entropy

MDPI

Article

Distinguishability and Disturbance in the Quantum Key Distribution Protocol Using the Mean Multi-Kings' Problem

Masakazu Yoshida [1,*], Ayumu Nakayama [2] and Jun Cheng [3]

[1] Faculty of Design Technology, Osaka Sangyo University, 3-1-1 Daito-shi, Osaka 574-8530, Japan
[2] Independent Researcher, Chiba 263-8522, Japan; chiba.u.nakayama@gmail.com
[3] Faculty of Science and Engineering, Doshisha University, 1-3 Kyotanabe-shi, Kyoto 610-0394, Japan; jcheng@mail.doshisha.ac.jp
* Correspondence: yoshida@ise.osaka-sandai.ac.jp

Received: 7 October 2020; Accepted: 9 November 2020; Published: 11 November 2020

Abstract: We introduce a quantum key distribution protocol using mean multi-kings' problem. Using this protocol, a sender can share a bit sequence as a secret key with receivers. We consider a relation between information gain by an eavesdropper and disturbance contained in legitimate users' information. In BB84 protocol, such relation is known as the so-called information disturbance theorem. We focus on a setting that the sender and two receivers try to share bit sequences and the eavesdropper tries to extract information by interacting legitimate users' systems and an ancilla system. We derive trade-off inequalities between distinguishability of quantum states corresponding to the bit sequence for the eavesdropper and error probability of the bit sequence shared with the legitimate users. Our inequalities show that eavesdropper's extracting information regarding the secret keys inevitably induces disturbing the states and increasing the error probability.

Keywords: quantum key distribution; mean-king's problem; mean multi-kings' problem; information disturbance theorem

1. Introduction

In the quantum state discrimination problems, one tries to discriminate the quantum states by performing the single measurement. Several strategies exist, e.g., in [1–3] and Section 9.1.4 in [4]. On the other hand, in the mean-king's problem [5], one can use not the single measurement but also post-information. Specific setting of the mean-king's problem is often told as a tale [6] of a king and a physicist Alice. In the tale, Alice prepares a qubit in an initial state at first. The king performs a measurement with one of observables $\sigma_x, \sigma_y, \sigma_z$ on the qubit and obtains an outcome. Then, Alice obtains an outcome by performing a measurement on the qubit. After the measurement, the king reveals the observable he has measured as the post-information. Then, Alice tries to guess king's outcome by using her outcome and the post-information. A solution to the problem is a pair of the initial state and Alice's measurement such that she can guess king's outcome correctly. Using Aharonov–Bergman–Lebowitz rule [7], a solution which consists of Bell state and a measurement on a bipartite system has been shown [5]. As an application of the solution to the mean-king's problem, a quantum key distribution protocol (QKD) has been shown [8]. In this protocol, Alice and the king employ the guessing result as a secret key, and security analysis of the protocol has been considered [8–11].

A QKD protocol by using mean multi-kings' problem has been shown [12] (see Section 2 for details). In this protocol, Alice and kings (called King$_1$, King$_2$, ..., King$_n$) are legitimate users. Alice guesses each king's measurement outcome by using her measurement outcome and post-information from each king; then, each guessing result is shared as a secret key between Alice and each king. The protocol has superior aspects, such as the number of measurements, state preparation and key discarding, to several realizations (whose components are the QKD protocol by using the mean-king's problem or BB84 protocol [13]) for Alice and each king to share the secret key. In the case of $n = 2$, security analysis against a simple attack so called intercept-resend attack has been considered and error rate of bits shared between Alice and the kings has been shown.

In this paper, we consider a relation between information gain by an eavesdropper (called Eve) and disturbance contained in the legitimate users' information in the QKD protocol by using the mean multi-kings' problem. In BB84 protocol, such relation is known as the so-called information disturbance theorem [14–18]. According to the theorem, Eve's information gain in a basis inevitably induces disturbance contained in the legitimate users' information in the conjugate basis. Therefore, the theorem is also regarded as an information theoretical version of the uncertainty relation. The theorem also plays an important role in the proof of the unconditional security [19]. We consider that Eve tries to extract information by employing an attack which she performs any measurement on her quantum system at any time after interacting the quantum system with kings' qubits after their measurements in the case of $n = 2$. In this setting, we give trade-off inequalities between distinguishability of quantum states corresponding to the bit sequences for Eve and error probability of the bit sequences shared with Alice and the kings. Our inequalities show that Eve's extracting information regarding the secret keys inevitably induces disturbing the states of kings' qubits and increasing the error probability even though the post-information and Alice's qubit are used in the guessing step, unlike BB84 protocol.

This paper is organized as follows. In the next section, we review a description of the quantum key distribution protocol by using the mean multi-kings' problem. In Section 3, we give the description of the protocol in the case of $n = 2$. In Section 4, we give the outline of the attack and the trade-off inequalities between distinguishability and disturbance. Finally, we summarize this paper in Section 5.

2. Protocol

Let us start by introducing the essence of the mean multi-kings' problem and the QKD by using it. Alice and King$_1$, King$_2$, ... , King$_n$ are the characters in this problem. The problem can be summarized as follows. Alice prepares a composite system, which consists of her system and n systems for kings, in an initial state. Each king performs a measurement on his system and obtains an outcome. After kings' measurement, Alice performs a measurement on the composite system and obtains an outcome. Furthermore, each king reveals post-information: the measurement type he has performed. Immediately, Alice guesses kings' outcomes by using her outcome and the post-information from each king. A solution to the problem is defined as a three-tuple of the initial state, Alice's measurement, and a guessing function such that she can guess kings' outcomes correctly. In this problem, the initial state will be changed depending on the kings' measurements and outcomes. In general, it is impossible to distinguish the changed states correctly. Therefore, Alice tries to get some potential answers by performing the measurement and to narrow down the correct outcome from them by using the guessing function of her outcome and the post-information.

We can construct the QKD protocol by using a setting of the mean multi-kings' problem and a solution to it, i.e., Alice and each king share the guessing result as a secret key. Figure 1 is a graphically demonstrated protocol. Let us consider a setting that Alice prepares a composite system which consists of $n + 1$ qubits and each king performs one of two fixed measurements on his qubit. Then, two solutions where the initial states are multipartite entangled states can be shown as described below; therefore, we can also construct the QKD protocol by using those solutions. In the QKD, Alice and each king try to share secret keys while she switches the solutions.

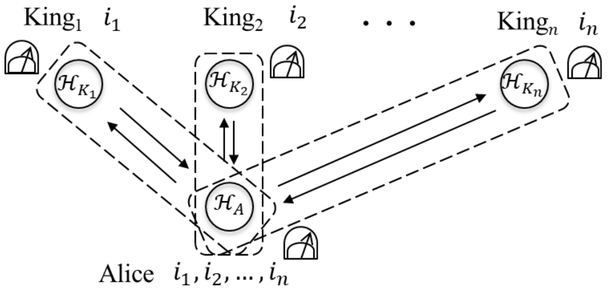

Figure 1. The QKD protocol by using the mean multi-kings' problem.

Before introducing details of the QKD protocol, we introduce some preliminary definitions, the setting of the mean multi-kings' problem, and the solutions to it. Define

$$Z_0 := |0\rangle\langle 0|, Z_1 := |1\rangle\langle 1|, X_0 := |\bar{0}\rangle\langle\bar{0}|, X_1 := |\bar{1}\rangle\langle\bar{1}| \tag{1}$$

for $|0\rangle := (1,0)^T, |1\rangle := (0,1)^T, |\bar{0}\rangle := \frac{1}{\sqrt{2}}(1,1)^T, |\bar{1}\rangle := \frac{1}{\sqrt{2}}(1,-1)^T$. Define an outcome set

$$\mathcal{K} := \{(s_1, t_1, s_2, t_2, \ldots, s_n, t_n) \mid s_j, t_j \in \{0,1\}\}, \tag{2}$$

operators for $(s_1, t_1, s_2, t_2, \ldots, s_n, t_n) \in \mathcal{K}$

$$E^{(Z)}_{(s_1,t_1,s_2,t_2,\ldots,s_n,t_n)} := X_{s_1} Z_{t_1} \otimes X_{s_2} Z_{t_2} \otimes \cdots \otimes X_{s_n} Z_{t_n}, \tag{3}$$

$$E^{(X)}_{(s_1,t_1,s_2,t_2,\ldots,s_n,t_n)} := Z_{s_1} X_{t_1} \otimes Z_{s_2} X_{t_2} \otimes \cdots \otimes Z_{s_n} X_{t_n}, \tag{4}$$

and an index set

$$S^{(W)}_{(J_j,i_j)_{j=1}^n} = S^{(W)}_{(J_1,i_1,J_2,i_2,\ldots,J_n,i_n)} := S^{(W)}_{(J_1,i_1)} \times S^{(W)}_{(J_2,i_2)} \times \cdots \times S^{(W)}_{(J_n,i_n)} \tag{5}$$

($W \in \{Z, X\}$) which consists of direct product of

$$S^{(Z)}_{(J,i)} := \begin{cases} \{(0,i),(1,i)\} & (J = 0, i \in \{0,1\}) \\ \{(i,0),(i,1)\} & (J = 1, i \in \{0,1\}), \end{cases} \tag{6}$$

$$S^{(X)}_{(J,i)} := \begin{cases} \{(i,0),(i,1)\} & (J = 0, i \in \{0,1\}) \\ \{(0,i),(1,i)\} & (J = 1, i \in \{0,1\}). \end{cases} \tag{7}$$

We define the setting of the mean multi-kings' problem. Alice prepares the composite system ($n+1$ qubits) $\tilde{\mathcal{H}} := \mathcal{H}_A \otimes \mathcal{H}_{K_1} \otimes \mathcal{H}_{K_2} \otimes \cdots \otimes \mathcal{H}_{K_n} \simeq (\mathbb{C}^2)^{\otimes n+1}$ in an initial state. Each King$_j$ performs one of the measurements on $\mathcal{H}_{K_j}$

$$M^{(J_j)} = (M_0^{(J_j)}, M_1^{(J_j)}) \ (J_j \in \{0,1\}), \tag{8}$$

where $M^{(0)} := (M_0^{(0)} := Z_0, M_1^{(0)} := Z_1)$ and $M^{(1)} := (M_0^{(1)} := X_0, M_1^{(1)} := X_1)$, and obtains an outcome $i_j \in \{0,1\}$. Alice performs a measurement on $\tilde{\mathcal{H}}$ and obtains an outcome. After Alice's measurement, the kings reveal $(J_j)_{j=1}^n$ as the post-information. Then, Alice tries to guess kings' outcomes by using her outcome and the post-information.

Here, we show two solutions to the problem. In this case, Alice can guess the kings' outcomes correctly by employing one of

$$|\Phi^{(Z)}\rangle := \frac{1}{\sqrt{2}}(|00\cdots 0\rangle + |11\cdots 1\rangle) \tag{9}$$

$$|\Phi^{(X)}\rangle := \frac{1}{\sqrt{2}}(|\bar{0}\bar{0}\cdots \bar{0}\rangle + |\bar{1}\bar{1}\cdots \bar{1}\rangle) \tag{10}$$

as an initial state, a measurement depending on the initial state $|\Phi^{(W)}\rangle$

$$P^{(W)} := \left(P_k^{(W)} := 2^{n+1}|(\mathbb{I}\otimes E_k^{(W)})\Phi^{(W)}\rangle\langle(\mathbb{I}\otimes E_k^{(W)})\Phi^{(W)}|\right)_{k\in\mathcal{K}} \tag{11}$$

and a guessing function $s(k,(J_j)_{j=1}^n,\Phi^{(W)})$ of her outcome $k\in\mathcal{K}$, the post-information $(J_j)_{j=1}^n$, and the initial state $|\Phi^{(W)}\rangle$, where $s(k,(J_j)_{j=1}^n,\Phi^{(W)})$ is defined as $(i_j)_{j=1}^n$ satisfying $k\in S^{(W)}_{(J_j,i_j)_{j=1}^n}$ (we regard $k=(s_1,t_1,s_2,t_2,\ldots,s_n,t_n)$ in the same light as $((s_1,t_1),(s_2,t_2),\ldots,(s_n,t_n))$).

We clear the number of non-zero matrices in her measurement and their orthogonality. We can observe

$$\begin{aligned}
|(\mathbb{I}\otimes E_k^{(Z)})\Phi^{(Z)}\rangle &= (\mathbb{I}\otimes X_{s_1}Z_{t_1}\otimes\cdots\otimes X_{s_n}Z_{t_n})\tfrac{1}{\sqrt{2}}(|00\cdots 0\rangle + |11\cdots 1\rangle)\\
&= \tfrac{1}{\sqrt{2}}(\delta_{t_1 0}\cdots\delta_{t_n 0}|0\rangle X_{s_1}|0\rangle\otimes X_{s_2}|0\rangle\otimes\cdots\otimes X_{s_n}|0\rangle\\
&\quad +\delta_{t_1 1}\cdots\delta_{t_n 1}|1\rangle\otimes X_{s_1}|1\rangle\otimes X_{s_2}|1\rangle\otimes\cdots\otimes X_{s_n}|1\rangle).
\end{aligned} \tag{12}$$

Then, the number of non-zero vectors is equal to 2^{n+1}. It leads to the conclusion that the number of non-zero matrices in $P^{(Z)}$ is equal to 2^{n+1}. Furthermore, we observe

$$\begin{aligned}
&\langle(\mathbb{I}\otimes E_k^{(Z)})\Phi^{(Z)}|(\mathbb{I}\otimes E_{k'}^{(Z)})\Phi^{(Z)}\rangle\\
=\ &\langle(\mathbb{I}\otimes X_{s_1}Z_{t_1}\otimes\cdots\otimes X_{s_n}Z_{t_n})\Phi^{(Z)}|(\mathbb{I}\otimes X_{s_1'}Z_{t_1'}\otimes\cdots\otimes X_{s_n'}Z_{t_n'})\Phi^{(Z)}\rangle\\
=\ &\tfrac{1}{2^{n+1}}(\delta_{t_1 0}\delta_{t_2 0}\cdots\delta_{t_n 0}+\delta_{t_1 1}\delta_{t_2 1}\cdots\delta_{t_n 1})\delta_{kk'}.
\end{aligned} \tag{13}$$

It implies that $P^{(Z)}$ is an orthogonal measurement on $\tilde{\mathcal{H}}$. When Z is switched to X, we have the same result in the case of $W=X$.

Next, we show that Alice can correctly guess kings' outcomes. We observe

$$S^{(W)}_{(J_j,i_j)_{j=1}^n}\cap S^{(W)}_{(J_j,i_j')_{j=1}^n}=\emptyset \tag{14}$$

for any J_j and $(i_1,i_2,\ldots,i_n)\neq(i_1',i_2',\ldots,i_n')$, and

$$M_{i_1}^{(J_1)}\otimes M_{i_2}^{(J_2)}\otimes\cdots\otimes M_{i_n}^{(J_n)}=\sum_{k\in S^{(W)}_{(J_j,i_j)_{j=1}^n}} E_k^{(W)} \tag{15}$$

holds for any J_j and i_j. When King$_j$ performs the measurement $M^{(J_j)}$ and obtains an outcome i_j, by Equation (15), the post-measurement state is proportional to

$$|(\mathbb{I}\otimes M_{i_1}^{(J_1)}\otimes M_{i_2}^{(J_2)}\otimes\cdots\otimes M_{i_n}^{(J_n)})\Phi^{(W)}\rangle\in\bigoplus_{k\in S^{(W)}_{(J_j,i_j)_{j=1}^n}}\mathcal{A}_k, \tag{16}$$

where $\mathcal{A}_k$ is a subspace spanned by $|(\mathbb{I}\otimes E_k^{(W)})\Phi^{(W)}\rangle$. $\mathcal{A}_k$ and $\mathcal{A}_{k'}$ are orthogonal for any $k\neq k'$ and $P^{(W)}$ is composed of orthogonal projections onto each subspace $\mathcal{A}_k$ by Equation (13). If Alice obtains an outcome k by performing $P^{(W)}$ and the post-information $(J_j)_{j=1}^n$ from the kings, then kings' outcomes

$(i_j)_{j=1}^n$ should satisfy $k \in S^{(W)}_{(J_j,i_j)_{j=1}^n}$. However, by Equation (14), such $(i_j)_{j=1}^n$ uniquely exists. Thus, Alice can correctly guess kings' outcomes.

A description of the QKD protocol by using the mean multi-kings' problem is as follows.

1. Alice prepares a composite system ($n+1$ qubits) $\tilde{\mathcal{H}} = \mathcal{H}_A \otimes \mathcal{H}_{K_1} \otimes \mathcal{H}_{K_2} \otimes \cdots \otimes \mathcal{H}_{K_n} \simeq (\mathbb{C}^2)^{\otimes n+1}$ in the initial state $|\Phi^{(W)}\rangle$ ($W \in \{Z, X\}$) with probability $\frac{1}{2}$. Then, she sends the qubit $\mathcal{H}_{K_j}$ to King$_j$ ($j = 1, 2, \ldots, n$).
2. Each King$_j$ performs the measurement $M^{(J_j)} = (M_0^{(J_j)}, M_1^{(J_j)})$ ($J_j \in \{0, 1\}$) with probability $\frac{1}{2}$ on $\mathcal{H}_{K_j}$ and obtains an outcome $i_j \in \{0, 1\}$. After the measurement, each King$_j$ returns $\mathcal{H}_{K_j}$ to Alice.
3. Alice performs the measurement $P^{(W)} = (P_k^{(W)})_{k\in\mathcal{K}}$ ($W \in \{Z, X\}$) on $\tilde{\mathcal{H}}$ when the initial state was $|\Phi^{(W)}\rangle$. Then, she obtains an outcome $k \in \mathcal{K}$.
4. After the measurement, each King$_j$ announces post-information J_j to Alice.
5. Alice obtains a sequence $s(k, (J_j)_{j=1}^n, \Phi^{(W)})$ from the outcome k, the post-information $(J_j)_{j=1}^n$, and the initial state $|\Phi^{(W)}\rangle$.
6. They repeat the above process. After that, Alice randomly chooses sequences $(i_j'^1)_{j=1}^n, (i_j'^2)_{j=1}^n, \ldots, (i_j'^r)_{j=1}^n$ from all sequences. Similarly, kings work together to choose sequences $(i_j^1)_{j=1}^n, (i_j^2)_{j=1}^n, \ldots, (i_j^r)_{j=1}^n$ which are the same positions as the positions Alice chose. Then, Alice and kings work together to calculate error rate $\frac{\sum_{u=1}^r (1-\delta_{(i_j'^u)_{j=1}^n (i_j^u)_{j=1}^n})}{r}$.

The rest of the process is the same as for ordinary QKD protocols, such as BB84 protocol. If the error rate is too large, the protocol is aborted. Otherwise, the leftover sequences are performed with error-correction and privacy amplification [20].

Remark that Alice and each King$_j$ can share the secret key when they employ the QKD protocol using the mean-king's problem or BB84 protocol. In the case of employing the QKD using the mean-king's problem (see left hand side of Figure 2), Alice prepares 2 qubits in the Bell state and performs a single measurement on the 2 qubits for each King$_j$. Therefore, she needs to prepare $2n$ qubits and perform n measurements to share the secret key with n kings. On the other hand, in the QKD protocol using the mean multi-kings' problem, Alice only prepares $n+1$ qubits in $|\Phi^{(Z)}\rangle$ or $|\Phi^{(X)}\rangle$ and performs the single measurement $P^{(Z)}$ or $P^{(X)}$. In the case where the BB84 protocol is employed (see right hand side of Figure 2), Alice just prepares n qubits in one of the states $|0\rangle, |1\rangle, |\bar{0}\rangle, |\bar{1}\rangle$ and no performing the measurement is required. Then, Alice and King$_j$ discard the raw key where their bases do not match before calculating error rate. On the other hand, in the QKD protocol using the mean multi-kings' problem, there is not such discarding step before calculating error rate.

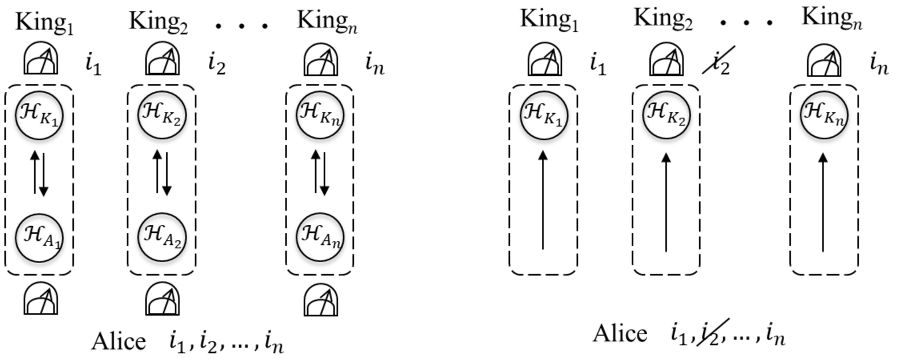

Figure 2. The QKD protocols using the mean-king's problem (**left hand side**) and BB84 protocols (**right hand side**) for Alice and the kings to share the secret key.

3. Protocol: n = 2

We describe the working of the protocol in the case of $n = 2$ by focusing on the case of $W = Z$ to reduce cumbersome notations.

By Equation (2), the index set takes the following form,

$$\mathcal{K} = \{(s_1, t_1, s_2, t_2) \mid s_j, t_j \in \{0,1\}\}. \tag{17}$$

And by Equation (3), the operator $E_k^{(Z)}$ for $k \in \mathcal{K}$ takes the following form,

$$E_k^{(Z)} = E_{(s_1,t_1,s_2,t_2)}^{(Z)} = X_{s_1} Z_{t_1} \otimes X_{s_2} Z_{t_2} \ \ (k = (s_1, t_1, s_2, t_2) \in \mathcal{K}). \tag{18}$$

Similarly, we can observe the operators for $W = X$. By Equation (5), we observe the index sets $S_{(J_1,i_1,J_2,i_2)}^{(W)}$ for $J_1 = 0, J_2 = 0, i_1, i_2 \in \{0,1\}$, and $W = Z$:

$$\begin{aligned}
S_{(0,0,0,0)}^{(Z)} &= S_{(0,0)}^{(Z)} \times S_{(0,0)}^{(Z)} \\
&= \{((0,0),(0,0)),((0,0),(1,0)),((1,0),(0,0)),((1,0),(1,0))\} \\
&= \{(0,0,0,0),(0,0,1,0),(1,0,0,0),(1,0,1,0)\} && (19)\\
S_{(0,0,0,1)}^{(Z)} &= S_{(0,0)}^{(Z)} \times S_{(0,1)}^{(Z)} \\
&= \{((0,0),(0,1)),((0,0),(1,1)),((1,0),(0,1)),((1,0),(1,1))\} \\
&= \{(0,0,0,1),(0,0,1,1),(1,0,0,1),(1,0,1,1)\} && (20)\\
S_{(0,1,0,0)}^{(Z)} &= S_{(0,1)}^{(Z)} \times S_{(0,0)}^{(Z)} \\
&= \{((0,1),(0,0)),((0,1),(1,0)),((1,1),(0,0)),((1,1),(1,0))\} \\
&= \{(0,1,0,0),(0,1,1,0),(1,1,0,0),(1,1,1,0)\} && (21)\\
S_{(0,1,0,1)}^{(Z)} &= S_{(0,1)}^{(Z)} \times S_{(0,1)}^{(Z)} \\
&= \{((0,1),(0,1)),((0,1),(1,1)),((1,1),(0,1)),((1,1),(1,1))\} \\
&= \{(0,1,0,1),(0,1,1,0),(1,1,0,1),(1,1,1,1)\}, && (22)
\end{aligned}$$

where we regard $((l_1, l_2),(l_3, l_4))$ in the same light as (l_1, l_2, l_3, l_4). Similarly, we can observe the index sets for other J_1, J_2, i_1, i_2, and W.

Let us consider that Alice prepares the qubits $\tilde{\mathcal{H}} = \mathcal{H}_A \otimes \mathcal{H}_{K_1} \otimes \mathcal{H}_{K_2}$ in the initial state

$$|\Phi^{(Z)}\rangle = \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle). \tag{23}$$

Let us consider that King$_1$ and King$_2$ choose the same measurement $M^{(0)}$ and obtain the same outcome 0, i.e., $J_1 = 0, J_2 = 0$ and $i_1 = 0, i_2 = 0$. After kings' measurement, Alice performs the measurement $P^{(Z)} = (P_k^{(Z)})_{k \in \mathcal{K}}$ on $\tilde{\mathcal{H}}$, where

$$\begin{aligned}
P_k^{(Z)} &= 8|(\mathbb{I} \otimes E_k^{(Z)})\Phi^{(Z)}\rangle\langle(\mathbb{I} \otimes E_k^{(Z)})\Phi^{(Z)}|r \\
&= 8|(\mathbb{I} \otimes X_{s_1} Z_{t_1} \otimes X_{s_2} Z_{t_2})\Phi^{(Z)}\rangle\langle(\mathbb{I} \otimes X_{s_1} Z_{t_1} \otimes X_{s_2} Z_{t_2})\Phi^{(Z)}|.
\end{aligned} \tag{24}$$

After the measurement, King$_1$ and King$_2$ announce the post-information $J_1 = 0$ and $J_2 = 0$ to Alice. When Alice obtains an outcome $k = (0,0,0,0)$, she is assured that kings' outcome (i_1, i_2) is $(0,0)$, because (i_1, i_2) satisfying $k = (0,0,0,0) \in S_{(J_1,i_1,J_2,i_2)}^{(W)} = S_{(0,i_1,0,i_2)}^{(Z)}$ is $(0,0)$. In Table 1, we summarize Alice's guessing rule by using her outcome and the post-information from the kings.

Table 1. The relationship among kings' measurements J_1, J_2, Alice's outcome k, and kings' outcomes i_1, i_2 when she chooses $|\Phi^{(W)}\rangle$. In this table, NA means that probability of obtaining the corresponding outcome k is zero unless Eve performs an attack because the corresponding matrix $P_k^{(W)}$ is a zero matrix. An example of Alice's guessing: Alice is assured that kings' outcome (i_1, i_2) is $(0,0)$ when $W = Z, J_1 = 0, J_2 = 0$, and $k = (0,0,0,0)$.

$W = Z, J_1 = 0, J_2 = 0$ $W = X, J_1 = 1, J_2 = 1$		$W = Z, J_1 = 0, J_2 = 1$ $W = X, J_1 = 1, J_2 = 0$		$W = Z, J_1 = 1, J_2 = 0$ $W = X, J_1 = 0, J_2 = 1$		$W = Z, J_1 = 1, J_2 = 1$ $W = X, J_1 = 0, J_2 = 0$	
k	(i_1, i_2)	k	(i_1, i_2)	k	(i_1, i_2)	k	(i_1, i_2)
$(0,0,0,0)$	$(0,0)$	$(0,0,0,0)$	$(0,0)$	$(0,0,0,0)$	$(0,0)$	$(0,0,0,0)$	$(0,0)$
$(0,0,0,1)$ NA	——	$(0,0,0,1)$ NA	——	$(0,0,0,1)$ NA	——	$(0,0,0,1)$ NA	——
$(0,0,1,0)$	$(0,0)$	$(0,0,1,0)$	$(0,1)$	$(0,0,1,0)$	$(0,0)$	$(0,0,1,0)$	$(0,1)$
$(0,0,1,1)$ NA	——	$(0,0,1,1)$ NA	——	$(0,0,1,1)$ NA	——	$(0,0,1,1)$ NA	——
$(0,1,0,0)$ NA	——	$(0,1,0,0)$ NA	——	$(0,1,0,0)$ NA	——	$(0,1,0,0)$ NA	——
$(0,1,0,1)$	$(1,1)$	$(0,1,0,1)$	$(1,0)$	$(0,1,0,1)$	$(0,1)$	$(0,1,0,1)$	$(0,0)$
$(0,1,1,0)$ NA	——	$(0,1,1,0)$ NA	——	$(0,1,1,0)$ NA	——	$(0,1,1,0)$ NA	——
$(0,1,1,1)$	$(1,1)$	$(0,1,1,1)$	$(1,1)$	$(0,1,1,1)$	$(0,1)$	$(0,1,1,1)$	$(0,1)$
$(1,0,0,0)$	$(0,0)$	$(1,0,0,0)$	$(0,0)$	$(1,0,0,0)$	$(1,0)$	$(1,0,0,0)$	$(1,0)$
$(1,0,0,1)$ NA	——	$(1,0,0,1)$ NA	——	$(1,0,0,1)$ NA	——	$(1,0,0,1)$ NA	——
$(1,0,1,0)$	$(0,0)$	$(1,0,1,0)$	$(0,1)$	$(1,0,1,0)$	$(1,0)$	$(1,0,1,0)$	$(1,1)$
$(1,0,1,1)$ NA	——	$(1,0,1,1)$ NA	——	$(1,0,1,1)$ NA	——	$(1,0,1,1)$ NA	——
$(1,1,0,0)$ NA	——	$(1,1,0,0)$ NA	——	$(1,1,0,0)$ NA	——	$(1,1,0,0)$ NA	——
$(1,1,0,1)$	$(1,1)$	$(1,1,0,1)$	$(1,0)$	$(1,1,0,1)$	$(1,1)$	$(1,1,0,1)$	$(1,0)$
$(1,1,1,0)$ NA	——	$(1,1,1,0)$ NA	——	$(1,1,1,0)$ NA	——	$(1,1,1,0)$ NA	——
$(1,1,1,1)$	$(1,1)$	$(1,1,1,1)$	$(1,1)$	$(1,1,1,1)$	$(1,1)$	$(1,1,1,1)$	$(1,1)$

In the case of $n = 2$, the following simple attack so called intercept-resend attack can be considered. An eavesdropper (called Eve) intercepts $\mathcal{H}_{K_j}$ returned to Alice from King$_j$ (step 2 in the protocol) and performs the measurement $M^{(0)}$ or $M^{(1)}$ probabilistically on $\mathcal{H}_{K_j}$. After the measurement, she resends $\mathcal{H}_{K_j}$ to Alice. When Eve performs the intercept-resend attack to only $\mathcal{H}_{K_1}$, the probability which the error occurs is $\frac{1}{8}$, where the error means the event: $\delta_{(i'^u_j)^2_{j=1}(i^u_j)^2_{j=1}} = 0$. When Eve performs the intercept-resend attack to both $\mathcal{H}_{K_1}$ and $\mathcal{H}_{K_2}$, the probability which the error occurs is $\frac{1}{32}(p_1 + p_2 - 2p_1p_2 + 7)$, where p_j denotes the probability, which Eve performs the measurement $M^{(0)}$ on $\mathcal{H}_{K_j}$ $(j \in \{1,2\})$. The minimum value of the probability is 0.21875 when $(p_1 = 1, p_2 = 1)$ or $(p_1 = 0, p_2 = 0)$ and the maximum value of the probability is 0.25 when $(p_1 = 1, p_2 = 0)$ or $(p_1 = 0, p_2 = 1)$.

4. Distinguishability vs. Disturbance

In this section, let us consider two types of the attacks and let us see whether Eve can extract information by employing the attacks without disturbing contained in legitimate users' information in the case of $n = 2$. First, Eve tries to gain information from the qubit returned to Alice by King$_1$ (step 2 in the protocol) by interacting the qubit $\mathcal{H}_{K_1}$ with her quantum system $\mathcal{H}_E$ (see Figure 3). Second, she tries to gain information from the qubits $\mathcal{H}_{K_j}$ returned to Alice by King$_j$ (step 2 in the protocol) by interacting $\mathcal{H}_{K_1} \otimes \mathcal{H}_{K_2}$ with her quantum system $\mathcal{H}_E$ (see Figure 4). In both of the attacks, Eve performs any measurement on her quantum system $\mathcal{H}_E$ at any time.

We can consider an attack that Eve interacts her quantum system with the qubits sent to the kings by Alice. However, in this attack, the qubits are not encoded because the kings have not measured the qubits. Especially, in the case of $n = 1$, the setting of the attack can be considered as monogamy of entanglement [21,22]. Moreover, we can also consider an attack that Eve interacts her quantum system with both of the qubits sent to the kings by Alice and the qubits returned to Alice by the kings. However, the setting of the attack is different from one for discussing the information disturbance theorem. In the setting for the theorem, Eve tries to information extract from only the encoded qubits. Therefore, we concentrate on the above two attacks that Eve tries to extract information from the qubits sent to Alice by the kings.

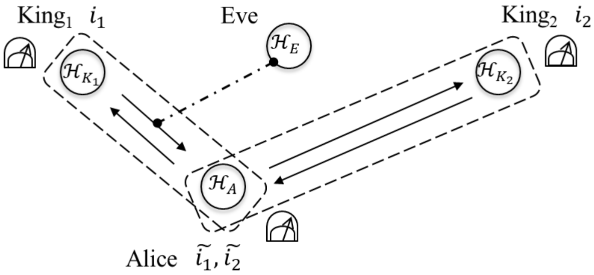

Figure 3. The interaction $\mathcal{H}_{K_1}$ with $\mathcal{H}_E$.

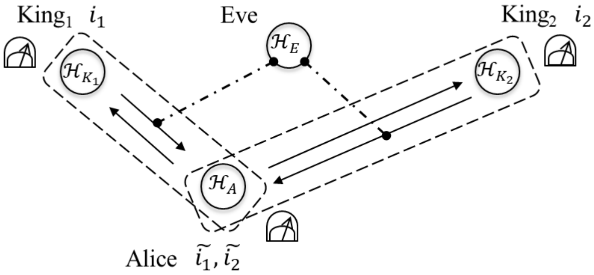

Figure 4. The interaction $\mathcal{H}_{K_1} \otimes \mathcal{H}_{K_2}$ with $\mathcal{H}_E$.

In the beginning, we define error probability which represents probability that Alice cannot guess king's outcomes correctly by using her outcome and the post-information. Remark that the error probability is different from the error rate (step 6 in the protocol). Let $P^{(W)}(k \mid J_1; i_1, J_2; i_2)$ be the probability that Alice obtains an outcome k when she chooses $|\Phi^{(W)}\rangle$ and King$_j$ obtains an outcome i_j with the measurement $M^{(J_j)}$ ($j \in \{1, 2\}$). We define

$$P^{(W)}_{\mathrm{suc}(J_1;i_1,J_2;i_2)} := \sum_{k \in S^{(W)}_{(J_j;i_j)_{j=1}^2}} P^{(W)}(k \mid J_1; i_1, J_2; i_2) \tag{25}$$

and

$$P_{\mathrm{suc}(J_1;i_1,J_2;i_2)} := \frac{1}{2} \sum_{W \in \{X,Z\}} P^{(W)}_{\mathrm{suc}(J_1;i_1,J_2;i_2)}. \tag{26}$$

Then, we define the error probability when King$_j$ obtains an outcome i_j with the measurement $M^{(J_j)}$:

$$P_{\mathrm{err}(J_1;i_1,J_2;i_2)} := 1 - P_{\mathrm{suc}(J_1;i_1,J_2;i_2)}. \tag{27}$$

Equation (27) represents probability that Alice's sequence and kings' sequence do not match when King$_j$ obtains an outcome i_j with the measurement $M^{(J_j)}$, i.e., Alice cannot guess kings' outcomes correctly by using her outcome and the post-information.

Let us consider that Eve tries to extract information from $\mathcal{H}_{K_1}$. Eve prepares her own quantum system $\mathcal{H}_E$ in a quantum state Ω. She intercepts $\mathcal{H}_{K_1}$ in the state $\rho^{(K_1)}$ returned to Alice by King$_1$ and interacts it with $\mathcal{H}_E$. Let us denote the interaction by

$$T^*(\rho^{(K_1)}) := U\rho^{(K_1)} \otimes \Omega U^\dagger, \tag{28}$$

where U is a unitary operator on $\mathcal{H}_{K_1} \otimes \mathcal{H}_E$. Moreover, we denote the local state of $\mathcal{H}_E$ (resp. $\mathcal{H}_{K_1}$) by partial trace over the $\mathcal{H}_{K_1}$ (resp. $\mathcal{H}_E$)

$$T^*_E(\rho^{(K_1)}) := \mathrm{tr}_{\mathcal{H}_{K_1}} T^*(\rho^{(K_1)}) \ \left(\text{resp. } T^*_{K_1}(\rho^{(K_1)}) := \mathrm{tr}_{\mathcal{H}_{K_E}} T^*(\rho^{(K_1)})\right). \tag{29}$$

Let us consider that King$_1$ obtains an outcome i with a measurement $M^{(1)}$. Then, the state of $\mathcal{H}_{K_1}$ before the interaction is $\rho^{(K_1)} = |\bar{i}\rangle\langle\bar{i}|$. Eve tries to extract information regarding to the secret key by distinguishing $T_E^*(|\bar{0}\rangle\langle\bar{0}|)$ and $T_E^*(|\bar{1}\rangle\langle\bar{1}|)$.

We employ trace distance as a measure for distinguishability of the states. Trace norm between a state ρ and a state σ is defined as $||\rho - \sigma||_1 := \sup_{||A||=1} |\operatorname{tr}(\rho - \sigma)A|$, where $||\cdot||$ denotes operator norm. Trace distance is defined as follows,

$$D(\rho, \sigma) := \frac{1}{2}||\rho - \sigma||_1. \tag{30}$$

It takes a value from 0 to 1. In addition, $D(\rho, \sigma) = 0$ if and only if $\rho = \sigma$, and $D(\rho, \sigma) = 0$ if and only if $\operatorname{tr}(\rho\sigma) = 0$. Let us remind the definition of fidelity [23,24]. Fidelity between ρ and σ is defined as $F(\rho, \sigma) := \operatorname{tr}\sqrt{\rho^{1/2}\sigma\rho^{1/2}}$. The following alternative expression of fidelity [25,26] has been shown,

$$F(\rho, \sigma) = \inf_{(M_a)_a:\text{POVM}} \sum_a \sqrt{p(a \mid \rho)p(a \mid \sigma)}, \tag{31}$$

where $p(a \mid \rho)$ and $p(a \mid \sigma)$ are defined as $p(a \mid \rho) := \operatorname{tr}(M_a\rho)$ and $p(a \mid \sigma) := \operatorname{tr}(M_a\sigma)$.

Lemma 1. *The following relation between trace distance and fidelity holds,*

$$\frac{1}{2}||T_E^*(|\bar{0}\rangle\langle\bar{0}|) - T_E^*(|\bar{1}\rangle\langle\bar{1}|)||_1 \leq F(T_{K_1}^*(|0\rangle\langle 0|), T_{K_1}^*(|1\rangle\langle 1|)). \tag{32}$$

Proof of Lemma 1. From Lemma 3 in [27], we have

$$|\langle 0|T(\mathbb{I} \otimes A)|1\rangle| \leq ||A||F(T_{K_1}^*(|0\rangle\langle 0|), T_{K_1}^*(|1\rangle\langle 1|)) \tag{33}$$

for any operator A on $\mathcal{H}_E$, where T is defined as $\operatorname{tr} T^*(\rho)X = \operatorname{tr}\rho T(X)$. By using Equation (33), we observe

$$\begin{aligned} \left|\operatorname{tr}\left[\left\{T_E^*(|\bar{0}\rangle\langle\bar{0}| - T_E^*\left(\tfrac{1}{2}\mathbb{I}\right)\right\}A\right]\right| &= \left|\operatorname{tr}\left\{\left(|\bar{0}\rangle\langle\bar{0}| - \tfrac{1}{2}\mathbb{I}\right)T(\mathbb{I}\otimes A)\right\}\right| \\ &= \left|\operatorname{tr}\left\{\tfrac{1}{2}(|0\rangle\langle 1| + |1\rangle\langle 0|)T(\mathbb{I}\otimes A)\right\}\right| \\ &\leq \tfrac{1}{2}\{|\langle 1|T(\mathbb{I}\otimes A)|0\rangle| + |\langle 0|T(\mathbb{I}\otimes A)|1\rangle|\} \\ &\leq ||A||F(T_{K_1}^*(|0\rangle\langle 0|), T_{K_1}^*(|1\rangle\langle 1|)). \end{aligned} \tag{34}$$

Then,

$$\begin{aligned} \tfrac{1}{2}||T_E^*(|\bar{0}\rangle\langle\bar{0}|) - T_E^*(|\bar{1}\rangle\langle\bar{1}|)||_1 &= \left|\left|T_E^*(|\bar{0}\rangle\langle\bar{0}|) - T_E^*\left(\tfrac{1}{2}\mathbb{I}\right)\right|\right|_1 \\ &= \sup_{||A||=1}\left|\operatorname{tr}\left[\left\{(T_E^*(|\bar{0}\rangle\langle\bar{0}|) - T_E^*\left(\tfrac{1}{2}\mathbb{I}\right)\right\}A\right]\right| \\ &\leq F(T_{K_1}^*(|0\rangle\langle 0|), T_{K_1}^*(|1\rangle\langle 1|)) \end{aligned} \tag{35}$$

holds. □

Theorem 1. *The following trade-off inequality holds,*

$$D(T_E^*(|\bar{0}\rangle\langle\bar{0}|), T_E^*(|\bar{1}\rangle\langle\bar{1}|)) \quad \leq \quad \sqrt{2P_{\text{err}(0;0,0;0)}} + \sqrt{2P_{\text{err}(0;1,0;1)}}. \tag{36}$$

The left hand side of the inequality represents distinguishability for Eve, and the right hand side is the sum of the error probabilities which represent probability that Alice's sequence and kings' sequence are not equal when the kings obtain the corresponding outcomes with the corresponding measurements, i.e., Alice cannot guess kings' sequence correctly by using her outcome and the post-information. This theorem shows that Eve's extracting information regarding King$_1$'s key related with the measurement $M^{(1)}$ inevitably induces disturbing the states and increases the error probability when both of kings choose the measurement $M^{(0)}$. This implies that the more Eve extracts information, the more possibility for Alice and the kings to detect the existence of the attack increases. In particular, Eve cannot extract information about the key at all (i.e., trace distance is zero) when the corresponding error probabilities are zero. Remark that similar inequalities between distinguishability of other pairs of states and the error probabilities can be proven in the similar way as below.

Proof of Theorem 1. Before obtaining the inequalities, let us observe the error probability. Define $\rho_i := T^*_{K_1}(|i\rangle\langle i|)$. By direct calculations (see Appendix A for details), we have the following probability,

$$P_{\mathrm{err}(0;i,0;i)} = \frac{1}{2}(1 - \langle i|\rho_i i\rangle). \tag{37}$$

By using Equations (31) and (37), we have

$$\begin{array}{rcl} F(\rho_0, \rho_1) & = & \inf_{(M_a)_a:\mathrm{POVM}} \sum_a \sqrt{\mathrm{tr}(M_a\rho_0)\,\mathrm{tr}(M_a\rho_1)} \\ & \leq & \sqrt{\mathrm{tr}(|0\rangle\langle 0|\rho_0)\,\mathrm{tr}(|0\rangle\langle 0|\rho_1)} + \sqrt{\mathrm{tr}(|1\rangle\langle 1|\rho_0)\,\mathrm{tr}(|1\rangle\langle 1|\rho_1)} \\ & = & \sqrt{\langle 0|\rho_0 0\rangle(1 - \langle 1|\rho_1 1\rangle)} + \sqrt{(1 - \langle 0|\rho_0 0\rangle)\langle 1|\rho_1 1\rangle} \\ & \leq & \sqrt{1 - \langle 1|\rho_1 1\rangle} + \sqrt{1 - \langle 0|\rho_0 0\rangle} \\ & = & \sqrt{2P_{\mathrm{err}(0;0,0;0)}} + \sqrt{2P_{\mathrm{err}(0;1,0;1)}}, \end{array} \tag{38}$$

where we employ $(|0\rangle\langle 0|, |1\rangle\langle 1|)$ as a POVM in the first inequality. Then, we have the trade-off inequality by the definition of trace distance, Equations (32) and (38). □

Let us consider that Eve tries to extract information from $\mathcal{H}_{K_1}$ and $\mathcal{H}_{K_2}$. Eve prepares a quantum systems $\mathcal{H}_E$ in a quantum state Ω. She intercepts $\mathcal{H}_{K_1} \otimes \mathcal{H}_{K_2}$ in the state $\rho^{(K_1,K_2)}$ returned to Alice by King$_1$ and King$_2$. Then, she interacts both systems with $\mathcal{H}_E$. Let us denote the interaction by

$$K^*(\rho^{(K_1,K_2)}) := V\rho^{(K_1,K_2)} \otimes \Omega V^\dagger, \tag{39}$$

where V is a unitary operator on $\mathcal{H}_{K_1} \otimes \mathcal{H}_{K_2} \otimes \mathcal{H}_E$. And we denote the local state of $\mathcal{H}_E$ (resp. $\mathcal{H}_{K_1} \otimes \mathcal{H}_{K_2}$) by partial trace over the $\mathcal{H}_{K_1} \otimes \mathcal{H}_{K_2}$ (resp. $\mathcal{H}_E$)

$$K^*_E(\rho^{(K_1,K_2)}) := \mathrm{tr}_{\mathcal{H}_{K_1}\otimes\mathcal{H}_{K_2}} K^*(\rho^{(K_1,K_2)}) \ \left(\text{resp. } K^*_{K_1,K_2}(\rho^{(K_1K_2)}) := \mathrm{tr}_{\mathcal{H}_{K_E}} K^*(\rho^{(K_1,K_2)})\right). \tag{40}$$

Let us consider that King$_1$ and King$_2$ perform the same measurement $M^{(1)}$ and obtain the same outcome i. Then, the state of $\mathcal{H}_{K_1} \otimes \mathcal{H}_{K_2}$ before the interaction is $|\bar{i}\bar{i}\rangle\langle\bar{i}\bar{i}|$. Eve tries to extract information regarding to the secret key by distinguishing $K^*_E(|\bar{0}\bar{0}\rangle\langle\bar{0}\bar{0}|)$ and $K^*_E(|\bar{1}\bar{1}\rangle\langle\bar{1}\bar{1}|)$.

Lemma 2. *The following relation between trace distance and fidelity holds,*

$$\begin{array}{rcl} ||K^*_E(|\bar{0}\bar{0}\rangle\langle\bar{0}\bar{0}|) - K^*_E(|\bar{1}\bar{1}\rangle\langle\bar{1}\bar{1}|)||_1 & \leq & \sum_{i\in\{0,1\}} F(K^*_{K_1K_2}(|ii\rangle\langle ii|), K^*_{K_1K_2}(|01\rangle\langle 01|) \\ & & + \sum_{i\in\{0,1\}} F(K^*_{K_1K_2}(|ii\rangle\langle ii|), K^*_{K_1K_2}(|10\rangle\langle 10|). \end{array} \tag{41}$$

Proof of Lemma 2. From Lemma 3 in [27], we have

$$|\langle i_1 i_2|K(I \otimes A)|i_1' i_2'\rangle| \leq ||A||F(K^*_{K_1K_2}(|i_1 i_2\rangle\langle i_1 i_2|), K^*_{K_1K_2}(|i_1' i_2'\rangle\langle i_1' i_2'|)) \tag{42}$$

for any operator A on $\mathcal{H}_E$, where K is defined as $\operatorname{tr} K^*(\rho)X = \operatorname{tr} \rho K(X)$. By using Equation (42), we observe

$$\begin{aligned}
|\operatorname{tr}[\{K_E^*(|\bar{0}\bar{0}\rangle\langle\bar{0}\bar{0}|) - K_E^*(|\bar{1}\bar{1}\rangle\langle\bar{1}\bar{1}|)\}A]| &= |\operatorname{tr}\{(|\bar{0}\bar{0}\rangle\langle\bar{0}\bar{0}| - |\bar{1}\bar{1}\rangle\langle\bar{1}\bar{1}|)K(\mathbb{I}\otimes A)\}| \\
&= \Big|\operatorname{tr}\Big\{\tfrac{1}{2}(|00\rangle\langle 01| + |00\rangle\langle 10| + |01\rangle\langle 00| + |01\rangle\langle 11| \\
&\quad +|10\rangle\langle 00| + |10\rangle\langle 11| + |11\rangle\langle 01| + |11\rangle\langle 10|)K(\mathbb{I}\otimes A)\Big\}\Big| \\
&\leq \textstyle\sum_{i\in\{0,1\}} |\langle ii|K(I\otimes A)|01\rangle| + \sum_{i\in\{0,1\}} |\langle ii|K(\mathbb{I}\otimes A)|10\rangle| \\
&\leq ||A||\Big\{ \textstyle\sum_{i\in\{0,1\}} F(K_{K_1K_2}^*(|ii\rangle\langle ii|), K_{K_1K_2}^*(|01\rangle\langle 01|) \\
&\quad + \textstyle\sum_{i\in\{0,1\}} F(K_{K_1K_2}^*(|ii\rangle\langle ii|), K_{K_1K_2}^*(|10\rangle\langle 10|)\Big\}.
\end{aligned} \tag{43}$$

In Equation (43), we take supreme over all A such that $||A|| = 1$, then we have Equation (41). □

Theorem 2. *The following trade-off inequality holds,*

$$D(K_E^*(|\bar{0}\bar{0}\rangle\langle\bar{0}\bar{0}|), K_E^*(|\bar{1}\bar{1}\rangle\langle\bar{1}\bar{1}|)) < \sum_{i_1,i_2\in\{0,1\}} \sqrt{2P_{\mathrm{err}(0;i_1,0;i_2)}}. \tag{44}$$

Although Eve tries to distinguish the states on $\mathcal{H}_{K_1} \otimes \mathcal{H}_{K_2}$, this theorem gives the same claim as the one of Theorem 1. This theorem shows that Eve's extracting information regarding kings' keys related with the measurement $M^{(1)}$ inevitably induces disturbing the states and increases the error probability when both of kings choose the measurement $M^{(0)}$. Remark that similar inequalities between distinguishability of other pairs of states and the error probabilities can be proven in the similar way as below.

Proof of Theorem 2. In the same manner, let us observe the error probability. Define $\rho_{i_1i_2} := K_{K_1K_2}^*(|i_1i_2\rangle\langle i_1i_2|)$. By direct calculations (see Appendix B for details), we have the following probability,

$$P_{\mathrm{err}(0;i_1,0;i_2)} = \begin{cases} \frac{1}{2}(1 - \langle i_1i_2|\rho_{i_1i_2}|i_1i_2\rangle) & (i_1 = i_2) \\ 1 - \frac{1}{2}\langle i_1i_2|\rho_{i_1i_2}|i_1i_2\rangle & (i_1 \neq i_2). \end{cases} \tag{45}$$

By using Equations (31) and (45), we have

$$\begin{aligned}
F(\rho_{00}, \rho_{01}) &= \inf_{(M_a)_a:\mathrm{POVM}} \textstyle\sum_a \sqrt{\operatorname{tr}(M_a\rho_{00}) \operatorname{tr}(M_a\rho_{01})} \\
&\leq \sqrt{\operatorname{tr}\{(|11\rangle\langle 11| + |01\rangle\langle 01|)\rho_{00}\} \operatorname{tr}\{(|00\rangle\langle 00| + |01\rangle\langle 01|)\rho_{01}\}} \\
&\quad + \sqrt{\operatorname{tr}\{(|00\rangle\langle 00| + |10\rangle\langle 10|)\rho_{00}\} \operatorname{tr}\{(|00\rangle\langle 00| + |10\rangle\langle 10|)\rho_{01}\}} \\
&< \sqrt{\operatorname{tr}\{(|11\rangle\langle 11| + |01\rangle\langle 01|)\rho_{00}\}} + \sqrt{\operatorname{tr}\{(|00\rangle\langle 00| + |10\rangle\langle 10|)\rho_{01}\}} \\
&= \sqrt{1 - \langle 00|\rho_{00}|00\rangle - \langle 10|\rho_{00}|10\rangle} + \sqrt{1 - \langle 01|\rho_{01}|01\rangle - \langle 11|\rho_{01}|11\rangle} \\
&< \sqrt{1 - \langle 00|\rho_{00}|00\rangle} + \sqrt{2 - \langle 01|\rho_{01}|01\rangle} \\
&= \sqrt{2P_{\mathrm{err}(0;0,0;0)}} + \sqrt{2P_{\mathrm{err}(0;0,0;1)}}.
\end{aligned} \tag{46}$$

where we employ $(|11\rangle\langle 11| + |01\rangle\langle 01|, |00\rangle\langle 00| + |10\rangle\langle 10|)$ as a POVM in the first inequality. In the same manner, we have

$$F(\rho_{ii}, \rho_{01}) < \sqrt{2P_{\mathrm{err}(0;i,0;i)}} + \sqrt{2P_{\mathrm{err}(0;0,0;1)}}, \tag{47}$$

$$F(\rho_{ii}, \rho_{10}) < \sqrt{2P_{\mathrm{err}(0;i,0;i)}} + \sqrt{2P_{\mathrm{err}(0;1,0;0)}} \quad (i \in \{0,1\}). \tag{48}$$

Then, we have the trade-off inequality by the definition of trace distance, Equations (41) and (48). □

5. Summary

In this paper, we discussed the quantum key distribution protocol using the mean multi-kings' problem. By using the protocol, Alice can share the secret key with King$_j$ ($j = 1, 2, \dots, n$). In the case of $n = 2$, we considered whether Eve can extract information when she can performs the interaction between her own quantum system and the qubit returned by King$_j$ and can performs any measurement on her quantum system at any time. We employed trace distance as a measure for distinguishability of the states for Eve. Furthermore, we gave the trade-off inequalities between trace distance of the quantum states corresponding to the secret key for Eve and the error probability which represents probability that the bit sequences shared by the legitimate users do not match. In BB84, such relation is know as the information disturbance theorem and the theorem is also regarded as an information theoretical version of the uncertainty relation. Our inequalities showed that Eve's extracting information regarding kings' keys inevitably induces disturbing the states and increases the error probability even though Alice can use the post-information to guess kings' outcomes. This implies that the information gain by Eve increases possibility for the legitimate users to detect the existence of the attacks. In particular, when the corresponding error probability is zero, Eve cannot extract any information.

Author Contributions: Conceptualization, M.Y.; investigation, A.N. and J.C. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Conflicts of Interest: The authors declare no conflict of interest.

Appendix A

We provide a direct calculation for obtaining the error probabilities in the proof of Theorem 1. Let us consider that the initial state is $|\Phi^{(W)}\rangle$, King$_j$ ($j \in \{1, 2\}$) obtains an outcome i_j with $M^{(J_j)}$, and Eve performs the interaction on $\mathcal{H}_{K_1} \otimes \mathcal{H}_E$. Let $\rho^{(W)}_{(J_1;i_1,J_2;i_2)}$ be a state of the composite system before Alice's measurement. The state takes one of the following forms,

$$\rho^{(Z)}_{(0;i_1,0;i_1)} = |i_1\rangle\langle i_1| \otimes \rho_{i_1} \otimes |i_1\rangle\langle i_1|, \tag{A1}$$

$$\rho^{(Z)}_{(0;i_1,1;i_2)} = |i_1\rangle\langle i_1| \otimes \rho_{i_1} \otimes |\bar{i}_2\rangle\langle \bar{i}_2|, \tag{A2}$$

$$\rho^{(Z)}_{(1;i_1,0;i_2)} = |i_2\rangle\langle i_2| \otimes \rho_{\bar{i}_1} \otimes |i_2\rangle\langle i_2|, \tag{A3}$$

$$\rho^{(Z)}_{(1;i_1,1;i_2)} = |\bar{i}_1\rangle\langle \bar{i}_1| \otimes \rho_{\bar{i}_1} \otimes |\bar{i}_2\rangle\langle \bar{i}_2|, \tag{A4}$$

$$\rho^{(X)}_{(0;i_1,0;i_2)} = |i_1 \oplus i_2\rangle\langle i_1 \oplus i_2| \otimes \rho_{i_1} \otimes |i_2\rangle\langle i_2|, \tag{A5}$$

$$\rho^{(X)}_{(0;i_1,1;i_2)} = |\bar{i}_2\rangle\langle \bar{i}_2| \otimes \rho_{i_1} \otimes |\bar{i}_2\rangle\langle \bar{i}_2|, \tag{A6}$$

$$\rho^{(X)}_{(1;i_1,0;i_2)} = |\bar{i}_1\rangle\langle \bar{i}_1| \otimes \rho_{\bar{i}_1} \otimes |i_2\rangle\langle i_2|, \tag{A7}$$

$$\rho^{(X)}_{(1;i_1,1;i_1)} = |\bar{i}_1\rangle\langle \bar{i}_1| \otimes \rho_{\bar{i}_1} \otimes |\bar{i}_1\rangle\langle \bar{i}_1|, \tag{A8}$$

where $\rho_i := T^*_{K_1}(|i\rangle\langle i|)$, $\rho_{\bar{i}} := T^*_{K_1}(|\bar{i}\rangle\langle \bar{i}|)$, and $\oplus$ denotes exclusive or.

By direct calculation of

$$P^{(W)}_{\mathrm{suc}(J_1;i_1,J_2;i_2)} = \sum_{k \in S^{(W)}_{(J_j,i_j)_{j=1}^2}} \mathrm{tr}\left(P^{(W)}_k \rho^{(W)}_{(J_1;i_1,J_2;i_2)}\right), \tag{A9}$$

we have the following probabilities,

$$P^{(Z)}_{\mathrm{suc}(0;i_1,0;i_1)} = P^{(Z)}_{\mathrm{suc}(0;i_1,1;i_2)} = 1, \tag{A10}$$

$$P^{(Z)}_{\mathrm{suc}(1;i_1,0;i_2)} = P^{(Z)}_{\mathrm{suc}(1;i_1,1;i_2)} = \langle \bar{i}_1 | \rho_{\bar{i}_1} \bar{i}_1 \rangle, \tag{A11}$$

$$P^{(X)}_{\mathrm{suc}(0;i_1,0;i_2)} = P^{(X)}_{\mathrm{suc}(0;i_1,1;i_2)} = \langle i_1 | \rho_{i_1} i_1 \rangle, \tag{A12}$$

$$P^{(X)}_{\mathrm{suc}(1;i_1,0;i_2)} = P^{(X)}_{\mathrm{suc}(1;i_1,1;i_1)} = 1, \tag{A13}$$

where we can find out the index set $S^{(W)}_{(J_j,i_j)_{j=1}^2}$ in Table 1. By the definition of $P_{\mathrm{suc}(J_1;i_1,J_2;i_2)}$, we have the following probabilities,

$$P_{\mathrm{suc}(0;i_1,0;i_2)} = \begin{cases} \frac{1}{2}(\langle i_1 | \rho_{i_1} i_1 \rangle + 1) & (i_1 = i_2) \\ \frac{1}{2}\langle i_1 | \rho_{i_1} i_1 \rangle & (i_1 \neq i_2), \end{cases} \tag{A14}$$

$$P_{\mathrm{suc}(0;i_1,1;i_2)} = \frac{1}{2}\langle i_1 | \rho_{i_1} i_1 \rangle, \tag{A15}$$

$$P_{\mathrm{suc}(1;i_1,0;i_2)} = \frac{1}{2}\langle \bar{i}_1 | \rho_{\bar{i}_1} \bar{i}_1 \rangle, \tag{A16}$$

$$P_{\mathrm{suc}(1;i_1,1;i_2)} = \begin{cases} \frac{1}{2}(\langle \bar{i}_1 | \rho_{\bar{i}_1} \bar{i}_1 \rangle + 1) & (i_1 = i_2) \\ \frac{1}{2}\langle \bar{i}_1 | \rho_{\bar{i}_1} \bar{i}_1 \rangle & (i_1 \neq i_2). \end{cases} \tag{A17}$$

Then, we can observe the error probabilities from these probabilities.

Appendix B

We provide a direct calculation for obtaining the error probabilities in the proof of Theorem 2. Let us consider that the initial state is $|\Phi^{(W)}\rangle$, King$_j$ ($j \in \{1,2\}$) obtains an outcome i_j with $M^{(J_j)}$, and Eve performs the interaction on $\mathcal{H}_{K_1} \otimes \mathcal{H}_{K_2} \otimes \mathcal{H}_{E_j}$. Let $\rho'^{(W)}_{(J_1;i_1,J_2;i_2)}$ be a state of the composite system before Alice's measurement. The state takes one of the following forms,

$$\rho'^{(Z)}_{(0;i_1,0;i_1)} = |i_1\rangle\langle i_1| \otimes \rho_{i_1 i_1}, \tag{A18}$$

$$\rho'^{(Z)}_{(0;i_1,1;i_2)} = |i_1\rangle\langle i_1| \otimes \rho_{i_1 \bar{i}_2}, \tag{A19}$$

$$\rho'^{(Z)}_{(1;i_1,0;i_2)} = |i_2\rangle\langle i_2| \otimes \rho_{\bar{i}_1 i_2}, \tag{A20}$$

$$\rho'^{(Z)}_{(1;i_1,1;i_2)} = |\bar{i}_1\rangle\langle \bar{i}_1| \otimes \rho_{\bar{i}_1 \bar{i}_2}, \tag{A21}$$

$$\rho'^{(X)}_{(0;i_1,0;i_2)} = |i_1 \oplus i_2\rangle\langle i_1 \oplus i_2| \otimes \rho_{i_1 i_2}, \tag{A22}$$

$$\rho'^{(X)}_{(0;i_1,1;i_2)} = |\bar{i}_2\rangle\langle \bar{i}_2| \otimes \rho_{\bar{i}_1 i_2}, \tag{A23}$$

$$\rho'^{(X)}_{(1;i_1,0;i_2)} = |\bar{i}_1\rangle\langle \bar{i}_1| \otimes \rho_{\bar{i}_1 i_2}, \tag{A24}$$

$$\rho'^{(X)}_{(1;i_1,1;i_1)} = |\bar{i}_1\rangle\langle \bar{i}_1| \otimes \rho_{\bar{i}_1 \bar{i}_1}, \tag{A25}$$

where $\rho_{ij} := K^*_{K_1 K_2}(|ij\rangle\langle ij|)$ $(i, j \in \{0, 1, \bar{0}, \bar{1}\})$.

By direct calculation of

$$P^{(W)}_{\mathrm{suc}(J_1;i_1,J_2;i_2)} = \sum_{k \in S^{(W)}_{(J_j,i_j)_{j=1}^2}} \mathrm{tr}\left(P^{(W)}_k \rho'^{(W)}_{(J_1;i_1,J_2;i_2)}\right), \tag{A26}$$

we have the following probabilities,

$$
\begin{aligned}
P^{(Z)}_{\mathrm{suc}(0;i_1,0;i_1)} &= 1, && \text{(A27)}\\
P^{(Z)}_{\mathrm{suc}(0;i_1,1;i_2)} &= \langle \bar{i}_1\bar{i}_2|\rho_{i_1\bar{i}_2}|\bar{i}_1\bar{i}_2\rangle + \langle \overline{i_1\oplus 1}\bar{i}_2|\rho_{i_1\bar{i}_2}|\overline{i_1\oplus 1}\bar{i}_2\rangle, && \text{(A28)}\\
P^{(Z)}_{\mathrm{suc}(1;i_1,0;i_2)} &= \langle \bar{i}_1\bar{i}_2|\rho_{\bar{i}_1 i_2}|\bar{i}_1\bar{i}_2\rangle + \langle \bar{i}_1\overline{i_2\oplus 1}|\rho_{\bar{i}_1 i_2}|\bar{i}_1\overline{i_2\oplus 1}\rangle, && \text{(A29)}\\
P^{(Z)}_{\mathrm{suc}(1;i_1,1;i_2)} &= \langle \bar{i}_1\bar{i}_2|\rho_{\bar{i}_1\bar{i}_2}|\bar{i}_1\bar{i}_2\rangle, && \text{(A30)}\\
P^{(X)}_{\mathrm{suc}(0;i_1,0;i_2)} &= \langle i_1 i_2|\rho_{i_1 i_2}|i_1 i_2\rangle, && \text{(A31)}\\
P^{(X)}_{\mathrm{suc}(0;i_1,1;i_2)} &= \langle i_1 i_2|\rho_{i_1\bar{i}_2}|i_1 i_2\rangle + \langle i_1 i_2\oplus 1|\rho_{i_1\bar{i}_2}|i_1 i_2\oplus 1\rangle, && \text{(A32)}\\
P^{(X)}_{\mathrm{suc}(1;i_1,0;i_2)} &= \langle i_1 i_2|\rho_{\bar{i}_1 i_2}|i_1 i_2\rangle + \langle i_1\oplus 1 i_2|\rho_{\bar{i}_1 i_2}|i_1\oplus 1 i_2\rangle, && \text{(A33)}\\
P^{(X)}_{\mathrm{suc}(1;i_1,1;i_1)} &= 1. && \text{(A34)}
\end{aligned}
$$

By the definition of $P_{\mathrm{suc}(J_1;i_1,J_2;i_2)}$, we have the following probabilities,

$$
\begin{aligned}
P_{\mathrm{suc}(0;i_1,0;i_2)} &= \begin{cases} \frac{1}{2}(\langle i_1 i_2|\rho_{i_1 i_2}|i_1 i_2\rangle + 1) & (i_1 = i_2)\\ \frac{1}{2}\langle i_1 i_2|\rho_{i_1 i_2}|i_1 i_2\rangle & (i_1 \neq i_2), \end{cases} && \text{(A35)}\\
P_{\mathrm{suc}(0;i_1,1;i_2)} &= \frac{1}{2}(\langle \bar{i}_1\bar{i}_2|\rho_{i_1\bar{i}_2}|\bar{i}_1\bar{i}_2\rangle + \langle \overline{i_1\oplus 1}\bar{i}_2|\rho_{i_1\bar{i}_2}|\overline{i_1\oplus 1}\bar{i}_2\rangle\\
&\quad + \langle i_1 i_2|\rho_{i_1\bar{i}_2}|i_1 i_2\rangle + \langle i_1 i_2\oplus 1|\rho_{i_1\bar{i}_2}|i_1 i_2\oplus 1\rangle), && \text{(A36)}\\
P_{\mathrm{suc}(1;i_1,0;i_2)} &= \frac{1}{2}(\langle \bar{i}_1\bar{i}_2|\rho_{\bar{i}_1 i_2}|\bar{i}_1\bar{i}_2\rangle + \langle \bar{i}_1\overline{i_2\oplus 1}|\rho_{\bar{i}_1 i_2}|\bar{i}_1\overline{i_2\oplus 1}\rangle\\
&\quad + \langle i_1 i_2|\rho_{\bar{i}_1 i_2}|i_1 i_2\rangle + \langle i_1\oplus 1 i_2|\rho_{\bar{i}_1 i_2}|i_1\oplus 1 i_2\rangle), && \text{(A37)}\\
P_{\mathrm{suc}(1;i_1,1;i_2)} &= \begin{cases} \frac{1}{2}(\langle \bar{i}_1\bar{i}_2|\rho_{\bar{i}_1\bar{i}_2}|\bar{i}_1\bar{i}_2\rangle + 1) & (i_1 = i_2)\\ \frac{1}{2}\langle \bar{i}_1\bar{i}_2|\rho_{\bar{i}_1\bar{i}_2}|\bar{i}_1\bar{i}_2\rangle & (i_1 \neq i_2). \end{cases} && \text{(A38)}
\end{aligned}
$$

Then, we can observe the error probabilities from those probabilities.

References

1. Chefles, A. Quantum state discrimination. *Contemp. Phys.* **2000**, *41*, 401–424. [CrossRef]
2. Bergou, J.A.; Herzog, U.; Hillery, M. *Quantum State Estimation, 11 Discrimination of Quantum States*; Lecture Notes in Physics; Springer: Berlin/Heidelberg, Germany, 2007; Volume 649.
3. Qiu, D.; Li, L. Relation between minimum-error discrimination and optimum unambiguous discrimination. *Phys. Rev. A* **2010**, *82*, 032333. [CrossRef]
4. Wilde, M. *Quantum Information Theory*; Cambridge University Press: Cambridge, UK, 2017.
5. Vaidman, L.; Aharonov, Y.; Albert, D.Z. How to ascertain the values of σ_x, σ_y, and σ_z of a spin-1/2 particle. *Phys. Rev. Lett.* **1987**, *58*, 1385–1387. [CrossRef] [PubMed]
6. Englert, B.-G.; Aharonov, Y. The mean-kings' problem: prime degrees of freedom. *Phys. Lett. A* **2001**, *284*, 1–5. [CrossRef]
7. Aharonov, Y.; Bergmann, P.G.; Lebowitz, J.L. Time Symmetry in the Quantum Process of Measurement. *Phys. Rev.* **1964**, *134*, B1410. [CrossRef]
8. Bub, J. Secure key distribution via pre- and postselected quantum states. *Phys. Rev. A* **2001**, *63*, 032309 . [CrossRef]
9. Werner, A.H.; Franz, T.; Werner, R.F. Quantum Cryptography as a Retrodiction Problem. *Phys. Rev. Lett.* **2009**, *103*, 220504. [CrossRef] [PubMed]
10. Yoshida, M.; Miyadera, T.; Imai, H. Quantum Key Distribution using Mean King Problem with Modified Measurement Schemes. In Proceedings of the International Symposium on Information Theory and Its Applications 2012, Honolulu, HI, USA, 28–31 October 2012; pp. 317–321.

11. Azuma, H.; Ban, M. The intercept/resend attack and the collective attack on the quantum key distribution protocol based on the pre- and post-selection effect. *arXiv* **2018**, arXiv:quant-ph/1811.07282.
12. Nakayama, A.; Yoshida, M.; Cheng, J. Quantum Key Distribution using Extended Mean King's Problem. In Proceedings of the International Symposium on Information Theory and Its Applications 2018, Singapore, 28–31 October 2018; pp. 339–343.
13. Bennett, C.H.; Brassard, G. Quantum Cryptography: Public Key Distribution And Coin Tossing. In Proceedings of the IEEE International Conference on Computers Systems and Signal Processing, Bangalore, India, 9–12 December 1984; pp. 175–179.
14. Fuchs, C.A.; Jacobs, K. Information-tradeoff relations for finite-strength quantum measurements. *Phys. Rev. A* **2001**, *63*, 062305. [CrossRef]
15. Boykin, P.O.; Roychowdhury, V.P. Information vs. Disturbance in Dimension D. *Quantum Inf. Comput.* **2005**, *5*, 396–412.
16. Miyadera, T.; Imai, H. Information-disturbance theorem for mutually unbiased observables. *Phys. Rev. A* **2006**, *73*, 042317. [CrossRef]
17. Miyadera, T.; Imai, H. Information-Disturbance theorem and Uncertainty Relation. *arXiv* **2007**, arXiv:quant-ph/0707.4559.
18. Busch, P. *No Information Without Disturbance: Quantum Limitations of Measurement*; Springer: Berlin/Heidelberg, Germany, 2009; pp. 229–256.
19. Biham, E.; Boyer, M.; Boykin, P.O.; Mor, T.; Roychowdhury, V. A proof of security of quantum key distribution. In Proceedings of the 32nd Annual ACM Symposium on Theory of Computing, Portland, OR, USA, 21–23 May 2000; pp. 715–724.
20. Bennett, C.H.; Brassard, G.; Crépeau, C.; Maurer, U.M. Generalized Privacy Amplification. *IEEE Trans. Inf. Theory* **1995**, *41*, 1915–1923. [CrossRef]
21. Deutsch, D.; Ekert, A.; Jozsa, R.; Macchiavello, C.; Popescu, S.; Sanpera, A. Quantum Privacy Amplification and the Security of Quantum Cryptography over Noisy Channels. *Phys. Rev. Lett.* **1996**, *77*, 2818–2821. [CrossRef] [PubMed]
22. Lo, H.-K.; Chau, H.F. Unconditional Security of Quantum Key Distribution over Arbitrarily Long Distances. *Science* **1999**, *283*, 2050–2056. [CrossRef] [PubMed]
23. Uhlmann, A. The "transition probability" in the state space of a $*$-algebra. *Rep. Math. Phys.* **1976**, *9*, 273–279. [CrossRef]
24. Jozsa, R. Fidelity for Mixed Quantum States. *J. Mod. Opt.* **1994**, *41*, 2315–2323. [CrossRef]
25. Fuchs, C.A.; Caves, C.M. Mathematical techniques for quantum communication theory. *Open Syst. Inf. Dyn.* **1995**, *3*, 345–356. [CrossRef]
26. Barnum, H.; Caves, C.M.; Fuchs, C.A.; Jozsa, R.; Schumacher, B. Noncommuting Mixed States Cannot Be Broadcast. *Phys. Rev. Lett.* **1996**, *76*, 2818–2821. [CrossRef] [PubMed]
27. Miyadera, T.; Imai, H. State collapse in Information Transfer and its applications. In Proceedings of the 2008 Symposium on Cryptography and Information Security, Miyazaki, Japan, 22–25 January 2008; p. 2D2-4.

Publisher's Note: MDPI stays neutral with regard to jurisdictional claims in published maps and institutional affiliations.