Robert Mingesz, Zoltan Gingl, Gergely Vadai, Security and performance analysis of the Kirchhoff-Law-Johnson-Noise secure key exchange protocol, Proceedings of the 23rd International Conference on Noise and Fluctuations (ICNF 2015), pp. 264-267., Xian, China, 2015.06.02-2015.06.05.

# Security and performance analysis of the Kirchhoff-Law-Johnson-Noise secure key exchange protocol

Robert Mingesz, Zoltan Gingl and Gergely Vadai
Department of Technical Informatics
University of Szeged
Szeged, Hungary
mingesz@inf.u-szeged.hu

***Abstract*—The Kirchhoff-Law-Johnson-(like)-Noise (KLJN) key exchange system is a promising low-cost alternative to the quantum key distribution and is based solely on the laws of classical physics. Although several papers have been published in the field, there is still an ongoing debate about the security of the method. In our paper we will give an overview the most important findings about the security of the KLJN system and show the effects of the non-idealities of the system on the information leak. We will also analyze different methods of proposed cracking the KLJN protocol, including the latest directional coupler attack.**

***Keywords—KLJN; secure key exchange; unconditional security; secure key distribution; noise***

## I. INTRODUCTION

The Kirchhoff-Law-Johnson-(like)-Noise (KLJN) or Kish key distribution system [1] is a competing very low cost and simple alternative to the quantum key distribution systems. The security of the system, in contrast to the quantum key distribution, is solely based on the laws of classical physics. This feature supports the development of secure communication systems with orders of magnitude lower cost than in the case of quantum based systems, while still maintaining the theoretical unconditional security.

### *A. Tthe KLJN secure key distribution system*

The original KLJN system uses only passive components: two different value resistors (lower and higher values, denoted by $R_L$ and $R_H$, respectively) at one side (Alice) and other two resistors with the same values at the other side (Bob). Switches are used to connect one of the resistors to the interconnecting wire, while the other terminals of the resistors are grounded to realize a closed loop circuit. The Johnson noise of the resistors provide random voltage and generate random current flowing in the loop. If different resistors at the different ends are selected, then in the middle the eavesdropper (Eve) can't determine at which end the lower resistor is used. This can be used by the communicating parties to realize two states (one bit, LH: $R_L$ at Alice, $R_H$ at Bob; and HL: $R_H$ at Alice, $R_L$ at Bob) that can be detected by them, but will remain hidden for the eavesdropper.

A more realistic realization can be seen on Fig. 1. Here the very small Johnson noise of the resistors is emulated by voltage noise generators providing the same kind of noise with much higher amplitude – equivalent to increasing the temperature to a very high value [1]. The resistance of the interconnecting wire $R_c$ is zero in the ideal system, but should be considered in practical realizations as we'll address this question in this work later.

Although numerous papers have been published in the field there is still an ongoing debate about the security of the KLJN system. Several attacks against the security of the protocol were discussed [2-7], but the ideal KLJN system is still considered to be secure. Besides the original proof of security based on physical laws [1], a purely mathematical statistical evidence has also been shown [8, 9]. However, during the realization it is inevitable to introduce non-idealities into the system. These non-idealities are caused by wire resistances and wire attenuation, tolerance of the components including resistor values, voltage noise amplitude, external noise sources - any of these can cause significant information leak [10, 11] in the system, therefore can serve as the basis of different attacks. In our paper we give a detailed overview of the latest findings about the security of the KLJN system.

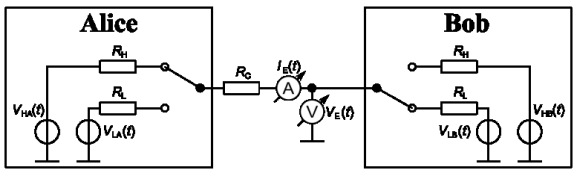


Fig. 1. Schematic of the KLJN key exchange system.

## II. SECURITY OF THE KLJN SYSTEM

### *A. Noise requirenments*

Using the classical physical approach it was shown that Gaussian white noise can ensure security and the following requirement must be satisfied [1]: $\sigma_H/\sigma_L = \sqrt{R_H/R_L}$, where $\sigma_H$ and $\sigma_L$ are the standard deviations of the noise voltages $V_H$ and $V_L$, respectively. Later it has been shown that only Gaussian noise can guarantee security [9], where the joint probability of the voltage $V_E$ and current $I_E$ can be observed by Eve are used in the analysis. In the following we use this joint probability density to estimate the effect of some practical parameters of a real KLJN system.

It has already been pointed out by Bergou [12], Scheuer and Yariv [4] that finite interconnecting cable resistance $R_c$ can cause information leak. Later Kish has introduced a method to completely eliminate this leak by adjusting the amplitude of the noise generators [13]. On Fig. 2 we show an example on how Eve can distinguish between HL and LH states. On the figure there is the scatter plot of $V_E$ versus $I_E$, the slope of the fitted line gives us the required information to extract bits. Note that the parameters are deliberately set to incorrect values to magnify the effect.

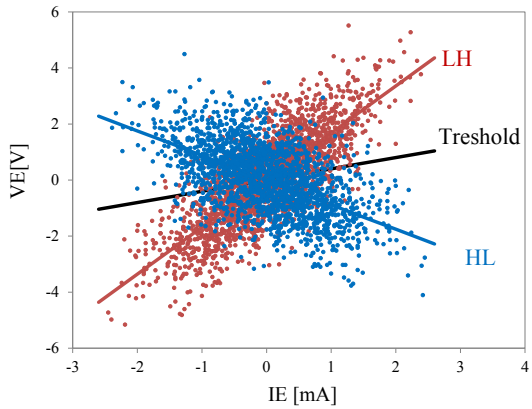


Fig. 2. Illustration of the method of extracting information from the KLJN system using joint probability. In the simulation 2000 samples were generated, and $R_L$=1000 Ohm, $R_H$=10000 Ohm, $R_C$=800 Ohm, while $\sigma_H/\sigma_L$ is.

## B. *Effects of resistance and voltage tolerance*

The limited accuracy of the resistors and voltage amplitude (that can depend on temperature in the original model) can also be sources of information leak. [1, 2]. One can easily see that according to Eq. (1) the error in resistance has smaller impact on security, since a small change in any of the resistor values causes smaller error in the equation than 1% deviation in the noise amplitude. On Fig. 3 the bit error rate as a function of the relative error of the resistance and voltage can be seen.

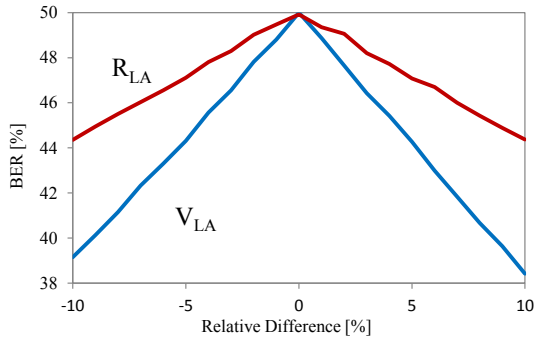


Fig. 3. Bit error rate as a function of the relative error of the nominal value of the resistance and voltage amplitude. Red and blue curves correspond to resistance and voltage changes, respectively. The measurement length was 100 correlation times, 5000000 bits were transferred.

## C. *Cable properties*

As it was mentioned above, the finite cable resistance if not compensated can cause information leak. Fig. 4 shows the simulation result for the bit error rate as a function of the cable resistance $R_c$. Eve will extract more and more information as the cable resistance increases.

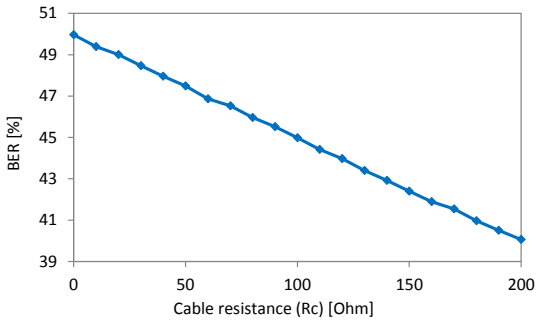


Fig. 4. Bit error rate as a function of cable resistance The measurement length was 100 correlation times, 5000000 bits were transferred.

## D. *Cable vulnerability against external noise sources*

In the current implementations of the KLJN system the resistance values are between 1 kOhm and 10 kOhm. This relatively high impedance makes the communication wire vulnerable to external noises which may be coupled in a capacitive or inductive way.

While the high frequency disturbances may be reduced by proper filtering, low frequency external noises, like 50/60 Hz and its harmonics may also influence the quantities measured on the wire. In one of our test we measured the voltage across a 3 m properly shielded coaxial wire with a differental amplifier (gain=2000). Although the cable was wound in a non-inductive bifilar configuration we could measure a relatively high 50 Hz component and several of its harmonics (Fig. 5). In order to reduce the effect we applied a 100 Hz high pass filter as used in [14], but as can be seen on the figure, it was not capable of reducing the higher frequency components, which were right in the frequency band of the communication. Although we identified the source of the interference (a nearby high quality Hameg HMP2030 laboratory power supply) this measurement showed that it is not trivial to get rid of the disturbances, and without proper measurement one should not assume that the system is properly protected against external noises.

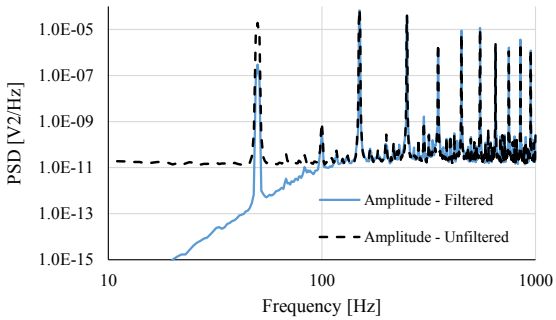


Fig. 5. Mains picup across a 3 m shielded cable after 2000x amplification. A 100 filter was applied to reduce the effect, but it is not enough in this case.

## III. Analysis of the Directional Coupler attack

In [14] Gunn et al presented a very interesting and original method for breaking the KLJN system. The method assumes that even in the no-wave limit operation of the KLJN system, the wave propagation is still applicable, moreover the waves travelling between Alice and Bob can be separated by a directional coupler. Based on this method the authors show that Eve may get reliable information about the exchanged bit in an astonishing short time (in some cases even within one correlation time).

However, their analysis also showed an important result: even if we can distinguish the right and left travelling waves, information leak only occurs if there is any attenuation in the system. If not, the directional coupler based attack cannot extract any information from the system.

Some aspects of the directional coupler attack were analyzed in a [15] and [16], one of the most important findings is that the attenuation rates which are causing excessive information leaks do not fulfill some basic restrictions of the KLJN system (like there cannot be any significant leakage current in the wire). Despite of the critics the "Gunn method" may still be applicable for lower attenuation values and may be used for information extraction. For further investigation of the method we performed numeric simulations and we reproduced some elements of the directional coupler system based on [14] and the additional information the authors provided to us.

### *A. Significant difference between the theory and measurement*

Comparing Figure 3 and 5 of article [14] it is hard not to notice that there is a significant difference between the theory and the practice. For cable attenuation of 0.1 according to the theory the 0.001 error rate is reached at around 90 correlation times while according to the measurement, this BER is already reached below 20 correlation times. The question is: what kind of artefacts may cause such a significant difference? In the next part we will show some problematic points.

In order to separate the right and left travelling wave Gunn et al are using a directional coupler. However, rather than calculating the exact coefficient values, the authors are using an LMS based adaptive filter to perform this task. The filter is calibrated when the end of the cable is terminated by a 50 Ohm resistor, the calibration is considered to be successful when the error drops below a given threshold. The benefit of this method is that imperfections in the directional coupler can be eliminated. At the same time, the result is affected by any other imperfection of the system and the result may not be the desired one. For example, according to our simulations the calibration can be considered to be "successful" even if there is no wave propagation. In this case, while the "right travelling wave" and the "left travelling wave" can still be used to extract information from the system, it is a different effect than the one stated by the theory. In our experimental tests we found similar results, although the resistance of the cable and connectors was significant, the calibration was also successful.

Similarly to the directional coupler, the second analysis step is also calibrated to the actual system. While this calibration may eliminate imperfections in the eavesdropping equipment and may give us promising results, nothing guarantees that it will behave according to the theory. This way we do not know whether the leakage is caused by wave propagation, cable attenuation or some other artefact like external noise (see section II/D), tolerance of components, unintended asymmetry of the test equipment or inadequate noise generation.

### *B. Effect of cable resistance and attenuation*

In [14] the author performed measurements while using the following attenuation values: 0.1 dB, 0.2 dB and 1 dB. Since the last two ones were performed by inserting an in-line attenuator into the KLJN system which violates the KLJN principles [16] the only relevant case is the 0.1 dB case which is measured using a 2 m coaxial cable.

We examined the datasheets of some commercially available coaxial cables and found that there is usually no attenuation data for frequencies below 1 MHz. At lower frequencies the effect of the cable inductance and cable capacitance becomes lower and lower, at the bandwidth of the KLJN the cable resistance dominates the attenuation. In order to get an estimation of the attenuation we measured the resistance of two different 3 m long cables which were connected to the system through BNC connectors. The total resistance of the RG58 cable with connectors was 0.257 Ohm while the resistance of the RG174 cable was 1.012 Ohm. If we terminate the cable with a 50 Ohm resistor, the resulting attenuation values are 0.05 dB and 0.17 dB respectively, which are comparable with the values Gunn et al measured. However, in the KLJN system, the smallest resistance in the system is typically 1000 Ohm yielding to attenuation values less than 0.01 dB. For this reason we conclude that the model of cable attenuation cannot be applied to the KLJN system as Gunn et al done.

Based on the available data we can calculate the voltage difference measurable on the cable.. Assuming a sinusoid signal with an amplitude of 1 V, a cable length of 3 m and a frequency of 5 kHz, the amplitude caused by wave propagation is 0.48 mV. If the cable is terminated by a 50 Ohm during the calibration procedure [14], the resulting voltage drop is 4.97 mV, an order of magnitude greater than the voltage measurable due to the wave propagation. Our opinion is that this voltage drop must significantly altered the calibration procedure. At the same time, during the KLJN key exchange, since the loop resistance is around 11 kOhm, the voltage drop will be order of magnitude smaller than the wave effect, rendering the original calibration useless.

## IV. Mitigation of the privacy leak

From the previous two parts it is clear that non-idealities of the implementation of the KLJN system will cause information leak. The severity of the information leakage can be mitigated by different tools. In [17] Horvath et al introduced an effective method for privacy amplification. The drawback of the method that it significantly reduce the key exchange rate.

In [13] Kish et al showed a method to eliminate the effect of cable resistance by modifying the noise scaling coefficient according to the actual cable resistance. While the method is

efficient, not all source of information leak can be eliminated this way. In the following we show a method that is independent of the source of the leak, and can be used against any statistical method based attack.

On Fig. 6 we present an example, where the statistics of HL and LH cases are distinguishable due to the cable resistance. The difference gives Eve the opportunity to successfully guess 60 % of the bits. To decrease Eve's success rate we can deliberately drop secure bits in order to achieve a completely overlapping statistic. At each secure bit, based on its measured parameters (like voltage SD difference) one can calculate the probability it should be dropped to achieve the best security. For the previous example, the resulting statistics is presented in the same figure (HH-leak.red and LH-leak.red. lines). By dropping the 20 % of the bits, the probability for Eve to guess the bits is reduced to 50.02 %.

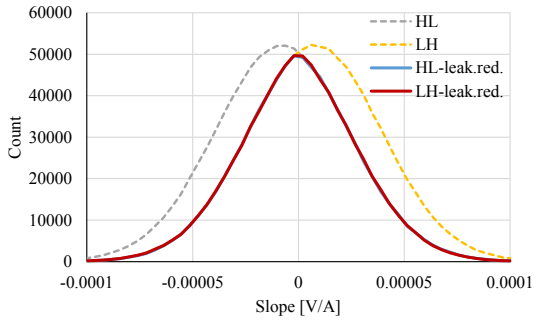


Fig. 6. Example of the effect of reducing privacy leak by deliberateli dropping secure bits. The HL and LH lines are the original statistics, the HL-leak.red. and LH-leak.red are the resulting statistics (note, they are complitly overlapping).

## V. Conclusions

Although the KLJN system may provide a low cost alternative to the quantum key distribution (QKD) a careful design is needed to provide adequate safety and mitigate privacy leakage.

In this paper we have reviewed and analyzed the effect of the parameters such as noise amplitude, tolerance of resistors or the cable resistance that may significantly affect the security of the system and if not properly handled may cause information leakage. At the same time we also demonstrated that this leak can be significantly reduced by deliberately dropping secure bits. The drawback of this method that the bit exchange rate will be reduced.

We also analyzed the attack method suggested by Gunn et al [14] and found that some aspects of the implementation may introduce such artefacts in the measurement that would compromise the results. Note that it is an important implication of the Gunn method that the wave propagation itself does not cause information leakage.

## Acknowledgment

We thank Lachlan Gunn for providing us helpful and detailed material describing the technical aspects of their method published in [14].

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] L.B. Kish, "Totally secure classical communication utilizing Johnson(-like) noise and Kirchhoff's law." Physics Letters A, 352, 178-182, 2006

[2] F. Hao, "Kish's key exchange scheme is insecure," IEE Proc. Inform. Soc. 153: 141–142., 2006

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

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

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

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

[7] 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: 2140–2142. doi: 10.1016/j.physleta.2010.03.021, 2010

[8] Z. Gingl, R. Mingesz, "Noise properties in the ideal Kirchhoff-Law-Johnson-Noise secure communication system," PLOS ONE 9:(4) Paper No e96109. 4 p., 2014

[9] R. Mingesz, G. Vadai, Z. Gingl, "What kind of noise guarantees security for the Kirchhoff-Law-Johnson-Noise key exchange?" Fluct. Noise Lett. 13:(3) Paper N°e1450021. 7 p. (2014)

[10] 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", Physics Letters A 372, 2008 978-984.

[11] R. Mingesz, "Experimental study of the Kirchhoff-Law-Johnson-Noise secure key exchange", Hot Topics in Physical Information (HoTPI-2013) International Journal of Modern Physics: Conference Series, Vol. 33, 1460365, DOI: 10.1142/S2010194514603652, 2014

[12] Bergou, J., interviewed in: Cho A. Simple Noise May Stymie Spies Without Quantum Weirdness. Science, 309 2148. DOI: 10.1126/science.309.5744.2148b, 2005

[13] L.B. Kish, C.-G. Granqvist, "Elimination of a Second-Law-Attack, and All Cable-Resistance-Based Attacks, in the Kirchhoff-Law-Johnson-Noise (KLJN) Secure Key Exchange System," Entropy 2014, 16, 5223-5231, 2014

[14] L.J. Gunn, A. Allison and D. Abbott, "A directional wave measurement attack against the Kish key distribution system," Sci. Reports 4 6461, doi: 10.1038/srep06461, 2014

[15] H.-P. Chen, L.B. Kish, C.-G. "Granqvist and G. Schmera, On the 'cracking' scheme, in the paper 'A directional coupler attack against the Kish key distribution system' by Gunn, Allison and Abbott," Metrol. Measurement Syst. 21 389–400, 2014

[16] L.B. Kish, Z. Gingl, R. Mingesz, G. Vadai, J. Smulko, C.-G. Granquist, "Analysis of an Attenuator Artifact in an Experimental Attack by Gunn–Allison–Abbott Against the Kirchhoff-Law–Johnson-Noise (KLJN) Secure Key Exchange System," Fluct. Noise Lett. 14, 1550011 (2015) DOI: 10.1142/S021947751550011X, 2015

[17] T. Horvath, L.B. Kish, J. Scheuer, "Effective Privacy Amplification for Secure Classical Communications," EPL (former Europhysics Letters) 94 28002-p1 - 28002-p6, 2011