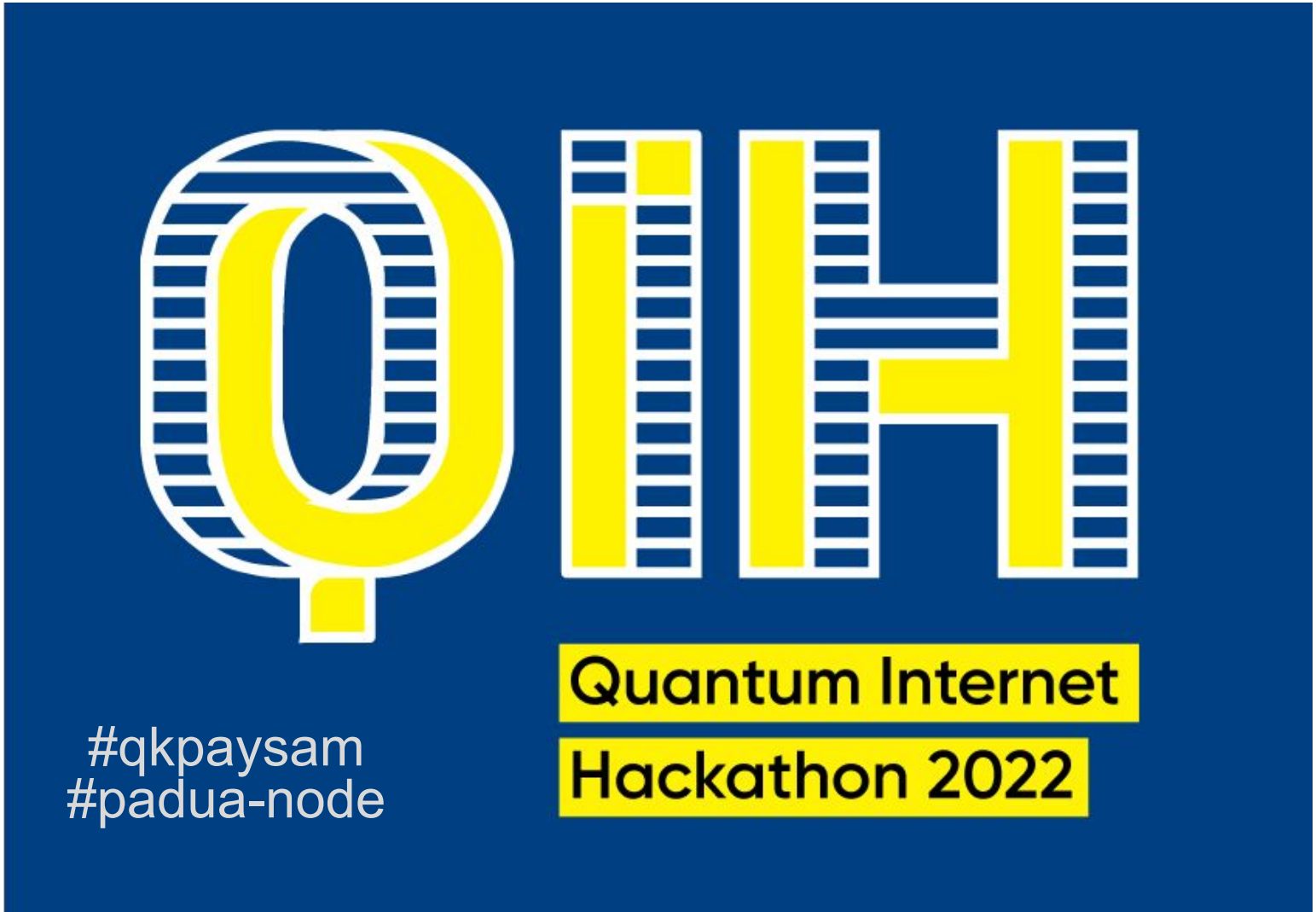

QIH
Quantum Internet
Hackathon 2022
#qkpaysam
#padua-node

Our group

Tommaso Faorlin

Alessandro Marcomini

Francesco De Giudici

Edoardo Rossi

Christy Jo Manthara

The challenge

OUR GOAL:

Learn to implement a full QKD protocol in a new library

- Implementation of the **E91 protocol** on the *Randstad* node.
- Implementation of a **eavesdropper** performing an intercept and resend attack
- Worked with **noisy qubits** and tried to distinguish eavesdropping from noise in the quantum channel

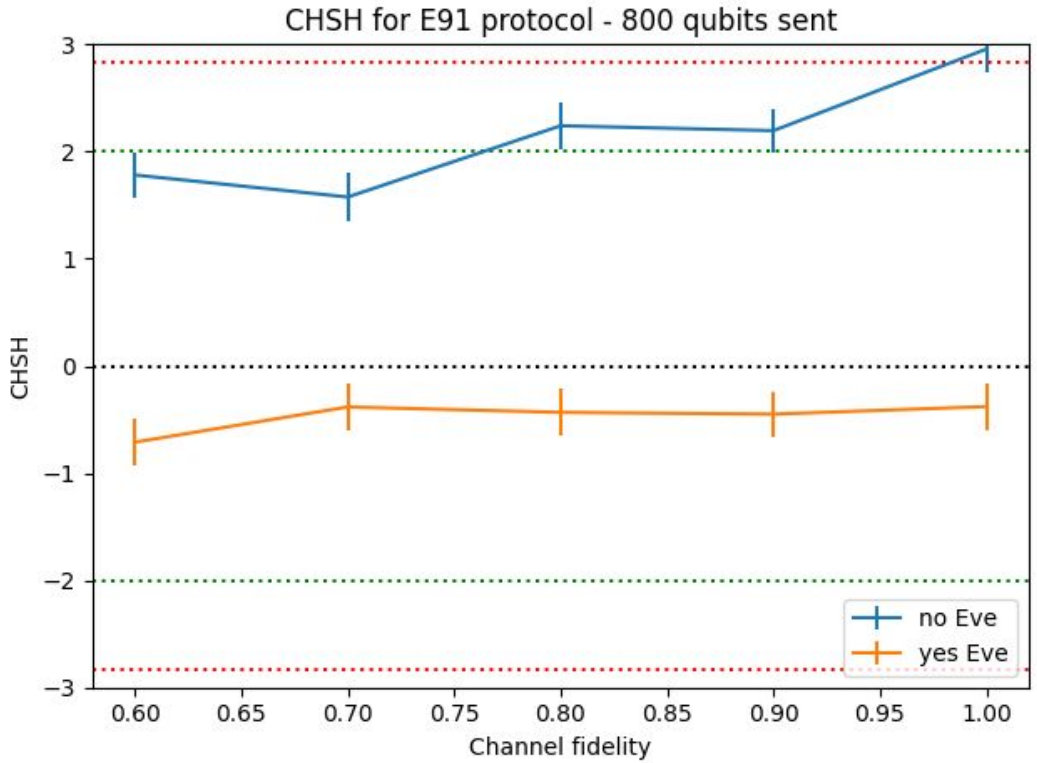
The system has been **successful with ideal channel** (F=1) condition and have **successfully detected** the presence of eve in the network.


```
"round_result": [
  {
    "app_alice": {
      "secret_key": "0101101001111101010111001110110011111100101"
    },
    "app_bob": {
      "secret_key": "0101101001111101010111001110110011111100101"
    }
  }
],
"instructions": [
```

Almost complete with the **information reconciliation part** and the detection of eavesdropper under fidelity <1.

```
2.8476747424115842
Alice parities:  ['0', '0', '0', '0', '0', '0', '0', '0', '0', '0']
Bob parities:  ['0', '0', '0', '0', '0', '0', '0', '0', '0', '0']
Alice parities:  ['0', '0', '0', '0', '0']
Bob parities:  ['0', '0', '0', '0', '0']
Alice parities:  ['0', '0', '0']
Bob parities:  ['0', '0', '0']
Alice parities:  ['0', '0']
Bob parities:  ['0', '0']
```

What if Eve is present (intercept-and-resend)?



Next steps

- **Finish** the Cascade protocol and adjust key rate based on S parameter
- **Autenticate** the classical channel
- **Work** (against the almost-impossible) in the distinction between eavesdropping and noise in the quantum channel