Integrated Cryptographic and Compression Accelerators on Intel® Architecture Platforms

High performance, scalability, and ease of use allow network device manufacturers to dramatically decrease development time.

Workload Acceleration Challenges
Demands on cloud and network equipment are escalating at breakneck pace, driving the need to deliver ever higher levels of traffic throughput and security. To keep up with market requirements, network equipment manufacturers often accelerate compression and cryptographic workloads using commercially-available add-in cards, which can be time consuming to optimize performance using scarce programming resources. Developers preferring to use open source software, like OpenSSL or IPsec, may find accelerator card vendors either deviate from open source APIs, hindering software portability, or are slow to respond to API updates, thus delaying support for new features.

Built-in Acceleration
With Intel QuickAssist Technology, Intel is making it easier for equipment manufacturers to deliver high-performance compression and cryptography on devices deployed in wireless, telecom, cloud, data centers, and enterprise systems. The technology is integrated in a family of pin-compatible Intel® chipsets that deliver scalable crypto performance - from 0 to 50 Gbps - via on-chip hardware accelerators. Additionally, crypto accelerators are available on select members of the Intel® Atom™ processor C2000 product family, which makes these system-on-chip (SoC) solutions ideal for entry-level, network equipment. The compression and cryptography performance of these products is shown in Table 1.¹

This solution brief provides an overview of the integrated cryptographic and compression accelerators available on select Intel® architecture platforms, and is one in a series of five briefs describing how to maximize the benefits from Intel® QuickAssist Technology. Please see the Resources section for links to the series.
Open Source Software Support

Intel QuickAssist Technology supports the open source frameworks and applications shown in Table 2, accelerating cryptography and data compression workloads. The use of open frameworks enables application developers to benefit from the acceleration technology with minimal software development effort.

---

**Table 1.** Results from Compression and Cryptography Performance Testing

<table>
<thead>
<tr>
<th>Workload</th>
<th>Open Source Framework</th>
<th>Open Source Applications</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cryptography</td>
<td>OpenSSL, libcrypto,</td>
<td>IPsec (NETKEY), Apache</td>
</tr>
<tr>
<td></td>
<td>Linux Kernel Crypto</td>
<td></td>
</tr>
<tr>
<td></td>
<td>API (scatterlist)</td>
<td></td>
</tr>
<tr>
<td>Data Compression</td>
<td>zlib</td>
<td>File Compression (minigzip)</td>
</tr>
</tbody>
</table>

---

**Table 2.** Supported Workloads and Open Source Frameworks and Applications
Ease of Use
With minor changes to a software build, developers can significantly boost performance of the open-source frameworks listed in Table 2 using Intel QuickAssist Technology. Software developers just need to add Intel-developed Linux® Kernel patches or Open Source Framework patches – available at no cost – to attain around an order of magnitude (e.g., ten-fold) performance improvement. Even higher performance levels can be achieved by equipment manufacturers when their network applications (in Linux user-space or kernel-space) communicate directly with the built-in accelerators through the highly-extensible API. Figure 1 depicts the symmetric cryptography, public key, and compression/decryption hardware accelerators present on an Intel® processor-based platform with Intel QuickAssist Technology.

These accelerators can be accessed by proprietary applications, or open-source functions and OS libraries via the Intel QuickAssist Technology API. The available patches and Linux kernel changes are designed to increase portability and performance.

Figure 1. Accessing Intel® QuickAssist Technology Accelerators
Hardware Options

Intel QuickAssist Technology is available in two different form factors: chipsets and server accelerator cards. For the lowest cost, power, and board footprint, the Intel® Communications Chipset 89xx series can be paired with the Intel® Xeon® processor E5-2600 v2 product family, or a two or four-core Intel processor in a BGA package. The recently launched Intel® Communications Chipset 8950 improves the crypto acceleration performance by 2.5 times over the Intel® Communications Chipset 8920 and accelerates compression workloads by up to 20 Gbps. All Intel Communications Chipset 89xx series are pin compatible, so a common board design can be configured from no crypto (Intel® Communications Chipset 8900) to 50 Gbps crypto acceleration performance (Intel Communications Chipset 8950).

Additionally, Intel offers Intel QuickAssist Technology Server Accelerator Cards (Figure 2), which plug into a PCI Express® Gen 3 x8 slot on existing servers based on the Intel Xeon processor E5-2600 v2 and Intel® Xeon® processor E5-2400 product families. Since most servers have an available x8 slot, these accelerator cards are typically easier to deploy than other accelerator cards that require the less common PCI Express Gen 2 x16 slot. Two server accelerator cards are available:

- Intel® QuickAssist Adapter 8920-SCC: up to 20 Gbps crypto acceleration performance
- Intel® QuickAssist Adapter 8950-SCCP: up to 50 Gbps crypto acceleration performance

Since these accelerator boards are based on the same technology as the Intel Communications Chipset 89xx series, they are low power and do not require active heat sinks.

Future Proof

Applications can use the Intel QuickAssist Technology API to communicate directly with acceleration hardware, providing the highest performance. Alternatively, applications can call the associated open source APIs, which will use either Intel-developed patches (for platforms containing hardware acceleration with Intel QuickAssist Technology) or software optimizations based on the latest Intel instruction set architectures. In other words, application code calling an open-source framework (e.g., OpenSSL) remains the same regardless of whether the acceleration is provided by a software module or a hardware accelerator on the platform. Likewise, application code does not have to change as technology evolves (i.e., new encryption feature) since the Intel QuickAssist Technology API will maintain backward-compatibility, thereby future-proofing equipment manufacturer software.

Flexible Workload Acceleration on Intel® Architecture

As the complexity of networking and security applications grows, more systems will need to offload cryptography and data compression workloads, making more CPU cycles available for other functions, like deep packet inspection (DPI) and traffic management. Intel QuickAssist Technology offers a high-level of flexibility with optimized support via shims for both open source or propriety implementations of these functions. Moreover, the high performance, scalability, and ease-of-use benefits derived from Intel QuickAssist Technology allow equipment manufacturers to shorten their time to market for next-generation network devices.

Performance tests and ratings are measured using specific computer systems and/or components and reflect the approximate performance of Intel® products as measured by those tests. Any difference in system hardware or software design or configuration, as well as system use patterns including wireless connectivity, may affect actual test results and ratings.

Copyright © 2013 Intel Corporation. All rights reserved. Intel, the Intel logo, and Xeon are trademarks of Intel Corporation in the United States and/or other countries.

*Other names and brands may be claimed as the property of others.

Printed in USA  MS/VC/1113  Order No. 329879-001US