Differentially Private Oblivious RAM

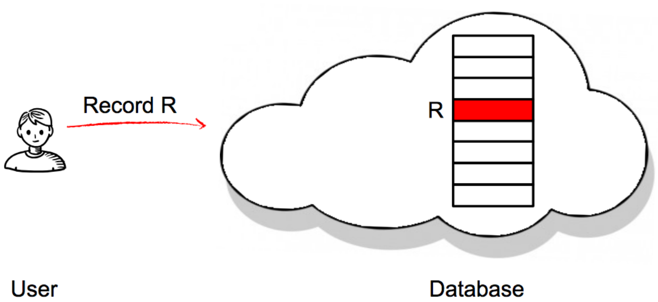
Sameer Wagh*, Paul Cuff†, Prateek Mittal*

July 24, 2019

*Princeton University, †Renaissance Technologies

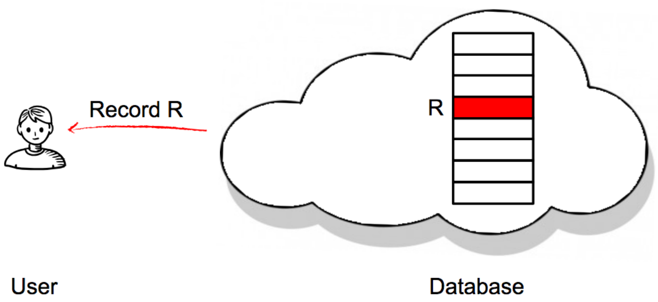
Introduction: Oblivious RAM

Access data **privately** from **private** database.

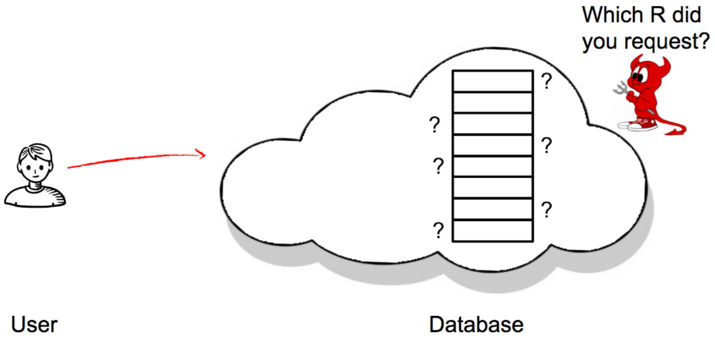


Introduction: Oblivious RAM

User receives record R

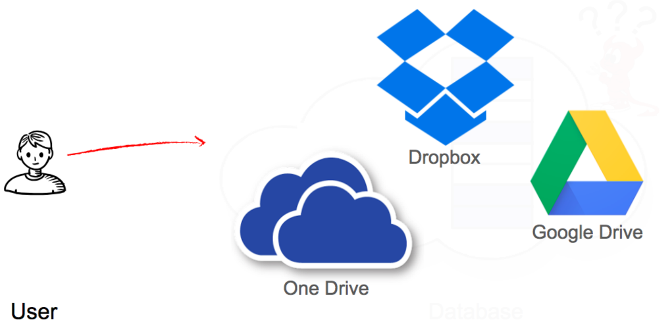


Obliviousness: Adversary should not know R



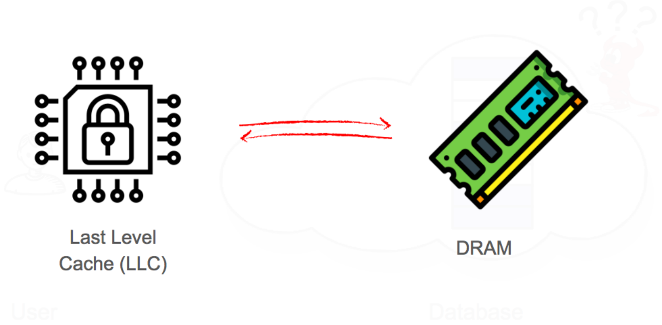
ORAM Application I

Client-server environments

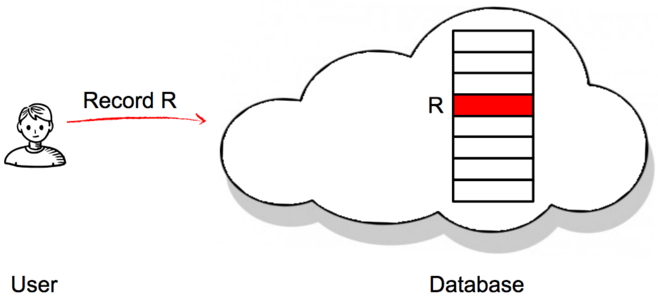


ORAM Application II

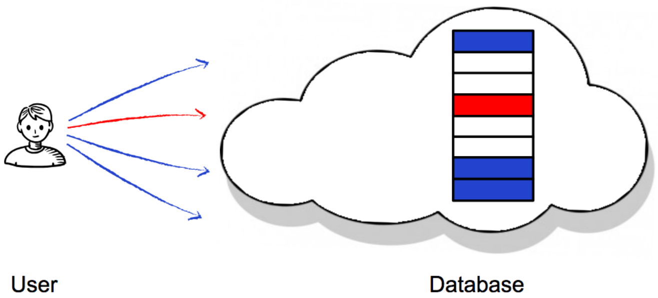
Trusted Execution Environments such as SGX-based enclaves



The Problem?

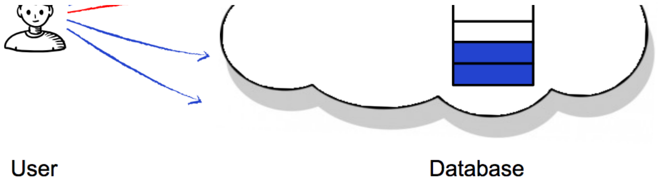


The Problem?



Overheads

- Logarithmic bandwidth overhead ($\geq 100\times$)
- Logarithmic storage overhead



Key Insight

Key Insight

Can we improve performance by relaxing privacy?

Key Insight: Improve Performance by Relaxing Privacy

- Statistically private ORAM
  - Better performance at the cost of privacy loss
  - Challenge: Can we provide rigorous guarantees?

Key Insight: Improve Performance by Relaxing Privacy

- Statistically private ORAM
  - Better performance at the cost of privacy loss
  - Challenge: Can we provide rigorous guarantees?

- Efficiency
  - Reduce performance overheads – bandwidth, local storage
  - Achieve privacy proportional to application resources

Key Insight: Improve Performance by Relaxing Privacy

Differential Privacy

- Formalize Differentially Private ORAM
- Introduce Root ORAM

Key Insight: Improve Performance by Relaxing Privacy

Differential Privacy

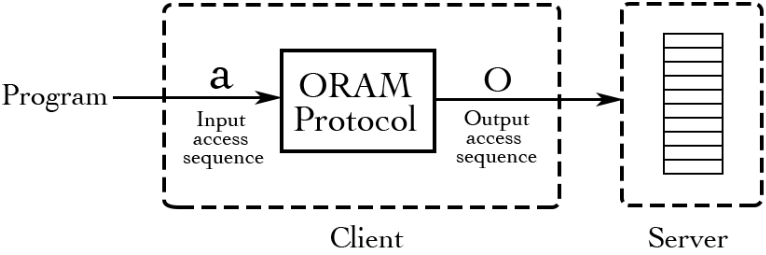
- Formalize Differentially Private ORAM
- Introduce Root ORAM

Root ORAM

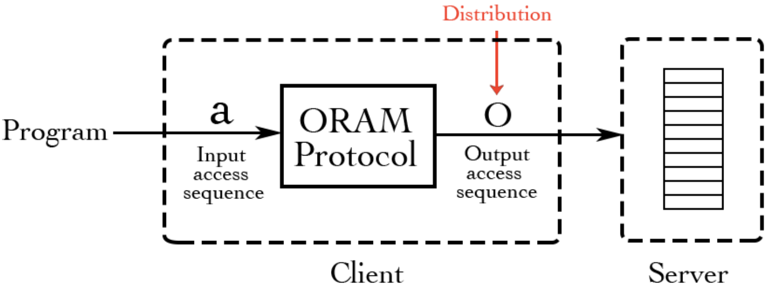
- Theoretical Results
- Empirical Results
- Private Information Retrieval

Differentially Private Oblivious RAM

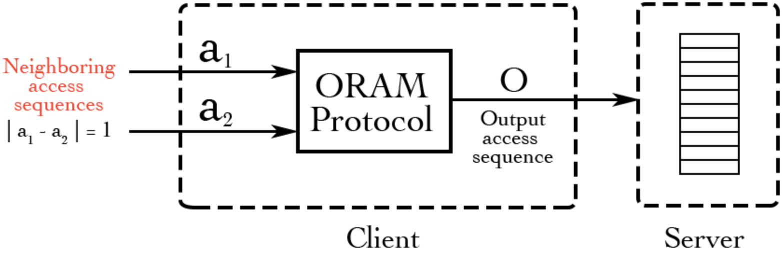
DP-ORAM Intuition



DP-ORAM Intuition

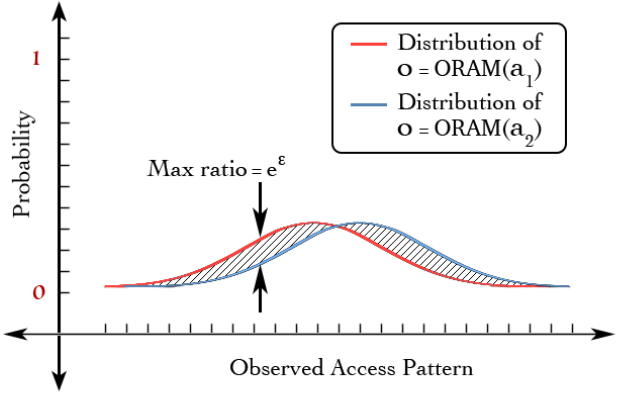


DP-ORAM Intuition



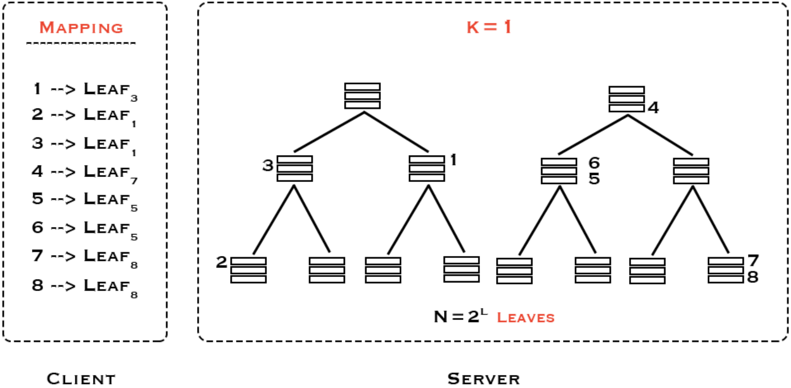
Statistical closeness - Differential Privacy

$$Pr[\texttt{ORAM}(\mathbf{a_1}) \in S] \leq e^{\epsilon} Pr[\texttt{ORAM}(\mathbf{a_2}) \in S] + \delta$$

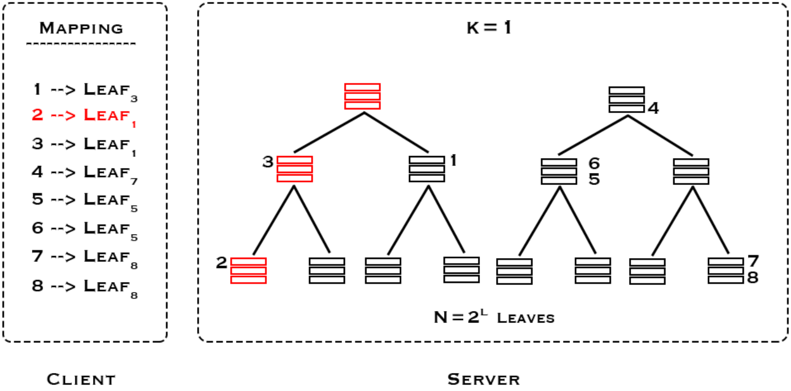


Protocol Construction

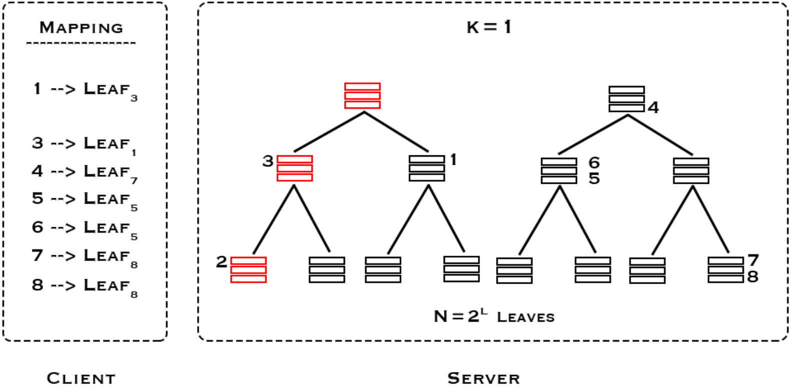
Root ORAM: Storage



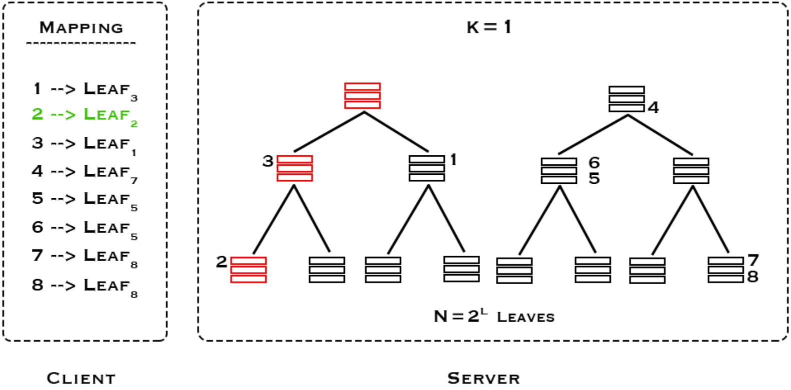
Root ORAM: Invariant



Root ORAM: Updated mapping



Root ORAM: Updated mapping



Root ORAM: Updated mapping

Key Insight

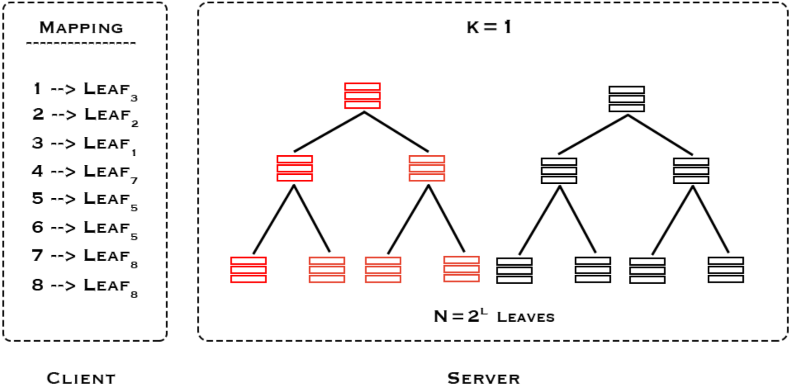
- Uniform mapping $\Rightarrow$ Conventional Security

Root ORAM: Updated mapping

Key Insight

- Uniform mapping $\Rightarrow$ Conventional Security
- Non-uniform mapping $\Rightarrow$ DP-ORAM Security

Root ORAM: Updated mapping

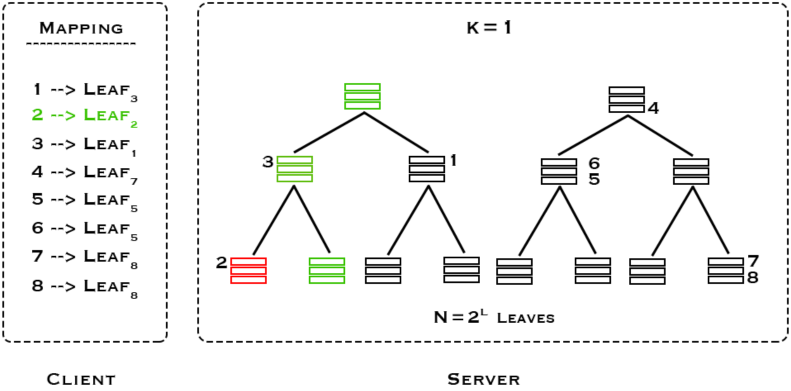


Root ORAM: Non-Uniform mapping

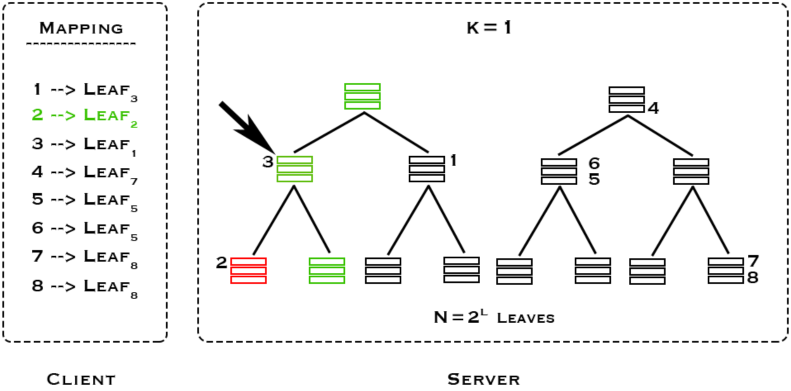
Impact

- Lower average placement $\Rightarrow$ Improved performance
- Privacy loss

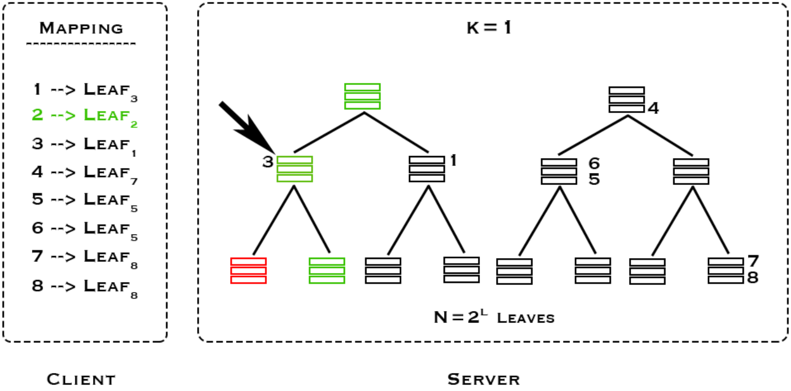
Root ORAM: Write back



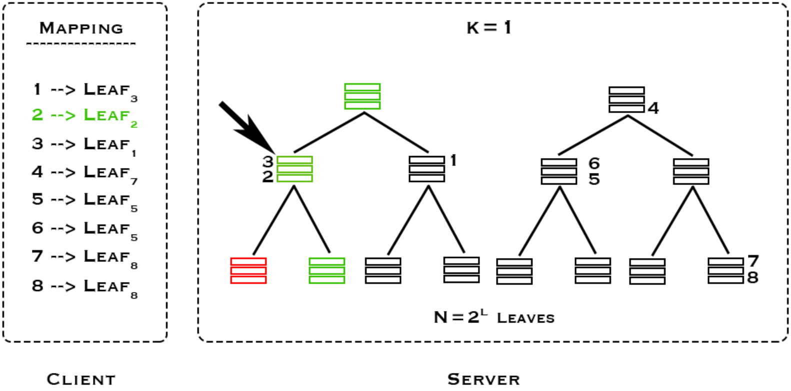
Root ORAM: Lowest Common Intersection



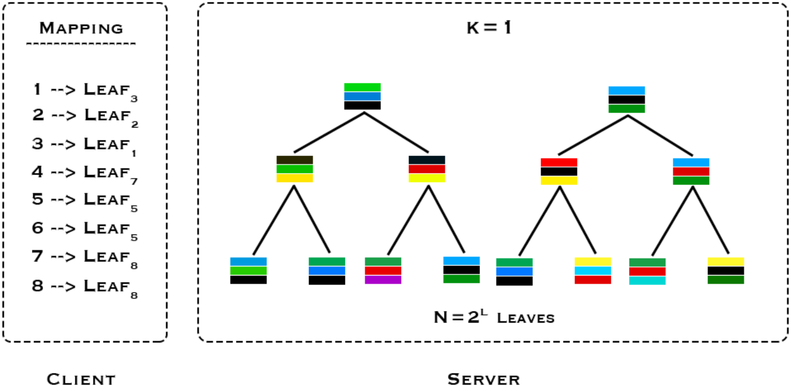
Root ORAM: Lowest Common Intersection



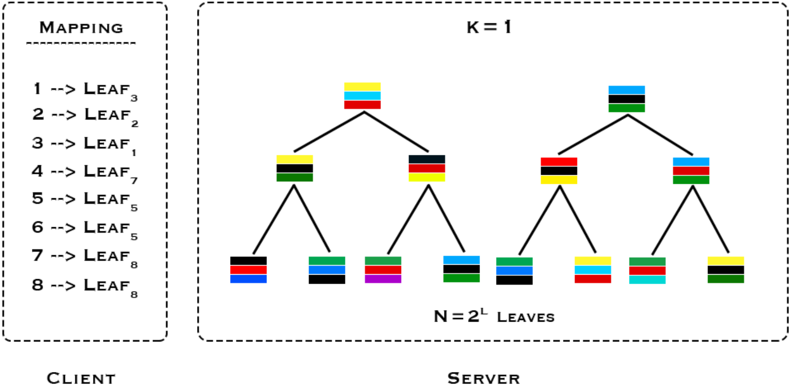
Root ORAM: Lowest Common Intersection



Database view before access



Database view after access



Results

Security Result: Root ORAM is DP-ORAM

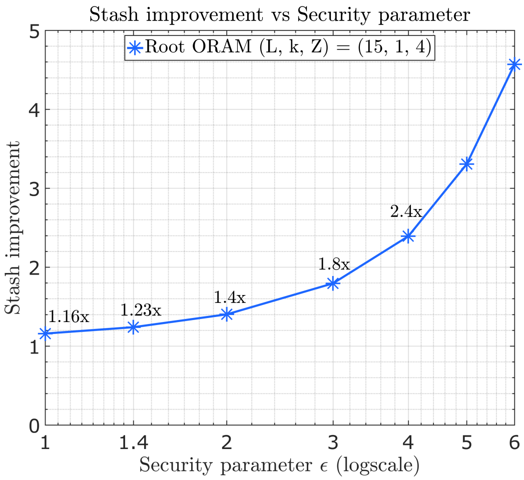
Differentially Private ORAM Protocol

The Root ORAM protocol with parameters k, p is (ϵ, δ)-differentially private for the following choice of ϵ and δ

$$\begin{aligned} \epsilon &= 2\log\left(\frac{1 + (2^k - 1)\cdot p}{1 - (1 - \delta_{k0})p}\right) \\ \delta &= M \cdot \left(\frac{1 + (2^k - 1)\cdot p}{N}\right)^M \end{aligned} \tag{1}$$

where δ_{k0} is the Kronecker delta, M is the size of the access sequence and $M >$ total stash size.

Performance Improvements



Improvement in stash usage for $(L, k, Z) = (15, 1, 4)$

Performance Improvements

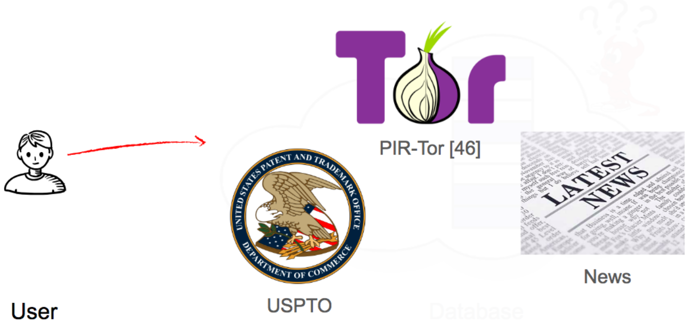
Key takeaway

DP-ORAM can enhance performance at the cost of privacy

Application: Private Information Retrieval

Private Information Retrieval (PIR)

Access data **privately** from **public** database.



[46] Mittal, Prateek, Femi G. Olumofin, Carmela Troncoso, Nikita Borisov, and Ian Goldberg. "PIR-Tor: Scalable Anonymous Communication Using Private Information Retrieval." *In USENIX Security Symposium*, p. 31. 2011.

ORAM based PIR

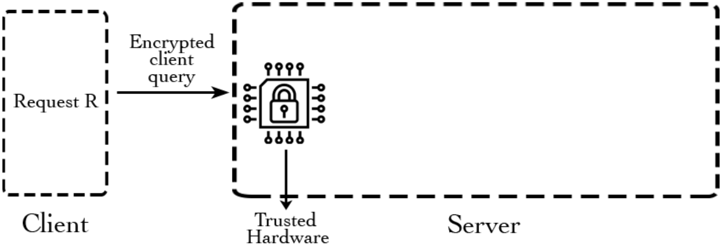
- ORAM has been used previously for PIR [7, 59]

[7] Michael Backes, Aniket Kate, Matteo Maffei, and Kim Pecina. ObliviAd: Provably secure and practical online behavioral advertising. *In IEEE Symposium on Security and Privacy (S&P)*, 2012.

[59] Peter Williams and Radu Sion. Usable PIR. *In Symposium on Network and Distributed System Security (NDSS)*, 2008.

ORAM based PIR

- ORAM has been used previously for PIR [7, 59]

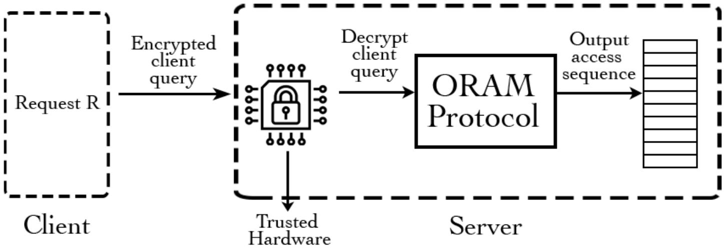


[7] Michael Backes, Aniket Kate, Matteo Maffei, and Kim Pecina. ObliviAd: Provably secure and practical online behavioral advertising. *In IEEE Symposium on Security and Privacy (S&P)*, 2012.

[59] Peter Williams and Radu Sion. Usable PIR. *In Symposium on Network and Distributed System Security (NDSS)*, 2008.

ORAM based PIR

- ORAM has been used previously for PIR [7, 59]

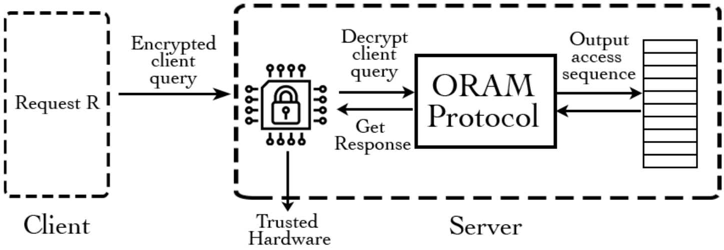


[7] Michael Backes, Aniket Kate, Matteo Maffei, and Kim Pecina. ObliviAd: Provably secure and practical online behavioral advertising. *In IEEE Symposium on Security and Privacy (S&P)*, 2012.

[59] Peter Williams and Radu Sion. Usable PIR. *In Symposium on Network and Distributed System Security (NDSS)*, 2008.

ORAM based PIR

- ORAM has been used previously for PIR [7, 59]

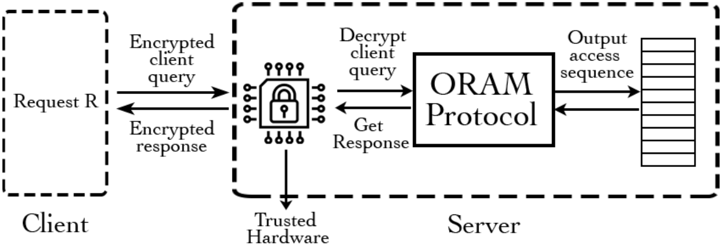


[7] Michael Backes, Aniket Kate, Matteo Maffei, and Kim Pecina. ObliviAd: Provably secure and practical online behavioral advertising. *In IEEE Symposium on Security and Privacy (S&P)*, 2012.

[59] Peter Williams and Radu Sion. Usable PIR. *In Symposium on Network and Distributed System Security (NDSS)*, 2008.

ORAM based PIR

- ORAM has been used previously for PIR [7, 59]

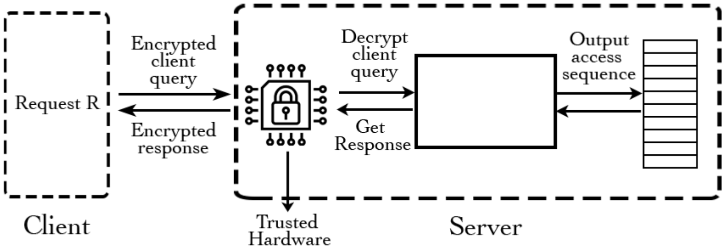


[7] Michael Backes, Aniket Kate, Matteo Maffei, and Kim Pecina. ObliviAd: Provably secure and practical online behavioral advertising. *In IEEE Symposium on Security and Privacy (S&P)*, 2012.

[59] Peter Williams and Radu Sion. Usable PIR. *In Symposium on Network and Distributed System Security (NDSS)*, 2008.

ORAM based PIR

- ORAM has been used previously for PIR [7, 59]

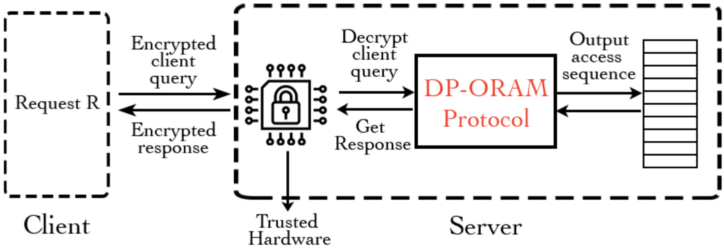


[7] Michael Backes, Aniket Kate, Matteo Maffei, and Kim Pecina. ObliviAd: Provably secure and practical online behavioral advertising. *In IEEE Symposium on Security and Privacy (S&P)*, 2012.

[59] Peter Williams and Radu Sion. Usable PIR. *In Symposium on Network and Distributed System Security (NDSS)*, 2008.

ORAM based PIR

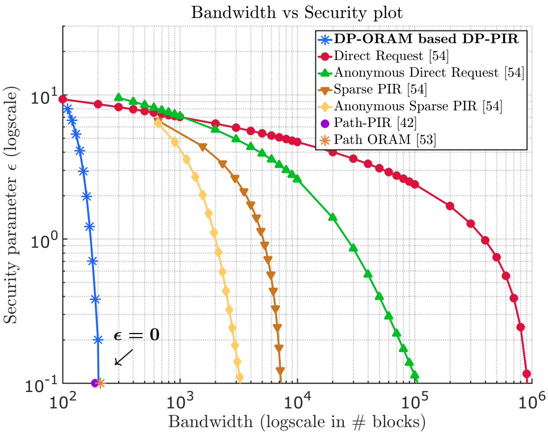
- ORAM has been used previously for PIR [7, 59]



[7] Michael Backes, Aniket Kate, Matteo Maffei, and Kim Pecina. ObliviAd: Provably secure and practical online behavioral advertising. *In IEEE Symposium on Security and Privacy (S&P)*, 2012.

[59] Peter Williams and Radu Sion. Usable PIR. *In Symposium on Network and Distributed System Security (NDSS)*, 2008.

DP-PIR Bandwidth Comparison



Security-Bandwidth trade-offs for DP-PIR protocols (Toledo *et.al.* [54], Path-PIR [42], and Path ORAM [53]).

DP-PIR Bandwidth Comparison

DP-ORAMs provide significant performance benefits for DP-PIR

Conclusion

Summary

- Formalized Differentially Private ORAMs
- Introduced a family of DP-ORAM protocols
- Analyzed security, performance
- Showcased utility for Private Information Retrieval

Summary

- Formalized Differentially Private ORAMs
- Introduced a family of DP-ORAM protocols
- Analyzed security, performance
- Showcased utility for Private Information Retrieval

- Possible to enhance performance by relaxing privacy

Summary

- Formalized Differentially Private ORAMs
- Introduced a family of DP-ORAM protocols
- Analyzed security, performance
- Showcased utility for Private Information Retrieval

- Possible to enhance performance by relaxing privacy

Source code is available at

`https://github.com/inspire-group/Root-ORAM`

Thank you!

Thank you!

Questions?