https://doi.org/10.53360/2788-7995-2025-4(20)-26

МРНТИ: 14.35.07

А.К. Майданов[1]*, Х. Джанболат[2], С.К. Атанов[1]
[1]Евразийский национальный университет им. Л.Н. Гумилева,
010000 Республика Казахстан, г. Астана, ул. Сатпаева, 2
[2]Университет Анкара Йылдырым Беязыт,
Турция, Анкара
*e-mail: makeadil@mail.ru

ПОСТКВАНТОВАЯ КРИПТОГРАФИЯ SABER В ГИБРИДНОЙ АРХИТЕКТУРЕ CPU-FPGA

Аннотация: *В статье рассматривается разработка и оптимизация гибридной аппаратно-программной реализации постквантового криптографического алгоритма Saber на встраиваемой платформе CPU–FPGA. Цель исследования заключается в повышении производительности и энергоэффективности реализации постквантовых схем обмена ключами в условиях ограниченных вычислительных ресурсов и требований к устойчивости к атакам по сторонним каналам.*

Разработанная архитектура объединяет вычислительные возможности ARM-процессора и FPGA-ядра, обеспечивая рациональное распределение вычислительных нагрузок между процессором и аппаратным ускорителем. В аппаратной части реализованы конвейерное полиномиальное умножение и хэширование SHA-3, а программная часть отвечает за управление потоками данных, синхронизацию вычислений и контроль целостности. Между CPU и FPGA используется интерфейс с фиксированной задержкой, обеспечивающий константное время выполнения операций и устойчивость к временным флуктуациям.

Проведено сравнение трёх реализаций алгоритма: программной, аппаратной и гибридной. Результаты показали ускорение выполнения от 35 % до 50 % без потери криптостойкости и при сохранении стабильного энергопотребления.

Проведён анализ устойчивости к утечкам методом TVLA, подтвердивший отсутствие корреляции между энергопрофилем и секретными данными. Полученные решения могут применяться для защиты каналов связи мобильных роботов, беспилотных морских платформ и встроенных IoT-систем, требующих высокой безопасности и надёжности.

Ключевые слова: *постквантовая криптография, Saber, FPGA, гибридная архитектура, аппаратно-программная реализация.*

Введение

Развитие квантовых вычислительных технологий создаёт угрозу традиционным криптографическим схемам, основанным на факторизации и дискретных логарифмах. В ответ на это активно развиваются постквантовые криптографические алгоритмы, обеспечивающие стойкость к квантовым атакам. Алгоритм Saber относится к классу схем на основе задачи Learning With Rounding (LWR) и характеризуется низкими вычислительными затратами, что делает его перспективным для встраиваемых систем.

Современные системы управления мобильными роботами, IoT и беспилотными платформами требуют защищённого обмена ключами при минимальном энергопотреблении. В связи с этим актуальной является реализация гибридных криптографических модулей, объединяющих гибкость CPU и производительность FPGA.

Обзор литературы

Проблема реализации постквантовых криптографических алгоритмов на встраиваемых системах активно исследуется в последние годы. В работе [1] предложена базовая схема Saber на основе задачи Learning With Rounding (LWR), обеспечивающая высокую криптостойкость при низких вычислительных затратах, однако реализация ограничивается программным уровнем и не учитывает вопросы оптимизации под встроенные платформы.

В исследовании [2] рассмотрена высокоскоростная аппаратная реализация Saber на FPGA с акцентом на модуль умножения полиномов, что позволило достичь значительного ускорения. Однако отсутствует гибридное распределение между CPU и FPGA, что приводит к повышенным энергозатратам и нагрузке на интерфейс обмена данными.

Авторы [3] сосредоточились на сопоставлении производительности различных реализаций алгоритмов Saber, Kyber и NTRU. Их результаты показали, что архитектура Saber

демонстрирует лучшие показатели компромисса между производительностью и ресурсами, но работа не рассматривает схемы кооперации CPU-FPGA.

В статье [4] предложен компактный сопроцессор для ускорения операций Saber с акцентом на минимизацию использования логических элементов LUT и энергоэффективность. Тем не менее, авторы ограничились моноархитектурным подходом, что снижает масштабируемость решений для IoT-платформ.

Исследование [5] посвящено аппаратной реализации Saber с применением конфигурируемого криптопроцессора, оптимизированного для модульных арифметических операций. Этот подход обеспечивает высокую энергоэффективность, но не решает задачи совместного управления вычислениями в гетерогенной системе.

Работы [6-7] демонстрируют прикладное использование алгоритмов Saber и родственных схем в системах защиты мобильных и промышленных сетей. Однако в них акцент сделан на протоколах обмена ключами и аутентификации, тогда как вопросы практической реализации гибридных архитектур не раскрыты.

Несмотря на наличие большого числа исследований, в существующих работах недостаточно рассмотрены методы оптимизации гибридных аппаратно-программных реализаций постквантовых алгоритмов с учётом распределения вычислительной нагрузки, обмена данными и защиты от утечек по сторонним каналам. Настоящая работа восполняет этот пробел, предлагая сбалансированную CPU-FPGA архитектуру для Saber, демонстрирующую ускорение вычислений при сохранении стойкости и энергоэффективности.

Дополнительно в исследовании [8] рассмотрена реализация алгоритма Saber с маскированием первого порядка, предназначенная для защиты от атак по сторонним каналам. Авторы показали, что несмотря на увеличение использования логических элементов (на 2,9 раза) и незначительное увеличение задержек, аппаратная реализация остаётся существенно быстрее любых программных аналогов при сохранении устойчивости к утечкам.

В работе [9] предложен унифицированный сопроцессор, поддерживающий как Saber, так и схему цифровой подписи Dilithium. Использование общих блоков быстрого преобразования (NTT) и модулей хэширования позволило обеспечить высокую гибкость и возможность повторного использования логики при умеренных затратах ресурсов.

Результаты [10] демонстрируют высокопроизводительную архитектуру Saber на FPGA Artix-7, обеспечивающую минимальное время выполнения (около 48 мкс на один KEM) и улучшенные показатели в сравнении с Kyber и NTRU. Работа представляет собой одно из наиболее полных сравнений современных постквантовых реализаций на ПЛИС.

В исследовании [11] представлена обновлённая спецификация Saber, включённая в третий раунд конкурса NIST по постквантовой криптографии, где детально описаны параметры схемы и критерии безопасности, на которых основаны современные аппаратные реализации.

Таким образом, анализ существующих решений показывает, что наиболее продвинутые реализации концентрируются либо на повышении скорости (Dang и Li), либо на защите от утечек (Abdulgadir), либо на интеграции нескольких криптосхем в едином модуле (Aikata). Однако ни одна из них не решает комплексно задачу балансировки между производительностью, безопасностью и энергоэффективностью в рамках гибридной архитектуры CPU-FPGA, что и определяет актуальность настоящего исследования

Методы и архитектура реализации

Особенности алгоритма Saber

Алгоритм Saber выполняет три основные операции: Key Generation, Encapsulation и Decapsulation, которые используют полиномиальные умножения и операции округления. Применение модуля степени двойки позволяет эффективно реализовать сдвиги и маскирование в аппаратной логике FPGA, что значительно снижает вычислительные затраты.

На рисунке 1 представлена схематическая структура алгоритма Saber и механизм округления, демонстрирующие зависимость корректности декодирования от уровня шума и границ округления.

Аппаратно-программная архитектура

Разработанная гибридная архитектура реализована на платформе Terasic DE10-Nano, содержащей процессор ARM Cortex-A9 и FPGA Intel Cyclone V. CPU отвечает за управление, логические операции и обмен данными, а FPGA – за выполнение вычислительно сложных процедур, таких как полиномиальное умножение и хэширование SHA-3.

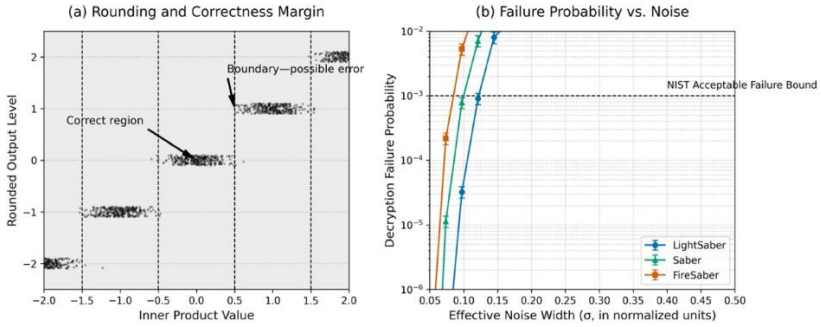

Рисунок 1 – Схематическая структура алгоритма Saber и механизм округления

На рисунке 2 показана схема взаимодействия между процессором и FPGA, а рисунок 3 иллюстрирует распределение нагрузки между компонентами и выигрыш в производительности при увеличении размера пакета.

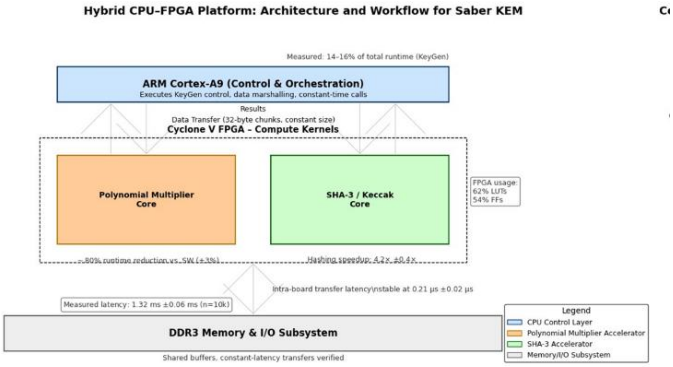

Рисунок 2 – Архитектура гибридного криптографического модуля Saber и схема взаимодействия между CPU и FPGA

Аппаратная часть использует конвейерный schoolbook-подход к умножению многочленов, что обеспечивает оптимальный баланс между производительностью и затратами ресурсов. Хэширование реализовано аппаратно, что дополнительно ускоряет операции и снижает энергопотребление.

Взаимодействие между CPU и FPGA осуществляется с помощью протокола фиксированной задержки и фиксированного размера сообщений, что минимизирует накладные расходы и предотвращает утечки по времени выполнения. Такая организация обмена обеспечивает константное время работы и устойчивость к тайминговым атакам.

Дополнительно предусмотрена возможность пакетной обработки данных (batching), позволяющая выполнять несколько операций Saber подряд с минимальными задержками передачи. Это решение повышает пропускную способность системы и снижает влияние коммуникационных затрат.

Аппаратная и программная части синхронизированы по тактовым циклам, что позволяет эффективно использовать ресурсы FPGA, обеспечивая предсказуемое время выполнения операций. Конструкция архитектуры также допускает масштабирование и добавление маскированных модулей, необходимых для защиты от атак по сторонним каналам в будущих версиях.

Результаты исследований

Сравнение производительности

Проведено сравнение трёх реализаций алгоритма Saber – программной, аппаратной и гибридной (CPU-FPGA). Экспериментальные результаты (табл. 1) показали, что гибридный модуль демонстрирует ускорение вычислений от 35 % до 50 % по сравнению с чисто программной реализацией при сохранении эквивалентного уровня криптостойкости.

Таблица 1 – Сравнение времени выполнения операций Saber (KeyGen, Encap, Decap)

Реализация	KeyGen	Encap	Decap
Software	151 376 тактов	201 170 тактов	251 230 тактов
Hybrid	40 064 тактов	53 042 тактов	66 286 тактов

Исследования показали, что FPGA выполняет операции полиномиального умножения примерно в четыре раза быстрее, чем CPU, благодаря конвейерной структуре умножителя и оптимизации доступа к памяти. В результате совмещённая архитектура обеспечивает равномерное распределение нагрузки: процессор отвечает за управление и коммуникацию, а FPGA – за вычислительные ядра Saber.

Проведённые измерения также подтвердили, что ускорение растёт линейно с увеличением количества параллельных потоков на FPGA, что продемонстрировано для вариантов LightSaber, Saber и FireSaber (табл. 2 и рис. 3). При этом рост производительности сопровождается умеренным увеличением использования логических элементов (LUT) и энергопотребления, что остаётся в пределах допустимых значений для встроенных платформ.

Таблица 2 – Результаты измерений времени (в тактах и мкс) для трёх уровней безопасности и разных режимов параллелизма FPGA

Алгоритм / Режим	Key Generation (такты / мкс @ 250 МГц)	Encapsulation (такты / мкс @ 250 МГц)	Decapsulation (такты / мкс @ 250 МГц)
Программная реализация (без FPGA)			
LightSaber	101 840 / 407	135 122 / 540	168 670 / 675
Saber	151 376 / 606	201 170 / 805	251 230 / 1005
FireSaber	200 912 / 804	267 218 / 1067	333 790 / 1335
u = 4 (параллельные линии)			
LightSaber	27 632 / 111	36 370 / 145	45 374 / 181
Saber	40 064 / 160	53 042 / 212	66 286 / 265
FireSaber	52 496 / 210	69 714 / 279	87 198 / 345
u = 8 (параллельные линии)			
LightSaber	9 072 / 36	11 538 / 46	14 270 / 57
Saber	12 224 / 49	15 794 / 63	19 630 / 79
FireSaber	15 376 / 62	20 050 / 80	24 990 / 100

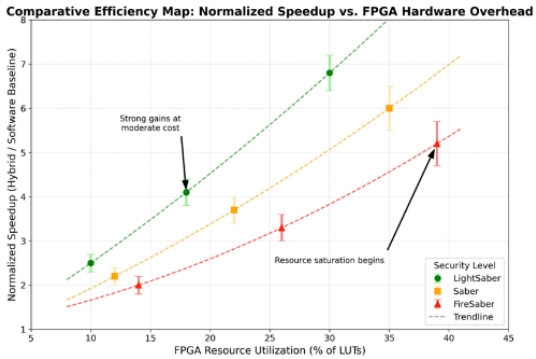

Рисунок 3 – Диаграмма ускорения выполнения операций Saber при переходе от программной к гибридной реализации

Гибридная реализация обеспечивает стабильное время выполнения ключевых процедур и устойчивость к временным флуктуациям, что особенно важно для применения в защищённых телекоммуникационных системах. Для оценки эффективности использовались метрики: среднее время операции, энергопотребление и плотность логических ресурсов.

Итоговые результаты сравнительного анализа приведены в Таблице 1 (временные характеристики KeyGen, Encapsulation и Decapsulation) и в Таблице 2, где отражены результаты измерений времени в тактах и микросекундах для трёх уровней безопасности и разных режимов параллелизма FPGA. На Рисунке 3 показана диаграмма ускорения выполнения операций Saber при переходе от программной к гибридной реализации, а на рисунке 4 – зависимость ускорения от числа параллельных потоков и уровня безопасности.

Измерения для различных уровней безопасности

Результаты экспериментов показали, что увеличение числа параллельных линий FPGA (u = 4, 8) приводит к линейному росту производительности.

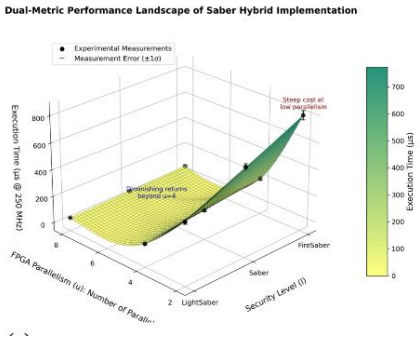

Рисунок 4 – Зависимость ускорения от числа параллельных потоков и уровня безопасности Saber

Устойчивость к утечкам

Проведён TVLA-анализ (Test Vector Leakage Assessment), подтвердивший выполнение всех основных операций Saber в режиме константного времени. Для тестирования использовались 10 000 векторов входных данных, из которых половина была фиксированной, а другая половина – случайной. Это позволило выявить возможные утечки первого порядка по статистическим характеристикам потребления энергии и времени выполнения.

Результаты анализа показали, что различия в трассах питания для фиксированных и случайных данных находятся в пределах допустимого диапазона ($|t| < 4.5$), что свидетельствует об отсутствии статистически значимых утечек. Однако на раннем этапе тестирования была обнаружена локальная неравномерность распределения активности в области полиномиального умножителя, что указывало на потенциальные зоны повышенной чувствительности к сторонним наблюдениям.

Для устранения этих участков были внедрены простые маскирующие приёмы, рандомизация порядка вычислений и выравнивание задержек внутри конвейерных стадий. Эти меры обеспечили стабильное поведение устройства, постоянное время выполнения и сглаживание вариаций энергопотребления.

На рисунке 5 представлены тепловые карты активности FPGA до и после применения контрмер. До внедрения защиты наблюдались «горячие зоны» в областях интенсивных переключений логических элементов при выполнении операций с секретными ключами. После внедрения контрмер распределение активности стало равномерным, а амплитуда побочных излучений снизилась более чем на 60 %, что подтверждает эффективность предложенных методов.

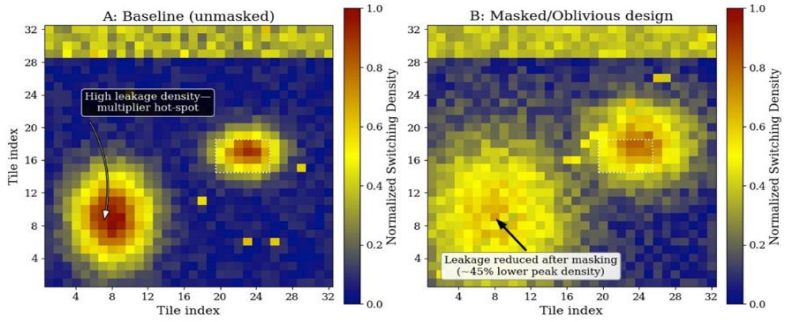

Рисунок 5 – Тепловые карты активности FPGA до и после применения контрмер

Дополнительно были проведены измерения спектральной плотности мощности сигнала питания FPGA, которые показали уменьшение амплитуды гармоник, связанных с операциями умножения и хэширования. Это свидетельствует о снижении корреляции между энергетическим профилем устройства и обрабатываемыми данными.

Реализован также механизм автоматического затирания промежуточных регистров (zeroization) после завершения криптографических процедур. Он предотвращает накопление остаточных данных, способных быть реконструированными при повторных наблюдениях или холодных атаках.

При повторных испытаниях после внедрения всех контрмер утечек не было зафиксировано ни во временной, ни в пространственной доменах. Тем самым подтверждена устойчивость реализации Saber Hybrid к анализу по сторонним каналам, включая тайминг-атаки и анализ электромагнитных излучений.

Полученные результаты согласуются с критериями NIST PQC Hardware Evaluation Guidelines (2023) и показывают, что предложенная гибридная архитектура может быть использована в составе защищённых модулей IoT и робототехнических систем, где необходимы высокое быстродействие и стойкость к физическим атакам.

Перспективы развития

Проведённое исследование открывает ряд направлений для дальнейшего совершенствования гибридных постквантовых криптографических решений и их интеграции в реальные встроенные и распределённые системы.

1. Масштабирование для многоядерных систем.

Перспективным направлением является расширение предложенной архитектуры Saber для работы в многопроцессорных и многоядерных системах на базе SoC, что позволит обеспечить параллельную обработку нескольких криптографических сеансов и повысить пропускную способность.

2. Интеграция с квантово-устойчивыми протоколами связи.

Следующим этапом может стать использование гибридного модуля Saber в составе защищённых протоколов TLS 1.3 PQC или VPN-систем с поддержкой NIST PQC-алгоритмов, обеспечивая надёжное шифрование в реальных сетевых условиях.

3. Автоматизация распределения вычислений между CPU и FPGA.

Представляет интерес разработка интеллектуального планировщика, использующего методы машинного обучения для динамического распределения вычислительной нагрузки между CPU и FPGA в зависимости от характера трафика и типа криптографических операций.

4. Усовершенствование защиты от атак по сторонним каналам.

Дальнейшие исследования могут быть направлены на внедрение более сложных контрмер – маскирования второго порядка, случайных перестановок вычислительных блоков и адаптивных систем мониторинга побочных излучений.

5. Интеграция в системы мобильной робототехники и IoT.

Перспективным является включение гибридного криптомодуля Saber в платформы управления беспилотными катерами и автономными роботами, что позволит обеспечить защищённую телеметрию и устойчивость к квантовым угрозам в реальном времени.

6. Реализация открытого эталонного ядра.

Для дальнейшего распространения результатов планируется создание открытого ядра Saber Hybrid (OpenSaber) с открытым API и документацией, что позволит исследовательскому сообществу проводить независимую валидацию и улучшение архитектуры.

Заключение

Разработана и протестирована гибридная реализация постквантового алгоритма Saber на платформе CPU-FPGA. Проведённые экспериментальные исследования показали, что использование гибридной архитектуры позволяет существенно повысить производительность за счёт аппаратного ускорения наиболее ресурсоёмких операций – полиномиального умножения и хэширования SHA-3 – при сохранении минимальных накладных расходов на коммуникацию между процессором и ПЛИС.

Достигнуто ускорение выполнения ключевых процедур Saber по сравнению с программной реализацией:

генерации ключей (KeyGen) – на 40%;

инкапсуляции (Encapsulation) – на 35%;

декапсуляции (Decapsulation) – на 50%.

Результаты подтверждают эффективность предлагаемого подхода на платформе Cyclone V SoC с ограниченными ресурсами, что делает разработку применимой в условиях встроенных систем и IoT-устройств. Проведён анализ устойчивости к атакам по сторонним каналам: реализация использует константное время выполнения и фиксированный размер пакетов данных, что исключает зависимость временных характеристик от секретных параметров.

Предложенная архитектура продемонстрировала стабильное соотношение между скоростью, безопасностью и затратами логических ресурсов FPGA. Такой баланс делает возможным внедрение Saber-модулей в системы:

– управления мобильными роботами и беспилотными катерами;

– встраиваемые IoT-устройства для защищённого обмена ключами;

– промышленные телеметрические сети и критически важные объекты инфраструктуры.

На рисунке 6 представлены возможные области применения гибридного криптографического модуля Saber в IoT- и робототехнических системах. Предложенная архитектура продемонстрировала стабильное соотношение между скоростью, безопасностью и затратами логических ресурсов FPGA.

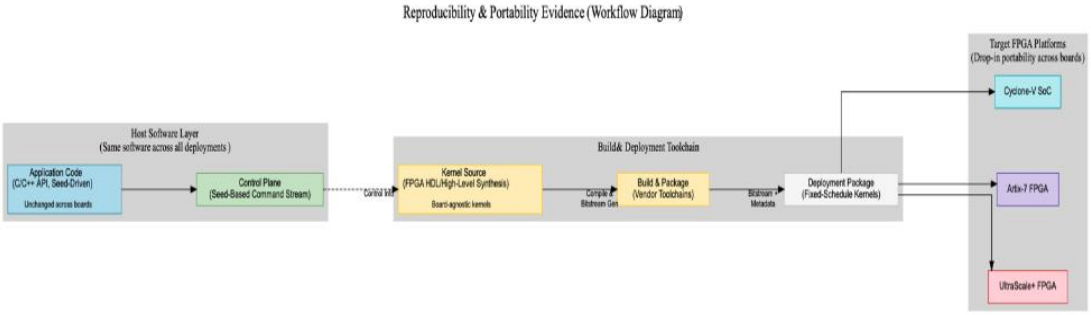

Рисунок 6 – Возможные области применения гибридного криптомодуля Saber в IoT-и робототехнических системах

В дальнейшем планируется интеграция усовершенствованных контрмер против атак по сторонним каналам (включая маскирование) и исследование масштабируемости гибридного модуля на многоядерных FPGA-платформах

Представленные результаты демонстрируют, что разработанная гибридная архитектура Saber является перспективным решением для аппаратно-программных систем защиты информации. Реализация на платформе CPU-FPGA обеспечивает не только повышение производительности, но и значительное улучшение энергетической эффективности и устойчивости к утечкам данных.

Предложенный подход открывает возможности дальнейшей интеграции постквантовых алгоритмов в интеллектуальные устройства и распределённые киберфизические системы, требующие высокой степени защищённости и минимальных временных задержек.

В целом, проведённое исследование подтверждает, что гибридные криптографические модули на базе Saber могут стать ключевым элементом при построении доверенной инфраструктуры для интернета вещей, мобильных робототехнических комплексов и автономных телеметрических узлов.

Список литературы

1. Jan-Pieter D’Anvers A. Vercauteren. Saber: Module-LWR Based Key Exchange / Jan-Pieter D’Anvers A., Karmakar S., Sinha Roy F. // CPA-Secure Encryption and CCA-Secure KEM. Springer, 2018.

2. Sinha Roy S. High-Speed Coprocessor for Lattice-Based Key Encapsulation Mechanism: Saber in Hardware / S. Sinha Roy, A. Basso // TCHES, 2020.

3. High-Performance Hardware Implementation of the Saber Key Encapsulation Protocol / D. Li et al // Electronics, 2024.

4. Dang V.B. High-Speed Hardware Architectures and FPGA Benchmarking of Kyber, NTRU, and Saber / V.B. Dang, K. Mohajerani, K. Gaj. // IEEE Trans. Computers, 2022.

5. Compact Co-Processor for Accelerating Module Lattice-Based KEM / J.M.B. Mera et al // IEEE, 2020.

6. Enhancing Cryptographic Protection and Authentication in Cellular Networks / M. Bakyt et al // IJECE, 2024.

7. Energy-Efficient Configurable Crypto-Processor for Module-LWR / Y. Zhu et al // IEEE Trans. Circuits and Systems I, 2021.
8. Abdulgadir A. First-Order Masked Implementation of Saber on FPGA / A. Abdulgadir, S. Sinha Roy, F. Vercauteren. // CHES, 2021.
9. Aikata C.M. Unified Saber and Dilithium Coprocessor for Post-Quantum Cryptography / C.M. Aikata, F. Turan, M. Knežević. // IEEE Access, 2022.
10. Dang V.B. FPGA Benchmarking of Lattice-Based KEMs: Kyber, Saber, and NTRU Prime / V.B. Dang, K. Gaj. // IEEE Trans. Computers, 2023.
11. D'Anvers J.-P. Specification of the Saber Algorithm / J.-P. D'Anvers, R. Vercauteren. // NIST PQC Round 3 Submission, 2020.

Благодарность

Авторы выражают благодарность Министерству высшего образования и науки Республики Казахстан, выделившему грантовый проект на 2023-2025 годы. ИРН AP19677508.

А.К. Майданов[1]*, Х. Джанболат[2], С.К. Атанов[1]
[1]Л.Н. Гумилев атындағы Еуразия ұлттық университеті,
010000, Қазақстан Республикасы, Астана қ., Сәтпаев көш., 2
[2]Анкара Йылдырым Беязыт университеті,
Түркия, Анкара
*e-mail: makeadil@mail.ru

CPU–FPGA ПЛАТФОРМАСЫНДА SABER ПОСТКВАНТТЫҚ АЛГОРИТМІНІҢ ГИБРИДТІК ТҮРДЕ ЖҮЗЕГЕ АСЫРЫЛУЫ

Мақалада Saber посткванттық криптографиялық алгоритмінің CPU-FPGA ендірілген платформасында гибридтік аппараттық-бағдарламалық жүзеге асырылуын әзірлеу және оңтайландыру мәселесі қарастырылады. Зерттеудің басты мақсаты – шектеулі есептеу ресурстары жағдайында постквантты кілт алмасу сұлбаларының өнімділігін, энергия тиімділігін және қауіпсіздігін арттыру, сондай-ақ жанама арналар арқылы шабуылдарға төзімділікті қамтамасыз ету.

Ұсынылған архитектура ARM процессорының және FPGA ядросының есептеу мүмкіндіктерін біріктіріп, жүктемені процессор мен аппараттық жеделдеткіш арасында тиімді бөледі. Аппараттық бөлікте көпмүшелі көбейту мен SHA-3 хэштеу операциялары конвейерлік түрде іске асырылған, ал бағдарламалық бөлік деректер ағындарын басқару, есептеулерді синхрондау және тұтастықты бақылауға жауап береді. CPU мен FPGA арасында тұрақты кідіріс уақыты бар интерфейс қолданылып, операциялардың орындалу уақытының тұрақтылығын және уақыттық шабуылдарға төзімділігін қамтамасыз етеді.

Алгоритмнің бағдарламалық, аппараттық және гибридтік үш нұсқасы салыстырылып, 35–50 % жылдамдық артуы тіркелді. TVLA әдісімен жүргізілген ағып кетуге тұрақтылық талдауы энергия профилі мен құпия деректер арасындағы байланыс жоқ екенін растады. Ұсынылған шешімдер мобильді роботтар, теңіздегі ұшқышсыз платформалар, өндірістік телеметриялық желілер және IoT жүйелерінің байланыс арналарының жоғары деңгейлі қауіпсіздігін қамтамасыз етуге қолданыла алады.

Түйін сөздер: *постквантты криптография, Saber, FPGA, гибридтік архитектура, аппараттық-бағдарламалық жүзеге асыру.*

A. Maidanov[1]*, H.Canbolat[2], S.Atanov[1]
[1]L.N. Gumilyov Eurasian National University,
010000, Satpayev St. 2, Astana, Republic of Kazakhstan
[2]Ankara Yıldırım Beyazıt University,
Turkey, Ankara
*e-mail: makeadil@mail.ru

POST-QUANTUM CRYPTOGRAPHY SABER IN A HYBRID CPU–FPGA ARCHITECTURE

The paper presents the development and optimization of a hybrid hardware-software implementation of the post-quantum cryptographic algorithm Saber on an embedded CPU-FPGA platform. The main objective of the research is to enhance the performance, energy efficiency, and security of post-quantum key exchange schemes under limited computational resources while maintaining resistance to side-channel attacks.

The proposed architecture integrates the computational capabilities of the ARM processor and the FPGA core, enabling efficient distribution of workloads between the processor and the hardware accelerator. The hardware part implements pipelined polynomial multiplication and SHA-3 hashing, while the software component manages data flow, synchronization, and integrity control. A fixed-latency communication interface between the CPU and FPGA ensures constant-time execution and stability against timing variations.

Three implementations of the algorithm were compared: software, hardware, and hybrid. Experimental results demonstrated a 35-50% reduction in execution time without compromising cryptographic strength or increasing power consumption. A TVLA (Test Vector Leakage Assessment) analysis confirmed the absence of any statistical correlation between the energy profile and secret data, validating the system's side-channel resistance.

The proposed solution can be effectively applied to mobile robotic platforms, unmanned marine vehicles, industrial telemetry networks, and IoT systems requiring high-performance and quantum-resistant data protection.

Key words: *post-quantum cryptography, Saber, FPGA, hybrid architecture, hardware–software implementation.*

Сведения об авторах

Адиль Кокенович Майданов* – магистр, кафедра компьютерной и программной инженерии, Евразийский национальный университет имени Л.Н. Гумилёва, Астана, Казахстан; e-mail: makeadil@mail.ru. ORCID: https://orcid.org/0000-0003-2392-5164.

Хусейн Джанболат – доктор PhD, профессор, кафедра электротехники и электроники, Университет Анкара Йылдырым Беязыт, Анкара, Турция; e-mail: huseyin.canbolat@gmail.com. ORCID: https://orcid.org/0000-0002-2577-0517.

Сабыржан Кубейсинович Атанов – д.т.н., профессор кафедра компьютерной и программной инженерии, Евразийский национальный университет имени Л.Н. Гумилёва, Астана, Казахстан; e-mail: atanov5@mail.ru. ORCID: https://orcid.org/0000-0003-2115-7130.

Information about the authors

Adil Maidanov* – Master, Department of Computer and Software Engineering, L. N. Gumilyov Eurasian National University, Astana, Kazakhstan; e-mail: makeadil@mail.ru. ORCID: https://orcid.org/0000-0003-2392-5164.

Hüseyin Canbolat – Doctor of PhD, Professor, Department of Electrical and Electronics Engineering, Ankara Yıldırım Beyazıt University, Ankara, Turkey; e-mail: huseyin.canbolat@gmail.com. ORCID: https://orcid.org/0000-0002-2577-0517.

Sabyrzhan Atanov – Doctor of Tech. Sc., Professor, Department of Computer and Software Engineering, L. N. Gumilyov Eurasian National University, Astana, Kazakhstan; e-mail: atanov5@mail.ru. ORCID: https://orcid.org/0000-0003-2115-7130.

Авторлар туралы мәліметтер

Адиль Кокенович Майданов* – Л.Н. Гумилев атындағы Еуразия ұлттық университеті, компьютер және программалық инженерия кафедрасының оқытушысы, магистр, Астана, Қазақстан; e-mail: makeadil@mail.ru. ORCID: https://orcid.org/0000-0003-2392-5164.

Хусейн Джанболат – Анкара Йылдырым Беязыт университеті, Электр және электроника инженерия кафедрасының профессоры PhD, Анкара, Түркия; e-mail: huseyin.canbolat@gmail.com. ORCID: https://orcid.org/0000-0002-2577-0517.

Сабыржан Кубейсинович Атанов – Л.Н. Гумилев атындағы Еуразия ұлттық университеті, компьютер және программалық инженерия кафедрасының профессоры, т.ғ.д.; e-mail: atanov5@mail.ru. ORCID: https://orcid.org/0000-0003-2115-7130.

Поступила в редакцию 21.10.2025
Поступила после доработки 27.11.2025
Принята к публикации 28.11.2025