Building Chipwhisperer Firmware with the SecAES-STmega8515 Library

Prepared by: Shane Reilly

Email: reillysp@mail.uc.edu

Class of CS 2023, University of Cincinnati

This document explains how to compile the masked AES for XMEGA (ChipWhisperer) used for the following paper:

Chenggang Wang, Jimmy Dani, Shane Reilly, Austhen Brownfield, Boyang Wang, John Emmert, "TripletPower: Deep-Learning Side-Channel Attacks over Few Traces," IEEE International Symposium on Hardware Oriented Security and Trust (HOST 2023), San Jose, CA, USA, May 1-4 2023

The purpose of this document is to provide instructions on how to compile the secAES-STmega8515 library and then load it onto the ChipWhisperer ATXMEGA128D4 target board. These instructions assume that you are using the virtual machine provided by ChipWhisperer that is available under the releases tab of their GitHub repo (https://github.com/newaetech/chipwhisperer/releases) and that is already set up with their provided directions (located at https://chipwhisperer.readthedocs.io/en/latest/installing.html).

1. On the Chipwhisperer virtual machine, navigate to the firmware directory:

   ```
   cd    ~/work/projects/chipwhisperer/hardware/victims/firmware
   ```

2. Create a new directory and copy the contents of simpleserial-aes into it

   ```
   mkdir test1 && cp -r simpleserial-aes/* test1/
   ```

3. Navigate to the secAES repo and download it. Initialize the git submodule.

   ```
   cd
   crypto
   git submodule update –-init secAES-ATmega8515
   ```

4. Edit **`Makefile.maskedaes`** with a text editor. Change the line :

   ```
   else ifeq ($(HAL), avr)
   ```

   to

   ```
   else ifeq ($(HAL), $(filter $(HAL), avr xmega))
   ```

Be careful not put any superfluous tabs or spaces in. Make is very sensitive to spaces and tabs.

5. Navigate back to the directory created earlier and build the firmware.

```
cd     ~/work/projects/chipwhisperer/hardware/victims/firmware/test1
make PLATFORM=CWLITEXMEGA CRYPTO_TARGET=MASKEDAES
CRYPTO_OPTIONS=ANSSI+VERSION1
```

6. Now, this firmware has been built and can be flashed on to the board.