Hot Topics in Physical Information (HoTPI-2013)
International Journal of Modern Physics: Conference Series
Vol. 33 (2014) 1460368 (8 pages)

DOI: 10.1142/S2010194514603688

Performance analysis of the "intelligent" Kirchhoff-Law-Johnson -Noise secure key exchange

Janusz Smulko

Faculty of Electronics, Telecommunications and Informatics, Department of Metrology and Optoelectronics, Gdansk University of Technology, 80-233 Gdansk, G. Narutowicza 11/12, Poland
jsmulko@eti.pg.gda.pl

Published 17 September 2014

The Kirchhoff-Law-Johnson-Noise (KLJN) secure key distribution system provides a way of exchanging information theoretic secure keys by measuring the random voltage and current through the wire connecting two different resistors at Alice's and Bob's ends. Recently new advanced protocols for the KLJN method have been proposed with enhanced performance. In this paper we analyze the KLJN system and compare with "intelligent" KLJN (iKLJN) scheme. This task requires the determination of the applied resistors and the identification of the various superpositions of known and unknown noise components. Some statistical tools to determine how the duration of the bit exchange window (averaging time) influences the performance of secure bit exchange will be explored.

Keywords: Johnson-Noise; secure communication; statistical hypothesis.

1. Introduction

Secure communication is a topical subject in modern society due to increasing importance of data transfer, internet banking and digital rights management. Therefore the introduction of Kirchof Law and Johnson (-like) Noise code which requires ordinary resistors and thermal noise analysis only is very promising[1]. The KLJN scheme is founded on the Second Law of Thermodynamics, which makes the scheme as secure as it is impossible to build a perpetual motion machine of the second kind. Additionally, enhanced secure key exchange system (e.g. "intelligent" KLJN – iKLJN) based on this scheme was proposed to assure practically-perfect security[2] by means of classical physic, without using quantum computing[3]. The KLJN scheme is a challenging proposal and requires in-depth analysis to establish how the KLJN protocols are resistant against eavesdrop at the settled noise bandwidth and averaging time. Moreover, it is another interesting application of noise in information processing, which starts to be developed, together with other examples of noise use in signal processing and sensing[4–7].

In this theoretical study some selected statistical tests are applied as a new tool to determine time of averaging which is necessary for correct bites detection at given

significance level. The same analysis method was applied to compare efficiency of two protocols: the classical KLJN[1] and the recently introduced iKLJN[2]. Efficiency of the secure data transfer is analyzed to establish statistical errors of incorrect detection of the transferred bites (a type I and type II errors). Influence of distance between the observed noise intensities responding to the transferred bites combinations and averaging time on errors of the transmitted data were considered. Finally, some conclusions achieved for the introduced iKLJN scheme were presented to highlight its new quality in secure code exchange, requiring shorter averaging time than the classical KLJN scheme.

1.1. *The Kirchhoff-Law-Johnson-Noise (KLJN) secure key exchange scheme*

The idealistic KLJN scheme comprises of two sets of resistors of low R_L and high R_H resistances at both communicating parties Alice (A) and Bob (B) which are randomly chosen and connected to the transmission line (Fig. 1). The resistances $R_H = a \cdot R_L$ are of significantly different values ($a >> 1$). Noise is introduced into the system by the Gaussian voltage noise generators, serially adjoined to the resistors. The generators deliver white noise at publically established bandwidth and at effective temperature T_{eff}, typically a few orders higher than the system temperature[4]. The noise sources are statistically independent and have the voltage power spectral density $S_u(f) = 4kT_{eff}R$, where R equals to R_L or R_H. Noise at transmission line (current $I_C(t)$ or voltage $U_C(t)$) can be observed within a clock period which responds to a single bit exchange rate. For simplicity of this paper only voltage fluctuations $U_C(t)$ at transmission line will be analyzed to determine which bites are exchanged. The same results can be received when the current $I_C(t)$ is considered.

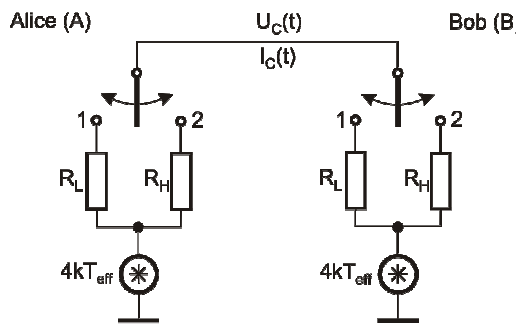

Fig. 1. Schematic circuit of the Kirchhoff-Law-Johnson-Noise (KLJN) secure key distribution system.

A secure bit transfer occurs only in a case when the resistors at both sides (A) and (B) have different values R_H and R_L or R_L and R_H which is adequate to a case of 01 or 10 bites exchange. Such case will result according to the Second Law of Thermodynamics in the same intensity of noise at the transmission line but information about the adjusted resistors will be secure because Alice and Bob will know their resistors positions. Otherwise (11 or 00 bites transmission) eavesdropper would be able to overhear the data.

Variance of voltage fluctuations for these cases at the normalized bandwidth Δf is derived by[2]:

$$\sigma_{01}^2 = \sigma_{10}^2 = 4kT_{eff}R_{loop}\,, \tag{1}$$

where R_{loop} is a substitute resistance of the transmission loop. Thus, we can expect that according to three various combinations of R_{L} and R_{H} at both ends of the loop three different variances in transmission line can be observed:

$$\sigma_{00}^2 = 4kT_{eff}\frac{R_L R_L}{R_L + R_L}\Delta f = 4kT_{eff}\frac{R_L}{2}\Delta f\,, \tag{2}$$

$$\sigma_{01}^2 = \sigma_{10}^2 = 4kT_{eff}\frac{R_L R_H}{R_L + R_H}\Delta f = 4kT_{eff}\frac{R_L R_H}{R_L + R_H}\Delta f = 4kT_{eff}R_L\frac{a}{1+a}\Delta f\,, \tag{3}$$

$$\sigma_{11}^2 = 4kT_{eff}\frac{R_H R_H}{R_H + R_H}\Delta f = 4kT_{eff}\frac{R_H}{2}\Delta f = 4kT_{eff}R_L\frac{a}{2}\Delta f\,. \tag{4}$$

The values of σ_{00}, σ_{01} and σ_{10}, or σ_{11} observed in the transition line are unevenly distributed because distances between them depend on the parameter a ($R_{\mathrm{H}} = a \cdot R_{\mathrm{L}}$) and at $a = 10$ are close to ratios 1:1.81:10. Voltage variance σ^2 at transmission line will be estimated over limited observation time and therefore random error of its value has to be considered to evaluate probability of false detection of the transmitted bites. Especially, relatively smaller difference between variances σ_{00} and σ_{01} or σ_{10} can influence strongly correctness of the transmitted data at established averaging time.

This problem was addressed in literature by utilizing Rice's formula for the level crossing statistics[8]. Error probability due to inaccuracies in noise voltage measurements was established for a case when the actual situation of the transmitted 00 bites was interpreted as the secure noise level 01 or 10. In the literature, to the best knowledge of the author of this article, there has been not presented any analysis how the distances between the estimated variances influence accuracy of bites recognition and how to establish averaging time to assure the assumed accuracy. Thus, the more in-depth analysis of that problem has to be conducted. To solve this issue an approach of statistical hypothesis testing can be utilized as a tool which considers random errors due to the accepted hypothesis of the transferred bites.

1.2. *The "intelligent" Kirchhoff-Law-Johnson-Noise (iKLJN) secure key exchange scheme*

Secure data exchange KLJN scheme of 01 and 10 bites transmission relies on noise intensity measurements in the line and secret knowledge of Alice and Bob on which of their sites resistors R_{L} or R_{H} are attached. A new KLJN scheme has been proposed recently where Alice and Bob utilize as well a knowledge of the stochastic time function of their own noise generator[2]. Thus, this new "intelligent" iKLJN scheme gives additional privilege to Alice and Bob when compared to Eve who can observe channel noise only. Therefore, the iKLJN scheme will reduce averaging time at the same correctness of bites transmission rate when compared with the earlier introduced KLJN scheme.

To reduce averaging time Alice and Bob have to observe line noise (e.g., voltage $U_C(t)$) and their noise generator stochastic time function (e.g., $U_B(t)$ for Bob and $U_A(t)$ for Alice). The observed channel noise $U_C(t)$ can be reduced by subtracting the scaled noise component of noise $U_B(t)$ for Bob and $U_A(t)$ for Alice according to the assumed positions of the resistors at Alice and Bob ends. If the assumption was true, the line noise component after subtraction is uncorrelated with Bob or Alice noise sequence. This fact can be investigated by estimating cross-correlation function which is independent source of information about the transferred bites. The detailed way of determining the cross-correlation function can be found elsewhere[2]. For simplicity of this paper let's consider exemplary situation when Bob having resistance R_L assumed correctly that Alice has different resistance $R_H = a \cdot R_L$. Thus, Bob knows time sequence $U_B(t)$ of his noise generator and can subtract from the observed line noise $U_C(t)$ a part coming from his generator and attenuated by the existing voltage divider of the resistances R_L and R_H[2]:

$$U_{C*}(t) = U_C(t) - U_B(t)\frac{a}{1+a} = \frac{U_A(t) + aU_B(t)}{1+a} - U_B(t)\frac{a}{1+a} = \frac{U_A(t)}{1+a}. \tag{5}$$

Correctness of Bob assumption can be proved by estimating cross-correlation function:

$$E\left[U_{C*}(t) \cdot U_B(t)\right] = \frac{E\left[U_A(t) \cdot U_B(t)\right]}{1+a} = 0 \tag{6}$$

if the assumption is true. Operator E means averaging. To sum up, we conclude that iKLJN scheme can comprise of two independent procedures:

- estimation of noise variance in the transmission line,
- determination if the cross-correlation function between the generator stochastic time function and the line noise after subtracting the respectively scaled generator stochastic time function.

Both functions will assure 01 or 10 secure bit exchange. Thus, a combination of these two procedures will strengthen data exchange by shortening averaging time or decreasing transmission error rate when compared with firstly proposed KLJN scheme.

We can consider cross-correlation between $U_{C*}(t)$ and $U_B(t)$ or voltage variance σ^2 in the channel line as independent probabilistic quantities which means that using both procedures probability of true bit detection is a product of joined probabilities of these two procedures. It means that keeping the same error of bites rate exchange we can decrease substantially averaging time. This conclusion is very substantial when no idealistic system is considered because the iKLJN scheme will make the bites exchange more robust against plausible attacks when compared with the KLJN scheme. This conclusion is valid even when the cross-correlation will not be absolutely independent from noise variance in line in non-idealistic system. It should be underlined that some preliminary tests of secure bites transmission has been performed to shed light on its limitations in practical applications[9].

Introduction of iKLJN scheme means that we have to test if the selected quantities $U_{C*}(t)$ and $U_B(t)$ are correlated or not. This fact can be explored using statistical tools, like testing correlation by statistical test of non-zero linear correlation coefficient or

testing if a mean value of the cross-correlation function defined by (6) is different from zero.

2. Discussions and results

In this paragraph a new approach to KLJN secure scheme will be considered by utilizing statistical hypothesis tests. The tests will take into account averaging time necessary to establish statistical hypothesis about transmitted bites at given error rate. Number of averaged noise samples will be considered which responds to averaging time at given sampling rate. Firstly, problems of determining variance σ^2 of noise at the transmission line at given error of false detection (detection of the bites 01 or 10 transmission instead of 00 and vice versa) will be considered. Secondly, methods of cross-correlation detection will be discussed according to their potential application in iKLJN scheme.

2.1. *Inaccuracy interval at the KLJN secure key exchange scheme*

Estimation of noise variance in transmission line requires averaging over limited number of voltage samples. The estimator s^2 of variance σ^2 by using N samples of $U_C(t)$ in the transmission line is derived by formulae:

$$s^2 = \frac{1}{N-1}\sum_{i=1}^{N}\left(U_C(t) - \mu_{U_C}\right)^2, \tag{7}$$

where μ_{Uc} is the estimated mean value derived by using the same voltage samples $U_C(t)$ as to estimate s^2. It is known[10] that the product:

$$\sum_{i=1}^{N}\left(U_C(t) - \mu_{U_C}\right)^2 = \sigma^2\chi_n^2, \tag{8}$$

where χ^2_n has a Chi-square distribution with $n = N - 1$ degrees of freedom. By applying information about distribution of the estimated variance its confidence intervals can be determined at given level of significance α – probability that variance σ^2 belong to this interval determined by variance estimator s^2:

$$\text{Prob}\left[\frac{ns^2}{\chi^2_{n,\alpha/2}} \le \sigma^2 < \frac{ns^2}{\chi^2_{n,1-\alpha/2}}\right] = \alpha, \tag{9}$$

where $\chi^2_{n,\alpha/2}$ and $\chi^2_{n,1-\alpha/2}$ are Chi-square distribution vales which can be read out from the distribution table at given level of significance α and which determines probability that the estimated variance exceeds the interval defined by (9).

At secure bites transmission using KLJN scheme the estimator s^2 of variance σ^2 is used to detect the transmitted bites. A fixed number, usually $\alpha = 0.05$, is referred as a level of significance and determines the probability of incorrect rejection of the true statistical hypothesis (s^2 is equal to σ^2 which is called the null hypothesis) in favor of the second alternative hypothesis (s^2 is not equal to σ^2). Such incorrect assumption is called

the Type I Error and its rate is equal α (false positive rate). At given level of significance α it is possible by using (9) to determine number of averaged voltage samples $N = n + 1$ which is necessary to detect the transmitted bites at given probability.

Another error type which can occur is when the hypothesis may be accepted when in fact it is false. Such case is called a Type II Error and can be established when the true value of the estimated parameter is different by a fixed constant from the hypothesized value. The type II error is equal β which can be different in general from the type I error equal α. The probability $1 - \beta$ is called power of the test. For any given number N of averaged samples a Type I Error can be reduced by reducing the level of significance α. At the same time the probability β of the Type II Error will be increased (reduced power of the test). The only way to reduce both errors is to increase number N of the averaged samples.

When the KLJN scheme is taken into account, the case of detecting bites transmission 00 or 01 and 10 will respond to the same situation as presented before when the estimated variance has to be assigned to one of two values σ_{00}^2 and σ_{10}^2 or σ_{01}^2, which are shifted by $\Delta\sigma^2$ (Fig. 2). The third observable variance σ_{11}^2 at the transmitted bites 11 can be omitted because its distance from other variances responding to transmissions of other bites is a few times bigger than between σ_{00}^2 and σ_{10}^2 or σ_{01}^2 according to the selected parameter $a \geq 10$ (see. the eq. (3), (4) and (5)).

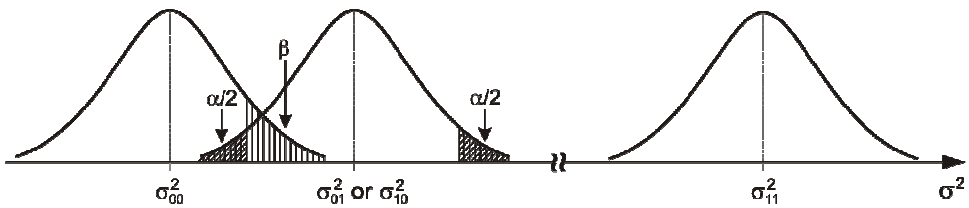

Fig. 2. Illustration of noise variance σ^2 at their given probability distributions (solid lines) observed in transmission line at different combination of resistances R_L, R_H at the ends of KLJN secure key distribution system; low index at variance responds to the combination of the resistances: R_L means 0 and R_H means 1.

To optimize selection of the averaged samples $N = n + 1$ to assure the same value of Type I Error and Type II Error it is necessary to write equations for lower and upper limit of variance estimator s^2 for both errors, when the distributions cross each other (Fig. 2). The difference between the variances according to (2) and (3) is equal to:

$$\Delta\sigma^2 = \sigma_{10}^2 - \sigma_{00}^2 = \sigma_{01}^2 - \sigma_{00}^2 = 4kT_{eff}\Delta f R_L \frac{a-1}{2(a+1)}. \tag{10}$$

Hence, the equations for lower limit of s^2 can be delivered from (9):

$$s^2 = \frac{\sigma_{01}^2 \chi_{n,\alpha/2}^2}{n}, \tag{11}$$

and at the same time higher limit for the Type II Error is given by:

$$s^2 = \frac{\sigma_{01}^2 \chi_{n,1-\beta}^2}{n} - \Delta\sigma^2 . \tag{12}$$

Chi-square distribution tends to Gaussian distribution, represented by normalized variable z (having zero mean value and variance equal to 1), at sufficiently high n, which usually exceeds at least a few tens of samples:

$$\chi_n^2 \approx \sqrt{2n}\, z + n . \tag{13}$$

Thus, by comparing (11) with (12) and using simplification to Gaussian distribution due to (13) we can get:

$$4kT_{eff}\Delta f R_L \frac{a\left(\sqrt{2n}\, z_{\alpha/2} + n\right)}{(1-a)n} = 4kT_{eff}\Delta f R_L \frac{a\left(\sqrt{2n}\, z_{1-\beta} + n\right)}{(1-a)n} - 4kT_{eff}\Delta f R_L \frac{a-1}{2(a+1)} . \tag{14}$$

Equation (14) after necessary rearrangements can be reduced to the statement describing how the number of noise samples $N = n + 1$ depends on both assumed error levels α, β and parameter a:

$$N = 8\left(z_{\alpha/2} - z_{1-\beta}\right)^2 \cdot \frac{a^2(a+1)^2}{(a-1)^4} + 1 . \tag{15}$$

Some interesting conclusions can be withdrawn from the resulting eq. (15). When a tends to 1 (the applied resistors R_H and R_L tends to have the same value) time necessary for averaging tends to infinity. Additionally, the function (15) is a continuous function of the parameter a without local extremes and tends to zero when a closes to infinity. This means that noise averaging time decreases when the distance between R_H and R_L became bigger which fact corresponds to general feeling of continuous character of classical physics laws applied in the KLJN scheme.

Number N of the averaged noise samples depends on the difference between $z_{\alpha/2}$ and $z_{1-\beta}$. Assuming typical value for $\alpha/2 = 2.5\%$ we can decrease N even to one ($z_{\alpha/2} = z_{1-\beta}$) when $1 - \beta = 2.5\%$ as well. Then the Type II Error is equal to $\beta = 97.5\%$ which means that this error is close to certainty and such case doesn't have any practical meaning. Independently from the considered borderline cases the eq. (15) can estimate necessary number of the averaged noise samples N at given transmission conditions (assumed Type I and Type II Errors by the selected levels of significance α and β).

2.2. *Benefits of the iKLJN secure key exchange scheme*

When the iKLJN scheme is applied the presented statistical approach for determination of noise variance in transmission line can be used as well. Additionally, the condition about independence between the considered noise time series (given by eq. 6) can be tested using another statistical test which is independent in idealistic case from the variance test applied at the KLJN scheme. The correlation between the selected noise time series $U_{C^*}(t)$ and $U_B(t)$ can be investigated using linear correlation coefficient[10] or another measure of correlation between two variables[11]. Statistical test of linear correlation

coefficient can establish at given level of significance α if the hypothesis about non-zero correlation between $U_{C*}(t)$ and $U_B(t)$ exist or should be rejected. Another possible and equivalent analysis to the mentioned above is to test whether the cross-correlation given by eq. (6) is equal to zero. This can be done by testing if the mean value of (6) is zero using acceptance interval similar as given by eq. (9) and determined for variance estimator s^2. Then, the proposed above statistical approach can establish number N of the averaged samples at given averaging time.

3. Conclusions

In this theoretical study a problem of secure bites detection using KLJN scheme was considered by applying statistical approach to noise parameters estimation. It has been proved that the presented method can determine the number N of noise samples necessary for averaging at the assumed level of statistical errors of Type I and Type II.

When the iKLJN scheme is applied an additional statistical test of cross-correlation or simple linear correlation between the noise time series can be utilized to decrease bites detection error at the same averaging time. Another possibility when using iKLJN scheme is to reduce averaging time at the same error rate of bites detection. This case requires additional analysis how to estimate averaging time by keeping the same error rate.

Acknowledgments

This research was financially supported by statutory project (Dzialalnosc Statutowa 2013), Faculty of Electronics, Telecommunications and Informatics, Gdansk University of Technology, Poland.

References

1. L. B. Kish, *Physics Letters A* **352**, 178 (2006).
2. L. B. Kish, *Metrology and Measurement Systems*, **20**, 191 (2013) DOI: 10.2478/mms-2013-0017.
3. C. H. Bennett, G. Brassard, S. Breidbart, S. Wiesner S. Quantum cryptography, or Unforgeable subway tokens. Advances in Cryptology, in *Proceedings of Crypto '82, Santa Barbara,* (Plenum Press, 1982), p. 267.
4. A. Kwiatkowski, M. Gnyba, J. Smulko, P. Wierzba, *Metrology and Measurement Systems*, **17**, 549 (2010).
5. J. Mroczka, D. Szczuczyński, *Metrology and Measurement Systems*, **16**, 333 (2009).
6. C. Kwan, G. Schmera, J. Smulko, L. B. Kish, P. Heszler, C. G. Granqvist, Sensors Journal, IEEE **8**, 706 (2008).
7. J. Smulko, Fluctuation and Noise Letters, **6**, R1 (2006).
8. Y. Saez, L. B. Kish, Errors and their mitigation at the Kirchhoff-law-Johnson-noise secure key exchange. arXiv preprint arXiv:1305.4787 (2013).
9. R. Mingesz, Z. Gingl Z, L. B. Kish, *Physics Letters A* **372**, 978 (2008).
10. J. S. Bendat, A. G. Piersol, *Random data analysis and measurement procedures*, (Measurement Science and Technology, 2000).
11. J. L. Rodgers, W. A. Nicewander. *The American Statistician*, **42**, 59 (1988).