Qwyit® Announces Major Break Through in Encryption Speed
The QCy™ Encryption Engine (patent pending)

Building on its 20-year track record of lightning fast provably secure patented encryption systems, Qwyit® today announces THE FASTEST possible encryption – AND it's provably secure. Qwyit®'s new patent-pending QCy™ Encryption Engine can encrypt incoming data in a single clock cycle. Nothing can ever be faster. Today's networks would benefit from true hardware encryption – and none exists. Qwyit® products meet today's needs: QwyitChip™ (hardware) and QwyitSDK™ (software) are the World's Fastest, Most Efficient, Provably Secure Encryption Engines available.

QwyitChip™ Demonstration

Qwyit® implemented its QCy™ Encryption Engine using an Intel® Arria V GX FPGA. Encrypting a reference file requires only two instructions to perform the entire QCy™ Encryption Engine: key selection, cipher (encrypt or decrypt) and key update, all in a single clock cycle.

In the demonstration architecture of the QCy™ Encryption Engine, Qwyit® used one bit per I/O pin. The Arria V chip can input and output 256 bits simultaneously. Propagation through the chip when running the QCy™ Encryption Engine is only 10 nanoseconds. The QCy™ Encryption Engine steps take two instructions thereby passing output data at the same rate as input data. This QCy™ Encryption Engine demo also updates the key *every 256-bits* in this single clock cycle. When comparing QCy™ to other systems like AES, 'key scheduling' (not included in their timing) would have to be performed *every 256-bits* and their published benchmarks would actually be 10-100X *slower.*

Benchmarks – Simulation and Verifiable - Arria V GX FPGA

- Intel Arria V GX FPGA 125 MHz data clock
- Encrypt and update key in 1 clock cycle
- Latency 10 nanoseconds
- 32 GBits/sec (4 GBytes/sec)
- Less than 200 source lines of Verilog code
- Portable HDL code for integration into any H/W architecture – FPGAs, CPUs, GPUs, etc.

Market Comparison – Let's put this Incredible Performance in perspective

2.5 Quintillion Bytes are added to the Internet every day (2.5 x 10^{18} bytes). Using a single desktop computer,

QCy™ would be able to encrypt every single bit of it in *18 hours*!
Using AES, it would take 5.1…*years!*

The AMD 3990X performs 2,356,230 MIPS at 4.35Ghz:

QCy™ Encryption Engine	**AES Encryption**
32 bytes in 2 Instructions; 37,699 GBytes/Sec on the AMD	1 byte in ~150 Instructions*; 15.708 GBytes/Sec on the AMD
Timing: 66,313.560 seconds (2.5 x 10^{18} bytes/ 37.699680 x 10^{12} bytes/sec)	Timing: 159,154,571 seconds (2.5 x 10^{18} bytes/ 15.708 x 10^{9} bytes/sec)
18.42 *hours* to encrypt an 'Internet Day' (66,313.560 sec /3600 sec/hr)	**5.1 *years* to encrypt an 'Internet Day'** (159,154,571 sec/ 31,536,000 sec/yr)

*Intel's fastest AES encryption (hardware accelerator chip running at 3.33 GHz) requires 5.7 cycles/Byte to encrypt at 0.5 GB/sec; measured when the Intel AES-NI chipset was released in 2011 (still the current version) on an Intel Core i7 computer executing ~30 Instructions/clock cycle