AES-T1400

- Trojan description
  - Once a predefined sequence of input plaintext is observed, the Trojan demonstrates an attack on the AES-128 block-cipher and its corresponding key schedule. The idea is to artificially introduce leaking intermediate states in the key schedule that depend on known input bits and key bits, but that naturally would not occur during regular processing of the cipher. The Trojan uses AND conjunctions to pairwise combine each key bit with another input bit. The output of the AND gates are then combined to the leaked intermediate value by XORing all of them. The Trojan leaks one byte of the AES round key for each round of the key schedule. The leakage circuit (LC) is a 16-bit shift register and loaded it with an initial alternating sequence of zeros and ones. The shift register is only enabled in case the input to the leakage circuit is one, which results in an additional dynamic power consumption [1].

- Trojan taxonomy
  - Insertion phase: Design
  - Abstraction level: Register Transfer level
  - Activation mechanism: Triggered Internally
  - 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

Reference:

[1] L. Lin, M. Kasper, T. Güneysu, C. Paar and W. Burleson, "Trojan Side-Channels: Lightweight Hardware Trojans through Side-Channel Engineering," 11th International Workshop Cryptographic Hardware and Embedded Systems (CHES), pp. 382-395, 2009.