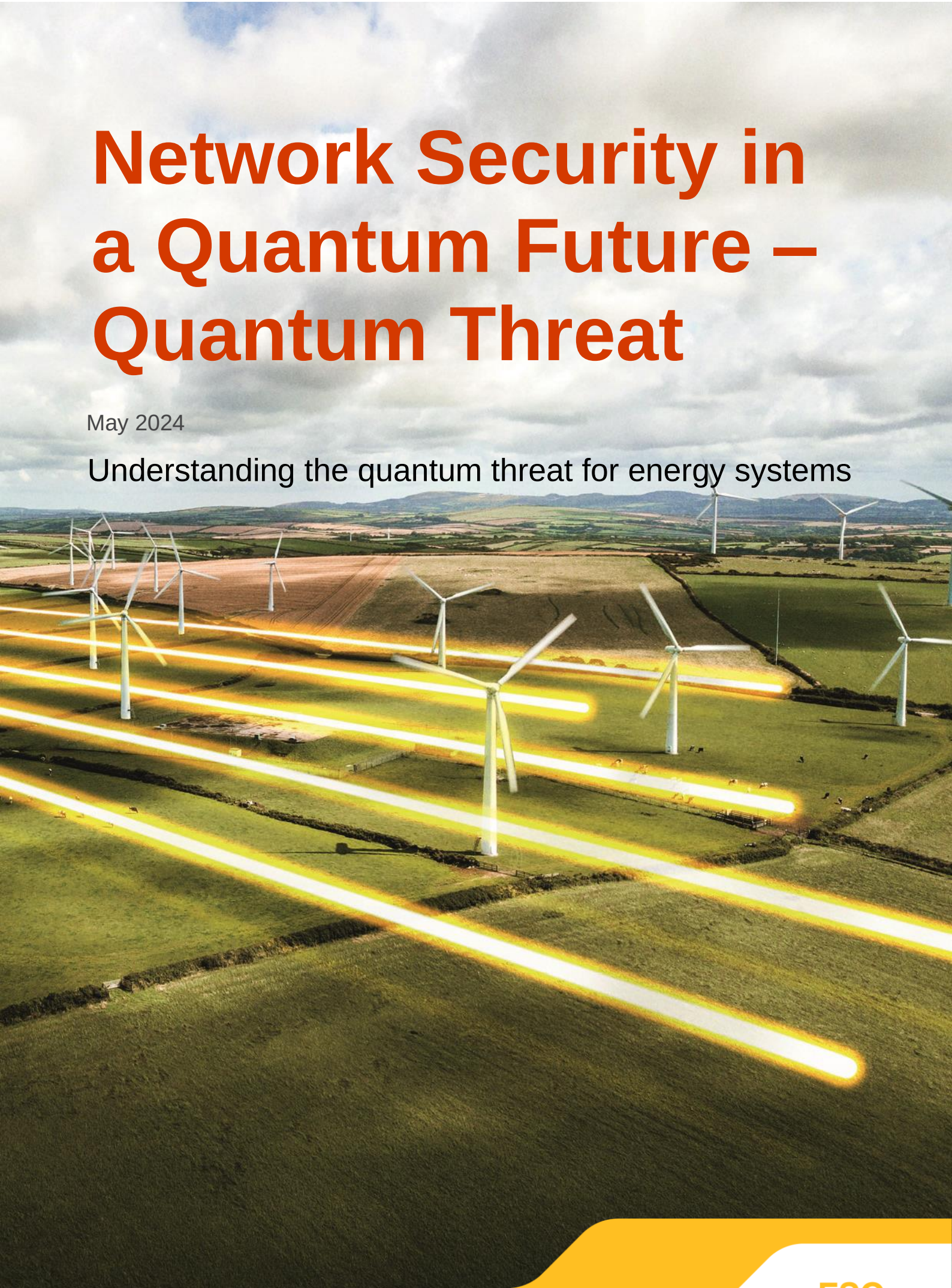
Network Security in a Quantum Future – Quantum Threat

May 2024

Understanding the quantum threat for energy systems



ESO

Ofgem Strategic Innovation Fund Contributing Partners

ESO	National Grid ESO
cambridge consultants Part of Capgemini Invent	Cambridge Consultants
THE UNIVERSITY of EDINBURGH	University of Edinburgh
WARWICK THE UNIVERSITY OF WARWICK	University of Warwick

Executive Summary

The ongoing security of the UK power system is of key national importance, with the potential interruption of supply having significant social and economic consequences. Threats to the ongoing security of the grid have increased in recent years, and cybersecurity of national energy infrastructure is becoming an ever-growing concern.

While methods of defending against current cyberattacks are well-established, looking ahead, there is the potential for a significant increase in the cyber threat to energy grid security from the development of quantum computers.

What is quantum?

Unlike current computers, quantum computers use an alternative computational paradigm that is based on using quantum mechanical phenomena for information processing [1]. This rapidly developing technology promises dramatic acceleration of computational speed on a wide range of tasks, enabling some computations that we currently consider impossible to become achievable. Future quantum computers will enable significant advances across a wide range of hard-to-solve industrial and technology development problems requiring computation- such as high-accuracy chemistry simulation, climate system modelling, or high-energy physics - by shortening the time needed; calculations which are predicted to take decades or longer on classical computers could be completed in only a few hours. Currently it is estimated that commercially relevant quantum computers will start to appear in the early 2030s.

Why does it matter for the energy grid?

While quantum will deliver many beneficial applications, quantum computers also have the potential to enable novel types of attacks on current cryptographic standards. As one example, breaking a 2048-bit RSA encryption scheme is impossible for 'traditional' computers due to the length of time (thousands of years) required for the necessary computations, but a quantum computer, with its dramatically greater compute power, could break such a scheme in as little as 8 hours.

For critical infrastructure such as energy systems, there is an important risk of such attacks becoming reality in the foreseeable future. However, there is significant hype, and a lack of clarity on when and how quantum computers will affect current cryptographic standards. This makes planning for mitigation extremely challenging.

How will the current work address the challenge?

The SIF Discovery project "Network Security in a Quantum Future" is designed to be the first step in providing insight into the scale and timing of the quantum threat for energy systems, and developing mitigation tailored to the particular technologies deployed in the UK energy system. This work has been undertaken by a consortium including National Grid ESO, Cambridge Consultants, the University of Edinburgh, and the University of Warwick.

The findings of the Discovery phase work are detailed in this report (Quantum Threat), which focuses on quantifying the threat from quantum computers; the companion report Cybersecurity Analysis looks at what type of attackers might exploit the threat and presents a potential framework for mitigation; and the third output report from this phase is the Worked Example report which shows a worked example applying the proposed threat evaluation process (the 'Quantum-Aware Risk Assessment' process) to an exemplar use case from the energy sector developed in collaboration with National Grid ESO.

Key questions we have aimed to address in this Quantum Threat report are (see Section 7.2 for a summary):

1) *Level of threat:* What is the quantum threat to the cryptographic schemes?
2) *Government initiatives:* What activities are being carried out within wider society with regards to the quantum threat?
3) *Specifications and enablers:* What system specifications are required for a CRQC?
4) *Threat timeline:* How long until we expect cryptographically relevant quantum computers (CRQCs) for current cryptographic standards?
5) *Continuous monitoring of quantum threat developments:* How do we track progress within the quantum industry?

6) *Potential mitigations for the energy sector:* What mitigations against the quantum threat are available to the energy industry? (primarily addressed in the companion report Cybersecurity Analysis)

The main findings of the Quantum Threat Report are:

Defining the quantum threat (Section 3)

- There are a number of quantum algorithms that threaten current cryptosystems.
- In particular, the quantum algorithm known as Shor's algorithm (and its variants) is capable of delivering an exponential speedup against a range of cryptographically relevant mathematical challenges – in other words, massively accelerating the speed at which an encryption scheme can be broken by an attacker with access to a quantum computer. In addition, ongoing research efforts are likely to shorten the time until a CRQC is deployed, bringing the threat timeframe closer.
- This will enable quantum attacks against current public key cryptography, which is a widely used approach to cybersecurity in the energy network.
- Conversely, symmetric cryptography is currently believed to be secure against quantum attacks. This is relevant to energy network operators, as it can offer a way to mitigate some (but not all) types of future quantum attacks.
- *Implication: To evaluate the level of threat, it will be important for energy system providers to evaluate the different types of schemes they are currently using – in order to establish which are most vulnerable and to start considering mitigation approaches.*

Quantum risk frameworks and key government and industry activities (Section 4)

- Several widely used frameworks for quantum risk assessment are already in place (e.g., Mosca's inequality, the Crypto Agility Risk Assessment Framework). These can provide a starting point for energy network operators looking for interpretable rules of thumb or scoring systems for assessing quantum risk.
- Many international governments are taking action to highlight the urgent nature of the challenge posed by the quantum threat, and the need to transition to quantum-safe cryptography. However, these are general in nature, rather than specific to energy networks.
    - Most national post-quantum programs are following the NIST standardisation process, with some notable exceptions (China and South Korea).
    - While governmental reports highlight the need to estimate the time to CRQC deployment, they generally do not provide specifics on how to do this, or take an overly simplistic and general 'X years to quantum' point of view.
- *Implication: Government initiatives are currently providing good general guidance and information on the quantum threat, but it is not specific enough to support energy network operators in understanding the nature of the quantum threat for their assets, or how best to assess it and plan for mitigations*.

Quantifying the quantum threat – progress and approaches (Sections 2, 5 and 6)

- Timelines for the quantum threat are shortening. To understand the current state-of-play and potential evolution, we reviewed views on timelines, progress on quantum algorithms and hardware, and potential approaches to quantifying the threat.
- Current expert opinion on quantum risk is that CRQCs are likely to appear in the 10-20-year time horizon. However, due to the potential of novel attacks such as 'store now, decrypt later' attacks, for assets with long lifespans it may be necessary to consider mitigations in the near future.
- A wide range of approaches and factors – including both algorithmic improvements and hardware factors - could shorten the estimated timeline until availability of CRQCs.
- On the algorithm front, algorithmic improvements have brought down the estimated required resources for a CRQC over time, and further improvements are likely.
- 'Resource estimation' is an approach to understanding quantum algorithmic performance that provides a way to realistically estimate requirements for a CRQC, and by extension, for timelines until the quantum threat to cybersecurity becomes significant. A commonly cited resource estimation result is that – based

on current understanding and state of play for quantum development - it would take 8 hours and 20 million physical qubits to break RSA 2048 cryptographic schemes.

- On the hardware front, quantum hardware companies have published ambitious hardware roadmaps, which if achieved will accelerate the path to CRQCs. Qubit counts (the key measure of quantum computer power) are doubling about every 18 months. This critical KPI gives an indication of how quickly quantum compute power is increasing.
- Quantum error correction is another key aspect of developing useful and valuable quantum computers, and there has been exciting recent progress in improved codes with lower overheads. Again, this is likely to accelerate quantum threat timelines.
- While resource estimation approaches are valuable for understanding the requirements and performance of quantum algorithms, they do not allow for easy incorporation of new information on changes across the wide range of factors that can impact quantum threat timelines. There is currently no easy way to assess different ranges of assumptions, and the impact of different factors that could shorten the threat timeline.
- *Implication: The timeline for the quantum threat is currently estimated to sit somewhere in the 10-20 year range, but this is a wide range, and could vary significantly (i.e. become much shorter), depending on how quickly types of novel attacks, improved algorithms, and/or enhanced compute capabilities emerge. This uncertainty creates risk for energy networks. It will be critical to extend and refine the capabilities of the 'resource estimation' approach (the current best-practice approach to estimating requirements for CRQCs), to accommodate changes, uncertainties, and impacts of different factors, in order to better inform understanding of evolving threat timelines.*

Gap analysis (Section 7)

- Our literature review highlighted the significant work already completed on the quantum threat, but there are still open questions which need to be addressed, to provide clarity on how best to develop an approach that could support energy network operators in assessing the threat on an ongoing basis.
- First, there is a need to understand the impact of improvements which may reduce algorithmic requirements.
- Second, qubit count alone does not give a clear picture of when CRQCs will be deployed. Other developments will accelerate this timeframe, for example in connectivity and quantum error correction. These need to be explored more fully.
- Third, resource estimation - as an approach to understanding quantum algorithmic performance - has provided significant insight into both the system specification for a CRQC, and the time to complete an attack. However, most resource estimates are completed for a specific hardware architecture and a given set of assumptions, with no clear way to update or explore alternative scenarios.
- A broader set of KPIs are needed to properly track the quantum ecosystem. Further, uncertainty is not properly captured in current risk frameworks, which limits their usefulness in making mitigation decisions for the energy sector (and more broadly).
- *Implication: To assess the quantum threat on an ongoing basis will require a multi-pronged approach to understanding the threat, considering the evolution of different factors that could impact the timeline.*

Recommendations and next steps:

We recommend building a flexible 'quantum threat tracker' tool to help energy system stakeholders, enabling them to clearly understand the timescales of relevant quantum threat aspects, and the impact of specific mitigations, as well as assessing these against the uncertainty of current and future developments on an ongoing basis.

Our major recommendations are:

- To build a 'quantum threat tracker' tool – based around a dynamic resource estimation tool, to allow rapid exploration of potential security scenarios that could impact the energy sector. The tool should have the following characteristics:
  - modularity, to allow easy updates when new advances in algorithms / hardware are announced;

    - uncertainty handling, to aid decision support systems and make better judgements on current and future risks;
    - ability to be applied to energy-specific scenarios, to ensure the high-impact scenarios for the energy sectors are explored (vs scenarios where an ‘off-the-shelf’ PQC solution could mitigate the threat).
    - ability to work as a stand-alone tool.
- To do further analysis to develop greater understanding of the energy-specific quantum threat scenarios: including:
    - mapping the energy-specific uses of cryptography, and the cost of changing these;
    - identifying the critical systems and longest lifespan assets;
    - and quantifying the risks.

Our secondary recommendations are:

- Further research to quantify predicted costs of mitigating the threat for the energy sector.
- Exploring whether some mitigation strategies are suitable for introduction for the energy sector at an early stage as a preventive measure before a full mitigation strategy is in place.
- Understand if the overreliance on a small number of post-quantum cryptographic (PQC) algorithms lead to an increased risk, especially given their relatively untested nature. Could previously discarded PQC algorithms provide alternative options for the specific use cases of energy networks, for example short lived timescales?
- Further validating the suitability of Mosca’s inequality as a key element of the threat rating framework (see Section 4.1), and whether a more mature solution is required.

We welcome comments and feedback on this research from energy system stakeholders, quantum and cybersecurity experts, and the broader public. Together we can provide strong and impactful support to the energy sector as the UK prepares for a post-quantum future.

Contents

1 Introduction

The ongoing security of the UK national power system is of key national importance, with the interruption of supply having significant social and economic consequences. Recently the number of threats to the ongoing security of the grid have increased, with cybersecurity becoming an ever-growing concern. The potential impact that the development of quantum computers will have on the ongoing cybersecurity of power networks is a threat that cannot be ignored.

The SIF Discovery project “Network Security in a Quantum Future” is designed to be the first step in providing insight into the scale and timing of the threat for energy systems, and developing mitigation tailored to the particular technologies deployed in the UK energy system. This work has been undertaken by a consortium including National Grid ESO, Cambridge Consultants, the University of Edinburgh, and the University of Warwick. The findings of the Discovery phase work are detailed in this report, which focuses on quantifying the threat from quantum computers; and the companion report (Cybersecurity Analysis), which looks at what type of attackers might exploit the threat and presents a potential framework for mitigation.

Over the last twenty years there has been significant progress on the development of novel computing platforms, of which one of the most promising technologies is quantum computing. Unlike current computers, quantum computers use an alternative computational paradigm that is based on using quantum mechanical phenomena for information processing [1]. This rapidly developing technology promises significant acceleration of computational speed for a wide range of tasks, enabling some computations that we currently consider impossible to become achievable in relatively short timespans. Quantum computing is expected to bring significant commercial and societal value over the coming decades, supporting a wide range of high-intensity computing applications including drug discovery, material design, network optimisation, and probabilistic simulation.

Unfortunately, as well as the potential positives, quantum computers also have the potential to enable novel types of attacks on current cryptographic standards. Such standards – for example, Public Key cryptography (PKC), are typically based on computational algorithms that are too complex for today’s digital computers to ‘break’ easily, but which much faster quantum computers could (in theory) solve relatively quickly.

There is significant hype and a lack of clarity on when and how quantum computers will affect current cryptographic standards. This potential ‘quantum threat’ is still some way off, due to both the relative immaturity of quantum technology, and the fact that availability of such resources to potential attackers is likely to be limited. Quantum computers and quantum algorithms are still nascent technologies, with many significant challenges to be overcome until they are fully realised. Building a quantum computer is an enormous engineering challenge and thus far, all physical realisations of quantum computers have been too small-scale and error-prone to pose a threat to real cryptographic systems. However, given the rapid technological development of the field, a Cryptographically Relevant Quantum Computer (CRQC) - i.e. a quantum computer that can break current cryptographic standards - is now expected to be developed and deployed within the next 15-20 years.

Despite what may seem to be long timescales, the quantum threat to the UK energy system needs to be considered now for two key reasons. Firstly, the development and implementation of mitigations against the quantum threat will take a number of years, and will require significant planning and coordination. Secondly, for information with a long lifespan - i.e., for which the confidentiality of the information is important for many years - it is worth considering the potential impact of ‘store now, decrypt later’ attacks [3]. Messages that are not currently decryptable may be stored by adversaries in their encrypted form, then decrypted once the quantum computing technology becomes sufficiently capable. For cryptosystems protecting digital assets with long confidential lifespans – which is an important consideration for energy system operators – the rapid progress of quantum development means it may be necessary to consider alternative encryption methods on a significantly accelerated timeframe.

1.1 Guiding questions

In the initial part of the project, the consortium worked together to define a number of questions that are important to address when understanding the potential quantum threat to energy systems. These questions have been used to guide the topics explored in the literature review, and to help identify the gaps in the literature that are critical to understanding the quantum threat for the energy industry. These gaps (see Section 7 for details) will need to be addressed for the energy industry to have a clear understanding of both

the scale and timing of the quantum threat, as well as enabling the development of a mitigation strategy. We hope to address these gaps in later stages of this Innovation project.

The list of guiding questions was initially developed during the first consortium workshop held on the 7th of March 2024, and then refined during the second consortium workshop held on the 2nd of April 2024.

For easy reading we have grouped the questions together by topic, with a fundamental question followed by more detailed sub-questions:

What is the quantum threat to the cryptographic schemes?

- What are the primary quantum algorithms of concern?
- Which cryptographic protocols are threatened?

What activities are being carried out within wider society with regards to the quantum threat?

- What activity is happening in parallel industries, especially within other critical national infrastructure?
- What have global government bodies said about the quantum threat?
- What skills investment is required, and when?

How long until we expect CRQCs for current cryptographic standards?

- How might this timeframe be shortened?
- When does the energy industry need to react against the future threat?
- For CRQCs, can we predict the length of time an attack will take to perform?
- Can we understand how quickly the threat changes, especially with regards to threat timings?
- How does uncertainty about our assumptions impact the expected timeframe for CRQCs?

What system specifications are required for a CRQC?

- How do recent algorithmic developments reduce resource requirements in practice?
- How do different hardware types and quantum error correction schemes affect systems specifications and feasibility of attacks?
- How do resource estimates change under different assumptions about future hardware architecture?

How do we track progress within the quantum industry?

- What are the key performance indicators that provide insight into the progress towards a CRQC?
- Which countries and organisations are investing and at what level is the investment?

What mitigations against the quantum threat are available to the energy industry?

- How much does increasing the key size of existing protocols extend their lifespan / security?
- What alternative cryptographic schemes are available and what are the constraints on their use?
- What are the costs, both one-time and maintenance, for upgrading cryptosystems?

1.2 Report contents

This report details the work completed in understanding the quantum threat to the energy industry within the Discovery Phase of the SIF project “Network Security in a Quantum Future”.

Section 2 provides a brief technical introduction covering the basics of quantum computing and cryptography. Readers interested in further details should explore the references in that section.

Sections 3-6 cover the findings of the literature review, which was guided by the questions posed in the previous section (Section 1.1). The analysis is split into four sections.

The first of these, Section 3, describes the findings around the quantum threat; specifically, the key quantum algorithms, including a discussion of recent progress and then details of which cryptographic protocols are and are not potentially vulnerable when we obtain a CRQC.

This is then followed in Section 4 by a study of the efforts by the wider world to quantify the threat, including developed risk frameworks for reasoning about the level of threat, and activities by government bodies and industry in assessing the threat and producing potential mitigation pathways.

In Section 5, we review the current capabilities of quantum computers with regard to cryptographic schemes and expert opinion on when this threat could be realised. We conclude this section by highlighting the academic work to estimate both the required future specifications of a CRQC and time needed to complete an attack.

The final part of the literature review, Section 6, focuses on the current and future progress within quantum hardware development. This includes a review of various publicly available hardware roadmaps and of current progress in quantum error correction.

Section 7 presents an analysis of the relevant gaps discovered in literature. We revisit the guiding questions discussed in Section 1.1 in light of the literature review and use these to identify gaps in the literature which need to be filled, to provide the energy industry with a clear understanding of the quantum threat and the main considerations in developing mitigations.

Finally, Section 8 provides recommendations for future work to tackle these gaps. These could potentially be taken forward in an Alpha stage of the project.

2 Technical background

2.1 What is Quantum computing?

A quantum computer is a computer which utilises quantum mechanical phenomena, such as superposition and entanglement, in its computations. Analogous to classical (non-quantum) computing in which the most elementary unit of information is a binary digit (bit), in quantum computing the most elementary unit of information is a quantum bit (qubit). Like classical bits, a qubit can be placed into states $|0\rangle$ and $|1\rangle$ (called basis states). However, unlike classical bits, qubits can also be in a linear combination of basis states (called a superposition), such as $\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$. We refer the reader to [1] for a comprehensive introduction to quantum computing.

2.1.1 Quantum error correction

Unlike most of classical computing, which is naturally self-correcting, errors are a key challenge for quantum computers. Protecting calculations from errors comes with a significant overhead both with regards to the extra number of qubits required for error correction and the reduction in clock speed to allow error detection and mitigation.

When considering error correction, there is an important distinction to be made between the logical and physical units of information. The need for redundancy when performing error correction necessitates the physical device having a greater number of (quantum) bits than those which may be directly accessible by the user. For example, consider a classical computer which offers resilience to bit-flip errors by using the five-bit repetition code: encoding one logical bit into five physical bits as $0 \mapsto 00000$ and $1 \mapsto 11111$. If a bit-flip error occurs, e.g., resulting in 01000, the computer can detect this and correct the physical register back to 00000. However, the cost of this resilience is a greater number of physical than logical bits. In this case, the computer has five physical bits but only one logical bit.

2.2 Understanding Cryptography Systems

Modern cryptosystems can broadly be partitioned into two types: symmetric-key algorithms (for example AES [4]) and public-key algorithms (for example RSA [5]). This has important implications for our investigation of the quantum threat to cybersecurity, because the vulnerability to quantum attack is expected to differ across these two types of schemes.

Generally, symmetric-key algorithms are much more computationally efficient at encrypting data,but require the involved parties to already share a pre-agreed secret (symmetric key). Public-key algorithms or cryptosystems (PKC) tend to be far slower for encrypting data, but do not require any pre-agreed secret between the involved parties. Thus, public-key protocols are typically used to distribute symmetric keys between users for bulk encryption / decryption, rather than directly encrypting messages.

As will be discussed in Section 3, current PKC implementations will be susceptible to quantum attacks, while it is believed that symmetric schemes are resistant. Both PKC and symmetric cryptography are widely used across the energy industry.

At a high-level, in public-key encryption protocols for sending messages, the intended receiver first generates public and private keys, the former of which can encrypt messages and the latter of which can decrypt them. The receiver distributes their public key whilst keeping the private key secret. Anyone can then encrypt messages using the receiver's public key, but only the receiver is able to decrypt them. In this way, any eavesdropper observing communication channels between the transmitter and receiver only has access to the public key and encrypted messages, and is unable to decrypt messages without knowing the private key. See Figure 1 for a diagrammatic representation of this process.

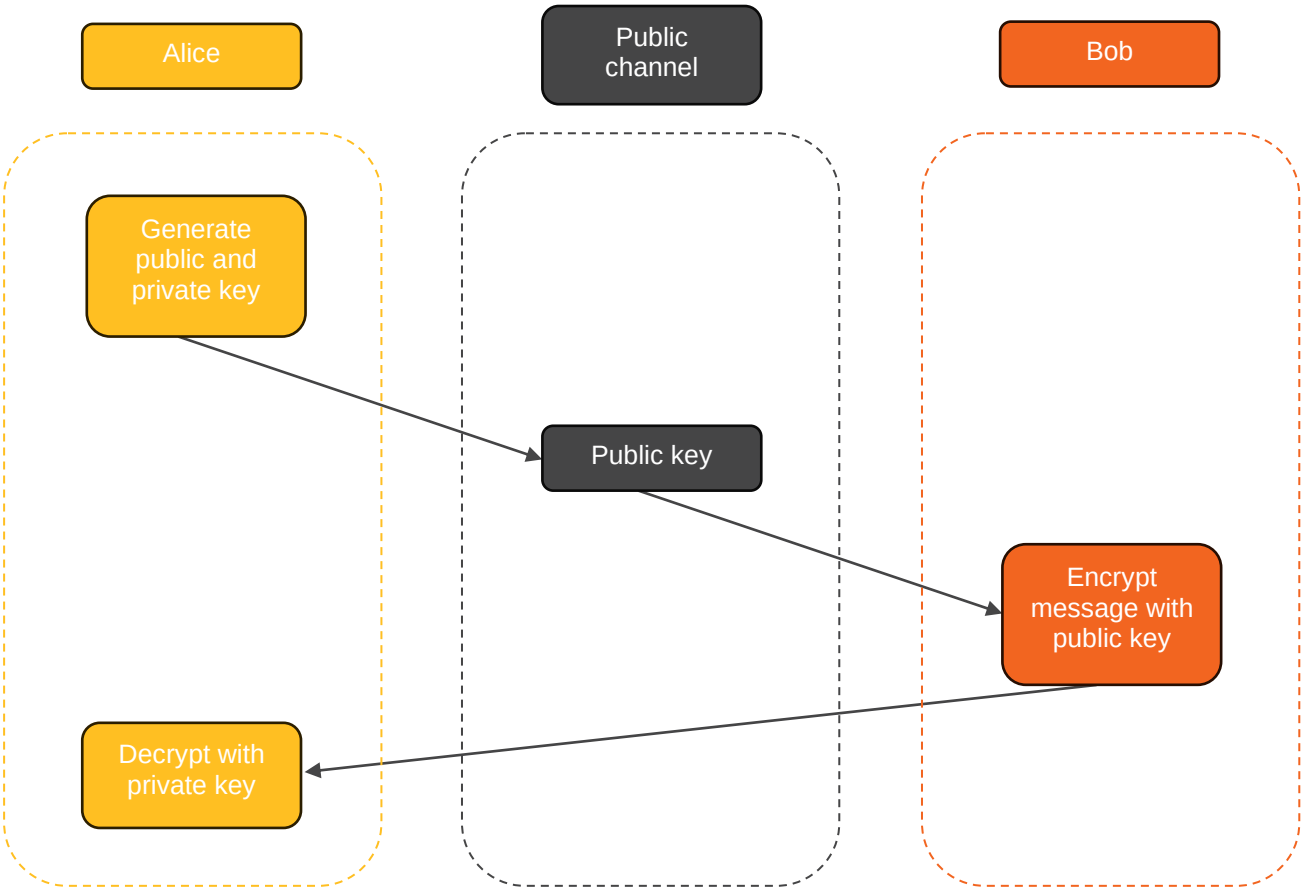


Figure 1 - Public-key encryption protocol allowing Bob to send a secret message to Alice using a public channel.

Public-key cryptosystems rely on the concept of one-way functions – functions which are computationally efficient at producing an output from any input, but it is assumed to be hard to find the input that produces a specific output. A cryptographically relevant example is integer factorisation – it is computationally very easy to multiply two large integers together, yet there is no known efficient classical algorithm for finding the factors of a composite integer. Public keys are generated using this concept of one-way functions. In the RSA protocol, (very broadly speaking) the private key can be considered to be two large prime numbers and the public key their product. Thus, an efficient algorithm for factoring integers would render the RSA protocol insecure.

A related use of public key cryptography is in generating digital signatures: the sender signs their message through a process using their private key, which the intended receiver verifies using the sender's public key. In this context, a malicious party with the ability to break public keys (e.g., factor integers efficiently) would be able to forge messages, i.e., sign them as if they were sent by a trusted party.

2.2.1 One-way functions and key sizes

The two most common one-way functions used for public-key cryptography are integer factorisation (solving this attacks RSA [5]) and the discrete logarithm problem (solving this attacks Diffie-Hellman[6], a widely used alternative PKC scheme). For RSA and integer factorisation, we use the term 'key size' to refer to the size of the integer to be factored – for example, a 2048-bit key refers to a product of two primes whose binary representation is at most 2048 digits long.

The discrete logarithm problem is, in its simplest form, as follows: given a prime number p and positive integers $a, b < p$, find an integer k such that $b^k = a$ modulo p. In this case, the term 'key size' refers to the size of the modulus p. Similarly, to RSA, a 2048-bit key refers to using a prime number p whose binary representation is at most 2048 digits long. Diffie-Hellman and the discrete log problem are easily extended to

work with other mathematical objects, groups, the most common examples are elliptic curves, for details see [7].

The key sizes are often used in combination with cryptographic protocols to refer to specific implementations of cryptosystems. RSA-2048 is widely referenced both as a specific public key [8], and the use of keys of bit-length 2048. For elliptic curve cryptography, NIST provide specific curves to be used [9], for instance, ECDH P-256 [10].

2.3 The relevance of asymptotic notation

In computer science, specifically complexity theory, the performance of an algorithm is often analysed with respect to the asymptotic complexity; that is, how the running time scales as the input gets large. This is relevant to our investigation of quantum impact on cybersecurity because the quantum algorithms studied typically do not specify the exact resources or runtimes, so we use asymptotic complexity to provide comparisons between them. For example, say we have two algorithms which solve a problem of size n:

- Algorithm 1, which solves the problem using $100n^2$ operations.
- Algorithm 2, which solves the problem using $0.01n^3$ operations.

Even though Algorithm 2 is far more efficient for small values of n, in complexity theory Algorithm 1 is often considered superior since $100n^2$ will eventually be smaller than $0.01n^3$ for sufficiently large n[1]. This motivates asymptotic notation, which effectively hides constant factors. The most famous member among the family of asymptotic notation is 'Big O' notation, which establishes an asymptotic upper bound. In the above example, we say that Algorithms 1 and 2 have running times (or complexities) of $O(n^2)$ and $O(n^3)$, respectively. We forgo a formal definition of Big O notation for this literature review, for which we refer the reader to [1]; however, we provide some more explicit examples for intuition. An algorithm which takes any of the following number of steps is said to have a complexity of $O(n^2)$:

- $n^2 + n$.
- $100n^2$.
- $n^2 + 50$.

An algorithm is said to run in polynomial time if it runs in time $O(n^d)$ for some positive integer d. An important separation is between polynomial-time algorithms and those which run in exponential time; for example, an algorithm which takes 2^n steps to execute is said to run in exponential time. For a case where it takes 2^n steps, just increasing the input size by 1 doubles the work needed. In contrast, for a polynomial-time algorithm, for instance one which executes in n^2 steps the problem would have to increase by nearly 1.5 times (of $\sqrt{2} \approx 1.41$) before the work needed was doubled. Algorithms which run in exponential time are generally considered to be inefficient and unscalable, whereas polynomial-time algorithms are comparatively much more efficient.

If Algorithm 1 takes $f(n)$ steps to run and Algorithm 2 takes $O\left(\sqrt[d]{f(n)}\right)$ steps for some integer d, then Algorithm 2 is said to offer a polynomial speedup over Algorithm 1. For $d = 2$ this is called a quadratic speedup, for $d = 3$ a cubic speedup, for $d = 4$ a quartic speedup, etc.

Due to the extremely slow-growing nature of logarithms, a common convention which we will also adopt is using a tilde symbol to hide polylogarithmic factors. For example, the Schönhage–Strassen integer multiplication algorithm, which runs in time $O(n \log n \log\log n)$ [11], can be said to have a complexity of $\tilde{O}(n)$.[12]

[1] Take any n > 10,000.

3 Defining the quantum threat

The advance of quantum computing threatens a range of different cryptographic algorithms using a relatively small number of key quantum algorithms. Here we seek to answer:

What is the quantum threat to the cryptographic schemes?

- What are the primary quantum algorithms of concern? (See Section 3.1)
- Which cryptographic protocols are threatened? (See Section 3.3)

In summary, the primary quantum algorithms of concern in the context of considering impact on energy network cybersecurity are Shor's algorithm, which can be used to rapidly factorise large numbers as well as enabling solution of other complex algorithms underlying commonly-used cryptographic schemes such as RSA; and to a lesser extent, Grover's algorithm, which can be applied to breaking symmetric key cryptosystems that rely on exponential search spaces as security.

3.1 Section summary – Defining the quantum threat

- Shor's algorithm and its variants provide the main quantum threat against current cryptographic schemes.
  - They provide an exponential speedup against a range of cryptographically relevant mathematical challenges like integer factorisation, and the discrete log problem including elliptic curve variants.
  - This speedup enables quantum attacks using these against known current public key cryptography, digital signatures and many blockchains.
- Shor's algorithm is still an area of active study, with improvements and alternative strategies regularly proposed.
  - These are looking to reduce the system specification necessary for a CRQC, both in regard to the number of qubits and circuit depth.
  - These developments will reduce the time until a CRQC is deployed.
- Alternative quantum algorithmic approaches have been explored but currently none show significant promise.
- Grover's algorithm does not provide any significant attack against symmetric cryptography.
  - Doubling the key size provides at least the same level of security.
  - Symmetric cryptography is currently believed to be secure against quantum attacks.

3.2 Key quantum algorithms

Of the known algorithms that threaten current cryptosystems, the most well-known is Shor's algorithm (see Section 3.2.1), typically used to factorise large numbers. We explore recent extensions and optimisations of this algorithm (see Section 3.2.2 and Section 3.2.3) in addition to more controversial methods of factorisation (see Section 3.2.4 and Section 3.2.5). We also consider the application of Grover's algorithm (see Section 3.2.6) to breaking symmetric cryptosystems.

3.2.1 Shor's algorithm

Shor's algorithm is a polynomial-time algorithm for integer factorisation on a quantum computer [12]. Specifically, Shor's algorithm shows that it is possible to find a factor of an n-bit integer in $O(n^2 \log n)$ time on a quantum computer, which is exponentially faster than the fastest known classical algorithms [1]. Shor's original formulation of the algorithm consists of a quantum circuit on $3n$ qubits with classical polynomial-time pre- and post-processing steps. Since practical executions of Shor's algorithm are not bottlenecked by the requisite classical parts, in this literature review we primarily focus on implementations of the quantum circuit. Some prerequisite quantum computing knowledge is required for this section, for which we again refer the reader to [1].

Shor shows that to factor an n-bit integer N, it is sufficient to run the following operations on a quantum computer.

1. Initialisation of a $2n$-qubit register to the uniform superposition.
2. Computation of $|r^x \pmod N\rangle$ in a new n-qubit register, where r is a some randomly chosen integer with $1 < r < N$ and x is the value in the first register.
3. Execution of the $2n$-qubit quantum Fourier transform in the first register.

Step 1 can be performed in constant time by preparing $2n$ qubits in the $|0\rangle$ state and applying a Hadamard gate to each. Step 3 can be performed using exactly $n(n+1)/2$ gates, given controlled rotations as a native gate (up to the ordering of the qubits which can be accounted for in classical post-processing). If the quantum hardware allows for mid-circuit measurements, the semiclassical Fourier transform [13] can be used to eliminate controlled rotations altogether. Thus, the bottleneck in Shor's algorithm is the middle step – that is, performing modular exponentiation in coherent quantum superposition – and this is the operation that most optimisations target.

Although the quantum part of Shor's algorithm does not always succeed, its failure probability is sufficiently low that repetition until success does not overwhelmingly hinder the running time. In particular, Shor shows that $O(\log\log n) = \tilde{O}(1)$ repetitions of the quantum circuit are enough to succeed with high probability.

Shor's algorithm is most commonly linked to factoring large numbers but can also be altered to solve other cryptographically hard problems. Algorithms that rely on the security of the discrete logarithm problem (see Section 2.2.1) can be attacked by a straightforward modification to Shor's algorithm, the first of which was proposed at the same time as the factoring algorithm [1]. Variants of Shor's algorithm can also be used to attack the elliptic curve discrete logarithm problem [14], making elliptic curve cryptosystems similarly vulnerable to quantum attacks.

3.2.2 Regev's algorithm

In [15], Regev shows that it is possible to lower the circuit depth in Shor's algorithm at the cost of a greater number of circuit repetitions. Specifically, Regev shows that $\tilde{O}(n^{0.5})$ repetitions of a circuit of depth $\tilde{O}(n^{1.5})$ suffices for finding a non-trivial factor of an n-bit integer. Contrast this with Shor's algorithm, which requires $\tilde{O}(1)$ repetitions of a circuit of depth $\tilde{O}(n^2)$.

Regev's algorithm requires $\tilde{O}(n^{1.5})$ qubits which is greater than the $\tilde{O}(n)$ qubits required by Shor's algorithm. Subsequent work[17] reduced this to $\tilde{O}(n)$ [16], which asymptotically matches Shor's algorithm; however, the constant factors hidden by this notation still seem to be significantly greater than those found in optimised variants of Shor's algorithm.

The shortening of circuit depth in Regev's algorithm is significant for cryptographic purposes since near-term quantum devices are expected to be limited in applicable circuit depth. However, all analysis thus far is asymptotic, and it is unclear yet as to whether Regev's algorithm provides improved performance for cryptographically relevant key sizes. Furthermore, Shor's algorithm has received decades of optimisations in circuit depth, qubit count, and constant factors, which are not directly applicable to Regev's algorithm. We expect Regev's algorithm to receive similar optimisations over the coming years but again it is unknown whether this will be enough to outperform optimised variants of Shor's algorithm. It is also worth noting that unlike Shor's algorithm which is rigorously proven to succeed with high probability, Regev's algorithm relies on a mild yet nonetheless unproven number-theoretic heuristic assumption.

3.2.3 Chevignard's algorithm

Recently, Chevignard et al. constructed the first rigorous quantum algorithm for factoring RSA numbers that requires a qubit count which is less than the size of the input [17]. Chevignard et al. show that it is possible to factor an n-bit RSA number using $n/2 + o(n)$ qubits[2] which is a significant improvement over previous works which typically require at least $2n$ qubits [18], [19], [20], [21], or $1.5n$ [22]. Although their analysis is primarily asymptotic, they estimate that less than 1700 logical qubits suffice for factoring a 2048-bit RSA number.

[2] Little o, $o(\cdot)$, is another member of the family of asymptotic notation (see Section 2.3) which defines a stricter bound than Big O notation.

3.2.4 Quantum Approximate Optimization Algorithm (QAOA)-based factoring

In [23], Yan et al. propose a factoring method based on reducing factoring to the closest vector problem by Schnorr's algorithm [24], [25] then solving the latter using the quantum approximate optimisation algorithm (QAOA) [26]. They report the successful factorisation of 48-bit integers using only 10 qubits and estimate that 2048-bit integers could potentially be factored using only 372 qubits. However, their method is heuristic, and several following works identify issues in both the complexity and correctness of the classical reduction [27], [28].

Similarly, reference [29] describes a reduction from factoring to satisfiability (a hard computational problem) with the promise that any quantum algorithm which solves satisfiability faster than classically offers an asymptotic speedup for factoring over the best classical algorithm. Whilst QAOA has shown promise in offering some speedup for solving satisfiability [30], there is no evidence to suggest that this ultimately yields a polynomial-time algorithm for integer factorisation.

3.2.5 Adiabatic quantum computation-based factoring

Adiabatic quantum computation [31] and quantum annealing [32] are alternative quantum computing paradigms which utilise the adiabatic theorem and quantum fluctuations, respectively. Although these methods have been used to experimentally factor numbers far greater than physical realisations of Shor's algorithm [33], there is no evidence that the running time scales favourably with the input size, as in Shor's algorithm.

3.2.6 Grover's algorithm

Grover's algorithm offers a quantum speedup for the problem of unstructured database search, allowing one to brute-force search a list using a number of queries which is asymptotically smaller than that which is required classically [34]. This theoretically poses a threat to the security of symmetric-key cryptosystems in that a symmetric key could be found through brute force using Grover's algorithm faster than by a classical computer. However, unlike Shor's algorithm, the speedup offered by Grover's algorithm is not exponential, only quadratic. Thus, a simple doubling of the key length (which in turn corresponds to a squaring of the magnitude of the key) effectively eliminates any threat which might be presented by Grover's algorithm against symmetric-key cryptosystems [35], [36], [37].

3.3 Quantum attacks

From the quantum threats identified (see Section 3.1), there are two general classes of algorithms that can be leveraged against current cryptosystems:

- Shor's algorithm: for cryptosystems relying on the hardness of factoring, the discrete logarithm problem, or the elliptic curve discrete logarithm problem as security.
- Grover's algorithm: for cryptosystems relying on exponential search spaces as security.

Of these, Shor's algorithm provides the far greater threat to security due to the exponential speedup it provides. The first cryptographically relevant quantum computer (CRQC), "quantum computers (sic) that are capable of actually attacking real world cryptographic systems that would be infeasible to attack with a normal computer." [38], will therefore likely use some form of Shor's algorithm.

3.3.1 Asymmetric cryptography

Literature concerning Shor's algorithm often focusses on the threat to the RSA cryptosystem. But, as advised by NIST [39], many other standard cryptographic schemes [9], [39] are also proven to be insecure against quantum cryptographic attacks. These include, but are not limited to:

- Key exchange protocols:
  - Rivest-Shamir-Adleman (RSA)
  - Diffie-Hellman (DH)
  - Elliptic Curve Diffie-Hellman (ECDH)
  - Menezes-Qu-Vanstone (MQV)

- Digital Signature protocols:
  - Digital Signature Algorithm (DSA)
  - Elliptic Curve Digital Signature Algorithm (ECDSA)
  - Edwards Curve Digital Signature Algorithm (EDDSA)
  - RSA

The standard cryptographic schemes, including symmetric schemes, have guidance on the level of security that each of them provides (see Table 1). These are currently based on the level of security against classical attacks, which allow for equivalent security of cryptosystems with different key lengths. Shor's algorithm introduces different scaling for these problems, requiring new classification for security levels. The current resource estimate trends (see Section 5.4) suggest that elliptic curve-based schemes may be those first threatened by CRQCs due to the comparatively smaller key sizes used in practice.

Security strength (bits)[3]	**Factorisation: RSA**	**Discrete logarithm: DSA, DH, MQV**		**Elliptic curve discrete logarithm: ECDSA, EDDSA, DH, MQV**
	Key size	**Public key size**	**Private key size**	**Key size**
112	2048	2048	224	224-255
128	3072	3072	256	256-383
192	7680	7680	384	384-511
256	15360	15360	512	512+

Table 1 - Current security strength estimates for standard asymmetric cryptosystems. Adapted from [40], Table 2.

Due to the focus on Shor's factoring algorithm, there have been a significant number of optimisations for breaking RSA via a quantum computer. The similarity between factoring and solving the discrete logarithm problem on a quantum computer means that these optimisations to factoring can often be lifted to the discrete logarithm problem; indeed, Regev's algorithm has already been extended to the base discrete log problem [41]. In general, these optimisations are much more difficult to extend to the elliptic curve discrete logarithm problem and sometimes it may not be possible. This potentially means elliptic curve-based schemes will take longer to break in future.

3.3.2 Symmetric cryptography

Symmetric cryptography is widely believed to be either secure or securable against quantum attacks [42]. For instance, the NIST PQC competition [43]only requested public key cryptosystems. As discussed in Section 3.2.6, Grover's algorithm is the most credible threat to symmetric encryption methods since it provides a speedup to unstructured search problems. This can be applied to brute-force search attacks on symmetric key algorithms like AES-256 [44], or collision finding for hash functions like SHA-256 [45]; in theory, the speedup would put both at risk. In practice, doubling the key length is sufficient to secure against either attack:

- If a generic brute force attack on a symmetric key algorithm on n bits requires 2^n queries to succeed, then a Grover-like speedup would only require $2^{n/2}$ queries to succeed. Hence, doubling the key length to $2n$ bits will recover the same level of security, as $2^{2n/2} = 2^n$ queries are now needed to succeed.
- For a generic collision finding attack on n bits taking $2^{n/2}$ queries, the equivalent Grover speedup is even less, now requiring $2^{n/3}$ queries to succeed [45]. Here, a key length of $1.5n$ bits would recover the equivalent security, as $2^{1.5n/3} = 2^{n/2}$.

[3] For x bits of security, it should take $O(2^x)$ operations to break the cryptosystem (see [40]).

There has been further work on improving attacks for brute-force searching [46] and collision finding [47], but there are no substantial improvements that would require further mitigation. In fact, it is claimed that Grover's algorithm is far less impactful than the theoretical speedup might suggest, and that for symmetric keys, adding a fixed number of bits instead of doubling is sufficient to remain secure [48]. Other directions for attacks are being explored [49], but their applicability is not well understood, relying on cryptographic assumptions that may be difficult to realise in practice.

3.3.3 Decentralised solutions

Decentralised solutions such as blockchain and cryptocurrency are also at risk from quantum attacks, with the risks identified as: use of digital signature schemes; internet communication protocols; block mining speed; inverting hash functions; rewriting blockchain history [50].

Of these, the digital signature schemes, and internet communication protocols, are at risk of attacks using Shor's algorithm for factoring and discrete logarithms. Other risks relate to symmetric protocols (this risk can be mitigated by doubling the key length), or to the concept of Proof of Work (PoW) (for which mitigation requires some rethinking of the proofs and adjustment of the security definitions). While other blockchains, for example those based on Proof of Stakes, are not affected, the full security analysis of PoW blockchains in view of quantum attacks is still unclear. For example, the definition of what constitutes "honest majority" has to be adjusted when parties have both quantum and classical capabilities.

In [51] the pessimistic scenario where only adversaries have quantum computing resources, while all the other parties use classical computational resources, the analysis concluded that security could be maintained for a much larger fraction of honest parties (in Bitcoin it is assumed that half or more of the computational power is controlled by honest parties). In [52] a hybrid classical-quantum query model was analysed. In [53] a simplified version of Bitcoin was analysed, where all parties have quantum resources, and a different PoW was suggested that is "harder" for quantum parties than the usual hash-based scheme of Bitcoin. Finally, in [54] another potential vulnerability of PoW blockchains in the presence of small quantum miners was also given.

The cryptocurrency Ethereum, for example, currently uses the Boneh-Lynn-Shacham (BLS) algorithm as a digital signature [55], and Kate-Zaverucha-Goldberg (KZG) for commitment [56]. These can both be attacked by the elliptic curve variant of Shor's algorithm and will need to be replaced by post-quantum cryptographic algorithms in future [57].

4 Quantum risk frameworks, and key government and industry activities

In understanding the quantum threat, we begin by reviewing current quantum risk frameworks (see Section 4.1), and the activity of governments and industry to quantify and respond to it (see Section 4.1 and Section 4.3). This enables us to provide initial answers to the questions:

- When does the industry need to react against the future threat?
- What activity is happening in parallel industries, including other critical nation infrastructure?
- What have global government bodies said about the quantum threat?
- Which countries and organisations are investing?

4.1 Section summary – Quantum risk frameworks and key government and industry activities

- Mosca's inequality and the related Crypto Agility Risk Assessment Framework (CARAF) provide easily interpretable rules of thumb for assessing quantum risk.
  - While useful, they are however potentially too simplistic for a number of scenarios.
  - In particular, they do not allow the easy incorporation of uncertainty about the quantum threat.
- Most national post-quantum programs are following the NIST standardisation process with some notable expectations (China and South Korea).
- International governments are highlighting the urgent nature of the challenge posed by the quantum threat and the need to transition to quantum-safe cryptography.
- Many governmental reports highlight the need to estimate the time to CRQC deployment, but fail to provide useful insights.

4.2 Risk frameworks

The Mosca inequality [58] is a widely referenced model to understand if assets might be at risk from quantum computers. It is stated as:

An asset is at risk if X + Y > Z where:

- X – the remaining lifespan of the device or data.
- Y – the time required to mitigate the threat and migrate to a new system.
- Z – the time to a realisable threat; the time to a CRQC.

This was later expanded to a 6-stage framework [59], designed to integrate with standard risk assessment frameworks [60], [61]:

1. Identify and document information assets, and their current cryptographic protection.
2. Research the state of emerging quantum computers and quantum-safe cryptography. Estimate the timelines for availability of these technologies. Influence the development and validation of quantum-safe cryptography.
3. Identify threat actors and estimate their time to access quantum technology 'Z'.
4. Identify the lifetime of your assets 'X', and the time required to transform the organisation's technical infrastructure to a quantum-safe state 'Y'.
5. Determine quantum risk by calculating whether business assets will become vulnerable before the organisation can move to protect them. (X + Y > Z?)
6. Identify and prioritise the activities required to maintain awareness, and to migrate the organisation's technology to a quantum-safe state.

In understanding risk management for telecommunication systems [62], GMSA have highlighted the drawbacks of the Mosca inequality / framework in categorising assets as purely at-risk or no risk. For

example, they cite the security of Operations, administration and management / Operational Support System in 5G infrastructure as critical, since gaining control would allow threat actors to bring the network down and have access to all data being transferred. Under the Mosca methodology, this could be categorised as not at risk, but the high impact nature of these systems necessitates higher prioritisation when compared to other systems not at risk.

More generally, risk is often defined as the combination of probability and consequence, and hence any framework which determines risk should incorporate probabilistic inputs. Mosca's inequality is lacking in this aspect – in practice we should expect (at least) the variables Y and Z to be subject to a significant amount of uncertainty.

Under the CARAF framework [63], this risk is given a threat level corresponding to the combination of risks for X, Y, Z (low-medium for the given example). However, GMSA raise concerns that this framework ignores risk transference i.e., allowing a third party to take cover the risk, and recommend the addition of an analysis phase to understand the effectiveness of mitigation strategies and identification of remaining risk.

Timeline (in years)	1 – Low risk	2 – Medium risk	3 – High risk	4 – Critical
X (shelf-life)	5	10	20	20+
Y (mitigation)	0-5	6-10	11-20	20+
Z (threat)	20+	10-20	5-10	0-5

Table 2 - Risk scoring for the Mosca methodology in the CARAF framework. Adapted from [63]**,** Table 4.

4.3 Governmental strategy

In transitioning towards quantum-safe cryptography, extensive guidance and programmes are being provided by a number of governments, as well as by industry [62], [64], [65], [66], [67], [68], [69]. As shown by Table 3, most countries are primarily considering the NIST PQC algorithms [43] for implementation, with much of the planning dependent on the outcome of the NIST standardisation process. It expected that NIST will produce a number of standards for PQC schemes covering a range of application areas including public key exchange and digital signatures. The initial standards are expected to be published this year followed by a regular review process.

Country	PQC algorithms under consideration	Published guidance	Timeline (summary)
Australia	NIST	PROTECT (2023) [70]	Start planning; early implementation
Canada	NIST	Cyber Centre (2021) [71]	Start planning; implementation from 2025
China	China-specific	CACR (2020) [72]	Start planning
European Commission	NIST	ENISA (2022) [73]	Start planning and mitigation
France	NIST (but not restricted to)	ANSSI (2022) [74]	Start planning; transition from 2025
Germany	NIST (but not restricted to)	BSI (2022) [75]	Start planning
Japan	Monitoring NIST	CRYPTREC [76]	Start planning; initial timeline
New Zealand	NIST	NZISM (2022) [77]	Start planning
Singapore	Monitoring NIST	MCI (2022) [78]	No timeline available
South Korea	KpqC	MSIT (2022) [79]	Start competition. First round (Nov 22 – Nov 23)
United Kingdom	NIST	NCSC (2020) [66]	Start planning;
United States	NIST	NSA (2022) [80]	Implementation 2023-2033

Table 3 - Summary of post-quantum programs by country. Adapted from [64], p11. Section 5; references to 'Published guidance' have been added where it was deemed to be the original source or equivalent.

Following the methodology of Mosca and Mulholland [58], [59], (see Section 4.1), the general approach of government quantum cyberthreat initiatives is to recommend that at-risk assets should be inventoried, at a minimum recording both their cryptographic security system, and the length of time that the asset is required to be protected. This is echoed by all guidance, with the US government reportedly making substantial progress on inventorying their cryptographic systems [81].

In planning the transition towards Quantum-Safe (QS) systems, challenges across technological, organisational, and environmental contexts have been identified [82]. Subject matter experts from the Dutch government, academic and research institutions and the tech industry then characterised the most urgent challenges for Public Key Infrastructure (PKI) for the Dutch government as:

- Lack of awareness – where the current understanding of quantum computing and the relevant threats are unknown, this greatly reduces the time available to transition to QS solutions.
    - Academic research is too technical for a general audience.
    - Perception of quantum relates to commercial advantage not cryptographic threat.
- Vulnerable root certificate authentication – these certificates are used to certify programs / data etc. so if this is compromised, software can be updated with malware or override new encryption etc.
    - Fake certificates can be incredibly hard to detect if the root certificate is compromised.

    - Transiting to quantum-safe solutions is meaningless if the root certificate is compromised during the transition.
- Unclear QS governance – when there is a lack of leadership and responsibility, there is a risk that organisations will wait instead of beginning to act.
    - Need cryptographic inventory to understand the necessary updates to infrastructure and protocols.
    - Not knowing how to facilitate the transition or who is responsible for different pieces.

In a further study by the Dutch government, a number of policy recommendations are highlighted to tackle the identified challenges [83], see Table 4.

Policy category	Policy recommendations
Assessment of organisational impact and readiness	• Conduct impact assessment of quantum threats in their businesses. • Make QS implementation obliged for a certain data. • Prepare pilot testing to assess the list of PQC algorithms. • Identify different use cases for QS solutions
Collaboration in the organisational ecosystem	• Map out the current PKI environment and coordinating collaborations. • Stimulate forums & open dialogues. • Create consortiums and collaboration across sectors. • Provide subsidies to stimulate the adoption of QS solutions.
Financial incentives and funding	• Incentivize cross-sectoral research. • Extend research on more complex protocols. • Upscale the market for hardware and software.
Policy guidance	• Raise legal implications for the QS transition. • Define clear roles and responsibilities for QS transition. • Develop a vision for how to implement changes for the QS transition. • Clarify what the hybrid structure for QS solution refers to.

Table 4 - Possible policy recommendations for the QS transition. Adapted from [83], Table 4.

5 Quantifying the quantum threat and the use of resource estimation

To understand the current level of risk posed by quantum computing, we investigate the current state-of-the-art implementations of Shor's algorithm (see Section 5.1) and estimates for timelines to CRQCs based on quantum expert opinions (see Section 5.3). Finally, we explore the use of resource estimation techniques to quantify the potential time scales to break different cryptosystems, and the properties of the quantum computers required to do so (see Section 5.4). We focus here on answering:

- When should we expect cryptographically relevant quantum computers?
- Can we understand the potential length of time for an attack?
- What are the key performance indicators that should be tracked?

5.1 Section summary – Quantifying the quantum threat and the use of resource estimation

- Shor's algorithm has been experimentally demonstrated for small examples.
- Expert opinion on quantum risk is that we should worry about the 10-20-year time horizon.
- Resource estimation provides a way to realistically estimate requirements for a CRQC.
- A resource estimation by Gidney and Ekerå in 2019 [2] provides the baseline result that is widely referenced.
  - Estimated that it would take 8 hours and 20 million physical qubits to break RSA 2048.
- Algorithmic improvements have brought down the estimated required resources for a CRQC over time.
- When considering resource estimation for CRQCs, there are wide range of potential directions which could bring the requirements down and little understanding of which would have the largest impact.
- There are significant variations in estimates due to wide range of assumptions made with resource estimation.
  - There is no easy way to adjust the estimates to accommodate different range of assumptions or explore sensitivity to the assumptions.

5.2 Hardware factoring records

While the risk posed by Shor's algorithm requires a quantum computer to be realised, current hardware is too error-prone to be used to factor large numbers (see Section 6.3). The current hardware record for Shor's algorithm stands at factoring 35 on a superconducting quantum computer [84], while simulators can act as error-corrected quantum computers and have been used to factor numbers many orders of magnitude larger (see Table 5).

Year	RSA modulus	Hardware / Simulator?	Groups
2001	15	Hardware	IBM / Stanford University
2011	21	Hardware	University of Bristol
2019	35	Hardware	CUNY Graduate Center / Pakistan Academy of Science / IBM
2019	961,307	Simulator	University of Melbourne
2023	247	Simulator	Norma Inc.
2023	549,755,813,701	Simulator	Jülich Supercomputing Centre / AIDAS / University of Groningen / RWTH Aachen University

Table 5 – Faithful state-of-the-art implementations of Shor's algorithm: where minimal or no information about the solution was used to optimise the quantum circuit. Adapted from [42]

There are claims to factor larger numbers than 35 on hardware e.g., IBM and Zapata factoring 1,099,551,473,989 using a variational algorithm in 2019; however, they used significant classical pre-processing and knowledge of the solution to do so which would not be available in realistic cryptographic scenarios.

5.3 Quantum expert timeline estimates

With relatively few datapoints available, assessing the current risk can also be achieved by surveying experts in quantum computing and cybersecurity. The Global Risk Institute in conjunction with evolutionQ have produced five annual reports tracking expert opinion on the current quantum threat [85], [86], [87], [88], [89].

The 2023 report [89], contains insights from 37 respondents based around the globe including: Peter Shor, Martin Ekerå, John Preskill, David DiVincenzo, Jay Gambetta and Dorit Aharanov and from the UK includes: Elham Kashefi, and Sir Peter Knight.

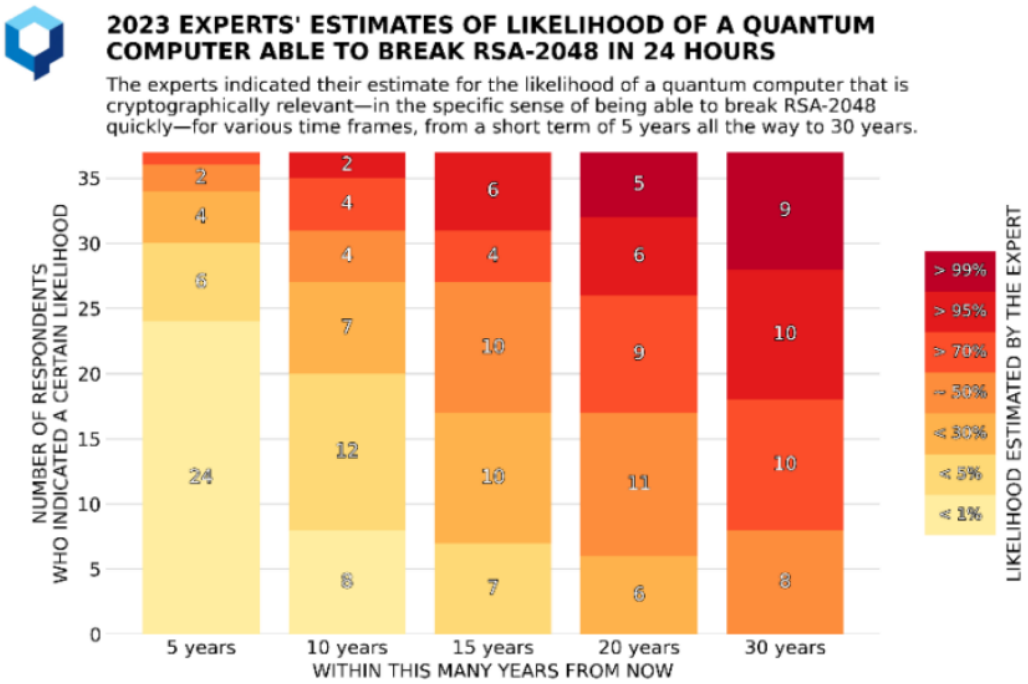


Figure 2 - 2023 experts' estimates of the likelihood of a quantum computer able to break RSA-2048 in 24 hours within different timeframes. This is a summary of responses to the question: “Please indicate how likely you estimate it is that a quantum computer able to factorize a 2048-bit number in less than 24 hours will be built within the next 5 years, 10 years, 15 years, 20 years, and 30 years”.

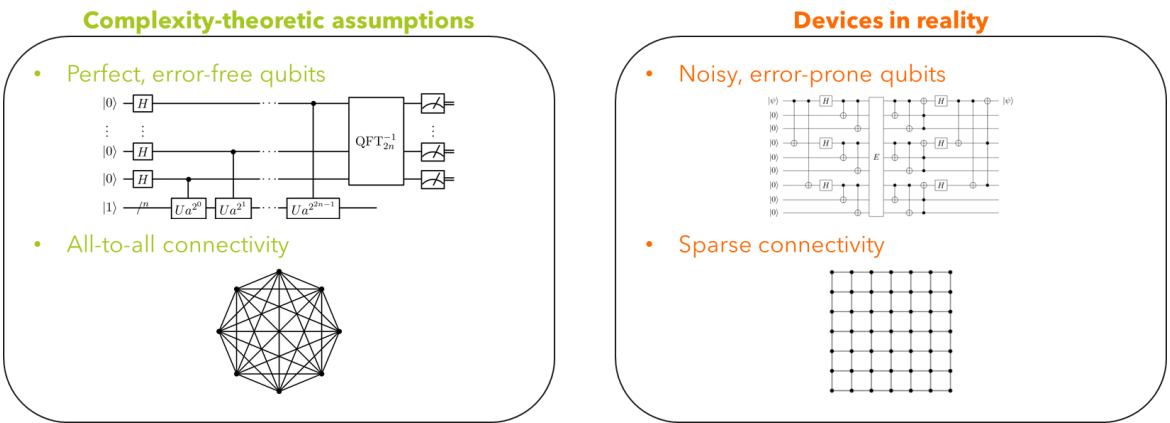
Figure 2 provides a summary of expert’s opinions on the current and future level of risk, revealing that most of the experts agree the risk to current public-key algorithms in the next 5 years is very low (<1% likely of a CRQC), but that there is a 50% likelihood or higher chance of a CRQC in the next 15 years.

The report also underscores the difficulty of estimating these timelines. There is a widely held belief that quantum computers will provide commercial value before they are cryptographically relevant that is reaffirmed by the responses. The onset of commercial value could increase investments and interest in quantum computing, resulting in accelerated timelines for key hardware improvements required for CRQCs. Suggestions for demonstrations of these improvements included: error correction, advanced logical qubit manipulation, and increased error and noise suppression. However, these suggestions also highlighted that these improvements would be different across different quantum computer modalities (see Section 6.1) i.e., judging the risk of CRQCs is unlikely to be achieved by quantifying the risk of a single modality.

5.4 Resource estimation

Resource estimation is the careful estimation of the physical quantum resources and wall-clock time required to execute an algorithm in practice and is essential in estimating the threat that quantum algorithms will have on modern cryptography. Whilst understanding how the algorithms run and surveying experts can provide a rough estimate of the time to threat and key indicators for algorithms and hardware, a thorough and rigorous end-to-end analysis of the resources required to execute an algorithm on hardware provides the most realistic estimates for cryptographic attacks.

So far, we have considered the quantum algorithms to be implemented on idealised devices, where for example, the quantum computers we have access to are error-free and any qubit can interact with any other



qubit. This is not the case for current quantum computers and will not be the case for the first CRQC.

Figure 3 - Theory-based assumptions versus practical reality of implementing algorithms on quantum computers.

Resource estimation allows us to simulate the possibility of a quantum threat by considering both the algorithmic model and the hardware model of the system.

The algorithmic model may consist of:

- The cryptosystem under attack e.g., RSA-2048, ECDH P-256 (see Section 2.2).
- The variant of the algorithm used e.g., Regev's algorithm (see Section 3.2.2), Chevignard's algorithm (see Section 3.2.3).
- Any classical pre / post-processing required.

The hardware model may consist of:

- The type / modality of quantum computer (see Section 6.1).
- The error correcting code (see Section 6.3).
- Connectivity constraints e.g., all-to-all vs nearest-neighbour grid.
- Gate application times / clock speed.

These models can be jointly optimised to understand the impact of the assumptions in producing credible threats:

- The time-to-solution – how fast can we break a single cryptosystem, and how fast can we break subsequent instances of the same system? What requirements does this put on the continuous operation of the quantum computer?
- The number of qubits – how many logical qubits and corresponding physical qubits does a computer need?
- The number of gates – how many 2-qubit gates, T gates, and total gates are required?

A dynamic resource estimation framework incorporating this modelling can provide valuable insight into:

- Basic threat assessments – given a specification for a quantum computer, is this quantum computer able to break a cryptosystem?
- Identification of key hardware indicators / limitations – given a specification for a quantum computer, what specific hardware improvements would be needed to be able to break a code and which improvements provide the biggest resource gains?
- Worst-case scenarios – the simulation can be optimised against credible current and future estimates of technology to inform relative risk levels e.g., for the Mosca inequality (see Section 4.1).
- Trade-off understanding – many quantum algorithms can trade computation speed for the number of logical qubits required, some threat models may come online earlier than others if they can exploit this.
- Algorithmic / error code improvement modelling – Improvements to either the algorithmic models or the error correcting codes can be modelled without requiring real-world progress e.g., what if the number of physical qubits per logical qubit was significantly reduced?

5.4.1 Gidney and Ekerå's resource estimation

In 2021, Gidney and Ekerå produced a comprehensive analysis of the estimated resources required to factor RSA numbers on a quantum computer [2]. Their construction assumes a planar grid of qubits with nearest-neighbour connectivity and a gate error rate of 10^{-3}. Combining several optimisations of Shor's algorithm and using the surface code [90] for error correction (see Section 6.3), Gidney and Ekerå estimate that 20 million qubits suffice for factoring 2048-bit RSA numbers (semiprimes). Under reasonable assumptions about

hardware speeds and the clock speed overhead introduced by the surface code, they estimate the factorisation to take about 8 hours on average.

As part of their work, Gidney and Ekerå compare their estimate against previous work for the same sized problem (see Table 6). Fundamentally, all these studies are based on the same algorithm but have had different levels of optimisation and fine tuning. As can be seen in the table, this has led to steady decrease in the require number of qubits and time-to-solution, highlighting the potential that algorithmic improvements can have in accelerating the path to CRQCs.

Resource estimation method	Physical qubits (millions)	Expected runtime (days)
Van Meter et al. 2009	6500	410
Jones et al. 2010	620	10
Fowler et al. 2012	1000	1.1
O'Gorman et al. 2017	230	3.7
Gheorghui et al. 2019	170	1
Gidney & Ekerå 2019	**20**	**0.31**

Table 6 - Resource estimates to factor an RSA-2048 instance by Gidney & Ekerå compared to previous estimates. Adapted from [2].

It is worth noting that their assumptions about the hardware are based on reasonable expectations for the architecture of future large-scale superconducting qubit platforms, but this is only one of many methods for realising quantum computation and it is impossible to know which platform(s) will eventually prevail. In particular, other platforms may differ drastically across a range of parameters including gate error rates, gate times, connectivity. These will likely affect both the qubit count and total runtime estimates reported by Gidney and Ekerå.

It is also important to keep in mind that this only an estimate on the resources needed to execute Shor's algorithm, given the state of algorithms and beliefs about hardware parameters at the time the work was completed. Developments in both the theory of quantum factoring algorithms and quantum error correction may reduce the resource requirements further. In fact, since Gidney and Ekerå's resource estimation in 2021, there have been several developments in the theory of quantum factoring algorithms which may have the potential to reduce the resource requirements for factoring; namely Regev's algorithm (see Section 3.2.2) and Chevignard's algorithm (see Section 3.2.3). Since analysis of these algorithms thus far is mostly asymptotic, it is currently unknown whether they will be able to reduce resource requirements in practice.

Regarding the time to solution, an important consideration is that 8 hours is the expected runtime. Both the classical and quantum parts of Shor's algorithm succeed probabilistically, which induces significant variance in the running time. In other words, an attacker who gets sufficiently 'lucky' may break an RSA-2048 instance in far less time than 8 hours in practice.

5.4.2 Elliptic curve resource estimation

Research into breaking elliptic curve cryptosystems is underdeveloped compared to that for breaking RSA, so there are far fewer resource estimations available. Concerningly, however, resource estimates [91], [92] for these problems consistently demonstrate far lower numbers of qubits are required to break elliptic curve schemes, compared to what is needed to break an equivalent level of security for RSA (see Table 7).

Security Strength (minimum)	RSA (Google / KTH Royal Institute of Technology / Swedish NCSA)			Elliptic curve (Korea University)		
	Key length	# Physical qubits	Runtime (rounded up)	Key length	# Physical qubits	Runtime (rounded up)
112	2048	20 million	8 hours	224	4.63 million	47 days
128	3072	38 million	14 hours	256	5.81 million	63 days
192	8192	140 million	4 days	384	8.32 million	261 days
256	16384	270 million	19 days	521	12.3 million	705 days

Table 7 - Resource estimates of physical qubits and runtime to factorise RSA numbers and compute elliptic curve discrete logarithms. Adapted from [2], Table 3 and [92], Table 3.

While the number of physical qubits required to break current elliptic curve schemes is typically much smaller than that for RSA, the runtimes are several orders of magnitude longer, due to the complexity of the quantum circuits required. This increase in circuit complexity is also responsible for the difficulty in transferring optimisations from Shor's factoring problem.

Some security can be recovered by increasing the key size for discrete logarithms in general, as demonstrated by the resource estimates for the base discrete logarithm problem by Gidney and Ekerå [2]. They estimate 20-26 million noisy qubits would take 1-8 hours to break a 2048-bit key Diffie-Hellman scheme depending on the variant of the discrete logarithm algorithm implemented. For certain use-cases, this may be enough to allow continued use of seemingly compromised algorithms if the private key is refreshed regularly enough.

The estimates above assume access to a generic superconducting quantum computer (see Section 6.2.1) and can dramatically change when further specialised to consider so-called cat qubits [93]. Table 8 summarises a combination of improvements from three different sources across two different sub-modalities of quantum computer, two different error correcting code types, three different algorithms, and numerous less-obvious differences.

Superconducting qubit type	RSA-2048		Elliptic Curve P-256	
	# Physical qubits	**Runtime (rounded up)**	**# Physical qubits**	**Runtime (rounded up)**
Generic	20 million	**8 hours**	12.3 million	705 days
Cat qubits (extra resistance to bit-flip errors)	**0.35 million**	4 days	**0.13 million**	**9 hours**

Table 8 - Resource estimates for breaking representative asymmetric cryptosystems with different superconducting qubit types. Adapted from [2], [92], [93] for the generic RSA-2048, generic Elliptic Curve P-256, and cat qubit statistics respectively.

These comparisons highlight that resource estimation is a multifaceted problem, containing complex interplay between physical qubit number, error rate and connectivity. Without a unified framework or specification for resource estimation, comparison is extremely challenging due to the different assumptions in implementations.

6 Hardware progress

In resource estimation (see Section 5.4), we have been provided with a guide to some quantities that are important to consider for the timeline to CRQCs: physical qubits and logical qubits. Here, we investigate the current state of the art in quantum computers (see Section 2) and the roadmaps given by industry in addition to the error correction methods that produce logical qubits from physical qubits (see Section 3).

6.1 Section summary – Hardware progress

- Qubit counts are growing rapidly: doubling about every 18 months.
- Quantum hardware companies have published ambitious hardware roadmaps which if achieved will accelerate the path to CRQCs.
- Tackling errors through quantum error correction is key to reaching useful and valuable quantum computers.
- Quantum error correction is currently receiving significant academic and industrial attention leading to exciting recent progress in improved codes with lower overheads.
- Improvements to the classical support processes for quantum error correction (decoders) has brought down clock speed overhead, allowing quantum computers to run faster.
- Understanding the quantum threat requires tools that can rapidly adapt to both algorithmic and hardware advances.

6.2 Industry roadmaps

Although still far from being able to execute Shor's algorithm on integers of practical relevance [84], [94], there have been significant advances in the development of quantum computing hardware in recent years [95]. The most promising platforms for the realisation of digital quantum computation include neutral atoms [96], trapped ions [97], [98], [99], superconducting qubits [100], [101], [102], and photonic qubits [103], [104], [105]. In this section we review the current state-of-the-art quantum computing hardware and its expected future growth as forecast by several quantum computing hardware manufacturers.

6.2.1 Superconducting qubits

As of the latest information available, IBM own the largest superconducting-qubit quantum computer: the IBM Condor, at 1121 qubits [106]. Last year, IBM announced their plan to build a 100,000-qubit quantum computer by 2033 [107] and laid out a more detailed roadmap in [108]. In particular, they aim to build a fully error-corrected machine with the capability to execute circuits with fault tolerance on up to 2,000 logical qubits and 1 billion gates.

Rigetti Computing is a developer of quantum integrated circuits also primarily focussing on development with superconducting qubits. The latest information available states that Rigetti plans to build quantum computers with 1,000 and 4,000 qubits by 2025 and 2027, respectively [109].

Google is also noteworthy for their involvement in developing superconducting quantum processors. As of the time of writing, their latest computer Sycamore, which was made public in 2019 and has 53 qubits [110].

6.2.2 Trapped ions

Notable quantum computing companies investing in development using trapped-ion qubits include Quantinuum and IonQ, which possess quantum processors with up to 36 qubits [111], [112]. Quantinuum's previous-generation H1-1 currently holds the record for the highest recorded quantum volume (a metric for measuring the performance of quantum computers [113]) at 524,288 [111].

IonQ's current roadmap is stated in terms of 'algorithmic qubits', a benchmark for assessing performance which includes gate fidelity. In particular, they aim to achieve a processor 64 algorithmic qubits by 2025 [114]. It is worth noting that algorithmic qubits have received criticism as a benchmark for assessing performance [115].

6.2.3 Neutral atoms

In [116], neutral atom-based quantum computing company QuEra outline a three-year roadmap with the eventual goal of building an error-corrected quantum computer with 100 logical qubits by 2026. They envision a three-phase release of their quantum computers over the following three years with 10, 30, and 100 logical qubits realised using over 256, 3,000, and 10,000 physical qubits, respectively.

Recently, quantum computing company PASQAL announced a roadmap to create a device with 10,000 physical qubits by 2026 and a fully fault-tolerance device able to execute circuits on up to 128 logical qubits by 2028 [117].

In [118], Infleqtion unveil their five-year roadmap to deliver commercial-ready quantum computing. Notably, their plan includes the realisation of 10 logical qubits by 2026 and 100 by 2028, using 8,000 and 40,000 physical qubits, respectively.

As of the time of writing, Atom Computing has developed the largest neutral atom quantum computer at 1,225 qubits [119]. As far as we know, Atom Computing has no publicly published roadmap for the development of their hardware.

6.2.4 Photonic qubits

We could not find any roadmaps from quantum computing companies involved in development using photonic qubits. Notable companies in this area include PsiQuantum, Xanadu, ORCA, Quandela and Photonic Inc. To the best of our knowledge, the current largest photonic quantum computer is Xanadu's Borealis, at 216 qubits [120]; however, Borealis is not a universal quantum computer and is thus incapable of executing Shor's algorithm.

6.3 Quantum error correction (QEC)

Given the key role QEC plays in the deployment of CRQCs, recent developments in both code and implementations can have a significant effect on the required specifications for a CRQC. For example, a number of alternative coding schemes in development show the promise of reducing the physical qubit overhead by a factor of 100 or higher. For further information about QEC see [1], [121].

6.3.1 Experimental demonstrations

In recent years, several quantum hardware companies have carried out practical demonstrations of quantum error correction on their computers. These experiments have demonstrated that the theoretical ideas from QEC can be leveraged in real quantum computers and applied in practice. Initial experiments focused on error detection and quantum memory i.e., maintaining a quantum state, often coding schemes that do not scale; notable examples include the work by [122]. Since these experiments, we have seen experiments using the surface code, see [90], [123], the current front runner for practical implementations, by quantum hardware companies and research groups including Google [124] and ETH [125]. While the early experiments created a single logical qubit, we have recently seen experiments generating multiple logical qubits in addition to entangling operations on the associated logical qubits, see for example Quera [126] and Quantinuum and Microsoft [127].

6.3.2 Code improvements

As mentioned above, the current front runner for implementation on real hardware is the surface code [90]. There have been some refinements proposed for this to reduce the number of qubits [128] or to adapt to specific noise models [129] but much of the development has been in decoders, see below.

Recently, there have been two significant classes of codes developed which show promise in reducing the qubit count overhead for error correction, at the cost of increased system performance. The first of these is Quantum LDPC codes, see [130] for a summary of recent work. Unlike the surface code, which has only a simple connectivity constraint, Quantum LDPC codes involve qubit connectivity, which is difficult to physically implement, generally requiring long distance links within the hardware. Recently IBM described a qLDPC code and a path for implementation on actual quantum hardware with significant reduction in the physical qubit requirements [131]. The second of these is the development of floquet codes [132], in which computation is easier but implementation is significantly more challenging.

6.3.3 Decoder improvements

Beyond qubit overhead, there is a significant clock speed overhead induced by error correction, primarily driven by the time required to identify the errors. Recent work on decoders - the classical computation side of QEC - has been focused on reducing this overhead and improving the error detection ability. This has included deployment for decoders into ASICs [133], decoders to incorporate wider information [134], and windowed schemes [135]. Understanding the effect these have on clock time and error detection efficiency is required to understand the system specification for CRQCs.

7 Gap analysis

Now we turn our attention to exploring the gaps in our understanding of the quantum threat to future energy network security, as highlighted by the literature review. Firstly, we re-examine the guiding questions from Section 1.1 and to what extent they have been addressed by the literature review. We follow this with a more detailed discussion of the identified gaps in the current literature.

The initial gap analysis was completed during the mid-phase consortium workshop held on 2nd April 2024 and then refined during the second half of this phase.

7.1 Section summary – Gap analysis

- The literature review has highlighted the significant work completed in understanding the quantum threat, but there are still several open questions and gaps that need to be addressed to provide clarity around the quantum threat.
- Significant efforts in developing algorithmic improvements to Shor's algorithm have reduced algorithmic requirements.
    - Significant optimisation has been carried out for integer factorisation, but less effort has been applied to the discrete log problem. Therefore, there are likely to be significant optimisations carried out in this case in future.
    - Larger algorithmic improvements are expected, for example Regev's algorithm (see Section 3.2.2), but these are difficult to predict.
- Quantum hardware is seeing rapid development; notably, qubit numbers are doubling on average every 18 months.
    - Qubit count alone does not give a clear picture of when CRQCs will be deployed. Other developments will accelerate this timeframe, for example connectivity and quantum error correction.
- Resource estimation of algorithmic performance has provided significant insight into both the system specification for a CRQC and the time to complete an attack.
    - However, most resource estimates are completed for a specific hardware architecture and a given set of assumptions with no clear way to update or explore alternative scenarios.
- Qubit count and gate fidelities alone are not enough to properly track the progress. A broader set of KPIs are needed to properly track the quantum ecosystem.
- Currently uncertainty is not properly captured in the risk frameworks and accurately capturing this is important for making mitigation decisions.

7.2 Review of the key questions with regards to the literature review

As with the rest of this report, this gap analysis will be guided by the questions of particular relevance for energy systems as discussed in the Introduction (see Section 1.1). Here we consider how the literature review has answered these questions, but also highlight when they have not been addressed.

What is the quantum threat to the cryptographic schemes?

The existing literature provides a comprehensive answer to this question (see Section 3 for details). Despite many algorithmic developments over the last few decades, the main algorithmic threat still comes from Shor's original 1994 algorithm and its derivatives. Most widely used public-key protocols, such as RSA and Diffie-Hellman, are under threat due to their reliance on the integer factorisation and discrete logarithm problems which are both broken by Shor's algorithm.

In comparison quantum attacks on symmetric-key cryptosystems, for example AES, by using Grover's algorithm are generally considered to be ineffective, leading the community to believe symmetric cryptography is still safe from quantum attacks (see Section 3.3).

What activities are being carried out within wider society with regards to the quantum threat?

We have reviewed the most relevant government reports in Section 4.3. Most countries seem to be awaiting NIST standardisation, with others hosting internal competitions to develop further PQC protocols. The United States is currently leading the charge through NIST with regards to PQC implementation. Note a number of private companies have already started incorporating PQC protocols into their software [136]. Furthermore, we have found industry and government reports highlight the societal challenges of delivering cryptographic change and the need to prepare but are often otherwise light on the technical detail.

While a significant portion of work has begun on building risk assessment frameworks, inventorying cryptosystems, and raising awareness of the quantum threat, there is a significant gap in understanding the time before a threat is realised. There is significant academic literature on quantum resource estimations required to break cryptosystems, but to our knowledge this has not been sufficiently translated to the Mosca framework.

How long until we expect CRQCs for current cryptographic standards?

Although it will be impossible to answer this question with complete certainty until the realisation of CRQCs, many attempts have been made in the literature to estimate this timeframe. These estimates may arise from querying expert opinions (Section 5.3), resource estimation (Section 5.4), and extrapolating hardware roadmaps (Section 6.1). It is known that a wide of factors affect the timeframe for the realisation of a CRQC, including: algorithmic developments (Section 3.2.2 and Section 3.2.3); hardware connectivity and associated error rates (Section 6.1); and quantum error correction schemes (Section 6.3). What is less well understood is how these various factors will shorten the timeframe in practice.

Now moving to consider, the question of how long an attack takes, we see there have been a number of efforts including the widely used baseline of 8 hours quoted in [2] (see Section 5.4.1). Again however, there is significant variability in the estimates produced in the literature highlighting the heavy dependence on the assumptions. There is a lack of tools to properly explore the effect of the assumptions on these times. Furthermore, there has been significant optimisation of Shor's algorithm applied to factoring but the application to discrete log has received significantly less attention leading to unquantified uncertainty and unreliability in the estimates produced.

The question of when an industry needs to react to the quantum threat is partially answered by risk assessment frameworks such as Mosca's inequality (Section 4.1), which categorises assets as being either at risk or not at risk based on their remaining lifespan, the time to migrate to a new cryptosystem, and the timeframe for the realisation of a CRQC. This provides an easily interpretable rule of thumb but at the expense of being simplistic and not necessarily capturing important nuances. Furthermore, there is a significant amount of uncertainty in practice, which Mosca's inequality is currently unable to accommodate. This is particularly problematic when making mitigation decisions because uncertainty needs to be accounted for.

What system specifications are required for a CRQC?

How much the cutting-edge quantum algorithms can reduce resource requirements in practice remains a significant open question in the literature. Recent algorithmic developments such as Regev's algorithm (Section 3.2.2) have been properly explored with regards to their resource requirements. Furthermore, there is no clear understanding of how improvements in quantum error correction will influence resource estimates. Some speculative predictions may be made by observing how previous improvements in error correction have affected requirements (see Table 6), but no comprehensive analysis of Shor's algorithm has been carried out.

A fundamental limitation of resource estimates such as [2] is that they assume one specific hardware architecture throughout. Although some exploration into various hardware architectures has been considered in the literature, currently there is no straightforward way to adapt existing estimates to account for changes in assumptions about the hardware.

How do we track progress within the quantum industry?

From our research we have not come across any comprehensive framework for tracking the cryptographically relevant development of quantum computers and predicting potential future progress. Generally, frameworks only track simple statistics, for example qubit count and fidelity but the literature clearly indicate this is not enough to gain full picture of progress in quantum hardware. There is a gap that can be filled by framework that captures a richer set of performance indicators which can be used to provide clear insight into the rate at which CRQCs are being developed.

According to the publicly available information, the cutting-edge hardware developments are being made primarily by academic and industrial institutions based in North America and Europe (see Section 6).

What mitigations against the quantum threat are available to the energy industry?

We have found the dependence of cryptographic protocols on key size to be well-studied in the literature, see for example Table 1 but as discussed above they can be highly dependent on the assumptions made. The cost of upgrading cryptosystems is highly dependent on the context of how the cryptosystem of interest is deployed, for more detail see the companion report (Cybersecurity Analysis). For cryptosystems present in consumer-level software we expect eventual NIST standardisation and for the upgrade cost to be negligible, whereas more application-specific systems may be far less trivial to upgrade, for more details see the companion report (Cybersecurity Analysis).

7.3 Tracking technological advances

Despite many incremental improvements and optimisations over almost 3 decades, the fundamental structure of Shor's algorithm has remained largely unchanged; that is, until Regev's recent work (see Section 3.2.2) which provides an asymptotic decrease in the resource requirements for factoring. A sudden significant improvement upon such a well-established algorithm serves as an indicator that there may yet be further developments to be made which unexpectedly and suddenly bring the quantum threat closer.

Beyond the development of novel algorithms, the literature review highlights that Shor's algorithm applied to factoring has received significant attention and optimisation, but this is not true of the application to the discrete log problem. This is especially true of the discrete log problem over an elliptic curve, where many of the refinements of Shor's algorithm do not immediately transfer across but require effort to incorporate. This means that there are likely to be significant improvements to algorithmic performance for this problem which have yet to be realised. This is particularly important as in recent years we have seen a general shift away from RSA (factoring based) to ECC (elliptic curve discrete log based).

Whilst physical qubit counts in devices have historically roughly increased according to a Moore's law (doubling every 18 months), the vastly differing technologies and research directions in developing quantum computing hardware make it very difficult to confidently forecast the time until the realisation of a CRQC. If qubit count continues to grow with Moore's law, then we should expect to see a quantum computer with the 20 million physical qubits required by Gidney and Ekerå's resource estimation by around 2045. Though it is important to note that qubit count alone is not enough; the error rate might not be low enough to run the required circuits. The reality, however, is that we will likely see a CRQC sooner than this due to a large range of potential improvements including algorithmic, error correcting codes, error rates, and connectivity.

7.4 Resource estimation challenges

It is important to reiterate that the current state-of-the-art resource estimates for the execution of Shor's algorithm (see Section 5.4) only establish upper bounds on the necessary physical resources. Gidney and Ekerå's resource estimation (Section 5.4.1) is now almost five years old and there have since been developments both in quantum factoring algorithms and quantum error correction which are not incorporated. In particular, both Regev's algorithm (Section 3.2.2) and Chevignard's et al.'s improvements (Section 3.2.3) purportedly reduce the resource requirements for factoring, but in both cases the current analysis is primarily asymptotic and it is unknown if and by how much they improve performance in practice, for example to factor 2048-bit RSA numbers. Furthermore, the static nature of academic papers means that it can be a number of years until the consequences of algorithmic developments are explored and understood.

There is also currently no resource estimation carried out for hypothetical 'best-case' hardware; all resource estimates thus far rely on reasonable assumptions about future hardware but given the rapid advancements of quantum computing hardware and vastly varying infrastructures, it is possible that the first CRQC uses an infrastructure differing to that of the currently leading technologies. For example: what resources would be required to break RSA-2048 on a hypothetical quantum computer which combines the gate speed of superconducting devices with the all-to-all connectivity of ion trap computers and extremely high coherence times of neutral atoms? These types of questions, establishing 'realistic' lower bounds, are currently unanswered in the literature.

Central to all is the highly dynamic nature of these estimates, in the sense that the resource estimates can change drastically depending on hardware architecture, algorithmic schemes, error correcting codes, etc. Thus far, all resource estimates for Shor's algorithm have been carried out 'statically' assuming a particular

algorithm, error correcting code, etc., but provide no framework for updating the estimates if any of the parameters were to change.

7.5 Performance indicators

A key performance indicator (KPI) is a type of measurement for evaluating the performance and development rate of a particular field or technology [137]. Currently only a small number of relatively simple metrics are tracked, for example qubit count and gate fidelity but we have seen from the resource estimation work these are inadequate to properly track hardware progress.

This highlights the need for a more comprehensive framework of KPIs for tracking hardware development. A potential direction may be through the development of benchmarks particularly tuned to the execution of Shor's algorithm. The definition of such KPIs would give us warning signs and subsequently preparation time for the quantum threat; yet there is currently no well-established set of said KPIs in the literature.

7.6 Incorporating uncertainty estimates

An important aspect regarding the decision-making around the quantum threat which is often unaddressed in the literature is the significant uncertainty present in the field, including the timeframe for the realisation of a CRQC and the physical / temporal resources needed to break encryption. Optimal decision-making as to the updating of cryptosystems should incorporate the uncertainty in one's beliefs, rather than naively relying on the assumption that cryptosystems will be broken by CRQCs at some fixed point in the future. Parallels may be drawn to uncertainty models and how they drive decision-making in fields such as climate modelling [138].

Consider for example the Mosca framework (Section 4.1). Recall that, at the highest level, Mosca's inequality states that an asset is at risk if X + Y > Z where:

- X – the remaining lifespan of the device or data.
- Y – the time required to mitigate the threat and migrate to a new system.
- Z – the time to a realisable threat; the time to a CRQC.

Although theoretically offering a convenient yes / no answer as to whether an asset is at risk, in practice the variables present in Mosca's inequality may be subject to a significant amount of uncertainty, which Mosca's framework currently offers no straightforward way of incorporating.

8 Recommendations

The mid-phase consortium workshop held on 2nd April 2024 included a prioritisation session to gauge the consortium's priorities re what future activities would be most impactful in bridging the identified gaps in understanding the quantum threat. The major recommendations of areas for high-impact future activity were:

- Building a 'quantum threat tracker' tool based on dynamic resource estimation tool to allow rapid exploration of potential security scenarios, incorporating:
  - Modularity, to allow easy updates when new advances in algorithms / hardware are announced. This could allow estimation around current PQC algorithms or other future cryptographic algorithms.
  - Uncertainty, to aid decision support systems and make better judgements on current and future risks.
  - Energy-specific scenarios, to ensure the high-impact scenarios for the energy sectors are explored instead of scenarios where an 'off-the-shelf' PQC solution would mitigate the threat.
- Obtaining greater understanding of the energy-specific scenarios:
  - Mapping the energy-specific uses of cryptography, and the cost of changing these.
  - Identification of the critical systems and longest lifespan assets, and quantification of the risks.

There were also further recommendations to consider:

- Cost and adoption:
  - What are the predicted costs of mitigating the threat?
  - Whether some mitigation strategies are suitable for introduction an early stage as a preventive measure before a full analysis is performed.
  - Overreliance on a small number of PQC algorithms could increase risk if a significant security flaw is discovered. Do some of the proposed but discarded PQC algorithms still hold security under relevant conditions like short time scales?
- The suitability of Mosca's inequality (see Section 4.1), and whether a more mature solution is required.

A central theme running through these recommendations is the value of building a flexible tool to help energy system stakeholders understand the timescales of relevant quantum threat aspects, and the impact of specific mitigations against the uncertainty of current and future developments, in order to aid decision making.

To meet this need, we propose that the consortium (with the support of additional partners as relevant) should undertake to specify and develop a dynamic resource estimation software tool that can operate:

- As a stand-alone tool.
- Within a novel risk framework, building on Mosca's inequality.

8.1 Quantum threat tracker tool design

As identified in Section 5.4, a flexible resource estimation tool can be used to generate valuable and timely insights into credible quantum threats. Due to the rapid pace of developments in algorithms and hardware, it is also necessary that the system be modular to facilitate up-to-date estimates of the timescale to CRQCs. This includes systems to integrate a range of traceable sources of updateable uncertainty: expert insights, industry roadmaps, and estimates from current and past quantum systems. In operating as a stand-alone tool, the resource estimator is designed from the ground up for modularity, ensuring it can answer the relevant questions for assessing risk without being coupled to functionally irrelevant risk model updates.

A potential structure for this tool is given in Figure 4 and explained in greater detail below. This is provided as an overview of the desired features, subject to further refinement and prioritisation. This does not capture the full details of each module, which will contain further sub-modules that increase the flexibility of the tool.

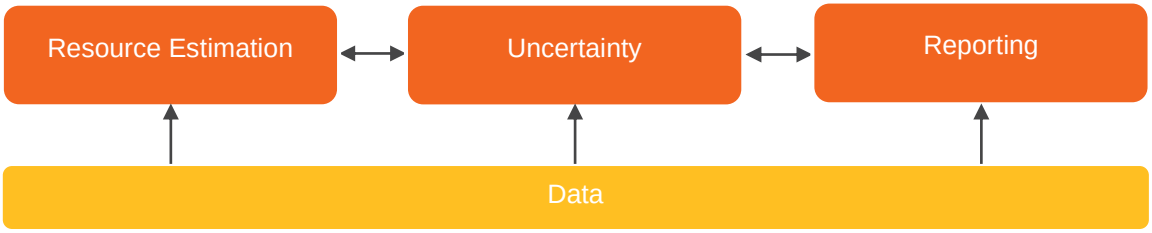


Figure 4 - Resource estimation software modular structure

8.1.1 Resource estimation module

The resource estimation module contains the tools to build resource models and generate relevant statistics.

The resource models are built from a set of primitives: an algorithmic model, a hardware model, and the error correction system that require validation to ensure they are realistic. This also includes an optimisation algorithm to ensure the least upper bound can be used as a worst-case scenario, which may be further constrained e.g., allowing only a certain set of error-correcting codes.

From this model, a range of statistics of interest can be generated e.g., the time-to-solution, number of physical / logical qubits required. The statistics will depend on how much of the base model is specified and may not require the full optimisation algorithm to run, for example, if the user only wants to understand the number of logical qubits required.

8.1.2 Uncertainty module

Quantifying the uncertainty in the resource estimates is essential for any decision support system, allowing more realistic estimates of the risks that quantum computing will present. This module should be able to process user-defined confidences for different parts of the resource estimation and allow modelling of ‘What if?’ scenarios where some quantities are unknown, by using historical data and industry roadmaps.

8.1.3 Reporting module

The reporting module allows the user to query the software to respond to a range of questions designed to understand different risk levels to benchmark cryptosystems. In order of increasing difficulty, the primary questions for a cryptosystem are:

1. Can a current quantum computer break this cryptosystem?
2. What would it take for a quantum computer to break this cryptosystem? This identifies KPIs for general or specific systems.
3. When could we expect a quantum computer to break this cryptosystem? This integrates directly with the uncertainty module to generate estimates.

This should also be able to explicitly expose the assumption modelling in generating estimates, so the effects of uncertainty can be seen. Greater analysis of this data will allow determination of the most impactful sources of uncertainty, and prioritisation of which sources should be studied to reduce uncertainty.

8.1.4 Data

The data in the system allows for explicit traceability of assumptions as well as records of the relevant KPIs for quantum threats to cybersecurity. It is expected that this will include:

- Historical hardware statistics – to allow basic extrapolation models with uncertainty modelling and act as a baseline for current quantum computers.
- Industry progress / roadmaps – to understand how quantum computers might expect to behave in the future.
- Expert uncertainty quantifications – to supplement the industry progress / roadmaps data.

8.1.5 Additional considerations

Beyond the structure outlined above, it may be desirable in future to add a UI to the software to enable greater dissemination. It is likely that the resource estimation tool will be designed for use primarily by a quantum expert but should have the capability to demonstrate a number of core default scenarios e.g., timelines to breaking RSA-2048 or ECC-224 for non-technical users.

8.2 Novel risk framework

A key use of the quantum resource estimation within the context of cybersecurity, is the application to risk modelling. The framework consists of both the methodology: completing risk assessments and understanding mitigations, as well as the software that implements those methods. In this report, we focus on the software aspect in relation to the resource estimation, with recommendations around the approaches to managing risks covered by the companion report (Cybersecurity Analysis).

In separating the tooling into risk framework and resource estimation, we allow non-quantum experts to make use of the learnings without needing to significantly upskill in quantum algorithms. Instead, this framework looks to generalises Mosca's inequality, with the resource estimation providing the input 'Z' – the time to quantum threat for a given scenario.

As discussed earlier (see Section 4.1), Mosca's inequality has a number of drawbacks, as it quantifies neither the uncertainty nor the level of individual threats. However, it remains an easily interpretable tool that aids understanding and education with regards quantum threat, so provides a good starting point.

In proposing and evaluating mitigation strategies, these too can be understood by the Mosca inequality. In essence, given an asset where we know the current values 'X, Y, Z' we could choose to:

- Reduce 'X' (lifespan of current scheme) – for some applications we can choose to generate new cryptographic keys at a faster rate.
- Reduce 'Y' (time to implement a mitigation) – some mitigations and / or assets may require significantly less effort to transition to quantum.
- Increase 'Z' (time to CRQC) – increase the security of the cryptosystem against quantum computers by e.g., increasing key length, using PQC algorithms or hybridised schemes.

Each mitigation will affect the threat level and incur a cost to implement. The adaptability of the resource estimation allows a range of these mitigation strategies from a taxonomy to be generated and studied for different assets, in addition to updating threat assessments based on, for instance, new hardware announcements and breakthroughs.

Uncertainty management will also be integrated into this framework, allowing a more refined Mosca's inequality when combined with the uncertainty metrics from the resource estimation. This will enable a better understanding of which assets are at the highest risk, and insights into the relative likelihood different scenarios of interest.

As the purpose of this framework is to support users in making decisions, clear visualisations of the results are vital, so will require significant interaction with the end-users to inform the design.

9 Glossary

Application-specific integrated circuit (ASIC)	An integrated circuit chip design for a single use case.
Asymptotic Notation	A family of mathematical notation which describes the behaviour of functions as the input gets large. See Section 2.3.
Boneh–Lynn–Shacham (BLS)	A digital signature scheme allowing users to authentic both the signature and signer.
Classical Computer	A conventional non-quantum computer, such as widely used laptop and desktop computers.
Clock Speed	The frequency at which a (quantum) processor is able to execute instructions.
Computational efficiency	The computational resource required to complete a calculation.
Connectivity	A description of how the qubits are connected in a quantum computer.
Cryptographically Relevant Quantum Computer (CRQC)	A quantum computer with the capability to break currently used cryptographic protocols.
Diffe-Hellman (DH)	A public key cryptosystem which relies on the difficulty of the discrete log problem.
Digital signature	A digital version of a signature which allows the sender of a piece of information to be authenticated.
Digital Signature Algorithm (DSA)	A specific algorithm for authenticating the sender of information.
Discrete log problem	The mathematical challenge of finding the exponent, a, to solve $g^a = b$ in given finite group, for known g and b.
Elliptic Curve Cryptography (ECC)	A method of public key cryptography based on elliptic curves which allows for smaller key sizes when compared to non-ECC schemes.
Elliptic Curve Diffe-Hellman (ECDH)	An elliptic curve-based version of the DH cryptographic scheme, an example of an ECC.
Elliptic Curve Digital Signature Algorithm (ECDSA)	A variant on DSA which built on ECC.
Edwards Curve Digital Signature Algorithm (EDDSA)	An alternative digital signature scheme based on twisted Edwards curves, a specific class of elliptic curve.
Integer Factorisation	The computational problem of taking a composite (non-prime) integer and outputting its prime factors.
Key Performance Indicator (KPI)	A type of measurement for evaluating the performance of a particular field or technology.
Low density parity check (LDPC) codes	A class of classical error correcting codes.
Logical (Quantum) Bit	The logical unit of information which is able to be freely programmed by the user. See Section 2.1.1.
Menezes–Qu–Vanstone (MQV)	A key sharing protocol based on DH.
National Institute of Standards and Technology (NIST)	A United States-based agency which, amongst other objectives, standardises widely used technologies including cryptographic schemes.
One-Way Function	A mathematical function which is computationally easy to compute given an input but hard to invert given an output.
Physical (Quantum) Bit	The physical units of information which encode information in the device. See Section 2.1.1.
Polynomial Time Algorithm	An algorithm which executes in $O(n^d)$ steps, where n is the size of the input and d is some positive integer.
Post Quantum Cryptography (PQC)	Cryptography consisting of protocols which are resistant to quantum attacks.
Proof of Work (PoW)	A cryptographic proof that one party has completed a given amount of computational effort (work) to another party.
Public Key Cryptography (PKC)	A class of cryptographic protocols based on one-way functions which allow users to agree upon a shared secret with no prior shared information. See Section 2.2.

Quantum Algorithm	An algorithm which runs on a quantum computer.
Quantum Approximate Optimisation Algorithm (QAOA)	A hybrid classical/quantum algorithm for solving combinatorial optimisation problems.
Quantum Bit (Qubit)	An elementary unit of information in quantum computing, generalising the binary digit (bit).
Quantum Circuit	A set of instructions defining an algorithm to execute on a quantum computer.
Quantum Circuit Depth	The total number of time steps required to execute a quantum circuit, where each time step may contain multiple quantum gates being executed in parallel.
Quantum Computer	A computer which is able to utilise quantum mechanical phenomena in its computations.
Quantum Error Correction (QEC)	A method for protecting quantum information against errors by encoding the information of logical qubits onto many more physical qubits.
Quantum Gate	An elementary instruction for a quantum computer, analogous to classical gates such as AND and NOT.
Quantum Low Density Parity Check (QLDPC) codes	A QEC code family based on ideas from classical LDPC codes.
Quantum Safe (QS) cryptography	Cryptographic schemes which are believed to be secure against attack by quantum computers.
Quantum speedup	A reduction in the computational complexity from using a quantum algorithm compared to classical algorithm.
Qubit Register	A collection of qubits.
Rivest–Shamir–Adleman (RSA)	A widely used public key cryptosystem which relies on the difficulty of integer factorisation.
RSA Number	The product of two (large) prime numbers, also called a semiprime.
Symmetric Key Cryptography	A class of cryptographic protocols which allow users to securely communicate over an insecure channel given some pre-agreed shared secret (symmetric key). See Section 2.2.
Wall Clock Time	The real-world time required to execute a (quantum) algorithm, as distinct from the concept of time in complexity theory which counts the number of operations.

10 References

[1] M. A. Nielsen and I. L. Chuang, “Quantum Computation and Quantum Information: 10th Anniversary Edition,” *Quantum Computation and Quantum Information*, Dec. 2010, doi: 10.1017/CBO9780511976667.

[2] C. Gidney and M. Ekerå, “How to factor 2048 bit RSA integers in 8 hours using 20 million noisy qubits,” *Quantum*, vol. 5, p. 433, Apr. 2021, doi: 10.22331/q-2021-04-15-433.

[3] K. Townsend, “Solving the Quantum Decryption ‘Harvest Now, Decrypt Later’ Problem,” *SecurityWeek*, Feb. 2022, Accessed: Apr. 22, 2024. [Online]. Available: https://www.securityweek.com/solving-quantum-decryption-harvest-now-decrypt-later-problem/

[4] D. L. Evans and K. H. Brown, “Advanced Encryption Standard (AES),” May 2023, doi: 10.6028/NIST.FIPS.197-UPD1.

[5] R. L. Rivest, A. Shamir, and L. Adleman, “A method for obtaining digital signatures and public-key cryptosystems,” *Commun ACM*, vol. 21, no. 2, pp. 120–126, Feb. 1978, doi: 10.1145/359340.359342.

[6] W. Diffie and M. E. Hellman, “New Directions in Cryptography,” *IEEE Trans Inf Theory*, vol. 22, no. 6, pp. 644–654, 1976, doi: 10.1109/TIT.1976.1055638.

[7] “18.783 Elliptic Curve Lectures.” Accessed: Apr. 08, 2024. [Online]. Available: https://math.mit.edu/classes/18.783/2017/lectures.html

[8] R. Laboratories, *RSA Factoring Challenge*. Accessed: Apr. 08, 2024. [Online]. Available: http://www.emc.com/emc-plus/rsa-labs/historical/the-rsa-factoring-challenge.htm

[9] E. Barker, L. Chen, A. Roginsky, A. Vassilev, and R. Davis, “NIST Special Publication 800-56A Revision 3 Recommendation for Pair-Wise Key-Establishment Schemes Using Discrete Logarithm Cryptography”, doi: 10.6028/NIST.SP.800-56Ar3.

[10] M. Adalier and A. Teknik, “Efficient and Secure Elliptic Curve Cryptography Implementation of Curve P-256,” *Workshop on elliptic curve cryptography standards*, vol. 66, no. 446, 2015, Accessed: Apr. 08, 2024. [Online]. Available: https://csrc.nist.gov/csrc/media/events/workshop-on-elliptic-curve-cryptography-standards/documents/papers/session6-adalier-mehmet.pdf

[11] A. Schönhage and V. Strassen, “Schnelle Multiplikation großer Zahlen,” *Computing*, vol. 7, no. 3–4, pp. 281–292, Sep. 1971, doi: 10.1007/BF02242355.

[12] P. W. Shor, “Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer,” *SIAM Journal on Computing*, vol. 26, no. 5, pp. 1484–1509, Oct. 1997, doi: 10.1137/S0097539795293172.

[13] R. B. Griffiths and C. S. Niu, “Semiclassical Fourier Transform for Quantum Computation,” *Phys Rev Lett*, vol. 76, no. 17, p. 3228, Apr. 1996, doi: 10.1103/PhysRevLett.76.3228.

[14] J. Proos and C. Zalka, “Shor’s discrete logarithm quantum algorithm for elliptic curves,” *Quantum Inf. Comput.*, vol. 3, no. 4, pp. 317–344, 2003.

[15] O. Regev, “An Efficient Quantum Factoring Algorithm,” *arXiv preprint arXiv:2308.06572*, Aug. 2023, Accessed: Apr. 24, 2024. [Online]. Available: https://arxiv.org/abs/2308.06572

[16] S. Ragavan and V. Vaikuntanathan, “Space-Efficient and Noise-Robust Quantum Factoring,” *arXiv preprint arXiv:2310.00899*, Oct. 2023, Accessed: Mar. 13, 2024. [Online]. Available: https://arxiv.org/abs/2310.00899v3

[17] C. Chevignard, P.-A. Fouque, and A. Schrottenloher, “Reducing the Number of Qubits in Quantum Factoring,” *Cryptology ePrint Archive*, 2024, Accessed: Mar. 13, 2024. [Online]. Available: https://eprint.iacr.org/2024/222

[18] BeauregardStephane, “Circuit for Shor’s algorithm using 2n+3 qubits,” *Quantum Inf Comput*, Mar. 2003, doi: 10.5555/2011517.2011525.

[19] Y. Takahashi and N. Kunihiro, “A quantum circuit for shor’s factoring algorithm using 2n + 2 qubits,” *Quantum Inf Comput*, vol. 6, no. 2, pp. 184–192, Mar. 2006, doi: 10.5555/2011665.2011669.

[20] T. Häner, M. Roetteler, and K. M. Svore, “Factoring using 2n + 2 qubits with Toffoli based modular multiplication,” *Quantum Inf Comput*, vol. 17, no. 7–8, pp. 673–684, Jun. 2017, doi: 10.5555/3179553.3179560.

[21] C. Gidney, “Factoring with n+2 clean qubits and n-1 dirty qubits,” *arXiv preprint arXiv:1706.07884*, Jun. 2017, [Online]. Available: https://arxiv.org/abs/1706.07884v2

[22] C. Zalka, “Shor’s algorithm with fewer (pure) qubits,” *arXiv preprint quant-ph/0601097* , Jan. 2006, [Online]. Available: https://arxiv.org/abs/quant-ph/0601097v1

[23] B. Yan *et al.*, “Factoring integers with sublinear resources on a superconducting quantum processor,” *arXiv preprint arXiv:2212.12372*, Dec. 2022, Accessed: Mar. 18, 2024. [Online]. Available: https://arxiv.org/abs/2212.12372v1

[24] C. P. Schnorr, “Factoring Integers by CVP Algorithms,” *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, vol. 8260 LNCS, pp. 73–93, 2013, doi: 10.1007/978-3-642-42001-6_6.

[25] C. P. Schnorr, “Fast Factoring Integers by SVP Algorithms, corrected,” *Cryptology ePrint Archive*, 2021, Accessed: Apr. 19, 2024. [Online]. Available: https://eprint.iacr.org/2021/933

[26] E. Farhi, J. Goldstone, and S. Gutmann, “A Quantum Approximate Optimization Algorithm,” *arXiv preprint arXiv:1411.4028*, Nov. 2014, Accessed: Apr. 08, 2024. [Online]. Available: https://arxiv.org/abs/1411.4028v1

[27] S. V. Grebnev, M. A. Gavreev, E. O. Kiktenko, A. P. Guglya, A. R. Efimov, and A. K. Fedorov, “Pitfalls of the sublinear QAOA-based factorization algorithm,” *IEEE Access*, vol. 11, pp. 134760–134768, Mar. 2023, doi: 10.1109/ACCESS.2023.3336989.

[28] T. Khattar and N. Yosri, “A comment on ‘Factoring integers with sublinear resources on a superconducting quantum processor,’” *arXiv preprint arXiv:2307.09651*, Jul. 2023, Accessed: Mar. 18, 2024. [Online]. Available: https://arxiv.org/abs/2307.09651v2

[29] M. Mosca, J. M. V. Basso, and S. R. Verschoor, “On speeding up factoring with quantum SAT solvers,” *Sci Rep*, vol. 10, no. 1, Oct. 2019, doi: 10.1038/s41598-020-71654-y.

[30] S. Boulebnane and A. Montanaro, “Solving boolean satisfiability problems with the quantum approximate optimization algorithm,” *arXiv preprint arXiv:2208.06909*, Aug. 2022, Accessed: Apr. 19, 2024. [Online]. Available: https://arxiv.org/abs/2208.06909v1

[31] E. Farhi, J. Goldstone, S. Gutmann, and M. Sipser, “Quantum Computation by Adiabatic Evolution,” *arXiv preprint quant-ph/0001106*, Jan. 2000, Accessed: Mar. 21, 2024. [Online]. Available: https://arxiv.org/abs/quant-ph/0001106v1

[32] T. Kadowaki and H. Nishimori, “Quantum Annealing in the Transverse Ising Model,” *Phys Rev E Stat Phys Plasmas Fluids Relat Interdiscip Topics*, vol. 58, no. 5, pp. 5355–5363, Apr. 1998, doi: 10.1103/PhysRevE.58.5355.

[33] R. Dridi and H. Alghassi, “Prime factorization using quantum annealing and computational algebraic geometry,” *Scientific Reports 2017 7:1*, vol. 7, no. 1, pp. 1–10, Feb. 2017, doi: 10.1038/srep43048.

[34] L. K. Grover, “A fast quantum mechanical algorithm for database search,” *Proceedings of the Annual ACM Symposium on Theory of Computing*, vol. Part F129452, pp. 212–219, Jul. 1996, doi: 10.1145/237814.237866.

[35] D. J. Bernstein, “Grover vs. McEliece,” *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, vol. 6061 LNCS, pp. 73–80, 2010, doi: 10.1007/978-3-642-12929-2_6/COVER.

[36] D. J. Bernstein, “Introduction to post-quantum cryptography,” in *Post-Quantum Cryptography*, D. J. Bernstein, J. Buchmann, and E. Dahmen, Eds., Springer Berlin Heidelberg, 2009, pp. 1–14.

[37] D. J. Bernstein, “Cost analysis of hash collisions: Will quantum computers make SHARCS obsolete?,” in *SHARCS’09 Workshop Record (Proceedings 4th Workshop on Special-purpose Hardware for Attacking Cryptograhic Systems, Lausanne, Switserland, September 9-10, 2009)*, 2009, pp. 105–116. Accessed: Mar. 25, 2024. [Online]. Available: https://cr.yp.to/hash/collisioncost-20090517.pdf

[38] “Quantum Computing and Post-Quantum Cryptography General Information.” Accessed: Apr. 08, 2024. [Online]. Available: https://media.defense.gov/2021/Aug/04/2002821837/-1/-1/1/Quantum_FAQs_20210804.PDF

[39] L. Chen, D. Moody, A. Regenscheid, and A. Robinson, “Digital Signature Standard (DSS),” Feb. 2023, doi: 10.6028/NIST.FIPS.186-5.

[40] E. Barker, “NIST Special Publication 800-57 Part 1 Revision 5 Recommendation for Key Management: Part 1-General”, doi: 10.6028/NIST.SP.800-57pt1r5.

[41] M. Ekerå and J. Gärtner, “Extending Regev’s factoring algorithm to compute discrete logarithms,” *arXiv preprint arXiv:2311.05545*, 2023.

[42] T. L. Scholten *et al.*, “Assessing the Benefits and Risks of Quantum Computers,” *arXiv preprint arXiv:2401.16317*, 2024.

[43] “Post-Quantum Cryptography | CSRC.” Accessed: Apr. 08, 2024. [Online]. Available: https://csrc.nist.gov/projects/post-quantum-cryptography/post-quantum-cryptography-standardization

[44] X. Bonnetain, M. Naya-Plasencia, and A. Schrottenloher, “Quantum Security Analysis of AES,” *IACR Transactions on Symmetric Cryptology*, vol. 2019, no. 2, pp. 55–93, Jun. 2019, doi: 10.13154/TOSC.V2019.I2.55-93.

[45] G. Brassard, P. Høyer, and A. Tapp, “Quantum cryptanalysis of hash and claw-free functions,” *Lecture Notes in Computer Science*, vol. 1380, pp. 163–169, 1998, doi: 10.1007/BFB0054319.

[46] M. Grassl, B. Langenberg, M. Roetteler, and R. Steinwandt, “Applying Grover’s algorithm to AES: quantum resource estimates,” *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, vol. 9606, pp. 29–43, Dec. 2015, doi: 10.1007/978-3-319-29360-8_3.

[47] A. Hosoyamada and Y. Sasaki, “Quantum Collision Attacks on Reduced SHA-256 and SHA-512,” *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, vol. 12825 LNCS, pp. 616–646, 2021, doi: 10.1007/978-3-030-84242-0_22.

[48] S. Fluhrer, “Reassessing Grover’s Algorithm,” *Cryptology ePrint Archive*, 2017, Accessed: Apr. 04, 2024. [Online]. Available: https://eprint.iacr.org/2017/811

[49] M. Kaplan, G. Leurent, A. Leverrier, and M. Naya-Plasencia, “Breaking symmetric cryptosystems using quantum period finding,” *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, vol. 9815, pp. 207–237, 2016, doi: 10.1007/978-3-662-53008-5_8.

[50] M. Allende *et al.*, “Quantum-resistance in blockchain networks,” 123AD, doi: 10.1038/s41598-023-32701-6.

[51] A. Cojocaru, J. Garay, A. Kiayias, F. Song, and P. Wallden, “Quantum Multi-Solution Bernoulli Search with Applications to Bitcoin’s Post-Quantum Security,” *Quantum*, vol. 7, p. 944, Mar. 2023, doi: 10.22331/q-2023-03-09-944.

[52] A. Cojocaru, J. Garay, and F. Song, “Generalized Hybrid Search and Applications to Blockchain and Hash Function Security,” *arXiv preprint arXiv:2311.03723*, Nov. 2023, Accessed: Apr. 22, 2024. [Online]. Available: https://arxiv.org/abs/2311.03723v1

[53] D. Aggarwal, G. K. Brennen, T. Lee, M. Santha, and M. Tomamichel, “Quantum attacks on Bitcoin, and how to protect against them,” *Ledger*, vol. 3, Oct. 2017, doi: 10.5195/ledger.2018.127.

[54] B. Bailey and O. Sattath, “51% Attack via Difficulty Increase with a Small Quantum Miner,” *arXiv preprint arXiv:2403.08023*, Mar. 2024, Accessed: Apr. 22, 2024. [Online]. Available: https://arxiv.org/abs/2403.08023v1

[55] D. Boneh, B. Lynn, and H. Shacham, “Short signatures from the Weil pairing,” *Journal of cryptology*, vol. 17, pp. 297–319, 2004, Accessed: Mar. 25, 2024. [Online]. Available: https://www.iacr.org/archive/asiacrypt2001/22480516.pdf

[56] A. Kate, G. M. Zaverucha, and I. Goldberg, “Constant-size commitments to polynomials and their applications,” *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, vol. 6477 LNCS, pp. 177–194, 2010, doi: 10.1007/978-3-642-17373-8_11/COVER.

[57] “Future-proofing Ethereum | ethereum.org.” Accessed: Mar. 25, 2024. [Online]. Available: https://ethereum.org/en/roadmap/future-proofing/

[58] M. Mosca, “Cybersecurity in an era with quantum computers: will we be ready?,” *Cryptology ePrint Archive*, 2015, Accessed: Mar. 26, 2024. [Online]. Available: https://eprint.iacr.org/2015/1075.pdf

[59] M. Mosca and J. Mulholland, “A Methodology for Quantum Risk Assessment,” Jan. 2017. [Online]. Available: https://globalriskinstitute.org/publication/a-methodology-for-quantum-risk-assessment/

[60] “NIST Risk Management Framework | CSRC.” Accessed: Apr. 08, 2024. [Online]. Available: https://csrc.nist.gov/Projects/risk-management/about-rmf

[61] “ISO - ISO 31000 — Risk management.” Accessed: Apr. 08, 2024. [Online]. Available: https://www.iso.org/iso-31000-risk-management.html/

[62] “GSMA | Guidelines for Quantum Risk Management for Telco - Working Groups.” Accessed: Mar. 26, 2024. [Online]. Available: https://www.gsma.com/get-involved/working-groups/gsma_resources/guidelines-for-quantum-risk-management-for-telco

[63] C. Ma, L. Colon, J. Dera, B. Rashidi, and V. Garg, “CARAF: Crypto Agility Risk Assessment Framework”, doi: 10.1093/cybsec/tyab013.

[64] “PQ.1 Post Quantum Telco Network - Impact Assessment - Whitepaper,” Feb. 2023. [Online]. Available: https://www.gsma.com/newsroom/gsma_resources/post-quantum-telco-network-impact-assessment-whitepaper/

[65] “TR 103 619 - V1.1.1 - CYBER; Migration strategies and recommendations to Quantum Safe schemes,” Jul. 2020. Accessed: Mar. 26, 2024. [Online]. Available: https://www.etsi.org/deliver/etsi_tr/103600_103699/103619/01.01.01_60/tr_103619v010101p.pdf

[66] “Preparing for Quantum-Safe Cryptography - NCSC.GOV.UK.” Accessed: Mar. 26, 2024. [Online]. Available: https://www.ncsc.gov.uk/whitepaper/preparing-for-quantum-safe-cryptography

[67] “Migrating to post-quantum cryptography - NCSC.GOV.UK.” Accessed: Mar. 26, 2024. [Online]. Available: https://www.ncsc.gov.uk/blog-post/migrating-to-post-quantum-cryptography-pqc

[68] W. Newhouse Murugiah Souppaya *et al.*, “Migration to Post-Quantum Cryptography Quantum Readiness: Cryptographic Discovery Volume B: Approach, Architecture, and Security Characteristics of Public Key Application Discovery Tools,” pp. 1800–1838, 2023, Accessed: Mar. 26, 2024. [Online]. Available: https://www.nccoe.nist.gov/.

[69] “Home - Pqreact.” Accessed: Mar. 26, 2024. [Online]. Available: https://pqreact.eu/

[70] “Planning for Post-Quantum Cryptography | Cyber.gov.au.” Accessed: Apr. 08, 2024. [Online]. Available: https://www.cyber.gov.au/resources-business-and-government/governance-and-user-education/governance/planning-post-quantum-cryptography

[71] “NIST announces post-quantum cryptography selections - Canadian Centre for Cyber Security.” Accessed: Apr. 08, 2024. [Online]. Available: https://www.cyber.gc.ca/en/news-events/nist-announces-post-quantum-cryptography-selections

[72] “Announcement of the results of the selection of algorithms in the National Cryptographic Algorithm Design Competition.” Accessed: Apr. 08, 2024. [Online]. Available: https://www.cacrnet.org.cn/site/content/854.html

[73] “Post-Quantum Cryptography - Integration study — ENISA.” Accessed: Apr. 08, 2024. [Online]. Available: https://www.enisa.europa.eu/publications/post-quantum-cryptography-integration-study

[74] “ANSSI views on the Post-Quantum Cryptography transition | ANSSI.” Accessed: Apr. 08, 2024. [Online]. Available: https://cyber.gouv.fr/en/publications/anssi-views-post-quantum-cryptography-transition

[75] “BSI - Quantum Technologies and Quantum-Safe Cryptography.” Accessed: Apr. 08, 2024. [Online]. Available: https://www.bsi.bund.de/EN/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Quantentechnologien-und-Post-Quanten-Kryptografie/quantentechnologien-und-post-quanten-kryptografie_node.html

[76] “CRYPTREC | TOP PAGE.” Accessed: Apr. 08, 2024. [Online]. Available: https://www.cryptrec.go.jp/en/

[77] “ISM Document | New Zealand Information Security Manual.” Accessed: Apr. 08, 2024. [Online]. Available: https://nzism.gcsb.govt.nz/ism-document

[78] “MCI Response to PQ on Quantum Computing Technology.” Accessed: Apr. 08, 2024. [Online]. Available: https://www.mci.gov.sg/media-centre/parliamentary-questions/quantum-computing-technology/

[79] “MSIT begins to cultivate quantum technology.” Accessed: Apr. 08, 2024. [Online]. Available: https://www.msit.go.kr/eng/bbs/view.do?sCode=eng&mId=4&mPid=2&bbsSeqNo=42&nttSeqNo=627

[80] “NSA Releases Future Quantum-Resistant (QR) Algorithm Requirements for National Security Systems > National Security Agency/Central Security Service > Press Release View.” Accessed: Apr. 08, 2024. [Online]. Available: https://www.nsa.gov/Press-Room/Press-Releases-Statements/Press-Release-View/Article/3148990/nsa-releases-future-quantum-resistant-qr-algorithm-requirements-for-national-se/

[81] “Federal agencies take ‘most important’ first step with inventorying cryptography ahead of quantum migration, OMB official says | FedScoop.” Accessed: Mar. 26, 2024. [Online]. Available: https://fedscoop.com/federal-agencies-take-most-important-first-step-with-inventorying-cryptography-ahead-of-quantum-migration-omb-official-says/

[82] I. Kong, M. Janssen, and N. Bharosa, “Challenges in the Transition towards a Quantum-safe Government,” in *DG. O 2022: The 23rd Annual International Conference on Digital Government Research*, L. Hagen, M. Solvak, and S. Hwang, Eds., ACM, 2022, pp. 282–292. doi: 10.1145/3543434.3543644.

[83] I. Kong, M. Janssen, and N. Bharosa, “Realizing quantum-safe information sharing: Implementation and adoption challenges and policy recommendations for quantum-safe transitions,” *Gov Inf Q*, vol. 41, p. 101884, 2024, doi: 10.1016/j.giq.2023.101884.

[84] M. Amico, Z. H. Saleem, and M. Kumph, “Experimental study of Shor’s factoring algorithm using the IBM Q Experience,” *Phys Rev A (Coll Park)*, vol. 100, no. 1, p. 012305, Jul. 2019, doi: 10.1103/PhysRevA.100.012305.

[85] “Quantum Threat Timeline - Global Risk Institute.” Accessed: Apr. 03, 2024. [Online]. Available: https://globalriskinstitute.org/publication/quantum-threat-timeline/

[86] “Quantum Threat Timeline Report 2020 - Global Risk Institute.” Accessed: Apr. 03, 2024. [Online]. Available: https://globalriskinstitute.org/publication/quantum-threat-timeline-report-2020/

[87] “2021 Quantum Threat Timeline Report: Global Risk Institute.” Accessed: Apr. 03, 2024. [Online]. Available: https://globalriskinstitute.org/publication/2021-quantum-threat-timeline-report-global-risk-institute-global-risk-institute/

[88] “2022 Quantum Threat Timeline Report - Global Risk Institute.” Accessed: Apr. 03, 2024. [Online]. Available: https://globalriskinstitute.org/publication/2022-quantum-threat-timeline-report/

[89] “2023 Quantum Threat Timeline Report - Global Risk Institute.” Accessed: Mar. 26, 2024. [Online]. Available: https://globalriskinstitute.org/publication/2023-quantum-threat-timeline-report/

[90] A. Yu. Kitaev, “Fault-tolerant quantum computation by anyons,” *Ann Phys (N Y)*, vol. 303, no. 1, pp. 2–30, Jul. 1997, doi: 10.1016/S0003-4916(02)00018-0.

[91] M. Roetteler, M. Naehrig, K. M. Svore, and K. Lauter, “Quantum Resource Estimates for Computing Elliptic Curve Discrete Logarithms.”

[92] J. Ha, J. Lee, and J. Heo, “Resource analysis and modifications of quantum computing with noisy qubits for elliptic curve discrete logarithms,” *Scientific Reports* |, vol. 14, p. 3927, 2024, doi: 10.1038/s41598-024-54434-w.

[93] É. Gouzien, D. Ruiz, F. M. Le Régent, J. Guillaud, and N. Sangouard, “Performance Analysis of a Repetition Cat Code Architecture: Computing 256-bit Elliptic Curve Logarithm in 9 Hours with 126 133 Cat Qubits,” *Phys Rev Lett*, vol. 131, no. 4, p. 040602, Jul. 2023, doi: 10.1103/PHYSREVLETT.131.040602.

[94] E. Martín-López, A. Laing, T. Lawson, R. Alvarez, X. Q. Zhou, and J. L. O’brien, “Experimental realization of Shor’s quantum factoring algorithm using qubit recycling,” *Nature Photonics 2012 6:11*, vol. 6, no. 11, pp. 773–776, Oct. 2012, doi: 10.1038/nphoton.2012.259.

[95] B. Fauseweh, “Quantum many-body simulations on digital quantum computers: State-of-the-art and future challenges,” *Nature Communications 2024 15:1*, vol. 15, no. 1, pp. 1–13, Mar. 2024, doi: 10.1038/s41467-024-46402-9.

[96] L. Henriet *et al.*, “Quantum computing with neutral atoms,” *Quantum*, vol. 4, p. 327, Sep. 2020, doi: 10.22331/q-2020-09-21-327.

[97] C. D. Bruzewicz, J. Chiaverini, R. McConnell, and J. M. Sage, “Trapped-ion quantum computing: Progress and challenges,” *Appl Phys Rev*, vol. 6, no. 2, Jun. 2019, doi: 10.1063/1.5088164/570103.

[98] B. P. Lanyon *et al.*, “Universal digital quantum simulation with trapped ions,” *Science (1979)*, vol. 334, no. 6052, pp. 57–61, Oct. 2011, doi: 10.1126/SCIENCE.1208001.

[99] C. Ospelkaus *et al.*, “Microwave quantum logic gates for trapped ions,” *Nature 2011 476:7359*, vol. 476, no. 7359, pp. 181–184, Aug. 2011, doi: 10.1038/nature10290.

[100] A. Blais, R. S. Huang, A. Wallraff, S. M. Girvin, and R. J. Schoelkopf, “Cavity quantum electrodynamics for superconducting electrical circuits: An architecture for quantum computation,” *Phys Rev A*, vol. 69, no. 6, p. 062320, Jun. 2004, doi: 10.1103/PHYSREVA.69.062320.

[101] M. Kjaergaard *et al.*, “Superconducting Qubits: Current State of Play,” *Annu Rev Condens Matter Phys*, vol. 11, no. Volume 11, 2020, pp. 369–395, Mar. 2020, doi: 10.1146/annurev-conmatphys-031119-050605.

[102] P. Krantz, M. Kjaergaard, F. Yan, T. P. Orlando, S. Gustavsson, and W. D. Oliver, “A quantum engineer’s guide to superconducting qubits,” *Appl Phys Rev*, vol. 6, no. 2, p. 21318, Jun. 2019, doi: 10.1063/1.5089550.

[103] C. Adami and N. J. Cerf, “Quantum computation with linear optics,” *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, vol. 1509, pp. 391–401, Jun. 1998, doi: 10.1007/3-540-49208-9_36.

[104] E. Knill, R. Laflamme, and G. J. Milburn, “A scheme for efficient quantum computation with linear optics,” *Nature 2001 409:6816*, vol. 409, no. 6816, pp. 46–52, Jan. 2001, doi: 10.1038/35051009.

[105] P. Kok, W. J. Munro, K. Nemoto, T. C. Ralph, J. P. Dowling, and G. J. Milburn, “Linear optical quantum computing with photonic qubits,” *Rev Mod Phys*, vol. 79, no. 1, pp. 135–174, Jan. 2007, doi: 10.1103/RevModPhys.79.135.

[106] M. Brooks, “Quantum computing is taking on its biggest challenge: noise,” MIT Technology Review. Accessed: Mar. 22, 2024. [Online]. Available: https://www.technologyreview.com/2024/01/04/1084783/quantum-computing-noise-google-ibm-microsoft/

[107] “IBM Quantum Computing Blog | Charting the course to 100,000 qubits.” Accessed: Mar. 22, 2024. [Online]. Available: https://www.ibm.com/quantum/blog/100k-qubit-supercomputer

[108] “IBM Debuts Next-Generation Quantum Processor & IBM Quantum System Two, Extends Roadmap to Advance Era of Quantum Utility.” Accessed: Mar. 22, 2024. [Online]. Available: https://newsroom.ibm.com/2023-12-04-IBM-Debuts-Next-Generation-Quantum-Processor-IBM-Quantum-System-Two,-Extends-Roadmap-to-Advance-Era-of-Quantum-Utility

[109] “Rigetti Pushes Back Roadmap on Development of 1,000-Qubit, 4,000 Qubit Models.” Accessed: Mar. 22, 2024. [Online]. Available: https://thequantuminsider.com/2022/05/18/rigetti-pushes-back-roadmap-on-development-of-1000-qubit-4000-qubit-models/

[110] F. Arute *et al.*, “Quantum supremacy using a programmable superconducting processor,” *Nature 2019 574:7779*, vol. 574, no. 7779, pp. 505–510, Oct. 2019, doi: 10.1038/s41586-019-1666-5.

[111] “Quantinuum H-Series quantum computer accelerates through 3 more performance records for quantum volume: 217, 218, and 219.” Accessed: Mar. 25, 2024. [Online]. Available: https://www.quantinuum.com/news/quantinuum-h-series-quantum-computer-accelerates-through-3-more-performance-records-for-quantum-volume-217-218-and-219

[112] “IonQ | Trapped Ion Quantum Computing.” Accessed: Mar. 25, 2024. [Online]. Available: https://ionq.com/

[113] A. W. Cross, L. S. Bishop, S. Sheldon, P. D. Nation, and J. M. Gambetta, “Validating quantum computers using randomized model circuits,” *Phys Rev A (Coll Park)*, vol. 100, no. 3, p. 032328, Sep. 2019, doi: 10.1103/PHYSREVA.100.032328.

[114] “Technical Roadmap Webinar: Getting Ready for the Era of Enterprise-Grade Quantum Computers.” Accessed: Mar. 25, 2024. [Online]. Available: https://ionq.com/resources/technical-roadmap-webinar-getting-ready-for-the-era-of-enterprise-grade

[115] Quantinuum, “Debunking algorithmic qubits.” Accessed: Mar. 25, 2024. [Online]. Available: https://www.quantinuum.com/news/debunking-algorithmic-qubits

[116] “QuEra Computing Releases a Groundbreaking Roadmap for Advanced Error-Corrected Quantum Computers, Pioneering the Next Frontier in Quantum Innovation.” Accessed: Mar. 22, 2024. [Online]. Available: https://www.quera.com/press-releases/quera-computing-releases-a-groundbreaking-roadmap-for-advanced-error-corrected-quantum-computers-pioneering-the-next-frontier-in-quantum-innovation

[117] “PASQAL Issues Roadmap to 10,000 Qubits in 2026 and Fault Tolerance in 2028.” Accessed: Mar. 22, 2024. [Online]. Available: https://www.hpcwire.com/2024/03/13/pasqal-issues-roadmap-to-10000-qubits-in-2026-and-fault-tolerance-in-2028/

[118] “Infleqtion Unveils 5-year Quantum Computing Roadmap, Advancing Plans to Commercialize Quantum at Scale — Infleqtion.” Accessed: Mar. 22, 2024. [Online]. Available: https://www.infleqtion.com/news/infleqtion-unveils-5-year-quantum-computing-roadmap-advancing-plans-to-commercialize-quantum-at-scale

[119] A. Wilkins, “Record-breaking quantum computer has more than 1000 qubits,” *New Sci (1956)*, Oct. 2023, Accessed: Mar. 22, 2024. [Online]. Available: https://www.newscientist.com/article/2399246-record-breaking-quantum-computer-has-more-than-1000-qubits/

[120] L. S. Madsen *et al.*, “Quantum computational advantage with a programmable photonic processor,” *Nature*, vol. 606, no. 7912, p. 75, Jun. 2022, doi: 10.1038/S41586-022-04725-X.

[121] V. V. Albert and P. Faist, “Quantum error-correcting code (QECC),” https://errorcorrectionzoo.org/c/qecc. Accessed: Apr. 24, 2024. [Online]. Available: https://errorcorrectionzoo.org/c/qecc

[122] N. Ofek *et al.*, “Extending the lifetime of a quantum bit with error correction in superconducting circuits,” *Nature 2016 536:7617*, vol. 536, no. 7617, pp. 441–445, Jul. 2016, doi: 10.1038/nature18949.

[123] A. G. Fowler, M. Mariantoni, J. M. Martinis, and A. N. Cleland, “Surface codes: Towards practical large-scale quantum computation,” *Phys Rev A*, vol. 86, no. 3, p. 032324, Sep. 2012, doi: 10.1103/PHYSREVA.86.032324.

[124] Google Quantum AI, “Suppressing quantum errors by scaling a surface code logical qubit,” *Nature* , vol. 614, pp. 676–681, 2023, doi: 10.1038/s41586-022-05434-1.

[125] S. Krinner *et al.*, “Realizing repeated quantum error correction in a distance-three surface code,” *Nature 2022 605:7911*, vol. 605, no. 7911, pp. 669–674, May 2022, doi: 10.1038/s41586-022-04566-8.

[126] D. Bluvstein *et al.*, “Logical quantum processor based on reconfigurable atom arrays,” *Nature 2023 626:7997*, vol. 626, no. 7997, pp. 58–65, Dec. 2023, doi: 10.1038/s41586-023-06927-3.

[127] M. P. da Silva *et al.*, “Demonstration of logical qubits and repeated error correction with better-than-physical error rates,” *arXiv preprint arXiv:2404.02280*, Apr. 2024, Accessed: Apr. 08, 2024. [Online]. Available: https://arxiv.org/abs/2404.02280v2

[128] H. Bombin and M. A. Martin-Delgado, “Optimal Resources for Topological 2D Stabilizer Codes: Comparative Study,” *Phys Rev A*, vol. 76, no. 1, Mar. 2007, doi: 10.1103/PhysRevA.76.012305.

[129] D. K. Tuckett, A. S. Darmawan, C. T. Chubb, S. Bravyi, S. D. Bartlett, and S. T. Flammia, “Tailoring surface codes for highly biased noise,” *Phys Rev X*, vol. 9, no. 4, Dec. 2018, doi: 10.1103/PhysRevX.9.041031.

[130] N. P. Breuckmann and J. Niklas Eberhardt, “Quantum Low-Density Parity-Check Codes,” *Phys Rev Appl*, vol. 10, doi: 10.1103/PRXQuantum.2.040101.

[131] S. Bravyi, A. W. Cross, J. M. Gambetta, D. Maslov, P. Rall, and T. J. Yoder, “High-threshold and low-overhead fault-tolerant quantum memory,” *Nature 2024 627:8005*, vol. 627, no. 8005, pp. 778–782, Mar. 2024, doi: 10.1038/s41586-024-07107-7.

[132] M. B. Hastings and J. Haah, “Dynamically Generated Logical Qubits,” *Quantum*, no. 5, Jul. 2021, doi: 10.22331/q-2021-10-19-564.

[133] B. Barber *et al.*, “A real-time, scalable, fast and highly resource efficient decoder for a quantum computer,” *arXiv preprint arXiv:2309.05558*, Accessed: Apr. 08, 2024. [Online]. Available: https://arxiv.org/abs/2309.05558

[134] C. A. Pattison, M. E. Beverland, M. P. da Silva, and N. Delfosse, “Improved quantum error correction using soft information,” *arXiv preprint arXiv:2107.13589*, Jul. 2021, Accessed: Apr. 08, 2024. [Online]. Available: https://arxiv.org/abs/2107.13589v1

[135] L. Skoric, D. E. Browne, K. M. Barnes, N. I. Gillespie, and E. T. Campbell, “Parallel window decoding enables scalable fault tolerant quantum computation,” *Nature Communications 2023 14:1*, vol. 14, no. 1, pp. 1–8, Nov. 2023, doi: 10.1038/s41467-023-42482-1.

[136] C. Crane, “Google Chrome Adds Support for a Hybrid Post-Quantum Cryptographic Algorithm,” Hashed Out by The SSL Store. Accessed: Apr. 25, 2024. [Online]. Available: https://www.thesslstore.com/blog/google-chrome-adds-support-for-a-hybrid-post-quantum-cryptographic-algorithm/

[137] C. Taylor. Fitz-Gibbon, “Performance indicators,” *BERA Dialogues*, no. 2, p. 111, 1990, Accessed: Apr. 12, 2024. [Online]. Available: https://books.google.com/books?id=uxK0MUHeiI4C

[138] V. P. Dymnikov and A. N. Filatov, “Mathematics of Climate Modeling,” *Mathematics of Climate Modeling*, 1996, doi: 10.1007/978-1-4612-4148-5.