A data protection coding method based on information theory and quantum technologies

Rostislav Motsyk[1,*,†], Serhii Toliupa[2,†], Tetiana Pylypiuk[1,†], Kateryna Heseleva[1,†], Oleksiy Vovk[3,†] and Oleksandr Matviichuk-Yudin[4,†]

[1]Kamianets-Podilskyi Ivan Ohiienko National University, Ivan Ohiienko Str., 61, Kamianets-Podilskyi, 32301, Ukraine
[2]Taras Shevchenko National University of Kyiv, Volodymyrska Str., 60, Kyiv, 03022, Ukraine
[3]Ivan Kozheduba Kharkiv National Air Force University, Sumska Str., 77/79, Kharkiv, 61023, Ukraine
[4]National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute", Beresteyskyi Ave., 37, Kyiv, 03056, Ukraine

Abstract

The rapid development of quantum computers presents both new opportunities and challenges for information security. Traditional cryptographic methods may prove ineffective against attacks leveraging quantum computing. This paper proposes the use of information theory principles to develop new data protection methods for quantum computing systems. It presents an approach based on the entropic analysis of quantum communication channels and the application of quantum coding to ensure confidentiality, integrity, and availability of data.

Keywords

quantum computers, information theory, entropy, quantum coding, information security

1. Introduction

The rapid advancement of quantum computing opens up new possibilities for solving complex computational problems. However, it also poses new challenges for information security. Traditional cryptographic methods, based on the complexity of factorization or discrete logarithms, can be broken by quantum algorithms such as Shor's algorithm [1]. Information theory, as the fundamental basis for coding, transmission, and processing of data, can be crucial in developing new information protection methods for quantum computing systems. Concepts such as entropy, mutual information, and quantum coding can be applied to ensure the confidentiality, integrity, and availability of data.

2. The main material presentation

Recent research in the field of data protection methods based on information theory for quantum computing systems has focused on the following key areas:

1. Quantum Key Distribution (QKD):

   - Development of continuous-variable-based QKD protocols for better efficiency;
   - Integration of QKD into existing fiber-optic networks;
   - Satellite-based QKD for secure long-distance communication.

2. Quantum Error Correction (QEC):

   - Optimization of QEC codes for specific quantum hardware platforms;

CH&CMiGIN'25: Fourth International Conference on Cyber Hygiene & Conflict Management in Global Information Networks, June 20–22, 2025, Kyiv, Ukraine
*Corresponding author.
†These authors contributed equally.
motsyk@kpnu.edu.ua (R. Motsyk); tolupa@i.ua (S. Toliupa); pylypyuk.tetiana@kpnu.edu.ua (T. Pylypiuk); heseleva@kpnu.edu.ua (K. Heseleva); aponnir@ukr.net (O. Vovk); ssmy41020@gmail.com (O. Matviichuk-Yudin)
0000-0003-0947-3579 (R. Motsyk); 0000-0002-1919-9174 (S. Toliupa); 0000-0002-4676-9830 (T. Pylypiuk); 0009-0009-2619-5604 (K. Heseleva); 0000-0002-2350-9059 (O. Vovk); 0009-0006-2658-0228 (O. Matviichuk-Yudin)

- Fault tolerance in quantum computing architecture;
- Machine learning for decoding QEC codes.

3. Quantum-Resistant Cryptography:

- Dissemination of NIST post-quantum cryptography standardization;
- Hybrid classical-quantum homomorphic encryption schemes.

4. Quantum Random Number Generation (QRNG):

- Device-independent QRNG protocols;
- Integration of QRNG into consumer devices and cloud services;
- Continuous-variable QRNG for further increasing the generation rates.

5. Quantum Secure Direct Communication (QSDC):

- Experimental demonstrations of the different QSDC protocols;
- A study on practical feasibility and limitations concerning QSDC.

6. Quantum Homomorphic Encryption (QHE):

- Development of more efficient QHE schemes;
- Hybrid approaches toward homomorphic encryption-classical and quantum.

7. Quantum Information Scrambling:

- Experimental demonstration of information scrambling in quantum systems.

Consider theoretical relations to black hole physics and holography. These research areas aim to develop practical and efficient data protection methods for quantum computing systems, combining knowledge from quantum physics, computer science, and information theory.

This paper proposes an approach based on the entropic analysis of quantum communication channels and the application of quantum coding for data protection in quantum computing systems. The key aspects discussed include:

1. Entropic analysis of quantum communication channels.
2. Quantum coding for ensuring data confidentiality.
3. Application of quantum coding for ensuring data integrity and availability.

If consider entropic analysis of quantum communication channels we can ascertain that entropy is a fundamental concept in information theory that characterizes the uncertainty or amount of information contained in a message or system. In classical information theory, entropy is defined as:

$$H(X) = -\sum p(x) \log p(x), \tag{1}$$

where X is a random variable and $p(x)$ is the probability of x.

In the quantum case, entropy is defined through the density matrix p of the system:

$$S(p) = -Tr(p \log p), \tag{2}$$

where Tr $(\bullet)$ denotes the trace of the matrix.

For a quantum communication channel, the Holevo entropy [2] is defined as:

$$H(A|B) = S(p_{AB}) - S(p_B), \tag{3}$$

where p_{AB} is the joint state of systems A and B, and p_B is the state of system B.

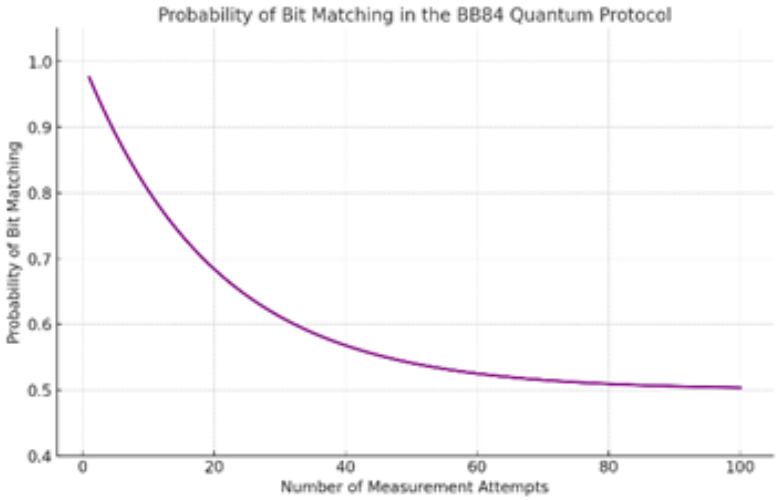

Figure 1: The graph of the dependence of mutual information on the level of noise in the channel.

Entropic analysis of quantum channels allows us to estimate the amount of information leaking through the channel and identify potential vulnerabilities in the system. This is crucial for developing data protection methods.

Why is entropy important for quantum channel analysis? From different researches we can say as answer for this question:

1) the greater the entropy, the more information the system contains;

2) entropy is used to characterize the degree of entanglement of quantum systems;

3) an increase in noise in a channel leads to an increase in entropy, which can indicate a loss of information;

4) malicious activities can affect the entropy of the system, which allows them to be detected.

Consider a quantum channel that converts the input state ρ into the output state $\rho\prime$. Entropy analysis allows you to estimate how much information is lost during transmission through a channel.

As to mutual information that it shows how much information about the input state is contained in the output.

$$I(\rho, \rho\prime) = S(\rho) + S(\rho\prime) - S(\rho \otimes \rho\prime), \tag{4}$$

where $\otimes$ is the tensor product.

Conditional entropy describes the uncertainty about the initial state if the input is known.

$$H(\rho\prime|\rho) = S(\rho \otimes \rho\prime) - S(\rho). \tag{5}$$

Graphic interpretation is presented in Figure1 [1].

It can be seen that with an increase in noise, the mutual information decreases, indicating a loss of information.

Let's consider quantum coding for ensuring data confidentiality. To ensure data confidentiality in quantum computing systems, quantum coding methods can be applied. One approach is to use quantum cryptographic protocols. Particularly the quantum cryptographic protocol BB84 [3, 4, 5]:

$$|\psi\rangle = (|0\rangle + e^{i\phi}|1\rangle)/\sqrt{2}, \tag{6}$$

where ϕ is a random phase, is enable to establish for two parties a secure key that can subsequently be used for data encryption. Leveraging the principles of quantum mechanics, these protocols provide a robust level of security.

Key steps in the BB84 protocol:

1. The sender sends random bits encoded in one of two possible bases (standard or diagonal).

2. The receiver randomly chooses a basis for measuring each received bit.

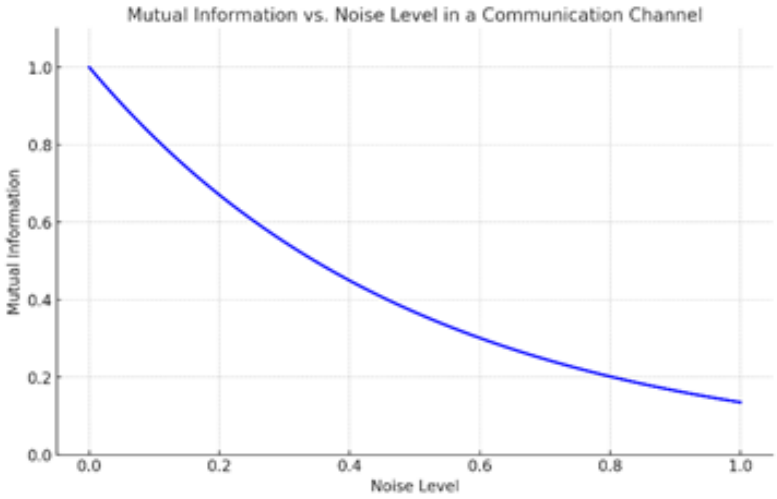

Figure 2: The graph showing the probability of bit matching in the BB84 quantum protocol [2].

3. Sender and receiver communicate to compare the bases used for each bit (but not the bits themselves).

4. Secret key creation. They keep only those bits where the bases match, forming a secret key.

A dependence of the probability of receiver correct bit detection on the number of measurement attempts is shown in Figure 2. This represents how using random bases affects the accuracy of the generated key.

In addition to the BB84 protocol, there are several other protocols in quantum cryptography that provide secure key distribution or other forms of information protection. Here are some of them:

1. Protocol B92. A simplified version of BB84 that uses only two quantum states instead of four. It is less resistant to some attacks, but may be easier to implement.

2. E91 protocol (Eckert scheme). This protocol is based on the principle of entangled states and uses pairs of entangled photons, and the security is based on the Einstein-Podolsky-Rosen (EPR) paradox and Bell's inequalities. The protocol makes it possible to verify whether a third party was present trying to intercept the key, thanks to quantum entanglement.

3. Skiddington Protocol (SARG04). An improved protocol similar to BB84, but with greater resistance to certain types of attacks such as photon splitters. Uses the same states as BB84, but changes the way information is exchanged for better stability.

4. Quantum protocols with a cross base includes schemes where transferred states are used in bases that are difficult to predict. These techniques help detect entanglement due to changes in the properties of quantum states.

5. Protocols based on entangled states. In addition to the E91 protocol, there are other methods that use quantum entanglement to distribute keys or authenticate data transmissions. For example, methods based on cluster states or multilateral entangled systems.

6. Continuous-variable QKD (CV-QKD) uses quantum properties of light (many possible values of variables) instead of individual photons. This approach allows the use of standard telecommunications equipment, which simplifies integration with existing systems.

7. DPS (Differential Phase Shift) protocol based on the use of a phase shift between successive light pulses. The protocol is less vulnerable to some photon-based attacks and provides effective protection in various data transmission conditions.

8. Confluence Protocol (Device-independent QKD). This type of protocol is independent of the specific hardware used and provides security even in the presence of potentially untrusted devices. Based on a test of Bell's inequalities.

9. Twin-Field QKD is a new protocol that allows you to significantly increase the distance of data transmission in quantum cryptography. Uses interference field techniques to increase safety and range.

These protocols extend the capabilities of quantum cryptography by adapting it to different scenarios and security requirements. Each of them has its own characteristics, advantages and limitations, which are important to consider when choosing for a specific application.

Quantum cryptographic protocols enable the establishment of a secret key between two parties, which can then be used to encrypt data. A key advantage is that unauthorized access to the quantum channel can be detected due to the fundamental laws of quantum mechanics.

In addition to ensuring confidentiality, quantum coding can be used to ensure data integrity and availability in quantum computing systems.

For ensuring data integrity, quantum error-correcting codes such as the Steane code [5] can be applied:

$$|\psi\rangle = (|0\rangle + |1\rangle)/\sqrt{2} \rightarrow |\psi_{encoded}\rangle = (|000\rangle + |111\rangle)/\sqrt{2}. \quad (7)$$

These codes allow the detection and correction of errors that may occur during the transmission or storage of data in quantum systems.

To ensure data availability in distributed quantum computing systems, methods like quantum error-correcting codes are used to increase data resilience. One of the most well-known approaches is Shor's code, which encodes quantum states to protect against noise and data loss.

Key steps for ensuring data availability using Shor's code [6]:

Step 1. Quantum State Encoding: an input qubit (primary data unit) is duplicated into a superposition across nine qubits, which increases its resilience to errors.

This can be formally represented as:

$$|\psi\rangle = \alpha|0\rangle + b|1\rangle) \rightarrow |\psi\rangle = \alpha|0_l\rangle + b|1_l\rangle), \quad (8)$$

where $|0_l\rangle$ and $|1_l\rangle$ represent logical qubits encoded for error protection.

Step 2. Error detection. If a random error occurs, quantum operations can detect and correct one of the possible errors (e.g., bit-flip or phase-flip).

In classical computing, errors can be detected and corrected using redundancy. For instance, a single bit of information can be encoded into three bits, and if one of these bits flips, the majority vote can correct the error.

Quantum computing, however, faces a unique challenge: the delicate nature of quantum states. Noise and decoherence can easily disrupt these states, leading to errors.

A simple quantum error correction code is the bit-flip code. It can detect and correct a single bit-flip error. To encode a single qubit, we use three qubits:

1. Q0=0; Q1=0; Q2=0.

2. Q0=1; Q1=1; Q2=1.

For error detection and correction let's say a bit-flip error occurs on Q1. The state becomes: Q0=0; Q1=1; Q2=0.

To detect and correct this error, we apply a series of quantum gates. For parity check we apply a controlled-NOT (CNOT) gate between Q0 and Q1, and another CNOT gate between Q1 and Q2. This creates a parity check, where the parity of the three qubits should always be even.

If the parity check fails, for error correction we can identify the error location by measuring the parity of Q0 and Q2. If the parity of Q0 and Q2 is odd, the error is on Q1. We can then apply a NOT gate to Q1 to correct the error.

While a full mathematical treatment involves density matrices and quantum operations, a simplified representation can be given using Dirac notation.

Original state: $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$.

Encoded state: $|\psi\rangle = \alpha|000\rangle + \beta|111\rangle$.

Bit-flip error on Q1: $|\psi\rangle \rightarrow \alpha|010\rangle + \beta|101\rangle$.

As error correction is applying appropriate gates to recover the original state, beyond bit-flip codes.

Step 3. Data Recovery. Using specific quantum operations, the original state can be recovered even after some qubits are damaged, thus maintaining overall data availability.

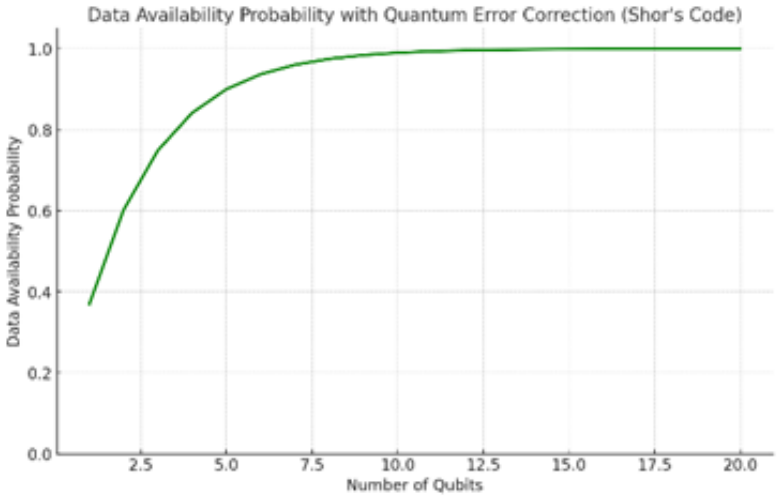

Figure 3: The graph demonstrating the probability of data availability in a distributed quantum computing system using error correction, specifically Shor's code [5].

Below is a graph (Figure 3) that illustrates the probability of data availability in a system using quantum error correction, as a function of the number of qubits. The graph shows that as more qubits are added to the error-correcting process, data availability improves.

As the number of qubits involved in error correction increases, the probability of maintaining data availability also rises, highlighting the effectiveness of quantum error correction for data resilience in noisy environments.

Quantum teleportation allows the transfer of an arbitrary quantum state between two parties using a classical communication channel and a pre-established quantum channel. This can be applied to ensure data availability in distributed quantum computing systems [7, 8].

More complex quantum error correction codes, such as the Shor code and the surface code, can detect and correct multiple errors, including phase-flip errors and combinations of both. These codes are essential for building large-scale, fault-tolerant quantum computers [9, 10].

While quantum error correction is a complex field, understanding the basic principles of error detection and correction is crucial for appreciating the potential and challenges of quantum computing.

3. Conclusions

The novelty of our study is to investigate data protection methods for quantum computing systems. We consider the entropy analysis of quantum communication channels to estimate the amount of information, the possibility of identifying potential vulnerabilities in the system of key steps to ensure data availability using the Shor code.

1. It is substantiated that methods of data coding based on information theory for quantum computing systems are focused on such key areas as: quantum key distribution (QKD); quantum error correction (QEC); quantum random number generation (QRNG); quantum coding of information.
2. It has been argued that in order to ensure data availability in distributed quantum computing systems, techniques such as quantum error-correcting codes are used to improve data robustness. The focus is on one of the most well-known approaches, the Shor code, which encodes quantum states to protect against noise and data loss, because these more sophisticated quantum error-correction codes, such as the Shor code and the surface code, can detect and correct numerous errors and are necessary to create large-scale, fault-tolerant quantum computers.
3. An approach based on the entropy analysis of quantum communication channels and the application of quantum coding for data protection in quantum computing systems is proposed, since for the entropy analysis of quantum communication channels, entropy is a fundamental concept

that makes it possible to estimate the amount of information flowing through the channel, and identify potential vulnerabilities in the system, which is important for developing data protection methods.

4. Quantum coding ensures that any attempt to change or affect the transmitted data will be impossible without disrupting the quantum states, which automatically reports the tampering attempt.
5. Although quantum systems have not yet become widespread, research in this field already allows the creation of highly attack-resistant network protocols that provide a high level of availability thanks to the use of the unique physical properties of quantum particles.
6. The combination of classical and quantum methods of protection, which is based on the concepts of entropy and mutual information, made it possible to significantly increase the level of data protection. The use of quantum coding opens up new opportunities for creating more reliable and secure communication systems.

Declaration on Generative AI

The authors have not employed any Generative AI tools.

References

[1] P. Shor, Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer, SIAM Journal on Computing 26 (1997) 1484–1509.

[2] A. S. Holevo, Quantum Systems, Channels, Information: A Mathematical Introduction, Studies in Mathematical Physics, De Gruyter, 2012.

[3] M. A. Nielsen, I. L. Chuang, Quantum Computation and Quantum Information, volume 710, Cambridge University Press, 2010.

[4] Z. Hu, S. Gnatyuk, T. Okhrimenko, S. Tynymbayev, M. Iavich, High-speed and secure prng for cryptographic applications, International Journal of Computer Network and Information Security 12 (2020) 1–10. doi:10.5815/ijcnis.2020.03.01.

[5] Y. Baseri, V. Chouhan, A. Hafid, Navigating quantum security risks in networked environments: A comprehensive study of quantum-safe network protocols, Computers and Security 142 (2024) 103883.

[6] V. Barannik, M. Lytvinenko, D. Okladnoy, O. Suprun, Description of the ofdm symbol with the help of mathematical laws. analysis of technologies that were used in this case, in: Proceedings of the 2nd International Conference on Advanced Information and Communication Technologies (AICT), 2017, pp. 183–187. doi:10.1109/AIACT.2017.8020095.

[7] V. Barannik, D. Barannik, V. Fustii, M. Parkhomenko, Evaluation of effectiveness of masking methods of aerial photographs, in: Proceedings of the 3rd International Conference on Advanced Information and Communications Technologies (AICT), 2019, pp. 415–418. doi:10.1109/AIACT.2019.8847820.

[8] V. Barannik, A. Hahanova, A. Slobodyanyuk, Architectural presentation of isotopic levels of relief of images, in: Experience of Designing and Application of CAD Systems in Microelectronics - Proceedings of the 10th International Conference (CADSM), 2009, pp. 385–387.

[9] V. Barannik, A. Shiryaev, Quadrature compression of images in polyadic space, in: Modern Problems of Radio Engineering, Telecommunications and Computer Science - Proceedings of the 11th International Conference (TCSET), 2012, p. 422.

[10] V. Barannik, N. Kharchenko, O. O. Shadi, A. Musienko, A method to control bit rate while compressing predicted frames, in: Proceedings of the 13th International Conference on the Experience of Designing and Application of CAD Systems in Microelectronics (CADSM), 2015, pp. 36–38. doi:10.1109/CADSM.2015.723078.