evolutionQ

A resource estimation framework for quantum attacks against cryptographic functions - final report

GRI quantum risk assessment report Feb. 2018 - Aug. 2018

Vlad Gheorghiu and Michele Mosca

evolutionQ Inc., Waterloo ON, Canada

August 31, 2018

Abstract. We analyze the space/time tradeoffs for attacking currently used asymmetric (public-key) cryptographic schemes that include RSA and ECDH, for various security parameters. We use the latest advances in cryptanalysis, circuit compilation and fault-tolerant theory (such as surface-code lattice surgery techniques [1,2,3]) when providing the estimates.
In addition to the more conservative (from a cybersecurity perspective) choice of a physical error rate per gate of 10^{-5}, here we also highlight the scaling for a 10^{-3} physical error rate per gate, which is more realistic in the short term[1].
We provide analytical formulas for the space/time tradeoffs for all the schemes we analyze. Those are based on fitting of our numerical simulation data (logarithm base 2 of the number of qubits required as a function of the logarithm base 2 of the time taken to break the scheme). Since most of the recent advances in quantum cryptanalysis are at the fault-tolerant layer, symmetric schemes or hash functions are far less affected, and as such a detailed analysis is left out of this report. The security parameter of symmetric schemes remains almost the same, the only significant difference between our previous analysis [4,5] being a decrease of the physical footprint required to attack the scheme.

1 Introduction

Quantum computers pose serious threats to current deployed cryptography, weakening symmetric cryptography and hash functions via Grover's searching

[1] Assuming a quantum computer that will run on a surface-code based fault-tolerant error-correcting layer, which, up to today, seems to be the most promising candidate for quantum error correction.

algorithm [6,7] and breaking public-key systems based on factoring large numbers (RSA [8]) or solving discrete logarithms in finite groups (Elliptic Curve Cryptography (ECC) [9,10]) via Shor's algorithm [11].

As mentioned in detail in our previous reports [4,12,5], a realistic attack using a fully fault tolerant quantum computer attack against a cryptographic scheme requires several layers, depicted for the sake of completeness in Fig. 1. Any improvement in any of the layers above decreases the resources (space,

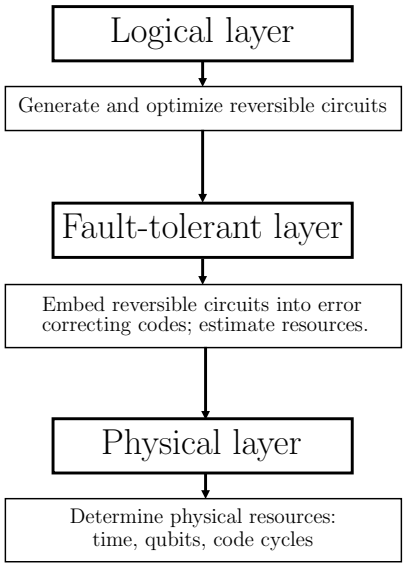

Fig. 1. Analyzing an attack against a cryptographic scheme with a fault-tolerant quantum adversary.

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.

In the remainder of this paper we investigate the security of asymmetric (public-key) cryptographic schemes such as RSA and ECC against quantum attacks, using the latest developments and advances related to the layers depicted in Fig. 1.

2 Methodology

Most of the recent progress in quantum cryptanalysis is related to the fault-tolerant layer in Fig. 1. New methods and techniques based on surface code lattice surgery [1,2,3] allow a significant decrease of the overall footprint (number of qubits, or space) taken by the quantum computation, and also a relatively

modest decrease in time, in comparison with braiding techniques. In all our previous reports [4,12,5] we used fault-tolerant methods based on surface code defects and braiding [13,14], which recently have been improved upon using lattice surgery.

As mentioned in detail in our previous reports, any quantum algorithm can be mapped to a quantum circuit, and the latter "executed" on a quantum computers. The quantum circuit represents what we call the "logical layer". Such a circuit can always be decomposed in a sequence of "elementary gates", such as Clifford gates (CNOT, Hadamard etc. [15]) augmented by a non-Clifford gate such as the T gate.

Running a logical circuit on a full fault-tolerant quantum computer is highly non-trivial. The sequence of logical gates have to be mapped to sequences of surface code measurement cycles (see e.g. [13] for extensive details). By far, the most resource-consuming (in terms of number of qubits required and time) is the T gate[2]. In comparison with surface code defects and braiding techniques [13], lattice surgery techniques [1,2,3] reduce the spatial overhead required for implementing T gates via magic state distillation by approximately a factor of 5, while also modestly improving the time.

In the following we consider the best up-to-date optimized quantum logical circuits for attacking RSA and ECC public-key schemes [17,18,19,20] then perform a resource estimation analysis using lattice surgery techniques. We remark that the overall time required to run the algorithm depends on the level of parallelization for the magic state factories[3].

For each scheme, we analyze the space/time tradeoffs and plot the results on a double logarithmic scale. We fit the data using a third degree polynomial[4] and obtain an analytical closed-form formula for the relation between the time and the number of qubits required to attack the scheme, in the form

$$y(x) = \alpha x^3 + \beta x^2 + \gamma x + \delta, \tag{1}$$

[2] Clifford gates are "cheap", i.e. they require relatively small overhead for implementation in the surface code, but are not universals, hence a non-Clifford gate is required. One such gate is the T gate. There are other possible choices, however all of the non-Clifford gates require special techniques such as magic state distillation [3,16] and significant overhead (order of magnitudes higher than Clifford gates) to be implemented in the surface code. In fact, to a first order approximation, for the purpose of resource estimation, one can simply ignore the overhead introduced by the Clifford gates and simply focus only on the T gates.

[3] Every T gate in the circuit must be implemented by a specialized magic state factory, each of which occupies a significant physical footprint. One can implement more magic states in parallel if one is willing to increase the physical footprint of the computation.

[4] A third degree polynomial fits the data very precisely, providing a coefficient of determination R^2 greater than 0.997.

where y represents logarithm base 2 of the number of qubits and x represents the logarithm base 2 of the time (in seconds). For example, the quantity

$$y\left(\log_2(24 \times 3600)\right) \approx y(16.3987) \tag{2}$$

represents how many qubits are required to break the scheme in one day (24 hours) for a fixed physical error rate per gate p_g, assuming a surface code cycle time of 200ns. Note that the computation time scales linearly with the surface code cycle time, e.g. a 1000ns surface code cycle time will result in a computation that is 5 times longer than a $200ns$ surface code cycle time. Therefore, for a specific cryptographic scheme for which we plotted the space/time tradeoffs using a surface code cycle time of $200ns$ and a fixed physical error rate per gate p_g, the number of qubits required to break a specific scheme in a time t using an alternative surface code cycle time t_c is given by

$$y\left(\log_2\left(\frac{200ns}{t_c}t\right)\right), \tag{3}$$

where t is expressed in seconds and t_c is expressed in nanoseconds.

In addition to the optimistic (from the perspective of experimental quantum computing) physical error rates p_g in the range $10^{-4} - 10^{-7}$ used in our previous reports [4,12,5], in all our current estimates we also used the more conservative (and realistic in the short term) physical error rate per gate of 10^{-3}. We assume a surface code cycle time of 200ns, in conformance with [13]. For each scheme we analyze, we compare its security using $p_g = 10^{-3}$ (more realistic) and $p_g = 10^{-5}$ (more optimistic). Note that assuming the more optimistic assumption from a quantum computing perspective is the more conservative assumption from a cybersecurity perspective.

Furthermore, in this analysis, we are reporting the full physical footprint, including the memory required for magic state distillation. Using present-day techniques, the memory required for generating these generic input states accounts for a substantial fraction of the total memory cost and thus we are including these in the total cost estimate and will track the impact of improved methods.

3 RSA schemes

In the following section we compute the space/time tradeoffs for attacking public-key cryptographic schemes based on factoring large numbers, namely RSA-1024, RSA-2048, RSA-3072, RSA-4096, RSA-7680 and RSA-15360. For each scheme, we plot the space/time tradeoff points then fit it with a third degree polynomial, for $p_g = 10^{-3}$ and $p_g = 10^{-5}$, respectively.

3.1 RSA-1024

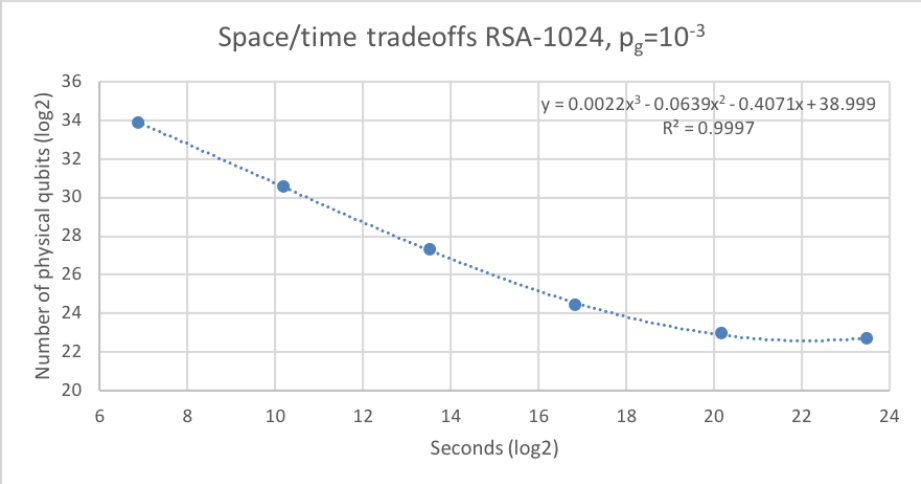

Fig. 2. RSA-1024 space/time tradeoffs with physical error rate per gate $p_g = 10^{-3}$. The scale is logarithmic (base 2). Approximately $y(16.3987) \approx 3.01 \times 10^7$ physical qubits are required to break the scheme in one day (24 hours). The number of T gates in the circuit is 3.01×10^{11}, the corresponding number of logical qubits is 2050, and the total number of surface code cycles is 5.86×10^{13}. The quantity R^2 represents the coefficient of determination (closer to 1, better the fitting). The classical security parameter is approximately 80 bits.

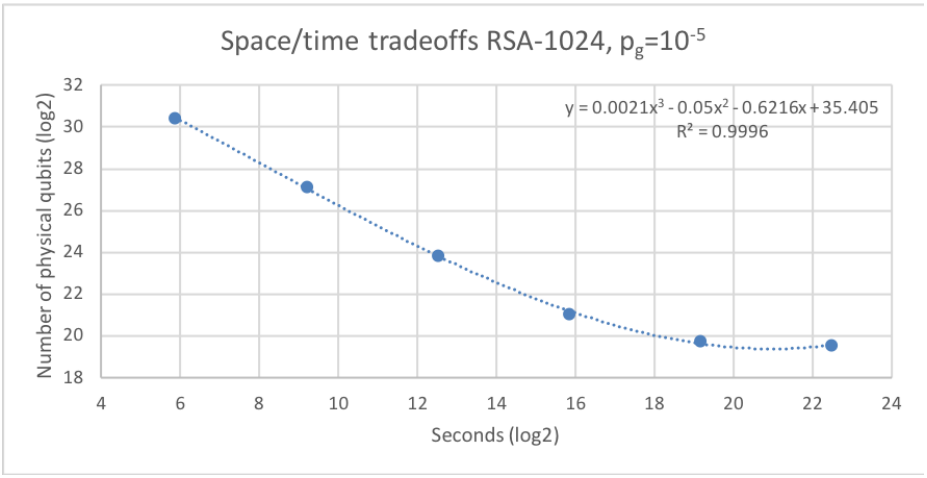

Fig. 3. RSA-1024 space/time tradeoffs with physical error rate per gate $p_g = 10^{-5}$. The scale is logarithmic (base 2). Approximately $y(16.3987) \approx 2.14 \times 10^6$ physical qubits are required to break the scheme in one day (24 hours). The number of T gates in the circuit is 3.01×10^{11}, the corresponding number of logical qubits is 2050, and

the total number of surface code cycles is 2.93×10^{13}. The classical security parameter is approximately 80 bits.

3.2 RSA-2048

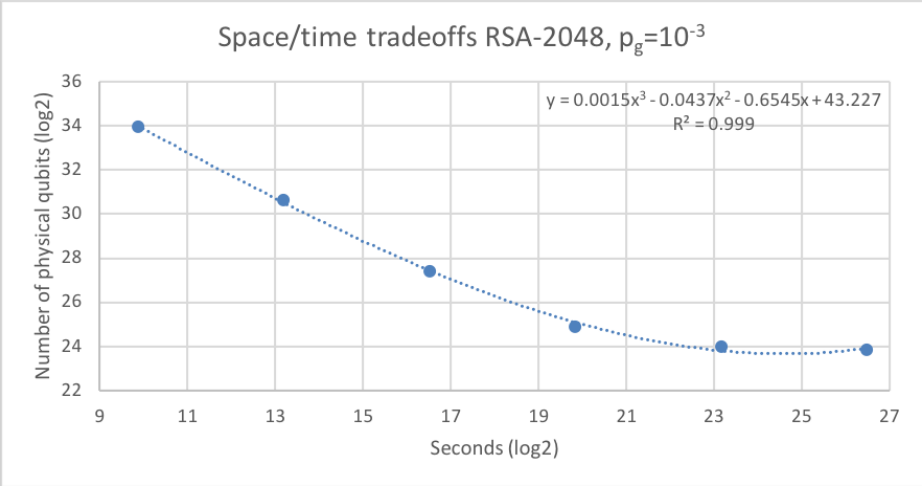

Fig. 4. RSA-2048 space/time tradeoffs with physical error rate per gate $p_g = 10^{-3}$. The scale is logarithmic (base 2). Approximately $y(16.3987) \approx 1.72 \times 10^8$ physical qubits are required to break the scheme in one day (24 hours). The number of T gates in the circuit is 2.41×10^{12}, the corresponding number of logical qubits is 4098, and the total number of surface code cycles is 4.69×10^{14}. The classical security parameter is approximately 112 bits.

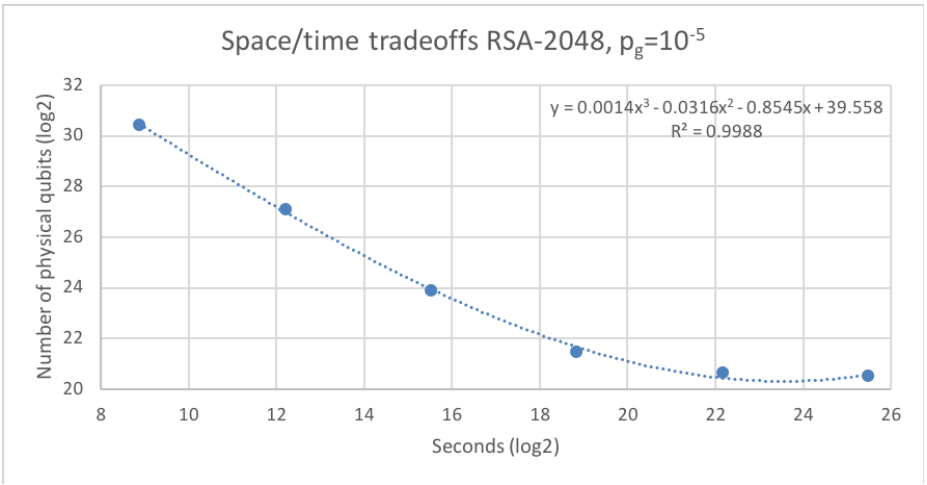

Fig. 5. RSA-2048 space/time tradeoffs with physical error rate per gate $p_g = 10^{-5}$. The scale is logarithmic (base 2). Approximately $y(16.3987) \approx 9.78 \times 10^6$ physical qubits are required to break the scheme in one day (24 hours). The number of T gates in the circuit is 2.41×10^{12}, the corresponding number of logical qubits is 4098, and the total number of surface code cycles is 2.35×10^{14}. The classical security parameter is approximately 112 bits.

Note that in comparison with fault-tolerant methods based on surface code defects and braiding, where we estimated (see Table 1 and [12]) that breaking a 2048 RSA module in 24 hours using a physical error rate $p_g = 10^{-5}$ requires around 52 million physical qubits, in this report, where we use lattice surgery techniques, we observe a reduction in the physical footprint to approximately 10 million physical qubits, which represents roughly a 5 times improvement in the physical footprint of the quantum computer required to break the scheme.

3.3 RSA-3072

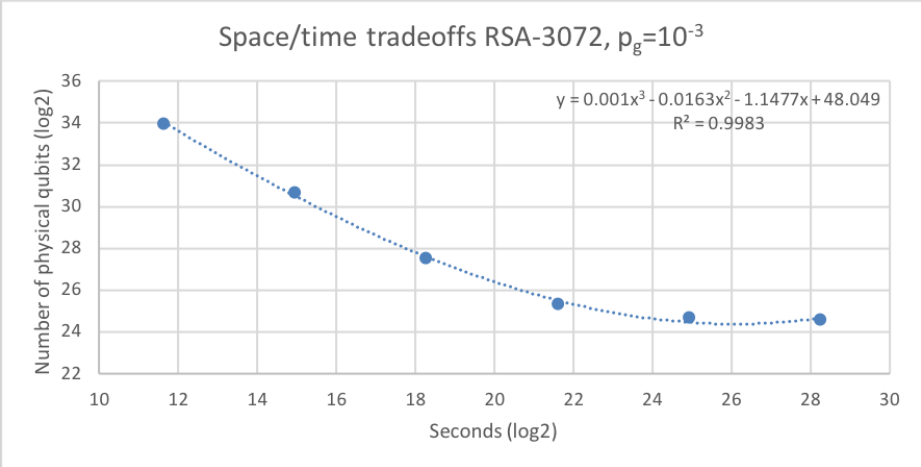

Fig. 6. RSA-3072 space/time tradeoffs with physical error rate per gate $p_g = 10^{-3}$. The scale is logarithmic (base 2). Approximately $y(16.3987) \approx 6.41 \times 10^8$ physical qubits are required to break the scheme in one day (24 hours). The number of T gates in the circuit is 8.12×10^{12}, the corresponding number of logical qubits is 6146, and the total number of surface code cycles is 1.58×10^{15}. The classical security parameter is approximately 128 bits.

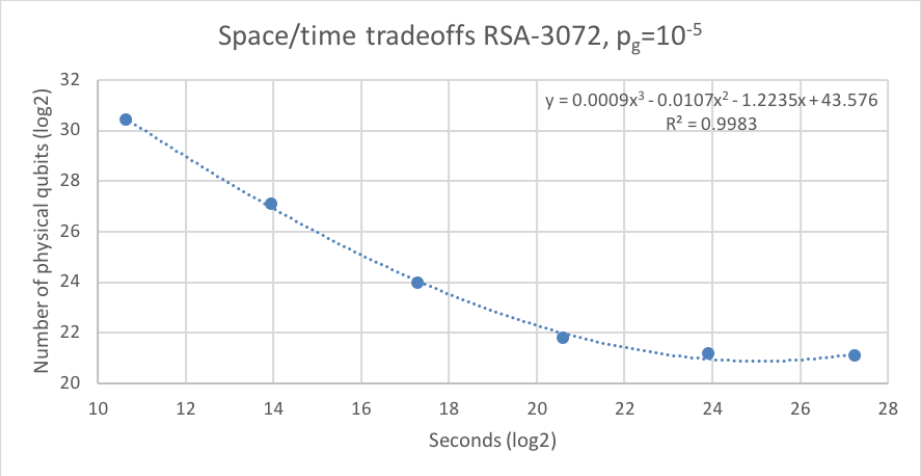

Fig. 7. RSA-3072 space/time tradeoffs with physical error rate per gate $p_g = 10^{-5}$. The scale is logarithmic (base 2). Approximately $y(16.3987) \approx 2.55 \times 10^7$ physical qubits are required to break the scheme in one day (24 hours). The number of T gates in the circuit is 8.12×10^{12}, the corresponding number of logical qubits is 6146, and the total number of surface code cycles is 7.91×10^{14}. The classical security parameter is approximately 128 bits.

3.4 RSA-4096

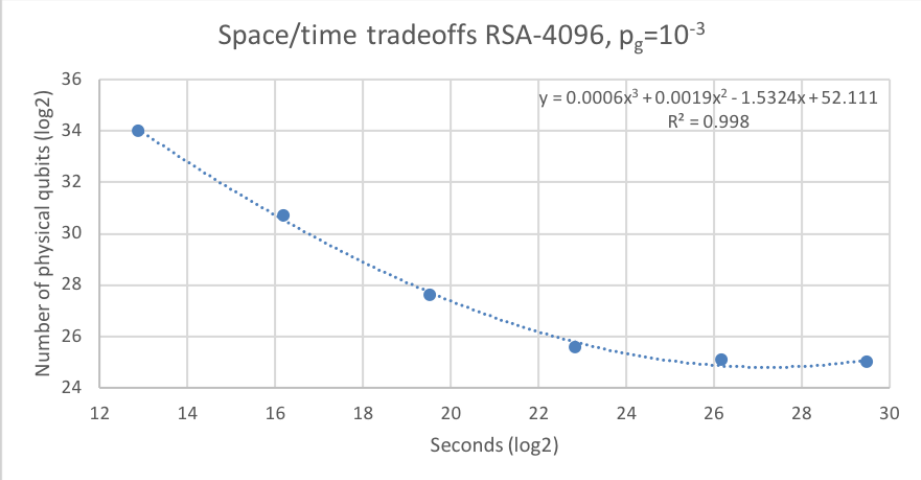

Fig. 8. RSA-4096 space/time tradeoffs with physical error rate per gate $p_g = 10^{-3}$. The scale is logarithmic (base 2). Approximately $y(16.3987) \approx 1.18 \times 10^9$ physical qubits are required to break the scheme in one day (24 hours). The number of T gates

in the circuit is 1.92×10^{13}, the corresponding number of logical qubits is 8194, and the total number of surface code cycles is 3.75×10^{15}. The classical security parameter is approximatively approximately 156 bits.

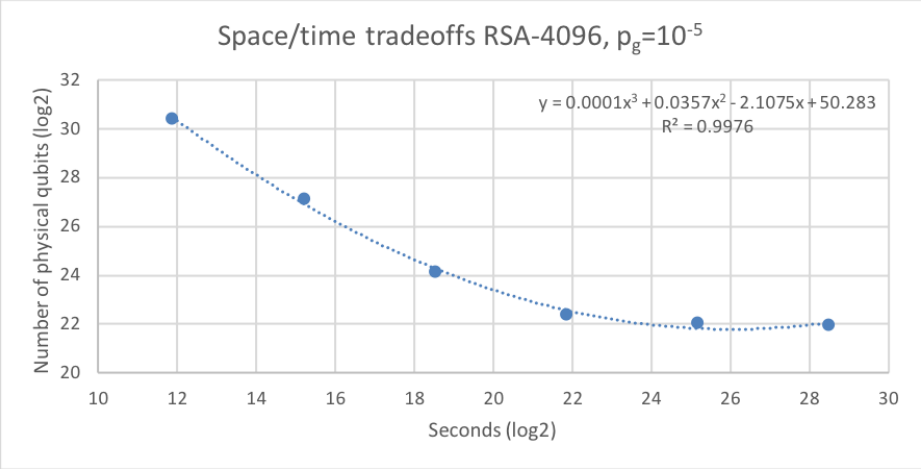

Fig. 9. RSA-4096 space/time tradeoffs with physical error rate per gate $p_g = 10^{-5}$. The scale is logarithmic (base 2). Approximately $y(16.3987) \approx 5.70 \times 10^7$ physical qubits are required to break the scheme in one day (24 hours). The number of T gates in the circuit is 1.92×10^{13}, the corresponding number of logical qubits is 8194, and the total number of surface code cycles is 1.88×10^{15}. The classical security parameter is approximatively approximately 156 bits.

3.5 RSA-7680

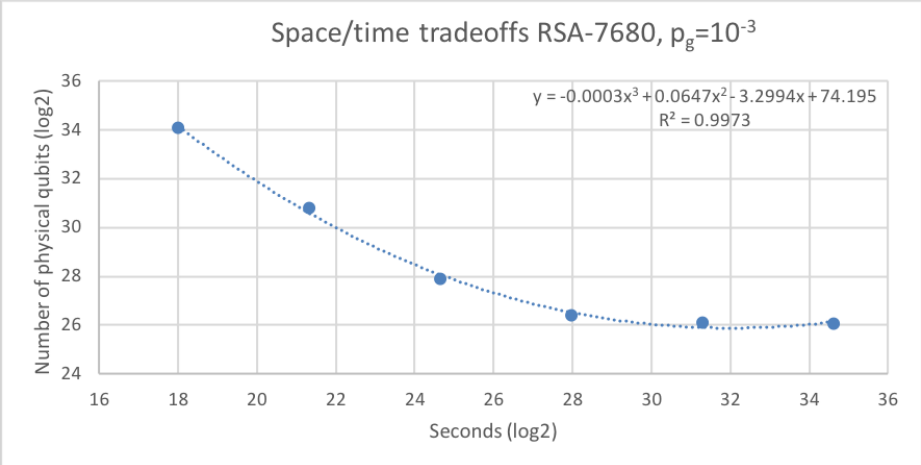

Fig. 10. RSA-7680 space/time tradeoffs with physical error rate per gate $p_g = 10^{-3}$. The scale is logarithmic (base 2). Approximately $y(16.3987) \approx 7.70 \times 10^{10}$ physical qubits are required to break the scheme in one day (24 hours). The number of T gates in the circuit is 1.27×10^{14}, the corresponding number of logical qubits is 15362, and the total number of surface code cycles is 2.64×10^{16}. The classical security parameter is approximately 192 bits.

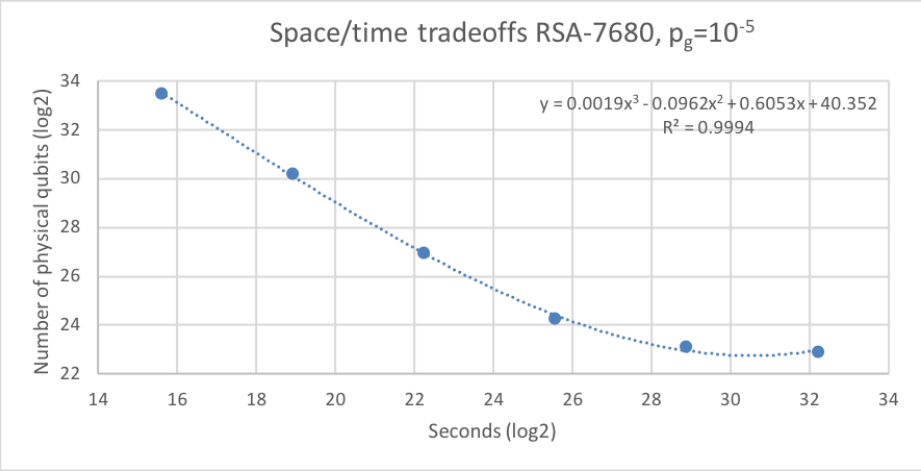

Fig. 11. RSA-7680 space/time tradeoffs with physical error rate per gate $p_g = 10^{-5}$. The scale is logarithmic (base 2). Approximately $y(16.3987) \approx 7.41 \times 10^{9}$ physical qubits are required to break the scheme in one day (24 hours). The number of T gates in the circuit is 1.27×10^{14}, the corresponding number of logical qubits is 15362, and the total number of surface code cycles is 2.47×10^{16}. The classical security parameter is approximately 192 bits.

3.6 RSA-15360

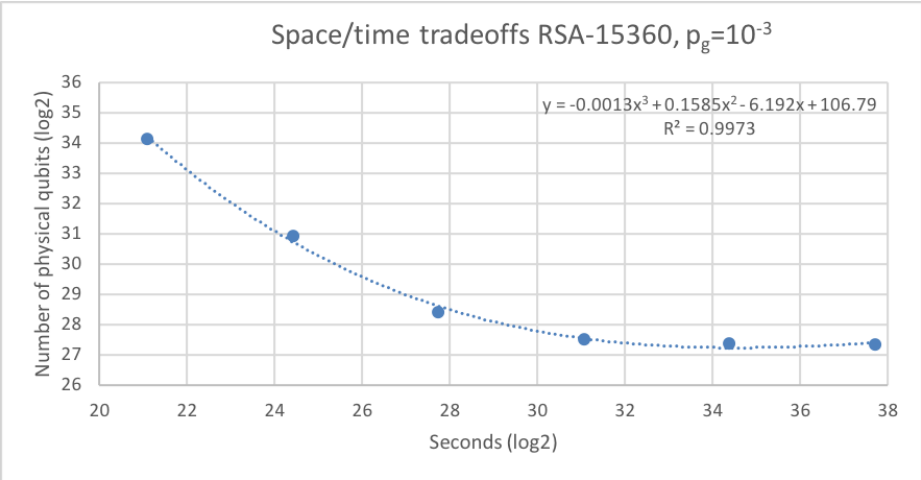

Fig. 12. RSA-15360 space/time tradeoffs with physical error rate per gate $p_g = 10^{-3}$. The scale is logarithmic (base 2). Approximately $y(16.3987) \approx 4.85 \times 10^{12}$ physical qubits are required to break the scheme in one day (24 hours). The number of T gates in the circuit is 1.01×10^{15}, the corresponding number of logical qubits is 30722, and the total number of surface code cycles is 2.24×10^{17}. The classical security parameter is approximately 256 bits.

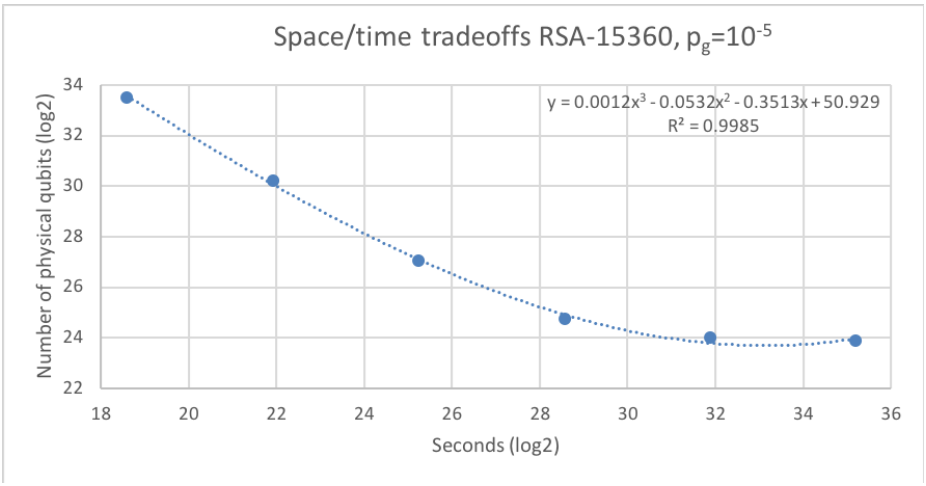

Fig. 13. RSA-15360 space/time tradeoffs with physical error rate per gate $p_g = 10^{-5}$. The scale is logarithmic (base 2). Approximately $y(16.3987) \approx 7.64 \times 10^{10}$ physical qubits are required to break the scheme in one day (24 hours). The number of T gates in the circuit is 1.01×10^{15}, the corresponding number of logical qubits is 30722, and

the total number of surface code cycles is 1.98×10^{17}. The classical security parameter is approximately 256 bits.

4 Elliptic curve schemes

In the following section we compute the space/time tradeoffs for attacking public-key cryptographic schemes based on solving the discrete logarithm problem in finite groups generated over elliptic curves, namely NIST P-160, NIST P-192, NIST P-224, NIST P-256, NIST P-384 and NIST P-521. For each scheme, we plot the space/time tradeoff points then fit it with a third degree polynomial, for $p_g = 10^{-3}$ and $p_g = 10^{-5}$, respectively. We used the logical circuits from [17].

4.1 NIST P-160

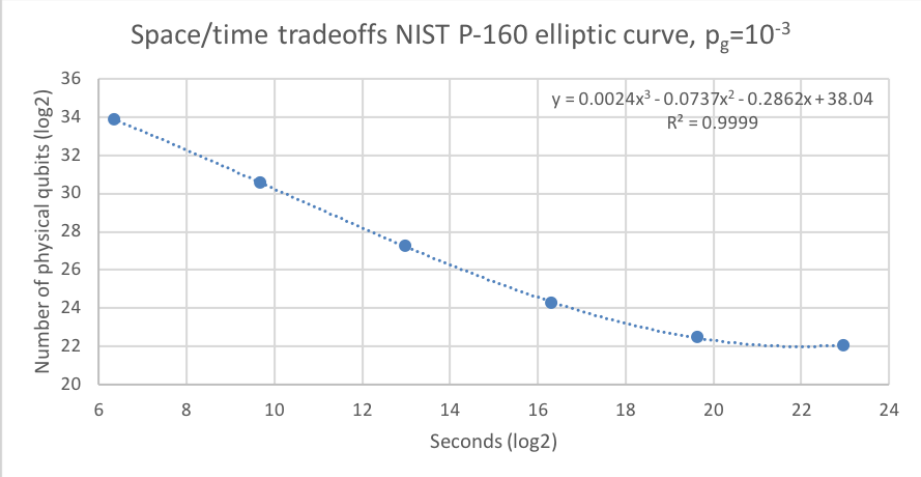

Fig. 14. NIST P-160 elliptic curve space/time tradeoffs with physical error rate per gate $p_g = 10^{-3}$. The scale is logarithmic (base 2). Approximately $y(16.3987) \approx 1.81 \times 10^7$ physical qubits are required to break the scheme in one day (24 hours). The number of T gates in the circuit is 2.08×10^{11}, the corresponding number of logical qubits is 1466, and the total number of surface code cycles is 4.05×10^{13}. The classical security parameter is 80 bits.

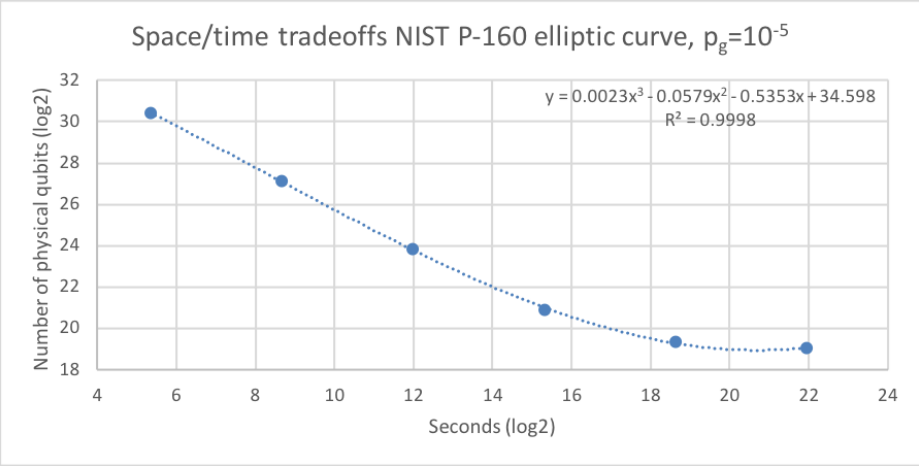

Fig. 15. NIST P-160 elliptic curve space/time tradeoffs with physical error rate per gate $p_g = 10^{-5}$. The scale is logarithmic (base 2). Approximately $y(16.3987) \approx 1.38 \times 10^6$ physical qubits are required to break the scheme in one day (24 hours). The number of T gates in the circuit is 2.08×10^{11}, the corresponding number of logical qubits is 1466, and the total number of surface code cycles is 2.03×10^{13}. The classical security parameter is 80 bits.

4.2 NIST P-192

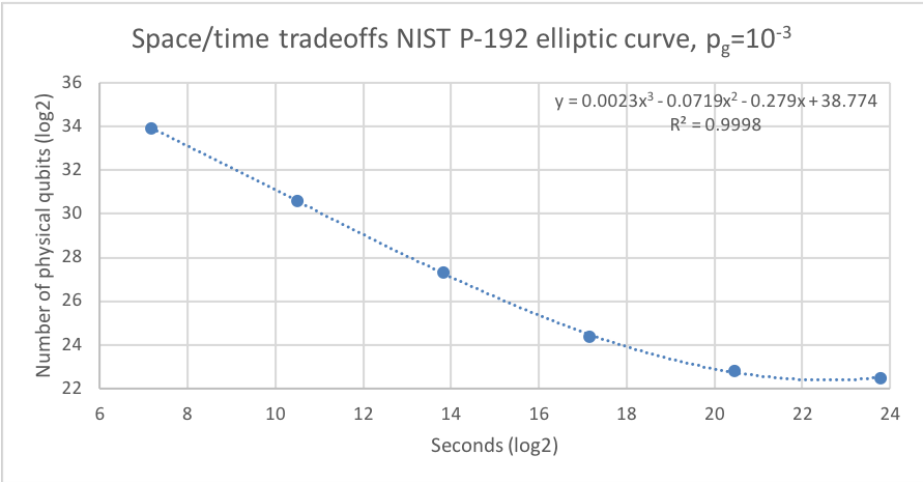

Fig. 16. NIST P-192 space/time tradeoffs with physical error rate per gate $p_g = 10^{-3}$. The scale is logarithmic (base 2). Approximately $y(16.3987) \approx 3.37 \times 10^7$ physical qubits are required to break the scheme in one day (24 hours). The number of T gates in the circuit is 3.71×10^{11}, the corresponding number of logical qubits is 1754, and

the total number of surface code cycles is 7.23×10^{13}. The classical security parameter is 96 bits.

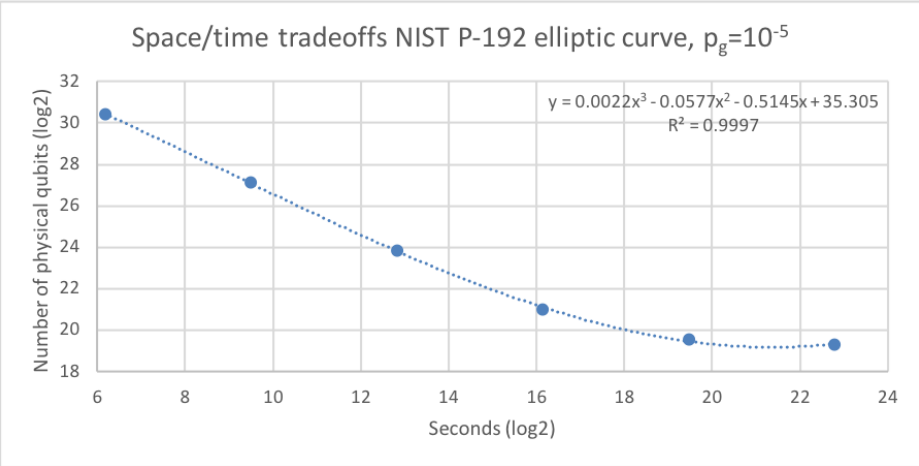

Fig. 17. NIST P-192 space/time tradeoffs with physical error rate per gate $p_g = 10^{-5}$. The scale is logarithmic (base 2). Approximately $y(16.3987) \approx 2.18 \times 10^6$ physical qubits are required to break the scheme in one day (24 hours). The number of T gates in the circuit is 3.71×10^{11}, the corresponding number of logical qubits is 1754, and the total number of surface code cycles is 3.62×10^{13}. The classical security parameter is 96 bits.

4.3 NIST P-224

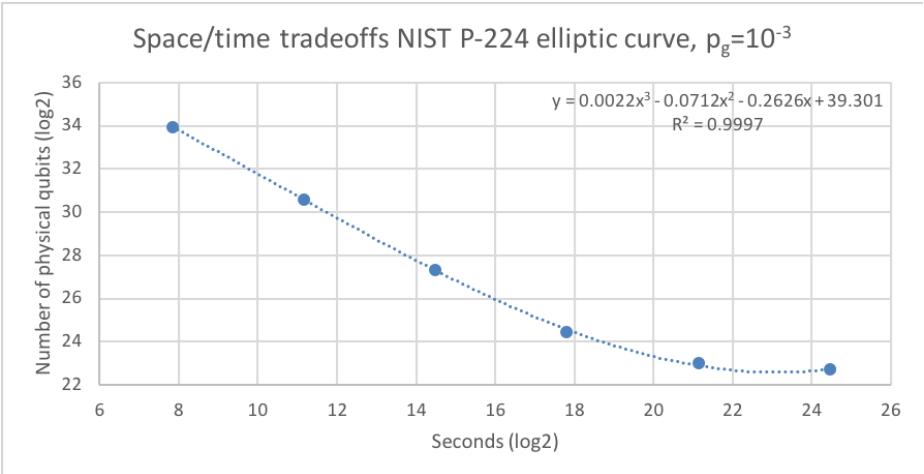

Fig. 18. NIST P-224 elliptic curve space/time tradeoffs with physical error rate per gate $p_g = 10^{-3}$. The scale is logarithmic (base 2). Approximately $y(16.3987) \approx 4.91 \times$

10^7 physical qubits are required to break the scheme in one day (24 hours). The number of T gates in the circuit is 5.90×10^{11}, the corresponding number of logical qubits is 2042, and the total number of surface code cycles is 1.15×10^{14}. The classical security parameter is 112 bits.

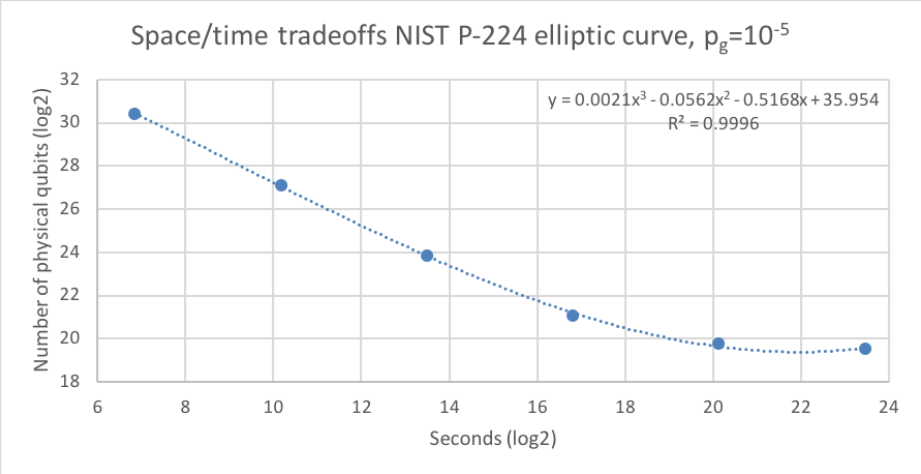

Fig. 19. NIST P-224 elliptic curve space/time tradeoffs with physical error rate per gate $p_g = 10^{-5}$. The scale is logarithmic (base 2). Approximately $y(16.3987) \approx 3.24 \times 10^6$ physical qubits are required to break the scheme in one day (24 hours). The number of T gates in the circuit is 5.90×10^{11}, the corresponding number of logical qubits is 2042, and the total number of surface code cycles is 5.75×10^{13}. The classical security parameter is 112 bits.

4.4 NIST P-256

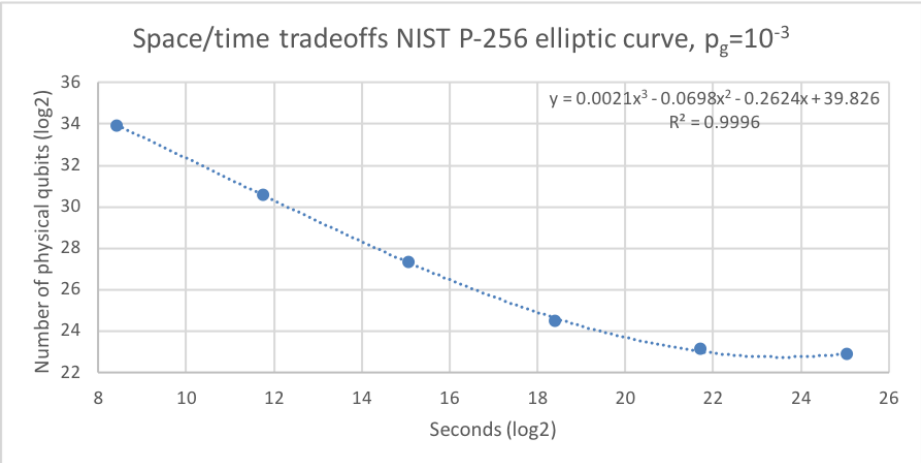

Fig. 20. NIST P-256 elliptic curve space/time tradeoffs with physical error rate per gate $p_g = 10^{-3}$. The scale is logarithmic (base 2). Approximately $y(16.3987) \approx 6.77 \times 10^7$ physical qubits are required to break the scheme in one day (24 hours). The number of T gates in the circuit is 8.82×10^{11}, the corresponding number of logical qubits is 2330, and the total number of surface code cycles is 1.72×10^{14}. The classical security parameter is 128 bits.

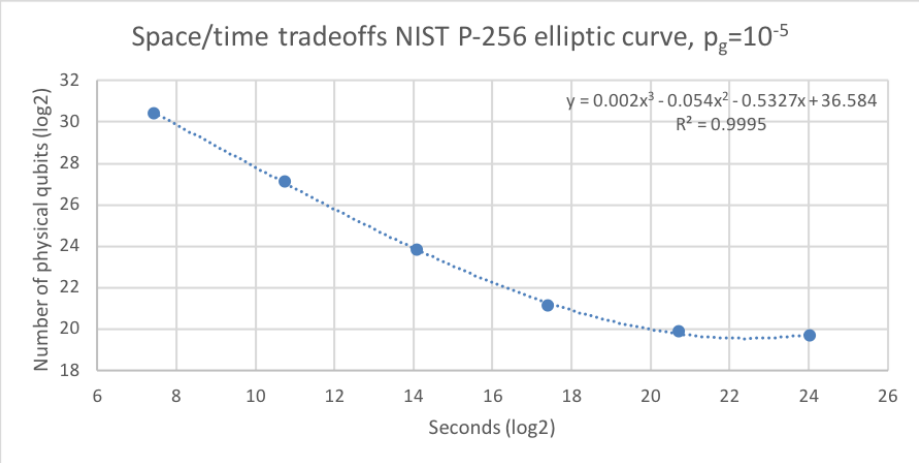

Fig. 21. NIST P-256 elliptic curve space/time tradeoffs with physical error rate per gate $p_g = 10^{-5}$. The scale is logarithmic (base 2). Approximately $y(16.3987) \approx 4.64 \times 10^6$ physical qubits are required to break the scheme in one day (24 hours). The number of T gates in the circuit is 8.82×10^{11}, the corresponding number of logical qubits is 2330, and the total number of surface code cycles is 8.60×10^{13}. The classical security parameter is 128 bits.

4.5 NIST P-384

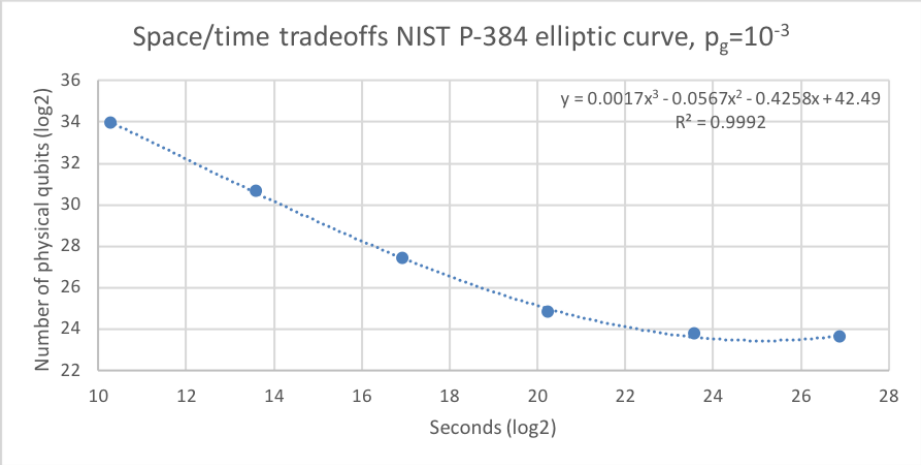

Fig. 22. NIST P-384 elliptic curve space/time tradeoffs with physical error rate per gate $p_g = 10^{-3}$. The scale is logarithmic (base 2). Approximately $y(16.3987) \approx 2.27 \times 10^8$ physical qubits are required to break the scheme in one day (24 hours). The number of T gates in the circuit is 3.16×10^{12}, the corresponding number of logical qubits is 3484, and the total number of surface code cycles is 6.17×10^{14}. The classical security parameter is 192 bits.

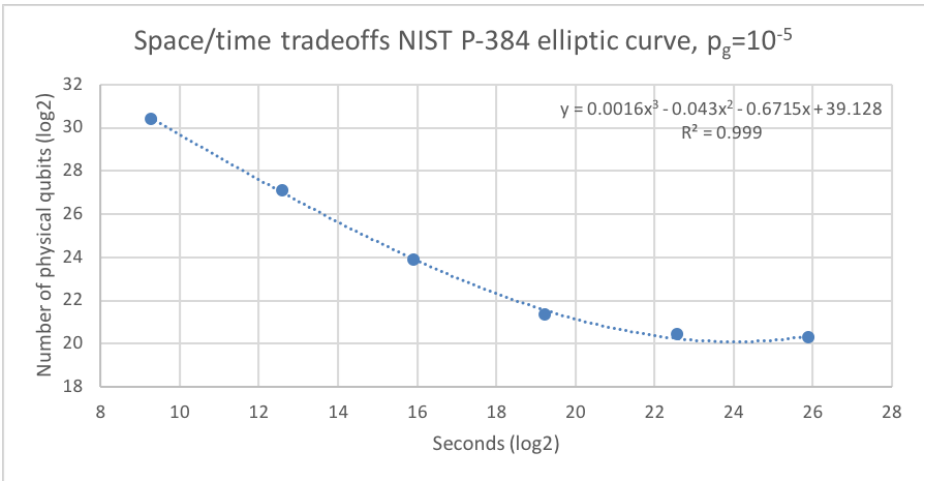

Fig. 23. NIST P-384 elliptic curve space/time tradeoffs with physical error rate per gate $p_g = 10^{-5}$. The scale is logarithmic (base 2). Approximately $y(16.3987) \approx 1.28 \times 10^7$ physical qubits are required to break the scheme in one day (24 hours). The number of T gates in the circuit is 3.16×10^{12}, the corresponding number of logical qubits is

3484, and the total number of surface code cycles is 3.08×10^{14}. The classical security parameter is 192 bits.

4.6 NIST P-521

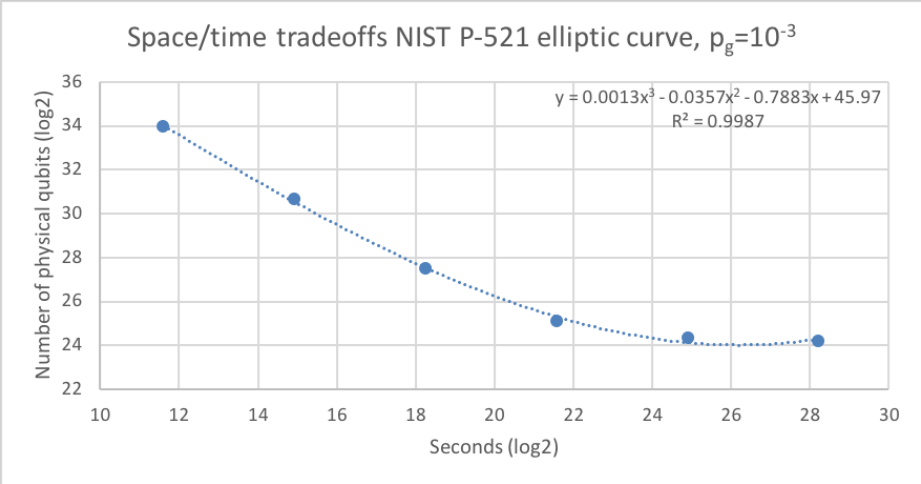

Fig. 24. NIST P-521 elliptic curve space/time tradeoffs with physical error rate per gate $p_g = 10^{-3}$. The scale is logarithmic (base 2). Approximately $y(16.3987) \approx 6.06 \times 10^8$ physical qubits are required to break the scheme in one day (24 hours). The number of T gates in the circuit is 7.98×10^{12}, the corresponding number of logical qubits is 4719, and the total number of surface code cycles is 1.56×10^{15}. The classical security parameter is 256 bits.

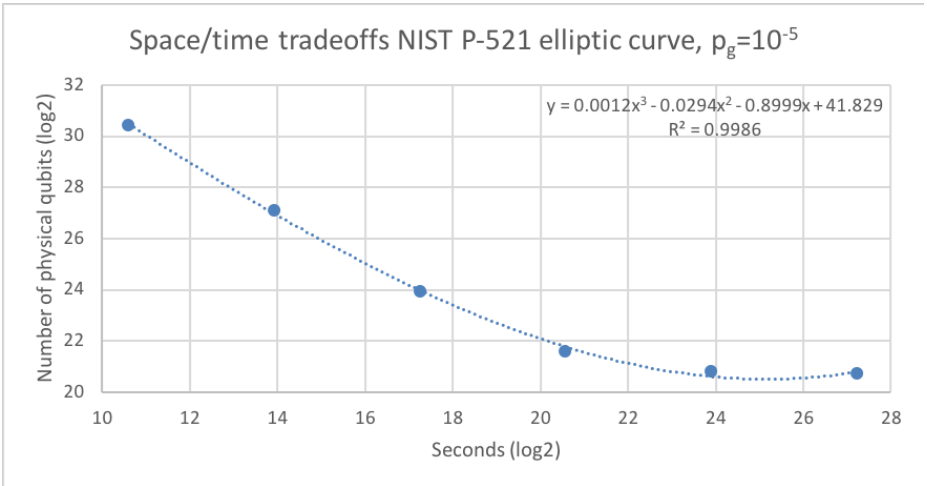

Fig. 25. NIST P-521 elliptic curve space/time tradeoffs with physical error rate per gate $p_g = 10^{-5}$. The scale is logarithmic (base 2). Approximately $y(16.3987) \approx 2.30 \times 10^7$ physical qubits are required to break the scheme in one day (24 hours). The number of T gates in the circuit is 7.98×10^{12}, the corresponding number of logical qubits is 4719, and the total number of surface code cycles is 7.78×10^{14}. The classical security parameter is 256 bits.

5 Asymmetric cryptography and hash functions

In comparison to surface code defects and braiding methods [13], lattice surgery techniques [1,2,3] mostly impact the physical footprint of the fault-tolerant layer required to run a specific quantum algorithm, reducing the distillation overhead by approximately a factor of 5. The temporal overhead (i.e. the number of surface code cycles) is reduced less drastically. For this reason, lattice surgery has less significant effects in estimating the security of symmetric schemes or hash functions, reducing the security parameter by at most 1 and decreasing the spatial overhead by at most a factor of 5. Therefore all of the results obtained before in [4,5] are mostly unchanged, except for the spatial overhead as mentioned before.

6 Conclusions and future directions

We analyzed the security of asymmetric (public-key) cryptography, in particular RSA and ECC, in the light of new improvements in fault-tolerant quantum error correction based on surface code lattice surgery techniques. We used more conservative (from a quantum computing perspective) error correction parameters, such as a physical error rate of 10^{-3}, in comparison with 10^{-5} used in our previous reports (which is more conservative from a cybersecurity perspective). We computed the space/time tradeoff required to attack every scheme. We fitted the data with a third degree polynomial, which resulted in an analytical formula of the number of qubits required to break the scheme as a function of time.

Note that the physical footprints in this report seem to be higher than the ones presented in our previous report [12] (which used surface code defects and braiding techniques instead of lattice surgery techniques used in this report). This is because in [12] we excluded from the footprint calculation the space required by magic state distillation (which represents roughly 90% of the total footprint), whereas in this report we included the total footprint.

In Table 1 we compare our current estimates with the total physical footprint following from our previous results in [12] with the magic state factories also included in the total footprint.

Recent developments in the theory of fault-tolerant quantum error correction have great impact on evaluating the effective strength of cryptographic schemes against quantum attacks, as the fault-tolerant layer of a quantum computation is the most resource-intensive part of running a quantum algorithm. Therefore,

Scheme name	Physical footprint (old estimates)	Physical footprint (new estimates)
RSA-1024	1.17×10^7	2.14×10^6
RSA-2048	5.18×10^7	9.78×10^6
RSA-4096	3.19×10^8	5.70×10^7
NIST P-160	7.43×10^6	1.38×10^6
NIST P-192	1.15×10^7	2.18×10^6
NIST P-256	2.54×10^7	4.64×10^6
NIST P-521	1.15×10^8	2.30×10^7

Table 1. Comparison of total physical footprints required (including magic state factories) to break the underlying scheme in 24 hours using techniques based on defects and braiding (old estimates) versus techniques based on lattice surgery (new estimates). We assume a physical error rate per gate $p_g = 10^{-5}$ and a surface code cycle time of 200 ns. One can observe a net reduction in the total physical footprint when using techniques based on lattice surgery.

monitoring the advances in the theory of quantum error correction is of crucial importance when estimating the strength (or weakness) of a cryptographic scheme against a quantum adversary. In the future we plan to use the most up-to-date fault-tolerant optimization techniques to re-evaluate the security of all cryptographic schemes analyzed so far.

Acknowledgements

Vlad Gheorghiu thanks Austin Fowler for helpful discussions and clarifications regarding lattice surgery methods.

References

1. Fowler, A.G., Gidney, C.: Low overhead quantum computation using lattice surgery (2018), arXiv:1808.06709 [quant-ph]
2. Litinski, D.: A Game of Surface Codes: Large-Scale Quantum Computing with Lattice Surgery (2018), arXiv:1808.02892 [quant-ph]
3. Horsman, C., Fowler, A.G., Devitt, S., Meter, R.V.: Surface code quantum computing by lattice surgery. New Journal of Physics 14(12), 123011 (2012), http://stacks.iop.org/1367-2630/14/i=12/a=123011
4. 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
5. Gheorghiu, V., Mosca, M.: A resource estimation framework for quantum attacks against cryptographic functions (part 3) (2017), Global Risk Institute quantum risk assessment report, Aug. 2017 - Feb. 2018
6. 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
7. Zalka, C.: Grover's quantum searching algorithm is optimal, e-print arXiv:quant-ph/9711070

8. 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
9. 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)
10. Koblitz, N.: Elliptic curve cryptosystems. Math. Comp. 48, 203–209 (1987)
11. 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
12. 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
13. 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
14. Fowler, A.G., Devitt, S.J., Jones, C.: Surface code implementation of block code state distillation. Scientific Reports 3, 1939 EP – (06 2013), http://dx.doi.org/10.1038/srep01939
15. Nielsen, M.A., Chuang, I.L.: Quantum Computation and Quantum Information. Cambridge University Press, Cambridge, 5th edn. (2000)
16. Bravyi, S., Haah, J.: Magic-state distillation with low overhead. Phys. Rev. A 86, 052329 (Nov 2012), http://link.aps.org/doi/10.1103/PhysRevA.86.052329
17. Roetteler, M., Naehrig, M., Svore, K.M., Lauter, K.: Quantum resource estimates for computing elliptic curves discrete logarithms (2017), arXiv:1706.06752 [quant-ph]
18. Barenco, A., Bennett, C.H., Cleve, R., DiVincenzo, D.P., Margolus, N., Shor, P., Sleator, T., Smolin, J.A., Weinfurter, H.: Elementary gates for quantum computation. Phys. Rev. A 52, 3457–3467 (Nov 1995), http://link.aps.org/doi/10.1103/PhysRevA.52.3457
19. Cuccaro, S.A., Draper, T.G., Kutin, S.A., Moulton, D.P.: A new quantum ripple-carry addition circuit. arXiv preprint quant-ph/0410184 (2004), http://arxiv.org/abs/quant-ph/0410184
20. Beauregard, S.: Circuit for shor's algorithm using 2n+3 qubits. Quantum Info. Comput. 3(2), 175–185 (Mar 2003), http://dl.acm.org/citation.cfm?id=2011517.2011525