CONJURA · OPEN PROBLEM

No Black-Box Secret-Key Doubly Efficient PIR from One-Way Functions

Proved for two-round passive-server schemes; the general case is what the source's main theorem waits on

Status. Statement: AI-written from Wei-Kai Lin, Ethan Mook and Daniel Wichs, *Black Box Crypto is Useless for Doubly Efficient PIR*, IACR ePrint 2025/552, EUROCRYPT 2025. Not yet checked by a human. The source proves the conjecture for the special case of two-round passive-server schemes; the general case — arbitrarily many rounds, an active server — is open and is stated by the source as a conjecture.

Category. *Private information retrieval; black-box separations.*

Conjecture (informal). *A doubly efficient private information retrieval scheme lets a server preprocess a database once and then answer each private lookup by touching only a sublinear number of stored positions. Only one standard assumption is known to give one, Ring-LWE. The source explains the scarcity: it shows that idealized generic cryptography — random oracles, generic multilinear maps, virtual black-box obfuscation, and anything else expressible as a deterministic program with access to a secret random function — can always be stripped out of such a scheme and replaced by a one-way function alone. That reduces the whole question to one statement, which the source cannot prove in general: one-way functions do not build a secret-key doubly efficient PIR in a black-box way. Prove it and every generic primitive is ruled out at once.*

1 The setting

A *secret-key doubly efficient private information retrieval* (SK-DEPIR) scheme, in the deliberately weak form the source fixes so that its negative results are as strong as possible, consists of

- $k \leftarrow \mathsf{KeyGen}(1^\lambda)$, sampling a secret key;
- $\widetilde{\mathsf{DB}} \leftarrow \mathsf{Prep}(1^\lambda, k, \mathsf{DB})$, preprocessing a database $\mathsf{DB} \in \{0,1\}^N$ into a data structure held by the server;

- a two-party protocol $\Pi(\widetilde{\mathsf{DB}}; (N, k, i))$ between the server, holding $\widetilde{\mathsf{DB}}$, and the client, holding N, the key k and an index $i \in [N]$, at the end of which the client outputs a bit.

Correctness asks that the client's output equal $\mathsf{DB}[i]$ except with probability $\varepsilon(\lambda)$. Security asks that no non-uniform polynomial-time semi-honest server, given $\widetilde{\mathsf{DB}}$ and any polynomial number of honest protocol executions of its choice, distinguish an execution on index i_0 from one on i_1 with more than negligible advantage. The *locality* of a scheme is the maximum number $\ell(\lambda, N)$ of distinct positions of $\widetilde{\mathsf{DB}}$ the server's algorithm touches in the worst case, and the definition requires only $\ell = o(N)$; the online protocol may run for any polynomial number of rounds and any polynomial time.

Theorem 1 (Crypto oracles are useless, [LMW25, Thm. 4.3]). *Let a* crypto oracle *be B^R, where B is a stateless deterministic polynomial-time function with oracle access to a secret random function $R : \{0,1\}^* \to \{0,1\}$, and where schemes and adversaries may query B^R but not R. Any SK-DEPIR relative to a crypto oracle can be converted into one in which the client alone has black-box access to a secret random function, preserving round complexity, locality, correctness and security; replacing that function by a pseudorandom function yields a SK-DEPIR making only black-box use of one-way functions.*

Virtual black-box obfuscation for programs with oracle gates and generic multilinear groups are both crypto oracles, and so are random oracles; the source proves the first two explicitly.

2 Notation and parameters

- λ is the security parameter and $N = \mathrm{poly}(\lambda)$ the database size.
- $\ell(\lambda, N) = o(N)$ is the locality: how many positions of the preprocessed database the server reads per query.
- A scheme is *passive-server* if the server performs no computation online and merely returns the values at the positions the client names; *two-round* means the client sends one set of positions and the server answers once.
- *Black-box construction* of a primitive Q from a primitive P is the standard fully black-box notion: a pair of oracle algorithms (Q, S) such that Q^P implements Q for every implementation

P of P, and such that $S^{P,A}$ breaks P whenever A breaks Q^P.

3 The conjecture

Conjecture 1 ([LMW25, §1.1]). *There is no black-box construction of secret-key doubly efficient private information retrieval from one-way functions.*

Remark 1 (How the source states it). Verbatim, page 4: "We conjecture that there is no black-box construction of SK-DEPIR from just one-way functions. While we do not know how to prove this conjecture in its full generality, we do prove it for the special case of 2-round passive-server SK-DEPIR."

Theorem 2 (The proved special case, [LMW25, Thm. 5.1, Cor. 5.2]). *Let $\delta(\lambda)$ be negligible, $\varepsilon(\lambda) \le 1/20$ and $\ell(\lambda, N) = o(N) + \mathrm{poly}(\lambda)$. Then no two-round passive-server SK-DEPIR with these parameters exists relative to a secret random function held by the client, hence none exists relative to any crypto oracle, and none can be built from one-way functions in a black-box way.*

Remark 2 (Why the conjecture is the load-bearing statement). Theorem 1 is stated by the source as a conditional elimination: "Under the conjecture that there is no black-box construction of SK-DEPIR from just one-way functions, this implies that there is no black-box construction of SK-DEPIR from any crypto oracle (without additional assumptions)." So Conjecture 1 is not one open problem among several — it is the single remaining hypothesis between the source's compiler and a clean statement that no idealized generic primitive helps.

It also matters that SK-DEPIR is the *weakest* of the three flavours of DEPIR, so ruling it out rules out public-key and unkeyed DEPIR with it.

Remark 3 (What makes it hard, in the source's own terms). The proved case is the one where the server is passive and the online protocol has two rounds, and the argument there is information-theoretic: in that shape the client's queries are a set of positions, and a counting argument over the secret random function applies. Neither ingredient survives in general. With many rounds the client's

later queries depend on earlier answers, and with an active server the positions the server reads are no longer the ones the client named. The source does show how to convert any DEPIR into a passive-server one, but that conversion is round-preserving only in the passive case, which is why the two restrictions appear together in Theorem 2 rather than separately.

Note also what the conjecture is *not* claiming. It does not say DEPIR is impossible. The source's reading is the opposite: "The main interpretation of our result is that DEPIR requires concrete hardness assumptions about real-world problems (e.g., hardness of Ring LWE), which cannot be captured by a black-box use of crypto oracles."

Remark 4 (The state of the art the conjecture sits against). Only one standard assumption is known to yield any flavour of DEPIR, namely Ring-LWE, via Lin, Mook and Wichs. The source records the gap on the positive side too — "It remains a fascinating open problem to construct any flavor of DPEIR under any standard assumption beyond RingLWE, such as standard LWE, DDH (in bilinear maps), factoring, etc." (the misspelling is the source's) — and on the reduction side: "Conversely, we do not know of any standard cryptographic primitives that would generically imply any flavor of DEPIR." Those are two further open questions, posed separately by the source, and are not what is published here.

4 Bibliography

[LMW25] Wei-Kai Lin, Ethan Mook and Daniel Wichs. *Black box crypto is useless for doubly efficient PIR*. IACR ePrint 2025/552; EUROCRYPT 2025. The conjecture and the proved special case are stated on page 4; the conditional elimination on page 5; the definition of SK-DEPIR is Definition 2.1, black-box constructions Definition 2.3, crypto oracles Definition 3.1; the compiler is Theorem 4.3 and the impossibility Theorem 5.1 with Corollary 5.2.

[LMW23] Wei-Kai Lin, Ethan Mook and Daniel Wichs. *Doubly efficient private information retrieval and fully homomorphic RAM computation from ring LWE*. 55th Annual ACM Symposium on Theory of Computing (STOC), pages 595–608, ACM Press, June 2023. The only construction of unkeyed DEPIR from a standard assumption, and the state of the art the conjecture is measured against.

[RTV04] Omer Reingold, Luca Trevisan and Salil P. Vadhan. *Notions of reducibility between cryptographic primitives.* TCC 2004, LNCS 2951, pages 1–20, Springer, February 2004. The fully black-box construction notion the conjecture quantifies over, cited by the source for its Definitions 2.3 and 2.4.

[BIPW17] Elette Boyle, Yuval Ishai, Rafael Pass and Mary Wootters. *Can we access a database both locally and privately?* TCC 2017, Part II, LNCS 10678, pages 662–693, Springer, November 2017. One of the two first candidate keyed DEPIR constructions, and the source of the fact that SK-DEPIR implies one-way functions. Its default object, 2-round passive-server SK-DEPIR, is exactly the case the source can prove.

[CHR17] Ran Canetti, Justin Holmgren and Silas Richelson. *Towards doubly efficient private information retrieval.* TCC 2017, Part II, LNCS 10678, pages 694–726, Springer, November 2017. The other first candidate, and the source of the secret-key-size lower bound the impossibility generalizes.

[DH24] Jesko Dujmovic and Mohammad Hajiabadi. *Lower-bounds on public-key operations in PIR.* EUROCRYPT 2024, Part VI, LNCS 14656, pages 65–87, Springer, 2024. The insight the source names as its inspiration: replacing a server's oracle calls by communication between the client and the server.