# Finite-Key Security Proofs and Key Rate Analysis of Entanglement-Based Quantum Key Distribution with Alternate Measurement Bases

Cao Xizhen[1], Kaylen Liew Tong En[1], Leong Wei Chan[1]

December 2025

## 1 Abstract

Most existing analyses of entanglement-based quantum key distribution protocols are performed in the asymptotic limit of infinite key exchange, producing ideal Bell Inequality parameters. However, these ideal values are often not achievable in practical implementations with finite datasets. In this work, we present a finite-key analysis of entanglement-based quantum key distribution and derive acceptable thresholds for deviations of the observed CHSH Bell parameters from ideal asymptotic values. Using the Ekert-91(E91) protocol, we investigate the effects of channel noise and varied measurement basis choices through numerical simulations. We show that appropriate selections of measurement bases can provide greater security and improve achievable key rates, even with finite exchanges. These findings can provide practical guidance for the optimisation of entanglement-based systems under realistic conditions.

# 2 Introduction

## 2.1 Review of existing work

### 2.1.1 Entanglement-based protocols and Bell paramters

### 2.1.2 Efficacy of multiple measurement Bases

### 2.1.3 Dataset size constraints

## 2.2 Hypothesis

### 2.2.1 Ideal error rate thresholds

### 2.2.2 Key rate bounds

# 3 Simulation and Results

## 3.1 System

## 3.2 Methodology

## 3.3 Results

### 3.3.1 Threshold for deviations

### 3.3.2 Effects of different dataset sizes

### 3.3.3 Comparison of security, key rate, and resource management for variable measurement bases

### 3.3.4 How eavesdroppers can practically leak information

# 4 Conclusion

# 5 Future work

# 6 References

# 7 Appendix