Dismantling the Quantum Threat

Masterarbeit

zur Erlangung des akademischen Grades Master of Science im Studiengang Security Managment an der Technischen Hochschule Brandenburg

Vorgelegt von:
Tilman Runge

Betreuer: Prof. Dr. Ivo Keller
Zweitgutachter: Dr. Heinrich Lücken

Berlin, 6. Dezember 2022

Table of Contents

List of illustrations

List of Tables

List of abbreviations

APT	Advanced Persistent Threat
BQP	Bounded Error Quantum Polynomial Time
CCS	Combined Charging System plug
CHAdeMO	CHArge de Move plug
CRL	Certificate revocation lists
CS	Charging Station
CSMS	Charging Station Management System
CSO	Charging Station Operator
CIA	Confidentiality, Integrity, Availability
DH	Diffie-Hellman Algorithm
DREAD	Damage, Reproducibility, Exploitability, Affected users, Discoverability
DSA	Digital Signature Algorithm
ECDH	Elliptic-Curve-Diffie-Hellman Algorithm
ECDSA	Elliptic-Curve Digital Signature Algorithm
EV	Electric Vehicle
EVSE	Electric Vehicle Supply Equipment
HDNL	Harvest-now-decrypt-later attack
IoT	Internet of Things
MaDIoT	Manipulation of Demand via IoT
MITM	Man-in-the-middle
NIST	National Institute of Standards and Technology
OCPP	Open Charge Point Protocol
OCSP	Online Certificate Status Protocol
OTA	Over the air

OTR	Off-the-Record Messaging
PCS	Post Compromise Security
PFS	Perfect Forward Secrecy
PKI	Public Key Infrastructure
PQC	Post-Quantum Cryptography
QCaaS	Quantum Computing as a Service
ROI	Return-on-investment
SC	Surface Code
SNDL	Store-now-Decrypt-Later attack
STRIDE	Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of Privilege
TA	Threat Actors
TAL	Threat Agent Library
TLS	Transport Layer Security
RSA	Rivest-Shamir-Adleman Algorithm
VPN	Virtual Private Network
VQFA	Variational Quantum Factoring Algorithm
X3DH	Extended Triple Diffie-Hellman
Y2Q	Year to Quantum

1 Introduction

1.1 Quantum Threat

Ever since Peter Shor published in 1994 his ground-breaking algorithm for fast prime factorization using quantum computers[1], public-key cryptography is facing the opening of its very own pandora's box with the new potential to reconstruct the private keys that are used for decrypting and signing messages. Although asymmetric (or public-key) cryptography is only one of several areas of cryptography and the only one severely affected, it may still be seen as one of the most critical ones and its failure could bring about a cascade of effects on a multitude of use cases.
Beyond securing private individuals' communication when surfing the internet, using mobile messaging, or using wireless internet, asymmetric cryptography is also used by an abundance of cyber-physical systems surrounding us and permeating our world, such as Internet of Things (IoT) devices and in a variety of increasingly digitalized fields such as automotive, railway, aviation, and energy.
Indeed, if the guarantees of asymmetric cryptography, which go beyond mere confidentiality but also provide for integrity and authentication, were to fail then attackers might not only be able to passively sniff and decrypt data but also intervene actively. This might create for unauthorized third parties the opportunity to decrypt encrypted communication (both private as well as institutional or commercial) or to disrupt the infrastructures such as the energy grid, production, attack financial institutions, or abuse modern operating system's update mechanisms to inject malware on a large scale.

This threat posed by quantum computers receives attention both in research and media, where it is often reported with alarming undertones and discussion depth tends to be shallow:

- *The race to save the Internet from quantum hackers* (Nature)[2]

[1] Shor 1994.
[2] Castelvecchi 2022.

- *Inside the fight to protect your data from quantum computers* (Scienceline)[3]
- *Quantum computers will crack your encryption—maybe they already have* (Cisco)[4]

Other articles demonstrate, presumably unwittingly, the complexity of the field and how hard it can be to come to conclusions that can be generalized:

- *Quantum computers may be able to break Bitcoin sooner than you think* (Techradar)[5]
- *Here's Why Quantum Computing Will Not Break Cryptocurrencies* (Forbes)[6]
- *Quantum computing will doom us. And only quantum computing can save us* (Techgenix)
- *Waiting for quantum computing: Why encryption has nothing to worry about* (Techbeacon)[7]

As the public sphere is generally missing a deeper understanding of both quantum computing and its often-complex applications it is not surprising to see commonly held expectations of the capabilities and readiness of quantum computers to be inflated[8]. This is a particular issue for the popularized reception of primary research literature where exceptional quantum computing achievements are reported that unfortunately come to exist only under specific circumstances not representative of real-life[9].

Secondary literature often treats concepts such as "breaking IT systems" or "quantum computer capable of cracking encryption" on a superficial level, leading to alarming conclusions that turn out not to hold up upon closer examination. The breakability of asymmetric encryption algorithms (such as RSA and DH) cannot instantly be equated with the breakability of complex real-world use cases (e.g. web browsing, encrypted email) as they build upon multiple layers of protocols, algorithms and safeguards. The intricacies of protocol implementation and the presence of an effective defense-in-depth application design need to be considered, as they can make all the difference between a collapse of security or resilience when under attack.

For this reason, the evaluation of the "quantum threat" needs to consider not just the intersection of quantum computing and cryptography but also the intersection

[3] Leonard 2022.
[4] Deign 2022.
[5] Khalili 2022.
[6] Huang 2020.
[7] Martin 2018.
[8] Beaudrap 2018.
[9] For examples see Grieu 2022.

of cryptography, protocols and applications to enable an end-to-end understanding of the prerequisites required for successfully breaking the real-life applications that build upon cryptography.

One of the still unaccomplished prerequisites for breaking asymmetric cryptography, is the availability of a sufficiently potent quantum computer. Although quantum computing research has made significant advancement in the past decade and further improvement is to be expected, the current performance and capabilities still need to be improved notably before present-day cryptography can be attacked on quantum computing with acceptably long run times. As of today, no reliable estimate was given if and when such an attack will be feasible and thus a breakout scenario for the quantum threat will materialize. However, it has been widely agreed that this point in time still is “at least 10 years from now”[10].
Furthermore, the popularized idea of “quantum disruption”[11] that frames the breakout scenario as a “Q-Day”[12] upon which “current encryption technologies will be neutralized”[13] by a potent quantum computer needs to be challenged in two aspects. First, the definition of what constitutes a “potent quantum computer” depends on various other variables, such as the length of the key to be broken and the time available to do so. Two, unlike the commercial release of a new smartphone from one day to the other will the availability of potent quantum computers likely be more a gradual process, becoming available to well-equipped organizations first before a larger audience can access, let alone own them. Here it is essential to examine which threat actors will likely have first access to this capability and what for they will use it.

1.2 Post-Quantum Cryptography

While the availability of capable quantum computers is still in an undetermined future, efforts are already taken to mitigate their eventual impact on asymmetric cryptography. There are two alternatives to the vulnerable algorithms: First, quantum cryptography can replace conventional cryptography and does not suffer from the same vulnerabilities. Quantum cryptography has already been successfully implemented in experimental environments and is on its way

[10] Grimes 2020.
[11] Sethi 2022.
[12] Nguyen 2022.
[13] Ibid.

becoming a robust technology. As its function is based on quantum mechanical effects, there are substantial physical and engineering challenges for integration into conventional digital devices (e.g. smartphones, IoT devices). For this reason, quantum cryptography is not discussed in-depth as a viable alternative.
Second, a new class of cryptographic protocols called Post-quantum Cryptography (PQC) constructed to be intrinsically invulnerable against quantum computing-based attacks, is a more likely solution to the quantum threat. Unfortunately, the field of PQC algorithms only offers limited options that come with various downsides related to performance, implementation incompatibilities and possible, only later to be detected, security issues. As with the yet unknown quantum computer development trajectory, it is hard to reliably predict which PQC algorithms will succeed in the long run. For this reason, an overzealous, imprudent and premature substitution of conventional public-key cryptography with novel PQC algorithms may thus at best degrade performance and at worst create new security problems. Therefore, as of 2022 conventional public-key cryptography cannot easily be replaced without introducing new, substantial issues.

The lack of options to defend against future quantum computing attacks creates already today challenges for some applications of cryptography:
Especially those industries are impacted that rely on distributed systems or where certain products are expected to reach a lifespan that can exceed the timespan necessary to develop a capable quantum computer. Examples of these industries and products are automobility, rail, energy and telecommunication. While deployed cryptographic algorithms could in theory be updated, it is questionable whether updates will find their way into these long-life products decades after being developed. Likewise affected will be technological ecosystems and protocols where innovation is hard to achieve due to decentralization[14] and the process of replacing cryptographic algorithms may take longer than the time necessary to develop capable quantum computers.

1.3 Contributions

This thesis' main contribution is to provide a better understanding of the quantum threat and potential breakout scenarios, which threat actors may attack real-world use cases initially, and which countermeasures can be used.

[14] Marlonspike 2020.

To achieve this, this thesis contemplates some general aspects of quantum computing-based attacks on conventional asymmetric cryptography to apply these insights later on a selected case study where an attacker uses quantum computing to break into electronic vehicle charging infrastructure to then destabilize the national power grid.

The thesis focuses on four central questions:

1) What quantum computing resources are required to successful break conventional asymmetric cryptography?
2) Once quantum computers approach the capability to break conventional asymmetric cryptography, which potential quantum breakout scenarios exist?
3) Based on the potential quantum breakout scenarios, which threat actors will obtain the attack capability when and what is their motivation to use it?
4) How can quantum computers be used to attack the power grid via remote-controlled electric vehicle charging infrastructure and what possible remedies exist?

1.4 Procedure

One significant objective of this contribution is to establish a comprehension of the real-life implications of the quantum threat and current state of research without presupposing previous in-depth knowledge of quantum mechanics, quantum algorithms and mathematics. For this reason, the ideas and work discussed in this thesis cover specific topics like quantum mechanics or Shor's algorithm only so much as it is a mandatory prerequisite for the research questions and has not already been covered more in-depth elsewhere, as for example the excellent and comprehensive discussion of the current state of quantum computing by the German Federal Office for Information Security[15].
Similarly, only such solutions to the quantum threat will be contemplated that can be considered realistic solutions as of today and for the approximate future. Therefore, no solutions involving quantum cryptography are considered as these technologies in turn are not a commercially viable option for most use cases.
A particular focus is made on the capabilities of quantum computers to break public RSA keys by means of factorization. Although other asymmetric algorithms such as Diffie-Hellman (DH), El-Gamal or elliptic-curve cryptography are not

[15] Federal Office for Information Security 2020.

based on the factorization problem but instead on the discrete logarithmic problem, their vulnerability is not discussed separately as it is widely accepted that they are equally breakable by Shor's algorithm with comparable computing requirements.[16]

The context and character of the quantum threat and the associated challenges have already been outlined in chapter 1 and shall be explored more in-depth in the upcoming chapters. To facilitate the exploration of the main questions an analysis will be applied with the objective to determine whether the advent of capable quantum computers poses a risk for a particular use case, and through which vector the use case could be attacked.
For this analysis, various related topics need to be incorporated and discussed before a conclusion can be made for which type of attacks will be observed and which use cases will be at risk. Figure 1 portrays the interrelatedness of the relevant topics.

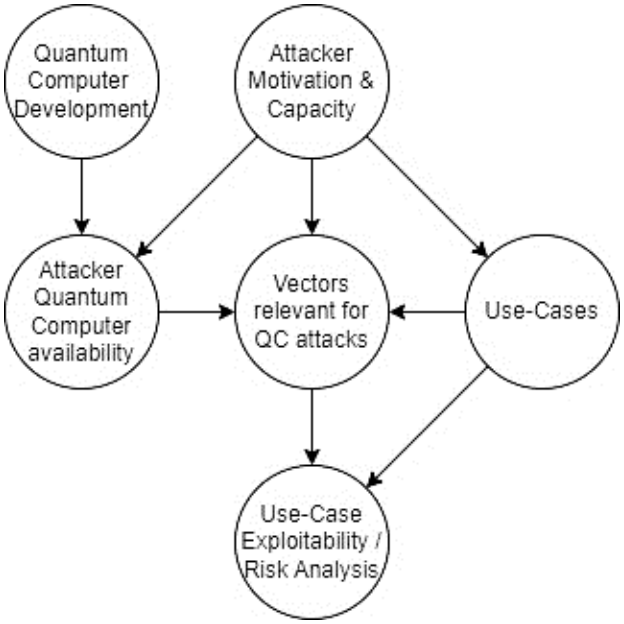


Figure 1: Interrelated topics to be discussed as part of this thesis.

Chapter 2 provides more context to the quantum threat and looks at the current state of factorization using quantum computers and the challenges to be solved for further development of quantum computers. An essential result of this discussion will be a better understanding of the otherwise unspecific notion of a "capable quantum computer", i.e., a quantum computer with the capability to attack public-key cryptography.

[16] Grimes 2020, Gidney et al. 2021.

Chapter 3 builds upon chapter 2's insights on what a "capable quantum computer" entails to develop and compare different quantum development trajectories and associated breakout scenarios and stages. The resulting breakout scenarios and stages can later be used to differentiate the quantum computer availability for different threat actors.

Chapter 4 presents a typology of threat actors and their respective attack motivations and resources. The threat actors' resources are matched with the quantum computing availability stages defined in chapter 3 to deduct which threat actors will be the forerunners in using quantum computing to attack cryptography.

Chapter 5 combines the previous chapters' conclusions to describe a realistic attack vector that a state-level threat actor might exploit to attack national power grids. Here the link is made between quantum computing requirements from chapter 2 and 3, the potential threat actors with the necessary motivation and resources to fulfill these requirements to then show how and where a real-world infrastructure would be vulnerable to quantum computing-based attacks.

Chapter 6 then provides an overview of different security controls that can be implemented to lower the risk of quantum computing-based attacks. These security controls explicitly go beyond the Post-quantum Cryptography frequently cited in this context to showcase that further remediation options exist. Each type of security control is evaluated against the showcased example from chapter 5 to determine the usefulness of the security control.

Chapter 7 summarizes this thesis' findings and concludes the chapters and the discussed topics.

2 The Quantum Threat on Cryptography

2.1 Quantum computing

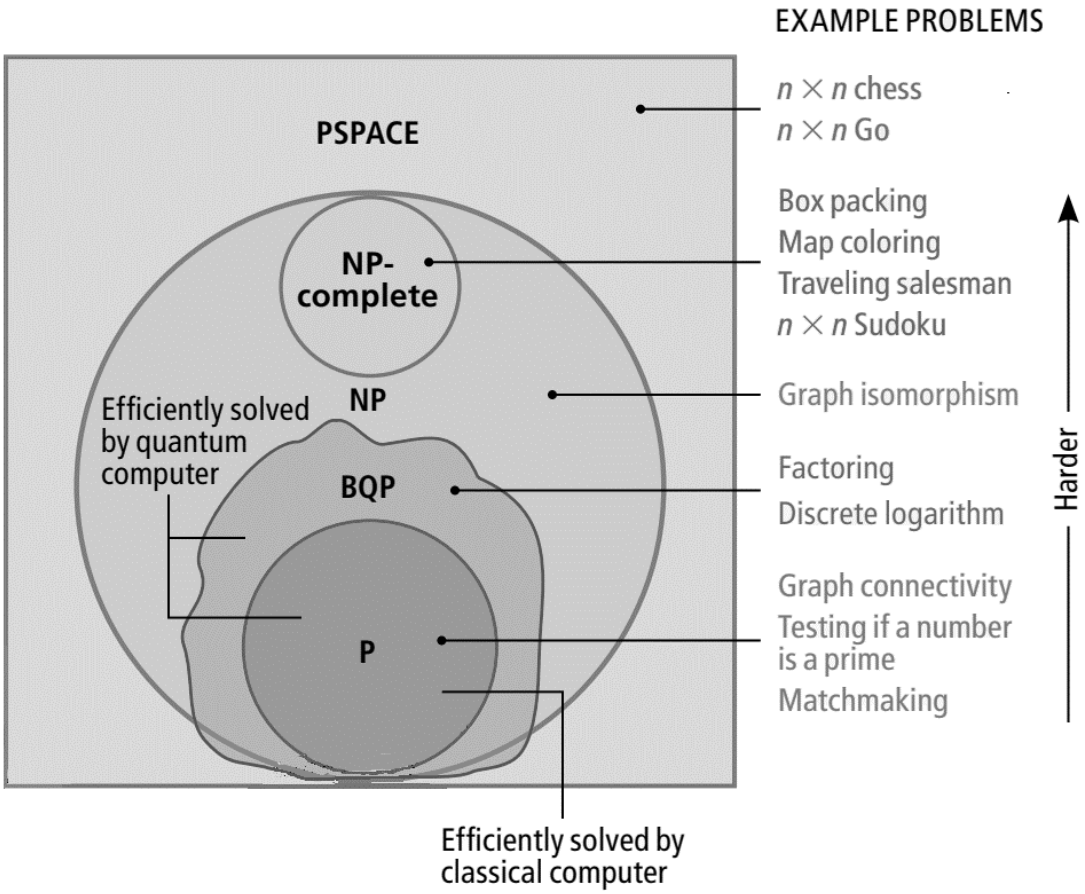
The unique capabilities evolving from computing using quantum mechanical effects enable the quantum threat. Of particular interest here are the effects of superposition and entanglement of quantum particles: Superposition refers to the effect where a particle‘s state is only determined once it is measured, before this moment it simultaneously exists in all possible states. Entanglement refers to the effect where one particle’s state becomes dependent on a different particle’s state. This holds true even when the particles are distanced from each other and without an observable communication channel between them[17], evidence strongly suggests that entanglement cannot be explained by covert communication channels[18].

It is a common misunderstanding that quantum computers are merely a faster version of classical computers, replacing them eventually and making it possible to run the same computations in less time[19]. Instead, quantum computers employ superposition and entanglement effects to allow calculations that are not possible with classical computing, thereby enabling new solution paths that are faster to complete. For these calculations quantum computers use “qubits”: whereas a classic computer uses binary bits, represented by electric or light impulses, qubits are based, depending on the type of quantum computer, on different types of particles for which quantum mechanical effects can be observed, such as trapped ions, photons, neutral atoms and other.[20]

Quantum computers and qubits can therefore be realized in quite different ways, each with their own development challenges to be solved. A discussion of these developmental challenges is due to the required comprehension of quantum physics, informatics and engineering vastly beyond the scope of this thesis, the interested reader can find a further discussion in the aforementioned research review of the Federal Office for Information Security[21].

[17] Lindsay 2020.
[18] Just 2021.
[19] Wallden and Kashefi 2019.
[20] Federal Office for Information Security 2020.
[21] Ibid.

Using qubits, a specific class of problems namely the “bounded error quantum polynomial time” (BQP) can be solved faster than with classical computers[22].



Source: Aaronson 2008.

Figure 2: Spaces of problems

Various real-world problems belonging to the BQP class exist, such as optimization, simulation, search, or factorization, that can benefit from a speed-up that quantum computing provides over classical computing.

Conventional cryptography also relies on problems for which quantum computing provides sped-up solutions. This concerns hashing, symmetric and asymmetric (i.e., public key) cryptography although only the latter is significantly impacted. Hashing (e.g., SHA) and symmetric cryptography (e.g. AES) can be attacked using Grover’s algorithm which is does so by accelerating the search for the correct key or pre-image[23]. Therefore, Grover’s algorithm is not an attack on the mathematical foundation of hashes or symmetric cryptography but a sped-up brute-force attack. It is also for this reason, that the concept of hashes and symmetric cryptography is vulnerable to Grover’s algorithm but not the specific

[22] Wallden and Kashefi 2019.
[23] Federal Office for Information Security 2020.

hashing and symmetric cryptography algorithms themselves. Thus, it is impossible to mitigate this vulnerability by improving or replacing insecure hashing or symmetric cryptography algorithms. Nevertheless, using Grover to attack hashes and symmetric cryptography is only of limited practical use: The speed up of finding a key or the hash pre-image is only quadratic but not exponential, as with Shor. A quadratic speed up can be mitigated by doubling key lengths, a measure easily implemented with conventional cryptography without having to devise and roll out new algorithms.[24] Although symmetric cryptography is relatively resilient against quantum computing-based attacks, it very often co-exists in hybrid schemes which combine symmetric with vulnerable asymmetric algorithms, rendering to entire implementation assailable.

For asymmetric or public-key cryptography, the vulnerability to Shor's algorithm is not a conceptual bug of asymmetric cryptography overall, instead it is specific to the mathematical problems employed by the currently used asymmetric cryptography algorithms. Therefore, mitigation can be achieved by updating these algorithms with quantum-proof ones, by the so-called class of post-quantum cryptography. The security of asymmetric cryptography algorithms in general relies on one-way trapdoor functions that are easy to compute into one direction (i.e. computations involving the public key) but hard to reverse unless a secret (i.e. the private key) is available. This asymmetry is derived from specific mathematical problems such as the prime factorization problem (for the RSA algorithm) and the discrete logarithm problem (for DH and others). Shor's algorithm can easily find solutions to both these problems and thereby compromise the security-guaranteeing asymmetry of these algorithms. Whereas factorizing a 2048-bit long RSA key using classical computation is currently estimated to take about 300 trillion years[25], a capable quantum computer theoretically might take as little as 8 hours[26].

To be precise, Shor's algorithm is not the only quantum algorithm targeting the prime factorization problem. Other algorithms, such as the variational quantum factoring algorithm (VQFA) can lead to the same goal, although through different routes. Whereas Shor's algorithm reformulates the factorization problem into a period-finding problem easily solved by quantum computers, the variational quantum factoring algorithm transforms the factorization problem into an optimization problem again easily solved by quantum computers. While various

[24] Ibid.
[25] Herman 2021.
[26] Gidney and Ekerå 2021.

quantum factorization algorithms have been proposed, only for some have the high-level functioning been translated into an actual, implementable quantum circuit, leaving the field with a number of theoretical, unprobed approaches of which not all are expected to scale with long key lengths[27]. Publications with new approaches to quantum factorization therefore need to be scrutinized closely for their practical relevance in a real-world setting outside the lab, as will be discussed next.

2.2 Shor's Algorithm

Some quantum algorithm's fundamental capacity for attacking asymmetric algorithms like RSA and DH have been experimentally proven. In 2001 a quantum computer successfully factorized the number 15 using Shor's algorithm[28]. In subsequent experimental studies it was attempted to factor larger numbers, in 2012 the integer 21 was factorized using Shor and in 2020 the integer 1,099,551,473,989 using a VQFA[29].

Number	# of factors	# of qubits needed	Algorithm	Year implemented	Implemented without prior knowledge of solution
15	2	8	Shor	2001 [2]	✗
	2	8	Shor	2007 [3]	✗
	2	8	Shor	2007 [3]	✗
	2	8	Shor	2009 [5]	✗
	2	8	Shor	2012 [6]	✗
21	2	10	Shor	2012 [7]	✗
143	2	4	minimization	2012 [1]	✓
56153	2	4	minimization	2012 [1]	✓

Source: Gidney et al. 2021.

Table 1: Quantum factorization records

It would seem reasonable to attribute the increased size of factorization to overall progress, this is however not necessarily the case. Notable with these records is that successful experimental factorization only is reported for a few specific integers but never a general capacity to factor all integers up until a certain size[30], as what would be the precondition for real-world relevance of attacking

[27] Federal Office for Information Security 2020.
[28] Crane 2019.
[29] Ibid.
[30] Grieu 2022.

asymmetric cryptography. The actual progress of each record is often enabled by optimizing the algorithm with prior knowledge of the solution and or selecting integers that are known to be easy to factorize for the given algorithm. Factorization records therefore usually cannot be generalized and instead have to be considered in the context of their respective research experiment and specific aspects such as the type of quantum computer used, the (combination of) algorithms used for factorization, optimization and selection of integers.

There is no evidence available that in the past 10 years any experimental advances were made for integer factorization using Shor purely. The factorization record for Shor thus remains at 21 (2012).[31] If the missing generalizability of the aforementioned records were to be set aside for a moment, some preliminary conclusions might be drawn about the breakability of asymmetric cryptography. For this, RSA with a 2048-bit key length has been considered in literature as the minimum usability benchmark for successfully attacking asymmetric cryptography[32], demarking the quantum threat "breakout scenario"[33]. If the record of factoring the integer 1,099,551,473,989 were to be generalized, i.e. all integers up until this length were to be factorizable, then the current achievement would imply that key lengths up until 41 bit could be attacked using a quantum computer, which is still well below the RSA 2048-bit benchmark key length.
Thus, substantial quantum computing advancements are still required to achieve a factorization power that can attack commonly employed key lengths. The question of how much advancement is needed is discussed in the following sections.

2.3 Requirements for quantum computers

Theoretically, a not particularly large number of qubits are required to run Shor's algorithm. The amount depends on the algorithm's implementation and optimization as well as the key bit length. A literature review updated last in 2020 by the German Federal Office for Information Security[34] compares various approaches to implementing the quantum factoring algorithm and estimations for the lower boundary minimum number of qubits required for factorization of any integer of n-bit length. Two studies stand out to give an appraisal of requirements:

[31] Grieu 2022.
[32] Lehto and Neittaanmäki 2022, p. 372.
[33] Grimes 2020.
[34] Federal Office for Information Security 2020.

Häner et al.[35] cites 2n+2 qubits (see table 4) and Gidney & Ekerå[36] with a different approach somewhat higher at approximately 3n.

n	Number of qubits	Number of Toffoli gates
1024	2050	$5.81 \cdot 10^{11}$
2048	4098	$5.20 \cdot 10^{12}$
3072	6146	$1.86 \cdot 10^{13}$
7680	15362	$3.30 \cdot 10^{14}$
15360	30722	$2.87 \cdot 10^{15}$

Source: Häner et al. 2017.

Table 2: Minimum number of qubits and gates required for factorizing n-bit long RSA keys

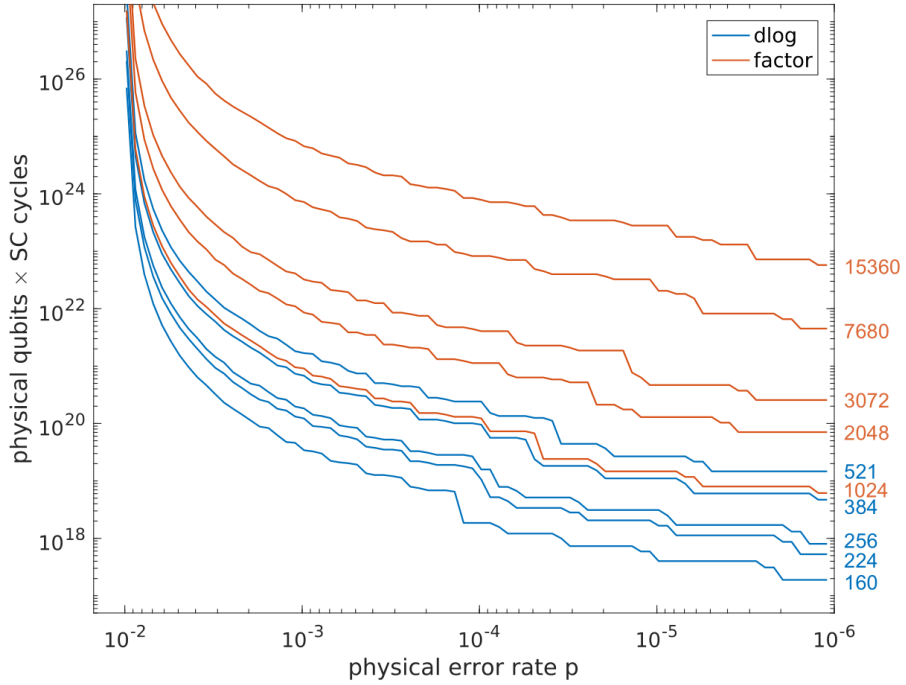
In practice however, quantum computers suffer from qubit state decoherence that causes measurement errors that need to be compensated, thereby driving up qubit count. The severity of qubit state decoherence is affected, among other variables, by the quality of the qubits which again depends upon the type of quantum computer which is why qubits can only be compared inadequately across different quantum computing platforms. Imperfect, “noisy” qubits need to be corrected before they can be used. Qubit error correction, a research field on its own, can be achieved by either re-running calculations or by combining multiple “noisy” qubits into perfect, logical qubits. Once dependable logical qubits are available, they can be used for computations. In the abovementioned study by Gidney & Ekerå a total of 20 million “noisy” physical qubits are needed to establish 14238 logical qubits (a relation of 1:1568), a number that can likely be lowered to some extend with further optimizations.

The time necessary to complete successful integer factorization represents an additional requirement that needs to be considered for breaking asymmetric cryptography. This contradicts the popularized idea that quantum computers can break asymmetric cryptography instantaneously[37]. Instead, the real-life situation is somewhat more complex: Running an algorithm requires the quantum mechanical manipulation of qubits by means of passing them through quantum logic circuits. These circuits contain gates and the number of gates to be passed or applied during one algorithm is often called circuit depth. Table 2 shows that the number of gates required increases roughly exponentially with key size. Simplistically expressed, each gate represents one clock cycle taking at least

[35] Häner et al. 2017.
[36] Gidney et al. 2021.
[37] For examples see: Grimes 2020, Herman 2021.

10ns, called the gate time. This time multiplied by the entirety of all gates to be passed for one run of the algorithm equals the total algorithm singular run time.[38]

It is possible to optimize an algorithm's implementation either towards the number of qubits required or the number of circuit steps. This space-time optimization[39] can enable a threat actor with access to a quantum computer with a low qubit number to still pursue an attack, provided they are willing to compensate for the low qubit number with a longer calculation time. The requirements for qubit count are further decreased if the length of the key to be broken is short, the qubit error rate is low and algorithm implementation has been optimized. Likewise, if a threat actor needs to break a private key in minutes or even seconds, extraordinarily high numbers of qubits must be available to allow for this calculation to succeed. This relationship between calculation time ("SC count"), physical qubit count, key size and qubit error rate is depicted in Figure 1:



Source: Federal Office for Information Security 2020, p. 124.

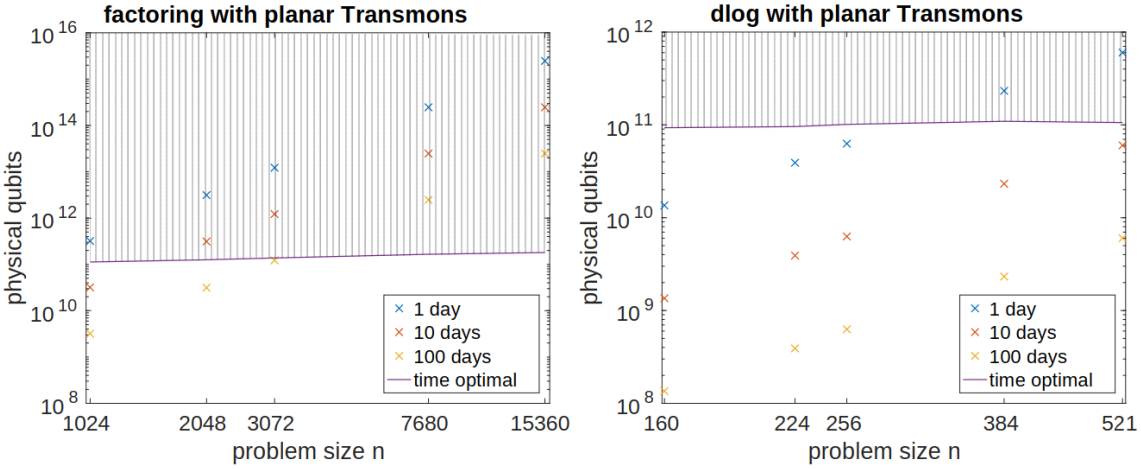
Figure 1: Required qubits*algorithm runs versus physical error rate for factorization

Depending on the specific quantum algorithm implementation, the calculation may not deliver the correct answer in 100% percent of the cases, making it necessary to repeat the calculation[40].

[38] Grimes 2020.
[39] Webber et al. 2021.
[40] Gidney et al. 2021.

Ultimately, the number of variables involved make it hard to reliably estimate the minimum number of qubits or runtime required in a real-world scenario. Not only is it hard to predict which type of quantum computer (e.g., solid-state versus ion-trap) will eventually be able to be scaled up to a large number of qubits easily or how qubit error levels will develop, but also future algorithmic advances and optimizations may or may not drive down qubit requirements.

Despite this lack of foreseeability, three estimates based on current research can be compared for a better appraisal of the approximate requirements. According to the German Federal Office for Information Security, a quantum computing setup using solid-state Josephson qubits and a planar transmon architecture, breaking 2048-bit RSA keys would take 100 days when 10 billion (10^{10}) qubits are available, 10 days with 100 billion (10^{11}) qubits available and 1 day with 1000 billion (10^{12}) qubits available[41].



Source: Federal Office for Information Security 2020.

Figure 3: Time required for breaking RSA and DH for different numbers of qubits available.

A second study from Gidney & Ekerå employs numerous optimizations on hardware, layout, error correction and algorithm to lower these requirements noticeably: The time required to break 2048-bit RSA keys would be approximately 5 hours with a 69% success rate (thus on average 8 hours) when 20 million ($2x10^6$) physical qubits are available[42]. Allowing more time for algorithm runtime can compensate for a lower number of available physical qubits, as table 3 shows. However, this relationship is not linear when using highly optimized implementations, as Gidney & Ekerå do.

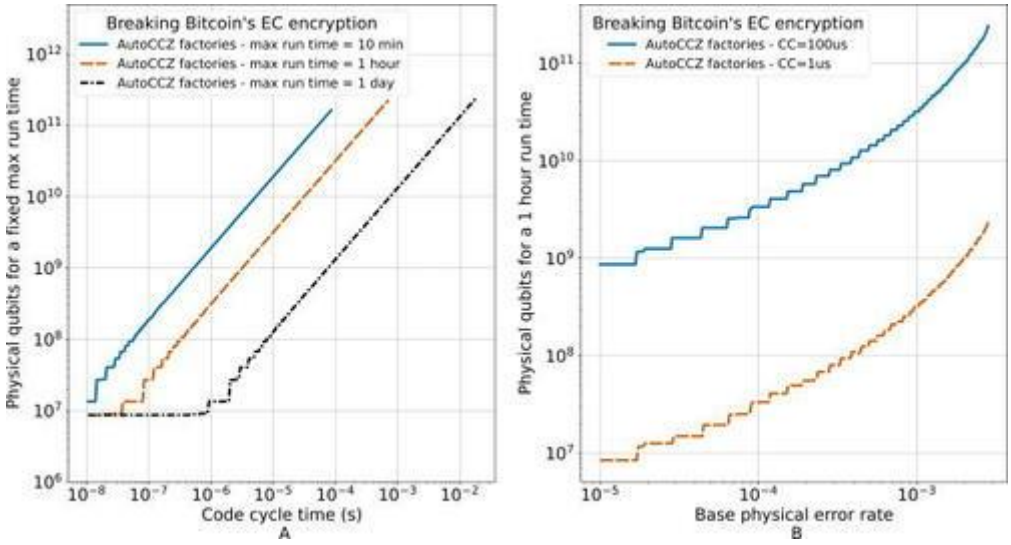
[41] Federal Office for Information Security 2020.
[42] The 20 million physical and error-prone qubits translate into 14.238 error-free logical qubits, a relationship of 1568 to 1.

Historical cost estimate at $n = 2048$	Estimated costs: Physical qubits (millions)	Expected runtime (days)	Expected volume (megaqubitdays)
Van Meter et al. 2009 [85]	6500	410	2600000
Jones et al. 2010 [46]	620	10	6200
Fowler et al. 2012 [28]	1000	1.1	1100
O'Gorman et al. 2017 [61]	230	3.7	850
Gheorghiu et al. 2019 [30]	170	1	170
(ours) 2019 (1 factory)	16	6	90
(ours) 2019 (1 thread)	19	0.36	6.6
(ours) 2019 (parallel)	**20**	**0.31**	**5.9**

Source: Own adaption from Gidney et al. 2021.

Table 3 RSA factorization runtime depends on optimizations employed

In a third study, estimations are made for breaking signatures based on the Elliptic Curve Digital Signature Algorithm (ECDSA) using a modified version of Shor's algorithm, as seen in Figure 3.



Source: Webber et al. 2021.

Figure 4: Time-Space tradeoff

To do this within 10 minutes, it would require 1.9 billion (1.9×10^9) physical qubits, with 1 hour available 317 million (3×10^8) physical qubits would be required and within 1 day only 13 million (1.3×10^7) would be required.

Next to the time resources needed for running Shor's algorithm there are also resources related to actual monetary costs. A reference for operating cost dimensions is provided in a study that blueprints a large-scale trapped-ion based quantum computer[43]. Here the capability of factoring RSA 2048 keys consumes 5 MW[44] of power which amounts to a total consumption of 13,2 GWh in 110 days

[43] Lekitsch et al. 2017.
[44] Federal Office for Information Security 2020.

that calculation takes to complete. With this proposed design breaking one RSA-2048 key would cost at 0,30€ per kWh about 3,96 million Euros.
A second approach to estimate costs can be made by pairing current pricing of commercially available quantum computing-as-a-service (QCaaS) with the required calculation runtime (qubit-seconds). The most efficient solution as cited from the aforementioned study by Gidney & Ekerå requires approximately $4*10^{14}$ (400 billion) qubit-seconds calculation runtime which would be priced on a QCaaS in 2022 at approximately 0,05€[45], bringing the total cost of breaking one RSA-2048 key to about 20 billion Euros.

The abovementioned studies can provide an idea for the dimensions of quantum computing resources required, both from an engineering and commercial point of view. Still, it must be cautioned that these numbers represent the current state of research development and further optimization improvements are expected to lower requirements. Nevertheless, building a quantum computer capable of factoring RSA 2048 is still years, if not decades away. How much time exactly depends on the long-term development trajectory that is difficult to predict.

[45] Andre Saraiva 2022.

3 Quantum Computing development trajectories

3.1 Assumptions

To discuss the real-world impact of the quantum threat, assumptions have to be made about the timing scenarios of its emergence. From a purely theoretical point of view, four emergence scenarios can be compared: One, unbeknownst to the general public, capable quantum computers are already available but only to a small circle of interested parties, such as intelligence agencies. Two, capable quantum computers will emerge in the more near future, i.e. in the next decades (2030-2060). Three, capable quantum computers will only emerge in the more distant future, which will be defined in the context of this research as the time from 2060 until 2150. Finally, four, capable quantum computers will never emerge.[46]
The further development trajectory discussion will focus on scenarios two and three, as scenario one is no ongoing development trajectory and scenario four would render the need for further discussion of this topic moot.

For the very much immediate future in the next decade it is a common consensus that the current development progress of quantum computers will not allow for a breakout scenario of the quantum threat[47]: As of 2022 the state-of-the-art quantum computers made by IBM (433 qubits)[48] and Google (53 qubits)[49] are still multiple magnitudes of orders away from the aforementioned $2x10^7$ qubits needed to attack RSA-2048[50]. Forecasting quantum computing development progress beyond the next decade is unlikely to generate reliable insights. This is exacerbated by the fact, that already today numerous different quantum computing platforms exist that are each challenged by their own, separate set of physical and engineering problems to be solved and it is hard to predict which one of them will become established.
The approach taken in this thesis instead aims to offer multiple conceivable development trajectories and respective real-world implications. It remains at the

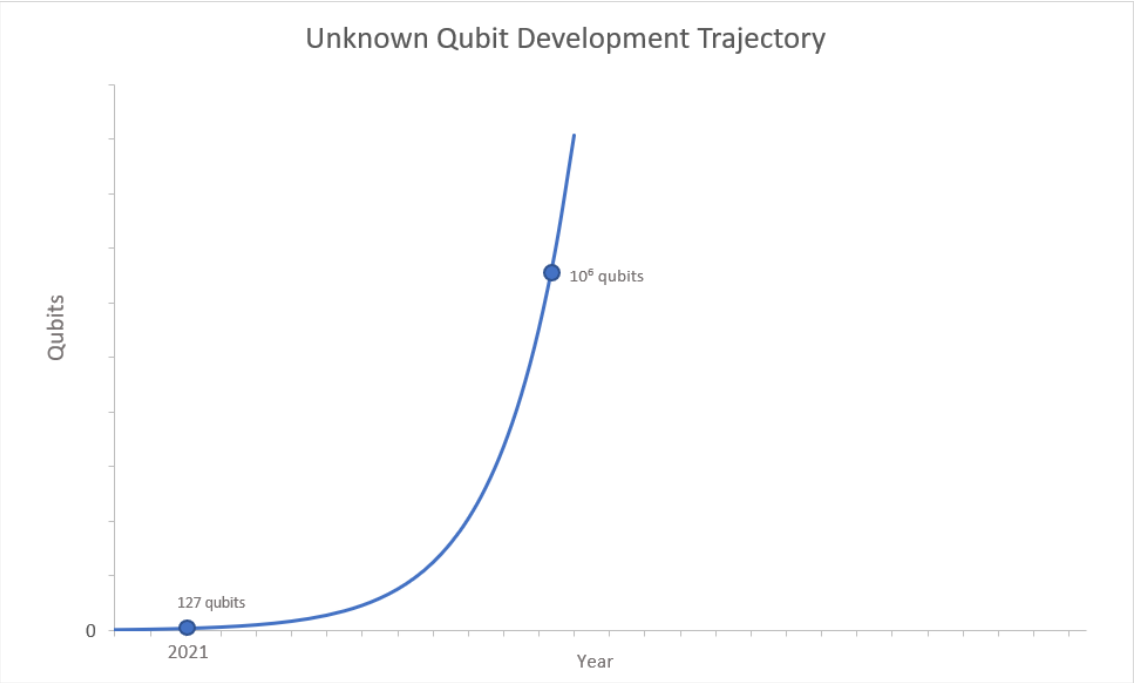
[46] Grimes 2020., p 90
[47] Grimes 2020., p 95
[48] IBM 2022.
[49] Arute et al. 2019.
[50] Although quantum annealing computers offer already today significantly higher numbers of qubits, they are not deemed to be capable to scale Shor to large key sizes.

reader's discretion to accept or reject the proposed development trajectories and to draw their own conclusions based on the suggested real-world implications.

For the breakout scenario to realize the gap between the currently most advanced quantum computers (433 qubits) and those that are needed (approximately $2x10^7$ qubits) needs to be bridged. While the chosen approach cannot satisfactorily answer the question of how much time is needed, it can offer other valuable insights.
As a prerequisite for this two assumptions about the nature of the progress of quantum computing need to be acknowledged:
First, the development progress will follow a gradual trajectory without sudden order-of-magnitude jumps. This assumption can reasonably be expected to hold true in the light of progress observed in many other areas. In the context of quantum computer development this assumption is likely to apply for another reason: Overall development progress is a war fought on many fronts and is determined by a multitude of minuscule improvements for a specific scientific or engineering problem. Each of these improvements is meaningful for development progress, however none of them are decisive, i.e., none on their own will enable a sudden, game-changing breakthrough as they only concern each a specific issue. Overall development progress is therefore likely to follow a gradual trajectory that is composed of the multitude of improvements.

Second, quantum computing must develop exponentially for a breakout scenario to realize within a reasonable timeframe, i.e. until the end of the century. If progress were to develop linearly and given that in the past 20 years "only" about 100 qubit of progress was made, then the qubit sizes required for breaking RSA 2048 would only be reached in a very distant future. Furthermore, if qubit growth is only linearly then the emerging quantum threat could be set off easily by increasing key lengths accordingly, a strategy that does not work with exponential qubit growth. A linear development trajectory can thus almost be equated to the abovementioned emergence scenario four, where capable quantum computers never materialize.

In figure 5 both assumptions, the current development status and yet-to-be-achieved progress can be seen in one graph. The graph's scale numbering has been intentionally left blank to indicate that this graph does not allow a forecast to be made for when a particular qubit count will be reached.

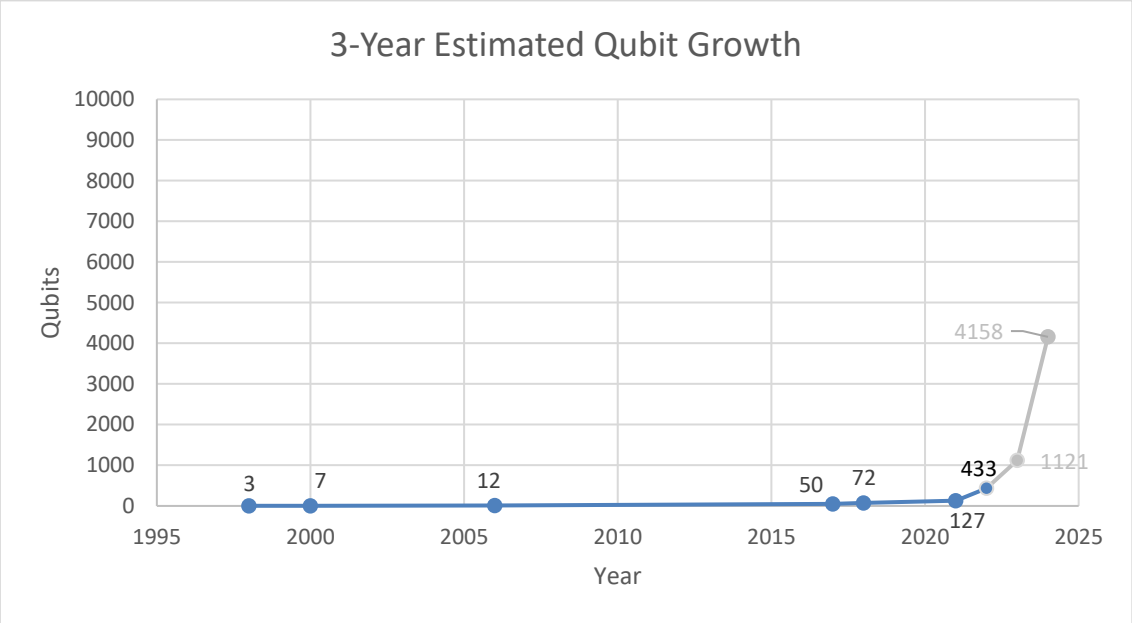


Source: Own depiction

Figure 5: Unknown Qubit Development Trajectory

If the assumption about exponential qubit growth is indeed applicable, then this exponential growth should already be observable with the current development progress.

In figure 6 a 25-year development timeline depicting both past[51] and expected development (IBM) is shown. Although the graph initially follows a linear curve, the projected growth in the last 3 years depicted strongly implicates an exponential development.



Source: Own depiction based on Finke 2022 and Grimes 2020.

Figure 6: Quantum Computing Qubit Development

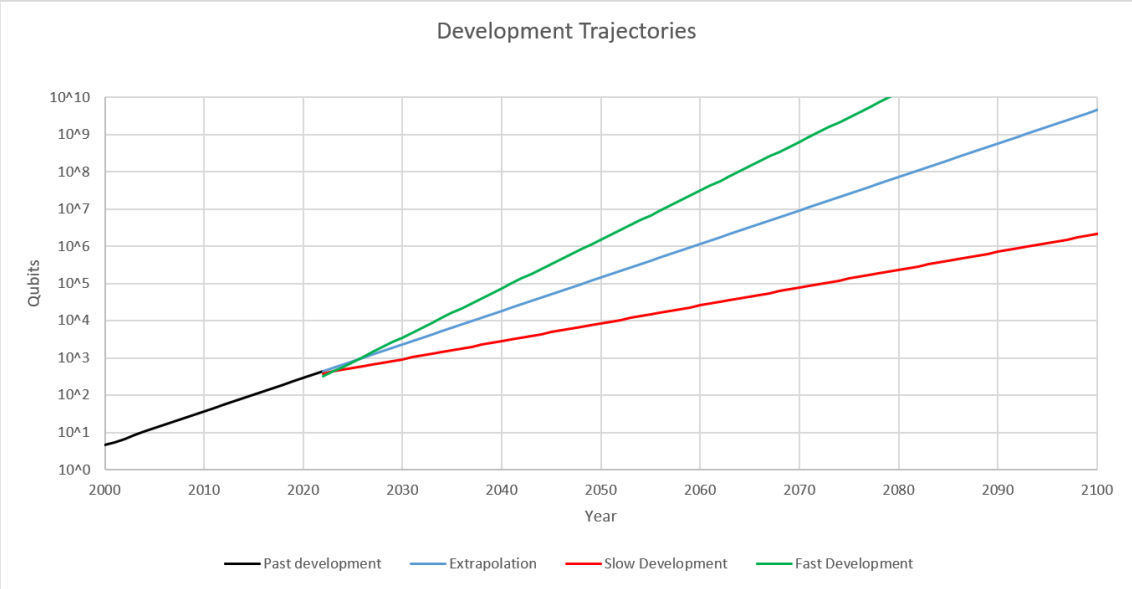
What is still unknown is whether (or when) the exponential development will taper off. Moore's Law which describes the development of transistor density (and thus performance) of conventional computer processing chips predicted exponential growth which is now declining due to various constraints[52]. It is not unreasonable to expect that quantum computer development likewise will taper off at some unknown moment in the future due to similar constraints.

3.2 Breakout scenarios

Even if it cannot be estimated very well "when" the quantum threat will be realized, some more insight is possible already today into the "how". Whereas in Figure 5 an unspecified exponential development was shown, Figure 7 portrays three potential development timelines on a logarithmic scale.

[51] Cryptocalypse p.92
[52] Shalf 2020.

The black line shows achieved development, ranging from a quantum computer with 3 qubits in 1998 to IBM's 433 qubits in 2022. The blue line extrapolates the current development, it is the prolongation of the black line into the future. The red and green lines represent arbitrarily chosen development trajectories: The red line depicts a slow development reaching $10^{3,5}$ (3.162) qubits in 2040, and the green line a fast development reaching 10^5 (100.000) qubits in 2040. The purpose of this graph is not to predict when a breakout scenario will occur but to enable an understanding of how a breakout scenario will be structured when it occurs.



Source: Own depiction using Quantum Development Milestone Calculator.xlsx

Figure 7: Depiction of arbitrarily chosen development trajectories. At about 10^6 qubits the first quantum computing-based attacks are likely to emerge, according to current research.

In chapter 2.3 different space-time requirements for quantum computers were presented, of which the most recent and efficient solutions are summarized in Table 4. Longer RSA key lengths generally require more qubits and longer runtimes. However, qubit requirements increase relatively linearly compared to RSA key length growth, so an increase in RSA key lengths would also have to be exponential to reasonably counter an exponential qubit growth[53].

[53] See a note on this in chapter 6.2 as well.

RSA key length	Qubits (Millions)	Qubits (log10)	Runtime (h)
1024	9,7	7,0	1,3
2048*	1	6,0	2400
2048	20	7,3	5,1
3072	38	7,6	12
4096	55	7,7	22
8192	140	8,1	86
12288	200	8,3	200
16384	270	8,4	350

* datapoint from BSI

Source: Own depiction based on Gidney & Ekerå and the German Federal Institute for Information Security

Table 4: Quantum computing requirements for different RSA key lengths

Combining the graph chart in Figure 6 with the requirements from Table 6 enables a modeling of different breakout scenarios.
If one were to assume that future quantum computing development speed can indeed be extrapolated from past progress, then table 5 projects when which capability milestones would be reached.

Extrapolation based on current progress	
Model predicts reaching cabability milestones	Year
Breaching RSA-2048@2400h in:	2059
Breaching RSA-2048@5h in:	2074
Breaching RSA-3072@12h in:	2077
Breaching RSA-4096@22h in:	2079
Breaching RSA-8192@86h in:	2083
Breaching RSA-12288@200h in:	2085
Breaching RSA-16384@350h in:	2086
Breaching RSA-64000 in:	2153

Table 5: Breakout scenario extrapolation based on current progress

Notably, the time period between reaching the capability for the first time to breaking RSA-2048 in 2400h (100 days) would be possible in 2059, breaking RSA-2048 in 5h would only be reached 15 years later and breaking RSA-8192 only twenty years later.
From this table three conclusions can be drawn:

1) The so-called “Q-Day” upon which quantum computers reach the capability to break asymmetric encryption is indeed not a moment in time but rather a decade-long period.
2) Longer RSA key sizes do have a temporary protecting effect: The nowadays increasingly common key size of RSA-4096 will be breakable approximately two decades after RSA-2048 first can be attacked. This advantage of long key sizes tapers off remarkably when comparing RSA-4096 with RSA-16384 where the time difference is less than 10 years.
3) Breaking asymmetric encryption does neither happen instantaneous, nor within seconds or minutes for the foreseeable future, limiting threat actors’ capabilities to mostly passive attacks that are less time critical.

Of course, the exact timelines for the capability milestones depend on the then realized quantum computing development speed and further optimized implementations of Shor’s algorithm. Despite that the level of yet-to-be-achieved optimization and development speed cannot be told in advance; it will remain true that longer key lengths or shorter algorithm run times require a higher amount of qubits that will only come to be available later.

To better understand how breakout scenarios are affected by faster or slower development trajectories we can compare two models. In table 6 a slow development reaching only 3.162 qubits in the year 2040 is compared with a fast development reaching 100.000 qubits in the same year.

Slow development			**Fast development**		
Qubit	Qubit (log)	Year	Qubit	Qubit (log)	Year
1.000	3,5	2040	100.000	5,0	2040
Model predicts reaching cabability milestones		Year	Model predicts reaching cabability milestones		Year
Breaching RSA-2048@2400h in:		2092	Breaching RSA-2048@2400h in:		2048
Breaching RSA-2048@5h in:		2119	Breaching RSA-2048@5h in:		2058
Breaching RSA-3072@12h in:		2125	Breaching RSA-3072@12h in:		2060
Breaching RSA-4096@22h in:		2128	Breaching RSA-4096@22h in:		2061
Breaching RSA-8192@86h in:		2137	Breaching RSA-8192@86h in:		2064
Breaching RSA-12288@200h in:		2140	Breaching RSA-12288@200h in:		2065
Breaching RSA-16384@350h in:		2143	Breaching RSA-16384@350h in:		2066

Table 6: Slow and fast development trajectories compared

Notable for the difference between these two models is that for the slow development trajectory the capability of breaking RSA-2048 for the first time is only reached in the year 2092. In contrast with the fast development trajectory this capability is already reached in 2048.

A second notable insight can be derived from the maximum time period between the capability of breaking RSA-2048 and breaking RSA-8192: For the slow development trajectory this period takes 45 years, whereas for the fast development trajectory this is only 16 years.
Therefore, each breakout scenario's timeline contracts or expands with the relative exponential speed of overall quantum computing development.

3.3 Quantum computer availability stages

Terms like "Q-Day", "year to quantum (Y2Q)"[54], "quantum disruption"[55] or "post-quantum cryptography" transport the idea there is a "before" and "after" when it comes to quantum computers reaching the capability to break encryption. The analysis of breakout scenarios paint a different picture in which this capability is conceived as a continuum. For easier discussion this continuum can be split into five different stages ranging from the current era in which capable quantum computers are not available until the era characterized by highly capable quantum computers and widespread availability.

Stage	Characteristics	Availability
1: Pre-QC era	QCs capable of breaking commercially used encryption not available. Research mostly modeling potential implementations and optimizations of Shor's algorithm. Cost per attack: not applicable	Nobody, research progress makes it unlikely that unknown single entities have obtained this capability.
2: Initial QC era	Research and QC development has progressed far enough that attacks on short key lengths with very long algorithm run times are conceivable. Passive attacks only, mostly academic or with targeting selected high-value targets, some initial Store-Now-Decrypt-Later. Cost per attack: >100 Million €[56]	Very limited, only passive attacks, only for state-sponsored threat actors. No commercial availability.
3: Low-powered QC era	Algorithm run time for short key lengths < 1 week, very long algorithm run times for long key lengths.	Initial commercial availability. State-sponsored threat

[54] Nguyen 2022.
[55] Sethi 2022.
[56] The costs indicated in table 7 are not the result of calculation but instead have been arbitrarily chosen to provide a potential frame of reference.

	Mostly passive attacks. Cost per attack: >1 Million €[56]	actors may have the capacity for active attacks.
4: High-powered QC era	Algorithm run time for short key lengths < 1 hour, for long key lengths < 1 day. Active attacks become common. Cost per attack: >1 Thousand €[56]	QC-attacks commercial established, becoming slowly affordable for most threat actor groups. Widespread use by state-sponsored threat actors.
5: QC fully established	Algorithm run time for large key lengths < 1 hour, active attacks possible for the most commonly used key lengths. Cost per attack: <1 Thousand €[56]	QC-attacks affordable for all threat actor groups.

Table 7: Quantum computing availability stages

An essential aspect of these stages is the matter of availability: During the initial stages quantum computing capable enough to attack asymmetric cryptography will remain costly enough as to limit availability to only a small circle of organizations or individuals. Later this circle will widen to ultimately be available to most individuals and organizations.

The whom capable quantum computers are available is essential for determining whether a particular real-world use case is at risk and from which threat actor this risk emanates. For example: Until stage 2 where only state-sponsored threat actors have the resources to access or acquire capable quantum computers, it is unlikely that this capability will be used by them to attack comparatively low-value targets such as online shopping websites. To elaborate this discussion, the following chapter introduces a threat actor typology including a differentiation of their resources, motivations and potential targets.

4 Threat actors

4.1 Threat Actor Typology

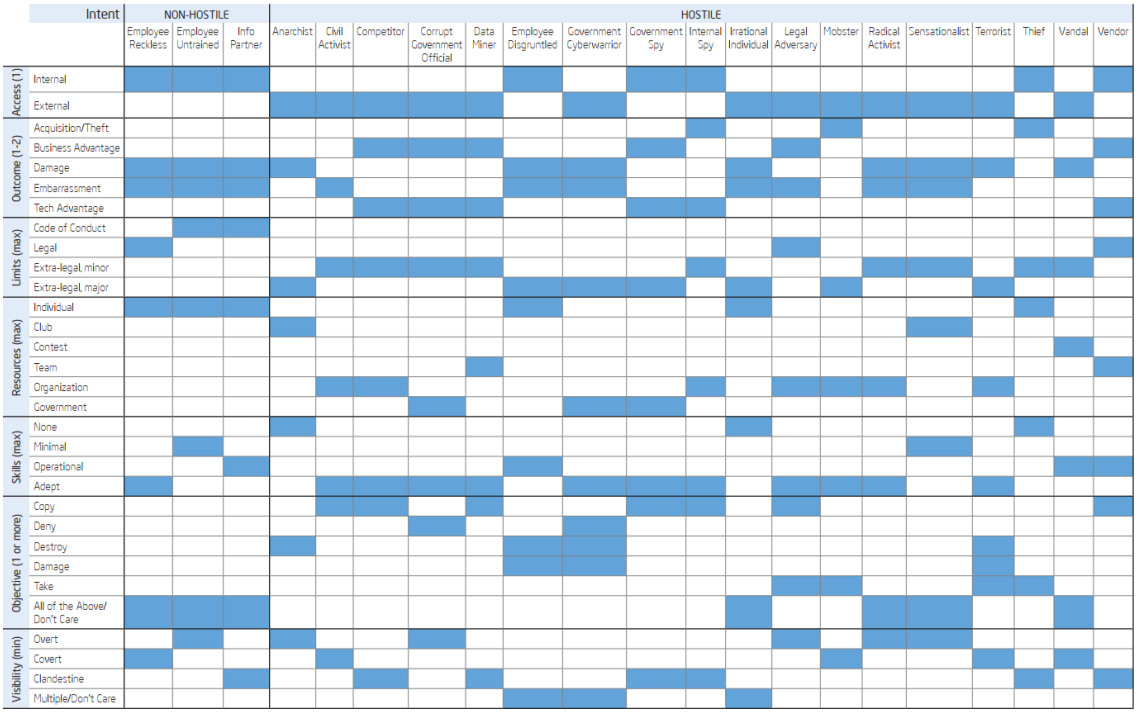
Different threat actors (TA) have different motivations, targets and resources, which makes the threat they pose to organizations and infrastructure not uniform. Not only will different threat actors have different capabilities to access quantum computing resources, but also different objectives and attack vectors available that they can make use of to accomplish their objectives.

This chapter aims to provide an overview of the different threat actors and modifies an existing threat actor typology to enable a reasoning base for each threat actor's relevance for quantum computing-powered attacks on cryptography.

Originally intended to standardize the threats human agents pose to IT assets, Intel's "Threat Agent Library"[57] (TAL) will be used to identify possible threat actors that are relevant in the context of quantum computing-based attacks on cryptography. It contains 22 standardized threat actor archetypes in a matrix with 8 attributes. The archetypes describe the type of threat actor (e.g. "Government Spy") and the attributes, the properties and capabilities (e.g. "Resources") of each threat actor.

Figure 8 depicts the Threat Agent Library in its original, unmodified form containing all 22 threat actors.

[57] Casey 2007.



Source: Casey 2007, page 5.

Figure 8: Unmodified Threat Agent Library by Intel[58]

4.2 Modified Threat Actor Typology

The 8 attributes can be used in a two-step approach to narrow down the number of threat actors to those, that are likely to use quantum computers to attack cryptography: In the first step, threat actors are excluded if the threat actor's attributes make the use of quantum computers for attacking cryptography unlikely. In the second step, an additional attribute will be created and added to indicate at which stage each threat actor will gain the capability to employ quantum computing for attacking cryptography.

The following attributes exclude threat actors from the scope as they preclude:

- **Threat actors with Non-Hostile Intent**: Friendly actors intend to protect assets and only accidentally will take actions that cause harm. As it appears unlikely that friendly actors will accidentally employ quantum computers to break encryption, "Employee Reckless", "Employee Untrained" and "Info Partner" are removed from scope.
- **Threat actors that act within the limits of applicable laws ("Legal") or follow a "Code of Conduct"**: It is assumed that these threat actors pose

no serious hazard and are thus removed from scope as well. Therefore, the threat actors “Legal Adversary” and “Vendor” are removed.

- **Threat actors with insufficient skills (“None”):** Threat actors that lack fundamental skills such as a basic understanding of cryptography or the knowledge of the prerequisites to attack encryption are removed from scope. This applies to the threat actor types “Anarchist”, “Irrational Individual” and “Thief”.

The remaining threat actors are now evaluated on their capacity to obtain and use quantum computers and matched to one of the previously defined five stages in which they are expected to gain the capability to use quantum computers for attacking cryptography. For this, a matching logic is devised and applied to the attributes “Skills”, “Resources” and.
Central to this matching logic is the assumption that more powerful, resourceful threat actors, such as nation-states or nation-state backed actors, obtain this capability in an earlier stage than individual or loosely organized ones. This assumption is summarized in table 8 which also provides Intel’s resource definitions[59]:

Resources	**Obtain the capability to use QC no earlier than in**
Individual Resources limited to the average individual; agent acts independently.	Stage 5: QC fully established
Club Members interact on a social and volunteer basis, often with little personal interest in the specific target.	Stage 5: QC fully established
Contest A short-lived and perhaps anonymous interaction that concludes when the participants have achieved a single goal	Stage 5: QC fully established
Team A formally organized group with a leader, typically motivated by a specific goal and organized around that goal. Group persists long term and typically operates within a single geography.	Stage 4: High-powered QC era
Organization Larger and better resourced than a Team; typically a company. Usually operates in multiple geographies and persists long term.	Stage 3: Low-powered QC era
Government[60]	Stage 2: Initial QC era

[59] Casey 2007.
[60] It shall be noted while the original TAL classifies the resource level of the “Corrupt Government Official’s” as “Government” they are classified in the modified TAL as “Team”. This is due to the fact, that the “Corrupt Government Official” likely does not command the resources required for quantum computing in one of the earlier stages.

Controls public assets and functions within a jurisdiction; very well resourced and persists long term.	

Table 8: Matching rule for "Resources"

Additionally, it is assumed that highly skilled threat actors develop the ability to use of quantum computing earlier than unskilled threat actors. Skill refers to the training or expertise a threat actor typically has. Table 9 summarizes the “Skill” matching rule.

Skills	**Obtain the capability to use QC no earlier than in**
None Has average intelligence and ability and can easily carry out random acts of disruption or destruction but has no expertise or training in the specific methods necessary for a targeted attack.	Out of scope (skills insufficient)
Minimal Can copy and use existing techniques.	Stage 4: High-powered QC era
Operational Understands underlying technology or methods and can create new attacks within a narrow domain.	Stage 3: Low-powered QC era
Adept Expert in technology and attack methods, and can both apply existing attacks and create new ones to greatest advantage.	Stage 2: Initial QC era

Table 9: Matching rule for "Skills"

Applying the two matching rules to the Threat Agent Library results in a Modified Threat Agent Library (Figure 9) from which irrelevant threat actors have been removed. For the remaining threat actors the stage upon which they gain the capability to use quantum computing to break encryption is indicated in the bottom rows.

	Intent	HOSTILE												
		Civil Activist	Competitor	Corrupt Government Official	Data Miner	Employee Disgruntled	Government Cyberwarrior	Government Spy	Internal Spy	Mobster	Radical Activist	Sensationalist	Terrorist	Vandal
Access	Internal					■		■	■					
	External	■	■	■	■		■			■	■	■	■	■
Outcome	Acquisition/Theft								■	■				
	Business Advantage		■	■	■			■						
	Damage					■	■				■	■	■	■
	Embarrassment	■				■	■				■	■		
	Tech Advantage		■	■	■			■	■					
Limits	Extra-legal, minor	■	■	■	■				■		■	■		■
	Extra-legal, major					■	■	■		■			■	
Resources (max)	Individual					■								
	Club											■		
	Contest													■
	Team			■	■									
	Organization	■	■						■	■	■		■	
	Government						■	■						
Skills (max)	None													
	Minimal											■		
	Operational					■								■
	Adept	■	■	■	■		■	■	■	■	■		■	
Objective (1 or more)	Copy	■	■		■			■	■					
	Deny			■			■							
	Destroy					■	■						■	
	Damage					■	■						■	
	Take									■			■	
	All of the Above/ Don't Care										■	■		■
Visibility (min)	Overt			■							■	■		
	Covert	■								■			■	■
	Clandestine		■		■			■	■					
	Multiple/Don't Care					■	■							
QC Stages	1: Pre-QC era													
	2: Initial QC era						■	■						
	3: Low-powered QC		■				■	■						
	4: High-powered QC	■	■	■	■		■	■	■	■	■		■	
	5: QC fully established	■	■	■	■	■	■	■	■	■	■	■	■	■

Source: Own depiction adapted from Casey 2007.

Figure 9: Modified Threat Agent Library with an additional 9th attribute describing the stage in which threat actors gain the capability to use quantum computers to attack cryptography. Threat actors identified as irrelevant have been excluded.

From the Modified Threat Agent Library, it can be seen that only two types of threat actors gain the capability early on to use quantum computers to attack cryptography. As time goes by, more threat actors with fewer resources catch on.

4.3 Threat Actors with early access to Quantum Computers

Which threat actors will be the ones leading in using quantum computers early on to attack cryptography is highly relevant for efficiently allocating resources when defending against the quantum threat. Table 10 summarizes at which stage which type of threat actors likely will have access to capable quantum computers.

From the type of threat actor conclusions can be drawn as to what their potential targets are, and thus which targets will need to be quantum-proofed as soon as possible and likewise, which organizations will be responsible for securing the targets.

Stage	Threat actors (TA)
1: Pre-QC era	None
2: Initial QC era	Government Cyberwarrior, Government Spy
3: Low-powered QC era	Competitor (+ Stage 2 TA's)
4: High-powered QC era	Civil Activist, Corrupt Government Official, Data Miner, Internal Spy, Mobster, Radical Activist, Terrorist (+ Stage 2 & 3 TAs)
5: QC fully established	All TAs

Table 10: Overview of QC stage availability to all threat actors

The threat actor types with the earliest capability for quantum computing-powered attacks are expected to be the Government Cyberwarrior and the Government Spy, which will be described in more detail in the following sections.

4.3.1 Government Cyberwarrior

Closely related to each other, the Government Cyberwarrior and the Government Spy are nation-state backed threat actors, often also called advanced persistent threat (APT). The Government Cyberwarrior partakes in offensive cyber warfare with the intent to bring about major disruption of organizational or national critical infrastructure or business disruption. The means of doing so is destroying or damaging infrastructure or interrupting service accessibility. The Government Cyberwarrior can achieve this using conventional means such as physical sabotage, infiltrating organizations, hacking or brute force denial of service attacks. Quantum computing-based attacks can offer them additional, specific advantages: First, they can enable new attack vectors that were previously not possible due to conventional cryptanalytic limitations. Second, they can facilitate a previously impossible stealthy and undetected intrusion by defeating cryptography-based access controls. Third, quantum computing-based attacks can also be openly flaunted as part of an intentional attack tactic to intimidate the opponent.[61]

[61] Intel 2007, page 8

An example of a Government Cyberwarrior is the Sandworm group deemed responsible for the successful attack on Ukraine's power grid in 2015[62]. Bringing down a power grid in an electricity-dependent world is one of the most effective ways to disturb civil life, industry and infrastructure and can be achieved without the attacking entity or country having to be present. It is therefore not unlikely, that in the future attacking power grids with the intent to disturb infrastructure on a large scale will establish itself as a popular attack vector for nation state-backed threat actors such as the Government Cyberwarrior.

4.3.2 Government Spy

The Government Spy may or may not partake in cyber warfare and can take an offensive or a defensive position. The goal is to obtain highly confidential information of individuals, organizations or states. The Government Spy will likely only be employed when the information to be obtained has a sufficiently high value to offset the costs that this attack is incurring, especially in the early stages of quantum computing availability. This means that this attack likely only targets specific individuals, organizations or states, which in turn may be able to understand that they are at risk and thus take action to protect themselves. As with the Government Warrior, the Government Spy can achieve their objective using conventional means such as infiltrating organizations, malware and hacking or social engineering attacks. Again, Quantum computing-based attacks can offer advantages: First, they can again enable new attack vectors that were previously not possible due to conventional cryptanalytic limitations. The most obvious example of this is the ability to decrypt all encrypted data using a hybrid encryption scheme that includes basically all data-in-transit[63], such as the Store-Now-Decrypt-Later attack (see chapter 6.3.1 for details). Second, they can facilitate a previously impossible stealthy, undetected intrusion by defeating cryptography-based access controls. [64]

An example of the Government Spy is Fancy Bear, an APT group most known for their exfiltration of emails from the Democratic National Committee in 2016[65]. Chapter 5 will describe how a Government Spy (or comparable) threat actor can use quantum computing to decipher encrypted communication.

---

[62] Case 2016.
[63] More secure are data-at-rest encryption schemes not relying on hybrid or asymmetric encryption.
[64] Intel 2007, page 8
[65] CNN 2018.

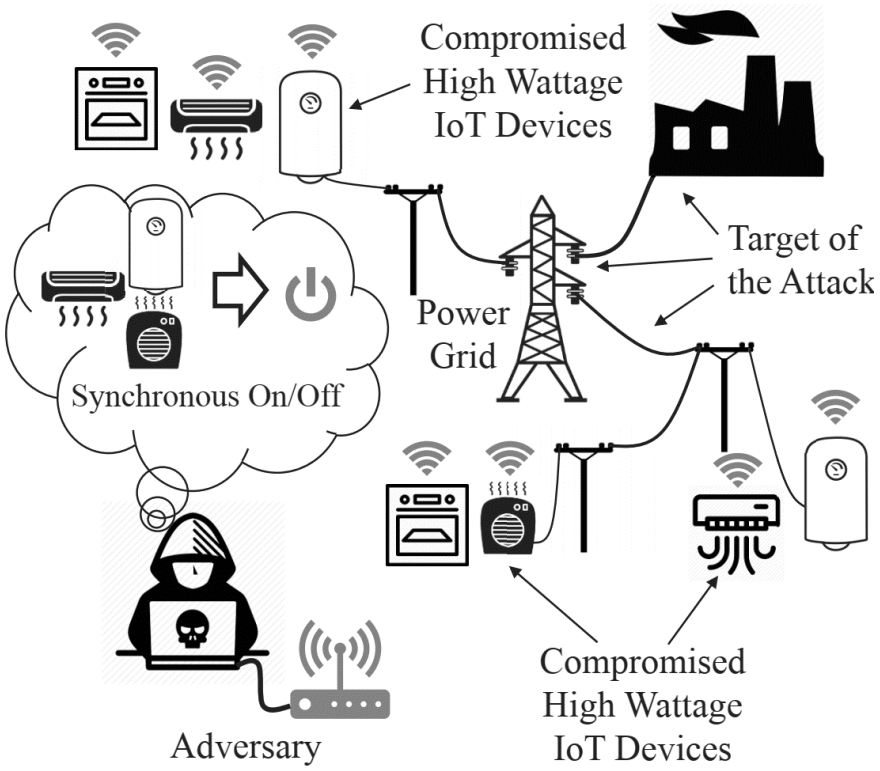
5 Attacking the power grid through electric vehicle charging stations

5.1 Electric vehicle charging

With the globally ongoing transition from fossil energy to more sustainable forms of energy, the booming electric mobility leads to a power grid load increase[66]. As electric vehicles (EV) depend on power grids for charging, security and safety issues in either may come to affect the other. With power grids often being part of national critical infrastructure this double-sided dependency between electric mobility and power grids has the potential for ripple effects: An EV charging fault interfering with the local power delivery network also may disturb other energy-dependent uses in that local power delivery (households, industry, water supply, heating, etc.). This issue was exacerbated, if a failure were to cascade beyond the local power delivery network to the national grid, leading to intermittent or even extended blackouts.[67]

The scenario of causing local or even cascading grid failures by maliciously manipulating power demand has been previously described in literature in the context of internet of things (IoT) devices and named Manipulation of Demand via IoT (MaDIoT). Here, compromised internet-connected devices capable of consuming high electrical power such as electric heaters, air conditioning devices, printers or EV chargers are remote controlled to draw high amounts of electrical power. This can be used to increase operating costs or, if a large number of these devices are manipulated in an orchestrated manner, to cause blackouts. Figure 10 depicts potential attack vectors for the MaDIoT attack.

[66] A two-stage protection
[67] Kern et al. 2021.



Source: Soltan et al. 2018.

Figure 10: Manipulation of Demand via IoT devices (MaDIoT)

The mechanism through which blackouts happen is that an increase in power demand needs to be matched by an increase in power generation. If power demand increase outspeeds power generation or total power generation capacity is exhausted, then power frequency will start to drop as generators cannot keep up with the electromagnetic resistance imposed by the power draw. Once the nominal power frequency drops below a pre-defined threshold, protection schemes will become active to protect the grid by dropping loads or disconnecting the generator to protect it. The instantaneous, local relief can have repercussions for other parts of the grid as power now needs to be distributed differently, thereby possibly overloading other generators or transmission lines that may automatically be disconnected as well.[68] More advanced attack forms that make use of different power draw patterns to be more stealthy or less preventable have been contemplated, along with possible countermeasures[69]. For this discussion however, the focus is placed on the question of how quantum computing-based attacks can be used to enable MaDIoT attacks.

[68] Shekari et al. 2022.
[69] Kabir et al. 2021 ; Sayed et al. 2022.

In the context of potentially cascading failures caused by MaDIoT attacks, employing EV charging as power sinks provides several advantages to threat actors:

First, EV charging is a high-energy consumer with regular charging stations providing around 10-40kW and high-energy charging stations providing more than 100kW[70]. The potentially high energy consumption of each charging station offsets the need for the threat actor to reign over a huge number of devices to be able to impact the grid by manipulating power consumption.

Second, the protocols used for communication in the EV charging ecosphere are standardized, publicly available and used across countries. This increases the return-on-investment (ROI) for the threat actors who can use the same known protocol to attack many devices without having to adjust the attack method greatly.

Third, apart from damaging a country's energy grid a welcome side-effect for threat actors can be the denial of service of charging stations, either temporary by actively suppressing charging or more permanently by rolling out over-the-air (OTA) firmware updates to charging stations, effectively creating a botnet. A country that has already migrated from carbon-powered vehicles to EVs may be impacted significantly by having their EVs cut off from functioning charging stations.

Fourth, the EV charging cryptographic public key infrastructure (PKI) lacks resilience, as will be shown in the following sections.

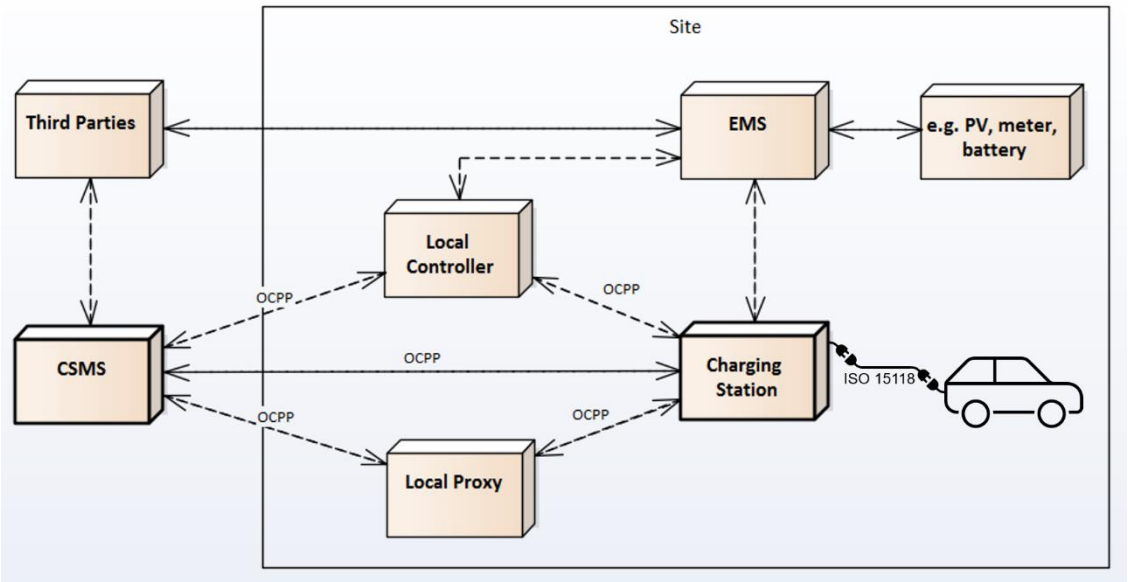
For these reasons, an attack on EV charging stations may be an attractive target for nation-state backed threat actors aiming to hurt or cripple another nation's infrastructure.

In the following a scenario will be described where a quantum computing-powered attack serves as an entry vector to manipulate charging stations with the goal of destabilizing energy grids and causing large-scale blackouts. As previous literature has already established the details of destabilizing energy grids, the focus for this scenario description will lie on how a threat actor can employ their quantum computing capability to execute an attack like this.

[70] Tran et al. 2017.

5.2 OCPP Design

EV charging consists of various interconnected parts and systems that could be targeted and manipulated.
Electronic vehicles are charged by connecting a power cable with a standardized connector (such as CCS, Type 2 or CHAdeMO) to both the EV and the charging station (CS). The part of the charging station that the power cable is attached to is called Electric Vehicle Supply Equipment (EVSE), one CS may contain multiple EVSE for charging multiple EVs at the same time[71]. The CS usually contains a user interface that the EV driver can use to authenticate themselves and monitor and control the charging process. Whereas both the EVSE and CS are physically present at the charging site and exposed to the public, the Charging Station Management System (CSMS) is not. Administered by the charging station operator (CSO), it acts as a backend coordinator for multiple CS, collecting charging information, communicating tariffs, steering charging activity in line with current energy availability in the grid and updating and configuring charge stations.[72] In Figure 11 a prototypical architecture is shown with various other optional elements included, such as an Energy Management System and Local Controller and Local Proxy.



Source: Own adaption from OCPP Part 1

Figure 11: Components in an EV charging setup. Dotted lines signify optional connections and elements.

[71] OCPP Part 1
[72] Garofalaki et al. 2022.

Communication between the CS and the EV via the charging cable is standardized in *ISO15118 Road vehicles -- Vehicle to grid communication interface* and employs TLS encryption[73]. Attacking this communication is unlikely to be the first choice when attempting to remotely attack charging control as physical presence is will likely be required. More effective will be an attack on a centralized entity that can control a multitude of CS such as the CSMS. There may be better options than attacking the CSMS directly though as different CSMS are offered by different vendors, requiring the threat actor to tailor their attack to each new encountered CSMS. A more rewarding target is the standardized communication between the CSMS and CS implemented by each CSMS through the Open Charge Point Protocol (OCPP) which was first released in 2011 by the Open Charge Alliance. OCPP enables a range of communication and commands by which the CSMS can exchange information and remote control the CS. The most recent version of OCPP 2.0.1 (2020) implements communication exchange and remote control of the CS for these functions:

- **Security**: Updating CS passwords and certificates
- **Provisioning**: Booting, configuring and resetting CS
- **Authorization**: Authorizing EV drivers using various factors such as PIN code, credit card, RFID token, etc.
- **Transactions**: Communication of transaction-related financial information such as tariffs and energy meter states
- **Remote Control**: Remote control of transaction, charging connector unlocking and displaying messages on the CS
- **Availability**: Remote (dis-)abling of the CS or individual EVSE
- **Reservation**: Management of reservations made by EV drivers
- **Tariff and Cost**: Communication of tariffs and cost of charging
- **Meter values**: Periodic sending of meter values to the CSMS
- **Smart Charging**: Remote control of charging, charging current and charging profiles
- **Firmware Management**: Updating the CS firmware
- **ISO 15118 Certificate Management**: Installation of certificates in CS, relayed installation, update and removal of certificates in EVs[74]

A threat actor with the objective of significantly damaging critical infrastructure could utilize these remote-control functions to achieve one of the following:

[73] International Organization for Standardization 2014.
[74] Open Charge Alliance 2020.

1) To permanently disable charging stations the **Firmware Management** function can be used to update the charging station's firmware to a non-functional firmware, making costly human intervention on each CS necessary for the charging station operator (CSO) to regain authority.
2) To take over control of charging stations and lock out CSOs the **Security** function can change a charging station's access codes and certificates. Again, human intervention on each CS is required to regain authority.
3) To destabilize the power grid (MaDIoT-attack) the **Smart Charging** function can orchestrate multiple charging stations to start and stop charging. Using the OCPP's in-built "Charging Profiles" this functionality can additionally be preprogrammed to become active even if the CS has been centrally cut off from the internet by the CSO in a last-resort measure.

Other attacks, such as manipulating the firmware to manipulate billing or to steal EV driver's payment data are also realistic but may not be the primary objective of a threat actor with the resources to access a quantum computer capable of breaking cryptography, at least not in the early stages of quantum computing-powered attacks.

5.3 Attacking OCPP

To use OCPP to remote control charging stations, the threat actor has to circumvent or break the cryptographic security controls implemented in the CS that prevent unauthorized third parties from pretending that they are a CSMS. To protect against this type of attacks, OCPP employs TLS (Transport Layer Security) since OCPP version 1.6. As of OCPP version 2.0.1 TLS unfortunately is not strictly mandatory as only two of the three security profiles require TLS to be active: Profile 1 only demands HTTP Basic Authentication without TLS, that provides no strong authenticity and does not protect integrity nor confidentiality and is only recommended to be used if network communication between CS and CSMS is secured by a Virtual Private Network (VPN)[75]. Due to the lack of CSMS authentication, any threat actor able to place themselves in a man-in-the-middle (MITM) position can immediately pretend to be a CSMS, giving them complete control over the CS. In this case, attacks can easily be mounted without the need to break cryptographic security controls using quantum computers.
As can be seen in Table 11, this only works with Security Profile 1 but not with Security Profiles 2 and 3.

[75] Garofalaki et al. 2022.

Profile	Charging Station Authentication	CSMS Authentication	Communication Security
1. Unsecured Transport with Basic Authentication	HTTP Basic Authentication	-	-
2. TLS with Basic Authentication	HTTP Basic Authentication	TLS authentication using certificate	Transport Layer Security (TLS)
3. TLS with Client Side Certificates	TLS authentication using certificate	TLS authentication using certificate	Transport Layer Security (TLS)

Source: OCPP Part 2

Table 11: OCPP Security Profiles

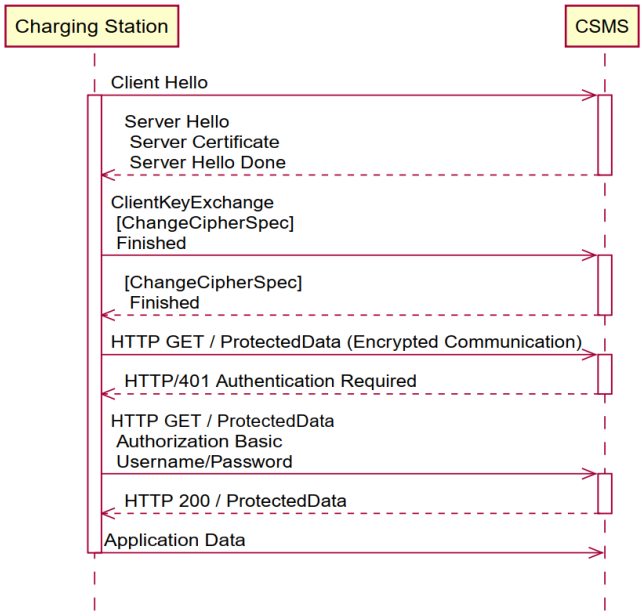
Profile 2 provides for TLS-level authentication of the CSMS and HTTP Basic Authentication of the CS and protects confidentiality and integrity of the communication. When data is exchanged between the CSMS and the CS, the CSMS will authenticate itself using an X.509 certificate which the CS can verify.
A threat actor wishing to pretend to be the CSMS now needs to present a TLS certificate that the CS would accept. To achieve this, various options exist that will be described later in more detail. The on its own rather insecure HTTP Basic Authentication is now secured by tunneling all communication through TLS, rendering HTTP Basic Authentication an acceptably secure option for authentication again[76].
Profile 3 abolishes HTTP Basic Authentication entirely by requiring the CS to authenticate by presenting a TLS (client) certificate. While this increases security related to attacks in which a malicious CS attempts to trick the CSMS by masquerading as a legitimate CS, profile 3 does not prevent attacks in which CS are tricked by malicious CSMS and does thus not provide any additional security advantage for the contemplated attack.

To summarize: The easiest way to compromise a CS is a setup in which OCPP security profile 1 is used, but the operator negligently does not tunnel network traffic through a third-party VPN. If a VPN is used, then the security of OCPP depends on the security guarantees of that specific VPN implementation. Both cases will not be discussed further: A missing VPN tunnel leads to immediate compromise, and if a VPN is used a multitude of VPN implementation and configuration options would have to be considered, which is beyond the scope of this case study.
The TLS-enabled security profiles 2 and 3 provide the same level of protection against threat actors targeting the CS and can thus be treated equally for this

[76] The use of HTTP Basic Authentication may still be criticized as it requires saving clear text credentials.

analysis. In all cases, the threat actor must have direct network connectivity to the CS. It is advantageous, although not required, to also be in a man-in-the-middle position between CSMS and CS to intercept messages between them to prevent that manipulated CS settings are overridden again by the CSMS or the CSMS learning about the manipulated state of the CS.

A threat actor attempting to remote control a CS needs to prove to the CS that they are a legitimate CSMS. Security profiles 2 and 3 require the threat actor to own the private keys to a TLS certificate that is accepted by the CS.
Authentication of the CSMS occurs during the TLS handshake, which serves to also agree on connection parameters, extensions and ciphersuites between CS and CSMS and to agree or exchange a session key for encryption. In Figure 12 the TLS handshake using one of the two RSA-based authentication ciphersuites[77] is shown.



Source: OCPP Part 1
Figure 12: Security Profile 2 TLS Handshake with an RSA-based ciphersuite

The handshake starts with the client sending a `Client Hello` message to the server, to which the server replies with the `Server Hello`, `Server Certificate` and `Server Hello Done` message. In the `Server Hello` message, the CSMS determines and communicates the ciphersuite to be used to the CS.

According to requirements, at least one of the following ciphersuites must be supported:

[77] TLS_RSA_WITH_AES_128_GCM_SHA256 and TLS_RSA_WITH_AES_256_GCM_SHA384

1) TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
2) TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
3) TLS_RSA_WITH_AES_128_GCM_SHA256
4) TLS_RSA_WITH_AES_256_GCM_SHA384

The first two ciphersuites can be considered as industry best-practice due to their use of elliptic-curve Diffie–Hellman (ECDH) key agreement that enables perfect forward secrecy (PFS)[78]. In contrast, the latter two have been criticized for not featuring PFS and being potentially vulnerable against padding oracle attacks[79]. Both potential vulnerabilities however are irrelevant as they only allow for a loss of confidentiality of the encrypted data and not for a loss of authenticity, as would be desirable to a threat actor wishing to spoof a CSMS.

The threat actor can choose between a ciphersuite that employs RSA or ECDSA (Elliptic Curve Digital Signature Algorithm) for authentication by not offering the other during the initial `Client Hello` message. As of 2022 research has optimized Shor's algorithm most effectively for RSA, making the RSA-based ciphersuites[80] the preferred choice over the ECDSA ciphersuites[81] for a hypothetical threat actor in 2022.

5.4 Quantum-Exploiting the PKI

For the threat actor two routes exist to pretend to be a legitimate CSMS: The first route requires obtaining a CSMS's (leaf) certificate (including private keys) and the second route requires obtaining a root certificate (including private keys) that can sign intermediate- or leaf certificates. The public part of both types of certificates can be easily obtained from a legitimate CSMS during the TLS handshake. In either route, the threat actor needs the public key contained in the certificate to derive the corresponding private key to subsequently be able to pretend to be a specific CSMS (route 1) or create and sign new CSMS certificates using the root certificate (route 2). Whereas route 1 attacks an individual identity-proving certificate, route 2 attacks the public key infrastructure at its literal root. For this reason, it is advantageous to choose route 2: Owning a root certificate and the corresponding private keys not only lends full ownership over the PKI but also makes it harder for legitimate PKI operators to exercise damage control.

[78] Rudolph et al. 2022.
[79] Gilles 2022.
[80] TLS_RSA_WITH_AES_128_GCM_SHA256 and TLS_RSA_WITH_AES_256_GCM_SHA384
[81] TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 and TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA38

Whereas a single certificate can easily be revoked and replaced, replacing a root certificate requires time to prepare and roll out new root certificates, which likely has to be done manually on all the CS and CSMS involved.

A second reason related to certificate revocation makes route 2 a more likely contender for threat actors:
According to the OCPP 2.0.1 definition, certificate revocation works differently for each type of certificate: The certificates used to authenticate the CS and new firmware updates must be verified via the Online Certificate Status Protocol (OCSP) to provide real-time assurance that the certificate has not been revoked. Responsible for this is the CSMS, who will forward firmware signing verification to the CS. For the CSMS certificate, no revocation mechanism is provided, instead a “fast expiry” is used with which certificate lifetime is limited to less than 24 hours. The motive is to remove the burden from the CS for obtaining revocation data which can instead rely on the short certificate expiration date[82].
For the threat actor potentially two unwelcome consequences arise from this: First, any certificate obtained from a CS will be valid for less than 24 hours which also means that factoring the public key into the private key must happen in significantly less time for the private key to still be of any use to the threat actor. Two, once the 24 hours validity time period elapses a new certificate will be reinstated by the original, legitimate CSMS and the threat actor will need to attack the renewed certificate anew[83], provided that private keys were not reused in the renewed certificate. The requirement to (repeatedly) compute the private key from the public key within 24 hours limits this attack vector’s utility to a later quantum computer availability stage and or those threat actors with the resources to repeatedly mount costly attacks.

The defined minimum key length can be criticized as too short in the context of quantum computers. For RSA, a minimum of 2048 bit long keys are required and for elliptic curve cryptography key exchanges at least 224 bit.
From a technological point of view, these requirements are slightly below industry best-practice. The Federal Office for Information Security recommends using the RSA-ciphersuites until 2026 and the ECDHE-ciphersuites until at least 2028. The use of RSA in certificates for signing should be replaced after 2025 with the Digital

[82] The protocol description does not specify whether the CS is also obliged to distrust certificates with a certificate lifetime longer than 24 hours.
[83] The necessity of this is debatable: Technically it should be possible for the threat actor in the limited access time window they have to either preprogram the CS’s charging schedule and/or to gain permanent access by adding their own, illegitimate CSMS root certificate into the CS’s root certificate storage.

Signature Algorithm (DSA) or Elliptic Curve Digital Signature Algorithm (ECDSA).[84] Ideally, certificate minimum key lengths should be doubled, and only PFS-enabling key agreement ciphersuites should be used.

OCPP's lack of PKI governance allows PKI operators to select key lengths detrimental to the PKI's security. Short key lengths such as RSA-2048 combined with potentially decade-long root certificate validity make it possible for threat actors such as the Government Cyberwarrior as early as in stage 2 Initial QC Era to start attacking national grids via electric vehicle charging infrastructure and for less well-equipped threat actors in the subsequent stages.

[84] Federal Office for Information Security 2022.

6 Mitigating the Quantum Threat

Mitigating the quantum threat implies that the quantum threat either does not occur or if it does, that there is only little impact. To achieve this, security controls need to be put in place that usually are categorized into preventive security controls, detective security controls and corrective security controls[85].
Like security measures against conventional threats, it is also advisable in the context of the Quantum Threat not to put all eggs in one basket and instead to take a layered, defense-in-depth approach to implementing security controls.
This chapter describes various preventive, detective and corrective controls that can be employed to counter the Quantum Threat.

6.1 Quantum-Cryptographic approaches

The quantum threat can be met using various methods on various levels, one of which is the technical or cryptographic level. These preventive security controls aim to eradicate the vulnerability posed by conventional asymmetric protocols by providing a quantum computing-safe alternative. Two major classes of defense are typically viewed as promising in preventing the quantum threat, quantum cryptography and post-quantum cryptography.[86]

6.1.1 Quantum Cryptography

Quantum cryptography uses quantum mechanical effects to construct an entirely new type of encrypted information exchange. It taps into the area of quantum communication as the data bits exchanged are qubits themselves. The sending and receiving party require specialized hardware capable of doing so which limits the number of use cases in which quantum cryptographic communication terminals could replace conventional asymmetric cryptography.
Due to the no-copy property of qubits, which can act both as a preventive and detective control, qubits cannot be re-routed, temporarily stored or broadcasted, lending them different properties than IP packets have. The use of quantum cryptography will likely mostly be limited to being a secure solution of the key exchange problem (“quantum key distribution”), meaning that it will only be used

[85] Chapple et al. 2021.
[86] Mosca 2018.

to exchange a symmetric key that is then used by conventional symmetric algorithms such as AES.
Quantum cryptography will not be the preferable solution for securing charging stations against the quantum threat: Neither is this attack scenario dependent on a secure key exchange nor does quantum cryptography solve the issues PKIs face in light of the quantum threat.

6.1.2 Post-Quantum Cryptography

Whereas Quantum Cryptography requires quantum mechanical effects, Post-quantum Cryptography (PQC) can be seen as an evolution of conventional asymmetric cryptography that can even exist independently of quantum physics and the quantum threat. All currently used protocols implement conventional asymmetric algorithms that base their hardness on either a factorization or discrete logarithm problem, problems to which Shor's algorithm can find an efficient solution. PQC algorithms base their security on different mathematical problems to which no efficient solutions are known, neither on classical nor quantum computers. Most PQC algorithms therefore are part of either Supersingular Elliptic Curve Isogeny, Lattice, Multivariate, Code-based or Hash-based Cryptography. Each of these fields of cryptography is defined by its own set of advantages and disadvantages for which further analysis is beyond the scope of this thesis.

Unfortunately, Post-quantum Cryptography cannot fully resolve the quantum threat on its own, at least not currently. Two major problems, amongst a number of other minor ones, prevent the timely replacement of conventional asymmetric algorithms such as RSA, DH and ECDH by PQC algorithms[87]:
First, PQC algorithms are still in a comparatively early development phase with potentially unknown vulnerabilities. To identify promising PQC algorithm candidates and standardize them eventually, the National Institute of Standards and Technology (NIST) announced a multi-round competition in 2016 which received a total of 82 submissions.

[87] Celi 2022.

In July 2022 after four selection rounds, the first group of four winners (table 12) were announced for standardization and four further algorithms (table 13) are kept as candidates for the next round of standardization.

Public Key Encryption	Signature
CRYSTALS-Kyber	Falcon
	CRYSTALS-Dilithium
	SPHINCS+

Table 12: 2022 Winner of the NIST PQC Competition

Public Key Encryption	Signature
Classic McEliece	None
HQC	
BIKE	
SIKE	

Table 13: 2022 Candidates for round 4 of the NIST PQC Competition

Despite the NIST's standardization efforts a certain level of insecurity remains:
If the conventional asymmetric algorithms were to be replaced by the 2022 competition winners entirely, chances are that in the proximate future new security issues would emerge given the questionable maturity of PQC algorithms. This is showcased by two previous standardization candidates of the NIST PQC competition (Rainbow and SIKE) being broken in 2022 only[88].

A second major issue with the shortlisted PQC algorithms is performance. This concerns both key and signature size as well as the speed of encryption and decryption or signing and verifying. Although most PQC candidates are either slow or large, none of them is as lean as RSA or ECDH are. In an experiment Cloudflare paired a conventional asymmetric algorithm with a PQC one to study the impact on real-world TLS connections used in web browsing. They found that the larger key- and signature lengths interfered with TCP packet size (maximum transmission unit) and increased the risk of packet loss which begets retransmission delays, making the handshake up to twice as long.[89] Here, security competes with business as slower page loads or dropped connections

[88] Goodin 2022.
[89] Westerbaan 2021.

are associated with a loss of sales conversions and revenue when consumers lose patience with accessing an online webshop[90].

Additionally, switching to PQC algorithms increases traffic due to larger signature sizes. In the case of CRYSTALS-Dilithium 17 kilobytes are added per page visit, which is not much individually but can add up on a global scale, which may be reason for concern in the context of reducing emissions. To alleviate this issue, an intelligent combination of different PQC algorithms has to be employed, such as using CRYSTALS-Dilithium for the TLS handshake and Falcon for certificate signatures that can be created beforehand.[91] Table 14 provides an overview of different PQC signature algorithms and their performance (size and time) compared to a conventional ECDSA P-256 and RSA-2048 algorithm as a baseline. It becomes apparent that each PQC algorithm candidate has their strengths and weaknesses that beget a specialized use case scenario where either size or time is not that relevant.

		Size (bytes)		Relative time	
		Public key	**Signature**	**Verification**	**Signing**
Non PQ	**NIST P-256**	64	64	1 (baseline)	1 (baseline)
	RSA-2048	256	256	0.2	25
NIST finalists	**Dilithium2**	1,320	2,420	0.3	2.5
	Falcon512	897	666	0.3	5 *
	Rainbow I	157,800	66	0.1	2.4
	Rainbow I CZ	58,800	66	12	2.4
NIST alternates*	**SPHINCS⁺-128ss har.**	32	7,856	1.7	3,000
	SPHINCS⁺-128fs har.	32	17,088	4	200
	Picnic-L1-full	34	32,061	21	60
	GeMMS128	352,190	33	0.4	5,000
Others	**SQISign**	64	204	500	60,000
	XMSS-SHAKE_20_128 *	32	900	2	10 *

Source: Westerbaan 2021.

Table 14: Different PQC signature algorithms compared to conventional asymmetric algorithms for time and size

[90] Brooks 2022.
[91] Westerbaan 2022.

Of all the PQC algorithms, it is Falcon512 that appears to deliver the best performance tradeoff between size and time. Unfortunately, Falcon512 cannot readily be implemented in all circumstances as its security depends upon being run in a constant-time 64-bit floating point arithmetic which is not implemented on many CPUs.[92]
For these issues, the NIST renewed their competition for secure PQC algorithms in 2022, hoping to identify more performant though secure PQC algorithms[93].

In the context of attacking the grid using compromised EV charging stations, the currently known PQC algorithms can nevertheless already play an important role as a preventative security control:
In order not to suffer from catastrophic failure when conventional asymmetric algorithms come under immediate threat by quantum computers or also when PQC algorithms are broken (as happened with Rainbow or SIKE) it is advisable to use them both in a combined, hybrid encryption scheme, which is encouraged by NIST and is even FIPS 140-compliant[94]. The added performance penalty on the TLS handshake likely plays a negligible role for customer behavior as TLS connections between the charging station and the charging station management system can be kept alive for days[95] and customers can reasonably be assumed to not abandon a CS, if it does take one or two seconds for the CS to establish connectivity to the CSMS. Unlike TLS in HTTPS can TLS in OCPP be immediately secured using PQC algorithms.

6.2 Conventional approaches

While quantum cryptography and post-quantum cryptography are often discussed as the only proper remedies against quantum computer-powered attacks, other and more readily available options exist. These options decrease the attack's return-on-investment (ROI) by driving up attack costs and or diminishing potential attack rewards. Although perfect security is not achieved in this way, it is in practice often sufficiently satisfactory to increase attack costs just high enough to make the attack inefficient for the threat actor.
Increasing attack costs function as a soft preventive security control. This can be done by implementing cryptography so that a successful attack requires more

[92] Westerbaan 2021. Westerbaan 2022.
[93] Westerbaan 2022 & NIST 2022.
[94] NIST 2017.
[95] Open Charge Alliance 2020.

resources. The most straightforward way of doing so is by increasing the key lengths of asymmetric cryptography algorithms.

From table 2 it can be derived that doubling key length also approximately doubles the number of required qubits and increases the number of gates by the factor of 10 when using Shor's algorithm. This postpones the moment from which any given threat actor should gain the capability to use quantum computers for attacking a certain use case by 3-10 years, depending on the speed of the development trajectory[96]. A further increase of RSA key sizes up to 8 kilobytes then increases the necessary quantum computing resources to a level that is incompatible with physics: Factoring an 8 kilobyte long RSA key necessitates approximately 50 years of quantum processing time which is beyond physically obtainable qubit coherence times. However, these long key sizes penalize the user unduly by slowing down the cryptographic processes so tremendously that en- and decryption operations become impractically slow (one encryption now takes several minutes), which may only be acceptable for a very small subset of use cases.[97]

A further option to drive up attack costs may be to stack multiple layers of encryption. This way, the threat actor needs to employ the quantum computer for each of the encryption layers anew, which drives up attack costs, especially in the early quantum computer availability stages. This stacking of encryption can either be done on the infrastructure layer, as for example by tunneling an encrypted TLS connection through another encrypted VPN or on the protocol layer: Here, multiple key exchanges can be done in parallel with the concatenated output to serve as the session key, as does the Signal protocol with its Extended Triple Diffie-Hellman (X3DH) key exchange[98].

Lowering attack rewards can be achieved by using short-lived session keys that limit the amount of data that can be recovered after breaking asymmetric key exchange (RSA) or key agreement (DH). The introduction of Perfect Forward Secrecy (PFS) to TLS, a corrective security control, has significantly improved security by requiring a new and unique session key to be negotiated with every new browsing session instead of relying on the same, static RSA-derived for all connections. PFS implies that even if a certificate's private keys are discovered at some point, none of the retrospectively exchanged encrypted data is compromised. However, this does not apply to data encrypted after the

[96] Refer to table 6 for details.
[97] Li et al. 2021.
[98] Marlinspike et al. 2016.

certificate's private keys are compromised as now the compromised certificate could be used in a man-in-the-middle attack to intercept and decrypt data.
With the implementation of Post Compromise Security (PCS), also a corrective security control, a significant step can be taken towards securing the confidentiality of encrypted data against the quantum threat and particularly against the Store-Now-Decrypt-Later attack[99] without having to rely on post-quantum cryptography. Whereas PFS protects data that was exchanged *before* the compromise of private keys, PCS also protects data exchanged *after* the compromise of private keys. This so-called self-healing property is achieved by renegotiating new session keys along with every message that is exchanged, which renders the private keys a threat actor obtained at the time t+0 with no use at t+1. Unfortunately, PCS has only been implemented in few messaging protocols such as the Signal protocol[100] and its precursor the Off-The-Record Messaging protocol (OTR)[101] as well as Matrix' Olm protocol and Wire.[102] This leaves the vast majority of other protocols relying on cryptography without this desirable self-healing property. Lamentably, PKIs cannot benefit from self-healing PCS as PKIs rely in their core on the existence of long-term keys that are not exchanged or renegotiated. For this reason, PCS is no viable remediation against the quantum threat for attacking the grid via compromised EV charging stations.

Instead, detective security controls can be applied that protect PKIs to some degree against the Quantum Threat. If an attack is possible but can be detected quickly and remediated easily, then it may be too uneconomic for an attacker to engage. In the context of PKIs, one efficient detective security control is Certificate Transparency which publicly logs actively used certificates. This makes illegitimately created certificates visible and enables certificate authorities to blacklist or revocate them using certificate revocation lists (CRL) or the Online Certificate Status Protocol (OCSP). While this does not prevent a threat actor from breaking and abusing (usually short-lived) leaf certificates, it does make it noticeably more challenging for them to sign their own leaf certificates after having cracked an intermediate or root certificate without being detected doing so. Although a threat actor can attempt to attack Certificate Transparency as well, they will at most be able to counterfeit the signatures of the two Certificate Transparency logs required to be embedded in each leaf certificate but unable to

[99] See chapter 6.3.1
[100] Marlinspike et al. 2016.
[101] Anonymous 2021.
[102] Olivier Blazy et al. 2023.

attack the log itself, which is based on quantum-resilient Merkle-Hash trees. This means that the preventive security aspect of Certificate Transparency can be broken, the detective however cannot.
As with other security controls, Certificate Transparency should not be relied upon on its own but provides a valuable addition nevertheless.
In the context of the quantum threat for attacking the grid via compromised EV charging stations Certificate Transparency can and should[103] play an important role for securing the PKI. This still holds true even if PQC algorithms were already implemented as Certificate Transparency can still be used to detect malicious certificate authorities.

6.3 Model-based approaches

Although implementing post-quantum algorithms and other security controls is the work that eventually needs to be done, there is yet another discussion of when this needs to be done and against which risks need to be considered and weighed up. Model-based approaches take on the issue from a risk-management perspective and can be used to develop roadmaps that guide decision-makers through the implementation of security controls. In the context of the quantum threat these model-based approaches specifically look at the question when action needs to be taken.

6.3.1 Store-Now-Decrypt-Later Modeling

While the previously discussed type of attack on grid infrastructure becomes feasible only once capable quantum computing is available, there is also a different, notable attack vector that must be mentioned in the context of the quantum threat, even if it is likely not useful for attacking EV charging infrastructure. With the store-now-decrypt-later[104] (SNDL) attack[105] a threat actor can take action even long before quantum computing-powered attacks become viable by intercepting and storing encrypted communication (e.g. TLS encrypted web browsing sessions, encrypted messaging). Once quantum computing has evolved sufficiently, the threat actor can then decrypt the previously intercepted and stored encrypted data. As a matter of fact, the mere perspective of being able

[103] In the OCPP v2.0.1 specification Certificate Transparency is neither mandatory nor mentioned.
[104] Sometimes also called „harvest-now-decrypt-later” (HNDL)
[105] Grimes 2020.

in the future to decrypt data that was harvested today may incentivize threat actors to do so[106]. Given this, it becomes necessary to consider countermeasures before quantum computer availability stage 2.

As to how early actions should already be taken to protect oneself against the threat of SNDL has been modelled in a publication by Michele Mosca (2018)[107]. The modeling builds on dependable timelines for quantum computer evolution which can only be approximated. Nevertheless, some practical deliberations can be made according to this model:

- First, the time span of which confidential data needs to be kept confidential must be determined (this variable will be called Security Shelf Life). Here the context of the encryption use case is important as for example communication between state leadership likely needs longer protection than web-browsing online newspapers.
- Additionally, the time necessary to facilitate such a switch to quantum-safe PQC-based protocols needs to be estimated (this variable will be called Migration Time). This time will be substantial for encryption protocols such as TLS implemented by a huge variety of software and devices, reflecting the effort and timespan needed to upgrade all implementations, libraries and installations of software using the protocol.
- Finally, the time until the quantum threat is realized by the development of quantum computers capable of breaking convention public-key cryptography needs to be estimated (this variable will be called Conventional Crypto Collapse Time). Likely, timelines for this development are discussed in chapter 2.

Once these values are established or estimated, then the sum of the "Security Shelf Life" and "Migration Time" should be less than the expected "Conventional Crypto Collapse Time". If for a particular use case or application the "Security Shelf Life" and "Migration Time" are higher than the expected conventional "Crypto Collapse Time" then it is likely that this use case can be exposed and is vulnerable to successful SNDL attacks. While SDNL attacks clearly can work very well from a technology point of view, some further elements must be considered in evaluating their likelihood, which relate to the economical angle: Attackers must know very well what data they are interested in and where to collect it. The generalized, indiscriminate capture of internet traffic would require massive amounts of data to be stored for an undetermined time, as the attacker can only draw limited conclusions about the value of the encrypted data they captured. Commercial long-term tape archival

[106] Mashatan et al. 2021.
[107] Mosca 2018.

data storage costs are at approximately 1€ per terabyte per month as of 2022[108], which can become prohibitively expensive if giant amounts of data need to be stored for decades. If data had been collected indiscriminately, then the attacker has to wait until a quantum availability stage has been reached that matches the financial resources available to repeat the decryption process for each individually encrypted session data stream contained in the captured datastore[109]. The SDNL attack additionally incurs lost opportunity costs as the attacker only can start to profit long after data was harvested.

For the attack to be economical, attackers therefore must have to be sufficiently familiar with their target's infrastructure, business case and data flows to then be able to selectively store only valuable data. Meeting these requirements puts attackers in a position where an attack using conventional means (social engineering, exploiting insecure server configuration, leveraging vulnerabilities, etc.) has good chance of succeeding as well. This means that attackers have to decide between launching a conventional attack right away or bearing the costs of storage, quantum resources and lost opportunity as well as the uncertainty of whether the quantum decryption capability will be reached before the harvested data loses their value.

In any case, the SDNL attack is most likely irrelevant to the security of EV charging infrastructure, outside of potential attack scenarios in which relevant confidential data or credentials are transmitted in encrypted form.

6.3.2 Quantum Readiness Roadmap

The Quantum Readiness Roadmap by Mashatan and Heintzman (2021) describes a process for organizations to manage their quantum risk and allows for different, flexible trajectories depending on how they assess their risk. This is especially important for large organizations that need a certain degree of forward planning and cannot always react on short notice.

According to the Quantum Readiness Roadmap, the first step is to set up a project or internal organization that enables governance: Here, it is important that the organization acknowledges the potential risk and values the need to become active by providing resources. Subsequently, the quantum risk must be assessed, and the organization's vulnerable cryptographic footprint be determined. This can be done similarly to the sequence of chapters as presented

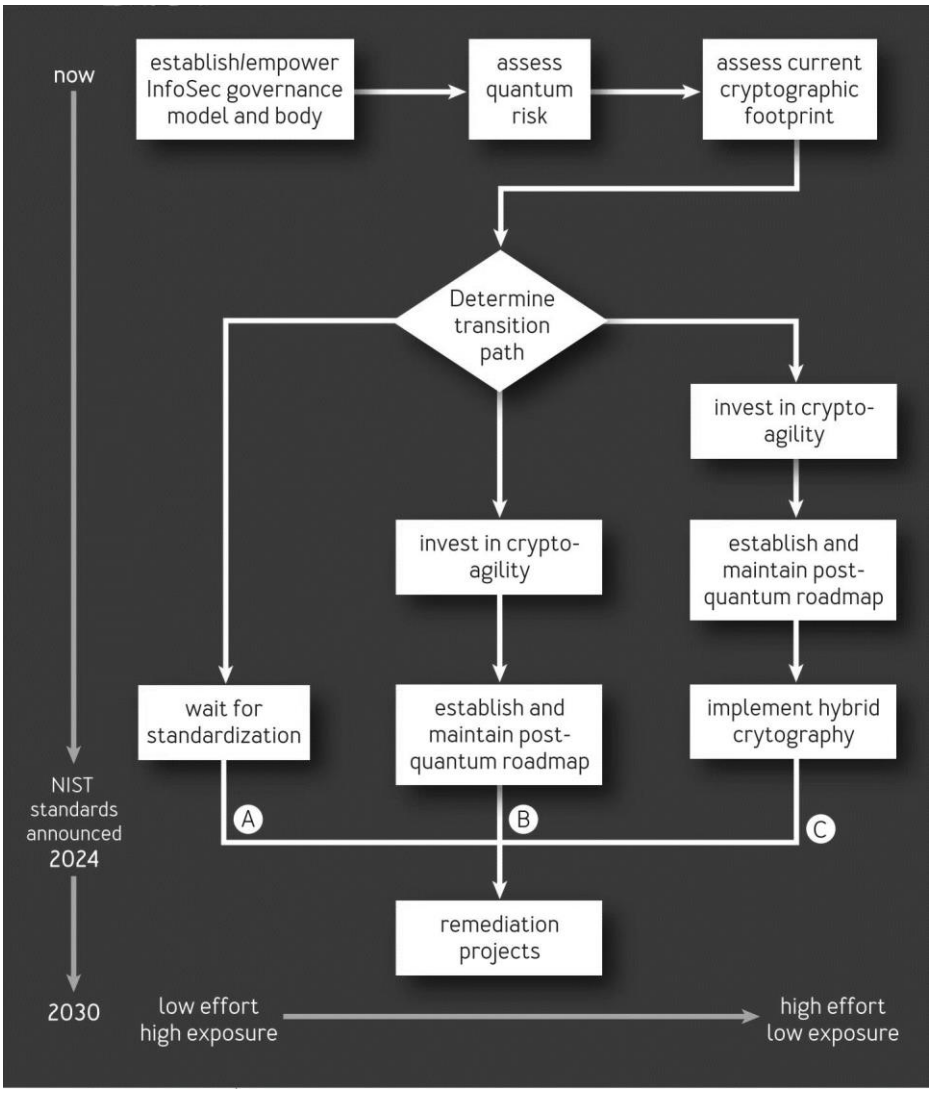
[108] Amazon 2022.

[109] This refers to the fact that indiscriminately captured internet traffic contains a myriad of connections and data streams that all are individually encrypted with individual keys. The costs to decrypt every one of them can easily become enormous.

in this thesis: Understanding the quantum threat, determining those outbreak scenarios that are seen as most probable and lastly understand on which vulnerable cryptographic schemes one is dependent. Additional proven and conventional approaches such as Microsoft’s STRIDE (Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of Privilege) or DREAD (Damage, Reproducibility, Exploitability, Affected users, Discoverability) can be applied to identify vulnerabilities and risk.

Based on this initial risk analysis, a long-term transition path can be determined that helps to guide action for the next 5-10 years. Depending on how severe the organization assesses its risk and how urgent action needs to be taken, Mashatan and Heintzman propose three different pathways.

The pathways differ in the amount of work an organization invests into becoming quantum-proof before reliable Post-quantum Cryptography is available as per the NIST's standardization process[110].



Source: Mashatan and Heintzman 2021, p. 83.
Figure 13: Quantum Readiness Roadmap

For those organizations that chose to make the lowest effort (because they see themselves with little quantum risk, path A) it can be sufficient to wait for the standardization of PQC algorithms to finish before taking action. Only once standardization has been completed remediation projects to replace vulnerable conventional asymmetric algorithms with quantum-proof PQC algorithms would be started.

[110] Especially for those organizations contingent on reliable cryptography it must be cautioned though, that the then standardized algorithms are still young and not sufficiently tested in the field.

Those organizations that choose to invest more effort (path B) can become active by preparing their technical infrastructure for easy and fast replacement or change of cryptographic algorithms and configuration (improving cryptoagility) to enable a faster transition to PQC algorithms once they become certified.
Organizations that see the need to react as early as possible (because they are at high risk or because their technical change processes take a long time) can take even more action by additionally layering security controls or implementing hybrid cryptography using PQC candidate algorithms in combination with proven conventional algorithms (path C).[111]

Given the potentially catastrophic effects of a successful attack on the electric grid and the long lifecycles of EV charging stations that can make it hard to upgrade these devices once rolled out to production, selecting path C today is the best option to meet the quantum threat. This is especially important as EV charging infrastructure will likely develop into a large PKI with complex dependencies for which short-notice patching can become an insurmountable task in the future. Implementing hybrid encryption schemes that combine conventional asymmetric algorithms with quantum-safe PQC algorithms is the best way to mitigate the quantum threat, considering that the performance penalties of today's PQC algorithms will not impact usage negatively.

[111] A similar approach is described by Zhang et al. 2021. in their "7E roadmap"

7 Discussion

7.1 Conclusions

This thesis dismantled the Quantum Threat into separate aspects to provide an end-to-end understanding of the circumstances required for this type of attack to function, how this attack capability may be used and how such a breakout scenario may look, based on the threat actors that first gain access to this capability. Additionally, the case study of disrupting the power grid by remotely manipulating power demand of EV charging stations was presented to give an example of how this capability can be utilized by state-backed threat actors to attack national critical infrastructures and which security controls can be employed to thwart this.

This thesis introduces some novel ideas to the current body of research: One main contribution is the notion that the capability to attack cryptography using quantum computers will emerge gradually rather than in a momentary instance. This notion builds upon the assumption that the eventual existence of a quantum computer capable of attacking conventional asymmetric cryptography will not come about as a sort of deus ex machina – sudden and unprecedented – but instead that development progress will follow a continuous trajectory that is without sudden order-of-magnitude jumps. The resulting implication is that initially, this capability will be available only to a few state-level actors and will be costly and limited even for them. In the beginning, only data that has been encrypted with short key lengths can be decrypted. Over time, quantum computing will become both more powerful and more accessible to a general audience. This will make attacks on longer key lengths possible and create more sources from which these attacks could come. To show how fast these breakout scenarios can progress and how much or how little time there can be between onset and widespread adoption, this thesis provides modeling that can be put to use by the security community to better understand an organization’s exposure to the quantum threat.

One new crucial question arises and will likely remain unanswered for still a while: (When) will an exponential development of quantum computers taper off, as

currently observable with Moore's Law for conventional computer development[112]?
The development of quantum computers needs to progress exponentially for at least long enough until a breakout scenario occurs, otherwise quantum computers with the capacity to break conventional asymmetric encryption will not be viable in the foreseeable future. Furthermore, if a limit to scaling quantum computers does exist, then this can greatly restrict how much the costs of using quantum computers can be lowered and thereby affect how ubiquitous they will become in attacking conventional asymmetric cryptography: As long as the costs of quantum computer attacks are higher than those of classical attack types (social engineering, exploiting vulnerabilities and misconfiguration, etc.), quantum computers will not represent a significant quantum threat to cryptography.

Another insight is that the threat that quantum computers pose for conventional asymmetric cryptography in the first instance is most likely more impactful for authenticity and integrity than for confidentiality: Although it is possible to decrypt confidential, encrypted data, successfully fooling authentication systems by forging certificates may be more enticing to attackers: Certificates allow access into live systems and to the data they contain, thereby violating both authenticity, integrity and confidentiality of systems and data. This means that when quantum proofing infrastructures, cryptographic authentication systems, as well as Public-Key-Infrastructures, should in most cases first be secured and encryption of data in transit only after, as the latter will automatically become vulnerable once the former has successfully been compromised.
This also applies very much to the portrayed case study where charging stations can immediately be compromised after obtaining the private keys of a root certificate. Due to the massive damage that can potentially be inflicted, immediate action should be taken to quantum-proof the EV charging infrastructure PKI.
This is especially important as the long lifetimes of the hard- and software involved and the open nature of the ecosystems involving many parties will make it challenging, if not impossible, to upgrade later the vulnerable encryption schemes employed to quantum-secure ones.

Furthermore, quantum proofing infrastructures are not limited to Quantum Cryptography or Post-quantum Cryptography. While both provide relief against the quantum threat, neither can replace current asymmetric cryptography without

[112] https://royalsocietypublishing.org/doi/full/10.1098/rsta.2019.0061

creating new challenges. Conventional approaches can strengthen current asymmetric cryptographic implementations against both conventional threats and the quantum threat by increasing attack costs and decreasing attack returns. Even if PQC algorithms are implemented, it is still advisable to layer security controls to establish defense-in-depth on a cryptographic layer.

7.2 Limitations and further research

As most research concerned with the quantum threat, this thesis cannot predict the future of quantum computing development, general trends in cyber-crime or the evolvement of novel threat actors. Therefore, neither the breakout scenarios nor further optimizations of Shor's algorithm can be predicted precisely. Instead, a model for evaluating the quantum threat is offered that the reader can either accept or reject or adapt with their own assumptions about the possible course of development.
Due to the chosen abstract approach that focuses not on minute details of different quantum computing architectures or implementation or optimization details of Shor's algorithm but rather on the big picture of the emerging quantum threat for real-world cryptography, some simplifications had to be made. For example, using the mere count of qubits as a benchmark for quantum computing capability neglects aspects such as qubit quality and implementation-specific performance details. Unfortunately, due to the different types of quantum computer platforms there is no one, singular perfect benchmark unit that can be used to identify the "best" platform, let alone reasonably compare platforms. Asking which is the "best" quantum computer platform is akin to asking which is the best mode of transport – each has its own set of advantages and challenges. Likewise, this thesis focuses on RSA and provides less information for (EC)DH and DSA, due to Gidney & Ekerå (2021) identifying the highest and most efficient optimization of Shor's algorithm for RSA. As Gidney & Ekerå (2021) note, this does not imply that attacking (EC)DH and DSA takes more resources, only that it has not been researched sufficiently yet.

At this point, the quantum threat has already been studied extensively and yet still not sufficiently. More research results are to be expected on multiple fronts that have the potential to change the dynamics of the quantum threat arms race: On the one side, research on the design and construction and usage of quantum computers will likely yield significant performance and capability improvements, bringing capable quantum computers closer to reality. Likewise, new studies

further optimizing Shor’s algorithm will help to lower the quantum resource requirements for these attacks. On the other side, research can be expected to produce improved Post-quantum Cryptography algorithms that have higher performance and are better suited to replace vulnerable, conventional algorithms 1-to-1, lowering the quantum threat’s risk. Until it becomes clearer which side will take the lead, this thesis hopes to have provided readers a better understanding of the quantum threat and valuable guidance in navigating it.

Literature

AARONSON, SCOTT, „The Limits of Quantum Computers“, in: *Scientific American* (2008).

AMAZON, „Amazon S3 Simple Storage Service Pricing“, in: Amazon Web Services (2022), URL: https://aws.amazon.com/de/s3/pricing/ (Accessed: 05.12.2022).

ANDRE SARAIVA, DIRAQ, „How Should Quantum Computations Be Priced?“, in: Quantum Computing Report (30.06.2022), URL: https://quantumcomputingreport.com/how-should-quantum-computations-be-priced/.

ANONYMOUS, „Off-the-Record Messaging Protocol version 3“, in: Off-the-Record Messaging (2021), URL: https://otr.cypherpunks.ca/Protocol-v3-4.1.1.html (Accessed: 27.11.2022).

ARUTE, FRANK et al., „Quantum supremacy using a programmable superconducting processor“, in: *Nature* 574, 7779 (10.2019), S. 505–510.

BEAUDRAP, NIEL DE, „Is quantum computing just pie in the sky?“, in: Quantum Computing Stack Exchange (02.07.2018), URL: https://quantumcomputing.stackexchange.com/a/2574/21847 (Accessed: 27.11.2022).

BROOKS, CHAD, „How Page Load Speed Affects Customer Behavior“, in: business.com (2022), URL: https://www.business.com/articles/website-page-speed-affects-behavior/ (Accessed: 27.11.2022).

CASE, DEFENSE USE, „Analysis of the cyber attack on the Ukrainian power grid“, in: *Electricity Information Sharing and Analysis Center (E-ISAC)* 388 (2016), S. 1–29.

CASEY, TIMOTHY, „Threat agent library helps identify information security risks“ (2007), URL: https://www.researchgate.net/profile/Timothy-Casey/publication/324091298_Threat_Agent_Library_Helps_Identify_Information_Security_Risks/links/5abd353445851584fa6fb597/Threat-Agent-Library-Helps-Identify-Information-Security-Risks.pdf (Accessed: 27.11.2022).

CASTELVECCHI, DAVIDE, „The race to save the Internet from quantum hackers“, in: *Nature* 602, 7896 (08.02.2022), S. 198–201.

CELI, SOFÍA, „The post-quantum state: a taxonomy of challenges“, in: *The Cloudflare Blog* (21.02.2022).

CHAPPLE, MIKE / STEWART, JAMES MICHAEL / GIBSON, DARRIL, *(ISC)2 CISSP Certified Information Systems Security Professional Official Study Guide, 9th Edition* | *Wiley*, Hoboken, NJ 2021, ISBN 978-1-119-78623-8.

CNN, KATELYN POLANTZ AND STEPHEN COLLINSON, „12 Russians indicted in Mueller investigation“, in: CNN (2018), URL: https://www.cnn.com/2018/07/13/politics/russia-investigation-indictments/index.html (Accessed: 27.11.2022).

CRANE, LEAH, „Quantum computer sets new record for finding prime number factors“, in: *New Scientist* (13.12.2019).

DEIGN, JASON, „Quantum computers will crack your encryption—maybe they already have“, in: Cisco Newsroom (2022), URL:

https://newsroom.cisco.com/c/r/newsroom/en/us/a/y2022/m03/is-2022-the-year-encryption-is-doomed.html (Accessed: 27.11.2022).

FEDERAL OFFICE FOR INFORMATION SECURITY, „Entwicklungsstand Quantencomputer“, in: (2020).

FEDERAL OFFICE FOR INFORMATION SECURITY, Technische Richtlinie BSI TR-02102-1 „Kryptographische Verfahren: Empfehlungen und Schlüssellängen“ 2022.

FINKE, DOUG, „IBM Extends Roadmap Up to 4,158 Qubits Using Multiprocessing and Advanced Software“, in: Quantum Computing Report (10.05.2022), URL: https://quantumcomputingreport.com/ibm-extends-roadmap-up-to-4158-qubits-using-multiprocessing-and-advanced-software/ (Accessed: 27.11.2022).

GAROFALAKI, ZACHARENIA et al., „Electric Vehicle Charging: A Survey on the Security Issues and Challenges of the Open Charge Point Protocol (OCPP)“, in: *IEEE Communications Surveys & Tutorials* 24, 3 (2022), S. 1504–1533.

GIDNEY, CRAIG / EKERÅ, MARTIN, „How to factor 2048 bit RSA integers in 8 hours using 20 million noisy qubits“, in: *Quantum* 5 (01.01.2021), S. 433.

GILLES, „Which cipher is more secure TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA or TLS_RSA_WITH_AES_256_GCM_SHA384?“, in: Information Security Stack Exchange (28.04.2022), URL: https://security.stackexchange.com/a/261602 (Accessed: 27.11.2022).

GOODIN, DAN, „Post-quantum encryption contender is taken out by single-core PC and 1 hour“, in: Ars Technica (08.02.2022), URL: https://arstechnica.com/information-technology/2022/08/sike-once-a-post-quantum-encryption-contender-is-koed-in-nist-smackdown/ (Accessed: 27.11.2022).

GRIEU, FRANCOIS, „rsa - Largest integer factored by Shor’s algorithm? - Cryptography Stack Exchange“ (08.09.2022), URL: https://crypto.stackexchange.com/questions/59795/largest-integer-factored-by-shors-algorithm/59796#59796.

GRIMES, ROGER A., *Cryptography apocalypse: Preparing for the day when quantum computing breaks today’s crypto*, Hoboken, NJ 2020, 248 S., ISBN 978-1-119-61823-2.

HÄNER, THOMAS / ROETTELER, MARTIN / SVORE, KRYSTA M., Factoring using 2n+2 qubits with Toffoli based modular multiplication 2017 arXiv:1611.07995 [quant-ph].

HERMAN, ARTHUR, „Q-Day Is Coming Sooner Than We Think“ (2021), URL: https://www.forbes.com/sites/arthurherman/2021/06/07/q-day-is-coming-sooner-than-we-think/ (Accessed: 16.10.2022).

HUANG, ROGER, „Here’s Why Quantum Computing Will Not Break Cryptocurrencies“, in: Forbes (2020), URL: https://www.forbes.com/sites/rogerhuang/2020/12/21/heres-why-quantum-computing-will-not-break-cryptocurrencies/ (Accessed: 27.11.2022).

IBM, „IBM Unveils 400 Qubit-Plus Quantum Processor and Next-Generation IBM Quantum System Two“, in: IBM Newsroom (2022), URL: https://newsroom.ibm.com/2022-11-09-IBM-Unveils-400-Qubit-Plus-

Quantum-Processor-and-Next-Generation-IBM-Quantum-System-Two (Accessed: 27.11.2022).

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION, Road vehicles - Vehicle-to-Grid Communication Interface – Part 2: Network and application protocol requirements (ISO 15118-2:2014) 2014.

KABIR, MOHAMMAD EKRAMUL et al., „A Two-Stage Protection Method for Detection and Mitigation of Coordinated EVSE Switching Attacks“, in: *IEEE Transactions on Smart Grid* 12, 5 (09.2021), S. 4377–4388.

KERN, DUSTIN / KRAUß, CHRISTOPH, Analysis of E-Mobility-based Threats to Power Grid Resilience, Ingolstadt, Germany 2021, ISBN 978-1-4503-9139-9.

KHALILI, JOEL, „Quantum computers may be able to break Bitcoin sooner than you think“, in: Techradar (2022), URL: https://www.techradar.com/news/quantum-computers-may-be-able-to-break-bitcoin-sooner-than-you-think (Accessed: 27.11.2022).

LEKITSCH, B. et al., „Blueprint for a microwave trapped-ion quantum computer“, in: *Science Advances* 3, 2 (03.02.2017).

LEONARD, DANIEL, „Inside the fight to protect your data from quantum computers - Scienceline“, in: ScienceLine (2022), URL: https://scienceline.org/2022/03/inside-the-fight-to-protect-your-data-from-quantum-computers/ (Accessed: 27.11.2022).

LI, KAI / CAI, QING-YU, „Practical Security of RSA Against NTC-Architecture Quantum Computing Attacks“, in: *International Journal of Theoretical Physics* 60, 8 (01.08.2021), S. 2733–2744.

LINDSAY, JON R., „Surviving the Quantum Cryptocalypse“, in: *Strategic Studies Quarterly* 14, 2 (2020), S. 49–73.

MARLINSPIKE, MOXIE / PERRIN, TREVOR, The Double Ratchet Algorithm 2016.

MARLINSPIKE, MOXIE / PERRIN, TREVOR, The X3DH Key Agreement Protocol 2016.

MARLONSPIKE, MOXIE, The ecosystem is moving. 36C3 Chaos Communication Congress, 01.01.2020.

MARTIN, KAREN, „Waiting for quantum computing: Why encryption has nothing to worry about“, in: TechBeacon (2018), URL: https://techbeacon.com/security/waiting-quantum-computing-why-encryption-has-nothing-worry-about (Accessed: 27.11.2022).

MASHATAN, ATEFEH / HEINTZMAN, DOUGLAS, „The Complex Path to Quantum Resistance“, in: *Queue* 19, 2 (01.01.2021), S. 65–92.

MOSCA, MICHELE, „Cybersecurity in an Era with Quantum Computers: Will We Be Ready?“, in: *IEEE Security & Privacy* 16, 5 (01.01.2018), S. 38–41.

NGUYEN, JAMES, „Y2Q Will Be Here Sooner Than You Think“, in: Cybercrime Magazine (27.07.2022), URL: https://cybersecurityventures.com/y2q-will-be-here-sooner-than-you-think/ (Accessed: 16.10.2022).

NIST, „Announcing PQC Candidates to be Standardized, Plus Fourth Round Candidates | CSRC“, in: Information Technology Laboratory - Computer Security Resource Center (24.03.2022), URL: https://csrc.nist.gov/News/2022/pqc-candidates-to-be-standardized-and-round-4 (Accessed: 27.11.2022).

NIST, „Post-Quantum Cryptography FAQ“, in: Information Technology Laboratory - Computer Security Resource Center (03.01.2017), URL: https://csrc.nist.gov/Projects/post-quantum-cryptography/faqs (Accessed: 27.11.2022).

OLIVIER BLAZY et al., How fast do you heal? A taxonomy for post-compromise security in secure-channel establishment, Anaheim, CA 2023.

OPEN CHARGE ALLIANCE, OCPP 2.0.1 Part 2 - Specification 2020.

RUDOLPH, HANS CHRISTIAN / GRUNDMANN, NILS, „TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384“, in: Ciphersuite Info (2022), URL: https://ciphersuite.info/cs/TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384/ (Accessed: 27.11.2022).

SAYED, M. et al., „Dynamic Load Altering EV Attacks Against Power Grid Frequency Control“, in: *IEEE Power & Energy Society General Meeting* (2022), S. 1–5.

SETHI, GURSIMRAN, „Quantum Computing Will Breach Your Data Security“, in: BRINK – Conversations and Insights on Global Business (2022), URL: https://www.brinknews.com/quantum-computing-will-breach-your-data-security/ (Accessed: 27.11.2022).

SHALF, JOHN, „The future of computing beyond Moore’s Law“, in: *Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences* 378, 2166 (06.03.2020), S. 20190061.

SHEKARI, TOHID / CARDENAS, ALVARO A. / BEYAH, RAHEEM, {MaDIoT} 2.0: Modern {High-Wattage} {IoT} Botnet Attacks and Defenses 2022, ISBN 978-1-939133-31-1.

SHOR, P.W., Algorithms for quantum computation: discrete logarithms and factoring 1994.

SOLTAN, SALEH / MITTAL, PRATEEK / POOR, H. VINCENT, BlackIoT: IoT Botnet of High Wattage Devices Can Disrupt the Power Grid. Baltimore, 2018.

TRAN, VIET T. / SUTANTO, DANNY / MUTTAQI, KASHEM M., The state of the art of battery charging infrastructure for electrical vehicles: Topologies, power control strategies, and future trend 2017.

WEBBER, MARK et al., The Impact of Hardware Specifications on Reaching Quantum Advantage in the Fault Tolerant Regime 2021, 22 S.

WESTERBAAN, BAS, „NIST’s pleasant post-quantum surprise“, in: *The Cloudflare Blog* (08.07.2022).

WESTERBAAN, BAS, „Sizing Up Post-Quantum Signatures“ (11.08.2021), URL: https://blog.cloudflare.com/sizing-up-post-quantum-signatures/.

ZHANG, LEI et al., Making Existing Software Quantum Safe: Lessons Learned 2021, 22 S.

Appendix

Excel Quantum Development Milestone Calculator

(own development)

Quantum Algorithm Performance			Development Extrapolation Calculator								
			Extrapolation based on current progress			Slow development			Fast development		
			Qubit	Qubit (log)	Year	Qubit	Qubit (log)	Year	Qubit	Qubit (log)	Year
		First year	3	0	1998	433	3	2022	433	3	2022
		Last year	433	2,6	2022	3.162	3,5	2040	100.000	5,0	2040
RSA	Million Qubits	Qubit (log)	Model predicts reaching cabability milestones		Year	Model predicts reaching cabability milestones		Year	Model predicts reaching cabability milestones		Year
RSA-2048@2400h	1	6,0	Breaching RSA-2048@2400h in:		2059	Breaching RSA-2048@2400h in:		2092	Breaching RSA-2048@2400h in:		2048
RSA-2048@5h	20	7,3	Breaching RSA-2048@5h in:		2074	Breaching RSA-2048@5h in:		2119	Breaching RSA-2048@5h in:		2058
RSA-3072@12h	38	7,6	Breaching RSA-3072@12h in:		2077	Breaching RSA-3072@12h in:		2125	Breaching RSA-3072@12h in:		2060
RSA-4096@22h	55	7,7	Breaching RSA-4096@22h in:		2079	Breaching RSA-4096@22h in:		2128	Breaching RSA-4096@22h in:		2061
RSA-8192@86h	140	8,1	Breaching RSA-8192@86h in:		2083	Breaching RSA-8192@86h in:		2137	Breaching RSA-8192@86h in:		2064
RSA-12288@200h	200	8,3	Breaching RSA-12288@200h in:		2085	Breaching RSA-12288@200h in:		2140	Breaching RSA-12288@200h in:		2065
RSA-16384@350h	270	8,4	Breaching RSA-16384@350h in:		2086	Breaching RSA-16384@350h in:		2143	Breaching RSA-16384@350h in:		2066
RSA-64000	256000000	14,4	Breaching RSA-64000 in:		2153	Breaching RSA-64000 in:		2267	Breaching RSA-64000 in:		2112