Quantum Secret Sharing of Classical Information

Alessandro Baccarini

University at Buffalo

anbaccar@buffalo.edu

May 4, 2020

Overview

Measuring a State

- A *state* $|\psi\rangle$ is defined by its *amplitudes* of classical states:

$$|\psi\rangle = \alpha_0 |0\rangle + \alpha_1 |1\rangle + \cdots + \alpha_{N-1} |N-1\rangle ,$$

- Measuring a state will cause it to "collapse" to its classical state $|i\rangle$.
- It is a destructive operation (information contained within the amplitudes is destroyed).

Example (Two Qubit State)

$$|\psi\rangle = \frac{1}{\sqrt{2}} |0\rangle + \frac{1}{\sqrt{2}} |1\rangle$$

$$\implies p(0) = p(1) = \frac{1}{2}$$

Protocol Summary

Quantum Key Distribution Scheme [Hillery, 1999]

Shared Input: The GHZ (Greenberger, Horne, and Zeilinger) state

$$|\psi\rangle = \frac{1}{\sqrt{2}}(|0_a 0_b 0_c\rangle + |1_a 1_b 1_c\rangle)$$

is shared among the three parties A, B, and C, where A is defined as the dealer.
Output: A bit b shared among the parties.
The Protocol:

1. The parties independently and randomly choose a measurement direction $d \in \{x, y\}$. and announce it to each other.
2. If $d_A = x$, then $d_B = d_C$. Otherwise, discard the round.
3. If $d_A = y$, then $d_B \neq d_C$. Otherwise, discard the round.
4. Each party measures their qubit in their respective directions, which causes it to collapse to a classical bit b_i.
5. Set A's measurement $b_A = b$ as the shared bit that B and C must determine.
6. B and C share their measurements b_B and b_C, and conduct a table lookup to determine b.

Alice/Bob's Measurements Effects on Charlie

- Alice and Bob's measurements impact Charlie's state.
  - E.g. Alice and Bob measure in the x direction and get $\frac{1}{\sqrt{2}}(|0\rangle_{a,b} + |1\rangle_{a,b})$, so Charlie will have the state $\frac{1}{\sqrt{2}}(|0\rangle_c + |1\rangle_c)$

B \ A	$+x$	$-x$	$+y$	$-y$
$+x$	$\|0\rangle + \|1\rangle$	$\|0\rangle - \|1\rangle$	$\|0\rangle - i\,\|1\rangle$	$\|0\rangle + i\,\|1\rangle$
$-x$	$\|0\rangle - \|1\rangle$	$\|0\rangle + \|1\rangle$	$\|0\rangle + i\,\|1\rangle$	$\|0\rangle - i\,\|1\rangle$
$+y$	$\|0\rangle - i\,\|1\rangle$	$\|0\rangle + i\,\|1\rangle$	$\|0\rangle - \|1\rangle$	$\|0\rangle + \|1\rangle$
$-y$	$\|0\rangle + i\,\|1\rangle$	$\|0\rangle - i\,\|1\rangle$	$\|0\rangle + \|1\rangle$	$\|0\rangle - \|1\rangle$

$\Longrightarrow$

B \ A	$+x$	$-x$	$+y$	$-y$
$+x$	$+x$	$-x$	$-y$	$+y$
$-x$	$-x$	$+x$	$+y$	$-y$
$+y$	$-y$	$+y$	$-x$	$+x$
$-y$	$+y$	$-y$	$+x$	$-x$

- We use IBM's quiskit [IBM, 2020] library to implement the protocol.
- We generate the shared GHZ state as follows:

$$|\psi\rangle = \frac{1}{\sqrt{2}}(|0_a 0_b 0_c\rangle + |1_a 1_b 1_c\rangle)$$

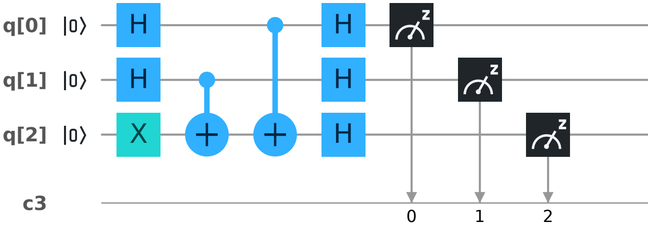
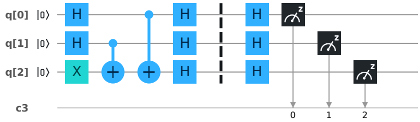


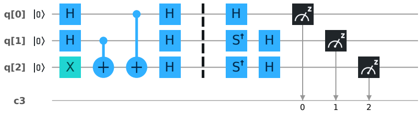
Figure: GHZ state as a quantum circuit in Quiskit.

Measurement Gates

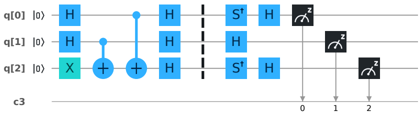
- Each gate is implemented in the `create_and_measure(directions)` function.
- `1` corresponds to a positive measurement, and `0` to a negative one.



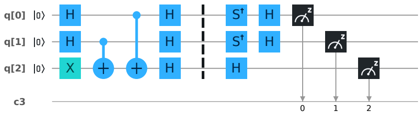
(a) *XXX*



(b) *XYY*



(c) *YXY*



(d) *YYX*

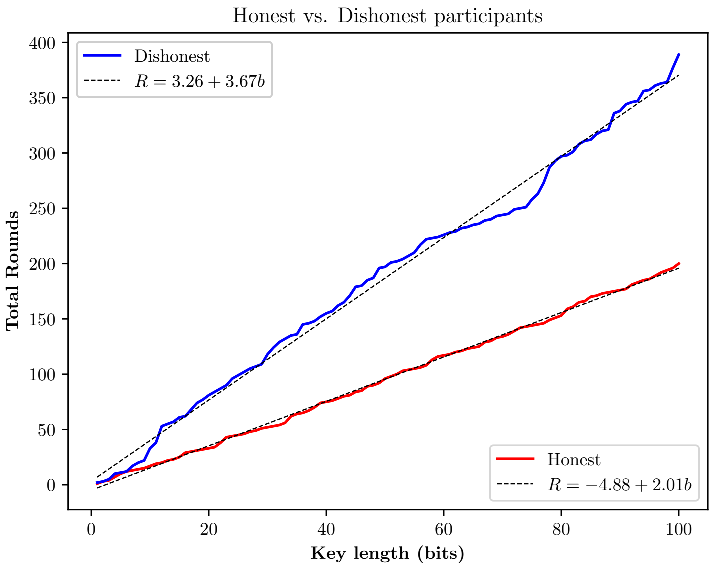
Figure: The four possible combinations of measurement bases of the GHZ state.

Example Usage

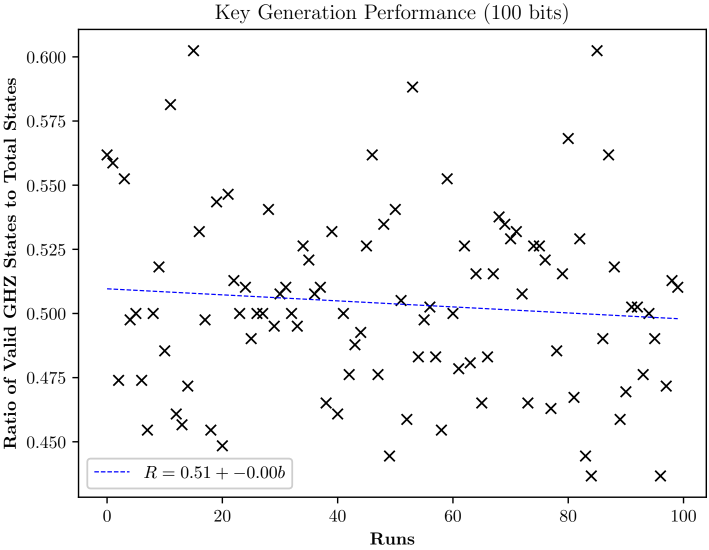
```
dirs = ['x', 'y', 'y']

result = create_and_measure(dirs)
measurements = getList(result)
>>> measurements = 011 # A got -x, B got +y, and C got +y
...
honesty = 0
A_bit = reconstruct(dirs, B_bit, C_bit, honesty)
>>> A_bit = 0
...
def reconstruct(dirs, B_bit, C_bit, honesty):
    if honesty == 0: # B and C cooperate
        return measure_table(directions, B_bit, C_bit)
    else: # B and C do not cooperate
        guess = random.randint(0, 1)
        return measure_table(directions, B_bit, guess)
```

Protocol Efficiency Analysis (Honest vs. Dishonest)



General performance



Conclusions

- We successfully implemented the protocol, and our results agree with the paper's prediction.
- The protocol is by no means practical or secure according to our classical definitions.
  - The communication component adds unnecessary overhead.
  - According to $\mathsf{KE}^{\mathsf{eav}}_{\mathcal{A},\Pi}(n)$ (p. 365 of [Katz, 2014]), if an adversary has the complete transcript `trans` from the protocol, they can predct with probability 1 what the final key bit is, such that

$$Pr(\mathsf{KE}^{\mathsf{eav}}_{\mathcal{A},\Pi}(n) = 1) = 1.$$

  - Any communication protection would require some degree of encryption (public- or private-key), which defeats the purpose of the protocol.

The End

References

Hillery, Mark and Bužek, Vladimír and Berthiaume, André (1999)
Quantum secret sharing
Physical Review A - Atomic, Molecular, and Optical Physics 3(59), 1829–1834.

IBM (2020)
IBM Quantum Experience
https://quantum-computing.ibm.com/.

Katz, Jonathan and Lindell, Yehuda (2014)
Introduction to modern cryptography
Chapman and Hall/CRC.