

ОТЗЫВ

научного руководителя о диссертационной работе

Сабри Наураса Хуссейна Сабри

«Методы снижения вычислительной сложности цифровой подписи для устройств с ограниченными ресурсами», представленной на соискание ученой степени кандидата технических наук по специальности 2.3.6 – Методы и системы защиты информации, информационная безопасность.

Сабри Н. Х. С., 1987 года рождения, в 2009 году получил степень бакалавра в области компьютерной инженерии, а в 2017 году окончил Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина) по направлению «Инфокоммуникационные технологии и системы связи», где ему была присвоена квалификация «магистр». В 2022 году он поступил в аспирантуру СПбГЭТУ «ЛЭТИ» по специальности 2.3.6 «Методы и системы защиты информации, информационная безопасность» и успешно завершил обучение в 2025 году. В период подготовки диссертации работал младшим научным сотрудником лаборатории «Фундаментальных основ построения интеллектуальных систем» кафедры информационной безопасности факультета компьютерных технологий и информатики.

Под моим руководством Сабри Н. Х. С. выполнил диссертационную работу, посвящённую разработке и исследованию методов снижения вычислительной сложности криптографических алгоритмов электронной цифровой подписи (ЭЦП) для устройств с ограниченными вычислительными ресурсами, таких как микроконтроллерные системы, применяемые в встроенных и беспилотных системах. Актуальность исследования обусловлена необходимостью обеспечения требуемого уровня информационной безопасности при ограниченных возможностях аппаратных средств в реальном времени, что представляет собой важную и недостаточно изученную задачу в области защиты информации.

В работе Сабри Н. Х. С. решена комплексная научная задача, заключающаяся в разработке математических методов оптимизации операции умножения точки на эллиптической кривой и построения схем электронной цифровой подписи, направленных на снижение вычислительной сложности без потери криптостойкости. Им предложены два новых математических метода, основанных на использовании свойств циклических групп и аддитивной инверсии из теории групп, а также усовершенствованный метод построения схемы ЭЦП на основе эллиптических кривых (ЕСС), обеспечивающий сокращение вычислительных операций, памяти и времени

выполнения. Разработанные методы прошли программную реализацию на платформе ATmega2560 и показали высокую эффективность — снижение вычислительной нагрузки до 82 %, сокращение числа процессорных тактов до 71 % и уменьшение использования оперативной памяти до 80 %.

Практическая значимость работы подтверждена внедрением результатов исследования в ООО «ТР-СОФТ» и АНО «Институт инженерной физики». Результаты могут быть использованы при проектировании и разработке защищённых микроконтроллерных систем, встроенных решений и беспилотных комплексов, где предъявляются повышенные требования к эффективности и надёжности криптографических протоколов при ограниченных вычислительных ресурсах.

Научные результаты диссертации Сабри Н. Х. С. опубликованы в 12 работах, включая статьи в рецензируемых журналах, рекомендованных ВАК («Вестник компьютерных и информационных технологий», «Труды учебных заведений связи»), международных изданиях, индексируемых в Scopus и Web of Science (Applied Sciences, IEEE Access, Mathematics, Scientific Reports), а также в свидетельствах о государственной регистрации программ для ЭВМ. Это подтверждает высокий уровень самостоятельности и научной активности автора.

В ходе выполнения диссертационной работы Сабри Н. Х. С. проявил себя как целеустремлённый, трудолюбивый и высококвалифицированный исследователь, обладающий глубокими знаниями в области информационной безопасности, системного анализа и теории криптографии. Ему присущи логичность мышления, высокий уровень математической культуры и способность к синтезу теоретических и прикладных аспектов исследования. Все результаты работы получены лично соискателем и свидетельствуют о его умении формулировать научные задачи, проводить их моделирование и анализировать результаты с высокой степенью достоверности.

Диссертация Сабри Наураса Хуссейна Сабри является завершённой научно-квалификационной работой, выполненной на высоком теоретическом и практическом уровне. Полученные в ней результаты обладают научной новизной, теоретической и практической значимостью и могут быть использованы при разработке современных методов и средств защиты информации для встраиваемых систем, и устройств с ограниченными ресурсами.

Считаю, что диссертационная работа Сабри Наураса Хуссейна Сабри полностью соответствует требованиям пп. 9–14 «Положения о присуждении учёных степеней»,

утверждённого постановлением Правительства РФ от 24 сентября 2013 г. № 842, предъявляемым к диссертациям на соискание ученой степени кандидата технических наук, и может быть представлена к защите в диссертационный совет по научной специальности 2.3.6 – «Методы и системы защиты информации, информационная безопасность».

Научный руководитель
кандидат физико-математических наук, доцент,
руководитель лаборатории «Фундаментальных основ построения интеллектуальных систем»,
доцент кафедры информационной безопасности
Санкт-Петербургского государственного электротехнического университета «ЛЭТИ»
им. В.И. Ульянова (Ленина)

 Левина Алла Борисовна

10 Ноября 2025 года
Рабочий адрес: ул. Профессора Попова, дом 5 литера Ф, Санкт-Петербург, 197022
Тел. +7 (911) 243-36-93
Email: alla_levina@mail.ru

