Abstract

This paper discusses the crypto engine within the DRAM controller and how to defend it against possible attacks which might permit access to the encrypted data stored within the DRAM by means of different attack vectors.

Contents

Libre Silicon DRAM encryption

David Lanzendörfer

May 28, 2018

The idea is to protect the DRAM from extraction by an attacker using for instance the cold boot attack[1], by having the store and fetch operations being piped through a crypto unit which then transparently encrypts and decrypts the data using a key which is dynamically generated during power up.

[1] https://en.wikipedia.org/wiki/Cold_boot_attack

1 The crypto engine

2 Attack vectors

2.1 JTAG