Заключение диссертационного совета МГУ.012.3
по диссертации на соискание ученой степени кандидата наук

Решение диссертационного совета от «12» ноября 2025 г. № 22 о присуждении Бабуевой Александре Алексеевне, гражданке Российской Федерации, ученой степени кандидата физико-математических наук.

Диссертация «Свойства безопасности схем подписи вслепую на основе уравнений Шнорра и Эль-Гамаля» по специальности 2.3.6 Методы и системы защиты информации, информационная безопасность принята к защите диссертационным советом «24» сентября 2025 г., протокол № 21.

Соискатель **Бабуева Александра Алексеевна**, 1995 года рождения, в 2018 году с отличием окончила магистратуру ФГБОУ ВО Московский государственный университет имени М.В.Ломоносова, факультет Вычислительной математики и кибернетики по кафедре информационной безопасности по специальности 01.04.02 «Прикладная математика и информатика». В 2023 году окончила очную аспирантуру факультета Вычислительной математики и кибернетики МГУ имени М.В.Ломоносова по направлению 10.06.01 «Информационная безопасность».

Соискатель работает в должности математика на кафедре информационной безопасности факультета Вычислительной математики и кибернетики МГУ имени М.В.Ломоносова.

Диссертация выполнена на кафедре информационной безопасности факультета Вычислительной математики и кибернетики МГУ имени М.В.Ломоносова.

Научный руководитель - Смышляев Станислав Витальевич, доктор физико-математических наук, генеральный директор ООО «КРИПТО-ПРО», математик кафедры информационной безопасности факультета Вычислительной математики и кибернетики МГУ имени М.В.Ломоносова.

Официальные оппоненты:

- **Нестеренко Алексей Юрьевич**, 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»;
- **Запечников Сергей Владимирович**, доктор технических наук, доцент, профессор кафедры криптологии и кибербезопасности Института интеллектуальных кибернетических систем ФГАОУ ВО «Национальный исследовательский ядерный университет «МИФИ»;
- **Коренева Алиса Михайловна**, кандидат физико-математических наук,

заместитель руководителя службы сертификации по научно-техническому сотрудничеству ООО «Код безопасности»;
дали положительные отзывы на диссертацию.

Выбор официальных оппонентов обосновывался тем, что оппоненты являются известными специалистами в области синтеза и анализа криптографических протоколов и имеют работы, близкие к теме диссертационного исследования, в центральных математических журналах.

Соискатель имеет 17 опубликованных работ, в том числе по теме диссертации 5 работ, из них 4 работы опубликованы в рецензируемых научных изданиях, рекомендованных для защиты в диссертационном совете МГУ по специальности 2.3.6. Методы и системы защиты информации, информационная безопасность (физико-математические науки). Результаты диссертационной работы опубликованы в открытой печати.

Основные публикации по теме диссертации:

1. Akhmetzyanova L. R., Alekseev E. K., Babueva A. A., Smyshlyaev S. V. «On the (im)possibility of secure ElGamal blind signatures» // Математические вопросы криптографии. 2023. Т. 14. №. 2. С. 25-42 (RSCI WoS, импакт-фактор 0,232 (РИНЦ), 1,1 п.л.). EDN: MTAYSS.

Соавторам принадлежит постановка задачи и обзор существующих схем подписи вслепую на основе уравнения Эль-Гамаля. Остальные результаты статьи получены Бабуевой А.А. (1 п.л., 90 %)

2. Akhmetzyanova L. R., Alekseev E. K., Babueva A. A., Taraskin O. G. «On blindness of several ElGamal-type blind signatures» // Прикладная дискретная математика. 2023. №. 62. С. 13-20 (Scopus, RSCI WoS, импакт-фактор 0,135 (SJR), 0,5 п.л.). EDN: IIXNSY.

Бабуевой А.А. принадлежат три метода нарушения свойства неотслеживаемости (0,4 п.л., 80 %). Остальные результаты статьи получены соавторами.

3. Akhmetzyanova L. R., Babueva A. A., Bozhko A. A. «Blind signature as a shield against backdoors in smart-cards» // Прикладная дискретная математика. 2024. №. 63. С. 49-64 (Scopus, RSCI WoS, импакт-фактор 0,135 (SJR), 1 п.л.). EDN: KLXDGE.

Соавторам принадлежит сравнение разработанного метода обеспечения безопасности систем формирования подписи на основе использования схем подписи вслепую с методом на основе использования доказательства с нулевым разглашением Шнорра. Остальные результаты статьи получены Бабуевой А.А. (0,9 п.л., 90 %).

4. Ахметзянова Л. Р., Бабуева А. А. «О свойстве неподделываемости схемы подписи вслепую Шаума-Педерсена» // Прикладная дискретная

математика. 2024. №. 65. С. 41-65 (Scopus, RSCI WoS, импакт-фактор 0,135 (SJR), 1,6 п.л.). EDN: VEOFUM.

Соавторам принадлежит постановка задачи и обзор сложных задач в группе точек эллиптической кривой. Остальные результаты статьи получены Бабуевой А.А. (1,4 п.л., 88 %)

Дополнительно поступило 6 отзывов на автореферат диссертации, все положительные, 1 акт о внедрении и 1 отзыв на диссертацию, отрицательный.

Диссертационный совет отмечает, что представленная диссертация на соискание ученой степени кандидата физико-математических наук является научно-квалификационной работой, в которой содержатся следующие результаты: для схемы подписи вслепую Шаума-Педерсена на основе уравнения Шнорра доказаны верхняя и нижняя оценки стойкости в моделях безопасности UF и wUF соответственно; для схем подписи вслепую на основе уравнения Эль-Гамаля доказаны верхние оценки стойкости в моделях безопасности UF, Blind и SEQ-UF; введены новые специализированные модели безопасности для схем подписи вслепую, для схем на основе уравнения Эль-Гамаля доказаны содержательные нижние оценки стойкости в этих моделях. Эти результаты вносят вклад и продолжают исследования в области синтеза и анализа криптографических протоколов.

Диссертация представляет собой самостоятельное законченное исследование, обладающее внутренним единством. Положения, выносимые на защиту, содержат новые научные результаты и свидетельствуют о личном вкладе автора в науку:

- Эффективный метод построения подделки в модели безопасности UF для схемы Шаума-Педерсена. Содержательная верхняя оценка величины преимущества нарушителя в модели безопасности wUF схемы Шаума-Педерсена, демонстрирующая, что достаточным условием стойкости схемы при соответствующих значениях параметров является сложность задач REPR и SOMDL в базовой группе точек эллиптической кривой.
- Синтез класса схем подписи вслепую GenEG-BS на основе уравнения Эль-Гамаля, не использующих дополнительные криптографические механизмы. Эффективный метод построения подделки в модели безопасности UF для подкласса схем из класса GenEG-BS. Эффективный метод восстановления первой компоненты подписи в модели безопасности Blind для подкласса схем из класса GenEG-BS. Эффективный метод построения подделки в модели безопасности SEQ-UF для подкласса схем из класса GenEG-BS.

- Метод модификации схемы подписи Эль-Гамаля, позволяющий уменьшить размер подписи на четверть и обеспечить безопасность в условиях использования недоверенного датчика случайных чисел при формировании подписи. Содержательная верхняя оценка величины преимущества нарушителя в модели безопасности SUF-CMRA для модифицированной схемы.
- Содержательные верхние оценки величины преимущества нарушителя в специализированных моделях безопасности SA-UF и HBC-UF для схем подписи вслепую на основе уравнения Эль-Гамаля.

В диссертации используются методы теории вероятностей, линейной алгебры и теории сложности вычислений.

Результаты диссертации имеют законченный характер и снабжены строгими математическими доказательствами, являются новыми, прошли апробацию на международных конференциях и научных семинарах. Основные результаты диссертационной работы опубликованы в научных изданиях, рекомендованных для защиты в диссертационном совете МГУ по специальности 2.3.6. Методы и системы защиты информации, информационная безопасность (физико-математические науки).

На заседании 12.11.2025 диссертационный совет принял решение присудить Бабуевой А.А. ученую степень кандидата физико-математических наук.

При проведении тайного голосования диссертационный совет в количестве 20 человек, из них 4 доктора наук по специальности рассматриваемой диссертации, участвовавших в заседании, из 26 человек, входящих в состав совета, проголосовали: за 19, против 1, недействительных бюллетеней нет.

Заместитель председателя
диссертационного совета,
д.ф.-м.н., профессор **Васенин В.А.**

Ученый секретарь
диссертационного совета,
к.ф.-м.н. **Галатенко А.В.**

Дата 12.11.2025