

AES-T800

🔑 Trojan description

- 🔑 Once a predefined sequence of input plaintext is observed, the Trojan leaks the secret key from a cryptographic chip running the AES algorithm through a covert channel. The channel adapts the concepts from spread spectrum communications (also known as Code-Division Multiple Access (CDMA)) to distribute the leakage of single bits over many clock cycles. The Trojan employs this method by using a pseudo-random number generator (PRNG) to create a CDMA code sequence, the PRNG initialized to a predefined value. The code sequence is then used to XOR modulate the secret information bits. The modulated sequence is forwarded to a leakage circuit (LC) to set up a covert CDMA channel in the power side-channel. The LC is realized by connecting eight identical flip-flop elements to the single output of the XOR gate to mimic a large capacitance [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.**