White Paper

Data Center
Security

Intel® Agilex™ FPGAs target IPUs, SmartNICs, and 5G Networks

Authors

Graham Baker
Product Marketing Manager
Intel Programmable Solutions Group

Stephen Cole
Product Marketing Manager
Intel Programmable Solutions Group

Steve Leibson
Senior Marketing Engineering Manager
Intel Programmable Solutions Group

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 these attacks. The latest members of the Intel® Agilex™ FPGA and SoC FPGA families (AGF023/AGF019 and AGI023/AGI019) now feature 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 the 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 gasoline buying that led to spot 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 amongst 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 clouds' network and storage system infrastructure 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 apps[2] and 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 abound. 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 support 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 overheard incurred when adding this cryptographic protection must not add too much latency or bandwidth so that service level agreements (SLAs) aren't violated. 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 FPGAs and SoCs

Intel Agilex 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, throughput 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 Gen4, PCIe Gen5, and 116 Gbps serial transceiver ports to interface to a wide variety of host processors such as the latest, 3rd 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.

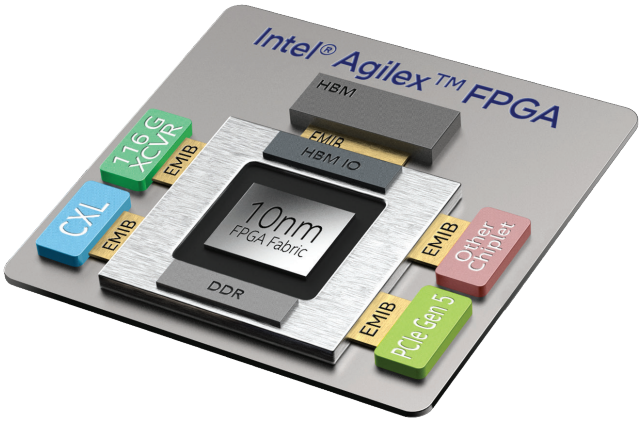

Figure 1. The tile-based design and manufacturing approach used to develop Intel Agilex FPGAs allows Intel to quickly address a broad array of applications with tailored, flexible solutions.

Hardened Cryptographic Support for 100G Ethernet

Four new members of the Intel Agilex FPGA and SoC families feature high-performance crypto blocks and MACsec soft IP capable of supporting authenticated and encryption-protected, bidirectional network traffic at wire speed over two 100G Ethernet ports or two unidirectional 200G Ethernet ports simultaneously. These Intel FPGAs and SoCs are optimized for IPUs, SmartNICs, and 5G wireless network equipment design. The four new members of the Intel Agilex FPGA and SoC families with hardened cryptographic support are:

- Intel Agilex 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 I-Series AGI 019 and AGI 023 devices, optimized for bandwidth-intensive applications that require an effective PCIe Gen5 processor interface and 116Gbps transceivers above what is provided by F-Series devices.

The four new Intel Agilex FPGA and SoC family members available with the high performance crypto blocks include:

- The Intel Agilex F-Series AGF 019 FPGA or SoC with:
  - 1.9M logic elements, 2581 ball package
  - One 18 megabit eSRAM block and 166 megabits of M20K SRAM
  - 1.3K DSP blocks
  - Two PCIe Gen4 x16 ports
  - 24 SERDES ports configurable as 24 channels at 28.9 Gbps (NRZ) or 12 channels operating at 57.8 Gbps (PAM4)
  - Quad-Core Arm Cortex-A53 hardened processor subsystem option
  - Two P-Tiles and one E-Tile
- The Intel Agilex F-Series AGF 023 FPGA or SoC with:
  - 2.3M logic elements, 2581 ball package
  - One 18 megabit eSRAM block and 204 megabits of M20K SRAM
  - 1.6K DSP blocks
  - Two PCIe Gen4 x16 ports
  - 24 SERDES ports configurable as 24 channels at 28.9 Gbps (NRZ) or 12 channels operating at 57.8 Gbps (PAM4)
  - Quad-Core Arm Cortex-A53 hardened processor subsystem option
  - Two P-Tiles and one E-Tile
- The Intel Agilex I-Series AGI 019 SoC with:
  - 1.9M logic elements, 3184 ball package
  - One 18Mbit eSRAM block and 166 megabits of M20K SRAM
  - 1.3K DSP blocks
  - 72 SERDES ports configurable as four PCIe Gen4 x16, 72 channels operating at 32 Gbps (NRZ), or 56 channels operating at 58 Gbps (PAM4), up to 8 channels operating up to 116Gbps
  - Quad-Core Arm Cortex-A53 hardened processor subsystem
  - Four F-Tiles
- The Intel Agilex I-Series AGI 023 SoC with:
  - 2.3M logic elements, 3184 ball package
  - One 18 megabit eSRAM block and 204 megabits of M20K SRAM
  - 1.6K DSP blocks
  - 72 SERDES ports configurable as four PCIe Gen4 x16, 72 channels operating at 32 Gbps (NRZ), or 56 channels operating at 58 Gbps (PAM4), up to 8 channels operating up to 116Gbps
  - Quad-Core Arm Cortex-A53 hardened processor subsystem
  - Four F-Tiles
- The Intel Agilex I-Series AGI 019 FPGA or SoC with:
  - 1.9M logic elements, 1935 ball package
  - One 18 megabit eSRAM block and 166 megabits of M20K SRAM
  - 1.3K DSP blocks
  - 16 SERDES channels operating at up to 32 Gbps (NRZ), or 12 channels operating at up to 57.8 Gbps (PAM4)
  - 16 SERDES channels configurable as one PCIe Gen5 x16 port, 2x PCIe Gen5x8, 4x PCIe Gen5x4
  - Quad-Core Arm Cortex-A53 hardened processor subsystem option
  - One F-Tile and one R-Tile

- The Intel Agilex I-Series AGI 023 FPGA or SoC with:
  - 2.3M logic elements, 1935 ball package
  - One 18 megabit eSRAM block and 166 megabits of M20K SRAM
  - 1.3K DSP blocks
  - 16 SERDES channels operating at up to 32 Gbps (NRZ), or 12 channels operating at up to 57.8 Gbps (PAM4)
  - 16 SERDES channels configurable as one PCIe Gen5 x16 port, 2x PCIe Gen5x8, and 4x PCIe Gen5x4
  - Quad-Core Arm Cortex-A53 hardened processor subsystem option
  - One F-Tile and one R-Tile

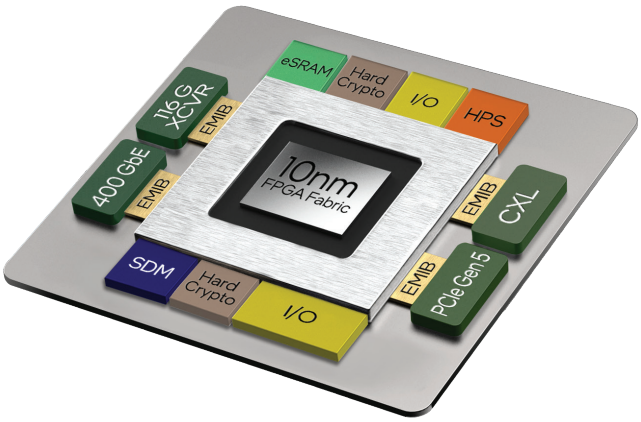

Figure 2. Four new Intel Agilex FPGA and SoC family members are available with high-performance crypto blocks

The advanced cryptographic features in these new Intel Agilex FPGAs and SoCs are critical to the development of high-performance IPUs and SmartNICs with 100G or 200G Ethernet ports and secure 5G wireless network equipment. The DSP and memory resources of these devices have been tuned for their target applications, which helps 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.

Call to Action—Learn More

For more details about the Intel Agilex FPGA and SoC families, see "Intel® Agilex™ FPGAs Deliver a Game-Changing Combination of Flexibility and Agility for the Data-Centric World."

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