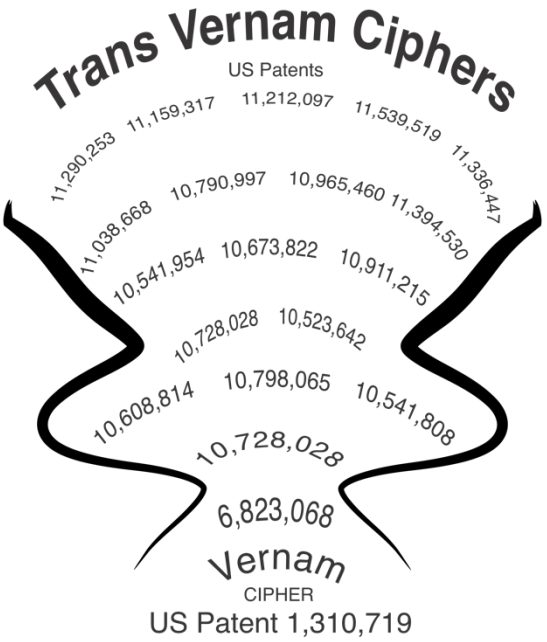
Cyber Security: Meeting the Quantum Threat

It is time to switch strategy. One by one NIST "post quantum ciphers" are breached. New ones in the same direction are put forth, likely to be breached much the same. It is time to go back to the fundamentals and apply a new thinking and new solutions.

For decades now cryptographic research was based on mixing bits of a small key with the bits of the protected message, making this mixing so complex that the plaintext cannot be pried out from the ciphertext. Alas, time and again, each new complex mixing has been exposed to have hidden vulnerabilities and were replaced. Today smart mathematicians and quantum computers can undo complex mixing much more efficiently than ever before. If we limit ourselves to this mixing-complexity strategy, we risk tipping the scale towards the attackers.

So strong is the *mixing-complexity* momentum that except for some foreigners, the budding alternative is by and large ignored.

What is the alternative?



Some 80 years ago Claude Shannon proved that a cipher using a key as large as the message will project absolute security. At the time one cipher complied: Vernam's one-time-pad. It was inconvenient to use, and when the message gets larger than the key, security collapses. *Well, let's replace the Vernam algorithm with a smarter one, which projects high security even when the message is larger than the key.* Several such smarter ciphers were developed -- Claude Shannon proof shields them from quantum attack. It even shields them from attackers much smarter than we are. And it so happens that they have assorted advantages: they hide the size of the message, they hide the pattern of the communication, and the key can be safeguarded off the digital grid -- in a newly patented BitMint nanotechnology chip where the data is written with chemistry (beyond the reach of hackers US patent: 10,467,522).

The security of Vernam, and the new Trans-Vernam ciphers is based on the simple fact that they are pattern devoid. Cryptanalysis is based on pattern detection and exploitation. Trans-Vernam ciphers have no pattern to be detected, no vulnerability to exploit. (See: https://eprint.iacr.org/2021/1510).

Yes, Trans-Vernam ciphers use large keys -- small price to pay for solving the quantum threat once and for all.

BitMint, Ltd. Amnon@BitMintMail.com 0544-200-400