Implementation of Cryptographic Ciphers

Hritik Bansal
2016EE10071

***Abstract*— In this report, the idea is to analyze the lightweight block ciphers – PRESENT and ESF, and provide a justification for the design choices. Logisim 2.7.1 was used to implement both the ciphers.**

I. PRESENT Cipher

A. Analysis and Justification

PRESENT cipher uses a SP-network with two possible key lengths-80bits or 128 bits. Depending upon the weight of the application, we would like to choose the key length. The state diagram of PRESENT cipher with 80-bits Key is given below.

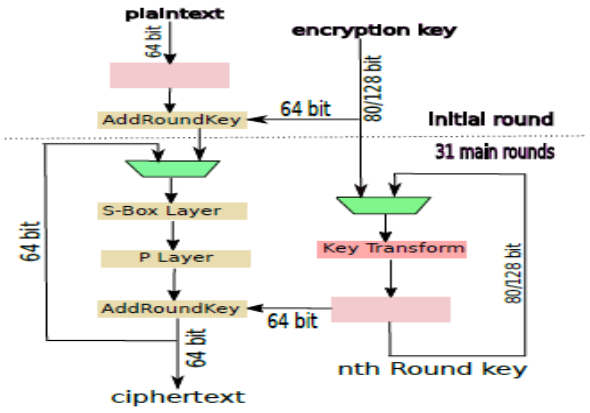

Fig. 1. PRESENT Cipher

As clear from the diagram, the basic components of the cipher are S-box,SP layer and Key Transform. 16 4x4 S-boxes were used in SP layer design and one 4x4 S-box was used in Key Transform. S-box can be implemented by constructing 4 K-Maps for 4-bits of the block. Control signals were generated by maintaining the state of the counter. When value of the counter=31, the halt output is set to 1. Some of the design choices were enforced due to the format of assignment submission. Loading data through command line required us to use RAMs. I used 5 RAMs along with a delay in the clock so that the data can load from the RAM to our main program. As we were supposed to print only the value at the end of the last iteration, I had to use a MUX which gets enabled when counter=31.

II. ESF Cipher

A. Analysis and Justification

Similar to the PRESENT cipher,there are two variants of ESF cipher-with 80bits key length and 128bits key length. We use 80-bits in this case as well. The state diagram is present below. It uses 8

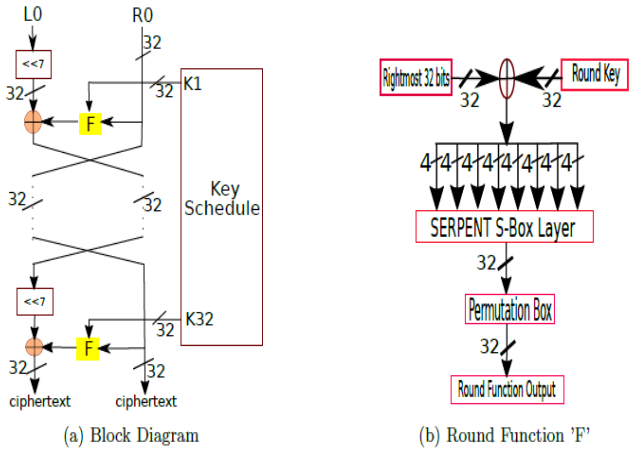

Fig. 2. ESF Cipher

different 4x4 S-boxes, and 2 S_0 boxes were used in the Key Transform. They form the basis for **non-linear** substitution layer.It is important to note that the shifting used in this cipher is **cyclic** in nature. The order of Serpent S-boxes in ESF is either 2 or 3. It can be proved by writing the expressions of each of the cipher for each possible 4-bit input.

III. Conclusion

It is important to understand the various hardware and software specifications of the cipher deployed in an application. Devices like **Smart bulbs** deploy lightweight ciphers because of computational limitation.