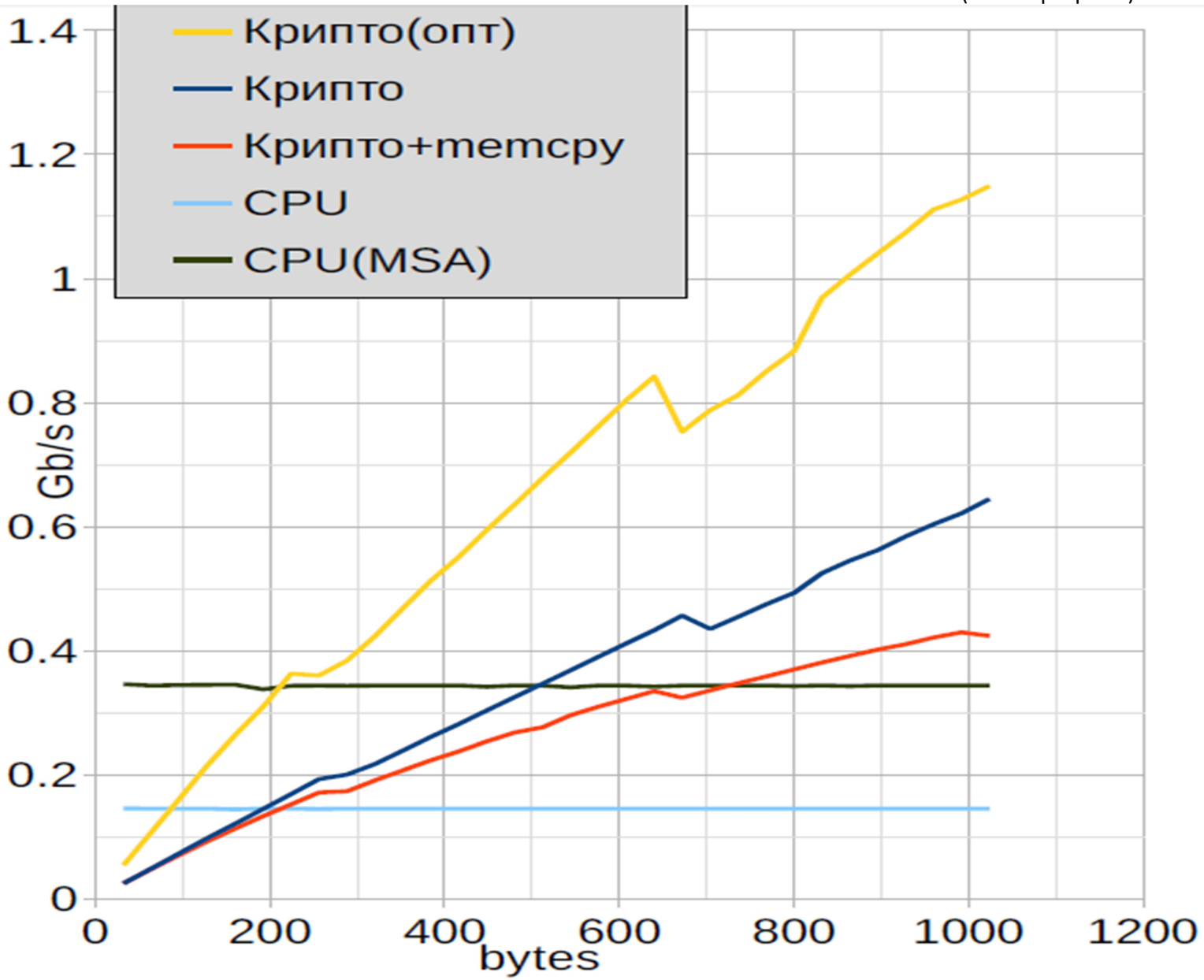
Обзор

3 варианта шифрования

Алгоритм	**на CPU и регистрах общего назначения**	**с применением векторного сопроцессора MSA**	**модулярный сопроцессор**
Скорость	2 * 150Mbit/s	2 * 350 Mbit/s	2500 Mbit/s
Минимальное время подготовки для начала шифрования	0 - без задержки	0 - без задержки	5мкс
Время шифрования блока	~450нс	~180нс	~20нс

Важно: построение шифрующего маршрутизатора потребует использования всех алгоритмов для разных размеров шифруемого пакета.


Крипто(опт)
Крипто
Крипто+memcpy
CPU
CPU(MSA)
1.4
1.2
1
0.8
0.6
0.4
0.2
0
Gb/s
0
200
400
600
800
1000
1200
bytes

Шифрование на CPU и регистрах общего назначения

Шифруется 1 блок размером 64бит..
Время шифрования 1 блока по 64 бит - 450ns
Важно: Наиболее гибкий подход, позволяет реализовать любой вариант зацепления(CTR, CBC и тд.), но достаточно медленный.

Скорость модели ~150Mbit/s на ядро. (Байкал T — 2 ядра.)

MSA

Шифруется 4 блока по 64бит.
Время шифрования 4 блоков по 64бит — 720ns
Скорость модели **~350Mbit/s** на ядро. (Байкал T — 2 ядра.)
Важно: Работает для данных без зацепления (ECB, CTR)

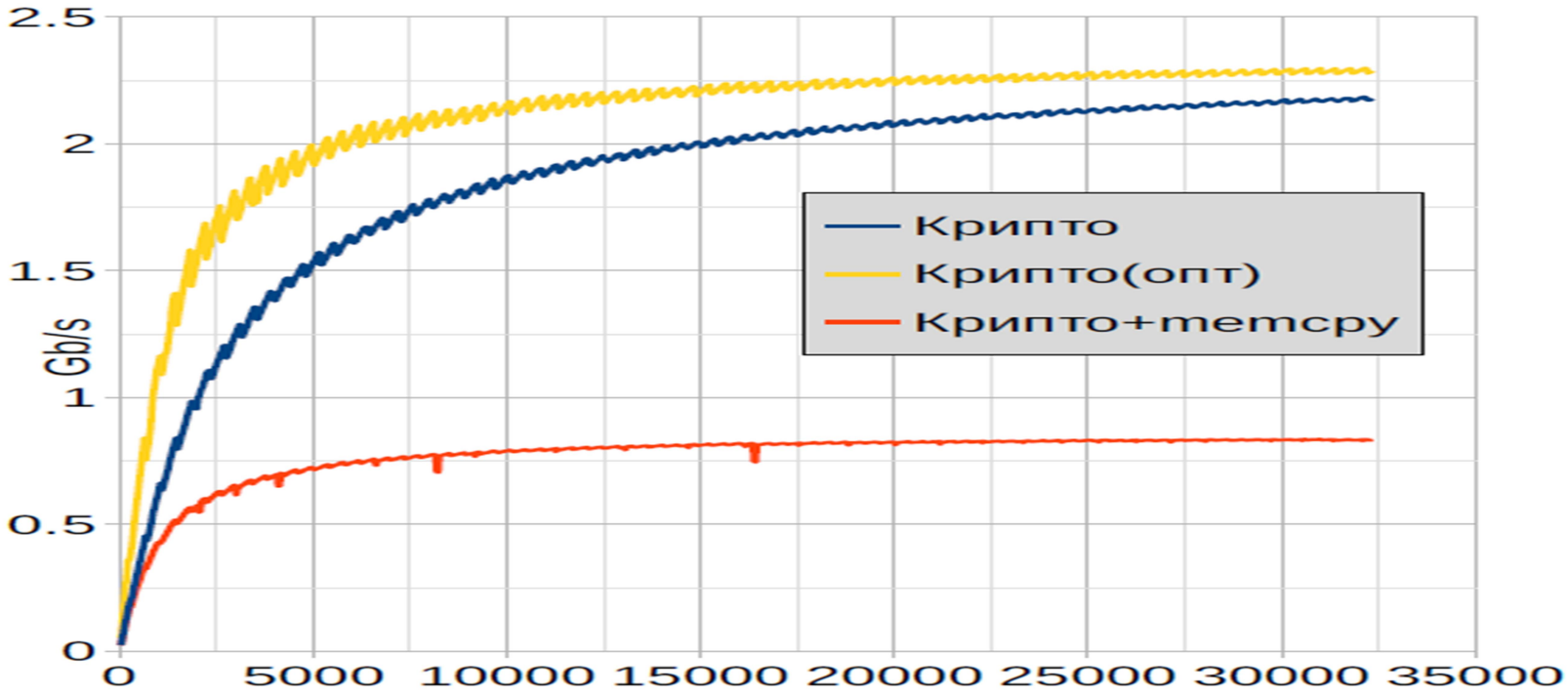
Код: http://www.elcomdesign.ru/ingineer/ingineer_141.html

Прим. Есть некоторые сложности с использованием MSA в ядре линукс т. к. текущая реализация предполагает, что использование MSA возможно только для некоторых процессов пользовательского уровня

Решения:
1. полностью отключать поддержку MSA+FPU и использовать MSA только для шифрования
2. включить поддержку для всех процессов и всегда сохранять контекст MSA

Шифрование на модулярном сопроцессоре

Иллюстрация ниже показывает сильную зависимость скорости шифрования от размера пакета. т. к. в сетевом трафике много пакетов небольшого размера (64байт) ,то использование только модулярного сопроцессора не даёт хороших результатов



Тестирование туннеля

Частота CPU 1.2GHz

iperf режим: TCP/IP

IPsec ESP (static key, MTU=1500)

Модельный пример для проверки концепта смешанного алгоритма шифрования с зависимостью от размера пакета.

ECB
Пакет менее 128байт шифруется на CPU+MSA
Пакеты больше 128байт шифруются модулярным сопроцессором

iperf:
поток 282 Мбит/с
дуплекс 235+184 Мбит /с

Смесь 7*66+4*518+1*1450 дуплекс **109+109** Мбит/с

CTR
Пакет менее 128байт шифруется на CPU+MSA
Пакеты больше 128байт шифруются модулярным сопроцессором (счётчик готовится на CPU модулярный сопроцессор шифрует в режиме ECB)

iperf:
поток 177 Мбит/с
дуплекс 166+126 Мбит/с

Смесь 7*66+4*518+1*1450 дуплекс **87+87** Мбит/с

CBC + Imito
Пакет менее 128байт шифруется на CPU
Пакеты больше 128байт шифруются модулярным сопроцессором

iperf:
поток 281 Мбит/с
дуплекс 216+188 Мбит/с

Смесь 7*66+4*518+1*1450 дуплекс **92+92** Мбит/с