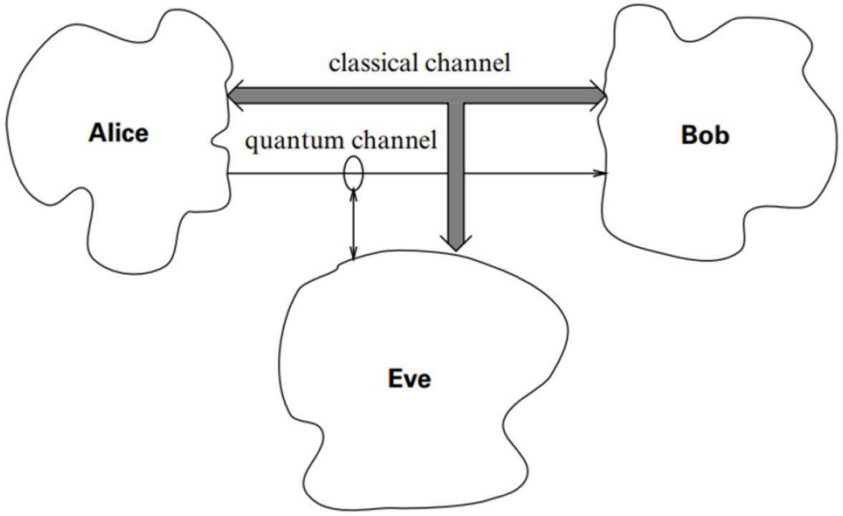
BB84 Protocol

Quantum Computing and Quantum Internet (WS 2025/26)

Carlo Mazzanti and Esther Kummetz

Background

- Protocol to produce a quantum key
- For each bit, Alice randomly chooses the bit-value and the basis (Z or X) used for encoding
- Alice sends to Bob the encoded Qubit
- Bob chooses randomly a basis to perform the measurement on the received Qubit and saves the result
- Alice and Bob exchange the used basis and save only the bits encoded and measured in the same basis
- If Eve performs eavesdropping, she performs measurement using random basis and sends the Qubit in the measured state to Bob (possibly changing information)



Simulations Overview

Parameters:

- L_{init} length of the initial bits string
- p probability of channel error
- k fraction of the disclosed quantum key

Scenarios:

- Ideal Conditions
- Channel errors occur
- Eavesdropping in the absence of channel errors
- Eavesdropping combined with channel errors

Metrics:

- Global $R_{mismatch}$, ratio of mismatched bits between Alice and Bob
- Z-basis $R_{mismatch}$, ratio of mismatched bits when Alice uses the Z-basis for encoding
- X-basis $R_{mismatch}$, ratio of mismatched bits when Alice uses the X-basis for encoding
- $P_{undetected}$, probability that Eve remains undetected after the partial disclosure of the key

Simulations configuration:

- Mismatch ratio's experiments are repeated 1000 times for each parameter composition
- Undetected eavesdropping probability's experiments are repeated 10000 times for each parameter composition
- Each plot's point represents the mean metric with a confidence interval of 99%

Qiskit Circuit Model

The circuit is composed by two channels:

- Channel from Alice to Eve, for simulating qubit interception
- Channel from Eve to Bob, for simulating the Eve's measure and resend strategy

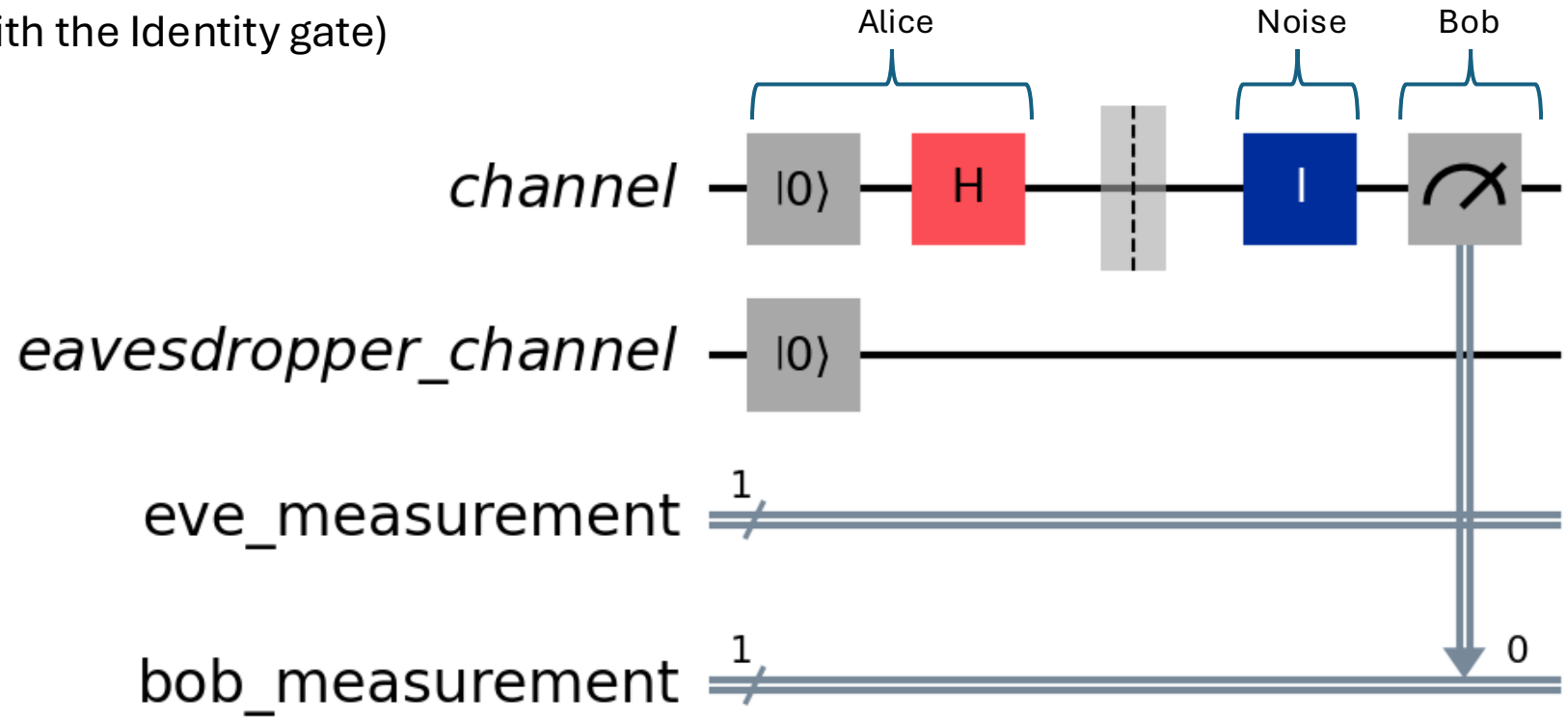
If the no-eavesdropping scenario is selected, Alice and Bob are directly connected by the first channel.

The channel error is modelled by a Noise Model, represented by a gate on the currently active channel

Qiskit Circuit Model

Example of circuit execution (no-eavesdropping scenario):

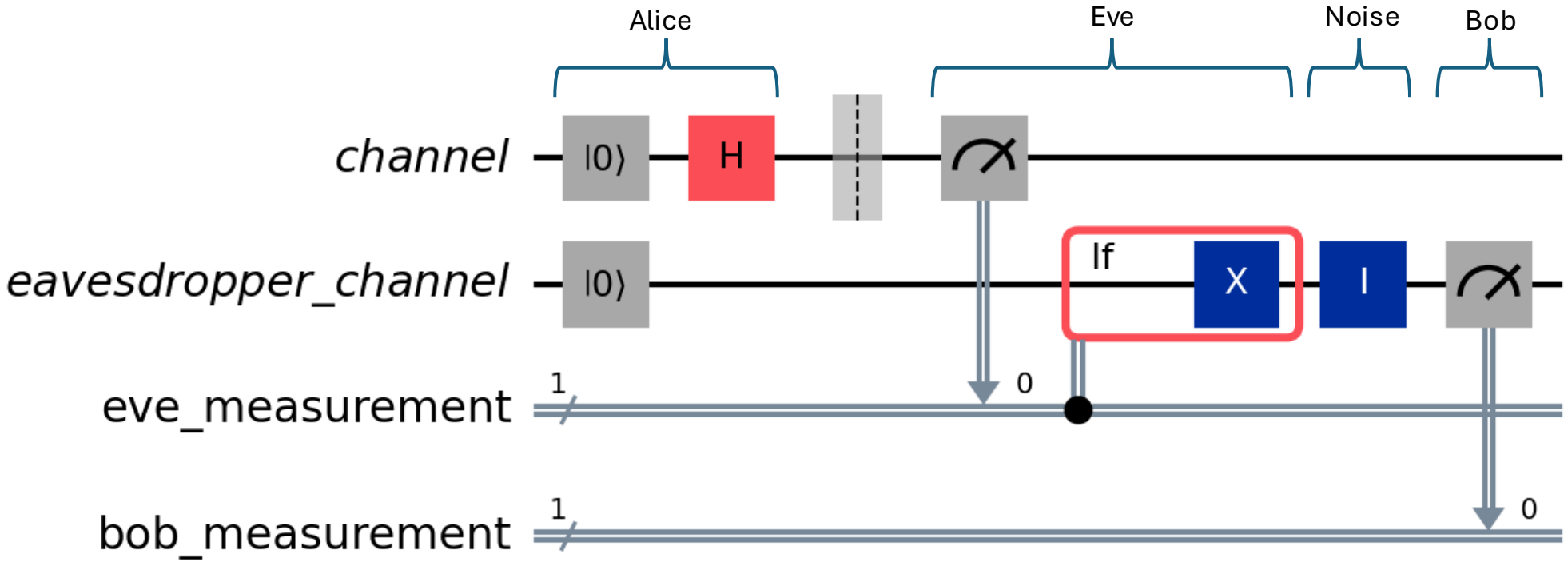
- Alice sends $|+\rangle$
- Bob measures in Z basis
- Channel errors applied with the I gate (not to be confused with the Identity gate)



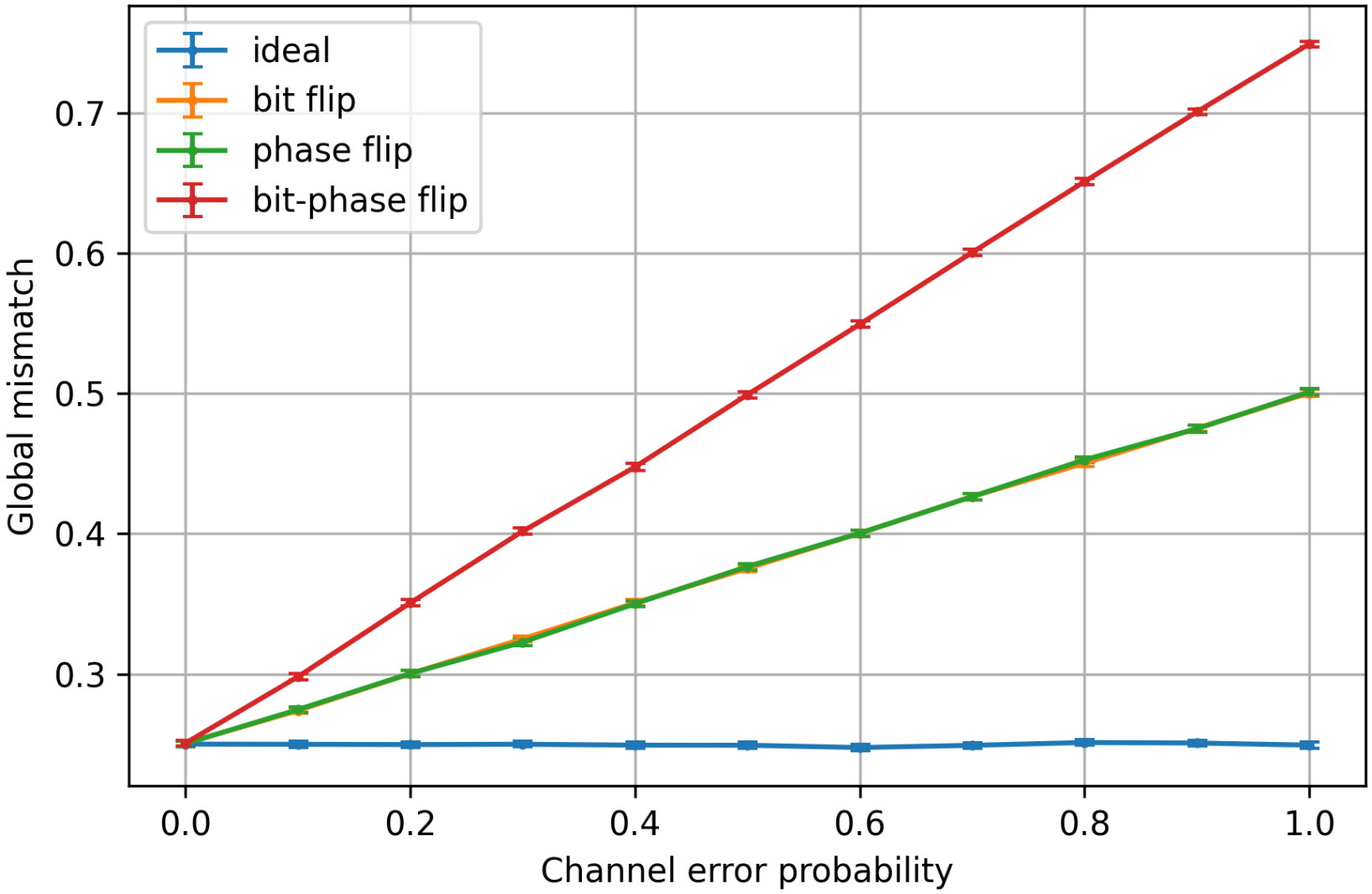
Qiskit Circuit Model

Example of circuit execution (eavesdropping scenario):

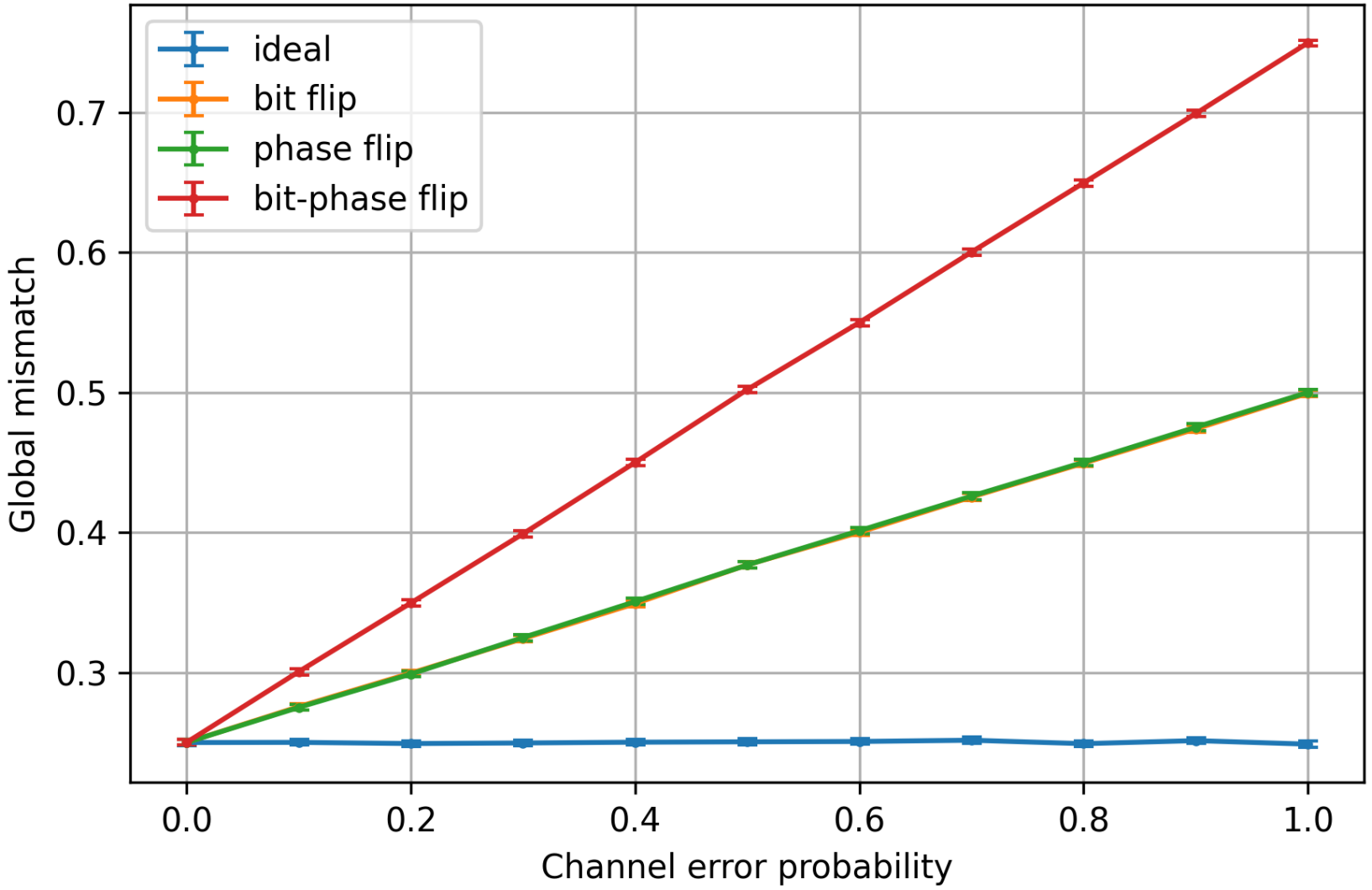
- Alice sends $|+\rangle$
- Eve measures in Z basis, obtains measurement result 0
- Eve resends the qubit $|0\rangle$
- Bob measures in Z basis



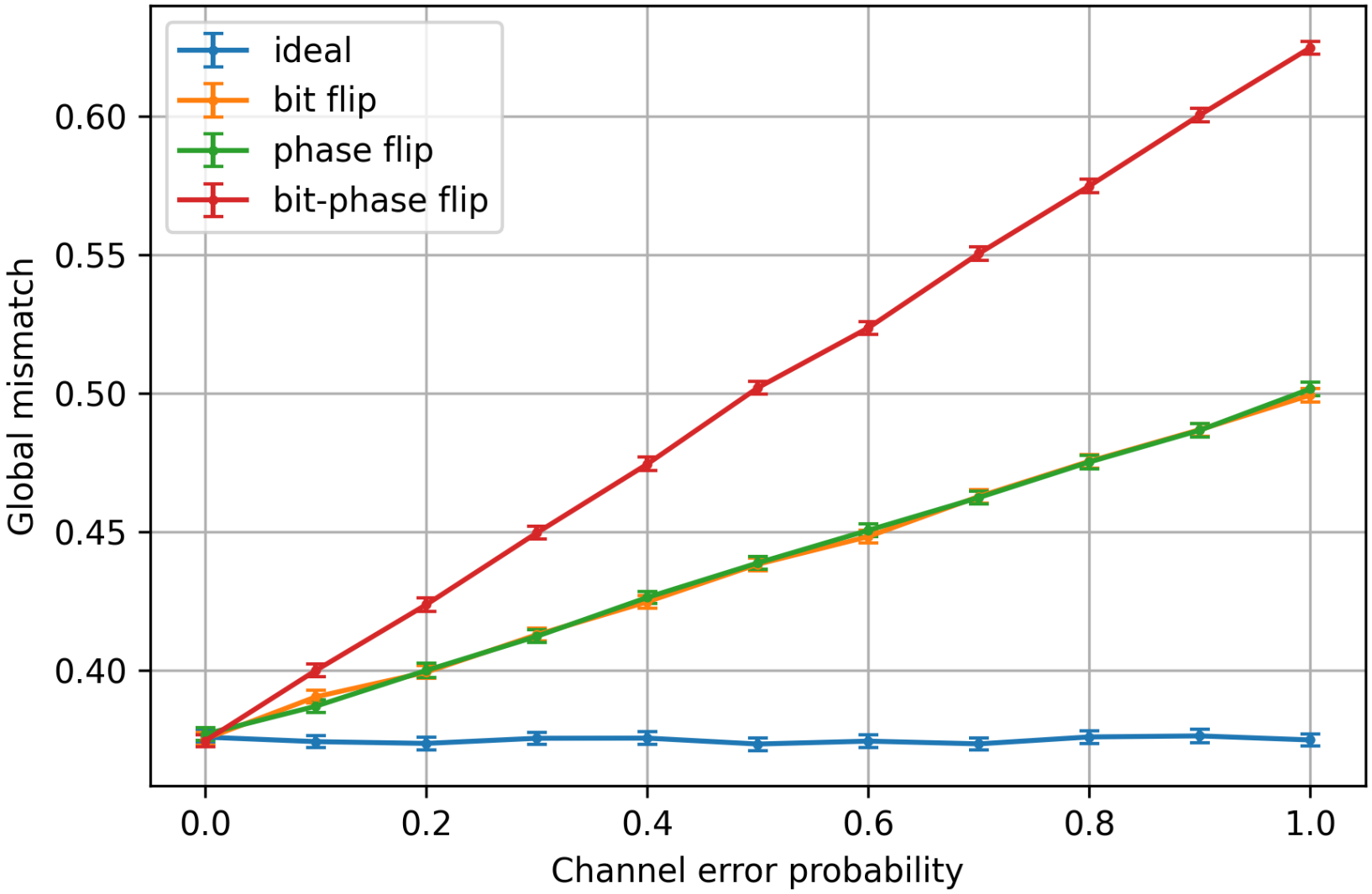
Global Mismatch Ratio – No Eavesdropping [Quantum Savory]



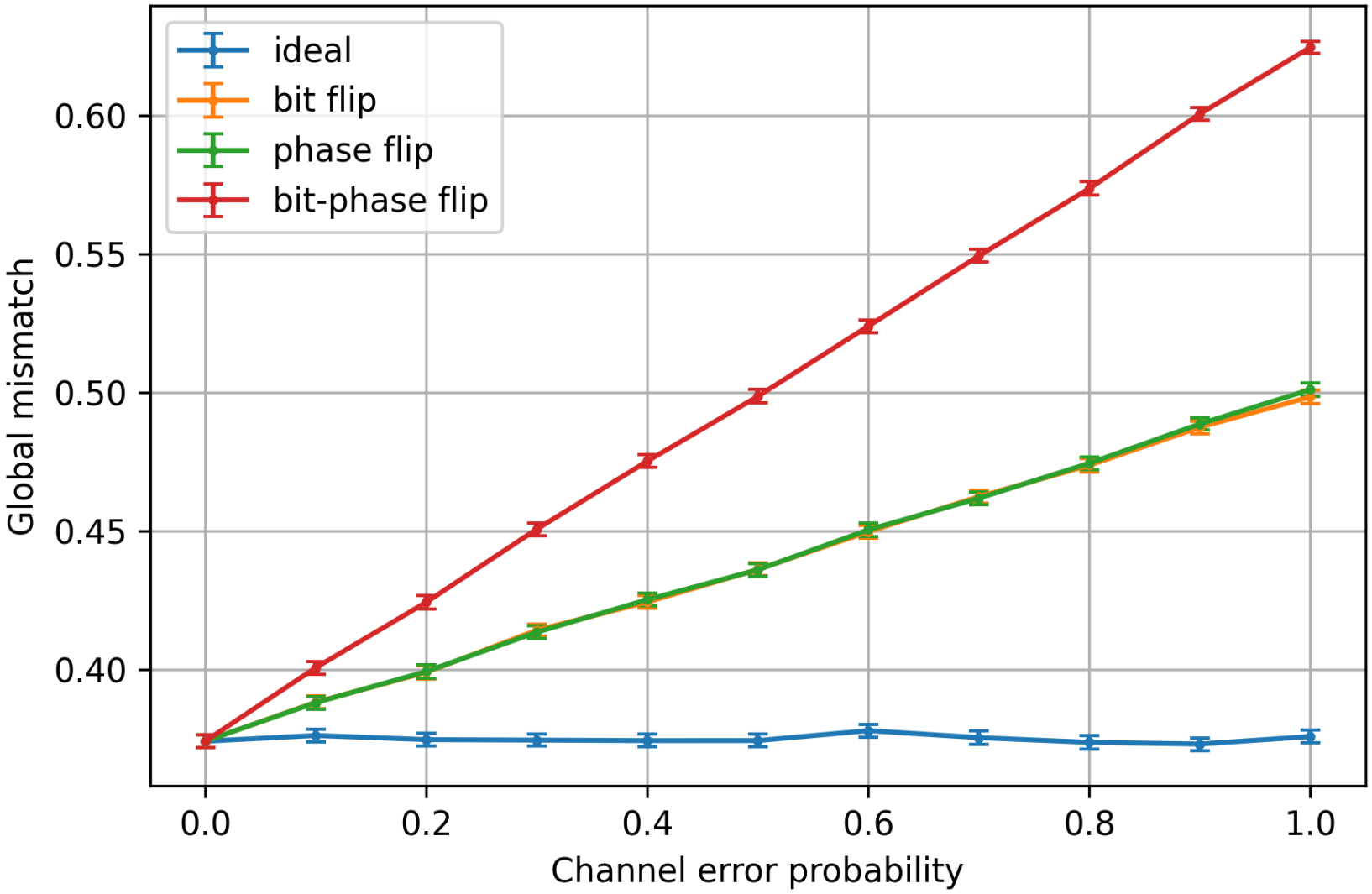
Global Mismatch Ratio – No Eavesdropping [Qiskit]



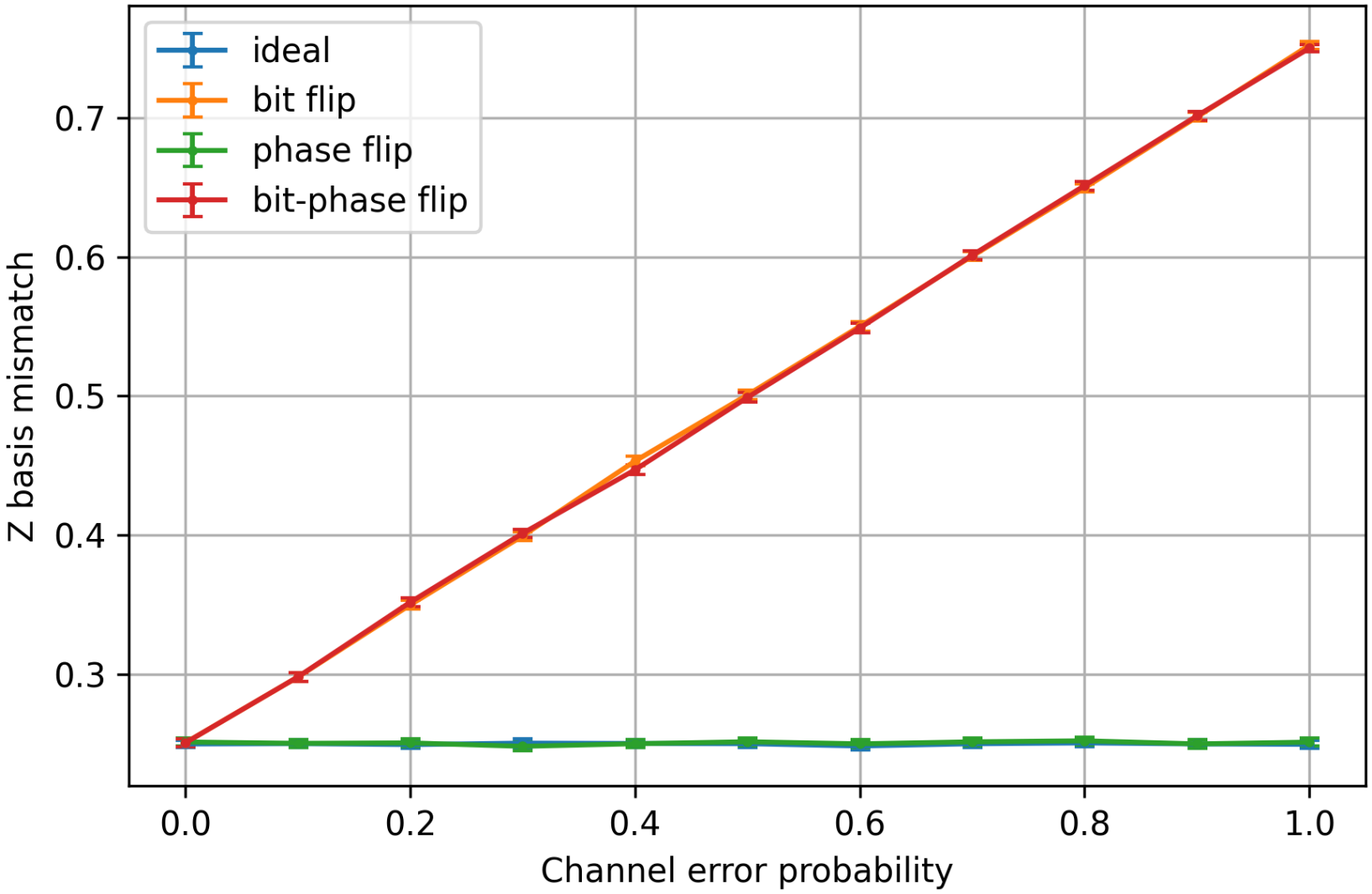
Global Mismatch Ratio – Eavesdropping [Quantum Savory]



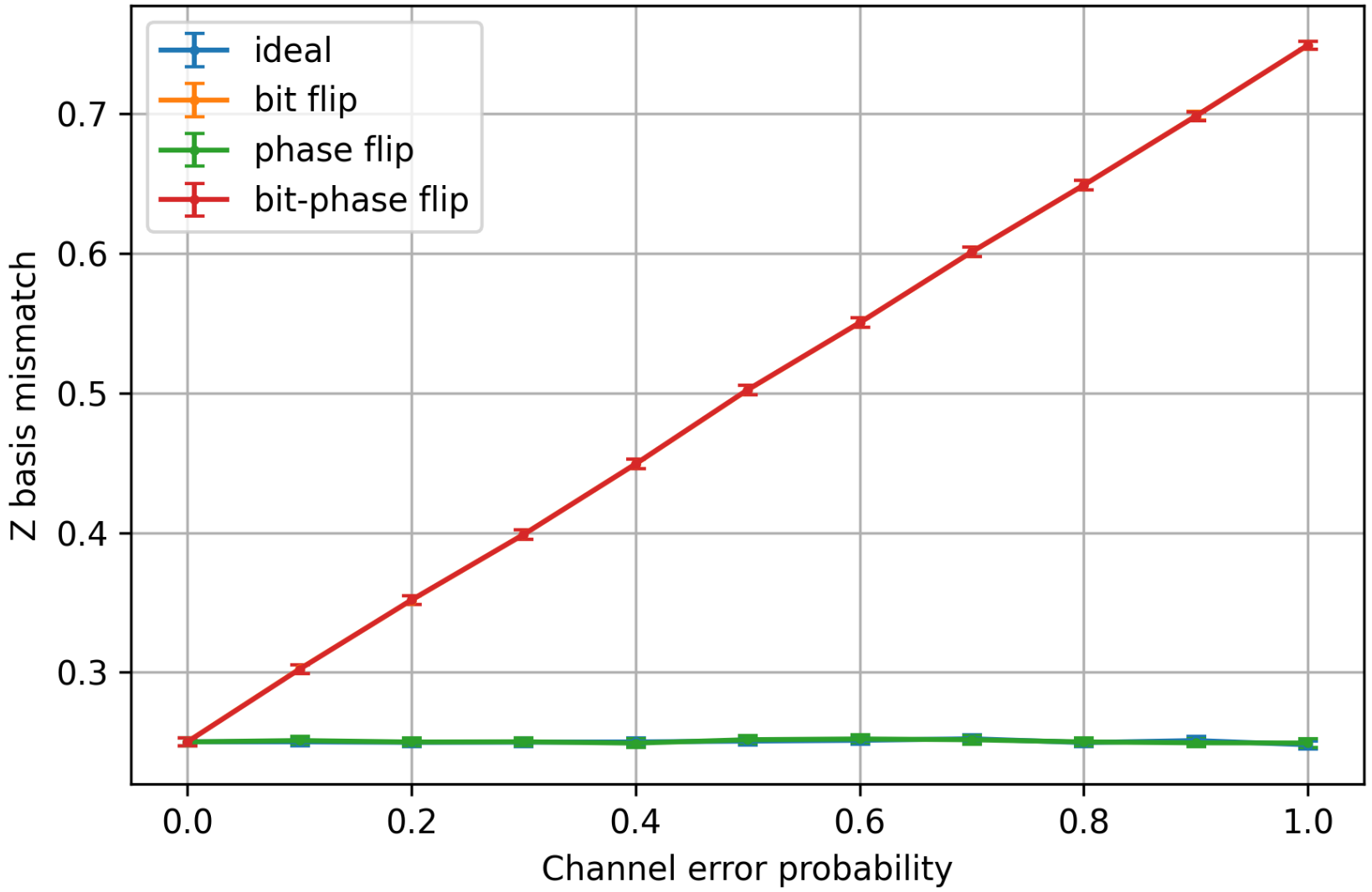
Global Mismatch Ratio – Eavesdropping [Qiskit]



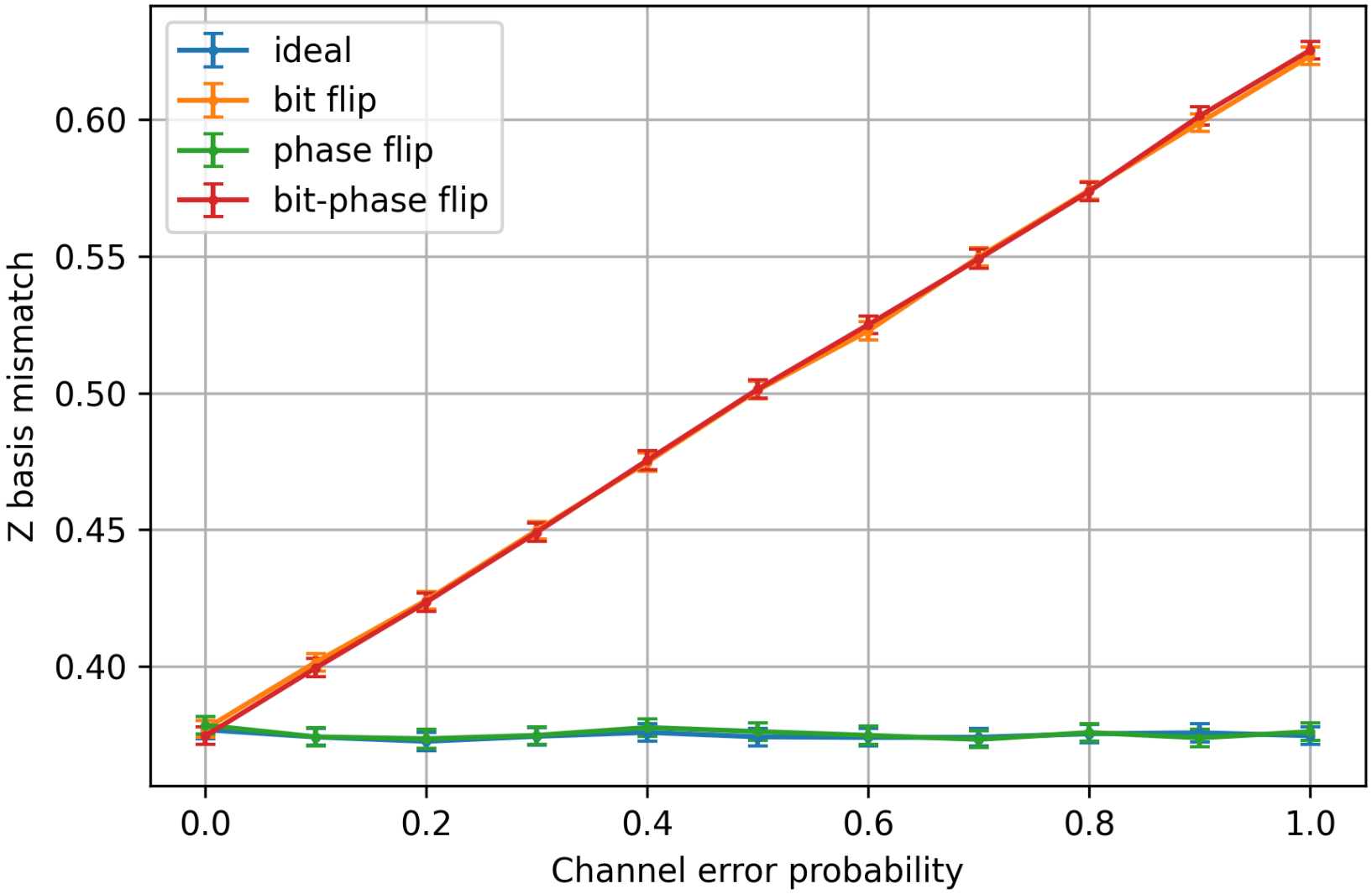
Z basis Mismatch Ratio – No Eavesdropping [Quantum Savory]



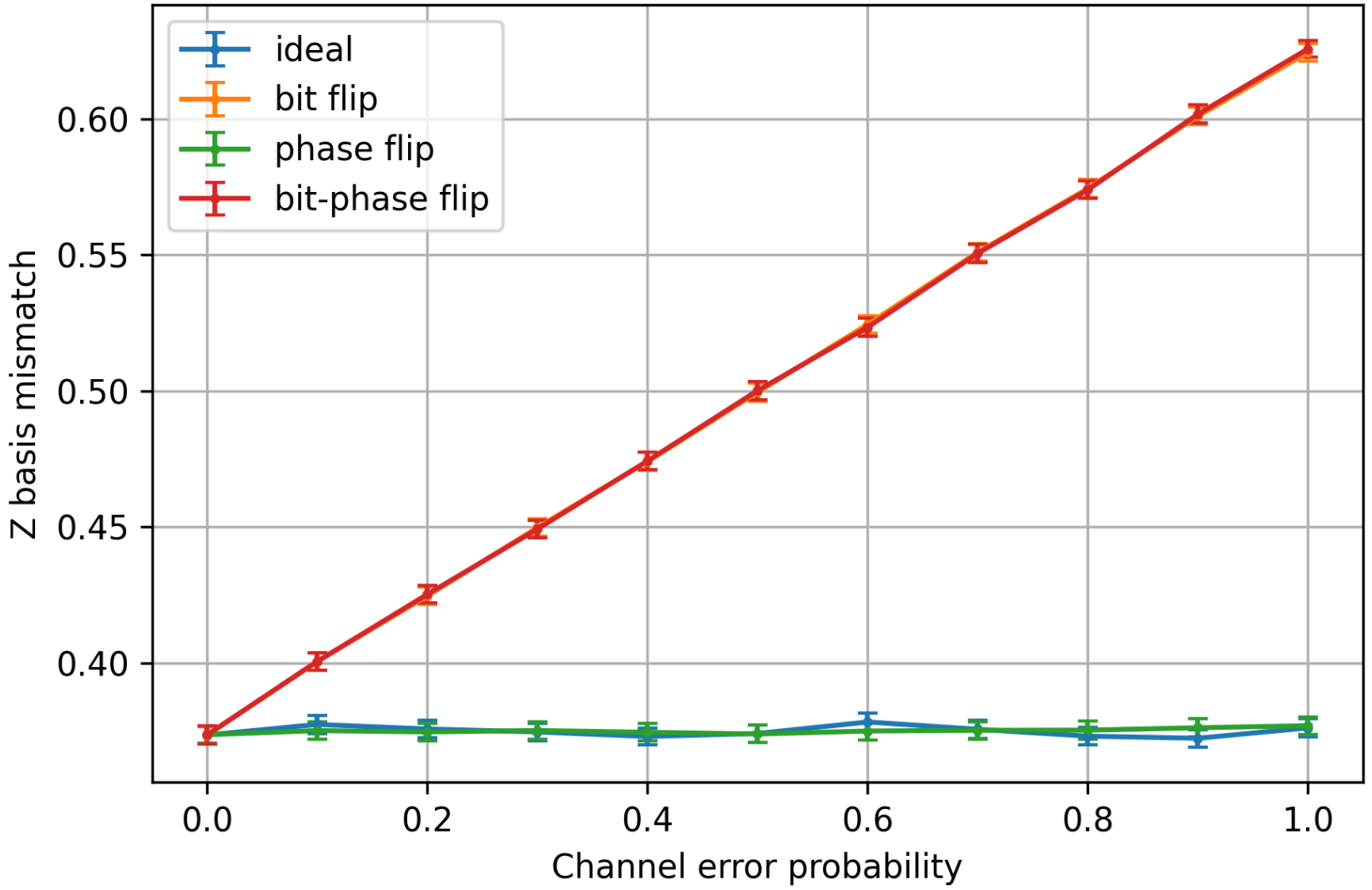
Z basis Mismatch Ratio – No Eavesdropping [Qiskit]



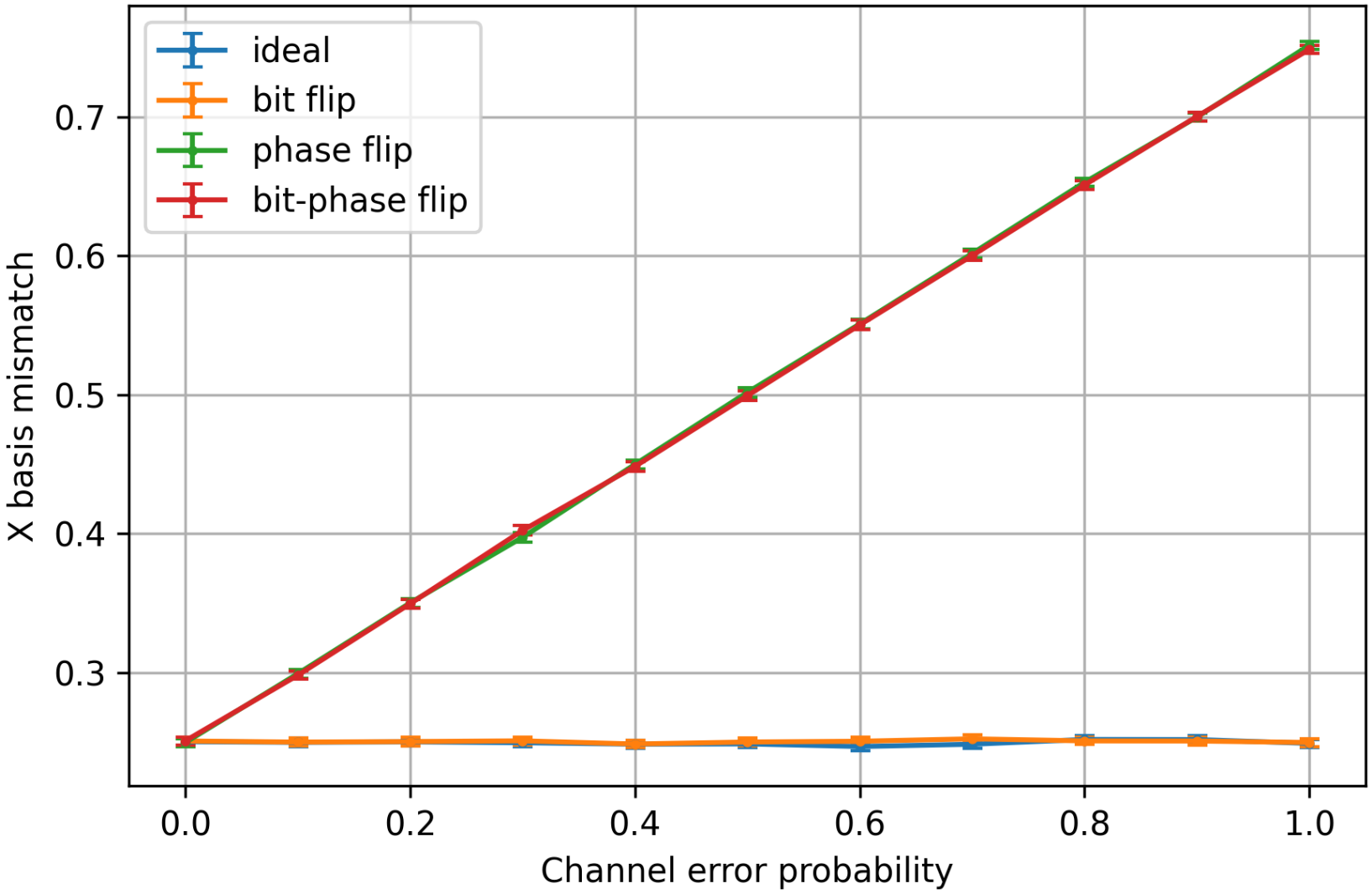
Z basis Mismatch Ratio – Eavesdropping [Quantum Savory]



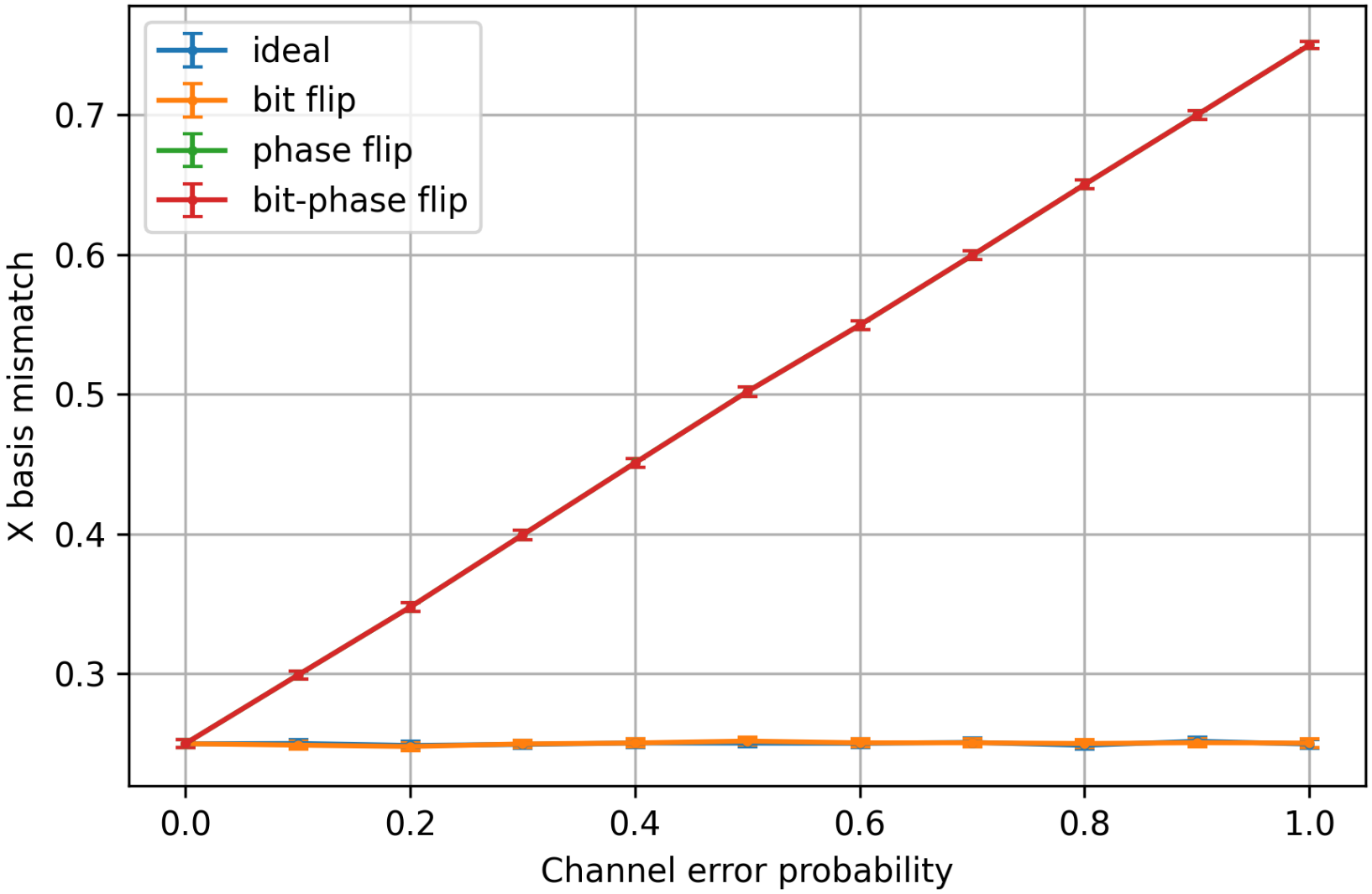
Z basis Mismatch Ratio – Eavesdropping [Qiskit]



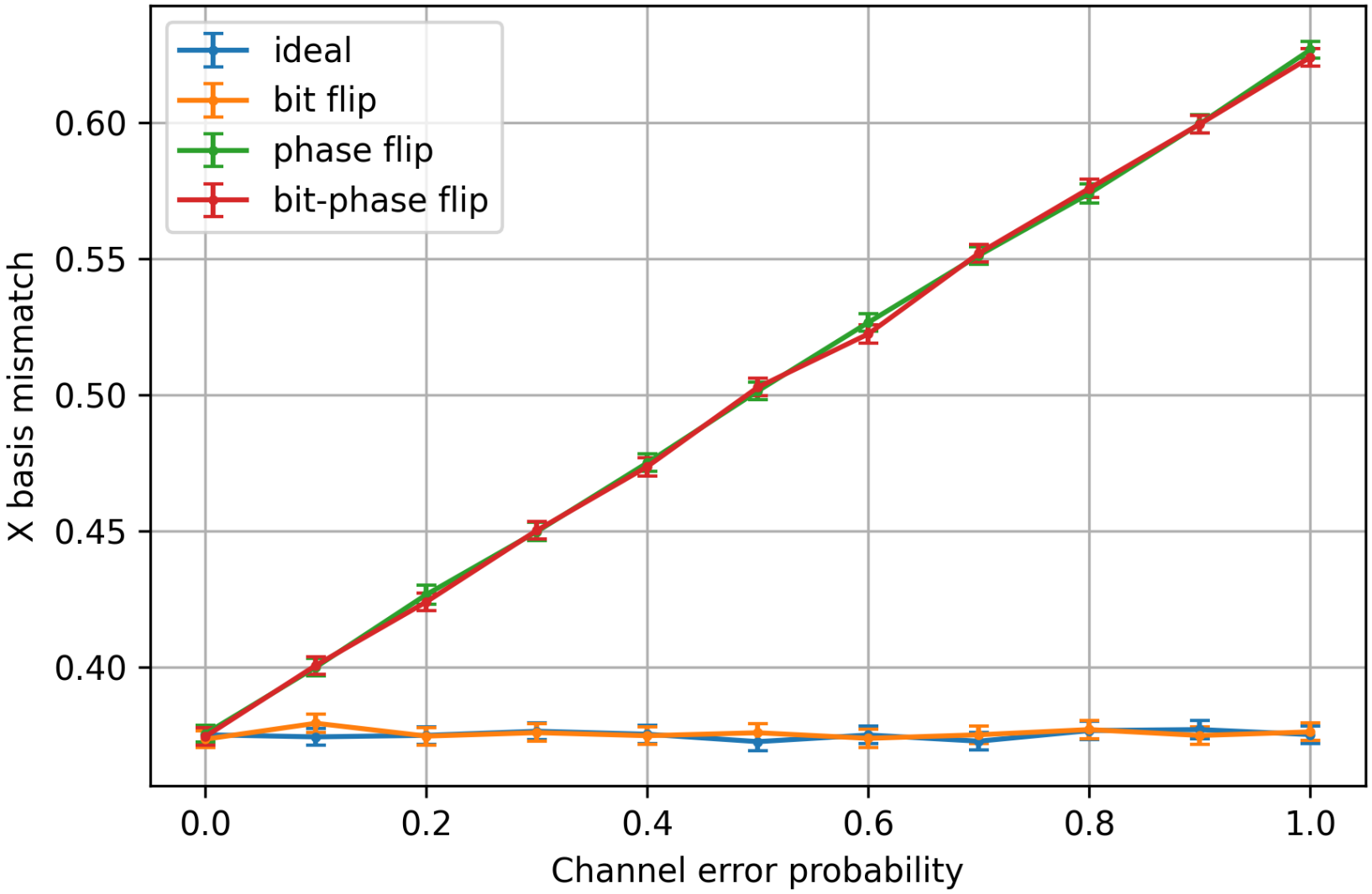
X basis Mismatch Ratio – No Eavesdropping [Quantum Savory]



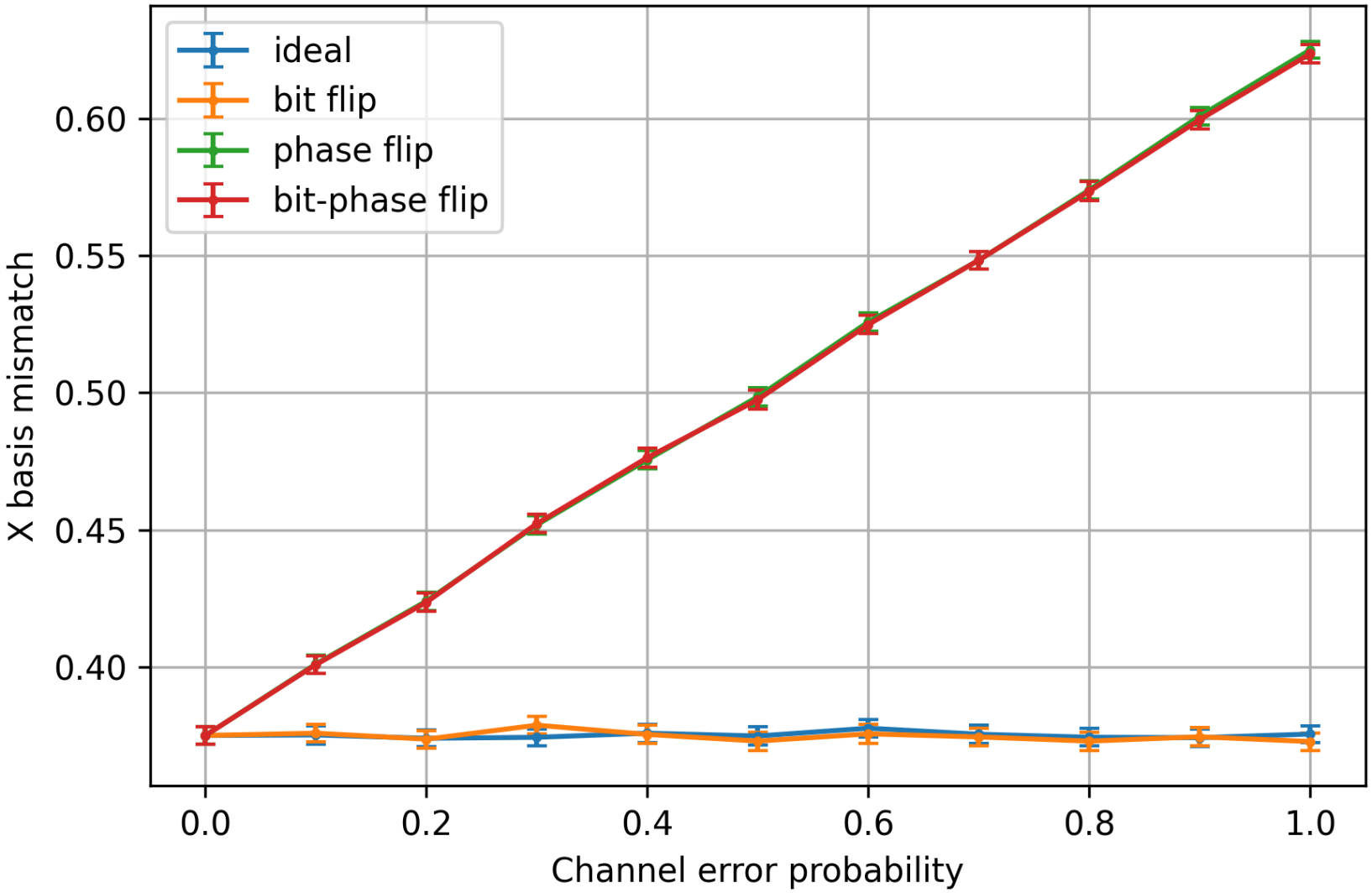
X basis Mismatch Ratio – No Eavesdropping [Qiskit]



X basis Mismatch Ratio – Eavesdropping [Quantum Savory]



X basis Mismatch Ratio – Eavesdropping [Qiskit]



Mismatch ratios – Conclusions

- There isn’t a particular encoding that is less error-prone under any conditions
- Z-basis is phase flip resistant but bit flip sensible
- X-basis is bit flip resistant but phase flip sensible
- With bit-phase flip errors, both basis will be sensible

Eavesdropping detection strategy

No channel errors scenarios:

- The mismatch of at least one bit in the disclosed fraction of the key

Channel errors scenarios:

- Threshold of mismatched bits in the disclosed fraction of the key based on the expected value of mismatched bits:

$$Threshold = P\{E\} \cdot Length_{disclosed\ key}$$

- The simulations are carried out with a fixed 20% channel error probability

Eavesdropping detection strategy

Probability of error in the Bit Flip scenario

$$P\{E\} = P\{E \mid Z\} \cdot P\{Z\} + P\{E \mid X\} \cdot P\{X\} = p \cdot \frac{1}{2} + 0 \cdot \frac{1}{2} = \frac{p}{2}$$

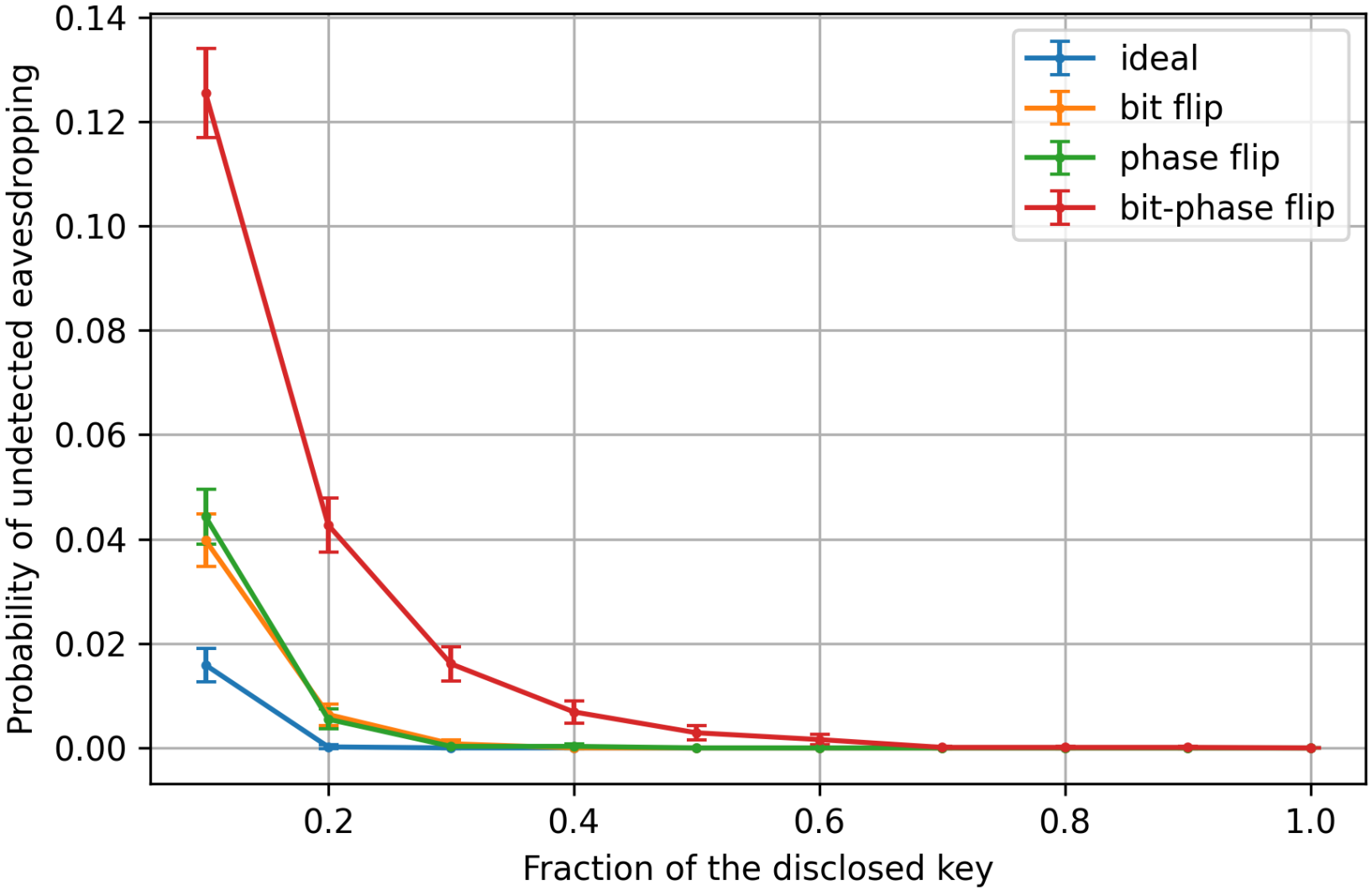
Probability of error in the Phase Flip scenario

$$P\{E\} = P\{E \mid Z\} \cdot P\{Z\} + P\{E \mid X\} \cdot P\{X\} = 0 \cdot \frac{1}{2} \cdot p + 1 \cdot \frac{1}{2} \cdot p = \frac{p}{2}$$

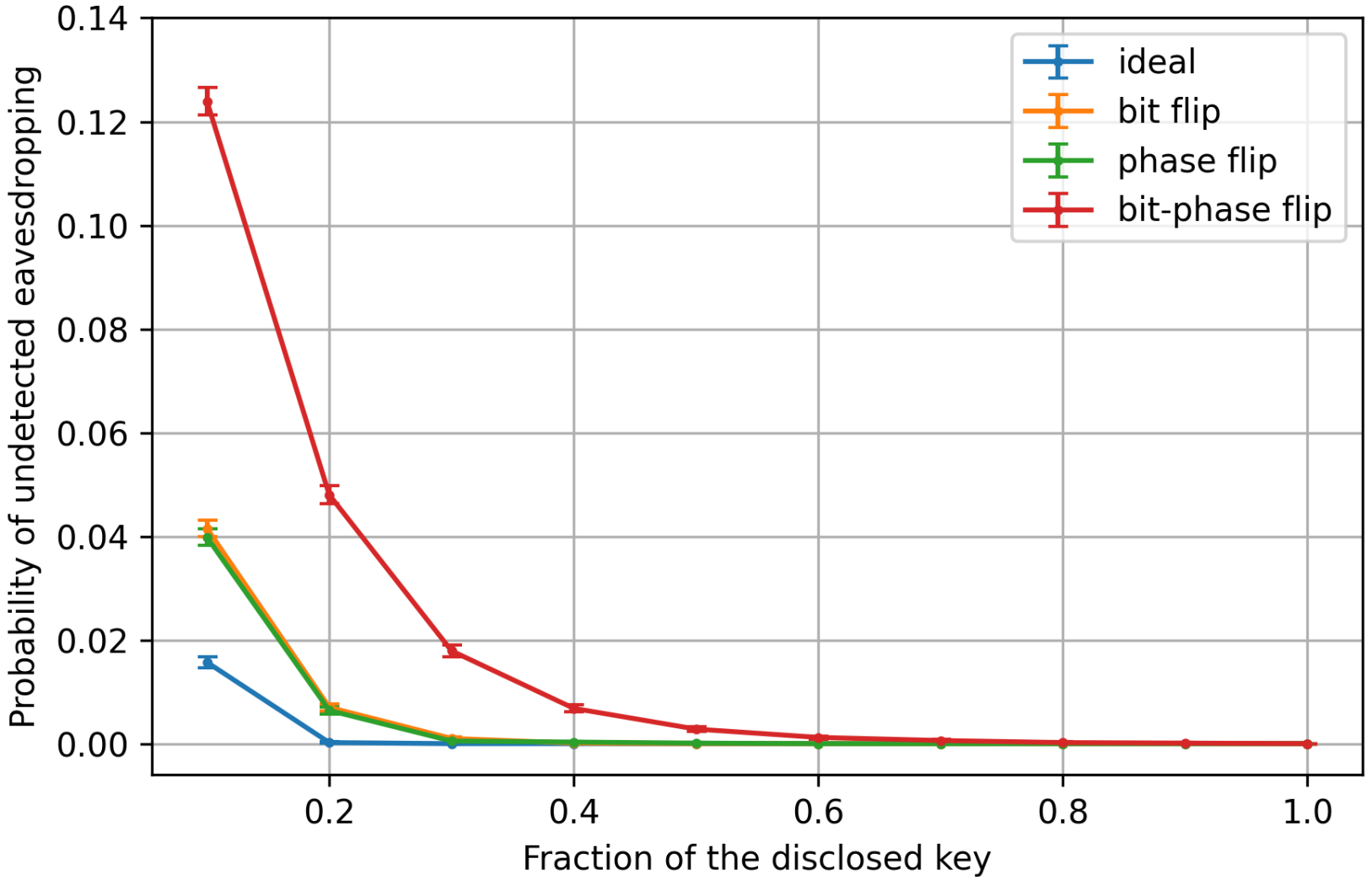
Probability of error in the Bit-Phase Flip scenario

$$P\{E\} = P\{E \mid Z\} \cdot P\{Z\} + P\{E \mid X\} \cdot P\{X\} = 1 \cdot \frac{1}{2} \cdot p + 1 \cdot \frac{1}{2} \cdot p = p$$

Undetected Eavesdropping Probability [Quantum Savory]



Undetected Eavesdropping Probability [Qiskit]



Undetected Eavesdropping Probability – Conclusions

- The probability lowers as the fraction of the key increases

- Channels errors makes the detection process more difficult because we need a number of different bits greater than the threshold to conclude that an eavesdropping has taken place

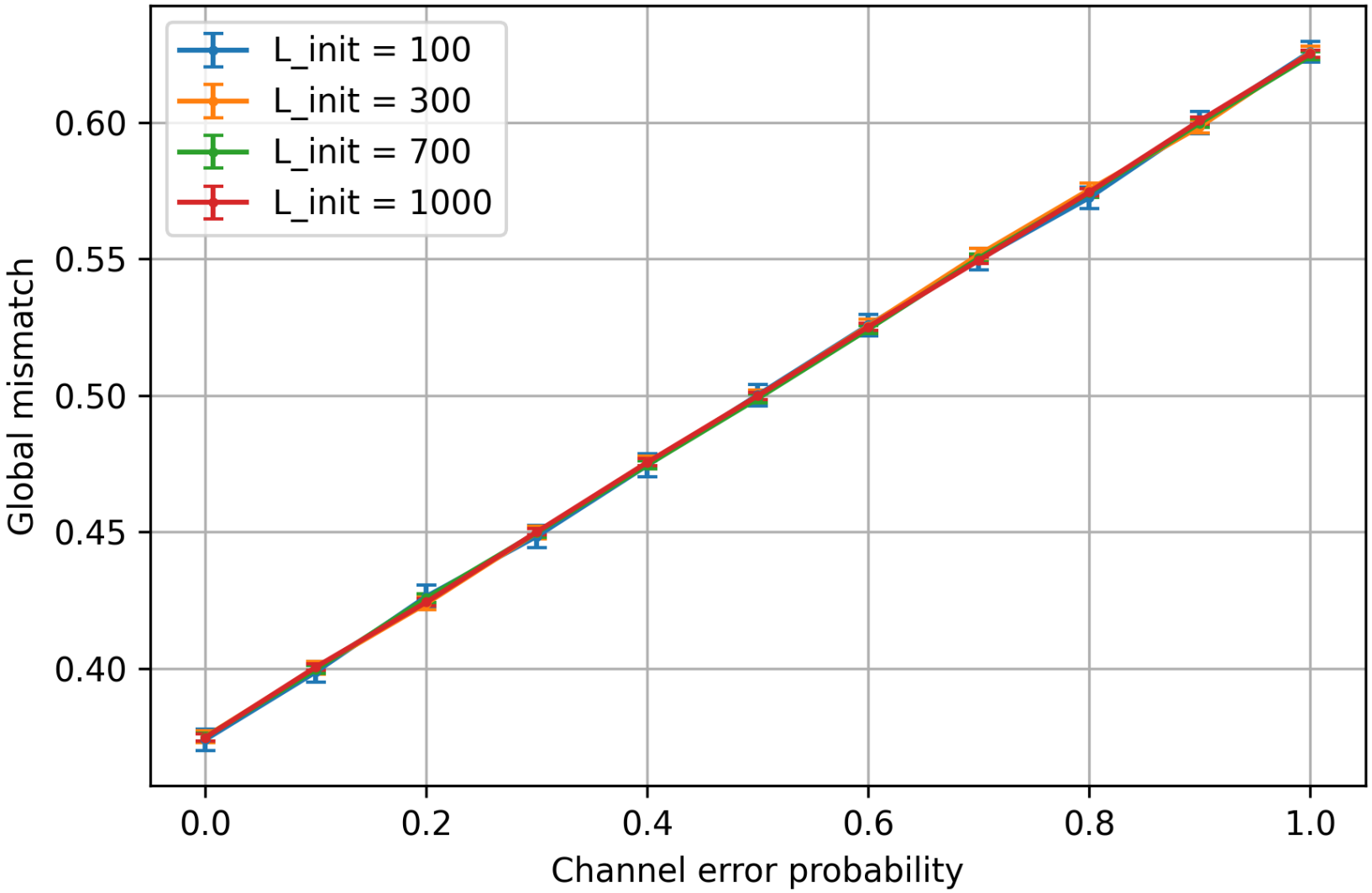
Effect of Key Length Variations

The same experiments are carried out considering the following configurations:

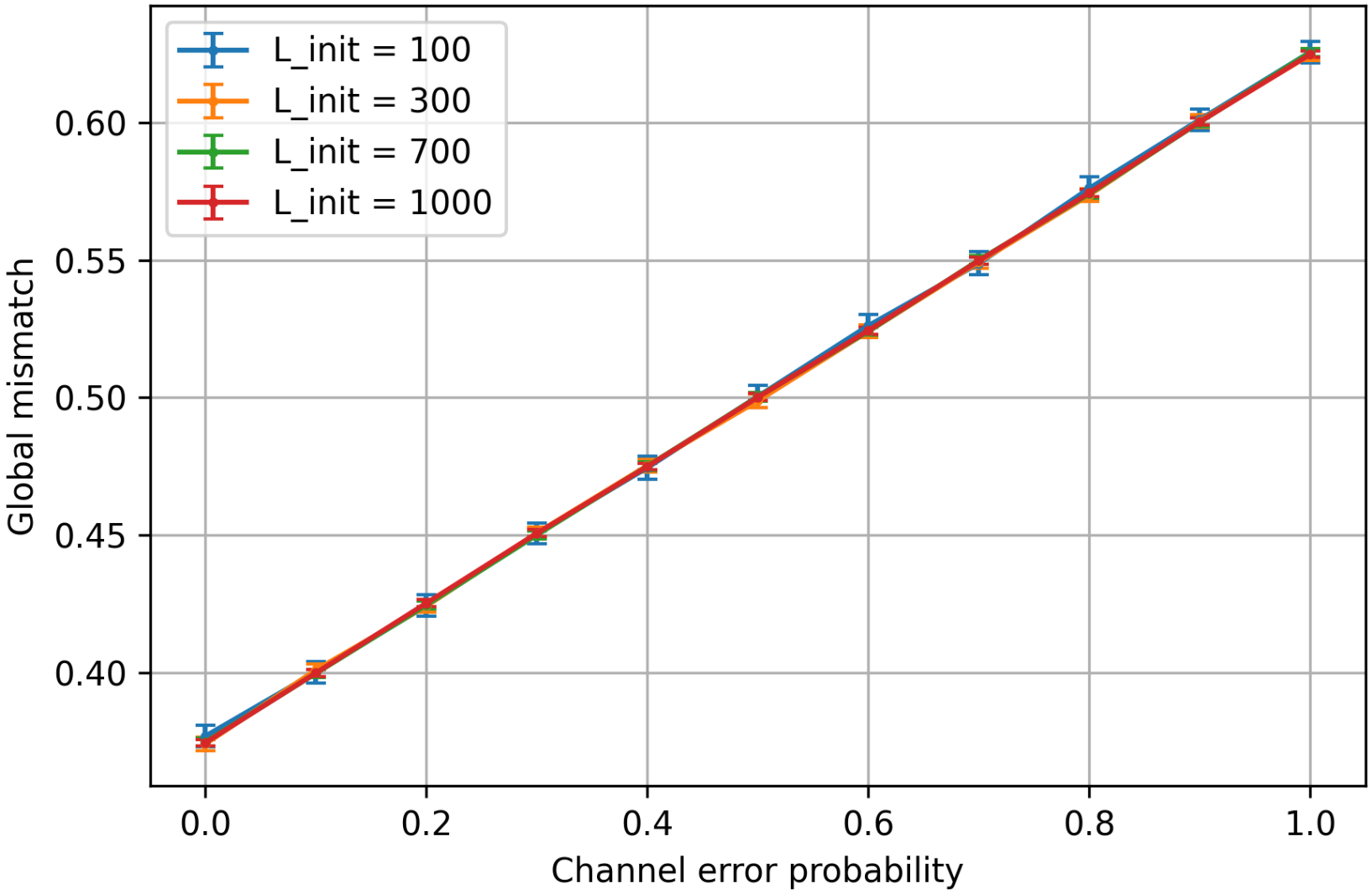
- $L_{init} = 100$
- $L_{init} = 300$ (for comparison purposes)
- $L_{init} = 700$
- $L_{init} = 1000$

In the following are reported only the interesting cases of eavesdropping with bit-phase flip channel

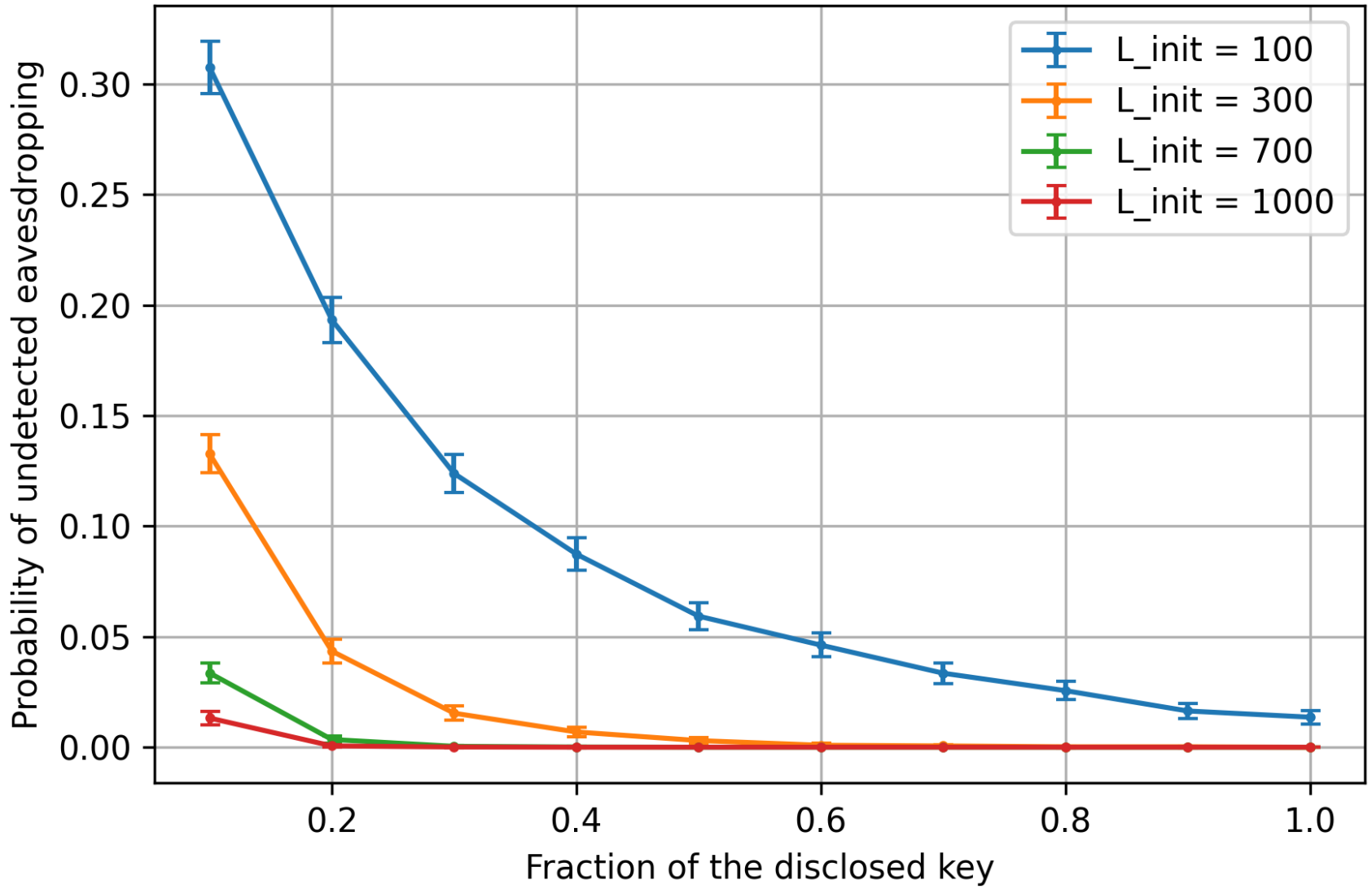
Effect of Key Length Variations – Global Mismatch Ratio [Quantum Savory]



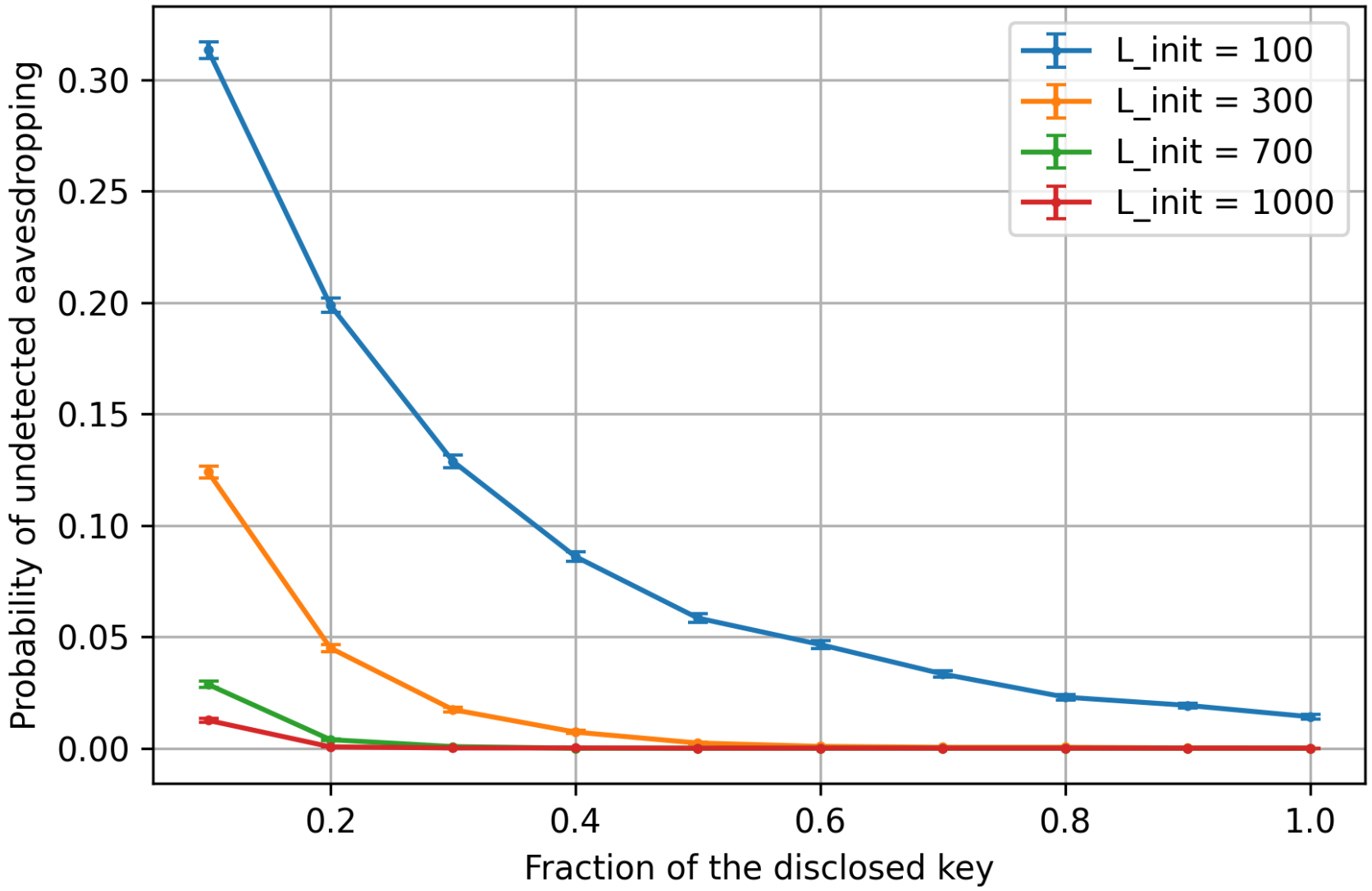
Effect of Key Length Variations – Global Mismatch Ratio [Qiskit]



Effect of Key Length Variations – Undetected Eavesdropping Probability [Quantum Savory]



Effect of Key Length Variations – Undetected Eavesdropping Probability [Qiskit]



Effect of Key Length Variations

- No effects on the Mismatch Ratios
- Probability of undetected eavesdropping lowers as the key length increases