MachXO3D™

Enhance Secure Control Applications with **Hardware Root-of-Trust** and **Dual Boot** capabilities to **simplify** implementation of comprehensive, flexible and robust hardware security throughout the product lifecycle.

Secure Control

- Built on proven MachXO3LF architecture.
- Adds on Embedded Security Block that enables Hardware Root-of-Trust and pre-verified cryptographic functions.
- On Device Configuration Flash enables dual boot eliminating the need for external memory.
- Hardened Device Configuration Engine ensures only FPGA configurations from a trusted source can be installed.

Features

<table>
<thead>
<tr>
<th></th>
<th>MachXO3D-4300</th>
<th>MachXO3D-9400</th>
</tr>
</thead>
<tbody>
<tr>
<td>LUTs</td>
<td>4300</td>
<td>9400</td>
</tr>
<tr>
<td>User Flash (kbits)</td>
<td>367/1122¹</td>
<td>1088/2693¹</td>
</tr>
<tr>
<td>Hardened Security</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>On-device Dual-boot</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>I3C compatible I/O²</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>MIPI D-PHY Support³</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Available Packages

<table>
<thead>
<tr>
<th></th>
<th>MachXO3D-4300</th>
<th>MachXO3D-9400</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>0.5 mm Spacing</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>I/O Count</td>
<td></td>
<td></td>
</tr>
<tr>
<td>72 QFN (10 mm x 10 mm)</td>
<td>58 (HC¹ / ZC²)</td>
<td>58 (HC¹ / ZC²)</td>
</tr>
<tr>
<td><strong>0.8 mm Spacing</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>I/O Count</td>
<td></td>
<td></td>
</tr>
<tr>
<td>256-ball caBGA (14 mm x 14 mm)</td>
<td>206 (HC¹ / ZC²)</td>
<td>206 (HC¹ / ZC²)</td>
</tr>
<tr>
<td>400-ball caBGA (17 mm x 17 mm)</td>
<td>335 (HC¹ / ZC²)</td>
<td></td>
</tr>
<tr>
<td>484-ball caBGA (19 mm x 19 mm)</td>
<td>383 (HC¹)</td>
<td></td>
</tr>
</tbody>
</table>

¹. When dual-boot is disabled, image space can be repurposed as extra UFM.
². 4 pairs of I/O in bank 3 with I3C dynamic pull up capability.
³. HC device only.
Robust Security
- MachXO3D complies with NIST SP 800-193 Platform Firmware Resiliency (PFR) Guidelines
- Protects non-volatile memory through access control
- Cryptographically detects and prevents boot from malicious code
- Recovers to latest trusted firmware in case of corruption
- Industry’s first control-oriented FPGA compliant with NIST PFR guidelines
- Programmable logic minimizes attack surface dynamically configuring access control throughout product lifecycle

Flexible
- Customizable approach allows implementation with wide range of system architectures
- Provides secure and reliable in system updates
- Dual Boot enables Fail Safe Reprogramming
- Hardened Device Configuration Engine prevents unauthorized access to configuration memory

Simple
- Simplifies chain of trust implementation by integrating Root-of-Trust with platform’s first on, last off device
- Protects platform processor firmware with no code changes
- MachXO3D is pin compatible with MachXO3

Comprehensive Security
MachXO3D Enables
- Data Security
- Equipment Security
- Data Integrity
- Design Security
- Brand Protection

Security Features
- Data Encryption
- Firmware Authentication
- Data Authentication
- Code Encryption
- Device Authentication

Chain of Trust with MachXO3D

Applications Support
www.latticesemi.com/support

Copyright © 2019 Lattice Semiconductor Corporation, Lattice Semiconductor, L (stylized) Lattice Semiconductor Corp., and Lattice (design). MachXO3D™ is either registered trademarks or trademarks of Lattice Semiconductor Corporation in the United States and/or other countries. Other product names used in this publication are for identification purposes only and may be trademarks of their respective companies.

May 2019
Order #: I0268 Rev. 1