BILL, RECORD LECTURE!!!!

BILL RECORD LECTURE!!!

Public Key LWE Cipher

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.

Noisy Equations

Everything is mod p, some prime p.

Noisy Equations

Everything is mod p, some prime p.

Let $\vec{k} = (k_1, \ldots, k_n)$, $\vec{r} = (r_1, \ldots, r_n)$, and C be such that

$$r_1 k_1 + \cdots + r_n k_n = C$$

Noisy Equations

Everything is mod p, some prime p.

Let $\vec{k} = (k_1, \ldots, k_n)$, $\vec{r} = (r_1, \ldots, r_n)$, and C be such that

$$r_1 k_1 + \cdots + r_n k_n = C$$

$r_1 x_1 + \cdots + r_n x_n = C$ is an **equation** that $\vec{k}$ satisfies.

Noisy Equations

Everything is mod p, some prime p.

Let $\vec{k} = (k_1, \ldots, k_n)$, $\vec{r} = (r_1, \ldots, r_n)$, and C be such that

$$r_1 k_1 + \cdots + r_n k_n = C$$

$r_1 x_1 + \cdots + r_n x_n = C$ is an **equation** that $\vec{k}$ satisfies.

Pick $e \in^r \{-\gamma, \ldots, \gamma\}$. Think of γ as small.

$r_1 x_1 + \cdots + r_n x_n \sim C + e$ is **noisy eq** that $\vec{k}$ satisfies.

Noisy Equations

Everything is mod p, some prime p.

Let $\vec{k} = (k_1, \ldots, k_n)$, $\vec{r} = (r_1, \ldots, r_n)$, and C be such that

$$r_1 k_1 + \cdots + r_n k_n = C$$

$r_1 x_1 + \cdots + r_n x_n = C$ is an **equation** that $\vec{k}$ satisfies.

Pick $e \in^r \{-\gamma, \ldots, \gamma\}$. Think of γ as small.

$r_1 x_1 + \cdots + r_n x_n \sim C + e$ is **noisy eq** that $\vec{k}$ satisfies.

Say $\vec{k}$ satisfies the noisy equations

$$r_1 x_1 + \cdots + r_n x_n \sim C_1 + e_1$$

$$s_1 x_1 + \cdots + s_n x_n \sim C_2 + e_2$$

Then $\vec{k}$ satisfy the sum:

$$(r_1 + s_1) x_1 + \cdots + (r_k + s_k) x_k \sim C_1 + C_2 + e_1 + e_2$$

Example of Setting Up The LWE-Public Cipher

Public Info Prime: 191. Length of Vector: 4. Error: $\{-1, 0, 1\}$.

Example of Setting Up The LWE-Public Cipher

Public Info Prime: 191. Length of Vector: 4. Error: $\{-1, 0, 1\}$.

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

Example of Setting Up The LWE-Public Cipher

Public Info Prime: 191. Length of Vector: 4. Error: $\{-1, 0, 1\}$.

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

1. She picks rand: $(1, 10, 21, 89)$.

Example of Setting Up The LWE-Public Cipher

Public Info Prime: 191. Length of Vector: 4. Error: $\{-1, 0, 1\}$.

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

1. She picks rand: $(1, 10, 21, 89)$. She picks 4 rand $\vec{r}$.
   $(4, 9, 1, 89)$, $(9, 98, 8, 1)$, $(44, 55, 10, 8)$, $(9, 3, 11, 99)$.

Example of Setting Up The LWE-Public Cipher

Public Info Prime: 191. Length of Vector: 4. Error: $\{-1, 0, 1\}$.

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

1. She picks rand: $(1, 10, 21, 89)$. She picks 4 rand $\vec{r}$.
   $(4, 9, 1, 89)$, $(9, 98, 8, 1)$, $(44, 55, 10, 8)$, $(9, 3, 11, 99)$.
   She picks 4 random $e \in \{-1, 0, 1\}$: 1,-1,0,1.

Example of Setting Up The LWE-Public Cipher

Public Info Prime: 191. Length of Vector: 4. Error: $\{-1, 0, 1\}$.

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

1. She picks rand: $(1, 10, 21, 89)$. She picks 4 rand $\vec{r}$.
   $(4, 9, 1, 89)$, $(9, 98, 8, 1)$, $(44, 55, 10, 8)$, $(9, 3, 11, 99)$.
   She picks 4 random $e \in \{-1, 0, 1\}$: 1,-1,0,1.
   She forms 4 noisy eqs which have $(1, 10, 21, 89)$ as "answer."

Example of Setting Up The LWE-Public Cipher

Public Info Prime: 191. Length of Vector: 4. Error: $\{-1, 0, 1\}$.

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

1. She picks rand: $(1, 10, 21, 89)$. She picks 4 rand $\vec{r}$.
   $(4, 9, 1, 89)$, $(9, 98, 8, 1)$, $(44, 55, 10, 8)$, $(9, 3, 11, 99)$.
   She picks 4 random $e \in \{-1, 0, 1\}$: 1,-1,0,1.
   She forms 4 noisy eqs which have $(1, 10, 21, 89)$ as "answer."

$$4k_1 + 9k_2 + 21k_3 + 89k_4 \equiv 84$$

$$9k_1 + 98k_2 + 8k_3 + k_4 \equiv 99$$

$$44k_1 + 558k_2 + 10k_3 + 8k_4 \equiv 179$$

$$9k_1 + 3k_2 + 11k_3 + 99k_4 \equiv 105$$

Example of Setting Up The LWE-Public Cipher

Public Info Prime: 191. Length of Vector: 4. Error: $\{-1, 0, 1\}$.

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

1. She picks rand: $(1, 10, 21, 89)$. She picks 4 rand $\vec{r}$.
   $(4, 9, 1, 89)$, $(9, 98, 8, 1)$, $(44, 55, 10, 8)$, $(9, 3, 11, 99)$.
   She picks 4 random $e \in \{-1, 0, 1\}$: 1,-1,0,1.
   She forms 4 noisy eqs which have $(1, 10, 21, 89)$ as "answer."

$$4k_1 + 9k_2 + 21k_3 + 89k_4 \equiv 84$$

$$9k_1 + 98k_2 + 8k_3 + k_4 \equiv 99$$

$$44k_1 + 558k_2 + 10k_3 + 8k_4 \equiv 179$$

$$9k_1 + 3k_2 + 11k_3 + 99k_4 \equiv 105$$

These equations are published.

Example of Setting Up The LWE-Public Cipher

Public Info Prime: 191. Length of Vector: 4. Error: $\{-1, 0, 1\}$.

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

1. She picks rand: $(1, 10, 21, 89)$. She picks 4 rand $\vec{r}$.
   $(4, 9, 1, 89)$, $(9, 98, 8, 1)$, $(44, 55, 10, 8)$, $(9, 3, 11, 99)$.
   She picks 4 random $e \in \{-1, 0, 1\}$: 1,-1,0,1.
   She forms 4 noisy eqs which have $(1, 10, 21, 89)$ as "answer."

$$4k_1 + 9k_2 + 21k_3 + 89k_4 \equiv 84$$

$$9k_1 + 98k_2 + 8k_3 + k_4 \equiv 99$$

$$44k_1 + 558k_2 + 10k_3 + 8k_4 \equiv 179$$

$$9k_1 + 3k_2 + 11k_3 + 99k_4 \equiv 105$$

   These equations are published.
   Note Any sum of the eqs also has $(1, 10, 21, 89)$ as "answer."

Bob Wants to Send a Bit

Bob wants to send bit 0.

Bob Wants to Send a Bit

Bob wants to send bit 0.

Pick two of the equations, add them, and sends publicly:

Bob Wants to Send a Bit

Bob wants to send bit 0.
Pick two of the equations, add them, and sends publicly:

$$13k_1 + 12k_2 + 32k_3 + 188k_4 \equiv 189$$

Bob Wants to Send a Bit

Bob wants to send bit 0.
Pick two of the equations, add them, and sends publicly:

$$13k_1 + 12k_2 + 32k_3 + 188k_4 \equiv 189$$

Eve She sees this equation but does not know which equations were added to form this one.

Bob Wants to Send a Bit

Bob wants to send bit 0.
Pick two of the equations, add them, and sends publicly:

$$13k_1 + 12k_2 + 32k_3 + 188k_4 \equiv 189$$

Eve She sees this equation but does not know which equations were added to form this one.
Alice She finds that $(1, 10, 21, 99)$ is **close to** solution, so $b = 0$.

Bob Wants to Send a Bit

Bob wants to send bit 0.
Pick two of the equations, add them, and sends publicly:

$$13k_1 + 12k_2 + 32k_3 + 188k_4 \equiv 189$$

Eve She sees this equation but does not know which equations were added to form this one.
Alice She finds that $(1, 10, 21, 99)$ is **close to** solution, so $b = 0$.

Bob want to send bit 1.

Bob Wants to Send a Bit

Bob wants to send bit 0.
Pick two of the equations, add them, and sends publicly:

$$13k_1 + 12k_2 + 32k_3 + 188k_4 \equiv 189$$

Eve She sees this equation but does not know which equations were added to form this one.
Alice She finds that $(1, 10, 21, 99)$ is **close to** solution, so $b = 0$.

Bob want to send bit 1.
Pick two of the equations, add them, add 50, and sends publicly:

$$13k_1 + 12k_2 + 32k_3 + 188k_4 \equiv 49$$

Bob Wants to Send a Bit

Bob wants to send bit 0.
Pick two of the equations, add them, and sends publicly:

$$13k_1 + 12k_2 + 32k_3 + 188k_4 \equiv 189$$

Eve She sees this equation but does not know which equations were added to form this one.
Alice She finds that $(1, 10, 21, 99)$ is **close to** solution, so $b = 0$.

Bob want to send bit 1.
Pick two of the equations, add them, add 50, and sends publicly:

$$13k_1 + 12k_2 + 32k_3 + 188k_4 \equiv 49$$

Eve She sees this equation but does not know which equations were added to form this one.

Bob Wants to Send a Bit

Bob wants to send bit 0.
Pick two of the equations, add them, and sends publicly:

$$13k_1 + 12k_2 + 32k_3 + 188k_4 \equiv 189$$

Eve She sees this equation but does not know which equations were added to form this one.
Alice She finds that $(1, 10, 21, 99)$ is **close to** solution, so $b = 0$.

Bob want to send bit 1.
Pick two of the equations, add them, add 50, and sends publicly:

$$13k_1 + 12k_2 + 32k_3 + 188k_4 \equiv 49$$

Eve She sees this equation but does not know which equations were added to form this one.
Alice She finds that $(1, 10, 21, 99)$ is **far from** solution, so $b = 1$.

LWE-Public: Security

Theorem If Eve can crack the LWE-public cipher then Eve can solve the LWE-problem. Note that this is the direction you want. (LWE equivalent to GAP-SVP which is thought to be hard.)

Theorem Worst Case is equivalent to Average Case.

BILL, STOP RECORDING LECTURE!!!!

BILL STOP RECORDING LECTURE!!!