European Journal of Science, Innovation and Technology
ISSN 2786-4936
Vol. 2 No. 5 (2022)

Quantum Computers and the Risks They Pose to Small and Medium-Sized Enterprises

Paulina Schindler
Friedrich Schiller University, Carl-Zeiss-Straße 3, 07743 Jena, Germany

Abstract. Quantum computers are currently being developed and are expected to supersede classical computers in many areas. Besides their positive use cases, they can pose significant dangers to data security in businesses. The aim of this paper is to raise awareness of this topic and support the preparation of all market participants for the advent of quantum computing. First, the possible dangers quantum computers pose to data security are identified. Approaches to solutions and the necessary transition process are researched that can help to protect data in the face of quantum computers, based on recommendations by the American National Institute of Standards and Technology and the German Federal Office for Information Security. Based on this knowledge and the need to create awareness, further research is planned to provide concepts to accelerate the spread of quantum computer-safe measures as soon as they become available. Throughout this paper, special focus lies especially on small and medium-sized enterprises that often can be characterised by a lack of resources to protect themselves and less interest in data security topics. Recommendations for a smooth transition to a quantum computer-safe environment for all market participants are given.

Keywords: quantum computing, data security, preparation, SME

The Relevance of Quantum Computers for Data Security

Quantum computers as part of quantum technologies have become a relevant topic for the public (Ernst, Warnke, & Schröter, 2020). They are expected to solve a broad range of existing computationally expensive problems, with a significant impact on our daily lives and existing industries (Ali, Yue, & Abreu, 2022) and great importance globally (Lindsay, 2022). However, this impact can not only be positive but also pose dangers. The aim of this paper is to inform and raise awareness of this topic, especially among vulnerable market participants so they can prepare for the arrival of quantum computers. Based on this, further research projects can be identified.

The development of quantum computers is currently underway, although they are not yet available for widespread use in practice (Mohr, Ostojic, Heid, Pautasso, & Biondi, 2021). The time of the release of quantum computers to the public is still unclear and difficult to predict (Dyakonov, 2018; Mailloux, Lewis II, Riggs, & Grimaila, 2016; Preskill, 2019). The day they will arrive is sometimes referred to as 'Q-Day' (Castelvecchi, 2022). In special cases, they can already partially be used to solve certain problems (Arute et al., 2019; Huh, Guerreschi, Peropadre, McClean, & Aspuru-Guzik, 2015; Schuld, Brádler, Israel, Su, & Gupt, 2020; Zhong et al., 2020).

Generally, quantum computers can either be developed with a certain task in mind (non-universal) or no predetermined purpose (universal) (Mavroeidis, Vishi, D., & Jøsang, 2018). Different technologies to reach this goal are being experimented on (Almudever et al., 2017; Bobier, Langione, Tao, & Gourévitch, 2021; Gyongyosi & Imre, 2019; van Meter & Oskin, 2006). First endeavours have been started to make quantum computers available to the public via cloud computing (Amazon; IBM; Microsoft). It is already clear that quantum computers will be superior at certain tasks that would overwhelm classical computers, utilizing their so-called 'quantum supremacy' (Dyakonov, 2018; Ernst et al., 2020; Preskill, 2019; Wittkopp, 2021). However, this supremacy will not apply to every computing task (Mavroeidis et al., 2018), which means that classical computers will not be rendered completely obsolete. This supremacy is made possible through their special architecture with their smallest computing unit qubits. Unlike classical computers, their base states 0 and 1 can overlap and thus be both

simultaneously until they are measured, where they fall back to one of their base states with a certain probability (Ernst et al., 2020; Mailloux et al., 2016). This makes true parallel processing possible (Mavroeidis et al., 2018). The ideal amount of qubits needed for quantum supremacy is not yet clear (Dalzell, Harrow, Koh, & La Placa, 2020; Dyakonov, 2018; Kelly, 2018) and may depend on the specific hardware that is used. Developmental challenges concerning quantum computers that are currently being worked on include error correction with necessary overhead (Bobier et al., 2021; Dyakonov, 2018; Mavroeidis et al., 2018; Mohr et al., 2021; Steane, 1998, 443 ff.), the difficulty of copying because of the no-cloning theorem (Buzek & Hillery, 1996; Gisin, Ribordy, Tittel, & Zbinden, 2002; Murer, 2021) and the general prevention of bugs in the system (Huang & Martonosi, 2019; Paltenghi & Pradel, 2022; Williams & Clearwater, 2000). Hardware errors still place limits on the current capabilities of quantum computers (Ali et al., 2022; Mavroeidis et al., 2018; Paltenghi & Pradel, 2022).

Because of the special characteristics of quantum computers which set them apart from classical computers (Mavroeidis et al., 2018), software applications for quantum computers need specialised software engineering methods and programmers need an understanding of quantum theory (Ali et al., 2022). Not only software for external purposes, but also means to protect quantum computers from attacks must be implemented (Deshpande, Xu, Trochatos, Ding, & Szefer, 2022). The development of appropriate software for quantum computers will take time because all phases of the development lifecycle (from development to testing, debugging, and maintenance) must be completed for a reliable result (Ali et al., 2022). Associated plans should not be limited to a specific programming language (Ali et al., 2022) to increase the availability of resources and personnel. The limited availability of appropriate algorithms in open source libraries can make the developing process more difficult (Hekkala, Halunen, & Vallivaara, 2022). Quantum computers and their possible use cases are expected to impact many industries, e.g. healthcare with drug research and finance with portfolio management and optimisation (Ali et al., 2022). Their improved performance in comparison to classical computers makes them also very interesting for simulation and optimisation tasks and machine learning (Ali et al., 2022; Mavroeidis et al., 2018; Mohr et al., 2021; Strohm, 2021; Wittkopp, 2021). However, programming solutions for specialised industry use cases place a lot of demands on programmers. It is not only necessary to understand classical programming principles but to have knowledge about quantum theory and the applicable industry (Ali et al., 2022). In this context exist several possible areas of research, e.g. in requirements engineering for quantum computer software (Ali et al., 2022), testing on quantum computers (Wang, Arcaini, Yue, & Ali, 2022), and cryptographic aspects.

Cryptography is an important aspect of modern communication, from messaging through emails or instant messaging tools to the safekeeping of personal information and digital payment (Mavroeidis et al., 2018; Ukwuoma, Arome, Thompson, & Alese, 2022). In encryption, a distinction between symmetric and asymmetric encryption methods can be made (Chandra, Paira, Alam, & Sanyal, 2014). Symmetric encryption methods use a single private key to encrypt and decrypt a message. This makes the secure transmission of the key from the sender to receiver important and a possible difficulty, making asymmetric encryption more attractive for remote communication using the Internet. Asymmetric encryption uses a public and private key pair (Mavroeidis et al., 2018). The public key can be transmitted to the sender via less secure communication channels because it is only used for encryption. The private key, which can be used to decrypt the encrypted information, remains with the recipient and is kept secret. Classically, the public key can be used to encrypt information in a way it can only be decrypted with knowledge of the corresponding private key (Mavroeidis et al., 2018). To make encryption in one direction but not decryption in the other direction possible, one-way functions are used (Diffie & Hellman, 1976). These are harder to calculate in one direction than the other (Castelvecchi, 2022; Joseph et al., 2022). Common in this regard are factorisation

problems (used in RSA) and discrete logarithm problems (which Diffie-Hellmann and Elliptic Curve Cryptography are based on) (Mavroeidis et al., 2018). Using their specialised superior capabilities (Murer, 2021), quantum computers can decrypt asymmetric cryptographic systems because they can solve one-way functions in the other direction as intended. Often, Shor's algorithm is used for breaking these asymmetric methods (Shor, 1994) like RSA, Diffie-Hellman, and elliptic curve cryptography (Hallgren & Vollmer, 2009). Symmetric cryptographic methods are not necessarily safe from quantum computers, either. While certain methods (e.g. one time-pad) still are considered safe from quantum computers under compliance with certain requirements (like a certain key length), in some cases symmetric encryption can be broken by quantum computers, which makes them a minor threat in this regard (Bellovin, 2011; Mailloux et al., 2016; Mavroeidis et al., 2018; Murer, 2021). Grover's algorithm can be used to run brute force encryption attacks faster if the key size is lacking (Grover, 1997). This can impact a lot of hash functions with shorter key lengths, for example (Brassard, HØyer, & Tapp, 1998). In some cases, cryptographic algorithms can be considered safe if they use longer keys (Ukwuoma et al., 2022). However, too long keys can make digital communication and processes more difficult, and an efficient balance needs to be found (Castelvecchi, 2022; Wallden & Kashefi, 2019). In summary, all currently widely-used asymmetric encryption systems are expected to be rendered insecure when quantum computers are established (Mavroeidis et al., 2018; NIST, 2022; Ukwuoma et al., 2022; Wallden & Kashefi, 2019). Besides the risk of data being compromised, important infrastructures could be victimised with catastrophic results (Barbeau & Garcia-Alfaro, 2022). However, this danger does not only lie in the future. Quantum computers pose two kinds of threats to information security (Joseph et al., 2022). The more obvious threat will exist when quantum computers are available for widespread use with the possibility of cryptosystems being broken. However, data is already in danger even without these being available right now because of the so-called store-now-decrypt-later attack. Encrypted data can be captured now and simply stored for later, where it will be decrypted as soon as quantum computers are available. This means that sensitive data is already susceptible to the danger of quantum computers (Castelvecchi, 2022; Joseph et al., 2022; Wallden & Kashefi, 2019), creating considerable urgency.

Why Especially Small and Medium-Sized Enterprises are Vulnerable

Over 99% of all companies can be considered small or medium-sized enterprises (SMEs) (IfM Bonn, 2021a; OECD, 2019; Statistisches Bundesamt, 2021) and thus are an important factor of economic growth (European Commission, 2020). Companies are classified as SMEs if they fall below certain limits in employee numbers and income that can differ per definition (Ayyagari, Beck, & Demirguc-Kunt, 2007; BSI, 2012; European Commission, 2020; IfM Bonn, 2021b). This can be seen as a lack of availability of resources in comparison to bigger companies. Just like their bigger counterparts, SMEs use IT for their business processes and are active on the internet (BSI, 2012). However, their lack of resources can make the preparation for IT security threats difficult. Often, SMEs have fewer financing options, are more dependent on a few business partners (Ihlau & Duscha, 2019), also concerning their IT applications (Taege, 2021), and generally have fewer IT resources, staff, and structures available (BSI, 2012; Taege, 2021). They know fewer details about their own IT security measures (Dreißigacker, Skarczinski, & Wollinger, 2020) and utilise IT security measures less than bigger companies (Dreißigacker et al., 2020; Pawlowska & Scherer, 2020). Although they are generally aware of IT security risks existing (BSI, 2012), they lack knowledge of and interest in them (ACSC, 2020; BSI, 2012). Because of this, even though bigger companies are attacked digitally more often than SMEs (Dreißigacker et al., 2020), SMEs are more likely to see an attack as threatening to their existence (Pawlowska & Scherer, 2020). Even though IT

security problems in SMEs continue to occur, they see their current measures as sufficient and locate the root of IT security problems outside of the company rather than inside (BSI, 2012).

Their lack of awareness and interest in the topic could place SMEs at risk and make them vulnerable to attacks, especially if they don't identify themselves as interesting targets (Dreißigacker et al., 2020). Because SMEs are less prepared for IT security risks, they are likely to be unguarded for new developments in IT security threats. Especially transitions that have a greater scope than classical security transitions, like the transition to quantum computing (Joseph et al., 2022), are posing great dangers to them. Combined with them possibly already being late preparing for this new threat (Joseph et al., 2022), SMEs can be considered especially vulnerable in this regard.

This lack of interest and resources suggests that SMEs, therefore, are more likely to have to rely on standard IT security solutions instead of creating their own. These will have to be updated to protect against attacks by quantum computers. Currently used IT security systems could collapse when quantum computers are introduced if they are not prepared for them (Alyami et al., 2022), leaving SMEs unprotected. To make the widespread implementation of quantum computer-secure encryption methods possible, potentially new algorithms must be researched and a consensus on a good solution must be found.

How to Protect Data from Attacks by Quantum Computers

To keep information safe in the face of quantum computers, quantum computer-secure encryption methods are being researched. Two major movements in this are quantum cryptography and post-quantum cryptography. Because quantum computers can not only be used for offense but also defence (Lindsay, 2022; Wallden & Kashefi, 2019), the movement of quantum cryptography relies on quantum phenomena and thus is implemented on quantum computers. The other movement, post-quantum cryptography, works on a classical computing architecture and thus is much more convenient for use with existing machines. Because of this, it is expected to have lower costs and less difficulty in integration (Joseph et al., 2022). The efforts to determine and implement quantum computer-safe cryptography measures have already begun (BSI, 2021; Castelvecchi, 2022; Joseph et al., 2022). Currently, research is done on cryptographic solutions that are expected to be able to resist quantum computer attacks if used accordingly, e.g. cryptography based on hashes, codes, lattices, multivariate-quadratic-equations, and generally cryptography with long enough keys (Bernstein, Buchmann, & Dahmen, 2009; Mavroeidis et al., 2018; Ukwuoma et al., 2022).

In an international effort for quantum-computer-safe standardisation since 2016, the U.S. Department of Commerce's National Institute of Standards and Technology (NIST) audits different encryption algorithms from cryptographers around the world for quantum computer-safe encryption solutions for general encryption and digital signatures. While four algorithms already have been chosen as a future part of NIST's cryptographic standard, currently, four additional algorithms are under consideration (NIST, 2022). The availability of different algorithms allows for choice in different situations. For general encryption, NIST has already selected the CRYSTALS-kyber algorithm. The algorithms CRYSTALS-Dilithium, FALCON, and SPHINCS+ were selected for digital signatures. While the majority is lattice-based, SPHINCS+ uses hash functions. The algorithms that were already chosen are currently being finalised. After the standardisation process is done, these algorithms still need to be implemented in all necessary systems (Castelvecchi, 2022). Although the protection of data from attacks by quantum computers is a time-sensitive topic with preparations possibly already late (Joseph et al., 2022) thus creating urgency, the NIST standardisation process is behind schedule (Johnson, 2021). Before a finalised standard is available, NIST advises users to inventory their applications for necessary changes in cryptography (NIST, 2022). To offer solutions for interested parties in the meantime, the German Federal Office for Information

Security (BSI) has issued recommendations for algorithms (BSI, 2021): the code-based Classic McEliece and the lattice-based FrodoKEM, both of which were involved in the NIST selection process. Preparing systems for crypto-agility can also help with the implementation of future standards (BSI, 2021; Joseph et al., 2022). Using hybrid solutions of post-quantum algorithms and classical cryptographic algorithms can serve to increase the protection even further and minimise the risk for data in the transition phase (BSI, 2021; Castelvecchi, 2022; Ernst et al., 2020; Joseph et al., 2022; Meier, 2019; Mohr et al., 2021).

Preparing the transition to post-quantum cryptography now will enable proper planning and prevent shortcomings through a rushed transition later. This preparation and strategic planning phase should be started early and completed before quantum computers can effectively attack current cryptosystems (Joseph et al., 2022). Because of the possibility of store-now-decrypt-later attacks, some companies can already be considered late in their preparations. Additionally, data that must be stored for over five years or is involved in the long-term planning of projects is also already in need of protection from quantum computers now. Because the protection of data from quantum computers proves to be very time-sensitive, efforts to reach this goal should already be underway.

After that, when post-quantum cryptography measures are determined and available, adoption of it in production systems is the next step (Joseph et al., 2022). This transition is expected to take years (Wallden & Kashefi, 2019), often estimated to take at least five (Castelvecchi, 2022; Joseph et al., 2022). In the transition process, a lot of possible variables will have to be considered because many parties are involved in modern digital communication. This will make testing necessary before implementation. Because of the requirements of future encryption standards, communications using these might be blocked by not yet updated devices because of unfamiliar structure (Castelvecchi, 2022) or of the higher hardware demands it may place on smaller devices like from the Internet of Things environment. However, the first experiments show that it can be possible (Chung, Pai, Ching, Wang, & Chen, 2022; Schöffel, Lauer, Rheinländer, & Wehn, 2022). Devices that are seldom updated or have hardwired security features (e.g. smart cars and ATMs) may have difficulties with the transition, too (Castelvecchi, 2022; Gupta, Ray, Singh, & Kumari, 2022). Software like Antivirus programs could also misunderstand the intention of these new encryption protocols if not updated accordingly (Castelvecchi, 2022).

How Particularly Small and Medium-Sized Enterprises Can be Kept Safe

In conclusion, while quantum computers can already pose dangers to data, protection measures are still in development and under evaluation. To bridge this gap, companies should already start the preparations for the transition. However, especially SMEs may have trouble adopting necessary changes in time. SMEs are shown to have three major areas of vulnerability: a lack of resources, including money; a lack of knowledge concerning quantum computers among management and employees and a lack of interest in the topic. Because of this, especially these three topics should be considered for support measures.

To mitigate a lack of resources, financial incentives and support are possible solutions. Reducing the difficulties of SMEs to work together with other companies and offering them resources like financial support and know-how can help with the introduction of innovation in an SME (Bigliardi, Colacino, & Dormio, 2011). Governmental support and teaching might improve the situation in SMEs but might not reach everyone. However, implementing post-quantum cryptography into standardised, ready-to-go security solutions and offering them at low cost may have the same effect and mitigate all three problem areas. Industrial integrators of cryptography (OEMs) can use existing algorithms and integrate them into their standardised solutions that are then offered to the end customer (Fraunhofer Institute, 2018). These end customers, in this example SMEs, do not have to concern themselves with the specifics of post-

quantum cryptography this way. The necessary algorithmic libraries for inclusion in the software of the OEMs will be provided by publicly available algorithms that are chosen in official standardisation processes (e.g. by NIST). Because there usually are a lot of algorithmic options to choose from, OEMs will profit from the standardisation of post-quantum cryptography, as it will make the necessary choices easier. Before the availability of such a standard, preparing a flexible, hybrid approach combining classical algorithms and post-quantum cryptography (BSI, 2021) might make the transition smoother. If a quantum computer-secure consensus among the most influential developers of standardised software is reached and implemented, all their customers will be safe automatically without them needing to act in this regard specifically. This has the additional benefit of fewer actors that need to be incentivised to act and is a good way to reach especially vulnerable companies like some SMEs.

The development of security measures against quantum computers beyond theoretical research is currently behind the development of the dangers quantum computers can already pose. Because of this, the advancement and spread of related security measures needs to be accelerated. Since SMEs can be seen as especially vulnerable in this regard, focus lies on them as important market participants. Additionally, their environment and other interacting market participants, like the government, customers and cooperating or competing companies (including OEMs) will have to be considered. Different areas of interest in this context include software development and engineering to provide appropriate security solutions, but also the management of technological innovations and the political and legal framework. To find out what influences the spread of appropriate security measures between market participants and how this spread can be accelerated, an agent-based simulation is planned. Simulating the interactions of market participants concerning data security in the face of quantum computing, and how the change of certain parameters may influence that, can lead to new findings that might otherwise have been overlooked. Additionally, new important actors or influences can be determined, and the influence of existing known participants can be tested. These findings can be used to create a new concept that incorporates the most important influences to speed up the spread of quantum computer-safe measures between all market participants as soon as appropriate solutions become available.

References

ACSC (2020). *Cyber Security and Australian Small Businesses*. Retrieved from https://www.cyber.gov.au/acsc/small-and-medium-businesses/small-business-survey-results

Ali, S., Yue, T., & Abreu, R. (2022). When software engineering meets quantum computing. *Communications of the ACM*, *65*(4), 84–88. https://doi.org/10.1145/3512340

Almudever, C. G., Lao, L., Fu, X., Khammassi, N., Ashraf, I., Iorga, D., . . . Bertels, K. (2017). The engineering challenges in quantum computing. In *Proceedings of the 2017 Design, Automation & Test in Europe (DATE): 27-31 March 2017, Swisstech, Lausanne, Switzerland* (pp. 836–845). Piscataway, NJ: IEEE. https://doi.org/10.23919/DATE.2017.7927104

Alyami, H., Nadeem, M., Alosaimi, W., Alharbi, A., Kumar, R., Kumar Gupta, B., . . . Ahmad Khan, R. (2022). Analyzing the Data of Software Security Life-Span: Quantum Computing Era. *Intelligent Automation & Soft Computing*, *31*(2), 707–716. https://doi.org/10.32604/iasc.2022.020780

Amazon (n.d.). Amazon Braket. Retrieved from https://aws.amazon.com/de/braket/

Arute, F., Arya, K., Babbush, R., Bacon, D., Bardin, J. C., Barends, R., . . . Martinis, J. M. (2019). Quantum supremacy using a programmable superconducting processor. *Nature*, *574*(7779), 505–510. https://doi.org/10.1038/s41586-019-1666-5

Ayyagari, M., Beck, T., & Demirguc-Kunt, A. (2007). Small and Medium Enterprises Across the Globe. *Small Business Economics*, *29*(4), 415–434. https://doi.org/10.1007/s11187-006-9002-5

Barbeau, M., & Garcia-Alfaro, J. (2022). Cyber-physical defense in the quantum Era. *Scientific Reports*, *12*(1), 1905. https://doi.org/10.1038/s41598-022-05690-1

Bellovin, S. M. (2011). Frank Miller: Inventor of the One-Time Pad. *Cryptologia*, *35*(3), 203–222. https://doi.org/10.1080/01611194.2011.583711

Bernstein, D. J., Buchmann, J., & Dahmen, E. (2009). *Post-Quantum Cryptography*. Berlin, Heidelberg: Springer Berlin Heidelberg. https://doi.org/10.1007/978-3-540-88702-7

Bigliardi, B., Colacino, P., & Dormio, A. I. (2011). Innovative Characteristics of Small and Medium Enterprises. *Journal of Technology Management & Innovation*, *6*(2), 83–93. https://doi.org/10.4067/S0718-27242011000200006

Bobier, J.-F., Langione, M., Tao, E., & Gourévitch, A. (2021). *What Happens When 'If' Turns to 'When' in Quantum Computing?* Retrieved from https://www.bcg.com/de-de/publications/2021/building-quantum-advantage

Brassard, G., HØyer, P., & Tapp, A. (1998). Quantum cryptanalysis of hash and claw-free functions. In G. Goos, J. Hartmanis, J. van Leeuwen, C. L. Lucchesi, & A. V. Moura (Eds.), *Lecture Notes in Computer Science. LATIN'98: Theoretical Informatics* (Vol. 1380, pp. 163–169). Berlin, Heidelberg: Springer Berlin Heidelberg. https://doi.org/10.1007/BFb0054319

BSI (2012). *IT-Sicherheitsniveau in kleinen und mittleren Unternehmen*. Berlin: Bundesministerium für Wirtschaft und Technologie.

BSI (2021). *Kryptographie quantensicher gestalten*. Berlin: Bundesamt für Sicherheit in der Informationstechnik. Retrieved from https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Broschueren/Kryptografie-quantensicher-gestalten.pdf?__blob=publicationFile&v=5

Buzek, V. & Hillery, M. (1996). Quantum copying: Beyond the no-cloning theorem. *Physical Review. A, Atomic, Molecular, and Optical Physics*, *54*(3), 1844–1852. https://doi.org/10.1103/PhysRevA.54.1844

Castelvecchi, D. (2022). Preparing for Q-Day. *Nature*, *602*(7896), 198-201.

Chandra, S., Paira, S., Alam, S. S., & Sanyal, G. (2014). A comparative survey of Symmetric and Asymmetric Key Cryptography. In *2014 International Conference on Electronics, Communication and Computational Engineering (ICECCE)* (pp. 83–93). IEEE. https://doi.org/10.1109/ICECCE.2014.7086640

Chung, C.-C., Pai, C.-C., Ching, F.-S., Wang, C., & Chen, L.-J. (2022). When post-quantum cryptography meets the internet of things. In N. Bulusu, E. Aryafar, A. Balasubramanian, & J. Song (Eds.), *Proceedings of the 20th Annual International Conference on Mobile Systems, Applications and Services* (pp. 525–526). New York, NY, USA: ACM. https://doi.org/10.1145/3498361.3538766

Dalzell, A. M., Harrow, A. W., Koh, D. E., & La Placa, R. L. (2020). How many qubits are needed for quantum computational supremacy? *Quantum*, *4*, 264. https://doi.org/10.22331/q-2020-05-11-264

Deshpande, S., Xu, C., Trochatos, T., Ding, Y., & Szefer, J. (2022, March 5). *Towards an Antivirus for Quantum Computers*. Retrieved from http://arxiv.org/pdf/2203.02649v1

Diffie, W., & Hellman, M. (1976). New directions in cryptography. *IEEE Transactions on Information Theory*, *22*(6), 644–654. https://doi.org/10.1109/TIT.1976.1055638

Dreißigacker, A., Skarczinski, B. von, & Wollinger, G. R. (2020). *Cyberangriffe gegen Unternehmen in Deutschland: Ergebnisse einer repräsentativen Unternehmensbefragung 2018/2019*. Forschungsbericht Nr. 152. Hannover: Kriminologisches Forschungsinstitut Niedersachsen e.V.

Dyakonov, M. (2018). The Case Against Quantum Computing. Retrieved from https://spectrum.ieee.org/the-case-against-quantum-computing

Ernst, C., Warnke, M., & Schröter, J. (2020). Der Quantencomputer – ein zukünftiger Gegenstand der Medienwissenschaft? Advance online publication. https://doi.org/10.25969/mediarep/14866

European Commission (2020). *User Guide to the SME Definition*. Luxembourg: Publications Office of the European Union.

Fraunhofer Institute (2018). *Eberbacher Gespräch on "Next Generation Crypto"* (Vol. 1). Fraunhofer. Retrieved from https://www.sit.fraunhofer.de/de/eberbach-crypto/

Gisin, N., Ribordy, G., Tittel, W., & Zbinden, H. (2002). Quantum cryptography. *Reviews of Modern Physics*, *74*(1), 145–195. https://doi.org/10.1103/RevModPhys.74.145

Grover, L. K. (1997). Quantum Mechanics Helps in Searching for a Needle in a Haystack. *Physical Review Letters*, *79*(2), 325–328. https://doi.org/10.1103/PhysRevLett.79.325

Gupta, D. S., Ray, S., Singh, T., & Kumari, M. (2022). Post-quantum lightweight identity-based two-party authenticated key exchange protocol for Internet of Vehicles with probable security. *Computer Communications*, *181*, 69–79. https://doi.org/10.1016/j.comcom.2021.09.031

Gyongyosi, L., & Imre, S. (2019). A Survey on quantum computing technology. *Computer Science Review*, *31*, 51–71. https://doi.org/10.1016/j.cosrev.2018.11.002

Hallgren, S., & Vollmer, U. (2009). Quantum computing. In D. J. Bernstein, J. Buchmann, & E. Dahmen (Eds.), *Post-Quantum Cryptography* (pp. 15–34). Berlin, Heidelberg: Springer Berlin Heidelberg. https://doi.org/10.1007/978-3-540-88702-7_2

Hekkala, J., Halunen, K., & Vallivaara, V. (2022). Implementing Post-quantum Cryptography for Developers. In *Proceedings of the 8th International Conference on Information Systems Security and Privacy* (pp. 73–83). SCITEPRESS - Science and Technology Publications. https://doi.org/10.5220/0010786200003120

Huang, Y., & Martonosi, M. (2019). Statistical assertions for validating patterns and finding bugs in quantum programs. In S. Manne, H. Hunter, & E. Altman (Eds.), *Proceedings of the 46th International Symposium on Computer Architecture* (pp. 541–553). New York, NY, USA: ACM. https://doi.org/10.1145/3307650.3322213

Huh, J., Guerreschi, G. G., Peropadre, B., McClean, J. R., & Aspuru-Guzik, A. (2015). Boson sampling for molecular vibronic spectra. *Nature Photonics*, *9*(9), 615–620. https://doi.org/10.1038/nphoton.2015.153

IBM (n.d.). IBM Quantum System One. Retrieved from https://research.ibm.com/interactive/system-one/

IfM Bonn (2021a). Unternehmensbestand: KMU insgesamt. Retrieved from https://www.ifm-bonn.org/statistiken/unternehmensbestand/kmu-insgesamt/deutschland

IfM Bonn (2021b). KMU-Definition des IfM Bonn seit 01.01.2016. Retrieved from https://www.ifm-bonn.org/definitionen-/kmu-definition-des-ifm-bonn

Ihlau, S., & Duscha, H. (2019). *Besonderheiten bei der Bewertung von KMU*. Wiesbaden: Springer Fachmedien Wiesbaden. https://doi.org/10.1007/978-3-658-18675-3

Johnson, D. (2021). *Post-quantum cryptographic standards to be finalized later this year*. Retrieved from https://www.scmagazine.com/news/data-security/post-quantum-cryptographic-standards-to-be-finalized-later-this-year

Joseph, D., Misoczki, R., Manzano, M., Tricot, J., Pinuaga, F. D., Lacombe, O., . . . Hansen, R. (2022). Transitioning organizations to post-quantum cryptography. *Nature*, *605*(7909), 237–243. https://doi.org/10.1038/s41586-022-04623-2

Kelly, J. (2018). *A Preview of Bristlecone, Google's New Quantum Processor*. Retrieved from https://ai.googleblog.com/2018/03/a-preview-of-bristlecone-googles-new.html

Lindsay, J. R. (2022). Quantum computing and classical politics. In M. D. Cavelty & A. Wenger (Eds.), *Cyber Security Politics* (pp. 80–94). London: Routledge. https://doi.org/10.4324/9781003110224-7

Mailloux, L. O., Lewis II, C. D., Riggs, C., & Grimaila, M. R. (2016). Post-Quantum Cryptography: What Advancements in Quantum Computing Mean for IT Professionals. *IT Professional*, *18*(5), 42–47. https://doi.org/10.1109/MITP.2016.77

Mavroeidis, V., Vishi, K., D., M., & Jøsang, A. (2018). The Impact of Quantum Computing on Present Cryptography. *International Journal of Advanced Computer Science and Applications*, *9*(3). https://doi.org/10.14569/IJACSA.2018.090354

Meier, C. (2019). *Hybridcomputer rechnet schneller*. Retrieved from https://www.spektrum.de/magazin/hybrid-aus-quantensimulator-und-pc/1675672

Microsoft (n.d.). Azure Quantum. Retrieved from https://azure.microsoft.com/de-de/services/quantum/#product-overview

Mohr, N., Ostojic, I., Heid, A., Pautasso, L., & Biondi, M. (2021). Die wundersame Welt der Quantencomputer: ein Wegweiser. *Digitale Welt*, *5*(2), 6–9. https://doi.org/10.1007/s42354-021-0328-6

Murer, G. (2021). *Eine Reise durch die Quantenwelt*. Berlin, Heidelberg: Springer Berlin Heidelberg. https://doi.org/10.1007/978-3-662-63269-7

NIST (2022). *NIST Announces First Four Quantum-Resistant Cryptographic Algorithms.* Retrieved from https://www.nist.gov/news-events/news/2022/07/nist-announces-first-four-quantum-resistant-cryptographic-algorithms

OECD (2019). *SME and Entrepreneurship Outlook 2019*. OECD. https://doi.org/10.1787/34907e9c-en

Paltenghi, M., & Pradel, M. (2022). Bugs in Quantum computing platforms: an empirical study. *Proceedings of the ACM on Programming Languages*, *6*(OOPSLA1), 1–27. https://doi.org/10.1145/3527330

Pawlowska, A., & Scherer, B. (2020). *IT-Sicherheit im Home-Office*. Berlin: BSI. Retrieved from https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Cyber-Sicherheitslage/Lageberichte/Cyber-Sicherheitsumfrage/IT-Sicherheit_im_Home-Office/it-sicherheit_im_home-office_node.html

Preskill, J. (2019). *Why I Called It 'Quantum Supremacy'*. Retrieved from https://www.quantamagazine.org/john-preskill-explains-quantum-supremacy-20191002/

Schöffel, M., Lauer, F., Rheinländer, C. C., & Wehn, N. (2022). Secure IoT in the Era of Quantum Computers-Where Are the Bottlenecks? *Sensors (Basel, Switzerland)*, *22*(7). https://doi.org/10.3390/s22072484

Schuld, M., Brádler, K., Israel, R., Su, D., & Gupt, B. (2020). Measuring the similarity of graphs with a Gaussian boson sampler. *Physical Review a*, *101*(3). https://doi.org/10.1103/PhysRevA.101.032314

Shor, P. W. (1994). Algorithms for quantum computation: discrete logarithms and factoring. In *Proceedings 35th Annual Symposium on Foundations of Computer Science* (pp. 124–134). IEEE Comput. Soc. Press. https://doi.org/10.1109/SFCS.1994.365700

Statistisches Bundesamt (2021). *Anteile Kleine und Mittlere Unternehmen 2019 nach Größenklassen in %.* Retrieved from https://www.destatis.de/DE/Themen/Branchen-Unternehmen/Unternehmen/Kleine-Unternehmen-Mittlere-Unternehmen/Tabellen/wirtschaftsabschnitte-insgesamt.html

Steane, A. M. (1998). Space, Time, Parallelism and Noise Requirements for Reliable Quantum Computing. *Fortschritte Der Physik*, *46*(4-5), 443–457. https://doi.org/10.1002/(SICI)1521-3978(199806)46:4/5%3C443::AID-PROP443%3E3.0.CO;2-8

Strohm, T. (2021). QC aus Anwendersicht. *Digitale Welt*, *5*(2), 52–53. https://doi.org/10.1007/s42354-021-0337-5

Taege, P. (2021). *Es steht so mittel: Mittelstand und IT-Sicherheit.* Retrieved from https://research.hisolutions.com/2021/01/warum-der-mittelstand-besonders-auf-it-sicherheit-achten-sollte/

Ukwuoma, H. C., Arome, G., Thompson, A., & Alese, B. K. (2022). Post-quantum cryptography-driven security framework for cloud computing. *Open Computer Science*, *12*(1), 142–153. https://doi.org/10.1515/comp-2022-0235

Van Meter, R., & Oskin, M. (2006). Architectural implications of quantum computing technologies. *ACM Journal on Emerging Technologies in Computing Systems*, *2*(1), 31–63. https://doi.org/10.1145/1126257.1126259

Wallden, P., & Kashefi, E. (2019). Cyber security in the quantum era. *Communications of the ACM*, *62*(4), 120. https://doi.org/10.1145/3241037

Wang, X., Arcaini, P., Yue, T., & Ali, S. (2022). Generating failing test suites for quantum programs with search (hot off the press track at GECCO 2022). In J. E. Fieldsend & M. Wagner (Eds.), *Proceedings of the Genetic and Evolutionary Computation Conference Companion* (pp. 47–48). New York, NY, USA: ACM. https://doi.org/10.1145/3520304.3534067

Williams, C. P., & Clearwater, S. H. (2000). Swatting Quantum Bugs. In C. P. Williams & S. H. Clearwater (Eds.), *Ultimate Zero and One* (pp. 173–190). New York, NY: Springer New York. https://doi.org/10.1007/978-1-4612-0495-4_8

Wittkopp, D. (2021). Ein Quantencomputer mit 1121 Qubits. *Digitale Welt*, *5*(2), 65–69. https://doi.org/10.1007/s42354-021-0340-x

Zhong, H.-S., Wang, H., Deng, Y.-H., Chen, M.-C., Peng, L.-C., Luo, Y.-H., . . . Pan, J.-W. (2020). Quantum computational advantage using photons. *Science (New York, N.Y.)*, *370*(6523), 1460–1463. https://doi.org/10.1126/science.abe8770