More Accurate Geometric Analysis on the Impact of Successful Decryptions for IND-CCA Secure Ring/Mod-LWE/LWR Based Schemes

Han Wu[1,2] and Guangwu Xu[1,2](✉)

[1] School of Cyber Science and Technology, Shandong University, Qingdao 266237, Shandong, China
hanwu97@mail.sdu.edu.cn

[2] Key Laboratory of Cryptologic Technology and Information Security of Ministry of Education, Shandong University, Qingdao 266237, Shandong, China
gxu4sdq@sdu.edu.cn

Abstract. Majority of lattice-based encryption schemes allow the possibility of decryption failures. It is now understood that this property makes such encryption systems susceptible to the so-called decryption failure attack. In such an attack, an adversary can use a large number of ciphertexts that cause decryption failures to help to recover a private key. In PQC2020, Bindel and Schanck observed that successful decryptions also imply some information about the secret as the secret vector must be away from certain spherical caps. In this paper, we revisit this problem by exploring certain geometric properties in lattice based schemes. We are able to produce more tools for crypt-analysis and operations of these schemes and provide a more accurate interpretation of the information brought from successful decryptions to enhance the failure boosting. By using (recent) precise formulas, we develop some techniques to accurately characterize relationships between a private key and successful queries to the decryption oracle. A finer estimation of the valid proportion of key candidates that can be excluded from successful queries is given. The decryption failure probability is also more accurately analysed. Our discussion addresses and corrects previous errors and our experimental data is usable in assessing the IND-CCA security of (R/M)-LWE/LWR based systems.

Keywords: Lattice-based cryptography · Decryption oracle · Failure boosting · Crypt-analysis

1 Introduction

Lattice-based cryptography has been an important field for research and applications. Over the past decades, many new ideas have been developed and new

Supported by National Key Research and Development Program of China (Grant No. 2018YFA0704702) and Department of Science and Technology of Shandong Province of China (Grant No. 2019JZZY010133).

S. D. Galbraith (Ed.): CT-RSA 2022, LNCS 13161, pp. 196–222, 2022.
https://doi.org/10.1007/978-3-030-95312-6_9

designs have been proposed. It is believed that several fundamental lattice problems are resistant to quantum attacks, public key systems using lattice construction have been a major option for new post-quantum cryptosystems.

The environment for setting up lattice-based encryption systems seems to be much more complicated than that for the classical public key encryption systems such as RSA and Elgamal (finite fields version and elliptic curve version). Because of the involvements of adding errors and rounding operations, the decryption is not a deterministic one. Given a valid pair of ciphertext and private key, one can only assert that such a system recovers the correct plaintext with overwhelming probability.

In 2018, the impact of decryption failures was studied for measuring the chosen-ciphertext security of (Ring/Module)-Learning With Errors/Rounding ((R/M)-LWE/LWR)-based primitives by D'Anvers etc. in [10,11]. Their results show that such an impact could be significant. Especially when the failure probability is relatively high, the security of (R/M)-LWE/LWR-based schemes could be reduced. On the other hand, since NIST poses some limits on the number of available oracle queries, the NIST post-quantum standardization candidates could be immune to this kind of attack. The authors of [10,11] have developed failure boosting technique to increase the failure rate in the above work. It is noted that more ways of achieving failure boosting have been proposed more recently [9,12–16].

In 2020, Bindel and Schanck [5] considered the problem from a new angle by arguing that for an imperfectly correct lattice-based public-key encryption scheme, information about their private key can be leaked even when the answers for decryption queries are successful. In their refinement of the D'Anvers-Guo-Johansson-Nilsson-Vercauteren-Verbauwhede failure boosting attack, through a geometric formulation of the problem, partial information about the private key can be obtained by calculating (a low order approximation of) a union of spherical caps. It should be pointed out that the discussion in [5] contains an error which also affects the correctness of bounds and corresponding experiments.

In this paper, we revisit the problem of using the information brought from successful queries to enhance the failure boosting. Combining with some recent mathematical tools, we develop some techniques to characterize the information about private key more accurately, given that decryption queries all succeed. Our discussion corrects previous errors and our experimental data is usable in assessing the security of (R/M)-LWE/LWR-based systems. More specifically, our contributions are

- We characterize the compression errors (rounding errors) that are used by several important lattice-based schemes. For the cases of practical interest, we are able to obtain their precise distributional behavior.
- The information inferred by a successful answer from querying the decryption oracle is correctly characterized. More precise geometric formulas are used to calculate the valid proportion of private key candidates that can be excluded in the decryption failure attack.

– By refining the (recently confirmed) orthogonality hypothesis, the effect of more queries and their overlaps are investigated and better estimations are obtained.
– Using the information of the success of previous queries, a more accurate posterior decryption failure probability is given according to Bayes' theorem.

The paper is organized into 6 sections. Necessary terminologies and notations are introduced in Sect. 2. We discuss the distributional behaviors of compression errors in Sect. 3. Section 4 reformulates the problem of extracting private key information from successful queries with more concise formulas. The content of dealing with general case by using the second-order approximation is included in Sect. 5 where the overlaps among queries are treated in detail and a more accurate way of estimating posterior decryption failure probability is given. Finally, experiments of our framework for some NIST post-quantum candidates are conducted in Sect. 6.

2 Preliminaries

We shall introduce necessary terminologies and notations for (R/M-) LWE/LWR-based encryption schemes.

2.1 (R/M-)LWE/LWR-Based Public-Key Encryption Scheme

First let us fix some notations. Let q be a positive integer. In lattice-based cryptography, one uses the minimum absolute residue system modulo q, with the notation "x mods q" denoting the remainder in the range $\left[-\frac{q}{2}, \frac{q}{2}\right)$ of x dividing by q (remainder with sign). By choosing the representatives accordingly, we may write

$$\mathbb{Z}_q = \mathbb{Z} \cap \left[-\frac{q}{2}, \frac{q}{2}\right).$$

Let n be another positive integer. We will mainly work on the rings $R = \mathbb{Z}[x]/(x^n+1)$ and $R_q = \mathbb{Z}_q[x]/(x^n+1)$. The ℓ_2-norm and ℓ_∞-norm are written as $\|\cdot\|$ and $\|\cdot\|_\infty$ respectively. More precisely, for $a = (a_0\ a_1\ \cdots a_{n-1})^T \in \mathbb{Z}_q^n$ or $a = a_0 + a_1 x + \cdots + a_{n-1}x^{n-1} \in R_q$,

$$\|a\| = \sqrt{\sum_{i=0}^{n-1} a_i^2}, \quad \|a\|_\infty = \max_{0\le i\le n-1} |a_i|.$$

As for $\alpha = (\alpha_1, \cdots, \alpha_k)^T \in R_q^k$, its norms are respectively $\|\alpha\| = \sqrt{\sum_{j=1}^k \|\alpha_j\|^2}$ and $\|\alpha\|_\infty = \max_{1\le j\le k} \|\alpha_j\|_\infty$.

For integers $p, q > 0$, we write $x_{q\to p} = \left\lceil \frac{px}{q} \right\rfloor$ where $\lceil\cdot\rfloor$ is the usual rounding to the nearest integer. We use $a \leftarrow \chi(X)$ to denote the sampling $a \in X$ according to the distribution χ, and X can be omitted when there is no ambiguity.

Table 1. A summary of some security parameters for NIST post-quantum schemes.

PKE.KeyGen()	**PKE.Enc**$(pk = (b, seed_A))$	**PKE.Dec** $(sk = s, c = (v', b'))$
$seed_A \leftarrow \mathcal{U}(\{0,1\}^{256})$	$A = \text{gen}(seed_A) \in R_q^{k\times k}$	$b'_r = \lceil b' \rfloor_{p\to q}$
$A = \text{gen}(seed_A) \in R_q^{k\times k}$	$s' \leftarrow \chi_{s'}(R_q^k),\ e' \leftarrow \chi_{e'}(R_q^k),\ e'' \leftarrow \chi_{e''}(R_q)$	$v'_r = \lceil v' \rfloor_{t\to q}$
$s \leftarrow \chi_s(R_q^k),\ e \leftarrow \chi_e(R_q^k)$	$b_r = \lceil b \rfloor_{p\to q}$	$v = b_r'^T s$
$b = \lceil As + e \rfloor_{q\to p}$	$b' = \lceil A^T s' + e' \rfloor_{q\to p}$	$m' = \text{dec}\ (v'_r - v)$
	$v' = \lceil b_r^T s' + e'' + enc(m) \rfloor_{q\to t}$	
return $(pk := (b, seed_A), sk := s)$	return $c = (v', b')$	return m'

The general model we discuss in this paper is the one that unifies the essential ideas of several (R/M-)LWE/LWR-based schemes. Here is the description:

The condition for a decryption failure of the (R/M-)LWE/LWR-based public-key encryption scheme described in the above model was extensively considered in [10,11]. To explain that, we first define u, u', u'' as the errors introduced by the rounding and reconstruction operations:

$$\begin{cases} u = As + e - b_r \\ u' = A^T s' + e' - b'_r \\ u'' = b_r^T s' + e'' + enc(m) - v'_r. \end{cases}$$

Then, we form $S = \begin{pmatrix} -s \\ e - u \end{pmatrix}, C = \begin{pmatrix} e' + u' \\ s' \end{pmatrix}$ and $G = e'' - u''$. The following lemma gives the precise condition for a decryption failure of the scheme.

Lemma 1 [10]**.** *For a fixed triple (S, C, G), the decryption failure occurs if and only if $\|S^T C + G\|_\infty > \frac{q}{4}$.*

A more convenient way of writing the failure condition just in terms of vectors with components in $\mathbb{Z}_q$ was described in [12]. Let $\alpha = (\alpha_1, \cdots, \alpha_k)^T \in R_q^k$ be a vector of polynomials, we write $\overline{\alpha} \in \mathbb{Z}_q^{kn}$ to be the concatenation of coefficient vectors of polynomials $\alpha_1, \cdots, \alpha_k$, namely

$$\overline{\alpha} = (a_{10}, a_{11}, \cdots, a_{1,n-1}, \cdots, a_{k0}, a_{k1}, \cdots, a_{k,n-1})^T$$

where $\alpha_j = a_{j0} + a_{j1}x + \cdots + a_{j,n-1}x^{n-1}$.

Fix a positive integer r, an *r-rotation* of a polynomial vector $\alpha = (\alpha_1, \cdots, \alpha_k)^T$ in R_q^k is

$$\alpha^{(r)} = \left(x^r \cdot \alpha_1(x^{-1}) \pmod{x^n + 1}, \cdots, x^r \cdot \alpha_k(x^{-1}) \pmod{x^n + 1}\right)^T \in R_q^k.$$

The following properties of rotations are evident.

1. For any polynomial vector $\alpha \in R_q^k$ and $r \in \mathbb{Z}$, we have $\alpha^{(n+r)} = -\alpha^{(r)}$ and $\alpha^{(2n+r)} = \alpha^{(r)}$.
2. For $a = \sum_{i=0}^{n-1} a_i x^i \in R_q$, the coefficients of $a^{(r)}$ satisfy

$$a_j^{(r)} = \begin{cases} a_{r-j} & 0 \le j \le r \\ -a_{n+r-j} & r+1 \le j \le n-1 \end{cases} \quad r, j = 0, 1, \cdots, n-1.$$

3. For any polynomial vectors $\alpha, \beta \in R_q^k$, we have $\alpha^T\beta = \sum_{j=0}^{n-1} \overline{\alpha}^T\overline{\beta^{(j)}}x^j$.

Thus, the failure condition of Lemma 1 can also be written as:

$$\exists r \in [0, 2n-1], \text{ such that } \left|\overline{S}^T\overline{C^{(r)}} + G_r\right| > \frac{q}{4}.$$

where G_i is the $i-$th degree coefficient of $G, i = 0, 1, \cdots, n-1$.

In our setting, the IND-CCA security for PKE schemes is considered. The adversary has no control on the random variables such as s', e', e'' as they are the results of hash function calls. This means that s', e', e'' can actually be seen as being extracted from particular distributions. As shown in Table 1, one treats $s' \leftarrow \chi_{s'}(R_q^k)$, $e' \leftarrow \chi_{e'}(R_q^k)$ and $e'' \leftarrow \chi_{e''}(R_q)$.

However, the adversary can pick a message and then get the values of s', e', e''. In a failure boosting attack, the adversary improves his odds of triggering a decryption failure by searching for s', e', e'' with large norms. The adversary needs to balance the cost of searching randomness that meet the length condition with the success rate of finding decryption failures. He only sends ciphertexts generated by such randomness to the decryption oracle as these ciphertexts have a failure probability greater than a certain value.

In this paper, we will focus on the case where the attacker only uses values of s', e' with a greater-than-average length (see Sect. 4.1). It is noticed that our discussion also applies to other cases.

The coefficients of s, s', e, e', e'' are always small. Let $\eta > 0$ be a positive integer. Recall that the centered binomial distribution β_η is the probability distribution defined on the set $X = \{-\eta, -\eta+1, \cdots, -1, 0, 1, \cdots, \eta\}$ with the probability assignment at $k \in X$ to be

$$\beta_\eta(k) = \binom{2\eta}{k+\eta}\frac{1}{2^{2\eta}}.$$

This distribution has variance $\frac{\eta}{2}$. To sample according to β_η, one sample $(a_1, \cdots, a_\eta, b_1, \cdots, b_\eta) \leftarrow \{0,1\}^{2\eta}$ and output $\sum_{i=1}^{\eta}(a_i - b_i)$.

When we write that a polynomial $f \in R_q$ or a vector of such polynomials is sampled from β_η, we mean that each coefficient of it is sampled from β_η. In practice, the number η is much smaller than q.

2.2 Spherical Cap

Let d be a positive integer. For vectors $u, v \in \mathbb{R}^d$, the angle between u, v is

$$\theta(u, v) = \arccos\left(\frac{< u, v >}{\|u\| \cdot \|v\|}\right).$$

This is a useful notation to describe the difference between two vectors and is known as "angular distance". It is an important tool in our analysis throughout this paper. We will focus more on the directions and the angles instead of

the length of vectors. In [5], the *spherical cap* is introduced to characterize the information available from each successful query.

Definition 1. *Let $\mathcal{S}_d$ be the unit hypersphere in $\mathbb{R}^d$. For any $u \in \mathcal{S}_d$, the spherical cap of angle θ about u is*

$$\mathcal{C}(d, u, \theta) = \{v \in \mathcal{S}_d : \theta(u, v) \leq \theta\}.$$

It is proved in [5] that each successful decryption can rule out key candidates in the corresponding spherical caps. Thus, the size of the surface area of caps is closely related to the number of excluded key candidates. Let σ_{d-1} denote the usual surface measure on $\mathcal{S}_d$, the following heuristic from [5] is useful in applying surface area of spherical caps to measure points of interest and will be assumed in our later discussion.

Heuristic 1. *For a fixed $u \in \mathcal{S}_d$, let v be a uniformly random point on $\mathcal{S}_d$. The probability of $\theta(u, v) \leq \theta$ is*

$$\sigma_{d-1}\left(\mathcal{C}(d, u, \theta)\right).$$

We shall perform some explicit calculation for the surface area of a spherical cap. In [19], a concise area formula for such a cap is derived in closed form. This formula involves with the so called *incomplete beta function* defined by

$$B(x, \nu, \mu) = \int_0^x t^{\nu-1}(1-t)^{\mu-1}dt, \ 0 \leq x \leq 1.$$

Note that $B(1, \nu, \mu)$ is the usual beta function $B(\nu, \mu) = \int_0^1 t^{\nu-1}(1-t)^{\mu-1}dt = \frac{\Gamma(\nu)\Gamma(\mu)}{\Gamma(\nu+\mu)}$. We normalize the incomplete beta function and denote it by

$$I_x(\nu, \mu) = \frac{B(x, \nu, \mu)}{B(\nu, \mu)}.$$

The formula for the cap surface area of $\mathcal{C}(d, u, \theta)$ given in [19] is

$$A_d^{cap}(\theta) = \frac{1}{2} A_d I_{\sin^2(\theta)}\left(\frac{d-1}{2}, \frac{1}{2}\right),$$

where $A_d = \frac{2\pi^{\frac{d}{2}}}{\Gamma\left(\frac{d}{2}\right)}$ is the surface area of $\mathcal{S}_d$.

As for the surface area of the intersection of two spherical caps, some concise formulas are given in [18]. Let $A_d\left(\theta, \theta(u_1, u_2)\right)$[1] be the intersection area of $\mathcal{C}(d, u_1, \theta)$ and $\mathcal{C}(d, u_2, \theta)$. The following two cases are of greatest concern to us:

1. When $\theta(u_1, u_2) \geq 2\theta$, $A_d\left(\theta, \theta(u_1, u_2)\right) = 0$.

[1] The surface area of the intersection does not depend on u_1 or u_2. It is only related to the angle between them.

2. When $\theta < \theta(u_1, u_2) < 2\theta < 2\pi - \theta(u_1, u_2)$,
$A_d\left(\theta, \theta(u_1, u_2)\right) = \frac{\pi^{\frac{d-1}{2}}}{\Gamma\left(\frac{d-1}{2}\right)} \cdot \left(J_d\left(\widetilde{\theta}, \theta\right) + J_d\left(\theta(u_1, u_2) - \widetilde{\theta}, \theta\right)\right)$, where

$$\begin{cases} \widetilde{\theta} = \arctan\left(\frac{1}{\sin(\theta(u_1,u_2))} - \frac{1}{\tan(\theta(u_1,u_2))}\right) \\ J_d(\theta_1, \theta_2) = \int_{\theta_1}^{\theta_2} \sin(\phi)^{d-2} I_{1-\left(\frac{\tan(\theta_1)}{\tan(\phi)}\right)^2}\left(\frac{d}{2} - 1, \frac{1}{2}\right) d\phi \end{cases}$$

The formulas for $A_d\left(\theta, \theta(u_1, u_2)\right)$ for other cases can be found in [18].

3 Compression Errors

As mentioned earlier, there are compression errors u, u', u'' in the (R/M-)LWE/LWR-based schemes. In practice, many schemes based on (R/M-)LWE also have a step for ciphertext compression, such as Kyber and Newhope, so there are also compression errors in these schemes. According to our experiments in Sect. 6, the compression error is sometimes as large as the LWE error when they both are present. Therefore, it is desirable to consider both errors. However, many previous works on schemes based on (R/M-)LWE only considered the LWE error and ignored the compression error. The purpose of this section is to characterize compression error more precisely by proving that it is essentially a uniform distribution on certain set. This will be useful in analyzing the distributions of S, C, G as well as decryption failure later.

Definition 2. *Fix two positive integers $p < q$, the compression error function $CD_{p,q} : \mathbb{Z} \to \mathbb{Z}$ is defined as*

$$CD_{p,q}(y) = y - \left\lceil \frac{q}{p} \left\lceil \frac{p}{q} y \right\rfloor \right\rfloor.$$

This function measures the difference caused by the rounding and reconstruction operations. It can be easily extended to the cases of vectors of integers and polynomials with integer coefficients, by working in a component-wise manner.

Now let us consider the characterization of the distribution of $CD_{p,q}(y)$. In practice, the only cases of interest are $\gcd(p, q) = 1$ and $p|q$, so we shall simply deal with these two cases. But we would like to remark that the discussion also applies to the general case of $\gcd(p, q) > 1$. The following theorem states the results whose proof is given in Appendix A.

Theorem 1. *For positive integers $p < q$, characterizations of $CD_{p,q}$ for the following two cases are:*

1. *If $(p, q) = 1$, then $CD_{p,q}(y) = \left\lceil \frac{b}{p} \right\rfloor$ where $b = py \bmod q$. Furthermore, if y is uniformly random chosen from $\mathbb{Z}$ or $\mathbb{Z}_q$, b is uniformly random in $\mathbb{Z}_q$, $CD_{p,q}(y)$ belongs to $\left\{-\left\lceil \frac{q}{2p} \right\rfloor, \cdots, \left\lceil \frac{q}{2p} \right\rfloor\right\}$ and has the same probability at all of the integer points except $-\left\lceil \frac{q}{2p} \right\rfloor$ and $\left\lceil \frac{q}{2p} \right\rfloor$.*

2. *If $p|q$, then with $m = \frac{q}{p}$, $CD_{p,q}(y) = d$ where $d = y \bmod m$. Furthermore, if y is uniformly random chosen from $\mathbb{Z}$ or $\mathbb{Z}_q$, $CD_{p,q}(y)$ is uniformly random in $\mathbb{Z}_m$.*

With this theorem, we are able to analyze the distributions of u, u' and u''.

Under the difficulty hypothesis of LWE, $As + e, A^T s' + e', b_r^T s' + e' + enc(m)$ are computationally indistinguishable from uniform distributions on R_q^k, R_q^k and R_q respectively. Therefore, when $\gcd(p, q) = \gcd(t, q) = 1$, each coefficient of u, u' belongs to $\left\{-\left\lceil \frac{q}{2p} \right\rfloor, \cdots, \left\lceil \frac{q}{2p} \right\rfloor\right\}$ and has the same probability at all integer points inside except $\pm \left\lceil \frac{q}{2p} \right\rfloor$, each coefficient of u'' belongs to $\left\{-\left\lceil \frac{q}{2t} \right\rfloor, \cdots, \left\lceil \frac{q}{2t} \right\rfloor\right\}$ and has the same probability at all integer points inside except $\pm \left\lceil \frac{q}{2t} \right\rfloor$.

While if $t|p|q$, each coefficient of u, u' is computationally indistinguishable from a uniform random point in $\mathbb{Z}_{\frac{q}{p}}$, each coefficient of u'' is computationally indistinguishable from a uniform random point in $\mathbb{Z}_{\frac{q}{t}}$.

We use $\psi_{p,q}^k$ to denote the *compression error distribution* for sampling a vector of k polynomials of degree $n - 1$ in the following steps

1. choose $y \leftarrow \mathcal{U}(R^k)$ where $\mathcal{U}$ denotes the uniform distribution;
2. return $CD_{p,q}(y)$ mods q.

This distribution will be used in our later discussion of the concrete schemes of Kyber and Newhope.

4 The Information Inferred by Successful Decryptions

In [5], the authors show that a successful decryption implies that the secret $\overline{S}$ (after normalization) stays away from one (or two) spherical caps.[2] It is noted that [5] contains some ideas for rotations of polynomials, but did not use it in a full extent. In addition, some formulas and experiment settings in [5] do not seem to be consistent. In this section, we will consider excluding caps corresponding to each rotation of a polynomial vector. A more accurate and precise calculation is given using the results in Sect. 3 and some formulas in [19].

4.1 The Relationship Between Successful Decryptions and Caps

We are considering CCA security for schemes where both C and G are obtained by hash function calls. We can view a pair of (C, G) as a query to the decryption oracle. Our setting will restrict to the reaction attack, namely, the adversary only cares if the query succeeds, not what it returns if the decryption fails.

Let $\overline{\overline{S}}$, $\overline{\overline{C}}$ be the normalization of $\overline{S}, \overline{C}$, namely, $\overline{\overline{S}} = \dfrac{\overline{S}}{\|\overline{S}\|}$, $\overline{\overline{C}} = \dfrac{\overline{C}}{\|\overline{C}\|}$. It has been proven in [5] that the success of query C is related to the fact whether $\overline{\overline{S}}$

[2] Two caps are considered at the end of page 8 of [5], but the definition of efficacy on page 9 contains only one cap.

belongs to some spherical caps about $\overline{\overline{C}}$. Combined with the analysis of the distributions of u, u', u'' given in Sect. 3, a finer description of the angle information obtained by a successful decryption can be obtained.

To this end, we know that for each pair of (C, G), the success of the decryption implies that

$$\left|\overline{S}^T \overline{C^{(r)}} + G_r\right| \leq \frac{q}{4}$$

holds true for all $r = 0, 1, \cdots, n-1$. Recall that $G = e'' - u''$. The distribution of the coefficients of u'' has been discussed in Sect. 3, while the distribution of the coefficients of e'' depends on the specific algorithm (and e'' is available to be selected by the adversary). So one can find a constant γ such that $\gamma \geq |G_r|,\ r = 0, 1, \cdots, n-1$. γ should be as small as possible. Therefore, for every successful query, the information that the attacker can definitely obtain is[3]

$$\left|\overline{S}^T \overline{C^{(r)}}\right| \leq \frac{q}{4} + \gamma, r = 0, 1, \cdots, n-1.$$

Let θ_r be the angle between $\overline{S}$ and $\overline{C^{(r)}}$ (which is also the angle between $\overline{\overline{S}}$ and $\overline{\overline{C^{(r)}}}$). We denote the distribution that the user uses to pick S by χ_S, and the distribution that the attacker uses to pick C by χ_C. Let $\mathfrak{S}, \mathfrak{C}$ be two random variables with $\mathfrak{S} \leftarrow \chi_S, \mathfrak{C} \leftarrow \chi_C$. Suppose that the attacker only selects those C such that $\|C\| \geq E[\|\mathfrak{C}\|]$ to query. The attack model assumes that S satisfies

$$\|S\| \geq E[\|\mathfrak{S}\|].$$

This means that some private key candidates cannot be treated in the present setting. However, as we will comment later that this condition can be weakened to cover a bigger set of private keys with some efficiency trade-off. With the assumption of $\|S\| \geq E[\|\mathfrak{S}\|]$, we see that

$$|\cos(\theta_r)| = \left|\frac{\langle \overline{S}, \overline{C^{(r)}} \rangle}{\left\|\overline{S}\right\| \cdot \left\|\overline{C^{(r)}}\right\|}\right| = \frac{\left|\overline{S}^T \overline{C^{(r)}}\right|}{\left\|\overline{S}\right\| \cdot \left\|\overline{C^{(r)}}\right\|} \leq \frac{\frac{q}{4} + \gamma}{\left\|\overline{S}\right\| \cdot \left\|\overline{C^{(r)}}\right\|} \leq \frac{\frac{q}{4} + \gamma}{E[\|\mathfrak{S}\|] \cdot E[\|\mathfrak{C}\|]}.$$

Let us denote $\theta^* \in \left[0, \frac{\pi}{2}\right)$ to be the angle that satisfies $\cos\theta^* = \frac{\frac{q}{4}+\gamma}{E[\|\mathfrak{S}\|] \cdot E[\|\mathfrak{C}\|]}$. If $\cos(\theta_r) \geq 0$, we have $\theta_r \geq \theta^*$, this implies that $\overline{\overline{S}} \notin \mathcal{C}\left(2kn, \overline{\overline{C^{(r)}}}, \theta^*\right)$. Similarly, if $\cos(\theta_r) < 0$, we have $\overline{\overline{S}} \notin \mathcal{C}\left(2kn, -\overline{\overline{C^{(r)}}}, \theta^*\right)$. In summary, for each successful C, we can exclude key candidates in $2n$ spherical caps, in the sense that

$$\overline{\overline{S}} \notin \mathcal{C}\left(2kn, \pm\overline{\overline{C^{(r)}}}, \theta^*\right),\ r = 0, 1, \cdots, n-1.$$

[3] $\frac{q}{4} - \gamma$ was used to bound the LHS in [5], the experiments were performed accordingly. Corrections are necessary.

In the above analysis, the attacker just deals with the set of S such that $\|S\| \geq E[\|\mathfrak{S}\|]$ since the exact value of $\|S\|$ is unknown.[4] This condition can be relaxed. For any $\beta > 0$, he can suppose that $\|S\| \geq \beta \cdot E[\|\mathfrak{S}\|]$ and the information he can get is $|\cos(\theta_r)| \leq \frac{\frac{q}{4}+\gamma}{\beta \cdot E[\|\mathfrak{S}\|] \cdot E[\|\mathfrak{C}\|]}$. (When $\beta \leq \frac{\frac{q}{4}+\gamma}{E[\|\mathfrak{S}\|] \cdot E[\|\mathfrak{C}\|]}$, nothing is available.) It is easy to see that, the larger β is, the larger θ^* is, the more information he can obtain, but the less likely S is to satisfy this condition. Moreover, we assume that the attacker only uses C that satisfies $\|C\| \geq E[\|\mathfrak{C}\|]$. That is, given a ciphertext C, if $\|C\| < E[\|\mathfrak{C}\|]$, he will discard it and regenerate another ciphertext for attack. Similarly, he can also choose to use only longer queries, but the cost of finding such ciphertexts will increase significantly. In this paper, we only consider the case where $\|S\| \geq E[\|\mathfrak{S}\|]$ and all queries used by the attacker have a length at least $E[\|\mathfrak{C}\|]$. In this way, we can always use the same θ^* for different queries. It is noticed that our discussion also applies to other cases.

4.2 The Range of the Proportion of Excluded Key Candidates

Recall that we use θ_r to denote the angle between $\overline{\overline{S}}$ and $\overline{\overline{C^{(r)}}}$. The following lemma from [5] is useful in numerical characterization of the proportion of key candidates.

Lemma 2. *For a fixed S and $C \leftarrow \chi_C$, for any $r \in [0, 2n-1]$, the probability that $\theta_r < \theta^*$ is $\sigma_{2kn-1}\left(\mathcal{C}\left(2kn, \overline{\overline{C^{(r)}}}, \theta^*\right)\right)$.*

This lemma says that the proportion of key candidates in $\mathcal{C}\left(2kn, \overline{\overline{C^{(r)}}}, \theta^*\right)$ is exactly $\sigma_{2kn-1}\left(\mathcal{C}\left(2kn, \overline{\overline{C^{(r)}}}, \theta^*\right)\right)$. In other words, candidates with a ratio of $\sigma_{2kn-1}\left(\mathcal{C}\left(2kn, \overline{\overline{C^{(r)}}}, \theta^*\right)\right)$ can be eliminated by each cap.

By the formula we mentioned in Sect. 2 (from [19]), we give an exact and effective[5] way of calculating of $\sigma_{2kn-1}\left(\mathcal{C}\left(2kn, \overline{\overline{C^{(r)}}}, \theta^*\right)\right)$ using the explicit expression of the surface area of a cap. That is

$$\sigma_{2kn-1}\left(\mathcal{C}\left(2kn, \overline{\overline{C^{(r)}}}, \theta^*\right)\right) = \frac{A_{2kn}^{cap}(\theta^*)}{A_{2kn}} = \frac{1}{2} I_{\sin^2(\theta^*)}\left(kn - \frac{1}{2}, \frac{1}{2}\right).$$

As mentioned earlier, each successful decryption can help with excluding key candidates in $2n$ spherical caps. However, the overlaps among them is not certain.

[4] In fact, the adversary might know what $\|S\|$ is. In some schemes, s, e are sampled according to the centered binomial distribution with fixed Hamming weight, such as LAC. In this case, $\|S\|$ is fixed and the attacker can just use the value of $\|S\|$. However, there are also some schemes that use a discrete Gaussian or centered binomial distribution to sample s, e, such as Kyber and Saber. Some restrictions on $\|S\|$ are necessary.

[5] The normal incomplete beta function can be effectively calculated using software such as Matlab.

It is easy to see that $\mathcal{C}\left(2kn, \overline{\overline{C^{(r)}}}, \theta^*\right) \cap \mathcal{C}\left(2kn, -\overline{\overline{C^{(r)}}}, \theta^*\right) = \emptyset, r = 0, 1, \cdots, n-1$, but different $\mathcal{C}\left(2kn, \overline{\overline{C^{(r)}}}, \theta^*\right)$ may intersect with each other. So the proportion of key candidates that can be excluded by a successful decryption belongs to

$$\left[I_{\sin^2(\theta^*)}\left(kn - \frac{1}{2}, \frac{1}{2}\right), nI_{\sin^2(\theta^*)}\left(kn - \frac{1}{2}, \frac{1}{2}\right)\right].$$

Then the proportion of key candidates that can be excluded by m successful decryptions belongs to

$$\left[I_{\sin^2(\theta^*)}\left(kn - \frac{1}{2}, \frac{1}{2}\right), mnI_{\sin^2(\theta^*)}\left(kn - \frac{1}{2}, \frac{1}{2}\right)\right].$$

We summarize the above analysis as the following proportion.

Proposition 1. *Suppose that an adversary has made some successful queries to the decryption oracle, then the proportion of key candidates that can be excluded is at least* $I_{\sin^2(\theta^*)}\left(kn - \frac{1}{2}, \frac{1}{2}\right)$.

In this section, we only give a rough range of the proportion of the excluded key candidates after m successful queries. It is noticed that, if the attacker has made m successful queries, this proportion could even be $mnI_{\sin^2_{\theta^*}}\left(kn - \frac{1}{2}, \frac{1}{2}\right)$ when certain conditions are met. In the next section, we shall specify such conditions in terms of overlap reduction by quantifying the overlaps among queries. Some exact formulas for the overlaps among queries are presented and a finer range of the proportion is given.

5 The Overlaps Among Queries and the Effect of Successful Decryptions on the Failure Probability

In Sect. 4, a more accurate calculation of the proportion of key candidates contained in each spherical cap has been developed. However, when considering several caps corresponding to one or more queries, the intersections of them will directly affect the attack efficiency. In [5], the notion of *efficacy* of a query set is defined to measure the information available from it, and the use of the principle of inclusion-exclusion to calculate the efficacy is proposed. Due to the complexity of the high-order inclusion-exclusion principle, a first-order approximation to the efficacy is used in [5].

However, it is noticed that the first-order approximation leads to an overestimate of the information available to the attacker, so it can not be used to calculate the number of queries needed for finding a decryption failure. In this section, we use a second-order approximation to measure the information from successful queries to get a lower bound. These two approximations result a fine range of the proportion of excluded key candidates together.

Let W_C denote the set of $2n$ spherical caps according to the query C, i.e.

$$W_C = \left\{\mathcal{C}\left(2kn, \pm\overline{\overline{C^{(r)}}}, \theta^*\right) : \ r = 0, 1, \cdots, n-1\right\}.$$

Suppose the attacker has made m successful queries $C_1, \cdots, C_m$. Not only the overlaps among the caps in each W_{C_i}, but also the overlaps among $W_{C_1}, \cdots, W_{C_m}$ should be considered. The former was considered in [5] as they only calculated one of the $2n$ caps in each W_{C_i}, but the latter was left untreated.[6]

In this section, we consider both of the overlapping situations. We give the conditions and probability of the first-order approximation. The second-order approximation is obtained with more precise formulas to quantify the overlaps. Meanwhile, we come up with some suggestions on how to make the overlaps smaller.

We shall start by dealing with the simplest case – the overlap between two spherical caps.

5.1 The Overlap Between Two Spherical Caps

First of all, we need the one-to-one correspondences between angle and inner product, distance respectively. Two useful relationships are given in the following proposition and the proofs are given in Appendix B.

Proposition 2. *For* $\overline{\overline{C_1}}, \overline{\overline{C_2}} \in \mathcal{S}_d$, *let* $\theta_{1,2} = \theta\left(\overline{\overline{C_1}}, \overline{\overline{C_2}}\right)$, $d_{1,2} = \left\|\overline{\overline{C_1}} - \overline{\overline{C_2}}\right\|$ *and* $ip_{1,2} = \langle \overline{\overline{C_1}}, \overline{\overline{C_2}} \rangle$, *then*

1. $\theta_{1,2} = \arccos\left(ip_{1,2}\right)$, $ip_{1,2} = \cos(\theta_{1,2})$.
2. $\theta_{1,2} = 2\arcsin\left(\frac{1}{2}d_{1,2}\right)$, $d_{1,2} = 2\sin\left(\frac{1}{2}\theta_{1,2}\right)$.

Let us consider the overlap between two caps $\mathcal{C}\left(2kn, \overline{\overline{C_1}}, \theta^*\right)$ and $\mathcal{C}\left(2kn, \overline{\overline{C_2}}, \theta^*\right)$. We denote $\mathcal{C}_{1,2} = \mathcal{C}\left(2kn, \overline{\overline{C_1}}, \theta^*\right) \cap \mathcal{C}\left(2kn, \overline{\overline{C_2}}, \theta^*\right)$. We will show that the disjointness of these two caps can be characterized by the inner product, angle, and distance of $\overline{\overline{C_1}}, \overline{\overline{C_2}}$ respectively. The following theorem is given and its proof is in Appendix C.

Theorem 2. *Let* $\overline{\overline{C_1}}, \overline{\overline{C_2}}$ *be two points on* $\mathcal{S}_d$, *then the following are equivalent:*

1. $\mathcal{C}_{1,2} = \emptyset$.
2. $\theta_{1,2} > 2\theta^*$.
3. $ip_{1,2} < \cos\left(2\theta^*\right)$.
4. $d_{1,2} > 2\sin\theta^*$.

The above theorem give strategies for selecting completely disjoint spherical caps. The adversary can choose one of the angle condition, the distance condition and the inner product condition to check the disjointness. However, sometimes it may be impractical to choose completely non-overlapping queries for reasons such as efficiency. Therefore, the situation where those caps intersect is of interest. The following proposition is a direct consequence of formulas in [18]. It can be used to calculate the proportion of key candidates in $\mathcal{C}_{1,2}$.

[6] In other words, they assumed that the first order approximation is true.

Proposition 3. *Let* $\overline{\overline{C_1}}$, $\overline{\overline{C_2}}$ *be two points on* $\mathcal{S}_{2kn}$. *Let* $\theta_{1,2}$ *be as in Proposition 2 and* $J_d(\theta_1, \theta_2)$ *be as in Sect. 2.2. Then, if* $\theta_{1,2} \geq 2\theta^*, \sigma_{2kn-1}(\mathcal{C}_{1,2}) = 0$. *If* $\theta^* < \theta_{1,2} < 2\theta^*$, *we have*[7]

$$\sigma_{2kn-1}(\mathcal{C}_{1,2}) = \frac{A_{2kn}(\theta^*, \theta_{1,2})}{A_{2kn}} = \frac{1}{2\sqrt{\pi}} \frac{\Gamma(kn)}{\Gamma\left(kn - \frac{1}{2}\right)} \cdot \left(J_{2kn}\left(\widetilde{\theta}_{1,2}, \theta^*\right) + J_{2kn}\left(\theta_{1,2} - \widetilde{\theta}_{1,2}, \theta^*\right)\right),$$

where $\widetilde{\theta}_{1,2} = \arctan\left(\frac{1}{\sin(\theta_{1,2})} - \frac{1}{\tan(\theta_{1,2})}\right)$. *In particular, if* kn *is even, we have*

$$\sigma_{2kn-1}(\mathcal{C}_{1,2}) = \frac{1}{2\pi} \cdot \frac{(2kn-2)!!}{(2kn-3)!!} \cdot \left(J_{2kn}\left(\widetilde{\theta}_{1,2}, \theta^*\right) + J_{2kn}\left(\theta_{1,2} - \widetilde{\theta}_{1,2}, \theta^*\right)\right).$$

The above proposition gives an efficient[8] way of calculating the total proportion of the keys candidates inside two intersecting caps by the following relation:

$$\sigma\left(\mathcal{C}\left(2kn, \overline{\overline{C_1}}, \theta^*\right) \cup \mathcal{C}\left(2kn, \overline{\overline{C_2}}, \theta^*\right)\right) = \sigma\left(\mathcal{C}\left(2kn, \overline{\overline{C_1}}, \theta^*\right)\right) + \sigma\left(\mathcal{C}\left(2kn, \overline{\overline{C_2}}, \theta^*\right)\right) - \sigma(\mathcal{C}_{1,2}).$$

From this, we can raise the lower bound in Proposition 1.

As we can see, $\theta_{1,2}$ is an important indicator for characterizing $\mathcal{C}_{1,2}$. However, because of the tedium of calculating the angles between each pair of queries one by one, an estimation of $\theta_{1,2}$ is needed. Since we are considering the CCA setting where queries are the results of hash function calls, we can view each query $\overline{C}$ (after normalization) as a uniform random point on $\mathcal{S}_{2kn}$. Then $\theta_{1,2}$ can be regarded as an angle in random packing on the sphere. To proceed further, we need some technical argument on this kind of random angles.

The dimension of (R/M-)LWE/LWR-based public-key encryption schemes is usually very high. There is a folklore conjecture that random vectors in high dimensional spaces are almost nearly orthogonal. This is also referred to as the orthogonality hypothesis. Recently, Cai et al. [7] presented a precise formulation and gave the proof of the orthogonality hypothesis.

Lemma 3 [7]**.** *Let* u, v *be two random points on* $\mathcal{S}_d$, *then*

$$Pr\left(\left|\theta(u, v) - \frac{\pi}{2}\right| \geq \epsilon\right) \leq K\sqrt{d}(\cos\epsilon)^{d-2}$$

for any $d \geq 2$ *and* $\epsilon \in \left(0, \frac{\pi}{2}\right)$, *where* K *is a universal constant.*

As indicated in [7], any number K satisfies $K \geq \sqrt{\frac{\pi}{d}} \frac{\Gamma\left(\frac{d}{2}\right)}{\Gamma\left(\frac{d-1}{2}\right)}$ would be sufficient.

It is remarked that a tighter estimation of K is of great interest in practice. To this end, we use some results for Wallis type inequalities. Let $P_d = \frac{(2d-1)!!}{(2d)!!}$ and $P_{d+\frac{1}{2}} = \frac{(2d)!!}{(2d+1)!!}$, then it has been proven in [8,17] that

$$\frac{1}{\sqrt{\pi(d + 4/\pi - 1)}} \leq P_d < \frac{1}{\sqrt{\pi(d + 1/4)}}, \quad \frac{\sqrt{\pi}}{2\sqrt{d + 9\pi/16 - 1}} \leq P_{d+\frac{1}{2}} < \frac{\sqrt{\pi}}{2\sqrt{d + 3/4}}.$$

[7] The conditions chosen here are satisfied in all of the schemes in our experiments. The result can be generalized to the case where $\theta_{1,2} < \theta^*$ by using formulas in [18].

[8] The code for computing $J_d(\theta_1, \theta_2)$ is given in [18]. Since we have made a slight change in the definition of $J_d(\theta_1, \theta_2)$, a small adjustment to the code is required.

From these, we can derive a better bound for $\sqrt{\frac{\pi}{d}}\frac{\Gamma\left(\frac{d}{2}\right)}{\Gamma\left(\frac{d-1}{2}\right)}$, namely

$$\sqrt{\frac{\pi}{d}}\frac{\Gamma\left(\frac{d}{2}\right)}{\Gamma\left(\frac{d-1}{2}\right)} \leq \begin{cases} \sqrt{\frac{\pi}{2}-\frac{2\pi-4}{d}} & \text{if } d \text{ is even} \\ \sqrt{\frac{\pi}{2}-\frac{\frac{5}{2}\pi-\frac{9}{16}\pi^2}{d}} & \text{if } d \text{ is odd.} \end{cases}$$

Normally, one can simply set $K = \sqrt{\frac{\pi}{2}}$. When considering specific schemes, the dimension $d = 2kn$ is even, so we get the following result about the distribution of $\theta_{1,2}$ with a better bound:

Corollary 1. *Let $\overline{\overline{C_1}}$, $\overline{\overline{C_2}}$ be two points on $\mathcal{S}_{2kn}$, let $\theta_{1,2}$ be as in Proposition 2. For any $\epsilon \in \left(0, \frac{\pi}{2}\right)$, we have*

$$Pr\left(\left|\theta_{1,2} - \frac{\pi}{2}\right| \geq \epsilon\right) \leq \sqrt{\pi kn + 4 - 2\pi}\left(\cos\epsilon\right)^{2kn-2}.$$

Let $M > 0$ be some security parameter and set $\epsilon(M) = \arccos\left(\frac{2^M-1}{2^M\sqrt{\pi kn+4-2\pi}}\right)^{\frac{1}{2kn-2}}$. Then it can be verified that

$$\epsilon(M) = \min_{\epsilon\in\left(0,\frac{\pi}{2}\right)}\left\{\sqrt{\pi kn + 4 - 2\pi}\left(\cos\epsilon\right)^{2kn-2} \geq 1 - \frac{1}{2^M}\right\}.$$

From this, an estimate of the range of $\theta_{1,2}$ is given.

Theorem 3. *Let $\overline{\overline{C_1}}$, $\overline{\overline{C_2}}$ be two points on $\mathcal{S}_{2kn}$. For any given security parameter M, we have*

$$\frac{\pi}{2} - \epsilon(M) \leq \theta_{1,2} \leq \frac{\pi}{2} + \epsilon(M)$$

with a probability no less than $1 - \frac{1}{2^M}$.

Together with Theorem 2, we know that if $2\theta^* < \frac{\pi}{2} - \epsilon(M)$, the probability of $\mathcal{C}_{1,2} = \emptyset$ is bigger than $1 - \frac{1}{2^M}$. On the other hand, if $2\theta^* > \frac{\pi}{2} + \epsilon(M)$, the probability of $\mathcal{C}_{1,2} = \emptyset$ is less than $\frac{1}{2^M}$. It is worth noting that, from our experiments in Sect. 6, θ^* is greater than $\frac{\pi}{4}$ in most schemes. Hence, $\mathcal{C}_{1,2} = \emptyset$ is almost not true and Proposition 3 is useful in measuring the surface area of the intersections.

5.2 The Overlaps Among Queries

Suppose that the attacker is making m queries. Just like [Equation (9), [5]], we only consider one cap for each query C_i, for example, $\mathcal{C}\left(2kn, \overline{\overline{C_i^{(0)}}}, \theta^*\right)$. The reason is that we want to consider the overlaps among the caps of different queries. This will not make much difference to the result as $m \gg n$ in practice. For convenience, for each C_i, we write $\mathcal{C}_i = \mathcal{C}\left(2kn, \overline{\overline{C_i^{(r_i)}}}, \theta^*\right), 0 \leq r_i \leq n-1$ to be the cap used by the attacker.

It is noted that $\overline{\overline{C_i^{(r_i)}}}(i = 1, 2, \cdots, m)$ can be seen as m uniformly random points on $\mathcal{S}_{2kn}$. Let $\theta_{i,j}$ $(1 \leq i < j \leq m)$ be the angles between $\overline{\overline{C_i^{(r_i)}}}$ and $\overline{\overline{C_j^{(r_j)}}}$. We assume that these angles are independent and identically distributed and are likely in the range described in Theorem 3 in the sense that

$$\frac{\pi}{2} - \epsilon(M) \leq \theta_{i,j} \leq \frac{\pi}{2} + \epsilon(M) \text{ with a probability no less than } 1 - \frac{1}{2^M}.$$

We use a second-order approximation to estimate the proportion of key candidates that can be excluded after m successful queries to get a lower bound, that is

$$\sigma\left(\bigcup_{i=1}^{m} \mathcal{C}_i\right) \geq \sum_{i=1}^{m} \sigma\left(\mathcal{C}_i\right) - \sum_{1 \leq i < j \leq m} \sigma\left(\mathcal{C}_{i,j}\right),$$

where $\mathcal{C}_{i,j}$ is the intersection of $\mathcal{C}_i$ and $\mathcal{C}_j$.

Consequently, we can get a range of the proportion of excluded key candidates, that is

$$\sigma\left(\bigcup_{i=1}^{m} \mathcal{C}_i\right) \in \left[\sum_{i=1}^{m} \sigma\left(\mathcal{C}_i\right) - \sum_{1 \leq i < j \leq m} \sigma\left(\mathcal{C}_{i,j}\right), \sum_{i=1}^{m} \sigma\left(\mathcal{C}_i\right)\right]$$

Now we give a more specific description. It is noted that if $2\theta^* \geq \frac{\pi}{2} - \epsilon(M)$, the spherical caps may intersect. From Proposition 3, if $\theta_{i,j} \geq 2\theta^*$, we have $\sigma\left(\mathcal{C}_{i,j}\right) = 0$. Otherwise, if $\theta_{i,j} < 2\theta^*$, we have (n is assumed to be even, which is always true in practice)

$$\sigma\left(\mathcal{C}_{i,j}\right) = \frac{J_{2kn}\left(\widetilde{\theta}_{i,j}, \theta^*\right) + J_{2kn}\left(\theta_{i,j} - \widetilde{\theta}_{i,j}, \theta^*\right)}{2\pi P_{kn-1}},$$

where $\widetilde{\theta}_{i,j} = \arctan\left(\frac{1}{\sin(\theta_{i,j})} - \frac{1}{\tan(\theta_{i,j})}\right), 1 \leq i < j \leq m$. Hence,

$$\sigma\left(\bigcup_{i=1}^{m} \mathcal{C}_i\right) \geq \frac{m}{2} I_{\sin^2\theta^*}\left(kn - \frac{1}{2}, \frac{1}{2}\right) - \sum_{1 \leq i < j \leq m} \frac{J_{2kn}\left(\widetilde{\theta}_{i,j}, \theta^*\right) + J_{2kn}\left(\theta_{i,j} - \widetilde{\theta}_{i,j}, \theta^*\right)}{2\pi P_{kn-1}}.$$

We denote the right-hand side of the above inequality by $\Omega(m)$, which represents the second-order approximation of the proportion of key candidates that can be excluded by m successful decryption. It can be calculated efficiently using the codes in [18].

On the other hand, if $2\theta^* < \frac{\pi}{2} - \epsilon(M)$, the probability that $\sigma\left(\mathcal{C}_{i,j}\right) = 0$ is at least $1 - \frac{1}{2^M}$ for each pair of (i, j). Hence, one can take M to be a large integer, then the following

$$\sigma\left(\bigcup_{i=1}^{m} \mathcal{C}_i\right) = \frac{m}{2} I_{\sin^2\theta^*}\left(kn - \frac{1}{2}, \frac{1}{2}\right)$$

holds with a probability no less than $\left(1-\frac{1}{2^M}\right)^{\frac{m(m-1)}{2}}$.

There is a little trick for picking a suitable M. Since $\lim_{x\to\infty}\left(1-\frac{1}{x}\right)^x=\frac{1}{e}$, the attacker can take $M=\left\lceil \log_2\left(\frac{m(m-1)}{2}\right)\right\rceil$ to make sure the probability is no less than $\frac{1}{e}$.

In fact, in the case where $2\theta^*<\frac{\pi}{2}-\epsilon(M)$, we can refine our results slightly. Since $\theta\left(\overline{\overline{C_i^{(r_i)}}},\overline{\overline{C_j^{(r_j)}}}\right)=\pi-\theta\left(\overline{\overline{C_i^{(r_i)}}},-\overline{\overline{C_j^{(r_j)}}}\right)$, $\theta\left(\overline{\overline{C_i^{(r_i)}}},-\overline{\overline{C_j^{(r_j)}}}\right)$ also belongs to $\left[\frac{\pi}{2}-\epsilon(M),\frac{\pi}{2}+\epsilon(M)\right]$ when $\theta_{i,j}\in\left[\frac{\pi}{2}-\epsilon(M),\frac{\pi}{2}+\epsilon(M)\right]$. So in this case, if we consider two caps associated with each query, the result can be improved to: $\sigma\left(\bigcup_{i=1}^{m}\mathcal{C}\left(2kn,\pm\overline{\overline{C_i^{(r_i)}}},\theta^*\right)\right)=mI_{\sin^2\theta^*}\left(kn-\frac{1}{2},\frac{1}{2}\right)$ with a probability no less than $\left(1-\frac{1}{2^M}\right)^{\frac{m(m-1)}{2}}$.

Then, Proposition 1 can be further extended to the following theorem.

Theorem 4. *Suppose that an adversary has made m successful queries to the decryption oracle. The proportion of excluded key candidates is greater than $\Omega(m)$. Moreover, for a positive integer M, if $2\theta^*<\frac{\pi}{2}-\epsilon(M)$, this proportion is at least $mI_{\sin^2_{\theta^*}}\left(kn-\frac{1}{2},\frac{1}{2}\right)$ with a probability no less than $\left(1-\frac{1}{2^M}\right)^{\frac{m(m-1)}{2}}$.*

The experimental data in Sect. 6 shows that, the results of the first-order and the second-order approximations are usually very close. Therefore, we can always get a finer range of the proportion of key candidates that can be excluded.

In the analysis above, we only consider one (or two) of the caps for each query because of the strong correlation between two different rotations of the same query. Theorem 3 does not apply in this case.[9] Moreover, we also give some results on the overlaps among different caps of the same query in Appendix D.

5.3 The Decryption Failure Probability

In this paper, we have been using the relationship between the fact that C fails to be correctly decrypted and the event that $\overline{\overline{S}}$ belongs to some spherical caps about C. However, how much are the two different? In this subsection, we discuss the relationship between their probabilities.

For each query C_i, we write F_i to denote the event that "C_i fails", S_i to denote the event "C_i succeeds". We denote $P[F_i]$ to be the unconditional failure probability of C_i (i.e., the probability is independent of the status of the previous decryptions). $P[F_i]$ is estimated in [10] for the first time, and is further improved by [9]. The main idea for calculating $P[F_i]$ is that, the longer C_i is, the more likely it is to fail.

[9] It is noted that, from our experiments, the coefficient vectors of different rotations of the same query are always nearly orthogonal in practice, so the actual situation of the attack may be better than that stated in Theorem 4.

Recall that $\mathcal{C}_i = \mathcal{C}\left(2kn, \overline{\overline{C_i^{(r_i)}}}, \theta^*\right), i = 1, 2, \cdots, m$. Now let us describe the relationship between $P[F_i]$ and $\sigma(\mathcal{C}_i)$. Because the failure of C_i is a necessary condition for $\overline{\overline{S}} \in \mathcal{C}_i$, the probability of $\overline{\overline{S}} \in \mathcal{C}_i$ should not be greater than that of F_i, in the sense that

$$P[F_i] \geq Pr\left[\overline{\overline{S}} \in \mathcal{C}_i\right] = \sigma(\mathcal{C}_i).$$

It should be noted that, since we have scaled up some conditions in the derivation in Sect. 4.1 and Sect. 5.2, $P[F_i]$ is very unlikely to be $\sigma(\mathcal{C}_i)$.[10]

Moreover, besides excluding wrong key candidates, the information obtained by successful decryptions can also give us a more accurate description of the failure probability of each query. For simplicity, let us take the case of two queries C_1 and C_2. We suppose that C_1 has been successful, then the posterior decryption failure probability of C_2 will be influenced by C_1. According to Bayes' theorem,

$$P[F_2|S_1] = \frac{P[S_1|F_2]}{P[S_1]} \cdot P[F_2] = \frac{P[S_1|F_2]}{1 - P[F_1]} \cdot P[F_2] = \frac{1 - P[F_1|F_2]}{1 - P[F_1]} \cdot P[F_2].$$

As previously mentioned, $P[F_1]$ and $P[F_2]$ can be estimated according to [9, 10]. Furthermore, how to estimate the failure probabilities of subsequent queries after one or more failed queries is exactly what failure boosting studied. The way of calculating $P[F_1|F_2]$ is proposed in [12] and improved in [9]. Hence, a more accurate characterization of the failure probability of C_2 can be obtained.

In summary, the method used for calculating the failure probability in failure boosting can be applied in a similar way to the case where the decryptions are successful. By using the information obtained by successful decryptions, a more accurate way of estimating the posterior decryption failure probability is obtained.

6 (R/M-)LWE-Based Public-Key Encryption Schemes

In the previous sections, by using (recent) precise geometric formulas, we get some finer numerical indication about the proportion of key candidates that can be excluded when an adversary makes successful queries to the decryption oracle. The decryption failure probability of (R/M-)LWE/LWR-based schemes has been analyzed in terms of more accurate formulations.

In this section, we use our analysis to specific encryption schemes including Kyber [3,6], Saber [4], Frodo [20], and Newhope [1]. We adopt $m = 2^{64}$ (the largest number of queries allowed by NIST) and $M = \log_2\left(\frac{m(m-1)}{2}\right)$ in

[10] An experiment in [Table 2, [5]] shows that $P[F_i]$ and $\sigma(\mathcal{C}_i)$ are approximately equal. This result is due to the incorrect use of $\frac{q}{4} - \gamma$, resulting in an overestimate of $\sigma(\mathcal{C}_i)$. In fact, from our experiments in Sect. 6, these two values will be very different in all schemes.

the following experiments. Given the failure probability δ (available from each parameter set of each individual scheme), we calculate the following values and display them in Table 2:

- $\epsilon(M)$, the maximum difference between the angles among queries and $\frac{\pi}{2}$, in the sense that, each angle will belong to $\left[\frac{\pi}{2}-\epsilon(M), \frac{\pi}{2}+\epsilon(M)\right]$ with a probability at least $1-\frac{1}{2^M}$.
- θ^*, the angle that an attacker can obtain.
- $\frac{1}{2}I_{\sin^2\theta^*}\left(kn-\frac{1}{2},\frac{1}{2}\right)$, the proportion of key candidates in each spherical cap.
- $J_{2kn}\left(\frac{\pi}{4},\theta^*\right)$, a quantity characterizing the overlaps. The larger $J_{2kn}\left(\frac{\pi}{4},\theta^*\right)$ is, the bigger the overlaps are.
- $\widetilde{\Omega}(m)$, an estimate of $\Omega(m)$, to be exact, an estimate of the second-order approximation of the proportion of key candidates that can be excluded by m successful decryption.

The estimation $\widetilde{\Omega}(m)$ of $\Omega(m)$ is derived by the following process. Since $\left|\theta_{i,j}-\frac{\pi}{2}\right| \le \epsilon(M)$ with a probability no less than $1-\frac{1}{2^M}$, and $\epsilon(M)$ is always a very small angle in practice, we have

$$\theta_{i,j} \approx \frac{\pi}{2} \quad \text{and} \quad \widetilde{\theta}_{i,j} \approx \arctan(1) = \frac{\pi}{4}.$$

From the fact that $\sqrt{\pi d+\frac{\pi}{4}} < \frac{1}{P_d} \le \sqrt{\pi d+4-\pi}$ for any positive integer d, an estimate of $\Omega(m)$ is obtained:

$$\widetilde{\Omega}(m) := \frac{m}{2}I_{\sin^2\theta^*}\left(kn-\frac{1}{2},\frac{1}{2}\right) - \frac{m^2 J_{2kn}\left(\frac{\pi}{4},\theta^*\right)\cdot\sqrt{\pi(kn-1)}}{2\pi}.$$

Table 2. A summary of some security parameters for NIST post-quantum schemes.

schemes	δ	$\epsilon(M)$	θ^*	$\frac{1}{2}I_{\sin^2\theta^*}\left(kn-\frac{1}{2},\frac{1}{2}\right)$	$J_{2kn}\left(\frac{\pi}{4}\right)$	$\widetilde{\Omega}(m)$
Kyber512	2^{-139}	4.87°	55.15°	2^{-297}	2^{-796}	2^{-233}
Kyber768	2^{-164}	4.08°	59.68°	2^{-331}	2^{-805}	2^{-267}
Kyber1024	2^{-174}	3.60°	66.65°	2^{-258}	2^{-572}	2^{-194}
LightSaber	2^{-120}	4.87°	56.20°	2^{-278}	2^{-727}	2^{-215}
Saber	2^{-136}	4.08°	65.90°	2^{-207}	2^{-464}	2^{-143}
FireSaber	2^{-165}	3.60°	69.54°	2^{-198}	2^{-429}	2^{-134}
Newhope512	2^{-213}	4.87°	20.03°	$<2^{-1000}$	\	\
Newhope1024	2^{-216}	3.60°	61.98°	2^{-374}	2^{-876}	2^{-310}
Frodo640	2^{-139}	4.42°	66.10°	2^{-171}	2^{-382}	2^{-107}

As can be seen from Table 2, all schemes except Newhope512 satisfy $2\theta^* > \frac{\pi}{2}+\epsilon(M)$, so there are overlaps in these cases. However, as the fact that $J_{2kn}\left(\frac{\pi}{4}\right) \ll I_{\sin^2\theta^*}\left(kn-\frac{1}{2},\frac{1}{2}\right)$ in all schemes, the surface area of the overlap

between two spherical caps is much smaller than that of these two caps. Therefore, for these schemes, the effect of overlaps is far from significant and $\widetilde{\Omega}(m)$ is a sufficiently accurate estimation of the proportion of key candidates that can be excluded by m successful decryption. As for Newhope512, since it satisfies $2\theta^* < \frac{\pi}{2} - \epsilon(M)$, the proportion of excluded key candidates is no less than $mI_{\sin^2\theta^*}\left(kn - \frac{1}{2}, \frac{1}{2}\right)$ with overwhelming probability. It is noted that because θ^* is small in Newhope512, $I_{\sin^2\theta^*}\left(kn - \frac{1}{2}, \frac{1}{2}\right)$ is too small to be calculated.

Recall that $\frac{1}{2}I_{\sin^2\theta^*}\left(kn - \frac{1}{2}, \frac{1}{2}\right)$ is the proportion of key candidates in a single spherical cap. We can see that $\delta \gg \frac{1}{2}I_{\sin^2\theta^*}\left(kn - \frac{1}{2}, \frac{1}{2}\right)$ in all schemes as mentioned earlier in Sect. 5.3. Such proportion of key candidates was calculated in [Table 1 (Adversary $\mathcal{B}$), [5]] using the approximation $Q_\alpha(\chi_e(2), \chi_e(2))$. It is pointed out that such an approximation is based on an erroneous interpretation of θ^* (i.e., incorrect use of $\frac{q}{2} - \gamma$). From the comparisons in Table 3, we can see that the values given in [5] are significantly bigger than the ones obtained after correction and by using accurate formulas. It is remarked that experimental data also shows that the security of those schemes in our discussion is not affected by knowing the key candidates are excluded from those spherical caps.

Table 3. Comparison with [5]

schemes	$2Q_\alpha(\chi_e(2), \chi_e(2))$ in [5]	$I_{\sin^2\theta^*}\left(kn - \frac{1}{2}, \frac{1}{2}\right)$ in this paper
Kyber512	2^{-187}	2^{-296}
Kyber768	2^{-169}	2^{-330}
Kyber1024	2^{-178}	2^{-257}
LightSaber	2^{-123}	2^{-278}
Saber	2^{-139}	2^{-206}
FireSaber	2^{-170}	2^{-197}
Frodo640	2^{-146}	2^{-170}

In the next subsection, we give the detailed calculation of each parameter of specific example of Saber. The calculations of other schemes can be seen in Appendix E.

6.1 Saber

Saber is a MLWR-based lattice scheme, and a third round candidate in NIST's post-quantum standardization effort. Its key generation, encryption, decryption algorithms as well as its common parameter set are given in [4]. The error term of Saber is the following

$$\omega = s'^T u - u'^T s + e_r,$$

where $s, s' \leftarrow \beta_\mu$, u and u' is the compression error of As and $A^T s'$ respectively. $e_r \in R_q$ is a polynomial with uniformly distributed coefficients in the range $\left[-\frac{p}{2t}, \frac{p}{2t}\right]$. Using the previous notation, we write

$$S = \begin{pmatrix} -s \\ u \end{pmatrix},\ C = \begin{pmatrix} u' \\ s' \end{pmatrix} \text{ and } G = e_r.$$

In Saber, $k = 3, n = 256, q = 2^{13}, p = 2^{10}, t = 2^4, \mu = 4, \delta = 2^{-136}$. Since $\frac{q}{p} = 8$, then from Theorem 1, each coefficient of each polynomial of u, u' is uniformly random in $\mathbb{Z}_8$. Let $\mathcal{E}_u$ be the expected values of $\|u\|$. Meanwhile, $\mathcal{E}_{u'}, \mathcal{E}_s, \mathcal{E}_{s'}$ and so on are defined in the same way. Then it can be calculated that $\mathcal{E}_u = \mathcal{E}_{u'} = \sqrt{4224}$.

As for the norm of s and s', since each coefficient of each polynomial of s, s' follows β_4, which is centered and has a variance of 2, we have $\mathcal{E}_s = \mathcal{E}_{s'} = \sqrt{1536}$.

As mentioned in [5], due to the difference in size between the coefficients of u' and s', we need to isotropize C. Let $w = \sqrt{\frac{\mathcal{E}_{s'}}{\mathcal{E}_{u'}}}$, we denote $\widetilde{S} = \begin{pmatrix} -\frac{s}{w} \\ u \cdot w \end{pmatrix}$ and $\widetilde{C} = \begin{pmatrix} u' \cdot w \\ \frac{s'}{w} \end{pmatrix}$. It is noted that $\langle \widetilde{S}, \widetilde{C} \rangle = \langle S, C \rangle$ and the expected values of $\|u' \cdot w\|, \left\| \frac{s'}{w} \right\|$ are both $\sqrt{\mathcal{E}_{u'} \cdot \mathcal{E}_{s'}}$. According to the above, we have

$$\mathcal{E}_{\widetilde{S}} = \mathcal{E}_{\widetilde{C}} = \sqrt{2 \times \mathcal{E}_{u'} \cdot \mathcal{E}_{s'}} \approx 84.88.$$

It's easy to see that $\gamma = \frac{p}{2t} = 32$, then

$$\theta^*_{Saber} = \arccos\left(\frac{\frac{q}{4} + \gamma}{\mathcal{E}_{\widetilde{C}} \cdot \mathcal{E}_{\widetilde{S}}}\right) \approx 65.90^\circ \text{ and } I_{\sin^2(\theta^*_{Saber})}\left(kn - \frac{1}{2}, \frac{1}{2}\right) \approx 2^{-206}.$$

Finally, as $J_{2kn}\left(\frac{\pi}{4}, \theta^*_{Saber}\right) \approx 2^{-464} \ll 2^{-206} \approx I_{\sin^2(\theta^*_{Saber})}\left(kn - \frac{1}{2}, \frac{1}{2}\right)$, the impact of the overlaps is negligible. Hence, the proportion of excluded key candidates after m successful queries is about

$$\widetilde{\Omega}(m) = \frac{m}{2} I_{\sin^2 \theta^*_{Saber}}\left(kn - \frac{1}{2}, \frac{1}{2}\right) - \frac{m^2 J_{2kn}\left(\frac{\pi}{4}, \theta^*_{Saber}\right) \cdot \sqrt{\pi(kn-1)}}{2\pi} \approx 2^{-143}.$$

A The Proof of Theorem 1

Let us consider the distribution of $CD_{p,q}(y)$. First of all, we start with a special case where $p = 1$, then

$$CD_{1,q}(y) = y - \left\lceil q \left\lceil \frac{1}{q} y \right\rfloor \right\rfloor.$$

Let $y = aq + b$ with b being the minimum absolute residue, i.e., $b = y \bmod q$, then

$$CD_{1,q}(y) = y - \left\lceil q \left\lceil \frac{1}{q} y \right\rfloor \right\rfloor = y - q \cdot \left\lceil \frac{aq + b}{q} \right\rfloor = y - aq = b.$$

In addition, when y is uniformly random in $\mathbb{Z}$ or $\mathbb{Z}_q$, $CD_{1,q}(y)$ is uniformly random in $\mathbb{Z}_q$.

Now we consider the general case. We decompose py into $py = aq + b$ in a similar manner, where $b = py \bmod q$, then

$$y - \left\lceil \frac{q}{p} \left\lceil \frac{p}{q} y \right\rfloor \right\rfloor = y - \left\lceil \frac{1}{p} \cdot q \left\lceil \frac{1}{q} (py) \right\rfloor \right\rfloor = y - \left\lceil \frac{1}{p} \cdot (py - b) \right\rfloor = y - \left\lceil y - \frac{b}{p} \right\rfloor = \left\lceil \frac{b}{p} \right\rfloor.$$

In this case, the value of $CD_{p,q}(y)$ entirely depends on b. The following two situations are of interest in practice.

1. $\gcd(p, q) = 1$
   In this case, when y is uniformly random in $\mathbb{Z}$ or $\mathbb{Z}_q$, $b = py \bmod q$ is also uniformly random in $\mathbb{Z}_q$, then $CD_{p,q}(y)$ is uniformly random in $\left\lceil \frac{\mathbb{Z}_q}{p} \right\rfloor$. In other words, $CD_{p,q}(y)$ belongs to $\left\{ -\left\lceil \frac{q}{2p} \right\rfloor, \cdots, \left\lceil \frac{q}{2p} \right\rfloor \right\}$ and has the same probability at all integer points inside except $-\left\lceil \frac{q}{2p} \right\rfloor$ and $\left\lceil \frac{q}{2p} \right\rfloor$.
   In particular, when $\frac{q}{2} \gg p$, we can roughly think that $CD_{p,q}(y)$ is uniformly random in $\left\{ -\left\lceil \frac{q}{2p} \right\rfloor, \cdots, \left\lceil \frac{q}{2p} \right\rfloor \right\}$.

2. $p|q$

   We denote $m = \frac{q}{p}$, then

$$CD_{p,q}(y) = y - \left\lceil \frac{q}{p} \left\lceil \frac{p}{q} y \right\rfloor \right\rfloor = y - \left\lceil m \left\lceil \frac{1}{m} y \right\rfloor \right\rfloor = CD_{1,m}(y).$$

   We decompose y into $y = cm + d$, where $d = y \bmod m$, then we have

$$CD_{p,q}(y) = CD_{1,m}(y) = d.$$

   Thus, when y is uniformly random in $\mathbb{Z}$ or $\mathbb{Z}_q$, $CD_{p,q}(y)$ is uniformly random in $\mathbb{Z}_m$.

B The Proof of Proposition 2

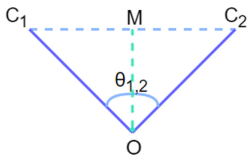

Fig. 1. The construction of C'.

As shown in Fig. 1, let O be the center of $\mathcal{S}_d$. Since $\overline{\overline{C_1}}, \overline{\overline{C_2}} \in \mathcal{S}_d$, then $O\overline{\overline{C_1}} = O\overline{\overline{C_2}} = 1$ and

$$ip_{1,2} = \langle \overline{\overline{C_1}}, \overline{\overline{C_2}} \rangle = \left\| \overline{\overline{C_1}} \right\| \cdot \left\| \overline{\overline{C_2}} \right\| \cdot \cos(\theta_{1,2}) = \cos(\theta_{1,2})$$

We denote M to be the midpoint of $\overline{\overline{C_1C_2}}$. According to the properties of isosceles triangles, we know that

$$\theta\left(O\overline{\overline{C_1}}, OM\right) = \frac{1}{2}\theta_{1,2} \text{ and } \overline{\overline{C_1}}M \perp OM$$

Hence,

$$\frac{1}{2}d_{1,2} = \left|M\overline{\overline{C_1}}\right| = \frac{\left|M\overline{\overline{C_1}}\right|}{\left|O\overline{\overline{C_1}}\right|} = \sin\left(\theta\left(O\overline{\overline{C_1}}, OM\right)\right) = \sin\left(\frac{1}{2}\theta_{1,2}\right)$$

C The Proof of Theorem 2

For $\overline{\overline{C_1}}$, $\overline{\overline{C_2}} \in \mathcal{S}_{2kn}$, let $\theta_{1,2}, d_{1,2}, ip_{1,2}$ and $\mathcal{C}_{1,2}$ be as in Sect. 5, then

$$\begin{aligned}\mathcal{C}_{1,2} \neq \emptyset &\iff \exists x \in \mathcal{S}_{2kn}, \text{ such that } x \in \mathcal{C}\left(2kn, \overline{\overline{C_1}}, \theta^*\right) \text{ and } x \in \mathcal{C}\left(2kn, \overline{\overline{C_2}}, \theta^*\right) \\ &\iff \exists x \in \mathcal{S}_{2kn}, \text{ such that } \theta\left(x, \overline{\overline{C_1}}\right) < \theta^* \text{ and } \theta\left(x, \overline{\overline{C_2}}\right) < \theta^*.\end{aligned}$$

From the analysis above, to make $\mathcal{C}_{1,2} = \emptyset$ true, we need the event that at most one of $\theta\left(x, \overline{\overline{C_1}}\right) \leq \theta^*, \theta\left(x, \overline{\overline{C_2}}\right) \leq \theta^*$ is true for any $x \in \mathcal{S}_{2kn}$. It is easy to find that $\theta_{1,2} > 2\theta^*$ is a sufficient condition for $\mathcal{C}_{1,2} = \emptyset$. Because when it is true, for any $x \in \mathcal{S}_{2kn}$, $\theta\left(x, \overline{\overline{C_1}}\right) + \theta\left(x, \overline{\overline{C_2}}\right) \geq \theta_{1,2} > 2\theta^*$.

Now let us prove that $\theta_{1,2} > 2\theta^*$ is a necessary condition $\mathcal{C}_{1,2} = \emptyset$. Using Proposition 2, we can easily give its equivalent representations, namely, the disjoint condition about inner product $(ip_{1,2} < \cos(2\theta^*))$ and about distance $(d_{1,2} > 2\sin(\theta^*))$. In the following, we take $d_{1,2} > 2\sin(\theta^*)$ as an example to prove that they are all necessary conditions for $\mathcal{C}_{1,2} = \emptyset$. Because these three conditions are equivalent, this will prove that each of them is a sufficient and necessary condition for $\mathcal{C}_{1,2} = \emptyset$ respectively.

Assume that $d_{1,2} \leq 2\sin(\theta^*)$, we will show that in this case we can always find a $C' \in \mathcal{S}_{2kn}$, such that $\theta\left(C', \overline{\overline{C_1}}\right) \leq \theta^*$ and $\theta\left(C', \overline{\overline{C_2}}\right) \leq \theta^*$.

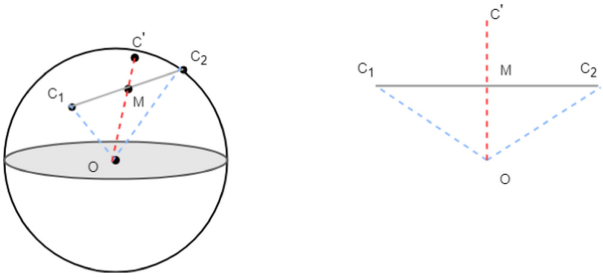

Fig. 2. The construction of C'.

Actually, as shown in Fig. 2, we denote the midpoint of $\overline{\overline{C_1}}$ and $\overline{\overline{C_2}}$ by M, and suppose that the line OM and $\mathcal{S}_{2kn}$ intersect at point C', then C' is the point we are looking for.

Since $O\overline{\overline{C_1}} = O\overline{\overline{C_2}} = 1$, the triangle $O\overline{\overline{C_1}}\,\overline{\overline{C_2}}$ is an isosceles triangle. Hence, $\theta\left(C', \overline{\overline{C_1}}\right) = \theta\left(C', \overline{\overline{C_2}}\right) = \frac{1}{2}\theta_{1,2}$. Then we have

$$\sin\left(\theta\left(C', \overline{\overline{C_1}}\right)\right) = \frac{\left|M\overline{\overline{C_1}}\right|}{\left|O\overline{\overline{C_1}}\right|} = \frac{1}{2}d_{1,2} < \sin(\theta^*).$$

Since $\theta^* < \frac{\pi}{2}$ and $\theta\left(C', \overline{\overline{C_1}}\right) = \frac{1}{2}\theta_{1,2} \leq \frac{\pi}{2}$, we have

$$\theta\left(C', \overline{\overline{C_1}}\right) < \theta^*.$$

We can prove that $\theta\left(C', \overline{\overline{C_2}}\right) < \theta^*$ in a similar way, then we know that $\mathcal{C}_{1,2} \neq \emptyset$, since $C' \in \mathcal{C}_{1,2}$.

D Some Results about the Overlaps among Different Caps of the Same Query

Let C be a query. Now let us consider the two rotations $C^{(r_1)}, C^{(r_2)} (0 \leq r_1 < r_2 \leq n-1)$ of C. Although the angle between $\overline{C^{(r_1)}}$ and $\overline{C^{(r_2)}}$ cannot be accurately described, we can instead use their inner product to analyze the overlap, achieving exactly the same effect. According to Theorem 2, the overlap between $\mathcal{C}\left(2kn, \overline{\overline{C^{(r_1)}}}, \theta^*\right)$ and $\mathcal{C}\left(2kn, \overline{\overline{C^{(r_2)}}}, \theta^*\right)$ depends entirely on $\langle\overline{C^{(r_1)}}, \overline{C^{(r_2)}}\rangle$.

It is mentioned in Sect. 2.1 that $\langle\overline{C^{(r_1)}}, \overline{C^{(r_2)}}\rangle$ is the r_2-th degree coefficient of $\langle C^{(r_1)}, C\rangle$, so we can get $\langle\overline{C^{(r_1)}}, \overline{C^{(r_2)}}\rangle$ by calculating $\langle C^{(r_1)}, C\rangle$. Let $C_{i,u} (i = 1, 2, \cdots, k; u = 0, 1, \cdots n-1)$ be the coefficient of the u-th degree coefficient of the i-th polynomial of C. From the properties of rotations given in Sect. 2.1, $\langle\overline{C^{(r_1)}}, \overline{C^{(r_2)}}\rangle$ can be represented by

$$\sum_{i=1}^{k}\left(\sum_{u=0}^{r_1} C_{i,r_1-u}C_{i,r_2-u} - \sum_{u=r_1+1}^{r_2} C_{i,n+r_1-u}C_{i,r_2-u} + \sum_{u=r_2+1}^{n-1} C_{i,n+r_1-u}C_{i,n+r_2-u}\right).$$

The following corollaries can be derived directly from Theorem 2.

Corollary 2. *For a given C and its two rotations $C^{(r_1)}, C^{(r_2)} (0 \leq r_1 < r_2 \leq n-1)$. The following are equivalent:*

1. $\mathcal{C}\left(2kn, \overline{\overline{C^{(r_1)}}}, \theta^*\right) \cap \mathcal{C}\left(2kn, \overline{\overline{C^{(r_2)}}}, \theta^*\right) = \emptyset$.
2. $\theta\left(\overline{\overline{C^{(r_1)}}}, \overline{\overline{C^{(r_2)}}}\right) > 2\theta^*$.
3. $\sum_{i=1}^{k}\left(\sum_{u=0}^{r_1} C_{i,r_1-u}C_{i,r_2-u} - \sum_{u=r_1+1}^{r_2} C_{i,n+r_1-u}C_{i,r_2-u} + \sum_{u=r_2+1}^{n-1} C_{i,n+r_1-u}C_{i,n+r_2-u}\right) < \cos(2\theta^*)\|C\|^2$.

Corollary 3. *For a given C, the following are equivalent:*

1. *all the caps* $\mathcal{C}\left(2kn, \pm\overline{\overline{C^{(r)}}}, \theta^*\right), r = 0, 1, \cdots, n-1$ *do not intersect each other.*
2. $2\theta^* < \theta\left(\overline{\overline{C^{(r_1)}}}, \overline{\overline{C^{(r_2)}}}\right) < \pi - 2\theta^*$, *for any* $0 \le r_1 < r_2 \le n-1$.
3. $$\left|\sum_{i=1}^{k}\left(\sum_{u=0}^{r_1} C_{i,r_1-u}C_{i,r_2-u} - \sum_{u=r_1+1}^{r_2} C_{i,n+r_1-u}C_{i,r_2-u} + \sum_{u=r_2+1}^{n-1} C_{i,n+r_1-u}C_{i,n+r_2-u}\right)\right| < \cos(2\theta^*)\|C\|^2,$$ *for any* $0 \le r_1 < r_2 \le n-1$.

The above corollary deals with the overlaps among $2n$ spherical caps in W_C, and gives the conditions for a query C to achieve the best query effect. This may provide advice to the attacker on how to choose queries.

E (R/M-)LWE-Based Public-Key Encryption Schemes

E.1 Kyber

Kyber is a MLWE-based lattice scheme, and a third round candidate in NIST's post-quantum standardization effort. [3] introduces the key generation, encryption, decryption algorithm of Kyber, and gives its common parameter set. [6] proves that the error term of Kyber is

$$\omega = e^T r + e_2 + c_v - s^T e_1 - s^T c_u,$$

where $e, s, r, e_1 \leftarrow \beta_{\eta_1}, e_2 \leftarrow \beta_{\eta_2}, c_u \leftarrow \psi^k_{2^{d_u},q}$, $c_v \leftarrow \psi^k_{2^{d_v},q}$. Using the previous notation, we write

$$S = \begin{pmatrix} -s \\ e \end{pmatrix},\ C = \begin{pmatrix} e_1 + c_u \\ r \end{pmatrix} \text{ and } G = e_2 + c_v.$$

Since all parameter sets of Kyber have $q = 3329$, then $\gcd(2^{d_u}, q) = 1$, $\gcd(2^{d_v}, q) = 1$. We denote the j-th degree coefficient of the i-th polynomial of c_u and c_v by $(c_u)_{i,j}$ and $(c_v)_{i,j}$ respectively, then from Theorem 4.1, $(c_u)_{i,j} = \left\lceil \frac{(b_u)_{i,j}}{2^{d_u}} \right\rfloor$, where $(b_u)_{i,j}, i = 1, \cdots, k, j = 0, 1, \cdots, n-1$ are independent and all uniformly random in $\mathbb{Z}_q$. $(c_v)_{i,j} = \left\lceil \frac{(b_v)_{i,j}}{2^{d_v}} \right\rfloor$, where $(b_v)_{i,j}, i = 1, \cdots, k, j = 0, 1, \cdots, n-1$ are independent and all uniformly random in $\mathbb{Z}_q$.

Let us take Kyber768 as an example, then $d_u = 10, d_v = 4, \eta_1 = \eta_2 = 2, \delta = 2^{-164}$. It can be prove that the expected value of $|(c_u)_{i,j}|$ is about $\sqrt{\frac{13}{14}}$. As for the value of $(c_v)_{i,j}$, since $q >> 2^{d_v}$ and $\frac{q/2}{2^4} \approx 104$, we can approximately think that $(c_v)_{i,j}$ is uniformly random in $[-104, 104]$.

As for the values of other parameters, since $\|G\|_\infty \le \|e_2\|_\infty + \|c_v\|_\infty \approx \eta_2 + 104 = 106$, we can take $\gamma = 106$. Taking $M = \log_2\left(\frac{m(m-1)}{2}\right)$, we have $\epsilon(M) \approx 4.08°$. As $s, e, r, e_1, e_2 \sim \beta_2$, and the variance of β_2 is 1, we have $\mathcal{E}_s = \mathcal{E}_e = \mathcal{E}_r = \mathcal{E}_{e_1} = \sqrt{768}$. Since e_1, c_u are independent, we have $D[(c_u + e_1)_{i,j}] = D[(c_u)_{i,j}] + D[(e_1)_{i,j}] = \frac{27}{14}$, then $\mathcal{E}_{e_1+c_u} \approx \sqrt{1481}$.

Just like before, due to the difference in size between the coefficients of $e_1 + c_u$ and r, we need to isotropize C. Let $w = \sqrt{\frac{\mathcal{E}_r}{\mathcal{E}_{e_1+c_u}}}$, then we form $\widetilde{S} = \begin{pmatrix} -\frac{s}{w} \\ e \cdot w \end{pmatrix}$ and $C = \begin{pmatrix} (e_1 + c_u) \cdot w \\ \frac{r}{w} \end{pmatrix}$. It is noted that $\langle \widetilde{S}, \widetilde{C} \rangle = \langle S, C \rangle$ and the expected values of $\|(e_1 + c_u) \cdot w\|, \left\|\frac{r}{w}\right\|$ are both $\sqrt{\mathcal{E}_{e_1+c_u} \cdot \mathcal{E}_r}$. According to the above, we have

$$\mathcal{E}_{\widetilde{S}} \approx 40.24 \text{ and } \mathcal{E}_{\widetilde{C}} \approx 46.19.$$

Then the angle that the attacker can obtain is $\theta^*_{Kyber768} = \arccos\left(\frac{\frac{q}{4}+\gamma}{\mathcal{E}_{\widetilde{S}} \cdot \mathcal{E}_{\widetilde{C}}}\right) \approx 59.68°$, the proportion is $I_{\sin^2(\theta^*_{Kyber768})}\left(kn - \frac{1}{2}, \frac{1}{2}\right) \approx 2^{-330}$. Finally, it can be calculated that $J_{2kn}\left(\frac{\pi}{4}, \theta^*_{Kyber768}\right) \approx 2^{-805}$ and $\widetilde{\Omega}(m) \approx 2^{-267}$.

E.2 Newhope

Newhope is a RLWE-based lattice scheme, which is proposed by Alkim et al. [2] in 2016. [1] describes in detail the key generation, encryption and decryption algorithm of Newhope. The error term of Newhope is

$$\omega = es' - e's + e'' + c_v,$$

where $e, s, s', e', e'' \leftarrow \beta_\mu, c_v \leftarrow \psi_{8,q}$. Using the previous notation, we write

$$S = \begin{pmatrix} -s \\ e \end{pmatrix}, \ C = \begin{pmatrix} e' \\ s' \end{pmatrix} \text{ and } G = e'' + c_v.$$

Let us take Newhope1024 as an example, then $n = 1024, q = 12289, \mu = 8, \delta = 2^{-216}$. From Theorem 1, since $\frac{q/2}{8} \approx 768$, we can approximately think that $(c_v)_{i,j}$ is uniformly random in $[-768, 768]$.

Now let us calculate the values of other parameters. Taking $M = \log_2\left(\frac{m(m-1)}{2}\right)$, we have $\epsilon(M) \approx 3.60°$. Since $\|G\|_\infty \leq \|e''\|_\infty + \|c_v\|_\infty \leq 8 + 768 = 776$, we can take $\gamma = 776$. As $S, C \sim \beta_8$, and the variance of β_8 is 4, we have $\mathcal{E}_S = \mathcal{E}_C = \sqrt{8192}$. Then the angle is $\theta^*_{Newhope1024} = \arccos\left(\frac{\frac{q}{4}+\gamma}{\mathcal{E}_S \cdot \mathcal{E}_C}\right) \approx 61.98°$ and the proportion is $I_{\sin^2(\theta^*_{Newhope1024})}\left(n - \frac{1}{2}, \frac{1}{2}\right) \approx 2^{-372.89}$. Finally, it can be calculated that $J_{2n}\left(\frac{\pi}{4}, \theta^*_{Newhope1024}\right) \approx 2^{-876}$ and $\widetilde{\Omega}(m) \approx 2^{-310}$.

E.3 Frodo

Frodo is a LWE-based lattice scheme, and a second round candidate in NIST's post-quantum standardization effort. [20] introduces the basic information about Frodo. The success condition is

$$\|E'''\|_\infty < \frac{q}{2^{B+1}},$$

where $E''' = S'E - E'S + E'', S, E \in \mathbb{Z}_q^{n\times\overline{n}},\ S', E' \in \mathbb{Z}_q^{\overline{m}\times n},\ E'' \in \mathbb{Z}_q^{\overline{m}\times\overline{n}}$, and each of their elements is sampled from the distribution χ (an approximation to the discrete Gaussian distribution).

Let us take Frodo640 as an example, then $q = 2^{15}, n = 640, \gamma = 12, \overline{m} = \overline{n} = 8, B = 2$ and $\delta = 2^{-139}$. It can be calculated that $\epsilon(M) \approx 4.42°$. [20] gives the probability distribution function of χ. For any $a \leftarrow \chi$, the expected value of a^2 is $\frac{64895}{2^{13}} \approx 7.92$.

As S, S', E, E', E'' are all matrices, the angles are uncomputable. Some transformation is needed. We write $S = (s_1\ s_2\ \cdots s_{\overline{n}}),\ E = (e_1\ e_2\ \cdots e_{\overline{n}})$ where $s_i, e_i, i = 1, 2, \cdots, \overline{n}$ are all column vectors. We write $S' = \begin{pmatrix} s'_1 \\ \vdots \\ s'_{\overline{m}} \end{pmatrix}, E' = \begin{pmatrix} e'_1 \\ \vdots \\ e'_{\overline{m}} \end{pmatrix}$ where $s'_j, e'_j, j = 1, 2, \cdots, \overline{m}$ are all row vectors. Then the success condition can be further expressed as

$$\left|s'_j e_i - e'_j s_i + e''_{ij}\right| < \frac{q}{8}, i, j = 1, 2, \cdots, 8.$$

Just like [5], we consider each entry of E''' respectively. For each pair of (i, j), the angle that an attacker can obtain is $\theta^*_{Frodo640} = \arccos\left(\frac{\frac{q}{8}+\gamma}{\sqrt{2\times n\times 7.92}\times\sqrt{2\times n\times 7.92}}\right) \approx 66.10°$, and the proportion is $I_{\sin^2(\theta^*_{Frodo640})}(n-\frac{1}{2}, \frac{1}{2}) \approx 2^{-169.6}$. Finally, it can be calculated that $J_{2n}\left(\frac{\pi}{4}, \theta^*_{Frodo640}\right) \approx 2^{-381.6}$ and $\widetilde{\Omega}(m) \approx 2^{-106.6}$.

References

1. Alkim, E., et al.: NewHope algorithm specifications and supporting documentation. NIST PQC Round **2**, 4–11 (2019)
2. Alkim, E., Ducas, L., Pöppelmann, T., Schwabe, P.: Post-quantum key exchange: a new hope. In: Proceedings of the 25th USENIX Conference on Security Symposium, pp. 327–343 (2016)
3. Avanzi, R., et al.: CRYSTALS-Kyber algorithm specifications and supporting documentation. NIST PQC Round **2**, 4 (2019)
4. Basso, A., et al.: SABER: mod-LWR based KEM (round 3 submission) (2020)
5. Bindel, N., Schanck, J.M.: Decryption failure is more likely after success. In: International Conference on Post-Quantum Cryptography, pp. 206–225 (2020)
6. Bos, J., et al.: CRYSTALS-Kyber: a CCA-secure module-lattice-based KEM. In: European Symposium on Security and Privacy, pp. 353–367 (2018)
7. Cai, T.T., Fan, J., Jiang, T.: Distributions of angles in random packing on spheres. J. Mach. Learn. Res. **14**, 1837 (2013)
8. Cao, J., Niu, D.W., Qi, F.: A Wallis type inequality and a double inequality for probability integral. Aust. J. Math. Anal. Appl. **4**, 6 (2007). Art. 3
9. D'Anvers, J.P., Batsleer, S.: Multitarget decryption failure attacks and their application to saber and kyber. Cryptology ePrint Archive, Report 2021/193 (2021)
10. D'Anvers, J.P., Vercauteren, F., Verbauwhede, I.: On the impact of decryption failures on the security of LWE/LWR based schemes. Cryptology ePrint Archive, Report 2018/1089 (2018)

11. D'Anvers, J.P., Guo, Q., Johansson, T., Nilsson, A., Vercauteren, F., Verbauwhede, I.: Decryption failure attacks on IND-CCA secure lattice-based schemes. In: Public-Key Cryptography - PKC 2019, pp. 565–598 (2019)
12. D'Anvers, J.P., Rossi, M., Virdia, F.: (One) failure is not an option: bootstrapping the search for failures in lattice-based encryption schemes. In: Advances in Cryptology - EUROCRYPT 2020, pp. 3–33. Springer, Cham (2020). https://doi.org/10.1007/978-3-030-45727-3_1
13. D'Anvers, J.-P., Vercauteren, F., Verbauwhede, I.: The impact of error dependencies on Ring/Mod-LWE/LWR based schemes. In: Ding, J., Steinwandt, R. (eds.) PQCrypto 2019. LNCS, vol. 11505, pp. 103–115. Springer, Cham (2019). https://doi.org/10.1007/978-3-030-25510-7_6
14. Guo, Q., Johansson, T.: A new decryption failure attack against HQC. In: Moriai, S., Wang, H. (eds.) ASIACRYPT 2020. LNCS, vol. 12491, pp. 353–382. Springer, Cham (2020). https://doi.org/10.1007/978-3-030-64837-4_12
15. Guo, Q., Johansson, T., Nilsson, A.: A generic attack on lattice based schemes using decryption errors. Cryptology ePrint Archive, Report 2019/043 (2019)
16. Guo, Q., Johansson, T., Yang, J.: A novel CCA attack using decryption errors against LAC. In: Galbraith, S.D., Moriai, S. (eds.) ASIACRYPT 2019. LNCS, vol. 11921, pp. 82–111. Springer, Cham (2019). https://doi.org/10.1007/978-3-030-34578-5_4
17. Koumandos, S.: Remarks on a paper by Chao-Ping Chen and Feng Qi. Proc. Am. Math. Soc. **134**(5), 1365–1367 (2006)
18. Lee, Y., Kim, W.C.: Concise formulas for the surface area of the intersection of two hyperspherical caps. KAIST Technical Report (2014)
19. Li, S.: Concise formulas for the area and volume of a hyperspherical cap. Asian J. Math. Stat. **4**, 66–70 (2011)
20. Naehrig, M., et al.: FrodoKEM: learning with errors key encapsulation-algorithm specifications and supporting documentation. NIST Technical Report (2019)