WHAT KIND OF NOISE GUARANTEES SECURITY FOR THE KIRCHHOFF-LAW-JOHNSON-NOISE KEY EXCHANGE?

ROBERT MINGESZ, GERGELY VADAI and ZOLTAN GINGL
Department of Technical Informatics, University of Szeged
Árpád tér 2, 6720 Szeged, Hungary

Received (received date)
Revised (revised date)
Accepted (accepted date)

This article is a supplement to our recent one about the analysis of the noise properties in the Kirchhoff-Law-Johnson-Noise (KLJN) secure key exchange system [Gingl and Mingesz, PLOS ONE 9 (2014) e96109, doi:10.1371/journal.pone.0096109]. Here we use purely mathematical statistical derivations to prove that only normal distribution with special scaling can guarantee security. Our results are in agreement with earlier physical assumptions [Kish, Phys. Lett. A 352 (2006) 178-182, doi: 10.1016/j.physleta.2005.11.062]. Furthermore, we have carried out numerical simulations to show that the communication is clearly unsecure for improper selection of the noise properties. Protection against attacks using time and correlation analysis is not considered in this paper. Related simulations are available at www.noise.inf.u-szeged.hu/Research/kljn/.

Keywords: KLJN; secure key exchange; unconditionally secure communication; secure key distribution; noise

1. Introduction

At present the security of the communication is mostly provided by software-based cryptographic solutions. Since the security is ensured only by the assumption that the eavesdropper does not have enough processing capability to break the code, considerable efforts have been made to develop unconditionally secure communication protocols. One promising research area is the quantum encryption, where security is based on the laws of quantum mechanics. However, recently an alternative communication scheme has been proposed, the Kirchhoff-Law-Johnson-Noise (KLJN) protocol, which is based only on the laws of classical physics [2]. One of the main advantages of the KLJN protocol is that it can provide at least the same security as quantum systems at orders of magnitude lower cost. Although until now there are only a few real implementations of the system [3,4], many potential applications, such as key distribution over Smart Grid [5], uncloneable hardware keys [6] or securing computer hardware [7] have been proposed. While several attack methods have been discussed [8-13], the debate is still going on concerning the security of the system [14, 15]. Furthermore new, extended protocols have been proposed for enhance the security of non-ideal devices [16].

The simplified diagram of the communication system is shown on Fig. 1. During the key exchange both Alice and Bob randomly select an L or H bit value. Then, they select the corresponding resistor (R_{L} and R_{H}) and connect it to the wire. The noise sources, $V_{\mathrm{L}}(t)$ and $V_{\mathrm{H}}(t)$ represent the thermal noise of the resistors. During the communication, the voltage and current noise measured in the wire ($V_{\mathrm{E}}(t)$ and $I_{\mathrm{E}}(t)$) are determined by the selected resistors and can be measured not only by Alice and Bob, but also by the eavesdropper, Eve. The security of the system is based on the assumption that even if Eve can measure these signals, she cannot differentiate between the LH state and HL state.

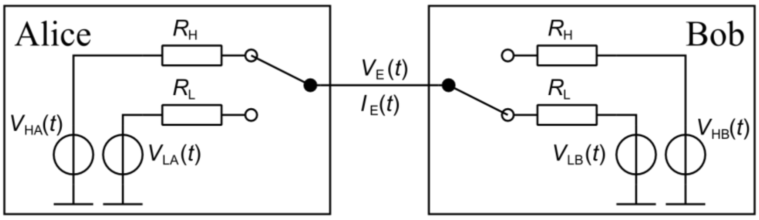

Fig. 1. Simplified diagram of the KLJN system (HL state is shown)

In real applications the thermal noise of resistors is too low therefore voltage noise generators are typically used to emulate high enough temperature [13]. It has already been stated that the security requires the use of Johnson-like noise, namely the noise must have normal distribution and the standard deviance must be scaled as the root of the resistance [2]. We have proven this statement using purely mathematical statistical tools [1], and in the present article we will show that these noise properties are not only needed, but also guarantee absolute security against statistical attacks. Note that in this paper we do not address protection against attacks based on the analysis of the time dependence of the signals.

2. Results

Eq. (1) and Eq. (2) show the voltage and current values that can be measured by the eavesdropper during the two secure states, LH and HL, respectively. The notation used in the equations is introduced in Fig. 1. The communication is secure if Eve cannot distinguish between these two states. The voltage and current measured by Eve in the LH state can be expressed as:

$$V_{\mathrm{E,LH}}(t)=\frac{V_{\mathrm{LA}}(t)\cdot R_{\mathrm{H}}+V_{\mathrm{HB}}(t)\cdot R_{\mathrm{L}}}{R_{\mathrm{L}}+R_{\mathrm{H}}}\ \text{and}\ I_{\mathrm{E,LH}}(t)=\frac{V_{\mathrm{HB}}(t)-V_{\mathrm{LA}}(t)}{R_{\mathrm{L}}+R_{\mathrm{H}}}. \tag{1}$$

The voltage and current signal measured by Eve in the HL state (corresponding to Fig. 1) are given by the following equations:

$$V_{\mathrm{E,HL}}(t)=\frac{V_{\mathrm{HA}}(t)\cdot R_{\mathrm{L}}+V_{\mathrm{LB}}(t)\cdot R_{\mathrm{H}}}{R_{\mathrm{L}}+R_{\mathrm{H}}}\ \text{and}\ I_{\mathrm{E,HL}}(t)=\frac{V_{\mathrm{LB}}(t)-V_{\mathrm{HA}}(t)}{R_{\mathrm{L}}+R_{\mathrm{H}}}. \tag{2}$$

For secure communication, the joint probability density function $p_{\mathrm{LH}}(I_{\mathrm{E}},V_{\mathrm{E}})$ and $p_{\mathrm{HL}}(I_{\mathrm{E}},V_{\mathrm{E}})$ must be the same. If I_{E} and V_{E} are independent, this is satisfied.

As it has been proven [17], linear combinations Y_A and Y_B of two independent random variables X_1 and X_2 in Eq. (3) will be statistically independent if and only if each random variable is normally distributed and Eq. (4) is satisfied:

$$Y_A = A_1 \cdot X_1 + A_2 \cdot X_2 \text{ and } Y_B = B_1 \cdot X_1 + B_2 \cdot X_2\,, \tag{3}$$

$$A_1 \cdot B_1 \cdot \sigma_1^2 + A_2 \cdot B_2 \cdot \sigma_2^2 = 0\,, \tag{4}$$

where σ_1 and σ_2 are the standard deviations of X_1 and X_2 respectively. In our case we obtain:

$$V_{\mathrm{E,HL}}(t) = \frac{R_\mathrm{L}}{R_\mathrm{L} + R_\mathrm{H}} V_\mathrm{HA}(t) + \frac{R_\mathrm{H}}{R_\mathrm{L} + R_\mathrm{H}} V_\mathrm{LB}(t)\,, \tag{5}$$

$$I_{\mathrm{E,HL}}(t) = -\frac{1}{R_\mathrm{L} + R_\mathrm{H}} V_\mathrm{HA}(t) + \frac{1}{R_\mathrm{L} + R_\mathrm{H}} V_\mathrm{LB}(t)\,, \tag{6}$$

$$\frac{R_\mathrm{L}}{R_L + R_H} \cdot \left(-\frac{1}{R_L + R_H} \right) \cdot \sigma_\mathrm{VH}^2 + \frac{R_\mathrm{H}}{R_L + R_H} \cdot \frac{1}{R_L + R_H} \cdot \sigma_\mathrm{VL}^2 = 0\,, \tag{7}$$

therefore

$$-R_\mathrm{L} \cdot \sigma_\mathrm{VH}^2 + R_\mathrm{H} \cdot \sigma_\mathrm{VL}^2 = 0\,, \tag{8}$$

where σ_VH and σ_VL are the standard deviations of V_HA and V_LB, respectively. Note, that we get a similar equation for the LH case. According to this, the distribution of V_HA and V_LB must be normal, and the scaling of the standard deviation must follow the rule:

$$\frac{\sigma_{VH}}{\sigma_{VL}} = \sqrt{\frac{R_H}{R_L}}\,, \tag{9}$$

in agreement with the results presented in [1]. We have carried out numerical simulations [18] to obtain the joint statistics of I_E and V_E. We have generated 2^{13} samples both for the current and voltage and made scatter plots for several cases. Figure 2 demonstrates what happens with the joint distribution of I_E and V_E if Eq. (9) is not satisfied: there is an asymmetry in the distribution that depends on the actual state, LH or HL.

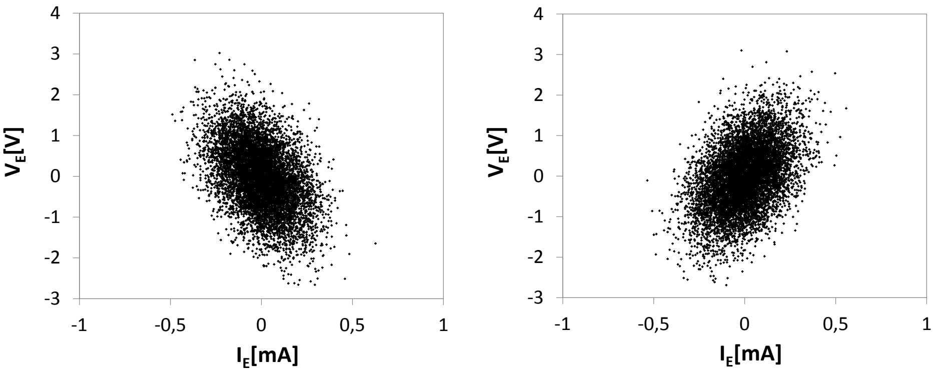

Fig. 2. Scatter plot for cases LH (left) and HL (right) using noise with normal distribution if the Eq. (9) is not satisfied. R_L=1 kΩ, R_H=10 kΩ, $\sigma_\mathrm{VH}/\sigma_\mathrm{VL}$=1,5.

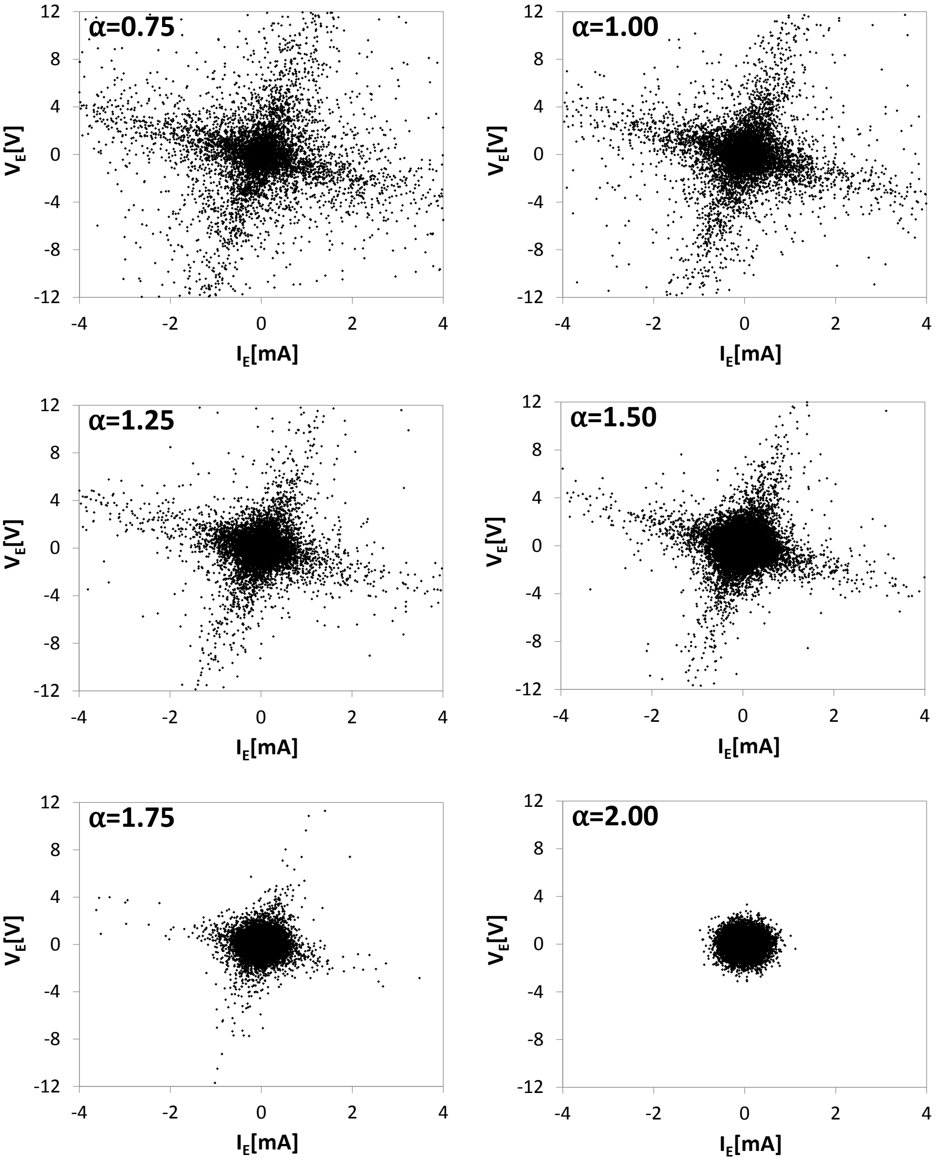

Fig. 3. Scatter plot for case HL using distributions with different values of α. Note that α = 1 and α = 2 correspond to Cauchy and normal distribution, respectively. R_L=1 kΩ, R_H=10 kΩ, $w_{VH}/w_{VL} = (R_H/R_L)^{½}$

In order to achieve a secure communication, the linear combination of noises must give the same type of probability distribution as the original one [1]. Such distributions are called stable distributions; here we consider symmetric α-stable distributions that include normal distribution as a special case. Assuming distributions symmetric around zero their characteristic function is defined by the following equation:

$$\varphi(t) = e^{-w^{\alpha}|t|^{\alpha}}, \tag{10}$$

where α is the stability parameter in the range from 0 to 2 and w is the scaling factor of the probability density function. Note that $\alpha = 2$ corresponds to normal distribution and $\alpha = 1$ corresponds to Cauchy distribution. However, according to [17], I_E and V_E are not independent except in the case of normal distribution ($\alpha = 2$) as can be seen on Fig. 3. Note that not all of such distributions have finite variance, therefore the scaling of the noise voltages was based on the scaling factor w which can be associated with the voltage noise magnitude and is defined in Eq. (10). Thus, the higher and lower noise voltages have scaling factors w_{VH} and w_{VL}, respectively.

Digital implementations of KLJN [3] require numerically generated random numbers. Pseudo-random number generators typically provide uniform distribution and generating normally distributed numbers is more complicated. However, in agreement with our results, Fig.4. clearly shows that the scatter plots for LH and HL cases are different for uniformly distributed signals, therefore they cannot be used for secure communication.

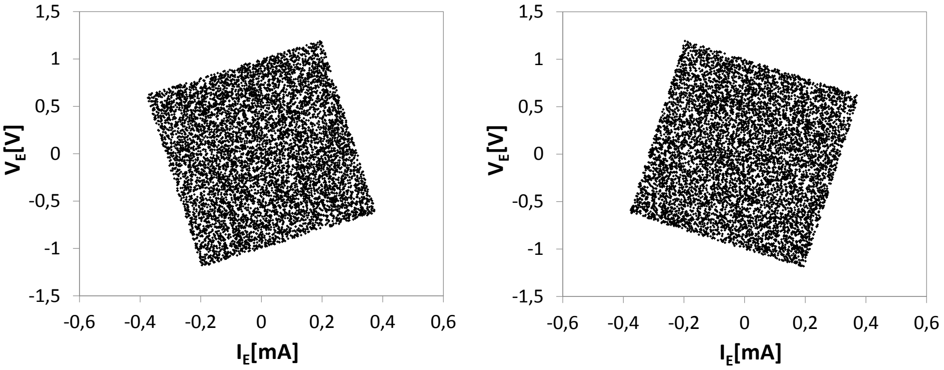

Fig. 4 Scatter plot for cases LH (left) and HL (right) using noise with uniform distribution. R_L=1 kΩ, R_H=10 kΩ, $\sigma_{VH}/\sigma_{VL} = (R_H/R_L)^{½}$

3. Conclusion

We have shown that communication using the KLJN protocol is secure if and only if noise voltages with normal distribution are used and the variance of the noise voltages follow the scaling defined by Eq. (9). This result is based on mathematical statistical derivation and it is in agreement with previous results [1,2]. Note that protection against attacks using time and correlation analysis is not considered and can be addressed in subsequent publications. Further analysis can clarify how the time domain properties of the noise influence the security of the system.

Acknowledgements

We thank the anonymous reviewer of our previous paper [1] for drawing our attention to the problem of statistical dependence of voltage and current fluctuations in the communication wire related to absolute security.

This research was supported by the European Union and the State of Hungary, co-financed by the European Social Fund in the framework of TÁMOP 4.2.4. A/2-11-1-2012-0001 'National Excellence Program'.

References

[1] Z. Gingl, R. Mingesz, *Noise Properties in the Ideal Kirchhoff-Law-Johnson-Noise Secure Communication System*, *PLoS ONE* **9** (2014) e96109. doi:10.1371/journal.pone.0096109

[2] L. B. Kish, *Totally secure classical communication utilizing Johnson(-like) noise and Kirchhoff's law*, *Phys. Lett. A* **352** (2006) 178–182. doi: 10.1016/j.physleta.2005.11.062

[3] R. Mingesz, Z. Gingl, 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. doi: 134 10.1016/j.physleta.2007.07.086

[4] R. Mingesz, L. B. Kish, Z. Gingl, C. G. Granqvist, H. Wen, et al., *Unconditional security by the laws of classical physics, Metrology & Measurement Systems* **XX** (2013) 3–16 doi: 10.2478/mms-2013-0001

[5] E. Gonzalez, L. B. Kish, R. S. Balog, P. Enjeti, *Information Theoretically Secure, Enhanced Johnson Noise Based Key Distribution over the Smart Grid with Switched Filters, PLOS ONE* **8** (2013) e70206. doi: 10.1371/journal.pone.0070206

[6] L. B. Kish, C. Kwan, *Physical Uncloneable Function Hardware Keys Utilizing Kirchhoff-Law-Johnson- Noise Secure Key Exchange and Noise-Based Logic, Fluctuation and Noise Letters* **12** (2013) 1350018 doi: 10.1142/S0219477513500181

[7] L. B. Kish, O. Saidi, *Unconditionally secure computers, algorithms and hardware. Fluct Noise Lett.* **8** (2008) L95–L98. doi: 10.1142/s0219477508004362

[8] F. Hao, *Kish's key exchange scheme is insecure. IEE Proc. Inform. Soc.* **153** (2006) 141–142. doi: 10.1049/ip ifs:20060068

[9] L. B. Kish, *Response to Feng Hao's paper "Kish's key exchange scheme is insecure". Fluct. Noise Lett.* **6** (2006) C37–C41. doi: 10.1142/s021947750600363x

[10] J. Scheuer, A. Yariv, *A classical key-distribution system based on Johnson (like) noise – How secure?, Phys. Lett. A* **359** (2006) 737–740. doi: 10.1016/j.physleta.2006.07.013

[11] L. B. Kish, *Response to Scheuer-Yariv: "A classical key-distribution system based on Johnson (like) noise – How secure?". Phys. Lett. A* **359** (2006) 741–744. doi: 10.1016/j.physleta.2006.07.037

[12] L. B. Kish, T. Horvath, *Notes on recent approaches concerning the Kirchhoff-law-Johnson-noise-based secure key exchange, Phys. Lett. A* **373** (2009) 901–904. doi: 10.1016/j.physleta.2009.05.077

[13] L. B. Kish, J. Scheuer, *Noise in the wire: The real impact of wire resistance for the Johnson(-like) noise based secure communicator, Phys. Lett. A* **374** (2010) 2140–2142. doi: 10.1016/j.physleta.2010.03.021

[14] C. H. Bennett, C. J. Riedel, *On the security of key distribution based on Johnson-Nyquist noise*, (2013) http://arxiv.org/abs/1303.7435

[15] 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. doi:10.1371/journal.pone.0081810

[16] L. B. Kish,. Enhanced secure key exchange systems based on the Johnson-noise scheme, Metrology & Measurement Systems **XX** (2013) 191-204. doi: 10.2478/mms-2013-0017

[17] E. Lukacs and E. P. King, *A Property of Normal Distribution*, *The Annals of Mathematical Statistics* **25** (1954) 389–394.

[18] Related simulations are available at www.noise.inf.u-szeged.hu/Research/kljn/