A Secure Quantum Key Distribution Protocol Using Two-Particle Transmission

Pratapaditya Bej

ExamRoom.AI, Konappa Agrahara, Electronic City Phase 1, Bengaluru-560100, India,

Vinod Jayakeerthi

ExamRoom.AI, 1025 Greenwood Boulevard Suite 401 Lake Mary, Florida 32746, USA

Abstract

The evolution of Quantum Key Distribution (QKD) relies on innovative methods to enhance its security and efficiency. Unextendible Product Bases (UPBs) hold promise in quantum cryptography due to their inherent indistinguishability, yet they are underutilized in QKD protocols. This work introduces a protocol utilizing UPBs to establish quantum keys between distant parties. Specifically, we propose a protocol utilizing a 3×3 tile UPB, where Alice sequentially transmits subsystem states to Bob through quantum channels. The protocol's security is underpinned by the no-cloning theorem, prohibiting the cloning of orthogonal states. We analyze potential attacks, including intercept-resend and detector blinding attacks when quantum channels are noiseless, and discuss the challenges posed by the indistinguishability of our protocol for eavesdroppers, thereby enhancing QKD security.

1 Introduction

In the landscape of information theory, cryptography plays a vital role in securing data and communications. However, traditional cryptographic systems like RSA, AES face a grave threat from quantum computing due to their reliance on classical computational limitations [1, 2]. Recognizing the impending threat posed by quantum computing to classical cryptosystems, the imperative for proactive countermeasures becomes evident. One such strategy is the pursuit of post-quantum cryptography [3], which entails the development of novel cryptographic schemes resilient to quantum attacks. However, while post-quantum cryptography offers a partial solution to the problem, it may be susceptible to undiscovered quantum algorithms, leaving its efficacy and long-term security in question. In contrast, Quantum Key Distribution (QKD) stands out as the ultimate solution, leveraging the unbreakable principles of quantum mechanics such as the uncertainty principle and no-cloning theorem [4, 5, 6, 7].

Quantum cryptography has seen significant advancements in protocol development. In 1984, Bennett and Brassard introduced the pioneering BB84 protocol, which utilizes quantum properties

to distribute keys between distant parties securely [8]. Following the introduction of BB84, a series of subsequent protocols surfaced, such as E91 [9], B92 [10], BBM92 [11], and the six-state protocol [12], significantly broadening the spectrum of quantum secure communication [4, 5, 6, 13]. Recent years witnessed the rise of variants such as Device-Independent (DI) QKD [14, 15], Measurement-Device Independent (MDI) QKD [16, 17], and Continuous Variable (CV) QKD [18, 19], driven by both theoretical innovations and experimental implementations [20, 21, 22, 23, 24].

Contemporary QKD primarily relies on non-orthogonal states for security. However, the adoption of orthogonal states in cryptographic protocols emerged later, with the inception of the pioneering protocol [25]. This groundbreaking approach introduced the concept of sending states with controlled time delays, making it nearly impossible for eavesdroppers to intercept an entire state without detection. Moreover, several other studies facilitate the implementation of QKD protocols using orthogonal states, as evidenced by various documented protocols [26, 27, 28, 29]. Experimental validation has recently been conducted in the case of quantum cryptography based on orthogonal states [30, 31]. While non-orthogonal state encoding is prevalent, orthogonal state encoding offers potential benefits, such as reduced quantum operation requirements. Understanding the theoretical application of orthogonal states for coding is invaluable due to their innate ability to be distinguished without errors.

The evolution of QKD relies on innovative methods to enhance its security and efficiency. Among these, integrating Unextendible Product Bases (UPBs) may hold promise in quantum cryptography due to their indistinguishability, potentially fortifying the security of quantum communication channels. UPBs are fundamental in quantum information theory [37]. A UPB for a quantum system is an incomplete orthogonal product basis whose complementary subspace cannot be extended to a complete orthogonal basis. UPBs are indistinguishable in the Local Operation and Classical Communication (LOCC) paradigm [37, 38, 46, 47, 48].

High-dimensional quantum states offer increased information capacity and noise resilience crucial for securing QKD. Qubit-based systems exhibit a quantum bit error rate threshold of 11%, whereas qudit-based protocols show heightened resilience to noise [40, 41, 42]. The increased noise tolerance also impacts the final secret key rate, as the secret key rate rises with Hilbert space dimensions for a fixed noise level [9, 43]. The no-cloning theorem underpins the security of quantum communication, increasing the input state dimension reduces cloning fidelity, emphasizing the benefits of high-dimensional states for quantum cryptography [7, 44, 45].

No widely recognized protocol frequently incorporates UPBs in QKD protocols. In addressing this gap, we present a protocol that showcases the utilization of UPBs to establish quantum keys between two distant parties. In our protocol, we take the 3×3 tile UPB [37] where Alice sends each subsystem state of a UPB through two quantum channels successively to Bob. During the transmission of particles, there is a time gap in the particle-sending process such that no eavesdropper has access to two particles simultaneously. The strategy involves dividing the transfer of information into two steps, ensuring that only a portion of the information is transmitted at each step. The security of this approach is guaranteed by the no-cloning theorem concerning orthogonal states [39]. Throughout the work, we assume noiseless quantum channels, ensuring no information loss during particle transmission through these channels. After Bob receives two particles, a quantum measurement is conducted to distinguish the states. Subsequently, we analyze potential attacks on our protocol, including an efficient intercept-resend attack and detector blinding attacks. We show theoretically that even if an adversary can perfectly blind each single-photon detector, there remains a 50% chance for the eavesdropper to blind the detectors. In our protocol, the indistinguishability of UPBs poses challenges for eavesdroppers attempting to discern between quantum states exchanged during the QKD process, particularly when LOCC is employed by Eve. We also demonstrate that the sequential transmission of the two particles comprising a UPB state through quantum channels hinders

the eavesdropper from perfectly distinguishing the transmitted state, even when the eavesdropper employs entanglement as a resource. This inherent indistinguishability of our protocol enhances the security of QKD. The rest of the paper is organized as follows: In Section 2, we describe the protocol, and in Section 3, we analyze different attacks. Finally, in the last section (Section 4), we conclude our results and discuss some future works.

2 Protocol

In the context of the quantum key distribution protocol, we focus on a 3×3 dimensional bipartite tiles UPB as outlined in the paper by Bennett et al. [38]. These bases are represented by:

$$\begin{aligned}
|\psi_1\rangle &= \frac{1}{\sqrt{2}}|0\rangle_A(|0\rangle - |1\rangle)_B \\
|\psi_2\rangle &= \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)_A|2\rangle_B \\
|\psi_3\rangle &= \frac{1}{\sqrt{2}}|2\rangle_A(|1\rangle - |2\rangle)_B \\
|\psi_4\rangle &= \frac{1}{\sqrt{2}}(|1\rangle - |2\rangle)_A|0\rangle_B \\
|\psi_5\rangle &= \frac{1}{3}(|0\rangle + |1\rangle + |2\rangle)_A(|0\rangle + |1\rangle + |2\rangle)_B
\end{aligned} \tag{1}$$

where A and B represent the states of particles A and B, respectively. The bases given by Eq.1 are not complete, indicating that $\sum_{i=1}^{5} |\psi_i\rangle\langle\psi_i| \neq \mathbb{I}$, where $\mathbb{I}$ represents the identity matrix. However, it's important to note that these bases are orthogonal to each other, meaning that $\langle\psi_i|\psi_j\rangle = 0$ for all $i \neq j$ within the set $\{1, 2, ..., 5\}$. Additionally, they exhibit a degree of nonlocality even in the absence of entanglement. Notably, these bases are indistinguishable under the framework of LOCC [37, 38, 46, 47, 48, 49].

Therefore, using Eq. 1 as the measurement basis, it seems that we cannot form a valid quantum measurement. To construct a valid quantum measurement, we need to ensure that the operators satisfy the completeness relation $\sum_{i=1}^{n} M_i M_i^\dagger = \mathbb{I}$.

To form a quantum measurement along with Eq. 1, we apply the Gram-Schmidt decomposition. First, we begin by constructing four orthogonal states represented as

$|h_k\rangle$ starting (for $k = 6, 7, 8, 9$) from $|\psi_1\rangle$ to $|\psi_4\rangle$.

$$\begin{aligned}
|h_6\rangle &= \frac{1}{\sqrt{2}}|0\rangle_A(|0\rangle + |1\rangle)_B \\
|h_7\rangle &= \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)_A|2\rangle_B \\
|h_8\rangle &= \frac{1}{\sqrt{2}}|2\rangle_A(|1\rangle + |2\rangle)_B \\
|h_9\rangle &= \frac{1}{\sqrt{2}}(|1\rangle + |2\rangle)_A|0\rangle_B
\end{aligned} \tag{2}$$

i.e. $\langle h_k|\psi_i\rangle = 0 \quad \text{for} \quad i = 1, ..., 4 \quad \text{and} \quad k = 6, ..., 9$. That means $|h_k\rangle$ and $|\psi_i\rangle$ are orthogonal to each other for $i = 1, 2, .., 4$ and $k = 6, ..., 9$. Next, we formulate:

$$
\begin{aligned}
|\psi_6\rangle &= \alpha_6(|h_6\rangle - \sum_{i=1}^{5}\langle\psi_i|h_6\rangle|\psi_i\rangle) \\
|\psi_k\rangle &= \alpha_k(|h_k\rangle - \sum_{i=1}^{5}\langle\psi_i|h_k\rangle|\psi_i\rangle - \sum_{j=6}^{k-1}\langle\psi_j|h_k\rangle|\psi_j\rangle) \quad \text{for } k = 7, 8, 9
\end{aligned} \tag{3}
$$

where α_k is the normalization constant of the k-th state that can be easily evaluated, and these values are $\alpha_6 = \sqrt{\frac{9}{7}}$, $\alpha_7 = \sqrt{\frac{7}{5}}$, $\alpha_8 = \sqrt{\frac{5}{3}}$, and $\alpha_9 = \sqrt{3}$.

Now, $\sum_{i=1}^{9}|\psi_i\rangle\langle\psi_i| = \mathbb{I}$ (identity matrix). Therefore, we form a valid quantum measurement by using $|\psi_1\rangle$ to $|\psi_9\rangle$ as the basis. Additionally, it's important to note that each of these basis states is orthogonal to the others, meaning that $\langle\psi_i|\psi_j\rangle = 0$ for all $i \neq j$ within the set $\{|\psi_1\rangle, ..., |\psi_9\rangle\}$. This specific set of quantum states $|\psi_1\rangle, \ldots, |\psi_5\rangle$ are product bases and $|\psi_6\rangle, \ldots, |\psi_9\rangle$ are entangled bases.

The protocol is as follows:

Step 1: Alice begins by preparing two quantum particles, labeled as A and B, randomly in one of five quantum states using Eq.1.

Step 2: After randomly preparing the state in one of the five quantum states using Eq.1, Alice sends either particle A or B randomly to Bob through quantum channel number 1. Upon receiving the particle, Bob informs Alice through an open classical communication channel.

Step 3: Alice then sends the second particle to Bob through channel 2. Importantly, she only sends the second particle after receiving confirmation that the first particle has reached Bob. This sequential transmission prevents potential eavesdroppers from having simultaneous access to both particles, ensuring security. We assume that both quantum channels are noiseless.

For example, if Alice wants to send the state $|\psi_i\rangle$ to Bob, she may send the second particle B through channel 1 and then A through channel 2, creating the sequence BA. Alternatively, she may send particle A first through channel 1 and then B through channel 2, resulting in the sequence AB. Alice will keep a record of which path she is sending each particle. In the AB sequence, the two-qutrit state received by Bob will be given by Eq.1. In the BA sequence, after the two-qutrit state reaches Bob, he will obtain the state described by Eq.4, thus forming another tile UPB.

$$
\begin{aligned}
|\xi_1\rangle &= \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)_B|0\rangle_A \\
|\xi_2\rangle &= \frac{1}{\sqrt{2}}|2\rangle_B(|0\rangle - |1\rangle)_A \\
|\xi_3\rangle &= \frac{1}{\sqrt{2}}(|1\rangle - |2\rangle)_B|2\rangle_A \\
|\xi_4\rangle &= \frac{1}{\sqrt{2}}|0\rangle_B(|1\rangle - |2\rangle)_A \\
|\xi_5\rangle &= \frac{1}{3}(|0\rangle + |1\rangle + |2\rangle)_B(|0\rangle + |1\rangle + |2\rangle)_A
\end{aligned} \tag{4}
$$

It is essential to note that $|\xi_i\rangle$ for all $i \in \{1, ..., 5\}$ are not orthogonal to the set $|\psi_1\rangle, \ldots, |\psi_9\rangle$. Therefore, it is impossible to distinguish all states of Eq.4 using $|\psi_1\rangle, \ldots, |\psi_9\rangle$ as measurement bases.

In the context of Quantum Key Distribution (QKD), the principle of sequential sending, where Alice transmits the second particle to Bob only after receiving confirmation of the safe arrival of the first particle, aligns with the fundamental prerequisites for employing a set of orthogonal product

states in five state composite systems where each subsystem are nonidentical and non-orthogonal to each other (for detail see table 1). These prerequisites, as established in the QKD scheme, demand that within the density matrix of any subsystem (represented as $\rho_{S|i}$, with S being either subsystem A or B), there must exist at least one $\rho_{S|j}$ that differs from $\rho_{S|i}$ and lacks orthogonality with it. This condition, grounded in the laws of quantum mechanics [39], upholds the standard no-cloning theorem [7], which is a cornerstone of quantum security. Therefore, the sequential sending of particles, a vital element of the QKD protocol, serves as a practical implementation of the quantum principles that safeguard the security of quantum communication.

Step 4: Upon receiving both particles A and B, Bob performs a collective measurement on them. This measurement is carried out using the basis of the nine quantum bases described earlier ($|\psi_1\rangle$ to $|\psi_9\rangle$) in Eq.1 and Eq.3. It helps Bob determine the quantum state in which the two-particle system has been prepared.

If Alice sends the AB sequence, Bob can successfully distinguish the state with certainty by forming a quantum measurement with the bases Eq.1 and Eq.3 ($|\psi_1\rangle$,...,$|\psi_9\rangle$). However, when Alice sends the BA sequence to Bob, he will not be able to distinguish the state with certainty, but Bob will register a click on one of his measurement bases. For both sequences, Bob will record all the clicks made by his measurements. Since Alice randomly prepares and sends the state in either the AB or BA sequence, both ways introduce randomness in these two situations; one is during the state preparation process, and the other is during the sequential particle-sending process.

Step 5: After the measurement process, Bob will communicate with Alice through classical channels to know the sequence of the particle-sending process. If Alice sends the AB sequence, Bob will retain the measurement results and record the information about which state he distinguished. If Alice sends the BA sequence, Bob will discard the results. Alice and Bob have a predefined agreement on how to assign bit values based on the measured quantum states

Repeating the entire procedure multiple times, Alice and Bob generate a random bit string. This bit string serves as the raw key for encryption purposes.

Step 6: To check for potential eavesdropping, Alice and Bob randomly sample and compare bits from their raw key. If the correlations between their bits remain intact with exact values, they can conclude that there is no eavesdropper. If the raw key remains unaltered and secure, Alice and Bob can confidently use the rest of the results as a cryptographic key for secure communication. However, if they suspect eavesdropping or find discrepancies during the random bit comparisons, they take security precautions by discarding the entire key and redistributing it.

In the forthcoming section, we delve into a comprehensive analysis of our protocol, shedding light on both the intercept-resend attack and the detector blinding attack, pertinent to our innovative patent-pending device.

3 Protocol analysis

Here, we explore two potential security vulnerabilities: the intercept-resend attack and the detector blinding attack. Initially, we delve into the intercept-resend attack, where an eavesdropper intercepts the quantum channel, measures the first particle, and sends a particle to Bob based on this measurement outcome. Subsequently, during the transmission of the second particle, the eavesdropper measures it and sends another particle to Bob based on the measurement results of the first particle. Additionally, we conduct an analysis of the detector blinding attack on the protocol in the subsequent section.

3.1 Intercept resend attack

The resend-intercept attack is one of the most significant threats to the security of quantum key distribution (QKD) protocols [50]. This attack allows an eavesdropper to intercept and measure the quantum states transmitted by Alice, then resend them to Bob while pretending to be Alice. If Eve is successful, she can obtain the shared secret key between Alice and Bob, compromising the security of their communication. In our protocol, two particles labeled A and B are sent through a quantum channel but with a time delay. Importantly, Eve, the potential eavesdropper, does not have simultaneous access to both particles. There are two types of resend intercept attack strategies in our protocol.

First: Eve intercepts the first particle sent by Alice through path 1. She performs a measurement on the particle to determine its quantum state. Based on the measurement outcome, Eve prepares a new particle in the same quantum state. Eve sends the prepared particle to Bob through path 1, pretending to be Alice.

Next, Eve intercepts the second particle sent by Alice through path 2. She analyzes the measurement outcome of the first particle to determine the basis (measurement reference) used by Alice for the second particle. Based on this information, Eve performs a specific measurement on the second particle to determine its quantum state. Using the basis information from the first particle and the new measurement outcome of the second particle, Eve prepares a new particle in the corresponding state. Eve sends the prepared particle to Bob through path 2, again mimicking Alice.

In our protocol, Alice randomly prepares a UPB state from Eq.1 and sends the particles through two different paths, randomly selecting either path 1 or path 2. If Alice sends the two particles in the AB sequence through these channels, then the state observed by Eve would follow Eq.1. On the other hand, if Alice sends the BA sequence, then the two-particle state observed by Eve would align with Eq.4. Eve does not know which specific state is transmitted through these channels, but she is aware that the intercepted state belongs to the set of 10 states $\{|\psi_1\rangle, \ldots, |\psi_5\rangle, |\xi_1\rangle, \ldots, |\xi_5\rangle\}$ represented by Eq.1 and Eq.4. For Eve, all the 10 states are equally probable. In this particular eavesdropping scenario, Eve employs a sequential approach.

When the first particle is intercepted in path 1, she conducts an orthogonal measurement using the basis $\{|0\rangle\langle 0|, |1\rangle\langle 1|, |2\rangle\langle 2|\}$. If she gets the first particle in the state $|0\rangle\langle 0|$, she infers the possible two-particle states for A and B, which are $|\psi_1\rangle$, $|\psi_2\rangle$, $|\psi_5\rangle$, $|\xi_1\rangle$, $|\xi_4\rangle$ and $|\xi_5\rangle$ with 1/10, 1/20, 1/30, 1/20, 1/10, 1/30 probabilities of each. Eve sends the first particle, having measured it, to Bob with the results of her measurement. When the second particle arrives, Eve intercepts it as well. She measures the second particle by using the bases $\{|0-1\rangle\langle 0-1|, |0+1\rangle\langle 0+1|, |2\rangle\langle 2|\}$. Based on this measurement, she sends the second particle to Bob. Eve's measurement results on the second particle, particularly if she observes $|0-1\rangle\langle 0-1|$, then the two-particle state is either $|\psi_1\rangle$ with 1/10 probability or $|\xi_1\rangle$ with 1/80 probability or $|\xi_4\rangle$ with 1/40 probability, which has collapsed to $|0\rangle|0-1\rangle$. If the second particle is observed in the state $|0+1\rangle\langle 0+1|$, the two-particle state collapses to $|0\rangle|0+1\rangle$. Bob then has a partial probability of 2/270 or 1/80 or 1/40 or 2/270 to find the two-particle state in either $|\psi_5\rangle$ or $|\xi_1\rangle$ or $|\xi_4\rangle$ or $|\xi_5\rangle$ respectively. If the second particle is observed in the state $|2\rangle\langle 2|$, the two-particle state collapses to $|0\rangle|2\rangle$. Bob then has a partial probability of 1/40 or 1/270 or 1/20 or 1/270 to find the two-particle state in either $|\psi_2\rangle$ or $|\psi_5\rangle$ or $|\xi_4\rangle$ or $|\xi_5\rangle$ respectively. So, when Eve gets the 1st particle in $|0\rangle$ and after getting the information of the first particle if Bob does a second measurement on the second particle with the measurement $\{|0-1\rangle\langle 0-1|, |0+1\rangle\langle 0+1|, |2\rangle\langle 2|\}$, then the probability for Eve to eavesdrop without detection is $\frac{1}{10}+\frac{1}{80}+\frac{1}{40}+\frac{2}{270}+\frac{1}{80}+\frac{1}{40}+\frac{2}{270}+\frac{1}{40}+\frac{1}{270}+\frac{1}{20}+\frac{1}{270}=0.2722$.

Instead of performing the measurement $\{|0-1\rangle\langle 0-1|, |0+1\rangle\langle 0+1|, |2\rangle\langle 2|\}$ on the second particle, Eve might choose alternative measurements like $\{|0\rangle\langle 0|, |1\rangle\langle 1|, |2\rangle\langle 2|\}$ or $\{|1-2\rangle\langle 1-2|, |1+2\rangle\langle 1+$

$2|, |0\rangle\langle 0|\}$. However, regardless of the measurement she chooses, the total probability of her successfully eavesdropping without detection remains the same, which is 0.2722, when the first particle is in the state $|0\rangle$.

Similarly in the same way, when Eve gets the 1st particle in $|1\rangle\langle 1|$ and after getting the information of the first particle if Bob does a second measurement on the second particle with the measurement $\{|0\rangle\langle 0|, |1\rangle\langle 1|, |2\rangle\langle 2|\}$, then the probability for Eve to eavesdrop without detection is $= 0.1222$.

Now, when Eve intercepts the 1st particle in $|2\rangle\langle 2|$, and if Bob performs a second measurement on the second particle with the measurement $\{|1-2\rangle\langle 1-2|, |1+2\rangle\langle 1+2|, |0\rangle\langle 0|\}$, then the probability for Eve to eavesdrop without detection is calculated to be 0.2722. Regardless of Eve's choice of alternative measurements, such as $\{|0\rangle\langle 0|, |1\rangle\langle 1|, |2\rangle\langle 2|\}$ or $\{|0-1\rangle\langle 0-1|, |0+1\rangle\langle 0+1|, |2\rangle\langle 2|\}$, the total probability of her successfully eavesdropping without detection remains the same at 0.2722 when the first particle is in the state $|2\rangle\langle 2|$.

So the total probability that Eve eavesdrops on the key information without being detected is $0.2722 + 0.1222 + 0.2722 = 0.6666$.

Second: The second eavesdropping strategy involves Eve focusing on the second particle, in path 2. Unlike the first strategy, this approach could lead to disruptions in particles in path 2. The motivation for this strategy is driven by the inherent symmetry between particles A and B within our subsystem. As our UPB state's subsystems are symmetric in this strategy, the resend intercept attack probability remains the same as the initial probability of 0.6666.

The calculation of the intercept-resend attack is based on LOCC. Cohen's paper [56] demonstrated that using LOCC and one ebit of entanglement resource, perfect distinction of the 3×3 UPB is achievable. However, in our scenario, if Eve attempts to distinguish the transmitted UPB states using LOCC with the entanglement resource, perfect distinction isn't possible. This is due to the random sequential transmission of the particles of each UPB state through the quantum channels, which makes her aware that the intercepted state belongs to the set of 10 states $\{|\psi_1\rangle, \ldots, |\psi_5\rangle, |\xi_1\rangle, \ldots, |\xi_5\rangle\}$. Among this set, some states are non-orthogonal, preventing perfect distinguishability. To determine the maximum success probability of unambiguous state discrimination, even if Eve employs two-particle measurements on each UPB state, we utilize a principle outlined in [55]. In this scenario, where a quantum system is prepared in one of the n states $|\phi_i\rangle, \ldots, |\phi_n\rangle$ in a d-dimensional Hilbert space with probabilities $p_1, \ldots, p_n$, the upper bound for the maximal success probability of unambiguous discrimination among n states using any measurement $\{M_m\}$ is given by:

$$D_m(p_1, \ldots, p_n, |\phi_1\rangle, \ldots, |\phi_n\rangle, \{M_m\}) \leq 1 - \frac{1}{(n-1)} \sum_{i \neq j} \sqrt{p_i p_j} |\langle \phi_i | \phi_j \rangle| \tag{5}$$

Here, n represents the number of states to be distinguished, $|\phi_i\rangle$ denotes each state to be discriminated, and p_i indicates the prior probability of the $|\phi_i\rangle$ state. In our specific system, if Eve aims to discriminate the transmitted state unambiguously among the set $\{|\psi_1\rangle, \ldots, |\psi_5\rangle, |\xi_1\rangle, \ldots, |\xi_5\rangle\}$ where each state is equally probable, the maximum success probability would be $\frac{8}{9}$. Thus the perfect discrimination of state in this set is not possible.

3.2 Detector blinding attack:

A detector blinding attack targets quantum key distribution (QKD) protocols, exploiting vulnerabilities in quantum signal detection to gain unauthorized access to sensitive information without raising the quantum bit error rate (QBER). In protocols like BB84, Eve intercepts Alice's qubits, measures them, and blinds Bob's detectors with intense light, controlling their firing to match her measure-

ments. Success relies on manipulating Bob's random number generator, rendering detectors blind. Without control, blinding alone wouldn't reveal the key, making detection challenging. Thus, the attack primarily hinges on controlling Bob's base selection, highlighting the importance of random number generator security in QKD [51].

Our protocol needs a two-particle joint measurement to distinguish the state, Eve cannot access both particles simultaneously during transmission. Hence, for eavesdropping, Eve needs to perform a single-particle measurement on the first particle and then choose the second-particle measurement based on the outcome of the first measurement. We assume that Eve can successfully blind the single-photon detectors.

In a linear optics setup, if Eve employs a faked-state attack, she intercepts the first particle, causing detector clicks based on her chosen measurement basis. Subsequently, based on the outcome of the first measurement, she selects which state to fake from the set $\{|\psi_1\rangle, \ldots, |\psi_5\rangle, |\xi_1\rangle, \ldots, |\xi_5\rangle\}$. She then sends the first particle's polarization state to Bob, accompanied by intense circularly polarized light. After intercepting the second particle sent by Alice, Eve performs a specific measurement on it to determine its quantum state. Depending on the predetermined state she intends to send after the first measurement, Eve forwards the polarization state of the second particle to Bob, again accompanied by intense circularly polarized light. Eve manipulates Bob's detectors to fire as she desires, aligning with her measurement results.

In our protocol, Alice randomly prepares and sends particles through quantum channels. After the measurement, Bob receives confirmation via a classical channel regarding the sequence (AB or BA) in which Alice sent the state. During this confirmation process, Bob can detect the presence of an eavesdropper. For instance, if Alice sends an AB sequence state but Eve decides to send a BA sequence state based on the first measurement outcome, Bob's detectors will not click any of the AB sequence states (Eq.1) but instead detect a different sequence, indicating interference. Therefore, Bob becomes aware of the eavesdropper. However, Eve has a 50% chance of blinding Bob's detectors successfully since her decision will align with either the AB or BA sequence half of the time.

As an example, let's consider Alice sending a state $|\psi_1\rangle$ in the AB sequence. Eve intercepts the first particle and measures it in the $\{|0\rangle\langle 0|, |1\rangle\langle 1|, |2\rangle\langle 2|\}$ bases, obtaining a click in the $|0\rangle\langle 0|$ basis. Based on this measurement outcome, Eve infers that the two-particle state could be one among the set $\{|\psi_1\rangle, |\psi_2\rangle, |\psi_5\rangle, |\xi_1\rangle, |\xi_4\rangle, |\xi_5\rangle\}$. Suppose Eve decides to send a fake state $|\xi_1\rangle$ and transmits the subsystem states to Bob sequentially. Due to the fake state sent by Eve, Bob's detector will not click any of the AB sequence states (Eq.1). When Bob communicates with Alice to confirm the sequence via the classical channel, he realizes that eavesdropping has occurred, even if Eve can intercept and listen to the classical messages.

Lastly, the security amplification process is also present, where Alice and Bob will compare their certain shared bits, right or wrong, during that process to identify the attack.

4 Conclusion:

A primary contribution of our research lies in the investigation of orthogonal state encoding and the incorporation of UPB into QKD protocols. Through theoretical analysis, we have demonstrated the viability of employing 3×3 tile UPB [37, 38] to establish secure quantum communication channels between distant parties.

Furthermore, our study has provided insights into the vulnerabilities of QKD protocols through the analysis of intercept-resend [50] and detector blinding attacks [51]. An intercept-resend attack is a cybernetic attack on quantum key distribution systems, where the attacker, often referred to as Eve, intercepts quantum signals intended for the recipient, Bob, without being detected. In the BB84

protocol, there is a 75% chance for an eavesdropper to remain undetected. By quantifying the probabilities and outcomes associated with these attacks within the framework of our protocol, we have identified an efficient intercept-resend attack, resulting in a 66% chance of successful eavesdropping without detection. There is a paper [56] that demonstrated how one ebit of entanglement enables perfect discrimination of 3×3 UPB states via LOCC. However, our protocol incorporates sequential particle transmission, complicating the eavesdropper's ability to distinguish the UPB state. Upon observing the transmitted UPB state, the eavesdropper encounters a set $\{|\psi_1\rangle, \ldots, |\psi_5\rangle, |\xi_1\rangle, \ldots, |\xi_5\rangle\}$ containing non-orthogonal states. This non-orthogonality hinders perfect state discrimination, resulting in imperfect discrimination even if she uses entanglement. Furthermore, we showed that even if an eavesdropper employs any measurement, she would only be able to unambiguously distinguish the transmitted state with a maximum success probability of $\frac{8}{9}$.

Other eavesdropping strategies include Eve storing the first particle in a quantum memory and sending a random state to Bob, followed by a joint measurement on both particles. However, success in this scenario is limited to $\frac{1}{3}$. In orthogonal state quantum cryptography, each subsystem of the orthogonal bipartite state is successively sent through the two quantum channels, dividing information transmission into two stages. This ensures that only a fraction of information is conveyed at any given moment. Additionally, quantum memories have limited storage time, and once this time limit is reached, extracting information becomes impossible [32, 33, 34, 35, 36]. Furthermore, the delay time in our scenario exceeds the time taken by particles to travel from Alice to Bob, enhancing security due to the no-cloning theorem applicable to orthogonal states [39].

While quantum key distribution (QKD) protocols are renowned for their unconditional secrecy, the security of QKD hardware hinges significantly on the intricacies of its implementation. A detector blinding attack poses a security threat in quantum cryptography, allowing an eavesdropper to manipulate quantum detectors to intercept communication without detection [51]. Even if we consider the possibility of an adversary successfully blinding the single-photon detectors, our protocol has a 50% chance for an eavesdropper to achieve successful detector blinding. It's worth noting that our protocol involves the transmission of two-particle states, which are product states.

Recent advancements in hardware and protocols offer robust countermeasures against detector-blinding attacks [52, 53, 54]. Enhancing the integrity of Bob's detectors is crucial, potentially achieved through incorporating randomized control mechanisms into their operation. By introducing randomness, it becomes more challenging for adversaries to predict and manipulate the detector's behavior, thus bolstering its resilience against manipulation attempts.

Our investigation into utilizing 3×3 tile UPBs for establishing secure quantum keys highlights their indistinguishability under the LOCC paradigm. While our protocol restricts eavesdroppers' access to two-particle states, a time gap between transmissions limits adversaries to LOCC tools for eavesdropping. We acknowledge the potential existence of better protocols for utilizing UPBs in QKD and generalizing them for $d \times d$ dimensions. To extend our protocol, one may follow the same steps and formulate a quantum measurement. Let $|\psi_1\rangle, \ldots, |\psi_l\rangle$ form the UPB in $\mathbb{C}^d \otimes \mathbb{C}^d$ [57, 58], where $\sum_{i=1}^{l} |\psi_i\rangle\langle\psi_i| \neq \mathbb{I}$ and $|\psi_l\rangle$ is the stopper basis. Construct complete measurement bases by first forming orthogonal bases $|h_{l+1}\rangle, \ldots, |h_{d^2}\rangle$ orthogonal to each basis of $|\psi_1\rangle, \ldots, |\psi_{l-1}\rangle$, with $\langle h_k|\psi_i\rangle = 0$ for $i = 1, \ldots, l-1$ and $k = l+1, \ldots, d^2$ and then, formulate:

$$
\begin{aligned}
|\psi_{l+1}\rangle &= \alpha_{l+1}\Big(|h_{l+1}\rangle - \sum_{i=1}^{l} \langle\psi_i|h_{l+1}\rangle|\psi_i\rangle\Big) \\
|\psi_k\rangle &= \alpha_k\Big(|h_k\rangle - \sum_{i=1}^{l} \langle\psi_i|h_k\rangle|\psi_i\rangle - \sum_{j=l+1}^{k-1} \langle\psi_j|h_k\rangle|\psi_j\rangle\Big) \quad \text{for} \;\; k = l+2, \ldots, d^2
\end{aligned} \tag{6}
$$

such that $\sum_{i=1}^{d^2} |\psi_i\rangle\langle\psi_i| = \mathbb{I}$. Here, α_k is the normalization constant of the state $|\psi_k\rangle$. Let's say, if the number of UPB in a $d \times d$ system is $d^2 - 2d + 1$, then one has to form $2d - 1$ number of entangled bases to construct a complete set of measurement bases [57]. Using our protocol, one can distribute the quantum key between distant parties using the $d \times d$ UPBs. Exploring the optimal intercept resend attack probability would be a compelling avenue for future research.

In conclusion, our study advances quantum cryptography by elucidating orthogonal state encoding principles, UPBs, and their role in fortifying quantum communication. Rigorous analysis of intercept-resend and detector blinding attacks provides valuable insights for establishing secure communication channels in the quantum technology era.

Acknowledgements:

This work is for the organization ExamRoom.AI. The authors are also thankful to Priti Kumari, and Ritobroto Mohanta for the helpful discussions.

References

[1] P. Shor, *Algorithms for quantum computation: discrete logarithms and factoring*, In Proceedings of 35th Annual Symposium on the Foundations of Computer Science, IEEE Computer Soc

[2] L. K. Grover, *A fast quantum mechanical algorithm for database search*, Proceedings of the twenty-eighth annual ACM symposium on Theory of Computing, Pages 212-219, (1996)

[3] D. J. Bernstein and T. Lange, *Post-quantum cryptography,*, Nature, **549**, 188–194, (2017).

[4] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, *Quantum cryptography*, Rev. Mod. Phys. **74**, 145, (2002).

[5] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dusek, N. Lutkenhaus, M. Peev, *The Security of Practical Quantum Key Distribution*, Rev. Mod. Phys. **81**, 1301, (2009).

[6] S. Pirandola, U. L. Andersen, L. Banchi, M. Berta, D. Bunandar, R. Colbeck, D. Englund, T. Gehring, C. Lupo, C. Ottaviani, J. Pereira, M. Razavi, J. S. Shaari, M. Tomamichel, V. C. Usenko, G. Vallone, P. Villoresi, and P. Wallden, *The Security of Practical Quantum Key Distribution*, Adv. Opt. Photon. **12**, 1012-1236, (2020).

[7] W. K. Wootters and W. H. Zurek , *A single quantum cannot be cloned*, Nature **299**, 802-803 (1982).

[8] C. H. Bennett, G. Brassard, *Quantum cryptography: Public key distribution and coin tossing*, Theoretical Computer Science, **560**, 2014, pp. 7-11, (1984).

[9] Artur K. Ekert, *Quantum Cryptography Based on Bell's Theorem*, Phys. Rev. lett. **67**, 661 (1991).

[10] C. H. Bennett, *Quantum cryptography using any two nonorthogonal states*, Phys. Rev. lett. **68**, 3121 (1992).

[11] C. H. Bennett, G. Brassard, and N. David Mermin, *Quantum cryptography without Bell's theorem*, Phys. Rev. lett. **68**, 557 (1992).

[12] Dagmar Bruß, *Optimal Eavesdropping in Quantum Cryptography with Six States*, Phys. Rev. lett. **81**, 3018 (1998).

[13] H.K Lo AND H. F. Chau, *Unconditional Security of Quantum Key Distribution over Arbitrarily Long Distances*, SCIENCE 283, **283**, Issue 5410, 2050-2056 (1999).

[14] D. Mayers, A. Yao, *Quantum cryptography with imperfect apparatus*, Proceedings 39th Annual Symposium on Foundations of Computer Science (Cat. No.98CB36280), Palo Alt

[15] A. Acín, N. Brunner, N. Gisin, S. Massar, S. Pironio, and V. Scarani, *Device-Independent Security of Quantum Cryptography against Collective Attacks*, Phys. Rev. lett. **98**, 230501 (2007).

[16] H. Lo, M. Curty, and B. Qi, *Measurement-Device-Independent Quantum Key Distribution*, Phys. Rev. lett. **108**, 130503 (2012).

[17] R Valivarthi, *Measurement-device-independent quantum key distribution coexisting with classical communication*, Quantum Sci. Technol. **4**, 045002 (2019).

[18] T. C. Ralph, *Continuous variable quantum cryptography*, Phys. Rev. A(R) **61**, 010303 (1999).

[19] A. Rani et. al., *Free space continuous variable Quantum Key Distribution with discrete phases*, Physics Open, **17**, 100162 (2023).

[20] M. Mehic et. al., *Quantum Key Distribution: A Networking Perspective*, ACM Computing Surveys, **53**, 96, 1-41 (2020).

[21] D. P. Nadlinger et. al., *Experimental quantum key distribution certified by Bell's theorem*, Nature **607**, 682-686 (2022).

[22] J. Yin et. al., *Satellite-based entanglement distribution over 1200 kilometers*, Science **356**, 1140-1144 (2017).

[23] E. Diamanti et. al., *Practical challenges in quantum key distribution*, npj Quantum Inf **2**, 16025 (2016).

[24] S. K. Liao et. al., *Satellite-to-ground quantum key distribution*, npj Quantum Inf **549**, 43 (2017).

[25] L. Goldenberg and L. Vaidman, *Quantum Cryptography Based on Orthogonal States*, Phys. Rev. Lett. **75**, 1239 (1995).

[26] Fu-Guo Deng and G. L. Long, *Controlled order rearrangement encryption for quantum key distribution*, Phys. Rev. A **68**, 042315 (2003).

[27] A. D. Zhu, Y. Xia, Q. B. Fan, and S. Zhang, *Secure direct communication based on secret transmitting order of particles*, Phys. Rev. A **73**, 02233 (2006).

[28] P. Yadav, R. Srikanth, and A. Pathak, *Two-step orthogonal-state-based protocol of quantum secure direct communication with the help of order-rearrangement technique*, Quantum Inf Process **13**, 2731–2743 (2014).

[29] G. P. Guo, C. F. Li, B. S. Shi, J. Li, and G. C. Guo, *Quantum key distribution scheme with orthogonal product states*, Phys. Rev. A **64**, 042301 (2001).

[30] A. Avella, G. Brida, I. Pietro Degiovanni, M. Genovese, M. Gramegna, and P. Traina, *Experimental quantum-cryptography scheme based on orthogonal states*, Phys. Rev. A **82**, 062309 (2010).

[31] G.B. Xavier, G.P. Temporão, J.P. von der Weid, *Employing long fibre-optical Mach-Zehnder interferometers for quantum cryptography with orthogonal states*, Electronics letter **48**, 775-777 (2012).

[32] S. Wehner, C. Schaffner, and B. M. Terhal, *Cryptography from Noisy Storage*, Phys. Rev. Lett. **100**, 220502 (2008).

[33] S. Wehner, M. Curty, C. Schaffner, and H. K. Lo, *Implementation of two-party protocols in the noisy-storage model*, Phys. Rev. A **81**, 052336 (2009).

[34] C. Erven, N. Ng, N. Gigov, R. Laflamme, S. Wehner, and G. Weihs, *An experimental implementation of oblivious transfer in the noisy storage model*, Nat Commun **5**, 3418 (2014).

[35] S. Wehner, and J. Wullschleger, *Composable Security in the Bounded-Quantum-Storage Model*, Automata, Languages and Programming. ICALP 2008. Lecture Notes in Computer Science. Springer, Berl

[36] I. Damgaard, S. Fehr, L. Salvail, and C. Schaffner, *Cryptography In the Bounded Quantum-Storage Model*, Proceedings of the 46th IEEE Symposium on Foundations of Computer Science-FOCS, 449

[37] C. H. Bennett, D. P. DiVincenzo, T. Mor, P. W. Shor, J. A. Smolin, and B. M. Terhal, *Unextendible Product Bases and Bound Entanglement*, Phys. Rev. lett, **82**, 5385, (1999).

[38] D. P. DiVincenzo, T. Mor, P. W. Shor, J. A. Smolin, B. M. Terhal, *Unextendible Product Bases, Uncompletable Product Bases and Bound Entanglement*, Comm. Math. Phys. **238**, 379-410 (2003).

[39] Tal Mor, *No Cloning of Orthogonal States in Composite Systems*, Phys. Rev. Lett. **80**, 3137 (1998).

[40] H. Bechmann-Pasquinucci and W. Tittel, *Quantum cryptography using larger alphabets*, Phys. Rev. A **61**, 062308 (2000).

[41] N. J. Cerf, Mohamed Bourennane, Anders Karlsson, and Nicolas Gisin, *Security of Quantum Key Distribution Using d-Level Systems*, Phys. Rev. lett. **88**, 127902 (2002).

[42] Lana Sheridan and Valerio Scarani, *Security proof for quantum key distribution using qudit systems*, Phys. Rev. A(R). **82**, 030301(R) (2010).

[43] Zhao Liu and Heng Fan, *Decay of multiqudit entanglement*, Phys. Rev. A. **79**, 064305 (2009).

[44] Patrick Navez and Nicolas J. Cerf, *Cloning a real d-dimensional quantum state on the edge of the no-signaling condition*, Phys. Rev. A, **68**, 032313 (2003).

[45] Dagmar Bruß, Chiara Macchiavello, *Optimal state estimation for d-dimensional quantum systems*, Physics Letters A, **253**, Issues 5–6, Pages 249-251 032313 (1999).

[46] Honghao Fu, Debbie Leung, and Laura Mancinska, *When the asymptotic limit offers no advantage in the local-operations-and-classical-communication paradigm*, Phys. Rev. A, **89**, 052310 (2013).

[47] Scott M. Cohen, *Local approximation of multipartite quantum measurements*, Phys. Rev. A, **105**, 022207 (2022).

[48] S. De Rinaldis, *Distinguishability of complete and unextendible product bases*, Phys. Rev. A, **70**, 022309 (2004).

[49] Scott M. Cohen, *Understanding entanglement as resource: Locally distinguishing unextendible product bases*, Phys. Rev. A, **77**, 012304 (2008).

[50] M. Curty, and N. Lütkenhaus, *Intercept-resend attacks in the Bennett-Brassard 1984 quantum-key-distribution protocol with weak coherent pulses*, Phys. Rev. A, **71**, 062301 (2004).

[51] I. Gerhardt, Q. Liu, A. Lamas-Linares, J. Skaar, C. Kurtsiefer, and V. Makarov, *Full-field implementation of a perfect eavesdropper on a quantum cryptography system*, Nat Communs, **2**, 349 (2011).

[52] Z. L. Yuan, J. F. Dynes, and A. J. Shields, *Avoiding the blinding attack in QKD*,Nature Photon, **2**, 800 (2010).

[53] M. Stipčević, *Preventing detector blinding attack and other random number generator attacks on quantum cryptography by use of an explicit random number generator*, arXiv:1403.0143 (2014).

[54] C. C. W. Lim et.al, *Random Variation of Detector Efficiency: A Countermeasure Against Detector Blinding Attacks for Quantum Key Distribution*,IEEE Journal of Selected Topics in Quantum Electronics **21**, 192 (2015).

[55] S. Zhang, Y. Feng, X. Sun, and M. Ying, *Upper bound for the success probability of unambiguous discrimination among quantum states*, Phys. Rev. A **64**, 062103 (2001).

[56] S. M. Cohen, *Understanding entanglement as resource: Locally distinguishing unextendible product bases*, Phys. Rev. A **77**, 012304 (2008).

[57] D. P. DiVincenzo, T. Mor, P. W. Shor, J. A. Smolin, and B. M. Terhal, *Unextendible Product Bases, Uncompletable Product Bases and Bound Entanglement*, Commun. Math. Phys. **238**, 379 (2003).

[58] F. Shi, X. Zhang, and L. Chen, *Unextendible product bases from tile structures and their local entanglement-assisted distinguishability*, Phys. Rev. A **101**, 062329 (2020).

Appendix:

A Reduced states:

The reduced subsystems of Eq.1 and Eq.3 for A and B are evaluated by using the relation $\rho_{A(B)|i} = \mathrm{Tr}_{B(A)}(|\psi_i\rangle_{AB}\langle\psi_i|)$, where $\rho_{A(B)}$ represents the reduced state of A and B for the i-th state $|\psi_i\rangle$.

Table 1: Reduced density matrices of individual subsystems

$\rho_{A\|i}$	$\rho_{B\|i}$
$\rho_{A\|1} = \|0\rangle\langle 0\|$	$\rho_{B\|1} = \frac{1}{2}\|0-1\rangle\langle 0-1\|$
$\rho_{A\|2} = \frac{1}{2}\|0-1\rangle\langle 0-1\|$	$\rho_{B\|2} = \|2\rangle\langle 2\|$
$\rho_{A\|3} = \|2\rangle\langle 2\|$	$\rho_{B\|3} = \frac{1}{2}\|1-2\rangle\langle 1-2\|$
$\rho_{A\|4} = \frac{1}{2}\|1-2\rangle\langle 1-2\|$	$\rho_{B\|4} = \|0\rangle\langle 0\|$
$\rho_{A\|5} = \frac{1}{3}\|0+1+2\rangle\langle 0+1+2\|$	$\rho_{B\|5} = \frac{1}{3}\|0+1+2\rangle\langle 0+1+2\|$
$\rho_{A\|6} = \frac{1}{21}(4\|0-1\rangle\langle 0-1\| + 4\|0-2\rangle\langle 0-2\| - 2\|1-2\rangle\langle 1-2\| + 9\|0\rangle\langle 0\|)$	$\rho_{B\|6} = \frac{1}{42}(19\|0+1\rangle\langle 0+1\| + 2\|0-2\rangle\langle 0-2\| + 2\|1-2\rangle\langle 1-2\| - 2\|0\rangle\langle 0\| - 2\|1\rangle\langle 1\|)$
$\rho_{A\|7} = \frac{1}{70}(25\|0+1\rangle\langle 0+1\| + 2\|1-2\rangle\langle 1-2\| + 10\|0-2\rangle\langle 0-2\| - 10\|0\rangle\langle 0\| + 6\|1\rangle\langle 1\|)$	$\rho_{B\|7} = \frac{1}{35}(4\|0+1\rangle\langle 0+1\| + 3\|0-2\rangle\langle 0-2\| + 3\|1-2\rangle\langle 1-2\| - 3\|0\rangle\langle 0\| - 3\|1\rangle\langle 1\| + 21\|2\rangle\langle 2\|)$
$\rho_{A\|8} = \frac{1}{15}(\|1-2\rangle\langle 1-2\| + 3\|1\rangle\langle 1\| + 10\|2\rangle\langle 2\|)$	$\rho_{B\|8} = \frac{1}{30}(9\|1+2\rangle\langle 1+2\| + 2\|0-1\rangle\langle 0-1\| + 6\|0-2\rangle\langle 0-2\| + 2\|1\rangle\langle 1\| - 6\|2\rangle\langle 2\|)$
$\rho_{A\|9} = \frac{1}{6}\|1+2\rangle\langle 1+2\| + \frac{4}{6}\|1\rangle\langle 1\|$	$\rho_{B\|9} = \frac{1}{3}\|0-1\rangle\langle 0-1\| + \frac{1}{3}\|1\rangle\langle 1\|$