AES Encryption in FPGA hardware

Patrik Dahlström
Electronic design

Daniel Josefsson
Electronic design

Staffan Sjöqvist
Electronic design

March 24, 2012

1 Introduction

AES encryption is a widely recognized standard encryption that is well used in many modern applications of today. It can be found not only in modern wireless network, but also in encryption devices designed for secure storage as well as in secure wired networks.

It is this group's intention to learn how this encryption works and also how to implement it in FPGA hardware.

Outline The remainder of this document is organized as follows. Section 2 describes the different classes of requirement defined. The actual requirements are then found in Section 3. Finally, Section 4 gives a preliminary time schedule.

2 Requirement Classification

The requirements outlined in this document are divided in three classes:

Class A

The requirements that fall under Class A are mandatory requirements that has to be met for the hardware implementation to be considered acceptable

Class B

Requirements in this class are to be considered as desirable and should be implemented if time allows it.

Class C

These requirements fall under the category ”Extra” and have the lowest priority of all requirements.

3 Requirements

As described above the requirements fall under three categories.

Class A

For this project to be considered complete the FPGA must be able to

- encrypt a reference data set (from AES specification)
- decrypt a reference data set (from AES specification)
- accept data from a PC
- send encrypted/decrypted data to a PC

and the computer software must be able to

- send data to be encrypted/decrypted to the FPGA
- accept encrypted/decrypted data from the FPGA
- verify that the implemented AES algorithm produce the expected result

Class B

It is desirable for the FPGA hardware to be able to

- encrypt arbitrary data sets
- decrypt arbitrary data sets

- use various hardware design techniques to increase performance

and the computer software to be able to

- present encrypted/decrypted data in a primitive GUI

Class C

It should be considered as low priority for the FPGA hardware to be able to

- encrypt/decrypt data using a highly optimized algorithm

and the computer software to

- present encrypted/decrypted data in an intuitive and beautiful GUI

4 Timeline

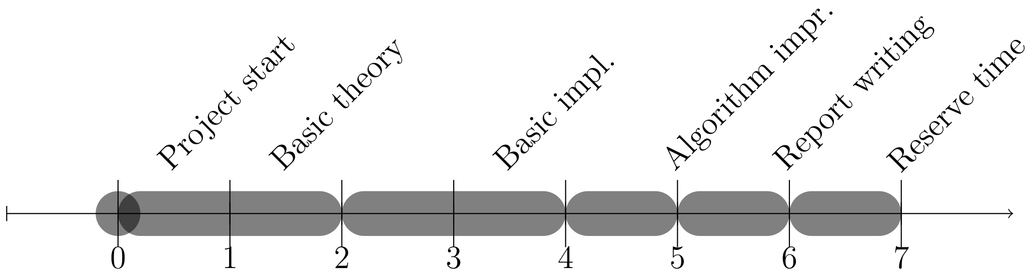

Figure 1: Project progress in weeks