Regulation of quantum communications in the "smart city" information system

A.V. Minbaleev[1,*], and *K.S.* Evsikov[1,2]

[1]Kutafin Moscow State Law University (MSAL), Moscow, Russia
[2]Tula State University, Tula, Russia

Abstract. Different countries are creating and improving information systems that increase the efficiency of city management. Their research takes place within the concept of a smart city. The article considers the formation of this concept in the Russian Federation and its evolution abroad. Information systems "smart city" involve the transfer of a significant amount of data, protected by the methods of classical cryptography, through communication lines. The level of development of quantum technologies allowed us to conclude that this method of information security will not be effective in the medium term. Smart city systems have already lost their cryptographic strength for retrospective attacks. The article analyzes data protection options for information system smart city under quantum threat conditions. Based on the classification of city services, the authors propose a differentiated approach to information security, combining post-quantum cryptography and quantum communication technologies. This will allow the optimal use of public resources and create a smart city information system resistant to quantum computer attacks. We completed this article within the Governmental Assignment: "Russian Legal System in the Realities of Digital Transformation of Society and State: Adaptation and Prospects for Responding to Modern Challenges and Threats (FSMW-2023-0006)". Registration number: 1022040700002-6-5.5.1.

1 Introduction

The information society puts new demands on public authorities for the provision of public services and the organization of the system of management of public relations. The authorities, to meet the demand, create various information technologies that are combined into public information systems and digital platforms, such as the smart city. They are used to improve living standards, quality of services, and management efficiency. The large amount of data collected makes this technology work. It allows decisions to be made with fewer unknowns.

The operators of the smart city system must prioritize information security among its many automated processes. Its solution requires consideration of quantum threat. New types of computing systems (quantum computers) will allow to achieve progress in different branches of science. One of them will solve mathematical problems, on which the current

[*] Corresponding author: alexmin@bk.ru

system of information security with a public key is based. The authors analyze options for the transition of smart city information systems to quantum-secure encryption technologies.

2 Research methodology

The authors used the universal dialectical method of knowledge.

1. The authors collected empirical material on the topics of smart city, quantum threat, and quantum communication.

2. The researchers systematized the empirical material, which allowed them to highlight the primary and secondary problems in the research topic.

3. Analysis of risks and threats to smart city systems in the second quantum revolution allowed planning proposals for their prevention in the long and medium term.

Using a method of modeling, the authors proposed the concept of information security of smart city systems based on quantum communication technologies.

3 Research results: a smart city

3.1. Smart city information system in the World

The educational portal National Geographic notes that people in cities have been dealing with the same problems for over 6,000 years: sanitation, crime, traffic congestion, taxes, maintenance of public facilities, and emergency services [1]. Universal digital technologies can help to automate the management process. For example, it is possible to improve the provision and quality of urban services by monitoring residents and infrastructure with rapid analysis of data on the deviation from the set parameters. This is ensured by introducing "Internet of Things (IoT)" technologies.

It is important to note that as of January 2023, there are 5.16 billion Internet users worldwide, representing 64.4 percent of the world's population. This means that not all countries and cities can base this technology on the Internet. It is possible to do so on a local, urban information and communication network that is not connected to the global network. This example allows us to talk about the high adaptability of digital technology to the peculiarities of a particular object of digitalization.

The concept of a "smart city" has been constantly changing in foreign literature.

1. In 2000-2005, the concept included the term "ubiquitous city" (U-City) (from the Latin ubiquitarius - existing or being everywhere). U-City is a concept of solving urban problems in any place using information technology.

2. In 2006-2010, the term Smart City appears. The authors explained the difference because U-City only uses digital technology to solve urban problems, while smart cities will solve the problems of residents. This process in South Korea led to the legislative adoption of the term "smart city services".

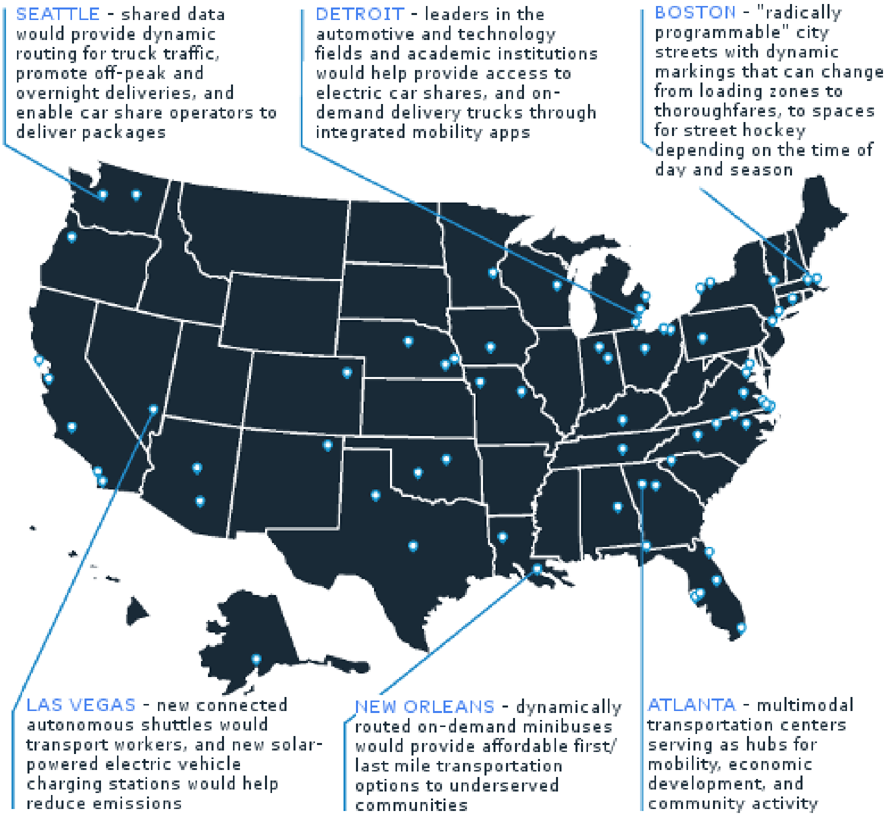
3. In 2011-2015, the concepts of smart city services take shape. This included experimental legal regimes in a particular area or for a particular type of service.

4. In 2016-2020, comprehensive development of the information system "smart city", focused on solving urban problems, begins. The U.S. Smart City Project has identified urban problems that have moved from department store-style services to practical services that citizens need.

5. After 2020, a new term "flexible and efficient smart city" appears. Smart city services respond to emerging urban threats under this concept and combine existing services. The concept of the flexible and efficient smart city maximizes efficiency by providing flexible services that can easily be added or removed as needed. An example of a flexible service is

COVID-19 infection control. These services included systems to track the movement of patients, which helped localize the spread of disease.

Representatives of different sciences (anthropology, information technology, sociology, law, and others) are studying smart city technology because it solves a huge list of problems. The results have led to the growing popularity of Smart Cities projects around the world [2]. Many states are studying the successful experience of digital transformation of city management to multiply it throughout their territory. For example, the U.S. held a competition "Smart City Challenge", 78 cities in America shared problems and ideas to solve them as part of the fifth information revolution. The most successful proposals were supported by the U.S. Department of Transportation (Figure 1), which in its report presented recommendations for improving the transport infrastructure in cities [3].



SEATTLE - shared data would provide dynamic routing for truck traffic, promote off-peak and overnight deliveries, and enable car share operators to deliver packages

DETROIT - leaders in the automotive and technology fields and academic institutions would help provide access to electric car shares, and on-demand delivery trucks through integrated mobility apps

BOSTON - "radically programmable" city streets with dynamic markings that can change from loading zones to thoroughfares, to spaces for street hockey depending on the time of day and season

LAS VEGAS - new connected autonomous shuttles would transport workers, and new solar-powered electric vehicle charging stations would help reduce emissions

NEW ORLEANS - dynamically routed on-demand minibuses would provide affordable first/last mile transportation options to underserved communities

ATLANTA - multimodal transportation centers serving as hubs for mobility, economic development, and community activity

Fig 1. Projects are the winners of the Smart City Challenge.

Analysts have found that, in most cases, a smart city is created by installing a variety of sensors to collect data about people and infrastructure in many countries around the world. Residents and city services get access to information from these sensors, which allows them to quickly and comfortably navigate in the urban environment, receiving or providing public services. Foreign authors note that the proliferation of sensors and monitoring systems of information about the population poses a threat of breach of confidentiality of data [4]. Therefore, all countries call for the highest possible level of information security of this digital technology.

3.2. Smart City information system in Russia

Russia has been implementing smart city projects since 2013. It included the accumulated experience in the unified data bank in 2018, it initially included 94 projects from 202 cities [5]. By March 2023, 134 normative legal acts of the Russian Federation had mentioned the term "smart city". The authorities adopted the concept of the project of digitalization of the urban economy "Smart City" under paragraph 1.1 of section 3 of the passport of the departmental project of digitalization of the urban economy "Smart City" [6]. The purpose of the concept:

- formulate the basic principles and goals of projects for implementing smart city technologies;
- unify the key concepts, terms, and definitions used for a unified description language;
- describe the architecture of smart cities - the basic organization of elements of a smart city, their relationships with each other and with the environment;
- identify and describe the key directions of development of smart cities;
- identify and describe the main approaches and mechanisms to ensure sustainable urban development.

Russia is at the beginning of the digitalization path. For introducing many urban services, it is necessary to engage in building the infrastructure of smart cities - sensors and the modernization of communication networks. The concept is focused on stimulating changes in any ecosystem of human activity, primarily at the level of Russian municipalities. We can only solve many urban management issues at the level of the subjects (regions) of the Russian Federation. Entities usually put in place urban data management systems, unify data storage methods, compare different solutions, and copy the most successful practices. The goals, principles, objectives, and approaches of the Concept are recommended for municipalities and for the development of the subjects of the Russian Federation.

According to the concept, a smart city is an approach to city development that uses digital tools to improve living standards, quality of services, and management efficiency while meeting the needs of present and future generations in all aspects of life. The following areas characterize it as a highly intelligent integrated system:

- urban environment;
- safe city;
- digital city management;
- investment climate;
- welfare of the people.

The architecture of a smart city is the basic organization of elements: information systems and platforms, databases, and automated workstations (standards and rules of data exchange and use, regulations of access levels, etc.). It includes the principles and standards governing the design and development of the information system. The analysis of existing regulations in this area, reports, and recommendations provided by public authorities for municipalities suggests we do not give the problem of information security of smart cities in Russia enough attention. Such an approach does not correspond to foreign experience and requires revision, considering the entry of the world into the quantum era.

4 Features of the use of quantum communication in smart cities

4.1. The second quantum revolution

Much of the smart city's information turnover is through public networks, where attackers can intercept it. Members of the information system use cryptography to protect information. This makes it possible to use cyberspace to transmit smart city system data because even if it is intercepted, an intruder cannot access it. Mathematicians in the 90's of the last century have created methods that allow decrypting information protected by modern means of cryptography in a reasonable period. These are Shor's Algorithm - 1994 (solving the factorization problem) and Grover's Algorithm - 1998, which quadratically speeds up the complete search of secret keys. The collapse of cybersecurity did not happen, because it can only implement the algorithms on a quantum computer.

Things have changed in the last 5 years. Several countries around the world have created and shown working prototypes of quantum computers. Google published the results of the Quantum Supremacy experiment in 2019 - the Sycamore quantum processor performed calculations in 200 seconds, which is equivalent to 10,000 years of a normal computer [7]. A Chinese group of scientists in 2021 described the Zuchongzhi processor, which is 2-3 times more powerful than Google [8]. Experts used these results to predict that the technology capable of cracking the Bitcoin cipher can be created in 2027, and the RSA cipher in 2031 [9].

The UK regulator (The National Cyber Security Centre - NCSC), in its 2020 recommendations, predicts an increase in the power of existing quantum computers to a critical level for information security in 2030 [10]. The French Information Security Agency (Agence nationale de la sécurité des systèmes d'information - ANSSI) published its position on the quantum threat in January 2022. The NCSC predicted in its 2020 recommendations an increase in the power of existing quantum computers to a critical level for information security, warning that the threat of retroactive attacks - "save now, decrypt later" - could not be ruled out, which could have implications for the security of sensitive information [11]. We focused most predictions on open data, and in geopolitical confrontation, the success in building a workable quantum computer will be confidential information and identifying this point is possible only after the compromise of a significant amount of data [12].

Predictions of quantum computer creation differ, but they all converge in two factors:
- current ciphers will be decrypted;
- rapid transition to new means of cryptography is not possible.

The U.S. Department of Homeland Security issued a Memorandum of Preparation for Post-Quantum Crypto In October 2021. They noted problems in national security, including critical infrastructure data protection [13]. The reason for this is insufficient preparation for the transition to quantum-secure cryptography.

The U.S. has shown increased attention to developments in quantum technologies in other countries. America has entered many cooperation agreements in this area (with Japan in 2019, with Australia in 2021, with the UK in 2021, with Denmark, Switzerland, Canada, South Korea in 2022). These agreements provide for an active exchange of information, which allows for a rapid assessment of information security risk and prediction of when the quantum computer will emerge. The 2022 U.S. National Security Memorandum is of concern because it requires the national security agency to update the national security algorithm suite to include quantum-resistant cryptography [14].

4.2. Ways to protect data in a quantum threat environment

Analysis of foreign law allows us to distinguish two ways to ensure information security in the quantum's era computer.

1. Post-Quantum Cryptographic Algorithms.
2. Quantum Key Distribution.

These methods of information protection are not exhaustive. The NCSC points out the possibility of using ciphers based on Quantum Random Number Generation [15]. The regulator notes that, although there are many scientific studies on the security and effectiveness of various post-quantum cryptographic schemes, it is difficult to give an exact recommendation. NCSC plans to use a post-quantum algorithm, which the U.S. regulator (National Institute of Standards and Technology - NIST) will standardize.

NIST is now the world center for analyzing post-quantum cryptography algorithms. Groups of researchers in an open competition in 2018 proposed ciphers that a quantum computer cannot break. Various scientific organizations (Korea University, Chinese Academy of Sciences, Sorbonne University, University of Waterloo, and others) and technology companies (IBM Research, Microsoft, Philips Research, Intel, and others) submitted 50 ciphers in the first phase [16]. Researchers in the open competition proposed 4 post-quantum encryption algorithms in July 2022 after three verification phases:

- one for public key encryption
- three for electronic signature encryption.

It assessed the level of cybersecurity of a particular encryption algorithm based only on expert evaluations, which can be erroneous. One participant in the NIST finals was decrypted in August 2022 on a computer, even though it was resistant to quantum computer attacks since 2018.

Similar examples in the history of cryptography occur regularly. The U.S. had previously recognized the MD5 and SHA-1 algorithms as crypto-resistant, but a math teacher from China, cracked MD5 in 2004 and SHA-1 in 2005. China is one leader in encryption and decryption, which is probably why it has bet on quantum key distribution.

While some countries are analyzing and standardizing cryptographic algorithms resistant to quantum computing, others are developing quantum key distribution technology. This information security technology is based not on mathematical rules, but on the laws of quantum physics, which cannot be violated by an intruder. China is a leader in this field. It created a 4600 km long communication line protected by quantum encryption protocols [17]. Two satellites ensure the functioning of the Chinese quantum communication line.

The PRC has reformed the regulatory framework for the development of quantum key distribution. Objectives of the Encryption Law enacted in 2020:

- the development of cryptography;
- standardization and management of cryptography;
- development of the cryptographic industry;
- stimulating the creation of quality market products [18].

China continues to regulate cryptography used to protect public authority data strictly, but allows the formation of «commercial cryptography». The PRC in 2021 approved three standards for equipment used in the quantum key distribution process and 16 new cryptography standards, two of which are entirely devoted to quantum key distribution [19].

5 Discussion of results

We can draw several conclusions and generalizations.

1. Suggest the language of regulation of the legal relations in question. A smart city is a set of public and private information systems that provides a digital transformation of urban services, urban services and urban environment.

We should understand digital transformation as a change in the methods of state and municipal services during the introduction of digital technologies, providing alternative forms of interaction between public authorities and citizens, and also new types of digital services and digital services. For example, a map of public transport traffic is available only to users of a particular software product.

Urban services - services implemented on the territory of the municipality by local authorities and legal entities, and in cities of federal importance - services implemented by public authorities and legal entities. It is necessary to speak about transferring powers based on a contract or agreement for legal entities that are not under the control of local governments to provide urban services, which is an established practice in the system of public administration by the Russian Federation.

2. Local governments must take responsibility for the quality and safety of city services and any damage caused to individuals and legal entities by smart city information systems. In the absence of the local government's fault or if the administrator of the information system included in the smart city acts based on a contract, they may recover their costs from it.

For this purpose, it is necessary to conclude agreements for the management of city services between a municipality and an operator of an information system. Such a contract would allow to delineate responsibilities and determine the rights and obligations of the parties.

3. As part of the formation of the institution of responsibility of operators of information systems of the smart city, we propose to divide them into three groups:

- important;
- especially important;
- critical.

To form a system of information security for "smart city" information systems, contracts with operators of critical city services should establish the obligation to use quantum-secure cryptography systems. It is reasonable to define the use of such technologies as voluntary for other participants of social relations.

4. We can classify the use of quantum-secure cryptography considering the measures to support quantum communication in the Russian Federation:

- quantum cryptography;
- quantum-secure cryptography.

As part of the digital economy program, if the operator chooses a way to ensure information security - quantum cryptography — the state should form a support program, which is proposed to include:

- preferential access to quantum communication trunk lines, if available;
- full subsidizing of the interest rate on the loan for the creation of quantum communication lines by an information system operator for personal use and/or for the provision of quantum communication services to other participants of legal relations inside the city environment.

6 Conclusions

A smart city is a multi-element digital platform with integrated information systems that solve different problems. According to the ability of information technology to influence a specific citizen, it is possible to distinguish:

- important, such as services for competence control, culture, and leisure technology;
- especially-important, such as services designed to improve the physical environment and the interaction between residents and city authorities;
- critical, e.g. services designed to increase the physical and virtual security of residents.

The emergence of the quantum computer may pose some threats, so critical services should be transferred to the quantum communication system. Since the use of quantum key distribution technology is costly, post-quantum cryptography should be allowed to protect particularly important services.

This article was completed within the framework of the Governmental Assignment: "Russian Legal System in the Realities of Digital Transformation of Society and State: Adaptation and Prospects of Responding to Contemporary Challenges and Threats (FSMW-2023-0006)". Registration number: 1022040700002-6-5.5.1.

References

1. Smart Cities, National geographic, https://education.nationalgeographic.org/resource/smart-cities/
2. Kim JungHoon, Cities **123**, 103551 (2022)
3. Smart City Challenge: Lessons for Building Cities of the Future, https://www.transportation.gov/sites/dot.gov/files/docs/Smart%20City%20Challenge%20Lessons%20Learned.pdf
4. Mircea Eremia, Lucian Toma, Mihai Sanduleac, Procedia Engineering **181**, 12-19 (2017)
5. Smart city. Departmental project of the Ministry of Construction of Russia, https://russiasmartcity.ru/
6. Order of the Ministry of Construction of Russia dated December 25, 2020 No. 866/pr "On Approval of the Concept for the Urban Digitalization Project "Smart City", Information bulletin on regulatory, methodological and standard project documentation, **1-2**, (2021)
7. F. Arute, K. Arya, R. Babbush, et al., Nature **574**, 505–510 (2019)
8. Wu Yulin et al., Physical Review Letters. American Physical Society **127**, (2021)
9. M. Mosca, IEEE Security & Privacy **16(5)**, 38-41 (2018)
10. Quantum-safe cryptography (white paper), https://www.ncsc.gov.uk/whitepaper/quantum-safe-cryptography
11. ANSSI views on the post-quantum cryptography transition, https://www.ssi.gouv.fr/en/publication/anssi-views-on-the-post-quantum-cryptography-transition/
12. T. A. Polyakova, A. V. Minbaleev, V. B. Naumov, State and Law **5 C**, 104-114 (2022).
13. Memorandum on Preparing for Post-Quantum Cryptography, https://www.dhs.gov/publication/memorandum-preparing-post-quantum-cryptography
14. Memorandum on Improving the Cybersecurity of National Security, Department of Defense, and Intelligence Community Systems, https://www.whitehouse.gov/briefing-room/presidential-actions/2022/01/19/memorandum-on-improving-the-cybersecurity-of-national-security-department-of-defense-and-intelligence-community-systems/
15. Quantum security technologies (white paper), https://www.ncsc.gov.uk/whitepaper/quantum-security-technologies
16. K. S. Evsikov, Kutafin Law Review (KULawR) **4**, 46-58 (2022).
17. Yu-Ao Chen, Q. Zhang, Teng-Yun Chen, et al., Nature **589**, 214–219 (2021).
18. 维护国家密码安全　促进密码事业发展丨国家密码管理局负责人就《中华人民共和国密码法》答记者问. https://www.163.com/dy/article/G7PL4J0G0522LGCU.html
19. 国家密码管理局公告（第43号）. http://www.oscca.gov.cn/sca/xxgk/2021-10/19/content_1060880.shtml