Andrej Bogdanov
UNIVERSITY OF OTTAWA

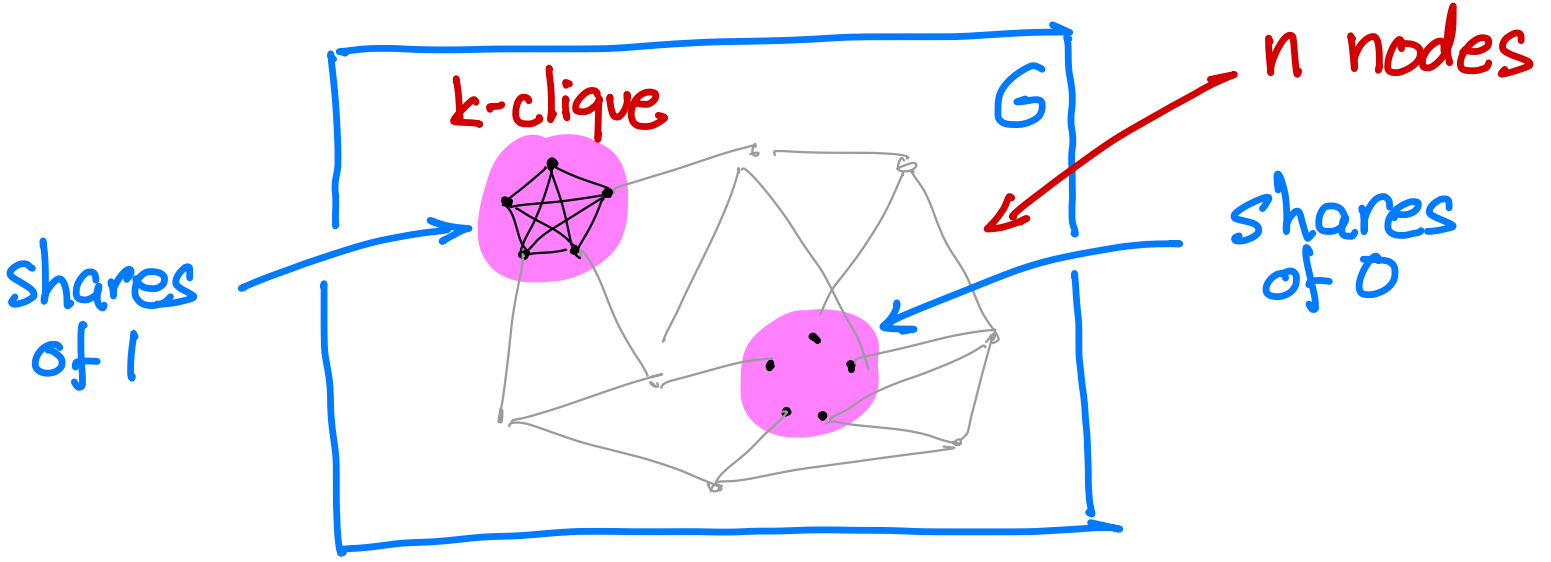
low-degree analysis of planted random subgraphs

with Chris Jones, Alon Rosen & Ilias Zadik

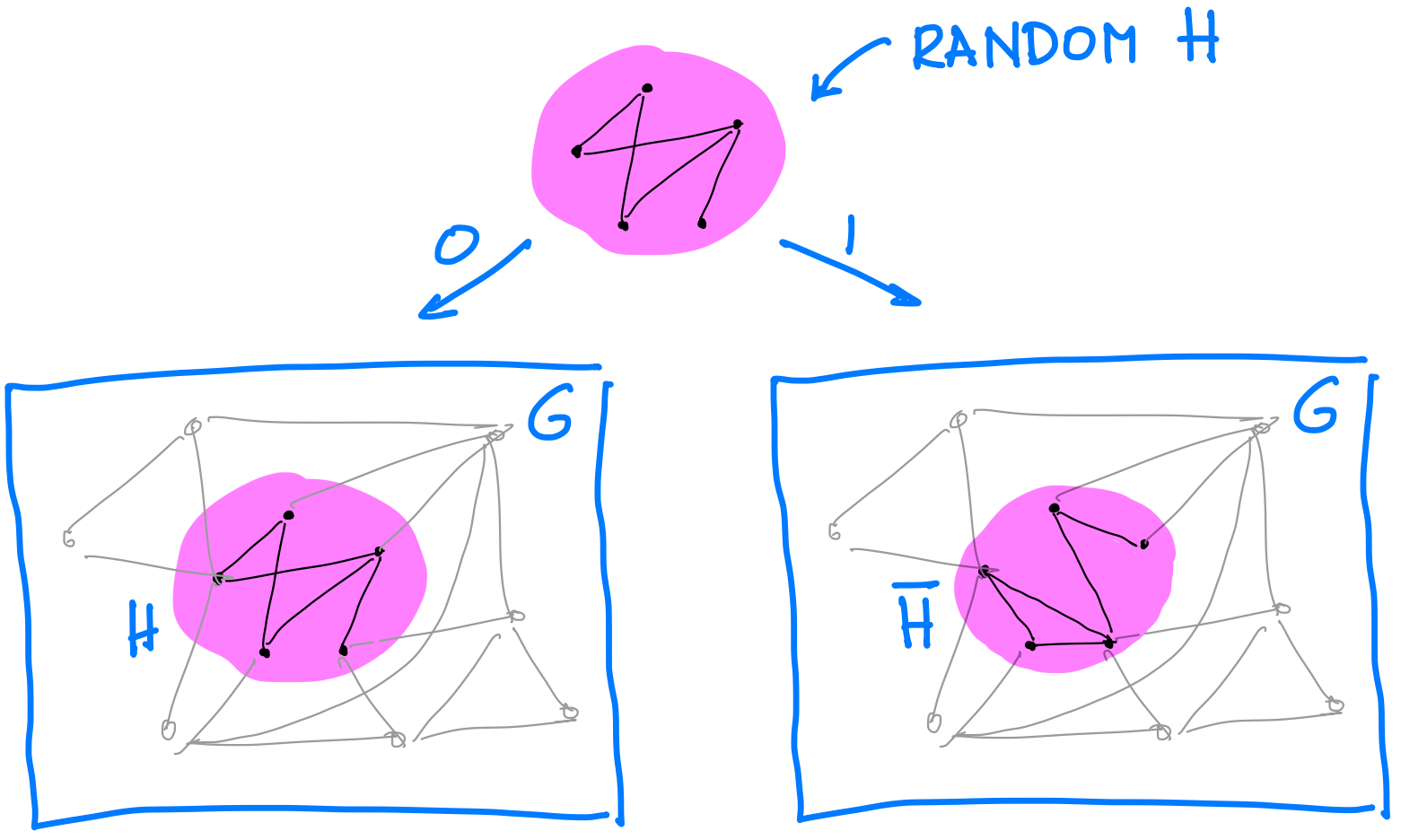
TCC 24

another way to share

Abraw-Beimel-Ishai-Kushilevitz-Narayanan

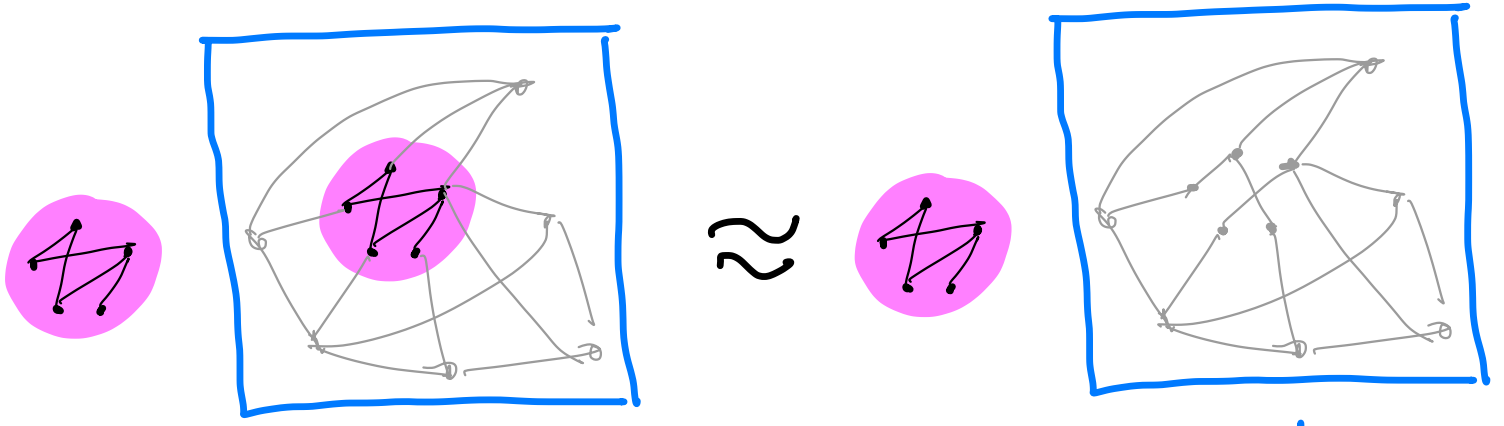


share size = $2 \log n$


RANDOM H
0
1
G
H
G
H

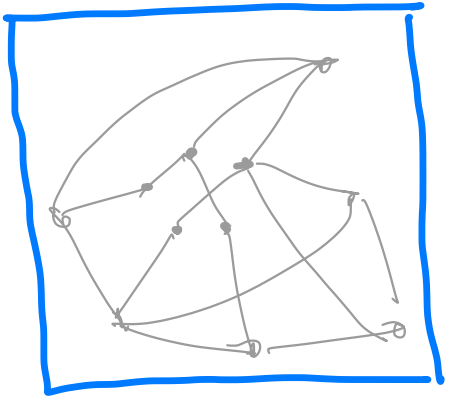
planted random subgraph conjecture

Abram-Beinel-Ishai-Kushilevitz-Narayanan

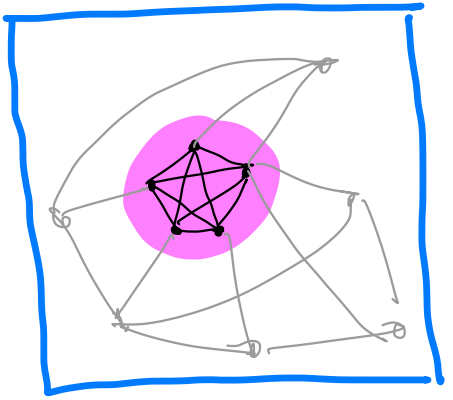


pseudo-independent

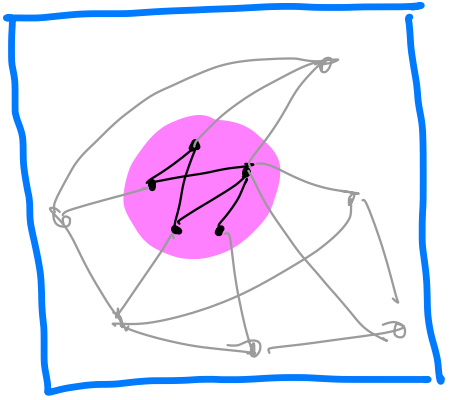
#edges - #nonedges



$\pm\Theta(n)$



$+\binom{k}{2}$

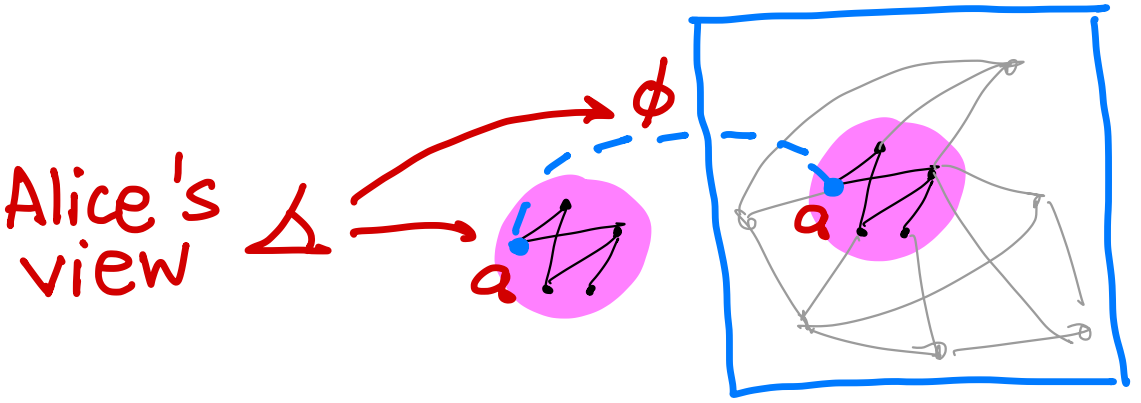


$\pm\Theta(k)$

our result

G is pseudorandom given H up to error $k/n + \text{l.o.t.}$ for degree $o(\log^2 n / \log\log n)$ (when $k = n^{1-o(1)}$)

and more...

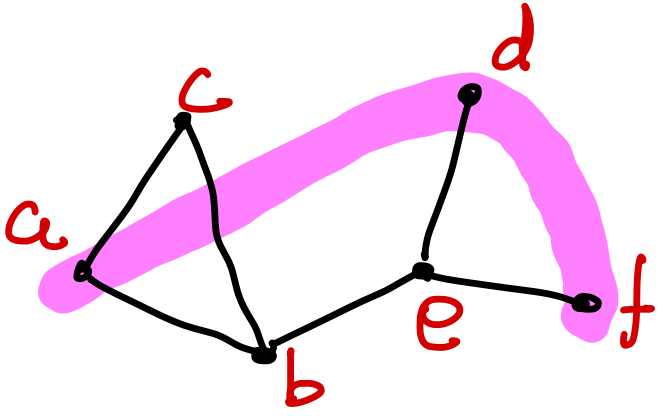


still secure if $\phi(a)$ leaked

error $\leq 2k/n$ + l.o.t.

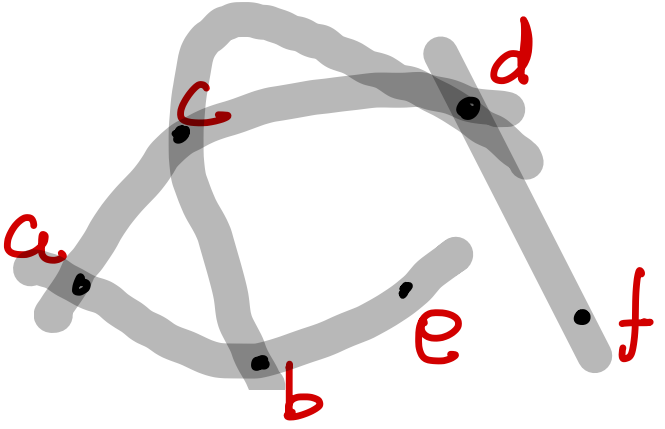
forbidden graph access structures

and more...



error against ℓ-coalitions $\leq 2^{\ell} \cdot \frac{k}{n}$

r-hypergraph access structure



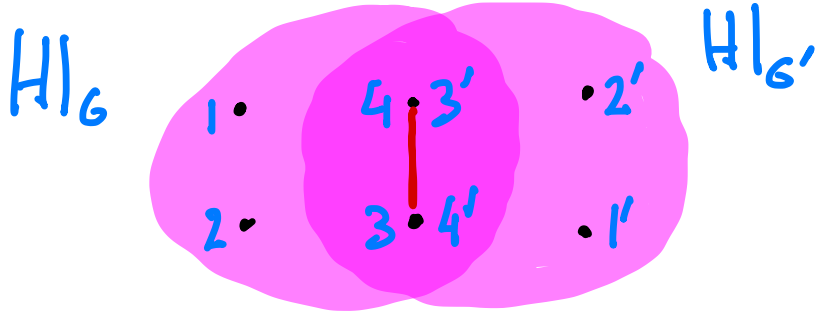
secure up to degree $\tilde{\Omega}((\log n)^{r/(r-1)})$

the replica calculation

$$\text{avg. } LR^2_{\le d} = E \sum_{1 \le |S| \le d} E[\text{PARITY}_S(G)|H]^2$$

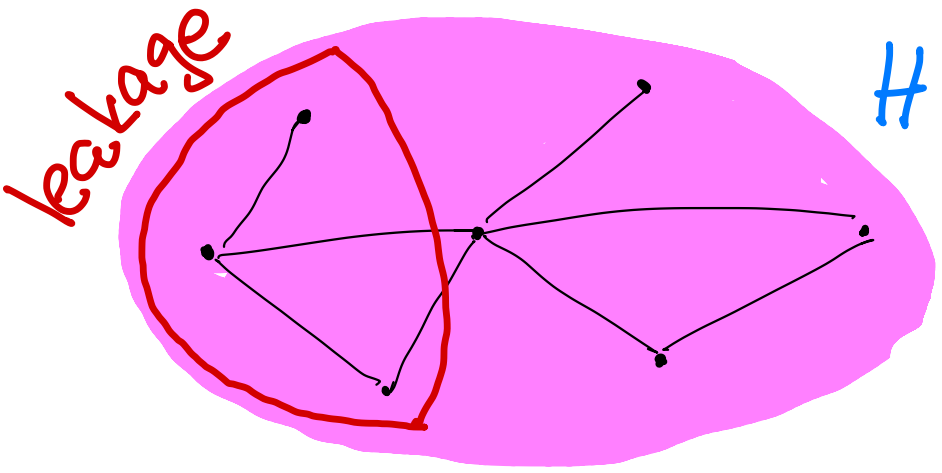
$$= \sum E\,E[\text{PARITY}_S(G)\,\text{PARITY}_S(G')|H]$$

$$= \sum E[\text{PARITY}_S(G)\,\text{PARITY}_S(G')]$$



private simultaneous messages for random functions

Abram-Beimel-Ishai-Kushilevitz-Narayanan



the best way to share

Abraw-Beimel-Ishai-Kushilevitz-Narayanan