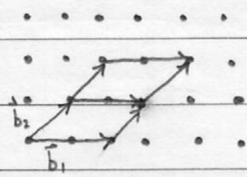
Lattice-Based Cryptography

- Quantum algorithms break traditional number-theoretic assumptions (factoring, discrete logarithms)
- Many symmetric primitives remain intact even with quantum computers (eg. double key size)
  - ↳ But public-key primitives (which rely on above algebraic assumptions) are broken ⇒ need new assumptions
  - ↳ One class of assumptions based on lattices

- A lattice $\mathcal{L}$ is a discrete additive subgroup of $\mathbb{Z}^n$ (more generally, $\mathbb{R}^n$)
  - Concretely: a lattice $\mathcal{L}$ is defined by a basis $B = \{\vec{b}_1, \ldots, \vec{b}_k\}$ where $\vec{b}_i \in \mathbb{Z}^n$ and $\mathcal{L}(B) = \left\{ \sum_{i=1}^{k} z_i b_i \;\middle|\; z_i \in \mathbb{Z} \right\}$
  - Pictorially:

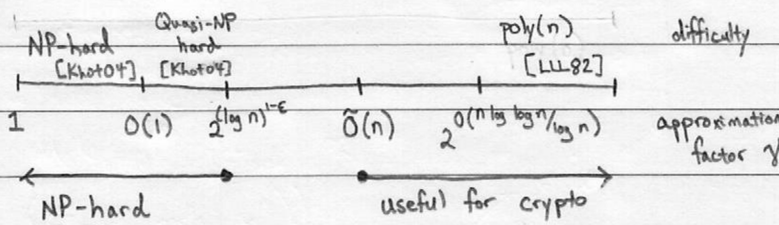


all integer combinations of basis vectors

- Hard lattice problems
  - Shortest vector problem (SVP): Given a basis B of some lattice $\mathcal{L} = \mathcal{L}(B)$, find shortest nonzero vector $\vec{v} \in \mathcal{L}$
  - Approximate SVP: (SVP_γ): Given a basis B of $\mathcal{L} = \mathcal{L}(B)$, find vector $\vec{v}$ where $\|\vec{v}\| \leq \gamma \cdot \lambda_1(\mathcal{L})$

    where $\lambda_1(\mathcal{L})$ denotes norm of shortest vector
  - $\mathrm{GapSVP}_{\gamma,d}$: Given a basis B of $\mathcal{L} = \mathcal{L}(B)$, decide if $\lambda_1(\mathcal{L}) \leq d$ or if $\lambda_1(\mathcal{L}) \geq \gamma \cdot d$
    - ↳ $\gamma(n)$ is the approximation factor

- Hardness in lattice-based cryptography (simplified)



- Major open problem: base crypto on NP-hardness
- Strong appeal of lattice-based crypto: average-to-worst case reduction

  (solving a random instance of a problem ⇒ approximating solution to a worst-case lattice problem)
  - ↳ very rare in cryptography
- Believed to be still difficult even on quantum computer!

The Learning with Errors Problem

Learning with errors (LWE) [Reg04]: one of the main assumptions in lattice-based crypto

↳ Reduces to solving worst-case lattice problems (approximating GapSVP)

↳ Surprisingly powerful and versatile assumption: gives constructions of FHE, ABE, predicate encryption, and many, many more!

The LWE problem: lattice parameters $(\underset{\text{lattice dimension}}{n}, \underset{\text{modulus}}{q}, \underset{\text{error distribution (discrete Gaussian distribution)}}{\chi})$

- LWE assumption: for $m = \text{poly}(n)$:

$$A \xleftarrow{R} \mathbb{Z}_q^{m \times n}, \quad s \xleftarrow{R} \mathbb{Z}_q^n, \quad e \leftarrow \chi^m, \quad u \xleftarrow{R} \mathbb{Z}_q^m$$

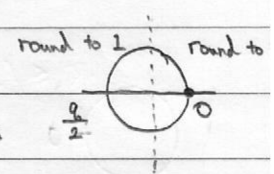
$$(A, As+e) \overset{c}{\approx} (A, u)$$

- Quite remarkable: without noise, problem is trivial (recover s using Gaussian elimination), but with noise, becomes intractable (approximating GapSVP to factor that depends on lattice parameters)

Symmetric Encryption from LWE:

Setup: $s \xleftarrow{R} \mathbb{Z}_q^n$

Encrypt (s, m): $a \xleftarrow{R} \mathbb{Z}_q^n$, $e \leftarrow \chi$ $\quad ct = (a, a^T s + e + m \cdot \lfloor \frac{q}{2} \rfloor)$



Decrypt (s, ct): output $\lfloor c_1 - c_0^T s \rceil_2$ where $\lfloor \cdot \rceil_2$ is a rounding operation

Correctness: $c_1 - c_0^T s = m \cdot \lfloor \frac{q}{2} \rfloor + e$ so if $|e| \ll q$, then will round correctly

Security: $(a, a^T s + e + m \cdot \lfloor \frac{q}{2} \rfloor) \overset{c}{\approx} (a, u + m \cdot \lfloor \frac{q}{2} \rfloor) \equiv (a, u)$ by LWE

Public-Key Encryption from LWE:

Observe: LWE encryption is additively homomorphic:

$$\left.\begin{array}{l} (a_0, \ a_0^T s + e_0 + m_0 \cdot \lfloor \frac{q}{2} \rfloor) \\ (a_1, \ a_1^T s + e_1 + m_1 \cdot \lfloor \frac{q}{2} \rfloor) \end{array}\right\} \left(a_0 + a_1, \ (a_0 + a_1)^T s + (e_0 + e_1) + (m_0 + m_1) \cdot \left\lfloor \frac{q}{2} \right\rfloor\right)$$

As long as noise is sufficiently small, correctness holds

Apply Rothblum's compiler of secret-key to public-key

PKE from LWE

Rothblum's trick: publish an encryption of 1 and many encryptions of 0 as the public key

- To encrypt a message m, use additive homomorphism (with encryption of 1) and re-randomize by taking a subset-sum of encryptions of 0
  ↳ leverages leftover hash lemma

Setup: $s \xleftarrow{R} \mathbb{Z}_q^n$ | sk: s

$A \xleftarrow{R} \mathbb{Z}_q^{m \times n}$ | pk: $(A, As + e)$ ← m encryptions of 0

$e \xleftarrow{R} \chi^m$

$$A = \begin{bmatrix} - a_1^T - \\ - a_2^T - \\ \vdots \\ - a_m^T - \end{bmatrix} \begin{bmatrix} s \end{bmatrix} + \begin{bmatrix} e_1 \\ e_2 \\ \vdots \\ e_m \end{bmatrix}$$

Encrypt(pk, m): Choose random subset $r \xleftarrow{R} \{0,1\}^m$ of encryptions of 0

$$ct = \Bigg(\underbrace{\sum_{i=1}^m r_i a_i^T, \left[\sum_{i=1}^m (a_i^T s + e_i) r_i \right]}_{\text{subset sum of encryptions of 0}} + \underbrace{m \cdot \left\lfloor \frac{q}{2} \right\rfloor}_{\text{message component}} \Bigg) = \left(r^T A,\ r^T(As+e) + m \cdot \left\lfloor \frac{q}{2} \right\rfloor \right)$$

Correctness: As before

Security: pk: $(A, As+e) \overset{c}{\approx} (A, u)$ by LWE

↳ $(r^T A, r^T u)$ looks uniform by leftover hash lemma (when $m = \Theta(n \log q)$)

- Can extend to larger message spaces
- Variant can be shown to be fully homomorphic

Decryption is an inner product in Regev-based encryption schemes

$m = [\langle c, s \rangle]_p$

homomorphisms:

$\langle c_1 + c_2, s \rangle = \langle c_1, s \rangle + \langle c_2, s \rangle$

$\langle c_1 \otimes c_2, s \otimes s \rangle = \langle c_1, s \rangle \langle c_2, s \rangle$

↳ useful for FHE

Key-Exchange from LWE (Frodo)

Conventional Diffie-Hellman broken by quantum computer - need something post-quantum

client		server
$y \xleftarrow{R} \mathbb{Z}_q$	$\xleftarrow{\ g^x\ }$	$x \xleftarrow{R} \mathbb{Z}_q$
	$\xrightarrow{\ g^y\ }$	
↓		↓
g^{xy}		g^{xy}

DDH assumption:

$$(g, g^x, g^y, g^{xy}) \overset{c}{\approx} (g, g^x, g^y, u)$$

client		server
		$A \xleftarrow{R} \mathbb{Z}_q^{n \times n}$
		$X, E \leftarrow \chi^{n \times m}$
	$\xleftarrow{\ A,\ AX + E\ }$	
$Y, E' \leftarrow \chi^{n \times m}$	$\xrightarrow{\ Y^T A + (E')^T\ }$	
↓		↓
$Y^T AX + Y^T E \approx Y^T AX$		$Y^T AX + (E')^T X \approx Y^T AX$

can be compressed (e.g. via PRG)

Relies on LWE with short secrets (hardness reduces to decision LWE)

By standard hybrid:

$$(A, AX+E) \overset{c}{\approx} (A, U)$$