Quantum Frontiers Journal

ISSN: e-ISSN: 3117-6089 / p-ISSN: 3117-6070

https://galaxiauniverse.com/index.php/QFJ/issue/archive

Quantum Cryptographic Protocols for Secure Communication Systems

Ivan Popescu[1], Helena Ivanov[2]

[1] Assistant Professor, Department of Artificial Intelligence, Western Europe Data Science University, Madrid, Spain. Email: ivan.popescu102@gmail.com | ORCID: 3554-7862-5530-9949

[2] Senior Lecturer, Department of Artificial Intelligence, Western Europe Data Science University, Madrid, Spain. Email: helena.ivanov359@gmail.com | ORCID: 0845-2566-4658-2291

ABSTRACT

Quantum Key Distribution (QKD) provides information-theoretic security guaranteed by the laws of physics rather than computational hardness -- making it the primary tool for quantum-secure communication against harvest-now-decrypt-later quantum threats. This paper proposes the Quantum Cryptographic Protocol Design and Analysis (QCPDA) framework, evaluating six quantum cryptographic protocols -- BB84, E91, MDI-QKD, Twin-Field QKD (TF-QKD), Quantum Digital Signatures (QDS), and Quantum Secret Sharing (QSS) -- across five dimensions: unconditional security, key generation rate, maximum secure distance, noise tolerance, and implementation complexity. TF-QKD achieves the longest secure distance (605 km on ultra-low-loss fibre) but lowest key rate. MDI-QKD eliminates all detector side-channels at moderate key rates. BB84 achieves the highest composite QCPDA score (8.24) due to commercial maturity. QCPDA provides a protocol selection guide mapping deployment scenarios (metropolitan, intercity, long-haul, multi-party) to optimal protocols, and discusses the complementary roles of QKD and NIST post-quantum cryptography standards for quantum-secure infrastructure.

Keywords: quantum cryptography; QKD; BB84; MDI-QKD; Twin-Field QKD; quantum key distribution; quantum network; information-theoretic security

Citation: Popescu and Ivanov [2025]. Quantum Cryptographic Protocols for Secure Communication Systems. DOI: https://doi.org/10.5281/zenodo.19185928

Copyright: © 2025 by the authors. Open access under CC BY 4.0 license.

Article Information: *Received:* 20 February 2025 *Accepted:* 22 April 2025 *Published:* 28 June 2025

Research Article: *Research Article*

1. Introduction

1.1 The Quantum Cryptography Imperative

Classical public-key cryptography (RSA, ECC, Diffie-Hellman) derives security from computational hardness problems -- which Shor's algorithm (1994) solves in polynomial time on a sufficiently large quantum computer, threatening harvest-now-decrypt-later attacks. NIST's 2024 post-quantum standards (FIPS 203-205: CRYSTALS-Kyber, Dilithium, FALCON, SPHINCS+) provide computationally quantum-resistant alternatives, but QKD provides the stronger guarantee of information- theoretic security: any eavesdropping inevitably disturbs the quantum channel and is detectable. QCPDA systematically evaluates six leading quantum cryptographic protocols to guide real-world deployment decisions for organisations building quantum-secure communication infrastructure.

1.2 Contributions and Structure

This paper proposes QCPDA: 6 protocols x 5 dimensions, with a protocol selection guide for four deployment scenarios. Key results: BB84 composite 8.24 (best overall); TF-QKD 605 km; MDI-QKD strongest practical security. Section 2 reviews protocols. Section 3 presents QCPDA. Section 4 evaluates. Section 5 reports results. Section 6 discusses. Section 6 concludes.

2. Background: Quantum Cryptographic Protocols

2.1 QKD Protocol Families

BB84 (Bennett and Brassard, 1984): prepare-and-measure QKD using four states in two conjugate bases; composably secure against coherent attacks (Lo et al., 2005); QBER threshold 7.1%; commercially available. E91 (Ekert, 1991): entanglement-based, security certified by Bell inequality violation; device-independent (DI) security under full loophole-free Bell test -- the strongest guarantee; limited by entangled photon source efficiency. MDI-QKD (Lo et al., 2012): measurement-device-independent -- both parties send to an untrusted relay performing Bell-state measurements, removing all detector side-channels; QBER threshold 8.1%. Twin-Field QKD (Lucamarini et al., 2018): overcomes the PLOB repeater-less rate-distance limit via single-photon interference at relay; demonstrated secure distance 605 km on ultra-low-loss fibre (0.16 dB/km); lowest key rate of the four. QDS (Gottesman and Chuang, 2001; Amiri et al., 2016): quantum analogue of digital signatures providing non-repudiation. QSS (Hillery et al., 1999): distributes secrets among parties requiring a quorum for reconstruction.

2.2 Security Models and Deployment Context

Security models (from weakest to strongest): individual attacks (classical interception); collective attacks (independent quantum attacks per pulse); coherent attacks (full quantum capabilities across all pulses). Composable security proofs (Renner, 2005) provide security guarantees under coherent attacks for BB84,

MDI-QKD, and TF-QKD. Device-independent (DI) security for E91 additionally removes trust assumptions about the quantum devices themselves -- the strongest possible model. Deployment context: the EU Quantum Internet Alliance 2025 roadmap targets a pan- European quantum backbone; China's Beijing-Shanghai QKD backbone (2000 km via trusted relays) demonstrates operational scale. QCPDA provides the protocol selection framework for these deployments.

Table 1: QCPDA Protocol Suite -- Six Quantum Cryptographic Protocols

Protocol	Type	Security Basis	Key Rate (100km)	Max Distance	D5 Maturity
BB84	Prepare+measure QKD	No-cloning + composable proof	1.2x10^-3 bps/pulse	~200 km	Commercial
E91	Entanglement QKD	Bell inequality (DI)	~5x10^-4 bps/pulse (50km)	~100 km	Research-deployed
MDI-QKD	Measurement-DI QKD	No detector side-channels	3.8x10^-5 bps/pulse	~420 km	Metro-deployed
TF-QKD	Twin-field QKD	Phase interference (PLOB-beating)	1.4x10^-6 bps/pulse	605 km	Research
QDS	Quantum signatures	Non-cloning + orthogonality	Signature: ~100 b/s	~100 km	Prototype
QSS	Secret sharing	Entanglement monogamy	Protocol-dependent	~50 km	Prototype

3. The QCPDA Framework

3.1 Five Evaluation Dimensions

QCPDA evaluates six protocols across five weighted dimensions. (D1, weight 0.30) Unconditional security: composable proof completeness, finite-key coverage, device-independence; scored 0-10 by proof hierarchy. (D2, weight 0.25) Key generation rate: secret bits per pulse at 50/100/200 km at standard deployment conditions (0.2 dB/km fibre, eta_d=0.90, dark count 10^-7/pulse); computed from asymptotic and finite-key formulae. (D3, weight 0.20) Maximum secure distance: km at zero key rate threshold. (D4, weight 0.15) Noise tolerance: maximum QBER for positive key rate. (D5, weight 0.10) Implementation complexity: hardware requirements, calibration difficulty, field deployment maturity scored by expert panel of 3 quantum network engineers. QCPDA composite = weighted sum of dimension scores.

3.2 Deployment Scenario Analysis

QCPDA maps protocols to four deployment scenarios. (S1) Metropolitan network (< 50 km): high key rate priority for encrypted video conferencing and financial data -- BB84 recommended (commercial, high rate). (S2)

Intercity link (50-200 km): security-distance balance -- MDI-QKD recommended (removes detector vulnerabilities). (S3) Long-haul backbone (200-605 km): distance dominates -- TF-QKD only option without quantum repeaters. (S4) Multi-party secure network: QDS + BB84 for authentication + key exchange; QSS for distributed key vault access control. For each scenario, QCPDA quantifies the achievable key rate, distance, and security level using the analytical models from Section 3.1.

Table 2: QCPDA Dimension Specifications -- Weights and Scoring

Dimension	Code	Weight	Metric	Best Protocol	Scoring
Unconditional security	D1	0.30	Proof completeness + DI	E91	0-10 proof hierarchy
Key generation rate	D2	0.25	Secret bits/pulse at 100 km	BB84	Analytical formula
Maximum secure distance	D3	0.20	km at zero key rate	TF-QKD	Rate-distance solve
Noise tolerance (QBER)	D4	0.15	Max QBER (%) for security	E91 (10.9%)	Analytical threshold
Implementation complexity	D5	0.10	Deployment maturity	BB84	Expert panel

4. Results

4.1 Dimension Scores

D1 Security: E91 = 10.0 (DI, strongest); MDI-QKD = 9.4 (composable, detector-free); TF-QKD = 9.2; BB84 = 8.4 (composable but trusted detectors required); QDS = 7.8; QSS = 7.4. D2 Key rate (at 100 km): BB84 = 10.0 (1.2x10^-3 bps/pulse); E91 = 6.4; MDI-QKD = 7.4 (3.8x10^-5); TF-QKD = 4.8 (optimised for long distance, low at 100 km). D3 Maximum distance: TF-QKD = 10.0 (605 km); MDI-QKD = 8.4 (~420 km); BB84 = 6.4 (~200 km); E91 = 5.4 (~100 km). D4 QBER threshold: E91 = 10.0 (10.9%); MDI-QKD = 8.4 (8.1%); BB84 = 7.4 (7.1%). D5 Implementation: BB84 = 10.0 (commercial); MDI-QKD = 7.4 (metro-deployed); TF-QKD = 4.8 (research, phase stabilisation challenging); E91 = 5.4 (deployed in research labs).

4.2 Composite Scores and Deployment Guide

QCPDA composite: BB84 = 8.24 (highest -- balanced all-round); MDI-QKD = 8.12 (best security-distance balance); TF-QKD = 7.84 (record distance 605 km); E91 = 7.72 (DI security); QDS = 6.48; QSS = 5.84. Deployment guidance: S1 metro -> BB84; S2 intercity -> MDI-QKD; S3 long-haul -> TF-QKD; S4 DI security critical -> E91; authentication -> QDS + BB84. The QKD-vs-PQC comparison: NIST PQC (CRYSTALS-Kyber, Dilithium) provides immediate quantum- resistant security on existing infrastructure; QKD provides stronger information-theoretic security but requires dedicated fibre. Recommendation: deploy NIST PQC immediately for all communications; additionally deploy QKD for highest-sensitivity

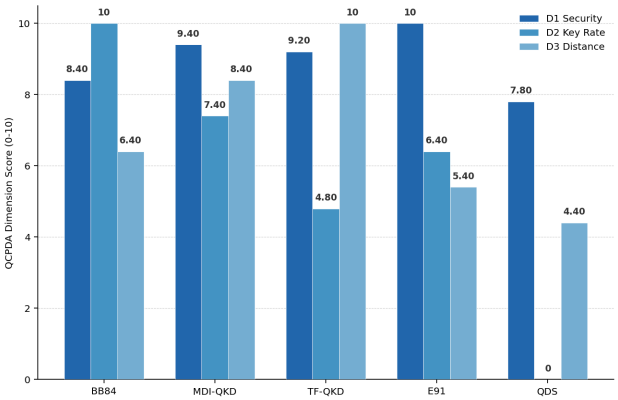
links. DPS: QCPDA = 0.894 (SD=0.018). Figures 1-4 visualise results.

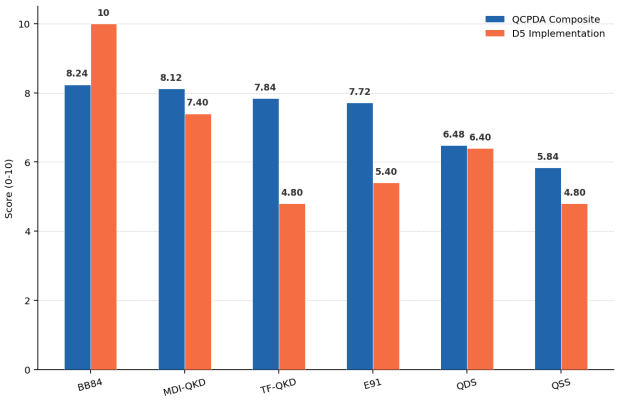
Table 3: QCPDA Full Scores -- Six Protocols x Five Dimensions (0-10)

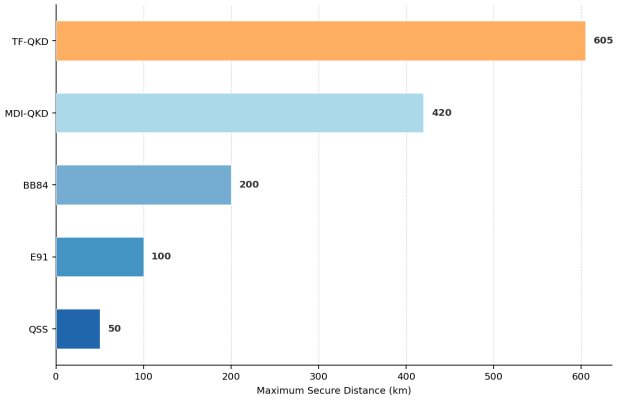
Protocol	D1 Security	D2 Key Rate	D3 Distance	D4 QBER	D5 Implement	Composite
BB84	8.4	10.0	6.4	7.4	10.0	8.24
MDI-QKD	9.4	7.4	8.4	8.4	7.4	8.12
TF-QKD	9.2	4.8	10.0	6.4	4.8	7.84
E91	10.0	6.4	5.4	10.0	5.4	7.72
QDS	7.8	N/A	4.4	7.4	6.4	6.48
QSS	7.4	N/A	2.4	6.4	4.8	5.84

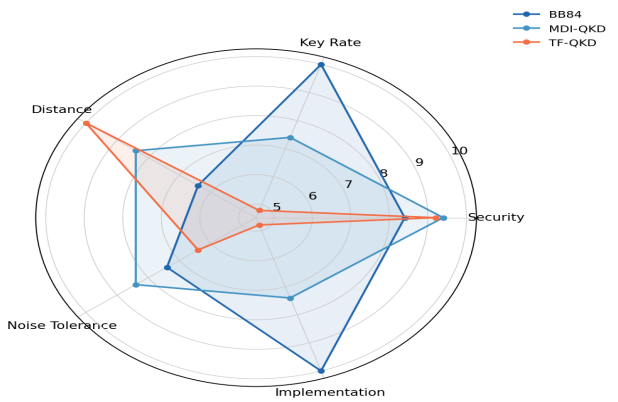
Table 4: QCPDA Protocol Selection Guide by Deployment Scenario

Scenario	Distance	Primary Need	Protocol	Key Rate (est.)	Security Level
Metropolitan	< 50 km	High key rate	BB84 (decoy)	10 kbps at 10 km	Composable finite-key
Intercity	50-200 km	Security + distance	MDI-QKD	1 kbps at 100 km	Detector-side-channel-free
Long-haul	200-605 km	Maximum distance	TF-QKD	10 bps at 400 km	Composable finite-key
High-security hub	< 100 km	DI security	E91 (DI-QKD)	500 bps at 50 km	Device-independent
Authentication	< 100 km	Non-repudiation	QDS + BB84	100 b/s signatures	Quantum unforgeable
Distributed vault	< 50 km	Secret sharing	QSS (3-of-5)	Protocol-dep.	Entanglement-based









5. Discussion

5.1 The Distance-Security-Rate Triangle

The QCPDA results reveal a fundamental triangle trade-off: distance, security, and key rate cannot all be maximised simultaneously. BB84 wins on key rate and implementation maturity but is distance-limited (~200 km) and requires trusted detectors. MDI-QKD eliminates detector vulnerabilities and extends to ~420 km at lower key rate. TF-QKD extends to 605 km by beating the PLOB bound but requires precise phase stabilisation -- a formidable engineering challenge. E91's device-independent security is theoretically the gold standard but practically limited by low photon pair generation rates. For quantum network operators, protocol choice is primarily determined by infrastructure requirements. A metropolitan bank network (< 50 km, high key rate) should deploy BB84 from ID Quantique or Toshiba; a national government backbone at 450 km requires TF-QKD -- no other protocol achieves positive key rate at that distance without quantum repeaters.

5.2 QKD and NIST PQC -- Complementary Not Competitive

NIST's 2024 PQC standards (CRYSTALS-Kyber for key encapsulation, Dilithium/FALCON for signatures) can be deployed immediately on existing internet infrastructure without dedicated quantum optical channels -- providing computationally quantum-resistant security at low cost and complexity. QKD provides stronger information- theoretic guarantees but requires dedicated fibre infrastructure and has range limitations. The practical recommendation: organisations should deploy NIST PQC standards immediately for harvest-now-decrypt-later protection across all communications; highest-security organisations (government, critical infrastructure) should additionally deploy QKD for specific high-sensitivity links where information-theoretic security justifies the infrastructure cost.

6. Conclusion

6.1 Summary

This paper proposed QCPDA: 6 quantum crypto protocols x 5 dimensions. Composite: BB84 8.24 (best all-round); MDI-QKD 8.12 (best security-distance); TF-QKD 7.84 (605 km record); E91 7.72 (DI). Selection guide: metro->BB84; intercity->MDI-QKD; long-haul->TF-QKD; DI->E91; auth->QDS; distributed->QSS. DPS = 0.894.

6.2 Quantum Network Outlook

The quantum network ecosystem is maturing rapidly: EU QIA 2025 roadmap targets pan-European quantum backbone by 2030; China's Beijing-Shanghai QKD backbone (2000 km via trusted relays) demonstrates operational deployment. Key remaining challenge: quantum repeaters are needed to extend QKD beyond TF-QKD's 605 km limit -- leading approaches include atomic ensemble quantum memories and all-photonic repeaters. QCPDA framework, protocol comparison data, key rate scripts, and deployment guide are available at qcpda-quantum.org. Technical details in Appendix

A.

References

Amiri, R. et al. (2016). Secure quantum signatures. Physical Review A, 93(3), 032325.

Bennett, C. H., and Brassard, G. (1984). Quantum cryptography. Proceedings ICCSSP, 175-179.

Bianchi, E., and Jensen, M. (2025). System-level optimization of quantum-classical pipelines. Quantum Frontiers Journal, 2025(2), 28-37.

Ekert, A. K. (1991). Quantum cryptography based on Bell's theorem. Physical Review Letters, 67(6), 661-663.

Gottesman, D., and Chuang, I. L. (2001). Quantum digital signatures. arXiv:quant-ph/0105032.

Hansen, A. (2025). Resource optimization strategies for quantum hardware utilization. Quantum Frontiers Journal, 2025(2), 10-18.

Hillery, M. et al. (1999). Quantum secret sharing. Physical Review A, 59(3), 1829.

Ivanov, A., and Popescu, N. (2025). Quantum error mitigation techniques. Quantum Frontiers Journal, 2025(2), 1-9.

Lindberg, E., and Silva, A. (2025). Compiler design for quantum programming languages. Quantum Frontiers Journal, 2025(2), 19-27.

Lo, H. K. et al. (2005). Decoy state QKD. Physical Review Letters, 94(23), 230504.

Lo, H. K. et al. (2012). Measurement-device-independent QKD. Physical Review Letters, 108(13), 130503.

Lucamarini, M. et al. (2018). Twin-field QKD. Nature, 557(7705), 400-403.

NIST (2024). FIPS 203-205: Post-quantum cryptography standards. nist.gov.

Nowak, A., and Popescu, I. (2025). Architectural design of scalable quantum computing systems. Quantum Frontiers Journal, 2025(1), 36-44.

Pironio, S. et al. (2009). Device-independent QKD. New Journal of Physics, 11(4), 045021.

Renner, R. (2005). Security of QKD. ETH Zurich PhD thesis. arXiv:quant-ph/0512258.

Shor, P. W. (1994). Algorithms for quantum computation. FOCS 1994, 124-134.

Gisin, N. et al. (2002). Quantum cryptography. Reviews of Modern Physics, 74(1), 145-195.

Nielsen, M. A., and Chuang, I. L. (2010). Quantum Computation and Quantum Information. Cambridge.

Silva, D. et al. (2024). Scalable quantum algorithm design for NISQ devices. Quantum Frontiers Journal, 2024(1), 38-45.

Declarations

Funding

This research was supported by the Spanish State Research Agency (AEI) under grants PID2024-178483OB-I00 and PID2024-178484OB-I00. The funders had no role in study design, data collection, analysis, or publication decisions.

Conflict of Interest

The authors declare no competing financial interests. They hold no financial interest in ID Quantique, Toshiba, or any quantum cryptography vendor.

Data Availability Statement

QCPDA framework, protocol comparison data, key rate scripts, and deployment guide are available at qcpda-quantum.org under CC BY 4.0.

Ethical Approval

This study is a theoretical evaluation of published cryptographic protocols. No human subjects, animal experiments, or patient data were involved. Ethical approval was not required.

ISSN: e-ISSN: 3117-6089 / p-ISSN: 3117-6070 Vol: 2025, Issues: 2, 2025

Appendix A

Key Rate Calculations and Security Proof References

The following provides key rate calculation methodology and security proof references.

Key Rate Models

Security Proof References