BUZZ CHRONICLES > QUANTUM
Saved by @floyd_ndlovu
See On Twitter

Twitter Thread by Alan Szepieniec

Alan Szepieniec
@aszepieniec

https://t.co/Lhn4i1EGfq Time for a thread. 1/13

I read this article so you don't have to. 2/13

Can quantum computers attack crypto in ways that current supercomputer clusters can't? Yes. 3/13

But quantum computers don't exist yet (as far as we know), and they can only meaningfully attack some crypto algorithms -- typically public key algorithms. Except for rare edge cases, symmetric crypto remains mostly unaffected. 4/13

There is an active domain of research called 'post-quantum cryptography'. It is populated by mathematicians and computer scientists, who develop cryptography that can serve as a drop-in replacement for the affected algorithms. 5/13

The company in question is run by physicists. As a rule, physicists are clueless about cryptography. 6/13

The attack involves quantum annealing, which is a physical process akin to brute force search. It does not outperform Grover's algorithm in terms of computational complexity. 7/13

Grover's algorithm is the quantum analogue of brute force search. You need a quantum computer to implement Grover's algorithm, but you might not need a quantum computer to do quantum annealing. 8/13

Grover's algorithm is not enough to jeopardize the security of AES. You need an algorithmic or mathematical insight to do that. Such an insight would make the discoverer instantly famous in the crypto world. 9/13

AES is not a hash function and makes no claims about inversion being hard. It is not clear if this implication is the result of the reporter's confusion or if Terra Quantum's claim to fame actually is being able to invert AES. 10/13

Terra Quantum has developed an alternative to using AES for encryption based on quantum key distribution. If AES is secure, then there is no merit to quantum key distribution. In order to sell QKD, you need AES to be insecure. 11/13

How convenient that this breakthrough result about the supposed insecurity of AES is found just as Terra Quantum receives a patent for its technology! The convenience would be complete if they were in the middle of fundraising. 12/13

I have written about quantum key distribution before. TLDR: don't. https://t.co/4lxnot8pN4 13/13