POST-QUANTUM CRYPTO

The issue: Quantum TMs are bad for crypto (at least in theory):

- Shor ('90's) invented an algorithm for FACTORING and DL that runs in poly time on a quantum machine / circuit.
- It requires many qubits and

billions of quantum gates assembly a 2048-bit modules.

While we are still far from implementing Shor's algo. (e.g. the record is factoring $n = 21$), people believe it's just a matter of time. The NIST is worried. Until 5 years ago almost the entire crypto was FACTORING or DL based (→ real world crypto).

Not only that: quantum attacks might be already happening. I.e. "store now, break later"!

Last but not least: Developing new crypto deployed in the real world takes $\gtrsim$ 10 years.

For these reasons, the NIST started the standardization process for post-QUANTUM crypto back in 2017.

Remark: PQ crypto means that Alice and Bob are still CLASSICAL. Eve has a quantum computer.

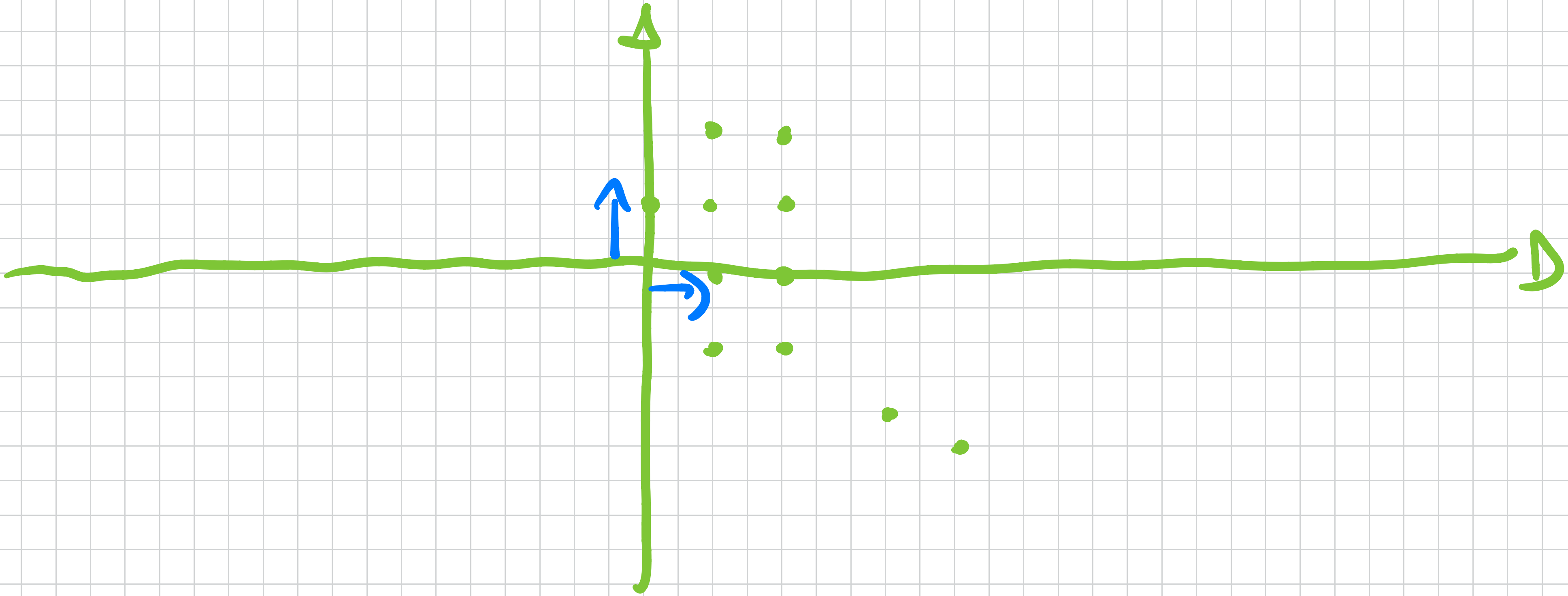
Minimal requirement: A computational problem believed to be hard for quantum machines. Many examples: lattices, isogenies over elliptic curves, codes, ...

We'll focus only on lattices. A lattice L consists of all INTEGER linear combinations of some linearly indep.

basis vectors $B = (\vec{b}_1, \dots, \vec{b}_n)$ over the reals.

$$\mathcal{L}(B) = B \cdot \mathbb{Z}^n =$$

$$= \left\{ \sum_{i=1}^{n} z_i \cdot \vec{b}_i : z_i \in \mathbb{Z} \right\}$$



Basis are not unique! For any $U \in \mathbb{Z}^{n \times n}$ UNIMODULAR (i.e. $\det(U) = \pm 1$) then $B \cdot U$ is also a basis because $U \cdot \mathbb{Z}^n = \mathbb{Z}^n$.

An important parameter for a lattice is the length of a shortest non-zero vector:

$$\lambda_1(\mathcal{L}) = \min_{\vec{v} \in \mathcal{L} \setminus \{\vec{0}\}} \|\vec{v}\|$$

$\|\cdot\|$ = EUCLIDEAN NORM

In general: $\lambda_i(\mathcal{L})$ the i-th successive MINIMA the smallest r s.t. $\mathcal{L}$ has i linearly independent vectors of length $\leq r$.

Here are some hard problems:

- SVP$_\gamma$: given B, find a shortest non-zero vector $\vec{v} \in \mathcal{L}(B)$ s.t.

$$\|v\| = \lambda_1(\mathcal{L}) \text{ or}$$
$$\leq \gamma(n) \cdot \lambda_1(\mathcal{L})$$

- $\underline{\text{Gap}}\ \underline{SVP}_\gamma$: Given B just decide iff $\lambda_1(\mathcal{L}) \leq 1$ or $\lambda_1(\mathcal{L}) > \gamma(n)$.

- $\underline{SIVP}_\gamma$: Given B, output $\{\vec{s}_i\}$ n linearly indep. vectors s.t.

$$\|\vec{s}_i\| \leq \gamma(n) \cdot \lambda_n(\mathcal{L})$$

$$\forall\ i = 1 \ldots n$$

__Fact__: The only poly-time algo. (even quantum) work for $\gamma(n) = 2^{\Theta(n \log\log n / \log n)}$

The modern perspective: we will use equivalent assumptions.

DEF (SIS). Given m RANDOM vectors $a_i \in \mathbb{Z}_q^n$ forming matrix $A \in \mathbb{Z}_q^{n \times m}$, the $SIS_{n,q,\beta,m}$ is to find a non-zero integer $\vec{z} \in \mathbb{Z}^m$ of norm $\|\vec{z}\| \leq \beta$ s.t.

$$f_A(z) = A \cdot z = \sum_i \vec{a}_i \cdot z_i = \vec{0} \in \mathbb{Z}_q^n \pmod q$$

REMARKS:

- SIS easy without the restriction on $\|z\|$. Also in case $\beta \geq q$, because $(q, 0 \dots 0)$ is a solution.
- Any solution w.r.t. A can be converted to solution for $[A \mid A']$ by appending zeroes.
- The values m, β must be large enough for a solution to exist.

In particular, $\beta \geq \sqrt{\bar{m}}$ and $m \geq \bar{m} = \lceil n \log q \rceil$. First, wlog assume $m = \bar{m}$. Since there are more than $2^{\bar{m}} = q^n$ vectors $x \in \{0,1\}^m$ and there must be two distinct x, x' s.t. $A\vec{x} = A\vec{x}' \in \mathbb{Z}_q^n$ and $\vec{z} = \vec{x} - \vec{x}' \in \{0, \pm 1\}^m$ is a solution of norm at most β.

$\Rightarrow f_A(\cdot)$ is automatically collision resistant!

Hardness: For $m = \text{poly}(n)$ and $q \geq \beta \cdot \text{poly}(n)$ solving $SIS_{n,q,\beta,m}$ is at least as hard as solving Gap SVP_γ and $SIVP_\gamma$ with $\gamma(n) = \beta \cdot \tilde{O}(\sqrt{n})$

$$(\beta \cdot \text{poly}(n))$$

DEF (LWE) For $\vec{s} \in \mathbb{Z}_q^n$, the LWE distribution $A_{\vec{s},\chi}$ over $\mathbb{Z}_q^n \times \mathbb{Z}_q$ is obtained by sampling $\vec{a} \in \mathbb{Z}_q^n$ RANDOM and $e \leftarrow \chi$ and outputting:

$$\vec{a}, \quad b = \langle \vec{s}, \vec{a} \rangle + e \mod q$$

given m samples $(\vec{a}_i, b_i) \in \mathbb{Z}_q^n \times \mathbb{Z}_q$ from $A_{\vec{s}, \chi}$ for RANDOM $\vec{s}$, find $\vec{s}$.

$$\text{SEARCH-LWE}_{n, q, \chi, m}$$

REMARKS:

- Without noise, the problem is easy.
- Error distribution: χ is taken

To be any distribution s.t.

$$\Pr[\,|e| > \alpha \cdot q \;:\; e \leftarrow \mathcal{X}\,] \leq negl(\lambda)$$

for $\alpha \ll 1$