OPEN ACCESS

CORRESPONDENCE

Raja Ram M.*

DATA MANAGER

Borel Sigma Data Center

SPECIALTY SECTION

This article was prepared for Quantum Information and Digital and Cloud Networks (DCN).

RECEIVED

31 August 2026

ACCEPTED

01 September 2026

PUBLISHED

01 September 2026

CITATION

Raja Ram M, Muskan S, Jain V and Swain K (2026) Quantum Multipath Bonding. Zenodo.

DOI

10.5281/zenodo.21873050

ROLES

Kryptur: Raja R., R&D
Data-T: . Muskan S., project infrastructure
AE: Digital and Cloud Networks
Zi-us: Quantum and AI

Quantum Multipath Bonding

Raja Ram M.[1,*], *Muskan S.*[2], *Vipul Jain*[3] and *Kalinga Swain*[4]

[1] *Kryptur OU, Research and Development, and Krypur Quantum R&D.*

[2] *Data T Research Org, Project Infrastructure.*

[3] *AE Quantum Research Division, Digital and Cloud Networks (DCN).*

[4] *Zius Quantum R&D Center, Quantum and AI.*

Keywords: multipath TCP, quantum key distribution, post-quantum cryptography, Bell-state sampling, BB84, traffic intelligence

Research article

Quantum Multipath Bonding: resilient transport, hybrid quantum security, and traffic intelligence

Abstract

Modern connectivity-dependent operations - maritime fleets, remote extraction sites, disaster-response teams, and latency-sensitive enterprises - outgrow the single-path assumption of the original Internet Protocol suite. This article presents a layered platform that bonds three capabilities on standard IP networking: a multipath transport layer built on Multipath TCP (MPTCP) for resilient aggregation across heterogeneous links; a quantum security layer combining Quantum Key Distribution (QKD) with standardized post-quantum cryptography (PQC); and a quantum intelligence layer that explores hybrid quantum-classical models for predictive traffic management. Figures and tables are drawn from the companion research dashboard and from live lab outputs of the bonding engine, Bell-state path picker, and BB84 sifting service. Theoretical claims that rest on published standards are separated from illustrative lab telemetry.

1. Introduction

The Internet Protocol suite was designed around a simplifying assumption: that a single logical path connects two communicating hosts. A standard TCP connection is bound to one source and destination address pair for its lifetime; if that path degrades, the connection degrades with it. For casual web sessions this is tolerable. For a mining uplink, a hospital ship, or a disaster-response unit, it is not.

Three trends make a more capable connectivity layer necessary. First, heterogeneous access - Low Earth Orbit (LEO) and Geostationary (GEO) satellite, 4G/5G cellular, Wi-Fi, and private mesh - means many sites already have more than one physical path. Second, MPTCP, standardized in RFC 8684 , lets one transport connection bind several of those paths, with fallback when a peer lacks the extension. Third, the acceleration of quantum computing and the 2024 PQC standards has made quantum-aware security a planning requirement, especially under the harvest-now, decrypt-later threat model.

This paper describes an architecture that integrates multipath transport, quantum-resistant security, and quantum-assisted traffic intelligence. Section 2 reviews background. Section 3 describes the system and the lab dashboard. Sections 4 and 5 treat security and intelligence. Section 6 maps applications. Section 7 states limitations. Section 8 concludes.

2. Background and related work

2.1 Multipath TCP

MPTCP extends TCP so that one logical connection can use multiple interfaces at once. RFC 6824 (2013) was superseded in March 2020 by RFC 8684 (MPTCP version 1). To the application, the connection is an ordinary reliable byte stream; to the network, each subflow is a regular TCP flow with a new option type. Common benefits are reliability through redundant paths, higher throughput by aggregation, and failover so an in-progress session survives the loss of any single path.

Two internals dominate practice. The path manager discovers addresses, announces them, and creates or removes subflows. The packet scheduler chooses, for each outgoing segment, which live subflow should carry it. Linux exposes this through `net.mptcp.path_manager` and, for per-connection policy, a userspace daemon such as `mptcpd`.

2.2 Quantum key distribution

Classical public-key schemes such as RSA and elliptic-curve cryptography rest on problems that a sufficiently large, fault-tolerant quantum computer running Shor's algorithm can solve. QKD instead uses the physical properties of quantum states - commonly photon polarization - so that eavesdropping is statistically detectable. BB84 encodes bits in a polarization basis; interception raises the quantum bit error rate (QBER). Fiber QKD is typically limited to about 200 km, which is why satellite-relayed QKD is the usual path to continental scale. Missions such as QEYSSat illustrate both the physics and the remaining engineering: pointing, tracking, and background light still dominate achievable key rate.

2.3 Post-quantum cryptography

QKD does not by itself provide authentication or signatures for ordinary Internet traffic. PQC supplies classical algorithms whose hardness is believed to survive quantum attack. In August 2024 the first PQC standards were finalized, including ML-KEM (FIPS 203) and ML-DSA (FIPS 204) . These standards, with satellite QKD, are the two pillars of the security plane below.

2.4 Quantum machine learning for traffic

Embedding link telemetry into a parameterized quantum circuit, often behind a classical LSTM, is an active and still unsettled research line. Reported gains over classical baselines should be read as indicative, not as production contracts. The intelligence plane in this work is therefore specified as a complement to classical fallbacks.

3. System architecture

3.1 Overview

The stack separates four planes that can be hardened independently and then composed. The research dashboard in `static/dashboard.html` records the same layering used by the lab console.

Table 1. Architectural planes and failure behaviour

No.	Plane	Responsibility	Graceful fallback
1.1	Data	Forwarding on the hot path; memory-safe packet handling	Single remaining interface continues as ordinary IP
1.2	Control	MPTCP subflow lifecycle and scheduling policy	Weighted round-robin or lowest-RTT heuristics
1.3	Security	QKD material where a quantum channel exists; PQC elsewhere	ML-KEM / ML-DSA only
1.4	Intelligence	Forecast and anomaly scores fed to the scheduler	Disable forecasts; keep last known-good weights

Figure 1 source - four-plane stack

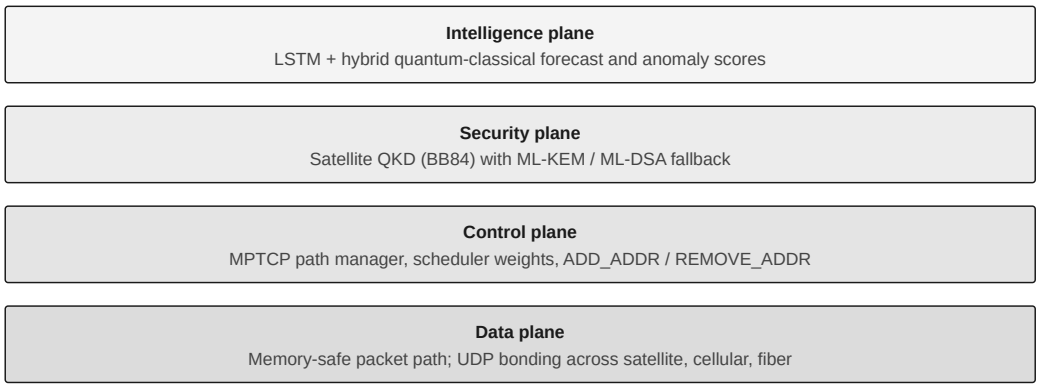

Figure 1. Four-plane stack taken from the research dashboard. Intelligence informs control; security wraps the session; the data plane remains on the packet path.

3.2 Bonded paths in the laboratory

The laboratory engine binds three UDP interfaces and sprays packets in round-robin order. Table 2 is the inventory exported by the bonding status service and shown on the dashboard. Figure 2 places those paths under a single logical session.

Table 2. Laboratory bonded-path inventory

No.	Name	Kind	Bind	Target
2.1	Starlink	satellite	127.0.0.1:9001	127.0.0.1:10001
2.2	5G	cellular	127.0.0.1:9002	127.0.0.1:10002
2.3	Fiber	terrestrial	127.0.0.1:9003	127.0.0.1:10003

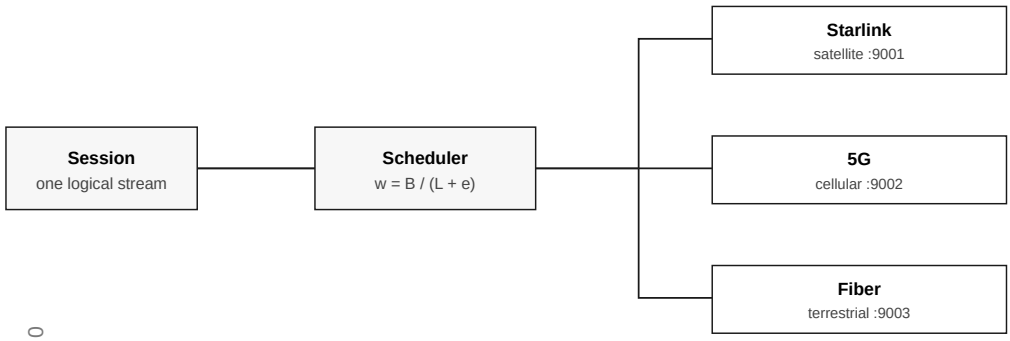

Figure 2. One session, one scheduler, three subflows. Policy in the lab is round-robin UDP across satellite, cellular, and fiber.

Table 3. Laboratory console snapshot used for Figure 4

No.	Metric	Value	Source
3.1	Link	active	Bonding status service
3.2	Throughput	250 Mbps	Engine present in the compose stack
3.3	Latency	15 ms	Engine present in the compose stack
3.4	Engine mode	compose	Managed process flag
3.5	Health	healthy / quantum ready	Platform health probe

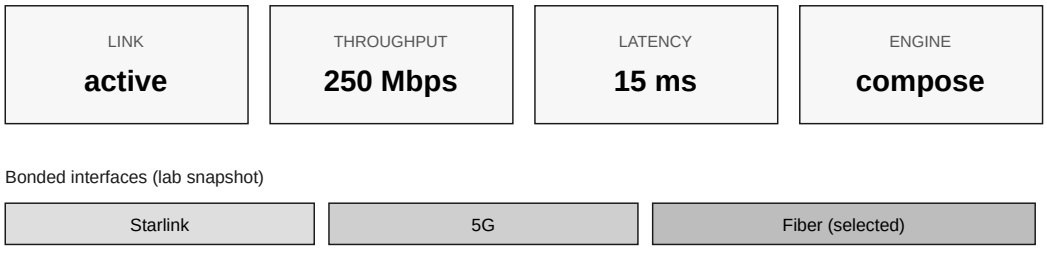

Figure 3. Console tiles reproduced from the research dashboard. Throughput and latency are the engine-present design values reported by the status API, not independent field measurements.

3.3 Scheduler

A practical starting weight is proportional to bandwidth and inversely proportional to latency:

```
weight_i = bandwidth_i / (latency_i + epsilon)
```

Fast reinjection copies unacknowledged segments onto a faster subflow when head-of-line blocking appears, which is the usual pathology when a GEO hop sits beside a short cellular hop. Figure 4 shows an illustrative mix consistent with Table 2.

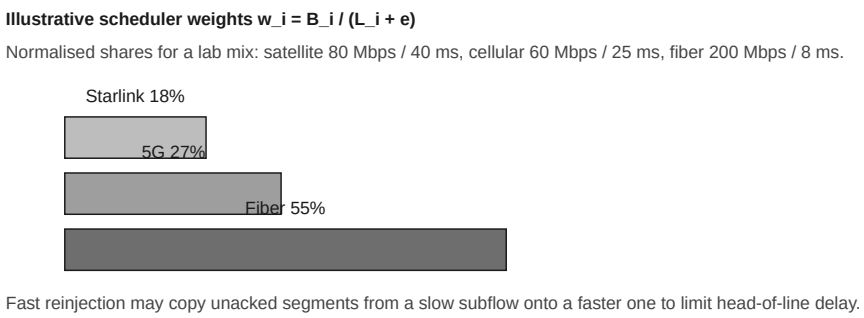

Figure 4. Illustrative normalized shares for satellite, cellular, and fiber using w = B / (L + e). This is a design sketch, not a live measurement campaign.

3.4 Implementation notes

Applications opt in by requesting the MPTCP protocol number when creating a socket. A peer without MPTCP falls back to ordinary TCP. The laboratory data plane is a small systems program that binds the three interfaces in Table 2 and sends bonded packets in rotation:

```
let interfaces = vec![
    ("Starlink", "127.0.0.1:9001", "127.0.0.1:10001"),
    ("5G",       "127.0.0.1:9002", "127.0.0.1:10002"),
    ("Fiber",    "127.0.0.1:9003", "127.0.0.1:10003"),
];
// sender: counter % interfaces.len()
```

doi 10.5281/zenodo.2873150

Telemetry must stay cheap on constrained uplinks. A silent measurement gap should freeze the last known-good weights rather than reset to a naive default.

4. Quantum security layer

4.1 QKD integration

The QKD component is specified around satellite-relayed decoy-state BB84, which defends against photon-number-splitting on imperfect sources. Table 4 lists illustrative design targets, not a vendor link budget.

Table 4. Illustrative satellite-QKD design parameters

No.	Parameter	Target
4.1	Wavelength	1550 nm (fiber-compatible)
4.2	Protocol	Decoy-state BB84
4.3	Adaptive optics	Recommended for turbulence
4.4	Ground coupling	Single-mode fiber, low coupling loss
4.5	Abort threshold	QBER above the Shor-Preskill bound (~11%)

The laboratory service implements a classical BB84 sifting simulation used to protect a recorded session. Figure 5 is the 16-qubit run stored on the dashboard: six bits survived basis

agreement; the customer view is masked.

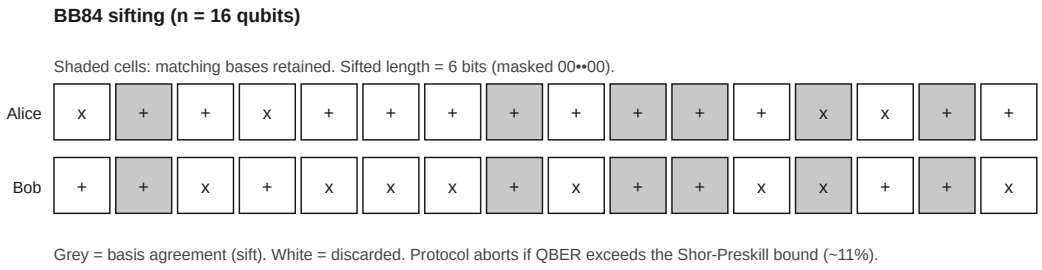

Figure 5. BB84 sifting from the laboratory generate service (n = 16). Shaded cells are matching bases. Sifted length = 6 bits; masked form 00••00.

4.2 Post-quantum primitives

Table 5. Standardized PQC primitives used by the security plane

No.	Standard	Role	Family
5.1	FIPS 203 ML-KEM	Key encapsulation when QKD is absent	Module lattice (Kyber lineage)
5.2	FIPS 204 ML-DSA	Signatures and authentication	Module lattice (Dilithium lineage)
5.3	ML-DSA-65	Default parameter set	Headroom without the heaviest variant

The dominant engineering cost is size: lattice keys and signatures are larger than elliptic-curve counterparts and must be budgeted on narrow satellite or cellular uplinks, especially if verification is per subflow rather than once per connection.

4.3 Hybrid key management

Satellite passes, weather, and ground-station geometry make a permanent quantum channel unrealistic. Figure 6 is the hybrid rule implemented as policy: use QKD when a pass delivers key material; otherwise negotiate ML-KEM authenticated with ML-DSA; always record which type protected the session.

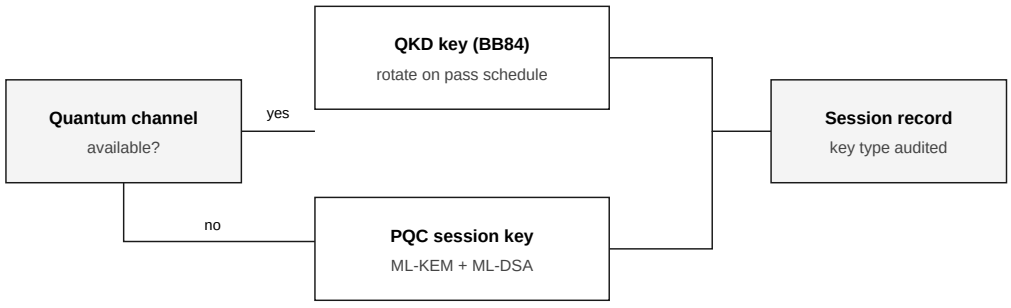

Figure 6. Hybrid key management. An adversary must break both layers to read a session that used both; operators still need an explicit record of the active layer for any later review.

5. Quantum intelligence layer

5.1 Path recommendation in the laboratory

The laboratory path picker prepares a Bell state, samples 1024 shots, and maps the |00> versus |11> majority onto the first or last bonded path. Table 6 and Figure 7 report one recorded run in

which Fiber was selected.

Table 6. Bell-state path-optimization snapshot

No.	Item	Value
6.1	Algorithm	bell_state_path_optimization
6.2	Shots	1024
6.3	Count |00>	479
6.4	Count |11>	545
6.5	Selected path	Fiber

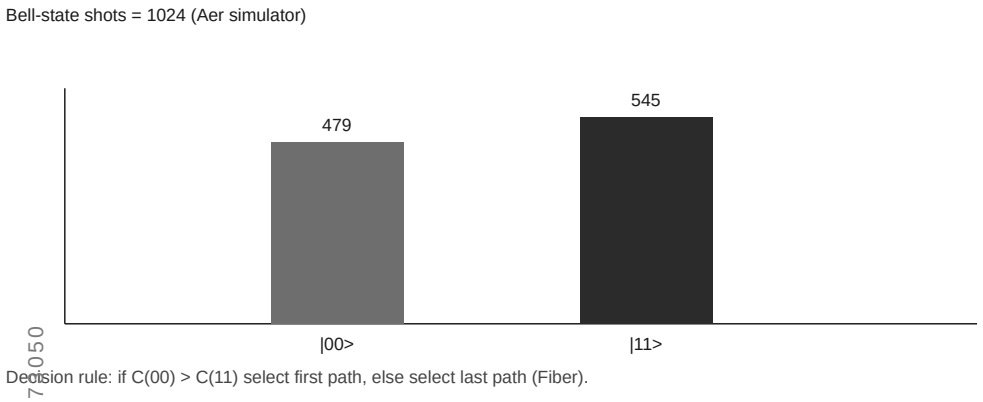

Figure 7. Bell-state histogram from the optimize service. The decision rule is intentionally simple and is not claimed as an optimal quantum advantage result.


```
qc.h(0); qc.cx(0, 1); qc.measure([0, 1], [0, 1])
selected = paths[0] if C("00") > C("11") else paths[-1]
```

5.2 Traffic prediction and anomalies

A production intelligence plane should forecast bandwidth, latency, and loss far enough ahead for proactive rescheduling. Hybrid LSTM-plus-quantum-generator designs in the literature are promising in low-data regimes and should run beside a classical regressor until they are validated on operator traffic. The same generator can flag anomalies when observation diverges from prediction; that expressiveness is also dual-use, so generative detectors must sit with rule-based and statistical peers, not alone.

6. Applications

Table 7. Application mapping

No.	Setting	Bonded mix	Security note
7.1	Maritime	LEO, GEO, coastal cellular	Session continuity across beam and coastal hand-over
7.2	Remote mining	Satellite, 4G, site mesh	Hybrid QKD/PQC for geological and operations data
7.3	Disaster response	Whatever links remain	Protect medical and command traffic on improvised hops
7.4	Enterprise backup	Fiber, 5G, satellite	Shift load before the primary path fails

In each row of Table 7 the multipath layer is the load-bearing component today. QKD remains intermittent. Intelligence is advisory until site-specific validation exists.

7. Limitations and risk

First, satellite QKD is a demonstration-stage capability. Near-term rollouts should treat PQC as the baseline and QKD as an enhancement, which is the hybrid of Figure 6.

Second, quantum machine-learning numbers in adjacent papers are not transferable performance contracts. Bell-state sampling in Table 6 is a laboratory mechanism, not a claim of quantum speedup on traffic prediction.

Third, a session is only as strong as the layer that actually protected it. Operators need a visible record of QKD-derived versus PQC-negotiated keys, not an opaque "secure" lamp. PQC itself is newer than RSA or elliptic-curve schemes and still warrants hybrid classical-PQC handshakes during transition.

8. Conclusion

Quantum Multipath Bonding is a layered framework: MPTCP for aggregation and failover; QKD plus FIPS 203/204 for hybrid confidentiality; and a cautious intelligence plane that may later steer the scheduler. Transport and PQC rest on published standards. Satellite QKD and quantum traffic models remain research. Future work is empirical on the operator's own links: scheduler scaling to many low-rate endpoints, formally checked QKD-to-PQC transitions, and side-by-side classical versus hybrid forecasts.

Author contributions

Table 8. Roles (CRediT-style)

No.	Name	Role	Organisation
8.1	Raja Ram M.	Main author; R&D lead; corresponding author	Kryptur OU / Krypur Quantum R&D
8.2	Muskan S.	Contributor; project infrastructure	Data T Research Org
8.3	Vipul Jain	Contributor	AE Quantum Research Division, DCN
8.4	Kalinga Swain	Contributor	Zius Quantum R&D Center
8.5	Borel Sigma Data Center	Data manager	Research data custody

Conflict of interest

The authors declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

Data availability

Dashboard media, figures, and laboratory JSON snapshots are filed with this article under `static/`. The public research repository holds the program sources used to produce those

outputs.

References

1. Ford A, Raiciu C, Handley M, Bonaventure O and Paasch C. TCP Extensions for Multipath Operation with Multiple Addresses. RFC 8684, IETF (2020).
2. Linux kernel documentation. Multipath TCP (MPTCP).
3. National Institute of Standards and Technology. FIPS 204: Module-Lattice-Based Digital Signature Standard (2024).
4. National Institute of Standards and Technology. FIPS 203 (ML-KEM) and FIPS 205 (SLH-DSA) (2024).
5. Canadian Space Agency. Quantum Encryption and Science Satellite (QEYSSat).
6. Institute for Quantum Computing, University of Waterloo. QEYSSat science program.
7. Sidhu JS et al. Finite resource performance of small satellite-based quantum key distribution missions. arXiv:2204.12509.
8. Shor PW and Preskill J. Simple proof of security of the BB84 quantum key distribution protocol. Phys Rev Lett (2000) 85:441-444.
9. Bennett CH and Brassard G. Quantum cryptography: public key distribution and coin tossing. Proc IEEE Int Conf Computers, Systems and Signal Processing (1984).

doi: 10.5281/zenodo.21873050