白皮书

数据中心和网络
安全性

英特尔面向 IPU、SmartNIC 和 5G 网络推出英特尔® Agilex™ 7 FPGA 和英特尔® eASIC™ 设备

英特尔® Agilex™ 7 FPGA 和 SoC 是一系列面向数据中心、核心网、边缘和嵌入式应用的设备，可使客户实现出色的每瓦性能和低时延，同时满足关键性的环保、安全和安保要求。

引言

随着针对高速网络的攻击成倍增加，从边缘到云端，以网络攻击和数据泄露形式出现的安全挑战空前严峻。不仅大量数据面临着安全风险，包括重要物理基础设施在内的物理资源同样也面临着风险。加密和身份验证是抵御上述攻击的有效措施。英特尔® Agilex™ 7 FPGA 家族的多个成员（AGF 023/AGF 019 和 AGI 041/AGI 040/AGI 035/AGI 023/AGI 019）采用高性能加密模块与 MACsec 软核 IP 配对，有助于降低风险，控制网络攻击的影响。

网络攻击和数据泄露：症结所在

据面向首席安全官的在线出版物 CSO 近期估计，在 21 世纪 15 起最大的数据泄露事件中，仅前两起事件就有大约 35 亿人的个人数据被盗[1]。数据泄露涉及的对象不乏 Adobe、eBay、Equifax、LinkedIn、万豪国际、麦当劳和大众汽车这些全球性大企业和大品牌的数据库。即使是列入 CSO 榜单的最小事件也牵涉到 1.34 亿人的个人数据被盗。

面临网络攻击威胁的不仅仅是数据，实物资产同样未能幸免。举个例子，因 IT 网络遭遇勒索软件攻击，科洛尼尔管道运输公司（Colonial Pipeline）被迫切断其 IT 和 OT（Operational Technology，运营技术）网络之间的连接，以防止事态扩大。此举导致该公司在 2021 年 5 月不得不将其 5,500 英里的运输管道关闭了数日。科洛尼尔的运输管道承担着向美国东部供应大量燃料的重要作用，管道的关闭引发市民恐慌性抢购汽油，一度导致汽油短缺。

毫不夸张地说，网络攻击已经发展到了“流行病”的程度。数据加密和身份验证可以显著降低这些网络攻击的风险和影响。一些有助于降低风险的加密和身份验证方法包括：

- 保护所有往返云端（网络）的数据
- 保护所有应用之间和微服务之间发送的数据
- 保护所有实时数据以及存储在云端和数据中心的备份数据库
- 保护所有通过蜂窝基站和 5G 网络基站传输的数据

随着网络数据传输速率不断攀升，额外产生的加密开销却因导致时延增加和可用带宽减少而让问题变得更棘手。因此，行业迫切需要能够尽量减少这种额外开销的解决方案。理想情况下，身份验证和加密功能会集成到数据中心、云网络和存储系统基础设施中，这样一来，就可以自动添加这种保护，而不是选择性添加。

目录

数据加密和网络接入控制

加密是保护数据不受安全威胁的第一步。得到妥善加密的数据即便被成功窃取，只要网络攻击者没有加密密钥，这些数据对他们而言就毫无用处。美国国家标准与技术研究院 (NIST) 2001 年制定的高级加密标准 (AES) 已成为全球公认的数据加密标准。据该研究院称，AES 目前的保护范围覆盖了从密级数据和银行交易到线上购物和社交媒体应用在内的各种场景[2]。美国政府已将 AES 作为其官方认可的加密标准。

确保安全的下一步措施是禁止未经授权的实体访问网络和数据。媒体接入控制安全协议 (MACsec，IEEE 标准 802.1AE) 为以太网链路提供点对点安全性。MACsec 可以识别并阻止拒绝服务、入侵、中间人攻击、伪装攻击、被动窃听和回放攻击等大多数安全威胁，能够保护几乎所有网络流量的以太网链路，包括来自链路层发现协议 (LLDP)、链路汇聚控制协议 (LACP)、动态主机配置协议 (DHCP) 和地址解析协议 (ARP) 等多个协议的帧。

安全和加密用例

随着网络攻击和数据泄露的威胁不断增加，安全加密通信的用例也日渐丰富。以下是全新英特尔® Agilex™ FPGA 直接支持的三个此类用例：

- **OvS**：Open vSwitch (OvS) 是一种具备量产级质量的多层虚拟交换机，用于在数据中心的虚拟机 (VM) 之间路由网络数据包。连接数据中心内部和多个数据中心之间各部分的庞大网络结构越来越需要借助安全加密连接来防止网络攻击。在虚拟机之间路由数据包的 OvS 开源网络堆栈可以作为软件在 CPU 上运行，也可以在硬件中实现。最初，数据中心架构师仅在数据中心之间部署安全网关，这是因为人们认为数据中心内的网络通信在物理上是安全的。但随着虚拟机和微服务的出现和普及，现在所有网络通信都可能存在安全风险，因此，整个云网络中使用安全加密通信的情况越来越多。加密技术的广泛使用，以及网络线速的不断提升，导致加密成为一个颇为棘手的通信瓶颈。而采用设计合理的 SmartNIC 和基础设施处理单元 (IPU) 在云和数据中心网络基础设施中建立硬件加密支持，可以从服务器 CPU 卸载加解密任务，进而消除这一瓶颈。
- **面向 5G 网络的 MACsec**：在 3GPP 术语中，Evolved Node B (演进型 Node B，eNB) 指 5G 网络中的小基站。这些小基站使用 IPsec 安全协议与更广泛的 5G 网络进行通信。随着基站设计向虚拟无线接入网 (vRAN) 迁移，部分基站相关的数字处理操作会转移到射频头 (RU)，RU 再通过未受保护的 CPRI 接口与其余的基站硬件进行通信。要将部分数字处理操作转移到 RU，RU 硬件必须支持数据加解密。保护这些 RU 通信的一种方法是通过 RU 设计固有的 CPRI 接口使用 MACsec 协议。
- **网络存储**：如果网络存储仅限于一个数据中心，那么存储通信在物理上是安全的。然而，随着面向网络存储的 NVMe over Fabrics 协议应用得越来越广，存储子系统可以位于世界上任何地方的任何数据中心。因此，网络存储通信如今需要安全的加密保护，因为与存储子系统的通信不再局限于一个物理上安全的数据中心。添加这种加密保护时产生的开销一定不要使时延或带宽压力增加太多，这样就不会出现违反服务级别协议 (SLA) 的情况。实际上，实施加密安全措施必须做到增加的时延可忽略不计，并且不得降低网络存储通信的线速带宽。

颠覆性产品：英特尔® Agilex™ 7 FPGA 和 SoC

英特尔® Agilex™ 7 FPGA 和 SoC 兼具出色的性能、每瓦性能、灵活性和敏捷性，可更好满足日益以数据为中心的世界的需求。它们结合英特尔在多个技术优势领域的数项创新，为边缘、整个网络、数据中心和云的终端产品开发带来重要价值。

这些设备使用英特尔® 嵌入式多芯片互连桥接 (EMIB) 技术和先进的 3D 封装技术，将采用英特尔® 10 纳米 SuperFin 制程工艺制造的高性能 FPGA 内核芯片与针对特定功能各异的通用 Tile (小芯片) 结合在一起。Tile 具备额外的 I/O 功能，包括速度很快的高带宽内存 (HBM) DRAM 以及 PCIe 4.0、PCIe 5.0、CXL 和 116 Gbps 串行收发器端口，以连接到各种主机处理器，如全新第四代英特尔® 至强® 可扩展处理器。这种用于开发 FPGA 和 SoC 的设计和生产方法，使英特尔能够利用量身定制的灵活解决方案快速满足广泛的应用需求。

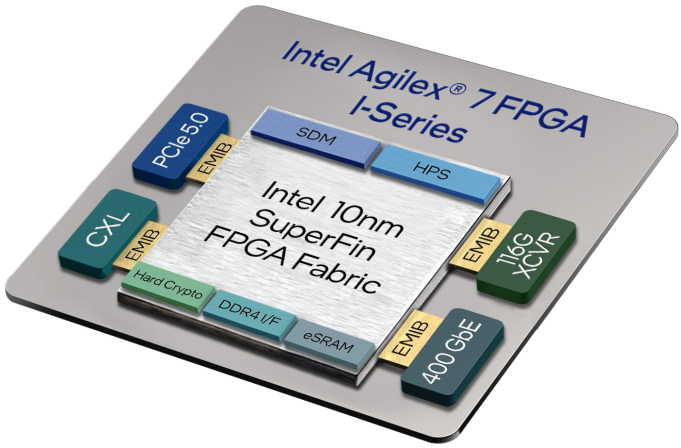

图 1. 开发英特尔® Agilex™ 7 FPGA 所用的基于 Tile 的设计和生产方法，使英特尔能够利用量身定制的灵活解决方案快速满足广泛的应用需求。

面向 200G 和 400G 以太网的加解密硬核支持

英特尔正为英特尔® Agilex™ 7 FPGA 和 SoC 家族增添新成员，这些产品采用高性能加密模块和 MACsec 软核 IP，能够同时以线速支持经过身份验证和加密保护的两个双向 200G 以太网端口或两个单向 400G 以太网端口。这些英特尔® FPGA 和 SoC 针对 IPU、SmartNIC 和 5G 无线网络设备设计进行了优化。具备加解密硬核支持的英特尔® Agilex™ 7 FPGA 和 SoC 家族产品为：

- 英特尔® Agilex™ FPGA F 系列 AGF 019 和 AGF 023 设备，它们具备面向数据中心、网络和边缘计算应用优化的高级数字信号处理 (DSP) 功能
- 英特尔® Agilex™ FPGA I 系列 AGI 019 和 AGI 023 设备，它们已面向需要 PCIe 5.0 处理器接口和 116 Gbps 收发器的带宽密集型应用进行了优化
- 英特尔® Agilex™ FPGA I 系列 AGI 041 设备，支持 400 GbE 和 116 Gbps 收发器，并面向需要增强功能的多主机 PCIe 5.0 以及 CXL 的 400G IPU 和带宽密集型应用进行了优化
- 英特尔® Agilex™ FPGA I 系列 AGI 035 和 AGI 040 设备，它们已面向需要大量网络 I/O 的应用进行了优化

表 1 所示为具有高性能硬核加密模块的英特尔® Agilex™ 7 FPGA 和 SoC 家族产品。有关这些产品更详细的信息，请见英特尔® Agilex™ 7 FPGA 和 SoC FPGA 网页。

全新英特尔® Agilex™ FPGA 和 SoC 的先进加密功能对于开发采用 100 GbE、200 GbE 和 400 GbE 端口的高性能 IPU 和 SmartNIC 以及安全的 5G 无线网络设备至关重要。这些设备的内存资源已针对目标应用进行了调优，这有助于降低功耗，与具有类似逻辑元件密度的其他英特尔® Agilex™ 设备相比，能以更小的封装形式提供。值得一提的是，FPGA 的可重新配置性使这些应用的开发者能够更新自身的产品，以利用硬件加速措施应对新的安全威胁，即使这些应用已经部署到现场，也可以做到。

具有硬核加密模块的英特尔® Agilex™ 7 FPGA 和 SoC														
	F 系列						I 系列							
	AGF 019			AGF 023			AGI 019		AGI 023		AGI 035	AGI 040	AGI 041	
逻辑元件 (LE)（百万）	1.9			2.3			1.9		2.3		3.5	4.0	4.0	
总 RAM (M20K, eSRAM) (Mb)	184			222			184		222		346	443	371	
HPS	支持										N/A		支持	
加密	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
网络 XCVR	24	32	64	24	32	64	72	16	72	16	120		72	20
Tile	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

表 1. 具有硬核加密模块的英特尔® Agilex™ 7 FPGA 和 SoC设备概述请见英特尔® Agilex™ 7 FPGA 和 SoC 设备概述网页。

例如，英特尔® 基础设施处理单元（Intel® Infrastructure Processing Unit，英特尔® IPU）平台 F2000X-PL 利用英特尔® Agilex™ FPGA AGF 023 实现基于 FPGA 的高性能云基础设施加速平台，该平台具有 2 个 100 GbE 网络接口和硬件加密模块，能以线速实现安全防护。它能够支持云基础设施工作负载，例如 Open vSwitch、NVMe Over Fabrics（NVMe-oF）和 RDMA over Converged Ethernet v2（RoCEv2）。更多信息请见英特尔® 基础设施处理单元平台 F2000X-PL 网页。

有助于优化 TCO 的英特尔® eASIC™ 设备

英特尔® Agilex™ FPGA 的可编程逻辑结构还能让开发人员对快速变化的标准和不断演进的协议及时作出响应，包括系统部署到现场后的更新。

除此之外，英特尔还提供英特尔® eASIC™ 设备。英特尔® eASIC™ 设备属于结构化 ASIC，这是一种介于 FPGA 和标准单元 ASIC 二者之间的中间技术。与 FPGA 相比，这些设备的单位成本和功耗更低；与标准单元 ASIC 相比，它们的上市时间（TTM）更快、一次性成本投入（NRE）更低。一旦基于英特尔® Agilex™ 7 FPGA 的设计得到验证，该设计就可以被固化然后置入成本和功耗更低的英特尔® eASIC™ 设备（图 2）。

图 2. 英特尔提供一种 FPGA 到英特尔® eASIC™ 设备的降本降耗路径

具体来说，对于 IPU 和 SmartNIC 应用，英特尔® eASIC™ N5X080 设备具备以下特性：

- 877 万个 eCell/逻辑元件、按照客户要求定制的封装
- 8 MB Mega SRAM、高达 229 Mb 的 bRAM 10K 嵌入式内存，加上高达 20 Mb 的寄存器文件内存
- 支持 64 路 SerDes（NRZ）收发器，速率范围是 250 Mbps 至 32.44 Gbps
- 8 路支持高达 53 Gbps 传输速率的 SerDes（PAM4）收发器
- 8 个硬核 PCIe 5.0 控制器，支持 x8 和 x4 配置
- 2 个可连接至 8 个 53G SerDes 收发器的硬核 200G 以太网 MAC*

注 *：硬核控制器采用旁路模式支持其他 SerDes 通道协议。

行动号召：了解更多信息

有关英特尔® Agilex™ 7 FPGA 和 SoC 家族的更多信息，请见以下网页：

- 英特尔® Agilex™ FPGA 为当今以数据为中心的世界提供出色的灵活性和敏捷性。
- 英特尔® Agilex™ 7 FPGA 和 SoC 设备概述

参考资料

1. The 15 biggest data breaches of the 21st century（21 世纪 15 起最大的数据泄露事件），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（新研究披露，NIST 的加密标准创造了至少 2,500 亿美元的经济效益），www.nist.gov/news-events/news/2018/09/nists-encryption-standard-has-minimum-250-billion-economic-benefit

intel