

AES-T2300

- Trojan Description
 - The Trojan is triggered whenever two predefined rare signals (s2[89] and s5[121] 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