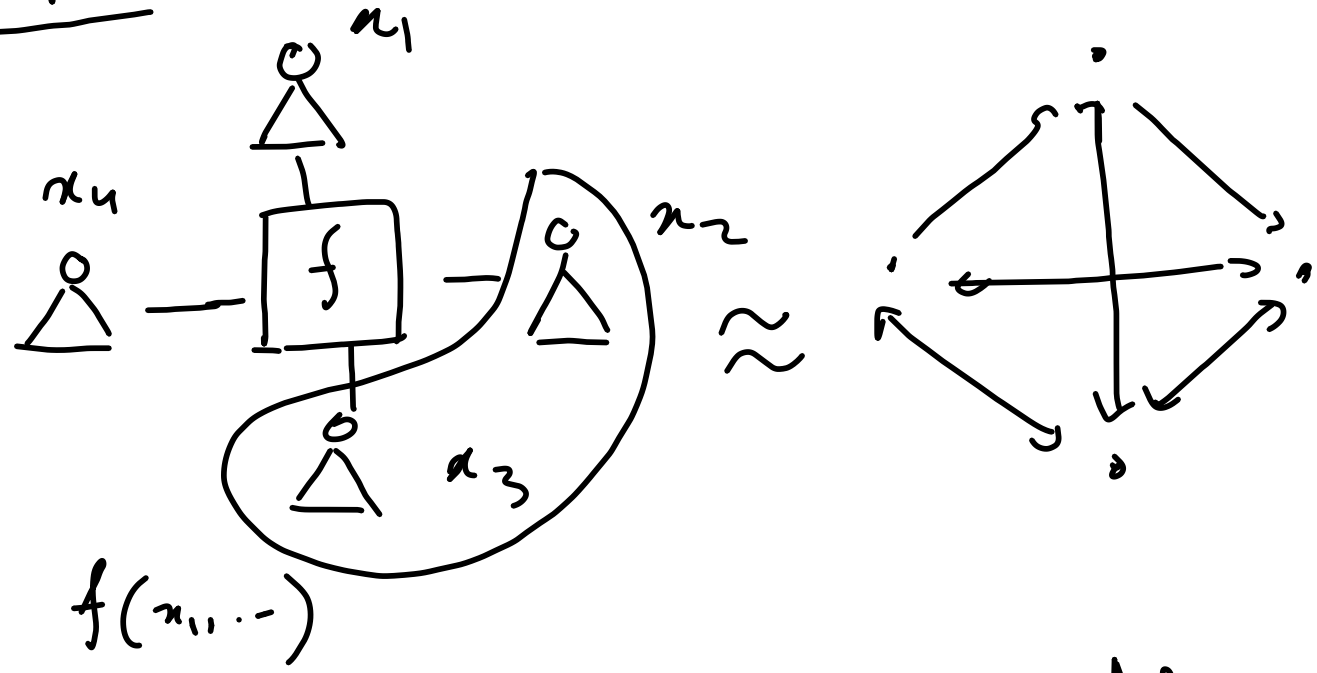
MPC



- Adversarial Model.

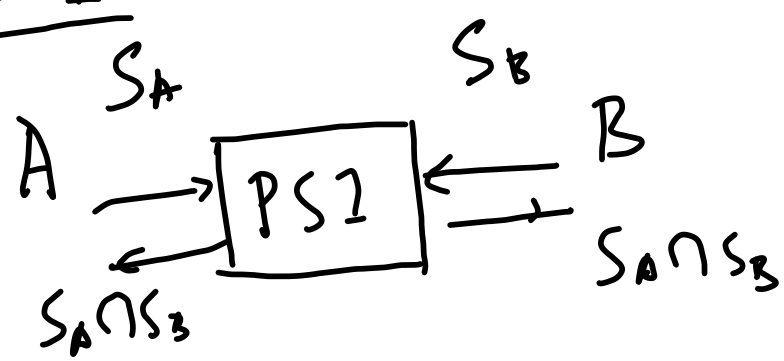
80's Yao, GMW

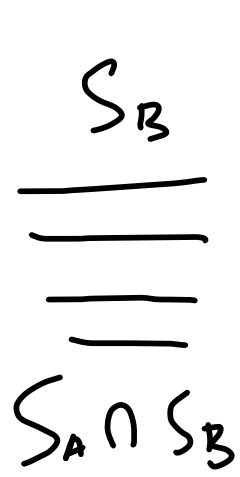
90', 2000: Damgh Sugarbit

NOW:

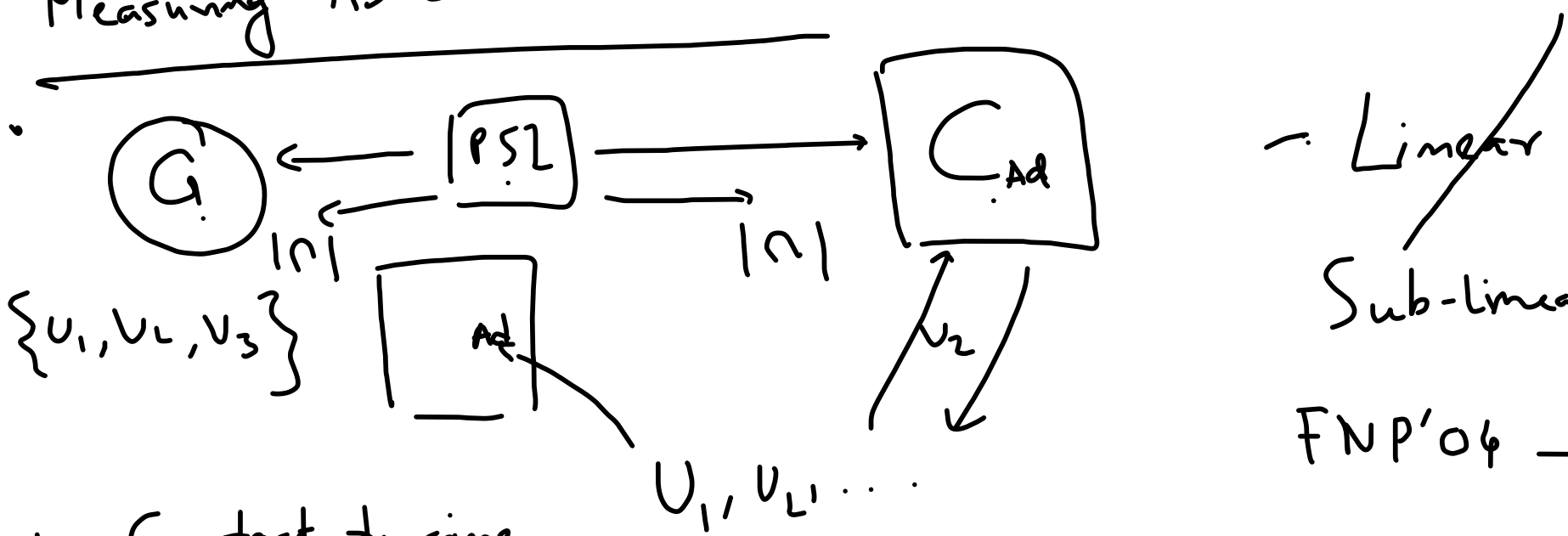
PSI

$|S_A| \leq |S_B| \leq n$





Measuring AD-conversion Rate:

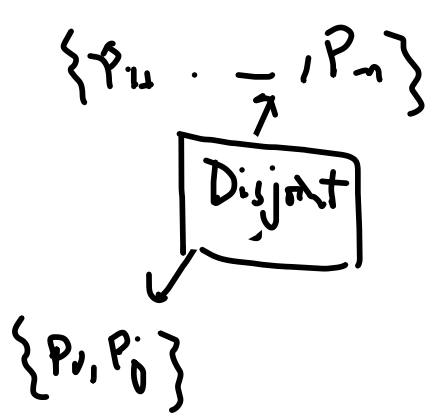


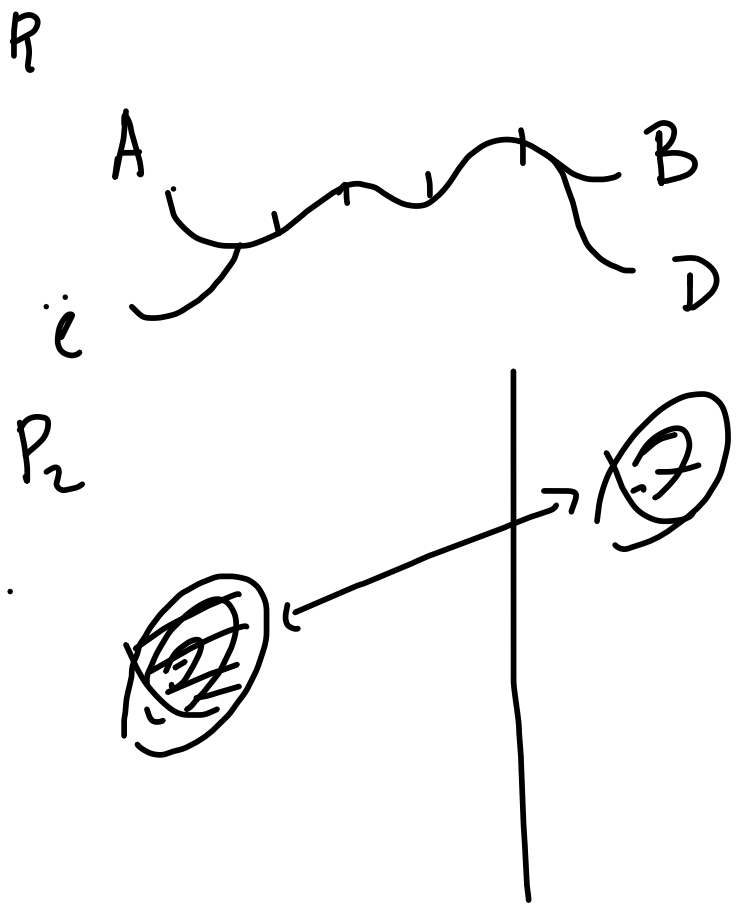
- Linear Communication

Sub-linear.

FNP'04 $\rightarrow \Omega(n)$

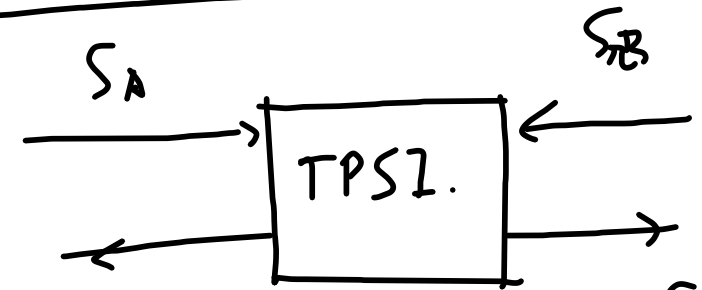
- Contact tracing





- Intersection Size Large.

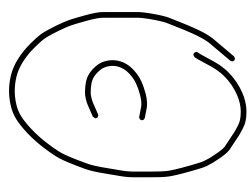
Threshold PSI.

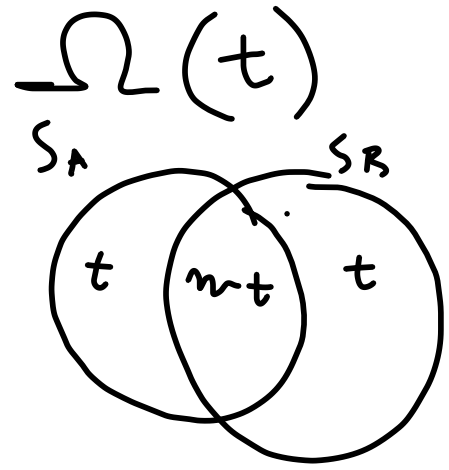


$S_A \cap S_B$ iff $|S_A \cap S_B| > n-t$

Avijit P.GE - $\tilde{O}(n)$

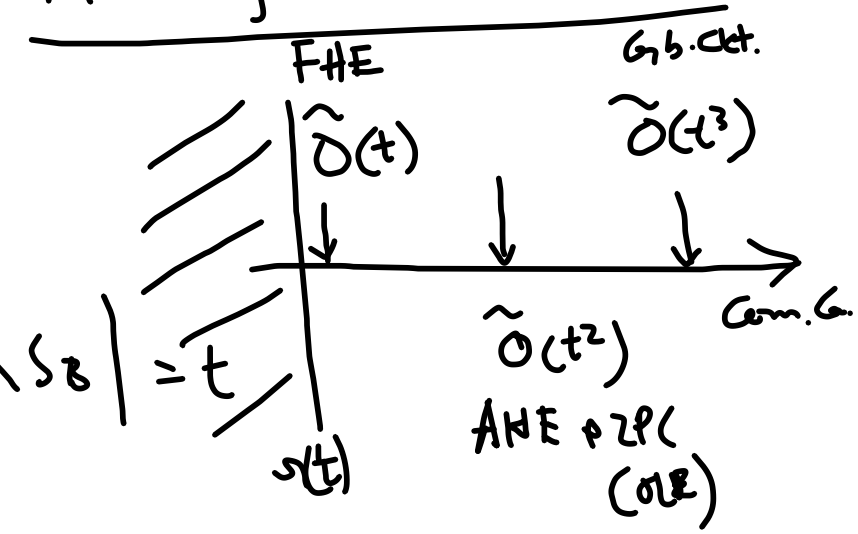
t { - P.P
- Com > 3 hr.





$|S_A \setminus S_B| = t$

Matching upper Bound.



Lower Bound.

$o(t)$

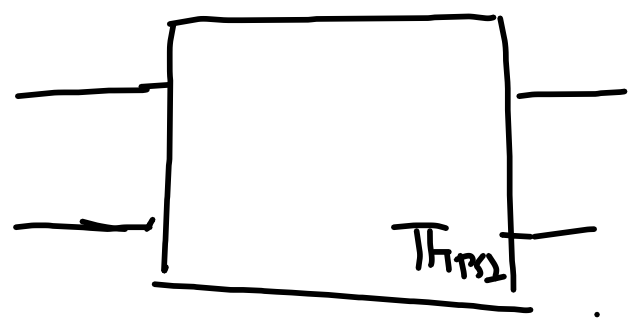
Π_{TPSI}

Π_{PSI}

$|S_A| = t$

$S_A \| \{a_{i_1}, \ldots\}$

$n-t$



$|S_B| = t$

$S_B \| \{a_{i_1}, \ldots\}$

Some $n-t$ elmts

PSI with $o(t)$ Com.

↳ Breaks PSI Lower Bound.

Construction

$S_A = \{a_1, \ldots, a_n\}$

$P_A(x) = (x-a_1) \cdots (x-a_n)$

$= P_\cap(x) \cdot P_{A\setminus B}(x)$

$S_B = \{b_1, \ldots, b_n\}$

$P_B = (x-b_1) \cdots (x-b_n)$

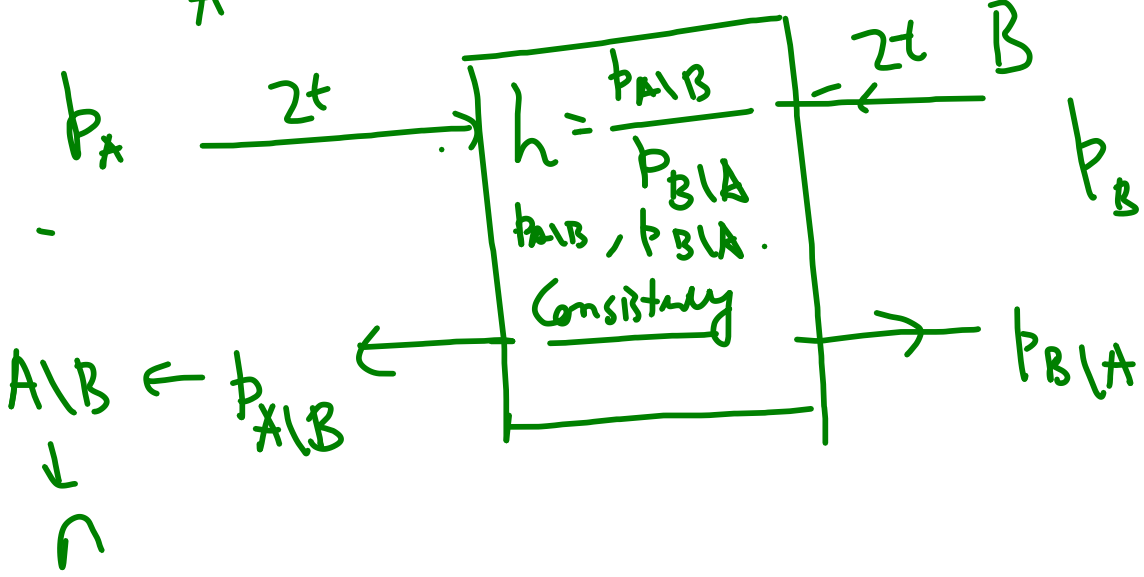
$= P_\cap(x) \cdot P_{B\setminus A}(x)$

$h = \frac{P_A}{P_B} = \frac{P_{A\setminus B}}{P_{B\setminus A}} \Rightarrow 2t$ points

($P_{A\setminus B}$: t points; $P_{B\setminus A}$: t points)

$A\setminus B$

$\cap = A \setminus (A\setminus B)$



FHE $\rightarrow \tilde{O}(1)$

Rational Interpolation

↓

Gaussian Elimination $2t \times 2t$

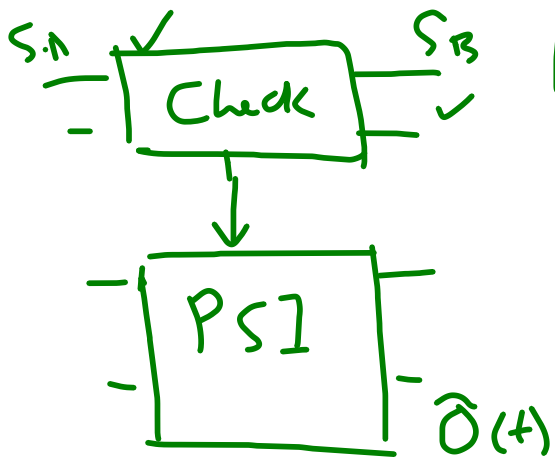
↓ $O(t^3)$

MPC (Ckt) $\rightarrow \tilde{O}(t^3)$

TPSI

Cardinality Check

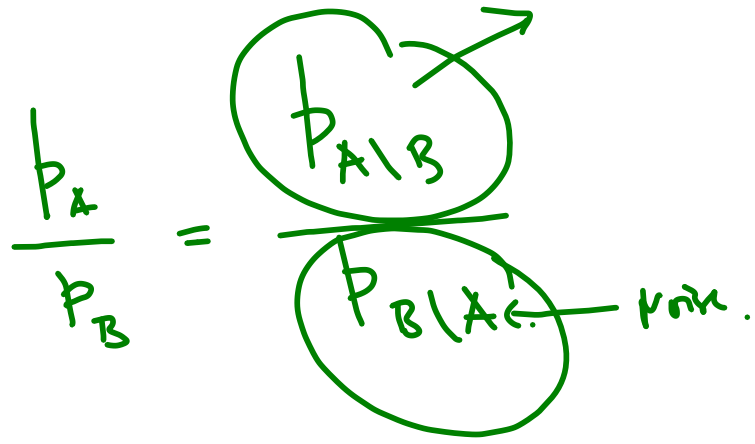
PSI.

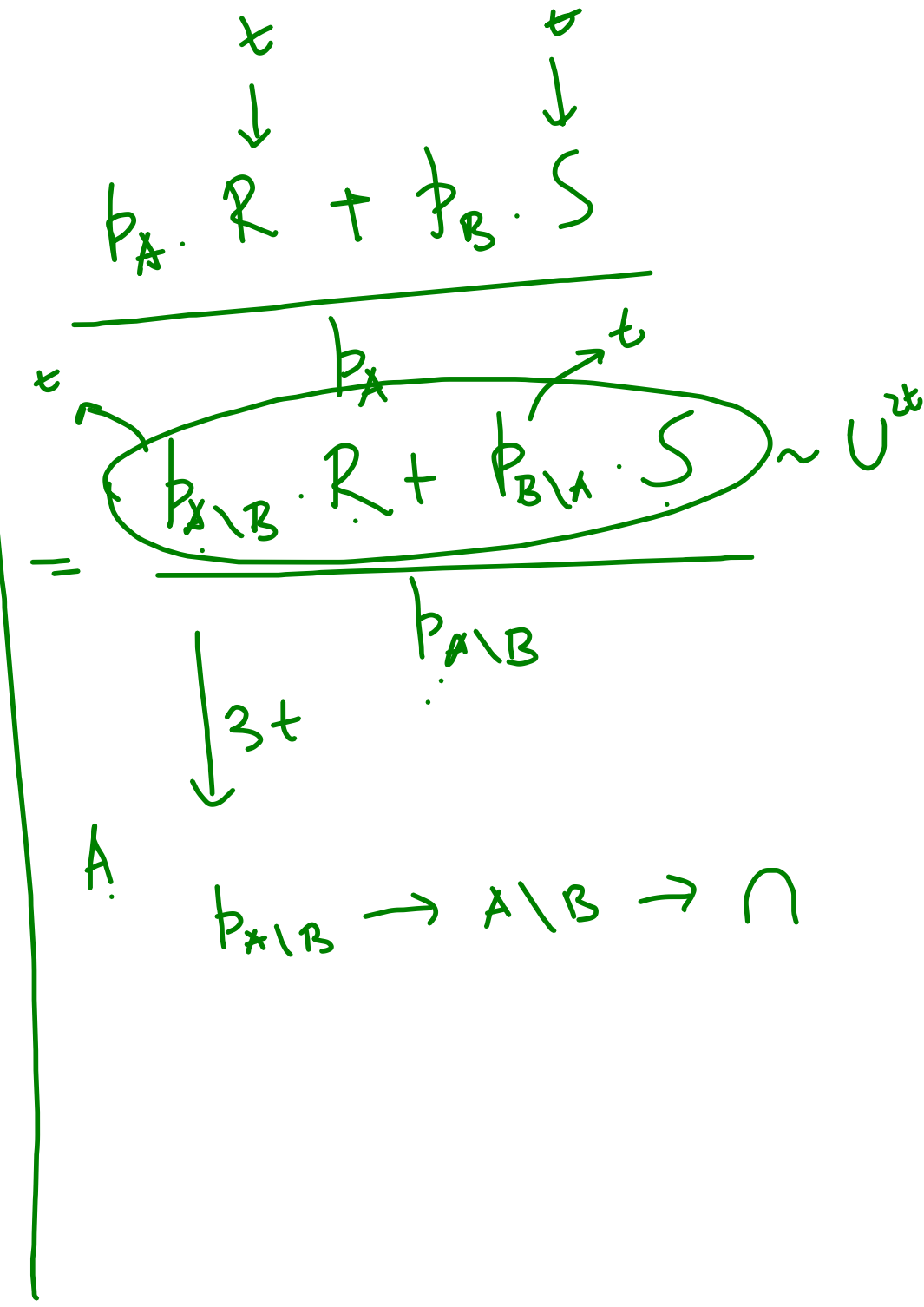


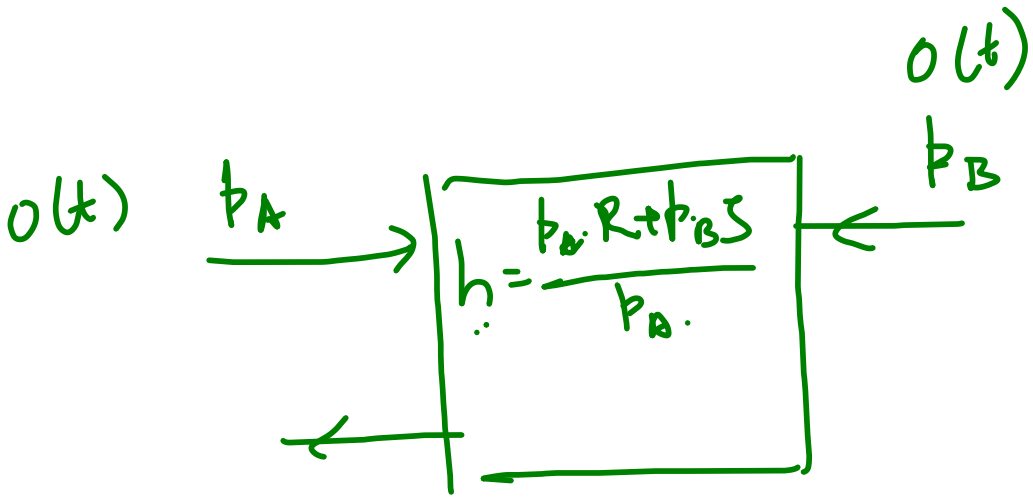
$|S_A \cap S_B| > n-t$

PSI

$|S_A \cap S_B| > n-t$

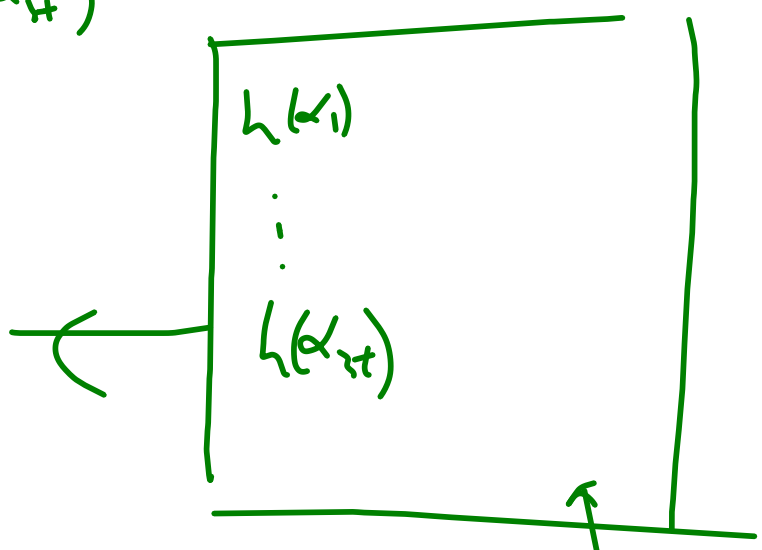






$\tilde{O}(t)$

$\flat_{A'}(\alpha_1), \ldots, \flat_A(\alpha_t)$



$\flat_B(\alpha_1), \ldots, \flat_B(\alpha_t)$

CDH, LWE

OT

Generic MPC with Constant Overhead

Check.

$\{a_1, a_2, a_3\}$

$p_A'(x) = x^{a_1} + x^{a_2} + x^{a_3}$

$\{a_1, a_2, b_3\}$

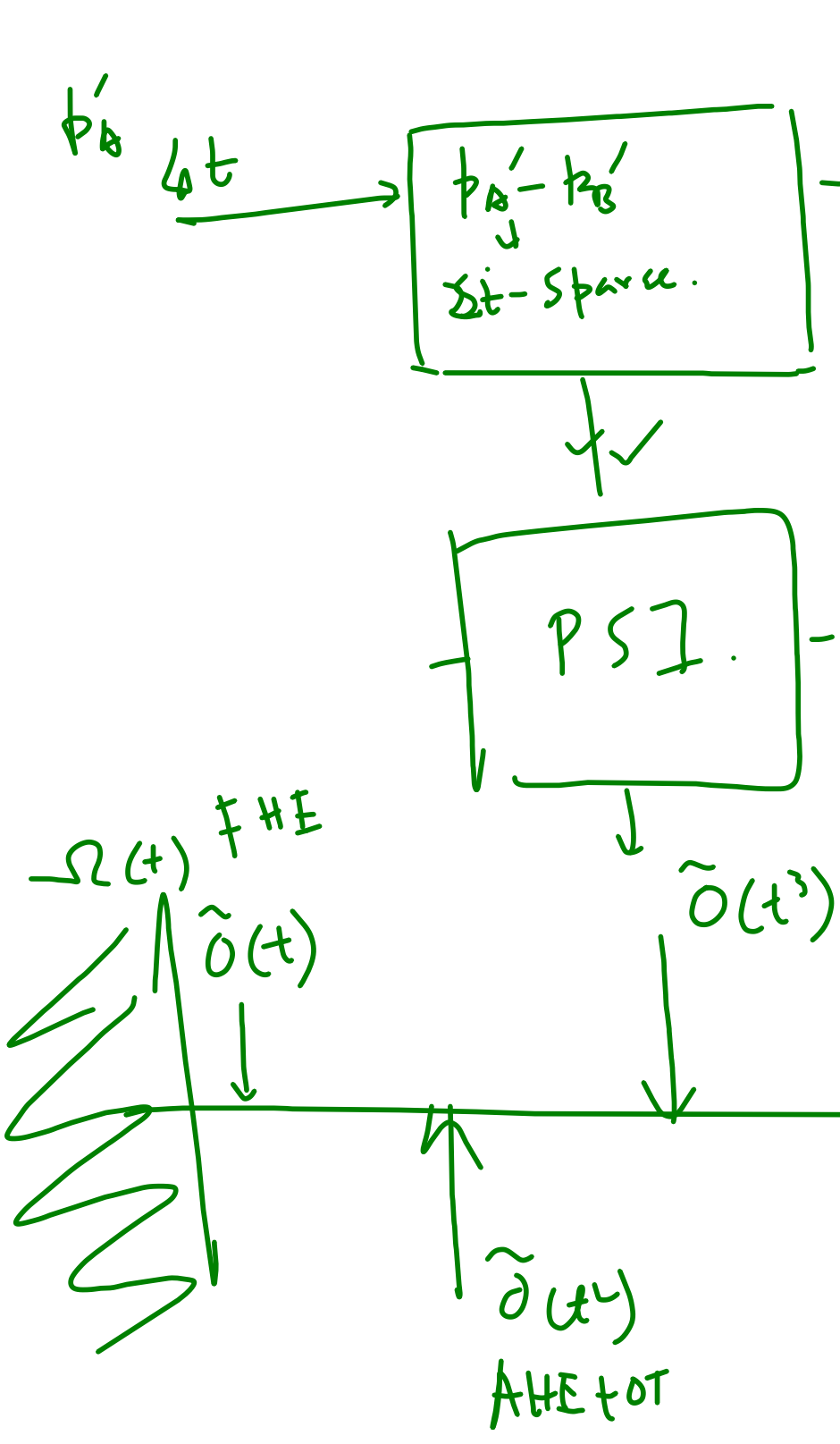
$p_B'(x) = x^{a_1} + x^{a_2} + x^{b_3}$

$p_A(x) - p_B(x) = \underbrace{x^{a_3} - x^{b_3}}$

↓ sparsity 2

$S_A \to p_A'$ $\quad h' = p_A' - p_B'$ $\quad$ 2t sparse? $\quad p_B' \leftarrow S_B$

$h'(\alpha_1), \ldots h'(\alpha_{4t})$



Find determinant of a $4t \times 4t$ matrix in a secure way.

$\downarrow$ $\tilde{O}(t^4)$ AHE

$\tilde{O}(t^2)$ with AHE + OT

BBP'24 → $O(\lambda l t^2 \text{ polylog } t)$

↓ # p-steps

BMRR'21 → $O(\lambda l t \text{ polylog } t)$

t^2 polylog t.

↓

$O(\lambda^2 l t \text{ polylog } t)$

EHE

$O(t \log^* t)$