

LATTICE-BASED ENCRYPTION II

PHONG NGUYEN

<http://www.di.ens.fr/~pnguyen>

October 2026



TODAY

Lattice Analogues of:

- Diffie-Hellman and El Gamal
 - Encryption **without** Trapdoors

DIFFIE- HELLMAN AND EL GAMAL

Encryption without Trapdoors

$$\begin{aligned}
 & e_1(x)y_1 + e_2(x)y_2 + e_3(x)y_3 \\
 &= \left(\frac{x(x-2)}{2} \right) 1 + (x(x-1))0 + \\
 &= \left(\frac{(x-1)(x-2)}{2} \right) 1 + (x(x-1)) \\
 & \quad \quad \quad f_p(x, y) \\
 &= \frac{(x^2+x^2)^4 - (2x^2+7x^2+8x)^2 (y+9x+}{(x+9)^4} \quad x(x+1) \\
 & \quad \quad \quad \sqrt{4a^3+27b^2} \frac{1}{3} (y+6x)^2 (y+10x+}{1/3 \quad 3^{2/3} \quad x(x+6)^2} \\
 & \quad \quad \quad \frac{(y+8x)^2}{(\sqrt{3})(-9b+\sqrt{3}\sqrt{4a^3+27b^2})^{1/3}} \\
 & \quad \quad \quad \frac{2^{4/9} 3^{2/3} x + 9}{(y+8x)^2 (y+7x+}
 \end{aligned}$$

TRAPDOOR-LESS ENCRYPTION

DIFFIE-HELLMAN KEY EXCHANGE

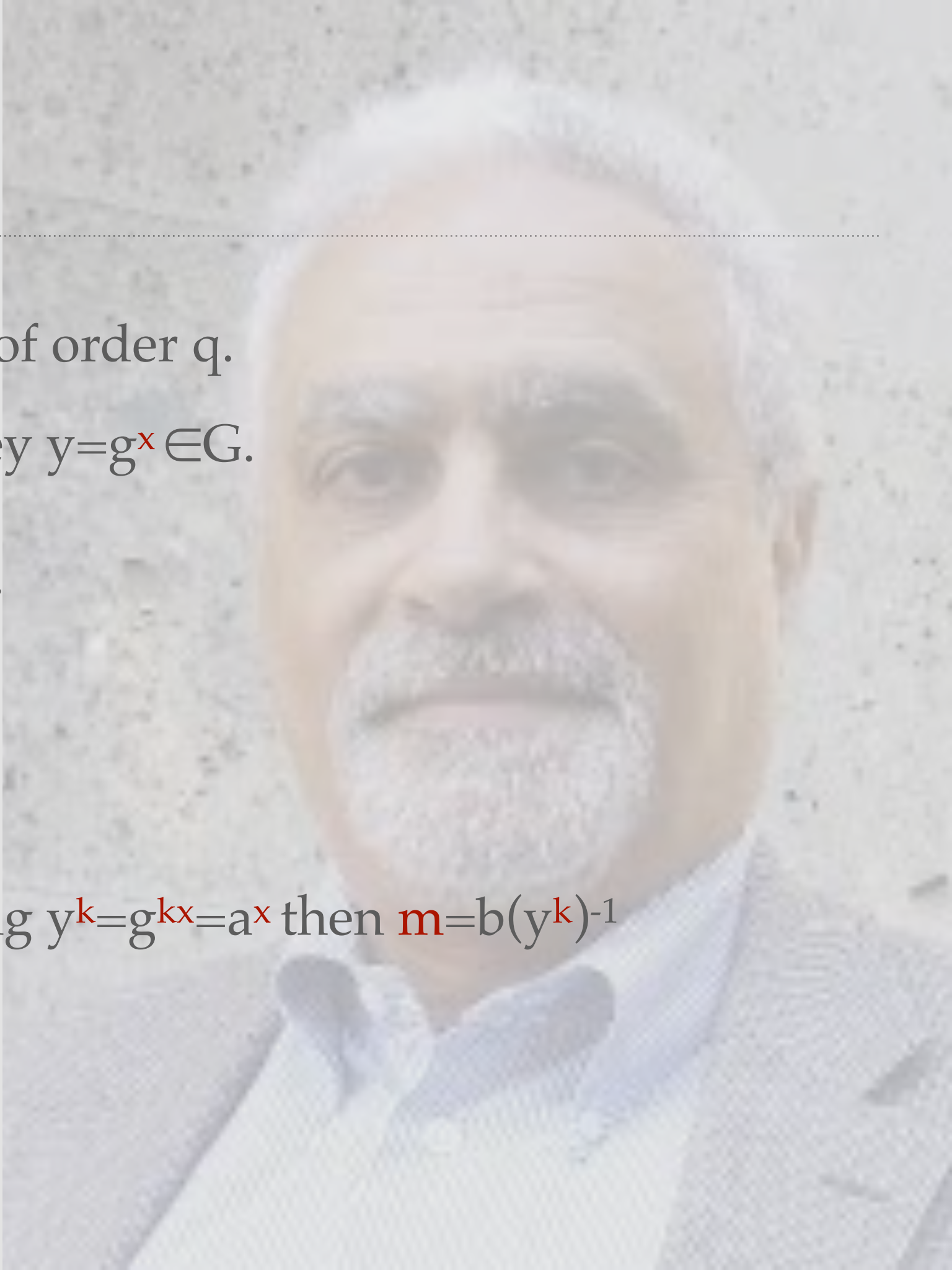
- Let $G = \langle g \rangle$ be generated by g of order q .



- Both can compute the shared key $g^{ab} = (g^a)^b = (g^b)^a$
- This key exchange is the core of [El Gamal public-key encryption](#).

ELGAMAL ENCRYPTION (1984)

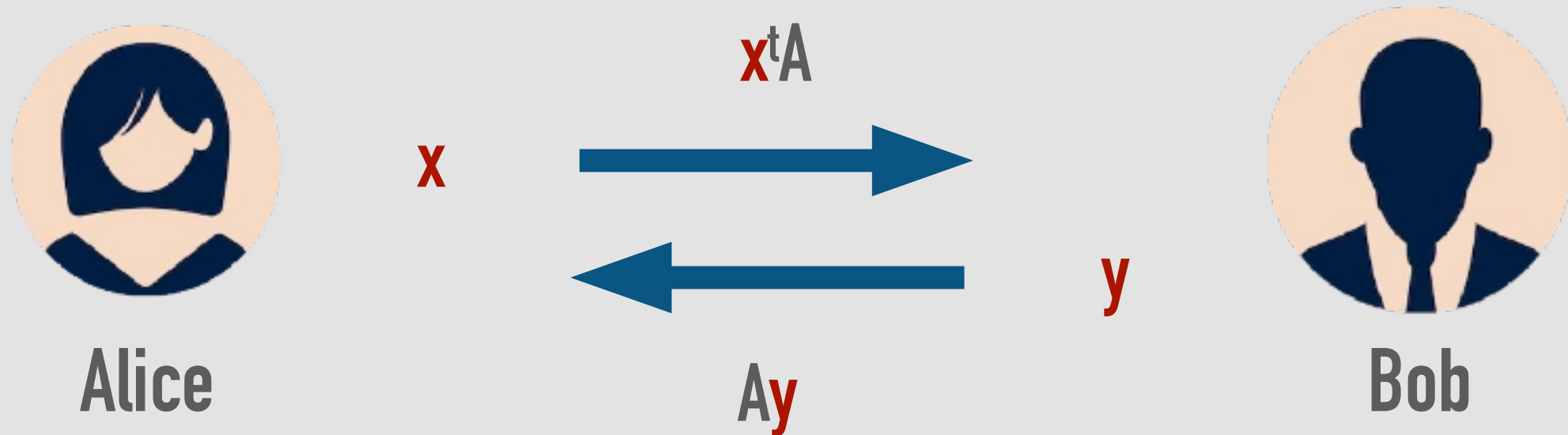
- Let G be a cyclic group $\langle g \rangle$ of order q .
- Secret key $x \in \mathbb{Z}_q$. Public key $y = g^x \in G$.
- Encrypt $m \in G$ as $(a, b) \in G^2$.
 - $a = g^k \in G$ where $k \in \mathbb{Z}_q$
 - $b = my^k \in G$
- Decrypt (a, b) by recovering $y^k = g^{kx} = a^x$ then $m = b(y^k)^{-1}$



ELGAMAL ENCRYPTION

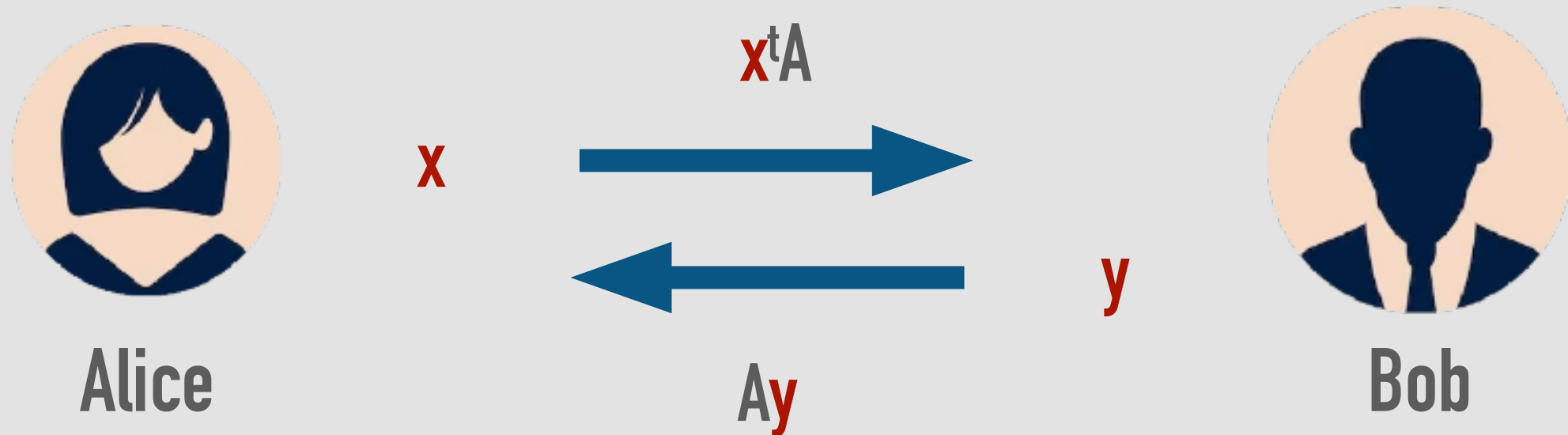
- Behind El Gamal, there is the **Diffie-Hellman key exchange**.
 - Alice has a secret key $x \in_R \mathbb{Z}/q\mathbb{Z}$ and discloses $y = g^x \in G$
 - Bob selects a one-time key $k \in_R \mathbb{Z}/q\mathbb{Z}$ and discloses $g^k \in G$
 - Both can compute the shared key g^{kx} .

MATRIX DIFFIE-HELLMAN



- $\mathbf{A}$ is a public matrix over some ring R . $\mathbf{x}$ and $\mathbf{y}$ are secret vectors.
 - Alice and Bob can compute $\mathbf{x}^t \mathbf{A} \mathbf{y} = (\mathbf{x}^t \mathbf{A}) \mathbf{y} = \mathbf{x}^t (\mathbf{A} \mathbf{y}) \in R$
- Is this secure?

MATRIX DIFFIE-HELLMAN



- Both can compute $x^t A y = (x^t A) y = x^t (A y) \in \mathbb{R}$
- But so would anyone who can compute x' or y' s.t. $x^t A = x'^t A$ or $A y = A y'$
which is easy: linear algebra!

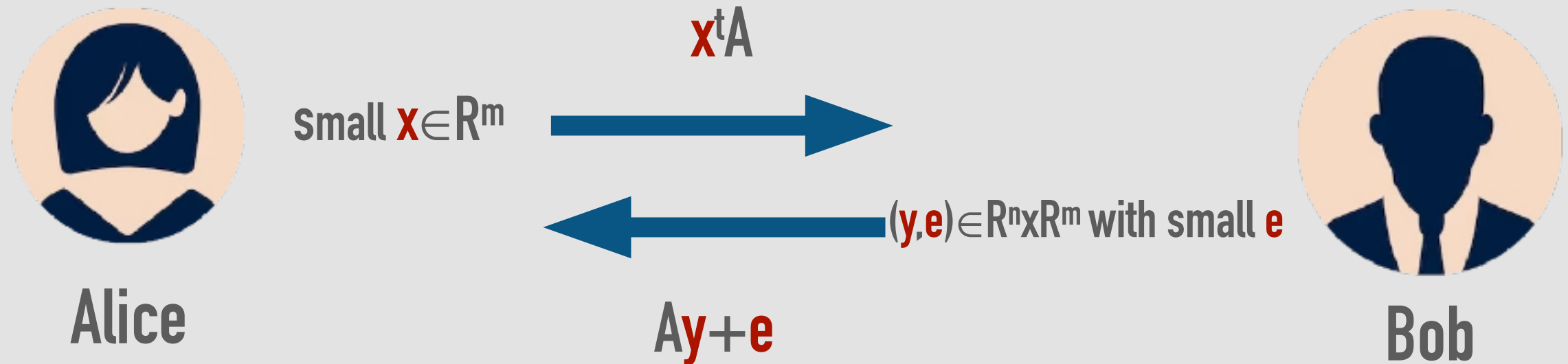
WHAT CAN WE DO?

KEY IDEAS

Introducing...

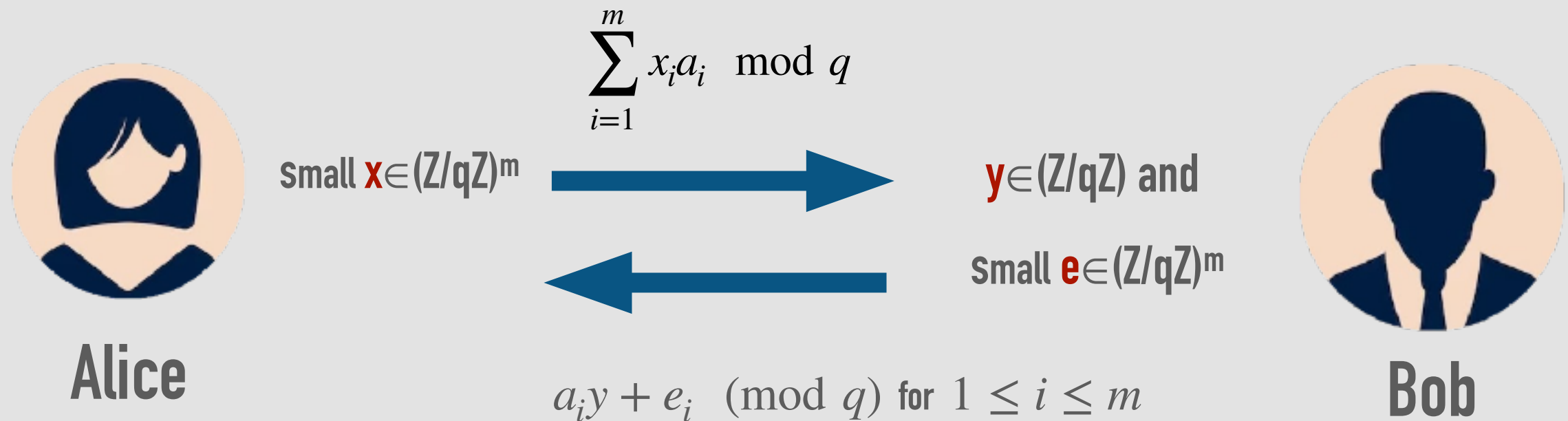
- Noise
- Small secrets

RECTANGULAR DIFFIE-HELLMAN



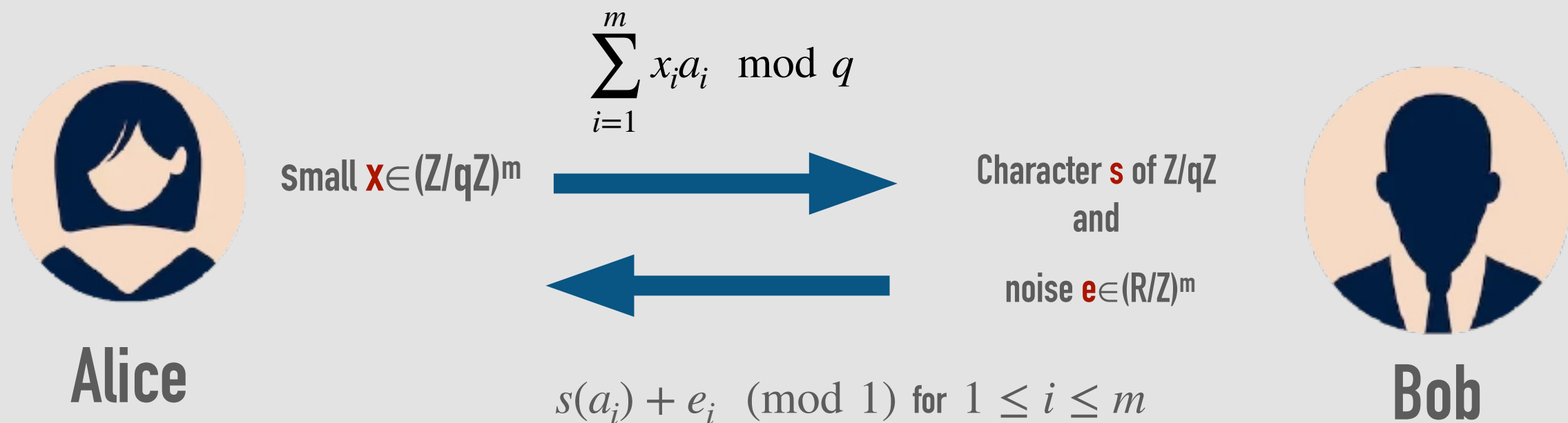
- Both can approximate $\mathbf{x}^t \mathbf{A} \mathbf{y} \approx \mathbf{x}^t (\mathbf{A} \mathbf{y} + \mathbf{e})$ if in the ring R :
 - $\text{small} + \text{small} = \text{small}$
 - $\text{small} * \text{small} = \text{small}$
- A is an $m \times n$ matrix over $R = \mathbb{Z}_q$ $m \gg n$

THE SIMPLEST CASE: SINGLE-COLUMN A



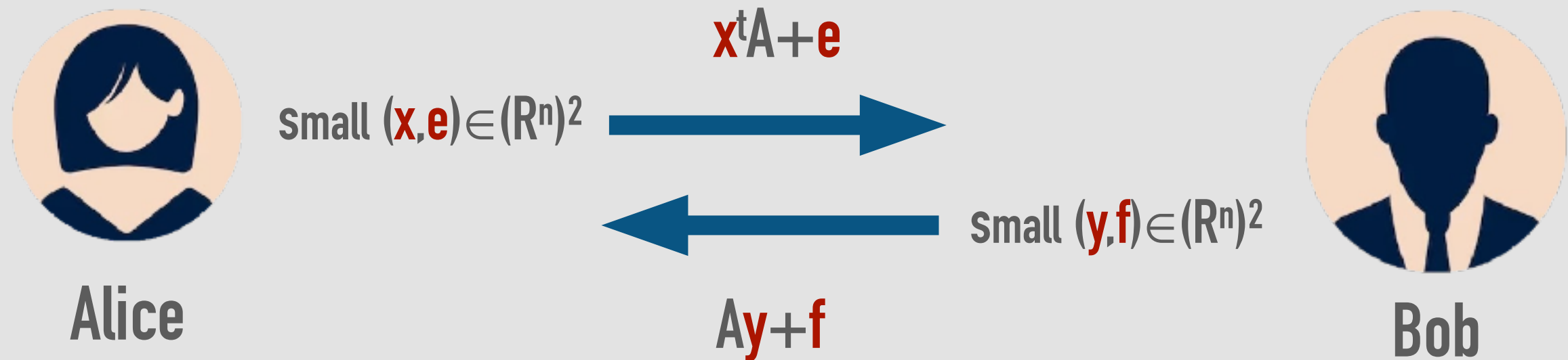
- Both can approximate $\sum_{i=1}^m x_i a_i y \approx \sum_{i=1}^m x_i (a_i y + e_i)$ in the ring $\mathbb{Z}/q\mathbb{Z}$
 - small+small = small
 - small*small = small
- Choose random integers $a_1, \dots, a_m \pmod q$.

RECTANGULAR DIFFIE-HELLMAN: THE SIMPLEST CASE



- Both can approximate $\sum_{i=1}^m x_i s(a_i) \approx \sum_{i=1}^m x_i (s(a_i) + e_i)$ in $\mathbb{R}/\mathbb{Z}$
- Choose random integers $a_1, \dots, a_m \pmod{q}$.

SQUARE DIFFIE-HELLMAN



- Both can approximate $\mathbf{x}^t \mathbf{A} \mathbf{y} \approx \mathbf{x}^t (\mathbf{A} \mathbf{y} + \mathbf{f}) \approx (\mathbf{x}^t \mathbf{A} + \mathbf{e}) \mathbf{y}$.
- $\mathbf{A}$ is an $n \times n$ matrix over $\mathbb{R} = \mathbb{Z}_q[X] / (X^{256} + 1)$
- This is the noisy Diffie-Hellman underlying Kyber:
Alice and Bob use MLWE.

WHICH RINGS?

- $R = \mathbb{Z}_q$ or $\mathbb{Z}_q[X] / (X^{256} + 1)$ so that:
 - $\text{small} + \text{small} = \text{small}$
 - $\text{small} * \text{small} = \text{small}$
- For suitable prime q , $X^{256} + 1$ splits into many factors mod q , allowing fast multiplication in $\mathbb{Z}_q[X] / (X^{256} + 1)$.

RECALL THE LATTICE MAGIC

THE SIS PROBLEM (1996): SMALL INTEGER SOLUTIONS

- Choose an $m \times n$ random matrix A over $R = \mathbb{Z}_q$ $m \gg n$
- Goal: Find « short » $\mathbf{x} \in R^m$ s.t. $\mathbf{x}^t A \equiv 0$
- This is essentially finding a short vector in a **random lattice**.

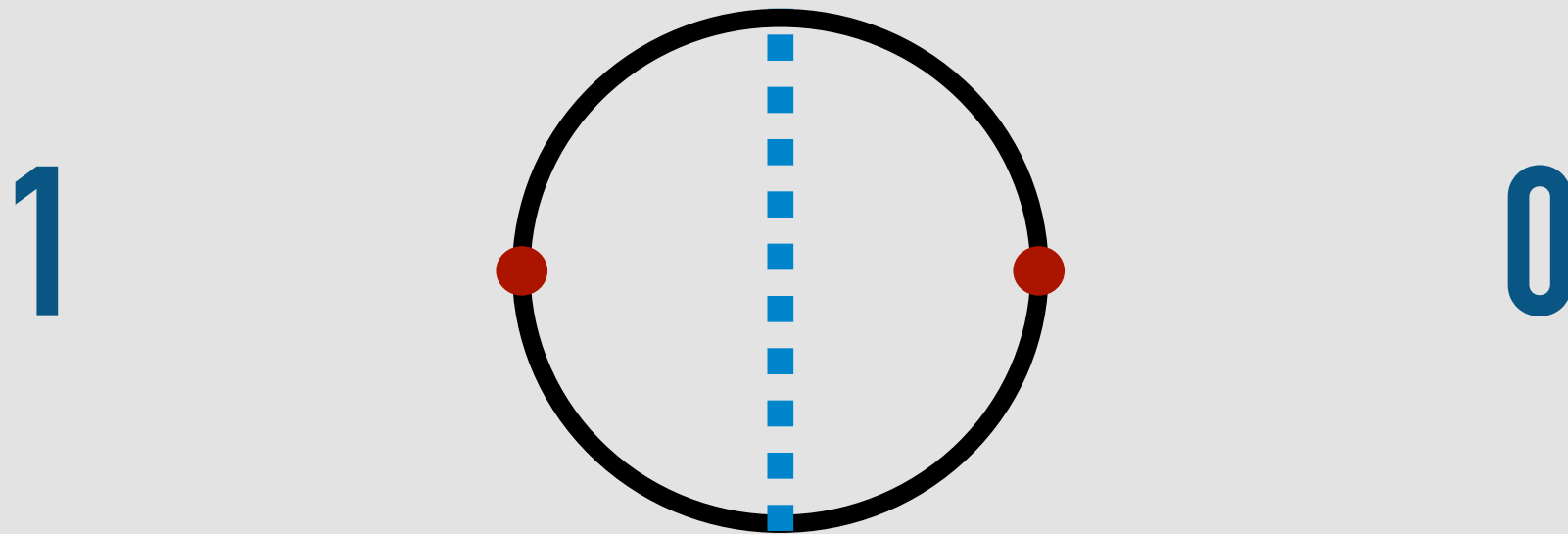
THE LWE PROBLEM: LEARNING (A CHARACTER) WITH ERRORS

- Choose an $m \times n$ random matrix A over $R = \mathbb{Z}_q$ $m \gg n$
- Pick a random $\mathbf{y}$ in R^n .
- Goal: recover $\mathbf{y}$ given $A\mathbf{y} + \mathbf{e}$ where $\mathbf{e} \in R^m$ is a small noise.

BACK TO NOISY DIFFIE HELLMAN

≠ DIFFIE-HELLMAN: THE NOISE

- The two values computed by Alice and Bob are elements of a torus which are **close** to each other.

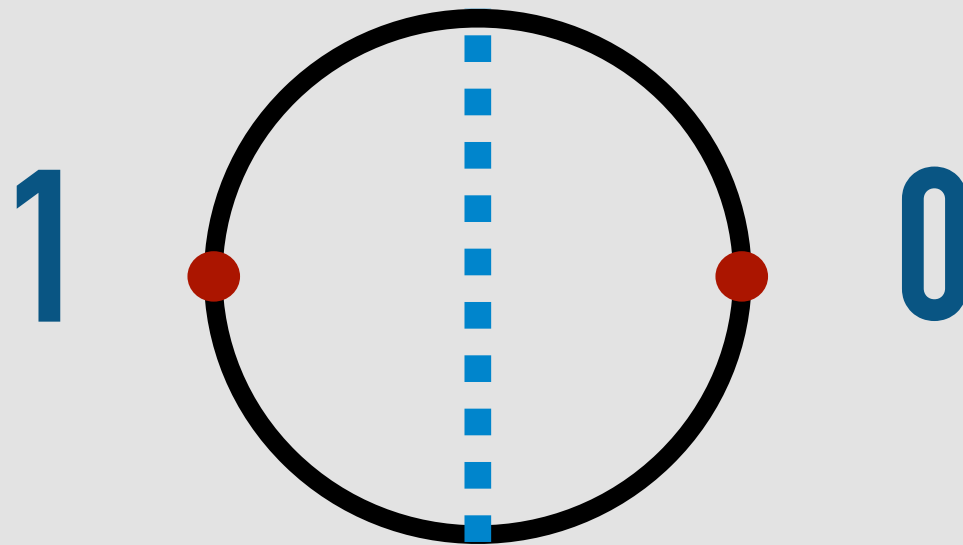


- But how can they extract a bit?

Key reconciliation.

NOISY EL GAMAL

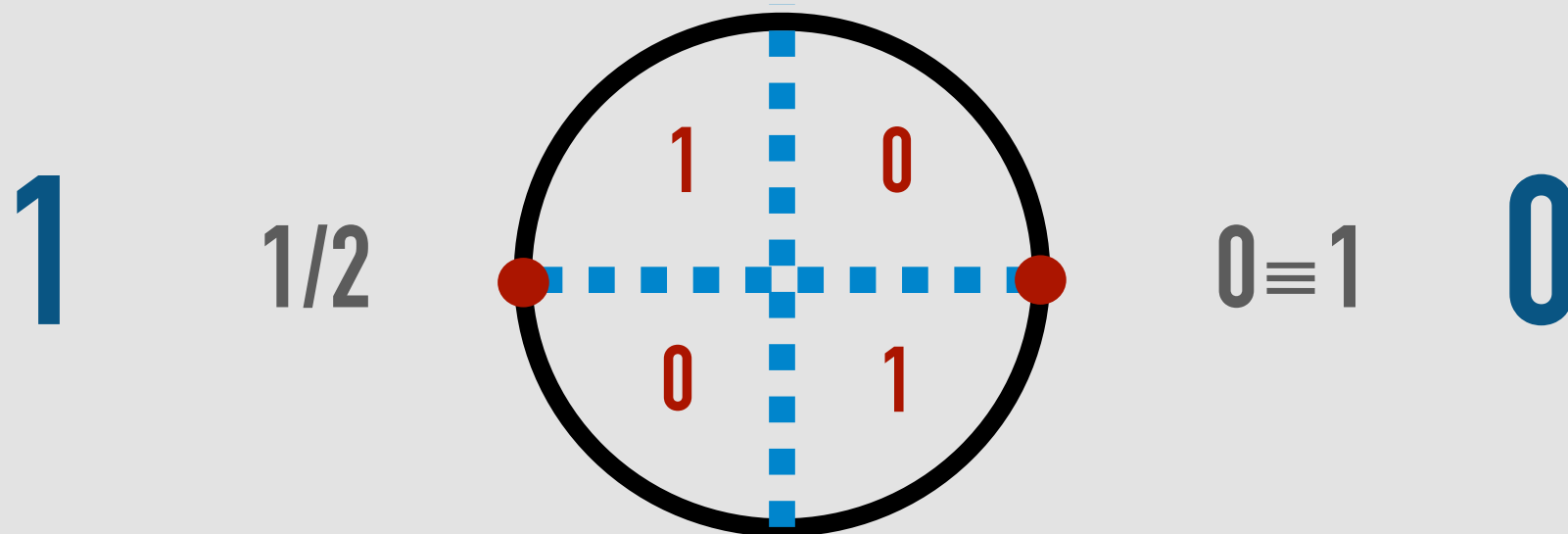
- No problem in El Gamal by encoding the message into torus elements which are far apart.



- $R = \mathbb{Z}_q[X] / (X^{256} + 1)$ encodes 256 bits.

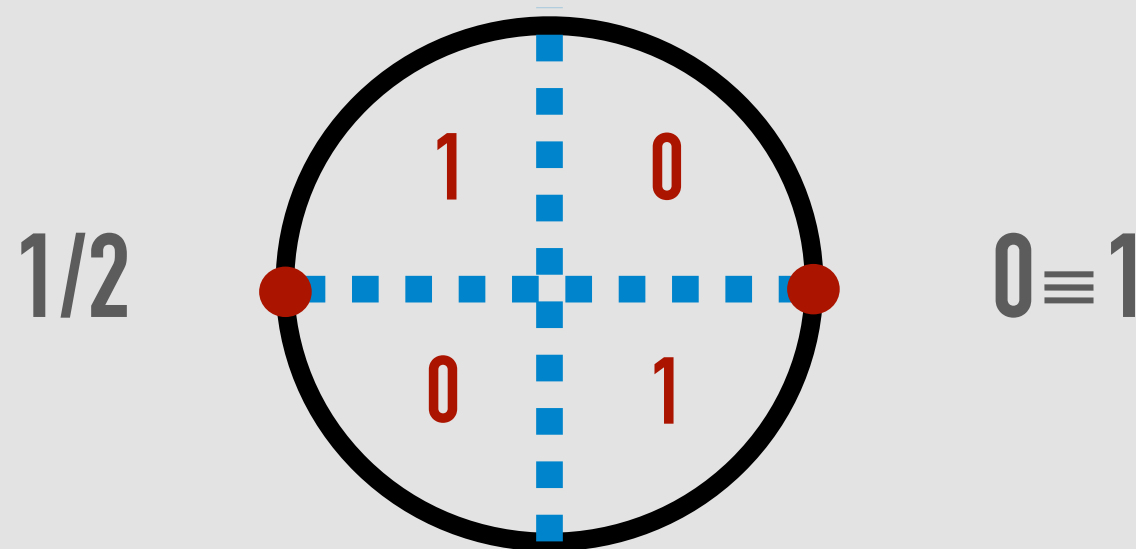
KEY RECONCILIATION

- If Alice's approximation is $k \in (\mathbb{R} / \mathbb{Z})$, Alice agrees on the bit $1 - \lfloor 2(k - 1/2) \rfloor$ and sends the **quadrant-bit** to help Bob correct his approximation: this bit is **uniformly distributed**.



KEY RECONCILIATION

- More sophisticated key reconciliation is possible using higher-dimensional lattices:
 - see NewHope and other NIST submissions.



KYBER SETTINGS

- Ring $\mathbb{Z}_{3329}[X] / (X^{256}+1)$ for fast NTT multiplication: $3329 \equiv 1 \pmod{256}$
- 2x2, 3x3 and 4x4 matrices
- Decryption failure probability $\leq 2^{-139}$
- Small distribution = binomial over $\{-2, \dots, 2\} = 0/1 + 0/1 - 0/1 - 0/1$

ANOTHER LOOK

ABSTRACTING DH

- Let $e: (a,b) \mapsto g^{ab}$.

This map is a **pairing**:

$\mathbb{Z}_q \times \mathbb{Z}_q \rightarrow G$ is bilinear.

- Let $f: a \mapsto g^a$ be the DL one-way function

$\mathbb{Z}_q \rightarrow G$

- $e(a,b)$ can be computed using $(f(a),b)$ or $(a,f(b))$, i.e. **even if a or b is hidden by f**.
- Security = hard to distinguish $(f(a),f(b),e(a,b))$ from $(f(a),f(b),\text{random})$. This is called **DDH**.

DH WITH LATTICES?

- What would be the pairing?
- What would be the one-way function to hide inputs?

THE SIS ONE-WAY FUNCTION

- Let $g_1, \dots, g_m$ be uniformly distributed over G .
 - The input set is $\{-1, 0, 1\}^m$ or any small subset of $\mathbf{Z}^m$.
 - $f_g(\mathbf{x}_1, \dots, \mathbf{x}_m) = \sum_i \mathbf{x}_i g_i \in G$.
- Inversion is as hard as SIS.

THE LWE ONE-WAY FUNCTION

- Let $g_1, \dots, g_m$ be uniformly distributed over G .
 - The input is a pair $(\mathbf{s}, \mathbf{e})$ where $\mathbf{s}$ is a character in $G^\times$ and $\mathbf{e}$ is small $\in (\mathbb{R}/\mathbb{Z})^m$
 - Then $f_g^x(\mathbf{s}, \mathbf{e}) = (\mathbf{s}(g_1), \dots, \mathbf{s}(g_m)) + \mathbf{e} \in (\mathbb{R}/\mathbb{Z})^m$
- Inversion is LWE.

PAIRING FROM LATTICES

- Let $g_1, \dots, g_m$ in G .

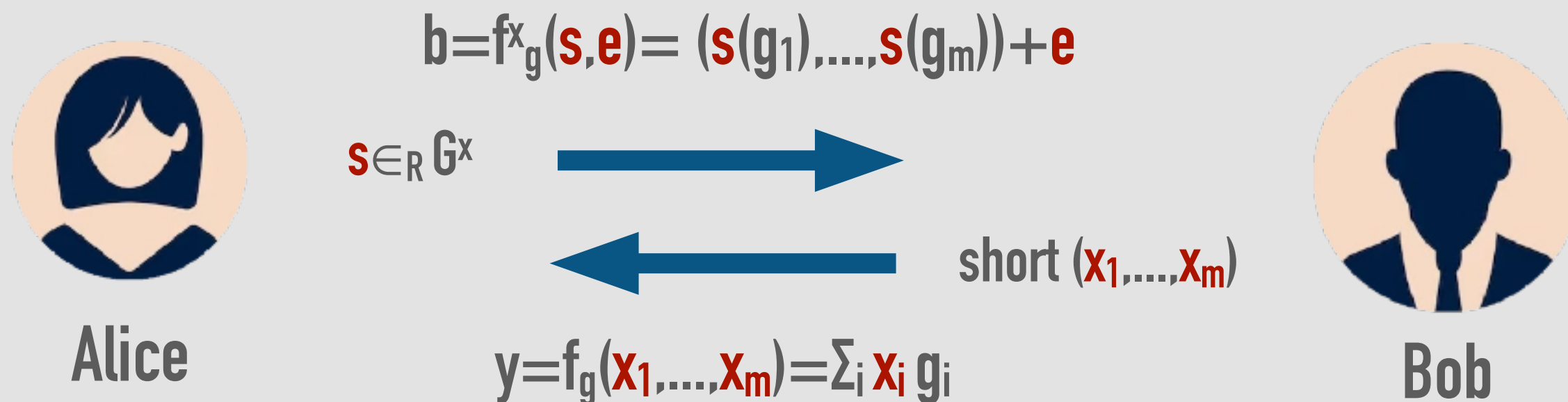
The dual group $G^\times$ induces a **pairing** $G^\times \times \mathbf{Z}^m \rightarrow \mathbf{R} / \mathbf{Z}$

by $\varepsilon(\mathbf{s}, (\mathbf{x}_1, \dots, \mathbf{x}_m)) = \mathbf{s}(\sum_i \mathbf{x}_i g_i)$

- Let $y = f_g(\mathbf{x}_1, \dots, \mathbf{x}_m) = \sum_i \mathbf{x}_i g_i \in G$ where $\mathbf{x}_i$'s small,
and $b = f_g^\times(\mathbf{s}, \mathbf{e}) = (\mathbf{s}(g_1), \dots, \mathbf{s}(g_m)) + \mathbf{e} \in (\mathbf{R} / \mathbf{Z})^m$, $\mathbf{e}$ small.
- Then $\varepsilon(\mathbf{s}, (\mathbf{x}_1, \dots, \mathbf{x}_m))$ can be computed from $(\mathbf{s}, y)$ or $(b, (\mathbf{x}_1, \dots, \mathbf{x}_m))$
as $\mathbf{s}(\sum_i \mathbf{x}_i g_i) = \sum_i \mathbf{x}_i \mathbf{s}(g_i) \approx \langle (\mathbf{x}_1, \dots, \mathbf{x}_m), b \rangle$ because the $\mathbf{x}_i$'s are small.

NOISY KEY-EXCHANGE FROM LATTICES

- Let $g_1, \dots, g_m$ generate G .



- Both compute an approx. of $\varepsilon(\mathbf{s}, (\mathbf{x}_1, \dots, \mathbf{x}_m)) = \mathbf{s}(\mathbf{y})$:
Alice computes $\mathbf{s}(\mathbf{y}) + \mathbf{e}'$ and Bob computes $\sum_i \mathbf{x}_i \mathbf{b}_i$.
- Security is related to DDH.

EL GAMAL ENCRYPTION FROM LATTICES

- This key exchange gives rise to **two El Gamal-like** public-key encryption schemes, because the lattice pairing is **not symmetric**.
- These El-Gamal-like schemes are IND-CPA-secure under the hardness of LWE / SIS.
- Similarly, many LWE / SIS schemes can be viewed as analogues of the RSA / DL world.

LATTICE EL GAMAL I [REGEV05]

- Let $g_1, \dots, g_m$ generate G
- Secret key $\mathbf{s} \in_R G^x$

Public key $\mathbf{b} = f_g^x(\mathbf{s}, \mathbf{e}) = (\mathbf{s}(g_1), \dots, \mathbf{s}(g_m)) + \mathbf{e}$

- Encrypt $\mathbf{m} \in \{0, 1\}$ as $(y, c) \in G^x(\mathbf{R} / \mathbf{Z})$
- $y = f_g(\mathbf{x}_1, \dots, \mathbf{x}_m) = \sum_i \mathbf{x}_i g_i$ where $(\mathbf{x}_1, \dots, \mathbf{x}_m)$ is short
- $c = \mathbf{s}(y) + \mathbf{e}' + (m / 2)$
- Decrypt (y, c) as $\lfloor 2(\mathbf{s}(y) - c) \rfloor \in \{0, 1\}$

LATTICE EL GAMAL II [GPV08]

- Let $g_1, \dots, g_m$ generate G
- Secret key **short** $(\mathbf{x}_1, \dots, \mathbf{x}_m) \in \mathbb{Z}^m$
Public key $y = f_g(\mathbf{x}_1, \dots, \mathbf{x}_m) = \sum_i \mathbf{x}_i g_i$
- Encrypt $\mathbf{m} \in \{0, 1\}$ as $(b, c) \in (\mathbb{R} / \mathbb{Z})^m \times (\mathbb{R} / \mathbb{Z})$
- $b = f_g^x(\mathbf{s}, \mathbf{e}) = (\mathbf{s}(g_1), \dots, \mathbf{s}(g_m)) + \mathbf{e}$ where $\mathbf{s} \in_R G^x$
- $c = \sum_i \mathbf{x}_i b_i + (m/2)$
- Decrypt (b, c) as $\lfloor 2(\sum_i \mathbf{x}_i b_i - c) \rfloor \in \{0, 1\}$

HOMOMORPHIC ENCRYPTION

- El Gamal is well-known to be homomorphic with respect to the group operation G : the product of ciphertexts is a ciphertext of the product.
- Our Lattice El Gamal are bounded-homomorphic.
- How about our Trapdoor Encryption?