NIST Upcoming Primary Standards: Kyber & Dilithium

Léo Ducas

Centrum Wiskunde & Informatica, Amsterdam
Leiden University, Mathematical Institute

Symposium on Post-Quantum Cryptography, Episode 4,
November 15, 2022

Cryptographic Suite for Algebraic Lattices (CRYSTALS)

https://pq-crystals.org/

CWI

ENS DE LYON

IBM

NXP

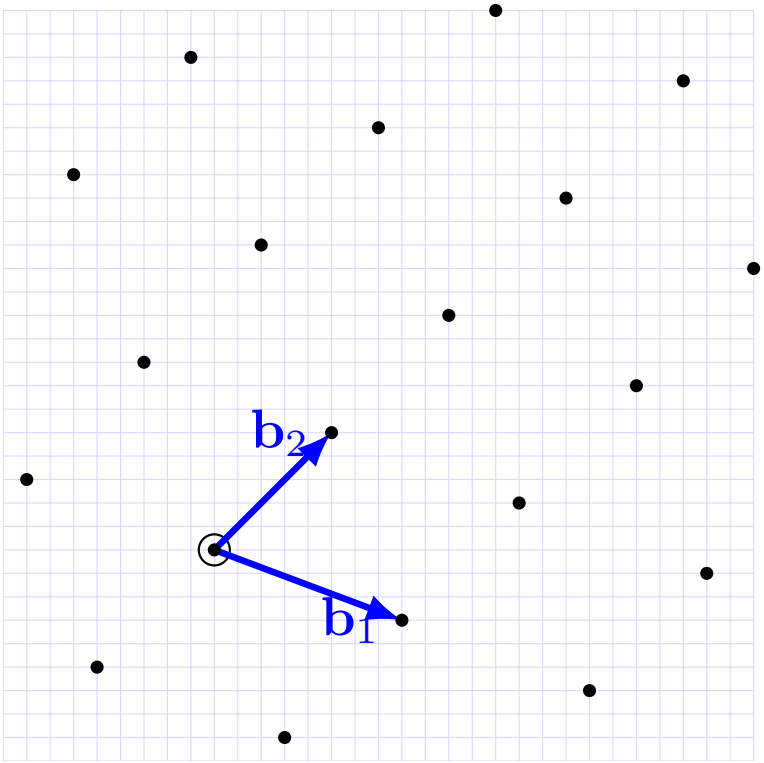
MAX PLANCK INSTITUTE FOR SECURITY AND PRIVACY

Radboud University

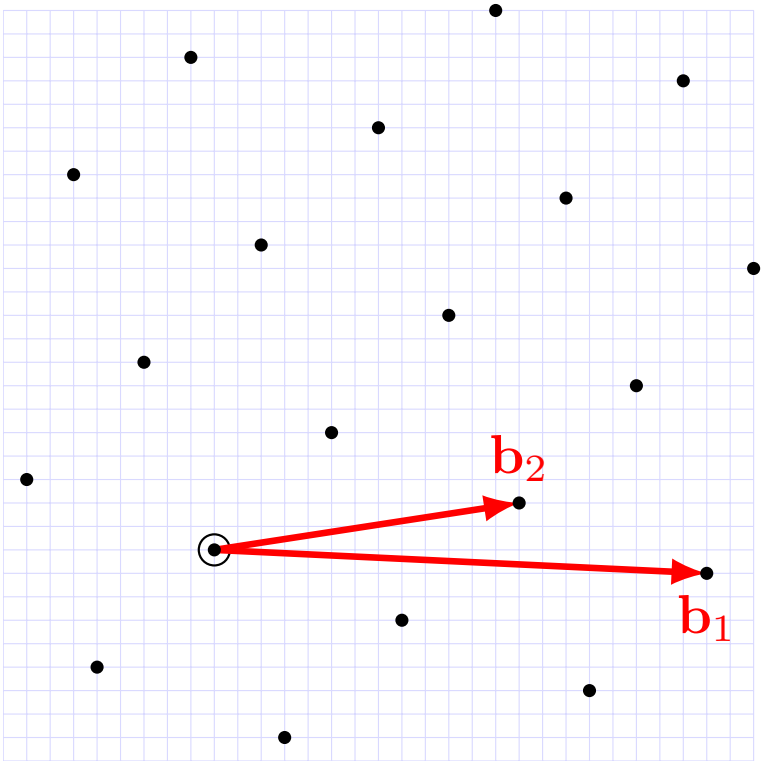
RUHR UNIVERSITÄT BOCHUM

RUB

Lattices, Bases, and Cryptography



Good Basis $\mathbf{G}$ of L



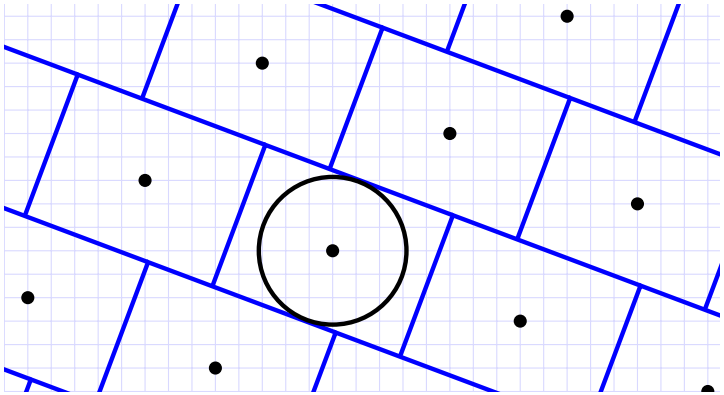
Bad Basis $\mathbf{B}$ of L

$\mathbf{G} \rightarrow \mathbf{B}$: easy (randomization);

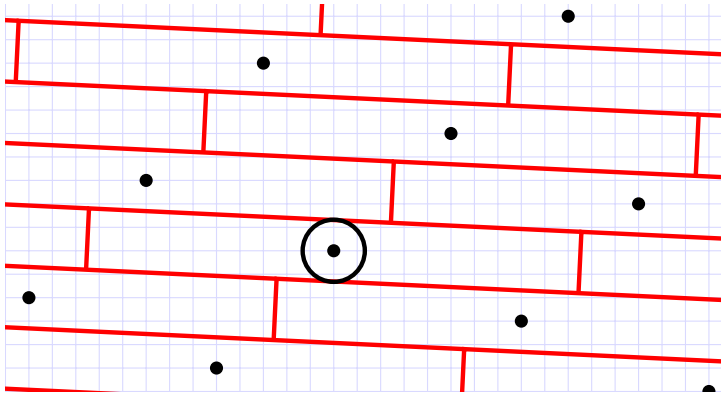
$\mathbf{B} \rightarrow \mathbf{G}$: hard (LLL, BKZ, Lattice Sieve...).

Decryption = Error Correction

Bases allow to 'tile' the space and to decode errors



Decoding radius with $\mathbf{G}^\star$



Decoding radius with $\mathbf{B}^\star$

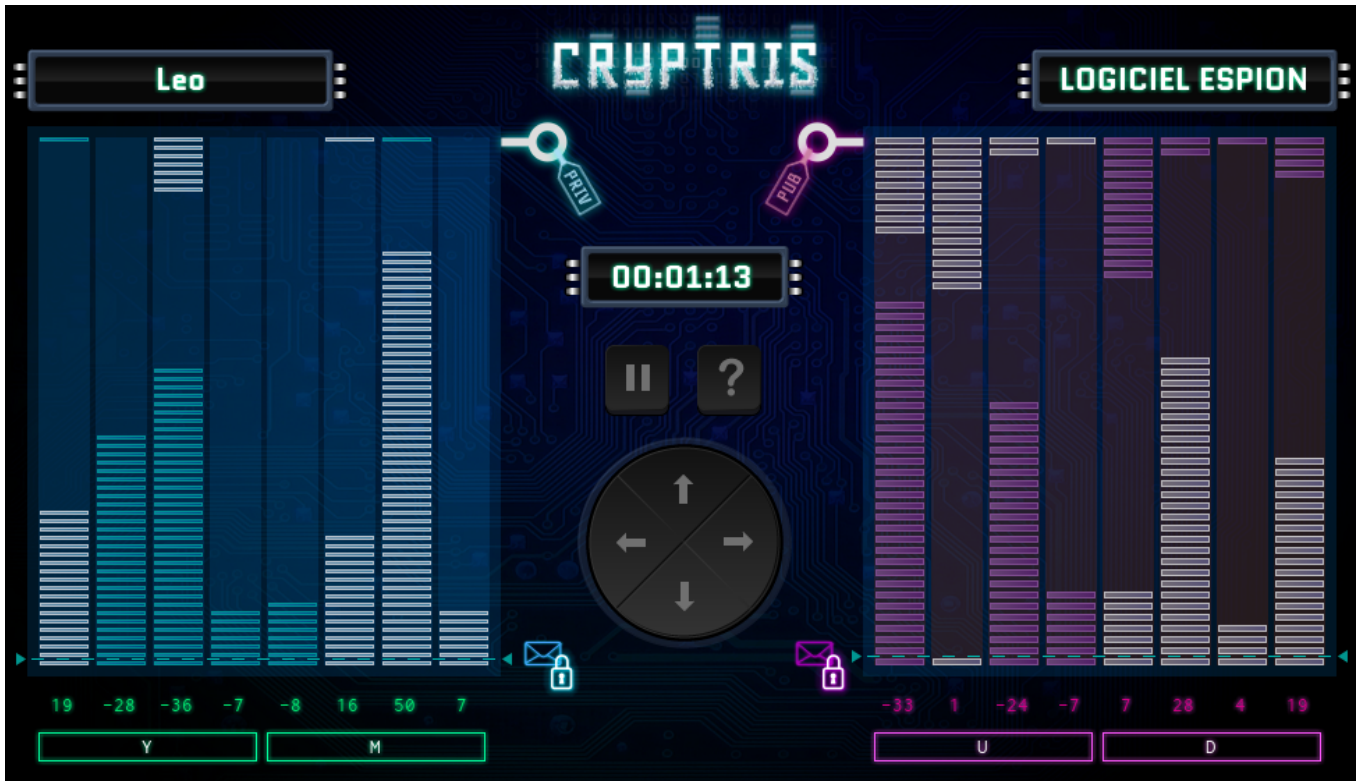
As dimension grows > 2, the error tolerance gap between **G** and **B** grows exponentially.

Lattice-Based Asymetric Cryptography

- secret key = good basis **G**
- public key = bas basis **B**

Lattice-based Crypto is as simple as Tetris

Cryptris:
A serious game to understand how it works, and why it is secure.



Developed with **Inria** (FR), translated to EN and NL at CWI
`https://cryptris.nl/`

CRYSTALS: A Coherent Suite

Key-Exchange + Signatures

- Same foundations: module-lattices $\Rightarrow$ less risk
  Less structure than ideal-lattices but still efficient
- Similar arithmetic: $\mathbb{Z}_q[X]/(X^{256}+1)$ $\Rightarrow$ less code
  $q_{\text{Kyber}} = 3329$, $q_{\text{Dilithium}} = 8380417$ for all security levels
- Simple distributions $\Rightarrow$ no Floating-Points
  uniforms, small binomial. **No Gaussians**
- Balanced performance

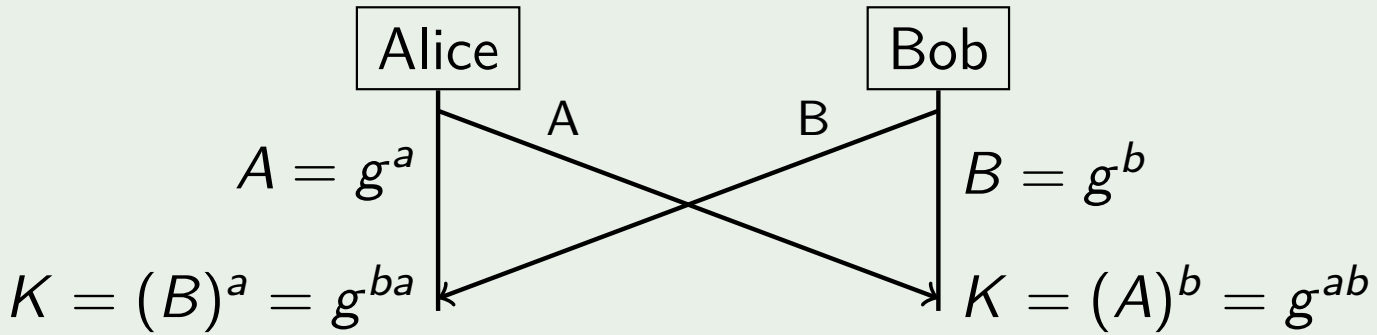
Many implementation available

for learning and testing

- `https://pq-crystals.org/`
- `https://github.com/PQClean/PQClean`
- `https://thelatticeclub.com/`
- `https://github.com/mupq/pqm4/blob/master/benchmarks.md`

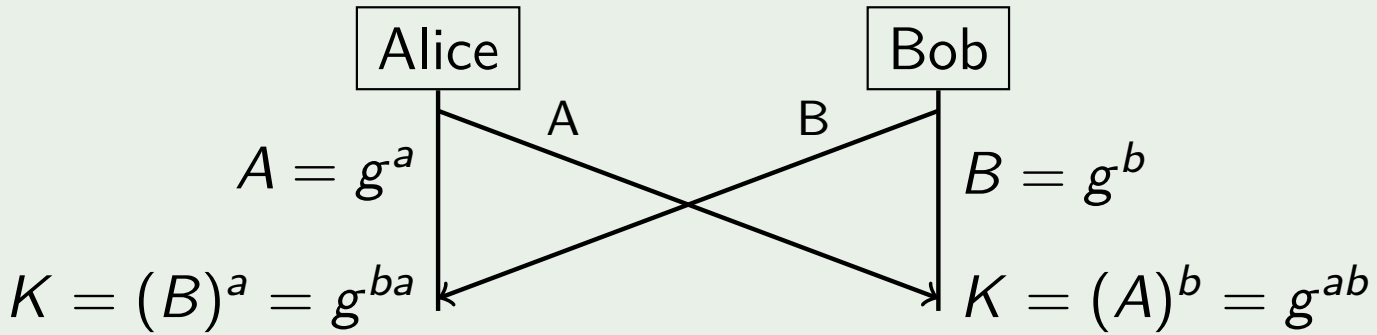
A Migration Challenge: Interactivity in Key-Exchange

DH & ECDH are non-interactive It doesn't matter who speaks first

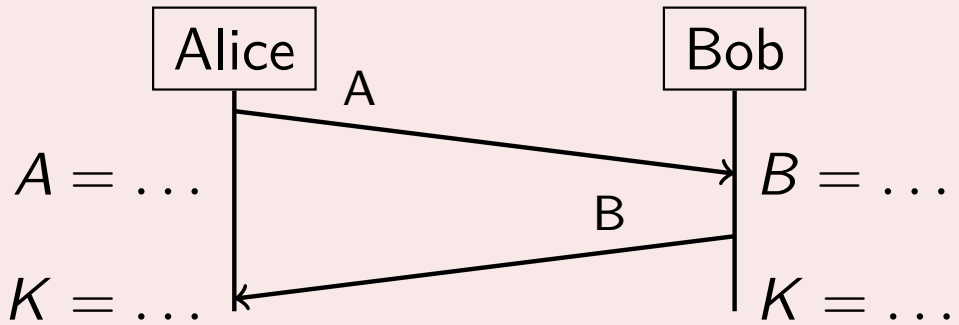


A Migration Challenge: Interactivity in Key-Exchange

DH & ECDH are **non-interactive** It doesn't matter who speaks first



Kyber is **interactive**



- the migration may require more than drop-in replacement
- the rest is only a matter of performances

Parameter Sets

Security Target	Key-Exchange	Signature
NIST level 1	Kyber-512	
NIST level 2		Dilithium-2
NIST level 3	Kyber-768	Dilithium-3
NIST level 4		
NIST level 5	Kyber-1024	Dilithium-5

Using Kyber-512 ?

- Ignoring cost of RAM, Kyber-512 security is borderline
- Attacks and cost estimates are still being refined
- NIST may decide to not standardize Kyber-512 right away
- Kyber-768 was and remain our recommendation

Performances

- Computation speed is **not** an issue
  worst operation is a **fraction of milli-second** on `x86-Haswell`
- Key and ciphertext sizes are larger than pre-quantum
  but nothing is particularly huge

Kyber-512

Sizes (bytes)	Cycles (ref)	Cycles (avx2)
sk: 2400	gen: 199k	gen: 52k
pk: 1184	enc: 235k	enc: 68k
ct: 1088	dec: 274k	dec: 53k

Dilithium-2

Sizes (bytes)	Cycles (ref)	Cycles (avx2)
	gen: 300k	gen: 124k
pk: 1312	sign: 1.3M	sign: 333k
sig: 2420	verif: 327k	verif: 118k

Profiling (on x86-Haswell)

SHAKE (SHA-3 Hash with Extended Output) $\approx 80\%$

- Hardware acceleration expected in future CPUs

Number Theoretic Transform for $\mathbb{Z}_q[X]/(X^{256}+1)$ $\approx 4\%$

- No alternative polynomial multiplication in current spec.

~~Karatsuba~~, ~~Toom-Cook~~

Miscellaneous $\approx 15\%$

- Sampling mod q, Arithmetic mod q, roundings $x \mapsto \lfloor \frac{p}{q} \cdot x \rceil$

Profile is similar on smaller architecture[1]

[1] e.g. m4 `https://github.com/mupq/pqm4/blob/master/benchmarks.md`

Summary

- Interactivity in KEM is the main challenge for migration

  the rest is a matter of performances

- Kyber & Dilithium form a coherent suite with balanced perf.

- Kyber & Dilithium selected as **primary** algorithms

  NIST recommends them for most use cases

- No major update to be expected

  Test with Round 3 version, wait standard to deploy

- Consider Kyber-768 when preparing migration

  Kyber-512 may be delayed for standardization