Отзыв

официального оппонента на диссертацию Нестеренко Алексея Юрьевича «Математические методы обеспечения защищенного взаимодействия средств защиты информации» на соискание ученой степени доктора физико-математических наук по специальности 2.3.6 — методы и системы защиты информации, информационная безопасность

Диссертационная работа А.Ю. Нестеренко посвящена развитию методов построения криптографических протоколов, применяемых для обеспечения защищенного обмена информацией по открытым каналам связи, а также совершенствованию методов получения обоснованных оценок безопасности таких протоколов. При этом основное внимание в диссертационной работе уделяется базовым преобразованиям, которые используются при построении повсеместно применяемых в настоящее время криптографических протоколов, в том числе протоколов аутентифицированной выработки общих ключей и защищенного с помощью данных ключей обмена сообщениями. Повсеместное применение указанных протоколов в системах защиты информации обуславливает несомненную актуальность темы диссертационного исследования.

В криптографических протоколах рассматриваемого вида применяются операции вычисления кратной точки эллиптической кривой, режимы аутентифицированного шифрования, обеспечивающие одновременное шифрование и имитозащиту передаваемых данных, а также процедуры выработки псевдослучайных последовательностей. Ряд основных результатов диссертационного исследования относится именно к этим базовым криптографическим механизмам.

В заключительной части (четвертой главе) диссертационной работы внимание уделяется непосредственно вопросам синтеза криптографических протоколов на основе базовых преобразований, а также получению оценок безопасности построенных протоколов с помощью разработанной автором модели. Предложенная автором модель позволяет получать оценки безопасности криптографических протоколов с учетом оценок уровня информационной безопасности базовых преобразований. Исходя из этого, автор уделяет существенное внимание некоторым из важных задач, возникающих при оценке стойкости вышеупомянутых базовых криптографических механизмов: задаче дискретного логарифмирования в группе точек эллиптической кривой и поиску случаев, в которых эта задача имеет относительно простое решение. Также в первой главе рассматривается метод вычисления кратной точки с использованием эндоморфизмов эллиптической кривой.

Вторая глава диссертации посвящена изучению вопроса о восстановлении начального состояния генератора псевдослучайных последовательностей специального вида. Рассматривается подход, основанный на представлении действительных иррациональных чисел в заданной системе счисления. Коэффициенты такого представления образуют вырабатываемую последовательность. В качестве примера практического применения рассматриваемого подхода приводится процедура выработки производной ключевой информации, например, из низкоэнтропийных данных, таких как пароль пользователя средства защиты информации.

Третья глава диссертации содержит результаты исследований, направленных на построение режимов аутентифицированного шифрования. Основное внимание уделено вопросам применения в таких режимах равновероятных сжимающих отображений,

представляющих собой линейные формы от взаимно однозначных функций. Доказываются теоремы о равновероятности построенных сжимающих отображений и предлагаются подходы к эффективной реализации таких отображений с применением алгоритмов блочного шифрования в качестве нелинейных преобразований.

Диссертационная работа состоит из общей характеристики работы, четырех глав, заключения, списка литературы, включающего 395 источников, и приложения с исходными текстами реализованных автором программ. В списке использованной литературы отмечены результаты большинства отечественных специалистов, проводящих исследования в смежных областях.

Основные результаты диссертации опубликованы в 29 научных публикациях, среди которых 21 публикация входит в перечень изданий, индексируемых Web of Science, Scopus, RSCI и списки ВАК Минобрнауки Российской Федерации, что является достаточным для представления диссертации.

Среди вынесенных на защиту результатов наибольшую значимость имеют следующие.

1. Доказательство теоремы о существовании алгоритма дискретного логарифмирования в группе точек эллиптической кривой, использующего информацию о мультипликативном порядке неизвестного значения. Доказанная теорема позволила в явном виде указать множество «слабых» секретных ключей криптографических схем и протоколов. Для таких ключей сложность их нахождения с помощью предложенного в диссертационной работе алгоритма существенно меньше, чем у алгоритмов, известных ранее. Полученные результаты позволяют говорить о том, что мощность множества «слабых» ключей однозначно определяется делителями числа q-1, где простое число q задает порядок подгруппы, в которой рассматривается задача дискретного логарифмирования. Из приведенных в тексте диссертации значений следует, что для стандартизированных в Российской Федерации эллиптических кривых множество «слабых» ключей невелико. При этом автор диссертационной работы сформулировал усиленные требования к параметрам эллиптических кривых, необходимые для минимизации множества «слабых» ключей, предложил алгоритм выработки таких параметров и реализовал его на практике. Значения выработанных параметров приводятся в приложении к диссертационной работе.

2. Алгоритм вычисления явного представления эндоморфизмов эллиптических кривых, применяемых в средствах защиты информации. Подход к вычислению кратной точки эллиптической кривой с использованием явно заданных эндоморфизмов исследовался в работах ряда отечественных и зарубежных авторов. Тем не менее, до появления работ автора диссертации, было известно ограниченное число явно заданных эндоморфизмов, которые могли бы применяться в практических приложениях. Это существенно сужало практическую значимость данного направления исследований. Разработанный автором диссертации алгоритм оказался достаточно эффективным, что позволило вычислить в явном виде большой класс новых отображений, часть из которых содержится в тексте диссертации.

3. Формальная модель, представляющая криптографический протокол в виде дискретной динамической системы, а также метод получения численных оценок безопасности, основанный на изучении сложности компрометации базовых криптографических преобразований. Предложенный автором диссертации метод имеет важные практические приложения и неоднократно применялся в рамках криптографических

исследований рекомендаций по стандартизации, разрабатываемых в рамках деятельности технического комитета №26 «Криптографическая защита информации». Среди таких рекомендаций можно отметить Р 1323565.1.004–2017 «Схемы выработки общего ключа с аутентификацией на основе открытого ключа», 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», МР 26.2.001–2022 «Использование российских криптографических алгоритмов в протоколе обмена ключами в сети Интернет версии 2 (IKEv2)».

Вместе с тем, следует отметить, что предлагаемый в диссертационной работе подход для определения оценок безопасности в диссертационной работе имеет существенные ограничения. Он позволяет получить численные значения только для известных аналитику методов компрометации базовых криптографических преобразований. Это не позволяет говорить о том, что вычисленная оценка является окончательной, поскольку существует возможность нахождения новых методов проведения атак, имеющих сложность, меньшую, чем у методов, известных аналитику на момент проведения исследования. Следовательно, полученные в ходе проведения исследований оценки должны рассматриваться исключительно как содержательные оценки сверху. Отметим, что на это существенное ограничение автор сам указывает на с. 354 диссертационной работы.

Автореферат диссертации правильно и полно отражает её содержание.

Все выносимые на защиту результаты являются новыми и получены автором лично. Результаты четко сформулированы и оформлены в виде строгих математических доказательств и формально описанных алгоритмов.

К тексту диссертации имеются следующие замечания.

1. С учетом основной заявленной цели диссертационного исследования, связанной с совершенствованием методов построения криптографических протоколов определенного вида, представляется целесообразным сперва изложить положения разработанного подхода к исследованию влияния свойств базовых криптографических механизмов на результирующий уровень информационной безопасности, а уже затем переходить к изложению полученных результатов о свойствах изучаемых базовых механизмов (механизмов на эллиптических кривых, механизмов порождения псевдослучайных последовательностей и механизмов аутентифицированного шифрования). В представленном тексте диссертации изложение построено иным образом: первые три главы посвящены базовым механизмам и только заключительная глава содержит общую методологию, обеспечивающую законченность и целостность диссертационного исследования.

2. В работе содержится ряд некорректных формулировок о связи между стойкостью криптографических протоколов и базовых криптографических механизмов. Так, например, в начале раздела 1.1.2 утверждается: «[…] алгоритмическая сложность решения задачи дискретного логарифмирования определяет стойкость, […], в частности: […] протоколов», а в числе протоколов посредством ссылок упомянуты такие как TLS 1.2, TLS 1.3, CRISP, – протоколы, стойкость которых зависит от сложности задачи дискретного логарифмирования (а точнее, от связанной с ней вычислительной задачи Диффи-Хеллмана) в соответствующих группах, но никак не «определяется ей», будучи зависимой также от стойкости ряда иных криптографических механизмов, а также стойкостью самих конструкций протоколов в

релевантных моделях нарушителя. Аналогично на с. 24 упоминается снижение алгоритмической сложности решения задачи, «обосновывающей стойкость средства защиты информации», хотя стойкость (защищенность, уровень информационной безопасности) конечного средства защиты, кроме алгоритмической сложности решения задач, связанных с базовыми механизмами, зависит и от упомянутых выше в настоящем абзаце факторов, и от свойств реализации данного средства защиты.

Отметим, что данное замечание относится именно к небрежности формулировок, но не к ошибочности используемых автором подходов: в разделах четвертой главы, непосредственно посвященных оценке стойкости протоколов, автором излагается корректная методология, учитывающая необходимые факторы, влияющие на стойкость конечных средств защиты информации.

3. Утверждение раздела «Теоретическая значимость работы» о том, что разработанная автором методика исследований безопасности криптографических протоколов является «единственным математически обоснованным документом, позволяющим […] проводить исследования всех факторов, влияющих на безопасность криптографических протоколов […] и получать численные значения показателей мер защиты информации», не является в полной мере корректным и требует существенных уточнений.

Не ставя под сомнение важность, новизну и безусловную теоретическую и практическую значимость разработанной автором методики, необходимо отметить, что ряд разработанных ранее протоколов проходил всесторонние исследования по обоснованным методикам как в России, так и за рубежом: в частности, публикации из списка литературы рассматриваемой диссертации содержат (частично или полностью), в том числе, результаты исследований криптографических протоколов TLS 1.2, TLS 1.3, SESPAKE, проводившихся отечественными и/или зарубежными авторами по методикам, учитывающим необходимые аспекты актуальных моделей нарушителя и позволявшим получать численные значения показателей мер защиты информации.

4. Многократно используемая автором аббревиатура «СКЗИ» не вводится в тексте диссертации.

5. В работе содержится ряд незначительных опечаток и несогласованных предложений, например, «одинокого высокого уровня» на с. 10, «МГУ им. В.В. Ломоносова» на с. 17, «свободное от квадратов, целое число» на с.33, «Конетти-Кравчука» на с. 49 и с. 249, «не удовлетворяло» в сноске на стр. 156. Кроме того, в работе отсутствует единство употребления первой гласной в термине «хэширование/хеширование» – многократно встречается каждый из вариантов написания.

Несмотря на сделанные замечания, диссертационная работа заслуживает положительной оценки.

Автором диссертации проведено разностороннее исследование поставленной проблемы, а предложенные методы ее решения подтверждаются результатами практических экспериментов. Отдельно стоит отметить важность и применимость ряда полученных результатов при проведении исследований массово используемых средств защиты информации.

В диссертации используется математический аппарат алгебры, теории чисел, теории функций комплексного переменного, теории вероятностей, теории автоматов. Диссертация обладает внутренним единством, ее содержание соответствует поставленным задачам, а

также паспорту специальности 2.3.6 – методы и системы защиты информации, информационная безопасность.

Основные выводы диссертации сформулированы достаточно полно и отражают суть полученных результатов. Диссертация представляет собой завершенную научно-техническую работу, в которой на основании выполненных автором исследований сформулированы результаты, совокупность которых можно квалифицировать как крупное научное достижение.

Считаю, что диссертация соответствует критериям, определенным в пп. 2.1–2.5 «Положения о присуждении ученых степеней в Московском государственном университете имени М.В. Ломоносова», предъявляемым к докторским диссертациям, а ее автор, Нестеренко Алексей Юрьевич, заслуживает присуждения ученой степени доктора физико-математических наук по специальности 2.3.6 — методы и системы защиты информации, информационная безопасность.

Официальный оппонент

доктор физико-математических наук,
заместитель генерального директора
ООО «КРИПТО-ПРО»

С.В. Смышляев

06.10.2023 г.