

POST-QUANTUM CRYPTOGRAPHY EXPLAINED

for security professionals

FrodoKEM

ALFRED MENEZES

INTRODUCTION

- **FrodoKEM** is a quantum-safe **key encapsulation mechanism** (KEM) whose security relies on hardness of the **Learning With Errors** (LWE) problem in **unstructured lattices**.
 - This is in contrast with Kyber (ML-KEM), whose security relies on hardness of LWE in structured lattices.
- FrodoKEM advanced to Round 3 as an alternate candidate in NIST's PQC standardization project, but was not selected.
 - **High bandwidth and performance costs** relative to Kyber.
- In June 2026, **ISO** standardized FrodoKEM (together with ML-KEM and ClassicMcEliece) as part of ISO/IEC 18033-2.
 - Several government agencies have also endorsed FrodoKEM, including Germany's **BSI**, France's **ANSSI**, and the Netherlands' **NLNCSA**.

LINDNER-PEIKERT PKE: KEY GENERATION

- **Key generation.** Alice does the following:

1. Select a random $n \times n$ matrix A with entries in $\mathbb{Z}_q$.

2. Select random length- n vectors s and e with entries in $[-B, B]$.

3. Compute $b = As + e \pmod{q}$.

$$b = As + e$$

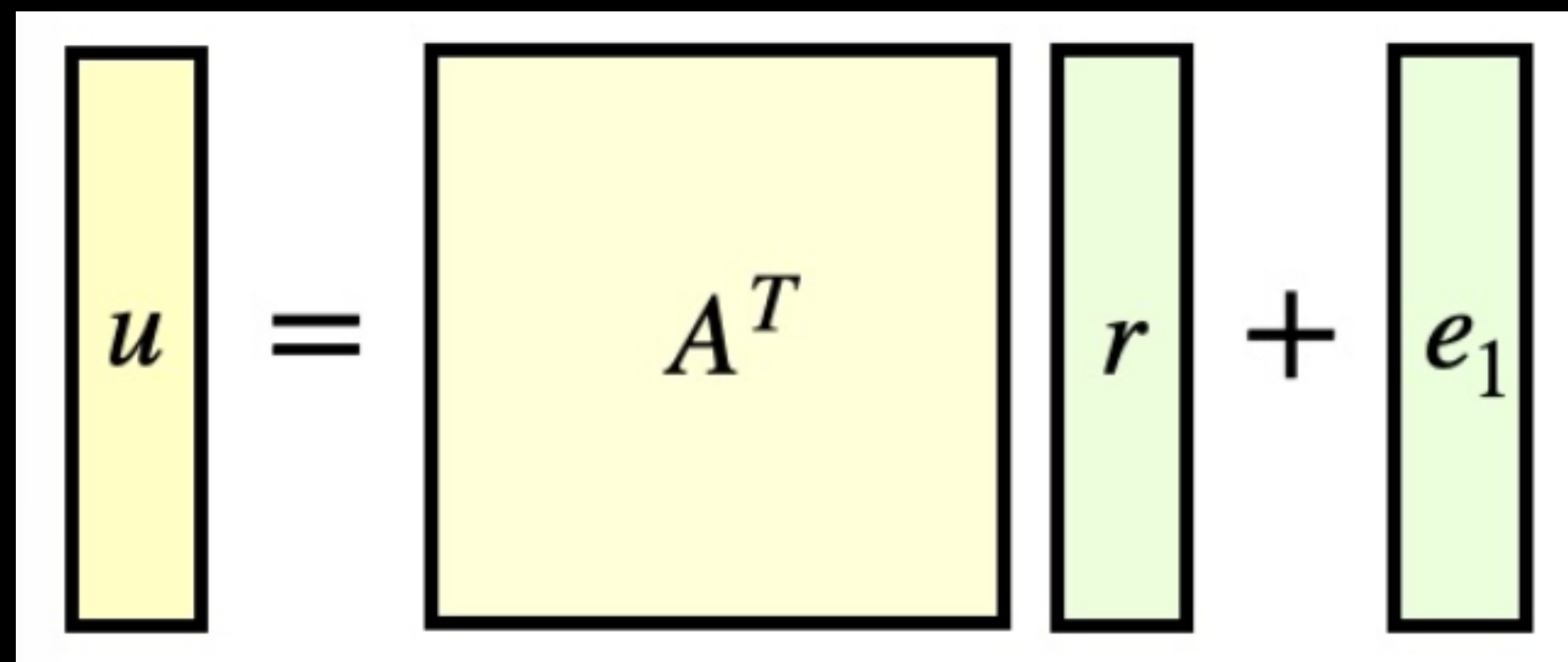
4. Alice's **public key** is (A, b) ; her **private key** is (s, e) .

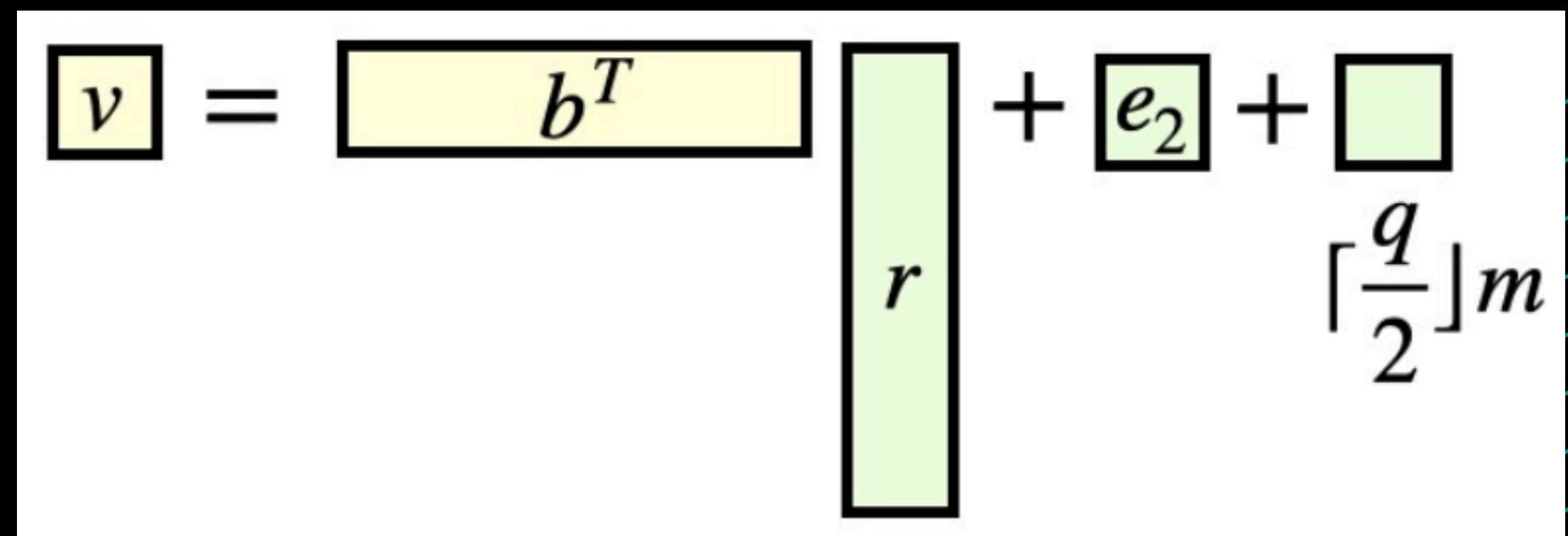
- **Note:** Computing the private key from the public key is an instance of **ss-LWE**.

LINDNER-PEIKERT PKE: ENCRYPTION

• **Encryption.** To encrypt a bit $m \in \{0,1\}$ for Alice, Bob does:

1. Select random length- n vectors r and e_1 with entries in $[-B, B]$, and a random number e_2 from $[-B, B]$.
2. Compute $u = A^T r + e_1$.
3. Compute $v = b^T r + e_2 + \lceil q/2 \rceil m$.
4. The **ciphertext** is $c = (u, v)$.

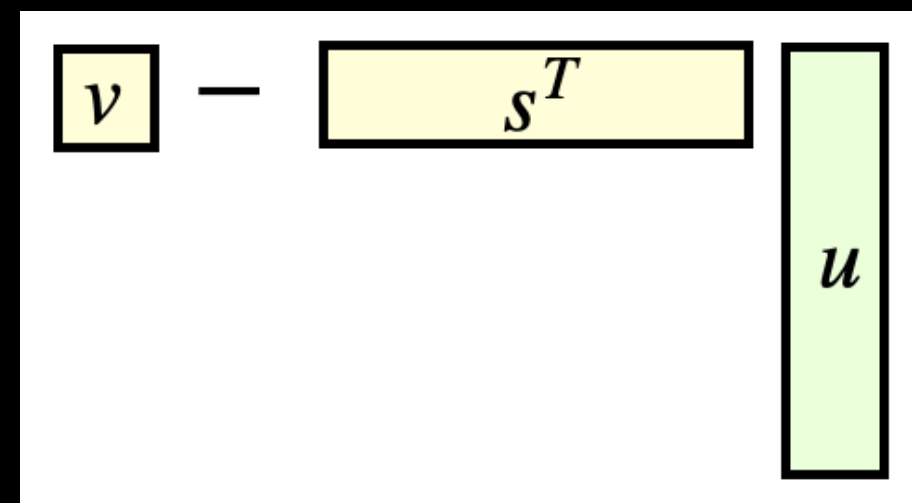

$$u = A^T r + e_1$$


$$v = b^T r + e_2 + \lceil \frac{q}{2} \rceil m$$

LINDNER-PEIKERT PKE: DECRYPTION

- **Decrypt.** To decrypt $c = (u, v)$, Alice does the following:

1. Compute $m = \text{Round}_q(v - s^T u)$.

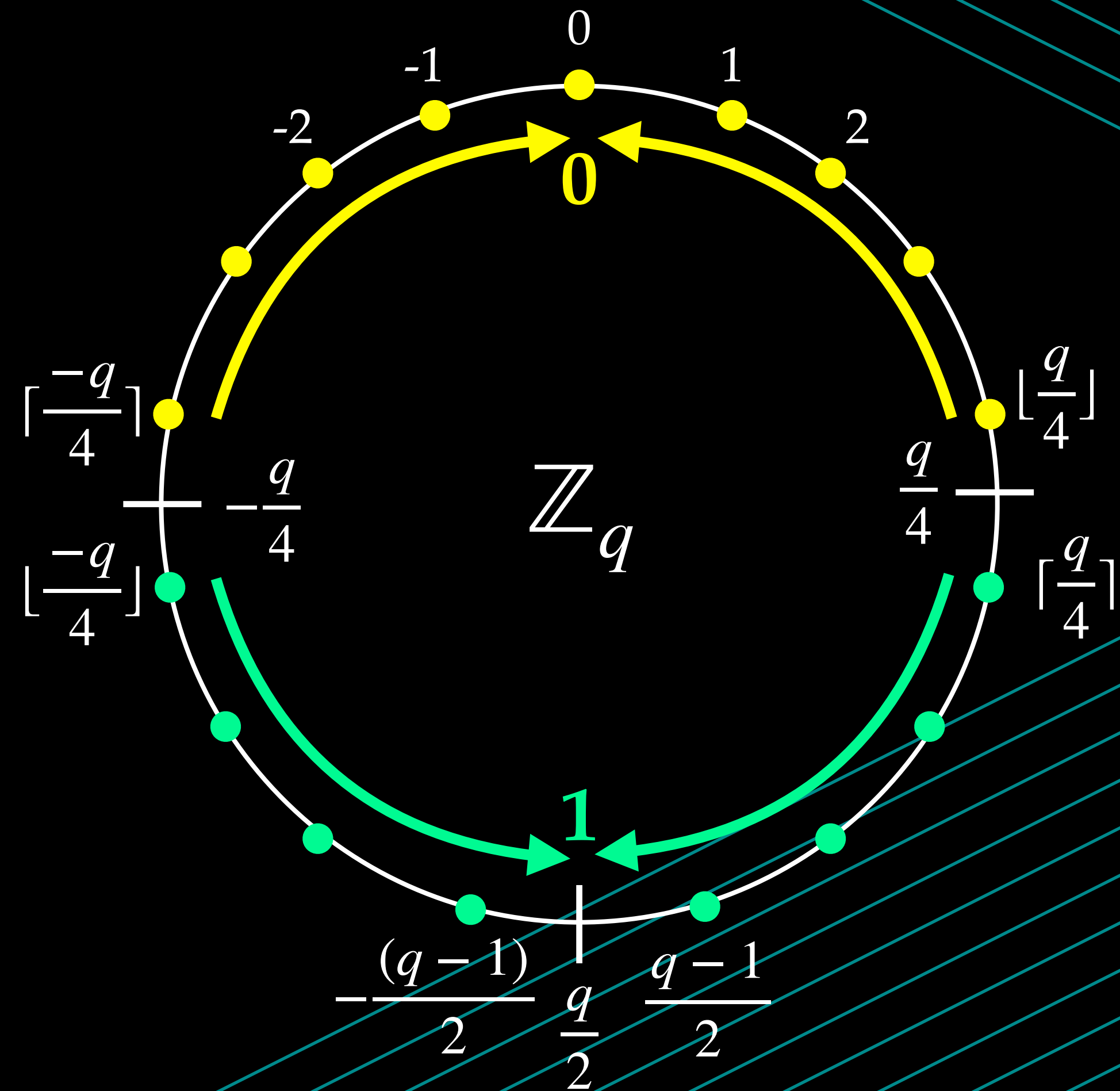


- **Correctness of decryption.** Observe that

$$\underline{v - s^T u} = \underline{e^T r - s^T e_1 + e_2 + \lceil q/2 \rceil m}.$$

So, decryption works if

$$\underline{|e^T r - s^T e_1 + e_2|} < q/4.$$



FROM LP-PKE to FrodoPKE

- The Kyber public-key encryption scheme (PKE) is derived from the Lindner-Peikert PKE by replacing elements in $\mathbb{Z}_q$ with **polynomials** of degree at most 255 with coefficients in $\mathbb{Z}_q$:
 $a_0 + a_1x + a_2x^2 + \dots + a_{255}x^{255}$.
- In contrast, FrodoPKE uses integers modulo a power of two ($q = 2^{15}$ or $q = 2^{16}$).
- Errors are sampled from a discrete approximation to a **rounded Gaussian distribution**.
- Within a key pair, the same matrix A is **reused** for several LWE instances.

FrodoPKE: KEY GENERATION

- **Key generation.** Alice does the following:

1. Select a random $n \times n$ matrix A with entries in $\mathbb{Z}_q$.
2. Select random $n \times \bar{n}$ **matrices** S and E with entries sampled from T_χ .
3. Compute $B = AS + E \pmod{q}$.
4. Alice's **public key** is (A, B) ; her **private key** is (S, E) .

$$A + S + E = B$$

- **Note:** Computing the private key from the public key is an instance of **ss-MatrixLWE**.
- **Notes:** A is generated from a 128-bit seed; $\bar{n} = 8$.

FrodoPKE: ENCRYPTION

$$U = A^T R + E_1$$

$$V = B^T R + E_2 + \text{Encode}(m)$$

Ciphertext is (U, V)

FrodoPKE: DECRYPTION

Compute $M = V - S^T U$

and

$m = \text{Decode}(M)$.

FROM FrodoPKE to FrodoKEM

- Apply the Fujisaki-Okamoto transform + salts to the Frodo public-key encryption scheme to obtain FrodoKEM.
- FrodoKEM has been proven to be indistinguishable under chosen-ciphertext attack assuming that the ss-D-MatrixLWE problem is intractable and that hash function H used is modelled as a random oracle.

PERFORMANCE

KEM	parameter set	NIST security level	public key (bytes)	ciphertext (bytes)	encapsulation time	decapsulation times
Kyber	ML-KEM-512	1	800	768	8.3μs	10.4μs
Frodo	Frodo-640	1	9,616	9,752	378.1μs	373.1μs
Kyber	ML-KEM-768	3	1,184	1,088	12.8μs	16.0μs
Frodo	Frodo-976	3	15,632	15,792	779.6μs	771.2μs
Kyber	ML-KEM-1024	5	1,568	1,568	18.8μs	23.3μs
Frodo	Frodo-1344	5	21,520	21,696	1.13ms	1.11ms

Source: PQShield <https://pqshield.github.io/nist-sigs-zoo/kems>

CLOSING

- FrodoKEM is a **conservatively-designed** quantum-safe lattice-based KEM.
- Its security relies on the hardness of standard LWE in **unstructured lattices**.
- The conservative design comes at a price: **increased bandwidth** and **slower speed**.
- FrodoKEM has been standardized by **ISO**, and is undergoing standardization by several organizations including the **IETF**.
- For details, see “**A Gentle Introduction to Lattice-Based Cryptography**”, <https://cryptography101.ca/latticecrypto>

