QCy™
Provably Secure

TECHNOLOGY PRESENTATION

Introduction - Security Engineering

Qwyit® is a Security Engineering company. We're not cryptographers, more like Information Theorists. Our protocol, Qwyit™, and QCy™ cipher , are real world solutions to the fundamental flaws and lack of universal, easy-to-use and properly applicable privacy and security in digital communications, storage and not-present transactions.

What follows is a presentation and discussion of QCy's security basis, taken directly from Shannon

Introducing QCy™

The Qwyit™ protocol provides authentication (QwyitKey™ key management) and data security (QCy™ encryption engine) for the digital world in a secret-key system

- The QCy™ cipher has been benchmarked as the World's Fastest and Most Efficient

Is QCy™ Provably Secure?

Non-Ideal Current Systems

"How can we ever be sure that a system which is not ideal and therefore *has* a unique solution for sufficiently large *N* will require a large amount of work to break with *every* method of analysis?"

- From Shannon's 1949 *Communication Theory of Secrecy Systems*, near the end of Part III *Practical Secrecy,* Section 21 *The Work Characteristic*
- The italics are his, and they emphasize that for cryptographic solutions that are "not ideal", he's asking, and pointing out, that one can't really *prove* that these non-ideal systems always work

What he's talking about – cryptosystems that aren't "ideal" – *are every single one of today's cryptographic algorithms!*

Perfect Secrecy

- Everyone knows his *Perfect Secrecy*, the proof, and definition (short version): Key as long as the message

““Perfect Secrecy” is defined by requiring of a system that after a cryptogram is intercepted by the enemy the *a posteriori* probabilities of this cryptogram representing various messages be identically the same as the *a priori* probabilities of the same messages before the interception. It is shown that perfect secrecy is possible but requires, if the number of messages is finite, the same number of possible keys. If the message is thought of as being constantly generated at a given “rate” R (to be defined later), key must be generated at the same or a greater rate.”

This is The One Time Pad.

What happened in cryptography to “Ideal Systems”?!

Ideal System Definition

- Shannon actually stated – and detailed – another definition of a Perfectly Secret system (our yellow accent, his italics):

"It is possible to construct secrecy systems with a finite key for certain "languages" in which the equivocation does not approach zero as $N \rightarrow \infty$. In this case, no matter how much material is intercepted, the enemy still does not obtain a unique solution to the cipher but is left with many alternatives, all of reasonable probability. **Such systems we call *ideal* systems**. It is possible in any language to approximate such behavior—i.e., to make the approach to zero of $H(N)$ recede out to arbitrarily large N."

Ideal System Structure

- Shannon goes on to define/explain the structure of an *Ideal System*:

"To approximate the ideal equivocation, one may first operate on the message with a transducer which removes all redundancies. After this almost any simple ciphering system—substitution, transposition, Vigen`ere, etc., is satisfactory. The more elaborate the transducer and the nearer the output is to the desired form, the more closely will the secrecy system approximate the ideal characteristic."

This is exactly our security engineering accomplishment…

QCy™ Ideal System Cipher

The PDAF_SEC's process of underdetermined linear equations. **It is a Perfect Secrecy Finite Key Ideal System:**

Qwyit™ ID:	**OpenID**	[This is the public Qwyit™ Community ID]
Qwyit™ Keys:	*EK*, *QK*	[These are the upper level Qwyit™ Authentication Keys]
Initialization Vector:	**OR**	[A randomly generated public Initialization Vector]

Session Start: QK MOD16 **OR** = VK^P then PDAF(EK, VK^P) = VK^C [Starting *ValueKey*]
EK MOD16 **OR** = OK^P then PDAF(QK, OK^P) = OK^C [Starting *OffsetKey*]

Selection: $VK^{Pc[1\ldots n]}{}_{Pv[1\ldots n]}$ MOD16 $OK_{Po[1\ldots n]} = W_{1\ldots n}{}^2$
Where pointer *Pv* and *Po* increment +1 through the key length for each cycle pointer *Pc* [This is a PDAF in Dual Key mode]
If repeating, substitute VK^N and OK^N for each new cycle

Cipher: $W_{1\ldots n}{}^2 \oplus PT_{1\ldots n}{}^2 = \mathbf{CT}_{1\ldots n}{}^2$ repeating w/next cycle selection if more *PT*

Update (more *PT*): Update ValueKey: PDAF(OK^C, VK^P) = VK^{Next}
Update OffsetKey: PDAF(VK^C, OK^P) = OK^{Next}
Where the PDAF performed is the Key Offset Add mode

Repeat: Cycle through Selection, Cipher, Updates, replacing *VK* and *OK* until *PT*, **CT** completed

Send: Per Message[**OpenID**, **OR**, **CT**] to the **OpenID** location of intended recipient

QCy™ Ideal System Solution

- The QCy™ PDAF, used in every step of the QCy™ cryptosystem that generates the endless *Perfect Secrecy* keys, is Shannon's "*transducer*" that *delivers* "*the ideal characteristic*"
- Our *transducer* operates on the key not the message; which led to our breakthroughs
- As part of that accomplishment, it isn't "*elaborate*" at all – it's incredibly simple and straightforward – which realizes QCy™'s most important goal: Real World speed and efficiency
- The QCy™ cipher is then the same "*simple ciphering system*" used in *Perfect Secrecy* – a simple plaintext XOR with the endless key

QCy™ Ideal System Solution

- What we've accomplished is a finite key *Ideal System* for any bit "*language*" where the PDAF generates *Perfect Secrecy* endless keys
  - PDAF creates an underdetermined equation set that produces a large keyspace of incorrect values, a small set of valid values and one correct value
  - Every PDAF Selection creates unique bit results, therefore Perfect Secrecy when applied to every plaintext bit
  - Every PDAF Key Update creates unique one-way results
  - PDAF Key Updates can be performed forever without randomness degradation
- QCy™ is underdetermined at every step (PDAF at the Start, in key Selection, and next key Update), producing the required property result: there are multiple possible answers throughout the entire use of the cryptosystem

Theorem 1. *The PDAF delivers multiple possible solutions throughout the entire QCy™ cryptosystem, realizing Shannon's stated, proved and exampled Perfect Secrecy in an Ideal System. Therefore QCy™ is Provably Secure.*

Cryptographic Innovation

- While Shannon stated, proved and exampled a *Perfect Secrecy Ideal System*, he concluded that other than working with "*natural languages*":

"The complexity of the system needed usually goes up rapidly when we attempt to do this, however. It is not always possible to attain actually the ideal characteristic with any system of finite complexity"

We solved Shannon's "*complexity*" issues for any bit stream '*language*' by engineering two distinct cryptographic innovations:

QCy™ Cryptographic Innovations

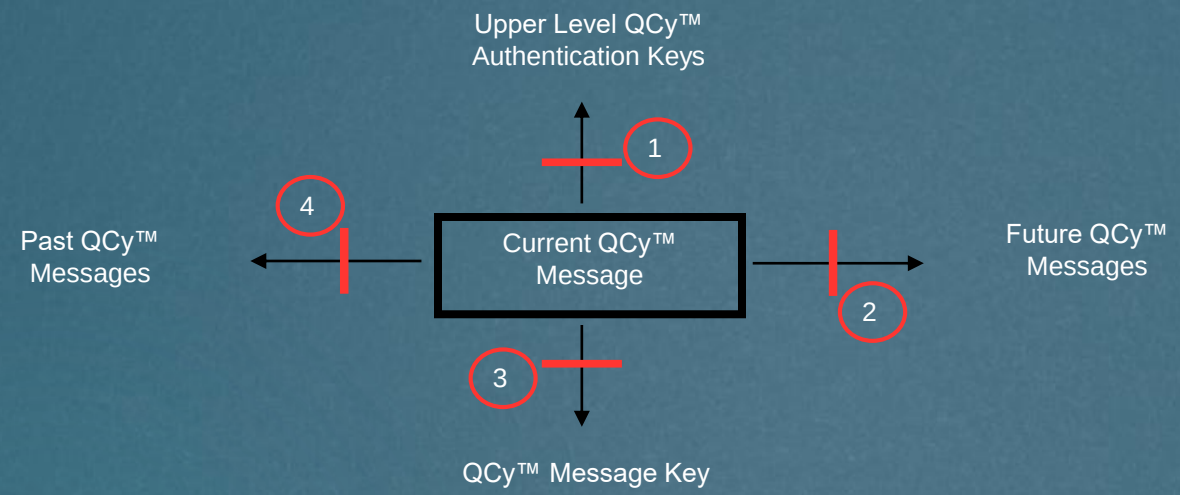
- *Random Rearrangement (RR)* – digit position manipulation, based upon random inputs and modular arithmetic properties, including the use of *remaining unused digit position values within a given input*, can be performed infinitely without any resulting randomness degradation; e.g., Keys created using *RR* from existing random keys are unique, random and possess all the characteristics of independently generated random keys
- No Communication Key Update – Reliant on *RR*, updating participant keys using a PDAF/OWC combination performed synchronously, without communication. The security is perfectly one-way: past keys cannot be *exclusively determined*
  - Any system keys – Master Authentication Keys, Session Start Keys, etc. – can forever be updated in a one-way, perfect, fast method *without any required communication between key partners*

QCy™ Provable Security

- These two techniques are used as the fundamental building blocks of our Qwyit Protocol and QCy™ cipher. Our cryptosystem presents the identical properties of *Perfect Secrecy*; and therefore a finite key *Ideal System*. There is never total discernment of any result
- PDAF will *always return an underdetermined one-way small set of valid possibilities*. Which continues during a cycle, into the next cycle, the next update, the next OR-seeded session – and *since it's possible that any session has been Master Key updated with no communication such that even an all-powerful adversary does not know this has occurred, QCy will never produce a known broken singular result*

Theorem 2. *The QCy™ cryptosystem, being Provably Secure, produces the first and only Perfect Cross Security*

QCy™ Perfect Security Cross



System Assumptions:

- Upper Level QCy™ Authentication Keys are securely pre-shared
  - By participant-managed, independent trust QwyitKey™ system, or other
- QCy™ Auth Keys create unique, new message keys for every message

Perfect Security IF:

Broken Current Message does NOT reveal Authentication Keys (One-way math gate)
Broken Current Message does NOT reveal Future Messages (One-way math gate)
Current Message is Provably Secure (Math proved, Shannon Secure)
Known Plaintext reveals key, but 1, 2 and 4 still hold – as does any remaining msg
Broken Current Message does NOT reveal Past Messages (One-way math gate)

QCy ™ is Perfect Cross Secure because the PDAF stops all attacks in all directions

QCy™ is Perfect Cross Secure:

1 – Continuously defeated by the underdetermined, irreversible PDAF Offset Key Add mode

2 – Even w/previous message knowledge, including *all* values except the Master Keys, new message breaks are defeated by the PDAF/OR reseed

3 – With only some PT knowledge and corresponding *W* section, the *VK/OK* keys all remain underdetermined for other sections, and maintain message key integrity

4 – Same as 2, PDAF/OR reseed

QCy™ Summary

- QCy™ is the best cryptographic engineering can accomplish: real world implementation of Shannon's *Perfect Secrecy Ideal System*
- After years of testing, including independent cryptographic reviews and NIST Lightweight Cryptography accepted submission (2015 – see Qwyit.com), *one thing is undeniably true*:

Compared to any existing system, QCy™ is faster, more efficient, more flexible and indicatively *more* secure

See the latest version of the QCy™ *Reference Guide* for complete cipher configuration, specifications, and security discussion. Appendix F contains empirical demonstrations of *Perfect Secrecy* results

Further Information

Contact Qwyit LLC

Info@qwyit.com

All truth passes through three stages. First, it is ridiculed. Second, it is violently opposed. Third, it is accepted as being self-evident. - Arthur Schopenhaue