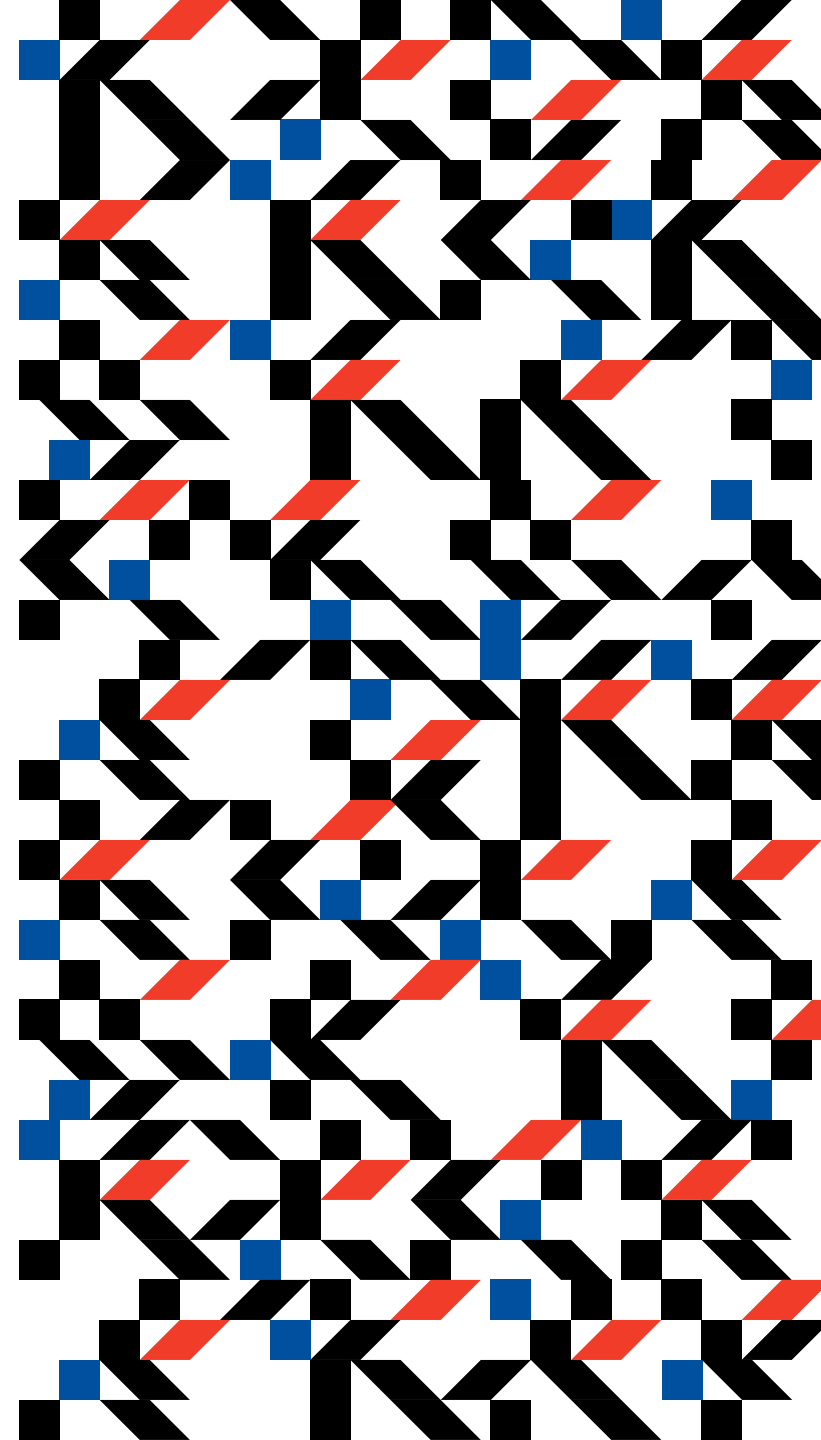


Кто быстрее: «Магма» или «Рамен-К»?

Щербаков Дмитрий Андреевич

Степин Дмитрий Дмитриевич



Если не ГОСТ, но очень хочется: «ПРАПОР-К» и «Рамен-К» — новые семейства (низкоресурсных) блочных шифров [1]

«Рамен-К»:

- ✓ размер блока 128/192/256 бит;
- ✓ ARX подстановка типа «Альзет»;
- ✓ простое линейное преобразование;
- ✓ const-time реализация с помощью 32-битных и 64-битных инструкций общего назначения;
- ✓ применимость SIMD обработки.



«Рамен-К»

Скорость референсной реализации — 226 МБ/с на AMD Ryzen 7 7800X3D.

[1] Матюхин Д.В. «Если не ГОСТ, но очень хочется: «ПРАПОР-К» и «Рамен-К» — новые семейства (низкоресурсных) блочных шифров», РусКрипто'2026

Наш взгляд на производительность

Алгоритм	Реализация	Скорость в режиме ECB в ГБ/с
Рамен-128K	Референсная [1]	~0.2
Кузнечик	Табличная (LUT 64 КБ) [2]	~0.4
Магма	SIMD (AVX-512) [3]	~3
Рамен-128K	SIMD (AVX-512) [3]	~3
AES-256-ECB	AES-NI (OpenSSL)	~11

[1] Матюхин Д.В. «Если не ГОСТ, но очень хочется: «ПРАПОР-К» и «Рамен-К» — новые семейства (низкоресурсных) блочных шифров», РусКрипто'2026. AMD Ryzen 7 7800X3D

[2] A. S. Rybkin, "On software implementation of Kuznyechik on Intel CPUs", Матем. вопр. Криптогр., 9:2 (2018), 117–127. Intel Core i7-6700

[3] Эта работа. AMD Ryzen 9 9950X3D



Спасибо
за внимание

