The current state of Doubly-Efficient Private Information Retrieval

Simon Pohmann

Royal Holloway, University of London

July 13, 2024

Approaches to PIR

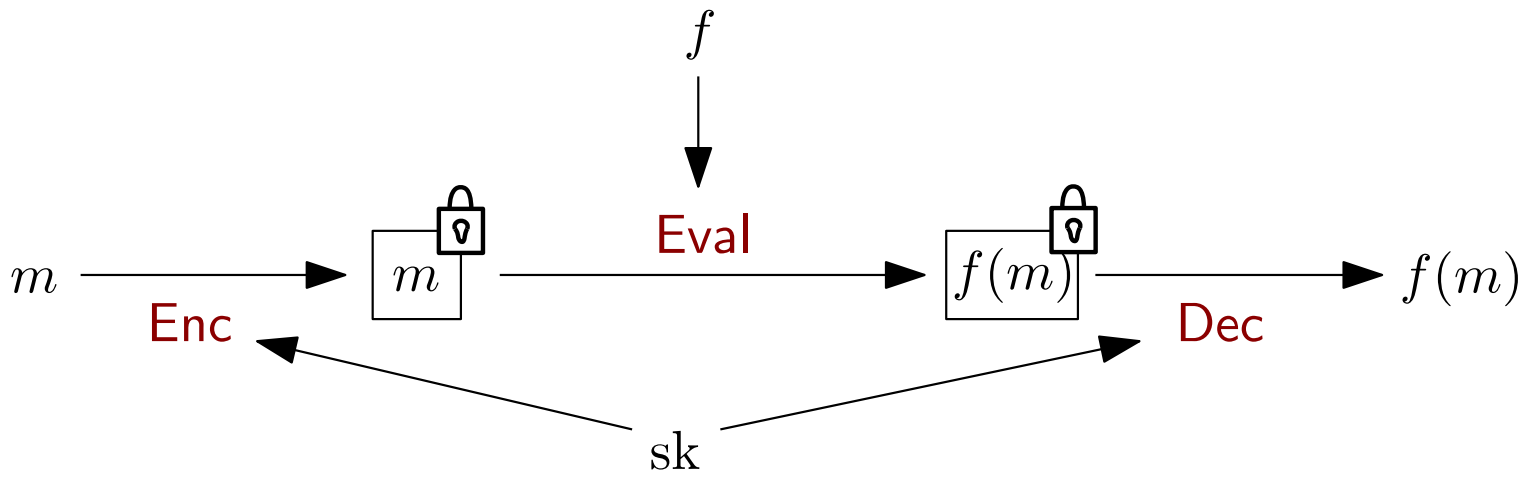
	Communication	Computation
Send the database	$O(N)$	$O(N)$
Stateless [Ang+17; MCR21; CLS24]	$\tilde{O}(1)$	$O(N)$
Stateful [CHK22; Zho+23]	$\tilde{O}(\sqrt{N})$	$\tilde{O}(\sqrt{N})$
Doubly efficient PIR [LMW23]	$\tilde{O}(1)$	$\tilde{O}(1)$

[BIM00]: Optimal without preprocessing

Requires client-dependent preprocessing $O(N)$

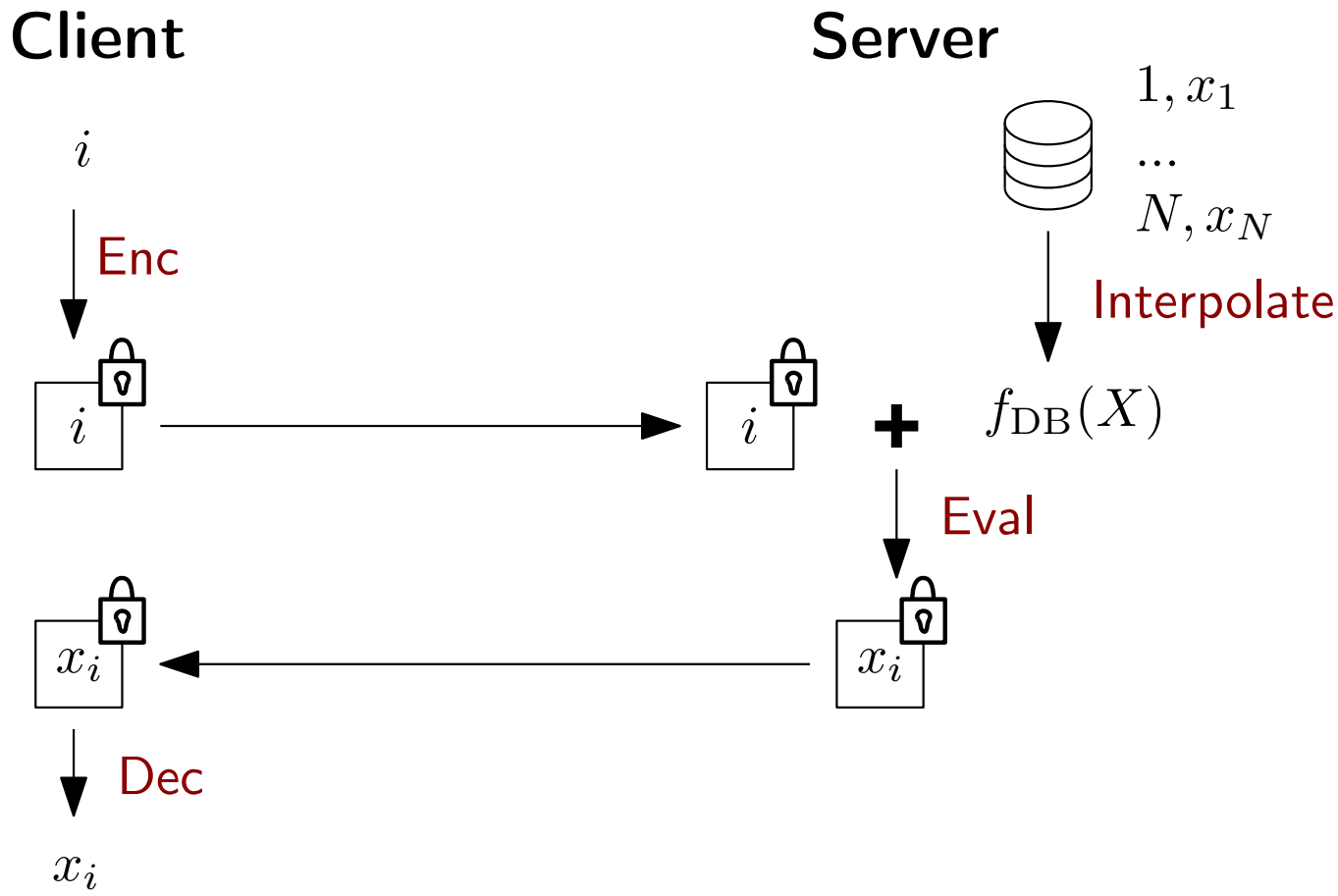
(Symmetric) Homomorphic Encryption

- Given by $(\mathrm{Enc}, \mathrm{Eval}, \mathrm{Dec})$



- Often modelled via $+$ and $\cdot$
- In this case, f is a polynomial

HE gives us PIR



Problem: Evaluating f_{DB} takes time $O(N)$

The solution

Problem: Evaluating f_{DB} takes time $O(N)$

$\Rightarrow$ Speed it up using [KU11]!

Theorem ([KU11, Thm. 2.1])

- *R finite ring*
- *$f \in R[X_1, ..., X_m]$ polynomial, degree d*

We can build a datastructure of size

$$\mathrm{poly}(m, d, \log \#R)(dm \log\log \#R)^m$$

and then use it to compute $f(x_1, ..., x_m)$ in time

$$\mathrm{poly}(d, m, \log \#R)$$

Another problem

Problem: f_{DB} is a polynomial, but not $\mathrm{Eval}(f_{\mathrm{DB}}, \cdot)$.

Definition (ASHE)

An HE scheme $(\mathrm{Enc}, \mathrm{Eval}, \mathrm{Dec})$ is called *algebraic (somewhat) homomorphic encryption*, if

$$\mathrm{Eval}(f, \mathrm{ct}_1, ..., \mathrm{ct}_m) = f(\mathrm{ct}_1, ..., \mathrm{ct}_m)$$

Requires the ciphertext space to be a ring.

$\Rightarrow$ Satsified for "old" FHE schemes, e.g. BV [BV11]

Caveat: BV has bad performance in practice

What about practice?

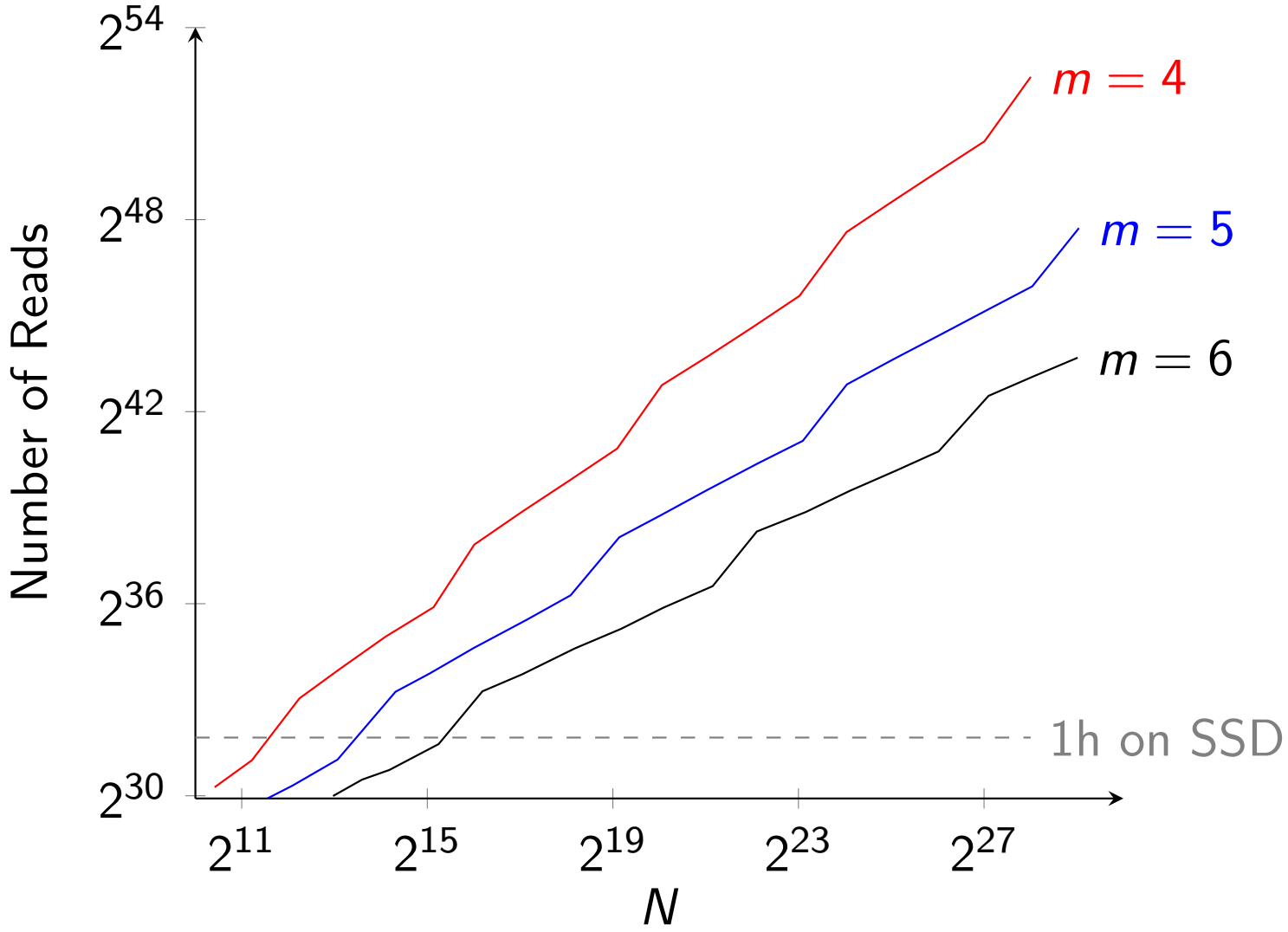
- Datastructure consists of tables

$$(x_1, ..., x_m, f(x_1, ..., x_m)) \quad \text{for all } x_1, ..., x_m \in \mathbb{F}_p$$

  for small primes p
  - Large storage p^m, depending on m
- Main bottleneck: Reading entries from those tables!
  - Scales with λ and $N^{4/m}$
- Implementation done by [Oka+24]

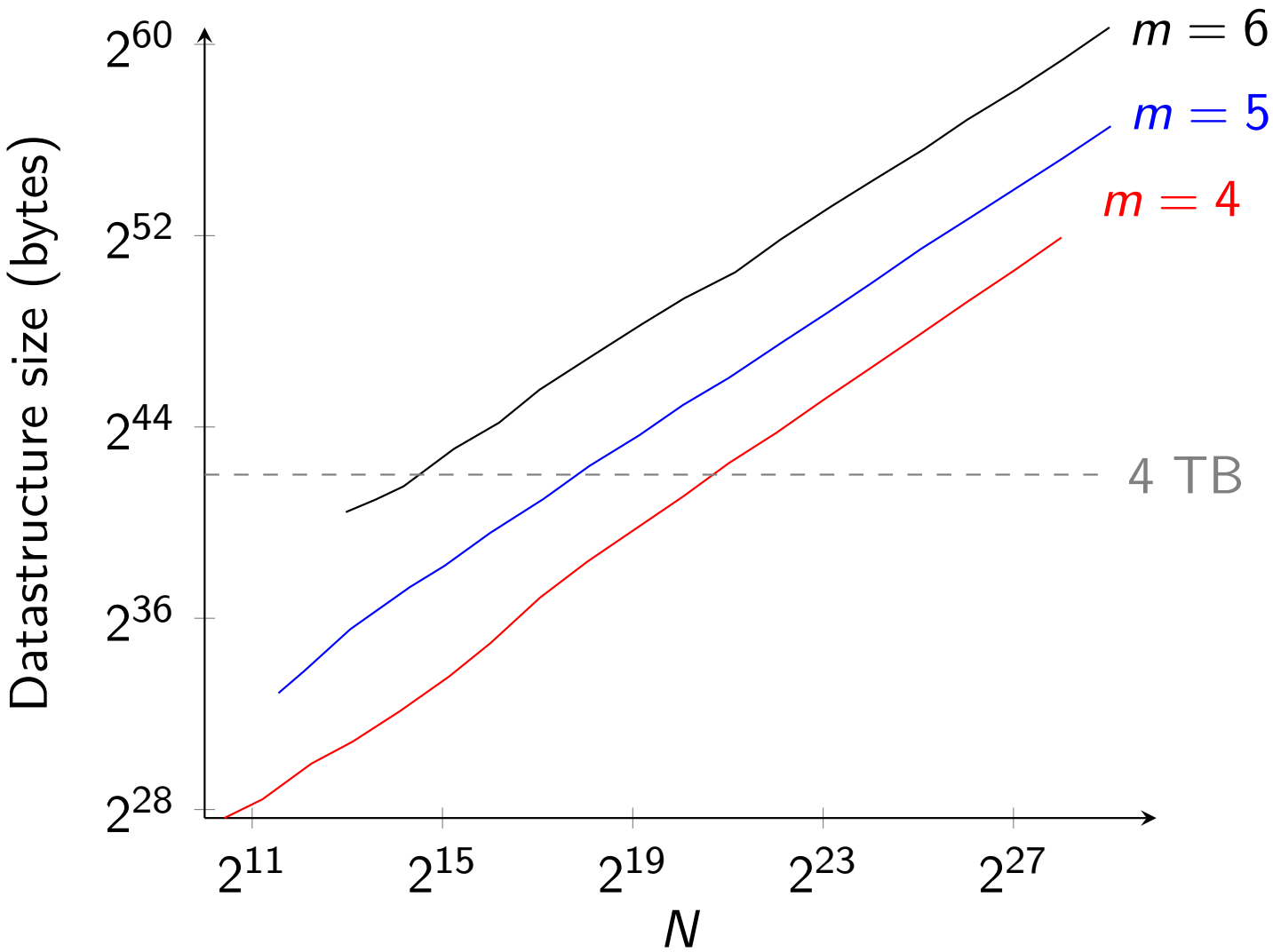
  "DEPIR is now ~~practical~~ at least implementable!"

Reading entries



SSD speed $\approx 2^{20}$ reads/sec

Datastructure size



Conclusion

- Interesting (still very theoretical) area
- Might become best choice for large databases in the future

- Improve ASHE scheme?
  - Unfortunately, NTRU-based seems not to work
- Improve datastructure?
- Expect our next paper :)

Thank you for your attention! I

[Ang+17] Sebastian Angel et al. *PIR with compressed queries and amortized query processing*. 2017.

[BIM00] Amos Beimel, Yuval Ishai, and Tal Malkin. "Reducing the servers computation in private information retrieval: PIR with preprocessing". 2000.

[BV11] Zvika Brakerski and Vinod Vaikuntanathan. "Fully Homomorphic Encryption from Ring-LWE and Security for Key Dependent Messages". Berlin, Heidelberg, 2011.

[CLS24] Leo de Castro, Kevin Lewi, and Edward Suh. "WhisPIR: Stateless Private Information Retrieval with Low Communication". In: *Cryptology ePrint Archive* (2024).

Thank you for your attention! II

[CHK22] Henry Corrigan-Gibbs, Alexandra Henzinger, and Dmitry Kogan. "Single-server private information retrieval with sublinear amortized time". 2022.

[KU11] Kiran S Kedlaya and Christopher Umans. "Fast polynomial factorization and modular composition". In: *SIAM Journal on Computing* 40.6 (2011).

[LMW23] Wei-Kai Lin, Ethan Mook, and Daniel Wichs. "Doubly Efficient Private Information Retrieval and Fully Homomorphic RAM Computation from Ring LWE". 2023.

[MCR21] Muhammad Haris Mughees, Hao Chen, and Ling Ren. "OnionPIR: Response efficient single-server PIR". 2021.

[Oka+24] Hiroki Okada et al. "Towards Practical Doubly-Efficient Private Information Retrieval". 2024.

Thank you for your attention! III

[Zho+23] Mingxun Zhou et al. *Piano: Extremely Simple, Single-Server PIR with Sublinear Server Computation*. 2023.