MachXO3 Using Password Security

Technical Note

FPGA-TN-02072-1.2

August 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 and with all faults, and all risk associated with such information is entirely with Buyer. Buyer shall not rely on any data and performance specifications or parameters provided herein. 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. No Lattice products should be used in conjunction with mission- or safety-critical or any other application in which the failure of Lattice's product could create a situation where personal injury, death, severe property or environmental damage may occur. 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.

Contents

Figures

Tables

Acronyms in This Document

A list of acronyms used in this document.

Acronym	Definition
IP	Intellectual Property
OTP	One-Time Programmable
NVCM	Non-Volatile Configuration Memory
SRAM	Static Random-Access Memory

1. Introduction

This technical note describes the MachXO3™ Password security feature. The Password security feature utilizes a Flash Protect Key to provide a method of controlling access to the configuration and programming modes of the device, encompassing aspects of both read- and write-protection. When the Password security feature is enabled, the configuration and programming edit mode operations (including Write, Verify and Erase operations) are allowed only when presented with a Flash Protect Key which matches that stored in the device.

For comparison, the MachXO3 devices provide a variety of other protection and security protocols to shield valuable customer Intellectual Property (IP) from being viewed or tampered. In addition to the Password security feature described here, the One-Time Programmable (OTP) features provide permanent *write-protection* against intentional or unintentional corruption of the FPGA configuration image, while still allowing verification operations. The *Security* and *Security-Plus* settings provide a complementary set of *read-protection* features. These features prevent the read-back of sensitive customer IP or data from the FPGA fabric while allowing Erase and reprogramming operations (for in-field updates, for example). Refer to the documents contained in the References section for more information on the OTP, Security and Security Plus features of the MachXO3.

Table 1.1. Password Security Feature Terminology Used in This Document

This Document	Diamond/Programmer Software	Also known as	Description
Flash Protect Key	Flash Protect Key/Password Key	Device Password	64-bit binary Flash Protect Key, stored in the MachXO3 feature row and in a .key file.
Passcode Encryptied File (.key)	<design_name>.key/Load Key, Save Key	Password file	AES encrypted file stored on a local file system. The Lattice Programmer software utilizes the Flash Protect Key stored within this file when communicating with a protected MachXO3 device.
File Protection Password	Password/Password	Encryption Passcode	The 8-16 character Passcode used to secure the .key file.

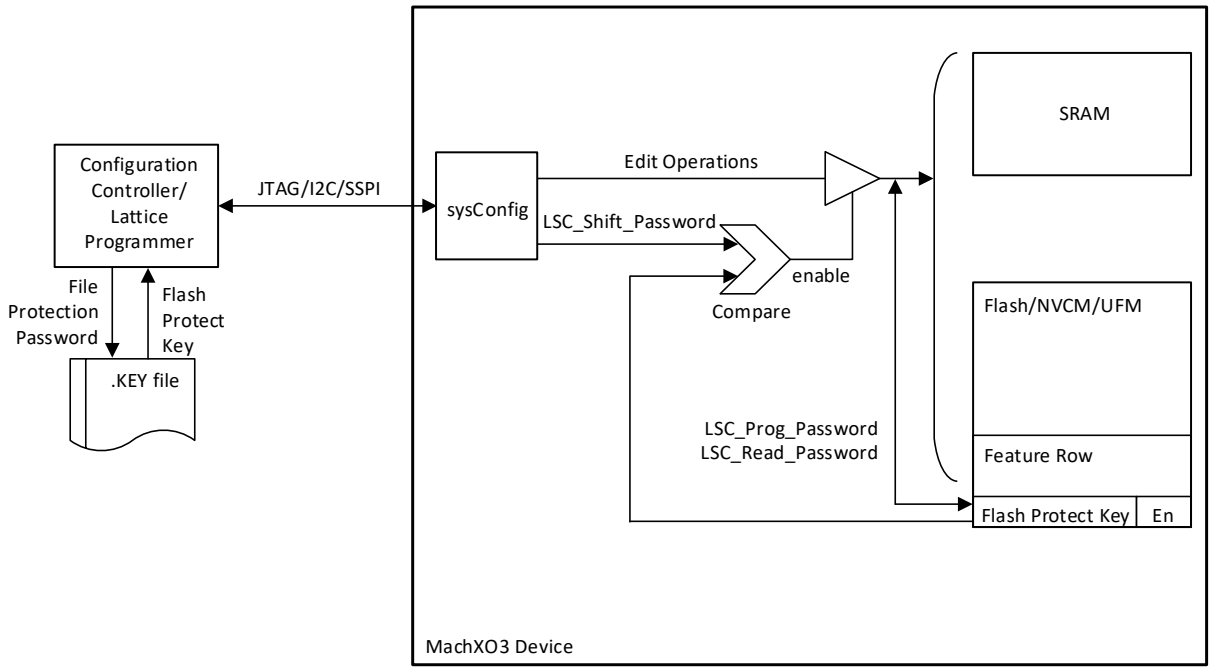

Figure 1.1. Password Security Block Diagram

2. Overview

2.1. Operation

The MachXO3 Password feature requires that a controller accessing MachXO3 through a sysConfig port (JTAG, SSPI, I^2C or WISHBONE) provide a valid Flash Protect Key. The Flash Protect Key unlocks the device and allows configuration or programming operations to proceed. Without a valid Flash Protect Key, the user can perform only rudimentary non-configuration operations such as Read Device ID.

The Lattice Diamond® and Lattice Diamond Programmer software tools support the secure generation and utilization of the Flash Protect Key. In addition, for embedded environments, the Deployment Tool of Diamond Programmer supports the generation of algorithm and data files for embedded programming and configuration of Flash Protect Key enabled devices.

The Flash Protect Key generated using Lattice Diamond is stored in a passcode encrypted file (.key) on the local file system (Windows or Linux) using Advanced Encryption Standard with a 128-bit encryption key (AES-128). The Flash Protect Key is therefore reasonably secure against attack. The encryption passcode, also known as the File Protection Password, is required to access the encrypted file for subsequent Flash Protect Key enabled programming and configuration operations.

The MachXO3 Flash Protect Key field and the feature enable status bit are contained in the Feature Row sector of the device Flash memory array. When the Password feature is enabled, the Flash Protect Key field cannot be read, erased or written without first presenting this same Flash Protect Key.

2.2. Security Limitations

When performing configuration operations, the Flash Protect Key is transmitted unencrypted (*in-the-clear*) by the configuration controller to the sysConfig port (JTAG, Slave SPI, or I^2C). It may be necessary to restrict physical access to the device for high-security remote operations (in-field updates, for example). Alternately, methods utilizing the internal WISHBONE sysConfig port to transmit the Flash Protect Key may be used to keep the Flash Protect Key secure against unauthorized probing.

When using the Deployment tool's 'Tester' capability to generate .SVF debugger files, caution should be applied. The Flash Protect Key is contained in the ASCII text .SVF. Neither the Flash Protect Key nor the .SVF file itself are encrypted to prevent unauthorized access. Delete or secure any debugger files as necessary.

Bitstream files (.bit) do not contain the Flash Protect Key. The Flash Protect Key feature is bypassed by the Master SPI port when booting from external SPI flash devices.

3. Creating and Securing the Flash Protect Key

3.1. Overview

The Flash Protect Key is specified by the user and stored in a .key file. The .key file is secured using a File Protection Password. The .key file may be referenced for subsequent secure configuration and programming operations.

3.2. Software Requirements

The Flash Protect Key feature for MachXO3 devices is available in Lattice Diamond software version 3.7 or later. To enable this security feature, you must also install the Encryption Control Pack, available at www.latticesemi.com.

3.3. Creating and Securing the Flash Protect Key Using Diamond Software

Follow these steps to create and secure the Flash Protect key:

1. In the Tools menu, select **Security Settings** to open the passcode file generation tool. The Enter Password dialog opens with a default File Protection Password (file passcode). To enhance password security, change the File Protection Password by clicking **Change**, as shown in Figure 3.1.

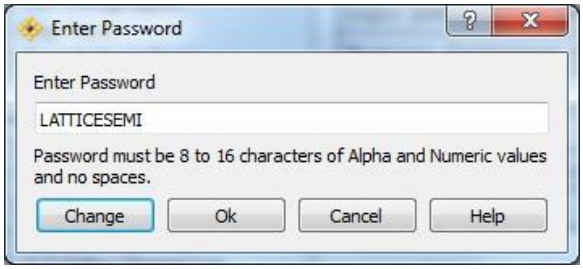

Figure 3.1. Enter Password Dialog Box

2. The new File Protection Password must be 8 to 16 alpha and numeric characters, and cannot contain spaces or special characters. If you need to record the new File Protection Password for future reference, choose a secure location. In the Change Password dialog shown in Figure 3.2, enter the new **File Protection Password** twice and click **OK**.

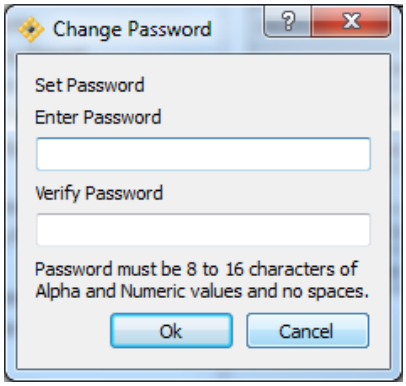

Figure 3.2. Change Password Dialog Box

3. The Security Settings dialog opens for you to specify the device Flash Protect Key as shown in Figure 3.3. Ensure that the Advanced Security Settings checkbox is marked. A default Flash Protect Key is provided. For enhanced security, change the Flash Protect Key. The Flash Protect Key is a 64-bit binary value. For convenience, the key can be specified in ASCII (8-character max), HEX (16-digit max), or Binary formats. After entering the Flash Protect Key, click **OK**.

Figure 3.3. Security Settings Dialog Box

Once you have specified all the security settings, an encrypted <design_name>.key file is generated in the project folder to hold the encrypted Flash Protect Key. The .key file contains readable header information that identifies the project, software version, device used, and creation date. The header is not encrypted so that you can identify the encrypted file.

Note: Additional output files (For example, .bek, .txt) files are generated but are not necessary for the Password feature. These additional files may be discarded.

4. Using Flash Protect Keys

4.1. Software Requirements

The Password feature for MachXO3 devices is available in Lattice Diamond and stand-alone Lattice Programmer software version 3.7 or later.

4.2. Programming the Device Using Programmer

You can use the Programmer software to perform password-related operations, either from within Lattice Diamond or stand-alone. The Password Key Options section is available in the Device Properties dialog as shown in Figure 4.1.

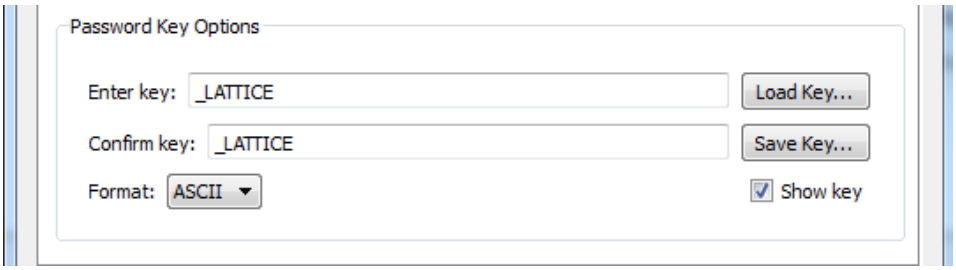

Figure 4.1. Password Key Options

Follow these steps to program the device in Programmer:

1. Enter the device Flash Protect Key into the Enter key and Confirm key fields. The 64-bit value is displayed in ASCII (8 character max) or HEX (16 digit max) formats. The password key is shown when Show key is selected, otherwise, the characters are represented by dots.

   Alternatively, you can load the Flash Protect Key from a previously generated .key file using the Load Key button. When prompted, provide the .key file location and the File Protection Password to access and decrypt the file.

   A Flash Protect Key entered in the Password Key Options section can be saved to disk by clicking the **Save Key** button. When prompted, provide the .key file location and a File Protection Password to save and encrypt the file.
2. After completing all sections of the Device Properties dialog box, click OK to proceed.

4.3. Programmer Operations

The following password related operations support the MachXO3 Password feature.

To program the Flash Protect Key (Password Key) into an un-protected MachXO3:

Access Mode	Operation
Advanced Security Keys Programming	Security Program Password Key Security Program Password Key with Lock Security Erase Feature Row with Password Key

To perform operations on a Flash Protect Key (Password Key) protected MachXO3 device:

Access Mode	Operation
Advanced Security File Programming	Security Flash EPV with Password Security XFlash EPV with Password Security SRAM EPV with Password Security Fast Program with Password Security XSRAM SEI Fast Program with Password

Note: Additional Advanced Security File Programming Operations not listed here are available in Diamond Programmer.

To program both an FPGA image and the Flash Protect Key (Password Key) into an unprotected MachXO3 device:

Access Mode	Operation
Advanced Security Production Programming	Security EPV with Password Key Option Security EPV with my_ASSP, Password Key Option

5. Low-Level Implementation

5.1. Password Feature Commands

The low-level sysConfig commands in Table 5.1 below are utilized by the Lattice Diamond, Programmer, and Deployment tools to implement the Flash Protect Key feature operations.

To unlock the device, transmit LSC_SHIFT_PASSWORD along with the Flash Protect Key prior to entering a configuration edit mode (ISC_ENABLE or ISC_ENABLE_X). If the transmitted Flash Protect Key matches the key previously programmed into the MachXO3, the device remains unlocked until the edit mode is exited. Edit modes are cancelled by issuing the ISC_DISABLE or ISC_REFRESH commands, asserting the PROGRAMN pin or power-cycling the device.

5.1.1. Set, Verify, Unlock

Table 5.1. Flash Protect Key-Related sysConfig Commands

Command	Op Code	Use	Description
LSC_PROG_PASSWORD	0xF1	0xF1 00 00 00 pp pp pp pp pp pp pp pp	1 byte Opcode + 3 bytes operand + 64-bit Passcode
LSC_READ_PASSWORD	0xF2	0xF2 00 00 00	1 byte Opcode + 3 bytes operand + read 64-bit Passcode
LSC_SHIFT_PASSWORD	0xBC	0xBC 00 00 00 pp pp pp pp pp pp pp pp	1 byte Opcode + 3 bytes operand + 64-bit Passcode

5.1.2. Enable

When the Flash Protect Key is successfully programmed and verified, it is made active by setting PWD_EN and PWD_ALL in the Feature Row. PWD_EN and PWD_ALL are set using command opcode 0xF8 LSC_PROG_FEABIT. PWD_EN is represented by bit 2, and PWD_ALL by bit 3. See Using Hardened Control Functions in MachXO3 Devices Reference Guide (FPGA-TN-02064) for more information regarding the Program FEABITS command.

5.2. Password-Required Operations

All sysConfig operations targeting the Feature Row are restricted when PWD_EN is set. Additionally, all sysConfig operations targeting the Configuration NVCM (MachXO3L), Flash (MachXO3LF), or SRAM (MachXO3L and MachXO3LF) are restricted when both PWD_EN and PWD_ALL are set.

In the MachXO3LF family, the User Flash Memory can also be protected by setting SECURITY PLUS in the Lattice Diamond project in conjunction with PWD_EN and PWD_ALL.

Table 5.2 below is a list of exempt sysConfig commands. These commands can be executed when PWD_EN is set regardless of Flash Protect Key match status.

Table 5.2. Exempt sysConfig Commands

Command Name	Op Code
ISC_NOOP Bypass	0xFF
IDCODE_PUB Read Device ID	0xE0
USERCODE Read USERCODE	0xC0
LSC_SHIFT_PASSWORD Check Flash Protect Key	0xBC
LSC_READ_STATUS Read Status Register	0x3C
LSC_CHECK_BUSY Check Busy Flag	0xF0
LSC_REFRESH Refresh	0x79
LSC_DEVICE_CTRL Standby	0x7D
ISC_ENABLE Enable Offline Configuration Mode	0xC6
ISC_ENABLE_X Enable Transparent Configuration Mode	0x74
ISC_DISABLE Disable Configuration	0x26

References

- MachXO3 Family Data Sheet (FPGA-DS-02032)
- MachXO3 Programming and Configuration Usage Guide (FPGA-TN-02055)
- Using Hardened Control Functions in MachXO3 Devices (FPGA-TN-02063)
- Using Hardened Control Functions in MachXO3 Devices Reference Guide (FPGA-TN-02064)

Below are some useful web pages related to using password security in MachXO3 devices.

- MachXO3 Family Devices Web Page
- Boards, Demos, IP Cores, and Reference Designs for MachXO3 Family Devices
- Lattice Insight for Training Series and Learning Plans

Technical Support Assistance

- Submit a technical support case via www.latticesemi.com/techsupport.
- For frequently asked questions, please refer to the Lattice Answer Database at www.latticesemi.com/Support/AnswerDatabase.

Revision History

Revision 1.2, August 2023

Section	Change Summary
All	Corrected overall formatting issues.
References	Newly added links to MachXO3 Family Devices Web Page, Boards, Demos, IP Cores, and Reference Designs for MachXO3 Family Devices, and Lattice Insight for Training Series and Learning Plans.
Technical Support Assistance	Newly added the link to the Lattice Answer Database.

Revision 1.1, January 2020

Section	Change Summary
All	• Changed document number from TN1290 to FPGA-TN-02060. • Updated document template.
Disclaimers	Added this section.

Revision 1.0, May 2016

Section	Change Summary
All	Initial release

www.latticesemi.com