

Implementing Encryption Algorithms with the Virtex-5 LXT Platform

The Virtex-5 LXT platform makes encryption product development easy.

by Mike Nelson
Sr. Staff System Architect,
Storage and Servers, Vertical Markets
Xilinx, Inc.
mike.nelson@xilinx.com

Encryption is a computationally intensive function, which makes extremely high-performance implementations a serious system design challenge. The Xilinx® Virtex™-5 LXT platform meets this challenge with performance-optimized features ideal for 10 Gbps and faster implementations of leading-edge encryption algorithms.

A world-class programmable fabric provides superior logic performance. Integrated GTP serial transceivers, hard PCI Express (PCIe) Endpoint blocks, and highly flexible SelectIO™ technology enable tremendous I/O bandwidth. And 65-nm device densities provide a family of devices appropriate to almost any system design need.

As the world of cryptography continuously evolves with additional modes and algorithmic refinements, your design can evolve with it...

The Virtex-5 architecture features several advances that enable the very high-performance logic necessary for high-bandwidth encryption applications:

- Real six-input LUT-based fabric means that you can map circuits into denser structures with fewer levels of logic, increasing device utilization and performance
- Improved routing architecture increases the reach of low-latency logic interconnection, providing more flexibility to synthesis tools and also increasing device utilization and performance
- 36-Kb dual-port block RAMs with integrated ECC allow extremely high-performance on-chip memory resources for creating FIFOs and computational logic structures

Combined, these resources enable very cost-effective 10 Gbps and faster implementations of IPsec AES-CBC/AES-XCBC-MAC-96, 802.1ae MACSec, LRW-AES, AES-GCM, SHA-256/384/512, and many other cryptographic algorithms. Furthermore, as the world of cryptography continuously evolves with additional modes and algorithmic refinements to these algorithms, your design can evolve with it – because the Virtex-5 family is a programmable logic platform.

I/O Bandwidth and Flexibility

Computationally intensive core logic requires high-bandwidth I/O. But the nature of that I/O will vary based on your system architecture. Figure 1 shows two common architectures for implementing encryption processing.

Look-aside co-processing is an attractive option widely used in x86-based system appliances. This model leverages the excellent value of the commodity x86 platform to implement the application framework and selectively “looks aside” to an optimized accelerator to achieve high perform-

ance for the target application. FPGAs have always been well suited for this role, but scaling to approach to very high performance has been problematic.

PCI and PCI-X solutions require modest soft logic but have limited performance and must share what bandwidth they do have. PCI Express can implement a very high-performance non-blocking switched fabric, but traditionally requires extensive soft-logic resources to implement the controller, and possibly an external PHY for the electrical connection.

Virtex-5 LXT platform FPGAs address these limitations by combining embedded RocketIO™ GTP transceivers and a hardened PCI Express Endpoint block in every device. With the LXT platform, extremely high-performance co-processor I/O is easy and efficient, as shown in Figure 2.

Virtex-5 LXT platform FPGAs are also ideal for in-line applications, as illustrated in Figure 3. A key requirement for in-line encryption applications is flexibility. They may require identical – or different – input and output ports, port aggregation,

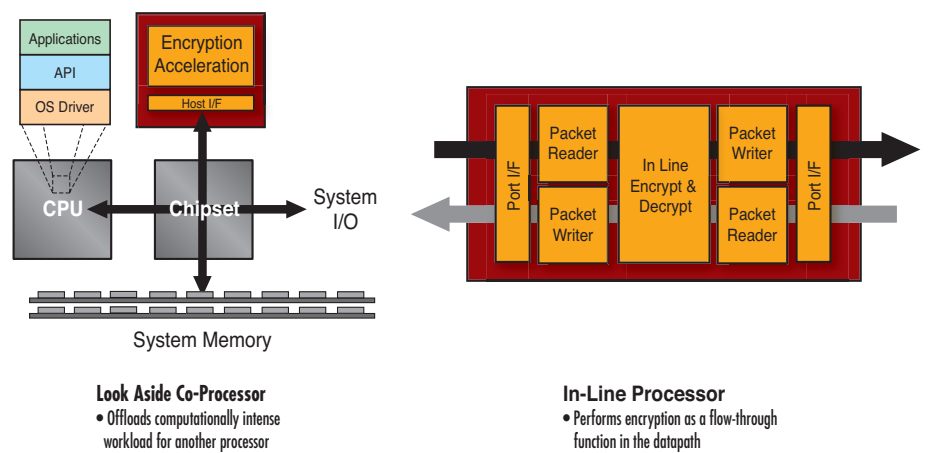


Figure 1 – Look-aside and in-line encryption processing

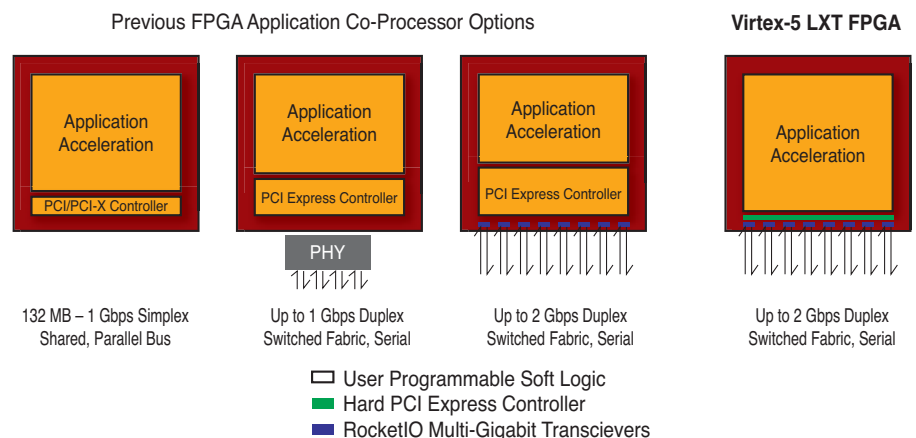


Figure 2 – I/O bandwidth and soft logic progression for FPGA co-processor options

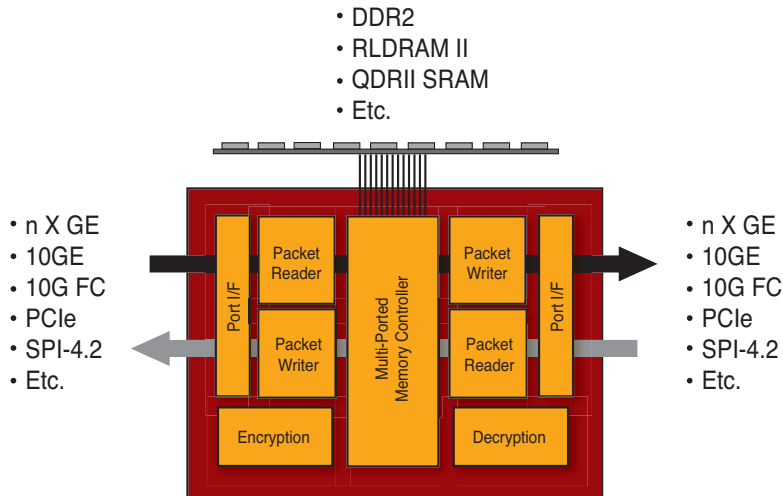


Figure 3 – Virtex-5 LXT device in-line encryption platform flexibility

or local subsystem memory. The Virtex-5 LXT platform meets this challenge with a wide range of capabilities:

- Gigabit Ethernet (GbE) – Each device in the Virtex-5 LXT platform includes four independent hardened GbE MACs, making multi-port Ethernet a very efficient I/O option. You can add additional ports as necessary with 100% form-, fit-, and function-equivalent soft LogiCORE™ IP.
- 10 Gigabit Ethernet – A Xilinx soft LogicCORE function is available that can be connected to four RocketIO MGTs for a XAUI interface or to a SelectIO pinout for an XGMII interface.
- 10 Gbps Fibre Channel (FC) – A XAUI-like Fibre Channel standard uses four RocketIO MGTs operating at 3.1875 Gbps in parallel to create a 10.2 Gbps FC channel.
- PCI Express – Available to interface to a variety of industry-standard PCIe-based port controllers.
- SPI-4.2 – Soft LogicCORE IP supports this networking industry standard for chip-to-chip connectivity over high-performance SelectIO technology.
- Memory – In addition to port I/O standards, Virtex-5 SelectIO technology also supports a wide range of memory interface technologies including

DDR2, RLDRAM II, and QDR II SRAM. These capabilities enable virtually any local memory subsystem that an in-line processing engine might require.

These features allow you to create in-line solutions that will connect to the ports you need with the integrated encryption technology you want.

Conclusion

The Virtex-5 LXT platform expands the capabilities of the Virtex-5 FPGA architecture with the addition of RocketIO GTP transceivers, plus hard PCI Express Endpoint and tri-mode Ethernet MAC blocks. The result is a platform ideally suited to support very high-performance look-aside and in-line encryption functions.

Other applications where LXT platform devices will excel include high-performance packet handling and deep content inspection for networking; high-speed data mining for databases; time-critical computational processing for industrial, scientific, and medical applications; and real-time image processing for aerospace/defense and video graphic applications.

To learn more about Virtex-5 LXT platform FPGAs, visit www.xilinx.com/virtex5. To learn more about Xilinx in encryption, visit www.xilinx.com/esp/security/data_security/index.htm. And to learn how Xilinx FPGAs can help you in other applications, visit www.xilinx.com/esp.

Supporting Your Future
HUNT ENGINEERING
www.hunteng.co.uk

USB connected Programmable FPGA systems

V-II Pro PowerPC

- Virtex-II Pro XC2VP7
- 256 Mbytes DDR Memory
- Configurable digital I/Os
- PowerPC boot FLASH
- USB 2 or Standalone

Software Defined Radio

- Virtex-II FPGA 1M gates
- 2 ch 125Mps A/D and D/A
- TI C6203 DSP
- 32Mbytes SDRAM
- Configurable Digital I/O
- USB 2 or Standalone

Imaging with Virtex-4FX

- Virtex-4 FPGA FX12
- 128Mbytes DDR Memory
- CameraLink connection
- VHDL and PowerPC Imaging Libs
- USB 2 or Standalone

Programmable hardware with cables, device drivers, loading tools, examples and Power Supply.
Systems can be used connected to a PC using USB, or can function standalone (without USB) using the initialisation PROMs.

sales@hunteng.co.uk
+44 (0)1278 760188

www.hunt-rtg.com