

在部署之前确保融合 5G 网络的安全

Maurizio Di Paolo Emilio

5G 网络在推动物联网应用变革方面潜力巨大。但日益严峻的安全问题甚至可能会在 5G 部署之前，对其性能产生威胁。

挑战从物联网设备密度开始。5G 可以支持每平方英里 **260 万台设备**，每个连接都必须是安全的。安全功能的列表越来越长。数据包检查、密钥生成和存储以及端到端加密只是网络架构师必须考虑的部分问题。

这些安全要求可能会成为束缚性能的严重瓶颈。例如，单个 **SSL/TLS 握手** 最多可以占用处理器资源的 2%，并增加 5 毫秒的延迟。

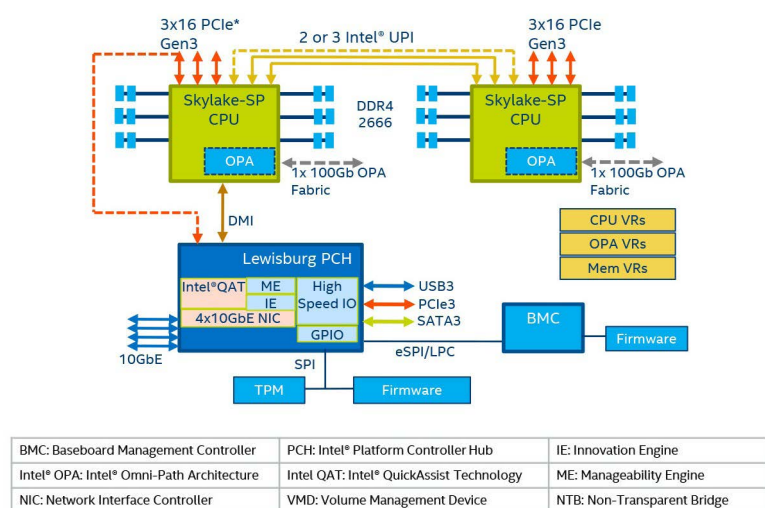
此外，安全要求也会增加系统成本。例如，深层数据包检查 (DPI) 通常需要添加专用的多核处理器或硬件加速器。

寻求利用 5G 的 CSP 应该警惕安全性可能影响其系统的方式，以及可以弥补这些局限性的解决方案。

将 5G 安全瓶颈转变为安全闸门

英特尔® 至强® 可扩展处理器 提供一种可能的解决方案。全新处理器在 8 插槽配置中支持多达 224 个内核和 12 TB 内存 (**图 1**)，提供安全 5G 网络运营所需的数据包处理和控制平面资源。

新的芯片在各种 5G 任务中可极大地提升性能。这些包括 L3 数据包转发的 **1.77X 倍速度提升**、IPSec 性能的 **2.5 倍加速**，以及 SSL Web Proxy 传输的 **2.4 倍速度提升** (**图 2**)。



Feature	Details
Socket	Socket P
Scalability	2S, 4S, 8S, and >8S (with node controller support)
CPU TDP	70W – 205W
Chipset	Intel® C620 Series (code name Lewisburg)
Networking	Intel® Omni-Path Fabric (integrated or discrete) 4x10GbE (integrated w/ chipset) 100G/40G/25G discrete options
Compression and Crypto Acceleration	Intel® QuickAssist Technology to support 100Gb/s comp/decomp/crypto 100K RSA2K public key
Storage	Integrated QuickData Technology, VMD, and NTB Intel® Optane™ SSD, Intel® 3D-NAND NVMe & SATA SSD
Security	CPU enhancements (MBE, PPK, MPX) Manageability Engine Intel® Platform Trust Technology Intel® Key Protection Technology
Manageability	Innovation Engine (IE) Intel® Node Manager Intel® Datacenter Manager

图 1. 英特尔® 至强® 可扩展处理器可在 8 插槽配置中提供最多 224 个内核和 12 TB 系统内存。这为安全的 5G 通信提供了充足的资源。
(来源: [PC Perspective](#))

Accelerate Network Traffic with Intel® Xeon® Scalable Platform, DPDK, and Intel® QAT

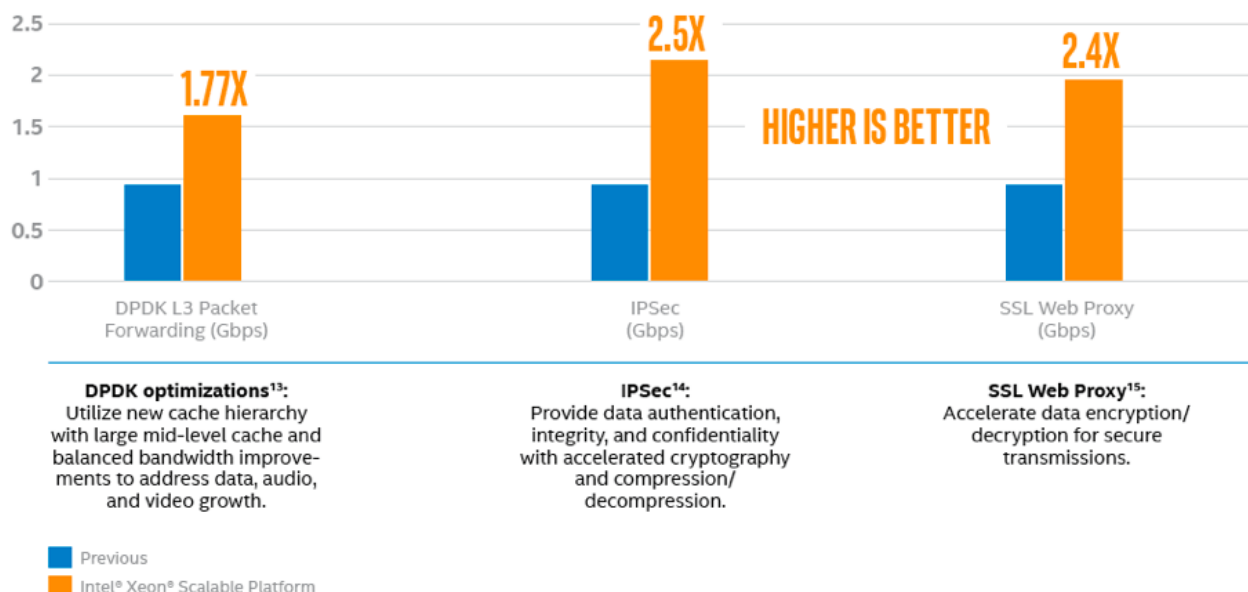


图 2. 英特尔® 至强® 可扩展处理器可加速重要的安全工作负载。（资料来源：英特尔）

与上一代处理器相比，英特尔® 至强® 可扩展处理器还支持 每台服务器运行的虚拟机数量增加 1.5 倍。因此，CSP 可以整合多个服务器平台，降低 5G 部署的成本和复杂性。

全新设计的高级网络安全性能

全新英特尔® 至强® 处理器包括几项重要的架构增强功能，从而支持它们达到上述基准。尤其是英特尔® 高级矢量扩展 512（英特尔® AVX-512）、改进的芯片架构以及更新的互连和结构接口，这些都有利于 5G 网络安全。

英特尔® AVX-512 是一组新的指令，旨在优化超宽（512 位）矢量运算，例如用于生成加密基元的矢量运算。每个内核的两个 512 位混合乘加 (FMA) 单元都支持这些指令，这有助于实现与上一代相比，AVX-512 每个时钟周期的每秒浮点运算次数增加一倍。

在利用英特尔® AVX-512 时，这种性能提升带来了 SHA 哈希算法 快 3.1 倍，Reed Solomon Erasure Code 的处理速度 快 2 倍。

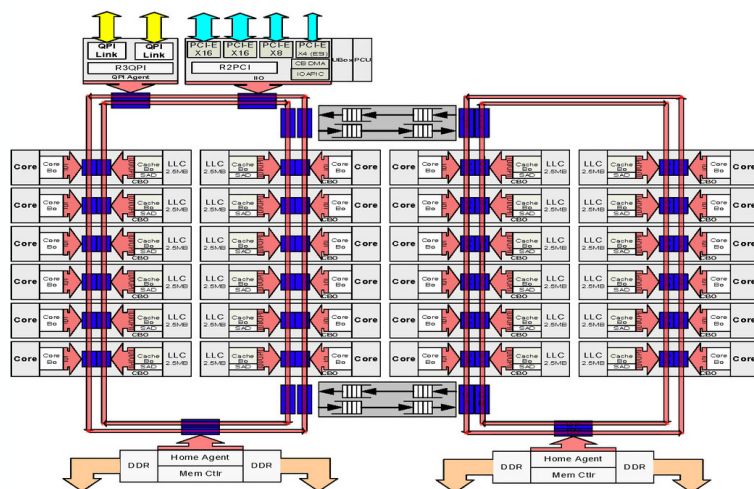
为了防止功能强大的全新英特尔® 至强® 处理器受 I/O 约束，14 纳米的 Skylake-SP 微架构也在网状拓扑中进行了重新设计（图 3）。片上网络互连有利于实现更高的带宽、更低的内核到内核通信延迟。这有助于优化任务调度/传输，并降低网络服务器和 UTM 系统的能耗。

片外 I/O 也进行了更新，可将性能扩展到单个处理器之外。对于初级入门者，全新的英特尔® 至强® 可扩展处理器包含最多 48 个 PCIe 3.0 链路和 6 个支持 2666 MHz DDR4 DRAM 的内存通道。后者相当于与上一代相比，内存带宽增加了 50%。

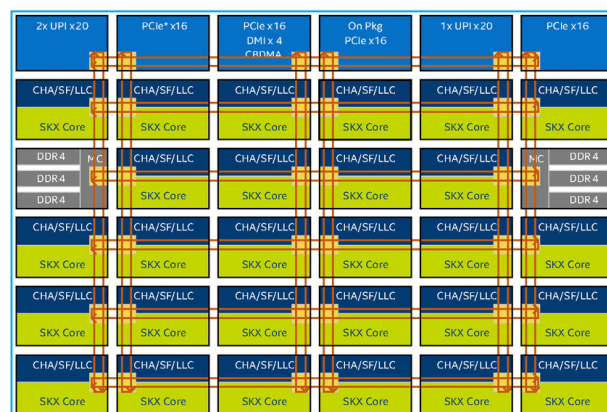
但是，大规模可扩展 5G 网络基础设施的主要 I/O 增强功能在于插槽到插槽和系统到系统的连接。

在插槽之间，英特尔® 超级通道互连（英特尔® UPI）提供了 CPU 插槽之间缓存一致的 10.4 GTps 数据路径（图 4）。互连可以扩展到每个系统在单个共享地址空间支持最多八个处理器，每个英特尔® 至强® 可扩展处理器包括 2 路或 3 路本机英特尔® UPI 链路。

Broadwell EX 24-core die



Skylake-SP 28-core die



CHA – Caching and Home Agent ; SF – Snoo Filter; LLC – Last Level Cache
SKX Core – Skylake Server Core ; UPI – Intel® UltraPath Interconnect

图 3. Skylake-SP 微架构采用全新的片上网状拓扑，可以在资源密集型多核网络应用中提高带宽并减少延迟。（来源：[Hardware.Info](https://www.hardware.info)）

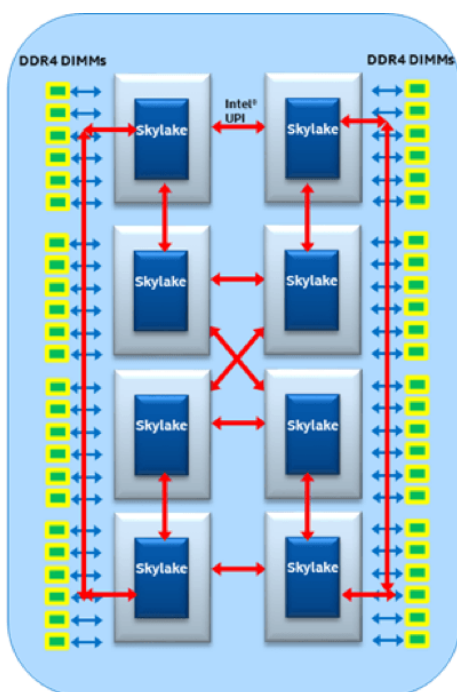


图 4. 英特尔® 超级通道互联（英特尔® UPI）可在 CPU 插槽之间提供缓存一致的 10.4 Gbps 通信。这可以使用相同的共享地址空间扩展到最多 8 个插槽。（资料来源：英特尔）

为了实现和保护由每平方英里数百万台设备组成的 5G 部署，英特尔® Omni-Path 架构（英特尔® OPA）为每个高性能计算（HPC）网络集群提供 10,000 或更多节点。

英特尔® OPA 是英特尔® TrueScale Fabric 的后续产品，并被定位为 InfiniBand 的下一代替产品。然而其成本和 100 Gbps 线路速率目前可与其他竞争技术相媲美，[英特尔® OPA 的功能集](#)是 5G 网络在竞争中脱颖而出的关键所在：

- **传输流量优化** – 无论数据包的顺序如何，较高优先级的数据包可以先于较低优先级的数据包进行传输
- **动态通道扩展** – 在通道发生故障时保持链路连续性
- **数据包完整性保护** – 将向所有数据包应用链路级错误检查，实现对传输错误进行透明检测和恢复

英特尔® OPA 集成在英特尔® 至强® 可扩展处理器的封装中，以轻松进行 HPC 网络和安全应用程序的部署。

实现近乎为零的加密开销的配套产品

为了最大化处理器性能，英特尔® C620 系列芯片组（原代号为“Lewisburg”）从主处理器卸载了加密工作负载。芯片组预装了英特尔® 通信加速技术（英特尔®

QAT) 以提供网络安全功能, 包括:

- 对称加密和身份验证
- 非对称加密
- 数字签名
- 无损数据压缩
- RSA、Diffie-Hellman 和椭圆曲线加密 (ECC) 功能

此外, 芯片组还集成了[英特尔® 密钥保护技术 \(英特尔® KPT\)](#)。英特尔® KPT 是一项新功能, 可帮助保护存储在硬件中的敏感私钥免受软件和探测攻击 (**图 5**)。

英特尔® KPT 与英特尔® QAT 相互配合, 实现了静态数据和动态数据近乎为零的加密开销, 减少了对专用硬件安全模块 (HSM) 的需求。

英特尔® QAT 还支持所有标准设备虚拟化模式。这将英特尔® QAT 和英特尔® KPT 的功能扩展到系统中运行的所有虚拟机 (VM)。

5G 和融合基础设施的转变

5G 网络架构打上了“融合”基础设施的印记。在这种模式中, 专用网络设备被同时处理多个网络功能的系统取代。

因此, 网络设备提供商 (NEP) 持续将基于标准的硬件平台推向市场, 该平台在单个软件包中支持网络、存储、安全和其他功能。

例如, [ADLINK Technology MCN-2610](#) 是基于英特尔® 至强® 可扩展处理器的计算节点 (**图 6**)。它提供 4×10 GbE 通道, 以最大限度地提高英特尔® 至强® 可扩展处理器在 UTM 系统和 5G 网络服务器中的性能优势。

MCN-2610 遵循开放计算项目 (OCP) OpenSled 规范。OpenSled 是 ADLINK Technology 出品的开放式电信级边缘计算参考架构 ([OCCERA](#)), 它强调基于模块化工业设计标准的 NFV 和 SDN 原则。

OpenSled 基于标准的方法能让模块在融合的基础设施平台中提供按需资源。例如, 随着需求的变化, UTM 系统中的 MCN-2610 模块可以在 DPI 和通用路由之间动态切换。

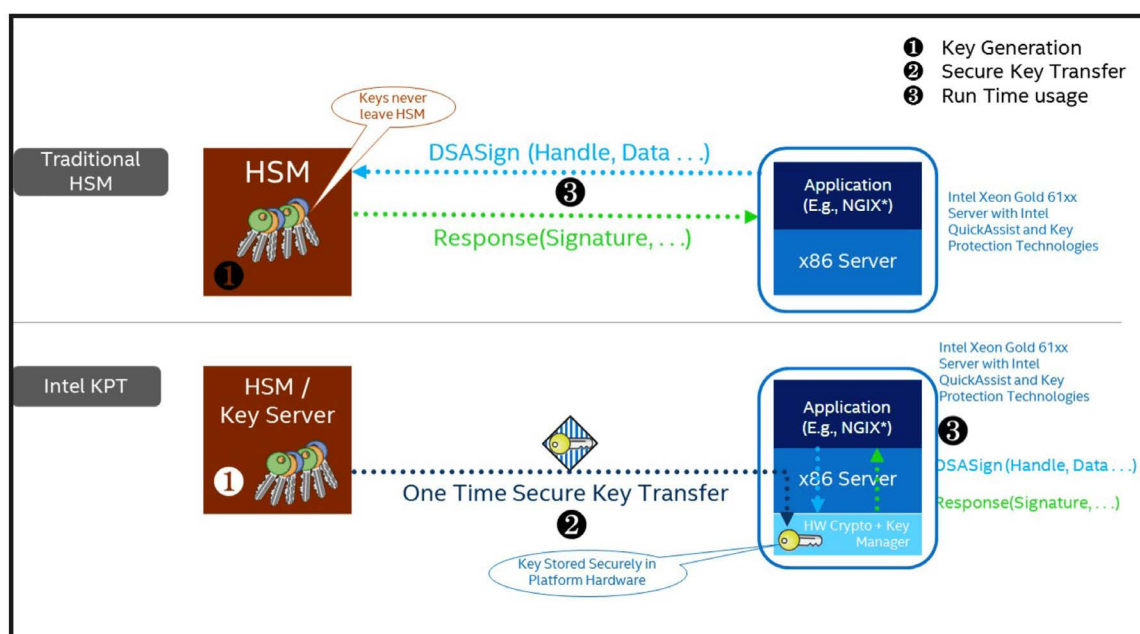


图 5. 英特尔® KPT 保护存储在硬件中的敏感私钥免受软件和探测攻击。(资料来源: 英特尔)

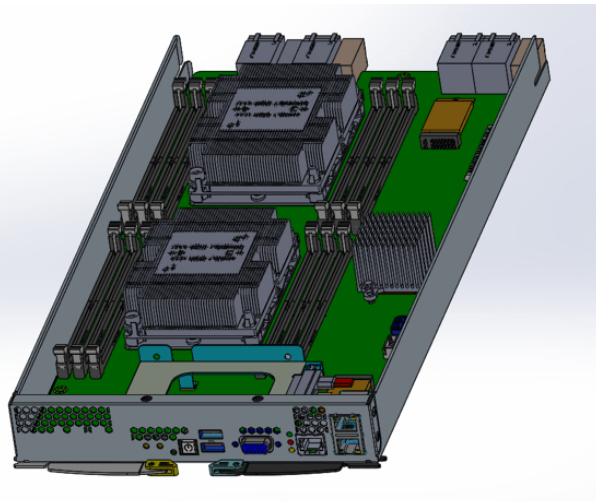


图 6. ADLINK Technology MCN-2610 是一款基于英特尔® 至强® 可扩展处理器的数据中心计算节点，最多可支持 28 个内核。
(资料来源: ADLINK Technology)

这样的架构将有助于轻松实现向 5G 网络架构的过渡。

在部署之前确保 5G 网络安全

由于性能的大幅提升，5G 网络有可能启用全新的生态系统和服务。除了传统的网络应用之外，这些优势还适用于蓬勃发展的物联网机会。

寻求利用 5G 优势的 CSP 应该警惕安全性可能影响其系统性能的方式，以及可以弥补这种开销的解决方案。

凭借英特尔® 至强® 可扩展处理器和像 MCN-2610 这样的计算节点，他们在向融合 5G 基础设施的转型中需要牢牢把握这些机会。