Advanced Data Security and Privacy Ensuring Methods in 5G Era

Maksim Iavich[1], Dinara Ospanova[2], Ketevan Grdzelidze[3], Rashit Brzhanov[4], and Yuliia Polishchuk[5]

[1] Caucasus University, 1 P. Saakadze str., Tbilisi, 0102, Georgia
[2] Kazakh Humanitarian Juridical Innovative University, 11 Mengilik str., Semey, 070000, Kazakhstan
[3] Scientific Cyber Security Association, 26 Otar Lortkipanidze str., Tbilisi, 0114, Georgia
[4] Yessenov University, 32 Microdistrict, Aktau, 130000, Kazakhstan
[5] National Aviation University, 1 Liubomyr Huzar ave., Kyiv, 03058, Ukraine

Abstract

The announcement about introduction and launch of 5G internet has sparked great discussion and turmoil all over the world not only, among scientists, but among general population as well. With the digitalization of the network functions and implementation thereof within the virtual machines, the new security threats are posed to the users, as well as other parties involved. In addition, the further development of quantum math and introduction of quantum computers, it is clear, the currently safe algorithms will become easily breakable in the nearest future. The presented paper analyzes the cryptographic algorithms of the 5G networks and outlines possible attacks thereof. It is offered the idea of converting the mentioned algorithms to 5G epoch for data security and privacy ensuring.

Keywords

5G, Cryptography, cyber security, cryptography, post-quantum cryptography, quantum cryptography, RSA, Diffie-Hellmann, safety, attack, cyberattack, algorithm

1. Introduction

The announcement about introduction and launch of 5G internet has sparked great discussion and turmoil all over the world not only, among scientists, but among general population as well. Aside the stereotypical widespread fears with regard to 5G, one of the main concerns within the scientific society remains the security of the internet in 5G era and consequent integrity and authenticity of the data transferred throughout.

The present paper discusses major security concerns with regard to the 5G systems, consequent possible solutions and issues of applicability and availability thereof. Contrary to its previous systems, 5G has moved most of the traffic to cloud architectures and „network functions are no longer provided by dedicated hardware devices or components, but are implemented in software and run inside virtual machines [1]. Consequently, with the rise of IoT (Fig. 1) and more digitalization of the world, the security issues can arise at any end of the processes, included but not limited to: vendors, users, service providers, merchandizers, etc. The present paper will attempt to discuss the challenges in communication between the users and the integrity of transferred data within the network.

2. Virtualization of the Processes

In August, 2018, the 3rd Generation Partnership Program (3GPP) has released information about security within 5G [2]. In the aforesaid documentation various security enhancements were outlined, compared to 4G. Considering, that 3GPP itself is a platform based on cooperation, the relevant working groups were involved in development of requirements and standards for 5G network [3]. In the initial

CPITS-II-2021: Cybersecurity Providing in Information and Telecommunication Systems, October 26, 2021, Kyiv, Ukraine
EMAIL: miavich@cu.edu.ge (M. Iavich); ospanova@gmail.com (D. Ospanova); grdzelidze@gmail.com (K. Grdzelidze); brzhanov@mail.ru (R. Brzhanov); polischuk.yu.ya@gmail.com (Y. Polishchuk)
ORCID: 0000-0002-3109-7971 (M. Iavich); 0000-0002-2206-7367 (D. Ospanova); 0000-0003-2354-8787 (K. Grdzelidze); 0000-0001-8755-8207 (R. Brzhanov); 0000-0002-0686-2328 (Y. Polishchuk)

release, the improvement of security features, protocols and algorithms were provided. While implementing and adopting 5G network over the world, the importance of quantum computers and quantum cryptography, as well as, postquantum cryptography has become more evident.

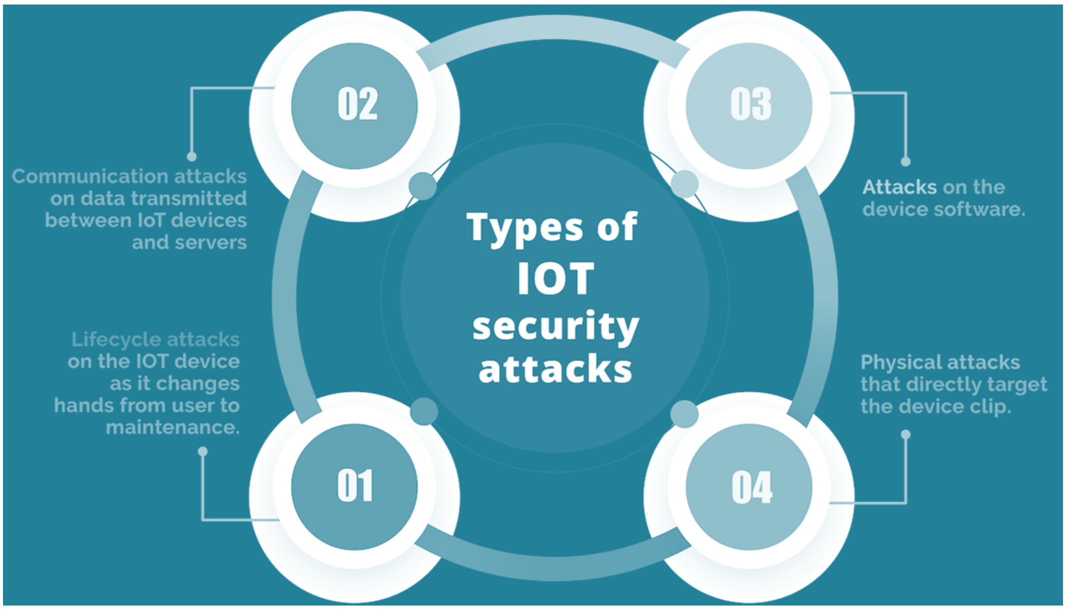

Types of IOT security attacks
02
03
01
04
Communication attacks on data transmitted between IoT devices and servers
Attacks on the device software.
Lifecycle attacks on the IOT device as it changes hands from user to maintenance.
Physical attacks that directly target the device clip.

Figure 1: IoT security issues

As stated above, within the 5G environment, most of the communication between users, service providers and other involved parties, have mainly been moved to virtual environment and, consequently, the importance and role of hardware has decreased. This does not mean, that hardware has been removed from the processes overall, merely that the main computing is carried out via software and/or within virtual machines. The update of the hardware and security issues thereof, has proven as a challenge up until now for service providers, as well as for vendors themselves. Consequently, despite the fact, that the security patches are frequently released and the users are informed of corresponding threats, the update of hardware and the network connected thereof has always been difficult due to its' high cost. In this new era of internet and cellular communication, the so-called virtualization of the processes will vastly reduce the cost of updates and therefore, will provide more secure environment for communication.

At the same time, there is a lot of skepticism related to this matter. The software, as well as virtual machines, are not immune to faults and failure. The more the technologies and corresponding security features are developed, the more sophisticated the hackers become. Therefore, despite the fact, that virtualized environment is able to disseminate the information about security related shortcomings as soon as they become available, the update and finding of appropriate solution takes time and the level of threat remain high.

Yet it is important to note, that the virtualization of the network functions poses wide scale of challenges and the configuration of the systems, need to be carried out with great attention. Security related functions related to Software Defined Networking include, but of course are not limited to: traffic analysis modules, firewalls, intrusion detection and prevention systems, Deep Packet Inspection systems, programmable and relocatable network probes for detection of modern sophisticated intrusions [4]. With this regard, properly configured and secure encryption of authorization, as well as further encryption of processes plays a vital role. Each part of the network, each function, each slice has to be protected with the level of security according to the sensitivity of the data it entails. With sophistication of cybersecurity protocols and measures, the virtualization of processes also requires higher speed for mobile networks and the algorithms, shall be able to run fast in software, otherwise RAN (Radio Access Network) can't happen and service providers would lose the benefits of using commercial of the shelf hardware in the cloud platform [5].

It is noteworthy, that today's digital vendors and communications market is very diverse. Despite the sophisticated security features in 5G network, the threat posed by dishonest or malicious manufacturers/vendors, remain a great threat. Especially considering that they mostly produce relatively cheap products and are able to cover larger portion of market. But this is not the main issue covered by the present paper, thus we will not discuss the matter any further.

3. Slicing of Network

Slicing of network was first introduced within 4G, but the new generation provides more sophisticated and highly developed features and role of slicing. In the processes, where the main part of communication processes is virtualized and software based, the division of the processes, both physical and logical, can play great role in ensuring the security and safety of users and transmitted data. With this in mind, within 5G network architecture, the division is also made between control plane and user plane. Running the slices of the network separately enables more advanced security of each slice, avoids overlap and/or leakage of information from one part to another. The division of the control plane and user plane, together with virtualization of the processes, enables to the parties involved to increase the data usage, change the storage, update processes on one end, without affecting the other. It also offers various degrees of security features, according to the slice the specific communication is being implemented [6].

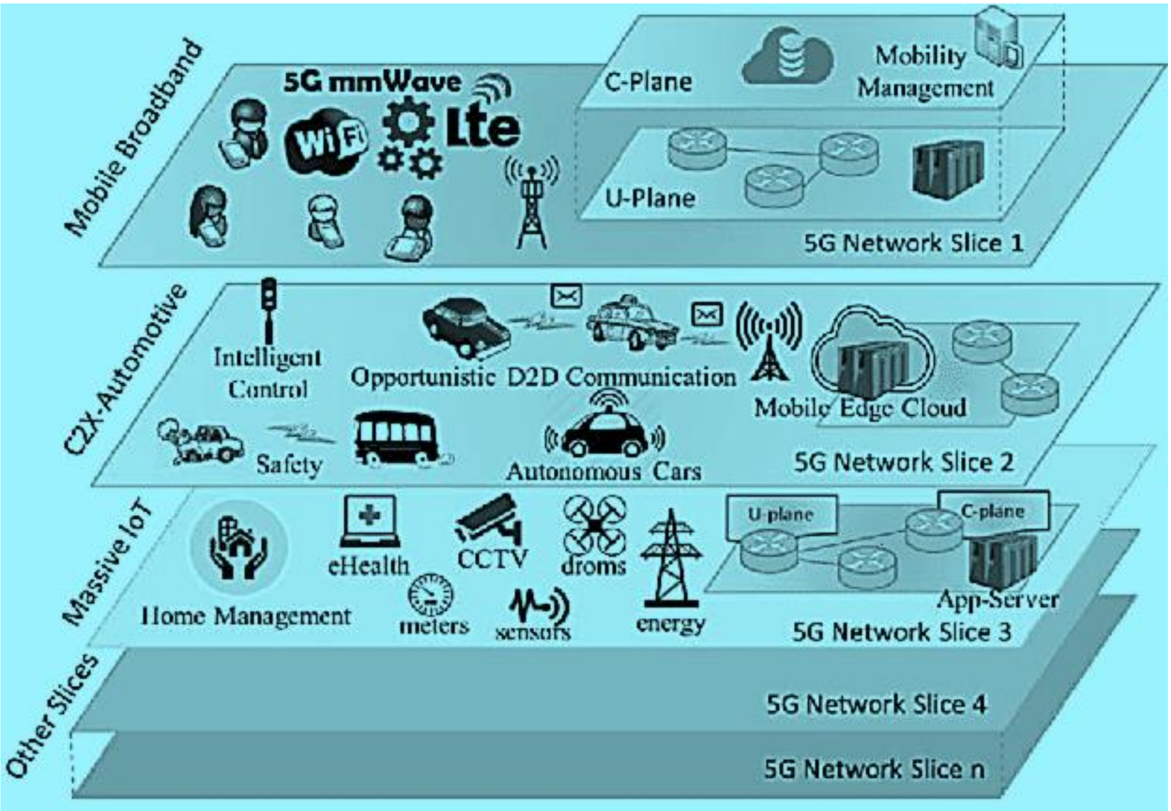


Figure 2: 5G network slices structure [7]

Fig. 2 provides information about the types of communications and users, which will be sharing the slices of the network among each other and where each type of communication will take part. It is important to note, that in addition to physical and logical segregation, traffic and resource isolation are also critical. Traffic isolation can be provided by creating specific virtual lanes to serve specific traffic types that can be routed through a specific logical/physical lane pair. Resource isolation should be supported in the underlying infrastructure [8].

4. Authentication in 5G

As stated above, as well as its'seen in Fig. 2, the 5G network includes various types of devices, users, service provides in its' communication processes. The protocol and level of encryption varies according to the type of communication, slice and device itself. The processes are also divided for primary and secondary authentication.

In 5G Phase 1 there are two mandatory authentication options: 5G Authentication and Key Agreement (5G-AKA) and Extensible Authentication Protocol (EAP)-AKA', i.e. EAP-AKA'. Optionally, other EAP based authentication mechanisms are also allowed in 5G - for specific cases such as private networks [9].

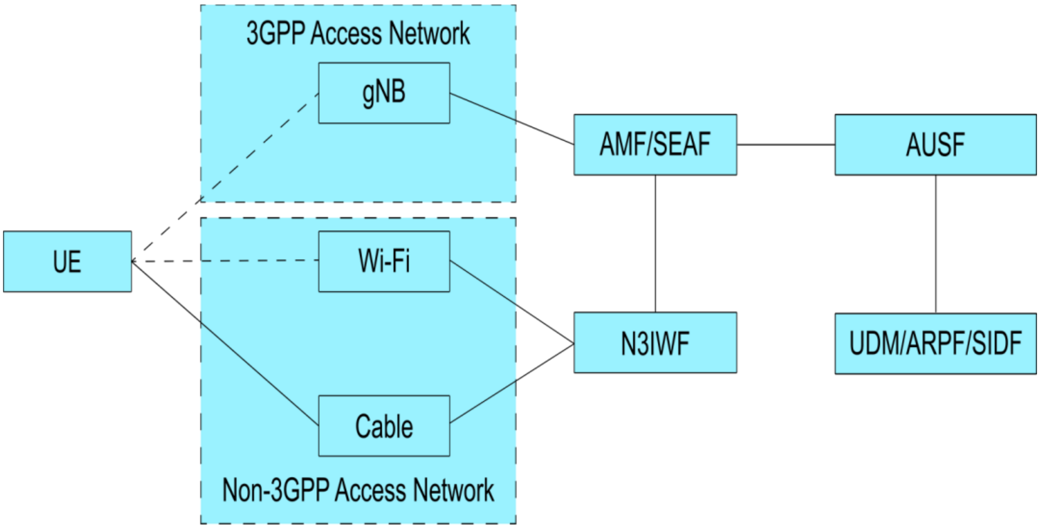


Figure 3: 5G Authentication Framework

In the Release 17 of 3GPP the issue of authentication for users, as well as for other parties involved, and possible types of attacks was addressed and corresponding recommendations were provided for [10]. The network communication can be attacked at various stages, including linkability attack, DDos attack, Man-in-the-middle attacks, also an attack during Device-To-Device (D2D) communication and so on.

In the latest *(as of March 18, 2021)* technical report published within Release 17 by 3GPP, it was outlined, that it is possible for attackers to intercept the communication at the stage of Authentication and Key Agreement. The attack mainly depends on the generation of International Mobile Subscriber Identifier (IMSI) and Subscription Permanent Identifier (SUPI).

The attacker is able to pose as a station resulting in the identity request. This on its' part will require the user to send the identity response, which can enable the attacker to change the location of the station, modify the registration request and forwarding the modified request to the network. This type of attack can be used solely for the purpose of attacking one specific user or types of users, but its' goal can be to direct the traffic to certain location. The attacker will also be able to gather large number of users through this, giving him/her the ability to carry out planned DDos attack on the slice, where the users are communicating [11]. The proper implementation of authentication protocol and encryption of the primary authentication can play a great role in avoiding the attack and protection of the communication.

Service-based architecture (SBA) has been proposed for the 5G core network. Accordingly, new entities and new service requests have also been defined in 5G. Some of the new entities relevant to 5G authentication are listed below.

- The Security Anchor Function (SEAF) is in a serving network and is a "middleman" during the authentication process between a UE and its home network. It can reject an authentication from the UE, but it relies on the UE's home network to accept the authentication.
- The Authentication Server Function (AUSF) is in a home network and performs authentication with a UE. It makes the decision on UE authentication, but it relies on

backend service for computing the authentication data and keying materials when 5G-AKA or EAP-AKA’ is used.

- Unified data management (UDM) is an entity that hosts functions related to data management, such as the Authentication Credential Repository and Processing Function (ARPF), which selects an authentication method based on subscriber identity and configured policy and computes the authentication data and keying materials for the AUSF if needed.
- The Subscription Identifier De-concealing Function (SIDF) decrypts a Subscription Concealed Identifier (SUCI) to obtain its long-term identity, namely the Subscription Permanent Identifier (SUPI), e.g., the IMSI. In 5G, a subscriber long-term identity is always transmitted over the radio interfaces in an encrypted form. More specifically, a public key-based encryption is used to protect the SUPI. Therefore, only the SIDF has access to the private key associated with a public key distributed to UEs for encrypting their SUPIs.

A unified authentication framework has been defined to make 5G authentication both open (e.g., with the support of EAP) and access-network agnostic (e.g., supporting both 3GGP access networks and non-3GPP access networks such as Wi-Fi and cable networks) (see Fig. 3).

When EAP (Extensible Authentication Protocol) is used (e.g., EAP-AKA’ or EAP-TLS), EAP authentication is between the UE (an EAP peer) and the AUSF (an EAP server) through the SEAF (functioning as an EAP pass-through authenticator) [23].

When authentication is over untrusted, non-3GPP access networks, a new entity, namely the Non-3GPP Interworking Function (N3IWF), is required to function as a VPN server to allow the UE to access the 5G core over untrusted, non-3GPP networks through IPsec (IP Security) tunnels.

Several security contexts can be established with one authentication execution, allowing the UE to move from a 3GPP access network to a non-3GPP network without having to be reauthenticated.

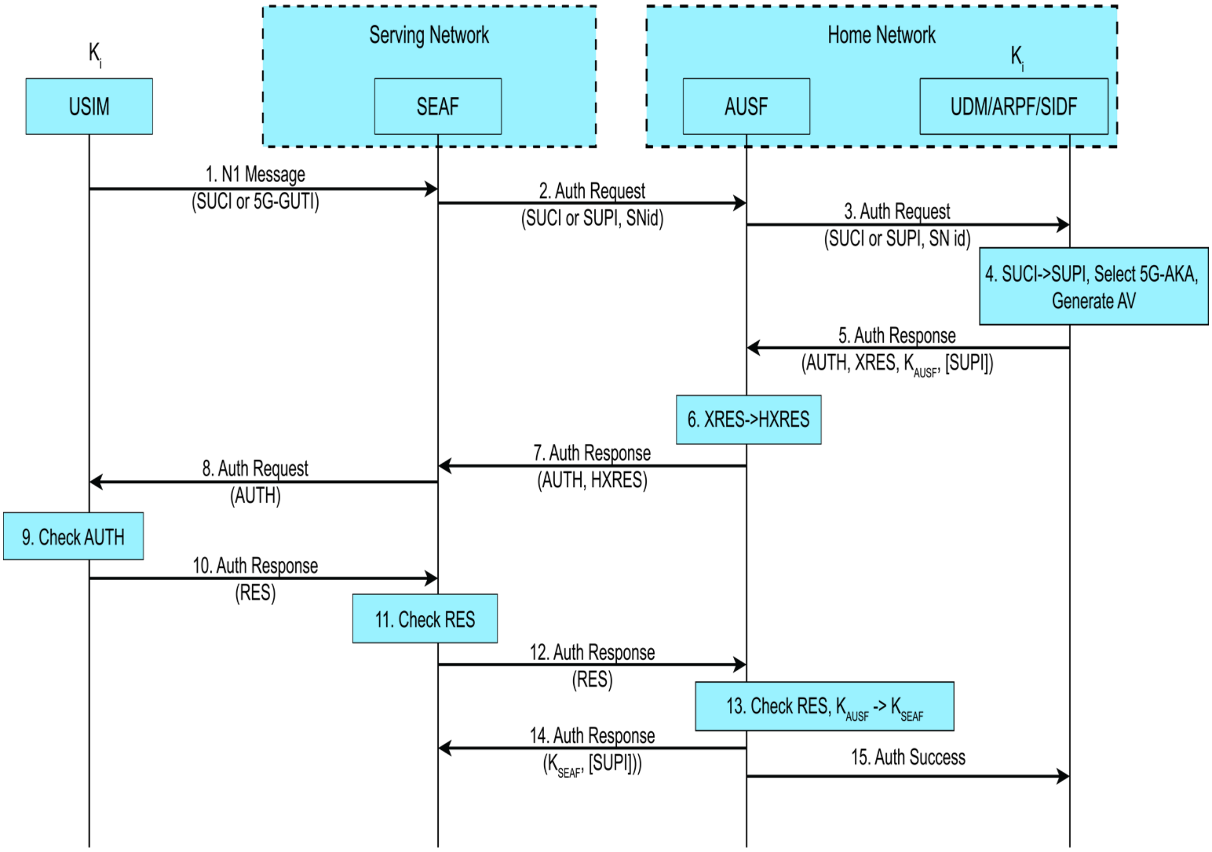
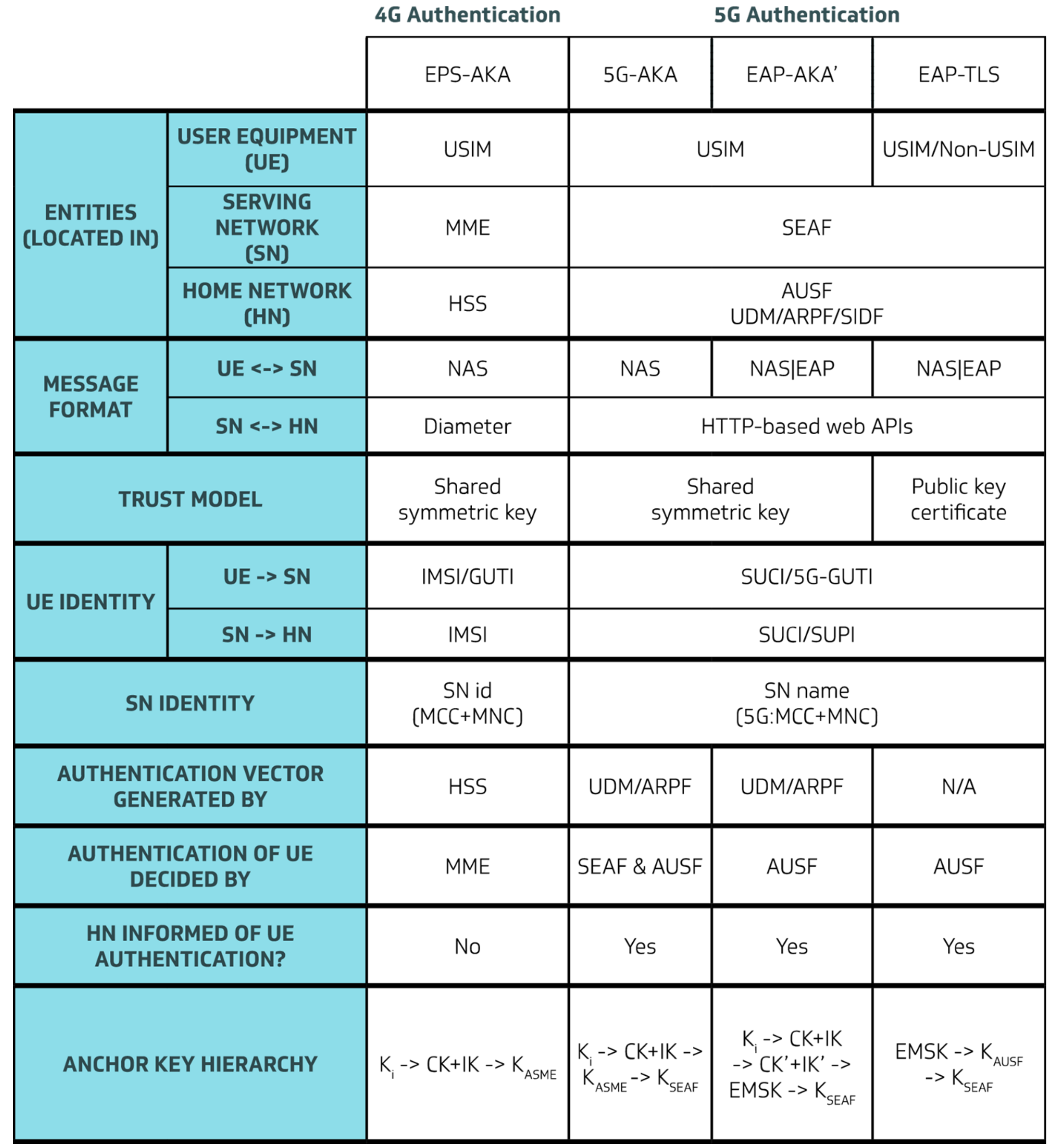


Figure 4: 5G-AKA Authentication Procedure

5G defines new authentication-related services. For example, the AUSF provides authentication service through Nausf_UEAuthentication, and UDM provides its authentication service through Nudm_UEAuthentication. For simplicity, generic messages such as Authentication Request and

Authentication Response are used in Fig. 4 without referring to the actual authentication service names. Further, an authentication vector includes a set of data, but only a subset is shown in Fig. 4.

In 5G-AKA (Fig. 4), the SEAF may start the authentication procedure after receiving any signaling message from the UE. Note that the UE should send the SEAF a temporary identifier (a 5G-GUTI) or an encrypted permanent identifier (a SUCI) if a 5G-GUTI has not been allocated by the serving network for the UE. The SUCI is the encrypted form of the SUPI using the public key of the home network. Thus, a UE's permanent identifier, e.g., the IMSI, is never sent in clear text over the radio networks in 5G. This feature is considered a major security improvement over prior generations such as 4G.



		4G Authentication	5G Authentication		
		EPS-AKA	5G-AKA	EAP-AKA'	EAP-TLS
ENTITIES (LOCATED IN)	USER EQUIPMENT (UE)	USIM	USIM		USIM/Non-USIM
	SERVING NETWORK (SN)	MME	SEAF		
	HOME NETWORK (HN)	HSS	AUSF UDM/ARPF/SIDF		
MESSAGE FORMAT	UE <-> SN	NAS	NAS	NAS|EAP	NAS|EAP
	SN <-> HN	Diameter	HTTP-based web APIs		
TRUST MODEL		Shared symmetric key	Shared symmetric key		Public key certificate
UE IDENTITY	UE -> SN	IMSI/GUTI	SUCI/5G-GUTI		
	SN -> HN	IMSI	SUCI/SUPI		
SN IDENTITY		SN id (MCC+MNC)	SN name (5G:MCC+MNC)		
AUTHENTICATION VECTOR GENERATED BY		HSS	UDM/ARPF	UDM/ARPF	N/A
AUTHENTICATION OF UE DECIDED BY		MME	SEAF & AUSF	AUSF	AUSF
HN INFORMED OF UE AUTHENTICATION?		No	Yes	Yes	Yes
ANCHOR KEY HIERARCHY		K_i -> CK+IK -> K_{ASME}	K_i -> CK+IK -> K_{ASME} -> K_{SEAF}	K_i -> CK+IK -> CK'+IK' -> EMSK -> K_{SEAF}	EMSK -> K_{AUSF} -> K_{SEAF}

Figure 5: 4G and 5G authentication comparison

The SEAF starts authentication by sending an authentication request to the AUSF, which first verifies that the serving network requesting the authentication service is authorized. Upon success, the AUSF sends an authentication request to UDM/ARPF. If a SUCI is provided by the AUSF, then the SIDF will be invoked to decrypt the SUCI to obtain the SUPI, which is further used to select the authentication method configured for the subscriber. In this case, it is 5G-AKA, which is selected and to be executed.

UDM/ARPF starts 5G-AKA by sending the authentication response to the AUSF with an authentication vector consisting of an AUTH token, an XRES token, the key KAUSF, and the SUPI if applicable (e.g., when a SUCI is included in the corresponding authentication request), among other data [23,24].

5G-AKA differs from 4G EPS-AKA in primarily the following areas:

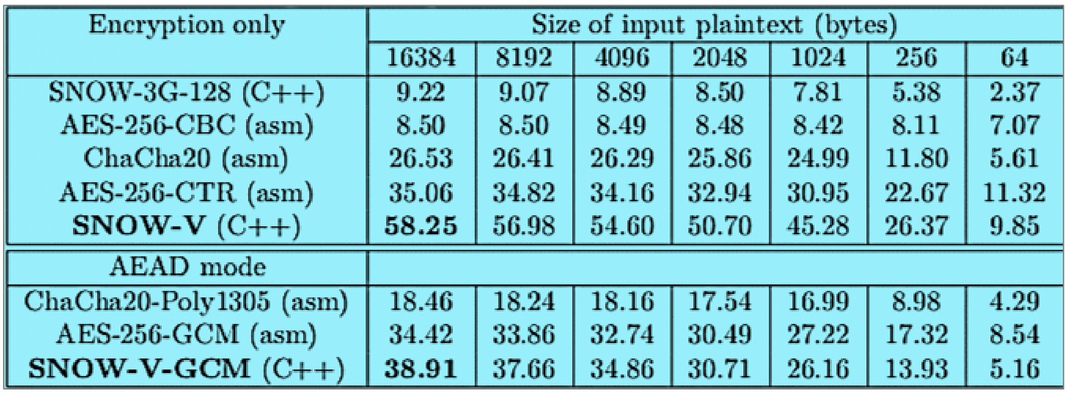
- Entities involved in the authentication are different because of the new service-based architecture in 5G. Particularly, the SIDF is new; it does not exist in 4G.
- The UE always uses the public key of the home network to encrypt the UE permanent identity before it is sent to a 5G network. In 4G, the UE always sends its permanent identifier in clear text to the network, allowing it to be stolen by either a malicious network (e.g., a faked base station) or a passive adversary over the radio links (if communication over radio links is not protected).
- The home network (e.g., the AUSF) makes the final decision on UE authentication in 5G. In addition, results of UE authentication are also sent to UDM to be logged. In 4G, a home network is consulted during authentication only to generate authentication vectors; it does not make decisions on the authentication results.
- Key hierarchy is longer in 5G than in 4G because 5G introduces two intermediate keys, KAUSF and KAMF. Note: KSEAF is the anchor key in 5G, equivalent to KASME in 4G.

4G and 5G authentication comparison is presented on Fig. 5.

5. Cryptography in 5G

5G mainly depends on the already existing cryptographic algorithms, some of which are at this point considered secure and have not yet been hacked. Such algorithms include: RSA, EDH and SNOW-V, proposed by Ericsson. Unlike 4G, 5G uses 256-bit encryption, which substantially increases the security of the algorithms already in use.

Ephemeral Diffie-Hellman cannot be used for primary authentication, because the key changes regularly. Yet, within the already established and authenticated parties, it can provide strong protection from attacks. Static Diffie-Hellman, if implemented correctly, still remains secure. EDH, providing the possibility of forward secrecy, is considered as the strongest key encryption within Diffie-Hellman algorithms. EDH differs from static Diffie-Hellman through its' regular update of encryption keys. The regular change of the keys means, that each part of the communication is encrypted differently. In this regard it is essential, that in case throughout the time one set of keys is hacked or part of the communication is decrypted, the forward secrecy ensures that the parts encrypted with different keys remain secure. Consequently, the hacking of previous communication does not affect the security of the later one and does not allow the attacker to gain any further information about the parties involved.



Encryption only	Size of input plaintext (bytes)						
	16384	8192	4096	2048	1024	256	64
SNOW-3G-128 (C++)	9.22	9.07	8.89	8.50	7.81	5.38	2.37
AES-256-CBC (asm)	8.50	8.50	8.49	8.48	8.42	8.11	7.07
ChaCha20 (asm)	26.53	26.41	26.29	25.86	24.99	11.80	5.61
AES-256-CTR (asm)	35.06	34.82	34.16	32.94	30.95	22.67	11.32
SNOW-V (C++)	**58.25**	56.98	54.60	50.70	45.28	26.37	9.85
AEAD mode							
ChaCha20-Poly1305 (asm)	18.46	18.24	18.16	17.54	16.99	8.98	4.29
AES-256-GCM (asm)	34.42	33.86	32.74	30.49	27.22	17.32	8.54
SNOW-V-GCM (C++)	**38.91**	37.66	34.86	30.71	26.16	13.93	5.16

Figure 6: Performance comparison of SNOW-V-(GCM) and best OpenSSL's algorithms. Performance values are given in Gbps [14]

Ephemeral Diffie-Hellman – This is considered the most secure implementation because it provides perfect forward secrecy. It is generally combined with an algorithm such as DSA or RSA to authenticate one or both of the parties in the connection [12].

RSA is a public key encryption algorithm, that at this point, has not yet been hacked. Since RSA uses a public key, it is mainly used for authentication purposes. Similar to EDH, if configured correctly, RSA remains secure and with today's development of technology, it has not yet been hacked. Consequently, 5G using both of the protocols, has built far more secure system for communication.

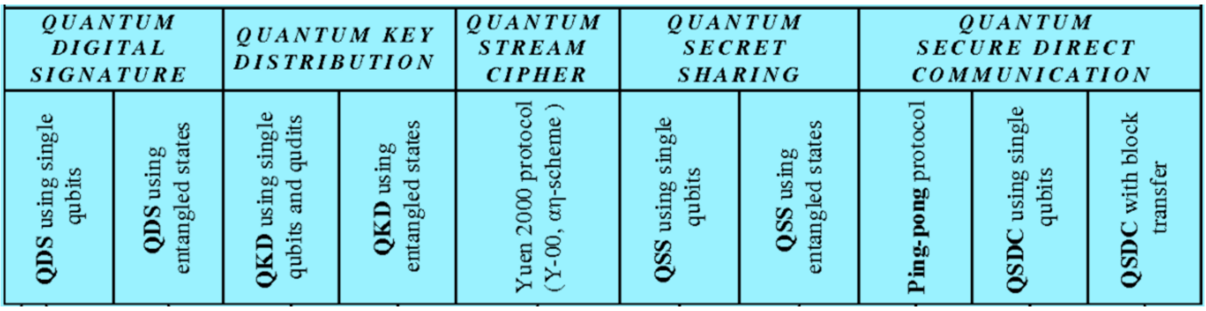
While tackling the diversity of the processes, with corresponding different levels of security, at the same time addressing the matter of the speed, the adoption of new version of already existing SNOW 3G algorithm was proposed. SNOW-V reuses the best design principles of SNOW 3G, but is extremely well suited for software implementation using vectorized instructions and also leverages hardware accelerated CPU instructions for AES Encryption available in all modern CPUs [13]. The speed as well as the security of the SNOW-V has become the reason, for it to gain further acceptance. Further research has proven, that SNOW-V outperforms most of known algorithms in speed (See Fig. 6), but it also is immune to most of the known hacker attacks as of today. As a result of this information, SNOW-V will be responsible for ensuring speed and integrity of the communication.

6. Quantum and Post-Quantum Cryptography

Several times already we have mentioned, that the algorithms mainly used within 5G are immune to currently known types of attacks and have not yet been broken. This does not mean, that the status quo will remain the same.

The high level of sophistication of the modern cybersecurity does not ensure the comprehensive and life-long safety from hackers, as the more enhanced the security features are, the more developed the hackings become. Even in case the hackers will not be able to decrypt the algorithms used in 5G or any other system, the rise of quantum computers poses a great threat to cybersecurity systems all over the world.

It is predicted, that the quantum computers will be able to decrypt RSA and EDH by 2030 [14, 15]. Yet, the quantum systems are highly costly products and therefore, are not accessible to anyone who simply wishes to acquire it. Yet, with the development and advancement of technology, like anything else, the prices will drop down in the coming years. Therefore, they will become more affordable. This has raised serious concerns with regard to network and cyber security overall. In certain parts of the world the attempts of developing quantum computing is actively carried out [16]. This on its' part has caused the scientists and researchers to work on post-quantum cryptography, which shall ensure the security in the new era, dominated by quantum computers. For example, Verizon, as one of the service providers, has launched its' trials with regards to quantum key distribution (QKD) [17, 18]. Among quantum technologies (Fig. 7) there are various security directions [25-27].



QUANTUM DIGITAL SIGNATURE		QUANTUM KEY DISTRIBUTION		QUANTUM STREAM CIPHER	QUANTUM SECRET SHARING		QUANTUM SECURE DIRECT COMMUNICATION		
QDS using single qubits	**QDS** using entangled states	**QKD** using single qubits and qudits	**QKD** using entangled states	Yuen 2000 protocol (Y-00, αη-scheme)	**QSS** using single qubits	**QSS** using entangled states	**Ping-pong** protocol	**QSDC** using single qubits	**QSDC** with block transfer

Figure 7: Quantum technologies of information security

Despite the early stages of trials and testing of the new technologies, it is clear, that the level of security provided by quantum cryptography and mathematics, as a basis thereof, is unparalleled in todays' world [18-20]. We offer to integrate lattice based cryptography instead of existing asymmetric cryptography schemes. We offer to use NTRU as it was selected as a finalist in the NIST PQC standardization competition [21-22, 28-30].

7. Conclusion

5G network offers the wide range of opportunities, possibilities and higher speed of communication, at the same time providing higher level of security and safety to its' users. The slicing and visualization of the network allow for service providers to localize the attack, to swiftly solve the problems. At the same time, the rise of quantum computers and development of quantum cryptography, while providing large amount of security, also poses great threats in long term. Unless the whole cybersecurity system will shift towards post-quantum cryptography, the threat posed not only to the data transferred through the network, but by the level of control that can be gained over the devices, can prove to be fatal. As discussed above, the cryptographic algorithms, that are considered safe as of today, will be easily decryptable through quantum computers within the upcoming years. Considering the speed of development of smart technologies, AI, machine learning systems, increasing level of distribution of IoT and the amount of dependability on technology by humans, it is impossible to imagine the amount of damage that can be caused by crumbling security system.

While deploying the 5G network, the configuration and proper usage of the cybersecurity protocols will play a vital role. At the same time, the virtualization and division of the network will allow for creation of malware, attack and/or malfunction detection software, which can play great role in securitization of the network. At the same time, the quantum cryptography will remain as a major solution for ensuring the greater security and its' development shall be the main topic on the agenda of security-driven entities. As 5G security scheme includes asymmetrical cryptography schemes and by means of this, it will be vulnerable to the attacks of quantum computers, it is offered to integrate lattice-based cryptography.

8. References

[1] G. Bianchi, "5G Security." 5G Italy White Book: from Research to Market, November 2018, https://www.5gitaly.eu/2018/wp-content/uploads/2019/04/5G-Italy-White-eBook.pdf.

[2] A.R. Prasad, M. C. Soveri, A. Escott, and A. Zugenmaier, "5GPP 5G Security." 3GPP 5G Security. 3GPP, August 6, 2018. https://www.3gpp.org/news-events/1975-sec_5g

[3] About 3GPP Home, 3GPP, accessed April 15, 2021, https://www.3gpp.org/about-3gpp/about-3gpp.

[4] Bessalov A., Sokolov V. Skladannyi P., Zhyltsov O. Computing of odd degree isogenies on supersingular twisted Edwards curves. Proceedings of the Workshop on Cybersecurity Providing in Information and Telecommunication Systems, Jan. 28, 2021 vol. 2923, pp. 1-11.

[5] P. Ekdahl and A. Maximov, "Encryption in Virtualized 5G Environments." Ericsson. June 2, 2020. https://www.ericsson.com/en/blog/2020/6/encryption-in-virtualized-5g-environments.

[6] 5G Americas. "Security Considerations for the 5G Era 2020." 5G Americas, July 2020. https://doi.org/[Online]. p. 8.

[7] K. Samdanis, X. Costa-Perez, and V. Sciancalepore, "From Network Sharing to Multi-Tenancy: The 5G Network Slice Broker." IEEE Communications Magazine 54, no. 7 (2016): 32–39.p.38 https://doi.org/10.1109/mcom.2016.7514161.

[8] A. Kuznetsov, O. Smirnov, D. Kovalchuk et al, "Formation of Pseudorandom Sequences with Special Correlation Properties," 2019 3rd International Conference on Advanced Information and Communications Technologies (AICT), 2019, pp. 395-399.

[9] A.R. Prasad, M. C. Soveri, A. Escott, and A. Zugenmaier, "5GPP 5G Security." 3GPP 5G Security. 3GPP, August 6, 2018. https://www.3gpp.org/news-events/1975-sec_5g.

[10] "3GPP TR 33.846, V0.11.0 Technichal Report." TDoc S3-211287. 3GPP, March 18, 2021. https://portal.3gpp.org/ngppapp/CreateTdoc.aspx?mode=view&contributionUid=S3-211287

[11] "Security architecture and procedures for 5G System", 3GPP TS 33.501, V17.1.0, (3GPP, April 6, 2021), https://www.3gpp.org/ftp/Specs/archive/33_series/33.501/p.10

[12] J. Lake, "What Is the Diffie–Hellman Key Exchange and How Does It Work?" Comparitech, March 23, 2021. https://www.comparitech.com/blog/information-security/diffie-hellman-key-exchange/.

[13] A. Bessalov, et al., “Analysis of 2-isogeny properties of generalized form Edwards curves”, in: Proceedings of the Workshop on Cybersecurity Providing in Information and Telecommunication Systems, July 7, 2020, vol. 2746, pp. 1-13.

[14] A. Bessalov, V. Sokolov, P. Skladannyi, “Modeling of 3- and 5-isogenies of supersingular Edwards curves”, in: Proceedings of the 2nd International Workshop on Modern Machine Learning Technologies and Data Science, June 2–3, 2020, no. I, vol. 2631, pp. 30–39.

[15] T.C Clancy, R. W. McGwier, and L. Chen, “Post-Quantum Cryptography and 5G Security.” Proceedings of the 12th Conference on Security and Privacy in Wireless and Mobile Networks, 2019. https://doi.org/10.1145/3317549.3324882.

[16] “Quantum-Safe Security in a 5G World.” QuantumXC. Quantumxc, July 15, 2019. https://quantumxc.com/quantum-safe-security-in-a-5g-world/.

[17] S. Gnatyuk, T. Okhrimenko, M. Iavich and R. Berdibayev, “Intruder Control Mode Simulation of Deterministic Quantum Cryptography Protocol for Depolarized Quantum Channel”, Proc. of 2019 Intern. Scien.-Pract. Conf. on the Problems of Infocommunications. Science and Technology, pp. 825-828, October 08-11, 2019.

[18] T.C Clancy, R. W. McGwier, and L. Chen, “Post-Quantum Cryptography and 5G Security.” Proceedings of the 12th Conference on Security and Privacy in Wireless and Mobile Networks, 2019. https://doi.org/10.1145/3317549.3324882.

[19] J.L Hardcastle, “Verizon Boosts 5G Security, Deploys Quantum Key Distribution” Sdxcentral. September 3, 2020. https://www.sdxcentral.com/articles/news/verizon-boosts-5g-security-deploys-quantum-key-distribution/2020/09/.

[20] M. Iavich, A. Gagnidze, G. Iashvili, S. Gnatyuk, V. Vialkova: Lattice based Merkle. CEUR Workshop Proceedings, vol. 2470, pp. 13–16 (2019)

[21] A.G. Gagnidze, M.P. Iavich, G.U. Iashvili: Analysis of post quantum cryptography use in practice. Bull. Georgian Natl. Acad. Sci. 11(2), 29–36 (2017)

[22] Hermans, F. Vercauteren, B. Preneel (2010) Speed Records for NTRU. In: Pieprzyk J. (eds) Topics in Cryptology - CT-RSA 2010. CT-RSA 2010. Lecture Notes in Computer Science, vol 5985. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-642-11925-5_6

[23] Altaf Shaik, Ravishankar Borgaonkar, N. Asokan, Valtteri Niemi, and Jean-Pierre Seifert, “Practical Attacks Against Privacy and Availability in 4G/LTE Mobile Communication Systems,” Proceedings of the Internet Society Symposium on Network and Distributed System Security (NDSS) (Feburary 2016).

[24] David Basin, Jannik Dreier, Lucca Hirschi, Saša Radomirovic, Ralf Sasse, and Vincent Stettler, “A Formal Analysis of 5G Authentication,” Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security (CCS '18) (October 2018).

[25] Korchenko O., Vasiliu Y., Gnatyuk S. “Modern quantum technologies of information security against cyber-terrorist attacks”, Aviation, Vol. 14, №3, pp. 58-69, 2010.

[26] Z. Hu, S. Gnatyuk, T. Okhrimenko, V. Kinzeryavyy, M. Iavich, Kh. Yubuzova, “High-Speed Privacy Amplification Method for Deterministic Quantum Cryptography Protocols Using Pairs of Entangled Qutrits”, CEUR Workshop Proceedings, Vol. 2393, pp. 810-821, 2019.

[27] Gnatyuk S., Okhrimenko T., Azarenko O., Fesenko A., Berdibayev R. “Experimental Study of Secure PRNG for Q-trits Quantum Cryptography Protocols”, Proceedings of the 2020 IEEE 11th International Conference on Dependable Systems, Services and Technologies (DESSERT 2020), Kyiv, Ukraine, May 14, 2020, pp. 183-188.

[28] Labadze G., Iavich M., Iashvili G., Gagnidze A., Gnatyuk S. “Post-quantum digital signature scheme with BB84 protocol”, CEUR Workshop Proceedings, Vol. 2915, pp. 35-44, 2021.

[29] Iavich M., Kuchukhidze T., Gnatyuk S., Fesenko A. “Novel certification method for quantum random number generators”, International Journal of Computer Network and Information Security, Volume 13, Issue 3, pp. 28-38, 2021.

[30] Iavich M., Gnatyuk S., Arakelian A., Iashvili G., Polishchuk Y., Prysiazhnyy D., “Improved Post-quantum Merkle Algorithm Based on Threads”, Advances in Intelligent Systems and Computing, Vol. 1247 AISC, pp. 454-464, 2021.