FPGA-based 128-bit AES decryption

[CSEE 4840 Project Proposal - February 2008]

Shrivathsa Bhargav, Larry Chen, Abhinandan Majumdar, Shiva Ramudit

{sb2784, lc2454, am2993, syr9}@columbia.edu

ABSTRACT

The goal of this project is to create a 128-bit AES decryption implementation of static Bitmap images on the Altera Cyclone II FPGA with the decryption done in a combination of hardware (in VHDL) and software (in C). The project will be very modular.

1. INTRODUCTION

The Advanced Encryption Standard (AES, also known as Rijndael) [1] is well-known block-cipher algorithm for portability and reasonable security. The nature of encryption lends itself very well to the hardware capabilities of FPGAs.

While the number of logic elements might limit the maximum size of the processed image, as well as the length of the cipher, and the limiting clock frequency might result in a longer-than-comfortable processing time, the implementation is entirely feasible on the Cyclone II.

The target for decryption will be a Bitmap image hardcoded on an SD-card. Since the (limited) SRAM will be used for storing the decrypted images, the original image cannot exceed a few kilobytes in size. A comfortable maximum resolution would be 320x240 pixels, in grayscale, with a "color" depth of 8-bits per pixel. Preliminary estimates[1] indicate a file-size of 70kb for such a Bitmap file.

2. RELATED WORK

Several open-source logic cores [2] exist for encrypting and decrypting AES, but most of them are written in Verilog, as opposed to VHDL. While it may be possible to integrate both Verilog and VHDL in the same project, this is usually not done. Instead, a VHDL implementation has been chosen. [3]

3. MAIN DELIVERABLE

The main deliverable of this project would be a working implementation of AES decryption on the Altera Cyclone II development board, with the decrypted image (stored on an SD-card) being shown on a flat-panel display through the use of the VGA peripheral.

[1] Using Adobe Photoshop

4. PLAN OF ACTION

- Familiarization with the open-cores project
- Familiarization with the AES algorithm
- Research usage of SD-cards in previous projects
- Implement Bitmap decoding and display
- Implement AES decryption (hardware) on image stored in SRAM
- Implement SD-card read
- Link modules together

5. MILESTONES

25%: Read and display (320*240) 8-bit grayscale Bitmap images from SRAM

50%: Able to decrypt data from SRAM and store it back

75%: Able to read encrypted Bitmap from an SD-card

6. REFERENCES

[1] Advanced Encryption Standard.
http://en.wikipedia.org/wiki/Advanced_Encryption_Standard
[2] What is Open Cores?
http://www.opencores.org/faq.cgi/section/1/1.4#1.4
[3] AES Crypto Core.
http://www.opencores.org/projects.cgi/web/aes_crypto_core/overview