Secure Quantum Key Distribution via Entangled Quantum Walkers

Chia-Tso Lai
JoS QUANTUM GmbH, c/o Tech Quartier, Platz der Einheit 2, 60327 Frankfurt am Main, Germany[*]

(Dated: August 8, 2025)

Quantum Key Distribution (QKD) is an emerging cryptographic method designed for secure key sharing. Its security is theoretically guaranteed by fundamental principles of quantum mechanics, making it a leading candidate for future communication protocols. Quantum Random Walks (QRWs), on the other hand, are quantum processes that exhibit intriguing phenomena such as interference and superposition, enabling the generation of decentralized and asymmetric probability distributions. Inspired by both fields of study, we propose a novel QKD protocol based on two entangled quantum walkers. Our protocol exploits the unique correlations between the walkers at extremal positions of the walk to establish secret keys shared exclusively by the two parties. The security of the protocol is augmented by analyzing the joint probability distributions of the walkers' measured positions and their associated coin states.

I. INTRODUCTION

Quantum Key Distribution (QKD) is a robust cryptographic scheme devised to defend against eavesdropping during secret communication. It leverages quantum properties such as the no-cloning theorem and quantum entanglement to ensure security. A variety of QKD protocols have been proposed since its inception. For instance, the pioneering BB84 protocol [1] introduced the first example of a prepare-and-measure QKD scheme. Any attempt at observation by an eavesdropper disturbs the quantum state if the measurement basis differs from the preparation basis, thereby revealing the intrusion. The E91 protocol [2] laid the foundation for entanglement-based QKD. E91 uses Bell's theorem as a security guarantee against eavesdropping. The strength of the correlations between the measured keys can be quantified using the CHSH test [3], which signals a potential attack if the correlations fall below a certain classical limit. Our proposed protocol can be categorized as a prepare-and-double-measure QKD scheme that incorporates entanglement to achieve secure and exclusive key distribution. We begin the protocol with an entangled ”coin” pair prepared by the sender and shared with the receiver. Each coin is then entangled with a ”walker” at the respective end of the communication channel. A specific connection between the walkers is established via entanglement swapping [4], in which a Bell state measurement (BSM) is performed on the coin pair once it is reunited at the sender's end. This process creates an entangled state shared between the two walkers, enabling the parties to derive a pair of secret keys (Fig. 1). The security of our protocol relies on quantum entanglement, though the verification method differs from the standard CHSH formulation.

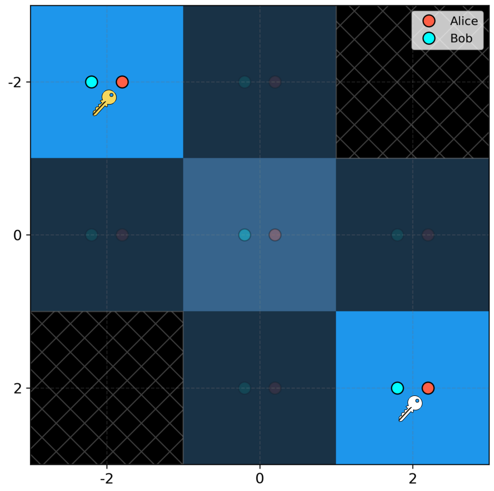


FIG. 1: Entangled walkers Alice and Bob obtain shared secret keys at opposite corners of the joint quantum walk.

Quantum Random Walks (QRWs) [5] are the quantum analog of classical random walks, which form the basis of many stochastic algorithms. Due to quantum interference and superposition, QRWs exhibit markedly different behavior, often resulting in faster, ballistic spreading of probability distributions compared to the centralized, diffusive binomial distributions of classical walks (Fig. 2). In this work, we focus on discrete coined quantum random walks [6], where the evolution of the walker is governed by a quantum coin state and a unitary coin-flip operator. Motivated by the properties of coined QRWs, we investigate the behavior of joint QRWs involving two entangled walkers. These joint walks show intriguing correlations in position space, particularly at the edges of the distribution. We demonstrate that these spatial correlations allow both parties to share mutual information about the measured positions, without revealing the actual outcomes. As a result, the walkers' positions can be effectively used to encode secret keys, making entangled QRWs a promising building block for secure quantum communication protocols.

[*] chiatsolai@gmail.com

II. THEORY

A. Discrete Coined QRW

A discrete coined QRW is composed of several elements: the number of steps $s \in \mathbb{Z}^+$, the walker's position state $|x\rangle$ (with $x \in \mathbb{Z}$), the coin state $|c\rangle$, a unitary coin-flip operator $\hat{U}(\theta, \lambda)$, and a shift operator $\hat{S}$. The entire system can be described by the product state $|\psi\rangle = |c\rangle \otimes |x\rangle$. The QRW evolves by repeatedly applying the coin-flip operator to the coin, followed by the shift operator applied to the position register, conditioned on the coin state.

We consider a general coin-flip operator $\hat{U}(\theta, \lambda)$ given by:

$$\hat{U}(\theta, \lambda) = \begin{bmatrix} \cos(\frac{\theta}{2}) & -e^{i\lambda}\sin(\frac{\theta}{2}) \\ \sin(\frac{\theta}{2}) & e^{i\lambda}\cos(\frac{\theta}{2}) \end{bmatrix}$$

The conditional shift operator $\hat{S}$ is defined as:

$$\hat{S} = |0\rangle\langle 0| \otimes \sum_i |i-1\rangle\langle i| + |1\rangle\langle 1| \otimes \sum_i |i+1\rangle\langle i| \tag{1}$$

Assume the walker starts from an initial position $|x_0\rangle$ and the coin is prepared in a state $|c_0\rangle = k_0|0\rangle + k_1|1\rangle$, with $k_1 = e^{i\phi}\sqrt{1-k_0^2}$, resulting in the initial product state $|\psi^0\rangle = |c_0\rangle|x_0\rangle$. After one step of QRW, the state becomes:

$$\begin{aligned} |\psi^1\rangle &= \hat{S}(\hat{U} \otimes \hat{I})|\psi^0\rangle \\ &= |0\rangle \otimes (k_0\cos(\frac{\theta}{2}) - k_1 e^{i\lambda}\sin(\frac{\theta}{2}))|x_0 - 1\rangle \\ &\quad + |1\rangle \otimes (k_0\sin(\frac{\theta}{2}) + k_1 e^{i\lambda}\cos(\frac{\theta}{2}))|x_0 + 1\rangle \end{aligned} \tag{2}$$

After s steps, the state evolves to:

$$|\psi^s\rangle = |0\rangle \otimes \sum_{i=-s}^{s-2} A_i^{(s)}|x_0 + i\rangle + |1\rangle \otimes \sum_{j=-s+2}^{s} B_j^{(s)}|x_0 + j\rangle \tag{3}$$

where the amplitudes $A_i^{(s)}$ and $B_j^{(s)}$ vanish at positions where the shift from $-s$ or s is odd (i.e., $i, j = -s+1, -s+3, \ldots, s-1$). The amplitudes can be computed recursively by:

$$\begin{cases} A_i^{(s+1)} = A_{i+1}^{(s)} \cdot \cos(\frac{\theta}{2}) - B_{i+1}^{(s)} \cdot e^{i\lambda}\sin(\frac{\theta}{2}) \\ B_i^{(s+1)} = A_{i-1}^{(s)} \cdot \sin(\frac{\theta}{2}) + B_{i-1}^{(s)} \cdot e^{i\lambda}\cos(\frac{\theta}{2}) \end{cases}$$

with initial conditions $A_i^{(0)} = k_0\delta_{i0}$ and $B_i^{(0)} = k_1\delta_{i0}$.

B. Entangled Quantum Walks

In our proposed QKD protocol, two QRWs are implemented with a shared entangled coin pair $|c_A, c_B\rangle = k_0|00\rangle + k_1|11\rangle$. Both walkers start at the origin, $x_0 = y_0 = 0$, and evolve for the same number of steps using publicly agreed coin-flip operators, $\hat{U}_A$ and $\hat{U}_B$, respectively. This results in a joint position distribution over the basis states $|x\rangle_A|y\rangle_B$ at the end of the walk. The state after s steps is given by:

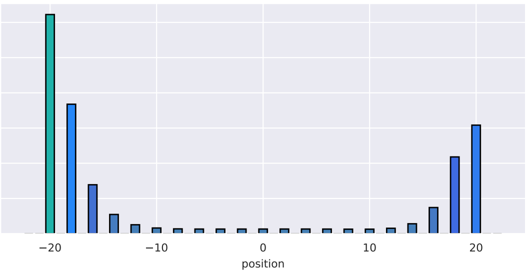


FIG. 2: Probability distribution after 20 steps of a discrete coined QRW.

$$\begin{aligned} |\psi^s\rangle = |00\rangle &\otimes \sum_{x=-s}^{s-2}\sum_{y=-s}^{s-2} A_{xy}^{(s)}|x\rangle_A|y\rangle_B \\ + |01\rangle &\otimes \sum_{x=-s}^{s-2}\sum_{y=-s+2}^{s} B_{xy}^{(s)}|x\rangle_A|y\rangle_B \\ + |10\rangle &\otimes \sum_{x=-s+2}^{s}\sum_{y=-s}^{s-2} C_{xy}^{(s)}|x\rangle_A|y\rangle_B \\ + |11\rangle &\otimes \sum_{x=-s+2}^{s}\sum_{y=-s+2}^{s} D_{xy}^{(s)}|x\rangle_A|y\rangle_B \end{aligned} \tag{4}$$

where the amplitudes $A_{xy}^{(s)}$, $B_{xy}^{(s)}$, $C_{xy}^{(s)}$ and $D_{xy}^{(s)}$ again vanish at positions where the shift from $-s$ or s is odd. Similar to a single-walker QRW, these amplitudes can be computed recursively. First we transform the amplitudes for the same positions (x, y) with the composite coin-flip operator:

$$\begin{bmatrix} A_{xy}'^{(s)} \\ B_{xy}'^{(s)} \\ C_{xy}'^{(s)} \\ D_{xy}'^{(s)} \end{bmatrix} = (\hat{U}_A \otimes \hat{U}_B) \begin{bmatrix} A_{xy}^{(s)} \\ B_{xy}^{(s)} \\ C_{xy}^{(s)} \\ D_{xy}^{(s)} \end{bmatrix} \tag{5}$$

Then, the recursive relations can be formulated as:

$$\begin{cases} A_{xy}^{(s+1)} = A_{x+1,y+1}'^{(s)} \\ B_{xy}^{(s+1)} = B_{x+1,y-1}'^{(s)} \\ C_{xy}^{(s+1)} = C_{x-1,y+1}'^{(s)} \\ D_{xy}^{(s+1)} = D_{x-1,y-1}'^{(s)} \end{cases} \tag{6}$$

with initial conditions $A_{xy}^{(0)} = k_0\delta_{x0}\delta_{y0}$, $B_{xy}^{(0)} = 0$, $C_{xy}^{(0)} = 0$, and $D_{xy}^{(0)} = k_1\delta_{x0}\delta_{y0}$.

We proceed to implement entanglement swapping on the state $|\psi^s\rangle$ to establish correlations between the two walkers' position distributions. This is achieved by performing a Bell state measurement (BSM) on the entangled coin pair $|c_A, c_B\rangle$. The BSM is realized by applying a CNOT gate to the pair, followed by a Hadamard gate on the control coin qubit, resulting in the state $|\psi'^s\rangle$ prior to measuring the coin pair. For notational convenience, we define the summations in Eq. (4) as:

$$\begin{aligned}
\mathbf{A}^{(s)} &= \sum_{x=-s}^{s-2}\sum_{y=-s}^{s-2} A_{xy}^{(s)} |x\rangle_A |y\rangle_B \\
\mathbf{B}^{(s)} &= \sum_{x=-s}^{s-2}\sum_{y=-s+2}^{s} B_{xy}^{(s)} |x\rangle_A |y\rangle_B \\
\mathbf{C}^{(s)} &= \sum_{x=-s+2}^{s}\sum_{y=-s}^{s-2} C_{xy}^{(s)} |x\rangle_A |y\rangle_B \\
\mathbf{D}^{(s)} &= \sum_{x=-s+2}^{s}\sum_{y=-s+2}^{s} D_{xy}^{(s)} |x\rangle_A |y\rangle_B
\end{aligned} \tag{7}$$

This allows us to express Eq. (4) more compactly such that the transformed state $|\psi'^s\rangle$ becomes:

$$\begin{aligned}
|\psi'^s\rangle = &\frac{1}{\sqrt{2}} |00\rangle \otimes \left[\mathbf{A}^{(s)} + \mathbf{D}^{(s)}\right] \\
&+ \frac{1}{\sqrt{2}} |10\rangle \otimes \left[\mathbf{A}^{(s)} - \mathbf{D}^{(s)}\right] \\
&+ \frac{1}{\sqrt{2}} |01\rangle \otimes \left[\mathbf{B}^{(s)} + \mathbf{C}^{(s)}\right] \\
&+ \frac{1}{\sqrt{2}} |11\rangle \otimes \left[\mathbf{B}^{(s)} - \mathbf{C}^{(s)}\right]
\end{aligned} \tag{8}$$

The Bell measurement collapses the state, projecting the coin pair onto one of the four possible outcomes: $|00\rangle, |01\rangle, |10\rangle, |11\rangle$.

We observe that the expansion of $\mathbf{A}^{(s)}+\mathbf{D}^{(s)}$ (and likewise $\mathbf{A}^{(s)}-\mathbf{D}^{(s)}$) contains the terms $A_{-s,-s}^{(s)} |{-s}\rangle_A |{-s}\rangle_B$ and $D_{s,s}^{(s)} |s\rangle_A |s\rangle_B$, while the terms $|{-s}\rangle_A |s\rangle_B$ and $|s\rangle_A |{-s}\rangle_B$ are absent. This implies that if the BSM outcome is $|00\rangle$ (or $|10\rangle$), the probability of the two walkers being on opposite ends of the distribution is zero (see Fig. (4a)). In other words, if both walkers are found at the extremities of their distributions, they must be at the same extremity (either both at $-s$ or both at s). A similar argument holds for the expansions of $\mathbf{B}^{(s)}+\mathbf{C}^{(s)}$ and $\mathbf{B}^{(s)}-\mathbf{C}^{(s)}$. In these cases, if the measurement outcome is $|01\rangle$ or $|11\rangle$ and both walkers are at their extremities, then they cannot be located at the same end of the distribution—only opposite ends are possible in such a scenario (see Fig. (4b)).

III. QKD VIA ENTANGLED QUANTUM WALKERS

Given the exclusive correlations between two entangled quantum walkers, as described by Eq. (8), a secure QKD protocol can be designed by utilizing the two extremities of the position distribution as secret keys. Based on this idea, we propose a robust quantum communication scheme between two parties—Alice and Bob—consisting of the following steps:

1. **Entangled coin pair preparation**: Alice chooses an initial coin state $|c_A\rangle = k_0 |0\rangle + k_1 |1\rangle$, with which she prepares an entangled coin pair $|c_A, c_B\rangle = k_0 |00\rangle + k_1 |11\rangle$.

2. **Transmission**: Alice sends one qubit from the entangled coin pair to Bob via a quantum channel.

3. **Distribution of QRW parameters**: Alice and Bob communicate over a classical channel to agree on the parameters of the QRWs, including the coin-flip operators $\hat{U}_A(\theta_1, \lambda_1)$ and $\hat{U}_B(\theta_2, \lambda_2)$, and the number of steps s. Choosing phase angles such that $|\theta_1| < 1$ and $|\theta_2| < 1$ increases the probability at the extremities of the position distribution (see Fig. 2), thereby improving the likelihood of successful key generation.

4. **QRW implementation**: Alice and Bob independently implement the QRW using the agreed-upon parameters.

5. **Entanglement swapping**: Bob sends his coin qubit back to Alice, who then performs a BSM to transfer the entanglement to the walkers' position states. The BSM outcome is kept by Alice as a reference for key inference.

6. **Position measurement**: Both parties measure the positions of their walkers, obtaining values $a, b \in \{-s, -s+2, \ldots, s\}$.

7. **Announcement**: After multiple rounds of steps 1 to 6, Alice and Bob announce the rounds in which their walkers were found at extremal positions (without revealing which extremity). In rounds where either Alice or Bob did not find their walker at an extremal position, Bob discloses the measured position to Alice.

8. **Key generation**: Using the BSM outcomes and her own measurement results, Alice infers which position Bob measured in the rounds where both observed extremal values. Bob's measured positions ($\pm s$) are then used as the sifted keys.

9. **Security check**: The protocol includes two layers of security verification. First, Alice checks whether the BSM outcomes follow the expected probability distribution of the coin pair, allowing a deviation up to ϵ_c based on a predefined metric. Second, the joint distribution of measured positions is compared against the theoretical model. If either test fails, the protocol is aborted.

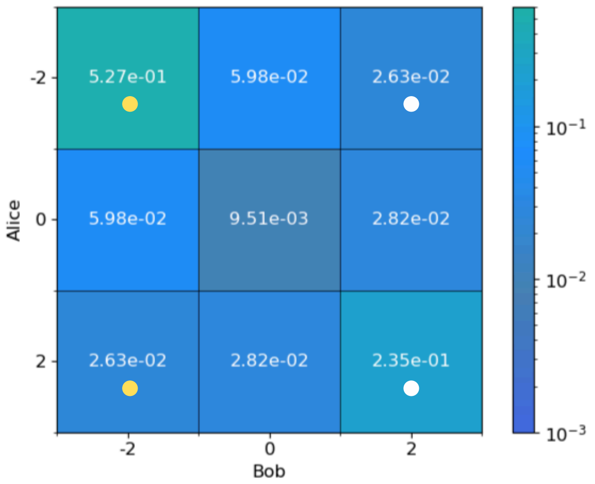
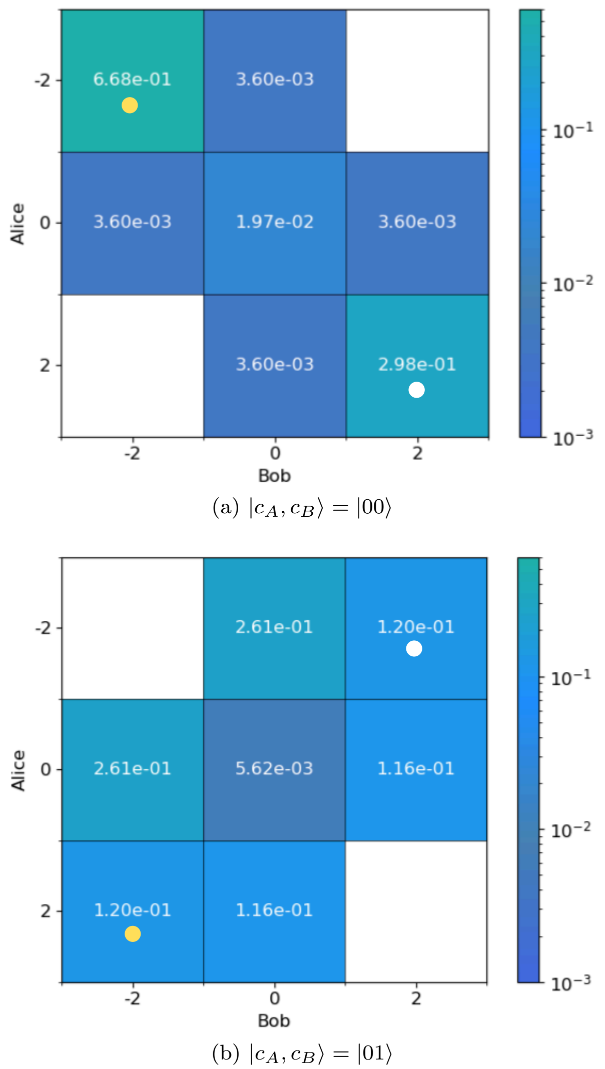


FIG. 3: Joint probability distribution of Alice and Bob's positions, considering all BSM outcomes. The four corners of the distribution correspond to scenarios where key pairs can be generated. Yellow dots denote the shared key value -2, while white dots indicate the key value 2.

IV. 2-STEP QRW PROTOCOL

In this section, we demonstrate a QKD protocol based on 2-step QRWs, i.e., with $s = 2$. The 2-step setup strikes a balance between hardware feasibility and complexity, making it suitable for near-term implementation. It requires only four qubits in total for the coin and position registers per party, which aligns well with current hardware limitations. Furthermore, the 2-step protocol is statistically efficient for security verification, as it yields only nine possible outcomes in the joint position distribution. This small outcome space reduces the number of required protocol rounds to obtain a meaningful match between the observed and theoretical distributions. While a 1-step QRW protocol is also viable for practical realization, its limited structure may not adequately demonstrate the features of generic s-step schemes. In contrast, the increased complexity of the 2-step QRW allows for a more representative example, and potentially offers stronger security guarantees against eavesdropping, due to the higher-dimensional correlations available for verification.

Assume Alice and Bob choose the same coin-flip operator, $\hat{U}_A(\theta, \lambda) = \hat{U}_B(\theta, \lambda)$, to perform the 2-step QRW with the following parameters: $\theta = 0.635$, $\lambda = 0$, and initial coin state $|c_A\rangle = 0.85\,|0\rangle + 0.527e^{i\frac{\pi}{4}}\,|1\rangle$. The joint probability distribution of all possible measured positions, aggregated over all BSM outcomes, is summarized in Fig. 3. The four corners of the heatmap correspond to measurement outcomes that enable key generation. In this instance, a valid key pair can be generated with a probability of approximately 81%. Other measurement results, while not used for key generation, serve as references for security verification. Fig. 4a shows the joint distribution of Alice's and Bob's positions when the BSM outcome is $|00\rangle$, which occurs with probability 39%. The heatmap reveals that when Bob measures -2 (respectively, 2), Alice has zero probability of measuring 2 (respectively, -2), ensuring the exclusivity of the shared key. Similarly, Fig. 4b shows the distribution when $|c_A, c_B\rangle = |01\rangle$, which occurs with probability 11%. In this case, when Bob measures -2 (2), Alice has zero probability of measuring -2 (2), maintaining exclusivity under a different correlation pattern.



(a) $|c_A, c_B\rangle = |00\rangle$

(b) $|c_A, c_B\rangle = |01\rangle$

FIG. 4: Joint probability distribution of measured positions when the BSM outcome is (a) $|c_A, c_B\rangle = |00\rangle$ and (b) $|c_A, c_B\rangle = |01\rangle$. Empty grid cells indicate zero probability for the corresponding position pair. The parity of the BSM outcome determines the correlation pattern of the two walkers, allowing Alice to infer Bob's key.

V. CONCLUSION AND OUTLOOK

We have shown that the unique correlations between two entangled quantum walkers, established via entanglement swapping, can be harnessed as a secure resource for quantum communication, enabling the development of a powerful QKD protocol. The behavior of the walkers at their spatial extremities, together with the Bell state measurement outcomes, provides both parties with exclusive information about the position states. Furthermore, the BSM results and the joint position distributions of the QRWs serve as a foundation for security verification, enhancing the robustness of the protocol.

For future research, the impact of noisy quantum channels and specialized attacks on this new protocol should be a primary focus. Additionally, incorporating CHSH tests or other security verification methods into the protocol may offer valuable enhancements. Experimental realizations, alongside suitable error reconciliation and privacy amplification schemes, will be essential for evaluating the practical viability of the proposed protocol. Finally, we emphasize the innovative and interdisciplinary nature of this work: the integration of entangled quantum random walks into quantum cryptography not only showcases a novel application of QRWs but also enriches the landscape of QKD protocols.

[1] C. H. Bennett, G. Brassard, *et al.*, Proceedings of the ieee international conference on computers, systems and signal processing (1984).

[2] A. K. Ekert, Quantum cryptography based on bell's theorem, Physical review letters **67**, 661 (1991).

[3] J. F. Clauser, M. A. Horne, A. Shimony, and R. A. Holt, Proposed experiment to test local hidden-variable theories, Physical review letters **23**, 880 (1969).

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

[5] Y. Aharonov, L. Davidovich, and N. Zagury, Quantum random walks, Physical Review A **48**, 1687 (1993).

[6] T. A. Brun, H. A. Carteret, and A. Ambainis, Quantum random walks with decoherent coins, Physical Review A **67**, 032304 (2003).