Estimate all the {LWE, NTRU} schemes!

Version: August 29, 2018

Martin R. Albrecht[1], Benjamin R. Curtis[1✉], Amit Deo[1], Alex Davidson[1], Rachel Player[1,2], Eamonn W. 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" of 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 the security of the proposed NTRU-based schemes against the primal 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.

1 Introduction

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 aimed at meeting one or more target security categories (out of a pool of five). These 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, and to use this cryptanalysis to roughly estimate the size of the security parameter for each parameter set.

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, and more specifically, of the BKZ lattice reduction algorithm. This algorithm, which combines SVP calls in projected sub-lattices or "blocks", is a vital building block in attacks on these schemes. These differences can result in the same scheme being attributed several 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 SVP oracle calls required by BKZ (cf. Section 4). A major source of divergence in estimated security is whether current estimates for sieving [AKS01,LMvdP15,BDGL16] or enumeration [Kan83,FP85,MW15] are 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 on the security assurances given by each submission, we extract the proposed parameter sets for each LWE-based and NTRU-based submission (Section 3). 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 4). Using this information, we then cross-estimate the security of each parameter set under every cost model from every submission (Section 5).

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 algebraic [AG11,ACFP14] and combinatorial [AFFP14,GJS15,KF15,GJMS17] attacks, 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. 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 a "lattice decoding" attack [Sch03,LP11]. The primal uSVP attack can be considered as a simplified variant of the decoding attack in the enumeration regime. For NTRU, we restrict our attention to the primal uSVP attack (possibly combined with guessing zero-entries of the short vector). We do not consider the hybrid lattice reduction and meet-in-the-middle attack [HG07,Wun16] or "guessing + nearest plane" after lattice reduction.

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 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].

2 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

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

vector $\boldsymbol{f}$. We write $\|\boldsymbol{f}\|$ 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 abuse notation to denote the expectation and variance of a random variable $X \sim \chi$ by $\mathbb{E}[\chi]$ and $\mathbb{V}[\chi]$ respectively. For $c \in \mathbb{Q}$, we use $\lfloor c \rceil$ to denote the procedure of rounding c to the nearest integer $z \in \mathbb{Z}$, rounding towards zero in the case of a tie. We denote by log the logarithm to base 2.

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 $s_i \leftarrow U_{[a,b]}$ as (a, b), and the distribution of $\boldsymbol{s}$ such that exactly h entries (selected at uniform) have been sampled from $U_{[a,b]\setminus\{0\}}$, and the remaining entries have been set to 0, as $((a, b), h)$.

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 an invariant of the lattice and is defined as $\mathrm{Vol}(L) = \sqrt{\det(\boldsymbol{B}^t\boldsymbol{B})}$. In a random lattice, the *Gaussian heuristic* estimates the length of a shortest non-zero vector of an full-rank m-dimensional lattice L to be

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

The quality of a lattice basis $\boldsymbol{B} = \{\boldsymbol{b}_1, \ldots, \boldsymbol{b}_m\}$ of a full-rank lattice L such that $\|\boldsymbol{b}_1\| \leq \|\boldsymbol{b}_2\| \leq \cdots \leq \|\boldsymbol{b}_m\|$ 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.

2.1 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, however 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 the Kannan [Kan87] or Bai and Galbraith [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 $\{\boldsymbol{x} \in \mathbb{Z}_q^m \mid \boldsymbol{x}^t \boldsymbol{A} \equiv \boldsymbol{0} \mod q\}$, where the rows of A are the m LWE samples a_i. Note that an oracle solving Decision-LWE can be turned into an oracle solving Search-LWE. For either attack, variants are known which exploit the presence of unusually short, or sparse, secret distributions [BG14,CHK⁺17,Alb17] 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 (s and e_i are "short") are drawn from a ring of the form $\mathcal{R}_q = \mathbb{Z}_q[x]/(\phi)$ 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 (of polynomials) $\boldsymbol{a}_i$, $\boldsymbol{s}$ and polynomials e_i are drawn from $\mathcal{R}_q^k$ and $\mathcal{R}_q$ respectively. Search-MLWE is the problem of recovering $\boldsymbol{s}$ from a set $\{(\boldsymbol{a}_i, \langle \boldsymbol{a}_i, \boldsymbol{s} \rangle + e_i)\}_{i=1}^m$, Decision-MLWE is the problem of distinguishing such a set from a set uniformly sampled from $\mathcal{R}_q^k \times \mathcal{R}_q$.

One can view RLWE and MLWE instances as LWE instances by interpreting the coefficients of elements in $\mathcal{R}_q$ as vectors in $\mathbb{Z}_q^n$ and ignoring the algebraic structure of $\mathcal{R}_q$. This identification with LWE is the standard approach to costing the complexity of solving RLWE and MLWE due to the absence of known cryptanalytic techniques exploiting algebraic structure. Therefore, we restrict our analysis of solving RLWE and MLWE to the primal and dual attacks mentioned above.

There is also a class of LWE-like problems that replace the addition of a 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 can 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 chosen from a uniform distribution on the set $\{-\frac{q}{2p} + 1, \ldots, \frac{q}{2p}\}$ [Ngu18]. The same ideas apply to the other variants of LWE that use deterministic rounding error, such as RLWR and MLWR.

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 or $2n$ plain LWE samples. In a typical setting, though, the adversary does not get to enjoy the full power of having two RLWE 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, and thus the noise in the second sample can be quite large. In the case of Module-LWE, a ciphertext in transit produces a smaller number of LWE samples, but n samples can still be recovered from the public key. In this work, we consider the n and $2n$ scenarios for all schemes. We note that, for many schemes, n samples are sufficient to run the most efficient variant of either attack.

2.2 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.*

Note that 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 polynomial 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 lattice $L(\boldsymbol{B})$ is 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]. $L(\boldsymbol{B})$ contains up to n linearly independent short vectors given by the rotations of $(\boldsymbol{f}, \boldsymbol{g})^t$, since $hf = g \bmod q$ and hence $(\boldsymbol{g}, \boldsymbol{f})^t = \boldsymbol{B}(\boldsymbol{w}, \boldsymbol{f})^t$ for some $\boldsymbol{w} \in \mathbb{Z}^n$. We treat the NTRU problem as a uSVP instance and account for the presence of rotations by amplifying the success probability p of guessing entries of the short vector correctly to $1 - (1-p)^k$, where k is the number of rotations. Further speedups as presented in [KF17] which exploit the structure of the NTRU lattice do not affect the proposals submitted to NIST and are therefore not considered.

In addition, if $f = pF$ or $f = pF + 1$ for some small polynomial F then one can construct a similar uSVP lattice that contains $(\boldsymbol{F}, \boldsymbol{g})^t$, see for example [Sch15,Wun16]. Similarly to LWE, in order to improve this attack, rescaling and dimension reducing techniques can be applied [MS01], and the impact of these techniques can be measured using the estimator [APS15]. Note that the dimension of the lattice must be between n and $2n$ by construction. The dual attack is not considered, as it does not apply.

2.3 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 successfully recover the shortest vector when running BKZ. 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 current generations of 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.

3 Proposed schemes

The three tables below specify the parameter sets for the schemes considered. In particular Table 1 gives the parameters for the NTRU-based schemes. Table 2 gives the parameters of the same schemes when converted into the LWE-based context, as detailed in Section 5. 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 5. 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 $\boldsymbol{c}$ 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.

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
SNTRU Prime	761	4591	16.91	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
SNTRU Prime	761	4591	0.82	$((-1,1),286)$	5	NTRU	x^n-x-1	KEM
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 5. The NIST column indicates the NIST security category aimed at.

Name	n	k	q	σ	Secret dist.	NIST	Assumption	ϕ	Primitive
KCL-RLWE	1024	—	12289	2.83	normal	5	RLWE	x^n+1	KEM
KCL-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

Name	n	k	q	σ	Secret dist.	NIST	Assumption	ϕ	Primitive
HILA5	1024	—	12289	2.83	normal	5	RLWE	x^n+1	KE
KINDI	768	3	16384	2.29	$(-4,4)$	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
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	1024	—	2048	1.12	$((-1,1),140)$	1	LWE, LWR	—	KEM, PKE
	1024	—	1024	1.12	$((-1,1),128)$	1	LWE, LWR	—	KEM, PKE
	1024	—	2048	1.12	$((-1,1),200)$	3	LWE, LWR	—	KEM, PKE
	1024	—	2048	1.12	$((-1,1),200)$	3	LWE, LWR	—	KEM, PKE
	2048	—	4096	1.12	$((-1,1),200)$	5	LWE, LWR	—	KEM, PKE
	2048	—	2048	1.12	$((-1,1),200)$	5	LWE, LWR	—	KEM, PKE
RLizard	1024	—	1024	1.12	$((-1,1),128)$	1	RLWE, RLWR	x^n+1	KEM, PKE
	1024	—	2048	1.12	$((-1,1),264)$	3	RLWE, RLWR	x^n+1	KEM, PKE
	2048	—	2048	1.12	$((-1,1),164)$	3	RLWE, RLWR	x^n+1	KEM, PKE
	2048	—	4096	1.12	$((-1,1),256)$	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	2.29	$((-1,1),74)$	1	LWR	—	KEM
	580	—	32768	4.61	$((-1,1),116)$	2	LWR	—	KEM
	630	—	32768	4.61	$((-1,1),126)$	3	LWR	—	KEM
	786	—	32768	4.61	$((-1,1),156)$	4	LWR	—	KEM
	786	—	32768	4.61	$((-1,1),156)$	5	LWR	—	KEM
uRound2.KEM	418	—	4096	4.61	$((-1,1),66)$	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	18.47	$((-1,1),96)$	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	4.61	$((-1,1),74)$	1	LWR	—	PKE
	585	—	32768	4.61	$((-1,1),110)$	2	LWR	—	PKE
	643	—	32768	4.61	$((-1,1),114)$	3	LWR	—	PKE
	835	—	32768	2.29	$((-1,1),166)$	4	LWR	—	PKE
	835	—	32768	2.29	$((-1,1),166)$	5	LWR	—	PKE
uRound2.PKE	420	—	1024	1.12	$((-1,1),62)$	1	RLWR	$\sum_{i=0}^n x^i$	PKE
	540	—	8192	4.61	$((-1,1),96)$	2	RLWR	$\sum_{i=0}^n x^i$	PKE
	586	—	8192	4.61	$((-1,1),104)$	3	RLWR	$\sum_{i=0}^n x^i$	PKE
	708	—	32768	18.47	$((-1,1),140)$	4, 5	RLWR	$\sum_{i=0}^n x^i$	PKE
nRound2.KEM	400	—	3209	3.61	$((-1,1),72)$	1	RLWR	$\sum_{i=0}^n x^i$	KEM
	486	—	1949	2.18	$((-1,1),96)$	2	RLWR	$\sum_{i=0}^n x^i$	KEM
	556	—	3343	3.76	$((-1,1),88)$	3	RLWR	$\sum_{i=0}^n x^i$	KEM
	658	—	1319	1.46	$((-1,1),130)$	4, 5	RLWR	$\sum_{i=0}^n x^i$	KEM

Name	n	k	q	σ	Secret dist.	NIST	Assumption	ϕ	Primitive
nRound2.PKE	442	—	2659	1.47	$((-1,1),74)$	1	RLWR	$\sum_{i=0}^{n} x^i$	PKE
	556	—	3343	1.86	$((-1,1),88)$	2	RLWR	$\sum_{i=0}^{n} x^i$	PKE
	576	—	2309	1.27	$((-1,1),108)$	3	RLWR	$\sum_{i=0}^{n} x^i$	PKE
	708	—	2837	1.57	$((-1,1),140)$	4, 5	RLWR	$\sum_{i=0}^{n} x^i$	PKE
LightSaber	512	2	8192	2.29	normal	1	MLWR	$x^{n/k}+1$	KEM, PKE
NTRU LPrime	761	—	4591	0.82	$((-1,1),250)$	5	RLWR	$x^n - x - 1$	KEM
Saber	768	3	8192	2.29	normal	3	MLWR	$x^{n/k}+1$	KEM, PKE
FireSaber	1024	4	8192	2.29	normal	5	MLWR	$x^{n/k}+1$	KEM, PKE
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 relies on a family of rings where $f_i \in \{-1,0,1\}$ and $f_0 \in \{-1,1\}$. † 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].

4 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 are whether they are in the sieving or enumeration regime, and how many calls to the SVP 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 this 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 the constant 16.4 [APS15], based on experiments in [Laa15b], some authors omit it. A "min space" variant of sieving is also considered in [BDGL16], which uses $c = 0.368$ with Grover speedups lowering this to $c = 0.2975$ [Laa15a]. 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. The estimates $0.187\beta\log\beta-1.019\beta+16.1$ [APS15] and $0.000784\beta^2+0.366\beta-0.9$ [HPS+15] are based on fitting the same data from [Che13].

We note that the different cost models diverge on the unit of operations they are using. In the enumeration models, the unit is "number of nodes visited during enumeration". It is typically assumed that processing one node costs about 100 CPU cycles [CN11]. For sieving the elementary operation is typically an operation on word-sized integers, costing about one CPU cycle. For quantum algorithms the unit is typically the number of Grover iterations required. It is not clear how this translates to traditional CPU cycles. Of course, for models which suppress lower order terms, the unit of computation considered is immaterial.

With respect to the number of SVP oracle calls required by BKZ, a popular choice was to follow the "Core-SVP" model introduced in [ADPS16], that considers a single call. Alternatively, the number of calls has also been estimated to be $8d$ (for example, in [Alb17]), where d is the dimension of the embedding lattice and β is the BKZ block size.

LOTUS [PHAM17] is the only submission not to provide a closed formula for estimating the cost of BKZ. Given their preference for enumeration, we fit their estimated cost model to a curve of shape $2^{c_1\beta\log\beta+c_2\beta+c_3}$ following [MW15]. We fit a curve to the values given by (39) in [PHAM17], the script used is available in the public repository.

The NTRU Prime submission [BCLvV17] utilises the BKZ 2.0 simulator of [CN11] to determine the necessary block size and number of tours to achieve a certain root Hermite factor prior to applying their BKZ cost model. In contrast, we apply the asymptotic formula from [Che13] to relate block size and root Hermite factor, and consider BKZ to complete in 8 tours while matching their cost asymptotic for a single enumeration call.

5 Estimates

For our experiments we make use of the LWE estimator[5] from [APS15], which allows one to specify 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. As mentioned previously, for every LWE-based scheme we estimate each attack twice; using n and $2n$ available samples. Our code is available at `https://github.com/estimate-all-the-lwe-ntru-schemes`.

Our results are given in Tables 5, 6, 7, 8, 9, and 10 in Appendix A. In addition, we make available at `https://estimate-all-the-lwe-ntru-schemes.github.io` a human-friendly version of these tables. In particular, the HTML version supports filtering and sorting the table. It also contains SageMath source code snippets to reproduce each entry. As discussed above, the meaning of the output values vary depending on cost model since the unit of computation is not consistent across different cost models. Furthermore, submissions might consider different units of computation, such as bit security, even when using a particular cost model. Furthermore, we do not consider memory requirements in this work.

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

Secret distributions. The majority of the submissions consider uniform, bounded uniform, or sparse bounded uniform secret distributions. In the case of Lizard, LWE secrets are drawn from the distribution $\mathcal{ZO}_n(\rho)$ for some $0 < \rho < 1$. $\mathcal{ZO}_n(\rho)$ is the distribution over $\{-1, 0, 1\}^n$ where each component s_i (of a vector $\boldsymbol{s} \leftarrow \mathcal{ZO}_n(\rho)$) satisfies $\Pr[s_i = 1] = \Pr[s_i = -1] = \rho/2$ and $\Pr[s_i = 0] = 1 - \rho$. We model this distribution as a fixed weight bounded uniform distribution, where the Hamming weight h matches the expected number of non-zero components of an element drawn from $\mathcal{ZO}_n(\rho)$.

[5] `https://bitbucket.org/malb/lwe-estimator`, commit 1850100.

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

Table 4. Cost models proposed as part of a PQC NIST submission. The name of a model is the log of its cost.

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, $\sqrt{\mathbb{V}[U_{[a,b]}]}$. In the case of LWR, we use a standard deviation of $\sqrt{\frac{(q/p)^2-1}{12}}$, following [Ngu18].

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 functionality is LIMA [SAL+17], which chooses to use a target success probability of 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 distribution centred at zero is small and we thus ignore it.

NTRU. For estimating NTRU-based schemes, we also utilise the LWE estimator as described here to evaluate the primal attack (and its improvements, when considered in combination with dimension reduction) on NTRU. In particular, we cost NTRU as a uSVP instance but note that when no guessing is performed, the geometry of the NTRU-lattice can possibly be exploited as in [KF17]. 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 error 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 $\boldsymbol{f}$. We limit the number of LWE samples to n. The estimator is set to consider the n rotations of $\boldsymbol{g}$ when estimating the cost of the primal attack on NTRU.

Beyond key recovery. We consider key recovery attacks on all schemes. In the case of LWE-based schemes, we also consider message recovery attacks by setting the number of samples to be $m = 2n$ and trying to recover the ephemeral secret key set as part of key encapsulation. A straightforward primal uSVP message recovery attack for NTRU-based schemes as described in Footnote 2 of [SHRS17] is not expected to perform better than the primal uSVP key recovery attack, and is therefore omitted in this work.

In the case of signatures, it is also possible to attempt forgery attacks. All four lattice-based signatures schemes submitted to the NIST process claim that the problem of forging a signature is strictly harder than that of recovering the signing key. In particular Dilithium and pqNTRUSign provide analyses which explicitly determine that larger BKZ block sizes are required for signature forgery than key recovery. Falcon argues similarly without giving explicit block sizes and qTESLA presents a tight reduction in the QROM from the RLWE problem to signature forgery, in particular from exactly the RLWE problem one would have to solve to yield the signing key. As such, since one may trivially forge signatures given possession of the signing key, forgery attacks are not considered further in their security analyses.

Several complications arise when attempting to estimate the complexity of signature forgery compared to key recovery. These include the requirement for a signature forging adversary to satisfy the conditions in the Verify algorithm, which for the four proposed schemes consists of solving different, sometimes not well studied, problems, such as the SIS problem in the ℓ_∞-norm for Dilithium and qTESLA and the modular equivalence required between the message and signature in pqNTRUSign. In attempts to determine how one might straightforwardly estimate the complexity of signature forgery against the Dilithium and qTESLA schemes, custom analysis was required which was heavily dependent on the intricacies of the scheme in question, ruling out a scheme-agnostic approach to security estimation in the case of signature forgeries.

6 Discussion

Our data highlights that cost models for lattice reduction do not necessarily preserve the ordering of the schemes under consideration. That is, under one cost model some scheme A can be considered harder to break than a scheme B, while under another cost model scheme B appears harder to break.

An example for the schemes EMBLEM and uRound2.KEM was highlighted in [Ber18]. Specifically, the example concerns the EMBLEM parameter set with $n = 611$ and the uRound2.KEM parameter set with $n = 500$. In the 0.292β cost model, the cost of the primal attack for EMBLEM-611 is estimated as[6] 76 and for uRound2.KEM-500 as 84. For the same attack in the $0.187\beta \log \beta - 1.019\beta + 16.1$ cost model, the cost is estimated for EMBLEM-611 as 142 and for uRound2.KEM-500 as 126. Similar swaps can be observed for several other pairs of schemes and cost models. In most cases the estimated securities of the two schemes are very close to each other (differing by, say, 1 or 2) and thus a swap of ordering does not fundamentally alter our understanding of their relative security as these estimates are typically derived by heuristically searching through the space of possible parameters and computing with limited precision. In some cases, though, such as the one highlighted in [Ber18], the differences in security estimates can be significant. There are two classes of such cases.

Sparse secrets. The first class of cases involves instances with sparse secrets. The LWE estimator applies guessing strategies when costing the dual attack (cf. [Alb17]) and the primal attack. The basic idea is that for a sparse secret, many of the entries of the secret vector are zero, and hence can be ignored. We guess τ entries to be zero, and drop the corresponding columns from the attack lattice. In dropping τ columns from a n-dimensional LWE instance, we obtain a $(n-\tau)$-dimensional LWE instance with a more dense secret distribution, where the density depends on the choice of τ and the original value of h. On the one hand, there is a probability of failure when guessing which columns to drop. On the other hand there may exist a τ for which the $(n-\tau)$-dimensional LWE instance is easier to solve, and in particular requires a smaller BKZ blocksize β.

[6] Any discrepancies in value from those cited in [Ber18] are due to rounding introduced to the estimator output since.

The trade-off between running BKZ on smaller lattices and having to run it multiple times can correspond to an overall lower expected attack cost. This probability of failure when guessing secret entries does not depend on the cost model, but rather on the weight and dimension of the secret, making this kind of attack more effective for very sparse secrets. In the case of comparing an enumeration cost model versus a sieving one, we have that the cost of enumeration is fitted as $2^{\Theta(\beta \log \beta)}$ or $2^{\Theta(\beta^2)}$ whereas the cost of sieving is $2^{\Theta(\beta)}$. The steeper curve for enumeration means that as we increase τ, and hence decrease β, savings are potentially larger, justifying a larger number τ of entries guessed. Concretely, the computed optimal guessing dimension τ can be much larger than in the sieving regime. This phenomenon can also be observed when comparing two different sieving models or two different enumeration models.

In Figure 1, we illustrate this for the EMBLEM and uRound2.KEM example. EMBLEM does not have a sparse secret, while uRound2.KEM does. For EMBLEM the best guessing dimension, giving the lowest overall cost, is $\tau = 0$ in both cost models. For uRound2.KEM, we see that the optimal guessing dimension varies depending on the cost model. In the 0.292β cost model, the lowest overall expected cost is achieved for $\tau = 1$ while in the $0.187\beta \log \beta - 1.019\beta + 16.1$ model the optimal choice is $\tau = 197$.

Dual attack. The second class of cases can be observed for the dual attack. Recall that the dual attack runs lattice reduction to find a small vector $\boldsymbol{v}$ in the scaled dual lattice of $\boldsymbol{A}$ and then considers $\langle \boldsymbol{v}, \boldsymbol{b} \rangle$ which is short when $\boldsymbol{A}, \boldsymbol{b}$ is an LWE sample. In more detail, the advantage of distinguishing $\langle \boldsymbol{v}, \boldsymbol{b} \rangle$ is $\varepsilon = \exp(-\delta^{2\,d} \cdot c_0)$ for some constant c_0 depending on the instance and with d being the dimension of the lattice under consideration [LP11]. To amplify this advantage to a constant advantage, we have to repeat the experiment roughly $1/\varepsilon^2$ times. Thus, the overall cost of the attack is $\approx C(\beta)/\exp(-\delta^{2\,d} \cdot c_0)^2$ where $C(\beta)$ is the cost of lattice reduction with block size β. In the sieving regime $C(\beta) \approx 2^{c_1 \beta}$ in the enumeration regime we have $C(\beta) \approx \beta^{c_2 \beta}$ (from enumeration costing $2^{\Theta(\beta \log \beta)}$). For large β we have $\delta \approx \beta^{1/2\beta}$ [Che13] (cf. Section 2), and thus we have overall log costs of roughly $c_1\, \beta + 2\, \log(e)\, \beta^{d/\beta}\, c_0$ resp. $c_2\, \beta \log(\beta) + 2\, \log(e)\, \beta^{d/\beta}\, c_0$. We wish to minimise both expressions (under the constraint that $\beta \geq 2$) and the optimal trade-off depends on c_0, c_1 and c_2. In particular, the

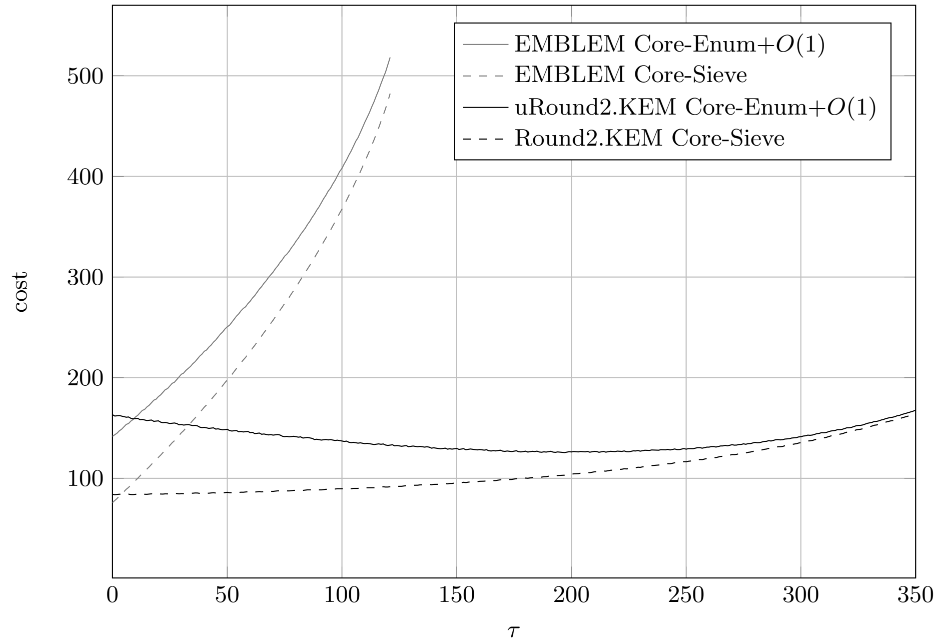

Fig. 1. Estimates of the cost of the primal attack when guessing τ secret entries for the schemes EMBLEM-611 and uRound2.KEM-500 using cost models Core-Enum+$O(1)$ and Core-Sieve.

optimal β in the sieving regime is not necessarily the optimal β in the enumeration regime.

We stress that while the above discussion gives an account of why our estimates show the behaviour we observe, it leaves the fundamental question partially unanswered: how does the security of the schemes considered in this work compare to one another. As it stands, the answer to this question depends on which between enumeration and sieving is the *correct* regime to consider for a given block size, i.e. from which dimension sieving beats enumeration. Thus, resolving this question is a pressing concern.

Multiple hardness assumptions. Lizard (RLizard) is based on two hardness assumptions: LWE (RLWE) and LWR (RLWR). Secret key recovery corresponds to the underlying LWE problem, and ephemeral key recovery corresponds to the underlying LWR problem. There are Lizard parameter sets for which ephemeral key recovery is harder than secret key recovery (i.e the underlying LWR problem is harder than the underlying

LWE problem), and there are also parameter sets for which the converse is true. To deal with this issue, for each parameter set, in each cost model, for each attack, we always choose the lower of the two possible costs.

Quantum security. In [Nat16], NIST defines five security categories that schemes should target in the presence of an adversary with access to a quantum computing device. They furthermore propose as a plausible assumption that such a device would support a maximum quantum circuit depth $\texttt{MAXDEPTH} \leq 2^{96}$ (although they do not mention a preferred set of universal gates to consider). Since concrete designs for large scale quantum computers are still an open research problem, not all schemes take this limitation into account, and many opt for using a (quantum) asymptotic cost model that considers the best known theoretical Grover speed-up, resulting in overestimates of the adversary's power.

This use of quantum cost models introduces a further difficulty when trying to compare schemes based on the outputs of the [APS15] estimator. For example, the security definition of Category 1 says that attacks on schemes should be as hard as AES128 key recovery. Some schemes address this by tuning their parameters to match hardness (using a quantum cost model) $\geq 2^{128}$, in the vein of "128 bit security". On the other hand, other schemes claiming the same category match hardness (using a quantum cost model) $\geq 2^{64}$ since key recovery on AES128 can be considered as a search problem in an unstructured list of size 2^{128}, which Grover can complete in $O(2^{n/2})$ time. This results in schemes with rather different cycle counts and memory usage claiming the same security category, as can be seen from the "claimed security" column in the estimates table.

Acknowledgements

We thank Jean-Philippe Aumasson, Paulo Barreto, Dan Bernstein, Leo Ducas, Mike Hamburg, Duhyeong Kim, Thijs Laarhoven, Vadim Lyubashevsky, Phong Nguyen and the anonymous reviewers for pointing out mistakes in earlier versions of this work.

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.

AKS01. Miklós Ajtai, Ravi Kumar, and D. Sivakumar. A sieve algorithm for the shortest lattice vector problem. In *33rd ACM STOC*, pages 601–610. ACM Press, July 2001.

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, April / 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.

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.

Ber18. Daniel J. Bernstein, 2018. Comment on PQC forum in response to an earlier version of this work. Available at `https://groups.google.com/a/list.nist.gov/d/msg/pqc-forum/h4_LCVNejCI/FyV5hgnqBAAJ`.

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.

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

CHK+17. Jung Hee Cheon, Kyoohyung Han, Jinsu Kim, Changmin Lee, and Yongha Son. A practical post-quantum public-key cryptosystem based on spLWE. In Seokhie Hong and Jong Hwan Park, editors, *ICISC 16*, volume 10157 of *LNCS*, pages 51–74. Springer, Heidelberg, November / December 2017.

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.

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.

HPS+15. Jeff Hoffstein, Jill Pipher, John M. Schanck, Joseph H. Silverman, William Whyte, and Zhenfei Zhang. Choosing parameters for NTRUEncrypt. Cryptology ePrint Archive, Report 2015/708, 2015. `http://eprint.iacr.org/2015/708`.

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.

KF17. Paul Kirchner and Pierre-Alain Fouque. Revisiting lattice attacks on overstretched NTRU parameters. In Jean-Sébastien Coron and Jesper Buus Nielsen, editors, *EUROCRYPT 2017, Part I*, volume 10210 of *LNCS*, pages 3–26. Springer, Heidelberg, April / May 2017.

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 / June 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.

Ngu18. P. Nguyen, 2018. Comment on PQC forum. Available at https://groups.google.com/a/list.nist.gov/forum/#!topic/pqc-forum/nZBIBvYmmUI.

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.

Sch03. Claus Peter Schnorr. Lattice reduction by random sampling and birthday methods. In *Annual Symposium on Theoretical Aspects of Computer Science*, pages 145–156. Springer, 2003.

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.

A Tables of Security estimates

We present the security estimates obtained, which can also be found at `https://estimate-all-the-lwe-ntru-schemes.github.io/`.

Scheme	Claim	NIST	Attack	0.265 β	0.265 β + 16.4	0.2975 β	0.265 β + log β	0.265 β + 16.4 + log (8d)	0.292 β	292 β + 16.4	0.368 β	0.292 β + log β	0.292 β + 16.4 + log (8d)
BabyBear-0624-0.79-1024	141.00	2	dual	180	192	197	186	205	193	206	232	203	218
BabyBear-0624-0.79-1024	141.00	2	primal	143	159	160	152	172	157	173	198	166	187
BabyBear-0624-1.00-1024	152.00	2	dual	193	206	211	202	218	207	223	253	216	231
BabyBear-0624-1.00-1024	152.00	2	primal	153	170	172	163	183	169	185	213	178	199
CRYSTALS-Dilithium-0768-3.74-8380417	91.00	1	dual	110	123	120	117	135	119	132	143	126	144
CRYSTALS-Dilithium-0768-3.74-8380417	91.00	1	primal	92	109	104	101	122	102	118	128	110	132
CRYSTALS-Dilithium-1024-3.16-8380417	125.00	2	dual	149	164	165	158	176	163	177	198	170	189
CRYSTALS-Dilithium-1024-3.16-8380417	125.00	2	primal	130	146	146	139	160	143	159	180	152	173
CRYSTALS-Dilithium-1280-2.00-8380417	158.00	3	dual	179	193	199	187	206	195	209	239	204	223
CRYSTALS-Dilithium-1280-2.00-8380417	158.00	3	primal	159	176	179	168	190	175	192	221	185	206
CRYSTALS-Kyber-0512-1.58-7681	102.00	1	dual	137	144	143	138	155	141	154	169	148	165
CRYSTALS-Kyber-0512-1.58-7681	102.00	1	primal	103	119	115	111	132	113	130	143	122	143
CRYSTALS-Kyber-0768-1.41-7681	161.00	3	dual	198	214	217	207	222	217	228	260	221	242
CRYSTALS-Kyber-0768-1.41-7681	161.00	3	primal	163	180	183	172	193	180	196	226	189	210
CRYSTALS-Kyber-1024-1.22-7681	218.00	5	dual	265	280	288	275	287	283	300	348	293	314
CRYSTALS-Kyber-1024-1.22-7681	218.00	5	primal	221	237	248	230	251	243	260	306	253	273
Ding Key Exchange-0512-4.19-120883	—	1	dual	116	129	128	123	140	126	139	150	132	149
Ding Key Exchange-0512-4.19-120883	—	1	primal	92	108	103	100	121	101	118	127	110	131
Ding Key Exchange-1024-2.60-120883	—	3, 5	dual	227	238	247	237	251	243	259	297	253	273
Ding Key Exchange-1024-2.60-120883	—	3, 5	primal	191	207	214	200	221	210	227	265	220	241
EMBLEM-0611-25.00-16777216	128.30	1	dual	85	98	93	91	109	91	105	110	98	115
EMBLEM-0611-25.00-16777216	128.30	1	primal	69	86	78	77	99	76	93	96	84	106
EMBLEM-0770-25.00-16777216	128.30	1	dual	103	117	114	110	129	112	126	135	119	138
EMBLEM-0770-25.00-16777216	128.30	1	primal	90	106	101	98	120	99	115	125	107	129
FireSaber-1024-2.29-8192	245.00	5	dual	308	325	339	318	339	338	347	413	341	361
FireSaber-1024-2.29-8192	245.00	5	primal	257	273	288	267	287	283	300	357	293	314
Frodo-0640-2.75-32768	103.00	1	dual	159	172	174	168	185	172	187	208	180	197
Frodo-0640-2.75-32768	103.00	1	primal	129	145	145	138	159	142	159	179	151	172
Frodo-0976-2.30-65536	150.00	3	dual	225	235	245	233	249	241	257	295	250	271
Frodo-0976-2.30-65536	150.00	3	primal	188	204	211	197	218	207	223	261	216	237
HILA5-1024-2.83-12289	255.00	5	dual	316	322	339	319	335	338	348	414	342	362
HILA5-1024-2.83-12289	255.00	5	primal	258	274	289	268	288	284	300	358	294	314
KCL-MLWE-0768-1.00-7681	147.00	4	dual	180	195	198	190	206	194	210	239	203	220
KCL-MLWE-0768-1.00-7681	147.00	4	primal	149	166	167	158	179	164	181	207	173	194
KCL-MLWE-0768-2.24-7681	183.00	4	dual	227	243	250	237	250	245	262	300	255	269
KCL-MLWE-0768-2.24-7681	183.00	4	primal	185	201	208	194	215	204	220	257	213	234
KCL-RLWE-1024-2.83-12289	255.00	5	dual	316	322	339	319	335	338	348	414	342	362

Scheme	Claim	NIST	Attack	$0.265\ \beta$	$0.265\ \beta + 16.4$	$0.2975\ \beta$	$0.265\ \beta + \log \beta$	$0.265\ \beta + 16.4 + \log(8d)$	$0.292\ \beta$	$292\ \beta + 16.4$	$0.368\ \beta$	$0.292\ \beta + \log \beta$	$0.292\ \beta + 16.4 + \log(8d)$
KCL-RLWE-1024-2.83-12289	255.00	5	primal	258	274	289	268	288	284	300	358	294	314
KINDI-0768-2.29-16384	164.00	2	dual	206	218	225	215	230	221	237	268	230	245
KINDI-0768-2.29-16384	164.00	2	primal	171	187	191	180	201	188	204	237	197	218
KINDI-1024-1.12-8192	207.00	4	dual	258	274	284	268	284	284	292	339	288	306
KINDI-1024-1.12-8192	207.00	4	primal	221	237	248	230	251	243	260	306	253	273
KINDI-1024-2.29-16384	232.00	4	dual	285	296	312	291	307	310	320	372	314	330
KINDI-1024-2.29-16384	232.00	4	primal	238	255	268	248	269	263	279	331	273	293
KINDI-1280-1.12-16384	251.00	5	dual	309	319	340	314	329	333	350	404	344	360
KINDI-1280-1.12-16384	251.00	5	primal	264	281	297	274	295	291	307	367	301	322
KINDI-1536-1.12-8192	330.00	5	dual	408	422	449	416	433	447	455	540	449	469
KINDI-1536-1.12-8192	330.00	5	primal	352	369	396	363	383	388	405	489	399	419
LAC-0512-0.71-251	128.00	1, 2	dual	178	190	195	183	199	191	203	231	197	213
LAC-0512-0.71-251	128.00	1, 2	primal	136	152	152	145	165	149	166	188	158	179
LAC-1024-0.50-251	192.00	3, 4	dual	327	343	354	337	348	349	364	422	358	378
LAC-1024-0.50-251	192.00	3, 4	primal	262	278	294	271	292	288	305	363	298	318
LAC-1024-0.71-251	256.00	5	dual	364	380	408	374	394	401	414	484	411	416
LAC-1024-0.71-251	256.00	5	primal	293	310	329	303	323	323	340	407	333	353
LIMA-2p-1024-3.16-133121	208.80	3	dual	237	246	258	240	260	253	269	310	263	281
LIMA-2p-1024-3.16-133121	208.80	3	primal	198	214	222	207	228	218	234	274	227	248
LIMA-2p-2048-3.16-184321	444.50	4	dual	493	510	554	504	525	544	560	652	554	575
LIMA-2p-2048-3.16-184321	444.50	4	primal	430	446	482	440	461	473	490	596	484	505
LIMA-sp-1018-3.16-12521473	139.20	1	dual	143	159	160	152	170	157	170	191	164	184
LIMA-sp-1018-3.16-12521473	139.20	1	primal	125	141	140	133	155	137	154	173	146	168
LIMA-sp-1306-3.16-48181249	167.80	2	dual	174	187	190	183	200	188	203	234	196	218
LIMA-sp-1306-3.16-48181249	167.80	2	primal	153	169	171	162	183	168	185	212	177	199
LIMA-sp-1822-3.16-44802049	247.90	3	dual	259	275	290	269	290	285	301	350	295	316
LIMA-sp-1822-3.16-44802049	247.90	3	primal	233	249	261	243	264	257	273	323	266	288
LIMA-sp-2062-3.16-16900097	303.50	4	dual	333	341	360	341	352	353	369	445	363	384
LIMA-sp-2062-3.16-16900097	303.50	4	primal	291	308	327	302	323	321	338	405	331	353
LOTUS-0576-3.00-8192	—	1, 2	dual	182	194	200	188	204	196	207	234	203	220
LOTUS-0576-3.00-8192	—	1, 2	primal	143	159	160	152	172	157	174	198	166	187
LOTUS-0704-3.00-8192	—	3, 4	dual	225	238	246	235	248	241	258	295	251	265
LOTUS-0704-3.00-8192	—	3, 4	primal	180	197	203	190	210	199	215	250	208	229
LOTUS-0832-3.00-8192	—	5	dual	270	281	298	275	295	293	307	348	302	313
LOTUS-0832-3.00-8192	—	5	primal	219	235	246	229	249	241	258	304	251	271
LightSaber-0512-2.29-8192	115.00	1	dual	153	158	169	153	169	169	170	188	169	182
LightSaber-0512-2.29-8192	115.00	1	primal	114	130	128	123	143	125	142	158	134	155

Scheme	Claim	NIST	Attack	$0.265\ \beta$	$0.265\ \beta + 16.4$	$0.2975\ \beta$	$0.265\ \beta + \log\beta$	$0.265\ \beta + 16.4 + \log(8d)$	$0.292\ \beta$	$292\ \beta + 16.4$	$0.368\ \beta$	$0.292\ \beta + \log\beta$	$0.292\ \beta + 16.4 + \log(8d)$
Lizard-1024-1.12-1024	131.00	1	dual	191	208	210	201	216	208	222	251	215	231
Lizard-1024-1.12-1024	131.00	1	primal	158	175	178	167	188	174	191	219	183	204
Lizard-1024-1.12-2048	130.00	1	dual	158	169	170	164	181	169	181	200	177	194
Lizard-1024-1.12-2048	130.00	1	primal	126	143	142	135	155	139	155	175	148	168
Lizard-1024-1.12-2048	193.00	3	dual	224	238	245	232	247	241	256	292	249	269
Lizard-1024-1.12-2048	193.00	3	primal	187	203	210	197	217	206	222	260	216	236
Lizard-1024-1.12-2048	195.00	3	dual	252	263	277	259	278	270	285	320	281	295
Lizard-1024-1.12-2048	195.00	3	primal	220	236	246	229	250	242	258	304	251	272
Lizard-2048-1.12-2048	264.00	5	dual	377	389	415	388	400	407	420	493	417	430
Lizard-2048-1.12-2048	264.00	5	primal	319	336	358	330	350	352	368	443	362	382
Lizard-2048-1.12-4096	257.00	5	dual	315	326	347	321	339	340	357	409	351	362
Lizard-2048-1.12-4096	257.00	5	primal	264	281	297	274	295	291	308	367	301	322
MamaBear-0936-0.71-1024	219.00	4	dual	273	282	298	275	295	292	309	352	302	317
MamaBear-0936-0.71-1024	219.00	4	primal	220	237	247	230	251	243	259	306	253	273
MamaBear-0936-0.94-1024	237.00	5	dual	294	310	327	304	321	321	331	387	331	341
MamaBear-0936-0.94-1024	237.00	5	primal	239	256	269	249	269	264	280	332	273	294
NTRU LPrime-0761-0.82-4591	225.00	5	dual	166	180	182	175	192	179	193	216	187	203
NTRU LPrime-0761-0.82-4591	225.00	5	primal	141	158	159	151	171	156	172	196	165	186
NewHope-0512-2.00-12289	101.00	1	dual	137	144	143	138	155	141	154	169	148	165
NewHope-0512-2.00-12289	101.00	1	primal	103	119	115	111	132	113	130	143	122	143
NewHope-1024-2.00-12289	233.00	5	dual	280	295	313	289	309	307	323	371	317	333
NewHope-1024-2.00-12289	233.00	5	primal	235	252	264	245	266	259	276	327	269	290
PapaBear-1248-0.61-1024	292.00	5	dual	350	366	388	360	380	381	398	462	392	412
PapaBear-1248-0.61-1024	292.00	5	primal	293	309	329	303	323	323	339	407	333	353
PapaBear-1248-0.87-1024	320.00	5	dual	390	406	437	400	420	429	446	525	440	456
PapaBear-1248-0.87-1024	320.00	5	primal	324	340	363	334	354	356	373	449	367	387
R EMBLEM-0512-25.00-65536	128.10	1	dual	126	139	138	133	150	135	149	164	143	160
R EMBLEM-0512-25.00-65536	128.10	1	primal	102	118	114	111	131	112	129	141	121	142
R EMBLEM-0512-3.00-16384	128.30	1	dual	113	126	123	120	136	122	135	146	129	146
R EMBLEM-0512-3.00-16384	128.30	1	primal	92	108	103	100	121	101	118	127	110	131
RLizard-1024-1.12-1024	147.00	1	dual	247	263	267	260	271	260	285	318	273	292
RLizard-1024-1.12-1024	147.00	1	primal	223	240	245	233	253	242	258	286	251	272
RLizard-1024-1.12-2048	195.00	3	dual	260	277	286	272	286	282	295	342	290	305
RLizard-1024-1.12-2048	195.00	3	primal	225	241	252	234	255	247	264	312	257	278
RLizard-2048-1.12-2048	291.00	3	dual	401	413	454	408	450	450	457	517	453	450
RLizard-2048-1.12-2048	291.00	3	primal	389	405	416	398	419	412	428	468	421	442
RLizard-2048-1.12-4096	318.00	5	dual	485	493	505	453	497	501	509	552	506	518

Scheme	Claim	NIST	Attack	0.265 β	0.265 $\beta + 16.4$	0.2975 β	0.265 $\beta + \log \beta$	0.265 $\beta + 16.4 + \log(8d)$	0.292 β	292 $\beta + 16.4$	0.368 β	0.292 $\beta + \log \beta$	0.292 $\beta + 16.4 + \log(8d)$
RLizard-2048-1.12-4096	318.00	5	primal	429	445	473	439	460	466	482	554	476	496
Saber-0768-2.29-8192	180.00	3	dual	226	242	249	236	250	244	261	299	254	268
Saber-0768-2.29-8192	180.00	3	primal	185	201	207	194	215	203	220	256	213	233
Titanium.KEM-1024-1.41-118273	128.00	1	dual	195	212	215	205	222	213	227	261	221	241
Titanium.KEM-1024-1.41-118273	128.00	1	primal	168	184	188	177	198	185	201	233	194	215
Titanium.KEM-1280-1.41-430081	160.00	1	dual	223	240	246	233	252	241	258	300	251	272
Titanium.KEM-1280-1.41-430081	160.00	1	primal	194	211	218	204	225	214	230	270	223	245
Titanium.KEM-1536-1.41-783361	192.00	3	dual	259	276	287	269	290	284	298	355	291	312
Titanium.KEM-1536-1.41-783361	192.00	3	primal	230	247	258	240	261	254	270	320	263	285
Titanium.KEM-2048-1.41-1198081	256.00	5	dual	350	366	392	360	381	385	401	483	395	416
Titanium.KEM-2048-1.41-1198081	256.00	5	primal	314	330	352	324	345	346	362	436	356	377
Titanium.PKE-1024-1.41-86017	128.00	1	dual	205	216	226	213	230	222	237	272	231	246
Titanium.PKE-1024-1.41-86017	128.00	1	primal	173	190	194	183	204	191	207	240	200	221
Titanium.PKE-1280-1.41-301057	160.00	1	dual	232	245	259	238	259	255	264	312	259	278
Titanium.PKE-1280-1.41-301057	160.00	1	primal	201	218	226	211	232	222	238	279	231	252
Titanium.PKE-1536-1.41-737281	192.00	3	dual	261	277	289	271	292	284	300	357	293	314
Titanium.PKE-1536-1.41-737281	192.00	3	primal	231	248	260	241	262	255	271	321	265	286
Titanium.PKE-2048-1.41-1198081	256.00	5	dual	350	366	392	360	381	385	401	483	395	416
Titanium.PKE-2048-1.41-1198081	256.00	5	primal	314	330	352	324	345	346	362	436	356	377
nRound2.KEM-0400-3.61-3209	74.00	1	dual	96	107	103	102	116	102	113	117	107	122
nRound2.KEM-0400-3.61-3209	74.00	1	primal	79	95	88	87	107	87	103	109	95	115
nRound2.KEM-0486-2.18-1949	97.00	2	dual	121	133	132	127	143	129	141	151	136	151
nRound2.KEM-0486-2.18-1949	97.00	2	primal	101	117	113	109	130	111	127	139	119	140
nRound2.KEM-0556-3.76-3343	106.00	3	dual	134	146	147	141	155	144	155	163	150	166
nRound2.KEM-0556-3.76-3343	106.00	3	primal	116	132	129	124	145	127	144	156	136	156
nRound2.KEM-0658-1.46-1319	139.00	4, 5	dual	169	181	185	177	192	181	194	214	189	205
nRound2.KEM-0658-1.46-1319	139.00	4, 5	primal	144	160	161	153	173	158	175	199	167	188
nRound2.PKE-0442-1.47-2659	74.00	1	dual	95	107	102	100	116	101	113	117	107	122
nRound2.PKE-0442-1.47-2659	74.00	1	primal	79	96	89	88	108	88	104	110	96	117
nRound2.PKE-0556-1.86-3343	97.00	2	dual	121	133	133	127	144	129	143	153	136	151
nRound2.PKE-0556-1.86-3343	97.00	2	primal	105	122	118	114	134	116	132	144	124	145
nRound2.PKE-0576-1.27-2309	106.00	3	dual	132	143	141	137	153	140	152	164	147	164
nRound2.PKE-0576-1.27-2309	106.00	3	primal	111	128	125	120	141	123	139	154	131	152
nRound2.PKE-0708-1.57-2837	138.00	4, 5	dual	166	180	181	174	191	180	193	212	189	206
nRound2.PKE-0708-1.57-2837	138.00	4, 5	primal	143	160	161	152	173	158	174	199	167	187
qTESLA-1024-8.49-8058881	128.00	1	dual	185	197	203	191	211	199	215	244	208	225
qTESLA-1024-8.49-8058881	128.00	1	primal	157	174	176	166	188	173	189	218	182	203

Scheme	Claim	NIST	Attack	$0.265\ \beta$	$0.265\ \beta + 16.4$	$0.2975\ \beta$	$0.265\ \beta + \log \beta$	$0.265\ \beta + 16.4 + \log(8d)$	$0.292\ \beta$	$292\ \beta + 16.4$	$0.368\ \beta$	$0.292\ \beta + \log \beta$	$0.292\ \beta + 16.4 + \log(8d)$
qTESLA-2048-8.49-12681217	192.00	3	dual	395	411	443	406	426	435	452	533	446	467
qTESLA-2048-8.49-12681217	192.00	3	primal	348	365	391	359	380	384	400	483	394	415
qTESLA-2048-8.49-27627521	256.00	5	dual	365	382	410	376	397	402	419	487	413	434
qTESLA-2048-8.49-27627521	256.00	5	primal	326	342	366	336	357	359	375	452	369	390
uRound2.KEM-0418-4.61-4096	75.00	1	dual	98	109	105	104	118	104	115	118	109	126
uRound2.KEM-0418-4.61-4096	75.00	1	primal	82	98	92	90	111	90	107	111	98	119
uRound2.KEM-0500-2.29-16384	74.00	1	dual	88	100	95	94	110	94	106	109	100	116
uRound2.KEM-0500-2.29-16384	74.00	1	primal	76	93	86	84	105	84	100	105	92	113
uRound2.KEM-0522-36.95-32768	97.00	2	dual	123	135	132	129	144	132	143	149	138	155
uRound2.KEM-0522-36.95-32768	97.00	2	primal	107	123	120	115	136	117	134	143	126	146
uRound2.KEM-0540-18.47-16384	106.00	3	dual	133	146	144	140	155	143	155	165	149	165
uRound2.KEM-0540-18.47-16384	106.00	3	primal	113	130	127	122	142	125	141	156	133	154
uRound2.KEM-0580-4.61-32768	96.00	2	dual	111	123	120	118	135	119	132	142	126	142
uRound2.KEM-0580-4.61-32768	96.00	2	primal	95	111	106	103	124	104	121	131	113	134
uRound2.KEM-0630-4.61-32768	106.00	3	dual	122	135	133	129	146	131	144	157	138	155
uRound2.KEM-0630-4.61-32768	106.00	3	primal	105	121	118	114	134	116	132	145	124	145
uRound2.KEM-0676-36.95-32768	139.00	5	dual	171	183	186	179	194	182	195	218	190	205
uRound2.KEM-0676-36.95-32768	139.00	5	primal	147	163	165	156	177	162	178	202	171	191
uRound2.KEM-0700-36.95-32768	140.00	4	dual	174	185	191	180	199	188	198	224	191	209
uRound2.KEM-0700-36.95-32768	140.00	4	primal	152	168	170	161	181	167	183	205	176	197
uRound2.KEM-0786-4.61-32768	138.00	5	dual	157	171	172	165	182	170	183	202	176	193
uRound2.KEM-0786-4.61-32768	138.00	5	primal	138	154	155	147	168	152	168	191	161	182
uRound2.KEM-0786-4.61-32768	139.00	4	dual	157	171	172	165	182	170	183	202	176	193
uRound2.KEM-0786-4.61-32768	139.00	4	primal	138	154	155	147	168	152	168	191	161	182
uRound2.PKE-0420-1.12-1024	74.00	1	dual	96	107	102	102	117	101	113	116	107	122
uRound2.PKE-0420-1.12-1024	74.00	1	primal	81	98	91	90	110	89	106	109	98	118
uRound2.PKE-0500-4.61-32768	74.00	1	dual	88	101	95	94	110	94	106	109	101	116
uRound2.PKE-0500-4.61-32768	74.00	1	primal	77	93	86	85	106	84	101	105	93	113
uRound2.PKE-0540-4.61-8192	97.00	2	dual	121	133	130	127	142	128	141	150	135	151
uRound2.PKE-0540-4.61-8192	97.00	2	primal	103	119	115	111	132	113	130	142	122	142
uRound2.PKE-0585-4.61-32768	96.00	2	dual	111	123	121	118	135	119	132	140	125	142
uRound2.PKE-0585-4.61-32768	96.00	2	primal	95	112	107	104	125	105	121	132	114	134
uRound2.PKE-0586-4.61-8192	107.00	3	dual	132	144	143	139	154	141	154	166	149	164
uRound2.PKE-0586-4.61-8192	107.00	3	primal	113	130	127	122	143	125	141	157	134	154
uRound2.PKE-0643-4.61-32768	106.00	3	dual	123	135	134	130	146	132	144	156	138	155
uRound2.PKE-0643-4.61-32768	106.00	3	primal	107	123	120	115	136	118	134	148	126	147
uRound2.PKE-0708-18.47-32768	138.00	4, 5	dual	167	180	181	174	191	179	193	213	186	202

Scheme	Claim	NIST	Attack	0.265 β	0.265 β + 16.4	0.2975 β	0.265 β + log β	0.265 β + 16.4 + log (8d)	0.292 β	292 β + 16.4	0.368 β	0.292 β + log β	0.292 β + 16.4 + log (8d)
uRound2.PKE-0708-18.47-32768	138.00	4, 5	primal	144	160	161	153	173	158	175	199	167	188
uRound2.PKE-0835-2.29-32768	138.00	4	dual	156	169	170	164	181	168	182	203	175	192
uRound2.PKE-0835-2.29-32768	138.00	4	primal	137	154	154	146	167	151	168	190	160	181
uRound2.PKE-0835-2.29-32768	138.00	5	dual	156	169	170	164	181	168	182	203	175	192
uRound2.PKE-0835-2.29-32768	138.00	5	primal	137	154	154	146	167	151	168	190	160	181

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	$0.265\ \beta$	$0.265\ \beta + 16.4$	$0.2975\ \beta$	$0.265\ \beta + \log\beta$	$0.265\ \beta + 16.4 + \log(8d)$	$0.292\ \beta$	$292\ \beta + 16.4$	$0.368\ \beta$	$0.292\ \beta + \log\beta$	$0.292\ \beta + 16.4 + \log(8d)$
BabyBear-0624-0.79-1024	141.00	2	dual	180	192	197	186	205	193	206	232	203	218
BabyBear-0624-0.79-1024	141.00	2	primal	143	159	160	152	172	157	173	198	166	187
BabyBear-0624-1.00-1024	152.00	2	dual	192	207	210	202	217	208	223	253	216	231
BabyBear-0624-1.00-1024	152.00	2	primal	153	170	172	163	183	169	185	213	178	199
CRYSTALS-Dilithium-0768-3.74-8380417	91.00	1	dual	108	121	118	114	133	116	130	141	123	142
CRYSTALS-Dilithium-0768-3.74-8380417	91.00	1	primal	91	108	103	100	121	101	117	127	109	131
CRYSTALS-Dilithium-1024-3.16-8380417	125.00	2	dual	148	162	164	156	175	161	175	196	168	188
CRYSTALS-Dilithium-1024-3.16-8380417	125.00	2	primal	129	146	145	138	160	142	159	179	151	173
CRYSTALS-Dilithium-1280-2.00-8380417	158.00	3	dual	178	194	197	187	206	195	210	239	203	222
CRYSTALS-Dilithium-1280-2.00-8380417	158.00	3	primal	159	175	178	168	190	175	192	221	184	206
CRYSTALS-Kyber-0512-1.58-7681	102.00	1	dual	130	143	141	136	154	139	152	167	147	163
CRYSTALS-Kyber-0512-1.58-7681	102.00	1	primal	103	119	115	111	132	113	130	143	122	143
CRYSTALS-Kyber-0768-1.41-7681	161.00	3	dual	196	212	220	206	222	216	227	258	221	241
CRYSTALS-Kyber-0768-1.41-7681	161.00	3	primal	163	180	183	172	193	180	196	226	189	210
CRYSTALS-Kyber-1024-1.22-7681	218.00	5	dual	264	280	288	274	287	286	298	345	292	312
CRYSTALS-Kyber-1024-1.22-7681	218.00	5	primal	221	237	248	230	251	243	260	306	253	273
Ding Key Exchange-0512-4.19-120883	—	1	dual	111	125	122	118	136	120	134	145	127	145
Ding Key Exchange-0512-4.19-120883	—	1	primal	90	106	101	98	119	99	115	125	107	128
Ding Key Exchange-1024-2.60-120883	—	3, 5	dual	222	236	246	230	250	245	255	296	248	269
Ding Key Exchange-1024-2.60-120883	—	3, 5	primal	190	207	214	200	221	210	226	264	219	240
EMBLEM-0611-25.00-16777216	128.30	1	dual	84	97	92	90	107	90	104	108	97	115
EMBLEM-0611-25.00-16777216	128.30	1	primal	69	86	78	77	99	76	93	96	84	106
EMBLEM-0770-25.00-16777216	128.30	1	dual	103	117	114	111	129	112	125	135	119	137
EMBLEM-0770-25.00-16777216	128.30	1	primal	90	106	101	98	120	99	115	125	107	129
FireSaber-1024-2.29-8192	245.00	5	dual	307	324	337	318	338	339	346	410	345	357
FireSaber-1024-2.29-8192	245.00	5	primal	257	273	288	267	287	283	300	357	293	314
Frodo-0640-2.75-32768	103.00	1	dual	155	170	172	163	180	170	182	204	175	193
Frodo-0640-2.75-32768	103.00	1	primal	128	144	144	137	158	141	157	178	150	171
Frodo-0976-2.30-65536	150.00	3	dual	223	233	242	229	247	241	253	290	246	267
Frodo-0976-2.30-65536	150.00	3	primal	188	204	211	197	218	207	223	261	216	237
HILA5-1024-2.83-12289	255.00	5	dual	306	322	344	316	337	337	348	409	347	356
HILA5-1024-2.83-12289	255.00	5	primal	257	273	288	267	287	283	300	357	293	314
KCL-MLWE-0768-1.00-7681	147.00	4	dual	180	196	197	187	205	194	210	238	203	220
KCL-MLWE-0768-1.00-7681	147.00	4	primal	149	166	167	158	179	164	181	207	173	194
KCL-MLWE-0768-2.24-7681	183.00	4	dual	224	237	248	231	251	243	258	295	253	267
KCL-MLWE-0768-2.24-7681	183.00	4	primal	185	201	207	194	215	203	220	256	213	233
KCL-RLWE-1024-2.83-12289	255.00	5	dual	306	322	344	316	337	337	348	409	347	356

Scheme	Claim	NIST	Attack	0.265 β	0.265 β + 16.4	0.2975 β	0.265 β + log β	0.265 β + 16.4 + log (8d)	0.292 β	292 β + 16.4	0.368 β	0.292 β + log β	0.292 β + 16.4 + log (8d)
KCL-RLWE-1024-2.83-12289	255.00	5	primal	257	273	288	267	287	283	300	357	293	314
KINDI-0768-2.29-16384	164.00	2	dual	202	217	221	211	227	218	233	265	226	246
KINDI-0768-2.29-16384	164.00	2	primal	170	186	191	179	200	187	203	236	196	217
KINDI-1024-1.12-8192	207.00	4	dual	257	274	284	267	284	283	293	339	288	305
KINDI-1024-1.12-8192	207.00	4	primal	221	237	248	230	251	243	260	306	253	273
KINDI-1024-2.29-16384	232.00	4	dual	279	292	307	286	306	302	317	369	313	327
KINDI-1024-2.29-16384	232.00	4	primal	238	255	267	248	269	262	279	331	272	293
KINDI-1280-1.12-16384	251.00	5	dual	309	320	340	314	329	333	347	404	344	360
KINDI-1280-1.12-16384	251.00	5	primal	264	281	297	274	295	291	307	367	301	322
KINDI-1536-1.12-8192	330.00	5	dual	408	422	449	416	433	447	455	540	449	469
KINDI-1536-1.12-8192	330.00	5	primal	352	369	396	363	383	388	405	489	399	419
LAC-0512-0.71-251	128.00	1, 2	dual	178	190	195	183	199	191	203	231	197	213
LAC-0512-0.71-251	128.00	1, 2	primal	136	152	152	145	165	149	166	188	158	179
LAC-1024-0.50-251	192.00	3, 4	dual	327	343	354	337	348	349	364	422	358	378
LAC-1024-0.50-251	192.00	3, 4	primal	262	278	294	271	292	288	305	363	298	318
LAC-1024-0.71-251	256.00	5	dual	364	380	408	374	394	401	414	484	411	416
LAC-1024-0.71-251	256.00	5	primal	293	310	329	303	323	323	340	407	333	353
LIMA-2p-1024-3.16-133121	208.80	3	dual	228	244	252	238	258	249	263	302	257	278
LIMA-2p-1024-3.16-133121	208.80	3	primal	196	213	220	206	227	216	233	272	226	247
LIMA-2p-2048-3.16-184321	444.50	4	dual	495	511	547	506	526	537	554	666	548	569
LIMA-2p-2048-3.16-184321	444.50	4	primal	429	446	482	440	461	473	489	596	484	504
LIMA-sp-1018-3.16-12521473	139.20	1	dual	141	157	157	151	169	154	170	190	163	181
LIMA-sp-1018-3.16-12521473	139.20	1	primal	124	140	139	133	154	136	153	172	145	167
LIMA-sp-1306-3.16-48181249	167.80	2	dual	171	187	192	180	199	188	201	232	198	215
LIMA-sp-1306-3.16-48181249	167.80	2	primal	152	169	171	162	183	168	184	211	177	199
LIMA-sp-1822-3.16-44802049	247.90	3	dual	260	272	287	265	287	281	298	349	291	313
LIMA-sp-1822-3.16-44802049	247.90	3	primal	232	249	261	242	264	256	272	322	266	287
LIMA-sp-2062-3.16-16900097	303.50	4	dual	322	337	360	331	352	360	366	440	361	381
LIMA-sp-2062-3.16-16900097	303.50	4	primal	291	308	327	301	323	321	337	404	331	352
LOTUS-0576-3.00-8192	—	1, 2	dual	176	188	191	182	199	189	203	230	196	213
LOTUS-0576-3.00-8192	—	1, 2	primal	141	158	159	151	171	156	172	196	165	186
LOTUS-0704-3.00-8192	—	3, 4	dual	221	232	242	225	245	237	252	287	247	261
LOTUS-0704-3.00-8192	—	3, 4	primal	179	196	201	189	209	197	214	249	207	227
LOTUS-0832-3.00-8192	—	5	dual	266	274	288	272	288	283	300	343	293	313
LOTUS-0832-3.00-8192	—	5	primal	218	234	244	227	248	240	256	302	249	270
LightSaber-0512-2.29-8192	115.00	1	dual	142	155	155	150	166	153	166	186	162	178
LightSaber-0512-2.29-8192	115.00	1	primal	113	130	127	122	143	125	141	157	134	154

Scheme	Claim	NIST	Attack	0.265 β	0.265 β + 16.4	0.2975 β	0.265 β + log β	0.265 β + 16.4 + log (8d)	0.292 β	292 β + 16.4	0.368 β	0.292 β + log β	0.292 β + 16.4 + log (8d)
Lizard-1024-1.12-1024	131.00	1	dual	191	207	210	201	216	209	222	251	215	231
Lizard-1024-1.12-1024	131.00	1	primal	158	175	178	167	188	174	191	219	183	204
Lizard-1024-1.12-2048	130.00	1	dual	157	170	172	163	180	169	182	202	175	190
Lizard-1024-1.12-2048	130.00	1	primal	126	143	142	135	155	139	155	175	148	168
Lizard-1024-1.12-2048	193.00	3	dual	226	236	245	231	250	242	255	292	249	269
Lizard-1024-1.12-2048	193.00	3	primal	187	203	210	197	217	206	222	260	216	236
Lizard-1024-1.12-2048	195.00	3	dual	252	263	277	259	278	270	285	320	281	295
Lizard-1024-1.12-2048	195.00	3	primal	220	236	246	229	250	242	258	304	251	272
Lizard-2048-1.12-2048	264.00	5	dual	377	389	415	388	400	407	420	493	417	430
Lizard-2048-1.12-2048	264.00	5	primal	319	336	358	330	350	352	368	443	362	382
Lizard-2048-1.12-4096	257.00	5	dual	314	331	344	324	339	340	352	409	347	365
Lizard-2048-1.12-4096	257.00	5	primal	264	281	297	274	295	291	308	367	301	322
MamaBear-0936-0.71-1024	219.00	4	dual	273	282	298	275	295	292	309	352	302	317
MamaBear-0936-0.71-1024	219.00	4	primal	220	237	247	230	251	243	259	306	253	273
MamaBear-0936-0.94-1024	237.00	5	dual	294	310	327	304	321	321	331	387	331	341
MamaBear-0936-0.94-1024	237.00	5	primal	239	256	269	249	269	264	280	332	273	294
NTRU LPrime-0761-0.82-4591	225.00	5	dual	166	180	182	175	192	179	193	216	187	203
NTRU LPrime-0761-0.82-4591	225.00	5	primal	141	158	159	151	171	156	172	196	165	186
NewHope-0512-2.00-12289	101.00	1	dual	128	142	140	135	153	138	151	168	146	163
NewHope-0512-2.00-12289	101.00	1	primal	103	119	115	111	132	113	130	143	122	143
NewHope-1024-2.00-12289	233.00	5	dual	283	295	309	293	304	304	320	374	314	334
NewHope-1024-2.00-12289	233.00	5	primal	235	252	264	245	266	259	276	327	269	290
PapaBear-1248-0.61-1024	292.00	5	dual	350	366	388	360	380	381	398	462	392	412
PapaBear-1248-0.61-1024	292.00	5	primal	293	309	329	303	323	323	339	407	333	353
PapaBear-1248-0.87-1024	320.00	5	dual	390	406	437	400	420	429	446	525	440	456
PapaBear-1248-0.87-1024	320.00	5	primal	324	340	363	334	354	356	373	449	367	387
R EMBLEM-0512-25.00-65536	128.10	1	dual	127	139	137	134	149	136	149	163	143	159
R EMBLEM-0512-25.00-65536	128.10	1	primal	102	118	114	111	131	112	129	141	121	142
R EMBLEM-0512-3.00-16384	128.30	1	dual	113	126	124	120	137	122	134	146	129	145
R EMBLEM-0512-3.00-16384	128.30	1	primal	92	108	103	100	121	101	118	127	110	131
RLizard-1024-1.12-1024	147.00	1	dual	247	263	267	260	271	260	285	318	273	292
RLizard-1024-1.12-1024	147.00	1	primal	223	240	245	233	253	242	258	286	251	272
RLizard-1024-1.12-2048	195.00	3	dual	260	277	286	272	286	282	295	342	290	305
RLizard-1024-1.12-2048	195.00	3	primal	225	241	252	234	255	247	264	312	257	278
RLizard-2048-1.12-2048	291.00	3	dual	401	413	454	408	450	450	457	517	453	450
RLizard-2048-1.12-2048	291.00	3	primal	389	405	416	398	419	412	428	468	421	442
RLizard-2048-1.12-4096	318.00	5	dual	485	493	505	453	497	501	509	552	506	518

Scheme	Claim	NIST	Attack	$0.265\,\beta$	$0.265\,\beta + 16.4$	$0.2975\,\beta$	$0.265\,\beta + \log\beta$	$0.265\,\beta + 16.4 + \log(8d)$	$0.292\,\beta$	$292\,\beta + 16.4$	$0.368\,\beta$	$0.292\,\beta + \log\beta$	$0.292\,\beta + 16.4 + \log(8d)$
RLizard-2048-1.12-4096	318.00	5	primal	429	445	473	439	460	466	482	554	476	496
Saber-0768-2.29-8192	180.00	3	dual	224	237	247	230	250	243	258	294	252	266
Saber-0768-2.29-8192	180.00	3	primal	184	201	207	194	214	203	219	256	212	233
Titanium.KEM-1024-1.41-118273	128.00	1	dual	194	210	217	203	224	214	228	260	223	239
Titanium.KEM-1024-1.41-118273	128.00	1	primal	168	184	188	177	198	185	201	233	194	215
Titanium.KEM-1280-1.41-430081	160.00	1	dual	222	238	245	231	253	244	260	299	254	268
Titanium.KEM-1280-1.41-430081	160.00	1	primal	194	211	218	204	225	214	230	270	223	245
Titanium.KEM-1536-1.41-783361	192.00	3	dual	262	278	289	272	293	289	297	353	291	312
Titanium.KEM-1536-1.41-783361	192.00	3	primal	230	247	258	240	261	254	270	320	263	285
Titanium.KEM-2048-1.41-1198081	256.00	5	dual	349	365	391	359	380	384	401	485	395	416
Titanium.KEM-2048-1.41-1198081	256.00	5	primal	314	330	352	324	345	346	362	436	356	377
Titanium.PKE-1024-1.41-86017	128.00	1	dual	202	219	223	212	229	219	235	271	228	249
Titanium.PKE-1024-1.41-86017	128.00	1	primal	173	190	194	183	204	191	207	240	200	221
Titanium.PKE-1280-1.41-301057	160.00	1	dual	231	247	255	241	260	250	267	311	260	281
Titanium.PKE-1280-1.41-301057	160.00	1	primal	201	218	226	211	232	222	238	279	231	252
Titanium.PKE-1536-1.41-737281	192.00	3	dual	264	280	289	274	295	284	300	356	294	315
Titanium.PKE-1536-1.41-737281	192.00	3	primal	231	248	260	241	262	255	271	321	265	286
Titanium.PKE-2048-1.41-1198081	256.00	5	dual	349	365	391	359	380	384	401	485	395	416
Titanium.PKE-2048-1.41-1198081	256.00	5	primal	314	330	352	324	345	346	362	436	356	377
nRound2.KEM-0400-3.61-3209	74.00	1	dual	96	107	103	101	116	102	113	117	107	122
nRound2.KEM-0400-3.61-3209	74.00	1	primal	79	95	88	87	107	87	103	109	95	115
nRound2.KEM-0486-2.18-1949	97.00	2	dual	121	133	131	128	143	129	143	153	135	151
nRound2.KEM-0486-2.18-1949	97.00	2	primal	101	117	113	109	130	111	127	139	119	140
nRound2.KEM-0556-3.76-3343	106.00	3	dual	135	145	145	141	157	143	157	164	150	164
nRound2.KEM-0556-3.76-3343	106.00	3	primal	116	132	129	124	145	127	144	156	136	156
nRound2.KEM-0658-1.46-1319	139.00	4, 5	dual	169	185	183	177	192	185	194	214	189	205
nRound2.KEM-0658-1.46-1319	139.00	4, 5	primal	144	160	161	153	173	158	175	199	167	188
nRound2.PKE-0442-1.47-2659	74.00	1	dual	94	107	102	100	116	100	113	117	107	122
nRound2.PKE-0442-1.47-2659	74.00	1	primal	79	96	89	88	108	88	104	110	96	117
nRound2.PKE-0556-1.86-3343	97.00	2	dual	121	134	130	129	144	129	143	150	136	151
nRound2.PKE-0556-1.86-3343	97.00	2	primal	105	122	118	114	134	116	132	144	124	145
nRound2.PKE-0576-1.27-2309	106.00	3	dual	130	143	141	137	153	140	152	164	147	162
nRound2.PKE-0576-1.27-2309	106.00	3	primal	111	128	125	120	141	123	139	154	131	152
nRound2.PKE-0708-1.57-2837	138.00	4, 5	dual	167	180	181	173	191	179	193	213	186	202
nRound2.PKE-0708-1.57-2837	138.00	4, 5	primal	143	160	161	152	173	158	174	199	167	187
qTESLA-1024-8.49-8058881	128.00	1	dual	179	191	196	184	205	192	208	238	201	218
qTESLA-1024-8.49-8058881	128.00	1	primal	154	170	173	163	184	170	186	214	179	200

Scheme	Claim	NIST	Attack	$0.265\ \beta$	$0.265\ \beta + 16.4$	$0.2975\ \beta$	$0.265\ \beta + \log\beta$	$0.265\ \beta + 16.4 + \log(8d)$	$0.292\ \beta$	$292\ \beta + 16.4$	$0.368\ \beta$	$0.292\ \beta + \log\beta$	$0.292\ \beta + 16.4 + \log(8d)$
qTESLA-2048-8.49-12681217	192.00	3	dual	381	397	427	391	412	420	436	532	430	451
qTESLA-2048-8.49-12681217	192.00	3	primal	344	361	387	355	376	380	396	478	390	411
qTESLA-2048-8.49-27627521	256.00	5	dual	368	376	396	376	385	389	406	490	400	421
qTESLA-2048-8.49-27627521	256.00	5	primal	322	339	362	333	354	355	372	448	366	387
uRound2.KEM-0418-4.61-4096	75.00	1	dual	98	108	104	103	118	105	117	118	109	124
uRound2.KEM-0418-4.61-4096	75.00	1	primal	82	98	92	90	111	90	107	111	98	119
uRound2.KEM-0500-2.29-16384	74.00	1	dual	88	100	95	94	110	94	106	109	100	116
uRound2.KEM-0500-2.29-16384	74.00	1	primal	76	93	86	84	105	84	100	105	92	113
uRound2.KEM-0522-36.95-32768	97.00	2	dual	122	135	132	129	146	133	144	151	139	155
uRound2.KEM-0522-36.95-32768	97.00	2	primal	107	123	120	115	136	117	134	143	126	146
uRound2.KEM-0540-18.47-16384	106.00	3	dual	134	145	144	141	155	142	154	165	149	164
uRound2.KEM-0540-18.47-16384	106.00	3	primal	113	130	127	122	142	125	141	156	133	154
uRound2.KEM-0580-4.61-32768	96.00	2	dual	111	124	120	118	134	119	132	141	126	142
uRound2.KEM-0580-4.61-32768	96.00	2	primal	95	111	106	103	124	104	121	131	113	134
uRound2.KEM-0630-4.61-32768	106.00	3	dual	122	136	133	129	146	131	145	158	138	157
uRound2.KEM-0630-4.61-32768	106.00	3	primal	105	121	118	114	134	116	132	145	124	145
uRound2.KEM-0676-36.95-32768	139.00	5	dual	170	183	185	178	193	182	196	213	190	205
uRound2.KEM-0676-36.95-32768	139.00	5	primal	147	163	165	156	177	162	178	202	171	191
uRound2.KEM-0700-36.95-32768	140.00	4	dual	175	186	187	181	195	191	201	216	191	207
uRound2.KEM-0700-36.95-32768	140.00	4	primal	152	168	170	161	181	167	183	205	176	197
uRound2.KEM-0786-4.61-32768	138.00	5	dual	157	171	172	165	183	170	183	203	180	194
uRound2.KEM-0786-4.61-32768	138.00	5	primal	138	154	155	147	168	152	168	191	161	182
uRound2.KEM-0786-4.61-32768	139.00	4	dual	157	171	172	165	183	170	183	203	180	194
uRound2.KEM-0786-4.61-32768	139.00	4	primal	138	154	155	147	168	152	168	191	161	182
uRound2.PKE-0420-1.12-1024	74.00	1	dual	96	107	102	102	117	101	113	116	107	122
uRound2.PKE-0420-1.12-1024	74.00	1	primal	81	98	91	90	110	89	106	109	98	118
uRound2.PKE-0500-4.61-32768	74.00	1	dual	89	100	95	95	110	95	106	112	100	117
uRound2.PKE-0500-4.61-32768	74.00	1	primal	77	93	86	85	106	84	101	105	93	113
uRound2.PKE-0540-4.61-8192	97.00	2	dual	120	133	131	127	144	130	141	150	135	151
uRound2.PKE-0540-4.61-8192	97.00	2	primal	103	119	115	111	132	113	130	142	122	142
uRound2.PKE-0585-4.61-32768	96.00	2	dual	111	124	121	118	134	119	132	141	125	142
uRound2.PKE-0585-4.61-32768	96.00	2	primal	95	112	107	104	125	105	121	132	114	134
uRound2.PKE-0586-4.61-8192	107.00	3	dual	132	145	144	138	155	142	154	165	148	164
uRound2.PKE-0586-4.61-8192	107.00	3	primal	113	130	127	122	143	125	141	157	134	154
uRound2.PKE-0643-4.61-32768	106.00	3	dual	122	136	134	129	146	133	145	155	138	155
uRound2.PKE-0643-4.61-32768	106.00	3	primal	107	123	120	115	136	118	134	148	126	147
uRound2.PKE-0708-18.47-32768	138.00	4, 5	dual	166	179	182	174	190	180	194	212	186	202

Scheme	Claim	NIST	Attack	0.265 β	0.265 β + 16.4	0.2975 β	0.265 β + log β	0.265 β + 16.4 + log (8d)	0.292 β	292 β + 16.4	0.368 β	0.292 β + log β	0.292 β + 16.4 + log (8d)
uRound2.PKE-0708-18.47-32768	138.00	4, 5	primal	144	160	161	153	173	158	175	199	167	188
uRound2.PKE-0835-2.29-32768	138.00	4	dual	156	170	171	163	180	169	181	200	175	193
uRound2.PKE-0835-2.29-32768	138.00	4	primal	137	154	154	146	167	151	168	190	160	181
uRound2.PKE-0835-2.29-32768	138.00	5	dual	156	170	171	163	180	169	181	200	175	193
uRound2.PKE-0835-2.29-32768	138.00	5	primal	137	154	154	146	167	151	168	190	160	181

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	$0.265\ \beta$	$0.265\ \beta + 16.4$	$0.2975\ \beta$	$0.265\ \beta + \log\beta$	$0.265\ \beta + 16.4 + \log(8d)$	$0.292\ \beta$	$292\ \beta + 16.4$	$0.368\ \beta$	$0.292\ \beta + \log\beta$	$0.292\ \beta + 16.4 + \log(8d)$
Falcon-0512-4.05-12289	103.00	1	primal	128	145	144	137	158	141	158	178	150	171
Falcon-0768-4.05-18433	172.00	2, 3	primal	193	210	217	203	223	213	229	268	223	243
Falcon-1024-2.87-12289	230.00	4, 5	primal	259	275	291	269	289	285	302	359	295	316
NTRU HRSS-0700-0.79-8192	123.00	1	primal	123	140	138	132	153	136	152	171	145	165
NTRUEncrypt-0443-0.80-2048	84.00	1	primal	85	101	95	93	114	93	109	117	101	123
NTRUEncrypt-0743-0.82-2048	159.00	1, 2, 3, 4, 5	primal	159	176	179	169	189	175	192	221	185	205
NTRUEncrypt-1024-724.00-1073750017	198.00	4, 5	primal	248	265	279	258	279	274	290	345	283	304
SNTRU Prime-0761-0.82-4591	248.00	5	primal	140	157	158	149	170	155	171	195	164	184
pqNTRUSign-1024-0.70-65537	149.00	1, 2, 3, 4, 5	primal	152	169	171	162	183	168	184	211	177	198

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 5.

Scheme	Claim	NIST	Attack	$\frac{1}{2}(0.187\beta\log\beta - 1.019\beta + 16.1)$	$0.125\beta\log\beta - 0.755\beta + 2.25$	$0.187\beta\log\beta - 1.019\beta + 16.1$	$0.000784\beta^2 + 0.366\beta - 0.9 + \log(8d)$
BabyBear-0624-0.79-1024	141.00	2	dual	257	289	409	473
BabyBear-0624-0.79-1024	141.00	2	primal	190	204	380	436
BabyBear-0624-1.00-1024	152.00	2	dual	297	297	442	553
BabyBear-0624-1.00-1024	152.00	2	primal	210	227	420	487
CRYSTALS-Dilithium-0768-3.74-8380417	91.00	1	dual	128	130	221	246
CRYSTALS-Dilithium-0768-3.74-8380417	91.00	1	primal	106	106	211	236
CRYSTALS-Dilithium-1024-3.16-8380417	125.00	2	dual	191	202	342	381
CRYSTALS-Dilithium-1024-3.16-8380417	125.00	2	primal	168	178	335	381
CRYSTALS-Dilithium-1280-2.00-8380417	158.00	3	dual	244	264	444	507
CRYSTALS-Dilithium-1280-2.00-8380417	158.00	3	primal	221	240	441	516
CRYSTALS-Kyber-0512-1.58-7681	102.00	1	dual	169	169	289	290
CRYSTALS-Kyber-0512-1.58-7681	102.00	1	primal	122	125	244	273
CRYSTALS-Kyber-0768-1.41-7681	161.00	3	dual	269	299	470	537
CRYSTALS-Kyber-0768-1.41-7681	161.00	3	primal	228	248	456	535
CRYSTALS-Kyber-1024-1.22-7681	218.00	5	dual	391	429	685	836
CRYSTALS-Kyber-1024-1.22-7681	218.00	5	primal	340	381	679	861
Ding Key Exchange-0512-4.19-120883	—	1	dual	154	163	229	250
Ding Key Exchange-0512-4.19-120883	—	1	primal	105	105	210	234
Ding Key Exchange-1024-2.60-120883	—	3, 5	dual	320	350	579	673
Ding Key Exchange-1024-2.60-120883	—	3, 5	primal	281	310	561	683
EMBLEM-0611-25.00-16777216	128.30	1	dual	91	90	152	169
EMBLEM-0611-25.00-16777216	128.30	1	primal	71	67	142	163
EMBLEM-0770-25.00-16777216	128.30	1	dual	118	120	207	229
EMBLEM-0770-25.00-16777216	128.30	1	primal	102	101	203	227
FireSaber-1024-2.29-8192	245.00	5	dual	478	528	829	1044
FireSaber-1024-2.29-8192	245.00	5	primal	414	469	828	1105
Frodo-0640-2.75-32768	103.00	1	dual	207	234	353	390
Frodo-0640-2.75-32768	103.00	1	primal	167	176	333	377
Frodo-0976-2.30-65536	150.00	3	dual	316	353	568	657
Frodo-0976-2.30-65536	150.00	3	primal	275	304	549	666
HILA5-1024-2.83-12289	255.00	5	dual	480	530	830	1052
HILA5-1024-2.83-12289	255.00	5	primal	416	471	832	1110
KCL-MLWE-0768-1.00-7681	147.00	4	dual	242	259	425	482
KCL-MLWE-0768-1.00-7681	147.00	4	primal	202	218	404	467
KCL-MLWE-0768-2.24-7681	183.00	4	dual	321	344	554	683
KCL-MLWE-0768-2.24-7681	183.00	4	primal	269	297	538	650
KCL-RLWE-1024-2.83-12289	255.00	5	dual	480	530	830	1052

Scheme	Claim	NIST	Attack	$\frac{1}{2}(0.187\beta\log\beta - 1.019\beta + 16.1)$	$0.125\beta\log\beta - 0.755\beta + 2.25$	$0.187\beta\log\beta - 1.019\beta + 16.1$	$0.000784\beta^2 + 0.366\beta - 0.9 + \log(8d)$
KCL-RLWE-1024-2.83-12289	255.00	5	primal	416	471	832	1110
KINDI-0768-2.29-16384	164.00	2	dual	298	325	487	598
KINDI-0768-2.29-16384	164.00	2	primal	242	265	484	573
KINDI-1024-1.12-8192	207.00	4	dual	378	413	687	875
KINDI-1024-1.12-8192	207.00	4	primal	340	381	679	861
KINDI-1024-2.29-16384	232.00	4	dual	420	469	739	916
KINDI-1024-2.29-16384	232.00	4	primal	376	424	751	977
KINDI-1280-1.12-16384	251.00	5	dual	472	519	839	1068
KINDI-1280-1.12-16384	251.00	5	primal	429	487	858	1156
KINDI-1536-1.12-8192	330.00	5	dual	673	761	1192	1780
KINDI-1536-1.12-8192	330.00	5	primal	622	718	1243	1882
LAC-0512-0.71-251	128.00	1, 2	dual	272	288	423	487
LAC-0512-0.71-251	128.00	1, 2	primal	178	190	356	405
LAC-1024-0.50-251	192.00	3, 4	dual	506	554	852	1297
LAC-1024-0.50-251	192.00	3, 4	primal	424	481	847	1137
LAC-1024-0.71-251	256.00	5	dual	565	682	970	1482
LAC-1024-0.71-251	256.00	5	primal	492	562	983	1377
LIMA-2p-1024-3.16-133121	208.80	3	dual	340	366	609	713
LIMA-2p-1024-3.16-133121	208.80	3	primal	294	326	587	722
LIMA-2p-2048-3.16-184321	444.50	4	dual	861	987	1585	2493
LIMA-2p-2048-3.16-184321	444.50	4	primal	800	933	1599	2665
LIMA-sp-1018-3.16-12521473	139.20	1	dual	185	193	331	371
LIMA-sp-1018-3.16-12521473	139.20	1	primal	159	167	317	358
LIMA-sp-1306-3.16-48181249	167.80	2	dual	235	257	436	488
LIMA-sp-1306-3.16-48181249	167.80	2	primal	209	225	417	484
LIMA-sp-1822-3.16-44802049	247.90	3	dual	403	445	750	937
LIMA-sp-1822-3.16-44802049	247.90	3	primal	364	410	728	940
LIMA-sp-2062-3.16-16900097	303.50	4	dual	533	612	1002	1312
LIMA-sp-2062-3.16-16900097	303.50	4	primal	488	557	975	1364
LOTUS-0576-3.00-8192	—	1, 2	dual	265	297	417	473
LOTUS-0576-3.00-8192	—	1, 2	primal	191	205	381	437
LOTUS-0704-3.00-8192	—	3, 4	dual	313	337	554	674
LOTUS-0704-3.00-8192	—	3, 4	primal	261	287	521	625
LOTUS-0832-3.00-8192	—	5	dual	400	429	682	813
LOTUS-0832-3.00-8192	—	5	primal	336	376	672	849
LightSaber-0512-2.29-8192	115.00	1	dual	183	224	303	332
LightSaber-0512-2.29-8192	115.00	1	primal	141	146	281	315

Scheme	Claim	NIST	Attack	$\frac{1}{2}(0.187\beta\log\beta - 1.019\beta + 16.1)$	$0.125\beta\log\beta - 0.755\beta + 2.25$	$0.187\beta\log\beta - 1.019\beta + 16.1$	$0.000784\beta^2 + 0.366\beta - 0.9 + \log(8d)$
Lizard-1024-1.12-1024	131.00	1	dual	289	289	371	386
Lizard-1024-1.12-1024	131.00	1	primal	219	237	372	391
Lizard-1024-1.12-2048	130.00	1	dual	198	204	321	344
Lizard-1024-1.12-2048	130.00	1	primal	162	170	322	362
Lizard-1024-1.12-2048	193.00	3	dual	312	334	491	520
Lizard-1024-1.12-2048	193.00	3	primal	273	302	480	505
Lizard-1024-1.12-2048	195.00	3	dual	338	355	491	520
Lizard-1024-1.12-2048	195.00	3	primal	318	336	480	505
Lizard-2048-1.12-2048	264.00	5	dual	581	602	706	703
Lizard-2048-1.12-2048	264.00	5	primal	533	552	695	720
Lizard-2048-1.12-4096	257.00	5	dual	476	539	653	670
Lizard-2048-1.12-4096	257.00	5	primal	430	488	664	689
MamaBear-0936-0.71-1024	219.00	4	dual	404	432	691	823
MamaBear-0936-0.71-1024	219.00	4	primal	339	380	678	859
MamaBear-0936-0.94-1024	237.00	5	dual	436	483	774	994
MamaBear-0936-0.94-1024	237.00	5	primal	378	425	755	982
NTRU LPrime-0761-0.82-4591	225.00	5	dual	219	232	365	404
NTRU LPrime-0761-0.82-4591	225.00	5	primal	189	202	365	398
NewHope-0512-2.00-12289	101.00	1	dual	169	169	289	290
NewHope-0512-2.00-12289	101.00	1	primal	122	125	244	273
NewHope-1024-2.00-12289	233.00	5	dual	429	475	755	936
NewHope-1024-2.00-12289	233.00	5	primal	369	416	738	955
PapaBear-1248-0.61-1024	292.00	5	dual	567	632	994	1291
PapaBear-1248-0.61-1024	292.00	5	primal	491	561	981	1375
PapaBear-1248-0.87-1024	320.00	5	dual	639	710	1134	1579
PapaBear-1248-0.87-1024	320.00	5	primal	558	641	1115	1627
R EMBLEM-0512-25.00-65536	128.10	1	dual	152	155	255	275
R EMBLEM-0512-25.00-65536	128.10	1	primal	121	123	242	270
R EMBLEM-0512-3.00-16384	128.30	1	dual	132	133	220	239
R EMBLEM-0512-3.00-16384	128.30	1	primal	105	105	210	234
RLizard-1024-1.12-1024	147.00	1	dual	325	305	371	384
RLizard-1024-1.12-1024	147.00	1	primal	272	276	370	390
RLizard-1024-1.12-2048	195.00	3	dual	369	412	596	579
RLizard-1024-1.12-2048	195.00	3	primal	346	378	570	609
RLizard-2048-1.12-2048	291.00	3	dual	498	512	587	605
RLizard-2048-1.12-2048	291.00	3	primal	466	476	593	615
RLizard-2048-1.12-4096	318.00	5	dual	615	652	963	864

Scheme	Claim	NIST	Attack	$\frac{1}{2}(0.187\beta \log \beta - 1.019\beta + 16.1)$	$0.125\beta \log \beta - 0.755\beta + 2.25$	$0.187\beta \log \beta - 1.019\beta + 16.1$	$0.000784\beta^2 + 0.366\beta - 0.9 + \log(8d)$
RLizard-2048-1.12-4096	318.00	5	primal	594	623	802	837
Saber-0768-2.29-8192	180.00	3	dual	320	343	555	640
Saber-0768-2.29-8192	180.00	3	primal	269	296	537	648
Titanium.KEM-1024-1.41-118273	128.00	1	dual	276	294	493	565
Titanium.KEM-1024-1.41-118273	128.00	1	primal	237	258	473	559
Titanium.KEM-1280-1.41-430081	160.00	1	dual	323	357	596	704
Titanium.KEM-1280-1.41-430081	160.00	1	primal	287	318	574	702
Titanium.KEM-1536-1.41-783361	192.00	3	dual	402	441	741	921
Titanium.KEM-1536-1.41-783361	192.00	3	primal	359	404	718	923
Titanium.KEM-2048-1.41-1198081	256.00	5	dual	595	652	1096	1474
Titanium.KEM-2048-1.41-1198081	256.00	5	primal	537	616	1073	1547
Titanium.PKE-1024-1.41-86017	128.00	1	dual	282	311	517	594
Titanium.PKE-1024-1.41-86017	128.00	1	primal	247	271	494	587
Titanium.PKE-1280-1.41-301057	160.00	1	dual	340	372	607	738
Titanium.PKE-1280-1.41-301057	160.00	1	primal	301	334	601	742
Titanium.PKE-1536-1.41-737281	192.00	3	dual	405	445	747	930
Titanium.PKE-1536-1.41-737281	192.00	3	primal	361	406	722	930
Titanium.PKE-2048-1.41-1198081	256.00	5	dual	595	652	1096	1474
Titanium.PKE-2048-1.41-1198081	256.00	5	primal	537	616	1073	1547
nRound2.KEM-0400-3.61-3209	74.00	1	dual	102	100	140	152
nRound2.KEM-0400-3.61-3209	74.00	1	primal	84	79	133	152
nRound2.KEM-0486-2.18-1949	97.00	2	dual	136	137	196	203
nRound2.KEM-0486-2.18-1949	97.00	2	primal	117	116	187	206
nRound2.KEM-0556-3.76-3343	106.00	3	dual	152	153	200	212
nRound2.KEM-0556-3.76-3343	106.00	3	primal	133	130	196	215
nRound2.KEM-0658-1.46-1319	139.00	4, 5	dual	207	211	315	338
nRound2.KEM-0658-1.46-1319	139.00	4, 5	primal	186	190	286	306
nRound2.PKE-0442-1.47-2659	74.00	1	dual	102	99	141	154
nRound2.PKE-0442-1.47-2659	74.00	1	primal	85	80	134	153
nRound2.PKE-0556-1.86-3343	97.00	2	dual	136	137	183	196
nRound2.PKE-0556-1.86-3343	97.00	2	primal	120	117	181	199
nRound2.PKE-0576-1.27-2309	106.00	3	dual	150	155	227	224
nRound2.PKE-0576-1.27-2309	106.00	3	primal	134	134	211	230
nRound2.PKE-0708-1.57-2837	138.00	4, 5	dual	203	210	334	319
nRound2.PKE-0708-1.57-2837	138.00	4, 5	primal	187	193	292	313
qTESLA-1024-8.49-8058881	128.00	1	dual	249	272	449	518
qTESLA-1024-8.49-8058881	128.00	1	primal	217	235	433	506

Scheme	Claim	NIST	Attack	$\frac{1}{2}(0.187\beta\log\beta - 1.019\beta + 16.1)$	$0.125\beta\log\beta - 0.755\beta + 2.25$	$0.187\beta\log\beta - 1.019\beta + 16.1$	$0.000784\beta^2 + 0.366\beta - 0.9 + \log(8d)$
qTESLA-2048-8.49-12681217	192.00	3	dual	658	762	1235	1783
qTESLA-2048-8.49-12681217	192.00	3	primal	612	707	1224	1847
qTESLA-2048-8.49-27627521	256.00	5	dual	628	697	1154	1590
qTESLA-2048-8.49-27627521	256.00	5	primal	563	647	1125	1649
uRound2.KEM-0418-4.61-4096	75.00	1	dual	102	101	142	148
uRound2.KEM-0418-4.61-4096	75.00	1	primal	86	80	131	150
uRound2.KEM-0500-2.29-16384	74.00	1	dual	93	90	127	144
uRound2.KEM-0500-2.29-16384	74.00	1	primal	80	75	126	145
uRound2.KEM-0522-36.95-32768	97.00	2	dual	133	133	177	189
uRound2.KEM-0522-36.95-32768	97.00	2	primal	119	114	173	192
uRound2.KEM-0540-18.47-16384	106.00	3	dual	156	152	206	237
uRound2.KEM-0540-18.47-16384	106.00	3	primal	134	132	204	223
uRound2.KEM-0580-4.61-32768	96.00	2	dual	125	126	192	203
uRound2.KEM-0580-4.61-32768	96.00	2	primal	109	110	188	207
uRound2.KEM-0630-4.61-32768	106.00	3	dual	141	143	227	224
uRound2.KEM-0630-4.61-32768	106.00	3	primal	126	128	213	232
uRound2.KEM-0676-36.95-32768	139.00	5	dual	212	210	301	295
uRound2.KEM-0676-36.95-32768	139.00	5	primal	187	189	278	297
uRound2.KEM-0700-36.95-32768	140.00	4	dual	207	212	279	286
uRound2.KEM-0700-36.95-32768	140.00	4	primal	187	188	271	290
uRound2.KEM-0786-4.61-32768	138.00	5	dual	194	202	296	306
uRound2.KEM-0786-4.61-32768	138.00	5	primal	181	188	294	314
uRound2.KEM-0786-4.61-32768	139.00	4	dual	194	202	296	306
uRound2.KEM-0786-4.61-32768	139.00	4	primal	181	188	294	314
uRound2.PKE-0420-1.12-1024	74.00	1	dual	100	101	136	143
uRound2.PKE-0420-1.12-1024	74.00	1	primal	84	78	126	145
uRound2.PKE-0500-4.61-32768	74.00	1	dual	93	90	129	144
uRound2.PKE-0500-4.61-32768	74.00	1	primal	80	75	126	146
uRound2.PKE-0540-4.61-8192	97.00	2	dual	135	136	192	201
uRound2.PKE-0540-4.61-8192	97.00	2	primal	120	118	187	206
uRound2.PKE-0585-4.61-32768	96.00	2	dual	125	125	185	198
uRound2.PKE-0585-4.61-32768	96.00	2	primal	110	110	184	203
uRound2.PKE-0586-4.61-8192	107.00	3	dual	154	156	211	222
uRound2.PKE-0586-4.61-8192	107.00	3	primal	136	135	210	229
uRound2.PKE-0643-4.61-32768	106.00	3	dual	141	141	202	223
uRound2.PKE-0643-4.61-32768	106.00	3	primal	128	128	205	224
uRound2.PKE-0708-18.47-32768	138.00	4, 5	dual	204	219	296	306

Scheme	Claim	NIST	Attack	$\frac{1}{2}(0.187\beta\log\beta - 1.019\beta + 16.1)$	$0.125\beta\log\beta - 0.755\beta + 2.25$	$0.187\beta\log\beta - 1.019\beta + 16.1$	$0.000784\beta^2 + 0.366\beta - 0.9 + \log(8d)$
uRound2.PKE-0708-18.47-32768	138.00	4, 5	primal	188	194	294	313
uRound2.PKE-0835-2.29-32768	138.00	4	dual	193	211	300	330
uRound2.PKE-0835-2.29-32768	138.00	4	primal	180	189	298	320
uRound2.PKE-0835-2.29-32768	138.00	5	dual	193	211	300	330
uRound2.PKE-0835-2.29-32768	138.00	5	primal	180	189	298	320

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	$\frac{1}{2}(0.187\beta\log\beta - 1.019\beta + 16.1)$	$0.125\beta\log\beta - 0.755\beta + 2.25$	$0.187\beta\log\beta - 1.019\beta + 16.1$	$0.000784\beta^2 + 0.366\beta - 0.9 + \log(8d)$
BabyBear-0624-0.79-1024	141.00	2	dual	257	289	409	473
BabyBear-0624-0.79-1024	141.00	2	primal	190	204	380	436
BabyBear-0624-1.00-1024	152.00	2	dual	297	297	442	553
BabyBear-0624-1.00-1024	152.00	2	primal	210	227	420	487
CRYSTALS-Dilithium-0768-3.74-8380417	91.00	1	dual	124	127	220	241
CRYSTALS-Dilithium-0768-3.74-8380417	91.00	1	primal	104	104	208	233
CRYSTALS-Dilithium-1024-3.16-8380417	125.00	2	dual	189	200	342	383
CRYSTALS-Dilithium-1024-3.16-8380417	125.00	2	primal	167	177	334	379
CRYSTALS-Dilithium-1280-2.00-8380417	158.00	3	dual	243	265	448	506
CRYSTALS-Dilithium-1280-2.00-8380417	158.00	3	primal	220	239	440	515
CRYSTALS-Kyber-0512-1.58-7681	102.00	1	dual	169	169	265	289
CRYSTALS-Kyber-0512-1.58-7681	102.00	1	primal	122	125	244	273
CRYSTALS-Kyber-0768-1.41-7681	161.00	3	dual	268	299	472	537
CRYSTALS-Kyber-0768-1.41-7681	161.00	3	primal	228	248	456	535
CRYSTALS-Kyber-1024-1.22-7681	218.00	5	dual	391	430	685	836
CRYSTALS-Kyber-1024-1.22-7681	218.00	5	primal	340	381	679	861
Ding Key Exchange-0512-4.19-120883	—	1	dual	138	138	224	241
Ding Key Exchange-0512-4.19-120883	—	1	primal	102	101	203	227
Ding Key Exchange-1024-2.60-120883	—	3, 5	dual	322	348	575	670
Ding Key Exchange-1024-2.60-120883	—	3, 5	primal	280	309	559	680
EMBLEM-0611-25.00-16777216	128.30	1	dual	90	89	151	168
EMBLEM-0611-25.00-16777216	128.30	1	primal	71	66	141	162
EMBLEM-0770-25.00-16777216	128.30	1	dual	119	121	208	227
EMBLEM-0770-25.00-16777216	128.30	1	primal	102	101	203	227
FireSaber-1024-2.29-8192	245.00	5	dual	479	521	834	1038
FireSaber-1024-2.29-8192	245.00	5	primal	414	469	828	1105
Frodo-0640-2.75-32768	103.00	1	dual	199	214	347	383
Frodo-0640-2.75-32768	103.00	1	primal	165	174	329	372
Frodo-0976-2.30-65536	150.00	3	dual	318	351	565	671
Frodo-0976-2.30-65536	150.00	3	primal	275	304	549	666
HILA5-1024-2.83-12289	255.00	5	dual	482	523	838	1040
HILA5-1024-2.83-12289	255.00	5	primal	414	469	828	1105
KCL-MLWE-0768-1.00-7681	147.00	4	dual	244	259	425	482
KCL-MLWE-0768-1.00-7681	147.00	4	primal	202	218	404	467
KCL-MLWE-0768-2.24-7681	183.00	4	dual	316	345	561	637
KCL-MLWE-0768-2.24-7681	183.00	4	primal	269	296	537	648
KCL-RLWE-1024-2.83-12289	255.00	5	dual	482	523	838	1040

Scheme	Claim	NIST	Attack	$\frac{1}{2}(0.187\beta\log\beta - 1.019\beta + 16.1)$	$0.125\beta\log\beta - 0.755\beta + 2.25$	$0.187\beta\log\beta - 1.019\beta + 16.1$	$0.000784\beta^2 + 0.366\beta - 0.9 + \log(8d)$
KCL-RLWE-1024-2.83-12289	255.00	5	primal	414	469	828	1105
KINDI-0768-2.29-16384	164.00	2	dual	278	320	480	565
KINDI-0768-2.29-16384	164.00	2	primal	241	263	481	569
KINDI-1024-1.12-8192	207.00	4	dual	378	413	687	875
KINDI-1024-1.12-8192	207.00	4	primal	340	381	679	861
KINDI-1024-2.29-16384	232.00	4	dual	417	464	738	907
KINDI-1024-2.29-16384	232.00	4	primal	375	423	750	975
KINDI-1280-1.12-16384	251.00	5	dual	472	519	839	1068
KINDI-1280-1.12-16384	251.00	5	primal	429	487	858	1156
KINDI-1536-1.12-8192	330.00	5	dual	673	761	1192	1780
KINDI-1536-1.12-8192	330.00	5	primal	622	718	1243	1882
LAC-0512-0.71-251	128.00	1, 2	dual	272	288	423	487
LAC-0512-0.71-251	128.00	1, 2	primal	178	190	356	405
LAC-1024-0.50-251	192.00	3, 4	dual	506	554	852	1297
LAC-1024-0.50-251	192.00	3, 4	primal	424	481	847	1137
LAC-1024-0.71-251	256.00	5	dual	565	682	970	1482
LAC-1024-0.71-251	256.00	5	primal	492	562	983	1377
LIMA-2p-1024-3.16-133121	208.80	3	dual	329	365	602	705
LIMA-2p-1024-3.16-133121	208.80	3	primal	291	323	582	714
LIMA-2p-2048-3.16-184321	444.50	4	dual	855	998	1585	2496
LIMA-2p-2048-3.16-184321	444.50	4	primal	799	932	1598	2662
LIMA-sp-1018-3.16-12521473	139.20	1	dual	181	193	331	366
LIMA-sp-1018-3.16-12521473	139.20	1	primal	157	166	314	355
LIMA-sp-1306-3.16-48181249	167.80	2	dual	232	255	431	492
LIMA-sp-1306-3.16-48181249	167.80	2	primal	208	225	416	483
LIMA-sp-1822-3.16-44802049	247.90	3	dual	399	448	745	939
LIMA-sp-1822-3.16-44802049	247.90	3	primal	363	409	726	937
LIMA-sp-2062-3.16-16900097	303.50	4	dual	529	607	970	1308
LIMA-sp-2062-3.16-16900097	303.50	4	primal	487	556	973	1362
LOTUS-0576-3.00-8192	—	1, 2	dual	234	274	398	441
LOTUS-0576-3.00-8192	—	1, 2	primal	189	202	377	431
LOTUS-0704-3.00-8192	—	3, 4	dual	303	337	536	625
LOTUS-0704-3.00-8192	—	3, 4	primal	258	284	516	618
LOTUS-0832-3.00-8192	—	5	dual	390	425	674	811
LOTUS-0832-3.00-8192	—	5	primal	333	373	666	841
LightSaber-0512-2.29-8192	115.00	1	dual	176	186	299	328
LightSaber-0512-2.29-8192	115.00	1	primal	140	145	279	313

Scheme	Claim	NIST	Attack	$\frac{1}{2}(0.187\beta\log\beta - 1.019\beta + 16.1)$	$0.125\beta\log\beta - 0.755\beta + 2.25$	$0.187\beta\log\beta - 1.019\beta + 16.1$	$0.000784\beta^2 + 0.366\beta - 0.9 + \log(8d)$
Lizard-1024-1.12-1024	131.00	1	dual	289	289	371	386
Lizard-1024-1.12-1024	131.00	1	primal	219	237	372	391
Lizard-1024-1.12-2048	130.00	1	dual	195	208	318	347
Lizard-1024-1.12-2048	130.00	1	primal	162	170	322	362
Lizard-1024-1.12-2048	193.00	3	dual	312	334	491	520
Lizard-1024-1.12-2048	193.00	3	primal	273	302	480	505
Lizard-1024-1.12-2048	195.00	3	dual	338	355	491	520
Lizard-1024-1.12-2048	195.00	3	primal	318	336	480	505
Lizard-2048-1.12-2048	264.00	5	dual	581	602	706	703
Lizard-2048-1.12-2048	264.00	5	primal	533	552	695	720
Lizard-2048-1.12-4096	257.00	5	dual	474	517	653	670
Lizard-2048-1.12-4096	257.00	5	primal	430	488	664	689
MamaBear-0936-0.71-1024	219.00	4	dual	404	432	691	823
MamaBear-0936-0.71-1024	219.00	4	primal	339	380	678	859
MamaBear-0936-0.94-1024	237.00	5	dual	436	483	774	994
MamaBear-0936-0.94-1024	237.00	5	primal	378	425	755	982
NTRU LPrime-0761-0.82-4591	225.00	5	dual	219	232	365	404
NTRU LPrime-0761-0.82-4591	225.00	5	primal	189	202	365	398
NewHope-0512-2.00-12289	101.00	1	dual	161	169	263	289
NewHope-0512-2.00-12289	101.00	1	primal	122	125	244	273
NewHope-1024-2.00-12289	233.00	5	dual	429	477	753	936
NewHope-1024-2.00-12289	233.00	5	primal	369	416	738	955
PapaBear-1248-0.61-1024	292.00	5	dual	567	632	994	1291
PapaBear-1248-0.61-1024	292.00	5	primal	491	561	981	1375
PapaBear-1248-0.87-1024	320.00	5	dual	639	710	1134	1579
PapaBear-1248-0.87-1024	320.00	5	primal	558	641	1115	1627
R EMBLEM-0512-25.00-65536	128.10	1	dual	151	155	247	265
R EMBLEM-0512-25.00-65536	128.10	1	primal	121	123	242	270
R EMBLEM-0512-3.00-16384	128.30	1	dual	131	134	221	240
R EMBLEM-0512-3.00-16384	128.30	1	primal	105	105	210	234
RLizard-1024-1.12-1024	147.00	1	dual	325	305	371	384
RLizard-1024-1.12-1024	147.00	1	primal	272	276	370	390
RLizard-1024-1.12-2048	195.00	3	dual	369	412	596	579
RLizard-1024-1.12-2048	195.00	3	primal	346	378	570	609
RLizard-2048-1.12-2048	291.00	3	dual	498	512	587	605
RLizard-2048-1.12-2048	291.00	3	primal	466	476	593	615
RLizard-2048-1.12-4096	318.00	5	dual	615	652	963	864

Scheme	Claim	NIST	Attack	$\frac{1}{2}(0.187\beta\log\beta - 1.019\beta + 16.1)$	$0.125\beta\log\beta - 0.755\beta + 2.25$	$0.187\beta\log\beta - 1.019\beta + 16.1$	$0.000784\beta^2 + 0.366\beta - 0.9 + \log(8d)$
RLizard-2048-1.12-4096	318.00	5	primal	594	623	802	837
Saber-0768-2.29-8192	180.00	3	dual	314	345	559	635
Saber-0768-2.29-8192	180.00	3	primal	268	295	535	645
Titanium.KEM-1024-1.41-118273	128.00	1	dual	274	293	493	565
Titanium.KEM-1024-1.41-118273	128.00	1	primal	237	258	473	559
Titanium.KEM-1280-1.41-430081	160.00	1	dual	323	360	598	704
Titanium.KEM-1280-1.41-430081	160.00	1	primal	287	318	574	702
Titanium.KEM-1536-1.41-783361	192.00	3	dual	405	447	741	921
Titanium.KEM-1536-1.41-783361	192.00	3	primal	359	404	718	923
Titanium.KEM-2048-1.41-1198081	256.00	5	dual	595	652	1096	1474
Titanium.KEM-2048-1.41-1198081	256.00	5	primal	537	616	1073	1547
Titanium.PKE-1024-1.41-86017	128.00	1	dual	282	312	518	594
Titanium.PKE-1024-1.41-86017	128.00	1	primal	247	271	494	587
Titanium.PKE-1280-1.41-301057	160.00	1	dual	340	372	606	738
Titanium.PKE-1280-1.41-301057	160.00	1	primal	301	334	601	742
Titanium.PKE-1536-1.41-737281	192.00	3	dual	406	451	747	930
Titanium.PKE-1536-1.41-737281	192.00	3	primal	361	406	722	930
Titanium.PKE-2048-1.41-1198081	256.00	5	dual	595	652	1096	1474
Titanium.PKE-2048-1.41-1198081	256.00	5	primal	537	616	1073	1547
nRound2.KEM-0400-3.61-3209	74.00	1	dual	102	100	140	160
nRound2.KEM-0400-3.61-3209	74.00	1	primal	84	79	133	152
nRound2.KEM-0486-2.18-1949	97.00	2	dual	139	142	196	203
nRound2.KEM-0486-2.18-1949	97.00	2	primal	117	116	187	206
nRound2.KEM-0556-3.76-3343	106.00	3	dual	151	153	200	212
nRound2.KEM-0556-3.76-3343	106.00	3	primal	133	130	196	215
nRound2.KEM-0658-1.46-1319	139.00	4, 5	dual	207	211	315	338
nRound2.KEM-0658-1.46-1319	139.00	4, 5	primal	186	190	286	306
nRound2.PKE-0442-1.47-2659	74.00	1	dual	102	99	141	154
nRound2.PKE-0442-1.47-2659	74.00	1	primal	85	80	134	153
nRound2.PKE-0556-1.86-3343	97.00	2	dual	136	137	183	196
nRound2.PKE-0556-1.86-3343	97.00	2	primal	120	117	181	199
nRound2.PKE-0576-1.27-2309	106.00	3	dual	150	155	227	224
nRound2.PKE-0576-1.27-2309	106.00	3	primal	134	134	211	230
nRound2.PKE-0708-1.57-2837	138.00	4, 5	dual	203	210	334	319
nRound2.PKE-0708-1.57-2837	138.00	4, 5	primal	187	193	292	313
qTESLA-1024-8.49-8058881	128.00	1	dual	243	257	436	501
qTESLA-1024-8.49-8058881	128.00	1	primal	211	228	422	490

Scheme	Claim	NIST	Attack	$\frac{1}{2}(0.187\beta\log\beta - 1.019\beta + 16.1)$	$0.125\beta\log\beta - 0.755\beta + 2.25$	$0.187\beta\log\beta - 1.019\beta + 16.1$	$0.000784\beta^2 + 0.366\beta - 0.9 + \log(8d)$
qTESLA-2048-8.49-12681217	192.00	3	dual	670	744	1241	1700
qTESLA-2048-8.49-12681217	192.00	3	primal	604	697	1208	1813
qTESLA-2048-8.49-27627521	256.00	5	dual	611	690	1136	1538
qTESLA-2048-8.49-27627521	256.00	5	primal	555	638	1110	1619
uRound2.KEM-0418-4.61-4096	75.00	1	dual	102	100	142	148
uRound2.KEM-0418-4.61-4096	75.00	1	primal	86	80	131	150
uRound2.KEM-0500-2.29-16384	74.00	1	dual	93	90	127	144
uRound2.KEM-0500-2.29-16384	74.00	1	primal	80	75	126	145
uRound2.KEM-0522-36.95-32768	97.00	2	dual	134	135	177	194
uRound2.KEM-0522-36.95-32768	97.00	2	primal	119	114	173	192
uRound2.KEM-0540-18.47-16384	106.00	3	dual	153	154	206	225
uRound2.KEM-0540-18.47-16384	106.00	3	primal	134	132	204	223
uRound2.KEM-0580-4.61-32768	96.00	2	dual	127	126	192	203
uRound2.KEM-0580-4.61-32768	96.00	2	primal	109	110	188	207
uRound2.KEM-0630-4.61-32768	106.00	3	dual	142	143	213	224
uRound2.KEM-0630-4.61-32768	106.00	3	primal	126	128	213	232
uRound2.KEM-0676-36.95-32768	139.00	5	dual	204	208	279	352
uRound2.KEM-0676-36.95-32768	139.00	5	primal	187	189	278	297
uRound2.KEM-0700-36.95-32768	140.00	4	dual	224	210	326	286
uRound2.KEM-0700-36.95-32768	140.00	4	primal	187	188	271	290
uRound2.KEM-0786-4.61-32768	138.00	5	dual	195	205	296	306
uRound2.KEM-0786-4.61-32768	138.00	5	primal	181	188	294	314
uRound2.KEM-0786-4.61-32768	139.00	4	dual	195	205	296	306
uRound2.KEM-0786-4.61-32768	139.00	4	primal	181	188	294	314
uRound2.PKE-0420-1.12-1024	74.00	1	dual	100	101	136	143
uRound2.PKE-0420-1.12-1024	74.00	1	primal	84	78	126	145
uRound2.PKE-0500-4.61-32768	74.00	1	dual	92	91	129	144
uRound2.PKE-0500-4.61-32768	74.00	1	primal	80	75	126	146
uRound2.PKE-0540-4.61-8192	97.00	2	dual	135	135	200	201
uRound2.PKE-0540-4.61-8192	97.00	2	primal	120	118	187	206
uRound2.PKE-0585-4.61-32768	96.00	2	dual	124	127	185	198
uRound2.PKE-0585-4.61-32768	96.00	2	primal	110	110	184	203
uRound2.PKE-0586-4.61-8192	107.00	3	dual	152	154	211	222
uRound2.PKE-0586-4.61-8192	107.00	3	primal	136	135	210	229
uRound2.PKE-0643-4.61-32768	106.00	3	dual	141	142	202	223
uRound2.PKE-0643-4.61-32768	106.00	3	primal	128	128	205	224
uRound2.PKE-0708-18.47-32768	138.00	4, 5	dual	204	209	293	306

Scheme	Claim	NIST	Attack	$\frac{1}{2}(0.187\beta\log\beta - 1.019\beta + 16.1)$	$0.125\beta\log\beta - 0.755\beta + 2.25$	$0.187\beta\log\beta - 1.019\beta + 16.1$	$0.000784\beta^2 + 0.366\beta - 0.9 + \log(8d)$
uRound2.PKE-0708-18.47-32768	138.00	4, 5	primal	188	194	294	313
uRound2.PKE-0835-2.29-32768	138.00	4	dual	194	200	300	330
uRound2.PKE-0835-2.29-32768	138.00	4	primal	180	189	298	320
uRound2.PKE-0835-2.29-32768	138.00	5	dual	194	200	300	330
uRound2.PKE-0835-2.29-32768	138.00	5	primal	180	189	298	320

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	$\frac{1}{2}(0.187\beta\log\beta - 1.019\beta + 16.1)$	$0.125\beta\log\beta - 0.755\beta + 2.25$	$0.187\beta\log\beta - 1.019\beta + 16.1$	$0.000784\beta^2 + 0.366\beta - 0.9 + \log(8d)$
Falcon-0512-4.05-12289	103.00	1	primal	165	175	330	373
Falcon-0768-4.05-18433	172.00	2, 3	primal	286	316	571	697
Falcon-1024-2.87-12289	230.00	4, 5	primal	418	474	836	1118
NTRU HRSS-0700-0.79-8192	123.00	1	primal	157	165	313	350
NTRUEncrypt-0443-0.80-2048	84.00	1	primal	93	92	186	208
NTRUEncrypt-0743-0.82-2048	159.00	1, 2, 3, 4, 5	primal	221	240	441	516
NTRUEncrypt-1024-724.00-1073750017	198.00	4, 5	primal	396	448	792	1043
SNTRU Prime-0761-0.82-4591	248.00	5	primal	187	200	370	410
pqNTRUSign-1024-0.70-65537	149.00	1, 2, 3, 4, 5	primal	208	225	416	480

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 5.