РОССИЙСКИЙ ФОРУМ
МИКРОЭЛЕКТРОНИКА 2026

27 сентября –
3 октября 2026

ФЕДЕРАЛЬНАЯ
ТЕРРИТОРИЯ
«СИРИУС»

трамплин
электроникс

иртыш

MALT
SYSTEM

Создание модуля доверенной загрузки в процессоре Иртыш

Сергей Елизаров, научный руководитель дизайн центра Мальт Систем, к.ф.-м.н

Василий Воробушков, директор по развитию Трамплин Электроникс

План доклада

В докладе рассмотрим разработку криптографической подсистемы процессора «Иртыш», обеспечивающей аппаратный корень доверия и контроль целостности загрузчиков криптографического ядра и UEFI основного вычислительного ядра, а также прозрачное шифрование данных в реальном времени с поддержкой российских криптографических стандартов («Кузнечик», «Магма», «Стрибог», ГОСТ Р 34.10-2012).

Обсудим архитектурные решения - отделение криптоблока от основного процессора с использованием интерфейсов DMA и Mailbox, реализация на базе специализированного процессора с вычислительными ядрами, допускающего загрузку различных алгоритмов.

Представим комплект разрабатываемого системного и прикладного ПО (микрокод, загрузчики, драйвер для Linux, эмулятор QEMU) и текущий статус интеграции криптографической подсистемы в процессор «Иртыш».

Назначение криптографической подсистемы

РОССИЙСКИЙ ФОРУМ
МИКРОЭЛЕКТРОНИКА 2026

- Аппаратный корень доверия (Root of Trust) обеспечивающий контроль целостности загрузчиков криптографического ядра и UEFI основного вычислительного ядра.
- Защита данных в реальном времени и шифрование потоков информации.
- Аппаратное ускорение различных приложений, требующих выполнения криптопреобразований.

Категории криптографических алгоритмов

РОССИЙСКИЙ ФОРУМ МИКРОЭЛЕКТРОНИКА 2026

Симметричное блочное шифрование (Symmetric Ciphers):

- **Назначение:** быстрое шифрование больших объемов данных (файловые системы, жесткие диски, сетевой трафик TLS/HTTPS, VPN, SSH)
- **Алгоритмы:** AES, ChaCha20, Twofish, SM4, Кузнечик, Магма

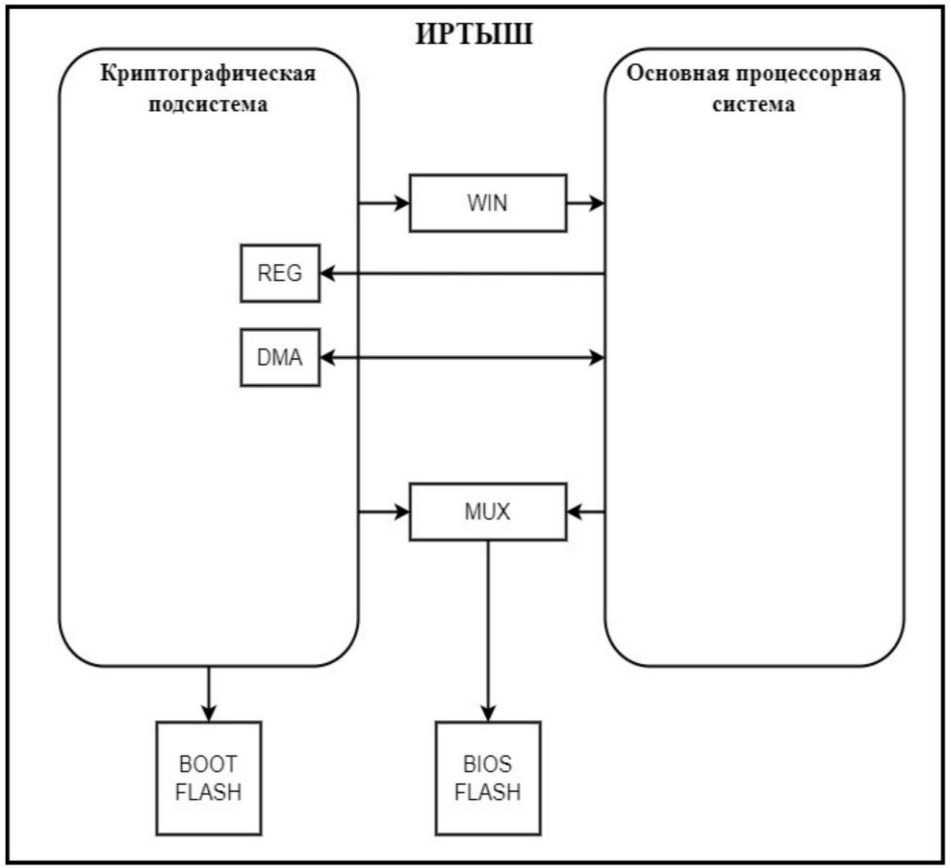
Криптографические хэш-функции (Cryptographic Hash Functions):

- **Назначение:** контроль целостности данных, контроль подлинности файлов в режиме доверенной загрузки, защита паролей, часть механизма проверки электронной цифровой подписи
- **Алгоритмы:** SHA-256, BLAKE3, SM3, Стрибог

Асимметричное шифрование (Asymmetric Ciphers):

- **Назначение:** аутентификация устройств, проверка подлинности загрузчиков BIOS/UEFI (аппаратный корень доверия), электронная цифровая подпись данных
- **Алгоритмы:** RSA, ECDSA/ECDH, ML-KEM/ML-DSA, SM2, ГОСТ ЭЦП

Процессор Иртыш с криптографической подсистемой



Структурная схема

Криптографическая подсистема отделена от основной процессорной системы.

Доступ основного процессора в криптографическую подсистему ограничен.

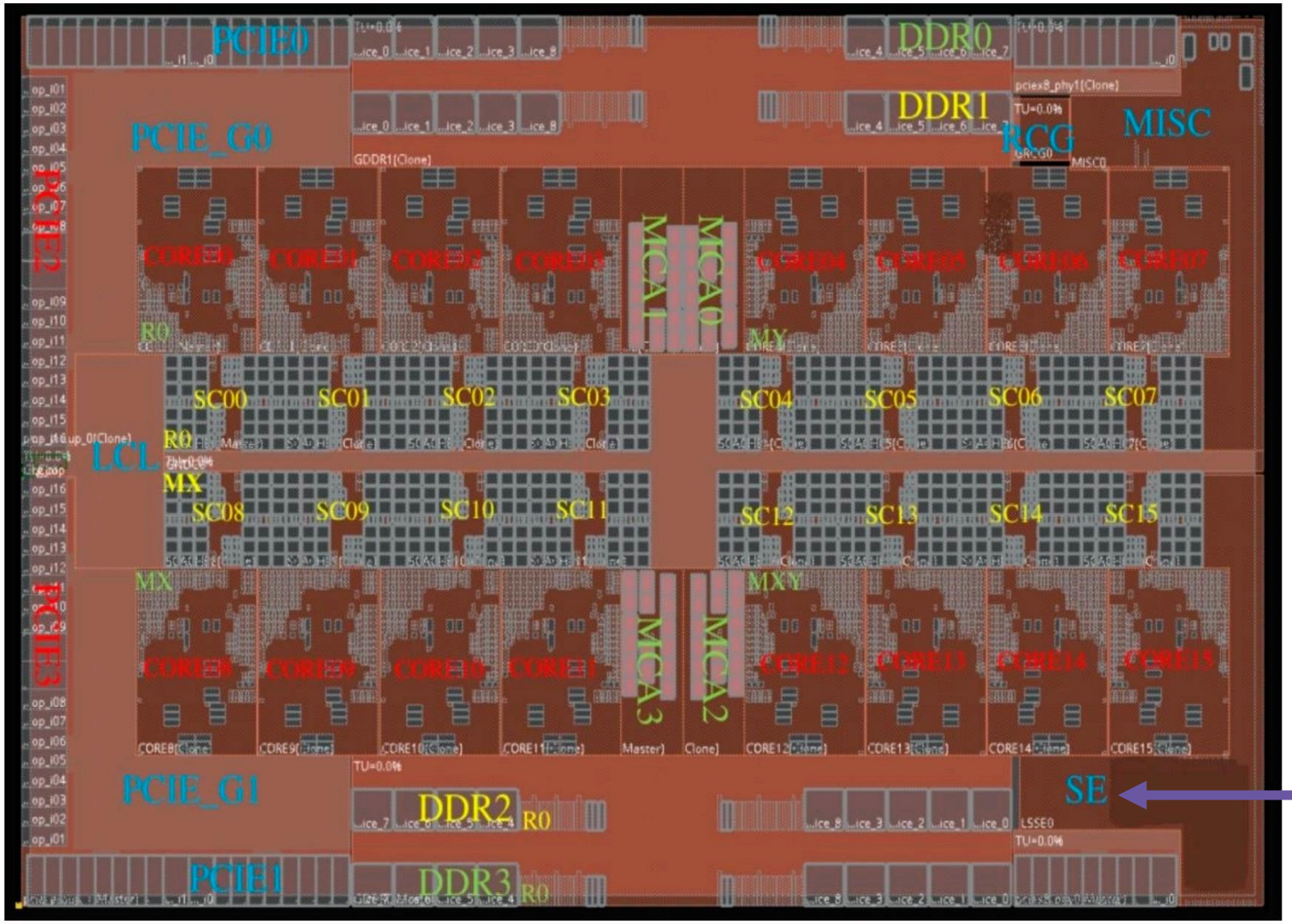
Обмен данными осуществляется посредством специальных механизмов (интерфейсов и модулей).

REG – регистры

WIN – интерфейс настраиваемых адресных окон доступа криптографической подсистемы к внешним устройствам

DMA – многоканальный контроллер прямого доступа к памяти; обеспечивает загрузку и выгрузку данных для блоков криптографии

Топология кристалла процессора Иртыш



Топология процессора

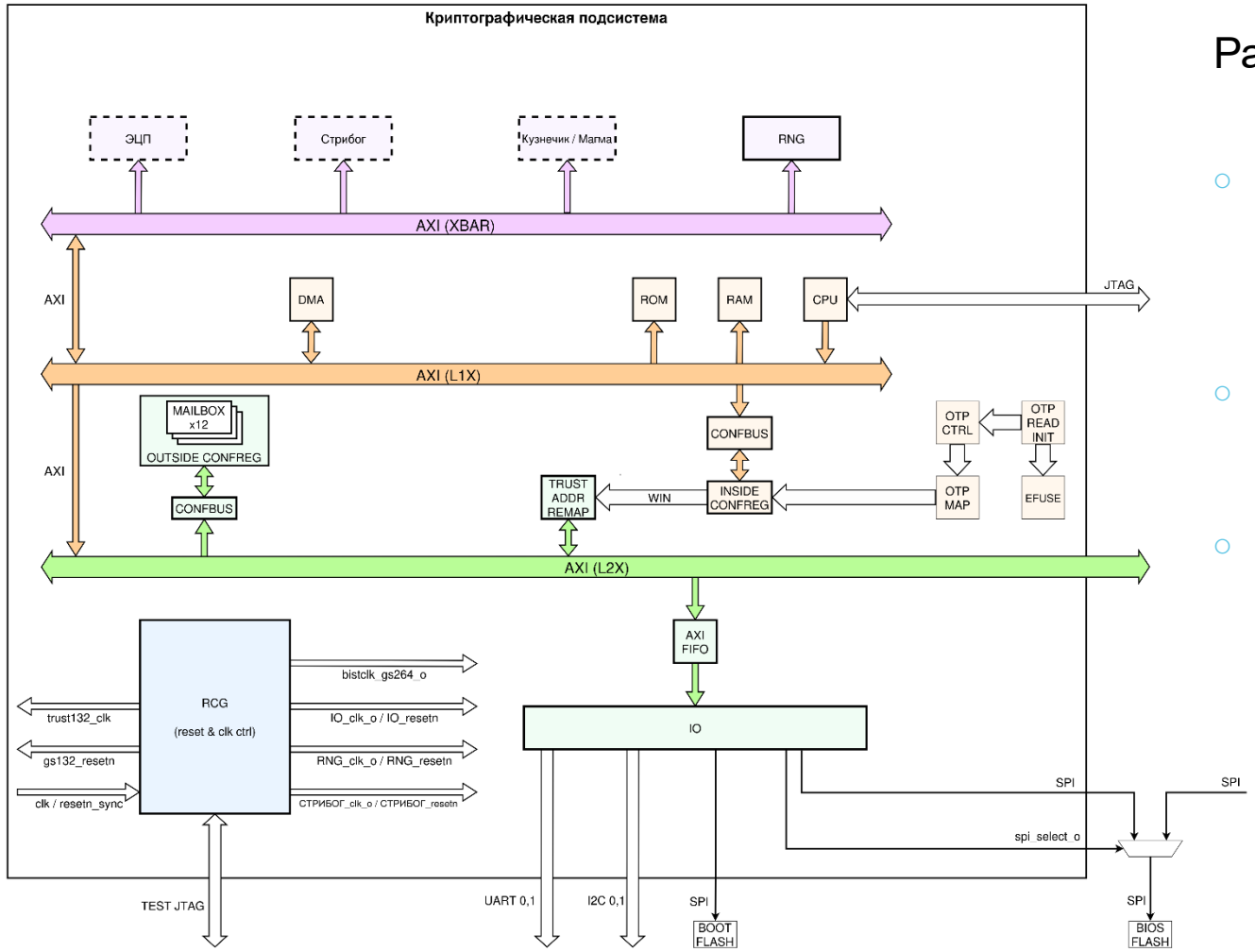
SE – криптографическая подсистема

Криптографические алгоритмы Реализуемые в криптографической подсистеме Иртыш

РОССИЙСКИЙ ФОРУМ МИКРОЭЛЕКТРОНИКА 2026

- Симметричное блочное шифрование:
  - **Стандарт блочного шифра «Кузнечик»** (ГОСТ 34.12-2018)
    длина блока – 128 бит; длина ключа – 256 бит.
  - **Стандарт блочного шифра «Магма»** (ГОСТ 34.12-2018)
    длина блока – 64 бит; длина ключа – 256 бит.
- Криптографические хэш-функции:
  - **Стандарт функции хеширования «Стрибог»** (ГОСТ 34.11-2018)
    длина хэш-кода – 256 бит
- Асимметричное шифрование:
  - **Стандарт формирования и проверки электронной цифровой подписи** (ГОСТ Р 34.10-2012)
    длина секретного ключа – 256 бит

Криптографическая подсистема



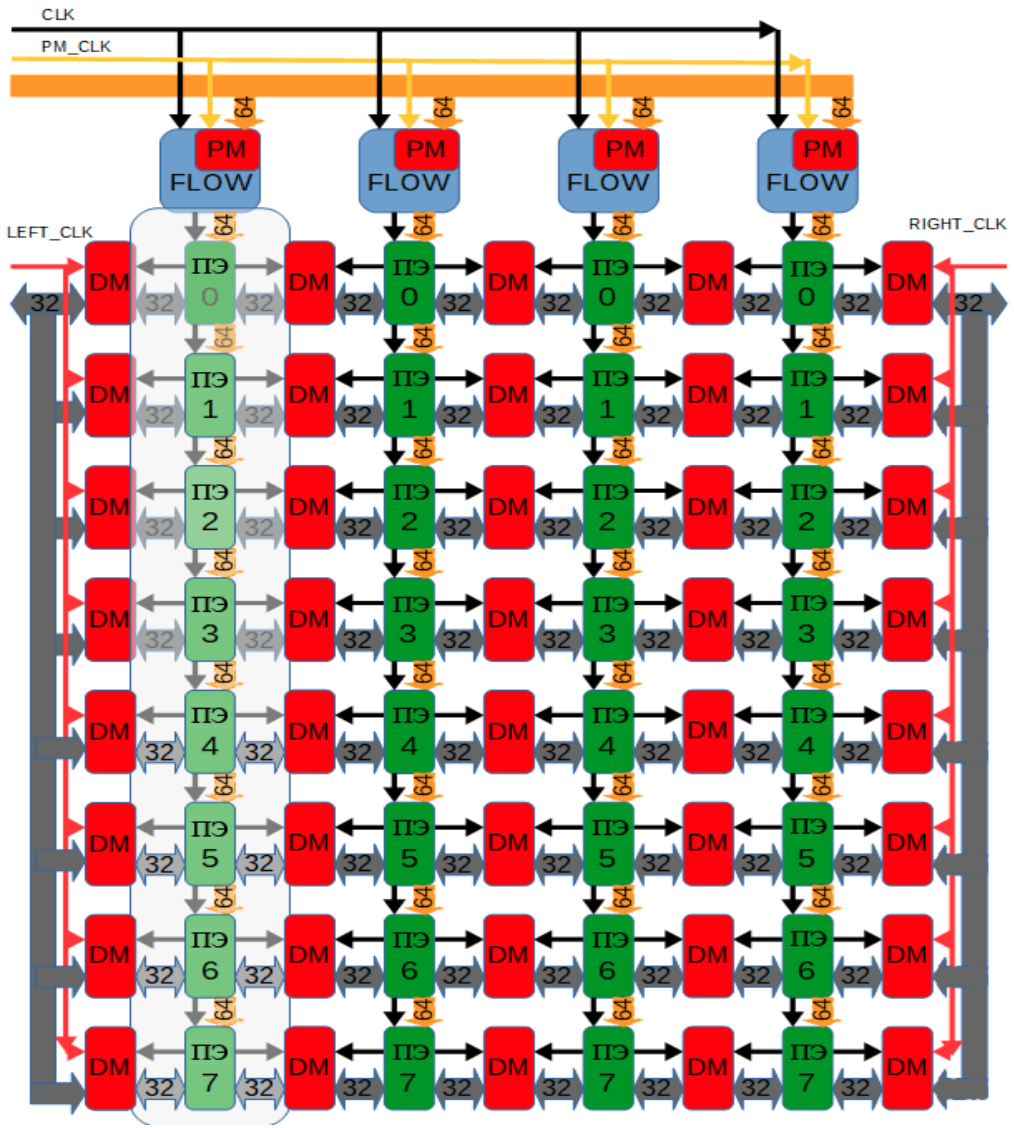
Структурная схема

Разрабатываемые и интегрируемые модули:

- **Кузнечик/Магма** – специализированный процессор для ускорения алгоритмов симметричного блочного шифрования;
- **Стрибог** – специализированный процессор для ускорения задач расчета хэш-функций;
- **ЭЦП** – программируемый модуль для операций на эллиптических кривых.

Специализированные процессоры представляют собой реконфигурируемые функциональные блоки и поддерживают выполнение задач шифрования на основе международных алгоритмов, таких как AES и SHA.

Специализированный процессор



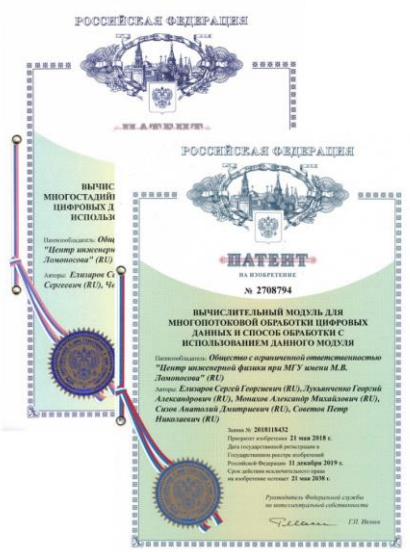
Структурная схема

Состав:

- **ПЭ** – процессорный (вычислительный) элемент
- **РМ** – память программы (криптографический алгоритм)
- **DM** – память данных (обрабатываемые данные)

Основные характеристики:

- программно-аппаратный блок;
- поддержка реконфигурации криптографических алгоритмов (Кузнечик, Магма, AES, SM4, Стрибог, SM3, SHA);
- 32 параллельных вычислительных ядра.

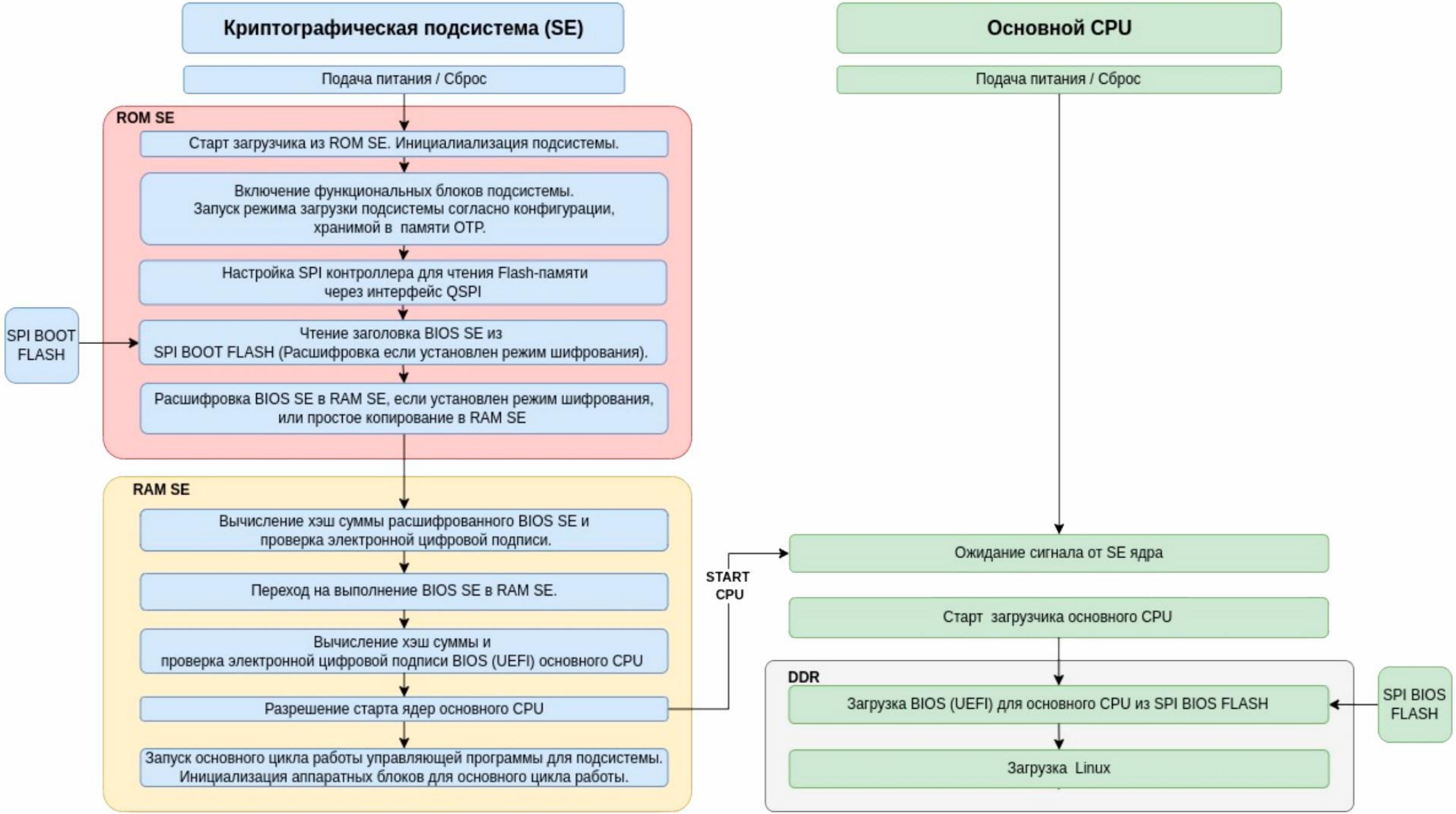


Патенты № 2681365 и № 2708794

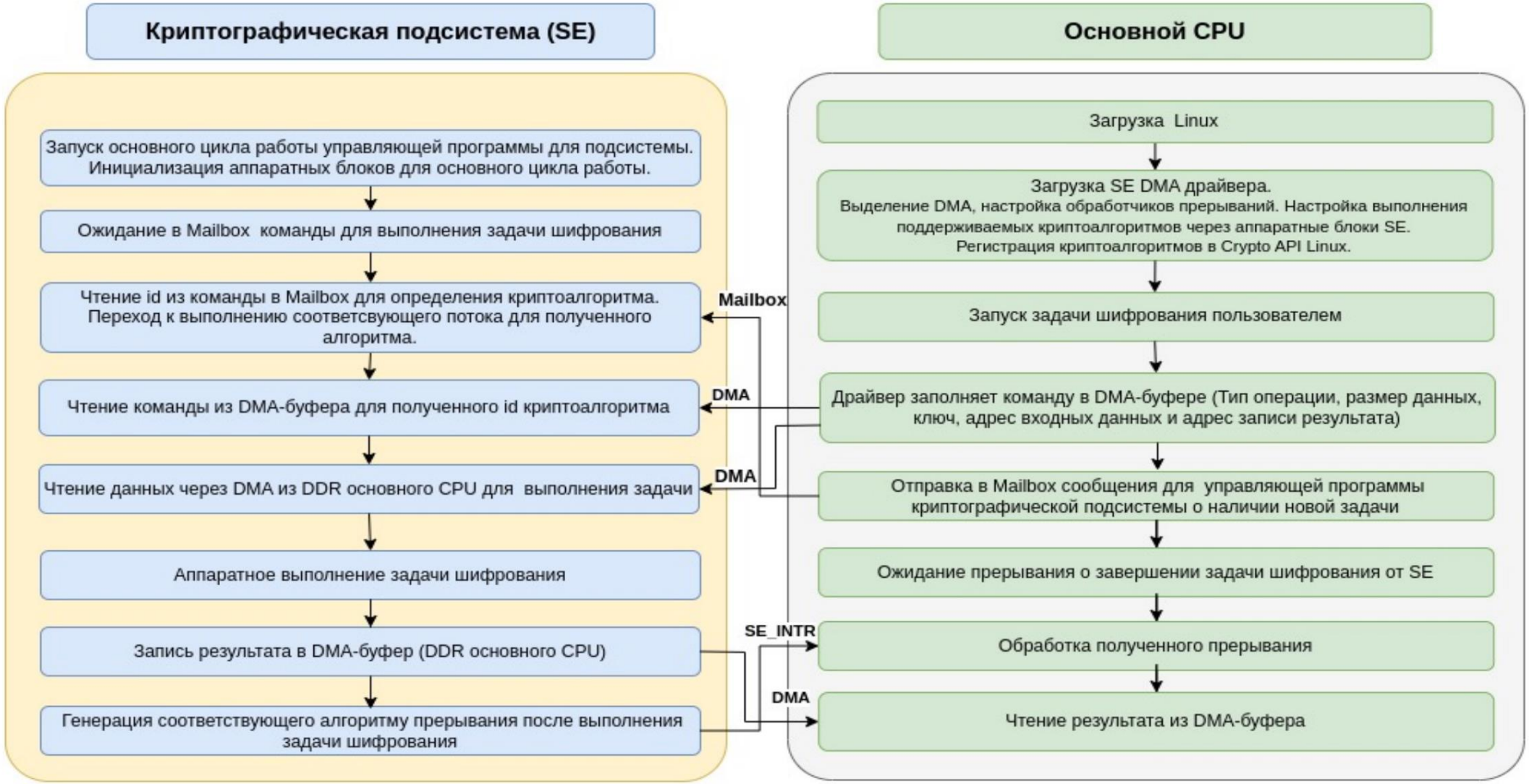
Архитектура защищена патентами.

Авторы патентов – ключевые разработчики проекта.

Алгоритм доверенной загрузки процессора Иртыш



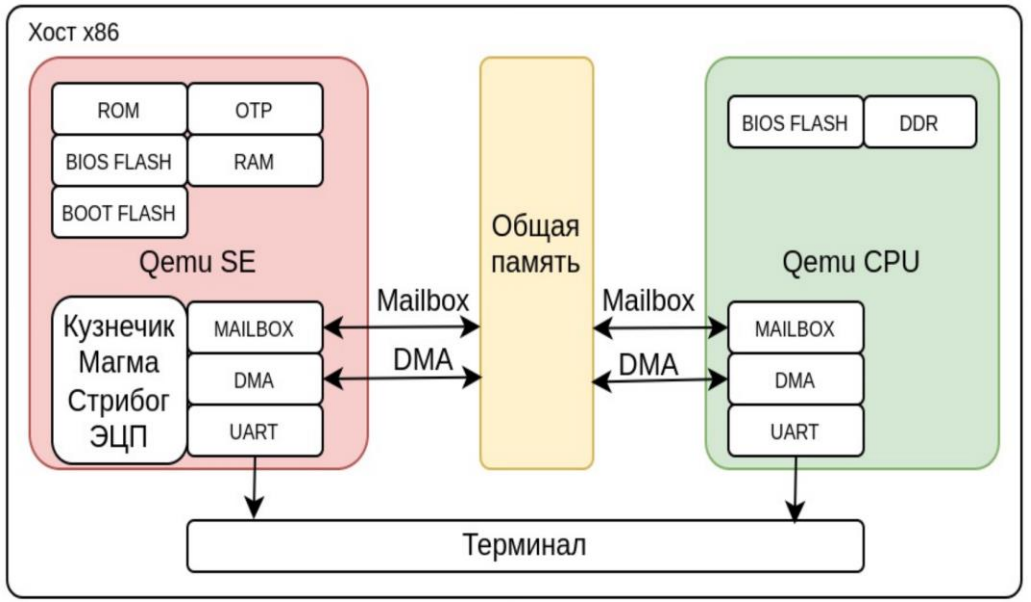
Алгоритм шифрования
В криптографической подсистеме



Эмуляция процессора Иртыш совместно с криптографической подсистемой

Qemu SE – эмулятор криптографической подсистемы:

- эмуляция загрузки бинарного файла из ROM;
- копирование бинарного файла BIOS из Flash в RAM и переход на его выполнение в RAM;
- чтение конфигурации процессора и режима загрузки из OTP;
- чтение/запись регистров Mailbox;
- чтение памяти CPU посредством контроллера DMA;
- загрузка/выгрузка данных в память специализированного процессора для ускорения задач шифрования (Кузнечик/Магма, Стрибог/ЭЦП);
- эмуляция команд запуска алгоритмов шифрования в криптографической подсистеме;
- запись результатов шифрования в память DDR основной процессорной системы посредством контроллера DMA.



Qemu CPU – модель основной процессорной системы:

- чтение/запись регистров Mailbox;
- доступ посредством контроллера DMA к данным, расположенным в памяти DDR и предназначенным для передачи в криптографическую подсистему.

Программные компоненты криптографической подсистемы

РОССИЙСКИЙ ФОРУМ
МИКРОЭЛЕКТРОНИКА 2026

- Микрокод криптографических алгоритмов для блоков ускорения вычислений
- Первичный аппаратный загрузчик Boot ROM
- Первичный программный загрузчик Boot Flash
- Драйвер криптографической подсистемы для ОС Linux

Комплект программных средств для работы с криптографической подсистемой

РОССИЙСКИЙ ФОРУМ МИКРОЭЛЕКТРОНИКА 2026

- Эмулятор аппаратного обеспечения QEMU
- SDK, включающий Linux-драйвер с регистрацией в Kernel Crypto API, поддержку OpenSSL, а также примеры шифрования (сетевого трафика, работы с диском).

СПАСИБО ЗА ВНИМАНИЕ!

РОССИЙСКИЙ ФОРУМ МИКРОЭЛЕКТРОНИКА

Сергей Елизаров, Научный руководитель дизайн центра Мальт Систем, к.ф.-м.н

Василий Воробушков, Директор по развитию Трамплин Электроникс

+7 499 284-60-60

partnership@tramplin.group