BLED 2021 Proceedings

BLED Proceedings

2021

Quantum Computer Resistant Cryptographic Methods and Their Suitability for Long-Term Preservation of Evidential Value

Christian Thiel

Cristoph Thiel

Quantum Computer Resistant Cryptographic Methods and Their Suitability for Long-Term Preservation of Evidential Value

Thiel Christian[1] & Thiel Christoph[2]

[1] OST Ostschweizer Fachhochschule, School of Management, Rosenbergstrasse 59, Postfach, 9001 St.Gallen, Switzerland; e-mail: christian.thiel@ost.ch
[2] FH Bielefeld University of Applied Sciences, Faculty of Minden Campus, 32427 Minden, Germany; e-mail: christoph.thiel@fh-bielefeld.de

Abstract In the areas of electronic identification and electronic trust services, the Regulation No. 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC (eIDAS) creates uniform regulations for electronic signatures, seals, time stamps, registered mail and website certificates in the European single market. All developments that affect the security of signature procedures have an impact. In this study, we consider the candidates for quantum computer-resistant asymmetric cryptographic (PQC) methods currently under investigation in international research and standardization and evaluate their suitability for PKI systems with a focus on long-term preservation of evidential value, as is the case in particular with eIDAS-compliant signature solutions. Based on an evaluation system proposed by us - an adaptation of the system from [2] - we compare the application requirements with the properties of the candidates and recommend suitable methods.

Keywords: post-quantum cryptography, feasibility study, eIDAS-compliant signature solutions, use cases

University of Maribor Press

DOI https://doi.org/10.18690/978-961-286-485-9.35
ISBN 978-961-286-485-9

1 Introduction

This study focuses on quantum computer-resistant crypto methods, also called post-quantum cryptography (PQC) after J.D. Bernstein (in particular in asymmetric methods). It is not comprehensive and does not list every quantum computer-resistant asymmetric method ever proposed. Instead, it lists a representative sample (as of End 2020) of cryptographic techniques that are being discussed in academia, are supported by currently active research teams, may be viable for real-world applications, and are therefore suitable candidates for consideration by various standardization organizations for standardization. Beyond NIST's PQC standardization, we also consider extensions of classical algorithms as well as quantum-assisted algorithms (i.e., the use of quantum technology to augment classical systems, see also [10]) with respect to the possibility of providing sufficient quantum computing resistance.

2 Overview of the procedures

In this study, we define PQC methods as cryptographic methods (in particular asymmetric cryptographic methods) which, according to the current state of research, can possibly provide sufficient security against attacks that use the capabilities and properties of quantum computers, i.e. are "quantum computer resistant". In this context, the procedures themselves do not use any support from quantum computers for preparation and execution.

The underlying principle of continuing to use the previously employed public-key methods such as RSA and ECDSA (Elliptic Curve Digital Signature Algorithm) with significantly larger keys than is currently customary in the post-quantum era is obvious at first glance. On the one hand, the approach of increasing the key sizes of RSA and ECDSA to cope with ever-improving cryptanalysis and newly discovered attacks is already a tradition (see, e.g., evolution of NIST's SP 800-57 Part 1[11]). In the context of quantum computers, this principle would very quickly lead to large and unwieldy key sizes that corresponding keys might not be usable in practice:

Quantum computers are based on the concept of qubits (quantum bit), where each qubit exists simultaneously as a superposition (superposition or also called coherence) of the states 1 and 0 and all those in between. The number of qubits needed on a quantum computer to break RSA[1] is estimated to be 2n+3 [12] and 2n+2 [13], which means that a quantum computer with about 4,000 qubits is needed to break an RSA-2048 signature (further algorithm optimizations are expected, so the actual number of qubits needed is expected to be lower). Shor's QFT algorithm can also be adapted to solve the discrete logarithm problem. The number of qubits to break ECDSA is "approximately" 6n [6]. This means that a quantum computer with about 1,500 qubits can break an ECC-P256 signature. Following the assumption of Neven's law [14] (the quantum equivalent of Moore's law), one can estimate that the computational power of quantum computers increases at a "double exponential rate" compared to classical computers.

If we start with 100 qubits in a given year and double the qubits every 18 months, 9 years later we will probably have computers with over 6000 qubits and in 32 years we will be able to break a 1-million-bit RSA key. Post-qubit RSA (i.e., RSA with such large key lengths) was studied by Bernstein [15], who showed the technical feasibility of implementing a terabit key using 231 4096-bit primes as factors. At these key sizes, each RSA operation amounted to tens or hundreds of hours. In practice, such a system can thus probably be ruled out. It should be noted, incidentally, that post-quantum RSA was in Round 1 of the NIST PQC competition but was not selected for Round 2.

Currently, it is unclear how many qubits the most powerful quantum computers have at the time of writing. The company IQM FINLAND OY is to build a quantum computer which is to have 50-qubits by the end of the third phase in 2024 ([36]). Google LLC, IBM, and others have developed machines with about 50 or more high-quality qubits (see [34], [35]). IBM is planning (even faster than Neven's law would suggest) more quantum computers with 127 qubits in 2021, 433 qubits in 2022, and over 1000 qubits in 2023 [35].

[1] i.e. breaking any private key

If IBM's development speed remains the same, we could expect the above-mentioned 6000 qubits to be reached around 2026 to 2027. Even with somewhat slower developments, one must assume that this will be the case from the year 2030. Although attacks against symmetric cryptosystems using quantum computers and algorithms by Grover or Simon (see [3] and [4]) are more effective than attacks using conventional computers, it is currently assumed that doubling the effective key length cancels out this advantage of quantum computers. Thus, for example, AES256 would be about as secure against a quantum computer as AES128 is against conventional computers.

Assuming the availability of sufficiently powerful quantum computers in the near future, it is obvious to use them not only as a tool to attack classical crypto methods, but also to investigate how quantum computer-resistant crypto methods could be realized with their help. The use of quantum computers to perform certain cryptographic operations is called quantum cryptography. Corresponding operations typically exploit the quantum properties of superposition, interference, and entanglement, which are not reproducible by classical computers. Quantum-enhanced security [17] is then understood to be the extension of classical non-quantum systems that make use of or are augmented by quantum technology to improve their ability to secure their data and transactions against adversaries that may be fully quantum capable.

While quantum key distribution (QKD) (see [18], [19]) is often equated with (general) quantum cryptography, QKD is based on the Vernam one-time pad and is therefore more suitable only for key exchange and encryption. Quantum researchers have introduced several quantum digital signature schemes (see [20] - [22]), but since they typically refer to QKD, they would be better referred to as data authentication schemes. As of this writing, we are unable to identify any quantum digital signature schemes in the literature that actually have the necessary constructs of a digital signature scheme and are EUF-CMA secure (existentially unforgeable under chosen message attack), let alone post-quantum secure.

Based on the above considerations classic cryptographic methods such as RSA and ECDSA with very large keys are ruled out (in the medium term) and can at best be used for a short transition phase (i.e., for the next 9 years at most). Signatures generally have a rather short lifetime and in principle only need to be secure up to the time of their verification. If a signature procedure can be broken by a quantum computer in the future, today's signature certificates will probably already have expired. Only in the case of very long validity periods for signature keys should caution already be exercised. According to the current state of research, quantum-enhanced processes do not (yet) play a role specifically for electronic signatures. In the medium and long term, therefore, the focus should be on PQC processes.

3 Parameterized evaluation of PQC methods and applications

The objective of this study is not to replicate NIST's research in the NIST PQC competition (see [23], [24])., but to build on it and make it more concrete in order to find a basis for assessing the concrete practical applicability of a procedure in building blocks of e-business applications. In doing so, we extend the evaluation scheme from [2]. We define the three value ranges Small (S), Medium (M), and Large (L) for different parameters of the procedures, respectively. Specifically, we consider the following parameters.

- Key Generation Resources (KeyGen() Resources)
- Key sizes of the public and private keys
- Key Lifetime: Certain signature processes only allow the private signature key to be used for a limited number of signature creations. We record this using the "key lifetime".
- Resources for signature creation (Sign() resources) or encryption (Crypt() resources).
- Size of a signature (Signature Size) or size of a ciphertext (Cipher Size)
- Time for the creation of a signature (Signature Time) or the creation of a ciphertext (Crypt Time)
- Resources for signature verification (Ver() resources) or decryption (Decrypt() resources).

The parameters are categorized as follows in table 2 (assuming a single core of a current Intel I7 processor for mobile devices running at 3.2 Ghz, as in [2] and [25]):

Table 2: Parameters and their categories for evaluating the practical usability of PQC methods in applications

	Small (Optimal)	**Medium**	**Large**
KeyGen() Resources	can be executed on a chip card. (< 3M cycles)	executable on a terminal/mobile phone (< 30 M cycles)	Requires operation on a powerful laptop (> 30 M cycles)
Sign() Resources			
Crypt() Resources			
Ver() Resources			
Decrypt() Resources			
Key Size	< 2Kbits (e.g. ECC-P256)	< 2Kbytes (e.g. RSA-8192)	> 2Kbytes
Signature Size			
Cipher Size			
Key Lifetime	< 1000 signatures per key	< 10000000 signatures per key	unlimited
Signature Time	< 1ms per signature	< 100ms per signature	> 100ms per signature
Crypt Time	< 1ms per encryption	< 100ms per encryption	> 100ms per encryption

In order to evaluate the suitability of different PQC methods for concrete applications, we first look at the applications from the ETSI (see [26]) and now use the parameters described above as the requirements of the applications for a PQC procedure to be deployed (the parameters are therefore no longer descriptive in nature but have a requirement character). Of course, there are other use cases for asymmetric (signature) procedures, but the selection considered covers common scenarios from the areas of finance (for business), infrastructure (for people and devices), cloud & Internet (for business-to-business, business-to-consumer, peer-to-peer, and Internet-of-Things interactions), and enterprise (for companies). Based on [2] and [26], the following picture emerges in Table 3.

Table 3: Parameter evaluation of typical use cases of asymmetric signature solutions

	KeyGen() Resource	Private Key Size	Public Key Size	Key Lifetime	Sign() Resource	Signature Size	Signature Time	Ver() Resource
3SKey	S	M	M	M	S	M	M	L
EMVSDA	L	L	S	L	L	S	L	M
EMVDDA	S	S	S	M	S	S	S	M
CA Key [2]	L	L	M	M	L	L	L	M
ICAO 9303	L	L	S	S	L	S	L	M
GSM eSIM	L	S	M	S	S	M	M	S
TLS server	L	L	L	L	L	L	S	M
TLS client	M	L	L	L	M	L	M	L
Bitcoin M	L	L	L	M	M	M	M	L
FIDO [3]	M	L	L	M	M	L	M	L
USB signature token [4]	M	L	L	M	M	L	M	L
PGP/ SMIME	M	L	L	L	M	L	M	M
PAdES / AES [5]	L	L	M	L	L	M	M	M
QES [6]	S	M	M	M	S	M	M	M
Code Sign	L	L	L	M	L	L	L	M

4 Status of standardization

To facilitate the development of new quantum computer-resistant and practical methods, the National Institute of Standards and Technology (NIST) initiated a standardization process in 2016 (see [7]). After an evaluation and selection process based on public feedback and internal review by NIST, those methods were identified to move to the third round of review as finalists [16]: The encryption and key agreement/transmission methods are Classic McEliece [30], CRYSTALS-

[2] Simplified consideration for qualified trust service providers

[3] We consider FIDO and other tokens with comparable computational power and memory for strong authentication

[4] Here we consider signature tokens that are more powerful than common smart cards.

[5] advanced electronic signatures when using a document server with HSM to sign documents

[6] qualified electronic signatures when using a signature creation device such as a smart card or USB token

KYBER [31]], NTRU [32], [33] and SABER [25]. The finalists for digital signatures are CRYSTALS-DILITHIUM [27], FALCON [28] and Rainbow [29].

A special feature are so-called stateful hash-based signatures, a special class of signature schemes with certain restrictions, from which currently XMSS (eXtended Merkle Signature Scheme) [8] and LMS (Leighton-Micali Signatures) [9] are in the process of standardization at the Internet Engineering Task Force (IETF) and at NIST, so that standards can be expected earlier than in the above-mentioned PQC process at NIST. The use cases mentioned are code signing and issuing PKI root certificates from certification authorities.

The standardization organizations ETSI and ISO are also involved in PQC standardization with their own working groups. At present, however, it looks as if ETSI and ISO will rely on NIST for the initial selection of procedures. At the moment it seems rather unlikely that other fundamentally new procedures not yet considered by NIST will emerge as part of the (international) standardization effort. In this study, we therefore restrict ourselves to the above mentioned candidates and go on to investigate their suitability for e-business applications.

5 Evaluation of the procedures

We apply the parameter description introduced in Section 3 to the procedures listed above. According to [2], we obtain the following parameter profiles for the current favorites of the NIST and IETF standardization of PQC signature methods in Table 4:

Table 4: Parameter profiles for PQC signature methods

	CRYSTALS-DILITHIUM	FALCON	Rainbow	XMSS	LMS
KeyGen() resource	S	M	L	L	L
Private Key Size	L	M	L	S	S
Public Key Size	M	M	L	M	S
Key Lifetime	L	L	L	M	M
Sign() resource	M	S	S	M	S
Signature Size	M	S	S	M	M
Signature Time	S	S	S	M	S
Ver() Resources	S	S	S	S	S

For encryption methods and key exchange or key transport (KEM) methods, we combine the results from [38, Table 3] with the evaluation method from [2] and obtain the following parameter profiles for the current favorites of NIST's standardization in Table 5:

Table 5: Parameter profiles for PQC encryption methods and key exchange/key transport methods

	Classic McEliece	CRYSTAL-KYBER	NTRU	SABER
KeyGen() resource	S	L	L	L
Private Key Size	L	S	L	S
Public Key Size	M	S	L	M
Crypt() resource	M	S	S	M
Cipher Size	M	S	S	M
Crypt Time	S	S	S	M
Decrypt() resources	S	S	S	S

If we contrast the parameterization of the procedures with the parameterization of the applications from Table 3, we can derive an evaluation scheme as in [2] based on a point assignment for the suitability of the procedures for the respective application. The basis of scoring is as follows: If the procedure provides a score for a single parameter that is equal to or better than what the application provides, then the score remains unchanged. If the procedure for a parameter is worse by a range (e.g. M instead of S) than what the application allows, then 1 is subtracted from the score for each such parameter[7]. If there is a parameter for which the procedure is two ranges worse (e.g., L instead of S) than what the application allows, then we consider the procedure to be not fit (NF = not fit). For quantitative purposes, we assign a score of -100 for each NF. Then the individual ratings of the parameters are summed up. The most suitable procedures can now be found for each application. A score of zero means that no changes are required and the process can most likely be used for the application. A negative score means that the procedure is not completely suitable, but that optimizations for the procedure may need to be found. After zero, the algorithm with the highest score (i.e., with the lowest negative score)

[7] For each individual parameter, the context determines whether a larger or smaller value is better. For example, a larger memory requirement is worse, but a longer lifetime of a key may be better.

is the next most suitable, as it requires the least number of changes to be used by the application.

Table 6: Selection of suitable processes per application

	CRYSTALS-DILITHIUM	**FALCON**	**Rainbow**	**XMSS**	**LMS**
3SKey	-2	**-1**	NF	NF	NF
EMV-SDA	-2	**-1**	NF	-2	-2
EMV DDA	NF	**-3**	NF	NF	NF
CA Key	**0**	**0**	-1	**0**	**0**
ICAO 9303	-2	**-1**	NF	-2	**-1**
GSM eSIM	NF	-1	NF	-1	**0**
TLS server	**0**	**0**	**0**	-2	-1
TLS Client	**0**	**0**	-1	-2	-2
Bitcoin	**0**	**0**	-1	-2	-2
FIDO	**0**	**0**	-1	-1	-1
USB signature	**0**	**0**	-1	-1	-1
PGP	**0**	**0**	-1	-2	-2
PDF-AES [8]	**0**	**0**	-1	-1	-1
PDF QES [9]	-2	**-1**	NF	NF	NF
Code sign	**0**	**0**	**0**	**0**	**0**
Points	**-208**	**-8**	**-606**	**-315**	**-312**

As a result no PQC method currently considered is suitable for all mentioned use cases in Table 3 (in particular for replacing RSA and EC in all use cases). For various use cases, such as for root CA keys, for code signing or for applications where signature creation and verification are performed on a powerful PC, the PQC procedures currently considered in the NIST standardization can be used. This also applies, with minor restrictions, to the use of tokens that are more powerful than "usual" smart cards such as signature cards. However, it becomes critical if the procedure is to be executed on hardware with limited computing power, such as a smart card. Thus, there are at least approaches for a first solution in the eIDAS context if not a completely satisfactory answer to the upcoming developments.

[8] when using a document server with HSM for signing documents

[9] when using a signature creation device such as a smartcard or USB token

6 Recommendations

Post-quantum cryptography will become the standard in the long term [1]. Consideration should be given at an early stage, as part of a measured risk management process, as to whether and when a switch to quantum computing resistant methods should be made (depending on the application) [1]. Especially in connection with signatures with a medium validity period of the certificates (3-5 years), there is no need to rush. For cryptographic applications that process information with long secrecy periods and high protection requirements, however, there may already be a need for action now [1]. The danger here is that messages for key negotiation and the data encrypted with the negotiated keys are collected in advance and decrypted in the future with the aid of a quantum computer ("store now, decrypt later"). Caution is also required with very long validity periods for signature keys. It is therefore already necessary to discuss how a migration to post-quantum cryptography to a Fully Quantum Safe Cryptographic State (FQSCS) for e-business applications can be initiated today.

References

Migration zu Post-Quanten-Kryptografie, Handlungsempfehlungen des BSI, August 2020

Teik Guan Tan und Jianying Zhou, "A Survey of Digital Signing in the Post Quantum Era", Cryptology ePrint Archive, Report 2019/1374, 2019, https://eprint.iacr.org/2019/1374

L. K. Grover, "Quantum mechanics helps in searching for a needle in a haystack," Physical review letters, vol. 79, no. 2, p. 325, 1997.

Simon, D.R. (1994), "On the power of quantum computation", Foundations of Computer Science, 1994 Proceedings., 35th Annual Symposium on: 116–123, retrieved 2011-06-06

D. J. Bernstein, "Comparing proofs of security for lattice-based encryption", Second PQC Standardization Conference, Cryptol. ePrint Arch., 2019, https://eprint.iacr.org/2019/691

Announcing Request for Nominations for Public-Key Post-Quantum Cryptographic Algorithms", 81 Federal Register 92787 (December 20, 2016), pp. 92787
92788. https://federalregister.gov/d/2016-30615

A. Hülsing, D. Butin, S. Gazdag, J. Rijneveld, and A. Mohaisen, "XMSS: eXtended Merkle signature scheme," Available Online: https://tools.ietf.org/html/rfc8391, 2018 [last accessed: September 2020].

F. T. Leighton and S. Micali, "Large provably fast and secure digital signature schemes based on secure hash functions," 1995, uS Patent 5,432,852.

P. Wallden and E. Kashefi, "Cyber security in the quantum era", Commun. ACM, vol. 62, no. 4, p. 120, 2019.

E. Barker, "SP 800-57 part 1 rev. 4 recommendation for key management part 1: General," NIST special publication, vol. 800, p. 57, 2016.

Y. Takahashi and N. Kunihiro, "A quantum circuit for shor's factoring algorithm using 2n+2 qubits," Quantum Information & Computation, vol. 6, no. 2, pp. 184–192, 2006.

S. Beauregard, “Circuit for shor’s algorithm using 2n+3 qubits,” arXiv preprint quant-ph/0205095, 2002.

K. Hartnett, “A new law to describe quantum computing’s rise?” Available Online: https://www.quantamagazine.org/does-nevens-lawdescribe-quantum-computings-rise-20190618/, 2019 [last accessed: September 2020].

D. J. Bernstein, N. Heninger, P. Lou, and L. Valenta, “Post-quantum RSA,” in International Workshop on Post-Quantum Cryptography. Springer, 2017, pp. 311–329.

Moody, D. , Alagic, G. , Apon, D. , Cooper, D. , Dang, Q. , Kelsey, J. , Liu, Y. , Miller, C. , Peralta, R. , Perlner, R. , Robinson, A. , Smith-Tone, D. and Alperin-Sheriff, J. (2020), Status Report on the Second Round of the NIST Post-Quantum Cryptography Standardization Process, NISTIR, National Institute of Standards and Technology, Gaithersburg, MD, [online], https://doi.org/10.6028/NIST.IR.8309

P. Wallden and E. Kashefi, “Cyber security in the quantum era”, Commun. ACM, vol. 62, no. 4, p. 120, 2019.

C. H. Bennett and G. Brassard, “Quantum cryptography: public key distribution and coin tossing,” Theor. Comput. Sci., vol. 560, no. 12, pp. 7–11, 2014.

A. K. Ekert, “Quantum cryptography based on bell’s theorem”, Physical review letters, vol. 67, no. 6, p. 661, 1991.

D. Gottesman and I. Chuang, “Quantum digital signatures,” arXiv preprint quant-ph/0105032, 2001.

M.-Q. Wang, X. Wang, and T. Zhan, “An efficient quantum digital signature for classical messages,” Quantum Information Processing, vol. 17, no. 10, p. 275, 2018.

W. Li, R. Shi, and Y. Guo, “Blind quantum signature with blind quantum computation,” International Journal of Theoretical Physics, vol. 56, no. 4, pp. 1108–1115, 2017.

NIST, “Submission Requirements and Evaluation Criteria for the Post-Quantum Cryptography Standardization Process,” Available Online: https://csrc.nist.gov/CSRC/media/Projects/Post-Quantum- Cryptography/documents/call-for-proposals-final-dec-2016.pdf, 2016 [last accessed: September 2020].

“Post-Quantum Cryptography Round 2 Submissions,” Available Online: https://csrc.nist.gov/Projects/Post-Quantum- Cryptography/Round-2-Submissions, 2019 [last accessed: September 2020].

“Saber: Module-LWR based key exchange, CPA-secure encryption and CCA-secure KEM”, Available Online: https://eprint.iacr.org/2018/230.pdf, 2018 [last accessed: September 2020].

ETSI, “Quantum safe cryptography; case studies and deployment scenarios etsi gr qsc 003 v1.1.1,” Available Online: https://www.etsi.org/deliver/etsi gr/QSC/001 099/003/01.01.01 60/ gr QSC003v010101p.pdf, 2017 [last accessed: September 2020].

Ducas, L., Kiltz, E., Lepoint, T., Lyubashevsky, V., Schwabe, P., Seiler, G., and D. Stehle, “Crystals-dilithium: A lattice-based digital signature scheme”, IACR Cryptology ePrint Archive , 2017, https://eprint.iacr.org/2017/633

Fouque, P-A., Hoffstein, J., Kirchner, P., Lyubashevsky, V., Pornin, T., Prest, T., Ricosset, T., Seiler, G., Whyte, W., and Z. Zhang, “Falcon: Fast-Fourier lattice- based compact signatures over NTRU”, IACR Cryptology ePrint Archive , 2018, https://falcon-sign.info/

Ding, J. and D. Schmidt, “Rainbow, a New Multivariable Polynomial Signature Scheme”, 2005, https://link.springer.com/chapter/10.1007/11496137_12

McEliece R (1978) A public-key cryptosystem based on algebraic coding theory. The Deep Space Network Progress Report, DSN PR 42-44. NASA. Available at https://tmo.jpl.nasa.gov/progress_report2/42-44/44N.PDF

CRYSTALS-Kyber (version 2.0) – Submission to round 2 of the NIST post-quantum project. Roberto Avanzi, Joppe Bos, Léo Ducas, Eike Kiltz, Tancrède Lepoint, Vadim Lyubashevsky, John M. Schanck, Peter Schwabe, Gregor Seiler, and Damien Stehlé. Specification document ,2019, Available at https://pq-crystals.org/kyber/data/kyber-specification-round2.pdf [last accessed: September 2020].

Institute of Electrical and Electronics Engineers (2009) IEEE Standard 1363.1-2008 - Specification for Public Key Cryptographic Techniques Based on Hard Problems over Lattices (IEEE, Piscataway, New Jersey, United States). https://doi.org/10.1109/IEEESTD.2009.4800404

American National Standards Institute (2010) ANSI X9.98-2010 -Lattice-Based Polynomial Public Key Establishment Algorithm for the Financial Services Industry (ANSI, New York City, United States). Available at https://webstore.ansi.org/standards/ascx9/ansix9982010r2017

Arute, F., Arya, K., Babbush, R. et al.: Quantum supremacy using a programmable superconducting processor. Nature 574, 505–510 (2019). https://doi.org/10.1038/s41586-019-1666-5

Gambetta, J.: „IBM's Roadmap For Scaling Quantum Technolog, IBM Research", IBM Research Blog, September 15, 2020, https://www.ibm.com/blogs/research/2020/09/ibm-quantum roadmap/, [last accessed: November 2020].

Finland selects IQM to build its first quantum computer; to deliver a 50-qubit machine by 2024., November 2020,https://www.meetiqm.com/articles/press-releases/finland-selects-iqm-to-build-its-first-quantum-computer-to-deliver-a-50-qubit-machine-by-2024, [last accessed: November 2020].