SQUIRRELS: Unstructured Lattice Digital signature

Thomas Espitau, Guilhem Niot, Chao Sun, Mehdi Tibouchi

\+ UNSTRUCTURED
\+ FAST + SMALL SIG
\+ VERY TAILORABLE

\– HUGE PUBLIC KEY
\– HEAVY KEYGEN
\– FLOATING POINT

MAIN TAKEAWAYS

- Hash-and-sign lattice signature
- Most conservative on lattices:
  plain LWE** and **SIS
- Fast and small signature size (comparable with ML-DSA)

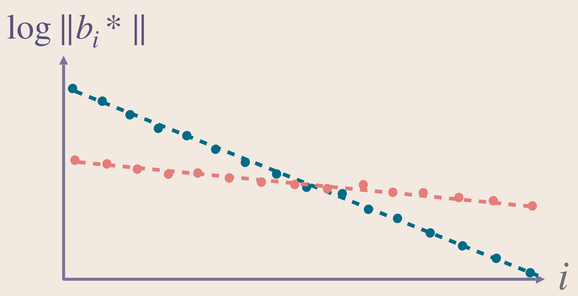
"Like FrodoKEM ··· for signatures"

SIGNATURE SIZE

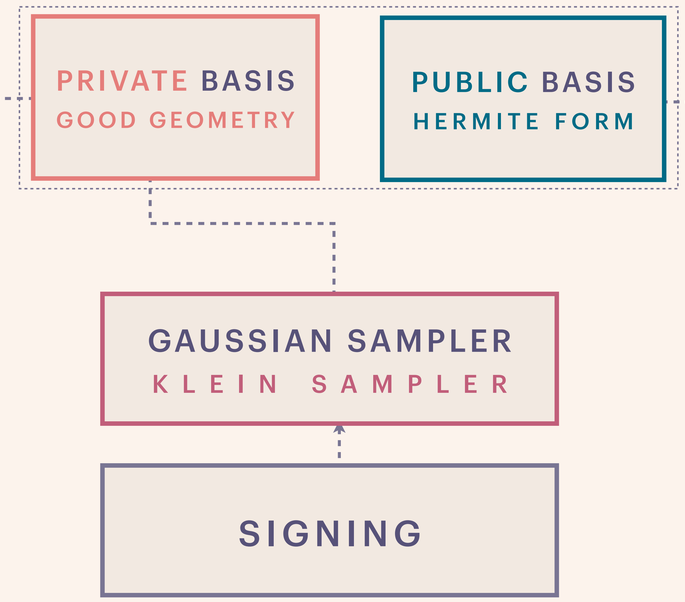
ADAPTIVE KEYGEN
GOOD GEOMETRIC STRUCTURE

Sampler size ∝ max Gram-Schmidt norms

> construct one vector after another by sampling in the good corresponding region of the space



DESIGN RATIONALE



VERIFICATION WITH SINGLE LINEAR EQUATION

"Co-representation" of a lattice as kernel of map

$$A : \mathbb{Z}^n \to (\mathbb{Z}/q\mathbb{Z})^m$$

$$v \in \mathscr{L} \Leftrightarrow Av = 0 \pmod q$$

> $m = 1$: single equation mod q !

$$\langle v, \underline{a} \rangle = 0 \pmod q$$