An upper bound on the decryption failure rate of static-key NewHope

John M. Schanck

Institute for Quantum Computing, University of Waterloo, Waterloo, Canada

Abstract. We give a new proof that the decryption failure rate of NewHope512 is at most $2^{-398.8}$. As in previous work, this failure rate is with respect to random, honestly generated, secret key and ciphertext pairs. However, our technique can also be applied to a fixed secret key. We demonstrate our technique on some subsets of the NewHope1024 key space, and we identify a large subset of NewHope1024 keys with failure rates of no more than $2^{-439.5}$.

1 Introduction

NewHope[1] is an instantiation of the Lindner–Peikert encryption scheme [2] that has been submitted to the second round of NIST's post-quantum standardization effort [4]. The NewHope decryption procedure can fail on an honestly generated ciphertext, though failures are extremely rare for the recommended parameter sets. NewHope512 and NewHope1024 are claimed to have failure rates of $\leq 2^{-213}$ and $\leq 2^{-216}$ respectively [4]. These upper bounds are already low enough to discourage reaction attacks, and the authors "do not expect [the upper bounds] to be so tight" [4, Section 4.2.7]. Nevertheless, there is interest in deriving tighter upper bounds (e.g. [6, 3]) as these could lead to parameter sets with smaller message sizes and higher security.

In the analysis of the original Lindner–Peikert scheme, a successful decryption is modelled by the event that n inner products between n pairs of random vectors all take values in some interval about zero. All $2n$ random vectors have independent and identically distributed coefficients, and it is typically feasible to compute the exact probability that one inner product is large. The decryption failure rate is no more than n times this.

NewHope is a ring variant of the Lindner–Peikert scheme. When one accounts for the ring structure, the $2n$ vectors in the model above are derived from just two vectors by way of signed cyclic permutations. This does not complicate the calculation of the decryption failure rate. However, NewHope also uses the additive threshold encoding technique of Pöppelmann and Güneysu [5]. With this technique, each bit of the shared secret is redundantly encoded into m out of n of the inner products. Because the $2n$ vectors are related, the m inner products that influence each bit of the shared secret are not independent.

[1] Throughout this document we use "NewHope" to refer to NewHope-Simple [1] (a.k.a. NewHope-CPA-PKE [4]).

1.1 Related work

If m is small, and the coefficient distribution has a narrow support, then it is feasible to calculate the exact probability of a single bit failure. As observed by Song, Lee, Lee, Shin, Kim, and No [6], if $u_1, \ldots u_m$ and $v_1, \ldots, v_m$ are random variables with the NewHope coefficient distribution, and $\mathbf{v}_2, \ldots, \mathbf{v}_m$ are $m \times 1$ vectors derived from $\mathbf{v}_1 = (v_1, \ldots, v_m)$ by signed cyclic permutations, then the exact probability of a single bit failure can be expressed in terms of the sum of n/m independent random variables distributed as $\sum_{i=1}^{m} u_i \mathbf{v}_i$.

Song, Lee, Lee, Shin, Kim, and No numerically compute the exact distribution of $\sum_{i=1}^{m} u_i \mathbf{v}_i$. They then find that the decryption failure rate of NewHope512 is no more than $2^{-399.0}$ and that the decryption failure rate of NewHope1024 is no more than $2^{-418.0}$. Plantard, Sipasseuth, Susilo, and Zucca have calculated similar failure rates using a heuristic method [3].

1.2 Contributions

The Song–Lee–Lee–Shin–Kim–No upper bound is tight, but it only measure the probability that a random honestly generated key fails to decrypt a random honestly generated ciphertext. An honest user might be more concerned about the probability that *their key* fails to decrypt a random honestly generated ciphertext.

We prove an upper bound on the probability that a fixed NewHope key fails to decrypt a random honestly generated ciphertext. We find that the average failure rate over the entire NewHope512 key space is at most $2^{-398.8}$. This essentially matches the Song–Lee–Lee–Shin–Kim–No result. The situation for NewHope1024 is more interesting, as our technique identifies a useful subset of keys with a lower than average failure rate.

We propose a fast, constant-time, procedure to sample from this subset of the NewHope1024 key space. We prove that every key output by our sampling procedure enjoy a failure rate of at most $2^{-405.2}$ (Lemma 2). Heuristically, the rate is at most $2^{-437.9}$ (Remark 1).

Finally, we provide software that computes our upper bound and its average value over certain subsets of the key space. Our software also reproduces the Song–Lee–Lee–Shin–Kim–No calculation.

1.3 Discussion

In practice, NewHope512 and NewHope1024 are perfectly correct KEMs. It is unlikely that there will be more than 2^{64} honest users. Each user fixes a set of 2^{256} possible ciphertexts as part of the Fujisaki–Okamoto transformation. The probability that there are any failures among 2^{320} key and ciphertext pairs is at most $2^{-79.0}$ for NewHope512 and at most $2^{-98.0}$ for NewHope1024. This follows from the Song–Lee–Lee–Shin–Kim–No calculation, but was not noted in [6].

Some users might prefer a more compact and/or more secure scheme over a perfectly correct scheme. We present some alternative parameters in Table 1.

Acknowledgements Thanks to Léo Ducas and Sanketh Menda for comments on drafts of this paper. This work was supported by the Institute for Quantum Computing (IQC). IQC is supported in part by the Government of Canada and the Province of Ontario

2 Preliminaries

2.1 NewHope

A complete description of the NewHope-Simple/NewHope-CPA-PKE can be found in [4]. We focus only on the parts that are relevant to our analysis. The system parameters are a *ring* R, a *dimension* n (the rank of R as a $\mathbb{Z}$-module), a *modulus* q, a *centered binomial noise parameter* k, a *ciphertext compression parameter* r, and a *redundancy parameter* m. The ring is $R = \mathbb{Z}[\mathbf{x}]/(\mathbf{x}^n + 1)$ for both of the recommended parameter sets: NewHope512 ($n = 512$, $m = 2$, $q = 12289$, $k = 8$, $r = 8$) and NewHope1024 ($n = 1024$, $m = 4$, $q = 12289$, $k = 8$, $r = 8$). Either parameter set can be used to exchange a $256(= n/m)$ bit shared secret.

2.2 The ring R

Elements of $R = \mathbb{Z}[\mathbf{x}]/(\mathbf{x}^n + 1)$ can be viewed as vectors in $\mathbb{R}^n$ by identifying the the power basis $\{1, \mathbf{x}, \mathbf{x}^2, \ldots, \mathbf{x}^{n-1}\}$ of R as an orthonormal basis of $\mathbb{R}^n$. The probability of decryption failure can then be stated in terms of the Euclidean inner product $\langle \cdot, \cdot \rangle$. We write $\bar{\mathbf{r}}$ for the image of $\mathbf{r}$ under $\mathbf{x} \mapsto -\mathbf{x}^{n-1}$. The following fact is immediate if one notes that $\bar{\mathbf{r}}$ corresponds to the transpose of $\mathbf{r}$ in the ring of "negacyclic matrices", which is isomorphic to R.

Fact 1 *The adjoint of R-multiplication by $\mathbf{r}$ is R-multiplication by $\bar{\mathbf{r}}$, i.e., $\langle \mathbf{a}, \mathbf{rb} \rangle = \langle \bar{\mathbf{r}}\mathbf{a}, \mathbf{b} \rangle$.*

2.3 Distributions on R

For a distribution χ on $\mathbb{Z}$, we view $\chi^{\times n}$ and as a distribution on R and write $\mathbf{f} \leftarrow \chi^{\times n}$ to say that the coefficients of $\mathbf{f}$ are drawn independently from χ. For distributions χ_1 and χ_2 on $\mathbb{Z}$, we write $\chi_1 * \chi_2$ for the distribution of $a + b$ with $a \leftarrow \chi_1$ and $b \leftarrow \chi_2$. The *centered binomial distribution* of parameter k, hereafter ψ_k, is the distribution of $\sum_{i=0}^{k-1} b_i - b'_i$ where b and b' are uniformly random elements of $\{0, 1\}^k$. The *compression artifact distribution* with parameters r_1 and r_2 is the distribution of $y - \lfloor z \frac{r_2}{r_1} \rceil$ when y is drawn uniformly from $\{0, 1, \ldots, r_1 - 1\}$ and $z = \lfloor y \frac{r_1}{r_2} \rceil$. Here $\lfloor \cdot \rceil$ is the nearest integer function; we apply it only to positive rationals and round 1/2 to 1. When a NewHope parameter set is clear from context, we write ρ for the compression artifact distribution with parameters $r_1 = q$ and $r_2 = r$.

3 Correctness

The NewHope key generation procedure involves ring elements $\mathbf{s}$ and $\mathbf{e}$. Key encapsulation involves ring elements $\mathbf{s}'$, $\mathbf{e}'$, and $\mathbf{e}''$. The correctness condition can be stated in terms of the quantity

$$\mathbf{d} = \mathbf{s}\mathbf{e}' + \mathbf{e}\mathbf{s}' + \mathbf{e}'', \tag{1}$$

where $\mathbf{s}, \mathbf{e}, \mathbf{s}', \mathbf{e}' \leftarrow \psi_k^{\times n}$ and $\mathbf{e}'' \leftarrow (\psi_k * \rho)^{\times n}$. The i-th coefficient of $\mathbf{d}$ is

$$\langle \mathbf{x}^i, \mathbf{d} \rangle = \langle \mathbf{x}^i \bar{\mathbf{s}}, \mathbf{e}' \rangle + \langle \mathbf{x}^i \bar{\mathbf{e}}, \mathbf{s}' \rangle + \langle \mathbf{x}^i, \mathbf{e}'' \rangle \tag{2}$$

Let $\mathbf{y} = \mathbf{x}^{n/m}$. The i-th bit of the session key will be recovered successfully if

$$\sum_{j=0}^{m-1} \left| \langle \mathbf{y}^j \mathbf{x}^i, \mathbf{d} \rangle \right| \leq \frac{mq}{4} \tag{3}$$

(c.f. [1, Line 4 of Algorithm 2]). For fixed $\mathbf{s}$ and $\mathbf{e}$ we define $\mathbf{v}_1, \ldots, \mathbf{v}_m$ to be elements of R^2 with

$$\mathbf{v}_j = \mathbf{y}^{j-1}(\bar{\mathbf{s}}, \bar{\mathbf{e}}). \tag{4}$$

With $\mathbf{w} = (\mathbf{e}', \mathbf{s}')$, this allows us to re-write Equation 3 as

$$\sum_{j=1}^{m} \left| \left\langle \mathbf{v}_j, \mathbf{x}^{-i} \mathbf{w} \right\rangle + \left\langle \mathbf{y}^{j-1}, \mathbf{x}^{-i} \mathbf{e}'' \right\rangle \right| \leq \frac{mq}{4}, \tag{5}$$

or, after applying a triangle inequality, as

$$\sum_{j=1}^{m} \left| \left\langle \mathbf{v}_j, \mathbf{x}^{-i} \mathbf{w} \right\rangle \right| \leq \frac{mq}{4} - \sum_{j=0}^{m-1} \left| \left\langle \mathbf{y}^j, \mathbf{x}^{-i} \mathbf{e}'' \right\rangle \right|. \tag{6}$$

Decryption is successful if Equation 6 holds for all $0 \leq i < n/m$; we emphasize that this is a sufficient but not necessary condition.

3.1 Dependencies between coefficients of d

It is relatively easy to calculate the exact distribution of $\left|\langle \mathbf{x}^i, \mathbf{d} \rangle\right|$, or the exact probability that $\left|\langle \mathbf{x}^i, \mathbf{d} \rangle\right| > 100$. However, the events $\left|\langle \mathbf{x}^i, \mathbf{d} \rangle\right| > 100$ and, say, $\left|\langle \mathbf{x}^{i+256}, \mathbf{d} \rangle\right| > 100$ are not independent. This makes it more difficult to calculate the exact probability that Equation 3 or 6 is violated.

As before, fix $\mathbf{s}$ and $\mathbf{e}$ and the corresponding values of $\mathbf{v}_1, \ldots, \mathbf{v}_m$. We define the Gram-Schmidt vectors and coefficients

$$\mathbf{v}_i^* = \mathbf{v}_i - \sum_{j=1}^{i-1} \mu_{i,j} \mathbf{v}_j^* \quad \text{and} \quad \mu_{i,j} = \langle \mathbf{v}_i, \mathbf{v}_j^* \rangle / \langle \mathbf{v}_j^*, \mathbf{v}_j^* \rangle$$

by induction on i, $1 \leq i \leq m$. We can then give an upper bound on the left hand side of Equation 6 in terms of the $\mu_{i,j}$:

$$\sum_{j=1}^{m} \left|\langle \mathbf{v}_j, \mathbf{x}^{-i}\mathbf{w}\rangle\right| \leq \sum_{j=1}^{m} \left(1 + \sum_{k=j+1}^{m} |\mu_{k,j}|\right) \left|\langle \mathbf{v}_j^*, \mathbf{x}^{-i}\mathbf{w}\rangle\right|. \tag{7}$$

We say that $(\mathbf{s}, \mathbf{e})$ has the α-*correlation* property if $\sum_{k=j+1}^{m} |\mu_{k,j}| \leq \alpha$, for all $1 \leq j < m$. For keys with the α-correlation property, we have

$$\sum_{j=1}^{m} \left(1 + \sum_{k=j+1}^{m} |\mu_{k,j}|\right) \left|\langle \mathbf{v}_j^*, \mathbf{x}^{-i}\mathbf{w}\rangle\right| \leq (1+\alpha) \sum_{j=1}^{m} \left|\langle \mathbf{v}_j^*, \mathbf{x}^{-i}\mathbf{w}\rangle\right|. \tag{8}$$

The right hand side is maximized when $\mathbf{x}^{-i}\mathbf{w}$ lies along a main diagonal of the parallelepiped formed by the $\mathbf{v}_j^*$. Suppose that k is such that $\left|\langle \mathbf{v}_k, \mathbf{x}^{-i}\mathbf{w}\rangle\right| \geq \left|\langle \mathbf{v}_j, \mathbf{x}^{-i}\mathbf{w}\rangle\right|$ for all j. Note that $\mathbf{v}_k = \mathbf{y}^k(\bar{\mathbf{s}}, \bar{\mathbf{e}})$ has the α-correlation property for the same values of α that $\mathbf{v}_1 = (\bar{\mathbf{s}}, \bar{\mathbf{e}})$ does, so we obtain the same correctness condition for this "rotated" key. The right hand side of Equation 8, relative to this rotated key, is no more than $(1+\alpha)\sqrt{m}\left|\langle \mathbf{v}_k, \mathbf{x}^{-i}\mathbf{w}\rangle\right|$.

The above argument implies that the i-th bit of the shared secret is decoded correctly if

$$\max_{1 \leq j \leq m} (1+\alpha)\sqrt{m}\left|\langle \mathbf{v}_j, \mathbf{x}^{-i}\mathbf{w}\rangle\right| \leq \frac{mq}{4} - \sum_{j=0}^{m-1} \left|\langle \mathbf{y}^j, \mathbf{x}^{-i}\mathbf{e}''\rangle\right|. \tag{9}$$

While this still depends on the $\mu_{i,j}$, it suggests that we can improve correctness by restricting the key space to keys with small α.

4 NewHope512

The case of $m = 2$, as in NewHope512, is particularly simple. Fact 1 implies that $\mu_{2,1} = 0$, so all keys have the α-correlation property with $\alpha = 0$. Taking a union bound over the m assignments of j and the n/m assignments of i in Equation 9, we see that the probability of failure for a fixed $\mathbf{v} = (\bar{\mathbf{s}}, \bar{\mathbf{e}})$ is no more than

$$n \cdot \Pr\left[\sqrt{2}\left|\langle \mathbf{v}, \mathbf{w}\rangle\right| + \sum_{j=0}^{1} \left|\langle \mathbf{y}^j, \mathbf{e}''\rangle\right| > \frac{q}{2}\right] \tag{10}$$

for $\mathbf{s}', \mathbf{e}' \leftarrow \psi_k^{\times n}$, $\mathbf{e}'' \leftarrow (\psi_k * \rho)^{\times n}$, $\mathbf{v} = (\bar{\mathbf{s}}, \bar{\mathbf{e}})$, and $\mathbf{w} = (\mathbf{e}', \mathbf{s}')$.

5 NewHope1024

When $m = 4$, as in NewHope1024, the following lemma shows that $(\mathbf{s}, \mathbf{e})$ has the α-correlation property with $\alpha = |\mu_{2,1}| \max\{2, 1/(1-|\mu_{2,1}|)\}$. In the subsection that follows, we describe a procedure that changes the signs of some coefficients of $(\mathbf{s}, \mathbf{e})$ to reduce $|\mu_{2,1}|$.

Lemma 1. *For all* $\mathbf{v} \in R^2$ *and* $\mu_{i,j}$, $4 \geq i > j \geq 1$, *as defined above, we have*

1. $|\mu_{2,1}| + |\mu_{3,1}| + |\mu_{4,1}| = 2\,|\mu_{2,1}|$,
2. $|\mu_{3,2}| + |\mu_{4,2}| = |\mu_{2,1}|\,/(1 - |\mu_{2,1}|)$, *and*
3. $|\mu_{4,3}| = |\mu_{2,1}|$.

Proof. Fact 1 implies $\langle \mathbf{x}^i \mathbf{v}_1, \mathbf{v}_1 \rangle = -\langle \mathbf{x}^{n-i} \mathbf{v}_1, \mathbf{v}_1 \rangle$. So $\mu_{2,1} = -\mu_{4,1}$ and $\mu_{3,1} = 0$, hence (1).

For (2), note that $\langle \mathbf{v}_i, \mathbf{v}_j \rangle = \langle \mathbf{v}_{i-j+1}, \mathbf{v}_1 \rangle$ for $i > j$. In particular, $\langle \mathbf{v}_4, \mathbf{v}_2 \rangle = \langle \mathbf{v}_3, \mathbf{v}_1 \rangle = \mu_{3,1} \langle \mathbf{v}_1, \mathbf{v}_1 \rangle = 0$. It follows that

$$\mu_{3,2} = \left(\langle \mathbf{v}_3, \mathbf{v}_2 \rangle - \mu_{2,1} \langle \mathbf{v}_3, \mathbf{v}_1 \rangle\right) / \langle \mathbf{v}_2^*, \mathbf{v}_2^* \rangle = \left(\langle \mathbf{v}_2, \mathbf{v}_1 \rangle - 0\right) / \langle \mathbf{v}_2^*, \mathbf{v}_2^* \rangle = c_1 \mu_{2,1}$$

where $c_1 = \langle \mathbf{v}_1, \mathbf{v}_1 \rangle / \langle \mathbf{v}_2^*, \mathbf{v}_2^* \rangle = 1/(1 - \mu_{2,1}^2)$. Moreover, since $\langle \mathbf{v}_4, \mathbf{v}_1 \rangle = -\langle \mathbf{v}_2, \mathbf{v}_1 \rangle$,

$$\mu_{4,2} = \left(\langle \mathbf{v}_4, \mathbf{v}_2 \rangle - \mu_{2,1} \langle \mathbf{v}_4, \mathbf{v}_1 \rangle\right) / \langle \mathbf{v}_2^*, \mathbf{v}_2^* \rangle = c_1 \mu_{2,1}^2.$$

Claim (2) follows.

For (3), we have

$$\mu_{4,3} = \left(\langle \mathbf{v}_4, \mathbf{v}_3 \rangle - \mu_{3,2} \langle \mathbf{v}_4, \mathbf{v}_2^* \rangle - \mu_{3,1} \langle \mathbf{v}_4, \mathbf{v}_1^* \rangle\right) / \langle \mathbf{v}_3^*, \mathbf{v}_3^* \rangle.$$

Observe that $\langle \mathbf{v}_4, \mathbf{v}_3 \rangle = \mu_{2,1} \langle \mathbf{v}_3, \mathbf{v}_3 \rangle$, that $\mu_{3,2} \langle \mathbf{v}_4, \mathbf{v}_2^* \rangle = \mu_{2,1} \mu_{3,2}^2 \langle \mathbf{v}_2^*, \mathbf{v}_2^* \rangle$, and that $\mu_{3,1} = 0$. We have

$$\mu_{4,3} = \mu_{2,1} \left(\langle \mathbf{v}_3, \mathbf{v}_3 \rangle - \mu_{3,2}^2 \langle \mathbf{v}_2^*, \mathbf{v}_2^* \rangle\right) / \langle \mathbf{v}_3^*, \mathbf{v}_3^* \rangle,$$

and, since $\langle \mathbf{v}_3^*, \mathbf{v}_3^* \rangle = \langle \mathbf{v}_3, \mathbf{v}_3 \rangle - \mu_{3,2}^2 \langle \mathbf{v}_2^*, \mathbf{v}_2^* \rangle$, (3) follows. □

Fix some $\mathbf{v} = (\bar{\mathbf{s}}, \bar{\mathbf{e}})$ and some α such that $\mathbf{v}$ has the α-correlation property. Let $\mathbf{w} = (\mathbf{e}', \mathbf{s}') \leftarrow \psi_k^{\times 2n}$ and $\mathbf{e}'' \leftarrow (\psi_k * \rho)^{\times n}$. Taking a union bound over the m assignments of j and the n/m assignments of i, we find that Equation 9 is violated with probability no more than

$$n \cdot \Pr\left[2(1+\alpha)\,|\langle \mathbf{v}, \mathbf{w} \rangle| + \sum_{j=0}^{3} \left|\left\langle \mathbf{y}^j, \mathbf{e}'' \right\rangle\right| > q\right]. \tag{11}$$

5.1 Ensuring $|\mu_{2,1}|$ is small

We will now describe a procedure that produces a $(\bar{\mathbf{s}}', \bar{\mathbf{e}}')$ that is the same length as $(\bar{\mathbf{s}}, \bar{\mathbf{e}})$ but has a potentially smaller value of $|\mu_{2,1}|$. Note that $\langle \bar{\mathbf{s}}, \mathbf{y}\bar{\mathbf{s}} \rangle = \langle \mathbf{s}, \mathbf{y}\mathbf{s} \rangle$ by Fact 1, so we can work with $(\mathbf{s}, \mathbf{e})$ rather than on $(\bar{\mathbf{s}}, \bar{\mathbf{e}})$. Let $\tau(\mathbf{s}) = \langle \mathbf{s}, \mathbf{y}\mathbf{s} \rangle$ and let $\sigma_i \mathbf{s} = \mathbf{s} - 2 s_i \mathbf{x}^i$ be the vector obtained by flipping the sign of the i-th coordinate of $\mathbf{s}$. We have

$$\tau(\sigma_i \mathbf{s}) = \begin{cases} \tau(\mathbf{s}) - 2 s_i (s_{i+n/4} - s_{i+3n/4}) & \text{if } i \in [0, \frac{n}{4}), \\ \tau(\mathbf{s}) - 2 s_i (s_{i-n/4} + s_{i+n/4}) & \text{if } i \in [\frac{n}{4}, \frac{3n}{4}), \\ \tau(\mathbf{s}) - 2 s_i (s_{i-n/4} - s_{i-3n/4}) & \text{if } i \in [\frac{3n}{4}, n). \end{cases} \tag{12}$$

Observe that if $\mathbf{s}^*$ is obtained from $\mathbf{s}$ by flipping the signs of coefficients in alternating runs of $n/4$ coefficients, i.e. by applying σ_i with $i \in [0, n/4) \cup [n/2, 3n/4]$, then $\tau(\mathbf{s}^*) = -\tau(\mathbf{s}^*)$. For $\mathbf{s}, \mathbf{e} \leftarrow \psi_k^{\times n}$, a sign flip in either $\mathbf{s}$ or $\mathbf{e}$ changes the value of $|\tau(\mathbf{s}) + \tau(\mathbf{e})|$ by at most $4k^2$. It follows that some sign flip in the Reduce algorithm results in an $(\mathbf{s}', \mathbf{e}')$ with $|\tau(\mathbf{s}') + \tau(\mathbf{e}')| \leq 2k^2$.

Reduce$(\mathbf{s}, \mathbf{e})$:

1. for $i = 0, 1, \ldots, n-1$
2. if $|\tau(\sigma_i \mathbf{s}) + \tau(\mathbf{e})| < |\tau(\mathbf{s}) + \tau(\mathbf{e})|$
3. $\mathbf{s} \leftarrow \sigma_i \mathbf{s}$.
4. if $|\tau(\mathbf{s}) + \tau(\sigma_i \mathbf{e})| < |\tau(\mathbf{s}) + \tau(\mathbf{e})|$
5. $\mathbf{e} \leftarrow \sigma_i \mathbf{e}$.
6. return $\mathbf{v}$

Lemma 2. *Let* $\mathbf{s}, \mathbf{e} \leftarrow \psi_k^{\times n}$ *and let* $\mathbf{s}' = \mathsf{Reduce}(\mathbf{s})$ *and* $\mathbf{e}' = \mathsf{Reduce}(\mathbf{e})$. *Then, with overwhelming probability,* $(\mathbf{s}', \mathbf{e}')$ *has the* α*-correlation property with* $\alpha = 6k/n$.

Proof (sketch). Note that $|\mu_{2,1}| = c_1/c_2$ where $c_1 = |\tau(\mathbf{s}') + \tau(\mathbf{e}')| \leq 2k^2$ and $c_2 = |\langle \mathbf{s}', \mathbf{s}' \rangle + \langle \mathbf{e}', \mathbf{e}' \rangle|$. By approximating ψ_k by a Gaussian and applying a standard tail bound on the chi-squared distribution, we find that c_2 is at least $2kn/3$ with probability at least $1 - 0.94^n$. Hence $|\mu_{2,1}| < 3k/n$ with high probability, and the claim follows by Lemma 1. □

Remark 1. We suspect that a much smaller value of α, even $\alpha = 0$, can be used in practice. In experiments with $n = 1024$, we have found that Reduce generally produces pairs $(\mathbf{s}, \mathbf{e})$ with $|\tau(\mathbf{s}) + \tau(\mathbf{e})| \leq 1$. One could enforce $\alpha = 0$ through rejection sampling. With $\alpha = 2/n$ we find a failure rate of $\leq 2^{-437.9}$, and with $\alpha = 0$ we find a failure rate of $\leq 2^{-439.5}$.

Remark 2. The conditional sign flips in Reduce can be implemented in constant time using standard techniques. The conditionals should be tested using Equation 12.

6 Software

Our software (file embedded in pdf) is based on the decryption failure script from the Kyber submission[2]. It computes distributions χ_1, χ_2, and χ_3 numerically, where: χ_1 is the distribution of $\sum_{i=1}^{2n} a_i \cdot b_i$ for $a_i, b_i \leftarrow \psi_k$; χ_2 is the distribution of $\sum_{i=1}^{m} c_i + d_i$ for $c_i \leftarrow \psi_k$ and $d_i \leftarrow \rho_{q,r}$; and χ_3 is the distribution of $(1 + \alpha)\sqrt{m}\,|e| + |f|$ for $e \leftarrow \chi_1$ and $f \leftarrow \chi_2$. Note that Equations 10 and 11 are of the

[2] https://github.com/pq-crystals/security-estimates

form $n \cdot \Pr[g > mq/4]$ for $g \leftarrow \chi_3$. Our software calculates the failure rate of a static key by fixing the a_i in the definition of χ_1. Note that the distribution of $\sum_{i=1}^{2n} a_i \cdot b_i$ is identical to the distribution of $\sum_{i=1}^{2n} \pm a_i \cdot b_i$ for any sequence of signs, in particular for signs applied by Reduce.

Verification We have not proven that our software is correct, but the results are plausible. Note that compression artifact noise is no more than $q/2r$ in magnitude, so the value on the right hand side of Equation 9 is no less than $x = mq\left(\frac{1}{4} - \frac{1}{2r}\right)$. The centered binomial distribution of parameter k has variance $k/2$, so we may approximate the term $\langle \mathbf{v}, \mathbf{w} \rangle$ in Equations 10 and 11 by a sum of $2n$ Gaussian variables of variance $k^2/4$. We may then approximate the probability of failure by $n \cdot \operatorname{erfc}(x/\sigma\sqrt{2})$ where $\sigma = (1+\alpha)\sqrt{2nmk^2/4}$. For $m = 2$ we take $\alpha = 0$ and for $m = 4$ we take $\alpha = 6k/n$. For the $q = 7681$ variants of NewHope512 and NewHope1024 this gives $2^{-178.0}$ and $2^{-160.9}$, respectively. Our exact calculations give $2^{-173.9}$ and $2^{-173.3}$.

n	m	k	r	q	pk	ct	sec	one-shot	$\alpha = 6k/n$	$\alpha = 0$
512	4	1	4	769	672	768	2^{124}	$2^{-118.2}$	$2^{-119.0}$	$2^{-121.7}$
512	2	4	8	3329	800	960	2^{123}	$2^{-135.0}$	—	$2^{-135.0}$
512	2	8	8	7681	864	1024	2^{120}	$2^{-173.9}$	—	$2^{-173.9}$
512	2	4	4	7681	864	960	2^{109}	$2^{-299.2}$	—	$2^{-298.9}$
512	2	8	8	12289	928	1088	2^{112}	$2^{-399.0}$	—	$2^{-398.8}$
1024	4	4	8	3329	1568	1920	2^{280}	$2^{-142.0}$	$2^{-139.5}$	$2^{-145.7}$
1024	4	8	8	7681	1696	2048	2^{275}	$2^{-183.1}$	$2^{-173.3}$	$2^{-188.5}$
1024	4	4	4	7681	1696	1920	2^{251}	$2^{-314.3}$	$2^{-313.8}$	$2^{-327.1}$
1024	4	8	8	12289	1824	2176	2^{259}	$2^{-418.0}$	$2^{-405.2}$	$2^{-439.5}$

Table 1: 'pk' is the size of the public key in bytes. 'ct' is the size of the ciphertext in bytes. 'sec' is the Core-SVP security relative to the $2^{0.292b}$ metric and was computed using the PQsecurity.py script provided with the NewHope submission. The three rightmost columns were computed using our script. 'one-shot' is the decryption failure probability as calculated in [6]. The two 'α' columns give the decryption failure probability as calculated above.

References

1. Alkim, E., Ducas, L., Pöppelmann, T., Schwabe, P.: NewHope without reconciliation. Cryptology ePrint Archive, Report 2016/1157 (2016), http://eprint.iacr.org/2016/1157
2. Lindner, R., Peikert, C.: Better key sizes (and attacks) for LWE-based encryption. In: Kiayias, A. (ed.) CT-RSA 2011. LNCS, vol. 6558, pp. 319–339. Springer, Heidelberg (Feb 2011)

3. Plantard, T., Sipasseuth, A., Susilo, W., Zucca, V.: Tight bound on newhope failure probability. Cryptology ePrint Archive, Report 2019/1451 (2019), https://eprint.iacr.org/2019/1451
4. Poppelmann, T., Alkim, E., Avanzi, R., Bos, J., Ducas, L., de la Piedra, A., Schwabe, P., Stebila, D., Albrecht, M.R., Orsini, E., Osheter, V., Paterson, K.G., Peer, G., Smart, N.P.: NewHope. Tech. rep., National Institute of Standards and Technology (2019), available at https://csrc.nist.gov/projects/post-quantum-cryptography/round-2-submissions
5. Pöppelmann, T., Güneysu, T.: Towards practical lattice-based public-key encryption on reconfigurable hardware. In: Lange, T., Lauter, K., Lisonek, P. (eds.) SAC 2013. LNCS, vol. 8282, pp. 68–85. Springer, Heidelberg (Aug 2014)
6. Song, M., Lee, S., Lee, E., Shin, D.J., Kim, Y.S., No, J.S.: Analysis of error dependencies on newhope (2019)