SECURE ASSISTED QUANTUM COMPUTATION

Arxiv > quant-ph/0111046 https://arxiv.org/abs/quant-ph/0111046 by Anderw M. Childs
Literature review for QUTech-Caltech Quantum Cryptography
by Gaetano Priori, Bachelor Physics Engineering student a Politecnico di Torino

0 – Intro, or the need for assisted quantum computation

By studying quantum cryptography we always supposed that every participant can perform universal quantum computation.
In reality we have to accept that universal quantum gates may be very difficult to produce and scale up, when instead it is quite easy to obtain Pauli Operators for multi-qubit states.
Also devices that perform quantum measurements with high precision can be very expensive.
So we can imagine a nearby future where we have access to limited quantum computation that is commercially affordable.

At first glance this should be a very strong limit to our capability of having safe and reliable communications in the quantum realm, but thanks to the result presented in this paper by Childs we can think of a protocol in which an universal computing agent, Bob, helps a 'weak' agent Alice without being able to learn her input and output or even the function she is trying to process.

1 – Introduction and recall of quantum cryptography.

Let's suppose that our heroine Alice needs to perform a very difficult task that requires an universal quantum computer, with Hadamard, π/8 , CNOT (controlled NOT), and measurement gates but she has only at her disposal Pauli X and Z operators.
Bob wants to help her with his brand new quantum computer, but he is not very trustworthy.
Anyway Alice remembers that in order to securely send a quantum state $|\psi\rangle$ to Charlie through a vulnerable channel she only needs to randomly choose a pair of classical bits j,k that represent wherever a Pauli X or Z gate is performed to the state.
Charlie knows j,k so he can recover $|\varphi\rangle$ but an eavesdropper Eve in the middle can only predict a purely mixed state. It's easy to prove that

$$\frac{1}{4}\sum_{j,k=0}^{1} Z^k X^j |\psi\rangle\langle\psi| X^j Z^k = \frac{I}{2}$$

How can this help for our goal of secure assisted quantum computation?

2 – Secure assisted measurement

Now Alice asks Bob to perform a measurement of her state in the computational basis.
Before sending her qubit however she chooses two random bits j,k and perform the unitary operator $Z^k * X^j$.
As before Bob has no information because he can only retrieve a purely mixed state, however if he performs a measurement in the computational basis and reports it to Alice she can retrieve it.
In fact the Z operator does not affect the measurement, and the X flips it. So she needs to flip it if j=1 or leave it unchanged if j=0.

3 – Secure assisted gates

Let's see how Bob can help Alice to perform universal quantum computation, in particulare by showing how to secure a universal set of gates. The Hadamard is the simplest

$$H := \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix};$$

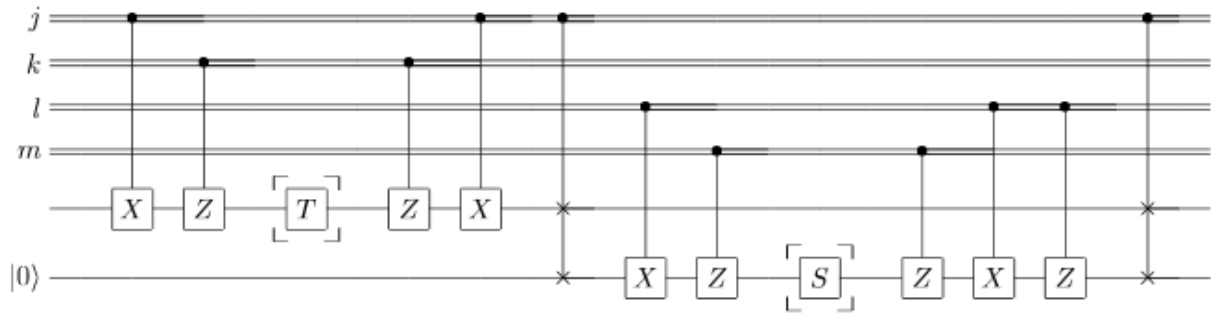
where Alice chooses two random classical bits j,k and performs the unitary transform $Z^k * X^j$ to her qubit.
Because XHZ = ZHX = H the Z gate can be undone by the X and vice-versa, Alice will be able to recover her qubit as if only the Hadamard gates were applied.
A similar procedure can be implemented for the CNOT (Controlled NOT) gate.

$$C := \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$

Since this is a two qubit gate, Alice needs four random qubits j,k,l,m.
She randomizes her result by applying $Z^k * X^j$ to the first and $Z^l * X^m$ to the second.
Now Bob's density matrix is maximally mixed, independently of Alice's state.
As before, Alice needs to correct her result as if only a CNOT was applied.
If j=1 then the target bit was inverted based on the inverted control bit, so she applies X^j to the qubits.
She then applies $X^l * Z^m$ to the target and $X^j * Z^k$ to the control.
X and Z anticommute, so if m=1 she also performed involuntary a (-1) control gate. This can be fixed by applying Z^m to the control bit.
The hardest of the universal quantum gates to be secured is the π/8 :

$$T := \begin{bmatrix} 1 & 0 \\ 0 & \sqrt{i} \end{bmatrix}$$

Although T is a one qubit gate Alice must implement a two round protocol, and needs four random classical bits j,k,l,m. First she randomizes her qubit by applying . $Z^k * X^j$.
Assuming that Bob is honest and has applied the T gate, she can undo the randomization by applying $X^j * Z^k$.
The Z operator commutes with T, but XTX = T† so it differs by a factor $S = T^2$.
Obviously Alice can't perform an S gate, but she can let Bob do it for her. Also $S^2 = Z$ so she can undo the randomization herself.
This problem arises only when the X gate is applied, i.e. when j=1.
However Alice can't reveal the value of j to Bob, so she should *always* ask him to complete this procedure.
If j=0 she can just SWAP the original qubit |ψ> with a dummy one (e.g. |0>) and then re-swap after the second round is complete. Here is the circuit implementation:



4 – Security risks and conclusions

As long as Alice outsources all the expensive computations to Bob she can not be sure of his complete loyalty. He can destroy her qubits, or try to randomly introduce errors.

One way in which Alice can check his fidelity is by inserting some solved problems in the memory flow and check their results. If she gets a wrong solution, the probability that Bob is cheating grows. For example if Alice needs to solve the Shor's Algorithm to factor prime numbers, she can simply multiply two primes with her classical computer and check if Bob gives the right result.
Anyway, for legitimate and random errors we can implement traditional Quantum Error Correction.

A more problematic scenario arises when Bob purposely introduces errors to hijack Alice's memory flow, something very similar to today's stack and heap exploitation. Of course for large n-qubit systems , considering that Alice is implementing obfuscation techniques like those previously analyzed that need at least 2n random classical bits, Bob should try over 2^n mixed states to compromise Alice's memory.
Anyway we should also consider that sometimes Alice won't be able to check the result of the gates computation.
For those cases the author of the paper proposes to just consider Bob as a black box memory agent, but of course this answer is not very satisfactory and could be the an interesting topic of research in the future.
Anyway this is the first theoretical study in this direction, and for the reasons given in the introduction it will become much more useful if ‘dumb’ quantum devices connected to universal quantum mainframes will become commercially available.
Also it is very interesting because the main idea beyond all its results is to give to Bob a maximally mixed state, and this idea is inherited from quantum cryptography.

One interesting thing to inquire deeper would be how can a quantum program that is remotely assisted be 100% sure that Bob, the provider, is not trying to hijack its memory execution. Of course as stated before the probability of this event decays exponentially as the size of the circuit grows, but there may be major flaws or patterns that make this much more probable or programming routines that avoid it almost completely.