Перспективы аппаратного ускорения криптографии в процессорах архитектуры «Эльбрус»

Советов Петр Николаевич,
АО «МЦСТ», РТУ МИРЭА

РусКрипто’2021

эльбрус

Тесты программных реализаций криптопримитивов

Результаты для **Эльбрус-8СВ**:

- 1550 МГц,
- Си-код без учета целевой архитектуры,
- последовательные преобразования,
- скалярные операции.

Реализация алгоритма	Пропускная способность (Мбайт/с)	Время преобразования одного блока (≈ тактов)
«Кузнечик»	97	256
«Магма»	53	234
«Стрибог»	81	1124
AES	140	**177**
ChaCha20	342	352
SHA256	54	**1844**

(использование параллельных режимов/SIMD-операций позволит добиться некоторого ускорения)

Процессор с аппаратным ускорением криптографии:

AES NI (**Intel**) ≈ **37** тактов (×5)
VAES NI CTR (**Intel**) ≈ **2.56** тактов (×69)
SHA NI (**AMD**) ≈ **115** тактов (×16)

Есть необходимость в аппаратной поддержке криптографии для новых «Эльбрусов»

https://w3.lasca.ic.unicamp.br/media/publications/p9-faz-hernandez.pdf https://eprint.iacr.org/2018/392.pdf

Аппаратная поддержка криптопримитивов

Преимущества:

- **производительность,**
- **энергоэффективность,**
- **возможность защиты от атак по побочным каналам.**

Масштаб поддержки	**Вид реализации**	**Степень программирумости**
Связка базовых операций	Специализированная команда в составе общего АЛУ	Фиксированная схема вычислений
Раунд или иной крупный шаг вычисления криптопримитива	Специализированный функциональный узел	Конфигурация основных параметров
Полная реализация криптопримитива	Сопроцессор	Микропрограмма

Выбор целей для аппаратного ускорения

Область применения	Важнейшие алгоритмы	Базовые операции	Приоритет аппаратной реализации
Симметричные шифры и хэш-функции, AEAD-режимы	«Кузнечик», «Магма», «Стрибог», MGM, AES, ChaCha20, SHA-2, GCM, Poly1305	Легковесные целочисленные, побитовые операции, обращения к таблицам, умножение в поле GF(2^n)	Высокий
Схемы выработки общего ключа с аутентификацией, формирование и проверка электронной цифровой подписи	«Эхинацея-2», «Эхинацея-3», «Лимонник-3», ГОСТ 34.10-2018, ECDH, ECDSA, EdDSA	Операции длинной арифметики	Средний
Постквантовая криптография и гомоморфное шифрование	Подходы, основанные на изогениях (SIDH), решетках и другие	Операции длинной арифметики	Низкий

Криптографически стойкий ГПСЧ с аппаратным источником энтропии

Аппаратная поддержка криптографии в архитектуре x86-64

Алгоритм	Команда	Аппаратное ускорение
AES	AESENC, AESENCLAST, AESDEC, AESDECLAST, AESKEYGENASSIST, AESIMC, VAESENC, VAESENCLAST, VAESDEC, VAESDECLAST	Вычисление раунда, конвейеризованные вычисления, до 4 параллельных преобразований в SIMD-режиме
	GF2P8AFFINEINVQB, GF2P8AFFINEQB, GF2P8MULB	Связка базовых операций (вычисления в $GF(2^8)$)
SHA-1, SHA-256	SHA1RNDS4, SHA1NEXTE, SHA1MSG1, SHA1MSG2, SHA256RNDS2, SHA256MSG1, SHA256MSG2	Вычисление 2 раундов
Режим **GCM**, вычисления в $GF(2^n)$	PCLMULQDQ, VPCLMULQDQ	До 4 параллельных умножений без переноса 64x64 в SIMD-режиме
Алгоритмы с использованием длинной арифметики	VPMADD52LUQ, VPMADD52HUQ	Умножение массивов 52-битных целых с добавлением результатов к 64-битным аккумуляторам

VPTERNLOG — произвольная булева функция от 3 аргументов над 512-битными векторами (хэш-функции, техника bitslicing)

https://newsroom.intel.com/articles/crypto-acceleration-enabling-path-future-computing https://eprint.iacr.org/2018/392.pdf https://eprint.iacr.org/2018/335.pdf

Аппаратная поддержка криптографии в архитектуре POWER

Алгоритм	Команда	Аппаратное ускорение
AES	vcipher, vcipherlast, vncipher, vncipherlast	Вычисление раунда, до 4 параллельных преобразований
	vsbox	Связка базовых операций (подстановка)
SHA-256, SHA-512	vshasigmaw, vshasigmad	Связка базовых операций (функции Sigma и Sum)
Режим **GCM**, вычисления над $GF(2^n)$	vpmsum[b,h,w,d]	Полиномиальное умножение-сложение с разрядностью до 64x64

https://regmedia.co.uk/2020/08/17/ibm_power10_summary.pdf

Аппаратная поддержка криптографии в архитектуре ARM

ARM

Алгоритм	Команда	Аппаратное ускорение
AES, SM4	AESD, AESE, SM4E, SM4EKEY	Вычисление раунда
	AESIMC, AESMC	Связка базовых операций
SHA-1, **SHA-256,** **SHA-512**, SM3	SHA1C, SHA1H, SHA1M, SHA1P, SHA1SU0, SHA1SU1, SHA256H, SHA256H2, SHA256SU0, SHA256SU1, SHA512H, SHA512H2, SHA512SU0, SHA512SU1, SM3SS1, SM3TT1A, SM3TT1B, SM3TT2A, SM3TT2B, SM3PARTW1, SM3PARTW2	Связка базовых операций
Режим **GCM** и другие вычисления над GF(2^n)	PMUL, PMULL, MULL2	Полиномиальное умножение с разрядностью до 64x64

EOR3 — X128 xor Y128 xor Z128,
RAX1 — X128 xor (rol(Y128[127:64], 1):rol(Y128[63:0], 1)),
XAR — ror((X128 xor Y128)[128:64], N):ror((X128 xor Y128)[63:0], M),
BCAX — X128 xor (Y128 and not(Z128)).

https://developer.arm.com/documentation/ddi0487/latest/

Аппаратная поддержка криптографии в архитектуре RISC-V

Алгоритм	Команда	Аппаратное ускорение
AES	aes64ks1i, aes64ks2, aes64im, aes64esm, aes64es, aes64dsm, aes64ds	Вычисление раунда
SM4	sm4ed, sm4ks	Вычисление раунда
SHA-256, SHA-512, SM3	sha256sig0, sha256sig1, sha256sum0, sha256sum1, sha512sig0, sha512sig1, sha512sum0, sha512sum1, sm3p1, sm3p0	Связка базовых операций
Режим **GCM** и другие вычисления над GF(2^n)	clmul, clmulh	Полиномиальное умножение с разрядностью до 64x64

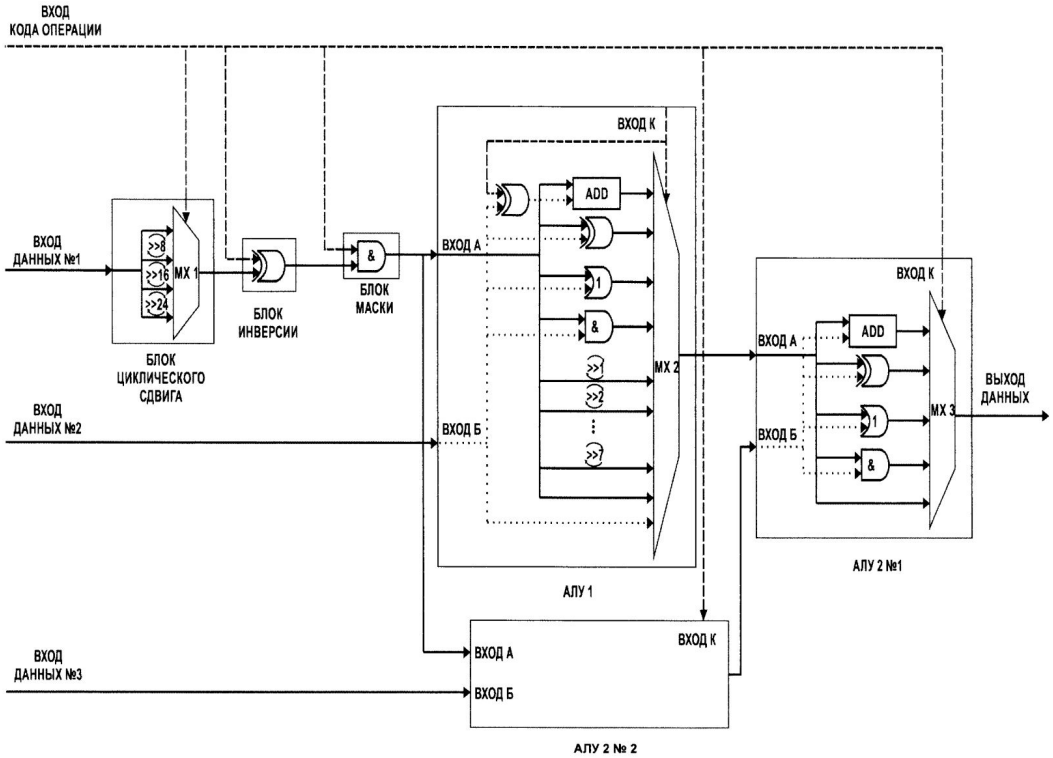
xperm — реализация произвольных 4/8-битных таблиц
(8 параллельных замен по вектору из 8 8-битных значений)

https://github.com/riscv/riscv-crypto/releases/download/v0.9.0-scalar/riscv-crypto-spec-v0.9.0-scalar.pdf

Специализированное АЛУ (2016)

Особенности:

- вычисление дерева выражений,
- реализация связок операций из области симметричной криптографии.

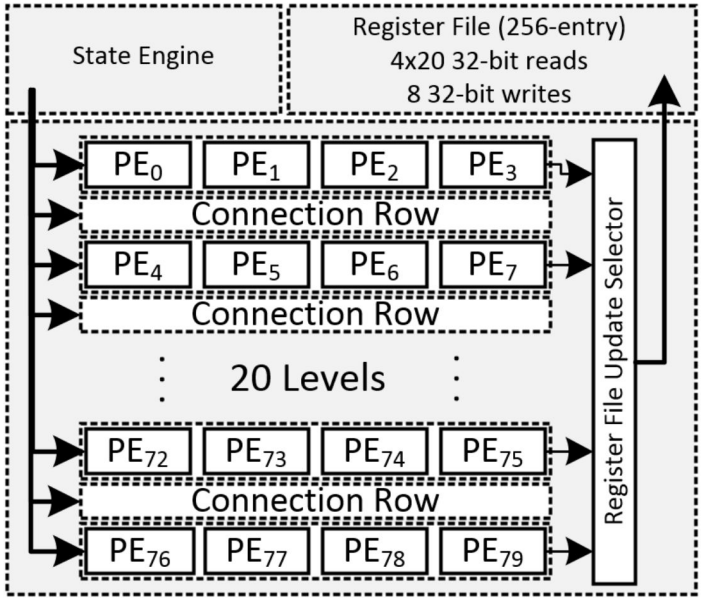


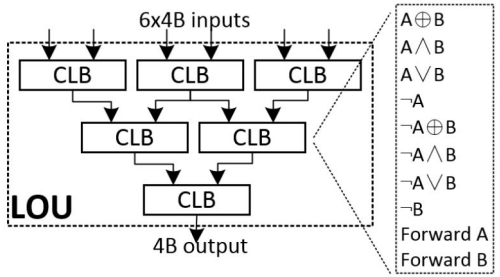
С. Г. Елизаров, Д. С. Марков, П. Н. Советов. Патент на изобретение № 2681702. Арифметико-логическое устройство и способ преобразования данных с использованием такого устройства

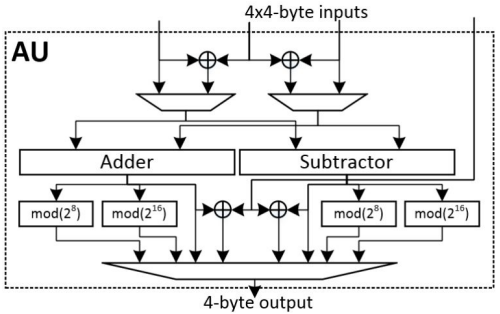
Криптопроцессор Cryptoraptor (2014)

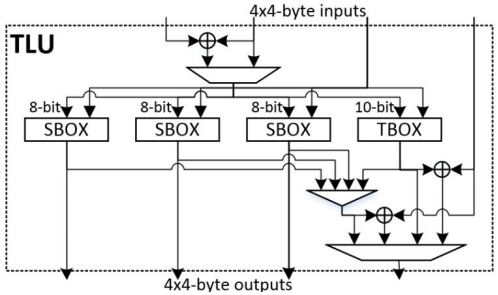
Особенности:

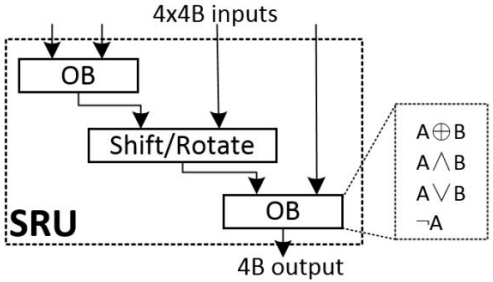
- крупноблочная реконфигурируемая структура,
- реализация алгоритмов из области симметричной криптографии.









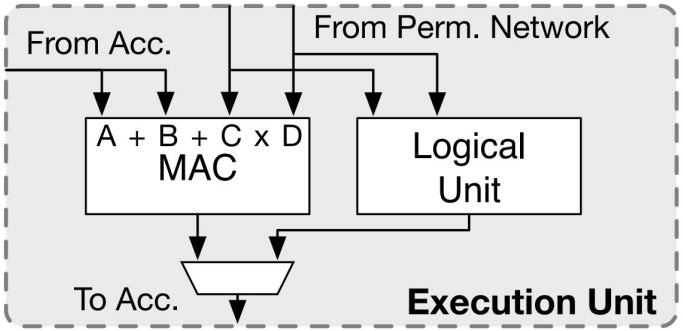


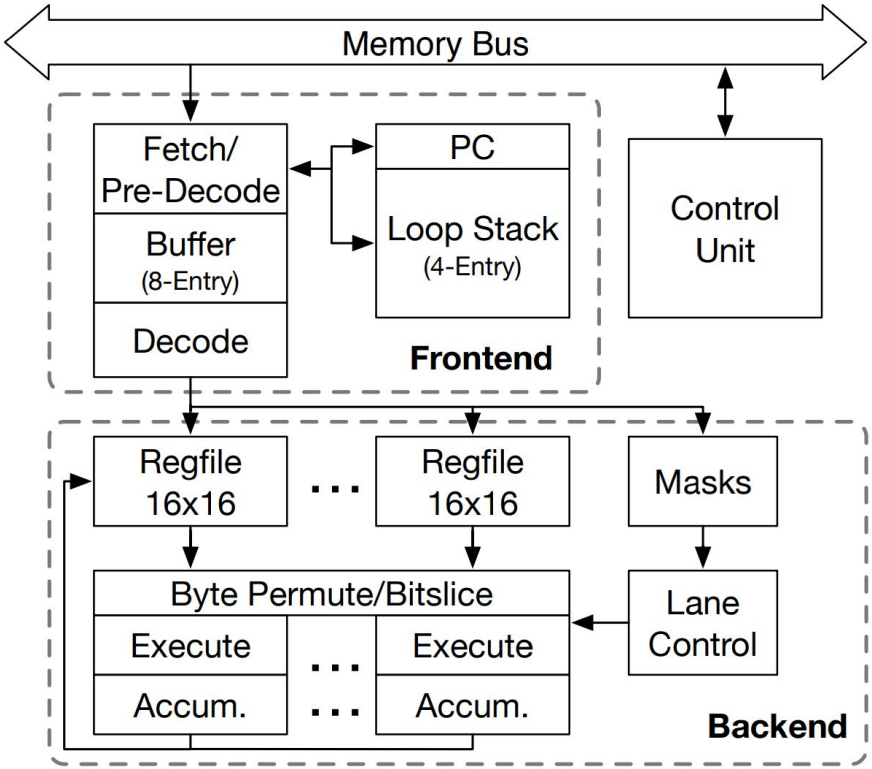
https://repositories.lib.utexas.edu/bitstream/handle/2152/28267/SAYILAR-THESIS-2014.pdf

Криптопроцессор Falcon (2019)

Особенности:

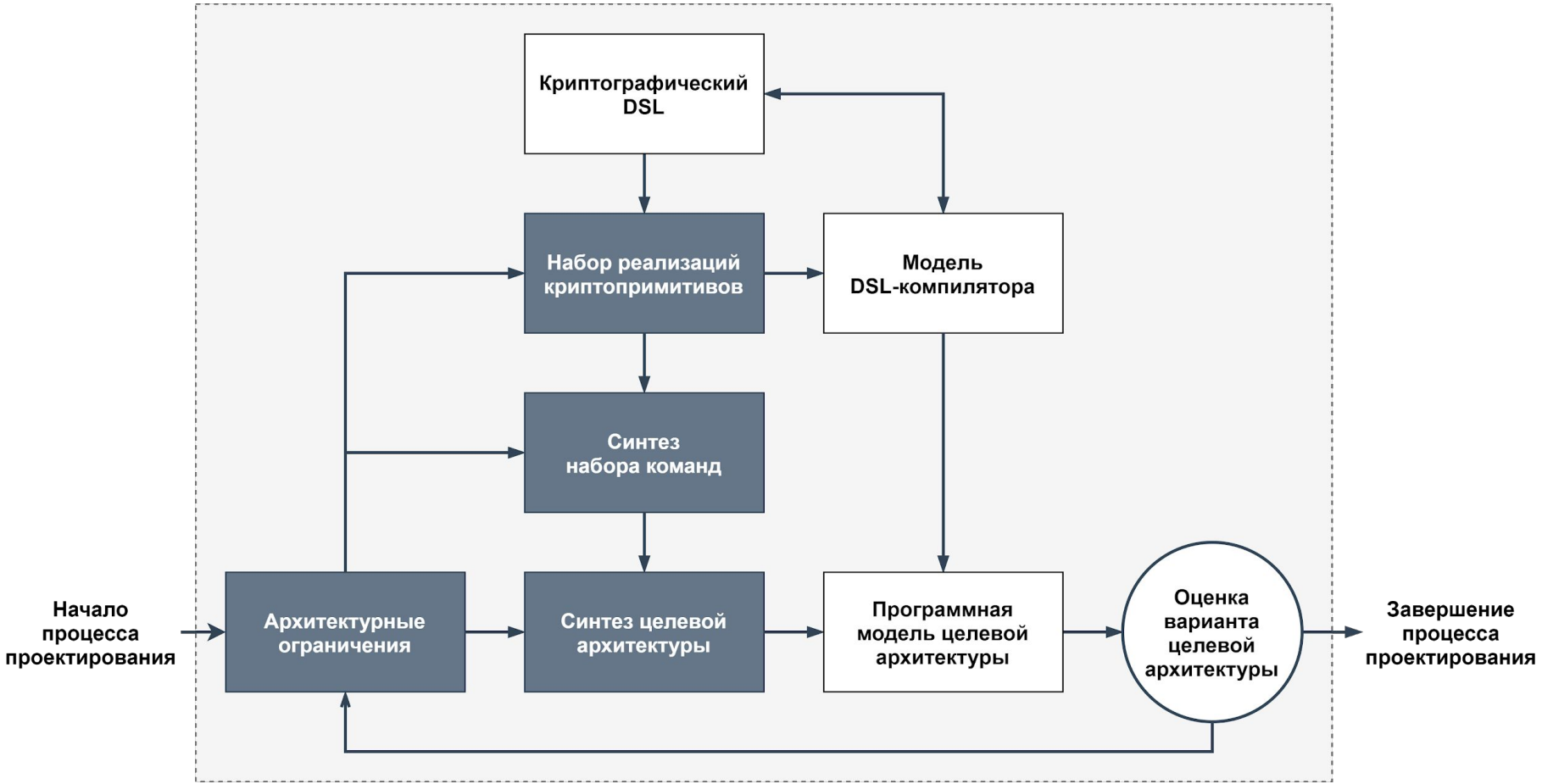
- SIMD-процессор с 256-битными регистрами,
- поддержка перестановок и техники bitslicing,
- параллельное 16-битное умножение с накоплением, поддержка длинного умножения в столбик,
- реализация алгоритмов симметричной и асимметричной криптографии.





https://sing.stanford.edu/site/publications/kiningham19falcon.pdf

Методика совместного проектирования

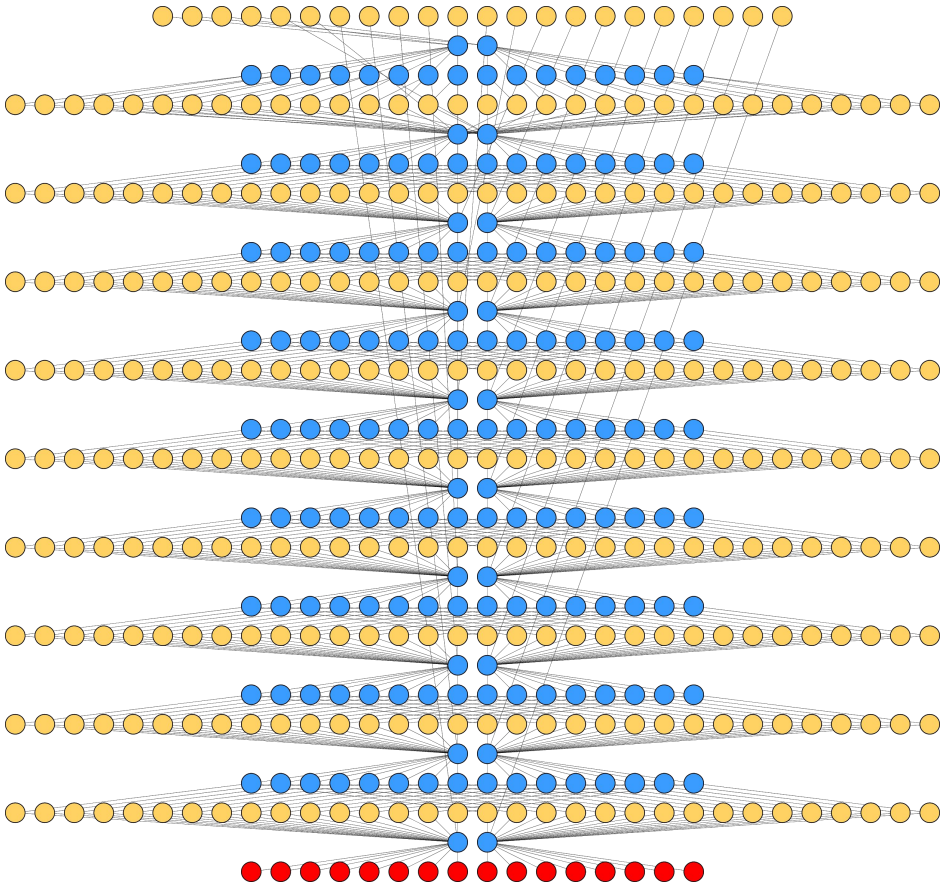


Ярусно-параллельная форма реализации «Кузнечика»

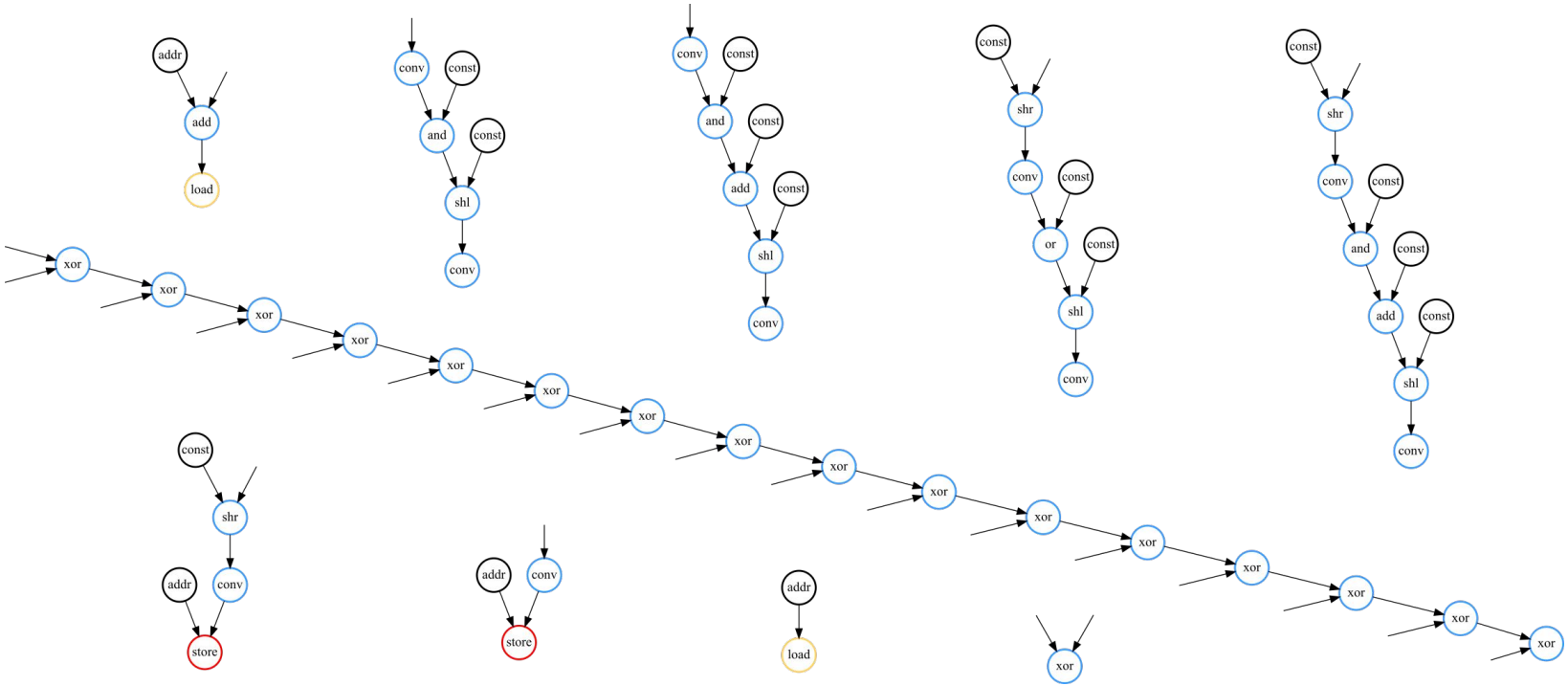
Результат синтеза набора команд для реализации «Кузнечика» с использованием таблицы размером 64 Кбайт:

- число синтезированных команд: 10,
- число ярусов: 30,
- макс. ширина яруса: 32.

Это нереалистичный вариант, но он представляет собой точку в пространстве поиска возможных вариантов целевой архитектуры.



Графы синтезированных команд реализации «Кузнечика»



Выводы

1. В аппаратной поддержке нуждаются и **международные**, и **российские** алгоритмы криптографии.
2. В первую очередь аппаратное ускорение требуется для алгоритмов **симметричной криптографии**.
3. Важнейшие криптопримитивы целесообразно аппаратно ускорить на уровне **раундов**. Для поддержки широкого набора криптопримитивов необходимо рассмотреть возможность реализации универсальных команд поддержки криптографии или программируемого **криптопроцессора**.
4. Многие популярные реализации криптопримитивов подразумевают исполнение на процессоре общего назначения и могут потребовать серьезной **переработки для аппаратной реализации** (это касается, например, различий в реализации блока подстановок).
5. Целесообразно применять методику **совместного проектирования**, а также ориентироваться на 64-битный тракт данных и поддержку параллельных режимов шифров.

Благодарю за внимание!