

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

Цифровизация информационного взаимодействия проникла во все сферы нашей жизни. Естественным образом это ведет к усилению требований по защите информации. С усложнением структуры и объема информационного взаимодействия, кроме традиционных услуг информационной безопасности, таких как обеспечение доступности, целостности и конфиденциальности информации, возникают запросы к предоставлению и других услуг. В частности, весьма востребованным является разработка протоколов дистанционного электронного голосования, требующих обеспечения неотслеживаемости пользователя по его волеизъявлению. Критическим элементом таких протоколов является, как правило, криптографически стойкая схема цифровой подписи вслепую. Поэтому тема и содержание диссертационной работы являются актуальными, как в теоретическом, так и в практическом аспектах.

Диссертационная работа Бабуевой А.А. решает задачу получения содержательных оценок стойкости для схем подписи вслепую в группе точек эллиптической кривой. Получение оценок стойкости возможно только в условиях конкретной модели угроз безопасности информации и возможным действиям нарушителя. В работе рассмотрены два класса моделей безопасности: расширенные модели и специализированные модели. В расширенных моделях безопасности учитываются классические угрозы безопасности для схем подписи вслепую (формирование подделки, получение информации о сообщении и подписи) и наиболее широкие классические

возможности нарушителя, определенные ранее в литературе. Специализированные модели безопасности учитывают классические угрозы безопасности и специфические возможности нарушителя, связанные с вопросами реализации подписей вслепую, в частности возникающие при хранении ключа подписи на так называемом функциональном ключевом носителе, когда последний потенциально содержит специально спроектированные уязвимости.

В диссертации проведен анализ безопасности конкретных схем подписи вслепую: схемы Шаума-Педерсена, построенной на основе уравнения подписи Шнорра, и схем из класса GenEG-BS, построенных на основе уравнения подписи Эль-Гамала. Для всех ранее известных схем разработаны методы нарушения, как минимум, одного свойства безопасности схемы подписи хотя бы в одной из известных моделей угроз и нарушителя.

Автореферат диссертации хорошо структурирован, позволяет сделать вывод о научной новизне результатов, их теоретической и практической значимости. Результаты диссертации опубликованы в 5 статьях, 4 из которых опубликованы в рецензируемых научных изданиях, рекомендованных для защиты в диссертационном совете МГУ по специальности 2.3.6. «Методы и системы защиты информации, информационная безопасность».

Отметим, однако, что в тексте автореферата не приведены конкретные формулы оценок стойкости рассматриваемых схем подписи вслепую. Что, впрочем, не снижает научной ценности полученных результатов, в предположении, что такие формулы приведены в тексте диссертации.

Считаю, что автореферат диссертации и процитированные публикации по уровню выполнения, новизне и актуальности в полной мере характеризуют соответствие диссертации 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,
заместитель генерального директора АО «ИнфоТеКС»
по науке и инновациям

Уривский А.В.

«29» октября 2025 г.

Контактные данные:

тел.:

e-mail: urivskiy@infotecs.ru

Адрес места работы:

127273, Москва, ул. Отрадная, д. 2Б, стр. 1

Я, Уривский Алексей Викторович, даю свое согласие на включение моих персональных данных в документы, связанные с работой диссертационного совета, и их дальнейшую обработку.

«29» октября 2025 г.

Подпись Уривского А.В. удостоверяю

Начальник отдела кадров АО «ИнфоТеКС»

Продан А.М.