AES: Портирование сопроцессора

Иван Заказов

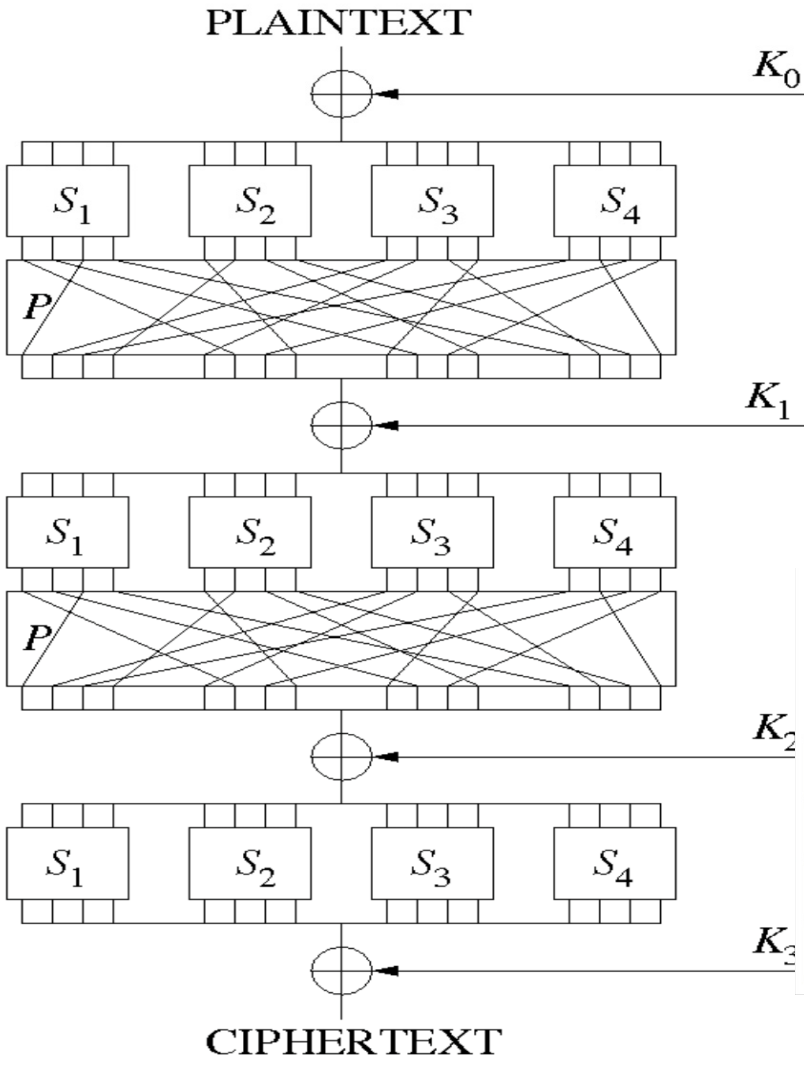
Под руководством Егора Лукьянченко

Май 2016

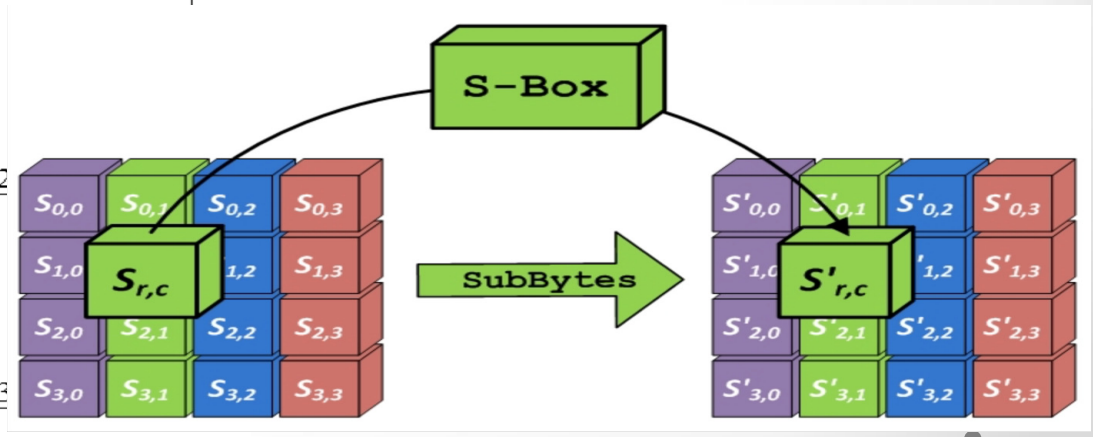
AES – алгоритм шифрования

- Симметричный (один ключ)
- Блочное шифрование (блок – 16 байт)
- Стандарт с 2002 года

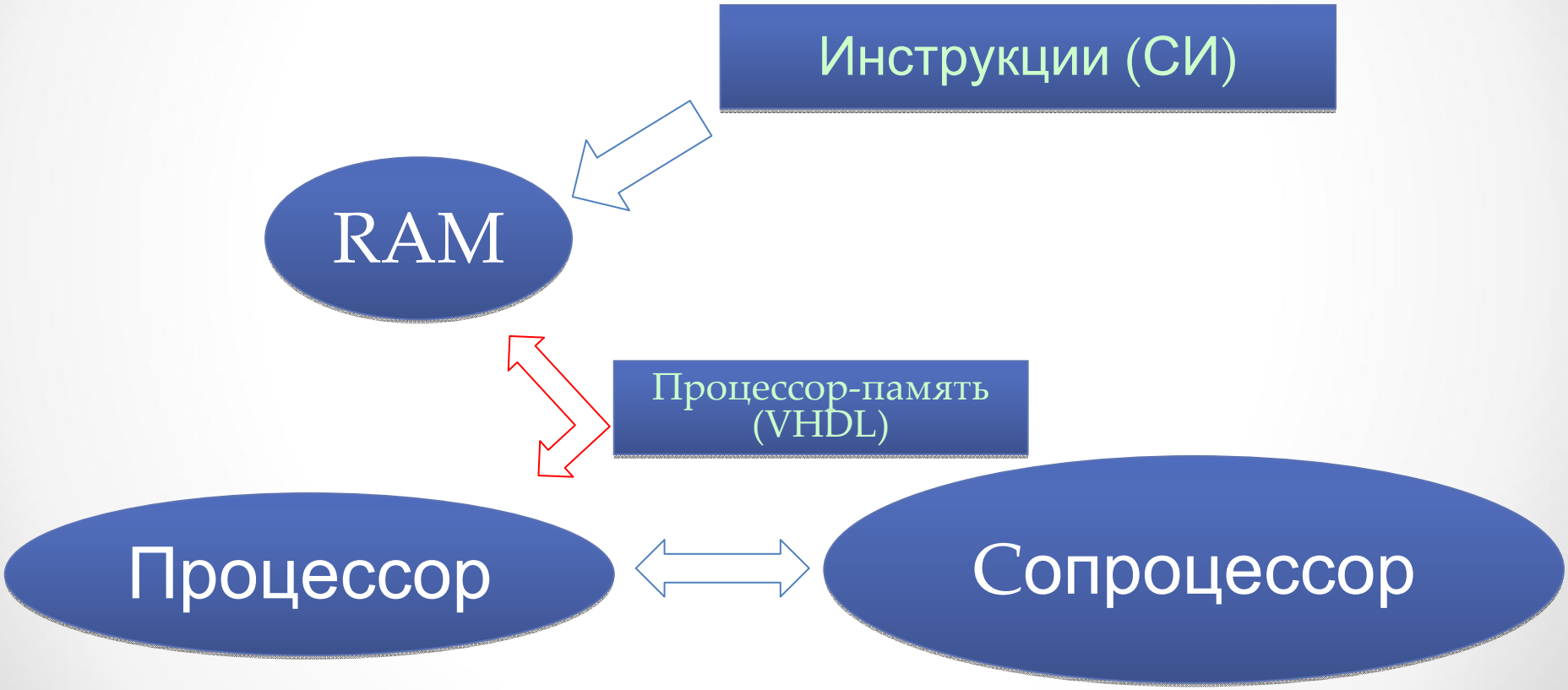
Подстановочно-перестановочная сеть



Подстановка делает шифр нелинейным
и увеличивает его криптостойкость



Прикрепление AES - сопроцессора



Результаты теста

Время выполнения AES, мкс		
С загрузкой	В железе	В симуляторе
14,5	1,5	0,9

Выполнено на плате Xilinx ML505

Чип Virtex 5

Clk = 20 ns

А на что время ушло?

AES работал лишь в один конец

no I didn't made any progress until now, I've no time to look for the cause.
The encryption is working, the decryption is NOT working.
Also my e-mail to the core writer Hemanth Satyanarayana was never answered ...

Выводы

- Я успешно портировал сопроцессор AES на MALT
- Измерил время шифрования
- Сделать AES двусторонним так и не смог, но отчасти решил проблему
- В ходе работы познакомился с основами криптографии
- Осознал, что правильнее было с самого начала разобраться с ядром на Verilog.