Quantum Inf Process (2015) 14:3523–3531
DOI 10.1007/s11128-015-1054-5

Secure sequential transmission of quantum information

Kabgyun Jeong[1] · **Jaewan Kim**[1]

Received: 29 January 2015 / Accepted: 19 June 2015 / Published online: 30 June 2015

Abstract We propose a quantum communication protocol that can be used to transmit any quantum state, one party to another via several intermediate nodes, securely on quantum communication network. The scheme makes use of the sequentially chained and approximate version of private quantum channels satisfying certain commutation relation of n-qubit Pauli operations. In this paper, we study the sequential structure, security analysis, and efficiency of the quantum sequential transmission protocol in depth.

Keywords Private quantum channel · Sequential transmission · Quantum secret sharing · β-biasedness

1 Introduction

One of the most popular quantum cryptographic primitives, except quantum key distribution, is the quantum secret sharing (QSS) protocols [1,2]. The primitive known as QSS is a process of splitting a piece of quantum information into several parts and then securely reconstructing the information, but certain subparts are not enough to restore the original quantum information. (In a strict sense, the secret sharing is different from the state sharing on its goal [3], but we treat the protocols as in the same category.) There are huge number of theoretical studies on QSS protocols, and also exist experimental demonstrations on QSS schemes in continuous-variable regime, e.g., Refs. [4,5].

✉ Kabgyun Jeong
kgjeong6@kias.re.kr

[1] School of Computational Sciences, Korea Institute for Advanced Study, 85 Hoegiro, Dongdaemun-gu, Seoul 130-722, Korea

Transmission or distribution of quantum information over several authorized nodes is essential for future applications in quantum communications. We here review the original QSS scheme from the point of view of (approximate) private quantum channels (PQC) and then propose an information transmission method, namely ε-secure quantum sequential transmission (QST) protocol. This protocol uses a concept of private quantum channel and aims to secure sequential transmission, where arbitrary quantum states pass through several authorized intermediate nodes (or participants). In the transmission process, all nodes must collaborate to reveal the original quantum information. In the sequentially chained scheme, we exploit the Pauli commutation relations on n-qubit quantum states, and derive the mathematical structure of multi-node ε-randomizing maps.

Using the idea of the general three-party QSS scheme, we construct our main protocol known as QST protocol under the security parameter ε. The parameter ε implies that security and efficiency of the protocols are dealt with an asymptotic consideration. Shortly speaking, the QST protocol can transmit any quantum states from one party to another under the consent of all authorized participants with classical secret bits. Note that any input quantum states into a quantum channel are arbitrary quantum information with a given dimension, and we exclude classical information. Thus, we expect that the protocol, QST, can be applied to certain applications such as quantum repeater [6], quantum key repeater [7], quantum sealed-bid auction [8], or quantum email protocol, since only authorized users can send, confirm, and read the quantum message. Furthermore, with the proposed schemes, we study the key question of finding minimal resources required to split and reconstruct a quantum state, and to transfer arbitrary quantum information sequentially.

Let us briefly review the quantum one-time pad or private quantum channel (PQC). Ambainis et al. [9] first proposed a quantum primitive known as a private quantum channel for secure transmission of quantum states, and already proved its security including the optimality [10,11]. The complete randomization method naturally gave birth to *approximate* approaches for randomizing quantum states [12–14]. We here adopt an approximate version of the Dickinson and Nayak's PQC [14], which has relatively few Pauli operations on multi-qubit encodings. Using conventions and definitions in Sect. 1.1, we construct a quantum communication protocol that is efficient and secure with a small information leakages ($\varepsilon \ll 1$) notwithstanding minimal use of resources. But, in this paper, we mainly focus our attention on constructing the mathematical structure of the ε-secure quantum sequential transmission scheme (QST).

Before finishing the section, we introduce the basic concept of (approximate) PQC or ε-randomizing map (or also known as random unitary channel). Moreover, we comment on security analysis from Holevo bound and the correspondence between (classical) keys and Pauli operations. In Sect. 2, we focus on our main construction of QST protocol, which is one step more advanced form of the well-known three-party QSS, on multi-party system. In Sect. 3, we summarize and conclude our work.

1.1 Background

For a given d-dimensional Hilbert space $\mathbb{C}^d$, $\mathcal{B}(\mathbb{C}^d)$ denotes the space of bounded linear operators on the space $\mathbb{C}^d$, and $U(d) \subset \mathcal{B}(\mathbb{C}^d)$ the unitary group on the space. We make use of a quantum map from $\mathcal{B}(\mathbb{C}^d)$ to itself generally known as a quantum channel. Then, we can define a private quantum channel: For any $\varepsilon \geq 0$, a completely positive and trace preserving (CPTP) map $\mathcal{R} : \mathcal{B}(\mathbb{C}^d) \to \mathcal{B}(\mathbb{C}^d)$ is said to be ε-randomizing with respect to the trace norm if, for all quantum state $\rho \in \mathcal{B}(\mathbb{C}^d)$,

$$\left\| \mathcal{R}(\rho) - \frac{\mathbb{1}_d}{d} \right\|_1 \leq \varepsilon, \tag{1}$$

where $\mathbb{1}_d$ denotes the identity matrix of a given dimension d. The input quantum source ρ is a d-dimensional density matrix. The map $\mathcal{R}$ satisfying Eq. (1) is the approximate private quantum channel (APQC), and $\|M\|_1 := \mathrm{tr}\sqrt{M^\dagger M}$ denotes the trace norm for any matrix M. Note that the mapping $\mathcal{R}$ is perfect (or complete) randomizing map if $\varepsilon = 0$. The definition with the security parameter ε always implies perfect PQC, and gives us the informational security rather than a security based on the computational complexity.

A simple way to create such an invertible encoding map is to choose a certain sequence of unitary operators $U_1, \ldots, U_{s \leq d^2} \in U(d)$ and define the encoding map as

$$\mathcal{R} : \rho \to \frac{1}{s} \sum_{i=1}^{s} U_i \rho U_i^\dagger. \tag{2}$$

The index i corresponds to the number of shared secret bits that all communicating parties share. We here assume that the secret bits are unknown to any eavesdroppers or unauthorized parties. With a suitable choice of s unitary operators not more than d^2, the mapping $\mathcal{R}$ satisfies to be an approximate private quantum channel. In fact, any orthogonal set of d^2 unitary operations form a perfect private quantum channel. Notice that the dimension d of our case is fixed to 2^n to accommodate the Hilbert space of n qubits.

If that is the case, how can we analyze the security of approximate private quantum channels? Roughly speaking, the accessible information to any attackers, for any quantum states $\rho = \sum_i p_i \rho_i$ supported on $\mathbb{C}^d$ and $d\varepsilon < 1$, is bounded above by Holevo information [15]

$$\begin{aligned} \chi\{p_i, \mathcal{R}(\rho_i)\} &= S\left(\sum_{i=1}^{d} p_i \mathcal{R}(\rho_i) \right) - \sum_{i=1}^{d} p_i S(\mathcal{R}(\rho_i)) \\ &\leq \log(1 + d\varepsilon) < d\varepsilon, \end{aligned}$$

where $\{p_i, \mathcal{R}(\rho_i)\}$ represents an ensemble of ρ_i's with probability p_i's through the quantum channel $\mathcal{R}$, and $S(\rho) := -\mathrm{tr}\rho \log \rho$, the von Neumann entropy. The above inequality is true because the definition of the ε-randomizing map with respect to the

trace norm in Eq. (1) implies that the eigenvalues of the channel output are almost uniformly distributed such that $\mathcal{R}(\rho_i) \simeq (1+d\varepsilon)\mathbb{1}_d/d$. This also means that attackers cannot obtain any information about the information of the ensemble $\{p_i, \mathcal{R}(\rho_i)\}$ under the condition $d\varepsilon < 1$.

Finally, a relation between keys and Pauli operators is crucial in the proof of following protocol, so we carefully investigate the key correspondence. An explicit construction for Eq. (2) depends on unitary operators chosen at random from the set of n-qubit Pauli matrices. For two n-bit strings a and b, let $a * b = \sum_{j=1}^{n} a_j b_j \mod 2$ denotes the standard inner product on $\mathbb{Z}_2^n$. We represent a tensor product of n single-qubit Pauli operators by a string of $2n$-bit K, $(a, b) \in \{0,1\}^{2n}$, by using the following correspondence

$$K = (a, b) : \iota^{a*b} X^a Z^b, \tag{3}$$

where $X^a Z^b = X^{a_1} Z^{b_1} \otimes \cdots \otimes X^{a_n} Z^{b_n}$ with $X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ and $Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$, and $\iota = \sqrt{-1}$ the imaginary number. Now, we define a set P_n as

$$\left\{ \iota^{a*b} X^a Z^b : (a, b) \in \{0,1\}^{2n} \right\} \subset U(2^n)$$

for all tensor products of n single-qubit Pauli operators. Then, the set P_n forms a basis for the $2^n \times 2^n$ complex matrices. (Note that the set $P_1 = \{\mathbb{1}_2, X, \iota XZ, Z\}$ is the usual Pauli operators on single qubit.) For convenience we substitute P_n to P_K under the correspondence in Eq. (3) to emphasize a classical key K.

As we mentioned above, n-qubit Pauli operators form a basis for the set of all $2^n \times 2^n$ matrices. So, for a given density matrix ρ, we can construct that

$$\rho = \frac{1}{2^n} \sum_{(a,b)\in\{0,1\}^{2n}} c_{a,b} X^a Z^b, \tag{4}$$

where $c_{a,b}$ is an element of a vector $(c_{a,b})$ in $\mathbb{C}^{2^n}$ with $\|c_{a,b}\|_2^2 \leq 2^n$, and $\|X\|_2 := \sqrt{\mathrm{tr} X^\dagger X}$ is the Frobenius (or Hilbert–Schmidt) norm on the space.

2 Quantum sequential transmission scheme

With additional modification of QSS [1,16,17] and approximate private quantum channels, we now propose a quantum transmission protocol of so-called *ε-secure* QST scheme. The main objective of our task is to send a unknown quantum information from a sender to a receiver when several authorized intermediate nodes exist. Although the quantum information is transmitted sequential ways on concatenated quantum channels, the crucial advantage of this protocol is to preserving its explicit security and efficiency. In the sequential structure, we take the generalized n-qubit Pauli commutation relations on any input quantum signal, and prove the mathematical consistency and security of the chained ε-randomizing maps.

As in three-party QSS protocol, suppose that, for all i-th position, Alice, Bob, and Charlie share a correlation key such that $k_i^A \oplus k_i^B \oplus k_i^C = \alpha_i \mod 2$, where

α_i is fixed to 0 under the mod 2 operation. The main purpose of this protocol is to securely transmit a quantum state from Alice to Charlie through a middle party Bob. The transmitted state between Alice and Charlie is asymptotically secure since the $2n$-bit-key-based PQC makes arbitrary n-qubit state into a *near* maximally mixed state (in three-party scenario). Extending the idea of three-party protocol, we can directly generalize it to an m-party concatenated-transmission protocol within n-qubit Pauli commutation relations.

First, we simply take account of three-party protocol for sequential quantum state transmission. Alice prepares an n-qubit quantum state $|\Phi\rangle \in \mathcal{B}(\mathbb{C}^{2^n})$ and encodes the state to $P_{K^A}|\Phi\rangle$ which will be transmitted to Bob. (Consideration of only pure states is enough since the convexity of trace norm ensures the previous statement.) Bob also encodes the state, by using the correlation key K^B, to $P_{K^B} \circ P_{K^A}|\Phi\rangle$, where $\circ$ denotes a composition of two Pauli sets, and sends the state to the third party Charlie. Remember that $k_i^A \oplus k_i^B \oplus k_i^C = \alpha_i$, so the receiver Charlie efficiently decodes the state to original quantum information

$$P_{K^C} \circ P_{K^B} \circ P_{K^A}|\Phi\rangle = |\Phi\rangle. \tag{5}$$

In Eq. (5), we use the following identity, for any Pauli operators,

$$P_{K^C} \circ P_{K^B} \circ P_{K^A} = P_{K^C \oplus K^B \oplus K^A \mod 2} = P_0 := \mathbb{1}_{2^n}. \tag{6}$$

This condition for (complete) private quantum channel needs exactly $2n$ secret bits. But if we use the approximate case of PQC, then we need about half-size ($\approx n$-bit) keys only instead of $2n$-bit keys [12,14], i.e., for sufficiently large d it satisfies our security level with small ε.

As shown in Fig. 1, m-party extension ($m \geq 3$) of QST scheme is simple and natural, but we need some technical calculations as shown below. We note that every intermediate user also accomplishes the role of sender and receiver. Before describing the m-party scenario, we define a bias of a set of $2n$-bit strings. For a given subset of $E \subset \{0,1\}^{2n}$, if

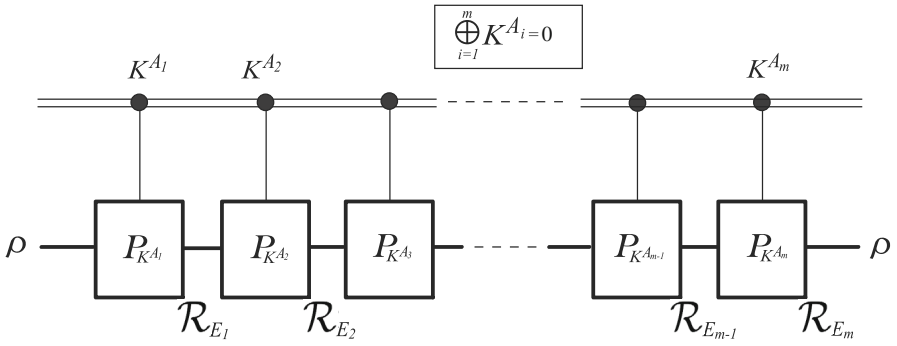

Fig. 1 Approximate m-party quantum sequential transmission protocol: By using a secret classical information K, a sender transmits any quantum state ρ securely to final node through the $m-1$ and ε-randomizing maps $\mathcal{R}_{E_j}$ for all j. *Boxes* with P_K represent the n-qubit Pauli operations corresponding a key K

$$\mathrm{Bias}(E,(a,b)) = \left|\mathbb{E}_{x\in E}(-1)^{x*(a,b)}\right|, \tag{7}$$

then we call the set E is *biased* with respect to a string $(a,b) \in \{0,1\}^{2n}$ [14,18], where $\mathbb{E}$ is an expectation value for some variable in E. Note that $*$ is also the inner product, and the bias is equal to $2\mathbb{E}_E\,[x*(a,b)]-1$ under the modulo 2 operations. When, for all $(a,b)\neq 0^{2n}$, $\mathrm{Bias}(E,(a,b)) \leq \beta$, we call the subset $E\subset\{0,1\}^{2n}$ to be β-biased.

A subset $E\subset\{0,1\}^{2n}$ defines a CPTP map on n-qubit as follows,

$$\begin{aligned}\mathcal{R}_E(\rho) &= \frac{1}{|E|}\sum_{(u,v)\in E} X^u Z^v \rho Z^v X_u \\ &= \frac{1}{2^n|E|}\sum_{(u,v),(a,b)} c_{a,b} X^u Z^v (X^a Z^b) Z^v X^u \\ &= \frac{1}{2^n}\sum_{(a,b)\in\{0,1\}^{2n}} c_{a,b}\beta_{a,b} X^a Z^b, \end{aligned} \tag{8}$$

where a real number $|\beta_{a,b}|$ is equal to the $\mathrm{Bias}(E,(a,b))$ in Eq. (7). The modulus of E, $|E|$, corresponds to some number $s(\leq 2^{2n})$ of n-qubit Pauli operations used in the map $\mathcal{R}_E$. By using commutation relations on Pauli matrices, above equations can be derived from

$$\begin{aligned} X^u Z^v (X^a Z^b) Z^v X^u &= (-1)^{a*v+b*u} X^a Z^b \\ &=: \beta_{a,b} X^a Z^b. \end{aligned} \tag{9}$$

If we choose $E=\{0,1\}^{2n}$, then we have a completely randomizing map. It is known that there *exists* a map $\mathcal{R}_E$ an ε-randomizing map with respect to the trace norm for n-qubit states, when the subset $E\subset\{0,1\}^{2n}$ be a set with bias at most $\varepsilon\cdot 2^{-n/2}$. (See also the proof in Ref. [13].)

From the existence of small β-biased subset E, the Frobenius norm of the randomized state is almost concentrated at the maximally mixed state, that is,

$$\|\mathcal{R}_E(\rho)\|_2^2 \leq \frac{1+\varepsilon^2}{2^n}. \tag{10}$$

This inequality can be directly calculated from the Eq. (8) of $\varepsilon\cdot 2^{-n/2}$-biasedness and the bound $\|c_{a,b}\|_2^2 \leq 2^n$.

Moreover, for any density matrix $N\in\mathcal{B}(\mathbb{C}^{2^n})$, the inequalities $\|N\|_1 \leq \sqrt{2^n}\cdot\|N\|_2$ and $\left\|N-\frac{\mathbb{1}_{2^n}}{2^n}\right\|_1^2 \leq 2^n\cdot\|N\|_2^2 - 1$ always hold. (See proof details in the appendix A of Ref. [14].) Thus, we obtain the following chain bounds

$$\left\|\mathcal{R}_E(\rho)-\frac{\mathbb{1}_{2^n}}{2^n}\right\|_1 \leq \sqrt{2^n\|\mathcal{R}_E(\rho)\|_2^2-1} \leq \varepsilon. \tag{11}$$

Thus, if we can choose a suitable subset E with β-biasedness, then we can always create ε-randomizing map or APQC in trace norm. The above equation, Eq. (11), is intrinsically identical to the Eq. (1); therefore, the security is well preserved.

Finally, we show that multi-party approximate private quantum channel and multi-party QST protocol are secure and efficient, i.e., we claim that $n_{DN} := n + 2\log\frac{1}{\varepsilon} + 4$ classical keys are sufficient for the m-party QST scheme. By choosing a dense subset E, we can initialize a subset $E_j \subset \{0,1\}^{2n}$ to be a set with bias at most $\varepsilon^{1/m} \cdot 2^{-n/2m}$ for each j [19]. Then, we assert that there exists an m-party ε-randomizing map with respect to the trace norm for n-qubit states: For any density matrix $\rho \in \mathcal{B}(\mathbb{C}^{2^n})$, we have

$$\left\| \mathcal{R}_{E_m} \circ \mathcal{R}_{E_{m-1}} \circ \cdots \circ \mathcal{R}_{E_1}(\rho) - \frac{\mathbb{1}_{2^n}}{2^n} \right\|_1 \leq \varepsilon. \tag{12}$$

We here denote that $\mathcal{R}_T = \mathcal{R}_{E_m} \circ \cdots \circ \mathcal{R}_{E_1}$ for convenience. Since the m-user encoding and transmitting for a quantum state under m-APQC form an m-party QST protocol, and it can be directly derived from the following commutation relation

$$X^{u_m} Z^{v_m} \cdots (X^{u_1} Z^{v_1} (X^a Z^b) Z^{v_1} X^{u_1}) \cdots Z^{v_m} X^{u_m} = (-1)^{\sum_{j=1}^m a * v_j + b * u_j} X^a Z^b. \tag{13}$$

This equation is just a generalization of Eq. (9). Suppose that, for every quantum state $\rho \in \mathcal{B}(\mathbb{C}^{2^n})$, each ε-randomizing map between two nodes $(j, j+1)$ satisfies

$$\left\| \mathcal{R}_j(\rho) - \frac{\mathbb{1}_{2^n}}{2^n} \right\|_1 \leq \varepsilon^{\frac{1}{m}}; \tag{14}$$

then, we can always construct multi-user QST protocol via approximate private quantum channels with

$$\left\| \mathcal{R}_T(\rho) - \frac{\mathbb{1}_{2^n}}{2^n} \right\|_1 \leq \varepsilon, \tag{15}$$

and consume about n bits of secret classical keys satisfying $\bigoplus_{i=1}^m K^{A_i} = 0$. This result implies that QST based on sequential private quantum channels is secure. The estimation of Eq. (15) for every ε promises to use the classical key of $n + 2\log\frac{1}{\varepsilon} + 4$ bits [14]. Notice that Dickinson and Nayak's efficient construction for the approximate PQC on n-qubit situation relies on McDiarmid's inequality in probability analysis and a net argument on discretizing pure quantum states. Strict security analysis for the approximate private quantum channel in security parameter ε is reported at Ref. [11], and see also Ref. [20].

3 Conclusion

In summary, we constructed a quantum communication protocol for quantum sequential and ε-secure transmission scheme via the extension of three-party QSS task. This scheme makes use of a relatively small (correlated) classical secret information of about $n_{DN} \simeq n$ bits, just half of the size or the perfect private quantum channel of $2n$-bit, and transmit any n-qubit states securely, so we say that the protocol is efficient.

The security argument only depends on the small security parameter ε in which an approximate private quantum channel guarantee its security. In fact, it is a small value ($\varepsilon < 1$) for sufficiently large d dimension of Hilbert space $\mathbb{C}^d$.

Beyond the mathematical construction of the quantum sequential transmission scheme, we need to exploit this type of communication protocols for potential future applications such as quantum (key) repeater, auction, and email scheme. So, the analysis of these protocols in quantum regime is significant and necessary. We finally point out that the security of the QST protocol must be systematically analyzed for several cases of attackers, and further study is needed for mathematical generalization in p-norm cases (for all $p > 1$). We hope that the quantum sequential transmission, QST, can be used for the realization of practical quantum communication networks.

Acknowledgments This work was supported by Korea Institute for Advanced Study grant funded by the Korea government (MSIP) and partly supported by the IT R&D program of MOTIE/KEIT [10043464].

References

1. Hillery, M., Bužek, V., Berthiaume, A.: Quantum secret sharing. Phys. Rev. A **59**, 1829 (1999)
2. Cleve, R., Gottesman, D., Lo, H.K.: How to share a quantum secret. Phys. Rev. Lett. **83**, 648 (1999)
3. Karlsson, A., Koashi, M., Imoto, N.: Quantum entanglement for secret sharing and secret splitting. Phys. Rev. A **59**, 162 (1999)
4. Tittel, W., Zbinden, H., Gisin, N.: Experimental demonstration of quantum secret sharing. Phys. Rev. A **63**, 042301 (2001)
5. Lance, A.M., Symul, T., Bowen, W.P., Sanders, B.C., Lam, P.K.: Tripartite quantum state sharing. Phys. Rev. Lett. **92**, 177903 (2004)
6. Sangouard, N., Simon, C., de Riedmatten, H., Gisin, N.: Quantum repeaters based on atomic ensembles and linear optics. Rev. Mod. Phys. **83**, 33 (2011)
7. Bäuml, S., Christandl, M., Horodecki, K., Winter, A.: Limitations on quantum key repeaters. Nat. Commun. **6**, 6908 (2015)
8. Naseri, M.: Secure quantum sealed-bid auction. Opt. Commun. **282**, 1939 (2009)
9. Ambainis, A., Mosca, M., Tapp, A., de Wolf, R.: Private quantum channels. In: IEEE Symposium on Foundations of Computer Sciences (FOCS), pp. 547–553 (2000)
10. Nagaj, D., Kerenidis, I.: On the optimality of quantum encryption schemes. J. Math. Phys. **47**, 092102 (2006)
11. Bouda, J., Ziman, M.: Optimality of private quantum channels. J. Phys. A **40**, 5415 (2007)
12. Hayden, P., Leung, D., Shor, P.W., Winter, A.: Randomizing quantum states: constructions and applications. Commun. Math. Phys. **250**, 371 (2004)
13. Ambainis, A., Smith, A.: Small pseudo-random families of matrices: derandomizing approximate quantum encryption. In: Proceedings of RANDOM 2004, pp. 249–260 (2004)
14. Dickinson, P.A., Nayak, A.: Approximate randomization of quantum states with fewer bits of key. In: AIP Conference Proceedings, vol. 864, p. 18 (2006)
15. Holevo, A.S.: Bounds for the quantity of information transmitted by a quantum communication channel. Probl. Inf. Transm. (USSR) **9**, 177 (1973)
16. Chi, D.P., Jeong, K.: Approximate quantum state sharings via pair of private quantum channels. J. Quantum Inf. Sci. **4**, 64 (2014)
17. Sun, Y., Gao, F., Yuan, Z., Li, Y., Wen, Q.: Splitting a quantum secret without the assistance of entanglements. Quantum Inf. Process **11**, 1741 (2012)

18. Naor, J., Naor, M.: Small-bias probability spaces: efficient constructions and applications. SIAM J. Comput. **22**(4), 838 (1993)
19. There exixts such a subset $E_j \subset \{0,1\}^{2n} \forall j$ with $\sqrt[m]{\varepsilon}/2^{n/2m}$-biased, because the subset E in Eq. (7) is upper bounded by $\varepsilon/2^{n/2}$
20. Ziman, M., Bužek, V.: All (qubit) decoherences: complete characterization and physical implementation. Phys. Rev. A **72**, 022110 (2005)