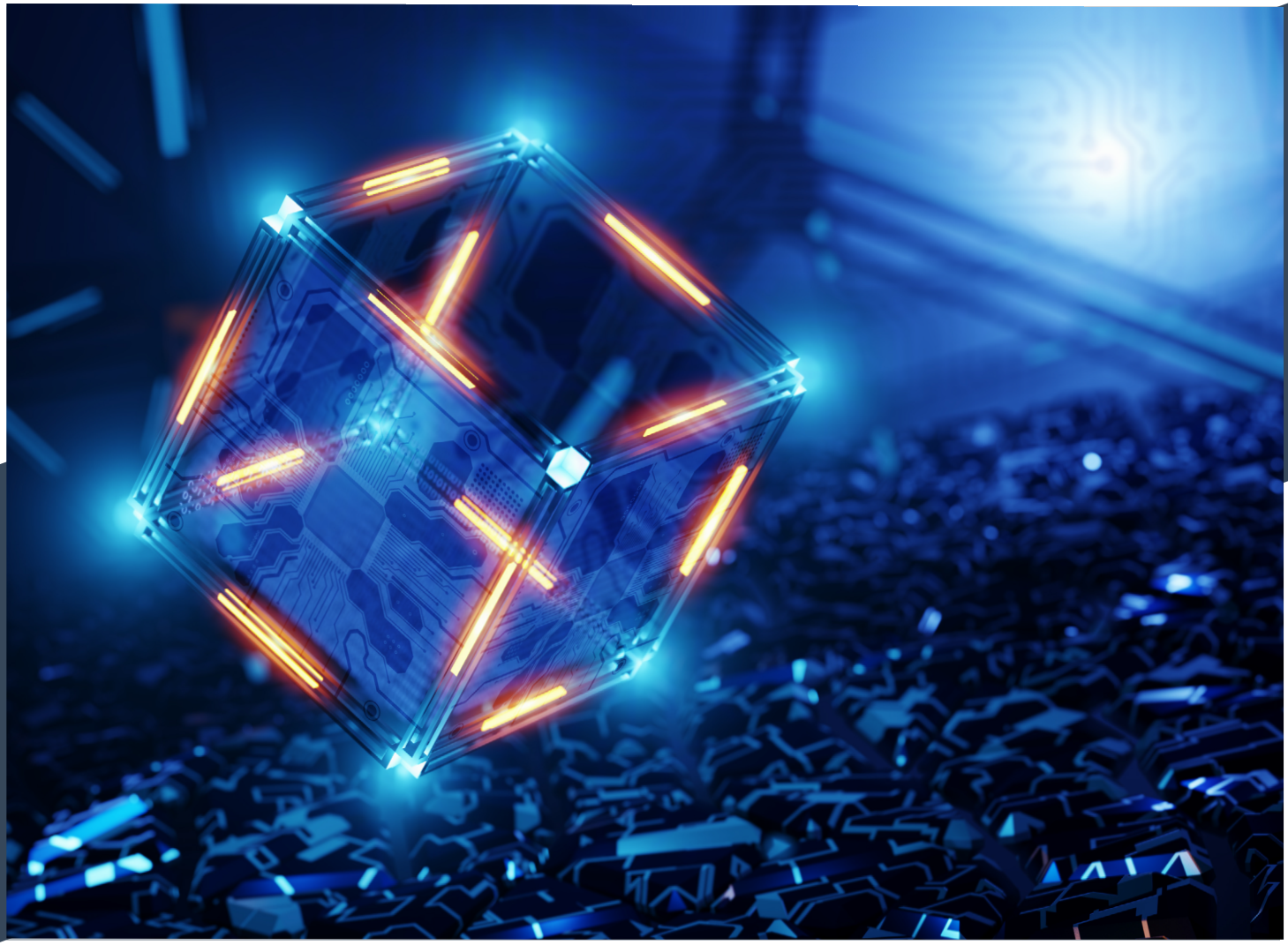
QUANTUM THREAT TIMELINE REPORT 2024



Authors

Dr. Michele Mosca

Co-Founder & CEO, evolutionQ Inc.

Dr. Marco Piani

Senior Research Analyst, evolutionQ Inc.

GLOBAL RISK INSTITUTE

evolution

DECEMBER 2024

Contents

Declaration on Potential Conflict of Interest
evolutionQ Inc. offers services and quantum-safe cybersecurity products to help clients deploy and manage quantum-safe technologies across their networks.
The basis of the report is a survey of leaders in the fields of quantum computing research and commercialization.

Summary

Cybersecurity protocols that are widely used today rely on computational challenges believed to be practically unsolvable with classical computers. We have known for decades that the advent of quantum computers that exploit quantum phenomena at the microscopic level in a highly controlled manner would allow some of those challenges to be overcome, posing severe risks to cybersecurity.

To mitigate this threat, new classical and quantum-based cryptographic techniques can be used that are considered or definitively known to be immune to quantum attacks. Unfortunately, upgrading cryptosystems to so-called *quantum-safe cryptography* is no easy task. It requires the creation and adoption of new hardware and new software, the development of standards, and the update of older systems, while maintaining a working cryptographic infrastructure and managing past and present sensitive data.

Because of the complexity and of the time required by such a process, a successful transition cannot take the form of reactive and rushed crisis management, but it should rather be made an integral part of a proactive technology lifecycle management.

The urgency of moving to quantum-resistant cryptography varies for each organization, based on its security needs and risk tolerance. This urgency can be gauged using three primary factors:

- the *shelf-life time*: how many years the data must remain secure for;
- the *migration time*: how many years it will take to securely upgrade the systems guarding that data;
- the *threat timeline*: the estimated time until potential adversaries gain access to quantum computers of cryptographic significance.

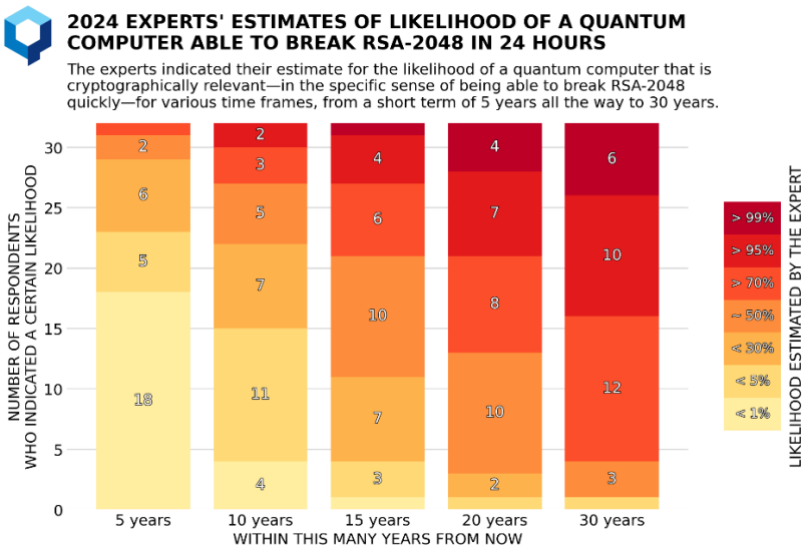
The *Mosca inequality* states that, if the quantum threat timeline (QTT) is less than the combined duration of the shelf-life and migration times, then organizations might fail to shield their assets from quantum-enabled breaches. The aim of this report is to provide an educated perspective of how far away the quantum threat is.

The mitigation of the quantum threat to cybersecurity requires a transition to quantum-safe cryptography that can be implemented safely only with enough time at disposal.

This report sheds light onto the quantum threat timeline by examining the perspectives of 32 global experts from academia and industry, involved in diverse aspects of quantum computing development. These experts responded to questions aimed at gaining valuable insights on the cyber-risk posed by quantum cryptanalysis.

Predicting the pace at which a cryptographically-relevant quantum computer (CRQC) will be developed – let alone *when* it will be developed – is plagued by uncertainty. The reason is that building such a device requires continuously pushing the boundaries of science and engineering, to the extent that some have suggested adopting an approach and effort not

dissimilar to that of Project Manhattan for the development of the atomic bomb[1].



The main challenge in building a CRQC lies in the fragility of the quantum properties a CRQC needs to harness to outperform standard computers. The building blocks of quantum computers are quantum bits, or *qubits*, which have several possible technological implementations, all necessarily imperfect. Quantum error correction (QEC) allows one to utilize multiple imperfect *physical* qubits with fragile quantum features to encode high-quality and robust *logical* qubits.

The last year has seen new remarkable demonstrations of the feasibility of such an approach, but scaling up to the numerous logical qubits needed for quantum cryptanalysis remains daunting. Despite the existing challenges, the polled experts generally accept that a CRQC will eventually be built on the basis that no specific fundamental roadblock has been identified and that there has been steady – and at times fast – progress. Quantum researchers and companies have identified and continued to achieve key milestones in their roadmaps to further scale the size and performance of current devices towards the level needed for cryptographic applications. In particular, the progress in the last year has induced many people both within and outside the quantum research community to realize that the quantum threat may be closer than they thought.

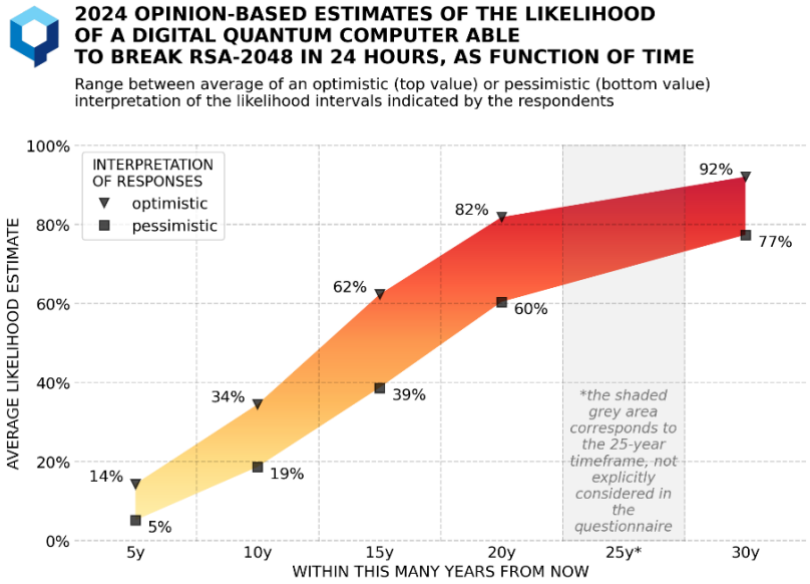
The progress in the last year has induced many people both within and outside the quantum research community to realize that the quantum threat may be closer than they thought.

Similarly to our previous surveys, our respondents have shared their estimates for the likelihood that a CRQC may become available in the future, within various timeframes. More than half (17/32) felt it was more than 5%-likely already within a 10-year timeframe, and almost a third of the respondents (10/32) indicated a likelihood of about 50% or more.

The responses can be averaged to produce an overall opinion-based estimated likelihood for the creation of a CRQC. An "optimistic" interpretation of the responses – focused on the upper bound of the likelihood ranges the respondents could choose among – leads on average to a ~34% estimate of a CRQC being developed within a decade and ~14% within 5 years. Even a "pessimistic" interpretation focused on the lower bound of the likelihood ranges gives a ~19% average likelihood

[1] Incidentally, that such a suggestion has been made should convey not only the size of the challenge, but also how consequential the creation of a large quantum computer is perceived by some.

estimate of a disruptive quantum threat in the next 10 years. We stress that, depending on the risk tolerance and needs of companies and institutions, this indicates that many organizations may unknowingly be facing already an intolerable level of risk requiring urgent action.



Independently of the exact time when a CRQC may become available, it is crucial to note that adversaries do not have to remain inactive while waiting for it: they can already now intercept, duplicate, and archive encrypted communications for eventual later decryption – a so-called "Harvest Now, Decrypt Later (HNDL)" attack strategy. This is factored into the aforementioned Mosca inequality, which considers the required shelf-life time of the data.

Many organizations may unknowingly be facing already an intolerable level of risk requiring urgent action.

Those responsible for managing cyber-risk should not wait to act; solutions that can start to be implemented are available today (Canadian Forum for Digital Infrastructure Resilience 2023; World Economic Forum 2023). This will be facilitated by the US National Institute of Standards and Technology (NIST) having recently issued the first standards for post-quantum cryptographic algorithms (NIST, 2024).

Given the recent advancements in quantum computing, the expert opinions collected in our survey, the momentum generated by the currently significant investments in the field, and the threat posed by the HNDL attack, there should be a conscious effort toward cryptographic modernization that enables visibility on cryptographic tools used, faster timelines for safely updating cryptography, and building layered defenses against the known and future threats to public-key cryptography. This proactive approach can also help to mitigate the risks associated with a hasty transition to quantum-safe cryptographic tools and infrastructure.

From the threat timeline to the migration timeline

Depending on specific shelf-lives, migration times and risk appetites, all organizations should evaluate their urgency in proceeding with migration to quantum-safe systems (Canadian Forum for Digital Infrastructure Resilience 2023; World Economic Forum 2023). The Global Risk Institute and evolutionQ Inc. have already made available a quantum risk assessment methodology (Mosca and Mullholland 2017) on which such a process may be based.

Those responsible for managing cyber-risk should not wait to act; solutions that can start to be implemented are available today.

1 Introduction

This is the sixth report in an annual series that started in 2019 with the intent to shine light on when we may expect the creation of a quantum computer powerful enough to be cryptographically relevant. The reports have been largely based on a recurring survey of expert leaders in the area of quantum computing research. These experts have been asked questions to assess the status and pace of development of the field and, most importantly, to provide their best estimates for when such a cryptographically-relevant quantum computer (CRQC) may become available.

This Introduction and the Appendix provide a minimal background to help the reader understand how quantum computers threaten cybersecurity, and the immense scientific and technological hurdles involved in building such computers.

1.1 Quantum computing

Quantum mechanics is our most successful scientific framework for understanding the microscopic world, including the behavior of physical systems like atoms and fundamental particles like electrons and photons.

Quantum computers leverage unique quantum phenomena to handle information in a manner radically different from current classical computers.

Quantum mechanics describes the world in terms that may appear counterintuitive or even absurd to the layperson. For example, a quantum system may be in a so-called *superposition* of states that would be mutually exclusive from the perspective of classical physics. One likely reason for which quantum phenomena tend to elude classical intuition is that quantum effects are not obvious in everyday experience. In turn, this happens because of the physical scales involved and, most importantly, because quantum phenomena are highly sensitive and easily disrupted by environmental interactions, which can degrade or effectively even eliminate quantum properties through a process known as *decoherence*.

In classical computing, information is stored in bits that represent binary and exclusive values, either "0" or "1." Quantum computing (Nielsen and Chuang 2000) aims at taking advantage of quantum phenomena like superposition to, for example, enable more complex information processing and to facilitate the simulation and understanding of general quantum systems.

The primary obstacle in advancing quantum computing is the unprecedented requirement to maintain and control quantum behaviour at a level that has never been attempted before in human history.

Correspondingly, the foundational unit of quantum information in quantum computing is the *quantum bit*, or *qubit*. Unlike a traditional bit that stores either a 0 or a 1, a qubit can exist in a superposition of both values, which can be thought of as “coexisting” and processed simultaneously.

The monumental challenge in the field of quantum computing is to mitigate and counteract the effects of decoherence to protect fragile quantum features while at the same time controlling quantum systems very precisely, in order to execute quantum algorithms.

There are several proposal and approaches under development for constructing a quantum computer. They differ in the physical substrate used—ranging from superconducting circuits and trapped ions to quantum optics, among others—and in which specific degrees of freedom qubits are defined—for example, atomic energy levels or quantum spin. They differ also in the techniques for implementing *quantum error correction* (QEC), with the intention of reaching so-called *fault tolerance*. QEC is essential for encoding quantum information into more resilient *logical qubits* "spread" over multiple inherently flawed physical qubits, thus enabling reliable information processing. A key milestone along the path towards a quantum computer is that of demonstrating that QEC schemes allow one to go beyond the so-called "break-even" condition, that is, that an encoded logical qubit performs better than the underlying physical qubits, and that by employing a sufficiently high number of physical qubits per logical qubit, it is possible to bring down logical errors to an arbitrary low level.

Once realized, quantum computers will not only fulfill Richard Feynman's vision of efficiently simulating quantum systems (Feynman 1982) but also, by cleverly leveraging quantum features like superposition via specialized algorithms, solve a range of mathematical, optimization, and search problems at speeds unattainable by classical computers (Nielsen and Chuang 2000).

For more details on physical implementations, QEC, and fault tolerance, please refer to the Appendix.

1.2 Quantum threat to cybersecurity

Quantum computers have the potential to compromise existing widely-adopted cryptographic systems. For example, RSA (Rivest, Shamir, and Adleman 1978) could be broken using Shor's quantum algorithm (Shor, 1994). Likewise, Grover's algorithm (Grover, 1996) enables a quantum computer to search a space of 2^n possible values in approximately $2^{n/2}$ steps, thereby reducing the security of symmetric-key cryptography. The emergence of quantum computing introduces the risk of severe failures in cyber-systems, either through direct cryptographic attacks or by undermining trust in these systems.

Quantum computers pose a threat to cybersecurity because they can break or weaken widely used cryptographic schemes.

This impending threat posed by a Cryptographically-Relevant Quantum Computer (CRQC) can be addressed through the implementation of quantum-resistant cryptographic techniques, which may be either classical or quantum-based (World Economic Forum 2023; Canadian Forum for Digital Infrastructure Resilience 2023; TNO 2023; FS-ISAC 2023). The former category includes cryptographic algorithms based on problems considered challenging also for quantum computers. Significant progress has been made in this direction, as demonstrated by the U.S. National Institute of Standards and Technology (NIST) issuing in 2024 the first standards for post-quantum cryptographic algorithms (NIST, 2024). On the other hand, a tool like quantum key distribution (QKD) utilizes quantum principles to establish shared secret keys to secure communications (Nielsen and Chuang, 2000).

Transitioning to this new breed of *quantum-safe* cryptography is a complex and delicate process (Mosca 2013): it requires the development and deployment of hardware and software solutions, the establishment of standards, the migration of legacy systems, and more[2].

With the necessity to devote enough time to an orderly and safe transition to a 'post-quantum world', the urgency for any organization to complete the transition to quantum-safe cryptography for a particular cyber-system can be determined by considering three simple but important parameters[3]:

- $T_{\text{SHELF-LIFE}}$ **(shelf-life time)**: the number of years the information should be protected by the cyber-system;
- $T_{\text{MIGRATION}}$ **(migration time)**: the number of years needed to properly and safely migrate the system to a quantum-safe solution;
- T_{THREAT} **(threat timeline)**: the number of years before the relevant threat actors will be able to break the quantum-vulnerable systems.

Figure 1 The timeline for the emergence of quantum computers capable of threatening cybersecurity needs to be compared with the combined time required for migrating to post-quantum security and the duration for which the data needs to be protected. See main text for details.

If $T_{\text{SHELF-LIFE}} + T_{\text{MIGRATION}} > T_{\text{THREAT}}$, that is, if the time required to migrate the system *plus* the time for which the information needs to be protected goes *beyond* the time when the quantum threat will become concrete, then an organization may not be able to protect its assets for the required $T_{\text{SHELF-LIFE}}$ years against the quantum threat (see Figure 1). This is the content of the *Mosca Inequality* (Mosca 2013), and is due to the possibility of *"Harvest Now, Decrypt Later"* attacks (Figure 2) which may affect current data/messages even if a CRQC is not yet available.

Figure 2 A malicious adversary may already now intercept/access, copy, and store encrypted data, deferring decryption to when a cryptographically-relevant quantum computer will become available. This is called a "Harvest Now, Decrypt Later" attack.

[2] As an example of the needed 'migration time', it is worth stressing that the NIST selection process started in 2016 (NIST 2016).

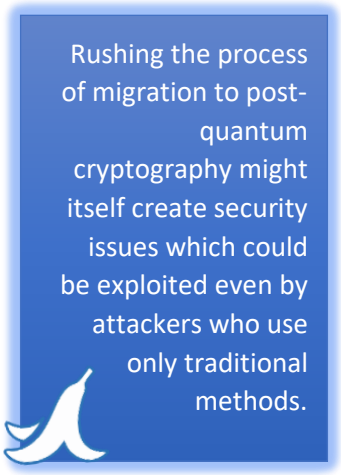
[3] Often, these parameters have respectively been called *x*, *y*, *z* in literature; see e.g., (Mosca 2013). Here we adopt a more explicit notation.

Organizations need to assess $T_{SHELF\text{-}LIFE}$ and T_{THREAT}. The difference

$$(T_{MIGRATION})^{MAX} := T_{THREAT} - T_{SHELF\text{-}LIFE}$$

is the **maximum available migration time**, that is, the maximum time organizations have at their disposal to safely realize the transition.

It is crucial to recognize that a rushed transition to post-quantum security systems may lead to the introduction of new vulnerabilities, which could be susceptible to conventional hacking techniques. These weaknesses might stem from design flaws, implementation errors, or overlooked details. Furthermore, challenges related to interoperability and backward compatibility could emerge, complicating the migration process.



The security shelf-life time $T_{SHELF\text{-}LIFE}$ is generally organization specific: it may be based on a business decision or dictated by regulations. On the other hand, assessing the threat timeline T_{THREAT} is more complex.

There are many scientific and engineering obstacles to developing a quantum computer powerful enough to crack existing cryptographic systems. These challenges suggest that CRQCs are likely years away, but breakthroughs, which are by nature unexpected, could potentially fast-track development. This last year has provided evidence for this, with several strong experimental results.

Investments in quantum computing and associated technologies are a crucial factor affecting the pace of development, potentially shortening the timeframe for transitioning to quantum-safe systems. Funding has flown into quantum computing research in recent years from diverse sources, including government bodies, established companies, and private investors backing new startups (Kung and Fancy 2021; McKinsey & Company 2024). This influx of funding highlights the necessity for a well-planned transition to post-quantum cryptographic systems.

1.3 Quantum computing towards fault tolerance

It is currently believed that quantum cryptanalysis requires running quantum algorithms on a sufficiently large quantum computer that employs quantum error correction. In general, such a fault-tolerant quantum computer is needed to run quantum algorithms developed to be run on an idealized error-free quantum computer. It will take still time to reach such a stage.

Meanwhile, there is undeniable excitement about the practical and business potential of “early-stage” quantum computers, which are not yet advanced enough to threaten cybersecurity. For those primarily wary of the cybersecurity risks posed by quantum computers, the interest in these nascent quantum applications may seem indirect. However, such applications would:

- offer tangible signs and early alerts of the impending quantum challenges to cybersecurity;
- increase the likelihood of consistent funding and resources for quantum computing research, aiming to develop a digital quantum computer with cryptographic significance.

In the past years, there has been interest in Noisy Intermediate Size Quantum (NISQ) devices (Preskill 2018), with tens to hundreds of physical qubits. There have been demonstrations – often controversial ones – of how such devices may go beyond what standard computers are capable of, the most famous example being perhaps the realization of so-called "quantum supremacy" (Arute et al. 2019). The controversies surrounding such demonstrations have typically two sources:

- the problems considered to prove a quantum advantage may be specifically designed with that goal in mind, but not be of any practical utility;
- the claim of surpassing the capabilities of standard computers may lack the solidity of a mathematical proof and consider only some classical approach/algorithm, while a better classical approach/algorithm may exist.

KEY POINTS

- Quantum computing leverages the principles of quantum mechanics to perform certain computational tasks more efficiently than classical computing. The fundamental unit of information in a quantum computer is the quantum bit, or qubit.
- A Cryptographically-Relevant Quantum Computer (CRQC) is a quantum computer powerful enough that, once developed, could break many widely used cryptographic systems, posing a significant threat to data security.
- Building a CRQC requires implementing quantum error correction techniques to manage and stabilize the inherently fragile quantum states that form logical qubits.
- Developing a CRQC presents an enormous scientific and engineering challenge, as it requires both scaling the number of physical qubits and maintaining high-quality control over them, making any estimates of a CRQC timeline inherently uncertain.
- To mitigate the risks posed by a CRQC, it is crucial to transition to quantum-safe cryptographic tools. This migration process is complex and requires careful planning to ensure new vulnerabilities are not introduced.
- The urgency of transitioning to quantum-safe cryptography depends on the projected timeline for a CRQC, the migration time required, and the shelf-life of the data that needs protection.
- If the time required for migration, combined with the data's shelf-life, exceeds the estimated timeline for the quantum threat, assets may be left vulnerable. This concept is captured by the so-called Mosca Inequality.
- There is undeniable excitement about the practical and business potential of "early-stage" quantum computers, which are not yet advanced enough to threaten cybersecurity. Such "early" applications of quantum computing are uncertain but, if concrete, they could facilitate the development of a CRQC.

2 Scope of this report

This document outlines the findings of a survey conducted by evolutionQ Inc., involving 32 globally recognized experts in quantum computing. Continuing the tradition of similar surveys from the past five years, the experts were invited to complete an online questionnaire regarding the current state of the field. In certain cases, participants were given the option to respond to a key question via email. Further details on the survey questions are provided in Appendix A.3 .

We aim to capture both a snapshot of the experts' opinions and to identify potential trends in how these opinions evolve over time. This evolution may result from consistent advancements, new key developments or challenges, as well as external factors such as funding levels that, while not directly related to research, still impact research activities.

When designing the questionnaire, we focused on being concrete and specific, particularly in evaluating quantum computers as a potential threat to cybersecurity. As such, the primary question directly addresses the breaking of RSA-2048, whose security relies on the difficulty of factoring a 2048-bit number.

Other methodologies have also been employed to estimate the timeline for the development of a fault-tolerant quantum computer that could pose a risk to cybersecurity. For example, in (Sevilla and Riedel 2020), the authors try to forecast future progress in the domain of quantum computing by extrapolating past progress in the field. They look at relevant metrics—roughly speaking, at how many effective logical qubits are available for computation. Sevilla and Riedel focus on superconducting implementations, and, similarly to what we do, on the task of breaking RSA-2048. Their estimates for when (superconducting) quantum computers could achieve such a feat are described by the authors themselves as “one piece of relevant evidence that can supplement expert opinion” and “more pessimistic but broadly comparable to those produced through the survey of experts in [(Mosca and Piani 2019)]”. They also write that a cryptographically relevant quantum computer could be built earlier than estimated by them, if progress is faster than what one can extrapolate from current trends. Such an extrapolation suffers at the very least from the fact that the field of quantum computing is relatively young, so that the progress achieved and tracked so far still covers only a limited temporal span.

Relevant indications about the quantum threat timeline come also from the roadmaps of companies working towards the realization of fault-tolerant quantum computers (see, e.g., the Google, the IBM, the Quantinuum, and the QuEra roadmaps).

KEY POINTS

- This report is part of a series based on annual surveys to collect and analyze opinions of tens of leading experts in the field of quantum computing.
- The major goal of the report is to provide unique insight into the quantum threat timeline based on expert opinions, complementing other approaches and sources of information.

3 Participants

Since the inaugural survey in 2019, we have annually reached out to top international experts with the aim of garnering a diverse and insightful array of perspectives on the progress in the quantum computing field. Throughout the years, we have endeavored to maintain the original group of 2019 respondents to monitor shifts in their views. Additionally, we have approached other potential participants, chosen from an extensive list of over a hundred preeminent experts. Those who agreed to participate were requested to fill out the online survey.

Some candidate respondents we contacted did not reply to our invitation, while some others declined, due to, for example, time constraints or policies of their institution/company. Overall, in 2024 we were able to collect responses from 32 experts (see Appendix A.1 for a complete list).

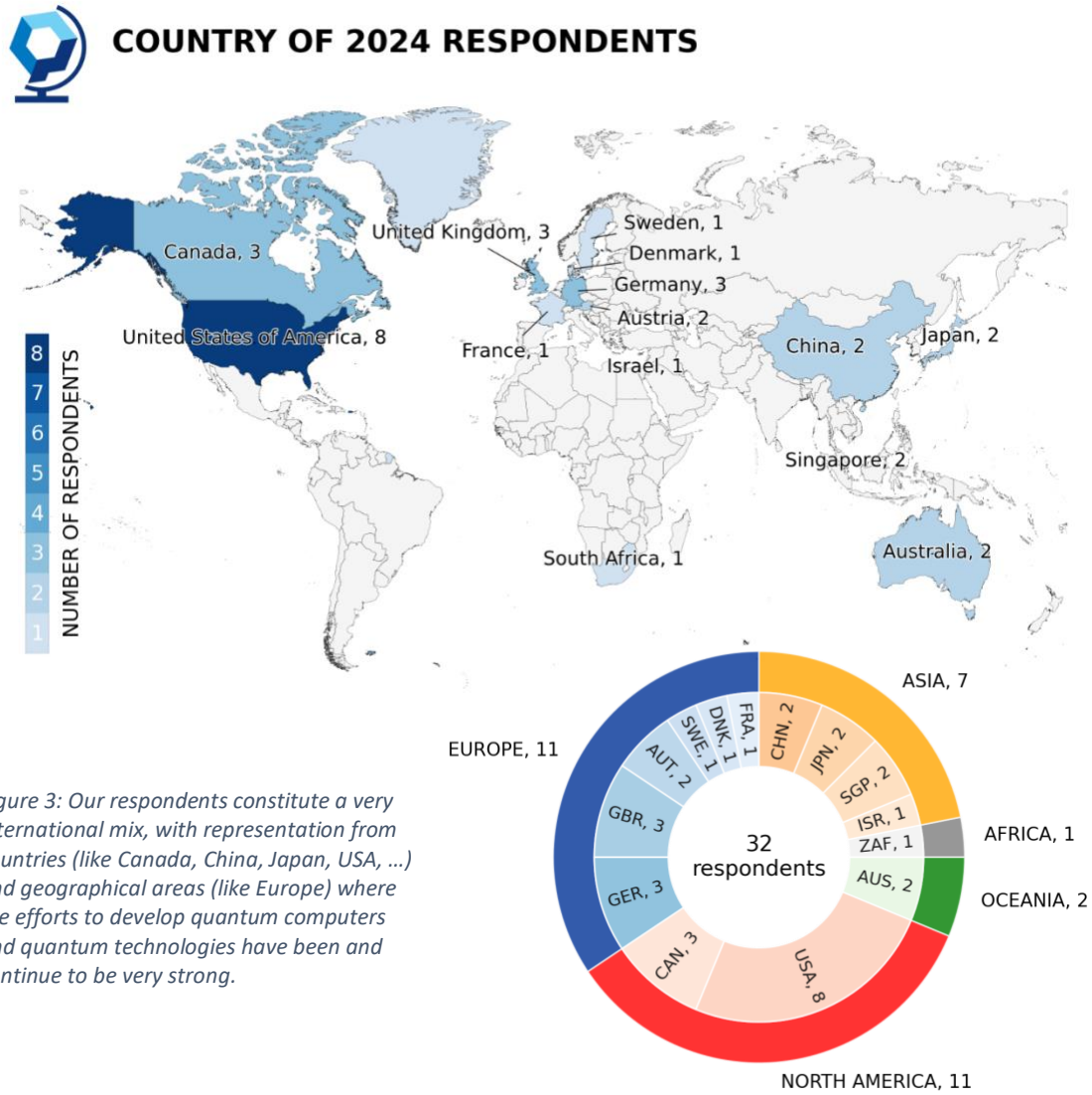


Figure 3: Our respondents constitute a very international mix, with representation from countries (like Canada, China, Japan, USA, …) and geographical areas (like Europe) where the efforts to develop quantum computers and quantum technologies have been and continue to be very strong.

Here we summarize graphically the composition of the group in terms of:

- country where they work (Figure 3),
- kind of activity they lead (Figure 4),
- kind of organization they belong to (Figure 5).

The captions of the figures provide guidance in interpreting the presented statistics. In essence, our respondent pool showcases a rich blend of expertise, national backgrounds, and representation from both academic and private sectors. Over the years, there has been a noticeable uptick in academics from our survey who also engage in corporate roles, signifying a heightened focus on the commercial aspects of quantum technologies and computing.

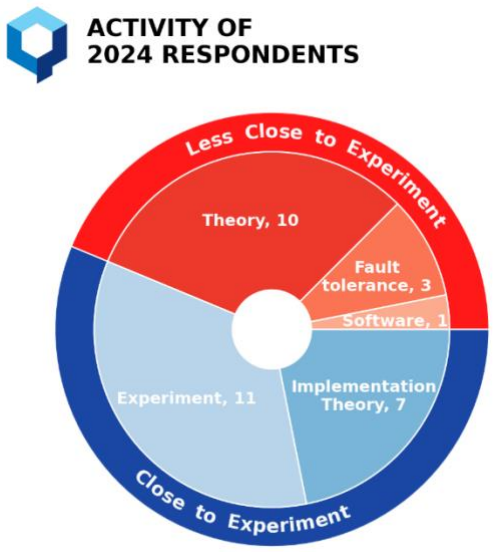


Figure 4 Our respondents cover a wide range of research activities. While the major division is between non-experimental research and experimental one, research that is not directly experimental can be very different. E.g., implementation theory focuses on guiding, supporting, and, in general, facilitating experimemental effort. Respondents are classified under simply "theory" if their more abstract activity is not specificically related to experiments or implementations, or to fault-tolerance, or to software development.

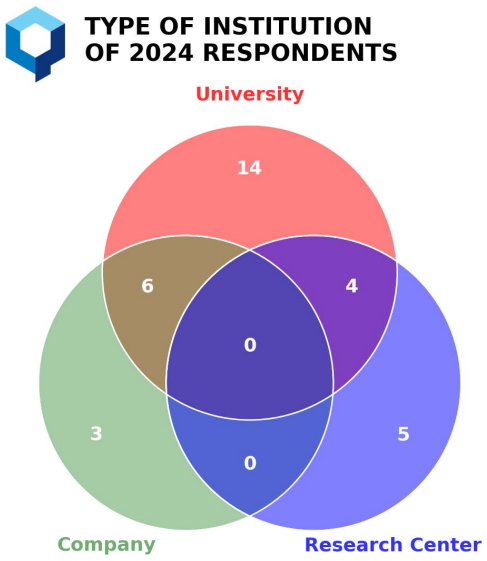


Figure 5 Most of the respondents work at universities, but some work at companies or research centres. Some researchers/academics may have some role in—or at least collaborate closely with—external companies. A larger fraction of our respondents has fallen in the latter category in the last two reports, also because some past academic respondents have joined or founded companies.

KEY POINTS

- Our respondent pool showcases a rich blend of expertise, national backgrounds, and representation from both academic and private sectors, reflecting the multifaceted nature of the quantum computing community.
- Thirty-two respondents took part in the 2024 survey.

4 Survey results

We provide an aggregate quantitative analysis of the key responses about the following:

- the potential of various physical implementations/platforms for quantum computing (Section 4.1);
- the quantum threat timeline (Section 4.2);
- views on potential concerns regarding the realization of a cryptographically-relevant quantum computer in the relatively-near future (Section 4.3);
- the most important upcoming experimental milestone convincingly demonstrating the feasibility of large-scale quantum computing (Section 4.4);
- the expected change in funding in support of quantum computing research (Section 4.7.1);
- the status and potential development of the so-called "quantum race" (Section 4.7.2);
- potential sources of unexpected speed-up in the development of a cryptographically relevant quantum computer (Section 4.8).

We also include:

- a selection of opinions about:
  - key recent research developments, as highlighted by the respondents;
  - near-future (that is, approximately, by mid-2025) developments that the respondents see as essential on the path to developing a fully scalable fault-tolerant quantum computer;
  - next milestones to track, not necessarily attainable by mid-2025;
- a collection of other notable remarks made by the respondents.

Comments by the respondents may be quoted with the respondents' permission. A quote may be attributed to the specific respondent or may be reported anonymously as coming from a "Respondent". Quotes may be lightly edited for conciseness and clarity.

Where we deem appropriate, we analyze shifts in the responses as compared to responses from the previous five years. In the aggregated analysis of the responses, we indicate how many of the respondents (alternatively, what percentage of them) chose a specific answer among the many possible ones, when dealing with multiple choices.

Not all the 32 respondents provided an input for all questions. Also, the respondents took part in the survey over a time during which new results were announced, so their input may be based on a slightly different status of the field.

Finally, some questions might have been modified or tweaked in their wording from survey to survey, but we have intentionally kept the key question about breaking RSA-2048 the same. Nonetheless, in order to assess how utilizing relatively large likelihood bins may affect the accuracy of the responses to such a question, we have asked the respondents to provide point estimates, if willing to.

Caution is recommended in interpreting any trend that may appear via a simple comparison with past responses, as it is challenging to disentangle confounding factors (see also the Appendix). Nonetheless, where we notice a trend that could potentially be significant, we point it out, and, where feasible and/or appropriate, we try to provide a rationale that may explain it.

4.1 Physical realizations

With respect to the physical realizations of quantum computers, we asked the respondents to indicate the potential of several physical implementations as candidates for fault-tolerant quantum computing. We specifically asked the respondents to consider the goal of implementing a quantum computer with ~100 logical qubits in the next 10 years[4].

Superconducting systems are still seen as perhaps the strongest competitor. On the other hand, the responses indicate that recent results by cold-atom experiments have made a significant impression among our 2024 respondents, with cold atoms passing trapped ions overall as perceived potential, almost on par with superconducting systems. This follows years during which we have seen the standing of cold-atom platforms improve in our surveys[5].

> *I consider it likely that we will see hybrid systems, that will probably take more than ten years to mature, but which may show great potential on a longer time scale. Example: superconducting + spin qubits.*
>
> KLAUS MØLMER
> University of Copenhagen

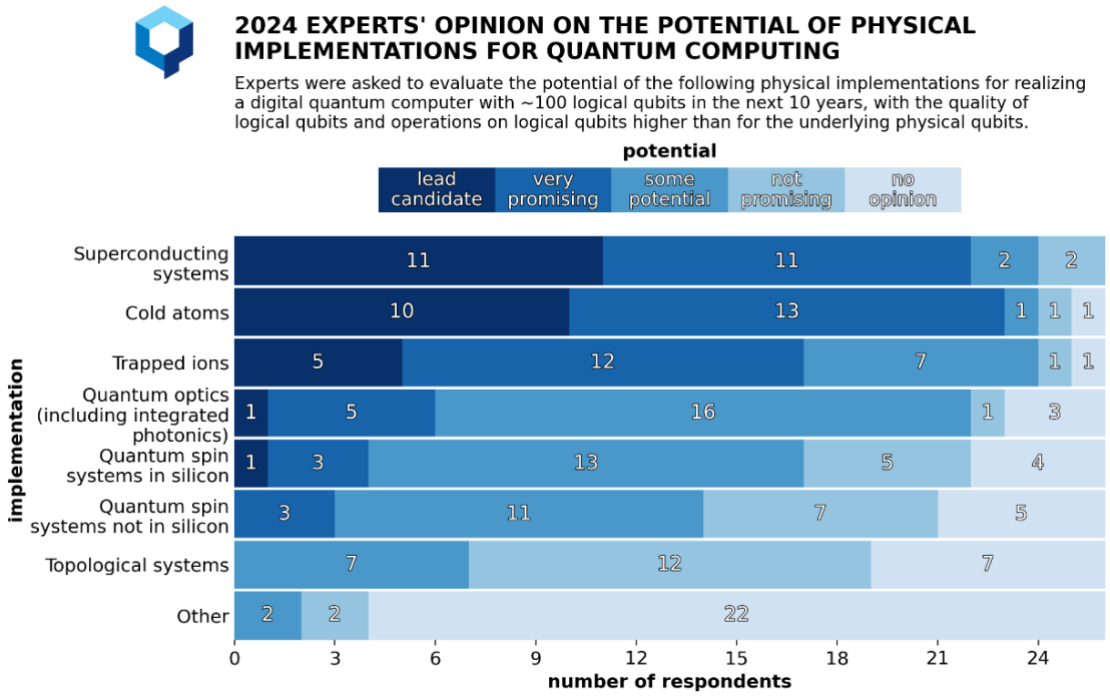


Figure 6: Similarly to previous years, superconducting-system implementations are perceived as presently having some edge over other physical realizations. Recent results have heightened the consideration of cold-atom platforms, which among our respondents have risen above trapped-ion systems for the specific goal indicated in our question.

[4] We changed the question from previous surveys, by focusing on a 10-year timeframe rather than a 15-year timeframe.

[5] It is worth noting that some recent significant experimental results of ion-trap platforms were not available at the time most respondents took the survey.

In this respect, Joe Fitzsimons, CEO of Horizon Quantum Computing, writes:

> *Neutral atoms are rapidly emerging as a leading candidate for scalable quantum computing. Recent results [..] demonstrating error detection and error correction in neutral atom arrays really serve to underscore progress of the technology.*

Daniel Gottesman, a professor at the University of Maryland, summarizes in this way how he perceives the potential of what appear to be the current leading platforms:

> *I feel like superconducting qubits still have the best chance of meeting the benchmark specified in the question, as they are already getting in the ballpark for number of physical qubits and need to get substantially more accurate. In contrast, trapped ions need both an accuracy improvement (although not as much of one) but need to scale up very considerably in size to have 100 logical qubits. Rydberg atoms have recently made a splash, but there are still some critical elements that need improvement.*

Another respondent provided a nuanced comment, pointing to the need to better establish the goal; interestingly, they also show significant optimism for the near future:

> *The question is not exactly well defined, because it depends on the depth of the logical circuits. If we are satisfied with, say, depth-100 circuits, then 100 logical qubits with better fidelity than that of the physical qubits will be realized by error mitigation earlier than by error correction, on both superconducting and ion-trap devices, and will be achievable already in 2-3 years in both these platforms. This might well be the case also for cold atoms. As for error correction, if all we want is to be able to improve the logical error even by a little bit, namely go beyond the breakeven point, I would estimate that all three platforms will achieve this milestone within the next 5 years with almost certainty for 100 logical qubits.*

> *I believe that a successful computer within the next ten years may look quite different than the systems we're working with today. I also expect that for 100 logical qubits, we will likely need to build local networks of smaller processors linked by optical or microwave channels (as we already see in the roadmaps for various companies).*
>
> TRACY NORTHUP
> University of Innsbruck

Some experts point to the potential of spin-systems, particularly when combined with their potential for taking advantage of efficient quantum-error-correcting schemes. For example, Stephanie Simmons, a professor at Simon Fraser University and Chief Quantum Officer of Photonic Inc., wrote:

> *Any spins that have a high-fidelity optical interface and/or shuttling can use QLDPC codes and thus produce logical qubits far sooner than otherwise anticipated*.

Nicolas Menicucci, a professor at RMIT University, makes a thought-provoking suggestion: that of tracking also a classically simulated quantum computer. He provided this rationale:

> *This is a useful benchmark because the marginal benefit of quantum technology is only defined in competition with classical technology. So as classical technology improves, it makes it even harder for quantum technology to show an advantage.*

KEY POINTS

- Several physical implementations of quantum computers are presently being developed; they differ in the kind of physical system that constitutes the fundamental qubit. Each implementation has strengths and weaknesses, which become even more relevant when considering the need to scale to a large number of qubits.
- While certain implementations like superconducting devices may currently be considered leading platform, many other implementations are promising and showing progress. In particular, the last year has seen cold-atoms arrays make quite an impact.
- There might not be just one winner; distinct kinds of physical systems may end up being integrated in modular fashion.

4.2 Quantum factoring

In this survey, as in the ones preceding it, the most directly relevant information about the quantum threat timeline comes from the experts' assessment of the likelihood of realizing a quantum computer able to break RSA-2048 in a short time in response to the following question (see also Appendix A.3):

Q: 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.

Estimates on the practical requirements to achieve such a feat, also considering the imperfections of physical implementations, are presented for example in (Gidney and Ekerå 2021) and (Gheorghiu and Mosca 2025).

> *My sense is that quantum computing is at an inflection point, given the recent demonstration of functioning error correction [..] and the rapid scale-up in qubit number across multiple technologies. Rapid progress in asymptotically good codes also appears to be opening the door to fault-tolerant quantum computing with significantly lower overhead than previously thought.*
>
> JOE FITZSIMONS
> Horizon Quantum Computing

In our surveys, we "only"[6] ask to provide a *likelihood* estimate, expressed as the choice of one likelihood bin among seven such bins, going from "extremely unlikely (<1% chance)" all the way to "extremely likely (>99%)". It is important to stress that such bins are not equally sized in terms of likelihood range: the just mentioned ones cover a range of 1%, while the intermediate bin, "neither likely nor unlikely (~50%)", covers a 40% range, from 30% likelihood to 70% likelihood. Using few bins of unequal size was a design choice, the result of considering:

- the large uncertainty in dealing with this kind of estimates;
- that from a risk assessment and risk management perspective, when dealing with very consequential risk it matters more whether the risk goes from "<1%" to ">1% but <5%" than whether it goes from "<30%" to ">30% but <35%".

We have kept the question the same, including the options for an answer, across the surveys. This year, in order to get some insight into the effect of using few relatively large likelihood bins of uneven size, we asked the respondents to optionally provide single values for the likelihood estimates.

The primary findings of our yearly survey are illustrated in Figure 7, which provides the aggregate distribution of the responses of the experts[7]. It depicts the estimated increase of the likelihood of the quantum threat as we transition from the near future to the more distant one. Some highlights of the collection of likelihood estimates are summarized in Table 1.

[6] Many participants in our annual surveys have emphasized the inherent challenges in making such predictions.
[7] The same data are provided in a more data-sharing-friendly table in Appendix A.4 .

I find it very difficult to estimate the likelihood of building a cryptographically-relevant quantum computer, because there are very few examples of successful engineering efforts that have overcome technical challenges of similar difficulty.

RESPONDENT

We note that there is large variability among the opinions of the experts: some lean towards optimism, while others are more cautious about the pace at which quantum computers will be developed. This is also illustrated in Figure 8 and Figure 9; in the latter, the individual pattern of responses for each expert is displayed.

For some respondents, their highest estimated likelihood for the quantum threat peaks before the 30y mark. For a subset of these, such maximum likelihood is less than the highest possible in our survey. Such perspectives can perhaps be seen as the acknowledgment of potential unforeseen technological hurdles or even insurmountable barriers (see also Section 4.3). One respondent explicitly explains why their estimates were capped at 50%:

In approximately 20–25 years' time, I expect that the objective will either have been reached, or that we will have identified and understood one or more key obstacle preventing it from being reached. This explains why I will not go above a 50% chance in the above estimates.

Figure 10 provides some insight into the effect of using few relatively large likelihood bins of variable size. It plots the trajectories of the point estimates of the respondents (12) who chose to provide also those besides a choice of likelihood bins.

The experts' comments reflect the diversity in the likelihood estimates. On one hand, some experts highlight the still existing chasm between the present quantum computing capabilities and what needed to break RSA-2048. On the other hand, some point to the general encouraging rate of progress and highlight the strong results of the last year. Even some of the more cautious comments often stress the potential for sudden accelerations.

A respondent wrote:

The gap between the current state and the requirement to break RSA is enormous. I think the odds of breaking RSA within 10 years are near-zero, and exactly zero within 5. But progress won't be linear. At some point along the way there may be enough understanding and capability to accelerate progress very suddenly.

Elham Kashefi, a professor at the University of Edinburgh and at the CNRS Sorbonne University, and Chief Scientist of the UK National Quantum Computing Centre, commented:

The recent progress on optimised quantum circuit for new factoring algorithms, better error correcting codes, and impressive list of demonstration of fault tolerant QC components all indicate that the timeline could suddenly shift quickly as a combination of these complementary efforts.

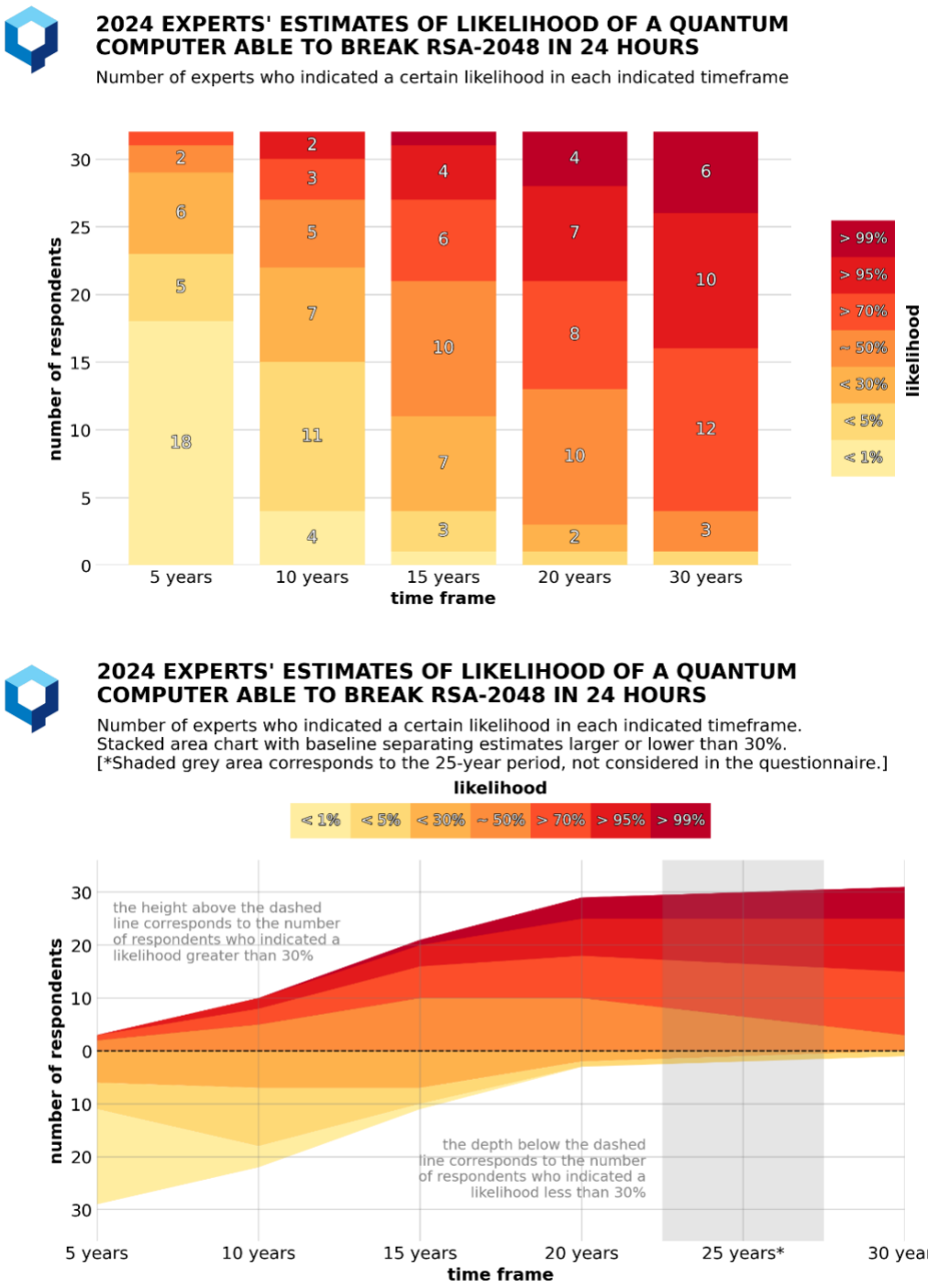


Figure 7 This figure illustrates the central information collected through our survey. The experts were asked to indicate their estimate for the likelihood of a quantum computer that is cryptographically relevant—in the specified sense of being able to break RSA-2048 in 24 hours—for various time frames, from a short term of 5 years all the way to 30 years.Top: stacked barchart with explicit indication of the number of experts estimating a certain likelihood. Bottom: stacked area chart conveying the same information, but allowing one to better appreciate the shift in likelihood estimates moving from short-term to long-term timeframes. Please note the inclusion of a dummy 25y timeframe.

TIMEFRAME	WHAT ONE MAY EXPECT BASED ON THE EXPERTS' OPINIONS ON THE LIKELIHOOD OF A QUANTUM COMPUTER ABLE TO BREAK THE RSA-2048 CRYPTOSYSTEM (IN 24 HOURS)
NEXT 5 YEARS	Most respondents (18/32) assessed the likelihood of a cryptographically relevant quantum computer emerging within the next five years as "extremely unlikely (<1% chance)." Approximately 13% (4/32) believe the likelihood is "very unlikely (<5% chance)," while almost a fifth (7/32) indicated it to be "unlikely (<30% chance)." Two respondents consider the event as having "about 50% chance" and one thinks it is even "likely (>70% chance)." Overall, *there seems to be a non-negligible chance of an impactful surprise within what would be considered a very short-term future.*
NEXT 10 YEARS	While 15 out of 32 respondents consider a CRQC "extremely unlikely" or "very unlikely", already 17 respondents consider it 5% or more likely. Among the latter, 5 respondents considered it about even ("~50%"), and 3 considered it "likely" (3/32) or "very likely" (2/32). We conclude that *there is a significant chance that the quantum threat becomes concrete in this timeframe*.
NEXT 15 YEARS	The majority (21/32) of respondents indicated "~50%" likely or more likely, among whom 11 indicated a likelihood greater than 70%. That is, w*ithin this timeframe, a significant majority of respondents assigns to the existence of cryptographically relevant quantum computer an about even likelihood or better.*
NEXT 20 YEARS	A majority (19/32) of the respondents indicated "likely (>70% chance)" or more likely, among whom 11 indicated a likelihood greater than 95%: *within this timeframe, the realization of the quantum threat appears to be seen as substantially more likely than not.*
NEXT 25 YEARS	We did not directly probe this timeframe in our questionnaire, as we believe the unavoidable uncertainty involved in the estimates does not warrant a such a fine-grained distinction between what may happen between 20 years and 30 years from now. In some graphs, this timeframe may be included by showing interpolated values, for the sake of preserving a linear timescale.
NEXT 30 YEARS	Twenty-eight experts out of 32 (88%) indicated that the quantum threat has a likelihood of 70% or more this far into the future, with 6 of the experts indicating a likelihood greater than 99%: *in general, there is a relatively low expectation of issues that would prevent a cryptographically-relevant quantum computer from being realized in the long run.*

Table 1 Summary analysis of the experts' likelihood estimates at the core of the present report.

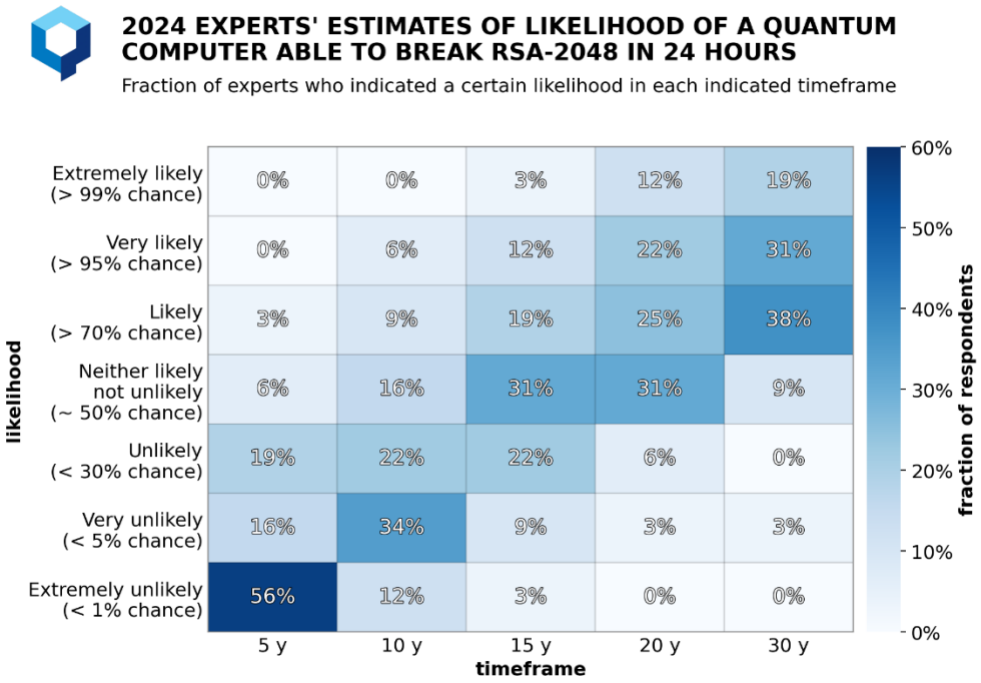


Figure 8 Heatmap and percentages for the distribution of the likelihood estimates of the 2024 survey, displaying the diversity in the opinion of the experts.

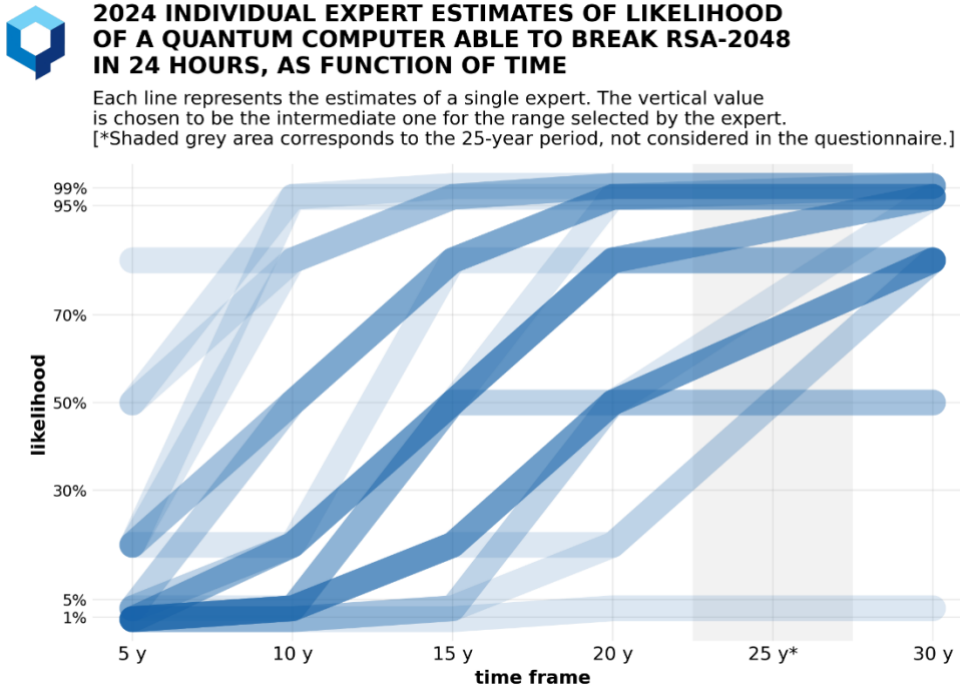


Figure 9 This figure illustrates the likelihood estimates of the individual experts, represented as growing curve in time. This plot allows one to appreciate not only the significant variance of the estimates for each timeframe considered, but also the diversity in how each expert estimates the likelihood will grow in time. One can nonetheless identify more common and more similar "trajectories" that are visually more opaque in this kind of plot.

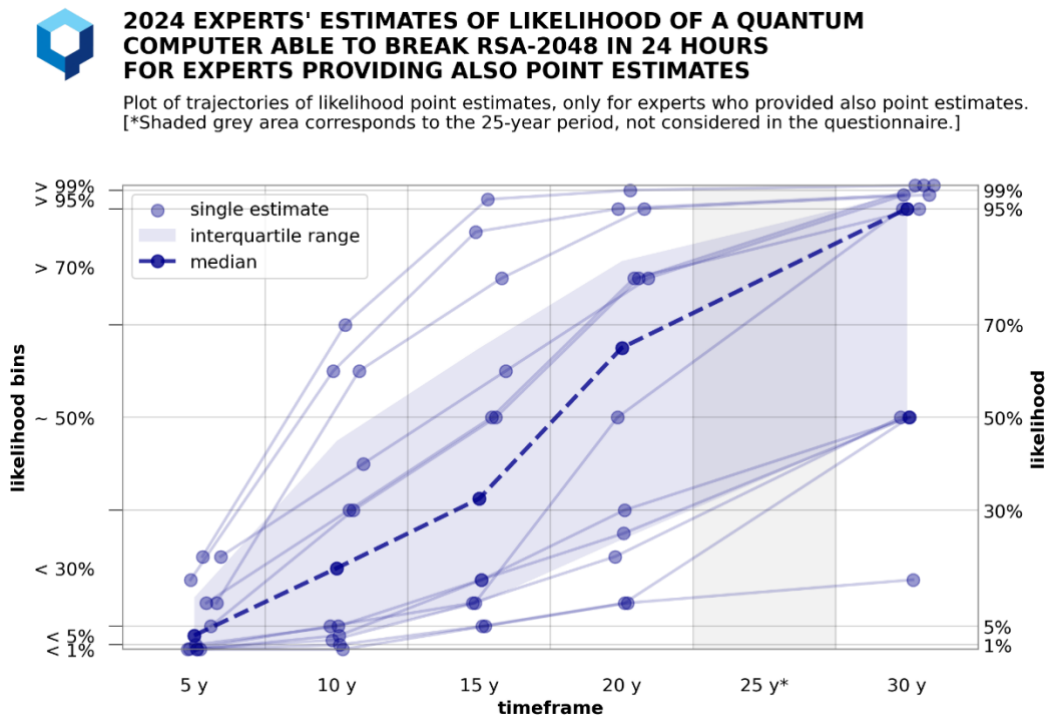


Figure 10 Comparison of choice of likelihood bins and likelihood point estimates for the 12 respondents who provided point estimates. This allows one to get a sense of the extent to which the bin-based likelihood estimates capture the best numerical estimates of the experts, and of the variability of the responses directly in terms of numerical likelihood, rather than in terms of likelihood bins.

4.2.1 Coarse-grained likelihood estimates

We aim to summarize succinctly the insight that the experts provided, to arrive at some single likelihood estimate. We do this by averaging the estimates of the experts.

We may interpret the choice of one of the likelihoods, e.g., "*likely*", as the indication of a numerical probability in the range associated to it, i.e., in this case, a probability greater than 70% but less than 95%. In general, we do not know what the best point estimate of each respondent for each timeframe would have been, although we have this information for a limited set of 12 respondents (see Figure 10).

We take a conservative approach and consider the two extreme alternatives where each respondent is assigned either the higher or the lower of the extreme values of the range they picked. This can be roughly described as considering a "pessimistic interpretation" or, alternatively, an "optimistic interpretation" of the answers' ranges. This approach allows us to calculate an average cumulative probability

Even in a '*pessimistic*' interpretation of expert likelihood estimates as the lowest compatible probability for a given likelihood range, the average probability associated to the disruptive quantum threat is already ~19% in the next 10 years.

2024 OPINION-BASED ESTIMATES OF THE CUMULATIVE PROBABILITY OF A DIGITAL QUANTUM COMPUTER ABLE TO BREAK RSA-2048 IN 24 HOURS, AS FUNCTION OF TIMEFRAME

Estimates of the cumulative probability of a cryptographically-relevant quantum computer in time: range between average of an optimistic (top value) or pessimistic (bottom value) interpretation of the estimates indicated by the respondents, and mid-point. [*Shaded grey area corresponds to the 25-year period, not considered in the questionnaire.]

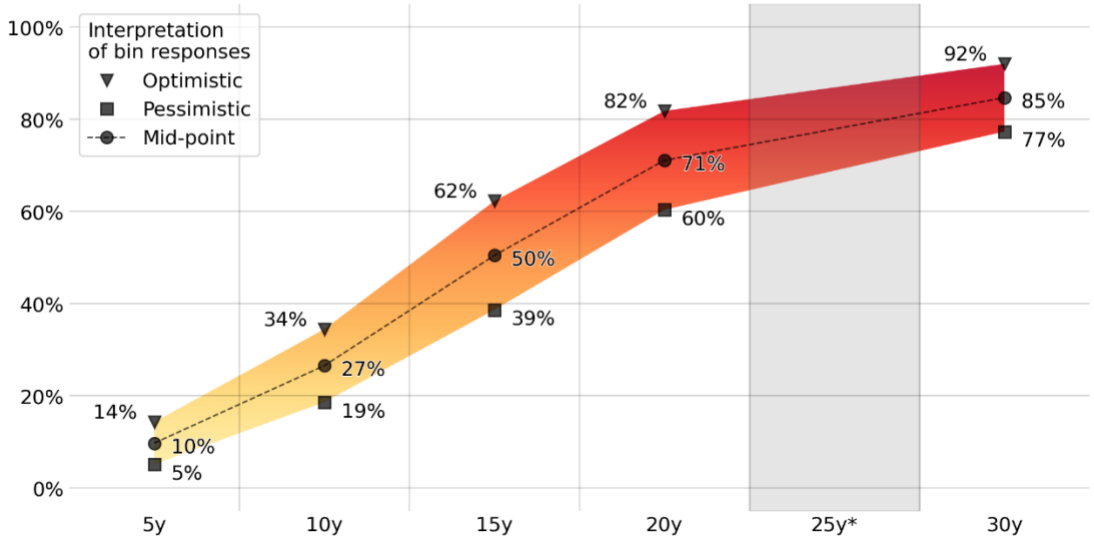


Figure 11 One way of reducing the set of likelihood estimates provided by the experts to some aggregate likelihood is that of interpreting optimistically or, alternatively, pessimistically, the answers of each respondent within the likelihood range they indicated, and averaging over the respondents. Note that, in line with the notion that all likelihood estimates are necessarily vague and imprecise and unable to really differentiate between 5-year intervals far in the future, we did not inquire about expectations for the 25-year timeframe; we introduced a dummy column in the figure to restablish a linear scale on the horizontal temporal axis.

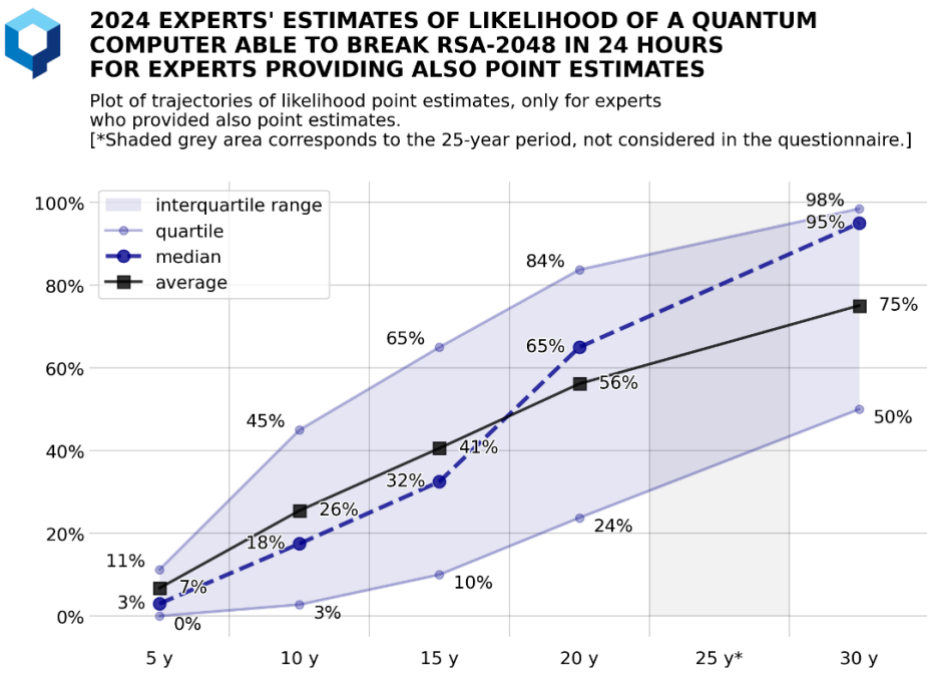


Figure 12 Mean, median and quartiles for the limited number (12) of respondents who provided best point likelihood estimates. This chart focuses on some aspects of the information presented already in Figure 10.

distribution for both interpretations. Had each respondent selected a precise estimate within the respective ranges, then the average estimate for the likelihood would sit in the range between the optimistic-interpretation and pessimistic-interpretation curves. In turn, the latter two curves provide what we may consider some notion of uncertainty about the average likelihood assigned by the experts, reflecting the width of the likelihood bins. An idea about the dispersion of the estimates is provided by Figure 8 and Figure 9. In Figure 11, we also show a mid-point estimate, which should not be interpreted as best estimate. More details on the method are given in Appendix A.4 .

One can appreciate the dispersion of the likelihood estimates also by looking at the distribution of the point estimates, for those respondents who chose to provide such point estimates (see Figure 10). Only 12 respondents volunteered this kind of information, thus not providing the same diverse range of views as the full set of respondents. In addition, we have discussed the rationale for not primarily asking the respondents to necessarily provide such kind of precise estimate. Overall, we do not present the analysis of point estimates as our major finding. Nonetheless, it is useful to consider an aggregation of those responses to compare with Figure 11: means, median, and quartiles of the point estimates are presented in Figure 12. Furthermore, in the Appendix we provide an additional version of Figure 11 where the point estimates – rather than the likelihood-bin values – are used in the averages for those respondents who provided a point estimate (Figure 26).

In general, Figure 11 should be interpreted cautiously as it is a coarse-grained summary of our respondents' opinions, but it offers valuable summary information. For example, even in a 'pessimistic' interpretation of responses, as the lowest compatible probability for a given likelihood range, the average probability associated by the above-described analysis to the disruptive quantum threat is already ~19% in the next 10 years and growing quickly in the timeframes that follow. Still within a

'pessimistic' interpretation, the average estimated probability is ~39% by the 15-year mark, and ~60% by the 20-year mark.

It is worth stressing that skewed distributions and/or outliers may affect the significance and interpretability of averages. Figure 8, Figure 9, Figure 10, and Figure 12 convey insightful information about the distribution of responses. They show how the responses spread out at 10y and 15y, where the estimates of the experts may differ more as there is more uncertainty in the rate of progress. On the other hand, the response distribution is quite skewed in the shortest timeframe of 5y – most experts think a CRQC is relatively unlikely – and in the longer timeframes of 20y and 30y – most experts think a CRQC is quite likely.

4.2.2 Comparison with previous years

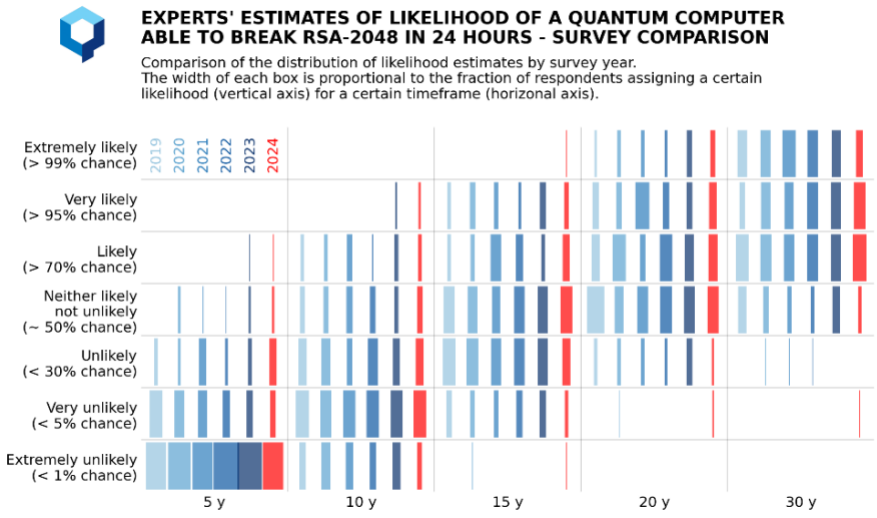
Our series of surveys, started in 2019, allows us to track changes in the likelihood estimates from survey to survey. We think this is useful for at least the two following reasons:

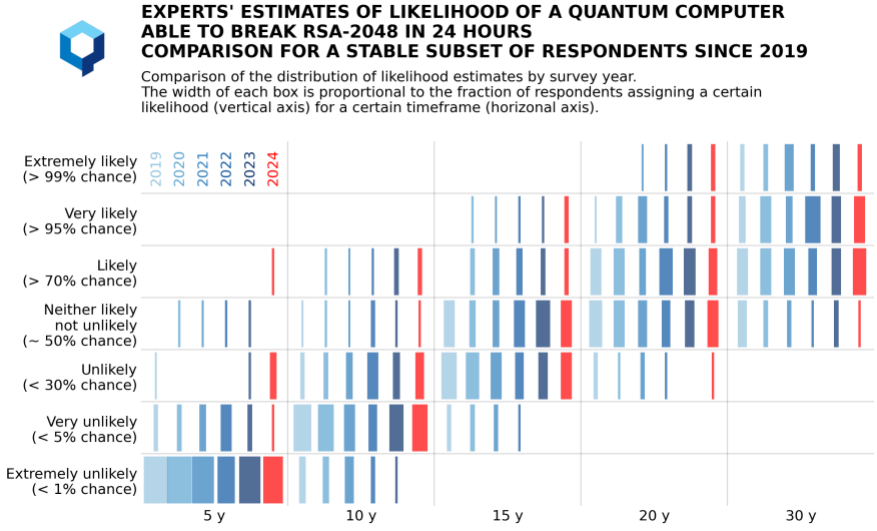
- it provides information on whether the sentiment expressed by the experts is becoming more pessimistic or more optimistic, as their opinions get affected by changing circumstances and recent progress; in turn, a change of sentiment may be interpreted in terms of a likely slowdown or speedup for the development of a quantum computer;
- it provides "differential" information that is conceivably less dependent on the baseline attitude of the pool of experts.

We stress that, while caution is already advisable when interpreting single-survey data, year-to-year comparisons carry additional risks. Among other factors, spurious signals may be introduced by changes in the composition and size of the pool of respondents, by year-to-year fluctuations in the responses – particularly relevant when dealing with small pools of respondents – and by the relatively wide and unequally spaced likelihood intervals we consider.

In Figure 13, we plot the distribution of the likelihood estimates, for each survey conducted so far – six surveys, from 2019 to 2024. We use distributions rather than the absolute number of respondents so that it is possible to compare surveys with different numbers of respondents. The top graph in Figure 13 considers all respondents for each survey; the middle graph is for the set of 14 respondents who regularly participated in our survey since 2019 (see Appendix for a list); finally the bottom graph is for the larger set of respondents that regularly participated in our survey since 2022. In Figure 14, we plot the average likelihood intervals for each survey, similarly to what was done in Figure 11 for just the 2024 survey. The top and the two bottom graphs refer to all respondents and to the just mentioned stable subsets, respectively.

Figure 15 and Figure 16 compare survey responses across the years by shifting the plots to match forecasts in absolute time. Overall, it appears that there is general consistency between the likelihood estimates from survey to survey, when considering the absolute time they refer to. E.g., an estimate made in 2019 for 10 years into the future, that is, for 2029, should be compared to an estimate made in 2024 (this year) for 5 years into the future. Such a consistency, which is stronger when focusing on stable sets of respondents, suggests that the experts perceive that continuous consistent progress is being made.





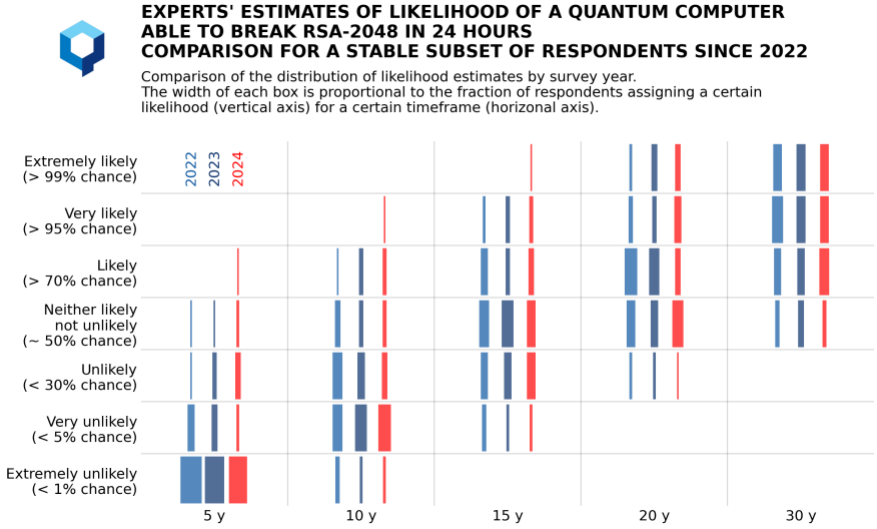


Figure 13 Distribution of the likelihood estimates for each survey conducted so far. Top: likelihood estimates for all the respondents to each survey. Middle: likelihood estimates for the subset of respondents who took part in all the surveys so since 2019. Bottom: likelihood estimates for the subset of respondents who took part in all the surveys since 2022.

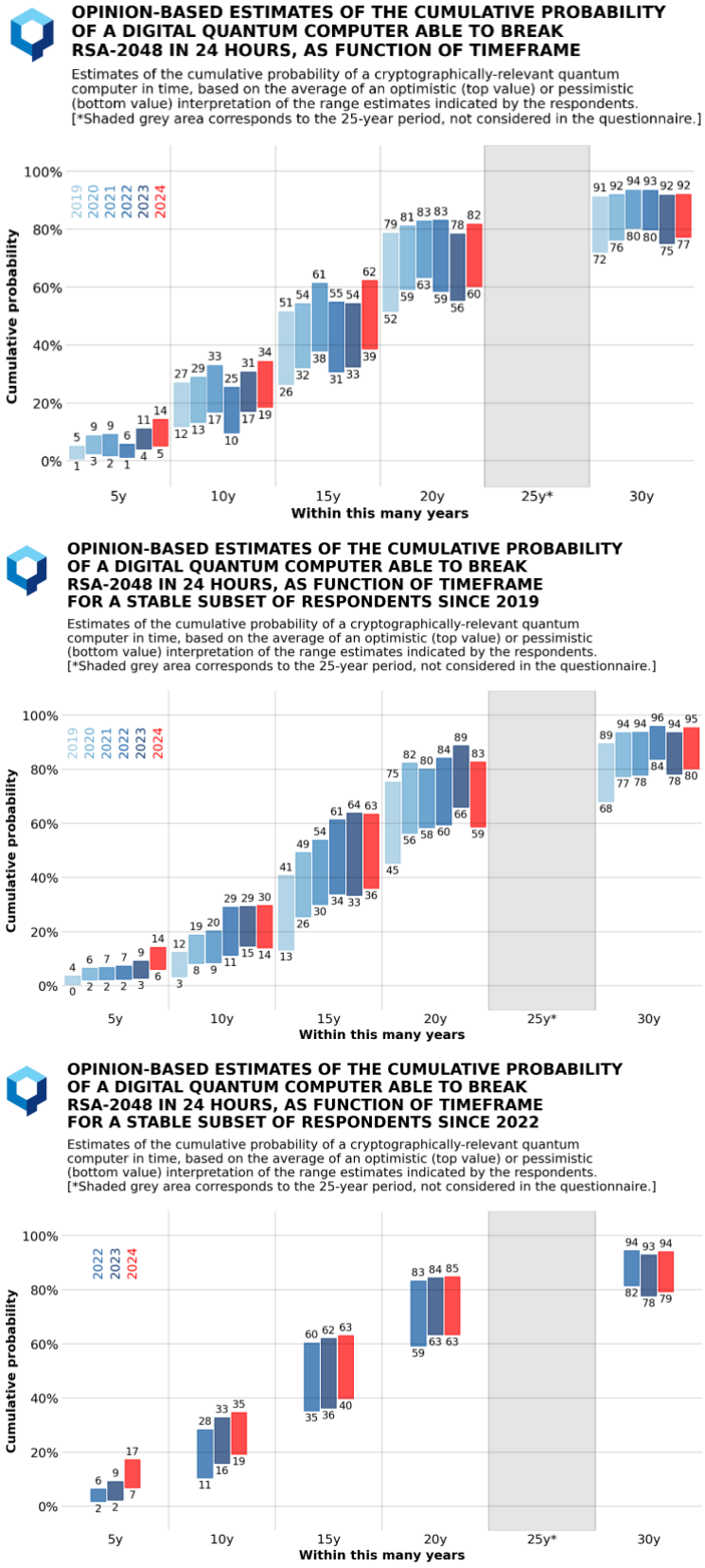


Figure 14 Evolution of the likelihood estimates by the experts in surveys about the quantum threat timeline conducted so far, for all respondents (top), for the stable subset of respondents since 2019, and for the stable subset of respondents since 2022 (bottom). Survey by survey and timeframe by timeframe comparison of such estimates. Note the inclusion of a dummy 25-year timeframe (grey area).

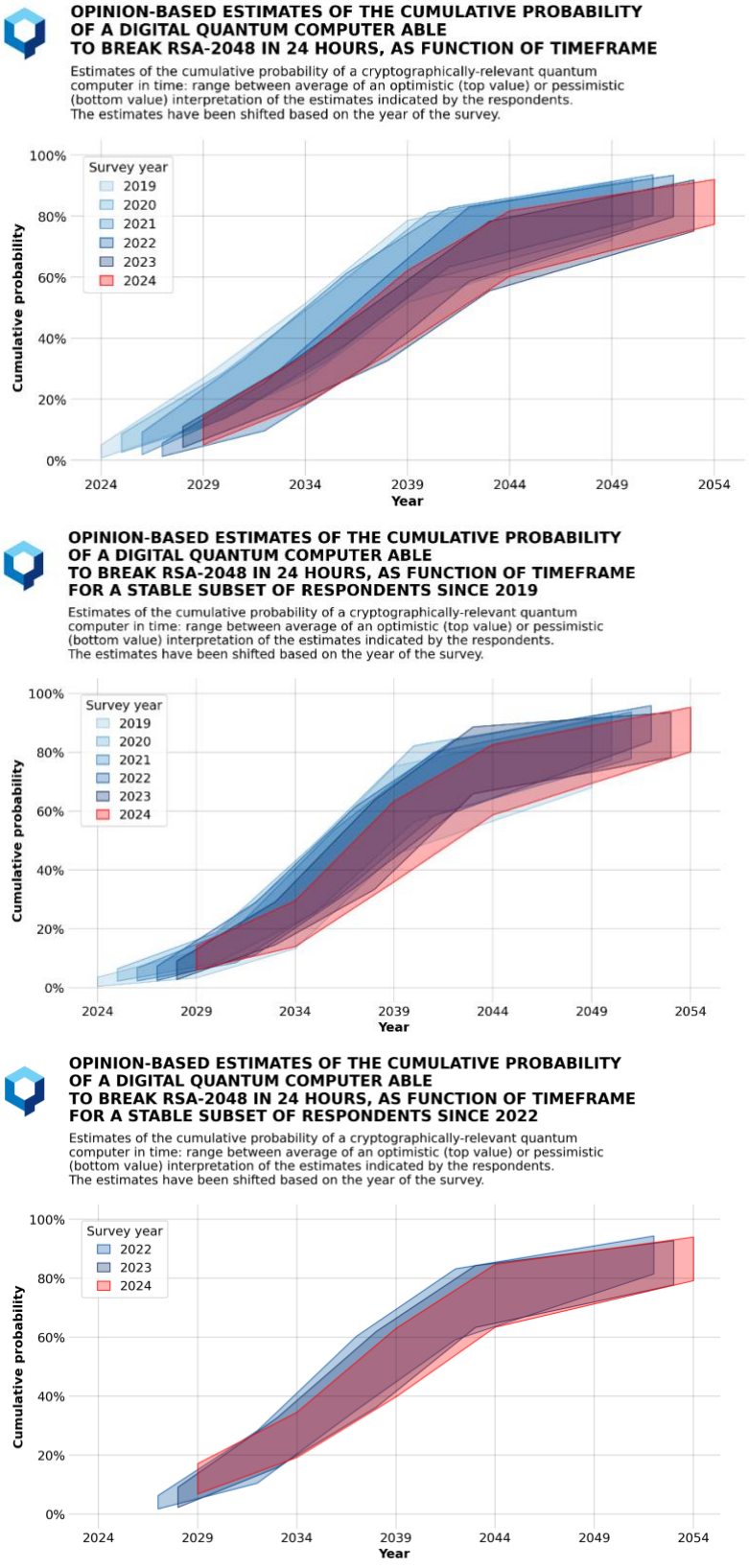
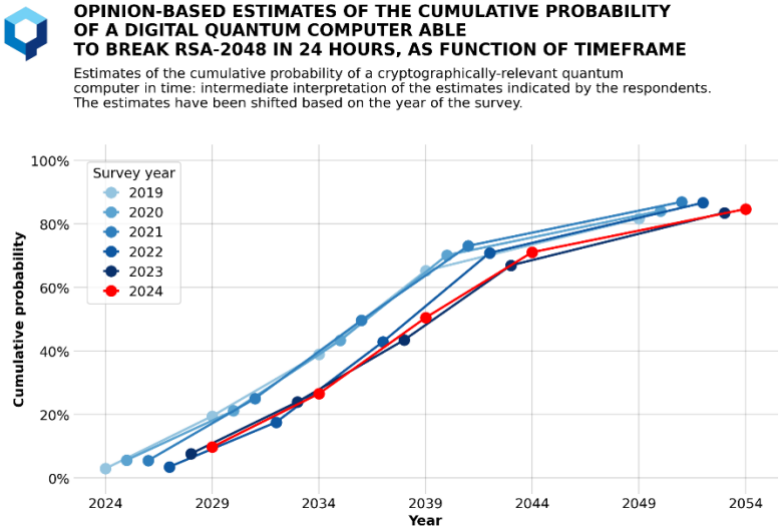
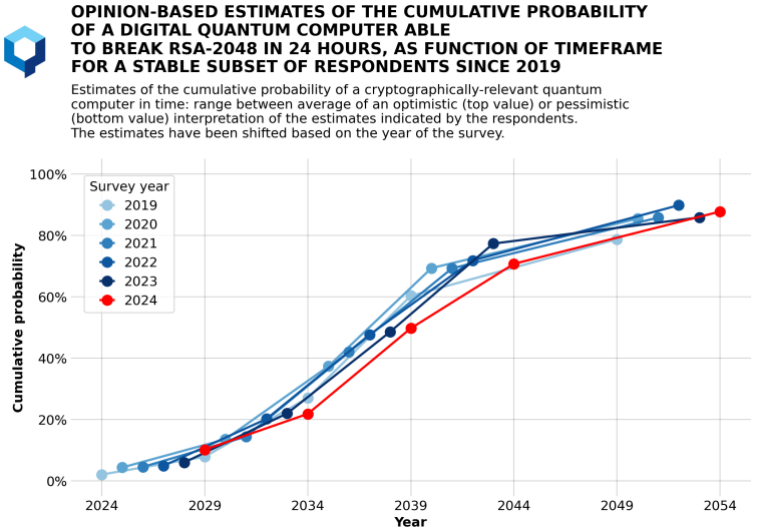


Figure 15 Comparison of the change of the coarse-grained estimates from survey to survey. The kind of range for coarse-grained estimates presented in Figure 11 for the 2024 survey is plotted for the previous surveys too. The plots are shifted so that the estimates produced in each survey align with respect to absolute time. Top: the computation includes all the responses in each survey. Middle: only the responses of the group of participants to all the surveys since 2019 are considered in computing the estimates of each survey. Bottom: same as the middle plot but only for the stable respondents since 2022.





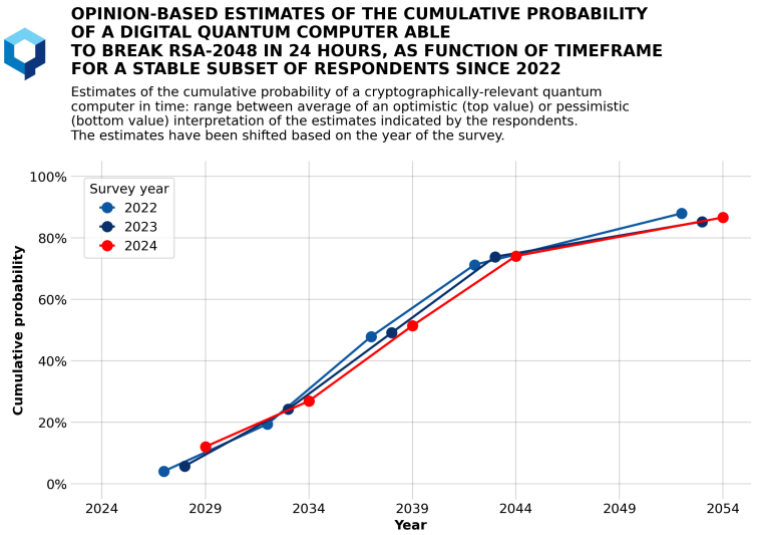


Figure 16 Comparison of the change of the coarse-grained estimates from survey to survey. The mid-point for coarse-grained estimates presented in Figure 11 for the 2024 survey is plotted for the previous surveys too. The plots are shifted so that the estimates produced in each survey align with respect to absolute time. Top: the computation includes all the responses in each survey. Middle: only the responses of the group of participants to all the surveys since 2019 are considered in computing the estimates of each survey. Bottom: same as the middle plot but only for the stable respondents since 2022.

KEY POINTS

- Year after year we have asked our pool of experts to provide their best likelihood estimate for when a quantum computer will be able to perform relatively quickly a specific cryptographically relevant task: breaking RSA-2048.
- The experts display a significant variety of opinions, but on average the likelihood of a cryptographically-relevant quantum computer grows quickly in time to what is an intolerable risk from a cybersecurity perspective.
- Even in a 'pessimistic' interpretation of the estimate associated to a given likelihood range, the average probability overall assigned to the disruptive quantum threat is already ~19% in the next 10 years.
- In an 'optimistic' interpretation, the average likelihood is the highest in our surveys so far both for the next 5 years (14%) and for the next 10 years (34%).
- Considering when the various surveys were run, the likelihood estimates for a specific time in the future are roughly compatible from survey to survey, and even more so when considering stables subset of respondents; this suggests that the experts perceive that continuous consistent progress is being made.

4.3 Potential Concerns

As reported in Section 4.2, 16 of the 32 experts have indicated less than a 95% chance 6hat a CRQC will be built within the next 30 years; of these 15 experts, 4 have estimated a likelihood less than 70%. We would like to better understand the rationale behind such estimates. In general, various reasons why a cryptographically-relevant quantum computer may take 30 years or longer to be built (if ever) have been articulated. We asked the experts to provide their opinion on the level of concern elicited by the following possible issues:

> *Technical challenges are certainly real and have been ongoing for a long time. I don't think by themselves they are likely to be sufficient to fully stop the development of quantum computation but could certainly slow progress by some unknown amount.*
>
> DANIEL GOTTESMAN
> University of Maryland

- new-physics phenomena, like a hypothesized random collapse of the wavefunction;
- yet unappreciated standard-physics phenomena that may disrupt quantum computation, like some yet unappreciated unavoidable source of correlated noise;
- yet unappreciated fundamental trade-offs in controlling quantum features, that is, something akin to the uncertainty principle;
- excessive technical challenges / requirements not attributable to any of the above, which, despite no being fundamental limitations, would make the scaling to a fault-tolerant quantum computer practically impossible.

The level of concern could be classified from a highest “Reasonable concern with substantial likelihood” down to the second-lowest “Reasonable concern but very unlikely” or the lowest “Concern is not appropriate”. The results are reported in Figure 17.

The experts consider the well-known technical challenges quantum researchers face daily as the most reasonable and likely issue that could delay the creation of a CRQC. Nonetheless, the experts express the general opinion that such challenges are being overcome, so a working CRQC should be considered an issue of “when” rather than “if”. One respondent wrote:

> *Given the amazing advances in hardware of the past few years and most importantly, in the past year, not just in one but in a variety of platforms [..], and in particular the evidence that are now accumulating that the break-even point for quantum error correction had either already been crossed or is extremely close to it, it seems to me that the skeptics must phrase their concerns on much (much) more solid grounds, or simply not express them at all.*

Given the above opinions it is unsurprising that far second, as a relatively reasonable concern, is the issue of known physical phenomena which may impact quantum computers more negatively that one may currently expect. In this respect, one respondent highlighted the obstacle posed by noise from cosmic rays.

Under “Other”, some respondents indicated the possibility that the economic and societal conditions, a shift in interest, or any other dynamics within the research community will be such that not enough

resources will be employed to quickly complete the path to a CRQC. One interesting point is made by Klaus Mølmer, a professor at the Niels Bohr Institute of the University of Copenhagen:

> *The global installation of Post-Quantum Cryptography will significantly reduce the motivation by sponsors and authorities to build a fault-tolerant factoring machine and focus efforts on fault tolerance and error mitigation in simulators that will not be optimal for factoring.*

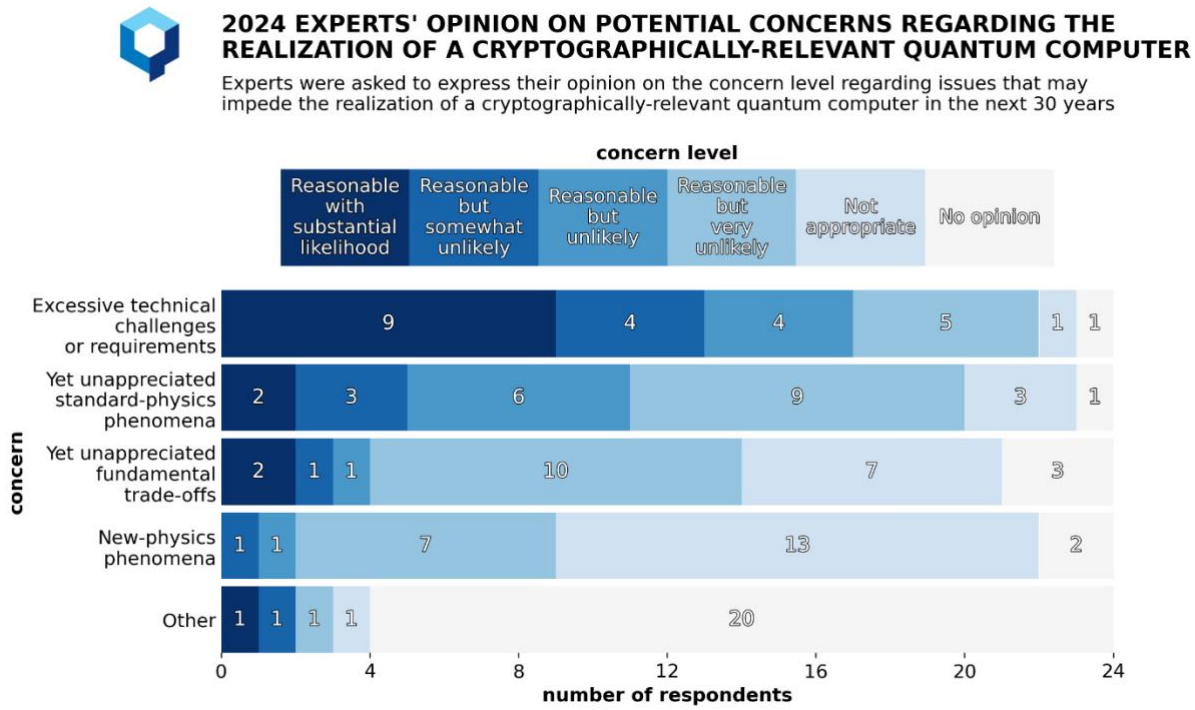


Figure 17 Experts' opinion on a number of concerns that may push the realization of a CRQC further in the future than our longest timeframe of 30 years, or impede it completely. See main text for details.

KEY POINTS

- Various reasons why a Cryptographically-Relevant Quantum Computer (CRQC) may take 30 years or longer to be built (if ever) have been articulated.
- The experts consider the well-known technical challenges quantum researchers face daily as the most reasonable and likely issue that could delay the creation of a CRQC.
- The experts express the general opinion that such challenges are being steadily being overcome, so the realization of a CRQC should be considered an issue of "when" rather than of "if".

4.4 Most important upcoming experimental milestone

For those tracking the quantum threat, it would be helpful to have a clear and meaningful milestone between today's current state and a CRQC that convincingly confirms that the major obstacles have been tamed. In order to better understand what such a signal could be, in the present survey we have posed the following question:

Q: What do you consider the most important upcoming experimental milestone to convincingly demonstrate the feasibility of building a cryptographically-relevant fault-tolerant quantum computer?

Most experts would like to see results regarding error correction, the logical encoding of quantum information, and, most importantly, the logical manipulation of quantum information. Scalability is a key aspect, and in the responses it is unsurprisingly associated with modularity, including interconnectivity of modules.

> *The experimental realization of a fully controllable logical qubit prototype, that is interconnectable, and that demonstrates error suppression as the code distance increases, and that in these respects is scalable.*
>
> RESPONDENT

Daniel Gottesman wrote:

Demonstration of fault-tolerant circuits with unambiguously lower error rates than the corresponding unencoded circuits, in a way that doesn't depend on choice of comparisons or which circuits are performed.

In his response Nicolas Menicucci provides quantitative platform-dependent targets:

1) Superconducting qubits [..] – in this case, the experimental milestones are (a) error rates below 1% and (b) quantum interconnection between three or more cryostats. (I made up the specific numbers – the point is to demonstrate low error rates and scalability.)

2) Photonic qubits [..] – a large-scale cluster state or large-scale fusion-based quantum computing must be demonstrated (> about 100 qubits). To date, we haven't seen any large-scale demonstrations of multi-photon entanglement [..].

3) Bosonic qubits [..] – a GKP state with squeezing above 10 dB. If that can be done, there's a chance for fault tolerance. Until it's done, there will always be doubts. [..]

> *In short, the demonstration of horizontal scale via modularity: high universal control fidelity and entanglement fidelity across remote modular quantum processors at a rate much faster than the coherence time, and ultimately the logical clock cycle time, of the constituent qubits.*
>
> STEPHANIE SIMMONS
> Photonic Inc.
> & Simon Fraser University

While there is some form on consensus on the type of milestone – see above – the "evidence" required varies both in capability of the devices involved and in the level of detail the experts go into when describing it. Nonetheless, we thought it would be useful to gather information about when each expert expects *their* specific milestone to be achieved. This could arguably be interpreted as information about when the experts expect the realization of a CRQC not to happen but to be convincingly proved as possible. A summary of the responses is reported in Figure 18.

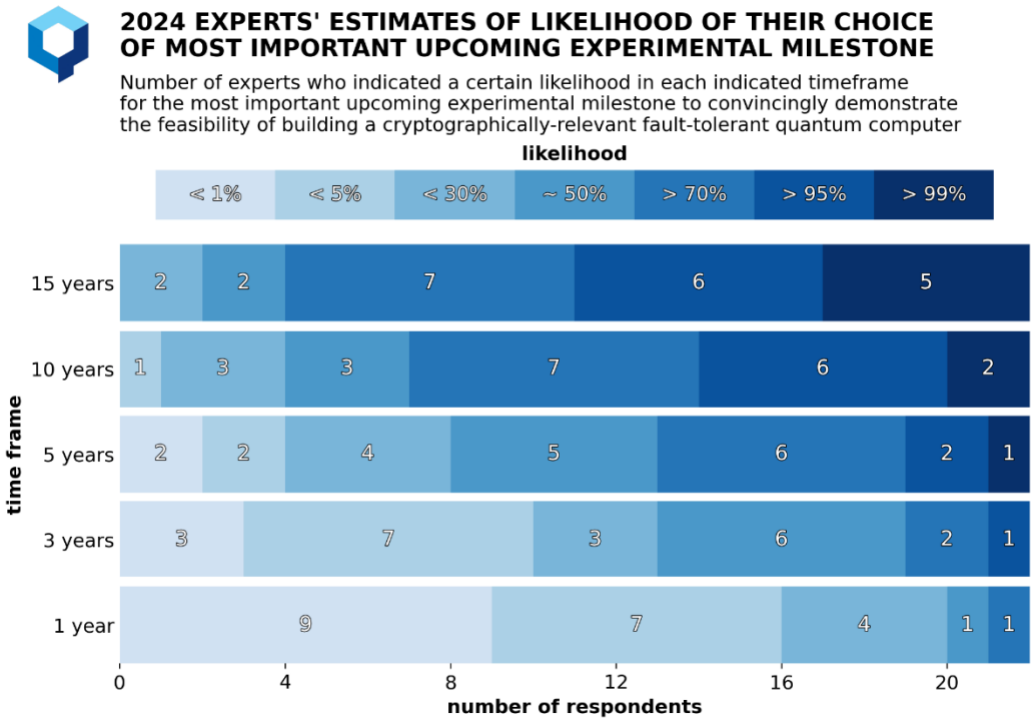


Figure 18 The experts were asked about the likelihood in time for the next most important upcoming experimental milestone to convincingly demonstrate the feasibility of building a CRQC. Each expert considered/described a potentially different milestone. See main text.

KEY POINTS

- We asked the experts about a clear and meaningful milestone, between today's current state of quantum computing development and a CRQC, that would convincingly confirm that the major obstacles towards a CRQC have been tamed.
- Most experts would like to see results regarding error correction and the manipulation of logical qubits, showing that errors and noise can be suppressed sufficiently well and efficiently, thus paving the road to the required scaling of the technology.

4.5 Most promising scheme for fault-tolerance

Fault-tolerance will be reached by the combination of improved performance of hardware implementations with a suitable error-correction / fault-tolerant scheme (see Appendix A.2). We have asked the experts to share their opinions on the most promising among such schemes.

I think the race is still open and many different schemes are making impressive progress.

YVONNE GAO
National University of Singapore

A straightforward answer is not possible; in the words of one respondent:

> *Quantum error correction is currently a very active research area. As time progresses, it is likely that we will see more advances. This in particular as systems are scaled up. We may also see adaptations to various hardware architectures, hybrids of error-correction schemes, and so forth.*

Correspondingly, the responses of the experts were relatively nuanced, highlighting for example that the choice of error-correction code may vary by architecture, and that even the same architecture may use different codes depending on the tasks – for example, memory vs computation.

Some variation of the surface code is still considered a leading choice for superconducting implementations, but quantum Low-Density Parity-Check (LDPC) codes (see Appendix) are actively being developed, including the study of how to best implement them in hardware. This is because such codes improve the encoding rate, that is, a smaller number of physical qubits is needed per logical qubit.

Daniel Gottesman emphasizes how open the question of which is the best fault-tolerant scheme is:

> *Fault tolerance with high-rate LDPC codes. However, I think the specific protocols that will be the best have not been developed yet. I also think the specific code is not going to be fixed but will change while running the protocol.*

Stephanie Simmons is very optimistic about LDPC codes:

> *[Quantum]LDPC codes are just so overwhelmingly advantageous on basically all metrics that it is great to see that most teams are designing for their implementation now – a complete turnaround in under 1 year.*

Other proposals for fault-tolerance that aim at reducing error correction overhead are based on encoding quantum information into physical qubits that are inherently protected against certain types of error, like qubits encoded in states of harmonic oscillators – so-called bosonic qubits. For such qubits, error correction schemes can focus on the remaining types of error.

KEY POINTS

- Research on quantum error-correction is a very active field and could see significant breakthrough results.
- The choice of error-correction code may vary by architecture. Some variation of the surface code is still considered a leading choice for superconducting implementations, but quantum Low-Density Parity-Check (LDPC) codes are actively being developed and adapted to hardware.

4.6 Useful applications of intermediate quantum processors

Developing quantum computers capable of compromising modern cybersecurity systems may still take considerable time. The rate at which these powerful machines are developed largely depends on the level of funding dedicated to quantum computing research. This funding may originate from research grants, venture capital investments, or income generated from preliminary applications of quantum technology. While there are several ways to encourage investment and generate revenue, having commercially viable applications would significantly boost the likelihood of sustained financial support for advancing quantum computing to the point where it could impact cryptography. Consequently, we sought expert opinions on the matter, by asking the following:

> *I think it is a good question to ask: We are approaching the point in time where quantum computers will have to begin creating value by delivering solutions to practically relevant problems. This so as to ensure continued investments.*
>
> RESPONDENT

Q: Please indicate your likelihood estimates for useful commercial applications of available processors – or of larger/less noisy processors but anyway not yet cryptographically-relevant – going beyond proof-or-concept and/or promotional activities, within the indicated timeframes.

The likelihood estimates provided by the respondents are summarized in Figure 19.

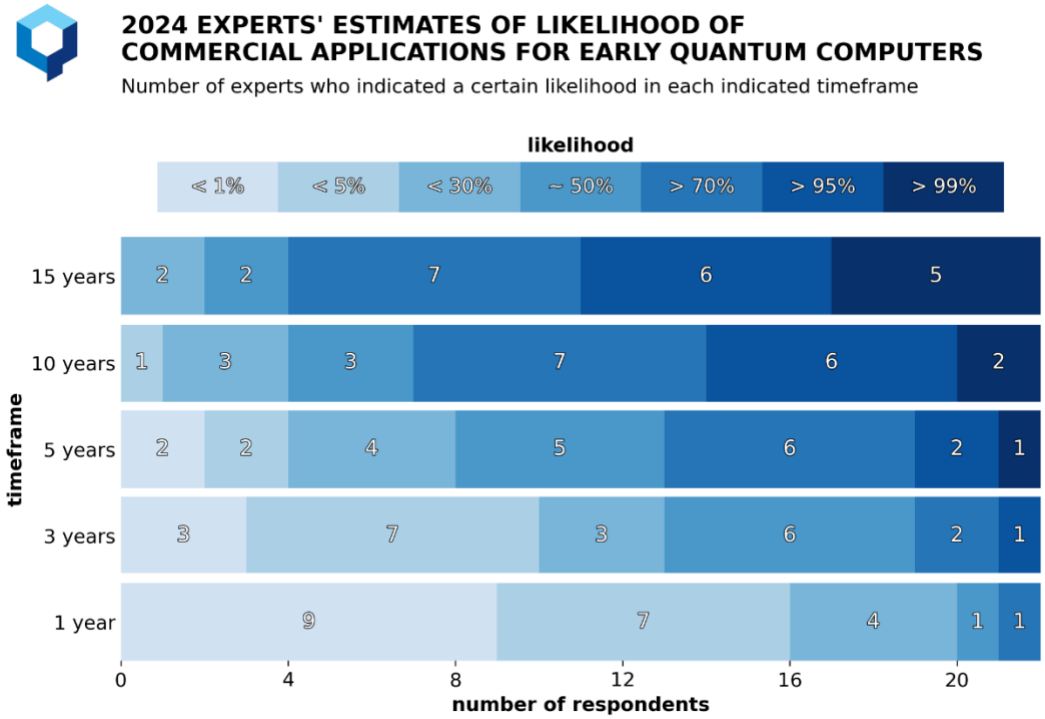


Figure 19 We asked the experts to indicate the likelihood for commercial applications of "early" quantum computers / quantum processors not powerful enough to be directly relevant from a cryptographic perspective. Not all experts expressed an opinion in this sense, but among those who did, more than half indicated a likelihood of about 50% or more within 5 years.

One cannot predict what type of new application or algorithms will emerge. [O]nce we enable true collaboration between academia and industry we could identify much wider notion of quantum advantage.

ELHAM KASHEFI
UK National Quantum Computing Centre
& University of Edinburgh
& CNRS

Several respondents speak of quantum computers used for simulations in quantum physics and quantum chemistry. A respondent makes it clear that one needs to distinguish between research-oriented applications and commercial applications for industries, also when it comes to the timeline:

> *Research centers will buy accurate simulators of quantum systems that cannot be simulated classically – [this] will be available within the next year. [C]ommercial applications of interest for industries rather than physicists [..] will likely be available as soon as two- or three- thousand physical qubits will be available, which are highly likely to be available in 4 years.*

Yvonne Gao, a professor at the National University of Singapore, emphasizes that it is a matter of matching capabilities of devices with suitable interesting problems:

> *The challenge is not only on making quantum hardware better but also figuring out what is a useful and tractable problem to solve for a given hardware capability. The latter is not a trivial question at all.*

KEY POINTS

- The experts express hope – and in some cases belief – that there will be useful applications of early quantum computing devices, significantly before a CRQC is realized.
- The respondents mention a potential useful role of such devices for simulations in quantum physics and quantum chemistry.
- Quantum computers will be proven useful first in a research context and later for commercial applications.
- It is difficult to predict future uses; collaboration between academia and industry will be instrumental in identifying opportunities for a quantum advantage.
- Figuring out what is a useful and tractable problem to solve for a given hardware capability is a challenging question.

4.7 Societal and funding factors

This section contains the results for the questions assessing how societal and funding factors may impact the timeline of the development of a cryptographically-relevant quantum computer.

4.7.1 Level of funding of quantum computing research

Long-term investments are essential to advance the development of a fully fault-tolerant quantum computer. As global leaders in this field—engaged in both national and international projects, collaborating with industry, and leading start-ups—our respondents possess a unique perspective for assessing the trajectory of funding.

As done since 2020, we have asked them to forecast what was likely to happen with respect to funding in the coming two years[8]. The results of the 2024 survey are presented in Figure 20 alongside earlier results. We note that the experts were asked to comment on overall funding, including venture-capital funding, funding within large corporations, and public support (Kung and Fancy 2021).

> *It is important that the cooling of some overhype does not tear down the high-quality research that is going on.*
>
> FRANK WILHELM-MAUCH
> Forschungszentrum Jülich

While the reported expectation that funding will *substantially* increase is going down year after year, this year there is a significantly stronger belief than in the last two years that funding will increase to some extent. A comment by Joe Fitzsimons suggests that this might be related to recent progress:

> *I believe that the recent demonstration of multi-round quantum error correction beyond break-even will be seen as a significant milestone and is likely to lead to increased investment in the field.*

> *Major state actors correctly view quantum computers' primary use cases as belonging to the sphere of defense and cybersecurity. As such, I foresee government investment increasing.*
>
> NICOLAS MENICUCCI
> RMIT University

The results of our surveys for the past years have been roughly in line with the investment figures analyzed by McKinsey & Company, like venture capital investment in quantum start-ups (McKinsey & Company 2024). Such a metric had seen a very rapid growth in 2020 and 2021, increased only by about 1% in 2022, and dropped substantially from peak in 2023. The McKinsey & Company report suggests that several factors are at play to induce such a decrease, including a shift to investments into generative AI and quantum technologies being assessed as a long-term play. As indicated by opinions expressed by the experts in our previous reports, economic and financial uncertainty in the wake of the pandemic, also in terms of high interest rates, may have contributed to the dynamics of investments. On the other hand, public funding has continued to be strong, as highlighted also in the McKinsey & Company report, as quantum technologies and quantum computing specifically are seen as strategic investments (see textbox).

[8] Despite one slight change in wording in the question from the 2020 survey to the 2021 survey, we think the direct comparison of the 2020-2024 responses is reasonable.

Alexandre Blais, a professor at the University of Sherbrooke, similarly to other respondents confirms the above view of the status and dynamics of funding:

> *The level of academic funding has not gone down over the last few years. On the other hand, it has been more challenging for startups to raise capital. This should not be taken as the sign of a 'quantum winter'. It is more simply a result of the sudden interest in [generative AI].*

Investment could further increase if early quantum computers were to be demonstrated to have practical applications. Stephanie Simmons writes:

> *Investment will increase substantially if there is a commercially useful algorithm identified that only requires a small handful of logical qubits.*

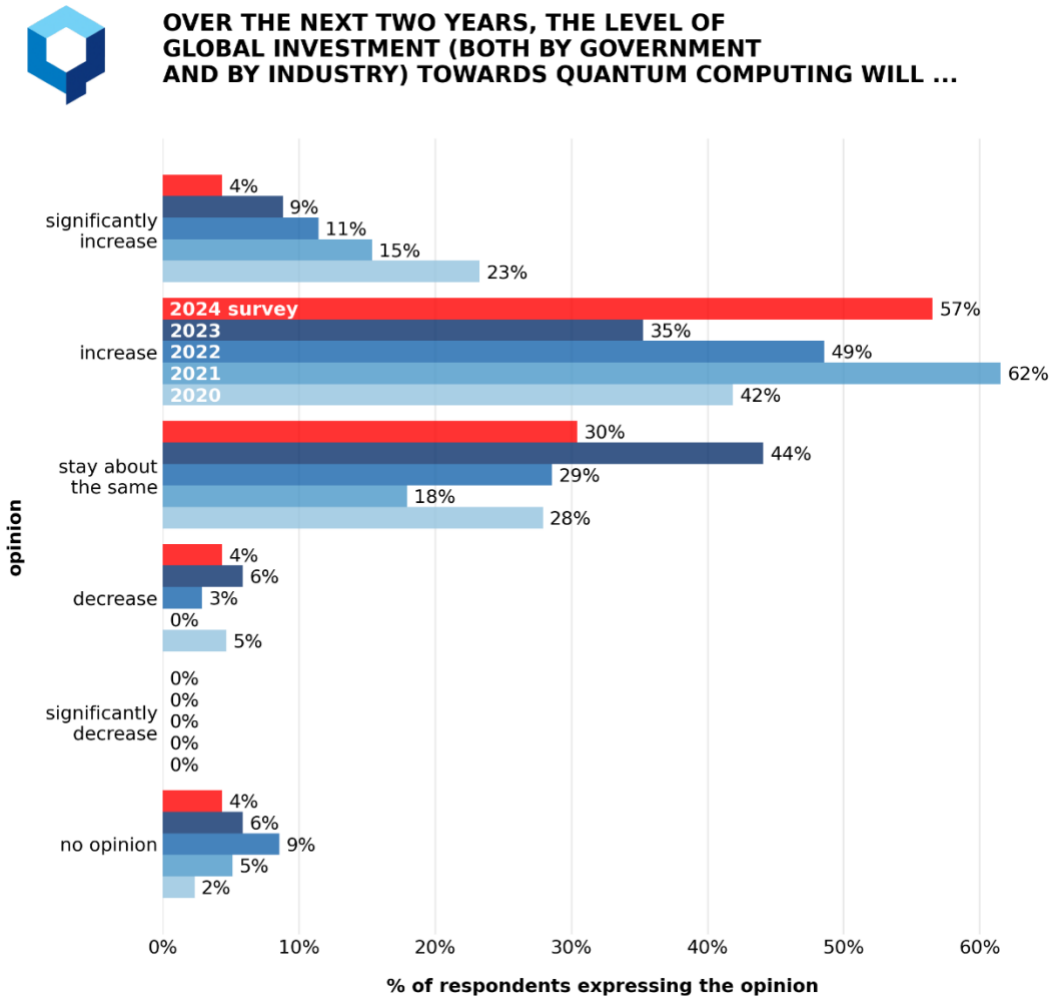


Figure 20 Expected change in the level of investment toward quantum computing in the next two years, comparing estimates by in the five surveys from 2020 to 2024.

4.7.2 Global race to build a fault-tolerant quantum computer

The pursuit of a quantum computer with cryptographic significance can be likened to a race on multiple fronts. In Section 4.1, we considered the "rivalry" among various architectures. In this section, our focus is on the contest involving both national and supranational entities, such as the European Union.

Many nations actively recognize the successful creation of a quantum computer as a strategic objective (Kung and Fancy 2021). This is because such a development would revolutionize not just cryptography and much of our digital framework — the main focus of this report — but also various societal and economic sectors. For instance, consider the potential to efficiently emulate quantum systems when developing innovative materials and drugs.

This underlying rivalry is a major driver of investments in the quantum computing sector. As a result, monitoring the developments and possible direction of this "race" provides valuable insights into the quantum threat's timeline. Additionally, for those tasked with mitigating the quantum threat, it is crucial to determine where it may emerge from. This involves identifying which entities are most likely to first develop a quantum computer capable of breaking current cryptography.

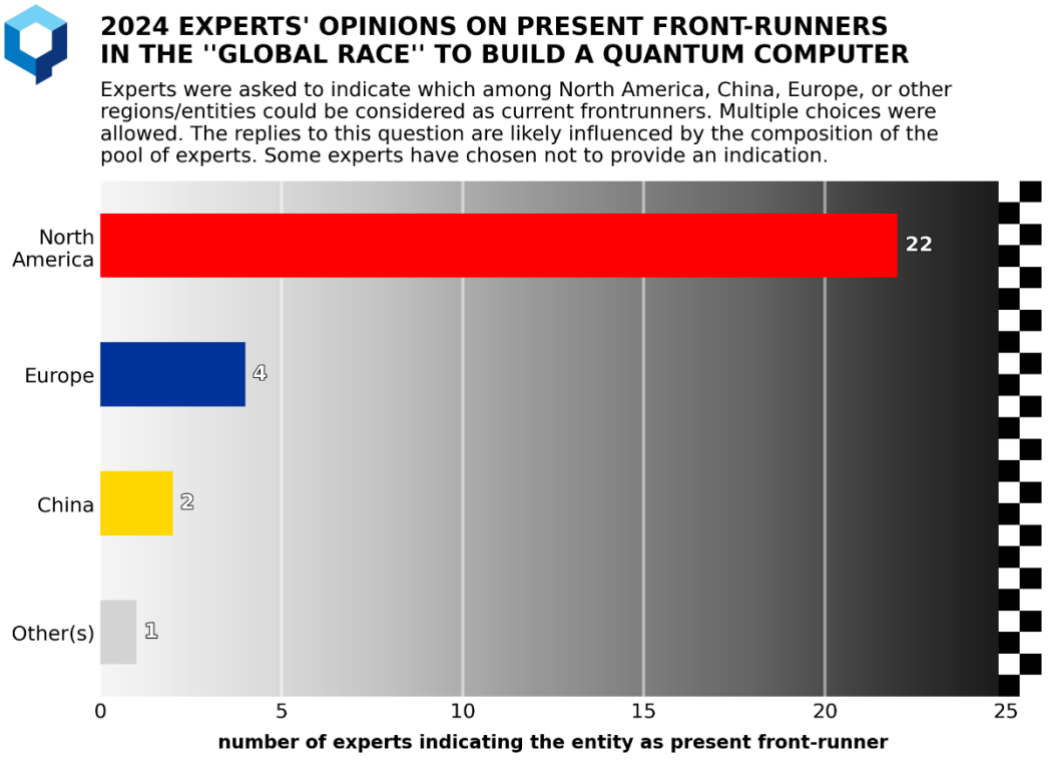


Figure 21 Number of respondents that indicated a region/entity as present front-runner in the global race to build a fault-tolerant quantum computer (multiple answers were allowed). North America appears to be in a strong position, followed by China and then Europe. The "Other(s)" answer reported here was given by a respondent who indicated uncertainty about the status of research in China.

We solicited expert opinions to identify which regions among China, Europe, and North America are currently leading, allowing for multiple responses and the inclusion of other regions[9]. The results are shown in Figure 21. Not all the experts provided an opinion, with one expert reiterating the following nuanced motivation, which highlights the importance of a qualified workforce:

> *I think that it is hard to state who is a front-runner, and therefore I have opted not to answer [..]. Recent developments have arguably been driven by [US-based companies], and one could hence argue that in this sense North America is a front-runner. This being said, the quantum work force that produces the results we are seeing is a very international one. It is all about attracting the right competence and sufficient investments over time.*

According to those who answered with specific choices, North America appears to be the present leading world region, followed by Europe and China, with the latter two ranked similarly. We note that compared to last year, North America has strengthened substantially its present leadership. While this might be in part an effect of the different composition of the pool of respondents, it is also likely dictated by the recent strong results in quantum error correction and logical encoding by U.S.-based companies and research teams.

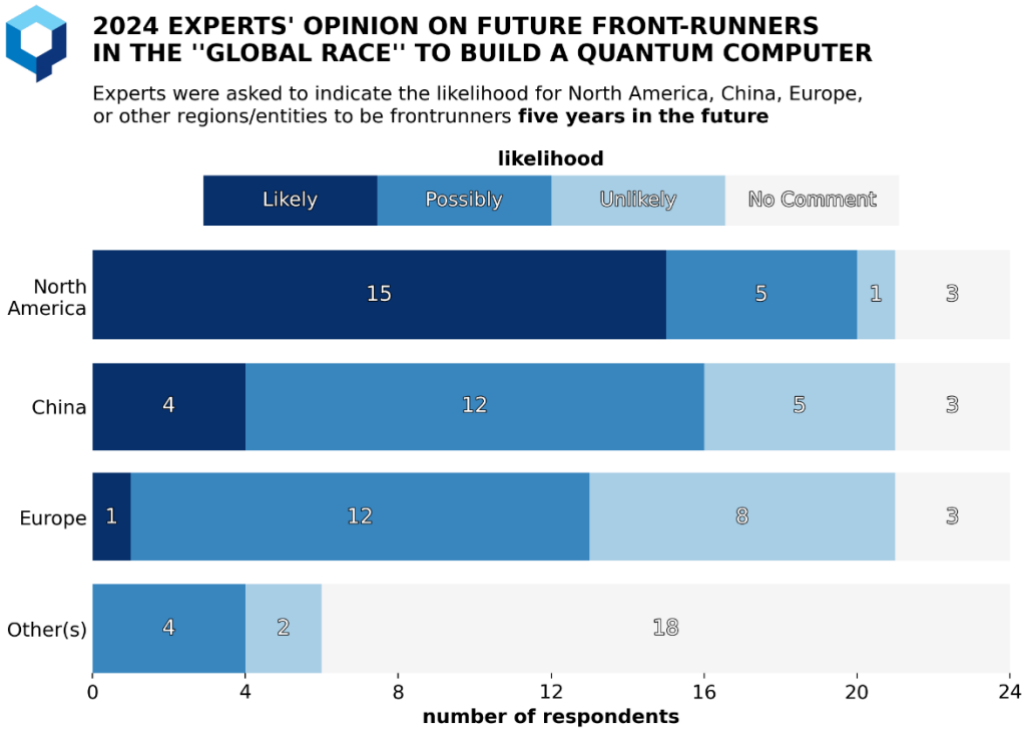


Figure 22 Number of respondents that indicated the likelihood of a given region/entity to be a front-runner in the global race to build a fault-tolerant quantum computer, five years from now. Among the "Others" mentioned: Australia and Japan.

[9] The reader may consider taking into account the geographical composition of our pool of respondents (see Section 3).

Given our interest in future trends, we also asked the experts to indicate the likelihood for each region previously considered to be a frontrunner five years from now, and whether new frontrunners may emerge. The results are presented in Figure 22. Most respondents consider it likely that North America will maintain its frontrunner position. China scores relatively highly as a likely future frontrunner and is considered to have significant potential. Europe appears to lag behind in expectations and many respondents consider it unlikely that it will have the status of frontrunner in five years. One respondent commented:

> *Europe is spreading out its effort too thinly, despite a wide presence of excellent R&D. Therefore, North America will remain the front runner. Australia is always a country to watch, with excellent and focussed basic research, and growing industrial activities.*

Klaus Mølmer points to the potential of joint efforts:

> *Joint efforts between U.S., Europe and Asia/Australia are growing in volume and political importance, and may well produce the strongest machine.*

When it comes to "Other(s)" countries, Frank Wilhelm-Mauch, a professor at Forschungszentrum Jülich, stresses that "Japan is still doing really well".

KEY POINTS

- The journey towards realizing a quantum computer is often termed the 'quantum race'.
- Competition exists both at the level of nations as well as of private companies.
- Investments in the field of quantum computing research contribute to determine the speed of development.
- The experts expect that investments in the field may continue to grow, and more than in the last two years, also driven by recent results in the field.
- We solicited expert opinions to identify which regions among China, Europe, and North America are currently leading the 'race', allowing for the inclusion of other regions. We further asked which regions are most likely to be leading five years from now.
- North America appears to be the present leading world region, followed by Europe and China, and it has consolidated its leadership in the last year.
- Most respondents consider it likely that North America will maintain its frontrunner position. China scores relatively highly as a likely future frontrunner. Europe appears to lag as future expectations go.
- Some other countries like Australia and Japan are also considered to have significant potential.

4.8 Sources of unexpected speed-up

Advancements in the quantum computing research could significantly and unexpectedly accelerate the development of a CRQC. The field encompasses various subfields, making it valuable to identify which areas hold the greatest potential for breakthroughs. Understanding this can also aid in monitoring overall progress.

To gather insights, we asked respondents to share their opinions on which aspects of quantum computing research are most likely to produce substantial and unexpected progress. As shown in Figure 23, while many areas could potentially lead to breakthroughs, experts identified hardware development as well as quantum error correction, as the most promising areas.

> *I feel there is great potential for new error-correction schemes to radically accelerate progress. Reducing the gate error rates will always be slow and difficult. Improving the error correction schemes to increase the threshold and reduce the overhead just needs one great idea.*
>
> DANIEL GOTTESMAN
> University of Maryland

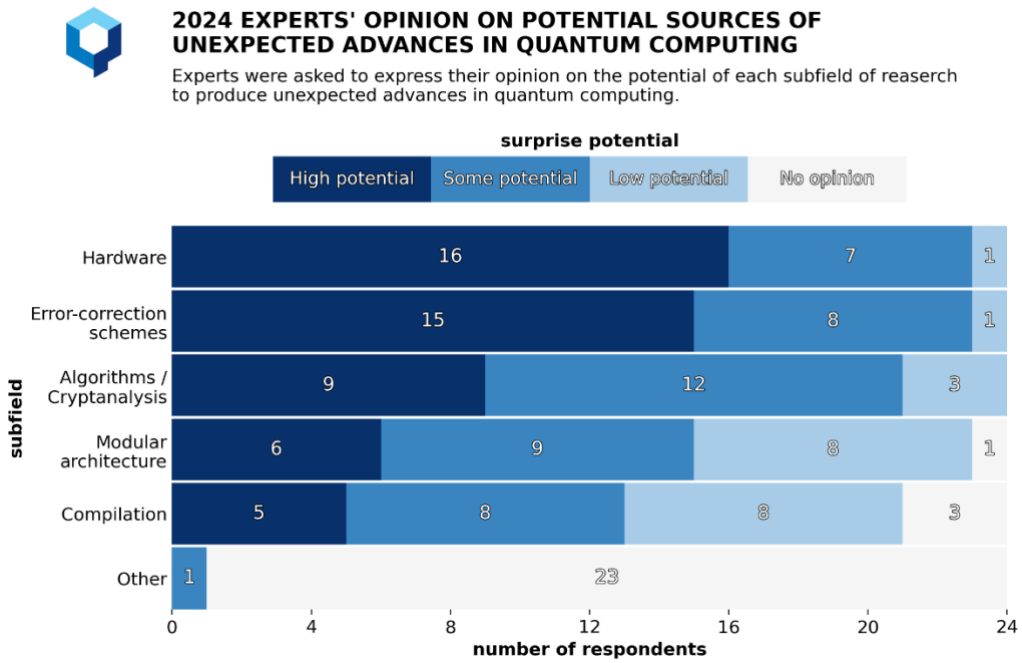


Figure 23 Number of respondents that indicated a certain "surprise potential" for several subfields of quantum computing research, which could also be seen as "layers" of a quantum stack.

KEY POINTS

- There can be significant and unexpected accelerations in quantum computing research.
- The experts identified hardware development as well as quantum error correction, as the subfields of research more likely to produce such accelerations.

4.9 Current progress

In this section we present opinions about the status of progress in quantum computing research and development.

> *After years of hope noisy intermediate-scale quantum devices would bring some tangible benefits, there is now a healthy trend towards focusing on better physical qubits, instead of more noisy qubits. This is the right direction to take.*
>
> RESPONDENT

4.9.1 Recent developments

The past year has seen significant developments, particularly with respect to the experimental realization of quantum error correction and logical qubits, in several physical realizations[10].

Such results need in general to be technically scrutinized to correctly assess the figures of merit considered and the potential limitations. Nonetheless, the consensus of the experts is that the results of the last year are impressive. Without claims of completeness, and at a high level, such results include:

- the realization of a programmable quantum processor based on reconfigurable atom arrays, encoding and operating on up to 48 logical qubits (Bluvstein et al. 2024);
- the encoding of one logical qubit using ~100 physical qubits, in a superconducting architecture, going beyond break-even and proving that logical coherence improves by utilizing more physical qubits for the encoding (Acharya et al. 2024).
- the preparation of entanglement between 12 logical qubits in a trapped-ion architecture, and logical computation on smaller set of logical qubits (Reichardt et al. 2024), expanding and improving on previous demonstrations (da Silva et al. 2024).

> *The logical qubit demonstrations of last year have shocked the quantum world and represent the sort of nonlinear progress one should expect in a disruptive technology.*
>
> STEPHANIE SIMMONS
> Photonic Inc.
> & Simon Fraser University

On the theory side – but still with implications for implementations – progress include:

- an end-to-end quantum error correction protocol that implements fault-tolerant memory based on a family of low-density parity-check codes (Bravyi et al. 2023);
- modifications of cryptanalytic algorithms potentially easing implementation requirements (Regev 2024; Ekerå and Gärtner 2024).

4.9.2 Next near-term step

We asked our respondents to identify a key step in the journey toward fault-tolerant quantum computation that they consider both essential and feasible within roughly one year.

Not surprisingly, the experts highlighted advancements similar to those already discussed in this report, such as enhancements in error rates, improved demonstrations of quantum error correction and fault tolerance, and the development of modular architectures.

[10] Given the timing of the announcements of such results and of our survey, not all the experts taking part in our survey were aware of the same set of results.

Stephanie Simmons would like to see

> *High-performance entanglement distribution links between systems that can support quantum LDPC codes.*

Tracy Northup, a professor at the University of Innsbruck, hints to the importance and potential impact on quantum computing research of advances that may not arise within the field itself:

> *[S]omething enabling (e.g., a technological advance in materials science) that by itself doesn't grab headlines but that opens up new perspectives in scaling up qubit number or achieving higher fidelities.*

KEY POINTS

- The past year has seen very significant progress, with impressive demonstrations of quantum error correction and logical encoding, in multiple types of architectures.
- Progress is expected to continue in such a direction in the near future.

4.10 Other notable remarks by participants

We asked the respondents to "comment freely on the present and near-future status of development of quantum computers". This section contains a selection of such comments as well as of comments made with respect to more specific questions in the survey.

The elephant in the room is the stubbornly small number of truly useful quantum algorithms that we know today. – RESPONDENT

Most groups building quantum computers are already thinking about modular architectures, and in many systems they are absolutely required for large-scale quantum computers. So, in that sense, modular architectures are already assumed in my estimates, and I think it is unlikely that further significant gains will occur beyond that. – DANIEL GOTTESMAN

On a 5+ year timeframe, my concern is more on the software than the hardware side. I think that within 5 years, quantum processors will have demonstrated quantum advantage. However, it is still unclear if we will know how to exploit this advantage in a useful way. – ALEXANDRE BLAIS

I find it extremely sad and destructive that this is becoming a race, and that collaboration between the strongest scientists in, e.g., China and the West is being discouraged or even prevented. The scientific and academic challenge is too important for the world to make it a destructive competition. – KLAUS MØLMER

It is good that we are now beginning to see large-scale commercial adoption of post-quantum secure asymmetric cryptography, and that final standards for such cryptography are [out]. At the same time, these developments imply that the window of opportunity for store-now-decrypt-later attacks is now slowly beginning to close: To drive continued investment into quantum computer development, we need to see concrete financially viable applications for quantum computers, besides breaking quantum-vulnerable asymmetric cryptography. Quantum computers will need to deliver solutions to practically relevant problems. – RESPONDENT

Summary and outlook

A quantum computer able to properly run quantum cryptanalysis algorithms is a threat for cryptosystems based on certain computational problems that are thought to be impossibly hard for present computational devices, but relatively easy for such a cryptographically-relevant quantum computer (CRQC).

Building a CRQC will necessitate years of advancements in both science and engineering, which can only be attained through dedicated commitment and ample resources. The key challenge to overcome is the natural 'fragility' of the quantum features that make quantum computing more powerful than classical computing.

Cyber-risk managers should track developments in the experimental realization of quantum error correction to understand how quickly cryptographically-relevant quantum computers are becoming a reality.

The effort to develop a quantum computer is frequently referred to as the "quantum race," involving competition both among nations and private companies. Recently, this race has accelerated, fueled by the entry of major corporations, significant government funding, and an influx of venture capital-backed start-ups. However, it is more fitting to view this endeavor as a marathon rather than a sprint, due to the extensive research and sustained investment needed.

That said, unexpected leaps forward are possible, owing to breakthroughs in science and/or engineering. The end goal is computations using logical qubits, a dependable way to encode and handle quantum information even when the underlying physical qubits are error-prone. The last year has seen convincing demonstrations of quantum error correction, logical encoding, and simple logical computation. Those in cybersecurity should monitor these progressions to gauge the speed at which quantum computers are materializing. In addition, one must consider the possibility of advancements in cryptanalysis algorithms, which would enable cryptanalysis with fewer quantum resources – say, fewer quantum qubits, or fewer computational steps – than the current state of the art.

Better error correction schemes, improvements in quantum cryptanalysis algorithms, and more efficient implementations of both algorithms and error correction, may well enable cryptanalysis with fewer quantum resources than seemingly required today, shortening the time to the concretization of the quantum threat.

In general, the expert opinions we have collected and summarized in this report offer unique insight into the quantum threat timeline. Thirty-two experts estimated the likelihood of the realization of a quantum computer that could break a scheme like RSA-2048 in 24 hours, and such opinions indicate a substantial likelihood within a 10-year timeframe: almost a third of the respondents (10/32) felt it was "about 50%" or more likely. The risk aversion/appetite of companies and institutions can vary significantly, but for critical systems, such estimated likelihoods represent a serious concern.

The perceived imminence of the quantum threat is dynamic and can shift based on each survey. Variables such as recent discoveries, investment fluctuations, and the economic and financial landscape can impact both the genuine threat timeline and the assessments of our experts. Our ongoing series of reports

offers a lens to track these variations, but it is essential to also consider potential variables like the change in the composition of the pool of respondents.

Current progress in error mitigation and in error correction, the increase in the number of physical qubits available on various platforms, as well as new results in the development of efficient error-correction schemes, all fuel positive expectations for the next steps in quantum computing development. The last year has seen a series of results in the experimental implementation of quantum error correction and logical encoding that our respondents generally consider impressive or even "shocking".

It is not yet clear which physical platform will be the winner, nor that there will be necessarily only one winner. In the last year, the major leap in capabilities has been demonstrated by arrays of atoms. There is also the potential of combining different technologies, both to take advantage of the specific strengths each of them may have, or to create modular systems that may facilitate scaling up the number of physical and logical qubits.

The logical possibility that consequential quantum cryptanalysis is infeasible or impossible is captured in the small but non-negligible likelihood implicitly assigned in our survey to the possibility that quantumly breaking RSA-2048 will take more than 30 years. When directly queried about what could prevent the realization of a CRQC within 30 years, the respondents generally indicate that they do not see any real roadblock. Many perceive it simply as a matter of overcoming scientific and technical hurdles, most likely also via breakthroughs that are expected to happen, as it has occurred often in the history of technology. The respondents seem generally confident that the recent streak of strong experimental results will help to maintain or even increase current levels of investment.

While it is up to each institution, company, and manager to decide what risk they are ready to accept, we think cyber-risk managers are naturally more concerned about the chance that the quantum threat materializes early — and potentially earlier than many could expect — rather than never. Progress in the last years, together with the significant momentum of the field, should trigger caution, directed to developing crypto-agility and resilience against quantum attacks.

This is particularly important for three reasons. First, one should consider that malicious agents may adopt a "Harvest Now, Decrypt Later" (HNDL) approach, storing valuable encrypted data waiting for a CRQC to become a reality. Second, much of the progress being made is no longer fully visible to the global academic community, and this trend is likely to grow in the coming years. Significant advancements will continue to emerge out of sight and remain partially concealed.

Third, not preparing now against the quantum threat sets the conditions where a hasty transition to quantum-safe tools may

> *It is important to stress — not least given the roadmaps presented by industry — the importance of migrating to post-quantum secure cryptography. In particular, this is important in applications where long-term confidentiality is sought. This is because adversaries can store ciphertexts that are intercepted now for decryption sometime in the future when large-scale fault-tolerant quantum computers become available.*
>
> RESPONDENT

suddenly become a forced choice, with all the risks associated to it, from a breakdown of services to involuntarily creating vulnerabilities even against more traditional attacks.

Those responsible for managing cyber-risk should not wait to act; solutions that can start to be implemented are available today (Canadian Forum for Digital Infrastructure Resilience 2023; World Economic Forum 2023). This will be facilitated by the US National Institute of Standards and Technology (NIST) having recently issued the first standards for post-quantum cryptographic algorithms (NIST, 2024).

The Global Risk Institute and evolutionQ Inc. have already made available a quantum risk assessment methodology for taking estimates of the threat timeline and evaluating the overall urgency of taking action (Mosca and Mullholland 2017).

References

Acharya, Rajeev, Laleh Aghababaie-Beni, Igor Aleiner, Trond I. Andersen, Markus Ansmann, Frank Arute, Kunal Arya, et al. 2024. "Quantum Error Correction below the Surface Code Threshold." arXiv. https://doi.org/10.48550/arXiv.2408.13687.

Arute, Frank, Kunal Arya, Ryan Babbush, Dave Bacon, Joseph C. Bardin, Rami Barends, Rupak Biswas, et al. 2019. "Quantum Supremacy Using a Programmable Superconducting Processor." *Nature* 574 (7779): 505–10. https://doi.org/10.1038/s41586-019-1666-5.

Bluvstein, Dolev, Simon J. Evered, Alexandra A. Geim, Sophie H. Li, Hengyun Zhou, Tom Manovitz, Sepehr Ebadi, et al. 2024. "Logical Quantum Processor Based on Reconfigurable Atom Arrays." *Nature* 626 (7997): 58–65. https://doi.org/10.1038/s41586-023-06927-3.

Bravyi, Sergey, Andrew W. Cross, Jay M. Gambetta, Dmitri Maslov, Patrick Rall, and Theodore J. Yoder. 2023. "High-Threshold and Low-Overhead Fault-Tolerant Quantum Memory." arXiv. https://doi.org/10.48550/arXiv.2308.07915.

Breuckmann, Nikolas P., and Jens Niklas Eberhardt. 2021. "Quantum Low-Density Parity-Check Codes." *PRX Quantum* 2 (4): 040101. https://doi.org/10.1103/PRXQuantum.2.040101.

Canadian Forum for Digital Infrastructure Resilience. 2023. "Canadian National Quantum-Readiness: Best Practices and Guidelines." Canadian Forum for Digital Infrastructure Resilience (CFDIR). https://ised-isde.canada.ca/site/spectrum-management-telecommunications/sites/default/files/attachments/2023/cfdir-quantum-readiness-best-practices-v03.pdf.

DiVincenzo, David P. 2000. "The Physical Implementation of Quantum Computation." *Fortschritte Der Physik* 48 (9–11): 771–83. https://doi.org/10.1002/1521-3978(200009)48:9/11<771::AID-PROP771>3.0.CO;2-E.

Ekerå, Martin, and Joel Gärtner. 2024. "A High-Level Comparison of State-of-the-Art Quantum Algorithms for Breaking Asymmetric Cryptography." arXiv. http://arxiv.org/abs/2405.14381.

Feynman, Richard P. 1982. "Simulating Physics with Computers." *International Journal of Theoretical Physics* 21 (6): 467–88. https://doi.org/10.1007/BF02650179.

Fowler, Austin G., Matteo Mariantoni, John M. Martinis, and Andrew N. Cleland. 2012. "Surface Codes: Towards Practical Large-Scale Quantum Computation." *Physical Review A* 86 (3): 032324. https://doi.org/10.1103/PhysRevA.86.032324.

FS-ISAC. 2023. "Post-Quantum Cryptography Report." 2023. https://www.fsisac.com/knowledge/pqc.

Gheorghiu, Vlad, and Michele Mosca. 2025. "Quantum Resource Estimation for Large Scale Quantum Algorithms." *Future Generation Computer Systems* 162 (January):107480. https://doi.org/10.1016/j.future.2024.107480.

Gidney, Craig, and Martin Ekerå. 2021. "How to Factor 2048 Bit RSA Integers in 8 Hours Using 20 Million Noisy Qubits." *Quantum* 5 (April):433. https://doi.org/10.22331/q-2021-04-15-433.

Kitaev, A. Yu. 2003. "Fault-Tolerant Quantum Computation by Anyons." *Annals of Physics* 303 (1): 2–30. https://doi.org/10.1016/S0003-4916(02)00018-0.

Kung, Johnny, and Muriam Fancy. 2021. "A Quantum Revolution: Report on Global Policies for Quantum Technology." CIFAR. April 7, 2021. https://cifar.ca/wp-content/uploads/2021/05/QuantumReport-EN-May2021.pdf.

McKinsey & Company. 2024. "Quantum Technology Monitor." McKinsey & Company.

Mosca, Michele. 2013. *E-Proceedings of 1st ETSI Quantum-Safe Cryptography Workshop*.

Mosca, Michele, and John Mullholland. 2017. "A Methodology for Quantum Risk Assessment." Global Risk Institute. 2017. https://globalriskinstitute.org/publications/3423-2/.

Mosca, Michele, and Marco Piani. 2019. “Quantum Threat Timeline.” Global Risk Institute. 2019. https://globalriskinstitute.org/publications/quantum-threat-timeline/.

Nielsen, Michael A., and Isaac L. Chuang. 2000. *Quantum Computation and Quantum Information*. Cambridge University Press.

NIST. 2016. “Announcing Request for Nominations for Public-Key Post-Quantum Cryptographic Algorithms.” Federal Register. December 20, 2016. https://www.federalregister.gov/documents/2016/12/20/2016-30615/announcing-request-for-nominations-for-public-key-post-quantum-cryptographic-algorithms.

———. 2024. “Announcing Issuance of Federal Information Processing Standards (FIPS) FIPS 203, Module-Lattice-Based Key-Encapsulation Mechanism Standard, FIPS 204, Module-Lattice-Based Digital Signature Standard, and FIPS 205, Stateless Hash-Based Digital Signature Standard.” Federal Register. August 14, 2024. https://www.federalregister.gov/documents/2024/08/14/2024-17956/announcing-issuance-of-federal-information-processing-standards-fips-fips-203-module-lattice-based.

Preskill, John. 2018. “Quantum Computing in the NISQ Era and Beyond.” *Quantum* 2 (August):79. https://doi.org/10.22331/q-2018-08-06-79.

Regev, Oded. 2024. “An Efficient Quantum Factoring Algorithm.” arXiv. http://arxiv.org/abs/2308.06572.

Reichardt, Ben W., David Aasen, Rui Chao, Alex Chernoguzov, Wim van Dam, John P. Gaebler, Dan Gresh, et al. 2024. “Demonstration of Quantum Computation and Error Correction with a Tesseract Code.” arXiv. http://arxiv.org/abs/2409.04628.

Rivest, R. L., A. Shamir, and L. Adleman. 1978. “A Method for Obtaining Digital Signatures and Public-Key Cryptosystems.” *Communications of the ACM* 21 (2): 120–26. https://doi.org/10.1145/359340.359342.

Sevilla, Jaime, and C. Jess Riedel. 2020. “Forecasting Timelines of Quantum Computing.” *arXiv:2009.05045 [Quant-Ph]*, September. http://arxiv.org/abs/2009.05045.

Silva, M. P. da, C. Ryan-Anderson, J. M. Bello-Rivas, A. Chernoguzov, J. M. Dreiling, C. Foltz, F. Frachon, et al. 2024. “Demonstration of Logical Qubits and Repeated Error Correction with Better-than-Physical Error Rates.” arXiv. https://doi.org/10.48550/arXiv.2404.02280.

TNO. 2023. “PQC Migration Handbook | TNO.” Tno.Nl/En. 2023. https://www.tno.nl/en/newsroom/2023/04-0/pqc-migration-handbook/.

World Economic Forum. 2023. “Quantum Readiness Toolkit: Building a Quantum-Secure Economy.” World Economic Forum. https://www.weforum.org/publications/quantum-readiness-toolkit-building-a-quantum-secure-economy/.

A. Appendix

In this Appendix, we provide detailed information about various aspects of the reports, from a list of the respondents, to background information about quantum computing, to aspects of our methodology.

A.1 List of respondents

A short description/bio that emphasizes the rationale for the inclusion of each respondent is provided after the table. Respondents who have started participating in our surveys in 2019 are listed at the beginning and highlighted in grey.

#	Name	Institution	Country
1	Dorit Aharonov	Hebrew University of Jerusalem & QEDMA Quantum Computing	ISR
2	Alexandre Blais	Institut quantique, Université de Sherbrooke	CAN
3	Ignacio Cirac	Max Planck Institute of Quantum Optics	GER
4	Bill Coish	McGill University	CAN
5	David DiVincenzo	Jülich Research Center	GER
6	Martin Ekerå	KTH Royal Institute of Technology and Swedish NCSA	SWE
7	Artur Ekert	University of Oxford	GBR/SGP
8	Daniel Gottesman	University of Maryland	USA
9	Andrea Morello	UNSW Sydney	AUS
10	Tracy Northup	University of Innsbruck	AUT
11	Stephanie Simmons	Simon Fraser University and Photonic Inc	CAN
12	Peter Shor	Massachusetts Institute of Technology	USA
13	Frank Wilhelm-Mauch	Forschungszentrum Jülich	GER
14	Shengyu Zhang	Tencent Quantum Lab	CHN
15	Sergio Boixo	Google	USA
16	Earl Campbell	Riverlane & University of Sheffield	GBR
17	Andrew Childs	University of Maryland Joint Center for Quantum Information and Computer Science	USA
18	Joe Fitzsimons	Horizon Quantum Computing	SGP
19	Jay Gambetta	IBM	USA
20	Yvonne Gao	Centre for Quantum Technologies, National University of Singapore	SGP
21	Aram Harrow	Massachusetts Institute of Technology	USA
22	Winfried Hensinger	University of Sussex Universal Quantum	GBR
23	Elham Kashefi	UK National Quantum Computing Centre & School of Informatics, University of Edinburgh & CNRS, LIP6, Sorbonne University	FRA/GBR

24	Yi-Kai Liu	US National Institute of Standards and Technology (NIST)	USA
25	Klaus Mølmer	Niels Bohr Institute, University of Copenhagen	DNK
26	William John Munro	Okinawa Institute of Science and Technology	JPN
27	Nicolas Menicucci	RMIT University	AUS
28	Kae Nemoto	Okinawa Institute of Science and Technology	JPN
29	Francesco Petruccione	Stellenbosch University	ZAF
30	Simone Severini	Amazon Web Services & University College London	GBR/USA
31	Gregor Weihs	University of Innsbruck	AUT
32	David J. Wineland	University of Oregon	USA

Dorit Aharonov
A leader in quantum algorithms and complexity, and co-inventor of the quantum fault-tolerance threshold theorem.

Alexandre Blais
A leader in understanding how to control the quantum states of mesoscopic devices and applying the theoretical tools of quantum optics to mesoscopic systems, he has provided key theoretical contributions to the development of the field of circuit quantum electrodynamics with superconducting qubits.

Sergio Boixo
He is the Chief Scientist for Quantum Computer Theory at Google's Quantum Artificial Intelligence Lab. He is known for his work on quantum neural networks, quantum metrology and was involved with the first ever demonstration of quantum supremacy.

Earl Campbell
He has nearly two decades of experience in creating fresh design concepts for fault-tolerant quantum computing architectures. He is Vice President of Quantum Science at Riverlane, where his research aims to bridge the gap between theoretical quantum computing principles and practical, scalable solutions.

Andrew Childs
Interested in the power of quantum systems to process information, he is a leader in the study and development of quantum algorithms. He is a Fellow of the Joint Center for Quantum Information and Computer Science (QuICS), and director of the NSF Quantum Leap Challenge Institute for Robust Quantum Simulation.

Ignacio Cirac
One of the pioneers of the field of quantum computing and quantum information theory. He established the theory at the basis of trapped-ion quantum computation. He devised new methods to efficiently study quantum systems with classical computers, and to use controllable quantum systems (like cold atoms) as quantum simulators.

Bill Coish
A theoretician working closely with experimentalists, he is a leading expert on solid-state quantum computing, including both spin-based and superconducting implementations.

David DiVincenzo
A pioneer in the field of quantum computing and quantum information theory. He formulated the "DiVincenzo criteria" that an effective physical implementation of quantum computing should satisfy.

Martin Ekerå
A leading cryptography researcher focusing on quantum computing algorithms for cryptanalysis, and on the development of post-quantum secure classical cryptographic schemes. He is the co-author of one of the most recent and influential estimates of the resources required by a realistic and imperfect quantum computer to break the RSA public-key encryption scheme.

Artur Ekert
A pioneer in the field of quantum information who works in quantum computation and communication. He invented entanglement-based quantum key distribution and was the founding director of the Centre for Quantum Technologies of Singapore.

Joe Fitzsimons
A leading theoretical physicist and CEO of Horizon Quantum Computing. He is renowned for his contributions to blind quantum computing. His current goal is to develop programming tools that simplify software development for quantum computers.

Jay Gambetta
He is an IBM Fellow and VP of IBM Quantum. He leads the team at IBM Thomas J Watson Research Center working to build a quantum computer.

Yvonne Gao
Leads a group to develop modular quantum devices with superconducting quantum circuits. In 2019, she was named one of the Innovators Under 35 (Asia Pacific) by MIT Tech Review for her work in developing crucial building blocks for quantum computers.

Daniel Gottesman
A pioneer of quantum error correction, and inventor of the stabilizer formalism for quantum error correction. He is a Co-Director of the Joint Center for Quantum Information and Computer Science (QuICS

Aram Harrow
He is a prominent physicist and professor at MIT, specializing in quantum computing and quantum information theory. He is known for making foundational contributions to quantum algorithms, most notably co-authoring the Harrow-Hassidim-Lloyd (HHL) algorithm, which offers an exponential speedup in solving certain linear systems of equations, with potential applications in fields like quantum machine learning and optimization.

Winfried Hensinger
He heads the Sussex Ion Quantum Technology Group and is the director of the Sussex Centre for Quantum Technologies. He is a co-founder, Chief Scientist and Chairman of Universal Quantum, a full-stack quantum computing company.

Elham Kashefi
A leading quantum cryptography researcher, renowned for her work on blind quantum computing. She is a professor at the University of Edinburgh, a CNRS researcher at the Sorbonne University, and Chief Scientist at UK's National Quantum Computing Centre.

Yi-Kai Liu
He is a leader in research on quantum computation, quantum algorithms and complexity, quantum state tomography and cryptography. He is the Co-Director of the Joint Center for Quantum Information and Computer Science, an Adjunct Associate Professor in the University of Maryland, and a staff scientist in the Applied and Computational Mathematics Division at the National Institutes of Standards and Technology (NIST)

Nicolas Menicucci
A leading researcher who contributed key results in the development of continuous-variable cluster states, and who further focuses on foundational quantum information and quantum theory, in particular in relation to relativity.

Klaus Mølmer
A pioneering physicist at the University of Aarhus, he has made outstanding and insightful contributions to theoretical quantum optics, quantum information science and quantum atom optics, including the development of novel computational methods to treat open systems in quantum mechanics and theoretical proposals for the quantum logic gates with trapped ions.

Andrea Morello
A leading experimentalist in the control of dynamics of spins in nanostructures. Prof Morello's group was the first in the world to achieve single-shot readout of an electron spin in silicon, and the coherent control of both the electron and the nuclear spin of a single donor.

William John Munro
A professor at the Okinawa Institute of Science and Technology Graduate University. Previously, he was a leader in HP's development of quantum enabled technologies and headed the NTT BRL's theoretical quantum physics research group.

Kae Nemoto
She is a professor at the National Institute of Informatics (NII) and the Graduate University for Advanced Studies. She further serves as the director of the Global Research Centre for Quantum Information Science at NII. She is a pioneering theoretical physicist recognized for her work on quantum optical implementations of quantum information processing and communication.

Tracy Northup
Leads the Quantum Interfaces Group at the University of Innsbruck. Her research uses optical cavities and trapped ions as tools to explore quantum-mechanical interactions between light and matter, with applications for quantum networks and sensors.

Francesco Petruccione
He is a professor in Quantum Computing at Stellenbosch University where he is also the interim director of the National Institute for Theoretical and Computational Sciences. He spearheaded quantum technology research in South Africa. His main is to close the gap between fundamental research, innovation and development to solve problems and ensure sustainable development.

Simone Severini
A leading researcher in quantum information and complex systems, particularly through the application of graph theory. He is currently Professor of Physics of Information at University College London, and Director of Quantum Computing at Amazon Web Services.

Stephanie Simmons
Co-leads the Silicon Quantum Technology Lab at Simon Fraser University and is an international expert on the experimental realization of spin qubits in silicon, and in interfacing them with photon qubits.

Peter Shor
The inventor of the efficient quantum algorithms for factoring and discrete logarithms that generated great interest in quantum computing, and a pioneer of quantum error correction.

Gregor Weihs
He is Professor of Photonics at the Institute for Experimental Physics at the University of Innsbruck, where he leads the Photonics group. His research in quantum optics and quantum information focuses on semiconductor nanostructures and on the foundations of quantum physics.

Frank Wilhelm-Mauch
A leading theoretician working closely with experimentalists, he focuses on modelling and controlling superconducting circuits. He is the director of the Peter Grünberg Institute for Quantum Computer Analytics.

David J. Wineland
World-leading experimental physicist awarded the Nobel-prize winner in 2012 (shared with Serge Haroche) "for ground-breaking experimental methods that enable measuring and manipulation of individual quantum systems."

Shengyu Zhang
A global expert in quantum algorithms and complexity, including recent work on quantum noise characterization. He leads the Quantum Lab at Tencent.

A.2 Realizations of quantum computers

Physical realizations

The various physical implementations of quantum computers have advantages and disadvantages in relation to factors such as (but not limited to):

- *scalability*, that is, the possibility of building and controlling larger and larger quantum devices with more and more qubits using physical/engineering resources that grow in a manageable way;
- compatibility with—and ease of implementation of—different computational models;
- typical decoherence time (that is, for how long quantum features like superpositions remain preserved and can be exploited);
- speed and precision with which gates can be applied.

The following is a very high-level classification of some physical realizations:

- **Quantum optics**, meaning that information is stored and manipulated in states of light; this includes polarization states or photon-number states, and can be implemented also on-chip by using integrated optics.
- **Superconducting systems**, meaning that information is stored and manipulated in electric circuits that exploit the properties of superconducting materials.
- **Topological systems**, meaning that information is stored and manipulated in some topological properties—that is, properties that depend on 'global' (geometric) properties insensitive to 'local' changes—of quantum systems.
- **Ion traps**, meaning that information is stored and manipulated in properties of ions (atoms with non-vanishing total electric charge) that are confined by electro-magnetic fields.
- **Quantum spin systems**, meaning that information is stored and manipulated in the internal degree of freedom called *quantum spin*; such systems may be realized in silicon, like standard microchips are, or in less conventional systems, like diamonds with point defects known as nitrogen-vacancy (or NV, in short) centers.
- **Cold atoms gases**, where neutral atoms (rather than ions) are cooled down to close to absolute zero. While ions repel each other because of their electric charge, neutral atoms do not and can be trapped and arranged in very regular arrays via the use of laser beams that generate so-called optical lattices; the atoms can then be controlled all the way down to the level of individual sites in the lattice.

Models of computation

Besides many possible physical realizations of quantum computers, there are also various *models* of quantum computation. While many models are known to be computationally equivalent (that is, roughly speaking, they allow one to solve the same class of problems with similar efficiency), each model offers different insights into the design of algorithms or may be more suitable for a particular physical realization. One such model is the *circuit* model—or *gate* model—where transformations are sequentially performed on single and multiple qubits (see Figure 24). From the perspective of analysing the quantum threat timeline, it is useful to focus on the circuit model as there is a well-articulated path to implementing impactful cryptanalytic attacks.

In the circuit model, to perform arbitrary computations it is enough to be able to realize a finite set of *universal gates* which can be combined to generate arbitrary transformations. Such a set necessarily includes at least one gate that let multiple qubits interact, typically two at a time.

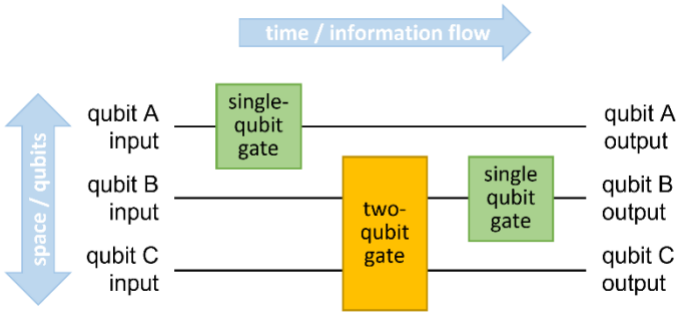


Figure 24 Illustration of the circuit/gate model for quantum computation. Each qubit corresponds to a horizontal line, so that multiple stacked lines illustrate many qubits. A qubit can be transformed individually by means of single-qubit gates, and two qubits can interact via a two-qubit gate. A given circuit transforms the initial input state of the qubits into their final output state, via the sequential action of said gates. The sequence of transformations is temporally ordered from left to right.

Historically, the following criteria, which are part of a larger set of desiderata, and which were listed by DiVincenzo in (DiVincenzo 2000) and hence are known as *DiVincenzo's criteria*, have been considered essential requirements for any physical implementation of a quantum computer:

1. *A scalable physical system with well characterized qubits.*
2. *The ability to initialize the state of the qubits to a simple fiducial state.*
3. *Long relevant decoherence times, much longer than the gate operation time.*
4. *A "universal" set of quantum gates.*
5. *A qubit-specific measurement capability.*

Unfortunately, the implementation of a single- or multi-qubit transformation can never be exactly the intended one, as the parameters defining a transformation are continuous, and because of the inevitable noise/decoherence. The quality of a gate implementation can be quantified by some notion of *fidelity*: the larger the fidelity, the closer the implementation of a gate is to the ideal one. A related parameter is the physical *error rate* with which gates are applied. In a sense, this parameter is the 'opposite' of fidelity. When characterizing the gate quality of experimental realizations or when studying the theory of how to correct them, most research groups use either the fidelity or the error rate.

Error correction, fault tolerance, and logical qubits

Errors and imperfections in the manipulation of (quantum) information, as well as decoherence, may be reduced by improving the physical implementation, including qubit control, but they cannot be entirely eliminated. Nonetheless, reliable storage and processing of quantum can still be achieved by employing *error correction* schemes: *logical* qubits are encoded into multiple *physical* qubits, so that errors affecting the underlying physical qubits can be detected and corrected, and logical information be protected. Error correction can ultimately lead to *fault tolerance* (Nielsen and Chuang 2000): under reasonable assumptions, one can prove that, if the error rate of the underlying physical components is low enough—below the so-called *fault-tolerance threshold*—then it is possible to implement logical encodings for information and information processing that can be made arbitrarily reliable, at the cost

of using a number of physical qubits that is potentially much larger than that of the encoded logical qubits, but that still scales in a manageable way, at least theoretically.

Some more details on such codes and techniques can be found below, but they are not as relevant as keeping in mind that quantum error correction and fault-tolerance do pave the way to digital quantum computers: in principle, quantum computing devices can be made as reliable as needed, once some "quality standard" and some scalability & integration of the underlying physical qubits are achieved. We provide information on some specific error-correcting codes to 1) facilitate the understanding of the expert opinions on the topic and 2) to make it clear that developing codes that enable fault tolerance, also considering their ease of realization and tailoring them to specific physical implementation, is an on-going and very important area of research. Most relevantly, improvements in error-correcting codes and/or in their hardware implementation may speed up the quantum threat timeline.

An important issue in error correction is the kind of errors that the adopted error-correction scheme/code can detect and correct.

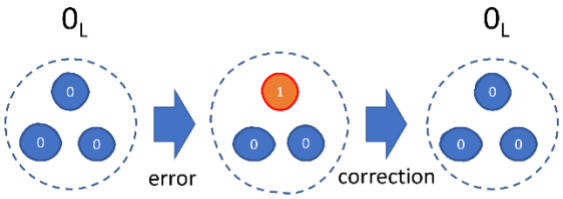


Figure 25 Example of classical information encoded logically. Several imperfect/error-prone physical bits (warped filled blue circles) are used to encode a logical 0, denoted 0_L (dashed perfectly round circle), by means of a repetition code: 0_L is encoded as 000 at the physical level. Errors can occur at the level of the physical bits, but they can be corrected, in this case by a simple majority-voting scheme, so that the logical bit is preserved. If the probability of a physical bit flipping is small enough, the probability of a logical bit being affected by an error—in this case, flipping from 0_L to 1_L—is less than the probability of a physical flip. Quantum error correction can be seen as a generalization of classical error correction to protect quantum *information; for example, a quantum code must preserve also (logical)* superpositions *of 0 and 1.*

In the case of classical bits, and excluding loss, the only possible type of error at the level of a single bit is the so-called *bit-flip*, which causes a 0 to turn into a 1, and vice versa. On the other hand, qubits can also undergo a so-called *phase-flip* error. Quantum codes can be designed and implemented that deal with just one of the two kinds of errors, but to protect quantum information both kinds need to be dealt with. Another important concept is that of *distance*, which roughly corresponds to the number of physical (qu)bits affected by an error that the error-correction scheme can handle. For example, the classical repetition code illustrated in Figure 25, using three physical bits to encode one logical bit, detects and corrects a single bit-flip error but would mishandle two bit-flips—confusing a logical 0 for a logical 1, and even introducing more physical errors upon correction. The special properties of quantum information prevent the use of simple repetition codes, but, in general, the ability to correct against more kinds of errors and against errors affecting more qubits leads to a higher number of physical qubits needed to encode a single logical qubit.

Examples of error correcting codes

Surface codes, which are an instance of so-called topological quantum error correcting codes (Kitaev 2003), are currently among the leading candidates for large-scale quantum error correction.

The surface code (Fowler et al. 2012) allows for the detection and correction of errors on a two-dimensional array of nearest-neighbour coupled physical qubits via repeatedly measuring two types of so-called stabilizers generators. A single logical qubit is encoded into a square array of physical qubits. A

classical error detection algorithm must be run at regular intervals (surface code cycle) to track the propagation of physical qubit errors and, ultimately, to prevent logical errors. Every surface code cycle involves some number of one- and two-qubit physical quantum gates, physical qubit measurements, and classical processing to detect and correct errors (i.e., decoding). Surface codes can provide logical qubits with lower overall error rates, at a price of increasing the number of physical qubits per logical qubit – that is, the size of the square array – and the cost of decoding.

Low-Density Parity Check (LDPC) codes have widespread use in the handling of classical information, as they have an essentially optimal scaling in terms of rate of encoding—the ratio between reliable logical bits and underlying faulty bits. Significant effort has recently been put into researching good *quantum LDPC codes*, which are characterized by the constraint that the number of underlying physical qubits involved in each error check and the number of checks each qubit is involved in are bounded by a constant (Breuckmann and Eberhardt 2021). One challenge with quantum LDPC codes is that the qubits used in the encoding and in the error correction, despite being "few", may be far apart.

A.3 Questions

Regarding the wording of the core questions, in general we wanted to minimize the chances that the respondents could interpret them very differently. For example, questions like "when will we have useful quantum computers?" or "is it likely that a quantum computer will break cryptography in 10 years?" would have been far too vague. Some could have assumed that a useful quantum computer could have just a few dozen physical qubits that can demonstrate some proof-of-concept speed-up over currently known classical methods. Others could have assumed that a useful quantum computer will require thousands of logical qubits (and thus perhaps millions of physical qubits) and should be performing something of immediate commercial value. Even sticking to cryptographic applications, it is important to pose questions in the right way: a quantum computer breaking RSA-2048 in 10 years may be unlikely, but is it 49%, 10%, or 1% unlikely? Some of the above considerations and goals are in—perhaps, unavoidable—tension for some of the questions.

Given the scope of our survey, and the above general principles and considerations, we proceeded as follows:

- We kept the questions largely focused on the issue of the implementation of fault-tolerant quantum computers that would be able to run quantum algorithms posing an actual threat to cryptosystems.
- We sought a range of relevant perspectives. Already in 2019, we invited a select number of respondents with authoritative and profound insights. They provided a great variety of expertise on the most recent developments and the next steps needed towards the realization of fault-tolerant quantum computers. The same philosophy guided the selection of respondents in the subsequent surveys, including this one.
- Considering the quality of the pool of respondents, all very busy professionals and researchers, we kept the questions limited in number, so that the estimated time to complete the questionnaire was less than 30 minutes. In some cases, to secure responses to at least the major key question revolving around the quantum threat timeline, we gave the option to provide input about only such a key question.

NOTE: Given the latter flexibility, not all respondents have provided answers to all questions, some of which were optional to begin with.

- Given the inherent uncertainty in the progress towards realizing a quantum computer, we asked the respondents to indicate in a relatively coarse-grained fashion how likely something was to happen.
- In addition, for the main question, we offered the option to provide point estimates for the likelihood
- We did keep several of the questions at the basis of previous reports the same or very similar, so to be able to detect a change in opinions.
- On the other hand, we modified to some extent the set of questions from survey to survey, due to:
  - recent developments in the field (such as the efforts shifting more and more towards quantum error correction and the realization of logical qubits) and in the economic, political, and social scenario;
  - the respondents' feedback from previous surveys;
  - the desire to seek opinions about other relevant aspects of the quantum threat timeline.
- For the non-free-form multiple-choice answers, we gave the possibility to leave more nuanced comments. This mitigated to some extent the issue of the experts potentially responding to the same questions under a different set of assumptions and allowed us to collect insightful opinions.

Here is a list of the main questions, grouped by questionnaire section.

Questions about "Implementations of quantum computing"

***Q**: Please indicate the potential of the following physical implementations for realizing a digital quantum computer with ~100 logical qubits in the next 10 years*[11].

Physical implementations listed: Superconducting Systems, Trapped Ions, Quantum Optics (including integrated photonics), Quantum spin systems in Silicon, Quantum spin systems not in Silicon, Topological Systems, Cold Atoms, Other

Options for answer: "Not promising", "Some potential", "Very promising", "Lead candidate", "No opinion"

Questions about "Timeframe estimates"

***Q (key 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.*

Possible classification for each period of time:

1. Extremely unlikely (< 1% chance)
2. Very unlikely (< 5% chance)
3. Unlikely (< 30 % chance)
4. Neither likely nor unlikely (about 50% chance)

[11] In the previous surveys, we had asked about "the next 15 years" but, this year, given the progress in the field, we decided to inquire about a shorter timeframe.

5. Likely (> 70 % chance)
6. Very likely (> 95% chance)
7. Extremely likely (> 99% chance)

***Q**: Various reasons for why a cryptographically-relevant quantum computer make take 30 years or longer to be built (if ever) have been articulated. Please indicate your opinion on the issues listed below, which may be among the reasons for an exceptionally long timeline.*

Concerns listed:

- Yet unappreciated fundamental trade-offs in controlling quantum features for cryptographically-relevant computational advantage (something akin to the uncertainty principle)
- Yet unappreciated standard-physics phenomena that may disrupt quantum computation (e.g., some unappreciated unavoidable source of correlated noise)
- New physics phenomena (e.g., random collapse of the wavefunction)
- Excessive technical challenges / requirements (e.g., the required scaling is practically impossible) not attributable to any of the above
- Other

Possible levels of concern:

- Concern is reasonable and has substantial likelihood (>30%)
- Concern is reasonable but somewhat unlikely (15%< likelihood <30%)
- Concern is reasonable but unlikely (5% < likelihood <15%)
- Concern is reasonable but very unlikely (likelihood <5%)
- Concern is not appropriate (likelihood <1% or the concern is unreasonable)
- No opinion

***Q**: What do you consider the most promising scheme for fault-tolerance?*

***Q**: What do you consider the most important upcoming experimental milestone to convincingly demonstrate the feasibility of building a cryptographically-relevant fault-tolerant quantum computer?*

***Q:** What is the likelihood that the milestone you have indicated will be achieved within the following timeframes?*

Timeframes: next 1 year, 3 years, 5 years, 10 years, and 15 years.
Possible classification for each period of time the same as for the key question.

***Q**: Please indicate your likelihood estimates for useful commercial applications of available processors -- or of larger/less noisy processors but anyway not yet cryptographically-relevant -- going beyond proof-or-concept and/or promotional activities, within the indicated timeframes.*

Timeframes: within 1 year, 3 years, 5 years, 10 years, and 15 years.
Possible classification for each period of time the same as for the key question.

Questions on "Non-research factors that may impact the quantum threat timeline"

***Q**: You think that, over the next two years, the level of global investment (both by government and by industry) towards quantum computing will ...*

Options: "Significantly Increase", "Increase", "Stay about the same", "Decrease", "Significantly Decrease", and "Prefer not to answer"

***Q**: Which of the following is currently the front-runner in the "global race" to build a scalable fault-tolerant quantum computer?*

Options [multiple selection was possible]: China, Europe, North America, Other(s)

***Q**: How likely are the following to be front-runners in the "global race" to build a scalable fault-tolerant quantum computer in five years?*

Each of "China", "Europe", "North America", "Other(s)" could be assigned one evaluation among "Likely", "Possibly", "Unlikely", "No Comment"

Questions on "Current progress in the development of a cryptographically-relevant quantum computer"

***Q**: What has been the most significant recent (since the second half of 2023) achievement in the progress towards building a fault-tolerant quantum digital computer?*

***Q**: What do you consider to be the next essential step towards building a fault-tolerant quantum digital computer? (something that could reasonably be achieved by approximately Summer 2025)*

***Q**: Please provide your opinion about the following aspects of quantum computing research as sources of substantial and potentially unexpected progress that may speed up the realization of cryptographically-relevant quantum computers.*

Aspects: "Quantum algorithms / quantum cryptanalysis", "Quantum hardware", "Error-correction schemes", "Modular architecture", "Compilation", "Other (please indicate below)"

Potential levels: "High", "Some", "Low", "No opinion"

***Q**: Please comment freely on the present and near-future status of development of quantum computers.*

A.4 Responses and analysis

In this section of the Appendix, we provide some details on our methodology in handling and analyzing the responses.

Quantum factoring responses and analysis

We asked the respondents to provide an informative but rough estimate of the likelihood of the availability of a quantum computer able to factorize a 2048-bit number in less than 24 hours within a certain number of years. We provide here the raw aggregate counts of the responses.

LIKELIHOOD ESTIMATE	Within 5 years	Within 10 years	Within 15 years	Within 20 years	Within 30 years
Extremely unlikely (< 1% chance)	18	4	1	0	0
Very unlikely (< 5% chance)	5	11	3	1	1
Unlikely (< 30% chance)	6	7	7	2	0
Neither likely not unlikely (~ 50% chance)	2	5	10	10	3
Likely (> 70% chance)	1	3	6	8	12
Very likely (> 95% chance)	0	2	4	7	10
Extremely likely (> 99% chance)	0	0	1	4	6

To derive from the responses the cumulative probability distributions as shown in Section 4.2, we assigned the following cumulative probabilities to each response, which are the largest and smallest ones compatible with the ranges among which the respondents could choose:

LIKELIHOOD ESTIMATE	OPTIMISTIC ASSIGNMENT	PESSIMISTIC ASSIGNMENT
Extremely likely (> 99% chance)	100%	99%
Very likely (> 95% chance)	99%	95%
Likely (> 70 % chance)	95%	70%
Neither likely nor unlikely (about 50% chance)	70%	30%
Unlikely (< 30 % chance)	30%	5%
Very unlikely (< 5% chance)	5%	1%
Extremely unlikely (< 1% chance)	1%	0%

The period option “More than 30 years, if ever” was implicit (not listed), and is trivially associated with a cumulative probability of 100%.

The resulting cumulative probabilities of the experts have simply been averaged for both the optimistic assignment and the pessimistic assignment. For those respondents who provided also point estimates, we considered mean, median, and quartiles based on the numerical answers. Based on this additional information, here we provide also a version of the average likelihood estimates where point estimates are utilized where available (Figure 26).

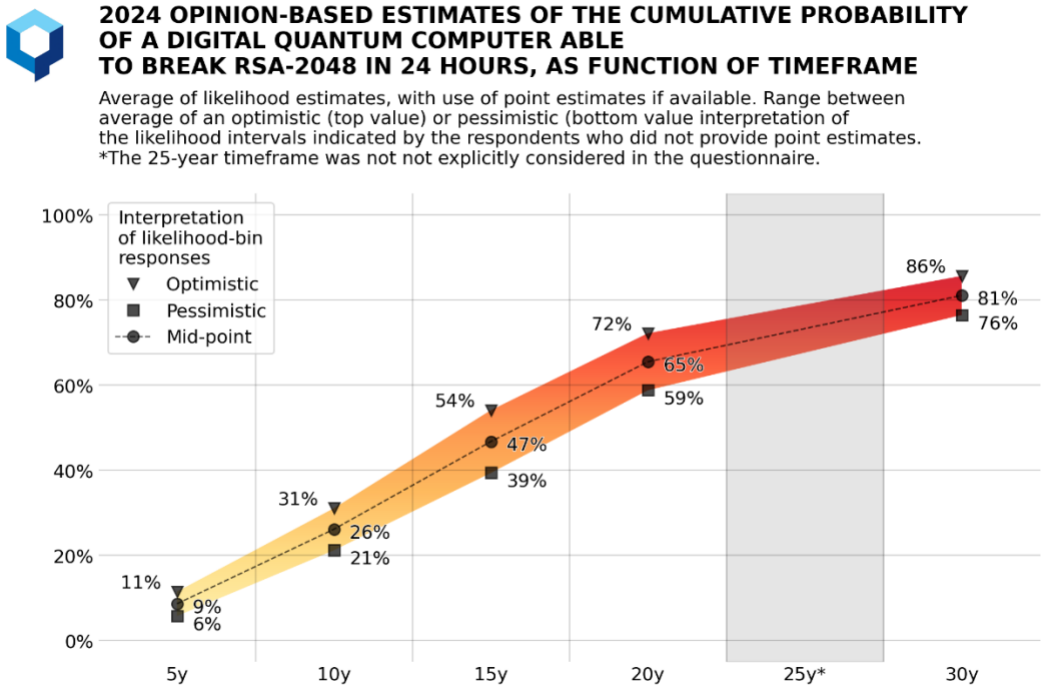


Figure 26 Average likelihood estimates, utilizing point estimates for those respondents who provided them.

General considerations on the reliability of the experts' estimates

We list here some considerations about factors that may influence the general reliability of the responses and/or lead to apparent changes in opinion trends:

- First and foremost, a general warning and an invitation to caution:
  - While the experts' likelihood estimates provide insight into the quantum threat timeline, the results of our surveys must always be interpreted cautiously.
  - The experts who take part in our surveys are uniquely qualified to estimate the quantum threat timeline, but that does not imply that any of them can correctly indicate what is going to happen and when.
  - Both in this survey and in the previous ones, several experts themselves have explicitly admitted the difficulty of making reliable forecasts.
- Considering averages does not provide necessarily the *best* possible estimates.
- When the pool of respondents changes from survey to survey, it may affect substantially the averages / the consensus.

- Statistically speaking, the number of respondents in our surveys is relatively small. Moreover, the time frame considered as well as the likelihood intervals constitute few, relatively coarse-grained bins. These factors may combine so that resulting estimates fluctuate noticeably form survey to survey, just because of few respondents answering slightly differently than they had done in the past. For example, if a respondent feels that a likelihood is around 25-35%, they might reasonably select “<30%” or “approximately 50%”, and “switch” choice from one survey to the next.
- The previous point is relevant even further when we adopt the approach of estimating likelihood ranges by interpreting optimistically or pessimistically the experts’ likelihood estimates; the reasons is that some of the likelihood ranges associated with some answers are larger than others.
- Especially from the perspective of someone working in quantum computing research and taking a survey like ours, the “time when a cryptographically relevant quantum computer will become available” is not a random value whose probability distribution is fixed. Our respondents are hard at work to make such a device become a reality, and the progress they achieve year after year is such that they are gaining a better understanding of the hurdles towards building it and of what needs to be done for circumventing them. This better understanding might increase confidence in the eventual realization of a quantum computer but might also allow them to better estimate how long it might take to overcome certain challenges. This corresponds to updating the above-mentioned distribution, for example making it more peaked some time in the future and, without contradiction, lower in the shorter term.
- Societal factors, including real or perceived issues related to the economy, may affect both the actual progress and perceptions/expectations about progress.