# Information-Theoretic Security in Quantum SPIR

Danning Zhan [1], Rihan Hai [1]

[1] Web Information System, TUDelft, Netherlands
{d.zhan, r.hai}@tudelft.nl

The task of private information retrieval is known to be a difficult problem. This is the problem of a client performing a query on an index from a source without the source being aware of the query index. Primarily because communication of O(N) for a size N database is necessary for information-theoretic security. One can guarantee information-theoretic security for PIR through various means [3]. The concept of information-theoretic security for query privacy can be explained as follows. The server will have formed a distribution of the client's query before query time. After query time, if the posterior distribution remains the same, it means that the transaction was information-theoretically secure. This means that no matter how much computational resources the adversary(server) has, the distribution will not change.

A generalization of this problem is symmetric private information retrieval (SPIR). This problem is a generalization in which the user does not discover any information regarding the data on the server beyond what is required for their index. This is especially true for a single-server setting, due to the information-theoretic guarantee of the query privacy. Which is only guaranteed by communicating the entire database. Any form of encryption, such as public key encryption, can lead to a computationally unbounded attacker brute-forcing the encryption; thus, it is only computationally secure.

Several tools have been employed for SPIR, including the use of homomorphic encryption. A lesser-studied tool that has been attempted to be used is quantum communication [1, 2]. Suppose we have a quantum channel through which we can communicate data. There have been works that utilize quantum technologies for implementation, due to the no-clone theorem [4]. Thus, works claim that there are information-theoretical security guarantees in the protocols. However, for many works, there is still an attack vector that can be exploited through the naive use of the measurement basis. Due to the no-clone theorem, one can imagine that any scheme that can utilize qubits of any form would be able to produce an SPIR scheme. Similarly, due to the probabilistic nature of quantum states, one can assert that the security also lies in the minimal number of trials to guarantee specific results. Due to the collapse of measurement, one could assume that the communication is thus secure.

This, however, is not true, as some attack vectors can be utilized. We analyze how information-theoretic security breaks down even in quantum communication channels. Several schemes have been proposed using quantum technologies; however, each scheme has its own unique set of attack vectors. Such as the attacks from the server side in [2], or attacks from the client side [1]. Meaning that there is no possibility for an information-theoretically secure SPIR even using quantum communications.

## References

[1] Giancarlo Gatti and Rihan Hai. Private quantum database, 2025. https://arxiv.org/abs/2508.19055.

[2] Vittorio Giovannetti, Seth Lloyd, and Lorenzo Maccone. Quantum private queries. *Phys. Rev. Lett.*, 100:230502, Jun 2008. https://link.aps.org/doi/10.1103/PhysRevLett.100.230502.

[3] Alexandra Henzinger, Matthew M. Hong, Henry Corrigan-Gibbs, Sarah Meiklejohn, and Vinod Vaikuntanathan. One server for the price of two: Simple and fast single-server private information retrieval. Cryptology ePrint Archive, Paper 2022/949, 2022. https://eprint.iacr.org/2022/949.

[4] W. K. Wootters and W. H. Zurek. A single quantum cannot be cloned. , 299(5886):802–803, October 1982.