The important thing is not to stop questioning. Curiosity has its own reason for existing. (Albert Einstein)

Facts, myths and fights about the KLJN classical physical key exchanger

Laszlo Kish
Department of Electrical and Computer Engineering, Texas A&M University, College Station

Claes-Göran Granqvist
Department of Engineering Sciences, The Ångström Laboratory, Uppsala University, Uppsala, Sweden

Derek Abbott
Department of Electrical Engineering, University of Adelaide, Adelaide, Australia

Tamas Horvath
Fraunhofer Institute for Computer Science, Sankt Augustin Germany

He Wen
Hunan University, Changsha, China

Regular talk at HoTPI 2013, Changsha, China

We appreciate feedback from: Horace Yuen, Robert Mingesz, Zoltan Gingl, Lachlan Gunn, Vincent Poor, Vadim Makarov, Renato Renner, Henning Dekant, Ferdinand Peper, Terry Bollinger, Olivier Saidi and Gabor Schmera.

The Kirchhoff-law-Johnson-noise (KLJN) secure key exchange utilizes the Fluctuation-Dissipation-Theorem in a simple loop with two resistors and its security is intimately related to the properties of Johnson noise including the Second Law of Thermodynamics and the properties of Gaussian stochastic processes. The unconditional security in non-ideal cases is maintained by the continuity functions describing stable classical physical systems. Since its creation, KLJN has been surrounded by doubts, myths and claims based on inappropriate approaches or just simple misunderstandings. This talk aims to lift the fog and shows a few essential points.

Bit errors in the Kirchhoff-law-Johnson-noise secure key exchange

Yessica Saez and Laszlo Kish
Department of Electrical and Computer Engineering, Texas A&M University, College Station

Robert Mingesz and Zoltan Gingl
Department of Technical Informatics, University of Szeged, Hungary

Claes-Göran Granqvist
Department of Engineering Sciences, The Ångström Laboratory, Uppsala University, Uppsala, Sweden

We classify and analyze bit errors in the voltage and current measurement modes of the Kirchhoff-law–Johnson-noise (KLJN) secure key distribution system. In both measurement modes, the error probability decays exponentially with increasing duration of the bit sharing period (BSP) at fixed bandwidth. We also present an error mitigation strategy based on the combination of voltage-based and current-based schemes. The combination method has superior fidelity, with drastically reduced error probability compared to the former schemes, and it also shows an exponential dependence on the duration of the BSP.

Regular talk at HoTPI-2013, Changsha, China

John Johnson
born: Göteborg, Sweden
died: Orange, NY, USA

Johnson-Nyquist noise voltage of resistors; 1928 (after 'quantum'—1926)

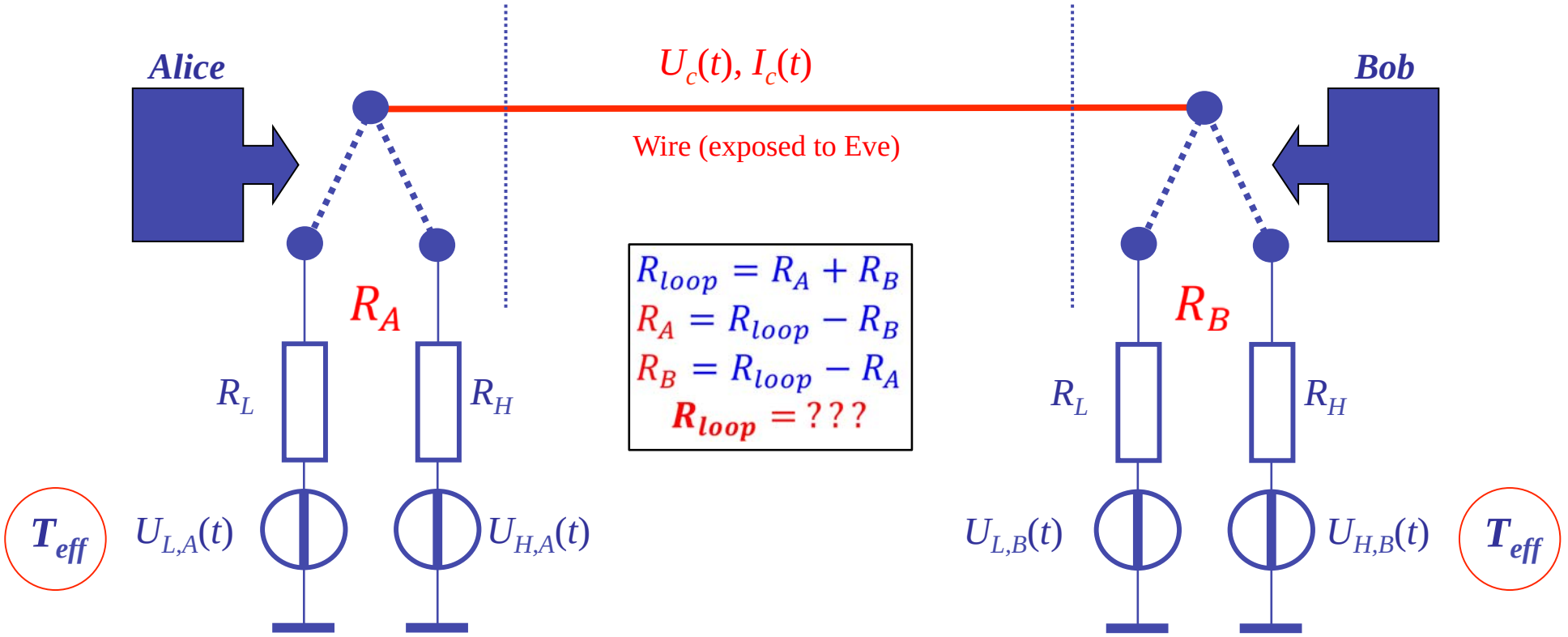
Harry Nyquist
born: Nilsby, Värmland, Sweden
died: Harlingen, Texas, USA

2005: KLJN secure key exchange utilizing Kirchhoff law and thermal noise

Potential: it can be integrated on a chip: PUF and secure computer/instrument applications

Content

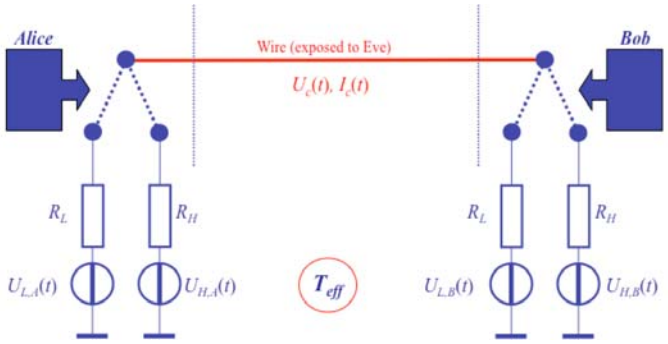
1. KLJN key exchanger, *idealized situation (zero range)*, passive attacks: U_c, I_c measurements



If Alice and Bob know the total loop resistance then they can deduce the resistance value at the other side by subtracting their own resistance from it.

But how to measure the loop resistance without informing Eve about their own resistance values???

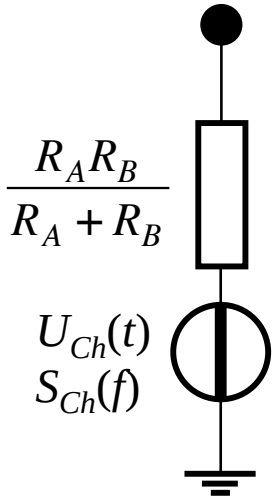
The loop resistance can be evaluated by measuring the thermal noise in two different ways

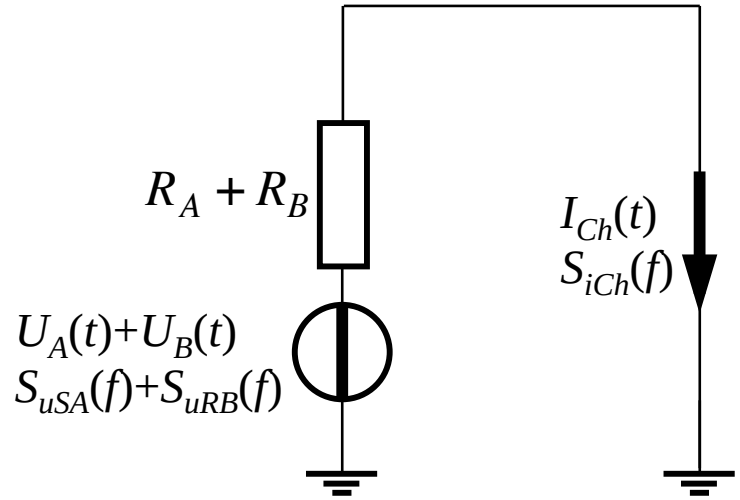


Voltage and current Johnson-Nyquist formulas for this loop:

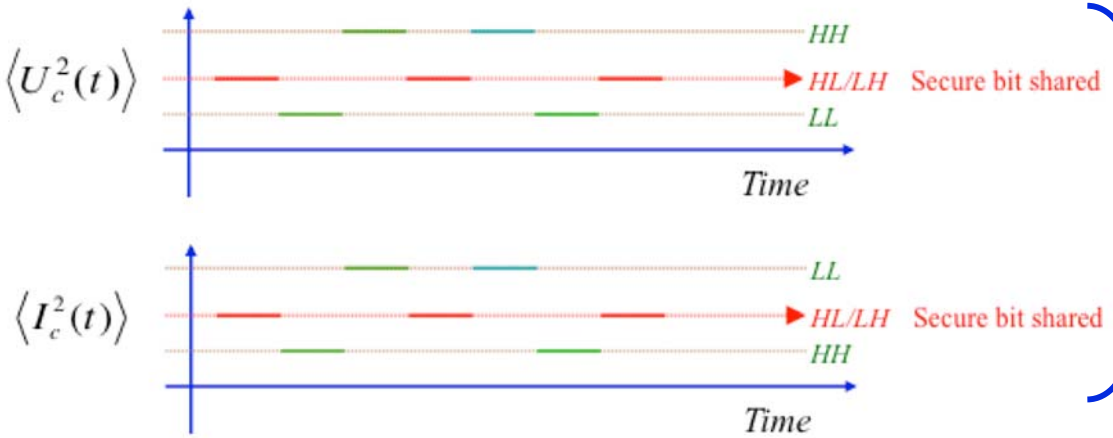
$$S_{u,R\|}(f) = 4kT\,\frac{R_A R_B}{R_A + R_B}$$

$$S_{i,R\|}(f) = \frac{4kT}{R_A + R_B}$$





If Eve could see a difference between the levels for HL and LH then she could extract the key or its inverse thus she could crack the secure communication by testing the message with them.



OBSERVE:
Large differences between secure and non-secure levels: small error prob.

No difference between HL and LH:
Zero information for Eve.

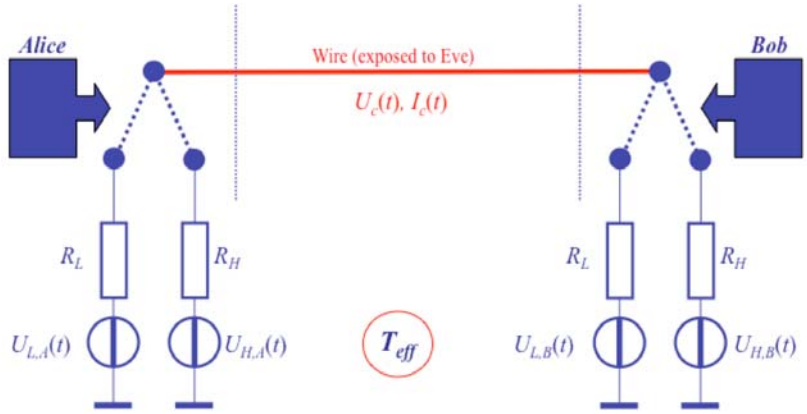
1.1 Foundation of its security in the *idealized case* (observe, *Eve's accuracy and speed are always unlimited*)

Is there any other passive attack for Eve in the idealized situation?

Gaussian stochastic process: power spectra of voltage and current contains all the information. However, also their crosscorrelation is a potential info source.

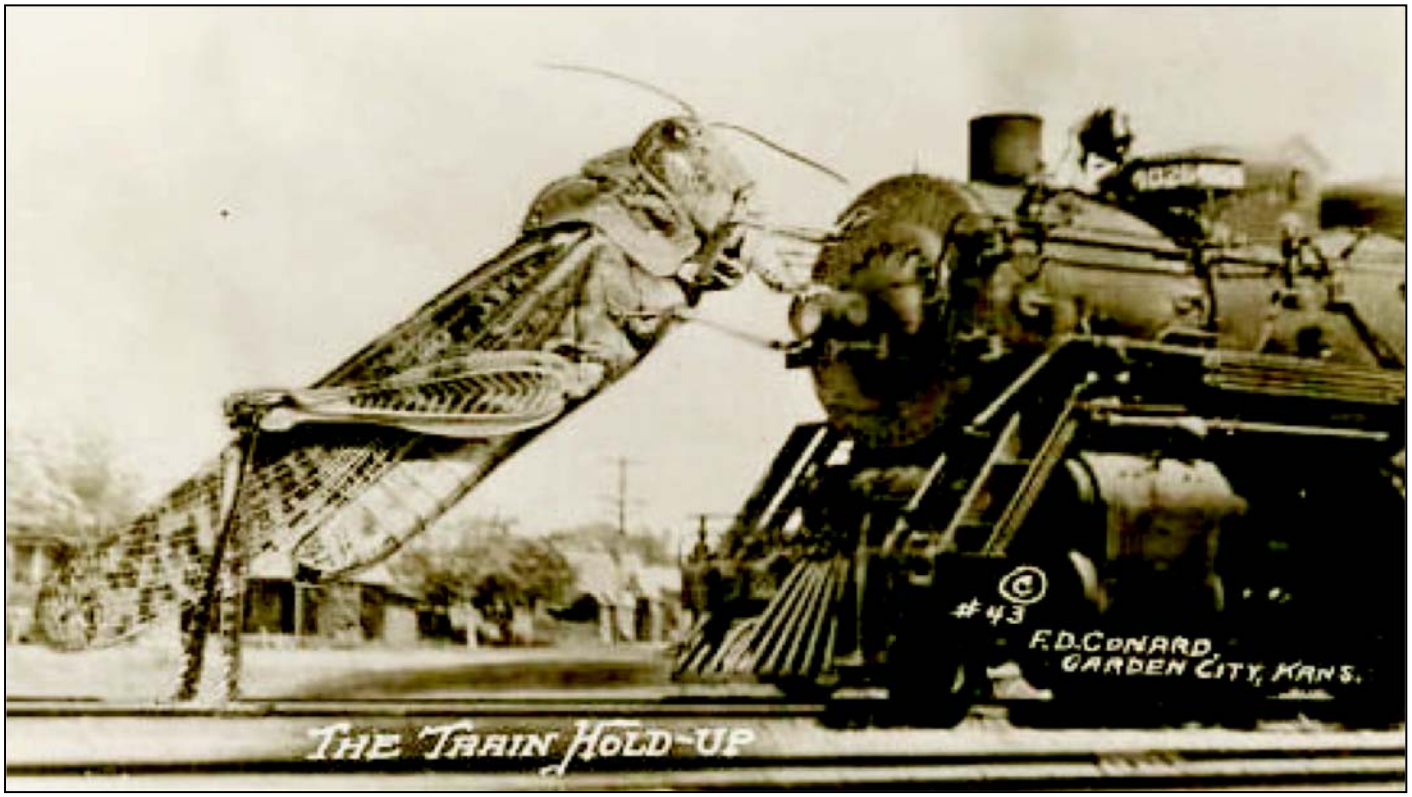
Indeed, the only directional quantity in the ideal system is the voltage-current crosscorrelation vector

$$\vec{P}(t) = \left\langle U_c(t)\vec{I}_c(t) \right\rangle$$



Will perhaps this vector show which side has the smaller resistance?

!!! The Second Law of Thermodynamics



No net power flow in a closed system in thermal equilibrium.

Forbids the construction of perpetual motion machines (of the second kind).

KLJN secure key exchanger, *idealized situation (zero range)*, passive attacks: U_c, I_c measurements

The only directional quantity in the ideal system is the power vector:

$$\vec{P}(t) = \left\langle U(t)\vec{I}(t) \right\rangle = 0$$

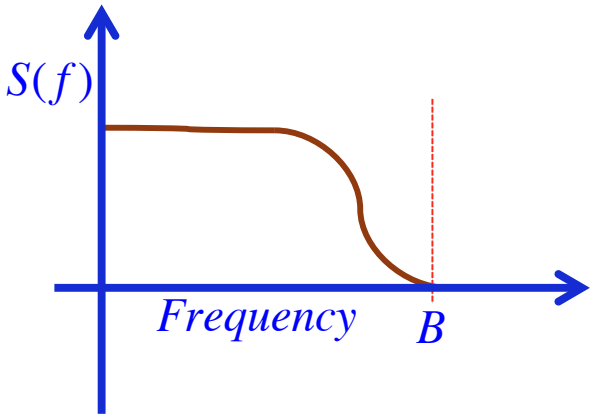
according to the Second Law of Thermodynamics

As difficult to crack the ideal system by a passive attack as to build a perpetual motion machine.

1.2 How many independent samples does the measurement statistics contain?

In non-ideal cases (see later) Eve will be able to extract miniscule information about the key due to second-order effects. Next we turn to Alice/Bob's bit error rate, and a relevant aspect for Eve, here.

Frequent point of misunderstanding) *Eve does have have infinite measurement speed and accuracy*!
Still, the amount of information that she is able to extract from the noise is strongly limited in accordance with *basic laws of information theory and signal processing*!



Band-limited noise: *Nyquist–Shannon sampling theorem*

$$n \leq 2B\tau$$

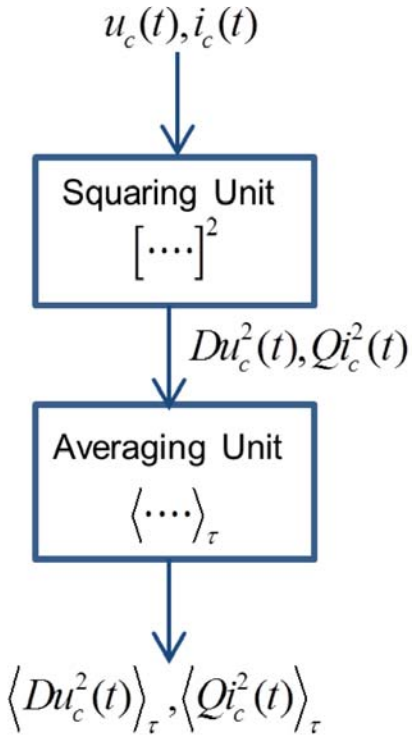
This is a hard limit for Alice, Bob and Eve.

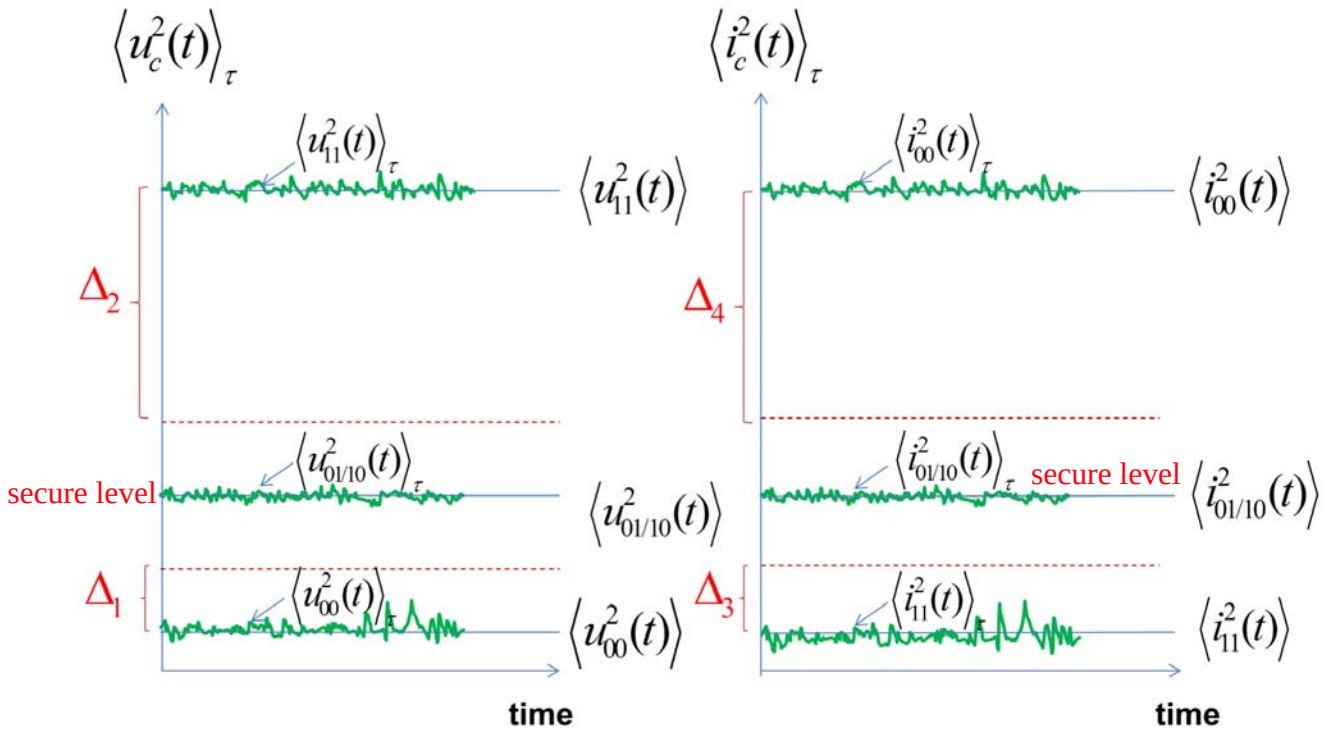
During τ duration, the measurement serves only with $n \leq 2B\tau$ independent samples about the measured noise. Alice and Bob has full control of n because they set the bandwidth and the duration of single bit exchange.

Eve's only way to extract information is to make statistics of the noise under *invasive (active) attacks* or by exploiting *non-ideal features* utilize *second-(or higher)-order effects*, which are however inefficient with small sample numbers.

1.3 Alice's/Bob's bit error probability: exponential decays versus the duration of single-bit exchange

The same $n \le 2B\tau$ sample limit is relevant for Alice and Bob but *they decide about first-order effects*.





Protocol

Current measurement interpretation	Voltage measurement interpretation: 00	11	01/10
00	00 (Insecure/Discard)	Discard (check attack)	00 (Insecure/Discard)
11	Discard (check attack)	11 (Insecure/ Discard)	11 (Insecure/ Discard)
01/10	00 (Insecure/ Discard)	11 (Insecure/ Discard)	01/10 (Secure)

$$\varepsilon_{t,00} = \varepsilon_{00}\varepsilon_{i,00} = \frac{1}{3}\exp\left(\frac{-\gamma(\beta^2+\rho^2)}{4}\right)$$

$$\varepsilon_{t,11} = \varepsilon_{11}\varepsilon_{i,11} = \frac{1}{3}\exp\left(\frac{-\gamma(\delta^2+\lambda^2)}{4}\right)$$

Combination of the voltage/current measurements results in a low bit error probability for Alice and Bob

$$\varepsilon_{t,00} = \varepsilon_{00}\varepsilon_{i,00} = \frac{1}{3}\exp\left(\frac{-\gamma(\beta^2+\rho^2)}{4}\right)$$

$$\varepsilon_{t,11} = \varepsilon_{11}\varepsilon_{i,11} = \frac{1}{3}\exp\left(\frac{-\gamma(\delta^2+\lambda^2)}{4}\right)$$

$$\gamma = 100$$

$$\text{else} = 0.5$$

$$\varepsilon_{tot} < 10^{-12}$$

Check Mingesz's talk tomorrow for optimized values.

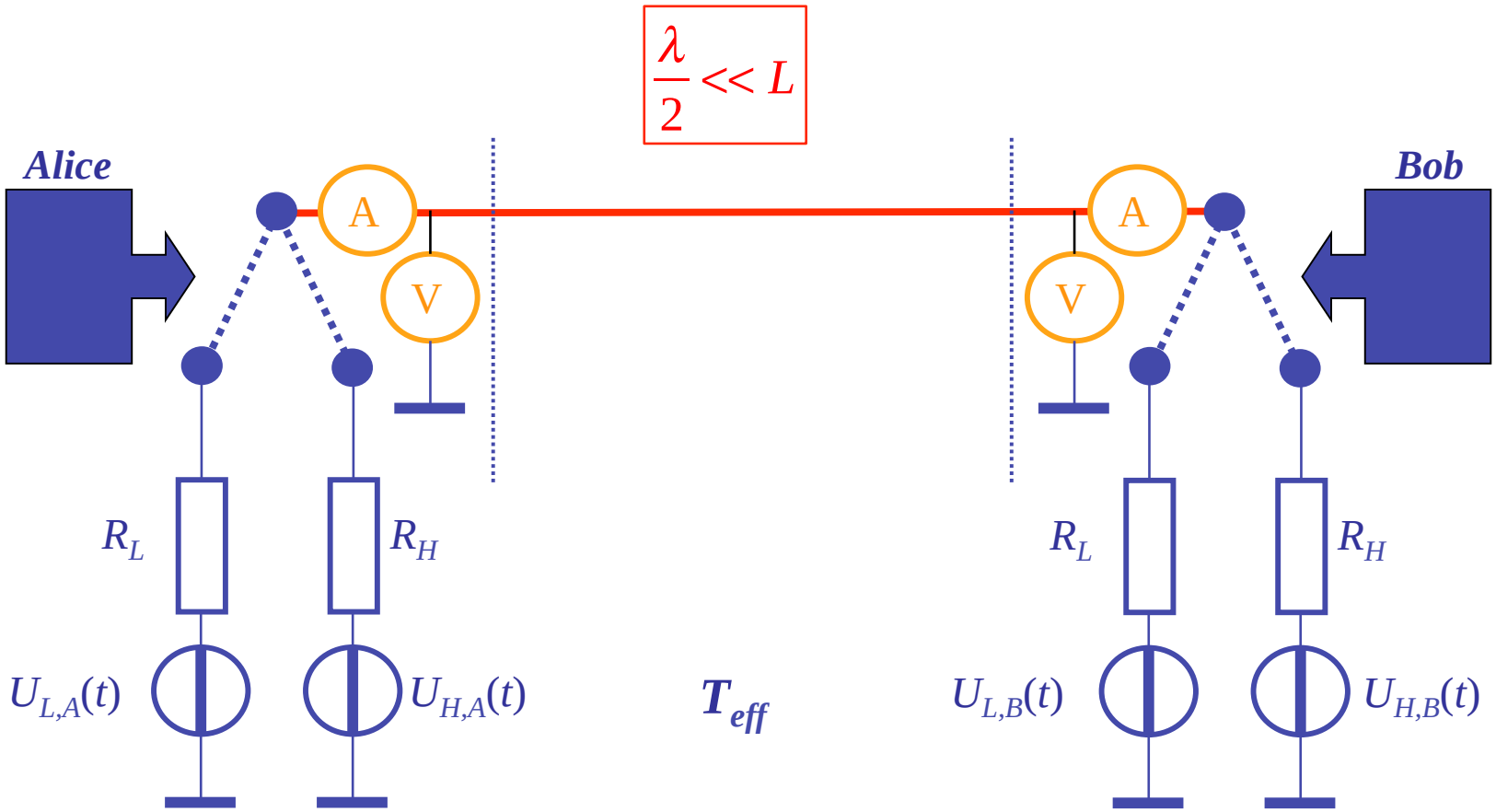
Excellent for XOR-based privacy amplification. Two steps of this privacy amplification (which is satisfactory to all practical applications) increases the error probability only by a factor of 4.

Horvath T, Kish LB, Scheuer J (2011) Effective privacy amplification for secure classical communications. *Europhys. Lett.* 94:28002

This does not give out information to Eve and does not introduce correlations between bits. (Horace Yuen says *privacy distillation* would the proper name).

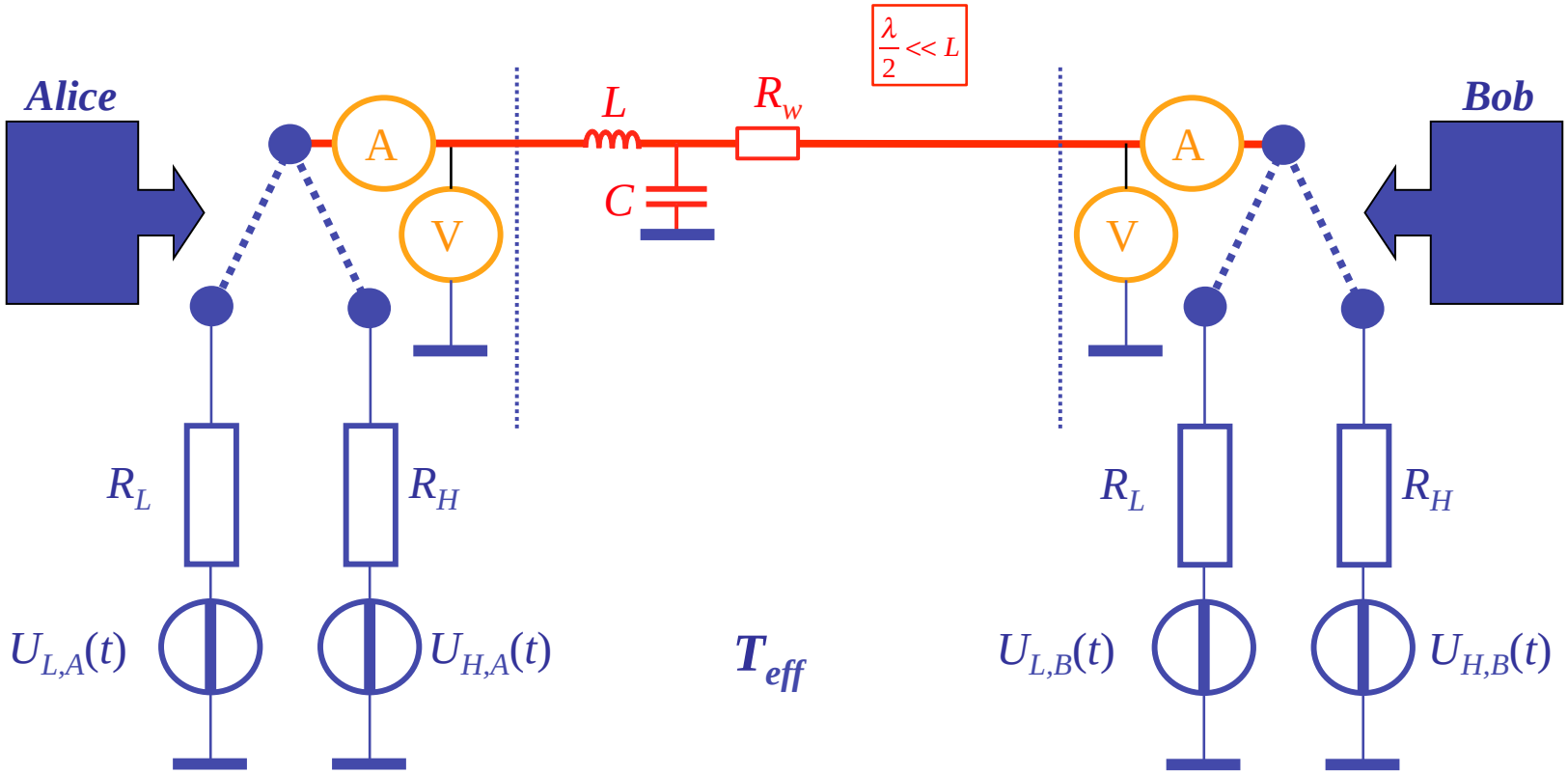
2. Security at *practical* situations against passive attacks

So, to reach high fidelity, Alice/Bob measure and evaluate both the current and voltage.



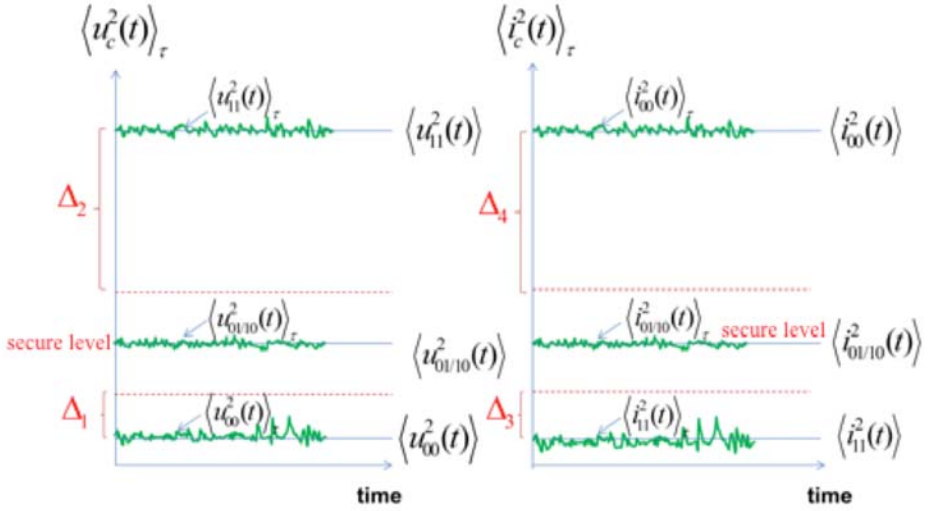
2. Security at practical situation against passive attacks

However, for non-zero distances *wire resistance, capacitance, inductance and delay effects* are present.
They are negligible only in chip applications within computers and instruments.
As a consequence: the voltages and currents at the ends of Alice and Bob will slightly be different.
Eve can utilize these difference thus *information leak about the key does exist*. ***But how much?***



The "secure levels" 01 and 10 will slightly split due to the second-(or higher)-order effects but the splitting is buried by a large noise due to finite-time statistics (*n*~100).

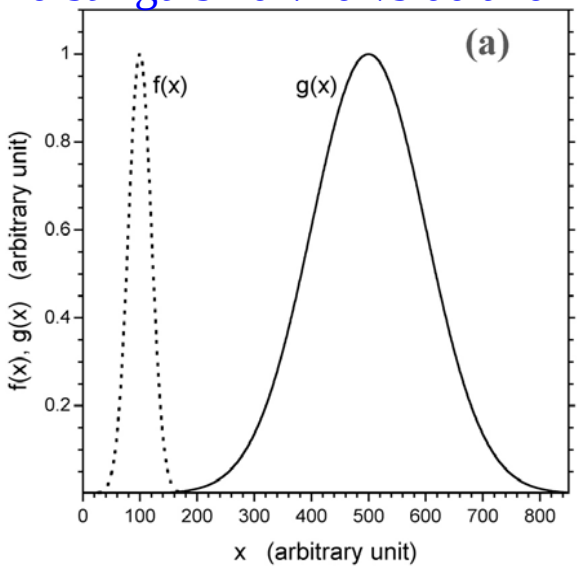
split 01/10 levels
enhanced for visibility



Practical distribution functions to:

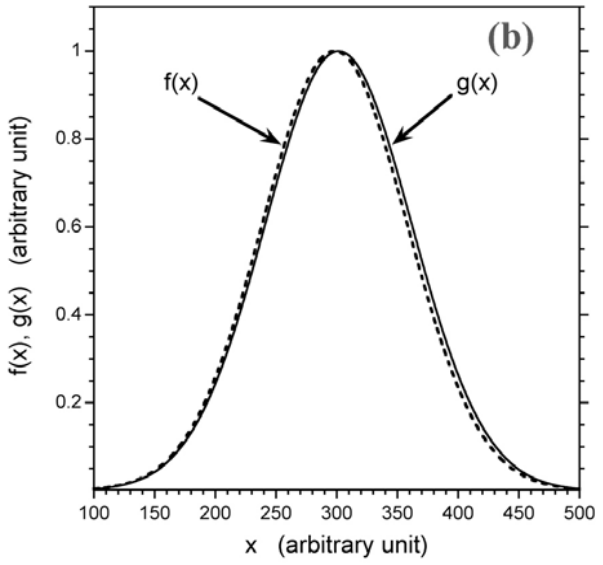
Kish, "Response to Scheuer and Yariv..." (PLA 2006)

Alice/Bob
distinguish 01/10 vs 00 and 11

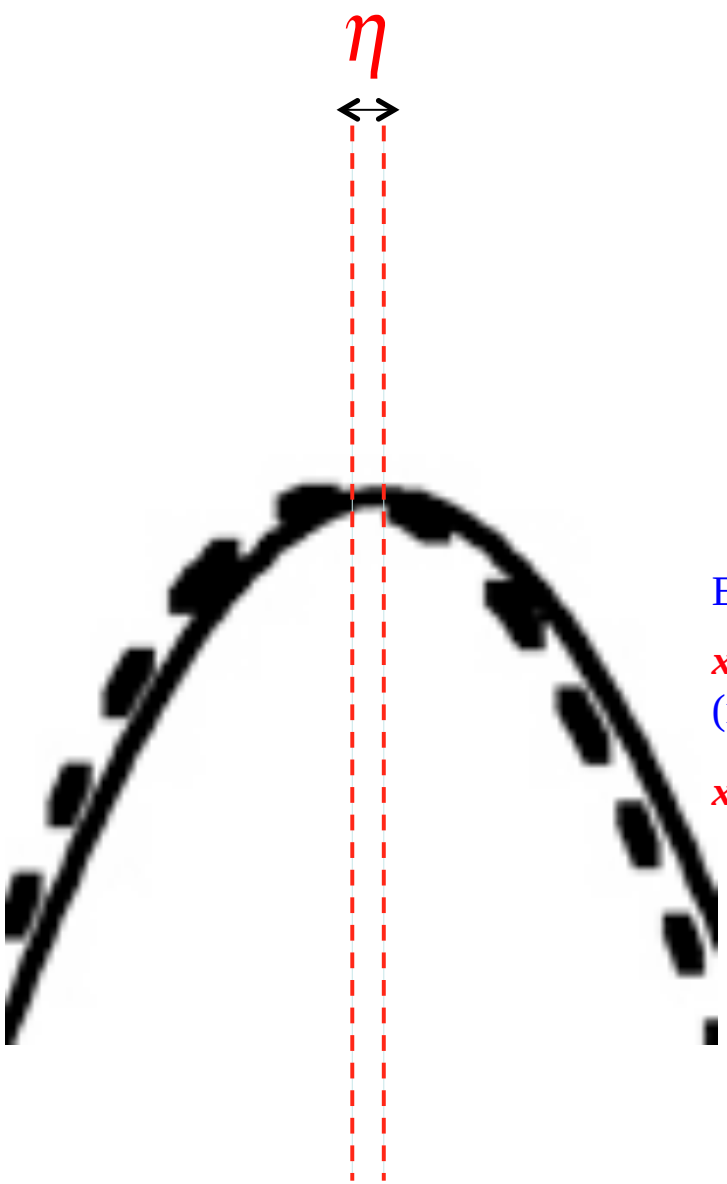


Eve
separate 01 from 10

(split is enhanced for visibility)



Eve's typical signal about non-idealities is a small DC in a large noise due to the weakness of the effects and the small statistics. (SNR around 10^{-3} - 10^{-4} and sample number n is around 100)



$$p = \int_0^\infty h(U)\,dU = 0.5$$

$\eta > 0, \quad \eta \propto V^{-x} \to 0$, where V is Alice/Bob's related resource and $x \geq 1$

$$p(\eta) = 0.5 + q = \int_\eta^\infty h(U)\,dU = 0.5 + \eta h(0)$$

$q = \eta h(0) \propto \eta \propto V^{-x} \to 0$ in a power-law fashion

$$p(V) = 0.5 + q = 0.5 + \vartheta V^{-x}$$ where $\vartheta > 0$

Examples for x:

x=4 if V= wire diameter at fixed wire length, at the Scheuer-Yariv attack (note, x=2 at Kish's unpublished more efficient wire resistance attack)

x=1 if V = the resolution of current-voltage comparison in current injection attack

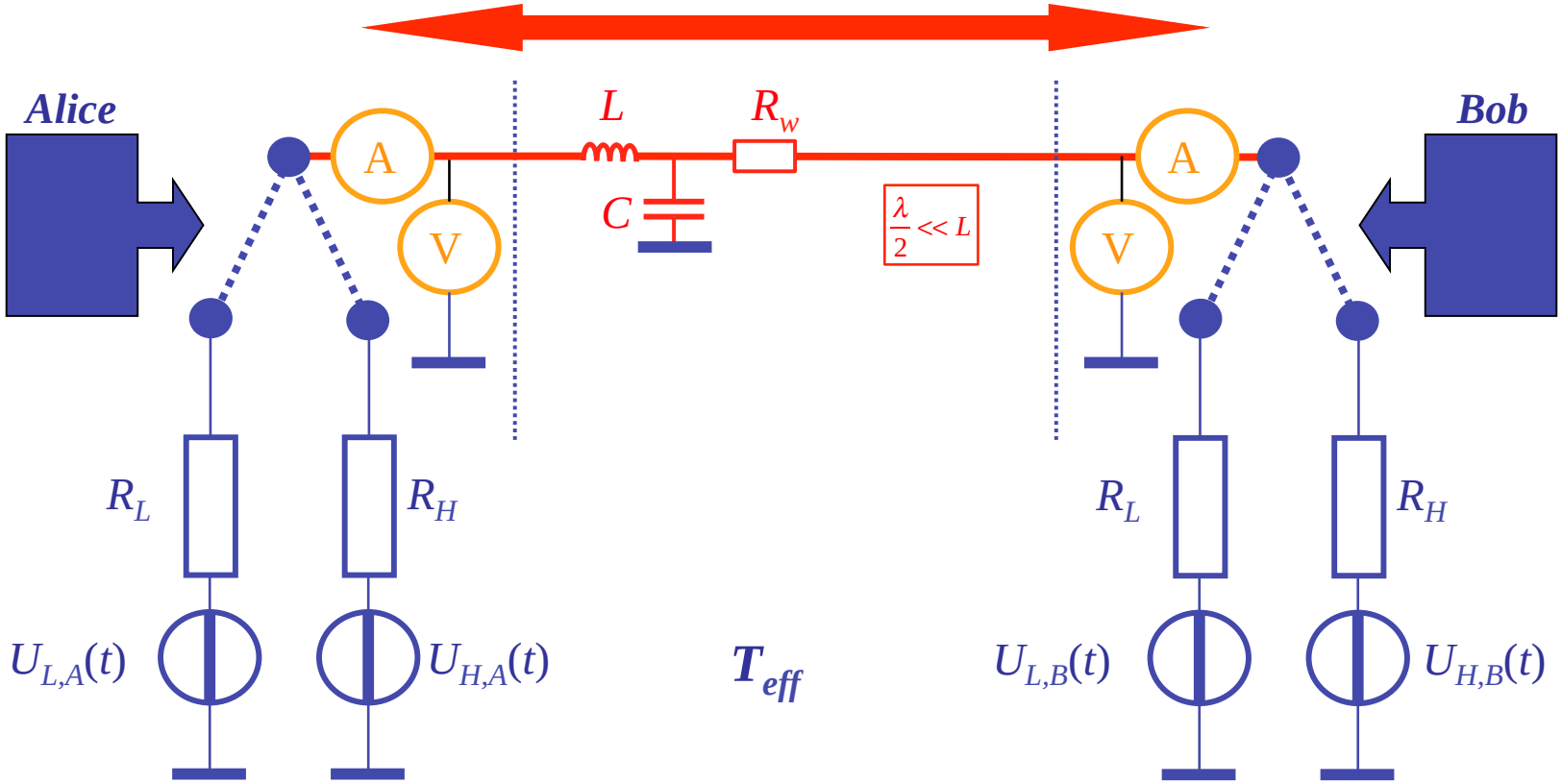
Example for p:

p=0.525 in the 2006 experimental test where R_w was 2% of R_0+R_1 (Mingesz, Gingl, Kish, PLA 2008)

Security at practical situation against passive attacks

Note: Even in the case of strong leak, Alice and Bob can limit Eve's success probability to p_{max} by *voltage-current comparison via authenticated channel because they have a deterministic model of the system (classical physics).*

Instantaneous voltage and current amplitude comparison by Alice and Bob via authenticated public channel. For this $\log_2 N$ secure bits are used up for the exchange of N authenticated bits (Hjelme, Lydersen, Makarov arXiv:1108.1718)



Statistical distance between the distributions of Eve's key and the ideal key

$$p(V) = 0.5 + q = 0.5 + \vartheta V^{-x}$$

Horace Yuen: "For single bit or bits with no correlation all criteria are equivalent. They can be easily translated into each other quantitatively".

Variational distance:

$$\Delta(E,I) = \max_{j=1,\ldots,2^N} \left[P(E_j) - P\left(I_j\right) \right]$$

where E and I indicate Eve's extracted key and a perfectly secure key, respectively, and $P(E_j)$ and $P\left(I_j\right)$ are the probabilities for correctly guessing the j^{th} version of Eve's key and of the perfectly secure key, respectively.

$$q_{\max} = \vartheta_{\max} V^{-x}$$

$$\Delta = \left(0.5 + q_{\max}\right)^N - 0.5^N \cong 2Nq_{\max} 0.5^N = 2N\vartheta_{\max} V^{-x} 0.5^N$$

$Nq_{\max} << 0.5$

For the 2006 experiments (Mingesz, et al, PLA 2008) with a two-stage XOR type privacy amplification the upper limit of key length is N<10000.

For N=1000, $\Delta(E,I)_{1000} = 9.3 \text{ x } 10^{-303}$ and for N=500, $\Delta(E,I)_{500} = 1.5 \text{ x } 10^{-152}$

Note: there is another general security proof for ***passive attacks*** in the situation where the **current/voltage comparison is not even used to limit *p*.** This is of only academic interest:

It is based on the *continuity of functions* in stable, practical *classical physical* systems.

See also Janusz Smulko's talk tomorrow who independently arrived at a similar conclusion.

$p_{\text{ideal}} = 0.5$ (Eve has zero information about the key)

If $x, y,$ etc. are the quantities representing the ideal situation at their zero value then, from the continuity of functions in stable classical physical systems, it follows that:

$$\lim_{x,y,\ldots \to 0} p_{\text{practical}}(x,y,\ldots) = 0.5$$

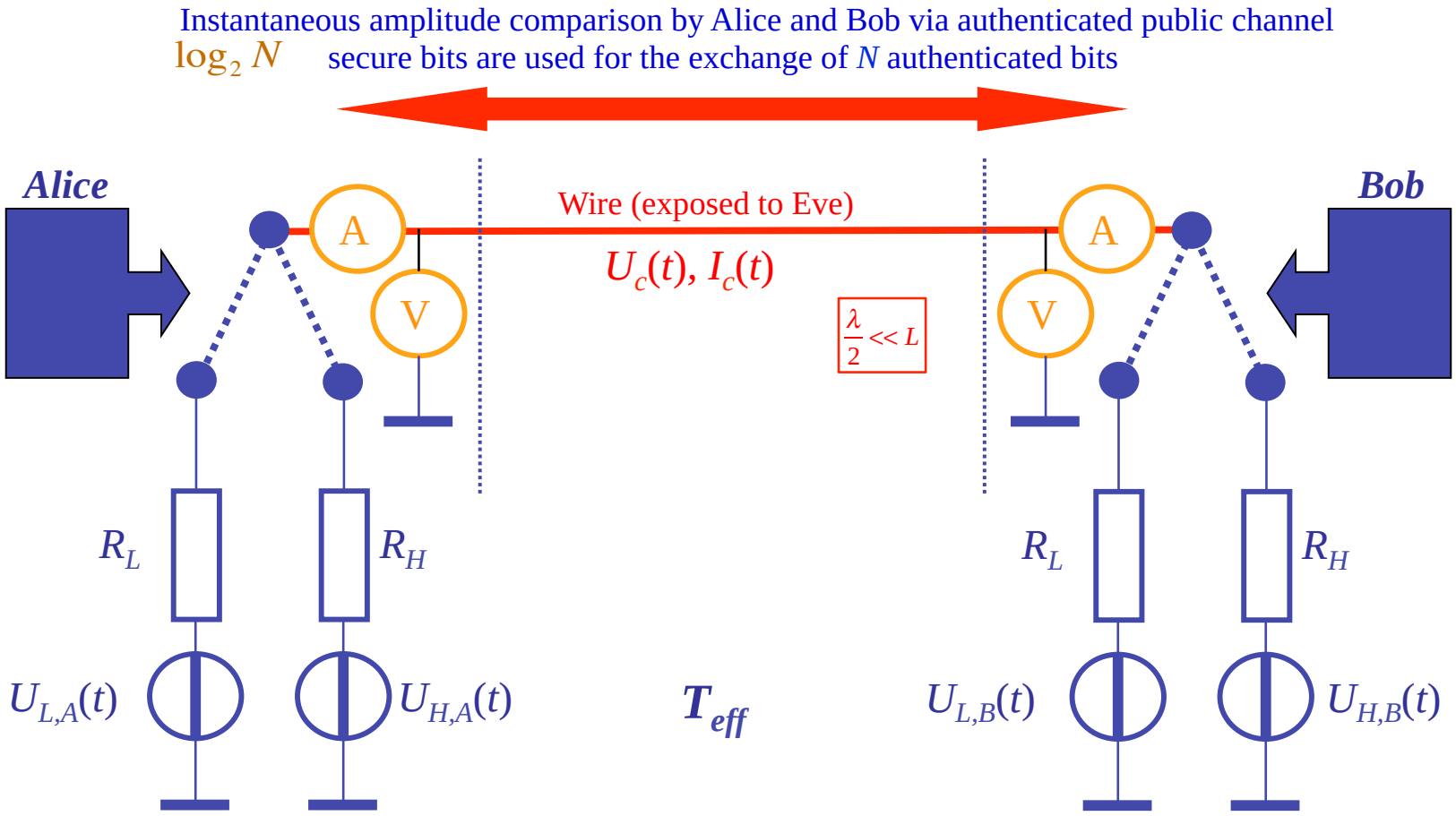
Examples: x = wire length; y = noise bandwidth; etc.

Note, $x, y, \ldots \to 0$ guarantees the ideal situation but *not all of them must be zero at the same time*.

For example: if x = wire length = 0 then y = noise bandwidth = can be *any finite value*

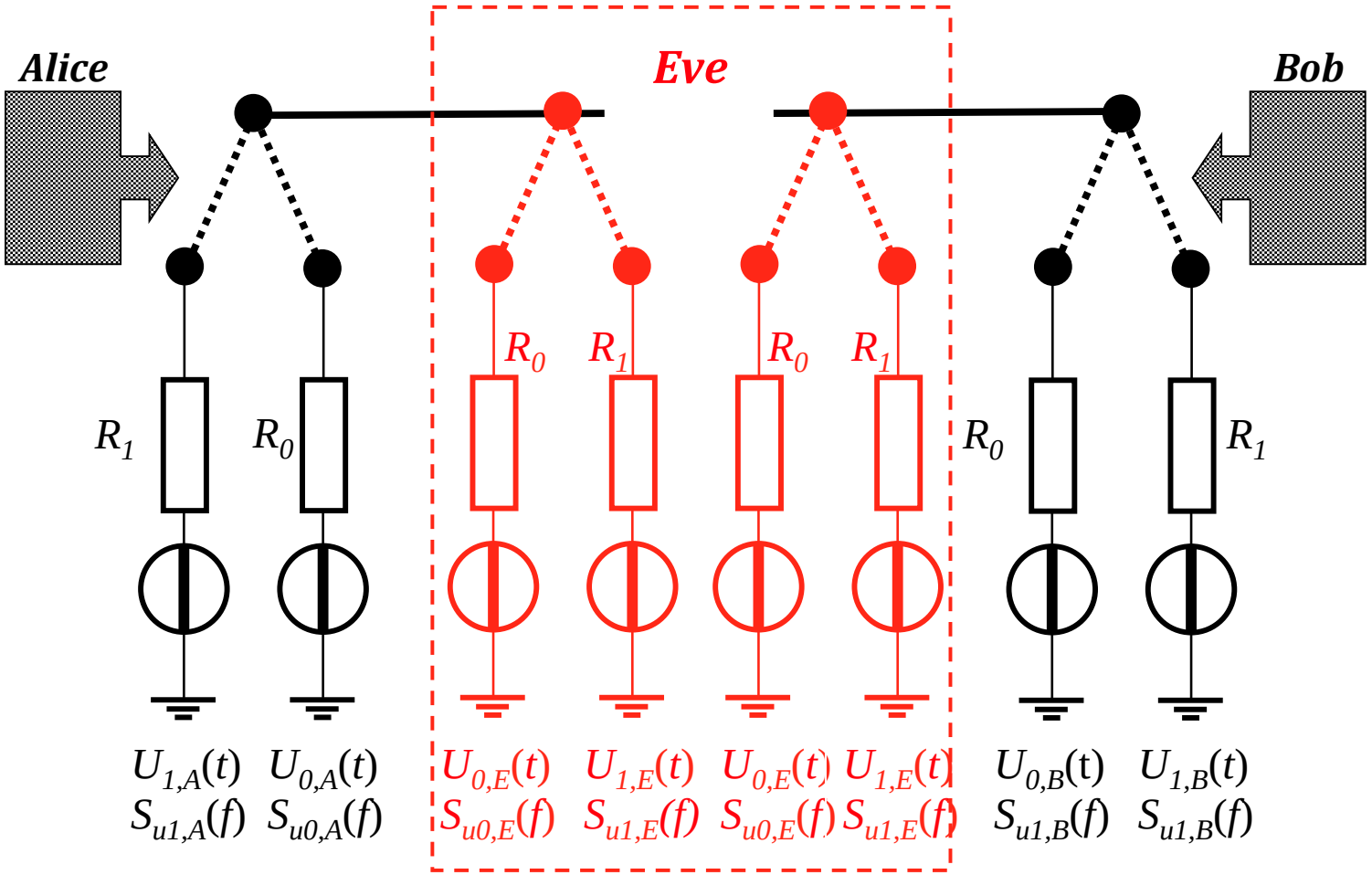
3. KLJN secure key exchanger, active (invasive) attacks

Eve modifies the system to extract information. Standard method is again the current/voltage comparison providing unconditional security. Two examples follow.

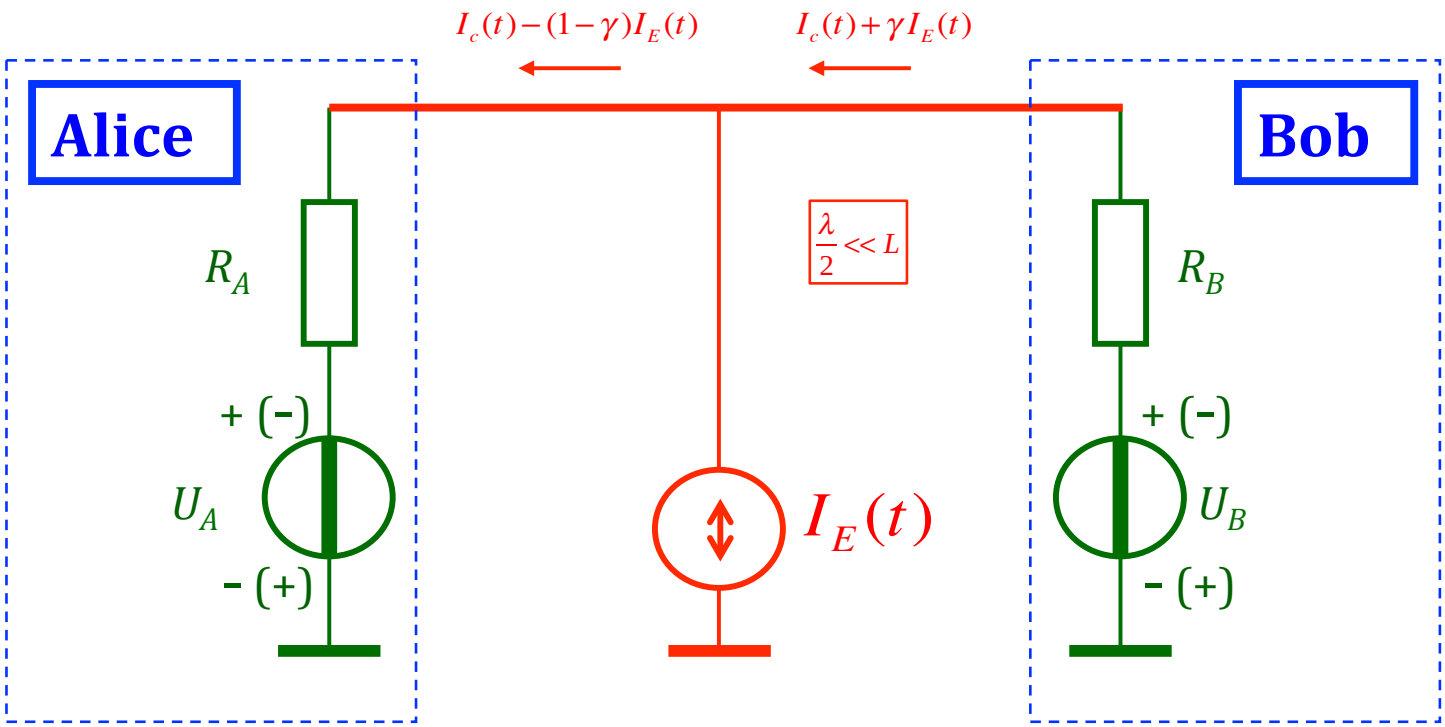


Man-in-the-middle attack: the least-effective active attack (Kish, FNL, 2006)

Totally independent voltages and currents in the two loops. The current-voltage comparison alarm goes on with near to 1 probability within the correlation time of the noise. Practical estimation: the probability that Eve can stay hidden for a single bit exchange period at only 7 bits accuracy of comparison is $P<10^{-20}$



Current injection attack (Kish PLA 2005; Rainer Plaga 2006; Bennett, Riedel arxiv:1303.7435 (2013)

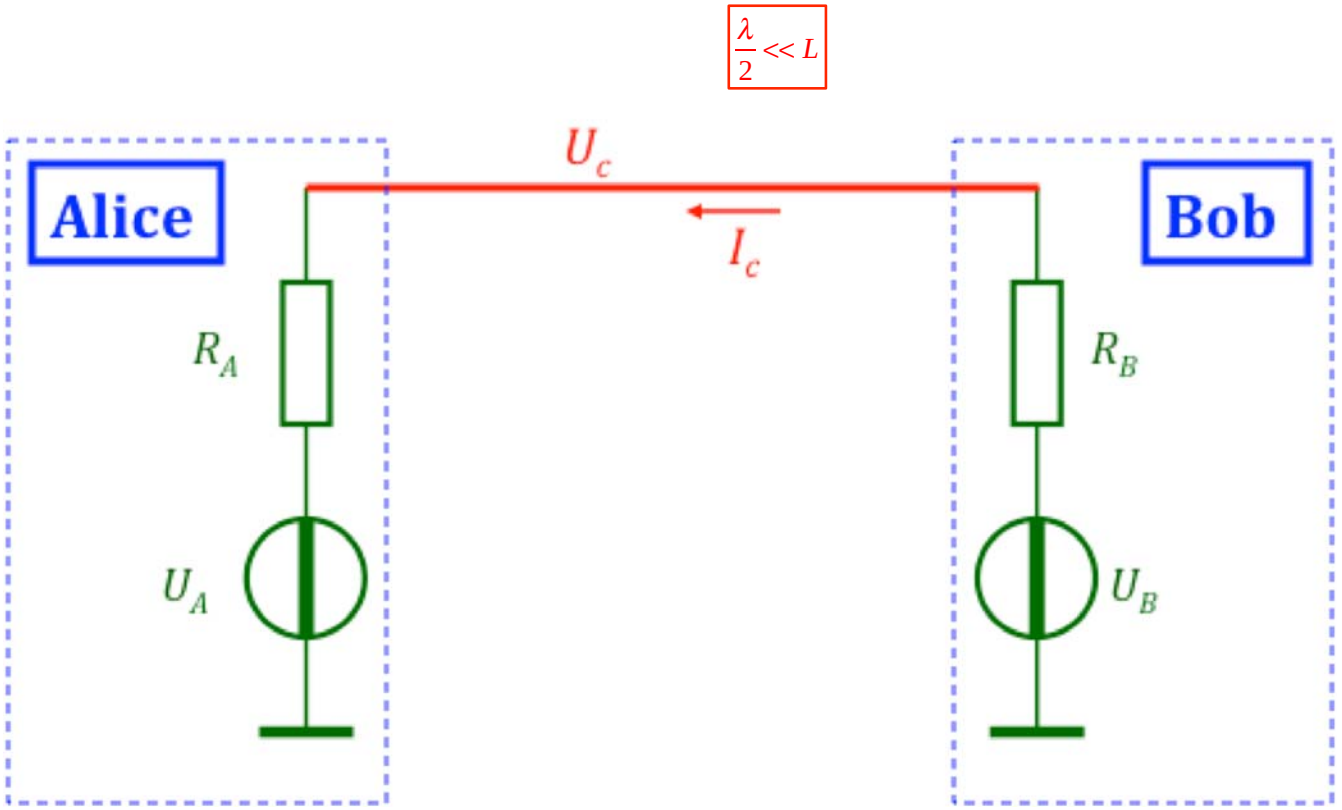


$p(V) = 0.5 + \vartheta V^{-1}$ where V = the relative current resolution of Alice/Bob > $\sqrt{\langle I_E^2(t)\rangle / \langle I_c^2(t)\rangle}$

A few words about directional couplers (see more in Kish, Abbott, Granqvist, 2013)

- Due to Rayleigh scattering, in the quasi-static limit (no-wave limit) where KLJN operates, wave-interference based directional couplers do not function.

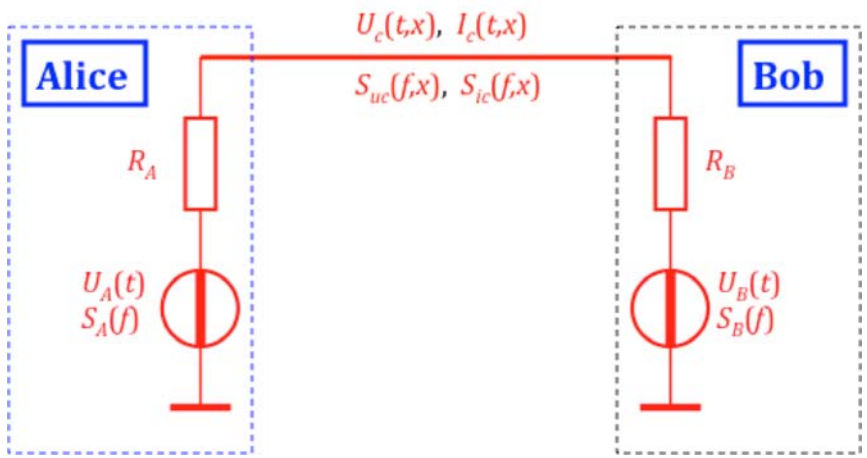
- Directional couplers based on utilizing current/voltage and Kirchhoff law do not work either to the second law and the Gaussianity of KLJN. They would would if Eve would know the resistor allocations however, because she does not know that, her 1 bit uncertainly remains.



A laymen summary. What do Alice and Bob know by the end of bit exchange? Shown in red.

Alice/Bob know the actual resistor choice, for example, by less than 10^{-12} error probability. They also know they own noise history and, by knowing the resistances (and wire parameters), they can deduce the noise history at the other end by linear superposition theory, with a certainty of 10^{-12} . This is: **iKLJN**, KLJN at its best.

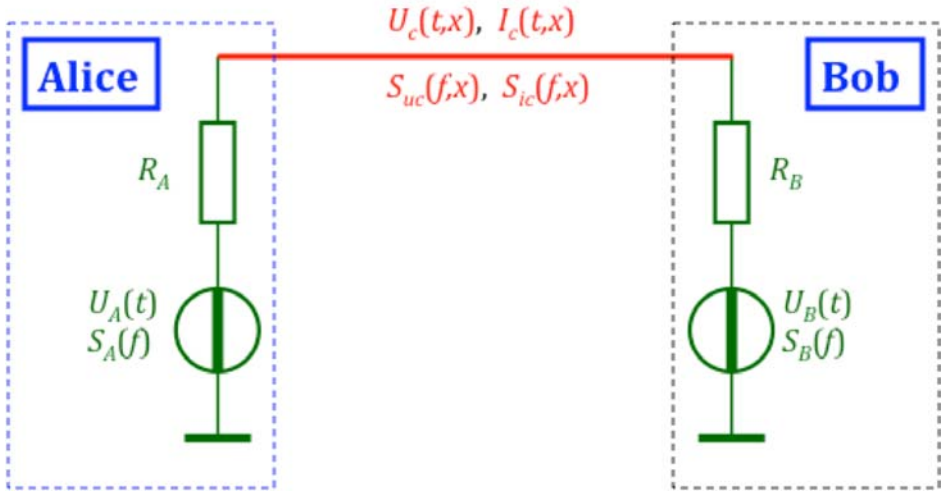
Classical physics is deterministic. They have full knowledge of the noise and resistance history in the system and can agree (via authenticated communications) to drop or keep any of the key bits.



$$\frac{\lambda}{2} << L$$

What does Eve know? Shown in red.

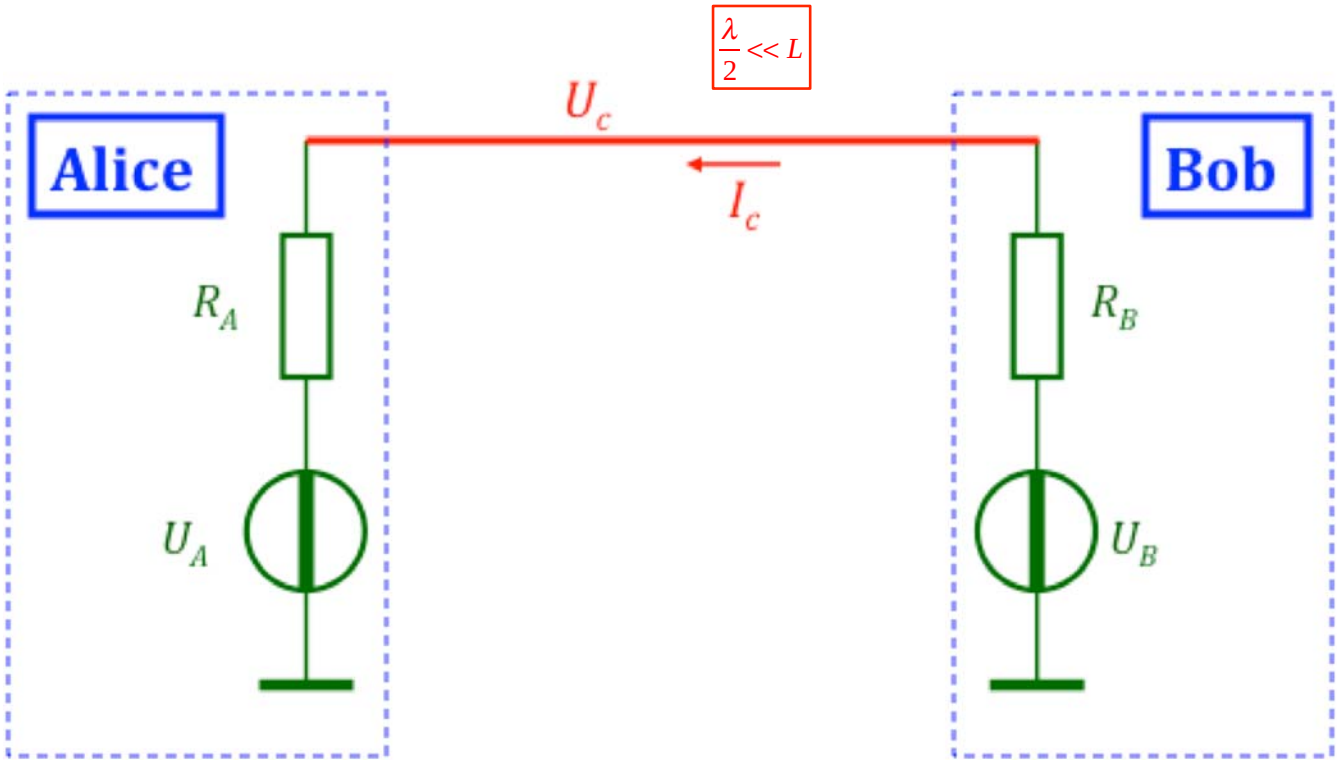
Eve is less fortunate. She knows only the noise history along the wire and the wire parameters. She can identify the 01/10 secure level occurrence, also with 10^{-12} error probability. But in the idealized case, she has 1 bit uncertainty about the actual 01/10 bit arrangement and, in real cases she has almost 1 bit uncertainty about it with success rate p close to 0.5 . Thus she *cannot use linear superposition theory* to deconstruct the superposition in the line to obtain the source voltages at the two ends.



4. Hacking (*à la* Makarov) ?

Hacking possibilities must carefully be analyzed. For example, Makarov-type blinding attacks seem to work at the first look without protocol in place to discard high voltage/current levels, if they equal at the two sides.

However, a more careful study indicates that these particular attacks fail either by the current-protection or voltage protection because of opposite signs of one of these values at the two sides.



5. Attacks and mistakes in the literature: disappointing

Past attacks by other authors have not resulted in any important results because:

i) They were made via violating the basic rules of operation,

ii) Changing the KLJN system,

iii) Misunderstanding the underlying physics and statistics,

iv) Or making fundamental flaws in the assumptions claims or calculations.

But some of them is useful of educational purposes and to deepen the understanding of the KLJN system

Jacob Scheuer, Amnon Yariv "A classical key-distribution system based on Johnson (like) noise—How secure?", PLA 359 (2006) 737–740.

Flaws, and unfortunately, no useful results:

a) Situation 1: Assuming *infinite noise-bandwidth* (Dirac delta autocorrelation function) and/or *infinitely long wire*, they found that Eve can read out the bit from the transient, provided *abrupt switching* is used *without line filters*. *All these are obvious but violates basic conditions of operation:*

i) The noise-bandwidth must be narrow compared to the length of the wire; or:

ii) The wire length must be short (compared to the shortest wavelength in the noise);

iii) At non-zero distance, transients components with short wavelength must be avoided by soft switching and filters and no information should be in the wire before the noises from Alice and Bob get mixed and "thermalized" there.

Jacob Scheuer, Amnon Yariv "A classical key-distribution system based on Johnson (like) noise—How secure?", PLA 359 (2006) 737–740.

Flaws, and unfortunately, no useful results:

b) Situation 2: Assuming narrow noise-bandwidth with short wire, they found that Eve can deterministically read out the bit from the transient, provided *abrupt switching* is used *without line filters*. *This is obvious but it violates a basic condition of operation:*

iii) At non-zero distance, transients components with short wavelength must be avoided by soft switching and filters and no information should be in the wire before the noises from Alice and Bob get mixed and "thermalized" there.

Jacob Scheuer, Amnon Yariv "A classical key-distribution system based on Johnson (like) noise—How secure?", PLA 359 (2006) 737–740.

Flaws, and unfortunately, no useful results:

c) Situation 3: Assuming narrow noise-bandwidth with short wire and *non-zero wire resistance*, they found that Eve can read out the bit from noise-measurements at different points provided *Eve has infinite time for the noise measurement* (hidden assumption).

As we have seen, this situation contradict basic KLJN conditions, where Eve's measurement time is extremely limited. But there is indeed information leak (first pointed out by Kish in his first seminar and Janos Bergou later in the Science magazine feature).

Errors in the their noise-analysis:

- Their current noise spectrum result has energy unit: $\langle S_i(f)\rangle = \dfrac{4kT\left(R_A+R_B\right)}{R_A+R_B+R_{W1}+R_{W2}}$ [Joule]

- Their main result implies: Eve's DC signal $\propto R_w$

The correct result later (Kish, Scheuer, PLA 2010): Eve's DC signal $\propto R_w^2$

Practically, Eve's signal-to-noise ratio is 100-1000 *times smaller*.

Feng Hao, "Kish's key exchange scheme is insecure, IEE Info. Security, 2006.

By assuming that the temperatures are different and (implicitly assuming that the bit exchange duration is infinite) concludes that the KLJN is cracked.

- *The effect and calculations are valid.*

- But the implicit assumption of infinite measurement time violates basic KLJN protocol.

- At practical conditions, such as only 14 bits accuracy for the noise generators setting the temperature, the effect is orders of magnitudes below the measurability limit.

Kish, in response to Feng Hao), FNL, 2006.

Inaccuracies generally provide information leak. The most dangerous effect is the accuracy of the resistors. However, practical accuracy of 1% allows similar success probability and statistical distance as at the studied levels of wire resistance. Basic practical rule of any inaccuracy thumb is to stay at 1% inaccuracy or less.

Pao-Lo Liu, PLA 2009 (two papers)

Among others, produced a very interesting circulator-based KLJN system with active elements. But Kish, Horvath (2009) fully cracked that later.

With a cable simulator showed high success rate of Eve at practical conditions. However, the parameters were shown *highly unphysical*, with cable diameter 28000 times greater than the known diameter of the universe (Kish, Horvath, 2009). Thus the simulator was out of range.

Came up with a software-based emulation of KLJN, which must be crackable because the noise signals propagating in the two directions are separately observable however *it has not been cracked yet*. If you want a great brain teaser, check out his related papers!

On the security of key distribution based on Johnson-Nyquist noise

Charles H. Bennett, C. Jess Riedel
IBM Watson Research Center, Yorktown Heights, NY, USA

(Dated: April 1, 2013)

We point out that arguments for the security of Kish's noise-based cryptographic protocol have relied on an unphysical no-wave limit, which if taken seriously would prevent any correlation from developing between the users. We introduce a noiseless version of the protocol, also having illusory security in the no-wave limit, to show that noise and thermodynamics play no essential role. Then we prove generally that classical electromagnetic protocols cannot establish a secret key between two parties separated by a spacetime region perfectly monitored by an eavesdropper. We note that the original protocol of Kish is vulnerable to passive time-correlation attacks even in the quasi-static limit. Finally we show that protocols of this type can be secure in practice against an eavesdropper with noisy monitoring equipment. In this case the security is a straightforward consequence of Maurer and Wolf's discovery that key can be distilled by public discussion from correlated random variables in a wide range of situations where the eavesdropper's noise is at least partly independent from the users' noise.

Quantum key distribution [1] boasts unconditional security even in the presence of realistic noise [2], and the techniques have matured enough that small commercial implementations have been explored. However, the practical difficulty of manipulating individual quantum states has prompted some investigation into purely classical schemes which might be able to achieve similar ends. In particular, Kish has proposed a strictly classical protocol (Kirchoff Law-Johnson Noise or KLJN) on an insecure transmission line using Johnson-Nyquist noise in

concepts of temperature and noise have been
they play no fundamental role in the proto
mining the recent claim of Kish et al. that th
the KLJN protocol follows from the 2nd law
dynamics [4]. This was already suggested by
observation in reference [3] that artificial n
tors were as good as true Johnson-Nyquist
resistors.

Kish has argued that many cryptograph
(such as quantum key distribution) were ir

PLOS ONE, in press

Critical analysis of the Bennett–Riedel attack on secure cryptographic key distributions via the Kirchhoff-law–Johnson-noise scheme

Laszlo B. Kish , Derek Abbott , Claes G. Granqvist

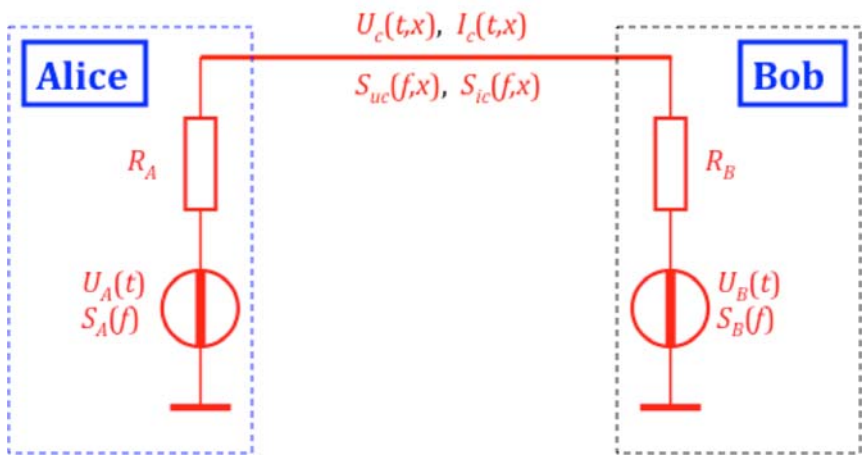
Abstract

Recently, Bennett and Riedel (BR) (http://arxiv.org/abs/1303.7435v1) argued that thermodynamics is not essential in the Kirchhoff-law–Johnson-noise (KLJN) classical physical cryptographic exchange method in an effort to disprove the security of the KLJN scheme. They attempted to demonstrate this by introducing a dissipation-free deterministic key exchange method with two batteries and two switches. In the present paper, we first show that BR's scheme is unphysical and that some elements of its assumptions violate basic protocols of secure communication. All our analyses are based on a technically-unlimited Eve with infinitely accurate and fast measurements limited only by the laws of physics and statistics. For non-ideal situations and at active (invasive) attacks, the uncertainly principle between measurement duration and statistical errors makes it impossible for Eve to extract the key regardless of the accuracy or speed of her measurements. To show that thermodynamics and noise are essential for the security, we crack the BR system with 100% success via passive attacks, in ten different ways, and demonstrate that the same cracking methods do not function for the KLJN scheme that employs Johnson noise to provide security underpinned by the Second Law of Thermodynamics. We also present a critical analysis of some other claims by BR; for example, we prove that their equations for describing zero security do not apply to the KLJN scheme. Finally we give mathematical security proofs for each BR-attack against the KLJN scheme and conclude that the information theoretic (unconditional) security of the KLJN method has not been successfully challenged.

A laymen summary. What do Alice and Bob know by the end of bit exchange? Shown in red.

Alice/Bob know the actual resistor choice, for example, by less than 10^{-12} error probability. They also know they own noise history and, by knowing the resistances (and wire parameters), they can deduce the noise history at the other end by linear superposition theory, with a certainty of 10^{-12} . This is: **iKLJN**, KLJN at its best.

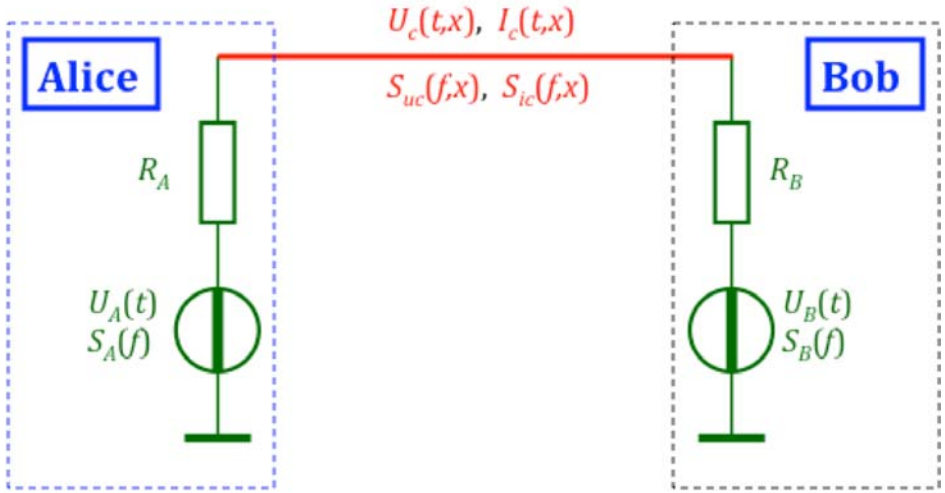
Classical physics is deterministic. They have full knowledge of the noise and resistance history in the system and can agree (via authenticated communications) to drop or keep any of the key bits.



$$\frac{\lambda}{2} << L$$

What does Eve know? Shown in red.

Eve is less fortunate. She knows only the noise history along the wire and the wire parameters. She can identify the 01/10 secure level occurrence, also with 10^{-12} error probability. But in the idealized case, she has 1 bit uncertainty about the actual 01/10 bit arrangement and, in real cases she has almost 1 bit uncertainty about it with success rate p close to 0.5 . Thus she *cannot use linear superposition theory* to deconstruct the superposition in the line to obtain the source voltages at the two ends.



End of presentation

But the story is not over: Lachlan Gunn has just came up with a new scheme which, if really works, will become the most serious hacking attack against KLJN and a 3-stage XOR privacy amplifier would be needed. Watch out for the developments...