Evaluating ML-KEM at (much) higher security levels

Swechchha Adhikari[1] Vadim Lyubashevsky[2] Peter Schwabe[1,3]

[1]Max Planck Institute for Security and Privacy, Bochum, Germany

[2]IBM Research, Zurich, Switzerland

[3]Radboud University, Nijmegen, The Netherlands

July 6, 2026

About Me

- Math & Computer Science undergraduate at BYU, United States
- Intern at MPI-SP, supervised by Peter Schwabe

About Me

- Math & Computer Science undergraduate at BYU, United States
- Intern at MPI-SP, supervised by Peter Schwabe
- From Nepal

Motivation

20 October 2025

What is post-quantum cryptography? Everything you need to know about this looming threat

Quantum computing could easily conquer some encryption methods, including those that protect banking data. The financial industry needs to prepare.

Motivation

20 October 2025

What is post-quantum cryptography? Everything you need to know about this looming threat

Quantum computing could easily conquer some encryption methods, including those that protect banking data. The financial industry needs to prepare.

The future of computing is quantum-centric

Updated March 2026

In Progress

2030

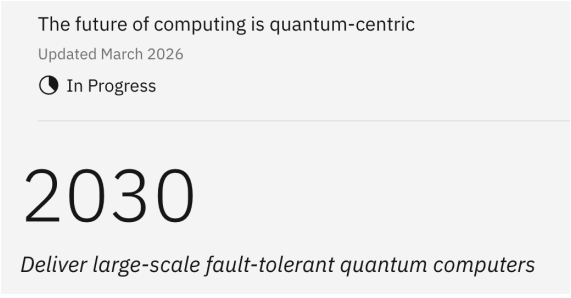
Deliver large-scale fault-tolerant quantum computers

Motivation

20 October 2025

What is post-quantum cryptography? Everything you need to know about this looming threat

Quantum computing could easily conquer some encryption methods, including those that protect banking data. The financial industry needs to prepare.



The future of computing is quantum-centric

Updated March 2026

In Progress

2030

Deliver large-scale fault-tolerant quantum computers

NIST Announces First Four Quantum-Resistant Cryptographic Algorithms

Federal agency reveals the first group of winners from its six-year competition.

- Kyber or ML-KEM
- **Goal**: push to much higher security levels

Scaling up

Table 1: Parameter sets for KYBER

	n	k	q	η_1	η_2	(d_u, d_v)	δ
KYBER512	256	2	3329	3	2	$(10, 4)$	2^{-139}
KYBER768	256	3	3329	2	2	$(10, 4)$	2^{-164}
KYBER1024	256	4	3329	2	2	$(11, 5)$	2^{-174}

Scaling up

Table 1: Parameter sets for KYBER

	n	k	q	η_1	η_2	(d_u, d_v)	δ
KYBER512	256	2	3329	3	2	$(10, 4)$	2^{-139}
KYBER768	256	3	3329	2	2	$(10, 4)$	2^{-164}
KYBER1024	256	4	3329	2	2	$(11, 5)$	2^{-174}

	KYBER512	KYBER768	KYBER1024
NIST Security level	1	3	5

Scaling up

Table 1: Parameter sets for KYBER

	n	k	q	η_1	η_2	(d_u, d_v)	δ
KYBER512	256	2	3329	3	2	$(10, 4)$	2^{-139}
KYBER768	256	3	3329	2	2	$(10, 4)$	2^{-164}
KYBER1024	256	4	3329	2	2	$(11, 5)$	2^{-174}

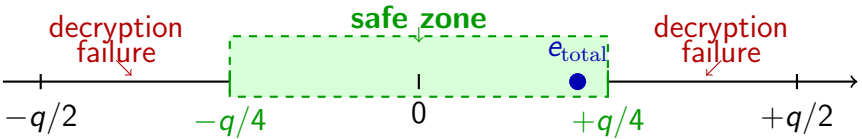
	KYBER512	KYBER768	KYBER1024
NIST Security level	1	3	5

Correctness: the other constraint

- Encryption $\implies$ noise from multiple sources
  - key error, ciphertext error, rounding
- Decryption $\implies$ canceling out all those errors

Correctness: the other constraint

- Encryption $\implies$ noise from multiple sources
  - key error, ciphertext error, rounding
- Decryption $\implies$ canceling out all those errors

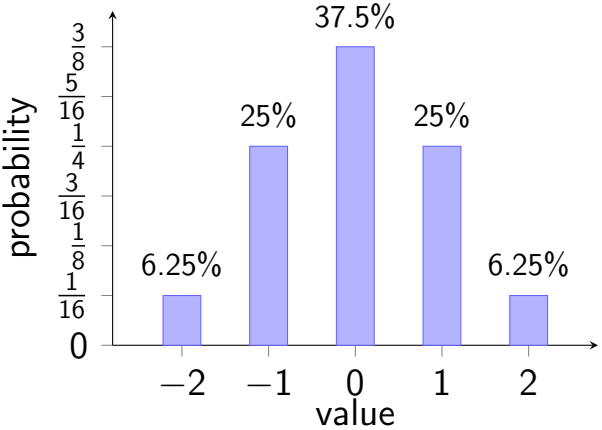


CBD: the problem

- Increase k in Kyber $\implies$ decryption failure probability worsens
- Explodes at $k = 8$

CBD: the problem

- Increase k in Kyber $\implies$ decryption failure probability worsens
- Explodes at $k = 8$



- Rigid probability distribution

The distribution $f(n)$

- Support: $\{-2, -1, 0, 1, 2\}$
- $\Pr[\pm 2] = 2^{-n}$, tunable via n

The distribution $f(n)$

- Support: $\{-2, -1, 0, 1, 2\}$
- $\Pr[\pm 2] = 2^{-n}$, tunable via n
- n's competing effects:
  - Larger n: lighter noise $\Rightarrow$ failure prob decreases ✓

The distribution $f(n)$

- Support: $\{-2, -1, 0, 1, 2\}$
- $\Pr[\pm 2] = 2^{-n}$, tunable via n
- n's competing effects:
  - Larger n: lighter noise $\Rightarrow$ failure prob decreases ✓
  - Larger n: lighter noise $\Rightarrow$ bit security decreases $\times$
- Can scale up to $k = 29$

Parameter sets

k	q	n	δ
7	3329	4	$2^{-133.7}$
18	3329	6	$2^{-134.1}$
24	3329	8	$2^{-139.9}$

Table: Candidate parameter sets using $f(n)$ with no compression applied

[0] δ denotes the decryption failure probability.

Parameter sets

k	q	n	δ
7	3329	4	$2^{-133.7}$
18	3329	6	$2^{-134.1}$
24	3329	8	$2^{-139.9}$

Table: Candidate parameter sets using $f(n)$ with no compression applied

- Future steps: implementation in Jasmin, benchmark on Pavona, formally-verified correctness bounds in EasyCrypt

[0] δ denotes the decryption failure probability.