Отзыв

на автореферат диссертации Нестеренко Алексея Юрьевича на тему «Математические методы обеспечения защищенного взаимодействия средств защиты информации», представленной на соискание ученой степени доктора физико-математических наук по специальности 2.3.6 «Методы и системы защиты информации, информационная безопасность»

Целью диссертационной работы Нестеренко А.Ю. является развитие методов построения криптографических протоколов, применяемых для обеспечения защищенного обмена информацией по открытым каналам связи, а также методов получения обоснованных оценок безопасности криптографических протоколов.

Актуальность полученных в диссертационной работе результатов обусловлена повсеместным использованием криптографических протоколов для защиты информации, циркулирующей в сети «Интернет», в автоматизированных системах управления, а также, для защиты критической информационной инфраструктуры Российской Федерации.

В диссертационной работе получены следующие **новые** результаты:

- метод дискретного логарифмирования в группе точек эллиптической кривой, в основе которого лежит алгоритм Госпера поиска двух совпадающих элементов последовательности, и получена асимптотическая оценка трудоемкости предложенного метода;

- доказана теорема о существовании алгоритма дискретного логарифмирования в группе точек эллиптической кривой, использующего информацию о мульти пликативном порядке неизвестного;

- введено понятие «слабого» ключа и определено значение средней трудоемкости алгоритма дискретного логарифмирования в группе точек эллиптической кривой.

- получено точное количество «слабых» ключей для эллиптических кривых, параметры которых содержатся в рекомендациях по стандартизации Р 1323565.1.024-2019;

- предложен алгоритм вычисления явного представления эндоморфизмов эллиптических кривых;

- предъявлены ранее не известные эндоморфизмы для всех эллиптических кривых, чье кольцо эндоморфизмов изоморфно порядку мнимого квадратичного поля с числом классов равным единице;

- предъявлены усиленные, по сравнению с ГОСТ Р 34.10-2012, требования к параметрам эллиптических кривых, рекомендуемых к применению в средствах защиты информации;

- приведены явные значения параметров построенных автором диссертационной работы эллиптических кривых;

- предложены новые алгоритмы представления действительных чисел специального вида в виде систематической дроби по произвольному основанию и способ применения предложенных алгоритмов для выработки псевдослучайных последовательностей;

- предложены алгоритмы восстановления неизвестных коэффициентов по известному рациональному приближению числа специального вида;

- предложен метод локальной аутентификации пользователей средств защиты информации, основанный на алгоритме представления действительных чисел специального вида в виде систематической дроби по произвольному основанию;

- определен новый класс ключевых равновероятных функций хеширования, представляющих собой линейные формы от перестановок на множестве кодов аутентификации;

- предложен режим аутентифицированного шифрования, в основе которого лежит построенный класс равновероятных ключевых функций хеширования;

- построена гибридная схема, реализующая процесс шифрования с помощью полиномиального преобразования;

- предложен новый протокол выработки общего ключа со взаимной аутентификацией субъектов взаимодействия;

- предъявлена формальная модель, имитирующая криптографический протокол в виде дискретной динамической системы, формализован перечень свойств безопасности и определены показатели эффективности мер защиты;

- предложена методика проведения исследования безопасности криптографических протоколов.

К тексту автореферата имеется ряд замечаний.

1. На стр. 8 имеется опечатка в перечне конференций и семинаров, на которых докладывались результаты автора, также имеются несогласованные предложения на стр. 31 и 32.

2. На стр. 25 во втором и третьем абзацах сверху основание логарифма должно принимать значение b, а не r, как указано в тексте автореферата.

Перечисленные замечания носят редакционный характер и не затрагивают научной сути диссертации.

Тема, объект и предмет исследований диссертации соответствуют паспорту научной специальности «Методы и системы защиты информации, информационная безопасность» по направлениям исследований, указанным в тексте автореферата.

Диссертация соответствует требованиям, предъявляемым к диссертациям на соискание учёной степени доктора физико-математических наук, и является существенным продвижением в решении крупной научной проблемы обеспечения стойкости криптографических протоколов.

Учитывая все вышеизложенное, считаю, что Нестеренко Алексей Юрьевич заслуживает присуждения ученой степени доктора физико-математических наук по специальности 2.3.6 «Методы и системы защиты информации, информационная безопасность».

Директор РУНЦ «Безопасность»
МГТУ им. Н.Э. Баумана, д.т.н., профессор М.П. Сычев

«09» октября 2023 года.

Ведущий научный сотрудник РУНЦ «Безопасность»
МГТУ им. Н.Э. Баумана, к.т.н., доцент А.В. Астрахов

Московский государственный технический университет имени Н.Э. Баумана
Адрес: 105005, г. Москва, ул. 2-я Бауманская д.5, стр.1
Тел. 8-495-632-22-47, e-mail: runc@bmstu.ru