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. В диссертационной работе Бабуевой Александры Алексеевны решается задача получения обоснованных оценок стойкости для схем подписи вслепую, реализуемых в группе точек эллиптической кривой. Схемы подписи вслепую применяются в ряде прикладных систем, например, в системах электронных платежей или электронного голосования, и позволяют обеспечивать анонимность пользователей. Использование в качестве базового механизма механизма эллиптических кривых обеспечивает высокую сложность решения математических задач, лежащих в обосновании стойкости рассматриваемых схем подписи вслепую.

Автором диссертации были выбраны для анализа конкретные схемы подписи вслепую – схема Шаума-Педерсена на основе уравнения подписи Шнорра и схемы на основе уравнения подписи Эль-Гамаля. Указанные схемы построены на основе классических схем электронной подписи Шнорра и Эль-Гамаля, и допускают эффективную реализацию в практических приложениях. Исследование стойкости данного класса схем представляется важной и актуальной задачей.

Содержание работы и научная новизна.

Полученные в работе новые научные результаты могут быть интерпретированы следующим образом.

1) В рамках выбранной модели безопасности разработан алгоритмический метод нарушения свойства сильной неподделываемости для схемы подписи вслепую Шаума-Педерсена.

2) Предложен алгоритм сведения задачи о слабой неподделываемости схемы подписи вслепую Шаума-Педерсена к задачам об одновременном решении нескольких задач дикретного логарифмирования (задача SOMDL) и задаче построения линейных форм для дискретных логарифмов заданного множества точек эллиптической кривой (задача REPL).

3) Для схем подписи вслепую, основанных на уравнении Эль-Гамаля, разработаны методы нарушения свойств неподделываемости и неотслеживаемости с учетом заданных возможностей нарушителя.

4) Предложена модификация схемы подписи вслепую Эль-Гамаля, позволяющая уменьшить размер подписи и обеспечить безопасность в условиях использования низкоресурсных вычислительных устройств.

5) Получены обоснованные оценки стойкости предложенной модификации схемы подписи вслепую.

Схемы подписи вслепую представляют собой интерактивные протоколы, в ходе которых происходит обмен информацией между участниками протокола по открытым (недоверенным) каналам связи с целью выработки электронной подписи под заданным сообщением.

Для исследования стойкости таких протоколов могут применяться различные подходы. В диссертационной работе рассматривается подход, при котором стойкость протокола рассматривается как совокупное выполнение двух свойств безопасности: свойства неподделываемости и свойства неотслеживаемости.

Для проверки выполнимости указанных свойств применяется метод, основанный на сведении вопроса о выполнимости рассматриваемых свойств к трудоемкости решения ряда сложных математических задач.

Содержательная часть диссертации посвящена построению алгоритмов сведения и подделки подписи.

Первая глава диссертации посвящена исследованию стойкости варианта схемы подписи вслепую Шаума-Педерсена в части нарушения свойства неподделываемости. Рассматриваются два варианта данного свойства, зависящие от того, что выступает в качестве подделки - подпись (слабая неподделываемость) или пара - сообщение/подпись под ним (сильная неподделываемость).

Автором диссертации предложен явный алгоритм построения подделки, нарушающий свойство сильной неподделываемости, а для слабой неподделываемости - предложен алгоритм сведения решения задачи о построении подделки к решению двух математических задач - задачи об одновременном решении нескольких задач дискретного логарифмирования (задача SOMDL), а также задачи о построении линейных форм для неизвестных дискретных логарифмов заданного множества точек эллиптической кривой (задача REPL). Указанные задачи, очевидно, могут быть решены с помощью методов решения задачи дискретного логарифмирования, однако вопрос о существовании более эффективного подхода к их решению, в настоящее время, представляется открытым.

Предложенный алгоритм сведения является вероятностным, использует вычисления с матрицами, а также алгоритмы поиска корней многочленов над конечными полями. Для алгоритма получены оценки числа операций, необходимых для его реализации, а также оценена вероятность успешного завершения, при этом используются известные ранее результаты о рангах случайных матриц. Приводится пример применения алгоритма к эллиптическим кривым, рекомендуемым для практического применения в отечественных средствах защиты информации.

Вторая глава диссертации посвящена исследованию стойкости схем подписи вслепую, построенных на основе схемы электронной подписи Эль-

Гамаля. Автором предлагается обобщение известных схем подписи вслепую, рассматриваются два класса таких схем и для каждого класса исследуется вопрос о выполнимости свойств безопасности неотслеживаемости.

Для первого класса схем предложен явный алгоритм построения подделки подписи по перехватываемой в канале связи информации. Получена оценка вероятности успешного завершения предложенного алгоритма.

Для второго класса предлагается атака, представляющая собой протокол сетевого взаимодействия в котором нарушитель, перехватывая и навязывая информацию, передаваемую между легитимными участниками протокола, получает информацию о сформированной паре сообщение/подпись и, тем самым, нарушает свойство неотслеживаемости. Для предложенного протокола получена оценка вероятности успешного завершения.

Последняя глава диссертации посвящена исследованию одной из практических областей применения схемы электронной подписи, определяемой отечественным стандартом ГОСТ Р 34.10-2012, а именно, вычислению электронной подписи на низкоресурсных вычислительных устройствах, не обладающих возможностью реализации криптографически стойких генераторов случайных чисел, например, на интеллектуальных картах.

Для возможности вычисления электронной подписи на таком классе устройств автором диссертации предлагается применять протоколы подписи вслепую, используя стойкие генераторы случайных чисел на стороне подписывающего участника протокола. В диссертации приводится пример протокола подписи вслепую, реализующего процесс выработки электронной подписи согласно ГОСТ Р 34.10-2012, а также уточняется перечень возможностей нарушителя. Приводятся математически обоснованные рассуждения, показывающие, что изменение возможностей нарушителя

приводит к невозможности реализации атак, предложенных во второй главе диссертационной работы.

Автореферат соответствует диссертации и достаточно полно отражает ее содержание. Считаю, что диссертационное исследование представляет собой завершенную научную работу, имеющую теоретическую и практическую значимость и вносящую существенный вклад в развитие математических методов анализа схем подписи вслепую.

Обоснованность и достоверность положений работы.

Все результаты диссертации являются новыми, имеют корректные формулировки и обоснованы строгими математическими доказательствами. Достоверность результатов подтверждается 5 публикациями в ведущих научных изданиях, из них 4 – в изданиях, рекомендованных для защиты в диссертационном совете МГУ по специальности 2.3.6. Методы и системы защиты информации, информационная безопасность. Также автором проведена апробация результатов на международных конференциях и научных семинарах по тематике диссертации.

Замечания.

К диссертационной работе имеются следующие замечания.

1) При определении свойства неотслеживаемости для схем подписи вслепую нарушение свойства безопасности понимается как получение нарушителем информации о сформированной паре сообщение/подпись. Для формализации этого свойства определяется эксперимент, в котором протокол формирования подписи выполняется дважды, а задачей нарушителя является сопоставление стенограммы протокола и сформированной пары сообщение/подпись. Однако условие отсутствия у нарушителя какой-либо информации о паре (сообщение, подпись) может быть математически строго описано и другими способами, например, с использованием понятий априорной и апостериорной вероятностей. В диссертации отсутствуют какие-либо комментарии о том, почему выбран именно такой способ формализации

свойства безопасности и, что важно, как он соотносится с другими возможными способами.

2) В ряде случаев для различных сущностей используются одни и те же обозначения, например, символ b обозначает бит, возвращаемый нарушителем в экспериментах, соответствующих задаче различения, выходное значение подписывающего в протоколе формирования подписи, а также длину первой компоненты подписи в модифицированной схеме подписи на основе уравнения Эль-Гамаля.

3) На ряд источников, включенных в список литературы, отсутствуют ссылки в тексте диссертационной работы, например, на ссылки с номерами 48, 49, 51, 59.

4) На странице 43 используется неопределенное ранее понятие «номер аккаунта абонента».

5) На рис. 2.5. на стр.75 в явном виде не указаны шаги протокола формирования подписи; содержание пропущенных шагов становится ясным из контекста изложения.

Вместе с тем, указанные замечания не умаляют значимости диссертационного исследования.

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:

Доктор физико-математических наук,
профессор кафедры компьютерной безопасности Московского института электроники и математики им. А.Н. Тихонова,
ФГАОУ ВО «Национальный исследовательский университет «Высшая школа экономики»

НЕСТЕРЕНКО Алексей Юрьевич

05.11.25г.

Контактные данные:

тел.: 7(495)7729590 доб. 15125, e-mail: anesterenko@hse.ru.
Специальность, по которой официальным оппонентом защищена диссертация:
2.3.6 Методы и системы защиты информации, информационная безопасность

Адрес места работы:

109028, Россия, Москва, Таллинская ул., д.34.
ФГАОУ ВО «Национальный исследовательский университет «Высшая школа экономики», кафедра компьютерной безопасности Московского института электроники и математики им. А.Н. Тихонова

Подпись заверяю