Article

A Simulated QKD Protocol Using KCBS Contextuality: Comparison with BB84

Samiksha BC * and Dipak Chaulagain

Posted Date: 29 September 2025

doi: 10.20944/preprints202509.2387.v1

Keywords: BB84; QuTip; QBER; CTX_QKD; RSA; KCBS

Article

A Simulated QKD Protocol Using KCBS Contextuality: Comparison with BB84

Samiksha BC [1,*] and Dipak Chaulagain [2]

[1] ACM Student Chapter, Indiana University South Bend, South Bend, IN, USA
[2] IT Engineer, Dish Media Network Ltd., Lalitpur, Bagmati, Nepal
* Correspondence: bcsamikshya@gmail.com

Abstract

This paper presents a detailed theoretical and simulation-based comparison between the BB84 quantum key distribution (QKD) protocol and a proof-of-concept contextuality-based QKD protocol (CTX-QKD) under depolarizing noise. We begin by contrasting classical cryptography's computational security with quantum cryptography's information-theoretic guarantees. The physics of quantum cryptography, including superposition, entanglement, and the no-cloning theorem, is explored, followed by a mathematical analysis of BB84 and a proposed CTX-QKD framework. Performance metrics include the quantum bit error rate (QBER) for BB84 and contextuality violation measures for CTX-QKD, with confidence intervals derived from proper statistical bounds. A comprehensive simulation methodology using QuTiP, NumPy, and SciPy is described. Simulation results demonstrate that while BB84 shows expected noise tolerance up to 11% QBER, the CTX-QKD protocol maintains strong contextuality violations of the fundamental security condition under high noise conditions where BB84 fails. This study highlights the potential of contextuality as a resource for quantum cryptography and demonstrates a proof-of-concept for physics-based cryptographic security beyond traditional approaches.

Keywords: BB84; QuTip; QBER; CTX_QKD; RSA; KCBS

1. Introduction

Cryptography underpins secure communication in the digital age. Classical cryptography, reliant on computational hardness assumptions, faces existential threats from quantum computing, necessitating quantum cryptography as a robust alternative. Quantum key distribution (QKD), exemplified by the BB84 protocol, leverages quantum mechanics to achieve information-theoretic security. Emerging protocols, such as those based on quantum contextuality, offer novel approaches to QKD, though their practical implementation presents unique challenges.

This paper compares BB84 with a contextuality-based QKD protocol (CTX-QKD) through theoretical analysis and numerical simulations. We discuss the foundations and limitations of classical cryptography, the physics and mathematics of quantum cryptography, and provide a detailed simulation methodology. The study aims to evaluate the protocols' performance under depolarizing noise, focusing on Quantum Bit Error Rate (QBER) and contextuality violation measures.

2. Classical Cryptography and Its Limitations

Classical cryptography consists of symmetric and asymmetric methods. Symmetric systems, such as AES, use a shared secret key: encryption is $C = E_K(P)$ and decryption is $P = D_K(C)$. However, the key distribution remains challenging.

Asymmetric systems, such as RSA, rely on mathematical hardness assumptions. In RSA, the public key (N, e) encrypts messages, while the private key d satisfies $ed \equiv 1 \pmod{\phi(N)}$. The difficulty of factoring N provides security. However, Shor's algorithm can factor integers efficiently on a quantum computer, threatening RSA and elliptic-curve cryptography.

 doi:10.20944/preprints202509.2387.v1

These vulnerabilities motivate post-quantum cryptography and quantum cryptography. Unlike classical systems, quantum protocols provide *information-theoretic security* guaranteed by physics, not computational assumptions.

3. Theoretical Foundations of Quantum Cryptography

Quantum cryptography builds security from the fundamental principles of quantum mechanics rather than computational hardness. This section explores its key concepts in detail.

3.1. Hilbert Space Formalism

Quantum states reside in a complex Hilbert space $\mathcal{H}$, a complete inner product space that provides the mathematical foundation for quantum mechanics. For quantum information processing:

- **Qubit Systems**: $\mathcal{H}_2 = \mathbb{C}^2$ spanned by orthonormal basis $\{|0\rangle, |1\rangle\}$
- **Qutrit Systems**: $\mathcal{H}_3 = \mathbb{C}^3$ spanned by $\{|0\rangle, |1\rangle, |2\rangle\}$
- **State Vectors**: Pure states $|\psi\rangle \in \mathcal{H}$ with $\langle\psi|\psi\rangle = 1$
- **Operators**: Physical observables represented by Hermitian operators $A : \mathcal{H} \to \mathcal{H}$

The inner product $\langle\phi|\psi\rangle$ induces the probability structure via Born's rule: $P(i) = |\langle\phi_i|\psi\rangle|^2$.

3.2. Quantum States and Measurement

The state of a quantum system is represented by a vector $|\psi\rangle$ in a Hilbert space $\mathcal{H}$. For a qubit:

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle, \quad |\alpha|^2 + |\beta|^2 = 1.$$

Measurement in basis $\{|0\rangle, |1\rangle\}$ yields 0 with probability $|\alpha|^2$ and 1 with probability $|\beta|^2$. More generally, mixed states are described by a density operator $\rho = \sum_i p_i|\psi_i\rangle\langle\psi_i|$, with $\mathrm{Tr}(\rho) = 1$. The Born rule gives the probability of the outcome i as $p_i = \mathrm{Tr}(M_i\rho)$, where $\{M_i\}$ are projectors.

3.3. Mutual Information and Holevo Bound

The secure key rate can be bounded as follows:

$$K \geq I(A:B) - I(A:E),$$

where $I(A:B)$ is the mutual information between Alice and Bob, and $I(A:E)$ is the information of Eve. Quantum information theory limits Eve's accessible information by the *Holevo bound*:

$$I(A:E) \leq \chi = S(\rho_E) - \sum_x p(x)S(\rho_E^x),$$

where $S(\cdot)$ denotes von Neumann entropy. Thus, QKD achieves security by ensuring that Eve's accessible information remains negligible.

3.4. Devetak–Winter Key Rate

The Devetak Winter formula refines the asymptotic key rate.

$$K = H(A|E) - H(A|B),$$

where $H(A|E)$ is the conditional entropy of Alice given to Eve and $H(A|B)$ is the error correction cost. For BB84, this leads to a secure threshold at QBER $\approx 11\%$.

3.5. Entanglement and Nonlocality

Entanglement is a uniquely quantum phenomenon where composite systems cannot be described by product states. For example:

$$|\Phi^+\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}}.$$

 doi:10.20944/preprints202509.2387.v1

Measurements on entangled qubits exhibit correlations that violate classical Bell inequalities. In QKD (e.g., the Ekert91 protocol), these correlations certify security because an eavesdropper cannot reproduce them without being detected.

3.6. The No-Cloning Theorem

The no-cloning theorem prohibits the perfect copying of an unknown quantum state. Suppose a universal cloner U exists such that $U|\psi\rangle|0\rangle = |\psi\rangle|\psi\rangle$ for all $|\psi\rangle$. Linearity implies:

$$U(\alpha|0\rangle + \beta|1\rangle)|0\rangle = \alpha|00\rangle + \beta|11\rangle,$$

which is not equal to $(\alpha|0\rangle + \beta|1\rangle)(\alpha|0\rangle + \beta|1\rangle)$. Hence, cloning is impossible. This ensures that eavesdropping attempts necessarily disturb the transmitted qubits.

3.7. Noise in Quantum Channels

Real-world channels introduce errors via:

- **Depolarizing noise**: transforms $\rho \to (1-p)\rho + \frac{p}{d}I$.
- **Amplitude damping**: models energy loss, such as photon absorption.
- **Phase damping**: models dephasing without energy loss.
- **Detector noise**: dark counts and efficiency mismatches.

These noise sources determine the practical security thresholds of QKD.

4. The BB84 Protocol

The BB84 protocol, proposed in 1984 by Bennett and Brassard, remains the most widely studied and experimentally implemented QKD scheme. Its security rests on the interplay of basis choice, measurement disturbance, and privacy amplification.

4.1. Protocol Steps

1. **State preparation**: Alice encodes each random bit into one of two bases:

   $$\text{Rectilinear: } |0\rangle, |1\rangle \quad \text{Diagonal: } |+\rangle, |-\rangle,$$

   where $|+\rangle = (|0\rangle + |1\rangle)/\sqrt{2}$ and $|-\rangle = (|0\rangle - |1\rangle)/\sqrt{2}$.
2. **Transmission**: Qubits are sent through a quantum channel (e.g., optical fiber or free space). Channel noise may disturb states.
3. **Measurement**: Bob randomly selects a basis (rectilinear or diagonal) and measures. Outcomes are probabilistic if his basis differs from Alice's.
4. **Sifting**: Alice and Bob announce bases publicly and keep only those bits where bases match. This produces the *sifted key*.
5. **Error estimation**: They publicly compare a subset of the sifted key. If QBER exceeds a threshold ($\approx 11\%$), they abort.
6. **Reconciliation**: Using classical error correction (e.g., Cascade), Alice and Bob reconcile discrepancies.
7. **Privacy amplification**: By applying universal hash functions, they compress the key to eliminate Eve's information.

4.2. Security Against Intercept–Resend

Suppose Eve intercepts and measures each qubit. If she guesses Alice's basis correctly, she forwards the correct bit. If she guesses incorrectly (50% chance), she forwards a wrong state, causing Bob to measure incorrectly with 50% probability. Thus, Eve introduces an error rate of:

$$\text{QBER} = 0.5 \times 0.5 = 25\%.$$

 doi:10.20944/preprints202509.2387.v1

Detecting such elevated QBER allows Alice and Bob to infer eavesdropping.

4.3. Mathematical Formalism

For each transmitted qubit:

$$P(\text{error}) = \frac{1}{2} \cdot P(\text{wrong outcome}|\text{wrong basis}) = \frac{1}{2} \cdot \frac{1}{2} = 0.25.$$

The security condition is $I(A:B) > I(A:E)$, where $I(\cdot:\cdot)$ denotes mutual information. For QBER $< 11\%$, Alice and Bob's mutual information exceeds Eve's, allowing secure key generation.

5. Contextuality-Based QKD (CTX-QKD)

Quantum contextuality arises from the Kochen-Specker theorem, formalized through inequalities such as KCBS. CTX-QKD employs qutrit states arranged to maximize contextual correlations.

5.1. Contextuality and KCBS Inequality

Contextuality is a nonclassical feature beyond entanglement. The KCBS inequality provides a test:

$$S_{\text{KCBS}} = \sum_{i=1}^{5} \langle A_i A_{i+1} \rangle \geq -3,$$

for noncontextual hidden-variable theories. Quantum mechanics violates this bound, achieving $S_{\text{KCBS}} \approx -3.94$ for optimal qutrit states.

5.2. CTX-QKD Protocol Design

Our CTX-QKD protocol represents a proof-of-concept implementation that focuses on the core security verification mechanism using quantum contextuality. The protocol uses five optimized qutrit states $\{|\psi_i\rangle\}_{i=1}^{5}$ defined by:

$$|\psi_i\rangle = r(\cos\theta_i|0\rangle + \sin\theta_i|1\rangle) + \gamma|2\rangle,$$

where $\theta_i = 2\pi(i-1)/5$, $r = 1/\sqrt{1+\cos(\pi/5)}$, and $\gamma = \sqrt{\cos(\pi/5)/(1+\cos(\pi/5))}$.

The protocol proceeds as:

1. **State Preparation**: Alice randomly prepares and sends one of the five contextuality states
2. **Measurement**: Bob randomly chooses between two measurement strategies:
   - *Key Generation Mode*: Measure in the same basis as preparation (for feasibility testing)
   - *Security Verification Mode*: Measure in adjacent bases to compute contextuality violation
3. **Security Check**: They evaluate adjacent measurements to compute the KCBS contextuality violation, which serves as the security precondition

Note: This implementation focuses on validating the core security mechanism—contextuality violation—rather than full key distribution. A complete protocol would require additional components for actual key generation and privacy amplification.

5.3. Security Analysis

In this proof-of-concept implementation, security is *indicated* when the observed KCBS value violates the noncontextual bound:

$$S_{\text{KCBS}} < -3.$$

In our implementation, we use the normalized contextuality measure:

$$C_{\text{norm}} = \frac{-S_{\text{KCBS}} - 3}{3.94 - 3},$$

with the security precondition threshold $C_{\text{norm}} > 0$.

 doi:10.20944/preprints202509.2387.v1

Important Distinction: Unlike BB84, where QBER directly determines security, in CTX-QKD the contextuality violation serves as a necessary *precondition* for security. A maintained violation indicates that the quantum channel preserves the contextual correlations needed for security, but does not by itself guarantee full cryptographic security. The protocol status "Secure" in our results indicates that this fundamental security precondition is satisfied, not that a full key distribution has been cryptographically secured.

This approach demonstrates the potential of contextuality as an alternative foundation for quantum cryptographic security, though a complete protocol would require integration with error correction and privacy amplification stages.

6. Methodology

To compare the performance of BB84 and Contextuality-based QKD (CTX-QKD), we designed a simulation framework incorporating both theoretical models and statistical validation. The methodology is divided into four key phases: system modeling, noise introduction, protocol simulation, and performance evaluation.

6.1. System Modeling

- **BB84 model**: Implemented using polarization encoding in two mutually unbiased bases. The primary parameter extracted is the Quantum Bit Error Rate (QBER).
- **CTX-QKD model**: Implemented using five optimized qutrit states for contextuality violation. The key metrics are QBER and normalized contextuality measure.

6.2. Noise Modeling

To ensure fair comparison, we introduced *depolarizing noise* into both systems:

$$\rho \to (1-p)\rho + \frac{p}{d}I,$$

where p is the noise probability and d the dimension of the system. Noise was varied systematically ($p = 0.0$ to 0.5) to simulate increasing channel imperfections.

6.3. Protocol Simulation

1. **Key generation**: Random states prepared in respective bases.
2. **Transmission**: States transmitted through noisy channel.
3. **Measurement**: Recipient performs measurements.
4. **Sifting and estimation**:
   - BB84: Sifted key obtained by basis reconciliation; QBER estimated from test subset.
   - CTX-QKD: Key bits from matching bases; contextuality from adjacent measurements.
5. **Security check**:
   - BB84 secure if QBER $< 11\%$.
   - CTX-QKD secure if $C_{\text{norm}} > 0$.

6.4. Statistical Analysis

Each protocol was simulated over 10^4 trials per noise level. Mean QBER and contextuality scores were computed. 95% confidence intervals were obtained using the Wilson score interval for proportions:

$$CI = \hat{p} + \frac{z^2}{2n} \pm z\sqrt{\frac{\hat{p}(1-\hat{p})}{n} + \frac{z^2}{4n^2}} \Big/ \left(1 + \frac{z^2}{n}\right),$$

where $\hat{p}$ is the observed proportion, n the sample size, and $z = 1.96$ for 95% confidence.

 doi:10.20944/preprints202509.2387.v1

7. Results and Discussion

Our simulation study conducted over 10,000 rounds per noise level provides statistically robust comparisons between BB84 and CTX-QKD protocols. The results, summarized in Table 1 with 95% Wilson confidence intervals, reveal important insights about both protocols' performance under depolarizing noise.

Table 1. Simulation Results: Means with 95% Wilson Confidence Intervals.

Noise	BB84 QBER		CTX-QKD QBER		Contextuality		BB84	CTX
p	Mean	$\pm$ CI	Mean	$\pm$ CI	Mean	$\pm$ CI	Status	Status
0.00	0.000	$\pm$ 0.000	0.000	$\pm$ 0.000	0.057	$\pm$ 0.006	Secure	Secure
0.10	0.045	$\pm$ 0.004	0.069	$\pm$ 0.005	0.068	$\pm$ 0.007	Secure	Secure
0.20	0.098	$\pm$ 0.006	0.135	$\pm$ 0.007	0.150	$\pm$ 0.010	Warning	Secure
0.30	0.143	$\pm$ 0.007	0.201	$\pm$ 0.008	0.157	$\pm$ 0.010	Compromised	Secure
0.50	0.252	$\pm$ 0.009	0.334	$\pm$ 0.009	0.197	$\pm$ 0.011	Compromised	Secure

7.1. Analysis of BB84 Performance

The BB84 simulation results demonstrate the protocol's characteristic behavior under depolarizing noise. The QBER increases monotonically with noise probability, showing:

- **Secure operation** ($p \leq 0.1$): QBER remains below 5%, well within the security threshold
- **Warning state** ($p = 0.2$): QBER approaches the 11% critical threshold at 9.8%
- **Compromised security** ($p \geq 0.3$): QBER exceeds 11%, reaching 25.2% at $p = 0.5$

These results align with theoretical expectations, where depolarizing noise at probability p produces a QBER of approximately $p/2$ for BB84. The narrow confidence intervals confirm statistical reliability across all noise levels.

7.2. Analysis of CTX-QKD Performance

The CTX-QKD protocol exhibits distinct but promising characteristics:

- **QBER Performance**: CTX-QKD shows higher baseline QBER compared to BB84 (6.9% vs 4.5% at $p = 0.1$, 33.4% vs 25.2% at $p = 0.5$). This indicates greater sensitivity to depolarizing noise in the key generation component.
- **Contextuality Robustness**: Despite higher QBER, the contextuality measure shows excellent noise resistance:
  - Maintains positive contextuality scores across all noise levels
  - Actually *increases* with noise (0.057 to 0.197 from $p = 0.0$ to $p = 0.5$)
  - Remains above security threshold (> 0) even at high noise levels
- **Security Status**: The protocol maintains "Secure" status across all tested noise levels due to persistent contextuality violations, despite elevated QBER values.

7.3. Comparative Analysis and Theoretical Implications

The divergent behavior between QBER and contextuality measures in CTX-QKD reveals fundamental differences in security mechanisms:

7.3.1. BB84 Security Foundation

BB84 security relies directly on low QBER, with the 11% threshold derived from information-theoretic bounds where $I(A:B) > I(A:E)$. Our results confirm this theoretical framework, with security compromise occurring precisely where expected.

 doi:10.20944/preprints202509.2387.v1

7.3.2. CTX-QKD Security Foundation

CTX-QKD demonstrates an alternative security paradigm where:

$$\text{Security Precondition} \propto \text{Contextuality Violation}$$

The persistent contextuality measure under noise suggests that contextuality-based approaches may offer advantages in high-noise environments. However, it is crucial to emphasize that this represents the *foundation* for security rather than complete cryptographic security, which would require additional protocol components.

7.3.3. Noise Tolerance Comparison

- **BB84**: Practical security limit at $p \approx 0.2$ (QBER $\approx 10\%$)
- **CTX-QKD**: Maintains theoretical security up to $p = 0.5$ (QBER $\approx 33\%$)

While CTX-QKD shows higher operational QBER, its contextuality-based security remains robust under conditions where BB84 fails. This suggests potential applications in high-noise environments where traditional QKD protocols are impractical.

7.4. Statistical Reliability

The Wilson confidence intervals provide proper uncertainty quantification for binomial proportions. The consistent interval widths across measurements (0.004-0.011) indicate:

- High statistical power with 10,000 rounds per configuration
- Reliable estimation of both QBER and contextuality measures
- Physically meaningful results without implementation artifacts

The statistical analysis confirms that observed differences between protocols are significant and not due to measurement uncertainty.

7.5. Limitations and Implementation Challenges

The current implementation reveals several important considerations for contextuality-based QKD:

- **Higher Operational Overhead**: CTX-QKD requires approximately twice the quantum transmissions for equivalent key generation due to separate contextuality verification rounds
- **Key Rate Considerations**: While maintaining security at higher noise levels, the elevated QBER reduces the final key rate after error correction
- **Practical Implementation**: The qutrit-based states required for optimal KCBS violation present experimental challenges compared to BB84's qubit-based implementation

8. Conclusion

This comparative analysis demonstrates that contextuality-based QKD offers a viable alternative to established protocols like BB84, with distinct advantages in noise resilience. Key findings include:

- **BB84** performs as theoretically expected, with security compromise at the predicted 11% QBER threshold
- **CTX-QKD** maintains contextuality-based security under high noise conditions where BB84 fails, despite higher operational QBER
- The separation between key generation reliability (QBER) and security verification (contextuality) in CTX-QKD represents a novel architectural approach to quantum cryptography
- Contextuality measures show unexpected noise resilience, potentially enabling QKD in environments previously considered too noisy for secure quantum communication

While BB84 remains the practical choice for current implementations due to its simplicity and extensive validation, CTX-QKD demonstrates theoretical promise for specialized applications requiring

 doi:10.20944/preprints202509.2387.v1

exceptional noise tolerance. Future work should focus on optimizing the bit encoding scheme to reduce operational QBER while maintaining contextuality violations, potentially through adaptive measurement strategies or advanced error correction techniques.

The successful demonstration of contextuality-based security under depolarizing noise opens new avenues for quantum cryptography beyond the no-cloning theorem, suggesting that quantum contextuality may serve as a fundamental resource for next-generation secure communication protocols.

Future work should focus on developing complete protocol implementations that integrate robust key generation, error correction, and privacy amplification with the contextuality-based security verification demonstrated here.

References

1. C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing*, 1984.
2. P. Shor, "Algorithms for quantum computation: discrete logarithms and factoring," *Proceedings 35th Annual Symposium on Foundations of Computer Science*, 1994.
3. A. Ekert, "Quantum cryptography based on Bell's theorem," *Phys. Rev. Lett.*, vol. 67, no. 6, 1991.
4. A. A. Klyachko, M. A. Can, S. Binicioğlu, and A. S. Shumovsky, "Simple test for hidden variables in spin-1 systems," *Phys. Rev. Lett.*, vol. 101, no. 2, 2008.
5. V. Scarani et al., "The security of practical quantum key distribution," *Rev. Mod. Phys.*, vol. 81, no. 3, 2009.