MEJOR ARTíCULO CIENTÍFICO del mes de Diciembre en la EPS 2020

Escuela Politécnica Superior

Francisco Eugenio Potestad Ordóñez – Departamento de Tecnología Electrónica

Sensors 2020, 20, 6909 - ***Q1***
https://doi.org/10.3390/s20236909

Título: Breaking Trivium Stream Cipher Implemented in ASIC using Experimental Attacks and DFA

Uno de los mejores métodos para aumentar la seguridad de los sistemas criptográficos utilizados para intercambiar información sensible, es atacarlos para encontrar sus vulnerabilidades y fortalecerlos en diseños posteriores. El cifrador de flujo Trivium es uno de los cifradores lightweight estándar diseñado para aplicaciones de seguridad en el Internet de las cosas (IoT por sus siglas en inglés). En el trabajo presentado se lleva a cabo un setup completo para atacar implementaciones ASIC del cifrador Trivium que permite recuperar las claves secretas utilizando ataques activos no invasivos mediante manipulación de la señal de reloj y combinándolo con un análisis diferencial de fallos (DFA por sus siglas en inglés). El sistema de ataque es capaz de inyectar fallos transitorios en el cifrador en un ciclo de reloj determinado y capturar los flujos cifrados erróneos. A partir de estos, es posible recuperar la clave secreta del dispositivo mediante un criptoanálisis DFA gracias a la comparación de los flujos cifrados correctos y erróneos. Además, se ha diseñado un cifrador Trivium inverso que permite recuperar las claves secretas a partir de un estado interno conocido. La recuperación de claves secretas ha sido verificada con numerosos datos de ataques por simulación y mediante datos experimentales obtenidos sobre el circuito ASIC. La clave secreta ha sido recuperada en el 100% de los casos considerando un escenario real con el mínimo de suposiciones necesarias.