mathbb{E}[s_{l+i}] = 0$ (independent of the value of e_i). We conclude that if $\delta \geq \beta$, then $\mathbf{e}$ cannot be recovered using the method given in Algorithm 1.

4.3 Case 2: $0 < \delta \leq \beta - \eta - |e_i|$ (including $0 < \delta \leq \beta - 2\eta$)

In this section, we shall simplify the formula for $\mathbb{E}[s_{l+i}]$ given in Proposition 1 in the case when $B = \gamma - \delta$ for some $0 < \delta \leq \beta - \eta - |e_i|$. We start by proving the following properties of $g(t)$.

Lemma 8. *For $t \in \mathbb{Z}$, define $g(t) := \sum_{j=-B-t}^{B-t} \overline{p_j}$. Then*

(a) If $t > B + \beta - \eta$, then $g(t) = 0$.
(b) If $t < -B - \beta + \eta$, then $g(t) = 0$.
(c) If $-(B - \beta + \eta) \leq t \leq B - \beta + \eta$, then $g(t) = 1$.
(d) For any $t \geq 1$, we have $g(t) = g(-t)$.

Proof. For (a), note that if $t > B + \beta - \eta$, then for any $j \in [-B - t, B - t]$ we have $j < -(\beta - \eta)$ and so $\overline{p_j} = 0$ by Remark 1(i). Thus, $g(t) = 0$. Similarly, for (b), we note that if $t < -B - \beta + \eta$, then for any $j \in [-B - t, B - t]$ we have $j > \beta - \eta$ and so $\overline{p_j} = 0$ by Remark 1(i). Consequently, $g(t) = 0$ in this case as well.

For (c), if $-(B - \beta + \eta) \leq t \leq B - \beta + \eta$, then $-B - t \leq -(\beta - \eta) < \beta - \eta \leq B - t$. It then follows from Remark 1(i), (ii) that

$$
g(t) = \sum_{j=-B-t}^{B-t} \overline{p_j} = \sum_{-(\beta-\eta)}^{\beta-\eta} \overline{p_j} = 1.
$$

For (d), as $\overline{p_j} = \overline{p_{-j}}$ for any j, we have

$$
g(-t) = \sum_{j=-B+t}^{B+t} \overline{p_j} = \sum_{j=-(B+t)}^{-(-B+t)} \overline{p_{-j}} = \sum_{j=-B-t}^{B-t} \overline{p_j} = g(t).
$$

□

Suppose $0 < \delta \leq \beta - \eta - |e_i|$. Then by Remark 4(ii), (iv), the numerator in Proposition 1 becomes

$$\begin{aligned}
\sum_{t=\max\{\epsilon_{l,i}e_i-B-\delta,\ -B-\beta+\eta\}}^{\min\{\epsilon_{l,i}e_i+B+\delta,\ B+\beta-\eta\}} f(t) &= \sum_{t=-(B+\delta-\epsilon_{l,i}e_i)}^{B+\delta+\epsilon_{l,i}e_i} f(t) \\
&= \sum_{t=1}^{B+\delta+\epsilon_{l,i}e_i} f(t) - \sum_{t=1}^{B+\delta-\epsilon_{l,i}e_i} f(t) \quad \text{(by Lemma 7)} \\
&= \begin{cases} 0 & \text{if } e_i = 0 \\ \displaystyle\sum_{t=B+\delta-\epsilon_{l,i}e_i+1}^{B+\delta+\epsilon_{l,i}e_i} f(t) & \text{if } \epsilon_{l,i}e_i > 0 \\ \displaystyle -\sum_{t=B+\delta+\epsilon_{l,i}e_i+1}^{B+\delta-\epsilon_{l,i}e_i} f(t) & \text{if } \epsilon_{l,i}e_i < 0. \end{cases}
\end{aligned}$$

On the other hand, in this case (where $0 < \delta \leq \beta - \eta - |e_i|$), by Remark 4(ii), (iv), the normalization factor is

$$\begin{aligned}
\sum_{t=-(B+\delta-\epsilon_{l,i}e_i)}^{B+\delta+\epsilon_{l,i}e_i} g(t) &= \sum_{t=-(B+\delta-\epsilon_{l,i}e_i)}^{-(B-\beta+\eta+1)} g(t) + \sum_{t=-(B-\beta+\eta)}^{B-\beta+\eta} 1 + \sum_{t=B-\beta+\eta+1}^{B+\delta+\epsilon_{l,i}e_i} g(t) \quad \text{(by Lemma 8(c))} \\
&= 2B - 2\beta + 2\eta + 1 + \sum_{t=-(B+\delta-\epsilon_{l,i}e_i)}^{-(B-\beta+\eta+1)} g(t) + \sum_{t=B-\beta+\eta+1}^{B+\delta+\epsilon_{l,i}e_i} g(t) \\
&= 2B - 2\beta + 2\eta + 1 + \sum_{t=B-\beta+\eta+1}^{B+\delta-\epsilon_{l,i}e_i} g(t) + \sum_{t=B-\beta+\eta+1}^{B+\delta+\epsilon_{l,i}e_i} g(t) \quad \text{(by Lemma 8(d))} \\
&= \begin{cases} 2B - 2\beta + 2\eta + 1 + 2\displaystyle\sum_{t=B-\beta+\eta+1}^{B+\delta-\epsilon_{l,i}e_i} g(t) + \sum_{t=B+\delta-\epsilon_{l,i}e_i+1}^{B+\delta+\epsilon_{l,i}e_i} g(t) & \text{if } \epsilon_{l,i}e_i \geq 0 \\ 2B - 2\beta + 2\eta + 1 + 2\displaystyle\sum_{t=B-\beta+\eta+1}^{B+\delta+\epsilon_{l,i}e_i} g(t) + \sum_{t=B+\delta+\epsilon_{l,i}e_i+1}^{B+\delta-\epsilon_{l,i}e_i} g(t) & \text{if } \epsilon_{l,i}e_i < 0. \end{cases}
\end{aligned}$$

Combining the above with Proposition 1, we have thus shown the following result.

Lemma 9. *Suppose $B = \gamma - \delta$ for some δ satisfying $0 < \delta \leq \beta - \eta - |e_i|$.*

- *If $e_i = 0$, then $\mathbb{E}[s_{l+i}] = 0$.*
- *If $\epsilon_{l,i}e_i > 0$, then*

$$\mathbb{E}[s_{l+i}] = \left(\sum_{t=B+\delta-\epsilon_{l,i}e_i+1}^{B+\delta+\epsilon_{l,i}e_i} f(t) \right) \Big/ \left(2B - 2\beta + 2\eta + 1 + 2\sum_{t=B-\beta+\eta+1}^{B+\delta-\epsilon_{l,i}e_i} g(t) + \sum_{t=B+\delta-\epsilon_{l,i}e_i+1}^{B+\delta+\epsilon_{l,i}e_i} g(t) \right);$$

- *if $\epsilon_{l,i}e_i < 0$, then*

$$\mathbb{E}[s_{l+i}] = -\left(\sum_{t=B+\delta+\epsilon_{l,i}e_i+1}^{B+\delta-\epsilon_{l,i}e_i} f(t)\right) / \left(2B-2\beta+2\eta+1+2\sum_{t=B-\beta+\eta+1}^{B+\delta+\epsilon_{l,i}e_i} g(t) + \sum_{t=B+\delta+\epsilon_{l,i}e_i+1}^{B+\delta-\epsilon_{l,i}e_i} g(t)\right),$$

where $f(t) := \sum_{j=-B}^{B} j\overline{p_{j-t}}$ and $g(t) := \sum_{j=-B-t}^{B-t}\overline{p_j}$ for any $t \in \mathbb{Z}$.

In particular, the above formulas hold when $\delta \leq \beta - 2\eta$.

We now explore further properties of $f(t) = \sum_{j=-B}^{B} j\overline{p_{j-t}} = \sum_{j=-B-t}^{B-t}(j+t)\overline{p_j}$ and $g(t) = \sum_{j=-B-t}^{B-t}\overline{p_j}$.

Lemma 10. *If $\beta - \eta - 2B \leq k \leq \beta - \eta$, then*

$$f(B+k) = B\sum_{j=k}^{\beta-\eta}\overline{p_j} - \sum_{j=k}^{\beta-\eta}(j-k)\overline{p_j} \approx B\sum_{j=k}^{\beta-\eta}\overline{p_j},$$

and

$$g(B+k) = \sum_{j=k}^{\beta-\eta}\overline{p_j}.$$

Proof. We have

$$\begin{aligned}
f(B+k) &= \sum_{j=-2B-k}^{-k}(j+B+k)\overline{p_j}\\
&= \sum_{j=-(\beta-\eta)}^{-k}(j+B+k)\overline{p_j} \qquad (\text{as } \beta-\eta-2B \leq k)\\
&= \sum_{j=k}^{\beta-\eta}(B+k-j)\overline{p_j} = B\sum_{j=k}^{\beta-\eta}\overline{p_j} + \sum_{j=k}^{\beta-\eta}(k-j)\overline{p_j}\\
&= B\sum_{j=k}^{\beta-\eta}\overline{p_j} - \sum_{j=k}^{\beta-\eta}(j-k)\overline{p_j}\\
&\approx B\sum_{j=k}^{\beta-\eta}\overline{p_j}.
\end{aligned}$$

We also note that

$$g(B+k) = \sum_{j=-2B-k}^{-k}\overline{p_j} = \sum_{j=-(\beta-\eta)}^{-k}\overline{p_j} = \sum_{j=k}^{\beta-\eta}\overline{p_j}.$$

□

The following corollaries are direct consequences of Lemma 10.

Corollary 1. *If $\delta + |e_i| \leq \beta - \eta$, then*

$$\sum_{t=B+\delta-|e_i|+1}^{B+\delta+|e_i|} f(t) = B \sum_{k=\delta-|e_i|+1}^{\delta+|e_i|} \sum_{j=k}^{\beta-\eta} \overline{p_j} - \sum_{k=\delta-|e_i|+1}^{\delta+|e_i|} \sum_{j=k}^{\beta-\eta} (j-k)\overline{p_j} \approx B \sum_{k=\delta-|e_i|+1}^{\delta+|e_i|} \sum_{j=k}^{\beta-\eta} \overline{p_j}.$$

Corollary 2. *If $\delta - |e_i| \leq \beta - \eta$, then*

$$\sum_{t=B-\beta+\eta+1}^{B+\delta-|e_i|} g(t) = \sum_{k=-(\beta-\eta-1)}^{\delta-|e_i|} \sum_{j=k}^{\beta-\eta} \overline{p_j}.$$

Corollary 3. *If $\delta + |e_i| \leq \beta - \eta$, then*

$$\sum_{t=B+\delta-|e_i|+1}^{B+\delta+|e_i|} g(t) = \sum_{k=\delta-|e_i|+1}^{\delta+|e_i|} \sum_{j=k}^{\beta-\eta} \overline{p_j}.$$

Theorem 4. *Suppose $B = \gamma - \delta$ for some δ satisfying $0 < \delta \leq \beta - \eta - |e_i|$.*

- *If $e_i = 0$, then $\mathbb{E}[s_{l+i}] = 0$.*
- *If $\epsilon_{l,i} e_i > 0$, then*

$$\begin{aligned}\mathbb{E}[s_{l+i}] &= \frac{B \sum_{k=\delta-\epsilon_{l,i}e_i+1}^{\delta+\epsilon_{l,i}e_i} \sum_{j=k}^{\beta-\eta} \overline{p_j} - \sum_{k=\delta-\epsilon_{l,i}e_i+1}^{\delta+\epsilon_{l,i}e_i} \sum_{j=k}^{\beta-\eta} (j-k)\overline{p_j}}{2B - 2\beta + 2\eta + 1 + 2 \sum_{k=-(\beta-\eta-1)}^{\delta-\epsilon_{l,i}e_i} \sum_{j=k}^{\beta-\eta} \overline{p_j} + \sum_{k=\delta-\epsilon_{l,i}e_i+1}^{\delta+\epsilon_{l,i}e_i} \sum_{j=k}^{\beta-\eta} \overline{p_j}} \\ &\approx \left(\sum_{k=\delta-|e_i|+1}^{\delta+|e_i|} \sum_{j=k}^{\beta-\eta} \overline{p_j} \right) /2.\end{aligned}$$

- *If $\epsilon_{l,i} e_i < 0$, then*

$$\begin{aligned}\mathbb{E}[s_{l+i}] &= \frac{-B \sum_{k=\delta+\epsilon_{l,i}e_i+1}^{\delta-\epsilon_{l,i}e_i} \sum_{j=k}^{\beta-\eta} \overline{p_j} - \sum_{k=\delta+\epsilon_{l,i}e_i+1}^{\delta-\epsilon_{l,i}e_i} \sum_{j=k}^{\beta-\eta} (j-k)\overline{p_j}}{2B - 2\beta + 2\eta + 1 + 2 \sum_{k=-(\beta-\eta-1)}^{\delta+\epsilon_{l,i}e_i} \sum_{j=k}^{\beta-\eta} \overline{p_j} + \sum_{k=\delta+\epsilon_{l,i}e_i+1}^{\delta-\epsilon_{l,i}e_i} \sum_{j=k}^{\beta-\eta} \overline{p_j}} \\ &\approx -\left(\sum_{k=\delta-|e_i|+1}^{\delta+|e_i|} \sum_{j=k}^{\beta-\eta} \overline{p_j} \right) /2.\end{aligned}$$

Proof. This is a direct consequence of Lemma 9 and Corollaries 1, 2, 3. □

Remark 5. *It is clear from Theorem 4 that $\mathbb{E}[s_{l+i}] \neq 0$ when $e_i \neq 0$ in this case. Moreover, we observe that $\mathbb{E}[s_{l+i}]$ for $\epsilon_{l,i}e_i < 0$ is equal to $-\mathbb{E}[s_{l+i}]$ for $\epsilon_{l,i}e_i > 0$.*

4.4 Case 3: $\beta - \eta - |e_i| < \delta < \beta - \eta + |e_i|$

In this section, we consider the case when $B = \gamma - \delta$ for some δ satisfying $\beta - \eta - |e_i| < \delta < \beta - \eta + |e_i|$. Note that $e_i \neq 0$ in this case. The situation when $e_i = 0$ (in which case we have $\mathbb{E}[s_{l+i}] = 0$ by Theorems 3 and 4) has been fully covered in Sections 4.2 and 4.3. We then only need to split into two subcases depending on whether $\epsilon_{l,i}e_i > 0$ or $\epsilon_{l,i}e_i < 0$.

4.4.1 $\epsilon_{l,i}e_i > 0$

Proposition 2. *Suppose $\beta - \eta - \epsilon_{l,i}e_i < \delta < \beta - \eta + \epsilon_{l,i}e_i$ (and $\epsilon_{l,i}e_i > 0$). Then*

$$\mathbb{E}[s_{l+i}] = \frac{B \displaystyle\sum_{k=\delta-|e_i|+1}^{\beta-\eta} \sum_{j=k}^{\beta-\eta} \overline{p_j} - \sum_{k=\delta-|e_i|+1}^{\beta-\eta} \sum_{j=k}^{\beta-\eta} (j-k)\overline{p_j}}{(2B - 2\beta + 2\eta + 1) + 2 \displaystyle\sum_{k=-\beta+\eta+1}^{\delta-|e_i|} \sum_{j=k}^{\beta-\eta} \overline{p_j} + \sum_{k=\delta-|e_i|+1}^{\beta-\eta} \sum_{j=k}^{\beta-\eta} \overline{p_j}}$$
$$\approx \left(\sum_{k=\delta-|e_i|+1}^{\beta-\eta} \sum_{j=k}^{\beta-\eta} \overline{p_j} \right) /2.$$

Proof. As $\beta - \eta - \epsilon_{l,i}e_i < \delta < \beta - \eta + \epsilon_{l,i}e_i$, by Remark 4(i), (iv), the numerator in Proposition 1 becomes

$$\begin{aligned}
\sum_{t=\max\{\epsilon_{l,i}e_i - B - \delta,\ -B-\beta+\eta\}}^{\min\{\epsilon_{l,i}e_i + B + \delta,\ B+\beta-\eta\}} f(t) &= \sum_{t=-B-\delta+\epsilon_{l,i}e_i}^{B+\beta-\eta} f(t) \quad = \sum_{t=-B-\delta+|e_i|}^{B+\beta-\eta} f(t) \\
&= \sum_{t=1}^{B+\delta-|e_i|} f(-t) + f(0) + \sum_{t=1}^{B+\beta-\eta} f(t) \\
&= -\sum_{t=1}^{B+\delta-|e_i|} f(t) + \sum_{t=1}^{B+\beta-\eta} f(t) \qquad \text{(by Lemma 7)} \\
&= \sum_{t=B+\delta-|e_i|+1}^{B+\beta-\eta} f(t) \\
&= \sum_{k=\delta-|e_i|+1}^{\beta-\eta} f(B+k) \\
&= B \sum_{k=\delta-|e_i|+1}^{\beta-\eta} \sum_{j=k}^{\beta-\eta} \overline{p_j} - \sum_{k=\delta-|e_i|+1}^{\beta-\eta} \sum_{j=k}^{\beta-\eta} (j-k)\overline{p_j},
\end{aligned}$$

where the last equality follows from Lemma 10.

Moreover, Remark 4(i), (iv) also implies that the normalization factor N in Proposition 1 becomes

$$\begin{aligned}
\sum_{t=\max\{\epsilon_{l,i}e_i-B-\delta,\ -B-\beta+\eta\}}^{\min\{\epsilon_{l,i}e_i+B+\delta,\ B+\beta-\eta\}} g(t) &= \sum_{t=-B-\delta+\epsilon_{l,i}e_i}^{B+\beta-\eta} g(t) \quad = \sum_{t=-B-\delta+|e_i|}^{B+\beta-\eta} g(t) \\
&= \sum_{t=-(B+\delta-|e_i|)}^{-B+\beta-\eta-1} g(t) + \sum_{t=-(B-\beta+\eta)}^{B-\beta+\eta} 1 + \sum_{t=B-\beta+\eta+1}^{B+\beta-\eta} g(t) \qquad \text{(by Lemma 8)} \\
&= (2B-2\beta+2\eta+1) + \sum_{t=B-\beta+\eta+1}^{B+\delta-|e_i|} g(t) + \sum_{t=B-\beta+\eta+1}^{B+\beta-\eta} g(t) \\
&= (2B-2\beta+2\eta+1) + 2\sum_{t=B-\beta+\eta+1}^{B+\delta-|e_i|} g(t) + \sum_{t=B+\delta-|e_i|+1}^{B+\beta-\eta} g(t) \\
&= (2B-2\beta+2\eta+1) + 2\sum_{k=-\beta+\eta+1}^{\delta-|e_i|} g(B+k) + \sum_{k=\delta-|e_i|+1}^{\beta-\eta} g(B+k) \\
&= (2B-2\beta+2\eta+1) + 2\sum_{k=-\beta+\eta+1}^{\delta-|e_i|} \sum_{j=k}^{\beta-\eta} \overline{p_j} + \sum_{k=\delta-|e_i|+1}^{\beta-\eta} \sum_{j=k}^{\beta-\eta} \overline{p_j},
\end{aligned}$$

where the last equality follows from Lemma 10.

The proof is then concluded by applying Proposition 1. □

4.4.2 $\epsilon_{l,i}e_i < 0$

Proposition 3. *Suppose $\beta-\eta+\epsilon_{l,i}e_i < \delta < \beta-\eta-\epsilon_{l,i}e_i$ (and $\epsilon_{l,i}e_i < 0$). Then*

$$\begin{aligned}
\mathbb{E}[s_{l+i}] &= \frac{-B\displaystyle\sum_{k=\delta-|e_i|+1}^{\beta-\eta}\sum_{j=k}^{\beta-\eta}\overline{p_j} + \sum_{k=\delta-|e_i|+1}^{\beta-\eta}\sum_{j=k}^{\beta-\eta}(j-k)\overline{p_j}}{(2B-2\beta+2\eta+1) + 2\displaystyle\sum_{t=-\beta+\eta+1}^{\delta-|e_i|}\sum_{j=k}^{\beta-\eta}\overline{p_j} + \sum_{t=\delta-|e_i|+1}^{\beta-\eta}\sum_{j=k}^{\beta-\eta}\overline{p_j}} \\
&\approx -\left(\sum_{k=\delta-|e_i|+1}^{\beta-\eta}\sum_{j=k}^{\beta-\eta}\overline{p_j}\right)/2.
\end{aligned}$$

Proof. As $\beta - \eta + \epsilon_{l,i}e_i < \delta < \beta - \eta - \epsilon_{l,i}e_i$, by Remark 4(ii), (iii), the numerator in Proposition 1 becomes

$$\begin{aligned}
\sum_{t=\max\{\epsilon_{l,i}e_i - B-\delta,\ -B-\beta+\eta\}}^{\min\{\epsilon_{l,i}e_i+B+\delta,\ B+\beta-\eta\}} f(t) &= \sum_{-B-\beta+\eta}^{B+\delta+\epsilon_{l,i}e_i} f(t) \quad = \sum_{-B-\beta+\eta}^{B+\delta-|e_i|} f(t) \\
&= \left[\sum_{t=1}^{B+\beta-\eta} f(-t) + f(0) + \sum_{t=1}^{B+\delta-|e_i|} f(t)\right] \\
&= \left[-\sum_{t=1}^{B+\beta-\eta} f(t) + \sum_{t=1}^{B+\delta-|e_i|} f(t)\right] \qquad \text{(by Lemma 7)} \\
&= -\sum_{t=B+\delta-|e_i|+1}^{B+\beta-\eta} f(t) \\
&= -\sum_{k=\delta-|e_i|+1}^{\beta-\eta} f(B+k) \\
&= -B\sum_{k=\delta-|e_i|+1}^{\beta-\eta}\sum_{j=k}^{\beta-\eta}\overline{p_j} + \sum_{k=\delta-|e_i|+1}^{\beta-\eta}\sum_{j=k}^{\beta-\eta}(j-k)\overline{p_j},
\end{aligned}$$

where the last equality follows from Lemma 10.

Moreover, Remark 4(ii), (iii) also implies that the normalization factor N in Proposition 1 becomes

$$\begin{aligned}
\sum_{t=\max\{\epsilon_{l,i}e_i - B-\delta,\ -B-\beta+\eta\}}^{\min\{\epsilon_{l,i}e_i+B+\delta,\ B+\beta-\eta\}} g(t) &= \sum_{-B-\beta+\eta}^{B+\delta+\epsilon_{l,i}e_i} g(t) \quad = \sum_{-B-\beta+\eta}^{B+\delta-|e_i|} g(t) \\
&= \sum_{t=-(B+\beta-\eta)}^{-B+\beta-\eta-1} g(t) + \sum_{t=-(B-\beta+\eta)}^{B-\beta+\eta} 1 + \sum_{t=B-\beta+\eta+1}^{B+\delta-|e_i|} g(t) \qquad \text{(by Lemma 8)} \\
&= (2B-2\beta+2\eta+1) + \sum_{t=B-\beta+\eta+1}^{B+\beta-\eta} g(t) + \sum_{t=B-\beta+\eta+1}^{B+\delta-|e_i|} g(t) \\
&= (2B-2\beta+2\eta+1) + 2\sum_{t=B-\beta+\eta+1}^{B+\delta-|e_i|} g(t) + \sum_{t=B+\delta-|e_i|+1}^{B+\beta-\eta} g(t) \\
&= (2B-2\beta+2\eta+1) + 2\sum_{t=-\beta+\eta+1}^{\delta-|e_i|} g(B+k) + \sum_{t=\delta-|e_i|+1}^{\beta-\eta} g(B+k) \\
&= (2B-2\beta+2\eta+1) + 2\sum_{t=-\beta+\eta+1}^{\delta-|e_i|}\sum_{j=k}^{\beta-\eta}\overline{p_j} + \sum_{t=\delta-|e_i|+1}^{\beta-\eta}\sum_{j=k}^{\beta-\eta}\overline{p_j},
\end{aligned}$$

where the last equaltiy follows from Lemma 10.

The proof is then concluded by applying Proposition 1. □

Remark 6. *Comparing Propositions 2 and 3, we see that* $\mathbb{E}[s_{l+i}]$ *for* $\epsilon_{l,i}e_i < 0$ *is equal to* $-\mathbb{E}[s_{l+i}]$ *for* $\epsilon_{l,i}e_i > 0$*.*

Remark 7. *From Propositions 2 and 3, we see that* $\mathbb{E}[s_{l+i}]$ *can be approximated as a sum of* $(\beta + |e_i| - \eta - \delta)$ *terms when* $\beta - \eta - |e_i| < \delta < \beta - \eta + |e_i|$*, where each term is of the form* $\sum_{j=k}^{\beta-\eta} \overline{p_j}$*. Together with Theorems 3 and 4, the number of terms in* $\mathbb{E}[s_{l+i}]$ *for various* δ *and* $\epsilon_{l,i}e_i$ *are given in the following table.*

	$e_i = 0$	$\epsilon_{l,i}e_i = 1$	$\epsilon_{l,i}e_i = 2$	$\dots$	$\epsilon_{l,i}e_i = \eta - 1$	$\epsilon_{l,i}e_i = \eta$
$\delta \geq \beta$	0	0	0	$\dots$	0	0
$\delta = \beta - 1$	0	0	0	$\dots$	0	1 term
$\delta = \beta - 2$	0	0	0	$\dots$	1	2 terms
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
$\delta = \beta - \eta$	0	1	2	$\dots$	$\eta - 1$	η terms
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
$\delta = \beta - (2\eta - 2)$	0	2	4	$\dots$	$2\eta - 3$	$2\eta - 2$ terms
$\delta = \beta - (2\eta - 1)$	0	2	4	$\dots$	$2\eta - 2$	$2\eta - 1$ terms
$\delta = \beta - 2\eta$	0	2	4	$\dots$	$2\eta - 2$	2η terms
$0 < \delta \leq \beta - 2\eta$	0	$2\|e_i\| = 2$	$2\|e_i\| = 4$	$\dots$	$2\|e_i\| = 2\eta - 2$	$2\|e_i\| = 2\eta$ terms

Table 3 Number of terms in $\mathbb{E}[s_{l+i}]$ for various values of $\epsilon_{l,i}e_i$

From Table 3 above, we observe that when $\delta \leq \beta - \eta$*, distinct values of* $\epsilon_{l,i}e_i$ *result in distinct values of* $\mathbb{E}[s_{l+i}]$*. Therefore, we can theoretically recover* $\mathbf{e}$ *completely if* $\delta \leq \beta - \eta$*.*

4.5 Normal Approximation of $\overline{p_k}$

Recall that for $k \in \mathbb{Z}$, we define

$$\overline{p_k} := \Pr[w_{l+i} = k],$$

where (from Equation (2))

$$w_{l+i} := \sum_{\substack{0 \leq j \leq n-1 \\ j \neq l}} \pm c_j e_{l+i-j}.$$

Moreover, as argued in Section 3.3, each w_{l+i} approximates to the normal distribution $\mathcal{N}(0, \sigma_{ce})$, where

$$\sigma_{ce} := \sqrt{\frac{\tau\eta(\eta + 1)}{3}}.$$

Then, for $-(\beta-\eta) \leq k \leq (\beta-\eta)$, we may estimate the value of $\overline{p_k}$ as follows:

$$\overline{p_k} := \Pr[w_{l+i} = k] = \Pr\left[w_{l+i} \in \left(k-\frac{1}{2}, k+\frac{1}{2}\right)\right] \approx \Phi\left(\frac{k+\frac{1}{2}}{\sigma_{ce}}\right) - \Phi\left(\frac{k-\frac{1}{2}}{\sigma_{ce}}\right),$$

where $\Phi(Z) := \frac{1}{\sqrt{2\pi}} \displaystyle\int_{-\infty}^{Z} e^{-t^2/2}\mathrm{d}t$.

On the other hand, as mentioned in Remark 1(i), it is clear that $\overline{p_k} = 0$ if $|k| > \beta-\eta$.

Remark 8. *We now give an estimate on the value of* $\sum_{j=k}^{\beta-\eta} \overline{p_k}$ *as follows.*

$$\begin{aligned}\sum_{j=k}^{\beta-\eta} \overline{p_k} = \Pr\left[w_{l+i} \geq k\right] \quad &= 1 - \Pr\left[w_{l+i} \leq k-1\right] \\ &= 1 - \Pr\left[w_{l+i} < k - \frac{1}{2}\right] \\ &\approx 1 - \Phi\left(\frac{k-\frac{1}{2}}{\sigma_{ce}}\right) \\ &= \Phi\left(-\frac{k-\frac{1}{2}}{\sigma_{ce}}\right).\end{aligned}$$

(i) For small k *(more precisely, if* $\left|\frac{k-\frac{1}{2}}{\sigma_{ce}}\right| < 4$*), the value of* $\Phi\left(-\frac{k-\frac{1}{2}}{\sigma_{ce}}\right)$ *can be obtained from the standard normal distribution table.*

(ii) For general k*, the value of* $\Phi\left(-\frac{k-\frac{1}{2}}{\sigma_{ce}}\right)$ *can be approximated using Lemma 4.*

4.6 Illustrative Example of Key Recovery Attack

In this section, we shall give an example to illustrate the fact that one could still perform key recovery attack on Schnorr-type signature scheme with aborts when the parameters are not carefully chosen.

Consider the following parameter: $n = 64$, $\tau = 16$, $\eta = 4$, $\gamma = 300$, $\delta = 7$, $\beta = \eta \cdot \tau = 64$, $B = \beta - \delta = 293$. Note that $7 = \delta \leq \beta - 2\eta = 56$. So, we may apply Theorem 4 to estimate $\mathbb{E}[s_{l+i}]$.

For this parameter, $\sigma_{ce} = \sqrt{\tau\eta(\eta+1)/3} = 10.3279555$. Recall from Remark 8 that $\sum_{j=k}^{\beta-\eta} \overline{p_k} \approx \Phi(-\frac{k-\frac{1}{2}}{\sigma_{ce}})$. We list the values for $\Phi(-\frac{k-\frac{1}{2}}{\sigma_{ce}})$ for $5 \leq k \leq 11$ in the following table (the values are obtained from the standard normal distribution table).

k	4	5	6	7	8	9	10	11
$-\frac{k-\frac{1}{2}}{\sigma_{ce}}$	-0.33	-0.43	-0.53	-0.62	-0.72	-0.82	-0.91	-1.01
$\sum_{j=k}^{\beta-\eta} \overline{p_k}$	0.37070	0.33360	0.29806	0.26763	0.23576	0.20611	0.18141	0.15625

Table 4 Estimate for $\sum_{j=k}^{\beta-\eta} \overline{p_k}$

For any fixed, $1 \leq \epsilon_{l,i} e_i \leq 4$, by Theorem 4, we have $\mathbb{E}[s_{l+i}] = \frac{1}{2} \sum_{k=8-\epsilon_{l,i}e_i}^{7+\epsilon_{l,i}e_i} \sum_{j=k}^{\beta-\eta} \overline{p_k}$. Using the estimate given in Table 4, we may compute $\mathbb{E}[s_{l+i}]$ for various $\epsilon_{l,i}e_i$ as follows.

$\epsilon_{l,i}e_i$	0	±1	±2	±3	±4
$\mathbb{E}[s_{l+i}]$	0	±0.251695	±0.503780	±0.761285	±1.024760

Table 5 The values of $\mathbb{E}[s_{l+i}]$ for different $\epsilon_{l,i}e_i$

Suppose we have collected a number of samples $s_{l+i}^{(1)}, s_{l+i}^{(2)}, \ldots, s_{l+i}^{(\hat{N})}$ from some known signatures. Then $\mathbb{E}[s_{l+i}]$ can be estimated as $\mathbb{E}[s_{l+i}] \approx \sum_{k=1}^{\hat{N}} s_{l+i}^{(k)}/\hat{N}$. One may then recover e_i as follows:

$\epsilon_{l,i} \sum_{k=1}^{\hat{N}} s_{l+i}^{(k)}/\hat{N}$	e_i
> 0.88	4
$(0.62, 0.88]$	3
$(0.37, 0.62]$	2
$(0.12, 0.37]$	1
$[-0.12, 0.12]$	0
$[-0.37, -0.12)$	-1
$[-0.62, -0.37)$	-2
$[-0.88, -0.62)$	-3
< -0.88	-4

Table 6 Recovering e_i from $\sum_{k=1}^{\hat{N}} s_{l+i}^{(k)}/\hat{N}$

Due to the abort condition, we have $\mathbf{s} \in S_B$. The standard deviation of $\mathbf{s}$ can be approximated as

$$\sigma_s \approx \sqrt{\frac{B(B+1)}{3}} = 169.452.$$

Since $\mathbf{c} \in B_\tau$, the expected number of 1 in $\mathbf{c}$ is $\tau/2$. Thus, taking $d = 0.12$ in Proposition 2, the number of required signatures is

$$N = \frac{\hat{N}}{\tau/2} = 2\left(\frac{Z\sigma_s}{0.12}\right)^2 /\tau.$$

Taking $Z = 3.2905$, we have $N = 2,698,763$.

We perform a simulation using Sagemath with $N_{exp} = 2,700,000$. The simulation successfully recovers the secret key $\mathbf{e}$ completely in less than 2.5 hours.

4.7 2018 Dilithium Signature with Abort Only on $||\mathbf{s}||_\infty$

Dilithium [7] is a lattice-based signature submitted to the NIST Call for PQC Standardization. It is a Schnorr-type signature with aborts. We briefly describe certain important part of the Dilithium signature, which is sufficient for our purpose. For more details on the Dilithium signature, please refer to [7].

In the Dilithium signature, we have

$$\mathbf{z} = \mathbf{y} + \mathbf{c}\mathbf{s}_1,$$

where $\mathbf{s}_1 \in S_\eta^l$ is part of the secret key, $\mathbf{y} \in S_{\gamma_1 - 1}^l$, and $\mathbf{c} \in B_{60}$ is a hash value of the message and some other inputs. The signature is outputted if and only if $\|\mathbf{z}\|_\infty \leq (\gamma_1 - 1) - \delta$ (note that if $\|\mathbf{z}\|_\infty > (\gamma_1 - 1) - \delta$, then the signer should repeat the signature generation process).

The 2018 version of Dilithium [7] uses $q = 8380417$, $n = 256$, and $\tau := \mathrm{wt}_H(c) = 60$. The other parameters for the 2018 version of Dilitihium is given in Table 7.

	$\gamma_1 - 1$	δ	$\gamma_1 - 1 - \delta$	η	$\beta := \eta\tau$
weak	523775	375	523400	7	420
medium	523775	325	523450	6	360
recommended	523775	275	523500	5	300
high	523775	175	523600	3	180

Table 7 Parameters of Dilithium 2018

Now we will derive an estimate on the number of signatures required to launch the statistical attack. Observe that all parameters except for the high security level satisfy $\delta \leq \beta - 2\eta$. Thus, for these parameters, we may apply Theorem 4 to conclude that $\mathbb{E}[s_{l+i}]$ is of the form $\pm \left(\sum_{k=\delta-|e_i|+1}^{\delta+|e_i|} \sum_{j=k}^{\beta-\eta} \overline{p_j} \right)/2$. We estimate d in Theorem 2 using Remark 8(ii) as

$$d \approx \frac{1}{2} \cdot \left(\sum_{k=\delta}^{\delta+1} \sum_{j=k}^{\beta-\eta} \overline{p_j} \right)/2 \approx \sum_{k=\delta}^{\delta+1} C_k/4,$$

where $C_k := [0.4361836 \times (1 + 0.33267|\kappa_k|)^{-1} - 0.1201676 \times (1 + 0.33267|\kappa_k|)^{-2} + 0.937298 \times (1 + 0.33267|\kappa_k|)^{-3}] \times \frac{\exp(-\kappa_k^2/2)}{\sqrt{2\pi}}$ and $\kappa_k := (k - \frac{1}{2})/\sigma_{ce}$ for $k = \delta, \delta + 1$, and $\sigma_{ce} = \sqrt{\tau\eta(\eta + 1)/3}$.

On the other hand, for the high security level, the parameter satisfies $\delta = \beta - 2\eta + 1$. We can still perform key recovery attack in this case as explained in Remark 7. The only difference is that when $|e_i| = \eta$, $\mathbb{E}[s_{l+i}]$ is a sum of $(2\beta - 1)$ terms (instead of 2β terms). As such, for the high security level, we estimate d more conservatively as $d \approx \frac{1}{4} \left(\sum_{k=\delta}^{\delta+1} \sum_{j=k}^{\beta-\eta} \overline{p_j} \right)/2 \approx \sum_{k=\delta}^{\delta+1} C_k/8$.

Since $\mathbf{c} \in B_\tau$, the expected number of 1 in $\mathbf{c}$ is $\tau/2$. Thus, by Theorem 2, the number of required signatures is

$$N = \frac{\hat{N}}{\tau/2} \approx 2 \left(\frac{Z\sigma_s}{d} \right)^2 /\tau.$$

Due to the abort condition, we have $\mathbf{s} \in S_B$ where $B := \gamma_1 - 1 - \delta$. The standard deviation of $\mathbf{s}$ can then be approximated as $\sigma_s \approx \sqrt{\frac{B(B+1)}{3}}$. Since $n = 256$, we will take $Z = 3.8905$.

In the following Table 8, we list an estimate on the number of required signatures to perform our proposed key recovery attack on the Dilithium 2018 parameters.

	σ_{ce}	d	σ_s	$\log_2(N)$
weak	33.4664	1.05×10^{-29}	302185.419	227.9
medium	28.9827	9.63×10^{-30}	302214.287	228.2
recommended	24.4948	8.35×10^{-30}	302243.154	228.6
high	15.4919	1.97×10^{-30}	302300.889	232.7

Table 8 Estimate on the number of required signatures to perform the proposed key recovery attack on Dilithium 2018 parameters

From Table 8, we see that the number of required signatures is $> 2^{227}$, which is more than the claimed security level. Therefore, this does not violate the security claim of the Dilithium 2018 parameters. Nevertheless, our attack gives a potential weakness, and the complexity of performing the attack should be considered when analysing the security of similar schemes.

Remark 9. *Note that the attack theoretically works on the parameters of Dilithium 2018 because $\delta \leq \beta - \eta$. However, the parameters for Dilithium have been updated. The current parameters satisfy $\delta = \beta = \eta\tau$. As shown in Theorem 3, in this case, $\mathbb{E}[s_{l+i}] = 0$ regardless of the value of e_i. Therefore, the attack does not work on the current parameters of Dilithium. It is thus important to set the parameters carefully. In particular, one should choose $\delta \geq \beta$.*

5 Information-Theoretic Analysis for $\delta \geq \beta$

In Section 4.2, we have shown that $\mathbb{E}[s_{l+i}] = 0$ if $\delta \geq \beta$. As such, we cannot use an attack similar to Algorithm 1 in order to recover the secret key $\mathbf{e}$. However, it does not rule out the possibility that there could be other methods of recovering $\mathbf{e}$ from $\mathbf{s}$. In this section, we shall show that in fact $\mathbf{s}$ does not leak any information about $\mathbf{e}$.

Recall that due to the abort condition, we have $\mathbf{s} \in S_B$ (where $(\mathbf{s}, \mathbf{c})$ is a signature produced using the secret key $\mathbf{e}$). We shall now show that the probability that any particular $\mathbf{s}' \in S_B$ appears as a signature does not depend on the secret key $\mathbf{e}$ if $\delta \geq \beta$.

Lemma 11. *If $\delta \geq \beta$, then for any $\mathbf{s}' \in S_B$ and any $\mathbf{e}' \in S_\eta$, we have*

$$\Pr[\mathbf{s} = \mathbf{s}' \mid \mathbf{e} = \mathbf{e}'] = \frac{1}{(2\gamma + 1)^n},$$

where the probability is taken over all $\mathbf{c} \in B_\tau$ and all $\mathbf{u} \in S_\gamma$

Proof. Fix any $\mathbf{s}' \in S_B$ and any $\mathbf{e}' \in S_\eta$. Note that

$$\Pr[\mathbf{s} = \mathbf{s}' \mid \mathbf{e} = \mathbf{e}'] = \frac{1}{|B_\tau| \cdot |S_\gamma|} |\{(\mathbf{c}, \mathbf{u}) \in B_\tau \times S_\gamma \mid \mathbf{s}' = \mathbf{c}\mathbf{e}' + \mathbf{u}\}|$$

$$= \frac{1}{|B_\tau| \cdot |S_\gamma|} |\{\mathbf{c} \in B_\tau \mid \mathbf{s}' - \mathbf{c}\mathbf{e}' \in S_\gamma\}|.$$

Observe that since $\mathbf{s}' \in S_B$ and $\mathbf{e}' \in S_\eta$, then for any $\mathbf{c} \in B_\tau$, we have

$$\begin{aligned} \|\mathbf{s}' - \mathbf{c}\mathbf{e}'\|_\infty &\leq \|\mathbf{s}'\|_\infty + \|\mathbf{c}\mathbf{e}'\|_\infty \\ &\leq \|\mathbf{s}'\|_\infty + \tau \cdot \|\mathbf{c}\|_\infty \cdot \|\mathbf{e}'\|_\infty \\ &\leq B + \tau\eta \\ &= \gamma - \delta + \beta \\ &\leq \gamma. \end{aligned}$$

Thus, the condition $\mathbf{s}' - \mathbf{c}\mathbf{e}' \in S_\gamma$ is always satisfied. It follows that

$$\Pr[\mathbf{s} = \mathbf{s}' \mid \mathbf{e} = \mathbf{e}'] = \frac{1}{|B_\tau| \cdot |S_\gamma|} |B_\tau| = \frac{1}{|S_\gamma|} = \frac{1}{(2\gamma + 1)^n}.$$

□

As the probability is independent of $\mathbf{e}'$ (and $\mathbf{s}'$), we conclude that any given value of $\mathbf{s}$ in the signature does not reveal any information about the secret key $\mathbf{e}$. Consequently, one cannot learn any information about the secret key $\mathbf{e}$ (in particular, one cannot recover $\mathbf{e}$) from $\mathbf{s}$.

6 Conclusion

In this paper, we examined the security of Schnorr-type signature schemes against statistical attack. We first considered the signature schemes without aborts. We showed that by considering the signatures with $c_l = 1$ and those with $c_l = -1$ separately, the expected value $\mathbb{E}[\mathbf{s}]$ of the signature reveals the secret key $\mathbf{e}$. This enables us to launch a key recovery attack via statistical method. We presented an algorithm to perform key recovery attack and gave a general formula for determining the number of signatures required to successfully recover the secret key using this statistical attack. Moreover, we applied our attack to EagleSign [4] signature scheme, which is a lattice-based signature scheme submitted to the NIST Call for PQC Additional Signature. Our results show that we can perform key recovery attack on the EagleSign 2 signature schemes with as few as 665 signatures, and our proof-of-concept Sagemath implementation of the attack can recover the secret key in less than 3 minutes.

We also analyzed Schnorr-type signature schemes with aborts. The use of aborts in Schnorr-type signature scheme was proposed as a countermeasure against statistical attacks. Our detailed analysis in this paper considered all possible cases with regards to a parameter δ related to the abort condition. We showed that the expected value $\mathbb{E}[\mathbf{s}]$ is correlated with the secret key $\mathbf{e}$ if $\delta \leq \beta - \eta$. Therefore, one could theoretically still launch a statistical attack to recover $\mathbf{e}$ completely if $\delta \leq \beta - \eta$. If $\beta - \eta < \delta < \beta$, then the statistical attack can only recover the secret key $\mathbf{e}$ partially. On the other hand, we proved that the statistical attack does not work if $\delta \geq \beta$. Furthermore, we proved information-theoretically that in fact the signature $\mathbf{s}$ does not leak any information about $\mathbf{e}$ at all if $\delta \geq \beta$, thereby ruling out any possible attack to recover $\mathbf{e}$ from $\mathbf{s}$.

We gave an example to demonstrate our proposed key recovery attack in the case when there is an abort during signature generation. We also analyzed the security of Dilithium [7] against our attack. We observed that the parameters of Dilithium proposed in 2018 satisfies $\delta \leq \beta - \eta$ and as such is susceptible to our attack. We provided an estimate on the number of signatures required to perform the proposed key recovery attack on the Dilithium 2018 parameters. On the other hand, the current parameters of Dilithium is secure against the attack as the updated parameters satisfy $\delta = \beta$. Our analysis shows that even when abort condition is employed, it is crucial to set the parameters carefully in order to defend against statistical attack. In particular, it is recommended to set $\delta \geq \beta$.

In this paper, we focus on the Schnorr-type signatures with aborts where the abort condition is on the infinity norm of the signature $\mathbf{s}$. This is the case for many signature schemes available in the literature, including the Lyubashevsky's signature [1], qTESLA [6], Dilithium [7], etc. Recently, there are a number of proposals for signature schemes (such as HAETAE [15], HuFu [16], etc.), where the abort condition is imposed on the Euclidean/ℓ_2 norm instead of the infinity norm. We leave the analysis of the ℓ_2-abort condition for future work.

Declarations

Conflict of interest. The authors have no relevant financial or non-financial interests to disclose.

References

[1] Lyubashevsky, V.: Fiat-shamir with aborts: Applications to lattice and factoring-based signatures. In: Matsui, M. (ed.) Advances in Cryptology – ASIACRYPT 2009, pp. 598–616. Springer, Berlin, Heidelberg (2009). https://doi.org/10.1007/978-3-642-10366-7_35

[2] Lyubashevsky, V.: Lattice signatures without trapdoors. In: Pointcheval, D., Johansson, T. (eds.) Advances in Cryptology – EUROCRYPT 2012, pp. 738–755. Springer, Berlin, Heidelberg (2012). https://doi.org/10.1007/978-3-642-29011-4_43

[3] Schnorr, C.P.: Efficient identification and signatures for smart cards. In: Brassard, G. (ed.) Advances in Cryptology — CRYPTO' 89 Proceedings, pp. 239–252. Springer, New York, NY (1990). https://doi.org/10.1007/0-387-34805-0_22

[4] Hounkpevi, A.C., Djimnaibeye, S., Seck, M.: EagleSign: A new post-quantum ElGamal-like signature over lattices (version 1) (2023). https://csrc.nist.gov/csrc/media/Projects/pqc-dig-sig/documents/round-1/spec-files/EagleSign-spec-web.pdf

[5] Fiat, A., Shamir, A.: How to prove yourself: Practical solutions to identification and signature problems. In: Odlyzko, A.M. (ed.) Advances in Cryptology — CRYPTO' 86, pp. 186–194. Springer, Berlin, Heidelberg (1987). https://doi.org/10.1007/3-540-47721-7_12

[6] Alkim, E., Barreto, P.S.L.M., Bindel, N., Krämer, J., Longa, P., Ricardini, J.E.: The lattice-based digital signature scheme qtesla. In: Conti, M., Zhou, J., Casalicchio, E., Spognardi, A. (eds.) Applied Cryptography and Network Security, pp. 441–460. Springer, Cham (2020). https://doi.org/10.1007/978-3-030-57808-4_22

[7] Ducas, L., Kiltz, E., Lepoint, T., Lyubashevsky, V., Schwabe, P., Seiler, G., Stehlé, D.: Crystals-dilithium: A lattice-based digital signature scheme **2018**, 238–268 (2018) https://doi.org/10.13154/tches.v2018.i1.238-268

[8] Song, Y., Huang, X., Mu, Y., Wu, W., Wang, H.: A code-based signature scheme from the lyubashevsky framework. Theoretical Computer Science **835**, 15–30 (2020) https://doi.org/10.1016/j.tcs.2020.05.011

[9] Aragon, N., Blazy, O., Gaborit, P., Hauteville, A., Zémor, G.: Durandal: A rank metric based signature scheme. In: Ishai, Y., Rijmen, V. (eds.) Advances in Cryptology – EUROCRYPT 2019, pp. 728–758. Springer, Cham (2019). https://doi.org/10.1007/978-3-030-17659-4_25

[10] Aragon, N., Baldi, M., Deneuville, J.-C., Khathuria, K., Persichetti, E., Santini, P.: Cryptanalysis of a code-based full-time signature. Designs, Codes and Cryptography **89**(9), 2097–2112 (2021) https://doi.org/10.1007/s10623-021-00902-7

[11] Tan, C.H., Prabowo, T.F.: A new key recovery attack on a code-based signature from the lyubashevsky framework. Information Processing Letters **183**, 106422 (2024) https://doi.org/10.1016/j.ipl.2023.106422

[12] Aragon, N., Dyseryn, V., Gaborit, P.: Analysis of the security of the pssi problem and cryptanalysis of the durandal signature scheme. In: Handschuh, H., Lysyanskaya, A. (eds.) Advances in Cryptology – CRYPTO 2023, pp. 127–149. Springer, Cham (2023). https://doi.org/10.1007/978-3-031-38548-3_5

[13] Panaretos, V.M.: Statistics for Mathematicians vol. 142, pp. 9–15. Springer, Switzerland (2016). https://doi.org/10.1007/978-3-319-28341-8

[14] Abramowitz, M., Stegun, I.A.: Handbook of Mathematical Functions with Formulas, Graphs, and Mathematical Tables. Dover, New York (1964)

[15] Cheon, J.H., Choe, H., Devevey, J., Güneysu, T., Hong, D., Krausz, M., Land, G., Möller, M., Stehlé, D., Yi, M.: HAETAE: Shorter Lattice-Based Fiat-Shamir Signatures. Cryptology ePrint Archive, Paper 2023/624. https://eprint.iacr.org/2023/624 (2023). https://eprint.iacr.org/2023/624

[16] Yu, Y., Jia, H., Li, L., Ran, D., Qiu, Z., Zhang, S., Lin, X., Wang, X.: HuFu: Hash-and-Sign Signatures From Powerful Gadgets. https://csrc.nist.gov/csrc/media/Projects/pqc-dig-sig/documents/round-1/spec-files/HuFu-spec-web.pdf