

# Outline

1. (Long) Introduction
2. Randomized Polynomials (w/applications to round-efficient MPC)
3. Randomized Encodings w/applications to  $NC^0$  Cryptography
4. Constant Input Locality
5. Computational Randomized Encodings (w/applications)
6.  $NC^0$  Linear Stretch PRG (w/applications)

# PRG - Parallelism vs. Stretch

complexity

stretch

poly-time

super linear

NC

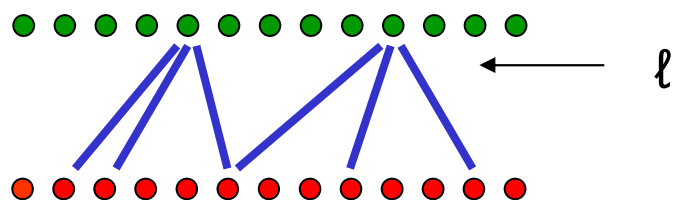
linear

**Motivation**

parallel implementation of crypto tasks  
(e.g., Naor commitment, stream cipher)

$NC^0$

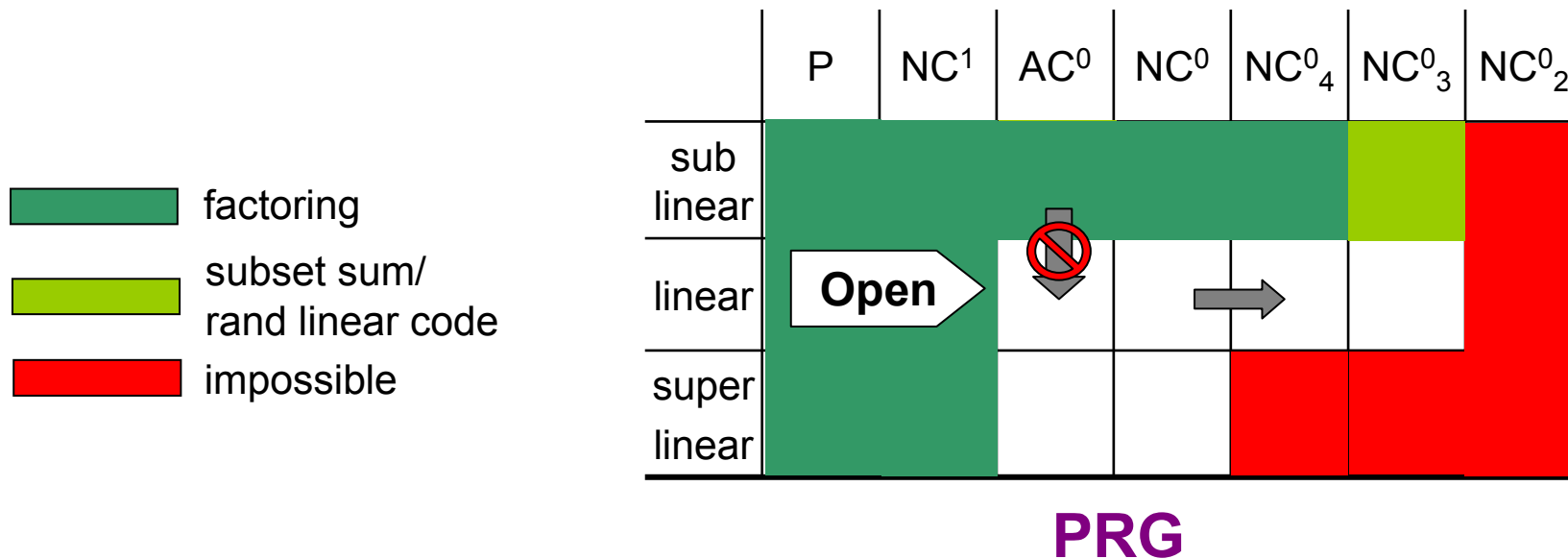
$NC^0_\ell$



# Previous Work

- **Negative results**

- No PRG in  $NC^2$  from any PRG [Goldreich 00, Cryan [Goldsch 01], Micali 84]
- No Super-linear PRG in  $NC^3$ ,  $NC^4$  [Naor, Reingold, Shpilka, Wigderson 03]
- Sub-Linear PRG in  $AC^0$  from subset sum ~~BB~~ [Vigna 05]
- Sub-Linear PRG in  $NC^4$  from any PRG in  $NC^1$  [AIK 04]
- Sub-Linear PRG in  $NC^3$  from decoding random linear code [AIK]
- Linear PRG in  $NC^4$  from Linear PRG in  $NC^0$  [AIK 04]



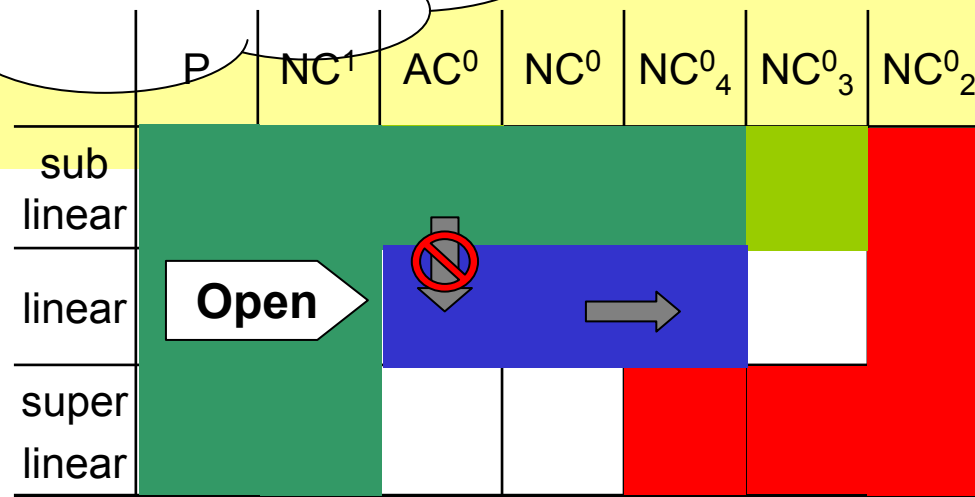
# Main Results

- Algebraic assumption of [Alekhovich 03]  $\Rightarrow$  LPRG in  $NC^0$
- LPRG in  $NC^0 \Rightarrow$  Inapproximability of MAX 3SAT.

Conclusion:

Algebraic  
Inapproximability

Already proven directly  
by [Alekhovich 03]  $\Rightarrow$



PRG

# NC<sup>0</sup> Crypto and Inapproximability

## k-Constraint Satisfaction Problem

$$\begin{array}{l} - X_1 + X_3 \cdot X_5 = 0 \\ - X_2 \cdot X_3 \cdot X_4 = 1 \\ \cdot \\ \cdot \\ \cdot \\ - X_2 + X_3 + X_4 = 1 \end{array}$$

- List of constraints over n variables  $x_1, \dots, x_n$
- Each constraint involves k variables

- Q. how many of the constraints can be satisfied together?

**Corollary of PCP thm**<sub>[ALMSS,AS 92]</sub>:

**If:**  $P \neq NP$

**Then:** Cannot distinguish:

- Satisfiable 3-CSP
- $\epsilon$ - unsatisfiable 3-CSP

**Here:**

**If:** Lin-Stretch PRG in NC<sup>0</sup>.

**Then:** Cannot distinguish:

- Satisfiable 3-CSP
- $\epsilon$ - unsatisfiable 3-CSP

# LPRG in $NC^0 \Rightarrow$ Inapproximability

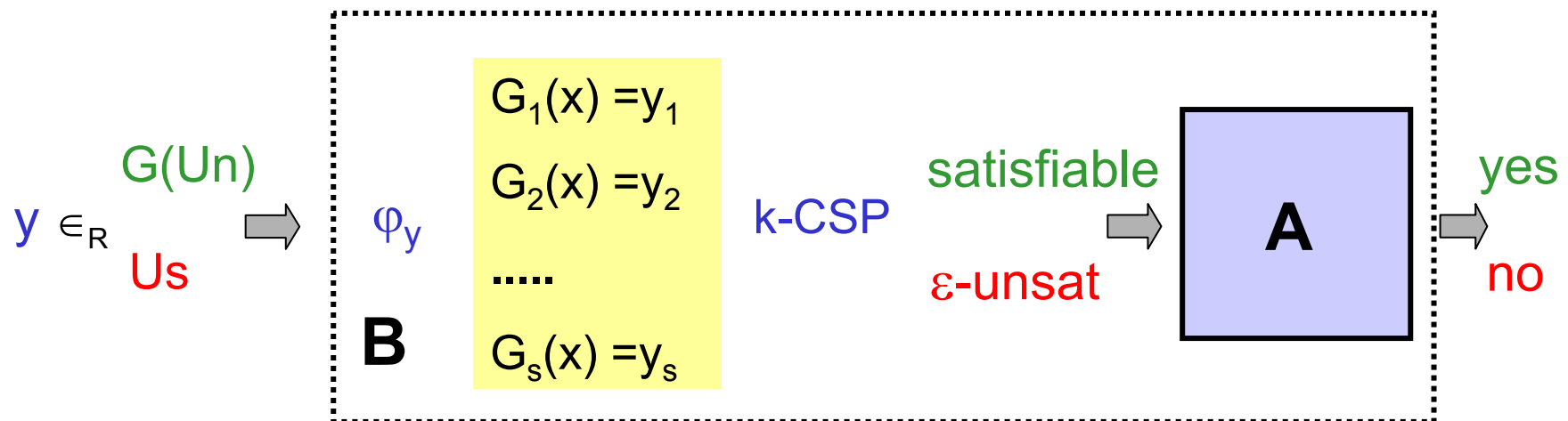
**Thm.** If  $G:\{0,1\}^n \rightarrow \{0,1\}^s$  is a PRG in  $NC_k^0$  and  $s-n=\Omega(n)$

**Then,**  $\exists \epsilon$  s.t **satisfiable k-CSP** and  **$\epsilon$ -unsat k-CSP** are indistinguishable

**Proof:** k-CSP distinguisher **A**  $\Rightarrow$  distinguisher for PRG **B**

• If  $y \in_R G(Un)$   $\Rightarrow$   $\phi_y$  is **satisfiable** (since  $\exists x$  s.t  $G(x)=y$ )

• If  $y \in_R Us$   $\Rightarrow$  (w.h.p.)  $\phi_y$  is  **$\epsilon$ -unsat**



# LPRG in $NC^0 \Rightarrow$ Inapproximability $\checkmark$

Claim: If  $y \in_R Us$   $\Rightarrow$  (w.h.p.)  $\varphi_y$  is  $\epsilon$ -unsat

Proof:

- Assume  $\varphi_y$  is not  $\epsilon$ -unsat, then  $\exists x$  s.t.  $\Delta_H(y, G(x)) < \epsilon$
- Hence,  $\Pr[\varphi_y \text{ is not } \epsilon\text{-unsat}] = \Pr[\Delta_H(y, \text{Image}(G)) < \epsilon]$

$$\leq (|\text{Image}(G)| \cdot \text{Vol}(s, \epsilon s)) / 2^s$$

$$\leq 2^{n+H(\epsilon)s - s} = \text{neg}(n)$$

