AES-T2700

- Trojan Description
  - The Trojan trigger is dependent on a 4-bit asynchronous counter, which is in turn contingent on a 4-bit synchronous counter (both inserted into the AES-128 block cipher). After each successive encryption, the synchronous counter is increased by 1. The asynchronous counter is also incremented provided that the fourth bit of the synchronous counter is high. The Trojan is active when the fourth bit of the asynchronous 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