

ОТЗЫВ на автореферат диссертации
Бабуевой Александры Алексеевны
«Свойства безопасности схем подписи вслепую на основе уравнений
Шнорра и Эль-Гамала», представленной на соискание ученой степени
кандидата физико-математических наук
по специальности 2.3.6. Методы и системы защиты информации,
информационная безопасность

Работа Бабуевой Александры Алексеевны, посвященная анализу свойств безопасности схем подписи вслепую, имеет несомненную теоретическую и практическую пользу в современном обществе.

Российская Федерация, являясь одним из несомненных лидеров в цифровизации повседневной жизни общества, с 2020 года проводит выборы с использованием Федеральной платформы электронного голосования (ДЭГ).

Уровень социальной значимости внутри страны, влияния на дальнейшую жизнь общества, доверия к системе выборов как со стороны международного сообщества, так и внутренних наблюдателей, является беспрецедентным. Именно по этим причинам теоретические основы и реализация используемых криптографических схем должны иметь строгую доказательную базу.

Электронное голосование, которое переносит обычное «бумажное» голосование в электронный вид, должно обеспечивать ровно те же свойства, которые закреплены в законодательстве Российской Федерации (как и в законодательстве большинства стран мира), а именно – неотслеживаемость (анонимность голосования) и неподделываемость (один бюллетень = один учтённый голос, защита от «вбросов»).

Такие свойства базово обеспечиваются схемами подписи вслепую, при которых подписант не имеет возможности ознакомиться с подписываемым сообщением, а получатель при этом может проверить его подлинность.

Необходимо учитывать, что при электронном взаимодействии с использованием общедоступных каналов связи, злоумышленник может пытаться действовать от имени неограниченного количества участников

информационного обмена (голосования), пытаюсь нарушить свойство неподделываемости, открывая при этом параллельные сеансы протокола формирования слепой подписи. И выбранная схема, которая ложится в основу электронного голосования, должна иметь теоретическую основу обеспечения указанных свойств.

В работе проведён детальный анализ существующих схем, основанных на уравнениях Шнорра и Эль-Гамала (построенных на основе группы точек эллиптической кривой), включая математические задачи, на которых основана их сложность, и известные работы по анализу сложности в различных условиях – множествах (моделях) нарушителей.

Несомненно, важной частью работы является разработка метода нарушения обязательных свойств схемы слепой подписи Шаума-Педерсена, а также получение при помощи разработанного метода практических результатов, которые показывают несостоятельность данной схемы для применения в практических условиях с выбранными возможностями нарушителя и с учетом отсутствия доказательства сложности решения задачи SOMDL.

Также проведён анализ схем подписи вслепую на основе уравнения Эль-Гамала (включая ГОСТ Р 34.10-2012), в процессе которого предложены методы, демонстрирующие недостаточную стойкость данных схем в расширенных моделях безопасности.

При этом разработан метод модификации схемы подписи Эль-Гамала, позволяющий не только обеспечить безопасность в условиях использования недоверенного датчика случайных чисел при формировании подписи, но и уменьшить размер подписи на четверть. А также доказаны содержательные верхние оценки преимущества нарушителя и, соответственно, нижние оценки стойкости в специализированных моделях безопасности для схем Эль-Гамала (с предложенными модификациями и без них).

Таким образом, практическая значимость диссертационной работы не вызывает сомнений.

Судя по автореферату и публикациям, диссертация Бабуевой А.А. по уровню выполнения, новизне и актуальности соответствует критериям, установленным в Положении о присуждении ученых степеней в Московском государственном университете имени М. В. Ломоносова для диссертаций на соискание ученой степени кандидата наук, а ее автор, Бабуева Александра Алексеевна, заслуживает присуждения ученой степени кандидата физико-математических наук по специальности 2.3.6. Методы и системы защиты информации, информационная безопасность.

Кандидат технических наук,
Технический директор
ООО «СэйфТек Лаб»

Мельниченко П.А.

Контактные данные:

тел.:

e-mail: p.melnichenko@safe-tech.ru

почтовый адрес: 123308, г. Москва, ул. 3-я Хорошевская д. 18, корп. 1, офис 104

Адрес места работы: 123308, г. Москва, ул. 3-я Хорошевская д. 18, корп. 1, офис 104

Я, Мельниченко Павел Александрович, даю свое согласие на включение моих персональных данных в документы, связанные с работой диссертационного совета, и их дальнейшую обработку.

«28» октября 2025 г.

Подпись Мельниченко П.А. удостоверяю.

Генеральный директор
ООО «СэйфТек Лаб»

А.И.Санин