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 являются важным криптографическим механизмом, используемым во многих прикладных информационных системах для обеспечения анонимности участников взаимодействия. Примерами таких систем являются системы электронных платежей и системы подтверждения персональных данных без их разглашения. Несмотря на то, что схемы подписи вслепую были предложены в литературе более 40 лет назад, многие вопросы, связанные с синтезом и анализом схем такого типа, до сих пор являются открытыми. Одним из таких вопросов является возможность построения схем подписи вслепую, обеспечивающих стойкость в наиболее сильных моделях безопасности, на основе группы точек эллиптической кривой. Интерес к таким схемам обусловлен следующими причинами. Во-первых, эллиптические кривые являются одним из наиболее изученных в мировом криптографическом сообществе, и, как следствие, надежных примитивов, используемых для построения высокоуровневых криптографических протоколов. Во-вторых, арифметика в группе точек эллиптической кривой реализована в большинстве средств защиты информации, так как она же лежит в основе работы стандартизированной в Российской Федерации схемы цифровой подписи ГОСТ Р 34.10-2012.

Диссертационная работа Бабуевой А.А. посвящена анализу безопасности конкретных схем подписи вслепую, построенных на основе группы точек эллиптической кривой: схем на основе уравнения Эль-Гамаля и схемы Шаума-Педерсена на основе уравнения Шнорра. Настоящие уравнения лежат в основе большинства классических схем цифровой подписи, построенных на основе группы точек эллиптической кривой, а

потому естественным образом возникает вопрос о возможности построения схемы подписи вслепую с использованием этих же уравнений.

Для известных в литературе схем подписи вслепую на основе уравнения Эль-Гамаля в диссертации получены отрицательные результаты, а именно, разработаны методы нарушения либо свойства неподделываемости в модели безопасности, предоставляющей нарушителю возможность открывать параллельные сеансы протокола формирования подписи, либо свойства неотслеживаемости. Более того, сформулированы условия, которым должна удовлетворять схема подписи вслепую (в частности, конкретные виды уравнения подписи Эль-Гамаля), при которых не применимы разработанные в диссертации методы. Настоящие результаты могут быть использованы для синтеза новых схем подписи вслепую на основе уравнения Эль-Гамаля, при этом они демонстрируют необходимость разработки принципиально новых подходов к порождению эфемерных точек на стороне клиента в протоколе формирования подписи.

Для схемы Шаума-Педерсена также разработан метод нарушения свойства неподделываемости в наиболее сильной модели безопасности. Настоящий метод позволяет строить подделки только для ранее подписываемых сообщений, при этом доказано, что задача построения подделки для нового, ранее не подписываемого сообщения является сложной в предположении сложности задач REPR и SOMDL в группе точек эллиптической кривой. Если задача REPR ранее была известна в литературе, то задача SOMDL является новой, и для поиска наилучших методов ее решения необходимы дополнительные исследования. Таким образом, использование схемы Шаума-Педерсена, так же как и схем на основе уравнения Эль-Гамаля, в прикладных системах, где нарушитель имеет возможность открывать параллельные сеансы протокола формирования подписи, не является безопасным.

Автореферат диссертации четко структурирован, позволяет сделать вывод о теоретической и практической значимости диссертации, о научной

новизне результатов, а также о достижении цели диссертационной работы. Согласно списку, приведенному в автореферате, автором подготовлено и опубликовано по теме диссертации 5 статей, 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.

Вместе с тем к автореферату имеются следующие замечания.

1) Автореферат диссертации не содержит в явном виде формулировок теорем, что не позволяет в полной мере определить конкретные параметры разработанных методов нарушения свойств неотслеживаемости и неподделываемости.

2) Автореферат диссертации содержит в разделе «Существующие схемы подписи вслепую» слишком краткое перечисление существующих подобных схем, как в части задач обоснования стойкости, так и в части дополнительных требований помимо неотслеживаемости и неподделываемости (Fair Blind Signature, Threshold Blind Signature, Proxy Blind Signature, Post-Quantum Blind Signature, Non-interactive Blind Signature, ID-based Blind Signature, Partially Blind Signature, Conditional Blind Signature, Group Blind Signature).

Настоящие замечания носят редакционный характер и не затрагивают научной сути диссертации.

В целом 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, доцент
Доцент кафедры ИУ-8 «Информационная безопасность»
МГТУ им. Н.Э. Баумана А.А. Варфоломеев

Контактные данные:

тел.:
e-mail:
почтовый адрес: , Москва,

Адрес места работы:

105005, Москва, 2-я Бауманская ул., д. 5, с. 1

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

«28» 10 2025 г.

Подпись Варфоломеева А.А. удостоверяю.

«ВЕРНО»
СПЕЦИАЛИСТ ПО ПЕРСОНАЛУ
ПОВАЛЯЕВА И.О.

ОТДЕЛ ПО ОРГАНИЗАЦИИ РАБОТЫ
ЕДИНОЙ ПРИЁМНОЙ
УКСА
МГТУ ИМ. Н.Э. БАУМАНА