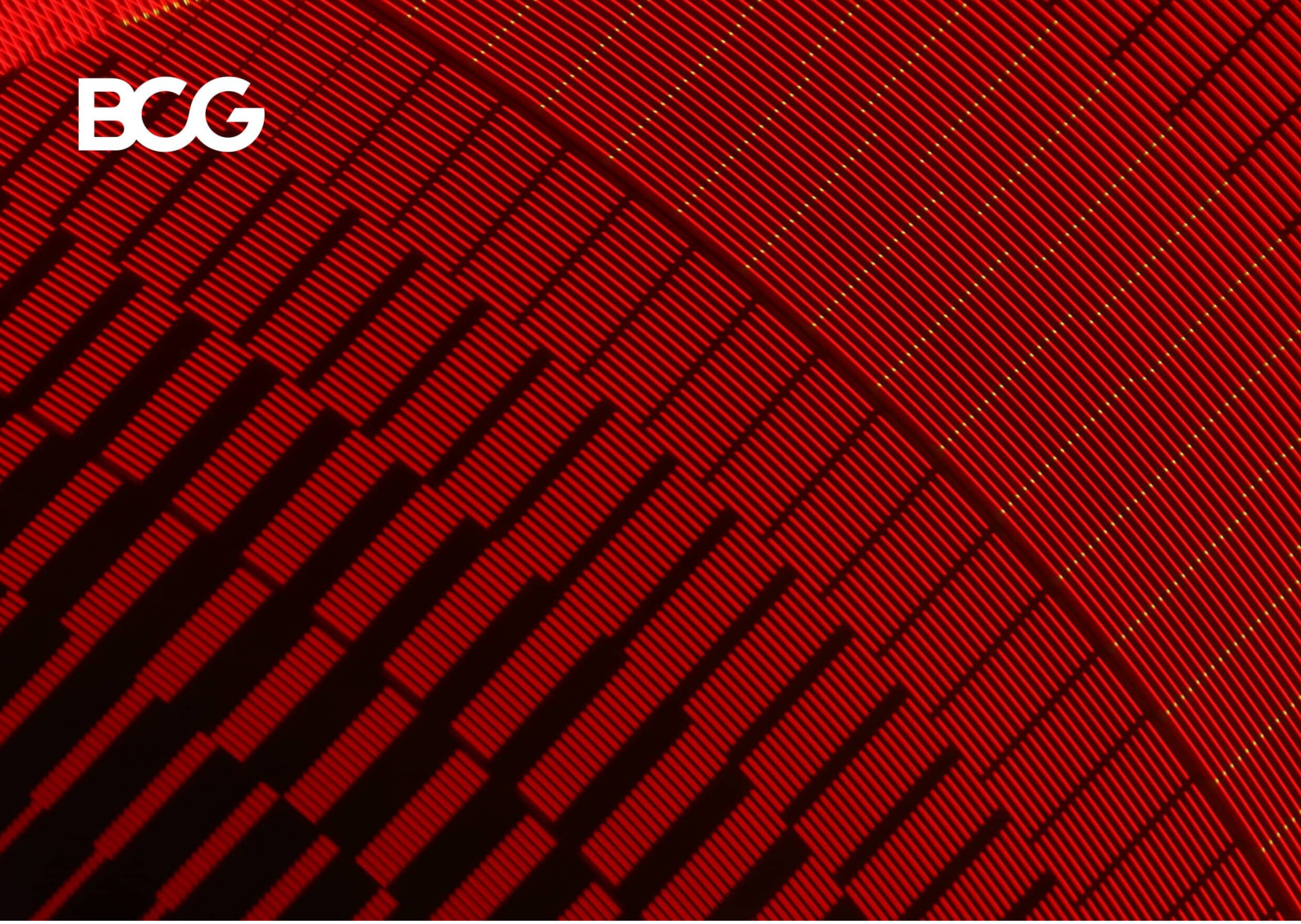


Are You Ready for Quantum Communications?

MARCH 22, 2023

By Jean-François Bobier, Cassia Naudet-Baulieu, Matt Langione, Brett Thorson, Jaroslav Šnajdr, and Stefan Deutscher

READING TIME: 12 MIN

In August 2022, US President Joe Biden signed into law the $280 billion CHIPS and Science Act, which dedicates around $500 million for the development of quantum networks along with additional funding for quantum research. It was yet another signal that the world's leading economies see quantum communications, which leverage quantum physics to enhance security, as a strategic imperative.

Government funding for quantum communications has surged in recent years. Among China's massive commitments to quantum technologies—including the formation of a $10 billion national quantum

laboratory and the launch, in 2016, of the first quantum satellite—is a 2,900-mile quantum network that combines over 700 optical fibers with two satellite-to-ground links. Europe's Quantum Flagship initiative, worth more than $1 billion, was launched in 2018 with a ten-year timeline; 25% of the overall budget is set aside for quantum communications.

The need for these technologies is clear—and urgent. Between smartphones, tablets, PCs, wearables, connected cars, smart homes, and industrial internet sensors, the installed base of connected devices will reach about 30 billion by 2030, according to Statista. The result will be a deluge of data: according to IDC, global data creation and replication will jump from 64 zettabytes in 2020 to 181 zettabytes by 2025 alone.

All that data will need to be secured. Meanwhile, current public encryption protocols risk being breakable in less than a decade.

Current public encryption protocols could be breakable in less than a decade.

Fortunately, the overhaul of communication security technologies is already underway, with the combined market for classical and quantum communications estimated to reach $10 billion by 2030. To capitalize on this burgeoning market, investors should understand the many functions and use cases of quantum communications—and the factors that will drive adoption of these technologies across the global economy.

Shifting Threats, New Responses

Since Shor's algorithm emerged in 1994, we've known that two main public encryption protocols—RSA and Diffie-Hellman—would eventually be broken by powerful quantum computers. Three decades later, that moment of reckoning is approaching fast. Dr. Michele Mosca from the University of Waterloo predicts quantum computers will have a 50% probability of breaking highly secure RSA-2048 keys by 2031.

Two major approaches, one classical and the other rooted in quantum technologies, have emerged in response.

Post-Quantum Cryptography, or PQC, is made up of cryptographic protocols that are secure against both quantum and classical computers. Currently being developed by the US National Institute of Standards and Technology (NIST) as well as agencies in China, PQC uses novel mathematical problems that are resistant to quantum attacks. The protocols are designed to run on classical computers and existing networks and can often be applied as a software update. (In some cases, bandwidth or central-processing-unit power might be insufficient, requiring a hardware upgrade as well.)

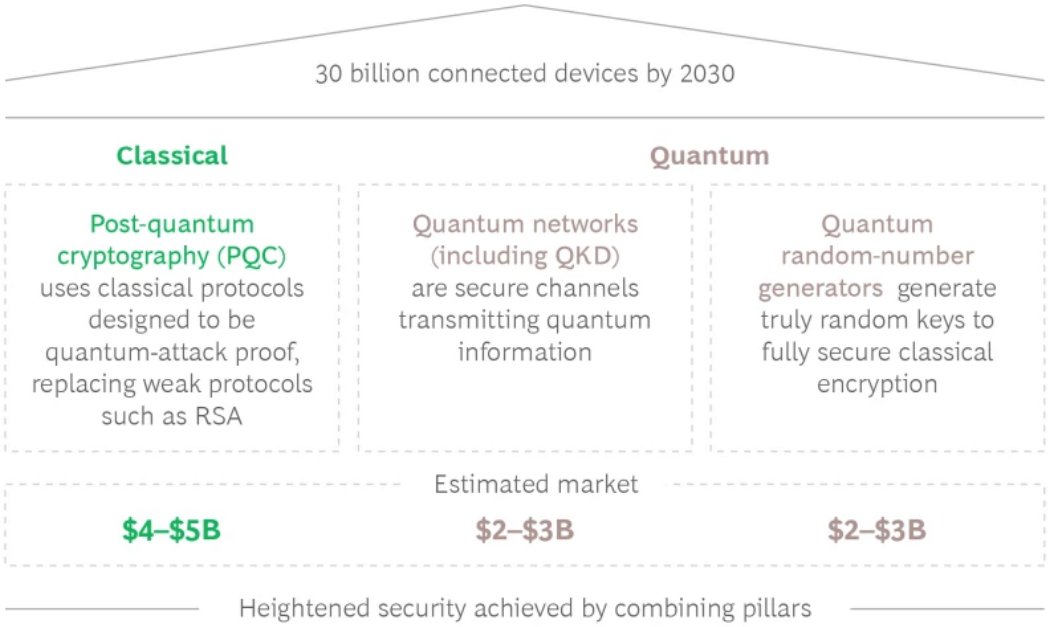
RSA was thought to be unbreakable—until it wasn't. Similarly, PQC protocol designers can't guarantee a clever mathematician won't eventually find a weakness by combining classical and quantum computers. Because of this looming threat, PQC should be implemented with cryptoagility—the capability to quickly switch protocols and certificates—if a new attack is discovered.

Quantum Communications, meanwhile, use quantum technologies to secure communications. There are two pillars to this approach:

- **Quantum networks,** including quantum key distribution (QKD), are communication channels in which any attack by an eavesdropper can be detected. Information is protected by quantum mechanics; because quantum states collapse when measured, attackers trying to eavesdrop the communication will leave a telltale sign. Quantum networks leverage this property to secure the communication channel itself; QKD uses such a channel to transmit a private key, securing a subsequent classical communication.
- **Quantum random number generators,** or QRNGs, are chips able to produce true random numbers—which attackers cannot guess—to generate highly secured keys in classical data encryption and decryption protocols.

While some observers advocate for one method over the other, the highest level of network security relies on a combination of classical and quantum approaches. (See Exhibit 1.)

Exhibit 1 - Three Pillars for Securing Future Communications



Sources: Inside Quantum Technology; Statista; BCG analysis.

Note: PQC figures include implementation costs. RSA = Rivest–Shamir–Adleman cryptosystem; QKD = quantum key distribution.

The Market for Quantum Communications

While classical protocols involving postquantum cryptography will remain an important pillar in securing future communications, the real growth potential lies in quantum communications. Let's examine the two technologies involved—and some potential applications—more closely.

Quantum Networks, Including QKD

Quantum networks are also referred to as a quantum internet. While the technology is still in the early stages, two uses stand out:

Transmitting Data Securely. Most communications are secured via public keys, also called asymmetric encryption. First, the sender generates and sends a public key based on a private key; then the receiver encrypts the message using the public key; finally, the sender decrypts the message using the private key.

In this approach, the attacker can always try to guess the private key based on the public key. In the case of RSA, the private key is hidden in the prime factors of the public key—which a future quantum computer will be able to factor using Shor's algorithm.

Exhibit 2 - Symmetric Encryption Resists Quantum Computer Attacks

Current cryptographic standards	Type	Purpose	Impact from large scale quantum computer
AES	Symmetric	Encryption	Larger key sizes needed (128→256 bits)
SHA-3	Hash function	Hashing	Larger output needed (128→284 bits)
RSA	Asymmetric	Signatures, key establishment	No longer secure
ECDSA, ECDH (elliptic curve cryptography)	Asymmetric	Signatures, key exchanges	No longer secure
DSA (finite field cryptography)	Asymmetric	Signatures, key exchanges	No longer secure

Sources: US Department of Commerce; NIST.

Note: AES = advanced encryption standard; SHA-3 = secure hash algorithm 3; RSA = Rivest–Shamir–Adleman cryptosystem; ECDSA = Elliptic Curve Digital Signature Algorithm; ECDH = Elliptic-curve Diffie–Hellman; DSA = Digital Signature Algorithm.

QKD uses a symmetrical approach, where a shared private key is transmitted securely using the quantum communication channel. The message is then encrypted and transmitted on a classical and insecure channel. An attacker would need to guess the private key from the encrypted message itself, which is considered impossible with sufficiently large keys and cryptography protocols such as advanced encryption standard. QKD works around the limitations of current networks (including limited bandwidth and noise) by securely transmitting only a small key, which is a number encoded in 256 bits or more. (See Exhibit 2.)

Interconnecting Quantum Computers. Quantum computers manipulate quantum states that can be carried over quantum-communications infrastructure without costly classical transcription. Quantum computers will eventually be networked together the same way the internet provided a network for classical computers; in the near term, quantum-networking technology will help quantum computers scale by interconnecting them inside a computer (also known as “QPU interconnect”) and in data-center racks. IBM plans to leverage quantum communications in their computers as early as 2026, according to the roadmap the company published in 2020.

Two forms of transmission can be used:

- **Fiber-based,** though limited today by distance (around 200 kilometers), is more reliable. The first commercial trials have been conducted by SK Telecom and ID Quantique in Seoul and BT and Toshiba in London.
- **Free-space transmission,** which includes satellites, can be used for long-distance transmission. However, the model carries high capital expenditures, offers short windows for data transfers,

and functions best during nighttime in clear skies. Companies such as Eutelsat Quantum and SpeQtral aim to offer commercial service in the near future.

Innovations such as quantum repeaters and quantum memory are expected to gradually reduce the current limitations in distance and bandwidth. (See Exhibit 3.) Overall, these deployments and innovations will unlock a broader market opportunity that will grow in scale and activity over the next ten years.

Exhibit 3 - Quantum Networks Will Unlock New Market Opportunities

Technology at experimental level	Network type	Transmission	Architecture	Key limitations	Applications
Current	Trusted node	Satellite and metro/regional fiber	Point to point	• Trusted node must be secured • Carrier can access keys	Simple QKD encryption
In three years	Simple repeater	• Satellite and metro/regional fiber • Carries quantum states	Point to point initially, then multipoint	QKD applications with keys that are genuinely secret; no carrier access	
In four years	Quantum repeater; enables entanglement sharing	Satellite but trending toward fiber, including long-haul	Multipoint	No storage of quantum states	Advanced QKD, secure payment, quantum computer networks
In six to ten years	Quantum repeaters with memory	Predominantly fiber	Multipoint	Unknown territory in terms of costs and demand	Quantum clouds for quantum computing and quantum IoT

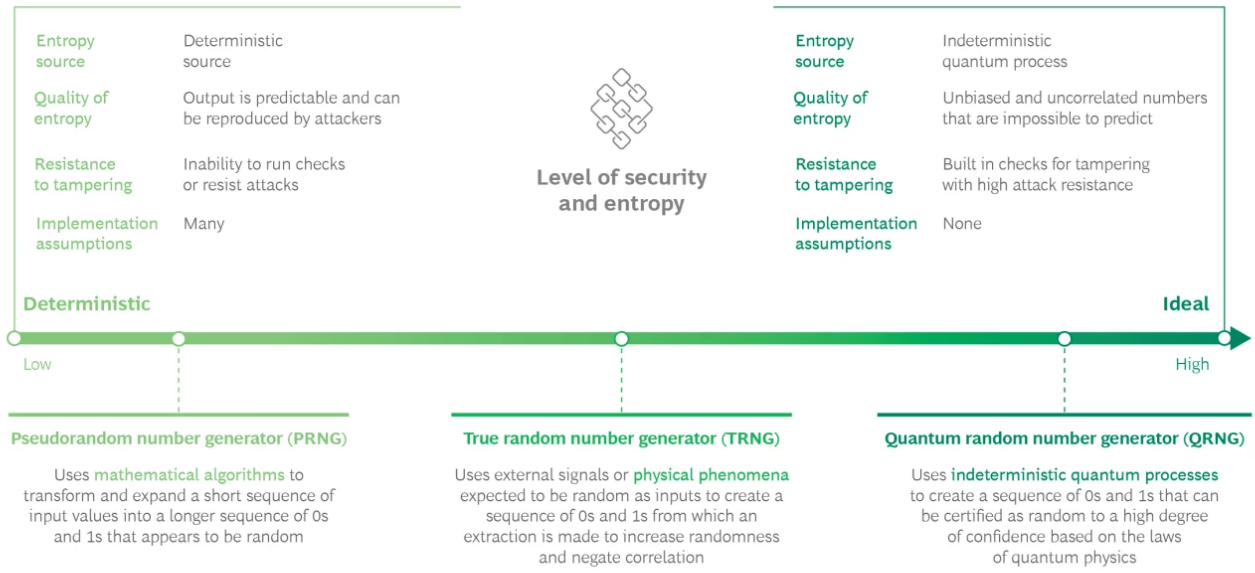
Source: Inside Quantum Technology.

Note: QKD = quantum key distribution.

Quantum Random Number Generation

Both the current and new security protocols require random numbers to create the keys that encrypt digital communication. As security threats grow in number and sophistication, most devices today have what is becoming a critical flaw: the keys they use are pseudorandom, meaning the numbers look random but come in a predetermined order. Like a card counter in a casino, a clever attacker could try to guess the next key—provided the attacker has seen enough of the keys the target system has generated in the past.

Exhibit 4 - Secure Key Generation Requires Truly Random Numbers



Source: BCG analysis.

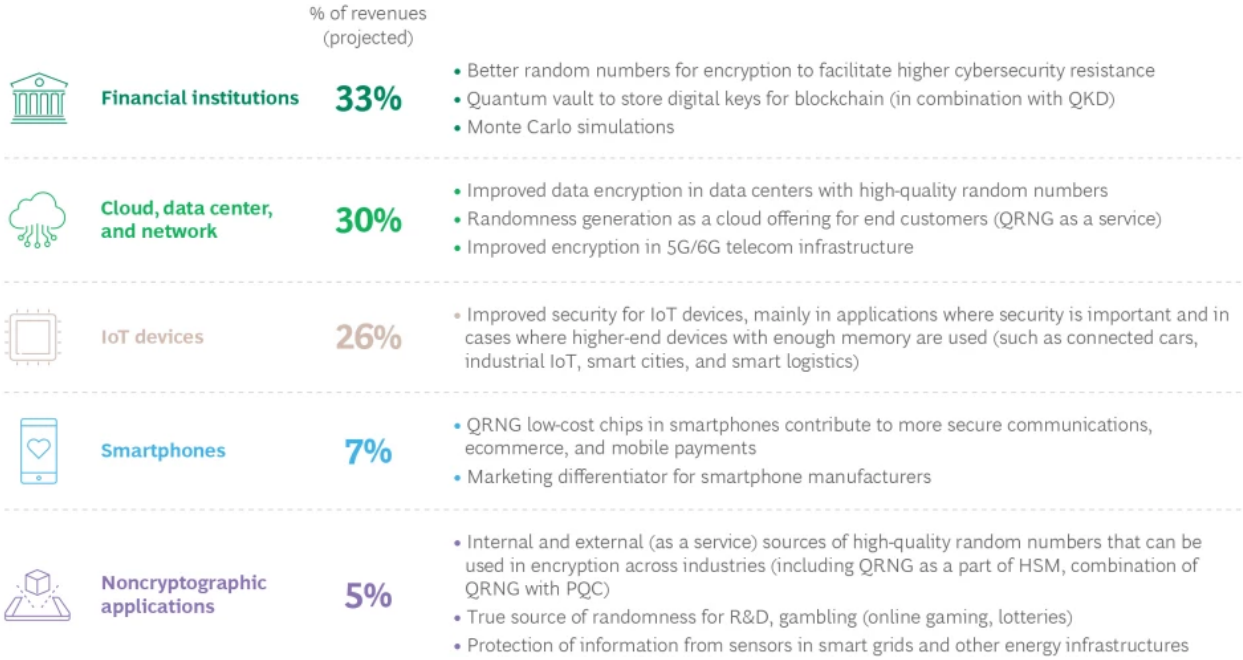
QRNG technology eliminates that flaw by leveraging quantum properties to generate truly random numbers. Regardless of the numbers generated by the system in the past, it is impossible for any actor to accurately predict the next one. (See Exhibit 4.)

QRNG technology is small enough to be embedded in mobile phone chips. Samsung has already deployed QRNG on premium smartphones using ID Quantique technology. The technology can also generate many random numbers per second—from 100 megabits per second up to 18.8 gigabits per second, the latter reached in 2021 by the University of Science and Technology of China—which is required in client-server workload use cases.

The true randomness that QRNG achieves is useful in other applications. Financial institutions rely on a methodology called Monte Carlo simulation to assess pricing and risk for products like options, fixed income securities, and interest rate derivatives. QRNG provides truly random numbers to these simulations, improving the accuracy of the analysis.

Industry experts expect QNRG to be deployed at scale as coprocessors or within system-on-chips. Adoption of QRNG will grow across many verticals, including finance and the Internet of Things (IoT), as organizations are drawn by these evolving use cases and the need to manage heightened security risks. (See Exhibit 5.)

Exhibit 5 - The Key Drivers of Adoption for Quantum Random Number Generation



Sources: Inside Quantum Technology; press reports; expert interviews; BCG analysis.

Note: QKD = quantum key distribution; QRNG = quantum random number generation; PQC = post-quantum cryptography; HSM = hardware security module. Because of rounding, percentages may not total 100.

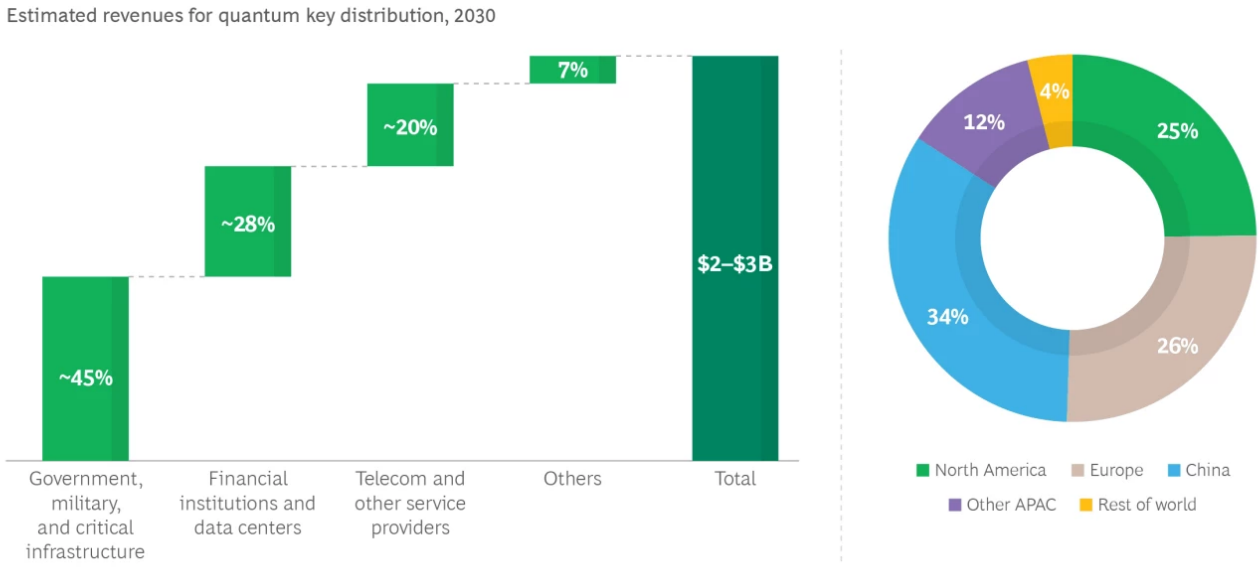
Drivers of Quantum-Communications Adoption

We have identified three waves of adoption of quantum communications technologies:

- The first wave (2015 to 2025) is being driven by several factors: government funding and applications in the government and military sectors; the spread of commercial QKD; and growing penetration of QRNG chips in smartphones, tablets, PCs, and data centers.
- The second wave (2025 to 2030) will feature more adoption by private companies and a growing penetration of QRNG chips in IoT infrastructure and devices.
- The third wave (2030 and beyond) will be driven by the emergence of new or improved technologies such as repeaters, memories, and better error-correction algorithms, which will reduce current loss of signal quality and enable the deployment of a broad network.

The first and second waves will be significant to three priority sectors (see Exhibit 6):

Exhibit 6 - Key Sectors and Geographies for Quantum Key Distribution



Sources: Inside Quantum Technology; The Quantum Insider; Quantum Safety; expert interviews; BCG analysis.

Note: Because of rounding, percentages may not total 100.

Government and Defense. A handful of governments are leading current adoption and development as they invest billions of dollars to build infrastructures and jumpstart commercial activity in quantum communications. Mitigating the quantum threat is a top priority; in the US, for example, the Quantum Computing Cybersecurity Preparedness Act requires government data to be quantum resistant—a state that an organization could attain only through a combination of classical and quantum approaches—by 2035. The US Department of Energy, meanwhile, has piloted a trusted-node QKD system deployed at an electrical utility in Tennessee. The EU is funding a massive, continent-wide implementation through the Euro-QCI initiative, with links already operational in the Netherlands. And China is expected to retain its early leading position by means of public investments, feeding its local market and its own PQC standards, which will compete with NIST's standards.

Technology and Telecommunications. Tech and telecom companies are already offering commercial quantum communications and leading standardization efforts. SK Telecom and ID Quantique are active participants in standards-development groups such as the ITU-T, IEEE, and ETSI.

SK Telecom offers QKD network infrastructure and QKD security, partnering with companies around the world such as Equinix, Orange, and Verizon. QRNG-as-a-service is offered by cloud providers such as Amazon Web Services (via its marketplace) and Telefónica Tech. Alibaba added ID Quantique's QRNG to its cloud-based services to improve the security of financial transactions and is testing the technology for other online services.

In partnership with SK Telecom and ID Quantique, Samsung introduced the world's first 5G smartphone in 2020, complete with a QRNG chip for security.

Financial Institutions. The need to secure sensitive financial data is driving adoption by key financial institutions. JPMorgan Chase is partnering with academic institutions to test quantum technologies, including QKD, to meet the need for speed and security while managing transactions and data. The firm also recently hired a leader for its quantum cryptography program.

ABN AMRO and QuTech are creating an advanced system for next-generation QKD, which will secure the Dutch bank's data. And the Industrial and Commercial Bank of China and the People's Bank of China are using operational next-generation QKD between cities.

We are fast entering an era of cryptographic uncertainty. After more than four decades of stability thanks to RSA and Diffie-Hellman, governments, businesses, and investors must prepare for a future of quantum communications and a new level of secure data transfer. Post-quantum cryptography and quantum communications could replace today's protocols as soon as 2030, but more likely by 2035; every government and company will need to implement one or several of these technologies to keep communications secure.

The stakes are high: secure cryptography underpinned $6.5 trillion of e-commerce in 2022, according to Statista, not to mention supply chains, online banking, and many other business activities that require the safe transmission of data. By understanding the specific secure-communications needs of each sector and the maturity of the technologies that will be deployed, investors can capitalize on the coming waves of quantum-communications adoption.

The authors would like to thank Lucian Comandar of Amazon Web Services and Pauline Boucher of Quantonation for their contributions to this research.

Authors

Jean-François Bobier

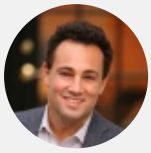
PARTNER & DIRECTOR

Paris

Cassia Naudet-Baulieu

SENIOR KNOWLEDGE ANALYST

Paris



Matt Langione

PARTNER

Boston

Brett Thorson

PLATINION ASSOCIATE DIRECTOR

Washington, DC

Jaroslav Šnajdr

MANAGING DIRECTOR & PARTNER

Prague

Stefan Deutscher

PARTNER & DIRECTOR

Berlin

ABOUT BOSTON CONSULTING GROUP

Boston Consulting Group partners with leaders in business and society to tackle their most important challenges and capture their greatest opportunities. BCG was the pioneer in business strategy when it was founded in 1963. Today, we work closely with clients to embrace a transformational approach aimed at benefiting all stakeholders—empowering organizations to grow, build sustainable competitive advantage, and drive positive societal impact.

Our diverse, global teams bring deep industry and functional expertise and a range of perspectives that question the status quo and spark change. BCG delivers solutions through leading-edge management consulting, technology and design, and corporate and digital ventures. We work in a uniquely collaborative model across the firm and throughout all levels of the client organization, fueled by the goal of helping our clients thrive and enabling them to make the world a better place.