AARMS Vol. 19, No. 3 (2020) 5–22.

10.32565/aarms.2020.3.1

Security of Encryption Procedures and Practical Implications of Building a Quantum Computer

Ferenc KOCZKA[1]

In ensuring the operation of an IT system, it is essential to maintain the data's confidentiality and integrity, which is based on some encryption processes. Encryption procedures are based on algorithms, the theory of which is given by cryptography. Due to their complexity, they are often hardly understandable not only to an average person but also to the majority of professionals who are familiar with IT. The algorithms used are not eternal; various designs or implementation errors or even performance gains from computer hardware improvements make one time high achieving algorithms obsolete and easily hackable. Strong algorithms can be circumvented in alternative ways, the necessary software and hardware infrastructure can already be built from personal computing devices. I tested its effectiveness on two different password databases: with the success of hacking university passwords, I prove that it is possible to circumvent strong algorithms with simple methods. Modern encryption algorithms have a relatively long life cycle and they become obsolete slowly. The construction of the quantum computer creates a new situation, which requires a number of procedures to be eliminated and its parameters to be modified or protected by additional methods. As it is an impossible task to modernise the encryption algorithms of all IT systems operating today, preparations must be started as soon as possible so that the new situation can be handled, at least for critical systems. In my article, I would like to draw attention to the weaknesses of encryption methods, present a possible method of circumventing the cryptographic methods currently in use, demonstrate the operation of a quantum computer and some algorithms relevant to the topic.

Keywords: *encryption, hash code, password security, crack, quantum computer*

Introduction

Most IT tools include some kind of encryption process, which is largely responsible for confidentiality and integrity, especially for the implementation of secure communication and data storage. Their application is unavoidable as there is no guaranteed technical

[1] Director of IT, Eszterházy Károly University; e-mail: koczka.ferenc@uni-eszterhazy.hu

possibility of preventing network communications interception, so those requirements can only be ensured by using encryption procedures. The theoretical support for hiding data is the task of cryptography, which has developed several procedures to achieve this goal. The use of cryptography in modern warfare is also essential. The usual practice of military developments being transferred to the civilian sphere has now been reversed after a while, so many military solutions build on public procedures to meet specific requirements.

These algorithms also play a role in counter-terrorism protection. Eavesdropping on terrorists' communications, preventing the communication capabilities of attack equipment built almost exclusively from ordinary devices, is impossible without cryptography. Several everyday devices can be used to activate a bomb: a mobile phone, garage opener, CB radio, wireless bell, or even children's toys. The Ukrainian Aerorozvidka group used a self-built drone to carry out successful military reconnaissance and data collection tasks.[2] The difficulty of this task is the use of a set of tools using various forms of communication. However, the IT procedures used in battlefield communication are different from those used in civilian life. The main reason for this is low computing power for low energy consumption and limited data transfer speeds available in combat conditions, which in many cases is only a fraction of what is common in everyday life.

An important goal of electronic protection is to intercept the enemy's communications, which is an important element in developing information superiority. Nowadays, warfare is present not only on the battlefield but also in civilian life, the protection of communications between constituents of national security importance turned to an essential task. Although not recognised by most states, detecting and purchasing security holes of computer systems[3] are generally used for developing offensive cyber weapons.[4]

Therefore, cybersecurity success depends greatly on the functioning of the cryptographic algorithms used; their vulnerability and inadequate implementation can have serious consequences.

Historical overview

From the point of view of warfare, important encryption procedures date back to ancient times. One of the first procedures is called the Caesar method, whose algorithm is very simple. It mingles each letter of the alphabet with another one at a certain distance to quickly encode the text to be encrypted and decode it at the destination. Although the procedure was considered safe at that time (even literacy was not typical), today, messages encrypted using these types of methods can be decoded in no time. Trying out possible cases is only one option because if the message's language is known, the frequency of characters in the message can also be an easy guide to determine which character has been replaced by which one. However, throughout history, especially in warfare, some variant of Caesar's method

[2] Péter Huszár, 'Ukrajna közösségi finanszírozású, katonai célokat szolgáló oktokoptereinek elemzése', *Hadmérnök* 14, no 2 (2019), 34–43.

[3] The Zerodium offers a high amount for vulnerabilities not published elsewhere. See https://zerodium.com.

[4] PA Media, 'UK has mounted covert attacks against Russian leadership, says ex-mandarin', *The Guardian*, 24 October 2020.

has been used on many occasions. The timeliness of the solutions based on the exchange of letters remains current in many modified versions, even in the two world wars.

In the history of encryption, we find some methods and tools, one of the most well-known of these was the German-made Enigma, which appeared in World War I and was used until the 1970s to encrypt and decrypt radio messages, which, through continuous developments, included a family of machines operating along with an increasingly complex set of rules. There was only a small chance of breaking the encryption of Enigma machines at the era's technical level. Combinations of rotors provided encryption, and the high number of variations made it impossible to decrypt the encrypted message in real-time. The practical procedure used by Enigma had several weaknesses. Due to the use on the battlefield, the risk of key transmission must be taken into account. Its cryptographic weakness stems from the very large keyspace defined by the equipment. The encryption was determined by the set of used rotors, their order and positions. In total, they gave 2,109,120 different options, which were not impossible to decrypt even in World War II by the try-and-try method.[5] As a result, one of the greatest minds in IT, Alan Turing, built a machine that could eventually be successfully used to decrypt battlefield messages, making it a major part of the war's outcome.

The development of encryption procedures and the competition for research into their hacking have accelerated with the appearance of electronic computers, and relatively demanding procedures can be quickly operated. Along the lines of modern mathematical approaches, many methods have been found that seem hopeless to crack today.

Encryption methods

There are several types of encryption procedures, but there are three types to address for our topic. In most cases, symmetric encoding is used to transmit encrypted messages after a key exchange using public-key encryption, and hash algorithms are used to verify (but not only for that purpose) integrity.

When symmetric key encryption is used, the key used for encrypting and decrypting is the same and can be used to encode and decode a message. Several great algorithms such as this are known as typical examples of highly complex 3DES or AES. These use the key in mathematical formulas to create an encrypted form of the message through multiple substitutions. Without knowing the key, decryption is not real with today's IT tools. The great advantage of symmetric encryption procedures is speed; the performance of most algorithms is sufficient to encrypt large amounts of data in a short period. In the case of Enigma, the key is the type of rotors used to encode the message, their initial positions, and the staple board settings. The key transmission plays an extremely important role in the process and in World War II, it caused a fatal error in the defence of the Navy's M3 model.

[5] Richard E Klima and Neil P Sigmon, *Cryptology: Classical and Modern* (Chapman and Hall/CRC Press, 2018).

The machine acquired during the interception of the U-110 submarine, and the documents requiring its settings allowed the Navy's messages to be decrypted for nearly 9 months.[6]

Public key encryption works completely differently from the point of view of the key. It is based on a pair of keys generated using an open process, using large prime numbers. One element of the key pair is made the public key, and the other is treated as the private key and is prevented from being known to others. The key pair is special in that a message encrypted with one party can only be decoded with the other party (that is, not with the encoding party itself). A public key encryption data is always performed with the public key of the target person or device, taking advantage of the knowledge of the private key that it owns to decrypt it. This procedure also implements the digital signature by encrypting the message with the sender's private key, the authenticity of which can be verified by decoding with the sender's public key.

These algorithms are not affected by the problem of key transfer. Therefore, they can ensure confidentiality and integrity, even in cases where the sender and receiver's entire communication is intercepted. Their practical usage, on the other hand, is greatly hampered by their high computing expectation. Perhaps the most popular members of this family are RSA and DSA. The combination of the two methods can eliminate their disadvantages. In many cases, including SSH operation,[7] public key encryption is used to create a secure connection, but this is only used until the symmetric key is transmitted. After a successful key exchange, the connection is continued with fast-functioning symmetric key encryption.[8]

In addition to encryption procedures, the priority area for our topic is the so-called hash algorithms. These algorithms do not actually encrypt, they just create a short code, named hash, from a series of data of any length.[9] Therefore, the hash is not the encrypted form of the original data series, from which the original series cannot be restored; it only allows to check its integrity. To do this, you need to re-calculate the hash value for the series and compare it to the original. Since changing the source involves a radical change in the hash, any modification is very easy to detect. Well-known hash procedures are variants of SHA[10] of varying strengths.

From a cryptographic point of view, hash algorithms also play a major role, from checking the integrity of transmitted data to the operation of several cryptocurrencies in network communication. Hashing procedures are also widely used when storing passwords. In most systems, to prevent an attacker from knowing the cleartext passwords in a system when user data is compromised, only the hash values that are made from them are stored, not

---

6 Forces.net, 'The First Man To Storm A Nazi U-Boat And Seize An Enigma Machine', 06 January 2016.

7 SSH stands for Secure Shell, which is the name of a computer protocol and the program that uses it. Using strong encryption, it implements a number of functions: it allows you to log on to remote computers, copy files and create encrypted tunnels.

8 Daniel J Barrett, Richard E Silverman and Robert G Barnes, *SSH, The Secure Shell: The Definitive Guide* (Sebastopol: O'Reilly, 2001).

9 Donald E Knuth, *The Art of Computer Programming* (Boston: Addison-Wesley, 1973).

10 The first version of SHA was published in 1993 and was provided in several versions (SHA-224, SHA-256, SHA-384 and SHA-512). The mining of Bitcoin actually means training mass SHA-256 hashes and finding an instance with a specific property.

the password itself. When a user logs on, the hash from the specified password must match the one stored in the system to allow access.[11]

Cryptographic algorithm errors

During the development of computing devices, many algorithms that had previously been widely used proved weak. The vulnerable md5 algorithm is already discouraged; therefore, all devices had to be replaced which contained it. This procedure is simple in systems where the developer still supports the software and knows its users so that the upgrade can be carried out, and the modified component can be sent to the destination. On the other hand, hardware and software components no longer supported or whose operators cannot be notified to perform the upgrade are more difficult tasks. Equipment designed to keep production costs low to such an extent that the device cannot run a component with higher computing needs at an acceptable speed is a separate category, typical examples of which are IoT devices.[12]

In principle, the exchange of procedures may be necessary for two reasons: a conceptual error in the algorithms used or an implementation error. The latter is caused in most cases by some programming error that weakens the otherwise well-functioning algorithm. Typical sources were faulty random number generators, which did not generate random numbers, so instead of unpredictable input data guaranteeing correct operation, they provided reproducible or repetitive input. Such an implementation error can be caused by leaving key data in memory after the code runs or making it available to other applications. In the case of Enigma, the implementation error is the constraint on the type of rotors selected, their order and their initial settings, which drastically reduced the size of the keyspace as described above. Implementation errors are characterised by the failure of only one operating system or device, while they do not occur in the case of other users of the same procedure.

Conceptual errors in algorithms are much more serious problems. An example that still affects many systems today is KRACK (Key Reinstallation Attack). This vulnerability affected the WPA2 algorithm; therefore, almost all Wi-Fi devices became unsafe,[13] and providing updates took months.[14] As the error was in the algorithm itself, many devices became vulnerable at the same time, regardless of their operating system. In the case of KRACK, the situation is further exacerbated by never updating the operating system of

---

11 Because the same hash value can come from several different input data, this method may allow access with a different password.

12 Internet of Things (IOT) devices are low-performance IT devices that are typically able to collect and transmit information over the Internet at low power consumption.

13 The whole point of vulnerability is when a wireless network connection is established, the client (computer, mobile phone, and so on) initiates a connection request to the network device (for example, Wi-Fi router). The connection is technically the result of a multi-step dialog, in the third step of which the two parties are identical to the encryption key used. Because a network error can occur at any time during connection creation, such as during this step, the procedure is able to resend this encryption key. An attacker could use this to collect and re-send these keys, forcing the device to reset its own internal counter (nounce). Because the algorithm is only secure if this counter is not repeated, this procedure can be used to break it.

14 Mathy Vanhoef and Frank Piessens, 'Key Reinstallation Attacks: Forcing Nonce Reuse in WPA2', *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security*, October 2017, 1313–1328.

some of the users' wireless network devices, which does not appear on old systems so that the error will be exploitable for years.

Brute force methods

One of the recipes for breaking an encrypted communication is to reduce the keyspace as much as possible and then try through possible combinations in as short a time as possible. The reduction can usually be made with higher mathematical knowledge, but the amount of time it takes to try depends mostly on the computing power of the computer used.

With the release of cryptocurrencies, many specialised devices with previously unimaginable computational power appeared on the market using this technique. Their purpose is mass hash computing, which was used to mine cryptocurrencies. The Antminer S19 Pro[15] is capable of 110 Terrahash per second with 3500W power consumption. Higher-value VGA cards can also be used to solve such tasks. Their processors (GPU – Graphical Processing Unit) are significantly faster than the processors of commonly used computers, so they are also suitable for brute force methods.

One of the most important motivations for cyberattacks is to obtain personal and economic data and access parameters. One way to protect them is encrypted storage, in particular access passwords, recorded in a readable form instead of the hash mentioned above value, which is now a professional error. Although the GDPR does not impose specific requirements on passwords, it does provide for sanctions in the event that an organisation leaks large amounts of personal information. That is the reason why it is not in the organisations' interest to store readable passwords. No legislation formulates any specific encryption procedure, so it is up to the developer to choose and implement its method.

The need to encrypt passwords in this form is also demonstrated by the fact that the systems of the world's largest IT companies have also been hit by cyberattacks in which large-scale personal data has occasionally been compromised by passwords, but mostly only by hashing it and has been offered for sale to spamming service providers, or on the Darknet.[16]

Check password hash cracking using traditional tools and methods

IT professionals are also divided on the chances of breaking different encryption procedures or hashing out original passwords. Internet sources provide measurement results on the speed at which systems developed along a specific hardware and software environment can generate password hash values.[17] These often refer to raw data and do not take into account

---

15 For more details see https://miners.eu/product/bitmain-antminer-s19-pro-110th-bitcoin-miner

16 On *haveibeenpwned.com* page, you can examine whether a specific email address was involved in an incident that is currently being investigated. Their database contains more than 10.5 billion records. The site also provides information about data breaches, which include very popular, large companies such as Adobe and Dropbox.

17 The results of the series of measurements using the NVidia GTX-1080 VGA card with Hashcat software on a Linux operating system. See https://gist.github.com/epixoip/a83d38f412b4737e99bbef804a270c40

users' password-training habits and fine-tuning techniques for brute force. To test this, I took measurements on the directory containing the real password impressions of Károly Eszterházy University (EKE).

Since the university's central IT organisation provides complex services with many different systems, several different hash values of passwords have been recorded in the central directory. This provided the opportunity to examine the strength of NTLM and SHA-1 hash algorithms.

An I5-based Linux desktop computer carried out the test with an SSD, in which an NVidia GTX Titan VGA card provided the necessary computing capacity. Hash computing was done with HashCat[18] software, which can use the GPU of the VGA card to perform the task. The time required for each measurement was capped at four days.

HashCat is not only capable of searching for a password for a hash but can also batch-operate by trying to crack all elements of a file containing hashes in a single operation. To be able to tune the hacking process, HashCat allows you to set so-called masks. These are regular expressions that can define specific password forms by describing the characters that can stand in each position. The suitable settings for masks greatly affect the effectiveness of decrypting passwords; in our experience, special characters are typically used by users towards the end of the password.

In the first phase of the test, I examined the 2650 NTLM password hash values by tuning the software's operation with different masks. We conducted the test in five different configurations:

1. No fine-tuning was performed in the default setting (default mask) test.
2. We did not refine the search process in the full ASCII namespace setting, that is, we attempted to find all possible passwords.
3. We tested different variants when applying our masks; the best result was given by the third. We assumed that either position could consist of upper- and lower-case letters, digits, and special characters for passwords of six characters or less. For longer ones, a special character was assumed in only two positions, and in the others, only lowercase or number.

Table 1 shows the number of compromised passwords based on their length.

Table 1: NTLM password length and the number of cracks

Hits	**Password length**					
	4	**5**	**6**	**7**	**8**	**9**
Default mask	2	11	26	25	186	117
Full ASCII namespace	2	11	28	26	–	–
Own mask 1	2	10	27	24	25	13
Own mask 2	2	11	28	25	435	–
Own mask 3	2	11	28	25	435	154

Source: Compiled by the author.

[18] For more information see https://gist.github.com/epixoip/a83d38f412b4737e99bbef804a270c40

The measurement shows that it was not practical to examine the entire namespace when cracking NTLM passwords. It performed better when examining 7-character passwords, but for 8- and 9-character passwords, we had to give up because of a very high run time. The best result was achieved with the type 3 mask, which decrypted a total of 655 passwords, which is 24.7 per cent of the total password space.

The time required for the above results is given in Table 2. According to this, the time needed to crack passwords was less than one second for six characters, and decrypting the eight-character passwords did not require too many resources. Therefore, based on the time data, 9-character passwords cannot yet be called secure, so it can be concluded that longer passwords must be required to be secured.

Table 2: NTLM password cracking times

	Password length					
Running times	**4**	**5**	**6**	**7**	**8**	**9**
Default mask	~0s	~0s	~0s	23s	18m 35s	12h 41m
Full ASCII namespace	~0s	3s	2m 14s	3h 39s	Not measured	Not measured
Own mask 1	~0s	2s	5s	2m 34s	1h 54m	3d 5h
Own mask 2	~0s	~0s	19s	5m 40s	4h 8m	Not measured
Own mask 3	~0s	1s	19s	3m 13s	2h 18m	3d 21h

Source: Compiled by the author.

Breaking the 2194 SHA1 hashes has proved to be a more difficult task. Due to the complexity of the procedure, the GPU of the VGA card produced fewer hashes in a time unit. The time available to decrypt the nine-character passwords was not enough, but compared to the previous values of NTLM cracking, it can be concluded that the result is not far behind in terms of success. However, the time taken to calculate was about tripled. Overall, 470 passwords were broken, which means a result of 21.4 per cent.

Table 3: SHA-1 password length and the number of cracks

	Password length				
	4	**5**	**6**	**7**	**8**
Number of variations	$2{,}40 \times 10^{7}$	$1{,}68 \times 10^{09}$	$1{,}18 \times 10^{11}$	$1{,}02 \times 10^{12}$	$4{,}18 \times 10^{13}$
Running time	~0s	~2s	1m 6s	10m 55s	7h 24m
Hits	2	11	21	22	414

Source: Compiled by the author.

Overall, it can be concluded that with a computer worth approximately HUF 200,000, the optimal setting of the hacking software, more than one-fifth of the organisation's passwords could be decoded in less than four days. By measuring, I found that 8-character passwords no longer provide sufficient protection.

Data on the Darknet

When examining password security, one must ask the following question: How many institutional email addresses were found in databases that have been stolen from companies that manage them? These addresses appear not only in the address lists that are the source of spam but also in databases with other data, obfuscated or readable passwords, for example, on the Darknet. To look at the extent to which email addresses of Eszterházy Károly University have been affected by these attacks, I have used a collection of more than ten billion records available at *http://haveibeenpwned.com.* The site's database of 485 different data breaches at the time of writing these lines contains 10.5 billion data access. Anyone can check which incident or collection their email address[19] was involved in. Bulk verification can be done[20] through so-called API calls, which I used in the verification software.

When examining email addresses, I used the university's full address list, which included not only the live addresses but also the delisted addresses, including the institution's previous domain,[21] which justifies the number of email addresses high relative to the size of the institution. The measurement results showed a very favourable condition; only 50 out of the 6,386 email addresses were found in this database, which is less than 1 per cent. These email addresses have been involved in 11 different incidents, a total of 87 times, so overall, it can be established that the email addresses of the University of Eger were only minimally present in these databases. The details are summarised in Table 4.

Table 4: Data leaks and the number of email addresses affected

#	Source	Number of hits
1.	Collection #1 [Collection1] 2019-01-07	52
2.	2,844 Separate Data Breaches [2844Breaches] 2018-02-19	11
3.	Canva [Canva] 2019-05-24	6
4.	Covve [db8151dd] 2020-02-20	5
5.	Apollo [Apollo] 2018-07-23	4
6.	Onliner Spambot [OnlinerSpambot] 2017-08-28	2
7.	Exploit.In [ExploitIn] 2016-10-13	2
8.	Anti Public Combo List [AntiPublic] 2016-12-16	2
9.	LinkedIn [LinkedIn] 2012-05-05	1
10.	Edmodo [Edmodo] 2017-05-11	1
11.	Data Enrichment Exposure From PDL Customer [PDL] 2019-10-16	1

Source: Compiled by the author.

[19] In addition to data obtained during multiple specific attacks, the site database contains data from other partially known incidents. The attackers sold them as collections named by them or the site operator.

[20] The Application Programming Interface (API) is a way of communication developed between programs. For *haveibeenpwned.com*, this is currently available as a monthly service.

[21] Prior to its change into a university, EKE operated its correspondence under the *ektf.hu* domain, which was replaced to uni-eszterhazy.hu in 2015. These types of changes are expected to occur in large numbers as a result of the ongoing reorganisation of universities.

The leakage of these 10.5 billion records does not mean that it contains passwords in readable format. These are often coded, so they are not usable but leaked in coded form. Examination of the university password database, on the other hand, points out that the theoretical security offered by the algorithms does not necessarily work well in practice. To improve the efficiency of encryption, industry-leading companies apply a number of security modifications to their software. Google has made it impossible for Chrome users to download files from pages that use https unencrypted (http).[22] Apple has reduced the validity of Safari browser certificates from two years to one, shortening the useful life of any compromised keys.[23] Safari also regularly checks the passwords stored in the user profile and alerts you if any of them have previously been made public.

Our investigation of password cracking was effective up to nine-character passwords. With more investment, this can be increased by additional characters, but the required computational capacity is multiplied by each character. This is why in many cases it is not worth experimenting with brute force methods, so hackers prefer to use phishing or social engineering methods. In a 2018 measurement, also at EKE, using social engineering methods, 17.3 per cent of users' passwords were obtained. Based on my measurement, it can be concluded that the efficiency of SE, which is much easier to implement, does not differ significantly from the 24.7 per cent and 21.4 per cent results measured in the present research.

Administrative regulations

Public communication services based on algorithms providing strong encryption are also a problem for defence organisations in nations. Well-known encryption procedures that are truly unbreakable or unrecognisable due to the transmission of an encrypted message put state law enforcement at a serious disadvantage.[24] Because some encryption procedures cannot be avoided from a technical point of view, administrative methods can solve the problem. The relationship between the largest IT companies and the authorities does not go beyond professional rumours. Still, in addition to the United States of America, the idea of restricting or weakening encryption algorithms and prohibiting applications using end-to-end encryption has already been raised in the Hungarian Government. In 2017, the Hungarian Government drafted a proposal that would have prohibited the use of communication applications. The authorities can exercise its right of access, but this was not finally accepted.[25]

However, the interception and processing of digital signals (SIGINT) are not illegal in all countries. A prominent example is the Echelon network, which aims to support SIGINT

---

22 For more details see https://blog.chromium.org/2020/02/protecting-users-from-insecure.html

23 See www.thesslstore.com/blog/ssl-certificate-validity-will-be-limited-to-one-year-by-apples-safari-browser

24 For example, steganography is the science of hiding a message in a normal message. In most cases, the message itself is hidden in an image or audio file during practical implementation. Many free programs are available to achieve this service.

25 Bitport, 'A titkosítás tiltása veszélyes', 30 March 2016.

operations, intercept and decipher private and business encrypted communications.[26] Its members were the states that accepted the UKUSA agreement, originally established by the NSA (National Security Agency) and GCHQ (Government Communications Headquarters). The International Surveillance Alliance, known as the Five Eyes, which is made up of the United Kingdom, USA, Canada, Australia and New Zealand, is the main objective of electronic intelligence.[27]

As a result of government-level support for these organisations, so-called backdoors are installed in the source code of some applications, ensuring that the authority can decrypt encrypted communications, review the service provider's event logs, and reveal the identity of the participants in the communication. General providers offering confidentiality of communication (typically VPN providers) are of great importance, and it is appropriate to establish, promote and control them with state aid. However, these methods do not work for software that implements encryption on endpoints, for example, the parties' devices involved in the communication. Besides, open source code can be a safeguard for the program's integrity.

Backdoors are considered dangerous by most IT security professionals, both in encryption algorithms and in applications. Keeping them secret is almost impossible, promotes crime in the wrong hands, undermines trust in IT systems, and would have a seriously debilitating economic effect. Therefore, the social acceptance of these methods is low. Their operation encourages civil society to transfer its network connections through less supervised zones, with which it is likely to have the opposite effect.

The quantum computer

Although most of the algorithms used today with traditional computing tools provide adequate protection with careful use, new technology is imminent that will completely revolutionise the IT world based on current cryptography; this is the quantum computer. Therefore, it can be assumed that preventing the leakage of data protected by encryption today will be even more important.

How a quantum computer works

The operation and algorithms of a quantum computer are significantly different from those of a traditional computer. The basic operating unit of a classic electronic computer is a two-stage unit. A bit can be used to store both the instructions of the program code and its associated data. A bit can take exactly one value at a time, either 0 or 1, which can be read at any frequency during operation.

---

[26] Franco Piodi and Iolanda Mombelli, *The ECHELON Affair* (Luxembourg: European Parliament, 2014).

[27] Organisations known as the Nine Eyes and Fourteen Eyes were created with the expansion of the Five Eyes, with the same purpose.

The structure of the quantum computer is different, based on some quantum physics phenomenon, so that the behaviour of suitable particles controls its functioning. Its base unit is the quantum bit, or qubit, which has completely different properties from classic bits, not only in the states 0 and 1 but also in between, at which point the qubit is in a superposition. Intermediate forms can describe many options, so a qubit can store many traditional bits of information that rise by the number of qubits on the machine: n quantum bits correspond to 2^n classic bits. According to this analogy, 300 quantum bits could handle more numbers than the amount of atoms existing in the universe.[28]

Several methods are known for the physical implementation of the qubit. In addition to the spin of an electron or nucleus, the polarisation of light, the number of electrons or photons, other quantum physics phenomena can also be used. Understanding the machine's physical structure without quantum mechanical knowledge is hardly possible; it is necessary to imagine a basic physical environment unknown in the macroworld. An elemental particle can be present at the same time at two different points in space. It is also a consequence of the physical nature of quantum phenomena that the computed results are only probabilities in themselves and reading the state of the qubits describing the result means an irreversible change in the state.

The inner workings of a quantum machine are also unusual for a traditional programmer. Even basic operations such as value assignment or initialisation are not trivial, and the content of a variable is lost when the calculated value is read out. This is the operational feature that requires programming of the quantum machine along completely new methods, adding that the execution of its program is not linear, generating all the results in one step. The result calculated by the quantum machine is not always correct, so it is natural to have a sometimes incorrect calculation result – one of the goals of the developments is precisely to reduce the likelihood of errors.

The quantum machine is currently highly sensitive to environmental impacts, so several problems still need to be solved to be universally usable. Due to environmental disturbances, it can be operated around absolute zero degrees, although there are also references to a solution functioning at room temperature.

Based on the above, it can be seen that usable quantum computing is currently in its infantry. IBM, MIT, the University of California and Oxford University built a rudimentary machine as early as 1998, with a processor of hydrogen and chlorine atoms. This was only suitable for a few basic operations as they could not run more serious algorithms on it. In addition to Google, Intel and IBM, Alibaba has already built such machines. Since the number of qubits greatly determines the machine's performance, the power rule doubles each additional qubit, so Google's 72 qubits machine can already carry an enormous capacity. Some sources say it will take much more than that,[29] with the number of qubits needed to hack 2048-bit RSA at 4,096.

Even if quantum machines are only partially used due to their extremely high prices, they will double impact IT systems. Still, the use of these machines is unlikely to replace

---

[28] Charles Q Choi, 'IEEE Spectrum', *IEEE Spectrum*, 21 May 2020.

[29] Aleksey K Fedorov, Evgeniy O Kiktenko and Alexander I Lvovsky, 'Quantum computers put blockchain security at risk', *Nature* 563, no 22 (2018), 465–467.

traditional computers. They should be used in areas that require high computational capacity and can be described with quantum algorithms. No concrete results are currently known, and the expectations are highlighting cryptography in addition to material design, weather modelling and other demanding tasks. The possible use of the quantum computer is mentioned in four key topics in scientific articles. In terms of our topic, the two most important are quantum computing and algorithms and quantum internet. Quantum sensing and metrology is mostly focused on improving the operation of a quantum computer, and quantum simulations are focused on researching high-complexity simulations with a quantum computer.

Quantum computing and Q-algorithms

Quantum computing is perhaps the most researched field. However, in the latter area, there are already results that make it clear that the quantum machine is changing the applicability of traditional cryptographic methods, implementing new foundations for encryption of communication and digital signatures. Therefore, in critical areas, standard encryption procedures need to be reconsidered; otherwise, encrypted information will be hacked by the quantum machine in the foreseeable future. For protection purposes, each affected node's direct connection can be a solution, preventing access to encrypted information by third parties.

However, the most important step is to implement new encryption features or quantum-proof existing ones to be produced on traditional machines and prevent quantum dominance for the future. A vast amount of research is aimed at creating Q-algorithms and mathematically proving their functionality. The practical use of this area is essential not only in cyberspace operations and cyber warfare, but also in the communication of economic and political actors and systems.

The algorithms written on the quantum machine were ahead of their time due to construction difficulties and could not be tested. However, because of the expected environment, those that could be operated immediately when a working machine was available could be developed.[30] The Lov Grover algorithm guarantees a result in an unsettled database under the square root of the number of items instead of the serial search method. From a defensive point of view, one of the most important algorithms is the Shor algorithm, which can also be used to crack a very widely used algorithm of public key encryption, RSA.

The Shor algorithm designed for a quantum machine specifies the prime-factor resolution of an integer that plays a role in several encryption algorithms,[31] which is why

[30] For experimental purposes, D-Wave Systems has developed a 2,000 and then 4,000-qubit quantum machine simulator that is suitable for testing algorithms but cannot actually achieve results.

[31] Peter W Shor, 'Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer', *Society for Industrial and Applied Mathematics* 26, no 5 (1997), 1484–1509.

it focuses on numerical research.[32] Although the problem does not seem particularly difficult at first sight, this is a serious algorithmic difficulty in case of large numbers. RSA Laboratories investigates the number of numbers for which prime resolution can be found, thus breaking encryption, which was the last time a 250-digit number that was successfully found when writing these lines.[33]

The Shor algorithm's primal resolution capability on a quantum computer leads to the breaking of any encryption process that owes its immunity to prime factorisation. But equally vulnerable are the procedures based on discrete logarithm – a quantum algorithm has also been created to solve this problem. The methods that apply them are, therefore, not considered safe in the future. In contrast, for others, security can be retained in the post-quantum age by changing parameters (increasing key length).

The NIST report summarises the quantum computer's impact on the most commonly used methods.[34]

Table 5: Cryptographic algorithms and their impact

Algorithm	Applicability	Security sustainability
AES	Encryption	Stays secure with a larger key
SHA-2, SHA3	Hash	Longer output required
RSA	Digital signature, key negotiation	Unsafe
ECDSA, ECDH	Digital signature, key exchange	Unsafe
DSA	Digital signature, key exchange	Unsafe

Source: Compiled by the author based on Shor, 'Polynomial'.

Quantum computers are primarily a threat to asymmetric encryption protocols, so attackers are expected to attack applications based on them. For protection, some parts of the X509 certificates, IKEv2, TLS, S/MIME and SSH protocols need to be modified. The widely used SSL and TLS protocols will no longer be reliable. This will affect almost all browser-based applications currently in use, even banking applications. Depending on the method used, encrypted media, VPN channels and remote login methods can be compromised with a quantum machine. Loss of SHA security can also compromise blockchain technology to have a serious impact on some cryptocurrencies. The SHA-256 hash algorithm used in the mining of Bitcoin may be at risk. The ability to retroactively change the blockchain guarantees creating a new chain and the loss of the Bitcoin owner's money under certain conditions. RSA's 2048-bit encryption breach is predicted by some sources within 8 hours.[35]

---

[32] Each compound number can be broken down into the product of a few prime numbers (for example, 15 to 5 and 3), this is the prime factor resolution. Prime numbers are numbers that cannot be divided by whole numbers other than 1 and themselves without residue, and it has been proven in ancient times that there are an infinite number of them.

[33] Source: https://lists.gforge.inria.fr/pipermail/cado-nfs-discuss/2020-February/001166.html

[34] Lily Chen et al., *Report on Post-Quantum Cryptography* (Gaithersburg: National Institute of Standards and Technology, 2016).

[35] Steve Jurvetson, 'How a quantum computer could break 2048-bit RSA encryption in 8 hours', *MIT Technology Review,* 30 May 2019.

In addition to extending the currently used algorithms, the development of new Q-algorithms has also begun. The NIST Post Quantum Cryptography Project[36] is investigating a number of new procedures. It currently includes 17 quantum secure algorithms that implement encryption and 9 digital signatures.[37]

Quantum computers are not required for quantum-safe algorithms to work, they can be used on traditional machines and can be developed in two different ways. The simpler procedure is the extension, which makes the current algorithms secure, if possible. The essence of these solutions is most often to increase the key sizes. Because of this, the number of possible permutations increases dramatically, making it an unsolvable task for the quantum machine, as well. This procedure can be successfully applied in the case of AES, but is unsuitable to improve RSA or DSA; therefore, they should be replaced by other procedures in the future.

In order to be able to change these procedures as well, the development of completely new procedures has also begun. Encryption procedures that are also indecipherable for quantum machines are called post-quantum or simply Q-algorithms. The NIST Post Quantum Cryptography Project[38] is exploring a number of new methods that currently include quantum secure algorithms that implement 17 encryptions and 9 digital signatures.[39] Lattice-based cryptography is based on complex math equations, these algorithms are very effective in creating new cryptographic methods, which are not able to break even with a quantum computer. Another effective cryptographic algorithm is the supersingular isogeny key exchange, which uses 2,688-bit long public keys. Ultimately, a quantum computer must also be used to test the new algorithms, so a collaboration between government and business was initiated under the coordination of NIST. The first draft standards are expected to be available by 2022, which will define the basics of defence against post-quantum algorithms.

The practical implementation of the algorithms has also started. The New Hope algorithm aims to replace the TLS algorithm in the world of quantum machines. Google has implemented this under the name Combined Elliptic-Curve and Post-Quantum (CECPQ) in the Canary version of Chrome,[40] although this is currently only available on an experimental basis, but can now be used in some services. DigiCert has developed software used to generate post-quantum cryptographic (PQC) hybrid certificates that includes a quantum-safe algorithm in addition to the traditional cryptographic procedure for backward compatibility.

DigiCert's solution makes one of the biggest difficulties clear: in addition to the very long time it takes to develop, standardise and implement cryptographic protocols, it takes even more time to get out of existing systems, so each of the old elements present in existing systems can be a vulnerability.

---

36 See https://csrc.nist.gov/projects/post-quantum-cryptography
37 See https://csrc.nist.gov/Projects/Post-Quantum-Cryptography/Round-2-Submissions
38 See https://csrc.nist.gov/projects/post-quantum-cryptography
39 See www.google.com/chrome/canary
40 See www.google.com/chrome/canary

Quantum internet

The quantum Internet uses one of the quantum phenomena to transmit information and uses quantum computing algorithms to encrypt it. However, quantum cryptography differs from traditional cryptography not only in the strength of encryption. Because the fact of the measurement itself causes irreversible changes in the quantum process, an attacker could be intercepted as soon as he peeks in the communication process.

The scientific findings of the quantum Internet are also contradictory, stemming from a professional debate between Bohr and Einstein. The operation of the quantum internet is based on the phenomenon of 'spooky action at a distance' created by Einstein. The essence of this is that the changes of the particles in quantum entanglement occur in parallel regardless of the distance between them. The existence of the phenomenon has been proven on several occasions experimentally, but serious professional debates have arisen over the question of whether the speed of communication between two particles in contact can exceed the speed of light. Although the paradigm of Einsteinian physics states that it is impossible, there is nonetheless research that does not rule this out. One U.S. Government report mentions investigating the compliance of black holes with wormholes.[41]

Many countries provide a vast amount of money for the development of quantum computers, as a truly efficient application requires a significantly larger number of qubits than it does today. It is almost impossible to predict the extent of development, but it can be said that Moore's law to increase the number of qubits was not fulfilled. The main difficulty is to minimise the number of errors; a breakthrough has not yet been achieved in this area. The biggest question in technological advances, then, is not whether a quantum computer works, but to what extent it can be scaled. In fact, the answer to this question indicates the danger posed by the proliferation of quantum machines to current informatics.

Conclusions

Cryptographic procedures can essentially ensure communication between modern IT devices, ensuring the confidentiality and integrity of data. In addition to offensive and defensive military equipment, economic and public organisations, and critical infrastructures, procedures are used in accordance with approximately the same principles for the civil sector.

The hacking of encryption procedures and the development of new procedures were typical of all ages. Today, the algorithms used in the civil sphere are also strong enough to be impossible for state cyber organisations to decipher. Some countries use backdoor-based solutions in technical devices or algorithms, while others make it impossible to access network services in other countries. Although there is no mathematical way to decrypt encrypted data, there are a number of solutions that will ultimately ensure that the

[41] Executive Office of the President of the United States, *Quantum Frontiers Report on Community Input to the Nation's Strategy for Quantum Information Science* (Washington: White House National Quantum Coordination Office, 2020), 25.

contents of the encrypted data are known. A well-known solution for this is the application of brute force methods for which the necessary infrastructure is widely available.

Data that gets out of data breaches is often encrypted, so it is essential to decode it, for which, in most cases, brute force methods are obviously used. With a higher-value VGA card and a simple office PC, I proved that a university employee password database could be decrypted with success above 20 per cent. Email and password pairs available on the Darknet may have affected university access by less than 1 per cent.

The principles of quantum computing go back to the 1980s, and over the past forty years, algorithms have been developed that can work on these machines. Since a functioning quantum computer has not been built in recent years, these have remained only theoretical possibilities. However, the emergence of working machines requires analysis, protection, or rethinking of existing algorithms to ensure the security of protection procedures. Cryptographic methods based on factorisation or discrete logarithm have become crackable with the construction of the quantum computer. Since the most commonly used algorithms, RSA and DSA, are based on factorisation, they should be replaced by other procedures in critical applications. As a first step, they should be tested and, if necessary, planned for replacement. It is essential to design controls that guarantee that the introduction of new equipment considers the possibility of the appearance of a working quantum machine. Also, the quantum computer's impact in other possible areas should be assessed, and protective procedures should be set up to respond to the challenge it faces, taking into account the principle of proportionality.

References

Barrett, Daniel J, Richard E Silverman and Robert G Barnes, *SSH, The Secure Shell: The Definitive Guide*. Sebastopol: O'Reilly, 2001.

Bitport, 'A titkosítás tiltása veszélyes', 30 March 2016. Online: https://bitport.hu/a-titkositas-tiltasa-veszelyes

Chen, Lily et al., *Report on Post-Quantum Cryptography*. Gaithersburg: National Institute of Standards and Technology, 2016.

Choi, Charles Q, 'IEEE Spectrum', *IEEE Spectrum*, 21 May 2020. Online: https://spectrum.ieee.org/tech-talk/computing/hardware/qubit-supremacy

Executive Office of the President of the United States, *Quantum Frontiers Report on Community Input to the Nation's Strategy for Quantum Information Science*. Washington: White House National Quantum Coordination Office, 2020, 25.

Fedorov, Aleksey K, Evgeniy O Kiktenko and Alexander I Lvovsky, 'Quantum computers put blockchain security at risk'. *Nature* 563, no 22 (2018), 465–467. Online: https://doi.org/10.1038/d41586-018-07449-z

Forces.net, 'The First Man To Storm A Nazi U-Boat And Seize An Enigma Machine', 06 January 2016. Online: www.forces.net/services/navy/first-man-storm-nazi-u-boat-and-seize-enigma-machine

Huszár, Péter, 'Ukrajna közösségi finanszírozású, katonai célokat szolgáló oktokoptereinek elemzése'. *Hadmérnök* 14, no 2 (2019), 34–43. Online: https://doi.org/10.32567/hm.2019.2.3

Jurvetson, Steve, 'How a quantum computer could break 2048-bit RSA encryption in 8 hours'. *MIT Technology Review*, 30 May 2019. Online: www.technologyreview.com/2019/05/30/65724/how-a-quantum-computer-could-break-2048-bit-rsa-encryption-in-8-hours

Klima, Richard E and Neil P Sigmon, *Cryptology: Classical and Modern.* Chapman and Hall/CRC Press, 2018. Online: https://doi.org/10.1201/9781315170664

Knuth, Donald E, *The Art of Computer Programming.* Boston: Addison-Wesley, 1973.

PA Media, 'UK has mounted covert attacks against Russian leadership, says ex-mandarin'. *The Guardian*, 24 October 2020. Online: www.theguardian.com/technology/2020/oct/24/uk-has-mounted-covert-attacks-against-russian-leadership-says-ex-mandarin

Piodi, Franco and Iolanda Mombelli, *The ECHELON Affair.* Luxembourg: European Parliament, 2014.

Shor, Peter W, 'Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer'. *Society for Industrial and Applied Mathematics* 26, no 5 (1997), 1484–1509. Online: https://doi.org/10.1137/s0097539795293172

Vanhoef, Mathy and Frank Piessens, 'Key Reinstallation Attacks: Forcing Nonce Reuse in WPA2', *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security*, October 2017, 1313–1328. Online: https://doi.org/10.1145/3133956.3134027