INSTITUTE FOR DEFENCE STUDIES & ANALYSES
रक्षा अध्ययन एवं विश्लेषण संस्थान

IDSA Backgrounder

Quantum Computing and its Impact on Cryptography

Kritika Roy

July 19, 2017

Summary

If Quantum Encryption becomes a reality, it will not only provide secure paths for distribution of these larger keys, but also allow movement of messages in ways that cannot be intercepted. On the other hand, if Quantum Computing turns out to eventually meet some of its expectations; it will have a profound and revolutionary affect on humanity. But the paradoxical question of offense and defence – whether Quantum Encryption will provide unbreakable ciphers, and whether Quantum Computing will result in ciphers being cracked – remain to be answered.

Advances in technology has brought into focus the need to have double assurance on data security, especially with the world moving from classical to Quantum Computing, which latter has the power to unlock the toughest of cyber-locks. In addition, this conundrum over cyber-security has also brought to the fore the dilemma between maintaining an individual's right to privacy and the state's obligation to undertake data surveillance in the interest of security.

In the ancient world, primitive methods were used to protect trade secrets, military orders, or simply keep confidential information from neighbours. These methods included masking of data or substituting parts of a message with symbols, numbers, picture, etc. This practice was later termed as encryption.

Over the years, as technology evolved, the practice of encryption also saw a shift from methods like Atbash cipher (a mono-alphabetic substitution cipher originally used to encode the Hebrew alphabet)[1] and Scytale transposition cipher (a method of encryption in which the plain text is reordered)[2] to digital encryption. In addition, the invention of the World Wide Web paved the way for global connectivity. Technological advances like cloud computing now provide easy access to information from anywhere at any given time. But this ease of accessibility has also brought in its wake the proliferation of high-profile data breaches. That, in turn, has led to a need for more advanced encryption systems to secure confidential data. While good IT (Information Technology) security strategies can be effective in protecting networks, it is still a Herculean task to account for the huge volume of data transiting among mobile devices, browsers, databases and the cloud.

Birth of Modern Encryption

The word "encryption" is derived from the Greek word *kryptos*, which means "hidden." The basic idea of encryption is to ensure confidentiality and provide security including "authentication, integrity and non-repudiation." This is done by converting data to an unknown form or code, which only an authorised person with the "Key" (a random string of characters) could read.[3] The encrypted data is referred to as "cipher text" and decrypted data is called "plain text." While several encryption methods have been developed over time, the basic principles followed remain the same.

---

1 "A brief History of Cryptography," *Cryptozine, May 16, 2008,* http://cryptozine.blogspot.in/2008/05/brief-history-of-cryptography.html

2 Fred Cohen, "A short history of Cryptography," 1995, http://all.net/edu/curr/ip/Chap2-1.html

3 "Encryption Definition," *TechTerms*, November 11, 2014, https://techterms.com/definition/encryption.

There are two main forms of encryption:

Symmetric Key Encryption: Also known as shared secret encryption, this form has been in use since ancient Egyptian times. It makes use of a secret key to enable the sender to rearrange the data into coded form and the recipient to unlock the data. Since the same key is used for both encryption and decryption, it is termed as "symmetric". Today, symmetric keys are usually used by technologies that cater for bulk encryption of data such as e-mails and document files.

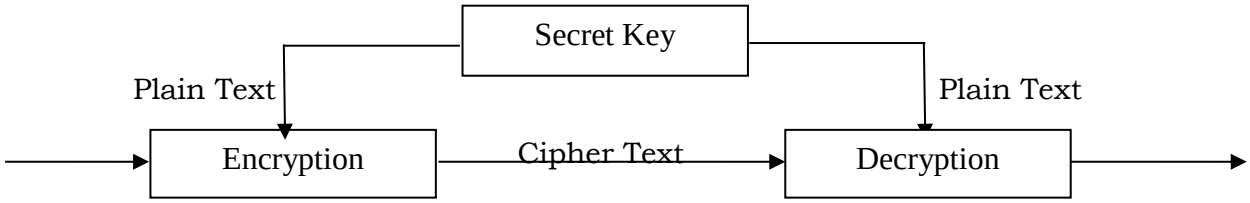

Fig. 1: Symmetric Key Encryption

The drawback of this technique is that one has to transmit the key securely to the intended recipient. Since there is always a risk of the key being intercepted and data stolen by a third party, various systems have been developed to get around this basic weakness.

Public Key Encryption: The invention of "Public Key cryptography" or "Asymmetric Encryption" by Whitfield Diffie, Martin Hellman, and Ralph Merkle revolutionised the field of encryption and provided an answer to the weakness of symmetric key encryption.[4] This technique uses different sets of keys for encryption and decryption – one is the private key or the secret key, while the other is a public key. Both keys are mathematically linked to each other. This encryption is generally used to create digital signatures.

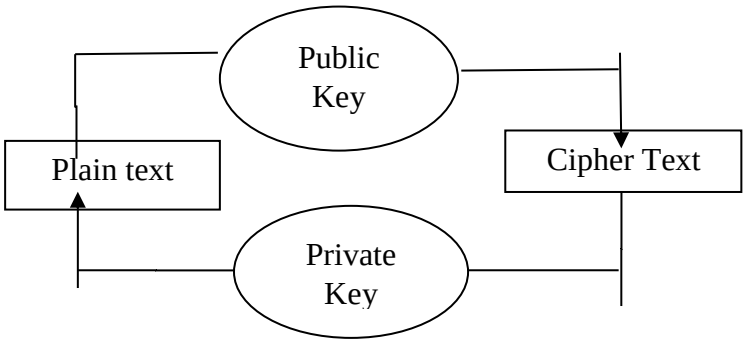

Fig. 2: Public Key Encryption

[4] Tony Howlett, "Open Source Security Tools: A Practical Guide to Security Applications," *Prentice Hall PTR*, July 29, 2004, http://books.gigatux.nl/mirror/securitytools/ddu/ch09lev1sec1.html

Applications of Encryption

With increased awareness and security needs, encryption has come to be seen as the default solution for all data security needs. Encryption is applicable at various levels, i.e., information being encrypted could either be "at rest" (stored data/files/folders present in hard disk or database) or be "in transit" (emails).

- **Full Disk Encryption** refers to encryption at the hardware level. Any file saved to the disk or the external disk is automatically encrypted.
- **File Encryption** enables files to be locally encrypted in order to protect confidential data from attackers with physical access to the systems.
- **End-to-end (E2E) Encryption** is a means by which only the communicating users can read the messages. E2E encryption takes care of all the vulnerabilities in the communication chain: midway (intercepting a message during delivery), and both ends (sender and receiver). Platforms like WhatsApp, Facebook Messenger, etc. use this encryption.
- **Encrypted Web Connections** are achieved by using Hyper Text Transfer Protocol Secure (HTTPS) in the Universal Resource Locator (URL). HTTPS pages utilise one of two secure protocols to encrypt communications –Secure Sockets Layer (SSL) or Transport Layer Security (TLS) – when a browser and server communicate over the web, thus making the connection secure.
- **Encrypted e-mail Servers** use a protocol called Secure/Multipurpose Internet Mail Extensions (S/MIME), i.e., a public key encryption that allows transfer of encrypted messages via Simple Mail Transfer Protocol (SMTP). Pre-encrypting the data that is synced with the cloud is another way of securing data before it gets to the cloud.

Why the Need to Encrypt?

The introduction of cloud computing has made it possible for the same server to handle multiple workloads simultaneously, thus making it cost effective, flexible and popular. But if these servers are running in a "public cloud infrastructure", one would have limited control over who shares the hardware, thus making the virtualised servers rich targets. Here, encryption makes it possible to reap the benefits of the infrastructure while at the same time ensuring data protection and privacy. Further, encryption also provides an upper hand to organisations over service providers when it comes to spinning up or decommissioning the servers since the former, as owners of the "Key," get to pull the strings.

Encryption also satisfies the PCI (Payment Card Industry) Data Security Standard of protecting stored data, which simply means using a credit/debit card or shopping

online with the assurance that the backend information is totally safe. When a payment card (debit or credit) is swiped, the card reading device (also called Point of Interaction or POI) immediately encrypts the information. A device, which is part of a PCI validated P2Pe (Point to Point encryption) solution, uses an algorithmic calculation to encrypt the data on the card and sends it to the payment gateway for decryption. At no point during the transaction are the keys for encryption and decryption available to the merchant, thus making card data entirely hidden and secure from the retailer.[5]

Encryption systems are continuously at work in nearly every dimension of modern technology, not just to coordinate plans (like the use of the Telegram app to send encrypted messages, videos, photos or files of any kind to up to 200 people) or protect information from criminals, enemies, or spies, but also to validate basic, personal information and provide confidentiality and integrity to the data.

Challenges to Contemporary Encryption Processes

Encryption does not make the data entirely secure; rather it provides an additional layer of security against data theft or compromise since criminals have to decrypt the data by deciphering the encryption key. The length of the key determines the possible number of combinations that can be attempted on the 'secure key'. In other words, the strength of encryption is directly proportional to the length of the key. The longer the key the less vulnerable it is to attacks.

The most common form of attack is trying out random keys (by trial and error method) until the right one is found. Other such attacks include side channel attack, which does not target the cipher itself but instead other information retrieved from the encryption device such as implementation time, radiation, power consumption, etc.[6] These parameters can be modified so as to generate predictable outcomes.

Likewise, there is cryptanalysis in which once the flaw is located in the cipher then it can be very easily exploited. Cryptanalysis is more likely to occur when there is a loophole in the cipher itself. Another drawback of encryption is its susceptibility to human error. Poorly developed encryption is not hack proof. For example, home-grown encryptions – cryptos designed by individuals – have rarely withstood the rigorous testing that is done in case of published encrypted algorithms.

With the rapid rise in the number of cyber-crimes, the time is not far ahead when advances in digital technology would be instrumental in breaking complex keys. Simply assuming that data is secure because no one has yet cracked open a complex

5 "P2PE:Payment Technology," *creditcall*, https://www.creditcall.com/what-we-do/p2pe

6 Nate Lord, "What is data Encryption," *Digital Guardian*, January 27, 2017, https://digitalguardian.com/blog/what-data-encryption

encryption key provides no guarantee that these keys, based on factoring large numbers, will be secure forever. For instance, a student at Notre Dame University used 10,000 computers working continuously for 549 days to break a 109-bit key.[7] This shows both the difficulty involved in decoding keys and the certainty that they can still be broken given enough computer power.

Where Does Encryption Stand Today?

Various government organisations and agencies enjoy the security of strong ciphers, yet often attempt to limit individuals from using strong encryption methods. States in particular have pushed for special exceptions in order to gain access to encrypted data. Such unauthorized access has several names like “backdoors”, “master keys”, and so on. Globally, intelligence agencies are concerned about terrorist organisations such as ISIS making effective use of social media for nefarious activities. In December 2015, there was a shooting incident at San Bernardino, USA, resulting in the deaths of 14 people.[8]Apple refused help to the Federal Bureau of Investigation for breaking the code of the iPhone used by one of the attackers. Similarly, on March 22, 2017, when a terrorist attack took place in the vicinity of the British Parliament, WhatsApp refused access to the encrypted messages of the attackers to the security services.[9]Over the years, major private organisations handling messaging and communications services have denied such access to government agencies for carrying out unlawful eavesdropping because of business, security or technical reasons. They also argue that providing such access would infringe upon human rights. Further, it would also weaken their overall levels of encryption, thus making their services more insecure. The dilemma between securing an individual's right to privacy and the obligation of state authorities to investigate and access information for reasons of national security is quite evident. According to Bruce Schneier, cryptographer and security and privacy specialist, "Backdoors are a vulnerability, and a backdoor deliberately introduces vulnerability. I can't design those systems to be secure, because they have a vulnerability."[10]

---

7 “Notre Dame math whiz cracks code,” *Reuters,* November 07, 2002, http://www.zdnet.com/article/notre-dame-math-whiz-cracks-code/

8 Evan Perez and Tim Hume, “Apple opposes judge’s order to hack San Bernardino shooter’s iPhone,” *CNN*, February 18,2017, http://edition.cnn.com/2016/02/16/us/san-bernardino-shooter-phone-apple/index.html

9 Gordon Rayner, “WhatsApp accused of giving terrorists 'a secret place to hide' as it refuses to hand over London attacker's messages,” *The Telegraph,* March 27, 2017, http://www.telegraph.co.uk/news/2017/03/26/home-secretary-amber-rudd-whatsapp-gives-terrorists-place-hide/

10 Max Eddy, “Crypto Wars: Why the fight to Encrypt Ranges on,” October 10, 2016, http://in.pcmag.com/encryption/108918/feature/crypto-wars-why-the-fight-to-encrypt-rages-on

The Future of Encryption

Cryptographic systems are difficult to crack, as they are based on the principle of factoring large numbers. In 1970, there was a breakthrough in factoring called "continued fractions". This discovery led to speculations that advances in factoring may reduce the complexity of cryptographic systems and render them much more vulnerable. Ten years later, factoring was pushed further by "Pomerance's quadratic sieve" and the work of Richard Schroeppel.[11] Now, with the possibility of quantum computing, which can factor large numbers in split seconds, every system that relies on encryption can easily be bypassed.

Quantum computing commenced with the work of Paul Benioff and Yuri Manin in 1980, Richard Feynman in 1982 and David Deutsch in 1985.[12] Quantum Computers are a new type of machine that juxtapose the quantum properties of matter and light with the field of information security. Precisely when that day will arrive is unclear, but experts call the countdown as Y2Q: "Years to Quantum."[13]

Classical computers use the binary 1-or-0 system to function. Quantum computing uses Quantum bits or "qubits". These bits are peculiar because they do not just have two states but multiple states (principle of superposition) all at the same time. This means a computer using these bits can store as well as process a huge amount of information that too by using less energy. The other principle that qubits follow is "Entanglement". This means that qubits in a superposition can be correlated with each other: the state of one (whether it is a 1 or a 0) can depend on the state of another; or a change in one part of the system will lead to the rest responding accordingly without changing the entire operation.

The ambivalent nature of Quantum computing, i.e., being a threat to the present encryption method and simultaneously also being the solution to the encryption threat makes it much more striking in the current security matrix. Quantum Computing might have paved the way for Quantum encryption. Currently, several scientists are in the race to deploy foolproof quantum encryption before anyone develops a computer that can break open a password in a split second.[14] This method of encryption will employ Heisenberg's Uncertainty Principle, which states that "the position and velocity of an object cannot both be measured exactly, at the same time,

---

11 Ibid

12 *Deutsch, David (1985). "Quantum Theory, the Church-Turing Principle and the Universal Quantum Computer," Proceedings of the Royal Society of London A., http://adsabs.harvard.edu/abs/1985RSPSA.400...97D*

13 Alex Hutchinson, "Hacking, Cryptography, and the countdown to Quantum Computing," *The New Yorker,* September 26, 2016, http://www.newyorker.com/tech/elements/hacking-cryptography-and-the-countdown-to-quantum-computing

14 Jeff McMahon, "Will Quantum Encryption come before quantum computers break all our passwords," *Forbes*, April 17, 2016, https://www.forbes.com/sites/jeffmcmahon/2016/04/17/will-quantum-encryption-arrive-before-quantum-computers-guess-all-our-passwords/#51a9260d281a

even in theory."[15] This principle is only applicable to quantum properties of light and matter. The unique point of using Quantum encryption is that it is impossible to interfere with messages being sent (using light waves) without hindering the basic properties of the message. Because, the quantum fact states that observing a quantum property irrevocably alters the object being observed. Besides, if the message is intercepted at any given point of time, it becomes useless to the recipient. Thus, the ability to detect an eavesdropper during a key transaction increases the utility of this encryption for data security.

Furthermore, Quantum technologies would also be able to handle problems of "image and speech recognition" as well as "real-time language translation". Though much work remains to be done in this field, there are already a few accomplishments like quantum-enabled sensors, quantum networks and rudimentary quantum computers.

Considering the uses that Quantum Technologies are going to demonstrate, countries have already made it an arena of race to gain supremacy. Lately, individuals in countries like Singapore, Canada, Japan, Italy and America are engaged in conscientious efforts to ensure complete data security. Like the development of China's Quantum Satellite, which envisages a technology that could make data breaches a thing of the past; this venture could be termed as the first successful initiative towards unmitigated security of data.[16] But again one needs to understand that issues like cyber security have a history of transcending boundaries and only with country-spanning networks and quantum enabled devices one could be assured of world-wide quantum-enhanced security.

Quantum Encryptions also have a few stumbling blocks to overcome like the issue of transmission loss or noise. Scientists have been experimenting to eliminate such snags and make the process foolproof. They are also trying to find out ways to reduce the occurrence of errors and increase reliability across longer distances and in longer strings of information. With the improvement in hardware as well as advances in technology, quantum networks may begin to look like a "strategic must-have"; if so, consumer applications are also likely to increase.

---

15 Werner Heisenberg, "Uncertainty Principle," *Britannica,* https://www.britannica.com/science/uncertainty-principle

16 "Here, there and everywhere," *The Economist*, http://www.economist.com/news/essays/21717782-quantum-technology-beginning-come-its-own#s-3.

Conclusion

Understanding Quantum technologies has become an essential national investment especially in the current milieu, wherein proficiency in Quantum technologies is likely to yield "quantum pre-eminence" and "strategic dominance". Governments across the world have started to invest heavily on these technologies not only to gain superiority in the cyber domain but also to avail the benefits of quantum research and innovation for defence and security. Also, with the exponential growth in the use of high encrypted technologies like the use of encrypted communications over various chat groups to facilitate terror activities, it becomes obligatory for states to develop and showcase "Quantum" capabilities just to have an upper hand over terrorists. The true potential of Quantum computing lies in identifying all the issues that classical computers are unable to solve and then finding ways of doing so.

However, Quantum breaking (the process of breaking present-day encryption via quantum computing) of classical encryption remains a major threat from state/non-state actors and simultaneously a driving force in the continued research and development of Quantum computing as well as Quantum encryption. If Quantum Encryption becomes a reality, it will not only provide secure paths for distribution of these larger keys, but also allow movement of messages in ways that cannot be intercepted. On the other hand, if Quantum Computing turns out to eventually meet some of its expectations; it will have a profound and revolutionary affect on humanity. But the paradoxical question of offense and defence – whether Quantum Encryption will provide unbreakable ciphers, and whether Quantum Computing will result in ciphers being cracked – remain to be answered.

About the Authors

Kritika Roy is a Post Graduate Scholar at Manipal University.

The Institute for Defence Studies and Analyses (IDSA) is a non-partisan, autonomous body dedicated to objective research and policy relevant studies on all aspects of defence and security. Its mission is to promote national and international security through the generation and dissemination of knowledge on defence and security-related issues.

Institute for Defence Studies and Analyses
1, Development Enclave, Rao Tula Ram Marg
New Delhi 110 010 India
T +91-11-2671 7983 F +91-11-2615 4191
contact.idsa@nic.in www.idsa.in
Twitter @IDSAIndia
www.facebook.com/InstituteforDefenceStudiesAnalyses