How the financial sector can anticipate the threats of quantum computing to keep payments safe and secure

Received (in revised form): 29th April, 2020

Oscar Covers*
Senior Information Risk Consultant and Cybersecurity Analyst, Dutch Payments Association, The Netherlands

Marco Doeland**
Manager Risk Management, Dutch Payments Association, The Netherlands

Oscar Covers

Marco Doeland

Oscar Covers *is Senior Information Risk Consultant and Cybersecurity Analyst at the Dutch Payments Association. He analyses ICT-related security risks for the Financial Institutes — Information Sharing and Analysis Centre and, where necessary, coordinates the response. He chairs the European Cards Payments Association Security Working Group and participates in the working group that maintains the international requirements for payment terminals. He is also a member of the board of advisors that advises the payment card industry on issuing and maintaining the international security standards used by American Express, Discover, JCB, Mastercard and Visa.*

Marco Doeland *is Manager Risk Management at the Dutch Payments Association and the Chief Information Security Officer of Currence. He is responsible for managing the shared interests with respect to the security and cyber security of the Dutch payment infrastructures, including online, cards, mobile, iDEAL and iDIN. He is also Chairman of the Security Task Force at the Dutch National Forum on the Payment System and Chairman of the Interbank Security Task Force. In addition, he is a member of the Dutch Financial Institutes — Information Sharing and Analysis Centre (FI-ISAC), the European EU FI-ISAC and the global FS-ISAC.*

Abstract

At the end of 2015, the Dutch General Intelligence and Security Service informed owners and managers of vital infrastructure in the Netherlands about the developments and threats emanating from the advent of quantum computing. Dutch financial institutions have since started to monitor developments in quantum computing and are seeking to understand the implications for their interbank business processes. This paper looks at how banks and payment institutions can anticipate how quantum computing will evolve and respond accordingly, even though developments remain ongoing. To gain and maintain a good understanding, the Dutch Payments Association brings together quantum computing experts and experts from financial institutions to discuss the impact of quantum computing advancements on the industry. The key deliverable is to offer an approach to dealing with the threats associated with quantum computing, so that payment systems can continue securely and undisturbed. As this paper will discuss, this has resulted in a quantum readiness programme and seven so-called low-regret moves.

Keywords: quantum computing, post quantum cryptography, financial sector, banks, cyber security, payments

Dutch Payments Association,
PO Box 83073,
1080AB
Amsterdam,
The Netherlands
**E-mail: o.covers@betaalvereniging.nl*

***E-mail: m.doeland@betaalvereniging.nl*

Journal of Payments Strategy & Systems
Vol. 14, No. 2 2020, pp. 147–156

INTRODUCTION

Research into quantum computing is evolving quickly.[1,2] Quantum simulation and quantum machine-learning algorithms can help find new medicines, elucidate reaction mechanisms in complex chemical systems, making it possible to mimic chemical processes found in nature that are more efficient than the processes currently used in the chemical industry, and so on. In short, quantum technologies are expected to have a profound impact on many of the world's largest markets.

One area where quantum technologies pose a particular threat, however, is cryptography, as quantum computing makes it much easier to retrieve corresponding cryptographic keys. While nobody knows exactly when this threat will actually manifest, it is essential for the financial sector to understand the extent to which advances in quantum computing affect the security of the core banking and payment services. To gain the required understanding, the Dutch Payments Association (DPA) is bringing together quantum computing experts and experts from financial institutions to discuss how advances in quantum computing may impact on the financial sector.

WHY THE QUANTUM COMPUTER IS A THREAT

It all starts with the information unit. The information unit of the classical computer is the 'bit'. A bit has two states: zero (0) and one (1). The quantum computer, however, uses a 'qubit' (quantum bit), which is in both states at the same time. This concept is known as superposition. Another quantum fact is that a qubit in a superposition cannot be observed directly. When the qubit is measured it will 'collapse' into a 0 or 1 in an unpredictable way. As the information unit has different properties, quantum calculations also follow a fundamentally different approach. First, the input must be presented as a superposition of all possible states, so the computation is performed on multiple states simultaneously; this is known as quantum parallelism. Secondly, the input is processed using a series of quantum gates that can create and process superposition states. A quantum gate is like a logical gate — a basic operating circuit performing a logical operation based on a small number of qubits leading to a result. Beside the gate operations, measuring the state of a qubits is also one of its functions. Measurements are often an indispensable aid in the calculation phase. Finally, a measurement is made of the qubits. However, if the final state is a superposition, the answer will not deliver a coherent result as the collapse delivers an unpredictable outcome. In that case, the calculation can be repeated multiple times to determine the result with the highest probability.

While quantum computing offers new directions to solve computational problems, the quantum parallelism causes it to scale up quickly. Adding one qubit doubles the computing capacity of the quantum computer. Some known 'hard problems' are exponentially faster to solve with a quantum computer. This opens up new possibilities for finding new chemical processes, new drugs and so on, but also weakens certain existing encryption algorithms, with clear consequences for the encryption currently used to secure data.

CURRENT ENCRYPTION, OR COMMON CLASSICAL CRYPTOGRAPHY

Symmetric-key algorithms

The most common and well-known encryption method is the symmetric encryption or, more accurately, symmetric-key encryption. The symmetric-key algorithms use the same key for both encryption of plaintext and decryption of the encrypted text. This key, which is used to secure the data, is a secret shared by the parties. Many secret writings

made by enthusiasts, such as Julius Caesar,[3] probably fall into the category of symmetric encryption.

Well-known symmetric-key algorithms include the Data Encryption Standard (DES) and its successor, the Advanced Encryption Standard (AES). DES dates from the early 1970s and ought to have been replaced already, but the trick of cycling through the algorithm three times with two or three different keys prolonged its life.[4] Today, there are still many systems that use triple DES. The current gold standard for symmetric-key algorithm is AES.[5]

The big advantage of symmetric encryption is that it is very fast; the disadvantage is the shared secret key. After all, if someone is able to discover this secret key, all encrypted messages can be decrypted and read as well as manipulated and re-encrypted. Furthermore, in the case of multiple communication partners, a unique key is needed for each communication partner, which soon results in an untenable situation. So, symmetric-key algorithms always lead to key distribution concerns.

Asymmetric public-key algorithm (classical)

Asymmetric public-key algorithms distinguish themselves by the fact that they employ two keys that together form a single pair. What is encrypted with one key can be decrypted only by the associated key. This makes it possible to make one key publicly known; after which anyone can use this public key to encrypt a message for the owner of the other key. In this case, the other key must be kept private to make sure that only the owner is able to decrypt the message, hence this key is known as the private key.

Based on the feature that what is encrypted with a public key can be decrypted only by using the associated private key, any person can encrypt a message using the receiver's public key, and that encrypted message can be decrypted only by using the receiver's private key. This is a big advantage. Public-key algorithms do not need a secure channel for the initial exchange of one or more secret keys between the communication parties. The drawback is that it is computation-intensive, particularly in comparison with symmetric-key algorithms.

Examples of asymmetric public-key algorithms include RSA (an acronym of the surnames of Ron Rivest, Adi Shamir and Leonard Adleman), the digital signature algorithm (DSA) and elliptic-curve cryptography (ECC).

Cryptographic hash functions

Cryptographic hash functions are a special class. The hash function can be used to map data of arbitrary size to data of fixed size. It is used to verify data integrity and is designed as a one-way function, which cannot be reversed.

Cryptographic hash functions are widely used not only to verify data integrity but also as building blocks to construct a digital signature or message authentication code. They are also used for pseudorandom generation and key derivation.

Examples of cryptographic hash algorithms include the MD5 message-digest algorithm and secure hash algorithms (SHAs). SHAs are cryptographic hash functions published by the National Institute of Standards and Technology (NIST).

Key distribution

Traditionally, a requirement of secure communication between two parties is that they first exchange key parts in a secure manner; for example, via a face-to-face meeting. At the key ceremony, each party brings its key part in order to

derive one secret key. It is also common to use multiple trusted couriers to deliver key parts in order to arrive at one key, and so on. As discussed, the disadvantage of symmetric key cryptography is that both parties must have a shared common secret key.

The Diffie-Hellman (DH) algorithm provides a method of generating a shared secret between two people in such a way that the secret cannot be obtained by observing the communication. For key exchange, the DH key exchange protocol is the de facto standard. Note, however, that DH is a non-authenticated key-agreement protocol. Two parties who do not know each other can jointly establish a shared secret key over an insecure channel. This key can then be used to encrypt the next communication using symmetric key encryption. The DH key exchange is a public-key technology which by itself is not an encryption algorithm. It is an asymmetric technology used to negotiate symmetric keys.

For payments, the aforementioned encryption algorithms are used for:

- encryption of data;
- exchange of encryption keys;
- guaranteeing data integrity; and
- authenticity and nonrepudiation of transactions.

Traditionally, financial transactions are secured with symmetrical encryption for performance reasons, but due to the advantages that asymmetrical encryption offers, current transactions also rely on asymmetrical encryption.

In general, it can be stated that encryption raises a computational barrier. However, the hard problems of classical cryptography are tailored to the current available computation power — some of the hard problems of today turn out to be easily solvable with a quantum computer. In this respect, two quantum algorithms have a high impact on current classical cryptography:

- *Shor's algorithm*,[6] named after mathematician Peter Shor, was formulated in 1994. Compared with its classical counterparts, it has the potential to provide exponential speedup of integer factorisation and related public-key primitives. By implication, it could be used to break almost any public-key algorithm that does not use extremely large keys.
- *Grover's algorithm*,[7] named after the computer scientist Lov Kumar Grover was formulated in 1996. This algorithm finds, with high probability, the unique input to a black box function that produces a particular output value. Grover's algorithm provides a quadratic speedup over a classical computer algorithm. However, even quadratic speedup is considerable and can affect the security levels of symmetrical encryption systems.

IMPACT IN WORST-CASE SCENARIOS

In the words of Daniel J. Bernstein, a leading academic in the field of post-quantum cryptography:

> 'Nobody has figured out a way to apply "Shor's algorithm" — the quantum-computer discrete-logarithm algorithm that breaks RSA and DSA and ECDSA — to any of these systems. Another quantum algorithm, "Grover's algorithm", does have some applications to these systems; but Grover's algorithm is not as shockingly fast as Shor's algorithm, and cryptographers can easily compensate for it by choosing somewhat larger key sizes'.[8]

According to a worst-case scenario, the current block ciphers can be made Grover-resilient by doubling the key length. For an algorithm like AES this is not a problem; for DES, however, this is not possible. With regard to cryptographic

hash functions, the Grover algorithm seems to provide some non-trivial quadratic speedup. However, no problem arises when the output of the hash function is doubled.

Shor's algorithm has the greatest impact on public-key algorithms, which can be considered broken.

The resources needed to implement the Grover or Shor algorithm to break current cryptography systems, however, are not yet available. To date, quantum computing does not yet constitute a threat to current protections. At the moment when this finally happens, referred to as *day z*, there will be varying degrees of impact on some notable and popular kinds of cryptography. The difficulty of putting a date on that moment does not reduce the impact of the inevitable consequences, but it may delay the prioritisation of mitigation.

So, how to continue? Mosca's theorem is helpful here.[9] In brief: if $x + y > z$, then it is time to panic. Here:

- x is the security shelf life — how long the encryption algorithm will remain secure in combination with that key;
- y is the migration time — the time needed to migrate from the current encryption solution to a secure encryption solution; and
- z is the quantum computer, or another method that breaks the aforementioned cryptography primitive x.

In other words, if the security shelf life of the current encryption solution in use and the time to migrate to a secure solution lie beyond the *day z* on which a quantum computer breaks the cryptography, then it is time to panic.

Consequently, if data must be guaranteed confidential into the long term, then the owner of the data has a major challenge — perhaps even a problem — should the confidential data be exchanged over a public channel. After all, an adversary can intercept the communication, store the encrypted communication and wait patiently for the moment the encryption can be broken to decrypt the communication retroactively. This is exactly the challenge faced by governments and embassies.

The question is: what encryption is still secure in the era of the quantum computer? For symmetric-key algorithms, the threat can be mitigated by doubling the key length. For public-key cryptographic algorithms, other alternatives are needed.

NIST POST-QUANTUM CRYPTOGRAPHY STANDARDISATION

In April 2016, NIST published a report on post-quantum cryptography, stating that it anticipates quantum technology will render the commonly used RSA algorithm insecure by 2030.[10] As a result, a need to standardise quantum-secure cryptographic primitives arose. The efforts therefore focus on public-key cryptography, explicit digital signatures and key encapsulation mechanisms. In December 2016, NIST initiated this standardisation process by issuing a call for proposals.

The academic world had already anticipated this. Even before 2005, many researchers had begun investigating post-quantum cryptography (PQC). This work received more attention after the PQCrypto conference series, which started in 2006, and several workshops on quantum safe cryptography, organised by the European Telecommunications Standards Institute (ETSI) and the Institute for Quantum Computing.

In the initial submission at the end of 2017, NIST received 23 signature schemes and 59 key encapsulation mechanisms, of which 69 were deemed complete and proper. At the beginning of 2019, nine signature schemes and 17 key encapsulation mechanisms went to the second

round. The work is expected to be completed between 2022 and 2024.

KNOWN COMPLICATIONS AND KNOWN UNKNOWNS

The appropriate response to the looming threat of quantum computing is to identify cryptography that is sensitive to quantum attacks and replace it with PQC. Practically, this raises significant challenges for asymmetric cryptography.

For the banking industry, replacing cryptography is a process with very long timelines. For example:

- The typical payment card replacement cycle takes about eight years. Certification and selection usually take three years, and issued cards can be used for five years, until they expire. While it is possible to replace a bank card within a year, this comes at a considerably higher cost.
- Point-of-sale (POS) terminals and automated teller machines (ATMs) have life cycles ranging from five to 20 years. In the Netherlands, a POS terminal has an economic service life of five years; however, the mean usage time of a POS terminal is currently seven years. No economic life span has been determined for ATMs, but many are at least 20 years old, and only some can be adjusted remotely.
- Many institutions are still using critical systems that are decades old, despite efforts to decommission them.
- Replacing cryptography may not be enough, as some of the essential PQC alternatives are expected not to be simple drop-in-replacements. The need to revisit design assumptions and redesign to-be-identified systems should be taken into account, as redesign will be time-consuming.
- Standards and policies for the use and roll-out of PQC do not exist yet and need to be developed.

Addressing quantum computing also suffers from the fact that several significant aspects are — just as *day z* — still largely unknown. The fields of quantum computing and PQC are still very much in flux, which means it is uncertain what form attacks will take and what defences will be effective.

SOME COMFORTING CERTAINTIES

While quantum computing may lead to the total collapse of some kinds of cryptography, other kinds of cryptography are expected to withstand quantum computing with no adjustments, or no fundamental adjustments, as mentioned above:

- Modern symmetric encryption algorithms such as AES remain secure. It is assumed that AES-256 can be used securely until 2031 and beyond.[11]
- Modern cryptographic hash functions such as SHA-256 and SHA-3 will remain secure through 2031 and beyond.[12] Technology built on these symmetric encryption and cryptographic hash functions and algorithms, such as message authentication code (MAC), key generation and key derivation, will remain secure.
- The protocol concepts of the 'old era' cryptographic card payments industry that predate the use of asymmetric cryptography remain valid and secure. The actual cryptographic algorithms used in these protocols of the old era, however, need to be replaced with modern variants if this has not already been done.
- The quantum computer will probably first demonstrate its added value for other, less demanding applications.[13] Only later will the quantum computer become powerful enough to break cryptography.[14] Such events, if made public, can be used as an early warning indicator announcing that *day z* is at hand.

THE DUTCH QUANTUM READINESS PROGRAMME

There are still many uncertainties relating to quantum computers, most notably when the first quantum computer will be available; however, there are also some certainties. Based on these certainties, it is possible to identify certain 'low-regret' moves to prepare for the advent of the quantum computer. Thus, the following seven low-regret moves or recommendations have been formulated to deal pragmatically and realistically with the threats associated with quantum computing.

These recommendations have been adopted within the governance of the Dutch Payments Association and its members, and have been approved by the CISOs of the DPA's member banks and adopted by the responsible board members. In ensuring board-level commitment, these recommendations become policy guidelines. Accordingly, support for the programme has been arranged and the work has started. The seven policy guidelines are:

1. Follow developments on quantum computing and PQC closely.
2. Maintain and extend the current inventory of interbank processes.
3. Urge international financial organisations to prepare for the advent of the quantum computer.
4. For classical symmetric cryptography, start the migration to AES, secure hashes and secure key derivation immediately.
5. Develop fallback to classical symmetric cryptography for the card payments infrastructure.
6. Develop an EMV smart card profile that does not rely on asymmetric encryption.
7. Enforce a policy to swiftly implement the latest official TLS releases and gain experience with PQC.

These seven policy guidelines will now be described in more detail.

Follow developments on quantum computing and PQC closely

Advances in quantum computing and PQC will influence the manoeuvring space the financial sector has to prepare and mitigate properly.

The DPA organises annual workshops and asks the broad expert group of participants to monitor the developments. The broad expert group consists of selected invitees: leading scientists from the field and relevant security experts from member banks, EMVCo, Mastercard and Visa.

With the outcome of the workshop, banking specialists can translate general developments into interbank-relevant actions, validate the established long-term interbank plan annually and provide advice when necessary to update the long-term plan. A second result is an updated set of questions and answers, which can be used to inform the press when questions are asked.

Maintain and extend the current inventory of interbank processes

The readiness project group is responsible for the inventory of interbank processes to guide the actions that must be taken. This inventory includes the security shelf life of encryption primitives used in addition to secure PQC alternatives (as stated by authoritative bodies such as EMVCo and NIST). Suppliers are included in the inventory, as standard packages regularly use old, possibly unsafe, techniques.

Urge international financial organisations to prepare for the advent of the quantum computer

In the Netherlands, the members of the DPA know how to find each other quickly and easily; however, payment transactions do not stop at the Dutch borders. It is therefore important that international parties in the

payments system take action to consider and act upon developments in quantum computing. If desired, the DPA is willing to share its approach to help other financial institutions to speed up their process.

For classical symmetric cryptography, start the migration to AES, secure hashes and secure key derivation immediately

Many symmetric encryption algorithms being used today are either insecure already without quantum computing (two-key triple DES, for example, is already disallowed by NIST) or come with a degree of security risk that will become unacceptable in the near future (for example, three-key triple DES is already deprecated by NIST and will be disallowed after 2023).[15] This migration will have a major impact on many financial institution systems, hence it is important to commence the migration to AES as soon as possible. Similarly, the migration to PQC cryptographic hash functions, such as SHA-256 and SHA-3, along with PQC key derivation functions, should be commenced without delay.

Develop fallback to classical cryptography for the card payments infrastructure

About 20 years ago, asymmetric public-key algorithms were introduced to the Dutch interbank infrastructure. This cannot simply be reversed. Furthermore, asymmetric public-key algorithms do have added value. Asymmetric encryption is used mainly for secure remote key distribution and signing. The classical symmetric encryption functions MAC, challenge response and traditional secure key distribution (using a secure physical link or using key custodians with key envelopes or smart cards) can also be used to provide the same functionality.

The change from the current to a modern-day PQC equivalent of the old-era protocols requires changes throughout the payment infrastructure, including POS and ATM systems. Fortunately, these systems have the necessary capabilities to make such a switch. Unfortunately, changing this infrastructure is a complicated and time-consuming operation. Given that *day z* is unknown, and POS and ATM protocol migration is a process with very long timelines, it is recommended that the development of the outlined fallback scenario be started immediately.

Develop an EMV smart card profile that does not rely on asymmetric encryption

Retail card payments depend greatly on cards using the EMV standard. In addition to symmetrical encryption, the current EMV card profile also uses asymmetrical encryption. The Dutch EMV card infrastructure offers the opportunity to develop a card profile that — to protect the transaction — relies entirely on symmetrical encryption using AES. For this option, all transactions must be authorised online, which fortunately is common in the Netherlands. However, for transactions in the transport sector, for example, offline EMV is commonly used. These transactions rely on the asymmetric encryption and cannot easily be processed entirely online in real time. For these transactions, it seems workable to develop a 'near real-time' scenario. In such a case, they remain offline EMV transactions but are frequently sent in for processing. The transactions will therefore be recorded in near-real time and will become irrefutable, reducing the dependence on asymmetric encryption.

Another topic is the processing host, which must also be able to process authorisation messages based on AES. The current EMV card specifications do support all necessary encryption primitives, but the international card brand schemes and the issuing processing host systems in the Netherlands do not.

With reference to the long migration route from introduction to withdrawal of the last card, it is advisable not to wait too long before issuing an instruction to develop an EMV smart card profile that does not rely on asymmetric encryption.

Enforce a policy to swiftly implement the latest official TLS releases and gain experience with PQC

TLS is widely used to secure data in transition, for example, the internet. External-facing systems using TLS are more flexible than back-office banking systems with respect to their ability to migrate smoothly and swiftly to PQC algorithms. For these systems, the readiness group expects that a quantum proof TLS version will arrive in time before *day z*. After all, the NIST competition submissions contain several practical algorithms for key exchange that can be used as drop-in replacement for current key exchange protocols. For example, New Hope is currently used in a pilot for TLS. However, other PQC NIST competition alternatives for RSA and ECC show that potential alternatives behave very differently in terms of key size, signature size, required computation and required storage. In all the alternatives, at least one of these parameters is many times worse than the current algorithms. This means that drop-in replacements are not likely to exist. Using the alternatives will entail significant changes in architecture, dimensioning or workflow and redesign of protocols.

Preparing and committing to swift adoption of new TLS versions will therefore help mitigate the negative impact of quantum computing and build up timely experience with PQC implementations.

NATIONAL AND INTERNATIONAL APPROACH

The DPA will use its relations and various roles to maintain a secure, stable and robust payment system. The experience of the Netherlands has taught that cooperation can lead to a safer and more secure payment world.[16] This is also the case for quantum computing. It is important to involve and advise the parties concerned, to ensure that information is exchanged and that these parties collaborate — not just within the Netherlands, but across the rest of Europe and the world too. To deal with the threats associated with quantum computing, the active involvement of participants is necessary. This applies to banks, payment processors, vendors and schemes, as well as to universities and governments. The DPA will make every effort to ensure that quantum readiness is on the national and international agenda.

AUTHORS' NOTE

The authors would like to thank the following members of the quantum readiness programme for their contributions: Harld Röling and Daphne Ma (ABN AMRO), René Steenbeeke (Dutch Payments Association), Arne de Boer (De Nederlandsche Bank), Jurjen Bos (equensWorldline), Wouter Teepe and Elif Yesilbek (ING), Arie Schilp (Rabobank) and Ron Werther (De Volksbank).

References

(1) Birch Consultants (2018) 'Building a Q-campus: realising a quantum ecosystem in Delft', available at: www.rijksoverheid.nl/binaries/rijksoverheid/documenten/rapporten/2018/10/04/building-a-qcampus-realising-a-quantum-ecosystem-in-delft/Building a Q-Campus - Realising a Quantum ecosystem in Delft.pdf (accessed 20th April, 2020).

(2) Russo, M., Thaker, A., and Adam, S. (2018) 'The coming quantum leap in computing', available at: www.bcg.com/publications/2018/coming-quantum-leap-computing.aspx (accessed 20th April, 2020).

(3) Van Der Lubbe, J.C.A. (1998) 'Basic Methods of Cryptography', Cambridge University Press, Cambridge.

(4) Karn, P., Metzger, P. and Simpson, W. (1995) 'The ESP triple DES transform', RFC1851, available at:

https://tools.ietf.org/html/rfc1851 (accessed 20th April, 2020)
(5) Rijmen, V. and Daemen, J. (2001) 'Advanced encryption standard', in 'Proceedings of the Federal Information Processing Standards Publications, National Institute of Standards and Technology', Gaithersburg, MD, pp. 19–22.
(6) Shor, P.W. (1994) 'Algorithms for quantum computation: discrete logarithms and factoring', in Proceedings the 35th Annual Symposium on Foundations of Computer Science, Santa Fe, NM, 20th–22nd November.
(7) Grover, L.K. (1996) 'A fast quantum mechanical algorithm for database search', in Proceedings of the 28th Annual ACM Symposium on Theory of Computing, Philadelphia PA, May
(8) Bernstein, D.J. (2009) 'Introduction to post-quantum cryptography', in 'Post-quantum Cryptography', Springer, Berlin and Heidelberg, pp. 1–14.
(9) Mosca, M. (2013) 'Setting the scene for the etsi quantum-safe cryptography workshop', e-proceedings of 1st Quantum-Safe-Crypto Workshop, Sophia Antipolis, 26th–27th September.
(10) Chen, L., Jordan, S., Liu, Y.-K., Moody, D., Peralta, R., Perlner, R. and Smith-Tone, D. (2016) 'NISTIR 8105 Report on Post-Quantum Cryptography', available at: https://csrc.nist.gov/publications/detail/nistir/8105/final (accessed 20th April, 2020).
(11) Barker, E., Barker, W., Burr, W., Polk, W. and Smid, M. (2007) 'Recommendation for Key Management – Part 1: General (Revision 3)', NIST special publication 800-57, available at: https://adgrafics.net/docs/other/sp800-57_part1_rev3_general.pdf (accessed 20th April, 2020).
(12) *Ibid*.
(13) Reiher, M., Wiebe, N., Svore, K.M., Wecker, D. and Troyer, M. (2017) 'Elucidating reaction mechanisms on quantum computers', *Proceedings of the National Academy of Sciences*, Vol. 114, No. 29, pp. 7555–7560.
(14) Roetteler, M., Naehrig, M., Svore, K.M., and Lauter, K. (2017) 'Quantum resource estimates for computing elliptic curve discrete logarithms', paper presented at the International Conference on the Theory and Application of Cryptology and Information Security, Hong Kong, 3rd–7th December, available at: https://eprint.iacr.org/2017/598.pdf (accessed 20th April, 2020).
(15) Barker, E. and Roginsky, A. (2019) 'Transitioning the Use of Cryptographic Algorithms and Key Lengths', NIST Special Publication 800-131A Revision 2, available at: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-131Ar2.pdf (accessed 20th April, 2020).
(16) Doeland, M.M. (2017) 'Collaboration and the sharing of information help reduce payment transactions fraud', *Journal of Payments Strategy & Systems*, Vol. 11, No. 3, pp. 81–85.