



Math-Net.Ru

All Russian mathematical portal

Information on the Symposium CTCrypt'2019,  
*Mat. Vopr. Kriptogr.*, 2020, Volume 11, Issue 2, 5–6

<https://www.mathnet.ru/eng/mvk345>

Use of the all-Russian mathematical portal Math-Net.Ru implies that you have read and agreed to these terms of use

<https://www.mathnet.ru/eng/agreement>

Download details:

IP: 18.97.9.169

April 19, 2025, 05:56:06



## Информационное сообщение о симпозиуме СТСcrypt'2019

С 4 по 7 июня 2019 года в г. Светлогорске Калининградской области состоялся VIII симпозиум «Современные тенденции в криптографии» (СТСcrypt'2019), в работе которого приняли участие более 140 специалистов из 7 стран мира.

СТСcrypt'2019 стал важным международным научным событием в России, посвященным теоретическим и практическим аспектам криптографии. Для участия в научной программе симпозиума было представлено 37 работ, что почти в два раза больше, чем в 2018 году. Возросшее число докладов свидетельствует о понимании научным сообществом важности вопросов обеспечения информационной безопасности.

В программу симпозиума вошли доклады по широкой тематике. Особенный интерес вызвали вопросы синтеза и анализа как классических блочных и поточных криптографических алгоритмов, так и широко обсуждаемых в последнее время постквантовых криптографических механизмов, способных противостоять криптографическим атакам с использованием квантовых вычислителей.

Отличительной особенностью симпозиума СТСcrypt является включение в научную программу приглашенных докладов ведущих отечественных и зарубежных специалистов. В 2019 году таких докладов было три. Первый подготовили Андрей Пичкур и Алексей Тарасов, посвятив его памяти действительного члена Академии криптографии Российской Федерации профессора Михаила Михайловича Глухова — одного из основателей российской алгебраической криптографической школы. Второй доклад прочитал ведущий специалист в области постквантовой криптографии на основе изогений эллиптических кривых Лука де Фео, и третий, представляющий новую версию протокола TLS, — профессор Швейцарской высшей технической школы Цюриха Кеннет Патерсон.

В рамках симпозиума были проведены также два круглых стола. Первый был посвящен создаваемому в России музею криптографии, а второй — деятельности лаборатории проблем стандартизации в области криптографии и безопасности информационных технологий, созданной в Академии криптографии Российской Федерации в рамках национальной программы «Цифровая экономика Российской Федерации».

Во время симпозиума в порядке эксперимента научная программа была дополнена популярными лекциями по криптографии для специ-

алистов в области защиты информации и школьников старших классов. В первом случае в роли лекторов выступили ведущие специалисты компаний-разработчиков средств криптографической защиты и эксперты технического комитета по стандартизации ТК 26 «Криптографическая защита информации». Преподаватели Института криптографии, связи и информатики — ведущего вуза страны, осуществляющего подготовку специалистов-криптографов, — устроили увлекательные выездные занятия для калининградских школьников, завершившиеся захватывающим криптографическим соревнованием.

Всего для участия в симпозиуме было отобрано 22 доклада, часть из них публикуется в настоящем и следующем выпусках журнала. В соответствии с правилами симпозиума статьи публикуются на английском языке с аннотациями на русском языке.

**Оргкомитет симпозиума**