Version 2, April 11, 2014. http://vixra.org/abs/1404.0081

ON THE "CRACKING" EXPERIMENTS IN GUNN, ALLISON, ABBOTT, "A DIRECTIONAL COUPLER ATTACK AGAINST THE KISH KEY DISTRIBUTION SYSTEM"

Hsien-Pu Chen [1], Laszlo B. Kish [1], Claes-Göran Granqvist [2], G. Schmera [3]

[1] *Texas A&M University, Department of Electrical and Computer Engineering, College Station, TX 77843-3128, USA*

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

[3] *Space and Naval Warfare Systems Center, San Diego, CA 92152, USA*

Abstract

Recently Gunn, Allison and Abbott (GAA) [http://arxiv.org/pdf/1402.2709v2.pdf] proposed a new scheme to utilize electromagnetic waves for eavesdropping on the Kirchhoff-law–Johnson-noise (KLJN) secure key distribution. In a former paper [http://vixra.org/pdf/1403.0964v4.pdf], we proved that CAA's wave-based attack is unphysical. Here we address their experimental results regarding this attack. Our analysis shows that GAA virtually claim that they can identify, in a few correlation times that, from two Gaussian distributions with zero mean, which one is wider when their relative width difference is $<10^{-4}$. Normally, such decision would need millions of correlations times to observe. We identify the experimental artifact causing this situation: existing DC current and/or ground loop (yielding slow deterministic currents) in the system. It is important to note that, while the GAA's cracking scheme, the experiments and the analysis are invalid, there is an important benefit of their attempt: our analysis implies that, in practical KLJN systems, DC currents ground loops or any other mechanisms carrying a deterministic current/voltage component must be taken care of to avoid information leak about the key.

Keywords: KLJN key exchange; information theoretic security; unconditional security.

Recently Gunn, Allison and Abbott (GAA) [1] proposed a new scheme to utilize electromagnetic waves for eavesdropping on the Kirchhoff-law–Johnson-noise (KLJN) secure key distribution. In a former paper [2], we proved that CAA's wave-based attack is unphysical due to the quasi-static limit holding for KLJN where no physical waves exist. Moreover, the correct analysis based on impedances showed that, in their equations, they should have used direction dependent phase velocity when treating the fluctuations.

GAA used an advanced statistical method to compare the distributions of the extracted voltage components and to identify the resistor situations at the two ends of the wire. They found that, in the case of lossy cables they were able to identify the resistor situations within a very short time.

It was proven in [2] that, in the KLJN (quasi static) frequency limit, the exact distributed impedance model of the cable shown in Figure 1 leads to the simplified serial impedance models in Figure 2 because the capacitive currents converge to zero toward the low frequency end. Figure 2a is the accurate model of the real cable while Figure 2b is the model of the situation where the cable is lossless or the voltage drop on the resistive component is negligible compared to that of the inductive component (in the higher frequency range of the quasi static regime).

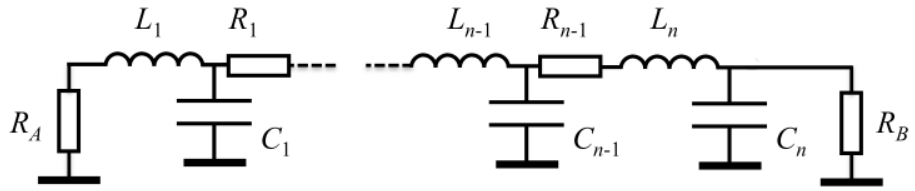

Figure 1. Outline of the pertinent part of the KLJN scheme with a distributed LCR model of a long and leakage-free cable [2]. When the cable losses can be neglected, one may omit the R_i resistors representing the distributed resistance of the cable. Alice's and Bob's resistors, denoted R_A and R_B, respectively, are randomly selected from the set $\{R_L, R_H\}$ with $(R_L \neq R_H)$ at the beginning of each bit-exchange period. These resistors, with associated serial generators (not shown), emulate thermal noise with high noise temperature and strongly limited bandwidth.

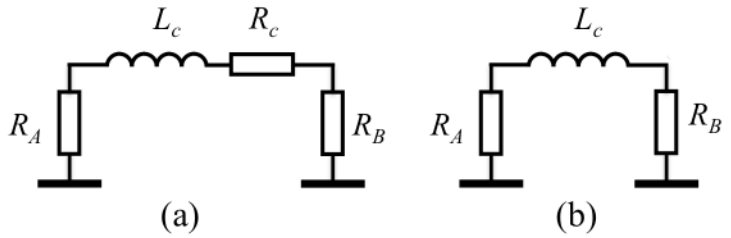

Figure 2. Lumped impedance-components-based model of a cable [2] at low frequencies for analyzing voltage drop along the cable and phase shift in the quasi static limit. Part (a) represents a cable with loss (cable inductance and resistance are designated L_c and R_c, respectively), and part (b) represents a lossless cable.

In the case of lossless short cable, Fourier transforming their D'alambert equation and substituting the proper phase velocities and impedances indicates that GAA do not have a directional coupler but a "separator", which is able to separate the voltages supplied by Alice and Bob if and only if the correct phase velocity is assumed. Because the phase velocity in the steady state is determined by the resistor value terminating the cable end toward the propagation direction [2], to get the correct voltage value, Eve must correctly guess that resistor at that end. In the case of an incorrect guess, the voltage will be the weighted superposition of the voltages of Alice and Bob so that the mean square voltage corresponds to that of the noise source of the assumed resistor. It is important to realize that the only role of the inductance of the loss-free cable is to detect the current in the wire.

Note, these types of "separator" can be more easily realized by simply measuring the current and using Ohm's law with guessed resistance values to obtain the voltages of Alice and Bob. The conclusion remains the same: the obtained mean-square voltages satisfy the supposed resistance value and Eve cannot extract any information by using them.

In the case of lossy cable, the voltage drop on the resistor makes GAA's D'alambert equation approach invalid even if the correct phase velocity is used. However, the wire resistance will cause a small imbalance of the calculated mean-square voltages, in the order of $\left(R_c / R_A\right)^2$ or $\left(R_c / R_B\right)^2$, respectively. While this maybe suitable for an attack, the same order of information leak is offered in the classical way [3] by simply comparing the mean-square voltages at Alice's and Bob's ends.

Let us estimate the larger one of $\left(R_c / R_A\right)^2$ and $\left(R_c / R_B\right)^2$ in GAA's experiment. The smaller resistor was 1 kOhm. The cable length was 2 meters. While the paper did not specify the

cable parameters, assuming 1 mm^2 copper wire, the corresponding cable resistance is $7.2x10^{-2}$ Ohm. Thus the imbalance of the mean-square voltages is less than 10^{-8} or that of the width of the related Gaussian distributions is less than 10^{-4}.

The claim to identify which one of the distributions is the narrower, by sampling a few correlation times, is a courageous step because normally millions of correlation times would be required for that.

Thus the question arises: what was GAA measuring, how did they obtain these surprising data?

The solution is that GAA had an experimental artifact. The artifact is a deterministic current component in the cable, which is either a DC current, or slow deterministic current component such as caused by a ground loop. The voltage drop originating from these parasitic currents will introduce a location-dependent bias into the distributions and quickly uncover the resistor situations at the two ends.

However, Eve does not need to use GAA's method [1] for that. She can simply measure and compare the DC voltage components of the strongly correlated voltage noises at the two ends of the wire and extract the key or it's inverse (because she does not know the polarity and location of the DC voltage). Figure 3 shows computer simulations of two strongly correlated noises with a small DC shift, as an example. In this particular case, a single-time measurement is able to identify the DC voltage shift and uncover the key (or its inverse).

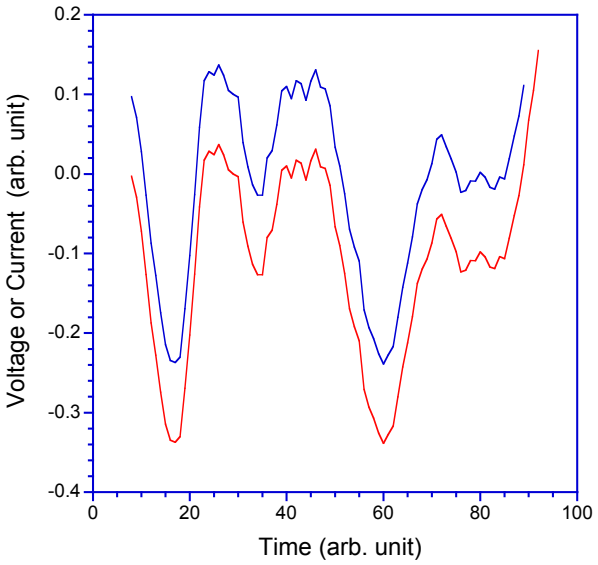

Figure 3. Computer generated example to illustrate how can a DC shift distinguish two strongly correlated noises by using a very shot sample. If the DC shift is greater than the stochastic difference between the time functions then *a single-time measurement is enough to distinguish the two noises* and the bit situations in KLJN.

Note, in the case of GAA's method, the time derivatives of the quantities (and a related spatial derivative) are used. The DC shift is added to the spatial derivative of the voltage on the wire, which compares to the time derivatives. This is another effect that further enhances the errors induced by a DC shift or ground loop.

It is important to note that, while GAA's approach [1] is invalid and the experimental results are caused by artifacts, the correct interpretation is very useful because it shows that such

parasitic currents are very dangerous potential non-idealities in a practical KLJN system. The removal o of their effects is straightforward, such as by filters, etc, ignoring them can lead t cracking the key. For the safes results, a well-defended KLJN system can execute spectral analysis on the noise in the cable to make it sure that no deterministic voltage and current components are present.

Acknowledgements

Discussions with Janusz Smulko are appreciated.

References

1. L.J. Gunn, A. Allison, D. Abbott, "A directional coupler attack against the Kish key distribution system", manuscript http://arxiv.org/abs/1402.2709 (2014) versions 1 and 2.
2. 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?", Fluctuation and Noise Letters, accepted for publication (April 7, 2014), http://vixra.org/abs/1403.0964
3. L.B. Kish, J. Scheuer, "Noise in the wire: the real impact of wire resistance for the Johnson (-like) noise based secure communicator", Physics Letters A 374 (2010) 2140-214.