White Paper

Data Center and Networking
Security

Intel Agilex® 7 FPGAs and Intel® eASIC™ Devices Target IPUs, SmartNICs, and 5G Networks

Intel Agilex® 7 FPGAs and SoCs are a series of devices targeted for data center, core, edge, and embedded applications. These devices allow customers to achieve high performance per watt with low latency all while meeting critical environmental, safety, and security requirements.

Table of Contents

Introduction

From the edge to the cloud, security challenges in the form of cyberattacks and data breaches loom ever larger as attacks on high-speed networks multiply. Massive amounts of data are at risk but so are physical resources including critical physical infrastructure. Cryptography and authentication represent potent countermeasures to combat these attacks. The multiple members of the Intel Agilex® 7 FPGA families (AGF023/AGF019 and AGI041/AGI040/AGI035/AGI023/AGI019) have featured high-performance crypto blocks paired with MACsec soft IP to help mitigate the risks and limit the effects of these cyberattacks.

Cyberattacks and Data Breaches: Defining the Problem

CSO, an online publication for chief security officers, recently estimated that about 3.5 billion people saw their personal data stolen in just the top two of fifteen biggest breaches during the 21st century.[1] These breaches involved databases at some of the largest companies and brands in the world including Adobe, eBay, Equifax, LinkedIn, Marriott International, McDonald's, and Volkswagen. The smallest incident on CSO's list involved the theft of personal data for 134 million people.

Data is not all that's at risk from these cyberattacks. Physical assets are also at risk. For example, a ransomware attack on its IT network prompted Colonial Pipeline to cut the connection between its IT and OT (operational technology) networks before the damage spread. This action shut down Colonial's 5500-mile pipeline for several days in May, 2021. Colonial's pipeline supplies a significant amount of fuel to eastern US and the pipeline's shutdown triggered panic buying of gasoline resulting in shortages.

It's no exaggeration to say that cyberattacks have grown to epidemic proportions. Data encryption and authentication can significantly mitigate the risks and effects of these cyberattacks. Some of the ways that encryption and authentication can help mitigate risks are:

- Protecting all data sent to and retrieved from the cloud (networking)
- Protecting all data sent between applications and among microservices
- Protecting all live data and backed up databases stored in the cloud and in data centers
- Protecting all data traveling through cellular and 5G network base stations

As network data rates climb, the additional cryptographic overhead becomes increasingly problematic due to latency increases and bandwidth reduction. Consequently, the industry needs solutions that minimize this additional overhead. Ideally, these authentication and cryptographic capabilities will be integrated into the data centers and cloud network and storage system infrastructures so that this protection is added automatically, not as an option.

Data Encryption and Network Access Control

Encryption is the first step in protecting data from security threats. Properly encrypted data obtained during a successful cyberattack will prove useless to the attacker without the encryption keys. The Advanced Encryption Standard (AES) developed by the U.S. National Institute of Standards and Technology (NIST) in 2001 has become the globally accepted standard for data encryption. According to NIST, AES now protects everything from classified data and bank transactions to online shopping and social media applications.[2] The US government has adopted AES as its officially recognized encryption standard.

The next security step is to deny network and data access to unauthorized entities. Media Access Control security (MACsec, IEEE standard 802.1AE) provides point-to-point security for Ethernet links. MACsec can identify and prevent most security threats such as denial of service, intrusion, man-in-the-middle, masquerading, passive wiretapping, and playback attacks. MACsec secures Ethernet links for almost all network traffic, including frames from many protocols such as the Link Layer Discovery Protocol (LLDP), Link Aggregation Control Protocol (LACP), Dynamic Host Configuration Protocol (DHCP), and the Address Resolution Protocol (ARP).

Security and Cryptographic Use Cases

With the growing threats of cyberattacks and data breaches, use cases for secure, encrypted communications are plentiful. Here are three such use cases directly supported by the new Intel Agilex® FPGAs:

- **OvS**: The Open vSwitch (OvS) is a production quality, multilayer virtual switch used to route network packets among virtual machines (VMs) in a data center. The extensive networking fabric that connects everything within a data center and among multiple data centers increasingly requires secure, encrypted connections to protect against cyberattacks. The OvS open-source networking stack that routes packets among VMs can run as software on a CPU or it can be implemented in hardware. Initially, data center architects placed secure gateways only between data centers because network communications within the data center were deemed physically secure. With the advent and widespread use of VMs and microservices, all networking communications are now suspect, which motivates the increasing use of secure, encrypted communications within the entire cloud network. This large jump in the use of encryption coupled with constantly increasing network wire speeds causes encryption to become a troublesome communications bottleneck. Building hardware encryption support into the cloud and data center network infrastructures through appropriately designed SmartNICs and Infrastructure Processing Units (IPUs) removes these bottlenecks by offloading the encryption and decryption tasks from the server CPUs.
- **MACsec for 5G Networks**: In 3GPP terminology, an Evolved Node B is a small cell in a 5G network. These small cells communicate to the wider 5G network using the IPsec security protocol. As cell designs migrate to virtual radio area networks (vRANs), some of the cell's associated digital processing moves into the radio heads (RUs), which communicate with the remaining cell hardware over an unprotected CPRI connection. Transferring some of the digital processing into the RU requires that the radio head hardware supports data encryption and decryption. One way to secure these RU communications is to use the MACsec protocol over the CPRI connection intrinsic to RU design.
- **Network Storage**: When network storage was confined to one data center, storage communications were secured physically. However, the growing use of NVMe over Fabric protocols for network storage means that the storage subsystems can be located in any data center, anywhere in the world. Consequently, network storage communications now require secure, cryptographic protection because communications with the storage subsystems are no longer confined to one physically secure data center. The overhead incurred when adding this cryptographic protection must not add too much latency or bandwidth so that violation of service level agreements (SLAs) does not occur. As a practical matter, cryptographic security must add a negligible amount of latency and must not reduce wire-speed bandwidth for network storage communications.

Game Changers: Intel Agilex® 7 FPGAs and SoCs

Intel Agilex® 7 FPGAs and SoCs deliver a game-changing combination of performance, performance per watt, flexibility, and agility for an increasingly data-centric world. They combine several important innovations in multiple areas of Intel technology leadership to deliver significant value to end-product development at the edge, throughout the network, to the data center and the cloud.

These devices meld a high-performance FPGA core die fabricated with the Intel 10 nm SuperFin manufacturing process with function-specific and general-purpose tiles (chiplets) using Intel's EMIB and advanced 3D packaging technology. Tiles provide additional I/O functionality including fast high bandwidth memory (HBM) DRAM and PCIe 4.0, PCIe 5.0, CXL, and 116 Gbps serial transceiver ports to interface to a wide variety of host processors such as the latest 4th Generation Intel® Xeon® Scalable processors. This design and manufacturing approach to FPGA and SoC development allows Intel to quickly address a broad array of applications with tailored, flexible solutions.

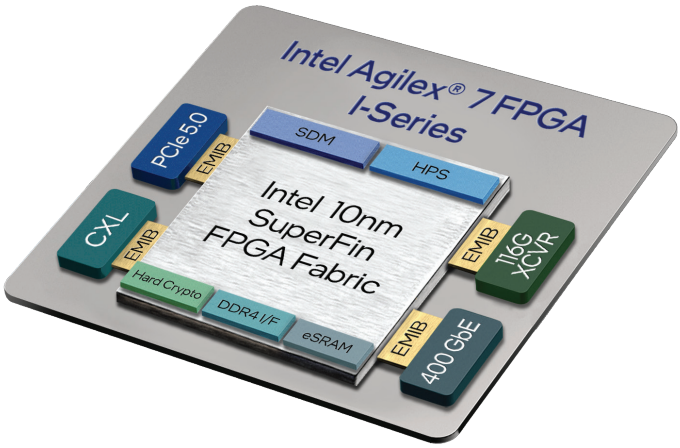

Figure 1. The tile-based design and manufacturing approach used to develop Intel Agilex 7 FPGAs allows Intel to quickly address a broad array of applications with tailored, flexible solutions.

Hardened Cryptographic Support for 200G and 400G Ethernet

Intel is adding new members of the Intel Agilex 7 FPGA and SoC families that feature high-performance crypto blocks and MACsec soft IP capable of supporting authenticated and encryption- protected, bidirectional network traffic at wire speed over two 200G Ethernet ports or two unidirectional 400G Ethernet ports simultaneously. These Intel FPGAs and SoCs are optimized for IPUs, SmartNICs, and 5G wireless network equipment design. The members of the Intel Agilex 7 FPGA and SoC families with hardened cryptographic support are:

- Intel Agilex FPGA F-Series AGF 019 and AGF 023 devices, with advanced digital signal processing (DSP) capabilities optimized for applications in the data center, networking, and edge computing
- Intel Agilex FPGA I-Series AGI 019 and AGI 023 devices are optimized for bandwidth-intensive applications that require a PCIe 5.0 processor interface and 116 Gbps transceivers.
- Intel Agilex FPGA I-Series AGI 041 device, optimized for 400G IPU and bandwidth intensive applications that require PCIe 5.0, CXL, and multi host enhancement with 400GbE and 116 Gbps transceivers
- Intel Agilex FPGA I-Series AGI 035 and AGI 040 devices, optimized for applications require high number of networking I/Os.

Table 1 shows Intel Agilex 7 FPGAs and SoCs family members available with high-performance hardened crypto blocks. For more detailed device information, refer to the Intel Agilex 7 FPGA and SoC FPGA web page.

The advanced cryptographic features in these new Intel Agilex FPGAs and SoCs are critical to the development of high-performance IPUs and SmartNICs with 100GbE, 200GbE, and 400GbE Ethernet ports and secure 5G wireless network equipment. The memory resources of these devices have been tuned for their target applications, which help to lower their power consumption and enables them to be offered in smaller packages compared to other Intel Agilex devices of similar logic element density. Finally, FPGA reconfigurability enables developers of these applications to update their products to address new security threats with hardware-accelerated measures, even after they have been deployed into the field.

Intel Agilex® 7 FPGAs and SoCs with Hardened Crypto Blocks														
	F-Series						I-Series							
	AGF 019			AGF 023			AGI 019		AGI 023		AGI 035	AGI 040	AGI 041	
Logic Elements - M (LEs)	1.9			2.3			1.9		2.3		3.5	4.0	4.0	
Total RAM - Mb (M20K, eSRAM)	184			222			184		222		346	443	371	
HPS	Support										N/A		Support	
Crypto	2x200G										4x200G			
PCIe	PCIe 4.0						PCIe 4.0	PCIe 5.0	PCIe 4.0	PCIe 5.0	PCIe 4.0		PCIe 4.0	PCIe 5.0
CXL	N/A						N/A	CXL	N/A	CXL	N/A		N/A	CXL
Network XCVRs	24	32	64	24	32	64	72	16	72	16	120		72	20
Tiles	E-Tile x1 P-Tile x2	F-Tile x2	F-Tile x4	E-Tile x1 P-Tile x2	F-Tile x2	F-Tile x4	F-Tile x4	F-Tile x1 R-Tile x1	F-Tile x4	F-Tile x1 R-Tile x1	F-Tile x6		F-Tile x4	F-Tile x1 R-Tile x3

Table 1. Intel Agilex 7 FPGAs and SoCs with hardened crypto blocks. For device overview, refer to the Intel Agilex 7 FPGAs and SoCs Device Overview web page.

For example, the Intel Infrastructure Processing Unit (Intel® IPU) Platform F2000X-PL leverages the Intel Agilex FPGA AGF 023 device enabling a high-performance FPGA-based cloud infrastructure acceleration platform with 2 x 100 GbE network interfaces with hardware crypto block to enable security at line rate. It has the capability to support cloud infrastructure workloads such as Open vSwitch, Non-Volatile Memory (Express) (NVMe) over Fabrics and Remote Direct Memory Access (RDMA) over Converged Ethernet v2 (RoCEv2). More information can be found on the Intel Infrastructure Processing Unit Platform F2000X-PL web page.

Intel® eASIC™ Devices for Optimized TCO

The programmable fabric in Intel Agilex 7 FPGAs allows developers to respond to rapidly changing standards and evolving protocols, including updates after systems have been deployed into the field.

Having said this, Intel also offers Intel eASIC devices. These are structured ASICs, which is an intermediate technology between FPGAs and standard-cell ASICs. These devices provide lower unit-cost and lower power consumption compared to FPGAs, and they also provide faster time to market (TTM) and lower non-recurring engineering (NRE) costs compared to standard-cell ASICs. Once an Intel Agilex 7 FPGA implementation of a design has been proven, that design can be hardened into a lower cost and lower power Intel eASIC device (Figure 2).

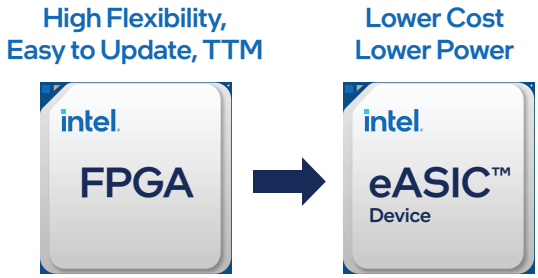

Figure 2. Intel offers an FPGA to Intel eASIC device cost and power reduction path

Specifically, for IPU and SmartNIC applications, there is the Intel eASIC N5X080 device with:

- 8.77M eCells/logic elements, package customized per customer requirements
- 8 MB of Mega SRAM, up to 229 Mbits of bRAM 10K embedded memory plus up to 20 Mb of register file memory
- 64 SERDES operating from 250 Mbps – 32.44 Gbps (NRZ)
- 8 SERDES supporting up to 53 Gbps (PAM4)
- 8X hardened PCIe 5.0 controllers support x8 and x4 configurations; PCIe controllers supported by 32G SERDES lanes*
- 2X hardened 200G Ethernet MACs that can connect to the to 8x 53G SERDES*

Note *: Hardened controllers can be bypassed to support other protocols on the SERDES channels.

Call to Action—Learn More

For more details about the Intel Agilex® 7 FPGA and SoC families, see the following web pages:

- Intel Agilex® FPGAs Deliver a Game-Changing Combination of Flexibility and Agility for the Data-Centric World.
- Intel Agilex® 7 FPGAs and SoCs Device Overview

References

1. The 15 biggest data breaches of the 21st century, Dan Swinhoe, www.csoonline.com/article/2130877/the-biggest-data-breaches-of-the-21st-century.html
2. NIST's Encryption Standard Has Minimum $250 Billion Economic Benefit, According to New Study, www.nist.gov/news-events/news/2018/09/nists-encryption-standard-has-minimum-250-billion-economic-benefit