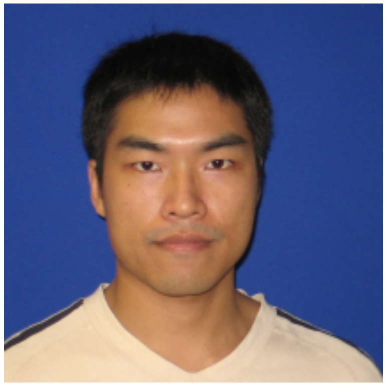
The important thing is not to stop questioning. Curiosity has its own reason for existing. (Albert Einstein)

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*
[2] *Department of Engineering Sciences, The Ångström Laboratory, Uppsala University, Uppsala, Sweden*
[3] *Department of Physical Informatics, University of Szeged, Arpad ter 2, H-6727, Hungary*



Barry

Claes

Robert

Zoltan

We call this system KLJN key exchanger or just KLJN.

Travel to the moon, French movie, from 1902. These 33 seconds are excellent illustration of the ***heat*** of the matter.

- *General comment: there is tremendous "heat" in Security more than in Stochastic Resonance at the* 1990s ☺

- The Kirchhoff-law-Johnson-noise (KLJN) secure key exchanger (2005) is a *classical statistical physical* alternative of quantum key distribution. It killed the dogma that only quantum informatics can offer unconditional security. Its security is based on the Second Law of Thermodynamics (Kish, PLA 2006) and the properties of Gaussian stochastic processes (PLA 2006; Gingl, Mingesz, PLoS ONE 2014). The unconditional security in *non-ideal cases* is maintained by the *continuity of functions describing stable classical physical systems* (Kish, Granqvist, Quantum Info. Proc. 2014).

- Since its creation, KLJN has often been exposed to some *incorrect science and fights*. This talk shows a few essential points and the currently most important unsolved problems.

- In the 2008-2013 period it had a poor quality *Wikipedia* site named *Kish cypher*, where the most annoying factor was the KLJN-supporters naivety, however the anonymous quantum-info supporters football-fun mentality was also interesting.

- 3 books entitled "Kish cypher" were published as wikipedia printouts and 3 more books with the same chapter title based also on wikipedia. They claims were fluctuating depending on the actual state of the wiki page made by the KLJN supporters or quantum supporters. This situation forced me into a book contract with the same title where the truth will be given.

- In March 2012, I officially requested the deletion of the Kish cypher wiki site but got denied. In the April of 2013, when Charles Bennett quantum-info founder emerged as main opponent, the quantum-info supporters also proposed the deletion and then the page got terminated.

- To prohibit that again such an unprofessional information source run by anonymous people emerges, a *Scholarpedia* site was created about the KLJN system with the kind help of *Derek Abbott* and *Gabor Schmera*, where the basic features are correctly outlined.

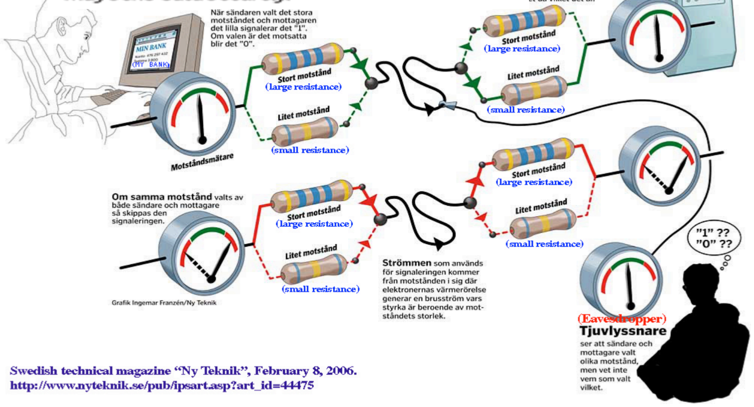
Kirchhoff-Law-Johnson-Noise (KLJN)

secure key exchange

(first scheme: 2005)

Stealth technology. A simple wire and resistors may send data securely.

Science Magazine, 2005
featuring article in arXive


eiver)
ttagare
garen ser på mätaren att
ren valt ett annat motstånd
et då vilket det är.
När sändaren valt det stora motståndet och mottagaren det lilla signalerar det "1". Om valen är det motsatta blir det "0".
MIN BANK
(MY BANK)
Stort motstånd
(large resistance)
Litet motstånd
(small resistance)
Motståndsmätare
Stort motstånd
(large resistance)
Litet motstånd
(small resistance)
Om samma motstånd valts av både sändare och mottagare så skippas den signaleringen.
Stort motstånd
(large resistance)
Litet motstånd
(small resistance)
Stort motstånd
(large resistance)
Litet motstånd
(small resistance)
Strömmen som används för signaleringen kommer från motstånden i sig där elektronernas värmerörelse generar en brusström vars styrka är beroende av motståndets storlek.
"1" ??
"0" ??
(Eavesdropper)
Tjuvlyssnare
ser att sändare och mottagare valt olika motstånd, men vet inte vem som valt vilket.
Grafik Ingemar Franzén/Ny Teknik

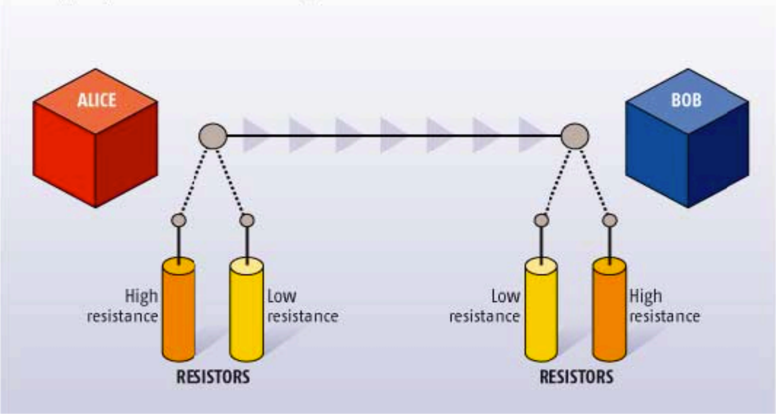
Swedish technical magazine "Ny Teknik", February 8, 2006.
http://www.nyteknik.se/pub/ipsart.asp?art_id=44475

Ny Teknik, 2005

New Scientist, 2007

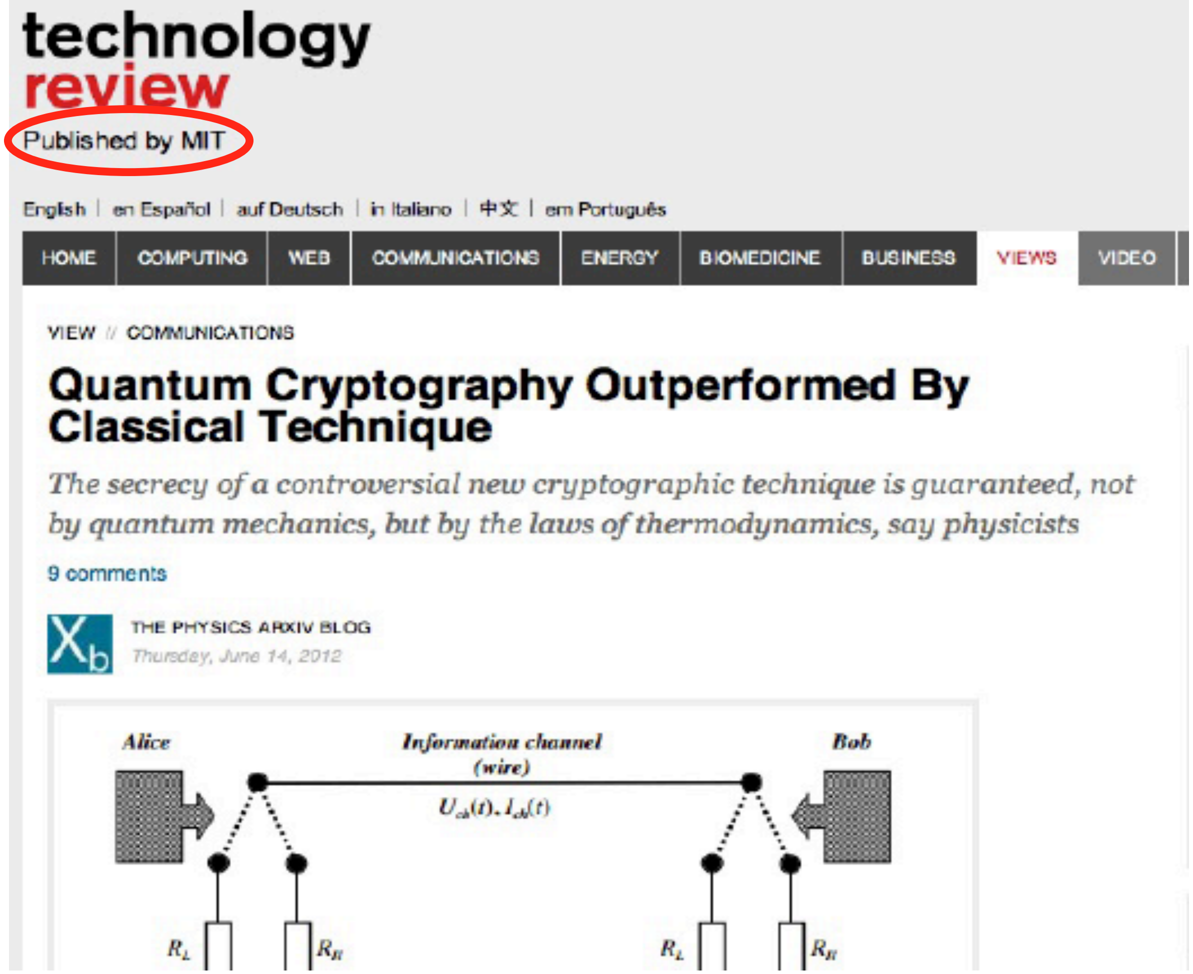
NOISE ENCRYPTION

Alice and Bob communicate securely along a fixed line by randomly choosing which resistor to use. If both choose high resistors, a high level of noise is produced on the line. If both choose low resistors, the noise level is low. In both situations the communication is void. However, half the time Alice and Bob will choose different resistors, producing an intermediate level of noise on the line. When that happens, a bit of information is sent, as Bob knows Alice must have chosen the other resistor to his



In 2012, the arXiv manuscript of my plenary talk at the IEEE 5th International Conference on Soft Computing Applications (2012) was featured by MIT Technology Review and other media.

Result: *all my arXiv endorsement rights were revoked* with no explanation, even when inquired about reasons.



VIEW // COMMUNICATIONS

Quantum Cryptography Outperformed By Classical Technique

The secrecy of a controversial new cryptographic technique is guaranteed, not by quantum mechanics, but by the laws of thermodynamics, say physicists

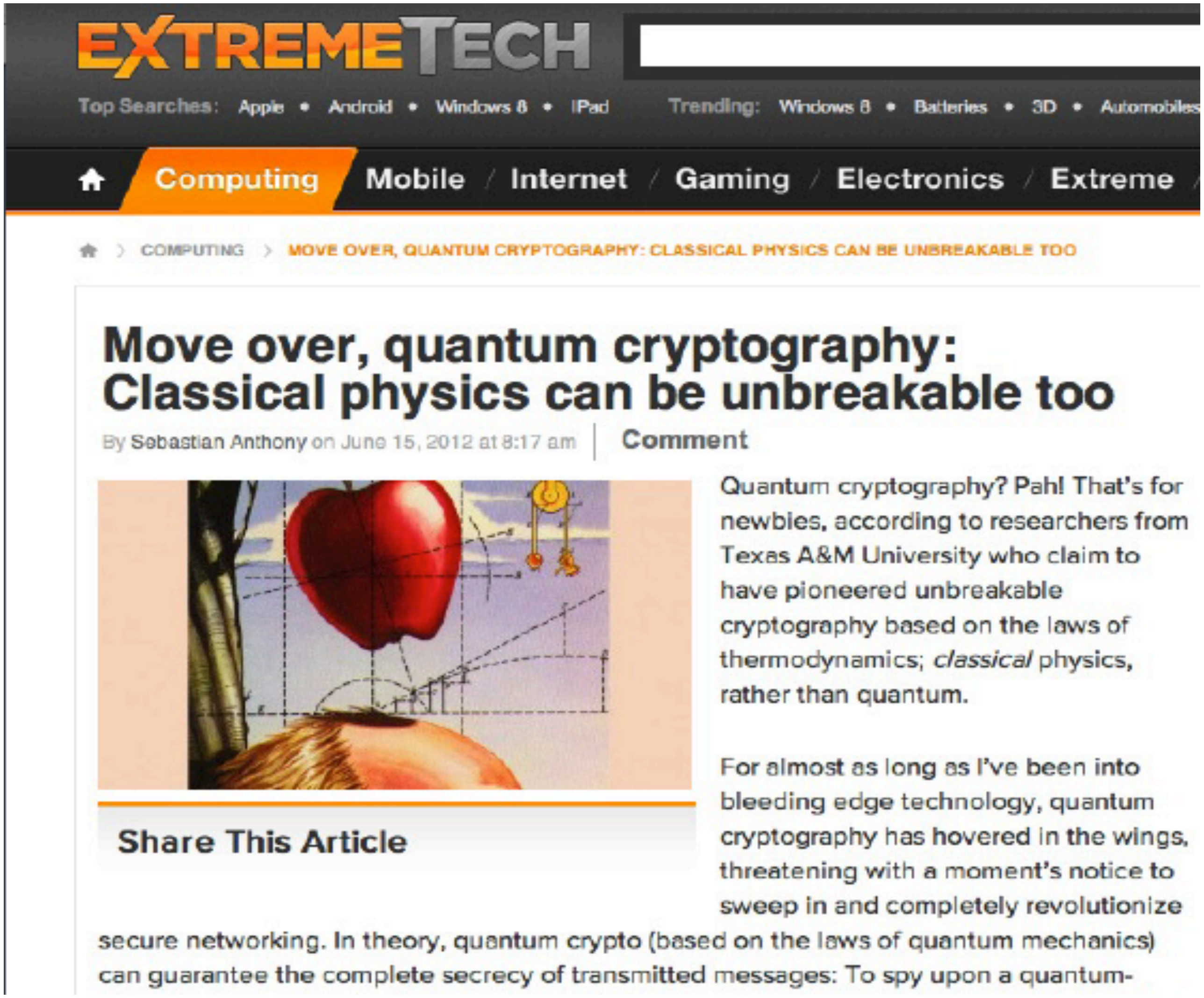
9 comments

THE PHYSICS ARXIV BLOG

Thursday, June 14, 2012

In 2012, the arXiv manuscript of my plenary talk at the IEEE 5th International Conference on Soft Computing Applications (2012) was featured by MIT Technology Review and other media.

Result: *all my arXiv endorsement rights were revoked* with no explanation, even when inquired about reasons.

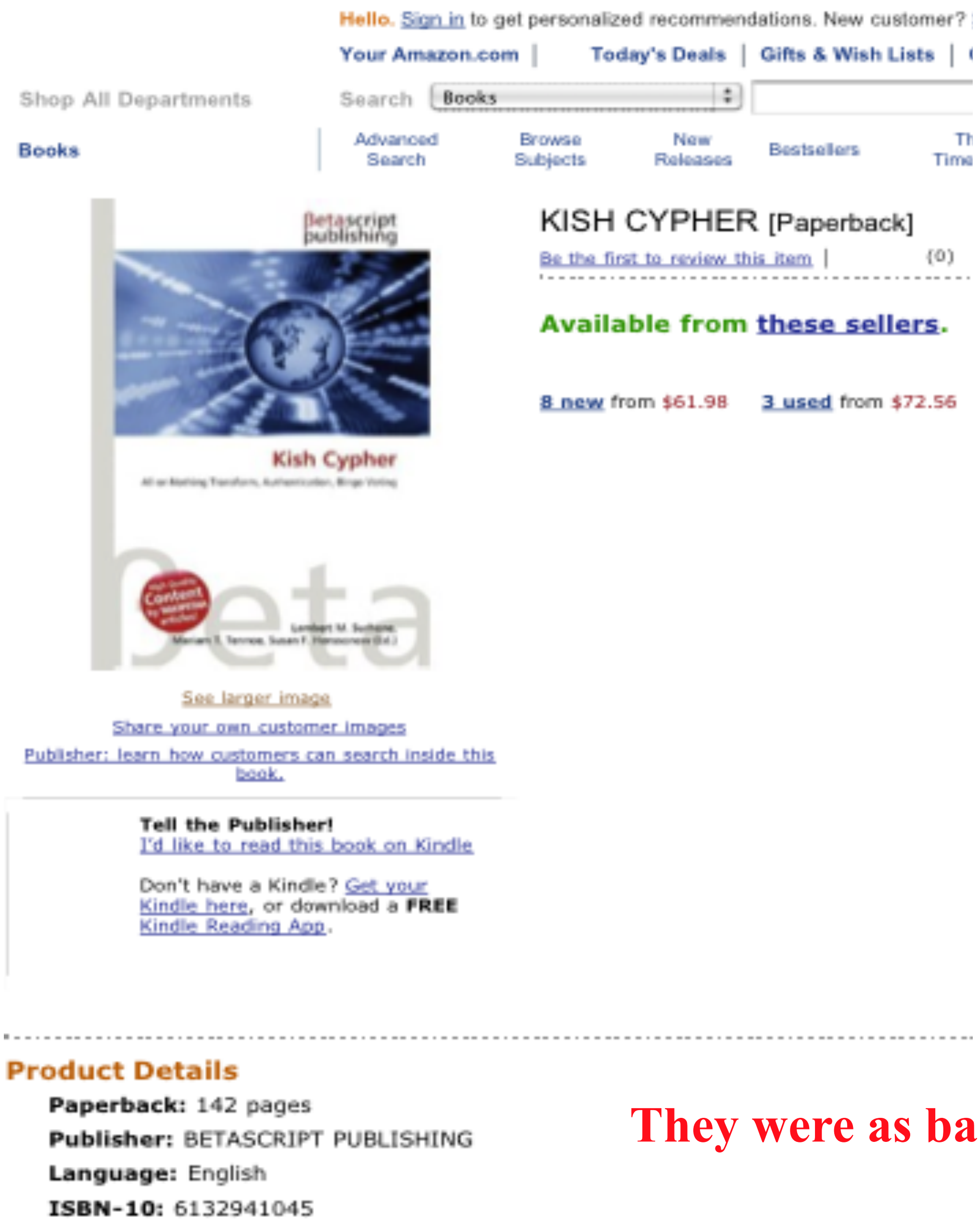

EXTREMETECH
Top Searches: Apple • Android • Windows 8 • iPad
Trending: Windows 8 • Batteries • 3D • Automobiles
Computing
Mobile
Internet
Gaming
Electronics
Extreme
COMPUTING
MOVE OVER, QUANTUM CRYPTOGRAPHY: CLASSICAL PHYSICS CAN BE UNBREAKABLE TOO
Comment
Share This Article

Move over, quantum cryptography: Classical physics can be unbreakable too

By Sebastian Anthony on June 15, 2012 at 8:17 am

Quantum cryptography? Pah! That's for newbies, according to researchers from Texas A&M University who claim to have pioneered unbreakable cryptography based on the laws of thermodynamics; *classical* physics, rather than quantum.

For almost as long as I've been into bleeding edge technology, quantum cryptography has hovered in the wings, threatening with a moment's notice to sweep in and completely revolutionize secure networking. In theory, quantum crypto (based on the laws of quantum mechanics) can guarantee the complete secrecy of transmitted messages: To spy upon a quantum-



Hello. Sign in to get personalized recommendations. New customer?

Your Amazon.com | Today's Deals | Gifts & Wish Lists |

Shop All Departments

Search Books

Books | Advanced Search | Browse Subjects | New Releases | Bestsellers | Th Time

See larger image

Share your own customer images

Publisher: learn how customers can search inside this book.

KISH CYPHER [Paperback]

Be the first to review this item | (0)

Available from these sellers.

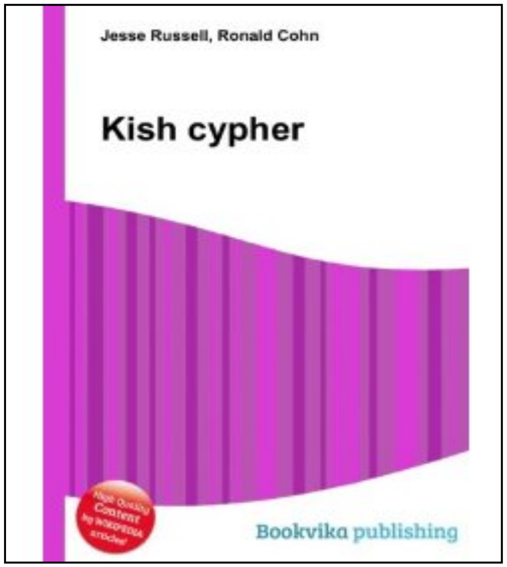
8 new from $61.98   3 used from $72.56

Tell the Publisher!
I'd like to read this book on Kindle

Don't have a Kindle? Get your Kindle here, or download a **FREE** Kindle Reading App.

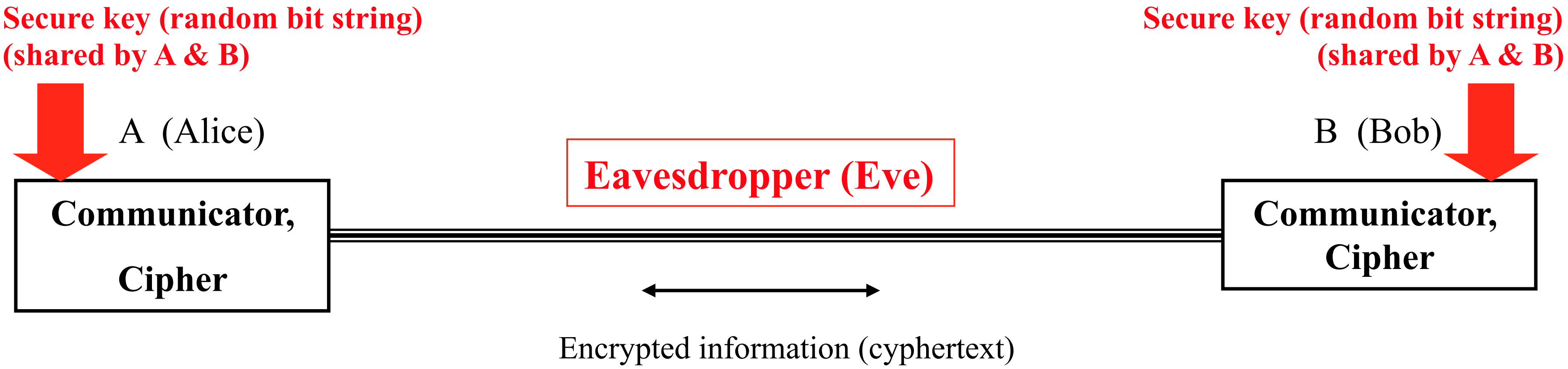
Product Details

Paperback: 142 pages
Publisher: BETASCRIPT PUBLISHING
Language: English
ISBN-10: 6132941045


Jesse Russell, Ronald Cohn
Kish cypher
High Quality Content by WIKIPEDIA articles!
Bookvika publishing

They were as bad as Kish cypher on Wikipedia

Symmetric-key secure communication



Secure key (random bit string)
(shared by A & B)

A (Alice)

Communicator,
Cipher

Eavesdropper (Eve)

Encrypted information (cyphertext)

Secure key (random bit string)
(shared by A & B)

B (Bob)

Communicator,
Cipher

- ***But how to share the secret key securely through the line when Eve is watching?***
- ***The generating/sharing of the secret key is itself a secure communication.***
- **Is there an unconditionally secure way to share the key?**

Some basic definitions

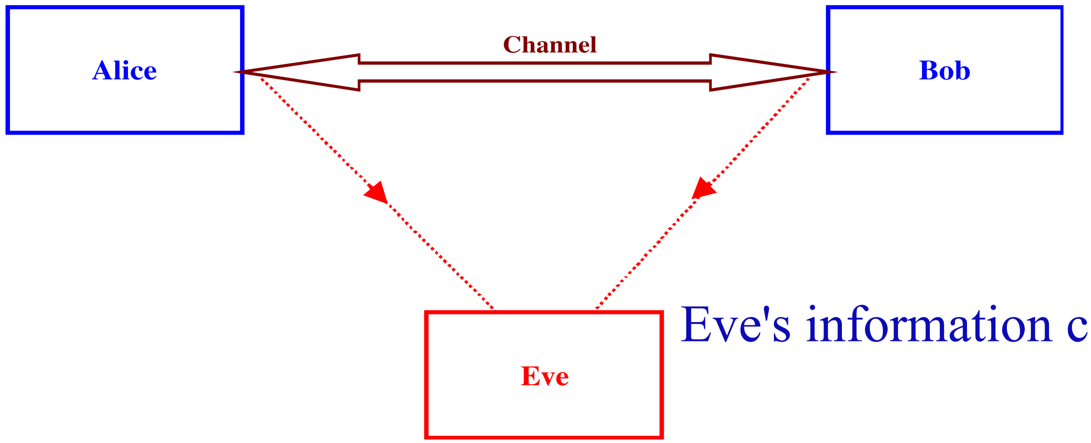
Information-theoretic (unconditional) security: At legal operations, the eavesdropper (Eve) is limited by information theory and not by her resources to extract information. In other words: *the information is simply not there for Eve*. Such security is **future-proof** because advancing Eve's technology cannot help.

Where **Legal operation:** The laws of physics and the rules set by the communicators Alice and Bob are fulfilled. For example, the energy conservation law is not violated and the eavesdropper cannot physically access and open the communicators.

Conditional security: The eavesdropper (Eve) is limited by her resources to extract information. In other words: all the information is there for Eve but her *current* resources are not enough to extract it. For example: today's software-based computationally secure communications, which offer **zero security** provided enough computational power or time is available. Such security is **not future-proof**.

Security by the laws of physics (classical or quantum)

Physical secure key exchange



Eve's information contained by **Measurement Data.**

Suppose Independent, Identically Distributed (I.I.D.) random variables, which KLJN offers.

Eve will use the measurement data to guess the key bit. Her success probability is p.

$p = 1$ means total success by Eve which means **Zero Security**

$p = 0.5$ corresponds to a random coin, which means **Perfect Security**

$0.5 < p < 1$ is **Imperfect Security** (common for all practical physical system)

Unconditional security for these systems: If Alice/Bob has sufficient resources then $p \longrightarrow 0.5$

I.I.D. Eve's potential information about the key. *p* is Eve's probability of successful guessing the key bits.

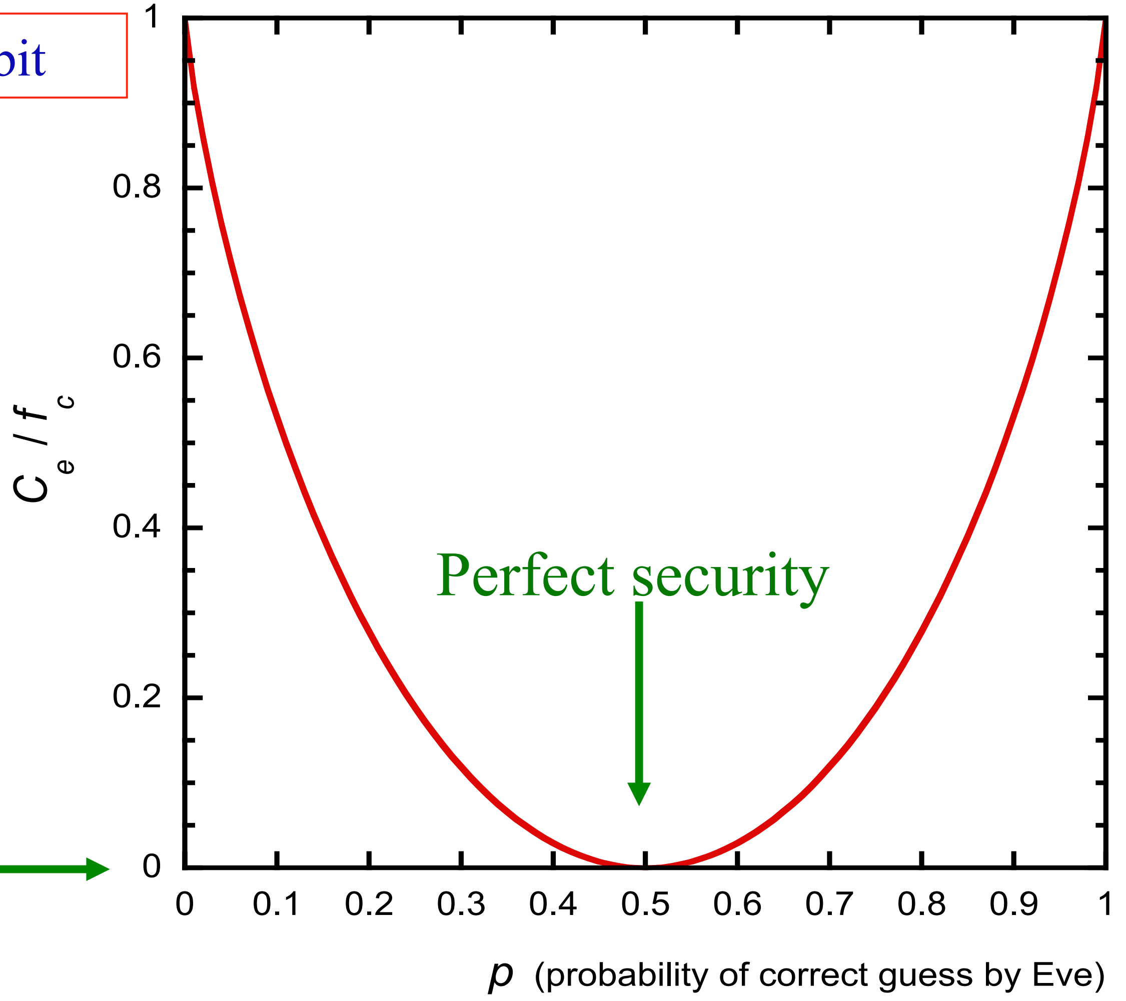
Shannon's binary channel capacity:

$$\boxed{C_e = f_c\left[1 + p\log_2 p + (1-p)\log_2(1-p)\right] \quad \text{bit/s}}$$

$$\boxed{p = 0.5006 \longrightarrow C_e/f_c = 10^{-8} \text{ bit}}$$

Eve's max information about the key that she may extract from a single key bit

Perfect security →

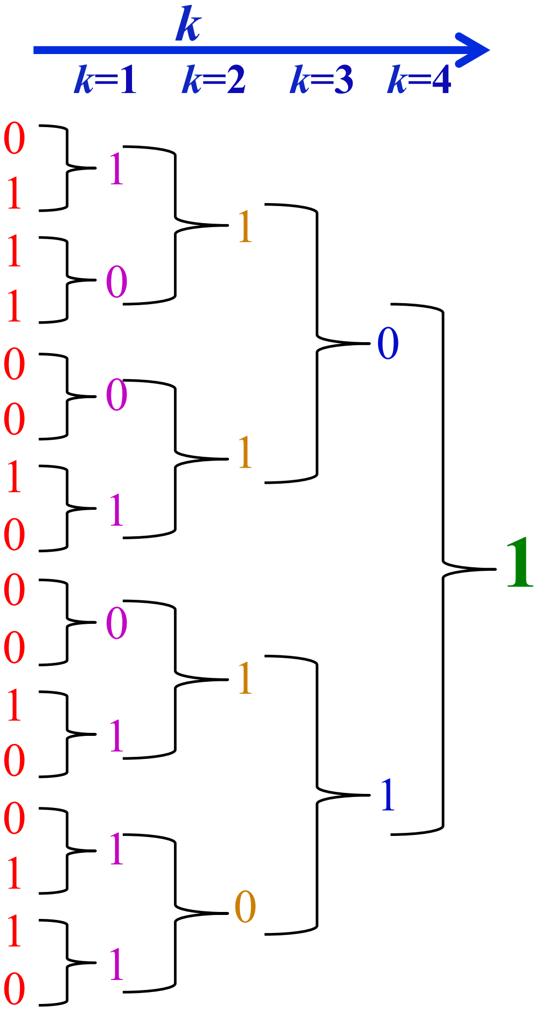


Unconditional security for physical systems: If Alice/Bob has sufficient resources then ***p* → 0.5**

Privacy amplifier: invented for quantum encryption: **the used resource is time. From a long key it makes a short key with improved security. A simple privacy amplifier by XOR-ing the pairs of key bits is studied in:**

T. Horvath, L.B. Kish, J. Scheuer, "Effective Privacy Amplification for Secure Classical Communications", EPL 94 (2011) 28002; http://arxiv.org/abs/1101.4264

$p = 0.5006$ → $C_e/f = 10^{-8}$ ***Practically Perfect Security***



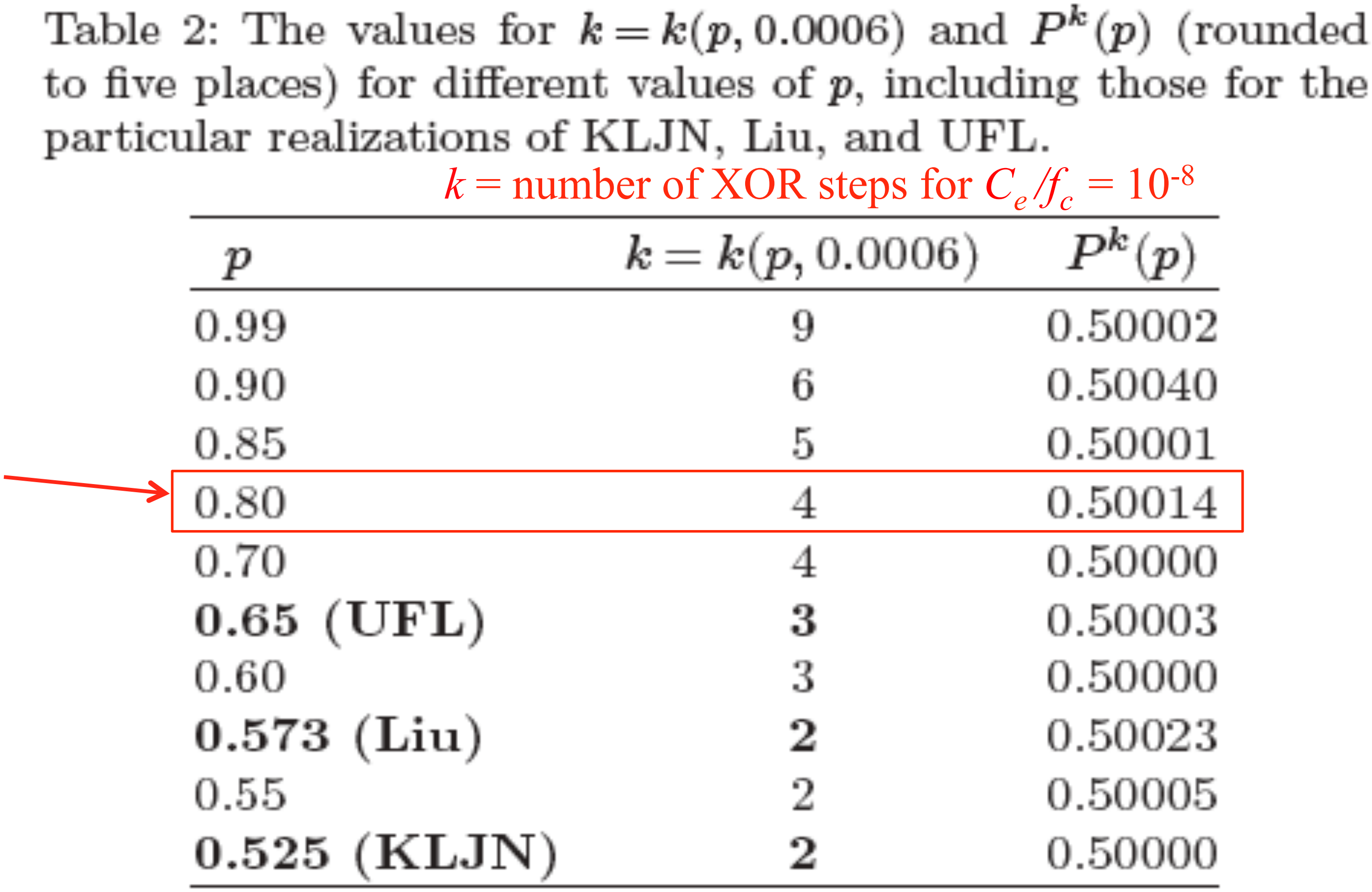


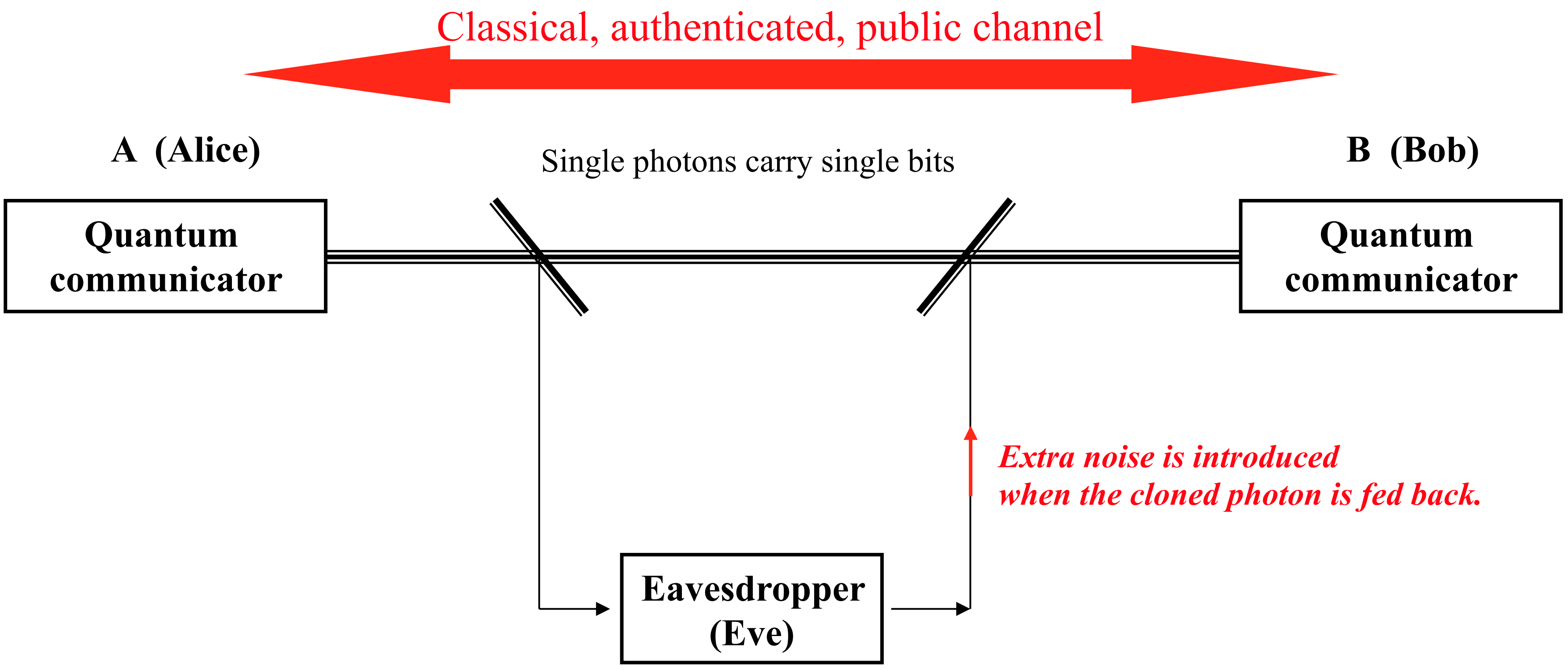
Table 2: The values for $k = k(p, 0.0006)$ and $P^k(p)$ (rounded to five places) for different values of p, including those for the particular realizations of KLJN, Liu, and UFL.

k = number of XOR steps for $C_e/f_c = 10^{-8}$

p	$k = k(p, 0.0006)$	$P^k(p)$
0.99	9	0.50002
0.90	6	0.50040
0.85	5	0.50001
0.80	4	0.50014
0.70	4	0.50000
0.65 (UFL)	**3**	0.50003
0.60	3	0.50000
0.573 (Liu)	**2**	0.50023
0.55	2	0.50005
0.525 (KLJN)	**2**	0.50000

Generic quantum communicator scheme (for quantum key distribution)

Base of security: quantum no-cloning theorem: copies of single photons will be noisy.
After making a sufficient error statistics, the eavesdropping can be discovered.



Classical, authenticated, public channel

A (Alice)

Quantum communicator

Single photons carry single bits

B (Bob)

Quantum communicator

Extra noise is introduced
when the cloned photon is fed back.

Eavesdropper (Eve)

Ongoing debates about the security of quantum key distribution (QKD)

Fundamental/conceptual problems:

Horace Yuen: variables are not I.I.D. due to error correction thus security measures and proofs are not satisfactory

permission:
Horace Yuen

Practical problems (hacking):

Vadim Makarov: real device non-idealities compromise security and offer ways for a 100% crack by hacking. They cracked all the commercial quantum communicators and practical schemes.

permission:
Vadim Makarov

Debates about the security of quantum key distribution (QKD) until 2012

Challenging the concept of QKD security; Response to fundamental challenges; 100% cracks (hacking) of practical/commercial QKD

1. **Yuen HP (2012) On the foundations of quantum key distribution — Reply to Renner and beyond, arXiv:1210.2804.**
2. **Hirota O (2012) Incompleteness and limit of quantum key distribution theory, arXiv:1208.2106v2.**
3. **Renner R (2012) Reply to recent scepticism about the foundations of quantum cryptography, arXiv:1209.2423v.1.**
4. **Merali Z (29 August 2009) Hackers blind quantum cryptographers. Nature News, DOI:10.1038/news.2010.436.**
5. **Gerhardt I, Liu Q, Lamas-Linares A, Skaar J, Kurtsiefer C, Makarov V (2011) Full-field implementation of a perfect eavesdropper on a quantum cryptography system. Nature Commun. 2; article number 349. DOI: 10.1038/ncomms1348.**
6. **Lydersen L, Wiechers C, Wittmann C, Elser D, Skaar J, Makarov V (2010) Hacking commercial quantum cryptography systems by tailored bright illumination. Nature Photonics 4:686-689. DOI: 10.1038/NPHOTON.2010.214.**
7. **Gerhardt I, Liu Q, Lamas-Linares A, Skaar J, Scarani V, Makarov V, Kurtsiefer C (2011) Experimentally faking the violation of Bell's inequalities. Phys. Rev. Lett. 107:170404. DOI: 10.1103/PhysRevLett.107.170404.**
8. **Makarov V, Skaar J (2008) Faked states attack using detector efficiency mismatch on SARG04, phase-time, DPSK, and Ekert protocols. Quantum Inf. Comp. 8:622-635.**
9. **Wiechers C, Lydersen L, Wittmann C, Elser D, Skaar J, Marquardt C, Makarov V, Leuchs G (2011) After-gate attack on a quantum cryptosystem. New J. Phys. 13:013043. DOI: 10.1088/1367-2630/13/1/013043.**
10. **Lydersen L, Wiechers C, Wittmann C, Elser D, Skaar J, Makarov V (2010) Thermal blinding of gated detectors in quantum cryptography. Opt. Express 18:27938-27954. DOI: 10.1364/OE.18.027938.**
11. **Jain N, Wittmann C, Lydersen L, Wiechers C, Elser D, Marquardt C, Makarov V, Leuchs G (2011) Device calibration impacts security of quantum key distribution. Phys. Rev. Lett. 107:110501. DOI: 10.1103/PhysRevLett.107.110501.**
12. **Lydersen L, Skaar J, Makarov V (2011) Tailored bright illumination attack on distributed-phase-reference protocols. J. Mod. Opt. 58:680-685. DOI: 10.1080/09500340.2011.565889.**
13. **Lydersen L, Akhlaghi MK, Majedi AH, Skaar J, Makarov V (2011) Controlling a superconducting nanowire single-photon detector using tailored bright illumination. New J. Phys. 13:113042. DOI: 10.1088/1367-2630/13/11/113042.**
14. **Lydersen L, Makarov V, Skaar J (2011) Comment on "Resilience of gated avalanche photodiodes against bright illumination attacks in quantum cryptography". Appl. Phys. Lett. 99:196101. DOI: 10.1063/1.3658806.**
15. **Sauge S, Lydersen L, Anisimov A, Skaar J, Makarov V (2011) Controlling an actively-quenched single photon detector with bright light. Opt. Express 19:23590-23600.**
16. **Lydersen L, Jain N, Wittmann C, Maroy O, Skaar J, Marquardt C, Makarov V, Leuchs G (2011) Superlinear threshold detectors in quantum cryptography. Phys. Rev. Lett. 84:032320. DOI: 10.1103/PhysRevA.84.032320.**
17. **Lydersen L, Wiechers C, Wittmann C, Elser D, Skaar J, Makarov V (2010) Avoiding the blinding attack in QKD; Reply (Comment). Nature Photonics 4:801-801. DOI: 10.1038/nphoton.2010.278.**
18. **Makarov V (2009) Controlling passively quenched single photon detectors by bright light. New J. Phys. 11:065003. DOI: 10.1088/1367-2630/11/6/065003.**

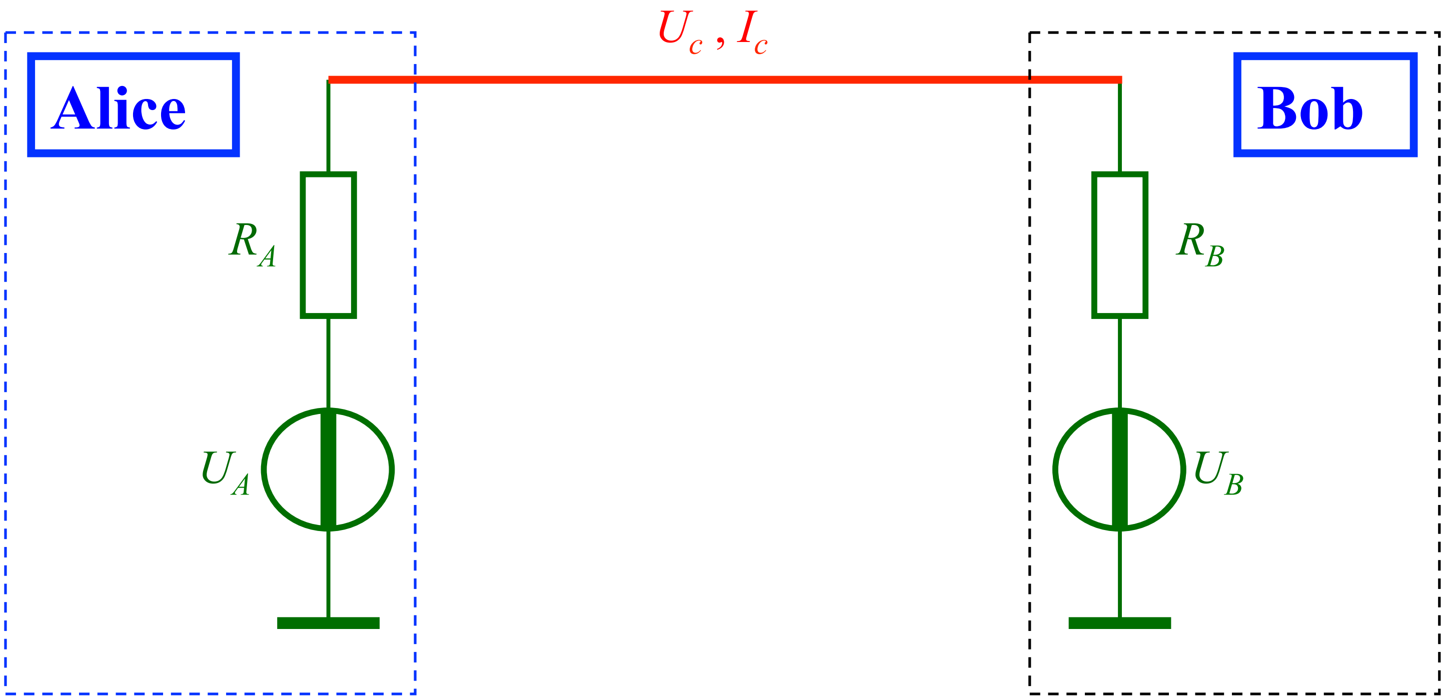
Pedestrian approach (original idea and failure, in July, 2005)

Secrets: R_A, U_A, R_B, U_B (continuum random numbers)

Public (measurements): U_c, I_c $\longrightarrow$ ***number of equations* = 2,**

Not enough for Eve to determine 4 unknown parameters!

But maybe enough for Alice and Bob to determine the 2 unknown parameters at the other end!

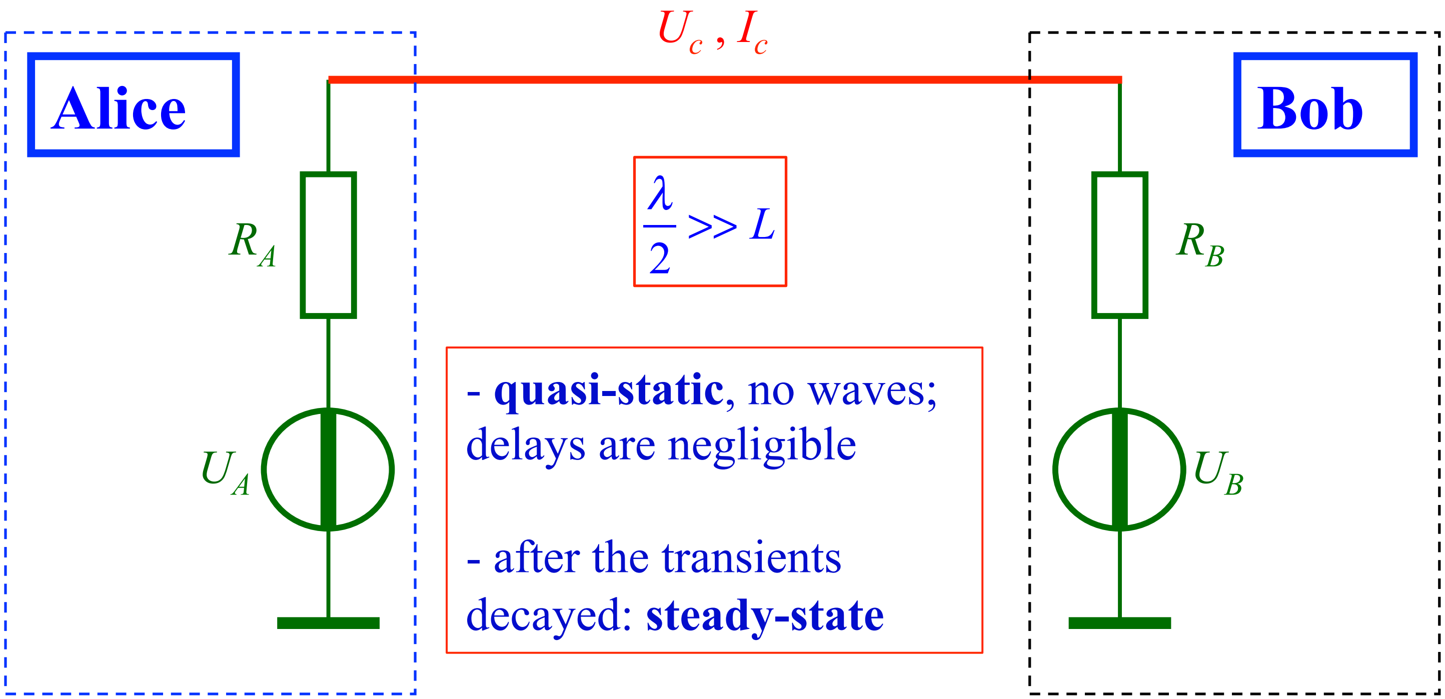


Pedestrian approach: the solution, Kirchhoff-law-Johnson-Noise (KLJN) system

The equations are not independent! The scheme is "too secure", even Alice and Bob cannot share their secret. Proper relation is needed between the voltage and resistor.

Johnson noise, publicly know common temperature!

For example, Alice and Bob can determine the total loop resistance $R_L = R_A + R_B$ as the current noise spectrum in the channel is $\boldsymbol{S_i = 4kT/R_L}$. Thus Alice uses $\boldsymbol{R_B = R_L - R_A}$, and Bob uses $\boldsymbol{R_A = R_L - R_B}$



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

- **quasi-static**, no waves; delays are negligible

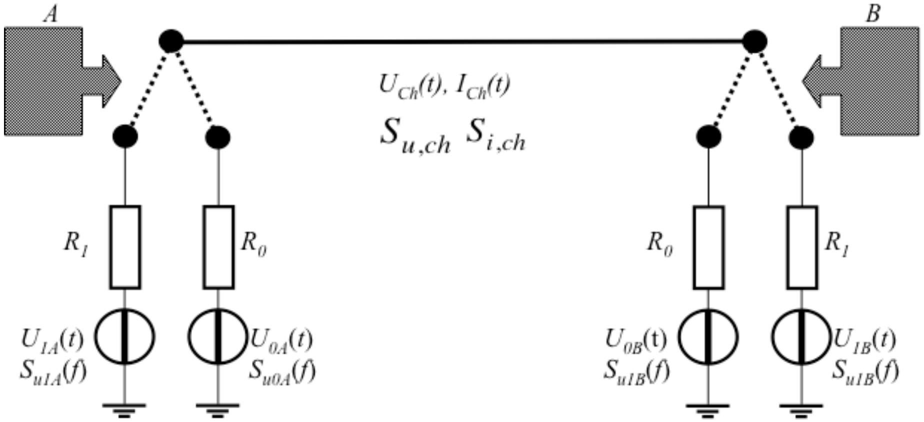
- after the transients decayed: **steady-state**

Eavesdropper's Passively Observed/Extracted Information: Resistance values but *not their locations*

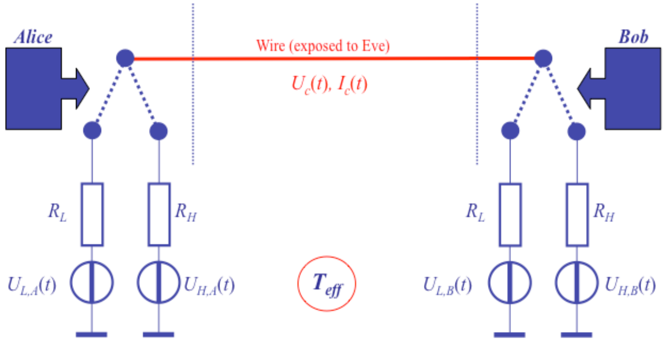
$$\boxed{R_{1,2} = \frac{4kTS_{u,ch} \pm \sqrt{\left(4kTS_{u,ch}\right)^2 - 4S_{u,ch}^3 S_{i,ch}}}{2S_{u,ch} S_{i,ch}}}$$

No more information for Eve in the ideal system at the steady state due to the Gaussianity and the Second Law guaranteeing zero cross-correlation between the channel voltage and current.

(see also Gingl-Mingesz, PLOS ONE, 2014)



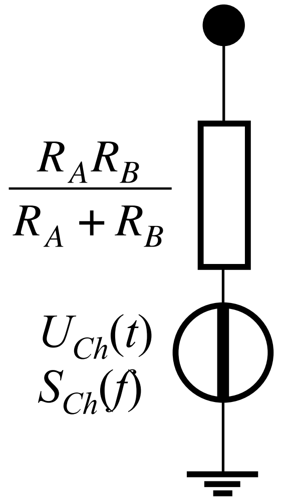
Binary KLJN: identical resistor pairs at Alice and Bob. As in the analog KLJN, the loop resistance can be evaluated by measuring the thermal noise in two different ways

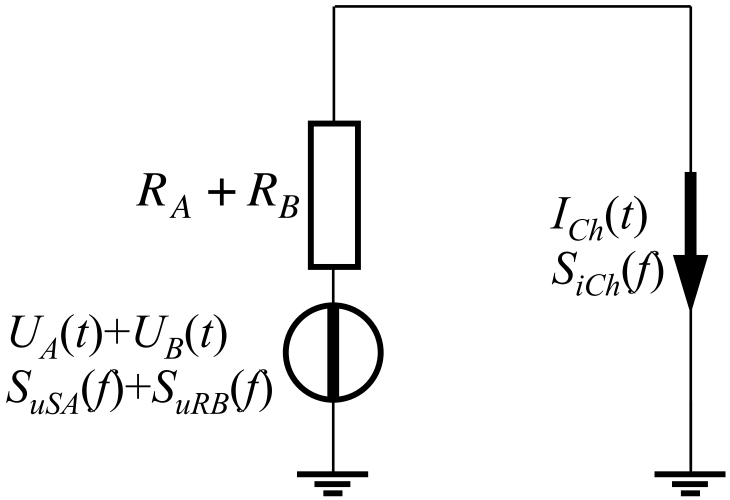


Voltage and current Johnson-Nyquist formulas for this loop:

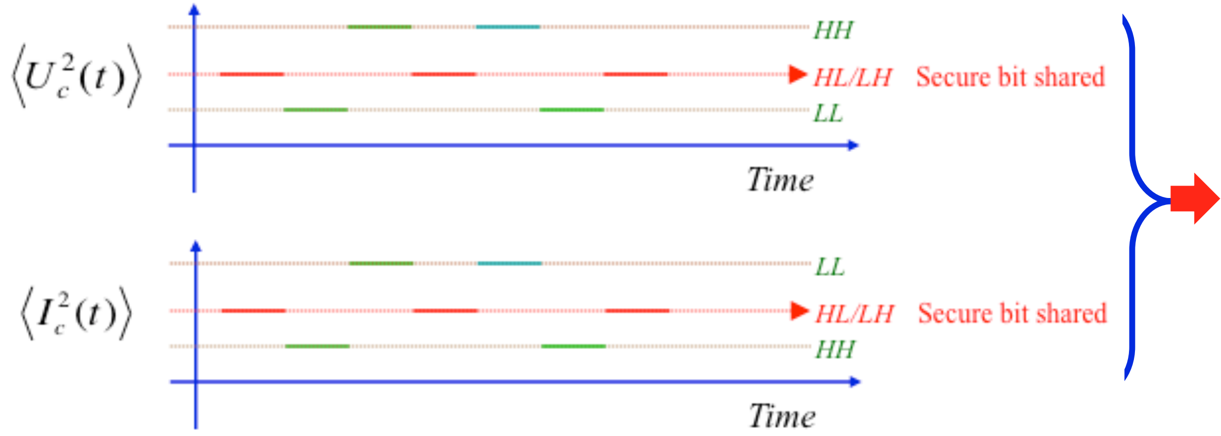
$$\boxed{S_{u,R\parallel}(f) = 4kT\,\frac{R_A R_B}{R_A + R_B}}$$

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





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.

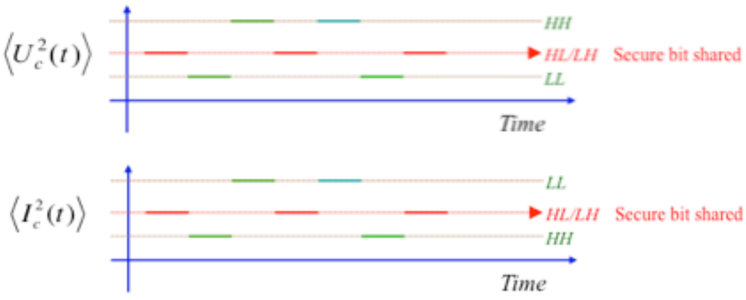


OBSERVE:

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

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

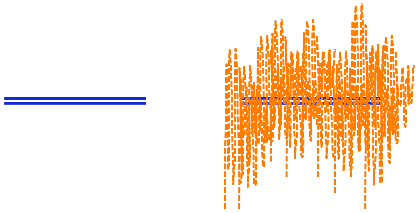
Passive attacks via non-ideal elements (wire resistance, capacitance, inaccuracies, etc).



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

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

split secure levels in large noise:
non-zero information leak

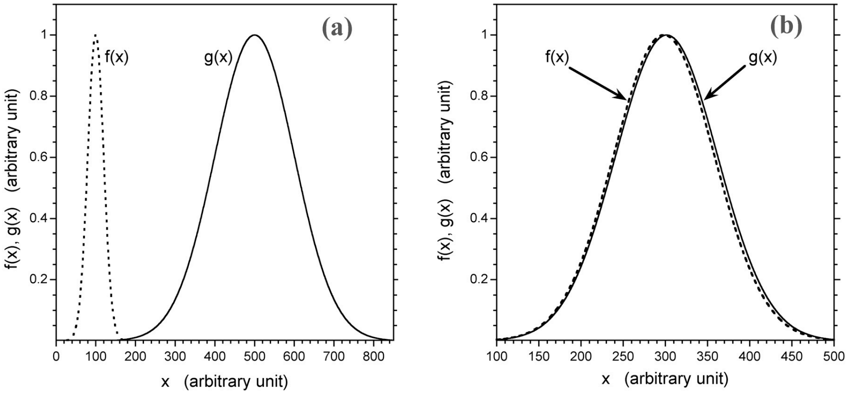


poor statistics for Eve!

Example: the wire-resistance attack: Mingesz, at at, PLA (2008) p=0.525 for Eve, while Alice's/Bob's error probability can be 10^{-20}

Alice/Bob
distinguish 01/10 vs 00 and 11

Eve
tries to separate 01 from 10
(split is enhanced for visibility)



small sample number (100 or less) due to Nyquist's sampling theorem !

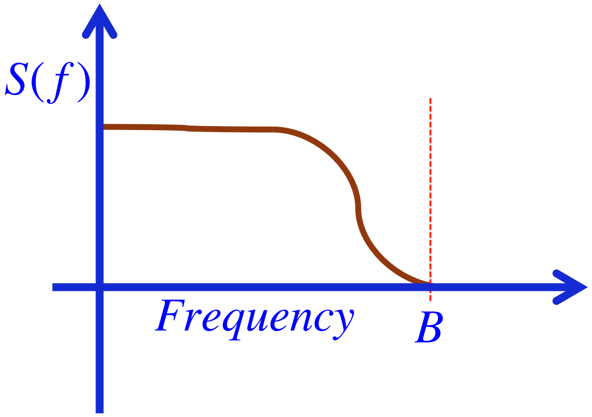
Huge error probability for Eve, p ➔ 0.5

The most important factor neglected by the Bennett-Riedel attack (and by others who ignore this):

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 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*

$$n \le 2B\tau$$

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

During τ duration, the measurement serves only with $n \le 2B\tau$ 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.

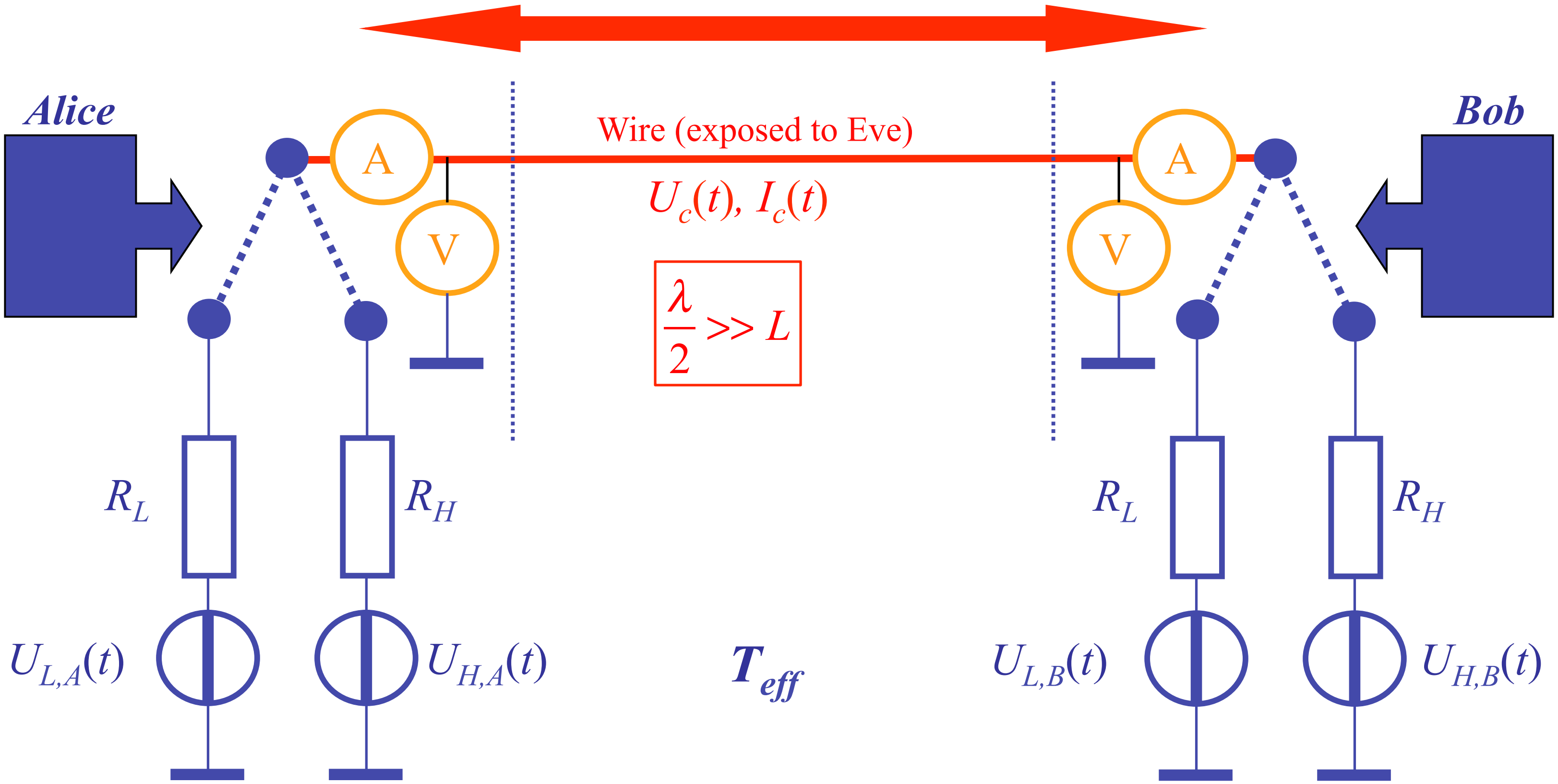
Eve's only way to extract information is to make statistics of the noise under *invasive (active) attacks* or by exploiting *non-ideal features* utilize *second-(or higher)-order effects*, which are however inefficient with small sample numbers.

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. Advanced models use a whole-cable model and random checking of integrity, too. **All these are possible because it is classical physics, not quantum.**

Instantaneous amplitude comparison by Alice and Bob via **authenticated public channel**

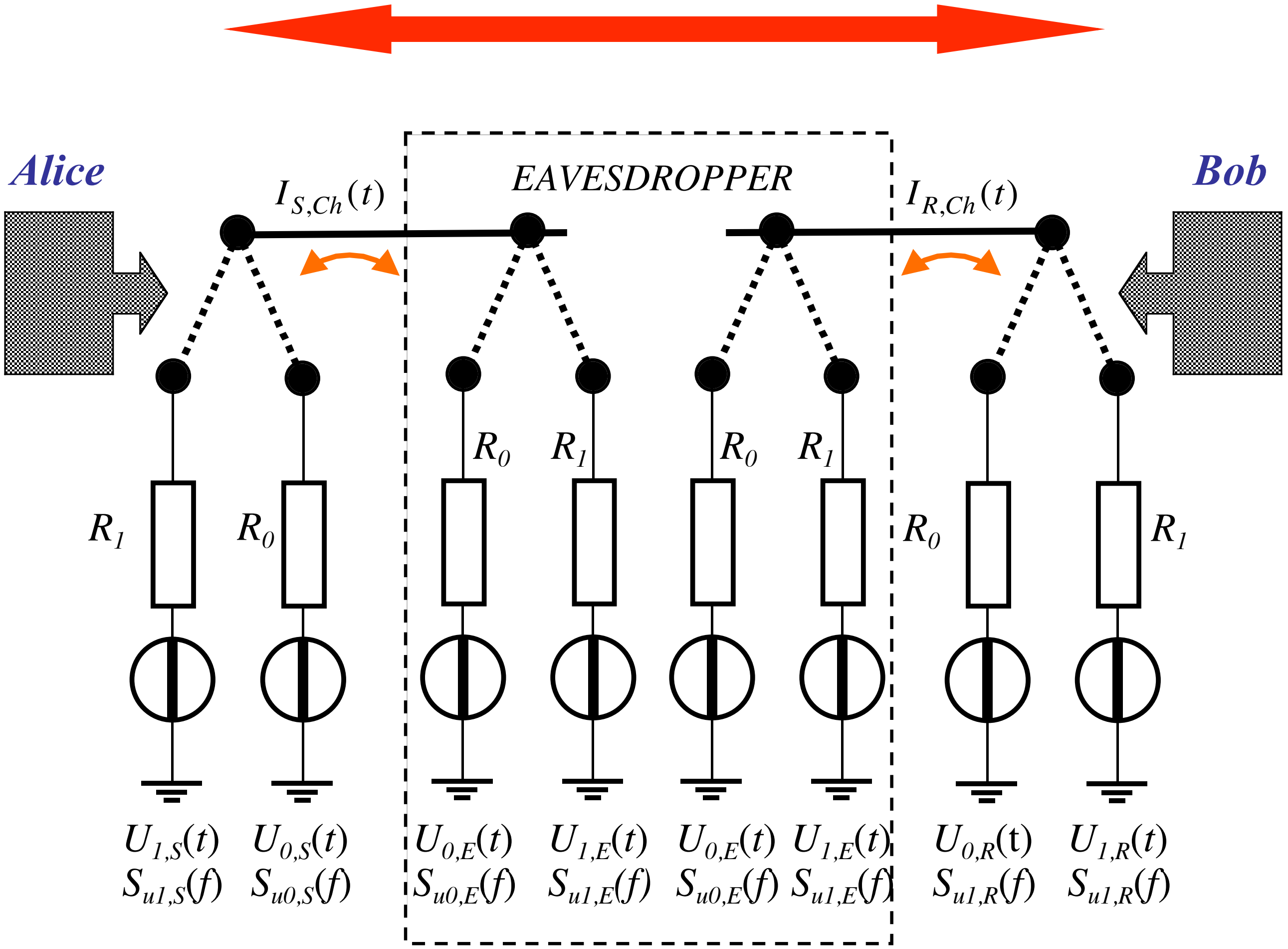
$\log_2 N$ secure bits are used for the exchange of N authenticated bits



Example: natural immunity against the *Man-in-the-middle-attack*

Instantaneous amplitude comparison by Alice and Bob via **authenticated public channel**

$\log_2 N$ secure bits are used for the exchange of N authenticated bits



Quick Conclusions: Summary of known facts, and some UPoN questions

- The ideal KLJN concept is the one represented by the circuitry. It offers ***perfect information-theoretic (unconditional) security*** against both passive and active (invasive) attacks; p=0.5

- The real (non-ideal) KLJN system offers ***practical unconditional security*** in the way it is claimed for quantum encryption: if sufficient resources are available for Alice and Bob (*time is enough – privacy amplification*) , the perfect information-theoretic security can arbitrarily be approached, p ➔ 0.5. This holds against both passive and active attacks because Alice/Bb's ultra-low error probability makes privacy amplification fashionable, more more than for QKD.

UPoN: transient attacks?

- So far, no accepted way of transient attack except against naive schemes with abrupt switching of resistors and not even a minimal transient protection, such as *ramping up/down the voltages* at the beginning at end without low-pass filters. Then high-frequency switching transients would cause waves and reflections.

- *How to make it?* Any information disappears after the noises reached the other end and the cable gets thermalized. Perhaps using wire resistance or capacitance? (Note: A new proposal, Gunn-Allison-Abbott, "A new transient attack on the Kish key distribution system", to be published against Mingesz' et al, simple voltage ramping of noise. p=0.7 information leak is claimed that would need 4 XOR privacy amplification stages. Yet to confirm and there is an easy total defense against the idea, but it points to the importance of the way of the signal startup).

- *How to make it?* Any information disappears after the noises reached the other end and the cable gets thermalized. Perhaps using wire resistance or capacitance for more advanced transient schemes?

- There is a software-based KLJN emulation by Pao-Lo Liu (PLA 2009), where the knowledge of signals propagation in the two directions cannot cause information leak in the steady state. But it leaks at transient attacks. Such signal separation cannot efficiently made in a physical KLJN system after mixing due to the quasi-static condition. Any way out of this?

- While no attacks, there are *various defense methods* against transient attacks. So far, the most robust transient defense is created by Kish (MMS, 2013) via an *adiabatically slow random walk of the resistors (and their noise intensity) starting from a common value*, at fixed temperature. *What kind of transient-based attack could be created against that?*

Former attack types (steady-state):

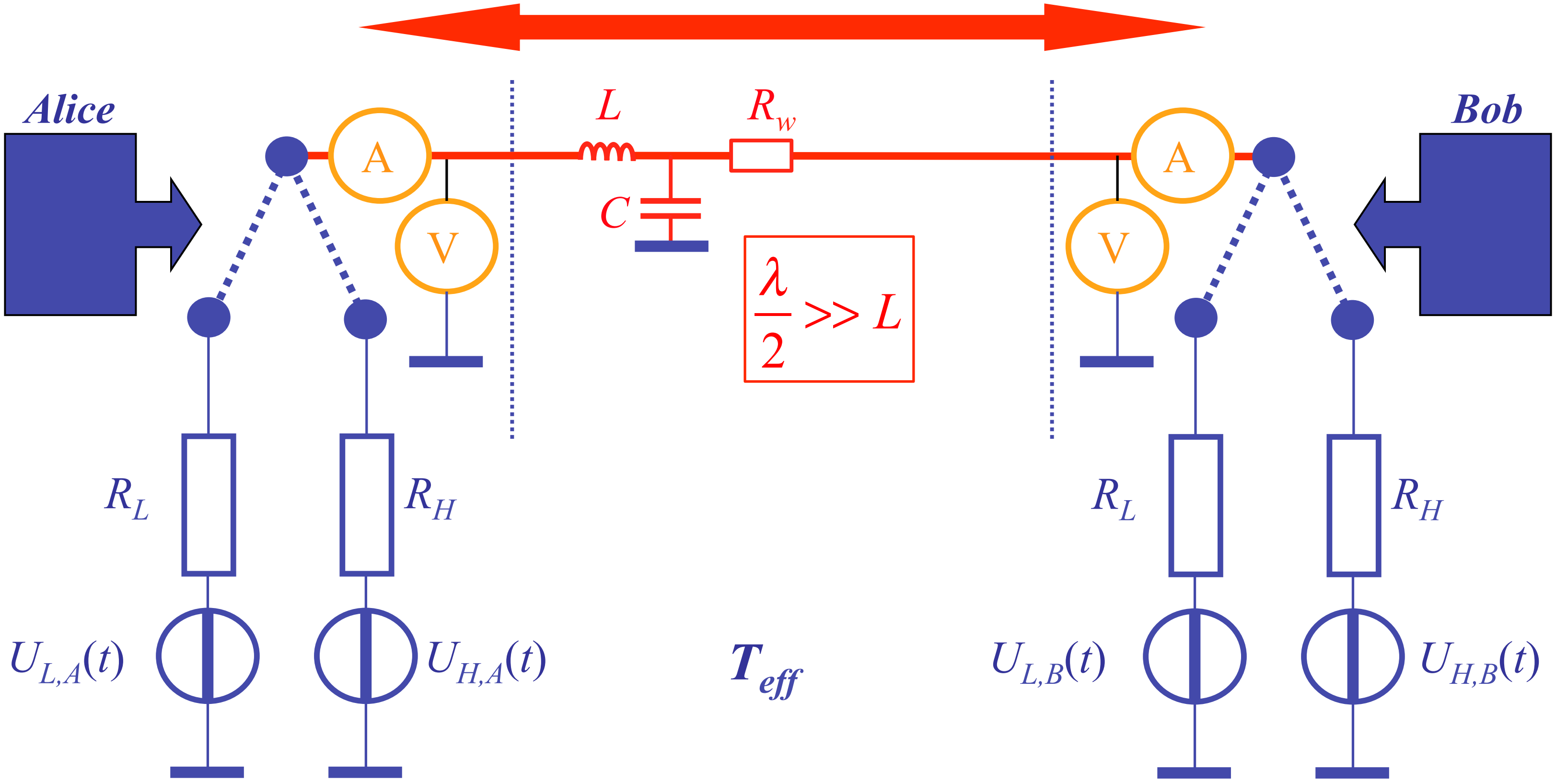
- Active: changing the circuit
- Passive (listening) utilizing (among others):
  - parasite elements (cable resistance, capacitance),
  - delays in the steady-state mode

Alternative defense against *passive attacks* using non-idealities by dropping key bits to form a cleaner key (out of privacy amplification)

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

Example: Mingesz, HoTPI-2013: p = 0.6 was reduced to p = 0.5002 by dropping 20% of the bits

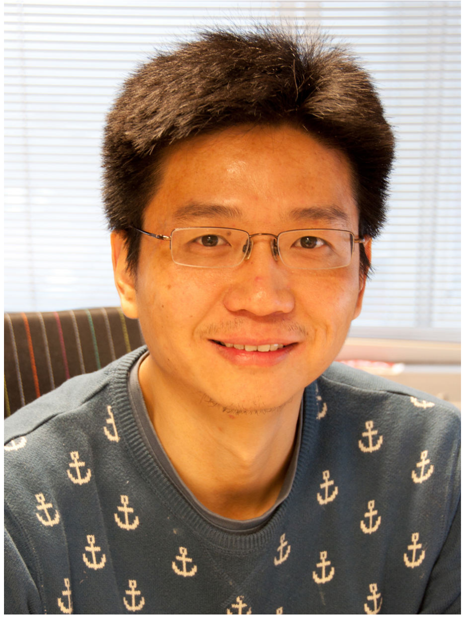
Instantaneous voltage and current amplitude comparison by Alice and Bob via authenticated public channel. For this $\log_2 N$ secure bits are used up for the exchange of N authenticated bits (Hjelme, Lydersen, Makarov arXiv:1108.1718)



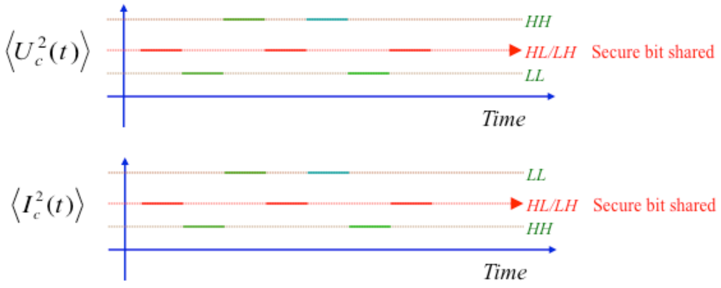
Most important concrete attacks, very briefly:

Almost all of ***the attacks had major errors***, except our own ones (except our attack against Liu) ☺

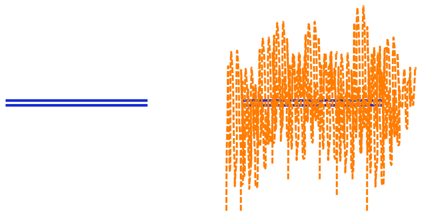
The only exception was **Feng Hao, a PhD student at Cambridge,** ***whose attack was flawless*** **(2006) .** Assumed temperature variations and showed that it causes an information leak because the secure level will split. In practice the effect is so small that not measurable, but the concept is correct and works for resistance inaccuracies, too.



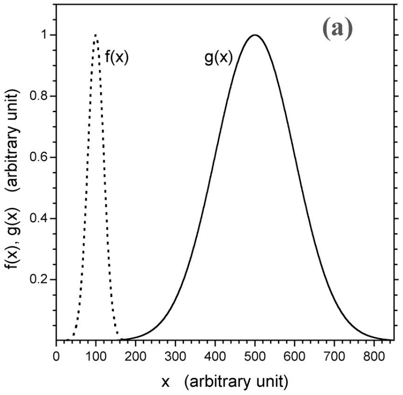
permission:
Feng Hao



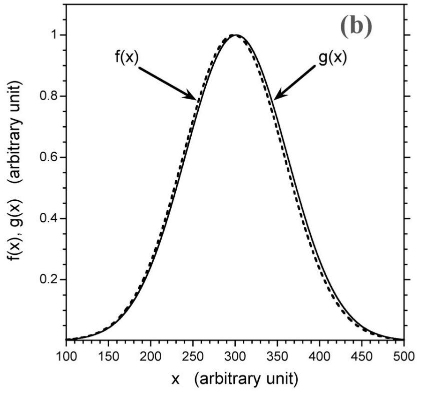
split secure levels in large noise:



Alice/Bob
distinguish 01/10 vs 00 and 11



Eve
tries to separate 01 from 10
(split is enhanced for visibility)



small sample number (100 or less)

Pao-Lo Liu tried to measure (simulate) and utilize current and voltage correlations at the two ends. Got large $p = 0.7 – 0.8$. The whole issue turned out to be a simulation artifact because for a 2 kilometer long cable, implicitly, a ***cable diameter of 28,000 greater than the size of known universe*** was assumed via the unphysical wave impedance.

Pao-Lo Liu later had a ***great contribution*** by introducing an abstract computer model of KLJN. He proved that knowing the ***separation of signals propagating in the two directions does not give out information in the steady-state situation***, thus ***directional couplers can never help Eve in the steady state***.

Note: separating the signals do help Eve during the transient period; this is why Pao-Lo considers his system not secure against transients. But it is impossible to create an efficient directional coupler against a hardware KLJN.

permission: Pao-Lo Liu

Pao-Lo at the La Rambla Drinking Fountain, the ***Fountain of Return*** *in Barcelona*

permission: Zoltan Gingl

Zoltan Gingl (2010) when, during unsuccessful attempts to crack Pao-Lo Liu's scheme, we honored Pao-Lo by tasting the local College Station wine Paolo.

Jacob (Koby) Scheuer and **Amnon Yariv** (PLA 2006) launched the first attack utilizing and analyzing the voltage drop due to the non-zero wire resistance (the idea was know before and even mentioned by ***Janos Bergou*** in the Science magazine interview however it was not analyzed). Unfortunately, the scheme and even the physical unit in the main results were incorrect. Koby visited me in 2010 when we corrected the calculations and got about a 1000 times less leak signal for Eve than stated earlier.

This attack is valid and was ***measured*** in 2006 by **Robert Mingesz** (Mingesz, et al, PLA (2008)) and gave a modest $p = 0.525$ value.

However, this attack can be ***totally eliminated*** by *properly boosting the temperature* at the lower resistor end, see (Kish & Granqvist, Entropy (2014)).

permission: Jacob Scheuer

Koby Scheuer

permission: Robert Mingesz, Zoltan Gingl

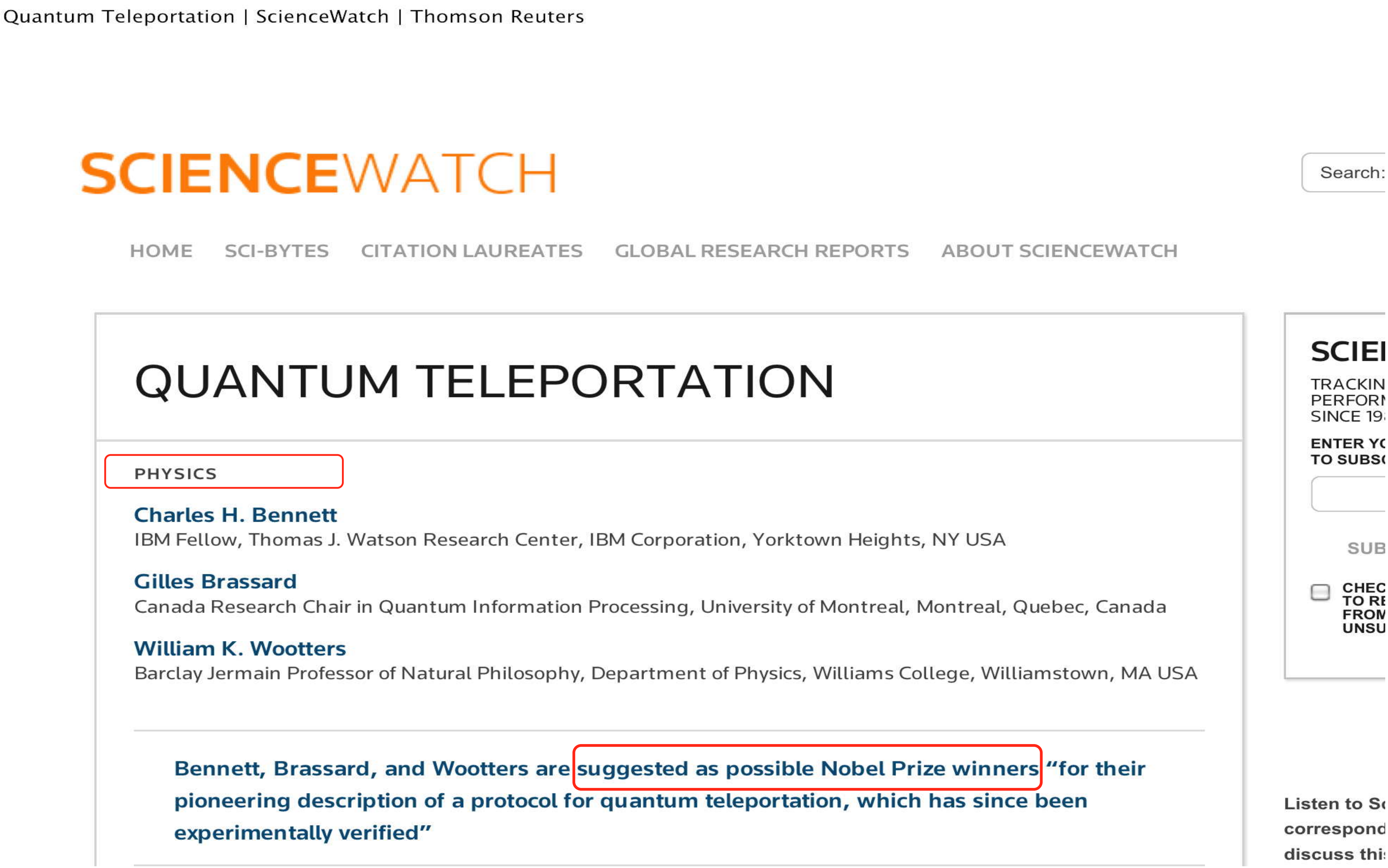
Robert Mingesz and Zoltan Gingl during the Szegedin Whisper project (2006) when we tested this attack, too.

Second Law Attack (Kish & Granqvist, Entropy, 2014). This is the most efficient wire resistance-based attack because it is comparing he power flow at the two ends, which is asymmetric due to the wire loss. Gives about twofold greater signal-to-noise ratio for Eve than the Scheuer-Yariv attack.

This attack is also totally eliminated by the same temperature boosting method and value and the former attack (Kish & Granqvist, Entropy (2014)).

Bennett-Riedel attack (arXiv 2013)

response: Kish, et al, PLOS ONE 2013



Quantum Teleportation | ScienceWatch | Thomson Reuters

SCIENCEWATCH

Search:

HOME SCI-BYTES CITATION LAUREATES GLOBAL RESEARCH REPORTS ABOUT SCIENCEWATCH

QUANTUM TELEPORTATION

PHYSICS

Charles H. Bennett
IBM Fellow, Thomas J. Watson Research Center, IBM Corporation, Yorktown Heights, NY USA

Gilles Brassard
Canada Research Chair in Quantum Information Processing, University of Montreal, Montreal, Quebec, Canada

William K. Wootters
Barclay Jermain Professor of Natural Philosophy, Department of Physics, Williams College, Williamstown, MA USA

Bennett, Brassard, and Wootters are suggested as possible Nobel Prize winners "for their pioneering description of a protocol for quantum teleportation, which has since been experimentally verified"

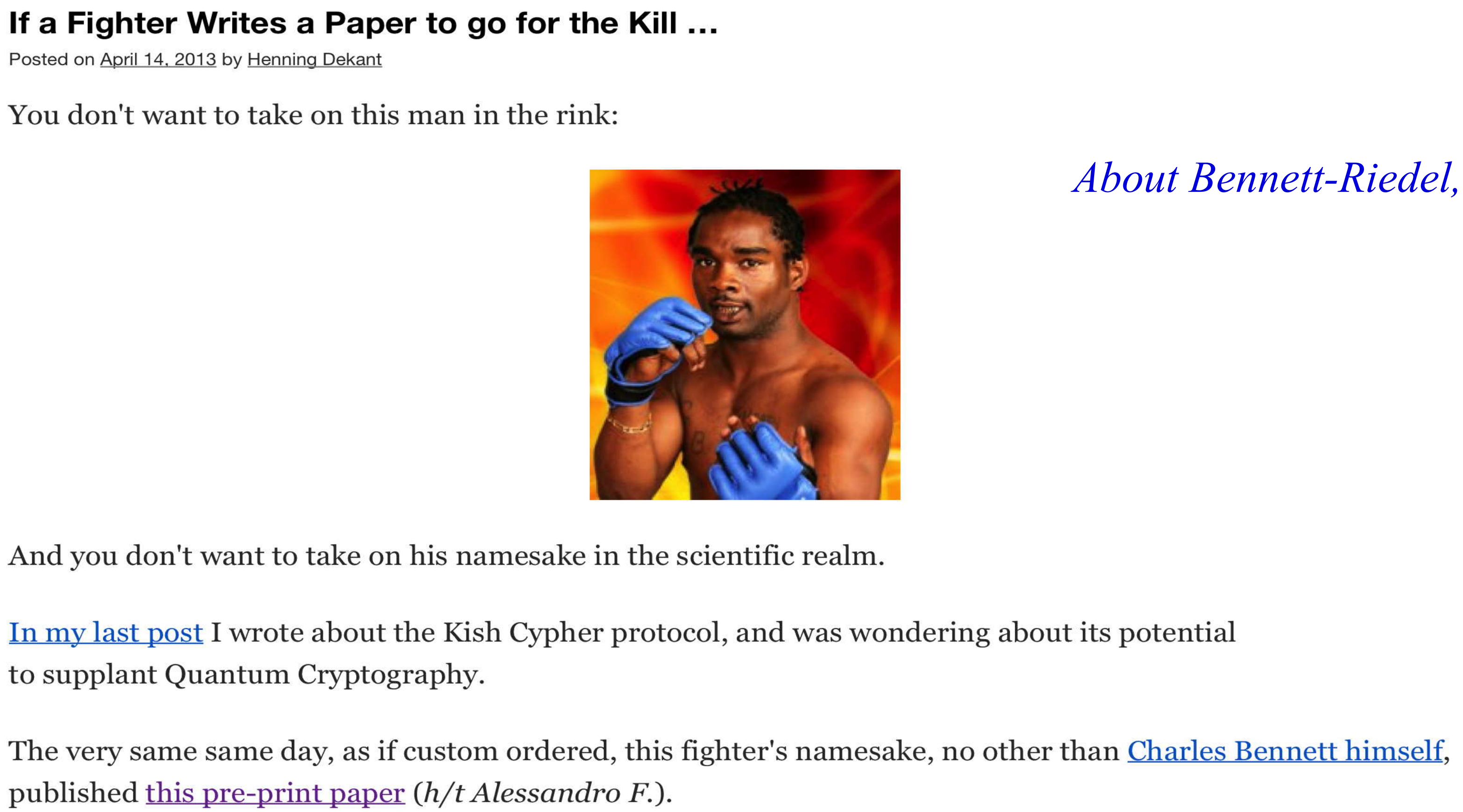
SCIE
TRACKIN
PERFORI
SINCE 19

ENTER YC
TO SUBSC

SUB

□ CHEC
TO RE
FROM
UNSU

Listen to Sc
correspond
discuss thi



If a Fighter Writes a Paper to go for the Kill …

Posted on April 14, 2013 by Henning Dekant

You don't want to take on this man in the rink:

And you don't want to take on his namesake in the scientific realm.

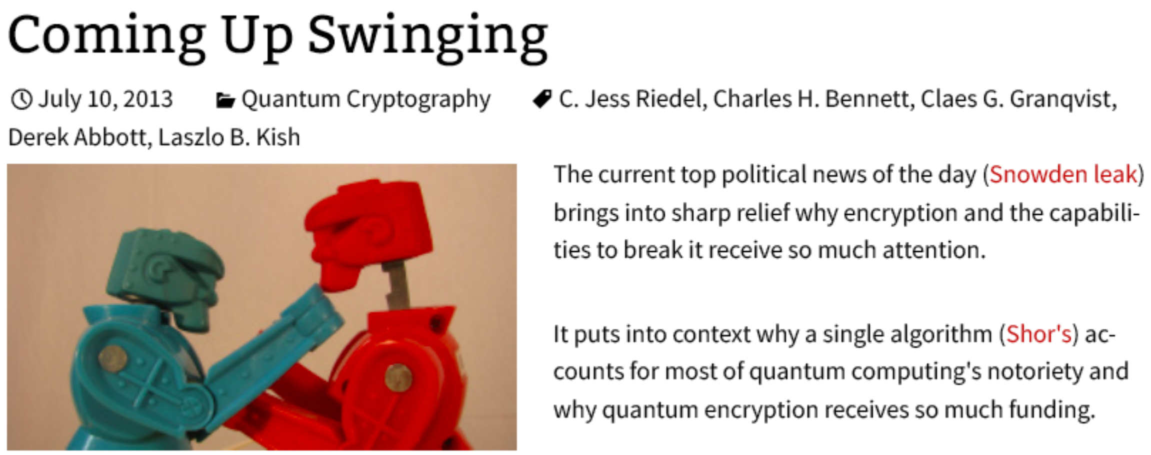
In my last post I wrote about the Kish Cypher protocol, and was wondering about its potential to supplant Quantum Cryptography.

The very same same day, as if custom ordered, this fighter's namesake, no other than Charles Bennett himself, published this pre-print paper (*h/t Alessandro F.*).

About Bennett-Riedel, arXiv, April, 2013.

Then about our response in PLoS ONE:

(50 page long manuscript)



Coming Up Swinging

July 10, 2013 Quantum Cryptography C. Jess Riedel, Charles H. Bennett, Claes G. Granqvist, Derek Abbott, Laszlo B. Kish

The current top political news of the day (Snowden leak) brings into sharp relief why encryption and the capabilities to break it receive so much attention.

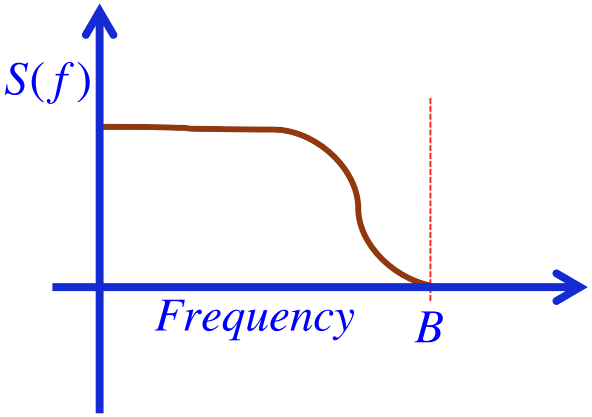
It puts into context why a single algorithm (Shor's) accounts for most of quantum computing's notoriety and why quantum encryption receives so much funding.

The most important factor neglected by the Bennett-Riedel attack (and by others who miss this):

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 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*

$$n \le 2B\tau$$

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

During τ duration, the measurement serves only with $n \le 2B\tau$ 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.

Chairman Mao

permission: Lachlan Gunn, Derek Abbott

The Gunn-Allison-Abbott "directional coupler" attack (Gunn, et al, Nature Science Report, 2014). It is a genuine design of **Lachan Gunn** but not a directional coupler, which would not work anyway, see Pao-Lo Liu above. According to our detailed analysis, it is a mixture and it gives somewhat less but roughly the same information as the Scheuer-Yariv resistance attack. *It took us 3 papers to partially clarify the misconceptions* in it, both conceptual and experimental ones, for example,

- **Experiments: invalid.** An *illegal voltage divider* in the cable during measurements causing double Kirchhoff loop and seemingly information leak; etc.

- **Concept and simulations: invalid**. We showed that it has nothing with propagation delay and it gives somewhat less leak then the resistance attack.

Yet, the impact of this invalid paper is valuable and ***not because it is in a Nature journal.*** It's example shows that designing a secure KLJN system *does require a highly careful design* and considerable efforts.

New: A new proposal, Gunn-Allison-Abbott, "A new transient attack on the Kish key distribution system", to be published against Mingesz' et al, simple voltage ramping defense. The same *wave-based* reflection coefficients used that are unphysical against the steady-state mode, even though no wave solutions exist, seemingly causing p=0.7 information leak that would need 4 XOR privacy amplification stages.

Lachlan Gunn and Derek Abbott a few minutes before Lachlan first told me about his "directional coupler" attack in 2013 (Changsha, China) and answered him that the believe in waves, when they are physically cannot be there, is dangerous.

Short cable vs. long cable; no-wave vs. wave

- LT-SPICE cable simulation (Linear Technology)
- Lossless Coaxial Cable, type: RG58
  - R=0
  - L=250nH/Meter
  - C=100pF/Meter
- Length
  - 1 km - **0.5% of wavelength (KLJN) - no wave, no reflection, no interference**
  - 200 km - **1 wavelength – wave behavior, reflections, interference, resonance**
  - 220 km - **1.1 wavelength – wave behavior, reflections, interference, no resonance**

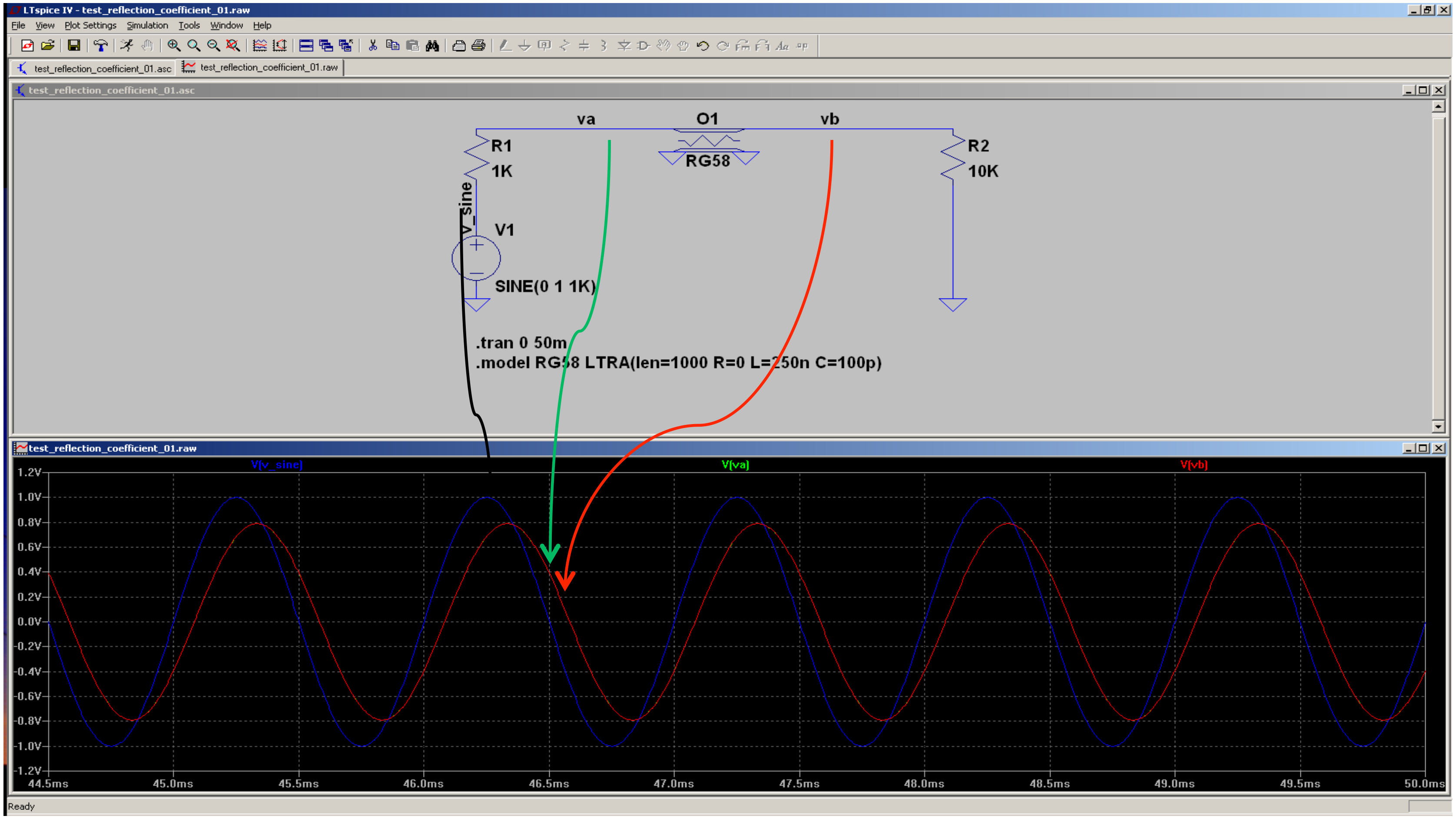
- Sine wave signal=1Vp @1KHz

- 1K and 10K (Ohm) in KLJN system

LT-SPICE cable simulator (Linear Technology).

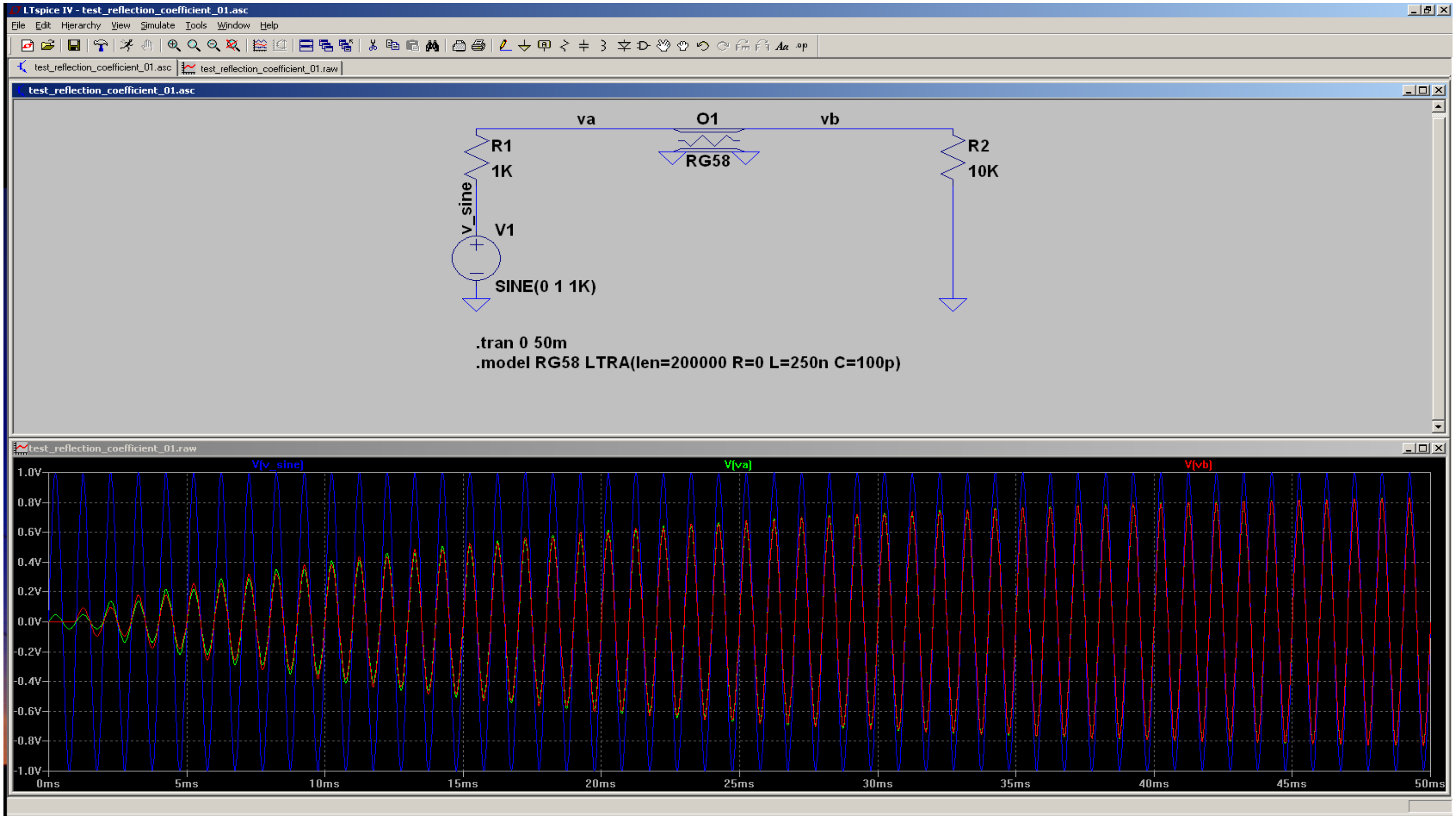
Cable length = 1 km; 0.5% of wavelength. **No wave, reflection, interference.**

Lumped-element voltage divider between the resistances with a phase shift.



```
.tran 0 50m
.model RG58 LTRA(len=1000 R=0 L=250n C=100p)
```

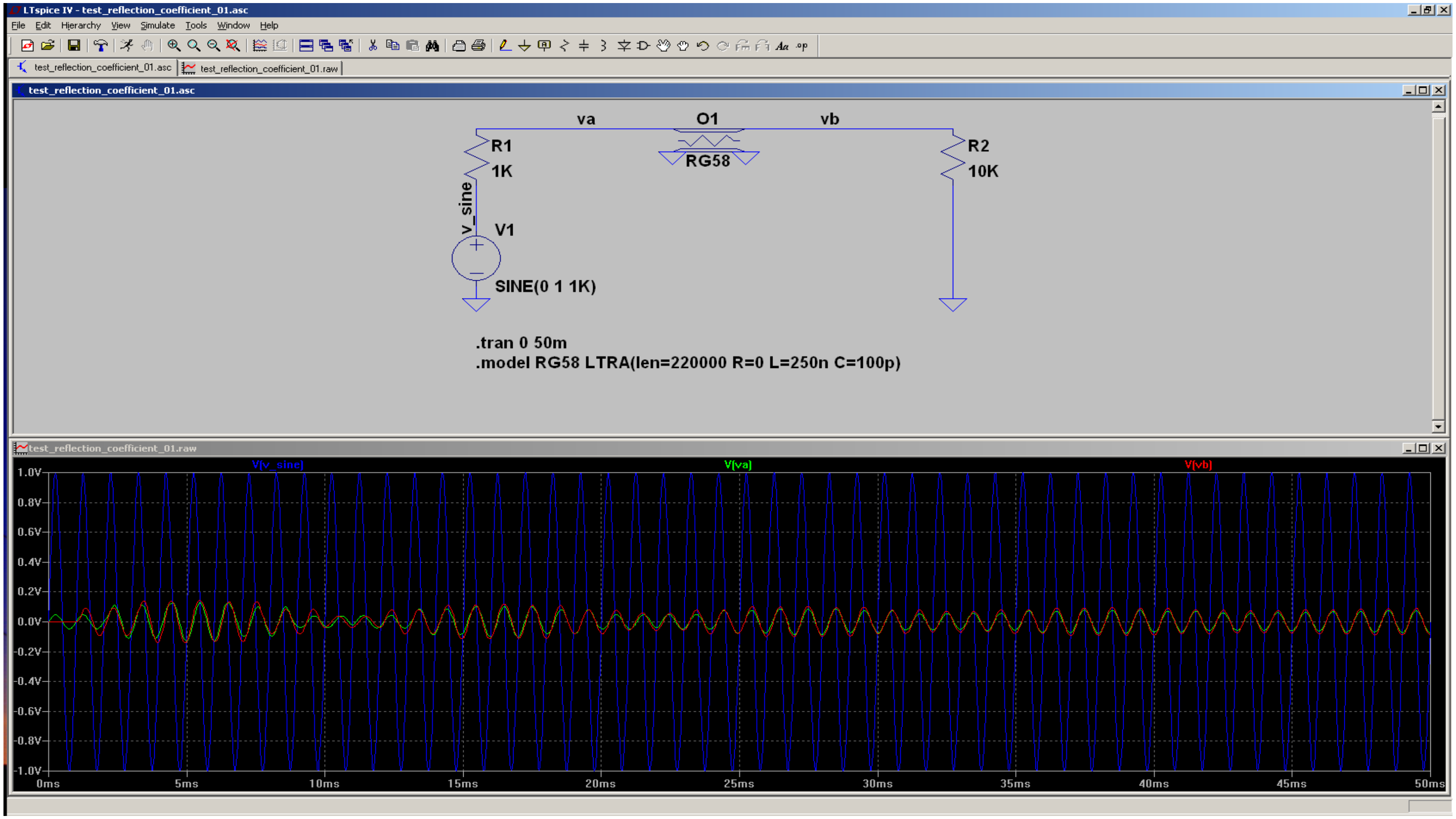
Cable length = 200KM



```
.tran 0 50m
.model RG58 LTRA(len=200000 R=0 L=250n C=100p)
```

LTspice IV - test_reflection_coefficient_01.asc
File Edit Hierarchy View Simulate Tools Window Help
test_reflection_coefficient_01.asc
test_reflection_coefficient_01.raw
va
O1
vb
R1
1K
RG58
R2
10K
v_sine
V1
SINE(0 1 1K)
V(v_sine)
V(va)
V(vb)
1.0V
0.8V
0.6V
0.4V
0.2V
0.0V
-0.2V
-0.4V
-0.6V
-0.8V
-1.0V
0ms
5ms
10ms
15ms
20ms
25ms
30ms
35ms
40ms
45ms
50ms

Cable length = 220KM

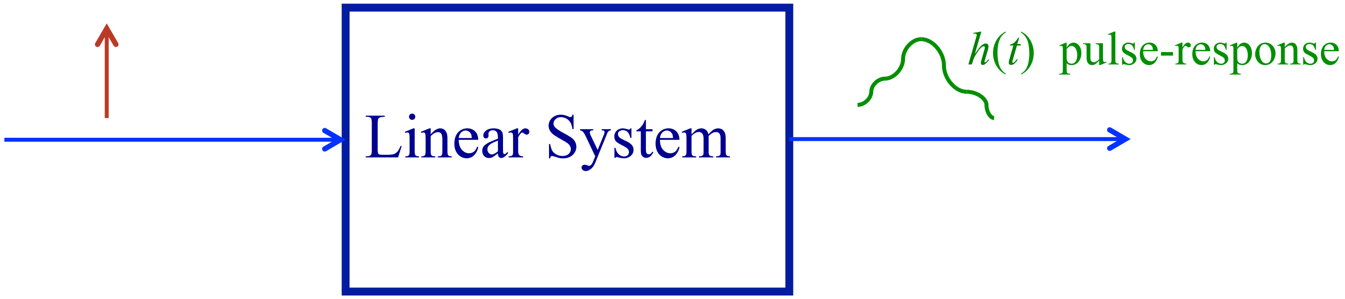


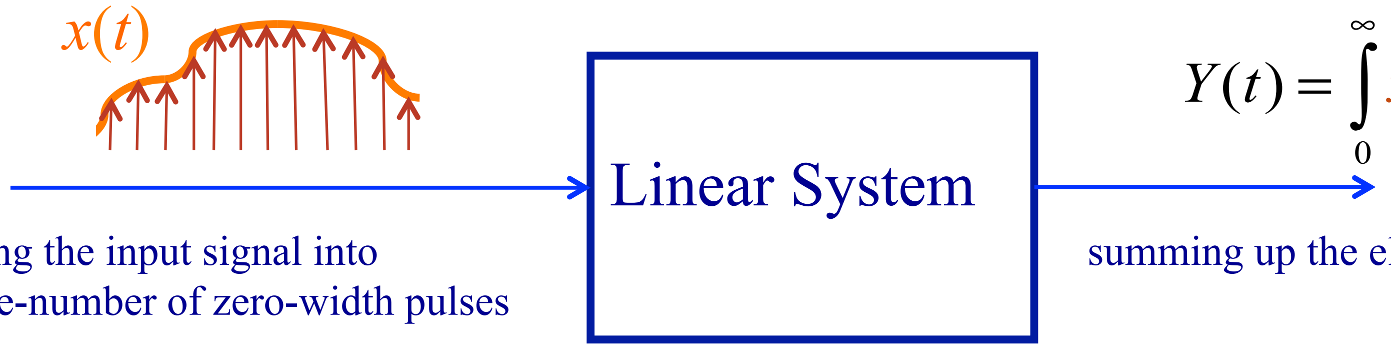
LTspice IV - test_reflection_coefficient_01.asc
File Edit Hierarchy View Simulate Tools Window Help
test_reflection_coefficient_01.asc
test_reflection_coefficient_01.raw
test_reflection_coefficient_01.asc
va
O1
vb
R1
1K
RG58
R2
10K
v_sine
V1
SINE(0 1 1K)
test_reflection_coefficient_01.raw
V(v_sine)
V(va)
V(vb)
1.0V
0.8V
0.6V
0.4V
0.2V
0.0V
-0.2V
-0.4V
-0.6V
-0.8V
-1.0V
0ms
5ms
10ms
15ms
20ms
25ms
30ms
35ms
40ms
45ms
50ms

```
.tran 0 50m
.model RG58 LTRA(len=220000 R=0 L=250n C=100p)
```

Engineering approaches with ***wave-based description of no-waves***

Relevant example for waves: Weighting function method utilizing pulse response
(Linear time-invariant network analysis)





$$Y(t) = \int_0^\infty x(t-\tau)h(\tau)\,d\tau$$

dividing the input signal into
infinite-number of zero-width pulses

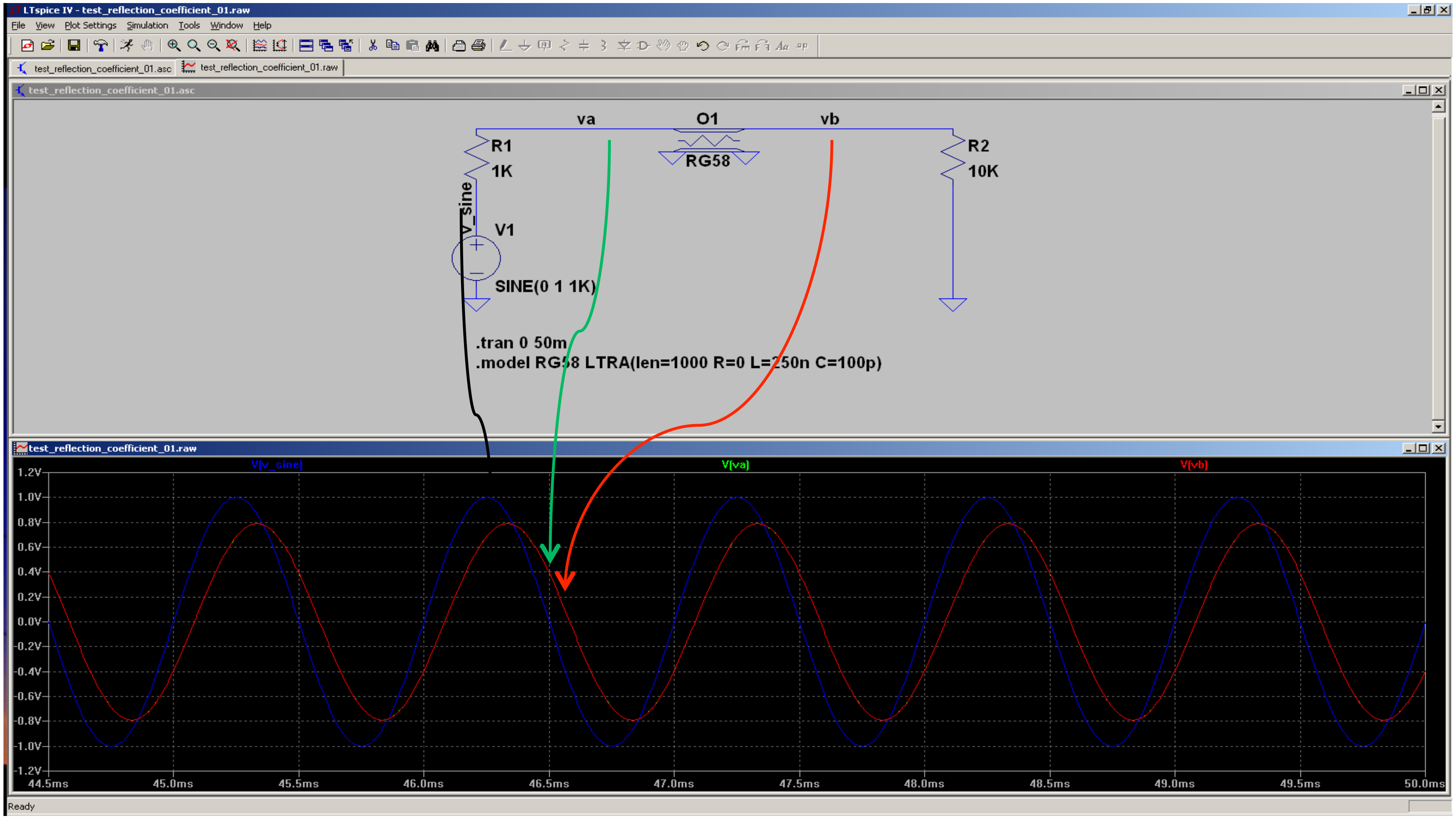
summing up the elementary pulse-responses

Such pulses have infinite bandwidth thus they would generate waves in any cable thus h(t) will be waves. However, these pulses (and the waves) are only mathematical artifacts; they don't exist physically. For example we don't see Xray's radiated due to their bandwidth ☺.

LT-SPICE cable simulator (Linear Technology).

Cable length = 1 km; 0.5% of wavelength. **No wave, reflection, interference.**

Lumped-element voltage divider between the resistances with a phase shift.



LTspice IV - test_reflection_coefficient_01.raw

```
.tran 0 50m
.model RG58 LTRA(len=1000 R=0 L=250n C=100p)
```

Cable capacitance attack (newest attack)
LT-SPICE cable simulations 1000 meter, 1k, 9k

Hsien-Pu Chen, et al, to be published

$$\rho_{iA} = \left\langle I_{CA}(t) \cdot \frac{dU_{CA}(t)}{dt} \right\rangle_{\tau=100}$$

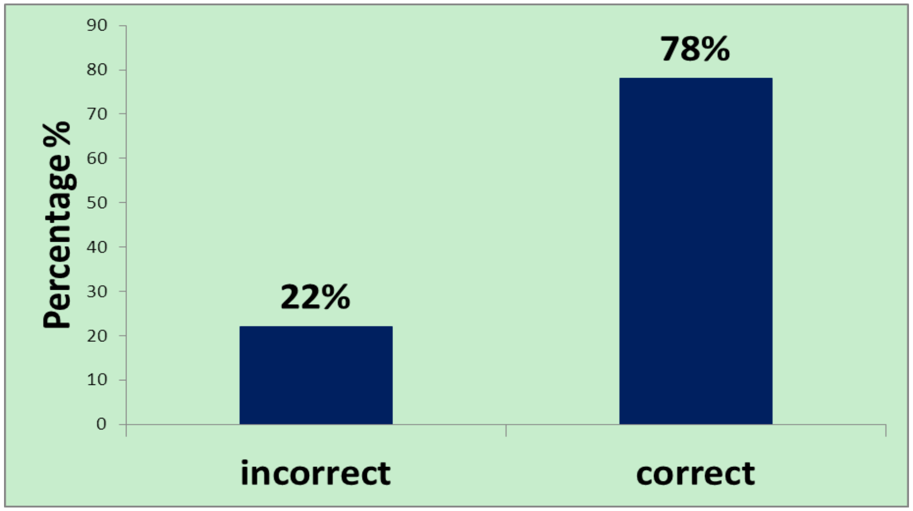
$$\rho_{iB} = \left\langle I_{CB}(t) \cdot \frac{dU_{CB}(t)}{dt} \right\rangle_{\tau=100}$$

$$\rho_i = \rho_{iA} - \rho_{iB}$$

$$\begin{cases} \rho_i > 0, sign(\rho_i)\text{=correct} \\ \rho_i < 0, sign(\rho_i)\text{=incorrect} \end{cases}$$

$$i = 1,2,3....M$$

$$M = 100$$



Cable capacitance attack (newest attack)
LT-SPICE cable simulations 100 meter, 1k, 9k
10% of the earlier cable length: similar to earlier leak via resistance

$$\rho_{iA} = \left\langle I_{CA}(t) \cdot \frac{dU_{CA}(t)}{dt} \right\rangle_{\tau=100}$$

$$\rho_{iB} = \left\langle I_{CB}(t) \cdot \frac{dU_{CB}(t)}{dt} \right\rangle_{\tau=100}$$

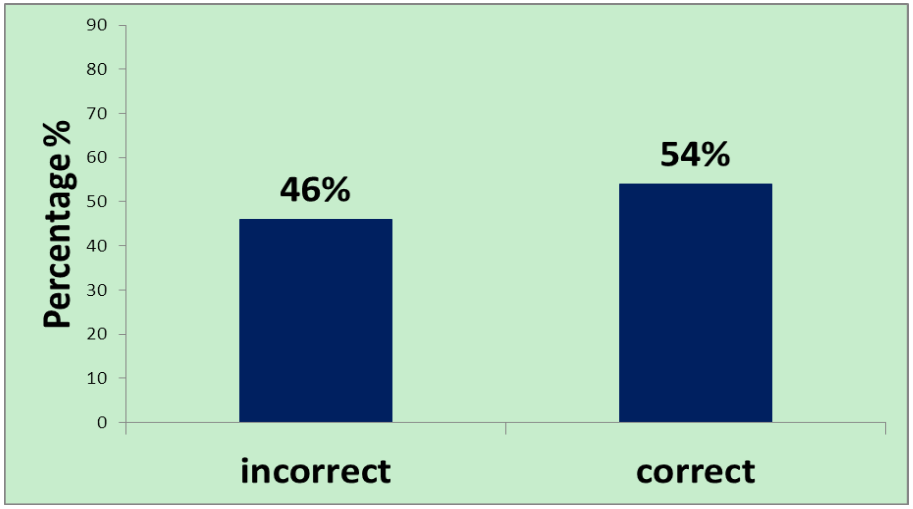
$$\rho_i = \rho_{iA} - \rho_{iB}$$

$$\begin{cases} \rho_i > 0, sign(\rho_i) = \text{correct} \\ \rho_i < 0, sign(\rho_i) = \text{incorrect} \end{cases}$$

$$i = 1, 2, 3 \ldots M$$

$$M = 100$$

Hsien-Pu Chen, et al, to be published



Cable capacitance attack (new attack)
LT-SPICE cable simulations 1000 meter, 1k, 9k
capacitor-killer defense

Hsien-Pu Chen, et al, to be published

$$\rho_{iA} = \left\langle I_{CA}(t) \cdot \frac{dU_{CA}(t)}{dt} \right\rangle_{\tau=100}$$

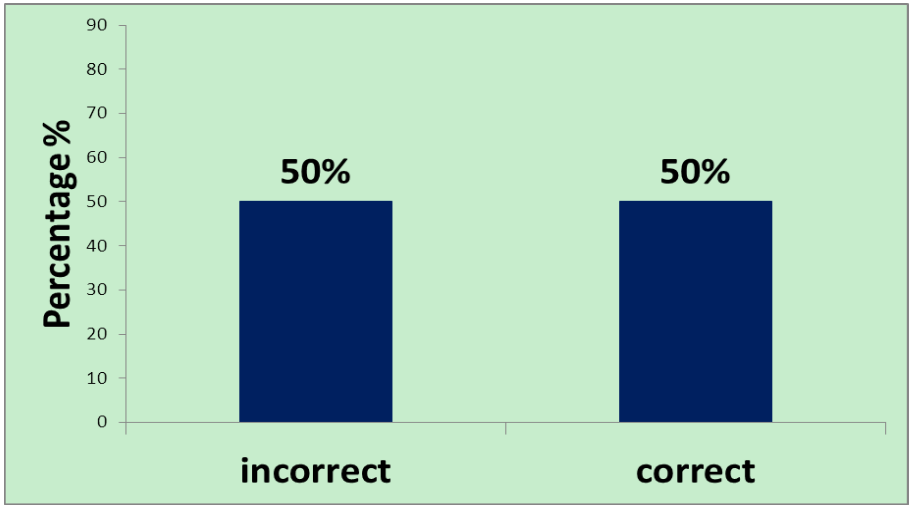
$$\rho_{iB} = \left\langle I_{CB}(t) \cdot \frac{dU_{CB}(t)}{dt} \right\rangle_{\tau=100}$$

$$\rho_i = \rho_{iA} - \rho_{iB}$$

$$\begin{cases} \rho_i > 0, sign(\rho_i)\text{=correct} \\ \rho_i < 0, sign(\rho_i)\text{=incorrect} \end{cases}$$

$$i = 1,2,3\dots M$$

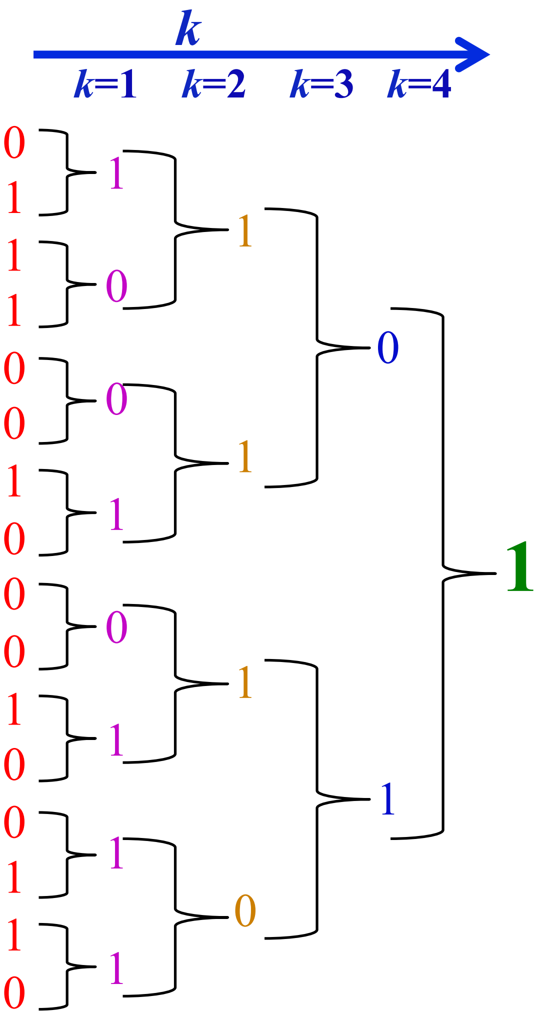
$$M = 100$$



Privacy amplifier: invented for quantum encryption: **the used resource is time. From a long key it makes a short key with improved security. A simple privacy amplifier by XOR-ing the pairs of key bits is studied in:**

T. Horvath, L.B. Kish, J. Scheuer, "Effective Privacy Amplification for Secure Classical Communications", EPL 94 (2011) 28002; http://arxiv.org/abs/1101.4264

$p = 0.5006$ → $C_e/f = 10^{-8}$ ***Practically Perfect Security***



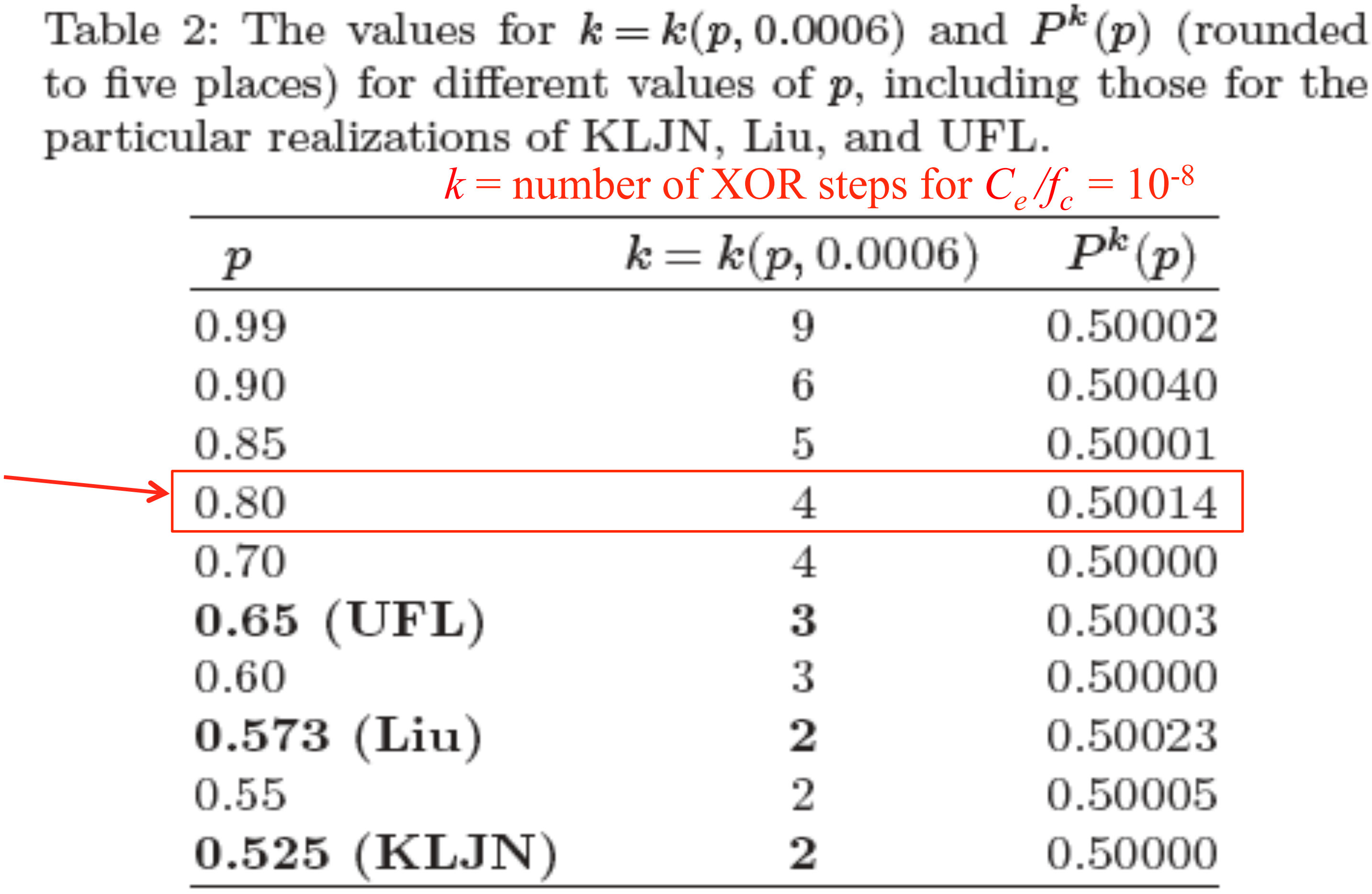


Table 2: The values for $k = k(p, 0.0006)$ and $P^k(p)$ (rounded to five places) for different values of p, including those for the particular realizations of KLJN, Liu, and UFL.

k = number of XOR steps for $C_e/f_c = 10^{-8}$

p	$k = k(p, 0.0006)$	$P^k(p)$
0.99	9	0.50002
0.90	6	0.50040
0.85	5	0.50001
0.80	4	0.50014
0.70	4	0.50000
0.65 (UFL)	**3**	0.50003
0.60	3	0.50000
0.573 (Liu)	**2**	0.50023
0.55	2	0.50005
0.525 (KLJN)	**2**	0.50000

End of presentation