LECTURE 9

* LATTICE TRAPDOORS
* APPLICATIONS TO DIGITAL SIGNATURES

FROM LAST CLASS.

"BOOTSTRAPPING".

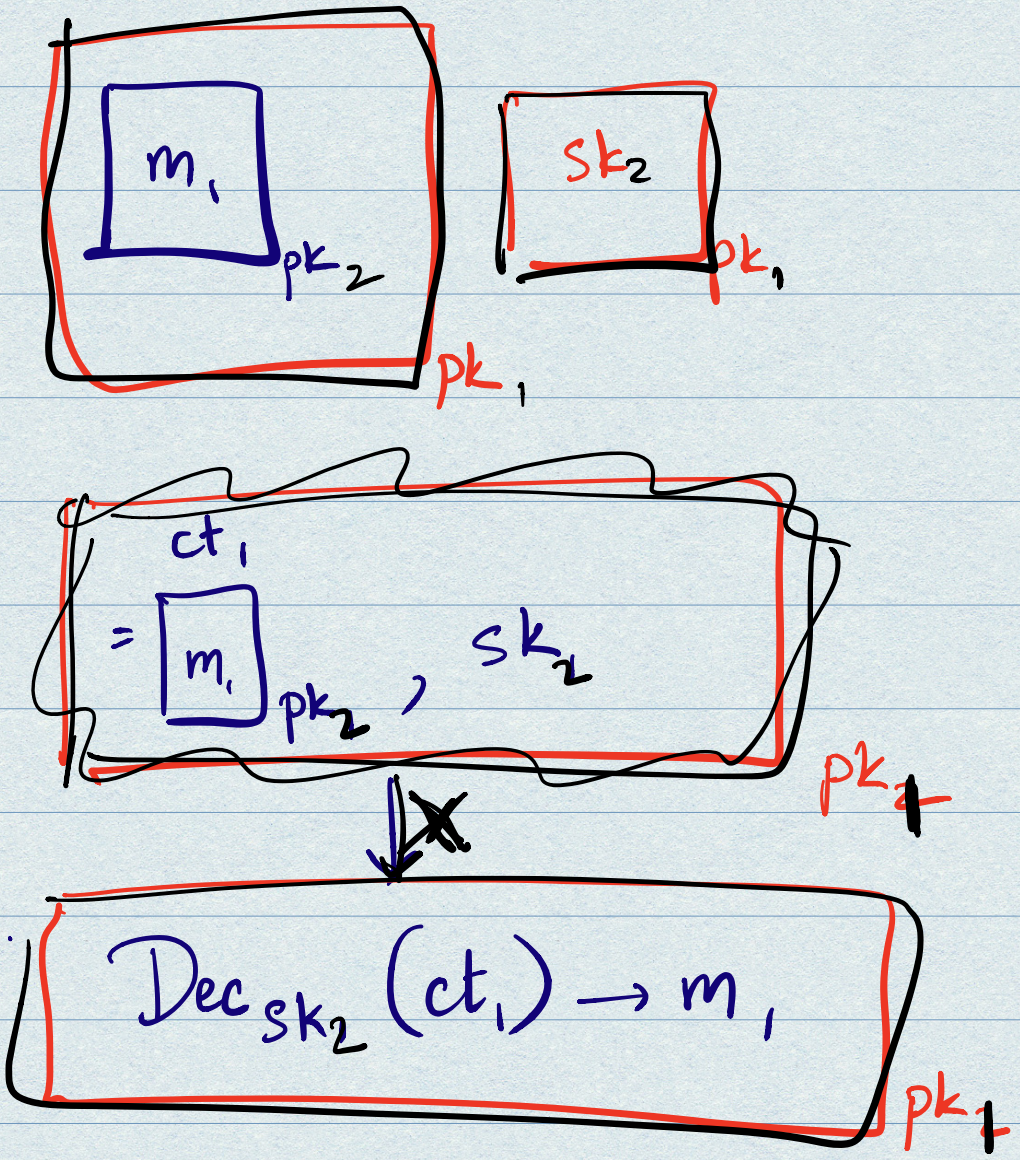
Q: $(pk_1, sk_1) \leftarrow KeyGen_{scheme1}$ (NOT HOMOMORPHIC)

$(pk_2, sk_2) \leftarrow KeyGen_{scheme\ 2}$ (HOMOMORPHIC)

Given $pk_1, pk_2, enc_{pk_2}(m_1), enc_{pk_1}(sk_2)$

can you obtain $enc_{pk_1}(m_1)$?

Ans: NO.


m_1
pk_2
pk_1
sk_2
pk_1
ct_1
$= m_1$
pk_2
,
sk_2
pk_1
$Dec_{sk_2}(ct_1) \rightarrow m_1$
pk_1

TRAPDOOR FUNCTIONS.

A trapdoor function family

$f_{ik} : \{0,1\}^n \to \{0,1\}^m$

consists of the following algorithms:

1) $\text{KeyGen}(1^n) \to (ik, td)$

2) $f_{ik}(x) \to y$ (efficiently)

3) $f^{-1}(td, y) \to x$

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

$$\Pr_{\substack{(ik,td) \leftarrow \text{KeyGen} \\ x \leftarrow \{0,1\}^n}}\left[\mathcal{A}(f(ik,x)) \in f^{-1}(f(ik,x))\right] = \text{negl}(n)$$

LWE gives a one-way function

$f_A(\vec{s}, e) = As + e$

How about a trapdoor one-way function?

Sample A with trapdoor T

s.t.

given (b^T, T) $\xrightarrow{\text{efficiently}}$ (s, e).

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

$(1 \times m)$ $\quad$ $(1 \times m)$ $\quad$ $n \times m$

$b^T T$? (1 x m vector $[c_1\ c_2 \ldots c_m]$)

$= (s^T A + e^T) T = e^T T$

LATTICE TRAPDOORS

For matrix $A_{n \times m}$ $\begin{bmatrix} & \\ & \end{bmatrix}$

define $\Lambda^{\perp}(A)$

$= \{ z \in \mathbb{Z}^m \text{ s.t. } Az = 0 \pmod q \}$

restrict this set to "short" z.

A lattice trapdoor for A is a "short basis" of $\Lambda^{\perp}(A)$.

Def. A matrix $T \in \mathbb{Z}^{n \times m}$ is a "good" trapdoor for $A \in \mathbb{Z}_q^{n \times m}$ if

(1) Every column of T, t_i is s.t. $At_i = 0 \pmod q$

(2) $\|t_i\|_\infty \leq B$

(3) T has rank m over $\mathbb{Z}$.

Note: Rank(T) in $\mathbb{Z}_q$ cannot be $> m-n$, but Rank(T) over $\mathbb{Z}$ can be m.

Given T, solve LWE as follows:

→ given b^T. compute $c^T = b^T T$

now we know $e^T T = c^T$

solve for e. (not modulo q but in $\mathbb{Z}$!)

How do we sample $(A, \boxed{T})$?

Simplified: Sample $(\overset{\text{uniform}}{\downarrow}{A}, t)$ s.t

① t is "short" and

② $At = 0 \pmod q$.

1) $A' \leftarrow \mathbb{Z}_q^{n \times (m-1)}$

2) $t' \leftarrow \{0,1\}^{m-1}$ $\quad (m-1) > 2n \log q$

3) $A = [A' \,||\, -A't']$

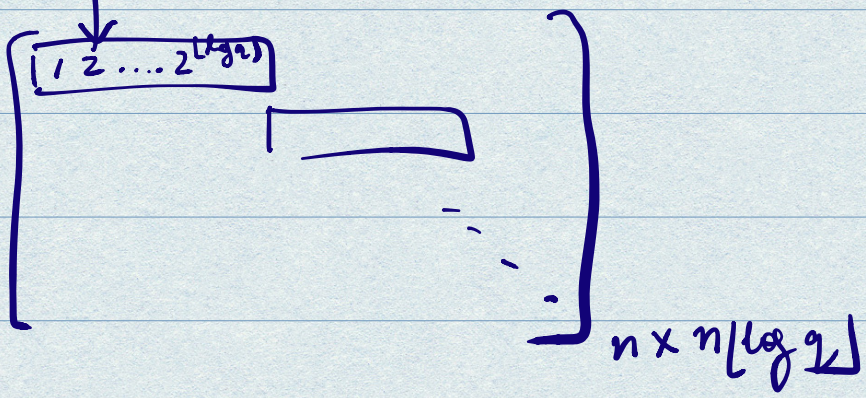
$t = \begin{pmatrix} t' \\ 1 \end{pmatrix}$

Why is A (close to) uniform over $\mathbb{Z}_q^{n \times m}$?

"Trapdoors of type-2"

T s.t. T has "short columns" and

$$A_{n \times m} \; T_{m \times n\lceil \log q \rceil} = G \pmod q$$



Type-2 trapdoor suffices to solve LWE!

$$b^T T = (s^T A + e^T) T = s^T G + e^T T$$

$e^T T$: short error

T_G s.t. $G T_G = 0$

↳ Type-1 td for G.

$b^T T T_G = e^T T T_G$.

Solve for e!

Type 1 trapdoor for G.

$$g = [1 \quad 2 \quad 4 \quad \ldots \quad 2^{\lfloor \log q \rfloor}]$$

Define T_g s.t. $g \cdot T_g = 0$.

$$T_g \in \mathbb{Z}^{\lfloor \log q \rfloor \times \lfloor \log q \rfloor}$$

$$[1 \quad 2 \quad 4 \quad \ldots \quad 2^{\lfloor \log q \rfloor}] \begin{bmatrix} 2 & 0 & & 0 \\ -1 & 2 & & \\ 0 & -1 & \ddots & \\ \vdots & & & -2 \\ 0 & & & -1 \end{bmatrix} \leftarrow T_g$$

$$= [0 \quad \ldots \quad 0 \quad 0]$$

$$G = \begin{bmatrix} & & \\ & & \\ & & \end{bmatrix} = I \otimes g$$

$$T_G = I \otimes T_g$$

Type-2 trapdoors for A

$B \leftarrow \mathbb{Z}_q^{n \times m'}$ where $\left(m' = n \log q + k\right)$

$A = \left[B \,\|\, BR + G \right]$ → By LHL, this is stat. close to uniform

$n \times m^*$; $\{0,1\}^{m^* \times n \log q}$; $(n \times n \log q)$

$$A \begin{bmatrix} -R \\ I \end{bmatrix} = \left[B \,\|\, BR+G \right] \begin{bmatrix} -R \\ I \end{bmatrix}$$

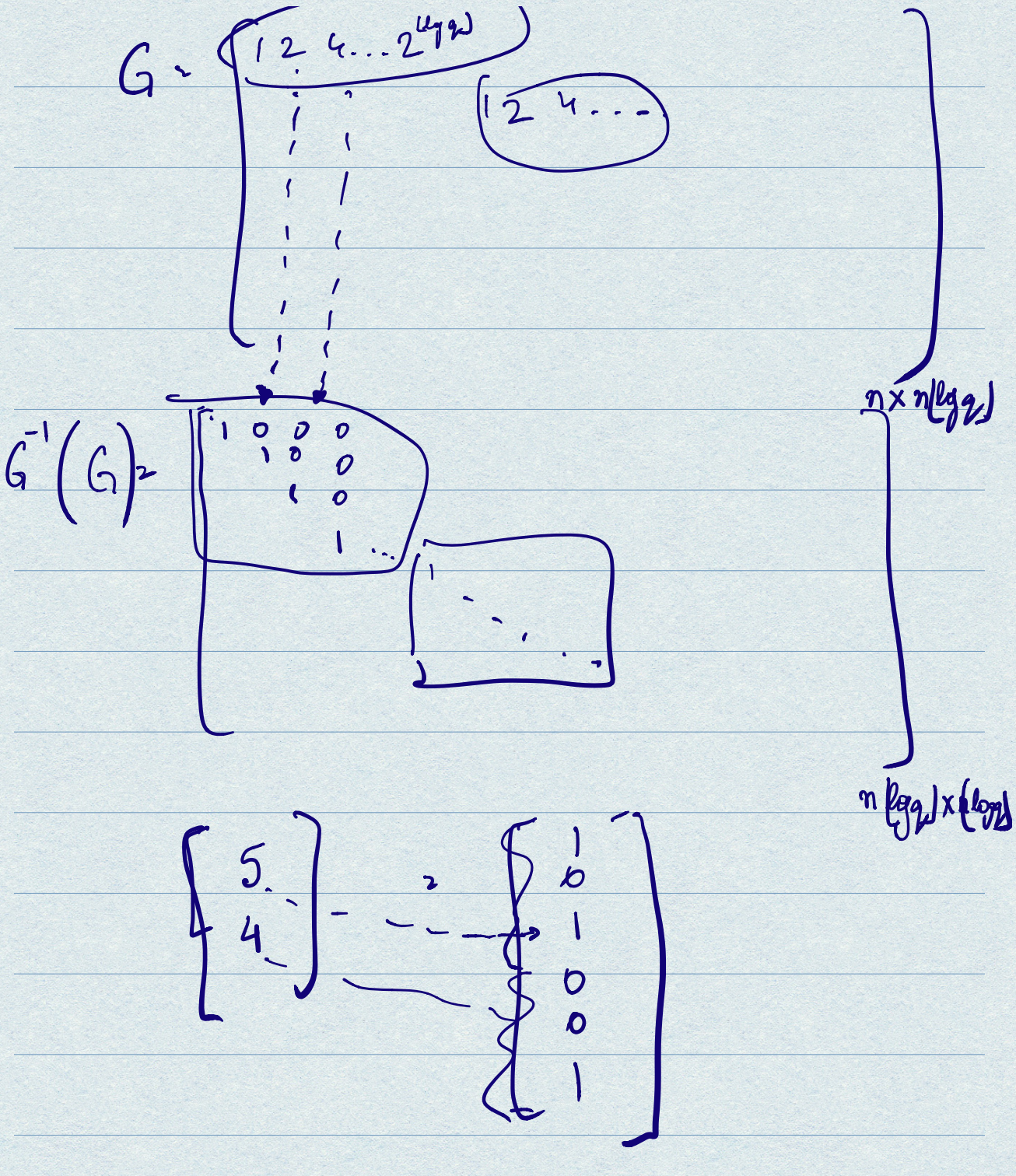
$\left(m' + n \log q\right) \times n \log q$

$$= -BR + BR + G$$

$$= G.$$

Sample $A = \left[B \,\|\, BR+G \right]$

type-1 $T_A = \begin{bmatrix} I + RG^{-1}(B) & -RT_G \\ -G^{-1}(B) & T_G \end{bmatrix}$


G =
1 2 4 ... $2^{(\lfloor \log q \rfloor)}$
1 2 4 ...
$n \times n\lfloor \log q \rfloor$
$G^{-1}(G)_2$
$n\lfloor \log q \rfloor \times \lfloor \log q \rfloor$
5
4
2