The Post-Quantum Cryptography Disaster

Qwyit Engineered Only Perfect Security Encryption

GREAT FALLS, VIRGINIA, UNITED STATES, April 19, 2023 /EINPresswire.com/ -- The Post-Quantum Cryptography algorithm search is at a critical juncture – and it sadly looks like a continuance of the same old mistakes. Current methods result in ever-increasing yearly losses in cybercrime ($6Trillion+), and the dysfunctional algorithm search is going to result in an even worse security disaster.

> “This is the second example in the past six months of a scheme that made it to the 3rd round of the NIST review process before being completely broken using a classical algorithm. (other was Rainbow.)”
>
> *Jonathan Katz, IEEE, UMd*

Here’s some evidence:
NIST began a years-long effort to select new Post-Quantum Computing algorithms for standardization in 2016. In July 2022, NIST announced 4 finalists. SIKE, one of the 4 finalists, was immediately broken – using a PC.

“A team of scientists report they were able to defeat one of the post-quantum safe algorithms…and it only took one computational core on a PC working for about an hour.” – The Quantum Insider, Matt Swayne 8/5/22

Jao, SIKE co-inventor, on why the weakness surfaced after acceptance by NIST as a finalist:
“It's true that the attack uses mathematics which was [sic] published in the 1990s and 2000s. In a sense, the attack doesn't require new mathematics; it could have been noticed at any time.”

So what did NIST do after this fiasco?
“It is perhaps a bit concerning that this is the second example in the past six months of a scheme that made it to the 3rd round of the NIST review process before being completely broken using a classical algorithm. (The earlier example was Rainbow.) Three of the four PQC schemes rely on relatively new assumptions whose exact difficulty is not well understood…” – Jonathan Katz, IEEE, UMd

Even with embarrassing and damning results, NIST’s course of action remains unchanged.

Here are the Quantum facts:
- Stronger algorithms are needed because future computers will always be better
- No one knows anything about those future computing capabilities
- That leaves only one PQC algorithm design guaranteed to work and be forever safe under any

computing platform – it must not be computationally bound.

Looking for a 'difficult to compute' algorithm (like all of current cryptography) will end up just like SIKE: it looks good until it isn't. And it's not just a matter of finding the math to break it; because if an answer can be computed, it will be found in a future computing real time. So how is looking for the same type of broken things we already have going to solve the problem? Bottom line: it isn't!

But luckily, cryptography already has the answer to this unknown future…and it lies in the past: There is only one absolute definition of any cryptography that is not computationally bound: Perfect Secrecy

Your immediate reaction is that Perfect Secrecy isn't practical – but here's Claude Shannon:
"It is possible to construct secrecy systems with a finite key for certain "languages" in which the equivocation does not approach zero as N□∞. 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."

Those practical, finite key Ideal Systems are defined as:
"We will define an "ideal" system as one in which HE(K) and HE(M) do not approach zero as N□∞. A "strongly ideal" system is one in which HE(K) remains constant at H(K)."

Turns out there is practical Perfect Secrecy in Shannon Strongly Ideal Systems – all that was required was for someone to create one – and Qwyit has done it. It's forever not computationally bound, meets the real-world definition of Perfect Secrecy (multiple plaintexts encrypting to identical ciphertext), and it delivers 100% safe Cryptography under any Binary, Quantum, AI, or future-unknown computing system.

So why is cybersecurity making all the same mistakes that already cause so many problems – only to be certain that the future is filled with more?

There's no need to find new PQC algorithms: Cryptography already has a universal, forever algorithm: Perfect Secrecy as defined by Shannon and efficiently engineered by Qwyit™ (www.qwyit.com).

Michael P. Fortkort
Qwyit LLC
+1 703-625-3233
email us here