Migration to Post Quantum Cryptography

Recommendations for action by the BSI
**Änderungshistorie**

<table>
<thead>
<tr>
<th>Version</th>
<th>Datum</th>
<th>Name</th>
<th>Beschreibung</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0</td>
<td>31.05.2021</td>
<td>Referat KM 21</td>
<td>Englische Übersetzung</td>
</tr>
</tbody>
</table>

*Tabelle 1: Beschriftung*
# Table of Contents

1. Background .............................................................................................................................................................................................. 4
2. Post quantum cryptography ........................................................................................................................................................................ 5
3. Recommendations for action ..................................................................................................................................................................... 6
   3.1 Cryptoagility ................................................................................................................................................................................ 6
   3.2 Hash-based signatures for firmware updates .................................................................................................................................. 6
   3.3 Key lengths for symmetric algorithms ........................................................................................................................................ 6
   3.4 Short-term protective measures .................................................................................................................................................. 6
   3.5 Hybrid solutions ............................................................................................................................................................................. 7
   3.6 Adaption of cryptographic protocols ......................................................................................................................................... 7
   3.7 Quantum computer resistant key agreement ............................................................................................................................... 7
4. Literature ............................................................................................................................................................................................................ 8
1 Background

The security of today's digital infrastructures is largely based on public-key cryptography, which in turn essentially relies on the presumed hardness of two mathematical problems. The RSA-cryptosystem, for instance, is based on the assumption that in general it is hard to factor large numbers into their prime factors. Typically, one uses a public-key algorithm (also referred to as "asymmetric") to agree on a cryptographic key, which is then used to encrypt messages with a "symmetric" algorithm (e.g., AES). It is not known how to break the public-key algorithms currently in use with the methods and technology available today. However, this is no longer the case when large-scale quantum computers are available.

This is due to the fact, that in 1994, Peter Shor presented algorithms, which can efficiently solve the mathematical problems mentioned above. However, within present knowledge those algorithms cannot be realized or simulated efficiently on a classical computer, but only on a quantum computer, which, at that time, was a purely theoretical concept. The development of a large-scale quantum computer, which is able to run Shor's algorithm on sufficiently large problem sizes, would therefore

Symmetric cryptography is not threatened by Shor's algorithm. However, by Grover's algorithm for searching unsorted databases, a "brute force" search for the symmetric key could be significantly accelerated asymptotically [2]. However, the use of symmetric keys with a length of 256 bits is sufficient to mitigate this risk - even for data with a need for long-term protection.

So far, no quantum computer is available that would be suitable for breaking cryptographic algorithms. In order to obtain a well-founded assessment of the current state of development or the potential future availability of a quantum computer, the BSI commissioned the study "Status of quantum computer development" [3]. This study was conducted by researchers at Saarland University and Florida Atlantic University.

The study shows that currently an enormous effort would be needed to scale up quantum computing technologies to a cryptographically relevant level. At the same time, however, it becomes clear that the development has gained momentum through strong industrial players and large research programs, and that further commercial applications could accelerate this even further.

The study estimates that short-term development leaps in the direction of cryptographically relevant quantum computers are rather unlikely. For cryptographic applications that process information with long secrecy periods and high security requirements, there is nevertheless a need for immediate action. The danger encountered here is that messages exchanged for key negotiation and the data encrypted with the negotiated keys are collected in advance and decrypted in the future with the help of a quantum computer ("store now, decrypt later").

Signatures for the purpose of authentication, on the other hand, usually have a rather short lifespan and in principle only need to be secure until the time of their verification. If a signature algorithm can be broken by a quantum computer in the future, today's signature certificates will probably have already expired. Only in the case of very long validity periods for signature keys caution is required.
2 Post quantum cryptography

In cryptographic research, a new field has developed parallel to the development of quantum technologies: post quantum cryptography (also known as quantum safe cryptography). Post quantum cryptography deals with the development of and investigation in cryptographic algorithms that cannot be broken even with quantum computers. These quantum computer resistant algorithms are based on mathematical problems for which neither classical nor quantum are known today that solve them efficiently.

Researchers pursue various approaches to realize post quantum cryptography. Candidates for such methods are based, for example, on the difficulty of efficiently decoding general error-correcting codes (“code-based methods”) or on the difficulty of certain problems in mathematical lattices (“lattice-based methods”).

In recent years, post quantum cryptography has gained considerable importance: In August 2015, the American National Security Agency (NSA) warned against quantum computers and initiated the migration to quantum computer resistant algorithms. As a justification, the NSA cited advances in physics and technology that could enable the development of a cryptographically relevant quantum computer. The NSA did not mention any concrete quantum computer resistant processes, but referred to future standards of the National Institute for Standards and Technology (NIST).

As a US authority, NIST is responsible for standardization processes. Among other things, it has conducted competitions that have produced the globally recognized algorithms AES and SHA-3. In response to the NSA announcement, NIST started a process in November 2016, at the end of which a selection of quantum computer resistant cryptographic methods should be available\(^1\). However, this process will not be completed until 2022/23 at the earliest.

One class of algorithms not considered in the NIST process are stateful hash-based signature methods. This is because their security properties are very well understood and they are already considered to be mature quantum computer resistant signature algorithms. However, a decisive disadvantage is the state dependence of those algorithms, i.e. the signature creator must exactly keep track of the already used one-time signature keys. In addition, the number of signatures that can be created with this key must be fixed when the private key is created. The stateful hash-based signature methods LMS [4] and XMSS [5] have already been standardized by the IETF. NIST published a draft for a Special Publication at the end of December 2019 that adopts these standards.

BSI welcomes NIST's activities to standardize post quantum cryptography. They have led to a significant intensification of research into quantum computer resistant algorithms. The BSI is part of an international network in the field of cryptography. In this respect, the NSA announcement and the NIST standardization process are significant for the BSI and the BSI follows these developments closely.

\(^1\)See https://csrc.nist.gov/Projects/Post-Quantum-Cryptography for more information on the NIST process.
3 Recommendations for action

From BSI's point of view, the question "whether" or "when" there will be quantum computers is no longer in the foreground. Post quantum cryptography will become the standard in the long term. Depending on the use case, however, considerations should start at an early stage (and continuously - adapted to current developments) within the framework of an appropriate risk management whether and when a switch to quantum computer resistant algorithms should be made. Here, we would like to give recommendations for actions that describe how the migration to post quantum cryptography can be initiated today.

3.1 Cryptoagility

In the development of new and the maintenance of existing applications, particular attention should be paid to making the cryptographic mechanisms as flexible as possible in order to be able to react to all conceivable developments, implement upcoming recommendations and standards and possibly replace algorithms in the future that no longer guarantee the desired level of security ("cryptoagility"). This is especially important due to the threat posed by quantum computers - but not exclusively: classical attacks can also evolve and make encryption algorithms or key lengths obsolete that were once considered secure. Cryptoagility should therefore become a design criterion for new products - regardless of the development of quantum computers.

3.2 Hash-based signatures for firmware updates

As described in section 2, stateful hash-based signature algorithms have certain disadvantages. For example, only a limited number of signatures can be executed. However, they are particularly suitable for signing firmware updates, as only a small number of signatures are required. The use of stateful hash-based signature algorithms have a long history in the recommendations of the BSI - for example in the Technical Guidelines TR-02102 [6] and TR-03140 [7]. They are an important contribution towards cryptoagility.

3.3 Key lengths for symmetric algorithms

As already mentioned, symmetric encryption algorithms are much less threatened by the development of quantum computers than asymmetric algorithms. However, when using keys with a length of 128 bits (or less), quantum computer attacks with Grover's search algorithm are potentially possible. Especially if long-term protection of data is important, one should consider a key length of 256 bits for new applications which implement a symmetric encryption algorithm.

3.4 Short-term protective measures

Usually, one needs asymmetric cryptography to exchange a shared secret between the communication partners, from which symmetric session keys are then derived. As a short-term protective measure against attacks with quantum computers, a pre-distributed symmetric long-term key can additionally be used in the key derivation process. Likewise, it is possible to symmetrically encrypt an asymmetric key exchange using a pre-distributed secret. In both cases, of course, the problem of distributing the symmetric long-term keys must be solved in each case individually.

For cryptography on elliptic curves, the use of secret curve parameters introduces a certain protection against attacks with quantum computers. It should be noted that the curve parameters can be calculated if three points on the curve are known. Measures (e.g. point compression) must therefore be taken to protect the curve parameters. In addition, it must be ensured that the curves used are cryptographically suitable. Details can be found in [8].
3.5 Hybrid solutions

The quantum computer resistant algorithms that are currently being standardized are not yet analyzed as well as the "classical" algorithms (RSA and ECC). This is especially true with regard to weaknesses that become largely apparent in applications, such as typical implementation errors, possible side-channel attacks, etc. Therefore, the BSI does not recommend using post-quantum cryptography alone, but only "hybrid" if possible, i.e. in combination with classical algorithms. In a hybrid key exchange, for example, the two negotiated secrets must be combined by means of a suitable key derivation function to form a session key. In high-security applications, the BSI requires the use of hybrid solutions.

3.6 Adaption of cryptographic protocols

The switch to quantum computer resistant algorithms, especially the use of hybrid solutions, requires adjustments to the cryptographic protocols used today. First concepts already exist for the Transport Layer Security (TLS) and Internet Key Exchange (IKEv2) protocols, see [9] and [10]. These adaptations are independent of the concrete selection of quantum computer resistant algorithms.

3.7 Quantum computer resistant key agreement

The need for action concerning key agreement is - as already mentioned in the beginning - significantly greater than concerning signature algorithms. For a key agreement, the lattice-based algorithm FrodoKEM [11] and the code-based algorithm Classic McEliece [12] are the most conservative choices from the BSI's point of view. Since the protection of long-term secrets may require prompt action, the BSI decided at the end of 2019 not to wait for NIST's decision and states in the current version of the Technical Guideline on cryptographic algorithms and key lengths [6] that the two methods mentioned are basically suitable for key agreement (in a hybrid solution).

In mid-July 2020, NIST announced the candidates for the third round of the standardization process. While Classic McEliece is one of the four remaining key agreement algorithms, FrodoKEM has been placed on the list of alternative candidates, see [13]. Besides Classic McEliece, three lattice-based key agreement algorithms (CRYSTALS-Kyber, NTRU, SABER) are still in the third round. NIST justifies the decision to consider FrodoKEM only as an alternative method with the less efficient performance compared to the other lattice-based methods. The drop in efficiency is due to the fact, that the other methods are based on problems in lattices that have an additional structure. The additional structure offers the advantage that the corresponding methods are more efficient and require smaller keys. However, it also means that the BSI does not yet have the same confidence in the security of those algorithms. NIST also sees a potential danger that new attacks on lattice-based algorithms based on problems in "structured" lattices could be developed and considers FrodoKEM as a "conservative backup", cf. [13].

For the reasons outlined above, the BSI upholds its recommendation for FrodoKEM, even though FrodoKEM might be rather unsuitable for very specific use cases. The recommendations in the Technical Guideline will probably be supplemented by further algorithms once these have been standardized by NIST.
Literature


