Quantum-related Cybersecurity in Denmark

OCTOBER 2022

UNIVERSITY OF COPENHAGEN

DTU

KMD An NEC Company

IBM

DANSK ERHVERV Danish Chamber of Commerce

IT-BRANCHEN

KPMG

cyber hub

DigitalLead.

QUANTUM-RELATED CYBERSECURITY IN DENMARK
October 2022

Supported by a Cyberboost grant from Cyber Hub.

Editorial team:
Niels Bohr Institute
DTU Physics
DTU Electro
KMD
IBM
Danish Chamber of Commerce (Dansk Erhverv)
The Danish ICT Industry Association (IT-Branchen)
KPMG

Layout: nxtbrand.dk

CONTENTS

MOTIVATION.. 4

THE NATURE OF THE THREAT
FROM QUANTUM COMPUTERS.. 5
What is being threatened?.. 5
What is the nature of the threat?.. 6
When will the threat materialize? 6

COUNTERMEASURES 8
PQC – Post Quantum Cryptography.. 8
Background..8
NIST PQC standards process and competition 8
Pros and cons of PQC 9
Specific implementation strategies 9
QKD – Quantum Key Distribution.. 10
Background.. 10
Commercialization of QKD.. 12
Current Limitations of QKD.. 12
PQC vs. QKD or PQC and QKD?.. 15
Recommendations for the transition to quantum-safe cryptography... 15
Industry relevance 15
Transition to quantum-safe cryptography 16
Get an overview.. 16
Create a migration plan 17
Migration execution 17
Recommendations.. 18

DANISH POSITIONS OF STRENGTH.. 19
Research groups 19
Current and recent research 19
Industry.. 20
Conclusion 20

OPPORTUNITIES.. 21
Next steps.. 21
Areas of potential research 22
Summary and conclusions 22

MOTIVATION

The likelihood of the advent of a quantum computer able to break widely used public-key-cryptography schemes is increasing. It is still difficult to say precisely when, but a timeframe of 10-15 years is estimated to be realistic. However, the risk is already present now, as encrypted data stolen and stored today may be exposed later when sufficiently powerful quantum computers become available.

The process of migrating from today's encryption schemes to quantum resistant schemes is not straightforward. It will take time and effort, and it will require additional research, standardization, and commercialization of solutions: this is why it is imperative to start now.

If the potential of quantum computing is realized, it can be used to break public-key-cryptography schemes such as RSA and ECC, both of which are widely used for securing data transmission, including the technology behind MitID[1]. This means that public sector institutions, corporations and others exchanging or holding sensitive information will potentially be exposed. Likewise, signed digital documents, such as long-term legal contracts, risk being altered and re-signed if no action is taken to counter the threat.

NSA (the US National Security Agency) already recommends that sensitive government information be protected by quantum-resistant cryptography[2] and NSA has very recently required that all national security systems are completely migrated to quantum-resistant cryptography by 2035[3]. Similar recommendations have recently been issued by public authorities in Germany[4], and UK[5]. Given the high level of digitalisation in Denmark, we must start preparing for the potential threat from quantum computers now.

This paper gives the reader an introduction to the potential threat and presents proposals for adequate countermeasures. Moreover, prevention of the threat can be seen as an opportunity to leverage Denmark's strengths within quantum-safe cryptography. Consequently, we also present Danish positions of strength in both research and industry as well as recommendations for future actions.

The intended audience for this paper is specialists and leaders in Danish industries and public organizations.

This paper is the result of a joint research project between The Niels Bohr Institute, DTU Physics, DTU Electro, KMD, IBM, Danish Chamber of Commerce, The Danish ICT Industry Association and KPMG and with valuable and insightful input from both Cryptomathic and Professor Ivan B. Damgaard at the Department of Computer Science at Aarhus University. The project has been supported by a Cyberboost grant from the Cyber Hub, funded by Industriens Fond.

[1] MitID uses both RSA and ECC according to: Digitaliseringsstyrelsen, Om MitID p. 11, https://digst.dk/media/24710/om-mit-id-baggrund-whitepaper_webtilgaengelig-version.pdf

[2] https://www.nsa.gov/Cybersecurity/Quantum-Key-Distribution-QKD-and-Quantum-Cryptography-QC/

[3] https://media.defense.gov/2022/Sep/07/2003071834/-1/-1/0/CSA_CNSA_2.0_ALGORITHMS_.PDF

[4] https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Brochure/quantum-safe-cryptography.html?nn=433196

[5] https://www.ncsc.gov.uk/whitepaper/preparing-for-quantum-safe-cryptography

THE NATURE OF THE THREAT FROM QUANTUM COMPUTERS

What is being threatened?

In the context of cybersecurity, the term “Quantum Threat” is often used to describe the threat posed by quantum computing to the viability of the most widespread type of cryptography in use today: Public Key Cryptography (PKC).

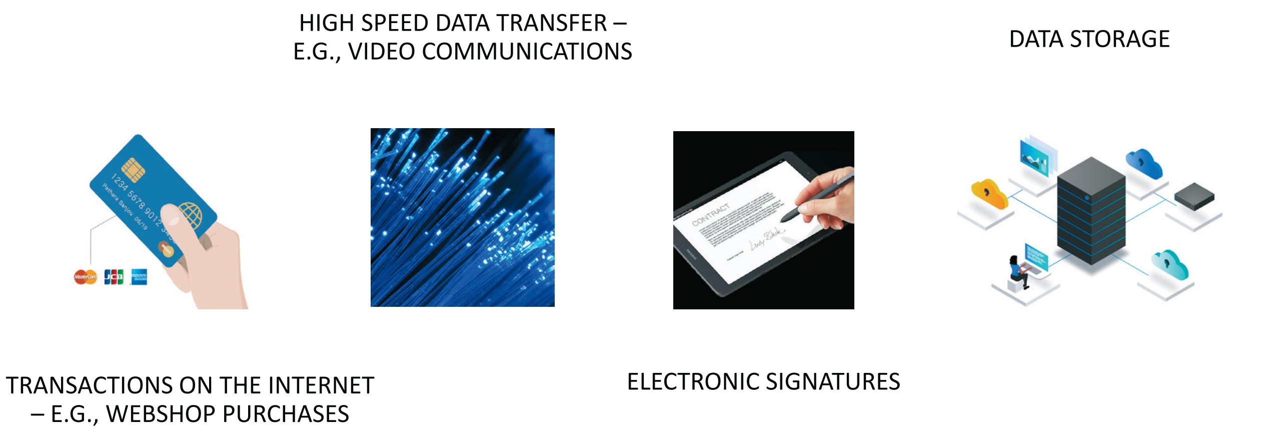
HIGH SPEED DATA TRANSFER – E.G., VIDEO COMMUNICATIONS
DATA STORAGE
TRANSACTIONS ON THE INTERNET – E.G., WEBSHOP PURCHASES
ELECTRONIC SIGNATURES

Figure 1 Danish society is highly digitized. Cybersecurity is established by means of various cryptographic schemes.

PKC (which is also referred to as asymmetric key cryptography) was originally developed in the 1970s, and is often synonymous with RSA, the first public key cryptosystem to be made public. It resolved a major roadblock to the widespread deployment of cryptography in general: key exchange. It does so by using a public (shared) key for the encryption of messages and a private (secret) key for the decryption of messages. It was discovered that it was possible to do so in a very secure manner by leveraging the computational difficulty involved in solving a certain class of mathematical problems known as one-way functions. As an example, it is easy to multiply two very large prime numbers, but it is very difficult to derive the prime factors from the product. The vast majority of the public key cryptography systems deployed today, including RSA’s successor, elliptic curve cryptography (ECC), are based upon this principle of one-way functions.

During the past 5 decades or so, the technology has undergone relatively little change, with major updates requiring only an increase in key length and, more recently, the introduction of the new variant, ECC, with a significantly reduced key length due to the increased effectiveness of the one-way function employed. The most widely used cryptosystems are RSA and ECC. RSA typically employs key lengths of 2,048-4,096 bits whereas ECC typically employs key lengths of 256 bits for the same level of security.

However, while the mathematical problems upon which the security of public key cryptography are predicated are computationally challenging for classical computers, it has been known since 1994 that this is *not* the case for adequately sized quantum computers. Current estimates[6] show that breaking RSA-2048 in 10-20 minutes (depending on the error rate) requires ~8,000 logical qubits. Current estimates indicate that approximately 1,000 physical qubits are required for each logical qubit. Consequently, a quantum computer with ~8 M physical qubits ought to be able to break RSA-2048 in the space of 10-20 minutes. The quantum computer with the greatest number of qubits currently on the horizon is IBM’s Condor with 1,121 physical qubits, and which is expected to become available by the end of 2023.

At this point, it is important to emphasise that this susceptibility only applies for *asymmetric* encryption: symmetric encryption is *not* as susceptible to the Quantum Threat to the same extent. As an example, the widely used symmetric encryption scheme, AES,

[6] https://globalriskinstitute.org/wp-content/uploads/2021/03/2021-03-MOSCA-Quantum-Risk-February-Report-V2.pdf

is assumed to be safe from the Quantum Threat if the key length is 256 bits or greater[7] By way of comparison with the estimates above for RSA-2048, it is currently estimated that breaking AES-256 will require a quantum computer with a logical qubit count of approximately 60,000[8]. However, when using a symmetric encryption scheme, one needs to find a secure way of exchanging the symmetric key. We will see later on in this report that quantum-technology can also facilitate this.

What is the nature of the threat?

Peter Shor published the quantum algorithm that now bears his name in 1994[9]. He showed how an adequately dimensioned quantum computer running his algorithm would be easily able to crack the most common forms of public key cryptography by virtue of its ability to factor integers many, many orders of magnitude faster than a classical computer. In other words, a sufficiently powerful quantum computer running this algorithm would be able to factor these integer numbers in a matter of seconds, minutes, or hours, as opposed to millions of years on the most powerful classical computer. This applies for both RSA and its successor, ECC. Increasing the key length is no longer a viable option to ensure an adequate level of security. Even if the key length were increased substantially, i.e. by an order of magnitude or more, quantum computers would *still* be able to perform the factorization within the same (reasonable) timeframes because of the vastly superior scaling characteristics of Shor's Algorithm.

When will the threat materialize?

Any discussion of *when* the Quantum Threat will occur may be illustrated using the so-called *Mosca's Inequality*[10]. This can be expressed (in a slightly modified form compared to the original version) as:

IF X + Y > Z, THEN "You are at Risk!"

where:

X is the amount of time (calendar time) required to *fully* deploy a quantum-safe (i.e. resistant to quantum computers running Shor's Algorithm) cryptographic solution in one's networks: note that this assumes that one starts today, i.e. no delays.

Y is the shelf life of one's data: in other words, for how many years must the encrypted information be kept secret?

Z is the number of years until the Quantum Threat manifests itself as a quantum computer capable of running Shor's Algorithm and hacking the vast majority of the public-key encryption schemes being used today. Z is often synonymous with Y2Q (Years to Q).

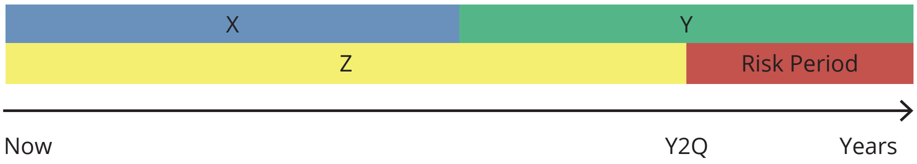

Figure 2 Visual representation of Mosca's Inequality.

[7] https://globalriskinstitute.org/wp-content/uploads/2021/03/2021-03-MOSCA-Quantum-Risk-February-Report-V2.pdf
[8] https://globalriskinstitute.org/wp-content/uploads/2021/03/2021-03-MOSCA-Quantum-Risk-February-Report-V2.pdf
[9] https://en.wikipedia.org/wiki/Shor's_algorithm
[10] https://csrc.nist.gov/csrc/media/events/workshop-on-cybersecurity-in-a-post-quantum-world/documents/presentations/session8-mosca-michele.pdf

The reason why the values for **X** and **Y** are added together is quite simple. Although one's data is protected from the Quantum Threat as soon as a quantum-safe cryptographic solution is fully deployed, there is still the shelf lifetime of the data that was *not* protected to consider because of Harvest Now – Decrypt Later hacking strategies.

It therefore follows that *if* **X + Y** *IS* greater than **Z**, (the number of years until the Quantum Threat manifests itself) then one will be at risk to an extent that is roughly proportional to the *remaining* shelf-life of any unprotected data.

However, unlike the value for **Z**, the values for **X** and **Y** will vary from industry to industry and application to application. The value of **X** will vary depending on the nature and complexity of one's network and the extent to which any modifications and/or enhancements need to be made to the infrastructure in order to implement PQC. By the same token, some values of **Y** are measured in decades while others are measured in days or less.

While the value of **X** can also be estimated to lie within a given interval with some degree of confidence for a given network configuration and complexity, and while it is also relatively easy to estimate the value of **Y** for a given type of data and application, estimating the value for **Z** is intrinsically more speculative.

One of the most comprehensive and authoritative estimates of Y2Q (i.e., **Z**) can be found in the Quantum Threat Timeline Report 2021[11]. The analysis is very detailed and nuanced and captures the opinions of 47 internationally leading experts on quantum computing.

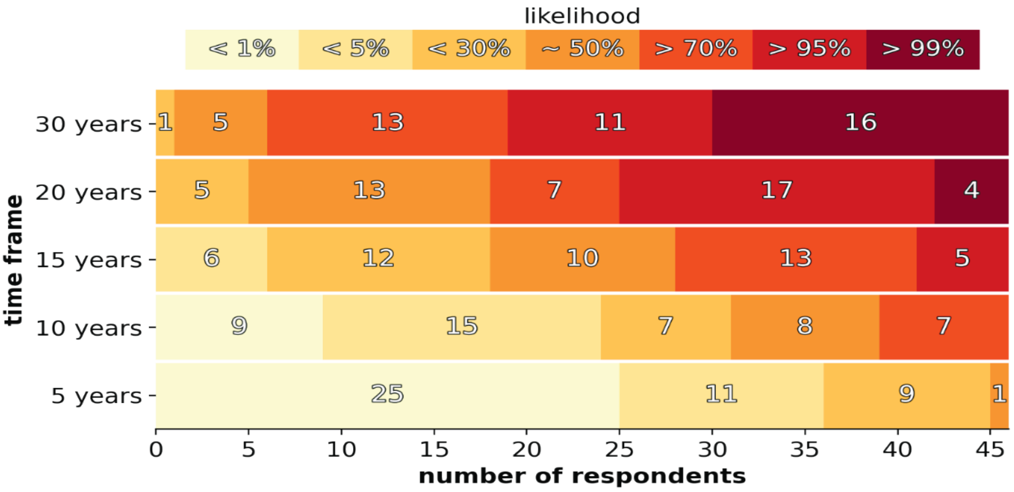

Figure 3 Experts' estimates of likelihood of a quantum computer able to break RSA-2048 in 24 hours.

The report shows that approximately 33% of the quantum computing experts estimated that the probability that a quantum computer capable of breaking RSA-2048 in 24 hours would be available in 10 years was at least of the order of 50% or greater. In addition, 61% believed that this would be the case in 15 years. By way of comparison, the corresponding numbers the year before (2020) were 25% and just over 50%, respectively. Thus, there is a growing perception among quantum computing experts that the threat of quantum computers is getting closer. This means that companies and public institutions need to escalate their perception of the threat from being a known issue that only requires monitoring to an issue that requires active planning and action.

[11] https://globalriskinstitute.org/publications/2021-quantum-threat-timeline-report/

COUNTERMEASURES

Perhaps the most obvious countermeasure for Public Key Cryptography (PKC) is to develop a new type of PKC based on hard mathematical problems that are resistant to attacks by quantum computers using Shor's Algorithm *as well as* classical hacks. This approach is often referred to as "Post-Quantum Cryptography" (PQC).

On the face of it, a mathematics-based solution such as PQC is attractive for a variety of reasons, primarily because it may be implemented purely in software but also because it falls within the same paradigm of leveraging the computational difficulty involved in solving mathematical problems, now just expanded to *also* encompass Shor's Algorithm (or any other known similar algorithm). However, as NIST has noted[12], the transition from ECC to PQC is considerably more complicated and uncertain compared to the transition from RSA to ECC, bearing in mind the increased proliferation of – and dependence upon - digital networks in today's society. Even in this scenario, there is still the risk that a new algorithm that can solve the underlying mathematical problem in a much simpler way is discovered. Should this happen, the encryption can be broken, and data will once again become vulnerable.

For this reason, Quantum Key Distribution (QKD), a physics-based solution to generate and distribute secret shared keys in a manner that *guarantees* channel security (according to the laws of quantum mechanics) against all conceivable classical and quantum computer-based hacks, is often proposed as an alternative solution to the Quantum Threat. However, unlike PQC, which is a "full-package" cryptographic solution, QKD only performs key generation and distribution. In addition, there are currently certain limitations associated with QKD, which restrict the general applicability and suitability of the solution.

We will consider each of the two countermeasures in turn before discussing their relative merits.

PQC – Post Quantum Cryptography

Background

Even though Shor's Algorithm was published as early as 1994, there was initially no immediate sense of urgency to develop quantum-safe cryptography for many years, not least because of the relatively immature level of quantum computing hardware at that time.

The first PQCrypto conference, held in 2006, is generally recognized as the start of a more concerted effort within the field of post quantum cryptography. But it was only approximately a decade later, around 2015, that companies such as IBM, Microsoft and others started investing more heavily (and openly) in the development of quantum computers and that venture capitalists started to get interested in quantum technology in general. It was also around that time the Quantum Threat morphed from being an interesting theoretical concept to a tangible threat. At this point in time, it became more a question of *when* a cryptographically relevant quantum computer, i.e., a quantum computer that would be able to break PKC, would materialize rather than *if* it would.

NIST PQC standards process and competition

At PQCrypto 2016, NIST[13] announced the PQC standards competition. In the NIST PQC Call for Proposals, the rationale for the call is clearly addressed in the second line: "If large-scale quantum computers are ever built, they will compromise the security of many commonly used cryptographic algorithms."

NIST then spells out the consequences in the subsequent paragraph: "In particular, quantum computers would completely break many public-key cryptosystems, including RSA, DSA (Digital Signature Algorithm), and elliptic curve cryptosystems (ECC). These cryptosystems are used to implement digital signatures and key establishment and play a crucial role in ensuring the confidentiality and authenticity of communications on the Internet and other networks."

[12] https://csrc.nist.gov/News/2022/pqc-candidates-to-be-standardized-and-round-4

[13] NIST is the US Agency: National Institute of Standards and Technology

At the same time, NIST is very much aware that PQC is an emerging field and that many types of PQC proposals exist, some of which will require additional research and development to improve confidence in the level of security provided and, not least, the level of performance. NIST is also aware that factors such as simplicity, flexibility and ease-of-adoption are of importance for successful deployment and had also included them in their selection criteria.

NIST began the selection process with 69 candidate algorithms and recently (July 5th, 2022)[14] announced the selection of one PQC algorithm for public-key encryption and key establishment (KE) and 3 PQC algorithms for digital signatures (DS) for standardization. At the same time, it also announced that 4 of the PQC algorithms for public-key encryption and key establishment still in contention would advance to Round 4 of the selection process.

It is *anticipated* that the standardization of the selected algorithms will be completed by the beginning of 2024. In any event, there is a general expectation that the announcement will be an inflection point and will galvanize both renewed and more focused activity within the space. It is certainly not coincidental that the "Quantum Computing Cybersecurity Preparedness Act" is currently making its way through the US congress: it was passed in the US House of Representatives in July of 2022 and is on its way to the US Senate. It will mandate PQC for all US government agencies and it requires that US industry also complies as part of a national economic security initiative. In Denmark, we have yet to see such initiatives.

Pros and cons of PQC

Security vis-à-vis performance

The complexity of some PQC algorithms means that there may be a trade-off between the desired level of security and the desired level of performance. However, this issue may be dealt with by only using PQC for the initial exchange of symmetric keys; encryption and decryption of the data will be done using symmetric cryptography, e.g., AES-256, which we can reasonably assume to be quantum-safe. This is what some systems already do today by "just" replacing RSA or ECC with a different algorithm. In other words, data transport rates are not going to be lower because of PQC.

Ease-of-adoption

The replacement of RSA by ECC has proved to be non-trivial, particularly if one is looking at entire business sectors (for example, the banking or health care sectors) rather than a single company. Implementing PQC is expected to be somewhat more complicated and NIST is very much aware of this. NIST released a white paper[15] in 2021 highlighting these issues where they write: "[the transition] is likely to be more problematic than the introduction of new classical cryptographic algorithms" and "performance and scalability issues may demand significant modifications to protocols and infrastructures."

Specific implementation strategies

Hybrid approach

A hybrid approach, combining the use of both classical PKC and PQC on the same data to improve the overall security during the PQC implementation phase, may be the most realistic first step even though it would entail additional resources compared to either classical PKC or PQC alone. This approach has already been successfully demonstrated in a test build of Google's Chrome web browser in 2016.

The main reason for using the hybrid approach is that it would ensure continued compliance with respect to any standards and regulations in place r*ight now*, an important consideration for those who are interested in deploying non-standardized PQC as soon as possible because of their risk profile.

[14] https://csrc.nist.gov/News/2022/pqc-candidates-to-be-standardized-and-round-4

[15] https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04282021.pdf

There is a growing consensus that a Hybrid Approach to PQC deployment may not just be a practical way to migrate to PQC; it may also be the most prudent way to do so given the non-negligible risk that even standardized PQC algorithms may prove to be vulnerable to new attack vectors earlier than anticipated.

In short, combining today's cryptographical solutions with PQC solutions in this manner will, where feasible, facilitate a smoother and safer transition to a post-quantum era.

Crypto agility

Crypto agility is defined as the ability of an information security system to switch between cryptographic primitives without any significant change to the system infrastructure. The switching takes place if the cryptosystem currently in use is compromised. The switch could be as simple as changing the key-length or, in a more complex situation, switching to a completely different cryptographic algorithm. This has always been a problem within the field of cybersecurity and will certainly also be a challenge for PQC.

The recent NIST PQC standardization process clearly illustrates that there is a risk that the new PQC algorithms may prove vulnerable to new forms of attack. Consequently, crypto agility should be an integral part of any cybersecurity strategy.

QKD – Quantum Key Distribution

Background

The idea of Quantum Key Distribution (QKD), a physics-based technique exploiting the laws of quantum mechanics to generate and distribute shared secret keys in an unconditionally secure manner, was first proposed in 1984, 10 years prior to Shor's Algorithm. The first QKD protocol, BB84, was proposed by Charles Bennett and Gilles Brassard that year and demonstrated at IBM Research some years later.

QKD involves encoding classical information into the quantum states of light, i.e. the polarization of single photons, the phase of weak pulses, or the phase and amplitude of continuous-wave coherent states of light. It is by virtue of the inherently probabilistic nature of measurements on these photonic quantum states that a secure encryption key can be generated and shared between the transmitting party (typically called Alice) and the receiving party (typically called Bob). By virtue of what is called the "no-cloning" theorem, it is impossible for an eavesdropper (typically called Eve) to hack the channel without altering the quantum states being transmitted and thereby alerting Alice and Bob to Eve's presence. A unique feature of QKD is that the protocol security can be guaranteed without any assumptions about Eve's resources, including computational power. This is what QKD can provide: 100% guaranteed channel security for shared secret key generation and distribution or, in more technical terms, "information theoretic security". The established shared keys can then be used as a resource for any classical symmetric encryption and decryption scheme such as an implementation of AES. QKD is intrinsically a point-to-point technology, but it has also been demonstrated in routed multi-user network topologies.

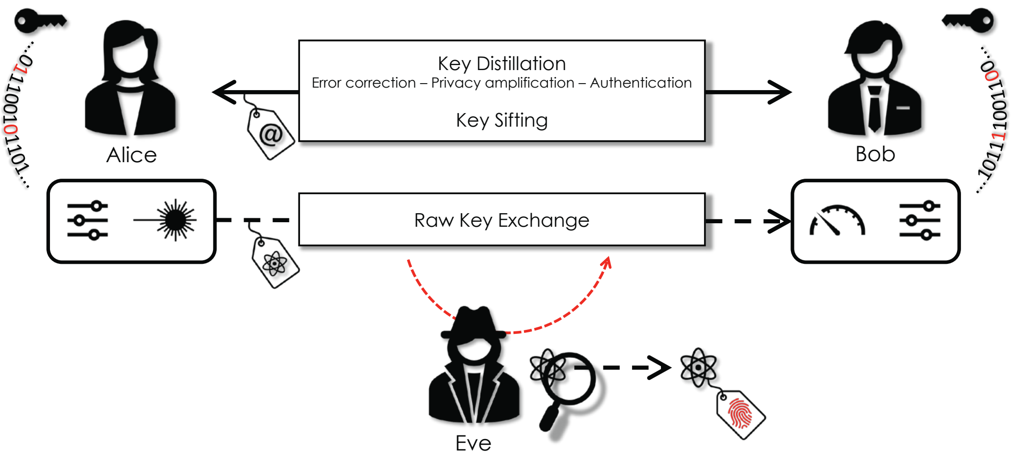

Figure 4 QKD enables two communicating parties, Alice and Bob, to establish a shared secret encryption key. Quantum physics guarantees that any attempt by an eavesdropper Eve to intercept the key exchange will inevitably leave a detectable 'fingerprint', thereby ensuring the privacy of the key. The protocol uses an optical quantum channel for the initial raw key exchange while an authenticated classical channel is required for subsequent post processing and distillation of the final key.

In addition to the quantum communication channel, QKD also requires an authenticated conventional communication channel. An authentication functionality, required for establishing the true identities of the communicating parties, is not supported by the QKD protocol itself. For this purpose, QKD must be supplemented by a classical cryptographic primitive such as 2-universal hashing, message authentication codes (MAC) or digital signatures. The initial authentication of the channel can also be realized by using a small amount of pre-shared random secret data. A portion of the generated key material can subsequently be used for session authentication.

An important feature of QKD is the long-term security the protocol provides. As stated in ETSI White Paper No.27 [16]: *"Another important consequence of QKD security, is the fact that it is "everlasting", in the sense that keys, established via QKD, cannot be broken retrospectively. In contrast this vulnerability is generic when one uses computational techniques. Interestingly, everlasting security of QKD holds even when the initial authentication relies on computational techniques so long as the authentication is not compromised during the key transfer itself. This offers a practical solution for the initial authentication of QKD devices in large-scale networks."*

Since the experimental demonstration of the first QKD protocol in 1989, many variations of the protocols and the physical realizations of the way the quantum states are prepared and measured have been implemented with a view to increasing performance and/or ability to withstand side-channel attacks on the QKD transmitters and receivers themselves, the Achilles heel of these systems. This is a very valid concern given that these parts of the QKD system, unlike the transmission channel, are generally *not* protected by the laws of quantum mechanics. Indeed, the susceptibility of the QKD transmitters and receivers to side-channel attacks is an ongoing point of discussion although substantial improvements have been made over the years. It should be noted that side-channel attacks are equally a concern for PQC.

These two arguments - the need to supplement QKD with (classical) authentication protocols and the susceptibility to side-channel attacks – are often raised by critics of QKD, many of them members of the mathematical cryptographic community. This also includes the US's National Security Agency (NSA) and the UK's Government Communications HQ (GCHQ) among others, even though both countries are also active in developing QKD test beds and performing field trials. Perhaps the most nuanced view can be found in the recent report (2022) – *Quantum-safe Cryptography* – from the German

[16] https://www.etsi.org/images/files/ETSIWhitePapers/etsi_wp27_qkd_imp_sec_FINAL.pdf

Federal Office for Information Security (BSI)[17]. Although the report clearly prioritized migration to PQC over QKD-based solutions, it also recommends continued research into *both* PQC and QKD, acknowledging the merits of both in the context of quantum-safe cryptography.

It should be noted, however, that fully secure, device-independent quantum key distribution protocols exist that close the potential loopholes associated with side-channel attacks. These protocols are significantly more demanding in terms of the specifications for the quantum hardware required to implement them in practice, and ought therefore be considered an active field of research. Nonetheless, detailed protocols exist for, by way of illustration, implementations based on high-efficiency and coherent single-photon sources, and prototype demonstrations could be within reach.

Commercialization of QKD

Notwithstanding the limitations and practical difficulties associated with implementing secure QKD systems, the first commercially available QKD systems appeared almost 20 years ago. The initially small niche market (first research networks and later government and military networks) has grown and expanded into other market segments (e.g. telecommunications and critical infrastructure) as the technology has matured and, not least, the prospect of the Quantum Threat has become more tangible.

In addition to ID Quantique, arguably the global pioneer in this field, and several recent start-ups, Toshiba Corporation also entered the QKD market in 2020. Toshiba continues to perform advanced R&D on next-generation products such as its "twin-field" QKD for extended reach and a QKD chipset (transmitter, receiver, and random number generator) which is expected to drive down costs substantially, thereby increasing the addressable market for QKD system solutions. Moreover, NEC recently (2022) sold their first QKD system to the Japanese Agency NICT[18], and continues to perform research into both fibre- and satellite-based QKD.

Seen from an EU and NATO perspective, there are currently no QKD products manufactured and accredited in an EU or a NATO country.

EU is in the process of establishing an EU-wide QKD-network: EuroQCI. The network will link the capitals of 22 EU member states (including Denmark) and will become operational in 2024. In addition, each country participating in EuroQCI will establish a national QKD infrastructure.

A Danish national proposal (QCI.DK) has also been submitted to the European quantum communication infrastructure (EuroQCI). In a concerted effort between Danish ministries, universities, and private companies, this project proposal aims to establish the first national quantum communication network deploying QKD in a metropolitan network between the participating public authorities as well as links for long distance communication. In the longer term, QCI.DK will also serve as a testbed for more advanced quantum communication protocols and allow companies to explore the applicability of QKD for their needs and requirements.

In April, 2022, British Telecom and Toshiba launched the world's first commercial service for quantum-secured communication based on QKD in a standard optical fiber network in London[19]. As the first commercial customer of the network, Ernst & Young will use the network to connect two of its London offices and explore how QKD-secured data transmission can benefit its customers.

Current Limitations of QKD

Quite apart from the susceptibility to side-channel attacks (in the current implementations) and the absence of a (quantum) protocol for authentication, there are several recognised limitations associated with the technology available to implement QKD solutions today. These limitations restrict, in each their own way, the extent to which QKD can practicably be deployed in global communications networks.

[17] https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Brochure/quantum-safe-cryptography.html?nn=433196

[18] National Institute of Information and Communications Technology

[19] https://newsroom.bt.com/bt-and-toshiba-install-uks-first-quantum-secure-industrial-network-between-key-uk-smart-production-facilities/

Cost

There seems to be general agreement among both end-users *and* suppliers that the biggest single barrier to greater adoption of QKD is the cost of the solution. In this regard, the recent entry of NEC and Toshiba into the QKD system market will undoubtedly generate increased competition between the existing QKD systems suppliers, leading to lower prices and/or increased performance. It is also conceivable that it could encourage other large corporations, with profiles and capabilities like those of NEC and Toshiba, to enter the QKD system market as well.

But this alone may not be sufficient. Ultimately, the key to widespread adoption of QKD capabilities through the reduction of costs is increased levels of integration. In the first instance with telecommunications equipment suppliers (and this is where the recent QKD standardization activities – particularly regarding interfaces - has greatly facilitated this effort) but the recent announcement of Toshiba's QKD chipset represents the next level in this progression[20].

Reach

One of the key technological challenges – and key constraint – for QKD is the distance limitation caused by attenuation of the photons as they propagate through a given transmission medium such as optical fibres or (free)-space. The problem is compounded by the fact that the optical signal cannot be amplified since this process would destroy the quantum states in which the information is encoded.

To overcome this limitation, a 'quantum repeater', that can transfer the quantum information encoded in the quantum state of the photons without violating the no-cloning theorem, is required. While a quantum repeater would greatly expand the addressable market for QKD, the consensus is that new scientific breakthroughs – in addition to resolving substantial engineering challenges – will probably be required, and that it could easily take a decade or more before quantum repeaters become commercially available. In the interim, it is likely that loss-robust encoding methods will be developed which, by encoding a single qubit non-locally in entangled multi-photon cluster states, will increase the transmission distance that can be achieved and thereby the reach of QKD systems.

Satellite-based solutions offer a relatively attractive and practical alternative to significantly increase the reach of QKD systems in the near-term. The experimental results achieved with the Chinese Micius satellite support this hypothesis as does the recent announcement of the European Commission's Quantum Communication Infrastructure (EuroQCI) initiative in the EU. China has further consolidated its leadership in satellite-based implementation of quantum communication with the launch of the second quantum satellite, Mozi, in July 2022[21] and we note that both the UK and Germany also have initiatives in this area[22] [23].

While trusted (terrestrial) nodes may be acceptable for certain users for certain applications, where measures can be taken to physically secure the nodes to an acceptable level, it will not be suitable or practicable for all. It is not a "quantum native" solution for long-distance QKD applications but a workaround until satellite-based solutions are in place and, ultimately, a viable quantum repeater solution is available.

Speed (key exchange rate)

Relatively low key exchange rates is another barrier to the widespread adoption of QKD solutions in a market in which cost and distance are generally perceived to be the biggest barriers to accelerated QKD penetration.

[20] https://news.toshiba.com/press-releases/press-release-details/2021/Toshiba-Shrinks-Quantum-Key-Distribution-Technology-to-a-Semiconductor-Chip/default.aspx

[21] https://news.satnews.com/2022/07/31/china-launches-new-satellite-in-important-step-towards-global-quantum-communications-network/

[22] https://www.quantumcommshub.net/industry-government-media/collaboration-opportunities/2253-2/partnership-resource/cubesat-qkd-and-groundstations/

[23] https://www.dlr.de/kn/en/desktopdefault.aspx/tabid-17795/#gallery/36425

The vast majority of the commercially available QKD systems today are based on an attenuated laser source. Strong attenuation of the light from the laser source ensures that a large proportion of the laser pulses in the QKD system will only contain one photon and thereby make the system correspondingly much less susceptible to photon-splitting attacks. However, strong attenuation of the light from the laser source also means that a large proportion of the laser pulses will have zero photons, i.e. no pulse, thereby reducing the *effective* transmission rate of single photon laser pulses. Reduced laser pulse rates translate directly into reduced key exchange rates.

Despite this, key exchange rates of the order of kbit/s to Mbit/s can be reliably achieved with these systems over distances of the order of 50 km or so (intra-metropolitan distances) depending on the specific system configuration and infrastructure used.

However, high speed, single-photon sources, some with the ability to potentially support key exchange rates of the order of 10's to 100's of Mbit/s, are beginning to become commercially available. Unlike earlier single-photon sources based on spontaneous parametric down conversion, the new single-photon sources are based on solid-state quantum dots and are "on-demand". While the single-photon emission rates are impressive, cryogenic cooling is typically required. Operation at telecommunication wavelengths, a requirement for optical fibre-based applications, is currently at the research stage.

Alternatively, continuous variable variants of QKD have also been developed. In this case, the information is encoded into the quadratures of a coherent light field using standard telecom lasers and modulation techniques. While key exchange rates of the order of Mbit/s have been demonstrated for such systems, they are more prone to optical losses, reducing the reach of these systems.

QKD field-trials and use-cases

- In 2021, QKD was successfully demonstrated in a field-trial in Padua, Italy, over a deployed metropolitan network[24]. For the trial, a low-cost polarization-based implementation of the BB84 protocol was used.
- In January, 2021, a demonstration of QKD for the secure transmission of medical data via data centers was performed between two hospitals in Graz, Austria[25].

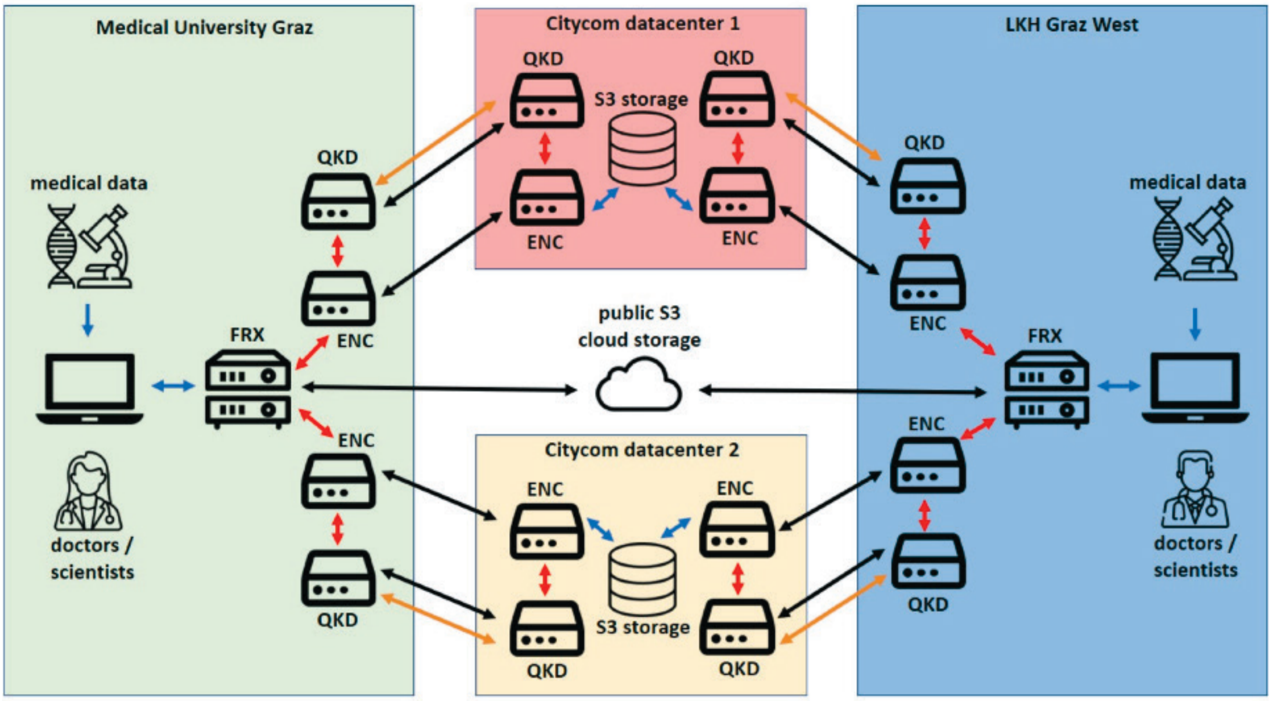

Figure 5 Schematic overview of the Graz QKD use-case. Source: https://openqkd.eu/use_case/its-securing-sensitive-medical-data-at-rest-and-in-transit-use-case-21/#

[24] https://quantumfuture.dei.unipd.it/confandevents/events/field-trial
[25] https://www.insidequantumtechnology.com/news-archive/medical-data-successfully-protected-by-quantum-cryptography-in-graz/

- In August 2021, Danish researchers participated in the first public demonstration of an intergovernmental demonstration of quantum communication between Italy, Slovenia, and Croatia[26].
- In February 2022, quantum-secured data transfer was implemented internally at Danske Bank, constituting the first Danish field demonstration of QKD[27].

PQC *vs.* QKD or PQC *and* QKD?

If a practical countermeasure to the Quantum Threat is to be:

- widely deployable in communications and data networks, *including* mobile networks,
- implementable at a cost commensurate with the level of security provided, and
- deployable in a relevant timeframe with respect to the expected timeframe of the Quantum Threat then PQC will be the preferred choice.

Whether or not QKD can already provide a viable, practical countermeasure to the Quantum Threat today largely depends on the use-case in question. Large-scale deployment would require significant reductions in cost combined with considerably improved reach and key exchange rate performance. However, in certain cases the high level and long-term perspective of the security provided by QKD may well prove to be more important than price and speed. In addition, if only point-to-point links or communication in static, pre-defined networks is required, the matter of establishing authenticated conventional channels will not be a constraining factor.

In view of the obvious benefits of both PQC and QKD, it therefore makes sense to continue R&D activities in both areas to strengthen countermeasures to the Quantum Threat in both the short-term *and* the long-term.

However, it also makes sense to combine PQC *and* QKD now as part of a "Defence-in-Depth" cybersecurity strategy in those instances where it is advantageous to do so. There is a growing consensus that no single cryptographical method will be sufficient to stave off all conceivable cyberattacks. Combining PQC Digital Signatures for authentication with QKD for key creation and key distribution, particularly in instances where additional protection of the physical layer is desirable, leverages the capabilities of both. By taking a hybrid approach, PQC could also be combined with existing cryptographic systems, such as RSA and ECC, to provide additional protection.

At this point in time, this approach is only recommended for highly confidential information since the cost and effort will be quite substantial. However, continued commercialisation of these technologies will, over time, drive down costs and make the approach viable for a growing number of use cases.

Recommendations for the transition to quantum-safe cryptography

Industry relevance

McKinsey[28] recently performed an industry-focused assessment of vulnerability to the cybersecurity threat posed by quantum-computers. By comparing data shelf life with typical system life cycles, the report concludes that the threats are especially critical within the Public Sector, Banking, and Insurance. This is because in these sectors, data shelf life is typically quite long and systems are typically in place for many years. In other industry sectors, this may also be the case for specific units such as the legal department (legal documents, procurement contracts, etc.).

As part of our research, we have asked CISOs (Chief Information Security Officers) at some of the leading Danish companies what their approach is to the threat from quan-

[26] https://www.units.it/en/news/first-intergovernmental-quantum-communication

[27] https://via.ritzau.dk/pressemeddelelse/nordens-forste-kvantesikre-dataoverforsel-gennemfort-i-danske-bank?publisherId=13560560&releaseId=13643861

[28] Source: McKinsey, May 2022 https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/when-and-how-to-prepare-for-post-quantum-cryptography

tum computers. The interviews revealed that while several CISOs had a basic awareness of the threat, none of them had considered or initiated specific activities to mitigate the risks. This clearly indicates that there is an urgent need to create more awareness of the quantum threat right now since the necessary actions need to be taken well in advance. These actions include:

- Mitigation of the risk for workloads with long data shelf life that may be harvested now and compromised later (when a sufficiently powerful quantum computer exists)
- Preparation for crypto agility. Ensuring that new cryptography systems support the substitution of cryptographic primitives, thereby facilitating the introduction of PQC algorithms.

Fortunately, there are several high-risk areas where solutions are currently being investigated:

Use case	Current actions
Communication between government agencies	Investigating and piloting a QKD-based solution as part of the EU-funded QCI.DK project
SCADA systems controlling the power distribution infrastructure	DTU Physics leads the CryptQ project (supported by Innovation Fund Denmark) with participation from Danske Bank and EnergiNet. CryptQ pilots QKD within critical infrastructure and banking
Exchange of stock exchange transaction data	

The Danish start-up company, Sparrow Quantum, has commercialised on-demand single-photon sources based on quantum dots. The first QKD field-trial using the company's technology was recently completed, clearly showing that the technology can be deployed in the field even if the solution is currently still expensive. The field-trial was part of the FIRE-Q project supported by Innovation Fund Denmark. The deterministic single-photon approach could potentially be upgraded further to realize full device independence, loss-tolerant encoding, and ultimately a one-way quantum repeater.

Transition to quantum-safe cryptography

Based on the recommendations[29] from the European Telecommunications Standards Institute (ETSI), we recommend the following approach for a migration strategy for companies and institutions.

Get an overview

Compile an inventory that captures the entities and functions that deliver cryptographic protection and that will potentially be subject to migration. This is an area that historically has not been tracked. The inventory should also quantify the level of risk by using, for example, the following format[30]:

Security Level	How is the data/information classified?
Business Criticality Level	What business risks will data/information disclosure or compromise (loss of data integrity) create?
Duration	How long has confidentiality to be maintained for each asset?
Scope	Are keys or certificates issued to third parties?
Damage	Can damage due to degradation or interruption of services be quantified?
Response	Is there a plan to protect the encrypted asset in case of a crypto failure?
Transition time	Transition time to quantum-safe cryptography (X in Figure 2)

This overview enables the organisation to assess the overall risk of the threat from quantum computers and to then decide how to prioritize, lead and fund its mitigation.

[29] https://www.etsi.org/deliver/etsi_tr/103600_103699/103619/01.01.01_60/tr_103619v010101p.pdf (ETSI)

[30] https://www.etsi.org/deliver/etsi_tr/103600_103699/103619/01.01.01_60/tr_103619v010101p.pdf (ETSI) p. 17

Create a migration plan

The next steps, based on the generated overview, are to identify the most suitable quantum-safe solution that is available, create awareness about it in the organisation, and establish a migration plan. When creating the plan, it is important to follow the two implementation strategies described in the PQC chapter of this report:

- Focus on a *hybrid approach*, combining classical algorithms (such as RSA and ECC) that have stood the test of time with the most promising quantum-resistant solutions
- Focus on *crypto-agility*, the ability to switch cryptographic primitives in and out without any significant changes to the system infrastructure

Even if no immediate action is taken, these implementation strategies should be taken into consideration going forward when making any decisions within the cybersecurity area.

The migration plan should include all assets in the inventory and specify, for each asset:

- Whether the asset will be migrated
- When the asset will be migrated and the orderly sequence of interdependent assets
- The migration solution chosen for each asset, duly considering a hybrid approach

Migration execution

When the migration plan has been validated, approved, properly organized and funded, the next step is execution. A key element in this phase is to conduct exercises to simulate and test the migrations; the objective here is to determine the viability of the plan. Such exercises may also uncover missing inventory elements or flaws in the migration plan.

An example of a migration timeline was made public by the NSA when they announced the so-called Commercial National Security Algorithm Suite 2.0[31] in September, 2022, (see figure below).

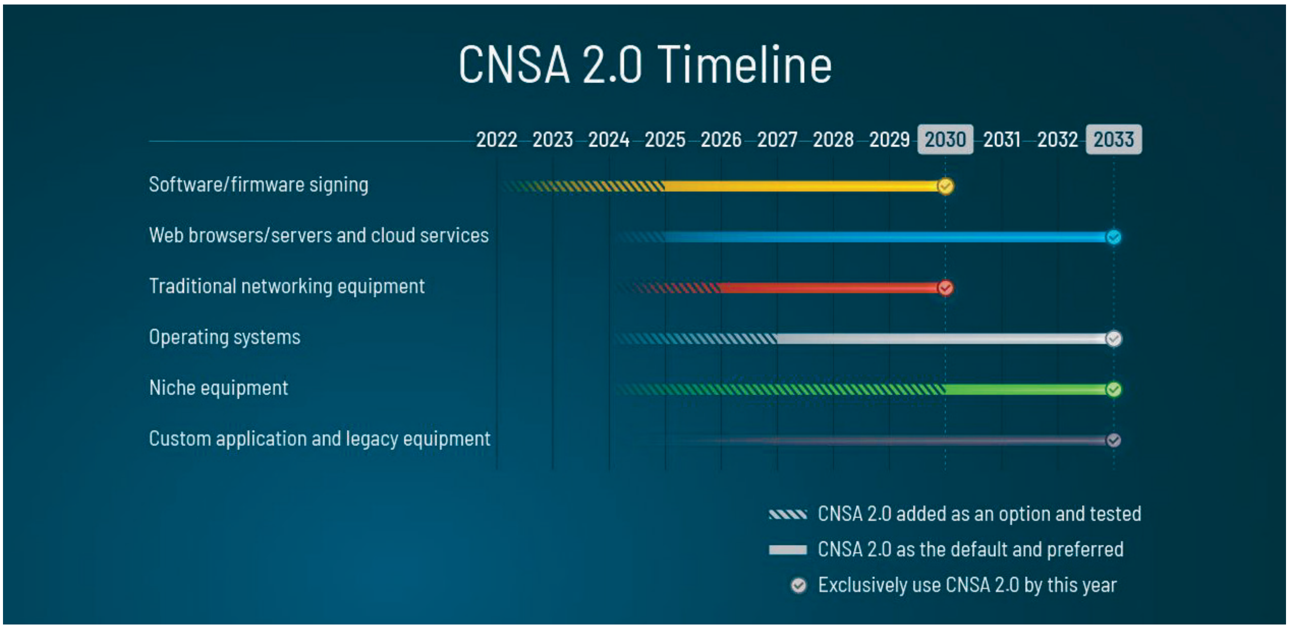

Figure 6 Transition timeline for various network components.

[31] https://media.defense.gov/2022/Sep/07/2003071834/-1/-1/0/CSA_CNSA_2.0_ALGORITHMS_.PDF

Recommendations

- Organizations need to start planning the transition to quantum-safe cryptography now and they also need to establish the necessary internal awareness
- Start by getting an overview of the risk for your organization by creating an inventory as described above
- Focus on crypto-agility and the ability to implement hybrid approaches in cybersecurity decisions going forward
- Start getting more insight and experience with both PQC and QKD
  - PQC seems to be the preferred solution in the short term.
  - PQC standards are expected to become available by 2024. Draft standards are available now.
  - QKD has the potential to provide unbreakable encryption, but this technology is not yet mature enough for network-wide deployment. More research is required in this field.
  - Combining QKD and PQC can be employed for ultra-secure point-to-point communications

DANISH POSITIONS OF STRENGTH

The threat from quantum computers is an issue that needs to be taken seriously by all organisations in Denmark, especially those working with data with a long shelf life. On the other hand, this threat can also be seen as an opportunity to leverage Denmark's strengths within the field of quantum-safe cryptography. In this chapter, we will provide an overview of these strengths.

Research groups

Denmark has several world class research groups within cryptology and quantum communications

Department	Contact	Area of expertise
Computer Science, AU	Professor Ivan B. Damgaard	Cryptology, cryptographic protocols, public key encryption, quantum computing, Quantum-safe cryptology
DTU Compute	Assist. Prof. Christian Majenz	Quantum-safe cryptology
DTU Electro	Professor Leif Oxenløwe	Quantum communications with emphasis on discrete-variable QKD (DV-QKD)
DTU Physics	Professor Ulrik L. Andersen	Quantum communications with emphasis on continuous-variable QKD (CV-QKD) and quantum random number generation (QRNG). Optical quantum computing
Niels Bohr Institute, KU	Professor Peter Lodahl	Single photon sources for quantum computing and DV-QKD Optical quantum computing
Department of Mathematical Sciences, KU	Professor Matthias Christandl	Quantum information theory, quantum cryptography, fault-tolerance, quantum repeaters, algorithms, and complexity.

Current and recent research

Recent and current Danish projects within Quantum Communications:

National Innovation projects:

- Innovation Fund Denmark's (IFD) largest single investment to date has been in Qubiz: Quantum Innovation Centre, where academic and industrial partners collaborated to promote applied scientific research within many fields of quantum technology (2016-19).
- In 2020, IFD invested in two academic-industry consortia developing technology for secure quantum communications: FIRE-Q[32] and CryptQ[33].
- In 2022, IFD invested in the QuantERA project CVSTAR[34] with DTU Physics and TDC NET A/S as Danish partners.
- In 2022, IFD invested in photonic quantum computing though the project PhotoQ[35]
- Qrypton – a Danish Defence funded project with Cryptomathic, NBI and Sparrow Quantum as partners.

National research projects:

- The Danish National Research Foundation has invested in several Centres of Excellence conducting research in the fields of quantum communication and cryptography. These include SPOC (Silicon Photonics for Optical Communications), bigQ (Center for Maroscopic Quantum States), and Hy-Q (Center for Hybrid Quantum Networks).

[32] https://nbi.ku.dk/english/industrial-collaboration-at-nbi/cases/fire-q-field-ready-single-photon-quantum-technology/
[33] https://cryptq.dtu.dk
[34] https://quantera.eu/cvstar/
[35] https://innovationsfonden.dk/da/nyhed/fotonisk-kvantecomputer-skal-give-dansk

- Both the Independent Research Fund Denmark and the Carlsberg Foundation invested in research into continuous-variable QKD in 2021 and 2022, respectively.

EU projects:

- Danish research institutions participate in multiple EU Quantum Flagship projects (Uniqorn, CiViQ, and QIA) and OpenQKD.
- Denmark participates in the European Quantum Communication Infrastructure (EuroQCI)[36] under the auspices of the EU Digital Europe Programme.

Industry

A growing number of small and medium-sized Danish companies are already working with quantum-safe cryptography (see table below).

Name	Description	Quantum-safe Cryptography
Alea Quantum Technologies ApS, Kgs. Lyngby	Building high-speed quantum random number generators. The technology has been developed by DTU Physics	Builds high-speed quantum random number generators that may be used for creating truly random keys for encryption purposes.
Cryptomathic A/S, Aarhus	Specializing in cryptography for e-commerce security systems. The company develops Security Software Solutions and Key Management Systems for the financial and governmental industries.	Security Software Systems and Key management systems. Key Management covers all mechanisms pertaining to keys, expiration, use etc. and not least key distribution, and thus accounts for the amalgamation of classical encryption algorithms and new protocols for key distribution, be it QKD or PQC.
Dencrypt A/S, Hvidovre	Specializing in so-called dynamic encryption technology for mobile devices.	AES-256 NATO approved Common Criteria Certified (ISO)
SiPhotonic ApS, Kgs. Lyngby	Design and fabrication services for advanced silicon photonic integrated circuits (PICs).	Integrated optical circuits for QKD
Sparrow Quantum, Copenhagen	Designing, developing, and manufacturing deterministic single-photon sources.	Single-photon sources for QKD
Zybersafe A/S, Taastrup	Designing, developing, and manufacturing hardware encryption systems.	AES-256 symmetric encryption

Conclusion

Denmark possesses a strong research community with several world-class research centres specializing in quantum-safe cryptography. We also have a growing number of SMEs working in this sector as well.

Public sector funding, however, still lags considerably behind that of countries we typically compare ourselves to in this field. In April 2021, the Quantum Delta NL foundation in the Netherlands received 615 M€ in grants from the National Dutch Growth Fund[37] for applied research and development of quantum technologies, including quantum-safe cryptography. Denmark also needs to take actions of this kind to bring its strengths in research into play. In the next chapter we will propose a number of such actions.

[36] https://digital-strategy.ec.europa.eu/en/policies/european-quantum-communication-infrastructure-euroqci
[37] https://quantumdelta.nl/general-overview-and-documents/

OPPORTUNITIES

We expect that investment in quantum communication networks and related cybersecurity solutions will grow as the next generation of quantum technologies emerge and as more organizations become aware of the threat from Quantum Computers.

The market potential is huge if Denmark can successfully transform its research strengths in quantum technology and cryptography into commercial products and solutions. As an example, if Denmark were to successfully commercialise technologies that capture 5% of the estimated global market for quantum-enhanced cybersecurity solutions and network technologies by 2040, it would generate $820 million in revenue and 3,300 new direct jobs[38].

Quite apart from the security issue, long-range quantum communication via a *quantum internet* will lead to a plethora of new opportunities in quantum technology. These include secure cloud quantum computing, parallelized quantum computing, and quantum sensing.

Next steps

For Denmark to take advantage of these opportunities within quantum-related cybersecurity, all stakeholders need to act in a coordinated manner. Key actions include:

- Establishing a strategy. The Danish Ministry of Industry, Business and Financial Affairs is currently heading up the development of a National Quantum Plan Of Action. We propose that an important part of the strategy should be focused on growing the domestic cybersecurity industry, leveraging our research excellence in both cryptography and quantum technology.
- To continue allocating public and private funds to facilitate the transition of quantum-safe cryptography from the research sector into the commercial sector.
- Leverage the NATO DIANA Center for Quantum Technologies in Copenhagen to drive innovation in quantum-safe cryptography and quantum communications.
- Industry end-users should take part in early demonstrations and the adoption of quantum cyber technologies, including research projects, to support their commercialisation

Specific cross-stakeholder initiatives could be to:

- Establish a centre of excellence for quantum-related cybersecurity
- Establish specific, targeted calls for proposals or competitions pertaining to quantum-related cybersecurity. This includes increasing awareness of and participation in EU-funded initiatives such as OpenQKD[39] and EuroQCI.
- Enable and support QCI.DK (see the QKD section) in serving as a testbed for more advanced quantum communication protocols and for companies to explore the applicability of QKD to their needs and requirements.
- Invest in R&D for advanced, long-term quantum communication technologies directed towards realizing the quantum internet
- Provide a combination of government investment and venture capital for start-ups

[38] Using the numbers from Growing Australia's Quantum Technology Industry, Australia's National Science Agency p. 33 https://www.csiro.au/en/work-with-us/services/consultancy-strategic-advice-services/csiro-futures/future-industries/quantum

[39] OpenQKD brings together 13 EU-countries to develop secure applications of quantum communication that can be applied in multiple sectors in society. It acts as a testbed for technologies that will be used to build a EU-wide cybersecure Quantum Communication Infrastructure (QCI). https://openqkd.eu/

Areas of potential research

We propose that the following research topics be considered:

Topic	Description
Measurement device independent QKD	Avoids side channel attacks on the detector (receiver) side and increases the reach compared to traditional QKD
Device independent QKD	Avoids side channel attacks on both the transmitter and receiver sides
QKD in telecom networks	Co-existence of QKD with traditional telecom traffic
Better and more efficient postquantum signatures	Currently QKD has no protocol for signatures. For this and many other applications, we need more efficient post quantum signatures based on diverse computational problems.
More efficient postquantum secure zero-knowledge proofs	We have very efficient tools for privacy preserving identity management on the internet, which is becoming vitally important, in part because of the growth in the blockchain sector. However, postquantum secure tools lack far behind, and this needs to be addressed.
Use-case demonstrations of QKD	Demonstrations of use-cases benefiting from security offered by QKD and being able to cope with the distance limitations.
Quantum repeaters	Extends the reach of quantum communications systems incl. QKD
Hybrid encryption schemes	Combinations of PQC and QKD protocols

Summary and conclusions

Quantum computers may well be able to break widely used public-key-cryptography schemes such as RSA and ECC within the next one to two decades. This makes information with a long shelf life vulnerable to being exposed and misused. The threat is already present today, as information can be tapped and stored now for exposure at a later date.

Public institutions and private companies need to assess the threat now and to prepare mitigating actions. This includes preparing for transitioning from the well-known RSA and ECC protocols to quantum-safe cryptography. Because PQC-protocols are relatively immature, they may be broken, and the user must be crypto agile and able to quickly switch to another protocol. Unfortunately, although no cost-effective and commercially available solutions are fully standardized yet, the first standardized solutions are expected to become available in late 2023 or early 2024.

Mitigating the quantum threat is an opportunity for Denmark to profit from its strengths within cryptography and quantum technologies. However, it requires additional public funding along with incentives for private companies and venture capitalists to invest more into this field.