ОТЗЫВ ОФИЦИАЛЬНОГО ОППОНЕНТА

на диссертационную работу Синева Валерия Евгеньевича
«Методы построения и разработка практичных протоколов групповой подписи и алгебраических алгоритмов защитных преобразований»,
представленную на соискание ученой степени кандидата технических наук по специальности 05.13.19 – Методы и системы защиты информации, информационная безопасность

Актуальность темы диссертационной работы

Задача комплексного обеспечения информационной безопасности включает задачи аутентификации пользователей и данных, защиты информации от несанкционированного доступа, обеспечения неотрекаемости от авторства электронных сообщений и документов. Задача последнего типа решается с использованием протоколов электронной цифровой подписи различного типа. В распределенных многопользовательских приложениях зачастую требуются протоколы, позволяющие подписывать документы коллегиально. Для защиты информации от несанкционированного доступа используются алгоритмы защитных преобразований, среди которых особое место занимают алгебраические алгоритмы псевдовероятностного шифрования, позволяющие выполнить одновременное зашифрование двух независимых сообщений так, чтобы формируемый шифртекст был вычислительно неотличим от шифртекста, полученного путем вероятностного зашифрования одного из сообщений. Такие алгебраические алгоритмы, как правило, обладают относительно низкой производительностью, что ограничивает их применение при разработке новых типов защитных механизмов.

Таким образом, тема диссертационной работы, направленной на разработку практичных протоколов групповой подписи и алгебраических алгоритмов защитных преобразований, является актуальной.

Степень обоснованности научных положений, выводов и рекомендаций

В диссертационной работе разработаны методы построения протоколов групповой цифровой подписи, а также предложены протоколы, обладающие новым набором свойств, что отличает их от известных протоколов мультиподписи. Синев В.Е. выполнил достаточно полный анализ состояния исследований в области защитных преобразований информации и протоколов цифровой подписи, что позволило обозначить цель диссертационного исследования как расширение функциональности и повышение уровня безопасности протоколов обеспечения неотрекаемости от электронных сообщений и документов и алгоритмов защитных

преобразований. С учетом этой цели была поставлена научно-техническая задача — разработать протоколы групповой подписи, функционирующие на базе стандартной инфраструктуры открытых ключей, и производительные алгебраические алгоритмы защитных преобразований. В соответствии с этой задачей были сформулированы подзадачи, в результате решения которых были получены следующие результаты:

1. Разработан метод повышения уровня информационной безопасности и протокол утверждаемой групповой подписи, отличающийся использованием двух сложных задач: дискретного логарифмирования и разложения на множители.

2. Разработан метод повышения уровня информационной безопасности и протокол слепой подписи, отличающийся использованием вычислений в конечном поле $GF(p)$.

3. Разработан протокол утверждаемой групповой подписи, основанный на вычислительной сложности задачи дискретного логарифмирования на эллиптической кривой и отличающийся вычислением открытого ключа в виде суммы точек эллиптической кривой и генерацией маскирующих коэффициентов в виде криптографической контрольной суммы, зависящей от секретного ключа руководителя группы подписантов.

4. Разработаны протоколы коллективной подписи для групповых и индивидуальных подписантов.

5. Разработан метод построения защитных преобразований информации с использованием алгебраических операций, отличающийся комбинированием операций из конечных алгебраических структур различного типа и разбиением входного блока данных на подблоки различного размера.

6. Разработан метод псевдовероятностных защитных преобразований, стойкий к атакам с принуждением отправителя и получателя сообщений к раскрытию ключа шифрования, отличающийся реализацией вычислений в конечных полях, заданных в явной векторной форме, благодаря чему обеспечивается повышение производительности.

Разработанные протоколы удобны для практического применения, что обусловлено, с одной стороны, использованием типовой инфраструктуры открытых ключей, реально функционирующей на практике, а с другой стороны, простотой механизма изменения штатного состава группового подписанта. Именно удовлетворение этим требованиям в диссертации понимается под термином «практичные».

Содержание диссертационного исследования дает возможность отметить высокую степень обоснованности основных научных положений, рекомендаций и выводов.

Достоверность научных положений, выводов и практических рекомендаций, полученных в диссертационной работе, обеспечивается анализом состояния исследований в данной области на сегодняшний день, математическими доказательствами и апробацией результатов на научных и научно-практических конференциях различного уровня.

Оценка научной новизны

Научная новизна состоит в разработке методов и протоколов мультиподписи нового типа и методов построения алгебраических алгоритмов защитных преобразований. Наиболее существенными новыми научными результатами, полученными соискателем, являются:

1. Метод построения протокола коллективной подписи, обеспечивающий фиксированный размер подписи для произвольного числа групповых подписантов, разделяющих ответственность за сформированную подпись, и возможность практического внедрения на базе типовой инфраструктуры открытых ключей.

2. Метод построения протокола комбинированной коллективной подписи для смешанного состава подписантов (индивидуальных и групповых), обеспечивающий фиксированный размер подписи для произвольного числа индивидуальных и групповых подписантов и возможность практического внедрения на базе типовой инфраструктуры открытых ключей.

3. Протоколы новых типов мультиподписи — коллективной подписи для групповых подписантов и комбинированной коллективной подписи, свободные от специальных процедур при изменении штатного состава подписантов.

4. Метод построения и алгебраический алгоритм псевдовероятностного защитного преобразования, отличающийся представлением двух совместно преобразуемых сообщений в виде элементов конечного расширенного поля, представленных в явной векторной форме.

5. Протокол аутентификации пользователей с нулевым разглашением, отличающийся использованием для его построения вычислительно сложной задачи дискретного логарифмирования в скрытой циклической подгруппе конечной некоммутативной группы.

Теоретическая и практическая значимость

Теоретическая значимость полученных результатов состоит в выделении нового подкласса протоколов мультиподписи — протоколов коллективной подписи для групповых подписантов (нескольких независимых коллегиальных органов, удостоверяющих электронные документы своими подписями) и протоколов комбинированной коллективной подписи для «смешанного» состава подписантов (включающего индивидуальных и групповых подписантов). Самостоятельную теоретическую значимость имеет предложенный метод повышения производительности алгебраических алгоритмов псевдовероятностного шифрования и протокол с нулевым разглашением на основе вычислительно сложной задачи дискретного логарифмирования в скрытой циклической подгруппе конечной некоммутативной группы.

Практическая ценность предложенных методов и протоколов коллективной и групповой подписи состоит в возможности их функционирования на базе практически развернутой инфраструктуры открытых ключей, поддержке высокой гибкости штатного состава группового органа-подписанта (за счет отсутствия специальных процедур включения/исключения сотрудников органа-подписанта). Практической значимостью обладает и разработанный алгебраический алгоритм псевдовероятностных защитных преобразований, представляющий интерес с точки зрения разработки средств защиты, направленных на навязывание ложной информации потенциальному нарушителю, и ориентированный на использование в составе программных и аппаратных средств защиты.

Оценка содержания диссертации

Диссертационная работа Синева В.Е. написана в достаточно хорошем стиле, изложена на 166 стр., включает 5 глав, 11 рисунков, 4 таблицы. Библиографический список содержит 126 наименований.

Структура работы логична и отвечает задачам исследований, Разработанные методы, протоколы и алгоритмы описаны достаточно полно.

Автореферат полно передает основное содержание диссертации, основные результаты и положения, выносимые на защиту.

Полнота опубликованных результатов и соответствие паспорту специальности

Синев В.Е. имеет 14 опубликованных научных трудов по теме диссертации (в том числе пять в изданиях в изданиях, рекомендованных ВАК для опубликования результатов диссертационных исследований). В

указанных работах полностью отражены основные научные и практические результаты, полученные автором и изложенные в диссертации и автореферате.

Тема диссертации, направленность проведенных исследований и полученных результатов соответствует паспорту специальности 05.13.19 — «Методы и системы защиты информации, информационная безопасность» по п. 1. Теория и методология обеспечения информационной безопасности и защиты информации; п. 5. Методы и средства (комплексы средств) информационного противодействия угрозам нарушения информационной безопасности в открытых компьютерных сетях, включая Интернет; п. 13. Принципы и решения (технические, математические, организационные и др.) по созданию новых и совершенствованию существующих средств защиты информации и обеспечения информационной безопасности.

Замечания по диссертационной работе

1. В диссертационной работе не рассмотрены сценарии потенциальных атак на разработанные протоколы коллективной подписи для групповых подписантов и комбинированной коллективной подписи, в частности, атаки сговора участников и атаки на удостоверяющий центр (регистрация ложного открытого ключа).

2. В п. 4.9 отсутствует оценка эффективности предлагаемого способа отрицаемого шифрования, подтверждающая повышение производительности по сравнению с аналогом, предложенным Березиным А.Н., Биричевским А.Р., Молдовяном Н.А., Рыжковым А.В.

3. В диссертации предлагается способ уменьшения вычислительной сложности протоколов, основанных на вычислениях в конечной группе матриц, который состоит в задании матриц над конечными расширенными полями, представленными в явной векторной форме, однако вопрос доказательства возможности такого представления и критерии его реализации не обсуждается.

4. Отсутствуют результаты экспериментальных испытаний, подтверждающих работоспособность и эффективность разработанных методов псевдовероятностных защитных преобразований.

5. В диссертации присутствуют ошибки и опечатки, затрудняющие восприятие изложенных протоколов, например: на с. 51 в уравнении проверки подлинности (п. 1) элемент a должен быть возведен в степень S^2, а не S, элемент y должен быть возведен в степень E, а не $-E$; при задании открытого ключа (с. 52) элемент α должен быть возведен в степень z, а не k; на с. 56 в п. 7 пропущена степень d у множителя H; на с. 73 в п. 4

формирования подписи в S_i вместо t_i нужно использовать k_i; на с. 121 в схеме отрицаемого шифрования в п. 2 при генерации вектора R_2 в степень e_2 должен возводиться вектор D, а не вектор M.

Отмеченные замечания не снижают общее положительное впечатление о работе и не влияют на главные теоретические и практические результаты диссертации.

Заключение

В целом диссертация Синева В.Е. является законченной научно-квалификационной работой, в которой содержится решение научной задачи разработки протоколов групповой подписи, функционирующих на базе стандартной инфраструктуры открытых ключей, и быстрых алгебраических алгоритмов защитных преобразований, имеющей существенное значение для развития методов и средств аутентификации пользователей и данных. Работа выполнена на достаточно высоком научном уровне.

Диссертационная работа и автореферат удовлетворяют требованиям пп. 9, 10 «Положения о присуждении ученых степеней», утвержденного Постановлением Правительства РФ от 24.09.2013 № 842, а автор, Синев Валерий Евгеньевич, заслуживает присуждения ученой степени кандидата технических наук по специальности 05.13.19 – «Методы и системы защиты информации, информационная безопасность».

Официальный оппонент

доктор технических наук, доц ександрова Елена Борисовна

«05» декабря 2017 г.

Сведения о составителе отзыва:
ФИО: Александрова Елена Борисовна
ученая степень: доктор технических на
ученое звание: доцент по кафедре информационной безопасности компьютерных систем
место работы: федеральное государственное автономное образовательное учреждение высшего образования «Санкт-Петербургский политехнический университет Петра Великого»
должность: профессор кафедры «Информационная безопасность компьютерных систем»
почтовый адрес: 195251, Санкт-Петербург, Политехническая ул., д. 29
телефон (рабочий): (812) 552-76-32
адрес электронной почты (при наличии): elena.aleksandrova@ibks.ftk.spbstu.ru