About Some Perspective Training Cryptography Disciplines

Alexander A. Varfolomeev
Information Security Department
Bauman Moscow State Technical University
Moscow, Russia
a.varfolomeev@mail.ru

***Abstract*— The work contains proposals for new training disciplines on cryptography that go beyond the traditional disciplines such as "Cryptographic methods of information protection", specifying and supplementing them. Particular attention is paid to the content of disciplines "Financial Cryptography", "Post-Quantum Cryptography", etc. These disciplines could be included in the disciplines section of choice for training specialists and bachelors.**

Keywords*— financial cryptography, post-quantum cryptography, lightweight cryptography, lattice-based cryptography, code-based cryptography, multivariate cryptography; supersingular elliptic curve isogeny cryptography.

I. Introduction

The quality of training and the demand for information security professionals largely depends on the disciplines studied by them in the university, including those from cryptographic disciplines. The purpose of the work was to select relatively new, relevant fields and areas of research in cryptography and to determine the possibility on their basis of developing new disciplines for training specialists and bachelors [1]. It is important not only to determine the name of the discipline, but also to its sections.

II. Methodology and Justification of the Choice of Disciplines and Their Content

We offer as the first sources for the selection of actual areas of cryptography the pages of website of the International Association of Cryptographic Research (IACR): Events and Open position.

The Events page contains a list of conferences, seminars and schools on cryptography and information security. The first step will be the consideration of the names of events, which in some cases can help with the choice of the name of the discipline. The second step is to review the sections and works presented at these events.

Activities related to concepts such as "Elliptic Curve cryptography", "Hash functions", can be only sections of disciplines, because of their narrow focus and connection with several areas. For example, without getting acquainted with these concepts it is impossible to set standards for digital signature, etc. On the contrary, many activities cover too large areas of cryptography (“Public Key Cryptography”, “Symmetric Key Cryptography”).

Similarly, in the list of cryptographic disciplines of the department there are names that say little about their content. For example, "Introduction to cryptography", "Cryptographic methods of information protection". The latter discipline can cover all cryptography.

The author has allocated the following activities for the formation of new disciplines:

- Financial Cryptography and Data Security (FC);
- Crypto Finance Conference (CFC);
- School on Cryptocurrency and Blockchain Technologies;
- International Conference on Post-Quantum Cryptography (PQCrypto);
- International Workshop on Lightweight Cryptography for Security & Privacy (LightSec);
- Workshop on Fault Diagnosis and Tolerance in Cryptography (FDTC);
- Annual Workshop on the Economics of Information Security (WEIS).

The second source of choice of subjects of disciplines - Open position - provides a list of areas of cryptography and information security that are of interest to employers from various organizations. A number of these areas are classical, and a number are quite new and promising. Here are some of them:

- homomorphic and split key encryption,

- function and format preserving encryption,

- lattice and pairing-based functional encryption,

- trusted computing,

- distributed ledger technologies,

- secure multiparty computation,

- financial cryptography,

- blockchain security,

- payments (micropayments),

- cryptocurrencies,

- smart contracts,

- secure cloud computing,

- IoT security protocols,

- bio-computation,

- quantum cryptography,

- quantum computation,

- post-quantum cryptography,

- elliptic curve cryptography,

- lattice-based cryptography,

- code-based cryptography,

- lightweight cryptography.

The third source for substantiating the choice and formation of disciplines are publications of domestic and foreign periodicals on cryptography. (For example, [2-12]). On the basis of the proposed approach, it is expedient to allocate the following cryptographic disciplines for study:

- "Financial cryptography";
- "Post-quantum cryptography";
- "Lightweight (low-resource, balanced) cryptography";
- "Quantum cryptography".

It is more difficult to justify the choice of sections and training modules for each of the disciplines.

“Financial cryptography”.

The notion of "financial cryptography" can be defined as ensuring the information security of financial transactions in electronic (digital) form by cryptographic methods.

In connection with this definition, in the discipline "Financial Cryptography", in the author's opinion, the following sections should be included:

- cryptographic schemes and protocols of electronic payments (including in remote banking systems (RBS);

- micropayments;

- electronic money;

- crypto-currencies;

- the use of smart cards;

- technology of digital watermarks;

- protocols of electronic auctions;

- special schemes for digital (electronic) signature, taking into account domestic and international standards and recommendations.

In work [4] it was noted that the scope of "financial cryptography" has changed significantly since the inception of this concept. If earlier cryptography ensured the security of operations with financial means presented in electronic form, now, in addition, cryptography itself provides financial resources in the form of crypto-currencies that do not have a physical basis in the real world.

As can be seen from the listed sections, it is difficult to determine the necessary time for the presentation of this material. In the case of a time limit of one semester, a complex selection of material for each section is required.

A feature of this area is its government regulation, imposing its limitations on the application of security measures. Apparently, for this it is necessary to select the separate training module. In support of this, it is sufficient to mention as examples Federal Law No. 161-FZ "On the National Payment System" dated June 27, 2011, Regulation No. 382-P of the Bank of Russia of June 9, 2012, RF Government Decree of April 16, 2012. No. 313.

In addition, in Russia and abroad systems of standards and best practices are developing. In view of their specifics, it is difficult to justify their inclusion in other cryptographic disciplines. The Bank of Russia created a number of industry standards (SRT BR IBBS -1.0., Etc.). The obligatory standard on plastic cards Payment Card Industry Data Security Standard (PCI DSS 3.2) still applies. We can say that financial cryptography in our country is represented mainly by the banking sphere of activity. Recently, the standard GOST R 57580.1-2017 "Safety of financial (banking) operations. Basic composition of organizational and technical measures".

“Post-quantum cryptography”.

Of course, it should be recalled that post-quantum cryptography deals with the development and analysis of cryptographic primitives that are resistant to methods of analysis using a quantum computer. Thanks to the timely raised security issue, the existing and widely used primitives from the advent of quantum computers have done a lot. A number of stable schemes based on various principles are proposed. Work continues to increase the effectiveness of their implementation, which is still inferior to those used in security systems.

Since 2006, the conference "PQCrypto" (in 2017 - the eighth). In fact, the names of its sections determine the different directions and principles of building persistent primitives. They can form training modules:

- Cryptosystems based on hash functions;
- Cryptosystems based on algebraic codes;
- Cryptosystems based on algebraic lattices;
- Cryptosystems based on multivariate systems;
- Cryptosystems based on isogenies of supersingular elliptic curves.

As can be seen from the names of these modules, the exposition of all of them requires a serious study of various complex mathematical constructions. Therefore, it is difficult to present these modules within one semester. Apparently, it is necessary to prepare separate curricula of disciplines for each of the listed directions.

Currently, the National Institute of Standards and Technology (NIST) has initiated a process to solicit, evaluate, and standardize one or more quantum-resistant public-key cryptographic algorithms. The deadline for submission of applications (November 30, 2017) has already passed. Sixty-nine applications were submitted, three of which were rejected. All applications are publicly available and can be downloaded from the NIST website. On the site you can find comments on the applications, you can participate in the discussion yourself.

Materials of the process can be used in the study of discipline in various ways. The lecture material should include the study of cryptosystems that have existed for quite a long time and have been subjected to a long analysis by many researchers. New cryptosystems can be used to select themes for course and diploma papers, topics for lectures in seminars.

Below we give a list of the algorithms announced for the NIST competition, selected according to the directions and principles of construction, mentioned above.

TABLE I. TABLE OF SOME QUANTUM-RESISTANT PUBLIC-KEY CRYPTOGRAPHIC ALGORITHMS FOR NIST STANDARTIZATION PROCES

Type	**Algorithms**
Cryptosystems based on hash functions	Gravity-SPHINCS; **SPHINCS+;**
Cryptosystems based on algebraic codes	BIG QUAKE; BIKE; Classic McEliece; DAGS; HQC; LAKE; LEDAkem; LEDApkc; Lepton; LOCKER; McNie; NTS-KEM; Ouroboros-R; pqsigRM; QC-MDPC KEM; RaCoSS; RankSign; RLCE-KEM; RQC;
Cryptosystems based on algebraic lattices; LWE and its variants	CRYSTALS-DILITHIUM; DRS; FALCON; LAC; LIMA; NTRUEncrypt; pqNTRUSign; NTRU-HRSS-KEM; NTRU Prime; Odd Manhattan; qTESLA; Titanium; CRYSTALS-KYBER; Ding Key Exchange; EMBLEM and R.EMBLEM; FrodoKEM; HILA5; KCL (pka OKCN/AKCN/CNKE); KINDI; Lizard; LOTUS; NewHope; Round2; SABER; Three Bears
Cryptosystems based on multivariate systems	DME; DualModeMS; GeMSS; HiMQ-3; LUOV; MQDSS; Rainbow**;**
Cryptosystems based on isogenies of supersingular elliptic curves	SIKE (SIDH)
New & others	Edon-K; Giophantus; Mersenne-756839; Ramstake;

All algorithms and systems participating in the NIST competition are related to asymmetric cryptography (for symmetric cryptography, the threat of the appearance of a quantum computer is not so terrible). Therefore, it is natural to study this discipline after studying the issues of classical asymmetric cryptography. It is possible to assign the module "Cryptosystems based on algebraic codes" to a discipline such as "The Mathematical Theory of Coding". But, even in this case, it is not possible to expound this discipline in one semester.

“Lightweight (balanced, low-resource) cryptography”

This area of cryptography has reached a sufficient level of development and has great practical application [2, 3]. Evidence of this can serve as the developed international cryptographic standards:

- ISO / IEC 29192-1: 2012 Information technology - Security techniques - Lightweight cryptography - Part 1: General.
- ISO / IEC 29192-2: 2012 - Lightweight cryptography - Part 2: Block ciphers.
- ISO / IEC 29192-3: 2012 - Lightweight cryptography - Part 3: Stream ciphers.
- ISO / IEC 29192-4: 2013 - Lightweight cryptography - Part 4: Mechanisms using asymmetric techniques.
- ISO / IEC 29192-5: 2016 - Lightweight cryptography - Part 5: Hash-functions.

The preparation of these standards in recent years was preceded by an active study of this field, the results of which were included in several useful surveys [6-8].

The presentation of them within the framework of this discipline will relieve the discipline "Cryptographic standards". It should also be noted that this discipline should be included in a block of disciplines for choice for the preparation of bachelors and specialists. Her teaching should naturally follow after studying the basic concepts of cryptography such as block and stream ciphers, hash functions and asymmetric cryptosystems, which are mentioned in the name of the above standards [13-21].

III. HARMONIZATION OF EDUCATIONAL MATERIAL OF VARIOUS DISCIPLINES IN CONDITIONS OF TIME LIMITATIONS OF THE EDUCATIONAL PROCESS..

In some universities, there was a separation of cryptographic disciplines depending on the mathematical apparatus used in the presentation and study. For example, cryptographic disciplines related to asymmetric cryptography require students to learn a lot from the theory of numbers that are set out in early student training courses.

At one time, the development and adoption of digital signature standards on the basis of a group of elliptic curve points led to a change and increase in the studied material in basic mathematical disciplines, which eliminated the need to present these issues in cryptographic disciplines. Similarly, these disciplines should be influenced by new proposed cryptographic disciplines. For example, one of the modules of Post-Quantum Cryptography requires a greater study of algebraic lattices. In addition, the discipline "Financial Cryptography" obviously affects the basic cryptographic disciplines themselves. Therefore, there is a lot of work to select the material and its methodological coordination among the mathematical and cryptographic disciplines, to ensure the possibility of presenting all the necessary material in a sufficiently tight framework of the educational process (e.g. [22, 23]).

IV. CONCLUSIONS

In this paper, a method for determining promising educational cryptographic disciplines is proposed, with the use of which a short list is compiled. The training modules that compose them and their sections are presented. The development and introduction of these cryptographic disciplines in the educational process requires a lot of methodological work to harmonize the material presented in both cryptographic and mathematical disciplines.

REFERENCES

[1] Sheremet I.A. Directions of a New Level Education to Counter Cyberthreats in Financial Sphere. Voprosy kiberbezopasnosti *[Cybersecurity issues]*. 2016. No 5(18), pp. 3-7. DOI: 10.21681/2311-3456-2016-5-3-7.

[2] Zhukov A. Lightweight Cryptography: Modern Development Paradigms. In Proceedings of the 8th International Conference on Security of Information and Networks (Sochi, Russian Federation, September 08-10, 2015). SIN '15. ACM New York, NY, USA, 2015, pp. 7-7. DOI: 10.1145/2799979.2799981.

[3] Zhukov A.E. Lightweight cryptography. Part 1. Voprosy kiberbezopasnosti *[Cybersecurity issues]*. 2015. № 1 (9), pp. 26-43. DOI: 10.21681/2311-3456-2015-1-26-43.

[4] Varfolomeev A.A. Analysis of the change of the concept «Financial cryptography» on the basis of 20 years subjects of the international conference «Financial cryptography and data security». Statistics and Economics. 2016; (4):12-15. (In Russ.) DOI:10.21686/2500-3925-2016-4-12-15. (In Russ)

[5] J. Yu and M. Ryan, “Evaluating web PKIs,” in Software Architecture for Big Data and the Cloud, 1st ed., I. Mistrik, R. Bahsoon, N. Ali, M. Heisel, and B. Maxim, Eds. Elsevier, 2017, ch. 7, pp. 1-13. URL: https://eprint.iacr.org/2017/526.pdf.

[6] Biryukov A., Perrin L., State of the Art in Lightweight Symmetric Cryptography, IACR Cryptology ePrint Archive, 2017, pp. 1-40. URL: https://eprint.iacr.org/2017/511.pdf.

[7] Cazorla M., Marquet K., Minier M., Survey and Benchmark of Lightweight Block Ciphers for Wireless Sensor Networks. IACR Cryptology ePrint Archive, 2013, pp. 1-13. URL: https://eprint.iacr.org/2013/295.pdf.

[8] Delvaux J., Peeters R., Gu D., Verbauwhede I., A Survey on Lightweight Entity Authentication with Strong PUFs, IACR Cryptology ePrint Archive, 2014. URL: https://eprint.iacr.org/2014/977.pdf.

[9] Atzei N., Bartoletti M., Cimoli T., A survey of attacks on Ethereum smart contracts, IACR Cryptology ePrint Archive, 2016. URL: https://eprint.iacr.org/2016/1007.pdf

[10] Halak B., Waizi S., Islam A., A Survey of Hardware Implementations of Elliptic Curve Cryptographic Systems, IACR Cryptology ePrint Archive, 2016. URL: https://eprint.iacr.org/2016/712.pdf

[11] Tschorsch F., Scheuermann B., Bitcoin and Beyond: A Technical Survey on Decentralized Digital Currencies, IACR Cryptology ePrint Archive, 2015. URL: https://eprint.iacr.org/2015/464.pdf

[12] Bernstein D.; Hopwood D., Hülsing A., Lange T., eds. "SPHINCS: practical stateless hash-based signatures". Lecture Notes in Computer Science. 9056 (Advances in Cryptology -- EUROCRYPT 2015): 368–397. DOI: 10.1007/978-3-662-46800-5_15. ISBN 9783662467992.

[13] Augot D., Batina L., Bernstein D.J., Bos J., Buchmann J., and etc. Initial recommendations of long-term secure post-quantum systems, Technical report 2015. URL: http://pqcrypto.eu.org/docs/initial-recommendations.pdf.

[14] Overbeck R., Bernstein D., ed. Code-based cryptography. Post-Quantum Cryptography. Springer Berlin Heidelberg, 2014. 95–145. DOI: 10.1007/978-3-540-88702-7_4.

[15] Misoczki R.., Tillich J., Sendrier N., Barreto, P. S. L. M. MDPC-McEliece: New McEliece variants from Moderate Density Parity-Check codes. 2013 IEEE International Symposium on Information Theory: 2069–2073. DOI: 10.1109/ISIT.2013.6620590.

[16] Hirschhorn P.S., Hoffstein J., Howgrave-Graham N., Whyte W. (2009) Choosing NTRUEncrypt Parameters in Light of Combined Lattice Reduction and MITM Approaches. In: Abdalla M., Pointcheval D., Fouque PA., Vergnaud D. (eds) Applied Cryptography and Network Security. ACNS 2009. Lecture Notes in Computer Science, vol 5536. Springer, Berlin, Heidelberg. DOI: 10.1007/978-3-642-01957-9_27.

[17] Peikert Chris. Lattice Cryptography for the Internet. IACR. Archived from the original, 2014. URl: https://eprint.iacr.org/2014/070.pdf , 2014.

[18] Lin J., Ding X., Xiaodong A Simple Provably Secure Key Exchange Scheme Based on the Learning with Errors Problem. IACR Cryptology ePrint Archive, 2012. URL: https://eprint.iacr.org/2012/688.pdf

[19] Güneysu, Tim; Lyubashevsky, Vadim; Pöppelmann, Thomas (2012). Practical Lattice-Based Cryptography: A Signature Scheme for Embedded Systems. In Proceeding CHES'12 Proceedings of the 14th international conference on Cryptographic Hardware and Embedded Systems, pp. 530-547. DOI:10.1007/978-3-642-33027-8_31.

[20] Alkim E., Ducas ., Pöppelmann T., Schwabe P. "Post-quantum key exchange - a new hope" . In 25th Security Symposium. 2016. URL: https://www.usenix.org/conference/usenixsecurity16/technical-sessions/presentation/alkim.

[21] Sun X., Tian W., Wang Y. Toward Quantum-Resistant Strong Designated Verifier Signature from Isogenies. In: Intelligent Networking and Collaborative Systems (INCoS), 2012 4th International Conference on. IEEE: 292–296. DOI:10.1109/iNCoS.2012.70.

[22] Zhukov A.E. Cellular Automata in Cryptography. Part 1. Voprosy kiberbezopasnosti *[Cybersecurity issues]*, 2017, No 3(21), pp.70-76. DOI: 10.21681/2311-3456-2017-3-70-76.

[23] Zhukov A.E. Cellular Automata in Cryptography. Part 2. Voprosy kiberbezopasnosti *[Cybersecurity issues]*, 2017, No 4 (22), pp. 47-66. DOI: 10.21681/2311-3456-2017-4-47-66.