CENTER FOR SPACE POLICY AND STRATEGY

GAME CHANGER | JULY 2020

QUANTUM KEY DISTRIBUTION IN SPACE

Joseph D. Touch, Lori W. Gordon

Quantum technologies enable us to harness the smallest particles of energy and matter to collect, generate, and process information in ways not achievable with existing technologies. One area of quantum—quantum communications—could significantly advance the secure transmission of government and business information. However, in a distributed communication or computing environment, the distribution of cryptographic keys (e.g., passwords) to remote sites can be dangerous. Attackers can eavesdrop and may be able to decode the keys from an encrypted stream either in realtime or at some possibly distant future date, rendering any communication using those keys vulnerable.

Quantum key distribution (QKD) is a technology that provides tamper-evident communication that can be used to securely deploy new cryptographic keys without direct physical contact. If tampering is not detected during the QKD exchange, the keys it generates can be trusted, regardless of future improvements in computational power, including potential improvements due to quantum computing. It has significant opportunity to advance secure communications across multiple sectors and to help secure national critical functions. Although QKD is already a commercial product in operational use in the banking and stock trading industries, its adoption is hindered by its reliance on dedicated physical fibers, which imposes geographic and cost considerations that have traditionally been onerous for government and private industry and limits deployments to the ground. This changed in 2017 when the Chinese satellite Micius conducted QKD with a ground station. Other countries, including the United Kingdom, Japan, and Canada, are increasingly gaining experience with experimental space- and ground-based QKD. According to some, quantum, and therefore QKD, is a lot like the space race in the 1960s—the United States cannot afford to come in second. Recent U.S. initiatives aim to steer billions of dollars of new funding toward civilian federal government research and development in quantum. To move QKD ahead as a game-changing technology will require investment in certification and standardization, starting with the attention of those making decisions in cybersecurity, satellite communications, and other industries requiring secure communications.

Quantum Key Distribution: Market Readiness
QKD is on the cusp of becoming a game-changing technology; however, it needs government involvement for R&D funding, certification, and accreditation to mature and advance.

Strengths	Weaknesses
• The only known way to deploy **new** keys remotely (to satellites) • Immediately **and forever** tamper-evident • **Future-proof cryptography** against future cracking (with one-time password) • Already being deployed in space by other countries	• Performance – needs a 100x to1000x speed improvement • Perceived technology hype (lack of trust) • Lack of standards and guidelines for integrated efforts • Fragility (susceptibility to denial-of-service attacks)

Introduction

Quantum key distribution (QKD) relies on the unique properties of quantum mechanics to enable secure communication between two or more parties, called *endpoints*. QKD enables each endpoint to compute the same key (or password) based on exchanged signals that are statistically impossible to intercept without detection. Cryptographic keys generated by QKD are already deployed in the finance industry using direct ground fiber links and are deployed experimentally in space by other countries.

QKD is the only known method for deploying new shared secrets to remote locations without transferring those keys via courier; instead, QKD exchanges public information that is used to compute the same key at both endpoints. It can generate new keys in ways that ensure they cannot be tampered with or copied in transit. The need for more frequent keying is motivated by advances in quantum computing algorithms, which, given corresponding advances in quantum computer implementation, could compromise keys as they are currently used; that is, keys that are not sufficiently updated frequently.

This paper explores the benefits of QKD and its unique support of three critical use cases (Figure 1):

1. **Safe rekey.** Deploy new keys using an algorithm that requires a small amount of predeployed keys for endpoint identification; e.g., to safely rekey a system without weakening the deployed keys. This is how QKD systems are currently used.
2. **Field boot key.** Deploy new keys without precoordination; e.g., to key devices after field deployment.
3. **Line-rate one-time password (OTP).** Deploy new keys that enable communication that can *never* be cracked.

The latter two uses require advances in technology, but, as equally important, all three also require trust in the QKD mechanism itself. This trust requires advancement in standards and validation techniques that are then accepted and endorsed by the appropriate operational authorities. The remainder of this paper discusses these issues in detail and explores the technology advances and endorsements

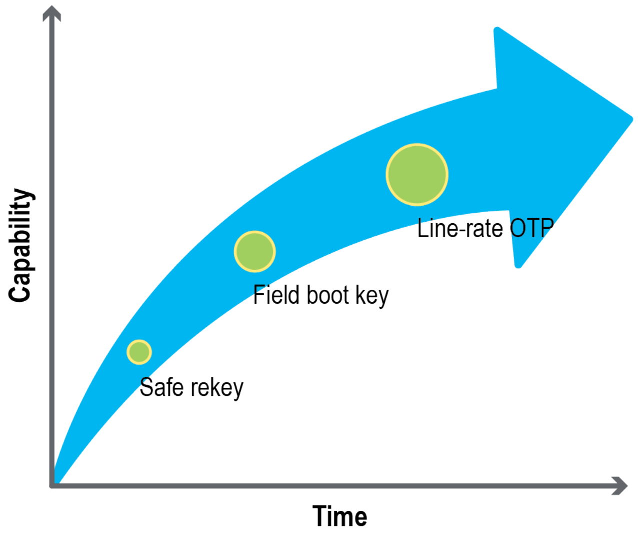


Figure 1: Progression of QKD use cases.

required to enable QKD to become a game-changing technology for cryptographic keying.

QKD is unique in its ability to create new shared secrets between two endpoints using only a communications channel. These established uses rely on dedicated, uninterrupted, direct fiber links and provide turnkey operation integrated with commodity Internet cryptography (IPsec, or internet protocol security).[1] However, QKD is an exotic technology that is highly sensitive to outside influence. This is a double-edged sword: on one hand, sensitivity uniquely enables QKD to detect and avoid the influence of eavesdroppers; on the other hand, the same sensitivity also enables denial of service (DOS) attacks. As a result, QKD is best applied only where other methods of key distribution are prohibitive, such as for spacecraft and remote ground locations. It also is applicable where predeployed keys are either too risky or not possible but where the endpoint can be identified directly. These issues and others are described in more detail below.

The Strategic Importance of QKD

QKD has significant opportunity to advance secure communications across multiple sectors and to help secure national critical functions. Although QKD is already a commercial product in operational use in the banking and stock trading industries, its adoption is hindered by its reliance on dedicated physical fibers, which imposes geographic and cost considerations that have traditionally been onerous for government and private industry and limits deployments to the ground. However, this changed in 2017 when the Chinese satellite Micius conducted QKD with a ground station. Recently, the National Aeronautics and Space Administration's (NASA's) National Space Quantum Laboratory (NSQL) initiative has begun developing technology to enable entanglement-based quantum network demonstrations over satellite-based downlinks and crosslinks, and to deploy infrastructure on the International Space Station to provide a collaborative research resource to characterize new technologies and evaluate new applications, including distributed quantum sensing, improved timing/synchronization, quantum computing over short-range links, and distributed computing and secure communication over long-haul links.

Both Japan's Small Optical TrAnsponder (SOTA) laser communication terminal onboard the microsatellite SOCRATES as well as a Chinese experiment with a small payload on Tiangong-2 Space Lab have already demonstrated space-to-ground QKD. Canada is planning the Quantum Encryption and Science Satellite (QUEYSSat). Additionally, Germany and Canada demonstrated QKD links between airplanes and ground stations in flying-sender and flying-receiver configurations, respectively.[2] Indeed, other nations have been working with QKD in the space segment and are increasingly gaining experience.[3]

Ground-based QKD is a significant area of research, particularly in European states, which are increasingly seeing the value of using quantum properties for a cyber secure communications network across the European Union (EU). These initiatives are intended to secure Europe's strategic autonomy and protect Europe's digital data economy against both near- and long-term threats, including from quantum computers.

The European quantum communication infrastructure (QCI) initiative includes 24 EU Member States that will develop a European cybershield within the next 10 years; Austria has led its first European pilot. Called the Open European Quantum Key Distribution Testbed (OPENQKD[4]), that pilot includes a range of manufacturers, network operators, system integrators, subject matter experts (SMEs), research institutions, universities, certification and standardization bodies, and end users.

In early 2020, the quantum communication infrastructure for the European Union (QCI4EU) initiative began to specify the user requirements and use cases to drive the overall system architecture for the European quantum communication infrastructure (EuroQCI), which is composed of both space-based and terrestrial solutions. It intends to span the EU and facilitate the secure transmission and storage of information and data, and link critical public communication assets throughout the EU. Applications include cloud infrastructures, the protection of sensitive medical information, communication data, and control signals used to operate critical infrastructure (i.e., telecommunication networks, energy supply).

The Continuous Variable Quantum Communications (CiViQ) project[5] focuses on the cost-efficient integration of quantum communication technologies in emerging optical telecommunication networks across 21 partners.

QUARTZ (Quantum Cryptography Telecommunication System),[6] supported by the European Space Agency (ESA), is designing solutions for the distribution of secure keys between optical terrestrial ground stations, each connected to a quantum-enabled satellite via quantum links; this unlimited satellite coverage will help overcome the limits of fiber-based QKD systems and provide connectivity in geographically dispersed areas.

Although the United States is currently ahead of China in quantum computing, China is ahead of the United States in QKD. According to John Prisco, CEO of the QKD company Quantum Xchange,[7] "This is a lot like the space race in the 1960s. The U.S. cannot afford to come in second on [QKD]." The United States is currently exploring QKD technology in national labs, universities, and FFRDCs. The U.S. National Quantum Initiative[8] (NQI) is the bulk of current support, yet of its $1.2 billion annual budget, $30 million is focused on quantum communication, of which only $3 million is focused on QKD (Figure 2).

Looking ahead, the "Industries of the Future" Act of January 2020 aims to steer tens of billions of new funding toward civilian federal government research and development efforts involving "industries of the future," including artificial intelligence (AI) and quantum information science (QIS). The act requires an assessment of federal investments in civilian research and development in the industries of the future and a plan to "double such baseline investments in AI and QIS" by FY22.[9] An overview of the unique capabilities of QKD is presented below, followed by a further discussion on the policy and investment issues in QKD.

The Mystery of Quantum: "Spooky" Phenomena

Before the game-changing technology of QKD can be explored, the basics of quantum phenomena must be understood. The term *quantum* has many meanings, originally referring to a discrete amount of energy (plural *quanta*). In common usage, it is shorthand for "quantum mechanical phenomena." Examples include photons interacting with certain ("birefringent") materials; e.g., those that bend light differently based on its polarization, atoms interacting with the boundaries of potential wells, or groups of atoms interacting with certain fields. Each of these properties involve interactions, not merely a particle or group of particles alone. Like the sound of falling trees in the forest, quantum properties exist only when they are observed.

Consider light, which has an electrical field with an orientation. That field can be vertical, horizontal, or anywhere in between, and it can even rotate. When light of any orientation passes through a certain (polarizing) filter, it is either absorbed or transmitted with a single, fixed orientation.

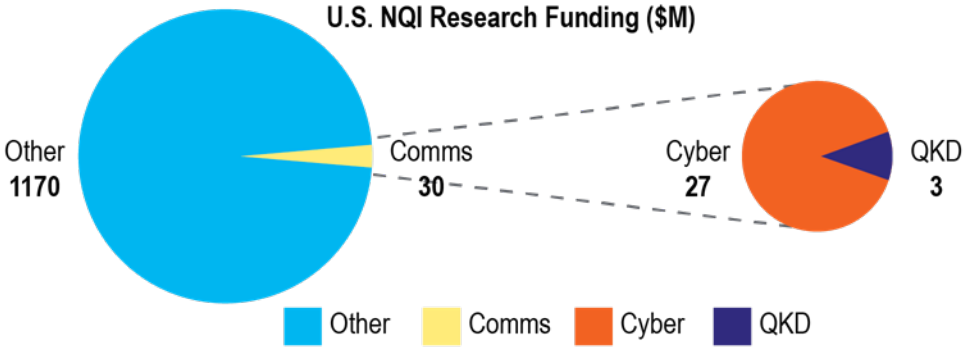


Figure 2: U.S. National Quantum Initiative (NQI) funding by area, showing the small fraction allocated to QKD.[8]

Quantum mechanical phenomena are defined as having the following three properties (also depicted visually in Figure 3):

1. **Quantized.** A measurable property that is observed only in a finite set of discrete values; e.g., horizontal or vertical polarization crystal transmission. For example, a tube of water can be filled to an (effectively) infinite number of different levels but a photon passing through a "birefringent" calcite crystal emerges with either vertical or horizontal polarization, never any value between.

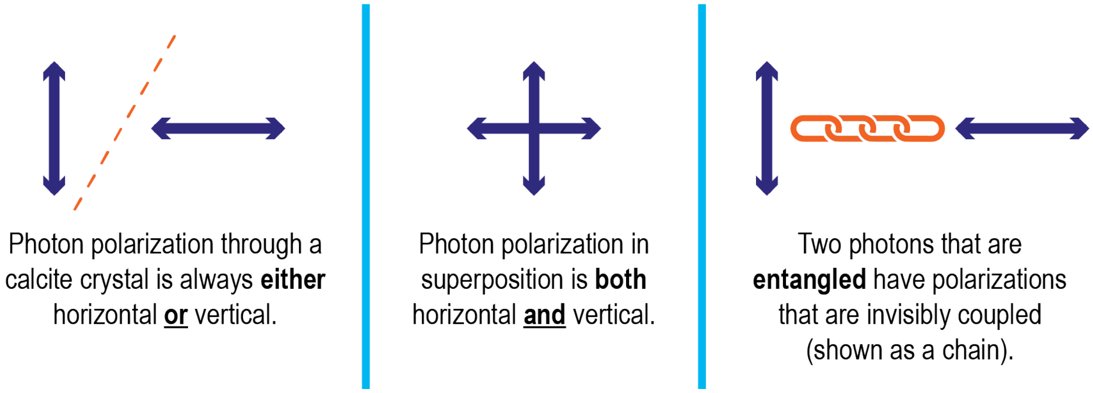
2. **Superposition.** Capable of having multiple discrete values at the same time, such that a measurement might yield any of the discrete values, each with some probability. In classical physics, a cat is either alive or dead; in the "Schrödinger's cat" thought experiment, the (quantum) cat placed in a box with a bottle of poison broken open by a random (typically radioactive) trigger is both alive and dead concurrently (see sidebar). For photons, this is equivalent to being partly both horizontally and vertically polarized. This is one way in which quantum systems are often called "magic"[10] (see sidebar).

3. **Entanglement.** Capable of coupling the superposition of two objects, such that the measurement of one results in the other's superposition collapsing to a single value correspondingly. This is called "spooky action at a distance" in which quantum objects (e.g., a pair of photons generated by a single event) are magically linked. Regardless of how far they are separated, measurement of one always precisely determines the state of the other; e.g., if two quantum cats are entangled, measuring one as alive always means the other is dead (they are typically converses of each other). This is the invisible linkage between entangled photons, where measuring one as vertical always means the other is horizontal.

More on the "Spookiness" of Quantum Mechanical Phenomena

Because they are not properties of everyday, macroscopic objects, superposition and entanglement are inherently impossible to explain in everyday terms. These are the properties that caused Albert Einstein to say that God does not play dice with the universe. They are deemed magical, even "spooky"; an entire published discussion addresses why "magic" is often the best description.[10] This is why they are, almost by definition, counterintuitive—our intuition is based on macroscopic objects that do not exhibit these properties.

The concepts are so challenging that physicists have nearly 20 different ways of trying to explain them (according to Wikipedia): in one, some objects (e.g., quantum cats, atoms, and photons) can exist in multiple states at once with different probabilities (the Copenhagen interpretation); in another, those objects are described as existing in separate universes (the "many worlds" interpretation). The former is the most widely taught to physicists; the latter is widely leveraged by science fiction writers; e.g., it is the basis of TV shows such as *Sliders, Stargate,* and *Dr. Who*, and movies like *Sliding Doors*, the *Cloverfield Paradox,* and the *Back to the Future* and *Terminator* series.



Photon polarization through a calcite crystal is always **either** horizontal **or** vertical.

Photon polarization in superposition is **both** horizontal **and** vertical.

Two photons that are **entangled** have polarizations that are invisibly coupled (shown as a chain).

Figure 3: Photon polarization depicted as quantized values that emerge from a calcite crystal (left); a photon in a superposition of states (center) and two entangled photons (right).

These three properties combine to yield some often surprising (even seemingly magical) results—surprising because they cannot be understood using classical methods. For example, if we shine a lamp (with mixed polarizations) through a vertical polarizer, only vertical light will pass and that light is then completely blocked by a horizontal polarizer (Figure 4, top path, left-to-right). If we insert a diagonal polarizer between the two others (Figure 4, bottom path, left-to-right), some light now emerges (25 percent, given perfect filters). Counterintuitively, adding an additional filter causes *more* light to pass, not less. This is one example of how quantum properties, notably leveraging polarization, enable QKD, including their quantization, superposition, and entanglement.

Three commonly distinct and largely independent uses of quantum mechanical properties (see Figure 5) include communication, computation, and sensing.

1. **Quantum communication** is used to detect the presence of eavesdroppers (tamper evidence) and is the basis of quantum key distribution.

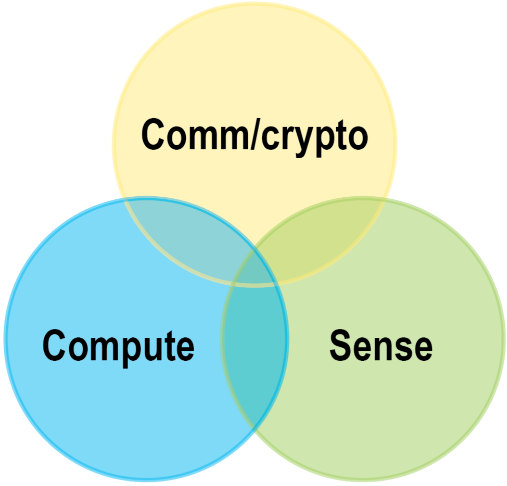


Figure 5: The commonly understood landscape of quantum uses. *Each area has a different target application, but there are cases where these perspectives overlap. Communications and cryptography use quantum properties to achieve tamper-evident information transfer. Computation uses those properties to achieve computing that scales linearly or polynomially, rather than exponentially, as the number of input parameters changes. Sensing uses those properties to improve the ability to distinguish remote events in space and time; i.e., increase resolution.*

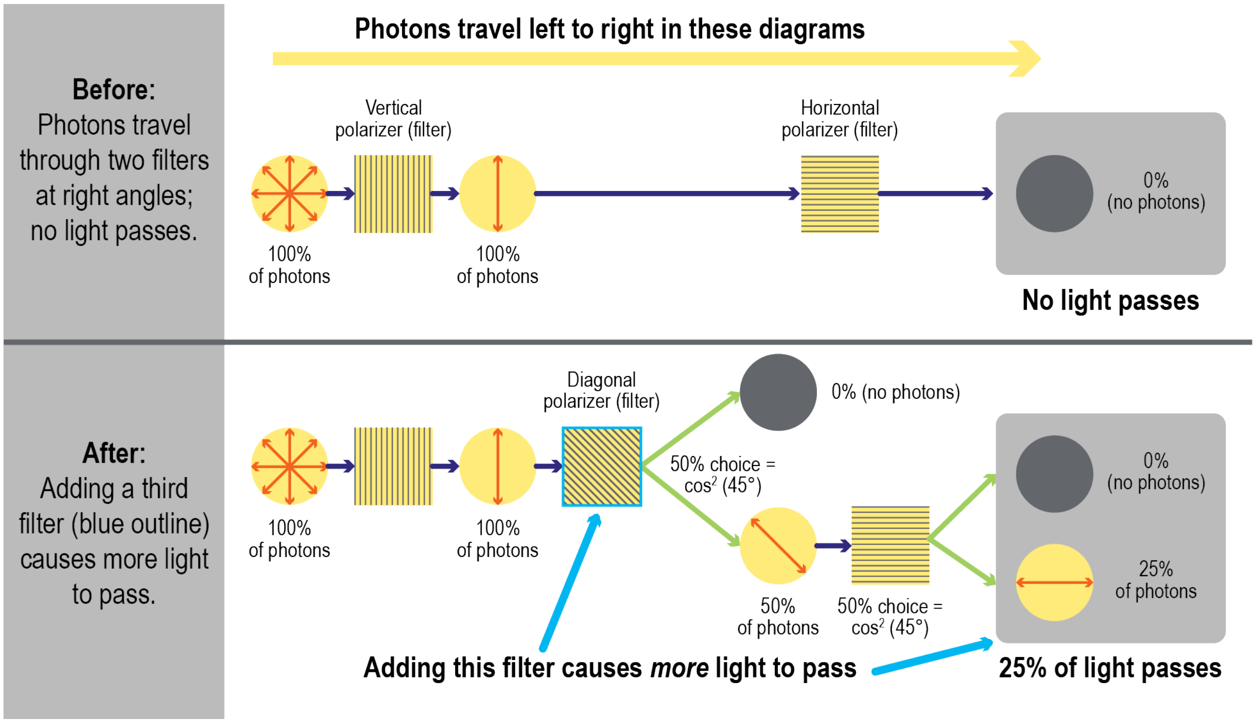

Photons travel left to right in these diagrams
Before:
Photons travel through two filters at right angles; no light passes.
Vertical polarizer (filter)
Horizontal polarizer (filter)
100% of photons
100% of photons
0% (no photons)
No light passes
After:
Adding a third filter (blue outline) causes more light to pass.
Diagonal polarizer (filter)
0% (no photons)
50% choice = cos² (45°)
100% of photons
100% of photons
50% of photons
50% choice = cos² (45°)
0% (no photons)
25% of photons
Adding this filter causes more light to pass
25% of light passes

Figure 4: An example of quantum "magic" in which adding a filter ("After," bottom) increases the light through a path in comparison ("Before," top). *The counterintuitive effect is that adding a diagonal filter allows more light to pass (25 percent to be precise).*[28]

2. **Quantum computation** is used to increase the scale of a problem that can be solved and is currently focused on specialized optimization techniques rather than general-purpose computing.[11]

3. **Quantum sensing** is used to increase measurement resolution and for space and planetary monitoring. It is also as a key component of lab equipment.

Additionally, each of these often uses quantum properties of very different objects; e.g., photons for communication, ions for computation, and a combination for sensing.

Each of these application areas leverages quantum properties in different ways. Communication and cryptography rely on the ability of superposition to collapse with any interaction, thus proving the presence of an eavesdropper. Conversely, quantum computation uses extreme electromagnetic and thermal isolation to avoid this collapse because it relies on superposition to increase scale. Quantum sensing uses this collapse to improve remote measurement. For a primer on the step-by-step operation of QKD, see Appendix A.

Comparison to Conventional Keying. Given that QKD is a technology for creating shared keys, it needs to be compared to conventional methods for keying, both direct (via physical contact) and indirect (via a communication channel). Preshared keys are a mature approach, widely used as a solution applied through a concept of operations in which the integrity of the key store can be trusted. Ground deployments rely on physical integrity protection; e.g., tamper-evident seals or self-destruct stores. Space deployments rely on radiation-hardened stable storage, where existing space-qualified parts support 256 MB in a single chip.[12] However, preshared keys eventually run out; for example, if 4,000-bit keys are changed every 5 minutes, the keys on that chip would be depleted in 5 years. On the ground this may not be an issue, but in space it can be, especially at geosynchronous Earth orbit (GEO), where 20-year deployments are typical. This duration decreases if there are multiple concurrent security associations or if keys are changed more frequently.

An alternative is to deploy new keys over a channel encrypted using existing keys, updating devices "over the air." However, classical (nonquantum) channels are susceptible to eavesdropping, and the collected data can be cracked later (offline), especially given advances in computing, new mathematical techniques, or if the keys used to encrypt the channel are compromised.

QKD overcomes both of these limitations to conventional keying, as the following subsections address.

Use Case 1: Safe Rekeying. Currently, QKD can be used to rekey a deployed system, using existing keys to authenticate endpoints. QKD protects the key that both endpoints create, and the existing key is needed only during the classical exchange (of the orientations of measurements at the receiver) to prevent a "man in the middle" attack. Information collected during the exchange either prevents QKD (eavesdropping the qubit stream) or is vulnerable only during the QKD algorithm, making those existing key uses invulnerable to offline attacks. This is the dominant existing ground use; e.g., for financial transactions over fiber links and experimentally at low Earth orbit (LEO) by others.

This case is difficult to motivate as a replacement for preshared keys, especially for space. At the current space-ground key generation rate of 1 Kb/s, it is comparable to the sustained lifetime output for a space-to-ground system. LEO systems are limited by ground contact duration and GEO systems are limited to nearly the same rates because their increased lifetime (4x) and contact duration (18x) are countered by decreased key rates due to the increased distance (1/100). Both solutions are comparable over their operating lifetime to a single 256 MB flash memory chip, which is already space-qualified and much less expensive. Note, however, that QKD protects only the key deployment; use of those keys in conventional communication channels and algorithms still presents the risk of future offline attacks.

Use Case 2: Field Boot Keying. QKD can support the boot keying of blank field-deployed devices, which can be useful either for space or remote ground deployments. It avoids issues with predeployed keys, such as the risk associated with protecting those keys as well as the potential inability to deploy the keys to new devices before first use, such as for special operations. This use requires the ability to authenticate the endpoints noncryptographically; e.g., using space (location) and time, which is a capability that still needs to be developed. It is an exotic case not expected to be deployed in large numbers, but it is a case uniquely enabled by QKD. As with the safe rekeying case, the generated QKD keys would be used on conventional communication channels and algorithms, which again presents the current risk to future offline attacks.

Use Case 3: Line Rate One-Time Password.
Uncrackable Keying. In the future, if key rates improve by several orders of magnitude to line communication rates, an additional use case becomes viable: QKD for one-time password (OTP). OTP is a future-proof algorithm that encrypts conventional (classical, nonquantum) communication channels; it cannot be decrypted in the future, regardless of advances in processing or mathematics.

As background, cryptography is based on the ability of two endpoints to generate what appear to be random streams but are predictable or meaningful to each other. A key is used to convert a plaintext message to an encrypted one; in most encryption algorithms, even the longest typical keys (4,000 bits, the size of this paragraph) are much shorter than the messages they encrypt (hundreds of papers such as this). There is an exception: OTP in which the key is the same size as the message and used only once.

Keys used in typical algorithms can be cracked, either by brute force (trying all combinations) or leveraging weaknesses in the encryption algorithm. A key is found because it is the only input that converts the encrypted text into recognizable plaintext, such as English; all other attempts generate gibberish. Advances in computing—speed improvements in classical computing or quantum computers—could help find these keys more quickly. Notably, quantum computing algorithms have already been developed that can crack both asymmetric (public key[13]) and symmetric (shared secret) cryptography using Shor's algorithm[14] and Grover's algorithm[15], respectively. An additional fear is the "unknown unknown"; that is, what we don't know, and cannot predict, such as a solution that may already be known by adversaries.

Paradoxically, OTP cannot be cracked exactly because every key is valid. The OTP key is the same length as the plaintext it encrypts, so many more potential keys exist. Every plaintext of the same length as the encrypted text has a corresponding valid OTP key. Recall that typical algorithms are cracked by finding one key that works where all others do not; for OTP, merely finding a key that works is no longer sufficient because OTP does not differentiate between the keys that result in plaintext. This makes OTP uncrackable forever, regardless of how long the attacker has to try to decrypt it, as long as the key is never reused.

The caveat is that OTP uses each bit of a key exactly and only once; thus, keys would need to be generated at the line rate of the channel being encrypted. Current space-ground QKD generation rates of 1 Kb/s are far too slow to be useful in that manner; improvements of 100x to 1000x would be needed; e.g., supporting a 0.1 Mb/s to 1 Mb/s encrypted stream. Existing QKD supports 1 Kb/s key generation using qubit rates of 10 Mbaud; OTP requires 1 Gbaud to 10 Gbaud qubit transmission with corresponding advances in receiver detector and sampling.

Technical Challenges of Operational Space QKD

QKD currently remains limited by a number of significant issues in engineering, algorithms, and systems implementation. Increased key generation rates require improvements in single-photon or entangled-photon generation rates and/or efficiency, increases in detector speeds (especially avoiding the need for cryocooling), and approaches for the classical optical issues of pointing stabilization, overcoming atmospheric losses, and suppressing background noise (atomic-line filters, narrowband transmitters, etc.). Post-processing algorithms for error estimation, error correction, and privacy amplification need to be standardized and validated and their risks quantified; notably, to reduce the risk of partially exposing the generated key due to exchanges over the classical channel. Alternate authentication methods need to be developed for the boot keying case, such as methods that rely on spatio-temporal information to replace signed hashes that rely on predeployed keys. Finally, there are numerous issues of integrating components, arranging and qualifying them for space (if deployed there), and managing the impact of QKD's inherent fragility—again, both its greatest strength (to detect eavesdroppers) and weakness (to DOS attacks and simply failing to operate).

Market Opportunities in Space QKD

Figure 6 depicts the expected evolution of the market penetration of QKD over time. QKD is already deployed for ground systems, largely for appearance; that market is small and not expected to increase. The first event expected to affect market utility is the development of spatio-temporal endpoint identification as a replacement for classical key-based authentication, enabling support for boot keying. While governments and industry around the world are investing in QKD applications, and QKD is on the cusp of being a critical technology, it needs to be standardized, verified during operation, and accredited for widespread deployment. Thus, the second expected event is certification, documenting the verification and validation procedures that establish the authority to deploy QKD operationally in critical infrastructure. An example would be the use of QKD to protect space assets; notably, their telemetry, tracking and command (TT&C) channels. The final notable event would be increased speed sufficient to support OTP; at that point, QKD finally becomes useful beyond niche cases (i.e., special operations and TT&C).

Market Challenges of Operational Space QKD

Although QKD has been the most widely used among quantum cryptography protocols since its inception in the late 80s, its potential for commercial application in the United States has not yet been fully exploited. Although research and the development of use cases in the European Union, Japan, and those countries mentioned previously are ongoing, market challenges can persist because the current QKD systems are often expensive, exhibit limited flexibility, and cannot operate seamlessly in telecommunication networks.

What is needed to achieve easier market penetration is broader endorsement to standardize, verify operations, and accredit QKD. Despite research and development activities at the international level, efforts by the European Commission's Joint Research Centre (JRC) to develop broad market-based consensus standards have not yet been established. And while the U.S. Congress and the private sector have directed some funding toward QKD, it is focused primarily in technology development rather than application. To fully mature a QKD market, significant attention to policies, partnerships, standards, and certification is needed (see Figure 7).

QKD market traction will also depend on whether QKD use cases remain primarily limited to highly sensitive security applications (government) or if they are able to extend beyond government and across a wider range of commercial sectors.

U.S. Government Funding. Signaling concern that the United States may fall behind in quantum development, in 2018, Congress enacted the National Quantum Initiative Act[8] (Table 1), which outlined a 10-year plan to accelerate the development of quantum information science with White House-led strategic oversight and interagency efforts to lead R&D and technology applications. The National Quantum Initiative (NQI) allocated $1.2 billion for research across a number of agencies, including the National Science Foundation, standardization at NIST, and critical infrastructure protection at the Department of Energy (DOE). Of the $30 million provided to DOE's

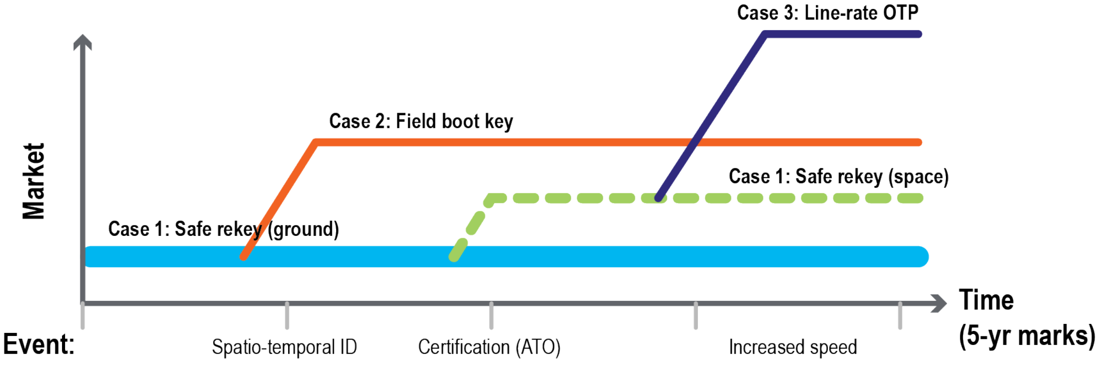


Figure 6: Anticipated market adoption over time for three different use cases.

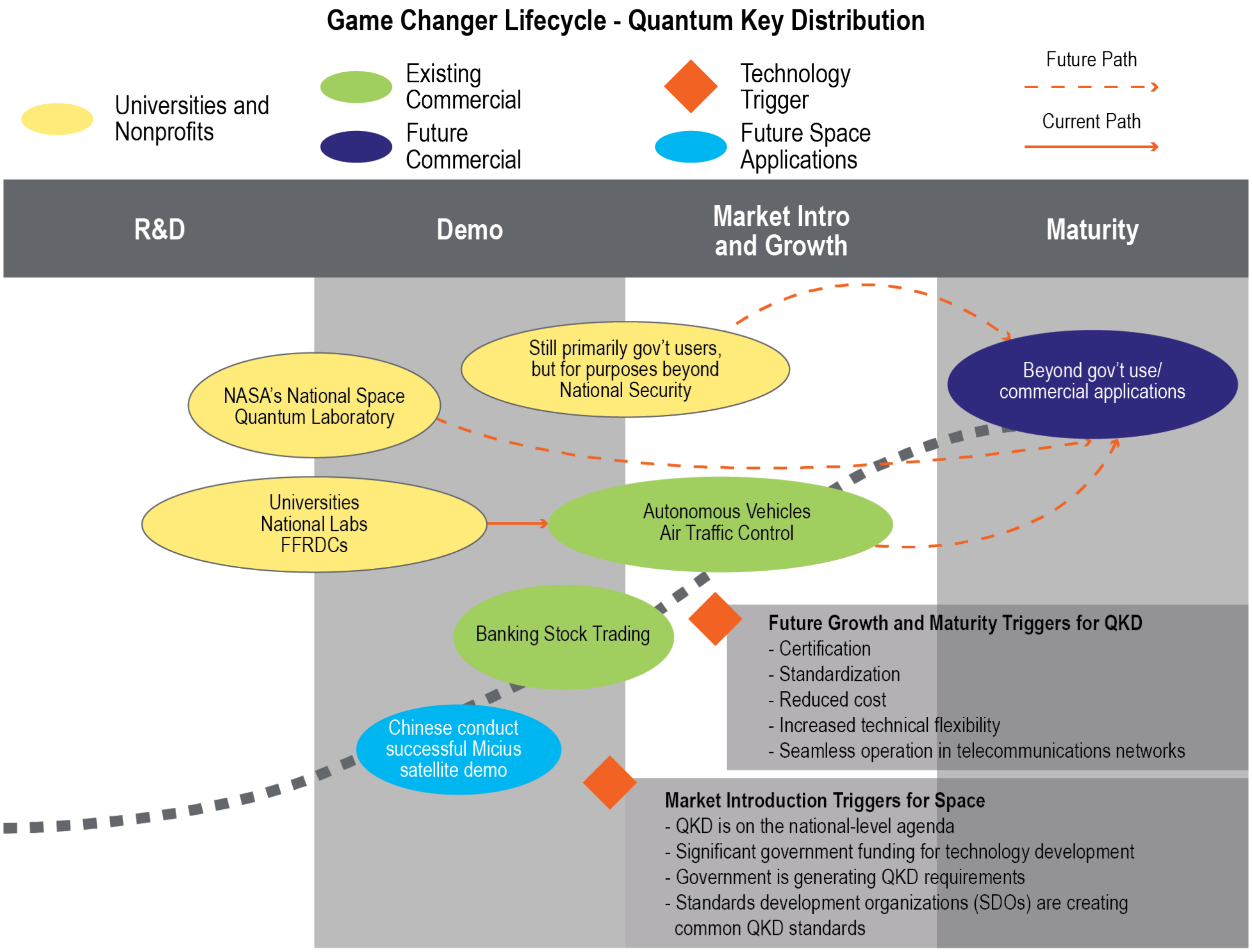

Game Changer Lifecycle - Quantum Key Distribution
Universities and Nonprofits
Existing Commercial
Future Commercial
Technology Trigger
Future Space Applications
Future Path
Current Path
R&D
Demo
Market Intro and Growth
Maturity
NASA's National Space Quantum Laboratory
Still primarily gov't users, but for purposes beyond National Security
Beyond gov't use/ commercial applications
Universities National Labs FFRDCs
Autonomous Vehicles Air Traffic Control
Banking Stock Trading
Chinese conduct successful Micius satellite demo
Future Growth and Maturity Triggers for QKD
- Certification
- Standardization
- Reduced cost
- Increased technical flexibility
- Seamless operation in telecommunications networks
Market Introduction Triggers for Space
- QKD is on the national-level agenda
- Significant government funding for technology development
- Government is generating QKD requirements
- Standards development organizations (SDOs) are creating common QKD standards

Figure 7: Market maturity and adoption forecast over time. *Triggers that advance QKD market maturity include funding, policies, standards, costs, and increased technical capabilities.*

Table 1: Key Events in the Development of the National Quantum Initiative (NQI) Act

Date	Document/Event	Source
June 2016	Advancing Quantum Information Science: National Challenges and Opportunities	White House Office of Science and Technology Policy
June 2017	Call for a National Quantum Initiative	National Photonics Initiative
October 2017	U.S. House Hearing on American Leadership in Quantum Technology	U.S. House Committee on Science, Space and Technology
April 2018	National Quantum Initiative Action Plan	National Photonics Initiative
June 2018	U.S. House Resolution (H.R.) 6227, National Quantum Initiative Act, introduced	U.S. House Committee on Science, Space and Technology
September 2018	H.R. 6227 passed U.S. House of Representatives	U.S. Congress H.R. 6227[16]
June 2018	Senate Bill S.3143, National Quantum Initiative Act, introduced	U.S. Senate Committee on Commerce, Science, and Transportation
September 2018	National Strategic Overview for Quantum Information Science	Subcommittee on Quantum Information Science, NSTC
December 2018	H.R. 6227, National Quantum Initiative Act, passed	U.S. Congress H.R. 6227[17]

Office of Cybersecurity, Energy Security, and Emergency Response, $3 million went to fund QKD initiatives. Industry has recommended that more of those funds be put toward a QKD proof of concept at DOE to support protection of critical infrastructure and to develop supervisory control and data acquisition systems using quantum keys.[18] More recently, the White House National Quantum Coordination Office has released a strategic vision for U.S. quantum networks for companies and laboratories to demonstrate, within five years, foundational science and key technologies to enable quantum networks and to identify the potential impact and applications for commercial, scientific, and national security benefit. It sets a goal that within the next 20 years, leverage networked quantum devices will enable new capabilities not possible with classical technology, as well as innovation in entanglement.[19]

Table 1 shows how U.S. investment in quantum information science technology policy has increased to parallel that of Austria, Australia, Canada, and the United Kingdom, whose federal quantum research budgets had previously long outpaced that of the United States. However, although the United States has established a broad policy for quantum information sciences and other initiatives are currently in Congress, these efforts do not significantly promote QKD to the level necessary to sufficiently advance its domestic or international market opportunities. QKD is still in the *early phases* of government investment.

Partnerships. The NQI is designed to model the United States' role in fostering open innovation across the public, private, and academic sectors, which provide opportunities to stimulate innovation in quantum information science. It also looks to foster stronger cooperation among like-minded nations and identify what international forums will help enable U.S. international dialogue and engagement.[20] NQI and other initiatives such as U.S.-Japan collaboration in The Tokyo Statement on Quantum Cooperation agreement on overlapping interests and issues of international importance will facilitate immediate U.S. gains in quantum technology capabilities.[21] Ensuring QKD is part of these partnership discussions is imperative to moving QKD forward and establishing broader market entry. However, investment across a wide number of research organizations and partnerships could also dilute the funding needed to achieve trusted QKD and paradoxically may further contribute to the quantum "hype." Instead, it is critical to establish and sustain deliberate, targeted partnerships to leverage U.S. national strategic advantages to accelerate QKD research and application.

As QKD and quantum cryptography are not yet working toward a coordinated research agenda and are farther down on the national-level agenda than quantum computing, QKD lies in the early phases of partnership maturity.

Standardization and Certification. Establishing trusted QKD would enable its broader application. As such, policy and partnership discussions should focus on the development of QKD standards and certification. This would reduce inaccurate QKD technology claims that may be deterring potential users, including organizations seeking to protect very high-value data, such as financial systems, military operations, ship-to-ship communication, airport traffic control, and communication between autonomous vehicles.

To deploy a QKD system, certification is necessary to validate the technology and enable more widespread adoption. Standardization is fundamental to promoting broad commercialization of QKD by building trust and consistency leading to certification. A well-established set of standards would be beneficial both to potential QKD users, as it provides definition to what they might consider buying, and to QKD vendors, as it provides a framework for requirements and how to specify them. Industry is lobbying for standards of compliance to be established using evaluation criteria similar to that of existing Federal Information Processing Standard (FIPS) 140-2 or Common Criteria certifications.[22] If QKD developers and consumers would increase focus on standardization and certification of QKD, its market readiness would accelerate. An option is to align this with traditional certified solutions or combine with emerging quantum cryptography technology.

A pathfinder in QKD component standardization is the work of the European Telecommunications Standards

Institute (ETSI) whose initial efforts began in 2007 with the creation of the Industry Specification Group for Quantum Key Distribution (ISG QKD) to develop a certification methodology.[23] Many countries outside Europe have already made efforts to launch national standardization for quantum technologies, and some companies are even attempting to establish de facto standards. None of these initiatives, however, have moved beyond the identification of a need for standardization, although it is clear that there is a critical mass of interested parties. QKD standards are in the early growth phase (see Figure 7), as organizations are only creating standards at the institutional level,[23] and QKD certification has not been achieved.

Conclusions

QKD is a critical technology that enhances communications security by the uniquely protected way it creates new shared keys without physical contact. At this stage, the commercial sector's QKD market ambitions and applications is outpacing that of the government. For the United States, issues with QKD's technology maturity, accreditation, and standardization continue to hinder widespread adoption and deployment. National policy has prioritized driving partnerships and technology development for other quantum technologies, thus allocating a smaller share of funding and resources to QKD.

The United States is faced with two opposing stances on QKD: (1) taking a watch-and-wait approach to assess other countries' technology innovation and development, or (2) shifting gears and investing heavily in this technology. If the United States invests, should the investment be in innovating the technology for new and diverse applications? Or, is it better spent on understanding how U.S. adversaries might be using this technology for hostile purposes? A significant path forward is the Defense Science Board's (DSB's) recommendations in its October 2019 report entitled *Applications of Quantum Technologies*[24], which recommends that the United States understand and track QKD developments and use by foreign parties and to encourage government and commercial sectors to work together to achieve mutual and/or complementary objectives for QKD advancement and adoption. This might include developing a path toward accreditation and endorsement, advancing QKD technologies further, to improve its speed and reliability, as well as enabling further uses that include safe initial keying and potentially invincible encryption.

For QKD to be successful, all of these areas should be actively pursued to fundamentally alter the security landscape and to enable more widespread adoption and operational deployment of QKD.

Appendix A: A QKD Primer

QKD is a mechanism by which endpoints exchange information and each compute the same key. The following is an overview of BB84, developed in 1984 as the earliest and simplest QKD protocol.[25] BB84 leverages superposition; other algorithms also use entanglement, notably E91[26] and BBM92[27]. A few key aspects are highlighted below.

As context, nearly all QKD protocols are based on polarized photons interacting with filters, just as light interacts with polarized sunglasses. Information is encoded in the angle of the polarization and measured with filters at the same angle. Two endpoints named Alice and Bob participate in the protocol. A third party, who might eavesdrop, is named Eve (short for "eavesdropper").[*]

The steps of BB84 are shown in detail in Figure 8.[†] Alice first sends qubits (quantum bits) encoded as individual photons to Bob. In these steps, *tuple* refers to an ordered set of bits (i.e., a one-dimensional array) and *basis* refers to one of the two orientations of perpendicular pairs of polarizations used for measurement, here indicated as level ("|" and "-") and tilted ("\" and "/").

1. Alice picks two random sequences
   a. One is a set of random measurement angles (e.g., level or tilted 45 degrees, Steps 1 and 2)
   b. One is a set of random bits (Step 3)

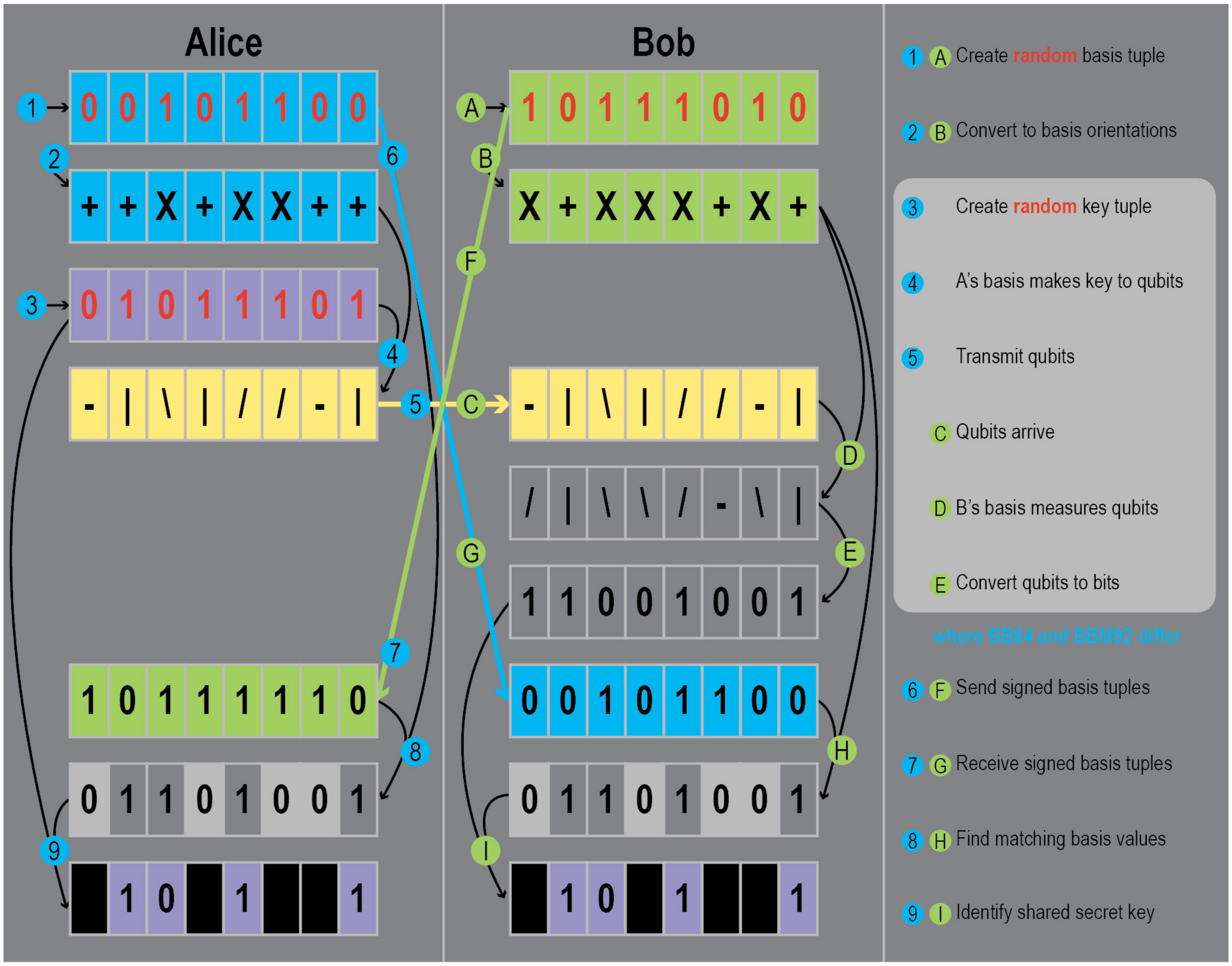


Figure 8: Diagram showing steps in QKD (as described in the text)[28]

[*] These names follow typical conventions used in cryptographic protocol descriptions.
[†] Alice is "A" and Bob is "B" in the description of the steps in the figure.

2. Alice combines these two random sequences to create qubits that are sent to Bob (Step 5/C)
    a. Using the bits and angles to determine the polarization of each photon (Step 4)
3. Bob picks a random sequence
    a. These are the measurement angles (Steps A and B)
    b. Bob measures the sent qubits at these angles (level or tilted, Steps D and E)

Alice and Bob then exchange their measurement angles over a conventional ("classical," not quantum) communications channel (Step 6/G and 7/F). Where the measurements match, Bob will receive the encoding Alice sent; the other measurements (which appear random) are discarded (Steps 8/H and I/9). Alice sends qubits in superposition and Bob's measurements collapse that superposition.

A small number of errors can be detected and corrected through additional exchanges over a conventional communications channel. A large number of errors indicates that Eve is present because if Eve were to measure the qubits, she would collapse their superposition, which Bob would detect as errors when Eve's measurement angle differed from Bob's. If Bob were to see too many errors, he would discard the key being computed and alert Alice to do the same. Bob can decide this before Alice, and he can decide to use the key they compute.

There are a few important takeaways from this review. Alice and Bob generate the same key; despite its name, QKD does not *distribute* a prespecified key. Alice and Bob need no shared secret in advance; they only need to know that they are speaking to each other and not to someone falsely claiming to be them (which can be accomplished in a variety of ways). Alice and Bob need no secret channel; their exchanges are either tamper-evident (the qubits) or public (the measurement angles and whether to abort). Eve cannot participate without exposing her presence and causing the exchange to abort—but this is her only and greatest power; i.e., to deny service. As a result, QKD exchanges a key that can be known secure and cannot be cracked offline using information measured during the exchange but is also (by design) susceptible to unpreventable DOS attacks. These properties explain why QKD is a niche technology and viable for only very particular uses.

References

[1] S. Kent and K. Seo, “Security Architecture for the Internet Protocol,” RFC 4301 Dec. 2005. https://www.rfc-editor.org/info/rfc4301

[2] I. Khan, B. Heim, A. Neuzner and C. Marquardt, “Satellite - Based QUD,” Optics & Photonics News, Feb. 2018. https://www.osa-opn.org/home/articles/volume_29/february_2018/features/satellite-based_qkd/

[3] S. Kent and K. Seo, “Security Architecture for the Internet Protocol,” RFC 4301 Dec. 2005. https://www.rfc-editor.org/info/rfc4301

[4] Open European Quantum Key Distribution Testbed (OPENQKD) web pages: https://www.openqkd.eu

[5] CiVIQ project web pages: https://cordis.europa.eu/project/id/820466

[6] QUARTZ description web pages: https://www.esa.int/Applications/Telecommunications_Integrated_Applications/Space_photons_bring_a_new_dimension_to_cryptography

[7] D. Nyczepir, “Are agencies like Energy funding quantum technology wisely?,” Fedscoop online, Oct. 4, 2019. (retrieved Apr. 20, 2020). https://www.fedscoop.com/quantum-key-distribution-energy/

[8] M. Raymer and C. Monroe, “The US National Quantum Initiative,” Quantum Science and Technology, V4 N2, Feb. 2019. https://iopscience.iop.org/article/10.1088/2058-9565/ab0441

[9] J. Curran, “Senate Bill Aims to Funnel Billions More to AI, Quantum R&D Efforts,” MeriTalk online, Jan. 16, 2020. https://www.meritalk.com/articles/senate-bill-aims-to-funnel-billions-more-to-ai-quantum-rd-efforts/ (retrieved Apr. 20, 2020).

[10] M. Ferrero, D. Salgado, J. L. Sánchez-Gómez, “Quantum Mechanics and Magic: An Open Discussion,” 2014. Published online in HAL archives-ouverts.fr as “hal-01057583”

[11] C. Williams, *Explorations in Quantum Computing*, 2nd ed., Springer, 2011.

[12] 3D-Plus Flash NOR product sheet, https://www.3d-plus.com/product.php?fam=8&prod=23 (retrieved Apr. 20, 2020).

[13] W. Diffie, M. Hellman, M., “New directions in cryptography,” IEEE Transactions on Information Theory, V22 N6, 1976, pp. 644–654. doi:10.1109/TIT.1976.1055638.

[14] P. Shor, “Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer,” SIAM Journal on Computing, V26 N5, 1997, p. 1484–1509, doi:10.1137/S0036144598347011

[15] L. Grover, “A fast quantum mechanical algorithm for database search,” Proc. 28th Annual ACM Symp. on the Theory of Computing, May 1996, p. 212.

[16] U.S. Congress, H.R. 6227 text: https://www.congress.gov/bill/115th-congress/house-bill/6227

[17] U.S. Congress, H.R. 6227 text: https://www.congress.gov/bill/115th-congress/house-bill/6227

[18] D. Nyczepir, “Are agencies like Energy funding quantum technology wisely” Fedscoop online, Oct. 4, 2019. https://www.fedscoop.com/quantum-key-distribution-energy/ (retrieved Apr. 20, 2020).

[19] U.S. White House National Quantum Coordination Office, “A Strategic Vision for America’s Quantum Networks,” Feb. 2020. https://www.whitehouse.gov/wp-content/uploads/2017/12/A-Strategic-Vision-for-Americas-Quantum-Networks-Feb-2020.pdf (retrieved Apr. 20, 2020).

[20] E. Kania, “China’s Quantum Future – Xi's Quest to Build a High-Tech Superpower,” Foreign Affairs, Sep. 26, 2018. https://www.foreignaffairs.com/articles/china/2018-09-26/chinas-quantum-future

[21] B. Vincent, “U.S., Japan Sign International Statement on Quantum Cooperation,” Nextgov online, Dec. 20, 2019. https://www.nextgov.com/emerging-tech/2019/12/us-japan-sign-international-statement-quantum-cooperation/162053/ (retrieved Apr. 20, 2020).

[22] N. Walenta, M. Soucarros, et al., “Practical aspects of security certification for commercial quantum technologies,” Proc. SPIE Electro-Optical and Infrared Systems: Technology and Applications XII; and Quantum Information Science and Technology, Oct. 2015. DOI: 10.1117/12.2193776.

[23] European Telecommunications Standards Institute (ETSI), Web pages on related technologies: Quantum Key Distribution (QKD). https://www.etsi.org/technologies/quantum-key-distribution (retrieved Apr. 20, 2020).

[24] U.S. Defense Science Board, “Applications of Quantum Technologies (Executive Summary),” U.S. Department of Defense, Oct. 2019. https://dsb.cto.mil/reports/2010s/DSB_QuantumTechnologies_Executive%20Summary_10.23.2019_SR.pdf (retrieved Feb. 2020).

[25] C. H. Bennett and G. Brassard. “Quantum cryptography: Public key distribution and coin tossing,” Proceedings of IEEE International Conference on Computers, Systems and Signal Processing, V175, p. 8, 1984.

[26] A. Ekert, “Quantum cryptography based on Bell’s theorem” Physical Review Letters. V67(N5), 1991, p. 661-663.

[27] C. H. Bennett, G. Brassard, N. D. Mermin, “Quantum Cryptography without Bell’s Theorem,” Phys. Rev. Lett., V68 N5, 1992. 557-559.

[28] J. Touch, J. Betser, J. Stoermer, A. Mollner, P. Ionov, U. Paudel, N. De la Cruz, “SMC/Aerospace Work on Free Space Quantum Key Distribution,” The Aerospace Corporation, TOR-2019-01630, July 2019.

About the Authors

Joseph D. Touch is a senior distributed systems architect in the Information Systems and Cyber Division at The Aerospace Corporation. He supports a variety of projects including quantum key distribution (QKD), proliferated low Earth orbit (LEO) networking, MILSATCOM networking, and ground systems architectures. He was previously the Postel Center Director and a research professor at the University of Southern California's Information Sciences Institute (USC/ISI), publishing more than 150 papers and receiving 5 U.S. patents in virtual network architecture, Internet protocols, nonlinear optical computing, and quantum networking. He is an ACM Distinguished Scientist, a senior member of the IEEE and OSA, a member of Sigma Xi, and actively participates in the development of Internet protocol standards. Touch has a dual bachelor's degree in biophysics and computer science from the University of Scranton, a master's degree in computer science from Cornell University, and a Ph.D. in computer and information science from the University of Pennsylvania.

Lori W. Gordon is a technology strategist at The Aerospace Corporation, specializing in national and homeland security, cybersecurity, and infrastructure protection and resilience. She has advised a range of federal agencies in strategy development, policy analysis, strategic foresight, and transformation. Gordon is an advisor to ISO, ANSI, and NIST technical working groups on topics ranging from commercial space standards to cybersecurity workforce to unmanned aerial systems. She also serves on curriculum advisory boards in the areas of cybersecurity and information technology, law and government, and resilient design with focus on the intersection of technology, ethics, and futures. Gordon has a bachelor's degree in geography with a minor in environmental science from the University of Maryland and a master's degree in public administration from the University of Massachusetts, Amherst.

About the Center for Space Policy and Strategy

The Center for Space Policy and Strategy is dedicated to shaping the future by providing nonpartisan research and strategic analysis to decisionmakers. The center is part of The Aerospace Corporation, a nonprofit organization that advises the government on complex space enterprise and systems engineering problems.

The views expressed in this publication are solely those of the author(s), and do not necessarily reflect those of The Aerospace Corporation, its management, or its customers.

For more information, go to www.aerospace.org/policy or email policy@aero.org.