

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

The Google logo is displayed in its standard multi-colored font: blue 'G', red 'o', yellow 'o', blue 'g', green 'l', and red 'e'.

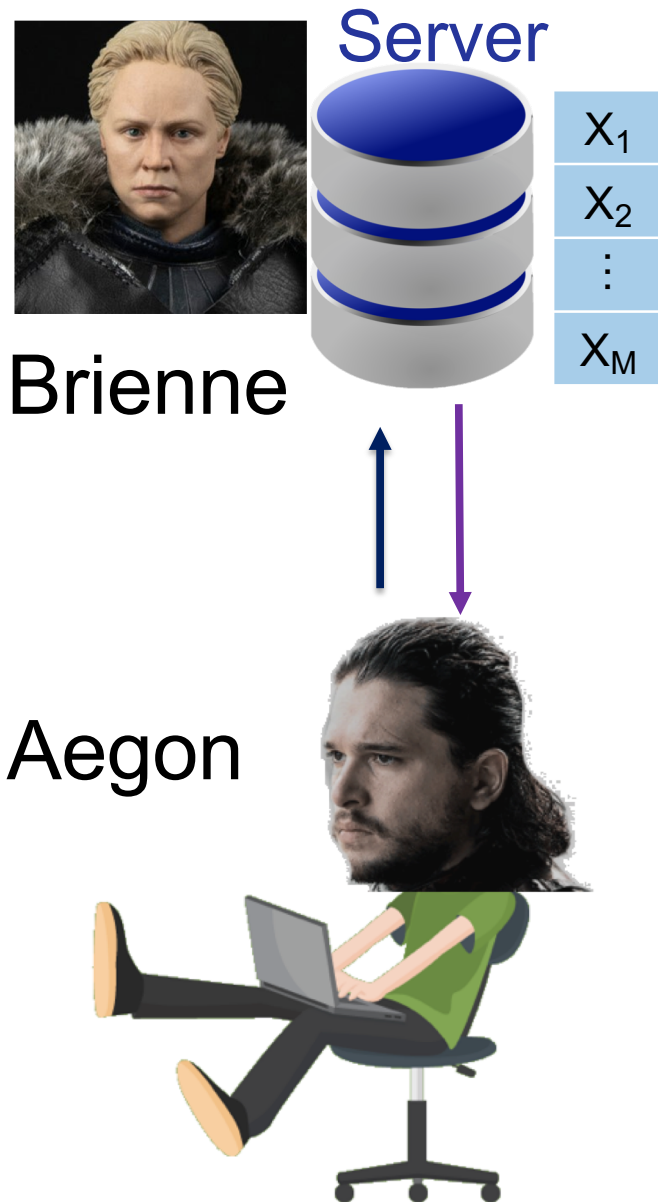
#@?f* a_+??#



Google Search

I'm Feeling Lucky

SETUP



- Aegon wants X_i 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

Communication

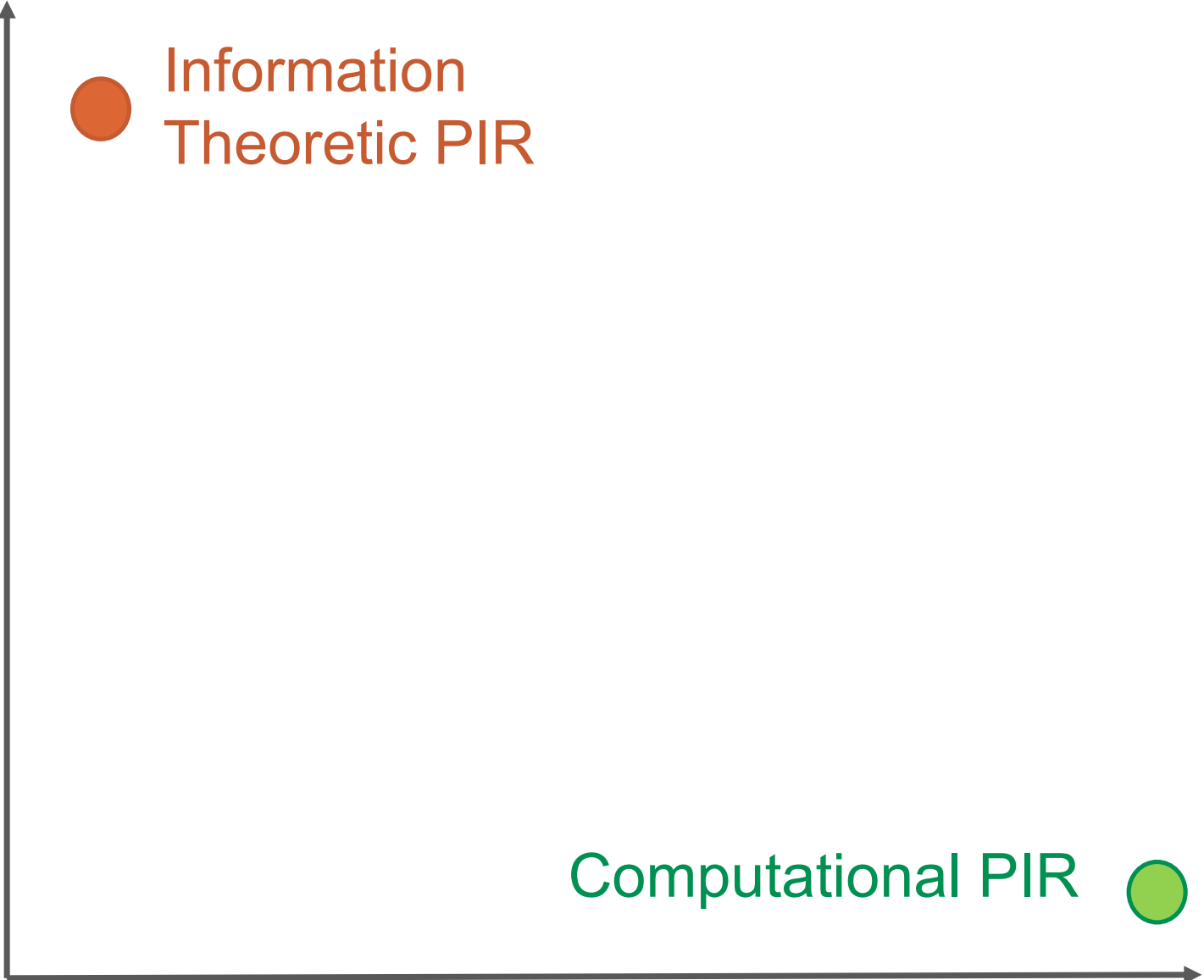
[Chor et al.
'95,...]

● Information
Theoretic PIR

[Kushilevitz
et al.
'97,...]

Computational PIR ●

Computation



SINGLE-SERVER PIR IS THE HOLY GRAIL

Communication

[Chor et al.
'95,...]

● Information
Theoretic PIR

Problem:
How to make Single-
Server PIR more
efficient?

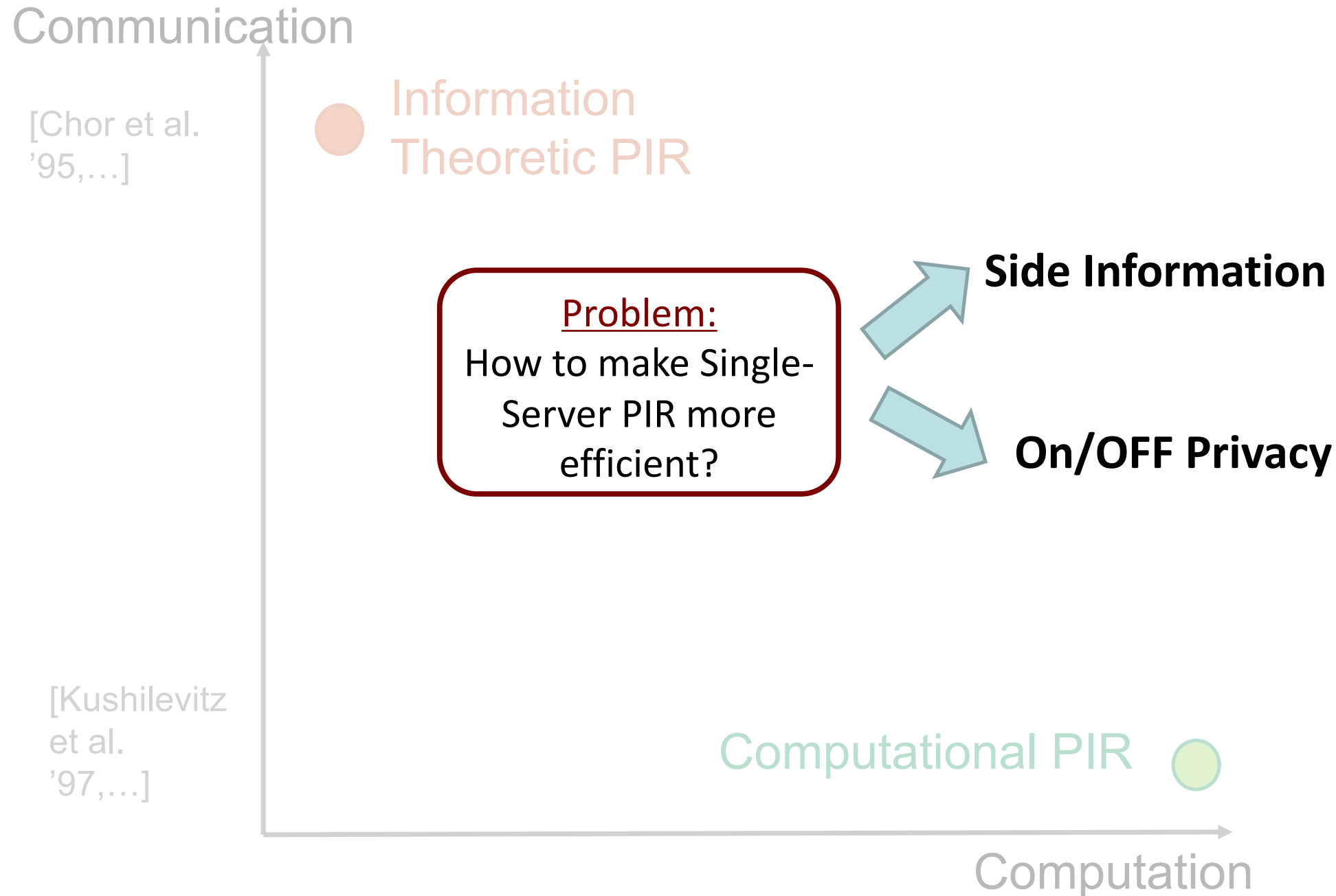
Side Information

On/OFF Privacy

[Kushilevitz
et al.
'97,...]

Computational PIR ●

Computation



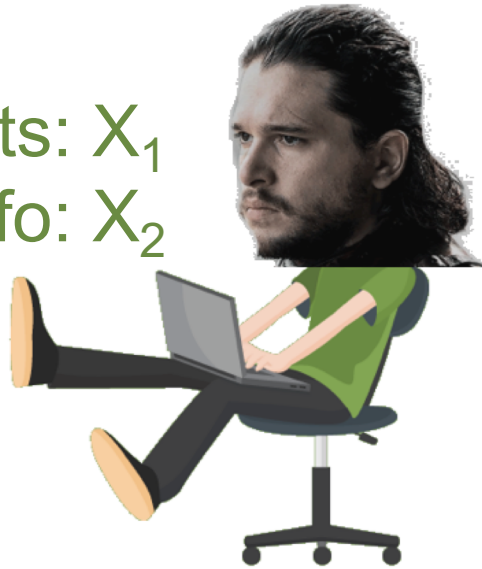
HOW CAN SIDE INFO HELP?

X_1, X_2, X_3, X_4

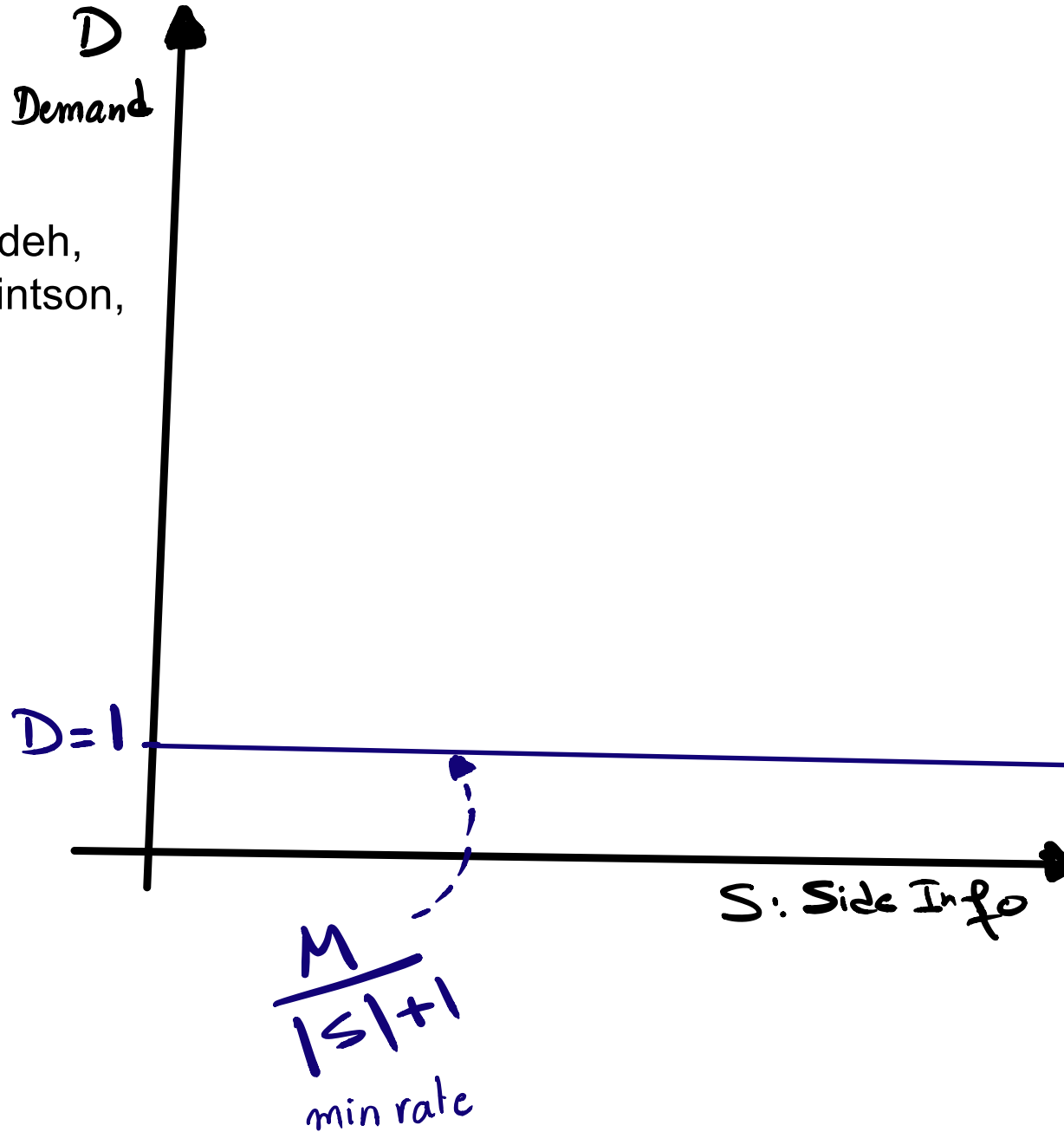


Puzzle:
Talk to me offline
if you figure it out

Wants: X_1
Has side info: X_2



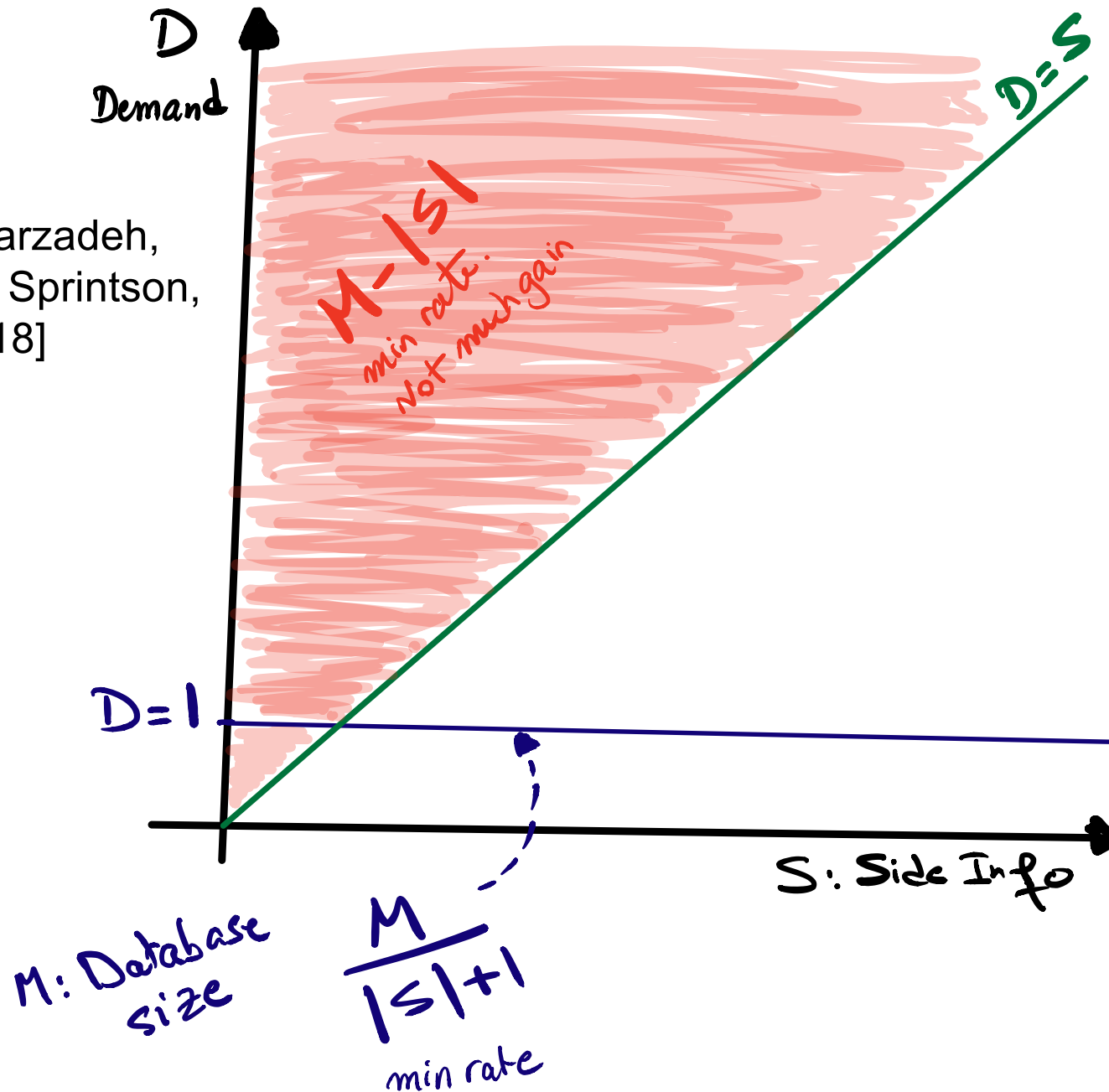
BACK TO OUR RESULTS



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

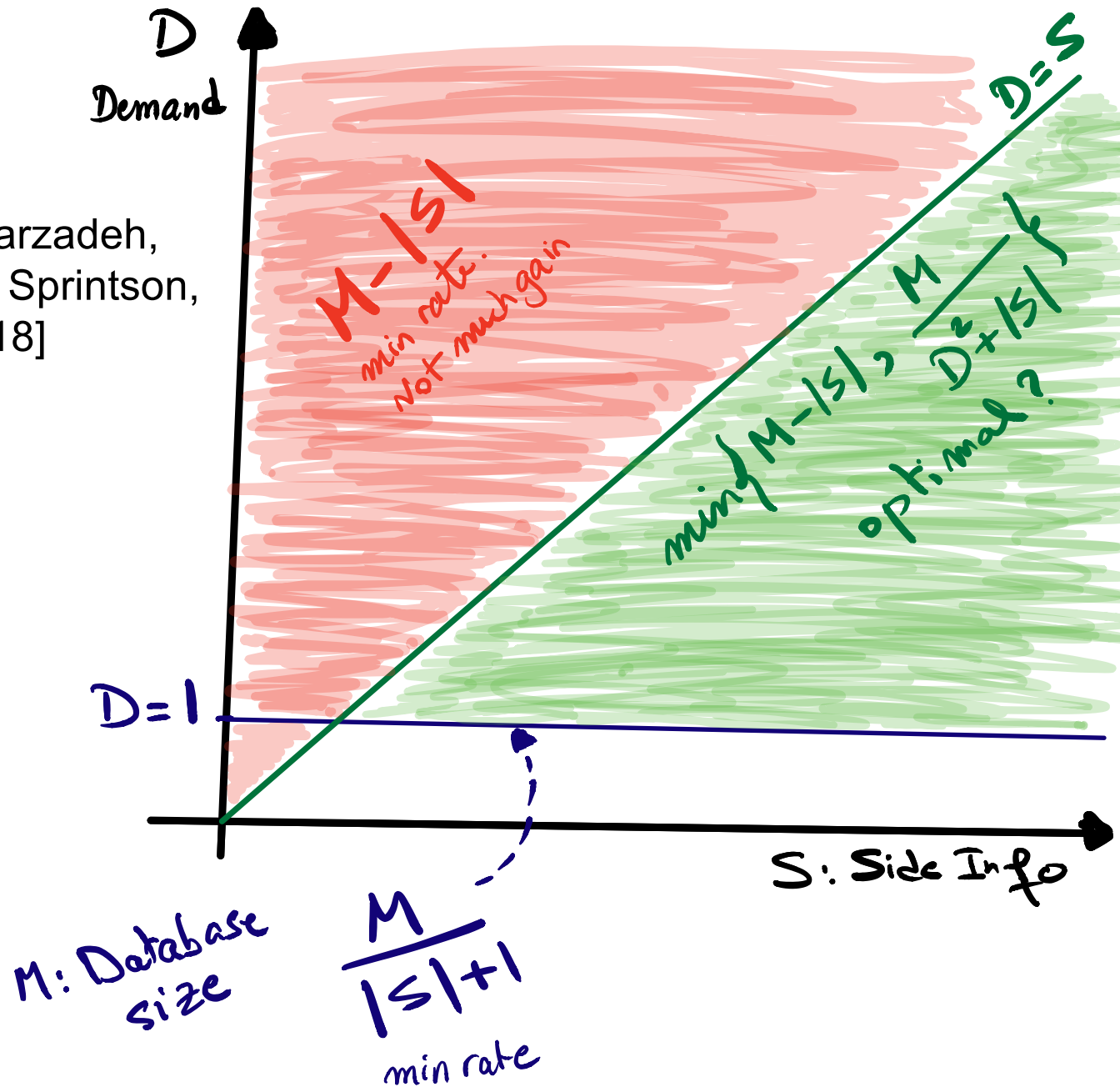
BACK TO OUR RESULTS

[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