Scholarpedia 8(8):31157, 2013.
DOI:10.4249/scholarpedia.31157

Secure communications using the KLJN scheme

Derek Abbott, University of Adelaide, Adelaide, SA, Australia

Gabor Schmera, Space and Naval Warfare Systems Center, San Diego, CA, USA

Introduction

Kirchhoff-Law-Johnson-Noise (KLJN) secure key distribution (Cho 2005),(Palmer 2007), (Kish 2006), (Mingesz 2013),(Kish 2009),(Mingesz 2008),(Kish 2006b), is a classical physical scheme that is a potential alternative to quantum key distribution. It is also sometimes loosely referred to as the *Kish cipher*, however, it is a hardware-based scheme for securely distributing cipher keys, and is not a cipher in itself.

The physical scheme, in its simplest idealized form, can be visualized as wire that connects two parties Alice and Bob that wish to secretly communicate. Both ends are terminated by a resistor. Both Alice and Bob randomly change each of their resistors between two values. By measuring the Johnson noise on the line, Alice can deduce Bob's resistor, and Bob can deduce Alice's resistor in a given switching cycle. This is achieved without either revealing their own resistor at each instant and thus an eavesdropper, Eve, is unable to decode the message. Eve only sees two resistors in parallel and cannot separate their values. It does not matter if the set of values of resistors is publicly known, what matters is that at a particular instant the binary choice Alice or Bob has made is unknown to Eve. The idea of measuring the resistances from the Johnson noise, via a spectrum analyser, rather than using a resistance meter is to avoid the situation where current is injected by the resistance meter thereby providing a security weakness. The spectrum analyser is entirely passive.

The security is a consequence of thermodynamic equilibrium, and hence the Second Law of Thermodynamics, as will be later discussed in further detail. The following protocols are adopted to maintain security:

a) Only random sequences of bits are exchanged rather than actual messages. These random bits can be used as a one-time pad or a secure key for the actual message that can then be securely sent via a conventional public telecommunications channel.

b) If Alice's two resistors represent 0 and 1 and Bob's resistors represent 0 and 1, then there are four combinations: 00, 01, 10, and 11. Every 00 and 11 is discarded, because 10 and 01 will be indistinguishable to Eve.

The idealized scheme requires a number of further enhancements for practical implementation, and these will be discussed later. One enhancement to note is that in practice an active noise source, rather than the Johnson noise from a resistor, is used so that the noise equivalent temperature is much higher than internal noise of the line. For this reason some papers use the term *Johnson-like* noise to indicate this, however, the 'like' can be dropped when the context is clear.

The core Kirchhoff-law-Johnson-noise secure key distribution system

In its practical implementation the KLJN scheme can operate with amplified Johnson noise, can possess defense units against invasive attacks and attacks that exploit non-ideality. There are also a number further improvements that will be discussed later. Let us first consider the core KLJN system (Kish 2006), without these enhancements, as shown in Figure 1. The idea behind the KLJN key exchange is as follows: two identical pairs of resistors representing bit values are used, one pair on Alice’s end and one pair on Bob's end. Depending on the state of each switch, which is randomly selected at the beginning of each clock cycle, one of the resistors is connected to the

cable. Thus there are four possible states in which the two binary switches can be in: 00, 01, 10, and 11. The two mixed states, 01 and 10, have identical channel noise voltage and current mean-square amplitudes, or power density spectra, and thus cannot be distinguished. Thus the eavesdropper, Eve, will be unable to separate/identify the two situations. However, Alice and Bob not only know the noise levels in the channel, but also the resistance value of their own resistor connected to the line. So, they can logically deduce the state of each other's resistor.

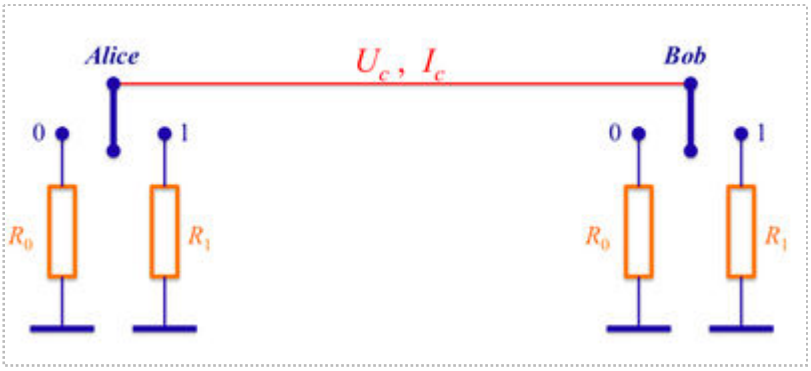

Figure 1: The heart of the KLJN or 'Kish cipher' secure key distribution system. It shows the core idea and serves an explanation why the Second Law of Thermodynamics offers conceptually perfect security against passive attacks. This simplified system is useful for understanding the basic principle, however, a practical realization is much more sophisticated in order to defend against invasive attacks and other types of attacks. There are also various other enhancements required for practical applications.

For a quantitative description of the noise spectra in the channels, the Johnson noise formulas for current and voltage can be used. The noise power density spectrum of thermal noise voltage of a resistor R is given as

$$S_u(f) = 4kTR, \tag{1}$$

while the power density spectrum of thermal noise current of the short-circuited resistor is

$$S_i(f) = \frac{4kT}{R}\,. \tag{2}$$

Thus the voltage noise spectrum in the channel is determined by the parallel combination of Alice and Bob's chosen resistances

$$S_{uc}(f) = 4kT\,\frac{R_{\rm A}R_{\rm B}}{R_{\rm A}+R_{\rm B}}\,, \tag{3}$$

while the current noise spectrum in the channel is determined by the series combination or total loop resistance,

$$S_{ic}(f) = \frac{4kT}{R_{\rm A}+R_{\rm B}}\,. \tag{4}$$

Alice, Bob, and Eve can perform appropriate measurements and by comparing the measurements with the values given by Eqs. 3-4, identify if the bit situation is all-low (00), all-high (11), or mixed (01, or 10).

In the all-low and all-high cases, the bit situation is obvious for everybody, including Eve, thus these situations

(which happen 50% of the time) offer no security. However, in the mixed state, Eve has no way to find out which side has bit 0 and which side has bit 1.

In the mixed state, by solving the system of equations (3) and (4), after inputting the measured spectra, a second-order equation for the resistances is determined. The two solutions will provide only the two resistor values, which are publicly known anyway. However, there is no directional information in these quantities and equations. The only directional information for Gaussian thermal noise is the cross-correlation of voltage and current, which is the net power flow between the two resistors,

$$P_{\mathrm{A}\to\mathrm{B}} = \langle U_c(t) I_c(t) \rangle \tag{5}$$

which is the average, net power flow from Alice toward Bob and the current in the channel is interpreted so that the current direction toward Bob has a positive sign. Equation (5) may potentially serve as useful information for Eve, if the temperatures of the resistors were different. However, with uniform temperatures in the system, according to the Second Law of Thermodynamics we have,

$$P_{\mathrm{A}\to\mathrm{B}} = \langle U_c(t) I_c(t) \rangle = 0 \tag{6}$$

which means that, in the ideal system defined by the scheme in Fig. 1, the passive eavesdropper is unable to extract any information about the key bits shared by Alice and Bob. Therefore the security level is perfect in the ideal situation. The level of security remains the same for arbitrarily great computational power, measurement accuracy and speed of Eve, and limited only by the laws of physics and by the conditions of the protocol. It is unconditional security or, in other words, information theoretic security (Mingesz 2013),(Liang 2008).

The minimally armed KLJN system against invasive and non-ideality based attacks

The defense method described here (Kish 2006),(Kish 2006b) offers a full protection against all known attack types including attacks utilizing the non-ideality of practical circuit elements and invasive attacks. One of the consequences is that imperfect information theoretical security, which non-ideal components imply, can approach the perfect security level (Kish 2009) even without using privacy amplification (Horvath 2011) tools.

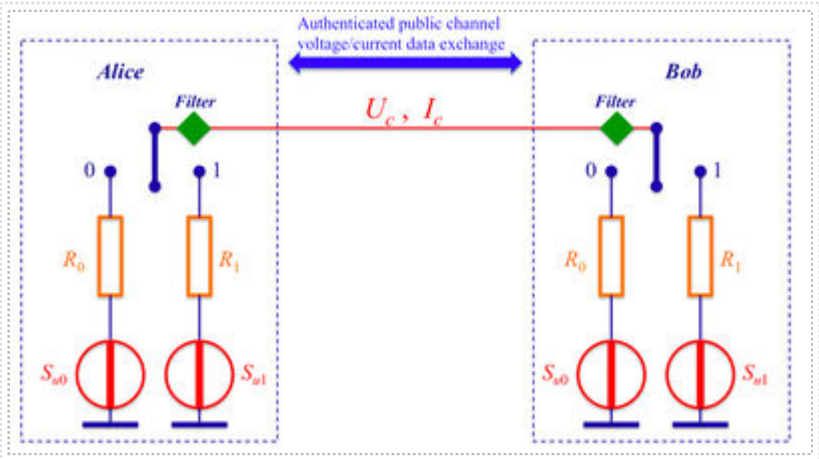

Figure 2: The minimally armed essential KLJN system against invasive and non-ideality attacks. Note, for simplicity, many other practical elements of existing defense systems are not shown, such as the cable capacitance killer, etc.

The *minimally armed* KLJN system is shown in Figure 2. It defends against all published attack types and this defense protocol and hardware can be conveniently expanded to more efficiently address further possible attacks. For all invasive and non-ideality attack types, the greatest information leak is obtained by comparing the voltage and current data at the two ends. To build a defense against these attacks, Alice and Bob

continuously measure the voltage and current data at their respective ends and communicate these data by authenticated communication via a public channel to the other party. Then they compare the received data with their own measurement results and, emulating Eve, they extract the eavesdropping information from the exchanged bit. Then, based on this comparison, they decide if they keep the bit or discard it (Kish 2009). They can also detect if an invasive attack occurs. To avoid the situation where Eve may use invasive or natural (eg. lightening transients, etc) probing signals out of the frequency range of their measurement, Alice and Bob use low-pass line-filters at the two ends to limit access to the monitored range of frequency (Mingesz 2013),(Mingesz 2008).

Note, low-pass filters are needed also for another reason. In those practical applications where propagation effects are potentially significant, low-pass filters are used (Kish 2006),(Mingesz 2013),(Mingesz 2008) to limit the channel-bandwidth because it must be sufficiently small that the time-dependence of the channel noise amplitudes, and possible switching transients, are slow enough that the voltage and current amplitudes are virtually homogenous all along the wire, implying that wave and propagation/delay effects are negligible. This is the quasi-static limit of electrodynamics. This is essential for the security and it strictly requires that the bandwidth is much smaller than the ratio of the propagation velocity and the length of the cable (Kish 2006),

$$f_c \ll \frac{c}{L}\,. \tag{7}$$

Another important improvement is to use artificial voltage noise generators that are connected in series with the resistors, where their noise intensity represent a publicly agreed high noise-temperature, such as 800 million Kelvin during the experimental tests (Mingesz 2008). This enhancement has multiple advantages, such as

i) The temperature and noise of the wire will be negligible even if it has non-zero resistance;

ii) The effective noise-temperatures of the resistors will be defined with extraordinary accuracy, eg. 14 bits during experiments, thus the Hao attack described in the next section provides negligible information to Eve.

iii) Artificial noise generators can be set to start from zero and they can also be ramped up and down, which are effective tools to reduce information leak due to transient effects (Mingesz 2008).

iv) Part of the low-pass filtering can be carried out at the noise-generator level; however, line filters are still needed.

If Alice's two resistors represent 0 and 1 and Bob's resistors represent 0 and 1, then there are four combinations: 00, 01, 10, and 11. Every 00 and 11 is discarded, because 10 and 01 will be indistinguishable to Eve. Note that for non-ideal cases, Alice and Bob may chose to drop further bits if they are judged to be high-risk. These so-called high-risk bits are dropped when Alice and Bob learn from comparing their current and voltage data that there is a risk that invasive eavesdropping has taken place, such as a man-in-the-middle-attack. Information leaks may also exist due to a vulnerability related to non-ideal elements or a design problem, resulting in the need to drop further high-risk bits.

Known attack types

Due to the simplicity of the KLJN system, there are very few attack types available. The method of comparing the instantaneous values of voltage and current and discarding risky bits, as previously described, protects against all these types of attacks. But even without discarding the risky bits, passive attacks by Eve utilizing non-idealities suffer from weak signal-to-noise ratio due to poor statistics, as discussed later.

Bergou proposed (Cho 2005) that, in the case of non-zero wire resistance the mean-square voltages are different at the two ends in the case of 01 and 10 bit situations. Scheuer and Yariv (2006) analyzed Bergou's attack, however,

their calculation was incorrect. Kish and Scheuer (2010) carried out new, correct calculations and showed that the actual effect is about 1000 times weaker than predicted by Scheuer and Yariv. Earlier, Kish (2006c) pointed out in his response to Scheuer and Yariv (2006) that Eve's statistic was very poor and the extracted information was practically miniscule even without the defense of discarding the risky bits. This claim was experimentally verified by Mingesz et al. (2008) who showed that at clock period of 50 times of the noise correlation time and wire resistance of 2% of the total loop resistance, without dropping any of the high-risk key bits, the information leakage to Eve was 0.19%, while the fidelity between Alice and Bob was 99.98%. These results indicate that the key exchange has excellent fidelity even without error correction and that the security is reasonably high even without dropping the risky key bit (see Section 3) and without privacy amplification (Horvath 2011). In order to reach this small error rate, 100 independent noise samples were averaged, which reduced the speed only by a factor of fifty compared to the reciprocal of original noise bandwidth in the channel Mingesz et al. (2008).

A less important but valid type of attack was shown by Hao (2006) who pointed out that the non-ideal situation of different temperatures can potentially separate the noise levels of the 01 and 10 bit situations, thus potentially leaking out some information to Eve. It was shown in the experimental paper (Mingesz 2008) that the 14 bit accuracy of temperatures practically prohibit Eve from extracting any information, with information leakage less than 10^{-10}, by utilizing the Hao attack.

Kish (2006d) pointed out in his response to Hao that, while the temperature is a practically unimportant source of information because of the 14 bit accuracy in the initial demonstration, inaccuracies of cheap commercial resistors (typically 1%, which is only 7 bits) can be exploited by Eve in a very similar fashion to the Hao attack. The analysis shows that the implications are similar to the wire resistance and the rule of the thumb is to keep inaccuracies at or below 1% to provide a raw-key-bit information leakage of the order of 0.01% or less (Mingesz 2008).

Liu (2009) used a cable simulator to evaluate the impact of delays and reflections on the security. He obtained the surprising result that, using experimental parameters (Mingesz 2008), Eve successfully guessed 70-80% of the key bits. A critical study of these simulations by Kish and Horvath (2009) pointed out that the chosen cable impedance of the simulation to reach these results were unphysical: given a diameter of 1 millimeter for the metal core of a coaxial cable, implies a coaxial cable outer diameter 28,000 times greater than the size of the known universe. Thus the resulting large inductance overloaded the simulator, as the correct result will have given Eve a 100% success rate for this unphysical situation.

Observing transients after switching and at the end of the clock period has been mentioned as a potential source of information leakage, however, so far they have never been utilized. The method of dropping the high-risk bits protects against such a leak. For experimental realization, the noise is ramped up at the beginning of the clock period and ramped down at the end thus resistor switching takes place when the voltage and currents are zero in the line. Kish (2013) outlined an improved transient protocol, where the resistors start from the resultant value of the mixed state and reach their randomly chosen value by an adiabatically slow random walk.

According to Kish (2006c), one of the most efficient attack types are potentially those that exploit capacitive currents via the cable capacitance, which is easy to calculate, but it has never been practically tested. Mingesz et. al (2008) demonstrated a hardware based defense, using a cable *capacitance killer,* against this attack. An alternative method is decreasing the noise bandwidth, and hence key exchange speed, so that capacitive currents are negligible. In any case, the method of discarding the risky bits and/or privacy amplification (Horvath 2011) are the ultimate tools for removal of any remaining information leakage.

Note that the capacitance killer arrangement is simply a coaxial cable with a bootstrapped shield. This is achieved in the standard way by driving the shield with a voltage follower. The input to the follower is the signal on the line. Thus there are no capacitive currents between line and the shield, as the voltage follower forces them to remain at the same potential.

Closing remarks

The KJLN scheme is an information-theoretic, i.e. unconditional, key exchange protocol with perfect security, in the mathematically ideal sense, and it can approach the level of perfect security in practical situations. One of the interesting potential applications (Kish 2008) is to integrate the KLJN system on computer chips and provide unconditional security within computers and high-security instrumentation where the processors, hard drives, keyboards, etc. can secure their communications by keys shared by the KLJN protocol.

References

- Cho A (2005) Simple noise may stymie spies without quantum weirdness. Science 309:2148; http://www.ece.tamu.edu/~noise/news_files/science_secure.pdf
- Hao F (2006) Kish's key exchange scheme is insecure. IEE Proc. Inform. Soc. 153:141-142.
- Horvath T, Kish LB, Scheuer J (2011) Effective privacy amplification for secure classical communications. Europhys. Lett. 94:28002.
- Kish LB (2006) Totally secure classical communication utilizing Johnson(-like) noise and Kirchhoff's law. Phys. Lett. A 352:178-182.
- Kish LB (2006b) 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. http://arxiv.org/abs/physics/0512177
- Kish LB (2006c) Response to Scheuer-Yariv: "A classical key-distribution system based on Johnson (like) noise–How secure?" Phys. Lett. A 359:741-744.
- Kish LB (2006d) Response to Feng Hao's paper "Kish's key exchange scheme is insecure." Fluct. Noise Lett. 6:C37-C41.
- Kish LB, Saidi O (2008) Unconditionally secure computers, algorithms and hardware. Fluct. Noise Lett. 8:L95-L98.
- Kish LB, Horvath T (2009) Notes on recent approaches concerning the Kirchhoff-law-Johnson-noise-based secure key exchange. Phys. Lett. A 373:901-904.
- Kish LB, Scheuer J (2010) Noise in the wire: The real impact of wire resistance for the Johnson(-like) noise based secure communicator. Phys. Lett. A 374:2140-2142.
- Kish LB (2013) "Enhanced secure key exchange systems based on the Johnson noise scheme. Metrology and Measurement Systems 20:191-204
- Liu PL (2009) A new look at the classical key exchange system based on amplified Johnson noise. Phys. Lett. A 373:901-904.
- Mingesz R, Gingl Z, Kish LB (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.
- Liang Y, Poor HV, Shamai S (2008) Information theoretic security. Foundations Trends Commun. Inform. Theory 5:355-580, DOI: 10.1561/0100000036.
- Mingesz, R, Kish, LB, Gingl Z, Granqvist CG, Wen H, Peper F, Eubanks T, Schmera G (2013) Unconditional security by the laws of classical physics. Metrology and Measurement Systems 20:11–25. Open access: http://www.degruyter.com/view/j/mms.2013.20.issue-1/mms-2013-0001/mms-2013-0001.xml?format=INT
- Palmer DJ (2007) Noise encryption keeps spooks out of the loop. New Scientist 2605:32; http://www.newscientist.com/article/mg19426055.300-noise-keeps-spooks-out-of-the-loop.html
- Scheuer J, Yariv A (2006) A classical key-distribution system based on Johnson (like) noise–How secure? Phys. Lett. A 359:737-740.

See also

- Cryptography
- Stochastic resonance

Sponsored by: Dr. Albert-Laszlo Barabasi, Harvard University, Boston, MA
Sponsored by: Lawrence M. Ward, University of British Columbia, Vancouver, CANADA
Sponsored by: Andre Longtin, Physics Department, University of Ottawa, Ottawa, Canada
Reviewed by (http://www.scholarpedia.org/w/index.php?title=Secure_communications_using_the_KLJN_scheme&oldid=134360) : Anonymous (via Leo Trottier, Department of Cognitive Science, University of California, San Diego, CA, USA)
Reviewed by (http://www.scholarpedia.org/w/index.php?title=Secure_communications_using_the_KLJN_scheme&oldid=135562) : Anonymous (via Dr. Riccardo Guida, Institut de Physique Théorique, CEA & CNRS, Gif-sur-Yvette, France)
Accepted on: 2013-08-12 22:47:48 GMT (http://www.scholarpedia.org/w/index.php?title=Secure_communications_using_the_KLJN_scheme&oldid=135562)

Categories: Noise | Statistical physics