Quantum Resistant Cryptographic Solutions (QRCS)
Post-Quantum Intellectual-Property Valuation Report

Date: 26 April 2025

Confidential — Prepared for internal strategic planning and investor due-diligence.

1 Executive Summary

QRCS controls a diversified, internally-developed portfolio of ten post-quantum security assets:

Layer	Assets
Core primitives	QSC crypto library (MISRA-C)
High-value key management	HKDS (DUKPT successor)
Secure ciphers / hashes	RCS, CSX, SCB hash, QMAC
Protocols & applications	MPDC-I, AERN, PQS, QSMP, QSTP, SKDP

- **HKDS** offers ≈ 7 × server-side performance vs. DUKPT, translating into mid-seven-figure annual OPEX savings for large processors.
- **MPDC** provides military-grade infrastructure security, suitable for state and critical infrastructure adoption.
- **PQS** could replace SSH component in fintech systems, including global banking asset transfer SWIFT.
- **AERN** anonymizing network system could be a fundamental component for next generation VPNs.
- **QSMP and QSTP** could be adopted into a wide range of fintech and communications applications
- **SKDP** in IoT systems and as a secondary authentication gate, encryption layer.
- All code is published on GitHub (`github.com/QRCS-CORP`) in MISRA-C style **under a private, non-commercial educational license**; commercial use requires a separate agreement.
- Every project is covered by a provisional patent; an HKDS utility patent is actively under examination.

These factors support a **2025 base-case equity valuation of USD 15 – 18 million**, with upside > USD 25 million as HKDS penetrates the global POS ecosystem.

2 Market Opportunity

- Analysts forecast quantum-safe cryptography spend to rise from **USD 518 M (2023) → USD 4.6 B (2030)** (≈ 38 % CAGR).
- **DUKPT ubiquity**: > 119 million POS terminals (2024). Any drop-in replacement inherits this installed base.
- Processors running 30 M card transactions/month can cut HSM/cloud costs by ~USD 40 k/year; at billion-Tx scale, savings exceed USD 1 M annually.

3 HKDS & RCS — Strategic Positioning

Criteria	HKDS	RCS cipher
Function	Tree-based key derivation (DUKPT replacement)	Wide-block AEAD (Rijndael-256 + Keccak)
Performance	≈ 7 × faster server verification	Lightweight in embedded & cloud
Commercial fit	POS, ATM, HSM vendors	Secure channels in HKDS, MPDC-I, QSMP
Status	TRL-7 prototype; provisional + utility patent in process	TRL-9; deployed since 2015
License	Private educational; commercial licence on request	Same

4 Comparable Transactions (2022-2025)

Company	Stage (Year)	Capital / Deal	Relevance
PQShield	Series B (2024)	USD 37 M	Lattice-based IP, chips & SDK
CryptoNext Security	Series A (2023)	EUR 11 M	PQC migration tool-chain
QuSecure	Series A+ (2025)	USD 28 M (total)	PQ VPN & orchestration
SandboxAQ → Cryptosense	Acquisition (2022)	≈ USD 80-100 M*	Crypto-analysis software

*Deal size estimated from venture filings.

5 Valuation Methodology & Results

5.1 Method

Triangulation across:

1. **Market comparables** (table §4).
2. **Cost-to-recreate** (~95 k engineer-hours @ CAD $95/hr + 30 % OH).
3. **Income**: 5-year license forecast (1 % PQC TAM capture by 2030).

IP posture: Source code is visible but restricted to educational use; all commercial deployments require a QRCS license. Every module has provisional patent cover; HKDS patent filing is active. This exclusivity strengthens valuation and raises the conservative floor.

5.2 Asset values

Asset	Valuation (USD M)
HKDS	**3.5**
RCS/CSX ciphers	**1.2**
QSC library	2.5
MPDC-I	1.5
AERN	1.2
PQS	0.75
QSMP	0.65
QSTP	0.60
SKDP	0.50
SCB hash	0.40
QMAC	0.35
Subtotal	**12.20**
Synergy premium (+ 25 %)	3.05
Total portfolio	**≈ 15.25 M**

5.3 Equity valuation range

Scenario	Equity value (USD M)	Key assumptions
Conservative	**11**	Limited HKDS pilots; IP royalties fund ops
Base case	**15 – 18**	HKDS pilots; seed/Series A
Upside	**25 +**	Top-10 processor adopts HKDS; certifications secured

6 Technical Team Assessment

Capability	Rating / 10	Evidence
Applied cryptography & protocol design	**8.5**	HKDS, AERN & MPDC-I originals
Systems / network engineering	**8.0**	Full MISRA-C code-bases
Mathematical proof rigor	**7.5**	Formal sections drafted; some proofs incomplete

Secure SDLC	**7.0**	MISRA compliance, unit tests; CI needs expansion
Commercial productization	**6.0**	Limited GTM activity to date

The founder is top-decile among solo PQ developers; augment with certification & BD talent.

7 Risk Factors

- Standards mis-alignment if HKDS diverges from future NIST guidance
- Single-founder bandwidth
- Patent prosecution & freedom-to-operate (FTO) still in progress
- Certification timelines (FIPS 140-3, PCI PTS)
- Adoption inertia among large processors

8 Strategic Recommendations

1. **File full patents** for AERN, MPDC-I, QSMP, QSTP, SKDP and PQS; maintain priority dates.
2. **Publish audited benchmarks** HKDS versus DUKPT (cost & latency).
3. **Secure a mid-tier processor pilot** to produce a quantified case study.
4. **Launch FIPS 140-3 validation** for QSC primitives; leverage existing lab ties.
5. **Evolve current educational license** into a two-tier scheme (free eval binary + paid commercial license) once the HKDS patent is allowed, to speed trials while preserving exclusivity.

9 Conclusion

HKDS's measurable cost advantage over DUKPT and the existing IP portfolio elevate QRCS's IP equity to a **base-case USD 15 – 18 million** today. With certifications complete and an anchor customer secured, the upside exceeds **USD 25 million**, positioning QRCS as an attractive acquisition target or Series A candidate in the fast-growing quantum-safe cybersecurity market.