First draft. October 21, 2014.

ANALYSIS OF THE ATTENUATOR-ARTIFACT IN THE EXPERIMENTAL ATTACK OF GUNN-ALLISON-ABBOTT AGAINST THE KLJN SYSTEM

LASZLO B. KISH [(1)], ZOLTAN GINGL [(2)], ROBERT MINGESZ [(2)], GERGELY VADAI [(2)], JANUSZ SMULKO [(3)], CLAES-GÖRAN GRANQVIST [(4)]

[(1)] *Department of Electrical Engineering, Texas A&M University, College Station, TX 77843-3128, USA; laszlo.kish@ece.tamu.edu*

[(2)] *Department of Technical Informatics, University of Szeged, Hungary*

[(3)] *Department of Electrical Engineering, University of Gdansk, Poland*

[(4)] *Department of Engineering Sciences, The Ångström Laboratory, Uppsala University, P.O. Box 534, SE-75121 Uppsala, Sweden*

After briefly summarizing our general theoretical arguments, we show that, the experienced strong information leak at the Gunn-Allison-Abbott attack [*Scientific Reports* **4** (2014) 6461] against the Kirchhoff-law-Johnson-noise (KLJN) secure key exchange scheme, resulted from a serious design flaw of the system. The attenuator broke the single Kirchhoff-loop into two coupled loops. This is an illegal operation because the single loop is essential for the security, thus the observed leak is obvious. We demonstrate this by cracking the system with an elementary current comparison attack yielding close to 1 success probability for Eve even without averaging within a sub-correlation-time measurement window. A fully defended KLJN system would not be able to function, at all, due to its built-in current-comparison defense against active (invasive) attacks.

Keywords: directional coupler; unconditional security; experimental artifacts.

1. Introduction

Very recently, Gunn-Allison-Abbott (GAA) published a new type of attack [1] (see criticism about it [2-4]) against the Kirchhoff-law-Johnson-noise (KLJN) secure key distribution system [5-11] and both their experiments and simulations showed an extraordinarily large information leak at cable losses of 0.1 - 1dB. Particularly, they showed that at 1dB cable loss, within a fraction of the correlation time of the noise, Eve can extract the key bit with an error probability around 0.1, which means her probability

p successfully guessing the key bit is $p \approx 0.9$. If this claim were correct, it would imply that Eve could separate two very different noise intensities with this method. Even though the validity of the mathematical claim about the unconditional security [5] of KLJN would stay unchallenged, the applications of the KLJN scheme would be limited to intra-instrument or inter-chip security.

Starting efforts at the Department of Technical Informatics at University of Szeged to reproduce the GAA experiment lead to personal communications between GAA and us. During this process, important unpublished details of the GAA experiments were learned including a serious design flaw by breaking up the Kirchhoff-loop in the KLJN system with an attenuator to provide the desired loss. This led to the above-mentioned claims indicating that they are only experimental artifacts. It is important to note that a complete (fully defended) KLJN scheme would not have been able to function, at all, due to its current comparison alarm [13] thus the GAA experiments could not have been carried out.

Lachlan Gunn, after we identified the problem, agreed that this is an artifact, however it is still useful to demonstrate how serious is this. After giving a brief summary of theoretical arguments why the GAA attack cannot work, we analyze this experimental artifact and demonstrate its information leak.

2. Why the GAA attack cannot work?

A detailed analysis [2] (after general arguments [4] about the impossibility of directional couplers) was conducted about this question and about the physical impossibility of slow waves in a short cables [3] (note, the latter issue is not directly related to security). Here we very briefly summarize our understanding of this problem.

a) The GAA attacks is aiming to create a directional coupler to separate the noise components generated by Alice and propagating toward Bob, and generated by Bob and propagating toward Alice, respectively.

b) While their model assumes reflections and propagation by the EM phase velocity c_p in the cable, which is justified only for waves, this is not a serious problem. Linear Response Theory allows dividing the slow signal into short spikes for which the wave equation works; to study the response against these spikes separately (including assuming reflections and propagation by c_p), and then to summarize these responses.

c) The wave-based D'alambert equation-based picture used by GAA [1] is well known and it works for such short transient signals. However, the directional coupler will provide the required output only up to the moment of reflection when the mixing of signals in the two directions will occur.

d) For slow signals in the no-wave (quasi stationary) limit, the infinite number of reflections creates a mixture of the signals injected at the two ends. This effect leads to an *effective phase velocity* c_{pe} which is inversely proportional to the resistance terminating the end toward the propagation, see Section 3 and Table 1 with computer simulation results in [3]. Note, $c_{pe}=c_p$ when the terminating resistor is equal to the wave impedance (50 Ohm in [1]) of the cable [3].

e) However, the GAA method [1] requires the knowledge of c_{pe} in both directions and that requires the knowledge of the resistance values of Alice and Bob. As a consequence, Eve cannot separate Alice's and Bob's signals unless she knows the resistor values of Alice and Bob.

f) In [2] this feature of the GAA attack was mathematically evaluated. The analysis showed that, if Eve, while attempting to extract Bob's noise, assumed the correct c_{pe} value of propagation toward Bob, she could indeed succeed with this goal. However, if Eve assumed the wrong c_{pe} value for the propagation toward Bob, that is the c_{pe} value of propagation toward Alice, then she extracted a non-existent noise that had the *same mean-square value as Alice's noise*. In conclusion, Eve gets what she assumes. If she assumes a termination with the *high* resistance value, her evaluated noise will conform that assumption. But if she assumes a termination with the *low* resistance value, her evaluated noise will confirm that assumption instead. In conclusion, her 1-bit uncertainty persists with the GAA method.

g) In fact, GAA's theoretical analysis and computer simulation results are in accordance with the above facts because they show that Eve *cannot extract any information from a lossless cable* [1]. Even GAA's computer simulations with the smallest loss of 0.01 dB (see Fig. 3 in [1] were in accordance with the former experimental tests [10] of KLJN with similarly losses showing a minor information leak that could be fixed by simple privacy amplification [12].

h) The *only* situations when GAA was able to extract information were the setups with *losses*. This fact indicates that not the propagation effects were behind the measured information leak but other phenomena. Unfortunately, GAA did not show a cable-length-dependent information leak to test the real role of propagation.

Note, according to the information we received from Lachlan Gunn, even at the experimental situation indicated as "zero" loss in their paper [1], there was a significant loss corresponding to 0.1 dB cable loss in their system. They mean on "zero" loss situation that there was no additional attenuator used to increase the losses.

In conclusion, both our [3] and GAA's [1] theoretical analysis agrees that no information leak exists in the loss-free case even if propagation delays are present. In the next section,

we show that GAA's experimental results with attenuators to produce their require loss contained a heavy artifact, which would have prohibited the functioning of a fully built KLJN system due its current comparison defense against active attacks [13]. We show that, Eve can extract the information by elementary measurements with very low error rate, virtually immediately, even without using GAA's statistical tool.

3. The attenuator artifact in the GAA experiments and its analysis

The attenuator is a symmetrized voltage divider to provide not only the attenuation but also 50 Ohm input impedance when the other end is terminated by 50 Ohm. The 1 dB attenuator (with approximate values) and its inclusion into the KLJN loop are shown in Figure 1. It looks immediately obvious that the shunt resistor R_2 breaks the originally single Kirchhoff-loop into two loops with a common side. This is an illegal realization of the KLJN system because security guarantee has been shown only for a single loop involving Alice and Bob. The violation is very significant because the value (500 Ohm) of R_2 is 20 times smaller than that of Bob's resistor R_B (10 kOhm) and 2 times smaller than Alice's resistor R_A (1 kOhm). These data prove that the experiments were not conducted on the KLJn system but on something else.

We show below that the currents $I_A(t)$ and $I_B(t)$ of Alice and Bob, respectively, instead of being equal (required for security), are strongly unbalanced; Alice's mean-square current is about 5 times greater than that of Bob's.

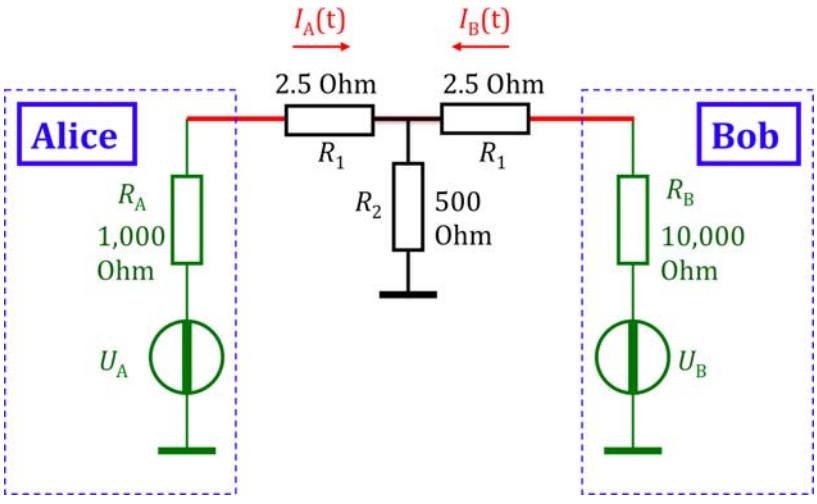

Figure 1. The 1 dB attenuator applied by Gunn-Allison-Abbott to crack the KLJN scheme. The mean-square current of Alice is about 5 times greater than that of Bob providing extraordinarily large information leak, and crack even by the simplest methods, see the analysis in the text. Note, the current-comparison defense [13] of the fully built KLJN would have prohibited running such tests (any tests with attenuators).

Straightforward circuit noise analysis provides the mean-square currents of Alice and Bob:

$$\left\langle I_{\mathrm{A}}^2(t)\right\rangle = S_{\mathrm{iA}}(f)B_{\mathrm{kljn}} = \frac{4kT_{\mathrm{eff}}R_{\mathrm{A}}}{\left[R_{\mathrm{A}}+R_{\mathrm{B}}R_2/\left(R_{\mathrm{B}}+R_2\right)\right]^2}B_{\mathrm{kljn}} + \left(\frac{R_{\mathrm{A}}^{-1}}{R_{\mathrm{A}}^{-1}+R_2^{-1}}\right)^2 \frac{4kT_{\mathrm{eff}}R_{\mathrm{B}}}{\left[R_{\mathrm{B}}+R_{\mathrm{A}}R_2/\left(R_{\mathrm{A}}+R_2\right)\right]^2}B_{\mathrm{kljn}} \qquad (1)$$

and

$$\left\langle I_{\mathrm{B}}^2(t)\right\rangle = S_{\mathrm{iB}}(f)B_{\mathrm{kljn}} = \frac{4kT_{\mathrm{eff}}R_{\mathrm{B}}}{\left[R_{\mathrm{B}}+R_{\mathrm{A}}R_2/\left(R_{\mathrm{A}}+R_2\right)\right]^2}B_{\mathrm{kljn}} + \left(\frac{R_{\mathrm{B}}^{-1}}{R_{\mathrm{B}}^{-1}+R_2^{-1}}\right)^2 \frac{4kT_{\mathrm{eff}}R_{\mathrm{A}}}{\left[R_{\mathrm{A}}+R_{\mathrm{B}}R_2/\left(R_{\mathrm{B}}+R_2\right)\right]^2}B_{\mathrm{kljn}} \quad , \qquad (2)$$

where $S_{\mathrm{iA}}(f)$ and $S_{\mathrm{iB}}(f)$ are the (white) noise spectra of the currents of Alice and Bob, and B_{kljn} and T_{eff} are the noise bandwidth and the effective noise temperature of the generators. Substituting the practical values used at the GAA experiments we obtain that:

$$\frac{\left\langle I_{\mathrm{A}}^2(t)\right\rangle}{\left\langle I_{\mathrm{B}}^2(t)\right\rangle} = 4.95 \quad , \qquad (3)$$

which means that Alice's mean-square current is about 5 times stronger than Bob's one. This extraordinary difference means that even the simplest comparison methods can extract the information thus GAA's complex statistical tool is unnecessary. To illustrate this fact, we show that a simple current comparison, without making statistics/averaging is sufficient to create an efficient attack.

Eve's job to be able extract the bit is to guess which mean-square current is the larger, Alice's one or Bob's one. In accordance with Equation 3, this task is equivalent with guessing from a few measurement samples if a current $I_1(t)$ with unit mean-square value

$$\left\langle I_1^2(t)\right\rangle = 1 \qquad (3)$$

or another current $I_2(t)$ with mean-square value

$$\left\langle I_2^2(t)\right\rangle = 4.95 \qquad (4)$$

is the greater. So, without the restriction of generality we use this example by assuming that the measurement noise current values are already normalized in accordance to Equations 3,4, which is straightforward because the $\left\langle I_{\mathrm{A}}^2(t)\right\rangle$ and $\left\langle I_{\mathrm{B}}^2(t)\right\rangle$ values are theoretically known by Eve because all the resistors and the effective temperature are public knowledge [4-6].

The simplest protocol is to do a single measurement on the currents and compare their square with the threshold 4.95. If one of the current square is greater than the threshold and the other is smaller than Eve concludes that the first one is $I_2(t)$.

We obtain the following probabilities about the behavior of the square of a *single measurement value* of the current:

$$\left.\begin{aligned} P\left(I_1^2(t)<4.95\right)&=1-F_1(4.95)\ =\ 0.974\\ P\left(I_1^2>4.95\right)&=F_1\left(4.95\right)\ =\ 0.026\\ P\left(I_2^2<4.95\right)&=F_2(4.95)=F_1\left(1\right)\ =0.68\\ P\left(I_2^2>4.95\right)&=1-F_2\left(4.95\right)=1-F_1\left(1\right)\ =0.32 \end{aligned}\right\} \qquad (5)$$

where F_1 and F_2 are the *chi-squared distribution* of $I_1^2(t)$ and $I_2^2(t)$, respectively, with 1 degree of freedom.

The probability of successful (but not necessarily error-free) guessing process, that is, $I_1^2(t)<4.95$ and $I_2^2(t)>4.95$, is:

$$P_{\mathrm{s}}=0.974*0.32=0.31\ . \qquad (6)$$

In this case, Eve's guess is $\left\langle I_1^2(t)\right\rangle<\left\langle I_2^2(t)\right\rangle$. The error probability of this decision is:

$$P_{\varepsilon}=P\left(I_1^2>4.95\right)\ P\left(I_2^2<4.95\right)=0.026*0.68=0.018\ , \qquad (7)$$

which is less than 2%, indicating over 98% fidelity of Eve's successful guessing process.

It is obvious that the probability of "*there is no answer*", that is, when both measured values are below the threshold or both values are over the threshold, is about 0.66. Thus, on the average, 3 measurement pots will be needed to get an answer and the answer will have over 98% fidelity. Note, because the threshold is at the mean-square value of I_2 and much greater than that of I_1 a successful measurement will happen with near-to-1 probability during the correlation time of the noise because the square of a Gaussian

noise typically goes through virtually all values between zero and its mean-square value during the correlation time.

This ad-hoc, non-optimized protocol and its small error probability is just an illustration of the astronomically large information leak due to the attenuator-artifact.

Acknowledgements

We are grateful to Lachlann Gunn for honestly sharing the unpublished details of their experimental realization of the KLJN scheme and, in this way, helping to identify the design artifact leading to the major information leak at the attack described in their paper.

References

1. L.J. Gunn, A. Allison, D. Abbott, "A directional wave measurement attack against the Kish key distribution system", *Scientific Reports* **4** (2014) 6461. DOI: 10.1038/srep06461.
2. H.P. Chen, L.B. Kish, C.G. Granqvist, G. Schmera. "On the "cracking" scheme in the paper "A directional coupler attack against the Kish key distribution system" by Gunn, Allison and Abbott", *Metrology and Measurement Systems* **21** (2014), 389–400. http://arxiv.org/abs/1405.2034 .
3. H-P. Chen, L.B. Kish, C.G. Granqvist, G. Schmera, "Do electromagnetic waves exist in a short cable at low frequencies? What does physics say?" *Fluctuations and Noise Letters*, 13 (2014) 1450016. http://arxiv.org/abs/1404.4664 , http://vixra.org/abs/1403.0964.
4. L.B. Kish, D. Abbott, C.G. Granqvist, "Critical analysis of the Bennett-Riedel attack on secure cryptographic key distributions via the Kirchhoff-law-Johnson-noise scheme", PLoS ONE 8 (2013) e81810. http://www.plosone.org/article/info%3Adoi%2F10.1371%2Fjournal.pone.0081810 .
5. L.B. Kish, "Totally Secure Classical Communication Utilizing Johnson (-like) Noise and Kirchoff's Law", *Phys. Lett. A* **352** (2006) 178–182.
6. L.B. Kish, C.G. Granqvist, "On the security of the Kirchhoff-law-Johnson-noise (KLJN) communicator", *Quantum Information Processing* **13** (2014) pp. 2213-2219. DOI: 10.1007/s11128-014-0729-7. http://arxiv.org/abs/1309.4112; http://vixra.org/abs/1309.0106.
7. J. Smulko "Performance analysis of the “intelligent” Kirchhoff’s-law–Johnson-noise secure key exchange", *Fluctuations and Noise Letters* **13** (2014) 1450024.
8. Z. Gingl, R. Mingesz, "Noise Properties in the Ideal Kirchhoff-Law-Johnson-Noise Secure Communication System. *PLoS ONE* **9** (2014) e96109 .
9. R. Mingesz, G. Vadai, Z. Gingl, "What kind of noise guarantees security for the Kirchhoff-Loop-Johnson-Noise key exchange? *Fluctuations and Noise Letters* **13** (2014) 1450021 http://arxiv.org/abs/1405.1196 .
10. R. Mingesz, Z. Gingl, and L.B. Kish, "Johnson (-like)-noise–Kirchhoff-loop based secure classical communicator characteristics, for ranges of two to two thousand kilometers, via model-line", *Phys. Lett. A* **372** (2008) 978–984.
11. Y. Saez, L.B. Kish, R. Mingesz, Z. Gingl, C.G. Granqvist, "Current and voltage based bit errors and their combined mitigation for the Kirchhoff-law-Johnson-noise secure key exchange", *Journal of Computational Electronics* **13** (2014) 271–277. http://vixra.org/abs/1308.0113 ; http://arxiv.org/abs/1309.2179
12. T. Horvath, L.B. Kish, J. Scheuer, "Effective Privacy Amplification for Secure Classical Communications", *EPL* **94** (2011 April) 28002-p1-p6 ; http://arxiv.org/abs/1101.4264 .
13. 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", *Fluctuations and Noise Letters* **6** (2006) L57-L63. http://arxiv.org/abs/physics/0512177 .