QwyitTalk™ *Universal connectivity for Unbreakable communication*

QwyitTalk™ Technology Summary

100 years ago, the perfect – that is, Unbreakable – cipher was invented. Cryptography is complete. All it took for anyone to send an unbreakable message was to pre-share a one-time-only encryption key – it's called a One-Time Pad or OTP. This is great for small groups of participants – but not so good for large networks – like the world! Since everyone, for every time they want to send a secret message, needs a new unbreakable OTP key…you can see this Key Distribution Problem (KDP) is…well…quite a problem!

50 years later in the 1970s, large networks were becoming envisioned and created. Cryptography's Luminaries at the time came up w/a dual-key approach as their attempted solution to the KDP – this way everyone only needed one key (a public key) and everyone/anyone could talk to them. The problem with their idea: it didn't work as an encryption capability (way too slow), so it was only an authentication mechanism. Their dual-keys are used to send a third key, the actual encryption key, and then use that in a cipher. They had to combine the two systems – causing a cascade of compounding problems for each: extra equations, extra processing, extra messages – Extra! Extra!

Not only did their new approach not work for encryption, it was too slow to do more than at the 'beginning' of any messaging session. So, the 'tag-along' encryption mechanisms had to be different than the already perfect OTP; since they couldn't get you an encryption key more than once in a while, you had to use the same key over and over again. So Unbreakable was lost. And to add insult to injury, both of the new approaches – for authentication and encryption – aren't based on fact, like the unbreakable OTP; they're based on theory. And leaving a secret 'theoretically' safe isn't a good idea – just ask any gossip columnist!

In the last 50 years, exponential increases in computing power has allowed those dual-system methods to continue to 'sort-of' work…at the expense of Unbreakable. We had it…then lost it.

At Qwyit, we revisited the original problem: key distribution. When we did, we realized that taking the best of what's been done and adding in our new fundamental capability *finally solves the problem!* Everyone gets one authentication key that verifies their identity. They use it in the QwyitTalk™ process, and it mathematically – not theoretically – *creates* (never sends!) a one-time encryption key: we are back to Unbreakable encryption. As part of the QwyitTalk™ process, the authentication key mathematically – not theoretically – changes every time it is used as well – without being sent: now we have Unbreakable key distribution too. One key, one time use, simple process, one message: Unbreakable.

And we did this, our QwyitTalk™ process, using an *unsolvable mathematic theorem* – the same one used to prove the 100-year old OTP: an underdetermined system of equations. Our QwyitTalk™ equations have all the necessary protections that keep anyone from breaking the system in total, in each use, at every past, present and future message. QwyitTalk™, our combination technology from OTP encryption and one-key authentication, yields Unbreakable in any communication system for today's global networks: Internet, Financial, IoT, telecommunications – hardware, software: everywhere, for everyone, for every message: Unbreakable.