AES-T2000

- Trojan description
  - After detecting a specific sequence of input plaintext, the Trojan leaks the secret key of AES-128 through the leakage current. The leakage circuit (LC) consists of a shift register holding the secret key and two inverters. The least significant bit is connected to one inverter whose output connected to the input of the other inverter. Whenever the least significant bit of the shift register is '0', a direct path between power and ground composed by the PMOS of the first inverter and the NMOS of the second inverter is created for a limited time. Therefore, the secret key can be retrieved by measuring the leakage current.

- Trojan taxonomy
  - Insertion phase: Design
  - Abstraction level: Register Transfer level
  - Activation mechanism: Internally conditionally triggered
  - Effects: Leak Information
  - Location: Processor
  - Physical characteristics: Functional

Please send your concerns/questions to

Dr. Hassan Salmani at SalmaniHSN@gmail.com

Administrator at admin@trust-hub.org