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

Актуальность исследования. Схемы подписи вслепую были предложены в работе Д. Шаума, опубликованной в 1982 году, для использования в системах электронных платежей. В этой же работе была предложена первая схема подписи вслепую – схема RSA, стойкость которой основана на сложности задачи факторизации. С тех пор как значительно расширилась область применения схем подписи вслепую (например, они стали использоваться в системах дистанционного электронного голосования и в системах подтверждения персональных данных без их разглашения), так и появилось большое количество схем, построенных на основе различных математических конструкций. Особенно интересным с точки зрения практического использования является класс схем подписи вслепую, построенных на основе группы точек эллиптической кривой и не использующих в алгоритмах формирования и проверки подписи специфичных свойств кривой, таких как возможность построения спариваний. Диссертационная работа А.А. Бабуевой посвящена разработке методов получения обоснованных оценок стойкости для схем подписи вслепую именно такого типа.

Несмотря на то, что в литературе были предложены различные схемы на основе эллиптических кривых, вопрос их стойкости с точки зрения обеспечения свойства неподделываемости долгое время оставался открытым. Так, для самой известной схемы, схемы подписи вслепую Шнорра, еще в 2001 году было доказано, что достаточным условием обеспечения свойства неподделываемости в наиболее сильной модели безопасности является

сложность задач ROS и OMDL. При этом в 2020 году задача ROS была решена за полиномиальное время, что позволило построить алгоритм формирования подделки для схемы подписи вслепую Шнорра (так называемая ROS атака) и, как следствие, доказать, что схема не обеспечивает свойство неподделываемости в наиболее сильной модели безопасности. Для схемы Шаума-Педерсена, построенной на основе такого же уравнения подписи, в принципе отсутствовали математически строго доказанные верхние или нижние оценки стойкости в каких-либо моделях безопасности, учитывающих угрозу нарушения свойства неподделываемости. Аналогичная ситуация сохранялась и для большого количества схем подписи вслепую, построенных на основе уравнения подписи Эль-Гамаля. Таким образом, актуальность темы диссертационного исследования не вызывает сомнений.

Содержание работы. Диссертационная работа состоит из введения, двух вспомогательных разделов, трех глав, заключения и списка литературы из 91 наименования.

Во введении обоснована актуальность темы диссертации, сформулированы цели и задачи исследования, отражены научная новизна, теоретическая и практическая значимость полученных результатов, представлены положения, выносимые на защиту.

Во вспомогательных разделах введены основные понятия, необходимые для понимания дальнейших глав диссертации, а также проведен обзор известных в литературе моделей безопасности для схем подписи вслепую.

Первая глава диссертации посвящена исследованию схемы подписи вслепую Шаума-Педерсена с точки зрения обеспечения свойства неподделываемости в расширенных моделях безопасности, предоставляющих нарушителю возможность открывать параллельные сеансы протокола формирования подписи. Доказано, что схема не обеспечивает свойство сильной неподделываемости в таких условиях, а достаточными условиями обеспечения свойства слабой неподделываемости в модели с алгебраической

группой и случайным оракулом является сложность задач REPR и SOMDL, определенных для группы точек эллиптической кривой.

Во второй главе диссертации введен класс схем подписи вслепую на основе уравнения Эль-Гамаля. Доказано, что существенная часть схем из этого класса не обеспечивает свойство неподделываемости в расширенной модели безопасности, а именно, построена атака, позволяющая построить подделку в результате открытия $l \geq \lceil \log q \rceil$ сеансов протокола формирования подписи, где q – порядок базовой группы точек эллиптической кривой. Схемы, для которых данная атака не применима и первая компонента подписи вырабатывается определенным образом, разделены на два типа. Доказано, что схемы первого типа не обеспечивают свойство неотслеживаемости, а схемы второго типа не обеспечивают свойство неподделываемости даже в слабой модели безопасности, где нарушитель может открывать сеансы протокола формирования подписи только последовательно.

Третья глава диссертации посвящена исследованию стойкости классических схем подписи и схем подписи вслепую на основе уравнения Эль-Гамаля в специализированных моделях безопасности, актуальных в системах формирования подписи, где ключ подписи хранится на потенциально уязвимом ключевом носителе. Предложен метод модификации классической схемы подписи Эль-Гамаля, применение которого позволяет обеспечить защиту от слабого нарушителя с агентом. Доказана нижняя оценка стойкости модифицированной схемы в специализированной модели SUF-CMRA, которая рассматривает угрозу построения подделки и предоставляет нарушителю возможность адаптивно выбирать сообщения для подписи, а также случайные значения и метки времени, используемые в процессе формирования подписи. Также предложен метод использования схем подписи вслепую, которые являются «слепыми модификациями» классических схем подписи, для защиты от сильного нарушителя с агентом. Доказана нижняя оценка стойкости произвольной схемы подписи вслепую в специализированной модели SA-UF (описывает нарушителя, обладающего

возможностями сервера и возможностью накапливать для адаптивно выбираемых сообщений значения подписей, формируемых честным клиентом в результате взаимодействия с нарушителем-сервером), а также нижняя оценка стойкости схем подписи вслепую на основе уравнения Эль-Гамаля в специализированной модели HBC-UF (предоставляет нарушителю возможность навязывать клиенту сообщения для подписи, получать стенограммы протокола формирования подписи и все случайные значения, выбранные клиентом в процессе выполнения протокола).

В заключении перечислены основные результаты диссертации.

Научная новизна, обоснованность и достоверность положений работы. В результате диссертационного исследования Бабуевой А.А. удалось решить все поставленные задачи. В диссертации для схемы подписи вслепую Шаума-Педерсена на основе уравнения Шнорра и схем подписи вслепую на основе уравнений Эль-Гамаля доказаны верхние и нижние оценки стойкости как в стандартных моделях безопасности, учитывающих угрозы нарушения свойств неподделываемости и неотслеживаемости, так и в специализированных моделях безопасности. Отдельно отмечу результаты диссертации, представляющие интерес с практической точки зрения.

1) Все известные в литературе схемы подписи вслепую на основе уравнения Эль-Гамаля не являются стойкими хотя бы в одной из расширенных моделей безопасности, учитывающих угрозы нарушения свойств неподделываемости и неотслеживаемости.

2) Не представляется возможным построить схему подписи вслепую на основе уравнения, используемого в схеме подписи ГОСТ Р 34.10-2012, обеспечивающую свойство неподделываемости в модели, предоставляющей нарушителю возможность открывать параллельные сеансы протокола формирования подписи, без использования дополнительных криптографических механизмов.

3) Разработан метод модификации классической схемы подписи Эль-Гамаля, позволяющий уменьшить длину подписи на четверть и

обеспечивающий свойство неподделываемости даже в условиях, когда датчик псевдослучайных чисел является недоверенным. Настоящий метод может быть использован не только в системах формирования подписи, где ключ подписи хранится на потенциально уязвимом ключевом носителе, но и в других прикладных системах, где сложно обеспечить генерацию «высокоэнтропийных» случайных значений на стороне подписывающего. Примером таких систем являются приложения, где подпись создается на стороне мобильного устройства.

Все выносимые на защиту результаты диссертации являются новыми, сопровождаются строгими математическими доказательствами и были получены и доказаны диссертантом самостоятельно. Результаты работы изложены в 5 публикациях в научных изданиях, индексируемых в Web of Science, Scopus, RSCI и из списка ВАК Минобрнауки России; из них 4 – в изданиях, рекомендованных для защиты в диссертационном совете МГУ по специальности 2.3.6. Методы и системы защиты информации, информационная безопасность. Достоверность выносимых на защиту результатов также подтверждена апробацией результатов на соответствующих данной тематике математических конференциях и семинарах.

Автореферат диссертации в полной мере отражает содержание работы. Полученные диссертантом результаты имеют теоретическую и практическую ценность. Считаю, что полученные автором результаты представляют самодостаточное и законченное исследование, которое является развитием математических методов синтеза и анализа стойких схем подписи вслепую на основе уравнений Шнорра и Эль-Гамаля.

Замечания. Вместе с тем к диссертационной работе имеются следующие замечания.

1) Модели безопасности для схем подписи вслепую и других криптографических механизмов, а также многие алгоритмы работы нарушителей определены в диссертации в формате псевдокода. Несмотря на

то, что такой способ позволяет лаконично и полно описать соответствующие алгоритмы, он не везде сопровождается текстовыми комментариями, что усложняет восприятие и понимание.

2) Для схем подписи вслепую на основе уравнения Эль-Гамаля в диссертации определен общий вид таких схем (класс GenEG-BS). При этом для уравнения Шнорра рассматривается только одна конкретная схема, схема Шаума-Педерсена. Было бы целесообразно определить общий класс схем подписи вслепую на основе уравнения Шнорра, а также выделить конструктивные особенности схем из этого класса, позволяющие построить метод нарушения свойства неподделываемости в различных моделях безопасности.

3) Вычислительные ресурсы, необходимые для реализации разработанных в диссертации методов нарушения свойств неподделываемости и неотслеживаемости, не указаны в явном виде в формулировках соответствующих теорем. Отмечу, однако, что настоящие значения могут быть несложным образом восстановлены из алгоритмов работы нарушителя, приведенных в доказательстве.

Считаю, что указанные замечания не умаляют значимости диссертационного исследования и не снижают общей положительной оценки данной работы.

Заключение. Диссертация отвечает требованиям, установленным Московским государственным университетом имени М.В.Ломоносова к работам подобного рода. Содержание диссертации соответствует специальности 2.3.6. Методы и системы защиты информации, информационная безопасность (по физико-математическим наукам), а также критериям, определенным пп. 2.1-2.5 Положения о присуждении ученых степеней в Московском государственном университете имени М.В.Ломоносова. Диссертационное исследование оформлено согласно требованиям Положения о совете по защите диссертаций на соискание ученой

степени кандидата наук, на соискание ученой степени доктора наук Московского государственного университета имени М.В.Ломоносова.

Таким образом, соискатель Бабуева Александра Алексеевна заслуживает присуждения ученой степени кандидата физико-математических наук по специальности 2.3.6. Методы и системы защиты информации, информационная безопасность.

Официальный оппонент:

Кандидат физико-математических наук,
заместитель руководителя службы сертификации
по научно-техническому сотрудничеству,
ООО «Код Безопасности»

КОРЕНЕВА Алиса Михайловна

23.10.2025

Контактные данные:

тел.: 7(495)9823020 доб. 782, e-mail: A.Koreneva@securitycode.ru.
Специальность, по которой официальным оппонентом
защищена диссертация:
05.13.19 – Методы и системы защиты информации, информационная безопасность

Адрес места работы:

115230, Россия, Москва, 1-й Нагатинский проезд, д. 10, стр. 1
ООО «Код Безопасности», Служба по сертификации, ИБ и криптографии
Тел.: 7(495)9823020; e-mail: info@securitycode.ru

Подпись сотрудника А.М. Кореневой удостоверяю:

подпись сотрудника
подтверждаю
23.10.2025

СТАРШИЙ СПЕЦИАЛИСТ
ПО КАДРОВОМУ
ДЕЛОПРОИЗВОДСТВУ
МОШКИНА Д.М.