SMART PAYMENT ASSOCIATION

The Security of Card Payment Systems in a Post-Quantum World

An SPA Position Paper

October 2022

Table of Contents

1. Introduction

Quantum computers have the potential to break cryptographic schemes, such as Rivest–Shamir–Adleman (RSA) and Elliptic Curve Cryptography (ECC); these are used in EMV® card payment systems for offline authentication to a payment terminal, offline PIN encryption from the terminal to the card and secure channel communications.

With this in mind, and assuming that quantum computers will be available in the future, this document discusses the specific risks quantum computing poses for card payment systems and introduces Post-Quantum Cryptography (PQC) – a new field at the intersection of mathematics, quantum physics, and computer science.

It also provides some timeline predictions, together with recommendations on migration paths from RSA to ECC to PQC for offline payment use.

2. The use of classical cryptography to protect card payments: an overview

Cryptography ensures the integrity, confidentiality, and authenticity of data exchanged during a card payment transaction across the entire payment processing circuit. Typically, asymmetric cryptography is used in offline payment processes between terminal and card, while symmetric cryptography is used in online payment processes between card and the issuer host system.

Asymmetric cryptography - RSA today, possibly ECC tomorrow - is used to perform offline card authentication. To achieve this, the card stores an asymmetric key pair and certificate and computes a cryptogram that is verified offline by the terminal to prove that the card is genuine. RSA cryptography may also be used to encrypt the PIN code entered on the terminal for secure transmission to the card where it is decrypted and verified.

Symmetric cryptography – Triple Data Encryption Standard (TDES) today and Advanced Encryption Standard (AES) tomorrow - is used in the transaction authorization process. The card stores an issuer TDES key and, during a payment transaction, computes an Application Cryptogram (AC) which is sent to the issuing bank. The AC signs transaction details, and its verification proves authenticity of both the card and the transaction.

When supported by the payment system and when the risk is low, the authorization may be granted offline by the terminal. Nevertheless, the card will still generate the application cryptogram using symmetric cryptography to produce a transaction signature called a Transaction Certificate (TC) which serves as a proof of the transaction. In this case, the AC is transferred together with the transaction details by the terminal, when it has an online connection, to start the actual settlement.

In card payment systems, both symmetric (TDES and AES) and asymmetric cryptographic mechanisms (RSA and ECC) are used according to EMV® specifications. Currently, international payment schemes use TDES for online and RSA for offline protocols. However, a migration towards AES for online and ECC for offline is anticipated in the very near future. Indeed, some regional card schemes are already using AES for online protocols today.

Historically, both algorithms (RSA and TDES) have proven to be very strong. When the cryptographic keys are properly generated and managed, the risk of fraud is negligible as illustrated by the figures published annually by the European Central Bank[1].

However, a migration from RSA to ECC and from TDES to AES is now being planned. This strengthening of both asymmetric and symmetric cryptography anticipates the perpetration of attacks on card payment systems using advanced classical cryptanalysis. SPA members are continuously evaluating future threats and developing countermeasures for card payment components. This is the reason why SPA supports the proposed ECC and AES planned migration for payment cards and terminals.

This paper discusses the potential threats to card payments should quantum computers become readily available for hacking purposes ("the post-quantum world").

3. Card payment systems in a post-quantum world

3.1. Quantum threats to symmetric cryptography

Commercial quantum computers do not exist today. The non-availability of this technology means that hackers could use the so called 'capture now, decrypt later' attack methodology. Essentially, this entails capturing highly confidential information (for example files containing inventions and industry secrets and/or government and defense secrets) that they cannot decrypt right now and holding this in anticipation of the day when they are able to access quantum computers.

Deploying this style of attack makes little sense for card payment systems due to the short time span involved in authorizing a payment by generating the application cryptogram and presenting it to the bank. Once the payment has been processed, application cryptograms are useless for fraud purposes as these cannot be reused in future without the fraud attempt being detected.

Of course, application cryptograms can be stored for some hours in the terminal before being transmitted and processed, so these could eventually be captured in real-time, decrypted, modified and re-encrypted. However, the TDES algorithm used by the card to generate the TC is robust and cannot be easily broken at present using classical computers, despite progress in cryptanalysis techniques (ex. the so called Oorschot-Wiener attack against TDES).

As previously discussed, the upcoming introduction of AES 128 bit, and even AES 256 bit, to replace TDES will give protection even if quantum computers are used. Contrary to asymmetric cryptography, the security of symmetric cryptography does not rely on the difficulty of solving "hard mathematical problems".

Symmetric algorithms are designed in such a way that the "easier" method to break them is to test all the possible keys that can be used to encrypt a particular message until the single right one is found out of 2^{128} (AES 128 bit) or even 2^{256} (AES 256 bit) possible combinations. With TDES, the

[1] Seventh report on card fraud (europa.eu)

effective level of security obtained is equivalent to "80 bit"[2], in other words finding one combination amongst 2^{80}, which could potentially be achievable in the future even with classical computers.

Therefore, TDES is not considered to be quantum-safe.

In 1996, Lov Grover found an algorithm[3], based on quantum computing, that could scan a list to find a particular data at an unprecedented speed. For cryptoanalysis, that was exactly what hackers needed to break symmetric algorithms. Grover's algorithm speeds up an unstructured search problem quadratically: if an algorithm takes O(N) steps to execute on a classical computer, the same result can be achieved in O (√N) steps on a quantum computer. So, the level of security measured in bits of entropy is halved. If, in a post-quantum world (when quantum computers are available), we target a "super high level of security" of 128 bit, we will need to migrate from AES 128 bit to AES 256 bit to achieve the same level of security. This migration is perfectly feasible. This is why the cryptographic community is confident about the quantum-resistant security properties of AES.

3.2. Threats to existing asymmetric cryptography in card payment systems

The present release of EMV® specifications limits the length of RSA keys to 1980 bit. The longer the keys, the higher the security of any cryptosystem. If card certificates are broken, then fake payment cards appearing as authentic could be used by fraudsters to, for example, perform offline transactions where the (symmetric) application cryptogram is not validated in real-time at the time of the purchase.

As explained earlier, SPA believes the RSA cryptosystem to be very robust and existing implementations should be considered practically unbreakable with classical computers for at least several years. But it is also true that, with increasing computing power at the disposal of hackers, less robust implementations of the RSA could be under threat. This could happen, even if quantum computers are not available yet for cracking cards.

To replace RSA, EMVCo has recently released specifications for the use of ECC in cards and terminals[4]. ECC provides an equivalent strength to RSA but with shorter key lengths. This opens the way to use longer keys providing increased security, while still using existing transmission protocols and smart card chip capabilities. SPA supports the migration to ECC cards and terminals as the best technical option to ensure the security of card payments and prevent existing RSA implementations from being compromised by classical cryptoanalysis in the future. Additional details are provided in section 4 below.

Yet, it has been argued that both RSA and ECC are vulnerable to quantum computing cryptoanalysis. The reasoning behind this is that the security of both RSA and ECC relies on the challenge of solving two difficult mathematical problems with classical computers. But with the power of quantum computers, hackers could solve these problems and thus break both of them. Let's examine the progress status in relation to quantum computing in some detail.

[2] On the Security of 2-key Triple DES - CJ Mitchell, Feb 2016

[3] A Fast Quantum Mechanical Algorithm for Database Search, Lov K. Grover, Nov 1996

[4] EMV® Specification Bulletin No. 243 First Edition October 2021

3.3. The real quantum threat to asymmetric cryptography

In 1994, Peter Shor designed an algorithm[5] that could be executed in a quantum computer and would be capable of breaking both RSA and ECC. Since then, significant optimizations have been published.

Nevertheless, this algorithm requires at least a few thousands of stable qubits to be operational. Recently, IBM announced the anticipated 2022 availability of its 433 physical qubit Osprey quantum processor and envisages the availability of one thousand qubits in upcoming years.

It should be noted that we are talking here about prototypes operating in a highly controlled laboratory environment, rather than commercial products. However, the actual level of performance of this computer has raised some questions[6]. Shor's algorithm requires the logical qubits stored in a quantum computer to remain stable, which is the number one challenge in quantum computing science today. At present, continuous error detection and correction of the few stored qubits is needed in quantum computer prototypes. In other words, many physical qubits need to be integrated together to achieve a single stable logical qubit.

Given the current state of quantum computing and real rates of progress, it is highly unlikely that a quantum computer capable of compromising RSA 2048 bit or comparable ECC-based cryptograms will be built within the next decade. Therefore, it is very reasonable to engage in a first migration of card payment systems to replace existing implementations of RSA by ECC to protect card payment systems from advanced cryptanalysis using classical computers. If quantum computing progresses at speed, then there will be time enough to plan a second migration to post-quantum crypto mechanisms.

To facilitate this second migration to a post-quantum world (assuming that commercial quantum computers will be available in future), crypto-agile payment systems will be needed. Crypto-agility can be defined as an operational characteristic of a cryptographic system that enables the switch from using an original crypto-mechanism to another crypto-mechanism while preserving, or minimizing, impact to the existing hardware and software system component and, ideally, in a way transparent for the end-users. Because payment cards are easy to replace and have a relatively short expiry date (3 to 5 years), crypto-agility should focus on card payment processing systems, starting with the terminal.

[5] Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer, Peter W. Shor, Jan 1996

[6] Speculative Preview of the IBM 433-qubit Osprey Quantum Computer, Jack Krupansky

4. The US National Institute of Standards and Technology (NIST) competition program for post-quantum cryptography

4.1. The NIST Program

Since 2016, NIST has sponsored an official competition to identify the next generation of cryptographic algorithms which can resist cryptanalysis using quantum computers, known as "post-quantum". This competition is organized in rounds. Prior to each round, NIST launches a call to the cryptographic community for post-quantum algorithms proposals/submissions. Those successfully selected progress to the next round. The key acceptance criteria for selection are the existence of security proofing and/or the absence of reported vulnerabilities and/or attacks. In a second step, these algorithms will be standardized by the NIST. The objective remains the standardization of a range of post-quantum algorithms covering most use cases for highly demanding applications including - but not limited to - payments.

Recently, NIST announced the selection of four algorithms as a result of the third round of the NIST PQC Standardization process: one public key algorithm for Key Encapsulation (Crystals Kyber) and three Digital Signature algorithms (Crystals-Dilithium, Falcon and Sphincs+). After their standardization, they are expected to be used in a wide variety of commercial security protocols, such as Transport Layer Security (TLS), Secure Shell (SSH), Internet Key Exchange (IKE) or Internet Protocol Security (IPsec). However, their implementation is challenging for the state-of-the-art card technology. This point is elaborated in the next section.

4.2. Payment cards and NIST 3rd round post-quantum algorithms

A key concern for the card payment industry is the substantial computing resources that will be required to implement the NIST post-quantum algorithms selected after the 3rd round.

Executing NIST post quantum algorithms on low-cost card crypto-processors is challenging. However, SPA Members have performed an impact assessment of the enhanced functional and processing features required by chips to execute the post-quantum algorithms pre-selected by the NIST[7]. Some of these algorithms (for example using post quantum key encapsulation mechanisms) may be run by new chips based on existing crypto-processors without radical evolutions in terms of extra-complexity and cost.

One common feature of the preselected NIST post-quantum algorithms is that their resistance to quantum computer attacks come at a cost. As an example, post-quantum algorithms require the execution of longer cryptographic keys, large RAM memories for intermediate crypto-calculations and in general a far more intensive computational effort, particularly for post-quantum digital signatures

[7] Post-Quantum Cryptography | CSRC (nist.gov)

such as Crystals-Dilithium. Transport protocols must be updated to convey longer certificates and more data is required by PQ cryptography.

Beyond the required technological hardware innovation, the evolution to a post-quantum world faces operational challenges. For instance, (1) finding ways to minimize risks during the migration process, (2) piloting hybrid post-quantum cryptographic solutions for cards, (3) understanding how crypto-agility could be facilitated with new card functionalities and (4) agreeing on a certification process for hybrid and later "pure" post-quantum payment cards.

To progress, agreements within the payments industry on one hand (standards bodies) and a more regular exchange of views with national security agencies and financial authorities on the other will be needed.

SPA notes that some European National Security agencies (for example, the French ANSSI and German BSI), even if supportive of the NIST post-quantum contest outline, recognize the lack of maturity of NIST post-quantum algorithms. Therefore, they are encouraging the industry to transition by first developing hybrid cryptography. In other words, designing cryptographic devices that combine a pre-quantum public key cryptographic scheme (RSA, ECC) with a post-quantum "well proven" algorithm. As an example, the NIST candidate algorithm Kyber could be a good option for the first hybrid deployments.

This combined approach would benefit from strong assurance on the resistance of the "classical" algorithm against classical attackers and the claimed resistance of the second post-quantum algorithm against quantum attackers. Indeed, hybrid solutions will probably facilitate a future progressive transition to post-quantum cryptography controlling risks.

4.3. The NIST fourth round

In July, NIST announced the start of the fourth round of the contest. In addition to the selected post-quantum algorithms at the end of the third round, four others are still in the race for the fourth round of the NIST program. This means that they are potential candidates for a later standardization after the conclusion of the fourth round. They all are Key Encapsulation mechanisms (BIKE, HQC, Classic McEliece and SIKE). However, since July, an attack on SIKE has already been published, compromising its future selection. The final outcome of the fourth round remains therefore very open.

Moreover, the NIST has launched a call for additional digital signature schemes for the PQC standardization process, by June 1 2023[8] . NIST is primarily interested in additional general-purpose signature schemes that are not based on structured lattices featuring short signatures and fast verification. Eligible digital signature schemes must include algorithms for key generation, signature generation and signature verification. Performance next to security is now a key criterion. Thus, submitters must include a statement describing the advantages and limitations of the candidate scheme. Interestingly, NIST notes that "this statement may address the ability to implement the algorithms in various environments, including, but not limited to, 8-bit processors (e.g., smartcards)".

[8] Call for Additional Digital Signature Schemes for the PQC Standardization Process (nist.gov)

In all, the criteria announced for the selection of new digital signature algorithms for the fourth round, could be a better fit for the technological capabilities of card crypto-processors.

SPA will continue to monitor the NIST selection process of post-quantum algorithms throughout the fourth round and regularly report progress to the payments industry.

5. The SPA efforts for a stronger cryptography in payment systems

Individual SPA Members are actively involved in different initiatives to mitigate the risks associated with the future quantum computing threat. The implementation of NIST post-quantum algorithms in card crypto-processors is a driver for innovation and creates the opportunity to reinforce industry partnerships between card and silicon vendors. Intensive R&D effort for a new generation of post-quantum small-size microcontrollers is ongoing.

Moreover SPA and its Members are actively involved in standards bodies (EMVCo, ECSG, PCI-SCC, ISO) to enhance the security of payment systems and facilitate a faster migration process to stronger cryptography. In the short to medium term, SPA recommends migration to Elliptic Curve Cryptography for payment cards and terminals. In the long term, the fourth round of the NIST context will enable the implementation of post-quantum public key cryptography in the card.

The drafting process of the new EMV® specifications to sustain ECC cryptography for payment cards and terminals has generated much discussion around the rationale of migrating to ECC cryptography, when ECC is not quantum resistant. To address the post-quantum challenge, one suggestion has been to move all card transactions online, avoiding the need for offline data authentication (ODA), and to use exclusively symmetric quantum resistant cryptography such as AES 256 bit. However, ODA capabilities continue to be essential for several use cases, such as at transit gates[9].

The SPA position in this debate has been clear since the beginning:

- We do not know if quantum computers will be available one day for ECC cryptoanalysis but what we do know is that the existing security of public key cryptography used in card payment systems needs to be reinforced.
- One key advantage of offline data authentication (ODA) is transaction speed and the replacement of RSA by the ECC will not impact the user experience in this respect.
- ECC is clearly the best public key cryptography option for cards and terminals as it offers the best trade-off between security and speed. Additionally, it makes it possible to increase security further by introducing the encryption of data transmitted with no significant increase in the transaction duration.
- ECC is a well-known and fully-mastered cryptographic algorithm that has been successfully used over the last two decades in highly demanding security applications, such as electronic passports and national ID cards.
- ECC migration is fully compatible with a simultaneous symmetric algorithm migration (TDES to AES) for cards and terminals because ECC and AES protect different stages of the payment transaction (see Section 2 of this paper).

[9] For more details see SPA's paper on "Why offline authentication still matters in today's online payments world"

- SPA members will support the payments industry to transition smoothly to the new ECC security mechanism and protocols that will protect issuers, merchants, and cardholders for at least the next decade.

6. Key take aways: SPA perspectives and recommendations

- The development of large-scale universal quantum computers would render virtually all of today's public-key cryptography insecure. But at present, we do not know when such machines will be available in the future.
- By contrast, progress in cryptanalysis techniques using classical computers is likely to put weaker public key implementations at risk. Cost-effective countermeasures exist and should be seriously considered by the payments community.
- As a consequence, SPA strongly recommends the adoption of more robust public key cryptography to counter emerging new cryptanalysis methods using classical computers in the coming years. For card payments, this means migrating from existing RSA to ECC crypto-systems that have key lengths long enough to ensure a higher level of security.
- SPA supports this transition to ECC cryptography being performed according to EMVCo specifications for both contact and contactless card payments.
- SPA emphasizes that application cryptograms of authorized card payment transactions are valid for a very short time only. This will make ‘capture now, decrypt later’ style attacks inapplicable to the card payment ecosystem.
- SPA does not underestimate the risks associated with future quantum computer developments. Technological breakthroughs are always possible and their potential impact on existing systems must be anticipated, especially considering the extended migration timelines that are typical for our industry.
- SPA closely monitors the ongoing developments and outcomes of the NIST contest for the selection and subsequent standardization of post-quantum public key algorithms and the positions of the National Security Agencies with respect to the cryptographic countermeasures.
- SPA supports the design and implementation of processes that speed up migration to stronger cryptography in the card payments industry. In particular, crypto-agile cards and terminals could be developed and rolled out as proposed by the standardization initiative in ISO.