Developing a New Cryptic Communication Protocol by Quantum Tunnelling over Classic Computer Logic

Mesut KAVAK*

I have been working for a time about basic laws of directing the universe [1,2]. It seems that the most basic and impressive principle which causes any physical phenomenon is the Uncertainty Principle of Heisenberg [3], that existence have any property because of the uncertainty. During this process, while I was thinking about conservation of information I noticed, that information cannot be lost; but at a point, it becomes completely unrecognizable according to us as there is no alternative. Any information and the information searched for become the same after a point relatively to us. The sensitivity increases forever but its loss. Each sensitivity level also has higher level; so actually an absolute protection seems possible.

1 Introduction

In accordance with the uncertainty, any measurable physical value of matter increases or decreases between absolute-ness and absolute absence but its loss. No physical value can take certain value. They can only be expressed as some approaches.

As a result of this condition, for example, if you want to measure process number of a CPU, you can only get some different numbers at least for the numbers after the comma each time of measurement. When ever you want to measure more sensitive, new different numbers emerge after the fixed numbers after the comma. Except this, you can never get a certain number. Additionally for example, if you make a division, for the same operation the processor always performs the operation in different times. Yes it performs by some packets like 32 or 64 and always gives to you the same number that actually this also is not exact, it does not perform at the same time for each repeat. If you set the interval to find out this and if you ask to it over a program, sometimes you can get some results like 33 or 65 by unpredictable changing frequencies like 1 of 50 or 20 for 1 second.

Actually this physical principle and condition can be used as a perfect unpredictable cyberspace security element; because it creates a way to select incalculable and unpredictable codes like the below.

2 Cryptobits

Let us use rounding the decimal numbers into closest one. For example, if the number is like x,xxxx6 it is rounded into x,xxxx and this condition is called as 1. If the number is like x,xxxx4 then it is rounded into x,xxxx and the condition is called as 0. If the number is like x,xxxx5 try again. These 0 and 1 are not bits.

Also there is another way from many other ways that I used this second one. For example while a timer performs countdown, ask the time of counting until a number. If you repeat again and again the countdown, many times you get the same number but some times you get different number which is closest number to the actual number. The following VB codes are for this.
The key was already random. Namely, even the system architects do not know. Nobody knows what the two computers do. We made them confidant. Even attacks can disrupt communication and packets but also they cannot steal from us even if we cannot perform communication. Nobody is going to know what the key is going to be next time approximately. It is not the solution recording only the calibration. You must save any act always. If you are a thief or a wicked engineer, then if you lost only one 10 KB packet for the life time of the communication during recording from the beginning, you cannot do anything.

2.3 Remote Calibration

This may be dangerous if you think that any signal is recorded by a third unknown computer. For the worst possibility, think that a user is recording any act and making a simulation of the communication by some algorithms over any possibility even by using new hardware architecture to catch the copy of the computers and the software. Namely, making them sensible.

Actually the solution is making the data packets smaller and thus making the key change at a high frequency at last only during remote calibration.

3 Conclusion

As it can be seen, any information and the information searched for become the same after a point relatively to us. If you have only one bit for encoding like 1 or 0, it can get any letter. Namely, there are 26 possibilities for 1 or 0. If you have a bit group like 10, 11, 01 or 00 each one of them can get the same letters. You cannot decide which one of them is the main aim if you do not know the random key. The condition is the same for any length bit group.

The key is also determined randomly. The builder system architect people also cannot know what is going to be the key. An approximately guess is also not going to be possible. It can suddenly be the worst and unpredictable possibility. Namely, does not give benefit to kidnap and threaten the engineers for the key.

To work of this build in the best manner, actually a new hardware support is required. Especially for some specific communication instruments, you should build a new hardware architecture, and then the hardware will be doing the selection over unknown new hardware characters or frequencies. Even so, it can block most of the disturbing attacks by some simple programs. For example a simple windows emulator can block this. All windows is going to work over a simple encoding program first. Even computers are going to answer to a keylogger software or email by meaningless characters. Namely actually they can steal from us but cannot know what that information mean. It can be any information.

Acknowledgement

Thanks to Microsoft for VS Community.
I shall not demand a patent right. Anyone who wants to use the above stated things can use freely without asking.

References

1. Kavak M. 2018, Complementary Inferences on Theoretical Physics and Mathematics, OSF Preprints, Available online: https://osf.io/t8zqw