MASTER’S DEGREE IN COMPUTER ENGINEERING

QUANTUM COMPUTING AND QUANTUM INTERNET

PROJECT DISCUSSION

E91 PROTOCOL

PROFESSORS

LUCIANO **LENZINI**
LEONARDO **BACCIOTTINI**

STUDENT

GIOVANNI **LIGATO**

IN SUPREMÆ DIGNITATIS
1343

UNIVERSITY OF PISA

INTRODUCTION

BACKGROUND

Securely sharing cryptographic keys over insecure channels is a fundamental challenge in modern cryptography.

THE PROBLEM

Classical key distribution methods rely on computational hardness, which can be broken by advances in computing.

The E91 protocol leverages quantum mechanics (*entanglement* and the *no-cloning theorem*) to enable infinitely secure key distribution, immune to eavesdropping.

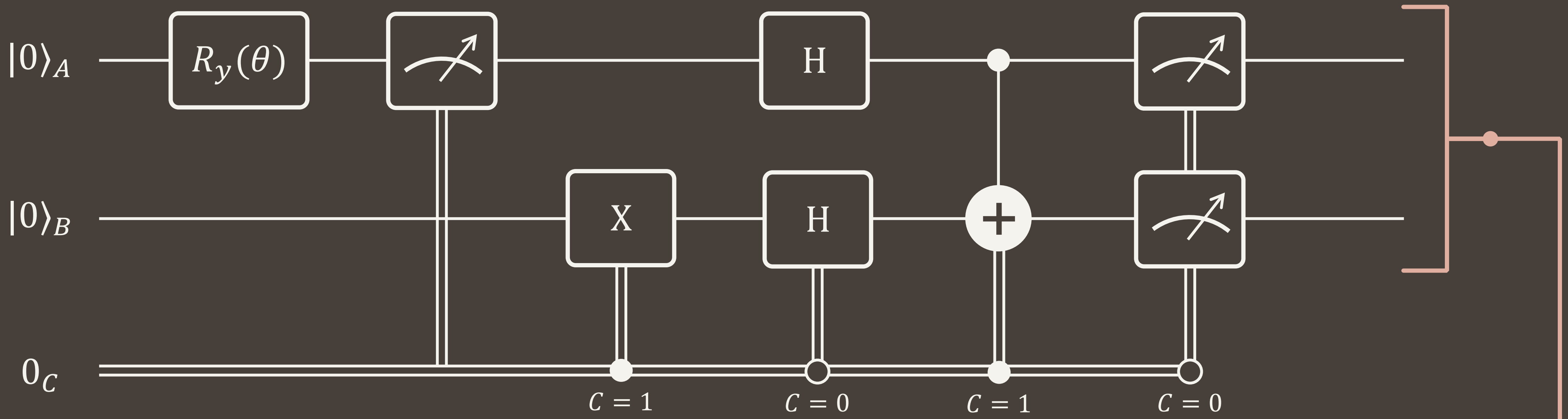
SOLUTION

SCENARIOS
TO ANALYZE

1. IDEAL CONDITIONS
2. CHANNEL ERRORS
3. EAVESDROPPING

THE **SPECIALIZED CIRCUIT** FOR GENERATING **WERNER STATES**

CONTROLLED BY **CHARLIE**



$$\rho_{AB} = \sin^2\left(\frac{\theta}{2}\right) \cdot |\psi^-\rangle\langle\psi^-| + \frac{\cos^2\left(\frac{\theta}{2}\right)}{4} \cdot I$$

$$\rho_{AB} = \sin^2\left(\frac{\theta}{2}\right) \cdot |\psi^-\rangle\langle\psi^-| + \frac{\cos^2\left(\frac{\theta}{2}\right)}{4} \cdot I$$

THIS IS A **WERNER STATE** WHEN THE **WERNER PARAMETER** (w) IS SET TO

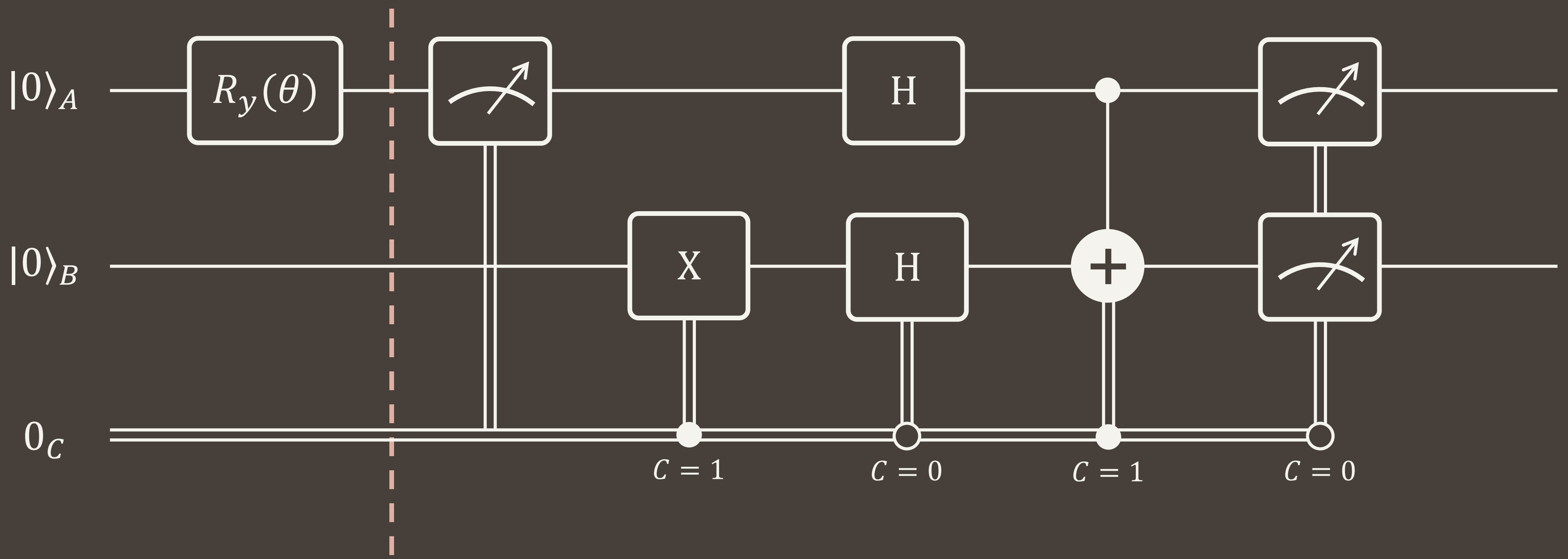
$$w = \sin^2\left(\frac{\theta}{2}\right) \quad \rightarrow \quad \rho_{AB} = w \cdot |\psi^-\rangle\langle\psi^-| + \frac{1-w}{4} \cdot I$$

THE **FIDELITY** CAN BE OBTAINED FROM THE WERNER PARAMETER USING THE FOLLOWING FORMULA:

$$F = \frac{3w+1}{4}$$

1. IDEAL CONDITIONS

CIRCUIT **ANALYSIS**



$$\cos\left(\frac{\theta}{2}\right)|0_B 0_A\rangle + \sin\left(\frac{\theta}{2}\right)|0_B 1_A\rangle$$

MEASUREMENT PROBABILITIES FOR ALICE'S QUBIT

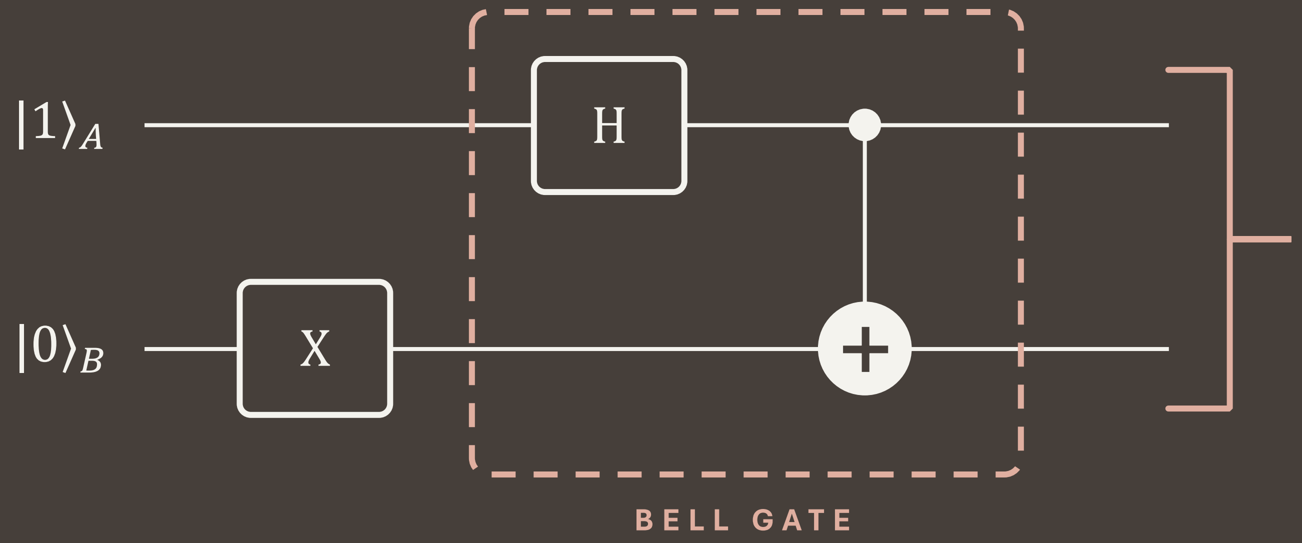
$$P\{0_A\} = \cos^2\left(\frac{\theta}{2}\right)$$

$$P\{1_A\} = \sin^2\left(\frac{\theta}{2}\right)$$

IN THE **IDEAL CASE**, SETTING $\boldsymbol{\theta} = \boldsymbol{\pi}$ SIMPLIFIES THE CIRCUIT AS FOLLOWS

(AFTER MEASURING ALICE'S QUBIT)

$$P\{1_A\} = \sin^2\left(\frac{\pi}{2}\right) = 1 \qquad P\{0_A\} = \cos^2\left(\frac{\pi}{2}\right) = 0$$



$$|\psi^-\rangle = \frac{|01\rangle - |10\rangle}{\sqrt{2}}$$

2. CHANNEL ERRORS

THE **CHANNEL ERRORS** ARE SIMULATED USING THE GENERAL CIRCUIT PREVIOUSLY ILLUSTRATED WITH THE FOLLOWING θ VALUES:

$$0 \leq \theta < \pi$$

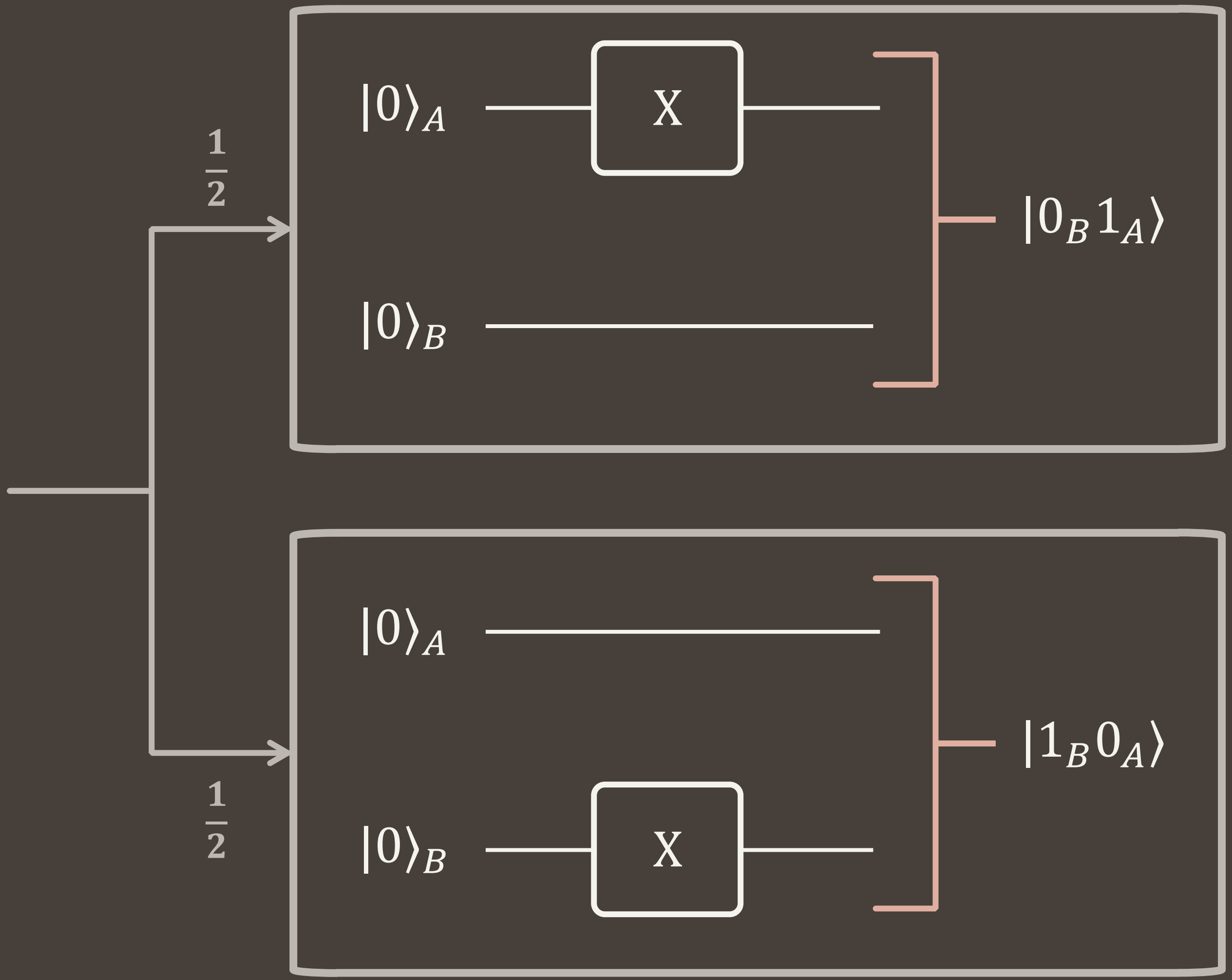
$$\rho_{AB} = \sin^2\left(\frac{\theta}{2}\right) \cdot |\psi^-\rangle\langle\psi^-| + \frac{\cos^2\left(\frac{\theta}{2}\right)}{4} \cdot I$$

NOTE: WHEN $\theta = 0$, THE OUTPUT OF THE CIRCUIT WILL BE A COMPLETELY MIXED STATE. THEREFORE, THE CHANNEL CONSIDERED IN THIS SCENARIO IS A DEPOLARIZING CHANNEL.

3. EAVESDROPPING

IN THE **EAVESDROPPING** SCENARIO **EVE** TAKES CONTROL OF THE SITE-GENERATING ENTANGLED PHOTON PAIRS

EVE SENDS ONE OF THE FOLLOWING TWO STATES TO ALICE AND BOB WITH EQUAL PROBABILITY (1/2), INSTEAD OF AN ENTANGLED PAIR OF PHOTONS.



KEY
DETAILS

PROTOCOL **DETAILS**

OBSERVABLES

ALICE

$$A_0 = Z$$

$$A_1 = X$$

$$A_2 = \frac{Z + X}{\sqrt{2}}$$

BOB

$$B_0 = Z$$

$$B_1 = \frac{Z - X}{\sqrt{2}}$$

$$B_2 = \frac{Z + X}{\sqrt{2}}$$

CHSH CORRELATION VALUE

$$S = \left| \langle A_0 B_2 \rangle + \langle A_0 B_1 \rangle + \langle A_1 B_2 \rangle - \langle A_1 B_1 \rangle \right|$$

The **0-indexed** notation is used, as in the Python code, to avoid confusion between slides and implementation.

THEORY

OBSERVABLE

HERMITIAN
MATRIX

REAL
EIGENVALUES

CAN BE **DISPLAYED** ON
THE MEASURING DEVICE

MEASUREMENT CAUSES
COLLAPSE INTO ONE OF THE
EIGENSPACES ASSOCIATED WITH
THE RELATIVE EIGENVALUE

NOTEWORTHY IMPLEMENTATION STEPS

1. DEFINE THE **OBSERVABLE O**
2. FIND ITS **EIGENVALUES** AND **EIGENVECTORS**

$$\lambda_i \rightarrow |\lambda\rangle_i = \begin{bmatrix} \lambda_i^{(1)} \\ \lambda_i^{(2)} \end{bmatrix} \quad i = 1{,}2$$

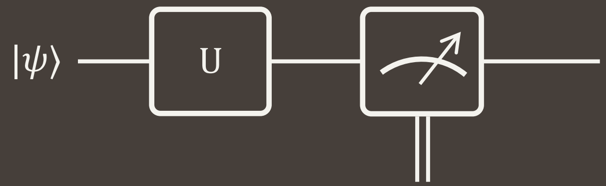
3. DETERMINE THE **UNITARY TRANSFORMATION** MAPPING EIGENVECTORS TO STANDARD BASIS STATES

$$\begin{bmatrix} \lambda_1^{(1)} & \lambda_1^{(2)} & 0 & 0 \\ 0 & 0 & \lambda_1^{(1)} & \lambda_1^{(2)} \\ \lambda_2^{(1)} & \lambda_2^{(2)} & 0 & 0 \\ 0 & 0 & \lambda_2^{(1)} & \lambda_2^{(2)} \end{bmatrix} \cdot \begin{bmatrix} a \\ b \\ c \\ d \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \\ 0 \\ 1 \end{bmatrix} \begin{array}{l} \left.\vphantom{\begin{matrix}1\\0\end{matrix}}\right\} |0\rangle \\ \left.\vphantom{\begin{matrix}0\\1\end{matrix}}\right\} |1\rangle \end{array}$$

4. VERIFY THE FOUND MATRIX IS **UNITARY**

$$U = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \rightarrow UU^\dagger = U^\dagger U = I$$

5. **APPLY** THE UNITARY TRANSFORMATION TO THE QUBIT AND **MEASURE** IN THE STANDARD BASIS



THIS ENTIRE PROCESS ENABLES
MEASUREMENT AS IF USING THE ORIGINAL OBSERVABLE O

METRICS AND PARAMETERS

METRICS TO EVALUATE

CHSH
CORRELATION VALUE

$$S = |\langle A_0 B_2 \rangle + \langle A_0 B_1 \rangle + \langle A_1 B_2 \rangle - \langle A_1 B_1 \rangle|$$

MISMATCH RATIO

$$R_{mis} = \frac{m}{l}$$

NUMBER OF **MISMATCHED BITS** BETWEEN ALICE'S AND BOB'S SECRET KEYS

TOTAL KEY LENGTH

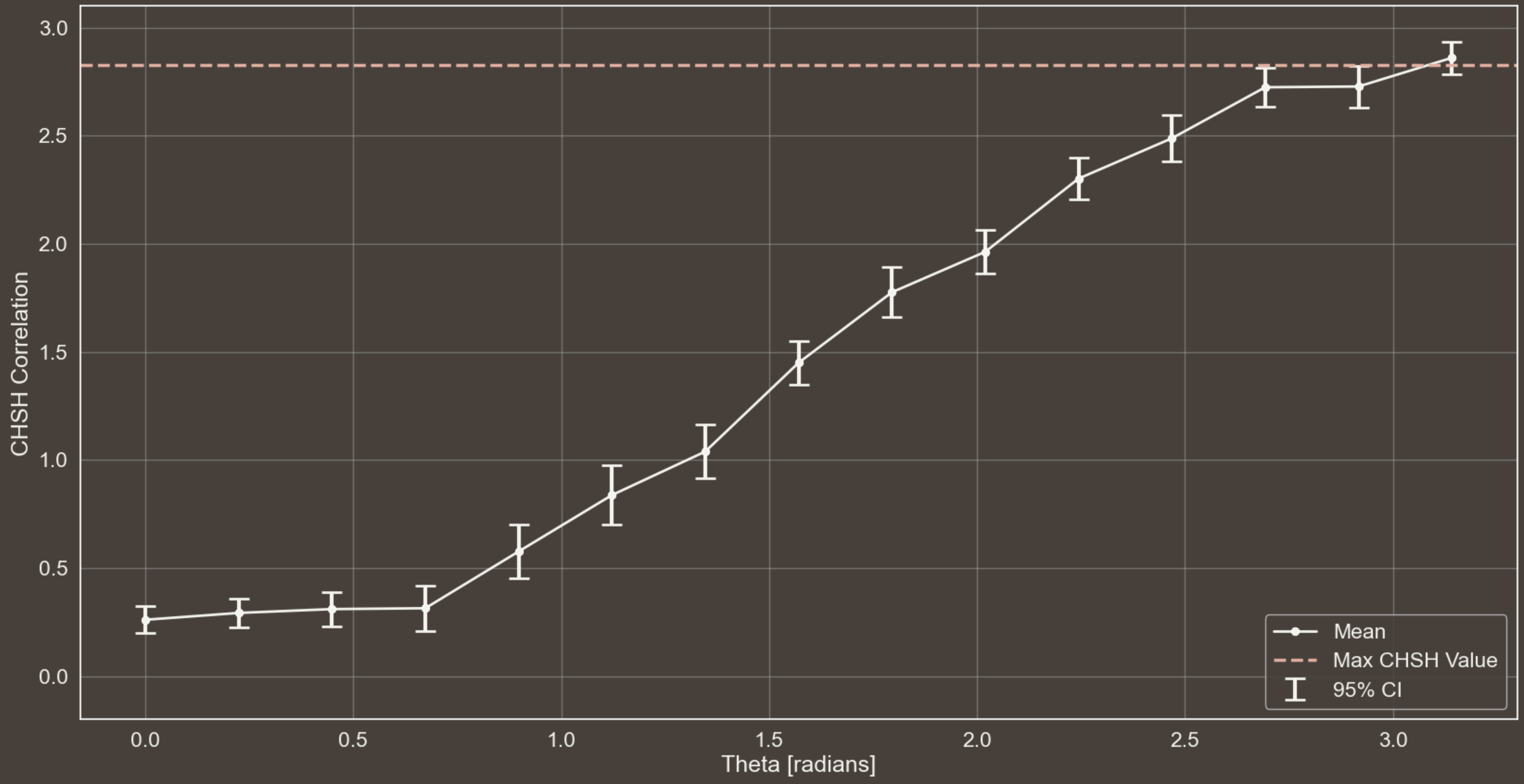
PLOTTED AS A FUNCTION OF $\boldsymbol{\theta}$ OR OF THE **WERNER PARAMETER**

EXPERIMENT **PARAMETERS**

- **n** → NUMBER OF EXECUTIONS PER SETTING
- **θ** → THETA VALUES USED FOR GENERATING THE WERNER STATES
- **Eavesdropping** → WHETHER EVE IS EAVESDROPPING OR NOT
- **#EPR Pairs** → NUMBER OF EPR PAIRS GENERATED IN ONE PROTOCOL EXECUTION

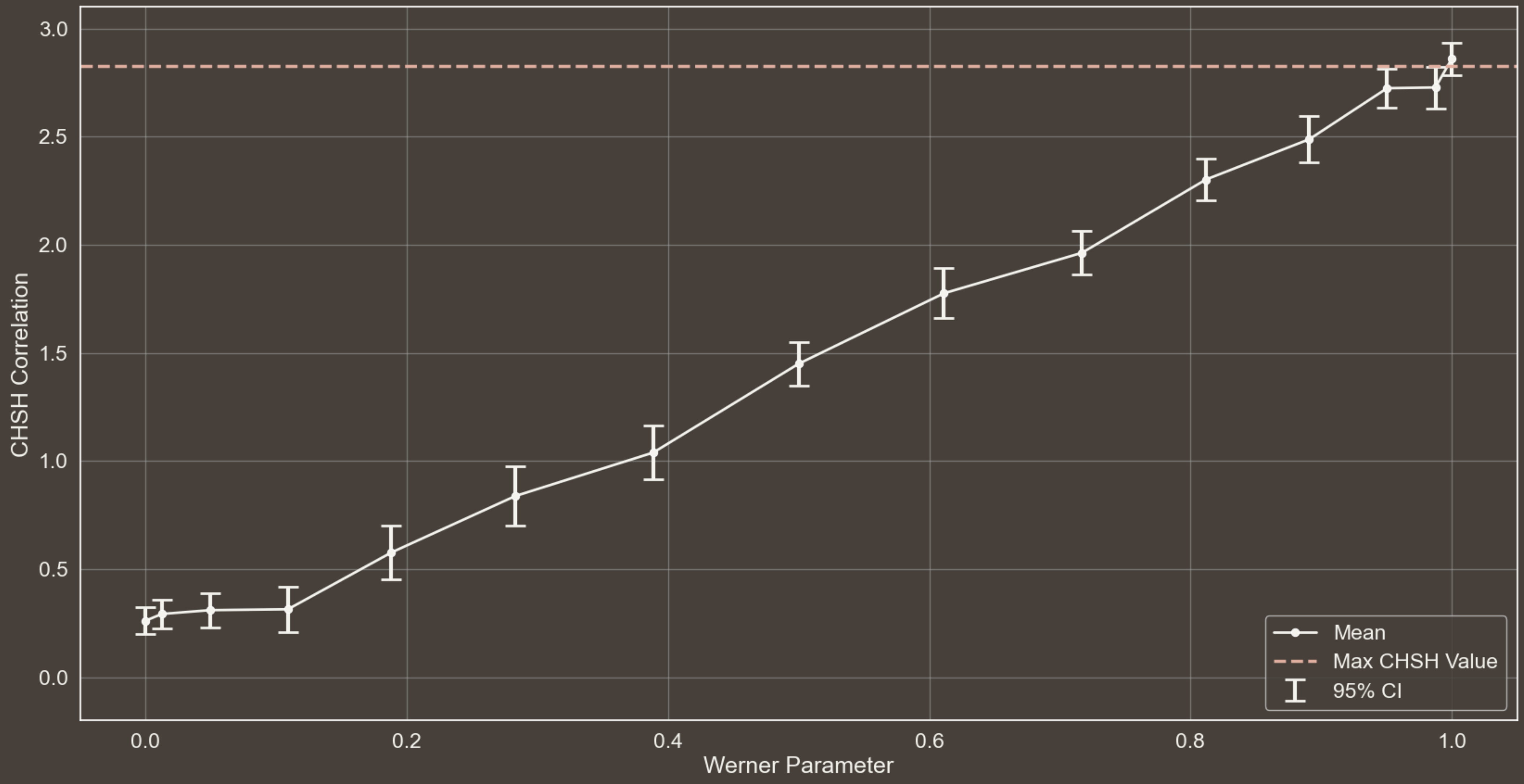
RESULTS ANALYSIS

CHSH CORRELATION WITH 95% CI **vs THETA**



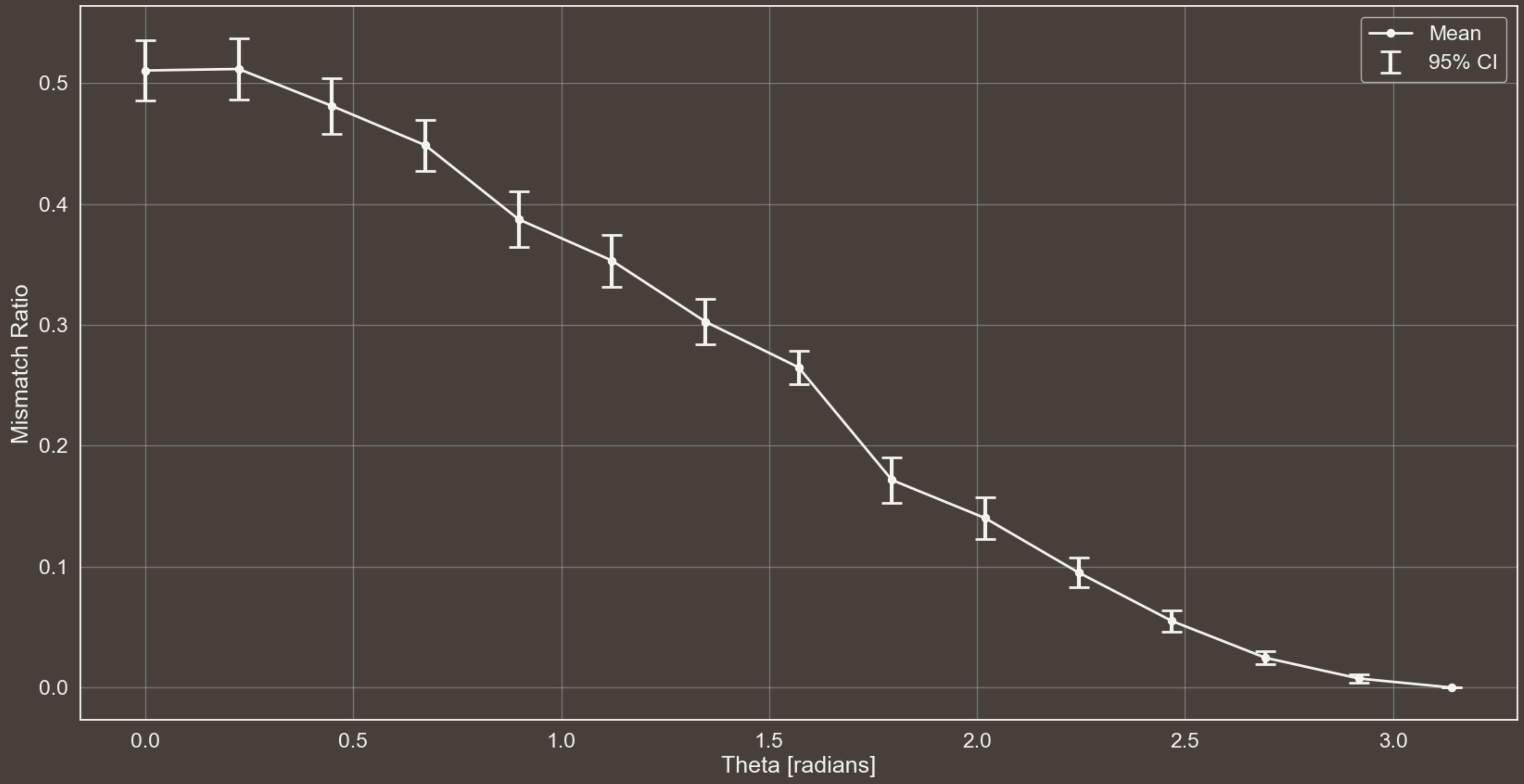
n → 30 **θ** → $\left[\frac{i}{14}\pi \mid i = 0,1,\ldots,14\right]$ **Eavesdropping** → False **#EPR Pairs** → 300

CHSH CORRELATION WITH 95% CI **vs WERNER PARAMETER**



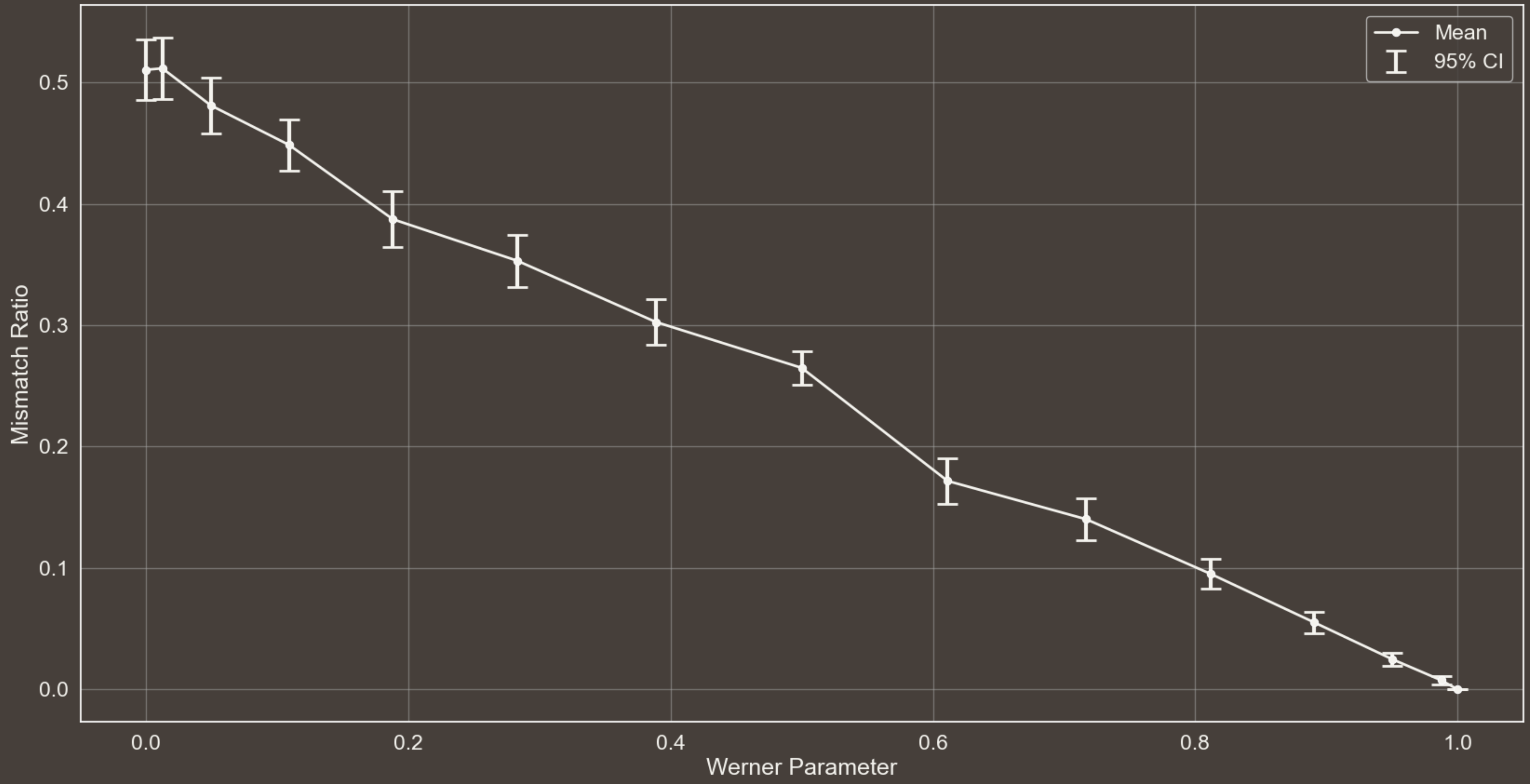
n → 30   **θ** → $\left[\frac{i}{14}\pi \mid i = 0,1,\ldots,14\right]$ **Eavesdropping** → False   **#EPR Pairs** → 300

MISMATCH RATIO WITH 95% CI **vs THETA**



n → 30 $\theta \rightarrow \left[\frac{i}{14}\pi \mid i = 0,1,\ldots,14\right]$ **Eavesdropping** → False **#EPR Pairs** → 300

MISMATCH RATIO WITH 95% CI **vs WERNER PARAMETER**



n → 30 **θ** → $\left[\frac{i}{14}\pi \mid i = 0,1,\ldots,14\right]$ **Eavesdropping** → False **#EPR Pairs** → 300

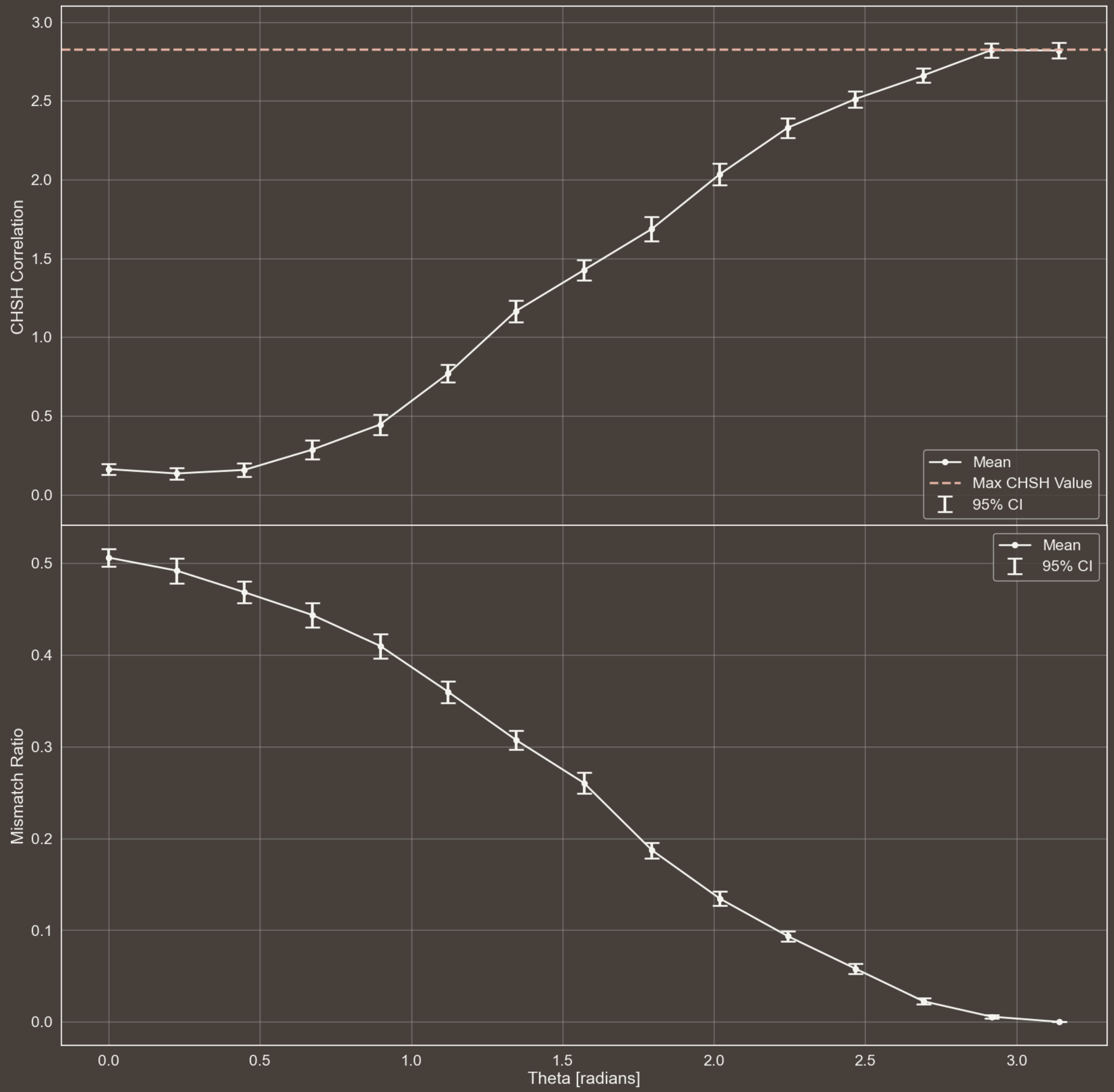
EFFECT OF VARYING **#EPR PAIRS**

n → 30

θ → $\left[\frac{i}{14}\pi \mid i = 0,1,\dots,14\right]$

Eavesdropping → False

#EPR Pairs → 1000



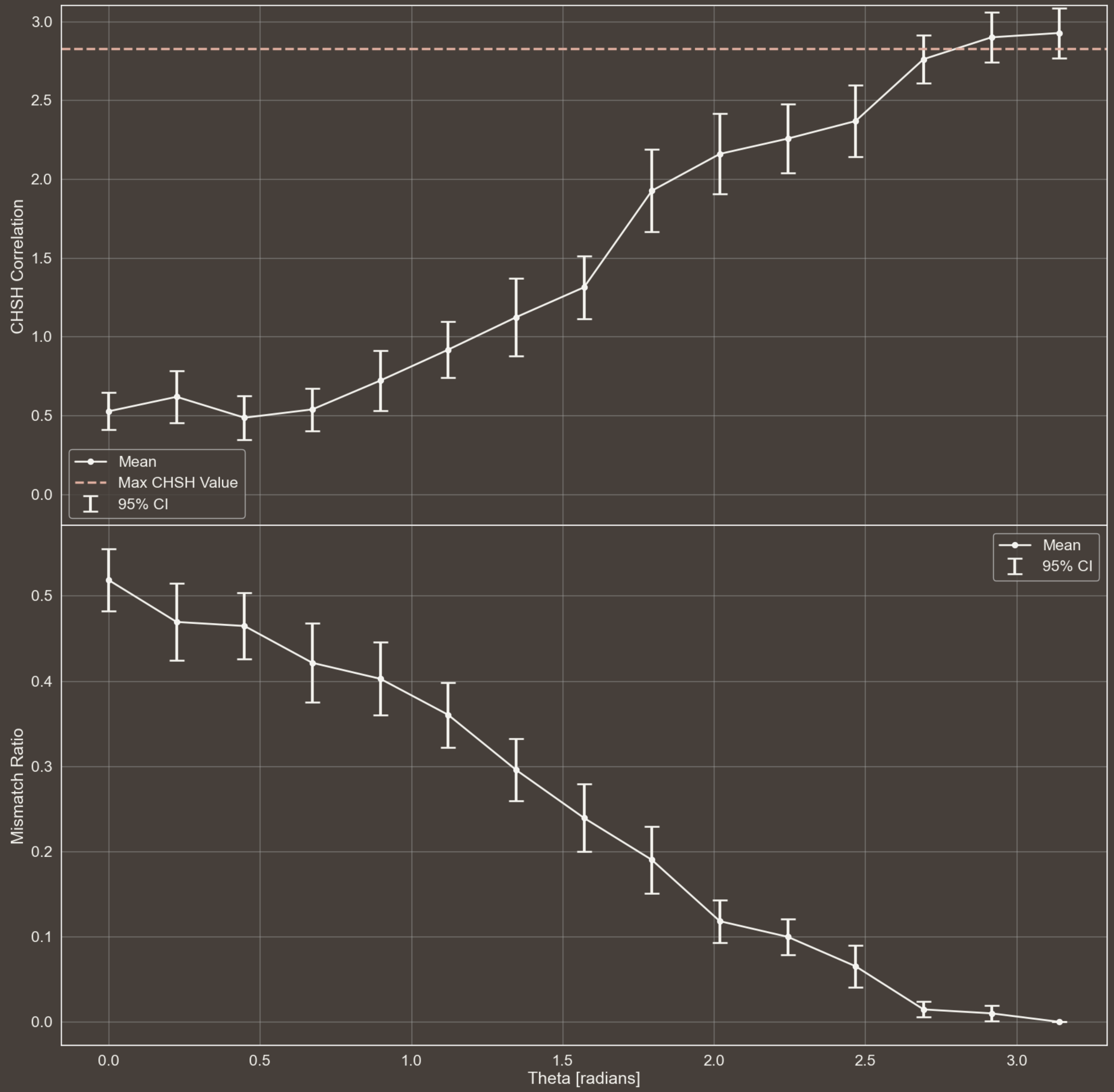
EFFECT OF VARYING
#EPR PAIRS

n → 30

θ → $\left[\frac{i}{14}\pi \mid i = 0,1,\ldots,14\right]$

Eavesdropping → False

#EPR Pairs → 80



WHAT'S THE EFFECT

OF VARYING THE NUMBER OF ENTANGLED PAIRS PER PROTOCOL EXECUTION ON THE EVALUATED METRICS?

THE PRIMARY EFFECT IS INCREASED **INSTABILITY** IN THE MEASURED QUANTITIES, REFLECTED IN THE **CONFIDENCE INTERVALS**. THIS OCCURS BECAUSE USING FEWER EPR PAIRS PER PROTOCOL EXECUTION AMPLIFIES **STATISTICAL NOISE**.

CONCRETE EXAMPLE

WHEN THE NUMBER OF EPR PAIRS IS LARGE, THE RATIO OF KEY BITS TO TOTAL EPR PAIRS CONVERGES TOWARD $\frac{2}{9}$, SINCE ONLY TWO OUT OF NINE POSSIBLE CHOICES OF OBSERVABLES BY ALICE AND BOB CONTRIBUTE TO KEY GENERATION. HOWEVER, WITH FEWER EPR PAIRS, RANDOMNESS HAS A MUCH GREATER IMPACT, CAUSING SIGNIFICANT DEVIATIONS FROM THE EXPECTED VALUE IN INDIVIDUAL EXECUTIONS. THIS INCREASED VARIABILITY MAKES THE RESULTS LESS RELIABLE, AS STATISTICAL FLUCTUATIONS BECOME MORE PRONOUNCED.

THE SAME REASONING APPLIES TO THE EVALUATED METRICS.

WHAT WILL BE THE

RESULTS

IN THE SCENARIO WHERE THERE IS

EVE

THE EAVESDROPPER?

IN THIS SCENARIO, EVE SENDS ALICE AND BOB ONLY QUBIT PAIRS IN THE STATES $|01\rangle$ AND $|10\rangle$.

SINCE THESE STATES ARE NOT ENTANGLED, THE **CHSH CORRELATION** SHOULD REFLECT THIS. INSTEAD OF REACHING THE THEORETICAL MAXIMUM OF $2\sqrt{2}$, THE VALUE WILL BE SIGNIFICANTLY LOWER. THIS ALLOWS ALICE AND BOB TO DETECT THE ANOMALY AND ABORT THE PROTOCOL.

REGARDING THE **MISMATCH RATIO**, WHEN BOTH ALICE AND BOB MEASURE USING THE Z OBSERVABLE, THEY WILL OBTAIN ANTI-CORRELATED RESULTS, PRODUCING A CORRECT MATCHING BIT FOR KEY GENERATION. HOWEVER, WHEN THEY BOTH MEASURE USING $\frac{Z+X}{\sqrt{2}}$, THE OUTCOME IS LESS STRAIGHTFORWARD, REQUIRING FURTHER CALCULATIONS.

MEASURING IN THIS OBSERVABLE REQUIRES A UNITARY TRANSFORMATION THAT MAPS ITS EIGENVECTORS TO THE STANDARD BASIS, FOLLOWED BY A MEASUREMENT IN THE Z BASIS. THE REQUIRED UNITARY U IS GIVEN BELOW AND MUST BE APPLIED TO BOTH QUBITS BEFORE MEASUREMENT.

$$U = \begin{bmatrix} 0.924 & 0.383 \\ -0.383 & 0.924 \end{bmatrix}$$

Results are **rounded to three decimal places** in the slides for presentation purposes. In Python, more decimals are considered for higher accuracy.

$$U = \begin{bmatrix} 0.924 & 0.383 \\ -0.383 & 0.924 \end{bmatrix}$$

CONSIDER THE CASE WHERE EVE SENDS $|10\rangle$ TO ALICE AND BOB (THE ANALYSIS FOR THE OTHER STATE IS ANALOGOUS). THE STATE OF THE QUBITS AFTER APPLYING U TO BOTH CAN BE COMPUTED.

$$|10\rangle \cdot (U \otimes U) = (0.383|0\rangle + 0.924|1\rangle) \otimes (0.924|0\rangle - 0.383|1\rangle) =$$

$$= 0.354|00\rangle - 0.147|01\rangle + 0.854|10\rangle - 0.354|11\rangle$$

ALL FOUR MEASUREMENT OUTCOMES IN THE Z BASIS ARE POSSIBLE. WHEN THE OUTCOMES ARE 00 OR 11, THE RESULTS ARE CORRELATED, CAUSING BOB, UPON FLIPPING HIS VALUE, TO INTRODUCE A MISMATCH BETWEEN HIS KEY AND ALICE'S. THE PROBABILITY OF OBTAINING CORRELATED RESULTS IS GIVEN BY:

$$0.354^2 + 0.354^2 = 0.251$$

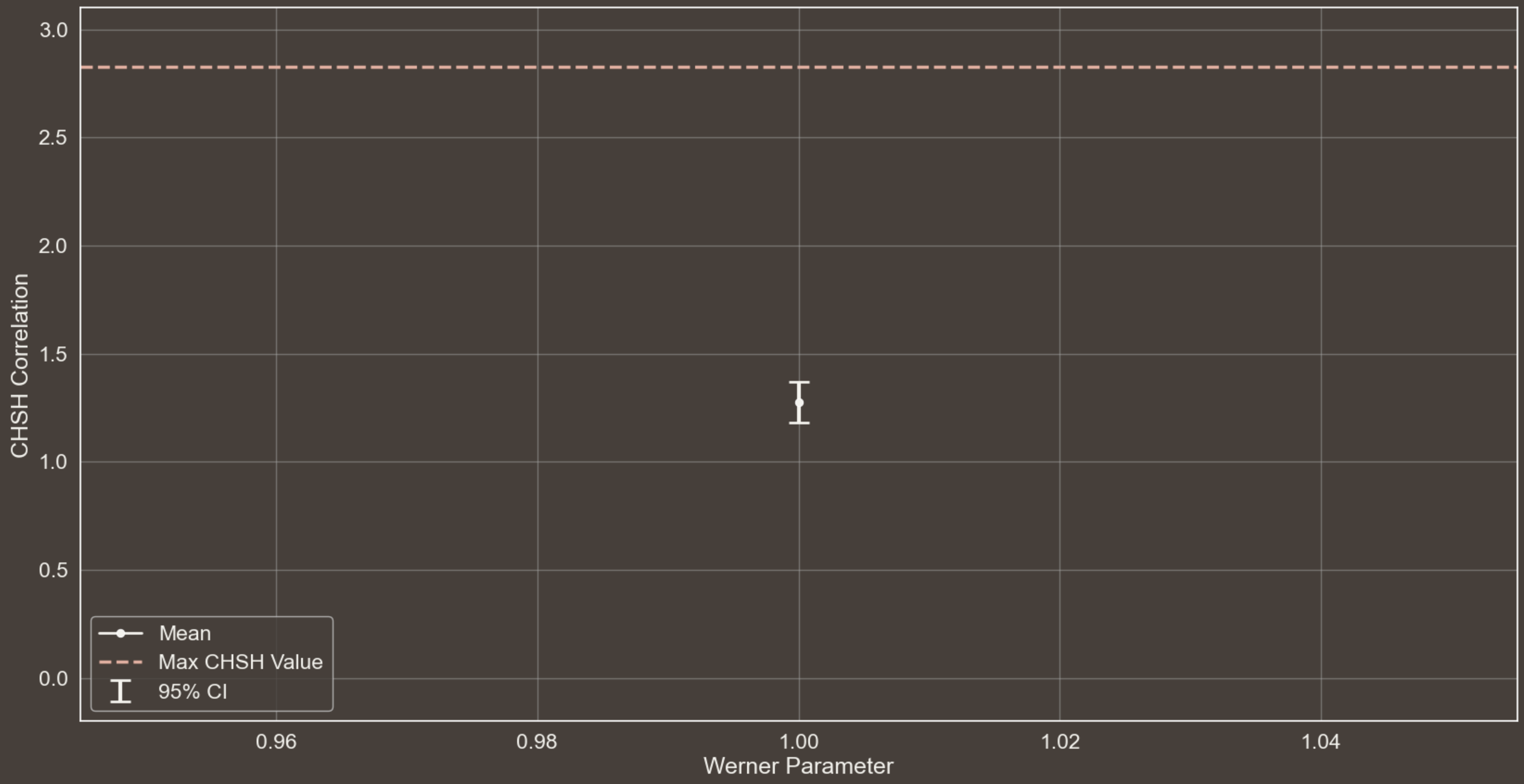
SINCE THIS SCENARIO REPRESENTS ONLY ONE OF THE TWO CASES CONTRIBUTING TO KEY GENERATION (THE OTHER BEING WHEN BOTH ALICE AND BOB CHOOSE Z AS THE OBSERVABLE, WHICH DOES NOT INTRODUCE MISMATCHED BITS), MULTIPLYING BY $\frac{1}{2}$ GIVES THE TOTAL PROBABILITY OF KEY ERRORS.

$$0.251 \cdot \frac{1}{2} = 0.125$$

IN THE MISMATCH RATIO PLOT, THE CONFIDENCE INTERVAL SHOULD ENCOMPASS THIS VALUE

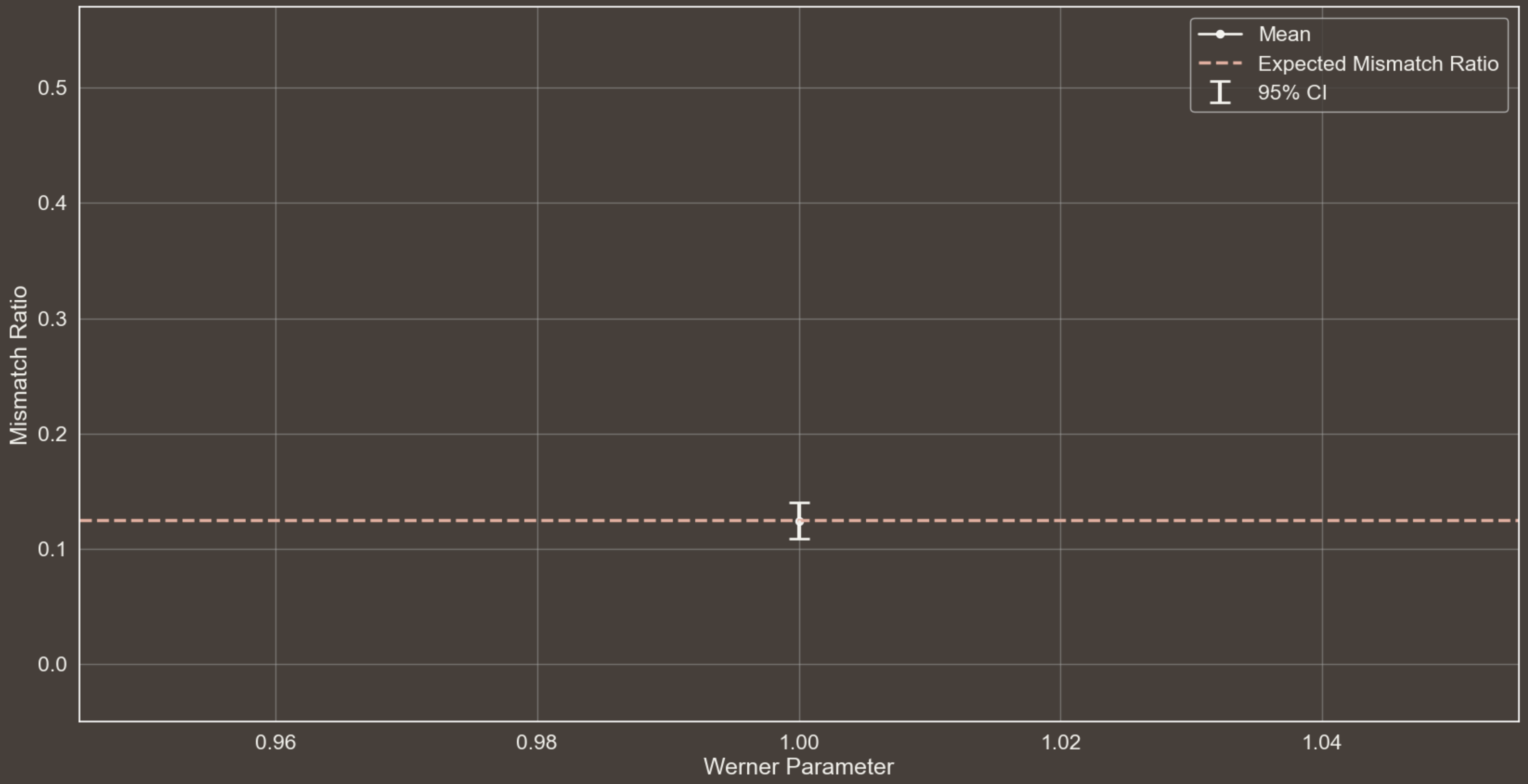
Results are **rounded to three decimal places** in the slides for presentation purposes. In Python, more decimals are considered for higher accuracy.

CHSH CORRELATION WITH 95% CI **vs** **WERNER PARAMETER**



n → 30 **θ** → [π] **Eavesdropping** → True **#EPR Pairs** → 300

MISMATCH RATIO WITH 95% CI vs WERNER PARAMETER



n → 30 **θ** → $[\pi]$ **Eavesdropping** → True **#EPR Pairs** → 300

REFERENCES

[1] CHSH INEQUALITY
https://en.wikipedia.org/wiki/CHSH_inequality

[2] QUANTUM CORRELATION
https://en.wikipedia.org/wiki/Quantum_correlation

[3] TSIRELSON'S BOUND
https://en.wikipedia.org/wiki/Tsirelson's_bound

PALETTE

coolors.co/palette/463f3a-8a817c-bcb8b1-f4f3ee-e0afa0

ICONS

flaticon

www.flaticon.com

THANKS

FOR YOUR ATTENTION