3-DES Encryption Accelerator
SoC Design

Phase 1 Proposal

Submission Date: 2/11/2018
Friday 8:30 Lab Section
TA: Mingxuan

Prepared by: Qifan Chang, Mohammed Al Saeed and Kevin Du

1. Executive Summary

Beyond question, computer and network security has emerged as one of the most important subjects of study in modern times. One of many important problems people face is the the security of IoT devices. There are numerous products in the market that are transferring data without any encryption, reason being that encryption is such a computationally expensive process and the resources on devices using IoT technology are too limited. Among all the popular ciphers, triple Data Encryption Standard (3-DES) provides the maximum level of security as well as backward compatibility with older dedicated infrustructures. The DES algorithm consists three consecutive applications of DES which itselves contains 16 rounds of processing with Feistel cipher structure using 56-bit keys. Each round of processing includes substitution, permutation and round key addition. This results in a high level of repeated process involving lots of parallel computation which is ideal to be designed as an ASIC design to efficiently accelerate modern System-on-Chip (SoC) designs that act as the core of IoT devices.

This proposed encryption accelerator will be designed to be added into SoC designs that are based around a shared AMBA AHB-Lite bus for intra-system communication. It will have the dedicated hardware to interface directly with external internet controllers to eliminate the unnecessity of accelerator-memory-external_controller transactions. It will also contain a dedicated compute core optimized for performing the 3-DES encryption utilizing parallel processing.

Successful design of the proposed accelerator will require the following resources:
- AHB_Lite SoC bus standard documentation
- Reference Standard Cell Simulation Library for Mapped Design Verification
- Reference Standard Cell Technology Library for Final Design Layout Verification
- Verilog HDL Simulation and Design Synthesis Tool Chain The following document

Content will describe:
- Intended usage expectations and constraints for the design, in brief. (Section 2)
- Intended main implementation architecture. (Section 3)

2. Design Specifications

2.1 System Usage

2.1.1 System Usage Diagram

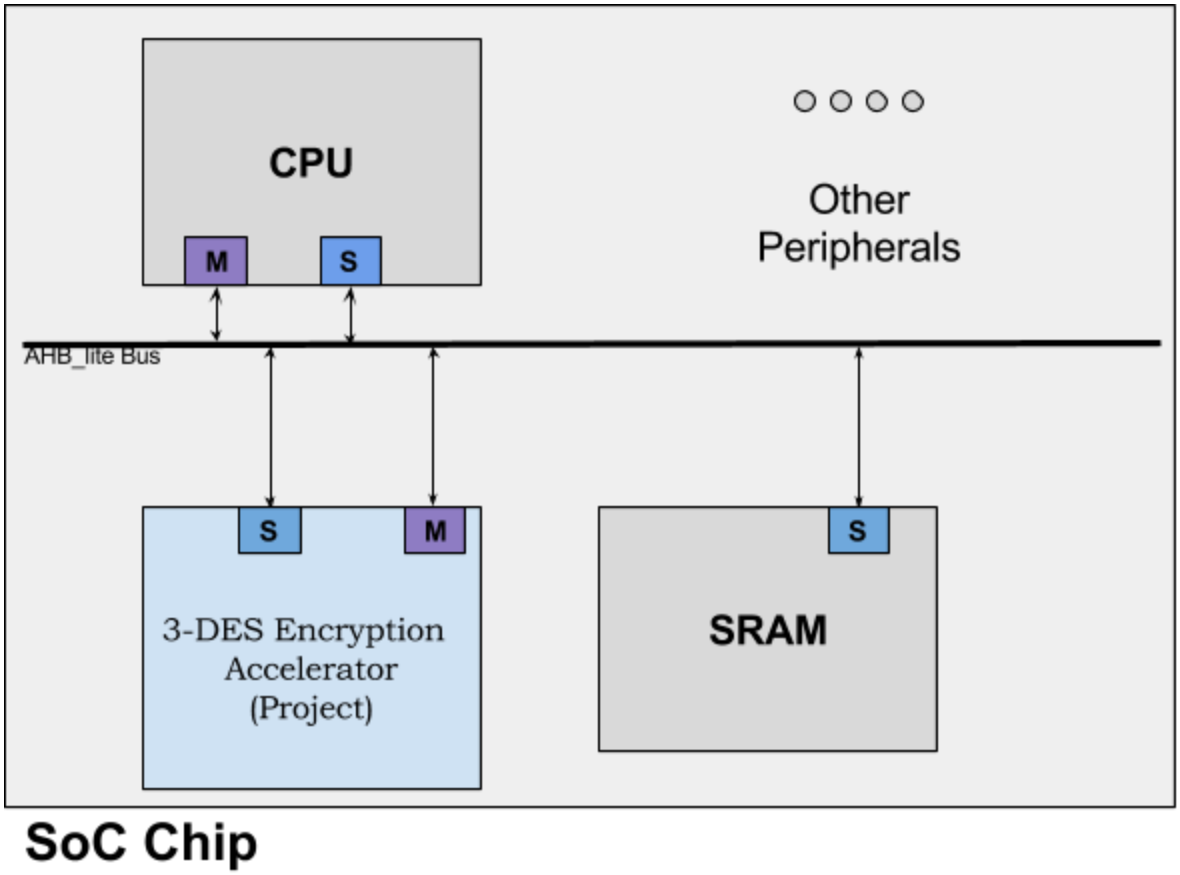

Figure 1: Example System Usage Diagram for 3-DES Encryption/Decryption Accelerator

2.1.2 Implemented standards and Algorithms

- 3-DES Encryption/Decryption
    - 16 round Feistel structure usage (Data Encryption Standard).
    - 3 applications of DES, with 2 keys. The middle application uses the second key, while the first and last applications use the first key.
    - When encrypting, the middle application of DES is actually decryption for backward compatibility. Similarly when decrypting the middle application is encryption.

- AHB_Lite Interface
    - 32 bit data bus
    - Burst Transfer supported
    - Read/Write Transfer

2.1.3 Address Mapping

Slave Address	Read/ Write	Data Size (Bits)	Description
0x000 - 0x0FF	R	256	Data read location
0x100 - 0x1FF	W	256	Data write location
0x200 - 0x27F	R	128	2 Keys storage location
0x280	R	8	Process register for encryption setup

2.2 Design Pinout

Table 1: Pinout Table for System Power

Signal Name	Direction	Number of Bits	Description
gnd	GND		Ground Pin
vcc	PWR		Power Pin
clk	IN	1	System clock / bus clock
n_rst	IN	1	Asynchronous Reset

Table 2: Interface Pins for AHB-Lite Bus and I/O Interface Module

Signal Name	Direction	Number of Bits	Description
address	IN	12	Memory location address to access data
read_write	IN	1	Read or write instruction
enable	IN	1	Enable reading or writing of data
data_ready	OUT	1	Signal telling the system the data is done processing and ready to be read or written
bus_data	IN/OUT	32	Encrypted or decrypted data, divided
mode	IN	1	Encrypt or decrypt
data_processing	OUT	1	Signal indicating the system is busy and cannot accept new data
data_read	IN	1	Signal showing that data has been read and is waiting for new data

3. Design Implementation

3.1 Design Architecture

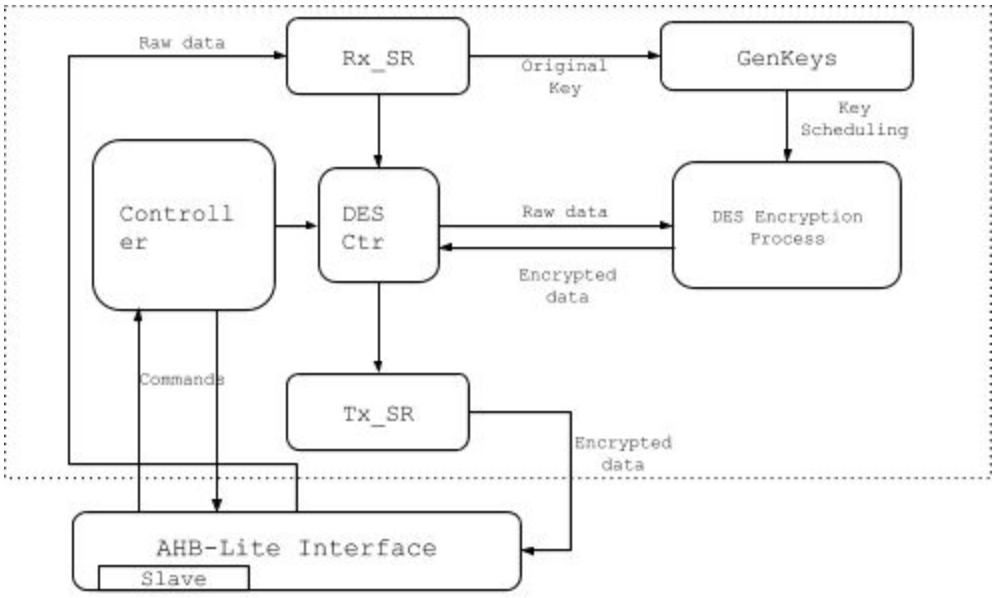

Figure 2: 3-DES Encryption Accelerator Block Architecture Diagram

Our intended implementation is depicted in Figure 2. A module handing all the communication between CPU and Memory in the SoC using AHB-Lite protocol. Since the 3-DES is using 64-bit data block and we are using 32-bit data bus, we use two shift register modules to handle the data from and to the AHB-Lite interface. The controller module is used to handle different mode of the encryption block and the DES_Ctr is used as a timer to let DES_Encryption_Process and shift registers work correspondingly. Finally we use the GenKeys block to generate the key scheduling for Encryption process.

4. References

1. AMBA 3 AHB-Lite Protocol Specification, v1.0, www.arm.com, accessed February 10th 2018.
2. ECE 404 Block Ciphers and the Data Encryption Standard, Janyary 15th 2018, engineering.purdue.edu, accessed February 10th 2018.