UMass Amherst | College of Information & Computer Sciences

Heterogenous Private Information Retrieval

Hamid Mozaffari, Amir Houmansadr
University of Massachusetts Amherst

Private Information Retrieval

- Private information retrieval (PIR) enables clients to query and retrieve data from untrusted servers without the untrusted servers learning which data was retrieved.

Untrusted Data Server (medical directory)

PIR Client (patient)

Goal: Download disease information without server learning

Private Information Retrieval: Applications

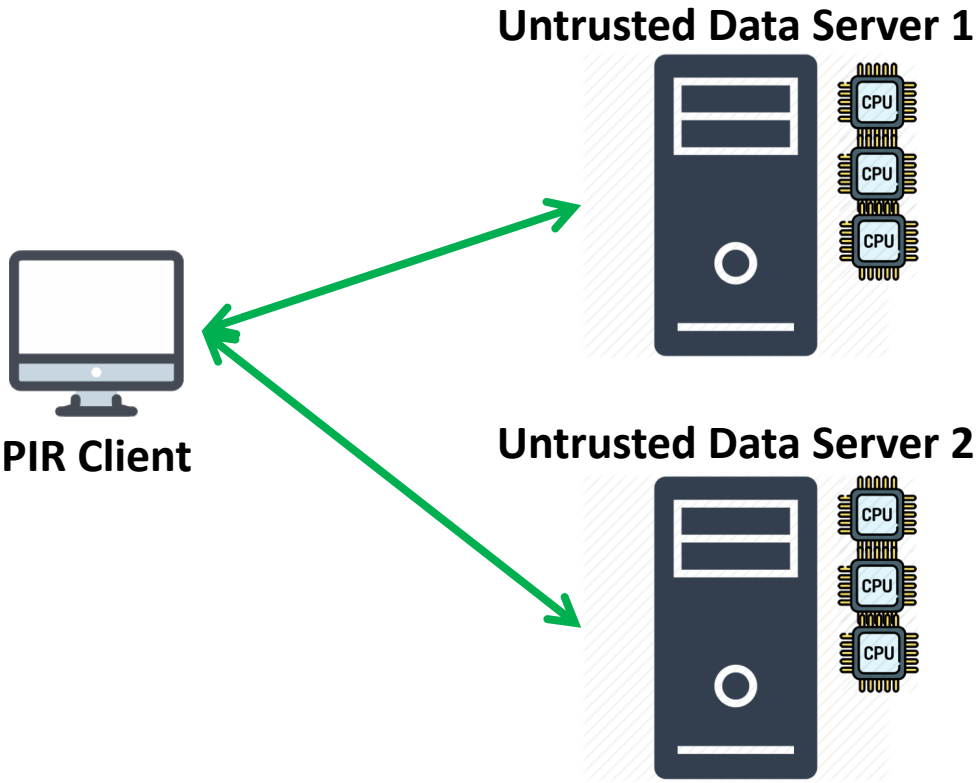
- Private Movie Streaming (Popcorn, NSDI'16)
- Private Tor Relay Information Retrieval (PIR-Tor, Usenix'11)
- Private Contact Discovery (DP5, PETS'15)
- Private Ad delivery (AdScale, CCS'16)

Private Information Retrieval: Types

- Single-Server PIR:
  - Provides computational security.
  - Requires cryptographic assumptions.
- Multi-Server PIR:
  - Usually provides information-theoretic security.
  - They need to assume that the servers do not collude.

Existing multi-server PIR protocols are homogeneous!

Impose symmetric computation and communication loads

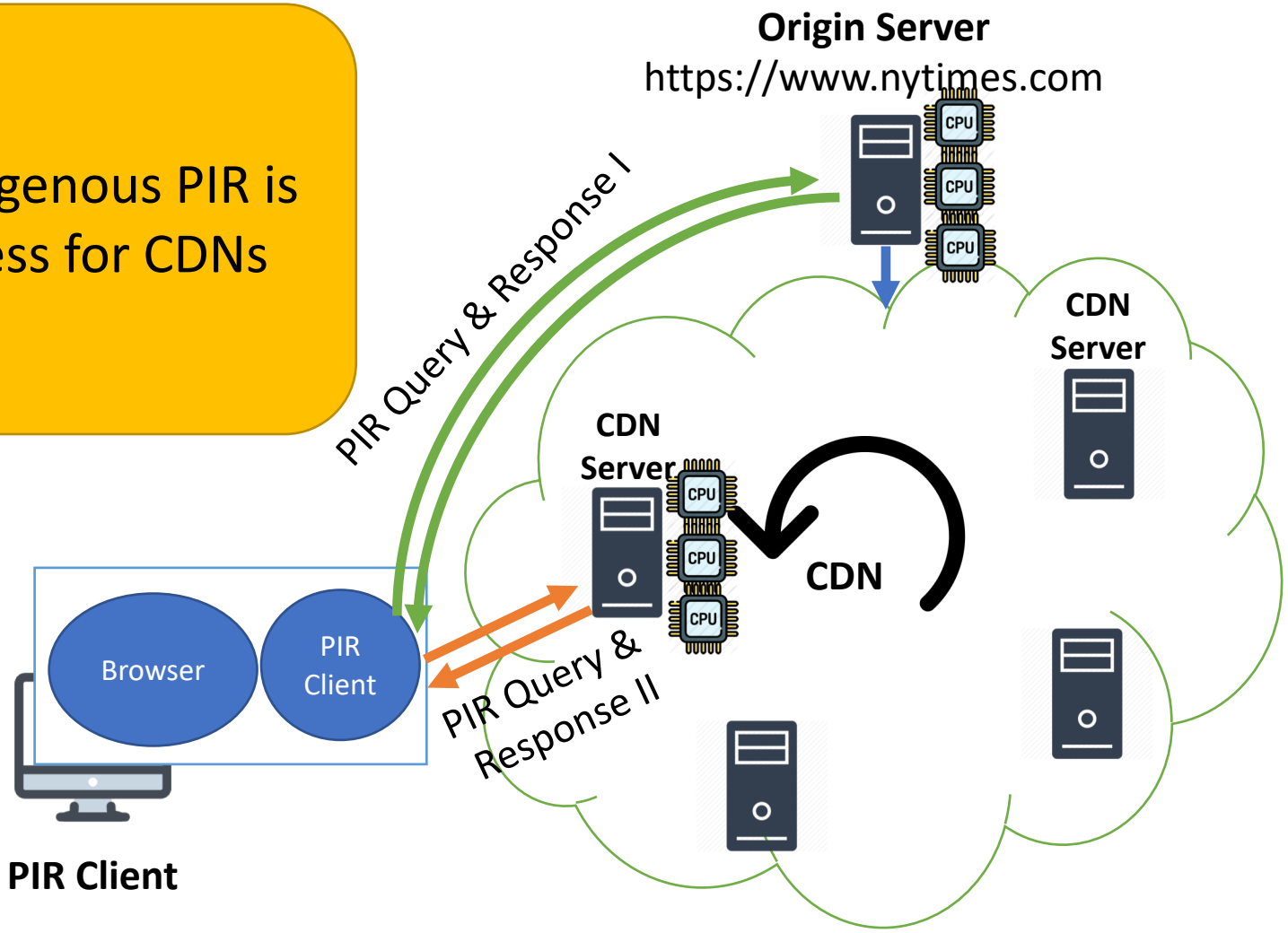


5

Homogeneous PIR protocols are not suitable for many real-world applications

Example Application: CDN Over PIR

Homogenous PIR is useless for CDNs



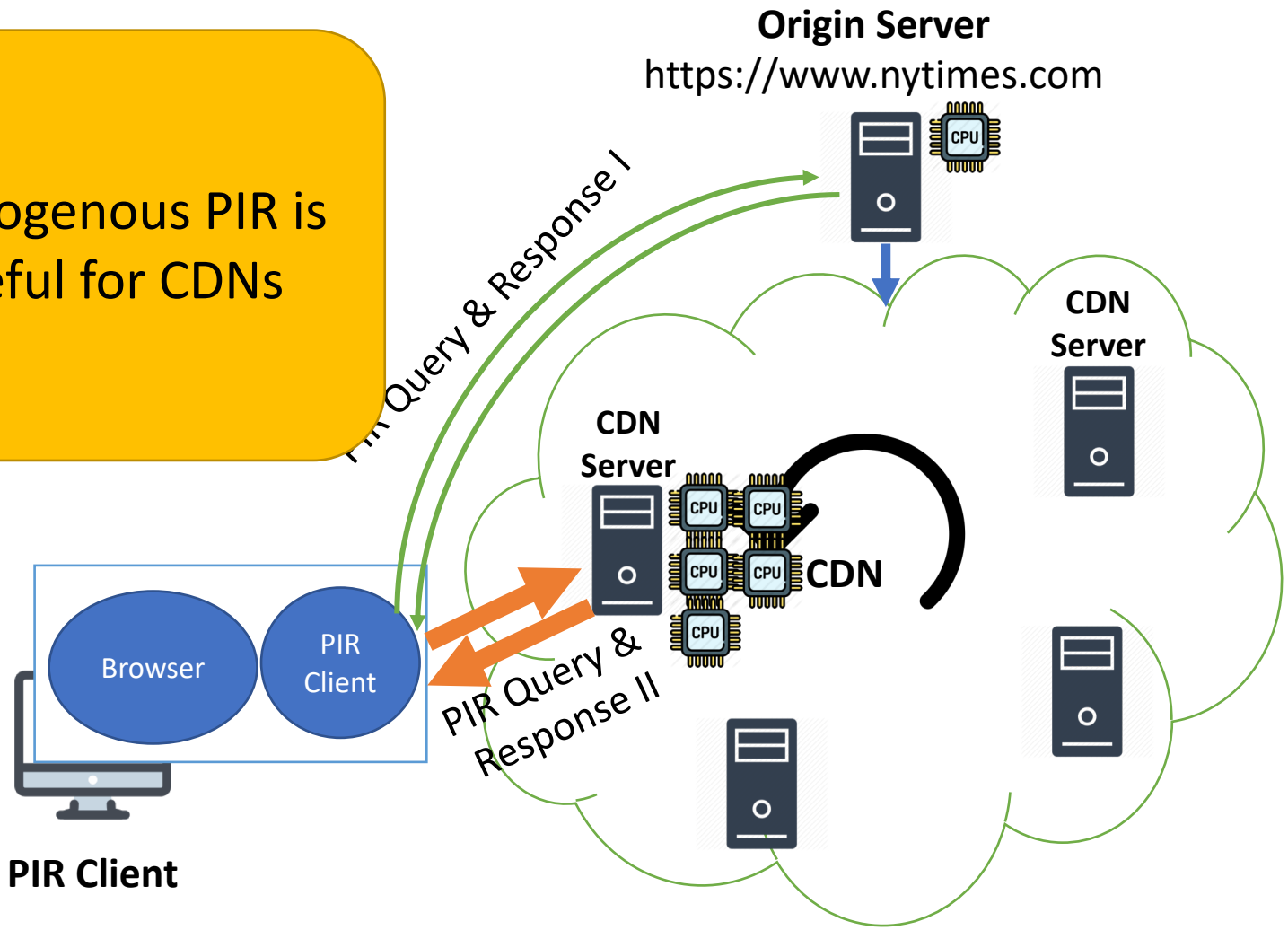
7

Homogeneous PIR protocols are not suitable for many real-world applications

Our goal: designing **heterogeneous PIR (HPIR)** protocols, which impose non-uniform computation and communication overheads.

Example Application: CDN Over PIR

Homogenous PIR is useful for CDNs

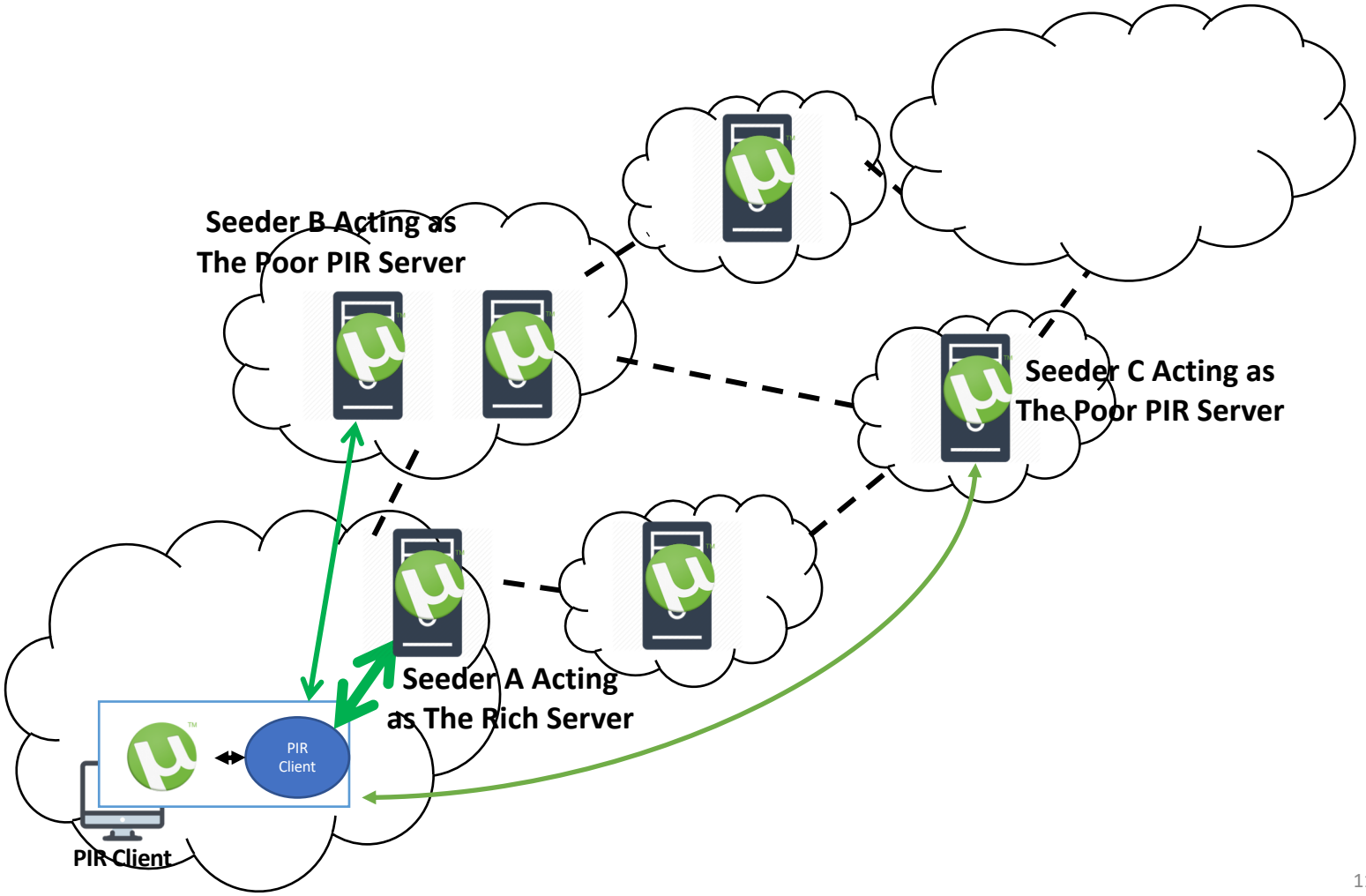


Homogeneous PIR protocols are not suitable for many real-world applications

Our goal: designing **heterogeneous PIR (HPIR)** protocols, which impose non-uniform computation and communication overheads.

HPIR can enable many potential applications for PIR as well as improve the usability of PIR in some existing applications.

Example Application: P2P Over PIR



HPIR is good but how we build it

Non-Private Information Retrieval

Client

$e_j = < 0\ 0\ \ldots 1 \ldots 0 >$

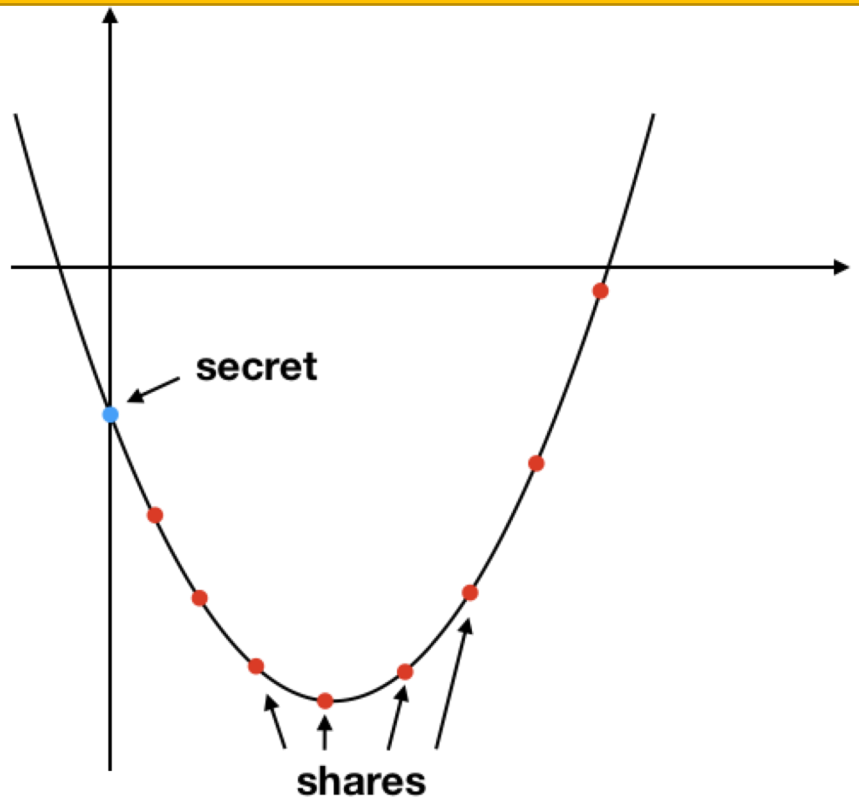
$e_j \,.D = < D_{j1}\ D_{j2}\ \ldots\ D_{js} >$

index	Word 1	…	Word c
1	$D_{1,1}$	…	$D_{1,c}$
…	…	…	…
j	$D_{j,1}$	…	$D_{j,c}$
…	…	…	…
r	$D_{r,1}$	…	$D_{r,c}$

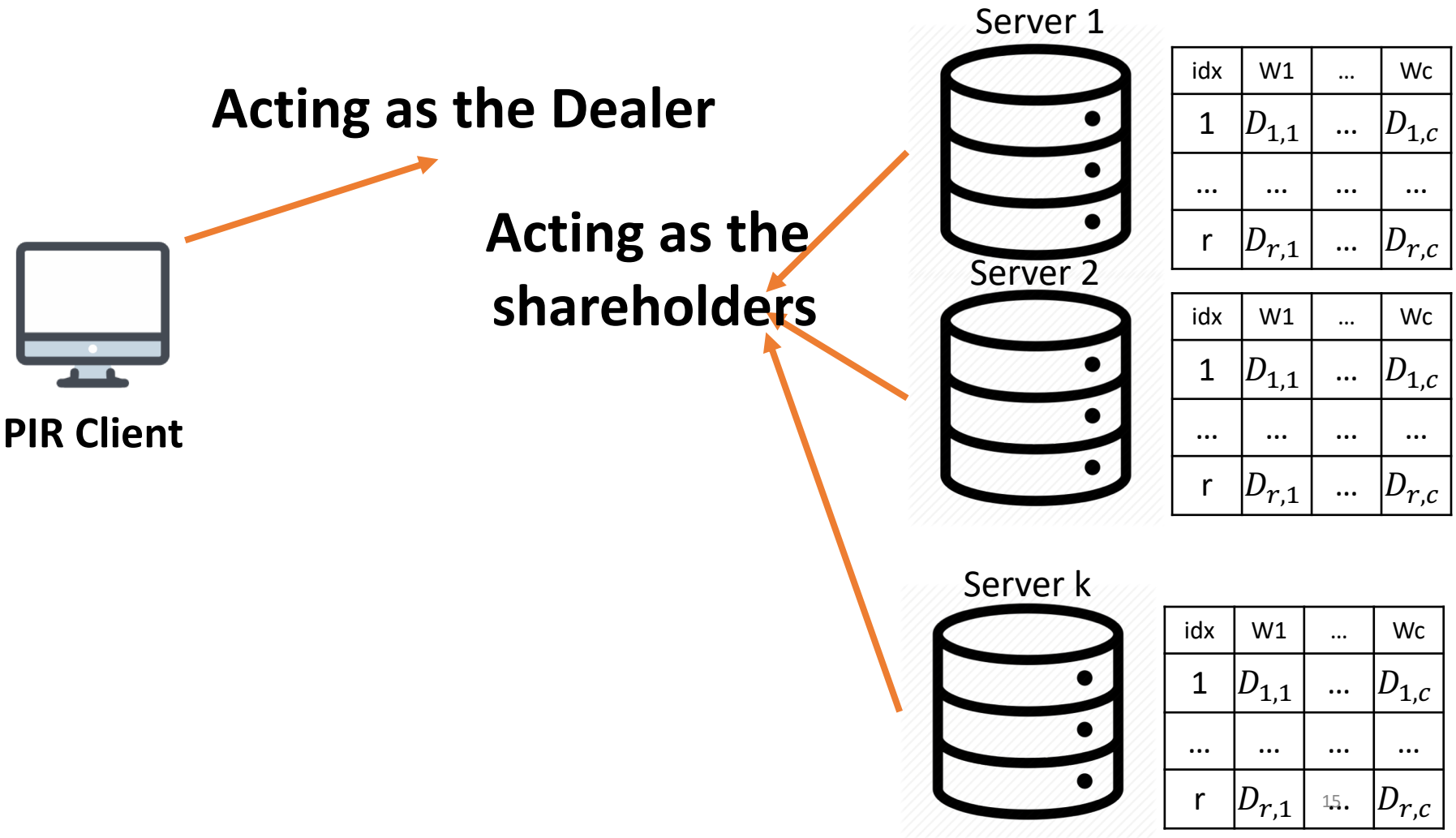
- Client is interested in j^{th} row
- Challenge: How to make e_j private?
  - Secret sharing
- Total of r rows
- Each row holds one c-words block of data
- Each word is an element of some finite field F

Shamir Secret Sharing

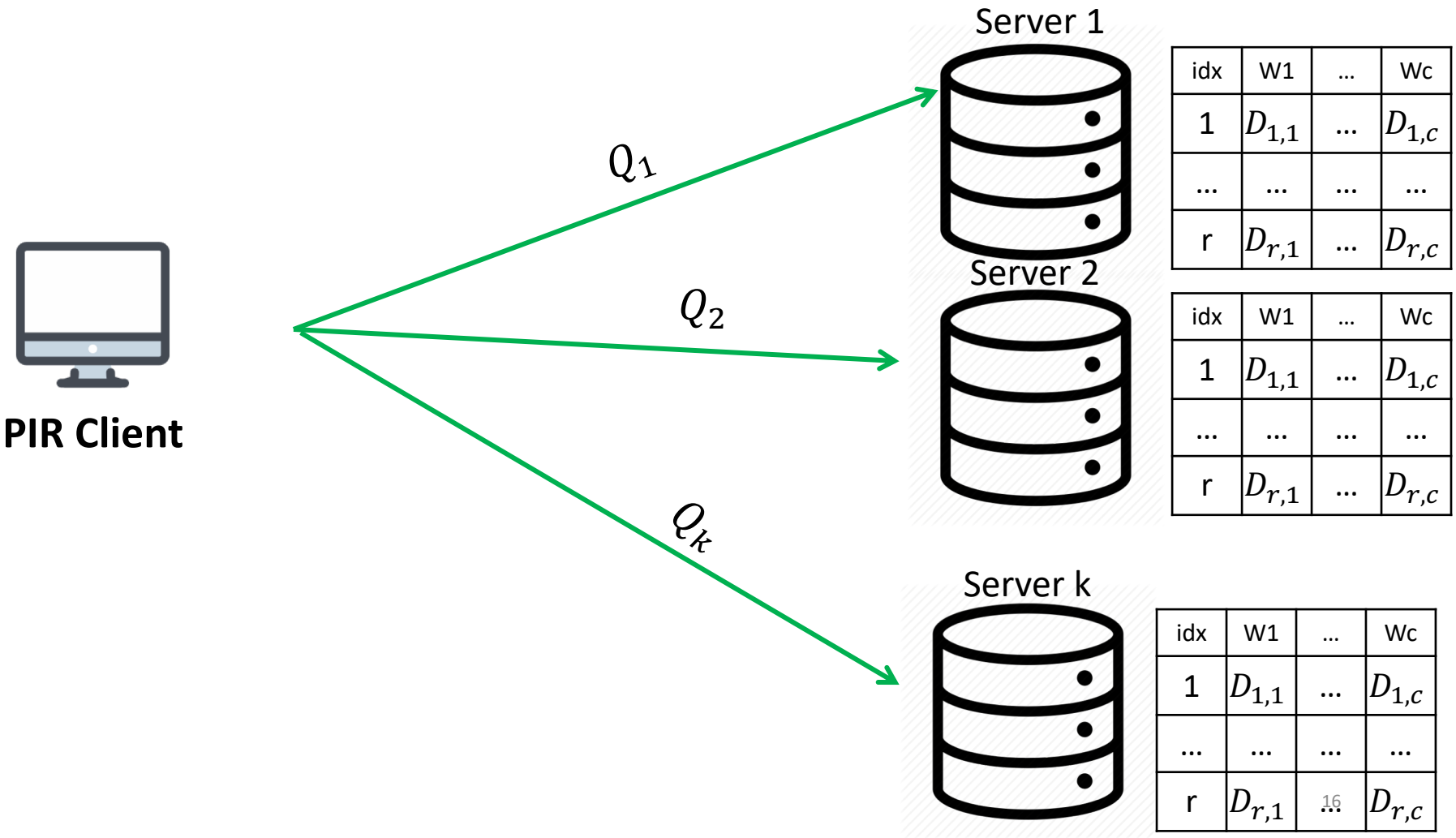
One secret s will be shared among L shareholders:



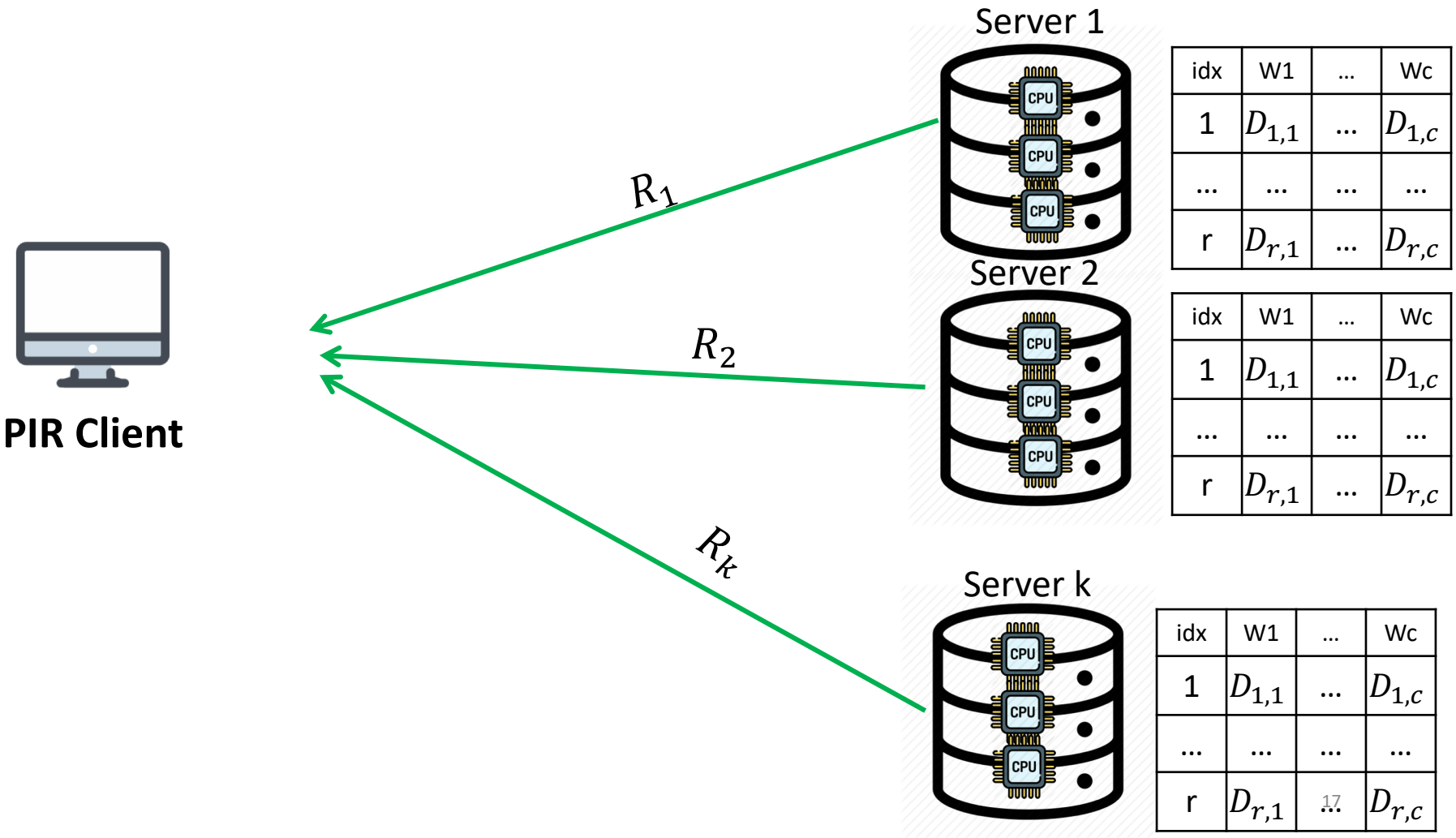
Secret Sharing in PIR [Goldberg SP'07]



Secret Sharing in PIR [Goldberg SP'07]



Secret Sharing in PIR [Goldberg SP'07]



PIR-Tailored Secret Sharing

- Features:
  - Allows sharing multiple secrets from values of {0, 1}.
  - Is not designed to enable recovering the secrets by the shareholders.
- Key ideas:
  - Increasing the degree of freedom of secrets by injecting more random numbers.
  - Attach the secrets to different prime numbers.

HPIR based on PIR-Tailored Secret Sharing

PIR Client

$e_j = < 0\ 0\ \ldots 1 \ldots 0 >$

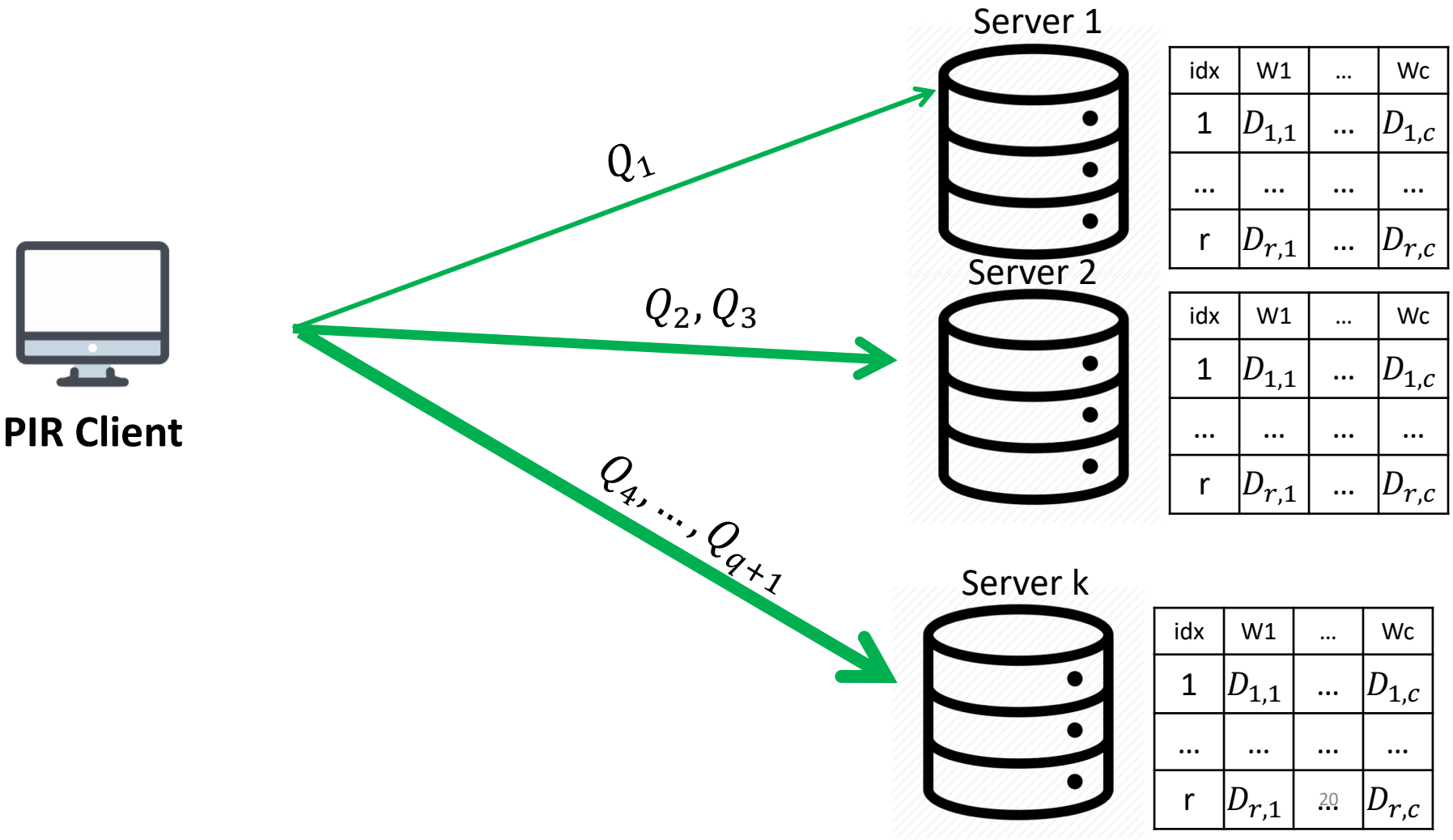
$Q_1 = < q_{1,1}\ q_{1,2} \cdots q_{1,r} >$

$Q_2 = < q_{2,1}\ q_{2,2} \cdots q_{2,r} >$

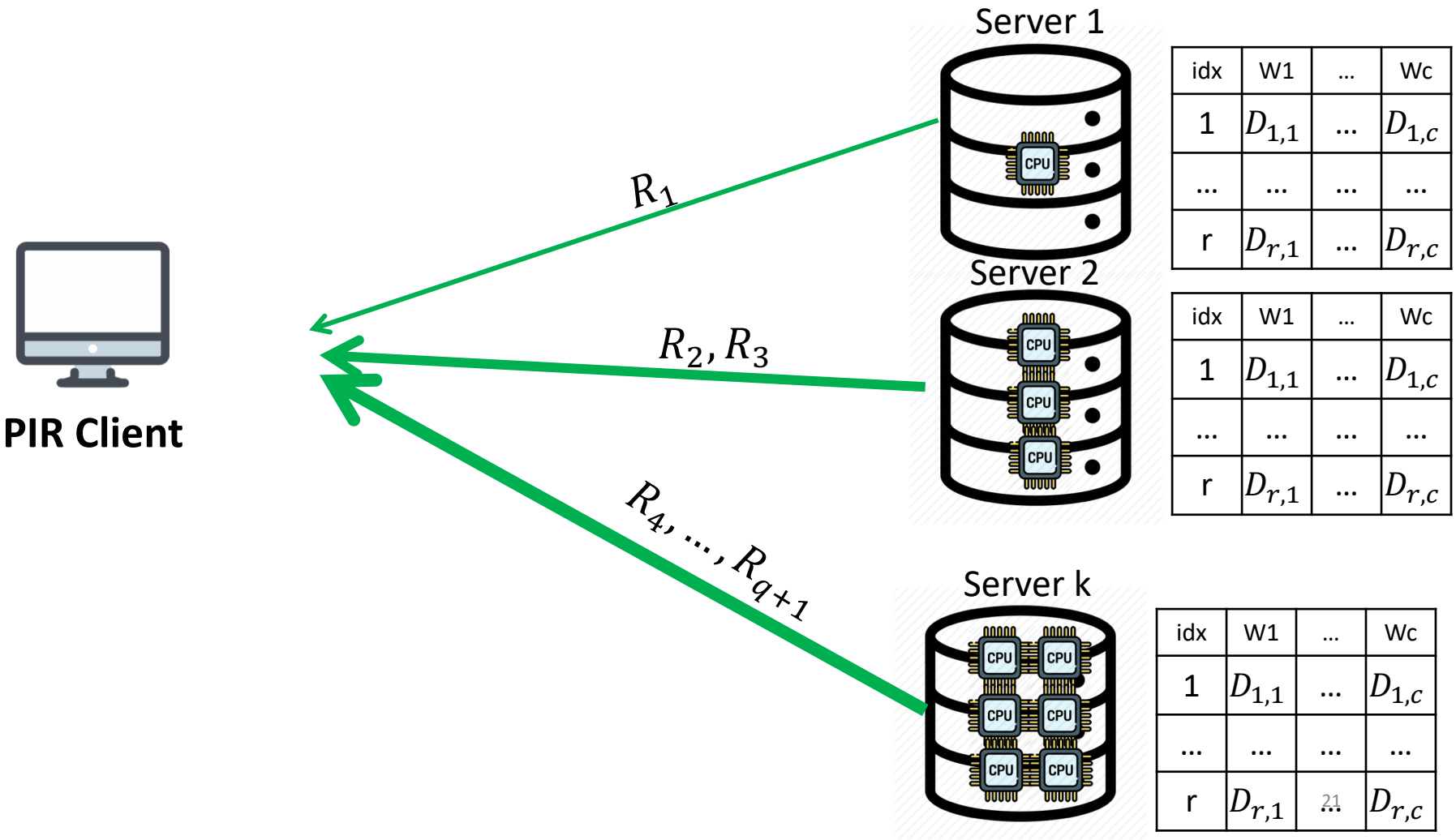
$\ldots = < \cdots >$

$Q_{q+1} = < q_{k,1}\ q_{k,2} \cdots q_{k,r} >$

HPIR based on PIR-Tailored Secret Sharing



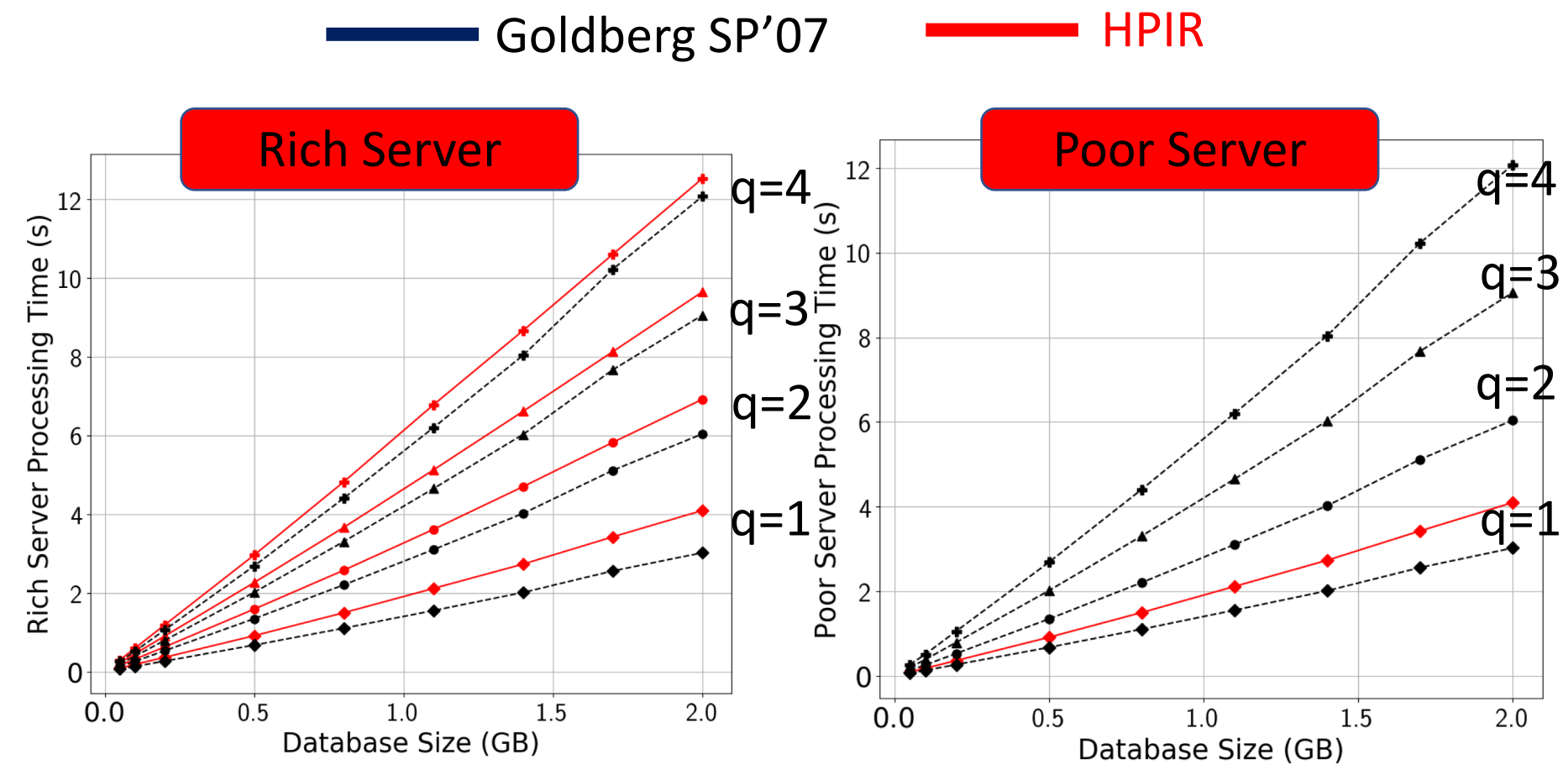
HPIR based on PIR-Tailored Secret Sharing



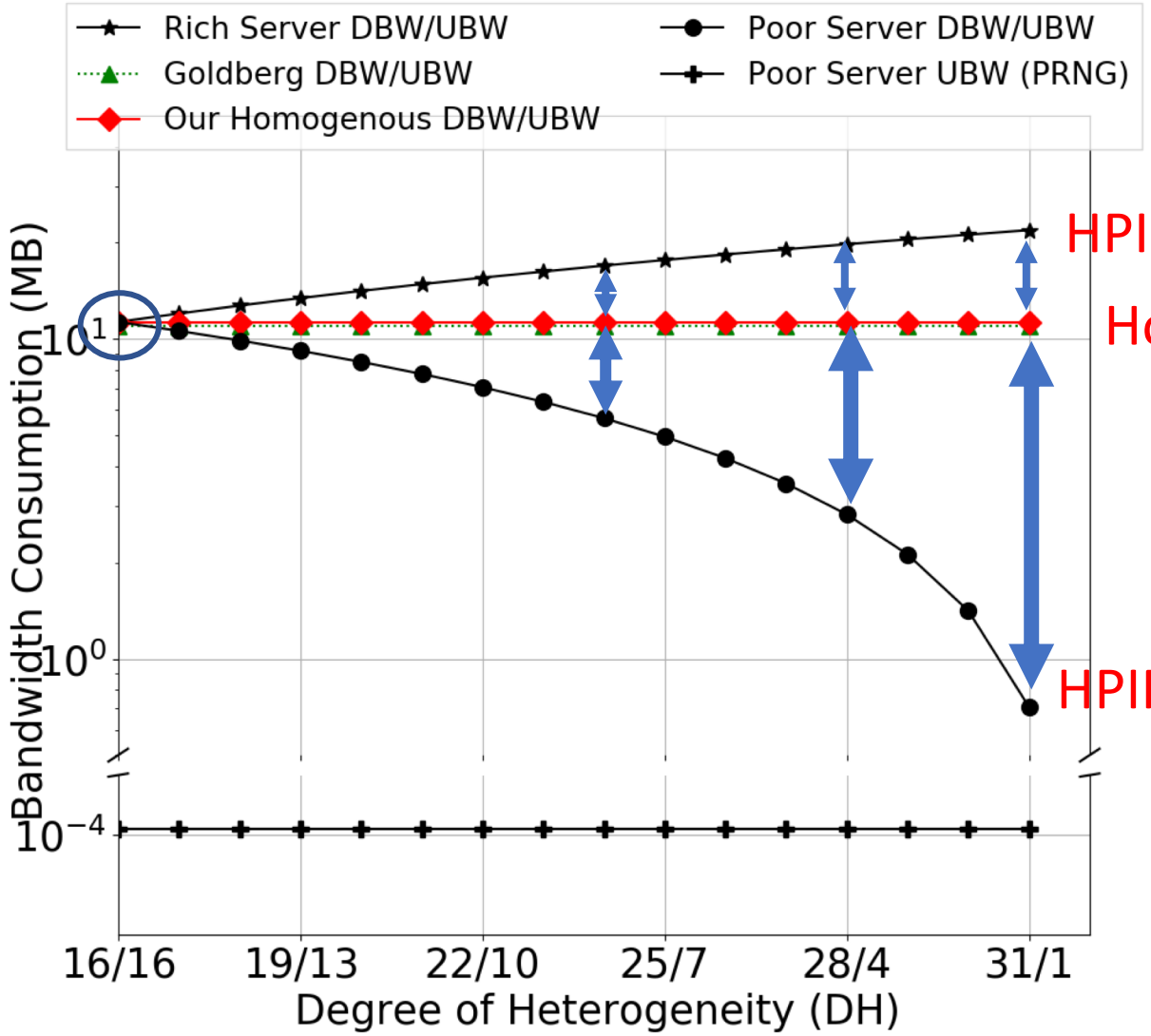
HPIR: Implementation

- Implemented in C++ in 800 lines
- Use NTL for handling big number operations
- Compatible with Percy++ PIR library
- Experiments are run on a single thread (a quad-core i7 CPU 3.6 GHz)

Server Processing Time for HPIR



The Communication Overheads



Conclusions

- All the previous multi-server PIR protocols are homogenous.
- We propose heterogenous PIR protocols
- We design and implement the first HPIR protocol
  - Using a new PIR-tailored secret sharing algorithm
- We believe HPIR will enable new applications for PIR and will improve the usability of some existing ones
- Our code is available at https://github.com/SPIN-UMass/HPIR.