FINAL PROJECT – HARDWARE TROJAN

Hardware Security

CPE426

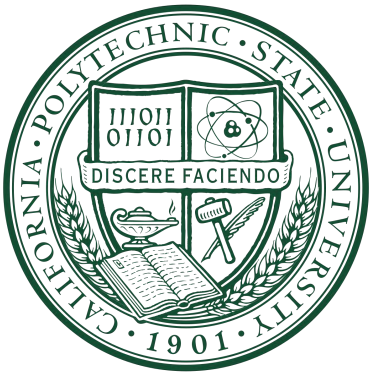
Fall Quarter 2023

Instructor: Dr. Beard

Team Evergreen

[redacted]

Date: November 30, 2023



0. Trojan-Free Module Function

Our module is an AES encryption and ciphertext broadcasting system. Applications for such a module are widely applicable, functioning as a means to wirelessly establish trust between communications devices, or verifying device integrity, to much more. Utilizing radio waves, the module takes in a 128 bit plaintext and key, AES-128 encrypts the plaintext, and broadcasts the bits one-by-one over radio frequency. It accomplishes this with three sub modules; 1. The AES encryption module, output buffer module, and Ultra-Wide Band (UWB) transmitter. The UWB transmitter takes in one bit per clock cycle, and uses two baseband and two radio frequency (RF) pulse generator units, one for the “1” bit and one for the “0” bit, each, as seen in Figure 1. Both baseband pulse generators get the same input, so thus flattens the bit using a return to zero function when the bit it receives is opposite. The frequency shift keying function modulates the signal for the RF pulse generator. The output of both pulse generators is filtered through an OR gate, and sent to a power amplifier module. For purposes of practical application and testing validation, the power amplifier module is disconnected. This means that the outgoing signal is not at the correct power levels for radio transmission; however, the unboosted signal is sufficient for power wave measurements with an oscilloscope.

1. AES128 Encryption Module Functional Description

The AES-128 encryption module, developed by Michael Muehlberghuber and acquired from github, operates by first expanding a 128-bit key into a series of round keys. The plaintext undergoes a series of rounds, each involving operations such as SubBytes (non-linear substitution), ShiftRows (permutation of bytes), and MixColumns (transformation combining column data). After 10 rounds, the result is the ciphertext. Decryption involves reversing these steps, starting with the key expansion and using inverse operations for decryption. The 128-bit signal is sent to an output buffer, which sends the ciphertext one bit at a time. The AES module is pre-loaded with dummy plaintext and cipherkey, for demonstration purposes.

2. Ultra Wide Band Transmitter

The Ultrawideband (UWB) transmitter module uses two sets of two pulse generators – one set for zeros, and one set for ones. The baseband generators create digital signals representing binary information. These signals are then sent through radiofrequency pulse generators, with each generator responsible for encoding either a zero or a one. The outputs are OR’ed and sent to a power amplifier module, which is sent to the antenna.

3. Schematics and Controls

The only applicable user inputs are switch15, which is used to send the ciphertext to the UWB transmitter, and the reset button found in the center of the button cluster. The UWB output is sent to the JXADC pinout K3.