Qwyit™ Security

As we've said throughout Qwyit's history, there is a fundamental problem with security technologies: they aren't used in every communication, in every digital application, they aren't baked into the multiple device architectures across all the various digital networks. If they were, almost all of the problems – from network intrusions to financial fraud – would be, if not solved, severely limited.

Why isn't everything secure?

There are two major problems:

- There's no universal, simple, fits-everywhere method
  - This is because the current methods aren't able to be universal – Qwyit has pointed out the defects for years now: too big, too complex, too slow, too…insecure
- Networks have become multi-dimensional, making end-to-end authentication and encryption impossible using current methods

We need new security tools that can solve both these problems:

Truly universal, constant mutual authentication and provably secure encryption that fits everywhere across all networks, is simple, and works the same way – everywhere!

Since our Qwyit™ protocol was designed for flexible implementation, we're introducing **QwyitChip™** for hardware and **QwyitSDK™** for software as two universal, identical data encryption products.

They perform our QwyitCipher™ (QC™) algorithm for 100% provably secure, uniquely keyed data encryption. All any digital developer needs to do is perform two simple steps:

1. Install either QwyitChip™ or QwyitSDK™ into your device, product, application
2. Make one single programming instruction: **Get a Key, Call QC™** (it even rhymes!)

We understand the ever-evolving multidimensional network's dynamic nature, so we've developed and are introducing a new trust model and method for the input into that simple instruction: Get a Key.

Now there's the **QwyitKey™** *Authentication Service*, the world's first participant-managed, independent-trust authentication service for secure messaging: *Any participant can anonymously join the service, and singly self-generates trusted keys for all of their communication recipients.*

We have the entire package that solves both the universal and end-to-end security problems:

QwyitChip™ and QwyitSDK™ solve the universal implementation problem

QwyitKey™ solves the universal end-to-end network problem

Qwyit Fits Anywhere, Works Everywhere.

QwyitChip™ Specifications

- **FPGA architecture, demos available**
- **Verilog code available, Amazon AWS Cloud available**
- **QwyitCipher™ is 4 Qwyit™ primitive instructions: MOD16, Combine, Extract, XOR**
- **Each instruction is a *single machine cycle***
- **FPGA space consideration is the only design constraint: key size can vary up to available space**
- ***QwyitChip™ can process the 'gate width' in 4 cycles – if this is 1KB, then QC™ encryption/decryption is 4 cycles/KB***
- ***QwyitChip™ is, and will always be, 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 key size of 1MB, ***would encrypt/decrypt 375TeraBytes per second***
    - 1.5GHz is 1,500,000,000 cycles/second
    - QwyitChip™ takes 4/cycles per *key size*
    - A 1MB key size would encrypt 375 million times per second (1,500,000,000/4)
    - 1,000,000 Bytes times 375,000,000 times per second is 375,000,000,000,000 bytes/sec
- *The 15TB Library of Congress would encrypt in Four One Hundredths of a Second (.04 sec)*
- **QwyitChip™ is 100% provably secure and *already Quantum Safe!***
- **QwyitSDK™ operates identically in Software – speed constrained only by programming/buffer sizes**
- **QwyitKey™ provides *one-step* programming for QwyitChip™/QwyitSDK™ instant operation: Get A Key, Call QC™!**