Partition-Based Security
Reference Design

1.0 **Reference Design Datasheet**

Description

The Partition-Based Security reference design demonstrates a secure way of assignment of security keys to multiple encrypted partial regions in the FPGA. This design can be used for different applications that consist of separate partitions reconfigured in an FPGA such as data center, secure communications, military, Multi-Tenancy, etc.

In Commercial Off-The-Shelf (COTS) boards, vendors may like to secure part of their design that is proprietary and allow end users to have flexibility in securing their design within the remainder of the FPGA fabric.

Partition-Based Security can also be utilized in commercial security applications. Within the data center, FPGA's may serve as accelerator platforms for multiple cloud instances, with each accelerator PR region requiring separate key protections.

In automotive applications, parts of the design are deployed to different vendors or collaborators. In some cases, the end user may want to do design modifications without affecting the existing design.

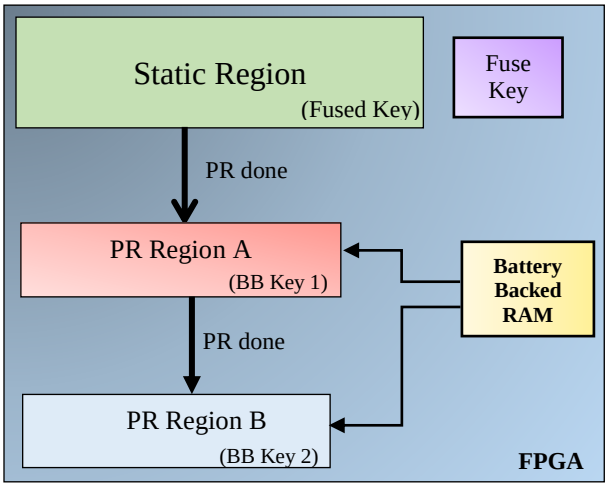
The Partition-Based Security reference design is an example of how we can protect PR regions in FPGA using different keys. The design allows in-field key update in Tamper protection and JTAG secure modes for Arria 10 FPGA. The security use case discussed is applicable to users who are concerned with implementing multi-level security in parts of their design.

Features

- Secure Partial Reconfiguration (PR)
- Simultaneous support for both OTP key and battery-backed key
- Qcrypt Security Tool
- PR Configuration from EPCQ flash
- Intel Arria 10 SOC Dev Kit DK-SOC-10AS066S-A

Applications

- Data Center/ Multi-Tenancy
- Automotive
- Secured Communications
- Commercial Off-The-Shelf (COTS) boards
- Applications requiring multi-level security



101 Innovation Drive San Jose, CA 95134

March 2017 Intel