**FTR-SE (Farimah Tehranipoor Rahman - Security Engine)**

Project Description:

FTR-SE is an open-source security subsystem developed by the Florida Institute of Cybersecurity (FICS) Research at the University of Florida. The primary aim of this project is to provide a RISC-V based security subsystem for System-on-Chip (SoC), enabling robust hardware security functionalities. FTR-SE addresses semiconductor supply chain vulnerabilities and incorporates various hardware primitive components, including Physical Unclonable Function (PUF), True Random Number Generator (TRNG), symmetric and asymmetric crypto accelerators, and life cycle management features.

**Key Features**

* **RISC-V Based:** FTR-SE leverages the RISC-V architecture, a free and open-source instruction set architecture, providing flexibility and openness.
* **Semiconductor Supply Chain Protection:** The project focuses on mitigating vulnerabilities in the semiconductor supply chain through the innovative fast Power On Chip Authentication (POCA) protocol, ensuring the integrity and security of hardware components.
* **Hardware Primitives:**
  + **PUF (Physical Unclonable Function):** FTR-SE incorporates PUF as a hardware primitive, contributing to secure key generation and authentication.
  + **TRNG (True Random Number Generator):** A robust TRNG is integrated for secure and unpredictable random number generation.
* **Crypto Accelerators:**
  + **Symmetric Crypto Accelerator:** Enables efficient symmetric cryptographic operations for secure data encryption and decryption.
  + **Asymmetric Crypto Accelerator:** Supports asymmetric cryptographic algorithms for secure key exchange and digital signatures.
* **Life Cycle Management:** FTR-SE includes features for managing the life cycle of the security subsystem, ensuring secure initialization, updates, and retirement.
* **MailBox:** FTR-SE incorporates a MailBox IP, facilitating secure communication between the Host processor and the RISC-V processor without relying on memory transactions.

**Block Diagram**

A diagram of a computer program

Description automatically generated

**Getting Started**

To use FTR-SE in your project, follow these steps:

* **Clone the Repository:**

git clone <https://github.com/mashahedurrahman/Security-Engine>

* **Build and Configure:**

1. Modify the TOP variable in ./ci/path-setup.sh
2. source sys\_ready.sh

* **Run the examples:**

1. Run "./gcc\_script.sh" to compile the C code
2. Run "./run.sh" to run simulation
3. Use "simvision ./xrun\_results/dump.vcd" to observe waveform

**Contact:**

For inquiries or more information, contact the project maintainers:

* Mridha Md Mashahedur Rahman (mrahman1@ufl.edu)
* Sujan Kumar Saha (sujansaha@ufl.edu)

Feel free to explore and contribute to FTR-SE! Your input is valuable in advancing hardware security in the open-source community.

**Reference Publication:**

Mohammad, Sajeed, Mridha Md Mashahedur Rahman, and Farimah Farahmandi. "Required Policies and Properties of the Security Engine of an SoC." *2021 IEEE International Symposium on Smart Electronic Systems (iSES)*. IEEE, 2021.