Source: https://www2.deloitte.com/us/en/insights/industry/public-sector/the-impact-of-quantum-technology-on-national-security.html

AN INVESTIGATION INTO THE USE OF QUANTUM SECURITY TECHNOLOGIES

Research question: To what extent can quantum security technologies be deployed in the banking sector and what are the associated security issues?

Subject: ITGS

Word Count: 3899

Contents

Introduction:

Quantum computing is a topic which I was always curious about, ever since I heard about it a few years ago. As I am a computer science student, I have been interested in machine language and how quantum computers can have bits existing in two states simultaneously. This intriguing property, which is very unlike conventional computers (where you have a bit which can be either ‘1’ or ‘0’ and nothing else), made me interested in finding out how today’s scientists and leading researchers are using this property of quantum computational methods. Starting out with this broad idea, I decided to hone this down to security, as I was extremely curious as to how the new calculation methods and new mathematical algorithms were created so as to exploit the advantages of quantum technologies. Hence I arrived at quantum security technologies, and with the digitalization of money and the state of the art security systems present in the banking industry, I decided to explore to what extent could quantum security technologies be deployed in the banking sector, and what would be the related issues.

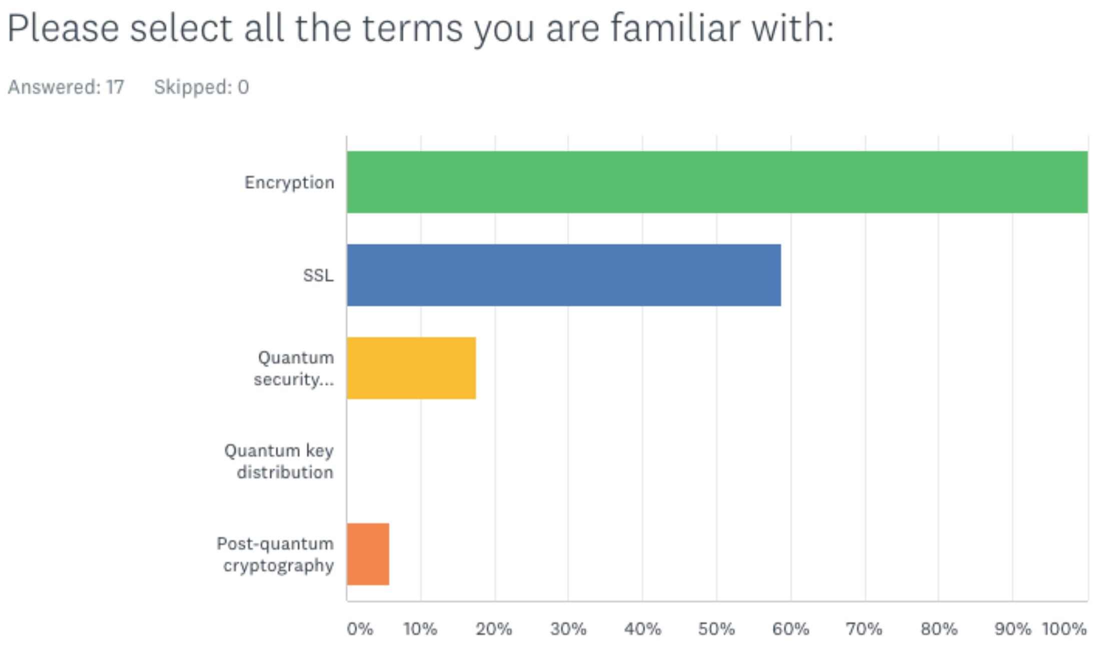
In a world governed and run by information, with data being sent through cables, wires, and even through the air, it is important that this data is being kept secure. In the banking sector, where there is a constant dealing and involvement with financial assets and money, it is imperative that important and sensitive details are kept a secret from prying eyes. Before, where banking and bank related work was only done by physically going to banks, there wasn’t a need to encrypt the data or information being given to banks. However, with banking companies going on the internet, and allowing customers to manage their accounts from the convenience of their device, advanced security methods are needed to ensure the financial security of all the relevant stakeholders. Currently, banks use public key encryption, which is a safe way of encrypting the sensitive information that is constantly being sent to and delivered by banks. However with the development of quantum computers, there are new and rising concerns regarding the security of the information being sent online, and current encryption methods and strategies are in danger of being obsolete, as quantum computers could rapidly break the encryption standards which took supercomputers an enormous amount of time to do. That is why there is a need for quantum security technologies. My research question therefore states ‘To what extent can quantum security technologies be deployed in the banking sector and what are the associated security issues?’.

Quantum Security technologies

Quantum security technologies are technological cryptographic methods that employ the use of quantum physics or can provide protection keeping quantum computing in mind. There are multiple examples of quantum security technologies, but in this essay, the main two which will be discussed are post quantum cryptography and quantum key distribution. Both of these methods have great advantages, but they also have certain drawbacks as well, which is why this essay will analyze each methodology and evaluate the use of quantum security technologies in the banking sector.

Post-quantum cryptography (PQC)

In a survey I conducted (results shown in the appendix) with people who used online banking services at least once a month, it was asked whether they had heard about ‘post quantum cryptography’, and only 6% of the respondents answered ‘yes’. Comparing this with the results for people who had heard about encryption, there is a 94% gap between the two. This shows that the public who might be heavily affected by PQC in the future, know very little or don’t even know about it. That is why there is a need to bring this information to light, as these systems might be the common way of encryption utilized in the future.



Please select all the terms you are familiar with:

Answered: 17 Skipped: 0

Post quantum cryptography is the use of specific types of encrypting algorithms to encrypt data. These ‘types’ of algorithms would have to be quantum-safe, which means that even if ciphertext is put in a powerful quantum computer, then it won't be able to properly decrypt the ciphertext, or it would be nearly impossible to do so[1].

Currently, computers and devices mainly use public key encryption protocols like SSL or TLS. These protocols rely on complex mathematical relationships, formulas and algorithms, which then are used in generating the keys which can encrypt and decrypt data. The algorithms and methods which are used to generate these keys, use the multiples of incredibly large prime numbers, making it extremely hard for the computers we use today to crack these algorithms and cause harm. Quantum computers on the other hand, can use a famous algorithm called Shor's algorithm to break these encryption protocols in a significantly little amount of time. To put things in perspective, classical computers would take approximately 300 trillion years to break a RSA-2048 bit key. However a quantum computer could complete such a task in a matter of 10 seconds (using Shor's algorithm)[2]. Therefore, in a world where quantum computers are constantly being developed, the use of SSL or TLS encryption standards would prove futile[3], therefore there would be a need for a method of cryptography which would be 'immune' to quantum computers. This would be post-quantum cryptography.

[1] Cardinal, D. (2019) Quantum cryptography demystified: How it works in plain language, Extremetech.com. Available at: https://www.extremetech.com/extreme/287094-quantum-cryptography (Accessed: December 1, 2020).

[2] Quintessence Labs. 2020. Breaking RSA Encryption - an Update on the State-of-the-Art - QuintessenceLabs. [ONLINE] Available at: https://www.quintessencelabs.com/blog/breaking-rsa-encryption-update-state-art/. [Accessed 26 June 2020].

[3] Post Quantum Cryptography. Huawei.com. Available at: https://www.huawei.com/en/trust-center/post-quantum-cryptography (Accessed: December 1, 2020).

PQC, mainly focuses on the mathematical and algorithmic side of cryptography, rather than the hardware and technology side. For example, according to MIT Technology Review, one instance of post-quantum cryptography is as simple as doubling or increasing the number of bits used for an encryption key, which would dramatically increase the number of combinations and permutations that a quantum computer would have to search through. Another example is to remodel and create newer mathematical functions, which actively keep Shor's algorithm in mind, and make it harder to crack the encryption key[4].

An example of PQC is NTRU (short for 'Nth Degree Truncated Polynomial Ring Units'), which instead of using RSA algorithm, uses another methodology called lattice based cryptography[5]. NTRU was founded by 3 mathematicians in 1996, Joseph H. Silverman, Jeffrey Hoffstein, and Jill Pipher. NTRU works and follows the same concepts from public key encryption, where a public key is generated and a private key is needed in order to decrypt information which was encrypted by the public key. Due to the fact that this cryptosystem is based off of lattices, it is significantly harder to solve when compared with cryptosystems based off of factorization or logarithms [6].

[4] MIT Technology Review. 2020. Explainer: What is post-quantum cryptography? | MIT Technology Review. [ONLINE] Available at: https://www.technologyreview.com/2019/07/12/134211/explainer-what-is-post-quantum-cryptography/. [Accessed 26 June 2020].

[5] RSA Conference (2020) Understanding and explaining post-quantum crypto with cartoons. Youtube. Available at: https://www.youtube.com/watch?v=6qD-T1gjtKw (Accessed: December 1, 2020).

[6] Christian Eichinger. 2020. What is NTRU and why do we like it so much? - tixlcurrency - Medium. [ONLINE] Available at: https://medium.com/tixlcurrency/what-is-ntru-and-why-do-we-like-it-so-much-4028d05eabb3. [Accessed 26 June 2020].

Advantages

Post quantum cryptography (in general) has many significant advantages. Firstly, it doesn't require the use of quantum technologies. This means that in terms of hardware, any users that may be involved during a specific session don't need to have access to quantum computers or quantum computer hardware. This means that implementing and using PQC would be relatively easier (when compared to other methods of quantum cryptography) as it can run on the current hardware in our computers. In terms of the banking sector, it would just require a change in the encryption protocol that the bank uses to communicate and send data. In addition to this, the banks wouldn't have to implement new and expensive hardware to keep their information secure[7].

A non-dramatic change in the system could also save the banking sector from having to totally revamp and restructure their existing systems. Restructuring existing systems could lead to periods of vulnerability, as staff and users wouldn't be used to and comfortable with the new system and there wouldn't be enough confidence or trust in the system. Using an implementing PQC could also offer another economical advantage, as it would save (or at least minimize) the cost of hiring or employing project managers or a whole project development team to implement new systems.

Another advantage is that due to the rising popularity and use of online banking, where account holders can manage and view their finances from their own home at their own convenience, it is very essential, that banks use encryption properly. This would require the account holder and the bank to use the same encryption standard or protocol. Since this encryption methodology wouldn't require a hardware change,

[7] Alienor (2018) Quantum cryptography explained: Applications, disadvantages, & how it works, Plixer.com. Available at: https://www.plixer.com/blog/quantum-cryptography-explained/ (Accessed: December 1, 2020).

then the customers of the bank can benefit from this technology as well[8]. Since they are using PQC, all their information being sent over the network will be protected from not just ordinary hackers with present technology, but also from hackers in the future with much more advanced technology such as quantum computers[9].

Disadvantages

However, Post quantum cryptography has multiple disadvantages as well. Since the process of developing post quantum cryptographic methods started in 2016, there were initially 69 proposals. In 2019, this was narrowed down to 26. The main disadvantage is that it took the NIST three years to narrow down and eliminate 41 proposals, which means that it would take at least 2 years to finally narrow down to one proposal. This shows that choosing the correct cryptographic method is a lengthy process, and can be very time consuming. This leads to another disadvantage. Although post quantum cryptography would be implemented in the future, this doesn't stop hackers from storing ciphertext which they intercept now, and later in the future, when they can get access to quantum computing technology, they can break the encryption in a matter of 10 seconds. In terms of the banking sector, where bank account information and details are usually long term, and they don't really change, this disadvantage could have a major impact. For example, if a hacker manages to intercept information or data regarding a bank's customer's private and sensitive details, then it isn't necessary that the hacker have to try and decrypt the intercepted ciphertext using present technology. Based on a discussion

[8] Wultra (2020) Digital banking and post-quantum cryptography. Youtube. Available at: https://www.youtube.com/watch?v=pwUMswT8YBA (Accessed: December 1, 2020).

[9] Dvořák, P. (2020) Video: Post-Quantum Cryptography in Digital Banking, Wultra Blog. Available at: https://medium.com/wultra-blog/video-post-quantum-cryptography-in-digital-banking-730a92d1a97d (Accessed: December 1, 2020).

with Dr. Faisal Khan (a professor at Khalifa university and technology advisor at Quantum Computing Inc.), a hacker can just wait until they can get access to quantum computing technology, or use cloud based quantum computers, to run the different algorithms such as Shor or Grover, to decrypt the information (full discussion in appendix). Once they decrypt the information and can read the data, such as bank account details, the CVV on their credit card, bank account PIN number, then the hacker can easily gain access to their bank account. This can lead to a massive economic loss to the customer. The bank would also be affected as their reputation would be ruined. Even if the bank later on did employ and implement post quantum cryptographic methods, the hacker already had the encrypted information, which allowed the hacker to completely bypass the PQC.

Another disadvantage, is that although it is relatively easier to implement PQC when compared to other quantum security technologies which require a change in hardware as well, changing any system (even existing encryption systems) can be quite difficult. Based on a discussion with Yazad Khandhadia (VP of information security at Emirates NBD), smaller digital banks won’t be facing as much of an issue as they don’t have that large of an infrastructure to deal with and change (full discussion in appendix). However, he says with large banks who have a much higher number of stakeholders involved and with a much larger infrastructure, it would be extremely challenging and tough. This is also because of how new and revolutionary the technology is and understanding how it works with its implementation paradigms will give arise to certain challenges which (according to Mr. Khandhadia) could take between 3-5 years to properly implement. In addition to this, when implementing new systems which require a hardware and software change, the company or the business can get extremely vulnerable, but even if it is only a software change, then there can be vulnerable periods as well. For instance, currently on many websites, SSL is used as the current encryption method. Changing the protocol or standard that they use can have many implications and would need certain organizations such as the IEEE to first accept it and declare it as a standard. Not only that, but all organizations would have to make sure that they follow the same standard, otherwise there can be miscommunication of data, and data integrity can be lost. In addition to this, according to a National academies paper, it took approximately a decade to disallow a widely-used cryptographic method[10]. This shows that changing the standard or protocol of encryption is not really easy.

[10] The National Academies Press. 2020. 1 Context | Cryptographic Agility and Interoperability: Proceedings of a Workshop | The National Academies Press. [ONLINE] Available at: https://www.nap.edu/read/24636/chapter/3#8. [Accessed 26 June 2020].

QKD (quantum key distribution)

QKD, or quantum key distribution, is another example of quantum security technologies. Quantum key distribution is used to send keys (which are used to encrypt or decrypt information) over a network, by using and employing quantum properties of a specific medium[11]. Usually the medium chosen is light, or photons. By using the quantum properties of light, and using laws of quantum physics, QKD is a highly secure method of sending keys to encrypt or decrypt data[12].

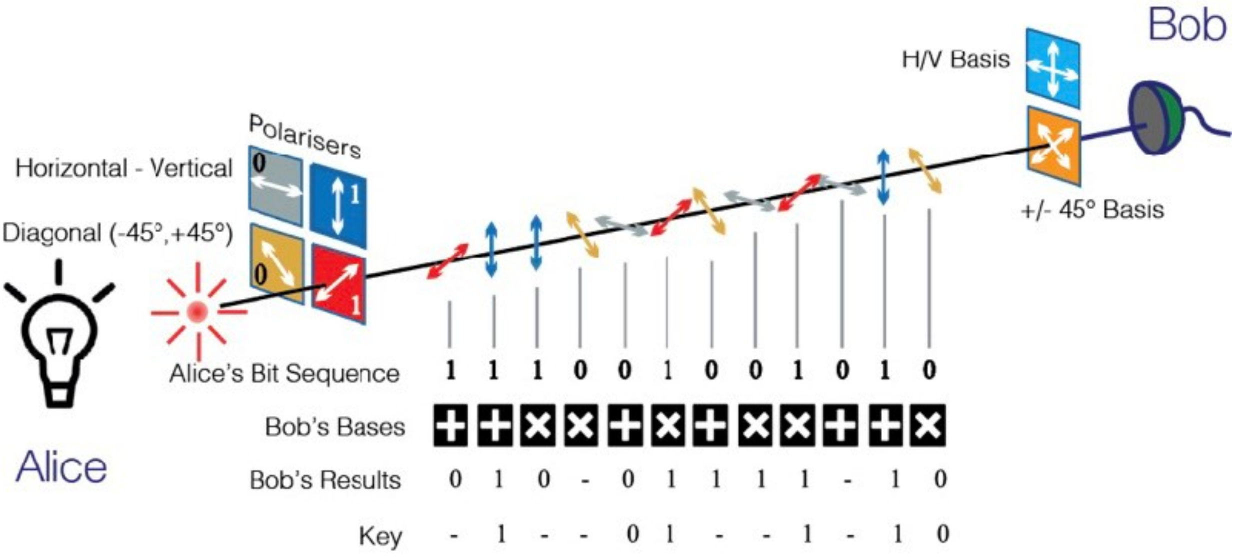
Quantum key distribution works by using the physical properties of the light to represent a piece of data. For example, a light particle can be polarized in many different ways, such as horizontally, vertically or even diagonally. If a person wants to send a key, then they would have to have a fiber optic connection with their recipient, as light is being used to send and receive the data. Then the sender would send a specific sequence of polarized light particles through a filter, and the type of polarization would determine what type of data it is, such as a 1 or a 0. After that, the receiver on the other end would have to measure the polarization of the light by using a filter as well. Due to certain laws in quantum physics, the polarization of the light particles would change depending on the type of filter used to measure it. For example, if the sender sent a light particle which was supposed to measure '1' with a horizontal filter, and the receiver measured it with a vertical or diagonal filter, then the value of the measured light particle could change to zero. In QKD, the receiver would measure the incoming light with different filters randomly, and then the

[11] BattelleInnovations (2014) Quantum key distribution: Provably secure encryption. Youtube. Available at: https://www.youtube.com/watch?v=IYvDGibT4Z8 (Accessed: December 1, 2020).

[12] Institute for Quantum Computing (2010) Quantum Key Distribution Animation. Youtube. Available at: https://www.youtube.com/watch?v=cWpqlgF7uEA (Accessed: December 1, 2020).

receiver would later communicate with the sender, and tell them which filter they used for each light particle. The sender would then reply ‘correct’ or ‘false’ for each filter the receiver used. If the receiver got the filter right, then they keep the data that they measured, and if the receiver chose the wrong filter, then they get rid of the data they measured. Usually, the receiver would have a 50% chance of getting the filter right, which means that half of the initial key is used as the final key[13].

There are multiple ways to use QKD, but the main example used is the BB84 protocol (the one explained in this paragraph). The BB84 was proposed by Bennett and Brassard in the year of 1984[14].



Alice’s Bit Sequence	1	1	1	0	0	1	0	0	1	0	1	0
Bob’s Bases	+	+	×	×	+	×	+	×	×	+	+	×
Bob’s Results	0	1	0	-	0	1	1	1	1	-	1	0
Key	-	1	-	-	0	1	-	-	1	-	1	0

Source: https://qt.eu/discover-quantum/underlying-principles/quantum-key-distribution-qkd/ [15]

[13] Verizon (2020) What is Quantum Key Distribution | Verizon. Youtube. Available at: https://www.youtube.com/watch?v=hArTusF4KPg

[14] Chekhova_Research_Group, 2020. Secret key. BB84, E91 and B92 protocols. Continuous-variable protocols.. Lecture 12: Quantum key distribution., [Online]. NA, 1. Available at: https://mpl.mpg.de/fileadmin/user_upload/Chekhova_Research_Group/Lecture_4_12.pdf [Accessed 19 June 2020].

[15] “QKD”.Quantum flagship. Available at: https://qt.eu/discover-quantum/underlying-principles/quantum-key-distribution-qkd/.

Advantages

Quantum Key distribution has a significant amount of advantages. The first advantage is that it doesn't require a third party to be present which means that only the primarily significant members involved in the communication of the data (i.e. the sender and the receiver) are present, and there isn't a 'middle-man' or a third party present[16]. This benefit has a great value when compared with TTP encryption schemes (short for 'Trusted Third party'). In TTP, the third party can read all the messages being sent between the sending and the receiving parties. This encryption scheme has a liability in the form of the third party. Due to the third party being able to view messages because of the fact that they are 'trusted', this doesn't stop them from ethically breaching the trust of the first two parties (sender and receiver).

For example in the banking industry, if a bank and their customer use TTP schemes as a method to generate encryption keys, and send private and sensitive data to each other. In this scenario, the trust that the bank and customer have placed with the third party comes with the risk of the third party having the ability to read all of the data and information that the bank wants to send their customer and the data and information that the customer wants to send to the bank. In the banking sector, such risks like this can be detrimental and if these risks are used to harm the bank or customer, then these can have major social and ethical impacts. To illustrate this, in a situation if money is stolen from the customer's bank account then the customer would suffer economically and would have to change their social lifestyle drastically. The bank would suffer from defamation as flaws in the system have been exposed,

[16] Korchenko, O., Vasiliu, Y. and Gnatyuk, S. (2010) "Modern quantum technologies of information security," arXiv [cs.CR]. Available at: http://arxiv.org/abs/1005.5553 (Accessed: December 1, 2020).

which would significantly reduce their number of customers which can then ruin their infrastructure. Due to the fact that the third party is completely redundant and has no place in quantum key distribution methodologies, this eliminates the potential liability of the third party ‘going rogue’. Thanks to the elimination of this risk, customers won’t have their personal data or their money stolen.

Another advantage regarding quantum key distribution is that if a hacker is trying to intercept the stream of light particles, then the polarization will change if the hacker uses the wrong filter. This will increase the error rate of the receiver, which will exceed the expected amount of errors (the number of errors that usually happen if there is no interceptor) or, in other words, surpass the error threshold. This would then indicate to the sender and receiver that there is an interceptor present. For instance, if a customer is communicating with their bank and is using QKD to send a key. If there is another person who wants to intercept the key and tries to use certain filters to measure the data, they will alter the light particles and increase the error rate above the error threshold. This will be noticed when the bank and the customer would compare the filters used and see the high number of ‘errors’ made by the receiving party. This would then alert the bank and not only tell them to change the channel being used but also would inform the bank that there is someone trying to intercept the data, which could help them to initiate the refortification of their channels and get rid of any intercepting devices or points.

The third advantage that quantum key distribution has is that it employs OTP encryption or one time pad encryption. One time pad encryption is when a key is generated only to be used for one time. In OTP, the plaintext is converted into ciphertext using a key which should be at least as long as the plaintext. This is because in OTP, each letter of the plain text is scrambled according to its corresponding letter in the key[17]. For example, if the word 'HI' was to be scrambled with the key 'CZ' then (usually, but not necessarily) the letters are assigned numerical values ('A' becomes 0, 'B' becomes 1, 'C' becomes 2 e.t.c.) and then the numerical value of the ciphertext letter is added to the plaintext letter. The new number will then be converted back into its alphabet form. So in this case 'Hi' will become 'JH'. There are different ways to actually employ OTP encryption but they all must have a key that is truly random, have a length greater than or equal to the length of the plaintext, can never be reused, and must be kept completely secret [18]. This is what allows QKD to be so secure as the randomness and non-reusability of the key make it so that even a computer cannot decode the information. Not only that but before QKD, OTP wasn't effectively used as the distribution of the keys was a problem. Thanks to the quantum technologies and the rules of quantum physics, an interceptor won't be able to get the proper key. Therefore because of the effective use of OTP encryption by QKD systems, the encryption is unbreakable as long as all the rules of OTP are correctly followed.

Disadvantages

Nonetheless, quantum key distribution has a couple of disadvantages as well. Firstly, to operate and run QKD protocols such as the BB84, one needs to have optical fiber

[17] Khan Academy. 2012. The one-time pad (video) | Cryptography | Khan Academy. [ONLINE] Available at: https://www.khanacademy.org/computing/computer-science/cryptography/crypt/v/one-time-pad. [Accessed September 1, 2020].

[18] One Time Pad Encryption Technique. 2012. One Time Pad Encryption Technique. [ONLINE] Available at: https://www.slideshare.net/Jonlitan/one-time-pad-encryption-technique. [Accessed September 1, 2020].

based system as information will be sent as light particles[19]. When comparing different methods of sending data, such as optical fibers, wireless radio transmission, and ethernet cables, optical fibers are the most expensive to implement, as the material, manufacturing processes and installation are quite complex. Not only that, but optical fibers are much more sensitive to damage and also are much more expensive to repair and replace[20]. Furthermore, implementing QKD would need a major revision or addition to current systems in place. Just like how PQC would be hard to implement due to software changes and protocol changes, QKD will be even harder to implement as there is also an expensive hardware system implementation needed along with the software and protocol implementation. Making QKD mainstream would have a colossal financial cost attached to it.

This drawback then creates another disadvantage, because since the costs are so high, not everyone will be able to implement QKD technology and use it. Since not everyone can use QKD, then the people who would have access will be limited with the people that they can securely communicate with and send sensitive information to. For example, if two banks want to communicate with each other in order to transfer money from one account to the other, then they both need access to QKD technologies to communicate on a secure channel. This shows that another main drawback is that both parties must have QKD technology implemented and due to the high costs associated with quantum key distribution, the significance of this disadvantage is increased.

[19] Mailloux, L. O. (no date) Quantum key distribution: Boon or bust?, Afit.edu. Available at: https://scholar.afit.edu/cgi/viewcontent.cgi?article=1168&context=facpub (Accessed: December 1, 2020).

[20] ElProCus - Electronic Projects for Engineering Students. 2020. Optical Fiber : Working Principle, Types, Advantages and Disadvantages. [ONLINE] Available at: https://www.elprocus.com/optical-fiber-working-and-its-applications/. [Accessed September 1, 2020].

Conclusion

In conclusion, Post-quantum cryptography and quantum key distribution both have significant advantages which can help in implementing such systems and also make sure that the banking sector can securely transmit and send data and information. Both of these methods provide a way to be safe against current hackers with access to current supercomputers and also something which could very much be a threat within the next 2 decades.

However, each methodology has certain drawbacks, such as PQC not being easily implemented into current banking infrastructures, and QKD being expensive and requiring complete new infrastructure and hardware implementations to actually run. These disadvantages emphasize on an initial investment to support a major revision of current communication and data transmission systems. In addition, quantum security technologies could offer vital and potentially unbreakable security for the banking sector, but in the wrong hands, it could usher in a total and completely new age of anonymity. Implementation of such quantum security technologies now within the banking industry would secure the relevant stakeholders in that they would be safe against any looming danger.

Nevertheless, if used by the correct organizations in the right manner, the implementation of quantum security technologies could possibly eliminate the fear of eavesdroppers and spark a revolution of data security and privacy not just for the banking sector, but for all global technologies. Despite the economic and logistic disadvantages in the short term, quantum security technologies could revolutionize the security of communication and data transfer in the banking sector, ensuring customer and organization confidence as a whole.

BIBLIOGRAPHY

Cardinal, D. (2019) Quantum cryptography demystified: How it works in plain language, Extremetech.com. Available at: https://www.extremetech.com/extreme/287094-quantum-cryptography (Accessed: December 1, 2020).

Quintessence Labs. 2020. Breaking RSA Encryption - an Update on the State-of-the-Art - QuintessenceLabs. [ONLINE] Available at: https://www.quintessencelabs.com/blog/breaking-rsa-encryption-update-state-art/. [Accessed 26 June 2020].

Post Quantum Cryptography. Huawei.com. Available at: https://www.huawei.com/en/trust-center/post-quantum-cryptography (Accessed: December 1, 2020).

MIT Technology Review. 2020. Explainer: What is post-quantum cryptography? | MIT Technology Review. [ONLINE] Available at: https://www.technologyreview.com/2019/07/12/134211/explainer-what-is-post-quantum-cryptography/. [Accessed 26 June 2020].

RSA Conference (2020) Understanding and explaining post-quantum crypto with cartoons. Youtube. Available at: https://www.youtube.com/watch?v=6qD-T1gjtKw (Accessed: December 1, 2020).

Christian Eichinger. 2020. What is NTRU and why do we like it so much? - tixlcurrency - Medium. [ONLINE] Available at: https://medium.com/tixlcurrency/what-is-ntru-and-why-do-we-like-it-so-much-4028d05eabb3. [Accessed 26 June 2020].

Alienor (2018) Quantum cryptography explained: Applications, disadvantages, & how it works, Plixer.com. Available at: https://www.plixer.com/blog/quantum-cryptography-explained/ (Accessed: December 1, 2020).

Wultra (2020) Digital banking and post-quantum cryptography. Youtube. Available at: https://www.youtube.com/watch?v=pwUMswT8YBA (Accessed: December 1, 2020).

Dvořák, P. (2020) Video: Post-Quantum Cryptography in Digital Banking, Wultra Blog. Available at: https://medium.com/wultra-blog/video-post-quantum-cryptography-in-digital-banking-730a92d1a97d (Accessed: December 1, 2020).

The National Academies Press. 2020. 1 Context | Cryptographic Agility and Interoperability: Proceedings of a Workshop | The National Academies Press. [ONLINE] Available at: https://www.nap.edu/read/24636/chapter/3#8. [Accessed 26 June 2020].

BattelleInnovations (2014) Quantum key distribution: Provably secure encryption. Youtube. Available at: https://www.youtube.com/watch?v=IYvDGibT4Z8 (Accessed: December 1, 2020).

Institute for Quantum Computing (2010) Quantum Key Distribution Animation. Youtube. Available at: https://www.youtube.com/watch?v=cWpqIgF7uEA (Accessed: December 1, 2020).

Verizon (2020) What is Quantum Key Distribution | Verizon. Youtube. Available at: https://www.youtube.com/watch?v=hArTusF4KPg

Chekhova_Research_Group, 2020. Secret key. BB84, E91 and B92 protocols. Continuous-variable protocols.. Lecture 12: Quantum key distribution., [Online]. NA, 1. Available at: https://mpl.mpg.de/fileadmin/user_upload/Chekhova_Research_Group/Lecture_4_12.pdf [Accessed 19 June 2020].

“QKD”.Quantum flagship. Available at: https://qt.eu/discover-quantum/underlying-principles/quantum-key-distribution-qkd/.

Korchenko, O., Vasiliu, Y. and Gnatyuk, S. (2010) “Modern quantum technologies of information security,” arXiv [cs.CR]. Available at: http://arxiv.org/abs/1005.5553 (Accessed: December 1, 2020).

Khan Academy. 2012. The one-time pad (video) | Cryptography | Khan Academy. [ONLINE] Available at: https://www.khanacademy.org/computing/computer-science/cryptography/crypt/v/one-time-pad. [Accessed September 1, 2020].

One Time Pad Encryption Technique. 2012. One Time Pad Encryption Technique. [ONLINE] Available at: https://www.slideshare.net/Jonlitan/one-time-pad-encryption-technique. [Accessed September 1, 2020].

Mailloux, L. O. (no date) Quantum key distribution: Boon or bust?, Afit.edu. Available at: https://scholar.afit.edu/cgi/viewcontent.cgi?article=1168&context=facpub (Accessed: December 1, 2020).

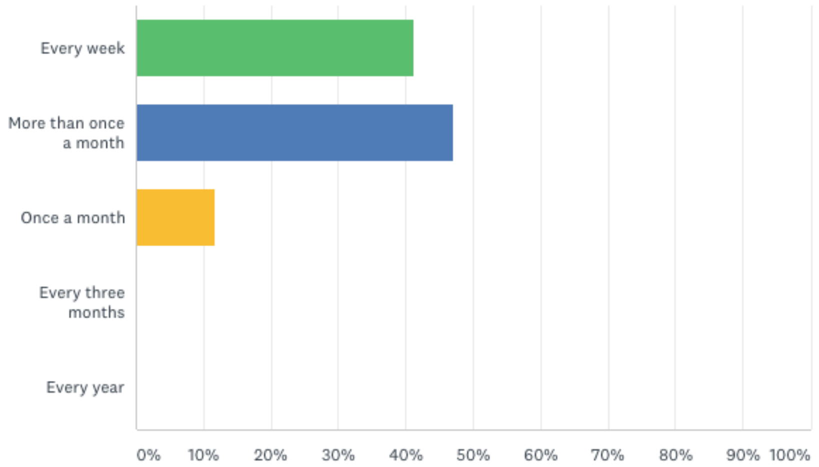
ElProCus - Electronic Projects for Engineering Students. 2020. Optical Fiber : Working Principle, Types, Advantages and Disadvantages. [ONLINE] Available at: https://www.elprocus.com/optical-fiber-working-and-its-applications/. [Accessed September 1, 2020].

Appendix

Survey results

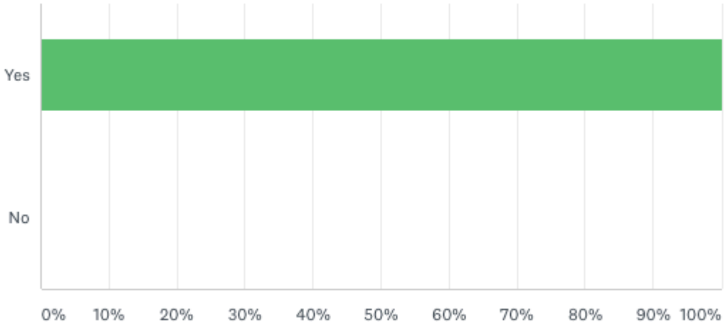
How often do you use the online banking services offered by your bank?

Answered: 17 Skipped: 0



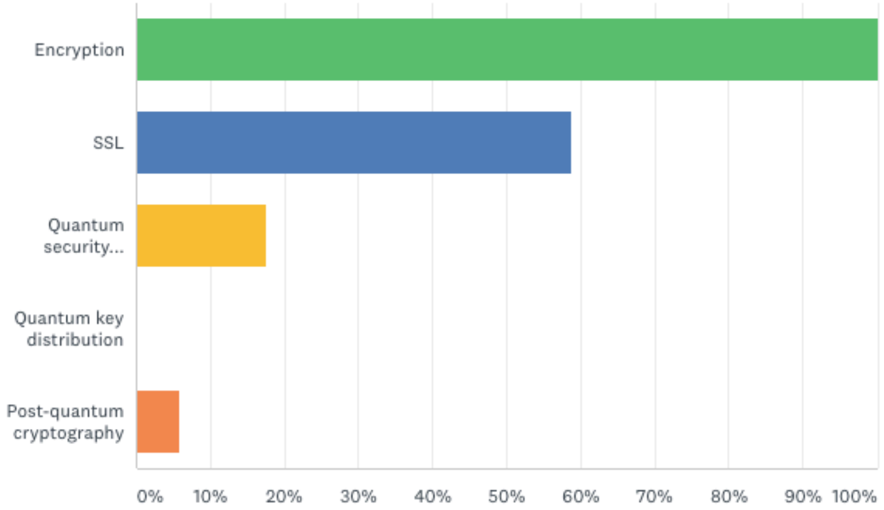
Are you aware of the security issues with online banking?

Answered: 17 Skipped: 0



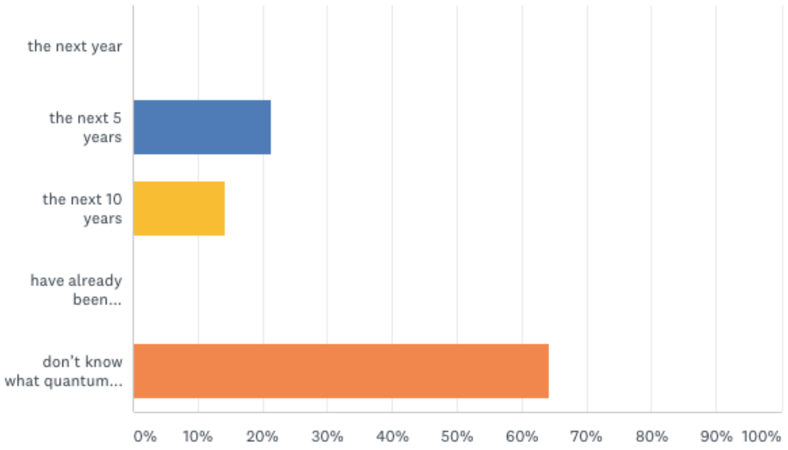
Please select all the terms you are familiar with:

Answered: 17 Skipped: 0



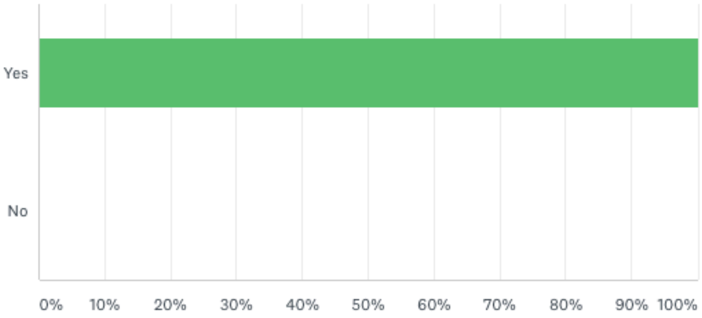
If you know what quantum security technologies are, by when do you think they will be implemented in the banking sector?

Answered: 14 Skipped: 3



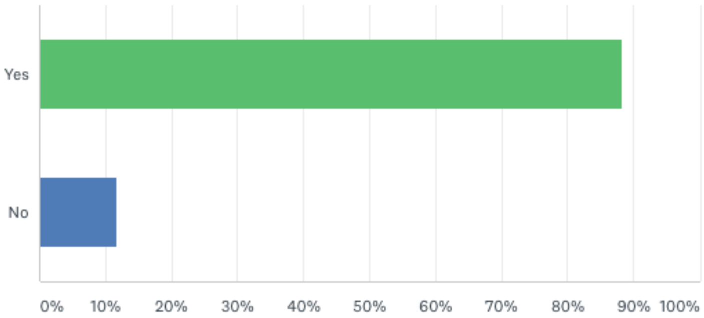
Do you think online banking can affect employment in the banking sector?

Answered: 17 Skipped: 0



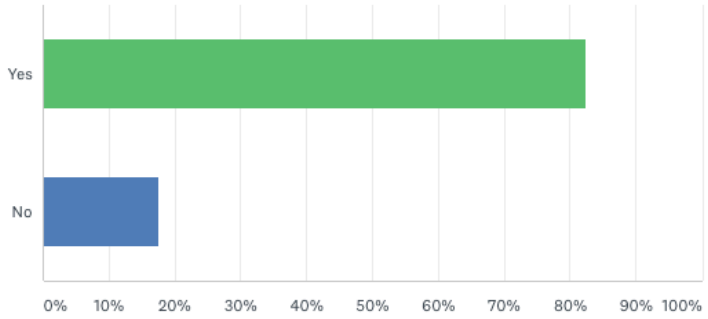
Do you think people need to be trained on how to use the online banking services?

Answered: 17 Skipped: 0



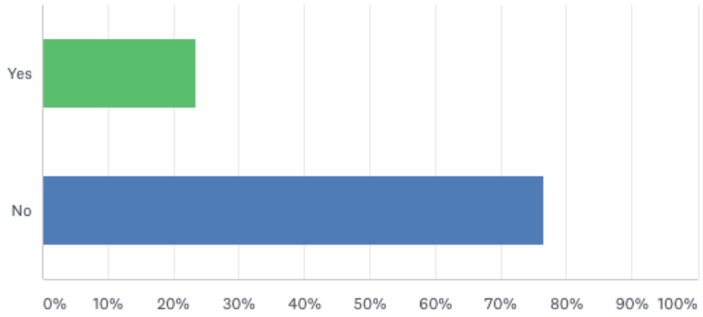
Do you think the bank needs to educate its customers on security implications regarding online banking?

Answered: 17 Skipped: 0



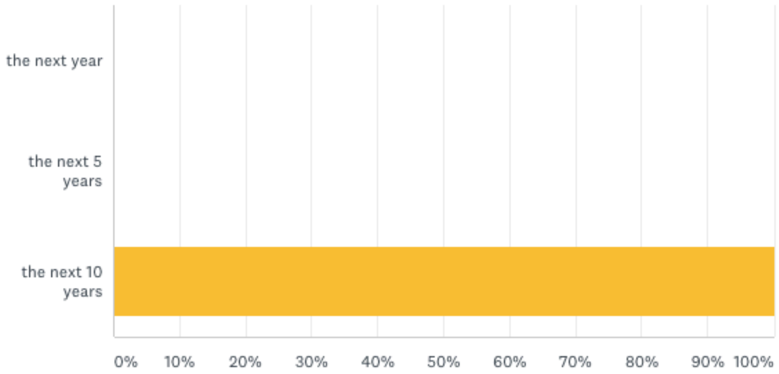
Do you think online banking would completely replace traditional banking?

Answered: 17 Skipped: 0



If you do think that online banking will completely replace traditional banking, by when do you think this will happen?

Answered: 4 Skipped: 13



Discussion with Dr. Faisal Khan (professor at Khalifa university)

Interview conducted over zoom

…

Student (A.J)
So, just the like, the general question would be, like, how does quantum computing work other than the fact that, like you have qubits and then how it can exist in one zero or just both at the same time.

Dr. Khan
How do you know about computer hardware?

Student (A.J)
So I take computer science and my other subjects. So like, I know about the CPU, like, its components such as the registers.

Dr. Khan
Perfect. Okay, so I'll start there. So basically, you have an understanding, it seems off what a qubit is, right?

Student (A.J)
Yeah, so it's basically just, like a normal regular bit, except I guess it can exist in three states. Like where it can be, like, one zero or both?

Dr. Khan
Okay good, so we must ask ourselves how does a manufacturer actually manufacture a bit. in regular computers? What does that look like? How's it implemented? Something that you call a zero, or you call a one? But what's the physics behind it? How do you actually make it realize in a computer hardware?

Student (A.J)
So I guess it would just be like an on and off search. Like how I guess, like, transistors were just like a really small switch.

Dr. Khan
It's a switch. And I guess the question would be, what is the switch regulating? Right? Yeah. So most likely some kind of electric current or electric potential. And that is exactly what they do. So when you have your, you know, your Mac, or your, whichever device you have, it's got a CPU or a motherboard, etc., right? That has silicon, you know, wells in their potential wells. And they're really good at actually capturing electric potential. So what they decide that manufacturers probably do differently, is that they decide that a certain amount of electric potential would be considered a value of one logical value one bit, and to be your physical manifestation of the debt. And if there's no electric potential, we'll go ahead and call that a zero. Yeah, it could also be the other way around, right? If there's low potential, then that's the one, etc. So that's how they do it. And I'm bringing it up, because it's going to be important for understanding what a qubit is, properly. So that's kind of how it begins, right? And then, of course, you know, over the past 60-70 years, people have gotten so good at manipulating this absence of presence of electric potential. So quickly, right, you'd have these things called assembly language, microprocessor language. And then faced with higher order, languages, language power. And you basically

have this ability to make these for them, those are your competitions, right? That they allow us to do what we're doing right now talking to each other remotely, right? So that's kind of, I think, a good place to begin when you talk about qubits. And quantum computers. The idea is that when you talk about a qubit, it's not any more the case that you're talking about a hardware that can capture a certain amount of electrical potential or not. It's more about a particular, you know, physical object, quantum physical object, like a photon, or electron. And you are looking at its individual particular properties, right. So something that's very common in physics, you know, property wise for these quantum particles or objects is spinning. Right? It's a funny name. It's a, it's a, it's called spin, but it doesn't look like spin in the sense of like, if I spend something right. Yeah, it does. It's just an idea. The point is that the spin can be in two different states, right? And we can call it what we want. We can call it blue state or red state, right? Kind of referring to American politics. You can call it whatever you like upstate, or downstate. So that's your cubic. Basically, it's trying to basically mimic the notion of a bit, right? It's in one state or the other. Now, because you are dealing directly with electron, or a photon a quantum object by itself, and if you can control it nicely enough, right, this is an issue we'll get into, you actually can access quantum properties of quantum features of that object. It's not like you're dealing with a bacterium, which is actually very small. But it's still not a quantum object to go into small part to get to electron or a photon. So it's a difficult thing to do. But the point is that that's what a qubit is. And if you can actually get a hold of its lecture saying that I can supposedly put it inside in a state that is both a zero a one, a red or a blue, right, some kind of a weighted average of the two. So the fancy word, the technical term for that is quantum superposition. But you know, think of it as an average, right? So if I take the average of two numbers, I add them and divide by two, right? Yeah. I take a weighted average of two numbers, I would take one number multiplied by something else, like instead of, you know, dividing it by two, I would divided by three. And I'll take the second number divided by five, for example, right? So the weight on the two numbers I was taking the average of, it's not the same, it's different. Yeah. So that's why we call it a weighted average. So now when it comes to quantum objects or qubits, another way to explain that is to say that I'm going to allow now weighted averages of my quantities, right? My numbers with respect to complex numbers.
…
Dr. Khan
Have you seen the movie that came out recently called The Imitation Game?

Student (A.J)
I heard of it. But I haven't seen it. No.

Dr. Khan
Okay. So it talks about, like how people, you know, developed computers back in the Second World War era. And, you know, one of the computers, early computers that were invented, were these huge, you know, room size boxes, vacuum tubes and stuff. So, yeah, so that's where we are, in terms of quantum computers today. Right? Unfortunately, we are not at a stage where we can say, Okay, I'm going to make a quantum, you know, a game, you know, that I can play on a quantum computer and beat everybody. The current generation of quantum processors is there's a few companies that have made some, there's a company called D wave. Their machine, their quantum processor is what's called a, it's more like a fancy calculator, it can do

very limited things. But those things that it can do, it does fairly quickly, compared to, you know, traditional computers. On the other hand, Google has come up with some sort of a platform, our
process.
…
there's something called an elliptic curve cryptosystem. So those cryptosystems can be broken by quantum computers.

Student (A.J)
And where are these crypto systems currently, like, you know, where they're currently being used?

Dr. Khan
Yeah. All the internet traffic on the planet is encrypted using elliptic curves or RSA. So they're everywhere.

Student (A.J)
Oh, yeah. So it can be also said that they're being used in banking systems and finance systems.

Dr. Khan
Absolutely. Every time you make an online purchase using a credit card or debit card, there's elliptic curve and RSA cryptography in the background, making that happen.
So quantum computers could break this type of crypto system. And potentially, like, if hackers got hold of quantum, then they could potentially gain access and intrude on these people's personal information.
Yeah, of course. We were worried about government. And then you know, hackers. So yeah, but yeah, you're absolutely right. The, the papers that came out in the 90s, basically, were the ones that got all the intelligence agencies around the world interested in quantum computing, because they mathematically proved that if you had one of these machines, and of course, when I say one of these machines, I mean, something that's not even available right now. Right? We're probably another 20 years away, unless some bright guy comes along and does something dramatic. We're still 20 years away, probably from those machines, right? But once you have them, yeah, this public key cryptosystem that drives all the commerce on the internet. It's, it's all going to be broken. It'll become obsolete.

Student
the breaking of current cryptosystems cannot happen with like, for example, say IBM's quantum computing, or like Google or…?

Dr. Khan
No, no. That's not possible because IBM and Google are both limited to 72 qubits.

So would there be a for let's say, like, how we could break…? Because right now we're talking about how we could break crypto systems and encrypting systems. But would there be a possible way to actually create new encrypting systems using quantum computing?

Dr. Khan
You can create new crypto systems, which are immune to attacks from quantum computers using qubits. Yes. But you wouldn't say that I'm using quantum computers to create those crypto systems, you would say that you're using what's called quantum cryptography. That's actually what they call it.

…
Student (A.J)
So basically, we can create quantum safe, quantum safe crypto systems, before we can actually use quantum computers to actually hack into current systems.

Dr. Khan
Exactly, exactly. And that is exactly the situation right now. Quantum cryptosystems. They're also known as quantum key distribution protocols, technology, that's been around for about 20 years,

Student (A.J)
So just to kind of like, put these in, like short points. So, if we use quantum computing to actually break current encryption systems, then it will take at least from what you said, 20 years to actually reach the technology capable to do so. But to create quantum safe encryption methods, or quantum safe crypto systems, then we can just use available qubits. And so we could be basically safe from something which wouldn't really affect us in 20 years, or until 20 years after.

Dr. Khan
So the consensus is that if you're not implementing quantum cryptographic protocols now, right, actually, as of like, four years ago, then there's so much data out there, right? That when quantum computers, real wants to become available 20 years from now, and you have not implemented quantum cryptography now, actually, right? You would be completely
unprepared for what to do. So the recommendation right now of security experts is that you should implement quantum There are two ways to talk there to kind of, you know, protocols that are quantum safe, right? We use that terminology. There are quantum cryptographic protocols, which use quantum principles of quantum mechanics. That's a separate thing. And there's actually what they call quantum safe for most quantum cryptographic protocols, they do not use any quantum cryptography of quantum mechanics or quantum properties. They just make the mathematics much more harder than it used to be with the hope. And sometimes they actually offer proofs as well. Not too often, but sometimes, that the mathematics would be difficult Enough even for a quantum computer. So the problem with that argument is that when they say the mathematics is going to be too difficult for quantum computers 20 years from now, well, what about quantum computers? 30 years from now, right. 40 years from now, the mathematics is still have difficulty. So that's not a very robust argument. I myself prefer quantum cryptographic protocols, because they give you what's called provable security, using a, you know, the same properties that make quantum computers really fast and powerful. Those same properties actually make them weak against, sorry, the same properties make quantum cryptographic protocols able to, you know, deflect quantum attacks, quantum computing attacks. So that's why I like them, because they're actually a very fundamental feature, and they won't change with time.

…

Discussion with Mr. Khandhadia (VP of information security at Emirates NBD)

(A.J)
So, firstly, like what current encryption systems do they use and banks like, like as of now?

So in the banking industry typically today, we use for symmetric encryption typically people use as, okay. And I think 256 AES two pi six is the is the de facto standard. And of course for asymmetric encryption, a lot of us use RSA for public private key exchanges and stuff like that, right, vividly RFC 2048, RSA 4096, which is the de facto standard for asymmetric encryption.

Okay. And, like, within the five to 10, year within the next five to 10 years, like, are there any existing prospects that like these security standards would change? Or like, maybe move on to like quantum security technologies?

I think the answer to that would depend on a lot of things, first is Moore's Law, right, which is, basically, Moore's law is basically a concept in computing where computing increases 1.5 times fold in a certain amount of time, right. So computation power increases. So as long as competition power increases, and it is able to break algorithms. In the next 10 years, we will need something stronger to prevent us from well, decrypting stuff easily to other prevent attackers from decrypting, deep decrypting stuff easily right. I think, I think in today's in today's banking landscape, or any landscape, actually, wherever encryption decryption happens, it is not the algorithm that is the weakness, it is the key. Right? So if you leave your symmetric key exposed, you are anyways described, so doesn't matter what how strong algorithms, the key is what determines whether you can encrypt or decrypt. So that ad plays a big part in the way that that we try to crack the encryption. Obviously, if you don't have the key, then you're going to have to derive it in some manner, which is where the combination power is required. Right? Yes. So I guess maybe in the next 10 years, if NIST, the national institutional standard technologies, which is what they are the guys who actually certify all the algorithms, if they, for example, state that, you know, a certain algorithm is not secure anymore, then obviously, we'll have to move to something more secure.

do you think that in the short and long term, will quantum security technologies have like a significant effect on the banking sector? Oh, such as like, quantum key distribution or like any other, like, post quantum cryptography?

So I think the answer would probably be yes. Because I think we are trying to protect people's money and data, right. So we will need some stronger from form of cryptography. I think we have not seen I don't think the industry has seen many implementations of common quantum cryptography yet today. In many, many sectors. Maybe in the military sector, you might see something military secret sector, you might see something. I think largely the implementation of quantum is an experimental stage. At least that's what I know so far, unless your research indicates otherwise, when you do research and obviously, what can also happen is that you know, if you look at quantum cryptography, it is good for us. Because it may be my

assumption that it is going to be very hard to break. But obviously if you also have quantum computing, which can break quantum cryptography. Nothing stops an attacker from getting access to a quantum computer. Because in the end, it all boils down to computational power, right? Yeah. Yeah. So today we, for example, we see that, you know, when I want to crack passwords, which are typically not encrypted, but they are hashed.
It won't take me too long to, you know, spin up a machine in Amazon, and start using Amazon's computing power to actually break passwords. Is it possible to do it? It'll take days, sometimes months? But yeah, eventually, patches will turn up. There will be some kind of passwords can that can be revealed?

How hard Do you think it will be for like, for example, like currently, you said that like, for symmetric, you guys are using a yes. And for asymmetric, you guys are using RSA. So how hard you think it would be to actually like, change from them? Like once quantum computing is implemented? And then it's much easier to break these encryption methods than how like, how long do you think on How hard would you think it would be for like, current, for example, say banks to actually move on from different systems?

Oh, God take a long time. Because banks, banks depend on two kinds of ecosystems, right? So basically, I can either buy a product, which suits my banking requirement, or I can build a product right? Now, the beauty with building is, it's in my control. So I can change it quickly if I want to, right. But let's see, if I buy a product, then I have to rely on my window or my supplier to ensure that he has the capability, the skill sets the technology in place to be able to move to quantum crypto. Okay. So a lot of I mean, it's, it's similar to what would happen, let's say, if you were moving from three days to a yes. Or let's say, you know, for example, SSL to TLS, right? It takes time, it takes a lot of time for organizations, to move to strengthen the security. Right. And that's primarily because a lot of organizations depend on vendor products, right. And also, they may have some legacy systems, right, like, even today, in some banks. They are running AES 400, which is like an amazingly strong operating system, but it is old, right? It's got that typical green screen. Remember, the one you seen, like old video games? like Dave, you get that weird font and you type commands, right? There's barely any mouse movement, as such, right? Everything is command based. But yeah, I mean, some banks still use it, right. So when you have legacy systems, also, you will, you may have challenges, because both systems may have some difficulty catching up to crypto. So it depends a lot of factors. It depends on even the size of the organization, right, let's say it's a very, let's say, for example, it's a very small digital bank, you know,
and it has very few systems, right? So in that case, it can be done very easily, maybe like within a year, because they build their own stuff. And, you know, they can easily just start changing their code in the backend and porting it, but when it comes to large banks,
it's going to be a mess can be difficult. I would say maybe at least three to four years.
Because first of all, the tech is so new and revolutionary, right? Understanding how it works, its implementation paradigms, its challenges. I think banks will just discover it on the way so it'd be like a learning for them.