VII Workshop
Current Trends in Cryptology
CTCrypt'18

May 28-30, 2018
Suzdal

Dear colleagues!

For seven consecutive years the «Current Trends in Cryptology» workshop gathers together leading national and foreign cryptography specialists. The year 2018 has seen 23 papers provided by authors from 5 countries. 16 papers have been included into the workshop program after a thorough review by members of a program committee, which is traditionally international.

I would like to point out that this year an issue of including of some articles into the program provoked a lot of debates among the program committee members. At the same time, since the workshop is a place to share new ideas, views, and conceptions it was unanimously agreed to give authors of the disputable articles an opportunity to represent the results of their researches and to talk them over with the workshop's audience.

More than 100 delegates from 9 countries all over the world have registered for participation in the 7th workshop. The number approximately corresponds to that of the previous years.

Subject of the included to the workshop program articles is vast and cover issues concerning synthesis and analysis of specific cryptographic mechanisms as well as fundamental problems of cryptography. An actively discussed post-quantum cryptography will be also mentioned.

In accordance with an established practice, scientific part of the Workshop will be enlarged by panel discussions of the most actual and urgent cryptography issues. Traditionally, the discussions are attended by representatives of cryptographic devices developers and producers, scientific community and regulatory authorities. Two panel discussions with an extremely pressing subjects, in our opinion, will be organized this year. The first one will be dedicated to the role and place of cryptography in digitalization of the society and, particularly, within the current «Digital Economy of the Russian Federation» program.

The second one will be devoted to the issues concerning peculiarities and distinctive aspects of blockchain and distributed ledger technology-based systems. Similar issues were raised within a last year's workshop panel discussion that appeared to be successful both in the entry list and discussed topics. This year we are to discuss, among others, changes in views on these technologies and on approaches of its implementation have undergone over the past year as well as issues of realization and non-realization of announced projects.

The workshop «Current Trends in Cryptology» has proved itself to be the place where everyone can take a look at state-of-the-art results of the researches conducted by foreign cryptography specialists and, moreover, ask them questions in person. Lightweight cryptography – one of the most popular direction of modern cryptography – is the subject of the report to be delivered by Thomas Peyrin. Phillip Rogaway, one of the «provable security» founders, will speak on authenticated encryption, another equally discussed issue. Aleksandr A. Nechayev's disciple Oleg Kozlitin, invited speaker of the Academy of Cryptography of the Russian Federation – one of the organizers of the Workshop – will share his research results in mathematical problems in cryptography.

The range of the discussed questions, high level professionalism participants, and impartial selection of papers allows to consider the workshop «Current Trends in Cryptology» to be a leading Russian scientific forum on cryptography.

Dear colleagues, we are facing three days of difficult but interesting work the results of which, I hope, will allow to develop the existing approaches and lay the groundwork for the new ones to solve the tasks which the modern society comes across increasingly in course of digitalization.

Thereon I would like to declare the 7th workshop «Current Trends in Cryptography» open.