НАУЧНО-ТЕХНИЧЕСКИЙ ВЕСТНИК ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ, МЕХАНИКИ И ОПТИКИ
январь–февраль 2025 Том 25 № 1 http://ntv.ifmo.ru/
SCIENTIFIC AND TECHNICAL JOURNAL OF INFORMATION TECHNOLOGIES, MECHANICS AND OPTICS
January–February 2025 Vol. 25 No 1 http://ntv.ifmo.ru/en/
ISSN 2226-1494 (print) ISSN 2500-0373 (online)

НАУЧНО-ТЕХНИЧЕСКИЙ ВЕСТНИК
ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ, МЕХАНИКИ И ОПТИКИ

doi: 10.17586/2226-1494-2025-25-1-174-177
УДК 004.056.55

# WaveVRF: постквантовая проверяемая псевдослучайная функция, основанная на кодах, исправляющих ошибки

**Жан-Мишель Никодэмович Дакуо**✉

Университет ИТМО, Санкт-Петербург, 197101, Российская Федерация
Санкт-Петербургский государственный университет аэрокосмического приборостроения, Санкт-Петербург, 190000, Российская Федерация
КуАпп, Москва, 121205, Российская Федерация
jeandakuo@mail.ru✉, https://orcid.org/0000-0002-4084-8829

**Аннотация**
Предложена новая проверяемая псевдослучайная функция (Verifiable Random Function, VRF), основанная на задаче синдромного декодирования и подписи Wave, устойчивая к атакам квантового компьютера. Разработанная новая схема VRF демонстрирует возможность применения задачи синдромного декодирования для реализации криптографически стойких решений. Представлено описание ключевых алгоритмов VRF (KeyGen, VRFEval, VRFVerify). Показаны основные свойства функции: полная доказуемость, уникальная доказуемость и псевдослучайность.

**Ключевые слова**
VRF, криптография, Wave, PRG, проблема синдромного декодирования

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

**Ссылка для цитирования:** Дакуо Ж.-М.Н. WaveVRF: постквантовая проверяемая псевдослучайная функция, основанная на кодах, исправляющих ошибки // Научно-технический вестник информационных технологий, механики и оптики. 2025. Т. 25, № 1. С. 174–177. doi: 10.17586/2226-1494-2025-25-1-174-177

# WaveVRF: post-quantum verifiable random function based on error-correcting codes

**Zhan-Mishel N. Dakuo**✉

ITMO University, Saint Petersburg, 197101, Russian Federation
Saint Petersburg State University of Aerospace Instrumentation, Saint Petersburg, 190000, Russian Federation
QApp, Moscow, 121205, Russian Federation
jeandakuo@mail.ru✉, https://orcid.org/0000-0002-4084-8829

**Abstract**
This paper introduces a novel Verifiable Random Function (VRF) based on the syndrome decoding problem and Wave signature, resistant to quantum computer attacks. The primary goal of this work is to present a new VRF scheme that demonstrates the applicability of the syndrome decoding problem for constructing cryptographically robust solutions. The paper describes the core VRF algorithms (KeyGen, VRFEval, VRFVerify) and highlights its essential properties: provability, uniqueness, and pseudo-randomness.

**Keywords**
VRF, cryptography, Wave, PRG, syndrome decoding problem

**Acknowledgments**
The work was carried out within the framework of the state assignment (project FSER-2025-0003).

**For citation:** Dakuo Zh-M.N. WaveVRF: post-quantum verifiable random function based on error-correcting codes. *Scientific and Technical Journal of Information Technologies, Mechanics and Optics*, 2025, vol. 25, no. 1, pp. 174–177 (in Russian). doi: 10.17586/2226-1494-2025-25-1-174-177

Проверяемая псевдослучайная функция (Verifiable Random Function, VRF) является важным криптографическим механизмом, который сочетает в себе свойства генерации псевдослучайных чисел и возможность проверки их подлинности. VRF широко применяется в блокчейн-системах [1], протоколах, используемых в WhatsApp [2], и других. В известных научных работах предложены подходы к реализации VRF, основанные на различных криптографических задачах, например, на задаче RSA [3], на эллиптических кривых [4], а также существуют постквантовые VRF, например, на решетках [5], изогениях [6] и хэшах [7].

Однако классические решения уязвимы к атакам квантового компьютера. С развитием квантовых вычислений возникла необходимость в новых криптографических подходах. Несмотря на то, что постквантовые VRF и предлагают защиту от атак квантовых компьютеров, но сталкиваются с проблемами высокой вычислительной сложности и ограниченной масштабируемости.

Предлагаемый подход, основанный на схеме подписи Wave [8], отличается использованием проблемы синдромного декодирования. Также подход имеет удобное масштабирование, так как его параметры зависят от параметров используемого помехоустойчивого кода. В результате предлагаемая VRF устойчива к квантовым атакам.

VRF состоит из трех основных алгоритмов: *KeyGen*() — отвечает за генерацию ключевой пары; *VRFEval*() — вырабатывает псевдослучайное число и доказательство для него из полученного на входе значения и секретного ключа; *VRFVerify*() — проверяет псевдослучайное значение на подлинность, используя открытые ключ и параметры.

Для соответствия критериям VRF предлагаемая схема должна обладать следующими свойствами: полная доказуемость (гарантирует, что вероятность принятия корректного доказательства любым пользователем, владеющим открытым ключом, практически равна единице); уникальная доказуемость (означает, что вероятность принятия поддельного доказательства пренебрежимо мала); псевдослучайность (обеспечивает вероятность того, что злоумышленник отличит результат VRF от случайного значения без знания секретного ключа, будет близка к 1/2).

Рассмотрим предлагаемую схему WaveVRF с использованием обозначений и классов кодов.

Введем краткие обозначения:

1. $\mathbb{F}_q$ — $q$-ичное конечное поле;
2. $\mathbf{a} \in \mathbb{F}_q^n$ — вектор $\mathbf{a} = (a_0, \ldots, a_{n-1}) \in \mathbb{F}_q^n$;
3. $wt(\mathbf{a})_H$ — вес Хэмминга $\mathbf{a} \in \mathbb{F}_q^n$, $wt(\mathbf{a})_H = |\{i, 0 \le i < n \mid a(i) \ne 0\}|$;
4. $\mathbf{M} \in \mathbb{F}_q^{r \times n}$ — матрица $(M_{i,j})_{0 \le i < r,\ 0 \le j < n}$ над полем $\mathbb{F}_q$;
5. $\mathbf{a} \star \mathbf{b}$ — покомпонентное умножение $\mathbf{a} \star \mathbf{b} = (a_i b_i)_{\ 0 \le i < n}$ $\mathbf{a}, \mathbf{b} \in \mathbb{F}_q^n$;
6. $\mathbf{b} \star \mathbf{M}$ — построчное умножение $\mathbf{b} \star \mathbf{M} = (a_j M_{i,j})_{0 \le i < r,\ 0 \le j < n}$;
7. $S_n$ — симметрическая группа перестановок $\{0, \ldots, n-1\}$;
8. $\mathbf{M}^\pi$ — перемешивание столбцов $\mathbf{M}^\pi = (M_{i,\pi(j)})_{0 \le i < r,\ 0 \le j < n}$, $\pi \in S_n$, $M \in \mathbb{F}_q^{r \times n}$.

Некоторые классы кодов, предназначенные для исправления ошибок, за последние 60 лет продемонстрировали свою криптографическую стойкость и надежность в различных приложениях. Линейным троичным $[n, k]_3$-кодом $\mathcal{C}$ называется $k$-размерное подпространство $\mathbb{F}_3^n$ вида:

$$\mathcal{C} = \{\mathbf{y} \in \mathbb{F}_3^n \mid \mathbf{y}\mathbf{H}^T = 0\},$$

где $\mathbf{H}$ — проверочная матрица размерности $n - k$ на $n$; $\mathbf{y}\mathbf{H}^T$ — синдром вектора $\mathbf{y}$.

Предлагаемая схема, как и подпись Wave строится с использованием перемешанных $(U \mid U + V)$-кодов.

**Определение 1 (перемешанный $(U \mid U + V)$-код).** Пусть $n$, $k_U$, $k_V$ — целые числа, где $n$ — четное и $k_U, k_V \le n/2$; $U$ — $[n/2, k_U]_3$-код с порождающей матрицей $\mathbf{G}_U$ и проверочной матрицей $\mathbf{H}_U$; $V$ — $[n/2, k_V]_3$-код с порождающей матрицей $\mathbf{G}_V$ и проверочной матрицей $\mathbf{H}_V$; $\pi$ — перестановка из $S_n$; $\mathbf{b}$, $\mathbf{c}$ — вектора из $\mathbb{F}_3^{n/2}$, где $\mathbf{c}_i \ne 0$ для всех $i \in [0, n/2)$.

Тогда перемешанный $(U \mid U + V)$-код, ассоциированный с $(U, V, \pi, \mathbf{b}, \mathbf{c})$ – $[n, k_U + k_V]_q$-код с порождающей $\mathbf{G}$ и проверочной $\mathbf{H}$ матрицами, определенных следующим образом:

$$\mathbf{G} = \begin{pmatrix} \mathbf{G}_U & \mathbf{c} \star \mathbf{G}_U \\ \mathbf{b} \star \mathbf{G}_V & \mathbf{d} \star \mathbf{G}_V \end{pmatrix}^\pi \text{ и } \mathbf{H} = \begin{pmatrix} \mathbf{d} \star \mathbf{H}_U & -\mathbf{b} \star \mathbf{H}_U \\ -\mathbf{c} \star \mathbf{H}_V & \mathbf{H}_V \end{pmatrix}^\pi,$$

где $\mathbf{d} = 1 + \mathbf{b} \star \mathbf{c}$. Очевидно, что матрица $\mathbf{H}$ может быть приведена к виду $(\mathbf{I}_{n-k} \mid \mathbf{R})$, где $\mathbf{I}$ — единичная матрица размера $n - k$ на $n - k$, а $\mathbf{R}$ матрица $\in \mathbb{F}_3^{(n-k) \times k}$.

Стойкость предлагаемой схемы VRF, подписи Wave и псевдослучайного генератора строится на задаче синдромного декодирования.

**Определение 2 (проблема синдромного декодирования (DP($q$; $n$, $k$, $t$))).** Конечное поле $\mathbb{F}_q$ и целые числа $n$, $k$, $t$ такие что, $n > k > 0$ и $0 < t < n$.

**Дано:** $(\mathbf{H}, \mathbf{s}) \in \mathbb{F}_q^{(n-k) \times n} \times \mathbb{F}_q^{n-k}$, где $wt(\mathbf{e}) = t$ и $\mathbf{e}\mathbf{H}^T = \mathbf{s}$.

**Задача:** при известном $\mathbf{H}$ и $\mathbf{s}$ найти $\mathbf{e} \in \mathbb{F}_q^n$, такое что $wt(\mathbf{e}) = t$ и $\mathbf{e}\mathbf{H}^T = \mathbf{s}$.

Так как используются случайные коды, то для них на DP($q$; $n$, $k$, $t$) накладываются некоторые ограничения по $t$, но проблема все также остается экспоненциально сложной, доказательство в работе [9].

Рассмотрим главную концепцию схемы WaveVRF. Предлагаемая схема в общем повторяет схему подписи Wave. За исключением того, что из входного значения сначала формируется псевдослучайное число, например, при помощи псевдослучайного генератора Фишера–Штерна (PRG), аргументами которого является случайный вектор и проверочная матрица $(U \mid U + V)$-кода [10, 11]. Уровень стойкости $\lambda$ подбирается на основе требований системы. В работе [8] доказано, что существует такой синдром $\mathbf{s}$, для которого есть решение тождества (1) при всех прочих известных параметрах, и он может быть получен при знании $(U \mid U + V)$-кода и перестановки. При построении кода было выбрано поле характеристики равное трем, потому что такая характеристика позволяет получить порождающую и проверочную матрицы статистически неотличимые от случайных. Также выбор такой характеристики поля позволяет попасть в параметры схемы, для которых вероятность неверного декодирования будет $2^{-87}$ [8].

**Параметры предлагаемой системы:**

1. характеристика поля $q = 3$;
2. уровень стойкости $\lambda$;
3. длина кода $n$;
4. вес $w$;
5. размерность $U$ кода: $k_U$;
6. размерность $V$ кода: $k_V$;
7. размерность $(U \mid U + V)$-кода: $k = k_U + k_V$.

**Секретный ключ.** Кортеж $\{U, V, \pi, \mathbf{b}, \mathbf{c}\}$, определяющий перестановочный $(U \mid U + V)$-код.

**Открытый ключ.** Матрица $\mathbf{R} \in \mathbb{F}_3^{(n-k)\times k}$, полученная из проверочной матрицы $\mathbf{H}$ $(U \mid U + V)$-кода.

**VRFEval.** Сначала вырабатывается псевдослучайное число $v := PRG(\mathbf{x}, \mathbf{H})$ где $\mathbf{x} \in \mathbb{F}_3^n$ — передаваемое на вход алгоритма значение. Далее выбирается случайный вектор $\mathbf{salt} \in \mathbb{F}_2^{2\lambda}$ и вычисляется подпись по парадигме «хэшируй и подписывай». Таким образом, при помощи алгоритма подписи Wave ([8], секция 1.1) с параметрами **salt** и $v$ вычисляется вектор $\mathbf{s} \in \mathbb{F}_3^k$ вида:

$$wt_H(\mathbf{s}) + wt_H(Hash(\mathbf{salt}||\mathbf{x}||v) - \mathbf{s}\mathbf{R}^T) = w. \qquad (1)$$

Результатом алгоритма является кортеж $proof = \{\mathbf{salt}, \mathbf{s}\}$ и $v$.

**VRFVerify.** Для проверки используются полученные *proof*, $v$, $\mathbf{x}$, $\mathbf{R}$ и открытые параметры схемы. Все значения подставляются в соотношение (1) и проверяется его корректность.

Полная доказуемость предложенной схемы прямо следует из схемы подписи Wave [8]. Уникальная доказуемость WaveVRF гарантируется использованием детерминированного алгоритма выработки числа $v$ и кортежа *proof*. Псевдослучайность обеспечивается благодаря тому, что в основе WaveVRF — псевдослучайный генератор Фишера–Штерна.

В результате данной работы предложена новая идея схемы построения постквантовой VRF с использованием задачи синдромного декодирования. Благодаря использованию псевдослучайного генератора Фишера–Штерна, WaveVRF сохраняет ключевые криптографические свойства VRF: полную доказуемость, уникальную доказуемость и псевдослучайность. Представленное решение открывает новые возможности для использования VRF в системах, требующих квантовой защищенности. Результаты работы могут быть использованы для дальнейших исследований в области постквантовых VRF.

**Литература**


1. Kiayias A., Russell A., David B., Oliynykov R. Ouroboros: A provably secure proof-of-stake blockchain protocol // Lecture Notes in Computer Science. 2017. V. 10401. P. 357–388. https://doi.org/10.1007/978-3-319-63688-7_12
2. Chagas V., Da-Costa G. WhatsApp and transparency: an analysis on the effects of digital platforms´ opacity in political communication research agendas in Brazil // Profesional de la información. 2023. V. 32. N 2. P. e320223. https://doi.org/10.3145/epi.2023.mar.23
3. Micali S., Rabin M., Vadhan S. Verifiable random functions // Proc. of the 40th Annual Symposium on Foundations of Computer Science (cat. No. 99CB37039). 1999. P. 1–11. https://doi.org/10.1109/SFFCS.1999.814584
4. Dodis Y., Yampolskiy A. A verifiable random function with short proofs and keys // Lecture Notes in Computer Science. 2005. V. 3386. P. 416–431. https://doi.org/10.1007/978-3-540-30580-4_28
5. Esgin M.F., Steinfeld R., Liu D., Ruj S. Efficient hybrid exact/relaxed lattice proofs and applications to rounding and VRFs // Lecture Notes in Computer Science. 2023. V. 14085. P. 484–517. https://doi.org/10.1007/978-3-031-38554-4_16
6. Leroux A. Verifiable random function from the Deuring correspondence and higher dimensional isogenies: Preprint // HAL science ouverte. 2023. https://hal.science/hal-04389904v1
7. Esgin M.F., Ersoy O., Kuchta V., Loss J., Sakzad A., Steinfeld R., Yang X., Zhao R.K., A new look at blockchain leader election: Simple, efficient, sustainable and post-quantum // Proc. of the ACM Asia Conference on Computer and Communications Security. 2023. P. 623–637. https://doi.org/10.1145/3579856.3595792
8. Gasparovic R.F., Apel J.R., Kasischke E.S. An overview of the SAR internal wave signature experiment // Journal of Geophysical Research: Oceans. 1988. V. 93. N C10. P. 12304–12316. https://doi.org/10.1029/jc093ic10p12304
9. Thomas Debris-Alazard. Post-Quantum Cryptography - Codes; Lecture 2: Random Codes [Электронный ресурс] URL: https://tdalazard.io/lecture2.pdf (дата обращения: 28.10.2024).
10. Fischer J.B., Stern J. An efficient pseudo-random generator provably as secure as syndrome decoding // Lecture Notes in Computer Science. 1996. V. 1070. P. 245–255. https://doi.org/10.1007/3-540-68339-9_22
11. Kuznetsov A., Kiian A., Smirnov O., Cherep A., Kanabekova M., Chepurko I. Testing of code-based pseudorandom number generators for post-quantum application // Proc. of the 2020 IEEE 11th


**References**


1. Kiayias A., Russell A., David B., Oliynykov R. Ouroboros: A provably secure proof-of-stake blockchain protocol. *Lecture Notes in Computer Science*, 2017, vol. 10401, pp. 357–388. https://doi.org/10.1007/978-3-319-63688-7_12
2. Chagas V., Da-Costa G. WhatsApp and transparency: an analysis on the effects of digital platforms´ opacity in political communication research agendas in Brazil. *Profesional de la información*, 2023, vol. 32, no. 2, pp. e320223. https://doi.org/10.3145/epi.2023.mar.23
3. Micali S., Rabin M., Vadhan S. Verifiable random functions. *Proc. of the 40th Annual Symposium on Foundations of Computer Science (cat. No. 99CB37039)*, 1999, pp. 1–11. https://doi.org/10.1109/SFFCS.1999.814584
4. Dodis Y., Yampolskiy A. A verifiable random function with short proofs and keys. *Lecture Notes in Computer Science*, 2005, vol. 3386, pp. 416–431. https://doi.org/10.1007/978-3-540-30580-4_28
5. Esgin M.F., Steinfeld R., Liu D., Ruj S. Efficient hybrid exact/relaxed lattice proofs and applications to rounding and VRFs. *Lecture Notes in Computer Science*, 2023, vol. 14085, pp. 484–517. https://doi.org/10.1007/978-3-031-38554-4_16
6. Leroux A. Verifiable random function from the Deuring correspondence and higher dimensional isogenies: Preprint. *HAL science ouverte*, 2023, https://hal.science/hal-04389904v1
7. Esgin M.F., Ersoy O., Kuchta V., Loss J., Sakzad A., Steinfeld R., Yang X., Zhao R.K., A new look at blockchain leader election: Simple, efficient, sustainable and post-quantum. *Proc. of the ACM Asia Conference on Computer and Communications Security*, 2023, pp. 623–637. https://doi.org/10.1145/3579856.3595792
8. Gasparovic R.F., Apel J.R., Kasischke E.S. An overview of the SAR internal wave signature experiment. *Journal of Geophysical Research: Oceans*, 1988, vol. 93, no. C10, pp. 12304–12316. https://doi.org/10.1029/jc093ic10p12304
9. Thomas Debris-Alazard. *Post-Quantum Cryptography — Codes; Lecture 2: Random Codes*. Available at: https://tdalazard.io/lecture2.pdf (accessed: 28.10.2024).
10. Fischer J.B., Stern J. An efficient pseudo-random generator provably as secure as syndrome decoding. *Lecture Notes in Computer Science*, 1996, vol. 1070, pp. 245–255. https://doi.org/10.1007/3-540-68339-9_22
11. Kuznetsov A., Kiian A., Smirnov O., Cherep A., Kanabekova M., Chepurko I. Testing of code-based pseudorandom number generators for post-quantum application. *Proc. of the 2020 IEEE 11th*

International conference on dependable systems, services and technologies (DESSERT). 2020. P. 172–177. https://doi.org/10.1109/dessert50317.2020.9125045

*International conference on dependable systems, services and technologies (DESSERT)*, 2020, pp. 172–177. https://doi.org/10.1109/dessert50317.2020.9125045

**Автор**

**Дакуо Жан-Мишель Никодэмович** — аспирант, Университет ИТМО, Санкт-Петербург, 197101, Российская Федерация; ассистент, Санкт-Петербургский государственный университет аэрокосмического приборостроения, Санкт-Петербург, 190000, Российская Федерация; криптограф-исследователь, КуАпп, Москва, 121205, Российская Федерация, SC 57884002100, https://orcid.org/0000-0002-4084-8829, jeandakuo@mail.ru

**Author**

**Zhan-Mishel N. Dakuo** — PhD Student, ITMO University, Saint Petersburg, 197101, Russian Federation; Assistant, Saint Petersburg State University of Aerospace Instrumentation, Saint Petersburg, 190000, Russian Federation; Cryptographer Researcher, QApp, Moscow, 121205, Russian Federation, SC 57884002100, https://orcid.org/0000-0002-4084-8829, jeandakuo@mail.ru

*Статья поступила в редакцию 09.01.2025*
*Одобрена после рецензирования 24.01.2025*
*Принята к печати 31.01.2025*

*Received 09.01.2025*
*Approved after reviewing 24.01.2025*
*Accepted 31.01.2025*