Security Implementation Using Present-Puffin Protocol

Rania Baashirah, Anusha Kommareddy, Sumanth Kumar Batchu, Vinusha Sunku, Rithvik Sai Ginjupalli, and Shakour Abuzneid
Department of Computer Science & Engineering
University of Bridgeport, Bridgeport, CT

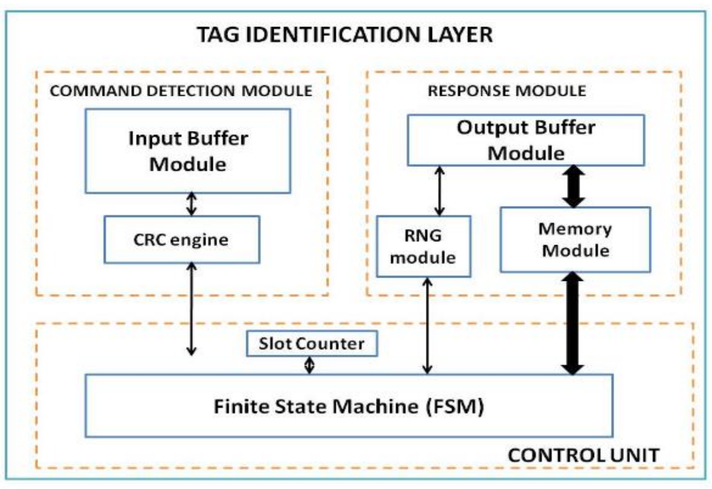
Abstract

The Electronic Product Code Generation 2 (EPC GEN2) protocol does not have any technique to authenticate the Reader before it gives access to the Tag's memory. In this paper, we use security implementation and mutual authentication between tag and reader of three different lightweight ciphers. We used Hummingbird (HB), PRESENT, and Extended Tiny Encryption Algorithm (XTEA) to encrypt the data and implemented all three algorithms to FPGA devices. We finally implemented PRESENT with PUFFIN as a trail and we got better results compared to the former three ciphers based on performance, data blocks and execution time.

RFID Components

- Antenna
- RF front end
- Physical layer
- Tag identification layer

The physical layer comprises of encoding and decoding of the bits from the decoder. Tag Identification layer gets the input from the physical decoder. Tag ID layer mostly depends on the FSM through it has many entities like slot counter, CRC, and random number generator. Tag ID plays the significant role in maintaining the security. As the tag ID performs more function, hence, it would use more hardware using VHDL.

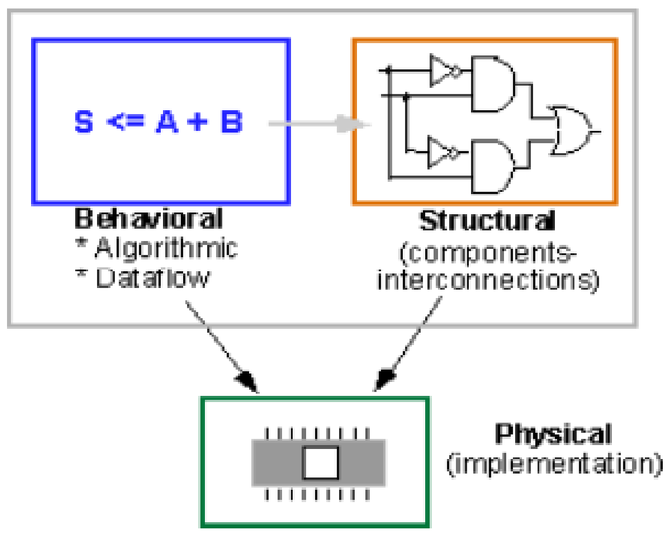


Tag-Reader Interaction: Inventory Rounds

- Ready
- Arbitrate
- Reply
- Acknowledged
- Open
- Secured
- Killed

Representation & Abstraction

A digital system can be represented at different levels of abstraction. This keeps the description and design of complex systems management. The highest level of abstraction is the behavioral level that describes a system regarding what it does (or how it behaves) rather than regarding its components and interconnection between them. A behavioral description specifies the relationship between the input and output signals. This could be a Boolean expression or a more abstract description such as the Register Transfer or Algorithmic level.



Encryption Algorithms

Advanced Encryption Standard:

It is adopted by US government which is based Upon the 128-bit block size and has different key sizes as 128,192 and 256 bits which are resembling 10,12 and 24 round transformation. Operations performed in AES are as ADD ROUND KEY which is a bit XOR operation for block text, we use a S-box for substitution of block shift rows and mix columns are used for shift operations. However, it uses more hardware resources.

XTEA Algorithms:

It is a block cipher based on Feistel structure. It consists of 64-bit plain text and 64-bit cipher text where it consists of 128-bit key operation. It performs 32 round iterations.

Humming Bird:

It is a lightweight protocol and also a rotor based encryption. It has 16 bit plain text and 16 bit cipher text which has 256 bit key. Input keys are been given as input to the four rotors. The output to the rotor is the cipher text. They use different keys in different steps of rotors and in each step the it gets different vector.

Present-Puffin:

The lightweight cipher PUFFIN was introduced and upgraded to PUFFIN2. Both ciphers are 64-bit SPN ciphers with round functions composed of a key addition, an S-box layer and a permutation. The main intention of this cipher permutation and the substitution layer are used for both encryption and decryption process. The first number of key bits in PUFFIN was 128, it has been reduced to 80 in PUFFIN2 while the number of rounds has been increased from 32 to 34. that in addition to the 32 rounds of PUFFIN, a sub-key addition and a permutation are performed at the beginning. In PUFFIN2, the S-box layer has 34-bits.

Implementation

Software Used:

- Xilinx ISE 14.5/13.2

Hardware that can be implemented:

- FPG Spartan

Applications:

- VLSI
- Permutations protocols

Analysis & Results

Compared to the previous implementations of RFID protocols this implementation using present with puffin protocol is observed to be having better results and this also can be further improved.

	Area	Time in ns	Frequency
AES	5000	113.4	1024
PRESENT_PU	140	30	300
HB	789	45	450

Conclusion

Accordingly, as per the comparison of the algorithms our algorithm(present with puffin) is of Low cost solution for many applications where privacy and security has been a major threat. It has Small area , low power requirements and less clock cycles compared to other algorithms. However, PRESENT consumes fewer hardware resources and is faster when compared to HB and XTEA, and is thus more suitable for RFID technology.