**REPORT OF STRATIX 10 FPGA SRAM PUF**

**INTRODUCTION:**

For the past decade, there has been a huge rise in the investment made by all the FPGA Company providers for investing in their security features. These features have existed for several generations of FPGA Families, and focuses on the encryption and authentication of configuration bit streams. Over time, many of these have proven to be useful and valuable and some to be vulnerable to published attacks and probing techniques.

Just as the explosive growth of cloud computing, software as a service and the ‘Internet Of Things’ have introduced new classes of threats to the internet (i.e cyber security), the potential malicious attacks on FPGA’s and SoC’s.

In SRAM and Flash device configuration processes, fixed state machines manage the order of authentication, decryption and decompression and actual device configuration. Intel has recognized these challenges and requirements across users of FPGA security features and responded with the device of security architecture [1].

**OVERVIEW OF SDM OF INTEL STRATIX 10:**

A screenshot of a social media post

Description generated with very high confidence

SDM Provides a high level summary of the Intel Stratix 10 functional blocks. The SDM is the point of entry to the FPGA for JTAG commands and interfaces as well as for device configuration data(from flash, SD card or through PCI Express). The first component of configuration data and microcode for SDM itself, which is authenticated with one or more digital signatures. Once the SDM is configured and processors are released from the reset, the SDM block manages all Intel Stratix 10 FPGA or ‘SOC Security’ and configuration functions.

SDM ENABLED SECURITY FUNCTIONS:

New security features have been introduced with each generation of FPGA and SOC Products. Intel stratix 10 FPGA’s continue to support these features, including bit stream encryption and authentication, volatile and non- volatile key storage, JTAG and test mode disable and tamper detection sensors and monitors (voltage and temperature).

PHYSICAL UNCLONABLE PROTECTION FOR KEY MATERIAL, PROTECTION AND IDENTITY:

Intel Stratix 10 FPGA enable users access to PUF as a part of device configuration process for key protection and key material generation or for device identification purposes.

The Stratix 10 FPGA uses a SRAM initialization pattern which is available in SDM through a dedicated field of SRAM cells that are powered up only when generating a PUF value.

Intel selected this algorithm from partner **IntrinsicID**, based on superior characterization data of SRAM cells generated on Intel’s 14 nm process technology.

The **IntrinsicID PUF algorithm** runs as an instruction code in the SDM, and is only incorporated in the SDM configuration of IntrinsicID licensees. The PUF function relies on dedicated hardware sources of entropy, but also has a software upgradeable algorithmic component to address changes and fixes resulting from longer lifetime characterization activities. It provides a firmware based methodology for algorithmic tuning and optimization as more characterization data becomes available.

ADVANCED KEY MANAGEMENT SCHEMES ENABLED BY SECURE PROCESSOR:

One of the advanced use cases enabled by the SDM is the key management and encryption key updating for intel stratix 10 FPGA’s and SOC’s. In this case, either the SDM code itself or an external command authenticated by the SDM, introduces new encryption key material into the SDM cache memory. Encryption keys can be used for securing and authenticating communication with external devices, for encrypting and decrypting sector configuration data, or applying new signatures to data processed within the FPGA. Encryption key updates can be effective as long as the device is powered.

SECTOR BASED CONFIGURATION:

One of the of important features that enables SDM use cases is the logical separation of the device into configuration sectors. Dividing FPGA configuration into logical sectors helps manage configuration times and bottlenecks when configuring very large devices.

After configuring data is authenticated and decrypted using the high performance encryption accelerator cores, configuring data blocks are distributed to the various sectors in parallel on a configuration network.

SECTOR LAYOUT:

FPGA Configuration sectors are a fixed size across the intel stratix 10 family, allowing for a natural design boundaries for IP re-use, security and reconfiguration. The sectors are logical for configuration purposes, but otherwise overlay the normal rows and columns of routing logic. There is no impact to Intel to Quartus prime Software Place and route or logical timing from logical and data paths that cross sector boundaries.

LOCAL SECTOR MANAGER:

Within each sector is another microprocessor called the local sector manager(LSM), The LSM parses sector configuration block data and configures the logic elements for each sector. After configuration, these microprocessors monitor for single event upsets at the sector level, process scripted responses to these SEU’s and can perform hashing in real time.

SECTOR BASED RECONFIGURATION:

AS we know that the device is divided into logical sectors, we can quickly reconfigure a portion of the Intel stratix 10 FPGA design. Because you configure the FPGA by logical sector, you can use a subset of this configuration process to reconfigure a subset of the sectors.

ZEROING DESIGN INFORMATION BY SECTOR IN PARALLEL:

Zeroing encryption keys or data is a common response mechanism when device sensors or I/O detect common signatures of an attack to probe the FPGA for sensitive data.

CONFIGURATION PROCESS:

Intel Stratix 10 FPGA’s and the SDM block provide the most robust and secure and authenticated device configuration process in the industry. Some customization is also available in the configuration processes and IP protection for each user design.

Figure 3 starts with a basic block diagram of the configuration data for a intel stratix 10 FPGA or SOC design. The configuration block data is the same in flash memory, SD card or over a hard PCI Express Connection. These configuration data is divided into several logical pieces of FPGA Sectors and code blocks for the hard processor systems.

LOADIN AND AUTHENTICATING THE CONFIGURATION IMAGE:

The first step is loading the SDM data. This stage manages all other security and keys for the Intel Stratix 10 FPGA. SDM data is 100% authenticated against an intel signature and verified with an on-chip Intel public encryption key. Other configuration option allow the designer to provide their own SDM image signature using private encryption key and then verify this signature in configuration with a user installed public encryption key.

VARIABLES MANAGED BY THE SDM:

SDM decides depending on user’s decision how to take, process and configure the remainder of the user design. These decisions include the configuration order of the Intel stratix 10 device. (FPGA first or HPS First and specific order of FPGA sector configuration). SDM instructions can also indicate thresholds and responses for environmental monitors. Licensable functions like the PU are optionally included in SDM code based on Quartus licenses.

AUTHENTICATING, DECRYPTING AND CONFIGURING BY SECTOR:

A key, flexible feature of the Intel Stratix 10 SDM Block is the ability to make a separate encryption and source encryption key decisions for the FPGA design on a logical sector basis. In this case, the designer can select different encryption keys for each sector or use a variety of encryption keys based on the sector sensitivity level. Different encryption key handling procedures can be designed for keys at different security. An encryption key can be used across multiple sectors, to reduce the attack surface of that design sector. All device decryption is protected by the device’s root key.

ADDRESSING SIDE CHANNEL LEAKAGE THROUGH PROGRAMMABILITY:

One of the most common, documented attacks on existing programmable logic devices are side channel leaks on the configuration process, primarily targeting power. Intel Stratix 10 devices use a variety of methods to limit side channel leakage and attack surfaces. These methods include the pre-authentication of all sector based data blocks by the SDM before encryption, dynamic encryption key updates, and encryption key diversity across sectors. The SDM itself is a key tool for reducing side channel leakage, as well as the many configuration methods available to the user. The configuration process ca be specific to a design and can scramble or randomize the configuration data processing order. The SDM controls the configuration scheme for each design. If a particular configuration process is found effective against the threat profile of user environment.