Published: R Mingesz, N Bors, G Vadai, Z Gingl, *In Proceedings of* 24th International Conference on Noise and Fluctuations (ICNF) Vilnius, Lithuania, 2017.06.20-23. IEEE, pp. 200-203.
DOI: 10.1109/ICNF.2017.7985976, Copyright ©2017 IEEE

Performance and security analysis of the generalized Kirchhoff-Law-Johnson-Noise key exchange protocol

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

***Abstract*— The Kirchhoff-Law-Johnson-Noise (KLJN) key exchange protocol had been introduced as an ultra-low cost alternative of quantum cryptography. Two years ago we have developed a generalized version of the KLJN key exchanger (VGM-KLJN), and we have proved that the system works perfectly secure under much more general conditions that allows compensation of many kinds of imperfections. In this work we focus on the experimental analysis of our recently introduced VGM-KLJN system. We determine the time required to transfer a bit, the error rate of the information transfer and we also evaluate the probability of successful eavesdropping in the case of different imperfections of the components. We demonstrate a method of real-time identification and compensation of these imperfections. The results of our analysis can greatly aid practical applications and at the same time can serve as a guide to design a system with the required security level.**

Keywords— KLJN; VGM-KLJN; secure key exchange; unconditional security; secure key distribution; noise

I. INTRODUCTION

The Kirchhoff-Law-Johnson-Noise (KLJN) key exchange protocol had been introduced in 2006 as an ultra-low cost classical physical alternative of quantum cryptography [1]. While it offers unconditional security as well, only a few electronic components – resistors with Johnson noise sources – are required to achieve very high levels of security, and it can even be integrated into circuits, microchips. In the KLJN system there are two selectable resistors with higher and lower values at both communication parties. The selected resistors at the ends of the communication line are connected to form a loop. Johnson noise of the resistors is used to exchange and hide the information from the eavesdropper at the same time. Measuring the noisy voltage and current in this loop informs the communicating parties about the selection state of the resistors at both ends, while the eavesdropper can't determine which resistors are used by the communicating ones. In other words, a bit can be securely exchanged.

A. The description of the KLJN protocol

The KLJN system can be used to exchange a secret key for single use to encrypt data. In the original system, the communication between the two parties, usually called Alice and Bob, are realized by resistor pairs. During the transfer of a bit of the secret key Alice and Bob connects one of their resistors with publicly known lower or higher value, R_L or R_H, to the communication wire randomly. Due to the Johnson noise (thermal noise) of the resistors random voltage will be present on the communication wire and random current can be observed in the loop. The resulting loop resistance therefore can be determined by measuring these signals. Since Alice and Bob know the resistor value at their side, they can determine the resistor value at the other side by measuring the loop resistance. On the other hand, the eavesdropper Eve has less information. If the selected resistors at the two ends have the same value (R_L or R_H), then Eve knows the state as well. However, if the resistors are different at the two terminals, Eve will measure the same noise properties for both possible states, therefore she does not have information about which party used R_L and which one connected R_H to the wire. It is important to note that in this case there is no correlation between the voltage and current observed by Eve, in other words, the system is in thermal equilibrium, no power flows from one end to the other. These two states, LH and HL can be used to share a bit secretly. Note that since the thermal noise amplitude is very small, separate voltage generators are needed in practical applications.

B. The generalized KLJN protocol

Recently we have developed a generalized version of the KLJN key exchanger (so called VGM-KLJN system, see Fig. 1), and we have proved that the system works perfectly in much more general conditions [2,3]. We have shown that all four resistor values can be arbitrarily chosen independently of each other. It is not required to have the same R_H and R_L values at the two ends, the only restriction is to have two different values at a given end. In this system, non-zero correlation can be present between the current and voltage at any point of the wire, i.e. the system is not any more in thermal equilibrium, power can flow from one end to the other. However, by properly tuning the amplitudes of the voltage noise generators, it can be the same for both the LH and HL cases. Many limitations caused by non-ideal component values, finite wire resistance can be compensated by tuning the amplitude of the voltage noise generators. Our results inspired a new protocol as well (RRRT-KLJN [4]).

This research was supported by the Hungarian Government and the European Regional Development Fund under the grant number GINOP-2.3.2-15-2016-00037 ("Internet of Living Things").

978-1-5090-2760-6/17/$31.00 ©2017 IEEE

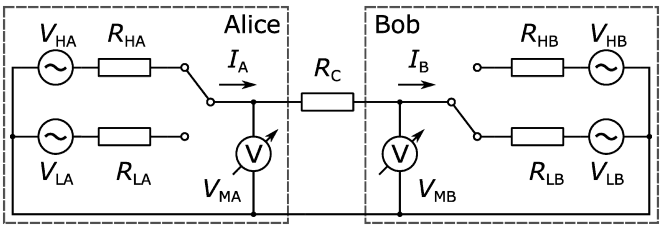

Fig. 1. The block diagram of the generalized VGM-KLJN system. Alice and Bob have two independent pairs of lower and higher resistors of any value. The only restriction is to have two different values at a given end. V_{MA}, I_A, V_{MB} and I_B are the voltage and current values measured and shared by Alice and Bob.

In this work, we focus on the experimental analysis of our VGM-KLJN system concerning the time required to transfer a bit, the error rate of the information transfer and the evaluation of the probability of successful eavesdropping. We show how efficient bit detection can be implemented by using the VGM-KLJN system. We also perform analytical and numerical analysis on how the required bit exchange time depends on the selection of the resistor values. Certain imperfection of the components, like the tolerance of resistors, causes information leakage. Here we also provide a detailed analysis of these effects, and show a method of real-time identification and compensation of these imperfections as well.

The results of our analysis can aid practical applications radically and can serve as a guide to design a system with the required security level in the same time as well.

II. Bit Detection for Alice And Bob

A sample voltage signal during a bit exchange process is shown in Fig. 2. In order to avoid the effects of the transients the signal is ramped up at the beginning and ramped down at the end of the bit exchange, then low pass filters are used to limit the bandwidth that is required to prevent information leak [5]. The stationary signal part followed by the ramping up is used by Alice and Bob to compute the statistics of the signals. As it was mentioned in section I.A for the original KLJN system, it can be easily determined using the voltage and current signals if the system is in the LL, HH or one of the secure LH or HL states [6].

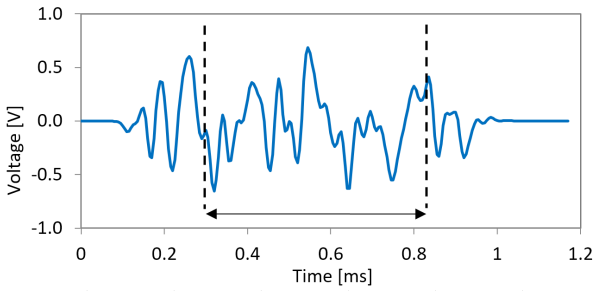

Fig. 2. Demonstration of the voltage signal of the wire during the transfer of a single bit. Alice and Bob can evaluate the statistics properly in the time window defined by the two vertical dashed lines.

Voltage signals can be used to distinguish between HH and other states, while current signals need to be analyzed in order to separate the LL state clearly from all other states, see Fig. 3 [6]. Since the probability densities are practically the same for the generalized VGM-KLJN key exchanger, the method is applicable in this case as well.

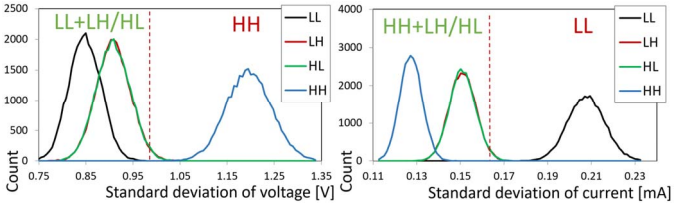

Fig. 3. Histograms of the measured standard deviation of voltage (left panel) and current (right panel). The HH or LL states can be separated efficiently by analyzing the voltage or current signals, respectively.

A. Statistics of the measured signals

The estimated standard deviations of the signals during the bit exchange have some uncertainty, therefore it has a certain likelihood for false detection of the real state.

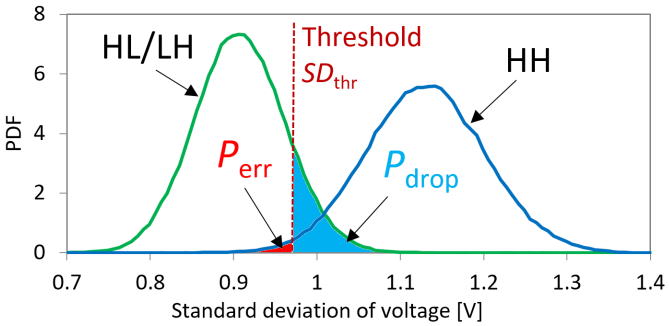

Fig. 4. Exaggerated figure of the voltage statistic, showing the meaning of P_{err} and P_{drop}.

As it is shown in Fig. 4, a threshold can be chosen to tune the probability P_{err} of falsely considering the HH state as a valid bit (LH or HL state), and to set the probability P_{drop} of dropping a valid secure bit due to recognizing a valid secure state as HH state:

$$P_{err} = F_{HH}(SD_{thr}) \quad (1)$$

$$P_{drop} = F_{sec}(SD_{thr}) \quad (2)$$

Here F_{HH} is the probability distribution function of the HH state, F_{sec} is the probability distribution function of the secure states, SD_{thr} is the selected threshold value.

The aim of the communicating parties is to reduce P_{err} as much as possible in order to avoid false detections of insecure bits. However, decreasing P_{err} will elevate P_{drop}, therefore some proportion of secure bits will be dropped which reduces the bit transfer rate. Improving the accuracy of the measurement during a single bit transfer requires more time, therefore the bit rate will be smaller again. Consequently, the goal is to find the optimal measurement time for a given P_{err} that provides the highest bit transfer rate.

Looking at Fig. 4. one could conclude that the probability density functions correspond to normal distribution, however, they do not. When determining the threshold levels it is easier to consider the voltage and current variances, since these are calculated by summing the square of a normally distributed variable, therefore the measured values follow χ^2 distribution. The expected value of the variances (σ^2) can be determined using the values of the resistors and the amplitudes of the voltage generators. The variance of the measured variances can be given as $2\cdot\sigma^4/k$, where k is the number of independent measurement points. Since the bandwidth (f_{bw}) of the system must be limited in order to prevent information leak [1], k is not equal to the number of samples (N) but can be approximated by the following formula [7]:

$$k \approx N \cdot \frac{f_{bw}}{f_{Nyquist}} = N \cdot \frac{2 f_{bw}}{f_s}, \qquad (3)$$

where f_s is the sample rate and $f_{Nyquist}$ is the corresponding Nyquist frequency. In our current analysis, we are only interested in the statistical analysis of the protocol and not in the transient behavior. For this reason, wherever possible we ignore the bandwidth limitations of the communication, this way all points in the measurement window can be statistically independent from each other. In the following, the length of the measurement window is expressed in the number of statistically independent measurement points (k).

B. Optimizing the bit detection time

In the VGM-KLJN system the amplitude of one of the four voltage generators can be arbitrarily chosen, the other three must be calculated and set accordingly in order to guarantee security [3]. Using these and the circuit shown in Fig. 1 it is possible to determine the distribution of the voltages and currents for a given bit detection time. If the desired bit error rate is known, then it is possible to find the threshold values and the rate of dropped secure bits.

Fig. 5 illustrates how the rate of dropped bits depends on the bit detection time for a certain set of resistor values and the error rate of 10^{-6}. Both the theoretical and simulated results are plotted.

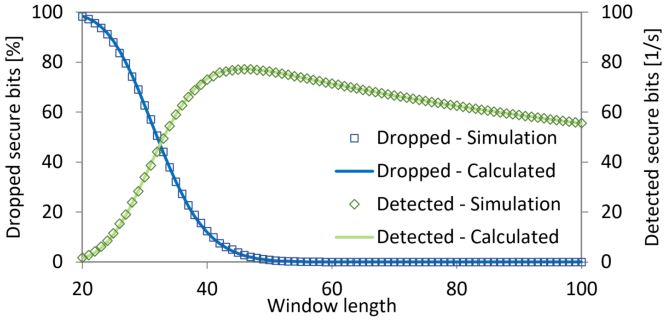

Fig. 5. Ratio of the dropped secure bits (P_{drop}) and bit transfer rate as a function of window length for a transfer of 20000 bits. R_L=R_{LA}=R_{LB}=1 kΩ, R_H=R_{HA}=R_{HB}=10 kΩ, R_C=200 Ω. To calculate the bit rate, we used a bandwidth of 5 kHz, with a constant overhead of 8 ms/bit.

The bit transfer rate can be calculated using the bit detection time and the rate of dropped bits. The bit transfer time depends on several factors including the bandwidth [8] and the ramp-up and ramp-down times used to avoid transients and the associated information leak. To calculate the bit rate, we used a bandwidth of 5 kHz, with a constant overhead of 8 ms (at the beginning and the end of measurements). The number of transferred bits are reduced further by the fact that only half of the states correspond to the secure LH or HL states.

It is easy to see on Fig. 5, that there is an optimal bit detection time that maximizes the secure bit transfer rate. This depends on the ratio of the higher and lower resistances R_H/R_L. As shown in Fig. 6, larger ratio reduces the required bit detection time therefore increases the bit transfer rate.

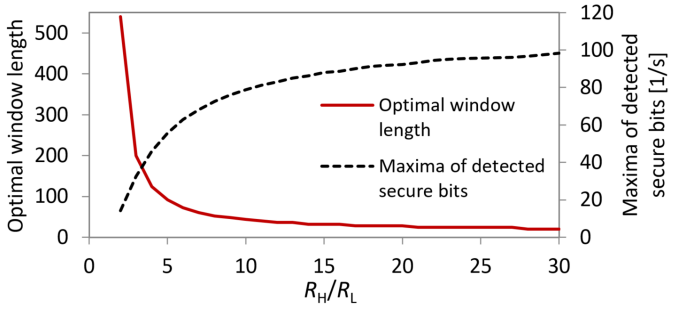

Fig. 6. Optimal window length and maxima of detected secure bits as a function of R_H/R_L ratio for a transfer of 50000 bits.

The results above were obtained using resistor values compatible with the original KLJN system, however the wire resistance was compensated according to the VGM-KLJN theory. Fig. 7 reports on results for more general resistor configurations used in [2]. Note that the lower transfer rates are due to the lower R_H/R_L rates on both sides.

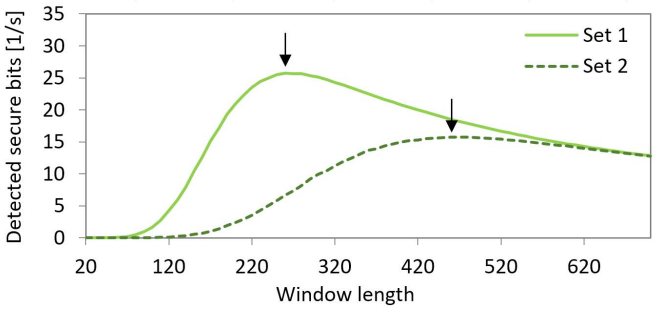

Fig. 7. Bit rate for more generalized resistance setups for a transfer of 30000 bits. In case of Set 1, R_{LA}=1 kΩ, R_{HA}=10 kΩ, R_{LB}=5 kΩ, R_{HB}=9 kΩ, R_C=200 Ω, optimal window length is 260 points, in case of Set 2 R_{LA}=1 kΩ, R_{HA}=5 kΩ, R_{LB}=5 kΩ, R_{HB}=9 kΩ, R_C=200 Ω, optimal window length is 460 points.

III. Information Leakage and Real-Time Compensation

Full security of KLJN key exchange cannot be achieved in real systems [9]. The eavesdropper can measure the statistics of the current, voltage and their correlation at any point of the interconnecting wire, however her bit error rate (BER) will be

higher than for Alice and Bob, can be very close to the perfectly secure 50%.

We have carried out numerical simulations to evaluate BER for values of resistors or voltage generators that deviate from the ones required for security [3]. Fig. 8 shows the BER calculated from three different quantities as a function of the error of Bob's higher value resistor. The system exhibits rather high sensitivity to the error of resistance, although resistors can be quite accurate and can be measured and compensated as well. Longer time available to the eavesdropper certainly increases the information leakage as depicted on Fig. 9. Note that the BER values and the effect of the components' tolerance also depends on the resistor configuration of the generalized KLJN.

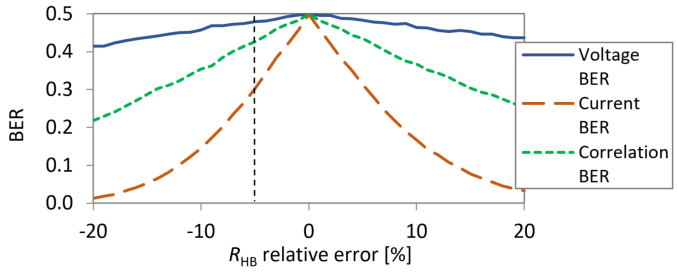

Fig. 8. Eavesdropper's bit error rate as a function of relative error of real R_{HB} and nominal R_{HB} value in case of Set 1 from Fig. 7. Time window has a length of 260 points.

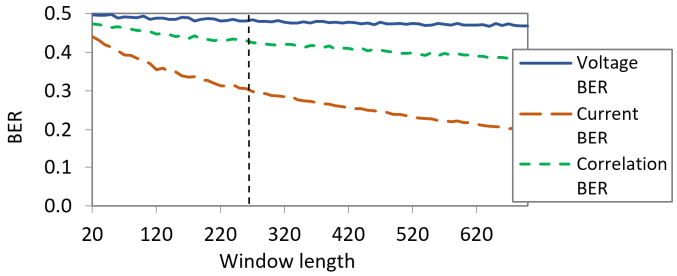

Fig. 9. Eavesdropper's bit error rate as a function of the window length in case of Set 1 from Fig. 7, when R_{HB} has a relative error of -5%.

In order to generate information leak one of the simplest possibilities for the eavesdropper is the significant modification of the wire resistance R_C. Fig. 10 shows that large changes in R_C result in moderate drop of the BER and Alice and Bob can quickly detect this intrusion as illustrated by Fig. 11.

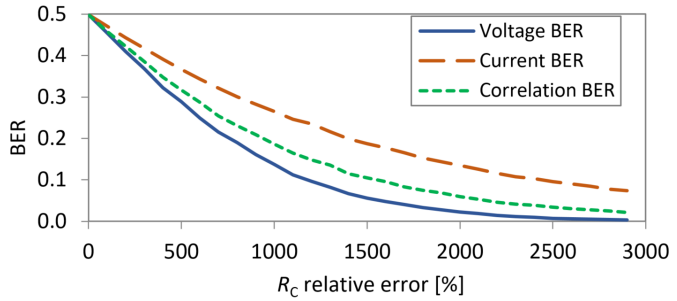

Fig. 10. Eavesdropper's bit error rate as a function of cable resistor relative error in case of Set 1 measuring 260 points.

Note that Alice and Bob can detect the change of R_C instantly by comparing I_A, I_B, V_{MA} és V_{MB}, see Fig. 1. They can retune their noise generators accordingly to prevent information leak.

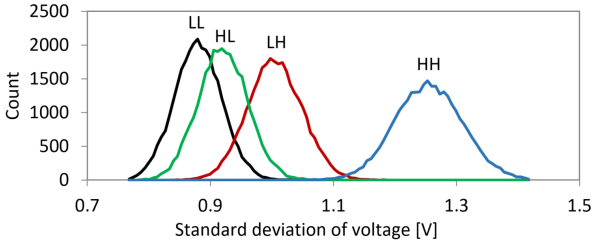

Fig. 11. Statistics measured by Alice in case of Set 1 if the eavesdropper tampered the cable resistance. R_C has a relative error of 1000% resulting in a voltage BER of 0.156.

IV. Conclusions

The most important advantage of the VGM KLJN system is the ability to compensate non-ideal values of its components. Measuring the inaccuracies allows the parties to tune the amplitude of their noise generators to ensure secure communication. In this paper, we have shown how to determine the bit detection time required to maximize the bit transfer rate and to reduce the time available to the eavesdropper at the same time. We have also investigated the bit error rate and associated information leak in certain cases of deviations from ideal component values. Our results show that the communicating parties Alice and Bob can detect such problems and can compensate them even in real time.

References

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

[2] G. Vadai, R. Mingesz, Z. Gingl, "Generalized Kirchhoff-Law-Johnson-Noise (KLJN) secure key exchange system using arbitrary resistors," Scientific Reports, vol. 5: Paper 13653. 7 p., 2015.

[3] G. Vadai, Z. Gingl, R. Mingesz, "Generalized Attack Protection in the Kirchhoff-Law-Johnson-Noise Secure Key Exchanger," IEEE ACCESS, vol. 4: pp. 1141-1147, 2016.

[4] L. B. Kish, C. G. Granqvist, "Random-Resistor-Random-Temperature Kirchhoff-Law-Johnson-Noise (Rrrt-Kljn) Key Exchange," Metrol. Meas. Syst. Vol. 23, No. 1, pp. 3-11., 2016.

[5] 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, vol. 372, pp. 978-984, 2008.

[6] 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, 2014.

[7] Effect ot the bandwith on the number of independent samples, available: http://www.noise.inf.u-szeged.hu/Research/kljn/bandwidth/

[8] R. Mingesz, Z. Gingl, G. 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). Xi'an, China,.pp. 264-267., 2015.

[9] L.B. Kish, C.G. Granqvist, "On the security of the Kirchhoff-law-Johnson-noise (KLJN) communicator," Quantum Information Processing, vol. 13, pp 2213-2219, 2014.