Making the eavesdropper's life harder

Gergely Vadai*
Department of Technical Informatics, Interdisciplinary Excellence Centre, University of Szeged
Szeged, H-6720, Hungary
vadaig@inf.u-szeged.hu

Laszlo B. Kish
Department of Electrical and Computer Engineering, Texas A&M University
TAMUS 3128, College Station, Texas, 77843-3128, USA
Laszlokish@tamu.edu

***Abstract* — The unconditionally (that is, information theoretically) secure Kirchhoff-law-Johnson-noise (KLJN) key exchanger operates with two pairs of resistors, one at Alice's side and another one at Bob's end. Whenever the cable resistance is not negligible, the original scheme leaks information to the eavesdropper (Eve). The typical way to reduce this leak is treating the exchanged key by privacy amplification. In the present work our goal is to reduce the leak earlier, during the bit exchange level. So far, the common belief has been that the resistance values in Alice's/Bob's pairs should be very different for an easy separation of the bit values to yield low bit error probability in the key exchange. However, such situation is helping Eve during all the currently known types of attacks owing to higher information leak. We explore the possibility of enhancing the security by narrowing the difference between the resistance values. The impact on security and the cost of reduced communication speed are demonstrated for the Bergou-Scheuer-Yariv attack.**

Keywords—information-theoretic security, KLJN key exchange, Bergou-Scheuer-Yariv attack, enhanced Johnson noise, unconditional security via wire channels

I. Introduction: The KLJN secure key exchange

The unconditionally (that is, information theoretically) secure Kirchhoff-law-Johnson-noise (KLJN) hardware key exchanger [1-16] operates with two pairs of resistors, one at Alice's side and another one at Bob's end, see Fig. 1. During the secure bit exchange operation, one of the resistors (R_L or R_H) are independently and randomly selected and connected to the wire by units A (Alice) and B (Bob), respectively. The noise generators represent either the Johnson noises of the resistors or external generators mimicking much higher effective noise temperature T_{eff}. In the secure state (mixed resistor index values, LH or HL at the two sides) passive measurements on the cable cannot identify the locations of the connected R_L and R_H however Alice and Bob know their own values thus, from passive noise measurements, they can calculate the value at the other end. For example, using the Johnson formula for the loop current

$$S_i(f) = \frac{4kT_{eff}}{R_L + R_H} \qquad (1)$$

yields the value of the loop resistance R_L+R_H from which Alice and Bob, who know their own connected resistance, can calculate the resistance value at the other side by subtraction.

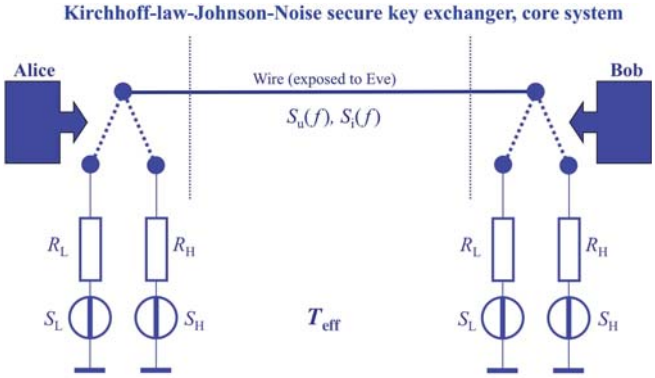

Fig. 1. The core KLJN scheme [1, 2]. The "thermal" noise voltage generators of the resistors R_L and R_H have power density spectra S_L and S_H, respectively, at effective temperature T_{eff}. Eve has access to the wire and can measure the noise voltage and current there and evaluate their power density spectrum $S_u(f)$ and $S_i(f)$, respectively.

II. Asymmetry based attacks

The asymmetry of the resistor values in the secure bit exchange (LH/HL) situations allows information leak to the eavesdropper (Eve). Such attacks have two major classes:

- Non-ideality based *passive attacks* [1]. When the system deviates from the core scheme, the security is not perfect with a passively listening (measuring) Eve. Examples are the non-zero wire resistance (Bergou-Scheuer-Yariv, BSchY) attack [9-11]; the temperature inaccuracy (Hao) attack [12]; cable capacitance attack [13]; transient attack [14]; etc. Making the difference greater between the R_L and R_H resistors increases not only Alice's and Bobs fidelity but also Eve's signal-to-noise-ratio and the information leak to her, provided the bit exchange duration (communication speed) is kept fixed.
- *Active attacks* [2] are present when Eve modifies the system. Relevant examples are the current injection attack [15]; the man-in-the-middle attack [16]; etc. The current injection attack is based on the distribution of currents injected into the wire and that will naturally increase Eve's signal-to-noise-ratio and information leak when the difference is greater between the R_L and R_H resistance values provided the bit exchange duration (communication speed) is kept fixed. On the other hand, the man-in-the-middle attack [16] is not utilizing these differences thus it is immune against the asymmetry of the resistors.

* Corresponding Author. On leave at the Electrical and Computer Engineering Department, Texas A&M University, January 18-31, 2019.

The typical ways to reduce the information leak, out of reducing non-idealities, are simulating the communication channel and Eve's attack, and then dropping high-risk bits [4, 15] (with a proper combination with other dropped bits), and/or treating the exchanged key by privacy amplification (hash functions). In the present work our goal is to reduce the leak also at an earlier stage, during the bit exchange level, by narrowing the difference between the resistance values, thus reducing the asymmetry. The cost, similarly to the above methods, is a reduced communication speed. The impact on security is demonstrated for the Bergou-Scheuer-Yariv cable resistance attack [9-11]. Note, for that attack, compensation techniques exist [e.g. 1,10,11] however they increase the vulnerability against several other attack types.

III. Impacts of Reducing the Resistance Difference

Reducing the resistance difference increases the *BEP* of Alice and Bob at a given communication speed. In the following, we show its impact on the communication speed while we keep the *BEP* at a fixed value, and we examine the effect on the information leak. Note, the communication speed is inversely proportional to the number of statistically independent measurement samples N during the exchange of a single bit.

A. The bit error probability of Alice and Bob

Alice and Bob must distinguish the insecure (HH and LL) and secure (HL and LH) bits. The parallel resultant resistance between the wire and the ground is $R_{HH} \equiv R_H / 2$ in the HH state and $R_{LL} \equiv R_L / 2$ in the LL state, and in the secure bit exchange situation it is

$$R_{\parallel} \equiv R_{HL/LH} = \frac{R_H R_L}{R_H + R_L}. \qquad (2)$$

The mean-square voltage and the current on the wire are proportional to the parallel resultant resistance between the wire and the ground. Alice and Bob measure the noise voltage and the current on the channel for a τ time window involving N statistically independent measurement points for the exchanged bit. They separate the secure and insecure bits by evaluating the mean-square voltage (and/or current) on the wire [1,2,7,8]. For the sake of simplicity, we examine the case of the noise voltage only.

The standard deviation of the mean-square voltage ΔHH of the HH state scales inversely with the root mean square of bit length [1,7]:

$$\Delta HH \propto \frac{1}{\sqrt{\tau}} \propto \frac{1}{\sqrt{N}}. \qquad (3)$$

For studying the impact of narrowing resistance difference, we fix the value of R_H – therefore R_{HH} is also fixed – and vary the value of R_L. The gap κ between $R_{\parallel}$ and R_{HH} is given as:

$$\kappa = \frac{R_H}{2} - R_{\parallel} = \frac{R_H^2 - R_L R_H}{2\left(R_L + R_H\right)}. \qquad (4)$$

The dependence of $R_{\parallel}$ and κ versus R_L are demonstrated in Fig 2.

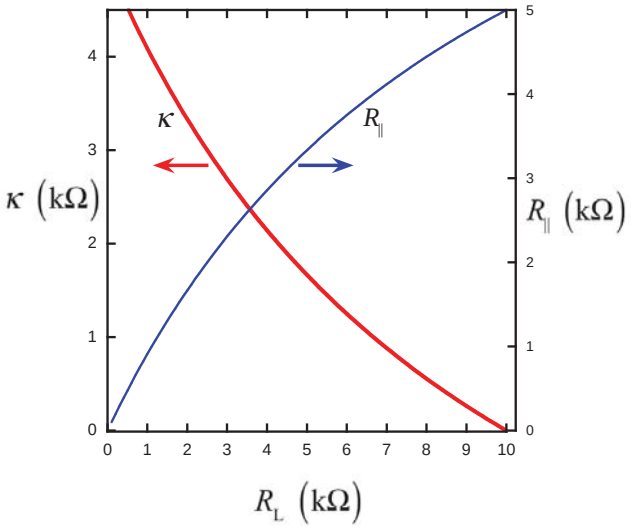

Fig. 2. The increase of loop resistance $R_{\parallel}$ defined by (2) and the decrease of the gap κ while the lower resistance value (R_L) value is approaching the resistance of the higher resistor value (R_H=10 kΩ).

For a given N, reducing the gap between R_L and R_H implies increasing *BEP* for Alice and Bob because, due to statistical errors, it makes harder to separate the mean square voltage values [1,7]. If we want to keep the *BEP* at a fixed value while κ is reduced, we must keep the ratio of ΔHH and the gap κ at a fixed value. From (3), N must be changed as:

$$N \propto \frac{1}{\kappa^2} \qquad (5)$$

In order to examine the *BEP* of the key exchange and the information leak we have carried out numerical simulations based on a code written in the LabVIEW environment. In the analyzed system, R_H was 10 kΩ, the rms voltage of the related external noise generator was 1 V and the resistance of the cable was 200 Ω. We varied the value of R_L from 330 Ω to 9 kΩ, while the rms voltage followed the Johnson formula [1].

The exchange of 50000 secure bits was simulated for each value of R_L. The value of N was 30 for the lowest R_L and it had been increased by following (5), see Fig. 3.

Fig. 4 shows that – in accordance with our goal – the ratio of ΔHH and κ remains constant; therefore the *BEP* of Alice and Bob remains the same for every value of R_L.

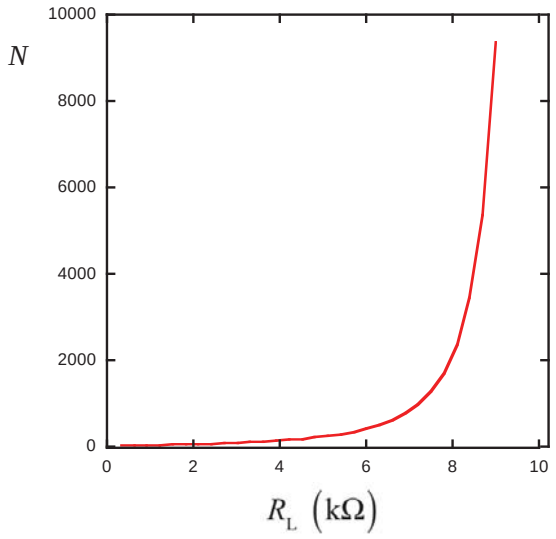

Fig. 3. Required number of independent samples N for a single secure bit exchange for a steady *BEP* value for Alice and Bob, see (5). The lower resistance (R_L) value is approaching the resistance of the other resistor ($R_H = 10\text{k}\Omega$).

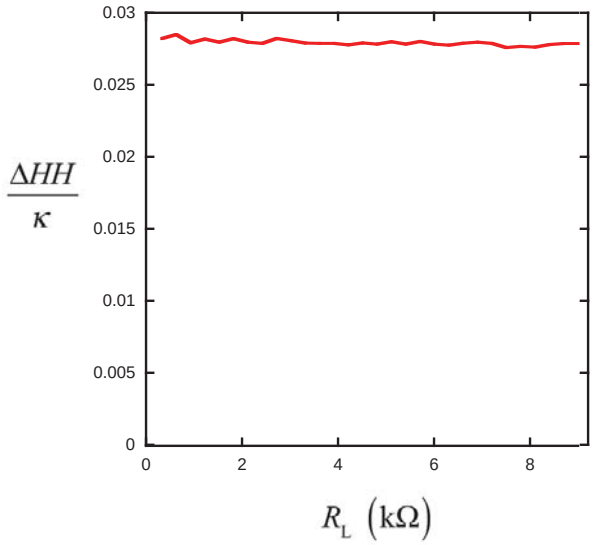

Fig. 4. The ratio of ΔHH and κ while the lower resistance (R_L) value is approaching the resistance of the other resistor ($R_H = 10\text{k}\Omega$) and N has been following (5) as shown Fig. 3. The wire resistance was 200 Ω.

B. Information leak during the BSchY attack

We examined the information leak caused by the non-zero wire for the Bergou-Scheuer-Yariv attack [1,9,10]. Note, at known other cable resistance based attacks (such as 10) Eve's *BEP* is proportional to the *BEP* in the present work.

As it is shown in Fig. 5, our new tool is favorable for Alice and Bob: while their *BEP* remains the same, Eve's *BEP* of her eavesdropping on the bit exchange is dramatically increasing and it is approaching the limit of 0.5, the limit of zero information entropy.

The obvious cost of the reduced information leak is the reduced communication speed, which is significant in the case of small difference between the resistances. However, the *BEP* of Eve is saturating when the relative resistance gap is small. For example at $R_L = 6\text{k}\Omega$ her *BEP* is nearly as large as at $R_L = 9\text{k}\Omega$, see Fig. 5, but the speed is much higher in the former case, see Fig. 3.

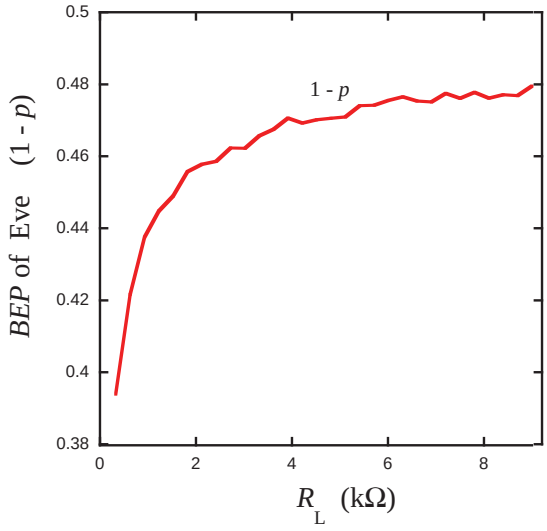

Fig. 5. Eve's bit error probability (=1-p where p is the probability of successful guessing of the bit value) while the lower resistance (R_L) value is approaching the resistance of the other resistor ($R_H = 10\text{k}\Omega$). Compare with N increase in Fig. 3. The wire resistance was 200 Ω.

IV. Conclusion

We have pointed out that reducing the gap between the resistor values in the KLJN secure key exchange protocol reduces Eve's signal-to-noise-ratio and the information leak during various types of attacks. We demonstrated this claim with the BSchY wire resistance attack where we could significantly reduce Eve's information. The price of the methods is slowdown. In practical situations, the gain and price of this method should be compared with that of the privacy amplification and the discarding of high-risk bits.

Acknowledgment

The research was carried out during GV's visit of Texas A&M University (January 18-31, 2019). The costs of the visit were covered by Ministry of Human Capacities, Hungary grant 20391-3/2018/FEKUSTRAT (University of Szeged) and the T3 grant scheme (2019) of Texas A&M University.

References

[1] L.B. Kish, The Kish Cypher. The Story of KLJN for Unconditional Security. World Scientific, 2017.

[2] L.B. Kish, "Totally Secure Classical Communication Utilizing Johnson (-Like) Noise and Kirchhoff's Law," Physics Letters A vol. 352, pp. 178-82, 2006.

[3] L.B. Kish, "Enhanced secure key exchange systems based on the Johnson-noise scheme," Metrology and Measurement Systems vol. 20, pp. 191–204, 2013.

[4] 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.

[5] G. Vadai, Z. Gingl, R. Mingesz, "Generalized Kirchhoff-law–Johnson-noise (KLJN) secure key exchange system using arbitrary resistors," Sci. Rep. vol. 2015, 13653, 2015.

[6] L.B. Kish, C.G. Granqvist. "Random-resistor–random-temperature Kirchhoff-law-Johnson-noise (RRRT-KLJN) key exchange." Metrology and Measurement Systems vol. 23, pp. 3-11, 2016.

[7] Y. Saez, L.B. Kish, "Errors and their mitigation at the Kirchhoff-law-Johnson-noise secure key exchange," PLoS ONE vol. 8, e81103, 2013.

[8] R. Mingesz, N. Bors, G. Vadai and Z. Gingl, "Performance and security analysis of the generalized Kirchhoff-Law-Johnson-Noise key exchange protocol," International Conference on Noise and Fluctuations (ICNF), Vilnius, 2017.

[9] L.B. Kish, J. Scheuer, "Noise in the Wire: The Real Impact of Wire Resistance for the Johnson (-Like) Noise Based Secure Communicator," Physics Letters A vol. 374, pp. 2140-42, 2010.

[10] 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 vol. 16, 5223-5231, 2014.

[11] 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.

[12] L.B. Kish, "Response to Feng Hao's paper "Kish's key exchange scheme is insecure"". Fluct. Noise Lett. vol. 6, pp. C37-C41, 2006.

[13] H.P. Chen, E. Gonzalez, Y. Saez, L.B. Kish. "Cable Capacitance Attack against the KLJN Secure Key Exchange." Information vol. 6: pp. 719-732, 2015.

[14] L.B. Kish, C.G. Granqvist, "Comments on "A New Transient Attack on the Kish Key Distribution System"". Metrology and Measurement Systems vol. 23, 321–331, 2016.

[15] H.P. Chen, M. Mohammad, L.B. Kish. "Current Injection Attack against the KLJN Secure Key Exchange," Metrology and Measurement Systems vol. 23, pp. 173-81, (2016).

[16] L.B. Kish, "Protection against the Man-in-the-Middle-Attack for the Kirchhoff-Loop-Johnson (-Like)-Noise Cipher and Expansion by Voltage-Based Security." Fluct. Noise Lett. vol. 6, L57-L63, 2006.