UNIVERSITY OF LEEDS

EPSRC Engineering and Physical Sciences Research Council

Topological protocols for quantum anonymous broadcast

James R. Wootton

What is a 'quantum anonymous broadcast?'

There are N players, one of which wishes to send a message to all of the others without revealing their identity: an anonymous broadcast

If the players have access to only classical resources then such a broadcast is possible. Even so, if malicious parties gain control of some of the resources during or after the protocol then the sender's identity may be revealed.

If, however, the players have access to quantum resources then not only are anonymous broadcasts possible, but they can also be resistant to such attacks: even if malicious parties gain control of resources then no information about the sender can be gained.

The property of resistance to these attacks is known as tracelessness, and achieving it is why we consider using quantum resources for anonymous broadcast.

An example of a quantum anonymous broadcast.

We will now look at an example, a protocol presented by Christandl and Wehner. We do this for the case of three players for the sake of simplicity, but it is easily generalized.

There are three players, each of which holds a qubit. The three qubits are in the state:

$$|\psi\rangle = \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)$$

This is the so-called GHZ state. It may also be expressed in the +/- basis as:

$$|\psi\rangle = \frac{1}{2}(|+++\rangle + |+--\rangle + |-+-\rangle + |--+\rangle)$$

A superposition of all states with an even number of minuses.

If any player applies a spin flip, that is a Pauli sigma Z operation, to their qubit then the result will be:

$$Z_n|\psi\rangle = \frac{1}{2}(|++-\rangle + |+-+\rangle + |-++\rangle + |---\rangle)$$

A superposition of all states with an odd number of minuses. This result is exactly the same, no matter who performed the spin flip.

This can be used to broadcast one classical bit anonymously and tracelessly. Assume that one and only one player wishes to send, and that the other players are not malicious. If the sender wishes to sent the bit value 0 then he does nothing to his qubit. If he wishes to send 1 then he applies a spin flip to his qubit.

The state is then:

$$|\psi\rangle=\frac{1}{2}(|+++\rangle+|+--\rangle+|-+-\rangle+|--+\rangle)$$

If 0 is sent and;

$$Z_n|\psi\rangle=\frac{1}{2}(|++-\rangle+|+-+\rangle+|-++\rangle+|---\rangle)$$

If 1 is sent. The players now measure in the +/- basis and share their results with each other. If they measured an even number of 1's then they know that 0 was sent and if they measured an odd number then they know that 1 was sent.

This protocol has therefore broadcast the classical bit. It is also anonymous and traceless as the result of the spin flip is the same, no matter who performed it.

Weaknesses of the Example

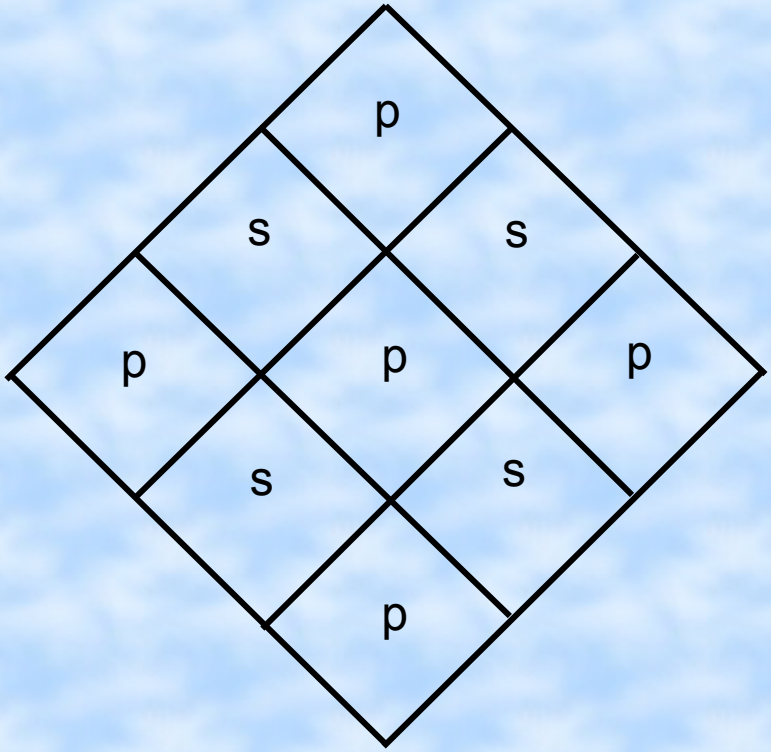
We saw that a spin flip applied by any player maintains anonymity and tracelessness. In fact this is the only non-trivial operation that can do so.

This means that this protocol is not resistant to noise of any kind. If the spin flip is not carried out perfectly and if the environment interacts with the qubits then anonymity and tracelessness may be compromised.

We will now consider a topological protocol for quantum anonymous broadcast which aims to maintain anonymity and tracelessness despite of noise.

Topological quantum anonymous broadcast

Consider a torus with a grid drawn on it. At each vertex of the grid lies a qubit.



The plaquettes of the grid are labelled p and s in alternation. For the four qubits at the corners of each s plaquette we have the operators:

$$A_s = \prod_{i \in s} X_i$$

The product of the four Pauli sigma X operators for these qubits. Similarly, for the p plaquettes we have:

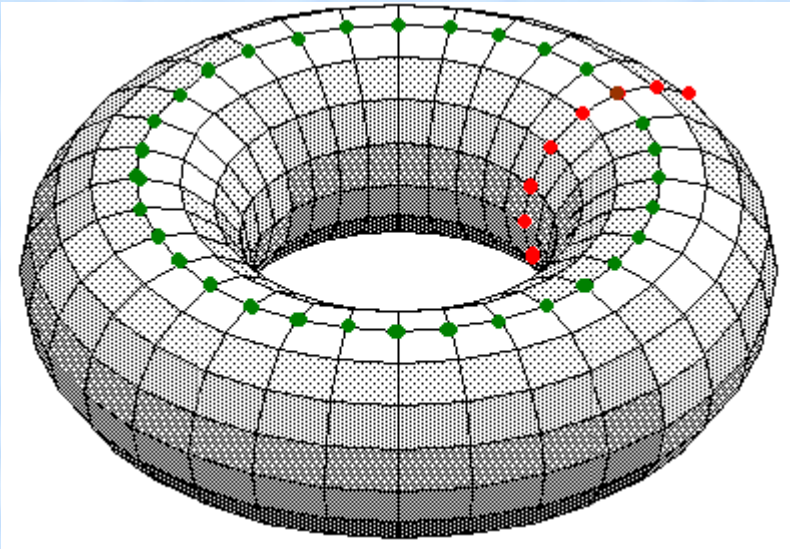
$$B_p = \prod_{i \in s} Z_i$$

These operations are observables which may be measured with outcomes +1 or -1.

Now consider the case where the qubits on the torus are in the state:

$$|\psi_{ee}\rangle = \prod_s \frac{1}{\sqrt{2}}(I + i\,A_s)|0\rangle^{\otimes d}$$

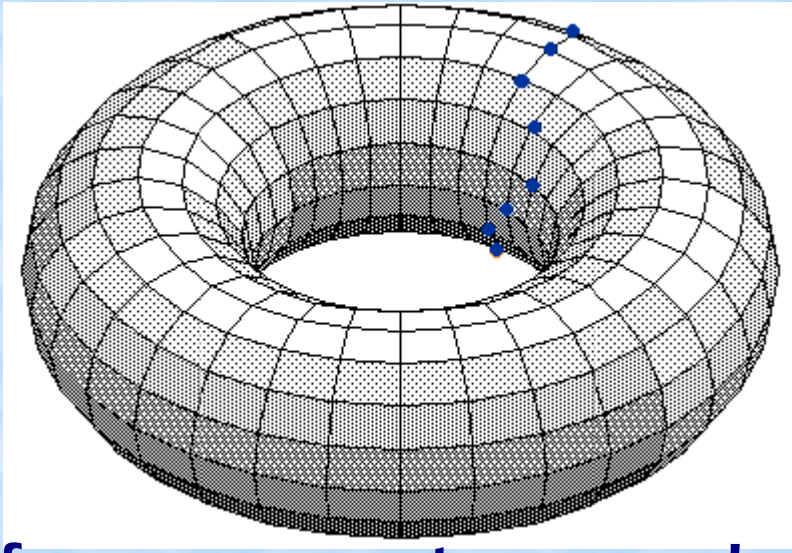
Where I is the identity and d is the number of qubits on the torus.



The second e in the subscript refers to the property of this state that if measurements are made in the computational basis on a chain of qubits which form a non-trivial loop through the hole of the torus, then the result will contain an even number of 1's.

The first e refers to the property that if measurements are made in the computational basis on a chain which forms a non-trivial loop encircling the hole of the torus, then the result will also contain an even number of 1's.

Now let us consider what happens when X operations are made on a chain of qubits forming a non-trivial loop through the hole of the torus.



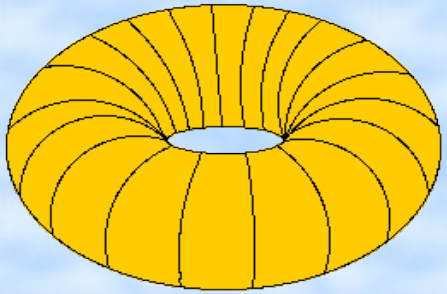
If a measurement in the computational basis is made on a qubit on which an X operation has occurred then the result will be the opposite of what it would have been previously.

If measurements are made in the on a chain which forms a non-trivial loop through the hole of the torus, then this chain will always pass through the loop of X operations an even number of times. The results will therefore still contain an even number of 1's.

For measurements made around a chain which forms a non-trivial loop encircling the hole, however, then this chain will always pass through the loop of X operations an odd number of times. This means that the results will contain an odd number of 1's.

Using the same notation as before we may therefore denote the state after such a loop of X operations as $|\psi_{oe}\rangle$.

The state after the X operations have been made on a chain of qubits will be the same, no matter its form nor where on the torus it was, so long as it is a non-trivial loop through the hole of the torus. We can therefore use this as the basis for a topological protocol for a broadcast which is both anonymous and traceless. We do this as follows.



First we split the torus up into N strips of qubits, one for each player. The qubits of the torus are initially in the state $|\psi_{ee}\rangle$.

One and only one of the players wishes to send a classical bit of data. If they wish to send the bit value 0 then they will do nothing to their qubits. If they wish to send 1 then they will apply X operations to a chain of qubits around a non-trivial loop through the hole of the torus.

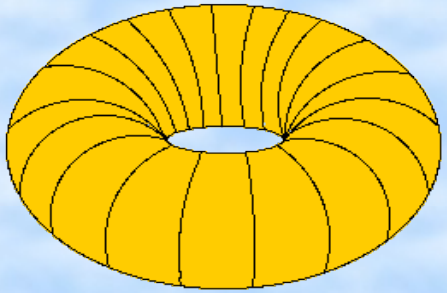
The state of the qubits will then be $|\psi_{ee}\rangle$ if 0 is sent and $|\psi_{oe}\rangle$ if 1 is sent. The players then choose a non-trivial loop encircling the hole and, together, make measurements in the computational basis around it. If the results have an even number of 1's then 0 was sent, if an odd number then 1 was sent.

Error correction of the topological protocol

Both the states $|\psi_{ee}\rangle$ and $|\psi_{oe}\rangle$ are stabilized by the plaquette operators, and so error correction can be done by using the toric code for error correction. This then eliminates any errors from interaction with the environment.

The problem that the X operations performed on a qubit may not be perfect is also eliminated by using the toric code. To see how, let us say that an imperfect X operation is performed on a qubit, and then the four plaquette operators bordering the qubit are measured. If the two s plaquette operators are measured to be +1 and the two p plaquette operators to be -1 then the state is collapsed into a perfect X operation on the qubit. Otherwise it is collapsed into either a Z operation, both an X and a Z or no operation at all.

In the former case we have success and may move on to the next qubit in the chain. In the latter case we must undo the error and try again. We try again until we get it right and repeat this for all qubits in the chain. This results in a chain of perfect X operations, as required.



In practice, however, this error correction may be difficult to carry out. This is because each player only controls a limited number of qubits, not all of them. This will make the measurement of the operators for the plaquettes along the boundaries between strips difficult.

This is especially true as the players need not necessarily be sitting around a torus. The protocol will still work if some players have their qubits on earth and some have theirs on the moon so long as they are initially in the state $|\psi_{ee}\rangle$. In this case the measurements of the boundary plaquettes would certainly not be a local measurement!

This problem can be solved by distributing a number of entangled pairs to neighbouring players such that they can make the measurements. This involves many more resources being used, though.

Another approach can be taken which does not require measurement of boundary plaquettes. Though this approach maintains anonymity it does, however, cease to be traceless. We will therefore not discuss it further here.

Future work

Future work on these topological protocols for quantum anonymous broadcast is to propose a simplified protocol that is experimentally accessible. This will attempt to use the least amounts of resources, use states that can be created and yet still provide anonymous boradcast with error correction.

References

Protocol for classical anonymous broadcast:

D. Chaum. The dining cryptographers problem: Unconditional sender and recipient untraceability.
Journal of Cryptology, 1:65–75, 1988.

Protocol for quantum anonymous broadcast:

M. Christandl and S. Wehner. Quantum anonymous transmissions, quant-ph/0409201.

Toric code:

A. Kitaev. Quantum error correction with imperfect gates. Proceedings of the third international conference on quantum communication and measurement, 181, 1997.

The End