QUANTUM CRYPTOGRAPHY

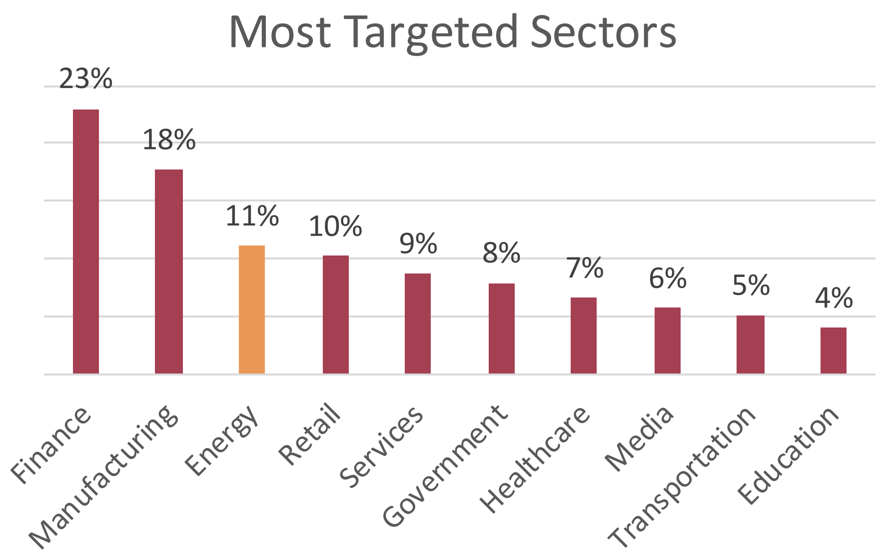
TEAM AVERAGE DODO ENJOYERS

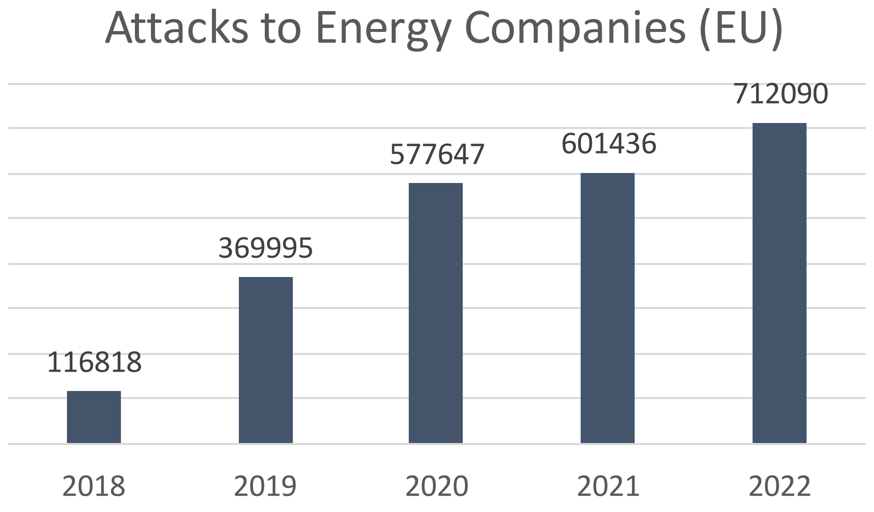
CAPUCINE BERAUD
FRANCESCO DE LUCA
CARLO ZOLLO
LUCA PARADISO
LEONARDO CRUCIANI

23.04.2023

AGENDA

- Introduction
  - Cybersecurity in the energy sector
  - Using QC to create randomness
- The Challenge
  - Understanding randomness measurements
  - Studying Toy noise models
  - Extracting randomness





INTRODUCTION

CYBERSECURITY IN THE ENERGY SECTOR

- Energy companies are the 3rd most targeted sector of cyberattacks
- The number of attacks to the sector have been steadily growing for the last 5 years
- Quantum cryptography may provide a useful tool to prevent attacks

RANDOMNESS

- Randomness is ***necessary*** for cryptography :
- It is used for :
  - cryptographic key generation
  - encryption
  - authentication

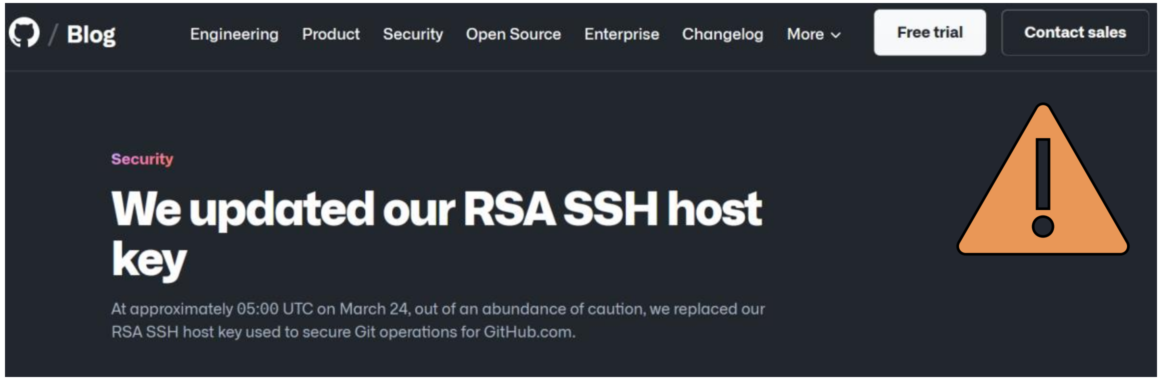
CLASSICAL

VS

QUANTUM

Pseudo-randomness

Example : open your slack !



Inherently random

What is the catch ? Noise !

environmental interference

THE CHALLENGE

QUANTIFYING RANDOMNESS IN A NOISY QUANTUM CIRCUIT

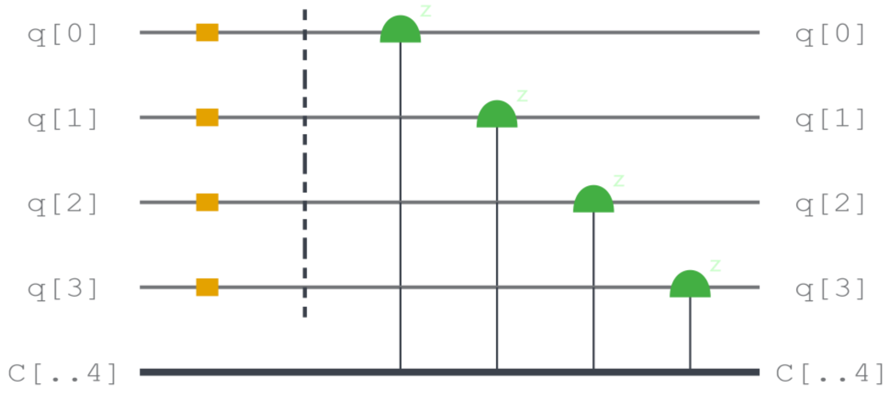
PRELIMINARY STEP

QUANTIFYING RANDOMNESS

- What is randomness? Why do we need it?
- How do we measure it?
  Why is the Shannon entropy not good enough?

$$\mathrm{H}_{min} = -\log \max_{\{\mathrm{x}\}} p(x)$$

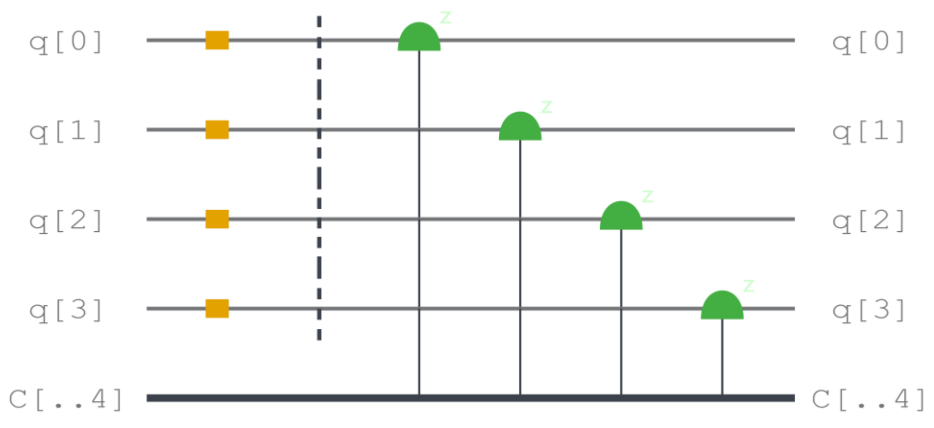
$$H_{shannon} = -\sum_{x} p(x) \log p(x)$$



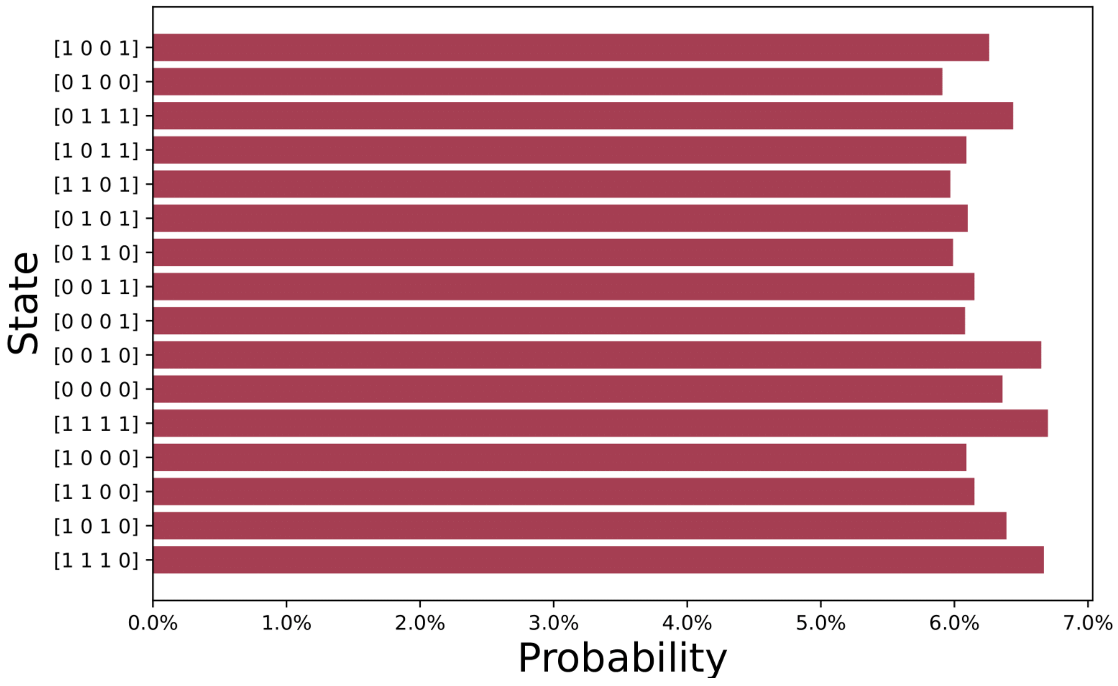
- What is the maximum randomness we can get given a number of qubits?
- How do we generate such a state?

TOY NOISE MODEL

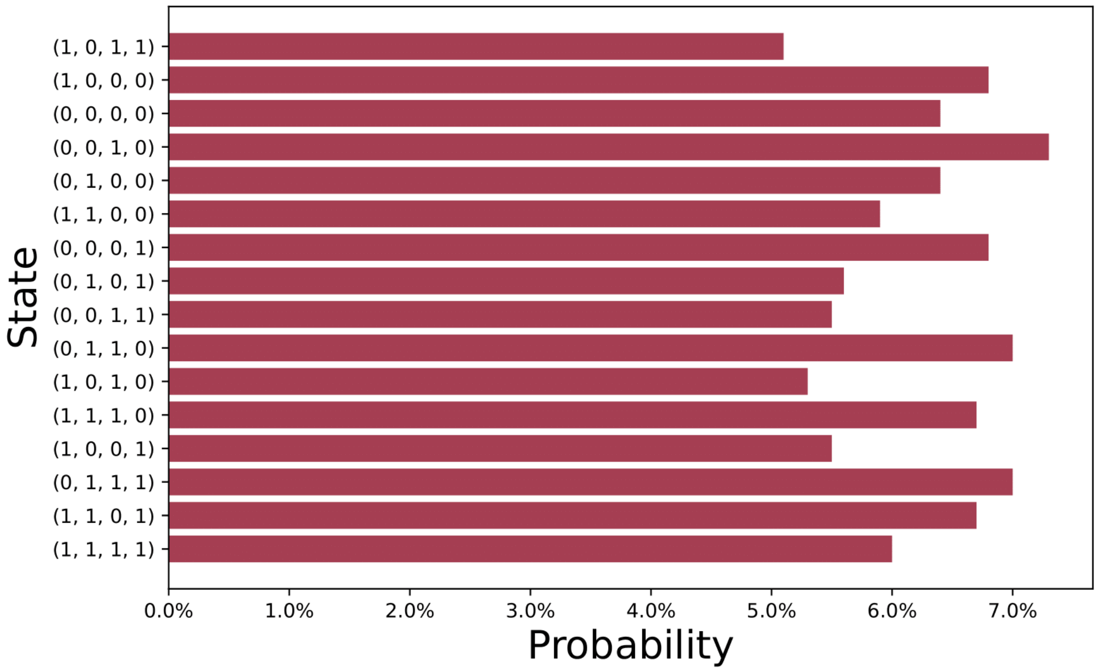
ALL HADAMARD CIRCUIT



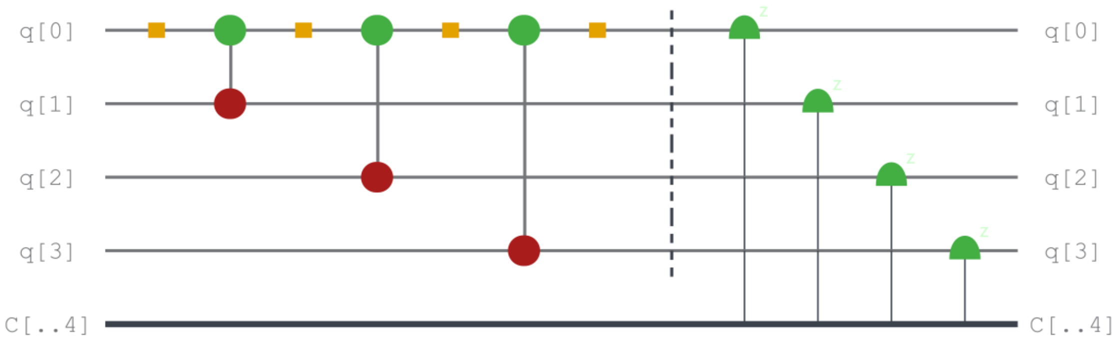
Noiseless



Noisy

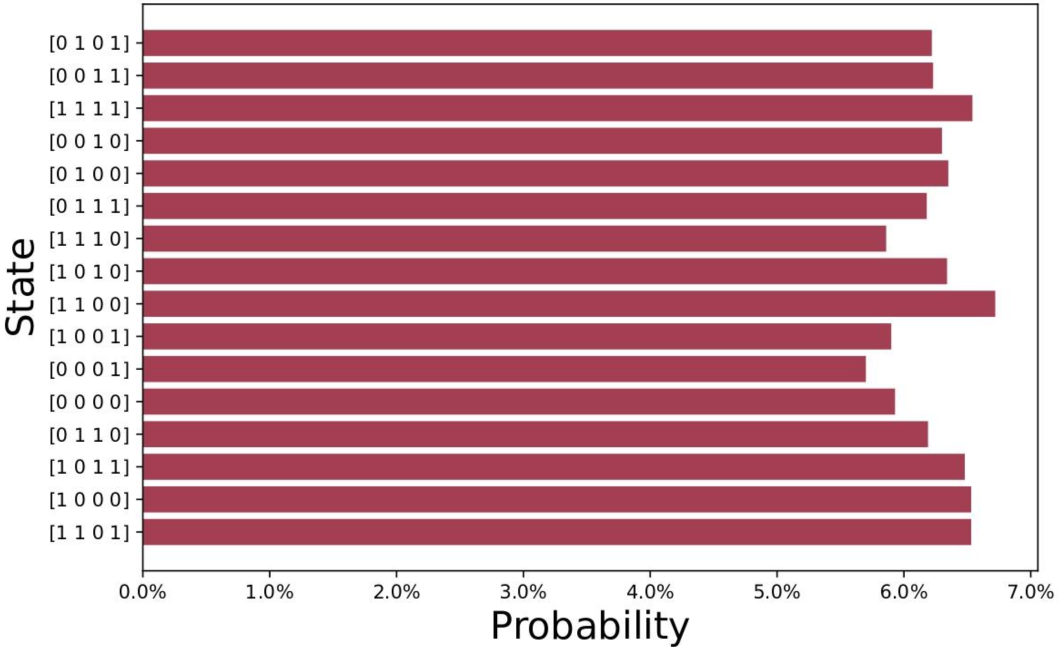


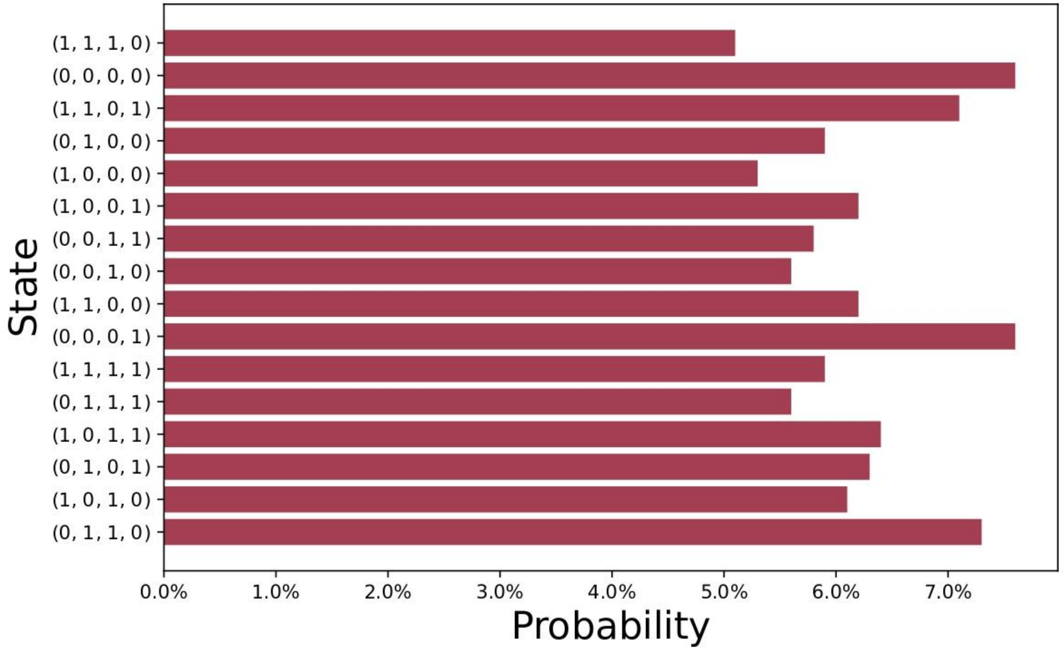
H AND CNOT CIRCUIT



Noiseless

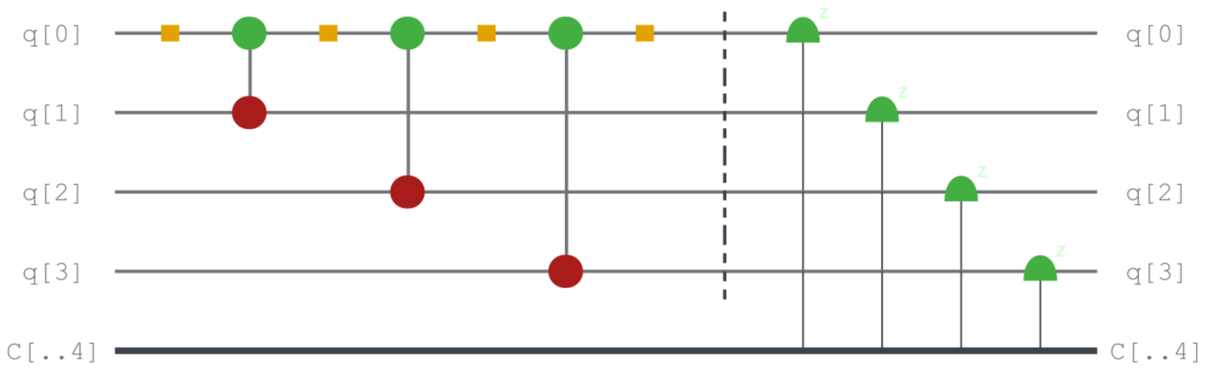
Noisy

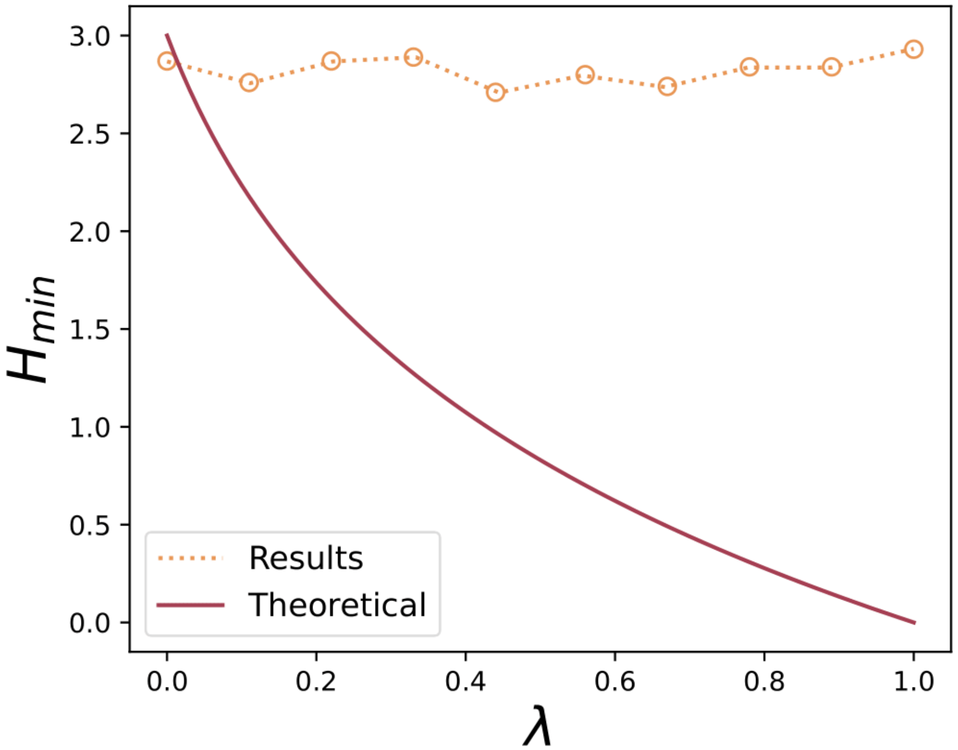




- A circuit with a lot of non-local gates fares much better than the local variant

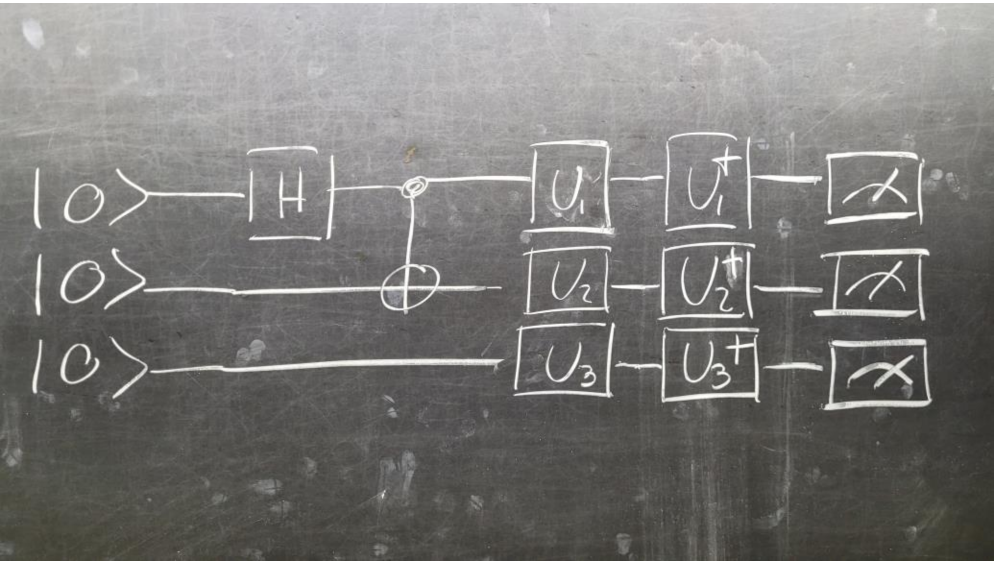
- Are non local gates safe against this noise model?



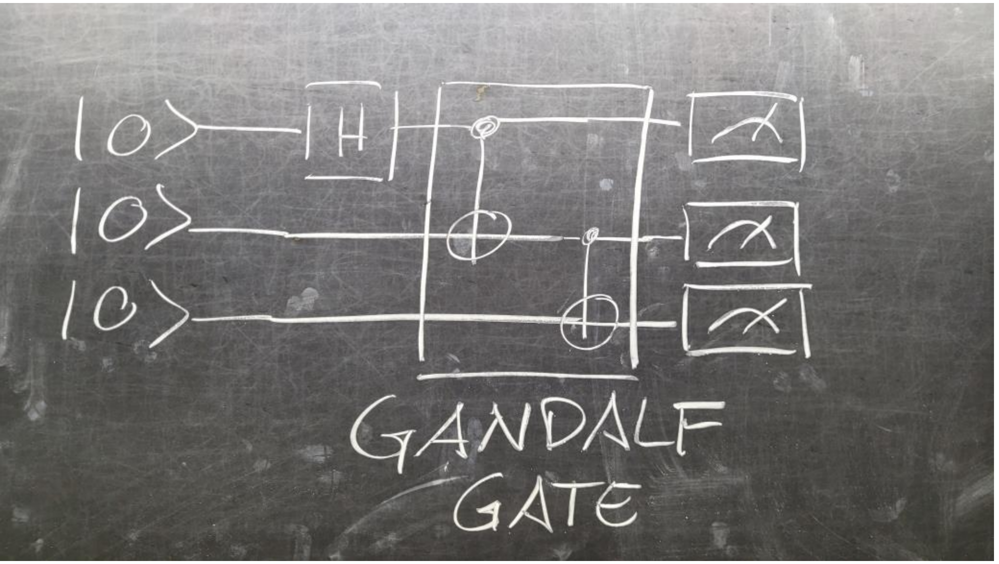


Min Entropy is bounded!

HOW TO HACK THE TOY NOISE MODEL ?



How does it works?



How to hack it ? The Gandalf gate

GENERAL NOISE MODEL

- Assume there is a general noise model

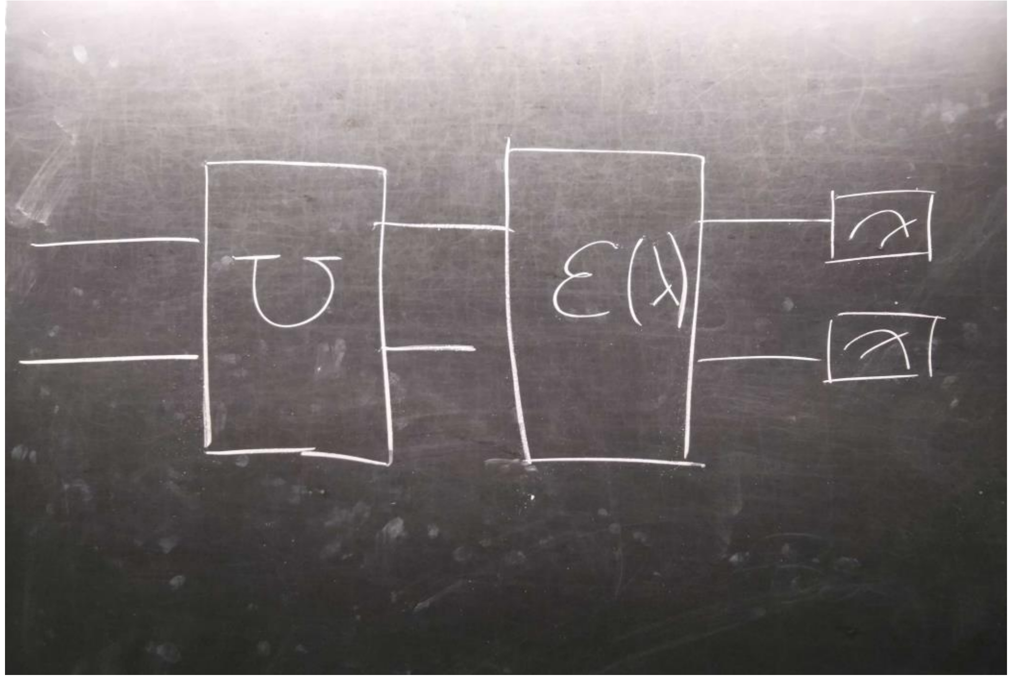
- Worst case scenario for any circuit : Hmin ≈0
- Single circuit is not enough
  - We need a certificate
- We implement it for the simplest case :
  - GHZ state
  - Alice measures in $\{X, Z\}$,
    Bob measures in a rotated with ϑ {X,Z}
  - Use CHSH inequality :
  - With A and B's measurement,

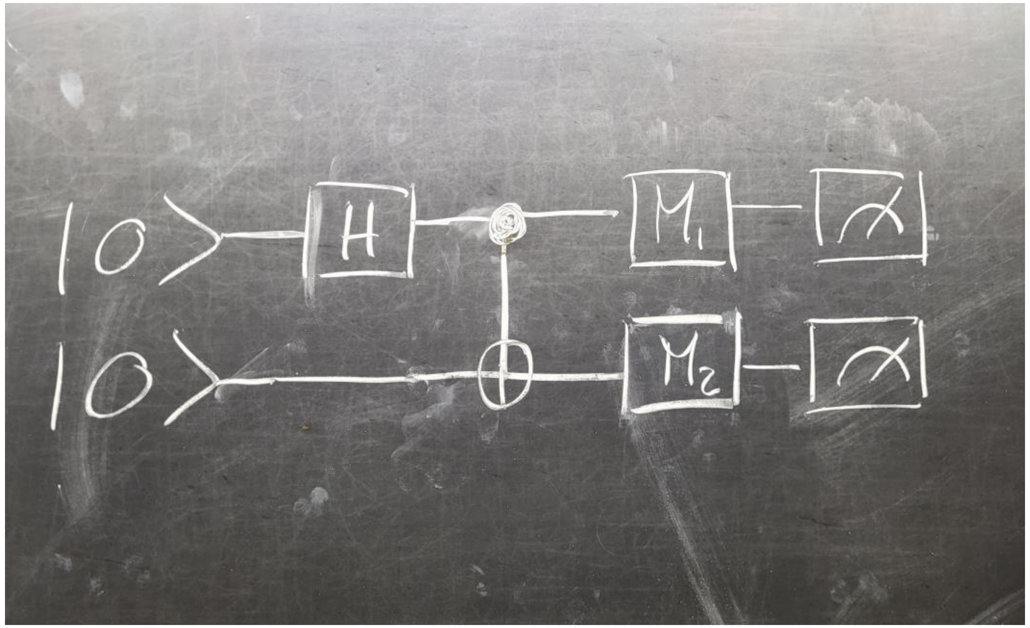
  if $C \approx 2\sqrt{2}$

  We still output the GHZ state!

  if $C \geq 2$: pretty good !

We store these results





RANDOMNESS EXTRACTORS

- GHZ is not maximally random …

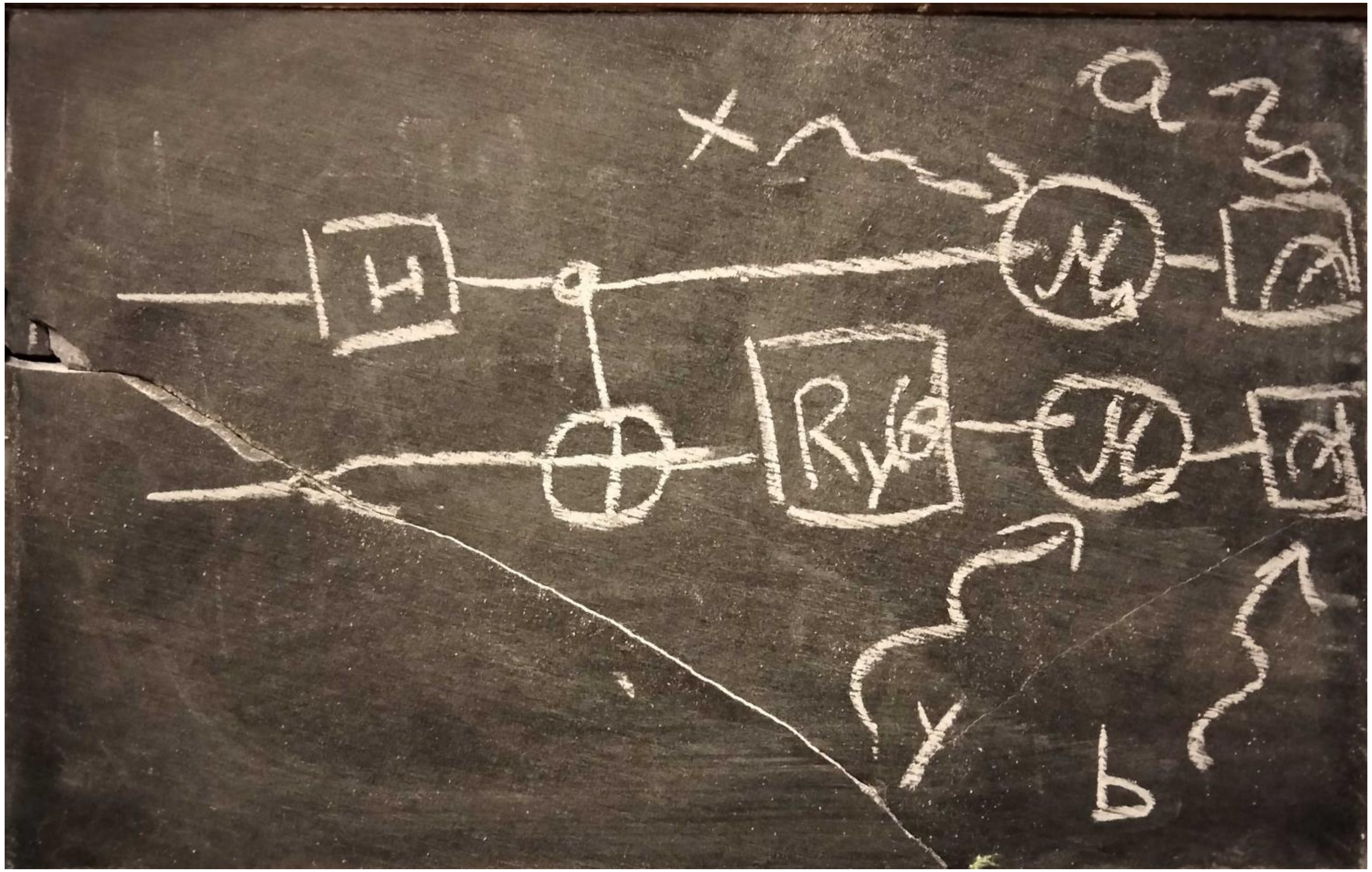
  ➡ We can use it to extract randomness from it in presence of noise!
- How ?

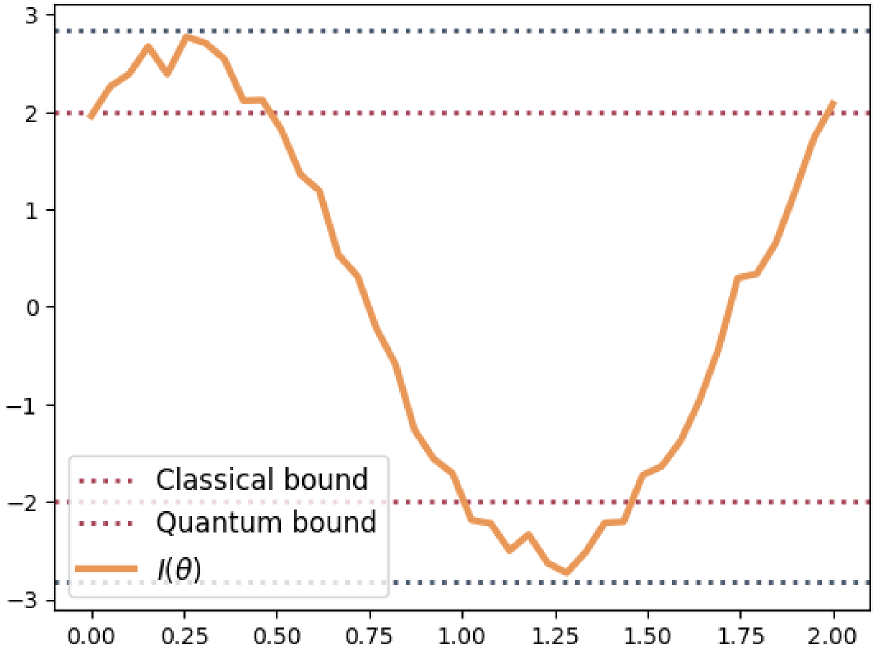
  ➡ Study a protocol that guarantees the ouput violates a CHSH inequality

  ➡ If the inequality is violated we are guaranteed there's some randomness in it, despite the noise

  ➡ A randomness extractor will help us get more from just one: It's part of the Quantum Origin product from Quantinuum

The approach is Device-Independent! No need to know the exact noise model





OUR CERTIFICATE IMPLEMENTATION

- Build the parametrized circuit
- Collect statistics $(a_1, b_1 \ldots, a_n, b_n)$ choosing the basis measurement with the string $(x_1, y_1 \ldots, y_n, y_n)$
- Statistics is used to compute C
- We would not choose every theta value

GENERAL PROTOCOL

- Alice has a key t = (t_1, t_2) Takes t_1 to generate a bit string s = $(x_1, y_1 \ldots, y_n, y_n)$
- Alice uses s to produce r = $(a_1, b_1 \ldots, a_n, b_n)$ string of measurements with her device
- If the certificate approves r, Alice uses an extractor and t_2 to have a smaller string $\bar{r}$ which is truly random
- $\bar{r}$ is then added to t to enhance this protocol and have a key of the desired length

A SIMPLE EXAMPLE OF THE EXTRACTOR'S WORK

- Fixed theta such that the parametrized circuit violates CHSH inequalities

$$\theta > 2$$

- We make a run with 4 shots, receiving a bit string:

$$r = (0, 1, 1, 1, 0, 0, 1, 0)$$

- To remove garbage bits and receive a truly random string we use the extractor, receiving:

$$\bar{r} = (1, 0, 0, 0)$$

Our github : https://github.com/Kraji/ICTP-QNTM-Hackathon-April-2023-team-7/tree/Luca/Average%20Dodo%20enjoyers%20solution

Thank you for listening

And for a wonderful Hackathon !