Qwyit® Announces Heretofore Impossible 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 or decrypt 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.

QwyitChip™ Demonstration

Qwyit® implemented its QCy™ Encryption Engine on video streaming using an Intel® Arria V GX 150 MHz FPGA and a Bitec HSMC HDMI 2.0 Daughter Card. Securing the content requires only three instructions to perform the entire QCy™ security: key selection, cipher (encrypt or decrypt) and key update, all in a single clock cycle.

In the demonstration architecture, an i7 Windows 10 laptop runs a YouTube Hi Def channel on two 24" 1080p 60Hz monitors, streaming ~3Gbits/sec. One monitor directly displays the content; the other runs first to the Bitec HDMI card connected to the Arria FPGA. The FPGA executes QCy™ Verilog/VHDL 360 SLOC encrypting the content, then decrypting it back through the HDMI card and out to the monitor, operating on 256 bits simultaneously. The entire encode IN (6.67 ns) and decode OUT (6.67 ns) display is only 13.34 nanoseconds.

The QCy™ Encryption Engine updates the key *every 256-bits* in the one clock cycle, operating on the video stream within the parameters of the RGB protocol – essentially displaying exactly as the direct line output. The AES-256 x86ni chip implementation doesn't fit on the FPGA; if it did, the Enc+Dec speeds of even a 3.1GHz implementation wouldn't work. Resorting to S/W (.16Gbits/s enc at 3.1GHz) would completely fail to display any output. Qwyit® has achieved what was up to now, impossible – revolutionary speed and efficiency.

Benchmarks - Arria V GX FPGA

- Intel Arria V GX FPGA 150 MHz data clock
- Encrypt or decrypt with updated key each in 1 clock cycle
- Latency 6.67 nanoseconds encode or decode; 13.34 ns total
- Capable of 64 Gbits/sec (8 GBytes/sec), easily displaying the 3Gbits/sec Video content stream
- Less than 400 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 World-Changing Performance in perspective

2.5 Quintillion Bytes are added to the Internet every day (2.5×10^{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 (2.5×10^{18} bytes/ 37.699680×10^{12} bytes/sec)	Timing: 159,154,571 seconds (2.5×10^{18} bytes/ 15.708×10^{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