UNIVERSITY OF SZEGED
FACULTY OF SCIENCE AND INFORMATICS
DEPARTMENT OF TECHNICAL INFORMATICS
Doctoral School of Computer Science

Measurement and secure communication protocols based on the analysis and exploitation of random fluctuations

Summary of the Ph.D. Thesis

Written by:
Gergely Vadai

Supervisor:
Dr. Zoltán Gingl
Professor, Head of Department

SZEGED
2018

1 Introduction

The paradigm shifts that have occured in the last century in natural sciences have affected our view of the natural laws' generality. While the complexity and unknown boundary conditions of equations describing deterministic correlations were traditionally identified as the reason for the unpredictability of events, quantum physics showed us that some processes can be described appropiately using randomness only.

Random signals – „noises" in the following – therefore aren't necessarily hindrances to be eliminated, they can carry information about the examined system. One can concider for example the acoustic noise of a car engine or boiling water. While in technical areas the noise spectrum of circuit components tell a lot about their reliability, heart rate fluctuations provide useful information about our health.

Noise can also play a constructive role – optimal functioning of some systems are made only possible by appropriate noise application. Good examples are the method of dithering used widely in microelectronics, image processing and telecommunication, or stochastic resonance – which received great attention in scientific circles. Such investigations and applications proved to be quite useful in various areas of numerous disciplines.

During my doctoral studies at the Noise Research Group I've had the opportunity to get involved in many different multidisciplinary research projects. In my dissertation I present my results in areas which are examples of utilising noises in a constructive role or as an information source. The thesis points summarizing these results are based on the publications [1-6] as listed in Table 1 of Section 4 while publications [7-9] are connected to them indirectly.

In noise research both the analytic description or modelling of processes and conclusions deduced from statistical analysis of experimental tests and measurement results take on a big role. The main results of my thesis confirm this well. For the theoretical proof and generalization of noise-based encryption protocols' security I've used the mathematical tools of statistics and probability theory. Detecting trends in fluctuations of kayak paddlers' movement signal however needed the appropriate measurement, processing, temporal and spectral analysis of signals and statistical evaluation of the metrics. Thus, my observations show both the usefulness of fluctuation analysis applied to a novel area and the effectiveness of the presented signal-to-noise ratio based method.

2 Unconditionally secure communication based on noise

Current cryptographic protocols' security is based on the assumption that the eavesdropper's (Eve) resources are insufficient to break them within a reasonable amount of time with the currently known methods. This is called conditional security which makes the current protocols breakable with time and technological advancement – just like it has happened with numerous older methods which are obsolete today.

A cryptographic protocol is said to be unconditionally secure from an information theory standpoint when Eve cannot derive any information about the plain text (apart from its length) – even in infinite time and with limitless computational resources. This is only possible with the key – which the encryption is based on and is considered critical information – being only used once, being completely random while being at least as long as the data to be encrypted [10]. This is called One-Time Pad (OTP).

Thus, the key has to be previously agreed on between the parties or it should be securely exchanged, which brings us back to the original cryptographic problem. One possible solution to this problem is the use of key exchange (or key generating) protocols. The goal with these protocols instead of securely sharing previously prepared key bit sequences is the joint generation of the key bit sequences during the communication through the measurement of a physical quantity which Eve cannot determine without revealing that the channel is compromised. Examples for these protocols are Quantum Key Distribution (QKD) [11] and the noise-based secure communication introduced by László Béla Kish in 2005 [12], the Kirchhoff-Law-Johnson-Noise (KLJN) key exchange protocol examined below.

The KLJN key exchange system

The KLJN protocol can provide unconditionally secure communication in an elegant and surprisingly simple way by utilizing the thermal noise of resistors. Moreover, the security of the protocol is merely based on the laws of classical physics [12]. The system consisting only of a few electronic components is simple, much less expensive (by a few orders of magnitude) and robust – therefore it becomes a promising alternative to quantum cryptography.

In the KLJN system shown in Figure 1, the the two communicating parties, Alice and Bob have an identical pair of resistors (R_L, R_H, $R_L \neq R_H$). They are randomly connecting one of the resistors to the interconnecting wire on which Eve can measure the current ($I_E(t)$) and the voltage ($V_E(t)$) comes from the thermal noise of the resistors. The four possible states of the system are represented – taking Alice and Bob's switches in order – as follows: LL LH, HL, HH.

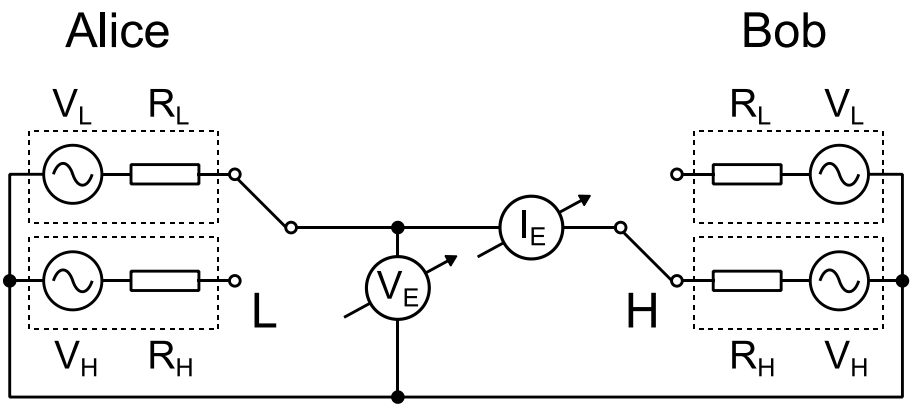

Figure 1: Model of KLJN system using noise generators (LH state is shown).

Due to the thermal noise of the resistors – represented by separate voltage generators in the figure – the mean value of the current and voltage noises are zero: $<I_E(t)>=0$ and $<V_E(t)>=0$. The power spectral densities and proportional variances – which can be calculated from the Kirchhoff-law – are equal in a thermal equilibrium in LH and HL states. Eve cannot differentiate between the two states due to in the case of normal distribution the expected value and the standar deviation defining the measurable current and voltage noises perfectly. Thus, Eve cannot deduce which of the two sides has chosen the high or low value resistors. In contrast, Alice and Bob can tell the state of the other parties switch knowing the state of their own, thus one bit of information can be securely exchanged in LH and HL states.

The classical physical proof of this systems' unconditional security is based on the second law of thermodynamics; in thermal equilibrium there is no energy flow between the two parties, thus information cannot be extracted about the state of the system. Because there is no energy flow, the $P=<V_E(t)I_E(t)>$ power on the cable, i.e. the correlation of $I_E(t)$ and $V_E(t)$ becomes zero [12, 13].

At room temperature the effective value of the current and voltage signals are extremely small. With the use of artificial voltage generators however the appropriate signal strength can be achieved which corresponds to extremely high (10^9 K) „virtual" temperatures. Ensuring the security of the system requires maintaining the mentioned equivalent temperatures on both sides. This can be achieved when the variance of the voltage noise for L and H states generated by the independent noise generators proportional to the appropriate resistance values.

During the key exchange Alice and Bob choose resistors randomly for every single bit. Afterwards the bits for HH and LL states – i.e. half of the cases – are deleted from the key. Alice and Bob can then coordinate the index of bits to be deleted and share the results of their measurements on a public authenticated channel to prevent active attacks. Next, they can encrypt the information using OTP and share with each other using the same channel. According to Kerckhoff's principle Eve can possess all information about the system – including the value of the resistor pairs

and effective value of the noise generators – because the unconditional security of the system is guaranteed by the fact that she cannot differentiate between LH and HL states.

The ideal KLJN key exchange system – in stationary case – is considered to be unconditionally secure; however numerous attacks have been introduced using the non-ideal properties that appear in practical realizations. The resistance of the interconnecting wires, different temperature of the parties, tolerance of resistor values can cause information leak, i.e. Eve can determine the value of the key bit with a probability greater than 50% (randomly guessing the value of the bits). The outstanding performance and the security of the KLJN system has been demonstrated by the first practical realization in Szeged [14] and has inspired the development of another secret key exchange method and further protocols. The simplicity and flexibility of the system motivated the proposal of many possible applications in different environments.

Requirements of noise properties for unconditional security

Zoltán Gingl and Róbert Mingesz used an opposite approach to the previous investigations; instead of examining the thermal noise based system's security they were investigating what noise properties are required for unconditional security in case of artificial noise generators merely with the tools of mathematical statistics [15]. Based on their results the *necessary* condition for security is a stable noise distribution – with only the variance of the normal distribution function being finite – furthermore the variance of noises have to fulfill the following relationship:

$$\frac{\left\langle V_{\mathrm{H}}^2(t)\right\rangle}{\left\langle V_{\mathrm{L}}^2(t)\right\rangle}=\frac{R_{\mathrm{H}}}{R_{\mathrm{L}}}. \qquad (1)$$

These two conditions are in agreement with the criterion from the classical physical approach. However, the need might arise to prove mathematically – similarly to the Kish's original proof based on thermodynamics – that there are sufficient conditions for the system's unconditional security.

Since Eve can only measure $V_{\mathrm{E}}(t)$ és $I_{\mathrm{E}}(t)$ the unconditional security of the system requires that the two quantities' statistical parameters and their joint distribution are equal in LH and HL states. Using the probability density functions of the random variables representing the quantitites ($p(I_{\mathrm{E}})$ és $p(V_{\mathrm{E}})$) and their joint probability density function ($h(I_{\mathrm{E}},V_{\mathrm{E}})$) the communication is unconditionally secure, if:

1. $p_{\mathrm{LH}}(I_{\mathrm{E}})=p_{\mathrm{HL}}(I_{\mathrm{E}})$,
2. $p_{\mathrm{LH}}(V_{\mathrm{E}})=p_{\mathrm{HL}}(V_{\mathrm{E}})$,
3. $h_{\mathrm{LH}}(I_{\mathrm{E}},V_{\mathrm{E}})=h_{\mathrm{HL}}(I_{\mathrm{E}},V_{\mathrm{E}})$.

The first two conditions are met with normally distributed noises scaled by relationship Eq. (1). To examine condition 3. I have first carried out numerical simulations in LabVIEW enviroment. I have analyzed the transmission of a single bit, i.e. an LH or HL state to investigate the joint statistics on a scatter plot with random number sequences of length 2^{13} [1]; which is significantly more data than needed for practical implementations. In the case of normal distribution, the scatter plot was only indistinguishable with scaling conforming to Eq. (1). In case of other stable distributions and uniform distribution, which is primarily occuring during pseudo-random number generation, the joint distribution of LH and HL states were distinguishable even with appropriate scaling. Consequently, in the case of probability distributions different from normal distribution, though the value of correlation and linear regression is zero with correct scaling, the two quantities are not independent; their regression function is nonlinear, which shows well the special role of normal distribution.

In our theoretical examination of security we used the fact that condition 3. is self-evidently assured if V_E and I_E are independent, which is consistent with the proof of Kish based on thermal equilibrium [13].

Based on this and using Lukacs and King's theorem for the linear combinations of independent variables published in 1954 [16], I showed that V_E and I_E are independent *if and only if* the voltage noises have normal distribution and the scaling condition given in Eq. (1) is met. In other words, these two conditions are the *necessary and sufficient* conditions for unconditional security. With this I have given a purely mathematical proof leaving out any classical physical considerations (but being consistent with those) for the KLJN protocol's unconditional security [1].

Generalization of the KLJN key exchange system

Linear combination of normal distribution voltage noises, i.e. V_E and I_E have normal distribution as well; which means that these are independent if their correlation is zero. I showed that an equal, nonzero correlation in LH and HL states is enough – since in case of normally distributed voltage noises the dependency of V_E and I_E is completely determined by their correlation – because this way Eve cannot differentiate between the two states [2]. Based on this the 3 conditions for unconditional security as defined above can be formulated assuming normal distribution as follows:

1. $\left\langle I^2_{E,LH}(t)\right\rangle = \left\langle I^2_{E,HL}(t)\right\rangle$,
2. $\left\langle V^2_{E,LH}(t)\right\rangle = \left\langle V^2_{E,HL}(t)\right\rangle$,
3. $\left\langle I_{E,LH}(t)V_{E,LH}(t)\right\rangle = \left\langle I_{E,HL}(t)V_{E,HL}(t)\right\rangle$.

Since in the case of the original setup, the correlation in LH and HL states was zero in case of noise parameters corresponding to the first two criterion, we have examined a more general system in which Alice and Bob are using two-two arbitrarily chosen resistors ($R_{LA} \neq R_{HA}$, $R_{LB} \neq R_{HB}$) as shown on Figure 2.

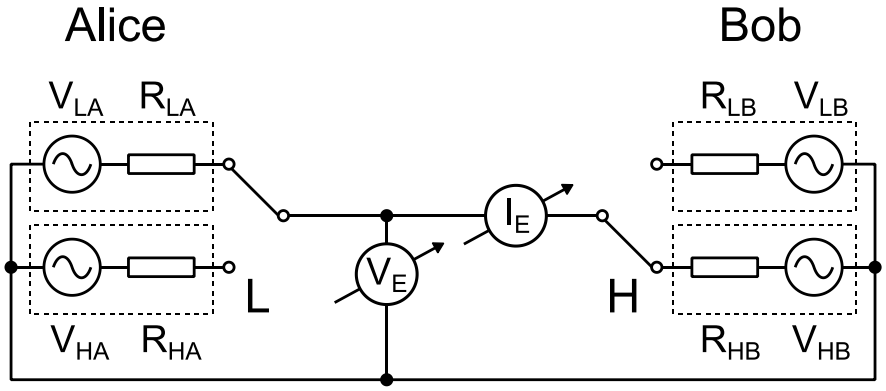

Figure 2: Model of the generalized KLJN system (in LH state) with four different resistors and noise generators with different effective values.

We can assign four random variables to the four noise generators whose linear combinations due to the Kirchoff-laws can be used to describe the measurable voltage and current on the communication cable in LH and HL states. Based on these the three criteria can be formulated as a function of the resistance values and noise generators' effective values. Solving the equation-system for the given four arbitrary resistance values and an arbitrary voltage noise variance, the variances of the other three voltage noises can be calculated to meet the conditions for unconditional security [2].

With this I have shown that the KLJN secure key exchange system provides security even under significantly generalized conditions. The resistor pairs used by the two parties don't have to be of equal value, the effective value of the noise generators can be selected that the eavesdropper won't be able to differentiate between LH and HL states in any way. I have confirmed this by numerical simulations as well; examining different asymmetrical setups for transfer of 10^6 bits, the variances of $V_E(t)$ and $I_E(t)$ were statistically indistinguishable. Studying Eve's bit error rate (BER) did not show any information leakage accordingly [2].

These results shed new light on the classical physical interpretation of the conditions for KLJN's unconditional security, since the generalized system is not in a thermal equilibrium. Furthermore, the correlation with a nonzero value means power flow between the two communicating parties. The original KLJN system in which there is no energy transfer is a special – symmetric – case of the generalized system. Based on these results Kish reinterpreted the classical physical description of the protocol's security using the fluctuation-dissipation theorem instead of the second law of thermodynamics additionally, moreover the results inspired him to introduce a new protocol [17].

The generalized system is a major step forward in the practical implementation of the protocol since the noise generators can be tune for any value of the components to provide perfect security for the communication.

Generalized KLJN secure key exchange system for practical applications

For practical applications of the KLJN system the main question is how the difference from idealized models during the realization of the system affects its security. Accordingly, a significant part of the attacks based on the non-ideality of the system. The nonzero cable resistance for example makes it possible for Eve to draw conclusions from the voltage drop or from the power flow on the cable. If Alice and Bob know Eve's point of measurement and the value of the cable resistance they can modify their noise generators to match the criterion for unconditional security based on our previous results. However, in a practical case Eve's measurement point (or points) cannot be known by the two parties, so the question arises: what can Alice and Bob do to maintain security?

To analyze the problem, we have complemented the system as shown on Figure 3 with the communication and reference cable' resistance on which Eve makes measurements on q_1 és q_2 relative observation points.

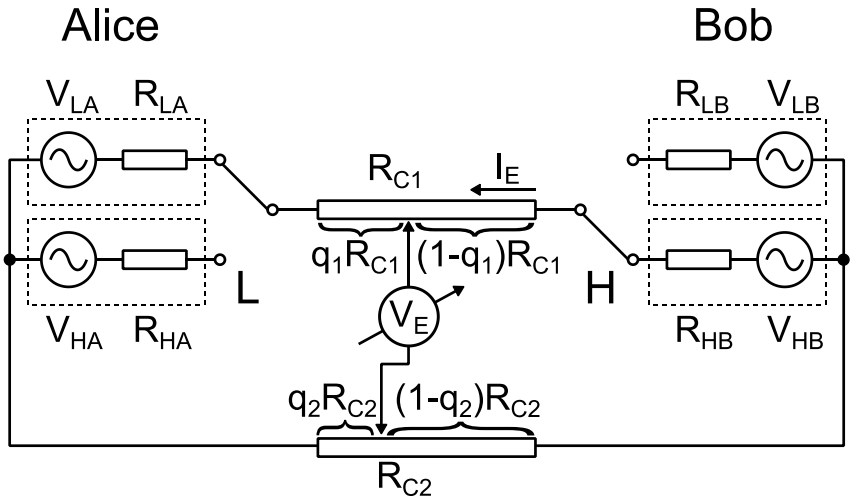

Figure 3: Model of the generalized KLJN system taking into account the communication cable's R_{C1} resistance, Eve's q_1 observation point, the reference cable's R_{C2} resistance and Eve's q_2 observation point in LH state.

I have used a similar method to determine the criterion for the unconditional security of the system complemented with the cable resistance to the one used for the generalized system [3]. I have formulated the three conditions required for unconditional security, i.e. the equivalence of variances and correlation of V_E and I_E in the function of the variance of the voltage noises, the components' resistance values and the observation point. I have then given the formulas needed to determine the three voltage noises' variances from the above values and one of the voltage noise variance by solving the equation-system [3]. These formulas do not

contain the observation point, which means that the security is maintained over the full length of the interconnecting cable, it doesn't matter where Eve's measurement point is. I have verified the unconditional security of the system by numerical simulations as well [3].

Based on the results the correlation of the voltage and current is different at different points of the cable, however it can be assured to be equivalent in LH and HL states. With this we have interpreted the independence of the compensation technique from the point of measurement given by Kish for the original system [18]; the correlation is still only zero in the middle of the wire, but the two states are still indistinguishable on any other points as well.

The results are especially important for practical applications, since using the original system the components required for implementation have caused information leakage, but these components are part of the new system which has unconditional security with an appropriate setting of the noise parameters, giving general protection from attacks in static case. For that only the exact values of the components have to be known.

The inaccuracy of these values will cause information leakage – the extent of which I have examined with numerical simulations [4]. Though the extent of the information leakage is dependent on the actual setup, the system proved to be quite sensitive to the accuracy of its components' values. On the other hand, it is more insensitive to the inaccuracy of the cable resistance by orders of magnitude.

Nonetheless, Alice and Bob can modify – even continuously – the effective value of their noise generators to eliminate information leakage. For this, only measuring the actual values of their communicators' components is needed, or conclusions can be drawn to compensate the errors from voltage and current values measured on the wire.

3 Fluctuation analysis of kayak paddlers' motion signals

While investigating periodic processes the fluctuations of the period or another quantity characterizing it can carry extra information; variability proved to be a useful diagnostic tool in case of periodically moving parts of mechanical machines or our heart's function [19]. Today numerous devices – for example smartphones, watches and actigraphs – are able to measure movement with inertial sensors which makes it possible to examine the steadiness of our gait or the rhythm of our daily activities.

Sensors of this type are commonly utilized in devices used to help professional kayak athletes and coaches, where the goal is the steady repetition of the optimal set of movements. The goal in our common project with the EDF DÉMÁSZ Szeged Water Sport Association was to develop a measurement system able to track the athletes' performance [9]. During my studies I have observed connection between the movement's steadiness and the technical skills of the athletes, so my focus

became to analyze the relationship between the period fluctuations and the quality of the paddling in detail.

Measurement and classification of the motion signals

The 3-axis acceleration and 3-axis angular velocity signals of the kayaks were measured by a special portable instrument developed in our laboratory with a sample rate of 1000 Hz – which is much higher than the commercial alternatives [9].

An athlete's current performance can be influenced by numerous factors, therefore, to ensure that the performances to be compared are recorded under the most similar circumstances possible, I have examined the first 10 minutes of long range (>5 km) training paddlings of 14 athletes with different age and technical skills.

I have analyzed the indicators as a function of the athletes' technical skills with the assumption that they were paddling with average performance and a technical implementation appropriate for their preparedness. For the quantitative description of this, I used the athletes' age and classification done by the trainer in the scale: 1-10.

The fluctuation-based indicators were calculated (both in the time and frequency domain) for a 30 second time window of the signals, of which 10 minute averages were used for the comparison.

Temporal and spectral fluctuation analysis of motion signals

The accurate spatial reconstruction of the motion is not possible from the measured signals thus we can gather information about the athletes' paddling by the detection of the motion signals' period and the study of their shape [20, 21]. The most important classical parameters characterising a paddling cycle are the *period*, the *stroke rate* calculated from the previous value and the *stroke impulse* specific of the pulling – calculated by integration of the positive part of the acceleration signal.

I have shown with statistical analysis of the quantities characterising the period of the paddling, that the degree of their fluctuation is connected to the athletes' technical skills, which is observable on Figure 4. The phenomenon is well described by the trend curves and the Poincaré plot representation of the quantities; the indicators of a beginner athlete are fluctuating much more than in the case of a professional athlete [5]. This fluctuation can be interpreted by the fact that steady paddling is required for the optimal movement of the kayak.

At the same time numerous questions arise about the determination of the standard deviation describing these fluctuations; should we normalize it with the mean of the quantities or does the trends in the changing of the quantities influence these values? These questions were examined by calculating the correlation between the different indicators and the technical level or the age of the athlete. Our studies were based on the periodicity of the kayak's motion, which period seems to

be a single paddling based on the forward axis acceleration signal, however the total period of the movement is combined from a right and a left hand paddling stroke because of the paddlings' asymmetry. This was confirmed by my results as well: all standard deviation based indicators were showing a stronger correlation between the quantities describing the two-handed time period and the technical level [6].

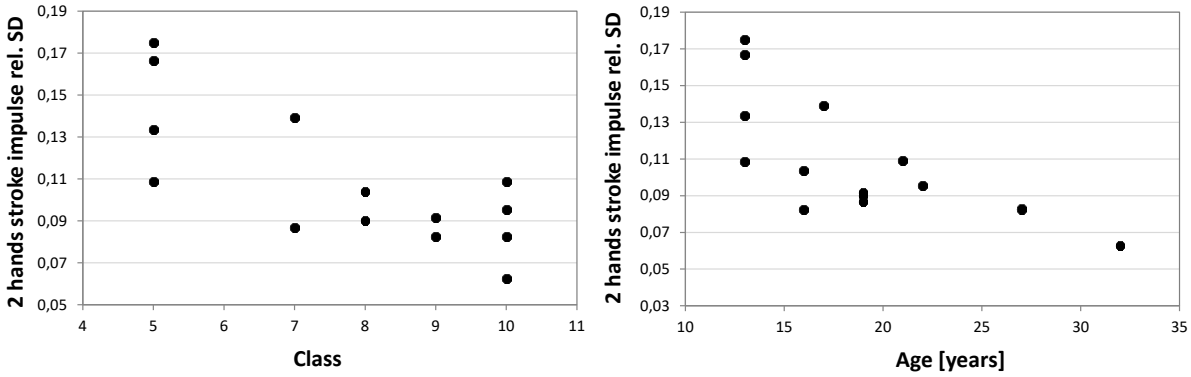

Figure 4: The relative standard deviation of the two-handed stroke impulse as a function of of the technical skill's classification (left) and the athlete's age (right).

The presented variability analysis requires the detection of the strokes which can be quite difficult case of complex signal shapes – for example when technical fault occures or at sprint race. I have examined if this information can be recovered from the raw signals without detecting the stroke periods, since this way the usage of the complex and computationally intensive detection algorithms could be eliminated, and our results would not be affected by their reliability and accuracy.

The steadiness of the motion can be analyzed in frequency-domain as well, because the periodic components of the movement can be separated from the other signal components using the frequency determined by the stroke period, and the ratio of their power can be characterized by the *signal-to-noise ratio* (*SNR*). A further advantage of the method is that we do not have to exclusively rely on the forward axis acceleration signal, we can calculate our indicators on all six motion signals.

The basic question for determining the spectral indicators based on the *SNR* is how we can separate the "signal" and the "noise". While defining the power of the periodic components, the identification of the fundamental frequency is not clear either in case of the determination of the peaks taken into account in the power spectral density. The period of the forward and vertical axis acceleration and the pitch axis angular velocity signals is seemingly independent of the hand in execution, in this case the the dominant frequency of the spectra is the first harmonic that belongs to the one hand stroke cycle, while the dominant frequency of the horizontal axis acceleration, the yaw and roll axis angular velocity belongs to the fundamental frequency identified by to the whole period of both hands strokes.

The shape of a single period of the motion signals determines the number of the harmonic peaks emerges significantly form the noise level in the power spectral

density, though its power – for example in case of a technical fault – does not belong to the optimal components of the motion exclusively. I have compared the signal and noise power and the *SNR* calculated by taking into account different numbers of harmonics using the coefficient of determination between these indicators and technical skills. Since the correct determination of the harmonic peak's power is not clear I have examined the effect of several similar numerical methods – fixed peak width or using estimated half-width, frequency dependent peak width and the use of Hanning- or rectangular spectral window – as well [6].

The connection between the *SNR* in case of the roll axis angular velocity and the athletes' age or technical skills can be observed well on Figure 5.

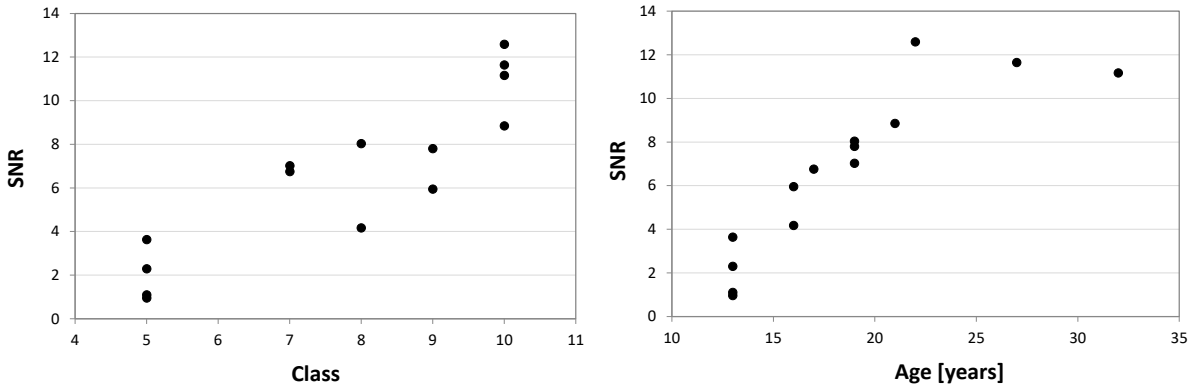

Figure 5: Signal-to-noise ratio (*SNR*) of roll axis angular velocity as a function of technical skills' classification (left) and of athletes age (right).

Based on these results the indicators calculated from the yaw and roll axis angular velocity signals showed the strongest correlation with the paddling quality, which means the paddling is better characterized by the two hands spectral indicators, as previously seen in the case of the temporal indicators [6].

This novel approach based on fluctuation analysis – which seems to be suitable for measuring quality of technique – raises interesting questions: what are the sources of these fluctuations, to what extent is the fluctuation dependent on the technique and the technical faults, external mechanical effects or the physical and mental state of the athlete? What further indicators could characterize the technical execution?

Examination of period fluctuations could be advantageous in case of analyzing other sports or periodic motions, performance estimation or diagnosing health parameters. The connection between temporal and spectral indicators characterizing the period fluctuations can be studied further with analytical and numerical methods as well. The indicators of spectral variability analysis based on *SNR* could be useful for numerous other periodic – e.g. physiological – signals because of the elimination peak detection in time domain, thus this approach is the subject of our current research.

4 Thesis statements

My new scientific results in the application of random fluctuations presented in the dissertation are summarized in the four thesis statements below. The supporting publications were referenced at the end of each statement. The first three points describe my results in the field of noise-based unconditionally secure communication. These were published in three international journal articles and an international conference article. The fourth point summarizes my results in evaluating kayak paddlers' performance by fluctuation analysis of the periodic motion signals, which were published in an international journal article (based on an invited talk) and an international conference article. The type of the supporting publications and their connection with the thesis statements are shown in Table 1.

Thesis state-ment	**Publications**					
	[1]	**[2]**	**[3]**	**[4]**	**[5]**	**[6]**
	Journal Q3 IF=0,811	Journal Q1 IF=5,228	Journal Q1 IF=3,244	Conference	Conference	Journal Q1 IF=2,196
1.	■					
2.		■				
3.			■	■		
4.					■	■

Table 1: The connection between the supporting publications and the thesis statements summarizing the new scientific results presented in the dissertation. In the case of journals, their impact factor and Web of Science ranking are also noted.

1. Proof of the noise requirements for unconditionally secure communication with the KLJN secure key exchange system

According to the earlier results of the KLJN protocol's examination with mathematical statistical tools the necessary conditions for unconditionally secure communication – in agreement with the results of the classical physical approach – are that noise generators produce normally distributed voltage noises whose variances are scaled with the ratio of the resistances. We have complemented the analysis with the examination of the joint probability distributions of the voltage and current noise measured by the eavesdropper. First, I demonstrated by numerical simulation of the system that the LH and HL states assigned to the 0 and 1 key bits are distinguishable making the exchange insecure in cases with the two above conditions unmet. Then I showed using the theorem regarding the independence of the linear combination of two independent random variables that the two requirements of the noise parameters are necessary and sufficient for the

unconditional security of the protocol. With this I have given the mathematical proof of the protocol's security without classical physical considerations. [1]

2. Generalization of the KLJN key exchange protocol

The original protocol requires the two communicating parties to use the same resistor pairs basing the security on the independence of the quantities measurable by the eavesdropper. I showed that the indistinguishability of the LH and HL states can be ensured with significantly less limitations. The independence of the current and voltage noises is not required, it is enough that their joint distributions are equal in the two cases. Based on this I showed that the condition for unconditional security in the case of normally distributed voltage noises is the equality of the variances and correlation of the measurable current and voltage noises in the LH and HL states. This can be accomplished with a much more general system in which the two parties are using two different sets of resistor pairs. I gave the formulas for the effective values of the noise generators based on the new criteria which make the generalized system unconditionally secure. I have verified these results by numerical simulations as well. The original KLJN system corresponds to the symmetrical case in which the two quantities measurable by the eavesdropper do not correlate, i.e. there is no power flow between the two parties, the system is in a thermal equilibrium. I showed by the generalization of the protocol that this condition is not necessary to achieve unconditional security. This resulted in the reinterpretation of the classical physical description of the KLJN protocol's security and the introduction of new protocols. The new key exchange protocol in which the two communicating parties' system does not have to be equivalent simplifies the hardware's realization and practical implementation greatly. [2]

3. Generalized KLJN key exchange for practical applications

We complemented the model of the generalized KLJN system with the communication wire's resistance on which the eavesdropper can make measurements at any position. I showed that the conditions guaranteeing the unconditional security (used in the 2. point) can be satisfied in this system as well. I gave the equations for the variance of the voltage noises, which show that the noise generators' required effective values do not depend on the observation point of the eavesdropper. The security is maintained over the full length of the interconnecting cable; the correlation of the voltage and current is different at different points of the cable, however it can be assured to be equivalent in LH and HL states. In the original system deviation from the ideal case – resistance of the wire and other components necessary for practical implementation – resulted in information leakage. In contrast these components are part of the new system in the ideal case as well which is unconditionally secure if the noise parameters are correctly set, providing general protection against attacks in static case. Therefore, this protocol, which is capable of completely detecting and compensating errors caused by components of real

physical systems even in real time, simplifies and facilitates the practical application of the method. I have verified the security of the system by numerical simulation as well. Furthermore, I investigated the extent of information leakage caused by the tolerance of the components used in the real physical implementation. [3, 4]

4. Performance estimation of kayak paddlers based on fluctuation analysis of movement signals

While analyzing the performance of kayak paddlers through the movement signals of the kayak I showed that the quality of the paddling is correlated to the fluctuations of the period and stroke impulse, which characterise the period of the motion. This means that indicators of that fluctuation – based on temporal variability or the signal-to-noise ratio calculated from the power spectra of the raw movement signals– could contain additional information.

I showed by plotting the temporal change of the classical parameters characterizing the period of the motion signals on trend curves and Poincaré plots that their fluctuations are connected to the technical skills of the athletes. For the examination of this connection I compared multiple indicators – based on the standard deviation of the stroke period and stroke impulse – and the numerical methods required for determining them. The strongest correlation was shown by the relative standard deviation of the stroke period's stroke impulse while paddlers were pulling with both hands.

I introduced a method based on the signal-to-noise ratio calculated from the power spectral density of the raw motion signals. The benefits of this method are that the peak detection in time domain can be eliminated, and that it allows the fluctuation analysis of the other acceleration and angular velocity signals besides the use of the forward axis acceleration signal. I compared different signal and noise separation methods and multiple numerical procedures for determining them for each of the six movement signals. There was a much stronger correlation in the case of the signals when the athletes were pulling with both hands.

A connection was shown between the technical skills and the period fluctuations based on the correlation of the indicators and the age and classification of the 14 paddlers with different age and different levels of training. Our results raise a number of interesting, open questions which could be the subject of further research. The approach could be applied to other periodic movements and the presented method of spectral variability analysis might also include new results for other periodic – eg. physiological – signals. [5, 6]

5 Publications on which the thesis is based

[1] R Mingesz, G Vadai, Z Gingl, What kind of noise guarantees security for the Kirchhoff-Law-Johnson-Noise key exchange? *FLUCTUATION AND NOISE LETTERS* 13:(3) Paper 1450021, 7 p. (2014)

[2] G Vadai, R Mingesz, Z Gingl, Generalized Kirchhoff-Law-Johnson-Noise (KLJN) secure key exchange system using arbitrary resistors. *SCIENTIFIC REPORTS* 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* 4: pp. 1141-1147 (2016)

[4] R Mingesz, N Bors, G Vadai, Z Gingl, Performance and security analysis of the generalized Kirchhoff-Law-Johnson-Noise key exchange protocol. *In Proceedings of 24th International Conference on Noise and Fluctuations (ICNF*) Vilnius, Lithuania, 2017.06.20-23. IEEE, pp. 200-203.

[5] G Vadai, Z Gingl, R Mingesz, G Makan, Performance estimation of kayak paddlers based on fluctuation analysis of movement signals*. In L Varani (ed.): Proceedings of 22nd International Conference on Noise and Fluctuations (ICNF)*, Montpellier, France, 2013.06.24-28. IEEE, Paper 6579010, 4 p.

[6] G Vadai, Z Gingl, Can the fluctuations of the motion be used to estimate performance of kayak paddlers? *JOURNAL OF STATISTICAL MECHANICS: THEORY AND EXPERIMENT* 2016: Paper 054040, 10 p. (2016), based on an invited talk presented at the 7th International Conference on Unsolved Problems on Noise, Barcelona, Spain, 2015.07.13-17.

6 Related publications

[7] R Mingesz, Z Gingl, G. Vadai, Security and performance analysis of the Kirchhoff-Law-Johnson-Noise (KLJN) secure key exchange protocol*. In Proceedings of 23rd International Conference on Noise and Fluctuations (ICNF)*, XI'An, China, 2015.06.2-5. IEEE, 4 p.

[8] LB Kish, Z Gingl, R Mingesz, G Vadai, J Smulko, CG Granqvist, Analysis of an Attenuator Artifact in an Experimental Attack by Gunn–Allison–Abbott Against the Kirchhoff-Law–Johnson-Noise (KLJN) Secure Key Exchange System. *FLUCTUATION AND NOISE LETTERS* 14:(1) Paper 1550011, 8 p. (2015)

[9] G Vadai, G Makan, Z Gingl, R Mingesz, J Mellár, T Szépe, A Csamangó, On-water measurement and analysis system for estimating kayak paddlers' performance. *In Proceedings of 36th Int. Conv., Microelectronics, Electronics and Electronic Technology*, Opatija, Croatia, 2013.05.20-24, IEEE, pp. 144-149.

7 References

[10] C Shannon, Communication Theory of Secrecy Systems. *BELL SYSTEM TECHNICAL JOURNAL* 28:(4) pp. 656–715 (1949)

[11] CH Bennett, G Brassard, Quantum cryptography: Public key distribution and coin tossing. *In Proceedings of IEEE Int. Conf. Computers, Systems, and Signal Processing* Bangalore, India, 1984, pp. 175–179.

[12] LB Kish, Totally secure classical communication utilizing Johnson(-like) noise and Kirchhoff's law. *PHYSICS LETTERS A*, 352:(3) pp. 178–182 (2006)

[13] LB Kish, CG Granqvist, On the security of the Kirchhoff-law–Johnson-noise (KLJN) communicator. *QUANTUM INFORMATION PROCESSING* 13:(10) pp. 2213–2219 (2014)

[14] R Mingesz, Z Gingl, LB 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:(7) pp. 978–984 (2008)

[15] Z Gingl, R Mingesz, Noise properties in the ideal Kirchhoff-Law-Johnson-noise secure communication system. *PLOS ONE* 9:(4) e96109 4 p. (2014)

[16] E Lukacs, EP King, A Property of Normal Distribution. *THE ANNALS OF MATHEMATICAL STATISTICS* 25 pp. 389–394 (1954)

[17] LB Kish, CG Granqvist, Random-resistor-random-temperature KLJN key exchange. *METROLOGY AND MEASUREMENT SYSTEMS* 23:(1) pp. 3-11 (2016)

[18] LB Kish, CG 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* 16:(10) pp. 5223–5231 (2014)

[19] U Rajendra Acharya, K Paul Joseph, N Kannathal, C Lim, JS Suri, Heart rate variability: a review. *MEDICAL AND BIOLOGICAL ENGINEERING AND COMPUTING* 44:(12) pp. 1031-1051 (2006)

[20] DA Aitken, RJ Neal, An on-water analysis system for quantifying stroke force characteristics during kayak events. *INTERNATIONAL JOURNAL OF SPORT BIOMECHANICS* 8:(2) pp. 165-173 (1992)

[21] Z Ma, J Zhang, Y Sun, T Mei, Sports Biomechanical Information Acquisition and Evaluation for Kayaking Events. *INTERNATIONAL JOURNAL OF INFORMATION ACQUISITION* 6:(3) pp. 213-223 (2009)