Quantum Network Coding

Masahito Hayashi[1*] Kazuo Iwama[2†] Harumichi Nishimura[3‡]
Rudy Raymond[4] Shigeru Yamashita[5§]

[1]ERATO-SORST Quantum Computation and Information Project,
Japan Science and Technology Agency
masahito@qci.jst.go.jp
[2]School of Informatics, Kyoto University
iwama@kuis.kyoto-u.ac.jp
[3]School of Science, Osaka Prefecture University
hnishimura@mi.s.osakafu-u.ac.jp
[4]Tokyo Research Laboratory, IBM Japan
raymond@jp.ibm.com
[5]Graduate School of Information Science, Nara Institute of Science and Technology
ger@is.naist.jp.

Abstract. Since quantum information is continuous, its handling is sometimes surprisingly harder than the classical counterpart. A typical example is cloning; making a copy of digital information is straightforward but it is not possible exactly for quantum information. The question in this paper is whether or not *quantum* network coding is possible. Its classical counterpart is another good example to show that digital information flow can be done much more efficiently than conventional (say, liquid) flow.

Our answer to the question is similar to the case of cloning, namely, it is shown that quantum network coding is possible if approximation is allowed, by using a simple network model called Butterfly. In this network, there are two flow paths, s_1 to t_1 and s_2 to t_2, which shares a single bottleneck channel of capacity one. In the classical case, we can send two bits simultaneously, one for each path, in spite of the bottleneck. Our results for quantum network coding include: (i) We can send any quantum state $|\psi_1\rangle$ from s_1 to t_1 and $|\psi_2\rangle$ from s_2 to t_2 simultaneously with a fidelity strictly greater than 1/2. (ii) If one of $|\psi_1\rangle$ and $|\psi_2\rangle$ is classical, then the fidelity can be improved to 2/3. (iii) Similar improvement is also possible if $|\psi_1\rangle$ and $|\psi_2\rangle$ are restricted to only a finite number of (previously known) states. (iv) Several impossibility results including the general upper bound of the fidelity are also given.

1 Introduction

In [3], Ahlswede, Cai, Li and Yeung showed that the fundamental law for network flow, the max-flow min-cut theorem, no longer applies for "digital information flow." The simple and nice example in [3] is called the Butterfly network as illustrated in Fig. 1. The capacity of each directed link is all one and there are two source-sink pairs: s_1 to t_1 and s_2 to t_2. Notice that both paths have to use the single link from s_0 to t_0 and hence the total amount of (conventional commodity) flow in both paths is bounded by one, say, 1/2 for each. In the case of digital information flow, however,
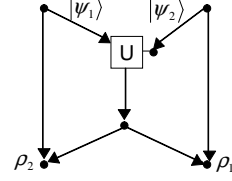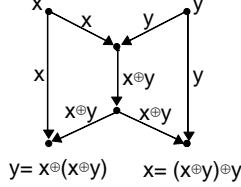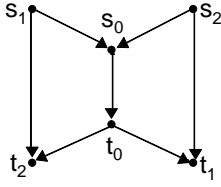

Figure 1: Butterfly network.

Figure 2: Coding scheme

Figure 3: Network using a controlled unitary operation

the protocol shown in Fig. 2 allows us to transmit two bits, x and y, simultaneously. Thus, we can effectively achieve larger channel capacity than what can be achieved by simple routing. This is known as *network coding* since [3] and has been quite popular (see e.g., Network coding home page [20] or [1, 15, 19, 21, 22] for recent developments).

Network coding obviously exploits the two side links, s_1 to t_2 and s_2 to t_1, which are completely useless graph-topologically. Now the primary question in this paper is whether this is also possible for *quantum* information: Our model is the same butterfly network with (unit-capacity) quantum channels and our goal is to send two qubits from s_1 to t_1 and s_2 to t_2 simultaneously. To this end, one should notice that the protocol in Fig. 2 uses (at least) two tricks. One is the EX-OR (Exclusive-OR) operation at node s_0; one can see that the bit y is encoded by using x as a key which is sent directly from s_1 to t_2, and vise versa. The other is the exact copy of one-bit information at node t_0. Are there any quantum counterparts for these key operations?

Neither seems easy in the quantum case: For the copy operation, there is the famous no-cloning theorem. Also, there is no obvious way of encoding a quantum state by a quantum state at s_0. Consider, for example, a simple extension of the classical operation at node s_0,i.e., a controlled unitary transform U as illustrated in Fig. 3. (Note that classical EX-OR is realized by setting $U = X$ "bit-flip.") Then, for any U, there is a quantum state $|\phi\rangle$ (actually an eigenvector of U) such that $|\phi\rangle$ and $U|\phi\rangle$ are identical (up to a global phase). Namely, if $|\psi_1\rangle = |\phi\rangle$, then the quantum state at the output of U is exactly the same for $|\psi_2\rangle = |0\rangle$ and $|\psi_2\rangle = |1\rangle$. This means their difference is completely lost at that position and hence is completely lost at t_1 also.

Thus it is highly unlikely that we can achieve an exact transmission of two quantum states, which forces us to consider an *approximate* transmission. As an approximation factor, we use a (worst-case) *fidelity* between the input state $|\psi_1\rangle$ at s_1 ($|\psi_2\rangle$ at s_2, resp.) and the output state $\boldsymbol{\rho}_1$ at t_1 ($\boldsymbol{\rho}_2$ at t_2, resp.) Recall that the fidelity is at most 1.0 by definition and 0.5 is automatically achieved by outputting a completely mixed state. Thus our question is whether we can achieve a fidelity of strictly greater than 0.5.

Our Contribution. This paper gives a positive answer to this question. We first show that we do need the (topologically useless) side channels for our goal exactly as in the classical case (Theorem 2.1). Namely, without them, we can prove that for any protocol, there exists a quantum state $|\psi_i\rangle$ ($i = 1$ or 2) and its output state $\boldsymbol{\rho}_i$ such that $F(|\psi_i\rangle, \boldsymbol{\rho}_i) \leq 1/2$. We then give our protocol which achieves a fidelity of strictly greater than $1/2$ for the butterfly network (Theorem 3.1). The idea is discretization of (continuous) quantum states. Namely, the quantum state from s_2 is changed into classical two bits by using what we call "tetra measurement." Those two bits are then used as a key to encode the state from s_1 at node s_0 ("group operation") and also to decode it at node t_1. Our protocol also depends upon the approximate cloning by Bužek and Hillery [9]. This obviously distorts quantum states, but interestingly, it also has a merit (creating entanglement between cloned states) by which we can handle the second problem on the state distinguishability previously mentioned.

2

Note that the present general lower bound for the fidelity is only slightly better than $1/2$ (some 0.52). However, if we impose restriction, the value becomes much better. For example, if $|\psi_1\rangle$ is a classical state (i.e. either $|0\rangle$ or $|1\rangle$), then the fidelity becomes $2/3$ (Theorem 4.1). Similar improvement is also possible if $|\psi_1\rangle$ and $|\psi_2\rangle$ are restricted to only a finite number of (previously known) states, especially if they are the so-called quantum random access coding states [4]. By using those states, we can design an interesting protocol which can send two classical bits from s_1 to t_1 (similarly two bits from s_2 to t_2) but only one of them, determined by adversary, should be recovered. It is shown that the success probability for this protocol is $1/2 + \sqrt{2}/16$ (Theorem 5.1), but classically the success probability for any protocol is at most $1/2$.

On the negative side, several upper bounds for the fidelity are given. Again, the most general one (Theorem 3.10) may not seem very impressive (some 0.983), but it is improved under restrictions. In particular, if we impose the BC (bit-copy) assumption, we can prove an upper bound of $11/12$ (Theorem 4.2). (BC means that whenever we need to copy a classical bit, we use the classical (exact) copy, which seems quite reasonable.) We also give a limit of transmitting random access coding states. Note that Theorem 5.1 can be extended to the three-bit case (with success probability some 0.525) but that is the limit; no protocol exists for the four-bit transmission with success probability strictly greater than $1/2$ (Theorem 5.3).

Related Work. We usually allow approximation and/or errors in quantum computation, which seems to be an essence of its power in some occasions. One example is observed in communication complexity: The quantum communication complexity to compute the equality function EQ_n exactly is n [18]. However, even one qubit communication enables us to compute EQ_n with success probability larger than $1/2$. Another example can be seen in locally decodable codes and private information retrievals: Any $2n$-bit Boolean function F can be computed with success probability $> 1/2$ from an $(n+1)$-qubit information [31]. Namely, $n+1$ qubits can encode $2n$ classical bits for computing *any* Boolean function approximately.

Thus "$1/2 + \epsilon$ for very small ϵ" seems very powerful. Interestingly, this is not the case in some other occasions. the Nayak bound [24] says that there is no way to send two bits by one qubit with success probability $> 1/2$. Moreover, [17] shows that one-qubit random access coding for four bits can only be done with success probability at most $1/2$, although we can enjoy a good success probability up to three bits. In this context, our model in this paper also shows a clear difference depending on whether or not the two side links exist.

The study of coding methods on quantum information and computation has been deeply explored for error correction of quantum computation (since [30]) and data compression of quantum sources (since [28]). Recall that their techniques are duplication of data (error correction) and average-case analysis (data compression). Those standard approaches do not seem to help in the core of our problem. More tricky applications of quantum mechanism are quantum teleportation [6], superdense coding [7], and a variety of quantum cryptosystems including the BB84 key distribution [5]. The random access coding by Ambainis, Nayak, Ta-shma, and Vazirani [4] is probably most related one to this paper, which allows us to encode two or more classical bits into one qubit and decode it to recover any one of the source bits. Our third protocol is a realization of this scheme on the Butterfly network.

The introduction of quantum network coding [16] triggered several new studies: Leung, Oppenheim, and Winter [23] examined the asymptotic relation between the amount of quantum information and channel capacities on the Butterfly network (and more). Shi and Soljanin [29] considered multicasting networks from the viewpoint of lossless compression and decompression of copies of quantum states.
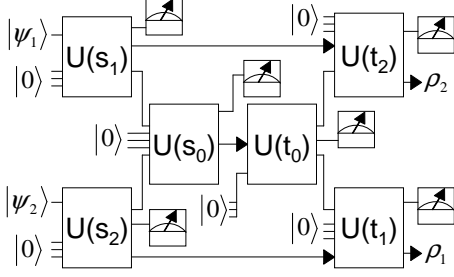
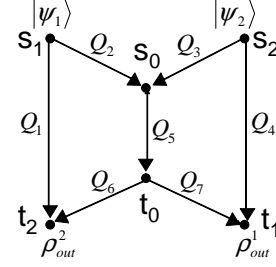Figure 4: Quantum circuit for coding on the Butterfly network

Figure 5: Protocol XQQ.

2 The Model

Our model as a quantum circuit is shown in Fig. 4. The information sources at nodes s_1 and s_2 are pure one-qubit states $|\psi_1\rangle$ and $|\psi_2\rangle$. (It turns out, however, that the result does not change for mixed states because of the joint concavity of the fidelity [25].) Any node does not have prior entanglement with other nodes. At every node, a physically allowable operation, i.e., trace-preserving completely positive map (TP-CP map), is done, and each edge can send only one qubit. They are implemented by unitary operations with additional ancillae and by discarding all qubits except for the output qubits [2, 25].

Our goal is to send $|\psi_1\rangle$ to node t_1 and $|\psi_2\rangle$ to node t_2 as well as possible. The quality of data at node t_j is measured by the fidelity between the original state $|\psi_j\rangle$ and the state $\boldsymbol{\rho}_j$ output at node t_j by the protocol. Here, the fidelity between two quantum states $\boldsymbol{\rho}$ and $\boldsymbol{\sigma}$ are defined as $F(\boldsymbol{\sigma},\boldsymbol{\rho}) = \left(\text{Tr}\sqrt{\boldsymbol{\rho}^{1/2}\boldsymbol{\sigma}\boldsymbol{\rho}^{1/2}}\right)^2$ as in [10, 8, 11]. (The other common definition is $\text{Tr}\sqrt{\boldsymbol{\rho}^{1/2}\boldsymbol{\sigma}\boldsymbol{\rho}^{1/2}}$.) In particular, the fidelity between a pure state $|\psi\rangle$ and a mixed state $\boldsymbol{\rho}$ is $F(|\psi\rangle,\boldsymbol{\rho}) = \langle\psi|\boldsymbol{\rho}|\psi\rangle$. (To simplify the description, for a pure state $|\psi\rangle\langle\psi|$ we often use the vector representation $|\psi\rangle$ and we also use bold fonts for a 2×2 or 4×4 density matrix for exposition.) We call the minimum of $F(|\psi_1\rangle,\boldsymbol{\rho}_1)$ over all one-qubit states $|\psi_1\rangle$ and $|\psi_2\rangle$ the *fidelity at node t_1* and similarly for *fidelity at node t_2*.

Before presenting our protocols achieving a fidelity of strictly greater than $1/2$, we show that the two side links, which are useless graph-topologically, are indispensable. One might think this is trivial from the Nayak bound [24]. Namely, if the two inputs are classical 0/1 bits, then they cannot be sent using a single quantum channel (s_0 to t_0) with success probability (= fidelity) greater than $1/2$. This is not true since our definition only requires a fidelity at *each* sink. In fact, we can achieve a fidelity of at least 0.75 in our definition, by simply using the one-qubit random access coding for two bits [4] and the phase-covariant cloning (a kind of approximated cloning) [8, 11]. (Note that $0.75^2 > 0.5$ but this does not violate the Nayak bound since the success probabilities at the two sides are not independent.) The proof of the following theorem needs a careful consideration of physical operations on the Bloch ball (see, e.g., [12, 27]) and the trace distance. Notice that in this paper, the trace distance between two quantum states $\boldsymbol{\rho}$ and $\boldsymbol{\rho}'$ is defined to be $||\boldsymbol{\rho} - \boldsymbol{\rho}'||_{tr}$ without the normalization factor 2 as in [25]. (If two states are qubits, this distance is equal to the geometrical distance of the corresponding points in the Bloch ball.)

Theorem 2.1 *No quantum protocol can achieve fidelity larger than $1/2$ if both side links are removed from the Butterfly.*

Proof. We show that, for any proper protocol, if the fidelity at t_2 is larger than $1/2$ (say, $1/2+\epsilon$

4

with $\epsilon > 0$) then the fidelity at t_1 is strictly less than $1/2$. For our purpose, we consider the case where the sources at s_1 and s_2 are a qubit $|\psi\rangle$ and a classical bit b, respectively. We can assume that they are sent to s_0 without any transformation (since otherwise their operations at s_1 and s_2 can be delayed until s_0). Now, let $\mathcal{E}_b$ be the images of the Bloch ball resulting from operations at s_0 when b is sent from s_2. Let the distance between $\mathcal{E}_0$ and $\mathcal{E}_1$ be the minimum trace distance between any state in $\mathcal{E}_0$ and that in $\mathcal{E}_1$. Then, the following lemma holds from the fidelity requirement at t_2:

Lemma 2.2 *The distance between $\mathcal{E}_0$ and $\mathcal{E}_1$ is at least 4ϵ.*

Proof. Let C_b be the TP-CP map at s_0 when b is sent from s_2. We can regard the operations at t_0 and t_2 along the path s_2-t_2 as the measurement defined by a POVM (positive operator-valued measure) $\{E_0, E_1\}$. (Recall that any measurement is defined by a POVM $\{E_i\}_i$, that is, each operator E_i is positive and $\sum_i E_i = I$.) Then, to prove the lemma we need to show that for any one-qubit states $|\psi\rangle, |\psi'\rangle$, $||C_0(|\psi\rangle) - C_1(|\psi'\rangle)||_{tr} \geq 4\epsilon$. However, by the fidelity requirement at t_2, for any $|\psi\rangle, |\psi'\rangle$ and any $b = 0, 1$, it must hold that $\text{Tr}(E_b C_b(|\psi\rangle)) \geq 1/2 + \epsilon$ and $\text{Tr}(E_b C_{1-b}(|\psi'\rangle)) \leq 1/2 - \epsilon$. Thus, we have $||C_0(|\psi\rangle) - C_1(|\psi'\rangle)||_{tr} \geq \sum_{b=0,1} |\text{Tr} E_b(C_0(|\psi\rangle) - C_1(|\psi'\rangle))| \geq 4\epsilon$, where the first inequality is obtained from the following fact: For any quantum states $\boldsymbol{\rho}, \boldsymbol{\rho}'$, $||\boldsymbol{\rho} - \boldsymbol{\rho}'||_{tr}$ equals $\max_{\{F_0, F_1\}} \sum_b |\text{Tr} F_b(\boldsymbol{\rho} - \boldsymbol{\rho}')|$ where the maximization is over all POVMs $\{F_0, F_1\}$ [25]. □ By

Lemma 2.2, the center of the Bloch ball is outside at least one of $\mathcal{E}_0$ and $\mathcal{E}_1$. Now let $\mathcal{F}_b$ be the final images at t_1 when b is the source at s_2, and let T be the composite TP-CP map of t_0 and t_1 along the path s_1-t_1. Note that $\mathcal{F}_0 = T(\mathcal{E}_0)$ and $\mathcal{F}_1 = T(\mathcal{E}_1)$, and T is linear. Since T transforms the Bloch ball into an ellipsoid within the Bloch ball [12, 27], the center of the Bloch ball is outside one of ellipsoids $\mathcal{F}_0$ and $\mathcal{F}_1$, say $\mathcal{F}_0$. This means that there exists some input state $|\psi\rangle$ at s_1 such that $|\psi\rangle$ and its output state $\boldsymbol{\rho}_\psi$ at t_1 are in different half of the Bloch ball, that is, $F(|\psi\rangle, \boldsymbol{\rho}_\psi) < 1/2$. Therefore the fidelity at t_1 is $< 1/2$. □

3 Protocol for Crossing Two Qubits

In this section we prove the following lower bound.

Theorem 3.1 *There exists a quantum protocol whose fidelities at nodes t_1 and t_2 are $1/2 + 2/81$ and $1/2 + 2\sqrt{3}/243$, respectively.*

3.1 Overview of the Protocol

Fig. 5 illustrates our protocol, Protocol for Crossing Two Qubits (XQQ). As expected, the approximated cloning is used at nodes s_1, s_2 and t_0. At node s_0, we first apply the tetra measurement to the state of one-qubit system $\mathcal{Q}_3$ and obtain two classical bits $r_1 r_2$. Their different four values suggest which part of the Bloch sphere the state of $\mathcal{Q}_3$ sits in. These four values are then used to choose one of four different operations, the group operations, to encode the state of $\mathcal{Q}_2$. These four operations include identity I, bit-flip X, phase-flip Z, and bit+phase-flip Y. At node t_1, we apply the reverse operations of these four operations (actually the same as the original ones) for the decoding purpose.

At node t_2, we recover the two bits $r_1 r_2$ (actually the corresponding quantum state for the output state) by comparing $\mathcal{Q}_1$ and $\mathcal{Q}_6$. This should be possible since $\mathcal{Q}_2$ ($\approx \mathcal{Q}_1$) is encoded into $\mathcal{Q}_5$ ($\approx \mathcal{Q}_6$) by using $r_1 r_2$ as a key but its implementation is not obvious. It is shown that for this purpose, we can use the Bell measurement together with the fact that $\mathcal{Q}_1$ and $\mathcal{Q}_2$ are partially

entangled as a result of cloning at node s_1.

Remark. It is not hard to average the fidelities at t_1 and t_2 by mixing the encoding state at t_1 with the Bell state $(|00\rangle + |11\rangle)/\sqrt{2}$, implying $1/2 + 2(2 - \sqrt{3})/27 \approx 0.52$ at both sinks.

3.2 Building Blocks

Universal Cloning (UC). As the first tool of our protocol, we recall the notion of the approximated cloning by Bužek and Hillery [9], called the *universal cloning*. Let $|\Psi^+\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$. Then, it is given by the TP-CP map UC defined by

$$UC(|0\rangle\langle 0|) = \frac{2}{3}|00\rangle\langle 00| + \frac{1}{3}|\Psi^+\rangle\langle\Psi^+|, \quad UC(|0\rangle\langle 1|) = \frac{\sqrt{2}}{3}|\Psi^+\rangle\langle 11| + \frac{\sqrt{2}}{3}|00\rangle\langle\Psi^+|,$$

$$UC(|1\rangle\langle 0|) = \frac{\sqrt{2}}{3}|11\rangle\langle\Psi^+| + \frac{\sqrt{2}}{3}|\Psi^+\rangle\langle 00|, \quad UC(|1\rangle\langle 1|) = \frac{2}{3}|11\rangle\langle 11| + \frac{1}{3}|\Psi^+\rangle\langle\Psi^+|. \tag{1}$$

This map is intended to clone not only classical states $|0\rangle$ and $|1\rangle$ but also any superposition equally well by mixing the symmetric state $|\Psi^+\rangle$ with $|00\rangle$ and $|11\rangle$ as the output. Let $\boldsymbol{\rho}_1 = \mathrm{Tr}_2 UC(|\psi\rangle)$ and $\boldsymbol{\rho}_2 = \mathrm{Tr}_1 UC(|\psi\rangle)$, where Tr_i is the partial trace over the i-th qubit. Then, easy calculation implies that $\boldsymbol{\rho}_1 = \boldsymbol{\rho}_2 = \frac{2}{3}|\psi\rangle\langle\psi| + \frac{1}{3}\cdot\frac{\boldsymbol{I}}{2}$, which means $F(|\psi\rangle, \boldsymbol{\rho}_1) = F(|\psi\rangle, \boldsymbol{\rho}_2) = 5/6$. We call its induced map $|\psi\rangle \mapsto \boldsymbol{\rho}_1$ (or $|\psi\rangle \mapsto \boldsymbol{\rho}_2$) the *universal copy*.

Tetra Measurement (TTR). Next, we introduce the tetra measurement. We need the following four states $|\chi(00)\rangle = \cos\tilde{\theta}|0\rangle + e^{\imath\pi/4}\sin\tilde{\theta}|1\rangle$, $|\chi(01)\rangle = \cos\tilde{\theta}|0\rangle + e^{-3\imath\pi/4}\sin\tilde{\theta}|1\rangle$, $|\chi(10)\rangle = \sin\tilde{\theta}|0\rangle + e^{-\imath\pi/4}\cos\tilde{\theta}|1\rangle$, and $|\chi(11)\rangle = \sin\tilde{\theta}|0\rangle + e^{3\imath\pi/4}\cos\tilde{\theta}|1\rangle$ with $\cos^2\tilde{\theta} = 1/2 + \sqrt{3}/6$, which form a tetrahedron in the Bloch sphere representation. The *tetra measurement*, denoted by TTR, is the POVM defined by $\{\frac{1}{2}|\chi(00)\rangle\langle\chi(00)|, \frac{1}{2}|\chi(01)\rangle\langle\chi(01)|, \frac{1}{2}|\chi(10)\rangle\langle\chi(10)|, \frac{1}{2}|\chi(11)\rangle\langle\chi(11)|\}$.

Group Operation (GR). In what follows, let $X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ be the bit-flip operation, $Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ be the phase-flip operation, and $Y = XZ$. Notice that the set of unitary maps on one-qubit states $\boldsymbol{\rho} \mapsto W\boldsymbol{\rho}W^\dagger$ ($W = I, Z, X, Y$) is the Klein four group. The *group operation under* a two-bit string $r_1 r_2$, denoted by $GR(\boldsymbol{\rho}, r_1 r_2)$, is a transformation defined by $GR(\boldsymbol{\rho}, 00) = \boldsymbol{\rho}$, $GR(\boldsymbol{\rho}, 01) = Z\boldsymbol{\rho}$, $GR(\boldsymbol{\rho}, 10) = X\boldsymbol{\rho}$, and $GR(\boldsymbol{\rho}, 11) = Y\boldsymbol{\rho}$. Note that we frequently use simplified expressions like $X\boldsymbol{\rho}$ instead of $X\boldsymbol{\rho}X^\dagger$.

3D Bell Measurement (BM). Moreover, for recovering $|\psi_2\rangle$ at node t_2 we introduce another new operation based on the Bell measurement, $BM(\mathcal{Q}, \mathcal{Q}')$ (or $BM(\boldsymbol{\sigma})$), which applies the following three operations (a), (b), and (c) with probability $1/3$ for each, to the state $\boldsymbol{\sigma}$ (a 4×4 density matrix) of the two-qubit system $\mathcal{Q} \otimes \mathcal{Q}'$.

(a) Measure $\boldsymbol{\sigma}$ in the Bell basis $\left\{|\Phi^+\rangle = \frac{|00\rangle+|11\rangle}{\sqrt{2}}, |\Phi^-\rangle = \frac{|00\rangle-|11\rangle}{\sqrt{2}}, |\Psi^+\rangle = \frac{|01\rangle+|10\rangle}{\sqrt{2}}, |\Psi^-\rangle = \frac{|01\rangle-|10\rangle}{\sqrt{2}}\right\}$, and output $|0\rangle$ if the measurement result for $|\Phi^+\rangle$ or $|\Phi^-\rangle$ is obtained, and $|1\rangle$ otherwise.

(b) Measure $\boldsymbol{\sigma}$ similarly, and output $|+\rangle$ if the measurement result for $|\Phi^+\rangle$ or $|\Psi^+\rangle$ is obtained, and $|-\rangle$ otherwise.

(c) Measure $\boldsymbol{\sigma}$ similarly, and output $|+'\rangle = \frac{1}{\sqrt{2}}(|0\rangle + \imath|1\rangle)$ if the measurement result for $|\Phi^+\rangle$ or $|\Psi^-\rangle$ is obtained, and $|-'\rangle = \frac{1}{\sqrt{2}}(|0\rangle - \imath|1\rangle)$ otherwise.

3.3 Protocol XQQ and Its Performance Analysis

Now here is the formal description of our protocol.

Protocol XQQ: Input $|\psi_1\rangle$ at s_1, and $|\psi_2\rangle$ at s_2; Output $\boldsymbol{\rho}_{out}^1$ at t_1, and $\boldsymbol{\rho}_{out}^2$ at t_2.
    Step 1. $(\mathcal{Q}_1, \mathcal{Q}_2) = UC(|\psi_1\rangle)$ at s_1, and $(\mathcal{Q}_3, \mathcal{Q}_4) = UC(|\psi_2\rangle)$ at s_2.
    Step 2. $\mathcal{Q}_5 = GR(\mathcal{Q}_2, TTR(\mathcal{Q}_3))$ at s_0.
    Step 3. $(\mathcal{Q}_6, \mathcal{Q}_7) = UC(\mathcal{Q}_5)$ at t_0.
    Step 4 (Decoding at node t_1 and t_2). $\boldsymbol{\rho}_{out}^1 = GR(\mathcal{Q}_7, TTR(\mathcal{Q}_4))$, and $\boldsymbol{\rho}_{out}^2 = BM(\mathcal{Q}_1, \mathcal{Q}_6)$.

We give the proof of Theorem 3.1 by analyzing protocol XQQ. For this purpose, we introduce the notion of shrinking maps (also known as a depolarizing channel [25]), which plays an important role in the following analysis of XQQ: Let $\boldsymbol{\rho}$ be any quantum state. Then, if a map C transforms $\boldsymbol{\rho}$ to $p \cdot \boldsymbol{\rho} + (1-p)\frac{\boldsymbol{I}}{2}$ for some $0 \leq p \leq 1$, then C is said to be *p-shrinking*. The following three lemmas are immediate:

Lemma 3.2 *If C is p-shrinking and C' is p'-shrinking, then $C \circ C'$ is pp'-shrinking.*

Lemma 3.3 *If C is p-shrinking, $F(\boldsymbol{\rho}, C(\boldsymbol{\rho})) \geq 1/2 + p/2$ for any state $\boldsymbol{\rho}$.*

Lemma 3.4 *The universal copy is $2/3$-shrinking.*

    Computing the Fidelity at Node t_1. We first investigate the quality of the path from s_1 to t_1. Fix $\boldsymbol{\rho}_2 = |\psi_2\rangle\langle\psi_2|$ as an arbitrary state at node s_2 and consider four maps C_1: $|\psi_1\rangle \to \mathcal{Q}_2$, $C_2[\boldsymbol{\rho}_2]$: $\mathcal{Q}_2 \to \mathcal{Q}_5$, C_3: $\mathcal{Q}_5 \to \mathcal{Q}_7$ and $C_4[\boldsymbol{\rho}_2]$: $\mathcal{Q}_7 \to \boldsymbol{\rho}_{out}^1$. We wish to compute the composite map $C_{s_1 t_1} = C_4[\boldsymbol{\rho}_2] \circ C_3 \circ C_2[\boldsymbol{\rho}_2] \circ C_1$ and its fidelity. We need two more lemmas before the final one (Lemma 3.7).

Lemma 3.5 $C_3 \circ C_2[\boldsymbol{\rho}_2] = C_2[\boldsymbol{\rho}_2] \circ C_3$.

Proof. We decompose the p-shrinking map $C^{(p)}$ into $C^{(p)} = pC^{(1)} + (1-p)C^{(0)}$. Here, the 1-shrinking map $C^{(1)}$ is the identity and the 0-shrinking map $C^{(0)}$ transforms any state to $\frac{\boldsymbol{I}}{2}$. Clearly, $C^{(1)}$ is commutative with $C_2[\boldsymbol{\rho}_2]$. For showing the commutativity between $C^{(0)}$ and $C_2[\boldsymbol{\rho}_2]$, we prove that, for any qubit $\boldsymbol{\rho}$ and any 2×2 matrix basis element $|b\rangle\langle b'|$ (where $b, b' \in \{0, 1\}$) on $\mathcal{Q}_3$, $C^{(0)}(GR(\boldsymbol{\rho}, TTR(|b\rangle\langle b'|))) = GR(C^{(0)}(\boldsymbol{\rho}), TTR(|b\rangle\langle b'|))$. The left-hand side is $\sum_{r \in \{0,1\}^2} \langle r|TTR(|b\rangle\langle b'|)|r\rangle\frac{\boldsymbol{I}}{2}$ since $GR(\boldsymbol{\rho}, TTR(|b\rangle\langle b'|)) = \sum_{r \in \{0,1\}^2} \langle r|TTR(|b\rangle\langle b'|)|r\rangle GR(r, \boldsymbol{\rho})$ and $C^{(0)}$ is 0-shrinking. The right-hand side is

$$GR(\boldsymbol{I}/2, TTR(|b\rangle\langle b'|)) = \sum_{r \in \{0,1\}^2} \langle r|TTR(|b\rangle\langle b'|)|r\rangle GR(r, \boldsymbol{I}/2) = \sum_{r \in \{0,1\}^2} \langle r|TTR(|b\rangle\langle b'|)|r\rangle\frac{\boldsymbol{I}}{2}.$$

Thus, by linearity, the p-shrinking map and $C_2[\boldsymbol{\rho}_2]$ are commutative. Now the proof is completed since C_3 is $2/3$-shrinking by Lemma 3.4. $\square$

Lemma 3.6 *(Main Lemma)* $C_4[\boldsymbol{\rho}_2] \circ C_2[\boldsymbol{\rho}_2]$ *is $\frac{1}{9}$-shrinking. (See below for the proof.)*

Lemma 3.7 *For any $|\psi_1\rangle$, $F(|\psi_1\rangle, C_{s_1 t_1}(|\psi_1\rangle)) \geq 1/2 + 2/81$.*

Proof. By Lemma 3.5, $C_{s_1 t_1} = C_4[\boldsymbol{\rho}_2] \circ C_2[\boldsymbol{\rho}_2] \circ C_3 \circ C_1$. C_3 and C_1 are both $2/3$-shrinking by Lemma 3.4 and $C_4[\boldsymbol{\rho}_2] \circ C_2[\boldsymbol{\rho}_2]$ is $\frac{1}{9}$-shrinking by Lemma 3.6. It then follows that $C_{s_1 t_1}$ is $\frac{4}{81}$-shrinking by Lemma 3.2 and its fidelity is at least $1/2 + 2/81$ by Lemma 3.3. $\square$

Proof of Lemma 3.6. See Fig. 5 again. Since we are discussing $C_4[\boldsymbol{\rho}_2] \circ C_2[\boldsymbol{\rho}_2]$, let $\boldsymbol{\rho}_1 = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$

7

be the state on $\mathcal{Q}_2$, $\boldsymbol{\rho}_2 = |\psi_2\rangle\langle\psi_2| = \begin{pmatrix} e & f \\ g & h \end{pmatrix}$ be the state at s_2 and assume that $\mathcal{Q}_5 = \mathcal{Q}_7$. We calculate the state on $\mathcal{Q}_2 \otimes \mathcal{Q}_3 \otimes \mathcal{Q}_4$, the state on $\mathcal{Q}_5 \otimes \mathcal{Q}_4$ ($= \mathcal{Q}_7 \otimes \mathcal{Q}_4$) and $\boldsymbol{\rho}_{out}^1$ in this order. For $\mathcal{Q}_2 \otimes \mathcal{Q}_3 \otimes \mathcal{Q}_4$, recall that $\boldsymbol{\rho}_2$ is cloned into $\mathcal{Q}_3$ and $\mathcal{Q}_4$ and so, by Eq.(1) in Sec. 3.2, the state on $\mathcal{Q}_2 \otimes \mathcal{Q}_3 \otimes \mathcal{Q}_4$ is written as

$$
\boldsymbol{\rho}_1 \otimes \left[\frac{2e}{3}|00\rangle\langle00| + \frac{e}{6}(|01\rangle + |10\rangle)(\langle01| + \langle10|) + \frac{f}{3}((|01\rangle + |10\rangle)\langle11| + |00\rangle(\langle01| + \langle10|)) \right.
$$

$$
\left. + \frac{g}{3}(|11\rangle(\langle01| + \langle10|) + (|01\rangle + |10\rangle)\langle00|) + \frac{2h}{3}|11\rangle\langle11| + \frac{h}{6}(|01\rangle + |10\rangle)(\langle01| + \langle10|) \right]
$$

$$
= \boldsymbol{\rho}_1 \otimes |0\rangle\langle0| \otimes \left(\frac{2e}{3}|0\rangle\langle0| + \frac{f}{3}|0\rangle\langle1| + \frac{g}{3}|1\rangle\langle0| + \frac{1}{6}|1\rangle\langle1| \right) + \boldsymbol{\rho}_1 \otimes |0\rangle\langle1| \otimes \left(\frac{1}{6}|1\rangle\langle0| + \frac{f}{3}\boldsymbol{I} \right)
$$

$$
+ \boldsymbol{\rho}_1 \otimes |1\rangle\langle0| \otimes \left(\frac{1}{6}|0\rangle\langle1| + \frac{g}{3}\boldsymbol{I} \right) + \boldsymbol{\rho}_1 \otimes |1\rangle\langle1| \otimes \left(\frac{1}{6}|0\rangle\langle0| + \frac{f}{3}|0\rangle\langle1| + \frac{g}{3}|1\rangle\langle0| + \frac{2h}{3}|1\rangle\langle1| \right). \quad (2)
$$

Then, we apply the group operation to the first two bits of $\mathcal{Q}_2 \otimes \mathcal{Q}_3 \otimes \mathcal{Q}_4$. In general, for $\mathcal{Q} \otimes \mathcal{Q}'$, $GR(\mathcal{Q}, TTR(\mathcal{Q}'))$ is given as follows (see Appendix for the proof).

Lemma 3.8 *Let $\boldsymbol{\rho}$ be the state on $\mathcal{Q}$. Then, $GR(\mathcal{Q}, TTR(\mathcal{Q}'))$ is the following TP-CP map:*

$$
\boldsymbol{\rho} \otimes |0\rangle\langle0| \mapsto \frac{1}{\sqrt{3}}V(I,Z)\boldsymbol{\rho} + \left(1 - \frac{1}{\sqrt{3}} \right) \cdot \frac{\boldsymbol{I}}{2}, \quad \boldsymbol{\rho} \otimes |1\rangle\langle1| \mapsto \frac{1}{\sqrt{3}}V(X,Y)\boldsymbol{\rho} + \left(1 - \frac{1}{\sqrt{3}} \right) \cdot \frac{\boldsymbol{I}}{2},
$$

$$
\boldsymbol{\rho} \otimes |0\rangle\langle1| \mapsto \frac{1}{2\sqrt{3}}(V(I,X)\boldsymbol{\rho} - V(Y,Z)\boldsymbol{\rho} + \imath(V(I,Y)\boldsymbol{\rho} - V(Z,X)\boldsymbol{\rho})),
$$

$$
\boldsymbol{\rho} \otimes |1\rangle\langle0| \mapsto \frac{1}{2\sqrt{3}}(V(I,X)\boldsymbol{\rho} - V(Y,Z)\boldsymbol{\rho} - \imath(V(I,Y)\boldsymbol{\rho} - V(Z,X)\boldsymbol{\rho})).
$$

Here, $V(I,Z)\boldsymbol{\rho} = \frac{1}{2}(I\boldsymbol{\rho} + Z\boldsymbol{\rho})$, and $V(X,Y)\boldsymbol{\rho}$, $V(I,X)\boldsymbol{\rho}$, $V(Y,Z)\boldsymbol{\rho}$, $V(I,Y)\boldsymbol{\rho}$, and $V(Z,X)\boldsymbol{\rho}$ are similarly defined. Those six operations are $\boldsymbol{I}$-invariant (meaning it maps $\boldsymbol{I}$ to itself) TP-CP maps.

Now the state on $\mathcal{Q}_5 \otimes \mathcal{Q}_4$ is obtained by applying Lemma 3.8 to Eq.(2). From now on, we omit the term for $\frac{\boldsymbol{I}}{2}$. Namely, if the one-qubit state is $\boldsymbol{\rho} + \alpha\frac{\boldsymbol{I}}{2}$, we only describe $\boldsymbol{\rho}$. This is not harmful since any operation in this section is $\boldsymbol{I}$-invariant and hence the $\frac{\boldsymbol{I}}{2}$ term can be recovered at the end by using the trace property. Thus, the state on $\mathcal{Q}_5 \otimes \mathcal{Q}_4$ looks like

$$
\frac{1}{\sqrt{3}}V(I,Z)\boldsymbol{\rho}_1 \otimes \left(\frac{2e}{3}|0\rangle\langle0| + \frac{1}{6}|1\rangle\langle1| \right) + \frac{1}{\sqrt{3}}V(I,Z)\boldsymbol{\rho}_1 \otimes \left(\frac{f}{3}|0\rangle\langle1| + \frac{g}{3}|1\rangle\langle0| \right)
$$

$$
+ \frac{1}{2\sqrt{3}}V(I,X;I,Y;+)\boldsymbol{\rho}_1 \otimes \frac{1}{6}|1\rangle\langle0| + \frac{1}{2\sqrt{3}}V(I,X;I,Y;+) \otimes \frac{f}{3}\boldsymbol{I}
$$

$$
+ \frac{1}{2\sqrt{3}}V(I,X;I,Y;-)\boldsymbol{\rho}_1 \otimes \frac{1}{6}|0\rangle\langle1| + \frac{1}{2\sqrt{3}}V(I,X;I,Y;-) \otimes \frac{g}{3}\boldsymbol{I}
$$

$$
+ \frac{1}{\sqrt{3}}V(X,Y)\boldsymbol{\rho}_1 \otimes \left(\frac{1}{6}|0\rangle\langle0| + \frac{2h}{3}|1\rangle\langle1| \right) + \frac{1}{\sqrt{3}}V(X,Y)\boldsymbol{\rho}_1 \otimes \left(\frac{f}{3}|0\rangle\langle1| + \frac{g}{3}|1\rangle\langle0| \right), \quad (3)
$$

where $V(I,X;I,Y;\pm)\boldsymbol{\rho} = V(I,X)\boldsymbol{\rho} - V(Y,Z)\boldsymbol{\rho} \pm \imath(V(I,Y)\boldsymbol{\rho} - V(Z,X)\boldsymbol{\rho})$, and the terms such that the state of $\mathcal{Q}_5$ is $\frac{\boldsymbol{I}}{2}$ are omitted.

We next transform the state of $\mathcal{Q}_5 \otimes \mathcal{Q}_4$ to $\boldsymbol{\rho}_{out}^1$ by using Lemma 3.8 again. For example, $V(I,Z)\boldsymbol{\rho}_1 \otimes |0\rangle\langle0|$ is transformed to $\frac{1}{\sqrt{3}}V(I,Z)V(I,Z)\boldsymbol{\rho}_1$. To simplify the resulting formula, the following lemma is used (see Appendix for its proof).

8

Lemma 3.9 1) $V(I,Z)V(I,Z)\boldsymbol{\rho}_1 = V(X,Y)V(X,Y)\boldsymbol{\rho}_1 = \begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix}$.

2) $V(I,Z)V(X,Y)\boldsymbol{\rho}_1 = V(X,Y)V(I,Z)\boldsymbol{\rho}_1 = \begin{pmatrix} d & 0 \\ 0 & a \end{pmatrix}$.

3) $V(I,X)V(I,X)\boldsymbol{\rho}_1 = V(Y,Z)V(Y,Z)\boldsymbol{\rho}_1 = \begin{pmatrix} \frac{1}{2} & \frac{b+c}{2} \\ \frac{b+c}{2} & \frac{1}{2} \end{pmatrix}$.

4) $V(I,X)V(Y,Z)\boldsymbol{\rho}_1 = V(Y,Z)V(I,X)\boldsymbol{\rho}_1 = \begin{pmatrix} \frac{1}{2} & -\frac{b+c}{2} \\ -\frac{b+c}{2} & \frac{1}{2} \end{pmatrix}$.

5) $V(I,Y)V(I,Y)\boldsymbol{\rho}_1 = V(Z,X)V(Z,X)\boldsymbol{\rho}_1 = \begin{pmatrix} \frac{1}{2} & \frac{b-c}{2} \\ \frac{c-b}{2} & \frac{1}{2} \end{pmatrix}$.

6) $V(I,Y)V(Z,X)\boldsymbol{\rho}_1 = V(Z,X)V(I,Y)\boldsymbol{\rho}_1 = \begin{pmatrix} \frac{1}{2} & \frac{c-b}{2} \\ \frac{b-c}{2} & \frac{1}{2} \end{pmatrix}$.

7) *For any two operators V, V' taken from any different two sets of $\{V(I,Z), V(X,Y)\}$, $\{V(I,X), V(Y,Z)\}$, and $\{V(I,Y), V(Z,X)\}$, $VV'\boldsymbol{\rho}_1 = \frac{\boldsymbol{I}}{2}$.*

Now it is a routine calculation (see Appendix for its sequence) to obtain $\boldsymbol{\rho}_{out}^1 = \begin{pmatrix} m_1 & m_2 \\ m_3 & m_4 \end{pmatrix}$ where m_1 through m_4 are equations using a, b, c and d (e, f, g and h disappear). Using the fact that $a + d = 1$, we have $\boldsymbol{\rho}_{out}^1 = \frac{1}{9}\boldsymbol{\rho}_1 + \frac{1}{9}\boldsymbol{I}$. Recovering the completely mixed state omitted in our analysis, we obtain $C_4[\boldsymbol{\rho}_2] \circ C_2[\boldsymbol{\rho}_2](\boldsymbol{\rho}_1) = \frac{1}{9}\boldsymbol{\rho}_1 + \frac{8}{9} \cdot \frac{\boldsymbol{I}}{2}$. Thus, the map is $\frac{1}{9}$-shrinking. □

Computing the Fidelity at Node t_2. By analyzing the quality of the path from s_2 to t_2, we have $F(|\psi_2\rangle, \boldsymbol{\rho}_{out}^2) \geq 1/2 + 2\sqrt{3}/243$. Its analysis is different from the previous one by the antisymmetry of the protocol. Details are given in Appendix.

3.4 Upper Bounds

The following theorem shows a general upper bound for the fidelity of crossing two qubits over Butterfly. Recall that we showed in Sec. 1 (also Fig. 3) that the operation at s_0 must not resemble a controlled unitary operation. Thus, it must be a more general TP-CP map (unitary operation with some ancillae). The basic idea of the proof is by showing that a good TP-CP map, the one which results in the protocol with fidelity close to 1.0, can be "approximated" by a controlled unitary operation. Hence, the fidelity of sending two qubits over Butterfly must be bounded away from 1.0. Similar to the proof of Theorem 2.1, we use a geometric view of the TP-CP map on the Bloch ball. However, it is much complicated since we have to consider the side links. See Appendix for details (whose technique is similar to Theorem 4.2 of the next section which the reader is recommended to read first.).

Theorem 3.10 *Let q be the fidelity of a protocol for crossing two qubits simultaneously. Then, $q < 0.983$.*

4 Protocol for Crossing a Qubit and a Bit

In this section, we consider the case where one of two sources (say, at s_2) is a classical bit. Under this situation, we can design a protocol, called as XQC (crossing a quantum bit and a classical bit), whose fidelity is much better than XQQ (see Appendix for details). The protocol is summarized in Fig. 6, where $M[B_z](\mathcal{Q})$ means that $\mathcal{Q}$ is measured in the basis $B_z = \{|0\rangle, |1\rangle\}$. (Similar notations are also used for bases $B_x = \{|+\rangle, |-\rangle\}$ and $B_y = \{|+'\rangle, |-'\rangle\}$ later.)
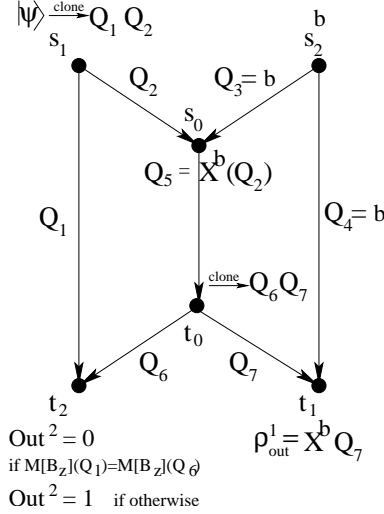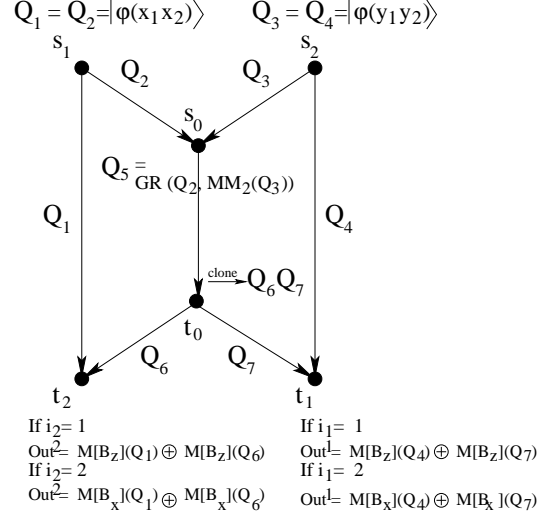
Figure 6 (Protocol XQC):

$|\psi\rangle \xrightarrow[s_1]{\text{clone}} Q_1 Q_2$ b at s_2

Q_2 $Q_3 = b$

s_0

$Q_5 = X^b(Q_2)$

Q_1 $Q_4 = b$

$\xrightarrow{\text{clone}} Q_6 Q_7$

t_0

Q_6 Q_7

t_2 t_1

$\text{Out}^2 = 0$ $\rho^1_{out} = X^b Q_7$

if $M[B_z](Q_1) = M[B_z](Q_0)$

$\text{Out}^2 = 1$ if otherwise

Figure 6: Protocol XQC

Figure 7 (Protocol X2C2C):

$Q_1 = Q_2 = |\varphi(x_1 x_2)\rangle$ $Q_3 = Q_4 = |\varphi(y_1 y_2)\rangle$

s_1 s_2

Q_2 Q_3

s_0

$Q_5 = \text{GR}(Q_2, MM_2(Q_3))$

Q_1 Q_4

$\xrightarrow{\text{clone}} Q_6 Q_7$

t_0

Q_6 Q_7

t_2 t_1

If $i_2 = 1$ If $i_1 = 1$

$\text{Out}^2 = M[B_z](Q_1) \oplus M[B_z](Q_6)$ $\text{Out}^1 = M[B_z](Q_4) \oplus M[B_z](Q_7)$

If $i_2 = 2$ If $i_1 = 2$

$\text{Out}^2 = M[B_x](Q_1) \oplus M[B_x](Q_6)$ $\text{Out}^1 = M[B_x](Q_4) \oplus M[B_x](Q_7)$

Figure 7: Protocol $X2C2C$

Theorem 4.1 *XQC achieves the fidelities of* $13/18$ *and* $11/18$ *at* t_1 *and* t_2. *(By averaging the fidelities at both sinks as before, we can also have a protocol whose fidelities are the same* $2/3$ *at* t_1 *and* t_2.)

On the contrary, assuming that the copies of the bit at s_2 are sent to s_0 and t_1, we can obtain an upper bound that is significantly better than Theorem 3.10. In general, this assumption, denoted as the *BC (bit-copy) assumption*, is reasonable since whenever we need to send a bit to multiple nodes in the network, simply sending its (classical) copies does not appear to cause disadvantages.

Theorem 4.2 *Let* p *be the fidelity of a protocol for crossing a bit and a qubit under the BC assumption. Then,* $p < 11/12$.

Proof. Suppose that there is a protocol whose fidelity is $1 - \epsilon$, and we wish to show $\epsilon > 1/12$. Here, we give the desired upper bound for the case that the capacity of the link from s_1 to t_2 is unlimited. In this case we can assume that the state sent from s_1 is pure. Let $|\psi\rangle$ and b be the inputs at nodes s_1 and s_2, respectively. By the Schmidt decomposition (see [25]), the state after the operation at s_1 is written as $|\xi\rangle = \alpha|\psi_2\rangle|\psi_1\rangle + \beta|\psi_2^\perp\rangle|\psi_1^\perp\rangle$ where $|\psi_1\rangle$ and $|\psi_1^\perp\rangle$ are single-qubit orthonormal states on the link to s_0 and $|\psi_2\rangle$ and $|\psi_2^\perp\rangle$ are the remaining (possibly multi-qubit) orthonormal states on the link to t_2. Note that $\alpha, \beta, |\psi_2\rangle$ and $|\psi_1\rangle$ depend on the input $|\psi\rangle$ at s_1. Without loss of generality, we assume $|\alpha| \geq |\beta|$ (and hence $|\beta|^2 \leq 1/2$).

We first investigate the fidelity on the path from s_1 to t_1, which is done by the following sequence of definitions and observations: (i) By the above definition of $|\xi\rangle$, we can write the state on $\mathcal{Q}_2$ (where we use the notations in Fig. 6 again) as $\boldsymbol{\rho} = |\alpha|^2|\psi_1\rangle\langle\psi_1| + |\beta|^2|\psi_1^\perp\rangle\langle\psi_1^\perp|$. (ii) Intuitively, the value of $|\beta|$ shows the strength of entanglement between $\mathcal{Q}_1$ and $\mathcal{Q}_2$; if it is large then the distortion of $\boldsymbol{\rho}$ compared to the original $|\xi\rangle$ must also be large. In other words, β must be small to obtain a small ϵ. (iii) For $b = 0$ and 1, let $C_b : \mathcal{Q}_2 \to \mathcal{Q}_5$ be the TP-CP map at s_0. Let C_b' be the corresponding affine map on Bloch-sphere states. Namely, C_b' maps a Bloch vector $\vec{r}$ to $O_b^1 \Lambda_b O_b^2 \vec{r} + \vec{d_b}$, where O_b^1 and O_b^2 are orthogonal matrices with determinant 1, and Λ_b is a diagonal matrix (see [12, 27]). (iv) Let U_b' be the map that transforms $\vec{r}$ to $O_b^1 O_b^2 \vec{r}$. Then, we can define the map U_b such that its Bloch-sphere correspondence is U_b'. Note that U_b is unitary. (v) Let k_b be the distance between the images of the Bloch ball by C_b' and U_b'. Note that $||(C_b - U_b)|\phi\rangle\langle\phi|||_{tr} \leq k_b$ for

10

an arbitrary pure state $|\phi\rangle$ (where the trace norm $||\cdot||_{tr}$ is defined by $||A||_{tr} = \sqrt{AA^\dagger}$). By a similar reason as (ii) k_b must be small for a small ϵ. (vi) Now we select the state ρ which is undesirable to achieve a high fidelity, i.e., the one such that $U_0\rho = U_1\rho$ (such ρ exists, which is parallel to the eigenvector of $U_0^{-1}U_1$). Let $\rho' = |\alpha|^2|\psi_1\rangle\langle\psi_1|$, which is an approximation of ρ represented as a product state. (vii) The operation at t_0 is considered to be the two TP-CP maps on the one qubits: One map CP_1 is for t_1 and the other CP_2 is for t_2. Their Bloch-sphere correspondence CP_1' and CP_2' have a trade-off on the size of their images. So, the image of CP_1' must be large for a small ϵ, and then we have a shrinking factor for CP_2'.

Now we are ready to bound both above and below $||(C_0 - C_1)\rho'||_{tr}$, which produces an inequality on ϵ as will be seen soon. For this purpose, we first evaluate the values of β and k_b using geometric properties of the Bloch sphere representation of the TP-CP map on the one qubits: it maps the Bloch ball to an ellipsoid within the Bloch ball. The proof of this technical lemma is given in Appendix.

Lemma 4.3 $|\beta|^2 \leq \frac{1}{2}f(\epsilon)$ and $k_b \leq f(\epsilon)$ where $f(\epsilon) = \frac{3}{2} + \epsilon - \sqrt{\frac{9}{4} + \epsilon^2 - 5\epsilon}$.

Second, we decompose $||(C_0 - C_1)\rho'||_{tr}$ as follows by the triangle inequality, and then bound it from above:

$$
\begin{aligned}
||(C_0 - C_1)\rho'||_{tr} &\leq ||(C_0 - U_0)\rho'||_{tr} + ||U_0\rho' - U_0\rho||_{tr} + ||U_1\rho - U_1\rho'||_{tr} + ||(U_1 - C_1)\rho'||_{tr} \\
&\leq |\alpha|^2 \cdot k_0 + ||\rho - \rho'||_{tr} \times 2 + |\alpha|^2 \cdot k_1 \\
&\leq (k_0 + k_1)|\alpha|^2 + 2|\beta|^2.
\end{aligned}
\tag{4}
$$

Third, for the shrinking factor by the operation at t_0 the following lemma from [26] is used.

Lemma 4.4 (Niu-Griffiths) Let CP_i' be the Bloch sphere representation of CP_i. Let l_1 be the shortest semiaxis length of the image of CP_1', and l_2 be the longest semiaxis length of the image of CP_2'. Then, $l_1 \leq \sqrt{1 - l_2^2}$.

Since $l_1 \geq 1 - 2\epsilon$ by the fidelity requirement at t_1, Lemma 4.4 gives us the condition for l_2:

$$
l_2 \leq 2\sqrt{\epsilon - \epsilon^2}.
\tag{5}
$$

Finally, we bound $||(C_0 - C_1)\rho'||_{tr}$ from below by focusing on the path s_2-t_2. Let M be the TP-CP map done at t_2, and $D = M(I \otimes CP_2)(I \otimes C_0 - I \otimes C_1)$. By the fidelity requirement at t_2, $||D|\xi\rangle\langle\xi|||_{tr} \geq 2 - 4\epsilon$ [2]. On the contrary, using the unnormalized product state $|\chi\rangle = \alpha|\psi_2\rangle|\psi_1\rangle$ we bound $||D|\xi\rangle\langle\xi|||_{tr}$ by

$$
||D|\xi\rangle\langle\xi|||_{tr} \leq ||D(|\xi\rangle\langle\xi| - |\chi\rangle\langle\chi|)||_{tr} + ||D|\chi\rangle\langle\chi|||_{tr}.
$$

The first term is bounded by $2|||\xi\rangle\langle\xi| - |\chi\rangle\langle\chi|||_{tr}$ since D is the difference between two TP-CP maps, each of which has the operator norm at most 1 [2]. Using the monotone decreasing property of the trace distance between two states by TP-CP maps, the second term is bounded by

$$
||D|\chi\rangle\langle\chi|||_{tr} \leq ||(I \otimes (CP_2 \cdot (C_0 - C_1)))|\psi_2\rangle\langle\psi_2| \otimes \rho'||_{tr} = ||(CP_2 \cdot (C_0 - C_1))\rho'||_{tr},
$$

which is at most $l_2||(C_0 - C_1)\rho'||_{tr}$ since CP_2' maps the Bloch ball to an ellipsoid within a ball with radius at most l_2. By a simple calculation of the trace norm, we have the following bound.

Lemma 4.5 $|||\xi\rangle\langle\xi| - |\chi\rangle\langle\chi|||_{tr} \leq 2|\beta|\sqrt{1 - |\beta|^2/2}$.
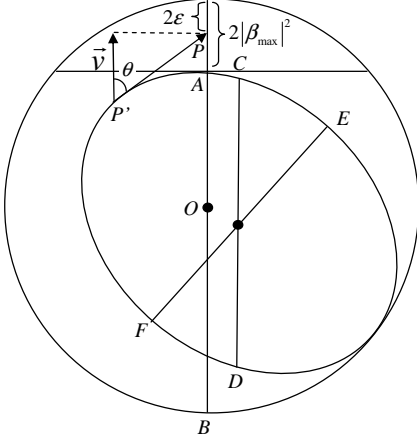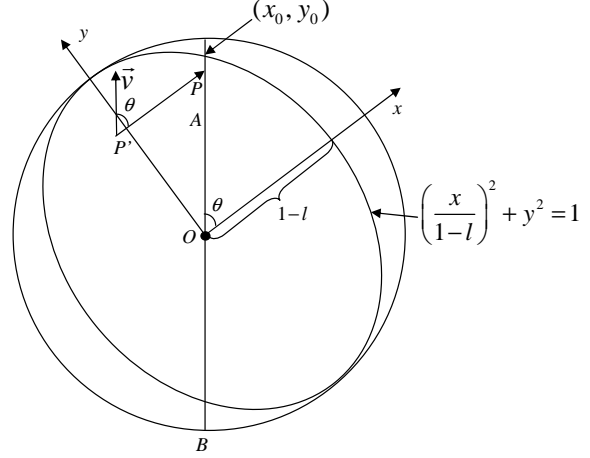
Figure 8: Image by the operation at s_1

Figure 9: Image by operations at s_0, t_0 and t_1

By Lemma 4.5 we have

$$2 - 4\epsilon \leq 2\||\xi\rangle\langle\xi| - |\chi\rangle\langle\chi|\|_{tr} + l_2\|(C_0 - C_1)\boldsymbol{\rho'}\|_{tr} \leq 2|\beta|\sqrt{1 - |\beta|^2/2} + l_2\|(C_0 - C_1)\boldsymbol{\rho'}\|_{tr}. \quad (6)$$

By Lemma 4.3, Ineqs.(4), (5) and (6), we produce an inequality on ϵ and $|\beta|$:

$$1 - 2\epsilon \leq 2|\beta|\sqrt{1 - |\beta|^2/2} + 2\sqrt{\epsilon - \epsilon^2}\left((1 - |\beta|^2)f(\epsilon) + |\beta|^2\right). \quad (7)$$

(Recall that $|\alpha|^2 = 1 - |\beta|^2$.) Note that the right-hand side of Ineq. (7) is monotone increasing on ϵ and $|\beta|$ while its left-hand side is monotone decreasing on ϵ. Therefore, by checking ϵ such that Ineq. (7) holds under the bound of $|\beta|$ from Lemma 4.3, we obtain $\epsilon > 1/12$.

It still remains to prove Lemma 4.3.

Proof of Lemma 4.3. We only prove the bound of $|\beta|$ since the bound of k_b is similarly shown.

Let β_{max} be the maximum of all β's when $|\psi\rangle$ varies on the pure qubits. Considering the Bloch sphere representation, the point A corresponding to $\boldsymbol{\rho}$ is on the circle of radius $1 - 2|\beta_{max}|^2$ since $\boldsymbol{\rho} = (1 - 2|\beta_{max}|^2)|\psi_1\rangle\langle\psi_1| + 2|\beta_{max}|^2 \cdot \frac{I}{2}$. Note that the image of the Bloch ball by the operation at s_1 is an ellipsoid whose cut CD parallel to segment AO has length $\leq 2 - 2|\beta_{max}|^2$ (see Fig. 8), where O is the center of the Bloch ball. Then, by geometric properties of the ellipsoid we can show the following lemma.

Claim 1 *After the operation at t_1, this cut is shrunk by a factor at least $1 - 2|\beta_{max}|^2 + 2\epsilon$.*

Proof. See Fig. 8 again. Let P be the point on the line AB such that the length of segment PO is $1 - 2\epsilon$. To satisfy the fidelity at t_1, some point P' in the image at s_0 must reach P in the final image at t_1. Letting l be the length of $\overrightarrow{P'P}$, this means that the composite map by operations at s_0, t_0 and t_1 shrinks the Bloch ball by a factor of $1 - l$ to the direction of $\overrightarrow{P'P}$ since any TP-CP map must transform the Bloch ball to an ellipsoid inside the ball. Let $\vec{v}$ be the component of $\overrightarrow{P'P}$ parallel to the line AB. Note that the length of $\vec{v}$ is at least $(1 - 2\epsilon) - (1 - 2|\beta_{max}|^2) = 2|\beta_{max}|^2 - 2\epsilon$. Now we analyze the maximum of the shrinking factor of the Bloch ball to the direction of AB since it is the worst case for our analysis. Since we want to know the maximum, we can assume that the length of $\vec{v}$ is exactly $2|\beta_{max}|^2 - 2\epsilon$. Then, the angle θ between $\overrightarrow{P'P}$ and $\vec{v}$ satisfies $\cos\theta = \frac{2|\beta_{max}|^2 - 2\epsilon}{l}$. Notice that the ellipse $(\frac{x}{1-l})^2 + y^2 = 1$ (Fig. 9) is obtained by the projection of the final image to

the plane including all the vectors we are considering. (Here, we assume that the plane has x-y coordinates. Note that the x-axis is the direction parallel to $\overrightarrow{P'P}$.) Let (x_0, y_0) be the intersection of the ellipse and the line $y = (\tan\theta)x$. We can see that $\sqrt{x_0^2 + y_0^2}$ is the shrinking factor we want. By a simple calculation, this value is

$$\sqrt{x_0^2 + y_0^2} = \sqrt{(1 + \tan^2\theta)\frac{1}{(\frac{1}{1-l})^2 + \tan^2\theta}} = \sqrt{\frac{l(1-l)^2}{2|\beta_{max}|^2 - 2\epsilon + (1-l)^2(l - 2|\beta_{max}|^2 + 2\epsilon)}},$$

which is monotone decreasing as the function of l (when $l \leq 1$). Since $l \geq 2|\beta_{max}|^2 - 2\epsilon$, the maximum value is obtained when $l = 2|\beta_{max}|^2 - 2\epsilon$ and it is $1 - 2|\beta_{max}|^2 + 2\epsilon$. □

After the operation at t_1, the distance between the Bloch sphere and its image by the operations along the s_1-t_1 line must be at most 2ϵ to satisfy the fidelity requirement at t_1. Thus, the shortest semiaxis length of the final image of all transformations on the s_1-t_1 line must be at least $1 - 2\epsilon$. On the contrary, Lemma 1 implies that the shortest semiaxis length is at most $(1 - |\beta_{max}|^2)(1 - 2|\beta_{max}|^2 + 2\epsilon)$. Hence, $1 - 2\epsilon \leq (1 - |\beta_{max}|^2)(1 - 2|\beta_{max}|^2 + 2\epsilon)$, and we obtain $|\beta_{max}|^2 \leq \frac{1}{2}\left(\frac{3}{2} + \epsilon - \sqrt{\frac{9}{4} + \epsilon^2 - 5\epsilon}\right)$. By the definition of β_{max} we also have the same bound on $|\beta|^2$ for any β corresponding to an input at s_1. □

Now the proof of Theorem 4.2 is completed. □

5 Protocols for Crossing Two Multiple Bits

In this section, we consider the case that both sources are restricted to be one of the four $(2, 1, 0.85)$-quantum random access (QRA) coding states [4]. Note that (m, n, p)-QRA coding is the coding of m bits to n qubits such that any one bit chosen from the m bits is recovered with probability at least p. In this case, we can achieve a much better fidelity. As an application, we can consider a more interesting problem where each source node receives two classical bits, namely, $x_1 x_2 \in \{0, 1\}^2$ at s_1, and $y_1 y_2 \in \{0, 1\}^2$ at s_2. At node t_1, we output one classical bit Out^1 and similarly Out^2 at t_2. Now an adversary chooses two numbers $i_1, i_2 \in \{1, 2\}$. Our protocol can use the information of i_1 only at node t_1 and that of i_2 only at t_2. Our goal is to maximize $F(x_{i_1}, \text{Out}^1)$ and $F(y_{i_2}, \text{Out}^2)$, where $F(x_{i_1}, \text{Out}^1)$ turns out to be the probability that $x_{i_1} = \text{Out}^1$ and similarly for $F(y_{i_2}, \text{Out}^2)$. Fig. 7 illustrates $X2C2C$ whose key is also on how to encode at s_0: it uses measurement MM_2 to estimate which QRA coding state is sent from s_2, and the group operation similar to XQQ. For optimal cloning at t_0, it uses the phase-covariant cloning [8, 11]. Its details are given in Appendix.

Theorem 5.1 $X2C2C$ achieves a fidelity of $1/2 + \sqrt{2}/16$ at both t_1 and t_2.

By contrast, any classical protocol cannot achieve a success probability greater than $1/2$ for the following reason: Let fix $y_1 = y_2 = 0$. Then the path from s_1 to t_1 is obviously equivalent to the $(2, 1, p)$-classical random access coding, where the success probability p is at most $1/2$ [4].

Extending $X2C2C$, we can also solve the above problem with probability $> 1/2$ for the case when each source node receives three bits. The protocol is denoted as $X3C3C$ whose details are given in Appendix. In particular, $X3C3C$ needs eight different operations instead of four in $X2C2C$. In addition to the Pauli operations, it uses an approximation of the universal NOT gate [10, 13], which maps a point within the Bloch sphere into its antipodes.

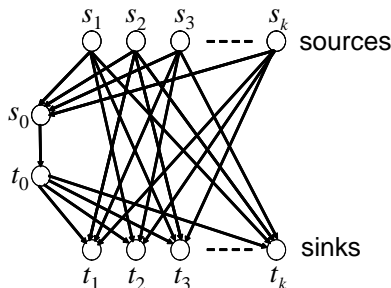**Theorem 5.2** $X3C3C$ achieves a fidelity of $1/2 + 2/81$ at both sinks.

Figure 10: Network G_k

Interestingly, there is no $X4C4C$, which is an immediate corollary of the nonexistence of $(4, 1, p > 1/2)$-QRA coding [17].

Theorem 5.3 *If an $X4C4C$ protocol achieves fidelity q, then $q \leq 1/2$.*

6   Beyond the Butterfly Network – Concluding Remarks –

Obviously a lot of future work remains. First of all, there is a large gap between the current upper and lower bounds for the achievable fidelity, which should be narrowed. Equally important is to consider more general networks. To this direction, it might be interesting to study the network G_k as shown in Fig. 10, introduced in [14]. Note that there are k source-sink pairs (s_i, t_i) all of which share a single link from s_0 to t_0. For this network G_k, we can design the protocol XQ^k by a simple extension of XQQ. The idea is to decompose the node s_0 (similarly for t_0) into a sequence of nodes of indegree two. At each of those nodes, we do exactly the same thing as before, i.e., encoding one state by the classical two bits obtained from the other state. It is not hard to see that such a protocol achieves a fidelity strictly better than $1/2$.

References

[1] M. Adler, N. J. Harvey, K. Jain, R. D. Kleinberg, and A. R. Lehman. On the capacity of information networks. *Proc. 17th ACM-SIAM SODA*, pp.241–250, 2006.

[2] D. Aharonov, A. Kitaev, and N. Nisan. Quantum circuits with mixed states. *Proc. 30th ACM STOC*, pp. 20–30, 1998.

[3] R. Ahlswede, N. Cai, S.-Y. R. Li, and R. W. Yeung. Network information flow. *IEEE Transactions on Information Theory* **46** (2000) 1204–1216.

[4] A. Ambainis, A. Nayak, A. Ta-shma, and U. Vazirani. Dense quantum coding and quantum finite automata. *J. ACM* **49** (2002) 496–511.

[5] C. H. Bennett and G. Brassard. Quantum cryptography: public key distribution and coin tossing. *Proc. IEEE International Conference on Computers, Systems and Signal Processing*, pp. 175–179, 1984.

[6] C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, and W. K. Wootters. Teleporting an unknown quantum states via dual classical and Einstein-Podolsky-Rosen channels. *Phys. Rev. Lett.* **70** (1993) 1895–1899.

[7] C. H. Bennett and S. J. Wiesner. Communication via one- and two-particle operators on Einstein-Podolsky-Rosen states. *Phys. Rev. Lett.* **69** (1992) 2881–2884.

[8] D. Bruß, M. Cinchetti, G. M. D'Ariano, and C. Macchiavello. Phase-covariant quantum cloning. *Phys. Rev. A* **62** (2000) 012302.

[9] V. Bužek and M. Hillery. Quantum copying: Beyond the no-cloning theorem. *Phys. Rev. A* **54** (1996) 1844–1852.

[10] V. Bužek, M. Hillery, and R. F. Werner. Optimal manipulation with qubits: universal NOT gate. *Phys. Rev. A* **60** (1999) 2626–2629.

[11] H. Fan, K. Matsumoto, X.-B. Wang, and H. Imai. Phase-covariant quantum cloning. *J. Phys. A: Math. Gen.* **35** (2002) 7415–7423.

[12] A. Fujiwara and P. Algoet. One-to-one parametrization of quantum channels. *Phys. Rev. A* **59** (1999) 3290–3294.

[13] N. Gisin and S. Popescu. Spin flips and quantum information for antiparallel spins. *Phys. Rev. Lett.* **83** (1999) 432–435.

[14] N. J. Harvey, R. D. Kleinberg, and A. R. Lehman. Comparing network coding with multicommodity flow for the k-pairs communication problem. MIT LCS Technical Report 964, September 2004.

[15] N. J. Harvey, D. R. Karger, and K. Murota. Deterministic network coding by matrix completion. *Proc. 16th ACM-SIAM SODA*, pp. 489–498, 2005.

[16] M. Hayashi, K. Iwama, H. Nishimura, R. Raymond, and S. Yamashita. Quantum network coding. Talk at *9th Workshop on Quantum Information Processing*, 2006. Preprint available at quant-ph/0601088, January 2006.

[17] M. Hayashi, K. Iwama, H. Nishimura, R. Raymond, and S. Yamashita. $(4,1)$-quantum random access coding does not exist. *New J. Phys.* **8** (2006) 129.

[18] P. Høyer and R. de Wolf. Improved quantum communication complexity bounds for disjointness and equality. *Proc. 19th STACS, Lecture Notes in Comput. Sci.* **2285** (2002) 299–310.

[19] S. Jaggi, P. Sanders, P. A. Chou, M. Effros, S. Egner, K. Jain, and L. M. G. M. Tolhuizen. Polynomial time algorithms for multicast network code construction. *IEEE Transactions on Information Theory* **51** (2005) 1973–1982.

[20] R. Koetter. Network coding home page. http://tesla.csl.uiuc.edu/˜koetter/NWC/

[21] A. R. Lehman and E. Lehman. Complexity classification of network information flow problems. *Proc. 15th ACM-SIAM SODA*, pp. 142–150, 2004.

[22] A. R. Lehman and E. Lehman. Network coding: does the model need tuning? *Proc. 16th ACM-SIAM SODA*, pp. 499–504, 2005.

[23] D. Leung, J. Oppenheim, and A. Winter. Quantum network communication –the butterfly and beyond. Preprint available at quant-ph/0608233, August 2006.

[24] A. Nayak. Optimal lower bounds for quantum automata and random access codes. *Proc. 40th IEEE FOCS*, pp. 369–376, 1999.

[25] M. A. Nielsen and I. L. Chuang. *Quantum Computation and Quantum Information*, Cambridge, 2000.

[26] C.-S. Niu and R. B. Griffiths. Optimal copying of one quantum bit. *Phys. Rev. A* **58** (1998) 4377–4393.

[27] M. B. Ruskai, S. Szarek, and E. Werner. An analysis of complete-positive trace-preserving maps on 2×2 matrices. *Lin. Alg. Appl.* **347** (2002) 159–187.

[28] B. Schumacher. Quantum coding. *Phys. Rev. A* **51** (1995) 2738–2747.

[29] Y. Shi and E. Soljanin. On multicast in quantum network. *Proc. 40th Annual Conference on Information Sciences and Systems*, 2006.

[30] P. Shor. Scheme for reducing decoherence in quantum computer memory. *Phys. Rev. A* **52** (1995) 2493–2496.

[31] S. Wehner and R. de Wolf. Improved lower bounds for locally decodable codes and private information retrieval. *Proc. 32nd ICALP, Lecture Notes in Comput. Sci.* **3580** (2005) 1424–1436.

A   Appendix

A.1   Proofs of Lemmas in Sec. 3.3

Proof of Lemma 3.8.   Consider the tetra measurement as a TP-CP map. For any mixed state $\boldsymbol{\rho}$, its TP-CP map, also denoted by TTR, transforms $\boldsymbol{\rho}$ to

$$\mathrm{Tr}\left[\frac{1}{2}|\chi(00)\rangle\langle\chi(00)|\boldsymbol{\rho}\right]|00\rangle\langle00| + \mathrm{Tr}\left[\frac{1}{2}|\chi(01)\rangle\langle\chi(01)|\boldsymbol{\rho}\right]|01\rangle\langle01|$$

$$+ \mathrm{Tr}\left[\frac{1}{2}|\chi(10)\rangle\langle\chi(10)|\boldsymbol{\rho}\right]|10\rangle\langle10| + \mathrm{Tr}\left[\frac{1}{2}|\chi(11)\rangle\langle\chi(11)|\boldsymbol{\rho}\right]|11\rangle\langle11|. \tag{8}$$

By linearity, TTR is defined by the map that transforms each basis matrix $|b\rangle\langle b'|$ $(b, b' = 0, 1)$ to the matrix obtained by replacing $\boldsymbol{\rho}$ in Eq.(8) by $|b\rangle\langle b'|$. Using the definition of the states $|\chi(00)\rangle, \ldots, |\chi(11)\rangle$ we obtain

$$TTR(|0\rangle\langle0|) = \frac{1}{2}(\cos^2\tilde{\theta}(|00\rangle\langle00| + |01\rangle\langle01|) + \sin^2\tilde{\theta}(|10\rangle\langle10| + |11\rangle\langle11|))$$

$$= 2\sin^2\tilde{\theta}\left(\frac{\boldsymbol{I}}{2}\otimes\frac{\boldsymbol{I}}{2}\right) + (\cos^2\tilde{\theta} - \sin^2\tilde{\theta})\left(|0\rangle\langle0|\otimes\frac{\boldsymbol{I}}{2}\right)$$

$$= \frac{1}{\sqrt{3}}\left(|0\rangle\langle0|\otimes\frac{\boldsymbol{I}}{2}\right) + \left(1 - \frac{1}{\sqrt{3}}\right)\left(\frac{\boldsymbol{I}}{2}\otimes\frac{\boldsymbol{I}}{2}\right). \tag{9}$$

Similarly, we can check that

$$TTR(|1\rangle\langle1|) = \frac{1}{\sqrt{3}}\left(|1\rangle\langle1|\otimes\frac{\boldsymbol{I}}{2}\right) + \left(1 - \frac{1}{\sqrt{3}}\right)\left(\frac{\boldsymbol{I}}{2}\otimes\frac{\boldsymbol{I}}{2}\right), \tag{10}$$

$$TTR(|0\rangle\langle1|) = \frac{1}{4\sqrt{3}}((|00\rangle\langle00| + |10\rangle\langle10| - |11\rangle\langle11| - |01\rangle\langle01|)$$

$$+ \imath(|00\rangle\langle00| + |11\rangle\langle11| - |01\rangle\langle01| - |10\rangle\langle10|)) \tag{11}$$

$$TTR(|1\rangle\langle0|) = TTR(|0\rangle\langle1|)^\dagger. \tag{12}$$

Now we consider the TP-CP map of $GR(\mathcal{Q}, TTR(\mathcal{Q}'))$. Assume that the state of $\mathcal{Q}$ is $\boldsymbol{\rho}$. Recall that $GR(\boldsymbol{\rho}, |00\rangle\langle00|) = \boldsymbol{\rho}$, $GR(\boldsymbol{\rho}, |01\rangle\langle01|) = Z\boldsymbol{\rho}$, $GR(\boldsymbol{\rho}, |10\rangle\langle10|) = X\boldsymbol{\rho}$, and $GR(\boldsymbol{\rho}, |11\rangle\langle11|) = Y\boldsymbol{\rho}$. If the GR operation under the two bits being selected uniformly at random, which means that the state of $TTR(\mathcal{Q}')$ is the state $\frac{\boldsymbol{I}}{2}\otimes\frac{\boldsymbol{I}}{2}$, is applied to $\boldsymbol{\rho}$, then $\boldsymbol{\rho}$ is mapped to $\frac{\boldsymbol{I}}{2}$ since the four GR operations are evenly applied to $\boldsymbol{\rho}$. Thus, Eqs.(9) and (10) imply that $GR(\cdot, TTR(\cdot))$ maps $\boldsymbol{\rho}\otimes|0\rangle\langle0|$ and $\boldsymbol{\rho}\otimes|1\rangle\langle1|$ to $\frac{1}{\sqrt{3}}\frac{I\boldsymbol{\rho}+Z\boldsymbol{\rho}}{2} + (1-\frac{1}{\sqrt{3}})\frac{\boldsymbol{I}}{2}$ and $\frac{1}{\sqrt{3}}\frac{X\boldsymbol{\rho}+Y\boldsymbol{\rho}}{2} + (1-\frac{1}{\sqrt{3}})\frac{\boldsymbol{I}}{2}$, respectively. Moreover, by Eq.(11) $\boldsymbol{\rho}\otimes|0\rangle\langle1|$ is mapped to

$$\frac{1}{4\sqrt{3}}((I\boldsymbol{\rho} + X\boldsymbol{\rho}) - (Y\boldsymbol{\rho} + Z\boldsymbol{\rho}) + \imath((I\boldsymbol{\rho} + Y\boldsymbol{\rho}) - (Z\boldsymbol{\rho} + X\boldsymbol{\rho}))),$$

which is $\frac{1}{2\sqrt{3}}(V(I,X)\boldsymbol{\rho} - V(Y,Z)\boldsymbol{\rho} + \imath(V(I,Y)\boldsymbol{\rho} - V(Z,X)\boldsymbol{\rho}))$. By Eq.(12) it is clear that $\boldsymbol{\rho}\otimes|1\rangle\langle0|$ is mapped to $\frac{1}{2\sqrt{3}}(V(I,X)\boldsymbol{\rho} - V(Y,Z)\boldsymbol{\rho} - \imath(V(I,Y)\boldsymbol{\rho} - V(Z,X)\boldsymbol{\rho}))$.

Next, we show that $V(I, Z)$, which maps $\boldsymbol{\rho}$ to $\frac{1}{2}(I\boldsymbol{\rho}+Z\boldsymbol{\rho})$, is an $\boldsymbol{I}$-invariant TP-CP map (similarly shown for the other five operations). In fact, $V(I, Z)$ is a TP-CP map since it is implementable by the following operation: Choose a bit r uniformly at random, and apply Z to $\boldsymbol{\rho}$ if $r = 1$. Its $\boldsymbol{I}$-invariance comes from the fact that the Pauli operations are $\boldsymbol{I}$-invariant. $\qquad\square$

Proof of Lemma 3.9. Let $\boldsymbol{\rho} = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$. Then, we can check that

$$Z\boldsymbol{\rho} = \begin{pmatrix} a & -b \\ -c & d \end{pmatrix}, \quad X\boldsymbol{\rho} = \begin{pmatrix} d & c \\ b & a \end{pmatrix}, \quad Y\boldsymbol{\rho} = \begin{pmatrix} d & -c \\ -b & a \end{pmatrix}.$$

Thus, $V(I, Z)$ is the TP-CP map that maps $\boldsymbol{\rho}$ to $V(I, Z)\boldsymbol{\rho} = \begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix}$. Similarly, we can see that $V(X, Y)$, $V(I, X)$, $V(Y, Z)$, $V(I, Y)$, and $V(Z, X)$ are TP-CP maps that map $\boldsymbol{\rho}$ to $V(X, Y)\boldsymbol{\rho} = \begin{pmatrix} d & 0 \\ 0 & a \end{pmatrix}$, $V(I, X)\boldsymbol{\rho} = \begin{pmatrix} \frac{1}{2} & \frac{b+c}{2} \\ \frac{b+c}{2} & \frac{1}{2} \end{pmatrix}$, $V(Y, Z)\boldsymbol{\rho} = \begin{pmatrix} \frac{1}{2} & -\frac{b+c}{2} \\ -\frac{b+c}{2} & \frac{1}{2} \end{pmatrix}$, $V(I, Y)\boldsymbol{\rho} = \begin{pmatrix} \frac{1}{2} & \frac{b-c}{2} \\ \frac{c-b}{2} & \frac{1}{2} \end{pmatrix}$, and $V(Z, X)\boldsymbol{\rho} = \begin{pmatrix} \frac{1}{2} & \frac{c-b}{2} \\ \frac{b-c}{2} & \frac{1}{2} \end{pmatrix}$, respectively. Using these TP-CP maps, we can check that 1)-7) hold. $\qquad\square$

Calculation of $\boldsymbol{\rho}_{out}^1$. Here, we give the calculation to obtain $\boldsymbol{\rho}_{out}^1$ in Sec. 3.3. Recall the state on $\mathcal{Q}_5 \otimes \mathcal{Q}_4$ (Eq. (3)). Using Lemma 3.9(7) and Lemma 3.8, the state $\boldsymbol{\rho}_{out}^1$ is represented as

$$\left(\frac{1}{\sqrt{3}}\right)^2 \left(\frac{2e}{3} V(I, Z)V(I, Z)\boldsymbol{\rho}_1 + \frac{1}{6} V(X, Y)V(I, Z)\boldsymbol{\rho}_1\right)$$

$$+ \left(\frac{1}{2\sqrt{3}}\right)^2 \frac{1}{6} V(I, X; I, Y; -)V(I, X; I, Y; +)\boldsymbol{\rho}_1 + \left(\frac{1}{2\sqrt{3}}\right)^2 \frac{1}{6} V(I, X; I, Y; +)V(I, X; I, Y; -)\boldsymbol{\rho}_1$$

$$+ \left(\frac{1}{\sqrt{3}}\right)^2 \left(\frac{2h}{3} V(X, Y)V(X, Y)\boldsymbol{\rho}_1 + \frac{1}{6} V(I, Z)V(X, Y)\boldsymbol{\rho}_1\right), \tag{13}$$

where the terms $\frac{\boldsymbol{I}}{2}$ produced from the second, fourth, sixth, and eighth terms of Eq.(3) by Lemma 3.8(7) are omitted. Moreover, Eq.(13) is rewritten as follows using Lemma 3.8(1-2) for the first and last terms of Eq.(13) and Lemma 3.8(3-7) for the second and third terms of Eq.(13):

$$\frac{1}{3}\left[\frac{2e+2h}{3}\begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix} + \frac{1}{3}\begin{pmatrix} d & 0 \\ 0 & a \end{pmatrix}\right] + \frac{1}{12}\left[\frac{1}{6}\begin{pmatrix} \frac{1}{2} & \frac{b+c}{2} \\ \frac{b+c}{2} & \frac{1}{2} \end{pmatrix} \times 4 - \frac{1}{6}\begin{pmatrix} \frac{1}{2} & -\frac{b+c}{2} \\ -\frac{b+c}{2} & \frac{1}{2} \end{pmatrix} \times 4\right]$$

$$+ \frac{1}{12}\left[\frac{1}{6}\begin{pmatrix} \frac{1}{2} & \frac{b-c}{2} \\ \frac{c-b}{2} & \frac{1}{2} \end{pmatrix} \times 4 - \frac{1}{6}\begin{pmatrix} \frac{1}{2} & \frac{c-b}{2} \\ \frac{b-c}{2} & \frac{1}{2} \end{pmatrix} \times 4\right],$$

where the terms $\frac{\boldsymbol{I}}{2}$ produced by Lemma 3.8 are omitted. Using $e+h = a+d = 1$, the above formula is finally rewritten as $\frac{1}{9}\boldsymbol{\rho}_1 + \frac{1}{9}\boldsymbol{I}$.

A.2   Computing $F(|\psi_2\rangle, \boldsymbol{\rho}_{out}^2)$

We investigate the quality of the path from s_2 to t_2. Fix $\boldsymbol{\rho}_1 = |\psi_1\rangle\langle\psi_1|$ as an arbitrary state at node s_1, and consider four maps $D_1\colon |\psi_2\rangle \to \mathcal{Q}_3$, $D_2[\boldsymbol{\rho}_1]\colon \mathcal{Q}_3 \to \mathcal{Q}_5$, $D_3\colon \mathcal{Q}_5 \to \mathcal{Q}_6$ and $D_4[\boldsymbol{\rho}_1]\colon \mathcal{Q}_6 \to \boldsymbol{\rho}_{out}^2$. We wish to compute the fidelity of the composite map $D_{s_2t_2} = D_4[\boldsymbol{\rho}_1] \circ D_3 \circ D_2[\boldsymbol{\rho}_1] \circ D_1$.

Lemma A.1 $D_3 \circ D_2[\boldsymbol{\rho}_1] = D_2[\boldsymbol{\rho}_1] \circ D_3$.

Proof. As with Lemma 3.5, it suffices to show that $C^{(0)}$ is commutative with $D_2[\boldsymbol{\rho}_1]$. For this purpose, we prove that, for any qubit $\boldsymbol{\rho}$ and any matrix basis element $|b\rangle\langle b'|$ (where $b, b' \in \{0,1\}$) on $\mathcal{Q}_2$, $C^{(0)}(GR(|b\rangle\langle b'|, TTR(\boldsymbol{\rho}))) = GR(|b\rangle\langle b'|, TTR(C^{(0)}(\boldsymbol{\rho})))$. We first evaluate the left-hand side. Let T_{00} (resp. T_{01}, T_{10}, T_{11}) be the map that transforms $\boldsymbol{\rho}$ to $I\boldsymbol{\rho}I^\dagger$ (resp. $Z\boldsymbol{\rho}Z^\dagger$, $X\boldsymbol{\rho}X^\dagger$, $Y\boldsymbol{\rho}Y^\dagger$). Since $C^{(0)}$ is 0-shrinking,

$$
\begin{aligned}
C^{(0)}(GR(|b\rangle\langle b'|, TTR(\boldsymbol{\rho}))) &= C^{(0)}\left(\sum_{r \in \{0,1\}^2} \langle r|TTR(\boldsymbol{\rho})|r\rangle T_r(|b\rangle\langle b'|) \right) \\
&= \sum_{r \in \{0,1\}^2} \langle r|TTR(\boldsymbol{\rho})|r\rangle T_r \circ C^{(0)}(|b\rangle\langle b'|) = \begin{cases} \boldsymbol{O} & (\text{if } b \neq b') \\ \frac{\boldsymbol{I}}{2} & (\text{if } b = b'). \end{cases}
\end{aligned}
$$

Here, we used the commutativity between $C^{(0)}$ and the group operations for the second equality. Next, we evaluate the right-hand side:

$$
\begin{aligned}
GR(|b\rangle\langle b'|, TTR(C^{(0)}(\boldsymbol{\rho}))) &= \sum_{r \in \{0,1\}^2} \langle r|\frac{\boldsymbol{I}}{2} \otimes \frac{\boldsymbol{I}}{2}|r\rangle T_r(|b\rangle\langle b'|) \\
&= \frac{1}{4} \sum_{r \in \{0,1\}^2} T_r(|b\rangle\langle b'|) = \begin{cases} \boldsymbol{O} & (\text{if } b \neq b') \\ \frac{\boldsymbol{I}}{2} & (\text{if } b = b'). \end{cases}
\end{aligned}
$$

Here, the first equality is obtained since the tetra measurement for $\frac{\boldsymbol{I}}{2}$ gives two bits uniformly at random, and the third equality is obtained since $I|b\rangle\langle b'|I^\dagger + Z|b\rangle\langle b'|Z^\dagger + X|b\rangle\langle b'|X^\dagger + Y|b\rangle\langle b'|Y^\dagger$ is $2\boldsymbol{I}$ if $b = b'$, and $\boldsymbol{O}$ otherwise. □

Lemma A.2 (*Main Lemma*) $D_4[\boldsymbol{\rho}_1] \circ D_2[\boldsymbol{\rho}_1]$ *is* $\boldsymbol{I}$-*invariant and for any pure state* $|\psi_2\rangle$, $F(|\psi_2\rangle, D_4[\boldsymbol{\rho}_1] \circ D_2[\boldsymbol{\rho}_1](|\psi_2\rangle)) = 1/2 + \sqrt{3}/54$.

Lemma A.3 *For any pure state* $|\psi_2\rangle$, $F(|\psi_2\rangle, D_{s_2 t_2}(|\psi_2\rangle)) = 1/2 + 2\sqrt{3}/243$.

Proof. By Lemma A.1, $D_{s_2 t_2} = D_4[\boldsymbol{\rho}_1] \circ D_2[\boldsymbol{\rho}_1] \circ D_3 \circ D_1$. By Lemmas 3.2 and 3.4, $D_3 \circ D_1(|\psi_1\rangle) = \frac{4}{9}|\psi_2\rangle\langle\psi_2| + \frac{5}{9} \cdot \frac{\boldsymbol{I}}{2}$. By Lemma A.2, we have $D_{s_2 t_2}(|\psi_2\rangle) = D_4[\boldsymbol{\rho}_1] \circ D_2[\boldsymbol{\rho}_1](\frac{4}{9}|\psi_2\rangle\langle\psi_2| + \frac{5}{9} \cdot \frac{\boldsymbol{I}}{2}) = \frac{4}{9}\boldsymbol{\rho} + \frac{5}{9} \cdot \frac{\boldsymbol{I}}{2}$ for some $\boldsymbol{\rho}$ such that $F(|\psi_2\rangle, \boldsymbol{\rho}) = \frac{1}{2} + \frac{\sqrt{3}}{54}$. Thus, $F(|\psi_2\rangle, D_{s_2 t_2}(|\psi_2\rangle)) = \frac{4}{9}(\frac{1}{2} + \frac{\sqrt{3}}{54}) + \frac{5}{9} \cdot \frac{1}{2} = \frac{1}{2} + \frac{2\sqrt{3}}{243}$. □

Proof of Lemma A.2. It is not hard to see that $D_4[\boldsymbol{\rho}_1] \circ D_2[\boldsymbol{\rho}_1]$ is $\boldsymbol{I}$-invariant from the following description. To compute $D_4[\boldsymbol{\rho}_1] \circ D_2[\boldsymbol{\rho}_1](|\psi_2\rangle)$, let $|\psi_2\rangle = \cos\theta_1|0\rangle + e^{i\theta_2}\sin\theta_1|1\rangle$ be the state on $\mathcal{Q}_3$, $\boldsymbol{\rho}_1 = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, and $\mathcal{Q}_5 = \mathcal{Q}_6$. Let $p[r_1 r_2]$ be the probability that $r_1 r_2$ is obtained by the tetra measurement of $\mathcal{Q}_3$. Then, we have the following values.

Lemma A.4

$$p[00] = \frac{1}{4} + \frac{\sqrt{3}}{12} \left(\cos 2\theta_1 + \sin 2\theta_1 (\cos \theta_2 + \sin \theta_2) \right),$$

$$p[01] = \frac{1}{4} + \frac{\sqrt{3}}{12} \left(\cos 2\theta_1 + \sin 2\theta_1 (- \cos \theta_2 - \sin \theta_2) \right),$$

$$p[10] = \frac{1}{4} + \frac{\sqrt{3}}{12} \left(- \cos 2\theta_1 + \sin 2\theta_1 (\cos \theta_2 - \sin \theta_2) \right),$$

$$p[11] = \frac{1}{4} + \frac{\sqrt{3}}{12} \left(- \cos 2\theta_1 + \sin 2\theta_1 (- \cos \theta_2 + \sin \theta_2) \right).$$

Proof. Let $\rho_2 = \begin{pmatrix} e & f \\ f^* & h \end{pmatrix}$. Then,

$$p[00] = \mathrm{Tr} \left[\frac{1}{2} |\chi(00)\rangle\langle\chi(00)| \begin{pmatrix} e & f \\ f^* & h \end{pmatrix} \right]$$

$$= \frac{1}{2} (e \cos^2 \tilde{\theta} + h \sin^2 \tilde{\theta} + f \sin \tilde{\theta} \cos \tilde{\theta} e^{i\pi/4} + f^* \sin \tilde{\theta} \cos \tilde{\theta} e^{-i\pi/4}).$$

Similarly, we obtain

$$p[01] = \frac{1}{2} (e \cos^2 \tilde{\theta} + h \sin^2 \tilde{\theta} + f \sin \tilde{\theta} \cos \tilde{\theta} e^{-3i\pi/4} + f^* \sin \tilde{\theta} \cos \tilde{\theta} e^{3i\pi/4}),$$

$$p[10] = \frac{1}{2} (e \sin^2 \tilde{\theta} + h \cos^2 \tilde{\theta} + f \sin \tilde{\theta} \cos \tilde{\theta} e^{-i\pi/4} + f^* \sin \tilde{\theta} \cos \tilde{\theta} e^{i\pi/4}),$$

$$p[11] = \frac{1}{2} (e \sin^2 \tilde{\theta} + h \cos^2 \tilde{\theta} + f \sin \tilde{\theta} \cos \tilde{\theta} e^{3i\pi/4} + f^* \sin \tilde{\theta} \cos \tilde{\theta} e^{-3i\pi/4}).$$

Because $e = \cos^2 \theta_1$, $h = \sin^2 \theta_1$, $f = e^{-i\theta_2} \sin \theta_1 \cos \theta_1$, and $\cos^2 \tilde{\theta} = 1/2 + \sqrt{3}/6$ (and hence $\sin \tilde{\theta} \cos \tilde{\theta} = 1/\sqrt{6}$), $p[00]$ is rewritten as

$$p[00] = \frac{1}{2} \left(\frac{1}{2} + \frac{\sqrt{3}}{6} (\cos^2 \theta_1 - \sin^2 \theta_1) + \frac{1}{\sqrt{6}} \sin \theta_1 \cos \theta_1 \left(e^{-i\theta_2} \frac{1+i}{\sqrt{2}} + e^{i\theta_2} \frac{1-i}{\sqrt{2}} \right) \right)$$

$$= \frac{1}{4} + \frac{\sqrt{3}}{12} (\cos 2\theta_1 + \sin 2\theta_1 (\cos \theta_2 + \sin \theta_2)),$$

which is the desired value. Similarly, we can calculate the desired values of $p[01], p[10], p[11]$. □

Then, after the group operation, the state on $\mathcal{Q}_1 \otimes \mathcal{Q}_5 = \mathcal{Q}_1 \otimes \mathcal{Q}_6$ can be written as

$$\boldsymbol{\sigma} = p[00]\boldsymbol{\rho}(I) + p[01]\boldsymbol{\rho}(Z) + p[10]\boldsymbol{\rho}(X) + p[11]\boldsymbol{\rho}(Y),$$

where $\boldsymbol{\rho}(I), \ldots$ can be given by the following lemma:

Lemma A.5 For $W \in \{I, X, Y, Z\}$,

$$\begin{aligned} \boldsymbol{\rho}(W) &= \left(\frac{2a}{3} |0\rangle\langle 0| + \frac{1}{6} |1\rangle\langle 1| + \frac{b}{3} |0\rangle\langle 1| + \frac{c}{3} |1\rangle\langle 0| \right) \otimes W (|0\rangle\langle 0|) \\ &+ \left(\frac{1}{6} |1\rangle\langle 0| + \frac{b}{3} I \right) \otimes W(|0\rangle\langle 1|) + \left(\frac{1}{6} |0\rangle\langle 1| + \frac{c}{3} I \right) \otimes W(|1\rangle\langle 0|) \\ &+ \left(\frac{1}{6} |0\rangle\langle 0| + \frac{2d}{3} |1\rangle\langle 1| + \frac{b}{3} |0\rangle\langle 1| + \frac{c}{3} |1\rangle\langle 0| \right) \otimes W (|1\rangle\langle 1|). \end{aligned}$$

Operation\Bell states	$|\Phi^+\rangle$	$|\Phi^-\rangle$	$|\Psi^+\rangle$	$|\Psi^-\rangle$
I	1/3	1/3	1/3	0
Z	1/3	1/3	0	1/3
X	1/3	0	1/3	1/3
Y	0	1/3	1/3	1/3

Table 1: Probabilities that the measurement values for the four Bell states by the measurement in the Bell basis at t_2 are obtained according to the approximated group operations at s_0.

Proof. By Eq.(1), we can see that the state of the system $\mathcal{Q}_1 \otimes \mathcal{Q}_2$ is

$$\left(\frac{2a}{3}|0\rangle\langle 0| + \frac{b}{3}|0\rangle\langle 1| + \frac{c}{3}|1\rangle\langle 0| + \frac{1}{6}|1\rangle\langle 1|\right) \otimes |0\rangle\langle 0| + \left(\frac{1}{6}|1\rangle\langle 0| + \frac{b}{3}\boldsymbol{I}\right) \otimes |0\rangle\langle 1|$$

$$+ \left(\frac{1}{6}|0\rangle\langle 1| + \frac{c}{3}\boldsymbol{I}\right) \otimes |1\rangle\langle 0| + \left(\frac{1}{6}|0\rangle\langle 0| + \frac{b}{3}|0\rangle\langle 1| + \frac{c}{3}|1\rangle\langle 0| + \frac{2d}{3}|1\rangle\langle 1|\right) \otimes |1\rangle\langle 1|,$$

and hence we obtain the desired formula. $\square$

Then, we apply the 3D Bell measurement to $\boldsymbol{\sigma}$, obtaining $\boldsymbol{\rho}_{out}^2 = BM(\boldsymbol{\sigma})$. For this calculation, we need the following lemma:

Lemma A.6 *1) If $W \in \{I, Z\}$ ($\in \{X, Y\}$, resp.), then by operation (a) we obtain the state $\frac{1}{3}|0\rangle\langle 0| + \frac{2}{3} \cdot \frac{\boldsymbol{I}}{2}$ ($\frac{1}{3}|1\rangle\langle 1| + \frac{2}{3} \cdot \frac{\boldsymbol{I}}{2}$, resp.) as $BM(\boldsymbol{\rho}(W))$.*
2) If $W \in \{I, X\}$ ($\in \{Y, Z\}$, resp.), then by operation (b) we obtain the state $\frac{1}{3}|+\rangle\langle +| + \frac{2}{3} \cdot \frac{\boldsymbol{I}}{2}$ ($\frac{1}{3}|-\rangle\langle -| + \frac{2}{3} \cdot \frac{\boldsymbol{I}}{2}$, resp.) as $BM(\boldsymbol{\rho}(W))$.
3) If $W \in \{I, Y\}$ ($\in \{Z, X\}$, resp.), then by operation (c) we obtain the state $\frac{1}{3}|+'\rangle\langle +'| + \frac{2}{3} \cdot \frac{\boldsymbol{I}}{2}$ ($\frac{1}{3}|-'\rangle\langle -'| + \frac{2}{3} \cdot \frac{\boldsymbol{I}}{2}$, resp.) as $BM(\boldsymbol{\rho}(W_1, W_2))$.

Proof. By calculating the probabilities that the measurement values for the four Bell states are obtained, we have Table 1. (This is checked by calculating $\langle \Phi^+|\boldsymbol{\rho}(W)|\Phi^+\rangle$, $\langle \Phi^-|\boldsymbol{\rho}(W)|\Phi^-\rangle$, $\langle \Psi^+|\boldsymbol{\rho}(W)|\Psi^+\rangle$, and $\langle \Psi^-|\boldsymbol{\rho}(W)|\Psi^-\rangle$ for each $W \in \{I, X, Y, Z\}$.) According to Table 1, we can obtain the desired result by a simple calculation. For example, in case where $W = Z$ is applied at s_0, by operation (a) we obtain the state $(\frac{1}{3} + \frac{1}{3})|0\rangle\langle 0| + (0 + \frac{1}{3})|1\rangle\langle 1| = \frac{1}{3}|0\rangle\langle 0| + \frac{2}{3} \cdot \frac{\boldsymbol{I}}{2}$. The other cases are similarly checked. $\square$

Now we can compute $\boldsymbol{\rho}_{out}^2 = BM(\boldsymbol{\sigma}) = p[00]BM(\boldsymbol{\rho}(I)) + \cdots$ by summing up (1)-(3) of Lemma A.6 with weight 1/3 for each, which implies $\boldsymbol{\rho}_{out}^2 = \frac{2}{3} \cdot \frac{\boldsymbol{I}}{2} + \frac{1}{9}\boldsymbol{\rho}_0$, where

$$\begin{aligned}
\boldsymbol{\rho}_0 &= p[00](|0\rangle\langle 0| + |+\rangle\langle +| + |+'\rangle\langle +'|) + p[01](|0\rangle\langle 0| + |-\rangle\langle -| + |-'\rangle\langle -'|) \\
&+ p[10](|1\rangle\langle 1| + |+\rangle\langle +| + |-'\rangle\langle -'|) + p[11](|1\rangle\langle 1| + |-\rangle\langle -| + |+'\rangle\langle +'|).
\end{aligned}$$

We can check the following lemma by a simple calculation.

Lemma A.7 $\langle \psi_2|\boldsymbol{\rho}_0|\psi_2\rangle = 3/2 + \sqrt{3}/6.$

Proof. By the definition of $p[r_1 r_2]$, $\boldsymbol{\rho}_0 = 3/2 + \sqrt{3}\boldsymbol{\rho}_0'/12$, where

$$\begin{aligned}
\boldsymbol{\rho}_0' &= (\cos 2\theta_1 + \sin 2\theta_1(\cos \theta_2 + \sin \theta_2))(|0\rangle\langle 0| + |+\rangle\langle +| + |+'\rangle\langle +'|) \\
&+ (\cos 2\theta_1 + \sin 2\theta_1(-\cos \theta_2 - \sin \theta_2))(|0\rangle\langle 0| + |-\rangle\langle -| + |-'\rangle\langle -'|) \\
&+ (-\cos 2\theta_1 + \sin 2\theta_1(\cos \theta_2 - \sin \theta_2))(|1\rangle\langle 1| + |+\rangle\langle +| + |-'\rangle\langle -'|) \\
&+ (-\cos 2\theta_1 + \sin 2\theta_1(-\cos \theta_2 + \sin \theta_2))(|1\rangle\langle 1| + |-\rangle\langle -| + |+'\rangle\langle +'|).
\end{aligned}$$

20

Thus, it suffices to show that $\langle\psi_2|\boldsymbol{\rho}'_0|\psi_2\rangle = 2$. We can rewrite $\boldsymbol{\rho}'_0$ as

$$\boldsymbol{\rho}'_0 = 2\cos 2\theta_1(|0\rangle\langle 0| - |1\rangle\langle 1|) + 2\sin 2\theta_1\cos\theta_2(|+\rangle\langle +| - |-\rangle\langle -|)$$
$$+ 2\sin 2\theta_1\sin\theta_2(|+'\rangle\langle +'| - |-'\rangle\langle -'|).$$

Recalling that $|\psi_2\rangle = \cos\theta_1|0\rangle + e^{i\theta_2}\sin\theta|1\rangle$, we can check that $\langle\psi_2||0\rangle\langle 0| - |1\rangle\langle 1|||\psi_2\rangle = \cos 2\theta_1$, $\langle\psi_2||+\rangle\langle +| - |-\rangle\langle -|||\psi_2\rangle = \sin 2\theta_1\cos\theta_2$, and $\langle\psi_2||+'\rangle\langle +'| - |-'\rangle\langle -'|||\psi_2\rangle = \sin 2\theta_1\sin\theta_2$. Thus, we obtain $\langle\psi_2|\boldsymbol{\rho}'_0|\psi_2\rangle = 2\cos^2 2\theta_1 + 2\sin^2 2\theta_1\cos^2\theta_2 + 2\sin^2 2\theta_1\sin^2\theta_2 = 2$. $\qquad\square$

By Lemma A.7, we finally obtain $\langle\psi_2|\boldsymbol{\rho}^2_{out}|\psi_2\rangle = \frac{1}{3} + \frac{1}{9}\left(\frac{3}{2} + \frac{\sqrt{3}}{6}\right) = \frac{1}{2} + \frac{\sqrt{3}}{54}$. This completes the proof of Lemma A.2. $\qquad\square$

A.3 Proof of Theorem 3.10

Our bound is given under the case where the sources at s_1 and s_2 are a qubit $|\psi\rangle$ and a classical bit b. Also, we assume that two side links have unlimited capacity, and then we can assume that the encoded states from sources are pure states. Suppose that there is a protocol with fidelity $1 - \epsilon$. Then, we show $\epsilon > 0.017$. Let $|\xi_\psi\rangle_{t_2 s_0}$ be the encoded state sent from s_1, and $|\phi(b)\rangle_{s_0 t_1}$ be the encoded state sent from s_2, where the subscript of the ket vector presents where they are in. By the Schmidt decomposition, they are written as: $|\xi_\psi\rangle_{t_2 s_0} = \alpha|\psi_2\rangle_{t_2}|\psi_1\rangle_{s_0} + \beta|\psi_2^\perp\rangle_{t_2}|\psi_1^\perp\rangle_{s_0}$, and $|\phi(b)\rangle_{s_0 t_1} = \gamma_b|\phi(b)_1\rangle_{s_0}|\phi(b)_2\rangle_{t_1} + \delta_b|\phi(b)_1^\perp\rangle_{s_0}|\phi(b)_2^\perp\rangle_{t_1}$. Without loss of generality, $|\beta| \leq |\alpha|$ and $|\delta_b| \leq |\gamma_b|$. Note that $\boldsymbol{\rho}_\psi = |\alpha|^2|\psi_1\rangle\langle\psi_1| + |\beta|^2|\psi_1^\perp\rangle\langle\psi_1^\perp|$ (and $\boldsymbol{\rho}(b) = |\gamma|^2|\phi(b)_1\rangle\langle\phi(b)_1| + |\delta|^2|\phi(b)_1^\perp\rangle\langle\phi(b)_1^\perp|$, resp.) are the states after the operations at s_1 (and s_2, resp.) when we focus on the path from s_1 to t_1 (the path from s_2 to t_2, resp.). Then, we have the following bounds on β and δ_b.

Lemma A.8 $|\beta|^2$ and $|\delta_b|^2$ are at most $\frac{1}{2}\left(\frac{3}{2} + \epsilon - \sqrt{\frac{9}{4} + \epsilon^2 - 5\epsilon}\right)$, and $|\delta_0| + |\delta_1| \leq 2\sqrt{\epsilon}$.

Proof. The bounds on $|\beta|$ and $|\delta_b|$ are obtained by the same proof as Lemma 4.3. So, we consider the bound of $|\delta_0| + |\delta_1|$. The fidelity requirement at t_2 gives us $||\boldsymbol{\rho}(0) - \boldsymbol{\rho}(1)||_{tr} \geq 2 - 4\epsilon$. Regard $\boldsymbol{\rho}(0)$ and $\boldsymbol{\rho}(1)$ as the points in the Bloch ball. By the triangle inequality, their distance is at most $(1 - 2|\delta_0|^2) + (1 - 2|\delta_1|^2)$. Thus, $|\delta_0|^2 + |\delta_1|^2 \leq 2\epsilon$. Then, it is easy to see that $|\delta_0| + |\delta_1| \leq 2\sqrt{\epsilon}$. $\square$

Similar to the proof of Theorem 4.2, we lead to two bounds on ϵ from the two paths. We first consider the path s_1-t_1. Let C be the TP-CP map at s_0, and M_1 be the composite TP-CP map by the operations at t_0 and t_1. Take an arbitrary $|\psi\rangle$ and its orthogonal state $|\psi^\perp\rangle$. The fidelity requirement at t_1 gives us the condition

$$||M_1(C \otimes I)(\boldsymbol{\rho}_\psi - \boldsymbol{\rho}_{\psi^\perp})|\phi(b)\rangle\langle\phi(b)|||_{tr} \geq 2 - 4\epsilon.$$

Note that, letting $|\tilde{\phi}(b)\rangle = |\phi(b)_1\rangle|\phi(b)_2\rangle$,

$$|||\phi(b)\rangle\langle\phi(b)| - |\tilde{\phi}(b)\rangle\langle\tilde{\phi}(b)|||_{tr} = 2\sqrt{1 - |\langle\phi(b)|\tilde{\phi}(b)\rangle|^2} = 2|\delta_b|.$$

Thus, by using the triangle inequality

$$||C(\boldsymbol{\rho}_\psi - \boldsymbol{\rho}_{\psi^\perp})|\phi(b)_1\rangle\langle\phi(b)_1|||_{tr} = ||(C \otimes I)(\boldsymbol{\rho}_\psi - \boldsymbol{\rho}_{\psi^\perp})|\tilde{\phi}(b)\rangle\langle\tilde{\phi}(b)|||_{tr}$$
$$\geq ||M_1(C \otimes I)(\boldsymbol{\rho}_\psi - \boldsymbol{\rho}_{\psi^\perp})|\tilde{\phi}(b)\rangle\langle\tilde{\phi}(b)|||_{tr}$$
$$\geq ||M_1(C \otimes I)(\boldsymbol{\rho}_\psi - \boldsymbol{\rho}_{\psi^\perp})|\phi(b)\rangle\langle\phi(b)|||_{tr} - ||M_1(C \otimes I)(\boldsymbol{\rho}_\psi - \boldsymbol{\rho}_{\psi^\perp})(|\tilde{\phi}(b)\rangle\langle\tilde{\phi}(b)| - |\phi(b)\rangle\langle\phi(b)|)||_{tr}$$
$$\geq 2 - 4\epsilon - ||\boldsymbol{\rho}_\psi - \boldsymbol{\rho}_{\psi^\perp}||_{tr} \cdot 2|\delta_b| \geq 2 - 4\epsilon - 4|\delta_b|.$$

21

Let $C(b)$ be the TP-CP map that transforms $\boldsymbol{\rho}$ to $C(\boldsymbol{\rho} \otimes |\phi(b)_1\rangle\langle\phi(b)_1|)$. Then, we have

$$||C(b)(|\psi\rangle\langle\psi| - |\psi^\perp\rangle\langle\psi^\perp|)||_{tr} \geq ||C(b)(\boldsymbol{\rho}_\psi - \boldsymbol{\rho}_{\psi^\perp})||_{tr} \geq 2 - 4\epsilon - 4|\delta_b|.$$

This leads to the condition

$$||C(b)|\psi\rangle\langle\psi|||_{tr} \geq 1 - 4\epsilon - 4|\delta_b| \tag{14}$$

since $||C(b)|\psi^\perp\rangle\langle\psi^\perp|||_{tr} \leq 1$. Recall that the Bloch sphere representation of $C(b)$ is written as the map: $\vec{r} \mapsto O_1(b)\Lambda(b)O_2(b)\vec{r} + \vec{d}(b)$ where $O_1(b), O_2(b)$ are orthogonal matrices with determinant 1, and $\Lambda(b)$ is a diagonal matrix. Let $U(b)$ be the unitary operator whose Bloch sphere representation maps a Bloch vector $\vec{r}$ to $O_1(b)O_2(b)\vec{r}$. Now we take $|\psi\rangle$ such that $U(0)\boldsymbol{\rho}_\psi = U(1)\boldsymbol{\rho}_\psi$. Then, we evaluate $||(C(0) - C(1))\boldsymbol{\rho'}_\psi||_{tr}$ with $\boldsymbol{\rho'}_\psi = |\alpha|^2|\psi_1\rangle\langle\psi_1|$ as follows:

$$||(C(0) - C(1))\boldsymbol{\rho'}_\psi||_{tr}$$
$$\leq ||(C(0) - U(0))\boldsymbol{\rho'}_\psi||_{tr} + ||U(0)(\boldsymbol{\rho'}_\psi - \boldsymbol{\rho}_\psi)||_{tr} + ||U(1)(\boldsymbol{\rho}_\psi - \boldsymbol{\rho'}_\psi)||_{tr} + ||(U(1) - C(1))\boldsymbol{\rho'}_\psi||_{tr}$$
$$= |\alpha|^2(||(C(0) - U(0))|\psi_1\rangle\langle\psi_1|||_{tr} + ||(C(1) - U(1))|\psi_1\rangle\langle\psi_1|||_{tr}) + 2||\boldsymbol{\rho}_\psi - \boldsymbol{\rho'}_\psi||_{tr}.$$

Noting Ineq.(14), $||U(b)|\psi_1\rangle\langle\psi_1|||_{tr} = 1$ and $||\boldsymbol{\rho}_\psi - \boldsymbol{\rho'}_\psi||_{tr} = |\beta|^2$, we obtain

$$||(C(0) - C(1))\boldsymbol{\rho'}_\psi||_{tr} \leq |\alpha|^2(8\epsilon + 4|\delta_0| + 4|\delta_1|) + 2|\beta|^2. \tag{15}$$

Second, we consider the path s_2-t_2. Let M_2 be the composite map by the operations at t_0 and t_2. By the fidelity requirement at t_2, $||M_2(I \otimes C)|\xi_\psi\rangle\langle\xi_\psi|(\boldsymbol{\rho}(0) - \boldsymbol{\rho}(1))||_{tr} \geq 2 - 4\epsilon$. The left-hand side is at most

$$||(I \otimes C)(|\psi_2\rangle\langle\psi_2| \otimes \boldsymbol{\rho'})(\boldsymbol{\rho}(0) - \boldsymbol{\rho}(1))||_{tr} + ||(I \otimes C)(|\xi_\psi\rangle\langle\xi_\psi| - |\psi_2\rangle\langle\psi_2| \otimes \boldsymbol{\rho'})(\boldsymbol{\rho}(0) - \boldsymbol{\rho}(1))||_{tr}$$
$$\leq ||C(\boldsymbol{\rho'}(\boldsymbol{\rho}(0) - \boldsymbol{\rho}(1)))||_{tr} + |||\xi_\psi\rangle\langle\xi_\psi| - |\psi_2\rangle\langle\psi_2| \otimes \boldsymbol{\rho'}||_{tr}||\boldsymbol{\rho}(0) - \boldsymbol{\rho}(1)||_{tr}$$
$$\leq ||(C'(0) - C'(1))\boldsymbol{\rho'}||_{tr} + 2|\beta|\sqrt{1 - |\beta|^2/2} \times 2,$$

where $C'(b)$ is the TP-CP map: $\boldsymbol{\sigma} \mapsto C(\boldsymbol{\sigma} \otimes \boldsymbol{\rho}(b))$ and the last term of the right-hand side is obtained by the same calculation as Lemma 4.5. Since $\boldsymbol{\rho}(b) = (1 - 2|\delta_b|^2)|\phi(b)_1\rangle\langle\phi(b)_1| + 2|\delta_b|^2 \cdot \frac{I}{2}$, $C'(b)$ is decomposed into $C'(b) = (1 - 2|\delta_b|^2)C(b) + 2|\delta_b|^2 C_I$ with some TP-CP map C_I. Now we assume that $|\delta_0|^2 \geq |\delta_1|^2$, which does not loss of generality. By the triangle inequality,

$$||(C'(0) - C'(1))\boldsymbol{\rho'}||_{tr}$$
$$\leq ||(1 - 2|\delta_0|^2)(C(0) - C(1))\boldsymbol{\rho'}||_{tr} + ||(2|\delta_0|^2 - 2|\delta_1|^2)C(1)\boldsymbol{\rho'}||_{tr} + ||(2|\delta_0|^2 - 2|\delta_1|^2)C_I\boldsymbol{\rho'}||_{tr}$$
$$\leq (1 - 2|\delta_0|^2)||(C(0) - C(1))\boldsymbol{\rho'}||_{tr} + 4|\alpha|^2(|\delta_0|^2 - |\delta_1|^2).$$

Thus, we have

$$2 - 4\epsilon \leq 4|\beta|\sqrt{1 - |\beta|^2/2} + (1 - 2|\delta_0|^2)||(C(0) - C(1))\boldsymbol{\rho'}||_{tr} + 4|\alpha|^2(|\delta_0|^2 - |\delta_1|^2). \tag{16}$$

By Ineqs.(15) and (16) from the two paths and Lemma A.8, we obtain

$$2 - 4\epsilon \leq 4|\beta|\sqrt{1 - |\beta|^2/2} + (1 - 2|\delta_0|^2)(|\alpha|^2(8\epsilon + 4|\delta_0| + 4|\delta_1|) + 2|\beta|^2) + 4|\alpha|^2(|\delta_0|^2 - |\delta_1|^2)$$
$$\leq 4|\beta| + 2|\beta|^2 + 4|\delta_0|^2 + 8\epsilon + 4(|\delta_0| + |\delta_1|)$$
$$\leq 4\sqrt{f(\epsilon)} + 6f(\epsilon) + 8\epsilon + 8\sqrt{\epsilon},$$

where $f(\epsilon) = \frac{1}{2}\left(\frac{3}{2} + \epsilon - \sqrt{\frac{9}{4} + \epsilon^2 - 5\epsilon}\right)$. Therefore, we have $1 - 4\sqrt{\epsilon} - 6\epsilon \leq 2\sqrt{f(\epsilon)} + 3f(\epsilon)$. The left-hand side is monotone decreasing on ϵ while the right-hand side is monotone increasing on ϵ. By checking ϵ satisfying the inequality, we obtain $\epsilon > 0.017$.

22

A.4   Proof of Theorem 4.1

Here is the formal description of XQC.

Protocol XQC: Input $|\psi\rangle$ at s_1, and b at s_2; Output $\boldsymbol{\rho}^1_{out}$ at t_1, and Out^2 at t_2.

   Step 1. $(\mathcal{Q}_1, \mathcal{Q}_2) = UC(|\psi\rangle)$ at s_1, and $\mathcal{Q}_3 = \mathcal{Q}_4 = |b\rangle$.
   Step 2. $\mathcal{Q}_5 = X^b(\mathcal{Q}_2)$ at s_0.
   Step 3. $(\mathcal{Q}_6, \mathcal{Q}_7) = UC(\mathcal{Q}_5)$ at t_1.
   Step 4 (Decoding at node t_1 and t_2). $\boldsymbol{\rho}^1_{out} = X^b(\mathcal{Q}_7)$, and Out$^2 = 0$ if $M[B_z](\mathcal{Q}_1) = M[B_z](\mathcal{Q}_6)$, 1 otherwise.

To average the fidelities at both sinks, implement XQC with probability 3/4 and replace Step 1 by the following operation with probability 1/4: send a bit r uniformly at random from s_1 to s_0 and t_2.

Now we show that XQC achieves fidelity 13/18 and 11/18 at t_1 and t_2, respectively. (The analysis of fidelity 2/3 by averaging is omitted since it is rather simpler.) First, we show that the fidelity at t_1 is 13/18. For this purpose, consider the path from s_1 to t_1 in Fig. 6. Note that along the path, the operations at nodes s_1 and t_0 are 2/3-shrinking, and the operation at s_0 is X^b. They are commutative, and hence the composite operation on the system $\mathcal{Q}_2$ along this path can be considered as a 4/9-shrinking map followed by X^b. Since X^b is applied at t_1 again, the final state at t_1 is $\frac{4}{9}|\psi\rangle\langle\psi| + \frac{5}{9} \cdot \frac{\boldsymbol{I}}{2}$. Hence, the fidelity is $F(\boldsymbol{\rho}^1_{out}, |\psi\rangle) = 13/18$.

Second, we show that the probability of recovering b at node t_2 is 11/18. For this purpose, we have to consider the path from s_2 to t_2 in Fig. 6 and the entangled state of $\mathcal{Q}_1 \otimes \mathcal{Q}_2$. Particularly, the cloning at t_0, which only operates on the later half of the system, can be regarded as p-shrinking map on $\mathcal{Q}_2$ in the following sense.

Lemma A.9   Let $\boldsymbol{\rho}_{12}$ be a two-qubit state and $\boldsymbol{\rho}'_{12}$ be the two-qubit state after applying a p-shrinking map on the second qubit of $\boldsymbol{\rho}_{12}$. Then,

$$\boldsymbol{\rho}'_{12} = p\boldsymbol{\rho}_{12} + (1 - p)\left(\mathrm{Tr}_2(\boldsymbol{\rho}_{12}) \otimes \frac{\boldsymbol{I}}{2}\right).$$

Proof.   Consider the cases of the 1-shrinking and 0-shrinking maps on the second qubit of $\boldsymbol{\rho}_{12}$. In those cases, $\boldsymbol{\rho}'_{12}$ is mapped to $\boldsymbol{\rho}_{12}$ and $\left(\mathrm{Tr}_2(\boldsymbol{\rho}_{12}) \otimes \frac{\boldsymbol{I}}{2}\right)$, respectively. (For $p = 0$, this is verified from the facts that $\mathrm{Tr}_1(\boldsymbol{\rho}'_{12}) = \frac{\boldsymbol{I}}{2}$ and $\mathrm{Tr}_2(\boldsymbol{\rho}'_{12}) = \mathrm{Tr}_2(\boldsymbol{\rho}_{12})$ for any $\boldsymbol{\rho}_{12}$.) For $0 < p < 1$, it is easy to see that $\boldsymbol{\rho}'_{12}$ can be described as a linear combination of the above two cases from the linearity of quantum operation. $\square$

Now, it is easy to compute the success probability of recovering b at node t_2 using the above lemma for $p = 2/3$. Let $\boldsymbol{\rho}_{12}$ and $\boldsymbol{\rho}'_{12}$ be the two-qubit state on $\mathcal{Q}_1 \otimes \mathcal{Q}_2$ and on $\mathcal{Q}_1 \otimes \mathcal{Q}_6$, respectively. We can check that $\langle 00|\boldsymbol{\rho}_{12}|00\rangle + \langle 11|\boldsymbol{\rho}_{12}|11\rangle = \frac{2}{3}$, and $\langle 00|\mathrm{Tr}_2(\boldsymbol{\rho}_{12}) \otimes \frac{\boldsymbol{I}}{2}|00\rangle + \langle 11|\mathrm{Tr}_2(\boldsymbol{\rho}_{12}) \otimes \frac{\boldsymbol{I}}{2}|11\rangle = \frac{1}{2}$. Note that when $b = 0$, $\boldsymbol{\rho}_{12}$ does not change at s_0. By Lemma A.9, the probability of recovering $b = 0$ at node t_2 is

$$\langle 00|\boldsymbol{\rho}'_{12}|00\rangle + \langle 11|\boldsymbol{\rho}'_{12}|11\rangle = \frac{2}{3} \cdot \frac{2}{3} + \frac{1}{3} \cdot \frac{1}{2} = \frac{11}{18}.$$

On the other hand when $b = 1$, $(I \otimes X)$ is applied to $\boldsymbol{\rho}_{12}$ at s_0 and therefore the probability of error, i.e., that of obtaining $b = 0$ at node t_2 is

$$\langle 00|(I \otimes X)\boldsymbol{\rho}'_{12}(I \otimes X)|00\rangle + \langle 11|(I \otimes X)\boldsymbol{\rho}'_{12}(I \otimes X)|11\rangle = \langle 01|\boldsymbol{\rho}'_{12}|01\rangle + \langle 10|\boldsymbol{\rho}'_{12}|10\rangle = 1 - \frac{11}{18} = \frac{7}{18}$$

since $I \otimes X$ is commutative with the p-shrinking map on the second qubit. Thus we obtain the fidelity $11/18$ at t_2.

A.5 Proof of Theorem 5.1

First, we recall the quantum random access (QRA) coding by Ambainis et al. [4]. An (n, m, p)-*QRA coding* is a function that maps n-bit strings $x \in \{0, 1\}^n$ to m-qubit states $\boldsymbol{\rho}_x$ satisfying the following: For every $i \in \{1, 2, \ldots, n\}$ there exists a POVM $E^i = \{E_0^i, E_1^i\}$ such that $\mathrm{Tr}(E_{x_i}^i \boldsymbol{\rho}_x) \geq p$ for all $x \in \{0, 1\}^n$, where x_i is the i-th bit of x. If the m-qubit states are classical, the coding is called an (n, m, p)-*classical random access coding*. In [4], an $(2, 1, 0.85)$-QRA coding is given by the following protocol.

> Let $|\varphi(00)\rangle = \cos(\pi/8)|0\rangle + \sin(\pi/8)|1\rangle$, $|\varphi(10)\rangle = \cos(3\pi/8)|0\rangle + \sin(3\pi/8)|1\rangle$, $|\varphi(11)\rangle = \cos(5\pi/8)|0\rangle + \sin(5\pi/8)|1\rangle$, and $|\varphi(01)\rangle = \cos(7\pi/8)|0\rangle + \sin(7\pi/8)|1\rangle$ be the one-qubit state used when the source $x \in \{0, 1\}^2$ is respectively 00, 10, 11, and 01. The first bit of x is obtained by measuring in the basis B_z, while the second one by measuring in the basis B_x.

In fact, the success probability of the above protocol is $\cos^2(\pi/8) \approx 0.85$. On the contrary, it was also shown that any $(2, 1, p)$-classical random access coding should satisfy $p \leq 1/2$.

A map that transforms an arbitrary equatorial state (i.e., the one-qubit state whose amplitudes are real) $|\psi\rangle\langle\psi|$ to $p|\psi\rangle\langle\psi| + (1-p)\frac{\boldsymbol{I}}{2}$ is called a p-shrinking map on equatorial qubits. The following lemma is verified from the transformation of the phase-covariant cloning machine [8, 11]. (The term "the phase-covariant copy" is defined similarly as the universal copy.) Fortunately, for our purpose the detail of the cloning machine except the fact that it is a $1/\sqrt{2}$-shrinking map is not needed.

Lemma A.10 *The phase-covariant copy is $1/\sqrt{2}$-shrinking map on equatorial qubits.*

Finally we introduce the 2D measurement. This measurement is defined by the POVM $\{\frac{1}{2}|\varphi(z_1 z_2)\rangle \mid z_1 z_2 \in \{0, 1\}^2\}$, denoted by MM_2. Its intuition is to do the two projective measurements in the bases $\{|\varphi(00)\rangle, |\varphi(11)\rangle\}$ and $\{|\varphi(01)\rangle, |\varphi(10)\rangle\}$ with probability $1/2$ for each. Notice that we estimate the QRA coding state from s_2 correctly if we choose the right one of the two bases.

The detailed description of $X2C2C$ is as follows. The term $(\mathcal{Q}, \mathcal{Q}') = PC(\mathcal{Q}'')$ means that $\mathcal{Q}$ and $\mathcal{Q}'$ are the two copies output by the phase-covariant quantum cloning machine when $\mathcal{Q}''$ is given as the input.

Protocol $X2C2C$: Input $x_1 x_2$ at s_1, $y_1 y_2$ at s_2; Output Out^1 at t_1, Out^2 at t_2.
  Step 1. $\mathcal{Q}_1 = |\varphi(x_1 x_2)\rangle$, $\mathcal{Q}_2 = |\varphi(x_1 x_2)\rangle$, $\mathcal{Q}_3 = |\varphi(y_1 y_2)\rangle$, and $\mathcal{Q}_4 = |\varphi(y_1 y_2)\rangle$.
  Step 2. $\mathcal{Q}_5 = GR(\mathcal{Q}_2, MM_2(\mathcal{Q}_3))$ at s_0.
  Step 3. $(\mathcal{Q}_6, \mathcal{Q}_7) = PC(\mathcal{Q}_5)$ at t_0.
  Step 4 (Decoding the j-th bit at t_1 and t_2). Out$^1 = M[B_z](\mathcal{Q}_4) \oplus M[B_z](\mathcal{Q}_7)$ if $j = 1$, and $M[B_x](\mathcal{Q}_4) \oplus M[B_x](\mathcal{Q}_7)$ if $j = 2$. Out$^2 = M[B_z](\mathcal{Q}_1) \oplus M[B_z](\mathcal{Q}_6)$ if $j = 1$, and $M[B_x](\mathcal{Q}_1) \oplus M[B_x](\mathcal{Q}_6)$ if $j = 2$.

Here, we analyze the success probability of $X2C2C$. By the definition of MM_2 the following lemma is immediate.

Lemma A.11 *Given a QRA coding state $|\varphi(y_1 y_2)\rangle$, the probability that $z_1 z_2$ is obtained by MM_2 is $1/2$ if $z_1 z_2 = y_1 y_2$, $1/4$ if $z_1 z_2 = \bar{y}_1 y_2$ or $y_1 \bar{y}_2$, and 0 if $z_1 z_2 = \bar{y}_1 \bar{y}_2$. Here, $\bar{b}$ denotes the negation of a bit b.*
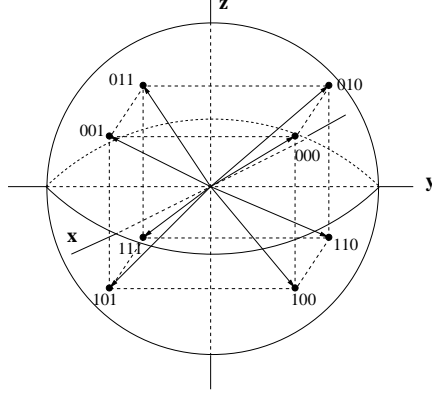
24

Figure 11: $(3, 1, 0.79)$-QRA coding in the Bloch sphere representation

For simplicity, let us assume that $y_1y_2 = 00$ (the analysis of the other cases are similar). By Lemma A.11, the state of $\mathcal{Q}_2 \otimes \mathcal{Q}_3$ after MM_2 is

$$|\varphi(x_1x_2)\rangle\langle\varphi(x_1x_2)| \otimes \left(\frac{1}{2}|00\rangle\langle 00| + \frac{1}{4}(|10\rangle\langle 10| + |01\rangle\langle 01|)\right).$$

Note that if $\tilde{y}_1\tilde{y}_2$ is obtained by MM_2, the state $|\varphi(x_1x_2)\rangle$ from s_1 is transformed into $|\varphi(x_1 \oplus \tilde{y}_1, x_2 \oplus \tilde{y}_2)\rangle$ by GR. Thus, the state of $\mathcal{Q}_5$ is

$$\frac{1}{2}|\varphi(x_1x_2)\rangle\langle\varphi(x_1x_2)| + \frac{1}{4}(|\varphi(\bar{x}_1x_2)\rangle\langle\varphi(\bar{x}_1x_2)| + |\varphi(x_1\bar{x}_2)\rangle\langle\varphi(x_1\bar{x}_2)|)$$

By Lemma A.10, the state of $\mathcal{Q}_6$ (or $\mathcal{Q}_7$) is

$$\frac{1}{2\sqrt{2}}|\varphi(x_1x_2)\rangle\langle\varphi(x_1x_2)| + \frac{1}{4\sqrt{2}}(|\varphi(\bar{x}_1x_2)\rangle\langle\varphi(\bar{x}_1x_2)| + |\varphi(x_1\bar{x}_2)\rangle\langle\varphi(x_1\bar{x}_2)|) + \left(1 - \frac{1}{\sqrt{2}}\right)\frac{I}{2}.$$

Now we check the success probability of decoding the first bit of $y_1y_2 = 00$, i.e., 0 at t_2 (the other cases are similarly checked). As seen from the state of $\mathcal{Q}_6$, the success probability of decoding the first bit of $x_1x_2 \oplus y_1y_2$, i.e., x_1 is

$$\frac{1}{2\sqrt{2}} \cdot \cos^2\frac{\pi}{8} + \frac{1}{4\sqrt{2}}(\cos^2\frac{\pi}{8} + \sin^2\frac{\pi}{8}) + \frac{1}{2}\left(1 - \frac{1}{\sqrt{2}}\right),$$

which is $5/8$. On the contrary, the success probability of decoding the first bit x_1 from the state of $\mathcal{Q}_1$ is $\cos^2\frac{\pi}{8}$. Thus, the success probability of decoding the first bit of y_1y_2 at t_2 is $\cos^2\frac{\pi}{8} \cdot \frac{5}{8} + \sin^2\frac{\pi}{8} \cdot \frac{3}{8} = 1/2 + \sqrt{2}/16$ as claimed.

A.6 Proof of Theorem 5.2

For the proof of Theorem 5.2, we need the following two primitives.

3D Measurement (MM$_3$). The *3D measurement*, denoted by MM_3, is defined by the POVM described by $\{\frac{1}{4}|\varphi(z_1z_2z_3)\rangle\langle\varphi(z_1z_2z_3)| \mid z_1z_2z_3 \in \{0,1\}^3\}$, where $|\varphi(z_1z_2z_3)\rangle$ is the $(3, 1, 0.79)$-QRA coding state of $z_1z_2z_3$ (Fig. 11).

Approximated Group Operation (AG). Before its definition, we introduce the operation Inv, which maps a pure state $|\psi\rangle = a|0\rangle + b|1\rangle$ to its "opposite" state $b^*|0\rangle - a^*|1\rangle$ in the Bloch sphere

(see e.g., [10, 13]). Formally, it is defined as follows: For any mixed state $\boldsymbol{\rho} = \begin{pmatrix} u & v \\ w & x \end{pmatrix}$, $\mathrm{Inv}\boldsymbol{\rho} = \begin{pmatrix} x & -v \\ -w & u \end{pmatrix}$. Note that the set of maps $\boldsymbol{\rho} \mapsto W\boldsymbol{\rho}W^{\dagger}$ ($W \in \{I, X, Y, Z, \mathrm{Inv}, \mathrm{Inv}X, \mathrm{Inv}Y, \mathrm{Inv}Z\}$) is an abelian group. Because Inv is not a TP-CP map, we introduce its approximation Inv', which maps $\boldsymbol{\rho}$ to $\mathrm{Inv}'\boldsymbol{\rho} = \frac{1}{3}\mathrm{Inv}\boldsymbol{\rho} + \frac{2}{3} \cdot \frac{\boldsymbol{I}}{2}$. We can check that Inv' is a TP-CP map. The *approximated group operation under* a three-bit string $r_1r_2r_3$, denoted by $AG(\boldsymbol{\rho}, r_1r_2r_3)$, is a transformation defined by $AG(\boldsymbol{\rho}, 000) = \boldsymbol{\rho}$, $AG(\boldsymbol{\rho}, 011) = Z\boldsymbol{\rho}$, $AG(\boldsymbol{\rho}, 101) = X\boldsymbol{\rho}$, $AG(\boldsymbol{\rho}, 110) = Y\boldsymbol{\rho}$ and, for any $r_1r_2r_3 \in \{001, 010, 100, 111\}$, $AG(\boldsymbol{\rho}, r_1r_2r_3) = \mathrm{Inv}'AG(\boldsymbol{\rho}, \bar{r}_1\bar{r}_2\bar{r}_3)$.

The description of the protocol $X3C3C$ is as follows.

Protocol $X3C3C$: Input $x_1x_2x_3$ at s_1, $y_1y_2y_3$ at s_2; Output Out^1 at t_1, Out^2 at t_2.

Step 1. $\mathcal{Q}_1 = |\varphi(x_1x_2x_3)\rangle$, $\mathcal{Q}_2 = |\varphi(x_1x_2x_3)\rangle$, $\mathcal{Q}_3 = |\varphi(y_1y_2y_3)\rangle$, and $\mathcal{Q}_4 = |\varphi(y_1y_2y_3)\rangle$.

Step 2. $\mathcal{Q}_5 = AG(\mathcal{Q}_2, MM_3(\mathcal{Q}_3))$ at s_0.

Step 3. $(\mathcal{Q}_6, \mathcal{Q}_7) = UC(\mathcal{Q}_5)$ at t_0.

Step 4 (Decoding the j-th bit at t_1 and t_2). $\mathrm{Out}^1 = M[B_z](\mathcal{Q}_4) \oplus M[B_z](\mathcal{Q}_7)$ if $j = 1$, $M[B_x](\mathcal{Q}_4) \oplus M[B_x](\mathcal{Q}_7)$ if $j = 2$, and $M[B_y](\mathcal{Q}_4) \oplus M[B_y](\mathcal{Q}_7)$ if $j = 3$. $\mathrm{Out}^2 = M[B_z](\mathcal{Q}_1) \oplus M[B_z](\mathcal{Q}_6)$ if $j = 1$, $M[B_x](\mathcal{Q}_1) \oplus M[B_x](\mathcal{Q}_6)$ if $j = 2$, and $M[B_y](\mathcal{Q}_1) \oplus M[B_y](\mathcal{Q}_6)$ if $j = 3$.

Now, we analyze $X3C3C$, which is similar to $X2C2C$. By definition of POVM MM_3, we can easily check the following lemma.

Lemma A.12 *Given a QRA coding state $|\varphi(y_1y_2y_3)\rangle$, the probability that $z_1z_2z_3$ is obtained by MM_3 is*

$$
\begin{cases}
1/4 & \text{if } z_1z_2z_3 = y_1y_2y_3, \\
1/6 & \text{if } z_1z_2z_3 = \bar{y}_1y_2y_3,\ y_1\bar{y}_2y_3,\ y_1y_2\bar{y}_3, \\
1/12 & \text{if } z_1z_2z_3 = \bar{y}_1\bar{y}_2y_3,\ \bar{y}_1y_2\bar{y}_3,\ y_1\bar{y}_2\bar{y}_3, \\
0 & \text{if } z_1z_2z_3 = \bar{y}_1\bar{y}_2\bar{y}_3
\end{cases}
$$

Henceforth, for simplicity of descriptions we only consider the case $y_1y_2y_3 = 000$. By Lemma A.12, the state of $\mathcal{Q}_2 \otimes \mathcal{Q}_3$ after MM_3 is

$$
|\varphi(x_1x_2x_3)\rangle\langle\varphi(x_1x_2x_3)| \otimes \left(\frac{1}{4}|000\rangle\langle000| + \frac{1}{6}(|100\rangle\langle100| + |010\rangle\langle010| \right.
$$

$$
\left. +|001\rangle\langle001|) + \frac{1}{12}(|110\rangle\langle110| + |101\rangle\langle101| + |011\rangle\langle011|) \right).
$$

Noting that $\mathrm{Inv}'(|\varphi(z_1z_2z_3)\rangle\langle\varphi(z_1z_2z_3)|) = \frac{1}{3}|\varphi(\bar{z}_1\bar{z}_2\bar{z}_3)\rangle\langle\varphi(\bar{z}_1\bar{z}_2\bar{z}_3)| + \frac{2}{3} \cdot \frac{\boldsymbol{I}}{2}$, the state of $\mathcal{Q}_5$ is

$$
\frac{1}{4}|\varphi(x_1x_2x_3)\rangle\langle\varphi(x_1x_2x_3)|
$$

$$
+ \frac{1}{18}(|\varphi(\bar{x}_1x_2x_3)\rangle\langle\varphi(\bar{x}_1x_2x_3)| + |\varphi(x_1\bar{x}_2x_3)\rangle\langle\varphi(x_1\bar{x}_2x_3)| + |\varphi(x_1x_2\bar{x}_3)\rangle\langle\varphi(x_1x_2\bar{x}_3)|)
$$

$$
+ \frac{1}{12}(|\varphi(\bar{x}_1\bar{x}_2x_3)\rangle\langle\varphi(\bar{x}_1\bar{x}_2x_3)| + |\varphi(\bar{x}_1x_2\bar{x}_3)\rangle\langle\varphi(\bar{x}_1x_2\bar{x}_3)| + |\varphi(x_1\bar{x}_2\bar{x}_3)\rangle\langle\varphi(x_1\bar{x}_2\bar{x}_3)|) + \frac{2}{3} \cdot \frac{1}{6} \cdot 3 \cdot \frac{\boldsymbol{I}}{2}.
$$

By Lemma 3.4, the state of $\mathcal{Q}_6$ (or $\mathcal{Q}_7$)) is

$$\frac{1}{6}|\varphi(x_1x_2x_3)\rangle\langle\varphi(x_1x_2x_3)|$$

$$+\frac{1}{27}(|\varphi(\bar{x}_1x_2x_3)\rangle\langle\varphi(\bar{x}_1x_2x_3)| + |\varphi(x_1\bar{x}_2x_3)\rangle\langle\varphi(x_1\bar{x}_2x_3)| + |\varphi(x_1x_2\bar{x}_3)\rangle\langle\varphi(x_1x_2\bar{x}_3)|)$$

$$+\frac{1}{18}(|\varphi(\bar{x}_1\bar{x}_2x_3)\rangle\langle\varphi(\bar{x}_1\bar{x}_2x_3)| + |\varphi(\bar{x}_1x_2\bar{x}_3)\rangle\langle\varphi(\bar{x}_1x_2\bar{x}_3)| + |\varphi(x_1\bar{x}_2\bar{x}_3)\rangle\langle\varphi(x_1\bar{x}_2\bar{x}_3)|) + \frac{5}{9}\cdot\frac{\boldsymbol{I}}{2},$$

where the last term is obtained by adding $\frac{1}{3}\cdot\frac{1}{4}\cdot\frac{\boldsymbol{I}}{2}$, $\frac{1}{3}\cdot\frac{1}{18}\cdot3\cdot\frac{\boldsymbol{I}}{2}$, $\frac{1}{3}\cdot\frac{1}{12}\cdot3\cdot\frac{\boldsymbol{I}}{2}$, and $\frac{2}{3}\cdot\frac{1}{6}\cdot3\cdot\frac{\boldsymbol{I}}{2}$. Now we check the success probability of decoding the first bit of $y_1y_2y_3 = 000$, i.e., 0. (The other cases are similarly checked.) As seen from the state of $\mathcal{Q}_6$, the success probability of decoding the first bit of $x_1x_2x_3 \oplus y_1y_2y_3$, i.e., x_1 is

$$\frac{1}{6}\left(\frac{1}{2} + \frac{\sqrt{3}}{6}\right) + \frac{1}{27}\left(2\cdot\left(\frac{1}{2} + \frac{\sqrt{3}}{6}\right) + \left(\frac{1}{2} - \frac{\sqrt{3}}{6}\right)\right)$$

$$+\frac{1}{18}\left(2\cdot\left(\frac{1}{2} - \frac{\sqrt{3}}{6}\right) + \left(\frac{1}{2} + \frac{\sqrt{3}}{6}\right)\right) + \frac{5}{9}\cdot\frac{1}{2} = \frac{1}{2} + \frac{2\sqrt{3}}{81}.$$

On the contrary, the success probability of decoding the first bit x_1 from the state of $\mathcal{Q}_1$ is $1/2 + \sqrt{3}/6$. Thus, the success probability of decoding the first bit of $y_1y_2y_3$ at sink t_2 is $(1/2+\sqrt{3}/6)(1/2+ 2\sqrt{3}/81) + (1/2 - \sqrt{3}/6)(1/2 - 2\sqrt{3}/81) = 1/2 + 2/81$ as desired.