Qryptos™: Quantum Framework for Secret-Shared Output Secure Assisted Computation

Josef Barabash, Hadas Barabash, Bo Jie Liu, Ishaan Saini, Islam Faisal

Assisted Quantum Computation [Childs'05]

$$Enc(M)$$

$$Enc(U(M))$$

Alice, a weak quantum client:

- Can generate random classical bits
- Can prepare the ground state
- Can NOT perform measurements
- Pauli Group Comp. **Only**
  - & Conditioned Evaluations

Quantum Server:

- Can perform universal quantum computations.
- The server is semi-honest (honest-but-curious),
- but can be made untrusted using verification of computation (such as Mahadev'18).

[Chi'05] Andrew Childs. Secure Assisted Quantum Computation.

Image Credits: Disney and Google

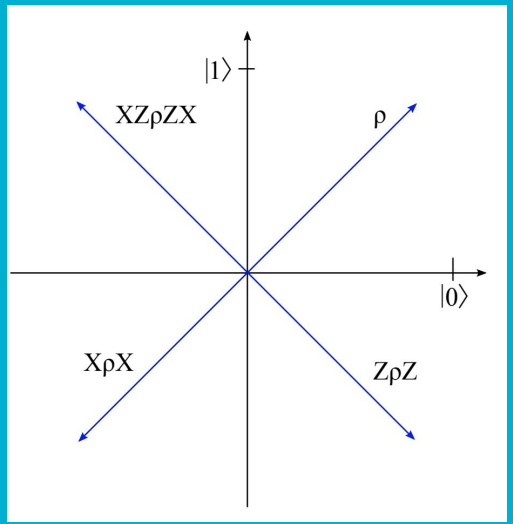
Quantum (Pauli) One-Time Pad

$k_1\, k_2$

$|\Psi\rangle$

$X^{k_1} Z^{k_2} |\Psi\rangle$

$k_1\, k_2$



To an observer, this is a maximally mixed state (Graphic: Vidick-Wehner)

Qryptos™

$Enc(M)$

$Enc(U(M))$

Share 1

Share 2

Alice, a weak quantum client

Step 1: Compute using [Chi'05]

Step 2: Quantumly secret-share the output to Bob and Charlie [CGL'99]

[CGL'99] Richard Cleve, Daniel Gottesman, Hoi-Kwong Lo. How to share a quantum secret.
[Chi'05] Andrew Childs. Secure Assisted Quantum Computation.

Qryptos™ Project Goals

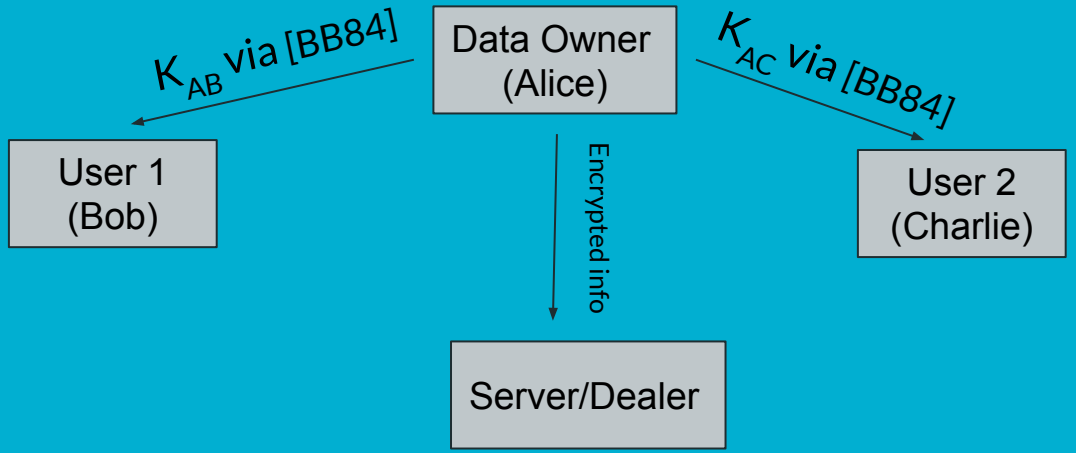
Universal Quantum Computation

- Create a secure computation platform where a strong honest-but-curious server can perform universal computation on an encrypted state.
- The server can not see the data in the clear.

Secret-Shared Output

- The output must be secret-shared to a group of shareholders.
- Qryptos™ does not give full knowledge or control of the data to a single individual in the output shareholders.
- This eliminates the risk of a party ‘going rogue’ stealing the data.

Approach: Step 1
Alice Interaction



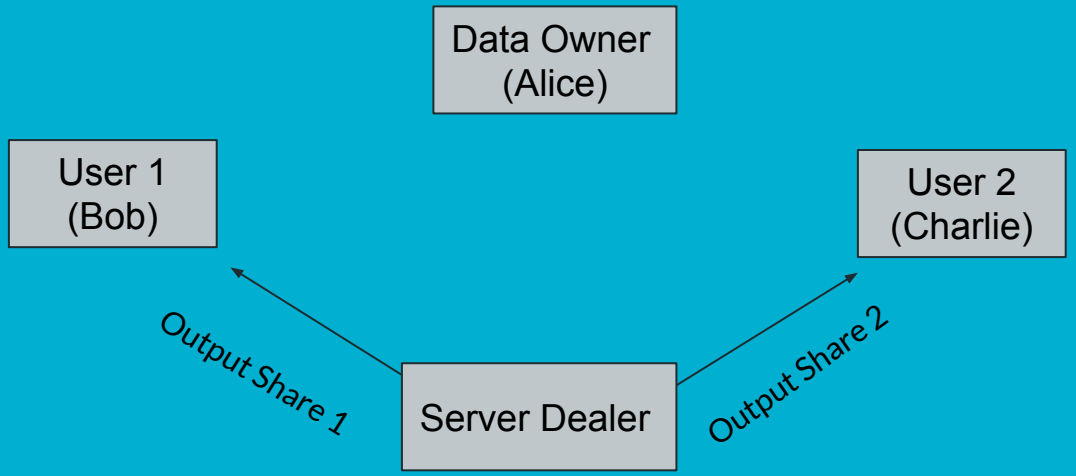
1.1) Alice, a data owner (*weak quantum client*) locally generates a key k, uses the Pauli one-time pad to encrypt the information sent to the dealer.

1.2) Using BB84, Alice shares two classical keys K_{AB}, K_{AC} with Bob and Charlie respectively.

1.3) Using a classical symmetric encryption scheme (such as the OTP), Alice sends K to Bob and Charlie using the respective keys.

Approach Step 2: Server Role

2.1) The server performs quantum computation operations on the encrypted information without accessing it [Childs'05].



2.2) Using quantum secret sharing [CGL'99], the dealer sends shares of the encrypted output to Bob and Charlie, making them dependent on each other.

Approach Step 3
Output Reconstruction

3.1) The output shareholders can now work together to reconstruct the teleported encrypted state.

3.2) They decrypt the state using the Pauli one-time pad and can now access the information or use in further computation.

Application Highlight: Federated Learning via Quantum Optimization Algorithms

Alice, Bob, and Charlie are 3 Banks wishing to jointly compute a risk model based on their data put together.

Each of them will use Qryptos™ to build a local model using their data and the output will be secret-shared among the three of them.

Alice, Bob, and Charlie will jointly run a quantum MPC protocol to obtain the final joint model.

Each of them will have access to the final big model, but no access to other parties' local model.

Possible applications

- Aggregation and Federation in Quantum Machine Learning.
- General-purpose decentralized quantum computation.
- Financial data requiring multiple users and building joint risk models.
- Sensitive organizations applications.
- Quantum cloud services

Conclusion

- We have implemented the components of BB84, Quantum One-Time Pad
- Used them to demonstrate the Childs'05 secure assisted quantum computation.
- Qryptos ™ achieves state privacy against a semi-honest (honest-but-curious) computationally unbounded quantum server.
- The output is secret to any proper subset of the output shareholders.
- The output can be accessed when all the shareholders jointly compute the reconstruction protocol.