

## Specifications

<p>Tested and Verifiable on Intel® Arria V GX FPGA FPGA 125 MHz</p> <ul style="list-style-type: none"> <li>• Encrypt and update key in 1 clock cycle</li> <li>• Latency 10 nanoseconds</li> <li>• 4 GBytes/sec</li> <li>• Less than 200 source lines of Verilog code</li> </ul>	<p>Next-Generation designed for Application Specific Integrated Circuit (ASIC)</p> <ul style="list-style-type: none"> <li>• 1000 MHz</li> <li>• 1 clock cycle</li> <li>• Latency 4 nanoseconds</li> <li>• 2500 MHz Throughput</li> <li>• 80 Gigabytes per second</li> </ul>	<p>To put these performance numbers in perspective:</p> <ul style="list-style-type: none"> <li>• Intel's fastest AES software encryption (using a hardware accelerator chip running at 3.33 GHz) requires 5.7 cycles/BYTE to encrypt at 0.5 GB/sec</li> <li>• Using the same implementation, QwyitChip™ would encrypt at 1.584 TeraBytes/Sec. This is <b>over 3,150 times faster!</b> *</li> <li>• And...Provably Secure (mathematically, not bit-fiddled like AES in CBC mode)</li> </ul>
---	---	--

- **FPGA architecture, demos available**
- **Verilog code available**
- **QwyitCipher™ is 1 Qwyit™ primitive, 2 instructions, 1 machine cycle: PDAF\_SEC**
- **FPGA space consideration is the only design constraint: key size can vary up to available space**
- **QwyitChip™ can process the 'gate width' in 1 cycle – if this is 1KB, then QC™ encryption/decryption is 1 KB/cycle**
- **QwyitChip™ is the world's fastest Encryption Chip – by several orders of magnitude**
- **Multiple FPGAs on a single 'Encryption Processor/Chip' produce unheard of speed**
  - Based on the new [Achronix Semiconductor 1.5GHz FPGA](#), a 1.5GHz Chip with a 1MB key size, **would encrypt/decrypt 1.5 PetaBytes per second**
    - 1.5GHz is 1,500,000,000 cycles/second
    - QwyitChip™ takes 1/cycle per *key size*
    - A 1MB key size would encrypt 1.5 billion times per second (1,500,000,000/1)
    - 1,000,000 Bytes times 1,500,000,000 times/second is 1,500,000,000,000,000 bytes/sec

***The 2.5 Quadrillion Bytes (2.5 x 10<sup>18</sup>) of daily Internet data would encrypt in less than 30 minutes!***

- **QwyitChip™ is 100% provably secure and already Quantum Safe!**
- **QwyitSDK™ operates identically in Software – speed limited only by programming/buffer sizes**
- **QwyitKey™ provides *one-step* programming for QwyitChip™/QwyitSDK™ instant operation: Get A Key, Call QC™!**

\*- Intel Core i7 executing ~30IPC ∴ ((256-bits x 15IPC) x 3.33 x10<sup>9</sup> cycles/sec)/8-bits/Byte = 1.584x10<sup>12</sup> Bytes/sec