The Post-Quantum Cryptography “Trial of the Century”

You’ve heard about the upcoming standardization of algorithms for Post-Quantum Cryptography (PQC). Right now is a critical juncture for the entirety of cybersecurity – and it doesn’t look like the industry is ready. What is being touted as preparation for the future, seems to be nothing more than repetition of the past. Using the current security techniques, we’ve got $6Trillion yearly in cybercrime. To not repeat the last 70+ years of mistakes, what we need is consensus of a better way forward.

In today’s fractured landscape, consensus is only delivered one way: go to Court and get a ruling. So let’s take NIST to court, and charge them with ‘Crimes Against Security’.

Here’s the evidence booked by the prosecution:

Item #1

NIST began a years-long effort to select new Post-Quantum Computing (PQC) algorithms for standardization in 2016. In July 2022, they announced the 4 finalists (after 6 years of analysis and review). SIKE, one of the 4 finalists, was broken right after the announcement – using a PC (no quantum required)

> “A team of scientists report they were able to defeat one of the post-quantum safe algorithms that is still under consideration as part of the National Institute of Standards and Technology’s (NIST) PQC program — and it only took one computational core on a PC working for about an hour.” – *The Quantum Insider*, Matt Swayne 8/5/22

Item #2

Jao, the 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 published in the 1990s and 2000s. In a sense, the attack doesn't require new mathematics; it could have been noticed at any time. In general there is a lot of deep mathematics which has been published in the mathematical literature but which is not well understood by cryptographers. I lump myself into the category of those many researchers who work in cryptography but do not understand as much mathematics as we really should. So sometimes all it takes is someone who recognizes the applicability of existing theoretical math to these new cryptosystems.”

Item #3

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, so what the latest attack indicates is that we perhaps still need to be cautious/conservative with the standardization process going forward.” – Jonathan Katz, IEEE, UMd

Even with this embarrassing and damning result, NIST’s course of action is unchanged.

Here are the Quantum facts of the case:

- There is consensus we need new, stronger algorithms because Quantum Computers are better – just not on how to find them

- We have absolutely *no way* of knowing what 20 years-worth of Quantum looks like: making assumptions about the platforms' future capabilities, the network architectures and apps, the measure of strength of any proposed algorithm, the users, etc. It's all a fool's errand

- The only *fact* we can be sure of is that there is only one absolute way to design a PQC algorithm guaranteed to work and be forever safe under *any* computing platform – it must not be *computationally bound*

Prosecution's Closing Argument: You can put up any defense you want – the evidence is too strong: looking for a 'difficult to compute' algorithm will put you into the SIKE jail: it looks good all the way up 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*. Quantum will most likely get there, Artificial Intelligence definitely will.

So what does cryptography do?

Luckily, it already did it:

- There is only one absolute definition of any cryptography that is not computationally bound: *Perfect Secrecy*

Oh I know what you're thinking: *'That's not practical! We've been there, done that. PS is a pipe dream.'* But let's call Claude Shannon to the stand:

> "It is possible to construct secrecy systems with a finite key for certain "languages" in which the equivocation does not approach zero as $N \to \infty$. 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."

Boom. Those italicized practical, finite key *Ideal Systems* are defined as:

> "We will define an "ideal" system as one in which $H_E(K)$ and $H_E(M)$ do not approach zero as $N \to \infty$. A "strongly ideal" system is one in which $H_E(K)$ remains constant at $H(K)$."

There's a simple reason cryptography doesn't like Perfect Secrecy: *none of the Cryptographers are Engineers*. Jao, above, is right: they're not really mathematicians either. Combining the two solves the 'How To' part of cybersecurity: *What are new ways to design, build and test Finite Key Strongly Ideal Systems that work?* Then we'd have *Perfect Secrecy – forever, in finite key (practical) ciphers.* No other science quits after finding something 'impractical' – there's just some engineering work to be done to make it all real. We wouldn't have almost *every bit of today's technology without engineering.*

Turns out that someone *has* engineered the first practical, Shannon Strongly Ideal System that is forever not computationally bound, that meets the real-world definition of Perfect Secrecy (multiple plaintexts encrypting to identical ciphertext), that delivers 100% safe Cryptography under any Binary, Quantum, Artificial Intelligence, or future-unknown computing system.

The Verdict? NIST is guilty – there isn't any need to find new PQC algorithms: Cryptography already has a universal, forever algorithm: Perfect Secrecy. And Qwyit™ made it practical (www.qwyit.com).