# О криптосистеме Шора-Ривеста в поле с оптимальным нормальным базисом второго типа

С. Б. Гашков*, А. А. Сесюкалов†, А. Б. Фролов§

Рассматривается модификация криптосистемы Шора—Ривеста, отличающаяся тем, что вычисления в случайном степенном базисе имитируются в оптимальном нормальном базисе второго типа с ускорением при использовании быстрых операции умножения и возведения в степень.

**Ключевые слова:** криптосистема Шора-Ривеста, оптимальный нормальный базис второго типа, быстрое умножение.

Целью работы является обоснование возможности ускорения вычислений в криптосистеме Б. Шора и Р.Л. Ривеста [1] при ее реализации в поле $GF(p^n)$, имеющем оптимальный нормальный базис второго типа (ОНБ 2) и гладкую мультипликативную группу при простых $p$ и $n$.

Предлагается следующая модификация указанной криптосистемы в таком поле.

1. Выбрать случайный элемент $t', t' \notin GF(p)$, поля $GF(p^n)$ и вычислить в ОНБ 2 его минимальный многочлен $f'(X) = \Pi_{i=0}^{n-1}(X - t'^{p^i})$. Вычислить $n \times n$ матрицу $A$ перехода из ССБ в ОНБ 2. Ее строки— элементы $1, t', t'^2, \ldots, t'^{n-1}$ в ОНБ 2. Для обратного перехода вычислить матрицу $B = A^{-1}$.
2. Выбрать случайно генератор $g'$ поля $GF(p^n)$ в ОНБ 2 .
3. Вычислить набор $a$ дискретных логарифмов $a_j = \log_{g'}(t' + j), j =$

*Гашков Сергей Борисович* — проф. каф. дискретной математики мех.-мат. ф-та МГУ имени Ломоносова (Москва), e-mail: sbgashkov@gmail.com, ORCID: 0000-0003-3406-0063.

*Gashkov Sergey Borisovich* — Doctor of Physical and Mathematical Sciences, Lomonosov Moscow State University, Faculty of Mechanics and Mathematics, Chair of Discrete Mathematics.

†*Сесюкалов Александр Алексеевич* — студент магистратуры НИУ МЭИ (Москва), e-mail: sesiukalovaa@mpei.ru, ORCID: 0009-0002-9770-3505.

*Sesiukalov Aleksandr Alekseevich* — Master's student of NRU MPEI.

§*Фролов Александр Борисович* — проф. каф. математического и компьютерного моделирования НИУ МЭИ (Москва), e-mail: frolovab@mpei.ru, ORCID: 0000-0002-2022-4533.

*Frolov Aleksandr Borisovich* — Doctor of Technical Sciences, professor, NRU MPEI, Institute of Information Technologies and Computer Science, Chair of Mathematical and Computer Modeling.

Опубликовано на условиях лицензии CC-BY 4.0
Published under CC-BY 4.0

$0, \ldots, p-1$.
4. Случайной перестановкой $\pi$ элементов набора $a$ получить набор $b$.
5. Прибавлением к элементам набора $b$ единого случайного числа $d$ получить «зашумленный» набор $c$.
6. Объявить открытый ключ $c, p, n$.
7. Сохранить секретный ключ $t'\, g,' \pi, d$.
8. Открытый текст: бинарная строка $x = (x_0, \ldots, x_i, \ldots, x_{p-1})$ длины $p$ и веса $n$.
9. Зашифрование: $s = \sum_{i=0}^{p-1} x_i c_i \mod (p^n - 1)$.
10. Расшифрование :
— вычислить $s' = s - nd \mod (p^n - 1)$,
— вычислить $q'(t) = g'^{s'}$,
— умножением на матрицу $B$ получить $q(t) = q'(t)B$,
— получить $f(X)$ как представление $f'(X)$ в ССБ и вычислить многочлен $F(X) = X^n + (r(X) + q(X))$, где $r(X) = f(X) - X^n$,
— найти, например, по схеме Горнера, все его корни,
— перестановкой $\pi^{-1}$ корней многочлена $F(X)$ получить номера позиций единичных элементов в открытом тексте.

В оригнальном варианте криптосистемы п.1 соответствует выбор корня $t$ и случайного многочлена $f(t)$ в ССБ. П.п. 2—10 соответсвуют такие же действия, но выполняемяе в ССБ (с заменой обозначений $t', g', q'$) обозначениями $t, g, q$.

Это позволяет по умолчанию выбрать примитивный элемент $g$ в ССБ путем генерации примитивного элемента $g'$ поля в ОНБ 2 как образа $g = g'B$ элемента $g'$ и далее вычисления в ССБ этого поля воспроизводить (имитировать) в ОНБ 2 с возвращением полученного результата в ССБ. Ускорение достигается за счет применения операции умножения в ОНБ 2, более быстрой по сравнению с умножением ССБ (см. таблицу 1), и «бесплатного» возведения в степень $p^d$, $d \geq 1$.

По таблице 2 можно судить о существенном превосходстве имплементации в поле $GF(10333^{11})$ с использованием ОНБ 2 по сравнению с имплементацией непосредственно в ССБ как по числу операций, так и по времени исполнения. Поле $GF(10333^{11})$ имеет ОНБ 2 и указано в [2] как поле, удовлетворяющее известным пяти условиям безопасности.

Числа операций получены непосредственным подсчетом. Для измерения времени используются функции стандартной библиотеки $C++$ или библиотека time в Python.

Таблица 1: Числа операций в $Z_{10333}$ при умножении в $GF(10333^{11})$, Python, PU@3.00GHz

| Базис | Время | умножений | сложений | всего |
|---|---|---|---|---|
| ОНБ 2 | 0.247 мс. | 66 | 266 | 332 |
| ССБ | 1.044 мс. | 225 | 235 | 460 |

Таблица 2: Вычислительные затраты на этапы логарифмирования (Л), получения ключей, зашифрования (З) и расшифрования (Р) в поле $GF(10333^{11})$, C++, NVIDIA GeForce RTX 4060 Laptop GPU

| | Базис | время, | умножений | всего |
|---|---|---|---|---|
| Л | ОНБ 2 | 190.9 с. | 967774374820 | 4868197567777 |
| З | | 0,28мкс. | 10344 | 20688 |
| Р | | 2000мкс. | 149387568 | 668743673 |
| Л | ССБ | 1230.1 | 3377540542049 | 7484865560846 |
| З | | 3,65мкс. | 10344 | 20688 |
| Р | | 7300 мкс. | 506911437 | 1194964258 |

## Список литературы

[1] Chor B., Rivest R.L., "A Knapsack-Type Public Key Cryptosystem Based on Arithmetic in Finite Fields.", *IEEE Transactions on information theory*, **34**:5 (1988), 901–909.

[2] L. Hernández Encinas , J. Muñoz Masqué, A. Queiruga Dios., "Safer parameters for the Chor–Rivest cryptosystem.", *Computers and Mathematics with Applications*, **56** (2008), 2883–2886.

Статья поступила 10 октября 2026 г.

### On the Chor-Rivest Cryptosystem in a Field with an Optimal Normal Basis of the Second Type

S. B. Gashkov, A. A. Sesiukalov, A. B. Frolov

A modification of the Shor–Rivest cryptosystem is considered, distinguished by the fact that computations in a random power basis are simulated using an optimal normal basis of type II, with acceleration achieved through fast multiplication and exponentiation.

**Keywords:** Shor-Rivest cryptosystem, optimal normal basis of the second type, fast multiplication, raising to a power equal to the field characteristic..

## References

[1] Chor B., Rivest R.L., “A Knapsack-Type Public Key Cryptosystem Based on Arithmetic in Finite Fields.”, *IEEE Transactions on information theory*, **34**:5 (1988), 901–909.

[2] L. Hernández Encinas , J. Muñoz Masqué, A. Queiruga Dios., “Safer parameters for the Chor–Rivest cryptosystem.”, *Computers and Mathematics with Applications*, **56** (2008), 2883–2886.

Received on October 10, 2026