Keywords: Alcatraz (MAXREFDES34), subsystem reference design, FPGA security, SHA-256 authentication, IP protection

SUBSYSTEM BOARD 5822

Alcatraz (MAXREFDES34#): SHA-256 Secure Authentication Design

By: Michael D'Onofrio

Feb 12, 2014

Abstract: The Alcatraz (MAXREFDES34#) subsystem provides a reference design for securing Xilinx FPGAs to protect IP and prevent attached peripheral counterfeiting. The system implements a SHA-256 challenge-response between the FPGA and a DS28E15 secure authenticator. Boards for purchase, hardware, and firmware design files provide complete system information for rapid prototyping and development.

Introduction



Smart factories, industrial and medical applications employ the flexibility and high performance of modern FPGAs. As these systems become increasingly connected, security emerges as a paramount feature to protect IP, enable system features using software and prevent counterfeiting. The Alcatraz (MAXREFDES34#) subsystem reference design uses the DS28E15 to immediately implement SHA-256 authentication on Xilinx® FPGAs. The DS28E15 communicates over the single-contact 1-Wire® bus, reducing the number of pins necessary to carry out the solution. The reference code defines a combined SHA-256 processor and 1-Wire Master on the host FPGA.

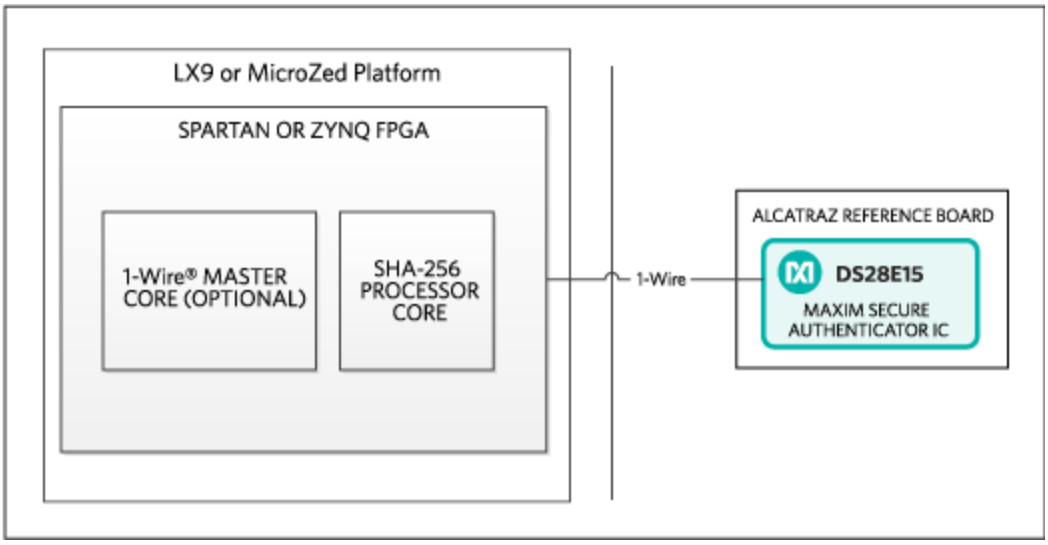


Figure 1. The Alcatraz subsystem design block diagram with development platform.

Features

- SHA-256 authentication
- Single-contact 1-Wire interface
- Example source code
- Pmod™-compatible form factor

Applications

- Counterfeit protection
- Peripheral authentication
- IP protection
- License and feature management

Competitive Advantages

- Crypto-strong authentication
- Single pin count interface
- Fast performance with hardware acceleration

Detailed Description of Hardware

Alcatraz interfaces with FPGA development boards using a 6-pin Pmod connector as illustrated. When plugging Alcatraz into a host board, make sure to correctly align the pins with the host Pmod connector, as shown in **Figure 2**.

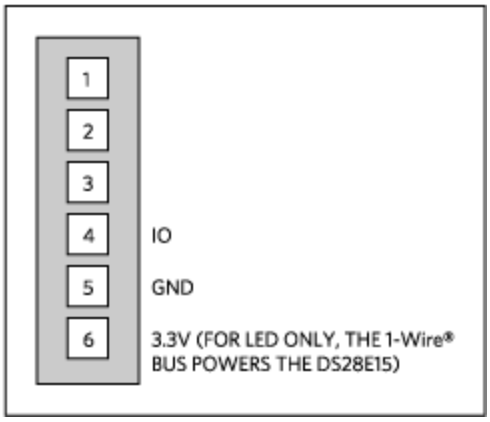




Figure 2. The Alcatraz subsystem design correctly inserted into the MicroZed development platform.

Table 1 shows the supported platforms and ports.

Table 1. Supported Platforms and Ports

Supported Platforms	Ports
LX9™ 3 platform (Spartan®-6)	J5
MicroZed™ platform (Zynq®-7000)	J5

For symmetric authentication schemes like SHA-256, protection of both the secure authenticator secret key, along with the FPGA secret key, are important. Symmetric authentication implementations with poor

®

FPGA secret key security can be risky. To this end, the DS28E15 uses DeepCover technology to protect against invasive and noninvasive attacks on its secret key; the reference design spells out various techniques to protect the FPGA secret key.

Additional detail on secret key protection techniques may be found in application note 5803, "Secure Your FPGA System Using a DeepCover Secure Authenticator."

Detailed Description of Firmware for LX9 Platform

Table 1 shows currently supported platforms and ports. Support for additional platforms may be added periodically under Firmware Files in the All Design Files section.

The firmware allows for immediate interfacing to the hardware. The firmware is written in Verilog, developed using the Xilinx SDK tool, based on the Eclipse™ open source standard.

The firmware program sequence is used to compute and lock the secret (CLS), write page data to the DS28E15, and authenticate the DS28E15. The complete source code speeds customer development. Code documentation resides in the corresponding firmware platform files.

Detailed Description of Firmware for MicroZed Platform

The Alcatraz firmware design also supports the MicroZed kit and targets an ARM® Cortex® -A9 processor placed inside a Xilinx Zynq system-on-chip (SoC).

The firmware allows for immediate interfacing to the hardware. The firmware is written in C, developed using the Xilinx SDK tool, based on the Eclipse™ open source standard.

The firmware program sequence is used to compute and lock the secret (CLS), write page data to the DS28E15, and authenticate the DS28E15. The complete source code speeds customer development. Code documentation resides in the corresponding firmware platform files.

Quick Start

Required equipment:

- Windows® PC with two USB ports
- Alcatraz (MAXREFDES34#) board
- Alcatraz-supported platform (i.e., LX9 development kit or MicroZed kit)

Detailed setup and programming instructions are included in the README.txt file within the provided firmware files.

All Design Files

Download All Design Files

Hardware Files

Schematic
Bill of materials (BOM)
PCB layout
PCB Gerber

Firmware Files

The associated firmware files LX9 Platform (Spartan-6) and ZedBoard Platform (Zynq-7000) are available upon request. Please contact us.

Buy Reference Design

Buy Direct: Alcatraz (MAXREFDES34#)

Or

Order the Alcatraz reference design (MAXREFDES34#) from your local Maxim representative.

1-Wire is a registered trademark of Maxim Integrated Products, Inc.
ARM is a registered trademark and registered service mark of ARM Limited.
Cortex is a registered trademark of ARM Limited.
DeepCover is a registered trademark of Maxim Integrated Products, Inc.
Eclipse is a trademark of Eclipse Foundation, Inc.
HyperTerminal is a registered trademark of Hilgraeve, Incorporated.
ISE is a registered trademark of Xilinx, Inc.
Pmod is a trademark of Digilent Inc.
Spartan is a registered trademark of Xilinx, Inc.
Windows is a registered trademark and registered service mark of Microsoft Corporation.
Windows XP is a registered trademark and registered service mark of Microsoft Corporation.
Xilinx is a registered trademark and registered service mark of Xilinx, Inc.
ZedBoard is a trademark of ZedBoard.org.
Zynq is a registered trademark of Xilinx, Inc.

Related Parts		
DS28E15	DeepCover Secure Authenticator with 1-Wire SHA-256 and 512-Bit User EEPROM	Free Samples

More Information
For Technical Support: http://www.maximintegrated.com/support

For Samples: http://www.maximintegrated.com/samples
Other Questions and Comments: http://www.maximintegrated.com/contact

---

Application Note 5822: http://www.maximintegrated.com/an5822
SUBSYSTEM BOARD 5822, AN5822, AN 5822, APP5822, Appnote5822, Appnote 5822
© 2013 Maxim Integrated Products, Inc.
Additional Legal Notices: http://www.maximintegrated.com/legal