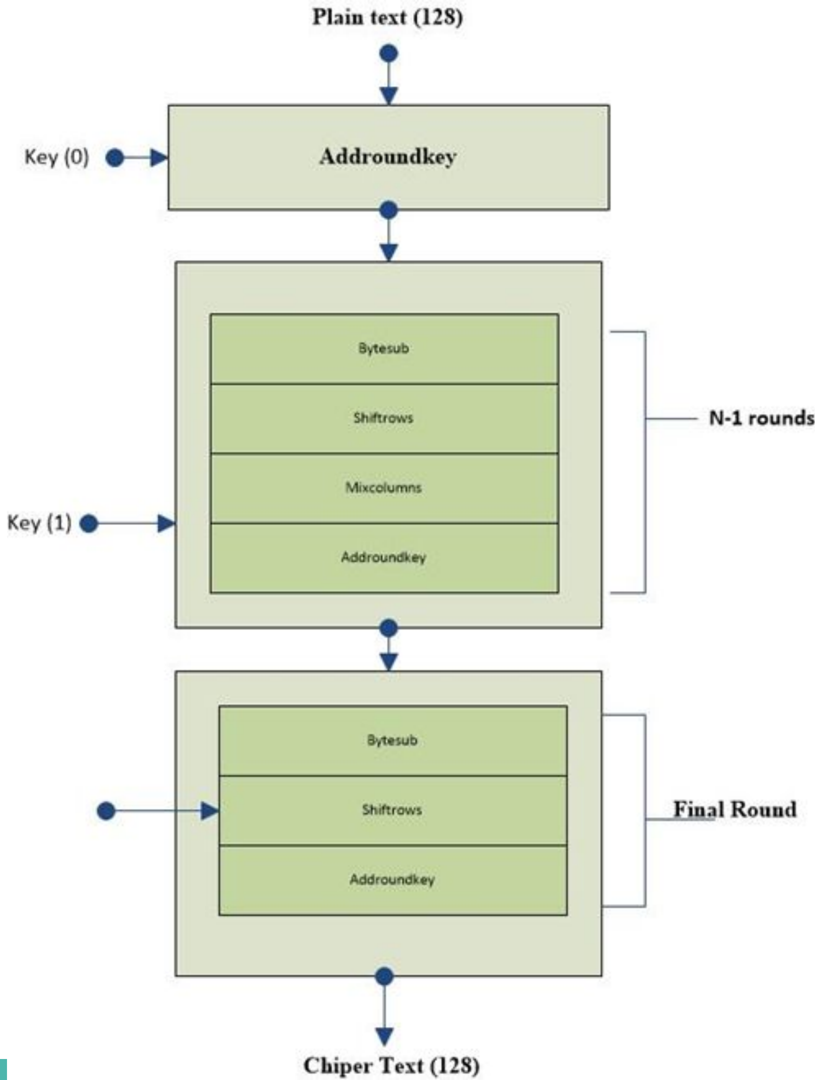
AES CryptoCore

Students: Mihai Olaru
Cătălina Sârbu
Teacher: Dan Dobrea

Encyption process

Steps of the encryption process:

1. Expanding the key that results in round keys; (using an algorithm from the main key)
2. Initial round in which the function is executed:
   - AddRoundKey
3. Intermediate rounds containing 4 transformations each:
   - SubBytes: non-linear transformation;
   - ShiftRows: a line transposition:
   - MixColumns: a mix of operations on the column;
   - AddRoundKey;
4. Last Round: containing follow transformations:
   - SubBytes;
   - ShiftRows;
   - AddRoundKey.

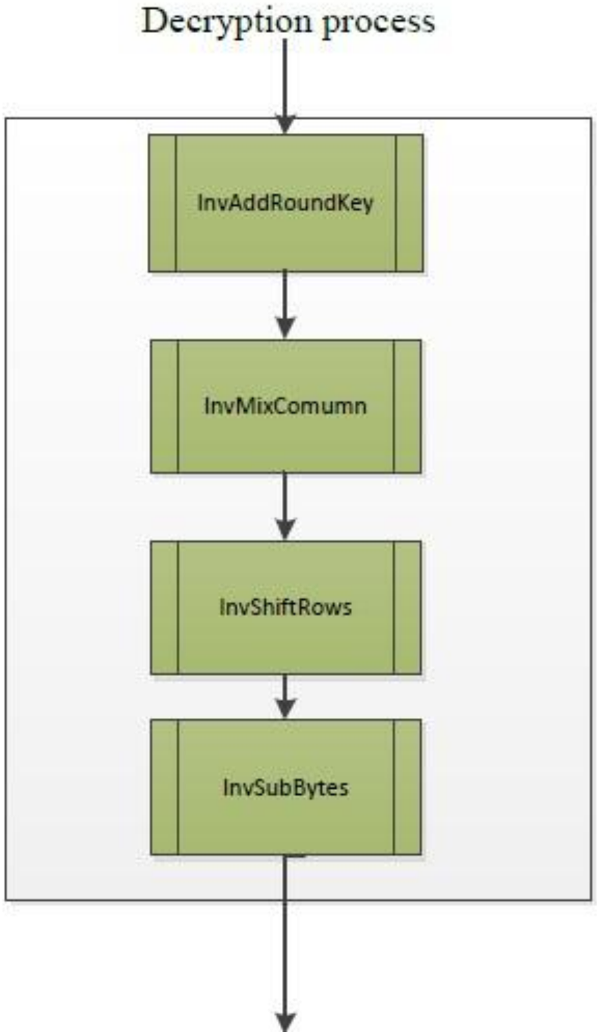


Decryption process

In the decryption process the steps are similar to the encryption.

Steps to the decryption process:

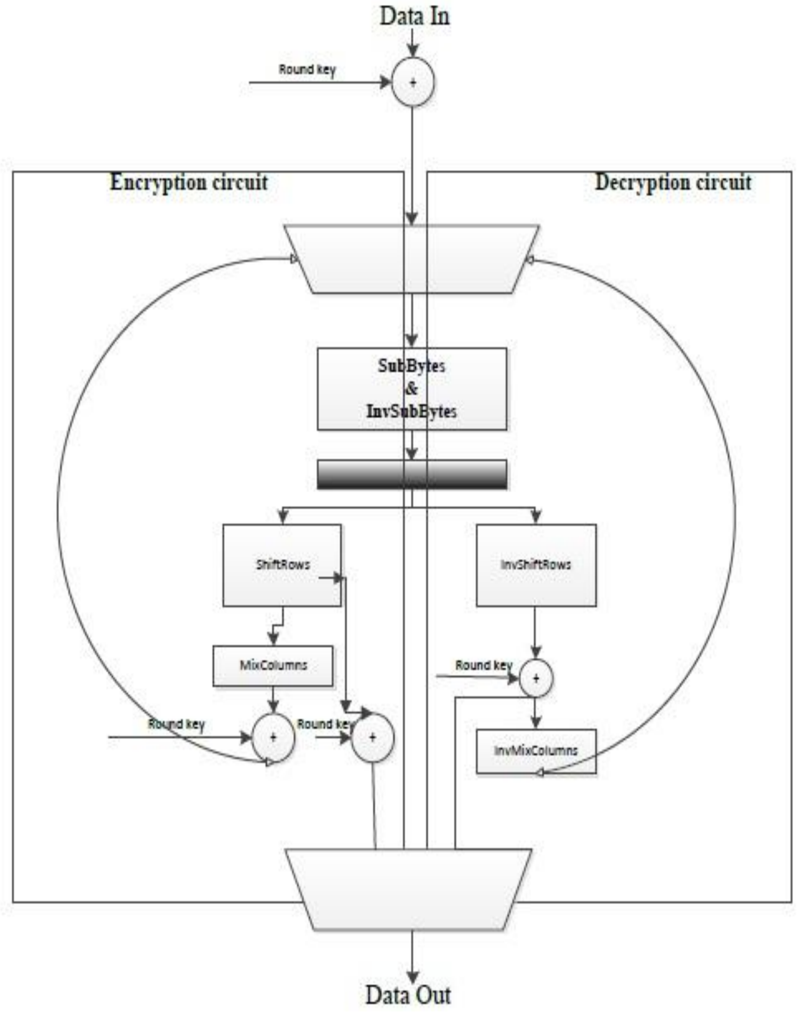
1. Transformation InvAddRoundKey
2. Transformation InvMixColumns
3. Transformation InvShiftRow
4. InvSubBytes transformation.



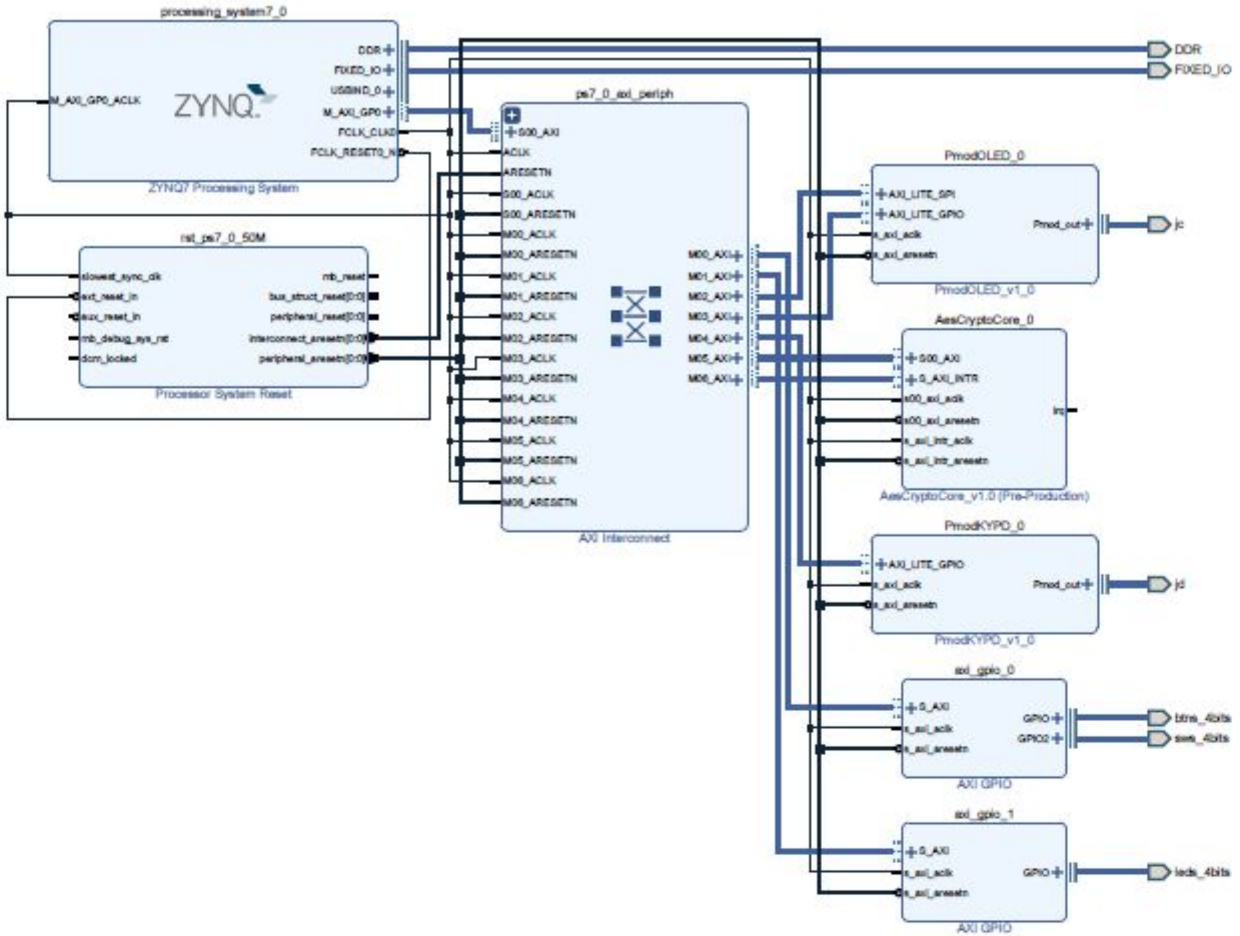
AES CryptoCore Design

AES is a symmetric-key block cipher. It is an iterative cipher, which means that bots decryption and encryption consist of multiple iterations of the same basic round function. In each round, a different key is generated according to the rounds index.

The structure of Block design is a pipeline architecture with two stages. The implementation is in a non-feedback mode.



System design



AES Verification Environment

For testing each component

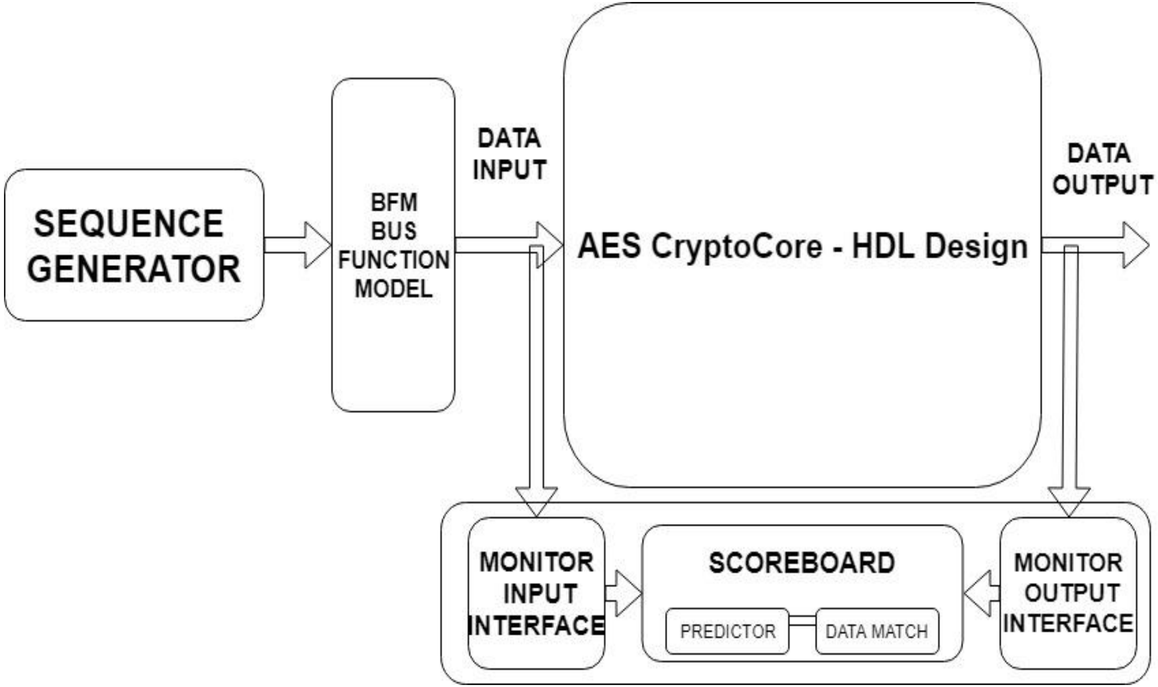
a verification environment is built using

SystemVerilog language.

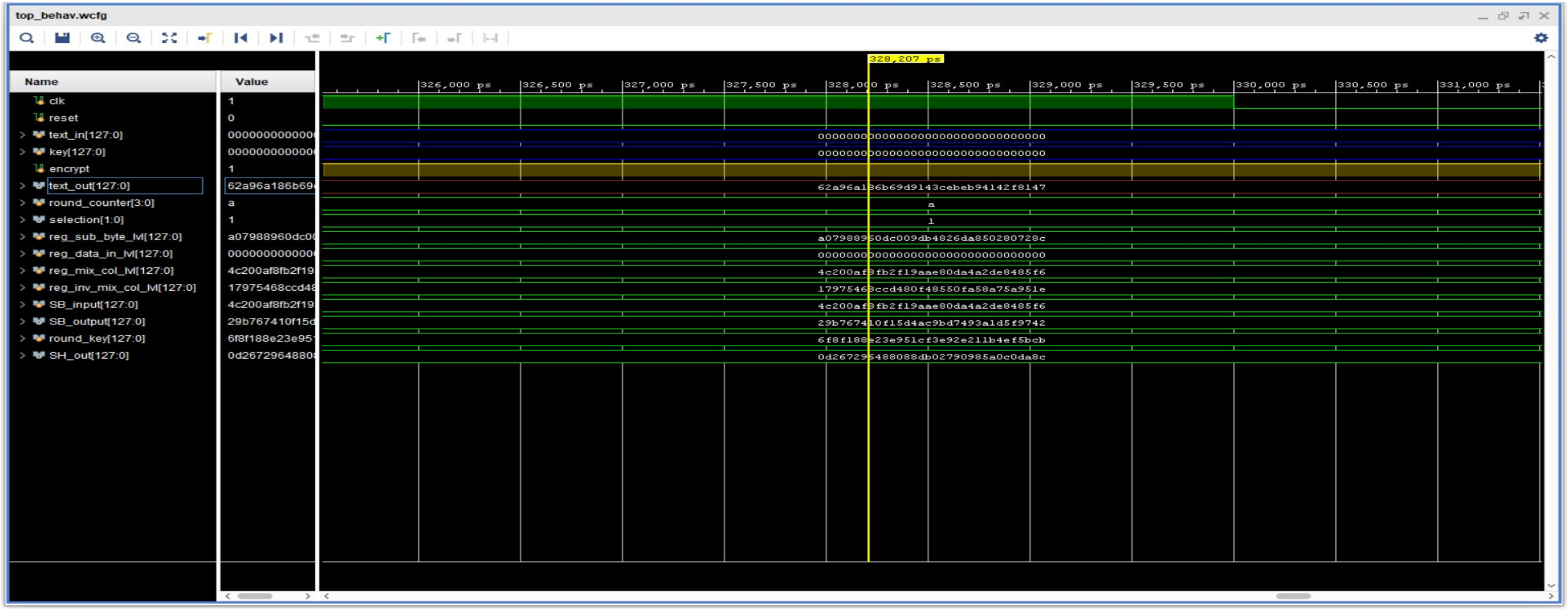
The environment uses lookup-tables

with precalculated values for S-box

and multiplication in GF(2).



WAVEFORM Simulation



top_behav.wcfg

```
                                        328,207 ps
|326,000 ps |326,500 ps |327,000 ps |327,500 ps |328,000 ps |328,500 ps |329,000 ps |329,500 ps |330,000 ps |330,500 ps |331,000 ps

Name                        Value
clk                         1
reset                       0
text_in[127:0]              000000000000     00000000000000000000000000000000
key[127:0]                  000000000000     00000000000000000000000000000000
encrypt                     1
text_out[127:0]             62a96a186b69     62a96a186b69d9143cebeb94142f8147
round_counter[3:0]          a                a
selection[1:0]              1                1
reg_sub_byte_lvl[127:0]     a07988960dc0     a07988960dc009db4826da850280728c
reg_data_in_lvl[127:0]      000000000000     00000000000000000000000000000000
reg_mix_col_lvl[127:0]      4c200af8fb2f19   4c200af8fb2f19aae80da4a2de8485f6
reg_inv_mix_col_lvl[127:0]  17975468ccd48    17975468ccd480f48550fa58a75a951e
SB_input[127:0]             4c200af8fb2f19   4c200af8fb2f19aae80da4a2de8485f6
SB_output[127:0]            29b767410f15d    29b767410f15d4ac9bd7493a1d5f9742
round_key[127:0]            6f8f188e23e95    6f8f188e23e951cf3e92e211b4ef5bcb
SH_out[127:0]               0d2672964880     0d26729648808 8db02790985a0c0da8c
```

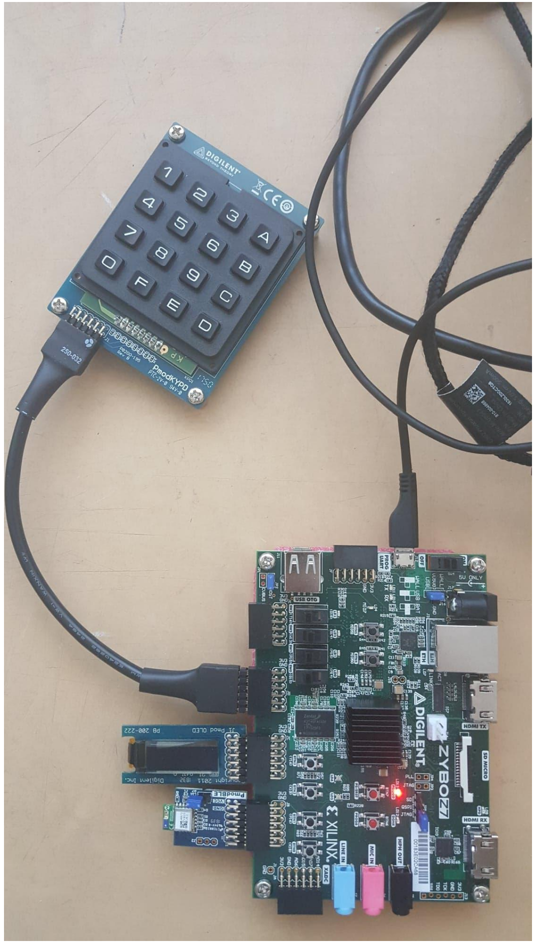
Hardware Resources

Digilent Zybo

Digilent Pmod KYPD

Digilent Pmod BLE

Digilent Pmod OLD



Project Status

AES CRYTO Core -> Verification Process

IP INTEGRATOR -> DOING

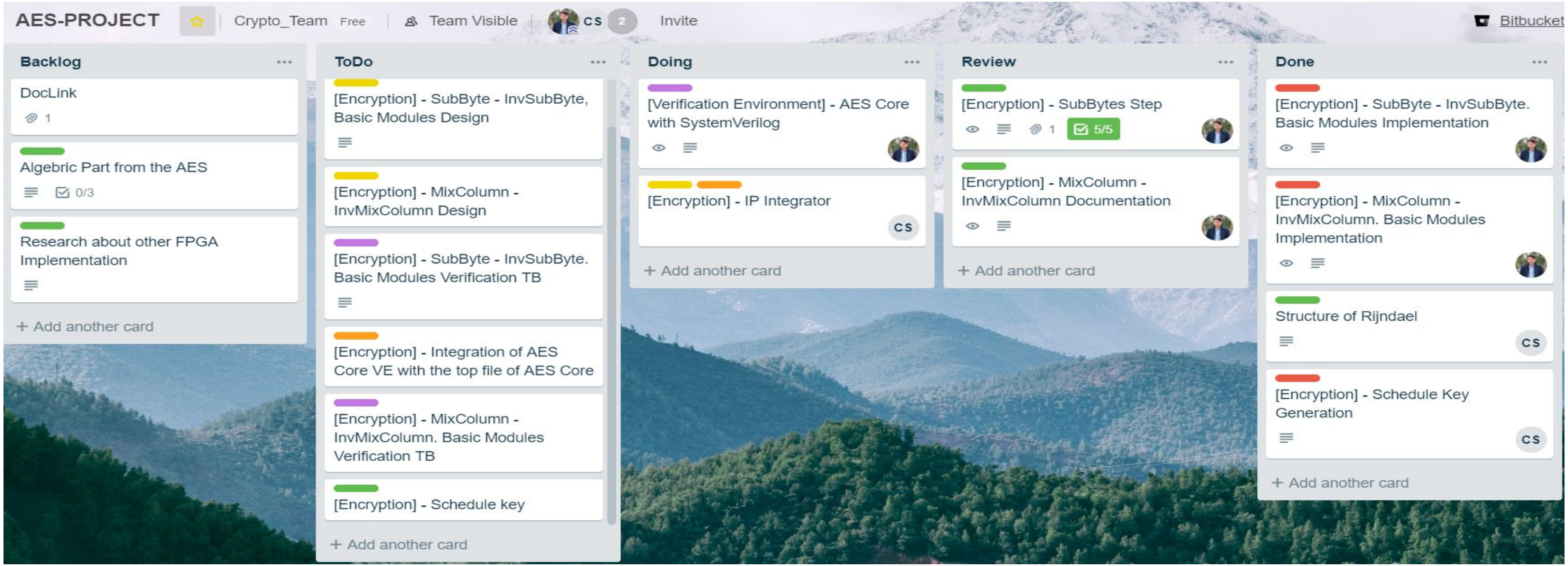
UART Transmission -> ToDo

KEY-Configuration and Display using hardware resources -> ToDo

Bluetooth transmission -> ToDo

Bluetooth Receiver application -> ToDo

Task Management



AES-PROJECT | Crypto_Team Free | Team Visible | CS 2 | Invite | Bitbucket

Backlog

- DocLink
  1
- Algebric Part from the AES
  0/3
- Research about other FPGA Implementation

+ Add another card

ToDo

- [Encryption] - SubByte - InvSubByte, Basic Modules Design
- [Encryption] - MixColumn - InvMixColumn Design
- [Encryption] - SubByte - InvSubByte. Basic Modules Verification TB
- [Encryption] - Integration of AES Core VE with the top file of AES Core
- [Encryption] - MixColumn - InvMixColumn. Basic Modules Verification TB
- [Encryption] - Schedule key

+ Add another card

Doing

- [Verification Environment] - AES Core with SystemVerilog
- [Encryption] - IP Integrator
  CS

+ Add another card

Review

- [Encryption] - SubBytes Step
  1 5/5
- [Encryption] - MixColumn - InvMixColumn Documentation

+ Add another card

Done

- [Encryption] - SubByte - InvSubByte. Basic Modules Implementation
- [Encryption] - MixColumn - InvMixColumn. Basic Modules Implementation
- Structure of Rijndael
  CS
- [Encryption] - Schedule Key Generation
  CS

+ Add another card

Conclusion

AES CryptoCore provides Real-Time Encryption/Decryption.

The algorithm can be implemented with very high throughputs in modern ASIC or FPGA technology.

Symmetric Encryption with today’s ciphers is extremely fast.

In this project, AES CryptoCore is used to provide a secure Bluetooth Transmission.