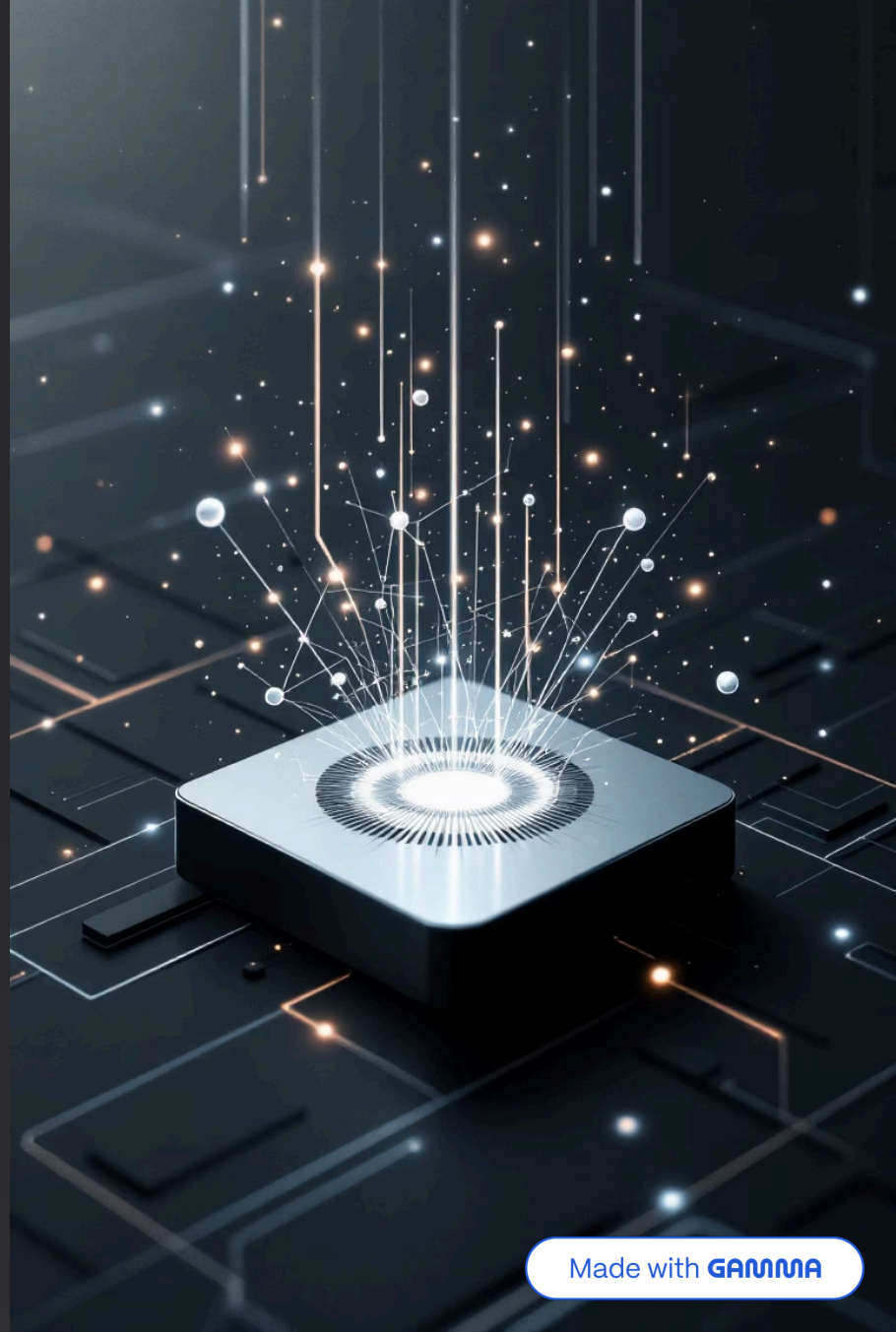
BB84 Quantum Key Distribution

Securing Communication with Quantum Physics

Exploring the revolutionary protocol that harnesses quantum mechanics to create theoretically unbreakable encryption.



Introducing BB84

The First Quantum Key Distribution Protocol

Foundation

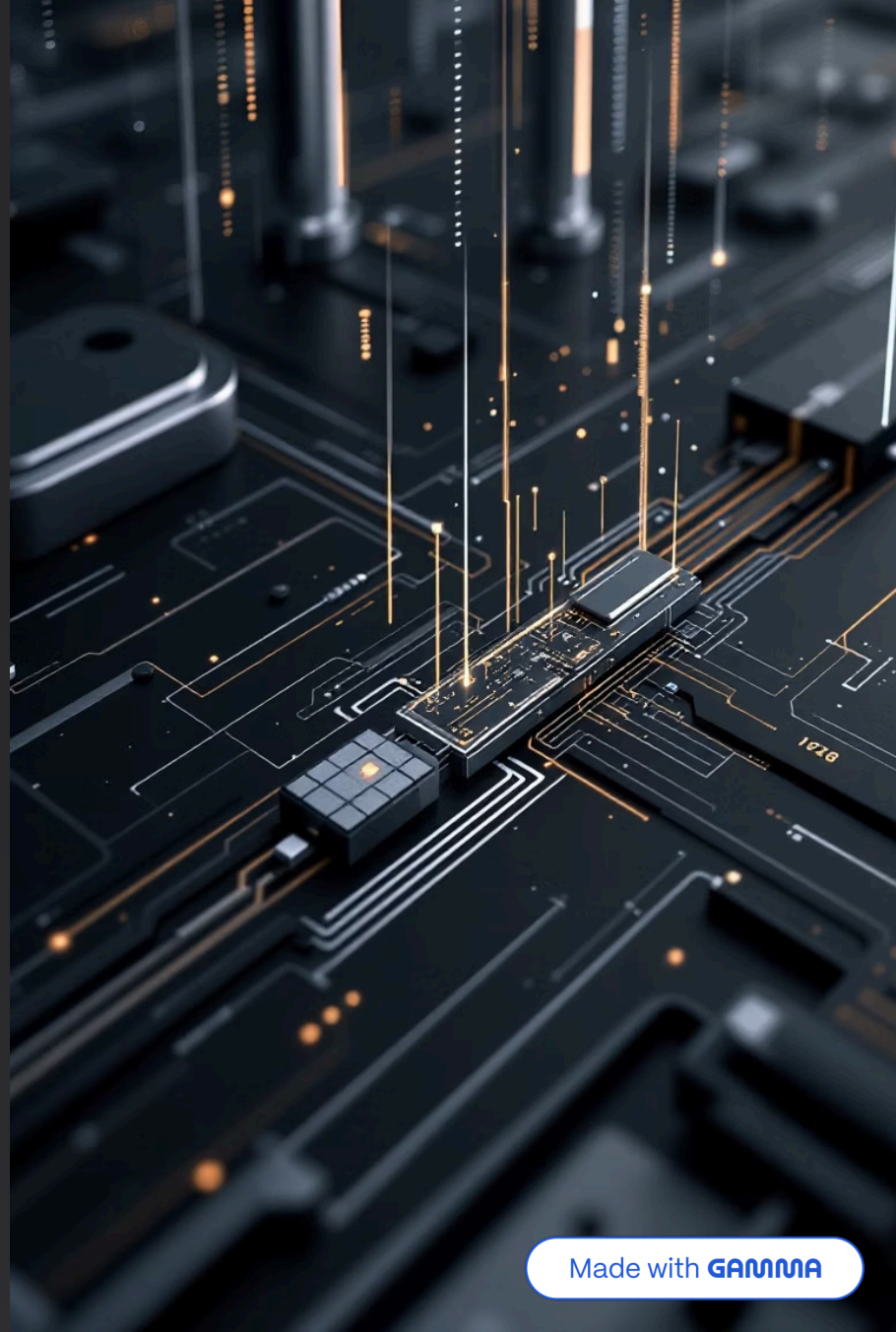
Proposed by Bennett and Brassard in 1984 as the pioneering QKD protocol

Mechanism

Uses polarization states of single photons to encode and transmit cryptographic bits

Security Principle

Measurement of quantum states inherently disturbs them, revealing any eavesdropping attempts



How BB84 Works

01

Preparation

Alice generates random bits and random basis choices, then sends encoded photons to Bob

02

Measurement

Bob receives photons and measures them using randomly selected bases, recording results

03

Sifting

Alice and Bob publicly compare bases (not bits). Matching bases yield the sifted key

04

Verification

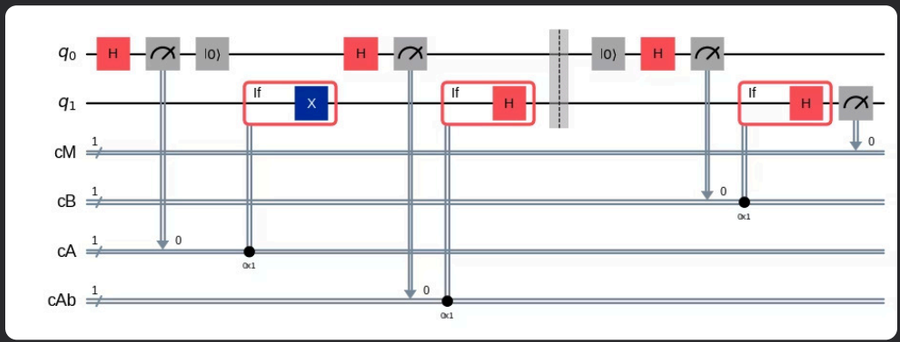
They test a sample of sifted key bits to detect eavesdropping via quantum bit error rate

BB84 Implementation in Qiskit

Quantum Circuit Architecture

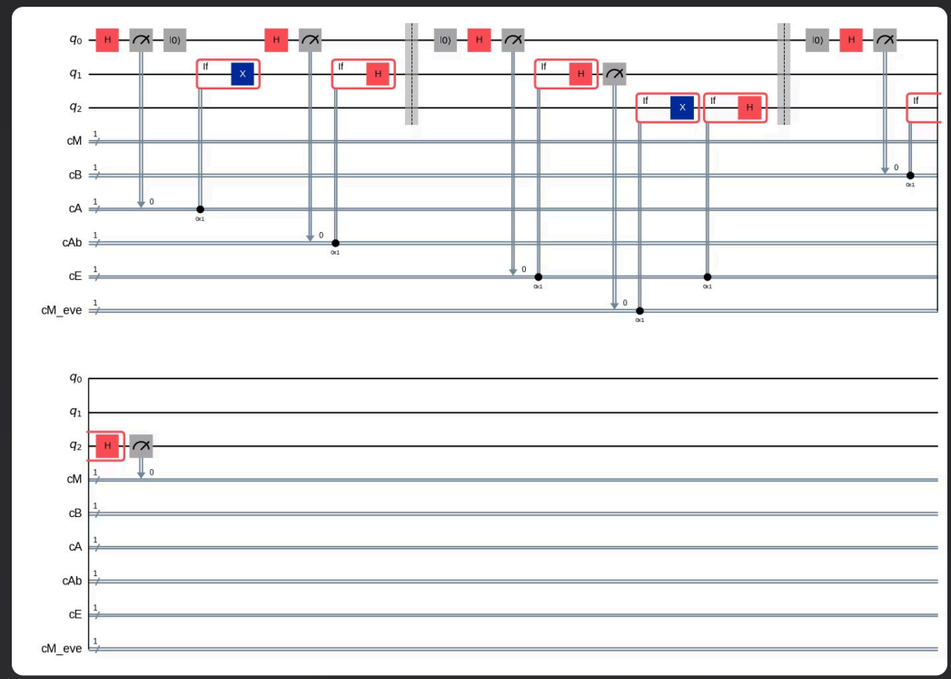
Standard Protocol Circuit

Qiskit implementation showing Alice's basis encoding, quantum channel transmission, and Bob's measurement basis selection.



With Eavesdropping Simulation

Extended circuit demonstrating Eve's interception, measurement, and re-transmission, illustrating quantum state disturbance.



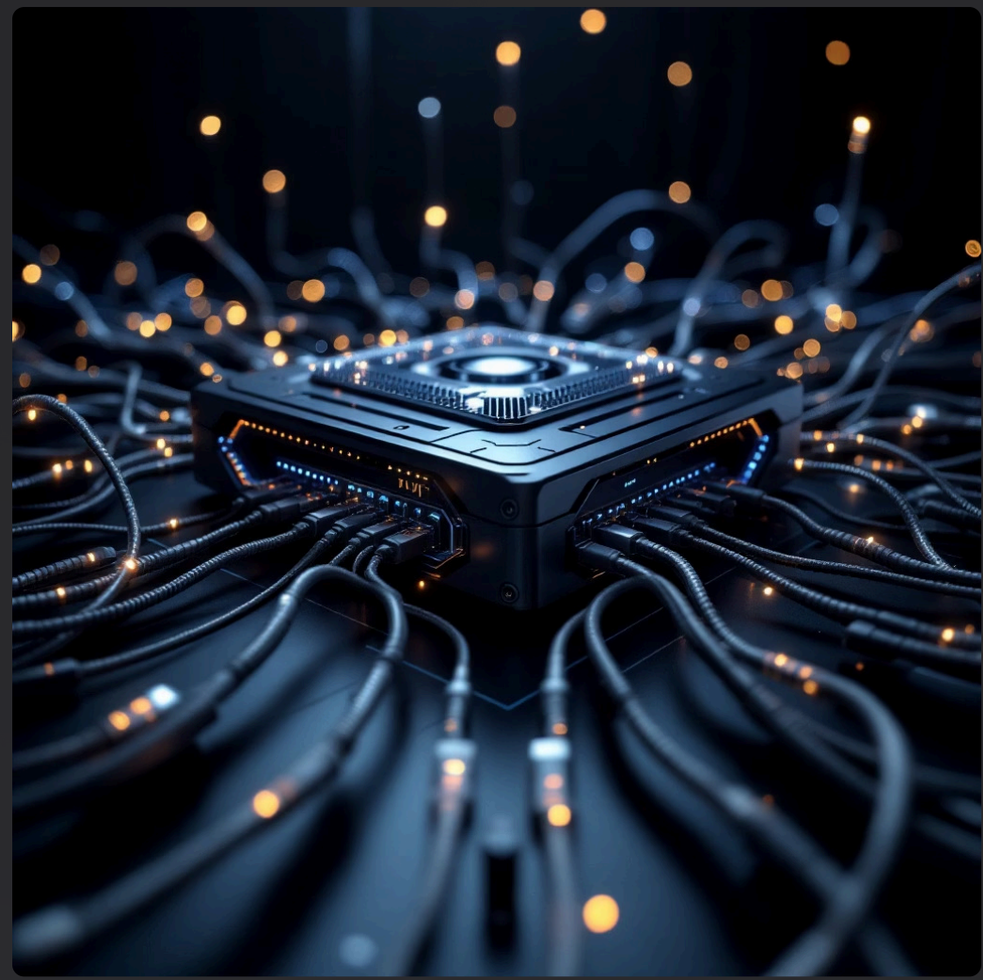
These circuits model the BB84 protocol flow that requires a quantum circuit (classical post-processing is excluded from this section). It also comprehend the generation of random bits and random bases using quantum state to ensure perfect randomness.

Channel Errors Impact on BB84

Error Sources

Environmental noise, detector inefficiencies, and fiber losses introduce errors independent of eavesdropping, complicating threat detection.

- Photon absorption and scattering
- Detector dark counts and inefficiencies
- Timing jitter and synchronization errors



→ **Baseline QBER:** Natural channel errors establish minimum QBER threshold for security analysis

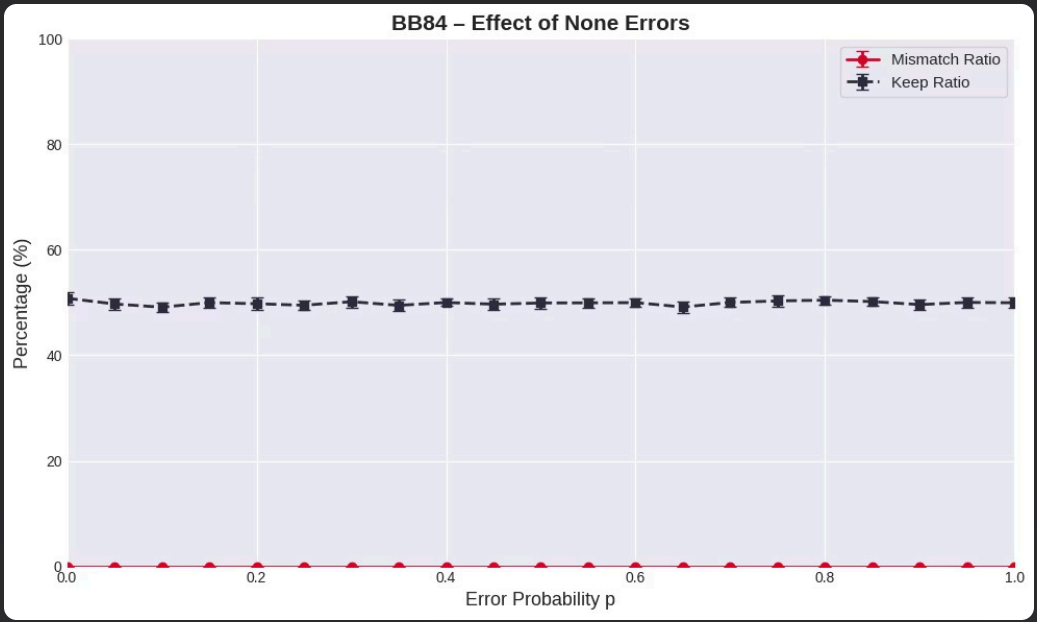
→ **Eve Detection Challenge:** QBER rise above baseline indicates eavesdropping vs. normal channel degradation

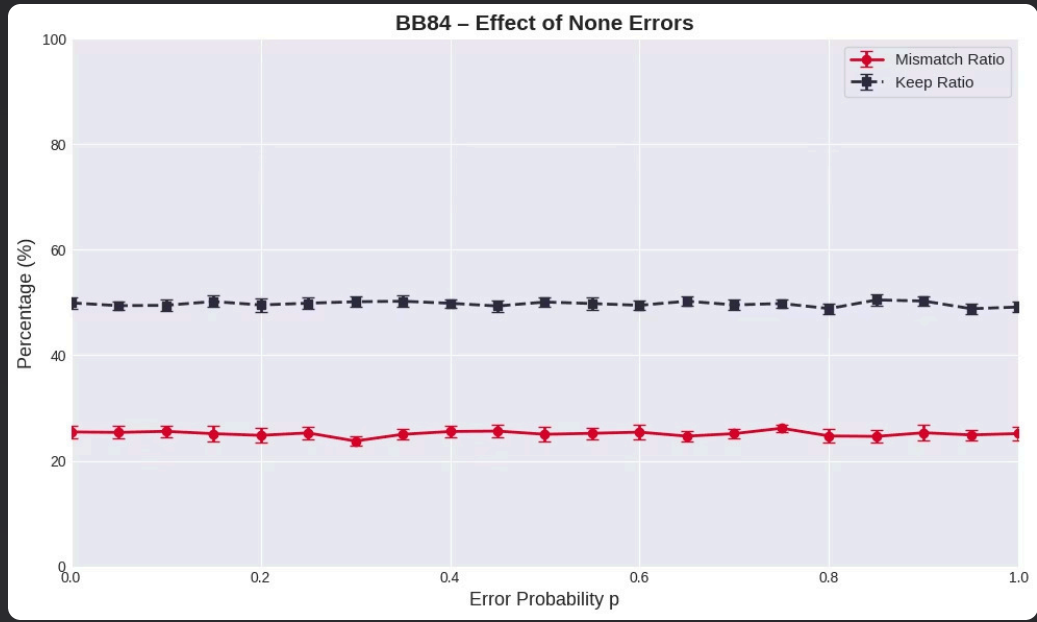
→ **Distance Dependency:** Increased transmission distance amplifies channel errors, reducing effective key generation rates

Visualizing BB84 Data

Mismatch Ratio Rmis Analysis for L = 300

The mismatch ratio quantifies basis disagreement between Alice and Bob, revealing protocol efficiency and eavesdropping signatures.

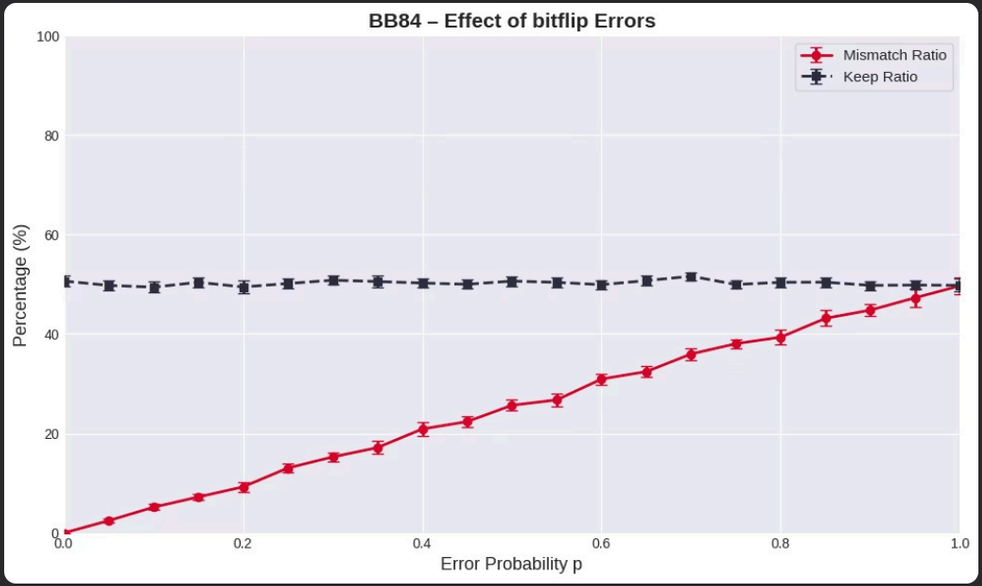


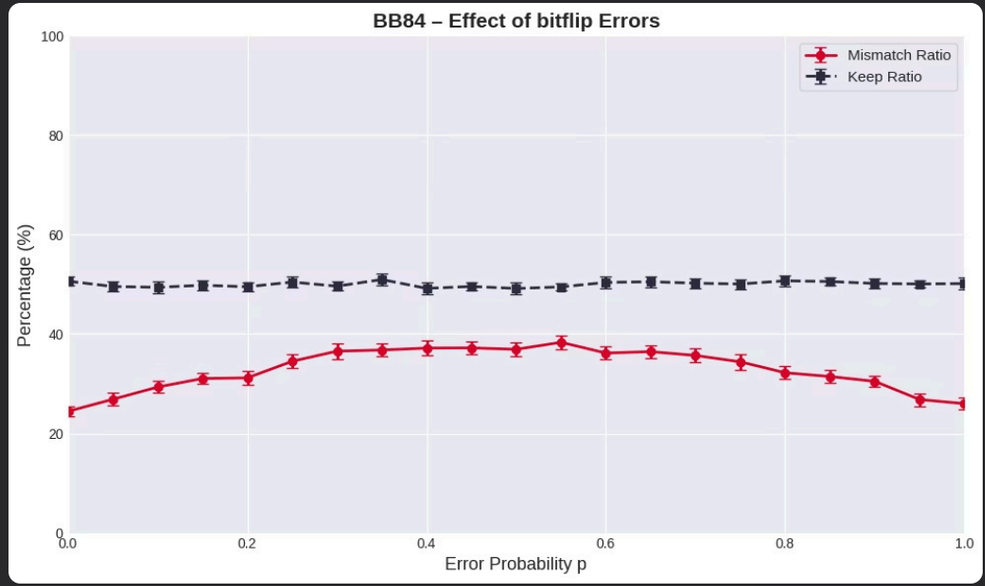


Key Insight: Mismatch ratio remains stable under normal conditions but increases significantly when eavesdropping is detected.

Visualizing BB84 Data

Mismatch Ratio Rmis Analysis for L = 300, Bit flip error



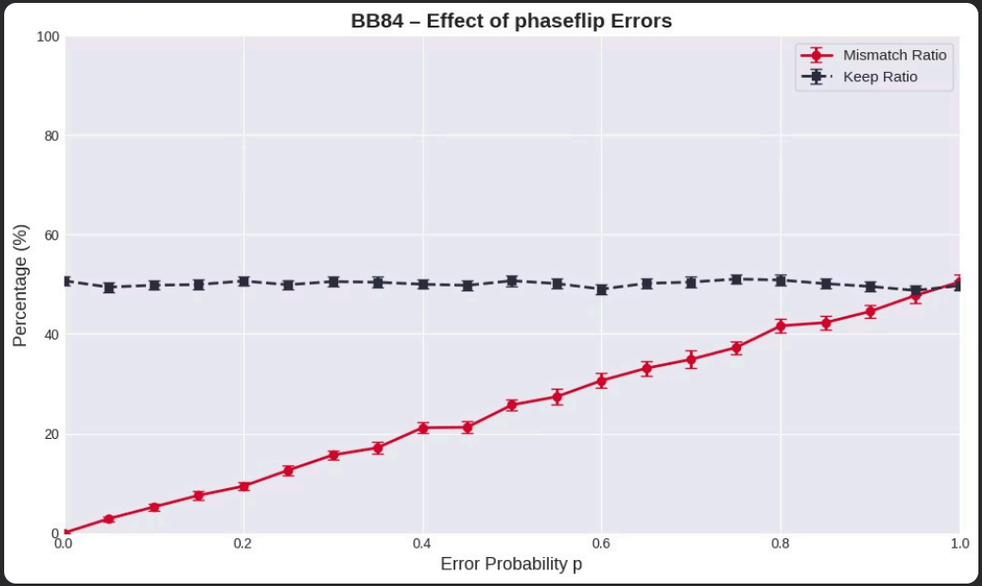


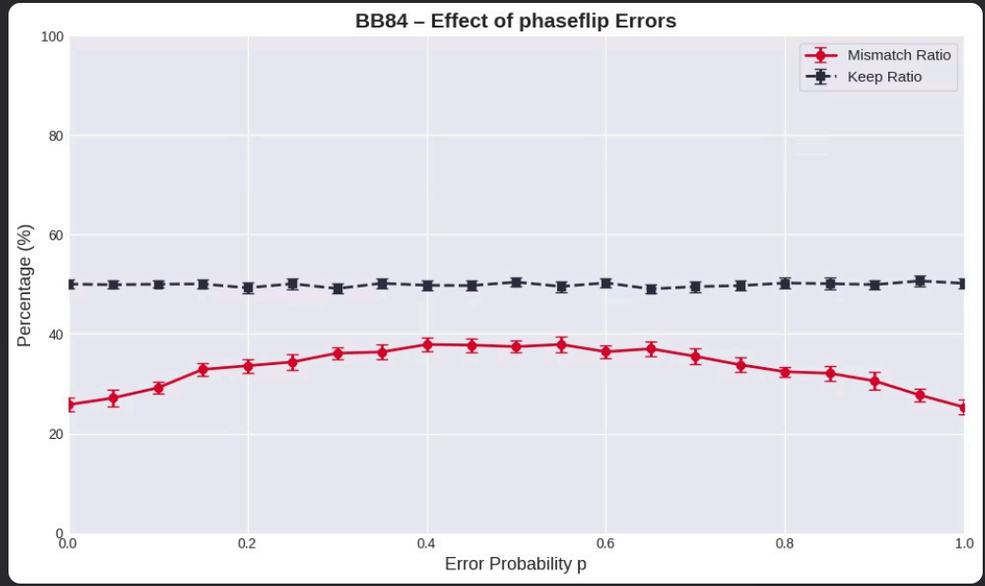
Key Insight:

- **Bit-flip (X) in Z basis:** Flips the bit $|0\rangle \leftrightarrow |1\rangle$.
  - *Result:* Certain mismatch if Bob measures in the correct basis.
- **Bit-flip (X) in X basis:** Does not change the state: $X|+\rangle = |+\rangle$ e $X|-\rangle = -|-\rangle$.
  - *Result:* No measurable error.
- **Average result:** Only half the time (when Alice and Bob use Z) produces mismatch $\rightarrow R_{mis} \approx 0.5$ when p=1.

Visualizing BB84 Data

Mismatch Ratio Rmis Analysis for L = 300, Phase flip error



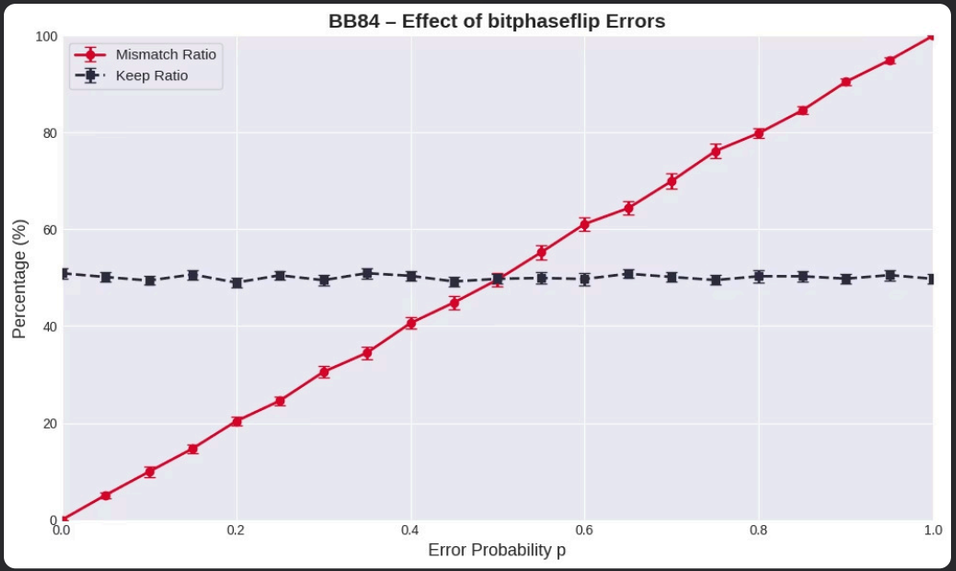


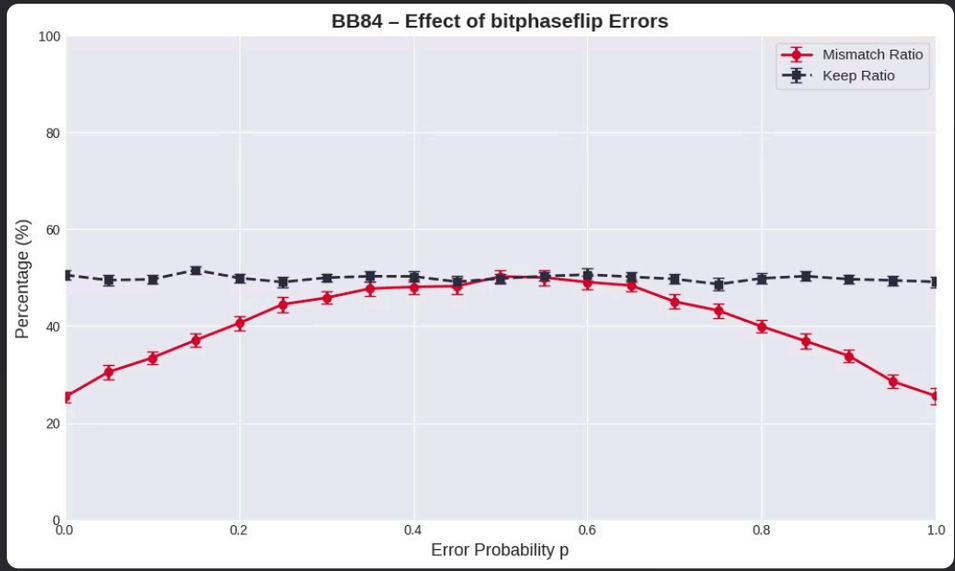
Key Insight:

- **Phase-flip (Z) in Z basis:** Does not change anything ($|0\rangle \to |0\rangle, |1\rangle \to -|1\rangle$, but the sign does not affect measurement).
  - *Result:* No error.
- **Phase-flip (Z) in X basis:** Flips $|+\rangle \leftrightarrow |-\rangle$.
  - *Result:* Certain mismatch.
- **Average result:** Only half the time (when Alice and Bob use X) produces mismatch $\to R_{mis} \approx 0.5$ when p=1.

Visualizing BB84 Data

Mismatch Ratio Rmis Analysis for L = 300, Bit+Phase flip error





Key Insight: Bit+Phase-flip (Y = iXZ)

This error applies **both X and Z operations**.

- **Bit+Phase-flip (Y) in Z basis:** Behaves like X → bit-flip ⇒ certain error.
  - *Result:* Certain mismatch.
- **Bit+Phase-flip (Y) in X basis:** Behaves like Z → flips $|+\rangle \leftrightarrow |-\rangle$ ⇒ certain error.
  - *Result:* Certain mismatch.
- **Average result:** In **both bases** an observable error is always generated $\rightarrow R_{mis} \rightarrow 1$ when $p \rightarrow 1$.

Eve's Eavesdropping & Channel Noise

Eve's "intercept-resend" strategy introduces a baseline disturbance (approx. 25% mismatch in ideal BB84). Channel noise doesn't simply add errors linearly, leading to complex interactions.

- **Non-Linear Error Impact**

  Channel noise doesn't always add errors linearly to Eve's baseline disturbance; the interaction is more nuanced.

- **Moderate Noise ('p')**

  At small to moderate channel noise probability (p), Eve's disturbance and channel noise combine, causing the mismatch ratio (R_{mis}) to rise.

- **High Noise ('p')**

  At high noise probability, channel randomization can mask Eve's disturbance, or deterministic flips can partially cancel her effects, potentially causing R_{mis} to decrease.

Detecting Eavesdropping

The Quantum Bit Error Rate (QBER)

Eve's Interference

Any measurement attempt by eavesdropper Eve disturbs photon states, introducing detectable errors into the key

QBER Calculation

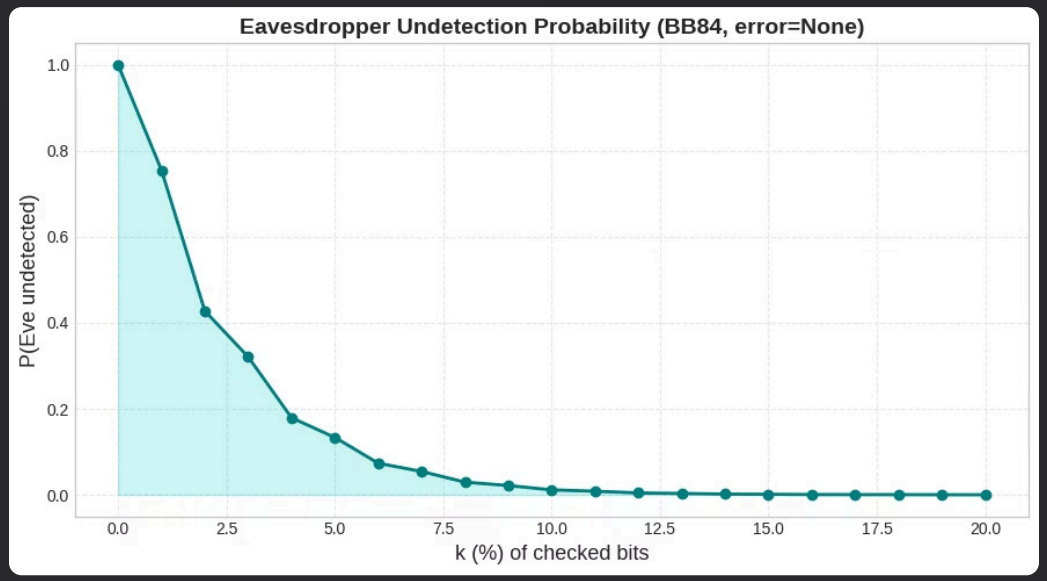
Alice and Bob compare a random subset of sifted key bits to quantify error rate and assess channel security

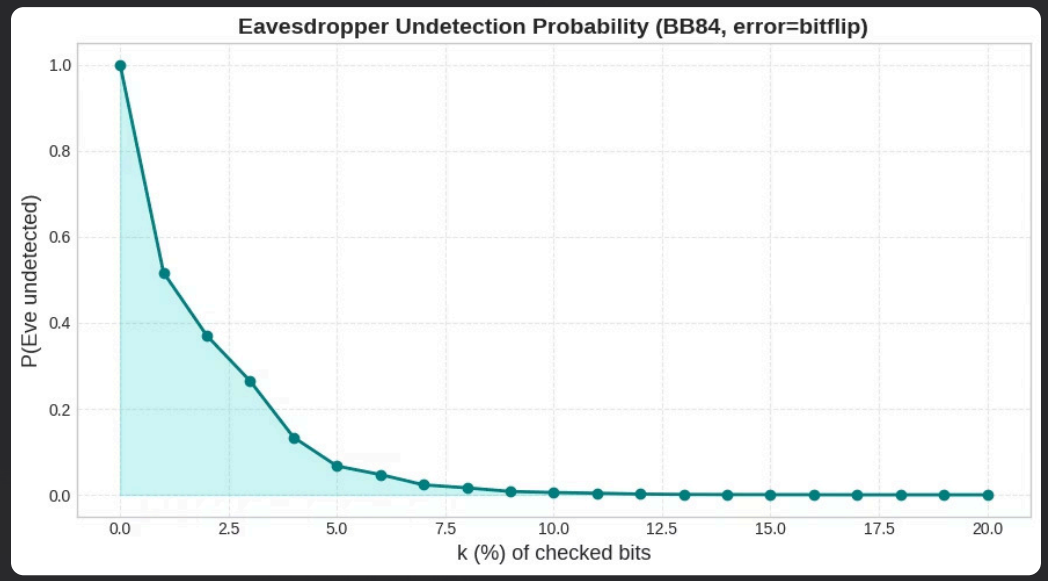
Threshold Decision

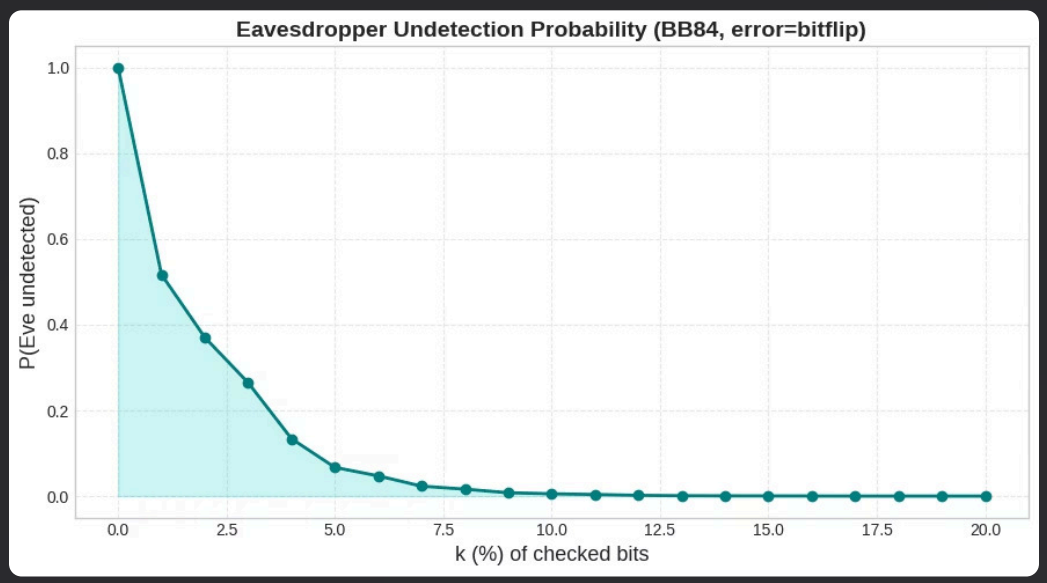
If QBER exceeds theoretical threshold, the key is discarded and transmission restarts to prevent compromised encryption

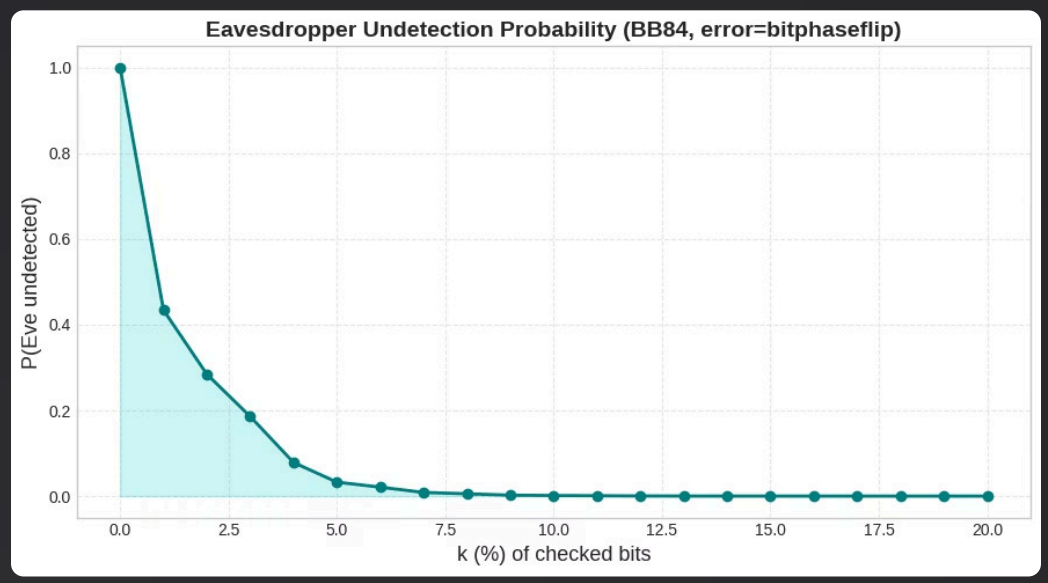
Eavesdropping Detection Probability

Pund Analysis for L = 300





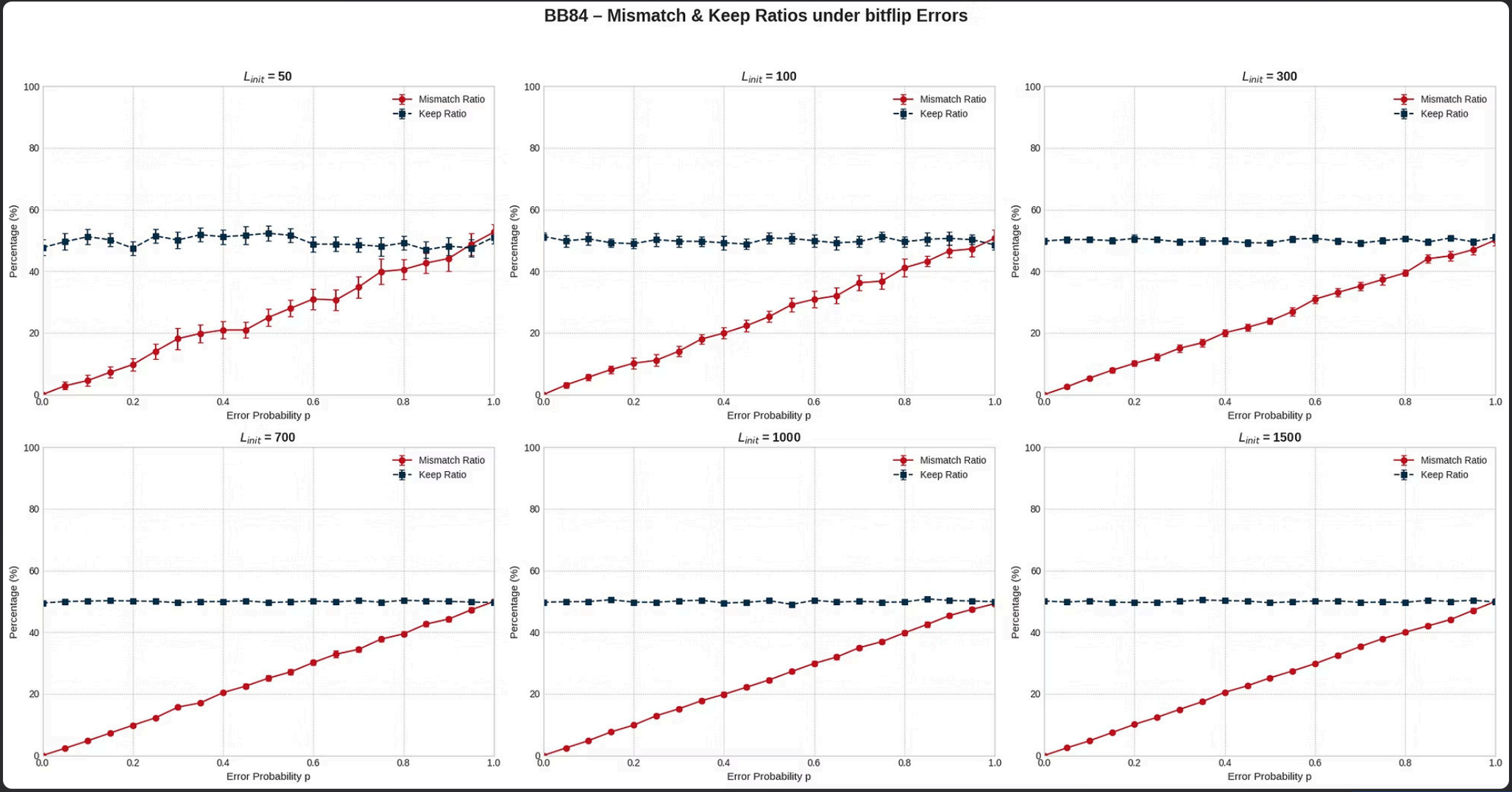




Comprehensive BB84 Performance Metrics

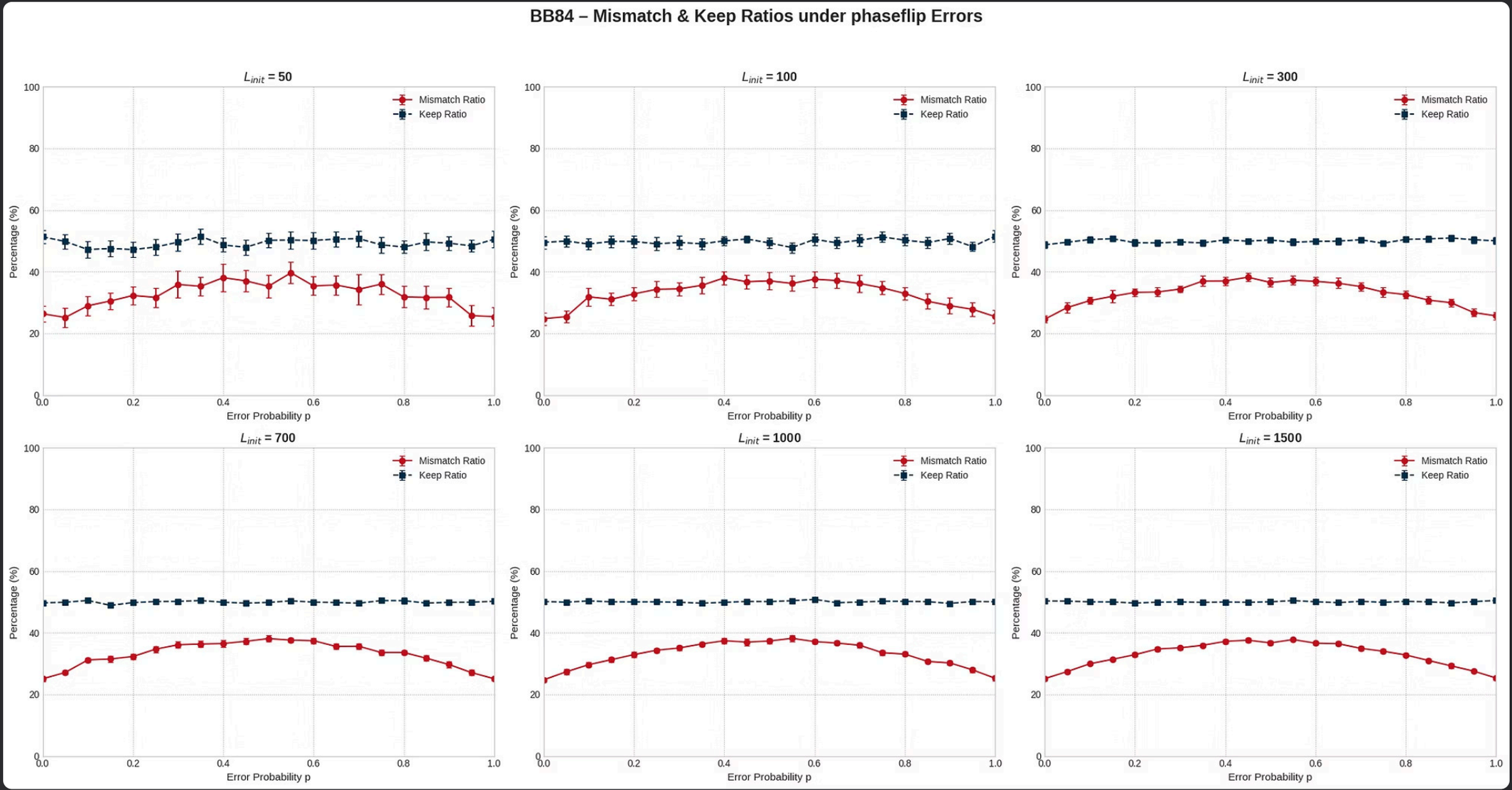
Multi-Length Experimental Analysis

Key metrics evaluated across different transmission distances to assess protocol scalability and practical security.



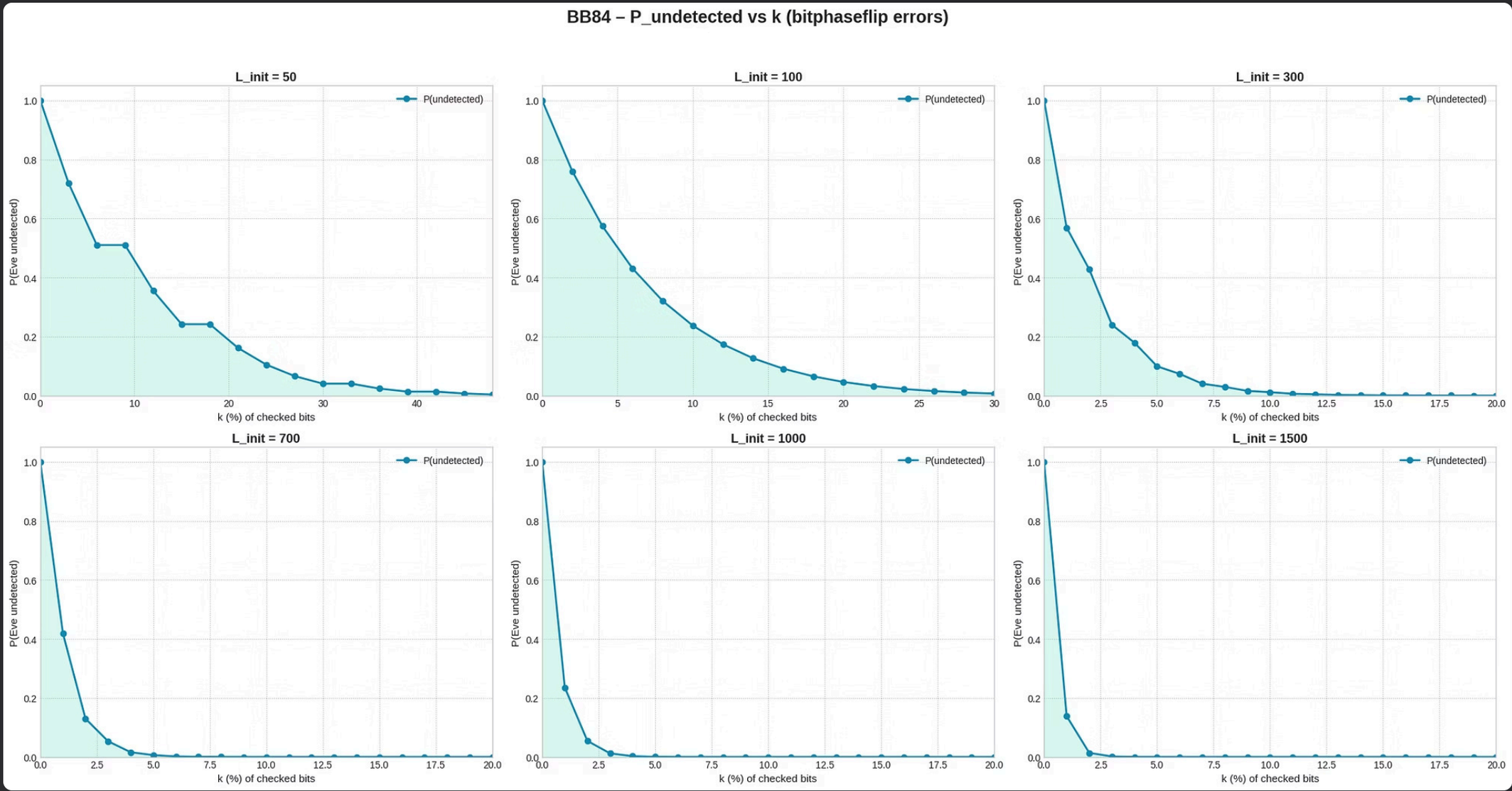
Comprehensive BB84 Performance Metrics

Multi-Length Experimental Analysis – Eve



Comprehensive BB84 Performance Metrics

Multi-Length Experimental Analysis - Pund



Thank You

Questions and Discussion

BB84 Protocol: Pioneering quantum key distribution securing the future of cryptography through fundamental quantum mechanics principles.