Birzeit University

Department of Electrical & Computer Engineering

Second Semester - 2024/2025

ENCS5337 Chip Design Verification

Dr. Ayman Hroub

Course Project

Design and Verification of a Simplified Substitution-Permutation Network Cryptographic Unit (SPN-CU) Using SystemVerilog/UVM

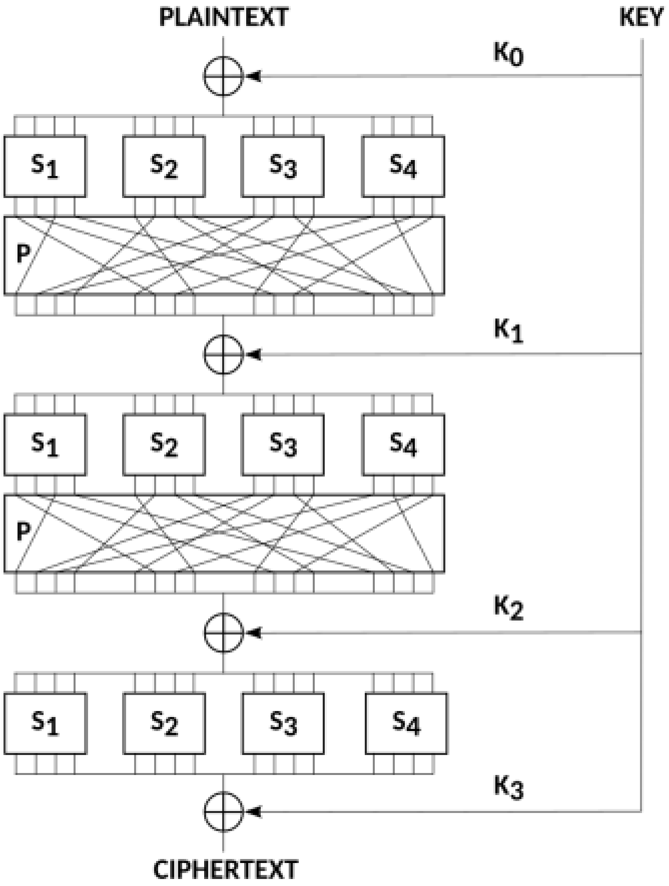
Deadline May 31, 2025

1. Project Objectives

1. SPN-CU RTL design using SystemVerilog
2. SPN-CU UVM based comprehensive design verification

2. SPN-CU Specifications

In this project, you are required to design and verify an SPN-CU with three rounds. This unit can perform encryption and decryption, where decryption is the reverse process of encryption. The figure below (taken from Wikipedia: Substitution–permutation network - Wikipedia) shows a substitution–permutation network with 3 rounds, encrypting a plaintext block of 16 bits into a ciphertext block of 16 bits. The S-boxes are the Si, the P-boxes are the same P, and the round keys are the Ki.



SPN-CU Input Ports:

1. clk
2. Active high reset
3. 2-bit opcode: 00: no operation, 01: encrypt, 10: decrypt, 11: undefined
4. 16-bit input data block that could be either ciphertext or plaintext
5. 32-bit symmetric secret key

SPN-CU Output Ports

1. 16-bit out data block that could be either ciphertext or plaintext
2. 2-bit valid signal. 00: no valid output, 01: successful encryption, 10: successful decryption, 11: internal error or undefined operation

Each round consists of the following three steps:

1. Round Key Mixing

Round keys are derived from the 32-bit secret input key using the following key schedule:

- Round 0 Key: Secret_key[7:0]] concatenated with key[16:23]
- Round 1 Key: Secret_key [15:0]
- Round 2 Key: Secret_key [7:0] concatenated with key[31:24]

In this round, the round's input is XORed with the round's key.

2. Substitution Layer (S-box)

Replace each 4-bit with the corresponding predefined 4-bit from the substitution table below

Input	Output
0000	1010
0001	0101
0010	1000
0011	0010
0100	0110
0101	1100
0110	0100
0111	0011

1000	0001
1001	0000
1010	1011
1011	1001
1100	1111
1101	1101
1110	0111
1111	1110

3. Permutation Layer (P-box):

   For simplicity, just rotate left by 2 bytes

3. Project Deliverables

1. RTL Design SystemVerilog Source Code
2. UVM TestBench Source Code
3. Golden Reference Model which could be a simple SystemVerilog function
4. Report:
   - Design and implementation detailed description
   - Detailed verification plan
   - Simulation snapshots
   - Coverage summary

4. Team Work

You can work on this project in teams of up to three students. Teams exceeding three members will not be permitted. All team members are expected to contribute equally and participate actively in all phases of the project, including design, implementation, verification, and documentation.

5. Grading Criteria

Evaluation Item	**Weight (%)**
RTL design	25%
UVM-based Testbench (including functional coverage and golden reference model)	35%
Verification plan	15%
The rest of the report	10%
The way of discussion and answering questions	10%
Code organization and documentation	5%
Total	**100%**