- Scribes?
- lecture recording

LWE (learning w/ errors assumption):

possible to generate (A, s)

- A is indistinguishable from uniform
- $\|s^T \cdot A\|_\infty$ small, last coordinate of s is -1

Regev encryption:

$pk: A$, $sk: s$

$\mathrm{Enc}_{pk}(b)$: choose 0/1-vector r

output ciphertext $A \cdot r - \begin{bmatrix} 0 \\ \vdots \\ 0 \\ b \cdot \lfloor q/2 \rfloor \end{bmatrix}$

$\mathrm{Dec}_{sk}(u)$: Compute $s^T \cdot u = b'$

- output 0 if b' is closer to 0
- output 1 if b' is closer to $\lfloor q/2 \rfloor$

$$s^T \cdot \left(Ar - \begin{bmatrix} 0 \\ \vdots \\ 0 \\ b\lfloor q/2 \rfloor \end{bmatrix} \right) = s^T A \cdot r + b\lfloor q/2 \rfloor$$

$$= \lambda + b \cdot \lfloor q/2 \rfloor = b'$$

Intuition (take 1): encryption of b is a matrix C such that $s^T C \approx b \cdot s^T$

addition works ok; multiplication gives noise too large

flattening gadget

$\gamma = \lceil \log q \rceil$

$$c = \begin{bmatrix} c_1 \\ \vdots \\ c_m \end{bmatrix} \xrightarrow{G^{-1}} \begin{bmatrix} c_{11} \\ c_{12} \\ \vdots \\ c_{1\gamma} \\ c_{21} \\ \vdots \\ c_{2\gamma} \\ \vdots \\ c_{m\gamma} \end{bmatrix}$$

$c_{11} \ldots c_{1\gamma}$: binary rep. of c_1

$c_{21} \ldots c_{2\gamma}$: binary rep. of c_2

$\exists G$ s.t. $\boxed{G \cdot G^{-1}(c) = c}$

$$G = \begin{pmatrix} 1 & 2 & 4 & \cdots & 2^{\gamma} & & & & & \\ & & & & & 1 & 2 & 4 & \cdots & 2^{\gamma} \\ & & & & & & & & \ddots & \end{pmatrix}$$

---

intuition: enc. of b is a matrix C s.t. $s^T C \approx b \cdot s^T \cdot G$

$s^T C = b s^T \cdot G + \lambda$

$s^T \cdot C_1 = b_1 s^T G + \lambda_1$

$s^T \cdot C_2 = b_2 s^T G + \lambda_2$

addition: $s^T (C_1 + C_2) = b_1 s^T G + \lambda_1 + b_2 s^T G + \lambda_2$

$= (b_1 + b_2) \cdot s^T G + \underbrace{\lambda_1 + \lambda_2}_{\text{noise}}$

Multiplication: $s^T C_1 \cdot G^{-1}(C_2) = (b_1 s^T G + \lambda_1) \cdot G^{-1}(C_2)$

$= b_1 s^T C_2 + \lambda_1 G^{-1}(C_2)$

$= \underline{b_1 b_2 s^T G} + \underbrace{\lambda_2 + \lambda_1 G^{-1}(C_2)}_{\text{noise}}$

$\Rightarrow \|\text{noise}\|_\infty \leq (N+1) \cdot \max\{\|\lambda_1\|_\infty, \|\lambda_2\|_\infty\}$

pk: A, sk: s

$Enc_{pk}(b)$: $b \cdot G + A \cdot R$, for $R \in \{0,1\}^{m \times N}$

$s^T(bG + AR) = s^T bG + \underbrace{s^T AR}_{\text{small}}$ ← 0/1-matrix

$\|s^T AR\|_\infty \leq \lambda m$

ZK from secure computation

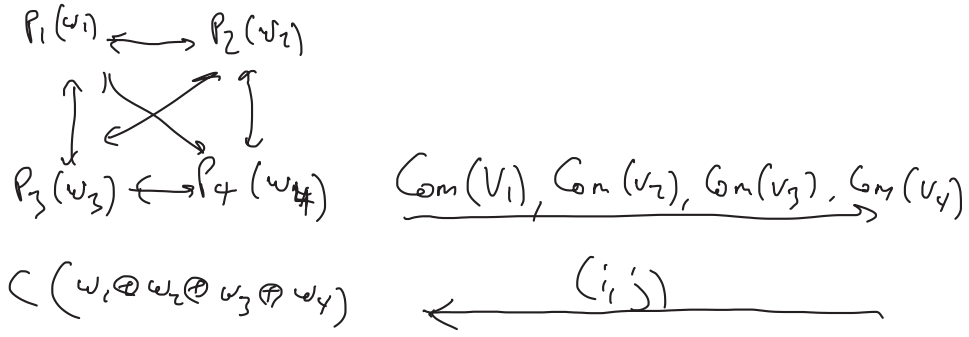
$\underline{P}(\omega)$ $\xrightarrow{C(\omega) \stackrel{?}{=} 1}$ $\underline{V}(C)$

Semi-honest MPC $\xrightarrow{ZK}$ malicious MPC

ZK ← malicious MPC w/ honest majority

MPC-in-the-head

P(w) V(C)



- If Π is secure for 2 semi-honest corruptions, this protocol is ZK
- This protocol has soundness error at most $1 - 1/\binom{n}{2}$
  - Assume C is not satisfiable
  - In any collection of n views, there must be at least one pair of inconsistent parties
  - V challenges on an inconsistent pair w/ prob. $\geq 1/\binom{n}{2}$

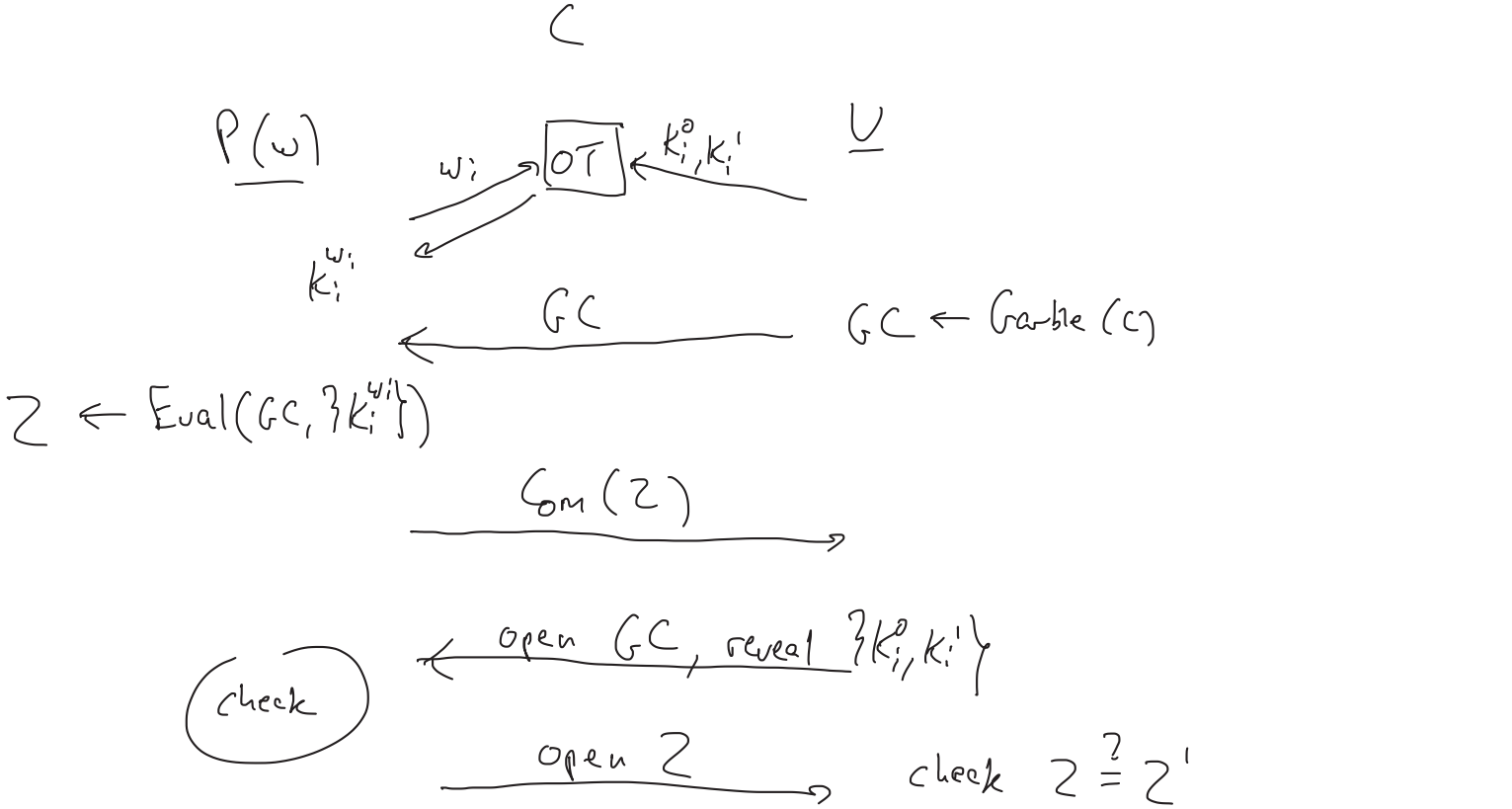
V can challenge t parties

- ZK holds as long as Π secure for t semi-honest corruptions

- If Π is correct for t malicious corruptions, soundness holds

---

2k from GC



Garbling should satisfy

- authenticity: P cannot determine z' unless it holds keys corresponding to an input w s.t. $C(w)=1$
- verifiability: if correctness check passes, then for any set of keys corresponding to a satisfying w, the z obtained by Eval is the same

Can use privacy-free garbling schemes - can be more efficient than semi-honest 2PC!