Estimate all the {LWE, NTRU} schemes!

Version: February 3, 2018

Martin R. Albrecht[1], Benjamin R. Curtis[1✉], Amit Deo[1], Alex Davidson[1], Rachel Player[1,2], Eamonn Postlethwaite[1], Fernando Virdia[1✉], Thomas Wunderer[3✉] ⋆

[1] Information Security Group, Royal Holloway, University of London, UK
[2] Sorbonne Université, CNRS, INRIA,
Laboratoire d'Informatique de Paris 6, LIP6, Équipe PolSys, France
[3] Technische Universität Darmstadt, Germany

benjamin.curtis.2015@rhul.ac.uk,
fernando.virdia.2016@rhul.ac.uk,
twunderer@cdc.informatik.tu-darmstadt.de

Abstract. We consider all LWE- and NTRU-based encryption, key encapsulation and digital signature schemes proposed for standardisation as part of the Post-Quantum Cryptography process run by the US National Institute of Standards and Technology (NIST). In particular, we investigate the impact that different estimates for the asymptotic runtime of (block-wise) lattice reduction have on the predicted security of these schemes. Relying on the "LWE estimator" by Albrecht et al., we estimate the cost of running primal and dual lattice attacks against every LWE-based scheme, using every cost model proposed as part of a submission. Furthermore, we estimate resistance of the proposed NTRU-like schemes against the primal attack resp. a simplified variant of the Hybrid attack under all cost models for lattice reduction.

⋆ The research of Albrecht was supported by EPSRC grant "Bit Security of Learning with Errors for Post-Quantum Cryptography and Fully Homomorphic Encryption" (EP/P009417/1) and by the European Union PROMETHEUS project (Horizon 2020 Research and Innovation Program, grant 780701). The research of Curtis, Deo and Davidson was supported by the EPSRC and the UK government as part of the Centre for Doctoral Training in Cyber Security at Royal Holloway, University of London (EP/K035584/1). The research of Player was partially supported by the French Programme d'Investissement d'Avenir under national project RISQ P141580. The research of Postlethwaite and Virdia was supported by the EPSRC and the UK government as part of the Centre for Doctoral Training in Cyber Security at Royal Holloway, University of London (EP/P009301/1). The research of Wunderer was supported by the DFG as part of project P1 within the CRC 1119 CROSSING.

In 2015, the US National Institute of Standards and Technology (NIST) began a process aimed at standardising post-quantum Public-key Encryption schemes (PKE), Key Encapsulation Mechanisms (KEM), and digital signature algorithms (SIG), resulting in a call for proposals in 2016 [Nat16]. The aim of this standardisation process is to meet the cryptographic requirements for communication (e.g. via the Internet) in an era where quantum computers exist. Participants were invited to submit their designs, along with different parameter sets that individually specify one or more target security categories (out of a pool of 5). These security categories roughly indicate how classical and quantum attacks on the proposed schemes compare to attacks on AES and SHA-3 in the post-quantum context. As part of their submissions, participants were asked to provide cryptanalysis supporting their security claims that roughly translate to estimating the size of the security parameter for each of their parameter sets.

Out of the 69 "complete and proper" submissions received by NIST, 23 are based on either the LWE or the NTRU family of lattice problems. Whilst techniques for solving these problems are well known, there exist different schools of thought regarding the asymptotic cost of these techniques. More specifically, the differences in cost for the BKZ algorithm for lattice reduction. This algorithm, which combines SVP calls in projected sub-lattices or "blocks", is a vital building block in attacks on these schemes. This can result in the same scheme being attributed multiple different security levels, and hence security categories, depending on the *cost model* being used. By "cost model" we mean the combination of the cost of solving SVP in dimension β and the number of required SVP oracle calls (cf. Section 3). A major source of divergence in estimated security is whether sieving [LMvdP15,BDGL16] or enumeration [MW15] is used to instantiate the SVP oracle in BKZ; we refer to the former as the "sieving regime" and the latter as the "enumeration regime". A second source of divergence is how polynomial factors are treated.

Thus, to provide a clearer view of the effect of the chosen cost model and the security assurances given by each submission, we extract the proposed parameter sets for each LWE-based and NTRU-like submission (Section 2). In particular, we consider each LWE-based scheme as a plain LWE instance, i.e. we mention algebraic (ring, module) structure but do not consider it further in our analysis, as is standard. We also extract the cost models used to analyse them (Section 3). Using this information, we then cross-estimate the security of each parameter set under every cost model from every submission (Section 4).

In this work, we restrict our attention to a subset of attacks on both families of problems. For LWE, we restrict our attention to the uSVP variant of the primal lattice attack as given in [BG14,ADPS16,AGVW17] and the dual lattice attack as given in [MR09,Alb17]. We disregard combinatorial [AFFP14,GJS15,KF15,GJMS17] and algebraic attacks [AG11,ACFP14], since those algorithms are not competitive

for the parameter sets considered here in the sieving regime.[4] Furthermore, we only consider the different cost models proposed in each submission and leave the consideration of variants of the dual and primal attack proposed in several submissions for future work. For the primal attack this, in particular, means that we do not consider the primal attack via a combination of lattice reduction and BDD enumeration often referred to as "lattice decoding" attack. While the primal uSVP attack can be considered as a simplified variant of the decoding attack in the enumeration regime, it typically outperforms the latter in the sieving regime. We intend to extend our analysis to the decoding attack in future work. For NTRU, besides the primal attack we consider only a simplified variant of the Hybrid attack [HG07,Wun16] where we do not consider the meet-in-the-middle variant or "guessing + nearest plane" after lattice reduction. Again, we intend to extend our analysis to cover the full Hybrid attack in future work. We note that the simplified Hybrid attack considered here also captures standard lattice attacks on NTRU without any guessing.

Related Work. NIST categorised each scheme according to the family of underlying problem (lattice-based, code-based, SIDH-based, MQ-based, hash-based, other) in [Moo17]. This analysis was refined in [Fuj17]. NIST then also provided a first performance comparison of all complete and proper schemes in [Nat17]. Bernstein provided a comparison of all schemes based on the sizes of their ciphertexts and keys in [Ber17].

1 Preliminaries

We write vectors in lowercase bold letters $\boldsymbol{v}$ and matrices in capital bold letters $\boldsymbol{A}$, and refer to their entries with a subscript index v_i, $A_{i,j}$. We identify polynomials f of degree $n-1$ with their corresponding coefficient vector $\boldsymbol{f}$. We write $\|f\|$ to mean the Euclidean norm of $\boldsymbol{f}$. Inner products are written using angular brackets $\langle \boldsymbol{v}, \boldsymbol{w} \rangle$. The transpose of $\boldsymbol{v}$ is indicated as $\boldsymbol{v}^t$. Generic probability distributions are labelled χ. We use the notation $a \leftarrow \chi$ to indicate that a is an element sampled from χ. We refer to the expectation of a as $\mathbb{E}_\chi[a]$, and its variance as $\mathbb{V}_\chi[a]$ and we may omit the subscript $_\chi$ if the distribution is clear from the context.

We write U_S to mean the discrete uniform distribution over $S \cap \mathbb{Z}$. If $S = [a, b]$, we refer to $U_{[a,b]}$ as a *bounded uniform* distribution. We write the distribution of $\boldsymbol{s}$ such that $\boldsymbol{s}_i \leftarrow U_{[a,b]}$ as (a, b), and the distribution of $\boldsymbol{s}$ such that exactly h entries have been sampled from $U_{[a,b]-\{0\}}$, and the remaining entries have been set to 0, as $((a, b), h)$.

[4] BKW-style algorithms do outperform BKZ in the enumeration regime for some medium-sized parameter sets, but, similarly to BKZ in the sieving regime, require $2^{\Theta(n)}$ memory.

An n-dimensional *lattice* is a discrete additive subgroup of $\mathbb{R}^n$. Every n-dimensional lattice L can be represented by a *basis*, i.e., a set of linearly independent vectors $\boldsymbol{B} = \{\boldsymbol{b}_1, \ldots, \boldsymbol{b}_m\}$ such that $L = \mathbb{Z}\boldsymbol{b}_1 + \cdots + \mathbb{Z}\boldsymbol{b}_m$. If $n = m$, the lattice is called a *full-rank* lattice. Let L be a lattice and $\boldsymbol{B}$ be a basis of L, in which case we write $L = L(\boldsymbol{B})$. Then the *volume* (also called *covolume* or *determinant*) of L is defined as $\mathrm{Vol}(L) = \sqrt{\det(\boldsymbol{B}^t\boldsymbol{B})}$. In a random lattice, the *Gaussian heuristic* estimates the length of the shortest non-zero vector of an n-dimensional lattice L to be

$$\frac{\Gamma(1+n/2)^{1/n}}{\sqrt{\pi}}\mathrm{Vol}(L)^{1/n} \approx \sqrt{\frac{d}{2\pi e}}\mathrm{Vol}(\Lambda)^{1/d}.$$

The quality of a lattice basis $\boldsymbol{B} = \{\boldsymbol{b}_1, \ldots, \boldsymbol{b}_m\}$ of a full-rank lattice L can be measured by its *root Hermite factor* δ defined via $\|\boldsymbol{b}_1\| = \delta^m \mathrm{Vol}(L)^{1/m}$. If the basis $\boldsymbol{B}$ is BKZ reduced with block size β we can assume [Che13] the following relation between the block size and the root Hermite factor

$$\delta = (((\pi\beta)^{1/\beta}\beta)/(2\pi e))^{1/(2(\beta-1))}.$$

In this work, we are concerned with schemes whose security is based on either the LWE or the NTRU assumption.

1.1 LWE

Definition 1 (LWE [Reg05]). *Let n, q be positive integers, χ be a probability distribution on $\mathbb{Z}$ and $\boldsymbol{s}$ be a secret vector in $\mathbb{Z}_q^n$. We denote the LWE Distribution $L_{\boldsymbol{s},\chi,q}$ as the distribution on $\mathbb{Z}_q^n \times \mathbb{Z}_q$ given by choosing $\boldsymbol{a} \in \mathbb{Z}_q^n$ uniformly at random, choosing $e \in \mathbb{Z}$ according to χ and considering it as an element of $\mathbb{Z}_q$, and outputting $(\boldsymbol{a}, \langle \boldsymbol{a}, \boldsymbol{s}\rangle + e) \in \mathbb{Z}_q^n \times \mathbb{Z}_q$.*

Decision-LWE *is the problem of distinguishing whether samples $\{(\boldsymbol{a}_i, b_i)\}_{i=1}^m$ are drawn from the LWE distribution $L_{\boldsymbol{s},\chi,q}$ or uniformly from $\mathbb{Z}_q^n \times \mathbb{Z}_q$.*
Search-LWE *is the problem of recovering the vector $\boldsymbol{s}$ from a collection $\{(\boldsymbol{a}_i, b_i)\}_{i=1}^m$ of samples drawn according to $L_{\boldsymbol{s},\chi,q}$.*

As originally defined in [Reg05], χ is a rounded Gaussian distribution, but now LWE is typically defined with a discrete Gaussian distribution [LP11]. It was later shown that the secret can also be drawn from the error distribution without any loss in security [ACPS09]. This variant is known as the "normal form". Many submissions consider alternative distributions for sampling errors and secrets such as small uniform, sparse or binomial distributions.

The *primal-uSVP attack* solves the Search-LWE problem by constructing an integer *embedding lattice* (using either Kannan's [Kan87] or Bai and Galbraith's [BG14] embedding), and solving the *unique Shortest Vector Problem* (uSVP). The *dual*

attack solves Decision-LWE by reducing it to the Short Integer Solution Problem (SIS) [Ajt96], which in turn is reduced to finding short vectors in the lattice $\{\boldsymbol{x} \in \mathbb{Z}_q^m \mid \boldsymbol{x}\boldsymbol{A} \equiv 0 \mod q\}$. For either attack, variants are know which exploit the presence of unusually short or sparse secret distributions and we consider these variants in this work where applicable.

Related problems. Expanding on the idea of LWE, related problems with a similar structure have been proposed. In particular, in the Ring-LWE [SSTX09,LPR10] problem polynomials s, a_i and e_i (wlog s and e_i are "short") are drawn from a ring of the form $\mathcal{R}_q = \mathbb{Z}_q/(\phi)$ for some polynomial ϕ of degree n. Then, given a list of Ring-LWE samples $\{(a_i, a_i \cdot s + e_i)\}_{i=1}^m$, the Search-RLWE problem is to recover s and the Decision-RLWE problem is to distinguish the list of samples from a list uniformly sampled from $\mathcal{R}_q \times \mathcal{R}_q$. More generally, in the Module-LWE [LS15] problem vectors $\boldsymbol{a}_i$, $\boldsymbol{s}$ and polynomials e_i are drawn from $\mathcal{R}_q^k$ and $\mathcal{R}_q$ respectively. Search-MLWE asks to recover $\boldsymbol{s}$ from a set $\{(\boldsymbol{a}_i, \langle \boldsymbol{a}_i, \boldsymbol{s}\rangle + e_i)\}_{i=1}^m$, Decision-MLWE asks distinguish such a set from a set uniformly sampled from $\mathcal{R}_q^k \times \mathcal{R}_q$.

In both cases above, by interpreting the elements of $\mathcal{R}_q$ as vectors in $\mathbb{Z}_q$, one can interpret RLWE and MLWE instances as being LWE ones by ignoring the extra algebraic structure of $\mathcal{R}_q$. Since no strategies making use of this structure are known that solve the RLWE and MLWE problem better than the above primal and dual attack, this identification with LWE is what is usually done to cost the complexity of solving RLWE and MLWE.

There is also a class of LWE-like problems that replace the noise term by a deterministic rounding process. For example, an instance of the learning with rounding (LWR) problem is of the form $\left(\boldsymbol{a}, b := \lfloor \frac{p}{q} \langle \boldsymbol{a}, \boldsymbol{s}\rangle \rceil\right) \in \mathbb{Z}_q^n \times \mathbb{Z}_p$. We interpret this as a LWE instance by multiplying the second component by q/p and assuming that $q/p \cdot b = \langle \boldsymbol{a}, \boldsymbol{s}\rangle + e$ where e is uniform over the interval $(-q/2p, q/2p]$ [BPR12]. The resulting variance of this error term can then be calculated as $q^2/(12p^2)$. The same ideas apply to the other variants of LWE — RLWE/RLWR, MLWE/MLWR — that use deterministic rounding as opposed to the addition of an error term.

Number of samples. LWE as defined in Definition 1 provides the adversary with an arbitrary number of samples. However, this does not hold true for any of the schemes considered in this work. In particular, in the RLWE KEM setting — which is the most common for the schemes considered here — the public key is one RLWE sample $(a, b) = (a, a \cdot s + e)$ for some short s, e and encapsulations consist of two RLWE samples $v \cdot a + e'$ and $v \cdot b + e'' + \tilde{m}$ where $\tilde{m}$ is some encoding of a random string and v, e', e'' are short. Thus, depending on the target, the adversary is given either n resp. $2n$ (normal form or short secret) plain LWE

samples. In a typical setting, though, the adversary does not get to enjoy the full power of having two samples at its disposal, because, firstly, the random string $\tilde{m}$ increases the noise in $v \cdot b + e'' + \tilde{m}$ by a factor of 2 and, secondly, because many schemes drop lower order bits from $v \cdot b + e'' + \tilde{m}$ to save bandwidth. Due to the way decryption works, this bit dropping can be quite aggressive. Thus, the noise in the second sample can be quite large. Hence, conservatively we may assume the adversary has access to $2n$ plain (normal form resp. short secret) LWE samples. Alternatively, we may assume the adversary has access to only n plain (normal form resp. short secret) LWE samples. In this work, we consider these two scenarios for all schemes and leave distinguishing which scenario applies to which scheme for future work.

1.2 NTRU

Definition 2 (NTRU [HPS96]). *Let n, q be positive integers, $\phi \in \mathbb{Z}[x]$ be a monic polynomial of degree n, and $\mathcal{R}_q = \mathbb{Z}_q[x]/(\phi)$. Let $f \in \mathcal{R}_q^\times, g \in \mathcal{R}_q$ be small polynomials (i.e., having small coefficients) and $h = g \cdot f^{-1} \bmod q$.*

Search-NTRU *is the problem of recovering f or g given h.*

Remark 1. One can exchange the roles of f and g (in the case that g is invertible) by replacing h with $h^{-1} = f \cdot g^{-1} \bmod q$, if this leads to a better attack.

The most common ways to choose the polynomials f (or g) are the following. The first is to choose f to have small coefficients (e.g., ternary). The second is to choose F to have small coefficients (e.g., ternary) and to set $f = pF$ for some (small) prime p. The third is to choose F to have small coefficients (e.g., ternary) and to set $f = pF + 1$ for some (small) prime p.

The NTRU problem can be reduced to solving uSVP in the NTRU lattice $L(\boldsymbol{B})$ generated by the columns of

$$\boldsymbol{B} = \begin{pmatrix} q\boldsymbol{I}_n & \boldsymbol{H} \\ \boldsymbol{0} & \boldsymbol{I}_n \end{pmatrix},$$

where $\boldsymbol{H}$ is the "rotation matrix" of h, see for example [CS97,HPS98]. Indeed, $L(\boldsymbol{B})$ contains the short vector $(\boldsymbol{f} \,|\, \boldsymbol{g})^t$, since $hf = g \bmod q$ and hence $(\boldsymbol{f} \,|\, \boldsymbol{g})^t = \boldsymbol{B}(\boldsymbol{w} \,|\, \boldsymbol{g})^t$ for some $\boldsymbol{w} \in \mathbb{Z}^n$. Furthermore, it can be assumed that the vector $(\boldsymbol{f} \,|\, \boldsymbol{g})^t$ (or a rotation of) is the unique shortest vector in $L(\boldsymbol{B})$. In addition, if $f = pF$ or $f = pF + 1$ for some small polynomial F one can construct a similar uSVP lattice that contains $(\boldsymbol{F}, \boldsymbol{g})^t$, see for example [Sch15,Wun16]. Similar to LWE, in order to improve this attack, rescaling and dimension reducing techniques can be applied [MS01]. Note that the dimension of the lattice must be between

n and $2n$ by construction. The dimension reducing technique can be seen as a simple version of hybrid attacks [HG07,GvVW17b,Wun16] on NTRU, where only zeros are guessed. In this work, only this simple version is considered since it can be readily costed using the [APS15] estimator.

1.3 Lattice reduction

The techniques outlined above to solve the LWE and NTRU problems rely on lattice reduction, the procedure of generating a "sufficiently orthogonal" basis given the description of a lattice. The lattice reduction algorithm attaining the best theoretical results is Slide reduction [GN08]. In this work, however, we consider the experimentally best performing algorithm, BKZ [SE94,CN11,DT17]. Given a basis for one of the lattices described above, we need to choose the *block size* necessary to run BKZ and successfully recover the shortest vector. This is done following the analysis introduced in [ADPS16, Section 6.3] for the LWE and NTRU primal attacks, and the analysis done in [MR09,Alb17] for the LWE dual attack.

BKZ in turn makes use of an oracle solving the Shortest Vector Problem (or SVP oracle) in a smaller lattice. Several SVP algorithms can be used to instantiate this oracle, the two most efficient are sieving [BDGL16] or enumeration [MW15]. Since we are considering security in the post-quantum setting, we also have to consider quantum algorithms, which as of writing mainly means to consider potential Grover [Gro96] speed-ups for these algorithms [LMvdP15,ADPS16]. We note that the reported speed-ups of these algorithms are assuming perfect quantum computers that can run arbitrarily long computations and disregard the inherent lack of parallelism in Grover-style search. A more refined understanding of the cost of quantum algorithms for solving SVP is a pressing topic for future research.

2 Proposed schemes

The three tables below specify the parameter sets for the schemes considered. In particular Table 1 gives the parameters for the NTRU-like schemes. Table 2 gives the parameters of the same schemes when converted into the LWE-based context, as detailed in Section 4. Finally, Table 3 gives the parameters for the LWE-based schemes in terms of plain LWE, that is, ignoring the potential ring or module structure.

Throughout, n is the dimension of the problem and q the modulus. The polynomial ϕ, if present, is the polynomial considered to form the ring from which LWE or NTRU elements are drawn. In particular, this ring is $\mathcal{R}_q = \mathbb{Z}_q[x]/(\phi)$, that is,

degree n polynomials with coefficients from the integers modulo q quotiented by the ideal generated by ϕ.

In Tables 2 and 3, the value σ is the standard deviation of the distribution χ from which the errors are drawn. This error distribution is not always Gaussian, and our approaches to such cases are explained in Section 4. Note that often in lattice based cryptography the notation $D_{\Lambda,s,\boldsymbol{c}}$ is used to denote a discrete Gaussian with support the lattice Λ, s a 'standard deviation parameter' and c a centre. In this work σ is the standard deviation, explicitly $\sigma = s/\sqrt{2\pi}$. If the secret distribution is 'normal', i.e., in the normal form, this means it is the same distribution as the error, namely χ. If not, the distribution given determines the secret distribution. Here the notation $((a, b), h)$ means sampled uniformly from the vectors with Hamming weight h and with each entry sampled independently and uniformly from $U_{[a,b]\setminus\{0\}}$. If h is absent, then there is no Hamming weight restriction and each sample is sampled from $U_{[a,b]}$.

Name	n	q	$\|f\|$	$\|g\|$	NIST	Assumption	ϕ	Primitive
NTRUEncrypt	443	2048	16.94	16.94	1	NTRU	$x^n - 1$	KEM, PKE
	743	2048	22.25	22.25	$1, 2, 3, 4, 5$	NTRU	$x^n - 1$	KEM, PKE
	1024	1073750017	23168.00	23168.00	$4, 5$	NTRU	$x^n - 1$	KEM, PKE
Falcon	512	12289	91.71	91.71	1	NTRU	$x^n + 1$	SIG
	768	18433	112.32	112.32	$2, 3$	NTRU	$x^n - x^{n/2} + 1$	SIG
	1024	12289	91.71	91.71	$4, 5$	NTRU	$x^n + 1$	SIG
NTRU HRSS	700	8192	20.92	20.92	1	NTRU	$\sum_{i=0}^{n-1} x^i$	KEM
NTRU Prime	761	4591	16.91	22.52	5	NTRU	$x^n - x - 1$	KEM
	761	4591	15.81	22.52	5	NTRU	$x^n - x - 1$	KEM
pqNTRUsign	1024	65537	22.38	22.38	$1, 2, 3, 4, 5$	NTRU	$x^n - 1$	SIG

Table 1: Parameter sets for NTRU-based schemes with secret dimension n, modulo q, small polynomials f and g, and ring $\mathbb{Z}_q[x]/(\phi)$. The NIST column indicates the NIST security category aimed at.

Name	n	q	σ	Secret dist.	NIST	Assumption	ϕ	Primitive
NTRUEncrypt	443	2048	0.80	$((-1, 1), 287)$	1	NTRU	$x^n - 1$	KEM, PKE
	743	2048	0.82	$((-1, 1), 495)$	1, 2, 3, 4, 5	NTRU	$x^n - 1$	KEM, PKE
	1024	1073750017	724.00	normal	4, 5	NTRU	$x^n - 1$	KEM, PKE
Falcon	512	12289	4.05	normal	1	NTRU	$x^n + 1$	SIG
	768	18433	4.05	normal	2, 3	NTRU	$x^n - x^{n/2} + 1$	SIG
	1024	12289	2.87	normal	4, 5	NTRU	$x^n + 1$	SIG
NTRU HRSS	700	8192	0.79	$((-1, 1), 437)$	1	NTRU	$\sum_{i=0}^{n-1} x^i$	KEM
NTRU Prime	761	4591	0.82	$((-1, 1), 286)$	5	NTRU	$x^n - x - 1$	KEM
	761	4591	0.82	$((-1, 1), 250)$	5	NTRU	$x^n - x - 1$	KEM

Name	n	q	σ	Secret dist.	NIST	Assumption	ϕ	Primitive
pqNTRUsign	1024	65537	0.70	$((-1,1),501)$	1, 2, 3, 4, 5	NTRU	x^n-1	SIG

Table 2: LWE parameter sets for NTRU-based schemes, with dimension n, modulo q, standard deviation of the error σ, and ring $\mathbb{Z}_q[x]/(\phi)$. The parameters are obtained following Section 4. The NIST column indicates the NIST security category aimed at.

Name	n	k	q	σ	Secret dist.	NIST	Assumption	ϕ	Primitive
AKCN-RLWE	1024	—	12289	2.83	normal	5	RLWE	x^n+1	KEM
AKCN-MLWE	768	3	7681	1.00	normal	4	MLWE	$x^{n/k}+1$	KEM
	768	3	7681	2.24	normal	4	MLWE	$x^{n/k}+1$	KEM
BabyBear	624	2	1024	1.00	normal	2	ILWE	$q^{n/k}-q^{n/(2k)}-1$	KEM
	624	2	1024	0.79	normal	2	ILWE	$q^{n/k}-q^{n/(2k)}-1$	KEM
MamaBear	936	3	1024	0.94	normal	5	ILWE	$q^{n/k}-q^{n/(2k)}-1$	KEM
	936	3	1024	0.71	normal	4	ILWE	$q^{n/k}-q^{n/(2k)}-1$	KEM
PapaBear	1248	4	1024	0.87	normal	5	ILWE	$q^{n/k}-q^{n/(2k)}-1$	KEM
	1248	4	1024	0.61	normal	5	ILWE	$q^{n/k}-q^{n/(2k)}-1$	KEM
CRYSTALS-Dilithium	768	3	8380417	3.74	$(-6,6)$	1	MLWE	$x^{n/k}+1$	SIG
	1024	4	8380417	3.16	$(-5,5)$	2	MLWE	$x^{n/k}+1$	SIG
	1280	5	8380417	2.00	$(-3,3)$	3	MLWE	$x^{n/k}+1$	SIG
CRYSTALS-Kyber	512	2	7681	1.58	normal	1	MLWE	$x^{n/k}+1$	KEM, PKE
	768	3	7681	1.41	normal	3	MLWE	$x^{n/k}+1$	KEM, PKE
	1024	4	7681	1.22	normal	5	MLWE	$x^{n/k}+1$	KEM, PKE
Ding Key Exchange	512	—	120883	4.19	normal	1	RLWE	x^n+1	KEM
	1024	—	120883	2.60	normal	3, 5	RLWE	x^n+1	KEM
EMBLEM	770	—	16777216	25.00	$(-1,1)$	1	LWE		KEM, PKE
	611	—	16777216	25.00	$(-2,2)$	1	LWE		KEM, PKE
R EMBLEM	512	—	65536	25.00	$(-1,1)$	1	RLWE	x^n+1 †	KEM, PKE
	512	—	16384	3.00	$(-1,1)$	1	RLWE	x^n+1 †	KEM, PKE
Frodo	640	—	32768	2.75	normal	1	LWE		KEM, PKE
	976	—	65536	2.30	normal	3	LWE		KEM, PKE
NewHope	512	—	12289	2.00	normal	1	RLWE	x^n+1	KEM, PKE
	1024	—	12289	2.00	normal	5	RLWE	x^n+1	KEM, PKE
HILA5	1024	—	12289	2.83	normal	5	RLWE	x^n+1	KE
KINDI	768	3	16384	2.35	$(-4,4)$	2	MLWE	$x^{n/k}+1$	KEM, PKE
	1024	2	8192	1.12	$(-2,2)$	4	MLWE	$x^{n/k}+1$	KEM, PKE
	1024	2	16384	2.29	$(-4,4)$	4	MLWE	$x^{n/k}+1$	KEM, PKE
	1280	5	16384	1.12	$(-2,2)$	5	MLWE	$x^{n/k}+1$	KEM, PKE
	1536	3	8192	1.12	$(-2,2)$	5	MLWE	$x^{n/k}+1$	KEM, PKE
LAC	512	—	251	0.71	normal	1, 2	PLWE	x^n+1	KE, KEM, PKE
	1024	—	251	0.50	normal	3, 4	PLWE	x^n+1	KE, KEM, PKE
	1024	—	251	0.71	normal	5	PLWE	x^n+1	KE, KEM, PKE

Name	n	k	q	σ	Secret dist.	NIST	Assumption	ϕ	Primitive
LIMA-2p	1024	—	133121	3.16	normal	3	RLWE	$x^n + 1$	KEM, PKE
	2048	—	184321	3.16	normal	4	RLWE	$x^n + 1$	KEM, PKE
LIMA-sp	1018	—	12521473	3.16	normal	1	RLWE	$\sum_{i=0}^{n} x^i$	KEM, PKE
	1306	—	48181249	3.16	normal	2	RLWE	$\sum_{i=0}^{n} x^i$	KEM, PKE
	1822	—	44802049	3.16	normal	3	RLWE	$\sum_{i=0}^{n} x^i$	KEM, PKE
	2062	—	16900097	3.16	normal	4	RLWE	$\sum_{i=0}^{n} x^i$	KEM, PKE
Lizard	536	—	2048	1.15	$((-1, 1), 140)$	1	LWE, LWR		KEM, PKE
	663	—	1024	1.15	$((-1, 1), 128)$	1	LWE, LWR		KEM, PKE
	816	—	2048	1.15	$((-1, 1), 200)$	3	LWE, LWR		KEM, PKE
	952	—	2048	1.15	$((-1, 1), 200)$	3	LWE, LWR		KEM, PKE
	1088	—	4096	1.15	$((-1, 1), 200)$	5	LWE, LWR		KEM, PKE
	1300	—	2048	1.15	$((-1, 1), 200)$	5	LWE, LWR		KEM, PKE
RLizard	1024	—	1024	1.15	$((-1, 1), 128)$	1	RLWE, RLWR	$x^n + 1$	KEM, PKE
	1024	—	2048	1.15	$((-1, 1), 264)$	3	RLWE, RLWR	$x^n + 1$	KEM, PKE
	2048	—	2048	1.15	$((-1, 1), 164)$	3	RLWE, RLWR	$x^n + 1$	KEM, PKE
	2048	—	4096	1.15	$((-1, 1), 256)$	5	RLWE, RLWR	$x^n + 1$	KEM, PKE
LOTUS	576	—	8192	3.00	normal	1, 2	LWE		KEM, PKE
	704	—	8192	3.00	normal	3, 4	LWE		KEM, PKE
	832	—	8192	3.00	normal	5	LWE		KEM, PKE
uRound2.KEM	500	—	16384	2.31	$((-1, 1), 74)$	1	LWR		KEM
	580	—	32768	4.62	$((-1, 1), 116)$	2	LWR		KEM
	630	—	32768	4.62	$((-1, 1), 126)$	3	LWR		KEM
	786	—	32768	4.62	$((-1, 1), 156)$	4	LWR		KEM
	786	—	32768	4.62	$((-1, 1), 156)$	5	LWR		KEM
uRound2.KEM	418	—	4096	4.62	$((-1, 1), 66)$	1	RLWR	$\sum_{i=0}^{n} x^i$	KEM
	522	—	32768	36.95	$((-1, 1), 78)$	2	RLWR	$\sum_{i=0}^{n} x^i$	KEM
	540	—	16384	18.48	$((-1, 1), 96)$	3	RLWR	$\sum_{i=0}^{n} x^i$	KEM
	700	—	32768	36.95	$((-1, 1), 112)$	4	RLWR	$\sum_{i=0}^{n} x^i$	KEM
	676	—	32768	36.95	$((-1, 1), 120)$	5	RLWR	$\sum_{i=0}^{n} x^i$	KEM
uRound2.PKE	500	—	32768	4.62	$((-1, 1), 74)$	1	LWR		PKE
	585	—	32768	4.62	$((-1, 1), 110)$	2	LWR		PKE
	643	—	32768	4.62	$((-1, 1), 114)$	3	LWR		PKE
	835	—	32768	2.31	$((-1, 1), 166)$	4	LWR		PKE
	835	—	32768	2.31	$((-1, 1), 166)$	5	LWR		PKE
uRound2.PKE	420	—	1024	1.15	$((-1, 1), 62)$	1	RLWR	$\sum_{i=0}^{n} x^i$	PKE
	540	—	8192	4.62	$((-1, 1), 96)$	2	RLWR	$\sum_{i=0}^{n} x^i$	PKE
	586	—	8192	4.62	$((-1, 1), 104)$	3	RLWR	$\sum_{i=0}^{n} x^i$	PKE
	708	—	32768	18.48	$((-1, 1), 140)$	4, 5	RLWR	$\sum_{i=0}^{n} x^i$	PKE
nRound2.KEM	400	—	3209	3.62	$((-1, 1), 72)$	1	RLWR	$\sum_{i=0}^{n} x^i$	KEM
	486	—	1949	2.20	$((-1, 1), 96)$	2	RLWR	$\sum_{i=0}^{n} x^i$	KEM
	556	—	3343	3.77	$((-1, 1), 88)$	3	RLWR	$\sum_{i=0}^{n} x^i$	KEM
	658	—	1319	1.49	$((-1, 1), 130)$	4, 5	RLWR	$\sum_{i=0}^{n} x^i$	KEM
nRound2.PKE	442	—	2659	1.50	$((-1, 1), 74)$	1	RLWR	$\sum_{i=0}^{n} x^i$	PKE
	556	—	3343	1.88	$((-1, 1), 88)$	2	RLWR	$\sum_{i=0}^{n} x^i$	PKE
	576	—	2309	1.30	$((-1, 1), 108)$	3	RLWR	$\sum_{i=0}^{n} x^i$	PKE
	708	—	2837	1.60	$((-1, 1), 140)$	4, 5	RLWR	$\sum_{i=0}^{n} x^i$	PKE
LightSaber	512	2	8192	2.31	normal	1	MLWR	$x^{n/k} + 1$	KEM, PKE
Saber	768	3	8192	2.31	normal	3	MLWR	$x^{n/k} + 1$	KEM, PKE
FireSaber	1024	4	8192	2.31	normal	5	MLWR	$x^{n/k} + 1$	KEM, PKE

Name	n	k	q	σ	Secret dist.	NIST	Assumption	ϕ	Primitive
qTESLA	1024	—	8058881	8.49	normal	1	RLWE	$x^n + 1$	SIG
	2048	—	12681217	8.49	normal	3	RLWE	$x^n + 1$	SIG
	2048	—	27627521	8.49	normal	5	RLWE	$x^n + 1$	SIG
Titanium.PKE	1024	—	86017	1.41	normal	1	PLWE	$x^n + \sum_{i=1}^{n-1} f_i x^i + f_0$ *	PKE
	1280	—	301057	1.41	normal	1	PLWE	$x^n + \sum_{i=1}^{n-1} f_i x^i + f_0$ *	PKE
	1536	—	737281	1.41	normal	3	PLWE	$x^n + \sum_{i=1}^{n-1} f_i x^i + f_0$ *	PKE
	2048	—	1198081	1.41	normal	5	PLWE	$x^n + \sum_{i=1}^{n-1} f_i x^i + f_0$ *	PKE
Titanium.KEM	1024	—	118273	1.41	normal	1	PLWE	$x^n + \sum_{i=1}^{n-1} f_i x^i + f_0$ *	KEM
	1280	—	430081	1.41	normal	1	PLWE	$x^n + \sum_{i=1}^{n-1} f_i x^i + f_0$ *	KEM
	1536	—	783361	1.41	normal	3	PLWE	$x^n + \sum_{i=1}^{n-1} f_i x^i + f_0$ *	KEM
	2048	—	1198081	1.41	normal	5	PLWE	$x^n + \sum_{i=1}^{n-1} f_i x^i + f_0$ *	KEM

Table 3: Parameter sets for LWE-based schemes with secret dimension n, MLWE rank k (if any), modulo q, standard deviation of the error σ. If the LWE samples come from a Ring- or Modulo-LWE instance, the ring is $\mathbb{Z}_q[x]/(\phi)$. The NIST column indicates the NIST security category aimed at. *For Titanium no ring is explicitly chosen but the scheme simultaneously relies on a family of rings where $f_i \in \{-1, 0, 1\}$, $f_0 \in \{-1, 1\}$. †For R EMBLEM we list the parameters from the reference implementation since a suitable ϕ could not be found for those proposed in [SPL+17, Table 2].

3 Costing lattice reduction

A variety of approaches are available in the literature to cost the running time of BKZ, e.g. [CN11,APS15,ADPS16]. The main differences between models is whether they are in the sieving or enumeration regime, and how many calls to the oracle are expected to recover a vector of length $\approx \delta^d \operatorname{Vol}(\Lambda)^{1/d}$. A summary of every cost model considered as part of a submission can be found in Table 4.

The most commonly considered SVP oracle is sieving. In the literature, its cost on a random lattice of dimension β is estimated as $2^{c\beta+o(\beta)}$, where $c = 0.292$ classically [BDGL16], with Grover speedups lowering it to $c = 0.265$ [Laa15a]. A "paranoid" lower bound is given in [ADPS16] as $2^{0.2075\beta+o(\beta)}$ based on the Kissing number. Some authors replace $o(\beta)$ by a constant based on experiments in [Laa15b], some authors omit it. Alternatively, enumeration is considered in some submissions. In particular, it can be found estimated as $2^{c_1\beta\log\beta+c_2\beta+c_3}$ [Kan83,MW15] or as $2^{c_1\beta^2+c_2\beta+c_3}$ [FP85,CN11], with Grover speedups considered to half the exponent.

With respect to the number of SVP oracle calls required by BKZ, a popular choice was that of following the "Core-SVP" model introduced in [ADPS16], that considers a single call. Alternatively, the number of calls has also been estimated

to be β (for example, in [BCD+16]) or $8d$ (for example, in [Alb17]), where d is the dimension of the embedding lattice and β is the BKZ block size.

To simplify the identification of every model, we denote models making a single call to the SVP oracle as "Core-", while those making N calls as "N-". We use "Sieve" to refer to the sieving oracle (adding "$+O(1)$" if a constant factor is included), and "Enum" for enumeration. Finally, if a model considers Grover speedups, we prepend "Q-". For example, using this notation, the CRYSTALS [LDK+17,SAB+17] submissions consider the Core-Sieve and Q-Core-Sieve cost models, while qTESLA [BAA+17] considers Q-$8d$-Sieve+$O(1)$.

LOTUS [PHAM17] is the only submission not to provide a closed formula for estimating the cost of BKZ. Given their preference for enumeration, we fitted their estimated cost model to a curve of shape $2^{c_1\beta\log\beta+c_2\beta+c_3}$, suggesting their model to be a form of Core-Enum.

The NTRU Prime [BCLvV17] utilizes the BKZ 2.0 simulator of [CN11] to determine the necessary block size and number of tour to achieve a certain root Hermite factor prior to applying their BKZ cost model. In contrast, here we apply the asymptotic formula from [Che13] to relate block size and root Hermite factor.

4 Estimates

For our experiments we make use of the LWE estimator[5] from [APS15], which allows for specifying arbitrary cost models for BKZ. We wrap it in a script that loops though the proposed schemes and cost models, estimating the cost of the appropriate variants of the primal and dual lattice attacks. For every scheme we estimate each attack twice, assuming either n and $2n$ available samples. In most cases, ciphertext in transit provides $2n$ LWE samples. Often, introducing stronger rounding on the second set of n samples, the total number of useful samples can be reduced to n. In the case of Module-LWE, ciphertext in transit produces a smaller number of LWE samples, but n samples can still be recovered from the public key. We note that for many schemes, n samples are sufficient to run the most efficient variant of either attack. Our code is available at `https://github.com/fvirdia/estimate-all-the-lwe-ntru-schemes`.

Our results are given in Tables 5, 6, 7, 8, 9, 10. A human friendly version of these tables is available at `https://estimate-all-the-lwe-ntru-schemes.github.io`. In particular, the HTML version supports filtering and sorting the table. It also contains SageMath sourcecode snippets to reproduce each entry.

[5] `https://bitbucket.org/malb/lwe-estimator`, commit `c5763b2`.

Model	Cost	Schemes
Core-Sieve Q-Core-Sieve	$2^{0.292\beta}$ $2^{0.265\beta}$	CRYSTALS [LDK+17,SAB+17] Falcon [PFH+17] HILA5 [Saa17] KINDI [Ban17] LAC [LLJ+17] New Hope [PAA+17] SABER [DKRV17] ThreeBears [Ham17] Titanium [SSZ17] NTRU HRSS [SHRS17] NTRUEncrypt [ZCHW17a] pqNTRUSign [ZCHW17b]
Core-Sieve+$O(1)$ Q-Core-Sieve+$O(1)$	$2^{0.292\beta+16.4}$ $2^{0.265\beta+16.4}$	LIMA [SAL+17]
Core-Sieve (min. space) Q-Core-Sieve (min. space)	$2^{0.368\beta}$ $2^{0.2975\beta}$	NTRU HRSS [SHRS17]
β-Sieve Q-β-Sieve	$\beta\, 2^{0.292\beta}$ $\beta\, 2^{0.265\beta}$	Frodo [NAB+17] Lizard [CPL+17] OKCN_AKCN_CNKE [ZjGS17] Round2 [GMZB+17]
$8d$-Sieve+$O(1)$	$8d\, 2^{0.292\beta+16.4}$	Ding Key Exchange [DTGW17] EMBLEM [SPL+17]
Q-$8d$-Sieve+$O(1)$	$8d\, 2^{0.265\beta+16.4}$	qTESLA [BAA+17]
Core-Enum+$O(1)$	$2^{0.187\beta \log \beta - 1.019\beta + 16.1}$	NTRU HRSS [SHRS17] NTRUEncrypt [ZCHW17a] pqNTRUSign [ZCHW17b]
Q-Core-Enum+$O(1)$	$2^{(0.187\beta \log \beta - 1.019\beta + 16.1)/2}$	NTRU HRSS [SHRS17]
$8d$-Enum (quadratic fit)+$O(1)$	$8d\, 2^{0.000784\beta^2 + 0.366\beta - 0.9}$	NTRU Prime [BCLvV17]
LOTUS-Enum	$2^{0.125\beta \log \beta - 0.755\beta + 2.25}$	LOTUS [PHAM17]

Table 4. Cost models proposed as part of a PQC NIST submission.

In the following, we illuminate some of the choices and assumptions we made to arrive at our estimates.

Error distributions. While the estimator assumes the distribution of error vector components to be a discrete Gaussian, many submissions use alternatives. Binomial distributions are treated as discrete Gaussians with the corresponding standard deviation. Similarly, bounded uniform distributions $U_{[a,b]}$ are also treated as discrete Gaussians with standard deviation, $\sqrt{\mathbb{V}_{U_{[a,b]}}[e_i] + \mathbb{E}_{U_{[a,b]}}[e_i]^2}$, since for any distribution χ,

$$e_{i=1\ldots n} \leftarrow \chi \implies \mathbb{E}_\chi[\|e\|^2] = n\left(\mathbb{V}_\chi[e_i] + \mathbb{E}_\chi[e_i]^2\right)$$

and the vector $(\boldsymbol{e} \,|\, 1)$ (or alternatively $(\boldsymbol{s} \,|\, \boldsymbol{e} \,|\, 1)$) is expected to be the unique shortest vector in the embedding lattice. In the case of LWR rounded continuous uniform error, we use a standard deviation of $\sqrt{q^2/(12p)^2}$ as done in [CPL+17,DKRV17,GMZB+17].

Success probability. The estimator supports defining a target success probability for both the primal and dual attack. The only proposal we found that explicitly uses this is LIMA [SAL+17], that sets it to 51%. For our estimates we imposed this to be the estimator's default 99% for all schemes, since it seems to make little to no difference for the final estimates as amplification in this range is rather cheap.

Known limitations. While the estimator can scale short secret vectors with entries sampled from a bounded uniform distribution, it does not attempt to shift secret vectors whose entries have unbalanced bounds to optimise the scaling. Similarly, it does not attempt to guess entries of such secrets to use a hybrid combinatorial approach. We note, however, that only the KINDI submission [Ban17] uses such a secret vector distribution. In this case, the deviation from a centred at zero distribution is small and we thus ignore it.

NTRU. For estimating NTRU-based schemes, we also utilise the LWE estimator as described in the following to evaluate the primal attack (and its improvements) on NTRU. The dual attack is not considered, as it does not apply. Let $(\boldsymbol{f}, \boldsymbol{g}) \in \mathbb{Z}^{2n}$ be the secret NTRU vector. We treat $\boldsymbol{f}$ as the LWE secret and $\boldsymbol{g}$ as the LWE error (or vice versa, as their roles can be swapped). The LWE secret dimension n is set to the degree of the NTRU polynomial ϕ. The standard deviation of the LWE distribution is set to $\|\boldsymbol{g}\| / \sqrt{n}$. The LWE modulus q is set to the NTRU modulus. The secret distribution is set to the distribution of $\boldsymbol{g}$. We limit the number of LWE samples to n. Furthermore, the success probability of "drop and solve" (i.e., the simplified Hybrid attack) is set to consider the n rotations of $\boldsymbol{g}$.

Scheme	Claim	NIST	Attack	Q-Core-Sieve	Q-Core-Sieve + O(1)	Q-Core-Sieve (min space)	Q-β-Sieve	Q-8d-Sieve + O(1)	Core-Sieve	Core-Sieve + O(1)	Core-Sieve (min space)	β-Sieve	8d-Sieve + O(1)
AKCN-MLWE-0768-1.00-7681	147.00	4	dual	179.42	194.28	197.26	189.34	205.15	193.83	209.60	238.10	202.97	219.10
AKCN-MLWE-0768-1.00-7681	147.00	4	primal	148.67	164.67	166.90	157.80	178.55	163.81	179.81	206.45	172.94	193.69
AKCN-MLWE-0768-2.24-7681	183.00	4	dual	226.31	242.31	249.31	236.05	249.73	244.70	260.70	299.55	254.41	268.09
AKCN-MLWE-0768-2.24-7681	183.00	4	primal	184.44	200.44	207.06	193.88	214.41	203.23	219.23	256.13	212.67	233.20
AKCN-RLWE-1024-2.83-12289	255.00	5	dual	315.62	320.81	338.79	318.59	334.89	337.93	347.42	413.26	341.68	361.82
AKCN-RLWE-1024-2.83-12289	255.00	5	primal	257.31	273.31	288.87	267.24	287.70	283.53	299.53	357.33	293.46	313.92
BabyBear-0624-0.79-1024	141.00	2	dual	179.14	190.93	196.35	185.98	204.50	192.73	205.25	231.51	202.09	217.72
BabyBear-0624-0.79-1024	141.00	2	primal	142.04	158.04	159.46	151.11	171.56	156.51	172.51	197.25	165.58	186.03
BabyBear-0624-1.00-1024	152.00	2	dual	192.40	205.02	210.36	201.89	217.04	206.77	222.44	252.08	215.91	230.94
BabyBear-0624-1.00-1024	152.00	2	primal	152.91	168.91	171.66	162.08	182.49	168.48	184.48	212.34	177.66	198.07
CRYSTALS-Dilithium-0768-3.74-8380417	91.00	1	dual	109.48	122.31	119.64	116.80	134.34	118.84	131.11	142.49	125.94	143.09
CRYSTALS-Dilithium-0768-3.74-8380417	91.00	1	primal	91.95	107.95	103.23	100.39	121.93	101.32	117.32	127.70	109.76	131.30
CRYSTALS-Dilithium-1024-3.16-8380417	125.00	2	dual	148.59	162.72	164.33	157.63	175.73	162.32	176.05	197.48	169.35	188.17
CRYSTALS-Dilithium-1024-3.16-8380417	125.00	2	primal	129.32	145.32	145.18	138.25	159.71	142.50	158.50	179.58	151.43	172.88
CRYSTALS-Dilithium-1280-2.00-8380417	158.00	3	dual	178.70	192.59	198.19	186.93	205.48	194.53	208.26	238.53	203.91	222.91
CRYSTALS-Dilithium-1280-2.00-8380417	158.00	3	primal	158.74	174.74	178.20	167.96	189.43	174.91	190.91	220.43	184.13	205.60
CRYSTALS-Kyber-0512-1.58-7681	102.00	1	dual	136.35	143.21	142.82	137.23	154.22	140.26	153.55	168.85	147.60	164.33
CRYSTALS-Kyber-0512-1.58-7681	102.00	1	primal	102.29	118.29	114.83	110.88	131.68	112.71	128.71	142.05	121.30	142.10
CRYSTALS-Kyber-0768-1.41-7681	161.00	3	dual	197.18	213.16	216.79	206.70	221.87	216.16	227.41	259.81	220.96	241.39
CRYSTALS-Kyber-0768-1.41-7681	161.00	3	primal	162.71	178.71	182.66	171.97	192.66	179.29	195.29	225.95	188.55	209.24
CRYSTALS-Kyber-1024-1.22-7681	218.00	5	dual	264.47	279.77	287.98	274.43	286.67	282.79	298.66	347.76	292.58	313.06
CRYSTALS-Kyber-1024-1.22-7681	218.00	5	primal	220.22	236.22	247.22	229.91	250.55	242.65	258.65	305.81	252.35	272.99
Ding Key Exchange-0512-4.19-120883	—	1	dual	115.67	128.77	127.34	122.38	139.15	125.01	138.05	149.48	131.50	148.60
Ding Key Exchange-0512-4.19-120883	—	1	primal	91.43	107.43	102.64	99.86	120.82	100.74	116.74	126.96	109.17	130.13
Ding Key Exchange-1024-2.60-120883	—	3, 5	dual	226.31	237.27	246.93	236.05	250.35	242.39	258.36	296.98	252.06	272.76
Ding Key Exchange-1024-2.60-120883	—	3, 5	primal	190.27	206.27	213.60	199.76	220.67	209.66	225.66	264.22	219.14	240.05
EMBLEM-0611-25.00-16777216	128.30	1	dual	84.08	97.33	92.46	90.73	108.46	90.81	104.12	109.24	97.84	114.42
EMBLEM-0611-25.00-16777216	128.30	1	primal	68.90	84.90	77.35	76.92	98.52	75.92	91.92	95.68	83.94	105.54
EMBLEM-0770-25.00-16777216	128.30	1	dual	102.74	116.45	113.36	109.96	128.81	111.32	125.50	134.92	118.45	137.42
EMBLEM-0770-25.00-16777216	128.30	1	primal	89.31	105.31	100.26	97.70	119.22	98.40	114.40	124.02	106.80	128.32
FireSaber-1024-2.31-8192	245.00	5	dual	315.62	320.78	338.72	318.47	334.89	337.80	347.42	413.26	341.67	361.82
FireSaber-1024-2.31-8192	245.00	5	primal	257.31	273.31	288.87	267.24	287.70	283.53	299.53	357.33	293.46	313.91
Frodo-0640-2.75-32768	103.00	1	dual	158.27	171.08	173.55	167.43	184.48	171.01	186.24	207.21	179.43	196.17
Frodo-0640-2.75-32768	103.00	1	primal	128.53	144.53	144.29	137.45	158.24	141.62	157.62	178.48	150.54	171.34
Frodo-0976-2.30-65536	150.00	3	dual	224.19	234.39	244.55	232.80	248.16	240.03	256.02	294.03	249.71	270.35
Frodo-0976-2.30-65536	150.00	3	primal	187.36	203.36	210.33	196.82	217.67	206.44	222.44	260.18	215.91	236.76

Scheme	Claim	NIST	Attack	Q-Core-Sieve	Q-Core-Sieve + O(1)	Q-Core-Sieve (min space)	Q-β-Sieve	Q-8d-Sieve + O(1)	Core-Sieve	Core-Sieve + O(1)	Core-Sieve (min space)	β-Sieve	8d-Sieve + O(1)
HILA5-1024-2.83-12289	128.00	5	dual	315.62	320.81	338.79	318.59	334.89	337.93	347.42	413.26	341.68	361.82
HILA5-1024-2.83-12289	128.00	5	primal	257.31	273.31	288.87	267.24	287.70	283.53	299.53	357.33	293.46	313.92
KINDI-0768-2.35-16384	164.00	2	dual	207.10	217.56	226.20	212.09	231.51	222.03	237.01	267.57	231.60	246.17
KINDI-0768-2.35-16384	164.00	2	primal	170.40	186.40	191.29	179.72	200.37	187.76	203.76	236.62	197.08	217.73
KINDI-1024-1.12-8192	207.00	4	dual	257.36	273.36	283.55	267.28	283.72	283.57	291.41	338.93	287.36	305.20
KINDI-1024-1.12-8192	207.00	4	primal	220.22	236.22	247.22	229.91	250.56	242.65	258.65	305.81	252.35	273.00
KINDI-1024-2.29-16384	232.00	4	dual	284.27	295.38	311.83	290.57	306.05	309.17	318.95	371.55	313.47	329.46
KINDI-1024-2.29-16384	232.00	4	primal	237.97	253.97	267.15	247.78	268.37	262.22	278.22	330.46	272.03	292.61
KINDI-1280-1.12-16384	251.00	5	dual	308.74	317.74	339.17	313.08	328.71	332.90	348.90	403.21	343.05	359.75
KINDI-1280-1.12-16384	251.00	5	primal	263.68	279.68	296.01	273.63	294.32	290.54	306.54	366.16	300.50	321.19
KINDI-1536-1.12-8192	330.00	5	dual	407.04	420.92	448.04	415.50	432.64	446.77	453.72	539.49	448.80	468.67
KINDI-1536-1.12-8192	330.00	5	primal	351.92	367.92	395.08	362.30	382.83	387.78	403.78	488.70	398.15	418.69
LAC-0512-0.71-251	128.00	1, 2	dual	177.29	189.05	194.27	182.83	198.34	190.68	202.02	230.77	196.28	212.10
LAC-0512-0.71-251	128.00	1, 2	primal	135.15	151.15	151.72	144.14	164.35	148.92	164.92	187.68	157.91	178.12
LAC-1024-0.50-251	192.00	3, 4	dual	326.48	342.48	353.45	336.75	347.61	348.14	362.90	421.73	357.11	377.09
LAC-1024-0.50-251	192.00	3, 4	primal	261.03	277.03	293.04	270.97	291.10	287.62	303.62	362.48	297.56	317.70
LAC-1024-0.71-251	256.00	5	dual	363.05	379.05	407.57	373.47	393.32	400.04	413.93	483.55	410.46	415.44
LAC-1024-0.71-251	256.00	5	primal	292.82	308.82	328.74	302.93	322.94	322.66	338.66	406.64	332.77	352.78
LIMA-2p-1024-3.16-133121	208.80	3	dual	236.12	245.23	257.34	239.23	259.63	252.58	268.58	309.49	262.34	280.61
LIMA-2p-1024-3.16-133121	208.80	3	primal	197.16	213.16	221.34	206.70	227.55	217.25	233.25	273.79	226.79	247.64
LIMA-2p-2048-3.16-184321	444.50	4	dual	492.90	508.90	553.35	503.76	524.30	543.12	559.12	651.73	553.98	574.52
LIMA-2p-2048-3.16-184321	444.50	4	primal	429.04	445.04	481.65	439.70	460.43	472.75	488.75	595.79	483.41	504.14
LIMA-sp-1018-3.16-12521473	139.20	1	dual	142.63	158.04	159.46	151.11	169.53	156.51	169.32	190.11	163.74	183.69
LIMA-sp-1018-3.16-12521473	139.20	1	primal	124.02	140.02	139.23	132.89	154.40	136.66	152.66	172.22	145.53	167.04
LIMA-sp-1306-3.16-48181249	167.80	2	dual	173.31	186.86	189.93	182.66	199.82	187.33	202.30	233.68	195.62	217.05
LIMA-sp-1306-3.16-48181249	167.80	2	primal	152.11	168.11	170.76	161.27	182.85	167.61	183.61	211.23	176.77	198.35
LIMA-sp-1822-3.16-44802049	247.90	3	dual	258.11	274.11	289.77	268.04	289.34	284.41	300.41	349.60	294.34	315.64
LIMA-sp-1822-3.16-44802049	247.90	3	primal	232.41	248.41	260.91	242.18	263.62	256.08	272.08	322.74	265.86	287.30
LIMA-sp-2062-3.16-16900097	303.50	4	dual	332.05	340.24	359.08	340.17	351.27	352.44	368.44	444.18	362.68	383.85
LIMA-sp-2062-3.16-16900097	303.50	4	primal	290.97	306.97	326.65	301.07	322.38	320.62	336.62	404.06	330.72	352.03
LOTUS-0576-3.00-8192	128.00	1, 2	dual	181.53	193.29	199.03	187.04	203.13	195.35	206.45	233.32	202.17	219.95
LOTUS-0576-3.00-8192	128.00	1, 2	primal	142.31	158.31	159.76	151.37	171.87	156.80	172.80	197.62	165.87	186.37
LOTUS-0704-3.00-8192	192.00	3, 4	dual	224.46	236.96	245.44	234.18	247.96	240.91	256.90	294.40	250.59	264.75
LOTUS-0704-3.00-8192	192.00	3, 4	primal	179.94	195.94	202.00	189.34	209.79	198.27	214.27	249.87	207.68	228.12
LOTUS-0832-3.00-8192	256.00	5	dual	269.51	280.21	297.50	274.22	294.31	292.00	306.89	347.63	301.97	312.78
LOTUS-0832-3.00-8192	256.00	5	primal	218.36	234.36	245.14	228.05	248.46	240.61	256.61	303.23	250.29	270.70

Scheme	Claim	NIST	Attack	Q-Core-Sieve	Q-Core-Sieve + O(1)	Q-Core-Sieve (min space)	Q-β-Sieve	Q-8d-Sieve + O(1)	Core-Sieve	Core-Sieve + O(1)	Core-Sieve (min space)	β-Sieve	8d-Sieve + O(1)
LightSaber-0512-2.31-8192	115.00	1	dual	152.37	158.07	168.37	160.37	168.60	168.37	169.26	187.72	168.38	181.53
LightSaber-0512-2.31-8192	115.00	1	primal	113.69	129.69	127.63	122.43	143.09	125.27	141.27	157.87	134.01	154.67
Lizard-0536-1.15-2048	130.00	1	dual	126.59	139.67	138.07	133.52	149.70	136.22	148.36	161.63	143.96	158.88
Lizard-0536-1.15-2048	130.00	1	primal	104.94	120.94	117.81	113.57	134.18	115.63	131.63	145.73	124.26	144.87
Lizard-0663-1.15-1024	147.00	1	dual	170.40	183.13	185.36	176.42	192.07	181.19	196.17	219.35	193.40	204.99
Lizard-0663-1.15-1024	147.00	1	primal	144.47	160.47	162.15	153.56	173.94	159.16	175.16	200.14	168.24	188.63
Lizard-0816-1.15-2048	195.00	3	dual	201.97	214.92	221.39	208.84	225.48	218.08	229.49	261.25	224.90	242.47
Lizard-0816-1.15-2048	195.00	3	primal	172.52	188.52	193.67	181.86	202.32	190.09	206.09	239.31	199.44	219.90
Lizard-0952-1.15-2048	195.00	3	dual	235.55	247.27	255.48	241.25	257.54	252.00	267.87	301.77	263.61	277.21
Lizard-0952-1.15-2048	195.00	3	primal	203.33	219.33	228.23	212.91	233.34	224.01	240.01	282.17	233.59	254.02
Lizard-1088-1.15-4096	257.00	5	dual	247.15	258.04	265.02	253.72	268.16	263.52	281.43	317.48	270.07	290.39
Lizard-1088-1.15-4096	257.00	5	primal	217.04	233.04	243.64	226.71	247.23	239.15	255.15	301.09	248.82	269.35
Lizard-1300-1.15-2048	291.00	5	dual	312.75	322.93	341.41	319.32	336.43	337.90	347.86	398.55	344.12	375.42
Lizard-1300-1.15-2048	291.00	5	primal	282.40	298.40	316.56	292.45	312.82	311.06	327.06	380.46	321.11	341.47
MamaBear-0936-0.71-1024	219.00	4	dual	272.02	280.74	297.20	274.91	294.93	291.71	307.71	351.44	301.67	316.12
MamaBear-0936-0.71-1024	219.00	4	primal	219.95	235.95	246.92	229.65	250.03	242.36	258.36	305.44	252.06	272.44
MamaBear-0936-0.94-1024	237.00	5	dual	293.09	309.09	326.66	303.20	320.13	320.62	330.59	386.03	330.52	340.34
MamaBear-0936-0.94-1024	237.00	5	primal	238.77	254.77	268.05	248.58	268.88	263.09	279.09	331.57	272.91	293.21
NewHope-0512-2.00-12289	101.00	1	dual	136.50	143.21	142.82	137.31	154.22	140.27	153.55	168.95	147.68	164.33
NewHope-0512-2.00-12289	101.00	1	primal	102.29	118.29	114.83	110.88	131.69	112.71	128.71	142.05	121.30	142.11
NewHope-1024-2.00-12289	233.00	5	dual	279.93	293.99	312.08	288.02	308.39	306.31	322.31	370.58	316.34	332.52
NewHope-1024-2.00-12289	233.00	5	primal	234.79	250.79	263.58	244.58	265.19	258.71	274.71	326.05	268.50	289.11
PapaBear-1248-0.61-1024	292.00	5	dual	349.35	365.27	387.94	359.63	379.83	380.77	396.77	461.84	391.12	411.32
PapaBear-1248-0.61-1024	292.00	5	primal	292.56	308.56	328.44	302.67	322.99	322.37	338.37	406.27	332.48	352.80
PapaBear-1248-0.87-1024	320.00	5	dual	389.02	405.02	436.73	399.54	419.64	428.66	444.66	524.40	439.18	455.62
PapaBear-1248-0.87-1024	320.00	5	primal	323.04	339.04	362.65	333.29	353.52	355.95	371.95	448.59	366.20	386.43
R EMBLEM-0512-25.00-65536	128.00	1	dual	125.69	138.76	137.20	132.07	149.14	134.90	148.29	163.39	142.37	159.04
R EMBLEM-0512-25.00-65536	128.00	1	primal	101.50	117.50	113.94	110.08	130.79	111.84	127.84	140.94	120.42	141.13
R EMBLEM-0512-3.00-16384	128.00	1	dual	112.50	124.99	122.80	119.12	135.76	121.17	134.28	145.40	128.57	145.31
R EMBLEM-0512-3.00-16384	128.00	1	primal	91.43	107.43	102.64	99.86	120.71	100.74	116.74	126.96	109.17	130.03
RLizard-1024-1.15-1024	147.00	1	dual	252.78	261.32	267.31	258.64	279.56	274.20	282.40	313.81	279.22	289.24
RLizard-1024-1.15-1024	147.00	1	primal	224.64	240.64	246.71	234.13	254.47	243.31	259.31	288.00	252.64	272.98
RLizard-1024-1.15-2048	195.00	3	dual	262.08	275.40	286.80	270.54	285.80	282.51	299.24	341.15	290.99	304.70
RLizard-1024-1.15-2048	195.00	3	primal	224.99	240.99	252.58	234.71	255.10	247.91	263.91	312.43	257.64	278.03
RLizard-2048-1.15-2048	291.00	3	dual	399.96	415.21	449.50	409.14	431.98	444.59	454.39	568.12	448.20	444.83
RLizard-2048-1.15-2048	291.00	3	primal	388.47	404.47	416.49	398.33	418.73	412.12	428.12	468.09	421.62	442.05

Scheme	Claim	NIST	Attack	Q-Core-Sieve	Q-Core-Sieve + O(1)	Q-Core-Sieve (min space)	Q-β-Sieve	Q-8d-Sieve + O(1)	Core-Sieve	Core-Sieve + O(1)	Core-Sieve (min space)	β-Sieve	8d-Sieve + O(1)
RLizard-2048-1.15-4096	348.00	5	dual	484.17	484.97	501.54	484.35	491.60	496.38	506.08	564.94	501.69	512.71
RLizard-2048-1.15-4096	348.00	5	primal	429.40	445.40	473.46	439.88	460.28	466.23	482.23	554.65	476.59	497.02
Saber-0768-2.31-8192	180.00	3	dual	226.31	242.31	249.31	236.05	249.73	244.70	260.70	299.55	254.41	268.10
Saber-0768-2.31-8192	180.00	3	primal	184.44	200.44	207.06	193.88	214.41	203.23	219.23	256.13	212.67	233.20
Titanium.KEM-1024-1.41-118273	128.00	1	dual	194.79	210.78	214.83	204.30	221.71	212.85	226.53	260.91	220.03	240.93
Titanium.KEM-1024-1.41-118273	128.00	1	primal	167.22	183.22	187.72	176.52	197.57	184.25	200.25	232.21	193.55	214.60
Titanium.KEM-1280-1.41-430081	160.00	1	dual	222.60	238.60	245.44	232.31	251.85	240.90	256.90	299.18	250.59	271.62
Titanium.KEM-1280-1.41-430081	160.00	1	primal	193.72	209.72	217.47	203.23	224.39	213.45	229.45	269.01	222.97	244.12
Titanium.KEM-1536-1.41-783361	192.00	3	dual	258.68	274.64	286.32	268.57	289.62	283.08	296.90	354.02	290.82	311.89
Titanium.KEM-1536-1.41-783361	192.00	3	primal	229.76	245.76	257.93	239.51	260.68	253.16	269.16	319.06	262.92	284.09
Titanium.KEM-2048-1.41-1198081	256.00	5	dual	349.01	365.01	391.81	359.37	380.41	384.56	400.56	482.64	394.93	415.96
Titanium.KEM-2048-1.41-1198081	256.00	5	primal	313.50	329.50	351.94	323.70	344.83	345.44	361.44	435.34	355.64	376.77
Titanium.PKE-1024-1.41-86017	128.00	1	dual	204.32	215.24	225.51	212.04	229.42	221.34	236.50	271.58	230.90	245.90
Titanium.PKE-1024-1.41-86017	128.00	1	primal	172.78	188.78	193.97	182.13	203.15	190.38	206.38	239.94	199.73	220.76
Titanium.PKE-1280-1.41-301057	160.00	1	dual	231.80	243.64	258.32	237.41	258.36	254.33	263.09	311.33	258.73	277.75
Titanium.PKE-1280-1.41-301057	160.00	1	primal	200.61	216.61	225.21	210.17	231.27	221.04	237.04	278.58	230.61	251.71
Titanium.PKE-1536-1.41-737281	192.00	3	dual	260.24	276.23	288.02	270.17	291.21	283.68	298.66	356.22	292.58	313.64
Titanium.PKE-1536-1.41-737281	192.00	3	primal	230.81	246.81	259.12	240.58	261.75	254.33	270.33	320.53	264.10	285.27
Titanium.PKE-2048-1.41-1198081	256.00	5	dual	349.01	365.01	391.81	359.37	380.41	384.56	400.56	482.64	394.93	415.96
Titanium.PKE-2048-1.41-1198081	256.00	5	primal	313.50	329.50	351.94	323.70	344.83	345.44	361.44	435.34	355.64	376.77
nRound2.KEM-0400-3.62-3209	74.00	1	dual	95.12	106.29	102.31	101.02	116.30	101.22	112.59	116.81	107.53	121.73
nRound2.KEM-0400-3.62-3209	74.00	1	primal	78.17	94.17	87.76	86.38	106.96	86.14	102.14	108.45	94.34	114.92
nRound2.KEM-0486-2.20-1949	97.00	2	dual	120.67	132.11	130.62	126.55	142.54	129.18	140.42	150.10	135.56	151.01
nRound2.KEM-0486-2.20-1949	97.00	2	primal	100.17	116.17	112.45	108.73	129.22	110.38	126.38	138.95	118.94	139.43
nRound2.KEM-0556-3.77-3343	106.00	3	dual	133.79	144.79	146.84	140.61	156.33	143.10	154.02	164.78	149.85	165.91
nRound2.KEM-0556-3.77-3343	106.00	3	primal	115.16	131.16	128.99	123.90	144.38	126.68	142.68	155.96	135.39	155.90
nRound2.KEM-0658-1.49-1319	139.00	4, 5	dual	169.60	180.56	184.90	175.94	191.53	182.46	193.44	213.74	188.51	204.69
nRound2.KEM-0658-1.49-1319	139.00	4, 5	primal	143.63	159.63	161.25	152.71	173.11	158.26	174.26	199.21	167.35	187.75
nRound2.PKE-0442-1.50-2659	74.00	1	dual	94.44	105.66	101.74	100.25	115.61	100.92	112.14	117.51	106.06	121.78
nRound2.PKE-0442-1.50-2659	74.00	1	primal	79.23	95.23	88.95	87.46	108.18	87.31	103.31	109.40	95.53	116.25
nRound2.PKE-0556-1.88-3343	97.00	2	dual	121.72	132.90	130.71	128.56	144.85	131.00	141.96	150.21	135.02	151.19
nRound2.PKE-0556-1.88-3343	97.00	2	primal	104.66	120.66	117.46	113.28	133.93	115.30	131.30	143.33	123.92	144.57
nRound2.PKE-0576-1.30-2309	106.00	3	dual	130.37	142.61	141.36	137.08	152.77	141.07	151.66	166.03	146.50	163.47
nRound2.PKE-0576-1.30-2309	106.00	3	primal	111.04	127.04	124.65	119.75	140.35	122.35	138.35	154.12	131.06	151.67
nRound2.PKE-0708-1.60-2837	138.00	4, 5	dual	166.49	178.91	181.25	174.03	190.44	179.11	191.99	211.94	185.26	201.37
nRound2.PKE-0708-1.60-2837	138.00	4, 5	primal	143.10	159.10	160.65	152.18	172.72	157.68	173.68	198.47	166.76	187.30

Scheme	Claim	NIST	Attack	Q-Core-Sieve	Q-Core-Sieve + O(1)	Q-Core-Sieve (min space)	Q-β-Sieve	Q-8d-Sieve + O(1)	Core-Sieve	Core-Sieve + O(1)	Core-Sieve (min space)	β-Sieve	8d-Sieve + O(1)
qTESLA-1024-8.49-8058881	128.00	1	dual	184.44	195.95	202.00	190.38	210.34	198.27	214.27	243.25	207.68	224.09
qTESLA-1024-8.49-8058881	128.00	1	primal	156.62	172.62	175.82	165.82	187.01	172.57	188.57	217.49	181.78	202.97
qTESLA-2048-8.49-12681217	192.00	3	dual	394.59	410.59	442.98	405.13	425.99	434.79	450.79	532.13	445.33	466.19
qTESLA-2048-8.49-12681217	192.00	3	primal	347.68	363.68	390.32	358.04	379.08	383.10	399.10	482.82	393.46	414.50
qTESLA-2048-8.49-27627521	256.00	5	dual	364.64	380.64	409.36	375.07	396.04	401.79	417.79	486.98	412.22	433.19
qTESLA-2048-8.49-27627521	256.00	5	primal	325.42	341.42	365.33	335.68	356.82	358.58	374.58	451.90	368.84	389.98
uRound2.KEM-0418-4.62-4096	75.00	1	dual	96.97	108.04	104.37	103.73	117.27	103.44	114.33	117.47	108.27	125.39
uRound2.KEM-0418-4.62-4096	75.00	1	primal	81.53	97.53	91.34	89.77	110.36	89.68	105.68	110.74	97.92	118.51
uRound2.KEM-0500-2.31-16384	74.00	1	dual	87.76	100.50	95.34	93.69	109.89	93.53	105.51	108.60	99.70	116.00
uRound2.KEM-0500-2.31-16384	74.00	1	primal	76.02	92.02	85.63	84.18	105.17	83.74	99.74	104.77	92.22	112.89
uRound2.KEM-0522-36.95-32768	97.00	2	dual	122.42	134.33	131.55	128.83	143.03	131.03	141.73	148.52	137.03	154.52
uRound2.KEM-0522-36.95-32768	97.00	2	primal	106.14	122.14	119.04	114.77	135.27	116.86	132.86	142.23	125.49	145.99
uRound2.KEM-0540-18.48-16384	106.00	3	dual	132.55	144.80	143.48	139.87	154.32	142.86	153.05	164.44	148.48	164.01
uRound2.KEM-0540-18.48-16384	106.00	3	primal	112.62	128.62	126.38	121.36	141.84	124.07	140.07	155.20	132.78	153.25
uRound2.KEM-0580-4.62-32768	96.00	2	dual	110.32	122.51	119.83	117.11	133.87	118.22	131.20	141.51	124.77	141.56
uRound2.KEM-0580-4.62-32768	96.00	2	primal	94.08	110.08	105.61	102.55	123.48	103.66	119.66	130.64	112.13	133.06
uRound2.KEM-0630-4.62-32768	106.00	3	dual	121.29	134.04	132.80	128.41	145.10	130.43	143.50	156.36	137.52	154.72
uRound2.KEM-0630-4.62-32768	106.00	3	primal	104.41	120.41	117.21	113.03	133.92	115.05	131.05	144.99	123.67	144.56
uRound2.KEM-0676-36.95-32768	139.00	5	dual	170.45	182.13	186.02	178.29	193.64	181.69	194.16	217.49	190.13	204.85
uRound2.KEM-0676-36.95-32768	139.00	5	primal	146.55	162.55	164.50	155.66	176.05	161.47	177.47	201.99	170.57	190.98
uRound2.KEM-0700-36.95-32768	140.00	4	dual	173.41	184.65	190.13	179.97	198.69	187.50	196.81	223.40	190.62	208.50
uRound2.KEM-0700-36.95-32768	140.00	4	primal	151.04	167.04	169.59	160.19	180.59	166.55	182.55	204.82	175.66	196.05
uRound2.KEM-0786-4.62-32768	138.00	5	dual	156.92	169.59	171.29	164.30	181.42	168.92	182.34	201.86	175.85	192.63
uRound2.KEM-0786-4.62-32768	138.00	5	primal	137.27	153.27	154.10	146.29	167.06	151.26	167.26	190.58	160.27	181.04
uRound2.KEM-0786-4.62-32768	139.00	4	dual	156.92	169.59	171.29	164.30	181.42	168.92	182.34	201.86	175.85	192.63
uRound2.KEM-0786-4.62-32768	139.00	4	primal	137.27	153.27	154.10	146.29	167.06	151.26	167.26	190.58	160.27	181.04
uRound2.PKE-0420-1.15-1024	74.00	1	dual	95.97	107.18	102.23	101.38	116.33	101.12	112.53	115.14	106.72	121.70
uRound2.PKE-0420-1.15-1024	74.00	1	primal	81.25	97.25	90.97	89.50	110.08	89.45	105.45	110.29	97.57	118.19
uRound2.PKE-0500-4.62-32768	74.00	1	dual	87.86	99.69	94.62	93.82	109.62	93.67	105.14	108.26	99.95	115.80
uRound2.PKE-0500-4.62-32768	74.00	1	primal	76.02	92.02	85.63	84.18	105.17	83.74	99.74	104.77	92.22	112.89
uRound2.PKE-0540-4.62-8192	97.00	2	dual	120.22	132.39	129.60	125.98	142.65	128.38	141.22	151.66	137.29	151.41
uRound2.PKE-0540-4.62-8192	97.00	2	primal	102.29	118.29	114.78	110.88	131.50	112.68	128.68	141.58	121.25	141.91
uRound2.PKE-0585-4.62-32768	96.00	2	dual	110.60	122.73	120.58	117.45	134.16	118.49	131.01	139.73	125.00	141.39
uRound2.PKE-0585-4.62-32768	96.00	2	primal	94.87	110.87	106.50	103.35	124.24	104.54	120.54	131.74	113.02	133.90
uRound2.PKE-0586-4.62-8192	107.00	3	dual	131.82	143.52	142.84	138.44	153.97	141.23	152.74	165.30	148.16	163.20
uRound2.PKE-0586-4.62-8192	107.00	3	primal	113.16	129.16	126.92	121.89	142.49	124.62	140.62	156.40	133.33	153.95

Scheme	Claim	NIST	Attack	Q-Core-Sieve	Q-Core-Sieve + O(1)	Q-Core-Sieve (min space)	Q-β-Sieve	Q-8d-Sieve + O(1)	Core-Sieve	Core-Sieve + O(1)	Core-Sieve (min space)	β-Sieve	8d-Sieve + O(1)
uRound2.PKE-0643-4.62-32768	106.00	3	dual	122.36	134.47	132.68	128.63	145.41	131.92	144.03	155.91	137.66	154.86
uRound2.PKE-0643-4.62-32768	106.00	3	primal	106.27	122.27	119.28	114.91	135.77	117.08	133.08	147.46	125.73	146.59
uRound2.PKE-0708-18.48-32768	138.00	4, 5	dual	166.50	179.22	181.05	173.70	190.12	178.39	191.83	212.43	185.12	201.37
uRound2.PKE-0708-18.48-32768	138.00	4, 5	primal	143.37	159.37	160.73	152.38	172.96	157.79	173.79	198.84	166.85	187.40
uRound2.PKE-0835-2.31-32768	138.00	4	dual	155.36	168.28	169.76	162.69	180.87	167.61	180.48	202.13	176.15	191.68
uRound2.PKE-0835-2.31-32768	138.00	4	primal	136.79	152.79	153.53	145.80	166.71	150.70	166.70	189.84	159.71	180.61
uRound2.PKE-0835-2.31-32768	138.00	5	dual	155.36	168.28	169.76	162.69	180.87	167.61	180.48	202.13	176.15	191.68
uRound2.PKE-0835-2.31-32768	138.00	5	primal	136.79	152.79	153.53	145.80	166.71	150.70	166.70	189.84	159.71	180.61

Table 5: Cost of primal and dual attacks against LWE-based schemes assuming n LWE samples using sieving. The column Scheme indicates each instantiation of a scheme using the format NAME-n-σ-q.

Scheme	Claim	NIST	Attack	Q-Core-Sieve	Q-Core-Sieve + O(1)	Q-Core-Sieve (min space)	Q-β-Sieve	Q-8d-Sieve + O(1)	Core-Sieve	Core-Sieve + O(1)	Core-Sieve (min space)	β-Sieve	8d-Sieve + O(1)
AKCN-MLWE-0768-1.00-7681	147.00	4	dual	179.16	195.14	197.00	186.51	204.66	193.86	209.30	237.73	202.68	219.08
AKCN-MLWE-0768-1.00-7681	147.00	4	primal	148.67	164.67	166.90	157.80	178.55	163.81	179.81	206.45	172.94	193.69
AKCN-MLWE-0768-2.24-7681	183.00	4	dual	223.73	236.48	247.52	230.20	250.62	242.94	257.00	294.77	252.64	266.36
AKCN-MLWE-0768-2.24-7681	183.00	4	primal	184.18	200.18	206.76	193.62	214.19	202.94	218.94	255.76	212.38	232.95
AKCN-RLWE-1024-2.83-12289	255.00	5	dual	305.55	321.55	343.02	315.72	336.11	336.68	347.94	408.11	346.85	355.55
AKCN-RLWE-1024-2.83-12289	255.00	5	primal	256.52	272.52	287.98	266.44	286.96	282.66	298.66	356.22	292.57	313.09
BabyBear-0624-0.79-1024	141.00	2	dual	179.14	190.93	196.35	185.98	204.50	192.73	205.25	231.51	202.09	217.72
BabyBear-0624-0.79-1024	141.00	2	primal	142.04	158.04	159.46	151.11	171.56	156.51	172.51	197.25	165.58	186.03
BabyBear-0624-1.00-1024	152.00	2	dual	191.90	206.67	209.89	201.36	216.54	207.26	221.86	252.08	215.32	230.91
BabyBear-0624-1.00-1024	152.00	2	primal	152.91	168.91	171.66	162.08	182.49	168.48	184.48	212.34	177.66	198.07
CRYSTALS-Dilithium-0768-3.74-8380417	91.00	1	dual	107.06	119.97	117.55	113.90	132.39	115.51	129.38	140.54	122.87	141.80
CRYSTALS-Dilithium-0768-3.74-8380417	91.00	1	primal	90.90	106.90	102.04	99.32	120.98	100.16	116.16	126.22	108.58	130.24
CRYSTALS-Dilithium-1024-3.16-8380417	125.00	2	dual	147.37	160.87	163.34	155.03	174.00	160.34	174.04	195.10	167.48	187.65
CRYSTALS-Dilithium-1024-3.16-8380417	125.00	2	primal	128.79	144.79	144.58	137.71	159.26	141.91	157.91	178.85	150.84	172.38
CRYSTALS-Dilithium-1280-2.00-8380417	158.00	3	dual	177.49	193.09	196.68	186.47	205.78	194.60	208.78	238.90	202.15	221.24
CRYSTALS-Dilithium-1280-2.00-8380417	158.00	3	primal	158.47	174.47	177.91	167.69	189.20	174.62	190.62	220.06	183.84	205.35
CRYSTALS-Kyber-0512-1.58-7681	102.00	1	dual	129.06	142.16	140.53	135.39	153.57	138.40	151.44	166.85	146.71	162.70
CRYSTALS-Kyber-0512-1.58-7681	102.00	1	primal	102.29	118.29	114.83	110.88	131.68	112.71	128.71	142.05	121.30	142.10
CRYSTALS-Kyber-0768-1.41-7681	161.00	3	dual	195.86	211.57	219.56	205.10	221.47	215.50	225.98	257.98	220.96	240.01
CRYSTALS-Kyber-0768-1.41-7681	161.00	3	primal	162.71	178.71	182.66	171.97	192.66	179.29	195.29	225.95	188.55	209.24
CRYSTALS-Kyber-1024-1.22-7681	218.00	5	dual	263.41	279.41	287.06	273.37	286.53	285.51	297.20	344.82	291.14	311.62
CRYSTALS-Kyber-1024-1.22-7681	218.00	5	primal	220.22	236.22	247.22	229.91	250.55	242.65	258.65	305.81	252.35	272.99
Ding Key Exchange-0512-4.19-120883	—	1	dual	110.31	124.12	121.39	117.04	135.18	119.19	133.09	144.99	126.10	144.70
Ding Key Exchange-0512-4.19-120883	—	1	primal	89.31	105.31	100.26	97.70	118.86	98.40	114.40	124.02	106.80	127.96
Ding Key Exchange-1024-2.60-120883	—	3, 5	dual	221.39	235.42	245.68	229.12	249.96	244.70	253.98	295.56	247.95	268.51
Ding Key Exchange-1024-2.60-120883	—	3, 5	primal	189.74	205.74	213.01	199.22	220.20	209.07	225.07	263.49	218.56	239.53
EMBLEM-0611-25.00-16777216	128.30	1	dual	83.75	95.80	91.37	89.20	106.96	89.18	103.63	107.52	96.78	114.97
EMBLEM-0611-25.00-16777216	128.30	1	primal	68.64	84.64	77.05	76.65	98.30	75.63	91.63	95.31	83.64	105.29
EMBLEM-0770-25.00-16777216	128.30	1	dual	102.90	116.23	113.02	110.35	128.32	111.57	124.58	134.91	118.95	136.78
EMBLEM-0770-25.00-16777216	128.30	1	primal	89.31	105.31	100.26	97.70	119.22	98.40	114.40	124.02	106.80	128.32
FireSaber-1024-2.31-8192	245.00	5	dual	307.67	323.67	337.07	317.85	338.20	339.01	345.19	410.32	344.73	357.85
FireSaber-1024-2.31-8192	245.00	5	primal	257.31	273.31	288.87	267.24	287.72	283.53	299.53	357.33	293.46	313.93
Frodo-0640-2.75-32768	103.00	1	dual	154.40	169.44	171.50	162.61	179.91	169.07	181.27	203.15	174.58	192.49
Frodo-0640-2.75-32768	103.00	1	primal	127.47	143.47	143.10	136.37	157.29	140.45	156.45	177.01	149.36	170.28
Frodo-0976-2.30-65536	150.00	3	dual	222.34	232.10	241.61	228.74	246.43	240.62	252.23	289.77	245.92	266.68
Frodo-0976-2.30-65536	150.00	3	primal	187.36	203.36	210.33	196.82	217.70	206.44	222.44	260.18	215.91	236.79

Scheme	Claim	NIST	Attack	Q-Core-Sieve	Q-Core-Sieve + O(1)	Q-Core-Sieve (min space)	Q-β-Sieve	Q-8d-Sieve + O(1)	Core-Sieve	Core-Sieve + O(1)	Core-Sieve (min space)	β-Sieve	8d-Sieve + O(1)
HILA5-1024-2.83-12289	128.00	5	dual	305.55	321.55	343.02	315.72	336.11	336.68	347.94	408.11	346.85	355.55
HILA5-1024-2.83-12289	128.00	5	primal	256.52	272.52	287.98	266.44	286.96	282.66	298.66	356.22	292.57	313.09
KINDI-0768-2.35-16384	164.00	2	dual	201.79	214.26	221.74	211.06	227.70	217.70	233.65	266.83	227.19	243.80
KINDI-0768-2.35-16384	164.00	2	primal	169.60	185.60	190.40	178.92	199.64	186.88	202.88	235.52	196.20	216.92
KINDI-1024-1.12-8192	207.00	4	dual	256.83	272.83	283.82	266.75	283.24	282.99	291.80	338.93	287.08	304.66
KINDI-1024-1.12-8192	207.00	4	primal	220.22	236.22	247.22	229.91	250.56	242.65	258.65	305.81	252.35	273.00
KINDI-1024-2.29-16384	232.00	4	dual	278.71	291.32	306.83	285.96	305.83	301.17	316.14	368.35	312.70	326.94
KINDI-1024-2.29-16384	232.00	4	primal	237.71	253.71	266.86	247.51	268.12	261.92	277.92	330.10	271.73	292.34
KINDI-1280-1.12-16384	251.00	5	dual	308.21	319.38	339.17	313.59	328.71	332.90	346.58	403.21	343.05	359.53
KINDI-1280-1.12-16384	251.00	5	primal	263.68	279.68	296.01	273.63	294.32	290.54	306.54	366.16	300.50	321.19
KINDI-1536-1.12-8192	330.00	5	dual	407.04	420.92	448.04	415.50	432.66	446.77	453.72	539.49	448.80	468.67
KINDI-1536-1.12-8192	330.00	5	primal	351.92	367.92	395.08	362.30	382.83	387.78	403.78	488.70	398.15	418.69
LAC-0512-0.71-251	128.00	1, 2	dual	177.29	189.05	194.27	182.83	198.34	190.68	202.02	230.77	196.28	212.10
LAC-0512-0.71-251	128.00	1, 2	primal	135.15	151.15	151.72	144.14	164.35	148.92	164.92	187.68	157.91	178.12
LAC-1024-0.50-251	192.00	3, 4	dual	326.48	342.48	353.45	336.75	347.61	348.14	362.90	421.73	357.11	377.09
LAC-1024-0.50-251	192.00	3, 4	primal	261.03	277.03	293.04	270.97	291.10	287.62	303.62	362.48	297.56	317.70
LAC-1024-0.71-251	256.00	5	dual	363.05	379.05	407.57	373.47	393.32	400.04	413.93	483.55	410.46	415.44
LAC-1024-0.71-251	256.00	5	primal	292.82	308.82	328.74	302.93	322.94	322.66	338.66	406.64	332.77	352.78
LIMA-2p-1024-3.16-133121	208.80	3	dual	227.42	243.37	251.21	237.11	257.93	248.15	262.45	301.96	256.17	277.00
LIMA-2p-1024-3.16-133121	208.80	3	primal	195.84	211.84	219.85	205.36	226.31	215.79	231.79	271.95	225.32	246.26
LIMA-2p-2048-3.16-184321	444.50	4	dual	494.23	510.22	546.80	505.09	525.74	536.70	552.70	665.46	547.54	568.20
LIMA-2p-2048-3.16-184321	444.50	4	primal	428.77	444.77	481.35	439.43	460.18	472.46	488.46	595.42	483.12	503.86
LIMA-sp-1018-3.16-12521473	139.20	1	dual	140.99	156.25	156.19	150.04	168.60	153.31	169.30	189.15	162.34	180.62
LIMA-sp-1018-3.16-12521473	139.20	1	primal	123.23	139.23	138.34	132.09	153.65	135.78	151.78	171.12	144.64	166.20
LIMA-sp-1306-3.16-48181249	167.80	2	dual	170.40	186.40	191.29	179.72	198.52	187.76	199.77	231.10	197.08	214.24
LIMA-sp-1306-3.16-48181249	167.80	2	primal	151.84	167.84	170.47	161.01	182.65	167.32	183.32	210.86	176.48	198.12
LIMA-sp-1822-3.16-44802049	247.90	3	dual	259.18	270.93	286.20	264.87	286.26	280.90	296.90	348.13	290.81	312.24
LIMA-sp-1822-3.16-44802049	247.90	3	primal	231.88	247.88	260.31	241.65	263.14	255.50	271.50	322.00	265.27	286.77
LIMA-sp-2062-3.16-16900097	303.50	4	dual	321.87	335.86	359.51	330.10	351.36	359.44	364.69	439.39	360.18	380.15
LIMA-sp-2062-3.16-16900097	303.50	4	primal	290.71	306.71	326.36	300.80	322.14	320.32	336.32	403.70	330.42	351.76
LOTUS-0576-3.00-8192	128.00	1, 2	dual	175.43	187.20	190.40	181.13	198.97	188.45	202.59	229.63	195.91	212.23
LOTUS-0576-3.00-8192	128.00	1, 2	primal	140.98	156.98	158.27	150.04	170.64	155.34	171.34	195.78	164.40	185.00
LOTUS-0704-3.00-8192	192.00	3, 4	dual	220.41	230.92	241.27	224.65	244.98	236.81	251.38	286.30	246.48	260.45
LOTUS-0704-3.00-8192	192.00	3, 4	primal	178.61	194.61	200.51	188.01	208.53	196.81	212.81	248.03	206.20	226.73
LOTUS-0832-3.00-8192	256.00	5	dual	265.53	273.58	287.98	271.13	287.60	282.66	298.66	342.75	292.57	312.94
LOTUS-0832-3.00-8192	256.00	5	primal	217.04	233.04	243.65	226.71	247.22	239.15	255.15	301.39	248.83	269.34

Scheme	Claim	NIST	Attack	Q-Core-Sieve	Q-Core-Sieve + O(1)	Q-Core-Sieve (min space)	Q-β-Sieve	Q-8d-Sieve + O(1)	Core-Sieve	Core-Sieve + O(1)	Core-Sieve (min space)	β-Sieve	8d-Sieve + O(1)
LightSaber-0512-2.31-8192	115.00	1	dual	141.32	154.37	154.86	149.40	165.32	152.55	165.49	185.17	161.45	177.79
LightSaber-0512-2.31-8192	115.00	1	primal	113.16	129.16	127.03	121.89	142.64	124.68	140.68	157.14	133.42	154.17
Lizard-0536-1.15-2048	130.00	1	dual	126.77	140.05	137.87	133.52	149.70	136.12	148.36	161.63	143.05	158.89
Lizard-0536-1.15-2048	130.00	1	primal	104.94	120.94	117.81	113.57	134.18	115.63	131.63	145.73	124.26	144.87
Lizard-0663-1.15-1024	147.00	1	dual	170.40	183.11	185.36	176.42	192.07	183.50	196.15	219.35	189.01	204.99
Lizard-0663-1.15-1024	147.00	1	primal	144.47	160.47	162.15	153.56	173.94	159.16	175.16	200.14	168.24	188.63
Lizard-0816-1.15-2048	195.00	3	dual	202.06	214.84	221.26	208.68	225.37	218.05	229.45	261.25	224.87	242.49
Lizard-0816-1.15-2048	195.00	3	primal	172.52	188.52	193.67	181.86	202.32	190.09	206.09	239.31	199.44	219.90
Lizard-0952-1.15-2048	195.00	3	dual	235.55	247.27	255.48	241.25	257.54	252.00	267.87	301.77	263.54	277.21
Lizard-0952-1.15-2048	195.00	3	primal	203.33	219.33	228.23	212.91	233.34	224.01	240.01	282.17	233.59	254.02
Lizard-1088-1.15-4096	257.00	5	dual	247.15	258.04	265.02	253.72	268.16	263.52	281.43	317.48	270.07	290.39
Lizard-1088-1.15-4096	257.00	5	primal	217.04	233.04	243.64	226.71	247.23	239.15	255.15	301.09	248.82	269.35
Lizard-1300-1.15-2048	291.00	5	dual	312.75	322.93	341.41	319.32	336.43	337.90	347.86	398.55	344.12	375.42
Lizard-1300-1.15-2048	291.00	5	primal	282.40	298.40	316.56	292.45	312.82	311.06	327.06	380.46	321.11	341.47
MamaBear-0936-0.71-1024	219.00	4	dual	272.02	280.74	297.20	274.91	294.93	291.71	307.71	351.44	301.67	316.12
MamaBear-0936-0.71-1024	219.00	4	primal	219.95	235.95	246.92	229.65	250.03	242.36	258.36	305.44	252.06	272.44
MamaBear-0936-0.94-1024	237.00	5	dual	293.09	309.09	326.66	303.20	320.13	320.62	330.59	386.03	330.52	340.34
MamaBear-0936-0.94-1024	237.00	5	primal	238.77	254.77	268.05	248.58	268.88	263.09	279.09	331.57	272.91	293.21
NewHope-0512-2.00-12289	101.00	1	dual	127.76	141.08	139.52	134.30	152.28	137.86	150.61	167.21	145.53	162.56
NewHope-0512-2.00-12289	101.00	1	primal	102.29	118.29	114.83	110.88	131.71	112.71	128.71	142.05	121.30	142.13
NewHope-1024-2.00-12289	233.00	5	dual	282.49	294.26	308.81	292.55	303.72	303.10	319.10	373.52	313.12	333.60
NewHope-1024-2.00-12289	233.00	5	primal	234.79	250.79	263.58	244.58	265.19	258.71	274.71	326.05	268.50	289.11
PapaBear-1248-0.61-1024	292.00	5	dual	349.35	365.27	387.94	359.63	379.83	380.77	396.77	461.84	391.12	411.32
PapaBear-1248-0.61-1024	292.00	5	primal	292.56	308.56	328.44	302.67	322.99	322.37	338.37	406.27	332.48	352.80
PapaBear-1248-0.87-1024	320.00	5	dual	389.02	405.02	436.73	399.54	419.64	428.66	444.66	524.40	439.18	455.62
PapaBear-1248-0.87-1024	320.00	5	primal	323.04	339.04	362.65	333.29	353.52	355.95	371.95	448.59	366.20	386.43
R EMBLEM-0512-25.00-65536	128.00	1	dual	126.02	137.79	136.86	133.17	148.95	135.27	147.79	162.66	142.88	158.54
R EMBLEM-0512-25.00-65536	128.00	1	primal	101.50	117.50	113.94	110.08	130.79	111.84	127.84	140.94	120.42	141.13
R EMBLEM-0512-3.00-16384	128.00	1	dual	112.79	125.21	123.57	119.58	136.47	121.49	133.51	145.16	128.15	144.57
R EMBLEM-0512-3.00-16384	128.00	1	primal	91.43	107.43	102.64	99.86	120.71	100.74	116.74	126.96	109.17	130.03
RLizard-1024-1.15-1024	147.00	1	dual	252.78	261.32	267.31	258.64	279.56	274.20	282.40	313.81	279.22	289.24
RLizard-1024-1.15-1024	147.00	1	primal	224.64	240.64	246.71	234.13	254.47	243.31	259.31	288.00	252.64	272.98
RLizard-1024-1.15-2048	195.00	3	dual	262.08	275.40	286.80	270.54	285.80	282.51	299.24	341.15	290.99	304.70
RLizard-1024-1.15-2048	195.00	3	primal	224.99	240.99	252.58	234.71	255.10	247.91	263.91	312.43	257.64	278.03
RLizard-2048-1.15-2048	291.00	3	dual	399.96	415.21	449.50	409.14	431.98	444.59	454.39	568.12	448.20	444.83
RLizard-2048-1.15-2048	291.00	3	primal	388.47	404.47	416.49	398.33	418.73	412.12	428.12	468.09	421.62	442.05

Scheme	Claim	NIST	Attack	Q-Core-Sieve	Q-Core-Sieve + O(1)	Q-Core-Sieve (min space)	Q-β-Sieve	Q-8d-Sieve + O(1)	Core-Sieve	Core-Sieve + O(1)	Core-Sieve (min space)	β-Sieve	8d-Sieve + O(1)
RLizard-2048-1.15-4096	348.00	5	dual	484.17	484.97	501.54	484.35	491.60	496.38	506.08	564.94	501.69	512.71
RLizard-2048-1.15-4096	348.00	5	primal	429.40	445.40	473.46	439.88	460.28	466.23	482.23	554.65	476.59	497.02
Saber-0768-2.31-8192	180.00	3	dual	223.74	236.22	247.22	229.93	250.36	242.65	257.02	294.77	252.35	266.07
Saber-0768-2.31-8192	180.00	3	primal	184.18	200.18	206.76	193.62	214.19	202.94	218.94	255.76	212.38	232.95
Titanium.KEM-1024-1.41-118273	128.00	1	dual	194.00	209.45	216.85	202.96	223.92	213.16	227.40	259.81	222.67	238.07
Titanium.KEM-1024-1.41-118273	128.00	1	primal	167.22	183.22	187.72	176.52	197.57	184.25	200.25	232.21	193.55	214.60
Titanium.KEM-1280-1.41-430081	160.00	1	dual	221.28	237.28	244.55	230.98	252.05	243.82	259.53	298.08	253.53	267.87
Titanium.KEM-1280-1.41-430081	160.00	1	primal	193.72	209.72	217.47	203.23	224.39	213.45	229.45	269.01	222.97	244.12
Titanium.KEM-1536-1.41-783361	192.00	3	dual	261.56	277.56	288.57	271.50	292.59	288.41	296.04	352.91	290.36	311.05
Titanium.KEM-1536-1.41-783361	192.00	3	primal	229.76	245.76	257.93	239.51	260.68	253.16	269.16	319.06	262.92	284.09
Titanium.KEM-2048-1.41-1198081	256.00	5	dual	348.44	364.21	390.91	358.57	379.63	383.69	399.69	484.29	394.05	415.11
Titanium.KEM-2048-1.41-1198081	256.00	5	primal	313.50	329.50	351.94	323.70	344.83	345.44	361.44	435.34	355.64	376.77
Titanium.PKE-1024-1.41-86017	128.00	1	dual	201.67	217.67	222.26	211.24	228.68	218.57	234.12	270.48	227.67	248.59
Titanium.PKE-1024-1.41-86017	128.00	1	primal	172.78	188.78	193.97	182.13	203.15	190.38	206.38	239.94	199.73	220.76
Titanium.PKE-1280-1.41-301057	160.00	1	dual	230.29	246.29	254.36	240.05	259.89	249.66	265.66	310.22	259.40	280.43
Titanium.PKE-1280-1.41-301057	160.00	1	primal	200.61	216.61	225.21	210.17	231.27	221.04	237.04	278.58	230.61	251.71
Titanium.PKE-1536-1.41-737281	192.00	3	dual	263.15	279.15	288.87	273.10	294.18	283.53	299.53	355.12	293.46	314.55
Titanium.PKE-1536-1.41-737281	192.00	3	primal	230.81	246.81	259.12	240.58	261.75	254.33	270.33	320.53	264.10	285.27
Titanium.PKE-2048-1.41-1198081	256.00	5	dual	348.44	364.21	390.91	358.57	379.63	383.69	399.69	484.29	394.05	415.11
Titanium.PKE-2048-1.41-1198081	256.00	5	primal	313.50	329.50	351.94	323.70	344.83	345.44	361.44	435.34	355.64	376.77
nRound2.KEM-0400-3.62-3209	74.00	1	dual	95.21	106.36	102.87	100.88	116.12	101.12	112.59	116.20	106.67	121.83
nRound2.KEM-0400-3.62-3209	74.00	1	primal	78.17	94.17	87.76	86.38	106.96	86.14	102.14	108.45	94.34	114.92
nRound2.KEM-0486-2.20-1949	97.00	2	dual	120.29	132.02	130.67	126.89	142.56	128.52	142.48	152.64	134.87	150.45
nRound2.KEM-0486-2.20-1949	97.00	2	primal	100.17	116.17	112.45	108.73	129.22	110.38	126.38	138.95	118.94	139.43
nRound2.KEM-0556-3.77-3343	106.00	3	dual	133.81	147.56	147.34	140.64	156.78	142.27	156.42	163.74	149.98	163.08
nRound2.KEM-0556-3.77-3343	106.00	3	primal	115.16	131.16	128.99	123.90	144.38	126.68	142.68	155.96	135.39	155.90
nRound2.KEM-0658-1.49-1319	139.00	4, 5	dual	169.81	180.94	184.98	176.06	191.99	180.91	193.38	213.74	188.90	204.64
nRound2.KEM-0658-1.49-1319	139.00	4, 5	primal	143.63	159.63	161.25	152.71	173.11	158.26	174.26	199.21	167.35	187.75
nRound2.PKE-0442-1.50-2659	74.00	1	dual	94.49	105.70	101.91	100.13	115.74	100.37	112.07	117.51	108.00	122.06
nRound2.PKE-0442-1.50-2659	74.00	1	primal	79.23	95.23	88.95	87.46	108.18	87.31	103.31	109.40	95.53	116.25
nRound2.PKE-0556-1.88-3343	97.00	2	dual	120.72	132.69	132.49	127.37	143.74	128.96	141.85	150.21	135.05	151.19
nRound2.PKE-0556-1.88-3343	97.00	2	primal	104.66	120.66	117.46	113.28	133.93	115.30	131.30	143.33	123.92	144.57
nRound2.PKE-0576-1.30-2309	106.00	3	dual	130.99	142.61	141.61	137.04	152.96	141.03	151.66	166.03	146.50	163.23
nRound2.PKE-0576-1.30-2309	106.00	3	primal	111.04	127.04	124.65	119.75	140.35	122.35	138.35	154.12	131.06	151.67
nRound2.PKE-0708-1.60-2837	138.00	4, 5	dual	166.29	179.10	181.18	174.21	190.74	179.28	192.12	212.36	188.90	206.16
nRound2.PKE-0708-1.60-2837	138.00	4, 5	primal	143.10	159.10	160.65	152.18	172.72	157.68	173.68	198.47	166.76	187.30

Scheme	Claim	NIST	Attack	Q-Core-Sieve	Q-Core-Sieve + O(1)	Q-Core-Sieve (min space)	Q-β-Sieve	Q-8d-Sieve + O(1)	Core-Sieve	Core-Sieve + O(1)	Core-Sieve (min space)	β-Sieve	8d-Sieve + O(1)
qTESLA-1024-8.49-8058881	128.00	1	dual	178.08	189.84	195.16	183.26	204.48	191.55	207.55	237.73	200.91	217.69
qTESLA-1024-8.49-8058881	128.00	1	primal	153.44	169.44	172.25	162.61	183.98	169.07	185.07	213.07	178.25	199.62
qTESLA-2048-8.49-12681217	192.00	3	dual	380.49	396.28	426.91	390.76	411.86	419.02	435.02	531.39	429.51	450.60
qTESLA-2048-8.49-12681217	192.00	3	primal	343.97	359.97	386.15	354.31	375.48	379.02	395.02	477.66	389.36	410.52
qTESLA-2048-8.49-27627521	256.00	5	dual	367.03	375.76	395.97	375.75	384.29	388.65	404.65	489.81	399.03	420.23
qTESLA-2048-8.49-27627521	256.00	5	primal	321.98	337.98	361.46	332.22	353.49	354.78	370.78	447.12	365.03	386.29
uRound2.KEM-0418-4.62-4096	75.00	1	dual	97.66	107.69	103.65	102.63	117.94	103.14	115.47	118.15	108.95	125.39
uRound2.KEM-0418-4.62-4096	75.00	1	primal	81.53	97.53	91.34	89.77	110.36	89.68	105.68	110.74	97.92	118.51
uRound2.KEM-0500-2.31-16384	74.00	1	dual	87.86	99.60	94.79	93.84	109.62	93.76	105.14	108.53	99.58	115.94
uRound2.KEM-0500-2.31-16384	74.00	1	primal	76.02	92.02	85.63	84.18	105.17	83.74	99.74	104.77	92.22	112.89
uRound2.KEM-0522-36.95-32768	97.00	2	dual	121.94	133.70	131.66	128.17	145.68	132.02	142.95	150.73	138.58	154.08
uRound2.KEM-0522-36.95-32768	97.00	2	primal	106.14	122.14	119.04	114.77	135.27	116.86	132.86	142.23	125.49	145.99
uRound2.KEM-0540-18.48-16384	106.00	3	dual	133.26	143.95	143.54	140.25	154.39	141.49	153.85	164.39	148.02	163.72
uRound2.KEM-0540-18.48-16384	106.00	3	primal	112.62	128.62	126.38	121.36	141.84	124.07	140.07	155.20	132.78	153.25
uRound2.KEM-0580-4.62-32768	96.00	2	dual	110.43	122.80	119.95	117.02	133.56	118.58	131.46	141.55	125.26	142.05
uRound2.KEM-0580-4.62-32768	96.00	2	primal	94.08	110.08	105.61	102.55	123.48	103.66	119.66	130.64	112.13	133.06
uRound2.KEM-0630-4.62-32768	106.00	3	dual	121.40	134.98	132.71	128.31	145.76	130.72	143.52	157.29	137.76	156.38
uRound2.KEM-0630-4.62-32768	106.00	3	primal	104.41	120.41	117.21	113.03	133.92	115.05	131.05	144.99	123.67	144.56
uRound2.KEM-0676-36.95-32768	139.00	5	dual	169.93	182.18	184.51	177.79	192.78	181.74	194.68	212.11	189.72	204.47
uRound2.KEM-0676-36.95-32768	139.00	5	primal	146.55	162.55	164.50	155.66	176.05	161.47	177.47	201.99	170.57	190.98
uRound2.KEM-0700-36.95-32768	140.00	4	dual	174.26	184.94	186.48	180.33	195.01	190.83	200.16	215.37	190.52	206.63
uRound2.KEM-0700-36.95-32768	140.00	4	primal	151.04	167.04	169.59	160.19	180.59	166.55	182.55	204.82	175.66	196.05
uRound2.KEM-0786-4.62-32768	138.00	5	dual	156.80	169.83	171.44	164.92	181.98	169.28	182.89	202.47	179.16	193.08
uRound2.KEM-0786-4.62-32768	138.00	5	primal	137.27	153.27	154.10	146.29	167.06	151.26	167.26	190.58	160.27	181.04
uRound2.KEM-0786-4.62-32768	139.00	4	dual	156.80	169.83	171.44	164.92	181.98	169.28	182.89	202.47	179.16	193.08
uRound2.KEM-0786-4.62-32768	139.00	4	primal	137.27	153.27	154.10	146.29	167.06	151.26	167.26	190.58	160.27	181.04
uRound2.PKE-0420-1.15-1024	74.00	1	dual	95.99	107.18	102.23	101.38	116.33	101.12	112.53	115.14	106.72	121.70
uRound2.PKE-0420-1.15-1024	74.00	1	primal	81.25	97.25	90.97	89.50	110.08	89.45	105.45	110.29	97.57	118.19
uRound2.PKE-0500-4.62-32768	74.00	1	dual	88.03	99.61	94.53	94.08	110.06	94.07	106.28	110.98	99.59	116.29
uRound2.PKE-0500-4.62-32768	74.00	1	primal	76.02	92.02	85.63	84.18	105.17	83.74	99.74	104.77	92.22	112.89
uRound2.PKE-0540-4.62-8192	97.00	2	dual	119.74	131.65	130.37	128.22	144.18	129.24	140.27	149.64	134.63	150.09
uRound2.PKE-0540-4.62-8192	97.00	2	primal	102.29	118.29	114.78	110.88	131.50	112.68	128.68	141.58	121.25	141.91
uRound2.PKE-0585-4.62-32768	96.00	2	dual	110.29	122.84	120.95	117.13	133.11	118.31	131.05	140.37	124.99	141.63
uRound2.PKE-0585-4.62-32768	96.00	2	primal	94.87	110.87	106.50	103.35	124.24	104.54	120.54	131.74	113.02	133.90
uRound2.PKE-0586-4.62-8192	107.00	3	dual	131.31	143.85	143.03	138.01	154.58	141.82	153.64	164.74	147.19	163.47
uRound2.PKE-0586-4.62-8192	107.00	3	primal	113.16	129.16	126.92	121.89	142.49	124.62	140.62	156.40	133.33	153.95

Scheme	Claim	NIST	Attack	Q-Core-Sieve	Q-Core-Sieve + O(1)	Q-Core-Sieve (min space)	Q-β-Sieve	Q-8d-Sieve + O(1)	Core-Sieve	Core-Sieve + O(1)	Core-Sieve (min space)	β-Sieve	8d-Sieve + O(1)
uRound2.PKE-0643-4.62-32768	106.00	3	dual	121.69	135.05	133.84	128.73	145.57	132.60	144.07	154.74	137.72	154.87
uRound2.PKE-0643-4.62-32768	106.00	3	primal	106.27	122.27	119.28	114.91	135.77	117.08	133.08	147.46	125.73	146.59
uRound2.PKE-0708-18.48-32768	138.00	4, 5	dual	165.99	178.25	181.37	173.92	189.60	179.08	192.76	211.90	185.18	201.37
uRound2.PKE-0708-18.48-32768	138.00	4, 5	primal	143.37	159.37	160.73	152.38	172.96	157.79	173.79	198.84	166.85	187.40
uRound2.PKE-0835-2.31-32768	138.00	4	dual	155.88	169.12	170.33	162.55	179.73	167.70	182.11	203.40	174.66	192.16
uRound2.PKE-0835-2.31-32768	138.00	4	primal	136.79	152.79	153.53	145.80	166.71	150.70	166.70	189.84	159.71	180.61
uRound2.PKE-0835-2.31-32768	138.00	5	dual	155.88	169.12	170.33	162.55	179.73	167.70	182.11	203.40	174.66	192.16
uRound2.PKE-0835-2.31-32768	138.00	5	primal	136.79	152.79	153.53	145.80	166.71	150.70	166.70	189.84	159.71	180.61

Table 6: Cost of primal and dual attacks against LWE-based schemes assuming $2n$ LWE samples using sieving. The column Scheme indicates each instantiation of a scheme using the format NAME-n-σ-q.

Scheme	Claim	NIST	Attack	Q-Core-Sieve	Q-Core-Sieve + O(1)	Q-Core-Sieve (min space)	Q-β-Sieve	Q-8d-Sieve + O(1)	Core-Sieve	Core-Sieve + O(1)	Core-Sieve (min space)	β-Sieve	8d-Sieve + O(1)
Falcon-0512-4.05-12289	103.00	1	primal	127.73	143.73	143.39	136.64	157.13	140.74	156.74	177.38	149.66	170.14
Falcon-0768-4.05-18433	172.00	2, 3	primal	192.92	208.92	216.58	202.43	222.90	212.58	228.58	267.90	222.08	242.56
Falcon-1024-2.87-12289	230.00	4, 5	primal	258.38	274.38	290.06	268.30	288.77	284.70	300.70	358.80	294.63	315.10
NTRU HRSS-0700-0.79-8192	123.00	1	primal	122.70	138.70	137.74	131.55	152.42	135.20	151.20	170.38	144.05	164.92
NTRU Prime-0761-0.82-4591	225.00	5	primal	138.86	154.86	155.89	147.89	168.61	153.01	169.01	191.49	162.04	182.76
NTRU Prime-0761-0.82-4591	248.00	5	primal	139.94	155.94	157.10	148.99	169.72	154.20	170.20	194.33	163.24	183.97
NTRUEncrypt-0443-0.80-2048	84.00	1	primal	84.54	100.54	94.16	92.85	113.60	92.42	108.42	116.44	100.73	122.21
NTRUEncrypt-0743-0.82-2048	159.00	1, 2, 3, 4, 5	primal	158.81	174.81	178.28	168.03	188.60	174.98	190.98	220.51	184.21	204.77
NTRUEncrypt-1024-724.00-1073750017	198.00	4, 5	primal	247.78	263.77	278.16	257.64	278.18	273.02	289.02	344.08	282.89	303.42
pqNTRUsign-1024-0.70-65537	149.00	1, 2, 3, 4, 5	primal	151.85	167.85	170.47	161.01	182.11	167.32	183.32	210.86	176.48	197.58

Table 7: Cost of primal attack against NTRU-based schemes using sieving. The column Scheme indicates each instantiation of a scheme using the format NAME-n-σ-q, where the equivalent LWE values are provided as seen in Section 4.

Scheme	Claim	NIST	Attack	Q-Core-Enum + O(1)	Lotus	Core-Enum + O(1)	8d-Enum + O(1) (quadratic fit)
AKCN-MLWE-0768-1.00-7681	147.00	4	dual	241.06	258.21	424.05	481.69
AKCN-MLWE-0768-1.00-7681	147.00	4	primal	201.88	217.62	403.76	466.57
AKCN-MLWE-0768-2.24-7681	183.00	4	dual	320.17	343.75	553.96	682.10
AKCN-MLWE-0768-2.24-7681	183.00	4	primal	268.80	296.45	537.60	649.17
AKCN-RLWE-1024-2.83-12289	255.00	5	dual	479.61	529.19	829.14	∞
AKCN-RLWE-1024-2.83-12289	255.00	5	primal	415.50	470.87	831.00	1109.81
BabyBear-0624-0.79-1024	141.00	2	dual	256.34	288.30	408.18	472.13
BabyBear-0624-0.79-1024	141.00	2	primal	189.94	203.62	379.88	435.55
BabyBear-0624-1.00-1024	152.00	2	dual	296.43	296.43	441.60	552.22
BabyBear-0624-1.00-1024	152.00	2	primal	209.60	226.68	419.20	486.41
CRYSTALS-Dilithium-0768-3.74-8380417	91.00	1	dual	127.65	129.42	220.79	245.00
CRYSTALS-Dilithium-0768-3.74-8380417	91.00	1	primal	105.42	105.47	210.84	235.91
CRYSTALS-Dilithium-1024-3.16-8380417	125.00	2	dual	190.88	201.86	341.76	380.73
CRYSTALS-Dilithium-1024-3.16-8380417	125.00	2	primal	167.47	177.35	334.93	380.29
CRYSTALS-Dilithium-1280-2.00-8380417	158.00	3	dual	243.63	263.11	443.71	506.84
CRYSTALS-Dilithium-1280-2.00-8380417	158.00	3	primal	220.31	239.27	440.62	515.87
CRYSTALS-Kyber-0512-1.58-7681	102.00	1	dual	168.35	168.35	288.35	289.09
CRYSTALS-Kyber-0512-1.58-7681	102.00	1	primal	121.92	124.47	243.84	272.03
CRYSTALS-Kyber-0768-1.41-7681	161.00	3	dual	268.17	298.10	469.21	536.24
CRYSTALS-Kyber-0768-1.41-7681	161.00	3	primal	227.68	247.94	455.36	534.88
CRYSTALS-Kyber-1024-1.22-7681	218.00	5	dual	390.68	428.37	684.96	835.77
CRYSTALS-Kyber-1024-1.22-7681	218.00	5	primal	339.28	380.02	678.55	860.64
Ding Key Exchange-0512-4.19-120883	—	1	dual	153.12	162.42	228.61	249.26
Ding Key Exchange-0512-4.19-120883	—	1	primal	104.59	104.52	209.18	233.52
Ding Key Exchange-1024-2.60-120883	—	3, 5	dual	319.54	349.27	578.68	672.45
Ding Key Exchange-1024-2.60-120883	—	3, 5	primal	280.06	309.77	560.12	682.05
EMBLEM-0611-25.00-16777216	128.30	1	dual	90.54	89.10	151.04	168.59
EMBLEM-0611-25.00-16777216	128.30	1	primal	70.87	66.09	141.74	162.29
EMBLEM-0770-25.00-16777216	128.30	1	dual	117.58	119.15	206.70	228.32
EMBLEM-0770-25.00-16777216	128.30	1	primal	101.28	100.72	202.51	226.67
FireSaber-1024-2.31-8192	245.00	5	dual	479.61	529.19	829.06	1051.37
FireSaber-1024-2.31-8192	245.00	5	primal	415.50	470.87	831.00	1109.80
Frodo-0640-2.75-32768	103.00	1	dual	206.21	233.75	352.58	389.87
Frodo-0640-2.75-32768	103.00	1	primal	166.08	175.74	332.17	376.23
Frodo-0976-2.30-65536	150.00	3	dual	315.88	352.31	567.32	656.45
Frodo-0976-2.30-65536	150.00	3	primal	274.42	303.09	548.83	665.65

Scheme	Claim	NIST	Attack	Q-Core-Enum + O(1)	Lotus	Core-Enum + O(1)	8d-Enum + O(1) (quadratic fit)
HILA5-1024-2.83-12289	128.00	5	dual	479.61	529.19	829.14	∞
HILA5-1024-2.83-12289	128.00	5	primal	415.50	470.87	831.00	1109.81
KINDI-0768-2.35-16384	164.00	2	dual	324.34	324.34	489.52	597.34
KINDI-0768-2.35-16384	164.00	2	primal	242.06	264.88	484.12	574.11
KINDI-1024-1.12-8192	207.00	4	dual	377.08	412.76	686.44	874.90
KINDI-1024-1.12-8192	207.00	4	primal	339.28	380.02	678.55	860.31
KINDI-1024-2.29-16384	232.00	4	dual	419.65	468.93	738.85	915.33
KINDI-1024-2.29-16384	232.00	4	primal	375.39	423.01	750.78	976.09
KINDI-1280-1.12-16384	251.00	5	dual	471.25	518.64	838.78	1067.04
KINDI-1280-1.12-16384	251.00	5	primal	428.85	486.82	857.71	1155.86
KINDI-1536-1.12-8192	330.00	5	dual	672.59	760.63	1191.80	1779.81
KINDI-1536-1.12-8192	330.00	5	primal	621.48	717.98	1242.96	1881.63
LAC-0512-0.71-251	128.00	1, 2	dual	271.67	287.97	422.51	486.45
LAC-0512-0.71-251	128.00	1, 2	primal	177.69	189.29	355.38	404.37
LAC-1024-0.50-251	192.00	3, 4	dual	505.20	553.17	851.02	1296.25
LAC-1024-0.50-251	192.00	3, 4	primal	423.28	480.16	846.56	1136.10
LAC-1024-0.71-251	256.00	5	dual	564.65	681.33	969.53	∞
LAC-1024-0.71-251	256.00	5	primal	491.03	561.24	982.06	1376.78
LIMA-2p-1024-3.16-133121	208.80	3	dual	339.28	365.49	608.83	712.21
LIMA-2p-1024-3.16-133121	208.80	3	primal	293.48	325.67	586.97	721.37
LIMA-2p-2048-3.16-184321	444.50	4	dual	860.12	986.23	∞	∞
LIMA-2p-2048-3.16-184321	444.50	4	primal	799.23	932.53	1598.46	2664.36
LIMA-sp-1018-3.16-12521473	139.20	1	dual	184.74	192.58	330.32	370.17
LIMA-sp-1018-3.16-12521473	139.20	1	primal	158.29	166.65	316.58	357.96
LIMA-sp-1306-3.16-48181249	167.80	2	dual	234.89	256.09	435.74	487.58
LIMA-sp-1306-3.16-48181249	167.80	2	primal	208.15	224.97	416.29	483.76
LIMA-sp-1822-3.16-44802049	247.90	3	dual	402.23	444.80	749.69	936.51
LIMA-sp-1822-3.16-44802049	247.90	3	primal	363.99	409.43	727.99	939.98
LIMA-sp-2062-3.16-16900097	303.50	4	dual	532.54	611.03	1001.55	∞
LIMA-sp-2062-3.16-16900097	303.50	4	primal	487.03	556.44	974.05	1363.41
LOTUS-0576-3.00-8192	128.00	1, 2	dual	264.88	296.88	416.88	472.88
LOTUS-0576-3.00-8192	128.00	1, 2	primal	190.42	204.18	380.83	436.79
LOTUS-0704-3.00-8192	192.00	3, 4	dual	312.27	336.67	553.75	673.75
LOTUS-0704-3.00-8192	192.00	3, 4	primal	260.16	286.24	520.32	624.50
LOTUS-0832-3.00-8192	256.00	5	dual	399.47	428.85	681.75	812.65
LOTUS-0832-3.00-8192	256.00	5	primal	335.54	375.58	671.09	848.75

Scheme	Claim	NIST	Attack	Q-Core-Enum + O(1)	Lotus	Core-Enum + O(1)	8d-Enum + O(1) (quadratic fit)
LightSaber-0512-2.31-8192	115.00	1	dual	182.42	224.02	303.87	333.16
LightSaber-0512-2.31-8192	115.00	1	primal	140.73	146.24	281.45	315.27
Lizard-0536-1.15-2048	130.00	1	dual	148.57	151.80	226.62	244.79
Lizard-0536-1.15-2048	130.00	1	primal	126.24	129.33	228.83	249.07
Lizard-0663-1.15-1024	147.00	1	dual	205.70	211.34	307.47	300.49
Lizard-0663-1.15-1024	147.00	1	primal	186.54	191.49	285.69	305.57
Lizard-0816-1.15-2048	195.00	3	dual	268.05	288.58	398.49	424.72
Lizard-0816-1.15-2048	195.00	3	primal	244.76	262.55	406.58	432.04
Lizard-0952-1.15-2048	195.00	3	dual	316.59	332.72	487.97	467.37
Lizard-0952-1.15-2048	195.00	3	primal	295.19	313.15	456.53	482.97
Lizard-1088-1.15-4096	257.00	5	dual	332.69	364.21	513.73	475.56
Lizard-1088-1.15-4096	257.00	5	primal	312.56	329.07	468.25	493.20
Lizard-1300-1.15-2048	291.00	5	dual	478.92	532.09	586.36	641.04
Lizard-1300-1.15-2048	291.00	5	primal	394.16	411.77	555.87	581.56
MamaBear-0936-0.71-1024	219.00	4	dual	403.33	431.48	690.31	822.40
MamaBear-0936-0.71-1024	219.00	4	primal	338.74	379.39	677.48	858.71
MamaBear-0936-0.94-1024	237.00	5	dual	435.56	482.82	773.70	993.76
MamaBear-0936-0.94-1024	237.00	5	primal	377.02	424.95	754.04	981.13
NewHope-0512-2.00-12289	101.00	1	dual	168.50	168.50	288.50	289.18
NewHope-0512-2.00-12289	101.00	1	primal	121.92	124.47	243.84	272.04
NewHope-1024-2.00-12289	233.00	5	dual	428.50	474.85	754.04	935.68
NewHope-1024-2.00-12289	233.00	5	primal	368.87	415.24	737.74	954.90
PapaBear-1248-0.61-1024	292.00	5	dual	566.99	631.31	993.77	1290.70
PapaBear-1248-0.61-1024	292.00	5	primal	490.46	560.55	980.91	1374.99
PapaBear-1248-0.87-1024	320.00	5	dual	638.23	709.36	1133.99	1578.83
PapaBear-1248-0.87-1024	320.00	5	primal	557.03	640.45	1114.05	1626.67
R EMBLEM-0512-25.00-65536	128.00	1	dual	151.03	154.42	254.21	274.55
R EMBLEM-0512-25.00-65536	128.00	1	primal	120.63	122.98	241.26	269.03
R EMBLEM-0512-3.00-16384	128.00	1	dual	131.30	132.92	219.67	238.22
R EMBLEM-0512-3.00-16384	128.00	1	primal	104.59	104.52	209.18	233.41
RLizard-1024-1.15-1024	147.00	1	dual	350.19	329.70	384.11	385.50
RLizard-1024-1.15-1024	147.00	1	primal	273.84	277.84	372.83	392.51
RLizard-1024-1.15-2048	195.00	3	dual	367.61	406.65	578.61	618.07
RLizard-1024-1.15-2048	195.00	3	primal	347.28	379.02	571.27	610.15
RLizard-2048-1.15-2048	291.00	3	dual	477.39	494.44	1053.46	604.06
RLizard-2048-1.15-2048	291.00	3	primal	466.34	476.50	593.51	616.69

Scheme	Claim	NIST	Attack	Q-Core-Enum + O(1)	Lotus	Core-Enum + O(1)	8d-Enum + O(1) (quadratic fit)
RLizard-2048-1.15-4096	348.00	5	dual	611.18	761.27	1358.03	1428.63
RLizard-2048-1.15-4096	348.00	5	primal	594.93	623.67	803.56	838.54
Saber-0768-2.31-8192	180.00	3	dual	320.17	343.75	553.96	682.12
Saber-0768-2.31-8192	180.00	3	primal	268.80	296.45	537.60	649.17
Titanium.KEM-1024-1.41-118273	128.00	1	dual	275.44	293.44	492.12	564.95
Titanium.KEM-1024-1.41-118273	128.00	1	primal	236.09	257.84	472.18	558.10
Titanium.KEM-1280-1.41-430081	160.00	1	dual	322.81	356.07	595.77	703.41
Titanium.KEM-1280-1.41-430081	160.00	1	primal	286.76	317.70	573.51	701.86
Titanium.KEM-1536-1.41-783361	192.00	3	dual	401.13	440.59	740.99	920.66
Titanium.KEM-1536-1.41-783361	192.00	3	primal	358.59	403.00	717.18	922.35
Titanium.KEM-2048-1.41-1198081	256.00	5	dual	594.12	651.72	∞	∞
Titanium.KEM-2048-1.41-1198081	256.00	5	primal	536.02	615.22	1072.04	1546.52
Titanium.PKE-1024-1.41-86017	128.00	1	dual	281.33	310.38	516.45	593.00
Titanium.PKE-1024-1.41-86017	128.00	1	primal	246.56	270.19	493.12	586.94
Titanium.PKE-1280-1.41-301057	160.00	1	dual	339.81	371.79	606.74	737.10
Titanium.PKE-1280-1.41-301057	160.00	1	primal	300.24	333.68	600.48	741.71
Titanium.PKE-1536-1.41-737281	192.00	3	dual	404.44	444.51	746.42	929.31
Titanium.PKE-1536-1.41-737281	192.00	3	primal	360.75	405.57	721.50	929.28
Titanium.PKE-2048-1.41-1198081	256.00	5	dual	594.12	651.72	∞	∞
Titanium.PKE-2048-1.41-1198081	256.00	5	primal	536.02	615.22	1072.04	1546.52
nRound2.KEM-0400-3.62-3209	74.00	1	dual	101.77	99.81	141.46	153.88
nRound2.KEM-0400-3.62-3209	74.00	1	primal	83.28	78.14	133.07	151.95
nRound2.KEM-0486-2.20-1949	97.00	2	dual	135.44	136.87	193.26	207.57
nRound2.KEM-0486-2.20-1949	97.00	2	primal	117.17	115.97	186.87	205.83
nRound2.KEM-0556-3.77-3343	106.00	3	dual	149.94	153.79	206.52	211.84
nRound2.KEM-0556-3.77-3343	106.00	3	primal	132.79	129.97	195.56	214.48
nRound2.KEM-0658-1.49-1319	139.00	4, 5	dual	205.01	213.06	288.52	299.22
nRound2.KEM-0658-1.49-1319	139.00	4, 5	primal	186.13	190.66	286.96	306.50
nRound2.PKE-0442-1.50-2659	74.00	1	dual	101.02	98.34	139.20	156.87
nRound2.PKE-0442-1.50-2659	74.00	1	primal	84.83	79.43	133.67	152.70
nRound2.PKE-0556-1.88-3343	97.00	2	dual	135.09	136.32	206.03	199.35
nRound2.PKE-0556-1.88-3343	97.00	2	primal	119.74	116.64	181.00	200.03
nRound2.PKE-0576-1.30-2309	106.00	3	dual	151.98	158.71	221.84	225.59
nRound2.PKE-0576-1.30-2309	106.00	3	primal	134.01	134.92	211.14	230.25
nRound2.PKE-0708-1.60-2837	138.00	4, 5	dual	205.50	209.41	306.30	326.72
nRound2.PKE-0708-1.60-2837	138.00	4, 5	primal	187.11	192.65	293.47	312.67

Scheme	Claim	NIST	Attack	Q-Core-Enum + O(1)	Lotus	Core-Enum + O(1)	8d-Enum + O(1) (quadratic fit)
qTESLA-1024-8.49-8058881	128.00	1	dual	248.57	271.03	448.47	517.42
qTESLA-1024-8.49-8058881	128.00	1	primal	216.40	234.67	432.81	505.17
qTESLA-2048-8.49-12681217	192.00	3	dual	657.48	761.35	∞	∞
qTESLA-2048-8.49-12681217	192.00	3	primal	611.94	706.49	1223.88	1846.24
qTESLA-2048-8.49-27627521	256.00	5	dual	627.45	696.47	∞	∞
qTESLA-2048-8.49-27627521	256.00	5	primal	562.30	646.78	1124.60	1648.15
uRound2.KEM-0418-4.62-4096	75.00	1	dual	101.82	100.00	141.83	147.86
uRound2.KEM-0418-4.62-4096	75.00	1	primal	85.88	80.02	130.42	149.29
uRound2.KEM-0500-2.31-16384	74.00	1	dual	91.73	89.84	129.75	141.39
uRound2.KEM-0500-2.31-16384	74.00	1	primal	79.92	74.16	125.93	145.21
uRound2.KEM-0522-36.95-32768	97.00	2	dual	132.71	132.04	176.79	188.42
uRound2.KEM-0522-36.95-32768	97.00	2	primal	118.13	113.59	172.51	191.40
uRound2.KEM-0540-18.48-16384	106.00	3	dual	155.55	151.66	205.63	236.46
uRound2.KEM-0540-18.48-16384	106.00	3	primal	133.45	131.75	203.36	222.28
uRound2.KEM-0580-4.62-32768	96.00	2	dual	124.42	125.14	188.44	202.38
uRound2.KEM-0580-4.62-32768	96.00	2	primal	108.76	109.30	187.18	206.64
uRound2.KEM-0630-4.62-32768	106.00	3	dual	140.88	144.31	212.03	227.64
uRound2.KEM-0630-4.62-32768	106.00	3	primal	125.37	127.71	212.43	231.90
uRound2.KEM-0676-36.95-32768	139.00	5	dual	211.60	209.36	300.26	294.09
uRound2.KEM-0676-36.95-32768	139.00	5	primal	186.24	188.71	277.63	296.54
uRound2.KEM-0700-36.95-32768	140.00	4	dual	206.17	211.17	278.78	285.17
uRound2.KEM-0700-36.95-32768	140.00	4	primal	186.36	187.83	270.58	289.83
uRound2.KEM-0786-4.62-32768	138.00	5	dual	193.07	199.92	297.25	326.61
uRound2.KEM-0786-4.62-32768	138.00	5	primal	180.36	187.46	293.02	313.97
uRound2.KEM-0786-4.62-32768	139.00	4	dual	193.07	199.92	297.25	326.61
uRound2.KEM-0786-4.62-32768	139.00	4	primal	180.36	187.46	293.02	313.97
uRound2.PKE-0420-1.15-1024	74.00	1	dual	100.36	100.94	132.48	142.62
uRound2.PKE-0420-1.15-1024	74.00	1	primal	84.00	77.59	125.57	144.36
uRound2.PKE-0500-4.62-32768	74.00	1	dual	92.30	89.95	128.00	141.58
uRound2.PKE-0500-4.62-32768	74.00	1	primal	79.92	74.35	125.93	145.22
uRound2.PKE-0540-4.62-8192	97.00	2	dual	134.66	135.11	189.36	200.65
uRound2.PKE-0540-4.62-8192	97.00	2	primal	119.67	117.27	186.28	205.32
uRound2.PKE-0585-4.62-32768	96.00	2	dual	124.34	124.58	182.15	197.92
uRound2.PKE-0585-4.62-32768	96.00	2	primal	109.66	109.14	183.54	202.89
uRound2.PKE-0586-4.62-8192	107.00	3	dual	155.93	152.30	215.32	221.50
uRound2.PKE-0586-4.62-8192	107.00	3	primal	135.60	134.67	209.46	228.54

Scheme	Claim	NIST	Attack	Q-Core-Enum + O(1)	Lotus	Core-Enum + O(1)	8d-Enum + O(1) (quadratic fit)
uRound2.PKE-0643-4.62-32768	106.00	3	dual	139.31	143.11	205.00	217.57
uRound2.PKE-0643-4.62-32768	106.00	3	primal	127.63	127.23	204.35	223.70
uRound2.PKE-0708-18.48-32768	138.00	4, 5	dual	203.96	212.66	295.10	305.24
uRound2.PKE-0708-18.48-32768	138.00	4, 5	primal	187.47	193.07	293.47	312.96
uRound2.PKE-0835-2.31-32768	138.00	4	dual	193.01	199.90	292.30	354.12
uRound2.PKE-0835-2.31-32768	138.00	4	primal	180.16	188.90	297.84	319.20
uRound2.PKE-0835-2.31-32768	138.00	5	dual	193.01	199.90	292.30	354.12
uRound2.PKE-0835-2.31-32768	138.00	5	primal	180.16	188.90	297.84	319.20

Table 8: Cost of primal and dual attacks against LWE-based schemes assuming n LWE samples using enumeration. The column Scheme indicates each instantiation of a scheme using the format NAME-n-σ-q.

Scheme	Claim	NIST	Attack	Q-Core-Enum + O(1)	Lotus	Core-Enum + O(1)	8d-Enum + O(1) (quadratic fit)
AKCN-MLWE-0768-1.00-7681	147.00	4	dual	243.06	258.22	424.05	481.69
AKCN-MLWE-0768-1.00-7681	147.00	4	primal	201.88	217.62	403.76	466.57
AKCN-MLWE-0768-2.24-7681	183.00	4	dual	315.43	344.87	560.12	636.36
AKCN-MLWE-0768-2.24-7681	183.00	4	primal	268.29	295.85	536.58	647.76
AKCN-RLWE-1024-2.83-12289	255.00	5	dual	481.32	522.82	837.69	∞
AKCN-RLWE-1024-2.83-12289	255.00	5	primal	413.84	468.88	827.68	1104.20
BabyBear-0624-0.79-1024	141.00	2	dual	256.34	288.30	408.18	472.13
BabyBear-0624-0.79-1024	141.00	2	primal	189.94	203.62	379.88	435.55
BabyBear-0624-1.00-1024	152.00	2	dual	296.43	296.43	441.60	552.22
BabyBear-0624-1.00-1024	152.00	2	primal	209.60	226.68	419.20	486.41
CRYSTALS-Dilithium-0768-3.74-8380417	91.00	1	dual	123.78	126.20	219.84	240.56
CRYSTALS-Dilithium-0768-3.74-8380417	91.00	1	primal	103.76	103.56	207.52	232.39
CRYSTALS-Dilithium-1024-3.16-8380417	125.00	2	dual	188.54	199.12	341.40	382.42
CRYSTALS-Dilithium-1024-3.16-8380417	125.00	2	primal	166.54	176.28	333.09	378.11
CRYSTALS-Dilithium-1280-2.00-8380417	158.00	3	dual	242.13	264.95	447.56	505.58
CRYSTALS-Dilithium-1280-2.00-8380417	158.00	3	primal	219.82	238.69	439.65	514.60
CRYSTALS-Kyber-0512-1.58-7681	102.00	1	dual	168.72	168.72	264.69	288.86
CRYSTALS-Kyber-0512-1.58-7681	102.00	1	primal	121.92	124.47	243.84	272.03
CRYSTALS-Kyber-0768-1.41-7681	161.00	3	dual	267.86	298.24	471.18	536.24
CRYSTALS-Kyber-0768-1.41-7681	161.00	3	primal	227.68	247.94	455.36	534.88
CRYSTALS-Kyber-1024-1.22-7681	218.00	5	dual	390.68	429.34	684.96	835.77
CRYSTALS-Kyber-1024-1.22-7681	218.00	5	primal	339.28	380.02	678.55	860.64
Ding Key Exchange-0512-4.19-120883	—	1	dual	137.87	137.87	223.40	240.93
Ding Key Exchange-0512-4.19-120883	—	1	primal	101.28	100.72	202.57	226.48
Ding Key Exchange-1024-2.60-120883	—	3, 5	dual	321.23	347.32	574.54	669.53
Ding Key Exchange-1024-2.60-120883	—	3, 5	primal	279.03	308.55	558.06	679.13
EMBLEM-0611-25.00-16777216	128.30	1	dual	89.71	88.80	150.96	167.77
EMBLEM-0611-25.00-16777216	128.30	1	primal	70.49	65.66	140.99	161.57
EMBLEM-0770-25.00-16777216	128.30	1	dual	118.09	120.98	207.52	226.99
EMBLEM-0770-25.00-16777216	128.30	1	primal	101.28	100.72	202.51	226.67
FireSaber-1024-2.31-8192	245.00	5	dual	481.62	521.02	833.48	1043.44
FireSaber-1024-2.31-8192	245.00	5	primal	415.50	470.87	831.00	1109.82
Frodo-0640-2.75-32768	103.00	1	dual	198.53	213.28	346.06	382.45
Frodo-0640-2.75-32768	103.00	1	primal	164.24	173.59	328.48	371.84
Frodo-0976-2.30-65536	150.00	3	dual	317.01	350.04	564.23	670.30
Frodo-0976-2.30-65536	150.00	3	primal	274.42	303.09	548.83	665.67

Scheme	Claim	NIST	Attack	Q-Core-Enum + O(1)	Lotus	Core-Enum + O(1)	8d-Enum + O(1) (quadratic fit)
HILA5-1024-2.83-12289	128.00	5	dual	481.32	522.82	837.69	∞
HILA5-1024-2.83-12289	128.00	5	primal	413.84	468.88	827.68	1104.20
KINDI-0768-2.35-16384	164.00	2	dual	279.94	313.74	480.23	563.20
KINDI-0768-2.35-16384	164.00	2	primal	240.57	263.12	481.13	570.06
KINDI-1024-1.12-8192	207.00	4	dual	377.08	412.76	686.44	874.90
KINDI-1024-1.12-8192	207.00	4	primal	339.28	380.02	678.55	860.31
KINDI-1024-2.29-16384	232.00	4	dual	416.38	463.68	737.77	906.73
KINDI-1024-2.29-16384	232.00	4	primal	374.84	422.36	749.69	974.33
KINDI-1280-1.12-16384	251.00	5	dual	471.25	518.64	838.78	1067.04
KINDI-1280-1.12-16384	251.00	5	primal	428.85	486.82	857.71	1155.86
KINDI-1536-1.12-8192	330.00	5	dual	672.59	760.63	1191.80	1779.81
KINDI-1536-1.12-8192	330.00	5	primal	621.48	717.98	1242.96	1881.63
LAC-0512-0.71-251	128.00	1, 2	dual	271.67	287.97	422.51	486.45
LAC-0512-0.71-251	128.00	1, 2	primal	177.69	189.29	355.38	404.37
LAC-1024-0.50-251	192.00	3, 4	dual	505.20	553.17	851.02	1296.25
LAC-1024-0.50-251	192.00	3, 4	primal	423.28	480.16	846.56	1136.10
LAC-1024-0.71-251	256.00	5	dual	564.65	681.33	969.53	∞
LAC-1024-0.71-251	256.00	5	primal	491.03	561.24	982.06	1376.78
LIMA-2p-1024-3.16-133121	208.80	3	dual	328.26	364.96	601.53	704.69
LIMA-2p-1024-3.16-133121	208.80	3	primal	290.89	322.60	581.78	713.81
LIMA-2p-2048-3.16-184321	444.50	4	dual	854.44	997.06	∞	∞
LIMA-2p-2048-3.16-184321	444.50	4	primal	798.61	931.78	1597.22	2661.47
LIMA-sp-1018-3.16-12521473	139.20	1	dual	180.50	192.58	330.32	365.81
LIMA-sp-1018-3.16-12521473	139.20	1	primal	156.92	165.06	313.84	354.71
LIMA-sp-1306-3.16-48181249	167.80	2	dual	231.63	254.34	430.86	491.47
LIMA-sp-1306-3.16-48181249	167.80	2	primal	207.66	224.41	415.33	482.56
LIMA-sp-1822-3.16-44802049	247.90	3	dual	398.92	447.02	744.25	938.30
LIMA-sp-1822-3.16-44802049	247.90	3	primal	362.91	408.15	725.82	936.55
LIMA-sp-2062-3.16-16900097	303.50	4	dual	528.47	606.16	969.48	∞
LIMA-sp-2062-3.16-16900097	303.50	4	primal	486.45	555.76	972.91	1361.35
LOTUS-0576-3.00-8192	128.00	1, 2	dual	233.49	273.43	397.04	440.57
LOTUS-0576-3.00-8192	128.00	1, 2	primal	188.05	201.40	376.09	430.87
LOTUS-0704-3.00-8192	192.00	3, 4	dual	302.91	336.77	535.56	624.62
LOTUS-0704-3.00-8192	192.00	3, 4	primal	257.63	283.25	515.26	617.43
LOTUS-0832-3.00-8192	256.00	5	dual	389.04	424.30	673.22	810.73
LOTUS-0832-3.00-8192	256.00	5	primal	332.88	372.42	665.77	840.57

Scheme	Claim	NIST	Attack	Q-Core-Enum + O(1)	Lotus	Core-Enum + O(1)	8d-Enum + O(1) (quadratic fit)
LightSaber-0512-2.31-8192	115.00	1	dual	175.84	185.06	301.15	327.82
LightSaber-0512-2.31-8192	115.00	1	primal	139.84	145.21	279.67	313.28
Lizard-0536-1.15-2048	130.00	1	dual	148.57	151.80	226.62	244.79
Lizard-0536-1.15-2048	130.00	1	primal	126.24	129.33	228.83	249.07
Lizard-0663-1.15-1024	147.00	1	dual	205.70	211.34	307.47	300.49
Lizard-0663-1.15-1024	147.00	1	primal	186.54	191.49	285.69	305.57
Lizard-0816-1.15-2048	195.00	3	dual	268.05	288.58	398.49	424.72
Lizard-0816-1.15-2048	195.00	3	primal	244.76	262.55	406.58	432.04
Lizard-0952-1.15-2048	195.00	3	dual	316.59	332.72	487.97	467.37
Lizard-0952-1.15-2048	195.00	3	primal	295.19	313.15	456.53	482.97
Lizard-1088-1.15-4096	257.00	5	dual	332.69	364.21	513.73	475.56
Lizard-1088-1.15-4096	257.00	5	primal	312.56	329.07	468.25	493.20
Lizard-1300-1.15-2048	291.00	5	dual	478.92	532.09	586.36	641.04
Lizard-1300-1.15-2048	291.00	5	primal	394.16	411.77	555.87	581.56
MamaBear-0936-0.71-1024	219.00	4	dual	403.33	431.48	690.31	822.40
MamaBear-0936-0.71-1024	219.00	4	primal	338.74	379.39	677.48	858.71
MamaBear-0936-0.94-1024	237.00	5	dual	435.56	482.82	773.70	993.76
MamaBear-0936-0.94-1024	237.00	5	primal	377.02	424.95	754.04	981.13
NewHope-0512-2.00-12289	101.00	1	dual	160.99	168.97	262.95	288.89
NewHope-0512-2.00-12289	101.00	1	primal	121.92	124.47	243.84	272.06
NewHope-1024-2.00-12289	233.00	5	dual	428.85	476.84	752.95	935.70
NewHope-1024-2.00-12289	233.00	5	primal	368.87	415.24	737.74	954.90
PapaBear-1248-0.61-1024	292.00	5	dual	566.99	631.31	993.77	1290.70
PapaBear-1248-0.61-1024	292.00	5	primal	490.46	560.55	980.91	1374.99
PapaBear-1248-0.87-1024	320.00	5	dual	638.23	709.36	1133.99	1578.83
PapaBear-1248-0.87-1024	320.00	5	primal	557.03	640.45	1114.05	1626.67
R EMBLEM-0512-25.00-65536	128.00	1	dual	150.59	154.46	246.67	264.77
R EMBLEM-0512-25.00-65536	128.00	1	primal	120.63	122.98	241.26	269.03
R EMBLEM-0512-3.00-16384	128.00	1	dual	130.32	134.00	220.88	239.86
R EMBLEM-0512-3.00-16384	128.00	1	primal	104.59	104.52	209.18	233.41
RLizard-1024-1.15-1024	147.00	1	dual	350.19	329.70	384.11	385.50
RLizard-1024-1.15-1024	147.00	1	primal	273.84	277.84	372.83	392.51
RLizard-1024-1.15-2048	195.00	3	dual	367.61	406.65	578.61	618.07
RLizard-1024-1.15-2048	195.00	3	primal	347.28	379.02	571.27	610.15
RLizard-2048-1.15-2048	291.00	3	dual	477.39	494.44	1053.46	604.06
RLizard-2048-1.15-2048	291.00	3	primal	466.34	476.50	593.51	616.69

Scheme	Claim	NIST	Attack	Q-Core-Enum + O(1)	Lotus	Core-Enum + O(1)	8d-Enum + O(1) (quadratic fit)
RLizard-2048-1.15-4096	348.00	5	dual	611.18	761.27	1358.03	1428.63
RLizard-2048-1.15-4096	348.00	5	primal	594.93	623.67	803.56	838.54
Saber-0768-2.31-8192	180.00	3	dual	314.90	344.90	559.09	643.30
Saber-0768-2.31-8192	180.00	3	primal	268.29	295.85	536.58	647.75
Titanium.KEM-1024-1.41-118273	128.00	1	dual	273.90	292.84	492.12	564.95
Titanium.KEM-1024-1.41-118273	128.00	1	primal	236.09	257.84	472.18	558.10
Titanium.KEM-1280-1.41-430081	160.00	1	dual	322.28	359.83	597.36	703.41
Titanium.KEM-1280-1.41-430081	160.00	1	primal	286.76	317.70	573.51	701.86
Titanium.KEM-1536-1.41-783361	192.00	3	dual	404.44	446.48	740.99	920.66
Titanium.KEM-1536-1.41-783361	192.00	3	primal	358.59	403.00	717.18	922.35
Titanium.KEM-2048-1.41-1198081	256.00	5	dual	594.12	651.01	∞	∞
Titanium.KEM-2048-1.41-1198081	256.00	5	primal	536.02	615.22	1072.04	1546.52
Titanium.PKE-1024-1.41-86017	128.00	1	dual	281.60	311.59	517.28	593.00
Titanium.PKE-1024-1.41-86017	128.00	1	primal	246.56	270.19	493.12	586.94
Titanium.PKE-1280-1.41-301057	160.00	1	dual	339.28	371.16	605.72	737.10
Titanium.PKE-1280-1.41-301057	160.00	1	primal	300.24	333.68	600.48	741.71
Titanium.PKE-1536-1.41-737281	192.00	3	dual	405.33	450.42	746.42	929.31
Titanium.PKE-1536-1.41-737281	192.00	3	primal	360.75	405.57	721.50	929.28
Titanium.PKE-2048-1.41-1198081	256.00	5	dual	594.12	651.01	∞	∞
Titanium.PKE-2048-1.41-1198081	256.00	5	primal	536.02	615.22	1072.04	1546.52
nRound2.KEM-0400-3.62-3209	74.00	1	dual	101.35	99.76	141.46	153.88
nRound2.KEM-0400-3.62-3209	74.00	1	primal	83.28	78.14	133.07	151.95
nRound2.KEM-0486-2.20-1949	97.00	2	dual	136.20	136.87	193.26	207.57
nRound2.KEM-0486-2.20-1949	97.00	2	primal	117.17	115.97	186.87	205.83
nRound2.KEM-0556-3.77-3343	106.00	3	dual	154.95	152.64	206.52	211.84
nRound2.KEM-0556-3.77-3343	106.00	3	primal	132.79	129.97	195.56	214.48
nRound2.KEM-0658-1.49-1319	139.00	4, 5	dual	205.01	213.06	288.52	299.22
nRound2.KEM-0658-1.49-1319	139.00	4, 5	primal	186.13	190.66	286.96	306.50
nRound2.PKE-0442-1.50-2659	74.00	1	dual	101.02	98.34	139.20	156.87
nRound2.PKE-0442-1.50-2659	74.00	1	primal	84.83	79.43	133.67	152.70
nRound2.PKE-0556-1.88-3343	97.00	2	dual	135.09	136.32	206.03	199.35
nRound2.PKE-0556-1.88-3343	97.00	2	primal	119.74	116.64	181.00	200.03
nRound2.PKE-0576-1.30-2309	106.00	3	dual	151.98	158.71	221.84	225.59
nRound2.PKE-0576-1.30-2309	106.00	3	primal	134.01	134.92	211.14	230.25
nRound2.PKE-0708-1.60-2837	138.00	4, 5	dual	205.50	209.41	306.30	326.72
nRound2.PKE-0708-1.60-2837	138.00	4, 5	primal	187.11	192.65	293.47	312.67

Scheme	Claim	NIST	Attack	Q-Core-Enum + O(1)	Lotus	Core-Enum + O(1)	8d-Enum + O(1) (quadratic fit)
qTESLA-1024-8.49-8058881	128.00	1	dual	242.06	256.17	435.74	500.19
qTESLA-1024-8.49-8058881	128.00	1	primal	210.57	227.82	421.14	489.92
qTESLA-2048-8.49-12681217	192.00	3	dual	669.56	743.94	∞	∞
qTESLA-2048-8.49-12681217	192.00	3	primal	603.61	696.47	1207.23	1812.57
qTESLA-2048-8.49-27627521	256.00	5	dual	610.75	689.07	∞	∞
qTESLA-2048-8.49-27627521	256.00	5	primal	554.68	637.63	1109.37	1618.59
uRound2.KEM-0418-4.62-4096	75.00	1	dual	101.88	99.95	141.83	147.86
uRound2.KEM-0418-4.62-4096	75.00	1	primal	85.88	80.02	130.42	149.29
uRound2.KEM-0500-2.31-16384	74.00	1	dual	92.43	89.84	129.75	141.39
uRound2.KEM-0500-2.31-16384	74.00	1	primal	79.92	74.16	125.93	145.21
uRound2.KEM-0522-36.95-32768	97.00	2	dual	133.77	134.25	176.79	193.39
uRound2.KEM-0522-36.95-32768	97.00	2	primal	118.13	113.59	172.51	191.40
uRound2.KEM-0540-18.48-16384	106.00	3	dual	150.77	153.51	205.66	224.11
uRound2.KEM-0540-18.48-16384	106.00	3	primal	133.45	131.75	203.36	222.28
uRound2.KEM-0580-4.62-32768	96.00	2	dual	126.18	125.35	188.54	202.38
uRound2.KEM-0580-4.62-32768	96.00	2	primal	108.76	109.30	187.18	206.64
uRound2.KEM-0630-4.62-32768	106.00	3	dual	141.14	142.81	212.03	227.64
uRound2.KEM-0630-4.62-32768	106.00	3	primal	125.37	127.71	212.43	231.90
uRound2.KEM-0676-36.95-32768	139.00	5	dual	203.77	207.39	278.55	351.67
uRound2.KEM-0676-36.95-32768	139.00	5	primal	186.24	188.71	277.63	296.54
uRound2.KEM-0700-36.95-32768	140.00	4	dual	223.31	209.85	325.91	285.17
uRound2.KEM-0700-36.95-32768	140.00	4	primal	186.36	187.83	270.58	289.83
uRound2.KEM-0786-4.62-32768	138.00	5	dual	195.07	204.28	296.54	326.61
uRound2.KEM-0786-4.62-32768	138.00	5	primal	180.36	187.46	293.02	313.97
uRound2.KEM-0786-4.62-32768	139.00	4	dual	195.07	204.28	296.54	326.61
uRound2.KEM-0786-4.62-32768	139.00	4	primal	180.36	187.46	293.02	313.97
uRound2.PKE-0420-1.15-1024	74.00	1	dual	100.36	100.94	132.48	142.62
uRound2.PKE-0420-1.15-1024	74.00	1	primal	84.00	77.59	125.57	144.36
uRound2.PKE-0500-4.62-32768	74.00	1	dual	91.75	90.65	128.00	141.58
uRound2.PKE-0500-4.62-32768	74.00	1	primal	79.92	74.35	125.93	145.22
uRound2.PKE-0540-4.62-8192	97.00	2	dual	134.12	136.04	189.36	200.65
uRound2.PKE-0540-4.62-8192	97.00	2	primal	119.67	117.27	186.28	205.32
uRound2.PKE-0585-4.62-32768	96.00	2	dual	123.79	126.14	190.18	197.92
uRound2.PKE-0585-4.62-32768	96.00	2	primal	109.66	109.14	183.54	202.89
uRound2.PKE-0586-4.62-8192	107.00	3	dual	150.64	153.55	215.32	221.50
uRound2.PKE-0586-4.62-8192	107.00	3	primal	135.60	134.67	209.46	228.54

Scheme	Claim	NIST	Attack	Q-Core-Enum + O(1)	Lotus	Core-Enum + O(1)	8d-Enum + O(1) (quadratic fit)
uRound2.PKE-0643-4.62-32768	106.00	3	dual	140.15	141.49	205.00	217.57
uRound2.PKE-0643-4.62-32768	106.00	3	primal	127.63	127.23	204.35	223.70
uRound2.PKE-0708-18.48-32768	138.00	4, 5	dual	203.92	208.72	292.09	305.24
uRound2.PKE-0708-18.48-32768	138.00	4, 5	primal	187.47	193.07	293.47	312.96
uRound2.PKE-0835-2.31-32768	138.00	4	dual	193.08	199.90	292.30	354.12
uRound2.PKE-0835-2.31-32768	138.00	4	primal	180.16	188.90	297.84	319.20
uRound2.PKE-0835-2.31-32768	138.00	5	dual	193.08	199.90	292.30	354.12
uRound2.PKE-0835-2.31-32768	138.00	5	primal	180.16	188.90	297.84	319.20

Table 9: Cost of primal and dual attacks against LWE-based schemes assuming $2n$ LWE samples using enumeration. The column Scheme indicates each instantiation of a scheme using the format NAME-n-σ-q.

Scheme	Claim	NIST	Attack	Q-Core-Enum + O(1)	Lotus	Core-Enum + O(1)	8d-Enum + O(1) (quadratic fit)
Falcon-0512-4.05-12289	103.00	1	primal	164.70	174.13	329.40	372.54
Falcon-0768-4.05-18433	172.00	2, 3	primal	285.21	315.86	570.41	696.63
Falcon-1024-2.87-12289	230.00	4, 5	primal	417.72	473.52	835.44	1117.38
NTRU HRSS-0700-0.79-8192	123.00	1	primal	156.01	164.00	312.02	349.91
NTRU Prime-0761-0.82-4591	225.00	5	primal	182.30	194.54	355.09	388.25
NTRU Prime-0761-0.82-4591	248.00	5	primal	186.18	199.21	369.26	409.16
NTRUEncrypt-0443-0.80-2048	84.00	1	primal	92.88	91.08	185.61	207.70
NTRUEncrypt-0743-0.82-2048	159.00	1, 2, 3, 4, 5	primal	220.39	239.34	440.70	515.04
NTRUEncrypt-1024-724.00-1073750017	198.00	4, 5	primal	395.62	447.14	791.25	1042.83
pqNTRUsign-1024-0.70-65537	149.00	1, 2, 3, 4, 5	primal	207.66	224.41	415.33	479.77

Table 10: Cost of primal attack against NTRU-based schemes using enumeration. The column Scheme indicates each instantiation of a scheme using the format NAME-n-σ-q, where the equivalent LWE values are provided as seen in Section 4.

References

ACFP14. Martin R. Albrecht, Carlos Cid, Jean-Charles Faugère, and Ludovic Perret. Algebraic algorithms for LWE. Cryptology ePrint Archive, Report 2014/1018, 2014. http://eprint.iacr.org/2014/1018.

ACPS09. Benny Applebaum, David Cash, Chris Peikert, and Amit Sahai. Fast cryptographic primitives and circular-secure encryption based on hard learning problems. In Shai Halevi, editor, *CRYPTO 2009*, volume 5677 of *LNCS*, pages 595–618. Springer, Heidelberg, August 2009.

ADPS16. Erdem Alkim, Léo Ducas, Thomas Pöppelmann, and Peter Schwabe. Post-quantum key exchange - A new hope. In Thorsten Holz and Stefan Savage, editors, *25th USENIX Security Symposium, USENIX Security 16*, pages 327–343. USENIX Association, 2016.

AFFP14. Martin R. Albrecht, Jean-Charles Faugère, Robert Fitzpatrick, and Ludovic Perret. Lazy modulus switching for the BKW algorithm on LWE. In Hugo Krawczyk, editor, *PKC 2014*, volume 8383 of *LNCS*, pages 429–445. Springer, Heidelberg, March 2014.

AG11. Sanjeev Arora and Rong Ge. New algorithms for learning in presence of errors. In Luca Aceto, Monika Henzinger, and Jiri Sgall, editors, *ICALP 2011, Part I*, volume 6755 of *LNCS*, pages 403–415. Springer, Heidelberg, July 2011.

AGVW17. Martin R. Albrecht, Florian Göpfert, Fernando Virdia, and Thomas Wunderer. Revisiting the expected cost of solving uSVP and applications to LWE. In Tsuyoshi Takagi and Thomas Peyrin, editors, *ASIACRYPT 2017, Part I*, volume 10624 of *LNCS*, pages 297–322. Springer, Heidelberg, December 2017.

Ajt96. Miklós Ajtai. Generating hard instances of lattice problems (extended abstract). In *28th ACM STOC*, pages 99–108. ACM Press, May 1996.

Alb17. Martin R. Albrecht. On dual lattice attacks against small-secret LWE and parameter choices in HElib and SEAL. In Jean-Sébastien Coron and Jesper Buus Nielsen, editors, *EUROCRYPT 2017, Part II*, volume 10211 of *LNCS*, pages 103–129. Springer, Heidelberg, May 2017.

APS15. Martin R Albrecht, Rachel Player, and Sam Scott. On the concrete hardness of Learning with Errors. *Journal of Mathematical Cryptology*, 9(3):169–203, 2015.

BAA+17. Nina Bindel, Sedat Akleylek, Erdem Alkim, Paulo S. L. M. Barreto, Johannes Buchmann, Edward Eaton, Gus Gutoski, Juliane Kramer, Patrick Longa, Harun Polat, Jefferson E. Ricardini, and Gustavo Zanon. qtesla. Technical report, National Institute of Standards and Technology, 2017. available at https://csrc.nist.gov/projects/post-quantum-cryptography/round-1-submissions.

Ban17. Rachid El Bansarkhani. Kindi. Technical report, National Institute of Standards and Technology, 2017. available at https://csrc.nist.gov/projects/post-quantum-cryptography/round-1-submissions.

BCD+16. Joppe W. Bos, Craig Costello, Léo Ducas, Ilya Mironov, Michael Naehrig, Valeria Nikolaenko, Ananth Raghunathan, and Douglas Stebila. Frodo: Take off the ring! Practical, quantum-secure key exchange from LWE. In Edgar R. Weippl, Stefan Katzenbeisser, Christopher Kruegel, Andrew C. Myers, and Shai Halevi, editors, *ACM CCS 16*, pages 1006–1018. ACM Press, October 2016.

BCLvV17. Daniel J. Bernstein, Chitchanok Chuengsatiansup, Tanja Lange, and Christine van Vredendaal. Ntru prime. Technical report, National Institute of Standards and Technology, 2017. available at `https://csrc.nist.gov/projects/post-quantum-cryptography/round-1-submissions`.

BDGL16. Anja Becker, Léo Ducas, Nicolas Gama, and Thijs Laarhoven. New directions in nearest neighbor searching with applications to lattice sieving. In Robert Krauthgamer, editor, *27th SODA*, pages 10–24. ACM-SIAM, January 2016.

Ber17. Daniel J. Bernstein. Table of ciphertext and key sizes for the NIST candidate algorithms. Available at `https://groups.google.com/a/list.nist.gov/d/msg/pqc-forum/1lDNio0sKq4/xjqy4K6SAgAJ`, 2017.

BG14. Shi Bai and Steven D. Galbraith. Lattice decoding attacks on binary LWE. In Willy Susilo and Yi Mu, editors, *ACISP 14*, volume 8544 of *LNCS*, pages 322–337. Springer, Heidelberg, July 2014.

BPR12. Abhishek Banerjee, Chris Peikert, and Alon Rosen. Pseudorandom functions and lattices. In David Pointcheval and Thomas Johansson, editors, *EUROCRYPT 2012*, volume 7237 of *LNCS*, pages 719–737. Springer, Heidelberg, April 2012.

Che13. Yuanmi Chen. *Réduction de réseau et sécurité concrète du chiffrement complètement homomorphe*. PhD thesis, Paris 7, 2013.

CN11. Yuanmi Chen and Phong Q. Nguyen. BKZ 2.0: Better lattice security estimates. In Dong Hoon Lee and Xiaoyun Wang, editors, *ASIACRYPT 2011*, volume 7073 of *LNCS*, pages 1–20. Springer, Heidelberg, December 2011.

CPL+17. Jung Hee Cheon, Sangjoon Park, Joohee Lee, Duhyeong Kim, Yongsoo Song, Seungwan Hong, Dongwoo Kim, Jinsu Kim, Seong-Min Hong, Aaram Yun, Jeongsu Kim, Haeryong Park, Eunyoung Choi, Kimoon kim, Jun-Sub Kim, and Jieun Lee. Lizard. Technical report, National Institute of Standards and Technology, 2017. available at `https://csrc.nist.gov/projects/post-quantum-cryptography/round-1-submissions`.

CS97. Don Coppersmith and Adi Shamir. Lattice attacks on NTRU. In Walter Fumy, editor, *EUROCRYPT'97*, volume 1233 of *LNCS*, pages 52–61. Springer, Heidelberg, May 1997.

DKRV17. Jan-Pieter D'Anvers, Angshuman Karmakar, Sujoy Sinha Roy, and Frederik Vercauteren. Saber. Technical report, National Institute of Standards and Technology, 2017. available at `https://csrc.nist.gov/projects/post-quantum-cryptography/round-1-submissions`.

DT17. Fplll Development Team. fplll, a lattice reduction library. Available at `https://github.com/fplll/fplll`, 2017.

DTGW17. Jintai Ding, Tsuyoshi Takagi, Xinwei Gao, and Yuntao Wang. Ding key exchange. Technical report, National Institute of Standards and Technology, 2017. available at `https://csrc.nist.gov/projects/post-quantum-cryptography/round-1-submissions`.

FP85. U. Fincke and M. Pohst. Improved methods for calculating vectors of short length in a lattice, including a complexity analysis. *Mathematics of Computation*, 44(170):463–463, May 1985.

Fuj17. Ryo Fujita. Table of underlying problems of the NIST candidate algorithms. Available at `https://groups.google.com/a/list.nist.gov/d/msg/pqc-forum/1lDNio0sKq4/7zXvtfdZBQAJ`, 2017.

GJMS17. Qian Guo, Thomas Johansson, Erik Mårtensson, and Paul Stankovski. Coded-BKW with sieving. In Tsuyoshi Takagi and Thomas Peyrin, editors,

ASIACRYPT 2017, Part I, volume 10624 of *LNCS*, pages 323–346. Springer, Heidelberg, December 2017.

GJS15. Qian Guo, Thomas Johansson, and Paul Stankovski. Coded-BKW: Solving LWE using lattice codes. In Rosario Gennaro and Matthew J. B. Robshaw, editors, *CRYPTO 2015, Part I*, volume 9215 of *LNCS*, pages 23–42. Springer, Heidelberg, August 2015.

GMZB+17. Oscar Garcia-Morchon, Zhenfei Zhang, Sauvik Bhattacharya, Ronald Rietman, Ludo Tolhuizen, and Jose-Luis Torre-Arce. Round2. Technical report, National Institute of Standards and Technology, 2017. available at `https://csrc.nist.gov/projects/post-quantum-cryptography/round-1-submissions`.

GN08. Nicolas Gama and Phong Q. Nguyen. Finding short lattice vectors within Mordell's inequality. In Richard E. Ladner and Cynthia Dwork, editors, *40th ACM STOC*, pages 207–216. ACM Press, May 2008.

Gro96. Lov K. Grover. A fast quantum mechanical algorithm for database search. In *28th ACM STOC*, pages 212–219. ACM Press, May 1996.

GvVW17a. Florian Göpfert, Christine van Vredendaal, and Thomas Wunderer. A hybrid lattice basis reduction and quantum search attack on LWE. Cryptology ePrint Archive, Report 2017/221, 2017. `http://eprint.iacr.org/2017/221`.

GvVW17b. Florian Göpfert, Christine van Vredendaal, and Thomas Wunderer. A hybrid lattice basis reduction and quantum search attack on LWE. In *Post-Quantum Cryptography - 8th International Workshop, PQCrypto 2017, Utrecht, The Netherlands, June 26-28, 2017, Proceedings*, pages 184–202, 2017.

Ham17. Mike Hamburg. Three bears. Technical report, National Institute of Standards and Technology, 2017. available at `https://csrc.nist.gov/projects/post-quantum-cryptography/round-1-submissions`.

HG07. Nick Howgrave-Graham. A hybrid lattice-reduction and meet-in-the-middle attack against NTRU. In Alfred Menezes, editor, *CRYPTO 2007*, volume 4622 of *LNCS*, pages 150–169. Springer, Heidelberg, August 2007.

HPS96. Jeffery Hoffstein, Jill Pipher, and Joseph H. Silverman. NTRU: A new high speed public-key cryptosystem. Technical report, Draft distributed at CRYPTO96, 1996. available at `https://cdn2.hubspot.net/hubfs/49125/downloads/ntru-orig.pdf`.

HPS98. Jeffrey Hoffstein, Jill Pipher, and Joseph H. Silverman. NTRU: A ring-based public key cryptosystem. In *Algorithmic Number Theory, Third International Symposium, ANTS-III, Portland, Oregon, USA, June 21-25, 1998, Proceedings*, pages 267–288, 1998.

Kan83. Ravi Kannan. Improved algorithms for integer programming and related lattice problems. In *15th ACM STOC*, pages 193–206. ACM Press, April 1983.

Kan87. Ravi Kannan. Minkowski's convex body theorem and integer programming. *Mathematics of Operations Research*, pages 415–440, 1987.

KF15. Paul Kirchner and Pierre-Alain Fouque. An improved BKW algorithm for LWE with applications to cryptography and lattices. In Rosario Gennaro and Matthew J. B. Robshaw, editors, *CRYPTO 2015, Part I*, volume 9215 of *LNCS*, pages 43–62. Springer, Heidelberg, August 2015.

Laa15a. Thijs Laarhoven. *Search problems in cryptography: From fingerprinting to lattice sieving*. PhD thesis, Eindhoven University of Technology, 2015.

Laa15b. Thijs Laarhoven. Sieving for shortest vectors in lattices using angular locality-sensitive hashing. In Rosario Gennaro and Matthew J. B. Robshaw, editors, *CRYPTO 2015, Part I*, volume 9215 of *LNCS*, pages 3–22. Springer, Heidelberg, August 2015.

LDK+17. Vadim Lyubashevsky, Leo Ducas, Eike Kiltz, Tancrede Lepoint, Peter Schwabe, Gregor Seiler, and Damien Stehle. Crystals-dilithium. Technical report, National Institute of Standards and Technology, 2017. available at `https://csrc.nist.gov/projects/post-quantum-cryptography/round-1-submissions`.

LLJ+17. Xianhui Lu, Yamin Liu, Dingding Jia, Haiyang Xue, Jingnan He, and Zhenfei Zhang. Lac. Technical report, National Institute of Standards and Technology, 2017. available at `https://csrc.nist.gov/projects/post-quantum-cryptography/round-1-submissions`.

LMvdP15. Thijs Laarhoven, Michele Mosca, and Joop van de Pol. Finding shortest lattice vectors faster using quantum search. *Designs, Codes and Cryptography*, 77(2–3):375–400, December 2015.

LP11. Richard Lindner and Chris Peikert. Better key sizes (and attacks) for LWE-based encryption. In Aggelos Kiayias, editor, *CT-RSA 2011*, volume 6558 of *LNCS*, pages 319–339. Springer, Heidelberg, February 2011.

LPR10. Vadim Lyubashevsky, Chris Peikert, and Oded Regev. On ideal lattices and learning with errors over rings. In Henri Gilbert, editor, *EUROCRYPT 2010*, volume 6110 of *LNCS*, pages 1–23. Springer, Heidelberg, May 2010.

LS15. Adeline Langlois and Damien Stehlé. Worst-case to average-case reductions for module lattices. *Designs, Codes and Cryptography*, 75(3):565–599, June 2015.

Moo17. Dustin Moody. The NIST post quantum cryptography "competition". Available at `https://csrc.nist.gov/CSRC/media/Projects/Post-Quantum-Cryptography/documents/asiacrypt-2017-moody-pqc.pdf`, 2017.

MR09. Daniele Micciancio and Oded Regev. Lattice-based cryptography. In Daniel J. Bernstein, Johannes Buchmann, and Erik Dahmen, editors, *Post-Quantum Cryptography*, pages 147–191. Springer, Heidelberg, Berlin, Heidelberg, New York, 2009.

MS01. Alexander May and Joseph H. Silverman. Dimension reduction methods for convolution modular lattices. In *Cryptography and Lattices, International Conference, CaLC 2001, Providence, RI, USA, March 29-30, 2001, Revised Papers*, pages 110–125, 2001.

MW15. Daniele Micciancio and Michael Walter. Fast lattice point enumeration with minimal overhead. In Piotr Indyk, editor, *26th SODA*, pages 276–294. ACM-SIAM, January 2015.

NAB+17. Michael Naehrig, Erdem Alkim, Joppe Bos, Leo Ducas, Karen Easterbrook, Brian LaMacchia, Patrick Longa, Ilya Mironov, Valeria Nikolaenko, Christopher Peikert, Ananth Raghunathan, and Douglas Stebila. Frodokem. Technical report, National Institute of Standards and Technology, 2017. available at `https://csrc.nist.gov/projects/post-quantum-cryptography/round-1-submissions`.

Nat16. National Institute of Standards and Technology. Submission requirements and evaluation criteria for the Post-Quantum Cryptography standardization process. `http://csrc.nist.gov/groups/ST/post-quantum-crypto/documents/call-for-proposals-final-dec-2016.pdf`, December 2016.

Nat17. National Institute of Standards and Technology. Performance testing of the NIST candidate algorithms. Available at https://drive.google.com/file/d/1g-l0bPa-tReBD0Frgnz9aZXpO06PunUa/view, 2017.

PAA+17. Thomas Poppelmann, Erdem Alkim, Roberto Avanzi, Joppe Bos, Leo Ducas, Antonio de la Piedra, Peter Schwabe, and Douglas Stebila. Newhope. Technical report, National Institute of Standards and Technology, 2017. available at https://csrc.nist.gov/projects/post-quantum-cryptography/round-1-submissions.

PFH+17. Thomas Prest, Pierre-Alain Fouque, Jeffrey Hoffstein, Paul Kirchner, Vadim Lyubashevsky, Thomas Pornin, Thomas Ricosset, Gregor Seiler, William Whyte, and Zhenfei Zhang. Falcon. Technical report, National Institute of Standards and Technology, 2017. available at https://csrc.nist.gov/projects/post-quantum-cryptography/round-1-submissions.

PHAM17. Le Trieu Phong, Takuya Hayashi, Yoshinori Aono, and Shiho Moriai. Lotus. Technical report, National Institute of Standards and Technology, 2017. available at https://csrc.nist.gov/projects/post-quantum-cryptography/round-1-submissions.

Reg05. Oded Regev. On lattices, learning with errors, random linear codes, and cryptography. In Harold N. Gabow and Ronald Fagin, editors, *37th ACM STOC*, pages 84–93. ACM Press, May 2005.

Saa17. Markku-Juhani O. Saarinen. Hila5. Technical report, National Institute of Standards and Technology, 2017. available at https://csrc.nist.gov/projects/post-quantum-cryptography/round-1-submissions.

SAB+17. Peter Schwabe, Roberto Avanzi, Joppe Bos, Leo Ducas, Eike Kiltz, Tancrede Lepoint, Vadim Lyubashevsky, John M. Schanck, Gregor Seiler, and Damien Stehle. Crystals-kyber. Technical report, National Institute of Standards and Technology, 2017. available at https://csrc.nist.gov/projects/post-quantum-cryptography/round-1-submissions.

SAL+17. Nigel P. Smart, Martin R. Albrecht, Yehuda Lindell, Emmanuela Orsini, Valery Osheter, Kenny Paterson, and Guy Peer. Lima. Technical report, National Institute of Standards and Technology, 2017. available at https://csrc.nist.gov/projects/post-quantum-cryptography/round-1-submissions.

Sch15. John Schanck. Practical lattice cryptosystems: NTRUEncrypt and NTRUMLS. Master's thesis, University of Waterloo, 2015.

SE94. Claus-Peter Schnorr and M. Euchner. Lattice basis reduction: Improved practical algorithms and solving subset sum problems. *Math. Program.*, 66:181–199, 1994.

SHRS17. John M. Schanck, Andreas Hulsing, Joost Rijneveld, and Peter Schwabe. Ntru-hrss-kem. Technical report, National Institute of Standards and Technology, 2017. available at https://csrc.nist.gov/projects/post-quantum-cryptography/round-1-submissions.

SPL+17. Minhye Seo, Jong Hwan Park, Dong Hoon Lee, Suhri Kim, and Seung-Joon Lee. Emblem and r.emblem. Technical report, National Institute of Standards and Technology, 2017. available at https://csrc.nist.gov/projects/post-quantum-cryptography/round-1-submissions.

SSTX09. Damien Stehlé, Ron Steinfeld, Keisuke Tanaka, and Keita Xagawa. Efficient public key encryption based on ideal lattices. In Mitsuru Matsui, editor, *ASIACRYPT 2009*, volume 5912 of *LNCS*, pages 617–635. Springer, Heidelberg, December 2009.

SSZ17. Ron Steinfeld, Amin Sakzad, and Raymond K. Zhao. Titanium. Technical report, National Institute of Standards and Technology, 2017. available at https://csrc.nist.gov/projects/post-quantum-cryptography/round-1-submissions.

Wun16. Thomas Wunderer. Revisiting the hybrid attack: Improved analysis and refined security estimates. Cryptology ePrint Archive, Report 2016/733, 2016. http://eprint.iacr.org/2016/733.

ZCHW17a. Zhenfei Zhang, Cong Chen, Jeffrey Hoffstein, and William Whyte. Ntruencrypt. Technical report, National Institute of Standards and Technology, 2017. available at https://csrc.nist.gov/projects/post-quantum-cryptography/round-1-submissions.

ZCHW17b. Zhenfei Zhang, Cong Chen, Jeffrey Hoffstein, and William Whyte. pqntrusign. Technical report, National Institute of Standards and Technology, 2017. available at https://csrc.nist.gov/projects/post-quantum-cryptography/round-1-submissions.

ZjGS17. Yunlei Zhao, Zhengzhong jin, Boru Gong, and Guangye Sui. Kcl (pka okcn/akcn/cnke). Technical report, National Institute of Standards and Technology, 2017. available at https://csrc.nist.gov/projects/post-quantum-cryptography/round-1-submissions.