BILL, RECORD LECTURE!!!!

BILL RECORD LECTURE!!!

Reminder
Types of Attacks

Recall Types of Attacks

Ciphertext Only Attack (COA) Eve just gets to see ciphertext.

Recall Types of Attacks

Ciphertext Only Attack (COA) Eve just gets to see ciphertext.

Known Plaintext Attack (KPA) Eve just gets to see ciphertext and some old ciphertext-plaintext pairs.

Recall Types of Attacks

Ciphertext Only Attack (COA) Eve just gets to see ciphertext.

Known Plaintext Attack (KPA) Eve just gets to see ciphertext and some old ciphertext-plaintext pairs.

Brute Force Attack (BFA) Try every key.

Recall Types of Attacks

Ciphertext Only Attack (COA) Eve just gets to see ciphertext.

Known Plaintext Attack (KPA) Eve just gets to see ciphertext and some old ciphertext-plaintext pairs.

Brute Force Attack (BFA) Try every key.
Eve's goal is to find out something about the plaintext she did not already know.

Learning With Errors
Private Key

Solving a System of Equations over Mod

Quick, find a solution to

$$40k_1 + 28k_2 + 111k_3 + 7k_4 \equiv 19 \pmod{191}.$$

Solving a System of Equations over Mod

Quick, find a solution to

$$40k_1 + 28k_2 + 111k_3 + 7k_4 \equiv 19 \pmod{191}.$$

One answer is $k_1 = 170, k_2 = 39, k_3 = 3, k_4 = 1$:

Solving a System of Equations over Mod

Quick, find a solution to

$$40k_1 + 28k_2 + 111k_3 + 7k_4 \equiv 19 \pmod{191}.$$

One answer is $k_1 = 170, k_2 = 39, k_3 = 3, k_4 = 1$:

$$40 \times 170 + 28 \times 39 + 111 \times 3 + 7 \times 1 \equiv -40 \times 21 + 137 + 340$$

$$\equiv -840 + 137 + 149 \equiv -76 + 137 + 149 \equiv 19$$

Solving a System of Equations over Mod

Quick, find a solution to

$$40k_1 + 28k_2 + 111k_3 + 7k_4 \equiv 19 \pmod{191}.$$

One answer is $k_1 = 170, k_2 = 39, k_3 = 3, k_4 = 1$:

$$40 \times 170 + 28 \times 39 + 111 \times 3 + 7 \times 1 \equiv -40 \times 21 + 137 + 340$$

$$\equiv -840 + 137 + 149 \equiv -76 + 137 + 149 \equiv 19$$

How did I know $(170, 39, 3, 1)$ worked?

Solving a System of Equations over Mod

Quick, find a solution to

$$40k_1 + 28k_2 + 111k_3 + 7k_4 \equiv 19 \pmod{191}.$$

One answer is $k_1 = 170$, $k_2 = 39$, $k_3 = 3$, $k_4 = 1$:

$$40 \times 170 + 28 \times 39 + 111 \times 3 + 7 \times 1 \equiv -40 \times 21 + 137 + 340$$

$$\equiv -840 + 137 + 149 \equiv -76 + 137 + 149 \equiv 19$$

How did I know $(170, 39, 3, 1)$ worked? Am I a math genius?

Solving a System of Equations over Mod

Quick, find a solution to

$$40k_1 + 28k_2 + 111k_3 + 7k_4 \equiv 19 \pmod{191}.$$

One answer is $k_1 = 170, k_2 = 39, k_3 = 3, k_4 = 1$:

$$40 \times 170 + 28 \times 39 + 111 \times 3 + 7 \times 1 \equiv -40 \times 21 + 137 + 340$$

$$\equiv -840 + 137 + 149 \equiv -76 + 137 + 149 \equiv 19$$

How did I know $(170, 39, 3, 1)$ worked? Am I a math genius?
(Spoiler Alert: No)

I Trebekked It!

On the TV show JEOPARDY Alex Trebek gives you the **answer** and you have to figure out the **question**. Same here. Our domain is mod 191 throughout.

I Trebekked It!

On the TV show JEOPARDY Alex Trebek gives you the **answer** and you have to figure out the **question**. Same here. Our domain is mod 191 throughout.

1. I picked four random numbers: $170, 39, 3, 1$ to be **my answer.**

I Trebekked It!

On the TV show JEOPARDY Alex Trebek gives you the **answer** and you have to figure out the **question**. Same here. Our domain is mod 191 throughout.

1. I picked four random numbers: $170, 39, 3, 1$ to be **my answer.**
2. I picked four random numbers: $40, 28, 111, 7$ to be **coefficients.**

I Trebekked It!

On the TV show JEOPARDY Alex Trebek gives you the **answer** and you have to figure out the **question**. Same here. Our domain is mod 191 throughout.

1. I picked four random numbers: $170, 39, 3, 1$ to be **my answer.**
2. I picked four random numbers: $40, 28, 111, 7$ to be **coefficients.**
3. I calculated $170 \times 40 + 39 \times 28 + 3 \times 111 + 1 \times 7 \equiv 19$.

I Trebekked It!

On the TV show JEOPARDY Alex Trebek gives you the **answer** and you have to figure out the **question**. Same here. Our domain is mod 191 throughout.

1. I picked four random numbers: $170, 39, 3, 1$ to be **my answer.**
2. I picked four random numbers: $40, 28, 111, 7$ to be **coefficients.**
3. I calculated $170 \times 40 + 39 \times 28 + 3 \times 111 + 1 \times 7 \equiv 19$.
4. I know $40k_1 + 28k_2 + 111zk_3 + 7k_4 \equiv 19 \pmod{191}$ has answer $(170, 39, 3, 1)$.

About Alex Trekek. . .

Alex Trebek passed away recently.

About Alex Trekek. . .

Alex Trebek passed away recently.

I made up these slides before he passed away.

About Alex Trekek...

Alex Trebek passed away recently.

I made up these slides before he passed away.

While not-planned, the last slide can now be considered a tribute to him.

About Alex Trekek. . .

Alex Trebek passed away recently.

I made up these slides before he passed away.

While not-planned, the last slide can now be considered a tribute to him.

Here is another tribute to Trebek:
`https://www.youtube.com/watch?v=A7UgxCayfV0`

Important Definition: DOT Product

We redo our math and introduce a notation.

Important Definition: DOT Product

We redo our math and introduce a notation.

1. I picked four random numbers: $170, 39, 3, 1$ to be **my answer.**

Important Definition: DOT Product

We redo our math and introduce a notation.

1. I picked four random numbers: $170, 39, 3, 1$ to be **my answer.**
2. I picked four random numbers: $40, 28, 111, 7$ to be **coefficients.**

Important Definition: DOT Product

We redo our math and introduce a notation.

1. I picked four random numbers: $170, 39, 3, 1$ to be **my answer.**
2. I picked four random numbers: $40, 28, 111, 7$ to be **coefficients.**
3. I calculated $170 \times 40 + 39 \times 28 + 3 \times 111 + 1 \times 7 \equiv 19$.

Important Definition: DOT Product

We redo our math and introduce a notation.

1. I picked four random numbers: $170, 39, 3, 1$ to be **my answer.**
2. I picked four random numbers: $40, 28, 111, 7$ to be **coefficients.**
3. I calculated $170 \times 40 + 39 \times 28 + 3 \times 111 + 1 \times 7 \equiv 19$.
4. This is called the **Dot Product**

Important Definition: DOT Product

We redo our math and introduce a notation.

1. I picked four random numbers: $170, 39, 3, 1$ to be **my answer.**
2. I picked four random numbers: $40, 28, 111, 7$ to be **coefficients.**
3. I calculated $170 \times 40 + 39 \times 28 + 3 \times 111 + 1 \times 7 \equiv 19$.
4. This is called the **Dot Product**

Generally:

$$(k_1, \ldots, k_n) \cdot (r_1, \ldots, r_n) = k_1 \times r_1 + \cdots + k_n \times r_n.$$

We will always be doing this Mod p.

Example of an Idea for a Cipher

Example of an Idea for a Cipher

1. Alice and Bob: $(170, 39, 3, 1)$ is private key. Mod 191 is public.

Example of an Idea for a Cipher

1. Alice and Bob: $(170, 39, 3, 1)$ is private key. Mod 191 is public.
2. If Alice wants to send 0 she sends Bob an equation that $(170, 39, 3, 1)$ DOES solve. She can generate such an equation as I did above.

Example of an Idea for a Cipher

1. Alice and Bob: $(170, 39, 3, 1)$ is private key. Mod 191 is public.
2. If Alice wants to send 0 she sends Bob an equation that $(170, 39, 3, 1)$ DOES solve. She can generate such an equation as I did above.
3. If Alice wants to send 1 she sends Bob an equation that $(170, 39, 3, 1)$ DOES NOT solve. She can generate such an equation by doing what I did above and add 1.

Example of an Idea for a Cipher

1. Alice and Bob: $(170, 39, 3, 1)$ is private key. Mod 191 is public.
2. If Alice wants to send 0 she sends Bob an equation that $(170, 39, 3, 1)$ DOES solve. She can generate such an equation as I did above.
3. If Alice wants to send 1 she sends Bob an equation that $(170, 39, 3, 1)$ DOES NOT solve. She can generate such an equation by doing what I did above and add 1.

- Would use a bigger mod and a longer equation in real life.

Example of an Idea for a Cipher

1. Alice and Bob: $(170, 39, 3, 1)$ is private key. Mod 191 is public.
2. If Alice wants to send 0 she sends Bob an equation that $(170, 39, 3, 1)$ DOES solve. She can generate such an equation as I did above.
3. If Alice wants to send 1 she sends Bob an equation that $(170, 39, 3, 1)$ DOES NOT solve. She can generate such an equation by doing what I did above and add 1.

- Would use a bigger mod and a longer equation in real life.
- This cipher only allows transmitting one bit.

Example of Using This Cipher

Private Key $(170, 39, 3, 1)$. Both Alice and Bob have this.
Public Info 191, the mod. All math is mod 191.

Alice Wants to Send $b \in \{0, 1\}$.

Example of Using This Cipher

Private Key $(170, 39, 3, 1)$. Both Alice and Bob have this.
Public Info 191, the mod. All math is mod 191.

Alice Wants to Send $b \in \{0, 1\}$.

1. Alice picks random set of 4 elements: $(40, 28, 111, 7)$.

Example of Using This Cipher

Private Key $(170, 39, 3, 1)$. Both Alice and Bob have this.
Public Info 191, the mod. All math is mod 191.

Alice Wants to Send $b \in \{0, 1\}$.

1. Alice picks random set of 4 elements: $(40, 28, 111, 7)$.
2. Alice computes $(40, 28, 111, 7) \cdot (170, 39, 3, 1) \equiv 19$.

Example of Using This Cipher

Private Key $(170, 39, 3, 1)$. Both Alice and Bob have this.
Public Info 191, the mod. All math is mod 191.

Alice Wants to Send $b \in \{0, 1\}$.

1. Alice picks random set of 4 elements: $(40, 28, 111, 7)$.
2. Alice computes $(40, 28, 111, 7) \cdot (170, 39, 3, 1) \equiv 19$.
3. To send b Alice sends $(40, 28, 111, 7; 19 + b)$.

Example of Using This Cipher

Private Key $(170, 39, 3, 1)$. Both Alice and Bob have this.
Public Info 191, the mod. All math is mod 191.

Alice Wants to Send $b \in \{0, 1\}$.

1. Alice picks random set of 4 elements: $(40, 28, 111, 7)$.
2. Alice computes $(40, 28, 111, 7) \cdot (170, 39, 3, 1) \equiv 19$.
3. To send b Alice sends $(40, 28, 111, 7; 19 + b)$.
4. If Bob gets $(40, 28, 111, 7; 19)$ he will do $(40, 20, 111, 7) \cdot (170, 39, 3, 1) \equiv 19$, note $19 \equiv 19$ and know $b = 0$.

Example of Using This Cipher

Private Key $(170, 39, 3, 1)$. Both Alice and Bob have this.
Public Info 191, the mod. All math is mod 191.

Alice Wants to Send $b \in \{0, 1\}$.

1. Alice picks random set of 4 elements: $(40, 28, 111, 7)$.
2. Alice computes $(40, 28, 111, 7) \cdot (170, 39, 3, 1) \equiv 19$.
3. To send b Alice sends $(40, 28, 111, 7; 19 + b)$.
4. If Bob gets $(40, 28, 111, 7; 19)$ he will do $(40, 20, 111, 7) \cdot (170, 39, 3, 1) \equiv 19$, note $19 \equiv 19$ and know $b = 0$.

   If Bob gets $(40, 28, 111, 7; 20)$ he will do $(40, 20, 111, 7) \cdot (170, 39, 3, 1) \equiv 19$, note $19 \not\equiv 20$ and know $b = 1$.

Eve Can Crack This: Eve's View

Private Key (k_1, k_2, k_3, k_4). Both Alice and Bob have this.
Public Info 191, the mod. All math is mod 191. 191^4 poss for key.

Alice Wants to Send $b \in \{0, 1\}$.

Eve Can Crack This: Eve's View

Private Key (k_1, k_2, k_3, k_4). Both Alice and Bob have this.
Public Info 191, the mod. All math is mod 191. 191^4 poss for key.

Alice Wants to Send $b \in \{0, 1\}$.

1. Alice picks random set of 4 elements: $(40, 28, 111, 7)$.

Eve Can Crack This: Eve's View

Private Key (k_1, k_2, k_3, k_4). Both Alice and Bob have this.
Public Info 191, the mod. All math is mod 191. 191^4 poss for key.

Alice Wants to Send $b \in \{0, 1\}$.

1. Alice picks random set of 4 elements: $(40, 28, 111, 7)$.
2. Alice computes $(40, 28, 111, 7) \cdot (k_1, k_2, k_3, k_4) \equiv C$ (Eve does not see C)

Eve Can Crack This: Eve's View

Private Key (k_1, k_2, k_3, k_4). Both Alice and Bob have this.
Public Info 191, the mod. All math is mod 191. 191^4 poss for key.

Alice Wants to Send $b \in \{0, 1\}$.

1. Alice picks random set of 4 elements: $(40, 28, 111, 7)$.
2. Alice computes $(40, 28, 111, 7) \cdot (k_1, k_2, k_3, k_4) \equiv C$ (Eve does not see C)
3. To send b Alice sends $(40, 28, 111, 7; C + b)$. Eve sees $C + b$.

Eve Can Crack This: Eve's View

Private Key (k_1, k_2, k_3, k_4). Both Alice and Bob have this.
Public Info 191, the mod. All math is mod 191. 191^4 poss for key.

Alice Wants to Send $b \in \{0, 1\}$.

1. Alice picks random set of 4 elements: $(40, 28, 111, 7)$.
2. Alice computes $(40, 28, 111, 7) \cdot (k_1, k_2, k_3, k_4) \equiv C$ (Eve does not see C)
3. To send b Alice sends $(40, 28, 111, 7; C + b)$. Eve sees $C + b$.

KPA attack: Eve later finds out that $b = 0$, so $C \equiv 19$. Eve knows:

Eve Can Crack This: Eve's View

Private Key (k_1, k_2, k_3, k_4). Both Alice and Bob have this.
Public Info 191, the mod. All math is mod 191. 191^4 poss for key.

Alice Wants to Send $b \in \{0, 1\}$.

1. Alice picks random set of 4 elements: $(40, 28, 111, 7)$.
2. Alice computes $(40, 28, 111, 7) \cdot (k_1, k_2, k_3, k_4) \equiv C$ (Eve does not see C)
3. To send b Alice sends $(40, 28, 111, 7; C + b)$. Eve sees $C + b$.

KPA attack: Eve later finds out that $b = 0$, so $C \equiv 19$. Eve knows:

$$40k_1 + 28k_2 + 111k_3 + 7k_4 \equiv 19$$

Eve Can Crack This: Eve's View

Private Key (k_1, k_2, k_3, k_4). Both Alice and Bob have this.
Public Info 191, the mod. All math is mod 191. 191^4 poss for key.

Alice Wants to Send $b \in \{0, 1\}$.

1. Alice picks random set of 4 elements: $(40, 28, 111, 7)$.
2. Alice computes $(40, 28, 111, 7) \cdot (k_1, k_2, k_3, k_4) \equiv C$ (Eve does not see C)
3. To send b Alice sends $(40, 28, 111, 7; C + b)$. Eve sees $C + b$.

KPA attack: Eve later finds out that $b = 0$, so $C \equiv 19$. Eve knows:

$$40k_1 + 28k_2 + 111k_3 + 7k_4 \equiv 19$$

Number of possibilities for key is now 191^3. If sees more messages can cut down search space to one possibility.

How to Fix This? Recall the Protocol

Protocol made a sharp distinction between:

- Key **is** solution.
- Key **is not** solution.

How to Fix This? Recall the Protocol

Protocol made a sharp distinction between:

- Key **is** solution.
- Key **is not** solution.

That is too sharp. Instead we will do distinction between:

- Key **is close to** to a solution.
- Key **is far from** a solution.

Notation We Will Need

$e \in^r A$ means that e is picked unif at random from the set A.

Notation We Will Need

$e \in^r A$ means that e is picked unif at random from the set A.

We will pick our error uniformily.

Notation We Will Need

$e \in^r A$ means that e is picked unif at random from the set A.

We will pick our error uniformily.

When LWE is really used they pick the error with a Gaussian around 0.

Notation We Will Need

$e \in^r A$ means that e is picked unif at random from the set A.

We will pick our error uniformily.

When LWE is really used they pick the error with a Gaussian around 0.

We are doing it in a way that is INCORRECT but BETTER FOR EDUCATION.

Example of Better Cipher

Private Key $(170, 39, 3, 1)$. **Public Info** mod 191.

Example of Better Cipher

Private Key $(170, 39, 3, 1)$. **Public Info** mod 191.

1. Alice picks random set of 4 elements: $(40, 28, 111, 7)$.

Example of Better Cipher

Private Key $(170, 39, 3, 1)$. **Public Info** mod 191.

1. Alice picks random set of 4 elements: $(40, 28, 111, 7)$.
2. Alice computes $(40, 28, 111, 7) \cdot (170, 39, 3, 1) \equiv 19$.

Example of Better Cipher

Private Key $(170, 39, 3, 1)$. **Public Info** mod 191.

1. Alice picks random set of 4 elements: $(40, 28, 111, 7)$.
2. Alice computes $(40, 28, 111, 7) \cdot (170, 39, 3, 1) \equiv 19$.
3. Bit b: A sends $(40, 28, 111, 7; 19 + e + 50b)$. $e \in^r \{-1, 0, 1\}$.

Example of Better Cipher

Private Key $(170, 39, 3, 1)$. **Public Info** mod 191.

1. Alice picks random set of 4 elements: $(40, 28, 111, 7)$.
2. Alice computes $(40, 28, 111, 7) \cdot (170, 39, 3, 1) \equiv 19$.
3. Bit b: A sends $(40, 28, 111, 7; 19 + e + 50b)$. $e \in^r \{-1, 0, 1\}$.
4. If Bob gets $(40, 28, 111, 7; 19 + e)$ he will do $(40, 20, 111, 7) \cdot (170, 39, 3, 1) \equiv 19 \sim 19 + e$, so bit is 0.

Example of Better Cipher

Private Key $(170, 39, 3, 1)$. **Public Info** mod 191.

1. Alice picks random set of 4 elements: $(40, 28, 111, 7)$.
2. Alice computes $(40, 28, 111, 7) \cdot (170, 39, 3, 1) \equiv 19$.
3. Bit b: A sends $(40, 28, 111, 7; 19 + e + 50b)$. $e \in^r \{-1, 0, 1\}$.
4. If Bob gets $(40, 28, 111, 7; 19 + e)$ he will do $(40, 20, 111, 7) \cdot (170, 39, 3, 1) \equiv 19 \sim 19 + e$, so bit is 0.

   If Bob gets $(40, 28, 111, 7; 19 + e + 50)$ he will do $(40, 20, 111, 7) \cdot (170, 39, 3, 1) \equiv 19 \not\sim 19 + e + 50$ so bit is 1.

Example of Better Cipher

Private Key $(170, 39, 3, 1)$. **Public Info** mod 191.

1. Alice picks random set of 4 elements: $(40, 28, 111, 7)$.
2. Alice computes $(40, 28, 111, 7) \cdot (170, 39, 3, 1) \equiv 19$.
3. Bit b: A sends $(40, 28, 111, 7; 19 + e + 50b)$. $e \in^r \{-1, 0, 1\}$.
4. If Bob gets $(40, 28, 111, 7; 19 + e)$ he will do $(40, 20, 111, 7) \cdot (170, 39, 3, 1) \equiv 19 \sim 19 + e$, so bit is 0.

   If Bob gets $(40, 28, 111, 7; 19 + e + 50)$ he will do $(40, 20, 111, 7) \cdot (170, 39, 3, 1) \equiv 19 \not\sim 19 + e + 50$ so bit is 1.

- $e \in \{-1, 0, 1\}$. Note that $-1 \equiv 190$.

Example of Better Cipher

Private Key $(170, 39, 3, 1)$. **Public Info** mod 191.

1. Alice picks random set of 4 elements: $(40, 28, 111, 7)$.
2. Alice computes $(40, 28, 111, 7) \cdot (170, 39, 3, 1) \equiv 19$.
3. Bit b: A sends $(40, 28, 111, 7; 19 + e + 50b)$. $e \in^r \{-1, 0, 1\}$.
4. If Bob gets $(40, 28, 111, 7; 19 + e)$ he will do $(40, 20, 111, 7) \cdot (170, 39, 3, 1) \equiv 19 \sim 19 + e$, so bit is 0.
   If Bob gets $(40, 28, 111, 7; 19 + e + 50)$ he will do $(40, 20, 111, 7) \cdot (170, 39, 3, 1) \equiv 19 \not\sim 19 + e + 50$ so bit is 1.

- $e \in \{-1, 0, 1\}$. Note that $-1 \equiv 190$.
- $e \in \{-1, 0, 1\}$. In real system $e \in \{-\gamma, \ldots, \gamma\}$, γ a param.

Example of Better Cipher

Private Key $(170, 39, 3, 1)$. **Public Info** mod 191.

1. Alice picks random set of 4 elements: $(40, 28, 111, 7)$.
2. Alice computes $(40, 28, 111, 7) \cdot (170, 39, 3, 1) \equiv 19$.
3. Bit b: A sends $(40, 28, 111, 7; 19 + e + 50b)$. $e \in^r \{-1, 0, 1\}$.
4. If Bob gets $(40, 28, 111, 7; 19 + e)$ he will do $(40, 20, 111, 7) \cdot (170, 39, 3, 1) \equiv 19 \sim 19 + e$, so bit is 0.

   If Bob gets $(40, 28, 111, 7; 19 + e + 50)$ he will do $(40, 20, 111, 7) \cdot (170, 39, 3, 1) \equiv 19 \not\sim 19 + e + 50$ so bit is 1.

- $e \in \{-1, 0, 1\}$. Note that $-1 \equiv 190$.
- $e \in \{-1, 0, 1\}$. In real system $e \in \{-\gamma, \ldots, \gamma\}$, γ a param.
- We picked 50 as our big number. In real system use $\sim \frac{p}{4}$.

Floor Ceiling Convention; Vector Notation

When we write something like $\frac{p}{4}$ where p is odd we really mean

$$\left\lfloor \frac{p}{4} \right\rfloor$$

Floor Ceiling Convention; Vector Notation

When we write something like $\frac{p}{4}$ where p is odd we really mean

$$\left\lfloor \frac{p}{4} \right\rfloor$$

In our concrete examples we had things like

$$\text{The Key is } (1, 2, 3, 40)$$

Floor Ceiling Convention; Vector Notation

When we write something like $\frac{p}{4}$ where p is odd we really mean

$$\left\lfloor \frac{p}{4} \right\rfloor$$

In our concrete examples we had things like

$$\text{The Key is } (1, 2, 3, 40)$$

We will now use $\vec{k}$ for the key of length n

Floor Ceiling Convention; Vector Notation

When we write something like $\frac{p}{4}$ where p is odd we really mean

$$\left\lfloor \frac{p}{4} \right\rfloor$$

In our concrete examples we had things like

$$\text{The Key is } (1, 2, 3, 40)$$

We will now use $\vec{k}$ for the key of length n

We will now use $\vec{r}$ for a random vector of length n.

Private Key LWE Cipher

Private Key $\vec{k}$. Both Alice and Bob have this.
Public Info p, γ. p is prime. All math is mod p.

Private Key LWE Cipher

Private Key $\vec{k}$. Both Alice and Bob have this.
Public Info p, γ. p is prime. All math is mod p.

Alice Wants to Send $b \in \{0, 1\}$.

Private Key LWE Cipher

Private Key $\vec{k}$. Both Alice and Bob have this.
Public Info p, γ. p is prime. All math is mod p.

Alice Wants to Send $b \in \{0, 1\}$.

1. Alice picks random vector $\vec{r}$.

Private Key LWE Cipher

Private Key $\vec{k}$. Both Alice and Bob have this.
Public Info p, γ. p is prime. All math is mod p.

Alice Wants to Send $b \in \{0, 1\}$.

1. Alice picks random vector $\vec{r}$.
2. Alice computes $\vec{r} \cdot \vec{k} \equiv C$ and $e \in^r \{-\gamma, \ldots, \gamma\}$.

Private Key LWE Cipher

Private Key $\vec{k}$. Both Alice and Bob have this.
Public Info p, γ. p is prime. All math is mod p.

Alice Wants to Send $b \in \{0, 1\}$.

1. Alice picks random vector $\vec{r}$.
2. Alice computes $\vec{r} \cdot \vec{k} \equiv C$ and $e \in^r \{-\gamma, \ldots, \gamma\}$.
3. To send b Alice sends $(\vec{r}; D)$ where $D \equiv C + e + \frac{bp}{4}$.

Private Key LWE Cipher

Private Key $\vec{k}$. Both Alice and Bob have this.
Public Info p, γ. p is prime. All math is mod p.

Alice Wants to Send $b \in \{0, 1\}$.

1. Alice picks random vector $\vec{r}$.
2. Alice computes $\vec{r} \cdot \vec{k} \equiv C$ and $e \in^r \{-\gamma, \ldots, \gamma\}$.
3. To send b Alice sends $(\vec{r}; D)$ where $D \equiv C + e + \frac{bp}{4}$.
4. Bob computes $\vec{r} \cdot \vec{k} \equiv C$. If $D \sim C$, $b = 0$, else $b = 1$.

Private Key LWE Cipher

Private Key $\vec{k}$. Both Alice and Bob have this.
Public Info p, γ. p is prime. All math is mod p.

Alice Wants to Send $b \in \{0, 1\}$.

1. Alice picks random vector $\vec{r}$.
2. Alice computes $\vec{r} \cdot \vec{k} \equiv C$ and $e \in^r \{-\gamma, \ldots, \gamma\}$.
3. To send b Alice sends $(\vec{r}; D)$ where $D \equiv C + e + \frac{bp}{4}$.
4. Bob computes $\vec{r} \cdot \vec{k} \equiv C$. If $D \sim C$, $b = 0$, else $b = 1$.

Is this a good cipher? Easy to use? Secure? Discuss.

Private Key LWE Cipher: Pick γ so Works

Private Key LWE Cipher: Pick γ so Works

- If $b = 0$ then Bob compares C to $C + e$.
  Diff: $e \in \{-\gamma, \ldots, \gamma\}$.

Private Key LWE Cipher: Pick γ so Works

- If $b = 0$ then Bob compares C to $C + e$.
  Diff: $e \in \{-\gamma, \ldots, \gamma\}$.
- If $b = 1$ then Bob compares C to $C + e + \frac{p}{4}$.
  Diff: $e + \frac{p}{4} \in \{-\gamma + \frac{p}{4}, \ldots, \gamma + \frac{p}{4}\}$.

Private Key LWE Cipher: Pick γ so Works

- If $b = 0$ then Bob compares C to $C + e$.
  Diff: $e \in \{-\gamma, \ldots, \gamma\}$.
- If $b = 1$ then Bob compares C to $C + e + \frac{p}{4}$.
  Diff: $e + \frac{p}{4} \in \{-\gamma + \frac{p}{4}, \ldots, \gamma + \frac{p}{4}\}$.

Need these intervals are disjoint.

Private Key LWE Cipher: Pick γ so Works

- If $b = 0$ then Bob compares C to $C + e$.
  Diff: $e \in \{-\gamma, \ldots, \gamma\}$.
- If $b = 1$ then Bob compares C to $C + e + \frac{p}{4}$.
  Diff: $e + \frac{p}{4} \in \{-\gamma + \frac{p}{4}, \ldots, \gamma + \frac{p}{4}\}$.

Need these intervals are disjoint. Two intervals mod p are disjoint iff when you shift them they are disjoint. We want to shift them to avoid wrap around.

Private Key LWE Cipher: Pick γ so Works

- If $b = 0$ then Bob compares C to $C + e$.
  Diff: $e \in \{-\gamma, \ldots, \gamma\}$.
- If $b = 1$ then Bob compares C to $C + e + \frac{p}{4}$.
  Diff: $e + \frac{p}{4} \in \{-\gamma + \frac{p}{4}, \ldots, \gamma + \frac{p}{4}\}$.

Need these intervals are disjoint. Two intervals mod p are disjoint iff when you shift them they are disjoint. We want to shift them to avoid wrap around.

Shift both by γ. Need
$\{0, \ldots, 2\gamma\}$ and $\{\frac{p}{4}, \ldots, 2\gamma + \frac{p}{4}\}$ disjoint.

Private Key LWE Cipher: Pick γ so Works

- If $b = 0$ then Bob compares C to $C + e$.
  Diff: $e \in \{-\gamma, \ldots, \gamma\}$.
- If $b = 1$ then Bob compares C to $C + e + \frac{p}{4}$.
  Diff: $e + \frac{p}{4} \in \{-\gamma + \frac{p}{4}, \ldots, \gamma + \frac{p}{4}\}$.

Need these intervals are disjoint. Two intervals mod p are disjoint iff when you shift them they are disjoint. We want to shift them to avoid wrap around.

Shift both by γ. Need
$\{0, \ldots, 2\gamma\}$ and $\{\frac{p}{4}, \ldots, 2\gamma + \frac{p}{4}\}$ disjoint.
So need $2\gamma < \frac{p}{4}$ and $2\gamma + \frac{p}{4} < p$. $\gamma < \frac{p}{16}$ suffices. (Actually $\frac{p}{8}$ suffices, but we will use $\frac{p}{16}$.)

Private Key LWE Cipher: Pick γ so Works

- If $b = 0$ then Bob compares C to $C + e$.
  Diff: $e \in \{-\gamma, \ldots, \gamma\}$.
- If $b = 1$ then Bob compares C to $C + e + \frac{p}{4}$.
  Diff: $e + \frac{p}{4} \in \{-\gamma + \frac{p}{4}, \ldots, \gamma + \frac{p}{4}\}$.

Need these intervals are disjoint. Two intervals mod p are disjoint iff when you shift them they are disjoint. We want to shift them to avoid wrap around.
Shift both by γ. Need
$\{0, \ldots, 2\gamma\}$ and $\{\frac{p}{4}, \ldots, 2\gamma + \frac{p}{4}\}$ disjoint.
So need $2\gamma < \frac{p}{4}$ and $2\gamma + \frac{p}{4} < p$. $\gamma < \frac{p}{16}$ suffices. (Actually $\frac{p}{8}$ suffices, but we will use $\frac{p}{16}$.)

- $b = 0$: Bob sees that diff is in $\{-\frac{p}{16}, \ldots, \frac{p}{16}\}$
  $= \{0, \ldots, \frac{p}{16}\} \cup \{\frac{15p}{16}, \ldots, p - 1\}$.

Private Key LWE Cipher: Pick γ so Works

- If $b = 0$ then Bob compares C to $C + e$.
  Diff: $e \in \{-\gamma, \ldots, \gamma\}$.
- If $b = 1$ then Bob compares C to $C + e + \frac{p}{4}$.
  Diff: $e + \frac{p}{4} \in \{-\gamma + \frac{p}{4}, \ldots, \gamma + \frac{p}{4}\}$.

Need these intervals are disjoint. Two intervals mod p are disjoint iff when you shift them they are disjoint. We want to shift them to avoid wrap around.
Shift both by γ. Need
$\{0, \ldots, 2\gamma\}$ and $\{\frac{p}{4}, \ldots, 2\gamma + \frac{p}{4}\}$ disjoint.
So need $2\gamma < \frac{p}{4}$ and $2\gamma + \frac{p}{4} < p$. $\gamma < \frac{p}{16}$ suffices. (Actually $\frac{p}{8}$ suffices, but we will use $\frac{p}{16}$.)

- $b = 0$: Bob sees that diff is in $\{-\frac{p}{16}, \ldots, \frac{p}{16}\}$
  $= \{0, \ldots, \frac{p}{16}\} \cup \{\frac{15p}{16}, \ldots, p - 1\}$.
- $b = 1$: Bob sees that diff is in $\{\frac{3p}{16}, \ldots, \frac{5p}{16}\}$.

Why did I use a Prime?

Recall the protocol:
Private Key $\vec{k}$. Both Alice and Bob have this.
Public Info p, γ, n. p is prime. All math is mod p.
Alice Wants to Send $b \in \{0, 1\}$.

Why did I use a Prime?

Recall the protocol:

Private Key $\vec{k}$. Both Alice and Bob have this.

Public Info p, γ, n. p is prime. All math is mod p.

Alice Wants to Send $b \in \{0,1\}$.

1. Alice picks random vector $\vec{r}$.

Why did I use a Prime?

Recall the protocol:
Private Key $\vec{k}$. Both Alice and Bob have this.
Public Info p, γ, n. p is prime. All math is mod p.
Alice Wants to Send $b \in \{0, 1\}$.

1. Alice picks random vector $\vec{r}$.
2. Alice computes $\vec{r} \cdot \vec{k} \equiv C$ and $e \in^r \{-\gamma, \ldots, \gamma\}$.

Why did I use a Prime?

Recall the protocol:
Private Key $\vec{k}$. Both Alice and Bob have this.
Public Info p, γ, n. p is prime. All math is mod p.
Alice Wants to Send $b \in \{0,1\}$.

1. Alice picks random vector $\vec{r}$.
2. Alice computes $\vec{r} \cdot \vec{k} \equiv C$ and $e \in^r \{-\gamma, \ldots, \gamma\}$.
3. To send b Alice sends $(\vec{r}; D)$ where $D \equiv C + e + \frac{bp}{4}$.

Why did I use a Prime?

Recall the protocol:
Private Key $\vec{k}$. Both Alice and Bob have this.
Public Info p, γ, n. p is prime. All math is mod p.
Alice Wants to Send $b \in \{0,1\}$.

1. Alice picks random vector $\vec{r}$.
2. Alice computes $\vec{r} \cdot \vec{k} \equiv C$ and $e \in^r \{-\gamma, \ldots, \gamma\}$.
3. To send b Alice sends $(\vec{r}; D)$ where $D \equiv C + e + \frac{bp}{4}$.
4. Bob computes $\vec{r} \cdot \vec{k} \equiv C$. If $D \sim C$, $b = 0$, else $b = 1$.

Why did I use a Prime?

Recall the protocol:
Private Key $\vec{k}$. Both Alice and Bob have this.
Public Info p, γ, n. p is prime. All math is mod p.
Alice Wants to Send $b \in \{0, 1\}$.

1. Alice picks random vector $\vec{r}$.
2. Alice computes $\vec{r} \cdot \vec{k} \equiv C$ and $e \in^r \{-\gamma, \ldots, \gamma\}$.
3. To send b Alice sends $(\vec{r}; D)$ where $D \equiv C + e + \frac{bp}{4}$.
4. Bob computes $\vec{r} \cdot \vec{k} \equiv C$. If $D \sim C$, $b = 0$, else $b = 1$.

Why did I use that p is prime?

Why did I use a Prime?

Recall the protocol:
Private Key $\vec{k}$. Both Alice and Bob have this.
Public Info p, γ, n. p is prime. All math is mod p.
Alice Wants to Send $b \in \{0,1\}$.

1. Alice picks random vector $\vec{r}$.
2. Alice computes $\vec{r} \cdot \vec{k} \equiv C$ and $e \in^r \{-\gamma, \ldots, \gamma\}$.
3. To send b Alice sends $(\vec{r}; D)$ where $D \equiv C + e + \frac{bp}{4}$.
4. Bob computes $\vec{r} \cdot \vec{k} \equiv C$. If $D \sim C$, $b = 0$, else $b = 1$.

Why did I use that p is prime?
I didn't!

Why did I use a Prime?

Recall the protocol:
Private Key $\vec{k}$. Both Alice and Bob have this.
Public Info p, γ, n. p is prime. All math is mod p.
Alice Wants to Send $b \in \{0, 1\}$.

1. Alice picks random vector $\vec{r}$.
2. Alice computes $\vec{r} \cdot \vec{k} \equiv C$ and $e \in^r \{-\gamma, \ldots, \gamma\}$.
3. To send b Alice sends $(\vec{r}; D)$ where $D \equiv C + e + \frac{bp}{4}$.
4. Bob computes $\vec{r} \cdot \vec{k} \equiv C$. If $D \sim C$, $b = 0$, else $b = 1$.

Why did I use that p is prime?
I didn't!
The proof that its secure uses that p is prime. The HW need not use p is prime.

Private Key LWE Cipher: Security

What problem does Eve need to solve to find the key?

Private Key LWE Cipher: Security

What problem does Eve need to solve to find the key?

Learning With Errors Problem (LWE) Eve is given p, γ and told there is a key $\vec{k}$ that she wants to find.

Private Key LWE Cipher: Security

What problem does Eve need to solve to find the key?

Learning With Errors Problem (LWE) Eve is given p, γ and told there is a key $\vec{k}$ that she wants to find.

Eve is given a set of tuples $(\vec{r}, D)$ and told that

$$\vec{r} \cdot \vec{k} - D \equiv e \in^r \{-\gamma, \ldots, \gamma\}.$$

(Eve is not told e, just that $e \in^r \{-\gamma, \ldots, \gamma\}$.)

Private Key LWE Cipher: Security

What problem does Eve need to solve to find the key?

Learning With Errors Problem (LWE) Eve is given p, γ and told there is a key $\vec{k}$ that she wants to find.

Eve is given a set of tuples $(\vec{r}, D)$ and told that

$$\vec{r} \cdot \vec{k} - D \equiv e \in^r \{-\gamma, \ldots, \gamma\}.$$

(Eve is not told e, just that $e \in^r \{-\gamma, \ldots, \gamma\}$.)

From these **noisy equations** she wants to learn $\vec{k}$.
Hard? This is thought to be a hard problem.

Private Key LWE Cipher: Security

What problem does Eve need to solve to find the key?

Learning With Errors Problem (LWE) Eve is given p, γ and told there is a key $\vec{k}$ that she wants to find.

Eve is given a set of tuples $(\vec{r}, D)$ and told that

$$\vec{r} \cdot \vec{k} - D \equiv e \in^r \{-\gamma, \ldots, \gamma\}.$$

(Eve is not told e, just that $e \in^r \{-\gamma, \ldots, \gamma\}$.)

From these **noisy equations** she wants to learn $\vec{k}$.
Hard? This is thought to be a hard problem.
(We will go into **why** LWE is thought to be hard when we do LWE-public, which won't be for a while.)

Theorem About Security

Informal Theorem If Eve can crack LWE-private cipher then Eve can solve the LWE-problem. Note that this is the direction you want.

Theorem About Security

Informal Theorem If Eve can crack LWE-private cipher then Eve can solve the LWE-problem. Note that this is the direction you want.
Proof We won't prove this, but we note that it requires some work.

Theorem About Security

Informal Theorem If Eve can crack LWE-private cipher then Eve can solve the LWE-problem. Note that this is the direction you want.

Proof We won't prove this, but we note that it requires some work.

1. Since LWE-problem is thought to be hard, the LWE-private cipher is thought to be hard-to-crack.

Theorem About Security

Informal Theorem If Eve can crack LWE-private cipher then Eve can solve the LWE-problem. Note that this is the direction you want.
Proof We won't prove this, but we note that it requires some work.

1. Since LWE-problem is thought to be hard, the LWE-private cipher is thought to be hard-to-crack.
2. So why is this cipher not used? Discuss.

Theorem About Security

Informal Theorem If Eve can crack LWE-private cipher then Eve can solve the LWE-problem. Note that this is the direction you want.
Proof We won't prove this, but we note that it requires some work.

1. Since LWE-problem is thought to be hard, the LWE-private cipher is thought to be hard-to-crack.
2. So why is this cipher not used? Discuss.
   Only one bit.

Theorem About Security

Informal Theorem If Eve can crack LWE-private cipher then Eve can solve the LWE-problem. Note that this is the direction you want.

Proof We won't prove this, but we note that it requires some work.

1. Since LWE-problem is thought to be hard, the LWE-private cipher is thought to be hard-to-crack.
2. So why is this cipher not used? Discuss.
   Only one bit.
   For private-key crypto, better schemes are known.

Theorem About Security: Very Nice PRO

Theorem (informal) The worst-case of LWE is the same as the Avg-case.

Theorem About Security: Very Nice PRO

Theorem (informal) The worst-case of LWE is the same as the Avg-case.
Proof We won't prove this, but we note that it requires some work.

Theorem About Security: Very Nice PRO

Theorem (informal) The worst-case of LWE is the same as the Avg-case.
Proof We won't prove this, but we note that it requires some work.

1. A problem that plagues complexity theory is that a problem can have a bad worst-case but a reasonable average-case.

Theorem About Security: Very Nice PRO

Theorem (informal) The worst-case of LWE is the same as the Avg-case.
Proof We won't prove this, but we note that it requires some work.

1. A problem that plagues complexity theory is that a problem can have a bad worst-case but a reasonable average-case.
2. For LWE this is NOT an issue.

Theorem About Security: Very Nice PRO

Theorem (informal) The worst-case of LWE is the same as the Avg-case.
Proof We won't prove this, but we note that it requires some work.

1. A problem that plagues complexity theory is that a problem can have a bad worst-case but a reasonable average-case.
2. For LWE this is NOT an issue.
3. Hence the assumption that LWE is hard for worst case already gives you hard for avg case.

BILL, STOP RECORDING LECTURE!!!!

BILL STOP RECORDING LECTURE!!!