Ежегодная международная научно-практическая конференция
«РусКрипто’2021»

Высокопроизводительные программные реализации алгоритмов шифрования Кузнечик и Магма на российских процессорах Эльбрус с учётом архитектурных особенностей

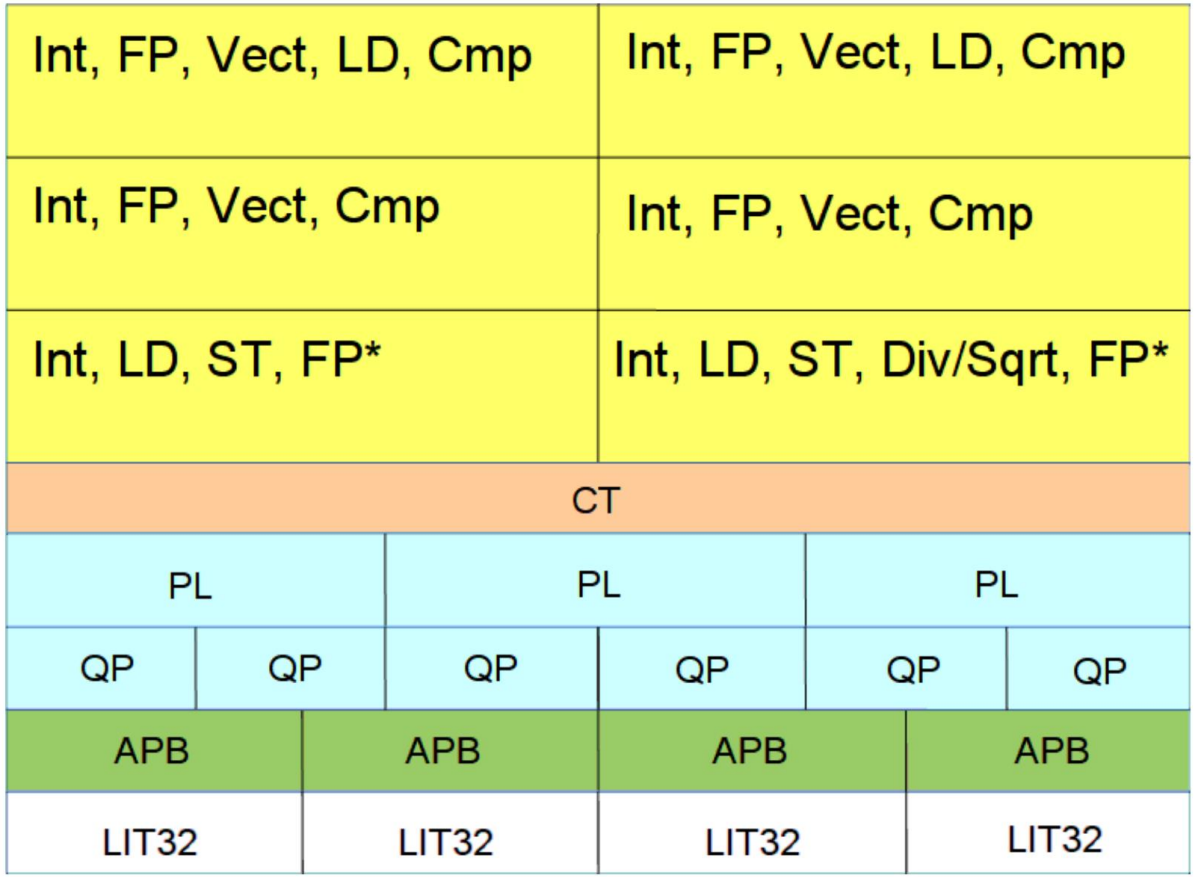
Русев А.А., начальник отдела системных разработок, КриптоПро
Сонина Л.А., начальник отдела криптографических разработок, КриптоПро
Щербаков Д.А., инженер-программист, КриптоПро

Известные результаты

- 1.44 МБ/с — почти 500 тактов на байт
- Отставание более чем на порядок от AMD64 (10-20 тактов на байт)?
- Сложность программирования?

Архитектура Эльбрус

- VLIW (Very Large Instruction Word) — явный параллелизм на уровне инструкций (6 АЛУ)
- Большой регистровый файл
- Асинхронная подкачка массивов (APB)



Широкая команда «Эльбрус», парк устройств

[1] Руководство по эффективному программированию на платформе «Эльбрус» — Нейман-заде М. И., Королёв С. Д. — 2020 — http://mcst.ru/elbrus_prog

Характеристики процессоров

Процессор	Версия архитектуры	Количество ядер	Тактовая частота	Кэш-память			
				L1d	L1i	L2	L3
Эльбрус-4С	V3	4	0.75 ГГц	4 x 64 КБ	4 x 128 КБ	4 x 2 МБ	Нет
Эльбрус-1С+	V4	1	0.985 ГГц	1 x 64 КБ	1 x 128 КБ	1 x 2 МБ	Нет
Эльбрус-8С	V4	8	1.2 ГГц	8 x 64 КБ	8 x 128 КБ	8 x 512 КБ	16 МБ
Эльбрус-8СВ	V5	8	1.55 ГГц	8 x 64 КБ	8 x 128 КБ	8 x 512 КБ	16 МБ

Кузнечик — выбор реализации

- Лучшие реализации: склеенное преобразование LS или R^8/R^8S [2]
- Больше таблица — меньше операций
- Возможности Эльбруса:
  - Большой кэш L1 — 64 КБ на данные
  - 4 параллельные инструкции загрузки 64-битных (для 8СВ 128-битных) значений из памяти
  - Много регистров для хранения промежуточных результатов

[2] A. S. Rybkin, “On software implementation of Kuznyechik on Intel CPUs”, Матем. вопр. криптогр., 9:2 (2018), 117–127
[3] ГОСТ Р 34.12 '15 на SSE2, или Не так уж и плох Кузнечик — https://habr.com/ru/post/312224/

Реализация Кузнечика

- Склеенное LS преобразование — таблица предвычислений размером 64 КБ [2]
- Оптимизация вычисления смещения в таблице [3]
- Основные операции: вычисление адреса в таблице, загрузка 128-битного значения из памяти, xor
- Измерение скорости:
  - Зашифрование в режиме ECB без смены ключа
  - Объём данных — 1 ГБ
  - Выровненные (по 8/16 байтов) и невыровненные данные
  - Последовательная и параллельная обработка блоков

[2] A. S. Rybkin, “On software implementation of Kuznyechik on Intel CPUs”, Матем. вопр. криптогр., 9:2 (2018), 117–127
[3] ГОСТ Р 34.12 '15 на SSE2, или Не так уж и плох Кузнечик — https://habr.com/ru/post/312224/

Кузнечик — последовательная обработка

Шифрование на одном ядре:

Процессор	Скорость на невыровненных данных	Скорость на выровненных данных	Производительность
Эльбрус-4С	52 МБ/с	69 МБ/с	10.4 такт/байт
Эльбрус-1С+	63 МБ/с	90 МБ/с	10.4 такт/байт
Эльбрус-8С	80 МБ/с	110 МБ/с	10.4 такт/байт
Эльбрус-8СВ	≥95 МБ/с	**142 МБ/с**	**10.4 такт/байт**

- Производительность на Intel Core i7-6700 @ 4 ГГц [2]: 170МБ/с, 22.4 такт/байт
- Преимущество Эльбруса в тактах — более **2** раз

Кузнечик — параллельная обработка

Шифрование на одном ядре, 8 блоков параллельно:

Процессор	Скорость на невыровненных данных	Скорость на выровненных данных	Производительность
Эльбрус-4С	78 МБ/с	83 МБ/с	8.6 такт/байт
Эльбрус-1С+	102 МБ/с	108 МБ/с	8.7 такт/байт
Эльбрус-8С	126 МБ/с	133 МБ/с	8.6 такт/байт
Эльбрус-8СВ	≥248 МБ/с	**291 МБ/с**	**5.1 такт/байт**

- Производительность на Intel Core i7-6700 @ 4 ГГц [2]: 360 МБ/с, 10.6 такт/байт
- Преимущество 3 и 4 поколения Эльбруса в тактах — 1.23 раза
- Преимущество 5 поколения Эльбруса в тактах — более **2** раз

Магма — выбор реализации

- Пример реализации описан в статье [4]
- Особенности на AMD64:
  - Использование расширений AVX или AVX2
  - До 3 параллельных целочисленных векторных операций над 128-битными регистрами (256 бит для AVX2)
- Особенности на Эльбрусе:
  - Явное планирование 6 целочисленных векторных операций над 64-битными регистрами (3 и 4 поколения)
  - Явное планирование 4 целочисленных векторных операций над 128-битными регистрами (5 поколение)
  - Гибкий набор инструкций

[4] Особенности национальной криптографии — https://www.securitylab.ru/analytics/480357.php

Реализация Магмы

- Основные операции: сложение по модулю, побитовые операции, битовый сдвиг, подстановки битовых векторов V4->V4
- Измерение скорости:
  - Зашифрование в режиме ECB без смены ключа
  - Объём данных — 1 ГБ
  - Выровненные (по 8/16 байтов) и невыровненные данные
  - Параллельная обработка блоков

[4] Особенности национальной криптографии — https://www.securitylab.ru/analytics/480357.php

Магма — параллельная обработка

Шифрование на одном ядре, 16x блоков параллельно:

Процессор	Скорость на невыровненных данных	Скорость на выровненных данных	Производительность
Эльбрус-4С	116 МБ/с	137 МБ/с	5.2 такт/байт
Эльбрус-1С+	151 МБ/с	179 МБ/с	5.2 такт/байт
Эльбрус-8С	185 МБ/с	220 МБ/с	5.2 такт/байт
Эльбрус-8СВ	≥402 МБ/с	**520 МБ/с**	**2.8 такт/байт**

- Производительность на Intel Core i3-7100 @ 3.9 ГГц:
  - AVX: 458 МБ/с, 8.1 такт/байт
  - AVX2: 1030 МБ/с, 3.6 такт/байт
- 3 и 4 поколения Эльбруса превосходят AMD64+AVX в тактах более чем в **1.5** раза
- 5 поколение Эльбруса превосходит AMD64+AVX2 в тактах в **1.3** раза

Спасибо за внимание!

Контактная информация:

das@cryptopro.ru