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

Схемы подписи вслепую представляют собой криптографический механизм, который позволяет одновременно обеспечить целостность данных и их неотслеживаемость. Использование этого механизма в большом количестве сложных прикладных систем привело к тому, что в 2020 году в Техническом Комитете 26 «Криптографическая защита информации» был начат процесс стандартизации отечественной схемы подписи вслепую. К настоящей схеме были, в частности, предъявлены следующие требования: она должна обеспечивать свойство неподделываемости и неотслеживаемости в наиболее сильных моделях безопасности, а стойкость схемы должна быть основана на сложности хорошо изученных задач в группе точек эллиптической кривой. На тот момент в литературе не было известно схем, удовлетворяющих этим требованиям. Однако для большого количества схем подписи вслепую было неизвестно также и обратных результатов, т.е. вопрос их стойкости в наиболее сильных моделях безопасности был открытым.

Диссертационная работа Бабуевой А.А. позволила существенно сузить круг перспективных для стандартизации схем подписи вслепую. Целью работы является получение содержательных оценок стойкости для схемы подписи вслепую Шаума-Педерсена, построенной на основе уравнения подписи Шнорра, и схем подписи вслепую, построенных на основе уравнения подписи Эль-Гамаля. Настоящая цель была успешно достигнута автором.

В первой главе диссертации для схемы Шаума-Педерсена была построена эффективная атака в модели безопасности UF (наиболее сильная модель безопасности, учитывающая угрозу нарушения свойства неподделываемости) и доказана нижняя оценка стойкости в модели

безопасности wUF (более слабая модель безопасности, учитывающая угрозу нарушения свойства неподделываемости) в модели с алгебраической группой и случайным оракулом. Эта оценка свидетельствует о том, что стойкость схемы Шаума-Педерсена в модели wUF основана на сложности решения задач SOMDL и REPR в группе точек эллиптической кривой. Задача REPR ранее была известна в литературе и на текущий момент неизвестно способов ее решения лучших, чем решение задачи дискретного логарифмирования. При этом задача SOMDL является новой, а потому ее надежность вызывает сомнения. Таким образом, из результатов диссертации следует, что схема Шаума-Педерсена не удовлетворяет критериям, предъявляемым к перспективной для стандартизации схеме подписи вслепую.

Во второй главе диссертации для существующих схем подписи вслепую на основе уравнения Эль-Гамаля, не использующих дополнительные криптографические механизмы, построены эффективные атаки, позволяющие нарушить одно из целевых свойств в наиболее сильных моделях безопасности UF и Blind. Этот результат также стал основанием для исключения из рассмотрения при стандартизации схем на основе уравнения Эль-Гамаля. Отмечу, что в третьей главе диссертации рассмотрены прикладные системы, предъявляющие к используемым в них схемам подписи вслепую менее жесткие требования (системы формирования подписи в условиях, когда ключ подписи хранится на функциональном ключевом носителе). Доказано, что в таких системах могут быть использованы и схемы подписи вслепую на основе уравнения Эль-Гамаля. Таким образом, практическая значимость диссертационной работы не вызывает сомнений.

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,
руководитель лаборатории криптографии,
АО "НПК "Криптонит" Шишкин В.А.

Контактные данные:

тел.:
e-mail: v.shishkin@kryptonite.ru
почтовый адрес: 115114, Россия, Москва, наб. Шлюзовая, д. 4.

Адрес места работы:

115114, Россия, Москва, наб. Шлюзовая, д. 4.

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

«__» _____2025 г.

Подпись Шишкина В.А. удостоверяю.