# Correction on LWE

# Small Vectors

### Definition

Assume $n \in \mathbb{N}$ and $p$ is a prime. Pick a random small $\vec{e} \in \mathbb{Z}_p^n$ means pick each component as a discrete Gaussian with mean 0 and variance to be specified.

# LWE-KE. Two Security Parameters $n, n'$

1. Alice: rand prime $p$ of length $n'$, rand $n \times n$ matrix $A$ over $\mathbb{Z}_p$.
2. Alice: rand $\vec{y} \in \mathbb{Z}_p^n$, small $\vec{e}_y \in \mathbb{Z}_p^n$. Sends $\vec{y}A + \vec{e}_y$.
3. Bob: rand $\vec{x} \in \mathbb{Z}_p^n$, small $\vec{e}_x \in \mathbb{Z}_p^n$. Sends $A\vec{x} + \vec{e}_x$.
4. Alice computes $a = \vec{y}(A\vec{x} + \vec{e}_x) = \vec{y}A\vec{x} + \vec{y} \cdot \vec{e}_x$.
5. Bob computes $b = (\vec{y}A + \vec{e}_y)\vec{x} = \vec{y}A\vec{x} + \vec{x} \cdot \vec{e}_y$.
6. They share $\vec{y}A\vec{x}$

# LWE-KE. Two Security Parameters $n, n'$

1. Alice: rand prime $p$ of length $n'$, rand $n \times n$ matrix $A$ over $\mathbb{Z}_p$.
2. Alice: rand $\vec{y} \in \mathbb{Z}_p^n$, small $\vec{e}_y \in \mathbb{Z}_p^n$. Sends $\vec{y}A + \vec{e}_y$.
3. Bob: rand $\vec{x} \in \mathbb{Z}_p^n$, small $\vec{e}_x \in \mathbb{Z}_p^n$. Sends $A\vec{x} + \vec{e}_x$.
4. Alice computes $a = \vec{y}(A\vec{x} + \vec{e}_x) = \vec{y}A\vec{x} + \vec{y} \cdot \vec{e}_x$.
5. Bob computes $b = (\vec{y}A + \vec{e}_y)\vec{x} = \vec{y}A\vec{x} + \vec{x} \cdot \vec{e}_y$.
6. They share $\vec{y}A\vec{x}$

Hey! That does not make sense! Neither one has $\vec{y}A\vec{x}$!

# LWE-KE

Alice has $a = \vec{y}(A\vec{x} + \vec{e}_x) = \vec{y}A\vec{x} + \vec{y} \cdot \vec{e}_x$.

Bob has $b = (\vec{y}A + \vec{e}_y)\vec{x} = yA\vec{x} + \vec{x} \cdot e_y$.

Since $\vec{e}_x, \vec{e}_y$ small, $a \sim b$.

# LWE-KE

Alice has $a = \vec{y}(A\vec{x} + \vec{e}_x) = \vec{y}A\vec{x} + \vec{y} \cdot \vec{e}_x$.

Bob has $b = (\vec{y}A + \vec{e}_y)\vec{x} = yA\vec{x} + \vec{x} \cdot e_y$.

Since $\vec{e}_x, \vec{e}_y$ small, $a \sim b$.

SO WHAT! $a \sim b$??? What does $\sim$ even mean over $\mathbb{Z}_p$? What kind of DELETED – WE ARE BEING TAPED is this? Discuss

# LWE-KE

Alice has $a = \vec{y}(A\vec{x} + \vec{e}_x) = \vec{y}A\vec{x} + \vec{y} \cdot \vec{e}_x$.

Bob has $b = (\vec{y}A + \vec{e}_y)\vec{x} = yA\vec{x} + \vec{x} \cdot e_y$.

Since $\vec{e}_x, \vec{e}_y$ small, $a \sim b$.

SO WHAT! $a \sim b$??? What does $\sim$ even mean over $\mathbb{Z}_p$? What kind of DELETED – WE ARE BEING TAPED is this? Discuss

CALM DOWN! If pick variance cleverly then with high prob either

$a, b \in \{0, 1, 2, \ldots, p/4\} \cup \{3p/4, \ldots, p-1\}$ ("close to 0"), OR

$a, b \in \{p/4 + 1, \ldots, 3p/4 - 1\}$ ("close to $p/2$")

(Paper with this on course website under notes.)

# LWE-KE. Two Security Parameters $n, n'$

1. Alice: rand prime $p$ of length $n'$, rand $n \times n$ matrix $A$ over $\mathbb{Z}_p$.
2. Alice: rand $\vec{y} \in \mathbb{Z}_p^n$, small $\vec{e}_y \in \mathbb{Z}_p^n$. Sends $\vec{y}A + \vec{e}_y$.
3. Bob: rand $\vec{x} \in \mathbb{Z}_p^n$, small $\vec{e}_x \in \mathbb{Z}_p^n$. Sends $A\vec{x} + \vec{e}_x$.
4. Alice computes $a = \vec{y}(A\vec{x} + \vec{e}_x) = \vec{y}A\vec{x} + \vec{y} \cdot \vec{e}_x$. If $a \in \{0, \ldots, p/4\} \cup \{3p/4, \ldots, p-1\}$, $s_A = 0$, else $s_A = 1$.
5. Bob computes $b = (\vec{y}A + \vec{e}_y)\vec{x} = \vec{y}A\vec{x} + \vec{x} \cdot \vec{e}_y$. If $b \in \{0, \ldots, p/4\} \cup \{3p/4, \ldots, p-1\}$, $s_B = 0$, else $s_B = 1$.
6. With high prob $s_A = s_B$. That is the bit they share.

PRO: Hardness Assumption NOT number-theoretic (see orig slides)
CON: Only 1 bit.
CON: As you know from hw06 THIS DID NOT WORK!!!!!!!!!

# LWE-KE. Two Security Parameters $n, n'$. MODIFIED

Why didn't it work? Because the error term was still too big.

- Alice has $\vec{y}A\vec{x} + \vec{y} \cdot \vec{e}_x$. ERROR$=$ $\vec{y} \cdot \vec{e}_x$.
- Bob has $\vec{y}A\vec{x} + \vec{x} \cdot \vec{e}_y$. ERROR- $\vec{x} \cdot \vec{e}_y$.

We need to make both of these ERROR's small
Idea! Make $\vec{y}$ and $\vec{x}$ small!

# LWE-KE. Two Security Parameters $n, n'$- OLD

1. Alice: rand prime $p$ of length $n'$, rand $n \times n$ matrix $A$ over $\mathbb{Z}_p$.
2. Alice: rand $\vec{y} \in \mathbb{Z}_p^n$, small $\vec{e}_y \in \mathbb{Z}_p^n$. Sends $\vec{y}A + \vec{e}_y$.
3. Bob: rand $\vec{x} \in \mathbb{Z}_p^n$, small $\vec{e}_x \in \mathbb{Z}_p^n$. Sends $A\vec{x} + \vec{e}_x$.
4. Alice computes $a = \vec{y}(A\vec{x} + \vec{e}_x) = \vec{y}A\vec{x} + \vec{y} \cdot \vec{e}_x$. If $a \in \{0, \ldots, p/4\} \cup \{3p/4, \ldots, p-1\}$, $s_A = 0$, else $s_A = 1$.
5. Bob computes $b = (\vec{y}A + \vec{e}_y)\vec{x} = \vec{y}A\vec{x} + \vec{x} \cdot \vec{e}_y$. If $b \in \{0, \ldots, p/4\} \cup \{3p/4, \ldots, p-1\}$, $s_B = 0$, else $s_B = 1$.
6. With high prob $s_A = s_B$. That is the bit they share.

PRO: Hardness Assumption NOT number-theoretic (see orig slides)
CON: Only 1 bit.
CON: As you know from hw06 THIS DID NOT WORK!!!!!!!!!

# LWE-KE. Two Security Parameters $n, n'$- NEW

1. Alice: rand prime $p$ of length $n'$, rand $n \times n$ matrix $A$ over $\mathbb{Z}_p$.
2. Alice: small $\vec{y} \in \mathbb{Z}_p^n$, small $\vec{e}_y \in \mathbb{Z}_p^n$. Sends $\vec{y}A + \vec{e}_y$.
3. Bob: small $\vec{x} \in \mathbb{Z}_p^n$, small $\vec{e}_x \in \mathbb{Z}_p^n$. Sends $A\vec{x} + \vec{e}_x$.
4. Alice computes $a = \vec{y}(A\vec{x} + \vec{e}_x) = \vec{y}A\vec{x} + \vec{y} \cdot \vec{e}_x$. If $a \in \{0, \ldots, p/4\} \cup \{3p/4, \ldots, p-1\}$, $s_A = 0$, else $s_A = 1$.
5. Bob computes $b = (\vec{y}A + \vec{e}_y)\vec{x} = \vec{y}A\vec{x} + \vec{x} \cdot \vec{e}_y$. If $b \in \{0, \ldots, p/4\} \cup \{3p/4, \ldots, p-1\}$, $s_B = 0$, else $s_B = 1$.
6. With high prob $s_A = s_B$. That is the bit they share.

PRO: Hardness Assumption NOT number-theoretic (see orig slides)
CON: Only 1 bit.
PRO: Nathan Coded it up and IT WORKS. Will be on next HW.

# LWE-KE. Practical Considerations

HW: version of LWE-KE where small means all comps in

$$\{0, 1, -1\} = \{0, 1, p-1\}$$

- $-1$ picked with prob $\frac{1}{n}$.
- $0$ picked with prob $\frac{n-2}{n}$.
- $1$ picked with prob $\frac{1}{n}$.

($n$ is dimension of matrix)

PRO: Easier to Code up then dealing with Gaussians
CON: No security proven. Not a known cipher. Its called:

LWG-KE

which stands for . . . can you guess?

# LWE-KE. Practical Considerations

HW: version of LWE-KE where small means all comps in

$$\{0, 1, -1\} = \{0, 1, p-1\}$$

- $-1$ picked with prob $\frac{1}{n}$.
- 0 picked with prob $\frac{n-2}{n}$.
- 1 picked with prob $\frac{1}{n}$.

($n$ is dimension of matrix)

PRO: Easier to Code up then dealing with Gaussians
CON: No security proven. Not a known cipher. Its called:

LWG-KE

which stands for ... can you guess?

Learning with Gasarch- Key Exchange