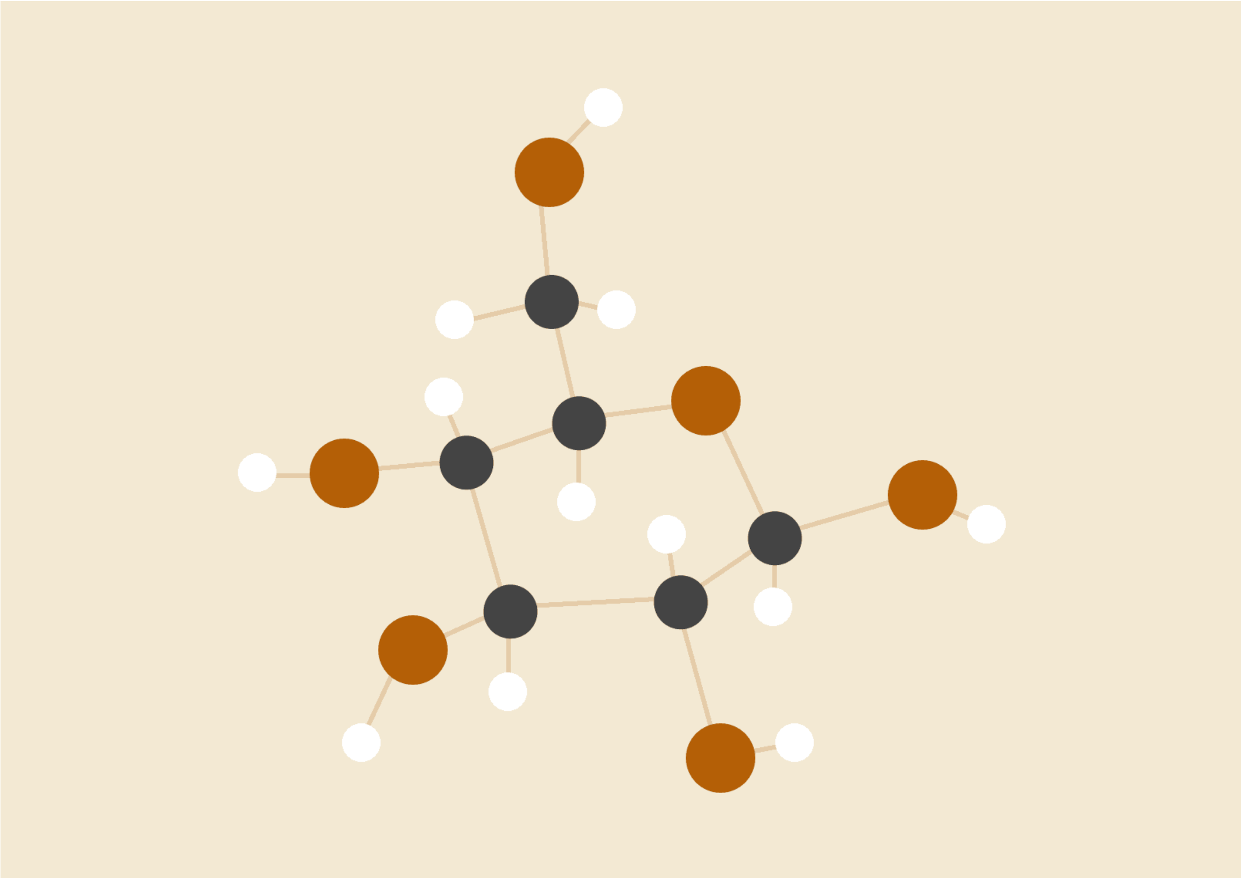
QUANTUM INTERNET APPLICATION

Enhancing QKD Performance with QND Measurements in QEC Codes



Hoceini Rihab

20/10/2023

QIA– Quantum Internet Alliance

Quantum Key Distribution (QKD) is a pivotal technology for quantum internet applications, ensuring secure communication through the exchange of quantum keys. The reliability and security of QKD systems depend on efficient error correction mechanisms, among other factors. In this section, we explore how integrating Quantum Non-Demolition (QND) measurements into Quantum Error-Correcting (QEC) codes can significantly impact the Secret Key Rate (SKR) in QKD systems.

INTRODUCTION

A quantum internet is a hypothetical network that utilizes the principles of quantum mechanics to enable secure communication and quantum information sharing between distant parties. It achieves this through quantum key distribution (QKD) protocols that provide a foundation for secure communication between quantum nodes.

THE QKD SYSTEM

The QKD system is a fundamental component of the quantum internet, ensuring secure key distribution to safeguard transmitted data from potential attacks, even against powerful quantum computers.

THE FINITE KEY-SKR

The Secure Key Rate (SKR) represents the rate at which secure key bits can be generated in a QKD system, accounting for real-world limitations and imperfections.

The finite-key SKR is a crucial measure, considering various factors like error rates, qubit transmission losses, and other parameters. It provides an estimate of the achievable key generation rate under realistic conditions, where the number of exchanged qubits is finite.

THE QUANTUM ERROR CORRECTION

The selection of an error-correcting code in a Quantum Key Distribution (QKD) system has a profound impact on performance, particularly concerning "Code Rate" and "Key Generation Rate" (SKR).

Code Rate: This rate represents the ratio of useful qubits to total qubits in a QKD system. It plays a pivotal role in determining the efficiency of key generation. A higher code rate results in a faster key generation rate but may compromise error correction capabilities.

Key Generation Rate (SKR): The SKR is a critical metric assessing a QKD system's efficiency, and it directly depends on the code rate. Opting for an error-correcting code with a higher code rate can accelerate key generation, enhancing overall system perform

INTEGRATION QND MEASUREMENTS INTO QEC CODES:

Integrating Quantum Non-Demolition (QND) measurements into Quantum Error-Correcting (QEC) codes within Quantum Key Distribution (QKD) systems promises to significantly enhance system efficiency and the Secret Key Rate (SKR). This approach allows for non-invasive error correction, reducing error rates and improving QKD performance. However, successful integration requires careful resource management, system adaptation, and possible experimentation for optimization. In conclusion, the inclusion of QND measurements in QEC codes fortifies quantum communication, ensuring higher SKR and heightened security in quantum internet applications.

CALCULATING QND MEASUREMENTS FIDELITY :

The formula for calculating the fidelity of a Quantum Non-Demolition (QND) measurement, denoted as F_QND, is defined as:

$$F\_QND = F (p\_in , p\_out)$$

Where:

- **p_in** represents the probability distribution of the input state.
- **p_out** represents the probability distribution of the state after the QND measurement.

This fidelity measure ranges from 0 to 1, with a value of 1 indicating that the input and output probability distributions are identical.

ANALYSIS :

1- Calculation of Secret Key Rate (SKR):

To assess the efficiency and security of our Quantum Key Distribution (QKD) system, we initiate our analysis by calculating the Secret Key Rate (SKR). This pivotal metric is essential for evaluating the performance of our system in generating secure keys. The SKR is determined using the following equation:

$$SKR = [s\_lZ,0 + s\_lZ,1(1 - h(\phi\_uZ)) - f \cdot nZ \cdot h(EZ) - 6\,log2\ (19/\epsilon sec) - log2(2/\epsilon cor)]\ /\ t$$

Where:

- **s_lZ,0 and s_lZ,1:** lower bounds on the number of single-photon contributions and vacuum-state contributions in the sifted keys.
- **h(ϕ_uZ):** an upper bound on the single-photon phase-error rate (ϕ_uZ).
- **f:** the efficiency of the error correction code.
- **nZ:** the sifted key length in the Z basis.
- **h(EZ):** the bit error rate in the Z basis (EZ).
- **ϵsec and ϵcor:** the secrecy and correctness parameters, respectively.
- **t:** the data accumulation time.

2- the key parameters of the Secret Key Rate (SKR) equation.

These parameters are based on prior research and are derived from the hardware setup and Quantum Error-Correcting (QEC) code used.

The specific parameter values are as follows:

sZ1: 1000 single-photon contributions in the Z basis

sZ0: 1000 vacuum-state contributions in the Z basis

phi_uZ: 0.01 upper bound on single-photon phase-error rate

f: 1.053 efficiency of the error correction code

nZ : 10^{8} sifted key length in Z basis

EZ: 0.05 bit error rate in Z basis

epsilon_sec: 10^{-10} secrecy parameter

epsilon_cor: 10^{-15} correctness parameter

t: 0.01 data accumulation time

They form the basis for our subsequent analysis, where we explore their impact on SKR within the Quantum Key Distribution (QKD) system

3- Exploring the Impact of FQND on SKR:

High Fidelity (F_QND ≈ 1): A measurement process with a high F_QND value is desirable for QKD systems. This is because it helps maintain the quality and security of the generated keys. When the measurement process is non-destructive and preserves the quantum properties of the keys, the SKR can potentially be higher. Higher fidelity in measurement contributes to a more efficient and secure key generation process.

CONCLUSION

the integration of Quantum Non-Demolition (QND) measurements into a Quantum Key Distribution (QKD) system offers significant advantages for achieving higher Secure Key Rates (SKR). The analysis demonstrated that QND measurements reduce the need for extensive Quantum Error Correction procedures, resulting in more efficient key generation.

Moreover, QND measurements led to improved parameter estimations, enhancing the security and correctness of the QKD system. the decrease in secrecy and correctness parameters, directly contributes to a higher SKR, making the system more practical for real-world applications where high-speed secure communication is essential.

The findings indicate that QND measurements can significantly advance the field of quantum internet and quantum key distribution, ultimately making secure quantum communication more accessible and robust in the face of potential threats.

REFERENCES :

1. Victor Lovic , **"Quantum Key Distribution: Advantages, Challenges and Policy"**
2. Insérez Wei Li1 , Likang Zhang , Hao Tan , Yichen Lu , Sheng-Kai Liao , Jia Huang4 , Hao Li , Zhen Wang , Hao-Kun Mao , Bingze Yan , Qiong Li , Yang Liu , Qiang Zhang , Cheng-Zhi Peng , Lixin You , Feihu Xu, Jian-Wei Pan , **" High-rate quantum key distribution exceeding 110 Mb/s "** , arXiv 5 Jul 2023
3. T. C. Ralph, S. D. Bartlett, J. L. O'Brien, G. J. Pryde, and H. M. Wiseman , **" Quantum nondemolition measurements for quantum information "** , 31 January 2006