ВЫЧИСЛЕНИЯ НАД ПОЛИНОМАМИ В ПОСТКВАНТОВЫХ СХЕМАХ ПОДПИСИ

Иваненко В. Г.[1], Иванова И. Д.[2], Иванова Н. Д.[3]

DOI: 10.21681/2311-3456-2024-4-65-70

Цель исследования: *ускорение операции проверки подписи в постквантовых криптографических системах путем применения к вычислениям над полиномами быстрых алгоритмов.*

Методы исследования: *сравнительный анализ принятых к стандартизации постквантовых алгоритмов, математическое моделирование операции проверки подписи, оптимизация путем синтеза быстрых алгоритмов.*

Результаты исследования: *на основании коммуникационных затрат, стойкости к атакам полным перебором, используемых парадигм и примитивов, и производительности на маломощных устройствах определены области применения схемы подписи Falcon, вследствие чего обоснована важность оптимизации данного алгоритма. Приведено математическое описание задачи, обосновывающей криптостойкость алгоритма Falcon, и определены ресурсоемкие операции над полиномами, применяемые в данной задаче. Рассмотрены алгоритмы, использующиеся для оптимизации операции проверки подписи в эталонной реализации схемы Falcon, и приведено обоснование их неэффективности при внедрении Falcon в маломощные устройства. Предложен метод оптимизации путем синтеза быстрых алгоритмов вычисления числового теоретического преобразования и быстрого алгоритма приведения целого числа по модулю. На основании данного метода разработана реализация оптимизационного алгоритма на языке Си.*

Практическая значимость: *предложенный метод оптимизации не использует архитектурные особенности среды, на которой тестируется данный алгоритм подписи, и не требует хранения дополнительных предвычисленных значений, благодаря чему может иметь широкое применение в различных областях. Разработанная реализация оптимизационного алгоритма на основе предложенного метода оптимизации может быть внедрена в эталонную реализацию схемы Falcon.*

Ключевые слова: *теория решеток, Falcon, оптимизация, NTT, мультипликативная группа, приведение по модулю, алгоритм Монтгомери.*

OPTIMIZATION OF COMPUTATIONS OVER POLYNOMIALS IN POST-QUANTUM SIGNATURE SCHEME

Ivanenko V. G.[4], Ivanova I. D.[5], Ivanova N. D.[6]

The purpose: *accelerating the signature verification in post-quantum cryptographic systems by applying fast algorithms to calculations over polynomials.*

Research methods: *comparative analysis of post-quantum algorithms accepted for standardization, mathematical modeling of the signature verification, optimization by synthesizing fast algorithms.*

Results: *the areas of application of the Falcon signature scheme are determined based on communication costs, resistance to brute-force attacks, the paradigms and primitives used, and performance on low-power devices, as a result the importance of optimization is justified. A mathematical description of the problem that substantiates the Falcon cryptographic strength is given, and resource-intensive operations used in this problem are determined. The algorithms used to optimize the signature verification in the Falcon reference implementation are considered, and the rationale for their ineffectiveness for Falcon in low-power devices is given. An optimization method by synthesizing fast algorithms for calculating the Number Theoretic Transform and a fast reduction algorithm is proposed. Based on this method, an implementation of the optimization algorithm in C language has been developed.*

1 Иваненко Виталий Григорьевич, доктор технических наук, профессор Института Интеллектуальных Кибернетических Систем (ИИКС) Национального исследовательского ядерного университета «МИФИ», г. Москва, Россия. E-mail: VGIvanenko@mephi.ru

2 Иванова Ирина Дмитриевна, магистрант кафедры «Криптология и кибербезопасность» Национального исследовательского ядерного университета «МИФИ», г. Москва, Россия. E-mail: iid.ivanova@yandex.ru, ORCID 0000-0003-3022-8973

3 Иванова Нина Дмитриевна, аспирант кафедры «Управление и защита информации» Российского университета транспорта (МИИТ), г. Москва, Россия. E-mail: IvanovaND.Nina@yandex.ru, ORCID 0000-0001-5942-8050

4 Vitaly G. Ivanenko, Dr.Sc., Associate Professor of the Institute of Intelligent Cybernetic Systems of the National Research Nuclear University «MEPhI», Moscow, Russia. E-mail: VGIvanenko@mephi.ru

5 Irina D. Ivanova, master's student of the Cryptology and Cybersecurity Department at NRNU MEPhI, Moscow, Russia. E-mail: iid.ivanova@yandex.ru, ORCID 0000-0003-3022-8973

6 Nina D. Ivanova, assistant of the Department of Management and Information Security, Russian University of Transport (MIIT), Moscow, Russia. E-mail: IvanovaND.Nina@yandex.ru, ORCID 0000-0001-5942-8050

Practical value: *the proposed optimization method does not use the architectural features of the environment and does not require storing additional precomputed values, due to which it can be widely used in various fields. The developed implementation of the optimization algorithm based on the proposed optimization method can be embedded in the Falcon reference implementation.*

Keywords: *lattice theory, Falcon, NTT, multiplicative group, reduction, Montgomery multiplication.*

Введение

В 1994 году был опубликован квантовый алгоритм Шора[7], в котором предлагается решение задач факторизации и дискретного логарифмирования за полиномиальное время. Это открытие ознаменовало, что в случае реализации алгоритма Шора на квантовом компьютере криптографические схемы, основанные на данных задачах, потеряют свою криптографическую стойкость [1, 2]. В частности использование алгоритма Шора злоумышленником может привести к резкой необходимости увеличения длин ключей в асимметричных схемах до критического уровня, не пригодного для их успешной эксплуатации в реальных информационных системах. Таким образом, изобретение достаточно мощного квантового компьютера повлечет за собой практически полное разрушение секретности и как следствие – глобальный финансовый кризис из-за разрушения банковской сферы и компрометации всех каналов связи [3].

С целью противодействия данной угрозе в 2016 году NIST был открыт прием заявок на участие в конкурсе по стандартизации постквантовых алгоритмов. В июне 2022 года по результатам третьего раунда конкурса к стандартизации были предложены три алгоритма цифровой подписи, среди которых две схемы – Falcon и CRYSTALS-Dilithium – используют криптографию на основе теории решеток.

Следует отметить, что хотя на настоящий момент еще не был создан квантовый компьютер, способный использовать алгоритм Шора, важно уже сейчас разрабатывать план интеграции стандартизованных постквантовых криптографических схем в существующие информационные системы. С этой целью в данной работе проводится сравнительный анализ финалистов NIST среди схем цифровых подписей, использующих криптографию на основе теории решеток, на примере алгоритма Falcon рассматриваются механизмы в устройстве постквантовых цифровых подписей, замедляющие выполнение ими операций создания и проверки подписей, и предлагается метод их оптимизации.

Сравнительный анализ финалистов конкурса NIST

Сравнение алгоритмов Falcon и CRYSTALS-Dilithium проводилось по трем аспектам:

- компромисс между коммуникационными затратами и криптостойкостью цифровой схемы;
- применяемые цифровой схемой криптографические примитивы и парадигмы;
- практическая применимость цифровой схемы.

Коммуникационные затраты криптографической схемы характеризуются длиной открытого ключа и подписи. Хотя с увеличением размеров ключей и подписей иногда удается повысить криптостойкость алгоритма, на практике важным является достижение компромисса между уровнем безопасности и коммуникационными затратами. В работе [4] предлагается оценивать стойкость постквантовых алгоритмов как объем затрат, требуемых квантовому злоумышленнику для проведения успешной атаки полным перебором ключей. Среди подписей-финалистов конкурса NIST у Falcon наименьшие размеры подписей, однако, как показывают эксперименты в работе [4], в сравнении с CRYSTALS-Dilithium данная схема также обладает большей стойкостью к атакам полным переборам.

Применяемые схемами криптографические примитивы и парадигмы не только обосновывают криптостойкость данных алгоритмов, но и являются причиной сложности их реализации [5]. В Falcon применяется парадигма «хеширование и подпись», в соответствии с которой для построения подписей применяется односторонняя функция с потайным входом, использующая нормальное распределение. В то же время схема подписи CRYSTALS-Dilithium применяет протокол Фиата-Шамира с прерываниями[8], использующий одностороннюю функцию на основе задачи нахождения короткого целочисленного решения. Проведение дополнительных раундов генерации подписи в данном алгоритме позволяет использовать равномерный закон распределения.

Хотя представленные на конкурсе NIST реализации цифровых подписей являются по большей части демонстрацией работы алгоритмов и не заявлены как эталонные, при оценке практической применимости Falcon и CRYSTALS-Dilithium можно также использовать их показатели производительности на маломощных устройствах [6].

7 Shor P. Algorithms for quantum computation: discrete logarithms and factoring. DOI:10.1109/SFCS.1994.365700

8 Lyubashevsky V. Fiat-Shamir with Aborts: Applications to Lattice and Factoring-Based Signatures. DOI:10.1007/978-3-642-10366-7_35

Результаты проведенного сравнительного анализа представлены в табл. 1.

Таблица 1.

Сравнительный анализ схем подписи Falcon и CRYSTALS-Dilithium

Параметры сравнения	Falcon	CRYSTALS-Dilithium
Коммуникационные затраты и криптостойкость схемы подписи		
Размеры подписей	На всех уровнях стойкости размеры подписей меньше, чем у CRYSTALS-Dilithium	На всех уровнях стойкости размеры подписей меньше, чем у Falcon
Соотношение коммуникационных затрат и криптографической стойкости	Близок к «идеальному» [4] криптографическому алгоритму (низкие коммуникационные затраты при высоком уровне стойкости)	Показатели уступают Falcon
Криптографические примитивы и парадигмы		
Применяемая для уменьшения размеров ключей и подписей парадигма	Хеширование и подпись (поддерживает восстановление сообщения по подписи)	Протокол Фиата-Шамира с прерываниями
Применяемое распределение вероятностей	Нормальное распределение (сложнее реализуется)	Равномерное распределение (проще реализуется)
Практическая применимость		
Время генерации ключей в реализации, представленной на конкурсе NIST	Требуется больше времени, чем Dilithium	Сравнительно быстро
Время выполнения подписи и проверки в реализации, представленной на конкурсе NIST	Требуется больше времени, чем Dilithium	Сравнительно быстро
Время выполнения подписи и проверки в реализации алгоритма для маломощных устройств [6]	Сравнительно быстро	Требуется больше времени, чем Falcon
Потребление памяти в реализации алгоритма для маломощных устройств [6]	Сравнительно небольшое потребление	Требуется больше ресурсов, чем Falcon

Сложность реализации схемы подписи Falcon обуславливает ее криптостойкость и компактность ее подписей. Данный алгоритм основывается на NTRU-подобных схемах, среди которых – схема шифрования NTRUEncrypt, которая была официально утверждена для использования в сфере финансов комитетом Accredited Standards Committee X9 [7]. Ввиду данных факторов важной является оптимизация данной схемы подписи с целью расширения сфер ее применения.

Операции над полиномами в постквантовых алгоритмах

Алгоритм Falcon основывается на задаче нахождения короткого целочисленного решения (Short Integer Solution, SIS). По условию данной задачи необходимо решить следующую систему уравнений:

$$\begin{cases} \|\vec{x}\| \le \beta \\ f_A(\vec{x}) := A\vec{x} = \vec{0} \in \mathbb{Z}_q^n, \end{cases} \quad (1)$$

где матрица $A = [a_1]...[a_m]$ состоит из случайных векторов из $\mathbb{Z}_q^n$, а $\vec{x}$ – ненулевой вектор из $\mathbb{Z}_q^m$.

В Falcon для создания подписей вместо $f_A(\vec{x})$ применяется односторонняя функция с потайным входом, основанная на NTRU-решетках [8]. При этом данная функция использует операцию умножения полинома на полином, которая технически требует значительных ресурсов при высоких степенях полиномов. В качестве механизма, упрощающего операцию умножения, может применяться числовое теоретическое преобразование (Number Theoretic Transform, NTT) [9]. Очевидно, что полином может быть записан как вектор, содержащий значения коэффициентов при степенях полинома. Потому NTT работает следующим образом:

1. Предполагается, что входной вектор является последовательностью из n неотрицательных целых чисел.
2. В мультипликативной группе $\mathbb{Z}_q$ определяется ω – примитивный корень единицы степени n.
3. Коэффициенты прямого преобразования $\tilde{a} = NTT(a)$ тогда определяются аналогично дискретному преобразованию Фурье как:

$$\tilde{a}_i = \sum_{j=0}^{n-1} a_j \omega^{ij} \bmod q, \quad (2)$$

где a_k – k-ый коэффицент исходного вектора a, $\tilde{a}$ – результирующий вектор, а индекс i проходит по всем координатам вектора $\tilde{a}$ от 0 до $n-1$.

4. Коэффициенты прямого преобразования $a = NTT(\tilde{a})$ определяются как:

$$a_i = \frac{1}{n} \sum_{j=0}^{n-1} \tilde{a}_j \omega^{-ij} \bmod q, \quad (3)$$

где $\tilde{a}$ – вектор, являющийся результатом применения NTT, а – исходный вектор, индекс i проходит по всем координатам вектора a от 0 до $n-1$.

Преобразование NTT, применяемое для круговой свертки векторов, может быть использовано для умножения полиномов в кольце $\mathbb{Z}_q[x]/(x^n-1)$. Если вектор c является круговой сверткой векторов a и $b \in \mathbb{Z}_q[x]/(x^n-1)$, для преобразования NTT выполняется свойство:

$$NTT(c) = NTT(a) \circ NTT(b), \quad (4)$$

где $\circ$ – покомпонентное умножение векторов.

Тогда для вычисления c необходимо применить n-мерные NTT и INTT в соответствии с упомянутым свойством:

$$c = INTT\,(NTT(a) \circ NTT(b)), \quad (5)$$

где $a, b, c \in \mathbb{Z}_q[x]/(x^n-1)$.

Для умножения полиномов в кольцах $\mathbb{Z}_q[x]$ и $\mathbb{Z}_q[x]/(x^n+1)$ используются модификации NTT, основанные на линейных и отрицательно завернутых (negative wrapped) свертках соответственно. В схеме подписи Falcon операции проводятся в кольце $\mathbb{Z}_q[x]/(x^n+1)$, из-за чего применяется следующий алгоритм NTT, основанный на отрицательно завернутых свертках (будем обозначать как NTT^{ψ}):

В мультипликативной группе $\mathbb{Z}_q$ помимо примитивного корня единицы степени n также вводится ψ – примитивный корень единицы степени $2n$ (порядок q должен удовлетворять $q \equiv 1 \bmod 2n$).

Для вектора a:

$$a = (a[0],\ldots,a[n-1]),\ b = (b[0],\ldots,b[n-1]), \quad (6)$$

где $\forall i \in [0,n-1]\ a[i] \in \mathbb{Z}_q$ вводится вектор $\hat{a}$:

$$\hat{a} = (a[0], \psi a[1],\ldots,\psi^{n-1} a[n-1]), \quad (7)$$

где ψ – примитивный корень единицы степени $2n$.

Коэффициенты прямого NTT^{ψ} и обратного $INTT^{\psi}$ преобразований NTT определяются следующим образом:

$$\tilde{a}_i = \sum_{j=0}^{n-1} a_j\, \psi^j\, \omega^{ij} \bmod q,$$

$$a_i = \frac{1}{n}\, \psi^{-j} \sum_{j=0}^{n-1} \tilde{a}_j\, \omega^{-ij} \bmod q,$$

где индекс i проходит по всем координатам вектора $\tilde{a}$ от 0 до $n-1$.

Для NTT^{ψ} аналогично справедливо свойство (4), потому отрицательно завернутую свертку векторов a и $b \in \mathbb{Z}_q[x]/(x^n-1)$ можно вычислить как:

$$c = INTT^{\psi}\,(NTT^{\psi}\,(a) \circ NTT^{\psi}\,(b)). \quad (8)$$

Сложность прямого вычисления циклической (отрицательно завернутой) свертки при помощи NTT (NTT^{ψ}) составляет $O(n^2)$: два преобразования NTT (NTT^{ψ}), одно покомпонентное умножение и одно преобразование INTT ($INTT^{\psi}$). Однако, как и в случае с дискретным преобразованием Фурье, возможно также применение быстрых алгоритмов.

Двумя такими алгоритмами являются алгоритм Кули-Тьюки и Джентльмена-Санде. Общая идея алгоритма Кули-Тьюки заключается в том, что из-за симметрии и периодичности корней из единицы коэффициенты $\tilde{a} = NTT(a)$ могут быть вычислены по формулам:

$$\tilde{a}_i = \tilde{a}_i' + \tilde{a}_i''\, \omega^i \bmod q, \quad (9)$$

$$\tilde{a}_{i+\frac{n}{2}} = \tilde{a}_i' - \tilde{a}_i''\, \omega^i \bmod q, \quad (10)$$

где $\tilde{a}_i = \sum_{j=0}^{\frac{n}{2}-1} a_{2j}\,(\omega^2)^{ij}$ и $\tilde{a}_i'' = \sum_{j=0}^{\frac{n}{2}-1} a_{2j+1}(\omega^2)^{ij}$, а $i = 0,1,\ldots, n/2-1$.

Идею симметричности и периодичности корней из единицы также использует алгоритм Джентльмена-Санде. Данные алгоритмы позволяют снизить сложность вычисления NTT до $O(n \log n)$. Однако хотя оба могут применяться для ускорения прямого и обратного преобразования NTT для циклических сверток, следует отметить, что в случае использования отрицательно завернутых сверток алгоритм Кули-Тьюки можно применить лишь к прямому преобразованию NTT^{ψ}, а алгоритм Джентльмена-Санде – только к обратному преобразованию $INTT^{\psi}$ [10].

Использование данных алгоритмов позволяет понизить сложность вычислений над полиномами, однако на практике существует еще одна проблема: операции по модулю могут быть достаточно затратными при больших значениях порядка q и требовать отдельных алгоритмов ускорения [11].

Оптимизация вычислений над полиномами с помощью алгоритма K-RED

В эталонной реализации Falcon[9], представленной на конкурсе NIST, для ускорения операций умножения по модулю в составе NTT используется алгоритм приведения Монтгомери. При умножении по алгоритму Монтгомери необходимо вычислить q' такое, что:

$$r * r^{-1} - q * q' = 1, \quad (11)$$

и перевести исходные числа a и $b \in \mathbb{Z}_q$ в «область Монтгомери»:

$$\bar{a} = a * r \bmod q, \quad (12)$$

$$\bar{b} = a * r \bmod q, \quad (13)$$

где $r \in \mathbb{Z}_q$ и $(r,q) = 1$.

Как видно из формул (9) и (10), в NTT^{ψ} ($INTT^{\psi}$) алгоритм Монтгомери может быть применен для вычисления $\tilde{a}_i''\psi^{2i+1}$ (аналог $\tilde{a}_i''\omega^i$ из (9) и (10) для отрицательно завернутых сверток) [12]. Поскольку q и ψ^{2i+1} для $i = 0,1,\ldots, n/2-1$ известны изначально и могут быть предварительно переведены в область Монтгомери, значения q' и $\bar{b}$ могут храниться отдельно и не вычисляться дополнительно в процессе проверки подписи. Однако на ограниченных устройствах, для которых

9 Falcon source files (reference implementation). URL: https://falcon-sign.info/impl/vrfy.c.html

Falcon является наилучшим кандидатом на внедрение ввиду малых коммуникационных затрат, это может стать критичным [13].

В Falcon порядок мультипликативный группы для бинарного случая (уровней стойкости 1-й и 5-й соответственно) равен $q = 12289 = 3 * 2^{12} + 1$, вследствие чего при $k = 3$ к NTT может быть применен алгоритм K-RED[10].

Алгоритм K-RED позволяет ускорить приведение целого числа по модулю вида $q = k * 2^m \pm l$, где k, l – малые положительные целые числа такие, что $k \geq 3$ и $l \geq 1$. В ходе алгоритма выполняются следующие шаги:

Число v представляется в виде:

$$v = v_0 + 2m * v_1, \quad (14)$$

где $0 \leq v_0 < 2^m$.

Алгоритм возвращает:

$$kv \equiv kv_0 - v_1 \ mod \ q, \quad (16)$$

Таким образом, в алгоритме приводится не само число v, а kv, поэтому при внедрении данного алгоритма в NTT$^{\psi}$ перед вычислением $\tilde{a}_i''\psi^{2i+1}$ необходимо вычислить:

$$\psi_k^{2i+1} = \psi^{2i+1} * k. \quad (17)$$

В эталонной реализации Falcon, представленной на конкурсе NIST, для вычисления NTT$^{\psi}$ применяется функция mq_NTT. Для ускорения выполнения преобразования используется предвычисленная таблица, обращение к которой происходит как к массиву Gmb и которая содержит степени ψ. Формула (17) может быть записана как:

$$s = mq\_div\_12289(Gmb[m+i], k)$$

При этом функция mq_div_12289 производит деление первого аргумента на второй по модулю q = 12289 (порядок $\mathbb{Z}_q$ для 1-го и 5-го уровней стойкости). В то же время реализация алгоритма K-RED, вызываемого вместо алгоритма Монтгомери mq_montymul для вычисления $\tilde{a}_i''\psi^{2i+1}$, может выглядеть следующим образом:

```
static inline uint32_t K_RED(uint32_t v)
{
    v_0 = v % pow2_m;
    v_1 = (v - v_0) / pow2_m;
    return k * v_0 - v_1;
}
```

В данном объявлении функции $pow2\_m$ и k – константы, хранящие значения 2^{12} и 3 соответственно. Поскольку деление осуществляется на степень 2, на практике это означает сдвиг или отсечение разрядов числа. Данные операции реализуются на вычислительных машинах очень быстро.

Алгоритм K-RED ускоряет вычисление обратного и прямого NTT на языке Си (на котором также была представлена реализация Falcon на NIST) до 2 раз в сравнении с алгоритмом Монтгомери. Кроме того, применение алгоритма K-RED также позволяет уменьшить в 2 раза количество умножений и приведений в процессе масштабирования коэффициентов INTT$^{-\psi}$, что может привести к значительному ускорению выполнения данного алгоритма в сравнении с другими оптимизациями Falcon [12, 14, 15].

С учетом того, что алгоритм Монтгомери требует выходящих за пределы NTT значительных расходов на хранение предвычисленных значений, в будущих исследованиях планируется на практике рассмотреть все преимущества использования алгоритма K-RED в составе Falcon.

Выводы

В результате настоящего исследования предложен метод оптимизации вычислений над полиномами в схеме Falcon. В ходе сравнительного анализа было определено, что для ограниченных и маломощных устройств лучшим кандидатом на внедрение является схема Falcon, вследствие чего была обоснована важность оптимизации данного постквантового алгоритма. По итогам анализа математического аппарата, реализующего вычисления над полиномами в рассматриваемой схеме подписи, было показано, что наиболее ресурсоемкой является операция приведения по модулю. Для ускорения вычислений над полиномами в Falcon в предлагаемом методе оптимизации используется синтез алгоритмов Кули-Тьюки и Джентельмена-Санде с быстрым алгоритмом приведения целого числа по модулю – алгоритмом K-RED.

На основании предложенного метода была написана реализация оптимизационного алгоритма на языке Си, которая может быть внедрена в эталонную реализацию Falcon. В дальнейших исследованиях планируется использовать ее для экспериментального подтверждения теоретических оценок, изложенных в данной работе, и сравнения эффективности предложенного метода оптимизации на разных платформах.

10 Longa P., Naehrig M. Speeding up the Number Theoretic Transform for Faster Ideal Lattice-Based Cryptography. DOI:10.1007/978-3-319-48965-0_8

Литература

1. *Vysotskaya V. V., Chizhov I. V. The security of the code-based signature scheme based on the Stern identification protocol // Прикладная дискретная математика. 2022. № 57. С. 67–90. DOI:10.17223/20710410/57/5*
2. *Asif R. Post-Quantum Cryptosystems for Internet-of-Things: A Survey on Lattice-Based Algorithms // IoT. 2021. Vol. 2. N. 1. P. 71–91. DOI:10.3390/IOT2010005*
3. *Комарова А. В., Коробейников А. Г. Анализ основных существующих пост-квантовых подходов и схем электронной подписи // Вопросы кибербезопасности. 2019. № 2 (30). С. 58–68. DOI: 10.21681/2311-3456-2019-2-58-68*
4. *Raavi M. et al. Security Comparisons and Performance Analyses of Post-Quantum Signature Algorithms // International Conference on Applied Cryptography and Network Security. 2021. Vol. 12727. 24 p. DOI:10.1007/978-3-030-78375-4_17*
5. *Singh S. XCRYPT: Accelerating Lattice Based Cryptography with Memristor Crossbar Arrays // IEEE Micro. 2023. Vol. 43. № 5. P. 45–54. DOI:10.1109/MM.2023.3248080*
6. *Gonzalez R. et al. Verifying Post-Quantum Signatures in 8 kB of RAM // Post-Quantum Cryptography: 12th International Workshop. 2021. P. 215–233. DOI:10.1007/978-3-030-81293-5_12*
7. *Cherckesova L. et al. Post-Quantum Cryptosystem NTRUEnCrypt and Its Advantage over Pre–Quantum Cryptosystem RSA // E3S Web of Conferences. 2020. Vol. 224. P. 01037. DOI:10.1051/e3sconf/202022401037*
8. *Espitau T. et al. Shorter Hash-and-Sign Lattice-Based Signatures // Annual International Cryptology Conference. 2022. P. 245–275. DOI:10.1007/978-3-031-15979-4_9*
9. *Liang Z. et al. Number Theoretic Transform: Generalization, Optimization, Concrete Analysis and Applications // International Conference on Information Security and Cryptology. 2020. P. 415–432. DOI:10.1007/978-3-030-71852-7_28*
10. *Abdulrahman A. et al. Multi-moduli NTTs for saber on Cortex-M3 and Cortex-M4 // Cryptology ePrint Archive. 2021. 33 p. DOI:10.46586/tches.v2022.i1.127-151*
11. *Mert A. C. et al. Design and Implementation of a Fast and Scalable NTT-Based Polynomial Multiplier Architecture // 2019 22nd Euromicro Conference on Digital System Design (DSD). 2019. P. 253–260. DOI:10.1109/DSD.2019.00045*
12. *Becker H. et al. Polynomial multiplication on embedded vector architectures // Cryptology ePrint Archive. 2021. 24 p. DOI:10.46586/tches.v2022.i1.482-505*
13. *Kim Y. et al. Accelerating Falcon on ARMv8 // IEEE Access. 2022. Vol. 10. 15 p. DOI: 10.1109/ACCESS.2022.3169784*
14. *Nguyen D. T., Gaj K. Fast Falcon Signature Generation and Verification Using ARMv8 NEON Instructions // International Conference on Cryptology in Africa. 2023. P. 417–441. DOI: 10.1007/978-3-031-37679-5_18*
15. *Seo E. Y. et al. Peregrine Toward Fastest FALCON Based on GPV Framework // Cryptology ePrint Archive. 2022. 21 p.*

References

1. *Vysotskaya V. V., Chizhov I. V. The security of the code-based signature scheme based on the Stern identification protocol // Prikladnaja diskretnaja matematika. 2022. № 57. S. 67–90. DOI:10.17223/20710410/57/5*
2. *Asif R. Post-Quantum Cryptosystems for Internet-of-Things: A Survey on Lattice-Based Algorithms // IoT. 2021. Vol. 2. N. 1. P. 71–91. DOI:10.3390/IOT2010005*
3. *Komarova A. V., Korobejnikov A. G. Analiz osnovnyh sushhestvujushhih post-kvantovyh podhodov i shem jelektronnoj podpisi // Voprosy kiberbezopasnosti. 2019. № 2 (30). S. 58–68. DOI: 10.21681/2311-3456-2019-2-58-68*
4. *Raavi M. et al. Security Comparisons and Performance Analyses of Post-Quantum Signature Algorithms // International Conference on Applied Cryptography and Network Security. 2021. Vol. 12727. 24 p. DOI:10.1007/978-3-030-78375-4_17*
5. *Singh S. XCRYPT: Accelerating Lattice Based Cryptography with Memristor Crossbar Arrays // IEEE Micro. 2023. Vol. 43. № 5. P. 45–54. DOI:10.1109/MM.2023.3248080*
6. *Gonzalez R. et al. Verifying Post-Quantum Signatures in 8 kB of RAM // Post-Quantum Cryptography: 12th International Workshop. 2021. P. 215–233. DOI:10.1007/978-3-030-81293-5_12*
7. *Cherckesova L. et al. Post-Quantum Cryptosystem NTRUEnCrypt and Its Advantage over Pre–Quantum Cryptosystem RSA // E3S Web of Conferences. 2020. Vol. 224. P. 01037. DOI:10.1051/e3sconf/202022401037*
8. *Espitau T. et al. Shorter Hash-and-Sign Lattice-Based Signatures // Annual International Cryptology Conference. 2022. P. 245–275. DOI:10.1007/978-3-031-15979-4_9*
9. *Liang Z. et al. Number Theoretic Transform: Generalization, Optimization, Concrete Analysis and Applications // International Conference on Information Security and Cryptology. 2020. P. 415–432. DOI:10.1007/978-3-030-71852-7_28*
10. *Abdulrahman A. et al. Multi-moduli NTTs for saber on Cortex-M3 and Cortex-M4 // Cryptology ePrint Archive. 2021. 33 p. DOI:10.46586/tches.v2022.i1.127-151*
11. *Mert A. C. et al. Design and Implementation of a Fast and Scalable NTT-Based Polynomial Multiplier Architecture // 2019 22nd Euromicro Conference on Digital System Design (DSD). 2019. P. 253–260. DOI:10.1109/DSD.2019.00045*
12. *Becker H. et al. Polynomial multiplication on embedded vector architectures // Cryptology ePrint Archive. 2021. 24 p. DOI:10.46586/tches.v2022.i1.482-505*
13. *Kim Y. et al. Accelerating Falcon on ARMv8 // IEEE Access. 2022. Vol. 10. 15 p. DOI: 10.1109/ACCESS.2022.3169784*
14. *Nguyen D. T., Gaj K. Fast Falcon Signature Generation and Verification Using ARMv8 NEON Instructions // International Conference on Cryptology in Africa. 2023. P. 417–441. DOI: 10.1007/978-3-031-37679-5_18*
15. *Seo E. Y. et al. Peregrine Toward Fastest FALCON Based on GPV Framework // Cryptology ePrint Archive. 2022. 21 p.*