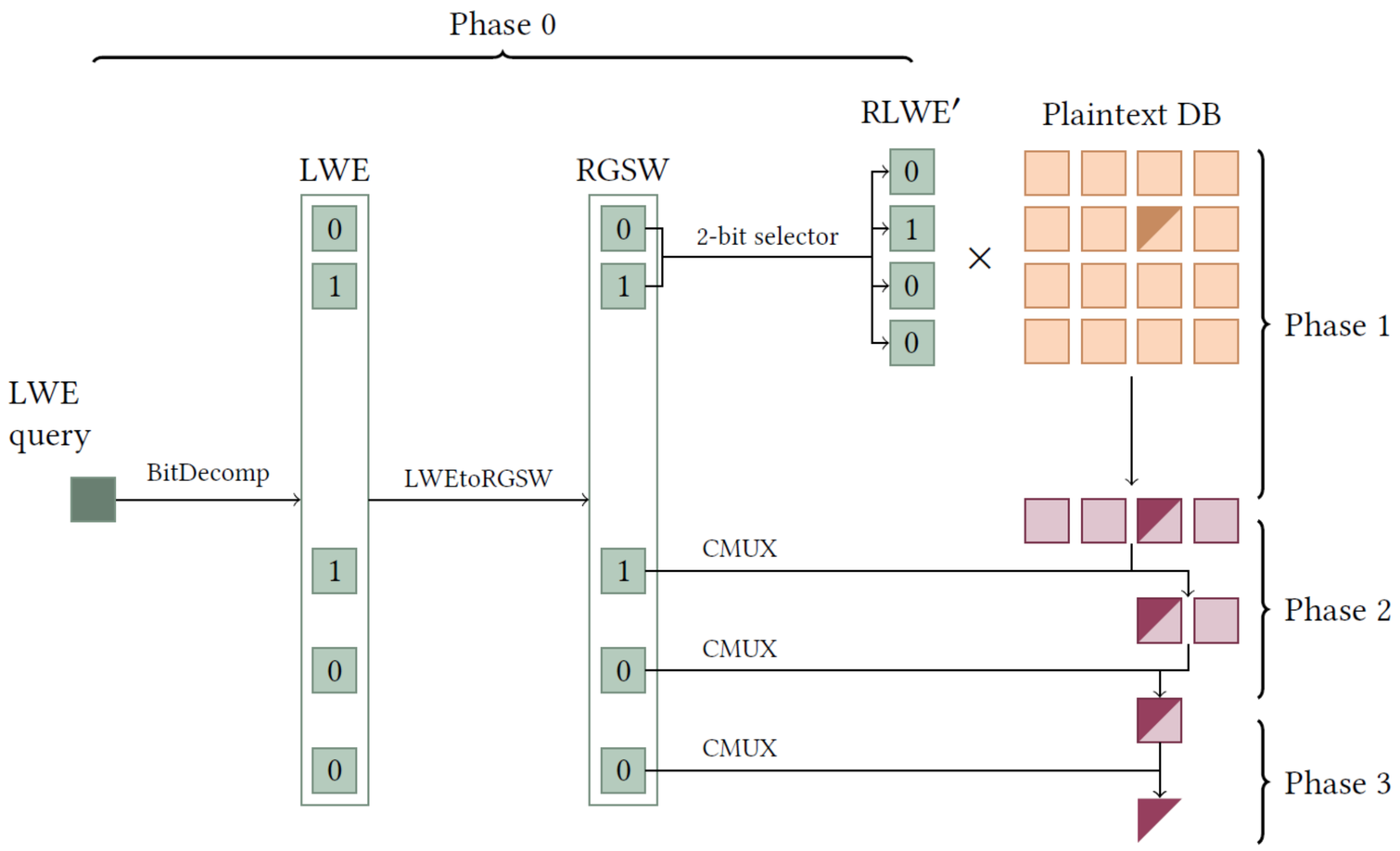
Jiayi Kang and Leonard Schild
COSIC, KU Leuven, Belgium
FHE.org Conference, 8 March 2026

Pirouette: Query Efficient Single-Server PIR



PIROUETTE protocol with toy parameters: $\nu_1 = \nu_2 = 2$ and $\nu_3 = 1$

Introduction

- Private information retrieval (PIR) allows a client to retrieve a record from a public database without revealing its query idx
- Our work introduces a novel alternative to transciphering for reducing the client-to-server communication and applies it to PIR

Our techniques

Starting point: Respire [3], where a database with $\mathcal{N} = 2^{\nu_1+\nu_2+\nu_3}$ records is encoded as a $(1 + \nu_2 + \nu_3)$-dimensional hypercube database

- the first dimension has size 2^{ν_1}
- the remaining dimensions have size 2
- entries are encoded as polynomials

High-precision homomorphic bit decomposition

- e.g. decomposing an input of 25 bits requires 15 BlindRotates for ring dimension 2^{11}
- in comparison, naively applying with a one-bit base in [5] requires 50 BlindRotates
- in the variant PIROUETTE$^{\mathsf{H}}$, a query consists of LWE encryptions of all the bits $\{\mathsf{LWE}(\mathsf{idx}_i)\}_{i\in[0,\log_2\mathcal{N}-1]}$, hence homomorphic bit decomposition is not needed

Construction of ν-bit selectors

- input ν encrypted control bits $\{\widetilde{\mathbf{Enc}}(b_j)\}_{j\in[0,\nu-1]}$
- output 2^ν ciphertexts $\{\mathbf{Enc}(\delta_{i,b})\}_{i\in[0,2^\nu-1]}$
- construction similar to a homomorphic decision tree

Concurrent work

The recent work [4] is also based on Resipre and employs a DMUX gate construction, which is equivalent to our ν-bit selector, to reduce the query size. Despite these similarities, the two works differ in their focus:

- [4] reduces the query size to $\approx$ response size and introduces other techniques to improve the throughput
- our work minimises the query size and compares with transciphering-based approaches

Evaluation

We compare PIROUETTE, and PIROUETTE$^{\mathsf{H}}$ to Respire, T-Respire (combining the state-of-the-art transciphering [2, 1] to Repire). Our implementation relies on the OpenFHE library and all experiments are performed using an Intel(R) Xeon(R) Gold 6248R CPU with 512 GB of RAM. The full paper includes results for both the sequential and parallel settings over 32 cores.

Database	Metric	Respire	T-Respire	PIROUETTE	PIROUETTE$^{\mathsf{H}}$
$2^{20} \times 256$ B	Offline Comm.	4 MB	91 MB	1.2 GB	650 MB
(256 MB)	Query Size	4.1 KB	144 B	36 B	55 B
	Response Size			2.0 KB	
	Computation	1.5 s	217 s	19 s	15 s
$2^{22} \times 256$ B	Offline Comm.	4 MB	91 MB	1.2 GB	650 MB
(1 GB)	Query Size	7.7 KB	208 B	36 B	57 B
	Response Size			2.0 KB	
	Computation	4 s	296 s	26 s	21 s
$2^{25} \times 256$ B	Offline Comm.	4 MB	91 MB	1.2 GB	650 MB
(8 GB)	Query Size	14.8 KB	336 B	36 B	60 B
	Response Size			2.0 KB	
	Computation	30 s	486 s	60 s	55 s

As such, PIROUETTE and PIROUETTE$^{\mathsf{H}}$ would be most applicable in scenarios where:

1. online bandwidth, particularly from client to server, is severely constrained
2. offline bandwidth is widely available, with offline and online phases exhibiting distinct network characteristics (e.g. wired device initialization vs wireless operation)
3. the server computation can leverage multi-core parallelisation on dedicated FHE hardware accelerators

Conclusion

- Novel approach to reduce the client-to-server communication
  - a lower server-side computational overhead than transciphering
  - applicable for many other FHE-based applications
- PIROUETTE, a PIR protocol with small query size
  - for a database of 2^{25} records, the query size is just 36B
  - $\Rightarrow$ 32 bits if the query seed is set once by the server, giving an expansion factor of $32/25 = 1.28$

Paper (to appear in PETS2026): https://ia.cr/2025/680
Code: https://github.com/KULeuven-COSIC/Pirouette

Contact Info
- jiayi.kang@esat.kuleuven.be
- leonard.schild@esat.kuleuven.be

References

[1] Sonia Belaïd et al. "Further Improvements in AES Execution over TFHE". In: *IACR Communications in Cryptology* (2025).
[2] Nicolas Bon, David Pointcheval, and Matthieu Rivain. "Optimized Homomorphic Evaluation of Boolean Functions". In: *IACR Transactions on Cryptographic Hardware and Embedded Systems* (2024).
[3] Alexander Burton, Samir Jordan Menon, and David J. Wu. "Respire: High-Rate PIR for Databases with Small Records". In: *ACM CCS 2024: 31st Conference on Computer and Communications Security*.
[4] Chenyang Liu, Xukun Wang, and Zhifang Zhang. *VIA: Communication-Efficient Single-Server Private Information Retrieval*. Cryptology ePrint Archive, Paper 2025/2074. to appear in S&P 2026.
[5] Zeyu Liu, Daniele Micciancio, and Yuriy Polyakov. "Large-Precision Homomorphic Sign Evaluation Using FHEW/TFHE Bootstrapping". In: *Advances in Cryptology – ASIACRYPT 2022, Part II*.