Геометрическая параметризация p-адического соленоида и её применение в квантовой криптографии

Т. Т. Троянок

***Аннотация*—В данной статье описано применение геометрической параметризации p-адического соленоида и её применение в квантовой криптографии. Представлено геометрическое отображение элементов соленоида на единичный квадрат, позволяющее параметризовать квантовые состояния кубита на сфере Блоха. На основе этого отображения предложены алгоритмы: алгоритм генерации секретного соленоидного ключа, алгоритм генерации открытого Серпинского ключа, алгоритм генерации квантового состояния по открытому Серпинскому ключу, алгоритм соленоидной стеганографии, схема соленоидной электронной подписи и протокол соленоидной challenge-response аутентификации, использующие преобразование ключа в квантовые параметры (ϕ, θ). Показана возможность интеграции представления элементов соленоида в протоколы квантового распределения ключей (например, BB-84) для кодирования состояний. Ключевое преимущество подходов — использование p-адической метрики и топологических свойств соленоида для повышения криптографической устойчивости.**

***Ключевые слова*—p-адический соленоид, квантовые состояния, сфера Блоха, ковёр Серпинского, информационная безопасность**

I. Представление элементов p-адического соленоида в позиционной системе

Классические гомоморфизмы образуют проективную систему $(\mathbb{R}/p^n\mathbb{Z}, \phi_n)_{n \geq 0}$ из топологических групп:

$$\begin{aligned} &\phi_n : \mathbb{R}/p^{n+1}\mathbb{Z} \to \mathbb{R}/p^n\mathbb{Z}, \\ &x \mod p^{n+1}\mathbb{Z} \mapsto x \mod p^n\mathbb{Z} \, (n \geq 0). \end{aligned} \tag{1}$$

Определение I.1. p-адическим соленоидом $\mathcal{S}_p$ называется проективный предел

$$\lim_{\leftarrow}(\mathcal{S}_p) = \lim_{\leftarrow}(\mathbb{R}/p^n\mathbb{Z})$$

в проективной системе $(\mathbb{R}/p^n\mathbb{Z}, \phi_n)$ ([1—3]).

p-адический соленоид $\mathcal{S}_p$ вляется компактной абелевой группой, снабжённой каноническими проекциями:

$$\psi_n : \mathcal{S}_p \to \mathbb{R}/p^n\mathbb{Z} (n \geq 0),$$

которые являются непрерывными сюръективными гомоморфизмами.

Рассмотрим представление элементов p-адического соленоида следующего вида ([4]):

$$\ldots \alpha_n \alpha_{n-1} \ldots \alpha_2 \alpha_1 \alpha_0, \alpha_{-1}\alpha_{-2} \ldots \alpha_{-n} \ldots, \tag{2}$$

Статья получена 19 июня 2025 г.

Татьяна Тимуровна Троянок, МГУ им. М.В. Ломоносова, (email: troyanok.tanya@mail.ru).

где

- $\ldots \alpha_2 \alpha_1 \alpha_0$ - целая часть соответствует целому p-адическому числу;
- $0, \alpha_{-1}\alpha_{-2} \ldots$ - дробная часть соответствует действительному числу из $[0, 1]$.

II. Отображение представления элементов p-адического соленоида на ковре Серпинского

Визуализируем соленоид 2 с помощью ковра Серпинского для $p = 2$.

A. Конструкция ковра Серпинского

Ковёр Серпинского строится рекурсивно:

1) Исходный квадрат делится на 9 равных квадратов.
2) Центральный квадрат удаляется.
3) Процесс повторяется для каждого из 8 оставшихся квадратов.

Каждый уровень рекурсии соответствует одному разряду элемента соленоида. Соленоид:

$$\ldots \alpha_k \alpha_{k-1} \ldots \alpha_1 \alpha_0, \alpha_{-1}\alpha_{-2} \ldots \alpha_{-(k-1)}\alpha_{-k} \ldots 2$$

отображается на позицию $(x; y)$ внутри ковра.

Дробная компонента (правая от запятой) определяет горизонтальную координату:

- Каждый бит α_{-k} выбирается между левой (0) или правой (1) третью текущего интервала;
- Средняя треть всегда исключается.

Целая компонента (левая от запятой) определяет вертикальную координату:

- Читается справа налево (от α_0 к α_1, α_2...)
- Каждый бит выбирает между нижней (0) или верхней (1) третью
- Средняя треть исключается

B. Связь представления элементов соленоида с отображением Монна

Преобразование целой части элемента соленоида для визуализации на ковре Серпинского соответствует отображению Монна на квадрате $[0, 1]$ ([1, 5, 6]).

Для p-адического числа $\sum\limits_{k=0}^{\infty} \alpha_k p^k, \alpha_i \in \{0, \ldots, p-1\}$ **отображение Монна** задаётся формулой:

$$\sum_{k=0}^{\infty} \alpha_k p^{-k-1}, \alpha_i \in \{0, \ldots, p-1\}$$

Свойства отображения:

- Отображение сохраняет меру Хаара на $\mathbb{Z}_p$, преобразуя её в меру Лебега на $[0, 1]$;
- Расстояние между точками в образе зависит от их p-адического расстояния (чем больше совпадающих старших разрядов, тем ближе точки);
- Отображение не является взаимно однозначным. Например, p-адические числа, различающиеся в старших разрядах, могут отображаться в одну точку (аналог периодических дробей в вещественных числах).

C. Алгоритм параметризации ковра Серпинского элементами соленоида

1) Инициализация исходного квадрата
   - $X = [0, 1]$ (горизонтальный интервал);
   - $Y = [0, 1]$ (вертикальный интервал);
2) Для дробной части ($k \geq 1$):
   - $\alpha_{-k} = 0$: оставляем левую треть X;
   - $\alpha_{-k} = 1$: оставляем правую треть X;
   - Удаляем среднюю треть X;
3) Для целой части ($k \geq 0$):
   - $\alpha_k = 0$: оставляем нижнюю треть Y;
   - $\alpha_k = 1$: оставляем верхнюю треть Y;
   - Удаляем среднюю треть Y;
4) После выполнения нескольких шагов координаты точки будут следующие:
   - $x =$ середина итогового X-интервала
   - $y =$ середина итогового Y-интервала

III. Геометрическая интерпретация соленоида на ковре Серпинского и её применение в квантовой механике

Сфера Блоха — это геометрическое представление квантового состояния кубита, задаваемого углами $\theta \in [0, \pi]$ и $\phi \in [0, 2\pi)$.

Между объектами 'Сфера Блоха' и 'Ковёр Серпинского' можно выделить следующие аналогии ([7—10])

Сфера Блоха	Ковёр Серпинского
Точка = квантовое состояние	Точка = представление элемента p-адического соленоида
Северный/южный полюс = $0, 1$	Вертикальная ось = целая часть элемента соленоида
Экватор = суперпозиции	Горизонтальная ось = дробная часть
Непрерывная поверхность	Фрактальная структура с "дырами"

Механизм отображения квантовых состояний ([7, 11]) на квадрат Серпинского с помощью представления элементов p-адического соленоида

1) Отображение сферы на единичный квадрат
   - Северный полюс $1 \to$ верхняя сторона квадрата ($y = 1$);
   - Южный полюс $0 \to$ нижняя сторона ($y = 0$);
   - Экватор $\to$ центральная горизонталь ($y = 0.5$);
2) Задание координат. Для точки сферы с полярными координатами (θ, ϕ):
   - Вертикальная ось θ кодируется целой компонентой элемента соленоида через 2-адическую норму:
   $$\theta = \pi \cdot y,$$
   где y - координата точки по оси OY на ковре Серпинского;
   - Горизонтальная ось ϕ задаётся дробной компонентой элемента соленоида:
   $$\phi = 2 \cdot \pi \cdot x,$$
   где x - координата точки по оси OX на ковре Серпинского.
3) Построение решётки. Каждому узлу ковра Серпинского ставим в соответствие состояние кубита:
$$\psi = \cos\Big(\frac{\theta}{2}\Big)0 + e^{i\phi}\sin\Big(\frac{\theta}{2}\Big)1,$$
где θ и ϕ вычисляются из позиции точки на ковре.

IV. Применение геометрической интерпретации соленоида на ковре Серпинского в информационной безопасности

Главная идея заключается в использовании топологических свойств фракталов (ковра Серпинского) и 2-адических соленоидов для создания безопасного шифрования.

A. Соленоидные ключи

Определение IV.1. Соленоидный ключ - ключ, который был построен с помощью представления элементов p-адического соленоида.

Секретным соленоидным ключом называется представление элемента соленоида вида:

$$(integer\_part, fractional\_part), \tag{3}$$

где:

- $integer\_part$ - целая часть представления элемента 2-адического соленоида;
- $fractional\_part$ - дробная часть представления элемента 2-адического соленоида.

Алгоритм генерации секретного соленоидного ключа

Назначение: Создание секретного ключа на основе представления элемента p-адического соленоида.
Вход: N (длина целой части), M (длина дробной части), CSPRNG (криптографически стойкий генератор).
Выход: $(integer\_part, fractional\_part)$.

1) Инициализировать пустые строки для целой и дробной частей.
2) Для M раз:
   - Сгенерировать случайный бит через CSPRNG.
   - Добавить бит в конец строки дробной части.
3) Для N раз:
   - Сгенерировать случайный бит через CSPRNG.
   - Добавить бит в конец строки целой части.
4) Вернуть пару $(integer\_part, fractional\_part)$.

Определение IV.2. Открытый Серпинский ключ - координата (x, y) представления элемента 2-адического

соленоида на ковре Серпинского, полученный с помощью *секретного соленоидного ключа*.

Алгоритм генерации открытого ключа Серпинского
Назначение: Преобразование секретного ключа в координаты на ковре Серпинского.
Вход: $(integer\_part, fractional\_part)$.
Выход: Координаты (x, y).

1) Развернуть целую часть (для корректной обработки).
2) Инициализировать $x = 0$, $y = 0$.
3) Для каждого бита дробной части (от первого до последнего):
   - Обновить $x = x +$ бит $\times\ 2 \times 3^{-k}$ (где k — позиция бита)
4) Для каждого бита целой части (от первого до последнего):
   - Обновить $y = y +$ бит $\times\ 2 \times 3^{-k}$.
5) Вернуть (x, y).

По координатам представления элемента 2-адического соленоида можно сгенерировать квантовое состояние.

Алгоритм генерации квантового состояния
Назначение: Преобразование координат на ковре Серпинского в квантовые параметры.
Вход: (x, y).
Выход: (ϕ, θ).

1) Вычислить $\phi = 2\pi \cdot x$.
2) Вычислить $\theta = \pi \cdot y$.
3) Вернуть (ϕ, θ).

Также для соленоидных ключей можно определить функцию циклического сдвига влево на k позиций.

Алгоритм циклического сдвига соленоидного ключа
Назначение: Модификация ключа.
Вход: Ключ $(integer\_part, fractional\_part)$, параметр сдвига k.
Выход: Сдвинутый ключ

$$(integer\_part', fractional\_part').$$

1) Объединить целую и дробную части в одну битовую строку.
2) Выполнить циклический сдвиг строки влево на k позиций.
3) Разделить результат на новые целую (первые N бит) и дробную (последние M бит) части.
4) Вернуть новый ключ

Секретный соленоидный и открытый Серпинский ключи можно использовать в квантовой криптографии. Ранее в разделе III была показана связь между геометрической интерпретацией элементов 2-адических соленоидов на ковре Серпинского и квантовыми состояниями:

$$\psi = \cos\Big(\frac{\theta}{2}\Big)0 + e^{i\phi}\sin\Big(\frac{\theta}{2}\Big)1, \tag{4}$$

$$\theta = \pi \cdot y, \tag{5}$$

где y - координата точки по оси OY на ковре Серпинского

$$\phi = 2 \cdot \pi \cdot x, \tag{6}$$

где x - координата точки по оси OX на ковре Серпинского

Такую связь можно использовать, например, в протоколе **BB-84**, следующим образом:

1) **Генерация**
   Алиса генерирует $(integer\_part, fractional\_part)$, преобразует в (θ, ϕ), подготавливает ψ.
2) **Передача**
   Алиса отправляет ψ по квантовому каналу Бобу.
3) **Измерение**
   Боб измеряет состояние в согласованном базисе (или случайном, как в **BB-84**).
4) **Постобработка**
   Алиса и Боб сравнивают часть базисов по открытому каналу, отбрасывают несовпавшие, оставляют совпавшие.
5) **Получение ключа**
   Боб восстанавливает (x, y), а значит и $(integer\_part, fractional\_part)$.
6) **Общий секретный ключ**
   Совпадающие $(integer\_part, fractional\_part)$ составляют общий секретный ключ, который известен только Алисе и Бобу.

Боб восстанавливает секретные соленоидные ключи по следующему алгоритму:

B. Соленоидная стеганография

Классическая LSB-стеганография - замена последних значащих битов в контейнере (изображения, аудио или видеозаписи) на биты скрываемого сообщения ([7, 11]). Но у такой замены есть недостатки:

- Легко обнаруживается анализом последовательных пикселей.
- Легко извлекается без ключа.
- Уязвима к статистическим и визуальным атакам.

Но можно использовать геометрическую интерпретацию соленоида на ковре Серпинского для решения данных проблем. Соленоидная стеганография будет скрывать данные в цифровых носителях (изображения, аудио, видео) через динамическое преобразование ключа и фрактальную адресацию. В отличие от классической стеганографии, где данные встраиваются в фиксированные участки (например, младшие биты пикселей), соленоидный подход использует:

- Циклические сдвиги ключа для генерации псевдослучайных позиций встраивания.
- Фрактальные координаты (ковёр Серпинского) для выбора точек в носителе.
- Криптографически стойкие генераторы (CSPRNG) для создания уникальных сдвигов.

Алгоритм встраивания сообщения
Назначение: Сокрытие данных в цифровом носителе с использованием соленоидных ключей.
Вход: Сообщение msg, ключ, носитель $carrier$, IV (вектор инициализации).
Выход: Модифицированный носитель $carrier'$.

1) Если IV не задан:
   - Сгенерировать IV через CSPRNG. Встроить IV в LSB первых 16 пикселей носителя.
2) Вычислить $seed = \text{SHA3}(\text{ключ}\|\text{IV})$.
3) Сгенерировать последовательность сдвигов $\{s_k\}$ через CSPRNG.
4) Для каждого бита сообщения:
   - Применить сдвиг ключа на s_k.

- Вычислить координаты на ковре Серпинского.
- Заменить LSB пикселя носителя в позиции (x_k, y_k) на бит сообщения.

5) Вернуть модифицированный носитель.

Алгоритм извлечения сообщения

Назначение: Восстановление скрытых данных из носителя.

Вход: Модифицированный носитель $carrier'$, ключ.

Выход: Сообщение msg.

1) Извлечь IV из LSB первых 16 пикселей.
2) Вычислить $seed = \text{SHA3}(\text{ключ} \| \text{IV})$.
3) Сгенерировать последовательность сдвигов $\{s_k\}$ через CSPRNG.
4) Для каждого бита сообщения
   - Применить сдвиг ключа на s_k.
   - Вычислить координаты (x_k, y_k).
   - Извлечь LSB пикселя в позиции (x_k, y_k).
5) Вернуть сообщение.

C. Соленоидная электронная подпись

Определение IV.3. Соленоидная электронная подпись — асимметричный криптографический протокол, где секретный ключ генерируется как элемент 2-адического соленоида, а открытый ключ вычисляется через его геометрическое представление на ковре Серпинского.

Алгоритм генерации подписи

Назначение: Создание подписи на основе соленоидного ключа.

Вход: Сообщение msg, секретный ключ sk.

Выход: Подпись $\sigma = (\phi, \theta, s)$.

1) Вычислить хеш сообщения $h = \text{Stribog}(msg)$.
2) Применить циклический сдвиг ключа на $h \mod (N + M)$.
3) Вычислить координаты на ковре Серпинского.
4) Преобразовать координаты в квантовые параметры.
5) Сгенерировать случайную маскирующую строку s через CSPRNG.
6) Вернуть подпись σ.

Алгоритм проверки подписи

Назначение: Верификация подписи с использованием открытого ключа.

Вход: Сообщение msg, подпись σ, открытый ключ pk.

Выход: True/False.

1) Восстановить координаты (x_G, y_G) из открытого ключа.
2) Вычислить хеш сообщения $h = \text{Stribog}(msg)$.
3) Проверить условия:
   - $\phi \equiv (2\pi \cdot x_G + s \cdot \pi) \mod 2\pi$,
   - $\theta \equiv (\pi \cdot y_G + s \cdot \pi/2) \mod \pi$.
4) Вернуть результат проверки.

D. Соленоидная Challenge-Response аутентификация

Определение IV.4. Challenge-response аутентификация — это протокол, при котором система (сервер) высылает пользователю случайную строку (challenge), а пользователь должен доказать знание секрета, сгенерировав корректный ответ (response, обычно подпись этого challenge). Это защищает от атак повтором (replay) и подделки, потому что challenge каждый раз новый.

Соленоидная Challenge-Response аутентификация использует динамическое преобразование секретного ключа через циклические сдвиги и фрактальные вычисления для генерации уникального ответа на случайный запрос (challenge). Ключевые особенности:

- **Динамический ключ**: Каждый challenge модифицирует ключ через циклический сдвиг, создавая «одноразовую» версию для ответа.
- **Фрактальная адресация**: Преобразование сдвинутого ключа в координаты на ковре Серпинского гарантирует нелинейность и устойчивость.
- **Квантовые параметры**: Ответ кодируется в углах кубита (ϕ, θ), что усложняет анализ даже при перехвате данных.

Алгоритм генерации ответа

Назначение: Создание ответа на запрос аутентификации.

Вход: Секретный ключ, параметры N, M, запрос s.

Выход: Параметры кубита (ϕ', θ').

1) Применить циклический сдвиг ключа на s позиций.
2) Вычислить координаты на ковре Серпинского.
3) Преобразовать координаты в квантовые параметры.
4) Вернуть (ϕ', θ').

Алгоритм верификации ответа

Назначение: Проверка корректности ответа на аутентификацию.

Вход: Полученные параметры $(\phi_{\text{client}}, \theta_{\text{client}})$, секретный ключ сервера, запрос s.

Выход: True/False.

1) Вычислить ожидаемые параметры $(\phi_{\text{server}}, \theta_{\text{server}})$.
2) Проверить условия:
   - $|\phi_{\text{client}} - \phi_{\text{server}}| < \epsilon$,
   - $|\theta_{\text{client}} - \theta_{\text{server}}| < \epsilon$ (где ϵ — допустимая погрешность).
3) Вернуть результат проверки.

V. Заключение

В данной статье предложен новый подход к построению криптографических примитивов и методов информационной безопасности, основанный на использовании топологических и алгебраических свойств p-адического соленоида и его геометрической интерпретации на ковре Серпинского.

Библиография

[1] A. M. Robert, *A Course in p-adic Analysis*, англ., 3-е изд. New York: Springer, 2000.

[2] Р. Н. Гумеров, *Групповые структуры и их приложение в анализе и топологической группе*. Казань: Изд-во КФУ, 2022.

[3] S. Semmes, *Some Remarks About Solenoids*, англ. 2012. doi: 10.48550/arXiv.1210.4788.

[4] A. Haynes, H. Koivusalo и J. Furno, «Bounded Remainder Sets for Rotations on p-adic Solenoids,» англ., *Proceedings of the American Mathematical Society*, т. 147, № 12, с. 5105—5115, 2019.

[5] Y. I. Manin, «Reflections on Arithmetical Physics,» англ., *Conformal Invariance and String Theory*, с. 293—303, 1989.

[6] И. В. Волович, В. С. Владимиров и Ю. И. Зеленов, *p-адический анализ и математическая физика*. Москва: Наука, 1995.

[7] А. С. Андрущенко и др., *Прикладные квантовые технологии для защиты информации*. Медиа Группа ”Авангард”, 2023.

[8] K. H. Hofmann и S. A. Morris, *The Structure of Compact Groups*, англ. 2020, т. 25.

[9] V. S. Anashin, «Free Choice in Quantum Theory: A p-adic View,» англ., *Entropy*, т. 25, № 2, 2023.

[10] A. Jadczyk, «On Quantum Iterated Function Systems,» англ., *Central European Journal of Physics*, т. 2, № 3, с. 492—503, 2004.

[11] К. В. Антипин. «Введение в квантовую теорию информации.» (2022), url: https://teach-in.ru/course/introduction-to-quantum-information-theory-antipun/lecture.

On geometric parametrization of the p-adic solenoid and applications to quantum cryptography

Troianok Tatiana Timurovna

***Abstract*—This article describes the application of geometric parametrization of the p-adic solenoid in quantum cryptography. A geometric mapping of solenoid elements onto the unit square is presented, enabling the parameterization of qubit quantum states on the Bloch sphere. Based on this mapping, the following algorithms are proposed: a solenoid secret key generation algorithm, a Sierpinski public key generation algorithm, a quantum-state generation algorithm from a Sierpinski public key, a solenoid steganography algorithm, a solenoid digital signature scheme, and a solenoid challenge-response authentication protocol, all utilizing the transformation of keys into quantum parameters (ϕ, θ). The possibility of integrating the representation of solenoid elements into quantum key distribution protocols (e.g., BB-84) for state encoding is demonstrated. The key advantage of these approaches is the use of the p-adic metric and the topological properties of the solenoid to enhance cryptographic strength.**

***Keywords*—p-adic solenoid, quantum states, Bloch sphere, Sierpinski carpet, information security**

[1–11]

References

[1] A. M. Robert, *A Course in p-adic Analysis*, 3rd ed. New York: Springer, 2000.

[2] R. N. Gumerov, *Gruppovye struktury i ikh prilozhenie v analize i topologicheskoy gruppe*, Russian. Kazan': Izd-vo KFU, 2022.

[3] S. Semmes, *Some Remarks About Solenoids*. 2012. doi: 10.48550/arXiv.1210.4788.

[4] A. Haynes, H. Koivusalo, and J. Furno, «Bounded remainder sets for rotations on p-adic solenoids», *Proceedings of the American Mathematical Society*, vol. 147, no. 12, pp. 5105–5115, 2019.

[5] Y. I. Manin, «Reflections on arithmetical physics», *Conformal Invariance and String Theory*, pp. 293–303, 1989.

[6] I. V. Volovich, V. S. Vladimirov, and Y. I. Zelenov, *p-adicheskiy analiz i matematicheskaya fizika*. Moskva: Nauka, 1995.

[7] A. S. Andrushchenko *et al.*, *Prikladnye kvantovye tekhnologii dlya zashchity informatsii*. Media Gruppa "Avangard", 2023.

[8] K. H. Hofmann and S. A. Morris, *The Structure of Compact Groups*. 2020, vol. 25.

[9] V. S. Anashin, «Free choice in quantum theory: A p-adic view», *Entropy*, vol. 25, no. 2, 2023.

[10] A. Jadczyk, «On quantum iterated function systems», *Central European Journal of Physics*, vol. 2, no. 3, pp. 492–503, 2004.

[11] K. V. Antipin. «Vvedenie v kvantovuyu teoriyu informatsii». (2022), [Online]. Available: https://teach-in.ru/course/introduction-to-quantum-information-theory-antipun/lecture.