Response to Bollinger's "On the Impossibility of Keeping Out Eavesdroppers Using Only Classical Physics" and to Some Other Comments at Bruce Schneier's Blog Sites

(Updated February 17, 2006)

Laszlo B. Kish

http://www.ece.tamu.edu/~noise/research_files/research_secure.htm

Abstract. First we refute Bollinger's arguments because they are irrelevant for the *Kirchhoff-loop-Johnson(-like)-noise* classical physical cipher. Then we compare the basic properties of quantum communicators with the classical cipher and show why the properties of the classical one are superior to the properties of quantum. Then, we answer the retardation (waves, delays, transients) related comments, which have already been dealt with in the first paper on the classical cipher and resulted in the bandwidth limit published there. Finally, we point out that breaking the code of the idealized cipher violates the Second Law of Thermodynamics thus such a task is equivalent with building a perpetual motion machine.

1. Introduction: Denial of Bollinger's argumentation

Bollinger [1] claims that it is impossible to execute secure communication with classical information therefore Kish's proposed method, the Kirchhoff-loop-Johnson(-like)-noise cipher [2,3,4] must be flawed. Bollinger's arguments are based on the properties and measurement characteristics of quantum-entangled states.

It is very easy to refute Bollinger's argumentation. Clive Robinson [6] and Alex Young [7] have already done that by pointing out the irrelevance of arguments based on quantum entanglement in a macroscopic classical physical system.

To illustrate the type of flaw in Bollinger's manuscript, let us consider a well-known and very similar historical mistake. Before the first airplanes, skeptics believed that airplanes couldn't be built without a hydrogen-filled balloon because Archimedes's law is saying that the mean mass density of a floating object should be less or equal than the mass density of the air. However, these skeptics *mixed up apple with orange.* Airplanes are not based on Archimedes's law which is a *law of hydrostatics* (physics of standing fluids and gases). Airplanes are based on Bernoulli's law, a *law of hydrodynamics* (moving fluids and gases).

Bollinger is making the same type of mistake. Just like those early skeptics who used *hydrostatics* to deny the possibility of *hydrodynamical* airplanes, he is using arguments valid in a *quantum physical system* (apple) to deny the possibility of secure communication based on a *classical statistical physical system* (orange).

A more concrete denial of Bollinger's arguments is also easy. Let us see the backbone of the claim [1]: "The nice thing about this visualization is that it provides a fairly vivid way of understanding why it is so hard to be sneaky in quantum communications. The problem is this: When someone attempts to sneak in an observation on an entangled set of particles in the here-and-now, the quantum result look just as if a record of that transgression was captured, sent back in time to the original generation of the entangled particles, and then rebroadcast for everyone in the future to see. It is a bit like breaking into a store today, only to find out that last week the store had already shipped out a video of you doing it to every police station in the area."

In other words, when the eavesdropper measures the quantum state (and extracts the information bit) she will disturb the system so that the eavesdropping will be obvious (but only after 1000, or so, such attacks, see below). *Remark*: the author of the comments seems to forget that there are quantum communicators *without* entangled states, too, so I wonder if he believes that those quantum communicators are less secure than the entangled ones. (They are at least as secure as the entangled ones).

However, the KLJN system is completely different. In the *idealized* KLJN system, the eavesdropper, which *measures* the current and the voltage, cannot extract *any* information. Observe: the eavesdropper measures the macroscopic classical physical quantities, however, dislike at QC, here she *cannot* learn the value of the bit. The theory in [2] is based on linear algebra and the statistical physical properties of thermal (-like) noise (*Fluctuation-Dissipation Theorem*). The eavesdropper can set up only two linear equations and, in accordance with *linear algebra*, two independent equations allow the determination of *only two* unknown variables. These are the *two resistor values* at the two sides *without any information about their location*. These equations do not contain any more information therefore the *location* of the small and the large resistance is *unknown*. To learn the location, a third equation would be needed because the location is a new unknown variable, however *Kirchhoff's laws* and the *Fluctuation-Dissipation Theorem* do not provide more equations.

However, the eavesdropper can be invasive, too. That means she can *not only* do measurements but can also inject current into the line. From the measurement of the current distribution in the two directions, she can determine the location of the small and the large resistors. If she does so, the eavesdropping will *immediately* be discovered because the current balance at the two ends will be violated and the sender and receiver are continuously monitoring that. Therefore, the eavesdropper can extract *at most a single bit* of information before she is discovered. Using similar wording as Bollinger, in the case of the KLJN cipher, *while the thief breaks the lock on the door, the police arrives*.

In the rest of this text, we address a few more issues discussed on Bruce Schneier's blog sites [8,9].

2. Quick comparison of quantum communication (QC) and the KLJN cipher

Due to the common belief that QC is totally secure (*it is not, see below*), many people have doubted the claim that the Kirchhoff-loop-Johnson-like-noise (KLJN) cipher can be more secure than quantum crypto. Here we will briefly show why it is so. First of all, let us see what are the main sources of limitations of quantum security. A relevent citation from a good analysis [10] follows here:

"Quantum Privacy Attacks

Quantum cryptographic techniques provide no protection against the classic bucket brigade attack (also known as the "man-in-the-middle attack"). In this scheme, an eavesdropper, E ("Eve") is assumed to have the capacity to monitor the communications channel and insert and remove messages without inaccuracy or delay. When Alice attempts to establish a secret key with Bob, Eve intercepts and responds to messages in both directions, fooling both Alice and Bob into believing she is the other. Once the keys are established, Eve receives, copies, and resends messages so as to allow Alice and Bob to communicate. Assuming that processing time and accuracy are not difficulties, Eve will be able to retrieve the entire secret key -- and thus the entire plaintext of every message sent between Alice and Bob -- without any detectable signs of eavesdropping.

If we assume that Eve is restricted from interference of this kind, there are similar methods she can still attempt to use. Because of the difficulty of using single photons for transmissions, most systems use small bursts of coherent light instead. In theory, Eve might be able to split single photons out of the burst, reducing its intensity but not affecting its content. By observing these photons (if necessary holding them somehow until the correct base for observation is announced) she might gain information about the information transmitted from Alice to Bob.

A confounding factor in detecting attacks is the presence of noise on the quantum communication channel. Eavesdropping and noise are indistinguishable to the communicating parties, and so either can cause a secure quantum exchange to fail. This leads to two potential problems: a malicious eavesdropper could prevent communication from occurring, and attempts to operate in the expectation of noise might make eavesdropping attempts more feasible. The first problem is not limited to quantum communication, and is generally ignored. The second has a solution in a recent paper by Deutsch et al. [1996]."

Now let us compare the security of QC with that of the KLJN cipher.

i) We can extra about every 100ths raw bit without being discovered by the *error statistics radar* of QC. This kind of eavesdropping is not detected and it can virtually extract an infinite amount of information. This information leak is about a *million times* stronger than the level of leak software security experts accept [11]. What is very important: *this information leak exists even in the idealized QC*.

ii) The *idealized* KLJN cipher has zero information leak.

iii) The practical KLJN cipher will also have information leak due to wire capacitance and resistance effects [3,4]. It depends on how much investment goes into the cable and how much we want to approach the maximal speed of the idealized case. However it is easy to keep this leak at orders of magnitude smaller level than that of QC, if needed.

iv) If the eavesdropper wants to extract information quickly and efficiently, he has to use a more invasive attack by extracting, multiplying and sending back the photons. In this case, QC detects the eavesdropper by the *changed error statistics*. To make that statistics we need a large number of communicated bits, typically in the order of 1000 bits. The eavesdropper will extract a similar amount of information before getting discovered.

v) If the eavesdropper is using similarly efficient attack at the KLJN cipher then she can extract *at most one bit* of information before getting discovered.

vi) The KLJN cipher is naturally protected against the man-in-the-middle attack [3]. This kind of attack is a difficult matter in QC (see above).

In conclusion, the fluctuation-dissipation mechanism and the maximal entropy state of thermal equilibrium is a very good cipher. Moreover, it is *extremely robust* compared to single photons. A single photon is *no match* for 20 V voltage and 10 mA current in the cable. At this example, the electrical power in the cable corresponds to about 10^{18} photons/second.

3. Arguments about delays, waves, transient effects, directional couples, etc.

These arguments are relevant for the *non-ideal* situation and their control is based on engineering design. The situation is very similar to quantum communication, where single photon sources, noise-free information channel and noise-free detectors would be needed for *ideally secure operation* however such things do not exist. At the KLJN cipher, the delay, transient and wave effects can be easily avoided by using the no-wave condition of Eq. (9) in paper [2]. This is basically a bandwidth limitation and it needs proper filters or related elements. In paper [4], these questions are analyzed with more details and one aspect is already mentioned earlier in [5]. It is easy to design a KLJN system with superior security and speed compared to any quantum communicator, even for a long distance.

4. Break the idealized KLJN cipher *or* build a perpetual motion machine

There are claims on Bruce Schneier's blog sites [8,9] stating that the theory the security of *idealized KLJN cipher* in [2] is weak. Moreover, other blogs compared the claimed total security of the idealized KLJN cipher to the task of building a perpetual motion machine. We can answer these two claims together.

Saying that the theory in [2] is week indicates insufficient background in *Statistical Physics* and/or *Linear Algebra* and/or doubting the existence of the impossibility of *Perpetual Motion Machines* and/or the *Energy Conservation Law*. The thermal noise equations (1-4) in [2] are strict consequences of the following laws of physics.

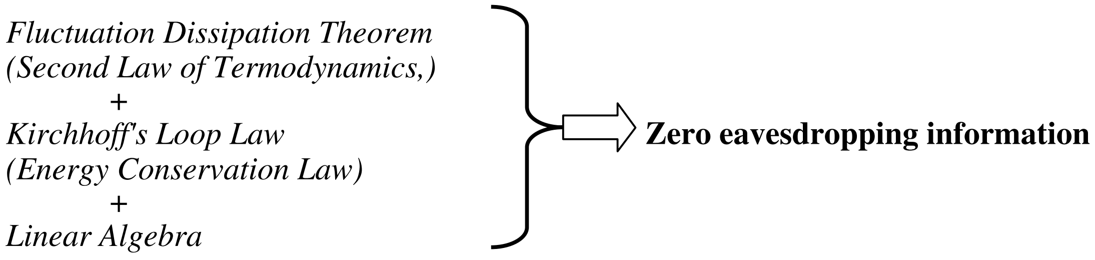
a) Fluctuation-Dissipation Theorem (FDT) of Statistical Physics. If the FDT is violated, then the *Second Law of Thermodynamics*, which is the *fundament of excluding the possibility of Perpetual Motion Machines*, is also violated.

and

b) Kirchhoff's Loop Law, which is a strict consequence of the Energy Conservation Law.

The security against a *passively measuring* (current *and* voltage) *eavesdropper* [2] is based on the claim that the thermal noise equations provide only *two independent linear equations* and according to Linear Algebra, *two independent equations* are enough to determine only *two unknown variables*. These two unknown variables are the *actual resistor values at the two ends*. There is no information about the location of these resistance values. That would need a third equation that does not exist.

The foundations and logic flow of the proof is shown in Figure 1.



Fluctuation Dissipation Theorem
(Second Law of Termodynamics,)
+
Kirchhoff's Loop Law
(Energy Conservation Law)
+
Linear Algebra

Zero eavesdropping information

Figure 1. Foundations and logic of the theoretical proof of the security of the KLJN cipher [2].

Therefore, the theory has extremely strong foundations. Let us investigate the implications of the claim that the idealized KLJN cipher cannot be totally secure because it is not a quantum system. Though we have pointed out that the *idealized quantum system* is not totally secure, it is interesting to see what would be the implication of such a situation in the idealized KLJN cipher. The logical consequences of *fictional* efficient passive eavesdropping are violations of basic laws of physics, see Figure 2.

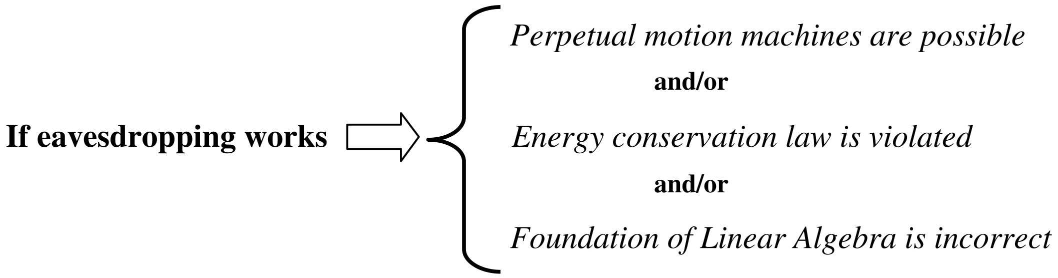

If eavesdropping works
Perpetual motion machines are possible
and/or
Energy conservation law is violated
and/or
Foundation of Linear Algebra is incorrect

Figure 2. The logical consequences of *fictional* efficient passive eavesdropping are violations of basic laws of physics.

Therefore, our conclusion is just the opposite of the conclusion in the blogs mentioned above. To break the idealized KLJN cipher or to build a perpetual motion machine are equivalently difficult tasks.

References

[1] T. Bollinger, "On the Impossibility of Keeping Out Eavesdroppers Using Only Classical Physics", preprint (January 23, 2006), http://terrybollinger.com/qencrypt/BollingerCritiqueOfKishPaper-2006-01-31.pdf

[2] L. B. Kish, "Totally secure classical communication utilizing Johnson (-like) noise and Kirchoff's law", *Physics Letters A*, in press http://dx.doi.org with code 10.1016/j.physleta.2005.11.062; also at http://arxiv.org/physics/0509136.

[3] L.B. Kish, "Protection against the man-in-the-middle attack for the Kirchhoff-loop-Johnson(-like)-noise cipher and expansion by voltage-based security", *Fluctuation and Noise Letters* **6** (2006) L57-L63.

[4] L.B. Kish, "Response to Scheuer-Yariv: "A Classical Key-Distribution System based on Johnson (like) noise - How Secure?", physics/0601022", preprint (Feb 2, 2006), http://arxiv.org/abs/physics/0602013.

[5] J. Bergou, in Adrian Cho, "Simple noise may stymie spies without quantum weirdness", *Science* **309** (2005) 2148.

[6] Clive Robinson, www.schneier.com/blog/archives/2006/02/more_on_kishs_c.html, (February 8, 2006 03:53 AM)

[7] Alex Young, www.schneier.com/blog/archives/2006/02/more_on_kishs_c.html (February 8, 2006 04:14 AM)

[8] http://www.schneier.com/blog/archives/2005/12/totally_secure.html

[9] http://www.schneier.com/blog/archives/2006/02/more_on_kishs_c.html

[10] http://www.cs.dartmouth.edu/~jford/crypto.html

[11] David Wagner (Berkeley), personal communication.