"Everything We Encrypt Today Could Be Cracked" – Exploring (Post) Quantum Cryptography Misconceptions

VICTORIA KUNDE, Chair for Human-Centred Security, Ruhr University Bochum, Germany
JAN MAGNUS NOLD, Chair for Human-Centred Security, Ruhr University Bochum, Germany
JONAS HIELSCHER, Chair for Human-Centred Security, Ruhr University Bochum, Germany

Misconceptions about (post) quantum cryptography among security experts could endanger the successful and appropriate build-up of defenses against attacks through quantum computers. We suspect that accurate knowledge about those quantum topics is not widely available yet. In the first, locally limited, exploratory study, we conducted $n = 19$ interviews with security experts & students with varying experiences to explore their knowledge and attitude towards (post) quantum cryptography. Through qualitative content analysis, we identified several quantum misconceptions, with *overestimating* or *underestimating*, *confusing topics or principles*, and *lack of context or knowledge* as general categories. The participants also showed general mistrust of the institutions, which led to the buildup of quantum computers. The identified patterns can help address (post) misconceptions about quantum cryptography in security education.

CCS Concepts: • **Security and privacy** → *Usability in security and privacy*.

Additional Key Words and Phrases: Human-Centered Security

ACM Reference Format:
Victoria Kunde, Jan Magnus Nold, and Jonas Hielscher. 2024. "Everything We Encrypt Today Could Be Cracked" – Exploring (Post) Quantum Cryptography Misconceptions. In *The 2024 European Symposium on Usable Security (EuroUSEC 2024),September 30 – October 1, 2024, Karlstad, Sweden.* ACM, New York, NY, USA, 20 pages. https://doi.org/00.00/0000

1 INTRODUCTION

Quantum Computers will likely change the security of the digitized society. They can break the most important cryptography the Internet is currently relying on [9, 38]. As mitigation, algorithms that can not be broken by quantum computers – *post quantum cryptography* – are needed. On the defender side, quantum computers could enable new ways of secured communication (through so-called *quantum cryptography*). While governments and private companies invest billions into the research of ever larger quantum computers [25] and the development of algorithms that can operate them, a race to prepare systems and their encryption to withstand an attack of quantum computers is on its way. Popularly, in 2022, the National Institute of Standards and Technology (NIST) announced the winners of a six-year-long research competition to develop *Quantum-Resistant Cryptographic Algorithms* [16] and in 2023, Google announced to build one of those algorithms [11] into its Chrome browser.

Authors' Contact Information: Victoria Kunde, Chair for Human-Centred Security, Ruhr University Bochum, Bochum, Germany; Jan Magnus Nold, Chair for Human-Centred Security, Ruhr University Bochum, Bochum, Germany; Jonas Hielscher, jonas.hielscher@ruhr-uni-bochum.de, Chair for Human-Centred Security, Ruhr University Bochum, Bochum, Germany.

The research into quantum computers, their applications, and algorithms already started in the 1980s and 90's [8, 17, 58] and just as old is the idea to attack encryption algorithms with them [26, 56, 57]. The research into software engineering for quantum computers is growing [47, 69] and even a few Human-Computer Interaction (HCI) studies with quantum computers exist [5, 31, 41, 55, 68]. However, to date (post), quantum cryptography and its real-world impact have been exclusively studied through a technical lens. There is no understanding of the security knowledge and perception of humans that develop, implement, and use quantum computers and their algorithms – or more generally, those who need to consider their impact on their products and organizations: security experts, software developers, managers, and others. Understanding their knowledge and perception is crucial in translating Human-Centred Security (HCS) principles into the realm of quantum computers.

Here, we present a first exploratory approach to understanding what security experts & students know and believe about (post) quantum cryptography. We interviewed $n = 19$ security experts & students with varying degrees of knowledge and experience in this area. Since we aimed for participants with at least some understanding of the topic, we first designed an online pre-screening to assess their eligibility. Our participants might, at some point, be responsible for planning and implementing (post) quantum cryptography in their own organizations, and hence, misconceptions could lead to false security decisions. We formulated the following research questions:

Q1: What are common misconceptions about (post) quantum cryptography held by security experts & students?
Q2: How do experts & students gain their knowledge about (post) quantum cryptography?

We find that 17 out of 19 experts & students hold some misconceptions. The experts & students gained their knowledge primarily through their university education and non-scientific sources, like YouTube and online news. They also mistrust some of the most influential bodies in this realm, such as Google or the NSA.

Our contributions are the following:

(1) We are the first to show that misconceptions about (post) quantum cryptography exist among security experts & students and that such needs to be addressed before organizations and their products can become *quantum ready*.
(2) We categorize types of (post) quantum cryptography misconceptions that can be used to create appropriate teaching materials.
(3) We show possible ways to address those misconceptions in security education for students and practitioners.
(4) We publish our instrument (pre-screening questionnaire and interview guide) that can inform further (larger-scaled) studies.

In Section 2, we will explain the current state of research into quantum computers, (post) quantum cryptography and related work with security misconceptions. In Section 3, we explain our method based on interviews with students and security experts. In Section 4, we present our findings based on the coding analysis of the interview transcripts. In Section 5, we discuss our findings and implications for academia and education before we conclude our work in Section 6.

2 BACKGROUND & RELATED WORK

Quantum computers utilize properties of quantum mechanics like superposition and entanglement [54] and "can perform certain kinds of computation more efficiently than a regular computer can". Similar to how classical computers

operate on *bits*, the concept for computation and information for quantum computers is called quantum bit or *qubit*. While quantum computers already exist, their number of qubits is currently too small to perform most operations more efficiently than classical (digital) computers[1] – while Google generally proved that quantum computers can (indeed) outperform classical computers in practice, which is called *Quantum Supremacy* [4].

2.1 Quantum Security

Here we explain *quantum cryptography* and *post quantum cryptography* and will summarize both concepts under the term *quantum security* in the remainder of the paper.

Quantum Cryptography (QC). QC makes advantage of quantum properties, which could e. g., be used to create communication channels that can not be eavesdropped without detection [7, 22, 48]. QC, therefore, presents not a form of novel attack through quantum computers but relatively new possibilities for secure communication. Although it has already been demonstrated that QC is possible, "it is not widely used due to significant technological limitations"[13]. One approach to implement QC is currently being tested in China, where a QC network linking cities is under construction [46]. A common misunderstanding is that quantum cryptography would be necessary to defend against attacks by quantum computers. This is a misconception as we "can use classical to stop quantum" [44].

Post Quantum Cryptography (PQC). Quantum computers threaten some of the currently used (classical) encryption algorithms since they can perform decryption in a much faster manner [26, 51, 56, 57]. Especially asymmetric encryption algorithms – like *RSA*, which is currently used to establish secure internet communication – will not withstand fast decryption of future quantum computers [9, 38, 59]. On the other hand, some essential symmetric encryption algorithms – like *AES* which is e. g., used to encrypt hard drives –, are affected little by quantum computers [10, 14, 24]. PQC describes such algorithms (symmetric and asymmetric) that are resistant to the attacks of quantum computers. The National Institute of Standards and Technology (NIST) launched a public research competition in 2016 to develop and standardize PQC algorithms [16]. In July 2022 – after we ran our interviews – the preliminary winners of this competition were announced [11, 18] and first organizations started to implement those algorithms in their products, e. g., Google in their Chrome Browser.[2] Security experts are asked to estimate when RSA will be broken by quantum computers in an annual survey [23].

According to the theorem of Mosca [42], data that needs to be protected from decryption in the future would already need to be PQC protected today – since an adversary could collect the data in the present to decrypt it in the future. The German Federal Agency for IT Security (BSI) performed a survey among German companies to asses their *quantum readiness* [20]. They found that most were aware of threats through quantum computers but did not plan to adapt their systems. Joseph et al. [32] described that such adaption might take an unsustainable amount of effort.handle.

2.2 Security Misconceptions

Security & privacy misconceptions have been studied extensively before. Herbert et al. [27] performed a global survey with 12,000 participants in 12 countries about security misconceptions – of which they found plenty. Other studies included general security & privacy misconception on the Internet [33], the protection of online accounts [35], WiFi [34], encryption [1, 36] and secure browsing [60, 67]. Non-experts sometimes confuse different security mechanisms and

[1] In 2022, the most powerful quantum computer used 433 qubits: https://www.technologyreview.com/2023/05/25/1073606/ibm-wants-to-build-a-100000-qubit-quantum-computer/, accessed August 19, 2024

[2] Google Adds Quantum-Resistant Encryption in Chrome 116: https://thehackernews.com/2023/08/enhancing-tls-security-google-adds.html, accessed August 19, 2024

security guarantees [53]. While non-experts may underestimate the strength of encryption and overestimate strength of attackers [36] (e.g. due to "special knowledge" or perceiving encryption as "steganography" [2]), even administrators do not always trust security mechanisms, such as PKI. Security misconceptions have also been studied among security experts [40], how unaligned advice given by experts affect users [43, 50] and why outdated security knowledge is rarely removed [28].

2.3 Quantum Security Misconceptions

To the best of our knowledge, no other research has been performed about quantum security misconceptions. While researchers have at least gathered a list of common misconceptions about quantum mechanics [62] we could not identify something similar for quantum security. However, multiple news articles and blog posts have pointed out the existence of quantum misconceptions.[3] Based on those articles, we hypothesize that the following misconceptions might exist:

(1) *Underestimating or overestimating.* One of the most general misconceptions, where thoughts and assumptions do not match the facts, is to either underestimate or overestimate a matter. In the context of this work, such misconceptions might be underestimating or overestimating the abilities or the current state of quantum computers. Further, it might also be possible to underestimate or overestimate attackers or security threats.
(2) *Confusion.* Another misconception might be confusing different topics or principles. One might, for example, have difficulties differentiating between quantum physics and quantum mechanics or between quantum cryptography and post-quantum cryptography.
(3) *Relevance.* Additionally, related to underestimating or overestimating matters, another misconception might be an inaccurate assessment of the relevance of the possessed knowledge. For example, one might see no relevance and deem something unimportant, either overall or especially for oneself, even though the matter might have real implications, thus underestimating it. On the other hand, it is equally possible to overestimate the relevance of something, giving it more importance than it has.
(4) *Lack of context.* Misconceptions might also be formed due to missing information or lack of context. One might know bits and pieces, but one lacks the context to fully understand the implications of one's knowledge.
These statements mainly express the awareness one possesses of the topic at hand.
(5) *Quantum computers are not good enough yet, so I do not have to worry.* In this statement, we focus on generalizing a quantum computer's abilities and uses. It claims that quantum computers are not good enough yet, without regard to their use.
(6) *Quantum is magic - quantum computers can solve (almost) everything.* This statement underlines the complexity and difficulty of understanding quantum computers, as highlighted in the motivation by comparing it to magic, and uses this to support the assumption that quantum computers could solve nearly anything like one would do with magic.
(7) *There is no need for post-quantum cryptography at the moment.* Because, for one, quantum computers can theoretically break types of encryption such as the *RSA* cryptosystem [21] and that it is, on the other hand, possible to either listen to encrypted communication and store it, or to store encrypted data, we can envision a particular scenario. In this scenario, a malicious party stores such encrypted data until it has access to a quantum computer that can break the used encryption, which it then does. Thus, data that is not encrypted

[3]For Example: https://blog.sciencemuseum.org.uk/quantum-computing-myths/, https://www.forbes.com/sites/startswithabang/2020/06/11/10-myths-about-the-quantum-universe/?sh=4a74c2bd5dd0, or https://www.amarchenkova.com/posts/top-3-quantum-myths-and-misconceptions, accessed August 19, 2024

using post-quantum secure cryptography can be recovered through such means. If one desires to ensure the future confidentiality of encrypted data, it is necessary to acknowledge this as a possible threat.

(8) *Symmetric encryption remains secure.* Although the consequences of quantum computers for asymmetric encryption appear to be significantly more severe, compromising entire cryptosystems [21], symmetric encryption remains not completely unaffected. However, because this seems less frequently communicated, there might be the misconception that symmetric encryption is unaffected and thus remains secure.

3 METHOD

We conducted semi-structured interviews with security experts & students in Germany to unveil misconceptions about quantum security. We aimed at experts & students with at least some self-reported knowledge in this field. We developed a pre-screening survey to find such experts & students. The online interviews were carried out in the first half of 2022 – due to the ongoing COVID pandemic as online interviews. Figure 1 summarizes our methodology.

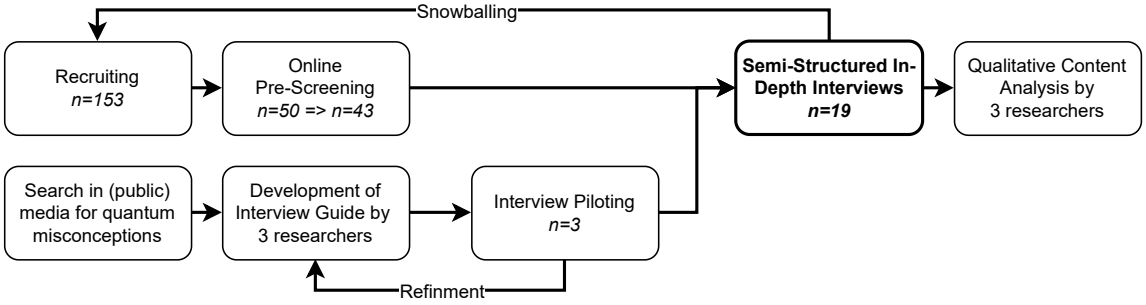

Fig. 1. Our methodology

3.1 Instrument Development

Based on our review of media coverage of quantum security, we hypothesized what misconceptions might exist (Section 2.3) and built our instruments around them.

Interview Guide. The interview guide (see Appendix B) was developed by three researchers and refined in multiple discussions over the course of three months. The interviews started with (I) a reflection on recent media reports about quantum computing, followed by questions about (II) the functionality of quantum computers, (III) their impact on security in general, (IV) QC & PQC, (V) quantum physics, (VI) a reflection on answers the participants gave in the pre-screening, and (VII) open questions about quantum security misconceptions. We piloted the interview with three security experts (one drawn from our participant pool, and two directly through personal connections). Following those pilots, we changed the interview guide to allow for more open questions around misconception topics.

Pre-Screening Questionnaire. With a pre-screening, we aimed to filter out participants without sufficient knowledge of quantum computing or quantum security. We developed an online questionnaire (see Appendix A), deployed on Qualtrics. Following a consent form and some demographic questions, we asked the participants to rate their skills on five quantum topics (e. g., QC, PQC) on a 5-point Likert scale. Based on their self-assessment, we then asked them to explain briefly what they knew about those topics. One researcher manually analyzed the answers to determine

whether the depth of knowledge was sufficient. Only participants who showed near-zero understanding of any topic were excluded.

3.2 Recruitment

Recruiting participants for the online survey was mainly done via email. Matching the topic of the questionnaire and the follow-up interview, the recruitment letter was published through one of our institution's mailing lists, which caters to an IT-security-related audience. Additionally, we recruited personal acquaintances and asked them to distribute the recruitment letter further, and we did the same with the participants. We did not inform the participants beforehand that we aimed to study quantum security misconceptions and instead stated that we would examine the experts' and students' perspectives on quantum security and quantum computing, in general, to prevent the participants from reading into the topics beforehand.

3.3 Analysis

We applied Braun & Clarkes' [12, 15] thematic analysis, following the *codebook-style*, combining deductive and inductive coding strategies and a category-based evaluation along main codes. The coding was done with MaxQDA – using Kurkatz guidance [37, 49] – and happened in multiple steps, carried out by three researchers, with only one coder directly working in the codebook, which is considered acceptable by Braun & Clarkes' [12] for *codebook-style* coding. We decided on this strategy since the coder was the only researcher in the project with sufficient knowledge of quantum security topics, with the other two being HCI experts. In the first step, (I), a deductive codebook based on the interview guide was created, followed by (II) the deductive and inductive coding of all 19 interviews. (III) After the final codebook was agreed upon, all interviews were coded again. Along with the coding, multiple memos were created to guide the coding and subsequent discussions. The coding was refined in multiple rounds of discussion with all three researchers present.

3.4 Ethics

Our institution does not have an institutional review board (IRB) nor an ethics review board (ERB) for security research. We followed best practices in human subject research [64] and considered the deanonymization of the participants as the primary threat to their safety & security. We followed strict European data privacy guidelines (GDPR) and informed the participants about the study procedure and their rights at the beginning of the questionnaire. All participants gave their explicit consent. After transcription, we deleted the audio files. We removed personal identifiers like names of individuals, organizations, or other terms that might reveal the participants' identity from the transcripts. All collected interview data was exclusively stored on servers and devices at our institution, and we used EU-based Qualtrics servers to be compliant with the GDPR. As we did not monetarily compensate the participants, we offered to share the results of our study prior to publication.

3.5 Limitations

Our work has several limitations: We present an exploratory study with 19 participants from Germany. While we can generate first insights into the topic, generalization towards other populations is impossible. This is especially true since we only recruited in the wider local network of our institution—our study is locally limited. A bias regarding received education about quantum topics could occur. Further, our sample contained 11 students who are only at the beginning of their careers and hence can only provide limited insights into quantum security from a practical point of view. We

recruited participants with at least some knowledge of quantum security, and other security experts might have even more misconceptions. We hypothesized misconceptions beforehand and were explicitly looking to confirm them. To prevent this, we continuously raised awareness in the research team during the coding process. Despite the main author of this thesis being a female quantum security expert, our recruiting strategy introduced a bias towards male participants. This only partly reflects the distribution of male/female/diverse students and faculty at our institution.

4 RESULTS

In the following, we present participants' demographics (4.1), the identified misconceptions (4.2), sources of information (4.3) and origins of misconceptions (4.4). The results are summarized in Table 1.

4.1 Pre-Screening & Demographics

153 participants filled out our pre-screening questionnaire, with only 50 (33%) answering all questions. Of those 43 passed the pre-screening and were eligible to participate in the interviews. All 43 were invited to participate in the interviews, with only 20 answering the invitation, resulting in $n = 19$ interview participants (the first was used for piloting). We asked for age, gender, field of experience, affiliation with our institution, and IT (security) background in the pre-screening. While 11 participants were enrolled students, only 3 were currently not working in the IT or IT-S industry, with 15 participants working in the industry. 13 participants were in some way affiliated with our institution (either currently or in the past). 2 participants identified themselves as female, and the remaining 17 as male.

4.2 Quantum Misconceptions

Overestimating. The majority of participants either overestimated quantum computers themselves (P2, P3, P8, P13, P14) or heard of aspects being overestimated (P1, P2, P4-P8, P13, P15, P17, P19). One overestimated aspect was the consequences of the existence of quantum computers on IT security. One participant expressed, *"that you just believe that IT security no longer works and that you might overreact. In other words, you simply develop mistrust where perhaps no mistrust would be necessary."* — [P13], or more concrete: *"I just get a bit incredulous when someone says, oh you can crack any password in one go with a technique in five years"* — [P15], whereas another said that *"In principle, the entire IT security is based on some kind of encryption algorithms, which in turn are based on the fact that, uh, theoretically I can decrypt all of them, but in practice I need too much computing time to do so. And almost every algorithm that is based on this fact, [...] then uh, but everything that is dynamic and that is practically applicable uh, that uh, if it goes badly, would be decryptable. And that would mean that there would be no more security for the time being."* — [P14].

P14 showed some overestimation by claiming that *"Cryptography is a problem because everything we encrypt here today could theoretically be cracked."* — [P14] and P3 said that *"it depends on whether they come, [...] and whether they can build a reasonably large one. And uh if they can, then it is very extreme, if not then not"* — [P3]. When it comes to the assumed overestimation by others, P5 explained that *"it's a bit of a myth, it's only half a myth, but that they [quantum computers] are incredibly strong in terms of computing capacity."* — [P5] and P4 stated that they *"can imagine that many people see it that way, that [these people] think quantum computers are completely superior to conventional computers in all aspects."* — [P4]

Underestimating. The same aspects were underestimated by other participants. Regarding the number of qubits, three participants (P7, P13, P19) either assumed the highest currently possible number of qubits to be lower than it actually is considering the existence of the 127-qubit quantum computer by IBM [6] or estimated the future development on this to

Table 1. The demographics, misconceptions and sources of quantum information of our participants. Highlighted cells are misconceptions that would be a direct threat to security if used for security decision making.

	Demographics					Misconceptions										Sources of Information							
P	Age	Gender	Working in IT/ IT-S	Enrolled Student	Duration [min]	Overestimating (self)	Overestimating (others)	Underestimating (Qubits)	Underest. (QC) useful	Underest. (QC) feasible	Lack of context	Lack of context (others)	Post QC vs. QC.	Symmetric vs. Asymmetric	Sum	Internet	YouTube	Wikipedia	Online Media	News Portals	University	Books	Paper
P1	25-29	m	✓	✓	21:48	-	✓	-	-	-	-	✓	✓	-	3	✓	✓	-	-	✓	✓	-	-
P2	25-29	m	-	✓	24:43	✓	✓	-	-	-	✓	-	-	-	3	✓	-	-	✓	-	✓	-	-
P3	20-24	m	✓	✓	17:59	✓	-	-	-	✓	✓	-	-	-	3	-	✓	-	✓	-	✓	-	-
P4	20-24	m	✓	✓	34:28	-	✓	-	-	✓	-	-	-	-	2	-	✓	-	✓	-	✓	-	-
P5	<= 19	m	-	-	27:35	-	✓	-	-	-	-	-	-	-	1	-	✓	✓	✓	-	-	-	-
P6	25-29	m	✓	-	23:30	-	✓	-	-	✓	-	-	-	-	2	-	-	-	-	✓	✓	-	-
P7	25-29	m	-	✓	48:27	-	✓	✓	-	-	-	-	-	-	2	✓	✓	✓	-	-	-	-	-
P8	20-24	f	✓	-	21:36	✓	✓	-	-	-	-	-	✓	-	3	-	-	-	-	✓	✓	-	-
P9	20-24	m	✓	-	31:40	-	-	-	-	-	-	-	-	-	0	✓	✓	✓	✓	-	✓	-	✓
P10	20-24	m	✓	✓	35:48	-	-	-	✓	✓	-	-	-	-	2	✓	-	-	✓	-	✓	-	-
P11	30-34	m	✓	-	32:29	-	-	-	-	-	-	-	-	✓	1	-	-	-	-	-	✓	✓	-
P12	55-59	m	✓	-	33:07	-	-	-	-	✓	-	-	✓	-	2	-	-	-	✓	-	✓	-	-
P13	30-34	m	✓	-	23:34	✓	✓	✓	✓	-	✓	✓	✓	-	7	-	-	-	-	✓	✓	-	-
P14	55-59	m	✓	-	22:06	✓	-	-	-	-	-	-	-	✓	2	-	-	-	✓	✓	-	-	-
P15	20-24	m	✓	✓	32:59	-	✓	-	-	-	✓	✓	-	-	3	✓	✓	-	-	-	-	✓	-
P16	20-24	m	✓	✓	24:36	-	-	-	-	-	-	-	-	-	0	-	-	-	✓	✓	✓	-	-
P17	20-24	m	✓	✓	20:48	-	✓	-	-	-	-	✓	-	-	2	-	-	-	✓	✓	✓	-	-
P18	20-24	f	-	✓	22:00	-	-	-	-	-	-	-	-	✓	1	-	-	-	-	✓	✓	-	-
P19	20-24	m	✓	✓	26:48	-	✓	✓	-	-	-	-	✓	-	3	-	-	-	-	-	✓	-	-
Sum			15	11		5	11	3	2	5	4	4	5	3	**42**	5	7	2	10	8	15	2	1

be far beneath the numbers envisioned in the current IBM roadmap. Two participants commented on the feasibility of a functioning quantum computer. One participant said that they were surprised when they heard a quantum computer had been built, as *"until then, [they] had always thought that this was such a distant theoretical idea and that it was not really physically feasible."* — [P13], whereas the other mentioned that *"there are certainly also still people, [that believe] it will never work properly"* — [P19]. Regarding the overall abilities of a quantum computer, five participants (P3, P4, P6, P10, P12) expressed their doubts about its abilities and usefulness for everyday tasks, stating that it either is not capable of them or would offer no advantages compared to using classic computers. That quantum computers are unable to fulfill these tasks does not hold, as quantum computers "*can do anything that a classical computer can do, and they can do so with at least the same computational complexity*", though there is no merit in utilizing *quantum computers for tasks at which classical computers already excel.*[4]

No need for post-quantum cryptography yet. Four participants (P1, P10, P11, P15) expressed that they saw no immediate need for post-quantum cryptography, with participant P1 stating that we could simply keep using AES encryption, overlooking the need for post-quantum secure asymmetric cryptosystems. Three of them (P10, P11, P15) emphasized

[4]Classical Computation on a Quantum Computer: https://qiskit.org/textbook/ch-gates/oracles.html, accessed August 19, 2024

that post-quantum cryptography would become necessary, but only in the future. Participants P10 and P11 further specified a time frame, both estimated post-quantum cryptography would become necessary in roughly 10 years, whereas one of them (P11) also assumed that the transition to post-quantum secure techniques would happen in time.

Lack of Context. Six participants (P1-P3, P13, P15, P17) made statements that can be attributed to either them lacking contextual information (P2, P3, P13, P15) or where they recount others lacking this (P1, P13, P15, P17). P1, for example, reported that they thought that *"the danger of quantum computers is mainly cryptography, and people don't even understand cryptography."* — [P1]. Participant P2, however, stated that after their knowledge, the AES encryption was deemed secure and that they did not see any reason why we would need new encryption schemes. This, however, disregards that AES is a symmetric encryption scheme and that asymmetric encryption schemes, which would predominantly be affected by quantum computers, are widely used in modern cryptography. Another participant (P3) assumed that utilizing dedicated algorithms to break specific asymmetric encryption, like Shor's algorithm for RSA [56, 57], might also be possible for symmetric encryption algorithms, which is incorrect. Similarly, P15 was unsure which encryption the services they utilized and to what extent they were thus affected. P13 themselves indicated that they felt they lacked an abstract understanding of what a quantum computer is capable of and what it is incapable of, and suggested that other people probably faced the same issue. Concerning others' lack of contextual knowledge, one participant (P1) described having yet to talk to someone who knows what a quantum computer is capable of and how it functions, and another (P17) emphasized that the literal quantum leap is, in contrast to the way it is used to highlight great steps, incredibly small.

Symmetric encryption remains secure. Four participants (P5, P7, P8, P16) supported the statement that symmetric encryption would stay secure even in the existence of quantum computers, with two participants (P5, P16) further elaborating that they had not heard of the opposite, admitting this might also be due to lack of information. Participant P8 additionally explained their reasoning, stating that due to the fact that symmetric cryptosystems are not, contrary to asymmetric cryptosystems, based on computational problems, they were unaffected. Although symmetric cryptosystems are, as of now, far less affected than numerous asymmetric cryptosystems and are still counted as secure, they are not completely unaffected. Using quantum computer-specific features such as Grover's algorithm, it is still possible to reduce the security level that symmetric cryptosystems provide [66]. Therefore again, symmetric encryption remains secure in no misconceptions in and of itself, the assumption that they remain completely unaffected on the other hand is.

Confusing topics or principles. There were indications that participants had uncertainties regarding the used terminology. When asked to explain the difference between quantum cryptography and post-quantum cryptography, eight participants said they did not know and had used the terms synonymously. P12 used the terms implicitly as one during the interview, and another (P19) stated that the differentiation between both terms might not be directly evident for others, even if they come from this discipline. Further, P8 defined quantum supremacy by saying that the one who holds quantum supremacy was the one possessing the quantum computer with the highest number of qubits, which is not correct, as the term quantum supremacy is used "to describe the demonstration of a quantum computer that can carry out tasks that are not possible or practical with a traditional computer" [45]. Three of the nineteen participants (P11, P14, P18) made no differentiation between symmetric and asymmetric encryption.

Further misconceptions. Three participants (P7, P9, P14) described the misconception that quantum computers always seem some years away, and years later, they still appear to be equally distant in the future. Or as phrased by participant

P9, *"the common joke is that people say that they will have quantum computers in twenty years, but they have been saying that for twenty years already"* — [P9]. Eight participants (P7, P8, P12-R16, P19) expressed the notion that capable quantum computers "destroy" or "break" something. Especially, they frequently mentioned cryptosystems, cryptography, or the encryption being broken or destroyed. The participants also heard more exaggerated statements, such as that the "internet" or "everything" gets broken because of quantum computers. Some participants expressed this more nuanced, stating that they heard that if quantum computers existed "then all these algorithms are obsolete" (P13), and that "cryptography is a problem because everything we encrypt here today could theoretically be cracked." (P14) and that they "just get a bit incredulous when someone says, oh you can crack any password in one go with a technique in five years" (P15). Seven participants (P1, P4, P5, P10, P11, P13, P19) expressed that a common misconception of quantum computers is that they can solve anything and are "superior to the classical computer in every aspect" (P4). This has to be considered more distinctly for several aspects. First take a look at the computations these computers perform, though quantum computers can simulate classical computers and are thus, in theory, able to compute anything a classical computer could, this does not make them superior in the tasks both can fulfill. Considering computations that classical computers already perform efficiently, even if a quantum computer were as efficient at this task, this would not immediately make it superior. Taking into account the costs to build and operate a quantum computer, as well as other limitations regarding the environment, the superiority of quantum computers has to be seen as much more nuanced, and it is a misconception to say that they are "superior to the classical computer in every aspect" (P4). Further, these statements seem to refer predominantly instead to the theoretical abilities of quantum computers than their current abilities which are severely lacking, without highlighting this circumstance.

4.3 Origin of Knowledge

Necessity of knowledge. All participants expressed that end users had the least need for background knowledge on quantum computers, that those who would implement or design applications for quantum computers would need substantially more know-how, and that experts and researchers required extensive and in-depth knowledge. Reflecting on quantum news spread by the media, twelve participants (P4, P5, P8-P10, P12, P14-P19) reasoned that it was also highly dependent on the consumed type of media and its target audience, which background knowledge was necessary, but that general news designed for the public required little to no previous knowledge. P1 remarked that they deemed it relevant to understand the basic features of a quantum computer, and P2 stated that it was mainly important to understand that quantum computers could solve specific problems faster and differently.

Source of knowledge. Participants listed various sources which they got their knowledge from (see Table 1). Five participants (P1, P2, P7, P10, P11) mentioned sourcing their knowledge from "the Internet" (with no further specification), seven (P1, P3-P5, P7, P9, P15) from YouTube, two from Wikipedia (P5, P7). The participants listed numerous different news sources, e. g., the most popular German online IT-Portal *heise* (P2, P4, P5, P9, P10, P12, P14, P16, P17), leading media like *ZEIT* and *SPIEGEL* (P1, P3, P8, P14, P16, P18), with only two (P1, P6) naming public news media, like *tagesschau*. Most participants (15 of 19) also stated that they had received some form of education, listing university lectures, high school subjects, seminars, and presentations, and two (P11, P15) reported reading a book on the quantum topic in question and only one (P9) that they read scientific articles. Four participants (P1, P13, P18, P19) further expressed that they acquired knowledge through conversations with others, for example, with fellow students or friends.

Credibility of and trust in information. More than the fact of where knowledge stems from, it is also key to consider how credible or trusted participants rate this source, as this "media credibility" [63] can "influence people's willingness

to change their attitudes toward different issues" [61]. Three participants (P2, P4, P7) commented on whether they trusted certain sources. Participants P2 and P4 expressed distrust of the news of Google's quantum supremacy, which was discussed at the beginning of each interview. They emphasized that Google undoubtedly pursues its economic interests and that it claims more quantum supremacy than providing distinctive proof. Similarly, participant P2 voiced the suspicion that intelligence agencies like the *NSA* might be already further along in their research and development, possibly enabling them to crack passwords. This appears to be, based on a past incident regarding supercomputers, not a completely unfounded assumption, as "intelligence agencies like the NSA hide code-breaking advances [...] because their disclosure might accelerate what has become a cryptographic arms race"[5] and information on the *NSA* decryption project Bullrun suggests.[6] P7 further stated that there were *"few articles that do not publish the latest information sensationally"* — [P7] and thus, one had to view them with some skepticism.

Lack of knowledge and consequences. Four participants (P1, P4, P7, P14) explicitly acknowledged their own and others' lack of knowledge, deeming it dangerous(P1, P7, P14) and addressed it as superficial knowledge(P4, P7, P14). Two participants (P2, P19) further stated possible consequences due to such lacking of superficial knowledge. P2 suggested that this leads to uninformed decisions, and participant P19 fears there might be currently overlooked aspects that can be exploited later on.

4.4 Origin of Misconceptions

Although the influence of media is highly dependent on what sources participants referred to and how trustworthy they are rated, participants' mindsets and behaviors also played a role in whether and how they were influenced. Furthermore, certain characteristics of news could also have influenced their audience. A statement that fits both aspects is P2's *"they [the news] will surely report about it"* — [P2], highlighting the mindset that an important topic or achievement will be reported on and simultaneously showing that the media's choice of what to report on has a direct influence on what one might learn. One major influence that six participants (P2, P5, P7, P8, P10, P19) saw was the phrasing of the news headlines created to attract an audience. Participant P19 even recounted that such a headline had caused them to have a quantum security misconception until they later took the time to read the full article in which the misconception was cleared. One participant (P12) further mentioned that news also would be artificially inflated to make them sound more relevant than they actually were, and another (P7) explained that such headlines could create fear in the audience.

Five participants (P1, P6, P7, P9, P14) elaborated on Google's influence in this. Participants P1 and P7 admitted that part of their knowledge was directly influenced by Google's algorithms. One of them (P1) reported that they used sources of information that Google provided them, whereas participant P7 chose to view the most watched YouTube videos on quantum topics they were interested in. Furthermore, two participants (P6, P14) doubted that reports on quantum topics were created based on altruistic reasons and highlighted the advertising character of Google's quantum-related news. Participant P9 further stated that Google had designed the problem to solve for their quantum computer so that it would achieve quantum supremacy rather than more general quantum supremacy. Lastly, two participants (P3, P5) discussed the influence of movies that remotely and rather briefly address quantum topics, one (P3) suggesting that nearly anything quantum-related in film might be complete nonsense, and the other with a similar stance (P5), addressing the out-of-context use of the word "quantum".

[5] https://theintercept.com/2017/05/11/nyu-accidentally-exposed-military-code-breaking-computer-project-to-entire-internet/, accessed August 19, 2024
[6] Revealed: how US and UK spy agencies defeat internet privacy and security: https://www.theguardian.com/world/2013/sep/05/nsa-gchq-encryption-codes-security, accessed August 19, 2024

Explanation. When asked why these misconceptions might exist, the main reason appeared to be that quantum-related issues were hard to imagine for participants or even counter-intuitive, as reported by twelve participants (P1, P2, P4-P6, P8, P9, P10, P13, P14, P16, P18). Another factor seemed to be the amount and character of news coverage the quantum topics received. Six participants (P1, P2, P7, P8, P10, P19) reasoned in that direction, listing a brief coverage of general news (P1), lacking thematic depth (P2, P8), misleading news articles (P7) or a significant simplification of topics (P19). Participant P10 also highlights that simply hearing of a topic does not equal understanding it, and P1 emphasized that "the danger of quantum computers lies mainly in the field of cryptography and people do not even understand cryptography".

Analogies. Lastly, we present the analogies participants gave because they provide particular insight into their awareness by comparing similarities of different things or topics. More than half, ten (P1, P2, P7-P11, P13, P16, P19) of the nineteen participants answered what would be necessary to know to use a quantum computer with an analogy. They presumed knowing how a quantum computer works was unnecessary, similar to how only a few people understand how a classical computer works (P1, P2, P7, P8, P10, P13, P16, P19). Participant P11 provided a more abstract analogy, explaining that "there are also people who drive a car without knowing how a car works". Two participants (P9, P15) additionally compared the development of quantum computers with that of classical computers, recounting the steep development of classical computers as their size became smaller and smaller and they became much more powerful, a development that was equally hard to imagine back in the past as it is in the future development of quantum computers. Participants P10 and P11 also explained the operating principle of a quantum computer using the analogy that on a path with several branches, a quantum computer could evaluate all of them in parallel instead of the sequential process of a classical computer.

5 DISCUSSION

Here, we discuss our findings concerning our research questions.

Our participants (students and more senior security experts) hold various quantum security misconceptions: those that we hypothesized (see Section 2.3, except *Quantum computers are not good enough yet, so I do not have to worry*) and others (like the confusion of principles or the belief that quantum computers do not exist to date). 15 participants held one or more misconceptions and 11 suspected such in others. Not all misconceptions have the same severity though, while e. g., the underestimation of the power of quantum computers or the confusion of their impact on symmetric versus asymmetric encryption endangers informed security decisions, the overestimation of their power does not. Here lies another danger: the spread of *security myths* [27, 40] and the creation of fear among non-tech-savvy users – in this case from quantum computers that *break encryption*. It has been shown before that the dramatization of attack techniques and the creation of fear negatively affects the ability of users to make rational security decisions [40, 52]. While some participants were aware that they might hold misconceptions, the majority suspected them in others, while holding some for themselves, which hints towards the existence of the *Dunning-Kruger effect* [39] among our participants: they have just enough quantum security knowledge to speak about this topic but can not see how limited their understanding is. University education was our participants' primary source of quantum security knowledge, followed by varying online sources and media. Our results hold little surprise despite the fact that a university education does not prevent misconceptions. Quantum Security is no *nice-to-have* knowledge for security experts. A basic understanding is as important as a basic understanding of cryptography (experts need to understand e. g., the basics about *https*, or *End-to-End encryption*). This is the case because quantum computers will fundamentally affect the encryption the internet is

currently built upon and hence organizations need to consider quantum security in many realms of security [20, 32, 42]. They cannot do their jobs if experts do not understand the fundamental threats and mitigation. Our findings are aligned with research that shows that organizations are not *quantum ready* [20].

Participants mistrusted IBM and Google to be transparent about their quantum research. Furthermore, some were even suspecting that the NSA could already be in possession of quantum computers powerful enough to break the Internet's encryption. On the other hand, no participant was aware of the ongoing NIST effort to standardize PQC algorithms in an open manner [16]. Full transparency by all stakeholders involved is key to building trust in new encryption systems standardized and deployed by US institutions – given the mistrust created in the *global surveillance disclosures* in 2013 [65]. Otherwise, the adoption of those crucial defensive techniques might be further delayed.

5.1 Implications For Research

We present an exploratory study, and our results are limited by the participant pool, which is small, tied to our institution, and consists of students in more extensive parts. However, we deem it likely that interviews with other groups of security experts would reveal similar or even more misconceptions since our participants all had at least basic knowledge in this field. Studying quantum security misconceptions among a general (non-security-savvy) population would only be purposeful if quantum security knowledge were spread to the general public. Our instrument and results can be used to create online questionnaires to study a large global sample of security experts. Such questionnaires could e. g., ask "Which encryption algorithms are threatened by quantum computers? [RSA, AES,...]" to confirm the existence of misconceptions that we identified in our study. We are currently working on creating such a questionnaire.

Studying the sources of security knowledge for software developers has shown how badly presented information directly leads to the implementation of vulnerabilities [3, 19]. Such studies should be carried out for quantum security as well. Developers would benefit from presenting quantum security information in ways that can directly be used to implement PQC securely in organizations and their products.

5.2 Implication for Quantum Security Education

Our study indicates that university education in (theoretical) quantum security does not prevent misconceptions. We suspect that new developments (like the proof of quantum supremacy [4]) do not automatically find their way into the curricula. We suggest that (I) quantum security should be taught as a practical topic in the intersection between organizational security architecture & cryptography. This helps students understand why quantum security must be considered in their jobs. (II) The misconceptions we identified should be directly pointed at and should be debunked. The students should learn how dangerous misconceptions can affect users' security [29]. (III) Additionally, quantum security should be part of any security lecture given e. g., to general computer science or engineering students, to build a basic foundation of understanding for everyone who needs to understand basics of encryption.

Only one participant reported to have gained quantum knowledge through reading scientific papers. While security experts can not be expected to read such, recent research indicated that a knowledge transfer from security research to organizational practice often fails [29]. For Quantum security, as a discipline born out of mathematical theory rather than applied engineering, this threat exists as well. If the field of applied quantum security research grows, those researchers should actively consider how new knowledge finds its way to non-academic experts, especially security decision-makers. We propose adding quantum security to the curriculum of security certificates common in the industry (like CISSP, CISM, and CISA) – as it has already been proposed for HCS [30]. Here, quantum security knowledge can reach senior professionals who have long left universities. While e. g., CISSP already touches on some quantum security

topics, it does not relate those to practical applications in organizations and products. Again, directly addressing the misconceptions is critical.

6 CONCLUSION

We conducted a first, locally limited, exploratory interview study to gain insights into the nature of misconceptions about (post) quantum cryptography. Misconceptions about (Post) Quantum Cryptography were widespread among the $n = 19$ security experts and students we interviewed. If security experts hold such misconceptions, they won't be able to guide the organizations they work for in making informed decisions about quantum security. Active myth-busting in training and science communication is required. Further, large-scale studies are necessary to assess how common the identified misconceptions are.

ACKNOWLEDGMENTS

We would like to thank all our study participants. Thanks to M. Angela Sasse, who helped us refine the instrument and coding through multiple discussions. Thanks to Jens Opdenbusch, Markus Schöps, Jana Eisoldt, and Marco Gutfleisch for their proofreading. Thanks also to the anonymous reviewers who provided us with unsparing and constructive feedback. The work was supported by the PhD School "SecHuman – Security for Humans in Cyberspace" by the federal state of NRW, Germany, and (partly) also by the Deutsche Forschungsgemeinschaft (DFG, German Research Foundation) under Germany's Excellence Strategy - EXC 2092 CASA - 390781972.

REFERENCES

[1] Ruba Abu-Salma, M. Angela Sasse, Joseph Bonneau, Anastasia Danilova, Alena Naiakshina, and Matthew Smith. 2017. Obstacles to the Adoption of Secure Communication Tools. In *IEEE Symposium on Security and Privacy (SP '17)*. IEEE, San Jose, California, USA, 137–153.

[2] Ruba Abu-Salma, M. Angela Sasse, Joseph Bonneau, Anastasia Danilova, Alena Naiakshina, and Matthew Smith. 2017. Obstacles to the Adoption of Secure Communication Tools. In *2017 IEEE Symposium on Security and Privacy (SP)*. 137–153.

[3] Yasemin Acar, Christian Stransky, Dominik Wermke, Charles Weir, Michelle L. Mazurek, and Sascha Fahl. 2017. Developers Need Support, Too: A Survey of Security Advice for Software Developers. In *2017 IEEE Cybersecurity Development (SecDev)*. IEEE, New York, 22–26.

[4] Frank Arute, Kunal Arya, Ryan Babbush, Dave Bacon, Joseph C Bardin, Rami Barends, Rupak Biswas, Sergio Boixo, Fernando GSL Brandao, David A Buell, et al. 2019. Quantum supremacy using a programmable superconducting processor. *Nature* 574, 7779 (2019), 505–510.

[5] Zahra Ashktorab, Justin D. Weisz, and Maryam Ashoori. 2019. Thinking Too Classically: Research Topics in Human-Quantum Computer Interaction. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems* (Glasgow, Scotland Uk) *(CHI '19)*. Association for Computing Machinery, New York, NY, USA, 1–12.

[6] Philip Ball. 2021. First 100-QUBIT quantum computer enters crowded race. *Nature* 599 (2021), 542.

[7] Charles H Bennett, Gilles Brassard, and Artur K Ekert. 1992. Quantum cryptography. *Scientific American* 267, 4 (1992), 50–57.

[8] Ethan Bernstein and Umesh Vazirani. 1993. Quantum Complexity Theory. In *Proceedings of the Twenty-Fifth Annual ACM Symposium on Theory of Computing* (San Diego, California, USA) *(STOC '93)*. Association for Computing Machinery, New York, NY, USA, 11–20.

[9] Vaishali Bhatia and K.R. Ramkumar. 2020. An Efficient Quantum Computing technique for cracking RSA using Shor's Algorithm. In *2020 IEEE 5th International Conference on Computing Communication and Automation (ICCCA)*. IEEE, New York, 89–94. https://doi.org/10.1109/ICCCA49541.2020.9250806

[10] Xavier Bonnetain, María Naya-Plasencia, and André Schrottenloher. 2019. Quantum security analysis of AES. *IACR Transactions on Symmetric Cryptology* 2019, 2 (2019), 55–93.

[11] Joppe Bos, Léo Ducas, Eike Kiltz, Tancrède Lepoint, Vadim Lyubashevsky, John M Schanck, Peter Schwabe, Gregor Seiler, and Damien Stehlé. 2018. CRYSTALS-Kyber: a CCA-secure module-lattice-based KEM. In *2018 IEEE European Symposium on Security and Privacy (EuroS&P)*. IEEE, IEEE, New York, 353–367.

[12] Virginia Braun and Victoria Clarke. 2021. One size fits all? What counts as quality practice in (reflexive) thematic analysis? *Qualitative research in psychology* 18, 3 (2021), 328–352.

[13] Caltech Science Exchange. 2022. How Will Quantum Technologies Change Cryptography? https://scienceexchange.caltech.edu/topics/quantum-science-explained/quantum-cryptography

[14] Chi Cheng, Rongxing Lu, Albrecht Petzoldt, and Tsuyoshi Takagi. 2017. Securing the Internet of Things in a quantum world. *IEEE Communications Magazine* 55, 2 (2017), 116–120.

[15] Victoria Clarke, Virginia Braun, and Nikki Hayfield. 2015. Thematic analysis. *Qualitative psychology: A practical guide to research methods* 222, 2015 (2015), 248.

[16] NIST Computer Security Resource Center (CSRC). 2022. Post-Quantum Cryptography Standardization. https://csrc.nist.gov/projects/post-quantum-cryptography/post-quantum-cryptography-standardization

[17] David Deutsch. 1985. Quantum theory, the Church–Turing principle and the universal quantum computer. *Proceedings of the Royal Society of London. A. Mathematical and Physical Sciences* 400, 1818 (1985), 97–117.

[18] Léo Ducas, Eike Kiltz, Tancrede Lepoint, Vadim Lyubashevsky, Peter Schwabe, Gregor Seiler, and Damien Stehlé. 2018. Crystals-dilithium: A lattice-based digital signature scheme. *IACR Transactions on Cryptographic Hardware and Embedded Systems* 2018 (2018), 238–268.

[19] Felix Fischer, Konstantin Böttinger, Huang Xiao, Christian Stransky, Yasemin Acar, Michael Backes, and Sascha Fahl. 2017. Stack Overflow Considered Harmful? The Impact of Copy&Paste on Android Application Security. In *2017 IEEE Symposium on Security and Privacy (SP)*. IEEE, New York, 121–136.

[20] Bundesamt für Sicherheit in der Informationstechnik (BSI). 2022. [GERMAN] Marktumfrage Kryptografie und Quantencomputing. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Krypto/Marktumfrage_Kryptografie_Quantencomputing.pdf?__blob=publicationFile&v=9

[21] Craig Gidney and Martin Ekerå. 2021. How to factor 2048 bit RSA integers in 8 hours using 20 million noisy qubits. *Quantum* 5 (2021), 433. https://doi.org/10.22331/q-2021-04-15-433

[22] Nicolas Gisin, Grégoire Ribordy, Wolfgang Tittel, and Hugo Zbinden. 2002. Quantum cryptography. *Reviews of modern physics* 74, 1 (2002), 145.

[23] Global Risk Institute. 2022. 2021 Quantum Threat Timeline Report - Global Risk Institute. https://globalriskinstitute.org/publications/2021-quantum-threat-timeline-report/

[24] Markus Grassl, Brandon Langenberg, Martin Roetteler, and Rainer Steinwandt. 2016. Applying Grover's Algorithm to AES: Quantum Resource Estimates. In *Post-Quantum Cryptography*, Tsuyoshi Takagi (Ed.). Springer International Publishing, Cham, 29–43.

[25] Dmitry Green, Henning Soller, Yuval Oreg, and Victor Galitski. 2021. How to profit from quantum technology without building quantum computers. *Nature reviews physics* 3, 3 (2021), 150–152.

[26] Lov K. Grover. 1996. A fast quantum mechanical algorithm for database search. In *Proceedings of the twenty-eighth annual ACM symposium on Theory of computing - STOC '96*, Gary L. Miller (Ed.). ACM Press, New York, New York, USA, 212–219. https://doi.org/10.1145/237814.237866

[27] Franziska Herbert, Steffen Becker, Leonie Schaewitz, Jonas Hielscher, Marvin Kowalewski, Angela Sasse, Yasemin Acar, and Markus Dürmuth. 2023. A World Full of Privacy and Security (Mis)Conceptions? Findings of a Representative Survey in 12 Countries. In *Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems* (Hamburg, Germany) *(CHI '23)*. Association for Computing Machinery, New York, NY, USA, Article 582, 23 pages.

[28] Jonas Hielscher, Annette Kluge, Uta Menges, and M. Angela Sasse. 2022. "Taking out the Trash": Why Security Behavior Change Requires Intentional Forgetting. In *Proceedings of the 2021 New Security Paradigms Workshop* (Virtual Event, USA) *(NSPW '21)*. Association for Computing Machinery, New York, NY, USA, 108–122. https://doi.org/10.1145/3498891.3498902

[29] Jonas Hielscher, Uta Menges, Simon Parkin, Annette Kluge, and M Angela Sasse. 2023. "Employees Who Don't Accept the Time Security Takes Are Not Aware Enough": The CISO View of Human-Centred Security. In *USENIX Security 2023*. USENIX Association, Berkeley, 1–19.

[30] Jonas Hielscher, Markus Schöps, Uta Menges, Marco Gutfleisch, Mirko Helbling, and M. Angela Sasse. 2023. Lacking the Tools and Support to Fix Friction: Results from an Interview Study with Security Managers. In *Nineteenth Symposium on Usable Privacy and Security (SOUPS 2023)*. USENIX Association, Anaheim, CA, 131–150. https://www.usenix.org/conference/soups2023/presentation/hielscher

[31] Rosa M. Gil Iranzo, Mercè Teixidó Cairol, Carina González González, and Roberto García. 2021. Learning Quantum Computing: An Interaction Protocol for Quantum Computing Interfaces. In *Proceedings of the XXI International Conference on Human Computer Interaction* (Málaga, Spain) *(Interacción '21)*. Association for Computing Machinery, New York, NY, USA, Article 13, 5 pages.

[32] David Joseph, Rafael Misoczki, Marc Manzano, Joe Tricot, Fernando Dominguez Pinuaga, Olivier Lacombe, Stefan Leichenauer, Jack Hidary, Phil Venables, and Royal Hansen. 2022. Transitioning organizations to post-quantum cryptography. *Nature* 605, 7909 (2022), 237–243.

[33] Ruogu Kang, Laura Dabbish, Nathaniel Fruchter, and Sara B. Kiesler. 2015. "My Data Just Goes Everywhere:" User Mental Models of the Internet and Implications for Privacy and Security. In *Symposium on Usable Privacy and Security (SOUPS '15)*. USENIX, Ottawa, Canada, 39–52.

[34] Predrag Klasnja, Sunny Consolvo, Jaeyeon Jung, Benjamin M. Greenstein, Louis LeGrand, Pauline Powledge, and David Wetherall. 2009. "When I Am on Wi-Fi, I Am Fearless": Privacy Concerns & Practices in Eeryday Wi-Fi Use. In *ACM Conference on Human Factors in Computing Systems (CHI '09)*. ACM, Boston, Massachusetts, USA, 1993–2002.

[35] Huzeyfe Kocabas, Swapnil Nandy, Tanjina Tamanna, and Mahdi Nasrullah Al-Ameen. 2021. Understanding User's Behavior and Protection Strategy upon Losing, or Identifying Unauthorized Access to Online Account. In *International Conference on Human-Computer Interaction (HCII '21)*. Springer, Virtual Conference, 310–325.

[36] Katharina Krombholz, Karoline Busse, Katharina Pfeffer, Matthew Smith, and Emanuel von Zezschwitz. 2019. "If HTTPS Were Secure, I Wouldn't Need 2FA" – End User and Administrator Mental Models of HTTPS. In *IEEE Symposium on Security and Privacy (SP '19)*. IEEE, San Francisco, California, USA, 246–263.

[37] Udo Kuckartz. 2012. *Qualitative inhaltsanalyse (German)*. Beltz Juventa, Weinheim, Germany.

[38] Vasileios Mavroeidis, Kamer Vishi, Mateusz D Zych, and Audun Jøsang. 2018. The impact of quantum computing on present cryptography.

[39] Matan Mazor and Stephen M Fleming. 2021. The Dunning-Kruger effect revisited. *Nature Human Behaviour* 5, 6 (2021), 677–678.

[40] Uta Menges, Jonas Hielscher, Laura Kocksch, Annette Kluge, and M. Angela Sasse. 2023. Caring Not Scaring – An Evaluation of a Workshop to Train Apprentices as Security Champions. In *Proceedings of the 2023 European Symposium on Usable Security* (Copenhagen, Denmark) *(EuroUSEC '23)*. Association for Computing Machinery, New York, NY, USA, 1–24.

[41] Piotr Migdał, Klementyna Jankiewicz, Paweł Grabarz, Chiara Decaroli, and Philippe Cochin. 2022. Visualizing quantum mechanics in an interactive simulation–Virtual Lab by Quantum Flytrap. *Optical Engineering* 61, 8 (2022), 081808–081808.

[42] Michele Mosca. 2018. Cybersecurity in an era with quantum computers: Will we be ready? *IEEE Security & Privacy* 16, 5 (2018), 38–41.

[43] Lorenzo Neil, Harshini Sri Ramulu, Yasemin Acar, and Bradley Reaves. 2023. Who Comes Up with this Stuff? Interviewing Authors to Understand How They Produce Security Advice. In *Nineteenth Symposium on Usable Privacy and Security (SOUPS 2023)*. USENIX Association, Anaheim, CA, 283–299. https://www.usenix.org/conference/soups2023/presentation/neil

[44] NIST. 2022. Cryptography in the Quantum Age. https://www.nist.gov/physics/introduction-new-quantum-revolution/cryptography-quantum-age

[45] NIST. 2022. Quantum Supremacy. https://www.nist.gov/physics/introduction-new-quantum-revolution/quantum-supremacy

[46] Physics World. 2021. Quantum cryptography network spans 4600 km in China – Physics World. https://physicsworld.com/a/quantum-cryptography-network-spans-4600-km-in-china/

[47] Mario Piattini, Manuel Serrano, Ricardo Perez-Castillo, Guido Petersen, and Jose Luis Hevia. 2021. Toward a Quantum Software Engineering. *IT Professional* 23, 1 (2021), 62–66. https://doi.org/10.1109/MITP.2020.3019522

[48] Stefano Pirandola, Ulrik L Andersen, Leonardo Banchi, Mario Berta, Darius Bunandar, Roger Colbeck, Dirk Englund, Tobias Gehring, Cosmo Lupo, Carlo Ottaviani, et al. 2020. Advances in quantum cryptography. *Advances in optics and photonics* 12, 4 (2020), 1012–1236.

[49] Stefan Rädiker and Udo Kuckartz. 2019. *Analyse qualitativer Daten mit MAXQDA*. Springer.

[50] Robert W. Reeder, Iulia Ion, and Sunny Consolvo. 2017. 152 Simple Steps to Stay Safe Online: Security Advice for Non-Tech-Savvy Users. *IEEE Security & Privacy* 15, 5 (Oct. 2017), 55–64.

[51] Oded Regev. 2023. An efficient quantum factoring algorithm. *arXiv preprint arXiv:2308.06572* (2023).

[52] Karen Renaud and Marc Dupuis. 2020. Cyber Security Fear Appeals: Unexpectedly Complicated. In *Proceedings of NSPW '19'* (San Carlos, Costa Rica) *(NSPW '19)*. Association for Computing Machinery, New York, NY, USA, 42–56. https://doi.org/10.1145/3368860.3368864

[53] Karen Renaud, Melanie Volkamer, and Arne Renkema-Padmos. 2014. Why Doesn't Jane Protect Her Privacy? In *Privacy Enhancing Technologies*, Emiliano De Cristofaro and Steven J. Murdoch (Eds.). Vol. 8555. Springer International Publishing, 244–262. https://doi.org/10.1007/978-3-319-08506-7_13 http://link.springer.com/10.1007/978-3-319-08506-7_13.

[54] SARA GAMBLE. 2019. Quantum Computing: What It Is, Why We Want It, and How We're Trying to Get It. In *Frontiers of Engineering: Reports on Leading-Edge Engineering from the 2018 Symposium*, SARA GAMBLE (Ed.). National Academies Press (US), Washington. https://www.ncbi.nlm.nih.gov/books/NBK538701/

[55] Zeki C Seskir, Piotr Migdał, Carrie Weidner, Aditya Anupam, Nicky Case, Noah Davis, Chiara Decaroli, İlke Ercan, Caterina Foti, Paweł Gora, et al. 2022. Quantum games and interactive tools for quantum technologies outreach and education. *Optical Engineering* 61, 8 (2022), 081809–081809.

[56] P. W. Shor. 1994. Algorithms for quantum computation: discrete logarithms and factoring. In *35th Annual Symposium on Foundations of Computer Science*, Shaffi Goldwasser (Ed.). IEEE Press, Los Alamitos, 124–134. https://doi.org/10.1109/SFCS.1994.365700

[57] Peter W. Shor. 1997. Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer. *SIAM J. Comput.* 26, 5 (1997), 1484–1509. https://doi.org/10.1137/S0097539795293172

[58] Daniel R Simon. 1997. On the power of quantum computation. *SIAM journal on computing* 26, 5 (1997), 1474–1483.

[59] John A Smolin, Graeme Smith, and Alexander Vargo. 2013. Oversimplifying quantum factoring. *Nature* 499, 7457 (2013), 163–165.

[60] Peter Story, Daniel Smullen, Yaxing Yao, Alessandro Acquisti, Lorrie Faith Cranor, Norman Sadeh, and Florian Schaub. 2021. Awareness, Adoption, and Misconceptions of Web Privacy Tools. In *Privacy Enhancing Technologies Symposium (PETS '21)*. Sciendo, Virtual Conference, 308–333.

[61] Jesper Strömbäck, Yariv Tsfati, Hajo Boomgaarden, Alyt Damstra, Elina Lindgren, Rens Vliegenthart, and Torun Lindholm. 2020. News media trust and its impact on media use: toward a framework for future research. *Annals of the International Communication Association* 44, 2 (2020), 139–156. https://doi.org/10.1080/23808985.2020.1755338

[62] Daniel F. Styer. 1996. Common misconceptions regarding quantum mechanics. *American Journal of Physics* 64, 1 (1996), 31–34. https://doi.org/10.1119/1.18288

[63] Yariv Tsfati. 2011. Media Credibility. In *Oxford bibliographies*, Patricia Moy (Ed.). Oxford University Press, [New York]. https://doi.org/10.1093/obo/9780199756841-0080

[64] U.S. Department of Homeland Security. 2012. The Menlo Report: Ethical Principles Guiding Information and Communication Technology Research. https://www.caida.org/publications/papers/2012/menlo_report_actual_formatted/, as of August 19, 2024.

[65] Joseph Verble. 2014. The NSA and Edward Snowden: surveillance in the 21st century. *ACM Sigcas Computers and Society* 44, 3 (2014), 14–20.

[66] WinMagic. 2014. Is Encryption Dead? – SecureSpeak | WinMagic Data Security Blog. https://winmagic.com/blog/is-encryption-dead/

[67] Yuxi Wu, Panya Gupta, Miranda Wei, Yasemin Acar, Sascha Fahl, and Blase Ur. 2018. Your Secrets Are Safe: How Browsers' Explanations Impact Misconceptions About Private Browsing Mode. In *The World Wide Web Conference (WWW '18)*. ACM, Lyon, France, 217–226.

[68] Alexander Zable, Lloyd Hollenberg, Eduardo Velloso, and Jorge Goncalves. 2020. Investigating Immersive Virtual Reality as an Educational Tool for Quantum Computing. In *Proceedings of the 26th ACM Symposium on Virtual Reality Software and Technology* (Virtual Event, Canada) *(VRST '20)*. Association for Computing Machinery, New York, NY, USA, Article 6, 11 pages.

[69] Jianjun Zhao. 2020. Quantum software engineering: Landscapes and horizons.

A PRE-SCREENING QUESTIONNAIRE

Demographics.

(1) How old are you? [Open]
(2) Which gender do you feel you belong to? [Open]
(3) What is your current employment status?
  (a) employed in the information sector (quaternary sector)
  (b) employed in the service industry (tertiary sector)
  (c) employed in the industrial sector (secondary sector)
  (d) job-seeking
  (e) not employed
  (f) self-employed
  (g) mainly student
  (h) mainly pupil
  (i) others, and that is ____
(4) Do you currently work, or have you worked, in the IT-security field?
(5) (Question removed for anonymity)

Self-assessment Quantum.

(1) Please give a self-assessment, to what extent you are familiar with the respective topic. [I have never heard of it; I have heard of it, but I don't know what it is.; I have an idea of it, but don't know when or how to use it.; I know what it is and can explain what it is used for.;I know what it is and have already actively used my knowledge.]
  (a) Quantum Physics
  (b) Quantum Mechanics
  (c) Quantum Computers
  (d) Quantum Cryptography
  (e) Post-Quantum Cryptography
(2) Do you know of any other topics that fits into the topic of quantum? [Open]
(3) Now please write in 1-2 sentences what you know about the topic of ...
  - Quantum Physics
  - Quantum Mechanics
  - Quantum Computers
  - Quantum Cryptography
  - Post-Quantum Cryptography
  - Other Quantum Topic

B INTERVIEW GUIDE

A: Introduction via news.

A1 Two years ago (2019), the company Google was featured heavily in the news with its quantum computer. It was announced that Google had achieved Quantum Supremacy. Have you ever heard about this?
A2 Or do you know of any other news stories related to the field quantum?
A3 What have you heard about this topic?
A4 What do you understand under the term quantum superiority?
A5 To what extent did this news affect you personally?

B: Quantum computer (vs. classical computer).

B1 How do you envision a quantum computer? [appearance, construction, functionality]
B2 Now let us take a look at the abilities of quantum computers. What can quantum computers do, and what can they not do? [theoretical capabilities, current/momentary capabilities]
B3 How do they [quantum computers] compare to the classical computer?
B3.1 What do you mean when you say *efficiently computable* here?
B4 What do you know about the current state of the art of (existing) quantum computers?
B5 IBM, for example, offers online access to various quantum computers to use. Have you already had (personal) experience with a quantum computer? What kind of experience?
B6 What benefits do you think quantum computers can offer?
B7 Do you see any dangers or risks that could be introduced or magnified by quantum computers? (with respect to previously mentioned capabilities)
B8 How do you estimate the (future) development/progress in the field of quantum computers? Do you see an increased use of quantum computers in the near future, or is something like the personal quantum computer for at home still a long way to go? And why do you assume that?
B9 How important is the topic of quantum computers for you personally? Do you think about this frequently, or does it have rather little relevance for you? Why?

C: Impact of quantum computing on IT security.

C0 So far, we have mainly focused on quantum computers. Let us now take a step further and look at it more closely in regard to the subject of IT security.
C1 What impact do quantum computers have on IT security?
C2 Which consequences do you see for symmetric encryption in particular? And which for asymmetric encryption?
C3 Which of these consequences exist currently only in theory? Which ones influence us already?
C4 And how, do you think, this will develop in the future? Will the theoretical consequences remain only theory, or will they soon be reality?
C5 Can you think of any other dangers or risks that quantum computers pose to IT security?
C6 How severe do you consider the dangers or risks mentioned, in general and for you personally?
C7 To what extent does this perception influence your behavior? Have you changed anything in particular as a result?
C8 Can you think of any other ways in which quantum computers could impact the field of IT security?

D: Quantum cryptography/post-quantum cryptography.

D0 Next, let us take a look at a specific area of IT security, the cryptography.

D1 Have you ever heard of the terms *quantum cryptography* or *post-quantum cryptography*? What do you understand under them?
D2 How important do you consider these topics to be? And why?
D3 Do you think we need quantum or post-quantum cryptography? Why?
D4 What do you think, when will we need quantum or post-quantum cryptography? Do we need it already or is it not that relevant yet? Why?
D5 What else comes to your mind when you think of the terms *quantum cryptography* and *post-quantum cryptography*?
D5.1 Inquiry on the mentioned topic
D6 Where did you acquire your knowledge on this?

E: Quantum physics/quantum mechanics.

E0 Let us now turn to the underlying principles on which quantum computers operate.
E1 How do you define *quantum physics*, and how do you define *quantum mechanics*? What do you consider to be the difference between both?
E2 What characteristics or principles do you consider to be particularly important for understanding what constitutes *quantum*? [superposition, entanglement, ...]
E3 Which of these characteristics or principles are important for quantum computers? Why? In what way or to what extent?
E4 In your opinion, is this knowledge necessary? How much knowledge is needed in general, how much for handling a quantum computer or for quantum cryptography?
E5 Now thinking about news (e.g. from newspapers or online), how much or what kind of background knowledge do you think is needed for understanding this news?
E6 How many people do you reckon understand this news, or how much of such news is understood?
E7 Do you consider this to be a little or a lot? And what could be the consequences?

F: Free quantum topic.

F0 We have now addressed various topics in the field of *quantum*. [Here, the theme mentioned in the pre-screening is picked up.]
F1 In the online survey you took part in previously, you also mentioned _____. Why exactly did you mention this, and what can you tell me about it? [Here, the possibility to choose a completely free topic is given.]
F2 Is there (other than that) another topic that is missing here, and which you would like to address? Which topic?
F3 You have just explicitly mentioned ___. Why does this topic have a special meaning to you? And what can you tell me about it?

G: Review & Misconceptions.

G0 We have already talked about various topics in the field of quantum, about the news you hear in the media, about quantum computers and their impact on IT security, about quantum and post-quantum cryptography, and finally about the theories on which all this is built - quantum physics and quantum mechanics. All this shows that these topics are very extensive and quite complex. This naturally can make comprehension more difficult and lead to misunderstandings.

G1 Have you encountered any misunderstandings or misconceptions about the topic of quantum? If yes, what kind of?

G2 Were you immediately aware that there were inconsistencies? Or how did you notice that it was a misconception/inconsistency?

G3 Can you think of any other misconceptions or misunderstandings about quantum that might exist? For example, about quantum computers or about quantum cryptography.

G4 How would you explain these misconceptions or misunderstandings?