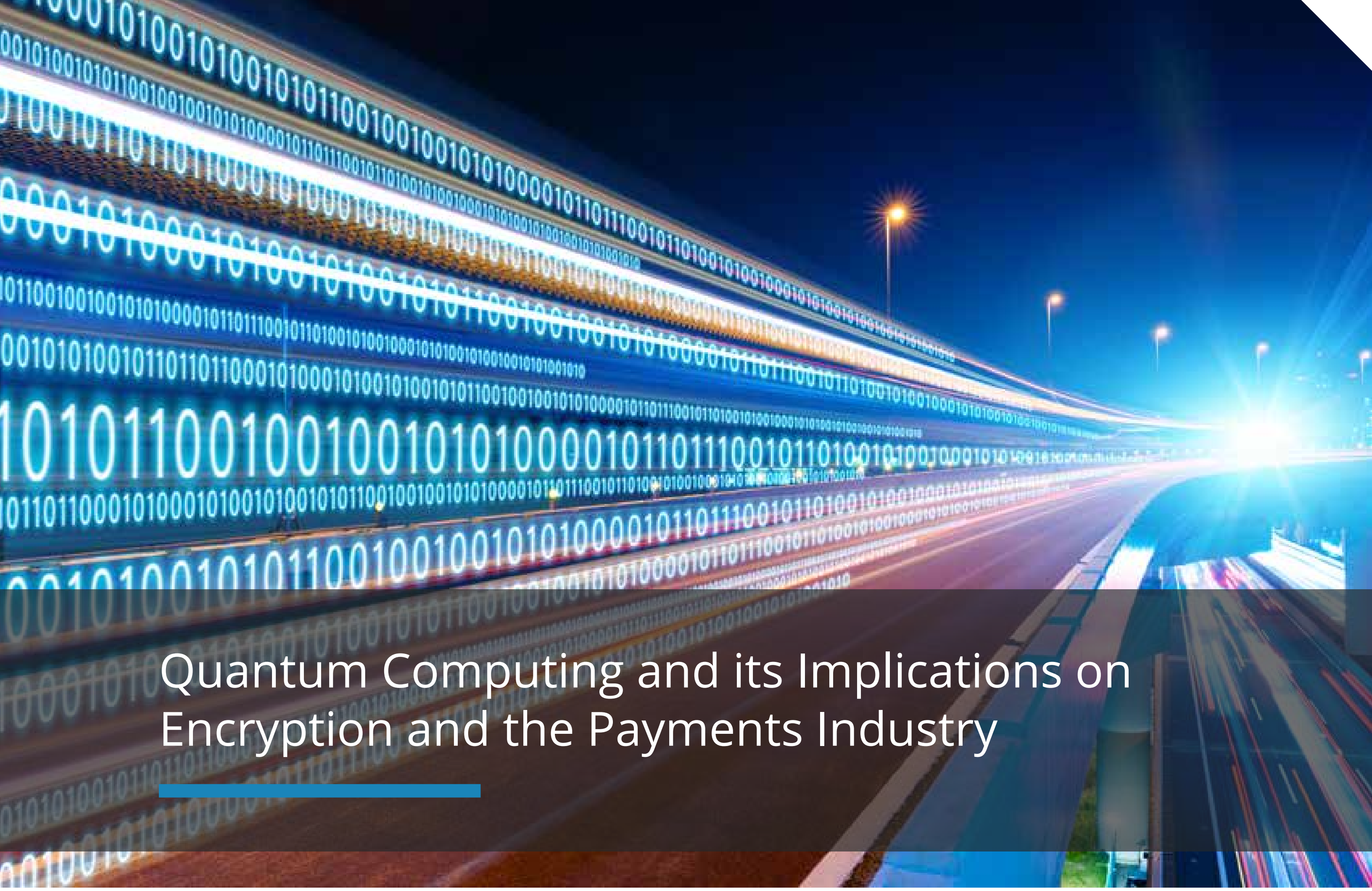

Quantum Computing and its Implications on Encryption and the Payments Industry

While current cyberthreats like ransomware and malware take center stage, there is a looming cyberthreat on the horizon and that is quantum computing.

Quantum computing harnesses quantum mechanics to perform high level computation. The resulting quantum computers are believed to be able to solve certain computational problems, such as integer factorization, substantially faster than classical computers.

The benefits of quantum computers are vast, with application in Artificial Intelligence (AI), molecular modeling, financial modeling, weather forecasting, particle physics, and more. Lockheed Martin is developing a quantum computer, D-Wave Two, to verify and validate control systems for complex platforms. For example, the D-Wave Two could exhaustively test every possible trajectory a spacecraft might take to get to its destination and then combine all permutations into the most efficient outcome within milliseconds.

But once quantum computers become functional, their ability to perform calculations exponentially faster than classical computers could enable them to destroy encryption that currently protects data, including several popular asymmetric public-key cryptography (PKC) systems, such as RSA (Rivest-Shamir-Adleman), ECC (elliptic-curve cryptography) and Diffie-Hellman.

Bluefin®
The Leader in Payment Security

Standards organizations and researchers have been actively working to identify the best alternatives and plan the transition to post-quantum cryptography, which will secure against both classical and quantum computers and can work with existing communications protocols and networks. A recommended solution is for entities to adopt the Advanced Encryption Standard (AES), which was introduced by the National Institute of Standards and Technology (NIST) in 2001 and is used widely throughout the U.S government.

However, industries using both asymmetric and symmetric cryptography have been slow to embrace AES – particularly in the payments industry, where the predecessor to AES, the Data Encryption Standard (DES) is still used, albeit in its triplicate form – also called Triple DES (TDES or 3DES).

Bluefin is a leading provider of encryption and tokenization solutions to protect sensitive data upon entry, in transit, and at rest. The company became the first North American provider of a PCI-validated point-to-point encryption (P2PE) solution in 2014 to secure point-of-sale (POS) payments and in 2019, introduced ShieldConex® for securing personally identifiable information (PII), protected health information (PHI) and payment information entered online. While implementing AES is not mandatory, Bluefin upgraded its payment security products to support AES in 2019 – with the company's Decryptx® P2PE solution supporting AES-128 and 256, and ShieldConex utilizing AES-256 for Format Preserving Encryption (FPE).

Asymmetric versus Symmetric Cryptography

Asymmetric cryptography, also known as public-key cryptography (PKC), uses one public key and one private key to encrypt and decrypt a message. A public key is a cryptographic key that can be used by any person to encrypt a message so that it can only be deciphered by the intended recipient with their private key. A private key, which can also be known as a secret key, is shared only with the initiator of the key.

Many widely adopted protocols rely on asymmetric cryptography, including the transport layer security (TLS) and secure sockets layer (SSL) protocols. Types of asymmetric cryptography algorithms include RSA, which is often used in web browsers to connect to websites, in virtual private network (VPN) connections and in many other applications; Diffie-Hellman, which was one of the first public-key protocols implemented within the field of cryptography; and ECC, which is an approach to PKC based on the algebraic structure of elliptic curves over finite fields.

In symmetric encryption, only one secret key is used to both encrypt and decrypt electronic information. The entities communicating via symmetric encryption must exchange the key so that it can be used in the decryption process.

> *"By using symmetric encryption algorithms, data is converted to a form that cannot be understood by anyone who does not possess the secret key to decrypt it. Once the intended recipient who possesses the key has the message, the algorithm reverses its action so that the message is returned to its original and understandable form. The secret key that the sender and recipient both use could be a specific password/code or it can be random string of letters or numbers that have been generated by a secure random number generator (RNG)."*

Examples of symmetric encryption include the Advanced Encryption Standard (AES) and its predecessor, the Data Encryption Standard (DES).

Quantum Computing and Encryption

There has been much written about how quantum computers will “break” encryption. But when discussing the effects of quantum computing on encryption, it’s important to keep in mind the type of cryptography being discussed.

The primary current concern is asymmetric cryptography. Shor’s algorithm, a quantum technique, can factor large numbers exponentially faster than classical machines. Because asymmetric algorithms like RSA rely heavily on the fact that normal computers can’t find prime factors quickly, they have remained secure for years. Unfortunately, many asymmetric encryption algorithms have been mathematically proven to be broken by quantum computers using Shor’s algorithm, including RSA, Diffie-Hellman and ECC.

Symmetric encryption, on the other hand, or more specifically AES-256, is believed to be quantum-resistant. That means that quantum computers are not expected to be able to reduce the attack time enough to be effective if the key sizes are large enough.

AES is widely being looked at as the solution to quantum computers. AES is a specification for the encryption of electronic data and was created in 2001 by NIST and is also included in the ISO/IEC 18033-3 standard making it an international standard. AES was implemented by the U.S. government to protect information in three categories: Confidential, Secret or Top Secret.

> *“The main benefit of AES lies in its key length options. The time required to crack an encryption algorithm is directly related to the length of the key used to secure the communication — 128-bit, 192-bit or 256-bit keys. AES-128 uses a 128-bit key length to encrypt and decrypt a block of messages, while AES-192 uses a 192-bit key length and AES-256 a 256-bit key length to encrypt and decrypt messages. Each cipher encrypts and decrypts data in blocks of 128 bits using cryptographic keys of 128, 192 and 256 bits, respectively.”*

Prior to AES’s introduction, the U.S. government used Data Encryption Standard (DES) algorithms. DES was developed in 1975 by IBM and turned into a standard by NIST in 1976. It served as the main protocol for government cryptography until 1999, when researchers broke the algorithm’s 56-bit key using a distributed computer system. As such, AES is exponentially stronger than DES and is also faster, making it ideal for applications, firmware and hardware that require low latency or high throughput.

DES versus AES in the Payments Industry

DES is still used in the payment industry, with the security limitation of the DES 56-bit key being addressed by implementing Triple DES (TDES or 3DES), officially known as the Triple Data Encryption Algorithm (TDEA or Triple DEA). TDES is a symmetric-key block cipher, which applies the DES cipher algorithm three times to each data block, producing a more secure encryption.

The payment industry has been dominated by TDES, and while it is still considered secure for another decade, the industry acknowledges that the shift to AES will need to be made.

However, there are significant considerations when switching from DES to AES. AES, like DES, is a block cipher, but AES has larger block and key sizes. Each iteration of the encryption or decryption process works on a block of data; 8 bytes with DES, 16 bytes with AES. AES keys are also different too – while DES/TDES has 8, 16 or 24 bytes, AES key lengths are 16, 24 or 32 bytes.

For many applications, these differences can quickly be accommodated – for example, in TLS, changing the cryptographic algorithms in the underlying cipher suite to use AES is a matter of updating the server and client browser software to accept it.

But in the payment environment, cryptography is performed in devices. To update to AES, every device deployed in the U.S. would need to be replaced or field-upgraded. Considerations also include ATMs, gas pumps and Hardware Security Modules (HSMs), all of which would also need to be updated. And finally, upgrades need to occur to the transaction messaging software to accommodate the larger block size for AES, especially PIN blocks.

However, organizations, such as Bluefin, have already begun to proactively update their systems to AES. In 2018, Verifone announced that it implemented AES DUKPT with its end-to-end encryption solution, VeriShield Total Protect, its Engage family of payment devices, and Carbon 8 & 10. Thales has upgraded its HSMs to support AES and most, if not all, EMV chip cards issued today are AES-capable.

The PCI Security Standards Council (SSC) has also begun putting out guidance on AES.

> *"The PCI SSC recognizes that the migration to AES is a major effort across the ecosystem and we are reevaluating how best to support this effort. PCI SSC will continue to solicit stakeholder feedback on the progress of migration efforts and the time frames needed for organizations to implement the changes properly. Additionally, PCISSC is preparing an Information Supplement for release in 2021 that will provide detailed guidance on implementing ISO Format 4 PIN Blocks. This Information Supplement will serve as a resource to help organizations understand what an ISO Format 4 PIN block is and why migration is important, as well as provide guidance for migration planning."*

The Council further goes on to say that:

> *"While both [TDES and AES] are still currently accepted encryption practices, the PCI SSC recommends that entities with environments subject to PCI Standards that require the use of symmetric encryption algorithms migrate to AES as it is a stronger cryptographic algorithm."*

In Conclusion

Estimates of when large-scale quantum computers will be available vary widely. Developers of quantum computers say it will happen soon, while some researchers argue that we may never have the capability to build them.

However, it's safe to say that as hackers continue their development methods, it makes sense for all industries – especially payments – to implement the highest level of encryption available, and that will be AES. While TDES is still approved for use, NIST is recommending phasing out TDES by 2031. Fundamentally, AES is stronger than TDES, is faster and more secure, and is our best shot at quantum-computing resistance.

Recognizing the importance of AES, Bluefin enabled both it's Decryptx and ShieldConex for AES in 2019..

> *"We knew terminal manufacturers would eventually start releasing AES capable devices and we wanted our Decryptx platform to be ready to support decryption of AES devices immediately," said Tim Barnett, Bluefin's Chief Innovation Officer. "As we are the leading P2PE service provider globally, it is important for Bluefin to provide leadership in the payment security industry so we can do our part in securing the payment ecosystem. This is why we also enabled AES-256 for the format-preserving encryption used in our ShieldConex data security platform."*

Visit our P2PE, Decryptx and ShieldConex pages for more information on our solutions.