For public-key cryptography, we will need new assumptions to get post-quantum security

We will see a brief flavor today — lattice assumptions

<u>Learning with Errors (LWE)</u>: The LWE problem is defined with respect to lattice parameters n, m, q, χ, where χ is an <u>error distribution</u> over $\mathbb{Z}_q$ (oftentimes, this is a discrete Gaussian distribution over $\mathbb{Z}_q$). The $\mathsf{LWE}_{n,m,q,\chi}$ assumption states that for a random choice $A \xleftarrow{R} \mathbb{Z}_q^{n \times m}$, $s \xleftarrow{R} \mathbb{Z}_q^n$, $e \leftarrow \chi^m$, the following two distributions are computationally indistinguishable:

$$(A, s^T A + e^T) \stackrel{c}{\approx} (A, r)$$

where $r \xleftarrow{R} \mathbb{Z}_q^m$.

Symmetric encryption from LWE (for binary-valued messages) [Regev]

Setup(1^λ): Sample $s \xleftarrow{R} \mathbb{Z}_q^n$.

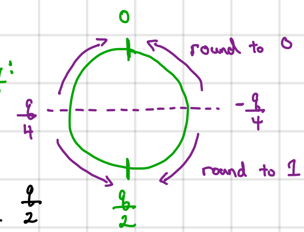
Encrypt$(s, \underset{\in\{0,1\}}{\mu})$: Sample $a \xleftarrow{R} \mathbb{Z}_q^n$ and $e \leftarrow \chi$. Output $(a, s^T a + e + \mu \cdot \lfloor \frac{q}{2} \rfloor)$.

Decrypt(s, ct): Output $\underbrace{\lfloor ct_2 - s^T ct_1 \rceil_2}_{\text{"rounding operation"}}$

$$\lfloor x \rceil_2 = \begin{cases} 0 & \text{if } -\frac{q}{4} \le x < \frac{q}{4} \\ 1 & \text{otherwise} \end{cases}$$

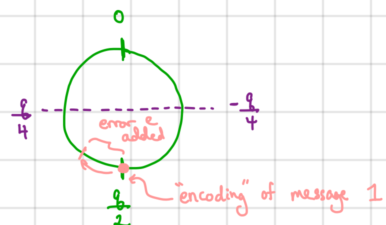
↳ take $x \in \mathbb{Z}_q$ to be representative between $-\frac{q}{2}$ and $\frac{q}{2}$

Visually:



<u>Correctness</u>:
$$\begin{aligned} ct_2 - s^T ct_1 &= s^T a + e + \mu \cdot \lfloor \tfrac{q}{2} \rfloor - s^T a \\ &= \mu \cdot \lfloor \tfrac{q}{2} \rfloor + e \end{aligned}$$

if $|e| < \frac{q}{4}$, then decryption recovers the correct bit



(message encrypted in "most significant bits" of the ciphertext)
↳ will see variant in HW5

<u>Security</u>: By the $\mathsf{LWE}_{n,q,\chi}$ assumption, $(a, s^T a + e) \stackrel{c}{\approx} (a, r)$ where $r \xleftarrow{R} \mathbb{Z}_q$. Thus,

$$(a, s^T a + e + \mu \cdot \lfloor \tfrac{q}{2} \rfloor) \stackrel{c}{\approx} (a, r + \mu \cdot \lfloor \tfrac{q}{2} \rfloor)$$

↳ $r \xleftarrow{R} \mathbb{Z}_q$: one-time pad encryption of the message μ

<u>Observe</u>: this encryption scheme is additively homomorphic (over $\mathbb{Z}_2$):

$$\begin{matrix} (a_1, s^T a_1 + e_1 + \mu_1 \cdot \lfloor \frac{q}{2} \rfloor) \\ (a_2, s^T a_2 + e_2 + \mu_2 \cdot \lfloor \frac{q}{2} \rfloor) \end{matrix} \Rightarrow \left(a_1 + a_2,\ s^T(a_1 + a_2) + (e_1 + e_2) + (\mu_1 + \mu_2) \cdot \lfloor \tfrac{q}{2} \rfloor \right)$$

decryption then computes

$$(\mu_1 + \mu_2) \cdot \lfloor \tfrac{q}{2} \rfloor + e_1 + e_2$$

which when rounded yields $\mu_1 + \mu_2 \pmod 2$ provided that $|e_1 + e_2 + 1| < \frac{q}{4}$

Idea: We will include encryptions of 0 in the public key and refresh ciphertexts by taking a subset sum of encryptions of 0:

Regev's public-key encryption scheme

Setup: $A \xleftarrow{R} \mathbb{Z}_q^{n \times m}$ output $pk = (A, b^T)$

$s \xleftarrow{R} \mathbb{Z}_q^n$ $\quad b^T \leftarrow s^T A + e^T$ $\quad sk = s$

$e \leftarrow \chi^m$

↳ can be viewed as m encryptions of 0 under the symmetric scheme with secret key s

Encrypt(pk, μ): sample $r \xleftarrow{R} \{0,1\}^m$

output $(Ar,\ b^T r + \mu \cdot \lfloor \frac{q}{2} \rfloor)$

Decrypt(sk, ct): output $\lfloor ct_2 - s^T ct_1 \rceil_2$

Correctness: $ct_2 - s^T ct_1 = b^T r + \mu \cdot \lfloor \frac{q}{2} \rfloor - s^T A r = s^T A r + e^T r + \mu \cdot \lfloor \frac{q}{2} \rfloor - s^T A r$

$= \mu \cdot \lfloor \frac{q}{2} \rfloor + e^T r$

if $|e^T r| < \frac{q}{4}$, then decryption succeeds (since e is small and r is binary, $e^T r$ is not large: $|e^T r| < m \|e\| \|r\| = m \|e\|$)

Security (Sketch): Under LWE assumption public key

$(A,\ s^T A + e^T) \approx (A, u)$ where $A \xleftarrow{R} \mathbb{Z}_q^{n \times m}$, $u \xleftarrow{R} \mathbb{Z}_q^m$

By the "leftover hash lemma," if we sample $A \xleftarrow{R} \mathbb{Z}_q^{n \times m}$, $u \xleftarrow{R} \mathbb{Z}_q^n$, $r \xleftarrow{R} \{0,1\}^m$ where $m > 2n \log q$

$(Ar,\ u^T r) \approx (v, w)$ where $v \xleftarrow{R} \mathbb{Z}_q^n$ and $w \xleftarrow{R} \mathbb{Z}_q$

$\Longrightarrow$ $b^T r$ in ciphertext functions as a one-time pad

So far ... we have developed public-key encryption; what about key agreement?

Alice

$A \xleftarrow{R} \mathbb{Z}_q^{n \times n}$

$S, E \leftarrow \chi^{n \times n}$

$\xrightarrow{\ A,\ \overbrace{AS + E}^{B}\ }$

$\xleftarrow{\ S'A + E'\ }$

↓ compute $(S'A + E')S$ and "round"

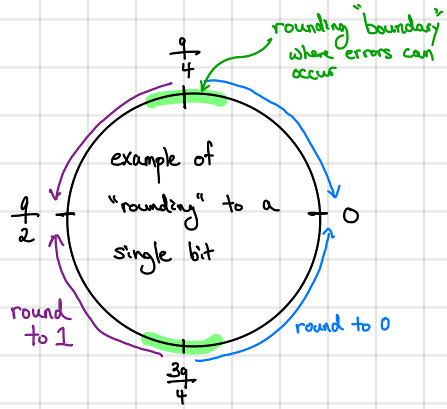
Bob

$S', E' \leftarrow \chi^{n \times n}$

$E'' \leftarrow \chi^{n \times n}$

↳ compute $S'B + E''$ and "round"

↳ drop least significant bits (similar to decryption in Regev encryption)



Under the LWE assumption:

$(A,\ AS + E) \approx U$ where $U \xleftarrow{R} \mathbb{Z}_q^{n \times m}$ [note: requires that LWE holds even if S is sampled from error distribution]

→ shared key then derived by $S'B + E''$ → by LWE, $(B,\ S'B + E'') \approx (B, U')$

→ shared key is derived from random matrix (similar to Diffie-Hellman, the key material is hashed to derive a symmetric key)

Practical considerations:

- Key reconciliation: presence of noise means Alice and Bob may end up with inconsistent keys
  Bob sends a "hint" with his message to reconcile any errors and ensure exact key agreement
- Message size: large matrix A is uniform — can be derived from a short seed (using PRG)
  ↳ justifiable using the random oracle model

Above construction relies on security of LWE where the secret key is sampled from error distribution

↳ This is LWE in "Hermite normal form" and is just as hard as standard LWE

LWE is a <u>versatile</u> assumption: yields key exchange, public-key cryptography, signatures

also enables <u>advanced</u> primitives like

- fully homomorphic encryption: <u>arbitrary</u> computation on ciphertexts
- identity-based encryption: public-key encryption scheme where public keys can be arbitrary strings
- functional encryption: fine-grained control of data access
- and many more!

→ also plausibly post-quantum resilient!