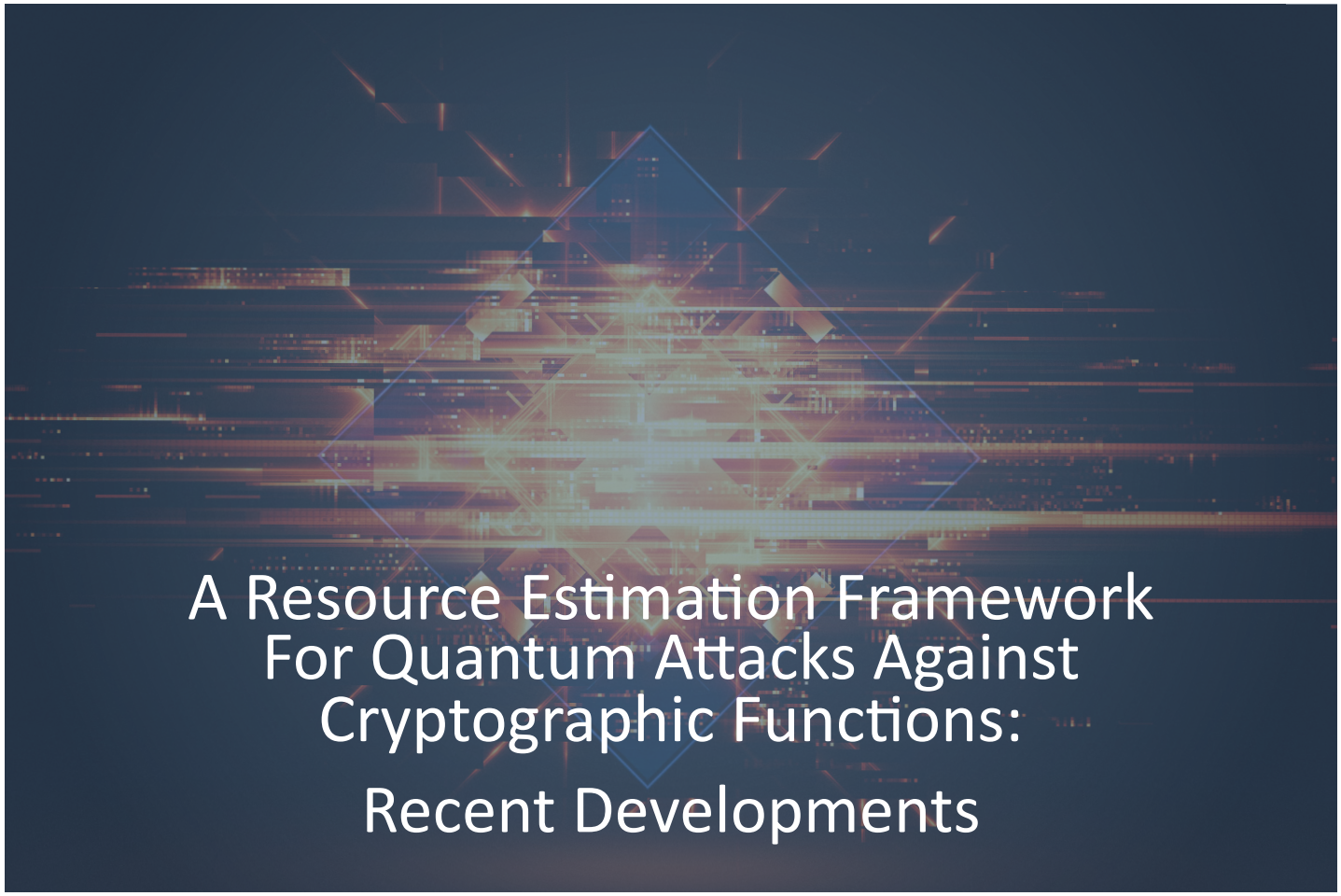
Global Risk Institute

FINAL REPORT



A Resource Estimation Framework For Quantum Attacks Against Cryptographic Functions: Recent Developments

Authors: Dr. Vlad Gheorghiu
evolutionQ Inc.

Dr. Michele Mosca
evolutionQ Inc.

March 2021

ABOUT THIS REPORT:

Cryptography fundamentally impacts every aspect of human life. It underpins the security and availability of systems upon which we rely deeply. These include communication systems, digital identity, internet of things, financial systems, and so on. Today's cryptographic algorithms fall into three categories: public key (asymmetric) systems, private key (symmetric) systems, and cryptographic hash functions. Public key systems are used to establish secret keys between two remote participants that are only allowed to communicate over a public channel (i.e., a channel that can be listened to). Public key cryptography is also used to establish digital signature systems for authenticating the origin and integrity of information. Encryption algorithms, or ciphers (an instance of symmetric key systems) assume that a secret key is already shared between the participants (via, for example, the use of a public key scheme), and are used for fast encryption and decryption of data using the shared secret key. Finally, cryptographic hash functions are so called "one-way functions" from which one cannot efficiently recover the input by looking at the output- a main ingredient of digital identity schemes such as digital signatures.

Quantum computers offer another means to attack the above schemes. In this study we update our previous security estimates considering new developments in the theory of quantum algorithms, quantum error correction, and quantum circuit optimization. We consider public-key systems such as RSA, as well as the AES family of symmetric ciphers and the SHA hash functions. All those schemes are widely deployed today and are heavily used in most of today's cryptographic infrastructure.

Since our previous report was published in February 2020, experimental and theoretical progress has been incremental, with no significant breakthroughs. Hence, our current estimates do not differ dramatically when compared to our previous report- the most significant developments to be outlined.

evolutionQ

A resource estimation framework for quantum attacks against cryptographic functions - recent developments

GRI quantum risk assessment report Feb. 2021

Dr. Vlad Gheorghiu and Dr. Michele Mosca

evolutionQ Inc., Kitchener ON, Canada

February 15, 2021

Abstract. We update our security estimates against quantum adversaries of currently deployed asymmetric (public-key) cryptographic schemes that comprise of the RSA family, as well as symmetric schemes (ciphers) that include the AES family, and cryptographic hash functions that include the SHA-256 and SHA3 families. We use the latest advances in cryptanalysis, circuit compilation and fault-tolerant theory when providing the updated estimates. In addition to our previous report from Feb. 2020, we also explore a novel approach to attacking symmetric cryptographic schemes, and justify why its cryptanalytic impact is negligible.

1 Introduction and methodology

Quantum computers represent a systemic risk to currently deployed cryptographic systems, weakening symmetric cryptography and hash functions [1,2] and shattering public-key systems based on factoring large numbers (RSA [3]) or solving discrete logarithms in finite groups (including Elliptic Curve Cryptography (ECC) [4,5]) via Shor's algorithm [6].

As summarized in our previous reports [7,8,9,10,11], the known realistic quantum attacks on cryptographic schemes require full-scale fault-tolerant quantum computers. Although such full-scale machines are not yet available, the risk they pose to cryptography is serious and must be addressed today, due to harvest-and-decrypt-later attacks, and more generally due to the long time required to reliably migrate systems to new cryptography. Moreover, the scientific community overwhelmingly agrees [12,13] that such machines will very likely become reality.

In our previous reports [7,8,9,10,11] we described in detail the "quantum hardware and software stack" that must be analyzed when performing a rigorous estimation of the *quantum security parameter* of the cryptographic schemes believed to be exponentially hard to attack (AES and SHA families), and we

calculated resource estimations for breaking schemes known to be vulnerable to quantum attacks (RSA and ECC families). As before, we consider the fault-tolerant implementations over the surface code [14], as the latter continues to be considered the most promising candidate for fault-tolerance, and we remind the reader that the quantum security parameter is defined as the logarithm base two of the number of fundamental operations (in our case surface code cycles) required to break the scheme. And for the schemes with polynomial time attacks, we calculate more precise resource estimates at the gate level and report space and time requirements (and calculate the overall quantum resources, as described in more detail below).

For the sake of completeness, we depict quantum hardware and software stack again in Fig. 1, and the interested reader can find more details in our previous reports. Fig. 1. We reiterate that any improvement in any of the layers in Fig. 1

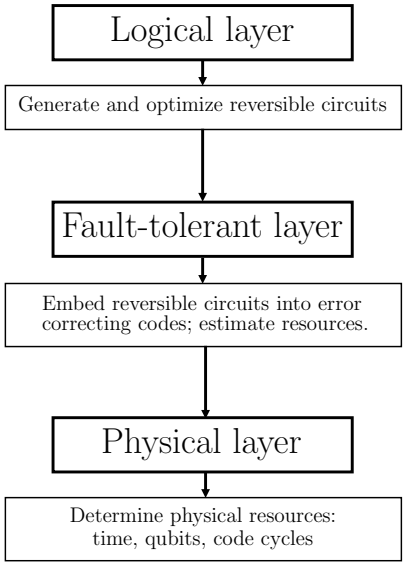


Fig. 1. Analyzing an attack against a cryptographic scheme with a fault-tolerant quantum adversary by considering several layers, going from the most abstract one (the logical layer), to the fault-tolerant layer that implements the circuit in a fault-tolerant way by taking into account that the physical implementation is imperfect, to the underlying physical layer itself.

decreases the resources (space, i.e., number of qubits, or time, or both) needed to break the scheme. Therefore keeping track of the latest developments and advances related to any of those layers is of paramount importance in quantum cryptanalysis.

For today's vulnerable public-key schemes, we represent the *quantum resources* as a single-number quantity that roughly quantifies the product between

the space (total number of physical qubits) occupied by a quantum circuit and the time required to run it (which is proportional to its depth, i.e., the number of non-parallel operations). Note that here is a trade-off between space and time: within the broad range of relevant parameters one can reduce the time required to run a quantum circuit by increasing the number of qubits (parallelization) and vice-versa, while keeping the product between space and time (almost) constant. Therefore the quantum resources can be seen as an "invariant" of the algorithm's implementation, roughly quantifying the efficiency of the implementation of a quantum circuit. In principle, one is free to chose any 'time/number of physical qubits' pairs from the trade-off line, while keeping the quantum resources constant. In this report we represent the quantum resources in units of *megaqubitdays*, i.e., millions of qubits required to break the scheme in 24 hours (1 day).

From the time our previous report [11] was published, the experimental and theoretical progress to any of the layers depicted in Fig. 1 was relatively incremental, with no significant breakthroughs. Hence, our current estimates do not differ dramatically in comparison to our previous report. The most significant progresses are outlined next. For the AES family of ciphers, new developments [15,16] were made at the logical layer, which contributed to a reduced complexity of the quantum oracle used to implement the AES reversibly via Grover's algorithm. For hash functions, again the most significant progress was made again at the logical layer [15], therefore reducing the logical resources required to implement the corresponding oracle in the Grover's searching algorithm. Finally, for public-key cryptography, most progress was related to improving controlled modular adders quantum circuitry [17] for attacking the RSA with Shor's algorithm. A novelty of our report is the analysis of quantum linear solver-based algorithms against symmetric ciphers[1] which highlights how the method is very unlikely to weaken the security of these schemes. The analysis is based on a very recent paper co-authored by an author of this paper [18].

Next, we summarize our main findings and compare our new security estimates with the ones from last year [11], for two physical error rates per gate p_g of 10^{-3} (first-generation fault-tolerant quantum computers) and 10^{-5} (potential future generation fault-tolerant quantum devices), respectively. For RSA public-key schemes we tabulate the number of logical qubits required to break the scheme, the total number of physical qubits, and the corresponding quantum resources (in megaqubitdays), for a physical error rate p_g of 10^{-3} and 10^{-5}, respectively. For symmetric schemes and hash functions, we tabulate their quantum security parameter (in bits), the number of logical qubits required to break the scheme, and the total number of physical qubits. Note that in all tables the number of logical qubits n_ℓ include the logical qubits used by the magic state distillation factories. In addition, we also plot the variation of our estimates of the quantum resources (public-key schemes) and quantum security parameter q_s (symmetric ciphers and hash functions) as a function of time (from Feb. 2018 to the present time), due to improved cryptanalytic techniques.

[1] This attack was mentioned in one of our previous reports [9]

Note that in all our estimates we used a surface code cycle time of 200ns. For this reason, if one wants to compare our running times (or the overall quantum resources) with the ones mentioned in [19], one should multiply our estimates by a factor of 5, as the authors of [19] used a surface code cycle time of 1000ns.

2 Public key cryptographic schemes – RSA

In [17], the authors present an optimized quantum adder that requires $4n + 2$ logical qubits, which, in comparison with previous ones, achieves a significant reduction (up to 20%) in the number of T gates[2]. Combining the construction of [17] with the current state-of-the-art methods in quantum circuitry [19] and fault-tolerance [20] give rise to the results summarized in the following subsections.

Note that as we mentioned in our previous reports, there is a trade-off between the total number of physical qubits required to break the scheme and the estimated time required to complete the attack. To facilitate the direct comparison with the similar work of [19] and with our previous estimates from [11], we fixed the expected time to break the scheme to the values outlined in the tables (or, in other words, we picked a specific point from the space/time trade-off curve). In principle, since the quantum volume is (to high precision) an invariant, we could have chosen an arbitrary value for the time, while modifying the corresponding number of physical qubits accordingly so the quantum resources remain unchanged.

We observe that the new techniques [17] we employ result in a slight increase of the number of logical qubits by a factor of $1.1 \sim 1.4$, but a net decrease of the total quantum resources (product of number of qubits and time) by a larger factor of $3.7 \sim 4.4$ due to the significant reduction of the T-count (number of T gates).

2.1 RSA-1024

RSA-1024	**Old estimates**				**Current estimates**			
p_g	n_ℓ	n_p	quantum resources	time	n_ℓ	n_p	quantum resources	time
10^{-3}	3093	9.62	0.11	0.27	4098	11.06	0.03	0.07
10^{-5}	3093	4.83	0.04	0.21	4098	6.38	0.01	0.05

Table 1. RSA-1024 security estimates. Here n_ℓ denotes the number of logical qubits, n_p denotes the number of physical qubits (in millions), time denotes the expected time (in hours) to break the scheme, and *quantum resources* are expressed in units of megaqubitdays. The corresponding classical security parameter is 80 bits.

[2] The T gates contribute to approximately 90% of the physical footprint of a realistic quantum circuit implemented fault-tolerantly.

2.2 RSA-2048

RSA-2048	**Old estimates**				**Current estimates**			
p_g	n_ℓ	n_p	quantum resources	time	n_ℓ	n_p	quantum resources	time
10^{-3}	6190	19.20	1.17	1.46	8194	22.27	0.27	0.34
10^{-5}	6190	9.66	0.34	0.84	8194	8.70	0.06	0.15

Table 2. RSA-2048 security estimates. Here n_ℓ denotes the number of logical qubits, n_p denotes the number of physical qubits (in millions), time denotes the expected time (in hours) to break the scheme, and *quantum resources* (*quantum resources*) are expressed in units of megaqubitdays. The corresponding classical security parameter is 112 bits.

2.3 RSA-3072

RSA-3072	**Old estimates**				**Current estimates**			
p_g	n_ℓ	n_p	quantum resources	time	n_ℓ	n_p	quantum resources	time
10^{-3}	9288	37.92	4.03	2.55	12290	44.34	0.94	0.59
10^{-5}	9288	14.53	1.14	1.89	12290	19.14	0.30	0.50

Table 3. RSA-3072 security estimates. Here n_ℓ denotes the number of logical qubits, n_p denotes the number of physical qubits (in millions), time denotes the expected time (in hours) to break the scheme, and *quantum resources* are expressed in units of megaqubitdays. The corresponding classical security parameter is 128 bits.

2.4 RSA-4096

RSA-4096	**Old estimates**				**Current estimates**			
p_g	n_ℓ	n_p	quantum resources	time	n_ℓ	n_p	quantum resources	time
10^{-3}	12387	54.62	10.10	4.44	16386	72.07	2.67	1.17
10^{-5}	12387	19.31	2.71	3.37	16386	25.48	0.72	0.90

Table 4. RSA-4096 security estimates. Here n_ℓ denotes the number of logical qubits, n_p denotes the number of physical qubits (in millions), time denotes the expected time (in hours) to break the scheme, and *quantum resources* are expressed in units of megaqubitdays. The corresponding classical security parameter is approximately 156 bits.

2.5 RSA-7680

RSA-7680	**Old estimates**				**Current estimates**			
p_g	n_ℓ	n_p	quantum resources	time	n_ℓ	n_p	quantum resources	time
10^{-3}	23239	92.51	86.5	22.41	30722	122.0	22.88	5.93
10^{-5}	23239	28.40	18.9	15.91	30722	37.49	5.00	4.21

Table 5. RSA-7680 security estimates. Here n_ℓ denotes the number of logical qubits, n_p denotes the number of physical qubits (in millions), time denotes the expected time (in hours) to break the scheme, and *quantum resources* are expressed in units of megaqubitdays. The corresponding classical security parameter is 192 bits.

2.6 RSA-15360

RSA-15360	**Old estimates**				**Current estimates**			
p_g	n_ℓ	n_p	quantum resources	time	n_ℓ	n_p	quantum resources	time
10^{-3}	46508	204.0	821	96.5	61442	242.8	195.0	22.9
10^{-5}	46508	72.51	143	47.5	61442	95.71	37.63	12.5

Table 6. RSA-15360 security estimates. Here n_ℓ denotes the number of logical qubits, n_p denotes the number of physical qubits (in millions), time denotes the expected time (in hours) to break the scheme, and *quantum resources* are expressed in units of megaqubitdays. The corresponding classical security parameter is 256 bits.

2.7 Historical trends

We next plot the variation of our estimates of the quantum resources as a function of time (from Feb. 2018 to the present time), due to improved cryptanalytic techniques, for today's routinely used RSA schemes: RSA-1024, RSA-2048, RSA-3072, and RSA-4096.

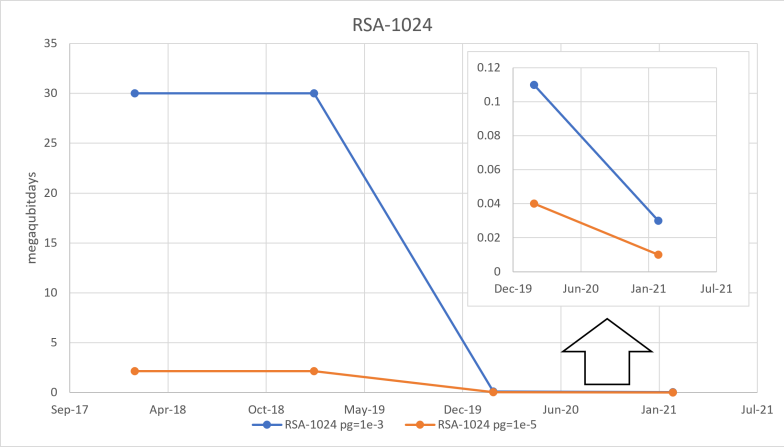


Fig. 2. RSA-1024 quantum resources variation with time due to improved quantum cryptanalytic techniques, for two physical error rates per gate p_g equal to 10^{-3} and 10^{-5}, respectively. The quantum resources is measured in megaqubitdays. The corresponding classical security parameter is 80 bits. The arrow in the figure points towards the zoomed-in portion of the plot.

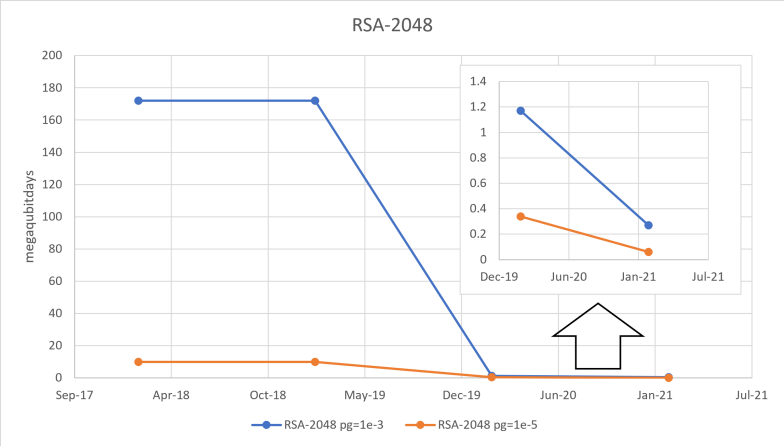


Fig. 3. RSA-2048 quantum resources variation with time due to improved quantum cryptanalytic techniques, for two physical error rates per gate p_g equal to 10^{-3} and 10^{-5}, respectively. The quantum resources is measured in megaqubitdays. The corresponding classical security parameter is 112 bits. The arrow in the figure points towards the zoomed-in portion of the plot.

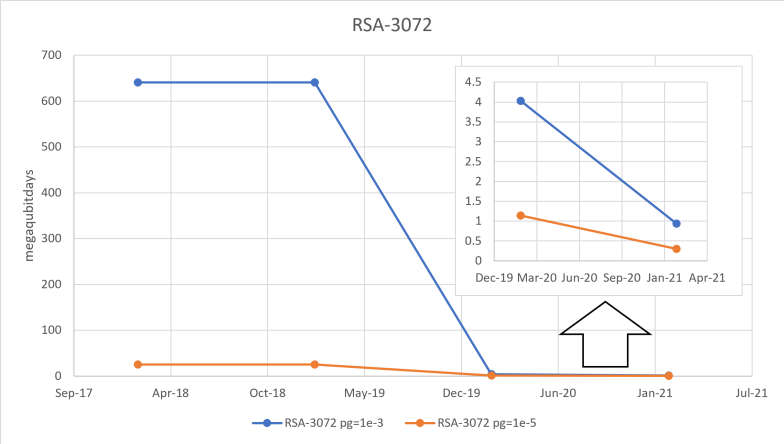


Fig. 4. RSA-3072 quantum resources variation with time due to improved quantum cryptanalytic techniques, for two physical error rates per gate p_g equal to 10^{-3} and 10^{-5}, respectively. The quantum resources is measured in megaqubitdays. The corresponding classical security parameter is 128 bits. The arrow in the figure points towards the zoomed-in portion of the plot.

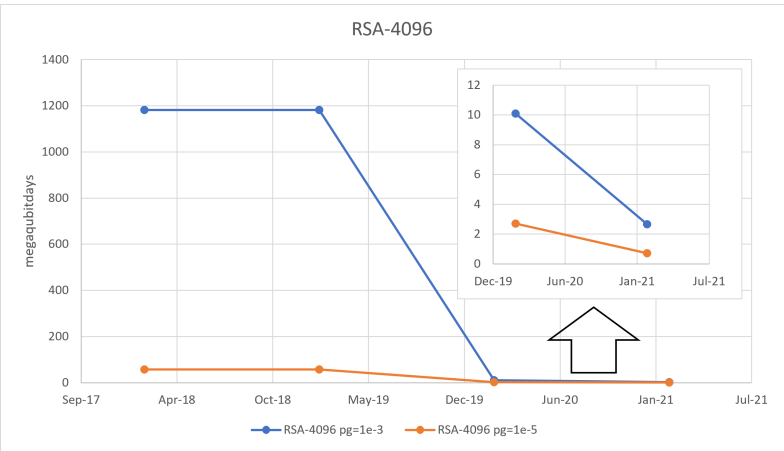


Fig. 5. RSA-4096 quantum resources variation with time due to improved quantum cryptanalytic techniques, for two physical error rates per gate p_g equal to 10^{-3} and 10^{-5}, respectively. The quantum resources is measured in megaqubitdays. The corresponding classical security parameter is approximately 156 bits. The arrow in the figure points towards the zoomed-in portion of the plot.

3 Public key cryptographic schemes – Elliptic-Curve Diffie-Hellman (ECDH)

Our ECC estimates do not differ from the time of our last report. For completeness, we plot the variation of our estimates of the quantum resources as a function of time (from Feb. 2018 to the present time), due to improved cryptanalytic techniques.

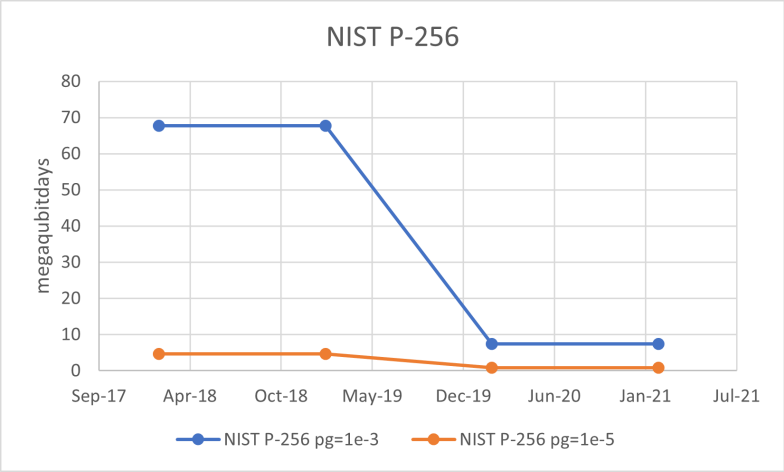


Fig. 6. NIST P-256 quantum resources variation with time due to improved quantum cryptanalytic techniques, for two physical error rates per gate p_g equal to 10^{-3} and 10^{-5}, respectively. The quantum resources is measured in megaqubitdays. The corresponding classical security parameter is 128 bits.

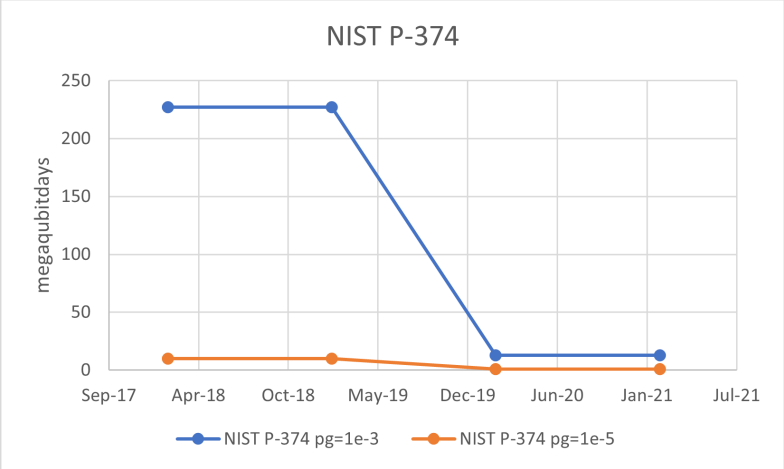


Fig. 7. NIST P-384 quantum resources variation with time due to improved quantum cryptanalytic techniques, for two physical error rates per gate p_g equal to 10^{-3} and 10^{-5}, respectively. The quantum resources is measured in megaqubitdays. The corresponding classical security parameter is 192 bits.

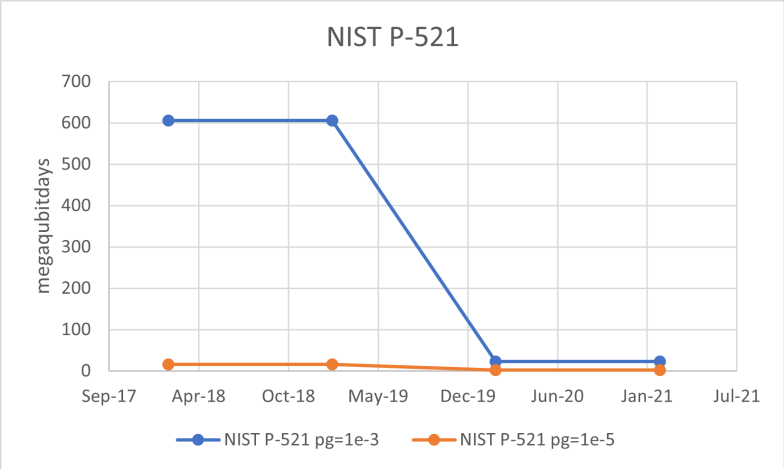


Fig. 8. NIST P-521 quantum resources variation with time due to improved quantum cryptanalytic techniques, for two physical error rates per gate p_g equal to 10^{-3} and 10^{-5}, respectively. The quantum resources is measurvlad gheorghiued in megaqubitdays. The corresponding classical security parameter is 256 bits.

4 Symmetric key cryptographic ciphers

A recent paper by [15] uses dynamic programming techniques to reduce the multiplicative depth of logic networks, which, for quantum circuits, translates into a T-depth and T-count reduction, at the cost of increasing the number of logical qubits by approximately one order of magnitude. Using those new circuits with our quantum resource estimation toolkit yield the results summarized next.

4.1 AES-128

AES-128	**Old estimates**			**Current estimates**		
p_g	s_q	n_ℓ	n_p	s_q	n_ℓ	n_p
10^{-3}	101.66	15265	7.17×10^8	98.95	10924	4.04×10^9
10^{-5}	97.19	2545	1.77×10^6	94.2	7564	1.74×10^7

Table 7. AES-128 security estimates. Here s_q denotes the quantum security parameter (in bits), n_ℓ denotes the number of logical qubits, and n_p denotes the number of physical qubits.

4.2 AES-192

AES-192	**Old estimates**			**Current estimates**		
p_g	s_q	n_ℓ	n_p	s_q	n_ℓ	n_p
10^{-3}	137.39	163793	2.93×10^9	135.29	62156	1.12×10^{10}
10^{-5}	132.81	23393	7.81×10^6	130.67	11756	6.53×10^7

Table 8. AES-192 security estimates. Here s_q denotes the quantum security parameter (in bits), n_ℓ denotes the number of logical qubits, and n_p denotes the number of physical qubits.

4.3 AES-256

AES-256	**Old estimates**			**Current estimates**		
p_g	s_q	n_ℓ	n_p	s_q	n_ℓ	n_p
10^{-3}	170.49	218465	6.56×10^9	167.67	63884	2.24×10^{10}
10^{-5}	166.0	34865	1.61×10^7	163.82	13484	1.15×10^8

Table 9. AES-256 security estimates. Here s_q denotes the quantum security parameter (in bits), n_ℓ denotes the number of logical qubits, and n_p denotes the number of physical qubits.

4.4 Historical trends

Below we display the variation of our estimates of the quantum security parameter q_s as a function of time (from Feb. 2018 to the present time), due to improved cryptanalytic techniques.

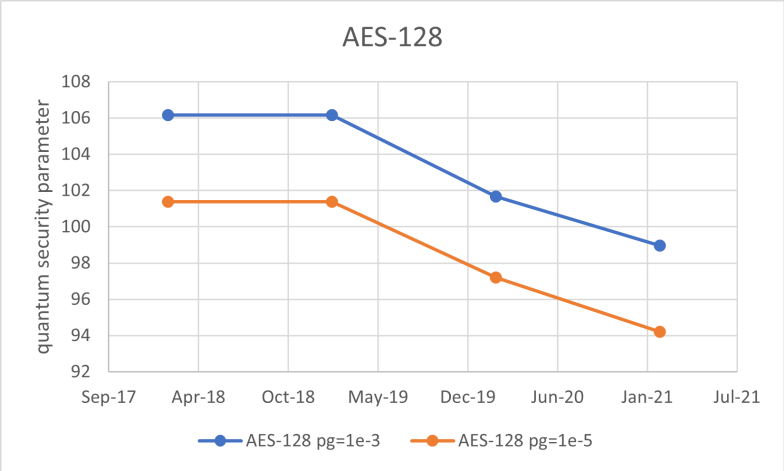


Fig. 9. AES-128 quantum security parameter variation with time due to improved quantum cryptanalytic techniques, for two physical error rates per gate p_g equal to 10^{-3} and 10^{-5}, respectively

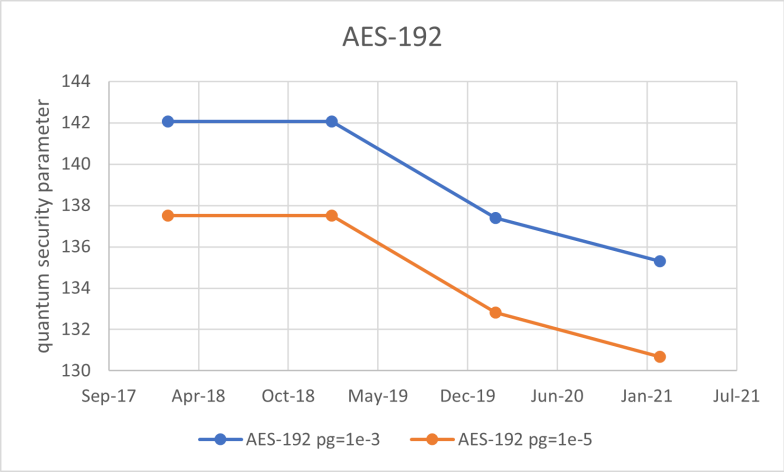


Fig. 10. AES-192 quantum security parameter variation with time due to improved quantum cryptanalytic techniques, for two physical error rates per gate p_g equal to 10^{-3} and 10^{-5}, respectively

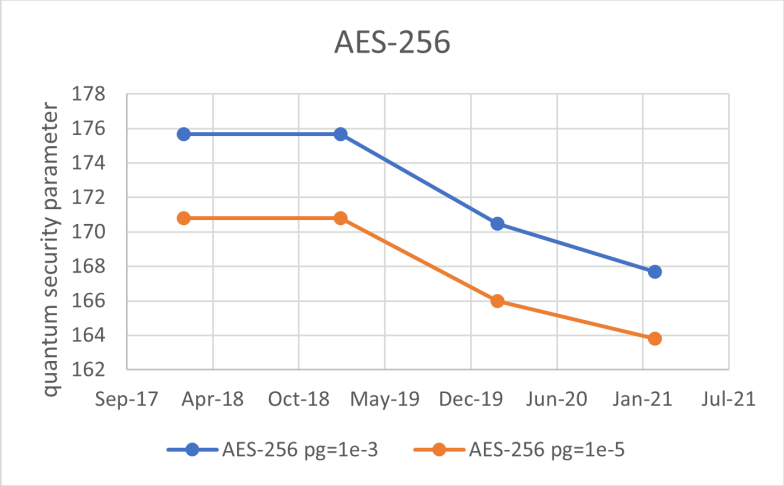


Fig. 11. AES-256 quantum security parameter variation with time due to improved quantum cryptanalytic techniques, for two physical error rates per gate p_g equal to 10^{-3} and 10^{-5}, respectively

5 Hash functions

Using the circuit optimization techniques from [15] we obtain the following estimates for the SHA-256 and SHA3-256 family of hash functions.

5.1 SHA-256

SHA-256	**Old estimates**			**Current estimates**		
p_g	s_q	n_ℓ	n_p	s_q	n_ℓ	n_p
10^{-3}	170.45	56402	6.58×10^9	168.95	77684	4.90×10^{10}
10^{-5}	166.36	6002	1.39×10^7	165.28	27284	1.10×10^8

Table 10. SHA-256 security estimates. Here s_q denotes the quantum security parameter (in bits), n_ℓ denotes the number of logical qubits, and n_p denotes the number of physical qubits.

5.2 SHA3-256

SHA3-256	**Old estimates**			**Current estimates**		
p_g	s_q	n_ℓ	n_p	s_q	n_ℓ	n_p
10^{-3}	168.45	6800	1.59×10^9	167.18	35152	1.06×10^9
10^{-5}	166.47	6800	1.81×10^8	166.14	35152	2.31×10^8

Table 11. SHA3-256 security estimates. Here s_q denotes the quantum security parameter (in bits), n_ℓ denotes the number of logical qubits, and n_p denotes the number of physical qubits.

5.3 Historical trends

Here we display the variation of our estimates of the quantum security parameter q_s as a function of time (from Feb. 2018 to the present time), due to improved cryptanalytic techniques.

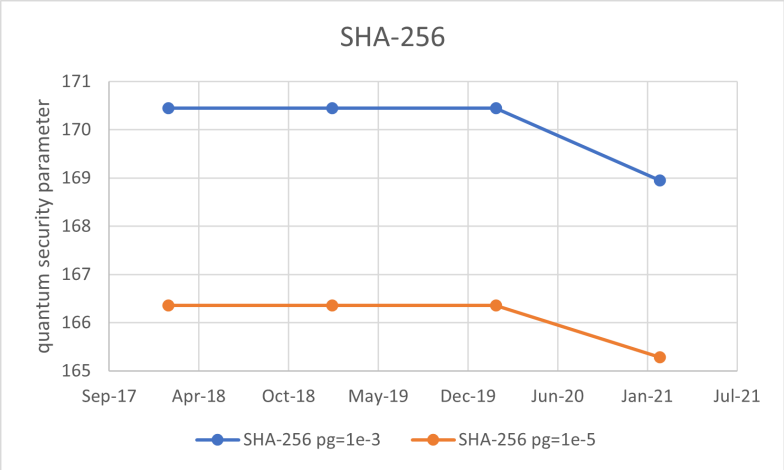


Fig. 12. SHA-256 quantum security parameter variation with time due to improved quantum cryptanalytic techniques, for two physical error rates per gate p_g equal to 10^{-3} and 10^{-5}, respectively

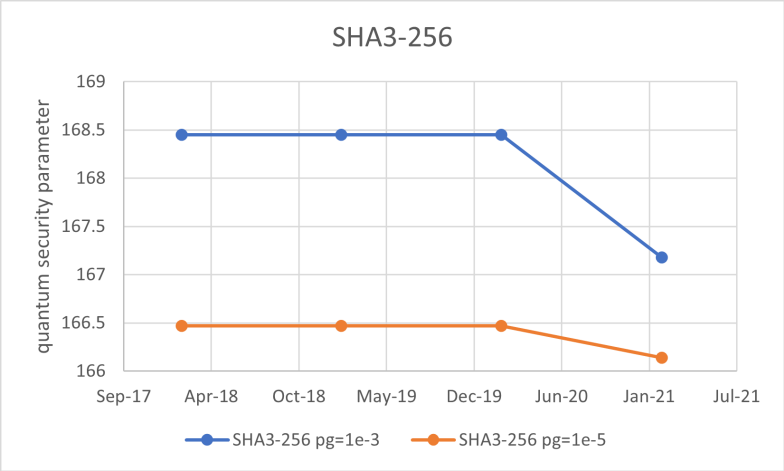


Fig. 13. SHA3-256 quantum security parameter variation with time due to improved quantum cryptanalytic techniques, for two physical error rates per gate p_g equal to 10^{-3} and 10^{-5}, respectively

6 Novel approaches to attacking symmetric cryptographic primitives

Solving systems of multivariate polynomial equations is a fundamental problem that is NP-complete even when the polynomials are restricted over $\mathbb{F}_2$, and reduces to solving an exponential number of linear equations. The main object used in this computation is called the Macaulay matrix, which holds coefficients of linear equations that come from the input polynomials, and multiples of them (multiplying each polynomial by each monomial up to a certain degree). Each monomial is represented by a new variable, recasting the polynomial equations and their multiples as linear equations. The usual classical approach to solve a polynomial system is based on computing the Gröbner basis of the corresponding polynomial ideal by triangularizing the Macaulay matrix. Depending on the type of the polynomial system, much work has been done to characterize and improve the complexity of solving polynomial systems using the Macaulay matrix [21,22,23,24,25,26,27].

In quantum computing, the HHL [28] Quantum Linear System (QLS) algorithm can take access to an exponential size matrix A with certain properties, a quantum state $|b\rangle$, and computes a quantum state $|x\rangle$ such that $\mu A\,|x\rangle = |b\rangle$ in time $\widetilde{\mathcal{O}}\left(\kappa^2 s^2\right)$,[3] where κ is the *condition number* of A, μ is a normalization factor, and s is the sparsity of the matrix A. State-of-the-art QLS algorithms have complexity $\widetilde{\mathcal{O}}\left(\kappa s\right)$. Although the QLS algorithm is BQP-complete [28], meaning that it captures all essential features of quantum computing, a natural "killer-application" is still to be discovered – showing the difficulty of connecting it to classical problems. For example, to efficiently solve the classical equation $Ax = b$, using the original HHL algorithm, where implicit access is given to an exponentially large matrix A and b, the following must be satisfied: the state $|b\rangle$ can be efficiently prepared, the sought data can be efficiently extracted from the output state $|x\rangle$, and the matrix A should be sparse and well-conditioned [29].

Chen and Gao [30] made an interesting connection between the exponential size Macaulay matrix and the HHL algorithm. While they use Gröbner bases in their proof of correctness, they do not explicitly compute the Gröbner basis and instead use the HHL algorithm to solve the exponentially large system of linear equations resulting from the Macaulay matrix. In this case, with proper setup, they show that the access requirements that usually cause so much trouble, can all be efficiently resolved, namely: having access to an appropriate matrix A, creating $|b\rangle$, and extracting the answer from $|x\rangle$. However, a question was left open: what is the condition number of the matrices, driving the running time? Intuitively, for arbitrary instances of polynomial systems, the condition number of the resulting matrix should be large because the approach would solve an NP-complete problem. But analysis of the size of the condition number was left open, both in general, and for special cases such as breaking cryptosystems which have distributions over the problem instances instead of being worst case.

[3] We denote $\mathcal{O}\left(T \cdot \operatorname{poly}\log\left(T\right) \cdot \operatorname{poly}(1/\varepsilon)\right)$ by $\widetilde{\mathcal{O}}\left(T\right)$, where ε is the required precision of the solution.

We mentioned such a potential attack based on Chen and Gao [30] work in our previous report [9], however at the time we were not aware whether such an attack is feasible or not. Very recently, we proved [18] an exponential lower bound on the condition number κ of the matrix A related to the Boolean polynomial system, which shows that the quantum algorithm in [30] takes exponential time. Our result implies that attacks based on the QLS algorithms are impractical, and therefore pose little threat to currently-deployed symmetric ciphers. We expect similar behaviour (i.e., exponentially-large condition number) for cryptographic hash functions, although we did not yet investigate the problem rigorously.

7 Conclusions and future directions

In this report we updated our quantum security estimates for the most common cryptographic primitives, including the RSA public-key schemes, AES ciphers, and the SHA-256/SHA3-256 hash functions. For RSA, we observe a reduction in the total quantum resources by a factor of $5 \sim 6$. For AES, the quantum security parameter q_s is reduced by approximately $2 \sim 3$ bits, and for hash functions, q_s is reduced by approximately $1 \sim 2$ bits.

In addition, in light of new research done with collaborators, we dismissed the threat posed by quantum linear solver-based algorithms to AES ciphers, which also strongly suggests they will be ineffective against other strong ciphers and hash functions. Since the time our previous report was published, most progress in quantum cryptanalysis was related to novel optimization techniques at the logical layer, i.e., better quantum circuits for the corresponding circuit elements used to construct circuits for attacking the aforementioned schemes.

In the future we plan to keep update our estimates for public-key schemes, symmetric ciphers, and hash functions. For the latter, we intend to prove that QLS algorithms do not pose a real threat to their security.

We reiterate that estimating the strength of current cryptographic schemes against realistic quantum attacks is a moving target that depends on a variety of parameters, such as fault-tolerant quantum error correction, circuit optimization and compilation, novel cryptanalysis results, improved quantum algorithms etc. Monitoring all those (future) advances is therefore our paramount priority and stresses the importance of preparing for migration to quantum-resistant cryptographic systems.

References

1. Grover, L.K.: Quantum mechanics helps in searching for a needle in a haystack. Phys. Rev. Lett. 79, 325–328 (Jul 1997), http://link.aps.org/doi/10.1103/PhysRevLett.79.325
2. Zalka, C.: Grover's quantum searching algorithm is optimal, e-print arXiv:quant-ph/9711070
3. Rivest, R.L., Shamir, A., Adleman, L.: A method for obtaining digital signatures and public-key cryptosystems. Commun. ACM 21(2), 120–126 (Feb 1978), http://doi.acm.org/10.1145/359340.359342

4. Miller, V.S.: Use of elliptic curves in cryptography. In Hugh C. Williams, editor, Advances in Cryptology - CRYPTO '85, Santa Barbara, California, USA, August 18-22, 1985, Proceedings, volume 218 of Lecture Notes in Computer Science, pages 417–426. Springer, 1985 (1985)
5. Koblitz, N.: Elliptic curve cryptosystems. Math. Comp. 48, 203–209 (1987)
6. Shor, P.W.: Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. SIAM Journal on Computing 26(5), 1484–1509 (1997), http://link.aip.org/link/?SMJ/26/1484/1
7. Gheorghiu, V., Mosca, M.: A resource estimation framework for quantum attacks against cryptographic functions (part 1) (2017), Global Risk Institute quantum risk assessment report, Sep. 2016 - Feb. 2017
8. Gheorghiu, V., Mosca, M.: A resource estimation framework for quantum attacks against cryptographic functions (part 2) (2017), Global Risk Institute quantum risk assessment report, Feb. 2017 - Aug. 2017
9. Gheorghiu, V., Mosca, M.: A resource estimation framework for quantum attacks against cryptographic functions (part 3) (2018), Global Risk Institute quantum risk assessment report, Aug. 2017 - Feb. 2018
10. Gheorghiu, V., Mosca, M.: A resource estimation framework for quantum attacks against cryptographic functions (part 4) (2018), Global Risk Institute quantum risk assessment report, Feb. 2018 - Aug. 2018
11. Gheorghiu, V., Mosca, M.: A resource estimation framework for quantum attacks against cryptographic functions (2020) (2020), Global Risk Institute quantum risk assessment report, Feb. 2020
12. Piani, M., Mosca, M.: Quantum threat timeline report 2019 (2019), Global Risk Institute
13. Piani, M., Mosca, M.: Quantum threat timeline report 2020 (2020), Global Risk Institute
14. Fowler, A.G., Mariantoni, M., Martinis, J.M., Cleland, A.N.: Surface codes: Towards practical large-scale quantum computation. Phys. Rev. A 86, 032324 (Sep 2012), http://link.aps.org/doi/10.1103/PhysRevA.86.032324
15. Häner, T., Soeken, M.: Lowering the T-depth of quantum circuits by reducing the multiplicative depth of logic networks (2020)
16. Jaques, S., Naehrig, M., Roetteler, M., Virdia, F.: Implementing grover oracles for quantum key search on aes and lowmc. In: Canteaut, A., Ishai, Y. (eds.) Advances in Cryptology – EUROCRYPT 2020. pp. 280–310. Springer International Publishing, Cham (2020)
17. Oonishi, K., Tanaka, T., Uno, S., Satoh, T., Meter, R.V., Kunihiro, N.: Efficient construction of a control modular adder on a carry-lookahead adder using relative-phase Toffoli gates (2020)
18. Ding, J., Gheorghiu, V., Gilyén, A., Hallgren, S., Li, J.: Limitations of the Macaulay matrix approach for using the HHL algorithm to solve multivariate polynomial systems. In: 24th Annual Conference on Quantum Information Processing (QIP). to appear. (2021)
19. Gidney, C., Ekerå, M.: How to factor 2048 bit RSA integers in 8 hours using 20 million noisy qubits (2019), arxiv:1905.09749 [quant-ph]
20. Fowler, A.G., Gidney, C.: Low overhead quantum computation using lattice surgery (2018), arXiv:1808.06709 [quant-ph]
21. Ars, G., Faugere, J.C., Imai, H., Kawazoe, M., Sugita, M.: Comparison between XL and Gröbner basis algorithms. In: International Conference on the Theory and Application of Cryptology and Information Security. pp. 338–353. Springer (2004)

22. Caminata, A., Gorla, E.: Solving multivariate polynomial systems and an invariant from commutative algebra (2017), arXiv1706.06319
23. Courtois, N., Klimov, A., Patarin, J., Shamir, A.: Efficient algorithms for solving overdefined systems of multivariate polynomial equations. In: International Conference on the Theory and Applications of Cryptographic Techniques. pp. 392–407. Springer (2000 (Extended version as of 24 Aug, 2004), http://www.minrank.org/xlfull.pdf)
24. Ding, J., Schmidt, D.: Solving degree and degree of regularity for polynomial systems over a finite fields. In: Number Theory and Cryptography, pp. 34–49. Springer (2013)
25. Diem, C.: The XL-algorithm and a conjecture from commutative algebra. In: International Conference on the Theory and Application of Cryptology and Information Security. pp. 323–337. Springer (2004)
26. Perret, L.: Bases de Gröbner en Cryptographie Post-Quantique. Ph.D. thesis, UPMC-Paris 6 Sorbonne Universités (2016)
27. Wiesinger-Widi, M.: Gröbner bases and generalized sylvester matrices. Ph.D. thesis, Johannes Kepler University Linz, Austria (2015)
28. Harrow, A.W., Hassidim, A., Lloyd, S.: Quantum algorithm for linear systems of equations. Phys. Rev. Lett. 103, 150502 (Oct 2009), http://link.aps.org/doi/10.1103/PhysRevLett.103.150502
29. Aaronson, S.: Read the fine print. Nature Physics 11(4), 291–293 (2015), https://doi.org/10.1038/nphys3272, https://scottaaronson.com/papers/qml.pdf
30. Chen, Y.A., Gao, X.S.: Quantum Algorithms for Boolean Equation Solving and Quantum Algebraic Attack on Cryptosystems (2017), arXiv:1712.06239 [quant-ph]