Actively secure two-party evaluation of any quantum operation

Frédéric Dupuis
ETH Zürich

Joint work with
Louis Salvail (Université de Montréal)
Jesper Buus Nielsen (Aarhus Universitet)

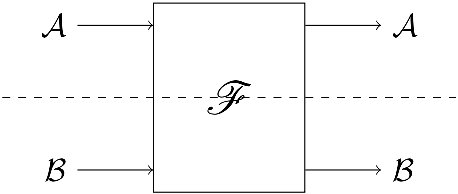
August 23, 2012

Outline

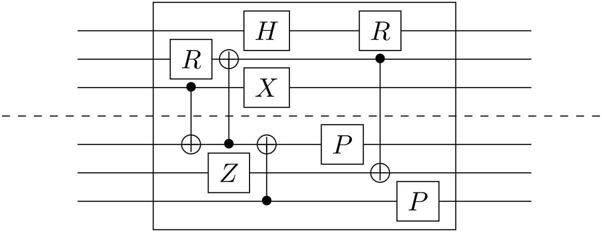
- Introduction: Task to be solved
- Security definition
- “Baby version” (semi-honest adversaries)
- Semi-honest $\rightarrow$ active adversaries
- (Very high-level) description of our protocol

Introduction

Alice and Bob want to execute a quantum circuit $\mathscr{F}$:

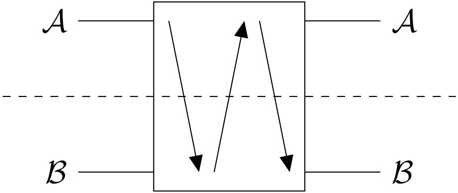


For example:

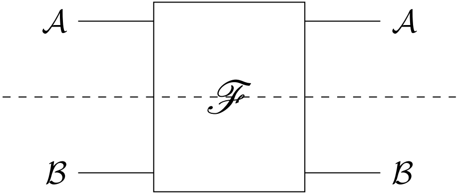


Introduction

They want a protocol



that imitates a black box:



Impossibility in the bare model

- Problem: This is impossible to achieve only by communication (quantum or classical).
- Why? Because it's impossible classically.
- We will assume that Alice and Bob can do *classical* two-party computation for free.
- Hallgren, Smith and Song (2011) have shown that classical ideal functionalities can be replaced by computationally secure protocols if the computational assumptions hold against quantum adversaries.
- What we show: Classical two-party computation $\Rightarrow$ quantum two-party computation

Previous work

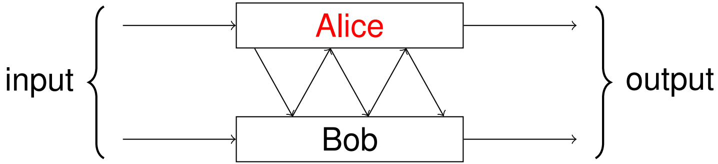
- Quantum multiparty computation:
  - Crépeau, Gottesman, Smith 2002: At most $n/6$ cheaters.
  - Ben-Or, Crépeau, Gottesman, Hassidim, Smith 2008: Strict honest majority.
- Us, CRYPTO2010: Two-party computation, but against "specious" (semi-honest) adversaries.

Brief detour: Security definition

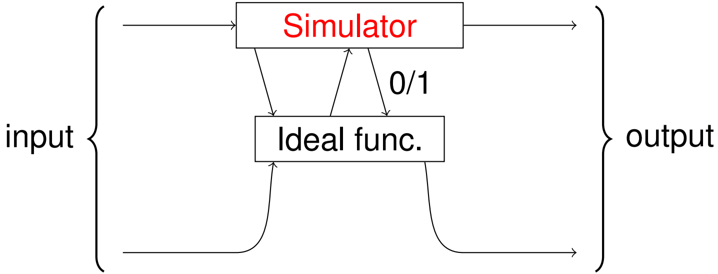
- We define security via simulation
- Problem: Player who goes last has an unavoidable advantage: He can prevent the other from getting his output.

Security definition: Dishonest Alice

Real protocol:

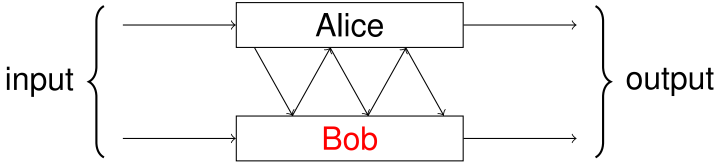


Simulation with ideal functionality:

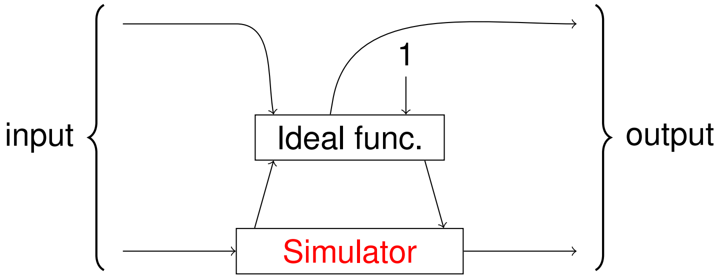


Security definition: Dishonest Bob

Real protocol:



Simulation with ideal functionality:



Baby version: semi-honest adversaries

First, represent $\mathscr{F}$ as a sequence of the following gates:

$|0\rangle$ — $\begin{pmatrix} 1 \\ 0 \end{pmatrix}$

X — $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$

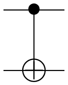
Y — $\begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$

Z — $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$

H — $\frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$

P — $\begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}$

R — $\begin{pmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{pmatrix}$



$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$

Baby version: semi-honest adversaries

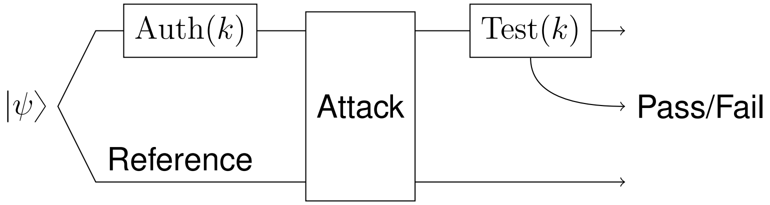
Suppose the adversaries are semi-honest [us, CRYPTO'10]. Then the protocol is as follows:

- Encrypt all the inputs with a quantum one-time pad.
- For each gate in the circuit, execute a subprotocol that performs the gates and updates the keys.
- All the gates can be done without communication except:
  - Non-local CNOT: Need classical communication
  - R-gate (non-Clifford): Need one oblivious transfer.
- Use a perfect SWAP gate to exchange the keys at the end.

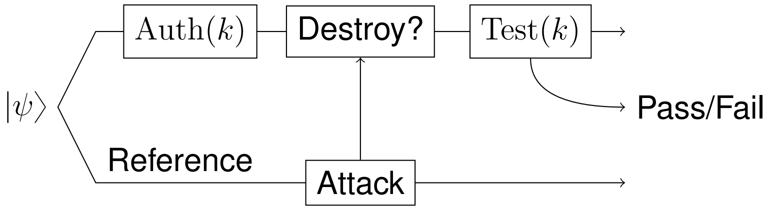
From semi-honest to full security

- We need a way to force a dishonest adversaries to follow the protocol
- Solution: Instead of just encrypting, we *authenticate* all the inputs and ancillas.
- We check the authentication at every step to ensure compliance with the protocol.

Authenticating quantum states



should be equivalent to



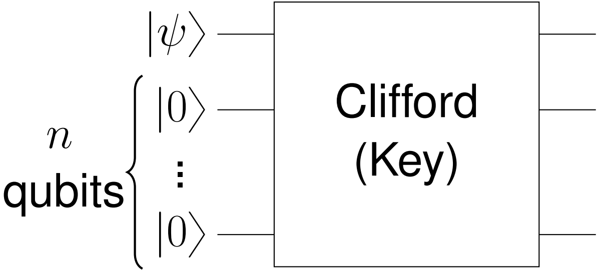
Clifford-based QAS: the Clifford group

[Aharonov, Ben-Or, Eban 2008]

- Pauli group: any tensor product of $\mathbb{1}, X, Y, Z$.
- Clifford group: U is Clifford if for any Pauli P, UPU^* is also Pauli.
- Need $O(n^2)$ bits to identify a Clifford operator.

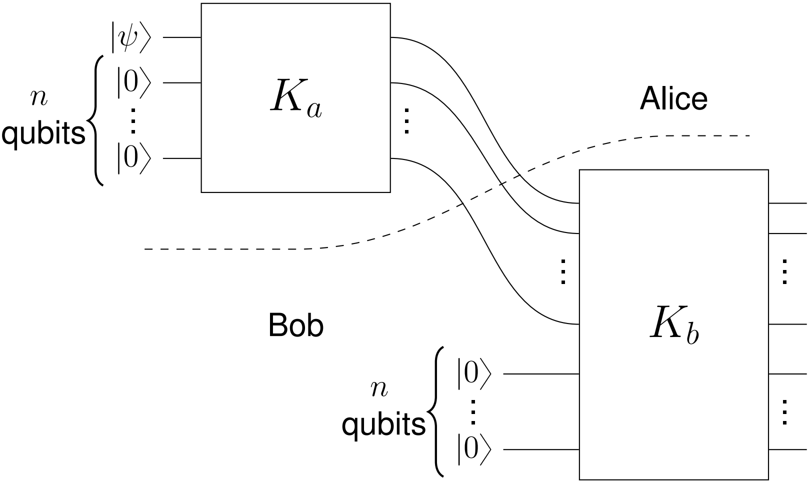
Clifford-based QAS

To authenticate $|\psi\rangle$, do the following:



To check, undo the Clifford and measure the ancillas. If we don't get all $|0\rangle$'s, declare an error.

Swaddling: double authentication

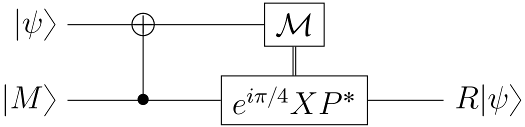


Our protocol

- Swaddle all the inputs and commit to the keys.
- Generate extra $|0\rangle$ and ensure that they are correct.
- For each gate, run a classical protocol that tells Alice and Bob how to execute the gates and update the keys.
- Verify the authentication whenever necessary.
- Open commitments (i.e. reveal all keys).
- Problem gate: the R-gate, the only non-Clifford gate in our set.

The R gate

We can reduce the R gate to Clifford operations by the following trick:



where $|M\rangle = \frac{1}{\sqrt{2}}(|0\rangle + e^{i\pi/4}|1\rangle)$ ("magic state").

The R gate

- We need to generate a supply of $|M\rangle$ states at the beginning.
- Have one player generate a large number of them, and the other player tests a random sample of them and aborts if any errors are found.
- This ensures a low error rate.
- We then use a distillation protocol by Bravyi and Kitaev to distill a smaller number of good $|M\rangle$ states.

Conclusion

- Classical two-party computation $\Rightarrow$ Quantum two-party computation

Thank you

Thank you!

Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

Université de Montréal

SOLIDUM PETIT IN PROFUNDIS · UNIVERSITAS ARHUSIENSIS ·