TODAY:

* Learning With Errors (LWE)
* (Cryptographic) Pseudorandomness
* Private-Key Encryption
* Public-Key Encryption

NOTE

SIS problem: Given $A_{n \times m}$, b find s s.t. $As = b$ ("short")

on $A_{n \times m}$, $s_{m \times 1}$, $b_{n \times 1}$ ("short")

(n = # equations)

- When $m \gg n \log q / \log B$ (Total SIS), many solutions exist

(m = # variables, # columns)

- When $m \ll n \log q / \log B$, no ("short") solutions exist (unless you plant one)

LWE ≡ Planted SIS

(m vs $m-n$)

A b

Pick A. Then pick "short" s. Then set $b = As$

Hardness of solving systems of linear equations (modulo a prime)

$$14s_1 + 15s_2 + 5s_3 + 2s_4 = 8 \pmod{17}$$

$$13s_1 + 14s_2 + 14s_3 + 6s_4 = 16 \pmod{17}$$

$$6s_1 + 10s_2 + 13s_3 + 15s_4 = 3 \pmod{17}$$

$$8s_1 + 7s_2 + 16s_3 + 25s_4 = 2 \pmod{17}$$

$s_1, \ldots, s_{10} \in \{0 \ldots q-1\}$

$e_1, \ldots \in$ "short" $\in \{-1, 0, 1\}$

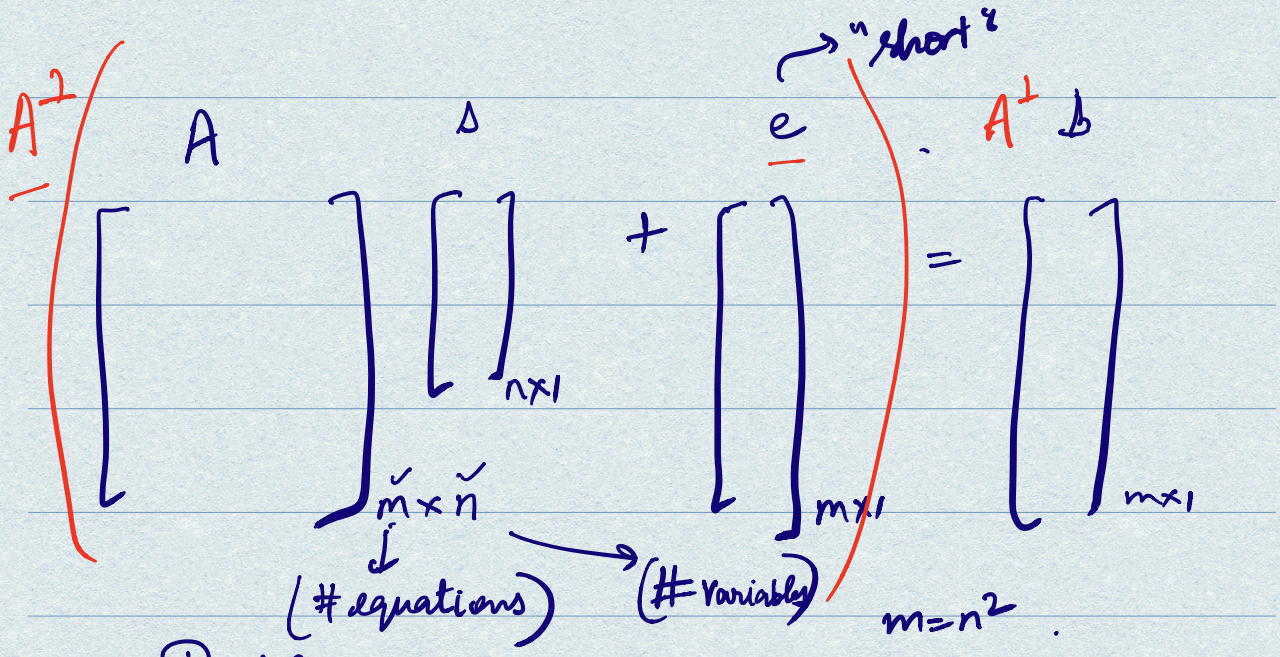
$$14s_1 + 15s_2 + 5s_3 + 2s_4 + e_1 = 8 \pmod{17}$$

$$13s_1 + 14s_2 + \ldots\ldots + e_2 = 16 \pmod{17}$$

$$6s_1 + 10s_2 + \qquad\quad + e_3 = 3 \pmod{17}$$

$$8s_1 + 7s_2 + \ldots\ldots + e_4 = 2 \pmod{17}$$

$$A s + e = b$$



$m = n^2$.

Problem: Given A, b

find s.

$n^2 \sim n^2 - n$

$m \sim m - n \gg n$

$m \approx n^2$

$n \log q \sim n$

For any matrix A, one can find the "kernel" of A

This is a full-rank set of vectors $A^{\perp}$ s.t. $A^{\perp}_{(m-n)\times m} A_{m\times n} = 0_{(m-n)\times n}$

To reduce LWE to SIS,

Given A, b, compute $c = A^{\perp} b = A^{\perp} e$

(A, b) LWE

↳ $(\underline{A}^{\perp}, \underline{c})_{SIS}$ is an SIS instance whose solution is e.

$$A^{\perp}_{\underline{(m-n)} \times (m)}$$

ξ_n

$$\left[\quad\right]_{\underline{(m-n)} \times m}$$

$(m-n)$ → rows, m → dims

$(m-n)$ equations in m variables

LWE

"Search" LWE $_{n,m,q,\chi}$

$\forall$ nu PPT $\mathcal{A}$,

$$\Pr_{\substack{A \leftarrow \mathbb{Z}_q^{m \times n} \\ s \leftarrow \mathbb{Z}_q^{n \times 1} \\ e \leftarrow \chi^m}} \left[\mathcal{A}(A, As+e) \rightarrow s \right] = \text{negl}(n)$$

"Decision" LWE $_{n,m,q,\chi}$

$\forall$ nu PPT $\mathcal{A}$,

$$\left| \Pr_{\substack{A \leftarrow \mathbb{Z}_q^{m \times n} \\ s \leftarrow \mathbb{Z}_q^{n \times 1} \\ e \leftarrow \chi^m}} \left[\mathcal{A}(A, As+e) = 1 \right] - \Pr_{\substack{A \leftarrow \mathbb{Z}_q^{m} \\ b \leftarrow \mathbb{Z}_q^{n}}} \left[\mathcal{A}(A, b) = 1 \right] \right| = \text{negl}(n)$$

Claim

If "Total" SIS is easy, then LWE is also easy

A m-n x m = Planted SIS.

$m = n^2$

Given $A_{m \times n}$, $b_{m \times 1}$ is either A, uniform or $A, As+e$

Suppose I can find "short" $\tilde{s}$ such that $A^T \tilde{s} = 0$ if SIS is easy

$$b^T = s^T A^T + e^T$$

multiply b^T with $\tilde{s}$

$$b^T \tilde{s} = s^T A^T \tilde{s} + e^T \tilde{s}$$

$$= 0 + e^T \tilde{s}$$

$\Rightarrow$ If A, b was an LWE sample, $b^T \tilde{s}$ would be "short".

o/w $b^T \tilde{s}$ would not.

LWE is "stronger assumption" than SIS.

SIS ≡ "Total" SIS

LWE ≡ "Planted" SIS.

If SIS assumption is false,

then LWE assumption is false.

Quantumly, if LWE assumption is false,

then SIS assumption is false.

(Not known under classical reductions)

PSEUDORANDOMNESS

"unpredictability".

$f : \{0,1\}^* \to \{0,1\}^*$ is a OWF.

Sample $x \xleftarrow{\$} \{0,1\}^k$

Q: Is the following true?

$\forall$ nu PPT $\mathcal{A}$

$$\Pr_{x \xleftarrow{\$} \{0,1\}^k}\left[\mathcal{A}(f(x)) \text{ outputs the first bit of } x\right] = \frac{1}{2} + \text{negl}(k)$$

A: This is false

Given f, construct g s.t. $g(x) = x_1 \| f(x)$

g is still one-way!

H.W.: Use any Adv that inverts g, to invert f.

Hard Core Predicate

A H.C.P. of an injective OWF $f : \{0,1\}^* \to \{0,1\}^*$ is a boolean predicate $B : \{0,1\}^* \to \{0,1\}$ such that

- $\forall x$, $B(x)$ is easy to compute
- $\forall$ nu PPT $\mathcal{A}$, $\forall c \in \mathbb{N}$, $\exists k_0$ s.t. $\forall k > k_0$,

$$\Pr_{x \leftarrow \{0,1\}^k}\left[\mathcal{A}(1^k, f(x)) = B(x)\right] = \frac{1}{2} + \text{negl}(k)$$

pseudorandomness :

"small" "true" randomness

↓ EXPAND

"large" "pseudo" random

Computational Indistinguishability

Def. Two distribution ensembles $X = \{X_k\}_{k \in \mathbb{N}}$ and $Y = \{Y_k\}_{k \in \mathbb{N}}$ are comp. indistinguishable if

$\forall$ nu PPT $\mathcal{D}$,

$$\left| \Pr_{x \leftarrow X_k}[\mathcal{D}(x) = 1] - \Pr_{y \leftarrow Y_k}[\mathcal{D}(y) = 1] \right| = \text{negl}(k)$$

$$X \underset{\text{comp. ind.}}{\approx_c} Y$$

$$\{f(x), B(x)\}_{x \leftarrow \{0,1\}^k} \approx \{f(x), B(x)+1\}_{x \leftarrow \{0,1\}^k}$$

$$\approx \{f(x), \text{uniform}\}$$

if B is a H.C.P.,

$$\{f(x), \underbrace{B(x)}_{0}\} \approx \{f(x), \underbrace{B(x)+1}_{1}\}.$$

$X = 01 \ldots 01$

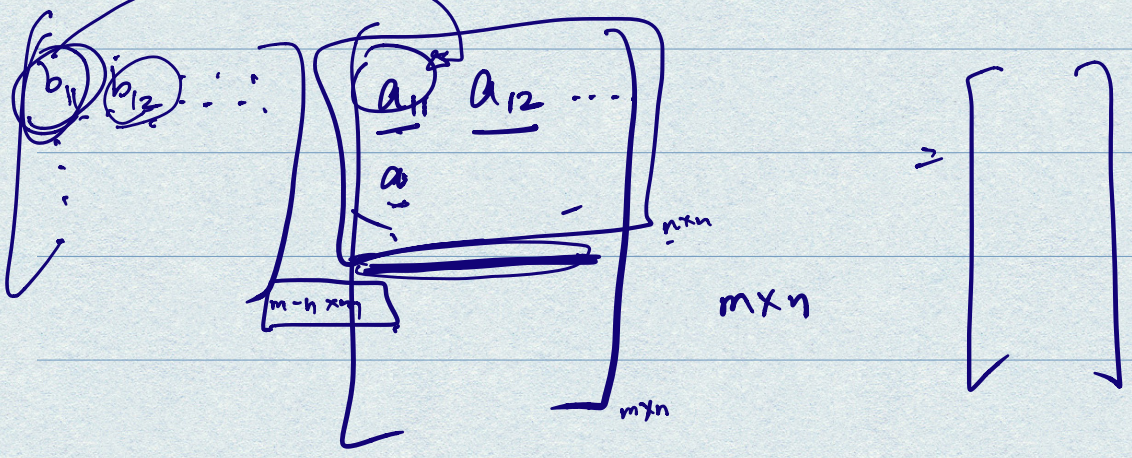
$B(x) = 0$

If f is inj., then the 2 dist. have disjoint support.

$$A^t \cdot (A^\perp)^t = 0.$$

$m \times n$

$$A^\perp A = 0_{m-n \times n}$$



$(m-n) \cdot n$ equations in $(m-n)m$ variables

$$b_{11}\, a_{11} + b_{12}\, a_{21} \ldots\ldots + \ldots = 0$$

$$b_{21}\, a_{12} + b_{22}\, a_{22} \ldots = \pm\ . \quad = 0$$

$$\vdots$$

$$b_{m-n\,1}$$

rows in A = # rows in $A^\perp$

+ rank of A

Alt.

columns in A^t = # columns in $(A^\perp)^t$ + rank of A.