TRAPDOORS – RECAP

$m \sim n \lg q$
$m > n$

Def. A matrix $T \in \mathbb{Z}^{m \times m}$ 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.

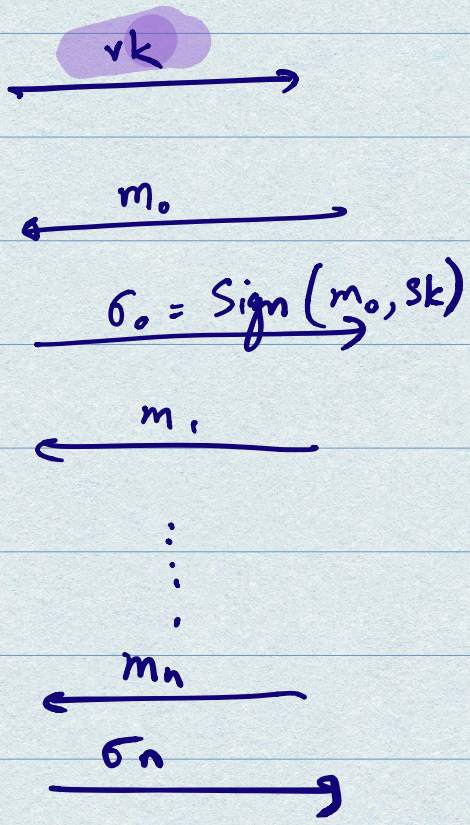
Type-1 T_A s.t. $AT_A = 0$

Type-2 T_{GA} s.t. $AT_{GA} = G$

Digital Signatures.

Ch | Adv

(vk, sk)



$(\tilde{m}, \tilde{\sigma})$

$$Pr\left[\tilde{m} \notin \{m_0 \dots m_n\} \wedge Verify(\tilde{m}, \tilde{\sigma}, vk) = 1\right] = negl(k)$$

GPV Signatures

KeyGen $\rightarrow$ sk, vk

$sk \downarrow T_A$ $\quad$ $vk \downarrow A$

Sign (m, sk) $\rightarrow$ H: Random Oracle

$sk \downarrow T_A$

Compute $H(m) \rightarrow v \in \mathbb{Z}_q^n$

Find "short" e s.t. $Ae = v$.

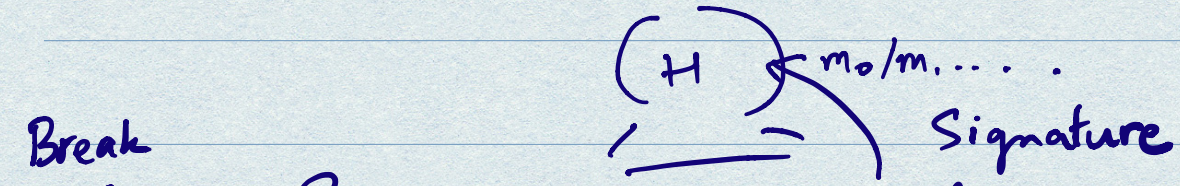
(using T_A)

Verify (σ, m, vk)

$vk = A$

Check if $A\sigma = H(m)$.

Also check σ is "short".



Break SIS.

Reduction

(A, v)

$vk = A$

m_0

σ_0

s.t. $A\sigma_0 = H(m_0)$

Sample σ_0 first,
then set $H(m_0) = A\sigma_0$

$(\tilde{m}, \tilde{\sigma})$

Set $H(\tilde{m}) = v$

$\Rightarrow \tilde{\sigma}$ is a short vector
s.t. $A\tilde{\sigma} = v$

Using T_A to find short e
s.t. $Ae = v$.

Can you find e' s.t. $Ge' = v$?
yes, $e' = G^{-1}(v)$

Given T_{GA} s.t. $AT_{GA} = G$
find e s.t. $Ae = v$?
$e = T_{GA} \cdot e'$

$A : [B \,||\, B.R]$

$\approx_{stat}$
uniform

IDENTITY BASED ENCRYPTION

A T_A

$\text{KeyGen}(1^\lambda) \to mpk, msk$

$v = H(id)$

$\text{Encrypt}(mpk, id, m) \to ct$

A

dual-Regev encryption

$\text{SKGen}(msk, id) \to sk_{id}$.

T_A $H(id)=v$ short e s.t. $Ae = v$

$\text{Dec}(ct, sk_{id}) \to m$

$id \| ct$

Dual-Regev decrypt using e.

SECURITY.

Ch $\qquad$ $\mathcal{A}$

mpk

id_1

sk_{id_1}

$\vdots$

id_n

sk_{id_n}

id^*, m_0, m_1

$b \xleftarrow{\$} \{0,1\}$

$\text{Enc}(mpk, id^*, m_b)$

b'?

ATTRIBUTE-BASED ENCRYPTION.

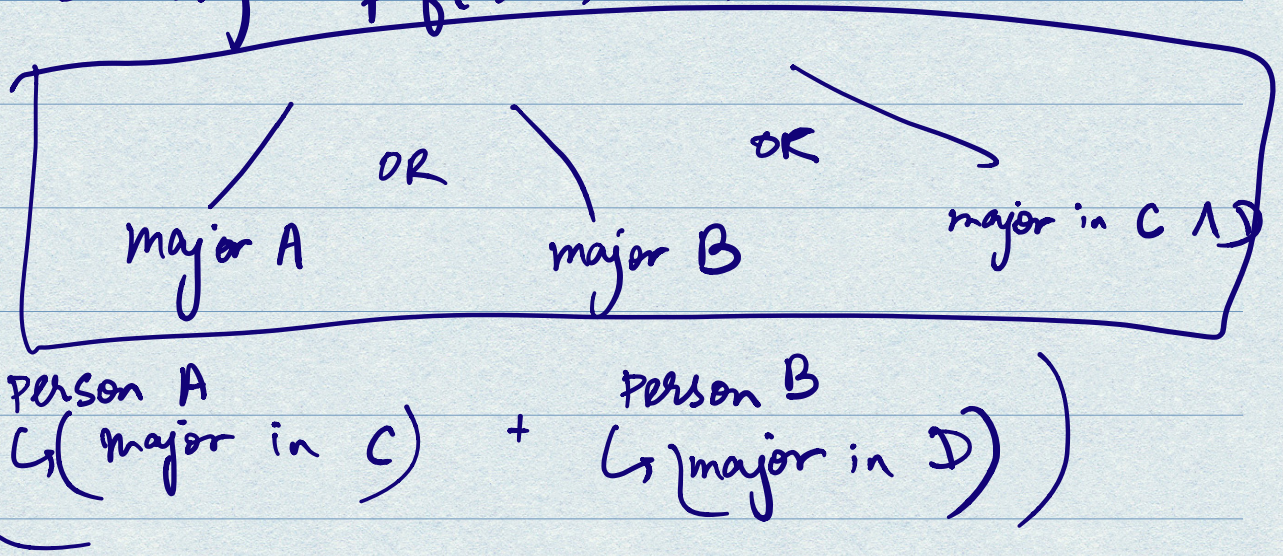
$\text{Enc}(m, x, mpk; r) \rightarrow ct$

$\text{SKGen}(f, msk; r) \rightarrow sk_f$

$\text{Dec}(ct, x, f, sk_f) \rightarrow m$ if $f(x)=1$

$\perp$ if $f(x)=0$

Security: If $f(x)=0$, m is hidden.



PREDICATE ENCRYPTION

$Dec(ct, f, sk_f) \rightarrow m$ or $\perp$

Security: If $f(x) = 0$, both x and m are hidden.

FUNCTIONAL ENCRYPTION

Security: If $f(x) = 0$, both x and m are hidden

If $f(x) = 1$, x is hidden (m is revealed).

FUNCTIONAL ENCRYPTION

KeyGen $\rightarrow$ (mpk, msk)

SKGen $(f, msk) \rightarrow sk_f$

Enc $(mpk, m) \rightarrow ct$

Dec $(sk_f, ct) \rightarrow f(m)$.

EXAMPLE: Email filtering.

Define f that outputs m iff m contains [course req] in its title outputs 0 o/w.

OBFUSCATION (IND-BASED)

[$\equiv$ FUNCTIONAL ENCRYPTION]

$\text{Obfuscate}(C) \rightarrow \hat{C}$

$\text{Eval}(\hat{C}, x) \rightarrow C(x)$.

IND-BASED OBFUSCATION

If $C_1 \equiv C_2$ [i.e. $\forall y, C_1(y) = C_2(y)$]
then $\text{Obfuscation}(C_1) \approx \text{Obfuscation}(C_2)$

+ONE-WAY FUNCTIONS.

↳ FUNCTIONAL ENCRYPTION

⇉ FHE

⇉ ABE

⇉ IBE