National Research University Higher School of Economics

*As a manuscript*

Semenov Aleksandr Mikhailovich

# Secure data transfer methods for low-resource computing devices

Dissertation summary

for the purpose of obtaining academic degree
Doctor of Philosophy in Engineering

Academic supervisor:
Candidate of Sciences in Physics and Mathematics
Nesterenko Alexei Yuryevich

Moscow – 2022

**Statement of the problem and relevance of the research topic**

Evolution of information and telecommunication technologies has led to the appearance of specific areas of application of computing devices, characterized by specific requirements, areas and conditions of operation. For example, an application area commonly referred to as the Internet of Things (IoT) provides the concept of combining the "things" of the physical world with the "things" of the digital world, allowing the interaction of the "things" among themselves and with humans.

Industrial Internet of Things (IIoT) is a subcategory of the Internet of Things, includes computer networks with connected industrial, manufacturing facilities and objects of critical information infrastructure (CII) . These devices are equipped with built-in sensors, with the possibility of remote monitoring and control in an automated mode with minimal human intervention.

Today's technologies, based on IoT and IIoT concepts, together with classic information and communications technologies, provide unprecedented opportunities for collecting, automating, analyzing, and processing large volumes of data for consumers and providers of various services in various spheres of life. At present, the Russian Federation is actively working on the standardization, unification and implementation of various IoT technologies within the framework of the projects of the national program "Digital Economy of the Russian Federation" by developing domestic solutions in this area.

The relevance of security issues when using different "smart" solutions based on the use of IoT (IIoT) technologies at the present time:

- expanding area of application of these technologies and active work on the standardization, adaptation and unification of solutions in the field of the Internet of Things, both in the Russian Federation and abroad;
- the national program "Digital Economy of the Russian Federation";
- competitiveness and the possibility of impotrosubstitution in the use of these technologies, both at the software and hardware level;
- a restriction on the use of foreign software at significant sites of critical information infrastructure from January 1, 2025 (Russian Federation Presidential decree by 30.03.2022 №166).

**The degree of scientific development of the issue**

Security issues of IoT technologies have been considered since the first developments in this area in the 2000s. Regulation of the field of "Internet of Things" both in terms of applied issues of data processing and transmission, and in terms of security is conducted by a number of foreign organizations on standardization and industry committees, among which can be distinguished: 3GPP, ITU-T, IETF, IRTF, NIST, Wi-Fi Alliance, Zigbee Alliance. These organizations have developed documents [1, 2, 3, 4, 5], whose purpose is to regulate the security issues in the use of IoT-technology.

In the Russian Federation, standardization activities in the field of the Internet of Things are carried out within the framework of technical committees №194, №26 and №362. Various Russian security technologies are being developed, adapted and researched within the framework of these organizations. Among the standardized technologies to date, the following specifications can be distinguished [6, 7, 8, 9, 10, 11, 12, 13, 14].

In the domestic standardization of ¡¡Internet of Things¿¿ technologies, a mandatory step is to justify security and evaluation of performance indicators of protection measures provided by the solution recommended for use. Approaches adopted in the Russian Federation to conduct such justification considered in papers [15, 16, 17, 18], as well as in the article [19]. In foreign publications, it is common to use approaches based on the Bellare – Rogaway [20] model and its modifications [21, 22, 23, 24], and the Canetti–Krawczyk [25] and its modifications [26, 27, 28]; the works of [29, 30, 32, 31] should also be highlighted.

**Research goals and tasks**

The dissertation goal is to develop mechanisms to provide data transmission protection for low-resource computing devices.

To achieve this goal, the following **tasks** were solved in the thesis:

- The main protocol stack vulnerabilities of different technologies ¡¡Internet of Things¿¿ (IoT) are revealed.
- A family of cryptographic protocols for secure interaction for control and measurement devices has been developed.
- Developed a method for evaluating the performance of protection.
- The exact values of the protection efficiency parameters for the developed protocol family.

- The developed protocol family for data transmission via UDP and TCP was tested.

**The theoretical significance** of the study is the development methods for evaluating the security qualities of secure communication protocols.

**The practical significance** of the results of this dissertation work lies in the development of a new family of secure interaction protocols and a method for assessing the effectiveness of protective measures of this family of protocols.

Developed family of secure interaction protocols:

- approved as a recommendation for standardization R 1323565.1.028-2019, with the effective date September 1, 2020 for SKZI classes from KS1 to KA (Order of the Federal Agency for Technical Regulation and Metrology for technical regulation and metrology №1503-st of December 30 2019);

- is included in the list of standardized protocols that can that can be used to organize information exchange between components of the smart power metering system (order №. 788 of the Ministry of Digitalization of Russia of December 30, 2020).

The developed method of estimation of efficiency of protection measures of cryptographic protocols is applied at carrying out works within the framework of Technical Committee on standardization № 26 ¡¡Cryptographic protection of information¿¿ at the analysis of cryptographic protocols ESP and IKEv2 [33].

**Provisions of the defense:**

- classification of vulnerabilities of ¡¡Internet of Things¿¿ technologies;

- family of secure communication protocols;

- method for developing a formal model of cryptographic protocols and formalization of security properties;

- method of estimation of protection effectiveness indicators within the framework of the built model;

- theorem about the values of the protection effectiveness indicators for the family of secure communication protocols.

**Research methods**

Methods of discrete mathematics, algebra, number theory, theory of algorithms and mathematical logic and automata theory (graph theory) were used to solve these problems.

**The research object** is a family of secure interaction protocols developed as part of this dissertation research, which includes:

- A key agreement protocol according to the Diffie-Hellman scheme in a group of elliptic curve points.
- Authentication protocol based on the use of pre-distributed key and PKI infrastructure or electronic signature algorithm GOST R 34.10-2012.
- Application data transfer protocol, independent of the type of transport channel used and the level of interaction within the ISO model.

**The subject of the study** are protection performance indicators, developed in the thesis research family of secure interaction protocols using the proposed in the study method of evaluation of protection performance indicators.

**Author's personal contribution**

The author's analytical research of IoT technologies allowed to compile a list of typical classes of vulnerabilities typical for IoT technologies. The author was actively involved in the process of developing and standardizing a new family of cryptographic protocols for secure interaction of control and measurement devices. The approach proposed by the author allowed to build a model of the family of cryptographic protocols and evaluate the effectiveness of their security measures, as well as justify the implementation of the required security properties. All results presented in the defense were obtained personally by the author.

**General conclusions of the study**

1. An analytical review of a number of guidance documents on the creation of secure IoT devices, IoT-infrastructures and services developed by international, industry committees and national standardization organizations was conducted. The protocol stack specifications of a number of IoT-technologies and scientific publications dedicated to the security issues of these technologies were studied. The classification of vulnerabilities of different protocol stacks

used in the ¡¡Internet of Things¿¿ technologies was performed. As a result of the analysis, a list of the main sources and vulnerabilities characteristic of the interaction of IoT devices is formulated.

2. Developed a new family of protocols SP-FIOT, which includes a protocol for generating a common key and application data transport protocol.

3. A method for constructing a formal model of cryptographic protocols and formalizing security properties within it is proposed.

4. Proposed method for constructing a formal model of cryptographic protocols and formalizing security properties within its framework.

5. A theorem on the values of performance indicators for the developed family of SP-FIOT secure interaction protocols is proved.

**Work approbation**

The results obtained in the thesis work were presented and discussed at the following scientific conferences:

1. V CTCrypt'2016 Symposium ¡¡Modern Trends in Cryptography¿¿ (Yaroslavl, 2016). Report: Analysis of Russian key agreement protocols using automated means of verification.

2. The Sixth China-Russia Conference on Numerical Algebra with Applications (CRCNAA 2017) (Moscow, 2017). Report: Grafting the Herbs family of key exchange protocols onto the TLS tree.

3. 17-th International Conference ¡¡Siberian scientific school-seminar ¡¡Computer security and cryptography¿¿ - SIBECRYPT'18 (Abakan, 2018). Report: Integration of native public keying protocols into TLS 1.3 protocol.

4. Annual interuniversity scientific and technical conference of students, graduate students and young specialists named after E.V. Armensky (Moscow, 2020). Report: protocol for secure interaction of cryptographic protection of information.

5. Annual interuniversity scientific and technical conference of students, graduate students and young specialists named after E.V. Armensky (Moscow,

2021).Report: Methodology for evaluating the security properties of cryptographic protocols.

The abstracts of the presented reports are published in [34], [35], [36], [37].

**Publications**

The author has published six papers on the topic of his dissertation research, two of them in international journals indexed in the Scopus database.

**Papers published by the author in peer-reviewed scientific publications included in the Scopus citation system**

1. Nesterenko A. Yu. Metodika ocenki bezopasnosti kriptograficheskih protokolov [Methodology for assessing the security of cryptographic protocols] / A. Yu. Nesterenko, A. M. Semenov // Prikl. Diskr. Mat. - 2022. - №56. - pp. 33-82. (In Russian).

2. Nesterenko A. Yu. On the practical implementation of Russian protocols for low-resource cryptographic modules / A. Yu. Nesterenko, A. M. Semenov // Journal of Computer Virology and Hacking Techniques. - 2020. - Vol. 16. - №4. - pp. 305-312.

**Papers published by the author in peer-reviewed scientific journals Journals included in the list of recommended journals of the Higher School of Economics**

3. Semenov A. M. Analysis of Russian key-agreement protocols using automated verification tools // Mathematical Issues in Cryptography. 2017. Vol. 8. № 2. pp. 131-142.

**Papers published in other journals**

4. Nesterenko A. Yu., Semenov A. M. Kriptograficheskie mekhanizmy zashchishchennogo vzaimodejstviya kontrol'nyh i izmeritel'nyh ustrojstv [Cryptographic mechanisms of secure interaction of control and measuring devices] // Bezopasnost' informacionnyh tekhnologij. 2020. Vol. 27. № 4. pp. 7-16. (In Russian).

5. Nesterenko A. Yu., Lebedev P. A., Semenov A. M., Kratkij analiz kriptograficheskih mekhanizmov zashchishchennogo vzaimodejstviya kontrol'nyh i izmeritel'nyh ustrojstv. Tekhnicheskij komitet po standartizacii "Kriptograficheskaya zashchita informacii". "Kriptograficheskie issledovaniya" [Brief analysis of cryptographic mechanisms for secure interaction of control and measuring devices. Technical Committee on Standardization Cryptographic protection of information. Cryptographic research]. 2019. URL: https://tc26.ru/standarts/kriptograficheskie-issledovaniya (access date: 17.07.2022).

6. Nozdrunov V.I., Semenov A.M., Podhody k kriptograficheskoj zashchite kommunikacij v IoT i M2M. Informacionnaya bezopasnost' [Approaches to cryptographic protection of communications in IoT and M2M. Information security], №5, 2019. pp. 38–40. URL: https://infotecs.ru/about/press-centr/publikatsii/podkhody-k-kriptograficheskoy-zashchite-kommunikatsiy-v-iot-i-m2m.html (access date: 17.07.2022).

# References

[1] RFC7452 - Architectural Considerations in Smart Object Networking. Internet Architecture Board (IAB). - 2015. - 24 p.

[2] Ross, R., McEvilley, M., and J. Oren, ¡¡Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems¿¿, NIST Special Publication 800-160, DOI 10.6028/NIST.SP.800-160. November 2016. URL: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/ NIST.SP.800-160.pdf. (access date 01.10.2021).

[3] Internet of Things Security Foundation Establishing Principles for Internet of Things Security. URL: https://iotsecurityfoundation.org/establishing-principles-for-internet-of-things-security. (access date 01.10.2021)

[4] Moore K. Best Current Practices for Securing Internet of Things (IoT) Devices / K. Moore, R. Barnes, H. Tschofenig // IETF-draft, draft-moore-iot-security-

bcp-01, January 2018. URL: https://tools.ietf.org/id/draft-moore-iot-security-bcp-01.html (access date 05.05.2022)

[5] European Union Agency for Network and Information Security, Communication network dependencies for ICS/ SCADA Systems, 2017, URL: https://www.enisa.europa.eu/publications/ ics-scada-dependencies. (access date 01.10.2019)

[6] R 1323565.1.028-2019 Informacionnaya tekhnologiya. Kriptograficheskaya zashchita informacii. Kriptograficheskie mekhanizmy zashchishchennogo vzaimodejstviya kontrol'nyh i izmeritel'nyh ustrojstv [Information technology. Cryptographic protection of information. Cryptographic mechanisms of secure interaction of control and measuring devices]. - M.: Standardinform, 2019. - 66 p. (In Russian).

[7] R 1323565.1.032-2020 Informacionnaya tekhnologiya. Kriptograficheskaya zashchita informacii. Ispol'zovanie rossijskih kriptograficheskih mekhanizmov dlya realizacii obmena dannymi po protokolu DLMS [Information technology. Cryptographic protection of information. The use of Russian cryptographic mechanisms for the implementation of data exchange under the DLMS protocol]. - M.: Standardinform, 2020. - 40 p. (In Russian).

[8] R 1323565.1.029-2019 Informacionnaya tekhnologiya. Kriptograficheskaya zashchita informacii. Protokol zashchishchennogo obmena dlya industrial'nyh sistem [Information technology. Cryptographic protection of information. Secure exchange protocol for industrial systems]. - M.: Standardinform, 2019. - 15 p. (In Russian).

[9] R 1323565.1.018-2018 Informacionnaya tekhnologiya. Kriptograficheskaya zashchita informacii. Kriptograficheskie mekhanizmy autentifikacii v kontrol'nyh ustrojstvah dlya avtotransporta [Information technology. Cryptographic protection of information. Cryptographic authentication mechanisms in control devices for vehicles]. - M.: Standardinform, 2018. - 19 p. (In Russian).

[10] GOST R 70036-2022 ¡¡Informacionnye tekhnologii. Internet veshchej. Protokol besprovodnoj peredachi dannyh na osnove uzkopolosnoj modulyacii radiosignala (NB-Fi) [¡¡Information technologies. Internet of all. Protocol of the wireless

data transmission on the basis of the base of the base-band modulation of the radio signal (NB-Fi)]. - Moscow: Russian Institute for Standardization, 2022. - 56 p. (In Russian).

[11] PNST Informacionnye tekhnologii. Internet veshchej. Protokol obmena dlya vysokoemkih setej s bol'shim radiusom dejstviya i nizkim energopotrebleniem [Information Technology. Internet of Things. An exchange protocol for high-capacity networks with a long range and low power consumption.]. URL: https://docs.cntd.ru/document/554596382 (access date 05.05.2022) (In Russian).

[12] PNST Informacionnye tekhnologii. Arhitektura otkrytoj seti radiodostupa [Information Technology. The architecture of an open radio access network.]. URL: https://www.normacs.info/projects/9439 (access date 05.05.2022). (In Russian).

[13] PNST Informacionnye tekhnologii. Interfejsy otkrytoj seti radiodostupa [Information Technology. The architecture of an open radio access network.]. URL: https://www.normacs.info/projects/10453 (access date 05.05.2022). (In Russian).

[14] PNST Informacionnye tekhnologii. Internet veshchej. Obshchie polozheniya [Information Technology. Internet of Things. General provisions.]. URL: https://allgosts.ru/35/110/pnst_419-2020.pdf (access date 05.05.2022). (In Russian).

[15] Alferov A. P. Osnovy kriptografii [Fundamentals of Cryptography] / A.P. Alferov, A.Yu. Zubov, A.S. Kuzmin, A.V. Cheremushkin. - M.: Gelios APB., 2002. - 480 p. (In Russian).

[16] Babash A. V. Kriptografiya [Cryptography] / A.V. Babash, G.P. Shankin - M.: Solon-Press, 2007. - 512 p. (In Russian).

[17] Kachalin I. F. Ob osnovnyh koncepciyah kriptograficheskoj stojkosti / I.F. Kachalin, A.S. Kuz'min, E.A. Suslov // Tezisy XII Vseros. shkoly-kollokviuma po stohasticheskim metodam i VI Vseros. simpoziuma po prikladnoj i promyshlennoj matematike. Sochi-Dagomys, 1–7 oktyabrya 2005 pp. 982–983. (In Russian).

[18] Los A.B. Kriptograficheskie metody zashchity informacii [Cryptographic methods of information protection] / A.B. Los, A.Yu. Nesterenko, M.I. Rozhkov // - M.: Preserve Jurait, 2016. - 473 p. (In Russian).

[19] Nesterenko A. YU. Metodika ocenki bezopasnosti kriptograficheskih protokolov [Methodology for security assessment of cryptographic protocols] / A. YU. Nesterenko, A. M. Semenov // PDM. - 2022. - №56. - pp. 33-82. (In Russian).

[20] Bellare M. Entity authentication and key distribution / M. Bellare, P. Rogaway // LNCS. - 1993. - Vol. 773. - pp. 232-249

[21] Bellare M. Authenticated key exchange secure against dictionary attacks / M. Bellare, D. Pointcheval, P. Rogaway // LNCS. - 2000. - Vol. 1807. - pp. 139-155

[22] Bellare M.Provably secure session key distribution — the three party case / M. Bellare, P. Rogaway // 27th ACM Symp. Theory Computing. - 1995. - pp. 57–66

[23] Blake-Wilson S. Key agreement protocols and their security analysis / S. Blake-Wilson, D. Johnson, A. Menezes // LNCS. - 1997. - Vol. 1355. - pp. 30–45

[24] Blake-Wilson S. Entity authentication and authenticated key transport protocols employing asymmetric techniques / S. Blake-Wilson, A/ Menezes // LNCS. - 1998. - Vol. 1361. - pp. 137–158

[25] Canetti R. Analysis of key-exchange protocols and their use for building secure channels/ R. Canetti, H. Krawczyk // LNCS. - 2001. - Vol. 2045. - pp. 453-474

[26] LaMacchia B.. Stronger security of authenticated key exchange / B. LaMacchia, K. Lauter, A. Mityagin // LNCS. - 2007. - Vol. 4784. - pp. 1–16

[27] Krawczyk H. HMQV: A high-performance secure Diffie — Hellman protocol / H. Krawczyk // LNCS. - 2005. - Vol. 3621. - pp. 546–566

[28] Menezes A. On the importance of public-key validation in the MQV and HMQV key agreement protocols/ A. Menezes, B. Ustaoglu // LNCS. - 2006. - Vol. 4329. - pp. 133-147

[29] Rabin M. Digitized Signatures and Public Key Functions as Intractable as Factorization / M. Rabin // Technical Report: MIT/LCS/TR-212. MIT Laboratory for Computer Science. - Cambrige. - 1979. - pp. 20.

[30] Goldwasser S. Probabilistic encryption / S. Goldwasser, S. Micali // J. Computer System Sci. - 1984. - Vol. 28. - pp. 270–299

[31] Mao W. Modern Cryptography: Theory and Practice. New Jersey: Prentice Hall, 2003. - 707 p.

[32] Boyd C. Protocols for Authentication and Key Establishment / Boyd C., Mathuria A., and Stebila D. // Second Ed. Berlin; Heidelberg: Springer Verlag. - 2020. - 521 p

[33] R 1323565.1.035–2021 Informacionnaya tekhnologiya. Kriptograficheskaya zashchita informacii. Ispol'zovanie rossijskih kriptograficheskih algoritmov v protokole zashchity informacii ESP [Information technology. Cryptographic protection of information. Using Russian cryptographic algorithms in the ESP information protection protocol]. - M.: Standardinform, 2021. - 52 pp. (In Russian).

[34] Semenov A., Analysis of Russian key-agreement protocols using automated verification tools, Pre-proceedings of 5th Workshop on Current Trends in Cryptology, CTCrypt 2016 (June 6-8, 2016, Yaroslavl, Russia), pp. 23-37

[35] Grebnev S. V., Lazareva E. V., Lebedev P. A., Nesterenko A. YU., Semenov A. M. Integraciya otechestvennyh protokolov vyrabotki obshchego klyucha v protokol TLS 1. 3 [Integration of native public keying protocols into TLS 1. 3] // PDM. Prilozhenie. 2018. №11, c. 62-65. URL: https://cyberleninka.ru/article/n/integratsiya-otechestvennyh-protokolov-vyrabotki-obschego-klyucha-v-protokol-tls-1-3 (access date: 17.07.2022) . (In Russian).

[36] Nesterenko A.Y., Semenov A.M. Protokol zashchishchennogo vzaimodejstviya sredstv kriptograficheskoj zashchity informacii [Protocol for secure interaction of cryptographic protection of information] // Interuniversity scientific and technical conference of students, graduate students and young specialists named

after E.V. Armensky. Conference materials. Moscow: 2020, pp. 172-174. (In Russian).

[37] Nesterenko A.Y., Semenov A.M. Metodika ocenki svojstv bezopasnosti kriptograficheskih protokolov [Methodology for Evaluating the Security Properties of Cryptographic Protocols] // E.V. Armensky Interuniversity Scientific and Technical Conference for Students, Postgraduate Students and Young Specialists. Conference materials. Moscow: 2021, pp. 249-251. (In Russian).