Full Paper: https://ia.cr/2023/274

KU LEUVEN

imec COSIC

Kelong Cong, Debajyoti Das, Georgio Nicolas, Jeongeun Park
imec-COSIC, KU Leuven, Leuven, Belgium
FHE.org 2023, Tokyo, Japan
26 Mar 2023

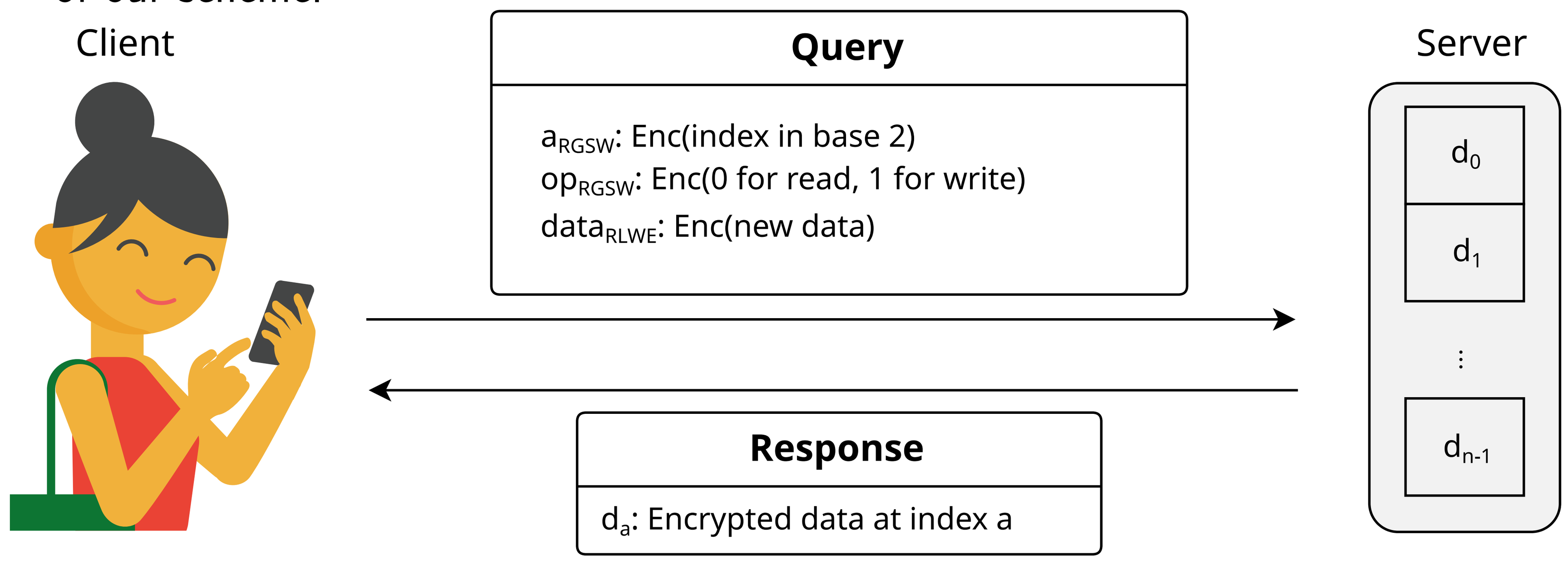
Panacea: Non-interactive and Stateless Oblivious RAM

Background and Motivation

- ORAM allows clients to obliviously read from or write to an encrypted database.
- But prior designs, e.g., [CCR19,SDSCF18], are interactive and/or stateful.
- Our goal is to design an ORAM protocol that can
  - Submit a query, go offline, and collect the server's response without interaction;
  - Query the same server from multiple devices without having to synchronize states;
  - Create batched read/write queries.

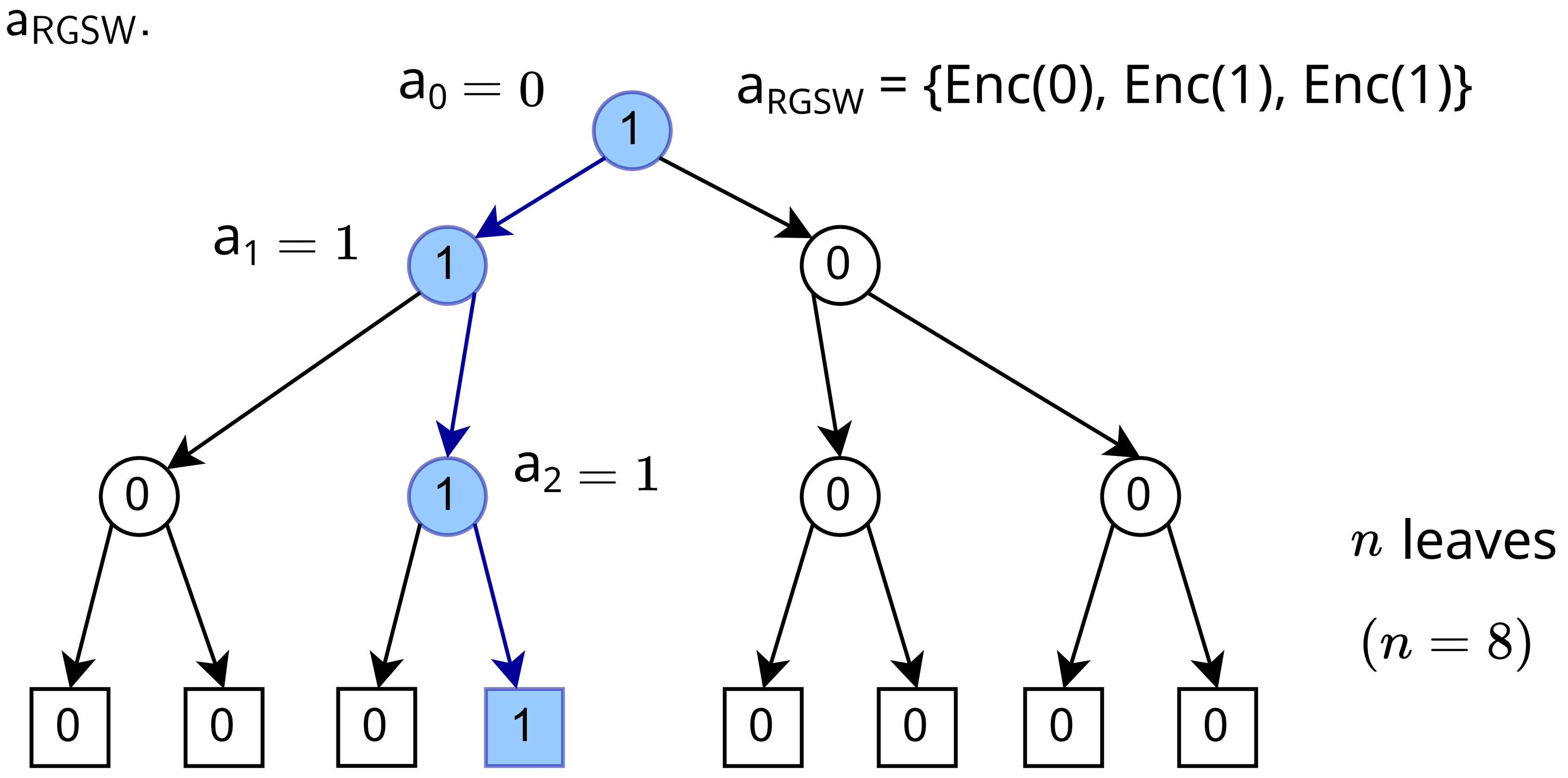
Our Result

- Panacea aims to achieve all goals above by leveraging FHE techniques and offloading all of the expensive computation to the server.
- We provide variants that support querying more than one data element at a time with significantly better amortized computational cost.
- Benchmarks of our proof of concept implementation demonstrate the practicality of our scheme.

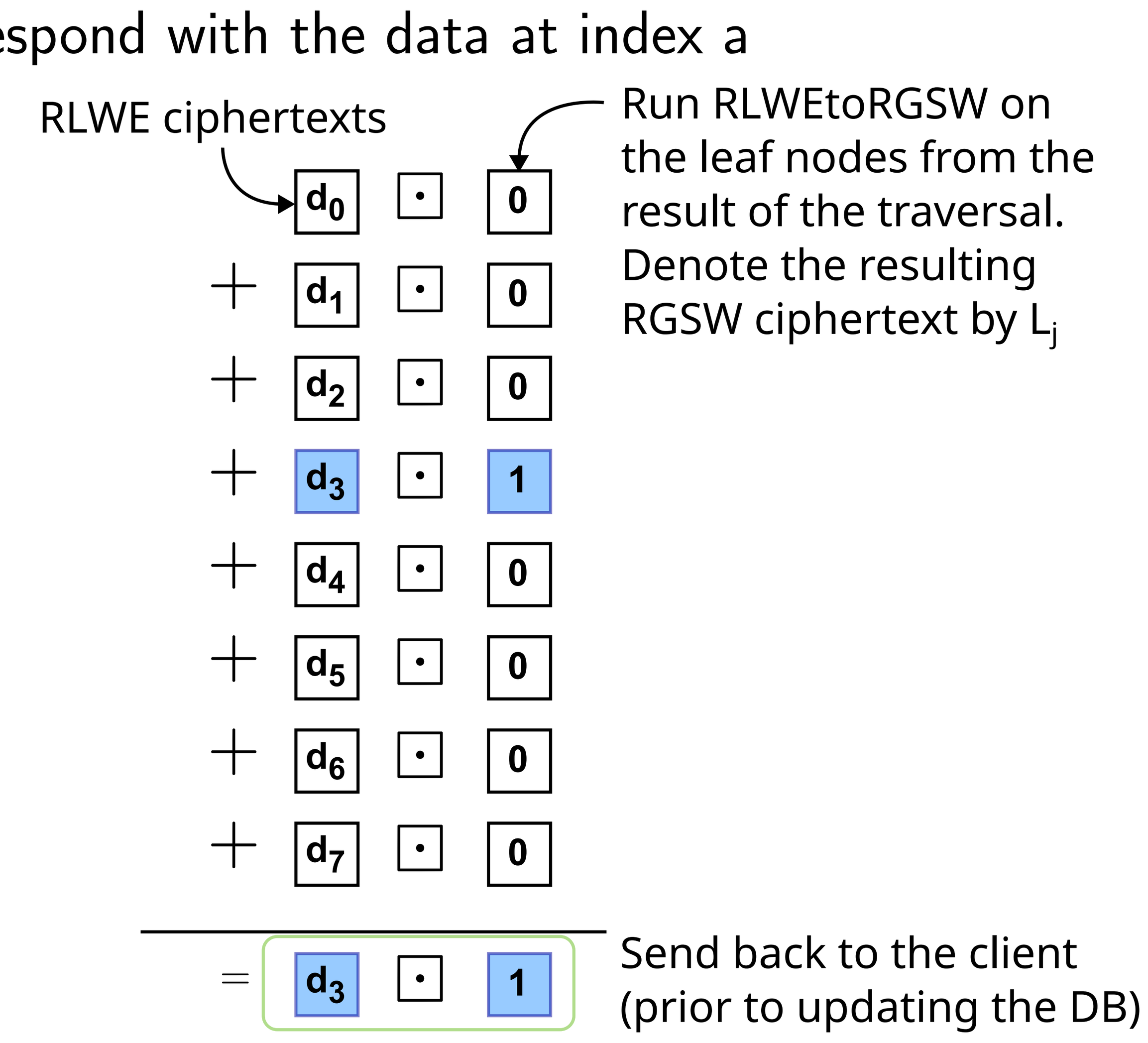


Response Phase (by the Server)

Step 1: Perform traversal to obtain a 1 at the index encrypted by a_{RGSW}.



Step 2: Respond with the data at index a



Update Phase

- Select data if the operation is write, otherwise the old data d_j

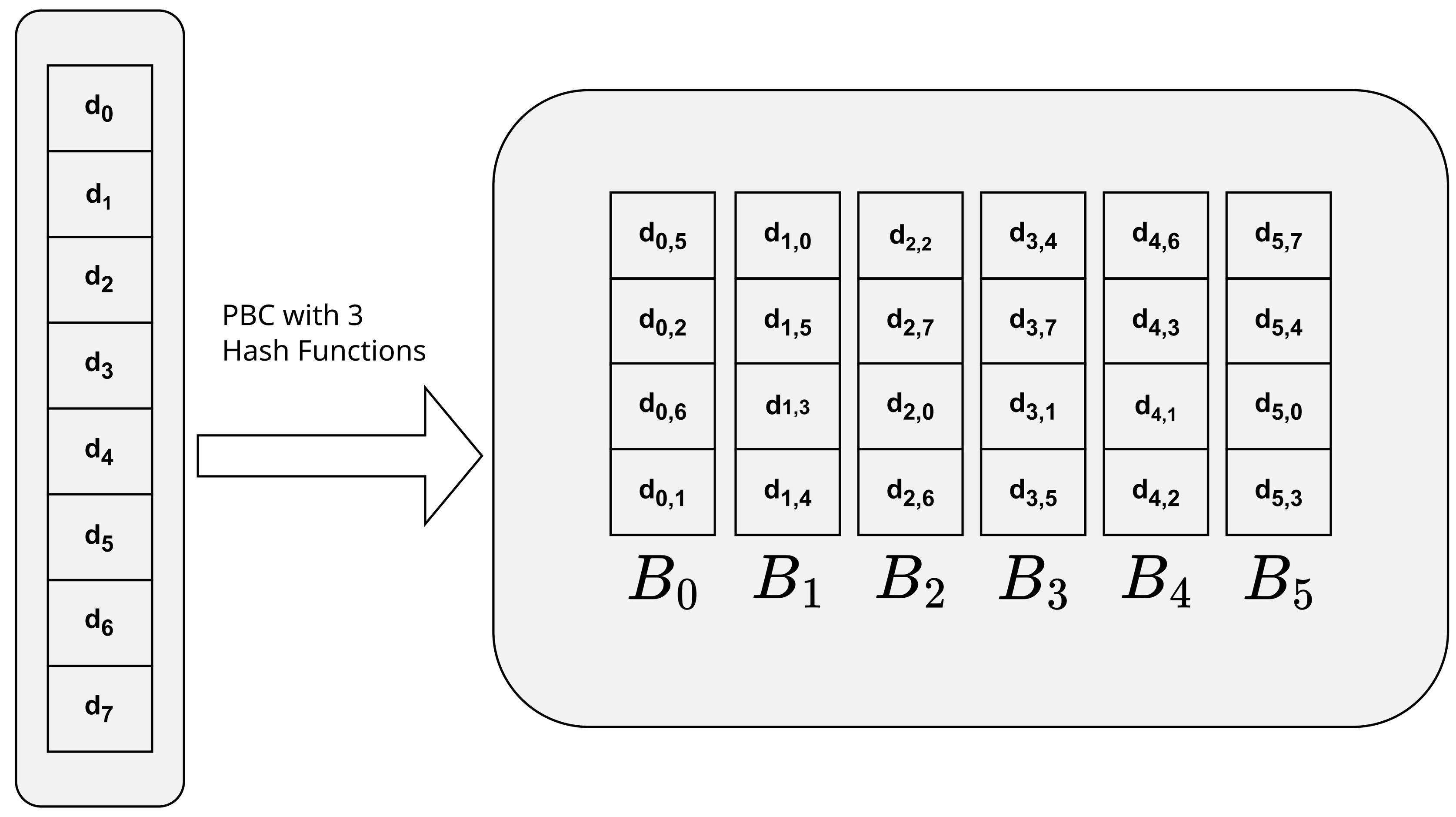
$$\mathrm{temp} \leftarrow \mathrm{CMUX}(\mathrm{op}, \mathrm{data}, d_j), j \in [n]$$

- Update the data on the leaf correspondent to a

$$d_j \leftarrow \mathrm{CMUX}(L_j, \mathrm{temp}, d_j)$$

Batching with PBCs

- The client can submit a batch of k queries at a time.
- The server needs to store $b = 1.5 \cdot k$ buckets (parameterized for correctness).
- Every data element is copied h times, where h is the number of hash functions.



Consistency Correction (Batch Only)

If one out of the three data elements $d_{i_1,j_1}, d_{i_2,j_2}, d_{i_3,j_3}$ is updated, the equation below outputs the updated element obliviously.

$$d_\iota^{new} = d_{i_1,j_1} \boxdot (1 - L_{i_1,j_1} \boxdot op_{i_1} - L_{i_2,j_2} \boxdot op_{i_2} - L_{i_3,j_3} \boxdot op_{i_3}) + (d_{i_1,j_1} \boxdot L_{i_1,j_1} \boxdot op_{i_1} + d_{i_2,j_2} \boxdot L_{i_2,j_2} \boxdot op_{i_2} + d_{i_3,j_3} \boxdot L_{i_3,j_3} \boxdot op_{i_3})$$

Implementation and Experimental Results

Our open source implementation is based on `concrete-core` [CJLOT20] and can be found at https://github.com/KULeuven-COSIC/Panacea.

n	Response Duration	Update Duration	Total Time
2^{12}	2.47 (0.0096)	1.01 (0.0004)	3.48 (0.014)
2^{14}	9.53 (0.037)	2.89 (0.011)	12.42 (0.049)
2^{16}	38.08 (0.15)	11.04 (0.043)	49.13 (0.19)
2^{18}	147.92 (0.58)	48.02 (0.19)	195.94 (0.77)
2^{19}	296.43 (1.16)	94.83 (0.37)	391.26 (1.53)

Table: Computation time in seconds required by the server for database size n, with n from 2^{12} to 2^{19}, for the size of the batch $k = 256$ with PBC. Numbers in brackets are the amortized cost.

References

[CGGI20] Chillotti, I., Gama, N., Georgieva, M., and Izabachène, M., "TFHE: Fast Fully Homomorphic Encryption Over the Torus," JoC, 2020.

[CCR19] Chen, H., Chillotti, I., and Ren, L., "Onion ring ORAM: Efficient constant bandwidth oblivious RAM from (leveled) TFHE," ACM CCS, 2019.

[SDSCF18] Stefanov, E., Dijk, M. V., Shi, E., Chan, T.-H. H., Fletcher, C., Ren, L., Yu, X., and Devadas, S., "Path ORAM: An Extremely Simple Oblivious RAM Protocol," J. ACM, 2018

[CJLOT20] Chillotti, I., Joye, M., Ligier, D., Orfila, J.-B., Tap, S., "CONCRETE: Concrete Operates oN Ciphertexts Rapidly by Extending TfhE," WAHC, 2020

Acknowledgements

The cloud resources and services used in this work were partly provided by the VSC (Flemish Supercomputer Center), funded by the Research Foundation - Flanders (FWO) and the Flemish Government. This work is partially supported by the Research Council KU Leuven under the grant C24/18/049, CyberSecurity Research Flanders with reference number VR20192203 and the Defense Advanced Research Projects Agency (DARPA) under contract number FA8750-19-C-0502.
Any opinions, findings and conclusions or recommendations expressed in this material are those of the authors and do not necessarily reflect the views of any of the funders. The U.S. Government is authorized to reproduce and distribute reprints for governmental purposes notwithstanding any copyright annotation therein.