insight.tech
POWERING IoT AND EMBEDDED INNOVATION

# 将数据中心计算融入到战术优势

Majeed Kamran

人工智能 (AI) 和其他先进的分析对于国防应用具有巨大的吸引力。 当这些技术整合到信号情报 (SIGINT) 和战术通信之中时，即可帮助指挥官加快决策速度以及提高任务成功率。

难点仍然是在严格的尺寸、重量和功耗 (SWaP) 限制下实施数据中心级计算。 长效性着实令人担忧，因为数据中心技术发展迅速，但国防技术的部署往往需要十年，甚至更长时间。

英特尔® 至强® 可扩展处理器（原代号为“Purley”）则解决了这两方面的难题。 这些芯片在每个插槽上最多可具备 28 个内核，但额定热设计功耗 (TDP) 低至 80 W，使芯片可以在 SWaP 受限的环境下应用，例如战术优势计算。

而且，新款处理器及其配套 C620 系列芯片组（原代号为“Lewisburg”）有长达 10 年的使用可靠性可供考证，并且生产供货期可长达 15 年， 这不啻为长期部署的可靠选择。

## 新指令大幅提升信号处理能力

新款处理器提供了一系列重要升级，可以在保持 TDP 限制的情况下提升性能。 最值得一提的是英特尔® AVX-512 指令集扩展。 英特尔® AVX-512 数学单元处理要求苛刻任务（例如 AI/深度学习工作负载、图像和音频/视频处理以及加密）吞吐量的能力翻倍。

Artesyn Embedded Technologies. 高级售前技术架构师 Rob Persons 说道：“战术系统一般使用 CPU 本身的计算能力，而不会依靠向量单元的能力提高。 因此，当战术系统尝试以较小的体量执行更多任务时，向量单元的能力就变得更有吸引力。”

Persons 还指出，内存带宽的大幅提升能够帮助支持 AVX-512 向量单元的性能提高。 现在，英特尔® 至强® 可扩展处理器与前几代产品相比，每个插槽的系统内存已经翻倍，达到了 1.5 TB，可支持内存受限的应用。

而且，这些增强功能还使 LINPACK 库执行能力提升了 2.2 倍。 LINPACK 基准性能测试测量数字线性代数表达式（例如信号处理应用中使用的表达式）的计算。

## 芯片组卸载加密

英特尔® C620 系列芯片组借助英特尔® QuickAssist 技术（英特尔® QAT）进一步增强了性能。 此功能可以从处理器卸载数据加密，帮助国防网络工程师实施物联网式的传感器数据通信，而不会增加主机处理器的加密工作负载负担。

C620 系列芯片组还整合了英特尔® 密钥保护技术（英特尔® KPT），确保对端到端通信进行加密 **（图 1）**。 英特尔® KPT 以近乎为零的主机处理器加密开销来提供安全密钥生成和存储、安全密钥调配、启动时间密钥共享及运行时使用。

此外，它还帮助基于硬件的安全密钥抵御各种电子战的侵袭，包括：

- 网络攻击
- 软件和固件 (BIOS) 攻击
- 侦听（硬件）

英特尔® KPT 与英特尔® QAT 结合，降低了对于昂贵的硬件安全模块 (HSM) 的需求。

如**图 2** 所示，可以通过 4 个 10 GbE 端口、一个 16 通道 PCIe 第三代链路和一个直接内存接口 (DMI) 从 C620 系列芯片组实现这些功能。

Persons 介绍道：“新推出的 10 Gb 通信信道 PCH 与英特尔® QAT 结合，可在远离系统的位置，创建加密数据网关。 新功能集可增加一些额外功能，从而提高数据离开系统时的安全性。”

| | |
|---|---|
| Types of Keys Protected | • Asymmetric Private Keys (Signing, Encryption) |
| Algorithms Supported | • RSA1K, RSA2K, RSA3K, RSA4K (Type 1, Type 2)<br>• DSA1K,DSA2K,DSA3K,DSA4K<br>• ECC Point Multiplization<br>• ECDSA with all NIST standard curves in FIPS PUB 186-3 |
| Keys are Protected from | • SW Attacks, Network Attacks, Privilege<br>• Escalation, Rootkit, BIOS/Firmware attacks<br>• HW Probe Attacks |
| Wrapping Algorithms | • AES128-CB AES192-CBC,AES256-CBC<br>• AES128-GCM, AES192-GCM, AES256-GCM<br>• Up to 256 iterations of keywrap |
| [1]Performance | • Over 95% of peak performance of Intel® QAT for corresponding private key operation without Intel® KPT |

**图 1.** 英特尔® 密钥保护技术（英特尔® KPT）帮助提供了安全的端到端通信。（资料来源：英特尔）

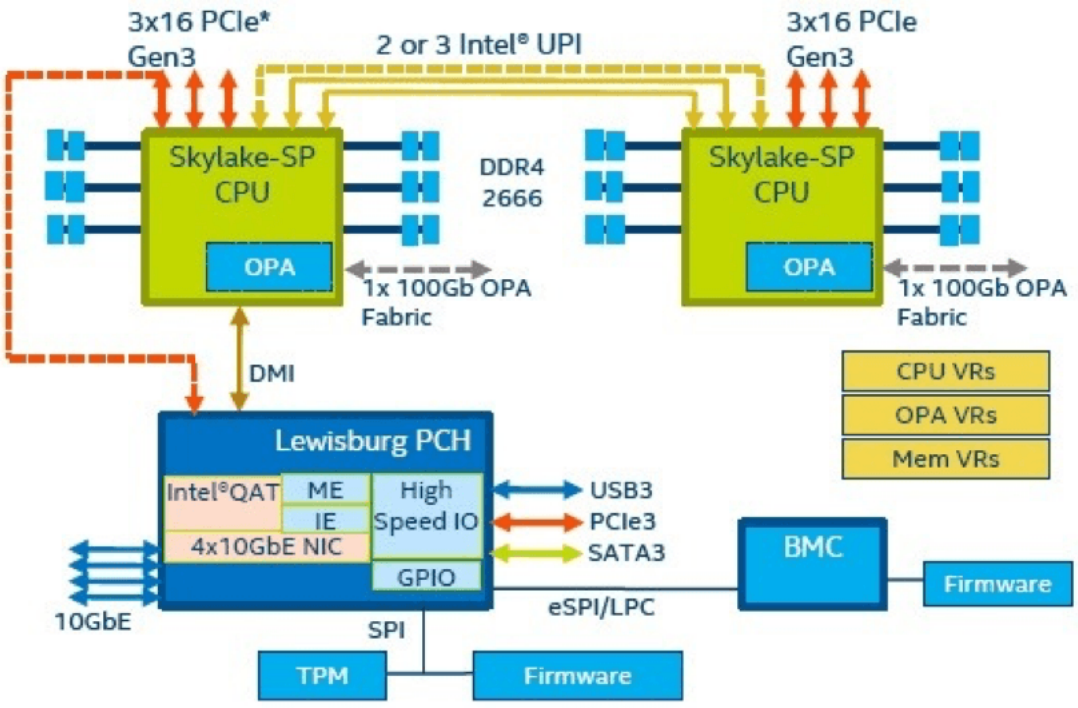


**图 2.** 英特尔® C620 系列芯片组嵌入英特尔® QAT，可降低加密开销。（资料来源：英特尔）

insight.tech

## 模块化开放式系统方法

当然，国防工程师必须遵守模块化开放式系统方法 (MOSA)，这样才能充分利用新款处理器。 MOSA 合规有助于实现一个由电子组件、主板和系统组成的具有竞争力的开放式生态系统，从而防止供应商闭锁。

ATCA 刀片（例如 Artesyn 开发的 ATCA-7540）便是这种方法的一个良好示例。 这些网络刀片遵守 MOSA 原则，而且可以搭载新款处理器。 例如，ATCA-7540 便配备了两个英特尔® 至强® 可扩展插槽 **（图 3）**。 主板已经为机载和舰载数据中心、地面控制站、网络数据分析及指挥、控制、通信、计算机、情报、监视和侦察 (C4ISR) 的运作而优化。


**图 3.** ATCA-7540 服务器刀片专为计算密集型国防通信设计。（资料来源：Artesyn Embedded Technologies）

英特尔® 至强® 可扩展处理器的 48 个 PCIe 通道支持 ATCA-7540 的高带宽背板连接、高性能前面板 I/O 以及载波模块区 **（图 4）**。

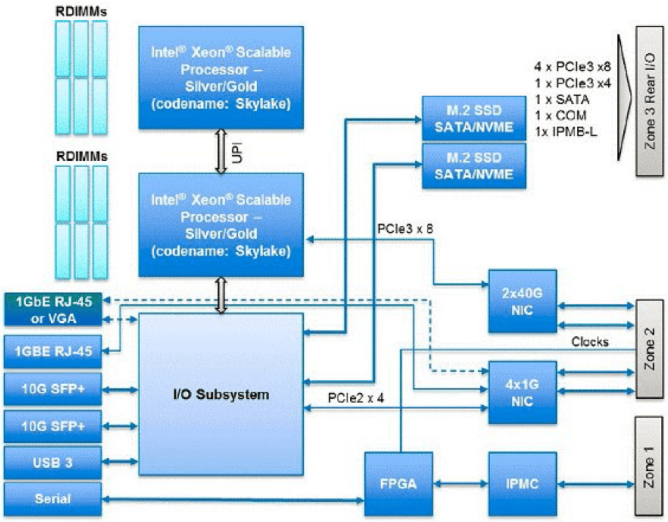


**图 4.** ATCA-7540 刀片受益于经过优化的内存和英特尔® 至强® 可扩展处理器的 I/O 设计。（资料来源：Artesyn Embedded Technologies）

借助 ATCA-7540，强大的多插槽信号处理系统可以部署在紧凑的 8U ATCA 服务器机柜中。 而且，通过此架构，操作人员可以热插拔替换主板，而不必更新系统软件或基础设施。

## Purley 提升了 ATCA 长效性

军事系统必须通过更新换代才能利用不断涌现的技术，例如可以改变战局的 AI 和物联网。 但执行这些技术必须考虑 SWaP 和长效性。

英特尔® 至强® 可扩展处理器与 ATCA 标准结合需要国防系统设计师们在这些方面有所作为。 指挥官们现可利用战术优势数据中心的强大功能。