УДК 517.9

Защита информации в сети связи с помощью AES

By Ван Киен
Московский Физико-технический институт (государственный университет)

Информационная безопасность всегда является главным приоритетом при построении информационной системы, которая требует конфиденциальности, скорости, гибкости и возможности модернизации в будущем времени. Для совместности с информационными системами алгоритмы шифрования, как правило, реализуются на аппаратном средстве, установленном в своих системах. Однако с точки зрения гибкости и универсальности, программное решение, такое как комбинация FPGA чипа и ARM микропроцессора на одной платформе, является лучшим выбором. Этот метод позволяет использовать преимущества и аппаратного и программного обеспечений с целью повышения безопасности информационных систем.

Advanced Encryption Standard (AES) – алгоритм, который широко используется в шифрующем устройстве. В этом докладе представлена реализация алгоритма блочного шифрования AES128 на платформе FPGA – ARM.

1. Защита информации в сети связи с помощью АЕШ

Рис. 1. Схема системы

Требование к кодам:

- Защищенность
- Гибкость (возможность изменять, обновлять алгоритмы, ключи, параметры)
- Скорость кодирования/декодирования
- Экономичность

2. Схема шифрования АЕШ

На передающей стороне: ARM считывает данные и передает их в AES_Encrypt ядро через Ethernet интерфейс. Зашифрованные на FPGA данные записаны в ARM для передачи через Ethernet интерфейс (рис. 2).

На приёмной стороне: ARM получает данные через Ethernet интерфейс и передает их в AES_Decrypt ядро. Данные после дешифрования поступают в ARM, а потом передают на выход через Ethernet интерфейс (рис. 3).

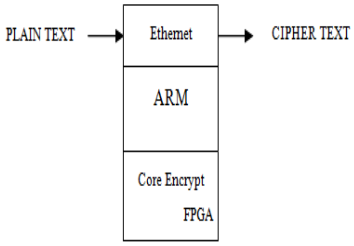

Рис. 2. В передатчике

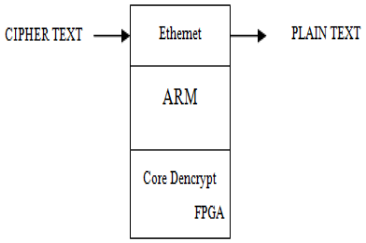

Рис. 3. В приемнике

3. Алгоритм AES128

AES (Advanced Encryption Standard) является алгоритмом блочного шифрования с размером блока данных 128 бит и длиной ключа 128, 192 или 256 бит. В этой работе, мы демонстрируем реализацию алгоритма AES128 (рис. 4).

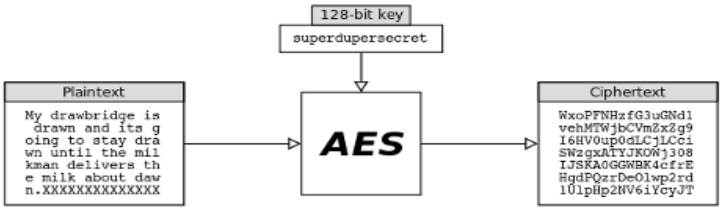

Рис. 4. Алгоритм AES128

Описание алгоритма АЕШ128 (рис. 5).

Процесс кодирования: сначала, входные данные скопировал в массив выполнения. После первого этапа кодирования , массив выполнения сделается 10 циклов: первые 9 циклы выполняются повторно(SubBytes, ShiftRows, MixColumns, и AddRoundKey), последний цикл не включается в себя Mix Columns. На конец, содержание массива состояния скопировано в массив выходных данных.

Процесс декодирования: аналогично но наоборот

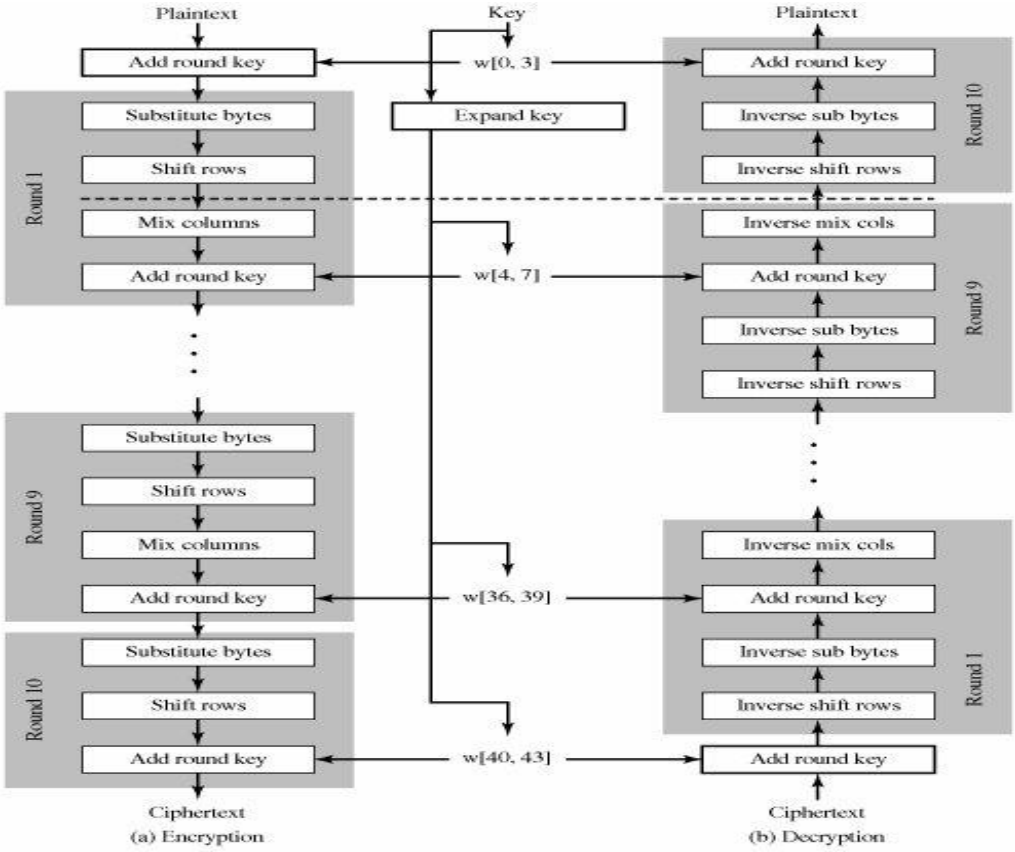

Рис. 5. Описание алгоритма АЕШ128

4. Дизайн ядер AES_Encrypt/AES_Decrypt на FPGA

Ядро AES_Encrypter/AES_Decrypter реализовано с использованием кода VHDL, включая следующие 8 модулей:

a. AES Top Level Module

b. AES State Machine Controller

c. Adder Key Module

d. Loading Key access Module

e. Loading Bytes into the S-Box Module

f. Bytes Sub by the S-Box Module

g. Shifting Rows Module

h. Mixing Columns Module

Вход ядра включает: данные (PLAIN/CIPHER TEXT), KEY (128 bit) и управляющие сигналы (start,reset). Эти сигналы используются для управления работой модулей (Encrypter/Decrypter и Key Expander).

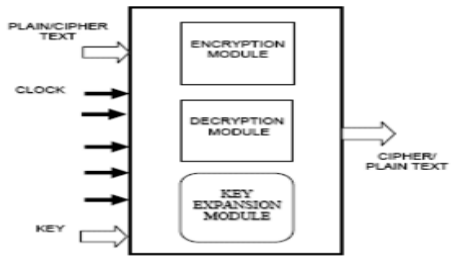

Рис. 6. AES Top Level Module

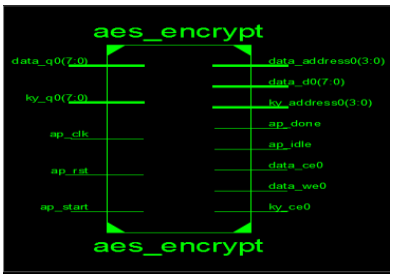

Рис. 7. AES_Encrypt Top Level Module

5. Дизайн модуля интерфейса FPGA-ARM

В этом модуле FPGA и ARM связываются друг с другом по SRAM-интерфейсу. FPGA считывается как периферийное устройство (запоминающее) ARM микропроцессора. Поэтому SRAM-память проектирована в чипе FPGA, используя регистры и процессы считывания/записи данных из/в SRAM выполняются ARM.

SRAM предназначена для хранения 128 бит данных, 128 бит ключа в качестве входов для AES128 блока (Encrypter/Decrypter) и хранения оригинальных/шифрованных данных (рис. 8).

Тактовая синхронизация для FPGA и ARM генерируется модулем lvo_clkmult (рис. 9).

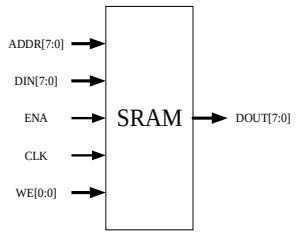

Рис. 8. Дизайн SRAM на FPGA

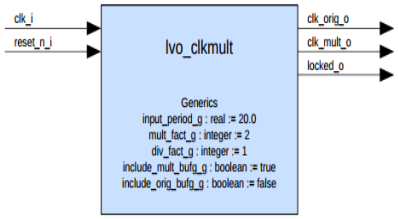

Рис. 9.Module синхронизации частоты между FPGA и ARM

6. Результаты

В информационной системе модуль шифрования реализуется на FPGA, таким образом обеспечиваются требования к безопасности, точности и скорости. Алгоритм шифрования использованный AES алгоритм шифрования обладает высоким уровнем безопасности и имеет способность предотвращать большинство типов известных аппаратных атак. Оригинальные/шифрованные данные контролируется ARM. Это удовлетворяет различные требования к гибкости.

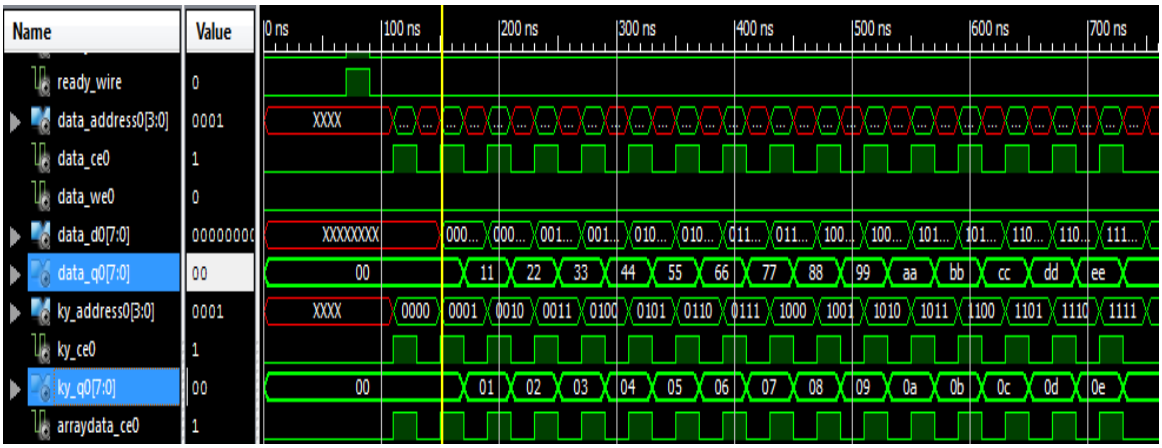

Рис. 10. Проверка симулятор с помощью ISIM (Input)

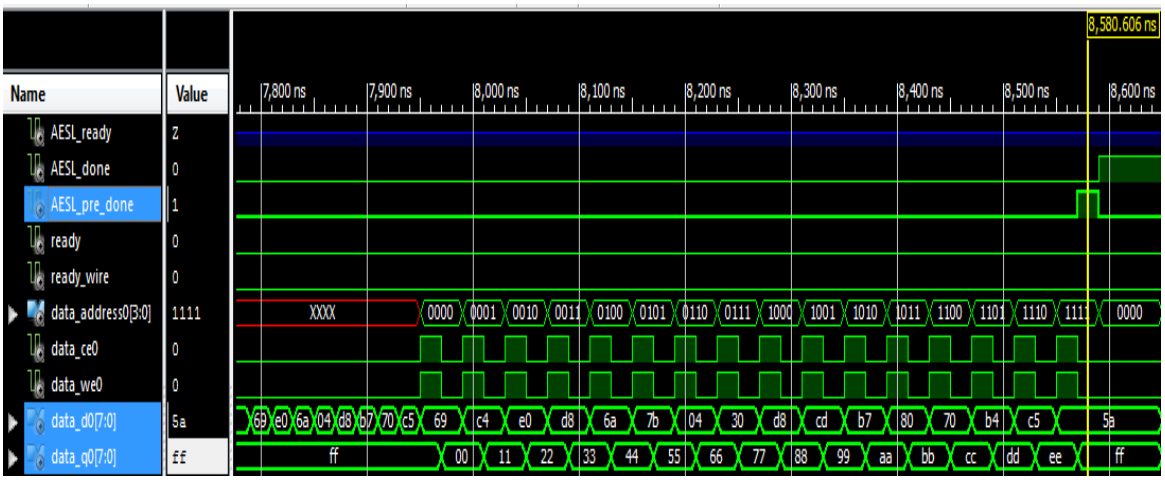

Рис. 11. Проверка симулятор с помощью ISIM (Output)

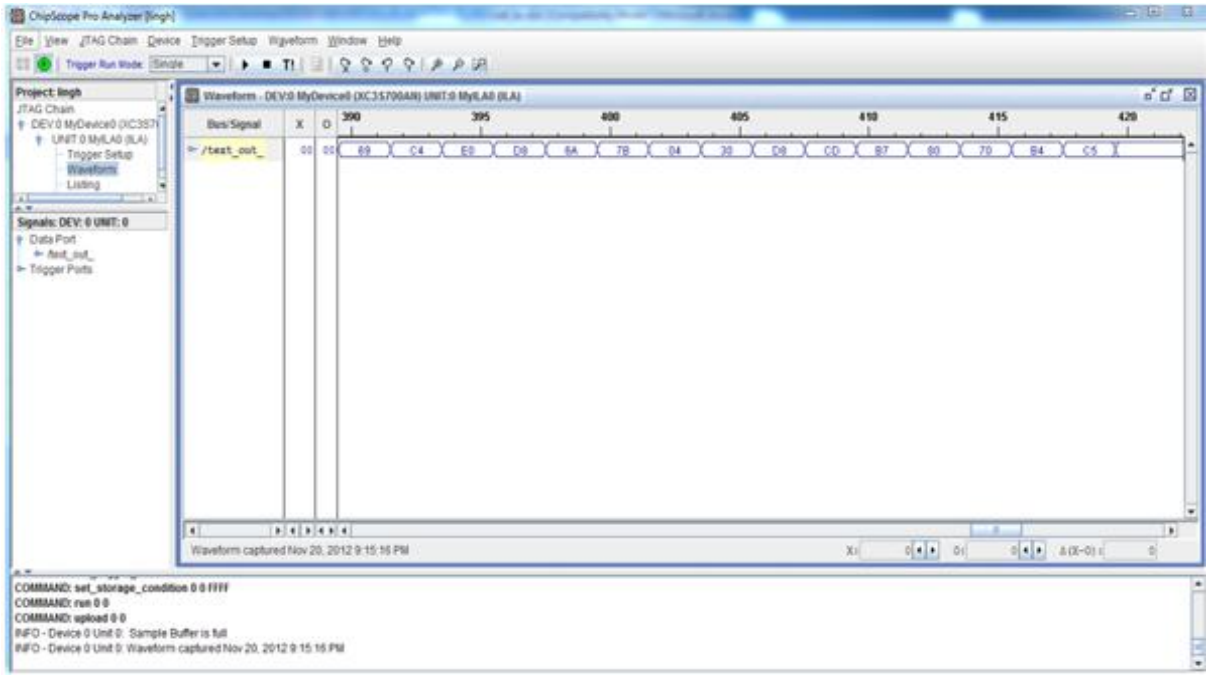

Рис. 12. Проверка действительных сигналов с помощью Chipcopro

Литература

1. *Doug Abbott* - Linux for Embedded and Real-time Applications
2. *Vinayak Bajirao Patil, Prof.Dr.Uttam.L.Bombale, Pallavi Hemant Dixit, Department of technology, Shivaji University, Kolhapur, India* - Implementation of AES algorithm on ARM processor for wireless network
3. *Hua Li and Jianzhou Li Department of Mathematics and Computer Science University of Lethbridge Canada T1K 3M4A* - High Performance Sub-Pipelined Architecture for AES
4. *Sounak Samanta, B.E. III Yr, Electronics & Communication Engg,Sardar Vallabhbhai National Institute of Technology, Surat* - FPGA Implementation of AES Encryption and Decryption
5. *Qitao Zhang,Department of Computer and Information Engineering,Harbin University of Commerce Harbin, China* - On a Hardware Implementing Method of the Optimized AES Encryption Algorithm
6. http://www.linuxforums.org/forum/
7. http://www.xilinx.com/