Qwyit and Quantum Computing

I recently found some of my kid pictures from the 1960's. In one of them, I am dancing my fool head off, while holding what was then an electronic revolution: a transistor radio! In some not-too-distant year, there might be a picture of me solving some deep universal mystery, while holding a similar-sized little Quantum Computer. The writing below that photo on FaceGram (after those two merge!) will say 'The Day That Everything Changed!' Those little QC bad boys are said to be right around the corner…and they'll make our entire current computing look like a transistor radio sitting next to a Smart Phone.

In "*Quantum computers may be more of an imminent threat than AI*", Washington Post technology writer Vivek Wadhwa tells us one of the main reasons for this 'threat' is because these newfangled boxes are going to turn our digital security blankets (encryption methods) into the monsters not just *under* the bed, but right there pulled up to our chins! Those methods are *toast – done and DONE!* But not to worry, he tells us – those nutty cryptography professors are working on their Chitty-Chitty-Bang-Bang methods, and they're going to make them 'Quantum Safe'. And that they're making 'substantial progress.' WHEW!!

Oh…I didn't tell you, did I? There already *is* a Safe Now…Quantum Safe…Star Trek Safe encryption method. It's called the One Time Pad. It was invented over 100 years ago, and it's…unbreakable. That's with a capital 'U'! And you know what *unbreakable* means, right? It doesn't have anything to do with computing. Computing Power, Computing Speed, Computing Intelligence…it doesn't have a damn thing to do with *how to figure it out*. It means **it can't be figured out**. Not now, not tomorrow…not ever. Here's an example:

??? is our message.

??? is our key (our One Time Pad)

These are added together (in a simple digital way to combine them – it's not a 'cipher', just a combination). For this easy example, we'll just use modular arithmetic, and assume our message is a number. Combining our message and our key gives us:

942, our Ciphertext (the thing we can send anywhere, anytime, publicly, unbreakably)

Now – you can tell that if our key is one thing, say 371, then our message would be 671, right? That 7+7 drops the 'tens' in modular arithmetic, giving us 4. But…I'm sure you realize that our key could have been 883, and then that would make our message 169. Uh-oh…now you get it: unless you know the *actual key*, the one only you and I know: **This Is Unsolvable.** That means…*Unbreakable*. It doesn't matter how much computing power you've got. You can never, ever know the message without knowing the key. This is *already* Quantum Safe. (If you know any cryptographers, like the ones that are 'working on Quantum Safe and making *substantial progress'* – let them know they should be working on something else….before they're 'found out'…and someone makes fun of them, like…the guy writing this article!)

There is a serious – an incredibly serious – reason to have shown this with a touch of low-brow cruelty: It is painfully obvious that the above is 100% correct; and anyone working on a 'different solution' isn't focused on delivering *true Quantum, and any kind of computing ,Safe*. They are masking – and masquerading – around the fact that today’s methods that are supposedly ‘safe’…*aren’t using this 100% unbreakable encryption either*! And what does that tell us? Two things:

1. The stuff used today is unsafe now
2. The stuff they’re going to claim is safe in the future will be just as suspect

And it tells us that those beautiful, order-of-magnitude computing improvements – like Quantum Computers – don’t have anything to do with making your digital life any more or less secure. It isn’t secure now, and it won’t be then; unless they focus on the only real problem with delivering the above simple, *unbreakable encryption:* solving The Key Distribution Problem. This is delivering a unique, one-time key to every person, for every message, every time. When that can be done – when that is *truly solved*, not just claimed to be by today’s methods – then one simply uses the above OTP unbreakably in every message. By every person. Every time. *Unbreakable to any and every computing platform, hacker, cryptanalyst – forever.*

There is a company out there who has actually done that. And they deliver the above *unbreakable encryption*. Their solution *is already Quantum Safe.* Qwyit. They make QC boxes look like transistor radios. And let you keep the monster under the bed…where it belongs! Check them out.