AES-T2600

- Trojan Description
  - The Trojan trigger is a 4-bit asynchronous counter inserted into the AES-128 block cipher. The counter is increased by 1 after each successive encryption if the value of a predetermined signal (s3[122] within the aes_128 module) is 1. The Trojan is active when the fourth bit of the counter is high. When triggered, the Trojan attacks encryption by flipping the least significant bit of the existing encrypted output.
- Trojan Taxonomy
  - Insertion phase: Design
  - Abstraction level: Register transfer level
  - Activation mechanism: Both physical-condition and time-based
  - Effect: Change functionality
  - Physical characteristic: Functional