The End of Encryption? – The Era of Quantum Computers

Chapter *in* NATO Science for Peace and Security Series C: Environmental Security · September 2022

DOI: 10.1007/978-94-024-2174-3_5

CITATIONS
6

READS
248

2 authors:

Péter Szikora
Obuda University
19 PUBLICATIONS **63** CITATIONS
SEE PROFILE

Kornélia Lazányi
Obuda University
94 PUBLICATIONS **823** CITATIONS
SEE PROFILE

The end of encryption? - the era of quantum computers

Working paper[1]

Péter Szikora[1] and Kornélia Lazányi[1][0000-0002-3841-8846]

[1] Óbuda University, Budapest, 1034, Hungary
szikora.peter@kgk.uni-obuda.hu, lazanyi.kornelia@nik.uni-obuda.hu

1 Introduction

In the 21st century, information technology is an integral part of our lives, and IT tools, which are now considered essential, make it impossible for organisations to operate without computers, networks and applications. According to the report of the KSH [1], the number of organisations using Internet is growing every year. By the end of 2020 their number has reached 93% of all enterprises [2]. Of course, one of the reasons for this development was the Covid-19 epidemic itself, which forced a lot of companies and thus workers and, of course, students and educators to work and study online due to the closure of schools [3][4]. demanding a continuous online presence, whether for work, study. 760 thousand people worked in the form of teleworking [5] and we cannot even estimate the number of those in home office or in blended environments.

The use of IT systems is a great help when it comes to high processes and tasks with high computational needs and real time communication or file-sharing with geographically distant entities. However, the high prevalence of info-communication technologies clearly has its own drawbacks. While according to Benjamin Franklin "Three can keep a secret, if two of them are dead", it is widely accepted that something two people know cannot be considered a secret anymore. Accordingly, the greatest threat to information security is the lack of awareness of its users [6]. In line with this, data, information, and knowledge created, stored and transmitted on ICT devices is a subject to security threats.

IT security is the state of the IT system, in which risks to the confidentiality, integrity and availability of the data processed in the IT system and to the integrity and availability of the system components is managed efficiently [7][8].

Confidentiality is a property of data that refers to the fact that the data can only be accessed, used or disposed of by those who have the right to do so. While integrity is a feature of a data that refers to the fact that the content and properties of the data are the

[1] To be published in Szikora, P., & Lazányi, K. (2022). The End of Encryption?–The Era of Quantum Computers. In Security-Related Advanced Technologies in Critical Infrastructure Protection (pp. 61-72). Springer, Dordrecht.

same as expected, including the certainty that it originates from the expected source (authenticity) and the certainty that the creation has occurred (undeniability) in line with the feature that the component can be used for its intended purpose Availability is the property of the data or the elements of the IT system that they can be used by those entitled to them for the time that is allowed for them.

The protection or security of an IT systems is a state that can be created by protection activities or other means of protection. The tasks to be delivered for IT security contain prevention and early warning, threat detection, early reaction and incident or crisis management [9]. Even though perfect security is nothing but a utopia, each system, and most users strive to protect their data as much as possible, to the extent they are able to. In present paper we will examine some traditional ways of such protection and investigate, whether the emergence of quantum computers is affecting them in a radical way.

2 Machine based identification

The procedures for machine based identification of users can be divided into two main groups: There are traditional personal identification techniques that are used to identify a specific person, such as knowledge-based and possession-based procedures. In addition, biometric methods are also spreading extremely rapidly. In different situations different types of procedures may be more appropriate, hence, the various solutions cannot and should not be ranked. Of course, there are some general aspects - such as the complexity of the program, the price, the certainty of the decision - that one shall consider before deciding on and applying them [10].

Knowledge-based identification can be considered basically free of charge if, no additional tools other than are already in the possession of the user are needed. Whatever we can keep in mind, like a password or a pin code can be used as means of identification. Passwords are far older than ICT itself and have always served as means of identification. Passwords are secret strings used for general user authentication. The mechanism is based on the fact that if only the user knows this confidential data, the owner of the password must be the same as the authorised user [11][12].

Possession-based procedures require specific tools, devices. A separate device for each user and one or more device readers per access points, depending on the expected level of throughput. Tools can range from simple tokens, or physical keys (opening certain spaces), but can also be complex systems, such as digital keys (possibly a badge with chip support, ID card, magnetic stripe, smart card, radio frequency chip), which, if provided as means of identification at the access point, will prove one's right to access premises or data. The big downside is that if lost or stolen, the original owner does not have the entry rights anymore, while the new owner will have the right to access all protected content [13] [14].

Biometric procedures require a device to read the biometric identifiers. Based on Földesi [12], biology-based biometric data can be skin pattern (fingerprint, fingerprint,

fingerprint, palmprint, footprint), hand geometry, vascular network (palm, finger), facial features (2D, 3D, thermal image), eye characteristics (iris, retina) or even DNA [15].

In the case of knowledge and possession-based procedures, the complexity of the program, and therefore the probability of error, is low: the application of the simple search theorem or, in the case of a large number of users, a simple database selection operation is required. However, in the case of biometric methods, the processing of the input biometric feature is a rather complicated procedure, so much so that the values of false positive and false negative frequency (FAR, FRR) have to be consciously considered as indicators of the quality of implementation. All in all, identification with the help of biometric data shall be subjected to cost/benefit analysis, and the final conclusion is heavily influenced not only by the field of application but also the budgetary constraints of the entities involved [16]. The greatest advantage of the biometric systems is that the human involvement is relatively low; and since when it comes to assessing the risk of information security, the human factor plays a leading role [17][18][19].

In line with this, the use of passwords as simple, secure and very cheap authentication procedures could persist for a long time to come, because of it being a mature procedure. However, the role of the human factor is much more prevalent, and hence the innate risk of the identification process is much more imminent. For this very reason it is especially strange that there are still many misconceptions and inaccurate practices related to knowledge-based identification procedures [11].

3 Understanding passwords

While certain elements of our digital life can be easily restored or replaced, since, if a file is lost, it may still be backed up or, failing that, the file may be retrieved, or if the operating system is damaged, or a software fails we may simply reinstall them. Passwords operate on a different logic. Passwords are and can be used independent from their original users. The authentication process does not distinguish between true and fake users. Hence it is of utmost importance to tackle password safety consciously [20].

Password security can be supplemented by multi-factor or multi-step authentication. The purpose of multifactor identification is to uniquely identify the user. Given that the user-password pair is based on one factor, it is expedient to supplement it with multifactor identification, which can be easily obtained (removed, copied) [21]. Multifactor identification is multifaceted. Out of the below listed 3 features the use of two different are required:

- to know something that only we know, (e.g. a PIN code);
- to possess something that only we own, (e.g. a bank card);
- to be who we are (own qualities on the basis of which a person can be clearly identified) [22].

Passwords can be stolen by trying different code lines ("brute force" or in other cases, automated, serious calculations or through experiments, using an artificially created dictionary [23]. Identification tools and devices can be forcefully taken away, but the third group of identifiers are not so easy to manipulate but are relatively costly.

In order to understand, whether we need multifactor identification, or simple password protection is sufficient, we have to look into the security features of different passwords. A password that cannot be easily cracked by brute force is considered secure. However, easy is a relative metric that needs further clarification. The total number of potential character combinations is one of the factors to be assessed – which calls attention to the importance of the human factor that usually gets to determine the length and complexity of a given password. In order to understand the importance of such choices, one needs to understand that the number of potential options for a certain password can be created as the number of different characters (V~ variablity of the characters used) used in a password on the length of a certain password's (L~ length of the password) power: V^L [24][25].

A password can contain characters that are easily accessible on the standard keyboard (uppercase and lowercase letters, numbers, punctuation, and other characters), the number of which is approx. 80. If the password length is 8, the number of character combinations to try is 80^8*10^{15}. This means that a 15-digit number consisting of only ten digits is as strong as an eight-digit password of eighty characters. This refutes the claim that the goodness of a password would be determined by a mixed composition [11].

Increasing the number of optional character sets by a quarter, from 80 to 100, increases the time required to crack the password. If, we stay with the eighty different kinds of characters, but increase the length, also by a quarter, from 8 to 10, then the time required increases even more radically. In line with this, the length of the password is more important than the composition thereof.

Another feature to be considered is the computation capacity available on the hacker's side, since this is strongly related to the number of trials (entry of potential passwords) that can be performed per a unit time. The break rate depends on two factors, the computational requirements of the hash function used to generate the shadow password, and the computational power available.

At the end of 2012, Jeremi Gosney was able to achieve a speed of 348 billion trials per second using NTLM hash using 25 AMD Radeon video cards [26]. Based on this, the crack rate is assumed to be at least 1012 trials/second (with safety error). If the operator would have used the Bcrypt hash function (but as a user we cannot be sure), then this speed would have been approximately 72,000 trials per second

The following table shows the data of cracking passwords of different length and composition.

password length	8	10	8
variety of characters	80	80	100

possibilities	10^{15}	10^{19}	10^{16}
time to crack	28 minutes	124 days	2.78 hours

Table 1. data of cracking passwords of different length and composition

Of course, as we increase the length - as indicated in the above table as well - we can get a password that is really hard to be broken with current machines. For example, if we increase the length of our password to 12 characters, it will take more than 2,000 years for such a machine to decrypt our password, and for 15 characters, it will take more than 1 billion years. Hence, a well-chosen password can provide optimal security against the password-breaking resources of today's generic machines.

4 Encryption

While necessarily long and complex passwords may provide a certain security, they are far from enough we do not only wish to access data or physical spaces, but also wish to communicate in a safe and secure way. As indicated in the previous chapter, passwords (keys) ensure that only those in possession of the key can access the content protected by it [27]. Using this method in communication is labelled symmetric or single-key encryption, where the message sent can only be read with the same key used to encrypt it. But what happens, if this content is a message, and its intended receiver is someone who does not own the key prior to the transaction.

The easy way out is to first send a key and then the message. However, this lapse in time will not provide security for the communication, since communication channels can be monitored, and keys retrieved by third parties [28]. This would mean, that even the longest password is superfluous. Hence, there is a need for a different kind of approach.

In asymmetric encryption methodologies each participant has two different keys. One of the keys is called a public key and is distributed as widely as possible. The other key is the private or secret key, which is kept secret by its owner in the most secure way possible. The essence of the operation is that what is encrypted with one of the keys can be decrypted with its pair [24]. The biggest advantage of this method is that there is no need for a secure channel for pre-exchanging keys, since public keys are widely accessible and can be known to everyone. If there is a need to send a secured message from the SENDER to the RECEIVER, the public key of the RECEIVER will be used for encryption, because it can only be decrypted with the RECEIVER's secret key, which is owned, and supposedly securely stored by the RECEIVER. In order to have an efficient communication the public keys must be verified before use to see if they really belong to the entity, they announce themselves to [29].

The system, however, also has one deficiency - it can be deciphered logically without keys, and this cracking requires nothing more than determining the prime factors of a number. If that number is large enough, making a prime resolution is close to impossible, especially with traditional computers [30]. However, nothing is impossible, while there is no complete security. At present the most powerful (traditional)computer in the

world is the IBM Summit built by IBM Corporation. Summit is the world's fastest supercomputer, with tens of thousands of processors that take a space equalling to two football fields. This supercomputer is capable of performing more than 1017 operations per second, hence it would be able to crack the previously introduced passwords and encryptions much faster than any other device, so in a sense, it may not be called or regarded a traditional computer anymore. Regardless, it is a fact that it still works on classical principles and its humongous capacity is owing to its sheer size.

5 Quantum computers

Quantum computers are computing devices that perform calculations based on quantum mechanical phenomena. A quantum computer may be able to perform calculations efficiently that would be practically unsolvable with traditional digital computers or could take years or decades to solve. [31]

Just as in classical (or traditional) informatics, the binary bit is the basic unit of information, the quantum bit (or qubit) is the basic unit of information in quantum informatics. Quantum bits can be represented as superpositions of several possible states. The quantum bits take advantage of the quantum mechanical phenomenon of superpositioning to assume a linear combination of two states [32] [33]. A classical binary bit can represent only a single binary value, such as 0 or 1, so it can only be in one of two possible states. However, a quantum bit can represent 0, 1, or a superposition of any ratio of states 0 to 1 with a certain probability of 0 and a certain probability of 1. Superposition provides greater computational capacity for quantum computers. Thanks to superpositioning, quantum algorithms are able to process information in a fraction of the time the fastest traditional systems would/could solve certain problems [34].

The amount of information that can be represented by quantum bit systems is growing exponentially. Information that can be easily represented in 500 quantum bits could not be presented in 2^500 classic bits. A classic computer could calculate the prime factors of a 2048-bit number in just millions of years. With quantum bits, this calculation can be done in minutes [35]. With the development of quantum technologies, we can get closer and closer to solving some of the most difficult problems in the world. The D-Wave Advantage annealer is a quantum computer of the Jülich Supercomputer Center (JSC) and D-Wave Systems that is operating since September 2020. The system operates in Jülich, Germany, and has a capacity of 5,000 qubits, which allows it to handle one million variables [36] at the same time which is a computing capacity that European researchers hope to achieve serious scientific results with.

This new paradigm holds enormous potential, but quantum informatics is still in its infancy. While classical computers are based on the well-known silicon-based chips, quantum bits, also called "quantum computer qubits," can be made of trapped ions, photons, artificial or natural atoms, or quasi-particles. Depending on the architecture and the applied quantum bit system, for some implementations, the quantum bits must be kept at a temperature close to absolute zero.

For the time being, the implementation of quantum computers is in the initial stages of an experimental phase. It seems that there is still a long way to go before they could become widespread. The main reason for this is that quantum computers need to be operated under specific conditions. For example, the systems operate completely closed to light, in a vacuum, at temperatures colder than space, and their management can also be quite a problem.

One of the most significant inhibitors of quantum informatics is the vulnerability of quantum bits. The entanglement of a quantum bit system with its environment, including the measuring equipment, can easily disrupt the system and lead to a loss of coherence. With this in mind, quantum computer hardware and debugging methods are currently being developed. The topological quantum bits are shielded from noise due to the topological characteristics of the quasi-particles, making this hardware more resistant to error. Thanks to this increased stability, the quantum computer can achieve dimensions suitable for longer and more complex calculations, bringing more complex solutions within reach.

2017	google	20 qubit
2019	google	53 qubit
2019	IBM	53 qubit
2020	USTC (China)	76 qubit
2021	IBM	127 qubit
2011	D-Wave (Canada)	128 qubit
2013	D-Wave (Canada)	512 qubit
2015	D-Wave (Canada)	1152 qubit
2017	D-Wave (Canada)	2048 qubit
2020	D-Wave (Canada)	5760 qubit

Table 2. Circuit-based and Annealing quantum processors

By the end of 2021, quantum computers are still rare. There are only few that operate on a circuit-base logic, and other 5 that contain annealin quantum processors. Since the cost and time of their development is extreme, and their operation is also difficult – owing to the special circumstances they necessitate – we cannot expect a rapid increase in hteir numbers in the comping 5 years. However, from 2030 they may become the norm for organisations with high computing neccesities.

It is interesting to note, that even though the first quantum processor has been built in 2017, various Quantum Computing Algorithms have been developed starting from the year 1992 [37].

Year	**Name**	**Type**
1992	Deutsch–Jozsa Algorithm	Based on Quantum Fourier Transform
1992	Bernstein–Vazirani Algorithm[	
1994	Simon's Algorithm	
1994	Shor's Algorithm	
1996	Grover's Algorithm	Based on AmplitudeAmplification
1998	Quantum Counting	
2014	Quantum Approximate Optimization Algorithm	Hybrid quantum/classicalalgorithm

Table 3. Quantum algorithms and their mathematical backgrounds

What is more, we are in the anteroom of a new technology, where it is not size that does matter anymore, but technology is the key to increasing computational capabilities.

C	QuEST, CHP, Eqcs
C++	Staq, Qrack, Quantum++, QMDD, Open Qubit, qsims, Q++, SimQubit
C, C++	libquantum (C)/ (C++)
CaML	Q-gol
Haskell	Qchas
Java Bloch	Sphere
Javascript	Quantum Programming Studio, BackupBrain, Quantum Circuit, Jsquis
Julia	QSWalk.jl, QuantumOptics.jl, QuantumWalk,jl
LanQ	LanQ
.Net	QuIDE, Quantum.NET
Maple	Feynman, OpenQUACS, Quantavo
Mathematica	Linear AI, QDENSITY, Quantum, QuantumUtils,Qi
MATLAB	Quantencomputer, Drqubit, Qubit4Matlab, M-fun
Maxima	Qinf
OCaML	QOCS
Protobuf	Quantum User
Python	Cirq, ProjectQ, QCircuits, Qiskit
Python, Q#	Quantum Development
QASM	OpenQasm
Qio +	Haskell QIO
Quantum	Code QX Simulator
Rust & OpenCL	QCGPU
Scaffold	Scaffold/ScaffCC

Table 4. Quantum languages and their basic programming languages

6 Quantum apocalypse

Nowadays, - especially because of Covid 19 - we do everything online, shopping, banking or communication with peers via social media. In order to protect the content and the individuals involved in these processes, these transactions are encrypted. But when a quantum computer starts operating, it allows its developer to empty anyone’s bank account or shut down a state’s defence systems in a matter of minutes.

As already presented in the previous chapter, quantum computers can perform operations that traditional computers would need an eternity for in minutes. They are specifically created to solve computation intensive problems. One such application is cryptography, namely the encryption and decryption of data. The advent of quantum computers is making the currently used encryption methods obsolete. Brute force is not a vocabulary than can be used in connection to them. Quantum computers will cause a serious upheaval - what experts call a "quantum apocalypse", since methodologies used on/for traditional computers will no longer be able to provide safety.

Quantum cryptography is a fundamental challenge classic cryptography, since quantum computers can easily break most standard mathematical cryptography problems, such as factoring and discrete logarithms [38][39][40] by using quantum mechanics' physics. Hence, the question arises, if traditional cryptography can no longer prevail, how will be able to maintain integrity and confidentiality while preventing different kinds of attacks in the era of quantum computers. Fortunately -even though the era of quantum computers is still far away, cryptography research is already searching for potential solutions. Ideas, such as symmetric key quantum resistance, multivariate cryptography and lattice-based cryptography, supersingular elliptic curve isogeny cryptography, code-based cryptography, hash-based cryptography, are being tested [41]. Quantum Key Distribution (QKD) for example with tis unlimited quantum key length is an example that has already been tested theoretically. But cryptography is not the only issue to be solved. The distribution of the keys is also a problem to be tackled [42]. while Mastriani [43] recommends the use of Quantum Drones (QD) and Quantum Satellites (QS) as means of sharing keys, Conrad and his colleagues [44] have focused their attention on how to create secure multimedia communications.

All in all, while it is obvious that quantum computing will be the end of traditional cryptography, it is also clear, that the challenges of security will not be solved, but only shifted to a more complex, novel field of mathematics.

7 Summary

Although quantum computers represent the future rather than the present for the public; in many countries, both the state and large research institutes are already working on developing them. In recent years, they have not only reached the computing capacity of supercomputers, but they have also overtaken their computational capacities spectacularly. At current such systems are extremely vulnerable to environmental effects, and their reliability is also volatile, but if the weaknesses of quantum computers can be eradicated and their reliability can be improved, the encryptions that have been used will soon be obsolate.

References

1. KSH Távközlés, televízió- és internetszolgáltatás – IKT-eszközök és használatuk a háztartásokban, a vállalkozásoknál és a közigazgatásban. https://www.ksh.hu/docs/hun/xftp/idoszaki/ikt/ikt17.pdf (2017):
2. KSH A háztartások információs- és kommunikációseszköz-használatának főbb jellemzői ,https://www.ksh.hu/docs/hun/xftp/idoszaki/ikt/2020/01/index.html (2020)
3. Katona F., Ágoston Z. Vírusfertőzés az online térben – a Covid hatása a virtuális piacra In: Garai-Fodor, Mónika; Varga, János; Csiszárik-Kocsir, Ágnes (szerk.) Vállalkozásfejlesztés a XXI. században 2021/2. kötet : Gazdasági kihívások és a megoldások keresése napjaink kritikus változásaira Budapest, Magyarország : Óbudai Egyetem Keleti Károly Gazdasági Kar pp. 79-91. (2021)

4. Lazânyi, K., Vincze, A. and Szikora, P., The Digital Skills In The Hungarian Higher Education During The First Wave of Covid-19. Higher Education Policies for Developing Digital Skills to Respond to the Covid-19 Crisis: European and Global Perspectives, pp.4-18. (2021)
5. KSH A háztartások információ- és kommunikációseszközök-használatának főbb jellemzői. (2021)
6. Szűcs, E., & Záhonyi, L. Információbiztonság fejlődés-történeti vizsgálata–Mérföldkövek, események és válaszok. Biztonságtudományi Szemle, 3(3), 81-91. (2021)
7. Muha, L. Az informatikai biztonság egy lehetséges rendszertana. BOLYAI SZEMLE 17:(4) pp. 137-156. (2008).
8. Nyikes, Z., Kovács T. A., Tokody D.: In situ testing of rail damages in accordance with Industry 4.0. Journal of Physics-Conference Series (1742-6588 1742-6596) 1045, 1-6 (2018). doi :10.1088/1742-6596/1045/1/012032
9. Wang, B., Wu, C.: Safety informatics as a new, promising and sustainable area of safety science in the information age. Journal of Cleaner Production, 252, 119852,1-13 (2020).
10. Rana, T. A., Cheah, Y. N., & Rana, T. Multi-level knowledge-based approach for implicit aspect identification. Applied Intelligence, 50(12), 4616-4630. (2020)
11. Keszthelyi, A.L.,. Jelszavakról-iparági legrosszabb gyakorlatok= Passwords-worst practices in user authentication. Taylor, 7(3-4), pp.261-268. (2015)
12. Balázs Á., Nyikes Z., Kovács T. A.: Building Protection with Composite Materials Application. Key Engineering Materials (1013-9826 1662-9795): 755, 286-291 (2017). https://doi.org/10.4028/www.scientific.net/KEM.755.286
13. Földesi, K.,. Paradigmaváltás a biztonságtechnikában – miért alkalmazzunk biometrikus rendszert?. Magyar Rendészet, 15(3), pp.37-48. (2015)
14. Nyikes, Z.: Digital competence and the safety awareness base on the assessments results of the Middle East-European generations. Procedia Manufacturing (2351-9789): 22, 916-922 (2018). https://doi.org/10.1016/j.promfg.2018.03.130
15. Chang, Y. C. The Many Faces of Adverse Possession: Economic and Empirical Analyses of Laws in 156 Jurisdictions. Available at SSRN 3558800. (2020).
16. O'Gorman, L. Comparing passwords, tokens, and biometrics for user authentication. Proceedings of the IEEE, 91(12), 2021-2040. (2003)
17. FEHÉR-POLGÁR Pál Felsőoktatásban tanuló hallgatók biztonságtudatossága. TAYLOR Gazdálkodás- és szervezéstudományi folyóirat, Szeged, 2015/3-4. szám pp. 15-17. (2015):
18. Jain, A. K., Ross, A., & Pankanti, S. Biometrics: a tool for information security. IEEE transactions on information forensics and security, 1(2), 125-143. (2006).
19. Nyikes, Z.: Contemporary Digital Competency Review. Interdisciplinary Description of Complex Systems (1334-4684 1334-4676): 16 1, 124-131 (2018). http://doi.org/10.7906/indecs.16.1.9
20. Tan, J., Bauer, L., Christin, N., & Cranor, L. F. Practical recommendations for stronger, more usable passwords combining minimum-strength, minimum-length, and blocklist requirements. In Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Securi-ty pp. 1407-1426 (2020)
21. KÁDÁR Sándor: Többfaktoros azonosítás. 2017.04.22. https://nws.niif.hu/ncd2007/docs/phu/109.pdf (2007)
22. OLÁH Gábor Többlépcsős azonosítás amit mindenkinek használnia kell(ene). Golnet Informatika. https://golnet.hu/blog/biztonsag/tobblepcsos-azonositas-amit-mindenkinek-hasznalnia-kellene/ (2019)
23. KÖDMÖN József Jelszómenedzser szoftver alkalmazása az egészségügyben. 2016. 157. évfolyam, 52. szám. Orvosi Hetilap. Akadémia Kiadó. Debrecen. pp. 2066-2073. (2016):

24. Stallings, W.: Cryptography and Network Security Principles and Practice, 5th ed., Prentice Hall Press, Upper Saddle River, NJ, USA, (2010)
25. Nyikes, Z.: Creation Proposal for the Digital Competency Framework of the Middle-East European Region. Key Engineering Materials (1013-9826 1662-9795): 755, 106-111 (2017). https://doi.org/10.4028/www.scientific.net/KEM.755.106
26. Gosney, J.. Password cracking HPC. In Passwords12 conference pp. 6-34. (2012)
27. Lozupone, V.. Analyze encryption and public key infrastructure (PKI). International Journal of Information Management, 38(1), 42-44. (2018)
28. Lamport, L. Password authentication with insecure communication. Communications of the ACM, 24(11), 770-772. (1981).
29. Qu, H., Yan, Z., Lin, X. J., Zhang, Q., & Sun, L. Certificateless public key encryption with equality test. Information Sciences, 462, 76-92. (2018)
30. Schnorr, C. P,. Factoring Integers by CVP and SVP Algorithms. (2017)
31. Maslov, D., Kim, J. S., Bravyi, S., Yoder, T. J., & Sheldon, S. Quantum advantage for computations with limited space. Nature Physics, 17(8), 894-897. (2021)
32. Ladd, T. D., Jelezko, F., Laflamme, R., Nakamura, Y., Monroe, C., & O'Brien, J. L. Quantum computers. Nature, 464(7285), 45-53. (2010).
33. Nyikes, Z.: Information Security Issues of RFID. In: Szakál, A. (ed.) SAMI 2016 : IEEE 14th International Symposium on Applied Machine Intelligence and Informatics 2016, pp. 111-114. IEEE, New York (2016). ISBN: 9781467387392
34. DiVincenzo, D. P., & Loss, D. Quantum computers and quantum coherence. Journal of Magnetism and Magnetic Materials, 200(1-3), 202-218. (1999).
35. Valiev, K. A. Quantum computers and quantum computations. Physics-Uspekhi, 48(1), 1. (2005)
36. McGeoch, C., & Farré, P. The D-wave advantage system: An overview. D-Wave Systems Inc., Burnaby, BC, Canada, Tech. Rep. (2020)
37. Gill, S. S., Kumar, A., Singh, H., Singh, M., Kaur, K., Usman, M., & Buyya, R. (2022). Quantum computing: A taxonomy, systematic review and future directions. *Software: Practice and Experience*, *52*(1), 66-114.
38. Abura'ed, Nour, Faisal Shah Khan, and Harish Bhaskar. "Advances in the quantum theoretical approach to image processing applications." ACM Computing Surveys (CSUR) 49, no. 4 (2017): 1-49.
39. Rieffel, Eleanor, and Wolfgang Polak. "An introduction to quantum computing for non-physicists." ACM Computing Surveys (CSUR) 32, no. 3 (2000): 300-335.
40. Nejatollahi, Hamid, Nikil Dutt, Sandip Ray, Francesco Regazzoni, Indranil Banerjee, and Rosario Cammarota. "Postquantum lattice-based cryptography implementations: A survey." ACM Computing Surveys 51, no. 6 (2019): 1-41.
41. Ott, David, and Christopher Peikert. "Identifying Research Challenges in Post Quantum Cryptography Migration and Cryptographic Agility." arXiv:1909.07353 (2019).
42. Tsai, C.W., Yang, C.W., Lin, J., Chang, Y.C. and Chang, R.S., 2021. Quantum Key Distribution Networks: Challenges and Future Research Issues in Security. Applied Sciences, 11(9), p.3767.
43. Mastriani, M., Iyengar, S.S. and Kumar, L., 2021. Satellite quantum communication protocol regardless of the weather. Optical and Quantum Electronics, 53(4), pp.1-14.
44. Conrad, A., Hill, A., Chaffee, D., Herndon, K., Wilens, B., Sanchez-Rosales, D., Gauthier, D. and Kwiat, P., 2019, May. Drone-based Quantum Key Distribution. In APS Division of Atomic, Molecular and Optical Physics Meeting Abstracts (Vol. 2019, pp. P08-003).