AES-T2400

- Trojan Description
  - The Trojan is triggered whenever two predefined signals (one rare: s2[89] and one nonrare: s7[127] of the aes_128 module) in the AES-128 block cipher are simultaneously high. Upon activation, 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: Physical-condition-based
  - Effect: Change functionality
  - Physical characteristic: Functional