



QUANTUM INSIDER

powered by **RESONANCE**

Space-based Quantum Key Distribution (QKD)

Technology Trends, Competitive Landscape and Market Size

March 2025

Table of Contents

Section	Contents	Page Number
Introduction to Quantum Key Distribution (QKD)	<ul style="list-style-type: none"> • Introduction to Quantum Key Distribution • Quantum Key Distribution Process • Variants of Quantum Key Distribution • Alternatives to Quantum Key Distribution 	7-11
Introduction to Space-based Quantum Key Distribution	<ul style="list-style-type: none"> • Introduction to Space-based Quantum Key Distribution • Technology Trends in Space-based QKD • Space-based QKD System • Space-based QKD Impact on Industry Sectors • Space-based / Terrestrial QKD Comparison 	12-17
Competitive Landscape Quantum Key Distribution Major Industry Players	<ul style="list-style-type: none"> • Major Industry Players (NA) • Major Industry Players (APAC) • Major Industry Players (EMEA) 	18-28
Market Sizing Model Space-based Quantum Key Distribution	<ul style="list-style-type: none"> • Market Growth Drivers • Market Challenges • Space-based QKD Market Size • QKD End-User Market Size 	29-35
Market Size Market Opportunity and Social Impact	<ul style="list-style-type: none"> • Space-based QKD Market Opportunity • QKD End-User Market Opportunity • Total Market Opportunity • Social Impact 	36-41
About Us	<ul style="list-style-type: none"> • About Us • Client Examples • Space Insider Core Team • Resonance Advisory Board 	42-46

Space-based QKD System

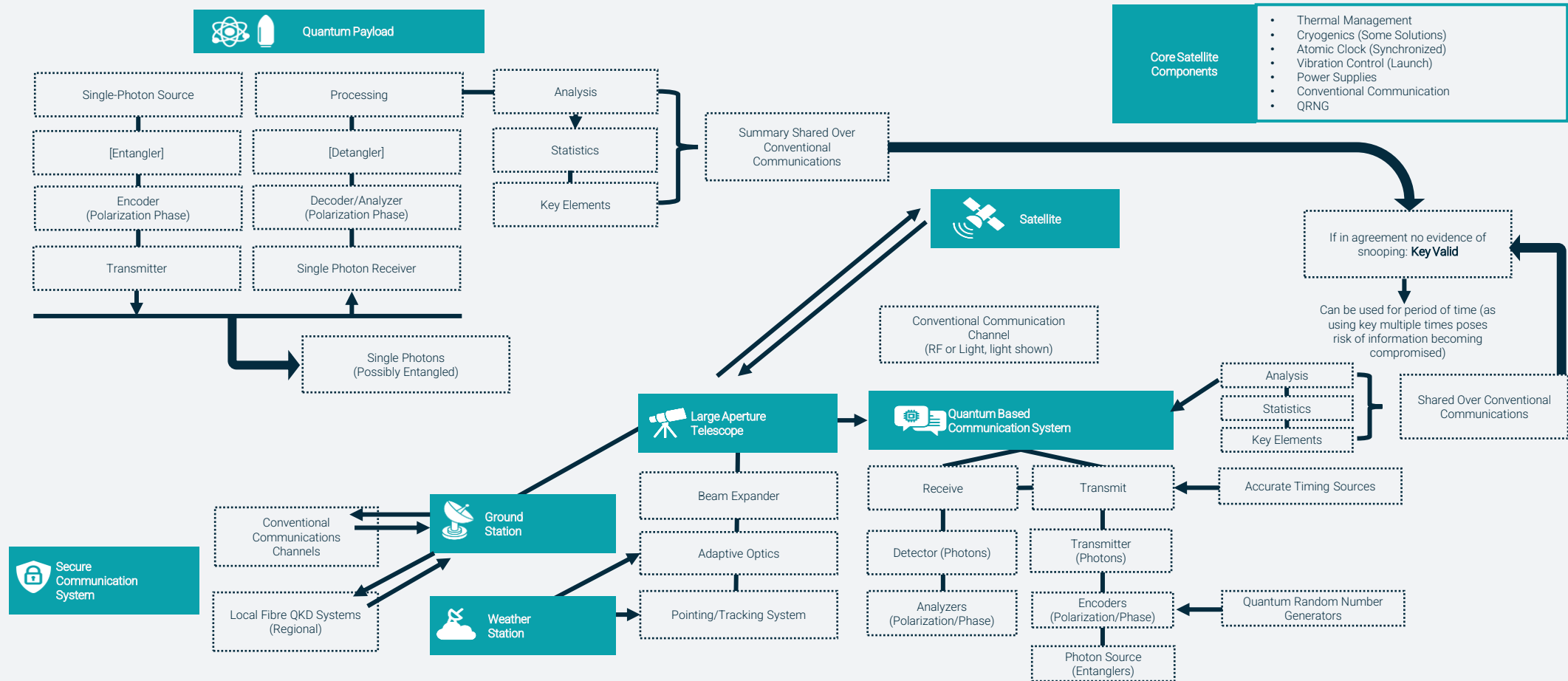


Figure 3. Space-based QKD System

Alternatives to Quantum Key Distribution

QKD ensures secure communications by exploiting quantum mechanics. However, these come at the cost of requiring dedicated communications quantum channels for key distribution by photons, with practical limitations in range requiring the complexities of space-based systems for global reach. Alternative solutions designed to resist quantum computing threats are being developed. These offer more accessible, if probably less secure, options that are more easily integrated into existing communication links. There is a market for both approaches, but QKD appears to offer the highest security options, including detection of snooping (unique), and is being pursued actively.

Lattice-based Cryptography

This is based on the 'hardness' of certain mathematical problems, such as the Shortest Vector Problem (SVP) and the Learning With Errors (LWE) problem. Such schemes are efficient and offer support for encryption, digital signatures and key distribution, but often involve large key sizes compared to classical cryptography.

In mid-2024, the National Institute of Standards and Technology (NIST) issued three finalized standards (TRL9):

- Kyber key encapsulation method (KEM) (for public-key encryption) based on SVP
- Dilithium digital signature algorithm for authenticity verification using SVP
- FrodoKEM as a secondary KEM standard using LWE

Code-based Cryptography

This approach relies on the difficulty of decoding random linear codes, such as the McEliece system, and is at TRL6-7. It is well researched and has a strong theoretical foundation, but key size remains an issue for widespread adoption. It was not selected by NIST, but remains an important option as new, more efficient options emerge (e.g. Niederreiter).

Hash-based Cryptography

This uses hash functions to build secure digital signature solutions. These functions are efficient and are considered quantum-resistant in their area of application. Large signature sizes and state management (some cases) remain as challenges for large-scale deployment. Status varies from TRL6 to TRL9 for the different systems.

- XMSS has been standardized and is in limited use
- SPHINCS+ exploits a Merkle tree structure and other techniques but suffers from large signature size
- LMS is similar to XMSS, but lighter weight

Isogeny-based Cryptography

Based on the finding of isogenies (mathematical mappings) between elliptic curves. These are attractive in constrained environments such as embedded systems or IoT, as they offer small key sizes and may have low resource consumption, though slow. Status is TRL6-7 (optimistic), with significant remaining challenges.

Examples include:

- SIDH (Supersingular Isogeny Diffie-Hellman) based on the traditional Diffie-Hellman key exchange
- SIKE (Supersingular Isogeny Key Encapsulation) is similar but targets the encapsulation of a shared secret.

Symmetric Cryptography with Larger Keys

Quantum computers are not expected to offer efficient attacks against symmetric cryptographic systems such as AES, so a short-term option is to use longer keys. An example would be AES with key sizes of 256 bits or greater. This requires greater computational resources, but it is still an efficient approach compared with the other quantum-safe options.

Quantum-safe Hybrid Cryptography













A combination of classical and quantum-safe algorithms aimed at providing an additional layer of security in the current transition period. These offer quantum resistance but maintain compatibility with existing systems if at the cost of speed and computational resource. Examples include RSA+Kyber, or ECC+Lattice.

Summary:

None of the Post-Quantum Cryptography (PQC) options described offer the intruder or snooping detection inherent in quantum-based solutions, such as QKD. This is a unique differentiator of QKD, and is of significant importance in several of the proposed applications.

Major Industry Players (NA, 1)

The space-based QKD market is limited in terms of the competitive landscape, as the market is still in the nascent phase (TRL7 achieved by China) and the technology is still in the development/demonstration phase. As the ground-based QKD market has greater levels of activity, and companies typically work across the space and terrestrial element – major industry player profiles are captured. An indication is provided of their involvement in space-based QKD technologies.

Company	Year Founded	HQ	Company Profile	QKD Technology	Funding	Space-based QKD	Legend
 Infleqtion	2007		Infleqtion's brand, ColdQuanta, specializes in cold atom quantum technology for next-gen space sensors and timing systems. It has deployed its Quantum Core™ on the ISS for NASA's Cold Atom Lab and participates in the DOE's Quantum & Space Collaboration to advance quantum sensing, computing, and communication in space.	<ul style="list-style-type: none"> Cold atom quantum technology Quantum Computing for Space Applications 	<ul style="list-style-type: none"> Total Raised: \$381M Lead Investors: U.S. Department of Defense, Advanced Strategic Capabilities Accelerator, BOKA Group Holdings 	✓	
 QUANTUMXCHANGE™	2018		QuantumXC is a pioneering company in the field of quantum-secure communications, specializing in QKD technology and quantum-safe encryption solutions..	<ul style="list-style-type: none"> Phio TX platform for QKD over fibre optic links Quantum safe encryption 	<ul style="list-style-type: none"> Total Raised: \$23.5M Lead Investor: New Technology Ventures 	✗	No direct involvement in space-based QKD ✗
 quantum eMotion	2017		Quantum eMotion, established in 2007 and headquartered in Canada, specializes in quantum-safe cybersecurity solution, with the focus on quantum random number generators (QRNG).	<ul style="list-style-type: none"> QRNGs (high-throughput version and algorithms) 	<ul style="list-style-type: none"> Total Raised: \$8.5M 	✗	Potential involvement / usability in space-based QKD ↔
 ANTARIS SOFTWARE FOR SPACE™	2021		Antaris, provides software platform for space to simplify the design, simulation and operation of satellites. In partnership with SpeQtral, Antaris is working to create, deliver, and deploy quantum-safe key distribution satellites for government and commercial operators.	<ul style="list-style-type: none"> QKD Satellite Software 	<ul style="list-style-type: none"> Total Raised: \$7.7M Lead Investors: Streamlined Ventures, Acequia Capital (AceCap), Possible Ventures 	✓	
 evolutionQ	2015		evolutionQ is a Canadian company focused on quantum-safe cybersecurity solutions. The company has been awarded funding by the Canadian Space Agency for space-based QKD network R&D to advance satellite-based secure quantum communication services and tools.	<ul style="list-style-type: none"> Quantum-Safe QKD Deployment: QKD Network Simulation 	<ul style="list-style-type: none"> Total Raised: \$5.5M Lead Investor: Quantonation 	✓	Directly involved in space-based QKD ✓
 ADVA™	2017		ADVA, now part of Adtran Networks SE, is a European telecommunications vendor with a strong focus on quantum-safe technologies. Since 2014, the company has been at the forefront of research and development in QKD and Post-Quantum Cryptography.	<ul style="list-style-type: none"> QKD-enabled optical transport Post-quantum cryptography (PQC) 	<ul style="list-style-type: none"> Total Raised: \$3M Lead Investors: Juniper Networks, Egora Holding 	✗	

Total Market Opportunity

Total Cumulative Revenue Estimates (2025 to 2030)

QKD End-User Market Opportunity

\$1.9B in revenue QKD end-user market opportunity	
Government and Diplomacy	\$1.1B
Finance and Banking	\$0.4B
Defence and National Security	\$0.2B
Energy & Critical Infrastructure	\$0.1B
Telecommunications	\$0.1B
Other	\$0.0B

Commercial space-based QKD end-user market opportunity likely to remain limited until post 2035 (operational and commercialization).

Space-based QKD (Infrastructure and Development) Vendor Market Size

\$4.9B in revenue (conservative / optimistic scenario) Value appropriated by space-based QKD infrastructure and development vendors			
Space-based QKD – Infrastructure Development and Implementation Vendor Types	Space-based QKD Model Legend	Conservative	Optimistic
	QKD Satellite Vendors	\$1.1B	\$1.1B
	Ground Station Upgrades	\$1.1B	\$1.1B
	Quantum Interface	\$1.1B	\$1.1B
	Existing Infrastructure Terminal Integration	\$0.6B	\$0.6B

This is a preview of the full report that is available on our platform

If you would like access to the full report or explore our platform, please contact us on hello@resonance.holdings