Scientific and Practical Cyber Security Journal (SPCSJ) 2(2):10-12
Scientific Cyber Security Association (SCSA), 2018 ISSN: 2587-4667

E91 NETWORK

Giorgi Iashvili, Aleksandre Lomadze-Gabiani
Scientific Cyber Security Association, European school (AHS)

ABSTRACT

E91, great as it is, becomes increasingly impractical as the network that it is implemented on grows. This is because as E91 only connects one end to another, so if one is trying to create a network using it they would have to store photons of every other device on each of the devices that are connected to the network. This requirement will cause the size of the devices on the network to bloat and make expansion and upkeep of the network extremely prohibitive. This paper suggests one modification of E91 that will make it more practical to implement.

To understand the modification that is being suggested in this paper we need to first understand several concepts; This part of the paper is meant to give a brief introduction to them.

Keywords: E91, modification, network, protocol;

1.1 Quantum Superposition

Particles can be described as probabilistic wave functions, which gives the likelihood of finding a particle in any specific position. Quantum superposition is the state in which the final state of the system is not known, therefore as Schrodinger's thought experiment posits the system exists in all the states at once. If the system is then observed, though the wave function "collapses" leaving us with a definite final state. To visualize this phenomenon in figure 1 there is illustration of a qubit that has its wave function collapse several times because of an observer. [2] [1] In the figure (?) represents the state of superposition (↓) and (↑) represent different spins that were observed.

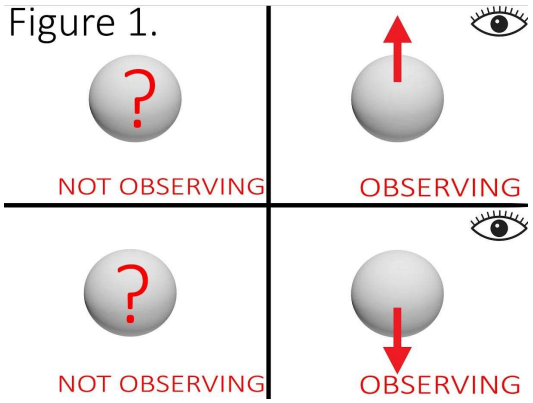

Fig. 1

1.2 Quantum Computer

Quantum computers are a new type of computers that are on the horizon which are significantly faster than their classical counterparts. , and as qubits in superposition are at all points between 0 and 1 quantum computers are able to operate at all values at once (which by extension increases our computational power.)

This leap in the computational power of computers will obsolete asymmetric key cryptosystems such as RSA. Then because of this, we are forced to use symmetric key cryptosystems (at least until someone comes up with asymmetric key cryptosystem that is quantum computer proof) which creates a new problem of distributing the keys to and from authorized parties without evesdroppers being able to steal them. (which is the large part of why we even need quantum key distribution in the first place.) [1]

1.3 Quantum Entanglement

To put it simply quantum entanglement is a phenomenon when pairs of quanta (also known as EPR pairs) behave as a single entity. For example, if we were to observe the spin of one we would at the same time destroy the wave function of another and be able to actually get information about it (spins of the pairs are inverse of each other).Though sadly entanglement cannot be used for teleportation purposes we are still able to send random information across. [1]

1.4 E91 Protocol

E91 works as such:

1. parties have separated pairs of photons between each other.
2. They measure photons with randomly with one of two orientations
3. Information is shared classically where parties determine whether pairs of photons are actually anti-correlated
4. Parties then share more information about the orientations that they have used to measure the photons
5. If the orientations match then that information can be used in the creation of the private key.

E91 protocol is great because utilizing entanglement allows us to send information that cannot be intercepted. This, if used in conjunction with unconditionally secure classical elements, will potentially make the network utilizing E91 unconditionally secure. [1]

2. Modification Proposed

Modification proposed is to introduce servers (essentially middle-man quantum computers) between the user base, which will make the burden of size shift on servers (which are already

big, so that additional size will cause much less trouble than bloating of other smaller devices on the network) ,and addition of new devices to the network will be made much easier.

So the problem that we are faced with is how do we transport the key from computer A to computer B with the relay server S. This means that computer A and B do not have each other entangled photons but they have entangled photons of server S which allows them to send random information to and fro the server (using E91 protocol).

The addition of the server poses one big problem in this case. After computer A observes its photons to send key 1 (K1) to the server that needs to be relayed to computer B The server is unable to control what spins the photons take when observed thus it cannot directly send the key with E91. To fix this my version the protocol proceeds as following - server observes entangled photons of computer B which sends K2 to computer B. Now the server encrypts K1 with K2 (with a cryptosystem of choice) and send it to computer Because computer B already has the key 2 it is able to decipher the ciphertext that is sent to it, and it is left with K1 in hand which successfully accomplished the goal of getting the key from 1 spot to another safely so that now the communication can commence safely!

3. Flaws in The Modification

3.1 Unable to Use OTP with the distributed key

There is a flaw in E91 network if OTP is used to encrypt both the key that needs to be distributed (c1) and the message that needs to be sent(c2). This flaw occurs because of the security flaw in OTP itself, which posits that if two messages that were encrypted using the same key were to be XORed over each other there would result in a data leakage. So in the iteration of E91 network that uses OTP if eve were to intercept both c1 and c2 she would be able to glean some information that was exchanged. This critical flaw, therefore, eliminates OTP as a viable cryptosystem to use for both c1 and c2 so there is a need for another cryptosystem to be added into the mix.

Conclusion

In conclusion addition of servers as the layers of keys between separate instances of E91 can help with certain problems that we would face if we were to only use direct connections through E91. There are a few setbacks such as the high cost of running such networks because of which most from being able to enjoy the perks of E91 network, and a need to use something other than OTP for encrypting some data. The future research could attempt to tackle these or try and test E91 network in practice to get data about how safe it would actually be when put into practice.

REFERENCES

1. "Quantum Key Distribution Protocols and Applications", Sheila Cobournem, Technical Report RHUL-MA-2011-05 8th March2011, https://www.ma.rhul.ac.uk/static/techrep/2011/RHUL-MA-2011-05.pdf
2. S.Singh, "The Code Book: the Secret History of Codes and Code - breaking" ,Fourth Estate, London, 1999