Quantum Entanglement in Photonic Quantum Computing and Cryptography: Theoretical Background and Simulations

Mohammed Nadir
Faculty of Engineering and Natural Sciences, Tampere University, Finland
email:mohammed.nadir.fi@ieee.org

***Abstract*—Quantum entanglement is a cornerstone of quantum mechanics and has profound implications for quantum computing and cryptography. This article explores the theoretical underpinnings of quantum entanglement in photonic systems, its application in quantum computing with qubits, and its role in quantum cryptography. We present the mathematical models and verification through simulations, including Bell test experiments and Quantum Key Distribution (QKD) protocols. The results show the feasibility of photonic qubits in secure communication and highlight future prospects for practical applications.**

I. Introduction

Quantum entanglement, a phenomenon where particles exhibit correlated behaviors regardless of distance, has revolutionized our understanding of quantum mechanics. Photonic qubits, due to their robustness against decoherence and ease of manipulation, serve as an ideal platform for implementing quantum computing and cryptographic protocols [1]. This paper delves into the theoretical background of quantum entanglement, demonstrates key experiments using simulations, and discusses the implications for future technologies [2].

II. Mathematical Background

Quantum entanglement can be mathematically represented through entangled states, such as Bell states. These states form a basis for two-qubit systems and are crucial for understanding quantum correlations [3].

A. Two-Qubit Systems and Bell States

In quantum mechanics, a qubit is the basic unit of quantum information, analogous to a bit in classical information theory. A single qubit can be in a superposition of the states $|0\rangle$ and $|1\rangle$, which are typically represented as:

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \quad |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

A two-qubit system consists of two such qubits, and its state can be represented in the combined basis $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$. The state of a two-qubit system can thus be written as:

$$|\psi\rangle = \alpha|00\rangle + \beta|01\rangle + \gamma|10\rangle + \delta|11\rangle$$

where $\alpha, \beta, \gamma, \delta$ are complex coefficients that satisfy the normalization condition $|\alpha|^2 + |\beta|^2 + |\gamma|^2 + |\delta|^2 = 1$.

Bell states are a specific set of maximally entangled quantum states of two qubits. They are named after physicist John Bell, who formulated Bell's theorem. The four Bell states are:

$$\begin{aligned} |\Phi^+\rangle &= \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle), \\ |\Phi^-\rangle &= \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle), \\ |\Psi^+\rangle &= \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle), \\ |\Psi^-\rangle &= \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle). \end{aligned} \tag{1}$$

These states form an orthonormal basis for the space of two qubits and are used to demonstrate quantum entanglement. Each Bell state represents a situation where the measurement outcomes of the two qubits are perfectly correlated or anti-correlated [7].

Entanglement is a quantum phenomenon where the quantum states of two or more objects are interconnected, such that the state of one object cannot be described independently of the state of the other(s). This leads to correlations between the measurement outcomes of entangled particles that are stronger than those predicted by classical physics [4].

For instance, if we measure both qubits of the $|\Phi^+\rangle$ state along the same axis, we always find them in the same state (both 0 or both 1), showing perfect correlation. Similarly, in the $|\Psi^+\rangle$ state, measurements along the same axis will always yield opposite outcomes (one 0 and one 1), showing perfect anti-correlation [8].

B. Spontaneous Parametric Down-Conversion (SPDC)

SPDC is a nonlinear optical process in which a photon (the pump photon) passing through a nonlinear crystal is converted into two lower-energy photons (signal and idler photons). This process is probabilistic and is widely used to generate entangled photon pairs. The generated photon pairs can exhibit quantum entanglement, making SPDC a fundamental process in experimental quantum optics [6].

Mathematically, the state of the entangled photon pair generated by SPDC can be written as:

$$|\psi\rangle = \frac{1}{\sqrt{2}}(|H\rangle_s|H\rangle_i + |V\rangle_s|V\rangle_i), \tag{2}$$

where $|H\rangle$ and $|V\rangle$ represent horizontal and vertical polarizations, respectively, and the subscripts s and i refer to the signal and idler photons [4].

C. Quantum Key Distribution (QKD)

QKD is a secure communication method that uses quantum mechanics to allow two parties to produce a shared random secret key, which can then be used to encrypt and decrypt messages. The security of QKD is based on the principles of quantum mechanics, particularly the no-cloning theorem and the detection of eavesdropping attempts [5], [9].

The BB84 protocol, developed by Charles Bennett and Gilles Brassard in 1984, is one of the most well-known QKD protocols. It involves the transmission of qubits in one of four possible states, chosen at random. The key steps of the BB84 protocol are as follows: *1. Preparation:* Alice randomly prepares qubits in one of four states (e.g., horizontal, vertical, diagonal, anti-diagonal). *2. Transmission:* Alice sends the qubits to Bob over a quantum channel. *3. Measurement:* Bob randomly chooses one of two bases to measure each qubit. *4. Sifting:* Alice and Bob publicly compare their basis choices and keep only the results where their bases match. *5. Key Distillation:* Alice and Bob apply error correction and privacy amplification to produce a shared secret key [4].

III. Verification by Simulations and Experiments

A. Bell Test Experiment

The Bell test experiment verifies quantum entanglement by comparing measurement results of entangled photons against classical predictions. A violation of Bell's inequality indicates quantum correlations [2].

B. Explanation of Bell's Inequality and Violation

Bell's inequality provides a way to test the predictions of quantum mechanics against those of classical physics. In a classical, local hidden variable theory, the Bell parameter S must satisfy the inequality $S \leq 2$.

In the context of the Bell test, the Bell parameter S is calculated using correlations between measurement outcomes of entangled particles. For example, consider a scenario where Alice and Bob each measure one of the entangled particles in different bases (e.g., horizontal, vertical, diagonal, anti-diagonal). The correlations between their measurement outcomes are used to compute S.

Quantum mechanics predicts that for certain entangled states and measurement settings, the value of S can exceed 2. Specifically, for maximally entangled Bell states and appropriately chosen measurement bases, quantum mechanics predicts that S can reach a value as high as $2\sqrt{2}$ (approximately 2.828). This violation of Bell's inequality ($S > 2$) is a direct indication of quantum entanglement and cannot be explained by any classical local hidden variable theory [7].

The key to observing a violation of Bell's inequality lies in the correct preparation of the entangled state, the choice of measurement bases, and the accurate calculation of correlations between measurement outcomes. When these conditions are met, the experimentally measured value of S will demonstrate the non-classical nature of quantum entanglement [6].

C. Quantum Key Distribution (QKD) Simulation

QKD ensures secure communication by exploiting quantum entanglement. The BB84 protocol, demonstrated through simulations, illustrates how keys can be securely shared [9].

1) Results and Justification: The QKD simulation using the BB84 protocol resulted in the generation of secure keys for Alice and Bob. The keys were generated only where their measurement bases matched. Sample keys generated were:

- Alice's key: [1, 0, 1, 1, 0, ...]
- Bob's key: [1, 0, 1, 1, 0, ...]

The matching keys indicate that the QKD protocol successfully established a secure communication channel, ensuring that any eavesdropping attempt would be detectable. This demonstrates the practical feasibility of using photonic qubits for secure communication [8].

IV. Conclusion and Future Prospects

Quantum entanglement in photonic systems offers a robust foundation for quantum computing and cryptography. The simulations utilize the theoretical models and demonstrate the feasibility of practical applications, such as secure communication through QKD. Future research will focus on scaling these technologies for widespread use, exploring advanced quantum algorithms, and enhancing the robustness of quantum networks.

Acknowledgement: Thanks to Tampere University.

References

[1] Aspect, A., Dalibard, J., & Roger, G. (1982). Experimental test of Bell's inequalities using time-varying analyzers. *Physical Review Letters, 49*(25), 1804.

[2] Hensen, B., Bernien, H., Dréau, A. E., Reiserer, A., Kalb, N., Blok, M. S., ... & Hanson, R. (2015). Loophole-free Bell inequality violation using electron spins separated by 1.3 kilometres. *Nature, 526*(7575), 682-686.

[3] Tegmark, M. (1998). The interpretation of quantum mechanics: Many worlds or many words?. *Fortschritte der Physik: Progress of Physics, 46*(6-8), 855-862.

[4] Pan, J.-W., Chen, Z.-B., Lu, C.-Y., Weinfurter, H., Zeilinger, A., & Żukowski, M. (2012). Multiphoton entanglement and interferometry. *Reviews of Modern Physics, 84*(2), 777.

[5] Bennett, C. H., & Brassard, G. (1984). Quantum cryptography: Public key distribution and coin tossing. *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing*, 175-179.

[6] Ursin, R., Tiefenbacher, F., Schmitt-Manderbach, T., Weier, H., Scheidl, T., Lindenthal, M., ... & Zeilinger, A. (2007). Entanglement-based quantum communication over 144 km. *Nature Physics, 3*(7), 481-486.

[7] Bell, J. S. (1964). On the Einstein Podolsky Rosen paradox. *Physics Physique Fizika, 1*(3), 195-200.

[8] Bennett, C. H., Brassard, G., Crpeau, C., Jozsa, R., Peres, A., & Wootters, W. K. (1993). Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels. *Physical Review Letters, 70*(13), 1895.

[9] Ekert, A. K. (1991). Quantum cryptography based on Bell's theorem. *Physical Review Letters, 67*(6), 661.