Single Server PIR: A Song of Computation & Information

SALIM EL ROUAYHEB

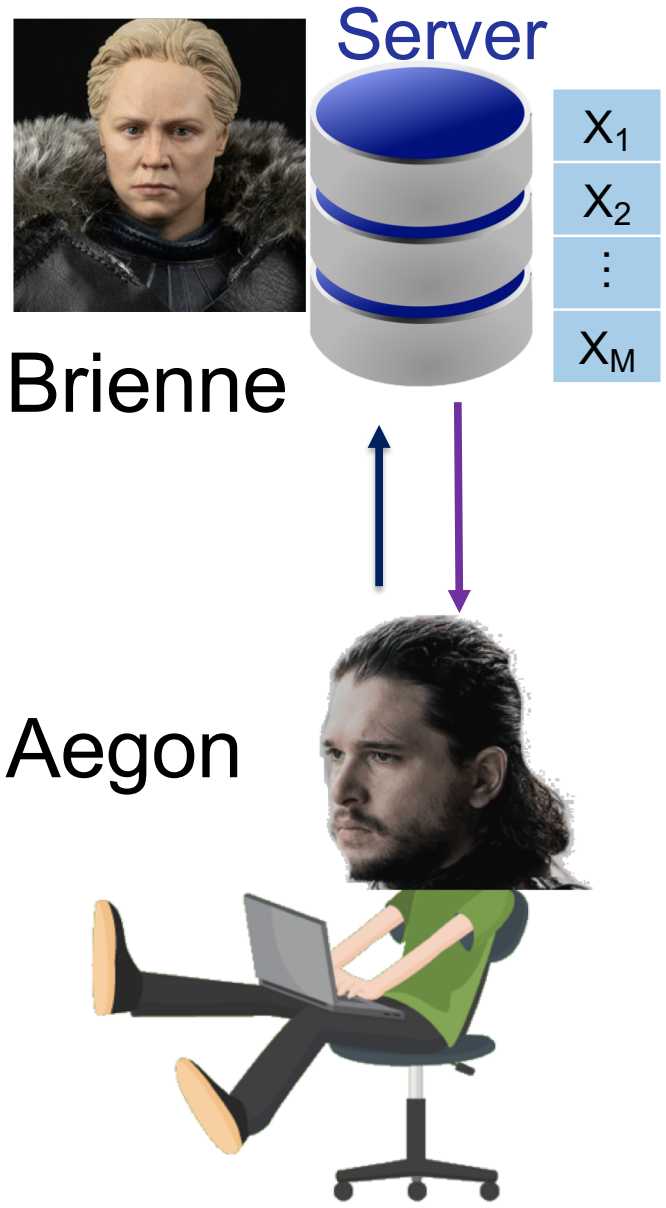
ECE Department
Rutgers University

Funding: NSF, Google

What is PIR?

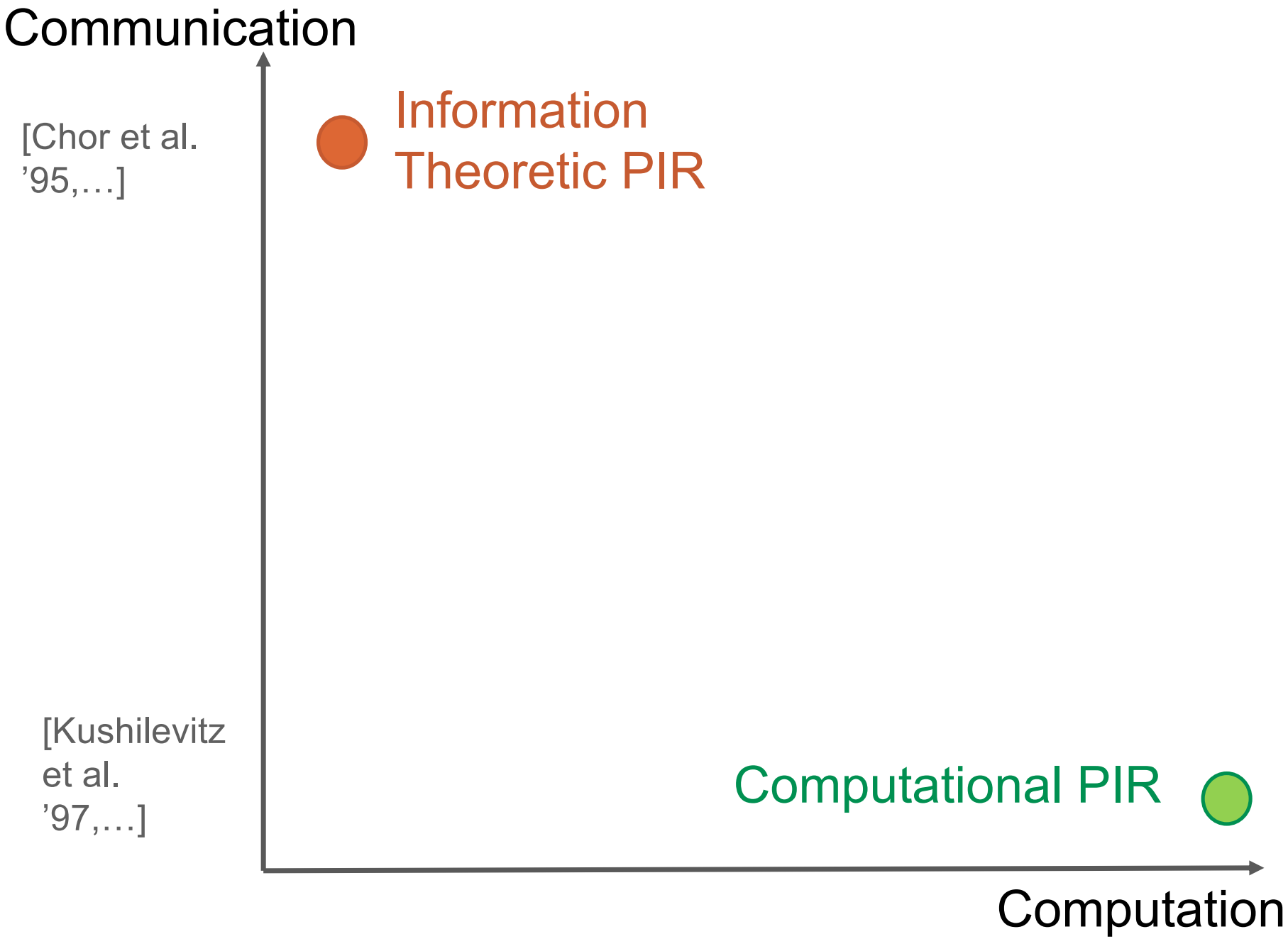
Private Information Retrieval
Or
How to search Google without revealing what you are searching for

SETUP

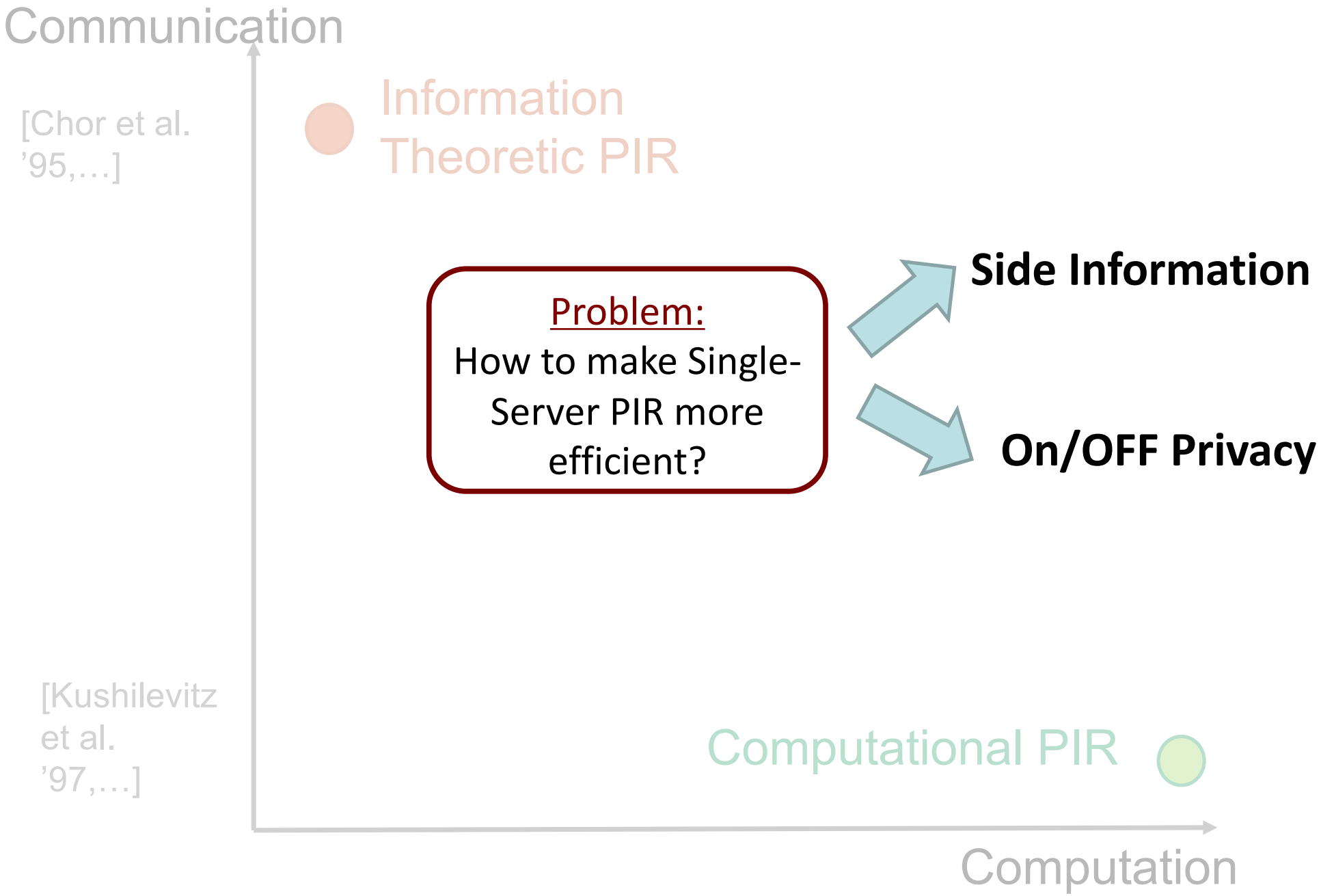


- Aegon wants Xi without revealing i to Brienne
- First studied by Chor et al. in ‘95
- Information Theoretic Privacy
- Single server ➔ Must download all the data
- Need multiple non-colluding servers #sad

Single-Server PIR is the Holy Grail



Single-Server PIR is the Holy Grail



How Can Side Info Help?

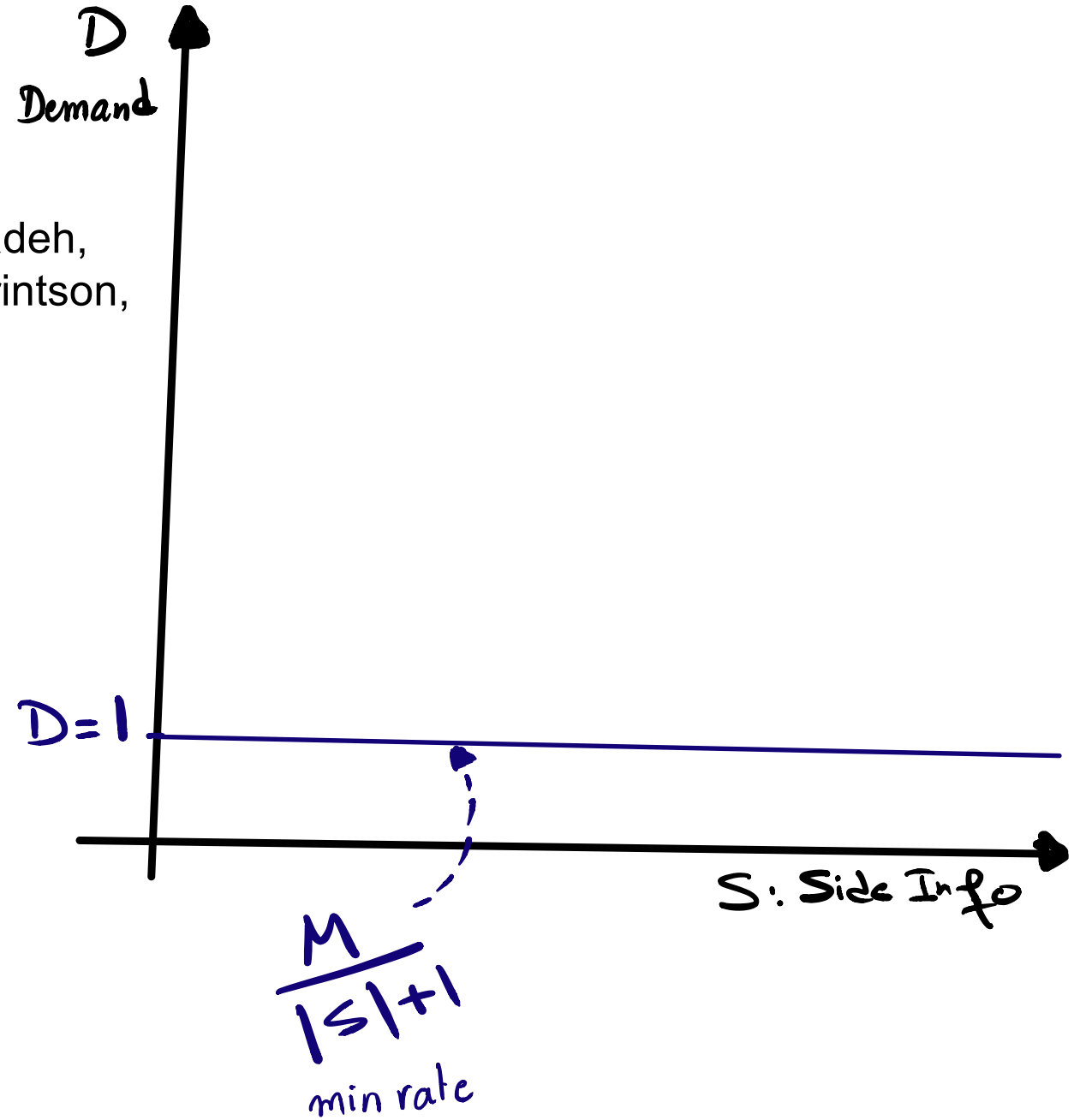
X_1, X_2, X_3, X_4

Puzzle:

Talk to me offline if you figure it out

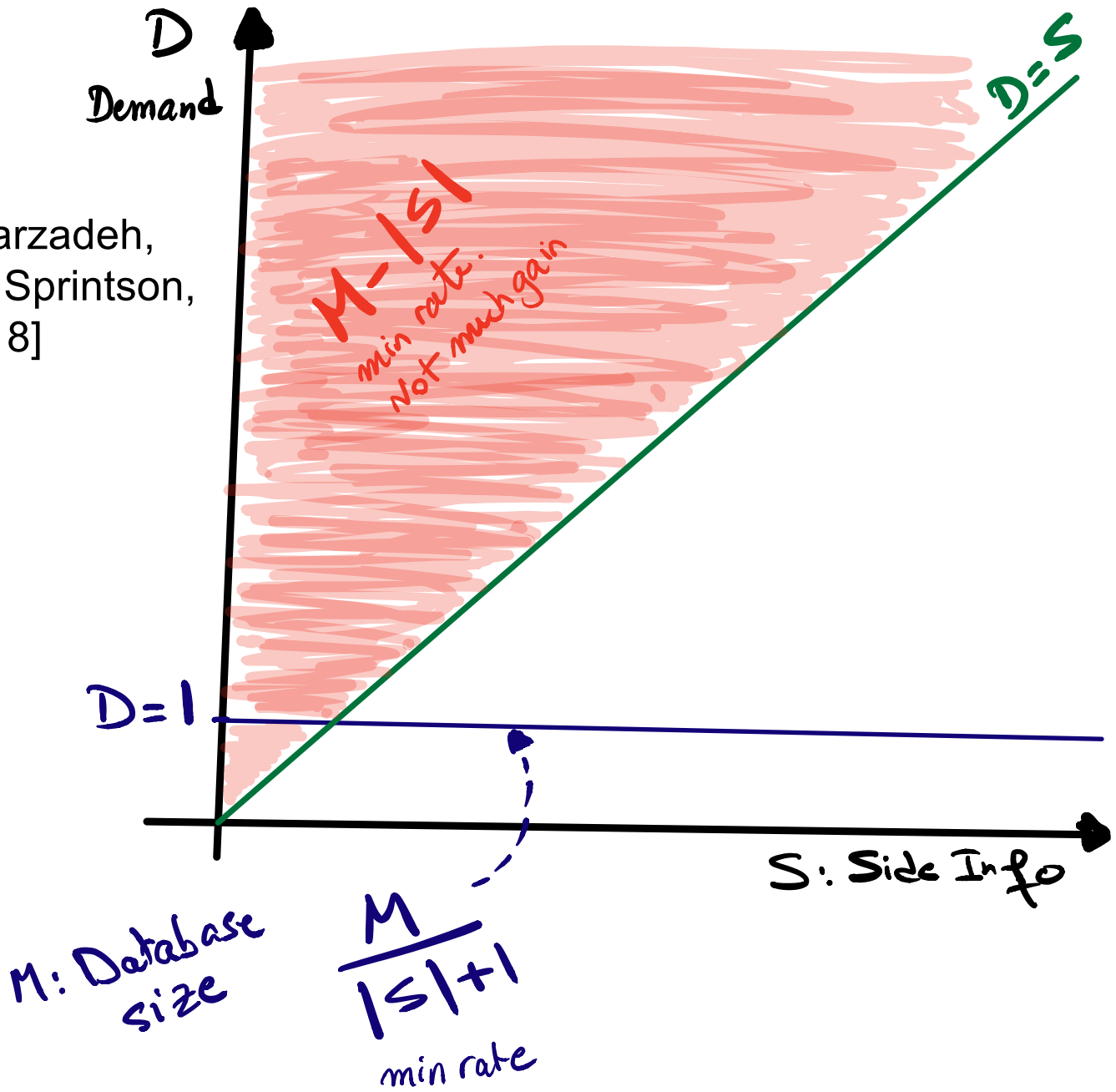
BACK TO OUR RESULTS

[kadhe, Heidarzadeh, Garcia, E.R., Sprintson, Allerton'17, '18]



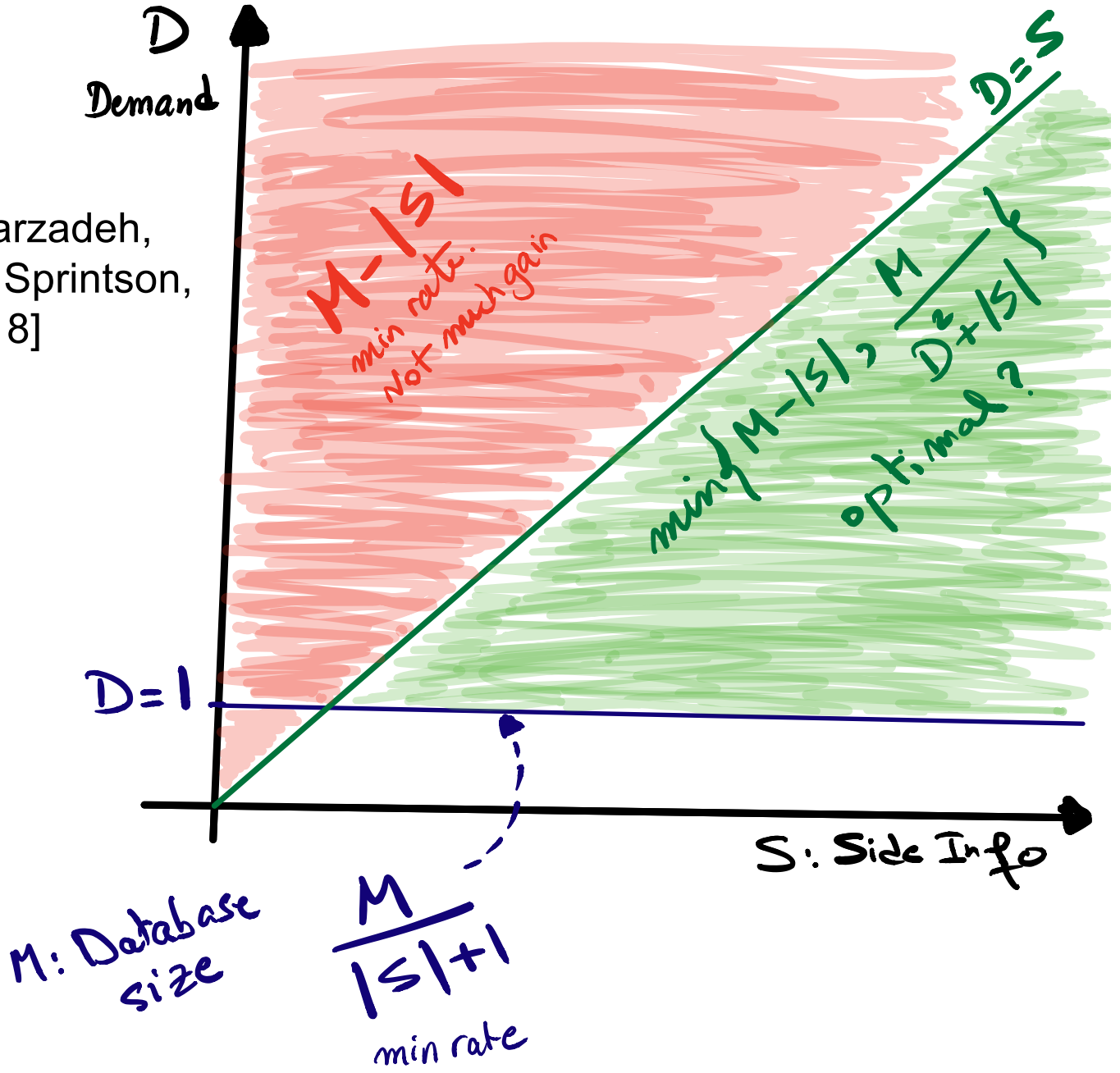
Back to Our Results

[kadhe, Heidarzadeh, Garcia, E.R., Sprintson, Allerton'17, '18]



BACK TO OUR RESULTS

[kadhe, Heidarzadeh, Garcia, E.R., Sprintson, Allerton'17, '18]



POSTERS

On/OFF Privacy with Correlated Requests

Secure Distributed Matrix Multiplication