Die Deutsche
Kreditwirtschaft

Position Paper of the German Banking Industry Committee on the Impact of the Development of Quantum Computers (12/2023)

Introduction

This document aims to provide an overview and raise awareness of the potential impact of quantum computing developments on the infrastructure of the German Banking Industry Committee (GBIC). It is intended for anyone responsible for the use of banking applications or their security.

Background

The IT security of the German banking sector relies heavily on cryptographic procedures. Within this context, GBIC uses standardised algorithms that have undergone rigorous scientific study. To reflect advancements in cryptanalysis and computer technology, GBIC adjusts its risk assessment at regular intervals. Based on this assessment, measures are designed and implemented to maintain a high level of security for banking applications going forward. This process led, for example, to specifications for the replacement of Triple DES by AES in card-based payment transactions, a move that has already been largely implemented.

Cryptographic algorithms can be divided into two classes: ***symmetric*** *and* ***asymmetric*** *algorithms.*
Symmetric cryptography requires a key to be shared beforehand between the communicating parties.
Asymmetric cryptography relies on a pair consisting of a public key, which may be known to others, and a private key, known only to its owner.
While symmetric methods are used for encryption and integrity and authenticity protection, asymmetric methods are primarily used for key establishment and digital signatures.

As considerable progress has been made in the development of quantum computers in recent years, particular attention is currently being paid to the threat to cryptographic procedures from quantum computers.

Security Agencies like BSI [1] and NSA [2] work under the hypothesis that cryptographically relevant quantum computers will be available by the early 2030s. This means that the quantum computers then available will be capable of carrying out realistic attacks on the asymmetric cryptographic procedures used today – RSA, DH and ECC – much more quickly than in attacks using ‘conventional’ computers [3, 4] by running variants of an algorithm introduced by Shor in 1997 [5].Security Agencies like BSI [1] and NSA [2] work under the hypothesis that cryptographically relevant quantum computers will be available by the early 2030s. This means that the quantum computers then available will be capable of carrying out realistic attacks on the asymmetric cryptographic procedures used today – RSA, DH and ECC – much more quickly than in attacks using ‘conventional’ computers [3, 4] by running variants of an algorithm introduced by Shor in 1997 [5].

Symmetric cryptography is also affected by a cryptographically relevant quantum computer, although the impact is more limited. Using an algorithm introduced by Grover [6] can accelerate a full key search (brute force) reducing the level of security to an extent equivalent to approximately halving the key size Based on current knowledge, the use of a key size of 256 bits is considered to provide sufficient protection for long-term sensitive data against attacks using quantum computers in the long term [1]. Grover's algorithm is currently regarded as the most relevant quantum attack on symmetric cryptography, even if other methods used in symmetric cryptography might be vulnerable as well, e.g., see the discussion of the impact of Simon's algorithm in [7].

To establish new standards for asymmetric cryptographic algorithms which are resistant to known quantum computer attacks the US National Institute of Standards and Technology (NIST) had initiated a standardisation process for so-called ‘post-quantum’ cryptography methods at the end of 2016 [8]. In August 2023, draft standards for the digital signature schemes CRYSTALS-Dilithium ("Module-Lattice-based Digital Signature", [9]) and SPHINCS+ ("Stateless Hash-based Digital Signature", [10]) as well as for the key establishment scheme CRYSTALS-Kyber ("Module-Lattice-based Key-Encapsulation Mechanism", [11]) were released. It is expected that the final standards will be available by 2024. The draft standard for the fourth algorithm selected to be standardised, FALCON, is also scheduled to be published in 2024 [12]. More algorithms are still under review by NIST and the scientific community, both in an additional round of the original standardisation process, and in a new process specifically looking for general-purpose signature schemes [13], and may be standardised at a later date.

Stateful hash-based signature schemes, which are also resistant to quantum computer attacks, are not subject of the NIST process. These schemes have limited applicability, but may be useful in certain scenarios, especially since two such schemes have already been standardised as RFCs [14, 15] and are recommended as a method for generating long-term secure signatures by the BSI [16].

Current status within GBIC

The replacement of Triple DES by AES in card-based payment transactions has been found to offer sufficient protection against attacks launched using quantum computers. This means that according to current knowledge there is no need for any additional action for the symmetric procedures that are used in direct communication between the card issuer and the card, as well as to secure the integrity and authenticity of messages during transmission and to encrypt the customer PIN for online transactions. Nevertheless, work should continue unabated on the migration process, and delays in the migration process are already to be assessed as critical today - irrespective of the quantum computer developments.

As far as asymmetric cryptographic procedures are concerned, the use of quantum computers heralds a paradigm shift, with the result that increased key sizes for procedures based on RSA, DH and ECC cannot, as might have been the case in the past, be considered an adequate countermeasure. Of the systems under the responsibility of GBIC, at least the following are affected:

- Card-based payment transactions, including the ATM system, payments at the POS, mobile payments, as well as the components used in these systems to execute cryptographic functions or store cryptographic material,
- Online banking for retail clients based on the German FinTS standard [17],
- EBICS standard for communication between financial market infrastructures and for communication with corporate clients [18],
- The banking interface based on the PSD2 standard (in particular the certificate infrastructure) [19],
- Secure internet communication.

Over and above these systems, systems that do not fall within GBIC's sphere of responsibility but are used in individual institutions also have to be taken into account.

Changes in cryptographic methods can very rarely be implemented by GBIC alone and GBIC is dependent on the agreements reached with international communication partners, including SWIFT, EMVCo, ECSG, EPC and manufacturers for terminals, cards, HSMs and EPPs, for instance.

Due to these dependencies and the need for investment in and modernisation of the existing infrastructure including terminals, payment system PKI and cards the migration of cryptographic procedures is a process with long timelines.

As post-quantum algorithms differ heavily in key and signature sizes und performance, there is no longer a one-scheme-fits-all-solution, which is applicable to a diverse range of application contexts. Therefore, selecting suitable algorithms and parameters and integrating them in the existing technical infrastructure presents a major challenge for GBIC.

As a consequence, it is important to start preparing for a migration to suitable post-quantum cryptographic procedures now.

Courses of action and recommendations

Although the standardisation of post-quantum cryptography is a process that will take a longer period of time yet, measures can already be taken at this point to prepare for a migration to quantum-safe cryptography. From the perspective of GBIC, these include the following measures (note that this list is not exhaustive):

1. **Closely follow the current state of science and industry**

One key prerequisite for migrating to quantum-safe cryptography is the continued monitoring of developments involving quantum computers and post-quantum cryptography. To this end, GBIC organises, for example, annual workshops with experts from the scientific community (universities and research organisations), security authorities (BSI) and industry to receive information on scientific, official and regulatory developments and to discuss the current status.

2. **Build inventory of cryptographic methods used throughout GBIC**

It is recommended that an inventory of the cryptographic procedures used throughout the German banking sector be prepared, including information on the parameters, the purpose, the need to store the information protected by the methods in the long term[1] and the expected lifetime of the cryptographic primitive used.

The GBIC Cryptography Working Group has already started to put this inventory together with the support of other GBIC committees. Individual institutions, data centres or banking industry service providers are also advised to create a similar overview of the procedures they use - other than the GBIC-wide applications.

3. **Prepare migration scenarios**

Since experience has shown that migration of cryptographic procedures can be a long process from planning to full implementation – particularly if hardware has to be replaced – it is necessary to develop migration scenarios at an early stage considering fallback strategies.

[1] This aspect is relevant because quantum-resistant methods may also have to be implemented (long) before the realisation of suitable quantum computers/critical algorithms.

Taking into account especially the recommendations of the BSI [5], working groups should develop migration scenarios for GBIC systems.

4. Prepare for crypto-agility

Crypto-agility should be considered as a matter of principle when designing new applications or adapting existing ones [1]. This means making the cryptographic mechanisms as flexible as possible in order to be able to react to all conceivable developments, easily implement future recommendations and standards, and replace algorithms including key sizes and parameters that no longer guarantee the desired level of security. This approach applies in particular to the growing threat posed by quantum computing developments but not exclusively so, as conventional attacks are also evolving and algorithms that were considered secure for years need to be replaced.

5. Use hybrid solutions

Since quantum computer-resistant methods have not yet been researched as well as conventional methods, so-called “hybrid solutions” should be taken into account wherever possible when new applications are designed, i.e. the use of post-quantum methods in combination with classical algorithms.

6. Increase key length for symmetric methods

In new applications that use symmetric encryption, the use of AES with a key size of 256 bits is recommended to provide long-term security against quantum attacks.

7. Use pre-shared symmetric keys for key establishment

Even though there is still no sufficiently powerful quantum computer that breaks the cryptographic algorithms currently used, it should be noted that encrypted data might be revealed in the future considering “store now - decrypt later”-attacks. Therefore, in terms of data with long-term protection requirements it is essential to act today, although post-quantum standards for key establishment are not yet available. A short-term solution can be the use of pre-distributed symmetric long-term keys. It is important, however, to remember that the problem of distributing the symmetric long-term keys has to be solved.

8. Increase use of online checks in card payment transactions

An increased use of online checks in card payment transactions can reduce dependency on the RSA procedure, which is currently used, e.g., for card authentication and offline PIN checks. As online authorisation based on AES can be used in card-based payment transactions – with only a few exceptions – it is recommended, from a cryptographic perspective, that this option be used.

9. Coordinate with international communication partners and manufacturers at an early stage

With a view to global payment transactions, discussions and consultation sessions on the introduction of quantum-safe cryptographic procedures must be conducted on an international level at an early stage. These talks are already under way in the context of card-based payments.

10. Use latest versions of standardised communication protocols for secure internet communication

Key agreement protocols, like those realised by protocols such as TLS, IPSec, and SSH, are in widespread use due to their connection to the back-end systems of banks and data centres, meaning that they would be particularly affected by attacks using quantum computers.

Depending on the protocol, (experimental) quantum-resistant versions are already being evaluated and are expected to be available in the near future [1]. Therefore, the principle of quickly updating to the latest versions will help mitigate the threat posed by quantum computing developments.

Abbreviations

AES	Advanced Encryption Standard
ATM	Automated Teller Machine
BSI	Bundesamt für Sicherheit in der Informationstechnik (German Federal Office for Information Security)
CRYSTALS	Cryptographic Suite for Algebraic Lattices
DES	Data Encryption Standard
DH	Diffie-Hellman key exchange
EBICS	Electronic Banking Internet Communication Standard
ECC	Elliptic Curve Cryptography
ECSG	European Cards Stakeholder Group
EPC	European Payments Council
EPP	Encrypting PIN Pad
FALCON	Fast Fourier lattice-based compact signatures over NTRU
FIPS	Federal Information Processing Standard
FinTS	Financial Transaction Services
GBIC	German Banking Industry Committee (Deutsche Kreditwirtschaft)
HSM	Hardware Security Module
IPsec	Internet Protocol Security
NIST	US National Institute of Standards and Technology
PIN	Personal Identification Number
PKI	Public Key Infrastructure
POS	Point of Sale
PSD2	EU Revised Payment Services Directive
RFC	Request for Comments
RSA	Rivest-Shamir-Adleman Cryptosystem
SSH	Secure Shell Protocol
SWIFT	Society for Worldwide Interbank Financial Telecommunication
TLS	Transport Layer Security

Bibliography

[1] BSI, “Kryptographie quantensicher gestalten, Grundlagen, Entwicklungen, Empfehlungen,” 2021.

[2] NSA, “https://www.nsa.gov/Press-Room/News-Highlights/Article/Article/3148990/nsa-releases-future-quantum-resistant-qr-algorithm-requirements-for-national-se/, NSA Press Release, 7 September 2022,” 7 September 2022. [Online].

[3] Deutscher Bundestag, “BT-Drucksache 19/26340 - auf die Kleine Anfrage - Drucksache 19/25549 - Die Verschlüsselungspolitik der Bundesregierung und das Engagement von ZITiS zum Brechen von Kryptografie,” 1 February 2021. [Online]. Available: https://dserver.bundestag.de/btd/19/263/1926340.pdf.

[4] ASC X9, “IR 01–2022, Informative Report - Quantum Computing Risks to the Financial Services Industry,” 2022.

[5] P. Shor, “Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer,” *SIAM Journal on Computing,* 1997.

[6] L. Grover, “A fast quantum mechanical algorithm for database search,” *Proceedings of the 28th Annual ACM Symposium on the Theory of Computing,* 1996.

[7] BSI, “Status of quantum computer development V2.0,” 2023.

[8] “NIST Projects - Post-Quantum Cryptography,” [Online]. Available: https://csrc.nist.gov/projects/post-quantum-cryptography/post-quantum-cryptography-standardization.

[9] NIST, FIPS 204 (Draft): Module-Lattice-Based Digital Signature Standard, August 2023 .

[10] NIST, FIPS 205 (Draft): Stateless Hash-Based Digital Signature Standard, August 2023.

[11] NIST, FIPS 203 (Draft): Module-Lattice-based Key-Encapsulation, August 2024.

[12] NIST, “NIST to Standardize Encryption Algorithms That Can Resist Attack by Quantum Computers,” 24 August 2023. [Online]. Available: https://www.nist.gov/news-events/news/2023/08/nist-standardize-encryption-algorithms-can-resist-attack-quantum-computers.

[13] NIST, “Post-Quantum Cryptography: Digital Signature Scheme - Call for Proposals,” 29 August 2022. [Online]. Available: https://csrc.nist.gov/projects/pqc-dig-sig/standardization/call-for-proposals.

[14] D. B. S. G. J. R. A. M. A. Huelsing, ““XMSS: eXtended Merkle Signature Scheme”, IETF RFC 8391,” 2018. [Online]. Available: https://tools.ietf.org/html/rfc8391.

[15] M. C. S. F. D. McGrew, “Leighton-Micali Hash-Based,” 2019. [Online]. Available: https://tools.ietf.org/html/rfc8554.

[16] BSI, “Technische Richtlinie TR-02102-1, Kryptographische Verfahren, Empfehlungen und Schlüssellängen, Version 2023-01,” 2023.

[17] “FinTS - Financial Transaction Services,” Die Deutsche Kreditwirtschaft, [Online]. Available: https://www.hbci-zka.de/.

[18] “EBICS - Electronic Banking Internet Communication Standard,” Die Deutsche Kreditwirtschaft, [Online]. Available: https://www.ebics.de/de/startseite.

[19] European Parliament, Council of the European Union, *Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market,* 2015.