

Abstract

Copyright © 2017 LANCEVILLE TECHNOLOGY GROUP CO., LIMITED. All rights reserved.

This process is licensed under the Libre Silicon public license; you can redistribute it and/or modify it under the terms of the Libre Silicon public license as published by the Libre Silicon alliance, either version 1 of the License, or (at your option) any later version.

This design is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the Libre Silicon Public License for more details.

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

1 The crypto engine 4

2 Attack vectors 5

2.1 JTAG 5

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 attack¹, 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.

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

1 The crypto engine

2 Attack vectors

2.1 JTAG