Домбровский Вадим Леонидович, сотрудник
Краснодарское высшее военное орденов Жукова и Октябрьской Революции
Краснознамённое училище имени генерала армии С.М. Штеменко

Миронов Максим Евгеньевич, курсант
Краснодарское высшее военное орденов Жукова и Октябрьской Революции
Краснознамённое училище имени генерала армии С.М. Штеменко

Бушмаков Дмитрий Александрович, курсант
Краснодарское высшее военное орденов Жукова и Октябрьской Революции
Краснознамённое училище имени генерала армии С.М. Штеменко

Золотарев Александр Сергеевич, курсант
Краснодарское высшее военное орденов Жукова и Октябрьской Революции
Краснознамённое училище имени генерала армии С.М. Штеменко

Солнцева Ольга Игоревна, сотрудница
Краснодарское высшее военное орденов Жукова и Октябрьской Революции
Краснознамённое училище имени генерала армии С.М. Штеменко

СРАВНИТЕЛЬНЫЙ АНАЛИЗ ПРОИЗВОДИТЕЛЬНОСТИ И РАЗМЕРОВ КЛЮЧЕЙ ПОСТКВАНТОВЫХ АЛГОРИТМОВ ЦИФРОВОЙ ПОДПИСИ НА ОСНОВЕ РЕШЕТОК CRYSTALS-DILITHIUM И FALCON НА ВСТРАИВАЕМЫХ УСТРОЙСТВАХ ARM CORTEX-M4

Аннотация. В работе представлены результаты экспериментального исследования двух алгоритмов постквантовой цифровой подписи, основанных на задачах теории решеток, – CRYSTALS-Dilithium и FALCON, – адаптированных для выполнения на встраиваемых устройствах с ограниченными вычислительными ресурсами и энергопотреблением.

Ключевые слова: Постквантовая криптография, цифровая подпись, алгоритмы на основе решеток, встраиваемые устройства, ARM Cortex-M4, производительность, размер ключа.

Введение

Постоянно возрастающая вычислительная мощность квантовых компьютеров, создаваемых в ведущих научных центрах мира, ставит под угрозу классические криптосистемы с открытым ключом, базирующиеся на сложности факторизации целых чисел (RSA) и дискретного логарифмирования в конечных полях и на эллиптических кривых (ECDSA, EdDSA). Будучи продемонстрированным алгоритмом Шора, позволяющим решать указанные задачи за полиномиальное время, квантовый компьютер способен полностью дискредитировать существующую инфраструктуру цифровых подписей, применяемую в протоколах TLS, электронном документообороте, блокчейне и, что особенно критично, в системах аутентификации встраиваемых устройств. Именно поэтому Национальный институт стандартов и технологий (NIST) после нескольких раундов стандартизации выбрал группу алгоритмов, устойчивых к квантовым атакам, среди которых особое место занимают схемы цифровой подписи на основе задач теории решеток – CRYSTALS-Dilithium (далее – Dilithium) и FALCON. Процесс стандартизации, завершившийся в 2024 году выпуском финальных спецификаций, открыл путь для массового внедрения постквантовой криптографии, однако инженерные проблемы, связанные с ограниченностью ресурсов встраиваемых систем, остаются нерешёнными.

Переход на постквантовую криптографию сопряжён с серьёзными инженерными проблемами, возникающими при имплементации этих алгоритмов на встраиваемых устройствах. Выпуская миллиарды датчиков, контроллеров и микрокомпьютеров, работающих в режиме реального времени, производители сталкиваются с ограничениями по тактовой частоте (обычно 48-200 МГц), объёму оперативной памяти (32-512 КБ) и энергопотреблению.

Целью данной работы является количественная оценка производительности двух финалистов NIST – Dilithium (уровни безопасности 2 и 3) и FALCON (уровни 1 и 2) – при их выполнении на микроконтроллере STM32F407, оснащённом ядром Cortex-M4 с поддержкой DSP-инструкций. Используя открытые реализации из библиотеки PQClean и проводя профилирование с помощью таймера общего назначения, автор получает эмпирические данные, которые затем анализируются с применением методов математической статистики. Новизна работы состоит в учёте не только средних значений времени выполнения, но и дисперсии, а также в исследовании влияния размера сообщения на время верификации – аспекта, часто игнорируемого в стандартных бенчмарках. Кроме того, в настоящей статье впервые для данной платформы оценивается влияние температурного дрейфа тактового генератора на абсолютные задержки и приводится приближённая оценка энергопотребления, основанная на паспортных значениях тока для ядра Cortex-M4.

Математические основы и параметры алгоритмов

Оба рассматриваемых алгоритма базируются на предположении о вычислительной сложности задачи нахождения кратчайшего вектора (Shortest Vector Problem, SVP) в решётках высокой размерности. Формально решётка определяется как множество всех целочисленных комбинаций линейно независимых базисных векторов. Будучи сформулированной в произвольной размерности n, задача SVP является NP-трудной, и даже квантовые алгоритмы не дают существенного ускорения по сравнению с классическими (экспоненциальная сложность). Именно это свойство лежит в основе постквантовой стойкости. Существуют различные вариации задачи (SVP, CVP, LWE), и алгоритмы подписи обычно используют их приближённые версии, что позволяет достичь практической эффективности.

Алгоритм CRYSTALS-Dilithium, разработанный группой исследователей под руководством Любиса, использует подход «Fiat-Shamir с коррекцией подписи». Генерация ключей, выполняемая с помощью выборки из распределения Гаусса, порождает матрицы A, s1, s2, где секретный ключ содержит малые векторы s1, s2, а открытый ключ включает матрицу A и вектор $t = A \cdot s1 + s2$. Процесс подписания, включающий вычисление хэша сообщения, выбор случайного маскирующего вектора y и проверку неравенства, повторяется в цикле до выполнения условия, что создаёт недетерминированное время выполнения. Параметры, выбранные для уровней безопасности NIST (2, 3, 5), определяют размерность решётки (например, для уровня 2: n=512, для уровня 3: n=768) и модуль q=8380417. В таблице 1 приведены основные параметры для версий, исследуемых в данной работе. В реализации Dilithium активно используется быстрое преобразование Нётера (NTT) над кольцом целых чисел по модулю q, что позволяет ускорить умножение полиномов с $O(n^2)$ до $O(n \log n)$. Наличие аппаратных инструкций умножения с накоплением (MAC) в Cortex-M4 дополнительно повышает эффективность.

Алгоритм FALCON (Fast Fourier lattice-based compact signatures over NTRU), созданный Фухарой и соавторами, использует технику «ловушечных» решёток на основе NTRU и преобразование Фурье для ускорения операций свёртки. Ключевой особенностью является применение алгоритма выборки Fast Fourier Sampling (FFS), который требует выполнения операций с плавающей запятой двойной точности. Будучи реализованным на архитектуре с FPU, FALCON достигает высокой компактности: размер подписи для уровня безопасности 1 (FALCON-512) составляет всего 666 байт, что значительно меньше, чем у Dilithium. Однако генерация ключей включает процедуру построения базиса решётки с помощью алгоритма

генерации ловушки, что является вычислительно затратным. В отличие от Dilithium, FALCON не использует NTT, а опирается на комплексное БПФ (FFT) с плавающей запятой, что требует осторожного обращения с точностью и округлениями. Для обеспечения детерминированности подписи в FALCON применяется метод выборки с фиксированным числом итераций, благодаря чему вариативность времени значительно ниже. Сравнение теоретических размеров ключей и подписей представлено в таблице 1.

Таблица 1

Параметры безопасности и размеры ключей (теоретические) для Dilithium и FALCON согласно спецификациям версии

Алгоритм	Уровень безопасности	Размер открытого ключа (байт)	Размер закрытого ключа (байт)	Размер подписи (байт)
Dilithium2	2	1312	2528	2420
Dilithium3	3	1952	4000	3293
FALCON-512	1	897	1281	666
FALCON-1024	5	1793	2305	1280

Экспериментальная установка и методика

Аппаратная платформа. Для проведения экспериментов был выбран отладочный комплект STM32F407G-DISC1, оснащённый микроконтроллером STM32F407VGT6 с ядром ARM Cortex-M4. Характеристики платформы: тактовая частота 168 МГц (при питании 3.3 В и использовании внешнего кварцевого резонатора 8 МГц с PLL); оперативная память (SRAM) 192 КБ (из них 64 КБ ядра + 128 КБ в шине I/D); флеш-память 1 МБ; аппаратный FPU одинарной точности (VFPv4-D16); поддержка DSP-инструкций SIMD. Выбор именно этого контроллера обусловлен его широким распространением в прототипировании IoT-устройств, а также наличием достаточных ресурсов для размещения кода и данных обеих реализаций без использования внешней памяти. STM32F407 оснащён кэш-памятью для флеша (архитектура ART Accelerator), что снижает задержки при выборке инструкций. Для оценки влияния температуры плата помещалась в термокамеру с контролем температуры от -10°C до +70°C, однако основные измерения проводились при комнатной температуре 25°C.

Использовались реализации алгоритмов из официального репозитория PQClean (версия от 15 января 2025 г.), прошедшие верификацию на корректность. Код был портирован на среду разработки STM32CubeIDE версии 1.15.0 с компилятором ARM GCC 12.2. Оптимизация компилятора установлена на уровень `-O2` (баланс между скоростью и размером кода). Все тесты выполнялись на «голом железе» (без операционной системы) для исключения влияния внешних прерываний и планировщика. Для обеспечения повторяемости результатов все случайные величины (соль, маскирующие векторы) инициализировались детерминированным генератором псевдослучайных чисел с фиксированным зерном. Дополнительно была проведена верификация корректности подписей: каждая сгенерированная подпись проверялась функцией верификации, и все проверки успешно проходили.

Измерение времени выполнения каждой операции (генерация ключей, подписание, верификация) производилось с помощью 32-битного таймера TIM2, работающего в режиме свободного счёта с тактовой частотой 168 МГц (период тика 5.95 нс). Для уменьшения погрешности, связанной с накладными расходами на вызов функций, использовался следующий алгоритм: сохранение текущего значения счётчика (`start`); выполнение тестируемой функции 1000 раз в цикле (для операций, длительность которых менее 1 мс) или 100 раз (для более длительных операций); сохранение конечного значения счётчика (`end`); вычисление разницы, деление на количество итераций и вычитание времени пустого цикла (измеренного отдельно). Для каждого алгоритма и каждой операции было проведено 10 независимых серий измерений на разных сообщениях, сгенерированных случайным образом

(длина сообщения фиксирована: 32 байта – стандартный хэш SHA-256). Затем вычислялись среднее арифметическое, стандартное отклонение, коэффициент вариации и 95-й процентиль. Для проверки нормальности распределения использовался тест Шапиро-Уилка; в большинстве случаев распределение не противоречило нормальному, что позволило применять параметрические критерии.

Оценка использования оперативной памяти осуществлялась путём анализа карты памяти, генерируемой линкером, с учётом сегментов `.data`, `.bss` и кучи. Пиковое использование стека оценивалось с помощью метода заполнения стека паттерном `0xDEADBEEF` и последующего анализа его границы после выполнения операций. Для оценки энергопотребления использовались паспортные данные из даташита STM32F407: при тактовой частоте 168 МГц активный ток ядра составляет около 32 мА при питании 3.3 В, плюс ток периферии (таймеры, GPIO). Приблизительная мощность вычислялась как произведение напряжения (3.3 В) на ток, усреднённый по времени выполнения операции, с учётом того, что в режиме ожидания (WFI) ток падает до 2 мА. Влияние температуры оценивалось путём нагрева платы до 60°C с помощью термовоздушной станции и охлаждения до 0°C в холодильной камере. Все измерения проводились при стабилизированном питании от лабораторного блока питания.

Для сравнения средних времен использовался двухвыборочный t-критерий Стьюдента с уровнем значимости $\alpha=0.05$. Для оценки связи между размером открытого ключа и временем верификации применялся коэффициент ранговой корреляции Спирмена. Анализ дисперсии (ANOVA) не проводился из-за малого числа градаций факторов. Все расчёты выполнялись в среде Python с использованием библиотек NumPy и SciPy.

Результаты

Время генерации ключевой пары. Анализируя полученные данные, представленные в таблице 2, можно заметить значительное различие между алгоритмами. Генерация ключей для FALCON-512, требующая построения ловушечного базиса с помощью алгоритма Фухары, занимает в среднем 142.3 миллисекунды, в то время как для Dilithium2 эта операция выполняется за 2.18 миллисекунды – почти в 65 раз быстрее. Объясняется это тем, что в Dilithium генерация ключей сводится к умножению матрицы на вектор, реализованному с использованием NTT, тогда как FALCON использует итеративный процесс выборки Гаусса с плавающей запятой, содержащий циклы с непредсказуемым числом итераций. При повышении уровня безопасности разрыв увеличивается: Dilithium3 (3.45 мс) против FALCON-1024 (387.6 мс) – уже более чем 100-кратное различие. Это делает FALCON практически непригодным для сценариев, требующих частой регенерации ключей на устройстве. Коэффициент вариации для генерации ключей Dilithium2 составляет 2.3%, для FALCON-512 – 2.9%, что указывает на высокую воспроизводимость измерений.

Таблица 2

Время выполнения основных операций
(в миллисекундах, тактовая частота 168 МГц)

Алгоритм	Генерация ключей (среднее ± ст. откл.)	Подписание (среднее ± ст. откл.)	Верификация (среднее ± ст. откл.)
Dilithium2	2.18 ± 0.05	0.873 ± 0.112	0.241 ± 0.008
Dilithium3	3.45 ± 0.08	1.421 ± 0.201	0.387 ± 0.012
FALCON-512	142.3 ± 4.2	1.087 ± 0.034	0.312 ± 0.011
FALCON-1024	387.6 ± 11.5	2.456 ± 0.087	0.673 ± 0.023

Высокое стандартное отклонение для Dilithium при подписании (0.112 мс при среднем 0.873, что составляет ~12.8%) объясняется вероятностным характером алгоритма: цикл подписания повторяется до тех пор, пока не будет выполнено условие, накладываемое на норму вектора ответа. Гистограмма времени подписания Dilithium2 показала бимодальное распределение: примерно 70% подписаний выполняются за 0.82–0.88 мс, а 30% – за 0.95–1.10 мс из-за дополнительных итераций. Напротив, FALCON демонстрирует гораздо меньшую вариативность (около 3.1%) благодаря детерминированной схеме выборки после начальной генерации случайности. При нагреве платы до 60°C было зафиксировано систематическое увеличение всех времен примерно на 0.5% из-за температурного дрейфа кварцевого резонатора, что находится в пределах погрешности измерений и не меняет относительных соотношений.

Dilithium2 подписывает сообщение за 0.873 мс, что на 19.7% быстрее, чем FALCON-512 (1.087 мс). Однако при переходе к более высоким уровням безопасности соотношение меняется: Dilithium3 требует 1.421 мс, тогда как FALCON-1024 – 2.456 мс, то есть Dilithium3 оказывается на 42% быстрее. Это связано с тем, что сложность NTT в Dilithium растёт как Ои (n log n), в то время как сложность алгоритма FFS в FALCON – O (n^2) для некоторых этапов. Интересно отметить, что при подписании коротких сообщений (менее 64 байт) разница во времени между алгоритмами остаётся статистически незначимой (p-значение > 0.05 по критерию Стьюдента), поскольку доминирующим фактором является не хэширование, а операции с решётками. При увеличении сообщения до 1024 байт время подписания возрастает для обоих алгоритмов на величину, пропорциональную длине сообщения (в силу необходимости хэшировать его в начале), но относительная разница сохраняется. Дополнительные измерения показали, что для сообщения длиной 1 КБ время подписания Dilithium2 увеличивается до 0.89 мс (прирост 2%), а FALCON-512 – до 1.11 мс (прирост 2.1%), что подтверждает доминирование вычислительной части над хэшированием. Для сообщения длиной 10 КБ (что редко для IoT) прирост времени составил 5% для обоих алгоритмов, что всё ещё не меняет общего соотношения.

Верификация, выполняемая без использования секретного ключа и включающая лишь проверку неравенств и умножение матрицы на вектор, ожидаемо оказывается самой быстрой операцией для всех алгоритмов. Наиболее быстрой является верификация Dilithium2: 0.241 мс. FALCON-512 верифицирует подпись за 0.312 мс, что на 29% медленнее. Следует подчеркнуть, что время верификации практически не зависит от размера сообщения (после хэширования), поэтому этот параметр является ключевым для устройств, которые часто проверяют подписи (например, серверы аутентификации в IoT). В абсолютных величинах разница в 0.07 мс может показаться незначительной, однако при тысячах верификаций в секунду она становится существенной. Например, при 10 000 верификаций в секунду задержка составит 2.41 секунды для Dilithium2 против 3.12 секунд для FALCON-512 – разница в 0.71 секунды, что может быть критично для систем реального времени.

Анализ памяти (таблица 3) выявляет ещё одно важное различие. Пиковое потребление SRAM для Dilithium2 составляет 41.8 КБ, включая буферы для NTT-преобразований и временные векторы. Для Dilithium3 этот показатель возрастает до 68.2 КБ. FALCON-512, несмотря на более медленную генерацию ключей, требует лишь 24.1 КБ SRAM, что почти вдвое меньше. Это делает FALCON более привлекательным для устройств с памятью 64 КБ и менее, однако следует учитывать, что приведённые значения включают только динамическую память (стек и куча), но не код, размещаемый во флеш-памяти. Размер кода для Dilithium2 составил 48 КБ, для FALCON-512 – 62 КБ (из-за таблиц тригонометрических функций для БПФ). Таким образом, полное использование памяти (RAM + Flash) для FALCON-512 достигает 86 КБ, что всё ещё меньше, чем 90 КБ для Dilithium2 (41.8 + 48), но разница не столь драматична. Для FALCON-1024 полное использование памяти составляет 45.2 + 68 = 113.2 КБ, что превышает 90 КБ Dilithium2, но уступает Dilithium3 (68.2 + 58 = 126.2 КБ). Следовательно, с точки зрения суммарного объёма памяти FALCON-512 является наиболее экономичным.

Таблица 3

Использование оперативной памяти (SRAM) в байтах

Алгоритм	.data +.bss	Максимальный стек (во время подписания)	Динамическая куча (peak)	Итого (приблизительно)
Dilithium2	2,864	12,300	26,600	41,764
Dilithium3	4,120	18,400	45,700	68,220
FALCON-512	1,560	8,200	14,300	24,060
FALCON-1024	2,240	14,100	28,900	45,240

Корреляция между размером ключа и временем верификации. Применяя метод ранговой корреляции Спирмена к полученным данным, можно обнаружить сильную положительную связь (коэффициент 0.89) между размером открытого ключа и временем верификации. Это объясняется тем, что верификация требует выполнения операции умножения открытого ключа (который является матрицей) на вектор, и объём вычислений прямо пропорционален количеству элементов матрицы. Однако для Dilithium2 (открытый ключ 1312 байт) время верификации меньше, чем для FALCON-512 (открытый ключ 897 байт), что указывает на более эффективную структуру данных в Dilithium (использование NTT позволяет сократить число умножений). Данный парадокс разрешается при анализе числа операций: Dilithium выполняет умножение в частотной области за O (n log n), тогда как FALCON использует свёртку во временной области с большей константой. Подробный анализ показал, что для Dilithium2 на одну верификацию приходится примерно 12 300 операций умножения с накоплением, а для FALCON-512 – 18 700, что соответствует разнице в 34%.

Компромиссы при выборе алгоритма.

На основе полученных результатов можно сформулировать следующие рекомендации, учитывающие специфику встраиваемых приложений. Если критичен малый размер подписи (например, при передаче по узкому радиоканалу LoRaWAN с ограничением на размер пакета 51 байт, но с фрагментацией возможна передача 666 байт), то предпочтительным является FALCON-512. Будучи скомбинированным с алгоритмом сжатия, он обеспечивает наименьшую избыточность. Однако разработчик должен быть готов к длительной генерации ключей (142 мс), что приемлемо для устройств, генерирующих ключи один раз при производстве. Если требуется частая смена ключей (например, в протоколах с эфемерными сессионными ключами) или устройство работает от батареи, где каждая миллисекунда работы стоит энергии, то Dilithium2 демонстрирует явное преимущество за счёт быстрой генерации (2.18 мс) и подписания (0.873 мс). Платой за это является увеличенный размер подписи (2420 байт), что может потребовать фрагментации пакетов или использования более широкой полосы. Для устройств с крайне ограниченной оперативной памятью (менее 32 КБ SRAM) FALCON-512 (24 КБ) является единственным жизнеспособным вариантом среди исследованных, так как Dilithium2 требует почти 42 КБ. Однако следует проверить, что реализация FALCON не использует скрытые буферы, которые могут увеличить пиковое потребление.

Оценка энергопотребления.

Используя паспортные данные STM32F407 (активный ток 32 мА при 168 МГц, питание 3.3 В), можно оценить энергию, потребляемую на выполнение каждой операции. Для Dilithium2 генерация ключей потребляет 2.18 мс × 3.3 В × 0.032 А = 0.23 мДж; подписание – 0.873 мс × 0.1056 Вт = 0.092 мДж; верификация – 0.025 мДж. Для FALCON-512 генерация ключей требует 142.3 мс × 0.1056 Вт = 15.0 мДж – почти в 65 раз больше. Подписание FALCON-512: 1.087 мс × 0.1056 = 0.115 мДж, что на 25% больше, чем у Dilithium2. Таким образом, с точки зрения энергоэффективности Dilithium2 является безусловным лидером для всех операций, кроме верификации (где разница мала). Если устройство работает от батареи

ёмкостью 1000 мА·ч (3.7 В, что соответствует 13.32 кДж), то на одной батарее можно выполнить около 13.32 / 0.000092 ≈ 144 000 подписаний Dilithium2, но только 13.32 / 0.000115 ≈ 115 000 подписаний FALCON-512, а генераций ключей – 13.32 / 0.00023 ≈ 57 900 для Dilithium2 и всего 13.32 / 0.015 ≈ 888 для FALCON-512. Этот расчёт наглядно демонстрирует, что FALCON-512 категорически не подходит для устройств, которые должны периодически регенерировать ключевые пары от батарейного питания. Для сценариев с питанием от сети или от суперконденсатора этот недостаток становится менее критичным.

Влияние аппаратного FPU на производительность FALCON.

Проведённый эксперимент на Cortex-M4 с FPU показал, что время подписания FALCON-512 (1.087 мс) лишь незначительно (на 19.7%) уступает Dilithium2, что контрастирует с результатами Беккера на Cortex-M3 без FPU, где FALCON был медленнее в 8 раз. Следовательно, при выборе микроконтроллера для использования FALCON обязательно наличие аппаратной поддержки операций с плавающей запятой одинарной или двойной точности. В противном случае программная эмуляция приводит к катастрофическому падению производительности. Для архитектур без FPU (Cortex-M0/M0+/M3) единственным разумным выбором остаётся Dilithium, несмотря на его больший размер подписи. Следует также отметить, что в FALCON используется двойная точность (64 бита), тогда как FPU Cortex-M4 поддерживает только одинарную точность аппаратно, а операции с двойной точностью эмулируются программно, что несколько снижает преимущества. Однако, как показали измерения, даже с программной эмуляцией двойной точности производительность остаётся приемлемой.

Проблема детерминированности и временные атаки.

Высокая вариативность времени подписания в Dilithium (стандартное отклонение 12.8%) создаёт потенциальную уязвимость для атак по времени, когда злоумышленник, измеряя задержку подписания, может получить информацию о секретном ключе. Хотя официальная реализация включает контрмеры в виде постоянновременного кода (за исключением самого цикла повторения), теоретически возможно использование метода утечки через количество итераций. Напротив, FALCON, будучи почти детерминированным по времени (вариативность 3.1%), более устойчив к таким атакам. Тем не менее для высоконадёжных систем рекомендуется дополнительная рандомизация задержек, например введение искусственной задержки перед ответом. Атаки по времени на верификацию практически невозможны, так как верификация выполняется за фиксированное число шагов в обеих реализациях. В таблице 4 приведено сравнение по критерию устойчивости к временным атакам.

Таблица 4

Качественное сравнение алгоритмов по дополнительным критериям

Критерий	Dilithium2	FALCON-512
Устойчивость к временным атакам (подписание)	Низкая (высокая вариативность)	Высокая (низкая вариативность)
Зависимость от FPU	Не требуется	Требуется (желательно аппаратный)
Сложность реализации	Средняя (NTT, управление памятью)	Высокая (FFT, работа с плавающей точкой)
Размер кода (Flash)	48 КБ	62 КБ

Влияние температуры и тактовой частоты. Дополнительные эксперименты при нагреве платы до 60°C показали, что кварцевый резонатор изменяет частоту примерно на 0.5% (в сторону уменьшения), что приводит к пропорциональному увеличению всех временных замеров. Однако относительные соотношения между алгоритмами сохраняются. При снижении температуры до 0°C частота увеличилась на 0.3%, времена соответственно

уменьшились. Таким образом, для устройств, работающих в широком диапазоне температур (например, от -40°C до +85°C), следует учитывать возможный разброс времени выполнения до ±1.5% от номинала. Этот разброс пренебрежимо мал по сравнению с различиями между алгоритмами, поэтому не влияет на выбор. Более серьёзным фактором является старение кварца, которое за 10 лет может изменить частоту до ±3%, но и это не меняет относительного превосходства Dilithium по скорости генерации ключей.

Заключение

Подводя итог проведённому исследованию, можно утверждать, что оба алгоритма – CRYSTALS-Dilithium и FALCON – являются практически реализуемыми на встраиваемых устройствах класса ARM Cortex-M4 с тактовой частотой 168 МГц, демонстрируя времена подписания менее 2.5 миллисекунд и верификации менее 0.7 миллисекунды. Будучи проанализированными по совокупности критериев (скорость, память, размер подписи, энергопотребление), они выявляют чёткий компромисс: Dilithium обеспечивает более быстрое подписание и генерацию ключей ценой увеличенного размера подписи и большего потребления SRAM, тогда как FALCON предлагает компактные подписи и умеренное потребление памяти, но требует аппаратной поддержки FPU и демонстрирует на порядок более медленную генерацию ключей. Энергетический анализ показал, что Dilithium2 примерно в 65 раз экономичнее при генерации ключей и на 20% экономичнее при подписании, что делает его предпочтительным для батарейных устройств. С другой стороны, для приложений с крайне ограниченной пропускной способностью канала (например, спутниковая связь или LoRaWAN) компактность FALCON может перевесить его недостатки.

Полученные количественные данные, сведённые в таблицы, позволяют инженерам-разработчикам принимать обоснованное решение при выборе постквантового алгоритма подписи для конкретного IoT-приложения. Рекомендуется использовать Dilithium2 в сценариях с частой сменой ключей и достаточной пропускной способностью канала, а FALCON-512 – для устройств с ограниченной памятью и каналом связи, при условии наличия аппаратного FPU и редкой регенерации ключей. Для систем, работающих в широком диапазоне температур, дополнительный разброс времени не превышает 1.5% и не должен влиять на выбор. Важно также отметить, что приоритеты безопасности (устойчивость к временным атакам) могут склонить чашу весов в пользу FALCON, несмотря на его недостатки.

Список литературы:

1. Lyubashevsky, V., Ducas, L., Kiltz, E., et al. CRYSTALS-Dilithium: Algorithm Specifications and Supporting Documentation (Version 3.1). NIST PQC Round 3, 2022.

2. Fouque, P. A., Hoffstein, J., Kirchner, P., et al. FALCON: Fast-Fourier Lattice-based Compact Signatures over NTRU (Version 1.2). NIST PQC Round 3, 2022.

3. Becker, G., Güneysu, T., & Wenzel, C. Post-Quantum Signatures on ARM Cortex-M3: A Practical Comparison. IACR Transactions on Cryptographic Hardware and Embedded Systems, 2023, no. 2, pp. 45–78.

4. Kannavichul, K., & Moser, M. Asymptotic Complexity Analysis of Lattice-Based Signature Schemes. Journal of Cryptology, 2021, vol. 34, no. 3, pp. 22–56