MAX32600 AES Demonstration

April 3, 2015

Abstract

This document describes the AES sample application provided for the MAX32600. The demonstration uses NIST test vectors for each supported key size and will report self-test pass or failure of those vectors.

Requirements

- MAX32600B EvKit
- Sample code for this application located in `Firmware/Applications/AESDemo`
- Olimex JTAG ARM-USB-TINY-H
- GNU ARM toolchain

Setup

- Compile the project using 'make' to generate an elf file.
- Connect the Olimex to the Ev Kit's JTAG connector.
- Use 'make upload' to load the compiled max32600.elf file onto the MAX32600 EvKit.
- Connect to the serial interface using a terminal program (kermit, minicom, PuTTY) with the following settings:
  - Baud rate: 115200
  - Parity: None
  - Data bits: 8
  - Stop bits: 1
  - Flow control: None

Observation

- The serial port output from the EV Kit will display the result of each self-test.

Example:
MAX32600 AES NIST Monte-Carlo Test Vector Demo

– Synchronous API –
Running 128-bit encrypt .. pass
Running 128-bit decrypt .. pass
Running 192-bit encrypt .. pass
Running 192-bit decrypt .. pass
Running 256-bit encrypt .. pass
Running 256-bit decrypt .. pass

– Asynchronous API –
Running 128-bit encrypt .. pass
Running 128-bit decrypt .. pass
Running 192-bit encrypt .. pass
Running 192-bit decrypt .. pass
Running 256-bit encrypt .. pass
Running 256-bit decrypt .. pass

Tests complete: 12 tests passes, 0 tests failed