# Learning With Errors (LWE)

## an explanation for beginners

Stephen Cornelius, Liam Thomassen, and Divyesh Pandey

A presentation for *MATH540: Linear Algebra II*
University of Wisconsin–Madison
December 12, 2025

# Learning With Errors (LWE)

- Sample uniformly random matrix $A \in \mathbb{Z}_q^{m \times n}$
- Sample secret key $\mathbf{x} \in \mathbb{Z}_q^n$
- Sample small error vector $\mathbf{e} \in \mathbb{Z}_q^m$ from discrete Gaussian
- Compute $\mathbf{b} = A\mathbf{x} + \mathbf{e} \pmod{q}$
- LWE assumption: $(\mathbf{b}, A)$ is computationally indistinguishable from random

# One-Time Pad

- Message $m$ and random key $r$ in vector space $V$ over finite field
- Ciphertext: $c = m \oplus r$
- Decryption: $m = c \oplus r$ (since $r \oplus r = 0$)
- Information-theoretic security: unbreakable even with infinite computing power
- Used as baseline for security proofs

# Our Construction

- Replace random vector $r$ with $A\mathbf{x} + \mathbf{e}$
- Ciphertext: $\mathbf{c} = m \oplus (A\mathbf{x} + \mathbf{e})$
- Store message in most significant digits
- Receiver recovers $m$ by removing least significant digits (error)

# Security Proof

- Assume attacker can break our construction
- Alice randomly chooses: One-Time Pad or LWE construction
- Attacker cannot break One-Time Pad (information-theoretic security)
- Therefore, attacker must break LWE ciphertexts
- Attacker's success distinguishes $(A\mathbf{x} + \mathbf{e}, A)$ from $(r, A)$
- This breaks LWE assumption—contradiction!
- Conclusion: No such attacker exists

# References I