# Studying Formal Security Proofs for Cryptographic Protocols

Konstantin Kogos, Sergey Zapechnikov



# Studying Formal Security Proofs for Cryptographic Protocols

Konstantin G. Kogos and Sergey V. Zapechnikov

The National Research Nuclear University MEPhI (Moscow Engineering Physics Institute), 31 Kashirskoye shosse, Moscow, Russia

{KGKogos, SVZapechnikov}@mephi.ru

**Abstract.** This paper discusses the problem of teaching provable security in cryptography when studying information security. The concept of provable security is one of the most important in modern cryptography, soit is necessary to integrate it into the syllabus on cryptographic protocols. Now provable security is not rare thing in basic cryptography courses. However, security proofs for cryptographic protocols are far more complicated than for primitives. We suggest the way of embedding Sequence of Games technique, Universally Composability framework, module design of protocols and other techniques into the cryptography protocols course. Our experience of teaching formal security proofs for cryptographic protocols brings quite positive effect for students' research and development.

**Keywords:** Information Security Science, Syllabus, Information Security Training, Cryptography, Provable Security

## 1 Introduction

The study of any science should base on a solid theoretical foundation. In modern cryptography, such foundation is provable security methodology. Comparing to classical cryptography, it replaces the empirical approach of proving security with a strict formal proofs. Nowadays, the concept of provable security becomes prevalent in cryptography. University courses should present modern science and technology quite adequately. So, a lot of attention should be paid to provable security in contemporary university courses. We see that the concept of provable security was included in many cryptography classes all over the world, but there are still some gaps.

At first, current courses use ideas of provable security just for cryptographic primitives, but the provable techniques for cryptographic protocols not covered in the courses. At second, security proofs for modern cryptosystems become more and more complicated. So, it becomes quite difficult to introduce such advanced techniques into the syllabus. At third, a suite of representative examples should be chosen for teaching purposes, and it is not evident how to make these examplesquite didactic, and reachable for classwork and self-studying.

adfa, p. 1, 2017.

The purpose of our work is to suggest a concept of integration provable security into modern university courses on cryptographic protocols for students specializing in the area of information security. Why is it so important? Because there is a growing demand for specialists capable not only to correctly apply the already existing methods, but also to solve new cryptographic problems "on the fly".

The paper is organized according to the tasks we have solved to achieve the goal. Section 2 briefly presents some related works. After discussing main approaches to proving security in modern cryptography in section 3, we observe and analyze existing practices for studying provable security in the current cryptography courses in section 4. In section 5 we discuss in detail how to integrate provable security into the syllabus on cryptographic protocols and preceding courses, taking into account that provable techniques for protocols are different from techniques for primitives. In section 6 we suggest how to optimally embed so-called Sequence of Games approach for proving security of cryptographic protocols. Section 7 is devoted to problems of embedding so-called Universal Composability (UC) approach and some more advanced related techniques. In section 8 we outline our experience of teaching formal security proofs for cryptographic protocols and conclude that it brings some positive effects. Finally, we identify main results and future directions of the work.

## 2 Related works

Of course, there is a number of research focusing on optimizing syllabus on modern cryptography. Some wide-known massive open online courses (MOOCs) and university courses include provable security foundations. In our mind, the best examples are Cryptography course on Coursera [1], MIT course [2], Stanford course [3], UC Davies course [4] and some others. However, we are essentially interested not in the courses themselves, but in teaching methods.

We have carefully analysed a lot of textbooks and scientific papers used in teaching practice. In our opinion, the best textbooks based on provable security approach are [5 – 7]. Also, we used some well-written papers on advanced proving techniques, such as UC framework by Canetti [8], guides on Sequence of Games techniques by Shoup [9] and Pointcheval [10], reactive security concept [11], an idea of modular design of UC-composable protocols by Camenisch et al. [12]. It is worth noting that most of these papers require essential adaptation to be used effectively in teaching.

## 3 Provable security in cryptography

We have investigated many approaches to proving security of cryptographic algorithms and protocols in modern cryptography. Here we are going to outline briefly our view on a landscape of proof techniques (Fig. 1).

There are three fundamentally different approaches to reasoning and proving security of cryptographic constructions: information-theoretic security, computational security, and symbolic security.

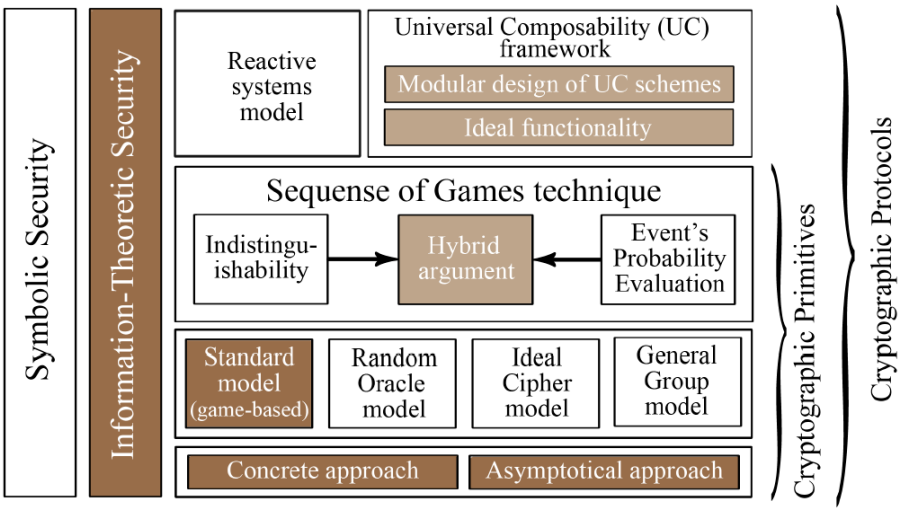


**Fig. 1.** A landscape of modern provable security methods

*Information-theoretic approach* is the oldest one. Shannon introduced it in the middle of 1940s [13]. It is well known, that the main idea of this approach is to provide a method of constructing cryptosystems secure against the computationally unlimited adversary. However, it is also well known, that the main drawback of such perfectly secure cryptosystems is its impracticality. For example, implementation of perfectly secure symmetric cipher must have key length no less than the plaintext length. But in some other applications perfectly secure cryptosystems are far more practical. Good examples are Shamir's secret sharing scheme [14] and Pedersen's verifiable secret sharing and commitment schemes [15], which play an important role in modern cryptographic constructions.

*Computational security* is the leading approach in modern cryptography. Goldwasser and Micali introduce it in the middle of 1980s [16], and Goldwasser, Micali and Rackoff extended it to cryptographic protocols soon [17].

At first, such proof requires a definition of secure cryptographic construction (primitive, protocol, scheme). Secondly, some suggestion about the computationally infeasible problem has to be made. Next, a construction solving the task is offered and a mathematical proof that the construction satisfies the definition must be outlined assuming existence of the infeasible problem. As a rule, the proof makes sure that only chance to violate the security of such a construction is to solve the above-mentioned infeasible task.

We believe it is convenient to allocate some "layers" in modern computationally secure proving techniques.

The lowest layer complies of two basic definitional concepts of security measuring – concrete approach and asymptotical approach. The first one was developed by Goldwasser [7], the last one – by Goldreich [18].

The second level is composed of some proving models using certain definitional approach. They bring a "mechanics" of proving assuming some agreements. Well-

known examples are standard model (game-based), random oracle model, ideal cipher model, generic group model (we do not discuss here the specificity of each model).

The next level is Sequence of Games technique. When a proof becomes too complicated, it should be presenred as a series of steps replacing security against ideal adversary to security against real one. Each step could be performed based on indistinguishability argument or event's probability evaluation. If both arguments are combined, this is so called hybrid argument. Sequence of Games technique with hybrid argument is one of the main tools for proving security of cryptosystems.

All three levels are necessary for proving security of cryptographic primitives and relatively simple cryptosystems. However, such levels are not sufficient for complicated cryptosystems composed of many building blocks such as zero-knowledge proofs, commitments and so on. Some kind of simulating cryptosystem's behavior model is desirable for such systems. That is why the forth level of computational security proofs goes on stage. The most known examples are Canetti's UC model [8] using ideal functionalities and reactive systems model [11] simulating dynamically interactive communities. However, when using all these techniques, the monolithic proofs obtained for complicated cryptographic constructions, are very difficult for synthesis and verification. Recently, some techniques to manage this complexity have been offered, for example, UC commitments for modular protocol design [12].

Currently, *symbolic security* approach has a limited scope in cryptography, but it is quite efficient for some protocols, such as key establishment. The first such technique – so-called BAN-logic was invented in 1990 [19]. Some other techniques were introduced in subsequent years, i.e. GNY-logic [20]. Tamarin is one of the currently evolving tools [21]. The main advantage of symbolic techniques is their easy automation. The drawback is that only special types of protocols can be analysed this way.

## 4 Provable security in current cryptography courses

As we noted earlier, provable security is an important part of many MOOC and university cryptography courses. Most of them include only historical Shannon's approach and basic computational security techniques. Of course, Shannon's perfect security idea is inavoidable element of cryptography syllabus. It should be emphasized to students, that Shannon was the first to find strong mathematical evidence of information security. His approach became the reference for all subseguent ones.

Computational security is the most usable approach, so it should be represented fully enough in the course. Existing practices mostly include definitional concepts and standard (game-based) model, in other words, first and second level of our landscape (Fig, 1). These are the most fundamental techniques, which ware used for analyzing security of basic symmetric and asymmetric cryptoschemes.

Of course, it is difficult to have enough time to combine both concrete and asymptotical approaches in one course, so just one definitional approach is used in every course. Examples of courses based on concrete security are [4, 7], and courses based on asymptotical security are [5, 6]. According to our research, asymptotical-based courses are far more common. More than 60 universities use it according to [22].

The second element of typical cryptography course is standard game-based model of proving security. The main idea of game-based security model is simulation of interaction among the adversary and responder (prototype of real-world party). It allows to prove that any supposed adversary can get an advantage over the responder if and only if she is able to solve some computationally infeasible problem (i.e., discrete logarithm, Diffie – Hellman, integer factorization etc.).

Symbolic security is rarely used in modern cryptography courses.

Thus, the main conclusion from the analysis of currently taught courses is the following. Currently, just basic methods of provable security are represented in cryptography courses. Evidently, the knowledge of them may be incomplete for construction and analyzing modern crypto algorithms and protocols. So, it is necessary to integrate advanced provable security techniques and tools into the syllabus not only on foundations of cryptography but also on cryptographic protocols.

## 5 Integrating provable security into the syllabus on cryptographic protocols

One of the main factors to expand provable security techniques in research and in training courses is a complication of cryptosystems' structure. Our view on the architecture of modern cryptosystems is shown on Fig. 2. There are several levels in every complicated cryptosystem:

- basic mathematical facts;
- cryptographic primitives, including engineering (confucion/diffusion) and algebraic/combinatorial;
- cryptographic algorithms (fucntions), including one-key (symmetric), two-key (asymmetric) and no-key algorithms;
- building blocks of cryptographic protocols, such as zero-knowledge proofs, key management infrastructure etc.;
- cryptographic protocols, including two-party and multi-party protocols;
- cryptographic schemes (security mechanisms);
- cryptographic systems (security services);
- security systems, including cryptographic and non-cryptographic security services.

We do not comment this scheme in details, so it is confirmed by wide analysis of numerous modern cryptosystems. We use this scheme as a framework for "Cryptographic protocols" course.

It is easy to notice that architecture on Fig. 2 is quite well correlated with the landscape on Fig. 1. Thus, the above-mentioned levels of proving techniques can be projected on the levels of cryptosystems' architecture. We identify on Fig. 1 a subset of proving techniques that is now included in typical cryptography course (dark grey blocks) and that we recommend including in the syllabus additionally (light grey blocks). Briefly, we recommend to add in syllabus the following:

- Sequence of Games technique, more precisely, hybrid argument method;

- Universal Composability framework and its extensions.

We will analyze special aspects of integrating of these techniques in next sections.

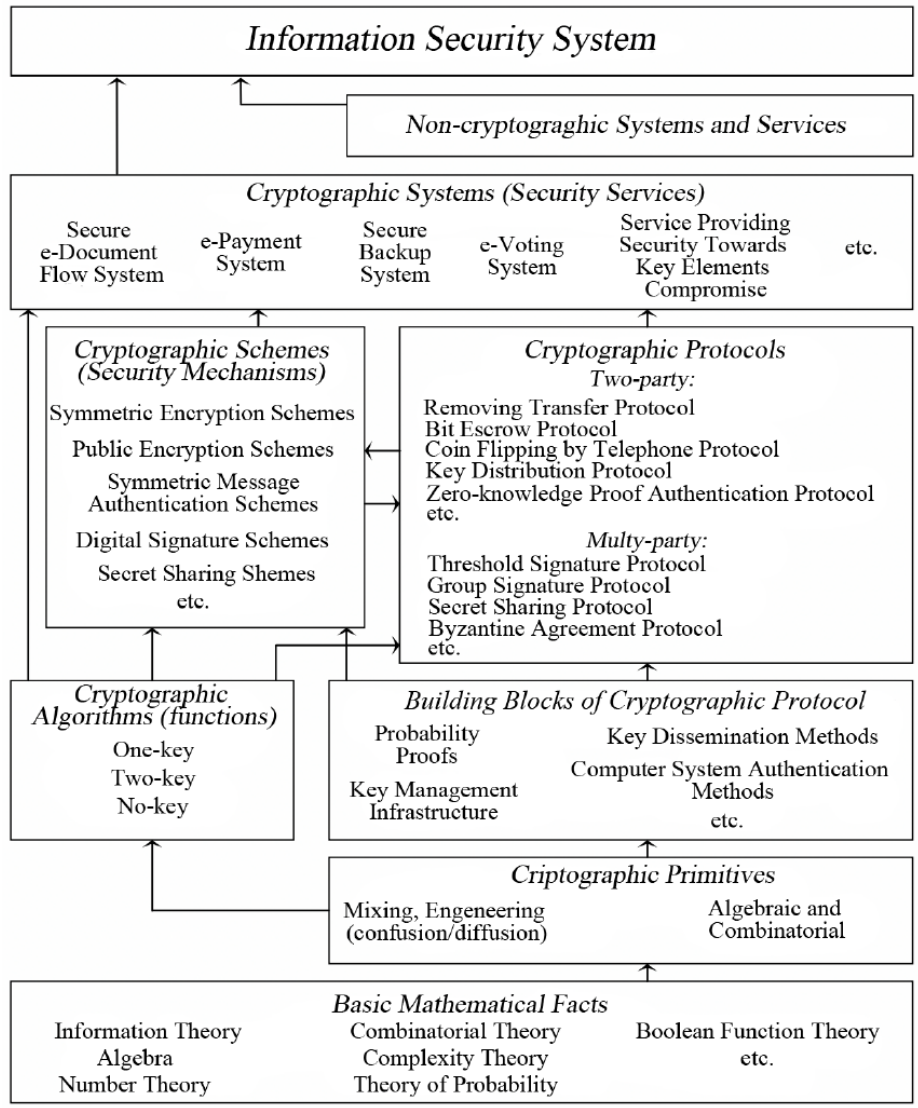


**Fig. 2.** Architecture of modern cryptosystems

## 6 Embedding Sequence of Games technique

Sequence of Games is a popular tool for structuring security proofs for cryptographic protocols and schemes. The purpose of this technique is to tame the complexity of security proofs that otherwise is so difficult as to repeat and verify is nearly impossi-

ble [9]. It is not a silver bullet, of course. As Shoup righteously notes, it is only a tool for organizing actual ideas for cryptographic constructions and security analysis.

The essence of this approach is as follows. To prove security one constructs a sequence of *N* games among the adversary and cryptographic primitive or protocol. The first game in the sequence is the original adversary's attack on the construction. Changes between successive games are minor, so probabilities of events connected to adversary's success or failure, differ very slightly. So, the last game in the sequence is ideal and a target probability of an event is typically either 0 or1/2 (i.e. probability that an adversary can guess, which of two plaintexts corresponds to given ciphertext).

This is quite powerful method. However, we stress that it was developed in scientific environment for research purposes, so it has to be adapted for teaching purposes. So, we note that for pedagogical purposes two aspects are necessary: inevitable simplifying of the technique and carefully selected examples.

To simplify the explanation of Sequence of Games technique for students we recommend limiting the types of possible transitions among games to transitions based on indistinguishability of 2-3 computationally infeasible problems (preferably, the discrete logarithm nad the Diffie – Hellman problems, integer factorization and the RSA problems, and, may be, the Bilinear Diffie – Hellman problem for advanced students), and also transitions based on failure events that students should be able to evaluate (i.e., probability to find collisions of hash functions).

As regards the examples, we select the following:

- some variants of Luby – Rackoff construction for building a pseudo-random permutation family and one of authenticated encryption modes for "Symmetric cryptography" course;
- El Gamal public key encryption scheme without message hashing and with it and also FDH-RSA scheme for "Asymmetric cryptography" course;
- chosen ciphertext secure symmetric encryption (prototype of TLS protocol), one of the provably secure group key establishment protocols (we used protocols from TDH1 family [23]) and oblivious transfer (we used protocols from [24]) for "Cryptographic protocols" course.

The above-mentioned examples of proofs for cryptographic protocols are quite tricky, so the tutor should explain them as clearly as possible. But we insist that so non-trivial examples should be presented in university courses because of their importance and representativeness.

## 7 Embedding Universal Composability framework

Universal Composability is one of the most powerful techniques of provable security in cryptography invented by Canetti in 1990s [8].

The essence of the approach is in its ability to simulate cryptographic protocol properties when many sessions of analyzed protocols along with other protocols are executed in parallel. The UC framework allows specifying the security requirements of most of cryptographic tasks in a unified manner. The advantage of this technique is

the possibility of designing complex protocols from relatively simple building blocks. The security of separate protocols is preserved under a composition. The kernel of protocol analysis under UC approach lies in the specification of protocol's ideal functionality and comparison it with execution in the real-world environment to prove that difference among real and ideal executions is negligible. This approach is widely used in research. It is not always used strictly in Canetti's form [25], but many of its elements can be composed with other techniques, such as above-mentioned Sequence of Games and other modular desing techniques.

The UC approach also requires adaptation for teaching purposes. We think, it is sufficient to inform students about main ideas of UC approach, without unnecessary details. The main things are Canetti's Composition theorem (proof is unnecessary) and technique for constructing ideal functionality based on virtual trusted third party.

We recommend the following well-documented examples for using during the studying the UC approach in classwork and homework: universally composable symmetric encryption [26], universally composable undeniable signatures [27], universally composable key management [28], universally composable role-based access control [29]. How to work with such examples? We recommend to analyze one of them in details in class and set analyzing slightly modified variant of one of the other schemes as a homework. It will require to make changes in the proof in many places of ideal functionality model, real protocol, game between the adversary and party of protocol and so on. Thus, students will learn how to construct proofs by themselves.

## 8 Experience of teaching formal security proofs for cryptographic protocols

Our ideas were embedded into the "Cryptographic protocols" course for graduate students in MEPhI. To measure an effect of changing the syllabus we have tested our students (60 people) studied on old and new syllabuses. In particular, the students had to solve some tasks when they passed all three courses:

- to prove the security of some simple RSA modifications;
- to prove the security of some variants of Luby-Rackoff construction;
- to prove the security of universally composable symmetric encryption scheme [26].

The result of students studying courses before their changing is as follows. 80 percent of students dealt with the first task, 20 percent of students got through the second task and nobody was successful with the third task. Such a result was not surprising, so the first task is easily solvable by most students with basic mathematical background, the second task is quite complicated for students not familiar with advanced provable security techniques, the third task is actually unsolvable by students without high-level qualifications in provable security.

Students studying courses after our changings showed significant improvement. 80 percent of students were still successful with the first task, but 60 percent of students got through the second task and about 25 percent of students were successful with the third task. It was predictable that the number of students dealt with the first task

would not change (it is not a difficult task). But the rate of students that were successful with the second and the third tasks has essentially increased.

## 9 Conclusion

Summarizing the results of our work, we conclude with the following.

1. A new pedagogical idea was formed. Its essence is to integrate modern provable security techniques into the "Cryptographic protocols" course and improve basic cryptography cources to harmonize them with the provable security based cryptographic protocols course.
2. Views on a suite of current provable security techniques and architecture of modern cryptosystems are offered. Proposals on embedding some proving techniques in the curriculum on cryptographic protocols were formulated.
3. New techniques of teaching cryptographic protocols based on constructing and proving security of prototypes or slightly modified real-life protocols were offered. A set of examples and use cases on proving techniques was selected.

Most of our findings are original, and they were tested on the graduate students specializing in the area of information security. Our experience indicates that integrating our approach has some positive effect, including improving students' competences and more active participation in research and innovations. We plan to improve our crypto syllabuses to monitor the leading crypto tracks.

**Acknowledgement.** This work was supported by Competitiveness Growth Program of the Federal Autonomous Educational Institution of Higher Professional Education National Research Nuclear University MEPhI (Moscow Engineering Physics Institute).

## References

1. Boneh D. Cryptography I. URL: https://www.coursera.org/learn/crypto (access date: 28.01.2017)
2. Cryptography and Cryptanalysis. MIT Open Courseware. URL: https://ocw.mit.edu/courses/electrical-engineering-and-computer-science/6-875-cryptography-and-cryptanalysis-spring-2005/ (access date: 28.01.2017)
3. Maurer U. Cryptography Foundations. 2016. URL: http://www.crypto.ethz.ch/teaching/lectures/Crypto16/ (access date: 28.01.2017)
4. Rogaway P. Cryptography course. URL: http://web.cs.ucdavis.edu/~rogaway/classes/127/spring16/ (access date: 28.01.2017)
5. Katz J., Lindell Y. Introduction to modern cryptography. 2nd ed. CRC Press. 2015. 598 pp.
6. Boneh D., Shoup V. A graduate course on applied cryptography. 2015. 400 pp. URL: https://crypto.stanford.edu/~dabo/cryptobook/ (access date: 28.01.2017)
7. Goldwasser S., Bellare M. Lecture notes on cryptography. 2008. 289 pp. URL: https://cseweb.ucsd.edu/~mihir/papers/gb.pdf (access date: 28.01.2017)
8. Canetti R. Universally Composable Security: A New Paradigm for Cryptographic Protocols. 2001. URL: http://eprint.iacr.org/2000/067.pdf (access date: 28.01.2017)

9. Shoup V. Sequences of games: a tool for taming complexity in security proofs. 2004. URL: http://eprint.iacr.org/2004/332.pdf (access date: 28.01.2017)
10. Pointcheval D. Contemporary cryptology provable security for public key schemes. Advanced Courses CRM Barcelona, pages 133-189, June 2005. ISBN: 3-7643-7294-X.
11. Backers M., Pfitzmann B., Waidner M. The reactive simulatability (RSIM) framework for asynchronous systems. Information and Computation. Vol.205, Issue 12. Dec. 2007. Pp. 1685-1720.
12. Camenisch J., Dubovitskaya M., Rial A. UC commitments for modular protocol design and applications to revocation and attribute tokens. URL: http://eprint.iacr.org/2016/581 (access date: 28.01.2017)
13. Shannon C. Communication Theory of Secrecy Systems. Bell System Technical Journal, vol. 28(**4**), 1949. pp. 656–715.
14. Shamir A. How to share a secret. Comm. of the ACM. 1979. No. 22. Pp. 612-613.
15. Pedersen T.P. Non-interactive and information-theoretic secure verifiable secret sharing. Adv. in Cryptology. Proc. of CRYPTO'91. Springer-Verlag, 1992. Pp.129-140.
16. Goldwasser, S., and S. Micali. Probabilistic Encryption. Journal of Computer and Systems Sciences 28, no. 2 (1984): 270-299. New York, NY: Academic Press.
17. Goldwasser, S., S. Micali, and C. Rackoff. The Knowledge Complexity of Interactive Proof-Systems. SIAM Journal on Computing 18, no. 1 (1989): 186-208. Philadelphia, PA: Society for Industrial and Applied Mathematics.
18. Goldreich O. Foundations of modern cryptography. Vol.1 – Basic Tools. Vol. 2 – Basic applications. Cambridge university press. 2004.
19. Burrows B., Abadi M., Needham R. A logic of authentication. ACM Transactions on computer System. Vol. 8. 1990. No. 1. Pp. 18 – 36.
20. Gong L., Needham R., Yahalom R. Reasoning about belief in cryptographic protocols. Proc. of the IEEE Computer Society Symposium on Research in Security and Privacy, 1990. Pp. 234 – 248.
21. Meier S., Schmidt B., Cremers C., Basin D. The TAMARIN prover for the symbolic analysis of security protocols. International Conference on Computer Aided Verification (CAV 2013). LNCS 8044. Springer, 2013. Pp 696 – 701.
22. Introduction to Modern Cryptography book's site. URL: http://www.cs.umd.edu/~jkatz/imc.html (access date: 28.01.2017)
23. Manulis M. Provably secure group key exchange. Ph.D. theses. 2007. 225 pp. URL: http://manulis.eu/papers/psgke.pdf (access date: 28.01.2017)
24. Dubovitskaya M. Cryptographic protocols for privacy-preserving access control in databases. Ph.D. theses. 2014. 213 pp. URL: http://e-collection.library.ethz.ch/eserv/eth:14431/eth-14431-02.pdf (access date: 28.01.2017)
25. Canetti R., Cohen A., Lindell Y. A simpler variant of universally composable security for standard multiparty computation. URL: https://eprint.iacr.org/2014/553.pdf (access date: 13.03.2017).
26. Kuesters R., Tuengerthal M. Universally composable symmetric encryption. URL: http://eprint.iacr.org/2009/055 (access date: 28.01.2017)
27. Kurosawa K., Furukawa J. Universally composable undeniable signature. URL: http://eprint.iacr.org/2008/094 (access date: 28.01.2017)
28. Kremer S., Kunnemann R., Steel G. Universally composable key-management. URL: http://eprint.iacr.org/2012/189 (access date: 28.01.2017)
29. Liu B., Warinschi B. Universally composable cryptographic role-based access control. URL: http://eprint.iacr.org/2016/902 (access date: 28.01.2017)