

## Piggybacking on quantum streams

Marco Chiani <sup>1,\*</sup>, Andrea Conti <sup>2,†</sup> and Moe Z. Win <sup>3,‡</sup>

<sup>1</sup>*Department of Electrical, Electronic and Information Engineering “Guglielmo Marconi”/CNIT, University of Bologna, Bologna 40136, Italy*

<sup>2</sup>*Department of Engineering/CNIT, University of Ferrara, Ferrara 44122, Italy*

<sup>3</sup>*Laboratory for Information and Decision Systems, Massachusetts Institute of Technology, Cambridge, Massachusetts 02139, USA*



(Received 30 November 2019; accepted 21 May 2020; published 9 July 2020)

This paper shows that it is possible to piggyback classical information on a stream of qubits protected by quantum error-correcting codes. The piggyback channel can be created by introducing intentional errors corresponding to a controlled sequence of syndromes. These syndromes are further protected, when quantum noise is present, by classical error-correcting codes according to a performance-delay trade-off. Classical information can thus be added and extracted at arbitrary epochs without consuming additional quantum resources and without disturbing the quantum stream.

DOI: [10.1103/PhysRevA.102.012410](https://doi.org/10.1103/PhysRevA.102.012410)

### I. INTRODUCTION

We foresee the possibility of piggybacking classical information on a stream of qubits protected by a quantum error-correcting code (QECC). To this end, we propose a method to send a sequence of classical bits on quantum streams by introducing intentional noise. This noise induces a controlled sequence of syndromes, which can be measured without destroying quantum superposition. The syndromes can then be used to encode classical information on top of quantum streams, enabling several possible applications. In particular, piggybacking on quantum streams can facilitate control and annotation for quantum systems and networks.

Consider, for example, a network in which nodes exchange quantum information among each other [1–7]. In addition to user data, control data such as synchronization patterns, node addresses, and routing parameters are needed for the network operation. In classical networks, control data consume physical resources. For instance, in-band synchronization requires that transmitting nodes insert specific patterns of bits into data streams (consuming additional bandwidth) to delimit packets, and that the receiving nodes search for such patterns from incoming bits [8]. However, inserting qubits as control data is not a viable option for quantum networks, since measuring can destroy quantum state superposition [9]. For this reason, several studies assert that quantum networks will need classical networks for out-of-band signaling and control [7]. On the other hand, transmission of classical bits together with random numbers (using continuous variables) for quantum key distribution (QKD) was developed in Refs. [10–12] for security enhancement of classical networks. Instead, we aspire to the transmission of classical bits together with quantum bits (using discrete variables) for control of quantum networks.

A possible way to create a control channel in quantum networks is to introduce dedicated auxiliary orthogonal states. For instance, consider a quantum system with qutrits (Hilbert space of dimension three) instead of qubits, where the orthogonal states  $|0\rangle$ ,  $|1\rangle$  are used as the basis for information, and an additional orthogonal state  $|2\rangle$  is used for synchronization [13]. Inserting states  $|2\rangle$  in different positions along the quantum stream can also carry classical information. Note that systems employing qutrits have read-only capability since altering the classical information would require changing the positions of the  $|2\rangle$ 's. Besides this limitation, the main difficulty is the need for working with qutrits instead of the usual qubits, thereby impacting the overall system architecture.

In this work, we propose a new method to write, read, and eventually rewrite classical information by piggybacking on top of quantum streams. Our method can add and extract the classical information at arbitrary epochs without consuming additional quantum resources and without disturbing the quantum stream. This technique enables new capabilities by unleashing a hidden classical channel provided by QECCs.

### II. PIGGYBACKING VIA INTENTIONAL ERRORS

This section first introduces the notation and the main elements of QECCs, then it proposes the idea of piggybacking classical information on a quantum stream for noiseless and noisy quantum channels.

#### A. Preliminaries

Consider quantum information carried by qubits, which are elements of the two-dimensional Hilbert space  $\mathcal{H}^2$ , with basis  $|0\rangle$  and  $|1\rangle$  [9]. An  $n$ -tuple of qubits ( $n$  qubits) is an element of the  $2^n$ -dimensional Hilbert space,  $\mathcal{H}^{2^n}$ , with basis composed by all possible tensor products  $|i_1\rangle|i_2\rangle \cdots |i_n\rangle$ , with  $i_j \in \{0, 1\}$ ,  $1 \leq j \leq n$ . The Pauli operators, denoted as  $\mathbf{I}$ ,  $\mathbf{X}$ ,  $\mathbf{Z}$ , and  $\mathbf{Y}$ , are defined by  $\mathbf{I}|a\rangle = |a\rangle$ ,  $\mathbf{X}|a\rangle = |a \oplus 1\rangle$ ,  $\mathbf{Z}|a\rangle = (-1)^a|a\rangle$ , and  $\mathbf{Y}|a\rangle = i(-1)^a|a \oplus 1\rangle$  for  $a \in \{0, 1\}$ . These operators either commute or anticommute. The Pauli

\*marco.chiani@unibo.it

†a.conti@ieee.org

‡moewin@mit.edu

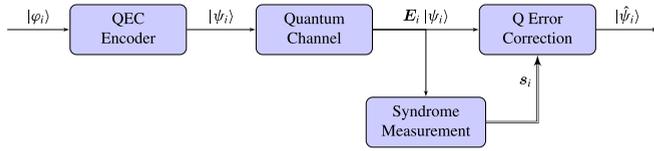


FIG. 1. Quantum communication link employing quantum error correction.

group  $\mathcal{G}_n$  on  $n$  qubits is generated by all possible  $n$ -fold tensor products of these four operators together with the factors  $\pm 1$  and  $\pm i$ . Two operators in  $\mathcal{G}_n$  commute if and only if there is an even number of places where they have different Pauli matrices that are not the identity  $I$ .

When necessary “q-codeword” and “c-codeword” will be used to distinguish quantum and classical codewords. In the block diagrams, single lines and double lines are used for qubits and classical bits, respectively. Figure 1 shows the block diagram of a generic quantum communication link between two nodes employing a QECC designed to cope with channel impairments [14–22]. While the proposed method is valid for all QECCs, for the sake of clarity our discussion is restricted to the case of block codes.

Let  $[[n, k]]$  denote a QECC that encodes  $k$  data qubits  $|\varphi\rangle$  into a codeword of  $n$  qubits  $|\psi\rangle$ . Specifically, consider a stabilizer code  $\mathcal{C}$  generated by  $n - k$  independent and commuting operators  $G_i \in \mathcal{G}_n$ , called generators, such that the subgroup generated by these  $G_i$ 's does not contain  $-I$  [9,18,21]. The code  $\mathcal{C}$  is the set of quantum states  $|\psi\rangle$  satisfying

$$G_i |\psi\rangle = |\psi\rangle, \quad i = 1, 2, \dots, n - k. \quad (1)$$

Consider a codeword  $|\psi\rangle \in \mathcal{C}$  affected by a quantum channel error described by the operator  $E \in \mathcal{G}_n$ . For error correction, the received state  $E|\psi\rangle$  is measured according to the generators  $G_1, G_2, \dots, G_{n-k}$ , resulting in a quantum error syndrome  $s(E) = (s_1, s_2, \dots, s_{n-k})$ , with each  $s_i = +1$  or  $-1$  depending on the fact that  $E$  commutes or anticommutes with  $G_i$ , respectively. Note that, due to (1), the syndrome depends on  $E$  and not on the particular q-codeword  $|\psi\rangle$ . Moreover, measuring the syndrome does not change the quantum state, which remains  $E|\psi\rangle$  [9,18,21]. Let  $\mathcal{S} = \{s^{(1)}, s^{(2)}, \dots, s^{(m)}\}$  be the set of  $m = 2^{n-k}$  possible syndromes, with  $s^{(1)} = (+1, +1, \dots, +1)$  denoting the syndrome of the operators  $E$  (including the identity  $I$ , i.e., the no-errors operator) such that  $E|\psi\rangle$  is still a valid q-codeword.

Among the set of channel errors on the  $n$  qubits producing the syndrome  $s^{(i)}$ , let  $Q^{(i)}$  denote the operator corresponding to the specific error that can be corrected, and let  $\mathcal{Q} = \{Q^{(1)}, Q^{(2)}, \dots, Q^{(m)}\}$ . In other words, if the measured syndrome is  $s^{(i)}$ , the quantum decoder applies the recovery operator  $Q^{(i)\dagger}$  to produce a valid codeword. For example, consider the  $[[3,1]]$  repetition QECC that can correct one bit-flip error by mapping a qubit  $\alpha|0\rangle + \beta|1\rangle$  into a q-codeword  $\alpha|000\rangle + \beta|111\rangle$ . This code has generators  $G_1 = ZZI$  and  $G_2 = IZZ$ , and syndromes  $\mathcal{S} = \{(+1, +1), (-1, +1), (-1, -1), (+1, -1)\}$  with corresponding correctable errors  $\mathcal{Q} = \{III, XII, IXI, IIX\}$ .

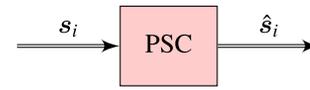


FIG. 2. The piggyback syndrome channel.

## B. Piggybacking: the basic idea

The basic idea of piggybacking is described in the following. Consider an  $[[n, k]]$  QECC that encodes  $k$  data qubits  $|\varphi\rangle$  into a codeword of  $n$  qubits  $|\psi\rangle$ . So, a sequence  $|\varphi_1\rangle, |\varphi_2\rangle, \dots$  of data qubits is encoded into a sequence of q-codewords  $|\psi_1\rangle, |\psi_2\rangle, \dots$ .

The transmitter inserts intentional errors by employing a sequence of operators  $P_1, P_2, \dots$  with corresponding error syndromes  $s_1, s_2, \dots$  so that the transmitted codewords are  $P_1|\psi_1\rangle, P_2|\psi_2\rangle, \dots$ . In particular, these intentional errors are chosen from the set of correctable errors, i.e.,  $P_i \in \mathcal{Q}$ . A decoder at the receiver side measures the quantum error syndromes and infers the sequence of intentional errors  $\hat{s}_1, \hat{s}_2, \dots$ .

The aforementioned procedure creates an  $m$ -ary discrete-input discrete-output channel with alphabet  $\mathcal{S}$  for both input and output symbols. This classical channel is referred to as a piggyback syndrome channel (PSC) (Fig. 2).

In the following, we describe in detail the proposed method for a noiseless quantum channel in Sec. II C and for a noisy quantum channel in Sec. II D.

## C. Piggybacking over a noiseless quantum channel

If the quantum channel is noiseless and an intentional error is introduced by applying the operator  $P_i \in \mathcal{Q}$  on the  $i$ th q-codeword, the transmitted state will be  $P_i|\psi_i\rangle$  (see Fig. 3). The quantum channel does not introduce further errors, and thus syndrome measured at the decoder will be  $\hat{s}_i = s(P_i) = s_i$ . Therefore a sequence of syndromes, carrying classical bits of information, is sent through this error free PSC. Moreover, the  $P_i$  can be determined from the measured syndrome and the state  $|\psi_i\rangle$  can be recovered by applying  $P_i^\dagger$  to the received state  $P_i|\psi_i\rangle$ . The proposed piggybacking method enables sending  $n - k$  classical bits per q-codeword, without additional qubits and without destroying quantum superposition.

A possible application consists in adding, to a group of q-codewords, control data in terms of classical bits that one can read and write without altering the quantum information. Figure 4(a) illustrates an application example, in which a unique pattern of intentional errors is sent over the PSC for quantum frame synchronization, similar to the classical case [8]. Another application is annotation of a quantum stream, as reported in Figs. 4(b) and 4(c).

## D. Piggybacking over a noisy quantum channel

We now consider a noisy quantum channel and, as in the previous case, an intentional error is introduced by applying  $P_i \in \mathcal{Q}$  on the  $i$ th q-codeword. If the quantum channel introduces an error  $E_i \in \mathcal{G}_n$ , then the measured syndrome will be  $\hat{s}_i = s(E_i P_i)$  corresponding to the composite operator  $E_i P_i$  (see Fig. 5). Therefore, the PSC can be viewed as a classical channel with errors. To cope with the effects of quantum

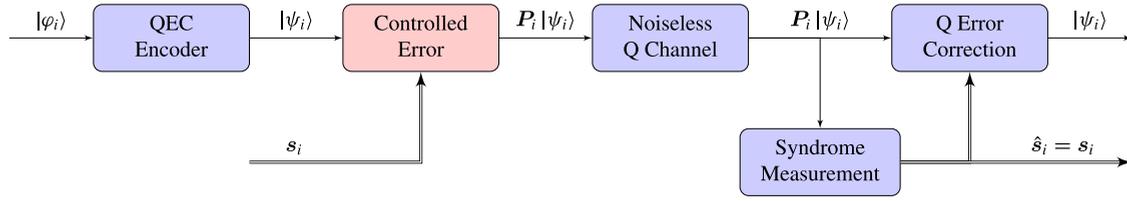


FIG. 3. Quantum piggybacking by intentional errors, noiseless quantum channel. The block added to realize the piggyback classical channel is in red.

channel on the PSC, we envision the use of classical error-correcting codes (CECCs), with alphabet  $\mathcal{S}$  for the encoded symbols. In particular, classical information is encoded at the transmitter so that a transmitted vector  $(s_1, s_2, \dots, s_N)$  is a c-codeword of  $N$  syndromes. The CECC can be any one of the classical codes, including BCH, RS, convolutional, LDPC, and turbo codes [23]. A classical error correction block at the receiver (see Fig. 5) aims to correct the errors due to the quantum channel; at its output the syndromes  $\hat{s}_i$  are equal to the transmitted syndromes  $s_i$  in case of successful correction. Indeed, by employing CECCs with rates below the capacity of the PSC, errors on the received syndromes caused by the quantum channel can be corrected with probability arbitrarily close to one [24]. Therefore applications similar to those for the noiseless case of Fig. 4 are also possible for the noisy case.

The presence of both intentional and unintentional errors, described respectively by the operators  $P_i$  and  $E_i$ , has to be taken into account in the quantum error correction process. Recall that the  $P_i$  is correctable by design; nevertheless, the combined error may not be in the set of correctable errors, i.e.,  $E_i P_i \notin \mathcal{Q}$  even if  $E_i \in \mathcal{Q}$ . For example, one intentional error together with one quantum channel error on different qubits of the same q-codeword would produce an uncorrectable

combined error for a QECC with single qubit error correction capability. The CECC can also help alleviating this problem, in addition to protecting the PSC from quantum channel errors as discussed before. In fact, if classical error correction on the PSC is successful, the intentional error with operator  $P_i$  is known and the quantum channel error with operator  $E_i \in \mathcal{Q}$  can be determined by observing that the measured syndrome is  $\hat{s}_i = s(E_i P_i) = s(E_i) \circ s(P_i)$ , where  $\circ$  denotes the Hadamard product. In fact,  $s(E_i P_i) = +1$  if  $E_i P_i$  commutes with  $G_i$ , which happens when  $E_i$  and  $P_i$  both commute or both anticommute with  $G_i$ . Since the syndrome elements are  $\pm 1$ , it follows also that  $s(E_i) = \hat{s}_i \circ s(P_i)$ .

The classical decoder provides  $\hat{s}_i = s(\hat{P}_i)$  where  $\hat{P}_i$  is the operator corresponding to the estimated intentional error. Therefore, the error computation block in Fig. 5 infers  $E_i$  by computing  $\hat{s}_i \circ \hat{s}_i = s(\hat{E}_i)$ , where  $\hat{E}_i$  is the operator corresponding to the estimated quantum channel error. Then, the quantum error correction block recovers the quantum state from the composite error by applying  $\hat{P}_i^\dagger \hat{E}_i^\dagger$ . Notice that, with the proposed method, the capability of the QECC is not affected by piggybacking, as long as the errors in the PSC are successfully corrected by the CECC.

### III. CAPACITY OF THE PIGGYBACK SYNDROME CHANNEL

As observed, if the quantum channel is noiseless,  $n - k$  [bits/q-codeword] can be sent over the PSC. On the other hand, if the quantum channel is noisy, the capacity of the PSC depends on the statistics of the quantum channel errors. In particular, if the quantum error process is memoryless (i.e., errors  $E_i$  and  $E_j$  are independent for  $i \neq j$ ), the PSC can be viewed as a classical discrete memoryless channel; its mutual information is determined by the transition probability together with the probability distribution  $p(\mathbf{s})$  of the input  $\mathbf{s}$ . The capacity in [bits/q-codeword] is

$$C_{\text{PSC}} = \max_{p(\mathbf{s})} \{H(\mathbf{s}) - H(\mathbf{s}|\hat{\mathbf{s}})\} \quad (2)$$

where  $H(\mathbf{s})$  is the Shannon entropy [24].

Define the probability that the measured syndrome at the receiver is different from the transmitted syndrome as

$$p_{\text{PSC}} = \Pr \{ \hat{\mathbf{s}} \neq \mathbf{s} \}. \quad (3)$$

Consider a quantum channel error that maps the transmitted syndrome into one of the remaining  $2^{n-k} - 1$  syndromes with equal probability, which is the worst case for the capacity. Then, the PSC is an  $m$ -ary symmetric channel ( $m = 2^{n-k}$ )

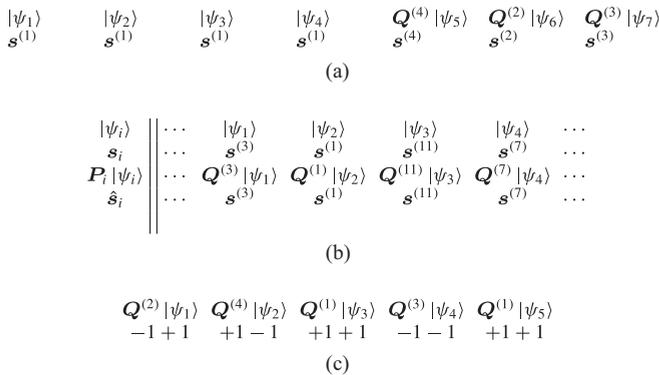


FIG. 4. Examples of piggybacking on a noiseless channel. (a) Piggybacking synchronization patterns on a quantum stream, frames composed of seven q-codewords. The synchronization word pattern used in this example is  $\mathbf{s}^{(4)}, \mathbf{s}^{(2)}, \mathbf{s}^{(3)}$ , and thus synchronization is obtained with three intentional errors on the last three q-codewords. (b) Piggybacking the classical information  $\mathbf{s}^{(3)}, \mathbf{s}^{(1)}, \dots$  on the quantum stream  $|\psi_1\rangle, |\psi_2\rangle, \dots$  (c) Piggybacking ten classical bits of information over a quantum packet composed of five q-codewords, assuming each q-codeword  $|\psi_i\rangle = \alpha_i|000\rangle + \beta_i|111\rangle$  is from a repetition  $[[3,1]]$  QECC. Here  $Q^{(1)}$  = no error,  $Q^{(2)}$  = bit-flip on the first qubit,  $Q^{(3)}$  = bit-flip on the second qubit,  $Q^{(4)}$  = bit-flip on the third qubit.

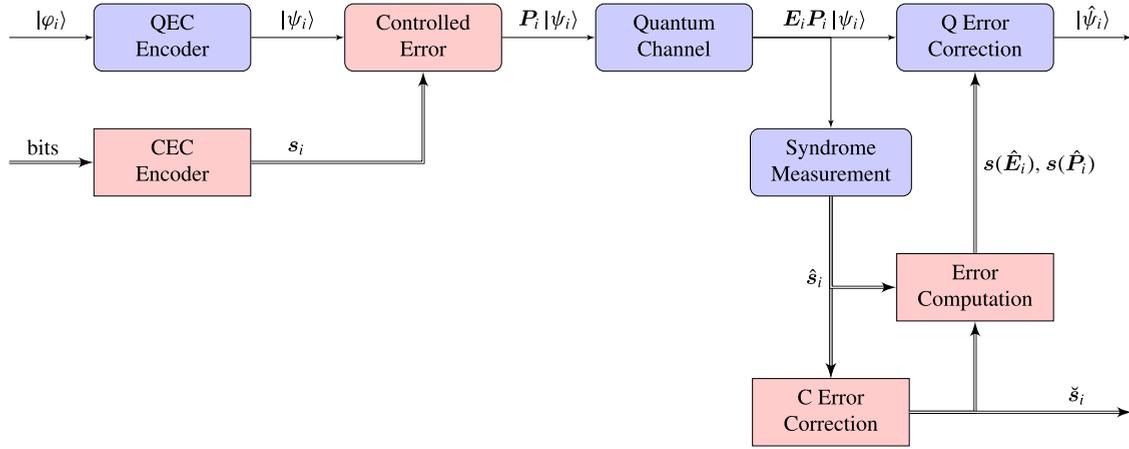


FIG. 5. Quantum piggybacking by intentional errors, noisy quantum channel. The blocks added to realize the piggyback classical channel are in red.

with transition probabilities

$$\Pr \{ \hat{\mathbf{s}} = \mathbf{s}^{(j)} | \mathbf{s} = \mathbf{s}^{(i)} \} = \begin{cases} 1 - p_{\text{PSC}} & j = i \\ \frac{p_{\text{PSC}}}{2^{n-k}-1} & j \neq i \end{cases}$$

From (2), the capacity results in

$$C_{\text{PSC}} = (n - k) - h(p_{\text{PSC}}) - p_{\text{PSC}} \log_2(2^{(n-k)} - 1), \quad (4)$$

where  $h(p) = -p \log_2 p - (1 - p) \log_2(1 - p)$  is the binary entropy function.

The capacity in (4) is completely characterized by  $p_{\text{PSC}}$  which depends on the characteristics of the quantum channel. An upper bound for  $p_{\text{PSC}}$  is the probability that the quantum channel introduces an error on a q-codeword,  $\Pr \{ \mathbf{E}_i \neq \mathbf{I} \}$ , since this accounts also for the undetectable quantum errors for which  $\mathbf{s}(\mathbf{E}_i \mathbf{P}_i) = \mathbf{s}(\mathbf{P}_i)$ .

For example, consider a memoryless quantum depolarizing channel, where each qubit is subject to no error (operator  $\mathbf{I}$ ) with probability  $1 - p_d$ , or to errors of type  $X, Y$  and  $Z$  each with probability  $p_d/3$  [9]. For a q-codeword of  $n$  qubits,  $p_{\text{PSC}} < \Pr \{ \mathbf{E}_i \neq \mathbf{I} \} = 1 - (1 - p_d)^n$ , which together with (4) provides a lower bound on the capacity for values of  $p_{\text{PSC}}$  below  $1 - 2^{-(n-k)}$ . Figure 6 shows  $C_{\text{PSC}}$  as a function of  $p_{\text{PSC}}$  for the  $[[5, 1]]$ ,  $[[7, 1]]$ , and  $[[9, 1]]$  QECCs with single qubit error correction capability [9]. Notice that for  $p_{\text{PSC}} = 0$  the capacity is that of the noiseless case, i.e.,  $n - k$  [bits/q-codeword]. For noisy channels with  $p_{\text{PSC}} = 0.1$  the loss in capacity is of around one bit. Figure 7 shows the lower bound on the capacity of a memoryless quantum depolarizing channel as a function of  $p_d$  for the same QECCs. For a given value of  $p_d$ , characteristic of the quantum depolarizing channel, it is possible to determine what is the minimum guaranteed capacity of the PSC for different quantum codes.

#### IV. IMPACT OF PIGGYBACKING ON THE QECC CAPABILITY

As observed, the PSC does not affect the capability of the QECC if the errors on the measured syndromes are successfully corrected by the classical error correction block in Fig. 5. If the classical error correction fails, then  $\check{s}_i \neq s_i$  for some  $i$ , causing also a failure in the quantum error correction

block. Thus, the probability of a q-codeword error due to piggybacking is equal to the probability of residual syndrome error after decoding

$$p_{\text{QEP}} = \Pr \{ \check{\mathbf{s}}_i \neq \mathbf{s}_i \} \quad (5)$$

which depends on both the quantum channel and the specific CECC used.

The case of a quantum link employing an  $[[n, k]]$  quantum code and a nonbinary  $(N, K)$  classical code over the Galois field  $\text{GF}(2^{n-k})$  is illustrated in the following. With this choice, each symbol of a c-codeword is mapped into a syndrome. The encoder then takes  $K$  information syndromes (i.e.,  $(n - k)K$  classical bits) and produces a c-codeword of  $N$  syndromes, resulting in  $(n - k)K/N$  [bits/q-codeword]. Thus the allowed code rates can be determined using (4) as

$$\frac{K}{N} < 1 - \frac{h(p_{\text{PSC}}) + p_{\text{PSC}} \log_2(2^{n-k} - 1)}{n - k}. \quad (6)$$

To characterize the  $p_{\text{QEP}}$  in (5), consider a Reed Solomon code  $\text{RS}(N, K)$  over  $\text{GF}(2^{n-k})$  with length  $N = 2^{n-k} - 1$ . Since it is a maximum distance separable code, the

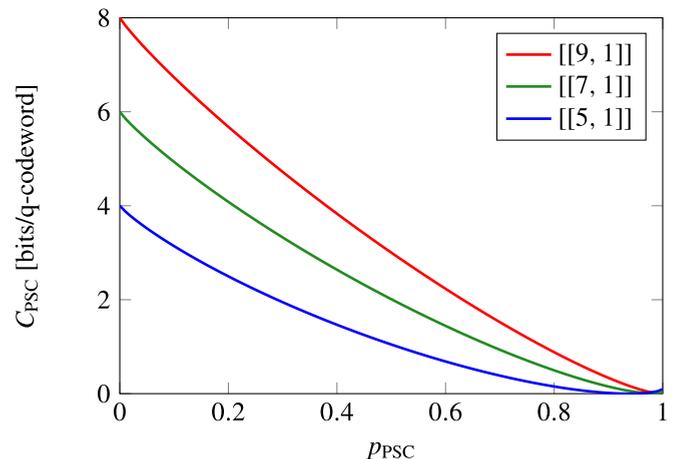


FIG. 6. Capacity of the piggyback syndrome channel as a function of  $p_{\text{PSC}}$  for different QECCs.

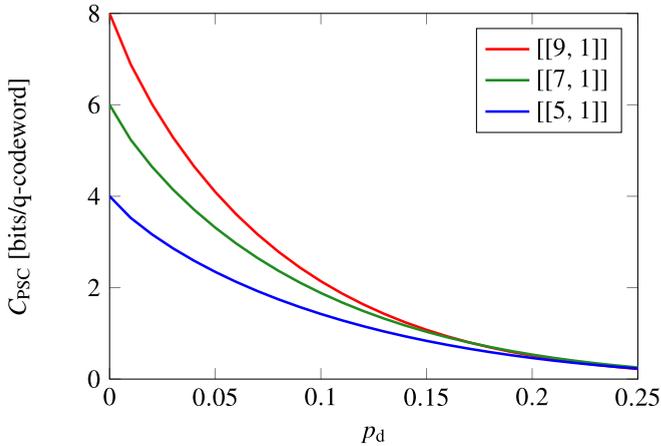


FIG. 7. Lower bound on the capacity of the piggyback syndrome channel for a quantum depolarizing channel as a function of  $p_d$  for different QECCs.

$RS(N, N - 2T)$  can correct up to  $T$  errors per  $c$ -codeword [23]. For this code, the probability of a  $q$ -codeword error due to piggybacking is upper bounded by

$$p_{\text{QEP}} \leq \sum_{\ell=T+1}^N \binom{N}{\ell} p_{\text{PSC}}^{\ell} (1 - p_{\text{PSC}})^{N-\ell}. \quad (7)$$

Figure 8 shows the upper bound as a function of  $p_{\text{PSC}}$  when using the  $[[7, 1]]$  QECC together with  $RS(63, 63 - 2T)$  codes over  $GF(2^6)$  for the PSC. It can be seen that with the  $RS(63, 23)$  code, which can correct up to  $T = 20$  erroneous syndromes per  $c$ -codeword, the PSC has a negligible impact on the quantum stream ( $p_{\text{QEP}} < 10^{-4}$ ) whenever  $p_{\text{PSC}} < 0.15$ . Notice that the quantum decoder will experience a delay of  $N = 63$   $q$ -codewords.

The impact of piggybacking on quantum streams can be reduced for a given quantum channel (equivalently, noisier quantum channels can be considered for a given maximum tolerable  $q$ -codeword error probability) by using more powerful CECCs, without consuming additional quantum resources. However, it is important to observe that using longer  $c$ -codewords results in larger delay for the quantum error correction. Therefore, a performance–delay trade-off has to be

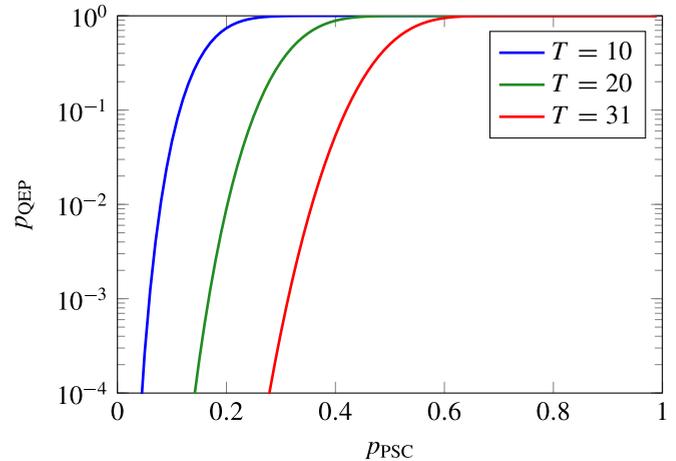


FIG. 8. Upper bound on the probability of a  $q$ -codeword error due to piggybacking,  $p_{\text{QEP}}$ , as a function of  $p_{\text{PSC}}$  for different correction capabilities  $T$ .

accounted for in designing CECCs to control the impact of piggybacking on quantum streams.

## V. CONCLUSION

We put forth a method to piggyback up to  $n - k$  classical bits on top of each  $q$ -codeword of an  $[[n, k]]$  quantum code. Such piggyback operation exploits the syndromes of a quantum code by utilizing classical codes according to a performance–delay trade-off. The proposed method enables new capabilities, even for noisy quantum channels, *without* consuming additional quantum resources and *without* disturbing the quantum stream.

## ACKNOWLEDGMENTS

This work was supported in part by the Italian Ministry for Education, University and Research (MIUR) under the program Dipartimenti di Eccellenza (2018-2022), in part by the University of Ferrara under the program Fondo di Ateneo per la Ricerca, in part by the Office of Naval Research under Grant N00014-19-1-2724, and in part by the MIT Institute for Soldier Nanotechnologies.

[1] P. Zoller *et al.*, *Eur. Phys. J. D* **36**, 203 (2005).  
 [2] H. J. Kimble, *Nature (London)* **453**, 1023 (2008).  
 [3] R. Van Meter and J. Touch, *IEEE Commun. Mag.* **51**, 64 (2013).  
 [4] W. Dai, T. Peng, and M. Z. Win, *IEEE J. Sel. Areas Commun.* **38**, 540 (2020).  
 [5] S. Wehner, D. Elkouss, and R. Hanson, *Science* **362**, eaam9288 (2018).  
 [6] *Quantum Computing: Progress and Prospects*, edited E. Grumbling and M. Horowitz (The National Academies Press, Washington, DC, 2019).  
 [7] *Quantum Networks for Open Science Workshop* (Office of Science US Department of Energy, Rockville, MD, USA, 2018).

[8] W. Suwansantisuk, M. Chiani, and M. Z. Win, *IEEE J. Sel. Areas Commun.* **26**, 52 (2008).  
 [9] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information*, 2nd ed. (Cambridge University Press, Cambridge, UK, 2010).  
 [10] B. Qi, *Phys. Rev. A* **94**, 042340 (2016).  
 [11] X. Wu, Y. Wang, Q. Liao, H. Zhong, and Y. Guo, *Entropy* **21**, 333 (2019).  
 [12] R. Kumar, A. Wonfor, R. Penty, T. Spiller, and I. White, *Sci. Rep.* **9**, 1 (2019).  
 [13] Y. Fujiwara, *IEEE Trans. Inf. Theory* **59**, 6796 (2013).  
 [14] P. W. Shor, *Phys. Rev. A* **52**, 2493(R) (1995).  
 [15] A. R. Calderbank and P. W. Shor, *Phys. Rev. A* **54**, 1098 (1996).

- [16] A. M. Steane, *Phys. Rev. Lett.* **77**, 793 (1996).
- [17] R. Laflamme, C. Miquel, J.-P. Paz, and W. H. Zurek, *Phys. Rev. Lett.* **77**, 198 (1996).
- [18] D. Gottesman, *Phys. Rev. A* **54**, 1862 (1996).
- [19] A. Ekert and C. Macchiavello, *Phys. Rev. Lett.* **77**, 2585 (1996).
- [20] A. S. Fletcher, P. W. Shor, and M. Z. Win, *Phys. Rev. A* **75**, 012338 (2007).
- [21] D. Gottesman, in *Proceedings of Symposia in Applied Mathematics* (2009), Vol. 68, pp. 13–58.
- [22] Z. Babar, D. Chandra, H. V. Nguyen, P. Botsinis, D. Alanis, S. X. Ng, and L. Hanzo, *IEEE Commun. Surveys Tuts.* **21**, 970 (2019).
- [23] W. Ryan and S. Lin, *Channel Codes—Classical and Modern* (Cambridge University Press, New York, NY, USA, 2009).
- [24] T. M. Cover and J. A. Thomas, *Elements of Information Theory*, 2nd ed. (Wiley, Hoboken, NJ, 2006).