# No need to wait for quantum computers...Post Quantum Cryptography is already here.... mathematically proven...

Published on February 1, 2020

A qtext will resist any quantum cryptanalysis because it does not contain the key that decrypts it to the generating plaintext.
This is the blueprint for tomorrow's cyber space (5G greatly helps).

## Post-Quantum Cryptography: Pivoting to Ciphertext Size!

BitMint - Freedom Bearing Money

The Definitive Answer to the security threat posed by quantum computing is ciphertext size

Entanglement mystery is only being scratched. Its practical computational potential is not yet bound, and hence the resistance of the new so called "post quantum" complexity amassing ciphers is an open question. It appears that security is dead. Soon everything that goes online will be an open book. The best that the industry can put forth today is "it's not around the corner". Really??!

Quantum computing is such a different direction away from Turing machines that to confront this threat one is challenged to come up with a solution equally novel compared to the direction cryptography has been evolving in the Turing machine decades.

The key word that reflects the edge of quantum computing over the common Turing computing is 'uncertainty', 'equivocation'. The key word that reflects the edge of post-quantum cryptography is the same: uncertainty, equivocation.

Consider something called composite ciphertext. It is a piece of data that can be decrypted with one key to yield one plaintext, but when decrypted with another key it yields a different plaintext. Same ciphertext evaluates to two distinct plaintexts — depending on which key is used. We can call it a "qtext" akin to "qbit".

A qtext will resist any quantum cryptanalysis because it does not contain the key that decrypts it to the generating plaintext. If the key is not in the qtext then no computer, quantum or otherwise, can find it there. The most powerful cryptanalyst will end up with terminal equivocation unable to

decide which plaintext is concealed by it. By contrast, AES ciphertext hides the key used to generate it.

A composite ciphertext, qtext, may comprise many more plaintexts than two — unlimited number of plaintexts in fact. What is the price we pay for hiding our message in a forest of equally likely message candidates? We end up with a proportionally large ciphertext. The more equivocation we desire, the larger the ciphertext we need to generate.

This very point introduces the other pivotal difference between post quantum cryptography and inertia-bound cryptography. Most of us today default thoughtlessly to AES — the symmetric cipher of record. Now think about it: AES was published in 2001. For almost two decades this cipher stood there as a stationary target for world class cryptanalysis shops. Do you really doubt that in such a long time, with so much at stake, that AES is not secretly broken? Now 'broken' does not necessarily mean that some brilliant math tears it apart (although this possibility should not be discarded). Broken may mean that some national security cyber bureau has identified a small subset of AES keys for which a de-facto feasible cryptanalysis strategy was developed. Even if among randomly picked keys only 10% qualify, or 5%, even 1% — this is a breach. I for one bet that is the case.

The AES user, though, is helpless. They have no control over the security that protects their data. Now let's turn the page to the new world of true post-quantum cryptography. The user is in the driver's seat. The user who knows best how sensitive a piece of data is, she is the one who determines how much security to use for it. For not very sensitive data, the composite cipher will be relatively small. For top security data, the qtext will be so large that Shannon's mathematical secrecy will apply. And then all that the user will have to worry about is to safeguard the key they used. The ciphertext, the qtext, is perfectly secure.

This is the blueprint for tomorrow's cyber space (5G greatly helps). What is going to be interesting is to watch the old guard protecting its revenue stream by dismissing this completely off-track post-quantum strategy, for as long they can.

It took a while for our society to replace our privilege culture with "equal protection under the law", now migrating to cyber space we rise to "equal protection under the qtext".