**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. Развитие и постоянное усложнение прикладных информационных систем, используемых в современном мире, приводит к необходимости разработки новых криптографических механизмов, обеспечивающих различные неклассические свойства безопасности. Одним из ярких примеров является появление схем подписи вслепую – схем цифровой подписи, обеспечивающих не только аутентичность данных, но и невозможность отслеживания подписей. Такие схемы позволяют пользователям системы получать значения подписи для некоторых сообщений в результате интерактивного взаимодействия с сервером, который является владельцем ключа подписи. Сервер при этом не получает никакой информации о сообщении пользователя и сформированном значении подписи. Использование таких схем потенциально позволяет обеспечивать анонимность участников прикладной системы, что востребовано, например, в системах дистанционного электронного голосования и в системах электронных платежей.

Диссертационная работа Бабуевой А.А. посвящена анализу безопасности схем подписи вслепую, построенных на основе эллиптических кривых. В качестве целевых схем выбираются схемы, построенные на основе уравнений подписи Шнорра и Эль-Гамаля, так как именно эти уравнения лежат в основе большинства классических схем цифровой подписи на основе эллиптических кривых. Несмотря на то, что данные схемы известны еще давно, начиная с 1980-х годов, для большинства из них в литературе не было представлено математически строгих доказательств обеспечения ими свойств невозможности отслеживания и невозможности фальсификации. Более того, для схемы подписи вслепую Шнорра в 2020 году была предложена атака, которая позволяет за полиномиальное время фальсифицировать подпись, используя возможность нарушителя открывать параллельные сеансы протокола формирования подписи. Таким образом, вопрос стойкости других схем, конструкция которых схожа с конструкцией схемы подписи вслепую Шнорра, оставался открытым на момент начала исследования.

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

Во введении обоснована актуальность темы диссертации, сформулированы цели и задачи исследований, отражены научная новизна, теоретическая и практическая значимость полученных результатов, представлены основные результаты, которые выносятся на защиту.

Во вспомогательных разделах вводятся основные определения и обозначения, используемые в диссертации. Так, первый раздел содержит определения базовых криптографических механизмов, а также базовые понятия алгоритмического подхода на основе экспериментатора, используемого в диссертации для математически строго описания моделей безопасности. Второй раздел содержит обзор моделей безопасности для схем подписи вслепую. В этом разделе проводится сравнение существующих моделей безопасности в части определения модели угроз и модели нарушителя, выделяются расширенные модели безопасности, а также специализированные модели безопасности, актуальные в системах формирования подписи, где ключ подписи хранится на функциональном ключевом носителе.

В первой главе диссертации проводится анализ схемы подписи вслепую Шаума-Педерсена, построенной на основе уравнения подписи Шнорра, в расширенных моделях безопасности. Делается вывод о том, что схема не является стойкой в модели, учитывающей угрозу нарушения свойства сильной неподделываемости. А именно, разработан метод нарушения свойства сильной неподделываемости, вероятность успешной работы которого близка к единице. В основе метода лежит так называемая ROS-атака, ранее предложенная зарубежными авторами для схемы подписи вслепую Шнорра. При этом в отличие от схемы Шнорра для схемы Шаума-Педерсена данный метод не позволяет строить подделки для новых сообщений, которые ранее не подписывались в результате честного взаимодействия с сервером. В модели, учитывающей угрозу нарушения свойства слабой неподделываемости, получена верхняя оценка преимущества нарушителя. Эта оценка представляет собой функцию от параметров схемы и модели безопасности, а также от преимуществ нарушителей по решению задач REPR и SOMDL в группе точек эллиптической кривой. Таким образом, достаточным условием обеспечения

свойства слабой неподделываемости в расширенной модели безопасности при соответствующих значениях параметров является сложность задач REPR и SOMDL.

Вторая глава посвящена анализу схем подписи вслепую на основе уравнения Эль-Гамаля в расширенных моделях безопасности. Синтезирован класс схем подписи вслепую GenEG-BS, в котором алгоритмы генерации ключей и проверки подписи полностью совпадают с соответствующими алгоритмами классической схемы подписи Эль-Гамаля. В протоколе формирования подписи определен алгоритм работы серверной стороны, для формирования второй компоненты подписи в нем используется уравнение Эль-Гамаля. Все схемы из класса GenEG-BS разделяются на два типа в зависимости от вида уравнения подписи. Для схем первого типа разработан метод нарушения свойства неподделываемости в расширенной модели безопасности, учитывающей возможность нарушителя открывать параллельные сеансы протокола формирования подписи. Среди схем второго типа выделен подкласс схем, использующий определенный способ генерации первой компоненты подписи. Схемы из этого подкласса также поделены на два вида. Для первого вида схем разработан метод нарушения свойства неотслеживаемости. Для второго вида схем получено утверждение о том, что если такие схемы существуют, то они не обеспечивают свойство неподделываемости даже тогда, когда нарушитель имеет возможность открывать только последовательные сеансы протокола формирования подписи. Поскольку все известные схемы подписи вслепую на основе уравнения Эль-Гамаля принадлежат классу GenEG-BS, делается вывод, что все они не являются стойкими в расширенных моделях безопасности.

Третья глава содержит результаты анализа схем подписи и схем подписи вслепую на основе уравнения Эль-Гамаля в специализированных моделях безопасности. Для классической схемы подписи Эль-Гамаля предложен метод модификации, позволяющий сократить длину подписи на четверть и обеспечивать свойство неподделываемости даже в условиях, когда датчик случайных чисел является недоверенным и возвращает низкоэнтропийные случайные значения. Для модифицированной схемы доказана верхняя оценка преимущества нарушителя в специализированной модели безопасности SUF-CMRA. Для схемы подписи вслепую на основе уравнения Эль-Гамаля доказаны верхние оценки преимущества нарушителя в

специализированных моделях безопасности SA-UF и HBC-UF, моделирующие нарушителя-сервера с агентом и «честного, но любопытного» нарушителя-клиента соответственно.

Характеристика работы. По оценке оппонента, основным достижением исследования является разработка методов анализа стойкости схем подписи вслепую на основе уравнения Эль-Гамаля. Автору диссертации удалось систематизировать подавляющее большинство из десятков известных в литературе схем такого типа, выделить их общие структурные элементы и определить класс схем подписи GenEG-BS, покрывающий все проанализированные схемы. Для этого класса схем удалось сформулировать условия общего вида, выполнение которых позволяет построить метод нарушения одного из целевых свойств безопасности. Указанные результаты позволяют сделать вывод об уровне стойкости всех известных в литературе схем такого типа в расширенных моделях безопасности. Более того, в диссертации были выделены условия, которым должна удовлетворять схема подписи вслепую на основе уравнения Эль-Гамаля (в частности, конкретный вид уравнения подписи), чтобы потенциально обеспечивать стойкость в расширенных моделях безопасности.

Особый интерес также представляет разработанный метод обеспечения защиты систем формирования подписи в условиях использования потенциально уязвимых функциональных ключевых носителей, основанный на использовании схем подписи вслепую. Во-первых, это единственный известный в литературе способ защиты от сильного нарушителя с агентом, во-вторых, задача анализа безопасности данного метода сведена к задаче анализа схемы подписи вслепую в стандартных моделях безопасности, не специфичных для данной прикладной системы. Отдельно отмечу, что этот метод можно применять и для защиты систем формирования подписи, где схема подписи использует другие базовые математические конструкции, отличные от группы точек эллиптической кривой. Единственным ограничением здесь является возможность построения слепой модификации целевой классической схемы подписи.

Все результаты, полученные в диссертации, имеют корректные формулировки и обоснованы строгими доказательствами; результаты работы изложены в публикациях в ведущих научных журналах. Работа апробирована на международных конференциях и научных семинарах.

Автореферат диссертации достаточно полно и точно отражает ее содержание.

Замечания. По диссертации имеются следующие замечания.

1. Для схем подписи вслепую на основе уравнения Эль-Гамаля в диссертации доказано два результата, характеризующих возможность обеспечения такими схемами свойства неподделываемости. Во-первых, доказано, что такие схемы (для большинства видов уравнения подписи) не являются стойкими в модели, где нарушитель имеет возможность открывать параллельные сеансы протокола формирования подписи. Во-вторых, доказано, что такие схемы (при определенном способе выработки первой компоненты подписи) обеспечивают стойкость относительно «честного, но любопытного» нарушителя. Вместе с тем открытым остается вопрос о возможности обеспечения промежуточного уровня стойкости, а именно, стойкости относительно нарушителя, имеющего возможность открывать сеансы протокола формирования подписи только последовательно. В диссертации отсутствуют рассуждения, связанные с этим вопросом.

2. В тексте диссертации используются синонимичные термины «безопасность» и «стойкость», которые употребляются в схожем контексте, но в разных сочетаниях, в частности, «модель безопасности», «свойства безопасности», но «оценка стойкости», «условие стойкости» и т.п. Использование единой терминологии придало бы тексту более строгий вид.

3. В третьей главе описания конструкций схем подписи вслепую на основе уравнения Эль-Гамаля даются в формате псевдокода. Несмотря на то, что такой способ позволяет лаконично и полно описать алгоритмы, он является скорее программистским, чем математическим, и может восприниматься с трудом без дополнительных текстовых комментариев и схем.

Приведенные выше замечания, однако, не снижают существенным образом общей положительной оценки диссертационной работы.

Заключение. Диссертация Бабуевой Александры Алексеевны соответствует требованиям, установленным Московским государственным университетом имени М.В. Ломоносова к кандидатским диссертациям. 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. Диссертация оформлена 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.

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

Официальный оппонент:
профессор кафедры криптологии и кибербезопасности
Института интеллектуальных кибернетических систем
ФГАОУ ВО «Национальный исследовательский
ядерный университет «МИФИ»,
д.т.н., доцент

Запечников Сергей Владимирович

30.10.2025.

Контактные данные:
тел.: +7(495)788-56-99 доб. 91-46, e-mail: SVZapechnikov@mephi.ru.
Специальность, по которой официальным оппонентом
защищена диссертация:
05.13.19 – Методы и системы защиты информации, информационная безопасность

Адрес места работы:
115409, г. Москва, ул. Каширское шоссе, д. 31
ФГАОУ ВО «Национальный исследовательский ядерный университет «МИФИ», кафедра криптологии и кибербезопасности Института интеллектуальных кибернетических систем
Тел.: +7(495)788-56-99; e-mail: info@mephi.ru

Подпись удостоверяю
специалист
отдела регистрации
и приказов НИЯУ МИФИ