Экз. № 1

МИНОБРНАУКИ РОССИИ
федеральное государственное автономное
образовательное учреждение высшего образования
«Санкт-Петербургский политехнический
университет Петра Великого»
(ФГАОУ ВО «СПбПУ»)

ИНН 7804040077, ОГРН 1027802505279,
ОКПО 02068574
Политехническая ул., 29, Санкт-Петербург, 195251
тел.: +7(812)297 2095, факс: +7(812)552 6080
office@spbstu.ru

Председателю
диссертационного совета МГУ 012.3
ФГБОУ ВО «Московский государственный
университет имени М. В. Ломоносова»,
академиуку РАН, д. ф.-м. н., профессору
Садовничему Виктору Антоновичу

119234, г. Москва, ГСП-1, Ленинские горы,
д. 1, Главное здание МГУ

ОТЗЫВ

на автореферат диссертации
НЕСТЕРЕНКО Алексея Юрьевича
«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

Актуальность выполненного исследования обусловлена развитием информационных систем и технологий хранения, передачи и обработки данных и необходимостью их защиты. Тема, цель и задачи исследования согласуются с Доктриной информационной безопасности РФ, Федеральным законом «О безопасности критической информационной инфраструктуры Российской Федерации», постановлением Правительства РФ о реализации государственной программы «Информационное общество».

Для использования средств обеспечения информационной безопасности они в обязательном порядке должны пройти процедуру сертификации на соответствие предъявляемым к ним требованиям ФСТЭК и ФСБ России. В частности, для криптографических средств (алгоритмов, схем, протоколов) необходимо иметь научно обоснованные оценки их стойкости и эффективности — только в этом случае возможна дальнейшая их стандартизация и использование на практике. В этой связи поставленная в диссертационном исследовании ***научная проблема*** *построения и математического обоснования безопасности криптографических протоколов, применяемых для обеспечения защищенного обмена информацией по открытым каналам связи*, является ключевой.

Научная новизна исследования заключается в том, что:

– разработан математический аппарат, позволяющий строить криптографические протоколы и их формализованные модели на основе предъявляемых требований по безопасности;

– получены новые методы и алгоритмы для решения задачи дискретного логарифмирования в группе точек эллиптической кривой, а также введено понятие «слабого ключа». Это позволило уточнить оценки стойкости криптопримитивов и протоколов, использующих ранее известные (стандартизованные) эллиптические кривые, а также разработать новые усиленные требования по выбору параметров таких кривых;

– предложен алгоритм вычисления явного вида представления эндоморфизмов эллиптических кривых, который позволил как найти ранее не известные эндоморфизмы, так и построить формы кривых, обеспечивающие минимальную трудоемкость вычисления эндоморфизмов. Разработан также новый эффективный метод вычисления кратной точки на эллиптической кривой;

– предложены и исследованы новые семейства действительных (иррациональных) чисел, определяемые рядами специального вида, а также способ применения таких чисел для выработки псевдослучайных последовательностей с гарантированными оценками их качества. Как пример использования таких последовательностей соискатель предлагает новый протокол локальной аутентификации пользователей;

– определен и исследован новый класс ключевых функций хэширования, на основе которых разработан режим шифрования с проверкой подлинности (аутентифицированного шифрования в терминологии соискателя);

– разработаны новые криптопротоколы: протокол гибридного шифрования, протокол выработки общего ключа с взаимной аутентификацией субъектов взаимодействия, семейство протоколов для защищенного взаимодействия в сетях «Интернета вещей», протоколы защиты каналов управления контрольными и измерительными устройствами. Для всех протоколов получены и строго обоснованы оценки их стойкости в заданных моделях нарушителей;

– разработаны имитационная модель криптопротокола в виде дискретной динамической системы и методика проведения исследования безопасности криптографических протоколов.

Теоретическая и практическая значимость исследования не вызывает никаких сомнений. Полученные теоретические результаты в виде описания новых криптографических алгоритмов и протоколов, оценки их свойств со строгими доказательствами (выносимые на защиту теоремы 1.2, 1.3, 1.6, 2.1, 2.3 – 2.6, 3.1 – 3.3, 4.1 – 4.2) имеют самостоятельное важное теоретическое значение в криптографии. Результаты использовались при подготовке государственных стандартов и рекомендаций по стандартизации в области криптографической защиты информации, в частности, ГОСТ Р

34.10 – 2012 «Процессы формирования и проверки электронной цифровой подписи», Р 1323565.1.004–2017 «Схемы выработки общего ключа с аутентификацией на основе открытого ключа», Р 1323565.1.018–2018 «Криптографические механизмы аутентификации в контрольных и измерительных устройствах для автотранспорта», Р 1323565.1.024–2019 «Параметры эллиптических кривых для криптографических алгоритмов и протоколов», Р 1323565.1.028–2019 «Криптографические механизмы защищенного взаимодействия контрольных и измерительных устройств».

Представленные в автореферате положения являются ***обоснованными и достоверными***, указанные результаты ***апробированы*** на всероссийских и международных конференциях по вопросам информационной безопасности.

Особо отметим, что ряд результатов, публикаций и монографий соискателя используется в образовательной деятельности при подготовке специалистов по защите информации. В частности, алгоритмы поиска длин циклов случайных отображений, предложенные соискателем методы дискретного логарифмирования в группе точек эллиптической кривой, а также алгоритмы вычисления эндоморфизмов эллиптических кривых, построения кривых с усиленными требованиями безопасности, алгоритм нахождения кратной точки изучаются студентами Высшей школы кибербезопасности Института компьютерных наук и кибербезопасности ФГАОУ ВО «Санкт-Петербургский политехнический университет Петра Великого» в рамках таких дисциплин, как «Теоретико-числовые методы в криптографии», «Криптографические методы защиты информации», «Быстрые вычислительные алгоритмы», «Методы алгебраической геометрии в криптографии» и «Криптографические протоколы».

Автореферат имеет строгую логическую последовательность изложения материала и завершенность выводов, текст лаконичен и содержит достаточное число ссылок на известные результаты других авторов по тематике диссертационной работы. Представленное исследование написано автором самостоятельно, имеет внутреннее единство и явно свидетельствует о личном вкладе соискателя в науку.

Вопросы и замечания:

1. В тексте автореферата присутствует незначительное число опечаток (например, на стр. 9, 14, 31 и 32).
2. Есть определенные затруднения с переводной терминологией. А именно, соискатель применяет такие термины, как «код аутентичности» (а на стр. 29 – «код аутентификации»), «аутентифицированное шифрование» и «инициализационный вектор». Если для термина «код аутентичности» сам соискатель указывает русскоязычный аналог – «имитовставка» (стр. 27 и 28), – то для двух оставшихся терминов мы предлагаем использовать более уместные для русского языка названия — «шифрование с проверкой подлинности» (или «шифрование с имитозащитой

данных») и «синхропосылка» («вектор инициализации» в функциях хэширования), соответственно.

3. В обозначениях на стр. 28 автореферата определено нелинейное отображение ϕ со ссылкой на ГОСТ Р 34.11 – 2012. Однако, во-первых, в ГОСТ Р 34.11 – 2012, как и в ГОСТ Р 34.12 – 2015, для этого отображения, задающего S-блоки симметричного шифра, используется обозначение π, и, во-вторых, оно определяет не *перестановку*, а *подстановку*. Аналогично, в формулировке теоремы 3.4 блочный шифр является *не перестановкой*, а *подстановкой*.
4. Проводилось ли исследование эффективности метода дискретного логарифмирования в группе точек эллиптической кривой с использованием алгоритма Госпера в зависимости от способа выбора параметров $(\gamma_i,\ \omega_i)$, $i=\overline{1,s}$, отображения f (стр. 11 автореферата)?

Приведенные замечания не снижают ценности результатов, полученных соискателем, и не влияют на общую положительную оценку.

Заключение. Содержание автореферата позволяет утверждать, что диссертация Нестеренко А. Ю. является ***законченной научно–квалификационной работой***, в которой на основании выполненного автором исследования разработаны теоретические положения, совокупность которых может быть квалифицирована как ***научное достижение***, внедрение которого вносит существенный вклад в развитие страны, а её автор на основании п.п. 9–10 «Положения о присуждении ученых степеней», утвержденного Постановлением Правительства РФ от 24.09.2013 г. № 842 (ред. от 18.03.2023), достоин присуждения ученой степени доктора физико-математических наук по специальности 2.3.6. Методы и системы защиты информации, информационная безопасность.

Доцент Высшей школы кибербезопасности
Института компьютерных наук и кибербезопасности
ФГАОУ ВО «СПбПУ»,
кандидат физико-математических наук Шенец Николай Николаевич

Профессор Высшей школы кибербезопасности
Института компьютерных наук и кибербезопасности
ФГАОУ ВО «СПбПУ»,
доктор технических наук, доцент _ Александрова Елена Борисовна

«04» октября 2023 года

Федеральное государственное автономное образовательное учреждение высшего образования «Санкт-Петербургский политехнический университет Петра Великого» (ФГАОУ ВО «СПбПУ», Высшая школа кибербезопасности Института компьютерных наук и кибербезопасности.
Почтовый адрес: 195251, г. Санкт-Петербург, Политехническая ул., д. 29, ауд. 173,
Тел. +7 (812) 552-76-32, электронная почта: kafedra@ibks.spbstu.ru