THE MATHEMATICS OF LATTICE-BASED CRYPTOGRAPHY

3. Learning With Errors (LWE) Problem

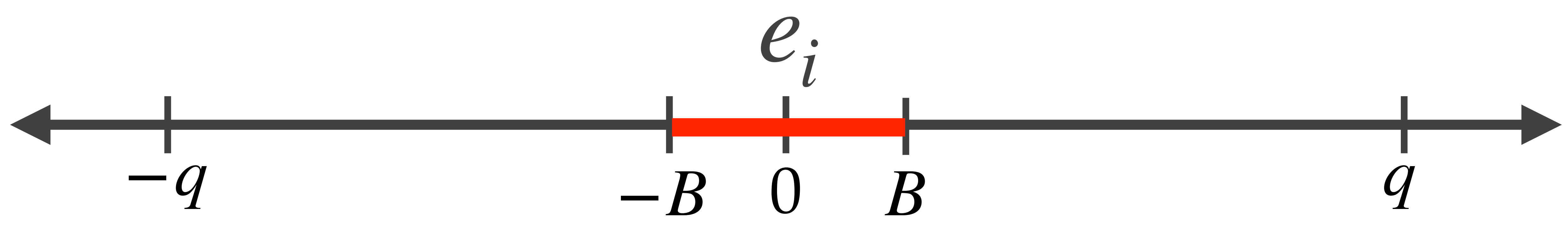
Alfred Menezes
cryptography101.ca

Outline

1. LWE definition
2. LWE parameters
3. Decisional LWE
4. Short-secret LWE (ss-LWE)
5. Application: Lindner-Peikert public-key encryption scheme

LWE definition

- **Notation**:
  - $\mathbb{Z}_q = \{0,1,2,\ldots,q-1\}$.
  - $x \in_R S$ means that x is selected uniformly (and independently) at random from S.
  - All vectors are column vectors.
- LWE was introduced by Regev in 2005.
- **Definition**. *Learning With Errors problem*: LWE(m,n,q,B)
  Let $s \in_R \mathbb{Z}_q^n$ and $e \in_R [-B,B]^m$ where $B \ll q/2$.
  Given $A \in_R \mathbb{Z}_q^{m\times n}$ and $b = As + e \pmod{q} \in \mathbb{Z}_q^m$, find s.



LWE example

- Let $m = 5, n = 3, q = 31$, and $B = 2$.
- **LWE instance:**

$$A = \begin{bmatrix} 11 & 3 & 27 \\ 12 & 21 & 7 \\ 6 & 23 & 30 \\ 5 & 6 & 2 \\ 21 & 0 & 14 \end{bmatrix}, \quad b = \begin{bmatrix} 25 \\ 25 \\ 12 \\ 29 \\ 17 \end{bmatrix}.$$

- **LWE challenge**: We need to find $s \in \mathbb{Z}_{31}^3$ and $e \in [-2,2]^5$ with $As + e = b \pmod{31}$.

- In fact, there are *three* LWE solutions:
  $s = (2,11,7)^T, \quad e = (-2,0,2,1,1)^T,$
  $s = (27,13,16)^T, \quad e = (1,-2,1,1,1)^T,$
  $s = (30,9,5^T), \quad e = (-2,-1,2,1,-1)^T.$
- In general, one cannot guarantee that there is a unique LWE solution.
- So, the LWE parameters must be carefully selected so that the probability that an LWE instance has more than one solution is negligibly small.

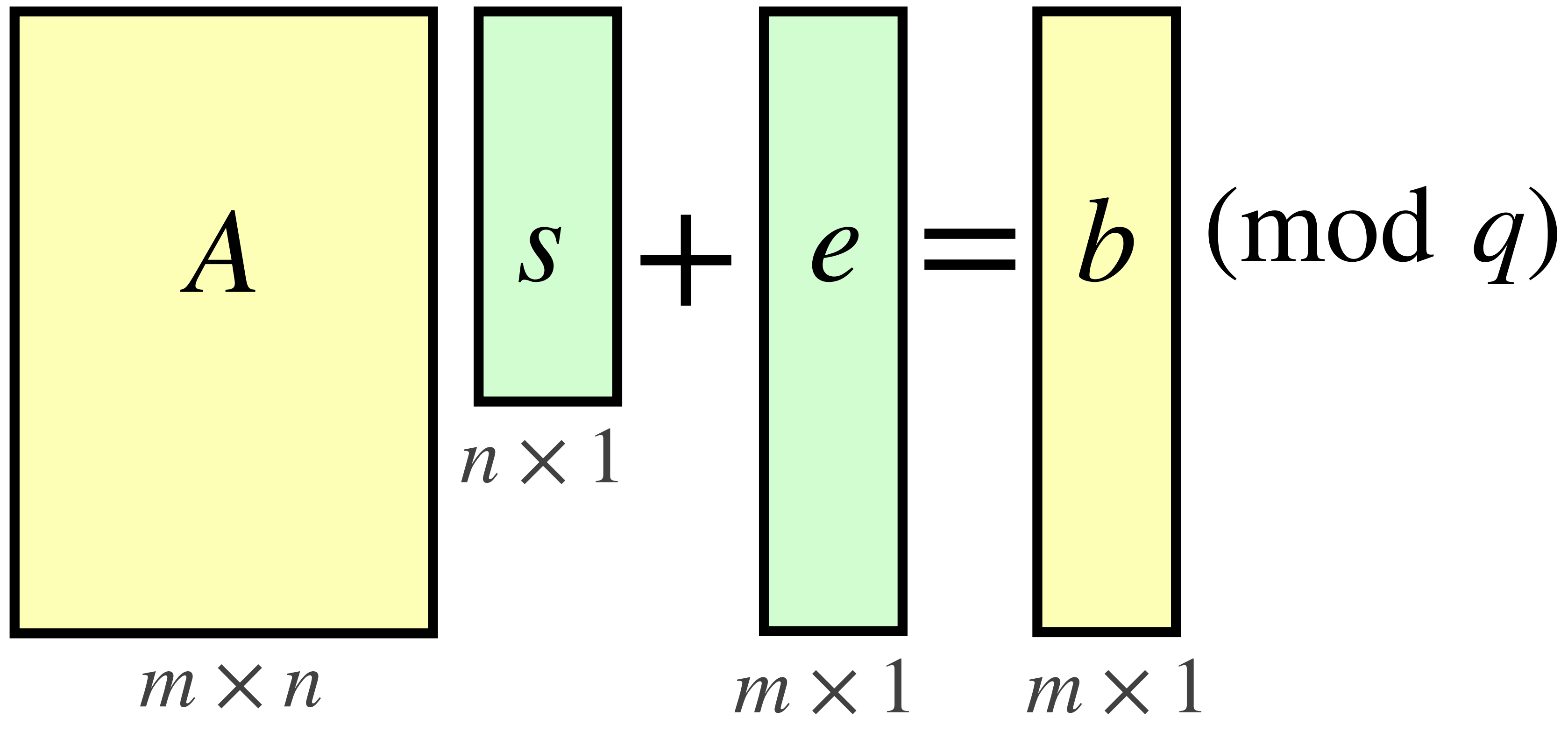
LWE parameter B

1. If $B = 0$ (so $e = 0$), then $As = b \pmod{q}$ can be solved efficiently.

2. If $B = (q-1)/2$, then finding s is information-theoretically impossible.
So, we'll henceforth assume that $B < q/4$.

3. (Arora-Ge) If B is asymptotically smaller than $\sqrt{n}$, then LWE can be solved in subexponential time for sufficiently large $m \gg n$.

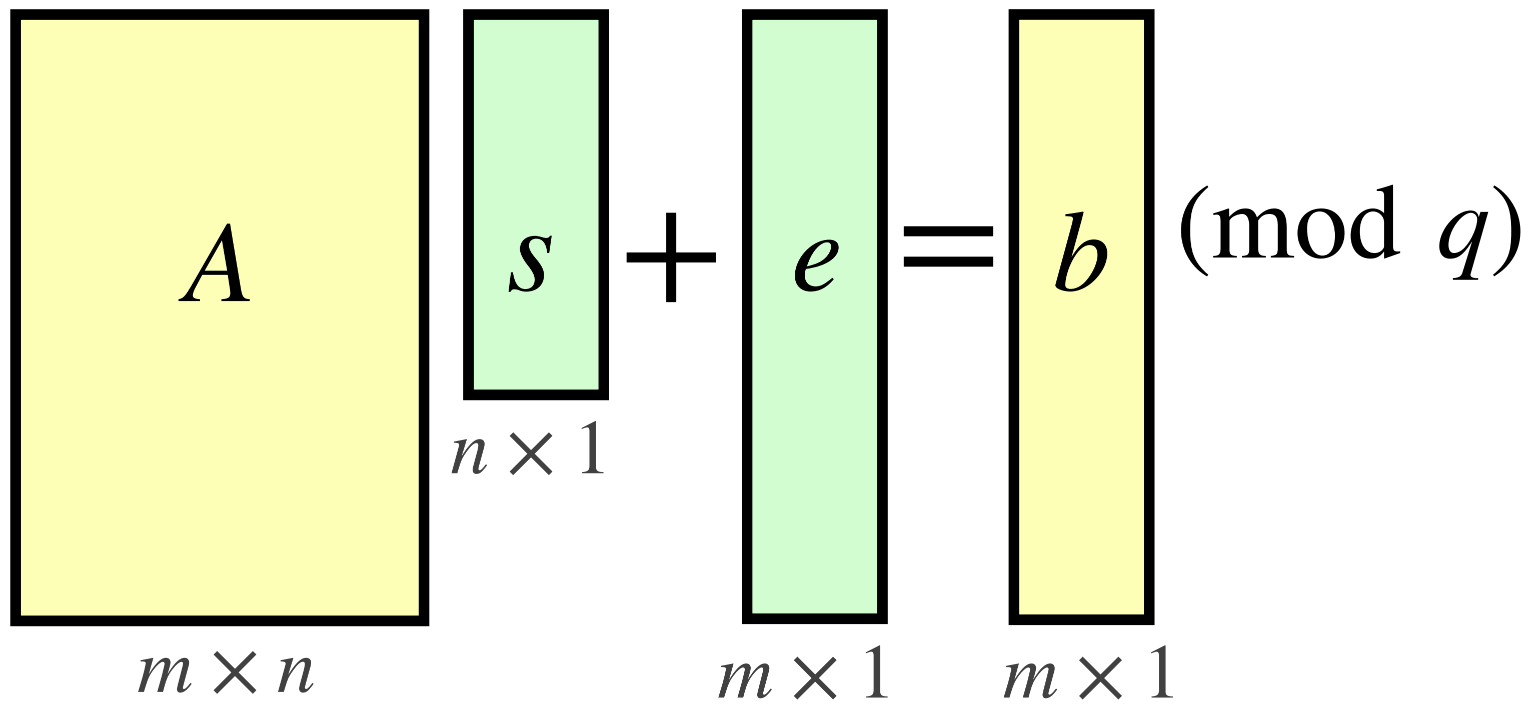
LWE: Let $s \in_R \mathbb{Z}_q^n$ and $e \in_R [-B, B]^m$ where $B \ll q/2$. Given $A \in_R \mathbb{Z}_q^{m \times n}$ and $b = As + e \pmod{q} \in \mathbb{Z}_q^m$, find s.

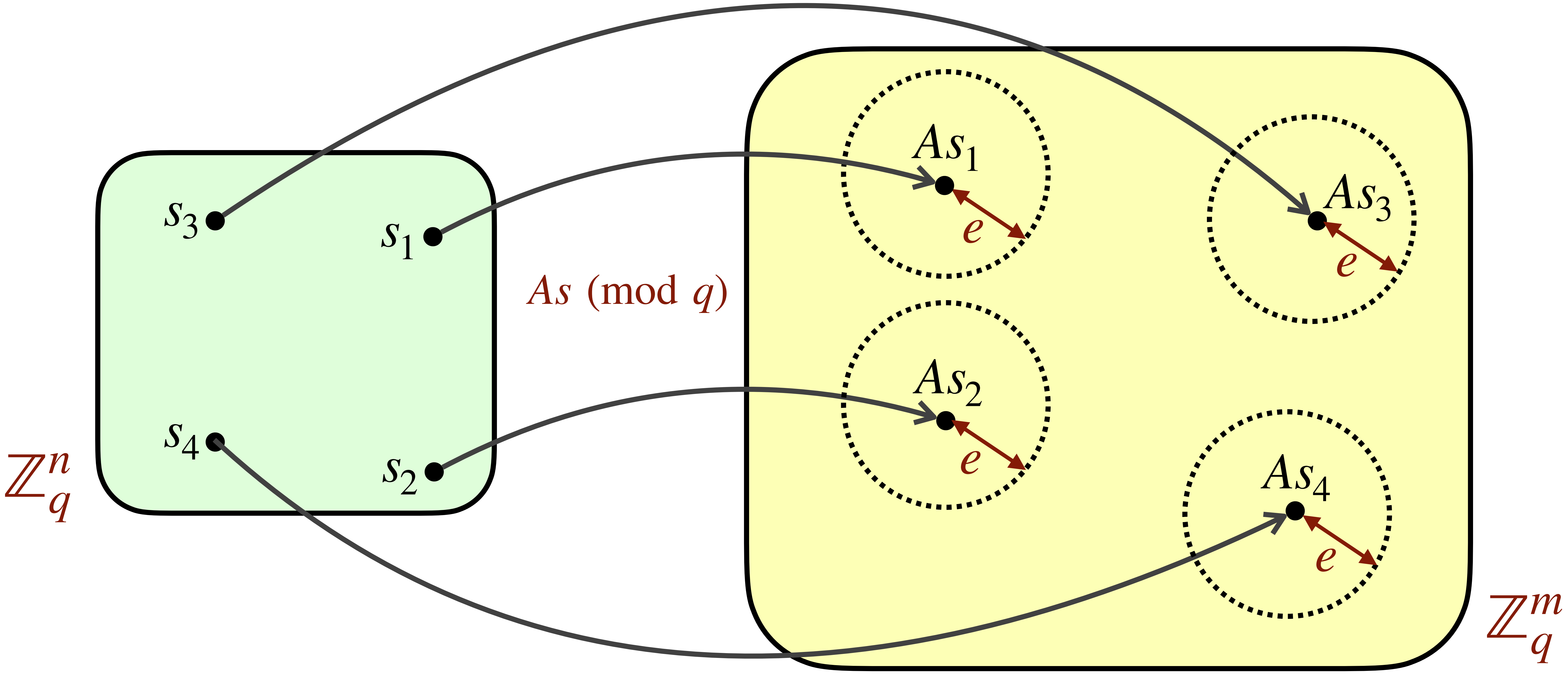


LWE parameters m and n

- If $m \gg n$, then one expects that there is a unique LWE solution (s, e).
- Henceforth, we'll assume that $m \gg n$.

LWE: Let $s \in_R \mathbb{Z}_q^n$ and $e \in_R [-B, B]^m$ where $B \ll q/2$. Given $A \in_R \mathbb{Z}_q^{m \times n}$ and $b = As + e \pmod{q} \in \mathbb{Z}_q^m$, find s.

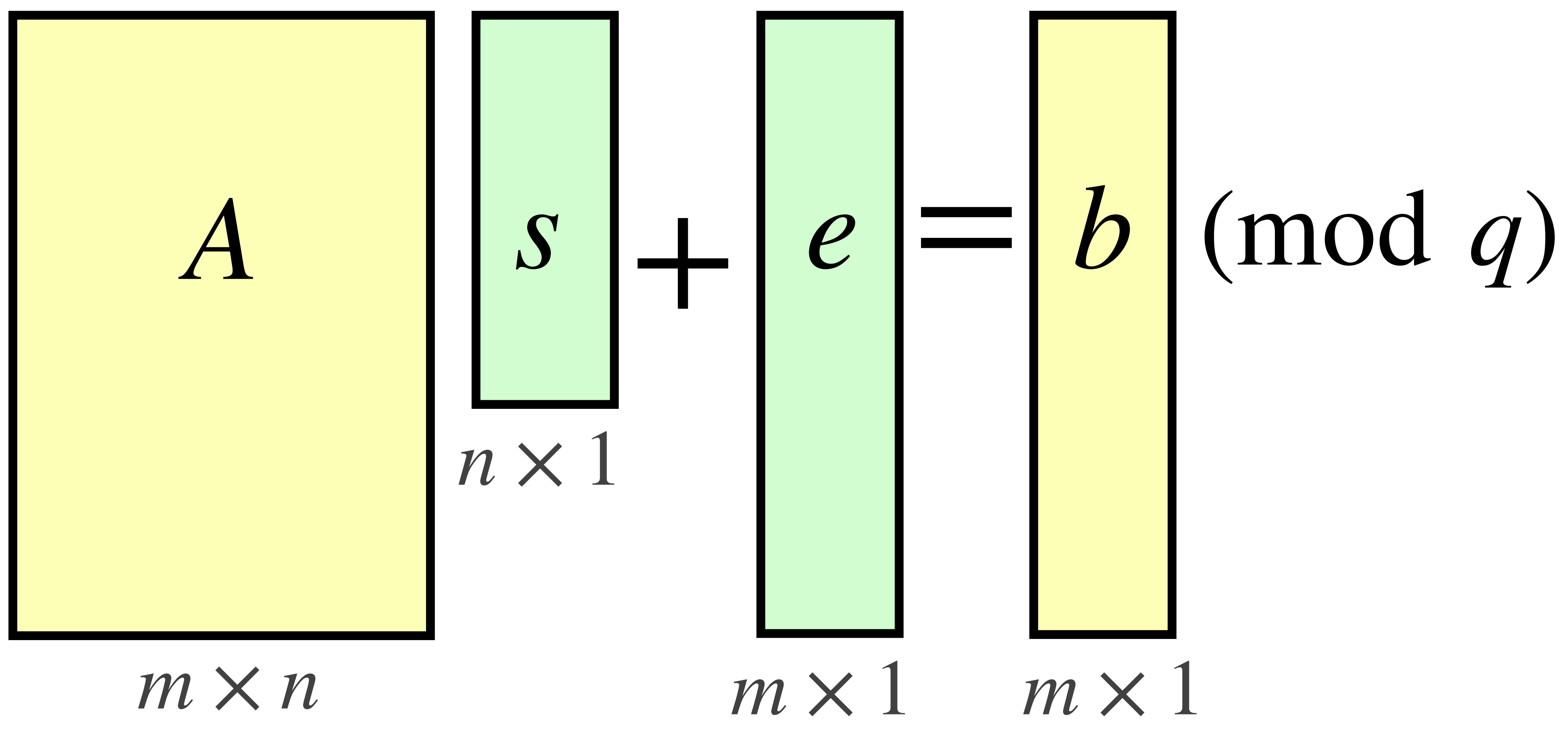


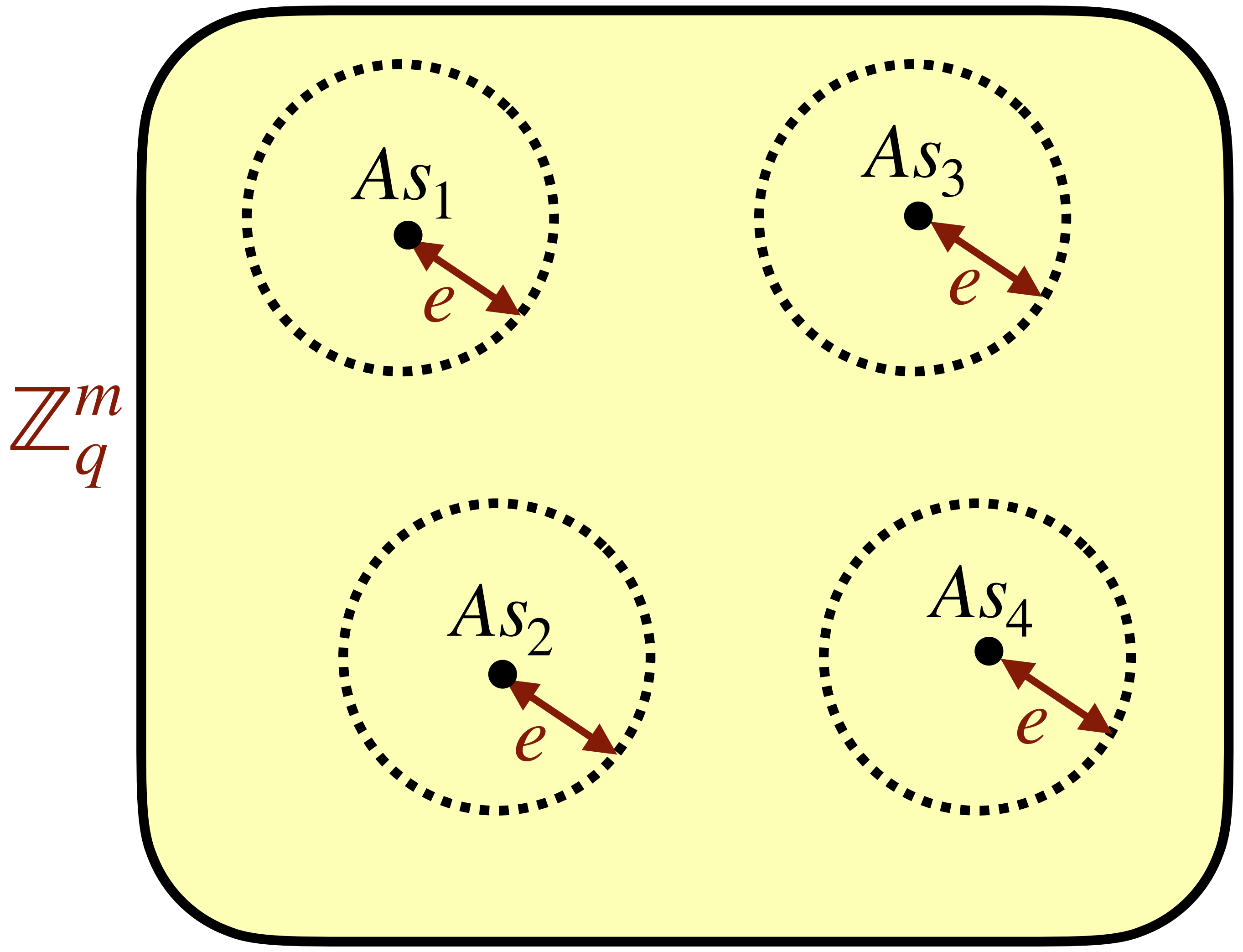


Uniqueness of the LWE solution is only guaranteed if no two of the q^n spheres centred at the vectors $As \pmod{q}$ overlap.

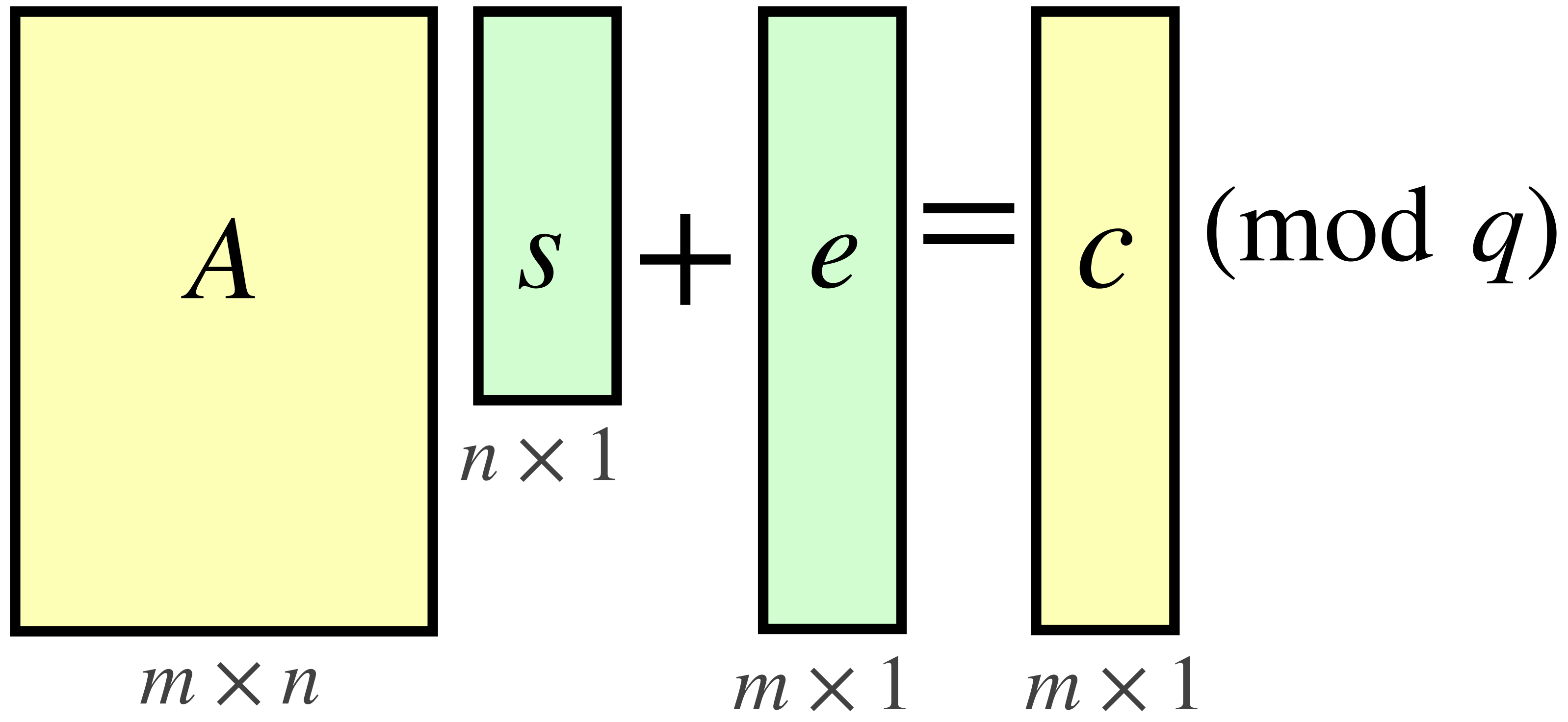
Decisional LWE (DLWE)

Definition. *Decisional LWE problem*: DLWE(m,n,q,B)
Let $A \in_R \mathbb{Z}_q^{m\times n}$, $s \in_R \mathbb{Z}_q^n$, $e \in_R [-B,B]^m$ where $B \ll q/2$, and $b = As + e$.
Let $r \in_R \mathbb{Z}_q^m$.
Let $c = b$ with probability $1/2$, and $c = r$ with probability $1/2$.
Given (A,c), the problem is to decide (with success probability significantly greater than $1/2$) whether $c = b$ or $c = r$.





DLWE and LWE are equivalent (1)



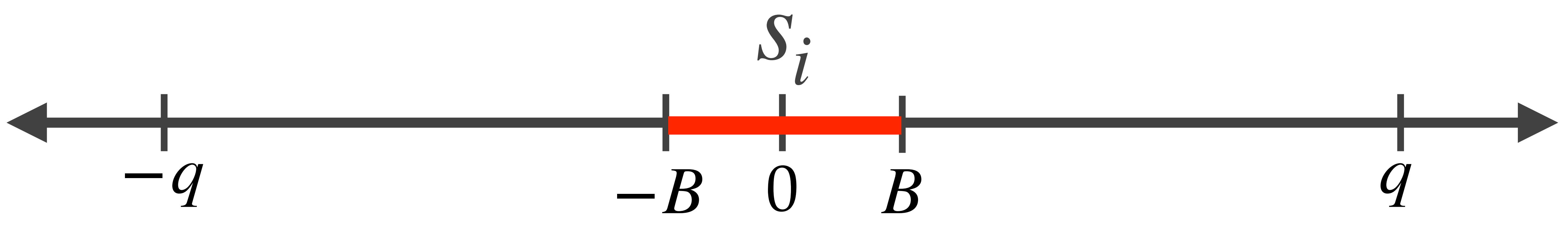
- **Claim**. DLWE and LWE are equivalent.
- **Claim 1**. DLWE $\leq$ LWE.
- **Proof**. Let (A, c) be a DLWE instance.
  Now, if $c = b$, then (A, c) is an LWE instance and so one expects that $As + e = c \pmod q$ has a unique LWE solution (s, e) (with $e \in [-B, B]^m$).
  And, if $c = r$, then one expects that $As + e = c$ does not have an LWE solution.
  So, the LWE solver is run with input (A, c). If a valid LWE solution is returned, then one concludes that $c = b$. If the LWE solver terminates without a valid LWE solution, or fails to terminate, then one concludes that $c = r$. $\square$

DLWE and LWE are equivalent (2)

- **Claim 2** LWE $\leq$ DLWE.
- **Proof**. Let (A, b) be an LWE instance (where $b = As + e$). We'll use a DLWE solver to test our guesses for the coordinates of s, one at a time, beginning with s_1.
  Let $d \in \mathbb{Z}_q$. Here's how we test whether $s_1 = d$.
  Select $\Delta \in_R \mathbb{Z}_q^m$. Let A' be the matrix obtained by adding Δ to the first column of A, and let $b' = b + d\Delta$.
  Now, if $s_1 = d$, then $b' = A's + e$, so (A', b') is a valid LWE instance.
  On the other hand, if $s_1 \neq d$, then $b' = A's + e + (d - s_1)\Delta$. Since $d - s_1$ is nonzero, and Δ in uniformly random and independent of A', s and e, it follows that b' is uniformly random and independent of A'.
  Thus, the DLWE solver with input (A', b') will inform us whether or not $s_1 = d$. $\square$

Short-Secret LWE (ss-LWE)

- **Definition**. *Short-secret LWE problem*: ss-LWE(m, n, q, B)
  Let $s \in_R [-B, B]^n$ and $e \in_R [-B, B]^m$ where $B \ll q/2$.
  Given $A \in_R \mathbb{Z}_q^{m \times n}$ and $b = As + e \pmod{q} \in \mathbb{Z}_q^m$, find s.



- **Claim**. LWE and ss-LWE are equivalent.
  More precisely, ss-LWE$(m, n, q, B) \leq$ LWE(m, n, q, B)
  and LWE$(m, n, q, B) \leq$ ss-LWE$(m - n, n, q, B)$.

- **Exercise**. ss-LWE and ss-DLWE are equivalent.

ss-LWE and LWE are equivalent (1)

- **Claim 1**. ss-LWE$(m, n, q, B) \leq$ LWE(m, n, q, B).
- **Proof**. Let (A, b) be an ss-LWE(m, n, q, B) instance, where $b = As + e \pmod{q}$ and $s \in_R [-B, B]^n$ and $e \in_R [-B, B]^m$.
  Select $d \in_R \mathbb{Z}_q^n$ and let $b' = b + Ad = (As + e) + Ad = A(s + d) + e$.
  Then (A, b') is an LWE(m, n, q, B) instance.
  The solution (s', e) to this LWE instance, immediately gives the solution $(s' - d, e)$ to the ss-LWE instance. $\square$

ss-LWE and LWE are equivalent (2)

- **Claim 2**. LWE$(m, n, q, B) \leq$ ss-LWE$(m-n, n, q, B)$.
- **Proof**. Let (A, b) be an LWE(m, n, q, B) instance, so $b = As + e$.
  Let $A = \begin{bmatrix} A_1 \\ A_2 \end{bmatrix}$, $b = \begin{bmatrix} b_1 \\ b_2 \end{bmatrix}$, and $e = \begin{bmatrix} e_1 \\ e_2 \end{bmatrix}$ where $A_1, A_2, b_1, b_2, e_1, e_2$ have dimensions $n \times n$, $(m-n) \times n$, $n \times 1$, $(m-n) \times 1$, $n \times 1$, and $(m-n) \times 1$, respectively.
  Let $A' = -A_2 A_1^{-1} \in \mathbb{Z}_q^{(m-n)\times n}$ and $b' = A'b_1 + b_2 \in \mathbb{Z}_q^{m-n}$.
  Now, $b' = A'b_1 + b_2 = (-A_2A_1^{-1})(A_1 s + e_1) + (A_2 s + e_2)$
  $= -A_2 s - A_2 A_1^{-1} e_1 + A_2 s + e_2 = A'e_1 + e_2$.
  Thus, (A', b') is an ss-LWE$(m-n, n, q, B)$ instance.
  A solution to the ss-LWE instance immediately gives a solution to the LWE instance. $\square$

PKE: Key generation

[Lindner-Peikert 2011]

Key generation: Alice does:

1. Select $s \in_R [-B, B]^n$ and $e \in_R [-B, B]^n$.
2. Select $A \in_R \mathbb{Z}_q^{n \times n}$.
3. Compute $b = As + e \pmod{q}$.
4. Alice's **public key** is (A, b); her **private key** is s.

- Determining any information about s from (A, b) is an instance of **ss-DLWE**(n, n, q, B).

PKE: Encryption and decryption

Encryption: To encrypt a message $m \in \{0,1\}$ for Alice, Bob does:

1. Obtain an authentic copy of Alice's encryption key (A, b).
2. Select $r, z \in_R [-B, B]^n$ and $z' \in_R [-B, B]$.
3. Compute $c_1 = A^T r + z$ and $c_2 = b^T r + z' + m\lfloor q/2 \rceil$.
4. Output $c = (c_1, c_2)$.

<u>**Note**</u>: $c \in \mathbb{Z}_q^n \times \mathbb{Z}_q$.

Decryption: To decrypt $c = (c_1, c_2)$, Alice does:

1. Output $m = \text{Round}_q(c_2 - s^T c_1)$.

<u>Note</u>: Alice uses her private key s.

Round$_q$: For $x \in [0, q-1]$, define

$$x \text{ mods } q = \begin{cases} x & \text{if } x \le (q-1)/2, \\ x - q & \text{if } x > (q-1)/2. \end{cases}$$

Then

$$\text{Round}_q(x) = \begin{cases} 0, & \text{if } -q/4 < x \text{ mods } q < q/4, \\ 1, & \text{otherwise}. \end{cases}$$

Toy example: PKE (1)

- **Domain parameters**: $n = 3,\ q = 229,\ B = 2.$
- **Key generation:** Alice selects:

$$A = \begin{bmatrix} 101 & 173 & 27 \\ 192 & 121 & 7 \\ 116 & 223 & 30 \end{bmatrix},\ s = \begin{bmatrix} 2 \\ -2 \\ 1 \end{bmatrix},\ \ e = \begin{bmatrix} 0 \\ -2 \\ 1 \end{bmatrix},\ \text{ and computes}$$

$$b = As + e \pmod{229} = \begin{bmatrix} 112 \\ 147 \\ 17 \end{bmatrix}.$$

Alice's **encryption key** is (A, b); her **decryption key** is s.

Toy example: PKE (2)

- **Encryption**: To encrypt the plaintext bit $m = 1$, Bob selects

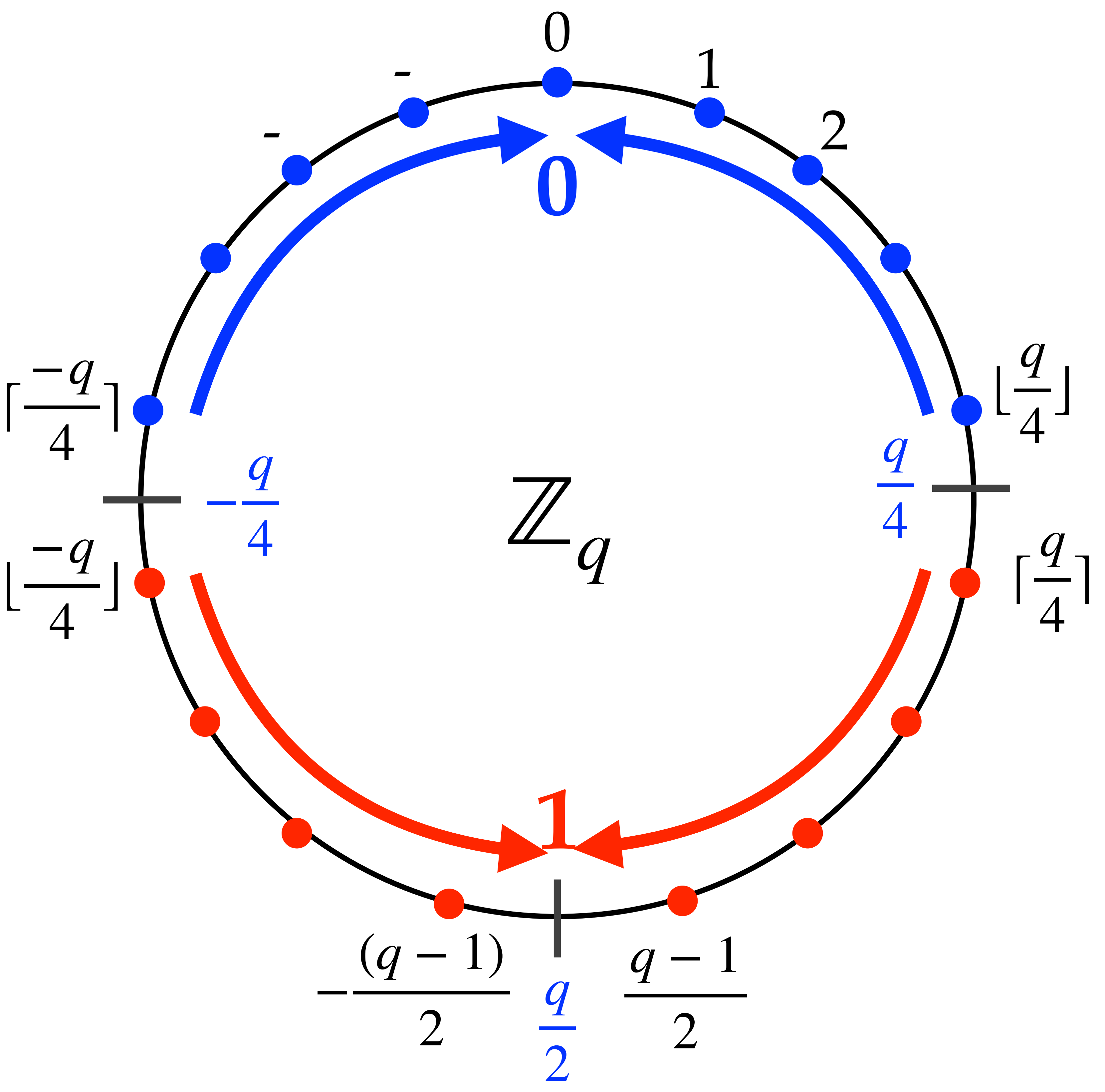
  $$r = \begin{bmatrix} 2 \\ -2 \\ -1 \end{bmatrix}, \quad z = \begin{bmatrix} 0 \\ 1 \\ -2 \end{bmatrix}, \quad z' = -2, \text{ and computes}$$

  $$c_1 = A^T r + z \pmod{229} = \begin{bmatrix} 160 \\ 111 \\ 37 \end{bmatrix} \text{ and } c_2 = b^T r + z' + 115m \pmod{229} = 26.$$

  The **ciphertext** is $c = (c_1, c_2)$.
- **Decryption**: To decrypt $c = (c_1, c_2)$, Alice uses her decryption key s to compute $c_2 - s^T c_1 \pmod{229} = 120$.
  Now, $120 \text{ mods } 229 = -109$, and $\text{Round}_{229}(-109) = 1$.
  Thus, Alice recovers the plaintext $m = 1$.

PKE: Decryption works

- **Question**: Does decryption work?
  i.e., does $m = \mathrm{Round}_q(c_2 - s^T c_1)$?
- We have $c_2 - s^T c_1 = (b^T r + z' + m\lceil q/2 \rfloor) - s^T(A^T r + z)$
  $$= (s^T A^T + e^T) r + z' + m\lceil q/2 \rfloor - s^T(A^T r + z)$$
  $$= e^T r - s^T z + z' + m\lceil q/2 \rfloor .$$
- So, decryption works iff
  $| e^T r - s^T z + z' \bmod s\ q | < q/4$.
- Now, suppose that $B \le \sqrt{q/(4(2n+1))}$.
- Then $| e^T r - s^T z + z' \bmod s\ q | \le nB^2 + nB^2 + B \le \dfrac{2nq}{4(2n+1)} + \sqrt{\dfrac{q}{4(2n+1)}}$
  $$= \frac{nq}{2(2n+1)} + \sqrt{\frac{q}{4(2n+1)}} < \frac{q}{4},$$
  so decryption works. $\square$



PKE: Security

- **Claim**: The Lindner-Peikert PKE is indistinguishable against chosen-plaintext attack assuming that ss-DLWE is hard.
- **Proof**: The encryption operation can be written as: $\begin{bmatrix} c_1 \\ c_2 \end{bmatrix} = \begin{bmatrix} A^T \\ b^T \end{bmatrix} r + \begin{bmatrix} z \\ z' \end{bmatrix} + \begin{bmatrix} 0 \\ \lceil \frac{q}{2} \rfloor m \end{bmatrix}$.

  By the ss-DLWE assumption, $\begin{bmatrix} A^T \\ b^T \end{bmatrix}$ is indistinguishable from random.

  Again by the ss-DLWE assumption, $\begin{bmatrix} A^T \\ b^T \end{bmatrix} r + \begin{bmatrix} z \\ z' \end{bmatrix} = \begin{bmatrix} A^T r + z \\ b^T r + z' \end{bmatrix}$ is indistinguishable from random.

  Thus, from the adversary's perspective, c_2 appears to be the sum of the random element $b^T r + z' \in \mathbb{Z}_q$ and the plaintext $\lceil \frac{q}{2} \rfloor m$, so the adversary can learn nothing about m. $\square$