РусКрипто

XXVIII НАУЧНО-ПРАКТИЧЕСКАЯ КОНФЕРЕНЦИЯ

Научно-академическая работа: опыт «Кода Безопасности»

Алиса Коренева, к.ф.-м.н.
Заместитель руководителя службы сертификации по научно-техническому сотрудничеству

Социальная миссия Компании

- Помощь в формировании и понимании культуры ИБ
- Сопровождение будущего специалиста
- Стажировки и практики
- Работа в реальной компании, карьерный рост

«Код Безопасности» ведет активное сотрудничество с ~100 учебными заведениями, которые занимаются профессиональной подготовкой, переподготовкой и повышением квалификации **специалистов в области защиты информации**. Компания содействует повышению качества обучения и принимает деятельное участие в развитии системы высшего и специального образования в России благодаря **некоммерческой Программе популяризации знаний в области ИБ.**

https://www.securitycode.ru/company/training/

Социальная миссия Компании

Школьник

- Экскурсии в компанию, встречи с экспертами Компании
- Рассказы о профессиональных ролях в IT-компании и процессе разработки
- Методическая поддержка профильных классов (задачи, виртуальные стенды)
- Развитие двусторонних и трехсторонних соглашений о сотрудничестве в области образования и профориентации школьников (школа + ВУЗ+ работодатель)

Студент

- Разработка и передача в ВУЗы методических пособий и стендов
- Экскурсии в компанию
- Базовые кафедры и лаборатории
- **Специализированные обучающие курсы и мастер-классы**
- **Организация интересных практик и стажировок**
- Руководство ВКР и проведение конкурсов ВКР
- **Участие и поддержка олимпиад**
- Ежегодная поддержка соревнований CTF

Специалист

- Специализированные курсы с виртуальными стендами, пособиями и презентациями
- Технические семинары – целевая аудитория инженеры, работающие с реальными кейсами
- Доступ к Базе знаний «Кода Безопасности»
- Вебинары и видео-инструкции по актуальным обновлениям и трендам и в отрасли
- Мастер-классы и доклады на всероссийских конференциях по ИБ

Школа Кода Безопасности

2019

Проведение первой школы «Кода Безопасности»

Бесплатный образовательный проект

- Для желающих повысить уровень своего профессионализма в вопросах ИБ
- Участники – все желающие, студенты и недавние выпускники ВУЗов и колледжей
- Спикеры – ведущие эксперты и специалисты компании «Код Безопасности»

Каждый участник имеет возможность получить именной сертификат, который даст преимущество при собеседовании на работу или стажировку в «Код Безопасности». Для получения сертификата необходимо успешно выполнить задания курса.

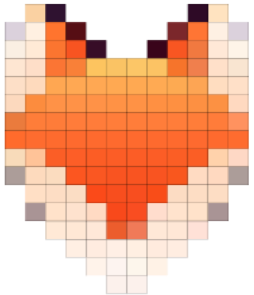
Криптографы Кода Безопасности

Криптографы Кода Безопасности

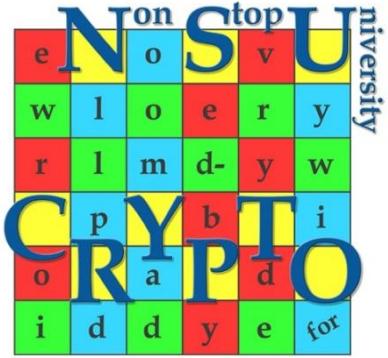
- R&D в области криптографии
- Участие в научно-исследовательских проектах и рабочих группах технических комитетов
- Преподавание в ведущих ВУЗах страны
- Публикации в научных изданиях и выступления на профильных конференциях

Олимпиады и научные школы

CryptoFox



NSUCrypto



- Возможность предложить студентам нестандартные задачи, которые возникают в нашей работе
- Продвижение Компании, как заинтересованной в кадрах, способных к нестандартному мышлению и решению сложных задач
- Реализация нашего творческого научного потенциала

Участие в NSUCrypto 2016 – 2025

	GF2	Alisa Koreneva	Russia	Moscow	MEPhI	12

https://nsucrypto.nsu.ru/archive/2016/total_results/#data

Олимпиада предлагает интересные практико-ориентированные, математические и криптографические задачи, некоторые из которых являются **нерешенными проблемами мировой науки**. В ходе решения одной из задач была усовершенствована идея низкоресурсной модификации коммерческого шифра КБ-256, разработанного сотрудниками «Кода Безопасности».

https://t.me/s/Kodnaprovode

Задача для NSUCrypto 2025

Технологические тренды / Борьба с новым поколением рисков и угроз

6 КВАНТОВО-УСТОЙЧИВАЯ КРИПТОГРАФИЯ
(Post-Quantum Cryptography)

Gartner: к 2029 году возможная угроза применения квантовых вычислений сделает традиционную криптографию небезопасной. Переход к квантово-устойчивой (постквантовой криптографии) стоит начинать уже сейчас.

Исследование Ассоциации Финтех «3х10 трендов 2025 года»:
https://www.fintechru.org/press-center/issledovaniya/3kh10-trendov-2025-goda/

Задача для NSUCrypto 2025

КОМПАНИЯ АКТИВ

КОД безопасности

International Olympiad in Cryptography NSUCRYPTO'2025
Second round October 13–20 General, Teams

Problem 2. «Studying quantum security»

Problem for a special prize!

Starting from papers of O. Goldreich, Sh. Goldwasser, and S. Micali cryptographers study how to construct random functions. Ok, let the function be random if *it looks random* to adversaries. It is possible to define a *pseudorandom function (PRF)* / *pseudorandom permutation (PRP)* as a function/permutation with the following property: no efficient classical algorithm, when given oracle access, can distinguish it from a truly random function/permutation.

There are some modern variants of modeling quantum adversaries for ciphers, see the paper M. Kaplan, G. Leurent, A. Leverrier «Quantum Differential and Linear Cryptanalysis» // IACR Transactions on Symmetric Cryptology, Vol. 2016, No. 1, pp. 71–94. DOI: 10.13154/tosc.v2016.i1.71-94. Namely, there are

Standard security: a block cipher is *standard secure* against quantum adversaries if no efficient quantum algorithm can distinguish the block cipher from PRP (or a PRF) by making only *classical* queries (denote this type as Q1).

Quantum security: a block cipher is *quantum secure* against quantum adversaries if no efficient quantum algorithm can distinguish the block cipher from PRP (or a PRF) even by making *quantum* queries (denoted this type as Q2).

The Q2 model of attacks assumes that an adversary can query a quantum cryptographic oracle in superposition. This model can be implemented, when an algorithm under analysis runs on a quantum computer with adequate resources. It is known that most of standardized modes of operation for block ciphers are insecure in the Q2 model. You can read about it for example in the paper M. V. Anand, E. E. Targhi, G. N. Tabia, and D. Unruh «Post-quantum Security of the CBC, CFB, OFB, CTR, and XTS Modes of Operation» // Lecture Notes in Computer Science, Vol. 9606, pp. 44-63, 2016. DOI: 10.1007/978-3-319-29360-8_4. This means that such block ciphers modes of operation can be considered broken after appearing a quantum computer with resources enough for implementing an attacked algorithm.

Propose and describe a new (previously unknown) block cipher mode of operation secure in the Q2 model, and justify its security in the Q2 model.

Block cipher modes for quantum security?

https://nsucrypto.nsu.ru/archive/2025/round/2/task/2/#data

Спасибо
за внимание!

РусКрипто XXVIII НАУЧНО-ПРАКТИЧЕСКАЯ КОНФЕРЕНЦИЯ

Коренева Алиса Михайловна,
a.koreneva@securitycode.ru