ОТЗЫВ
на автореферат диссертации
Бабуевой Александры Алексеевны
«Свойства безопасности схем подписи вслепую на основе уравнений Шнорра и Эль-Гамаля», представленной на соискание ученой степени кандидата физико-математических наук
по специальности 2.3.6. Методы и системы защиты информации, информационная безопасность

В современном мире активно развиваются системы электронных платежей. Такие системы, в частности, должны обеспечивать невозможность отслеживания трат пользователей. Одним из подходов к обеспечению этого свойства является использование схем подписи вслепую. Так, банк может вслепую подписывать «банкноты» пользователей системы после прохождения ими процедуры аутентификации, при этом он не получает никакой информации о номерах этих банкнот в силу обеспечения схемой свойства неотслеживаемости, и, как следствие, не может связать конкретные банкноты с конкретным пользователем. Таким образом, вопросы синтеза и анализа стойкости схем подписи вслепую являются крайне актуальными. Особенно важно отметить использование таких схем подписи при трансграничных платежах в качестве контрсанкционной меры для Российской Федерации, которая может обеспечить защиту иностранного контрагента от наложения вторичных санкций со стороны западных стран и/или Соединенных Штатов Америки.

Диссертационная работа Бабуевой А.А. посвящена разработке математических методов получения обоснованных оценок стойкости для схем подписи вслепую, построенных на основе уравнений подписи Шнорра и Эль-Гамаля. Оценка стойкости проводится в моделях безопасности, релевантных в прикладных системах, использующих схемы подписи вслепую. Для исследования выбраны два вида схем: схема Шаума-Педерсена, предложенная в зарубежной литературе в 1992 году, и схемы на основе

уравнения Эль-Гамаля (все они объединены в общий класс схем GenEG-BS). Актуальность рассмотрения именно этих схем обусловлена тем фактом, что для них ранее не были доказаны ни нижние, ни верхние оценки стойкости в моделях безопасности, учитывающих угрозу построения подделки и возможность нарушителя открывать параллельные сеансы протокола формирования подписи (модели UF и wUF в диссертации).

Для схемы Шаума-Педерсена в диссертации разработан метод нарушения свойства неподделываемости в модели UF, позволяющий нарушителю сформировать подделку подписи для сообщения, ранее подписываемого легитимным образом, и доказана нижняя оценка стойкости в модели wUF, учитывающей угрозу построения подделки для нового, ранее не подписываемого сообщения. Для схем из класса GenEG-BS разработаны методы нарушения свойств неподделываемости и неотслеживаемости в стандартных моделях безопасности для схем подписи вслепую.

Для указанных схем доказаны нижние оценки стойкости в специализированных моделях безопасности, релевантных в прикладных системах формирования подписи, где ключ подписи хранится на функциональном ключевом носителе.

Автореферат диссертации позволяет сделать вывод о научной новизне результатов, их теоретической и практической значимости, а также о достижении автором цели диссертации. Результаты диссертации опубликованы в 5 статьях, 4 из которых опубликованы в рецензируемых научных изданиях, рекомендованных для защиты в диссертационном совете Московского государственного университета имени М.В. Ломоносова по специальности 2.3.6. «Методы и системы защиты информации, информационная безопасность».

Судя по автореферату и публикациям, диссертация Бабуевой А.А. по уровню выполнения, новизне и актуальности соответствует критериям, установленным в Положении о присуждении ученых степеней в Московском

государственном университете имени М.В. Ломоносова для диссертаций на соискание ученой степени кандидата наук, а ее автор, Бабуева Александра Алексеевна, заслуживает присуждения ученой степени кандидата физико-математических наук по специальности 2.3.6. Методы и системы защиты информации, информационная безопасность.

Кандидат физико-математических наук,
Советник экономический
Управления методологии и стандартизации
информационной безопасности
и киберустойчивости
Департамента информационной безопасности
Банка России

Елистратов А.А.

Контактные данные:

тел.:
e-mail: elistratovaa01@cbr.ru
почтовый адрес: 107016, г. Москва, ул. Неглинная, д.12, к. В.
адрес места работы: г. Москва, Ленинский пр-т, д.1к2.

Я, Елистратов Андрей Алексеевич, даю свое согласие на включение моих персональных данных в документы, связанные с работой диссертационного совета, и их дальнейшую обработку.

«6» ноября 2025 г.

Подпись Елистратова А.А. удостоверяю.

Кандидат технических наук,
Заместитель директора
Департамента информационной безопасности
Банка России

Выборнов А.О.