AES-T2500

- Trojan Description
  - The Trojan trigger is a 4-bit synchronous counter inserted into the AES-128 block cipher. The counter is increased by 1 after each successive encryption and 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: Time-based
  - Effect: Change functionality
  - Physical characteristic: Functional