Unconditional security in practical Kirchhoff-law–Johnson-noise key exchangers

Barry Chen [1], Laszlo B. Kish [1], Claes G. Granqvist [2], Robert Mingesz [3], and Zoltan Gingl [3]
[1] *Department of Electrical and Computer Engineering, Texas A&M University, College Station, TX 77843-3128, USA*
e-mail address: barrychen@tamu.edu ; Laszlokish@tamu.edu
[2] *Department of Engineering Sciences, The Ångström Laboratory, Uppsala University, P. O. Box 534, SE-75121 Uppsala, Sweden*
e-mail address: Claes-Goran.Granqvist@angstrom.uu.se
[3] *Department of Technical Informatics, University of Szeged, Szeged-6720, Hungary*
e-mail address: mingesz@inf.u-szeged.hu ; gingl@inf.u-szeged.hu

In physical secure key exchangers, the mathematical definition of the unconditional security [1] of the distributed keys is that the probability p of successfully guessing the bit by Eve can arbitrarily approach the value 0.5 when enough resources are available to Alice and Bob. One should note that this definition supposes a technically unlimited Eve, which means that the speed and accuracy of Eve's measurements are curtailed only by the laws of physics and by rules of the protocol. For example, while Eve's technical skills are unlimited she still cannot violate the *Second Law of Thermodynamics* or the *Quantum No-Cloning Theorem*, and she cannot record a *longer* sample of the signal than its *actual cut-off length* set by the protocol of Alice and Bob, who are in control of gating the signal. Similarly, Eve cannot utilize higher bandwidth with non-zero frequency components than the actual bandwidth set by Alice and Bob. Alternative definitions of unconditional security are based on statistical distance measures [2,3] between the shared keys and ideal, perfectly secure keys, but these definitions are equivalent with the above one when the key bits are *identical, independently distributed* random variables [1].

Whereas the unconditional security of practical quantum key distribution (QKD) systems is still debated [2–4], the classical physical Kirchhoff-law–Johnson-noise (KLJN) key exchange scheme [1,5–24] (Figure 1) has a general security proof [1] that is valid even for practical, weakly non-ideal situations.

The unconditional security [1] against *passive* attacks in the *ideal* KLJN scheme is founded on the Second Law of Thermodynamics [1,5–8], Kirchhoff's Loop Law and the statistical properties of Gaussian noise [1,4,6,10,11]. For *active* (invasive) attacks [1,5,6,9], however, an additional law is required: the information limit posed by *Nyquist's Sampling Theorem* for signals with finite length and bandwidth [1,5,6,9]. For the practical cases with weak non-ideality, an additional, fundamental rule applies to offer unconditional security, namely, the continuity of classical physical functions in linear systems and in stable non-linear systems [1]. As an example, will also show a new (capacitance) attack type with the so far highest success rate and the defense against it.

Important practical applications of KLJN [12–15], impose the less fundamental but still essential question:

How much would it take in terms of resources to reach a prescribed (outstanding) security level?

Various ways have been proposed to reduce *practical* information leaks based on non-ideal components [7,8], and the extraordinarily small [16,17] bit-error probabilities (after error removal) in the KLJN scheme allow plenty of privacy amplification [18] to further diminish the information leak under laboratory conditions [20] to imperceptible levels. Still, important attack types have not been analyzed for practical conditions, such as:

(*i*) *information leak due to propagation delays in steady-state conditions,* and

(*ii*) *information leak due to propagation delays at transients.*

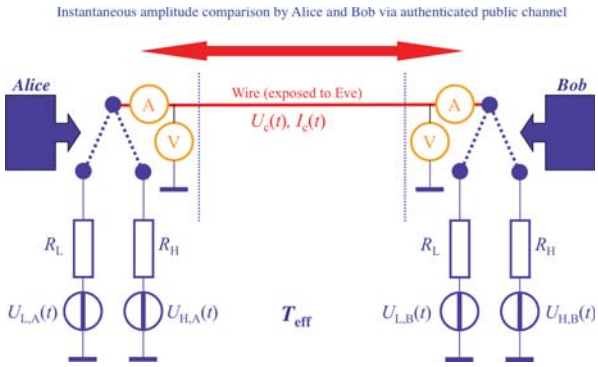

Figure 1. Schematic of the Kirchhoff-law–Johnson-noise (KLJN) secure key exchange system. At the beginning of the key exchange, Alice and Bob make a random choice from the resistors representing the two bit-values and connect the selected one to the wire. Then they execute passive and public current/voltage noise measurements on the cable and, based on these data, they determine the total loop resistance from the Johnson formula. The unknown resistance at the other end of the cable is then the difference between their own resistor and the total loop resistance. Eve does not know any of the connected resistor values; thus for her the loop resistance tells only if a secure bit exchange was performed (High/Low or Low/High situation). The High/High and Low/Low situations are not secure, and those bits are discarded. To defend against active and hacking attacks, the cable parameters and cable integrity are randomly monitored; the instantaneous voltage $U_c(t)$ and current $I_c(t)$ amplitudes in the cable are measured and compared via public authenticated data exchange, and full spectral and statistical analysis/checking is carried out by Alice and Bob. R, t and T_{eff} denote resistance, time and effective temperature, respectively. Line filters, *etc*., are not shown. The effective noise temperature of the generators is public knowledge and is very much higher than room temperature (800 million to 800 billion Kelvin during an experimental demonstration [20]).

Concerning item (*i*), Pao-Lo Liu, with a model-KLJN scheme [25], proved that, in the steady-state, even if propagating signal components were known in the two directions (by a directional coupler), the KLJN system would have remained perfectly secure. Gunn–Allison–Abbott (GAA) [21] recently tried to build a directional coupler for a new attack scheme by utilizing propagation effects during steady-state conditions, and their experiments seemed to demonstrate a huge information leak even under quasi-ideal conditions. However, subsequent careful studies clarified that the GAA scheme [21] was flawed at all levels [22–24]: fundamentally, conceptually and experimentally. Moreover,

provided that the KLJN system is implemented with care, GAA's scheme [21] actually yields less information leak than in an old cable-resistance attack [23]. Furthermore, and analogously to the old situation, even this small leak can completely be nullified by the protocol [8] eliminating wire resistance based attacks, which also indicates that the scheme is a wire loss based attack. Nevertheless the GAA attack and its analysis were beneficial by highlighting that security is a very serious matter and that a KLJN system, which is able to approach the security of idealized situations, requires very careful and thorough design even though its principle circuit looks relatively simple.

In conclusion, currently there is no successful attack against the KLJN scheme that is able to extract information from propagation effects under *steady-state* conditions.

Concerning item (*ii*), which considers *transient* effects, the situation is similar. Such effects should provide some information leak at the beginning and/or end of the key-exchange period. While a generic analysis shows [5] that unconditional security cannot be challenged by this kind of attack, it is essential to consider such attacks schemes in order to estimate the required resources in a practical KLJN design.

However, we have not yet seen any serious attack against even the most primitive transient protocol, such as ramping up/down the noise at the beginning/end of the measurement [20]. Such transient protection, when done in the simplest way [20], protects only against high-frequency reflections and its excessive information leak however it still leaks out about a single-point noise measurement information [25] , (which can easily be eliminated).

So far, the most elaborate transient defense protocol has embodied a simple random walk of resistance values and noise envelopes until they reach the desired values [7].

But there must be transient-based attacks on the KLJN scheme—at least intuition suggests that would extract information even in such a case. What are those schemes and what ways can they be eliminated?

These represent important unanswered questions which are open for future research.

[1] L.B. Kish, C.G. Granqvist, "On the security of the Kirchhoff-law–Johnson-noise (KLJN) Communicator", Quantum Inf. Process. **13**, 2213–2219 (2014).

[2] H.P. Yuen, "Essential lack of security proof in quantum key distribution", arXiv:1310.0842 (2013).

[3] O. Hirota, "Incompleteness and limit of quantum key distribution theory", arXiv:1208.2106 (2012).

[4] N. Jain, E. Anisimova, I. Khan, V. Makarov, C. Marquardt, G. Leuchs, "Trojan-horse attacks threaten the security of practical quantum cryptography", New J. Phys. **16**, 123030 (2014).

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

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

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

[8] 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 **16**, 5223–5231 (2014).

[9] 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. **6**, L57–L63 (2006).

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

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

[12] L.B. Kish, Ch. Kwan, "Physical uncloneable function hardware keys utilizing Kirchhoff-law–Johnson-noise secure key exchange and noise-based logic", Fluct. Noise Lett. **12** (2013) 1350018.

[13] L.B. Kish, O. Saidi, "Unconditionally secure computers, algorithms and hardware, such as memories, Fluct. Noise Lett. **8** (2008) L95–L98.

[14] E. Gonzalez, L.B. Kish, R. Balog, P. Enjeti, PLoS ONE **8** (2013) e70206.

[15] Y. Saez, X. Cao, L. B. Kish, G. Pesti, "Securing vehicle communication systems by the KLJN key exchange protocol", Fluct. Noise Lett. **13** (2014) 1450020.

[16] Y. Saez, L.B. Kish, R. Mingesz, Z. Gingl, C.G. Granqvist, "Current and voltage based bit errors and their combined mitigation for the Kirchhoff-law–Johnson-noise secure key exchange", J. Comput. Elect. **13**, 271–277 (2014).

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

[18] T. Horvath, L.B. Kish, J. Scheuer, "Effective privacy amplification for secure classical communications", EPL **94**, 28002 (2011).

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

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

[21] L.J. Gunn, A. Allison, D. Abbott, "A directional wave measurement attack against the Kish key distribution system", Sci. Reports **4**, 6461 (2014).

[22] H.P. Chen, L.B. Kish, C.G. Granqvist, G. Schmera, "Do electromagnetic waves exist in a short cable at low frequencies? What does physics say?" Fluct. Noise Lett. **13**, 1450016, (2014).

[23] H.P. Chen, L.B. Kish, C.G. Granqvist, G. Schmera, "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**, 389–400 (2014).

[24] L.B. Kish, Z. Gingl, R. Mingesz, G. Vadai, J. Smulko, C.G. 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", Fluct. Noise Lett. **14**, 1550011 (2015).

[25] P.L. Liu, "A key agreement protocol using band-limited random signals and feedback", IEEE J. Lightwave Tech. **27** (2009) 5230–5234.

[26] L. Gunn, A. Allison, D. Abbott, to be published.