Отзыв официального оппонента

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

1. Актуальность выполненного исследования

Диссертация посвящена методам построения и разработке протоколов групповой подписи и алгоритмов защитных преобразований. В работе выполнен аналитический обзор известных методов, алгоритмов и протоколов защитных преобразований информации, применяемых для обеспечения информационной безопасности информационно-телекоммуникационных технологий, в том числе протоколов электронной цифровой подписи (ЭЦП).

Придание юридической значимости электронным документам и сообщениям на основе ЭЦП играет важную роль в информационных технологиях различного типа, в том числе в технологиях электронного документооборота, электронных денег, тайного электронного голосования. Разнообразие информационных технологий, в которых применяются протоколы ЭЦП обусловливает потребности использования протоколов ЭЦП с разнообразной функциональностью протоколов ЭЦП. Откликом на такую практическую потребность явились исследования в области построения и анализа протоколов «мультиподписи», частными случаями которых являются протоколы коллективной и групповой ЭЦП.

Несмотря на достаточное представительное разнообразие существующих протоколов групповой ЭЦП, вопрос разработки практичных протоколов этого типа, внедрение которых в практику может быть осуществлено на базе существующей стандартной инфраструктуры открытых ключей, оставался открытым на момент выполнения диссертационных исследований. Это определяет актуальность темы диссертационной работы.

Другим аспектом обеспечения информационной безопасности информационных технологий является защита информации от несанкционированного доступа. Для расширения спектра атак этого типа, отражаемых с помощью механизма шифрования, сравнительно недавно предложены алгебраические алгоритмы защитных преобразований, вычислительно неотличимые по шифртексту от вероятностных защитных преобразований. Такие псевдовероятносные защитные преобразования

представляют существенный интерес для реализации механизмов защиты информации, направленных на навязывание потенциальному нарушителю ложной информации. Однако практическое применение в средствах обеспечения информационной безопасности новых защитных механизмов требует повышения производительности известных алгоритмов данного типа, что обусловливает актуальность разработки новых алгебраических алгоритмов псевдовероятностного защитного преобразования.

Таким образом, тема диссертационного исследования «Методы построения и разработка практичных протоколов групповой подписи и алгебраических алгоритмов защитных преобразований» является актуальной.

2. Новизна исследования и полученных результатов, степень обоснованности научных положений, выводов и рекомендаций, сформулированных в диссертации

Научная новизна диссертационного исследования заключается в разработке новых методов построения протоколов групповой ЭЦП и алгебраических алгоритмов псевдовероятностного защитного преобразования, новых протоколов и алгоритмов, основанных на предложенных методах. Новыми научными результатами являются следующие:

1. Впервые предложен метод построения протоколов коллективной ЭЦП для групповых подписантов, в котором формируется единая цифровая подпись фиксированного размера для произвольного числа групповых подписантов аутентификации пользователей.
2. Разработан новый протокол ЭЦП – протокол коллективной ЭЦП для групповых подписантов.
3. Впервые предложен метод построения протоколов комбинированной коллективной ЭЦП для индивидуальных и групповых подписантов, в котором формируется единая цифровая подпись фиксированного размера к некоторому электронному документу, удостоверяющая то, что документ подписан каждым подписантом из приложенного списка индивидуальных и групповых подписантов.
4. Разработан новый протокол коллективной ЭЦП – протокол комбинированной коллективной ЭЦП для индивидуальных и групповых подписантов.
5. Метод построения и протокол утверждаемой групповой ЭЦП, построенный на основе вычислений по модулю простого числа p с трудно разложимым значением функции Эйлера $\varphi(p)$.
6. Разработан новый метод повышения производительности алгебраических алгоритмов псевдовероятностного защитного преобразования.

Обоснованность представленных положений, выводов и рекомендаций обеспечивается корректным использованием выбранного математического аппарата и применением системного подхода к решению поставленных задач. Результаты диссертации прошли достаточную апробацию, использованы в производственной деятельности ООО «Удостоверяющий центр ГАЗИНФОРМСЕРВИС» и внедрены в учебный процесс кафедры информационной безопасности Санкт-Петербургского государственного электротехнического университета «ЛЭТИ» имени В.И.Ульянова(Ленина).

3. Значимость для науки и практики результатов диссертации

Научная значимость полученных результатов состоит в разработке новых методов построения протоколов коллективной ЭЦП и протоколов групповой ЭЦП, нового метода построения алгебраических алгоритмов псевдовероятностных защитных преобразований.

Практическая значимость результатов заключается в расширении класса протоколов коллективной и групповой ЭЦП, внедрение которых осуществимо на основе существующей на практике инфраструктуры открытых ключей.

4. Оценка содержания диссертации

Диссертационная работа изложена на 166 страницах, состоит из введения, 5-и глав исследования, которые включают анализ текущего уровня исследования в данной области, выводов по каждой главе. Также в работе имеется заключение и список литературы, включающий 126 отечественных и зарубежных источников. В работе представлены 4 таблицы и 11 рисунков.

Основные результаты диссертации представлены в 14 публикациях, в том числе, в 5 статьях, опубликованных в ведущих рецензируемых журналах, входящих в перечень ВАК.

Полученные автором в ходе исследования результаты могут быть использованы при разработке программно-аппаратных средств обеспечения информационной безопасности информационно-телекоммуникационных систем и информационных технологий.

Протокол коллективной ЭЦП для групповых подписантов, протокол комбинированной коллективной ЭЦП для групповых и индивидуальных подписантов, а также разработанный алгебраический алгоритм псевдовероятностного защитного преобразовании могут быть использованы в учебном процессе на старших курсах обучения студентов по специальностям, связанным с областью информационной и компьютерной безопасности.

Направление выполненных исследований, решаемые научные задачи, полученные результаты и положения, выносимые на защиту, соответствуют

паспорту специальности 05.13.19 – «Методы и системы защиты информации, информационная безопасность» по пунктам 5, 11, 13.

Автореферат соответствует содержанию выполненной диссертационной работы и дает ясное представление о выполненном исследовании, основных результатах и положениях, выносимых на защиту.

По содержанию диссертационной работы можно отметить следующие недостатки и возражения:

1. В разработанном протоколе утверждаемой групповой подписи процедуры формирования ЭЦП и проверки подлинности подписи являются достаточно быстрыми, однако процедура раскрытия заданной групповой подписи является медленной, что обусловлено использованием переборного способа индентификации подмножества индивидуальных подписантов, принявших участие в формировании заданной групповой подписи. Этот недостаток существенно усугубляется для протоколов коллективной ЭЦП для групповых подписантов, в рамках которых идентификация подмножества индивидуальных подписантов даже в рамках одного группового подписанта требует участия руководителей всех групповых подписантов, разделяющих заданную коллективную ЭЦП.

2. Предложенный метод псевдовероятностного защитного преобразования приводит к формированию шифртекста удвоенного размера по сравнению с размером секретного сообщения.

3. Сравнительно мало внимания уделено вопросу анализа стойкости разработанных протоколов.

4. В разработанных протоколах ЭЦП в процедуре формирования ЭЦП требуется участие руководителей всех групповых подписантов, разделяющих формируемую подпись.

5. В диссертации значительное внимание уделено вопросу разработки алгебраических защитных преобразований, однако только одно положение, выносимое на защиту, отражает эту часть диссертационного исследования.

Указанные замечания и недостатки носят частный характер и не снижают общей ценности диссертационной работы и значимости изложенных в ней научных результатов.

5. Заключение о соответствии

Диссертационная работа «Методы построения и разработка практичных протоколов групповой подписи и алгебраических алгоритмов защитных преобразований» представляет собой завершенную научно-квалификационную работу, в которой содержится решение важной научно-технической задачи разработки протоколов групповой электронной

цифровой подписи, внедрение которых осуществимо на основе существующей на практике инфраструктуры открытых ключей, и повышения производительности алгебраических алгоритмов псевдовероятностного защитного преобразования, имеющей существенное значение для развития методов и средств обеспечения информационной безопасности информационных технологий.

Диссертационная работа «Методы построения и разработка практичных протоколов групповой подписи и алгебраических алгоритмов защитных преобразований» Синева Валерия Евгеньевича соответствует требованиям п. 9 «Положения о порядке присуждения учёных степеней», утверждённого постановлением Правительства РФ№ 842 от 24.09.2013 г., предъявляемым к кандидатским диссертациям, а ее автор заслуживает присуждения ученой степени кандидата технических наук по специальности 05.13.19 – «Методы и системы защиты информации, информационная безопасность».

Официальный оппонент
д.т.н, доц. Т.М. Татарникова

«27» ноября 2017 г.

Подпись Татарниковой Т.М.
удостоверяю

Сведения о составителях отзыва:
ФИО: Татарникова Татьяна Михайловна
ученая степень: доктор технических наук
ученое звание: доцент по кафедре информационных управляющих систем
место работы: федеральное государственное автономное образовательное учреждение высшего образования «Санкт-Петербургский государственный университет аэрокосмического приборостроения»
должность: профессор кафедры безопасности информационных систем
почтовый адрес: 190000, Россия Санкт-Петербург, ул. Большая Морская, д. 67, лит. А, ГУАП
телефон (рабочий): 8-(812)-494-70-52
адрес электронной почты (при наличии): kaf51@vu.spb.ru