PAN POLSKA AKADEMIA NAUK

METROLOGY AND MEASUREMENT SYSTEMS

Index 330930, ISSN 0860-8229

www.metrology.pg.gda.pl

M&MS

THE PROBLEM OF INFORMATION LEAK DUE TO PARASITIC LOOP CURRENTS AND VOLTAGES IN THE KLJN SECURE KEY EXCHANGE SCHEME

Mutaz Y. Melhem, Laszlo B. Kish

Texas A&M University, Department of Electrical and Computer Engineering, College Station, TX 77843-3128, USA
(✉ *yar111@tamu.edu, Laszlokish@tamu.edu,* +1 979 847 9071)

Abstract

The Kirchhoff-law-Johnson-noise (KLJN) secure key exchange scheme offers unconditional security, however it can approach the perfect security limit only in the case when the practical system's parameters approach the ideal behavior of its core circuitry. In the case of non-ideal features, non-zero information leak is present. The study of such leaks is important for a proper design of practical KLJN systems and their privacy amplifications in order to eliminate these problems.

Keywords: unconditional security; key exchange; parasitic loop currents and voltages; information leak.

The *Kirchhoff-law-Johnson-noise* (KLJN) secure key exchange system offers unconditional (information-theoretic) security [1–13].

The core system is shown in Fig. 1. The key exchange protocol of a single secure bit is as follows: Alice and Bob randomly pick one of their resistors (R_L or R_H), connect it to the wire channel, and keep them there during the bit exchange period while they execute passive voltage and/or current measurements to learn the resistor value at the other end. We can present 4 different situations of the connected resistors (R_L and/or R_H) at Alice's and Bob's ends by the indices of the connected resistors, LL, LH, HL, and HH, respectively. These 4 situations correspond to 3 different noise levels (current and/or voltage) in the wire. The LL and HH levels are different but the LH and HL situations produce the same noise intensity [3]. Thus, these are secure levels because the eavesdropper cannot distinguish the HL from LH situation, while Alice and Bob can do it, since they know their own connected resistor value. In the LL and the HH cases (this happens in 50% of the bit exchange attempts), the results are discarded because then the result is publicly known.

Non-ideal (parasitic) features in a practical system change this circuitry and cause information leak. Even though the information leak can be reduced by privacy amplification [13], it is desirable to optimize the system as much as possible, because privacy amplification is reducing the speed of key exchange.

One of the most important and least explored classes of possible information leaks in long-range practical applications is the existence of parasitic current/voltage components in the wire

Article history: received on Nov. 21, 2018; accepted on Dec. 29, 2018; available online on Mar. 29, 2019; DOI: 10.24425/mms.2019.126335.

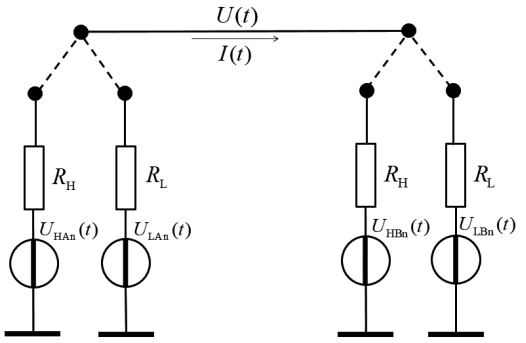

Fig. 1. The core of the KLJN key generation and exchange system. $U_{\mathrm{HAn}}(t)$, $U_{\mathrm{LAn}}(t)$, $U_{\mathrm{HBn}}(t)$, and $U_{\mathrm{LBn}}(t)$, are the (thermal) noise voltage generators for the related resistances. $U(t)$ and $I(t)$ are the measured noise voltage and the current in the wire. The resistors at Alice's and Bob's sides are randomly chosen and connected at the beginning of the bit exchange period.

connection. A special situation of a parasitic DC loop voltage mentioned (but not explored) in [14] is that, in the case of a *significant wire resistance*, the secure levels can split at Alice's vs. Bob's end, see Fig. 2.

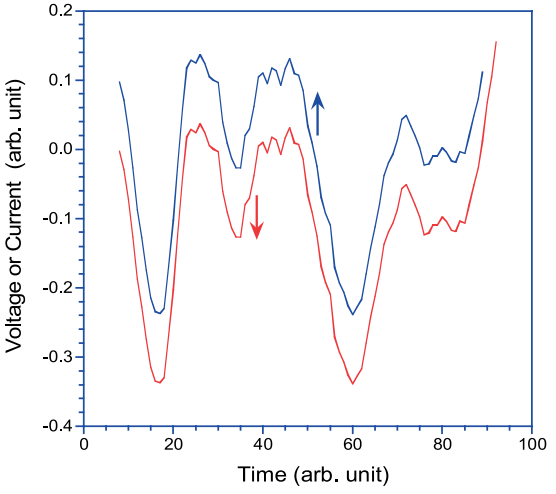

Fig. 2. A computer-generated illustration [14] of how a DC shift can split two strongly correlated noises and enables their easy comparison at a given moment. The arrows indicate the directions of shift.

In another work [15], it is shown that a parasitic DC loop voltage can cause significant information leak *even at zero wire resistance*.

However, the above mentioned considerations are very introductory and large body situations involving *Unsolved Problems of Noise* emerge, such as:

- Addressing the various ground loop problems, including one or more parasitic sources at various points along the line/loop.
- How to treat loop currents induced by external magnetic fields?

– What is the impact of attacks using periodic time function components with unknown frequency in the loop?
– A related question is if we can avoid the problems by using coax cables or twisted pairs (these are relatively robust against external magnetic fields) and how to handle the loss of economical advantages of grounding and single wire connection?
– How to defend the system against spurious currents/voltages at high frequencies: how efficiently can line filters prohibit information leak, or rather can they do contribute to it?
– The problem of stochastic loop currents/voltages in arbitrary frequency ranges and locations.

In conclusion, for the practical installation of KLJN systems, especially for significant communication ranges, the general and multi-faceted problems of loop currents and voltages (built-in and induced) must be clarified. After the installation of the system, it must be inspected for potential information leaks. After the optimization, a proper privacy amplification scheme must be set up. All these tasks pose as Unsolved Problems of Noise at the moment.

References

[1] Kish, L.B. (2017). *The Kish Cypher- The story of KLJN for unconditional security*. World Scientific.

[2] Kish, L.B., Granqvist, C.G. (2014). On the security of the Kirchhoff-law–Johnson-noise (KLJN) communicator. *Quant. Inform. Proc.*, 13, 2213–2219.

[3] Kish, L.B. (2006). Totally secure classical communication utilizing Johnson(-like) noise and Kirchhoff's law. *Phys. Lett. A*, 352, 178–182.

[4] Mingesz, R., Kish, L.B., Gingl, Z. (2008). Johnson(-like)-noise–Kirchhoff-loop based secure classical communicator characteristics, for ranges of two to two thousand kilometers, via model-line. *Phys. Lett. A*, 372, 978–984.

[5] Kish, L.B., Abbott D., Granqvist C.G. (2013). Critical analysis of the Bennett-Riedel attack on secure cryptographic key distributions via the Kirchhoff-law-Johnson-noise scheme. *PLoS ONE* 8:e81810/1–e81810/15.

[6] Smulko, J. (2014). Performance analysis of the "intelligent" Kirchhoff's-law-Johnson-noise secure key exchange. *Fluct. Noise Lett.*, 13, 1450024.

[7] Gingl, Z., Mingesz R. (2014). Noise properties in the ideal Kirchhoff-law-Johnson-noise secure communication system. *PLoS ONE* 9:e96109/1–e96109/4.

[8] Mingesz, R., Vadai G., Gingl Z. (2014). What kind of noise guarantees security for the Kirchhoff-loop-Johnson-noise key exchange? *Fluct. Noise Lett.*, 13, 1450021.

[9] Vadai, G., Gingl, Z., Mingesz, R. (2014). Generalized attack protection in the Kirchhoff-law-Johnson-noise secure key exchanger. *IEEE Access*, 4(1).

[10] Mingesz, R., Kish, L.B., Gingl Z., Granqvist, C.G., Wen H., Peper, F., Eubanks, T., Schmera, G. (2013). Unconditional security by the laws of classical physics. *Metrol. Meas. Syst.*, 20(3), 16.

[11] Kish, L.B. (2013). Enhanced secure key exchange systems based on the Johnson-noise scheme. *Metrol. Meas. Syst.*, 20(2), 191–204.

[12] Kish, L.B., Horvath, T. (2009). Notes on recent approaches concerning the Kirchhoff-law–Johnson-noise-based secure key exchange. *Phys. Lett. A*, 373, 2858–2868.

[13] Horvath, T., Kish, L.B., Scheuer, J. (2011). Effective privacy amplification for secure classical communications. *EPL* 94:28002/1–28002/6.

[14] Chen, H.P., Kish, L.B., Granqvist, C.G. (2014). On the "Cracking" Scheme in the Paper "A Directional Coupler Attack Against the Kish Key Distribution System" by Gunn, Allison and Abbott. *Metrol. Meas. Syst*., 21(4), 389–400.

[15] Melhem, M.Y., Kish, L.B. (2018). A Static-Loop-Current Attack against the KLJN Secure Key Exchange System. arXiv:1806.05596

Journal version of the paper presented at the 8th International Conference on Unsolved Problems of Noise (UPoN-2018, chaired by Janusz Smulko), Gdańsk, Poland, 9–13 July 2018. The meeting was dedicated to the 70th birthday of Michael F. Shlesinger.