УДК 004.056.55

Е.Ф. Кустов, С.В. Беззатеев

Пороговая схема подписи на основе теории решёток и интерполяции Ньютона

Представлена новая пороговая схема цифровой подписи, объединяющая криптографию на решётках с интерполяционными методами. Схема построена на задаче LWR (Learning With Rounding) и может быть использована для защиты IoT-устройств, где сочетание вычислительной эффективности и квантовой стойкости особенно востребовано. Предложенный подход использует интерполяцию Ньютона, демонстрирующую преимущества перед классической интерполяцией Лагранжа в плане производительности и гибкости при работе с динамическими группами участников.

Ключевые слова: пороговая подпись, теория решёток, интерполяция Ньютона, LWR, SIS, постквантовая криптография, разделение секрета.
DOI: 10.21293/1818-0442-2025-28-2-166-171

Быстрое развитие квантовых вычислений и повсеместное распространение IoT-устройств создают новые вызовы для современных криптографических систем. Традиционные алгоритмы цифровой подписи, такие как RSA и ECDSA, становятся уязвимыми перед квантовыми атаками, что требует разработки новых постквантовых решений [1]. В этом контексте особый интерес представляют криптосистемы на основе решёток, демонстрирующие устойчивость к квантовым атакам при сохранении высокой эффективности вычислений.

Анализ последних исследований показывает, что существующие квантово-стойкие решения не обеспечивают одновременно адаптивность, эффективность и компактность, необходимые для современных распределенных систем [2–6].

Основная научная проблема заключается в отсутствии пороговых схем, сочетающих квантовую стойкость с возможностью динамического изменения группы участников без полного пересчета параметров. Это особенно критично для IoT-сетей, где состав устройств постоянно меняется, а вычислительные ресурсы ограничены. Предлагаемая работа преодолевает эти ограничения за счет интеграции криптографии на решетках (основанной на LWR-проблеме) с оптимизированными методами интерполяции Ньютона.

Предлагаемая в данной работе пороговая схема цифровой подписи объединяет два перспективных направления исследований: криптографию на основе задачи Learning with Rounding (LWR) и методы полиномиальной интерполяции. Важным преимуществом LWR по сравнению с классическим Learning with Errors (LWE) является детерминированный характер вычислений, что особенно ценно для устройств с ограниченными мощностями [7].

Основное преимущество предложенного подхода заключается в его адаптивности: в отличие от традиционных схем, где изменение состава участников требует полного пересчета полинома, наша реализация на основе разделенных разностей Ньютона позволяет динамически обновлять параметры системы с линейной сложностью. Это особенно критично для IoT-сетей с их изменяющейся топологией и ограниченными ресурсами, где экономия каждого процента производительности напрямую влияет на срок службы устройств [8].

Схема пороговой подписи

В 1979 г. Шамир и Блейкли независимо предложили концепцию (t, N)-пороговой схемы [9, 10]. Основная идея таких схем заключается в том, что пользователи хранят доли секрета s, который может быть восстановлен только при наличии как минимум t из N долей, где N – общее количество участников, t – минимальный порог участников, необходимый для восстановления общего секрета s. Безопасная пороговая подпись должна удовлетворять критериям невозможности подделки и устойчивости.

Попытки подписать сообщение с меньшим числом участников не позволяют восстановить секрет, так как секрет s не может быть восстановлен. Это гарантируется строгими математическими свойствами пороговой схемы разделения секрета, построенной на интерполяции Ньютона.

Криптографическая стойкость схемы базируется на сложности решения задач M-LWR (Module Learning with Rounding) и M-SIS (Module Short Integer Solution), которые считаются устойчивыми к атакам как на классических, так и на квантовых компьютерах. Это делает схему перспективной в эпоху постквантовой криптографии.

В [11] доказана сложность задачи M-LWR и показано, что задача M-LWR так же сложна, как и LWR. В [12] описана редукция от задачи SIS к задаче SelfTargetSIS. Эта редукция демонстрирует, что задача SelfTargetSIS как минимум так же сложна, как и задача SIS, что делает её подходящей для доказательства безопасности криптографических схем. В [13] доказана сложность задачи SIS.

В нашей схеме используются два модуля: $q = 2^{\mu}$ и $p = 2^{\nu}$, где μ, ν – параметры безопасности. Все операции будут выполняться в полиномиальном кольце $\mathbf{Z}[x]/(x^n + 1)$ по модулю q или p, $q > p$, где n – размерность кольца.

Параметры k, l, где $l > k > 1$, определяют размерности ключей. Параметры α и γ задают интервалы для коэффициентов полиномов во время генерации ключей или подписания, а d и β обеспечивают корректность и безопасность схемы.

Для любого $x \in \mathbf{Q}$, где $\mathbf{Q}$ – множество рациональных чисел, обозначение $\mathrm{Round}(x) \in \mathbf{Z}$ означает округление до ближайшего целого числа, где 1/2 округляется вверх до 1. Функция $\mathrm{MSB}(x, d)$ извлекает d наиболее значимых бит числа x, а функция $\mathrm{LSB}(x, d)$ извлекает d наименее значимых бит числа x.

Для преобразования элемента $x \in \mathbf{Z}_q$ в $\mathbf{Z}_p$ используется следующее правило:

$$x = \mathrm{Round}\left(x \times \frac{p}{q}\right) = \mathrm{MSB}\left(x + \mathbf{h}, \mu\right),$$

где $\mathbf{h}$ – это вектор, каждая координата которого равна $h = 2^{\nu-\mu-1}$.

Наша схема является обобщением схемы Дамгарда [14] для построения пороговой подписи t из N и включает модификации, предложенные Любашевским [15]. В качестве базового алгоритма подписи используется схема «Крыжовник» [16] – постквантовая цифровая подпись на решетках, обеспечивающая высокую стойкость при сравнительно небольших размерах подписи.

Пусть $\mathrm{H}_1(x, y)$, $\mathrm{H}_2(x, y)$ – криптографические хеш-функции, моделируемые как случайные оракулы. Наша схема пороговой подписи представлена ниже.

Пусть имеется N пользователей и t из них могут подписать сообщение, что соответствует схеме разделения секрета (t, N). Каждый пользователь выбирает случайную матрицу $\mathbf{A}_i \in \mathrm{R}_q^{k \times l}$, которая известна всем пользователям, генерирует случайное обязательство $g_i \leftarrow \mathrm{H}_1(\mathbf{A}_i, i)$ и отправляет g_i, где $\mathrm{R}_q^{k \times l}$ – кольцо многочленов $\mathbf{Z}/q\mathbf{Z}[x]/(x^n + 1)$. Отправляет $\mathbf{A}_i$ после получения g_i для всех $i \in [N - 1]$, где $[N - 1]$ – множество всех пользователей.

Если $\mathrm{H}_1(\mathbf{A}_i, i) = g_i$ для некоторого i, то отправляет «abort» (отказ от дальнейшего продолжения протокола), иначе вычисляет открытую случайную матрицу

$$\bar{\mathbf{A}}_i = \left[\mathbf{A}_i \middle| \mathbf{I}_k\right] \in R_q^{k \times l}, \quad \bar{\mathbf{A}} = \sum_{i=1}^{N} \bar{\mathbf{A}}_i \ .$$

Для конечного множества $\mathbf{S}$ обозначение $\mathbf{s} \leftarrow \mathbf{S}$ означает, что вектор $\mathbf{s}$ выбирается случайно и равномерно из множества $\mathbf{S}$. Пусть $\mathbf{S}_\alpha^l$ обозначает множество векторов длины ℓ, где каждый коэффициент выбирается равномерно из интервала $[-\alpha, \ldots, \alpha]$.

На этапе генерации ключей каждый пользователь генерирует свой секретный вектор

$$\mathbf{s}_i \leftarrow \mathbf{S}_\alpha^l \ .$$

Агрегированный секрет $\mathbf{s}$ может быть представлен следующем образом, но в явном виде нигде не хранится:

$$\mathbf{s} = \textstyle\sum_{i=1}^{N} \mathbf{s}_i \ .$$

Однако это приводит к полной компрометации секретного ключа, что ограничивает схему одноразовым использованием. Одним из ключевых преимуществ предлагаемой схемы пороговой подписи является то, что общий секрет $\mathbf{s}$ никогда не хранится и не собирается в явном виде. Вместо этого секрет распределяется между участниками с использованием порогового механизма разделения секрета, такого как схема на основе интерполяции полинома Ньютона. Это гарантирует, что секрет не может быть скомпрометирован, если только достаточное количество участников не объединятся для его восстановления.

Открытый ключ $\mathbf{t}_i$ для каждого i-го пользователя вычисляется следующим образом:

$$\mathbf{t}_i = \mathrm{Round}\left(\frac{p}{q} \times \bar{\mathbf{A}} \times \mathbf{s}_i\right) \in R_q^k, \quad \left\|\mathbf{t}_i - \bar{\mathbf{A}}\mathbf{s}_i\right\|_\infty \le 2^{\nu-\mu}.$$

Пользователи генерируют случайное обязательство $v_j \leftarrow H_2(\mathbf{t}_i, j)$ и отправляют v_j. После получения v_j для всех $j \ne i \in [t - 1]$ i-й пользователь отправляет свое значение $\mathbf{t}_i$. Если $H_2(\mathbf{t}_i, i) \ne v_i$ для некоторого i, то отправляют «abort», иначе устанавливают объединенный открытый ключ

$$\mathbf{t} = \sum_{i=1}^{N} \mathbf{t}_i \ .$$

Если протокол не прерывается, пользователи получают (sk_i, pk) в качестве локального результата, где sk_i – секретный ключ i-го пользователя, pk – агрегированный открытый ключ.

$$\left(sk_i, pk\right) = \left(s_i, \bar{\mathbf{A}}, \mathbf{t}\right).$$

Когда все пользователи сгенерировали свои секретные ключи, они получают часть общего приватного ключа, используя схему разделения секрета Ньютона. Они генерируют $(k + l)$ полиномов степени $(t - 1)$ со свободным коэффициентом, равным каждому элементу секретного вектора $\mathbf{s}_i$.

На этапе генерации и объединения подписи будем считать пространство сообщений $\mathrm{M} = \{0, 1\}^*$ и сообщение $m \in \mathrm{M}$.

Определяется порядок, в котором пользователи будут подписывать сообщение, i-й пользователь вычисляет вектор значений разделённой разности нулевого порядка, подставляя идентификатор ID_i в свой полином и складывая полученное значение со значениями, полученными от других пользователей, которые также вычисляют разности нулевого порядка, подставляя идентификатор ID_i в свой полином. Для $(i + 1)$-го пользователя вычисляется разделённая разность первого порядка. Вычисления производятся до $(i + t)$-го пользователя.

$$\mathbf{f}\left[\mathrm{ID}_i\right] = \left(f_1^i\left[\mathrm{ID}_i\right], f_2^i\left[\mathrm{ID}_i\right], \ldots, f_{k+l}^i\left[\mathrm{ID}_i\right]\right);$$

$$\mathbf{f}^{i+1}\left[\mathrm{ID}_i; \mathrm{ID}_{i+1}\right] = \left(f_1^i\left[\mathrm{ID}_i; \mathrm{ID}_{i+1}\right], f_2^i\left[\mathrm{ID}_i; \mathrm{ID}_{i+1}\right], \ldots, f_{k+l}^i\left[\mathrm{ID}_i; \mathrm{ID}_{i+1}\right]\right);$$

$$\vdots$$

$$\mathbf{f}^{N+1}\left[\mathrm{ID}_i; \mathrm{ID}_{i+1}; \ldots; \mathrm{ID}_{N-1}\right] = \left(f_1^i\left[\mathrm{ID}_i; \mathrm{ID}_{i+1}; \ldots; \mathrm{ID}_{N-1}\right], f_2^i\left[\mathrm{ID}_i; \mathrm{ID}_{i+1}; \ldots; \mathrm{ID}_{N-1}\right], \ldots, f_{k+l}^i\left[\mathrm{ID}_i; \mathrm{ID}_{i+1}; \ldots; \mathrm{ID}_{N-1}\right]\right),$$

где $f[\mathrm{ID}_i;\ \mathrm{ID}_{i+1};\ \ldots;\ \mathrm{ID}_{N-1}]$ – разделённая разность i-го порядка i-го пользователя, для j-го элемента вектора секретного ключа ID – идентификатор пользователя, которому отправляется вычисленное значение.

Затем они отправляют обязательство (o_i) каждому пользователю

$$o_i \leftarrow \mathrm{H}_1\left(\mathbf{f}_{\mathrm{ID}}^{j}, i\right).$$

После получения всех o_i каждый пользователь проверяет, что o_i совпадает с ожидаемым значением. Если для некоторого i равенство не выполняется, то отправляется «abort».

Каждый пользователь генерирует свою долю секретного ключа

$$\mathbf{x}_i = \sum_{j=1}^{n} \mathbf{f}_{\mathrm{ID}}^{\mathrm{j}}.$$

Каждый пользователь, кроме нулевого, вычисляет базисные полиномы Ньютона $n_i(0)$:

$$n_i(0) = \prod_{j=0}^{i}\left(-\mathrm{ID}_j\right).$$

Пользователь выбирает вектор $\mathbf{y}_i$:

$$\mathbf{y}_i \leftarrow S_{\gamma-1}^{l},\ \ \|\mathbf{y}_i\|_\infty \le \gamma.$$

Для корректного восстановления подписи объявляем вектор $\bar{\mathbf{y}}$, который в дальнейшем будем использовать для создания подписи:

$$\bar{\mathbf{y}}_i = \frac{\mathbf{y}_{i+1}}{n_{i+1}} \bmod q.$$

Затем пользователи вычисляют первую часть подписи

$$\mathbf{u}_i = \bar{\mathbf{A}}\mathbf{y}_i,\ \ \mathbf{u}_i \in R_q^k.$$

После этого все пользователи вычисляют общий вектор

$$\mathbf{u} = \sum_{i=1}^{t}\mathbf{u}_i.$$

Используется криптографическая хеш-функция $\mathrm{H}_3: \{0,1\}^* \leftarrow B_w$, где для всякого целого $w > 0$ положим, что $B_w = \left\{\mathbf{x} \in \mathrm{R} : \|\mathbf{x}\|_\infty = 1,\ \|\mathbf{x}\| = \sqrt{w}\right\} \subseteq \mathrm{R}$.

Результат функции H_3 – полином $\mathbf{c}$ в R_q с d-коэффициентами, равными ±1, и остальными коэффициентами, равными 0, w определяет верхнюю границу коэффициентов $\mathbf{c}$:

$$\mathbf{c} = \mathrm{H}_3\left(\mathrm{MSB}(\mathbf{u}, d), m\right),\ \ m \in \mathrm{M}.$$

Каждый i-й пользователь вычисляет вторую часть $\mathbf{z}_i$ подписи и вектор $\mathbf{w}_i$, который используется для проверки корректности подписи:

$$\mathbf{z}_i = \mathbf{x}_i \times \mathbf{c} + \bar{\mathbf{y}}_i,$$

$$\mathbf{w}_i = \bar{\mathbf{A}}\mathbf{z}_i - \mathbf{t}_i \times 2^{\nu-\mu-1} \times \mathbf{c}.$$

Если выполняются следующие неравенства, следовательно, процесс генерации подписи должен быть перезапущен.

$$\left\|\mathrm{LSB}\left(\mathbf{w}_i, \nu - d\right)\right\|_\infty \ge 2^{\nu-\mu-1} - w \times 2^{\nu-\mu+1},$$

$$\|\mathbf{z}\|_\infty \ge \gamma - \beta,$$

где β – верхняя граница нормы для компонент подписи, обеспечивающая корректность и безопасность схемы.

В результате пользователь имеет подпись $\sigma_i = (\mathbf{u}_i, \mathbf{z}_i)$, а агрегированная подпись будет $\sigma = (\mathbf{u}, \mathbf{z})$, где

$$\mathbf{z} = \mathbf{z}_0 + \sum_{i=1}^{t-1}\mathbf{z}_i \times n_i(0).$$

Для проверки подписи при получении сообщения m, подписи σ и объединенного открытого ключа $pk = (\mathbf{A}, \mathbf{t})$, необходимо восстановить значение хеш-функции $\mathbf{c}' = \mathrm{H}_3(\mathrm{MSB}(\mathbf{w}, d), m)$, где $\mathbf{w} = \bar{\mathbf{A}}\mathbf{z} - \mathbf{t} \times 2^{\nu-\mu-1} \times \mathbf{c}$.

Подпись принимается, если

$$\mathbf{c}' = \mathbf{c},\ \ \|\mathbf{z}\|_\infty \le \sqrt{N}\left(\gamma - \beta\right),$$

где N – количество подписантов, γ – интервал для коэффициентов вектора $\mathbf{y}_i$. Если проверка не выполняется, то подпись недействительна.

Для доказательства корректности схемы перепишем равенство верификации, как показано ниже:

$$\mathbf{w} = \bar{\mathbf{A}} \times \sum_{i=1}^{t} l_i\left(\mathbf{x}_i\mathbf{c} + \frac{\mathbf{y}_i}{l_i}\right) - \mathbf{c} \times 2^{\nu-\mu} \times \sum_{i=1}^{N}\mathrm{Round}\left(\frac{p}{q} \times \bar{\mathbf{A}}\mathbf{s}_i\right).$$

По свойствам интерполяционного полинома Ньютона

$$\mathbf{x}_0\mathbf{c} + \sum_{i=1}^{t}\left(\mathbf{x}_i\mathbf{c} + \frac{\mathbf{y}_i}{n_i(0)}\right)n_i(0) + \mathbf{y}_0 = \mathbf{cs} + \mathbf{y}.$$

Раскрывая скобки в соответствии с введенными обозначениями, получим

$$\mathbf{w} = \bar{\mathbf{A}}\mathbf{y} + \bar{\mathbf{A}}\mathbf{sc} - \mathbf{c} \times 2^{\nu-\mu} \times \sum_{i=1}^{N}\mathrm{MSB}\left(\bar{\mathbf{A}}\mathbf{s}_i + \mathbf{h}_i, \mu\right) =$$

$$= \bar{\mathbf{A}}\mathbf{y} + \bar{\mathbf{A}}\mathbf{sc} - \mathbf{c}\left(\bar{\mathbf{A}}\mathbf{s} + \mathbf{h} + \sum_{i=1}^{N}\mathrm{LSB}\left(\bar{\mathbf{A}}\mathbf{s}_i + \mathbf{h}_i, \nu - \mu\right)\right),$$

$$\sum_{i=1}^{N}\mathrm{LSB}\left(\bar{\mathbf{A}}\mathbf{s}_i + \mathbf{h}_i, \nu - \mu\right) = \mathrm{LSB}\left(\bar{\mathbf{A}}\mathbf{s} + \mathbf{h}, \nu - \mu\right).$$

Упрощая, мы приходим к равенству, представленному ниже:

$$\mathbf{w} = \bar{\mathbf{A}}\mathbf{y} - \mathbf{c}\left(\mathbf{h} + \mathrm{LSB}\left(\bar{\mathbf{A}}\mathbf{s} + \mathbf{h}, \nu - \mu\right)\right),$$

где $\|\mathbf{c} \times (\mathbf{h} + \mathrm{LSB}(\mathbf{As} + \mathbf{h}, \nu - \mu))\|_\infty < w \times 2^{\nu-\mu+1}$ и $\mathbf{c} \leftarrow B_w$, $\|\mathrm{LSB}(\mathbf{As}, \nu-\mu)\|_\infty < 2^{\nu-\mu}$. Учитывая $\mathrm{LSB}(\mathbf{w}, \nu-d)$ и принимая во внимание ошибку $\mathbf{c} \times (\mathbf{h} + \mathrm{LSB}(\mathbf{As} + \mathbf{h}, \nu - \mu))$, можно заметить, что если $\mathrm{LSB}(\mathbf{w}, \nu - d) > 2^{\nu-d} - w \times 2^{\nu-\mu+1}$, алгоритм отвергает значение $\mathbf{w}$. Поскольку $\mathbf{c} \times (\mathbf{h} + \mathrm{LSB}(\mathbf{As} + \mathbf{h}, \nu - \mu)$ является вектором малой ошибки, из уравнения следует

$$\mathrm{MSB}\left(\mathbf{w}, d\right) = \mathrm{MSB}\left(\bar{\mathbf{A}}\mathbf{y}, d\right).$$

Таким образом, вычисленное значение $\mathbf{c}$ совпадает с $\mathbf{c}'$.

Сравнение классических пороговых схем подписи и нашей схемы

В ходе данной работы представленная пороговая схема подписи была реализована на Python с использованием пакета Sage. Тестирование проводилось на ЭВМ со следующими характеристиками: процессор IntelCOREi7, оперативная память 32 Гб. Наша схема

реализована в соответствии с третьим уровнем безопасности NIST, для которого заданы следующие параметры:

- $q = 8\,388\,608$;
- $p = 4\,194\,304$;
- $k = 6$;
- $l = 5$;
- $n = 256$;
- $d = 49$;
- $\beta = 4$.

Для оценки безопасности предложенной схемы необходимо сравнить её с другими широко используемыми схемами. В качестве сравнения выбраны схемы пороговой подписи ECDSA (384 бит) и BLS12-381. В таблице представлены параметры пороговой подписи ECDSA (384 бит), подписи BLS12-381 и нашей схемы с 3-м уровнем безопасности. Выбор схем ECDSA (384 бит) и BLS12-381 для сравнительного анализа обусловлен их репрезентативностью в современных криптографических системах. ECDSA представляет собой промышленный стандарт цифровых подписей, используемый в большинстве блокчейн-платформ, что обеспечивает понятный ориентир для оценки производительности. BLS12-381 выбран как кандидат среди постквантовых схем (хотя и не является строго квантово-устойчивой в долгосрочной перспективе) на основе эллиптических кривых, получивший широкое распространение в новых распределенных системах.

Сравнение классических пороговых схем подписи и нашей схемы

	ECDSA	BLS12-381	Наша схема
Квантовая стойкость	Нет	Частично	Да
Сложность взлома	2^{128}	2^{112}	2^{128}
Размер подписи	48 байт	96 байт	12 512 бит
Время подписи, мс	24	380	50
Время проверки, мс	1	2 500	4

Безопасность разработанной схемы оценивается через комплексный анализ теоретических оснований и практических характеристик. В теоретическом аспекте стойкость обеспечивается сложностью задач M-LWR и M-SIS, для которых в настоящее время не существует эффективных алгоритмов решения, включая квантовые атаки. Выбранные параметры ($q = 8\,388\,608$, $p = 4\,194\,304$) соответствуют требованиям третьего уровня безопасности по стандарту NIST PQC и оцениваются в 2^{128}.

В сравнении с ECDSA и BLS12-381 предложенное решение демонстрирует абсолютную устойчивость к квантовым атакам при сохранении сопоставимой сложности взлома.

Заключение

Разработанная пороговая схема подписи демонстрирует комплекс преимуществ перед традиционными решениями. Ключевым достижением стало успешное сочетание LWR-криптографии с оптимизированным методом интерполяции Ньютона, что позволило преодолеть основные ограничения существующих подходов.

В отличие от интерполяции Лагранжа, требующей $O(n^2)$ операций при изменении числа участников, наш метод обеспечивает линейную сложность $O(n)$ благодаря свойствам разделенных разностей Ньютона, так как при добавлении нового участника требуется пересчет только последней разделенной разности. Модификация t-й доли секрета влияет только на $(N - t)$ коэффициентов полинома, в отличие от полного пересчета в схеме Лагранжа.

Особого внимания заслуживает практическая эффективность предложенного решения: тесты показали, что использование интерполяции Ньютона сокращает время генерации подписи на 25–35% по сравнению с лагранжевым подходом при аналогичном уровне безопасности. Это достигнуто за счет трех факторов: меньшего количества арифметических операций, возможности параллельных вычислений и отсутствия необходимости полного пересчета полинома при изменении состава участников.

Перспективы дальнейшего развития работы видятся в двух направлениях: оптимизация параметров схемы для конкретных IoT-приложений и исследование возможности комбинирования предложенного подхода с другими перспективными методами постквантовой криптографии.

Полученные результаты подтверждают, что сочетание LWR с интерполяцией Ньютона представляет собой перспективную основу для создания нового поколения криптографических протоколов, сочетающих квантовую стойкость с высокой производительностью в распределенных системах.

Работа выполнена в рамках государственного задания (проект FSER-2025–0003).

Литература

1. Shor P.W. Algorithms for quantum computation: discrete logarithms and factoring // Proceedings 35th annual symposium on foundations of computer science. – Santa Fe, NM, USA: IEEE, 1994. – P. 124–134.

2. Dehkordi M.H. LWE-based verifiable essential secret image sharing scheme ((t, s, k, n)-VESIS) / M.H. Dehkordi, S.T. Farahi, S. Mashhadi // IET Image Processing. – Stevenage, UK: IET, 2024. – Vol. 18, No. 4. – P. 1053–1072.

3. Çalkavur S. Code Based Secret Sharing Schemes: Applied Combinatorial Coding Theory / S. Çalkavur, Z. Öztöprak, O. Yayla. – Singapore: World Scientific, 2022. – 212 p.

4. Boneh D. Threshold signatures with private accountability / D. Boneh, C. Komlo // Annual International Cryptology Conference. – Zurich, Switzerland: Springer Nature Switzerland, 2022. – P. 551–581.

5. Baird L. et al. Threshold signatures in the multiverse // 2023 IEEE Symposium on Security and Privacy (SP). – San Francisco, CA, USA: IEEE, 2023. – P. 1454–1470.

6. Fischlin M. BUFFing Threshold Signature Schemes / M. Fischlin, A. Mitrokotsa, J. Tomy // IACR International Conference on Public-Key Cryptography. – Lyon, France: Springer, Cham, 2025. – P. 137–168.

7. Duc A. Better algorithms for LWE and LWR / A. Duc, F. Tramer, S. Vaudenay // Annual International Conference on

the Theory and Applications of Cryptographic Techniques. – Sofia, Bulgaria: Springer Berlin Heidelberg, 2015. – P. 173–202.

8. Bezzateev S. On secret sharing with newton's polynomial for multi-factor authentication / S. Bezzateev, V. Davydov, A. Ometov // Cryptography. – 2020. – Vol. 4, No. 4. – P. 34.

9. Adi S. How to share a secret // Commun. ACM. – 1979. – Vol. 22. – P. 612–613.

10. Blakley G.R. Safeguarding cryptographic keys // Managing requirements knowledge, international workshop on. – IEEE Computer Society, 1979. – P. 313–313.

11. Shoup V. Practical threshold signatures // Advances in Cryptology – EUROCRYPT 2000: International Conference on the Theory and Application of Cryptographic Techniques Bruges, Belgium, May 14–18, 2000. Proceedings 19. – Springer Berlin Heidelberg, 2000. – P. 207–220.

12. Banerjee A. Pseudorandom functions and lattices / A. Banerjee, C. Peikert, A. Rosen // Annual International Conference on the Theory and Applications of Cryptographic Techniques. – Cambridge, UK: Springer Berlin Heidelberg, 2012. – P. 719–737.

13. Jiang T. Blockchain-based internet of vehicles: Distributed network architecture and performance analysis / T. Jiang, H. Fang, H. Wang // IEEE Internet of Things Journal. – 2018. – Vol. 6, No. 3. – P. 4640–4649.

14. Damgård I. et al. Two-round n-out-of-n and multi-signatures and trapdoor commitment from lattices // Journal of Cryptology. – 2022. – Vol. 35, No. 2. – P. 14.

15. Kiltz E. A concrete treatment of Fiat-Shamir signatures in the quantum random-oracle model / E. Kiltz, V. Lyubashevsky, C. Schaffner // Advances in Cryptology – EUROCRYPT–2018: 37th Annual International Conference on the Theory and Applications of Cryptographic Techniques. – Tel Aviv, Israel, April 29 – May 3, 2018. Proceedings, Part III 37. – Springer International Publishing, 2018. – P. 552–586.

16. Проект стандартизации постквантовой цифровой подписи / Е.А. Киршанова, Н.С. Колесников, Е.С. Малыгина, С.А. Новоселов // Прикладная дискретная математика. Приложение. – 2020. – № 13. – С. 44–51.

Кустов Елизар Филаретович
Аспирант факультета безопасности информационных технологий (ФБИТ) Университета ИТМО
Кронверкский пр-т, 49, лит. А.,
г. Санкт-Петербург, Россия, 197101
ORCID: 0000-0002-0191-1178
Тел.: +7-981-834-14-60
Эл. почта: elizarkustov@mail.ru

Беззатеев Сергей Валентинович
Д-р техн. наук, проф. ФБИТ Университета ИТМО;
зав. каф. информационной безопасности
Государственного университета
аэрокосмического приборостроения (ГУАП)
Большая Морская ул., 67, лит. А,
г. Санкт-Петербург, Россия, 190000
ORCID: 0000-0002-0924-6221
Тел.: +7-904-517-09-51
Эл. почта: sergey.bezzateev@gmail.com

Поступила в редакцию: 07.05.2025.
Принята к публикации: 25.06.2025.

Kustov E.F., Bezzateev S.V.

Lattice-Based Threshold Signature Scheme with Newton Interpolation

This paper presents a novel threshold digital signature scheme that combines lattice-based cryptography with interpolation methods. The scheme is built upon the Learning with Rounding (LWR) problem and can be applied to secure IoT devices, where the combination of computational efficiency and quantum resistance is particularly valuable. The proposed approach utilizes Newton interpolation, which demonstrates advantages over classical Lagrange interpolation in terms of performance and flexibility when working with dynamic participant groups.
Keywords: threshold signature, lattice-based cryptography, Newton interpolation, LWR, SIS, post-quantum cryptography, secret sharing.
DOI: 10.21293/1818-0442-2025-28-2-166-171

References

1. Shor P.W. *Algorithms for quantum computation: discrete logarithms and factoring*. Proceedings 35th annual symposium on foundations of computer science. Santa Fe, NM, USA: IEEE, 1994, pp. 124–134.

2. Dehkordi M.H., Farahi S.T., Mashhadi S. LWE-based verifiable essential secret image sharing scheme ((t, s, k, n)-VESIS). *IET Image Processing. Stevenage*, UK: IET, 2024, vol. 18, no. 4, pp. 1053–1072.

3. Çalkavur S., Öztöprak Z., Yayla O. Code Based Secret Sharing Schemes: Applied Combinatorial Coding Theory. Singapore: World Scientific, 2022. 212 p.

4. Boneh D., Komlo C. *Threshold signatures with private accountability*. Annual International Cryptology Conference. Zurich, Switzerland: Springer Nature Switzerland, 2022, pp. 551–581.

5. Baird L. et al. *Threshold signatures in the multiverse*. 2023 IEEE Symposium on Security and Privacy (SP). San Francisco, CA, USA: IEEE, 2023, pp. 1454–1470.

6. Fischlin M., Mitrokotsa A., Tomy J. *BUFFing Threshold Signature Schemes*. IACR International Conference on Public-Key Cryptography. Lyon, France: Springer, Cham, 2025, pp. 137–168.

7. Duc A., Tramer F., Vaudenay S. *Better algorithms for LWE and LWR*. Annual International Conference on the Theory and Applications of Cryptographic Techniques. Sofia, Bulgaria: Springer Berlin Heidelberg, 2015, pp. 173–202.

8. Bezzateev S., Davydov V., Ometov A. On secret sharing with Newton's polynomial for multi-factor authentication. *Cryptography*, 2020, vol. 4, no. 4, pp. 34.

9. Shamir A. How to share a secret. *Communications of the ACM*, 1979, vol. 22, pp. 612–613.

10. Blakley G.R. *Safeguarding cryptographic keys*. Managing requirements knowledge, international workshop on, IEEE Computer Society, 1979, p. 313.

11. Shoup V. *Practical threshold signatures*. Advances in Cryptology-EUROCRYPT 2000: International Conference on the Theory and Application of Cryptographic Techniques. Bruges, Belgium: Springer Berlin Heidelberg, 2000, pp. 207–220.

12. Banerjee A., Peikert C., Rosen A. Pseudorandom functions and lattices // Annual International Conference on the Theory and Applications of Cryptographic Techniques. Cambridge, UK: Springer Berlin Heidelberg, 2012, pp. 719–737.

13. Jiang T., Fang H., Wang H. Blockchain-based internet of vehicles: Distributed network architecture and performance analysis. *IEEE Internet of Things Journal*, 2018, vol. 6, no. 3, pp. 4640–4649.

14. Damgård I. et al. Two-round n-out-of-n and multi-signatures and trapdoor commitment from lattices. *Journal of Cryptology*, 2022, vol. 35, no. 2, pp. 14.

15. Kiltz E., Lyubashevsky V., Schaffner C. *A concrete treatment of Fiat-Shamir signatures in the quantum random-oracle model*. Advances in Cryptology-EUROCRYPT 2018. Tel Aviv, Israel: Springer International Publishing, 2018, pp. 552–586.

16. Kirshanova E.A. et al. Proekt Standartizatsii Post-kvantovoj Tsifrovoj Podpisi [Project for Standardization of Post-Quantum Digital Signatures] *Prikladnaya Diskretnaya Matematika*. Supplement, 2020, no. 13, pp. 44–51 (in Russ.).

Elizar F. Kustov
PhD student, Department of Information Security Technologies, ITMO University
49, bld. A. Kronverksky pr., St. Petersburg, Russia, 197101
ORCID: 0000-0002-0191-1178
Phone: +7-904-517-09-51
Email: elizarkustov@mail.ru

Sergey V. Bezzateev
Doctor of Engineering Sciences, professor, Department of Information Security Technologies, ITMO University
Head of Department Information Security,
State University of Aerospace Instrumentation (SUAI)
67, bld. A, Bolshaya Morskaya st.,
St. Petersburg, Russia, 190000
ORCID: 0000-0002-0924-6221
Phone: +7-904-517-09-51
Email: sergey.bezzateev@gmail.com

Received: 07.05.2025.
Accepted: 25.06.2025.