QED-C

MAY 2024

QKD: PART OF A DEFENSE-IN-DEPTH SECURITY STRATEGY

QKD: Part of a Defense-In-Depth Security Strategy

ABSTRACT

Quantum technology can provide benefits and risks to cybersecurity. Quantum key distribution (QKD), first described by Charles Bennett and Gilles Brassard in 1984[1], is the basis for secure encryption based on the principles of quantum mechanics. In the ensuing four decades QKD systems have been deployed around the world to provide secure encryption for terrestrial as well as satellite communication. On the other hand, quantum computers of sufficient capability will be capable of breaking currently used public key encryption. In 2016 the National Institute of Standards and Technology (NIST) began a program to standardize a series of quantum resistant algorithms to replace current encryption standards thereby protecting against future cryptographically relevant quantum computers. This program is known as post-quantum cryptography or PQC. One of the tenets of cybersecurity is defense in depth, an approach that simultaneously provides multiple protections and seeks to avoid single points of failure. Here we describe the benefits of a hybrid QKD / PQC approach for a defense-in-depth strategy and address one of the limitations of QKD: initial authentication.

1 INTRODUCTION

Today the security of our information systems is more important than ever for personal, economic, and national security reasons. At the same time, attackers, both individual and state sponsored, are continually seeking and finding vulnerabilities. In addition, technological advances pose threats to existing cybersecurity.

A key component of cybersecurity systems is the use of encryption to exchange information securely. There are two cryptographic approaches—symmetric and asymmetric. Symmetric or private key encryption uses the same key to encrypt and decrypt the information. It requires less computational horsepower and is generally faster than asymmetric key encryption. However, it requires that the sender and receiver securely share the key in advance. Asymmetric or public key encryption depends on two keys that are related by a mathematical algorithm—one that is public for encryption by the sender and one that is private for

[1] C. H. Bennett and G. Brassard. "Quantum cryptography: Public key distribution and coin tossing". In *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing*, volume 175, page 8. New York, 1984. http://researcher.watson.ibm.com/researcher/files/us-bennetc/

decryption and is only known to the receiver. Public key encryption avoids the need for secure exchange of a secret key. However, the approach is more computationally intensive and therefore slower than symmetric encryption. The security of public key encryption depends on the inability to crack the mathematical algorithm, however there are threats to this assumption on the horizon.

Based on the principles of quantum mechanics, quantum computers will be able to perform computations that classical computers cannot. In particular, current algorithms used in public-key encryption can be broken by a sufficiently powerful quantum computer and will have to be replaced by new cryptographic algorithms that are "quantum resistant." With some modification (which may involve the doubling of the key lengths to protect against the Grover's search algorithm), symmetric cryptography is understood to be quantum safe.

Public-key cryptography based on factoring or discrete logarithm is widely used to protect online transactions. However, Shor's algorithm for factoring large numbers can break this type of cryptography, once a quantum computer that is sufficiently powerful, also known as a cryptographically relevant quantum computer (CRQC), is available. By destroying the security of most current public-key algorithms, such a quantum computer represents an existential threat to our cybersecurity infrastructure.

One approach to address the threat posed by CRQCs is to implement new post-quantum cryptographic (PQC) standards that are, to the best of our knowledge, not vulnerable. NIST is leading an effort to identify and select PQC algorithms (which are quantum-resistant mathematical algorithms) to become the new standards.[2] This project, which has been open to the public, was launched in 2016. Four algorithms were selected in 2022[3] and draft standards are in review[4]. NIST is expected to publish final standards in 2024. To provide algorithms with more diversity than the primarily lattice-based algorithms selected in 2022, NIST announced a new selection round for key exchange (fourth round) and reopened its submission process for signatures. Forty new qualified proposals were added to the pool of candidates being reviewed.

Another approach to address the threat of CRQCs is to take advantage of characteristics of quantum mechanics to provide cryptographic functions that do not depend on computing power. Two such characteristics are the generation of random secret keys using a Quantum

[2] See the NIST Post Quantum Cryptography webpage, accessed on 1/6/2024.
[3] NIST PQC Selected Algorithms, accessed on 5/28/2024
[4] NIST PQC request for comments on Draft FIPS for Post-Quantum Cryptography , accessed on 5/28/2024

Random Number Generator and the Key Exchange Mechanism using Quantum Key Distribution (QKD).

QKD is a secure communication method for exchanging encryption keys only known between the sharing parties, Alice and Bob. It uses properties of quantum physics, namely that a measurement modifies the state of the quantum system measured, to enable the detection of the presence of an eavesdropper and therefore provides assurance for secure exchange of the keys. QKD is a two-step process. The first step is the exchange of qubits between Alice and Bob through a quantum channel. The quantum channel is entirely open to a potential eavesdropper. However, as stated above, any attempt to eavesdrop on this quantum channel will result in modifications of the state of the qubits. The second step consists of classical exchanges between the users through a classical channel, also known as a service channel. This step is necessary to discover the changes caused by the eavesdropper and to process the qubits to obtain a secret key. The service channel must be authenticated, i.e. Alice and Bob have to be sure that they are talking to one another and that their transactions are not tampered with. Therefore, QKD requires an authenticated classical channel to manufacture secret keys.

If certain criteria are met, QKD exchanges cryptographic keys in a way that is provably secure and guarantees security. These secret keys are used to encrypt and decrypt messages, by means of symmetric cryptography.[5] Benefits of QKD vs. PQC include a reduced vulnerability to increasing computational power and an immediate detection of the presence of eavesdroppers.

Despite these benefits, the suitability of QKD in a practical cybersecurity strategy is still under discussion. In 2020, the U.S. National Security Agency published a statement entitled "Quantum Key Distribution (QKD) and Quantum Cryptography (QC)"[2] that describes five technical limitations of QKD. Several European governments have expressed similar concerns and restrictions regarding the use of QKD to protect national security systems.[6]

1. Quantum key distribution is only a partial solution lacking hardware authentication.
2. Quantum key distribution requires special purpose equipment.
3. Quantum key distribution increases infrastructure costs and insider threat risks.
4. Securing and validating quantum key distribution is a significant challenge.
5. Quantum key distribution increases the risk of denial-of-service attacks.

[5] Quantum Key Distribution (QKD), by Alexander S. Gillis, TechTarget, accessed on 1/6/2024.

[6] Quantum Security Technologies, and Position Paper on Quantum Key Distribution, accessed on 3/18/2024

A paper by Renato Renner and Ramona Wolf entitled "The debate over QKD: A rebuttal to the NSA's objections" (arxiv.org) reviews and offers pathways to overcome each of these issues. In this paper we focus primarily on the issue of authentication. We review the theoretical advantage of QKD and examine the various QKD authentication solutions. Addressing this issue increases the value of QKD alongside other approaches in the cybersecurity arsenal.

Given its complementary properties, QKD in combination with PQC generally strengthens a post-quantum computer defense-in-depth strategy. Implementing such a combined approach practically will require further development of QKD performance. This is what is currently underway in China with a vast QKD network along the east coast, in Europe with the Euro-QCI project, in Korea with a 2,000-km QKD backbone which will offer Quantum-Safe as a Service (QaaS), and in Singapore with a nationwide quantum-safe network that will be developed by the main telecom operator, Singtel. Currently, the U.S. government is not investing in such testbeds or demonstrations, ensuring it will be a follower and not a leader in the development of technical advances in the field.

2 THE ADVANTAGES OF QKD

Recognizing that QKD requires special purpose equipment, which may increase the infrastructure cost, it needs to demonstrate advantages with respect to purely algorithmic solutions. Here we show that QKD offers a clear theoretical advantage, since it enables Information Theoretically Secure (ITS) confidentiality from ITS authentication alone, a feat that is not possible classically. In practical schemes, since ITS is not easily implemented, QKD can offer perfect forward secrecy and long-term confidentiality.

2.1 Information Theoretical Security

Figure 1 shows schematically how QKD offers a clear theoretical advantage for the users of a communication channel. Classically, if Alice and Bob want to transform an unprotected communication channel into an authenticated one, they need to share a short secret key and use, for example, the Wegman-Carter protocol for authentication. This short secret key can only be used once and then must be replaced. If they wish to establish a confidential channel, they need to share a long secret key (by long, we mean as long as the data they wish to share) and use a one-time pad. There is no possibility to extend this key for the next round, so new pre-shared keys must be exchanged each time through a different channel.

With QKD, a short pre-shared key is sufficient to initiate the protocol and generate new ITS keys. A fraction of these keys must be kept as pre-shared keys for the next round. QKD is sometimes referred to as a key expansion scheme, that is, starting from a short seed key, it enables unlimited generation of new keys in an ITS manner.

ITS is the gold standard for information security. However, encrypting data with ITS is not practical, as it uses a one-time pad, which requires keys as long as the data and is used only once. Therefore, we normally settle for symmetric encryption, specifically the AES protocol, which is considered quantum safe. AES uses short symmetric keys to encrypt a large amount of information. When QKD keys are used in conjunction with AES, the requirement for ITS is no longer fulfilled for the encrypted data. However, even when ITS is not implemented, QKD still offers advantages with respect to algorithmic methods for confidentiality. In particular, it provides perfect forward secrecy.

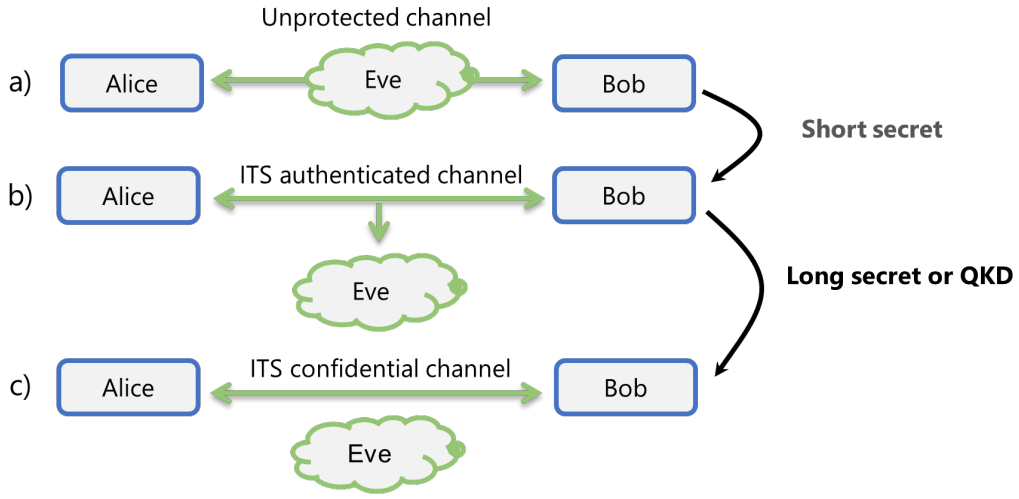

Figure 1: Communication channels

a) *Represents an unprotected channel, where the eavesdropper Eve can manipulate the data at her will.*
b) Represents an authenticated channel: Eve can extract the data but cannot modify it. Alice and Bob know that the data exchanged between them has not been tampered with. To build an Information Theoretically Secure (ITS) authenticated channel, Alice and Bob need to share a short secret key.
c) Represents a secure channel, which excludes Eve completely. To build an ITS secure channel, Alice and Bob either need to have a long secret key (the key must be as long as the data they wish to exchange, and should be used only once), or they need QKD.

QKD therefore transforms an authenticated ITS channel into a confidential ITS channel. This is not possible classically.

2.2 Perfect Forward Secrecy

As described above, when used in conjunction with short pre-shared keys for authentication, QKD offers an ITS key exchange mechanism. In practical implementations, where QKD is used with symmetric encryption, such as AES, the resulting data exchange is not ITS, but remains quantum-safe. However, since the initial pre-shared keys are used only for authentication and are then renewed with independent keys obtained from QKD, the resulting scheme achieves perfect forward secrecy. The session keys used for encryption cannot be obtained from any previous keys. The scheme is reset at each new QKD exchange.

In contrast, in a classical setting, an initial pre-shared key can be expanded through a key derivation function, to provide a stream of new keys. These keys can be used for encrypting data. If the key expansion scheme is quantum-safe, the resulting scheme is also quantum-safe. However, leakage of the initial seed key leaks the whole series of future keys. Therefore, this initial key must be kept secret for the duration of the confidentiality requirement of the data.

2.3 Long-term Confidentiality

Large QKD networks with many end users require a large number of initial pre-shared key pairs. If the number of users is N, the number of pre-shared key pairs necessary to provide links between all users is N^2. Adding a single user requires N new key pairs. This makes the option of pre-shared keys difficult to implement in practice in large networks. Therefore, different authentication methods, such as hash based or PQC, may be preferable, as described in Section 3.

Figure 2 shows the time-dependence of authentication and confidentiality schemes. For authentication, it suffices that the scheme is secure until the transaction. For confidentiality, the requirement is higher: the scheme must be secure for the lifetime of the data.

Security of approaches that are based on a hard mathematical problem (examples include RSA and the proposed PQC algorithms) is not immune to being compromised by advances in computational capabilities. Such advances may be in the form of increased performance of classical or quantum computers or in the form of newly discovered algorithms, or both. This is

precisely what happened with current public-key cryptosystems, which can be destroyed by Shor's algorithm implemented on a CRQC.

In contrast, the security of QKD as a key exchange mechanism is not impacted by computational progress. If the authentication scheme used in conjunction with QKD is safe at the time of the transaction, the security of the QKD keys remains forever. Therefore, QKD is an appealing option for information with a long lifetime.

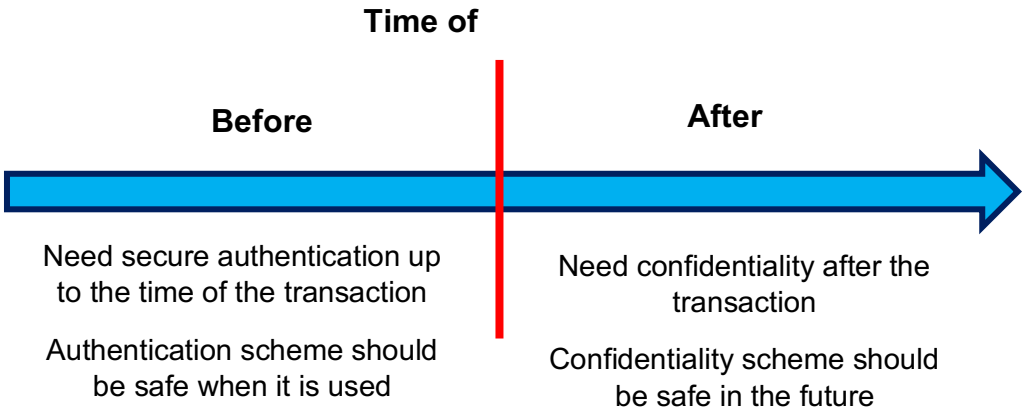

Figure 2: Time-dependence for authentication and confidentiality

3 AUTHENTICATION SCHEMES FOR QKD SECURITY

As explained in Section 1, QKD requires a classical authenticated channel to provide secure keys. If the authentication keys are not secure, an attacker can break them and thereby bring all classical and quantum communications under the attacker's control with the objective of relaying the information by means of a man-in-the-middle attack. As noted in the NSA statement, there is concern with initial authentication or "entity source authentication". For QKD to be secure, the classical messages exchanged for processing the key must be authenticated. This is meant to solve the problem of "we have negotiated a key securely over the quantum channel, but we don't know who we have negotiated a key with" because one now knows from whom specifically the bits came from. In this Section, we discuss the various means of authentication, which must be used to obtain a secure key exchange and offer some recommendations. These solutions are summarized in Table 1.

3.1 Information Theoretically Secure Authentication

ITS is provable security for both authentication and confidentiality and is easily achievable for authentication. It requires a short initial pre-shared key between Alice and Bob. Then, Alice and Bob store the whole discussion they had during the key processing in a file. The Wegman-Carter protocol explains how to add the pre-shared key to the file and generate a tag. Alice sends this tag to Bob, who can verify that the tag received is the same as the one he has generated. An eavesdropper, who has no access to the pre-shared key cannot build the same tag, and therefore cannot pretend to Bob that she is Alice.

This solution offers the maximum security and works best for point-to-point links or QKD networks with a small number of participants. However, when the number of potential pairs of users increases, it can quickly become too cumbersome. In this case another approach is preferable.

3.2 Authentication with Hash-Based Signatures

The most secure authentication algorithms, which do not rely on the same kind of complex mathematical problems needed by other PQC algorithms, are hash-based signatures. The security of a hash-based signature relies solely on the existence of one-way functions (and, of course, on correct implementations). Several candidates have been considered. Stateful signatures are generally the fastest and smallest, but the users must keep track of each signature to prevent re-use of the same keys leading to serious implementation issues. Therefore, stateless signatures, such as Sphincs+, have been proposed. Sphincs+ is one of the signatures algorithms selected for standardization by NIST.

3.3 Authentication with other PQC Signatures

The other signature schemes under consideration rely on the existence of a one-way function with “trapdoors”. The mathematical structure of these schemes is much more complex, and it is distinctly possible that a quantum computer, or even a classical computer, eventually could break them. The immediate question when relying on PQC signatures for authenticating QKD is: if we use PQC for signatures, why do we need QKD at all? We could indeed use PQC for both authentication and key exchange. However, there are long-term confidentiality benefits of using PQC for signature and QKD for key exchange. Authentication must be safe up to the time of the key exchange. On the other hand, confidentiality should be safe as long as the encrypted information remains secure. If we trust an *authentication PQC algorithm* to be safe today, we

can safely use it. In contrast, we have to be sure that a *key exchange PQC algorithm* stays safe for a potentially much longer period. This is what is offered by QKD. Moreover, using QKD and PQC provides defense-in-depth by eliminating a single point of failure.

Table 1: Authentication schemes that can be used with QKD

Authentication Scheme	Pre-Shared Keys	Hash-based PQC	Non-Hash-based PQC
Security Hypothesis	None	Existence of one-way function	Existence of one-way function with trapdoor
Applicability	Point-to-point links and small QKD networks	QKD networks; Critical Infrastructures	Global QKD networks
Examples	Wegman-Carter authentication	Sphincs+...	CRYSTALS Dilithium...

3.4 Recommendations

As shown in Table 1, the various authentication schemes have different security hypotheses and different scopes of application.

For single point-to-point links and small networks, pre-shared keys offer the best security, with an ITS scheme. This solution works best for example for datacenter-to-datacenter applications, where the main datacenter is linked to a mirror one, for example for duplication or disaster recovery. It is also applicable for small networks, with a restricted number of permanent nodes. This type of scheme is limited in situations in which there is a need to be able to change the number of nodes dynamically. For an *N* node network, adding a single extra node requires *N* new pre-shared keys, which must be brought to all the existing nodes. In this case, it is preferable to use a slightly less secure, but more convenient solution, such as the reduced key size variants of NIST-reviewed PQCs.

The basic security hypothesis, namely that one-way functions exist, is an almost absolute requirement for cryptography. Without it, even symmetric key cryptography fails. This would generate the so-called “cryptopocalypse”, where no crypto would exist, except for ITS. We would be back to trusted couriers transferring data. Fortunately, it seems that a CRQC will not be able to destroy one-way functions and symmetric key cryptography, so it is safe to rely on them to build authentication schemes. This type of authentication should be used for networks with very long lifetime, which cannot be easily upgraded, such as critical infrastructures. In this

case, the choice of the authentication scheme with the highest security is worth the extra implementation complexity.

For even larger networks where long term confidentiality is required but that can be upgraded if needed, the choice of a PQC algorithm for authentication seems best. The caveat is that if the chosen scheme, or the chosen parameters of the scheme, become unsafe it must be possible to upgrade to a new scheme or to new parameters. Of course, we would need to know that the scheme is broken in order to modify it. The previously exchanged data would remain secure, thanks to the properties of QKD. The more standard public-key infrastructure with PQC algorithms in conjunction with QKD for confidentiality would make this type of scheme easier to implement, while providing good security.

4 CONCLUSIONS

Progress in the development of quantum computers poses real threats to cybersecurity. When a cryptographically relevant quantum computer will be available is not precisely known, but it is essential to prepare now for the eventuality. Given the advantages and disadvantages of various quantum-safe strategies, using just one system or relying on just one approach, while less complex, is inherently less secure. A defense-in-depth strategy provides layers of protection resulting in superior resilience. Therefore, overcoming issues with QKD offers improved security that leverages the strengths of multiple protocols.

The various authentication schemes discussed in this paper provide solutions to address a major concern in the overall security of QKD. By addressing the authentication issue, QKD can be implemented in use cases that require assured cybersecurity among a limited number of nodes and over relatively short distances (approximately 100 km for a single link). Other issues remain; today QKD long distance networks require trusted nodes. However, enabling technologies for long-distance QKD, including quantum memories and quantum repeaters, are under development. Research and development of these technologies is underway and will further expand the utility and practical implementations of QKD.

QKD investments, both public and private, are primarily being made in Europe and Asia. As a result, the United States has a dearth of expertise, which is now concentrated in countries and regions that are adversaries of the United States and its partners. Moreover, U.S. companies that are developing relevant technologies have little access to funding and fewer U.S. customers. We advocate that the U.S. maintain a presence in the field and in particular support

development of hybrid solutions integrating both PQC and QKD for the greatest protection from threats posed by future quantum computers.

Acknowledgments

We would like to thank the following members of QED-C who contributed to this paper.

Bruno Huttner is Director of Strategic Quantum Initiatives at ID Quantique and co-chair of the Quantum-Safe Security working group of the Cloud Security Alliance; **John Prisco** is CEO of Safe Quantum Incorporated; **Carl Dukatz**, Accenture Managing Director-Global Lead for Quantum Computing at Accenture; **William Trost**, Lead Member of Technical Staff at AT&T, Chief Security Office (CSO), Quantum Computing Cybersecurity Initiative; **Kirk McGregor**, Chief Strategy Officer at Iff Technologies and affiliate researcher with the Lung Center in the Department of Internal Medicine, School of Medicine at the UC Davis Medical Center and with Expolab in the Department of Computer Science at UC Davis; **Elizabeth Wood,** Professional in the AT&T Chief Security Office (CSO), Quantum Computing Cybersecurity Initiative.

Special thanks to **Celia Merzbacher,** Executive Director of the Quantum Economic Development Consortium (QED-C) for her helpful review of this paper.

This paper is not a statement or recommendation of policy or any particular position on quantum key distribution by QED-C itself and may or may not be a policy recommendation or position held by any QED-C member.