Отзыв научного руководителя

на диссертацию Бабуевой А. А. «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

Диссертация Бабуевой Александры Алексеевны «Свойства безопасности схем подписи вслепую на основе уравнений Шнорра и Эль-Гамаля» посвящена анализу безопасности схем подписи вслепую, построенных на основе группы точек эллиптической кривой. Данные схемы позволяют клиенту, обладающему некоторым сообщением, сформировать значение подписи для данного сообщения в результате взаимодействия с подписывающей стороной, обладающей ключом подписи. При этом подписывающая сторона не получает никакой информации ни о сообщении, ни о сформированном значении подписи (свойство неотслеживаемости), а клиент может сформировать подпись только в результате успешного взаимодействия с подписывающей стороной (свойство неподделываемости).

Вопросы синтеза и анализа схем подписи вслепую за последние десятилетия приобрели особую актуальность, поскольку данные схемы применяются для обеспечения безопасности во многих сложных прикладных информационных системах, таких как системы подтверждения персональных данных без их разглашения, системы электронных платежей, системы дистанционного электронного голосования. В частности, в системах дистанционного электронного голосования, организатор голосования может вслепую подписывать бюллетень избирателя после прохождения им процедуры аутентификации, подтверждая тем самым его право на голосование. При этом вброс бюллетеня от нелегитимного пользователя будет невозможен за счет обеспечения схемой подписи вслепую свойства неподделываемости, а организатор не узнает информацию о голосах избирателей за счет обеспечения схемой свойства неотслеживаемости.

Важным вопросом является возможность построения стойких схем подписи вслепую на основе группы точек эллиптической кривой. Настоящая задача не

является полностью решенной ни в России, ни за рубежом. Так, в международном сообществе IETF/IRTF единственной стандартизированной схемой подписи вслепую является схема RSABSSA, стойкость которой основана на сложности задачи факторизации (см. RFC 9474). В международной организации ISO/IEC стандартизирован ряд схем подписи вслепую на основе задачи дискретного логарифмирования в группе точек эллиптической кривой (см. ISO/IEC 18370-2), однако для всех этих схем известны атаки, позволяющие нарушить свойство неподделываемости в наиболее сильных моделях безопасности, предоставляющих нарушителю возможность открывать параллельные сеансы протокола формирования подписи. В Российской Федерации в настоящее время идет процесс выбора и стандартизации отечественной схемы подписи вслепую, однако на данный момент исследования еще не завершены.

В литературе предложено большое число схем подписи вслепую на основе группы точек эллиптической кривой, однако для большинства из них отсутствуют обоснованные оценки стойкости в моделях безопасности, учитывающих угрозу нарушения свойства неподделываемости. Среди таких схем наибольший интерес представляют следующие. Во-первых, это схема подписи вслепую Шаума-Педерсена, в основе которой лежит уравнение подписи Шнорра. Особое внимание этой схеме стоит уделить, так как ее модификация, схема Брандса, использующая то же самое криптографическое ядро и обладающая дополнительными эксплуатационными свойствами, используется в системе подтверждения персональных данных без их разглашения U-Prove. Другим классом схем, представляющим интерес с практической точки зрения, является класс схем подписи вслепую, в основе которых лежит уравнение подписи Эль-Гамаля. Внимание к этим схемам обусловлено тем, что они используют такой же алгоритм проверки подписи, как и классические схемы подписи на основе уравнения Эль-Гамаля (например, схема подписи ГОСТ Р 34.10-2012 и схема ECDSA). Тогда подписи, сформированные «вслепую» с использованием этих схем, могут быть проверены прикладными системами, использующими соответствующие классические схемы подписи, без реализации какого-либо дополнительного функционала. Диссертационная работа Бабуевой А.А. посвящена получению

обоснованных оценок стойкости для схемы подписи вслепую Шаума-Педерсена, а также схем подписи вслепую на основе уравнения Эль-Гамаля.

Важно отметить, что получение обоснованных оценок стойкости возможно только в определенной модели безопасности. Для схем подписи вслепую в литературе предложено большое количество моделей безопасности, учитывающих реализацию угроз нарушения свойств неотслеживаемости и неподделываемости и отличающихся между собой особенностями задания модели угроз и модели нарушителя. Для свойства неподделываемости, например, ключевым отличием в существующих моделях безопасности является предоставление нарушителю возможности открывать параллельные или последовательные сеансы протокола формирования подписи. Для известных в литературе схем подписи вслепую важно определить границы их защищенности, т.е. выявить наиболее сильные модели безопасности, в которых данные схемы обеспечивают (при некоторых предположениях) стойкость. Соответствующие результаты позволяют сформулировать требования к прикладным системам, в которых потенциально возможно использование данных схем.

Таким образом, актуальность работы Бабуевой А.А. не вызывает сомнений.

В первой главе диссертационной работы Бабуевой А. А. проводится анализ безопасности схемы подписи вслепую Шаума-Педерсена, в основе которой лежит уравнение Шнорра. Несмотря на то, что данная схема была предложена в литературе еще в 1992 году, для нее отсутствовали доказанные оценки стойкости в моделях безопасности, учитывающих угрозу нарушения свойства неподделываемости. В диссертационной работе получена верхняя оценка стойкости в модели, учитывающей угрозу нарушения свойства сильной неподделываемости при атаке с параллельными сеансами, и нижняя оценка стойкости в модели, учитывающей угрозу нарушения свойства слабой неподделываемости при атаке с параллельными сеансами. Таким образом, сделан вывод о невозможности безопасного применения данной схемы подписи вслепую в прикладных системах, допускающих возможность одновременной выдачи подписи

вслепую различным пользователям и не гарантирующим уникальность подписываемых сообщений.

Вторая глава диссертации посвящена анализу схем подписи вслепую на основе уравнения Эль-Гамаля в расширенных моделях безопасности. Автором впервые был описан общий вид таких схем (класс GenEG-BS), в частности, было продемонстрировано, что все существующие схемы на основе уравнения Эль-Гамаля отличаются лишь алгоритмом работы запрашивающей стороны в протоколе формирования подписи. Были выявлены особенности уравнения Эль-Гамаля, позволяющие применить к целевым схемам атаку, аналогичную ROS атаке, предложенной для схемы подписи вслепую Шнорра. Как следствие, были выявлены условия, при которых схемы класса GenEG-BS не обеспечивают свойство неподделываемости в модели, учитывающей атаку с параллельными сеансами. К уязвимым в данной модели схемам относятся и схемы подписи вслепую, построенные на основе уравнения подписи ГОСТ Р 34.10-2012. Далее был проведен анализ безопасности схем, для которых не применима ROS-атака и в которых зафиксирован способ выработки первой компоненты подписи. Было доказано, что все эти схемы не обеспечивают либо свойство неотслеживаемости, либо свойство неподделываемости даже относительно слабых нарушителей, не обладающих расширенными возможностями. Сделан вывод о том, что все известные в литературе схемы подписи вслепую на основе уравнения Эль-Гамаля, использующие механизмы только на основе группы точек эллиптической кривой, не являются стойкими в расширенных моделях безопасности.

Третья глава диссертации посвящена рассмотрению прикладных систем формирования подписи, в которых ключ подписи хранится на потенциально уязвимом ключевом носителе. Анализируются два метода обеспечения защиты такого типа систем: на основе классической схемы подписи и на основе схемы подписи вслепую. Для данных криптографических механизмов определяются специализированные модели безопасности, релевантные в рассматриваемом классе прикладных систем. Так, для схемы подписи такой моделью является ранее известная в литературе модель безопасности SUF-CMRA, предоставляющая нарушителю возможность навязывать случайные значения, используемые в

процессе формирования подписи, и являющаяся более сильной моделью безопасности, чем стандартная модель SUF-CMA. Для модифицированной схемы подписи Эль-Гамаля доказывается нижняя оценка стойкости в модели SUF-CMRA. Для схем подписи вслепую вводятся две новые модели безопасности: SA-UF и HBC-UF, соотношение данных моделей с расширенными моделями безопасности ранее не было известно. В диссертационной работе доказано, что любая схема подписи вслепую обеспечивает стойкость в специализированной модели SA-UF, если она обеспечивает свойство неотслеживаемости в модели HS-BL, где нарушитель честным образом генерирует ключи подписи, и свойство неподделываемости в модели SUF-CMA, где нарушитель является пассивным и имеет только возможность знать промежуточные значения, используемые клиентом в процессе формирования подписи. Таким образом, модель SA-UF является более слабой моделью, чем расширенные модели безопасности. Также для частного случая схем подписи вслепую из класса GenEG-BS в диссертационной работе доказано, что они обеспечивают стойкость в специализированной модели HBC-UF, если они обеспечивают свойство неподделываемости в модели SUF-CMA, т.е. данная специализированная модель безопасности для таких схем также является более слабой, чем расширенные модели безопасности. Отсюда следует, что в рассматриваемом классе прикладных систем потенциально можно использовать схемы подписи вслепую на основе уравнения Эль-Гамаля. Более того, для прикладных систем, реализующих схему подписи ГОСТ Р 34.10-2012, предложена конкретная схема подписи вслепую на основе уравнения Эль-Гамаля, схема Камениша. Для этой схемы доказано, что она обеспечивает стойкость в специализированных моделях безопасности при единственном предположении, что схема подписи ГОСТ Р 34.10-2012 обеспечивает свойство неподделываемости в стандартном смысле (в модели SUF-CMA).

Научные результаты диссертации, выносимые на защиту, получены автором самостоятельно, являются новыми и обоснованными. Результаты других авторов, упомянутые в тексте диссертации, отмечены соответствующими ссылками. Результаты диссертации докладывались и обсуждались на семинаре «Математические методы криптографического анализа» факультета ВМК МГУ

имени. М.В. Ломоносова, международной конференции «Современные информационные технологии и ИТ-образование» в 2021 году, а также на международной конференции CTCrypt в 2022, 2023 и 2024 годах.

Материалы диссертации изложены в 5 печатных работах. Из них четыре работы опубликованы в изданиях, индексируемых в базе ядра Российского индекса научного цитирования «eLibrary Science Index», рекомендованных для защиты в диссертационном совете МГУ имени М.В. Ломоносова. Автореферат соответствует требованиям и правильно отражает содержание диссертации.

Считаю, что диссертационная работа Бабуевой Александры Алексеевны удовлетворяет всем требованиям Положения о присуждении ученых степеней в МГУ имени М.В. Ломоносова и рекомендую ее к защите в диссертационном совете на соискание ученой степени кандидата физико-математических наук по специальности 2.3.6 – «Методы и системы защиты информации, информационная безопасность».

Научный руководитель,

математик кафедры информационной безопасности
факультета вычислительной математики и
кибернетики
МГУ имени М.В. Ломоносова,
д.ф.- м.н. Смышляев Станислав Витальевич

« » _____ 2025 г.

Почтовый адрес: 119991, Москва, ГСП-1, Ленинские горы, МГУ имени М.В. Ломоносова, 2-й учебный корпус
Телефон: +7 (495) 930-43-86
Адрес электронной почты:

Подпись С.В. Смышляева удостоверяю.

Декан факультета вычислительной математики и
кибернетики ФГБОУ ВО
«МГУ имени М.В. Ломоносова»,
академик РАН Соколов Игорь Анатольевич