International Journal of Applied Research 2025; 11(6): 19-25

International Journal of Applied Research

ISSN Print: 2394-7500
ISSN Online: 2394-5869
Impact Factor (RJIF): 8.4
IJAR 2025; 11(6): 19-25
www.allresearchjournal.com
Received: 17-03-2025
Accepted: 19-04-2025

Laxmi Kumari
Department of Mathematics,
Srinath University,
Jamshedpur, Jharkhand, India

Tarun Kumar Mahato
Department of Mathematics,
Srinath University,
Jamshedpur, Jharkhand, India

Corresponding Author:
Tarun Kumar Mahato
Department of Mathematics,
Srinath University,
Jamshedpur, Jharkhand, India

A survey on communication complexity in quantum private information retrieval: Efficiency challenges and advances

Laxmi Kumari and Tarun Kumar Mahato

DOI: https://www.doi.org/10.22271/allresearch.2025.v11.i6a.12630

Abstract
Quantum Private Information Retrieval (QPIR) is a new and growing area that uses quantum computing to improve privacy and efficiency in database searches. Traditional Private Information Retrieval (PIR) methods often require a large amount of communication between the user and the server, making them slow and costly. QPIR aims to solve this problem by using quantum techniques like superposition and entanglement to reduce communication while keeping the user's query private. In this paper, we review different QPIR methods and analyze how they handle communication complexity. We compare multi-server and single-server models, discussing their strengths and weaknesses. We also explore the practical challenges of QPIR, such as the need for quantum resources, errors in quantum systems, and security against quantum attackers. Additionally, we highlight important research gaps, including how to make single-server QPIR more efficient, balancing security with speed, and understanding how future quantum computers might impact QPIR security. By addressing these challenges, this survey aims to support further research and help develop practical, efficient, and secure QPIR systems for real-world use.

Keywords: Communication, single-server model, multi-server model, quantum security, Quantum Private Information Retrieval (QPIR)

1. Introduction

In today's digital world, protecting user privacy during data retrieval is a major challenge. Private Information Retrieval (PIR) is a method that allows users to fetch information from a database without revealing what they are looking for. However, traditional PIR methods often have high communication costs, making them inefficient when dealing with large databases [1]. With the rise of quantum computing, researchers have explored Quantum Private Information Retrieval (QPIR) as a more efficient alternative [2]. QPIR takes advantage of quantum properties like superposition and entanglement to reduce communication complexity and improve privacy.

QPIR aims to minimize the amount of data exchanged between the user and the server while ensuring that the server learns nothing about the user's query. Unlike classical PIR, which often requires multiple non-colluding servers to function efficiently, QPIR offers new possibilities, including single-server solutions [3] shows in Figure.1. This is an important advancement because relying on multiple servers is often impractical in real-world applications.

Over the years, researchers have proposed different models for QPIR. Some methods rely on entangled quantum states shared between the user and the server, while others use quantum computation to encode queries in a way that hides the user's intent. Many of these approaches have demonstrated lower communication costs compared to classical PIR, making them promising for large-scale applications such as cloud storage and secure database access [3].

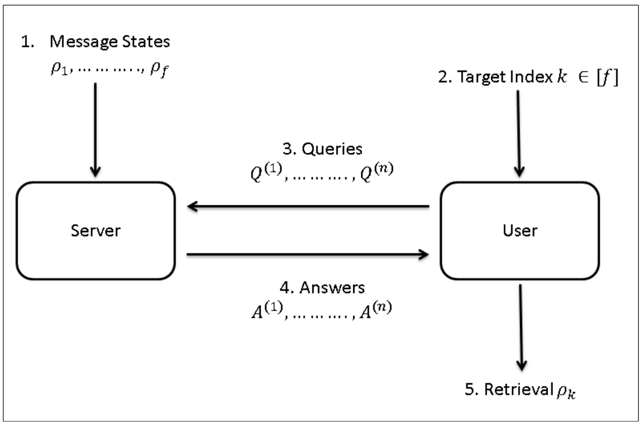

Fig 1: One-server QPIR protocol with quantum messages. In round i, the user sends a quantum query $Q^{(i)}$ to the server and receive a quantum answer $A^{(i)}$ [3].

Despite its potential, QPIR still faces several challenges. The practical implementation of QPIR protocols requires quantum hardware, which is still in its early stages of development. Additionally, most existing schemes assume ideal conditions, but real-world quantum systems suffer from noise and errors that can affect performance [4]. Security is another concern, as researchers need to study how QPIR holds up against powerful quantum attackers. Finally, the trade-offs between efficiency, security, and resource requirements in different QPIR schemes are not fully understood.

In this paper, we analyze the efficiency and communication complexity of various QPIR schemes. We discuss how different methods compare in terms of communication cost, security, and feasibility. We also highlight current research gaps and suggest possible future directions to make QPIR more practical. By addressing these issues, we hope to contribute to the development of efficient and scalable QPIR protocols that can be used in real-world applications.

The present paper aims to address the following objectives: it reviews various Quantum Private Information Retrieval (QPIR) schemes, analyzes the trade-offs involved in communication complexity, and identifies key challenges along with potential directions for future research.

2. Background and Preliminaries

2.1 Private Information Retrieval (PIR)

Private Information Retrieval (PIR) is a technique that allows a user to fetch information from a database without revealing what they are searching for. This is important for privacy, especially in cases where users do not want the database provider to track their interests.

Imagine you are searching for a specific medical condition on an online health database, but you don't want the website to know what you are looking for. Normally, when you search for something online, the server can track your query and store it for advertising or other purposes. Private Information Retrieval (PIR) is a method that allows you to get the information you need without revealing what you are searching for.

Traditional PIR methods involve one or multiple servers storing the database. If multiple servers are used and they do not communicate with each other, the user can design a query that keeps their request hidden. However, many PIR schemes require a large amount of communication between the user and the server, making them inefficient for large databases.

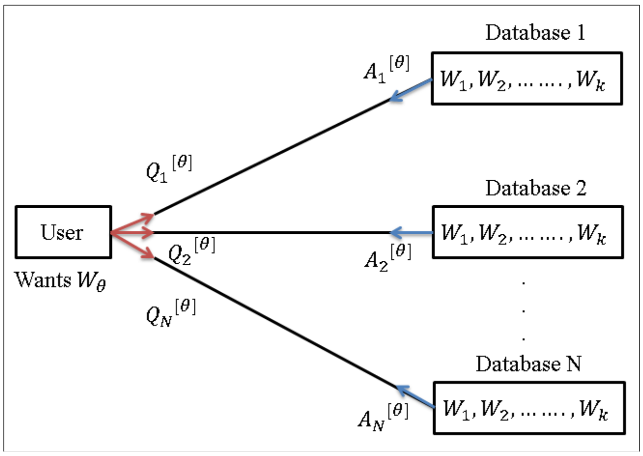

Fig 2: Traditional PIR with N number of database and K messages [11], [12].

In Figure.2, there are N databases, and each one store all the messages denoted by $W_1, W_2, \ldots\ldots W_K$ respectively. In classical PIR, a user secretly generates $\theta \in [K]$ and a user chooses one message to retrieve W_θ while keeping the θ is a secret from each database. Depending on θ, there are K strategies that get the message without letting any database know which one the user is asking for. To do this, the user creates a special query $Q_N{}^{[\theta]}$ to the database and this query send to each database. When a database receives the query $Q_N{}^{[\theta]}$, it uses it to create an answer, called $A_N{}^{[\theta]}$, and sends it back to the user. The answer is made using the information in the query, but it doesn't reveal which message the user is really interested in.

2.2 Quantum Private Information Retrieval (QPIR) [10]

Quantum Private Information Retrieval (QPIR) is a more advanced version of PIR that uses quantum computing to improve efficiency. Instead of relying only on classical data exchanges, QPIR takes advantage of quantum properties such as:

Superposition in Quantum Private Information Retrieval (QPIR)

In QPIR, superposition is a key quantum mechanical principle that enables the user to privately and efficiently retrieve data from a server without revealing which specific item is being requested. Superposition allows a quantum bit (qubit) to exist in a combination of the classical states |0⟩ and |1⟩ simultaneously. This means that, instead of querying a single database index, the user can query all possible indices at once using a quantum state. To achieve this, the user prepares a query in a quantum superposition of all database indices:

$$\sum_i \alpha_i |i\rangle$$

Here, each |i⟩ represents a possible index in the database and are complex coefficients. This quantum query is sent to the server, who performs quantum operations that entangle the query with the corresponding database entries. Due to the linearity of quantum mechanics, the server processes all

components of the superposed query simultaneously this is known as quantum parallelism. After processing the superposed query, the server sends the quantum state back to the user, who then applies further quantum operations and measurements to extract the data corresponding to the desired index without revealing their interest to the server.
Entanglement: Two or more qubits can be linked, allowing secure communication and reducing the number of messages exchanged. This property is used to enhance both privacy and efficiency during data retrieval.
QPIR can significantly lower the communication cost while maintaining privacy, making it a promising approach for secure database access.

2.2.1 Types of QPIR Models
There are different types of QPIR models based on how they are implemented:

Multi-Server QPIR [5]: This model is like using multiple cashiers in a supermarket who don't talk to each other. If you want to ask for a discount without revealing which product you're interested in, you could cleverly split your question between them so that no single cashier knows the full request. This helps improve efficiency but requires multiple independent servers, which may not always be practical.

Single-Server QPIR [6]: The user retrieves information from a single server while ensuring privacy. This model is like asking a librarian for a book without telling them exactly which one. The challenge is that since there's only one librarian (server), they might be able to guess what book (query) you want unless the request is carefully designed. Single-server QPIR is harder to achieve but is more useful in real-world applications where relying on multiple independent servers is not feasible.

2.2.2 Communication Complexity in QPIR [7]
One of the main goals of QPIR is to reduce communication complexity, which refers to the amount of data that needs to be exchanged between the user and the database. Classical PIR methods often require downloading a large portion of the database, leading to high costs. QPIR, on the other hand, aims to minimize this cost by using quantum techniques to encode and process queries more efficiently.

2.2.3 Challenges in QPIR [3, 8]
While QPIR offers many benefits, there are still several challenges that researchers need to address:

Quantum Hardware Limitations: Imagine trying to use a high-tech self-driving car when the roads aren't built for it yet. Similarly, quantum computers are still developing, and implementing QPIR in real-world systems requires advanced quantum hardware that is not yet widely available.

Security Concerns: Just like how hackers try to break into secure online banking systems, attackers could try to exploit weaknesses in QPIR schemes. Ensuring that QPIR remains secure, even against powerful quantum-based attacks, is a critical challenge.

Balancing Efficiency and Privacy: While QPIR can reduce communication complexity, ensuring strong privacy protections at the same time is not always easy. It's like trying to make a fast, lightweight bulletproof vest the lighter it is, the harder it is to maintain full protection.

3. Existing QPIR Models and Their Communication Complexity
Over the years, researchers have developed different QPIR models with various structures. The three main types are:

3.1 Multi-Server QPIR [3, 5, 9]
In a multi-server QPIR model, the database is copied and stored on more than one server usually two or more. These servers must not communicate with each other, which mean they can't share what the user asks them.

Working
Let's say there are two servers, A and B. The user wants to get the third item from a database with five items. Instead of directly asking both servers for item 3, the user sends cleverly prepared queries that split the request in such a way that each server receives a part of the query that does not reveal what the actual item is. But when the responses from both servers are combined, the user gets the correct answer shown in Figure 3.

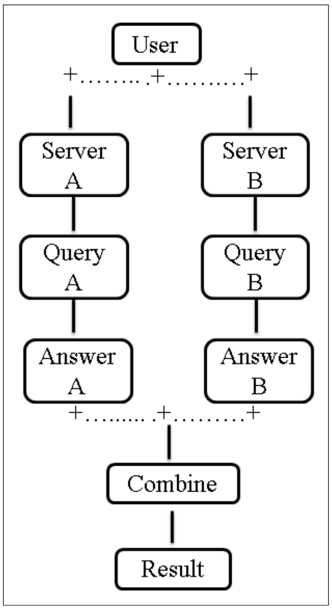

Fig 3: Flow chart of Multi-Server QPIR

Communication Complexity
Multi-server QPIR schemes can achieve sub-linear or even logarithmic communication complexity, which means that the user doesn't have to download the whole database only a small portion, even when the database is large.

Advantages
Very low communication cost.
Simple to analyze theoretically.

Limitations
Requires multiple servers that do not talk to each other, which is hard to guarantee in real-life situations.

3.2 Single-Server QPIR [6]
In a single-server QPIR model, the entire database is stored on only one server. This is more realistic because most real-

world systems only have one central server. But this setup is more difficult, because the server can easily observe any query from the user.

Working

Quantum techniques like entanglement and quantum teleportation are used to hide the user's query. The user can prepare a quantum state that encodes the position of the desired item in a special way. The server performs operations on this quantum state and sends it back. With this, the user can extract the desired item without revealing which one it is. It's like asking a librarian for a book without telling the exact title. You use a coded message (quantum state) to make the request, and the librarian replies based on that without knowing what book you actually wanted.

In Figure.4 illustrate a one-server Quantum Private Information Retrieval (QPIR) protocol, where the user prepares a quantum query$|\Psi_Q\rangle$ and sends it to the server. The server processes this quantum query using entangled quantum states and accesses the database accordingly. The resulting quantum state, representing the response$|\Psi\rangle$, is then sent back to the user. Both the server and the user perform decoding operations, enabling the user to retrieve the desired information without revealing which item was accessed. The protocol also includes an entanglement channel between the user and server, enhancing security and enabling more efficient communication.

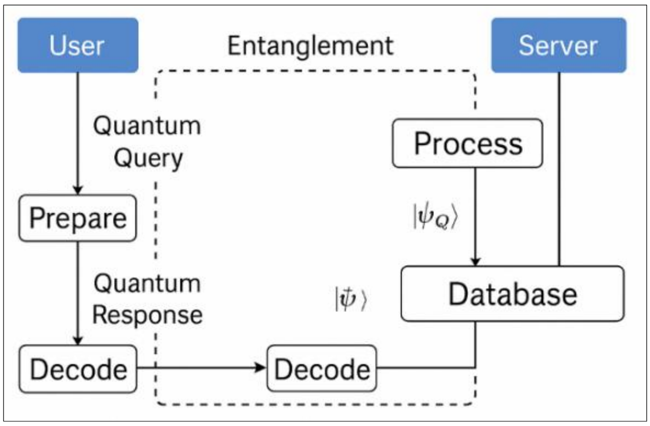

Fig 4: Flow chart of Single-Server QPIR

Communication Complexity

Single-server QPIR generally has higher communication costs than the multi-server model, especially if we want it to be secure against quantum attacks. However, some modern protocols try to reduce this cost using pre-shared entanglement or quantum error-correcting codes.

Advantages

More practical (only one server).
Easier to deploy in real-world networks.

Limitations

Harder to reduce communication cost.
Requires stronger quantum techniques.
Often needs pre-shared quantum resources, which is not easy with current technology.

3.3 Hybrid and Other Advanced Models

Some researchers have explored hybrid models, which mix quantum and classical methods or use other resources such as quantum homomorphic encryption (where data can be processed without revealing it) or pre-shared entangled states between user and server. These models try to offer the best of both worlds the practicality of single-server systems and the low communication cost of multi-server ones [9].

Communication Complexity

These models show promise in reducing complexity, but they are still in the experimental stage and require further research and testing.

Table 1: Strength and Limitations of Different QPIR Models [3, 6, [9]]

Model Type	No. of Servers	Communication Cost	Practicality	Security Level
Multi-Server QPIR	2 or more	Low	Low	High
Single-Server QPIR	1	Moderate to High	High	Moderate
Hybrid Models	1 or more	Moderate	Medium	High

From the comparison of different QPIR models, we can see that each model has its own strengths and weaknesses. The multi-server QPIR model is very efficient in terms of communication it requires less data to be exchanged between the user and the servers. However, it is less practical in real-world situations because it depends on having two or more servers that do not communicate with each other, which is difficult to ensure. On the other hand, the single-server QPIR model is more practical because most systems in the real world use only one server. But it comes with a higher communication cost, meaning it takes more data and time to get the required information while keeping the user's query private. It is also harder to make it fully secure against all types of quantum attacks. Hybrid models are newer and try to combine the advantages of both multi-server and single-server models. These models aim for a balance between efficiency and practicality. They are not as efficient as multi-server models but more practical, and they can offer good security. However, many hybrid techniques are still under research and not fully developed for real use.

4. Efficiency Challenges in QPIR

Although Quantum Private Information Retrieval (QPIR) offers a promising way to protect user privacy while retrieving data, there are still several major challenges that affect its efficiency and practicality in real-world use. One of the biggest challenges is the need for advanced quantum hardware. QPIR protocols rely heavily on quantum technologies such as qubits, quantum memory, and secure quantum communication channels. However, current quantum systems are still in the early stages of development, and maintaining stable quantum states for a long time remains difficult due to noise and errors in quantum hardware. This makes it hard to implement QPIR protocols on a large scale using the technology available today [13].

Another key challenge is the high communication cost in practice. Even though QPIR is designed to reduce the amount of data exchanged between the user and the server, many existing protocols still involve a large amount of communication, especially when the database is large or when strong privacy is required. This becomes a problem when communication speed and bandwidth are limited. For example, in a single-server setting, the protocol may require the user to download a significant portion of the database just to retrieve one item privately, which makes the system inefficient [14], [15].

Moreover, there is an important trade-off between privacy and efficiency. Protocols that offer very strong privacy guarantees tend to be slower and require more resources. On the other hand, making the protocol faster and simpler often means sacrificing some level of privacy. Finding the right balance between these two aspects is a major research challenge. This trade-off becomes even more critical in systems where users expect fast responses but still want their data requests to remain private [16], [17], [20].

In addition to this, quantum systems are extremely sensitive to errors. Small disturbances in the system can affect the accuracy of the results or even corrupt the entire query. To deal with this, QPIR protocols often need to use error-correcting techniques, which add extra steps and increase communication costs. While error correction can improve reliability, it also makes the protocol more complex and harder to scale to large databases [18].

Finally, scalability is another major issue. Many QPIR protocols work well when dealing with small datasets, but they become inefficient when applied to large-scale databases. As the size of the data increases, so does the complexity of the protocol, and this can make it unsuitable for practical applications such as cloud storage or large information systems [19].

5. Open Research Problems and Future Directions

Although Quantum Private Information Retrieval (QPIR) has seen strong theoretical development, several open challenges remain before it can be used effectively in real-world applications. One major problem is designing practical and scalable single-server QPIR protocols. While many efficient protocols assume multiple non-communicating servers, such setups are hard to achieve in practice. Research study by [22] proposed a lattice-based single-server PIR model, but it still faces limitations in terms of performance and deployment [21, 24].

Another critical issue is the sensitivity of QPIR protocols to noise in quantum channels. Quantum communication can be affected by even small disturbances, leading to errors in retrieval [23]. The research study of [25] found that quantum neural networks work well for detecting noise in channels, even in both 2D and 3D setups, and they can be used for more complex systems too. Simpler networks actually performed better when trained for the same amount of time. One of the important settings, called lambda (λ), affects how fast the training goes. A smaller value helps the network learn faster, but if it's too small, it can cause problems, especially in more complex networks. So, the structure of the network and the value of λ should be chosen based on the specific problem [26].

Researchers are also exploring hybrid models that combine classical and quantum techniques. These models aim to leverage the privacy advantages of quantum systems with the affordability and accessibility of classical infrastructure. The research study [29] explores hybrid algorithms that combine classical and quantum computing to overcome their individual limitations. Classical computers struggle with complex problems due to scalability issues, while quantum computers are still limited by undeveloped hardware. The study introduces the Quantum Metropolis Solver (QMS), which blends quantum walk and the Metropolis-Hastings method. QMS performed better than classical methods in real-world areas like AI, energy, and chemistry, both in simulation and on quantum hardware. However, challenges remain due to the current limitations of quantum hardware, such as noise and limited capacity for large data processing [27, 28].

Additionally, understanding the communication complexity of QPIR remains an open theoretical question. The research study [30] focuses on improving the efficiency and understanding of secure communication systems. The first major finding is that the authors were able to figure out the exact minimum number of bits that a sender needs to communicate during the commit stage of a system based on trapdoor permutations. This lower bound perfectly matches the known upper limit, making their result very accurate. The second contribution is an improvement in how statistically-hiding commitment schemes (which keep information private) are linked to single-server PIR (Private Information Retrieval) systems, allowing the whole process to use less communication and become more efficient. However, reaching these results came with challenges. It was difficult to prove the tight lower bound while making sure the security of the system wasn't compromised. Also, improving the connection between commitment schemes and PIR required careful planning to reduce communication without weakening privacy or security.

Finally, it is important to test and implement QPIR models on real quantum hardware to evaluate their practical performance. Programs like DARPA's Quantum Benchmarking Initiative (2024) are actively working on validating theoretical quantum algorithms through real-world experimentation [32]. The study [31] described the goal of the Quantum Benchmarking Initiative which is to figure out whether any current approach to quantum computing can become truly useful by 2033. It plays an important role in advancing Quantum Private Information Retrieval (QPIR) by providing a practical platform to test and evaluate quantum algorithms on real hardware. Since many QPIR protocols are still theoretical, this initiative helps researchers identify how these protocols perform under real-world conditions, including the effects of quantum noise and hardware limitations. By enabling experimental validation, DARPA's efforts support the development of more reliable and efficient QPIR systems, ultimately helping to bridge the gap between theory and practical application in secure quantum data retrieval.

Conclusion and Suggestions

In conclusion, this study has explored the concept of Quantum Private Information Retrieval (QPIR), with a focus on communication complexity and efficiency challenges. We have reviewed the basic principles, existing models, and current research in the field and it is clear that while QPIR offers strong privacy guarantees, several limitations still hinder its practical implementation. Most current QPIR protocols, especially those based on single-server settings, suffer from high communication costs, sensitivity to noise, and limited scalability. Multi-server models show better efficiency, but they rely on unrealistic assumptions like non-communicating servers, which are difficult to achieve in practice.

Through the comparison of existing QPIR schemes, it is evident that there is a trade-off between privacy, communication efficiency, and system complexity. Furthermore, the lack of robust protocols that can function over noisy quantum channels and the absence of clear communication complexity lower bounds highlight the need for more research. The study also finds that real-world implementation and testing are still missing in many proposed models, making it difficult to judge their practical value.

To address these issues, future research should focus on developing practical and scalable single-server QPIR protocols, designing schemes that are resilient to quantum noise, and exploring hybrid models that combine the strengths of both classical and quantum systems. It is also important to test QPIR protocols using real quantum devices, such as those supported by DARPA's Quantum Benchmarking Initiative, to validate their performance under realistic conditions. Additionally, continued theoretical work is needed to better understand the communication limits and optimize the efficiency of QPIR systems.

References

1. Fanti G, Ramchandran K. Efficient private information retrieval over unsynchronized databases. IEEE J Sel Top Signal Process. 2015;9(7):1229-39. doi:10.1109/JSTSP.2015.2432740.
2. Allaix M. Quantum private information retrieval from coded storage systems [Preprint]. arXiv. 2023 Dec 10. Available from: https://arxiv.org/abs/2312.07570
3. Song S, Hayashi M. Capacity of quantum private information retrieval with multiple servers. IEEE Trans Inf Theory. 2020;PP:1-1. doi:10.1109/TIT.2020.3022515.
4. Sun J, Yuan X, Tsunoda T, Vedral V, Benjamin S, Endo S. Mitigating realistic noise in practical noisy intermediate-scale quantum devices. Phys Rev Appl. 2021;15:034026. doi:10.1103/PhysRevApplied.15.034026.
5. Song S, Hayashi M. Capacity of quantum private information retrieval with multiple servers. IEEE Trans Inf Theory. 2021;67(1):452-63. doi:10.1109/TIT.2020.3022515.
6. Song S, Le Gall F, Hayashi M. Prior entanglement exponentially improves one-server quantum private information retrieval for quantum messages. EPJ Quantum Technol. 2024;11(1):1-25.
7. Gall F. Quantum private information retrieval with sublinear communication complexity. Theory Comput. 2012;8:369-97. doi:10.4086/toc.2012.v008a016.
8. Baumeler Ä, Broadbent A. Quantum private information retrieval has linear communication complexity. J Cryptol. 2015;28(1):161-75. doi:10.1007/s00145-014-9180-2.
9. Song W, Zeng G, Zhang W, *et al*. Research on privacy information retrieval model based on hybrid homomorphic encryption. Cybersecurity. 2023;6:31. doi:10.1186/s42400-023-00168-7.
10. Song S, Hayashi M. Quantum private information retrieval for quantum messages. In: Proc IEEE Int Symp Inf Theory (ISIT). 2021; p.1052-7.
11. Tak JW, Kim SH, Kim Y, No JS. Weakly private information retrieval under Rényi divergence [Preprint]. arXiv. 2021. doi:10.48550/arXiv.2105.08114.
12. Sun H, Jafar SA. The capacity of private information retrieval. IEEE Trans Inf Theory. 2017;63(7):4075-88. doi:10.1109/TIT.2017.2689028.
13. Yang YG, Yang PZ, Xu GB, Zhou YH, Shi WM. Quantum private information retrieval over a collective noisy channel. Mod Phys Lett A. 2023;38(01). doi:10.1142/S0217732323500013.
14. Kerenidis I, Lauriere M, Le Gall F, Rennela M. Information cost of quantum communication protocols. Quantum Inf Comput. 2016;16:181-96.
15. Luo M, Wang M. Faster spiral: Low-communication, high-rate private information retrieval. Cryptography. 2025;9(1):13. doi:10.3390/cryptography9010013.
16. Khan A, Khalid U, Ur Rehman J, Shin H. Quantum anonymous private information retrieval for distributed networks. IEEE Trans Commun. 2022;70:1-1. doi:10.1109/TCOMM.2022.3168079.
17. Allaix M. Quantum private information retrieval from coded storage systems. arXiv. 2023. arXiv:2312.07570.
18. Giovannetti V, Lloyd S, Maccone L. Quantum private queries. Phys Rev Lett. 2008;100:230502. doi:10.1103/PhysRevLett.100.230502.
19. Khoshgozaran A, Shirani-Mehr H, Shahabi C. SPIRAL: A scalable private information retrieval approach to location privacy. In: MDMW 2008. p.55-62. doi:10.1109/MDMW.2008.23.
20. Kon WY, Lim CCW. Provably secure symmetric private information retrieval with quantum cryptography. Entropy. 2021;23(1):54. doi:10.3390/e23010054.
21. Davidson A, Pestana G, Celi S. FrodoPIR: Simple, scalable, single-server private information retrieval. Proc Priv Enhancing Technol. 2023;2023(2):365-83. doi:10.56553/popets-2023-0022.
22. Melchor C, Gaborit P. A lattice-based computationally-efficient private information retrieval protocol. IACR Cryptol ePrint Arch. 2007;2007:446.
23. Yang Y, Yang P, Xu G, Zhou Y, Shi W. Quantum private information retrieval over a collective noisy channel. Mod Phys Lett A. 2023;38(01). doi:10.1142/s0217732323500013.

24. Menon SJ, Wu DJ. Spiral: Fast, high-rate single-server PIR via FHE composition. In: 2022 IEEE Symp Secur Privacy (SP). 2022; p.930-47.
25. Song J, Lu B, Liu L, Wang C. Noisy quantum channel characterization using quantum neural networks. Electronics. 2023;12(11):2430. doi:10.3390/electronics12112430.
26. Barnum H, Nielsen MA, Schumacher B. Information transmission through a noisy quantum channel. Phys Rev A. 1998;57(6):4153-75. doi:10.1103/physreva.57.4153.
27. Terno DR. Classical-quantum hybrid models [Preprint]. arXiv. 2023 Sep 10. Available from: https://arxiv.org/abs/2309.05014
28. Ricci S, Dobias P, Malina L, Hajny J, Jedlicka P. Hybrid keys in practice: Combining classical, quantum and post-quantum cryptography. IEEE Access. 2024;PP:1-1. doi:10.1109/ACCESS.2024.3364520.
29. Hybrid quantum-classical algorithms [Preprint]. arXiv. Available from: https://arxiv.org/html/2406.12371v1
30. Haitner I, Hoch JJ, Segev G. A linear lower bound on the communication complexity of single-server private information retrieval [Preprint]. IACR Cryptol ePrint Arch. 2007;2007:351.
31. New DARPA initiative challenges the creation of operational quantum computers. AFCEA Int. 2025 Apr 7. Available from: https://www.afcea.org/signal-media/emerging-edge/new-darpa-initiative-challenges-creation-operational-quantum-computers
32. Tripathi P. DARPA's quantum benchmarking initiative: A make-or-break for quantum computing. Observer Res Found (ORF). 2025 May 6. Available from: https://www.orfonline.org/expert-speak/darpa-s-quantum-benchmarking-initiative-a-make-or-break-for-quantum-computing