Cryptographic Engine (CRE) Demo for CertusPro-NX

User Guide

FPGA-UG-02193-0.80

September 2023
Disclaimers

Lattice makes no warranty, representation, or guarantee regarding the accuracy of information contained in this document or the suitability of its products for any particular purpose. All information herein is provided AS IS, with all faults and associated risk is the responsibility entirely of the Buyer. The information provided herein is for informational purposes only and may contain technical inaccuracies or omissions, and may be otherwise rendered inaccurate for many reasons, and Lattice assumes no obligation to update or otherwise correct or revise this information. Products sold by Lattice have been subject to limited testing and it is the Buyer’s responsibility to independently determine the suitability of any products and to test and verify the same. LATTICE PRODUCTS AND SERVICES ARE NOT DESIGNED, MANUFACTURED, OR TESTED FOR USE IN LIFE OR SAFETY CRITICAL SYSTEMS, HAZARDOUS ENVIRONMENTS, OR ANY OTHER ENVIRONMENTS REQUIRING FAIL-SAFE PERFORMANCE, INCLUDING ANY APPLICATION IN WHICH THE FAILURE OF THE PRODUCT OR SERVICE COULD LEAD TO DEATH, PERSONAL INJURY, SEvere PROPERTY DAMAGE OR ENVIRONMENTAL HARM (COLLECTIVELY, "HIGH-RISK USES"). FURTHER, BUYER MUST TAKE PRUDENT STEPS TO PROTECT AGAINST PRODUCT AND SERVICE FAILURES, INCLUDING PROVIDING APPROPRIATE REDUNDANCIES, FAIL-SAFE FEATURES, AND/OR SHUT-DOWN MECHANISMS. LATTICE EXPRESSLY DISCLAIMS ANY EXPRESS OR IMPLIED WARRANTY OF FITNESS OF THE PRODUCTS OR SERVICES FOR HIGH-RISK USES. The information provided in this document is proprietary to Lattice Semiconductor, and Lattice reserves the right to make any changes to the information in this document or to any products at any time without notice.
Cryptographic Engine (CRE) Demo for CertusPro-NX
User Guide

Contents

Acronyms in This Document ................................................................. 6
1. Introduction .................................................................................. 7
   1.1. Validated Configuration .................................................... 7
2. Features ....................................................................................... 8
3. Demo Requirements ...................................................................... 9
   3.1. Hardware Requirements .................................................. 9
   3.2. Software Requirements .................................................. 9
4. Setting Up Projects ....................................................................... 10
   4.1. Importing an existing Propel SoC Project ....................... 10
   4.2. Generating a Lattice Radiant Project ......................... 12
   4.3. Importing a Propel RISC-V Project ......................... 13
   4.4. Programming the Board ............................................... 14
   4.5. Testing the design using Propel Debugger ............... 16
References ....................................................................................... 21
Technical Support Assistance ............................................................ 23
Revision History .............................................................................. 24
Figures
Figure 4.1. Importing Propel SoC Project..............................................................................................................10
Figure 4.2. CRE Demo SoC Project Schematics........................................................................................................11
Figure 4.3. CRE Demo SoC Project Memory Address Mapping ..................................................................................11
Figure 4.4. Launch Radiant from Propel Builder ......................................................................................................12
Figure 4.5. Setting Top-Level Unit to "cre_wrapper.v".................................................................................................12
Figure 4.6. Radiant Project Compilation .....................................................................................................................12
Figure 4.7. Importing Propel Project ..........................................................................................................................13
Figure 4.8. Propel Build Project Successful Console Message .....................................................................................13
Figure 4.9. Launch Programmer ....................................................................................................................................14
Figure 4.10. Radiant Programmer Configuration ........................................................................................................14
Figure 4.11. Cable Setup ..............................................................................................................................................15
Figure 4.12. Selecting Cable ........................................................................................................................................16
Figure 4.13. Programming the Device .........................................................................................................................16
Figure 4.14. Launch Terminal Window .......................................................................................................................17
Figure 4.15. Launching Debug Configurations ........................................................................................................17
Figure 4.16. GDB OpenOCD Debugging Window ........................................................................................................18
Figure 4.17. Debugger Cable and Device Settings .......................................................................................................18
Figure 4.18. Run Debugger ..........................................................................................................................................19
Figure 4.19. Demo Design Message ...........................................................................................................................20
Tables
Table 1.1. IP Version ......................................................................................................................................................7
Table 4.1. Exported Signals ..............................................................................................................................................11
# Acronyms in This Document

A list of acronyms used in this document.

<table>
<thead>
<tr>
<th>Acronym</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>AES</td>
<td>Advanced Encryption Standard</td>
</tr>
<tr>
<td>APB</td>
<td>Advanced Peripheral Bus</td>
</tr>
<tr>
<td>CRE</td>
<td>Cryptographic Engine</td>
</tr>
<tr>
<td>LMMI</td>
<td>Lattice Memory Mapped Interface</td>
</tr>
<tr>
<td>SHA</td>
<td>Secure Hash Algorithm</td>
</tr>
<tr>
<td>SoC</td>
<td>System on a Chip</td>
</tr>
<tr>
<td>UART</td>
<td>Universal Asynchronous Receiver/Transmitter</td>
</tr>
<tr>
<td>USB</td>
<td>Universal Serial Bus</td>
</tr>
</tbody>
</table>
1. Introduction

This document provides instructions on how to set up and use the CRE Module IP with CertusPro™-NX devices. This document includes the following topics:

- Setting up the demo
- Programming the board
- Testing the design on the board with Lattice Propel™ software

CRE stands for Cryptographic Engine, which is a module built on the Security Hard IP. This module includes the following features:

- Supports the following user mode security features:
  - High throughput Secure Hash Algorithm – 256 bits (SHA 256)
  - Hash Based Message Authentication Code – HMAC-SHA
- Supports True Random Number Generation
- Supports multiple bus interfaces:
  - Lattice Memory Mapped Interface (LMMI)
  - LMMI + FIFO (High-speed SHA/AES)
  - Advanced High-Performance Bus (AHB) – Lite
  - Advanced Peripheral Bus (APB)

1.1. Validated Configuration

- Board: This module functions on the CertusPro-NX Evaluation Board and is also compatible with the CertusPro-NX Versa Board and CertusPro-NX PCIe Bridge Board.
- Lattice Radiant™ Version: 2022.1.1.289.4
- Lattice Propel Version: 2022.1.2211240753

<table>
<thead>
<tr>
<th>Table 1.1. IP Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Name</td>
</tr>
<tr>
<td>CRE</td>
</tr>
<tr>
<td>OSC for CRE</td>
</tr>
<tr>
<td>PLL</td>
</tr>
<tr>
<td>RISC-V MC</td>
</tr>
<tr>
<td>AHB Lite Interconnect</td>
</tr>
<tr>
<td>AHB Lite to APB Bridge</td>
</tr>
<tr>
<td>APB Interconnect</td>
</tr>
<tr>
<td>System_Memory</td>
</tr>
<tr>
<td>GPIO</td>
</tr>
<tr>
<td>APB Feedthrough</td>
</tr>
<tr>
<td>UART</td>
</tr>
</tbody>
</table>
2. Features

- Refer to CRE Module IP User Guide (FPGA-IPUG-02067) for supported features.
- Demonstrate the usage of the Secure Hash Algorithm – 256 bits (SHA-256).
- Demonstrate the usage of the Advance Encryption Standard – 128 Bits (AES-128).
3. Demo Requirements

3.1. Hardware Requirements

Hardware requirements for the demonstration:
- CertusPro-NX Evaluation Board or CertusPro-NX Versa Board
- USB connection for device programming
- USB connection for UART communication

3.2. Software Requirements

The following software are required for the steps outlined in this guide. Install the software in the order listed below:
1. Lattice Radiant v2022.1
2. Lattice Radiant v2022.1.1 – Service Pack
3. Lattice Radiant v2022.1.1 Control Pack CRE
   Contact Technical Support for the control pack
4. Lattice Propel v2022.1
4. Setting Up Projects

This section provides instructions on how to set up Lattice Propel software and Lattice Radiant software for Lattice CRE Demo for CertusPro-NX devices. A complete project contains three parts:

- Lattice Propel SoC project. The hardware portion of the project builds and generates the RISC-V SoC system that contains a CPU and peripherals that are instanced in the FPGA portion of CertusPro-NX using the Lattice Propel Builder.
- Lattice Radiant project. This portion of the project instantiates the CRE Module IP (only supported in Lattice Radiant software) and interfaces the CRE Module IP to the SoC system generated from Lattice Propel Builder. It is also used to synthesize, place and route, and generate the programming file to be loaded into the FPGA portion of CertusPro-NX devices.
- Lattice Propel RISC-V project. The software portion of the project is used to develop and test software codes running on the RISC-V processor using Lattice Propel software.

4.1. Importing an existing Lattice Propel SoC Project

To import the CRE Demo SoC project:

1. Unzip CPNX_CRE_DEMO.zip to C:\lscc.
2. In Lattice Propel Builder, import Demo SoC Project by clicking File > Open Design > Open C:\lscc\CPNX_CRE_DEMO\CPNX_CRE_Demo_Eval\CPNX_CRE_Demo\CPNX_CRE_Demo.sbx.

![Image](image.png)

Figure 4.1. Importing a Lattice Propel SoC Project

This SoC project uses RISC-V MC “Hello World” template with an APB Feedthrough IP to export out the APB interface ports as CRE Module IP is only available in the Lattice Radiant software. Refer to Figure 4.2 and Table 4.1 for signals exported out from Lattice Propel SoC Project.
Table 4.1. Exported Signals

<table>
<thead>
<tr>
<th>IP Name → Signal Name</th>
<th>Exported Signal Name</th>
<th>Direction</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>PLL → clki_i</td>
<td>pll_clki_i</td>
<td>Input</td>
<td>Export signal using Create Port feature, to be connected to OSC for CRE IP in Lattice Radiant software.</td>
</tr>
<tr>
<td>PLL → clkos_o</td>
<td>pll0_clkos_o</td>
<td>Output</td>
<td>Export signal using Create Port feature, to be connected to CRE Module IP in Lattice Radiant software.</td>
</tr>
<tr>
<td>RISC-V MC → system_resetn_o</td>
<td>cpu0_system_resetn_o</td>
<td>Output</td>
<td>Export signal using Create Port feature, to be connected to CRE Module IP in Lattice Radiant software.</td>
</tr>
<tr>
<td>APB Feedthrough → APB_M0</td>
<td>apb2cre_inst_APB_M0_interface</td>
<td>Inout</td>
<td>Export APB interface using Export Interface feature, to be connected to CRE Module IP's APB interface. Refer to Lattice-Propel-2022-1-Builder User-Guide (FPGA-UG-02177) for more information on the Export Interface.</td>
</tr>
</tbody>
</table>

Figure 4.3. CRE Demo SoC Project Memory Address Mapping

The CRE Module IP in this demo SoC project is configured and accessed using the APB Interface. Figure 4.3 shows the memory address mapping for the SoC project, with the APB interface designated for controlling and accessing the CRE Module IP starts at address 0x10000.

3. Generate a Lattice Radiant Project. Refer to the Generating a Lattice Radiant Project section.
4.2. Generating a Lattice Radiant Project

To generate a Lattice Radiant project from the CRE Demo SoC Project:

1. Launch Lattice Radiant software from Lattice Propel Builder by clicking Design > Run Radiant or clicking the icon.

![Figure 4.4. Launch Lattice Radiant from Lattice Propel Builder](image)

2. In Lattice Radiant software, Navigate to File List Hierarchy > right-click on the original top-level unit CPNX_CRE_Demo - CPNX_CRE_Demo.v > click Unset Top-Level Unit > right-click cre_wrapper.v > click Set as Top-Level Unit.

Note: cre_wrapper.v is a module that is used to instantiate OSC for CRE IP and CRE Module IP that is only supported in Lattice Radiant software. Its purpose is to provide an interface to the original module generated by Lattice Propel Builder without requiring any modifications to the original module.

![Figure 4.5. Setting Top-Level Unit to "cre_wrapper.v"](image)

3. Re-run synthesize flow.

![Figure 4.6. Lattice Radiant Project Compilation](image)

Note: Repeat steps 2 and 3 if the top-level unit is not cre_wrapper.v after any subsequent launch of Lattice Radiant software from Lattice Propel Builder. To prevent the top-level unit from being overwritten, launch Lattice Radiant software separately.
4.3. Importing a Lattice Propel RISC-V Project

To import the CRE Demo RISC-V software project:

1. In Lattice Propel workspace, click File > Import.
2. Select Existing Projects into Workspace under the General group.
3. Click Next.
4. In Import Projects page, choose Select Root Directory, click Browse and select the folder \lscc\CPNX_CRE_DEMO\CPNX-CRE-DEMO-C as shown in Figure 4.7.

5. Under Options, select Copy projects into workspace. This provides a new copy of the source files that can be modified.
6. Click Finish. This Lattice Propel project contains the CRE Demo RISC-V software project, which includes the main test program, a simple driver and header file for CRE.
7. Right-click the RISC-V software project CPNX-CRE-DEMO-C in the Project Explorer tab and select Build Project. The console window at the bottom of the screen displays the output as shown in Figure 4.8. This indicates a successful compilation. There should be no error in the console window and warnings can be safely ignored.

8. Make sure the executable file CPNX-CRE-DEMO-C.elf is generated in \lscc\CPNX_CRE_DEMO\CPNX-CRE-DEMO-C\Debug to be used in Testing the design using Lattice Propel Debugger section. Debugger downloads the executable file (.elf) into the target processor for software execution.
4.4. Programming the Board

This section provides instructions on how to program the board with the .bit files generated from Lattice Radiant software.

1. Launch Programmer from Lattice Radiant software by clicking **Tools > Programmer**.

   ![Figure 4.9. Launch Programmer](image)

2. In the **Radiant Programmer** window, ensure the **Device Family**, **Device** and **Operation** matches the configuration shown in **Figure 4.10**. Select the .bit file generated from the **Generating a Lattice Radiant Project** section.

   ![Figure 4.10. Radiant Programmer Configuration](image)
3. In the **Cable Setup** window, click **Detect Cable**.

![Cable Setup Window](image)

**Figure 4.11. Cable Setup**

4. In the **Select Cable** window, select the **FTUSB-0** option as shown in **Figure 4.12** and click **OK**.

**Note:** For CertusPro-NX boards, FTUSB-0 is connected to JTAG port. Refer to CertusPro-NX board schematic or diagram for more information.
Figure 4.12. Selecting Cable

5. Click Program Device. Status should display PASS and the console window at the bottom of the screen should display the logs as shown in Figure 4.13. This indicates that the configuration is successful.

Figure 4.13. Programming the Device

4.5. Testing the design using Lattice Propel Debugger

1. In the Terminal window, click Open a Terminal, this opens the Launch Terminal window.
2. In the Launch Terminal window, make the following selections.
   a. Choose terminal: Serial Terminal
   b. Serial Port: COMXX, choose the larger number. For example, if you see COM1 and COM2, choose COM2.
      Note: COMXX is the port on the laptop that represent UART. Refer to CertusPro-NX board schematic or diagram for more information.
   c. Baud rate: 115200
3. Click **OK**.

4. In Lattice Propel software, click **Run > Debug Configurations**

![Figure 4.14. Launch Terminal Window](image)

5. In the **Debug Configurations** window, select and double-click GDB OpenOCD Debugging. A window should appear on the right that automatically populates the fields as shown in **Figure 4.15**.

![Figure 4.15. Launching Debug Configurations](image)
6. Click on the **CableConn** tab.

7. Click **Detect Cable** and **Scan Device**. This automatically detects the FTUSB cable port and device. If not, check to ensure the connections and configurations of the board are set up properly and retry.

8. Click **Apply > Close**. This creates a debug configuration for the user which can be used to launch the program.
9. In the Propel main window, look for **Terminal** window. If not available, click **Window > Show View > Terminal**. This displays the output of the program through UART.

10. In the **Debug Configuration** window, select **CPNX-CRE-DEMO-C Debug** and click **Debug**.

![Debug Configurations](image)

Create, manage, and run configurations

![Run Debugger](image)

**Figure 4.18. Run Debugger**

11. In the Propel SDK window, you can see messages from the demo design in the Serial Terminal.
Figure 4.19. Demo Design Message
These messages show the demo design flow, demonstrating the usage of the SHA-256 encryption, AES-128 encryption, and AES-128 decryption. The demo software does not print messages for all the procedures involved to serial terminal. For the complete procedure and description, refer to CRE Module IP User Guide (FPGA-IPUG-02067).

For SHA-256 encryption, the demo starts by polling the CRE IP ready status, then the SHA data source is configured to be from APB bus before initializing and starting SHA engine. Message to be hashed with SHA-256 will then be written 1B at a time. The CRE IP will then be polled for the transaction done status before the encrypted SHA message is read and displayed in serial terminal.

For AES-128 encryption, the demo starts by polling the CRE IP ready status, then AES data source is configured to be from APB bus. Next, the CRE IP is configured with the AES encryption mode and the AES key size is set to 128 bits. The AES key is then written to memory address (0x2810) before the demo polls AES to finish key expansion and start the AES engine. The AES message to be encrypted will then be written into the IP. Afterward, the CRE IP will be polled for the AES finish encryption status. When encryption is done, the encrypted message will be read and displayed in the serial terminal.

For AES-128 decryption, the demo starts by polling the CRE IP ready status. The AES data source is then configured to be from APB bus. Next, the CRE IP is configured with the AES decryption mode and the AES key size is set to 128 bits. The AES key is then written to memory address (0x2810) before the demo polls AES to finish key expansion and start the AES engine.

Note that if AES encryption/decryption is being run back-to-back, value in memory address for AES STAT [1] will still be 1 and will not reset, hence the poll value will be 0x3. The AES message to be decrypted will then be written into the IP. Afterwards, the CRE IP will be polled for AES finish decryption status. Once decryption is done, the message is then read and displayed in the serial terminal.
References

For more information, refer to:

- CRE Module IP User Guide (FPGA-IPUG-02067)
- CertusPro-NX FPGA website
- Lattice Propel Design Environment website
- Lattice Radiant FPGA design software
- Lattice Diamond FPGA design software
- Lattice Insights for Lattice Semiconductor training courses and learning plans
Technical Support Assistance
Submit a technical support case through www.latticesemi.com/techsupport.
For frequently asked questions, refer to the Lattice Answer Database at www.latticesemi.com/Support/AnswerDatabase.
## Revision History

### Revision 1.0, September 2023

<table>
<thead>
<tr>
<th>Section</th>
<th>Change Summary</th>
</tr>
</thead>
<tbody>
<tr>
<td>All</td>
<td>Initial release.</td>
</tr>
</tbody>
</table>