# Learning With Errors (LWE): 15-Minute Presentation Script

Stephen Cornelius, Liam Thomassen, and Divyesh Pandey

## Part 1: Learning With Errors (LWE) — [3.5 minutes]

Good morning. I'm , and I'll be introducing the Learning With Errors assumption, which is the mathematical foundation for our entire presentation.

Imagine Alice wants to create a secure encryption system. She starts by sampling a large random matrix $A$ from $\mathbb{Z}_q^{m \times n}$—think of this as an $m$ by $n$ grid where each entry is a number between 0 and $q-1$, chosen uniformly at random.

Next, Alice picks a secret key $\mathbf{x}$, which is a column vector of $n$ entries, also from $\mathbb{Z}_q$. This is what only she knows.

Here's the clever part: Alice samples a small error vector $\mathbf{e}$ of length $m$. This error is not uniformly random—instead, it's sampled from a discrete Gaussian distribution. This means most values cluster near zero, and the probability drops sharply as we move away from zero.

Now Alice computes $\mathbf{b} = A\mathbf{x} + \mathbf{e} \pmod{q}$. She sends $(\mathbf{b}, A)$ to everyone, including our attacker Charles.

The LWE assumption states something powerful: Charles cannot tell the difference between this vector $\mathbf{b}$ and a truly random vector $\mathbf{b}'$ sampled uniformly from $\mathbb{Z}_q^m$—even knowing $A$. That small error $\mathbf{e}$ is what makes everything look random.

If Charles could distinguish these, he would break LWE. But we believe LWE is hard to break, which is why it's so useful for cryptography.

## Part 2: One-Time Pad — [3.5 minutes]

Thank you, . I'm , and I'm going to show you something magical: a cipher that is mathematically proven unbreakable.

The one-time pad is simple. Suppose Alice has a message $m$—a vector in some vector space $V$ over a finite field. She also has a random key $r$ of the same length.

To encrypt, Alice computes $c = m \oplus r$, where $\oplus$ denotes XOR (or vector addition over the field). She sends both $c$ and the key $r$ to Bob.

Bob decrypts by computing $m = c \oplus r$. Since $r \oplus r = 0$, he recovers the original message.

Here's why it's unbreakable: from Charles's perspective, $c$ looks completely random because $r$ is random. Charles learns nothing about $m$, even with infinite computing power. This is called information-theoretic security.

The one-time pad is our gold standard. We'll use it as a reference point to prove our real construction is secure.

## Part 3: Our Construction — [4 minutes]

I'm , and I'll show you how we turn the one-time pad idea into something practical using LWE.

Our construction is almost identical to the one-time pad—with one key difference. Instead of using a truly random vector $r$, we replace it with $A\mathbf{x} + \mathbf{e}$.

So our ciphertext is:

$$\mathbf{c} = m \oplus (A\mathbf{x} + \mathbf{e})$$

But there's a catch: when Bob decrypts, he'll recover $m + \mathbf{e}$, not just $m$. The error gets added in.

So here's the trick: Alice stores the message $m$ in the most significant digits of the ciphertext. When Bob decrypts, he ignores the least significant digits—those are where the error lives. By throwing away the noise, Bob recovers the original message.

This construction is practical: we don't need a shared random vector $r$, just the matrix $A$ and the secret key $\mathbf{x}$.

## Part 4: Security Proof — [4 minutes]

Now for the punchline. Why is our construction secure?

Here's a proof by contradiction. Suppose there exists an attacker Charles who can break our construction.

Alice will now run a clever test. She flips a coin:

- Heads: She uses the magical one-time pad system.
- Tails: She uses our LWE-based construction.

She sends Charles either $(c = m \oplus r, A)$ or $(c = m \oplus (A\mathbf{x} + \mathbf{e}), A)$.

Now, Charles claims he can break ciphertexts. But if Alice is in one-time-pad mode, Charles cannot break it—information-theoretic security guarantees this. He has zero advantage.

Therefore, Charles must only break our construction. This means he can distinguish between: - $(A\mathbf{x} + \mathbf{e}, A)$ — our LWE construction - $(r, A)$ — random noise

If Charles has a way to tell them apart, he can distinguish $(A\mathbf{x} + \mathbf{e}, A)$ from random. But that's the definition of breaking the LWE assumption!

We've created a contradiction. No such attacker Charles can exist. Therefore, our construction is secure.

The security of our scheme reduces to the hardness of LWE—and LWE is believed to be hard. So our scheme is secure.

Thank you.