DOI:10.1145/3241037

Quantum systems will significantly affect the field of cyber security research.

BY PETROS WALLDEN AND ELHAM KASHEFI

Cyber Security in the Quantum Era

CYBER SECURITY DEALS with the protection of computer systems from attacks that could compromise the hardware, software or information. These attacks, by allowing unauthorized use, could leak private information and cause damage or disruption. In the future, the part of everyday life and economy requiring computer systems is bound to increase further and become fully dominant. Cyber warfare and cyber crime will be common and the role of cyber security crucial.

SINCE THE COMPUTER systems (and attackers) evolve both in hardware and software, the constant evolution of this field is of high importance. Arguably the most dramatic development that one can envision is a change in the paradigm of computational model used. Quantum technologies appear to bring us close to such a change. Here, we explore the research field that lies on the intersection of cyber security and quantum technologies research.

The dawn of the quantum technologies era. One of the major scientific revolutions of the 20th century was the development of *quantum theory*. From its early days,[33] all the way until the development of the full mathematical formalism[38] and the subsequent development of first wave of applications (for example, transistors, laser, superconductors, among others) quantum theory has been very successful in many different settings being confirmed in unprecedented accuracy (record accuracy of 10^{-8} for the anomalous magnetic dipole moment).[24] Crucial in this first wave of applications was the new understanding of nature that quantum theory provided. However, the ability to control quantum systems as desired was limited, putting restrictions on the class of technological applications that one could envision.

In recent years this has changed[16] and the control of quantum systems has advanced considerably, while further progress appears very plausible in the near future due to the increased interest and investments as well as the scientific breakthroughs that have already occurred. Many countries all around the globe have launched national

» key insights

- **Quantum computers will pose a significant threat for cyber security. When large fault-tolerant quantum computers are constructed the most commonly used cryptosystems will break. Therefore dealing with this threat is crucial and timely.**
- **Securing fully classical protocols against quantum-technology-equipped adversaries is possible but requires extra care that goes beyond a careful choice of cryptosystems.**
- **Quantum technologies will also have a positive impact on cyber security. Quantum devices with current state-of-the-art technology can be used to enhance the security by achieving tasks impossible classically, such as, secret-key expansion with perfect security. Since quantum computers will become an integral part of our future network of communications and computations, we need to develop practical ways to use the quantum computers with same security guarantees with those of secure (classical) computing.**

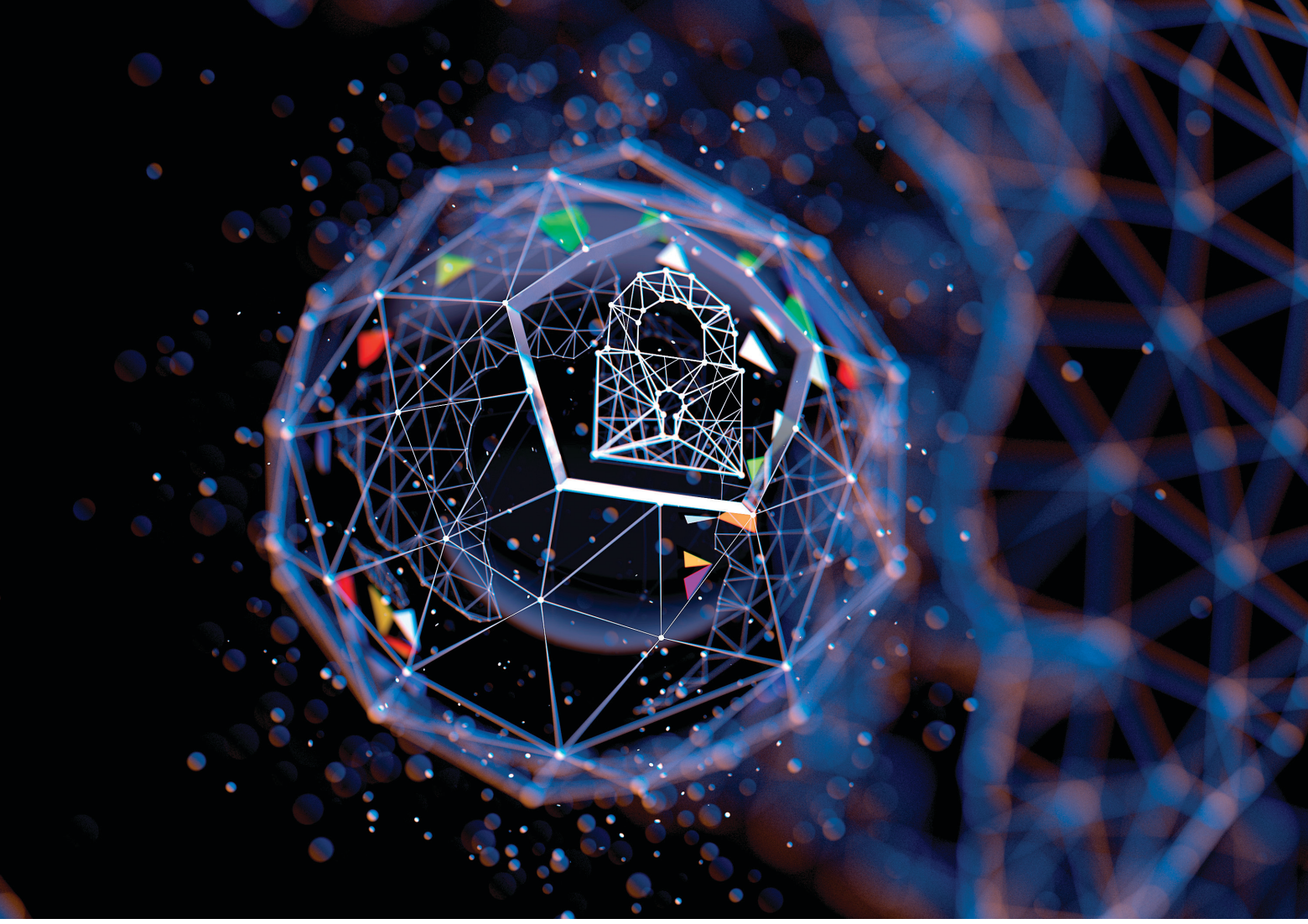


IMAGE BY PINKEYES

quantum technologies programs, varying from millions to billions, including those of Australia, Canada, China, EU, Japan, Netherlands, Russia, Singapore, U.K., U.S. At the same time, major industrial players such as Google, IBM, Microsoft, Intel, Atos, Baidu, Alibaba, Tencent along with numerous smaller and bigger quantum start-ups have initiated labs developing quantum hardware and software. This has led to what is now called "the second quantum revolution," where the ability to manipulate quantum systems as desired is leading to an era in which a variety of new technologies will appear and, in certain cases, could potentially replace existing solutions.

Arguably, the most important quantum technology will be the development of computation devices that exploit quantum phenomena, which we refer to as *quantum computers*. Quantum computers are likely to become a disruptive innovation as they can offer considerably greater computational power than their classical counterparts.

Here, we must stress that this is not something that will become relevant in the far future. Impressive quantum technological achievements are already available. To name two recent examples: Google's latest quantum processor "Bristlecone" has a record of 72 qubits with very low error rates, and is expected to be larger in size than what the best classical supercomputers can simulate.[3] Satellite quantum key distribution has been realized, enabling information theoretic secure encryption over distances of 7600km (intercontinental) and used as basis for a secure teleconference between the Austrian Academy of Sciences and the Chinese Academy of Sciences.[27]

Quantum cyber security. The development of large quantum computers, along with the extra computational power it will bring, could have dire consequences for cyber security. For example, it is known that important problems such as factoring and the discrete log, problems whose presumed hardness ensures the security of many widely used protocols (for example, RSA, DSA, ECDSA), can be solved efficiently (and the cryptosystems broken), if a quantum computer that is sufficiently large, "fault tolerant" and universal, is developed.[35] While this theoretical result has been known since the 1990s, the actual prospect of building such a device has only recently become realistic (in medium term). However, addressing the eminent risk that adversaries equipped with quantum technologies pose is not the only issue in cyber security where quantum technologies are bound to play a role.

Quantum cyber security is the field that studies *all* aspects affecting the security and privacy of communications and computations caused by the development of quantum technologies.

Quantum technologies may have a negative effect to cyber security, when viewed as a resource for adversaries, but can also have a positive effect, when honest parties use these technologies to their advantage. The research can, broadly speaking, be divided into three categories that depend on who has access to quantum technologies and how developed these technologies

are (see Figure 1). In the first category we ensure that currently possible tasks remain secure, while in the other two categories we explore the new possibilities that quantum technologies bring.

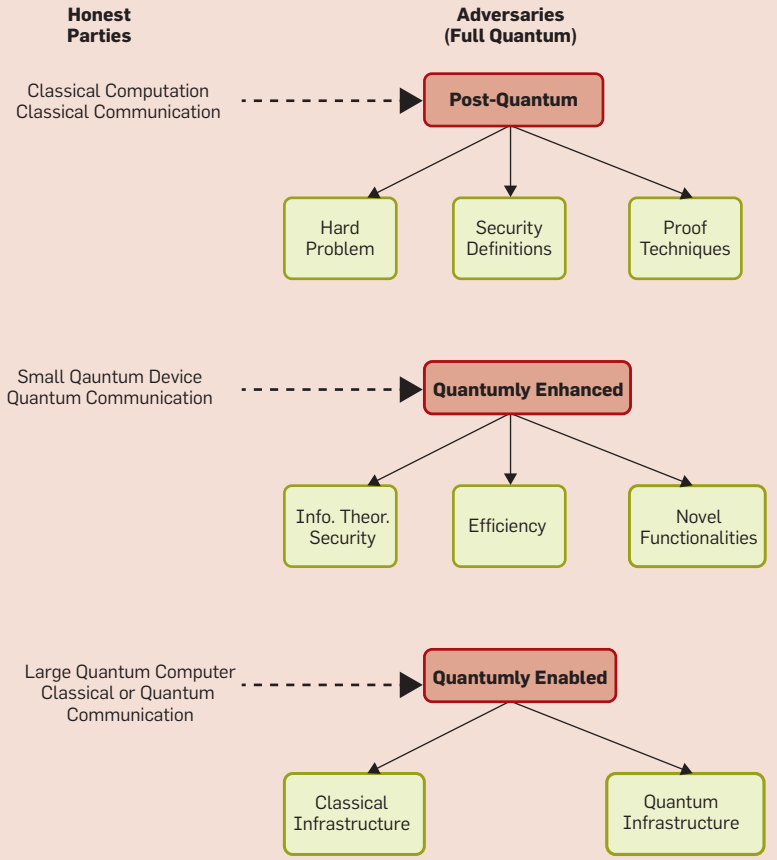
As is typical in cryptography, we first assume the worst-case scenario in terms of resources, where the honest parties are fully classical (no quantum abilities), while the adversaries have access to any quantum technology (whether this technology exists currently or not). In particular we assume they have a large quantum computer. Ensuring the security and privacy guarantees of a classical protocol remain intact is known as *post-quantum* (or "quantum-safe") security.

In the second category we allow honest parties to have access to quantum technologies in order to achieve enhanced properties, but we restrict this access to those quantum technologies that are currently available (or that can be built in near-term). Requesting this level of quantum abilities comes from the practical demand to be able to construct now, small quantum devices/gadgets that implement the "quantum" steps of (the honest) protocols. The adversaries, again, can use any quantum technology. In this category we focus on achieving classical functionalities but we are able to enhance the security or efficiency of the protocols beyond what is possible classically by using current state-of-the-art quantum gadgets.

Finally, the third category looks further in the future and examines the security and privacy of protocols that are possible (are *enabled*) by the existence of quantum computers. We assume there exist quantum computation devices that offer advantages in many useful applications compared with the best classical computers. At that time, there will be tasks that involve quantum computers and communication and processing of quantum information, where the parties involved want to maintain the privacy of their data and have guarantees on the security of the tasks achieved. This period may not be too far, since quantum devices being developed now are already crossing the limit of quantum computations that can be simulated by classical supercomputers.

Figure 1. Schematic representation of the quantum cyber security research landscape.

Red boxes are the three categories of research. Dotted lines indicate the resources (computation and communication) required from the honest parties. Green boxes represent issues on which we focus in this review. For the post-quantum category, we consider the changes required: which are the hard problems used, security definitions and proof techniques. For the quantumly enhanced category we consider the types of enhancements we may get in different protocols: information theoretic security (from computational), increased efficiency, functionalities impossible classically (even with computational assumptions). For the quantumly enabled category we consider separately the different communication infrastructures available (classical/quantum).



These categories, in general, include all aspects of cyber security. We will focus on the effects that quantum technologies have for cryptographic attacks and attacks that exploit vulnerabilities of the new quantum hardware when such hardware is used. As far as exploits of other vulnerabilities of existing classical hardware is concerned (for example, timing attacks), we do not expect they will significantly benefit from quantum technologies and thus we do not expand further.[a]

This review. First of all we clarify what this review is not. It is not an exhaustive list of all research in quantum cyber security, neither a historical exposition on how quantum cryptography developed, nor a proper introduction to the field including the background required. Excellent such reviews have been written (for example, Broadbent[13]).

Our aim in this article is twofold. On the one hand, we want to clarify misconceptions and organize/categorize the research landscape in quantum cyber security in a comprehensible and approachable way to the non-experts. On the other hand, we want to focus on specific aspects, for each of the quantum cyber security research categories given here that we believe have been underrepresented in research and exposure to the public, despite being very important. We clarify some facts about quantum computers and quantum adversaries, setting the stage to ana-

a One could imagine that enhanced quantum sensing and quantum metrology could improve certain side-channel attacks, but this is beyond the scope of this article.

lyze the three categories of quantum cyber security research. We explore post-quantum security, giving a brief overview of the field and focusing on the issue of security definitions and proof techniques. Then we sketch the research directions in quantumly enhanced security, focusing on the issue of implementation attacks and device independence. Later, we focus on classical clients securely delegating computations to the quantum cloud and conclude with a glimpse of how we envision cyber security will be reshaped in the decades to come.

Myths and Realities about Quantum Computing

In many popular accounts, quantum computers are described as some mythical computation devices that, if ever constructed, would magically solve pretty much anything one can imagine in a fraction of a second. In reality, the power of quantum computers is much more modest. Here, we clarify four of the most common misconceptions on the computational power and possibilities of quantum computers and quantum adversaries. In this way we can see the effects on cyber security research more clearly.

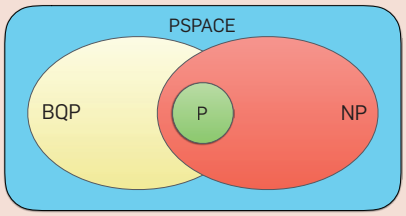
Myth 1. *Quantum computers are much faster in performing operations than classical computers.*

Reality. Quantum computers are not faster in the sense of implementing larger number of operations per second. The computational speed-up that quantum computers offer is achieved because quantum theory allows algorithms that include operations practically impossible for classical computers. Therefore, to achieve a speed-up is a task that requires the invention of new algorithms that use these operations suitably and is not straightforward. Indeed, the exact speed-up highly depends on the specific problem considered. This problem-dependency of the speed-up justifies why a quantum adversary can break only certain public-key cryptosystems, while others may remain secure with minor modifications (for example, in the key lengths).

Myth 2. *Quantum computers simultaneously perform all branches of a (probabilistic) computation and can find accepting paths instantly.*

Figure 2. Conjectured relation of complexity classes.

The conjectured relations are reinforced by the existence of oracle results that separate BQP with NP.



Reality. Quantum computers span the space of possibilities, computational branches, in a peculiar way. It is similar with classical probabilistic computers (BPP),[b] with the important difference that quantum computers behave as having "probabilities" that take complex values. This behavior, leads to "cancellations" of certain branches, since adding complex numbers is not monotonically increasing (unlike adding numbers in the interval [0, 1] as for BPP devices). This property, along with algorithms that exploit it, leads to quantum speed-ups. However, at the end of a quantum computation, the result (accepting/rejecting in a decision problem) is obtained by a single read-out/measurement and, therefore, all the "unrealized" branches do not contribute, contrary to the myth that quantum computers perform all branches in parallel in a way that someone can meaningfully extract all the information present in those branches.

Myth 3. *Quantum computers can efficiently solve NP-complete problems (such as Traveling Salesman Problem).*

Reality. The class of decision problems that quantum computers can solve efficiently is called BQP. Its (conjectured) relation to other known classes can be seen in Figure 2. In particular, we see that NP is *not* contained in BQP and, therefore, a quantum computer cannot solve a NP-complete problem efficiently. Having said that, it is important to note that quantum computers may (and do) provide polynomial or constant speed-up in many problems outside BQP (for example, quadratic search speed-up), including such speed-ups for NP-complete problems. For many tasks, even such a moderate speed-up could be of great importance. In cyber security, for example, it affects the size of keys needed to guarantee a requested level of security.

Myth 4. *Using problems that are hard for a quantum computer (outside BQP) suffices to make a cryptographic protocol secure against any quantum attack.*

Reality. This is a necessary but not sufficient condition. A quantum attacker can use quantumness in various ways, not only in order to solve some classical problems quicker. Next, we give such examples (superposition attacks) and specify that both the security definitions and the proof techniques need to be modified.

Post-Quantum Security: Quantum Adversaries

Even if one is not convinced of the necessity to drastically change the existing cryptographic protocols and infrastructure to use quantum technologies in a positive way, they still must address the possibility that current or future adversaries might use such technologies to their benefit. Since scalable, fault-tolerant, quantum computers that could break current cryptography require thousands of qubits, one could assume this is unlikely to happen in this decade.

However, there are three important reasons why we need to address quantum attackers now. Firstly, security can be broken retrospectively. For instance, if some agency intercepts and stores encrypted email messages sent today, and 10 years later develops a quantum computer, they can then use it to decrypt them.[1] Secondly, to develop cryptographic solutions that are post-quantum secure, to achieve high efficiency and to build confidence on the security of these solutions is an endeavor that requires years of research by multiple, independent, top research groups. Thirdly, changing the cryptographic infrastructure will also require years once we have decided to do it.

We will divide the research in post-quantum cryptography in three classes, according to the ways we allow the adversaries to use their "quantum

b It is the class of decision problems that can be solved efficiently by a probabilistic Turing machine with error bounded away from 1/2. This class captures well the problems that can be solved efficiently by modern classical computers.

abilities" (see Figure 1). The first class is where the adversaries are classical with the extra ability to also solve problems in BQP. In other words, these adversaries are like the standard classical adversaries, with extra access to an oracle/quantum-computer. This class is the best known and, in many accounts of post-quantum security, the only one discussed. In the second and third classes we give extra abilities to the adversaries, for example, we allow them to send input (queries) in quantum states (superposition of classical bits) and then use the (quantum) output, along with their quantum computer oracle, to compromise the security of protocols. The second class addresses the modeling and modification of security definitions, along with the immediate consequences. In the third class we deal with the changes required in (involved) proof techniques in this new quantum security model. For example, the internal state of an adversary during an interactive protocol is described by a general quantum state and their actions by a general quantum map.

We should note that all protocols in the post-quantum security category are, in terms of technologies used, fully classical protocols. All the honest steps are realized in classical devices. Still, understanding quantum computation (hardness of problems) and quantum technologies in general (modeling other types of attacks) is crucial to prove the *security*.

Security against an adversary with an oracle quantum computer. The first, and by far the most thoroughly researched area, is to ensure the security of protocols used is based on the hardness of problems which remain hard for quantum computers. This is clearly a priority since, once quantum computers are built, attacking cryptosystems that use problems that are not hard for quantum computers will be trivial. As explained in Myth 3 and depicted in Figure 2, it is believed that there exist NP problems outside BQP, therefore public key cryptography *is* still possible in the setting that adversaries have access to an oracle quantum computer.

There are many cryptosystems believed to be resistant to attacks of this type. They can be divided to hash-based, code-based, lattice-based, multivariate, and secret-key cryptography (see details in Bernstein[7]). Here, we will comment on three issues: confidence, usability, and efficiency.

The belief that a problem is hard, while in some cases it comes from theoretical implications that involve containments of complexity classes, is frequently based on the inability to find efficient solutions (or improve on existing solutions) despite the effort of many groups during a long period of time. This is the case for the hardness of factoring for classical computers. When we examine the hardness of problems used in cryptosystems against *quantum* computers, the confidence we have is generally even smaller. For example, with the exception of Merkle's hash-tree public signature system and McEliece's hidden-Goppa-code public-key encryption system, all other post-quantum proposals are relatively new. What is even more important is that research in quantum algorithms and quantum complexity theory is also new and proper cryptanalysis of the systems from the perspective of a quantum adversary is not yet as thorough as for the classical case.

This brings us to the issue of standardization and usability. Such initiatives are active, for example, the National Institute of Standards and Technology (NIST) had a recent call to standardize post-quantum public-key cryptosystems. In order to define the quantum-bit security of a cryptosystem, one must establish which is the fastest algorithm that attempts to break the system. This would also determine what key-length is required for a given security level. For example, the quadratic speed-up due to Grover's algorithm lead to a need for keys of double size. This, of course, would change if a better algorithm is invented, but good candidates for standardized use should be well enough researched to build confidence that (even moderate) speed-ups are not to be found continuously. In contrast, only recently a new speed-up was found for problems using multivariate quadratic equations.[18] Furthermore, after the standardization of encryption functions, one still needs software implementations that are suitable for integration into a variety of applications.

Finally, possibly the greatest challenge, is the issue of efficiency. While for certain applications (defense, financial market, among others) the highest security is desired even with the cost of worse performance, for a great range of everyday applications slowing down the services is not acceptable (people frequently prefer insecure but high-speed services). Existing post-quantum cryptosystems, when taking all aspects into account, lack efficiency (public key-size, signature size, speed of encryption and decryption algorithms, speed of key generation algorithm, and so on). Improving this, or identifying applications that can tolerate one of these aspects being less efficient, is an active field of research.

Superposition attacks: Modifying security notions. Security is frequently defined in terms of the probability that an adversary can succeed in certain hypothetical, interactive games. For example, one defines indistinguishability as a game that adversaries cannot win with probability higher than 1/2, indicating that randomly guessing the plaintext bit is the best they can do. In this game, the adversary is given extra ability to use a learning phase in which they can request ciphertexts of their chosen plaintexts. The motivation for giving these extra abilities is that one can imagine a scenario that an adversary could persuade an honest party to encrypt a message of their choice. To ensure privacy, this action should not give the adversary any advantage in trying to decrypt other, unknown to the attacker, messages. Now we want to consider adversaries that have the extra ability to make *quantum* queries (and receive quantum answers) in such a game. Mathematically, if the encryption (for example) is described by a function f_k, a "classical" query a quantum party can make is described as $|x\rangle|y\rangle \rightarrow |x\rangle|f_k(x) \oplus y\rangle$, where we note the first register maintains the information on x since quantum (unitary) operations are necessarily reversible. However, a quantum adversary could have initiated the query in superposition $\Sigma_{x,y} \Psi_{x,y} |x\rangle|y\rangle$ which by quantum linearity would lead to a superposition ciphertext $\Sigma_{x,y} \Psi_{x,y} |x\rangle|f_k(x) \oplus y\rangle$. The quantum adversary could attempt to use these superposition ciphertexts to break a cryptosystem. It is worth stressing that having a superposition is not the same

as having access to all the terms of the superposition, in the same way that in Myth 2 we explained not all paths are realized. For example, if one measured directly this superposition they would receive a single ciphertext of one (randomly chosen) plaintext and the security would not be compromised. Instead, attacks involve using this output superposition of ciphertexts state in another quantum algorithm that would reveal hidden structures of the cryptosystem.

Requesting from protocols to be secure against this type of attacks leads to new security definitions for a number of functionalities (for example, quantum indistinguishability). Boneh[8] was the first paper to offer such definitions, where the quantum random oracle model was defined.[c] Since then encryption, signatures, pseudo-random functions and message authentication codes have been similarly defined.[9]

Interestingly, there have been attacks of this type to symmetric cryptosystems recently, that provide an exponential speed-up.[25] This was the first quantum attack with exponential speed-up to symmetric cryptosystems, using Simon's algorithm. It does not use Shor's or Grover's algorithm[d] that are the quantum algorithms typically used to attack cryptosystems, and demonstrates that post-quantum security is much more subtle than generally believed. It is important to require these higher notions of security and to review all candidate post-quantum cryptosystems in the light of quantum cryptanalysis as described.

We should comment on an obvious objection that one could raise, namely that our systems are classical and therefore applying (for example) the encryption algorithm "coherently" on a superposition input, seems not physically motivated.[e] We use a hypothetical example of "Frozen Smart-Card" given in Gagliardoni[21] to demonstrate that one should not ignore this type of attacks even now. Real-world encryption and authentication is frequently implemented on small electronic devices such as smart cards. A quantum attacker could implement a side-channel attack where they get hold of the smart card and attempt to freeze it to a temperature that starts behaving quantum mechanically. Then they attempt to query it in superposition. This type of side-channel attack is not very different to side-channel attacks considered on cryptographic hardware in today's labs, using thermal or electromagnetic manipulation.

In order to define the quantum-bit security of a crypto system, one must establish which is the fastest algorithm that attempts to break the system.

Proof techniques against quantum adversaries. To take the most general view, we should model the internal space of a quantum adversary as a generic quantum state and all their actions and communication (with honest parties) as generic quantum operations. Modeling the adversary quantumly has two effects. On the one hand it gives the adversary more ways to deviate/attack, as for example in the superposition attacks described previously. On the other hand, it has an effect on how to prove security since simulating their view requires simulating quantum rather than classical processes. Note that showing that a proof technique is not applicable does not mean finding an attack that breaks the corresponding cryptosystem, it only means it is no longer provably secure.

For example, to define and prove security in functionalities such as secure multiparty computation (SMPC) the concept of simulation is frequently used. In particular, an adversary should be unable to distinguish whether they are interacting with the real (honest) parties or a simulated view that has no direct access to the private information of the parties involved.[28] However, since the internal space of the adversary and the interaction with the simulator are quantum the simulated view should also be quantum. This is incompatible with existing constructions of simulators, where the steps taken are not possible for general quantum states.

The key example that we implicitly assume having classical systems when constructing the simulators is the "rewinding" step (for example, see Lindell[28] for a detailed explanation of the simula-

c The (classical) random oracle is an oracle that to each call it responds with a random response. It is used, for example, as a mathematical abstraction to capture the idea of cryptographic hash functions in security proofs.

d Attacks using Grover's algorithm were performed, for example, on the original Merkle's key exchange, and only recently post-quantum secure modification was developed.

e Such attacks will be crucial in the future when the infrastructure will, by default, allow for quantum information processing, but here we argue that even before that, these attacks could be implementable.

tion proof technique and the role of rewinding). In rewinding, the simulator is given the ability to copy the internal state, and in some cases to rewind it to an earlier step. However, due to the no-cloning theorem we know that general quantum states *cannot* be copied. This problem was identified early[37] while two weaker versions of quantum rewinding, attempting to fix this issue, have been later developed. The first is the oblivious quantum rewinding,[39] where one can rewind but is not allowed to "remember" the transcripts of the previous runs apart from whether a rewinding was necessary or not. The second is the special quantum rewinding,[36] where by demanding some extra conditions (special and strict soundness) one can retain information from two runs of the rewinding process. Using quantum-rewinding steps comes at a cost, since it can only be proven that the rewound state is close but not exactly the same as the non-rewound state. This leads to a (small) distinguishing possibility between the real and simulated views, affecting the security parameters of the protocol.

These (limited) quantum-rewinding steps can be used to achieve important primitives. In particular the oblivious rewinding was used to prove quantum security of zero-knowledge proofs, while the special quantum rewinding to prove quantum security of proofs of knowledge.

Another application of the quantum rewinding is as subroutine in certain proof techniques. In order to prove security one frequently proves the security against a very weak (essentially honest) adversary and then adds a mechanism that enforces fully malicious adversaries to behave as the weak adversary or else abort. Such techniques are the Goldreich-Micali-Wigderson (GMW) compiler and the cut-and-choose technique. Both can be used to prove the security of Yao's seminal secure two-party computation protocol against malicious adversaries, and both require rewinding. The GMW compiler uses zero-knowledge proofs and thus the quantum secure version already mentioned suffices, while the cut-and-choose technique can also be proven quantum secure using the special quantum rewinding.[26]

To recap, considering fully quantum adversaries has consequences in security definitions, proof techniques and methods used, and on the cryptanalysis of existing protocols beyond what is implied from giving an oracle access to a quantum computer.

We should model the internal space of a quantum adversary as a generic quantum state and all their actions and communication (with honest parties) as generic quantum operations.

Quantumly Enhanced Security: Quantum Gadgets for Classical Parties

Quantum technologies can also offer advantages for cyber security research. To view this positive aspect, we should consider the possibility of including quantum steps in (honest) protocols with the aim of achieving certain improvement compared to the corresponding fully classical setting. The fact that improvements are in principle possible is well established, with the best known example that of quantum key distribution (QKD).[6] In QKD, using untrusted quantum channels and classical authenticated channels one can establish a shared, secret key between two spatially separated parties, with information theoretic security. This task, essentially information theoretic secure key expansion, is impossible using only classical communications. Importantly, having a protocol with information theoretic security means the security is not based on *any* computational assumption and therefore remains secure even in the presence of an attacker with a quantum computer. Another example of quantum enhancement is the quantum fingerprints,[40] where two parties can establish if they are sharing the same bit-string using minimal communication. The best classical communication complexity is $\Omega(\sqrt{n})$, which is exponentially more than the quantum communication of $O(\log_2 n)$.

We are interested in using "quantum gadgets," usually with simple quantum devices (available with current state-of-the-art technologies), to boost classical protocols in a number of ways. The types of enhancement/advantages offered could be, for example, information theoretic security from a computationally secure classical protocol (as in QKD); "computational" security against quantum attackers from no security against quantum or classical attackers;[f]

f For example, in position verification one can achieve a quantum protocol with security against adversaries with bounded amounts of shared entanglement,[14] while no fully secure classical position verification protocol exists, against multiple colluding adversaries.

and improved efficiency, that is, achieving tasks with fewer resources (as in quantum fingerprinting).

The majority of research on quantumly enhanced security is done on QKD, however, many other protocols, functionalities, and primitives exist that admit enhancement and that require similar or slightly more involved quantum technologies. Some of these technologies include: quantum random number generators, quantum fingerprinting, quantum digital signatures, quantum coin flipping, e-voting, Byzantine agreement, quantum money, quantum private information retrieval, secure multiparty computation (SMPC), and position verification.

Since quantum technologies develop rapidly, the possibilities of practical quantum gadgets increase, as more and more quantumly enhanced protocols become realistic. For example, on top of simple quantum communication between parties, we can now have each of the parties having small quantum processors. It is therefore an exciting time for this type of research since we can now consider tailor-made constructions to enhance the performance of specific involved cryptographic protocols such as e-voting or SMPC.

Practicality. Research in this category involves quantum technologies that are currently possible. While this requirement makes such applications possible, for adaptation of quantumly enhanced solutions for wide use, one must establish the necessary infrastructure, namely a reliable and wide quantum communications network. The development of quantum internet is more than a vision for the future, since a big initiative pushing towards this direction is currently under development ("Quantum Internet Alliance").[2] In the meantime, priority should be given to applications that involve few parties and do not require a fully developed quantum network.

Quantum hacking. The use of quantum gadgets opens the possibility for new attacks, specific to the physical implementations. Standard side-channel attacks (for example, timing) may be less applicable, but there are new side-channel attacks specific to the quantum devices. The best known quantum hacking attacks are the photon number splitting and beam-splitting attacks, both exploiting the fact that the real systems used for qubits are not single photons as they are modeled theoretically.[10] The thermal blinding of detectors that leak to the adversary information on the measurement choices before the classical post-processing phase,[30] something that invalidates the security proof. The latter attacks have been realized against (previous versions) of the commercially available QKD systems of ID Quantique and MagiQ Technologies. Naturally these attacks are specific to each of the implementations of the quantumly enhanced protocols.

Countermeasures discovered to "fix" systems after side-channel attacks come at a cost (for example, better single photon sources or protocols involving decoy states or monitoring the detectors), but other side-channel attacks are likely to appear. Interestingly, quantum theory offers a theoretical method to deal with all side-channel attacks on the quantum gadgets with some extra cost in resources.

Device-independence. What enables side-channel attacks is the mismatch between the ideal modeling of the (quantum) device and the real implementation. One of the most exciting new possibilities that quantum theory offers is that using the fundamental property of quantum non-locality one can achieve quantum cryptographic tasks based only on the classical statistics/correlation of the measurement outcomes, without the need to make *any* assumption on the (quantum) devices used.[17] In particular, security is maintained even if the devices were prepared by adversaries and given as black-boxes to the honest parties. Device-independent protocols are secure against any side-channel attack on the quantum device and have been developed for many functions: QKD, QRNG, among others. These protocols come with some cost in resources, currently too high for practical use. However, based on weaker correlations, one can make protocols that are secure without trusting some, but not all, devices with considerably reduced cost compared to fully device independent protocols. For example, in measurement-device independent protocols,[11,29] security is maintained without trusting the measuring/detecting device and thus one avoids the thermal blinding detector attacks mentioned earlier. In general, there is a trade-off between the extra cost in resources and the amount of trust assumed on quantum devices.

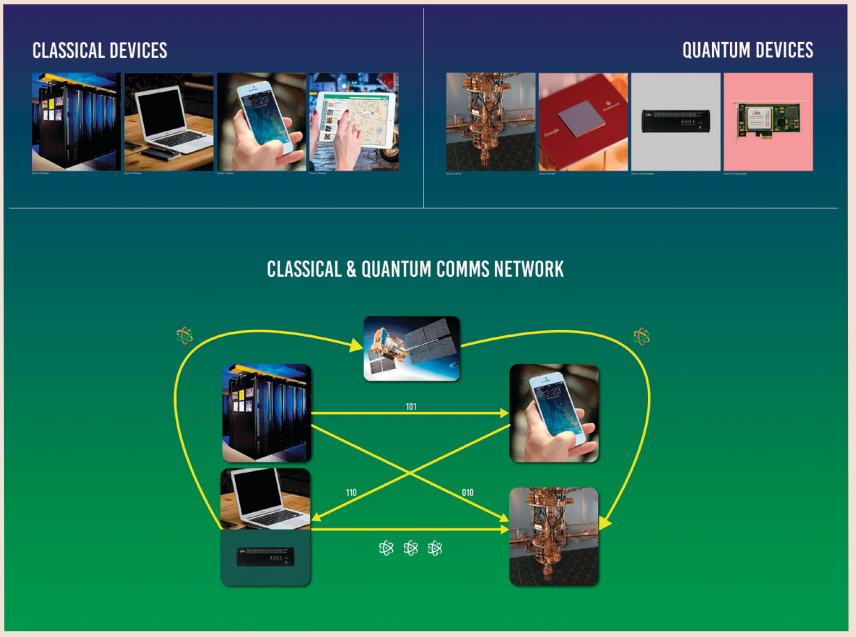
Standardization. For the adoption of quantumly enhanced solutions by industry it is important to establish standards for quantum gadgets compatible and acceptable by the general cyber security community. For QKD, discussions already exist for example within the European Telecommunications Standards Institute (ETSI), while in the case of quantum random number generators, ID Quantique, offers the Quantis product that is validated with the AIS31 methodology. It is important and timely to address the standards issues for all quantumly enhanced functionalities.

Quantumly Enabled Security: Secure Use of Quantum Computers

As we have seen, quantum computers will offer computational advantages in many problems, varying from exponential to much more modest quadratic or even constant. It is natural that when such devices are available, one might want to use this extra computational power in tasks that also require privacy and security, in other words we seek security for quantumly enabled protocols. All security concepts, such as authentication, encryption but also more involved concepts as computation on encrypted data and secure multiparty computation, would need to be modified to apply to *quantum* information and *quantum* computation. Of course, for this type of question to be meaningful, we first must have quantum computation devices of size that can offer concrete computational advantages for everyday problems. This is not the case today, but since we are expected to cross the classical simulation limit (real quantum computers that exceed in size those that can be simulated by classical supercomputers) soon, we are entering the era that will have realistic quantum speed-ups. The time for speed-ups being applied to important everyday problems might not be too far away.

Research in this category is developing rapidly, and already a number of protocols exist for quantum encryption, quantum authentication, quantum non-malleability, blind

Figure 3. The future communication and computation networks.



quantum computation, quantum fully homomorphic encryption, secure multiparty quantum computation, functional quantum encryption, and so on (for example, see the review of Fitzsimons[19]). There is a variety of protocols optimizing with respect to different figures of merit, for example, minimizing the quantum (or classical) communication, minimizing the overall quantum resources or the quantum resources of some specific parties, offering the highest possible level of security (information theoretic vs. post-quantum computational).

The majority of these protocols require quantum communication between parties and in most cases, quantum computation must be applied on the communicated quantum information. This raises two concerns: one theoretical and one practical. To achieve such tasks one needs quantum computation devices that are compatible with the quantum communication devices. On the one hand, the best platform for quantum communication is photonic, since it is simple to send quantum information encoded in photons in long distances. On the other hand, one of the most promising approaches for quantum computation devices, the one used by the major industrial players and that is leading the "bigger quantum computer" race, is based on superconducting qubits. The preferred types of qubits, for communication and computation, do not coincide, and moreover, currently it is not even known if they are compatible. It is unknown if superconducting quantum computers can be part of a "networked architecture," since they are currently built in a monolithic architecture and is not clear if it will ever be possible to send and receive quantum states.

The practical concern is the two quantum technological developments, namely the quantum computing devices and the large quantum network, are independent and we should be able to use "local" quantum computation devices before establishing the infrastructure required for a full quantum Internet network. For example, even if a single quantum computer is built in some central university or company lab, we may wish to use it to delegate computations before establishing a quantum network infrastructure. This is precisely the case for some of the current, small-scale, quantum computers (IBM, Rigetti); they offer their quantum computer in a cloud service to the public using a classical interface. Therefore, we turn to a question of both practical and theoretical interest: Can we provide quantum computation protocols that *maintain privacy and security guarantees* using this classical interface, that is, to clients with no-quantum abilities, and what would be the cost of it? This is a question that very recently has attracted attention and following the first key research we analyze here, we expect that it will become very important.

Here, we refer to "blind quantum computation" as all the protocols where a client with no quantum-computing device delegates a computation to a server with a quantum computer maintaining the privacy of her input/output. There is strong evidence from quantum complexity theory ruling out information theoretic secure, classical-client, blind quantum computation protocols.[4] To achieve a fully classical client, one should weaken some of the assumptions: either allow some (well defined) leakage of information or aim for post-quantum computationally secure protocols.[g]

A protocol was developed in Mahadev[31] where a fully classical client delegates a (generic) quantum computation, without leaking information on the input and output. This protocol was post-quantum computationally secure. The key element in the construction was a mechanism to use a classical ciphertext to apply a (generic) quantum gate conditional on the corresponding plaintext, without ever decrypting and without leaking any information.

A second approach is to construct a mechanism that mimics a quantum channel by having a classical client interact with a quantum server,[15] again with the consequence that the resulting protocol is post-quantum computational secure. Depending on the specifics of the simulated quantum channel, this functionality could enable classical clients to use all the protocols given in this section.

An important consequence is that classical clients could use *verifiable* blind quantum computation protocols. Here the clients can test the correctness of the delegated blind quantum computation, a feature crucial for commercial use of the quantum cloud. Finally, providing means that a classical agent can confirm the validity of a generic quantum computation

g Classical client protocols with multiple noncommunicating quantum servers have been proposed,[23,34] based on quantum non-locality. However, the noncommunication of the quantum servers cannot be ensured indefinitely and the privacy gets compromised when those servers, eventually, communicate.

is a topic of great importance, both theoretically and practically, in its own right irrespective of whether it is used in a cryptographic setting or not.[22] Another method to achieve verification of quantum computation in the post-quantum computational security setting, which does not necessarily rely in hiding the computation, was proposed in Mahadev.[32]

In Cojocaru et al.,[15] a quantum channel is replaced by a functionality of delegated pseudo-secret random qubit generator. Communicating random (secret) qubits is the only quantum communication required in many protocols (for example, Broadbent et al.[12] and Fitzsimons et al.[20]). The key idea to achieve this functionality is to instruct the server to generate a state where some qubits are entangled, while some are unentangled. This is done in such a way that the connectivity is known to the client (that has access to trapdoor information) but is unknown to the server (that does not have access). The client uses this advantage and instructs the server to prepare an output qubit in a random state, of which the client knows its classical description while the server is totally ignorant. This exactly mimics a random single-qubit quantum channel.

The Future

The ability to communicate securely and compute efficiently is more important than ever to society. The Internet and increasingly the Internet of Things, has had a revolutionary impact on our world. Over the next 5–10 years, we will see a flux of new possibilities, as quantum technologies become part of this mainstream computing and communicating landscape. Future networks will certainly consist of both classical and quantum devices and links, some of which are expected to be dishonest, with functionalities of various sophistication, ranging from simple routers to servers executing universal quantum algorithms (see Figure 3). The realization of such a complex network of classical and quantum communication must rely on a solid novel foundation that, nevertheless, is able to foresee and handle the intricacies of real-life implementations and novel applications.

While post-quantum security paves the way for our classical Internet to remain safe in that era, quantum enhanced security aims to benefit actively from the development of quantum Internet in order to achieve unparalleled performances that are provably impossible using classical communication. Meanwhile quantum cloud services with various capabilities are becoming available. Quantum enabled security provides the platform that will ensure potential users that this new, unprecedented computational power in the quantum cloud, comes with the appropriate standards of accuracy, reliability and privacy. C

References

1. 2013. Stored Encrypted Emails; https://www.technewsworld.com/story/79117.html
2. 2017. Quantum Internet Alliance; http://quantum-internet.team/
3. 2018. Google aims for quantum supremacy; https://physicsworld.com/a/google-aims-for-quantum-supremacy/
4. Aaronson, S., Cojocaru, A., Gheorghiu, A. and Kashefi, E. On the implausibility of classical client blind quantum computing, 2017; arXiv:1704.08482.
5. Belovs, A. et al. Provably secure key establishment against quantum adversaries. In *Proceedings of the 12th Conf. Theory of Quantum Computation, Communication and Cryptography*. M.M. Wilde, ed. Schloss Dagstuhl–Leibniz-Zentrum fuer Informatik, 2018, 3:1–3:17.
6. Bennett, C.H. and Brassard, G. Quantum cryptography: Public key distribution and coin tossing. *Theor. Comput. Sci. 560*, P1 (2014), 7–11.
7. Bernstein, D.J. Introduction to post-quantum cryptography. *Postquantum Cryptography*. Springer, 2009, 1–14.
8. Boneh, D. et al. Random oracles in a quantum world. *Advances in Cryptology—ASIACRYPT 2011*. D.H Lee and X. Wang, eds. Springer.
9. Boneh, D. and Zhandry, M. Secure signatures and chosen ciphertext security in a quantum computing world. *Advances in Cryptology–CRYPTO 2013*. Springer, 361–379.
10. Brassard, G., Lütkenhaus, N., Mor, T. and Sanders, B.C. Limitations on practical quantum cryptography. *Physical Review Letters 85*, 6 (2000),
11. Braunstein, S.L. and Pirandola, S. Side-channel-free quantum key distribution. *Physical Review Letters 108*, 13 (2012), 130502.
12. Broadbent, A., Fitzsimons, J. and Kashefi, E. Universal blind quantum computation. In *Proceedings of the 50th Annual Symp. Foundations of Computer Science*. IEEE CS, 2009, 517–526.
13. Broadbent, A. and Schaffner, C. Quantum cryptography beyond quantum key distribution. *Designs, Codes and Cryptography 78*, 1 (2016), 351–382.
14. Buhrman, H. et al. Position-based quantum cryptography: Impossibility and constructions. *SIAM J. Comput. 43*, 1 (2014), 150–178.
15. Cojocaru, A., Colisson, L., Kashefi, E. and Wallden, P. On the possibility of classical client blind quantum computing, 2018; arXiv:1802.08759.
16. Dowling, J.P. and Milburn, G.J. Quantum technology: The second quantum revolution. *Philosophical Transactions of the Royal Society of London A: Mathematical, Physical and Engineering Sciences 361*, 1809 (2003), 1655–1674.
17. Ekert, A. and Renner, R. The ultimate physical limits of privacy. *Nature 507*, 7493 (2014), 443.
18. Faugere, J.C. et al. Fast Quantum Algorithm for Solving Multivariate Quadratic Equations, 2017; arXiv:1712.07211.
19. Fitzsimons, J.F. Private quantum computation: An introduction to blind quantum computing and related protocols. *NPJ Quantum Information 3*, 1 (2017), 23.
20. Fitzsimons, J.F. and Kashefi, E. Unconditionally verifiable blind quantum computation. *Physical Review A 96* (2017), 012303.
21. Gagliardoni, T., Hülsing, A. and Schaffner, C. Semantic security and indistinguishability in the quantum world. *Advances in Cryptology—CRYPTO 2016*. M. Robshaw and J. Katz, eds. Springer, 60–89.
22. Gheorghiu, A., Kapourniotis, T. and Kashefi, E. Verification of quantum computation: An overview of existing approaches. *Theory of Computing Systems* (Jul 6, 2018).
23. Gheorghiu, A., Kashefi, E. and Wallden, P. Robustness and device independence of verifiable blind quantum computing. *New J. Physics 17*, 8 (2015), 083040.
24. Hanneke, D., Fogwell, S. and Gabrielse, G. New measurement of the electron magnetic moment and the fine structure constant. *Physical Review Letters 100*, 12 (2008), 120801.
25. Kaplan, M., Leurent, G., Leverrier, A. and Naya-Plasencia, M. Breaking symmetric cryptosystems using quantum period finding. *Advances in Cryptology—CRYPTO 2016*. M. Robshaw and J. Katz, eds. Springer, 207–237.
26. Kashefi, E., Music, L. and Wallden, P. The Quantum Cut-and-Choose Technique and Quantum Two-Party Computation, 2017; arXiv:1703.03754 (2017).
27. Liao, S.K. et al. Satellite-relayed intercontinental quantum network. *Physical Review Letters 120*, 3 (2018), 030501.
28. Lindell. Y. How to simulate it—A tutorial on the simulation proof technique. *Tutorials on the Foundations of Cryptography*. Springer, 2017, 277–346.
29. Lo, H.K., Curty, M. and Qi, B. Measurement-device-independent quantum key distribution. *Physical Review Letters 108*, 13 (2012), 130503.
30. Lydersen, L. et al. Hacking commercial quantum cryptography systems by tailored bright illumination. *Nature Photonics 4*, 10 (2010), 686.
31. Mahadev, U. Classical homomorphic encryption for quantum circuits. In *Proceedings of the IEEE 59th Annual Symposium on Foundations of Computer Science* (Paris, France, 2018), 332–338.
32. Mahadev, U. Classical verification of quantum computations. In *Proceedings of the IEEE 59th Annual Symposium on Foundations of Computer Science* (Paris, France, 2018), 259–267.
33. Bohr, N. On the constitution of atoms and molecules. *The London, Edinburgh, and Dublin Philosophical Magazine* and *J. Science 26*, 151 (1913), 1–25.
34. Reichardt, B.W., Unger, F. and Vazirani, U. Classical command of quantum systems. *Nature 496*, 7446 (2013), 456.
35. Shor, P.W. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM Review 41*, 2 (1999), 303–332.
36. Unruh, D. Quantum proofs of knowledge. *Advances in Cryptology—EUROCRYPT 2012*. D. Pointcheval and T. Johansson, eds. Springer, 135–152.
37. van de Graaf, J. Towards a Formal Definition of Security for Quantum Protocols. Ph.D. Dissertation, 1998. Montreal, Canada.
38. Von Neumann, J. *Mathematical Foundations of Quantum Mechanics*. Number 2. Princeton University Press, 1955.
39. Watrous, J. Zero-knowledge against quantum attacks. *SIAM J. Comput. 39*, 1 (2009), 25–58.
40. Xu, F. et al. Experimental quantum fingerprinting with weak coherent pulses. *Nature Communications*, (2015), 8735.

Petros Wallden (petros.wallden@ed.ac.uk) is Lecturer at the University of Edinburgh, Scotland, U.K.

Elham Kashefi (ekashefi@staffmail.ed.ac.uk) is a professor at the University of Edinburgh, Scotland, U.K. and Sorbonne Université, CNRS, Laboratoire d'Informatique de Paris, France.

Watch the author discuss this work in the exclusive *Communications* video. https://cacm.acm.org/videos/cyber-security-in-the-quantum-era