

# Anonymous broadcasting with a continuous variable surface code

G.K. Brennen<sup>1</sup>, T.F. Demarie<sup>2,1</sup> and N.C. Menicucci<sup>3</sup>

<sup>1</sup>Centre for Engineered Quantum Systems, Department of Physics and Astronomy, Macquarie University, North Ryde, NSW 2109, Australia

<sup>2</sup>Singapore University of Technology and Design, 20 Dover Drive, Singapore 138682

<sup>3</sup>School of Physics, The University of Sydney, Sydney, NSW 2006, Australia

## Introduction and motivation

Almost every aspect of modern society relies on information processing. As made evident by recent events [1], there is a pressing need for protocols able to protect the identity of potential users against malicious entities attempting to interfere with information exchange. An example of such protocols is anonymous broadcasting (AB). In the original classical formulation [2], this involves setting up shared keys between  $n$  parties, which allows for one party to send a bit of information without revealing her identity to the others. Repeated use of such scheme could be used, for example, for tipping off the police, secret balloting, and secure electronic auctions [3]. Classical protocols for AB suffer certain critical limitations [4]: collision between communicating parties, disruption from a malicious party, and the need for shared keys between every pair of participants; though some of these deficiencies can be overcome at the cost of additional resources. A more efficient and secure *quantum* protocol for AB was introduced in [5], which uses a  $n$ -partite  $|\text{GHZ}\rangle$  entangled state as a resource. The quantum version exhibits a property that cannot be achieved classically: it is completely *traceless*, meaning the sender's identity cannot be determined even allowing for all resources used to be made public at the end of the protocol. However, it still suffers from collision and, more importantly, from errors due to decoherence from unwanted interactions with the environment.

## Impact of our work

In this work we show how the advantages of quantum resources for AB can be enhanced by encoding the resource state in a quantum error correction code. By choosing a surface code, errors are for the most part locally correctable by each party. We first introduce the main idea using the discrete variable toric code, which allows for error correction but can only broadcast one bit of information for the qubit case and up to  $\log d$  bits using  $d$ -dimensional qudits. We then generalise the discussion to the recently developed continuous-variable (CV) analogue of the surface code [7]. In fact, while such a state offers natural resilience against errors, it also allows for a larger bit rate than either the classical or the (quantum) discrete counterpart. Furthermore, it can be easily prepared using Gaussian resources and operations. In particular, a novel proposal for production of temporal-mode CV states [8, 9] offers a promising means to implement our schemes experimentally with current technology, as we discuss in [6].

To summarise, our schemes elegantly exploit the topological properties of the surface codes to broadcast information anonymously by means of logical operators. In contrast with the classical protocols these do not require exchange of keys between pairs of parties, but rather are based on a single shared quantum resource, with players performing only local operations on their share. In addition the degree of anonymity and the channel capacity can be controlled by adjusting the squeezing of the CV modes in the state preparation. The efficient preparation and error tolerance of the CV surface code make it an attractive candidate for AB.

## Original contributions

For our protocols  $n$  parties participate and one of them, named Alice, wants to broadcast anonymously. Let us illustrate the main idea of the AB protocol using a qubit toric code. Consider a two dimensional square lattice with periodic boundaries and qubits placed on the edges. The code states are  $+1$  co-eigenstates of the stabiliser sets  $\{\hat{A}_v = \prod_+ \hat{X}_e\}$  and  $\{\hat{B}_f = \prod_\square \hat{Z}_e\}$  defined at the vertices and faces of the lattice [10, 11]. On the torus there are

four such stabiliser states  $\{|GS_{ab}\rangle = X_{\tilde{\mathcal{P}}_1}^a \otimes X_{\tilde{\mathcal{P}}_2}^b |GS_{00}\rangle\}_{a,b \in \{0,1\}}$  encoding two logical qubits., The logical operators are string operators given by  $\hat{Z}_{\mathcal{P}_j} = \prod_{e \in \mathcal{P}_j} \hat{Z}_e$  and  $\hat{X}_{\tilde{\mathcal{P}}_j} = \prod_{e \in \tilde{\mathcal{P}}_j} \hat{X}_e$  where  $\mathcal{P}_j$  and  $\tilde{\mathcal{P}}_j$  are loops on the lattice and dual lattice, threading through or around the hole in the torus (see Fig. 1).

The AB protocol works by preparing the fiducial state  $|GS_{00}\rangle = \prod_v \frac{(1+A_v)}{\sqrt{2}} |0 \dots 0\rangle$  and distributing  $n$  wedges of the network, one to each party (see Fig. 1). Notably since errors in the toric code can be diagnosed by measuring stabilisers, all such measurements and corrections are local to each party except for those stabilizers that straddle the boundary between wedges (see Fig. 1d). Those stabilisers could be measured with the assistance of Bell pairs shared between nearest neighbour parties to enable non local gates [13]. When Alice wants to anonymously broadcast the message  $r = 1$  she performs the string operation  $\hat{X}_{\tilde{\mathcal{P}}_2}$  around the loop on her wedge (see Fig.(1)c) while for the message  $r = 0$  she does nothing. Next, each party  $j$  measures qubits in the  $\hat{Z}$  basis along an arc of the wedge, and publicly announces the parity  $m_j$  of  $+1$  outcomes. The broadcast message is recovered from the sum  $\bigoplus_{j=1}^n m_j = r$ . As with a  $|GHZ\rangle$  state resource, the variance of any individual party's measurement is maximal and only a collusion by all  $n - 1$  of the parties after Alice's announced measurement result would reveal her identity as the broadcaster.

### Continuous variable toric code anonymous broadcasting

Using the CV extension of the toric code as a quantum resource [7], allows for additional features such as the broadcasting of real numbers and potentially even multiple party broadcasting. In this system each edge  $e$  of the lattice is occupied by a bosonic mode with quadrature operators  $\hat{q}_e, \hat{p}_e$  obeying  $[\hat{q}_e, \hat{p}_{e'}] = i\delta_{e,e'}$  (having set  $\hbar = 1$ ). The CV code state is defined as the state annihilated by the set of nullifiers  $\{\hat{a}_v, \hat{b}_f\}$ , with:

$$\hat{a}_v = \frac{1}{\sqrt{8}} \sum_+ (s\hat{q}_e + is^{-1}\hat{p}_e), \text{ and } \hat{b}_f = \frac{1}{\sqrt{8}} \sum_{\square} o(e,f) (s\hat{p}_e - is^{-1}\hat{q}_e),$$

where  $s \geq 1$  is the squeezing factor. Here the orientation sign factor is  $o(e,f) = \pm 1$  if edge  $e$  is oriented the same (opposite) as face  $f$ . A CV surface code state  $|GS\rangle$  satisfies  $\hat{a}_v|GS\rangle = \hat{b}_f|GS\rangle = 0$  at every vertex and face.

Analogous to the two qubits encoded in the qubit toric code, there are two unconstrained *string modes* in the CV toric code defined by the annihilation operators  $\hat{f}_j = \sum_{e \in \mathcal{P}_j} \frac{o(e)}{\sqrt{2|\mathcal{P}_j|}} (s\hat{p}_e - is^{-1}\hat{q}_e)$  for  $j = 1, 2$ , where  $|\mathcal{P}_j|$  is the loop length. These operators satisfy the canonical commutation relations and  $o(e) = \pm 1$  if edge  $e$  is oriented in the same (opposite) direction as  $\mathcal{P}$ . The analogue of the measured qubit string operator is the string momentum operator:

$$\hat{M} \equiv \frac{1}{\sqrt{|\mathcal{P}_2|}} \sum_{e \in \mathcal{P}_2} o(e)\hat{p}_e = \frac{1}{s} \frac{(\hat{f}_2 + \hat{f}_2^\dagger)}{\sqrt{2}}.$$

The protocol for AB is summarised in Fig. 1. Prior to the distribution of the wedges of the code to the  $n$  parties, the CV toric code state is prepared with the string modes in the vacuum state and string mode 2 may, if desired, be momentum squeezed by a factor  $s'$  so that the variance of the string momentum operator is  $(\Delta M)^2 = \frac{1}{2s^2 s'^2}$ . The code is distributed one wedge to each party and if Alice wishes to anonymously broadcast the real number  $r$  she performs the unitary  $e^{-ir \sum_{e \in \tilde{\mathcal{P}}_2} f(e)\hat{q}_e}$  along a loop  $\tilde{\mathcal{P}}_2$  of her wedge. That operation has the effect of displacing the string momentum  $\hat{M}$ . Then each party holding wedge  $j$  measures the Hermitian operator  $\hat{M}_j$  along an arc  $\mathcal{P}_2(j)$ . The result of the measurement of the scaled operator  $\sqrt{|\mathcal{P}_2(j)|}\hat{M}_j$  is recorded as  $m_j \in \mathbb{R}$ . After the measurements, all parties publicly announce their results  $\{m_j\}$  and the transmitted message from Alice can then be inferred from the sum  $\sum_{j=1}^n m_j = r$ . The variance of the local party measurements is  $(\Delta M_j)^2 = \frac{1}{2s^2} + \frac{s^2}{|\mathcal{P}_2(j)|}$ . Consequently, for large squeezing  $s$ , the local measurements have large variance meaning little information can be obtained by any single party or group of parties, while the global variable  $\hat{M}$  that encodes the broadcast message has small variance. This is the key feature that makes the protocol work.

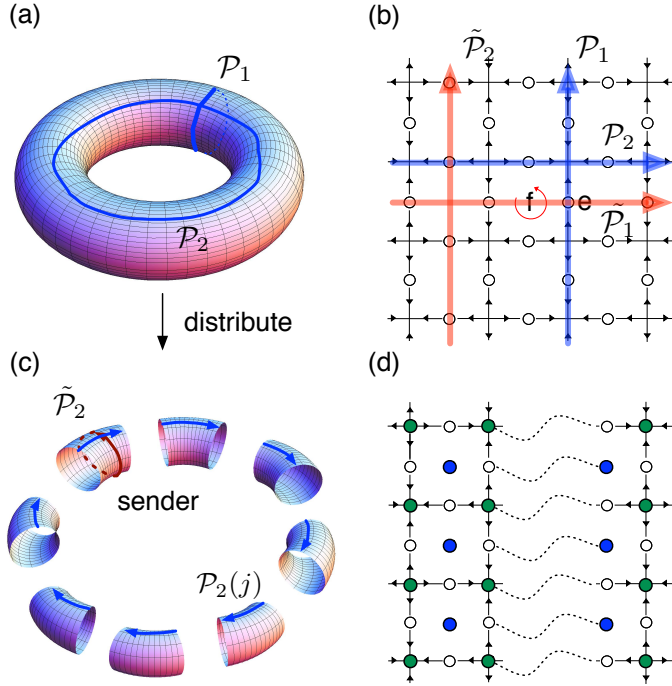


Figure 1: Sketch of the protocol. (a) A CV toric code is prepared in the vacuum state of the two non-local string modes (blue). (b) Close up of the lattice. Physical bosonic modes reside on the edges and each edge is assigned an orientation. Similarly, the faces are given a uniform orientation. (c) The state is distributed to  $n$  parties, one wedge to each. A sender Alice performs the unitary  $e^{-ir \sum_{e \in \tilde{\mathcal{P}}_2} f(e) \hat{q}_e}$  on a loop (shown in red) around her wedge which encodes a message  $r \in \mathbb{R}$ . Then each party  $j$  measures an operator  $\sum_{e \in \mathcal{P}_2(j)} o(e) \hat{p}_e$  along an arc (shown in blue) and publicly announces the measurement outcome  $m_j$ . The broadcast message is obtained from  $\sum_{j=1}^n m_j = r$ . (d) Error mitigation. The blue (green) ancilla are coupled to modes surrounding faces(vertices) and are monitored for decay to inhibit errors via the quantum Zeno effect. Couplings across wedge boundaries are enabled via long range bosonic channels (dotted lines), while the ancillary modes are subject to additional local decay.

**Implementations** – A CV surface code state can be prepared by means of appropriate quadrature measurements on a CV cluster state [7, 16]. Recently, a number of efficient schemes to prepare large CV cluster states have been proposed, using either temporal-modes [8, 9] or frequency-modes [17, 18, 19, 20]. In particular, in [6] we describe how a temporal-mode CV cluster state can be easily distributed among different players using an adjustable mirror. Then the players would do the necessary measurements themselves in order to transform the state into a CV surface code and enable the realisation of the AB protocol.

## Discussion

In the infinite squeezing limit, the input message  $A$  equals the output reconstructed message  $B$  but finite squeezing acts as noise in the channel. The channel capacity is  $C = \max_{p_A(a)} I(A;B)$  where the maximum is over all input probability distributions  $p_A(a)$ , and  $I(A;B)$  is the mutual information between  $A$  and  $B$ . The conditional probability  $p_{B|A}(b|a)$  is a normal distribution in output  $b$  with mean  $a$  and variance  $(\Delta M)^2$ . Assuming a normal prior  $p_A(a)$  with zero mean and variance  $\tau^2$ , we obtain a lower bound:  $C \geq \ln(1 + 2s^2 s'^2 \tau^2)/2$ . Demanding anonymity constrains this value. The information gain by the other players or an outside agency based on the measurement record  $W = \{m_j\}_1^n$  about the identity of Alice, described by a random variable  $D \in \mathbb{Z}_n$ , is the mutual information  $I(W;D)$ . We find  $I(W;D) \leq \frac{nw\tau^2}{12s^2}$  where  $w$  is the width of each wedge held by the  $n$  players. Writing  $I(W;D) = \beta \log(n)$  where  $\beta \ll 1$  so that little is revealed, the channel capacity is [6]

$$C \geq \frac{\ln(1 + 24s'^2 s^4 \beta \log(n)/nw)}{2 \ln 2} \text{ bits.}$$

For example, choosing  $s = 2.22$  (10dB squeezing),  $s' = 1$ ,  $n = 10$ ,  $w = 4$ ,  $\beta = 0.10$ , then  $C \geq 1.06$  bits.

**Error mitigation** – In [6] we propose a scheme to actively drive the CV toric code into the null space of its nullifiers  $\hat{a}_v, \hat{b}_f$ . This can be achieved by embedding ancillary modes  $\{\hat{c}_v\}$  and  $\{\hat{d}_f\}$  prepared in the vacuum state at each vertex and face of the lattice respectively, and using controlled interaction sequences with the system followed by ancillary mode decay. A suitable interaction between the code state and the ancilla is the quadratic Hamiltonian  $\hat{H}_{\text{int}} = g[\sum_v (\hat{c}_v^\dagger \hat{a}_v + \hat{c}_v \hat{a}_v^\dagger) + \sum_f (\hat{d}_f^\dagger \hat{b}_f + \hat{d}_f \hat{b}_f^\dagger)]$ ,

These interactions could be left on for the duration of the protocol so that errors are inhibited from occurring by the quantum Zeno effect [12, 14, 15]. Because each resource state is one time use only, errors that do occur such as loss can be detected and worked around provided they don't percolate across any party's wedge.

## References

- [1] Global surveillance disclosures page on Wikipedia [http://en.wikipedia.org/wiki/Global\\_surveillance\\_disclosures\\_\(2013%E2%80%93present\)](http://en.wikipedia.org/wiki/Global_surveillance_disclosures_(2013%E2%80%93present)); see the references therein for additional details.
- [2] D. Chaum. *Journal of Cryptology*, **1** 65, (1988).
- [3] S. Frank and R. Anderson. *In Proceedings of the Third International Workshop on Information Hiding*, IH 99, pages 434-447, London, UK. Springer-Verlag (2000).
- [4] A. Broadbent and A. Tapp. *Proceedings of ASIACRYPT 2007*, pages 410-426 (2007); arXiv:0706.2010.
- [5] M. Christandl and S. Wehner, *Proceedings of ASIACRYPT 2005*, LNCS 3788, pages 217-235 (2005); arXiv:0409201.
- [6] G.K. Brennen, T.F. Demarie and N.C. Menicucci, unpublished manuscript.
- [7] T.F. Demarie, T. Linjordet, N.C. Menicucci, and G.K. Brennen, *New J. Phys.* **16**, 085011 (2014).
- [8] N. C. Menicucci, *Phys. Rev. A* **83**, 062314 (2011).
- [9] S. Yokoyama *et al.*, *Nature Photonics* **7**, 982 (2013).
- [10] A. Kitaev, *Annals. Phys.*, **303**, 2, 2003.
- [11] J. K. Pachos, *Introduction to Topological Quantum Computation*, Cambridge University Press (2012).
- [12] J.M. Dominy, G.A. Paz-Silva, A.T. Rezakhani, and D.A. Lidar, *J. Phys. A* **46**, 075306 (2013).
- [13] G. Brennen, D. Song, and C. Williams, *Phys. Rev. A* **67**, 050302(R) (2003).
- [14] A. Beige and G.C. Hegerfeldt, *Phys. Rev. A* **53**, 53 (1996).
- [15] M.J. Gagen and G.J. Milburn, *Phys. Rev. A* **47**, 1467 (1993).
- [16] J. Zhang, C. Xie, K. Peng and P. van Loock, *Phys. Rev. A* **78**, 052121 (2008).
- [17] N. C. Menicucci, S. T. Flammia, and O. Pfister, *Phys. Rev. Lett.* **101**, 130501 (2008).
- [18] S. T. Flammia, N. C. Menicucci, and O. Pfister, *J. Phys. B* **42**, 114009 (2009).
- [19] P. Wang, M. Chen, N. C. Menicucci, and O. Pfister, arxiv:1309.4105v1 [quant-ph] (2013).
- [20] M. Chen, N. C. Menicucci, and O. Pfister, *Phys. Rev. Lett.* **112**, 120505 (2014).