"We can't solve problems by using the same kind of thinking we used when we created them." **(Albert Einstein)**

Zaj-alapu információ technológia?

L.B. Kish

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

"A zaj-alapu informacio technologia egy fiatal terulet, ahol az informaciot sztochasztikus folyamatok statisztikus tulajdonsagai vagy pillanatnyi amplitudojanak egy referencia folyamattak valo koincidenciaja hordozza. A tema 2005-ben lett eloszor felvetve adatatvitel kapcsan, es az elso eredmenyek ""nulla jel-energiaju adatatvitel"" es ""abszolut biztonsagos adatatvitel"" volt, melynek a kiserleti demonstralasa Szegeden tortent 2007-ben. A kovetkezo attorest a ""zaj-alapu logika"" jelentette 2009-ben, melyet az agy jeleinek veletlen jellege inspiralt es a kvantum szamologepekhez hasonlo tulajdonsagokkal redelkezik: a logikai allapotok szuperpozicioja is megengedett allapot, mely a hordozott informacio tartalom exponencialis novekedeset jelenti. A szeminarium rovid attekintest ad a tema egy-egy teruleterol.

http://www.ece.tamu.edu/~noise/research_files/research_secure.html

http://www.ece.tamu.edu/~noise/research_files/noise_based_logic.htm

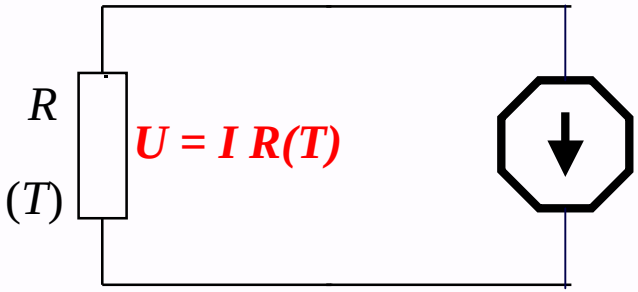
Noise-based informatics:

1. **(more generally): Sensory information**

2. **Communications**

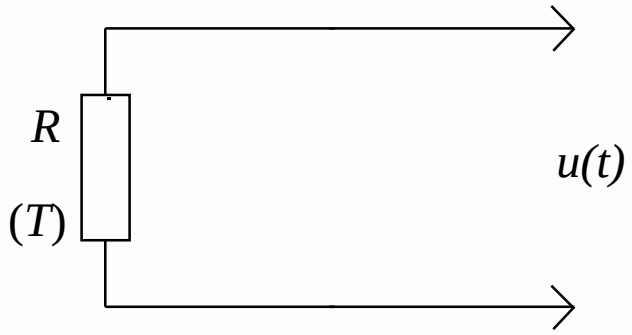
3. **Logic ad computing**

Example for classical sensing: Resistor Thermometer



- We need to know the $R(T)$ function.
- We need to provide the accurate driving current I.
- We are **heating the sensor** during the measurement and that causes errors.

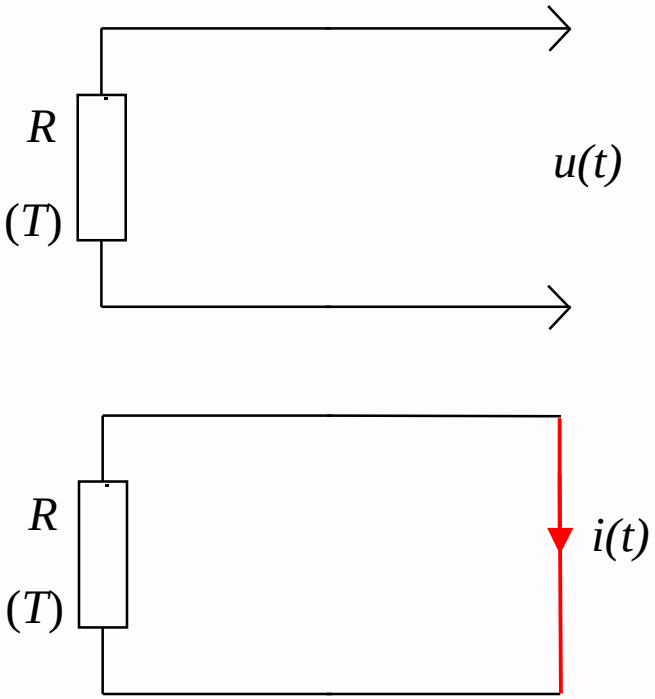
Example: Thermal noise thermometry in practice



$$S_u(f) = 4kTR$$

- We do not need to know the $R(T)$ calibration function.
- It is enough to measure the actual R.
- We still need to provide the calibrated driving current I for the R - measurement.
- We are still causing an error by heating; however this error can strongly be reduced by using a resistor material of resistivity of virtually independent of temperature.

Thermal noise thermometry from first principles



$$S_u(f) = 4kTR$$

$$S_i(f) = \frac{4kT}{R}$$

$$R = \sqrt{S_u / S_i}$$

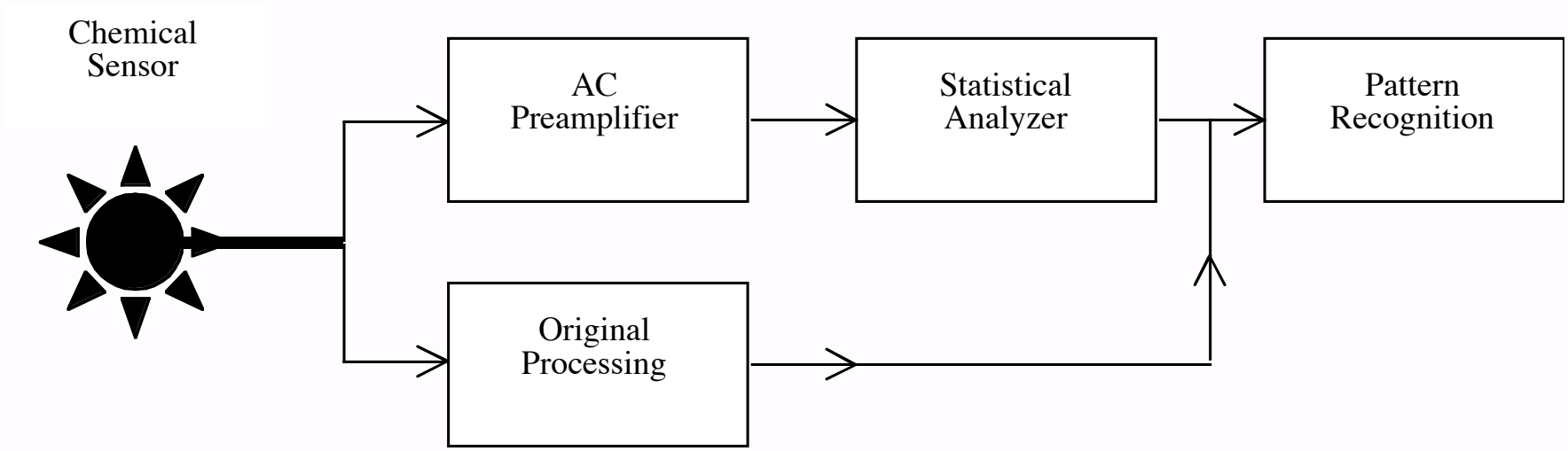
$$T = \frac{\sqrt{S_u S_i}}{4k}$$

1. We can determine the *T* and *R*(*T*) from the above equations.

2. Thus, we do not need to know the function *R*(*T*).

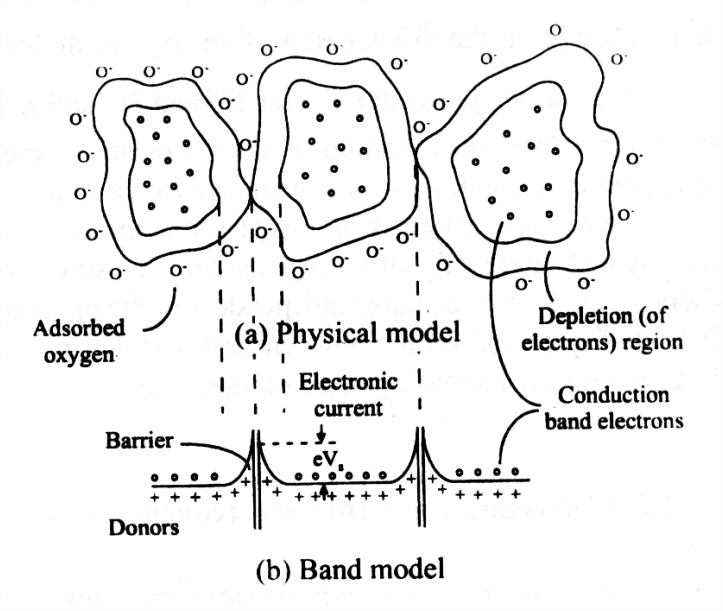
3. No heating because no external bias current is needed. Least perturbation of the system.

Fluctuation-enhanced chemical sensing.



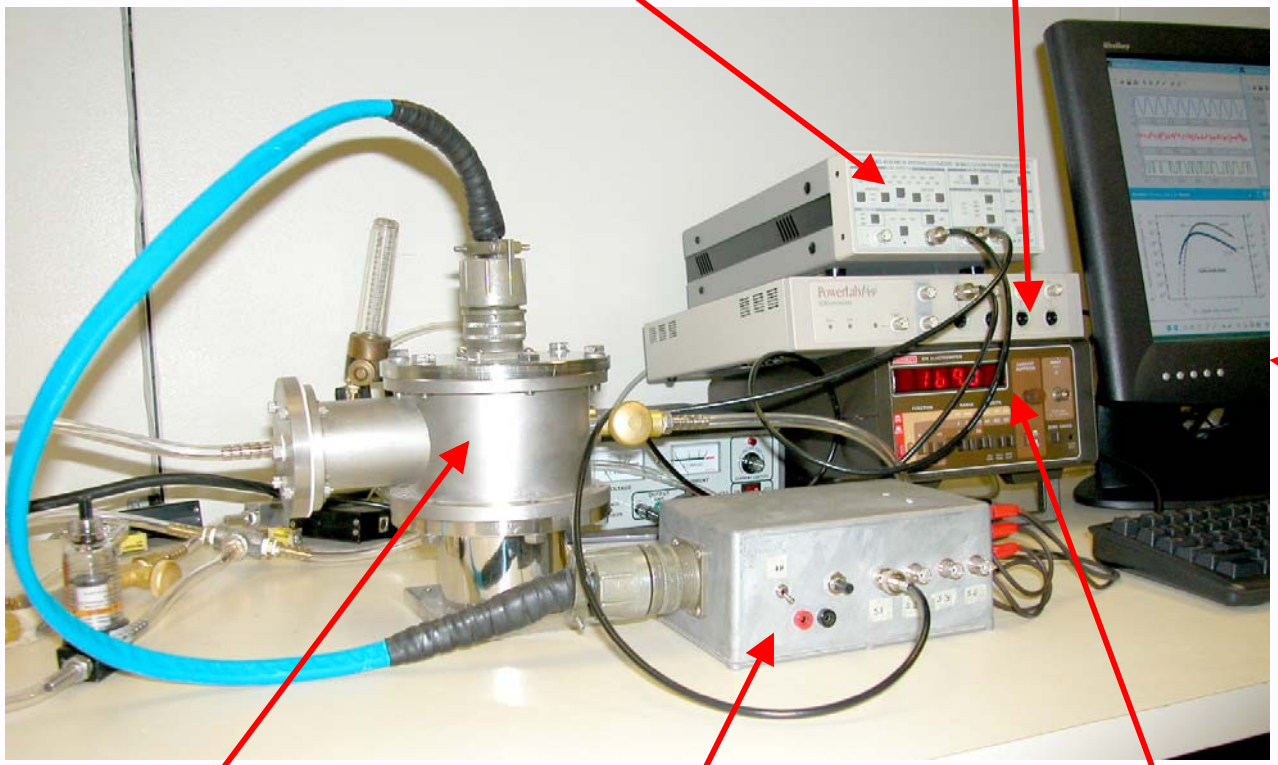
Taguchi gas sensors.

Taguchi sensors are heated semiconductor-oxide films where the resistance of the inter-grain junctions is modulated by the adsorbed agent which act as doping.



Stochastic microscopic fluctuations are generated in the junction resistance due to the diffusion of agents along the grain boundaries.

Lab Demo Prototype of Fluctuation-Enhanced Sensing
(Fluctuation and Noise Exploitation Lab, TAMU)



Preamplifier and Filters

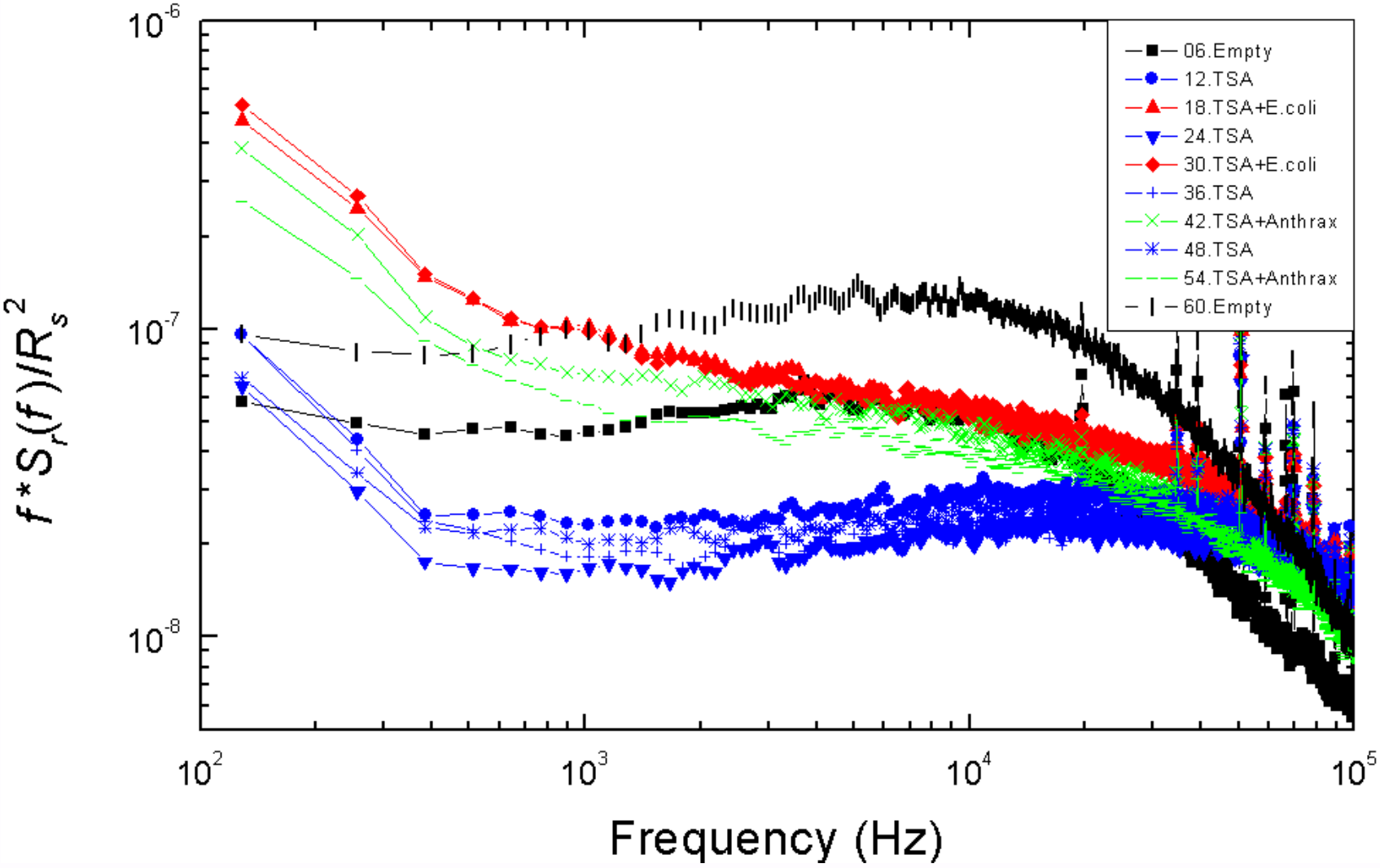
Signal Conditioning, AD Conversion

Statistical Analyzer,
Pattern Recognizer,
Pattern Databank,
Output Display,
Keyboard Control

Gas Sensor Chamber

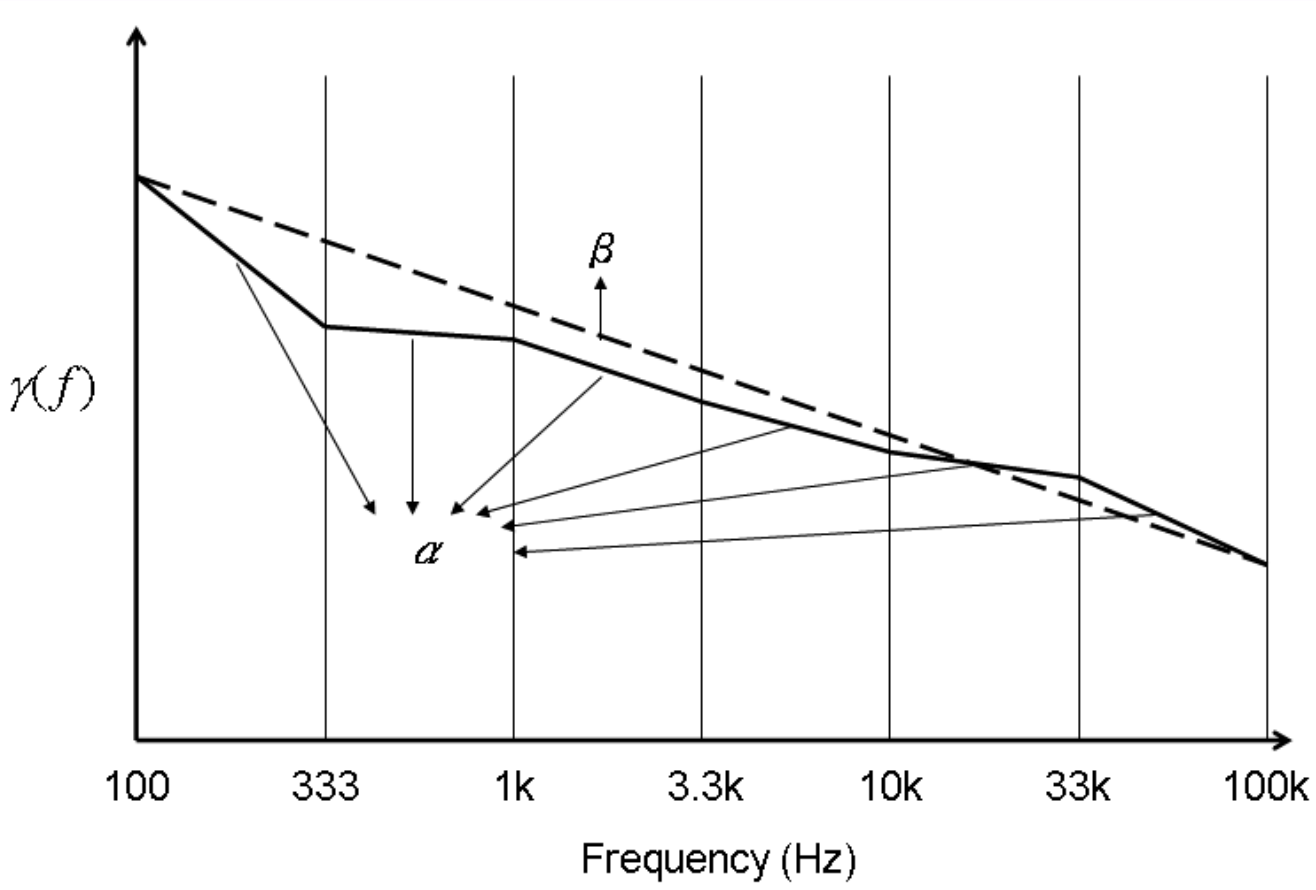
Sensor Driver and Signal Distributor

Classical Signal Output (Single Number)



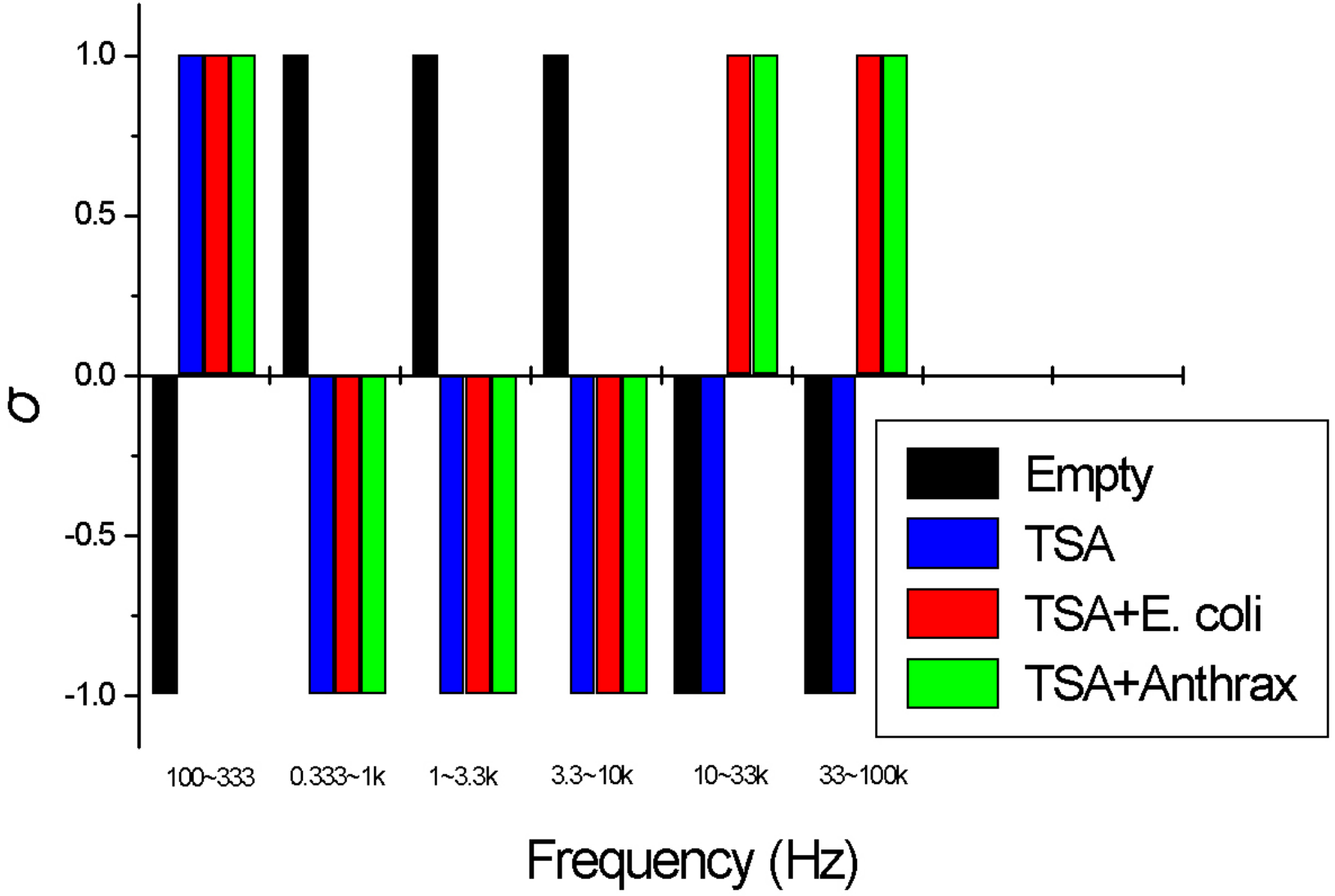
Normalized power spectra of the Taguchi sensor SP11 in sampling-and-hold-mode. The alias "Anthrax" stands for anthrax surrogate *Bacillus subtilis*.

simple way of binary and analog pattern generation

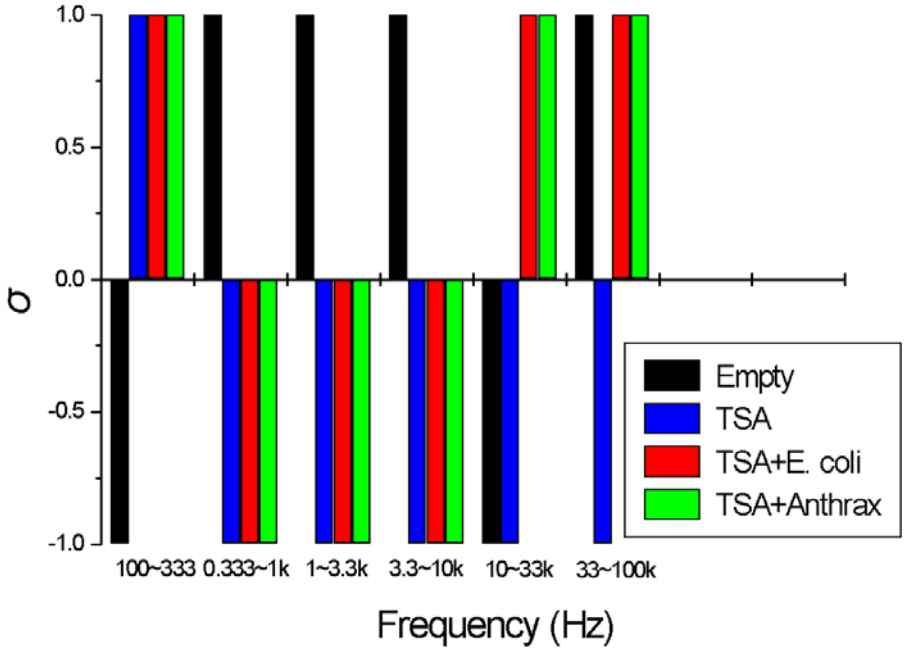


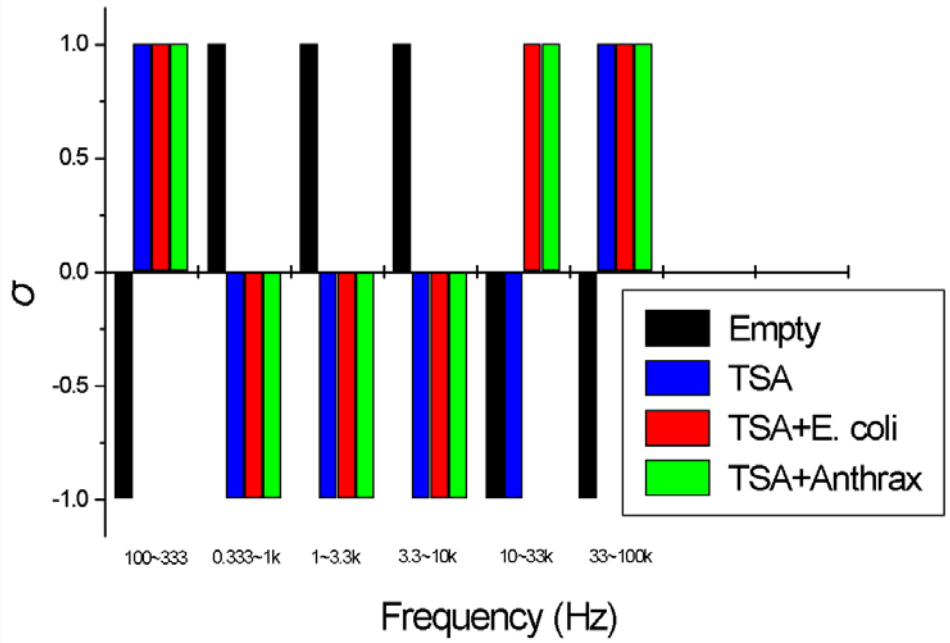
$$\gamma(f) = f\frac{S_r(f)}{R_s^2} \qquad \Delta = \alpha - \beta \qquad \sigma = \frac{\Delta}{|\Delta|} \qquad \Delta_n = \log\left|\frac{\Delta}{\beta}\right|$$

binary fingerprints of bacteria



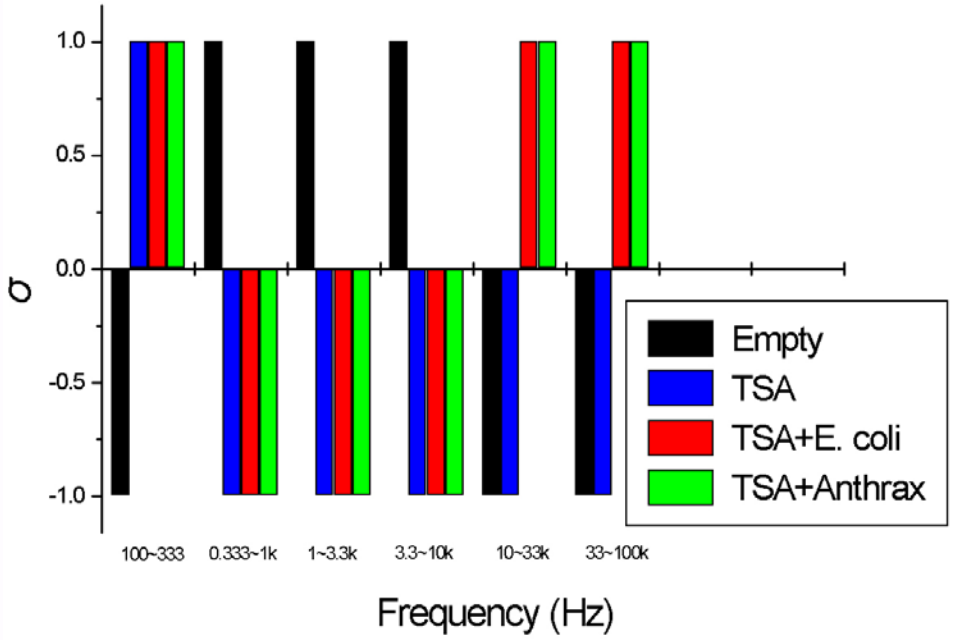
Generating binary pattern from the power spectra (sampling-and-hold, SP11). The alias "Anthrax" stands for anthrax surrogate *Bacillus subtilis*.





Reproducibility of the bacterial fingerprints (sampling-and-hold, SP11).

The alias "Anthrax" stands for anthrax surrogate *Bacillus subtilis*.



Noise-based communications

Collaborators (*failed attackers are not included*) (alphabetical order):

Zoltan Gingl (Univ. Szeged): experimental demo; security; cracking the Liu cypher

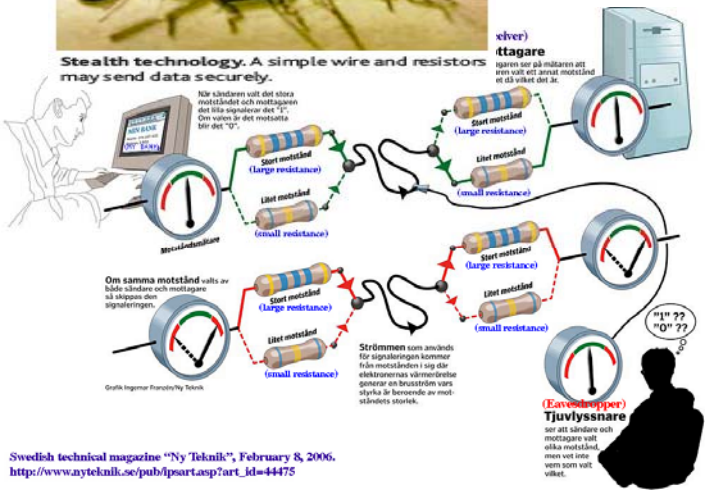
Tamas Horvath (Fraunhofer IAIS and Univ. of Bonn): security and privacy amplification

Robert Mingesz (Univ. Szeged): experimental demo; networks, security

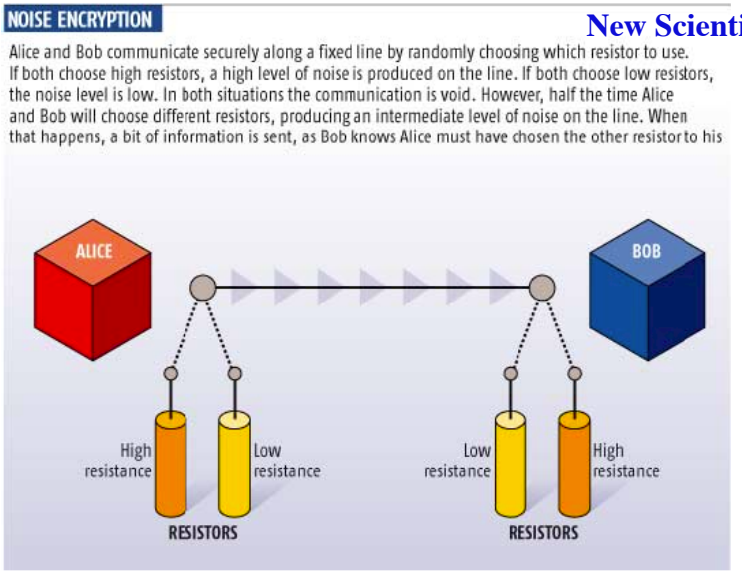
Ferdinand Peper (NICT, Kobe, Japan): recent survey including power lines

Jacob Scheuer (Tel-Aviv Univ.): attack, correcting their error of factor of 1000; privacy amplification

Science Magazine, 2005



Ny Teknik, 2005



New Scientist, 2007

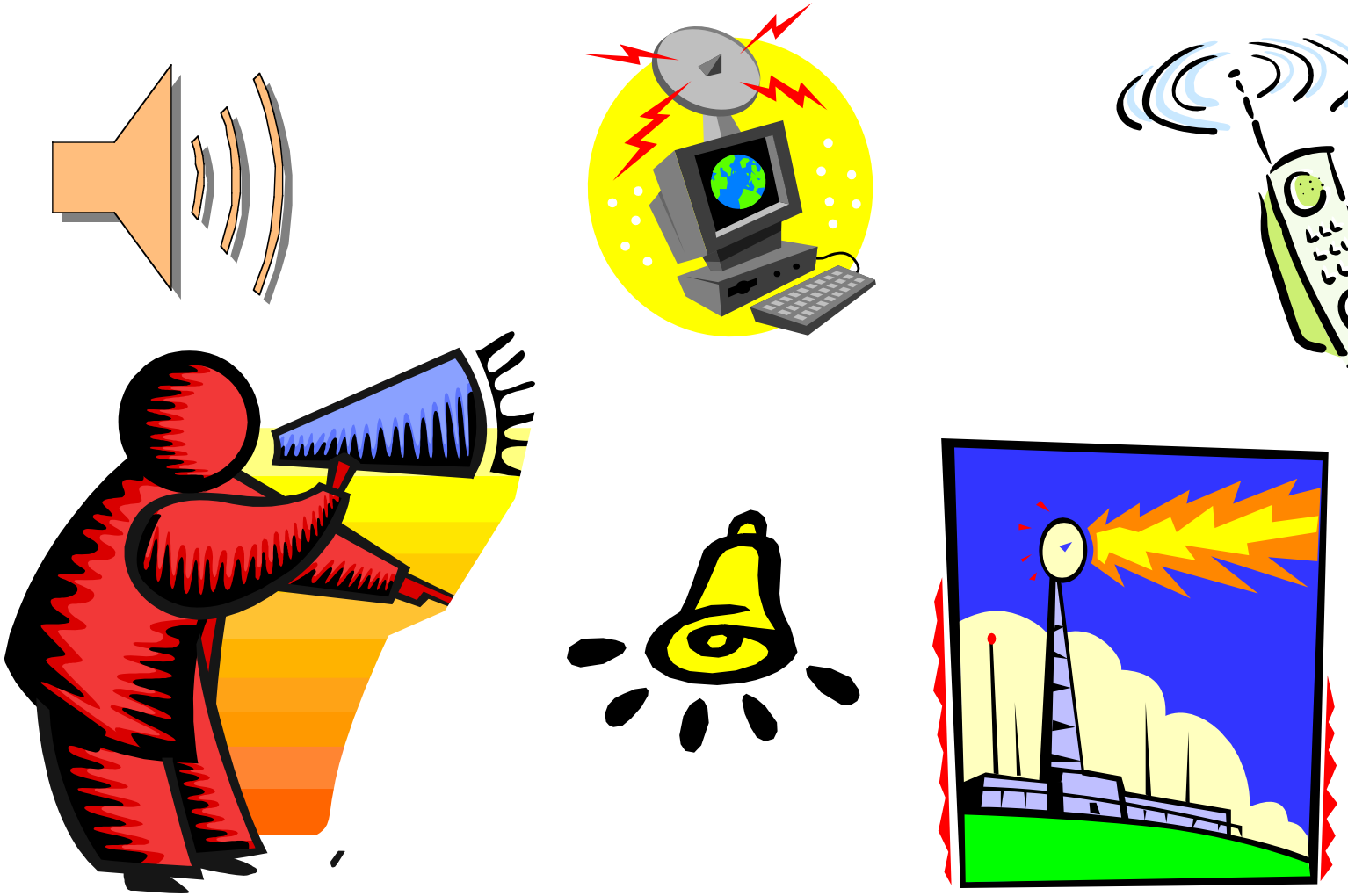
Pre-history:

L.B. Kish, "Stealth communication: Zero-power classical communication, zero-quantum quantum communication and environmental-noise communication", *Applied Physics Lett*. **87** (December 2005), Art. No. 234109

Introduction:

"Stealth communication: Zero-power classical communication, zero-quantum quantum communication and environmental-noise communication", *Applied Physics Lett.* **87** (December 2005), Art. No. 234109

Classical and quantum communication today: ***the sender emits signal energy***



Is it possible to do communication without emitting signal energy in the information channel?

(*Ask around and, most probably, you will hear consistent "no" answers"...*)

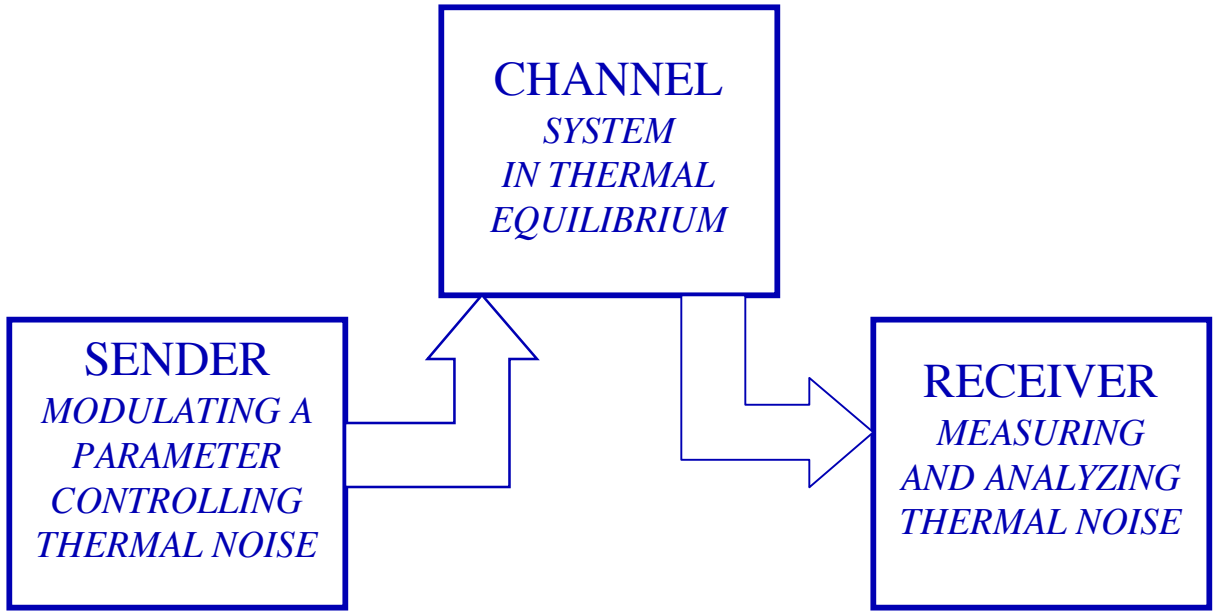
Is it possible to do communication without emitting signal energy in the information channel?

The answer is YES

Introduction:

"Stealth communication: Zero-power classical communication, zero-quantum quantum communication and environmental-noise communication", *Applied Physics Lett.* **87** (December 2005), Art. No. 234109

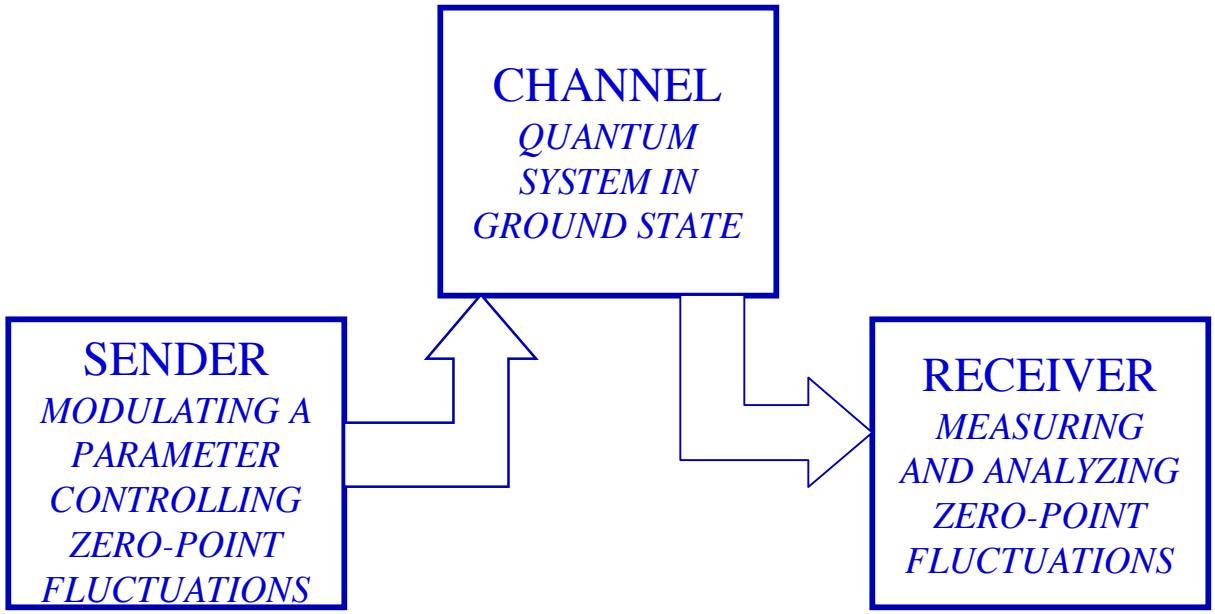
Zero-Signal-Power Classical Communication



Introduction:

"Stealth communication: Zero-power classical communication, zero-quantum quantum communication and environmental-noise communication", *Applied Physics Lett.* **87** (December 2005), Art. No. 234109

Zero-Quantum Quantum Communication

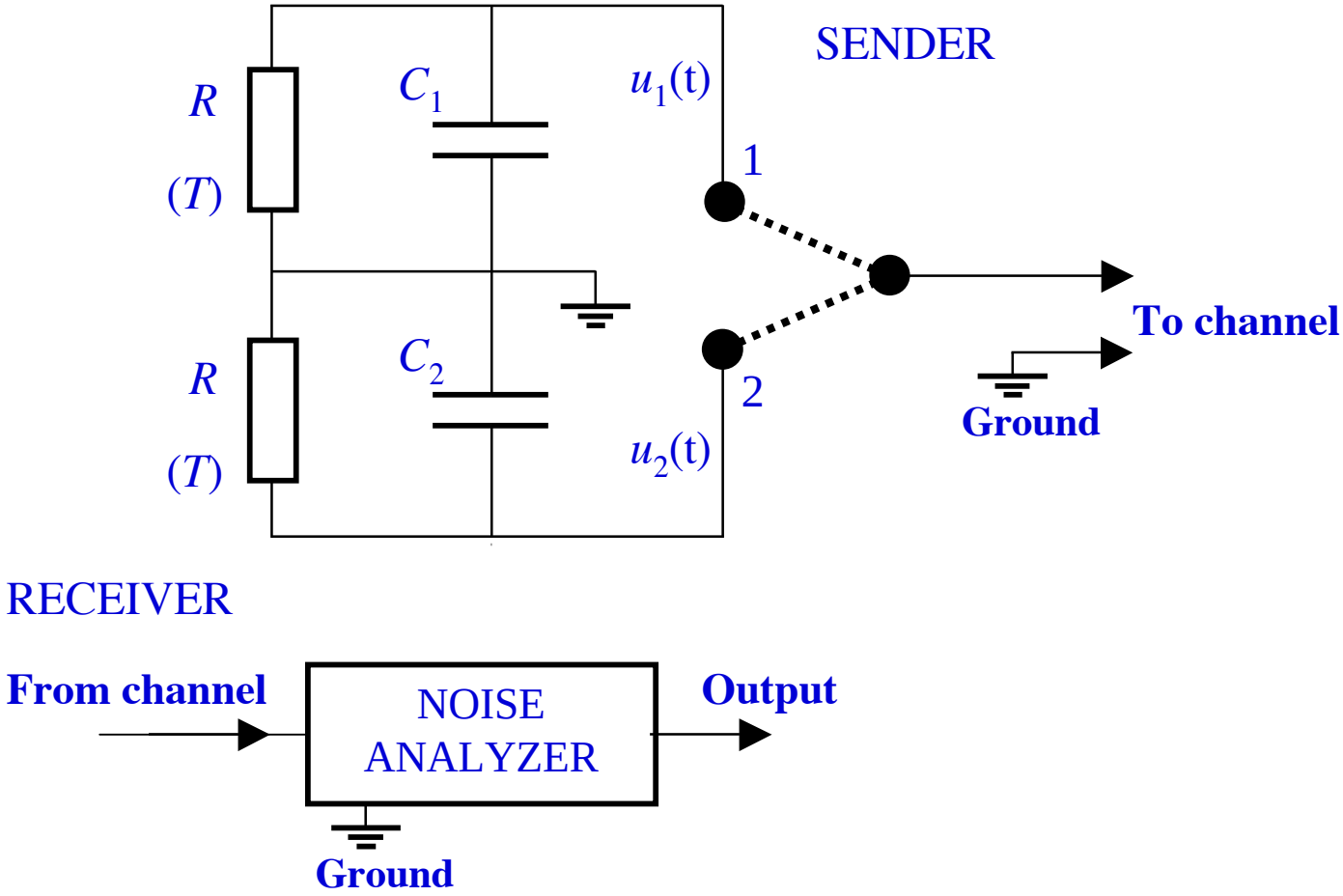


Introduction:

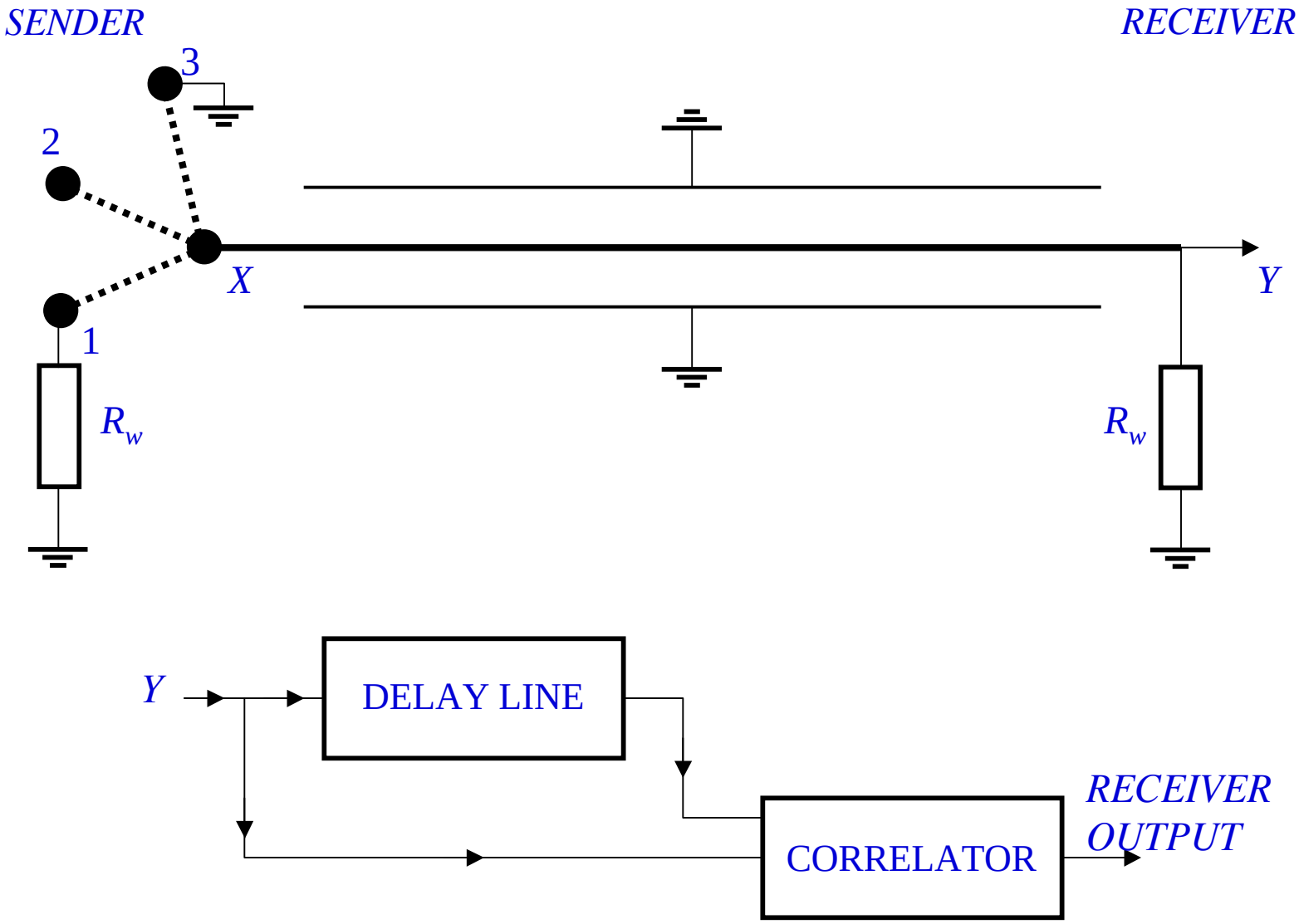
"Stealth communication: Zero-power classical communication, zero-quantum quantum communication and environmental-noise communication", *Applied Physics Lett.* **87** (December 2005), Art. No. 234109

Bandwidth-based method (for wires)

Classical: ($kT>>h/(RC)$) **Quantum:** ($kT<<h/(RC)$)

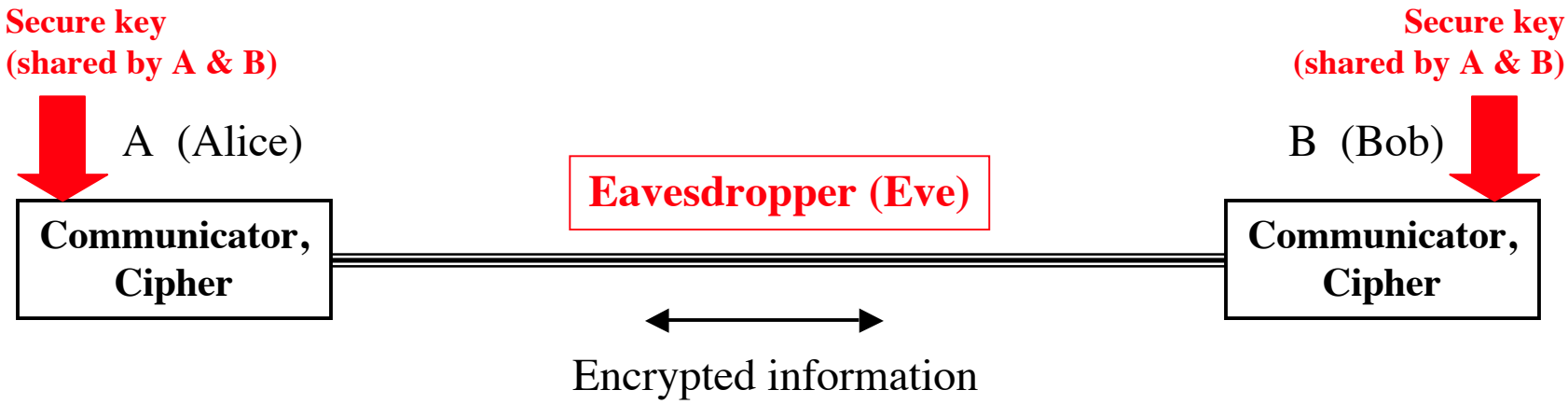


Reflection-based method (for waves)



Introduction:

Secure communication via the internet by encryption

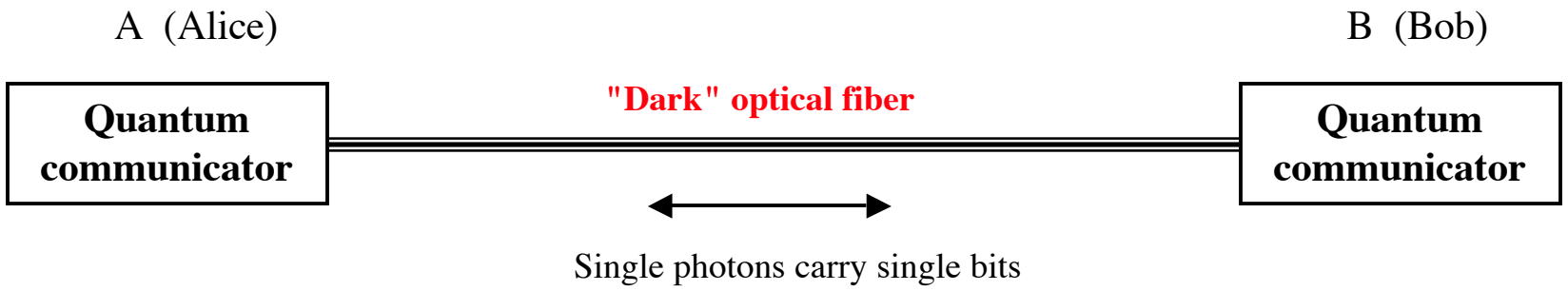


The eavesdropper (Eve) does not have the secure key thus she is unable to decrypt the information.

- ***But how to share the secret key securely through the line when Eve is watching?***
- ***The sharing of the secret key is itself a secure communication.***
- ***It is not secure, only "computationally secure". The condition is that Eve's computing hardware and/or her algorithm is not significantly more advanced than that of Alice and Bob.***

Generic quantum communicator scheme (for quantum key distribution)

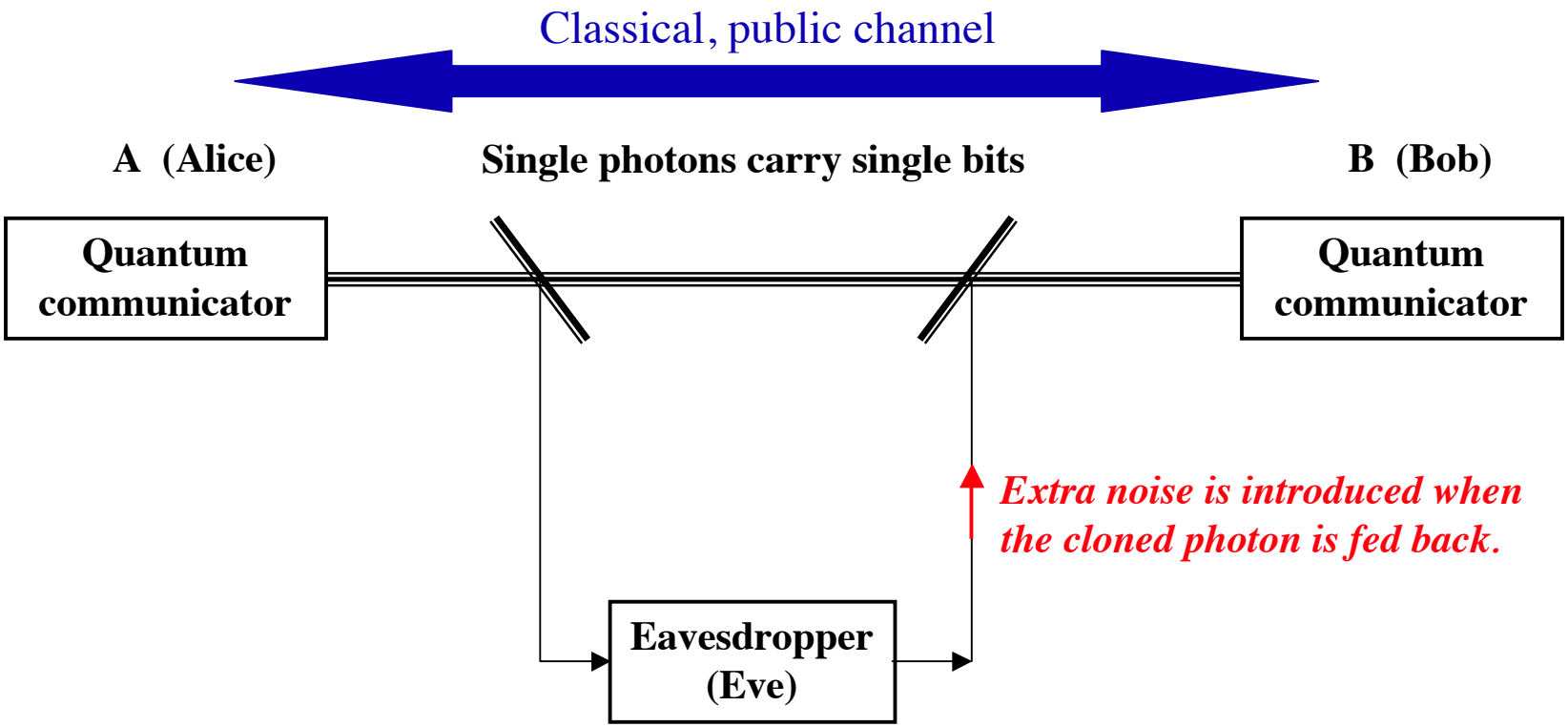
(until 2005, about $1 billion/year research funding for quantum informatics)



Actually, one photon effectively has less than a bit information due to noise in the detection, channel and detector.

Generic quantum communicator scheme (for quantum key distribution)

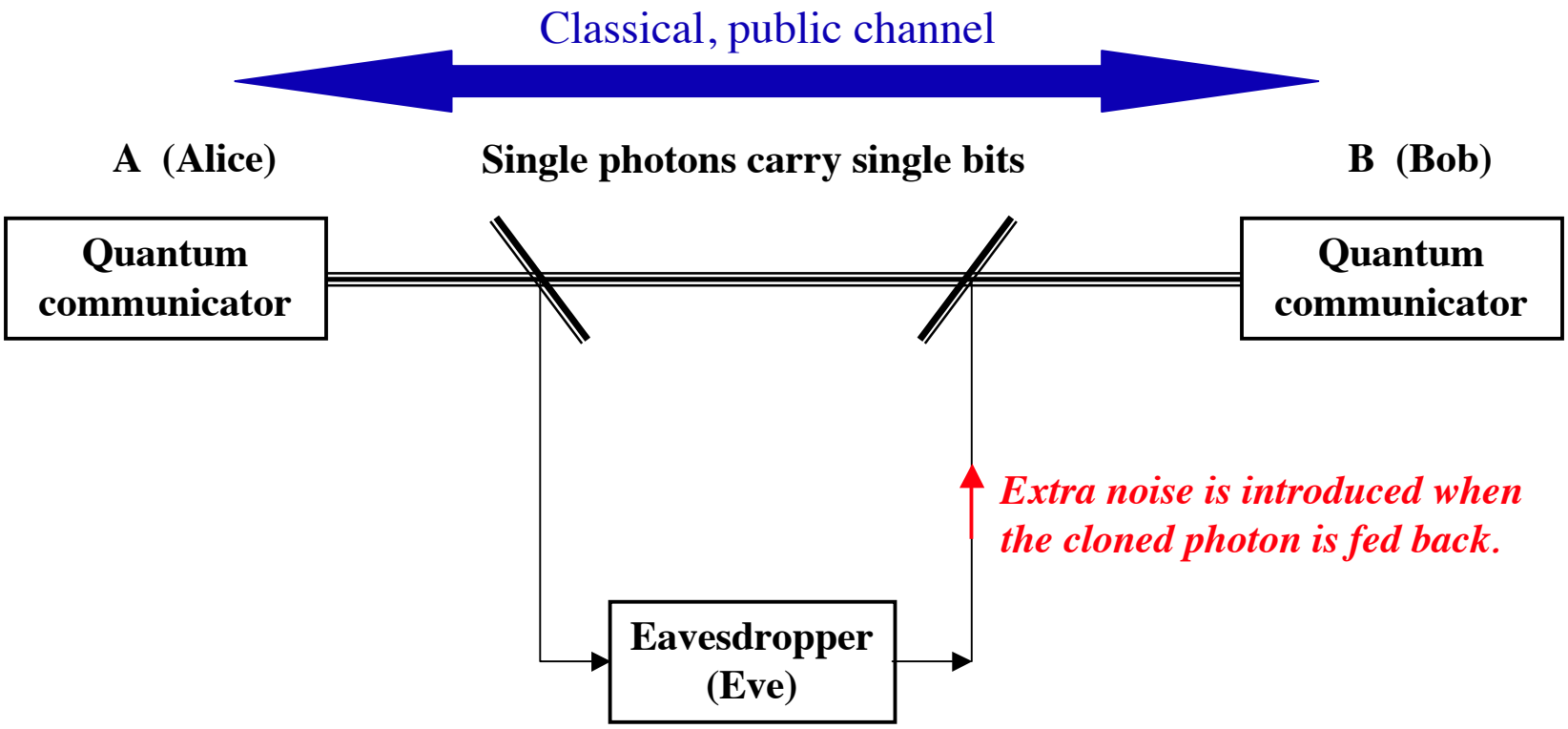
Base of security: quantum no-cloning theorem: copies of single photons will be noisy.
After making a sufficient error statistics, the eavesdropping can be discovered.



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.

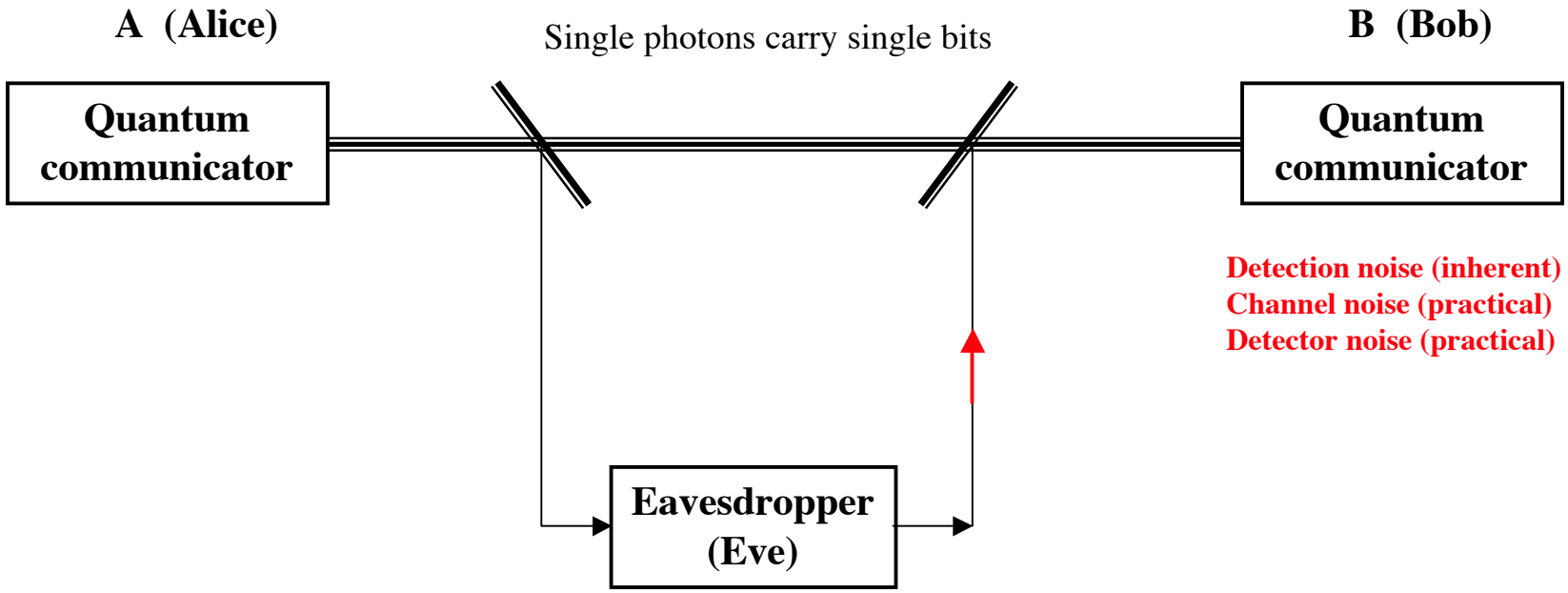
TO DISCOVER THE EAVESDROPPING WE NEED TO BUILD AND EVALUATE A STATISTICS!



Some practical problems at the conceptual level

Conceptual weakness of quantum communication is the *need of making a statistics to discover the eavesdropping*. *One-time eavesdropping on a single photon cannot be detected*. This is called *information leak*. In practical realizations, *even in the idealized case of ideal single photon source and no detector or channel noise, at least 1% of the raw bits can be extracted without a reasonable chance to discover the eavesdropping*.

THE EAVESDROPPER CAN HIDE IN THE NOISE AND COLLECT INFORMATION.



Solution (by Ch. Bennett): *Privacy Amplifier (classical information software-tool)* to make a *short, highly secure key* from a *long poorly secure key*. This can reduce the information leak by orders of magnitude.

Heretic question back in 2005

Is it possible to do absolutely secure communication with classical information?

(*When we asked it around, we had heard consistently "no" answers...*)

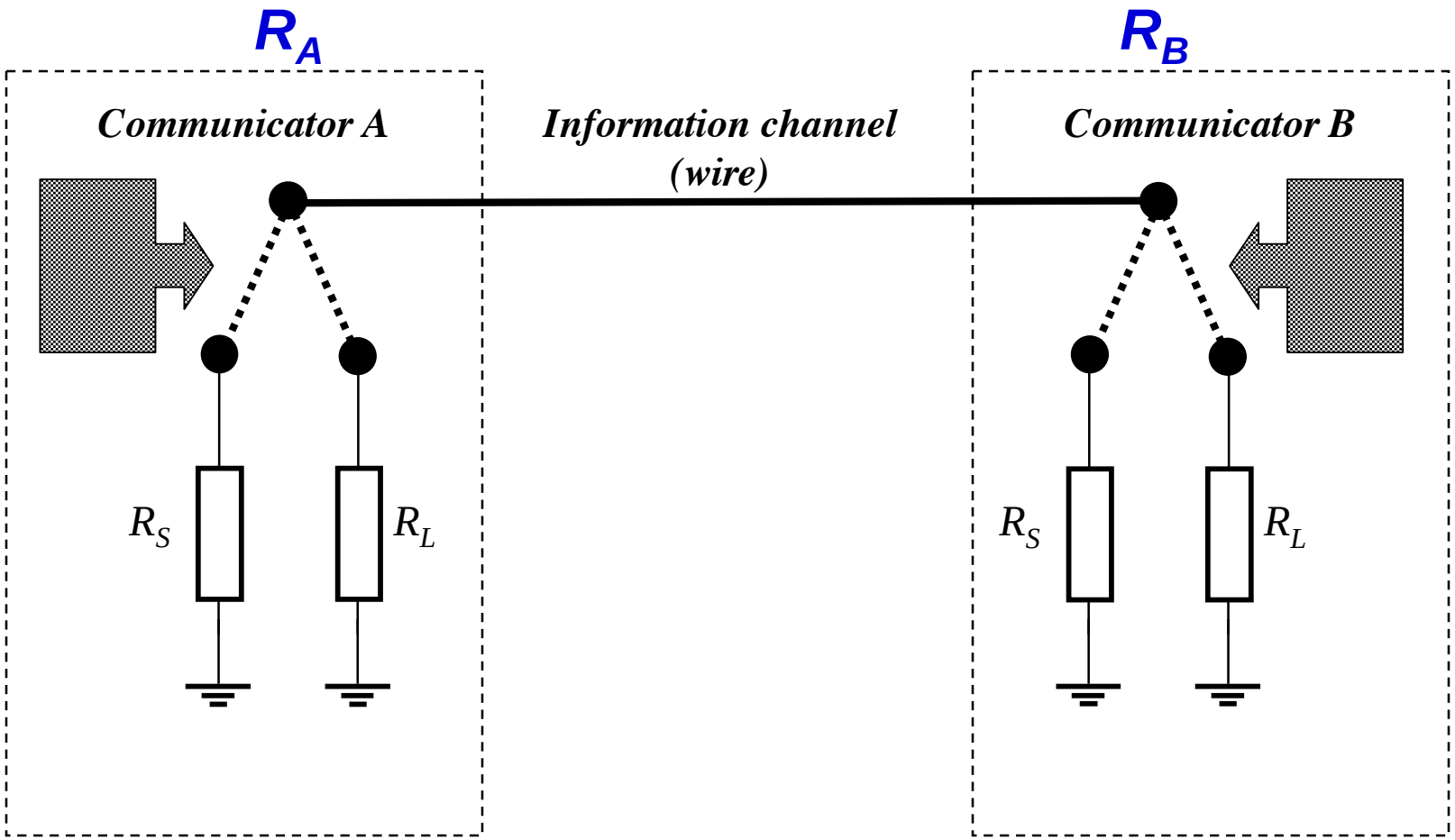
Even more heretic question back in 2005

Is it possible to do *totally secure* communication with classical information, such as ***voltage and/or current in a wire***?

Basic idea: resistor loop (Kirchhoff loop): secure key generation and sharing

Possible loop resistance R_{loop} values: $R_{loop} = 2*R_S$, $2*R_L$, $R_S + R_L$

NOTE: THIS CIRCUIT MUST BE THE CORRECT MODEL OF THE SYSTEM OTHERWISE THE SYSTEM IS NOT SECURE!

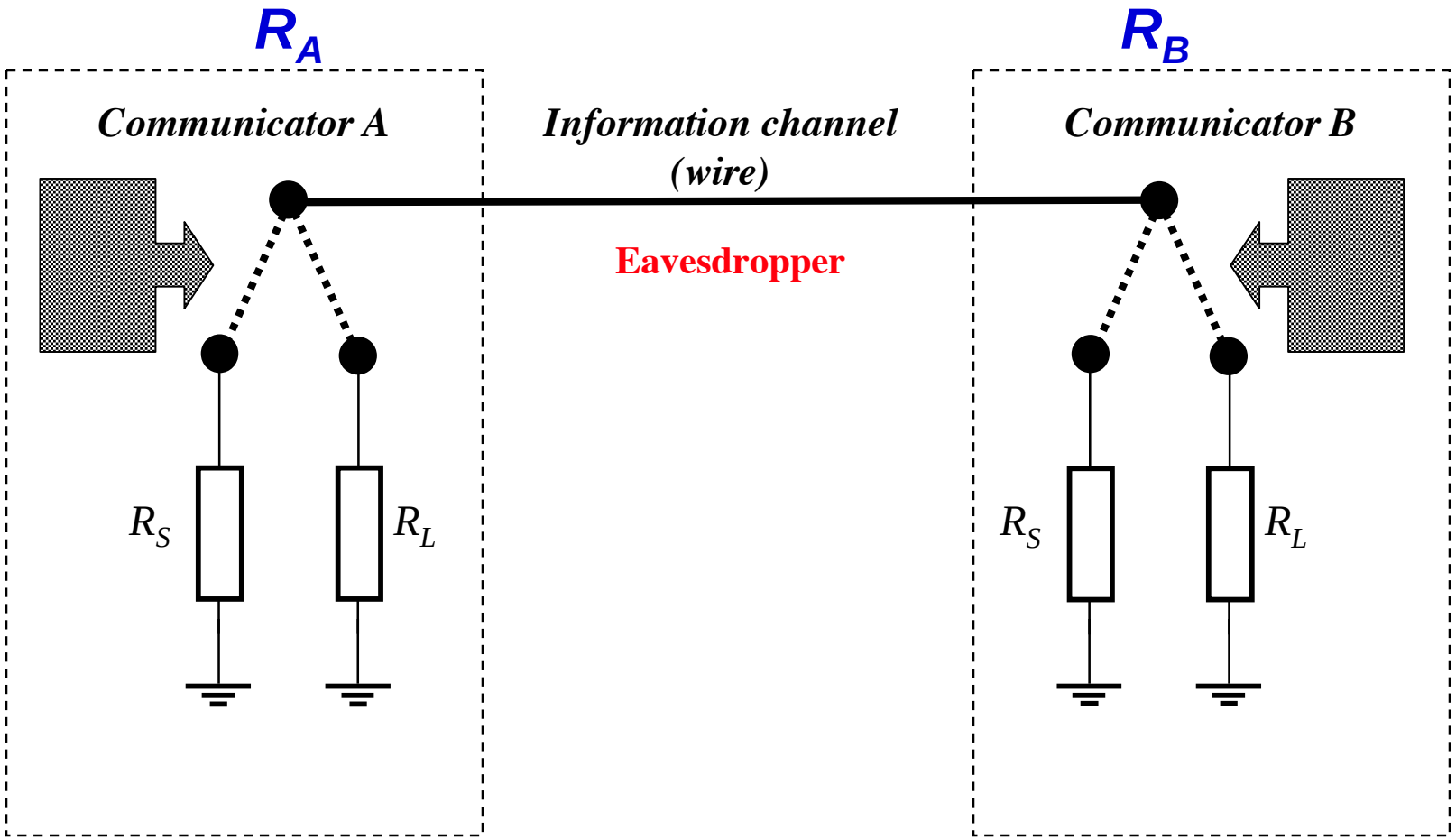


Basic idea: resistor loop (Kirchhoff loop): secure key generation and sharing

Possible loop resistance R_{loop} values: $R_{loop} = 2*R_S$, $2*R_L$, $R_S + R_L$

If the Eavesdropper was only *passively observing* and Alice and Bob could publicly measure the loop resistance *without uncovering the location of the resistors* then secure communication could be established in the mixed state:

$$R_B = R_{loop} - R_A \;;\; R_A = R_{loop} - R_B$$



CRYPTOGRAPHY

Simple Noise May Stymie Spies Without Quantum Weirdness

With the grand ambition of sending unbreakable coded messages, some physicists are using exotic tools—streams of individual photons and quantum mechanics—to shut out prying eyes. But a wire and a few resistors may convey a message as securely, says a physicist who has devised a simple and—he claims—uncrackable scheme. The idea shows that "classical" methods might compete with budding "quantum cryptography," others say. "I believe in beautiful and simple ideas, and this is one of them," says János Bergou, a theorist at Hunter College of the City University of New York.

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

Take the hypothetical secret sharers, Alice and Bob: They transform a message into binary numbers and use a numerical "key"—a secret string of random 0's and 1's—to scramble and unscramble it. Quantum cryptography allows them to pass the key under the nose of an eavesdropper, Eve, because she cannot measure the condition of a particle without affecting it. So if Alice and Bob encode the key in individual photons, Eve cannot read it without revealing herself.

But Alice and Bob might do just as well by measuring the electrical noise on the ends of a wire, says Laszlo Kish of Texas A&M University in College Station. In Kish's scheme, Alice and Bob have two resistors each, one with a big resistance and one with a small resistance. Each randomly connects one resistor or the other between his or her end of the wire and ground and measures the voltage between the wire and ground.

On average, that voltage is zero. But electrons in the resistors jiggle about with thermal energy, so the voltage fluctuates, and the size of the fluctuations, or "Johnson noise," depends on the resistances Alice and Bob choose. If both use the large resistance, the fluctuations will be big. If both use the small resistance, they will be small. And if one uses large and the other uses small, the noise takes an intermediate value.

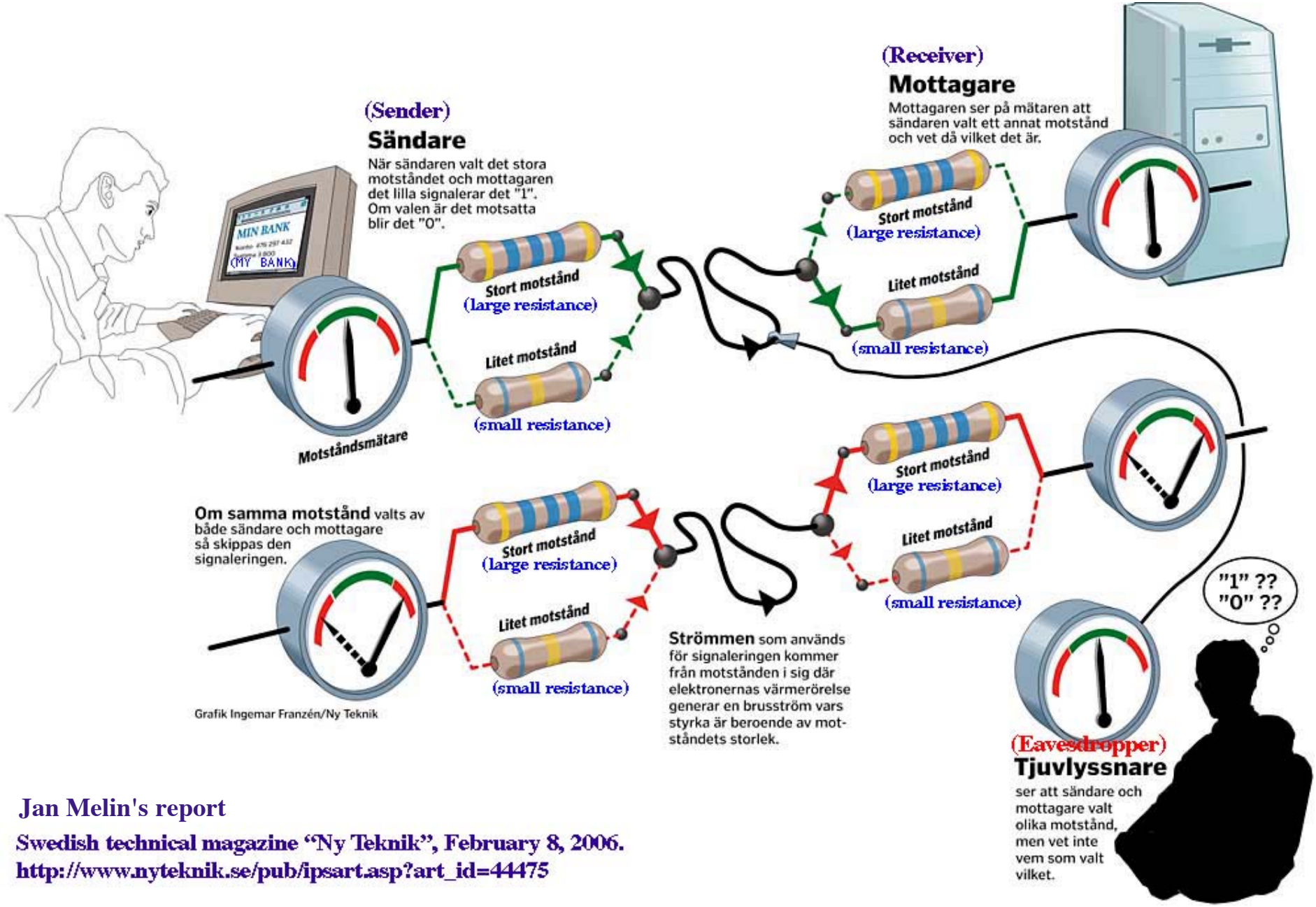
Eve can measure the fluctuations, too. But when the noise is at its intermediate level, she cannot tell whether Alice or Bob has chosen the large resistance unless she injects a current, which will reveal her presence, as Kish describes in a paper posted on the Web site www.arxiv.org and submitted to the journal *Physics Letters A*. So Alice and Bob can use the large-small pairs to generate the key.

Making the scheme work over long distances may not be easy, says Weston Tew, a physicist at the National Institute of Standards and Technology in Gaithersburg, Maryland. And Bergou notes that if the wire itself has a sizable resistance, then the fluctuations should be slightly larger on the end with the large resistance, a fact Eve might exploit if she spies on both ends at once. Still, today's quantum technologies only approximate the uncrackable ideals, and Kish's idea suggests that simpler schemes might match their performance, says Julio Gea-Banacloche, a theorist at the University of Arkansas in Fayetteville. "The more I think about it," he says, "the more I think that within limits it's workable."

–ADRIAN CHO

CREDITS (TOP TO BOTTOM): M. MASSIMINI ET AL., *SCIENCE*; PHOTODISC BLUE/GETTY IMAGES

Published by AAAS



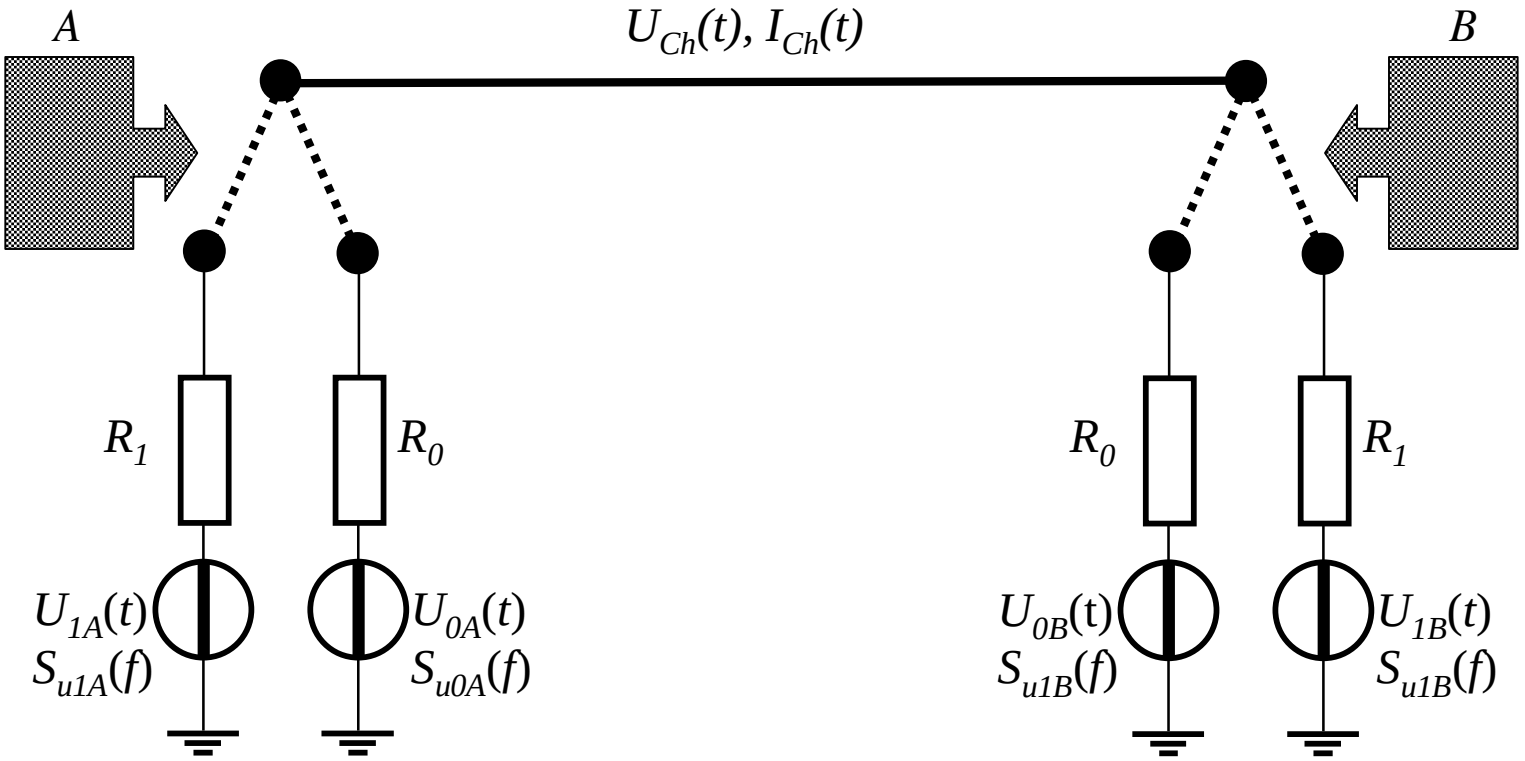
Jan Melin's report

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

Secret Key Generation and Exchange: Simplest Example for Totally Secure Classical Communication

The idealized system defined by this circuit diagram is *totally secure*, conceptually/theoretically.

The foundation of this security is: The *Second Law of Thermodynamics* (out of Kirchhoff's laws).

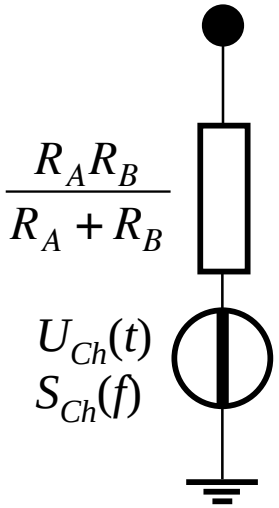


The loop resistance can be evaluated in two different ways

Johnson-Nyquist formulas for this Kirchhoff loop:

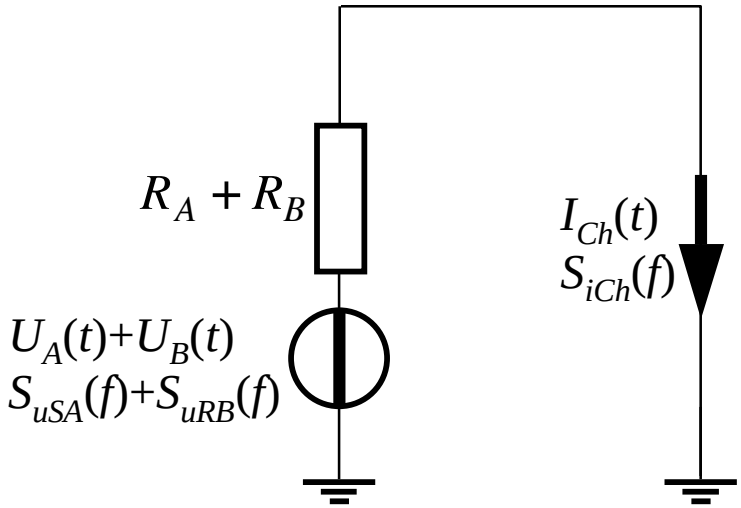
$$S_{u,R\|}(f) = 4kT\,\frac{R_A R_B}{R_A + R_B}$$

(a)

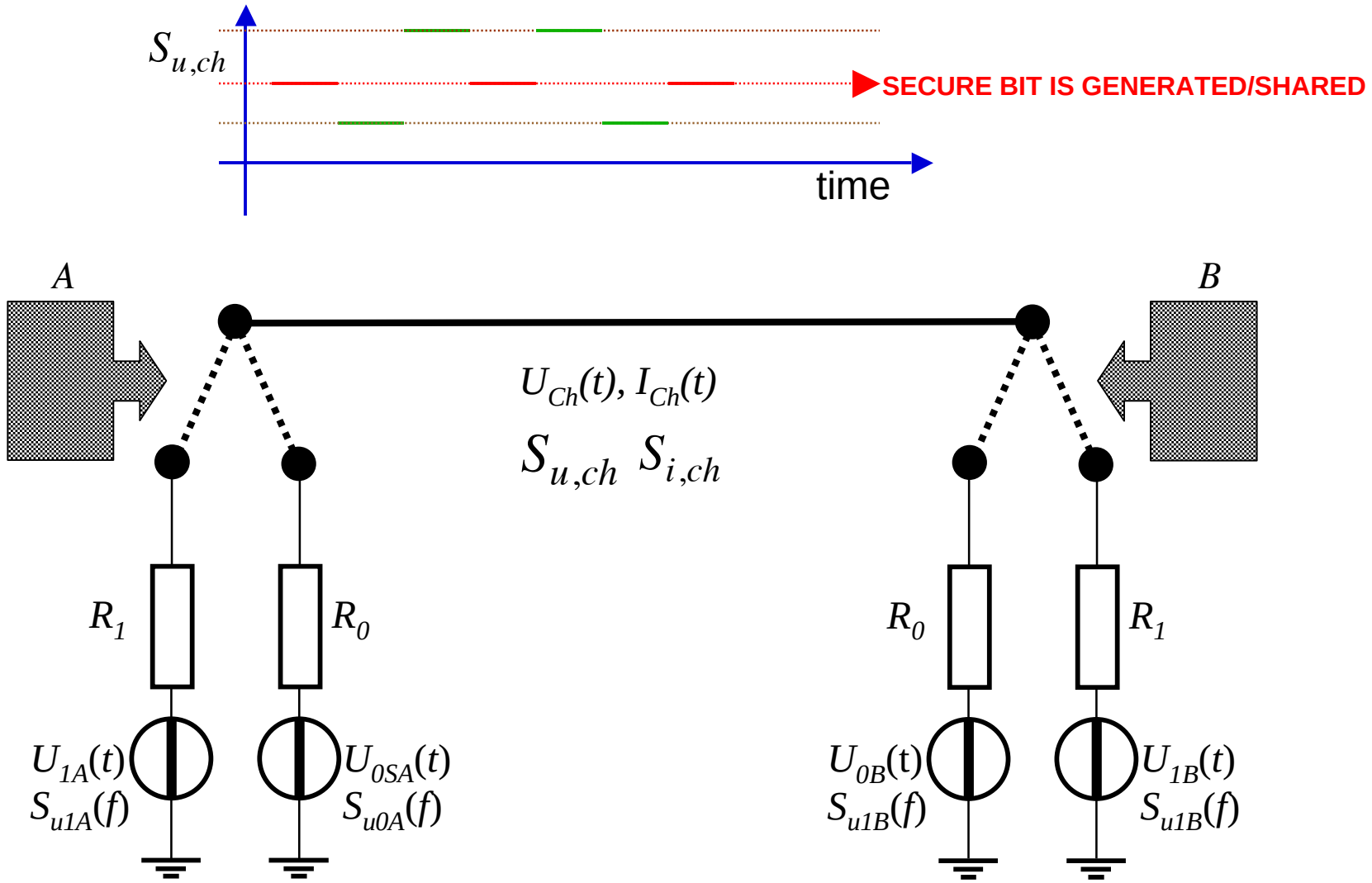


$$S_{i,R\|}(f) = \frac{4kT}{R_A + R_B}$$

(b)

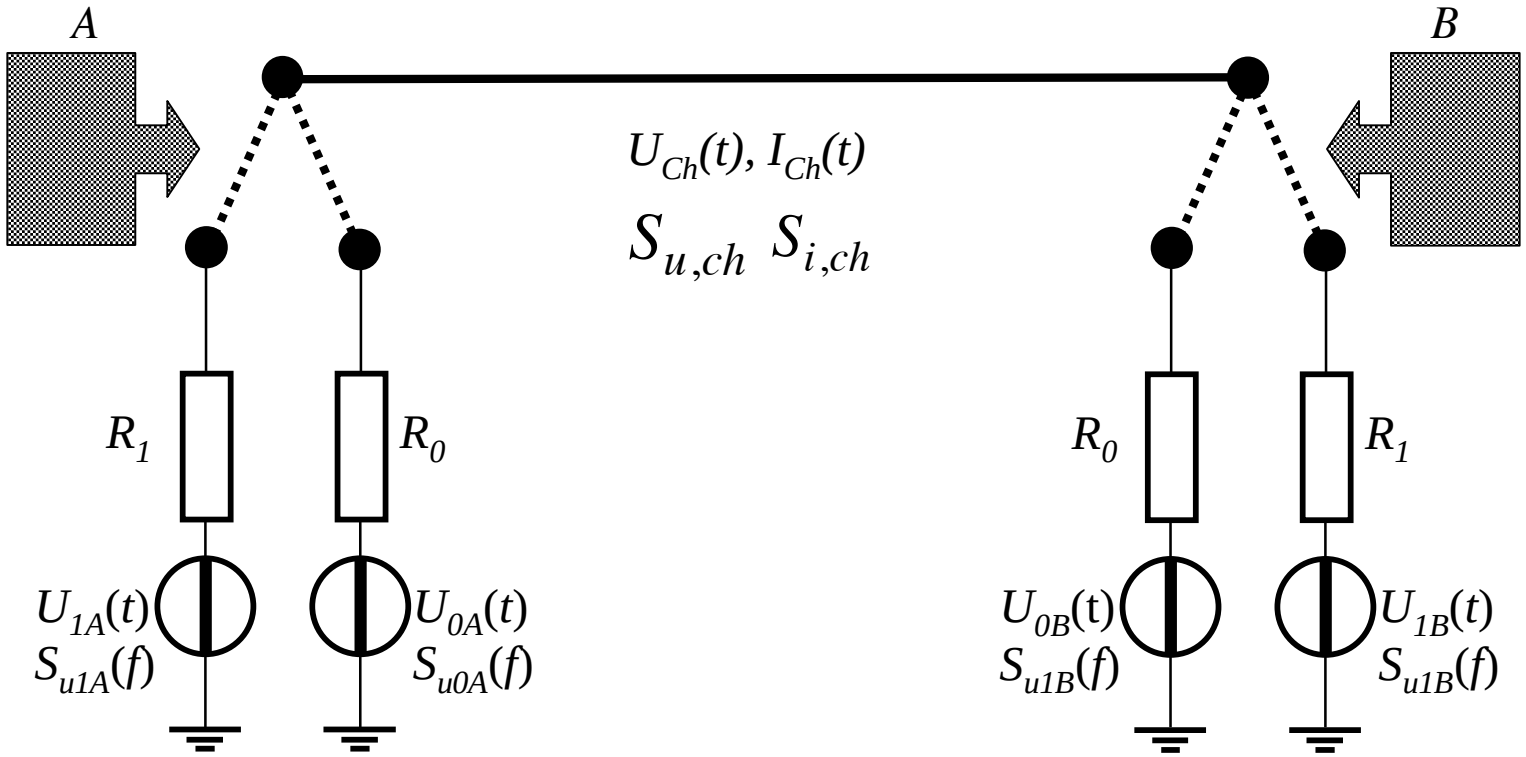


SECURE KEY GENERATION AND EXCHANGE BY VOLTAGE MEASUREMENTS



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

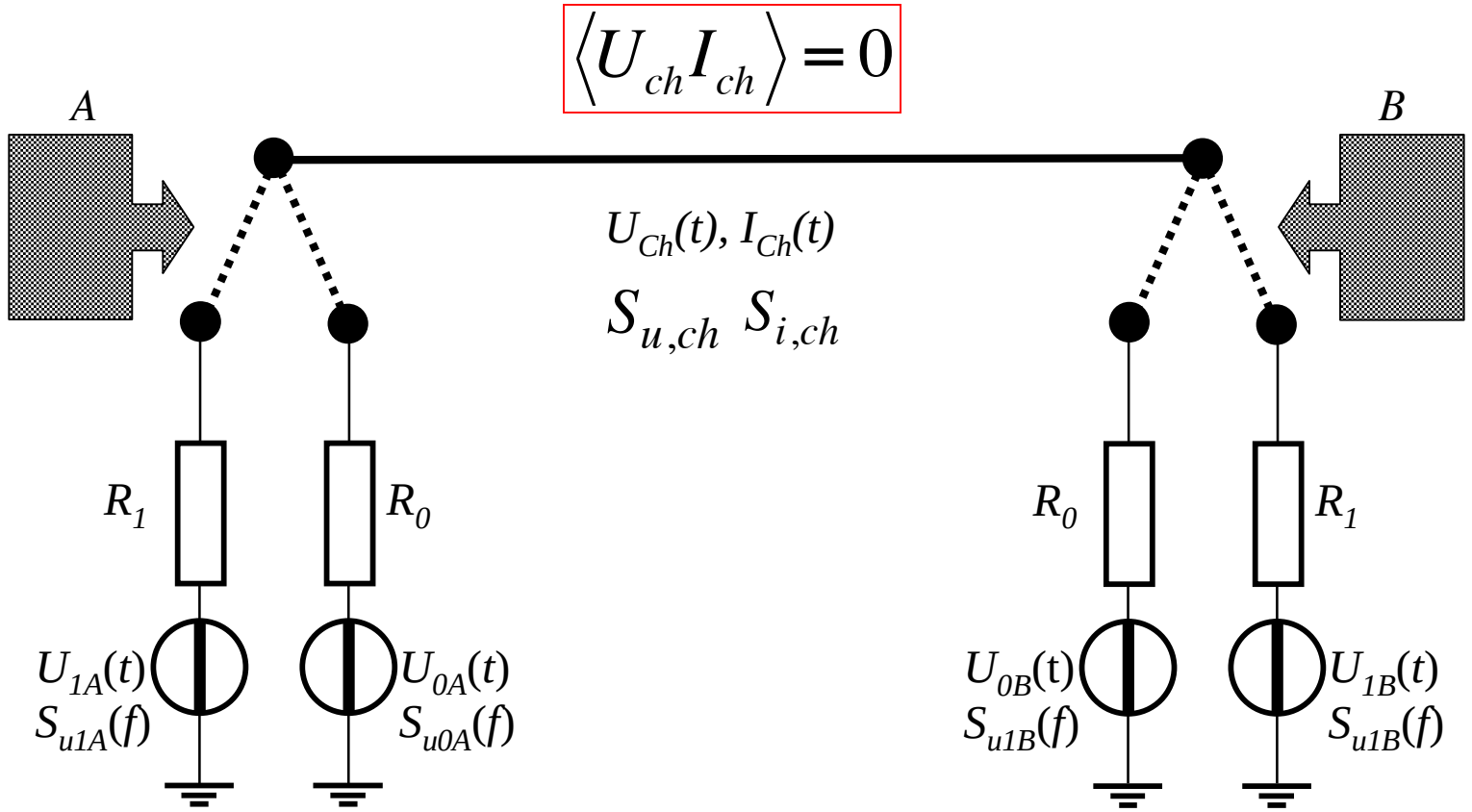
$$R_{1,2} = \frac{4kTS_{u,ch} \pm \sqrt{\left(4kTS_{u,ch}\right)^2 - 4S_{u,ch}^3 S_{i,ch}}}{2S_{u,ch}S_{i,ch}}$$



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

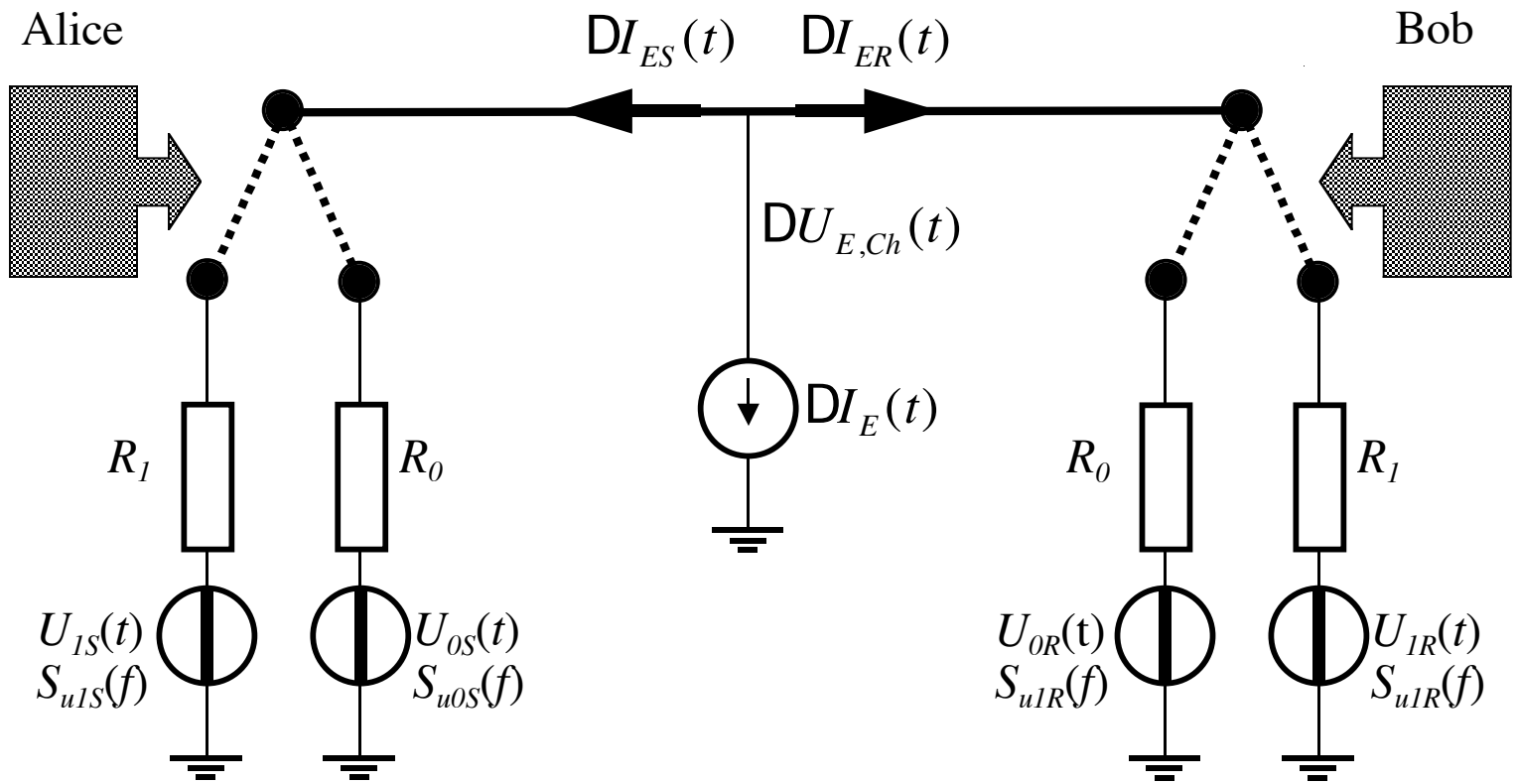
Gaussian processes **allow distribution functions** ***up to the second order only*****. But the net power flow is zero because the** ***Johnson-Nyquist formula*** **of thermal noise is based on the** ***Fluctuation-Dissipation Theorem*** **which satisfies the** ***Second Law of Thermodynamics*****.**

Therefore the total security is related to the impossibility of constructing a perpetual motion machine.



Hacking into the Communicator: Active Eavesdropping

ΔI can be small stochastic (crosscorrelation between ΔU and ΔI)
or a large, short current pulse

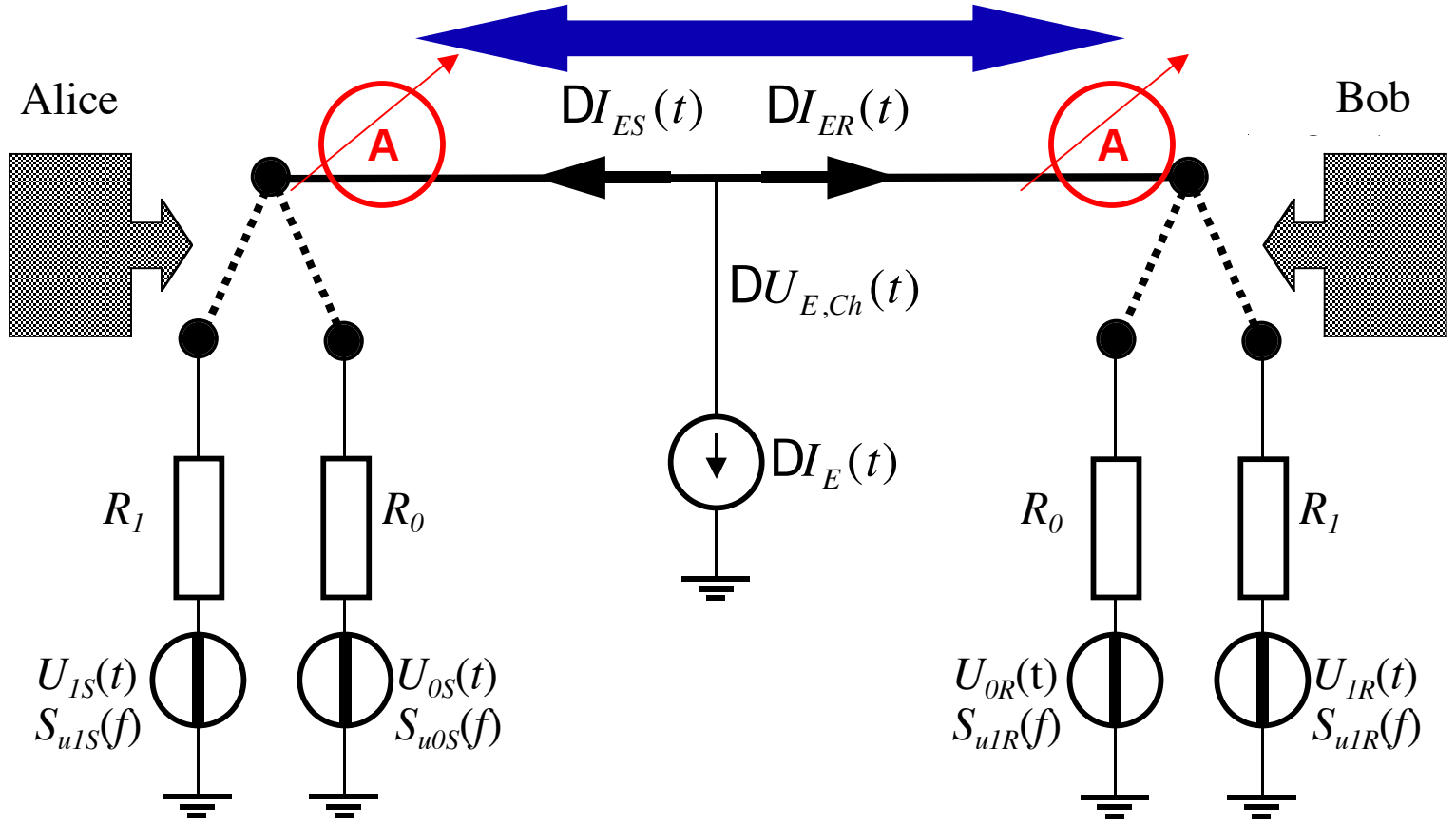


Uncovering the eavesdropper by:
Broadcasting the instantaneous current data and comparing them

THE EAVESDROPPER IS DISCOVERED WHILE EXTRACTING A SINGLE BIT OF INFORMATION.

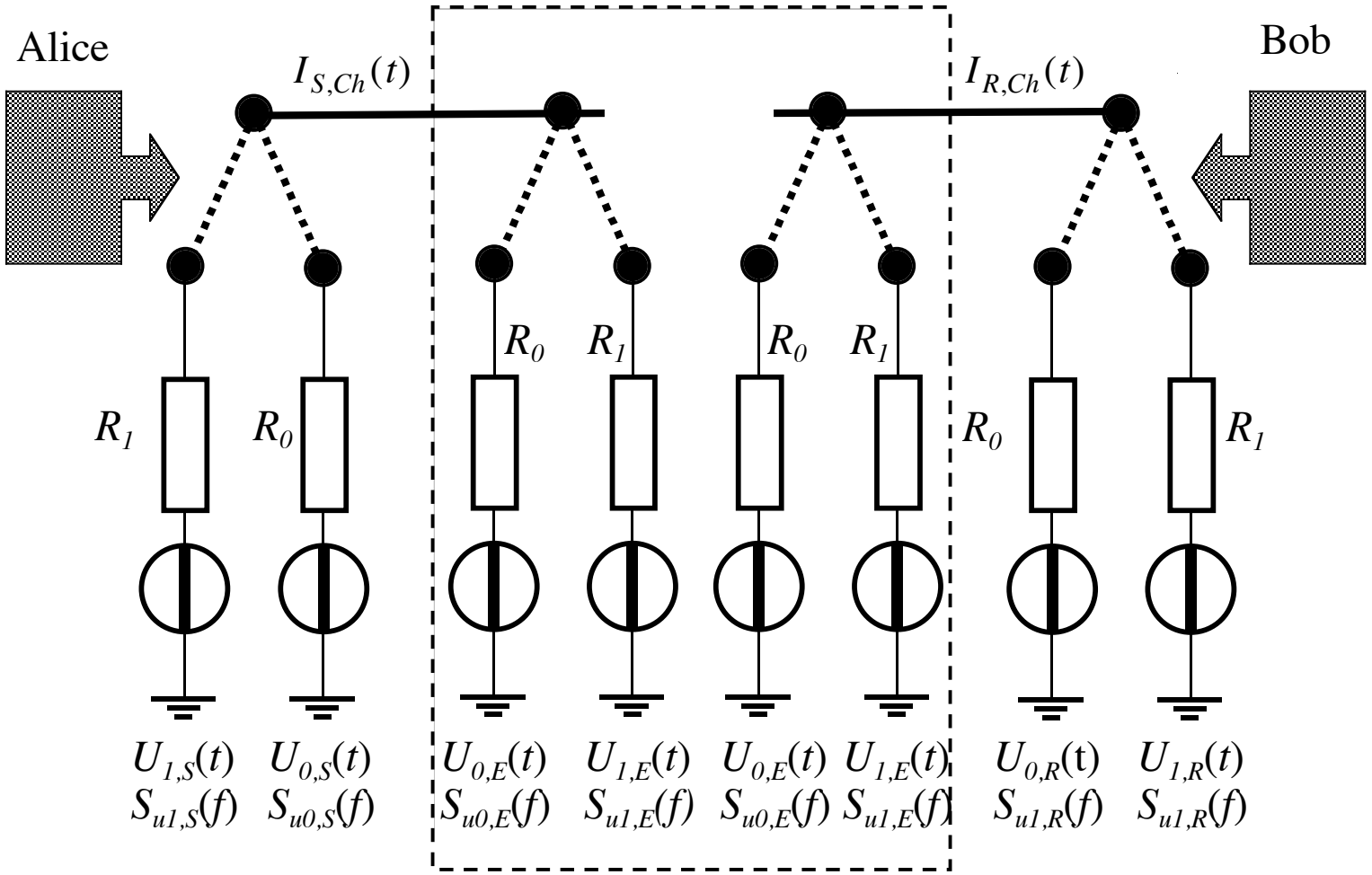
The stochastic current method can extract zero bit, the large current pulse method can extract one bit.

BETTER THAN KNOWN QUANTUM COMMUNICATION SCHEMES BECAUSE NO STATISTICS IS NEEDED.



The attack "below the belt": Man-In-The-Middle (MITM) attack

The original current-comparison naturally defends against it



Let us suppose 7 bits resolution of the measurement (a pessimistic value), then $P_0 = 1/128$, which is less than 1% chance of staying hidden. On the other hand, P_0 is the probability that the eavesdropper can stay hidden during the correlation time τ of the noise, where τ is roughly the inverse of the noise bandwidth. Because the KLJN cipher works with statistics made on noise, the actual clock period T is $N >> 1$ times longer than the correlation time of the noise used [1]. Thus, during the clock period, the probability of staying hidden is:

$$P_{clock} = P_0^N$$

Supposing a practical $T = 10\tau$ (see [1]) the probability at the other example $P < 10^{-20}$.

This is the estimated probability that, in the given system the eavesdropper can extract a single bit without getting discovered. The probability that she can stay hidden while extracting 2 bits is $P < 10^{-40}$, for 3 bits it is $P < 10^{-60}$, etc. In conclusion, we can safely say that the eavesdropper is discovered immediately before she can extract a single bit of information.

At 7 bit current comparison, the probability of staying hidden for a single clock period is less than 10^{-20}

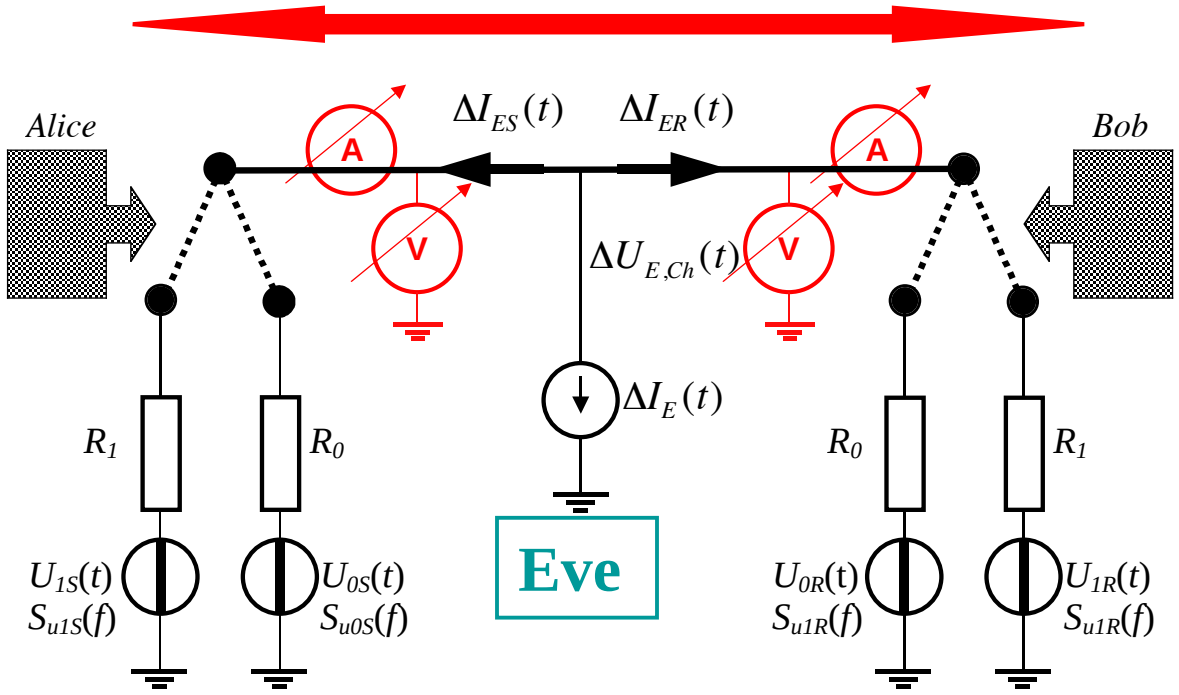
Kirchhoff-Law-Johnson-(like)-Noise (KLJN) secure key exchange.

The fully protected idealistic communicator. Protected against any passive or invasive attacks.

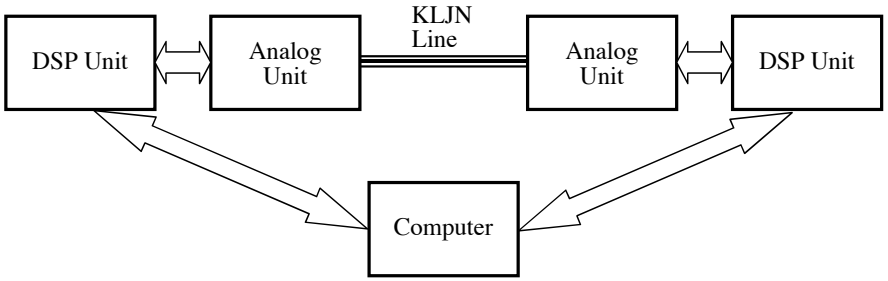
Measuring and comparing the *instantaneous* voltage and current values provides *deterministic, zero-bit security* against any invasive attacks. Thus, naturally protected against the *man-in-the-middle-attack*, too.

SECURITY GUARANTEED BY CLASSICAL PHYSICS*: THE SECOND LAW OF THERMODYNAMICS, KIRCHHOFF'S LAWS AND THE ROBUSTNESS OF CLASSICAL INFORMATION*

Public channel, broadcasting for comparing instantaneous local current (A) and voltage (V) data



R. Mingesz, Z. Gingl, L.B. Kish, ***Realization and Experimental Demonstration of the Kirchhoff-loop-Johnson(-like)-Noise Communicator for up to 2000 km range***; **www.arxiv.org/abs/physics/0612153**



The computer control parts of the communicator pair have been realized by ADSP-2181 type Digital Signal Processors (DSP) (Analog Devices).

The communication line current and voltage data were measured by (Analog Devices) AD-7865 type AD converters with 14 bits resolution from which 12 bits were used. The DA converters were (Analog Devices) AD-7836 type with 14 bits resolution. The Johnson-like noise was digitally generated in the Gaussian Noise Generator unit where digital and an alog filters truncated the bandwidth in order to satisfy the KLJN preconditions of removing any s purious frequency components. The major bandwidth setting is provided by an 8 -th order Butterworth filter with sampling frequency of 50 kHz. The remaining small digital quantization noise components are removed by analog filters.

The experiments were carried out on a model-line, with assumed cable velocity of light of $2*10^8$ m/s, with ranges up to 2000 km, which is far beyond the range of direct quantum channels, or of any other direct communication method via optical fibers. The device has bit rates of 0.1, 1, 10, and 100 bit/second for ranges 2000, 200, 20 and 2 km, respectively.

Robert Mingesz **Zoltan Gingl**

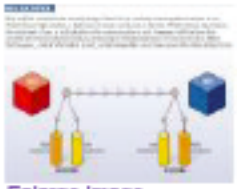
The wire diameters of the line model are selected so that they resulted in about 200 Ohm internal resistance for all the different ranges. The corresponding copper wire diameters are reasonable practical values for the different ranges are 21 mm (2000 km), 7 mm (200 km), 2.3 mm (20 km) and 0.7 mm (2 km). Inductance effects are negligible with the selected resistance values, R_0 and R_1, at the given ranges and the corresponding bandwidths. If the wire is a free hanging one with a few meters separation from earth, such as power lines, parasitic capacitances are not a problem up to 10% of the nominal range. For longer ranges than that, either coaxial cables driven by the capacitor killer are needed or the speed/bandwidth must be decreased accordingly.

Noise keeps spooks out of the loop

23 May 2007
NewScientist.com news service
D. Jason Palmer

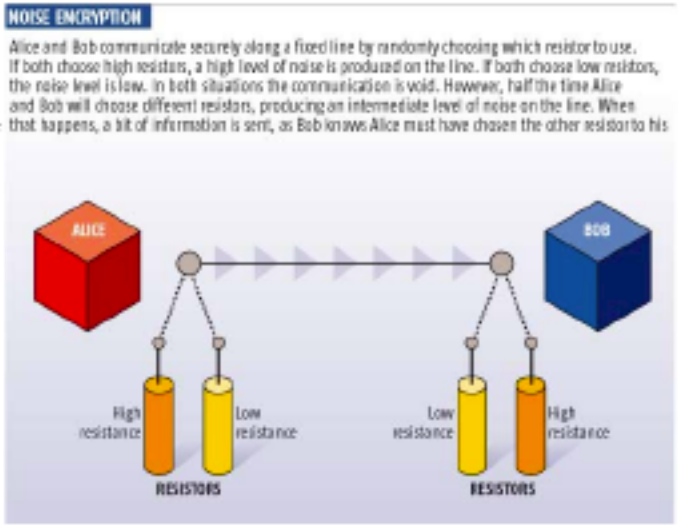
SPYING is big business, and avoiding being spied on an even bigger one. So imagine if someone came up with a simple, cheap way of encrypting messages that is almost impossible to hack into?

American computer engineer Laszlo Kish at Texas A&M University in College Station claims to have done just that. He says the thermal properties of a simple wire can be exploited to create a secure communications channel, one that outperforms quantum cryptography keys.



Enlarge image
Noise encryption

His cipher device, which he first proposed in 2005, exploits a property called thermal noise. Thermal noise is generated by the natural agitation of electrons within a conductor, which happens regardless of any voltage passed through it. But it does change depending on the conductor's resistance.



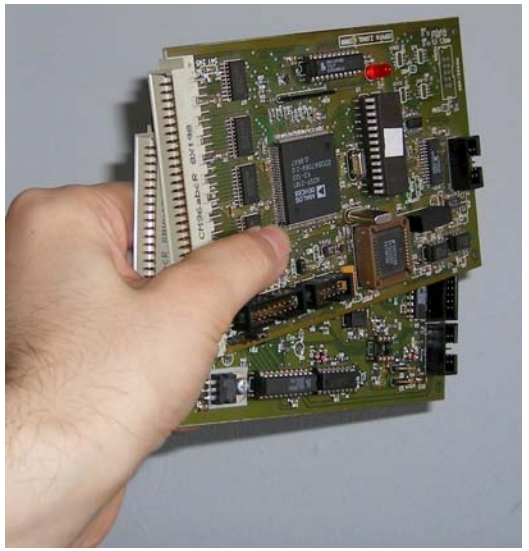
Kish and his collaborators at the University of Szeged in Hungary say this can be used to securely pass information, or an encryption key, down any wire, including a telephone line or network cable. In their device, both the sender Alice and the receiver Bob have an identical pair of resistors, one producing high resistance, the other low resistance. The higher the total resistance on the line, the greater the thermal noise.

Both Alice and Bob randomly choose which resistor to use. A quarter of the time they will both choose the high resistor, producing a lot of noise on the line, while a quarter of the

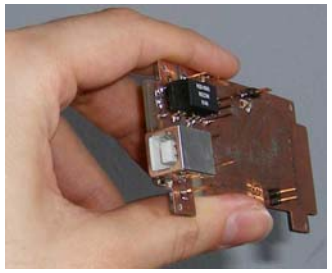
The prototypes of the two internet network elements, quantum and classical (enhanced Johnson) noise. Pictures from 2006.

Quantum telecloning to 2 network Units, **Fidelity ≈ 60%**, at Furusawa's Lab (Tokyo)
http://aph.t.u-tokyo.ac.jp/~furusawa/t_Lab_Setup.jpg

Kirchhoff-Johnson network element tested
Fidelity 99.98%



Future Kirchhoff-Johnson network element



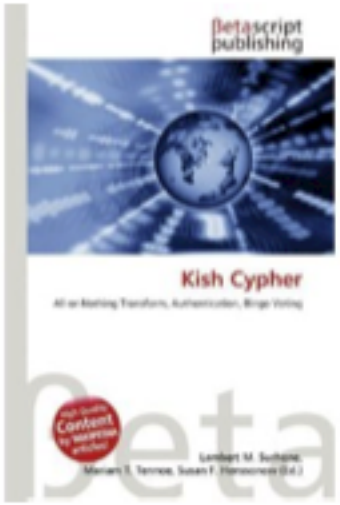
Hello. Sign in to get personalized recommendations. New customer? Start here.

Up to 50% off select Father's Day gifts
Presented by DEWALT

Your Amazon.com | Today's Deals | Gifts & Wish Lists | Gift Cards | Your Digital Items | Your Account | Help

Shop All Departments | Search Books | Cart | Wish List

Books | Advanced Search | Browse Subjects | New Releases | Bestsellers | The New York Times® Bestsellers | Libros en español | Bargain Books | Textbooks



See larger image

Share your own customer images

Publisher: learn how customers can search inside this book.

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.

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

11 used & new from $61.98

Have one to sell?

Share

Some other people are making money of it :-)

Product Details

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

The focus question:

Two contradictory statements:

1. It was said: secure communication requires "quantum" because quantum information is **very fragile** and that fragility is essential for security.

2. We will see that classical information can be even more secure because classical information is **extremely robust**. ***Its security is superior to quantum security:***

   - Zero-bit eavesdropping security;

   - Natural, zero-bit defense against the Man-in-the-Middle-Attack.

What is the outcome of these two contradictory claims?

The focus question:

Secure communication needs stochastics

(the common factor in the quantum and classical secure communication methods).

Noise-based logic:
The logic information is carried by noise (stochastic processes)

Motives

1. To reduce power dissipation and the related heat.

2. To achieve deterministic multi-valued logic.

3. To utilize superpositions and the logic hyperspace: 2^N bits [2^(2^*N*) logic values] in a single wire, like in a quantum computer.

4. Deterministic, multivalued brain logic with stochastic neural spikes.

5. Special-purpose large, parallel operations with low hardware/time complexity.

Present and past collaborators to noise-based logic (Alphabetical order of coathors).

Brown color: joint results in this talk.

Sergey Bezrukov (NIH): brain: information processing/routing, circuitry, efficiency, etc.

Zoltan Gingl (Univ. of Szeged, Hungary): modeling for circuit realization, etc.

Tamas Horvath (Frauenhofer for Computer Science, Bonn, Germany): string verification

Sunil Khatri, (computer engineering faculty, TAMU): hyperspace, squeezed instantaneous logic, etc

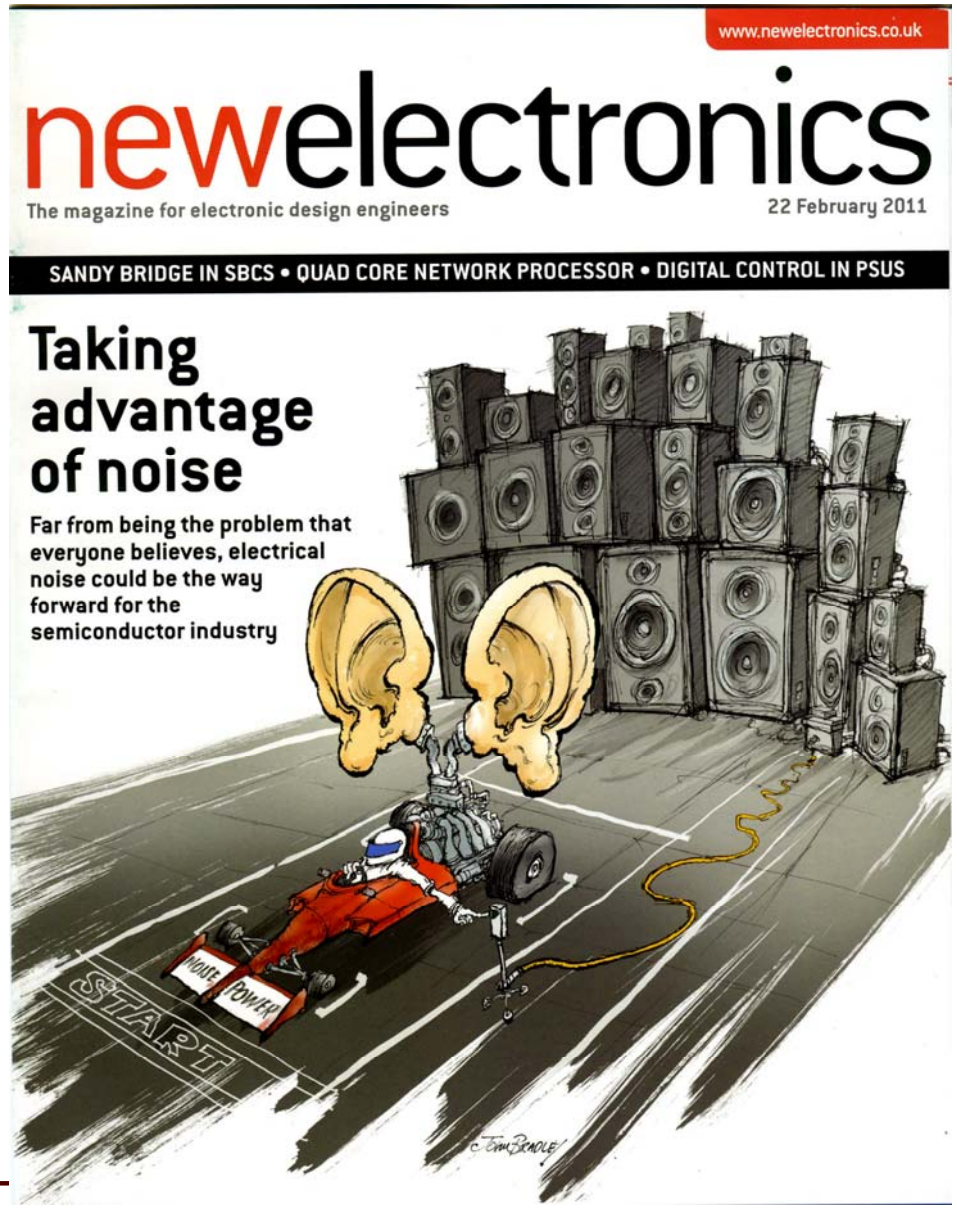
Ferdinand Peper (Kobe Research Center, Japan): squeezed and non-squeezed instantaneous logic, etc.

Swaminathan Sethuraman (former math. PhD student, TAMU): "Achilles ankle operation".

Khalyan Bollapalli (former computer engineering PhD student, TAMU): sinusoidal version

Zoltan Bacskai (physics PhD student, Univ. of Szeged, Hungary): some useful comments

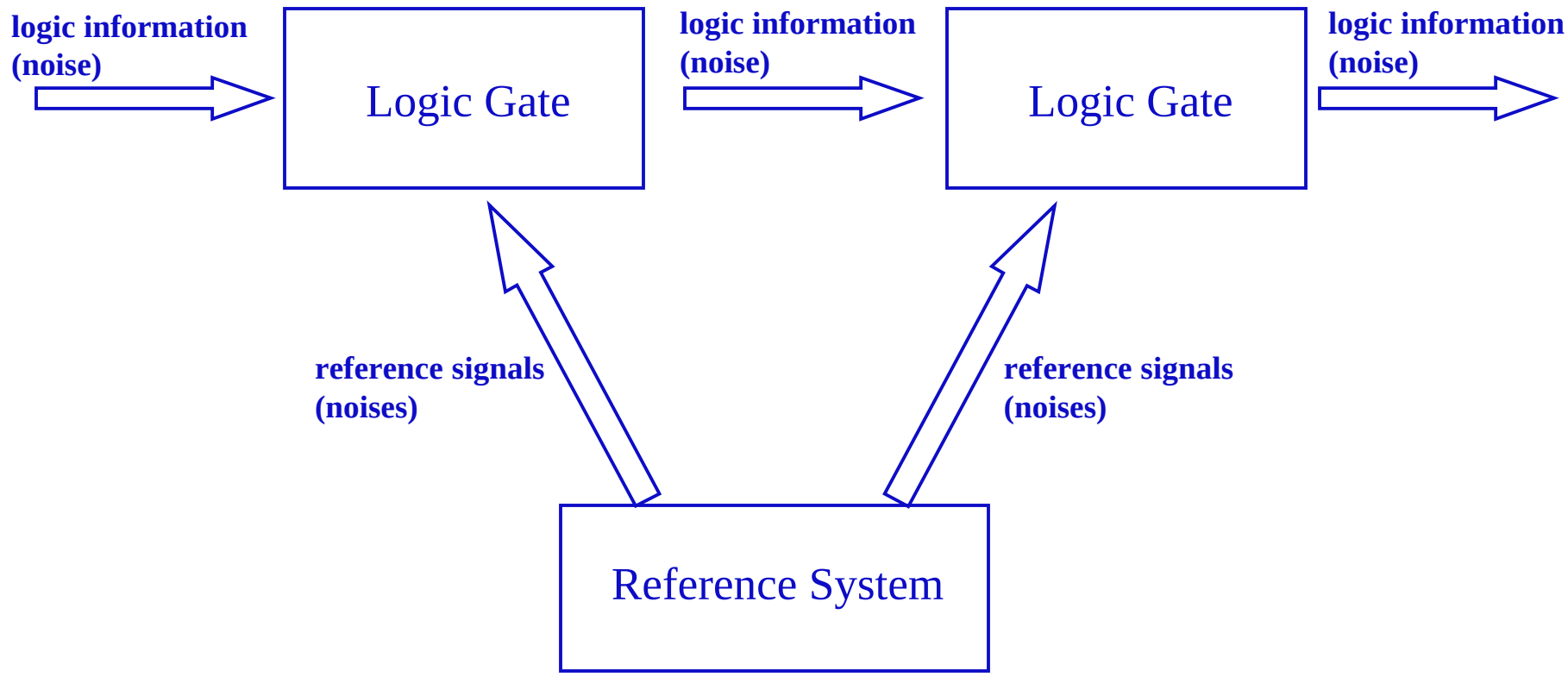
"noise-based logic is one of the most ambitious attempts..."



Our related "*non-repetition*" papers in chronological order (brown: subject of this talk):

- L.B. Kish, "Thermal noise driven computing", *Appl. Phys. Lett.* **89** (2006) 144104; http://arxiv.org/abs/physics/0607007
- L.B. Kish, "Noise-based logic: binary, multi-valued, or fuzzy, with optional superposition of logic states.", *Physics Letters A* **373** (2009) 911-918; http://arxiv.org/abs/0808.3162
- L.B. Kish, S. Khatri, S. Sethuraman, "Noise-based logic hyperspace with the superposition of 2^N states in a single wire", *Physics Letters A* **373** (2009) 1928-1934, http://arxiv.org/abs/0901.3947
- S. Bezrukov, L.B. Kish, "Deterministic multivalued logic scheme for information processing and routing in the brain", *Physics Letters A* **373** (2009) 2338-2342, http://arxiv.org/abs/0902.2033
- K. Bollapalli, S. Khatri, L.B. Kish, "Low-Power VLSI Design using Superposition of Sinusoidal Supplies" *Austin Conference on Integrated Systems and Circuits* (ACISC) 2009.
- L.B. Kish, S. Khatri, F. Peper, "Instantaneous noise-based logic", *Fluctuation and Noise Letters* **9** (2010 December) 323-330.
- Z. Gingl, S. Khatri, L.B. Kish, "Towards brain-inspired computing", *Fluctuation and Noise Letters* **9** (2010 December) 403-412.
- L.B. Kish, S. Khatri, T. Horvath, "Computation using Noise-based Logic: Efficient String Verification over a Slow Communication Channel", *European Journal of Physics B* **79** (2011 January) 85-90, http://arxiv.org/abs/1005.1560
- F. Peper, L.B. Kish, "Instantaneous, non-squeezed, noise-based logic", *Fluctuation and Noise Letters* **10** (June 2011) 231-237.

Generic noise-based logic outline



To identify and manipulate (gates) of the logic states (stochastic processes):

- **Correlators (includes multiplication and time average of zero-mean noises);** **Correlator-based**

- **Algebraic operations between stochastic processes (no time average);**
- **Set-theoretical operations (coincidence based, no time average): brain logic**

} **Instantaneous**

Types of noise-based logic envisioned so far:

Correlator-based noise-based logic

Boolean (universal) **Multivalued**

Instantaneous noise-based logic

Boolean (universal) **Multivalued**

Correlator-based-noise-based logic:

Binary, multi-valued, or fuzzy, with optional superposition of logic states

L.B. Kish, *Physics Letters A* **373** (2009) 911-918, (http://arxiv.org/abs/0808.3162)

Noises: ***independent realizations of a stochastic process (electronic noise) with zero mean.***

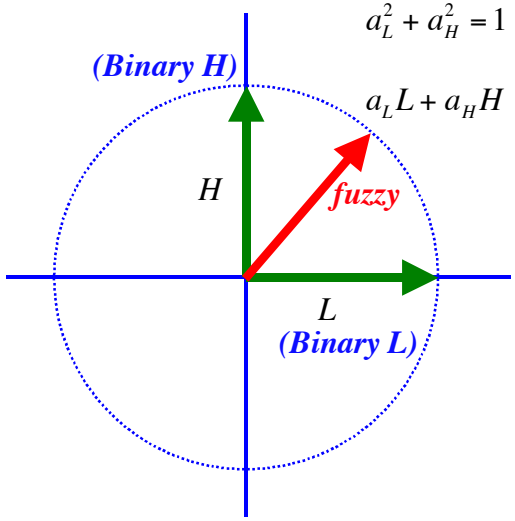
Examples: thermal noises of different resistors or current noises of different transistors: $V_k(t)$

N-dimensional logic space with orthogonal logic base vectors:

$$\langle V_i(t)V_j(t)\rangle = \delta_{i,j}$$

Generally, a logic state vector is the weighted superposition of logic base vectors:

$$X(t) = \sum_{i=1}^{N} a_i V_i(t)$$



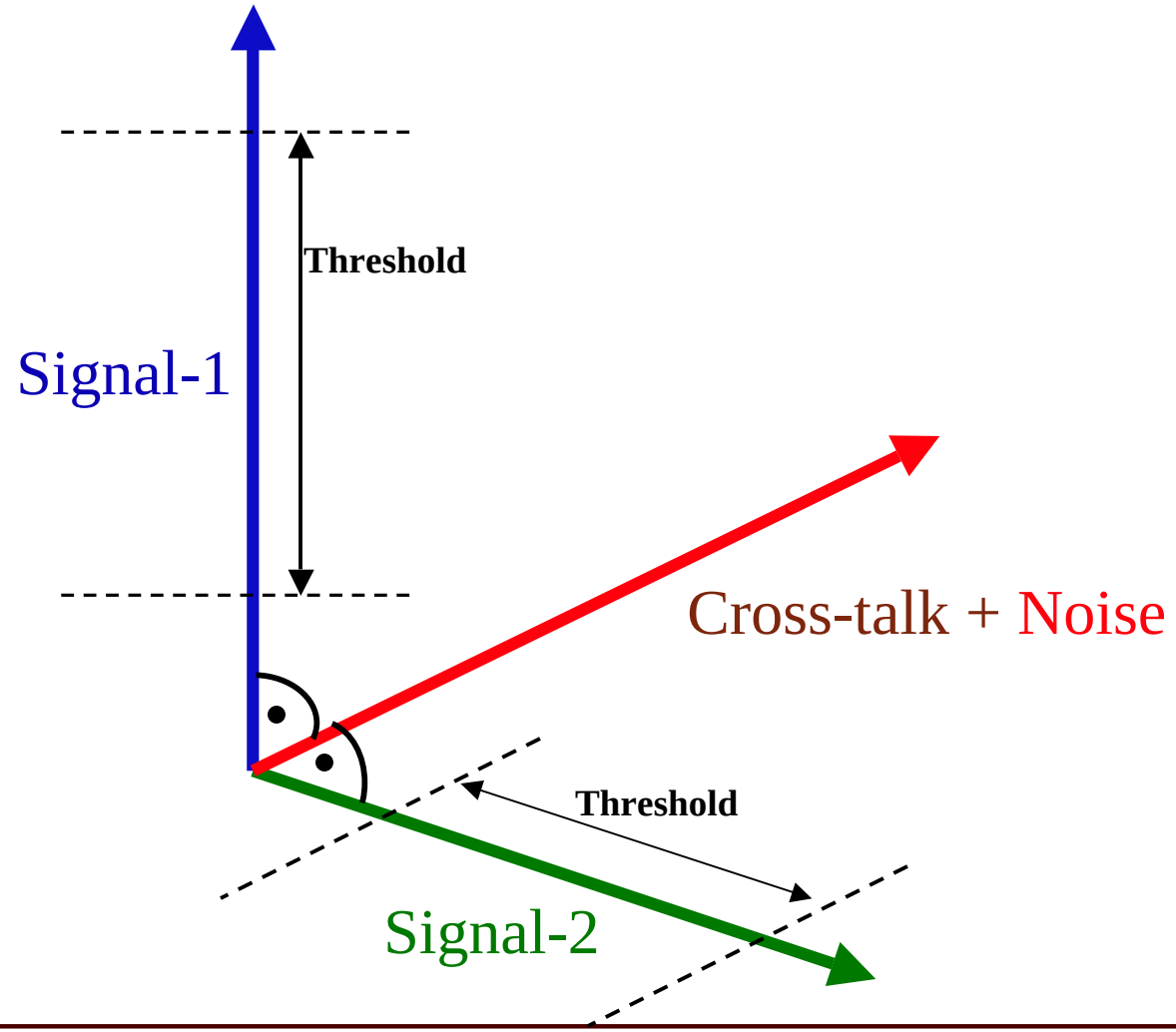
For example, a binary logic base is:

$$\langle L^2(t)\rangle = 1 \qquad \langle H^2(t)\rangle = 1 \qquad \langle H(t)L(t)\rangle = 0$$

Multidimensional logic hyperspace was also introduced by multiplying the base noises, see later.

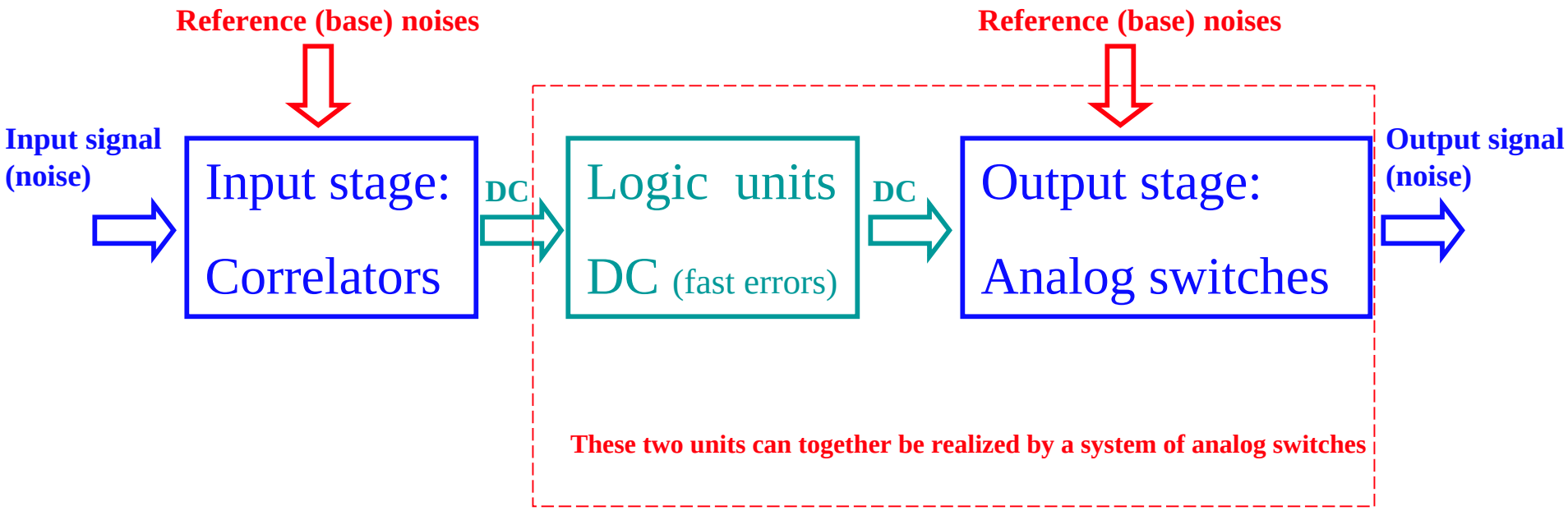
1. Can we use signals which is orthogonal on the crosstalk+noise?
2. Can we use N>1 signals which are orthogonal to each other, to make a multivalue logic?

If we use superposition of the vectors in a binary fashion (on/off) then an N-dimensional signal space would make a logic scheme with $K=2^N$ logic values in a single wire. Orthogonal sinusoidal signals would do, however the smallest possible signal is the noise in the information channel. Thus we explore the noise-based direction here.



Basic structure of noise-based logic with continuum noises:

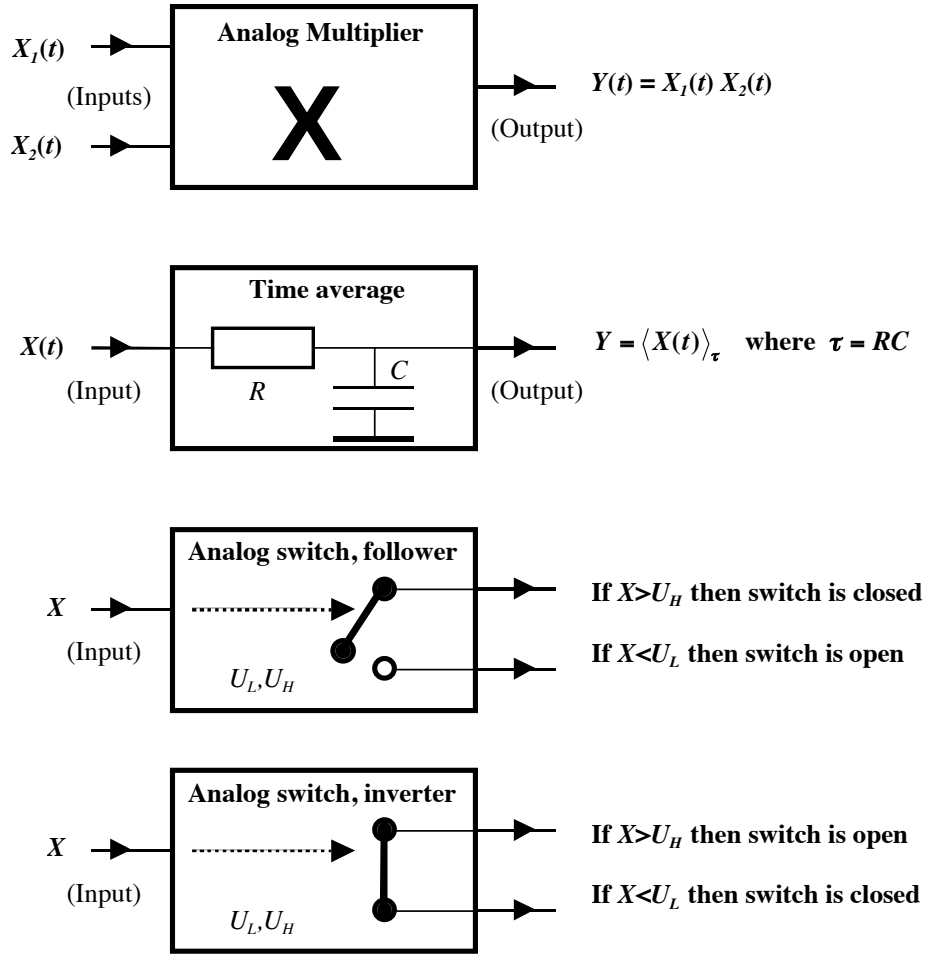
L.B. Kish, *Physics Letters A* **373** (2009) 911-918



Note: analog circuitry but *digital accuracy* due to the saturation operation represented by the switches!

The basic building elements of noise based-logic (out of the noise generators which can be simply resistors or transistors) are **the same as that of analog computers:** linear amplifiers; analog multipliers; adders; linear filters, especially time average units which are low-pass filters; analog switches; etc.

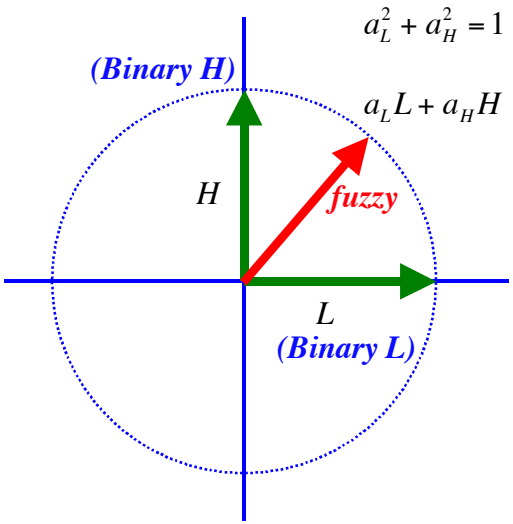
Note: analog circuitry but *digital accuracy* due to the saturation operation represented by the switches!



Logic hyperspace by multiplying the base noises:

If $i \neq k$ and $H_{i,k}(t) \equiv V_i(t)V_k(t)$ then for all $n = 1...N$, $\left\langle H_{i,k}(t)V_n(t)\right\rangle = 0$

The hyperspace can be grown further by multiplying hyperspace vectors made with different base elements.



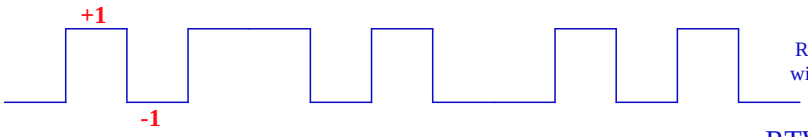
L.B. Kish, *Physics Letters A* **373** (2009) 911-918

L.B. Kish, S. Khari, S. Sethuraman, *Physics Letters A* **373** (2009) 1928-1934

Multidimensional

2^{N-1} dimensions with N noises

with superpositions, *N* noise-bit represents 2^N classical bits in a single wire



Random Telegraph Wave (RTW) taking +1 or -1 with 50% probability at the beginning of each clock period.

$RTW^2 = 1$; $RTW_1 * RTW_2 = RTW_3$ all orthogonal

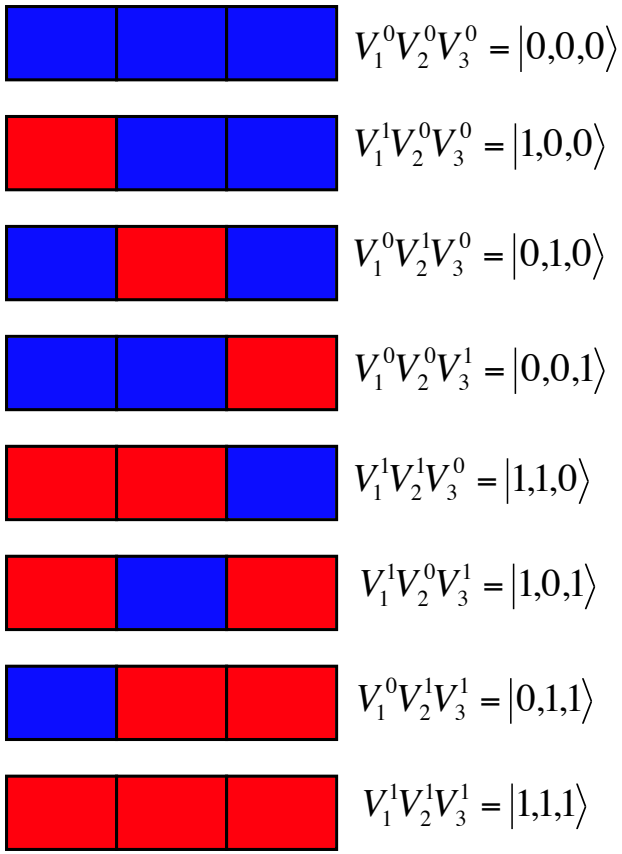
$(RTW_0 * RTW_1) * RTW_1 = RTW_0$

$(RTW_0 * RTW_1) * RTW_0 = RTW_1$

Instantaneous logic; parallel operations in hyperspace

The first bit in 2^N binary numbers is inverted by an $O(N^0)$ hardware complexity class operation !

Single wire



$V_1^0 V_2^0 V_3^0 = |0,0,0\rangle$

$V_1^1 V_2^0 V_3^0 = |1,0,0\rangle$

$V_1^0 V_2^1 V_3^0 = |0,1,0\rangle$

$V_1^0 V_2^0 V_3^1 = |0,0,1\rangle$

$V_1^1 V_2^1 V_3^0 = |1,1,0\rangle$

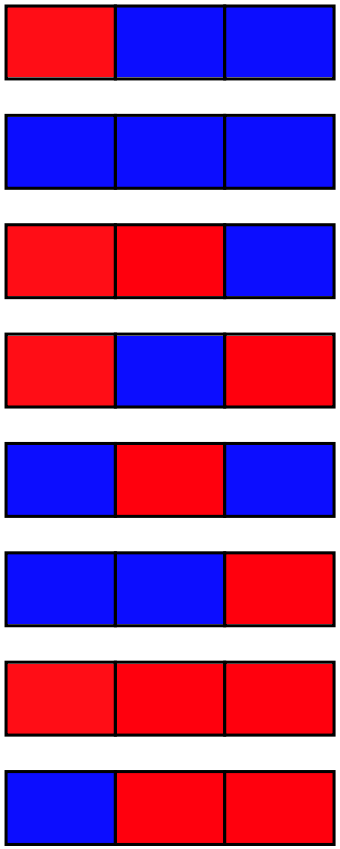
$V_1^1 V_2^0 V_3^1 = |1,0,1\rangle$

$V_1^0 V_2^1 V_3^1 = |0,1,1\rangle$

$V_1^1 V_2^1 V_3^1 = |1,1,1\rangle$

$$* \left(V_1^0 * V_1^1 \right) =$$

Single wire



$V_1^1 V_2^0 V_3^0 = |1,0,0\rangle$

$V_1^0 V_2^0 V_3^0 = |0,0,0\rangle$

$V_1^1 V_2^1 V_3^0 = |1,1,0\rangle$

$V_1^1 V_2^0 V_3^1 = |1,0,1\rangle$

$V_1^0 V_2^1 V_3^0 = |0,1,0\rangle$

$V_1^0 V_2^0 V_3^1 = |0,0,1\rangle$

$V_1^1 V_2^1 V_3^1 = |1,1,1\rangle$

$V_1^0 V_2^1 V_3^1 = |0,1,1\rangle$

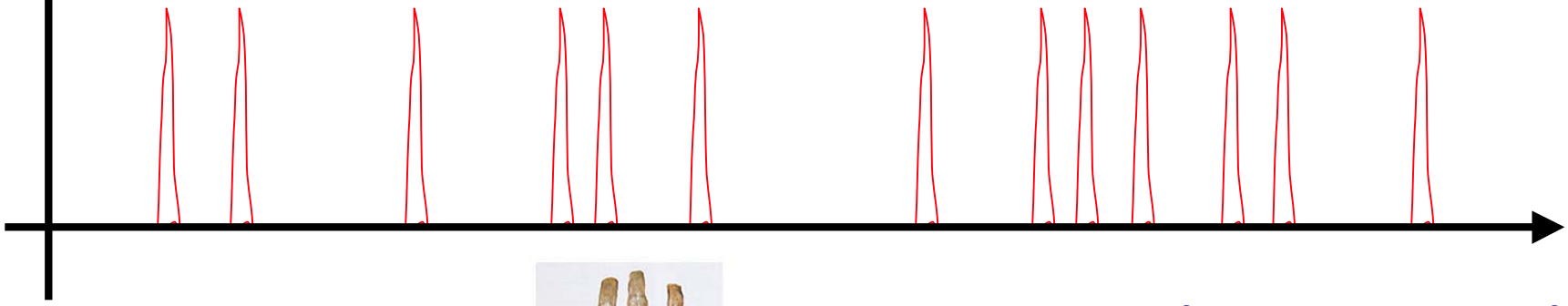
Note: orthogonality is only half of the picture; stochasticity is also essential for special purpose operations with large parallelism and small complexity!

For example, in the application in the former page, a sinusoidal representation would require and exponential time complexity to represent all the possible states, while the stochastic version requires that only of we want to measure the superposition.

Similar situation to quantum computing: those special-purpose operations fly, which require large calculation in a classical computer but yields a small answer (no superposition or small superposition), which is easy to analyze and output.

$$\Delta = 1/\sqrt{n}$$

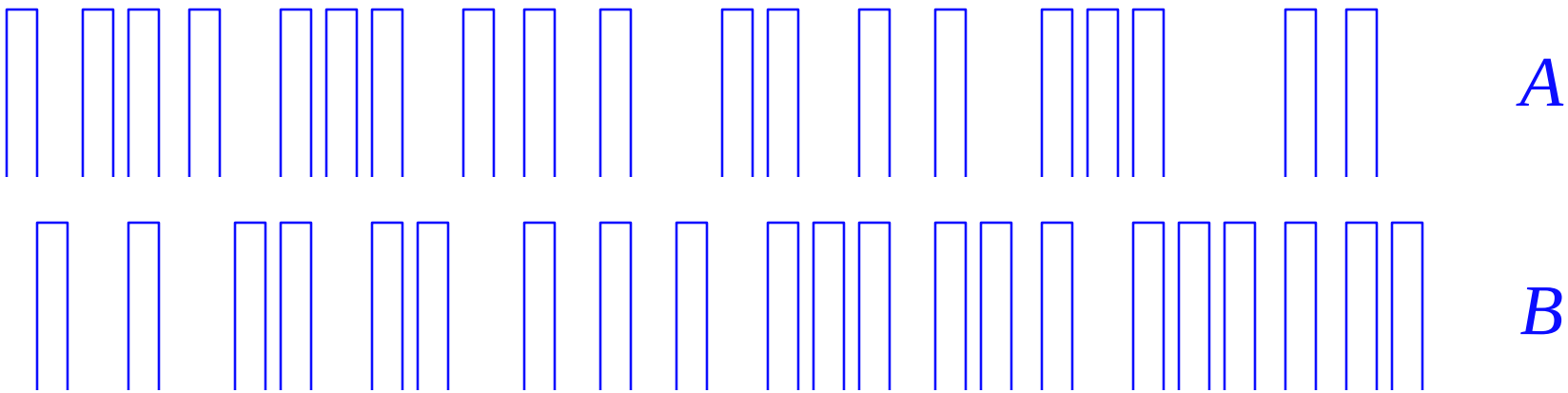
Often a Poisson-like spike sequence.
The relative frequency-error scales as the reciprocal of the square-root of the number of spikes.



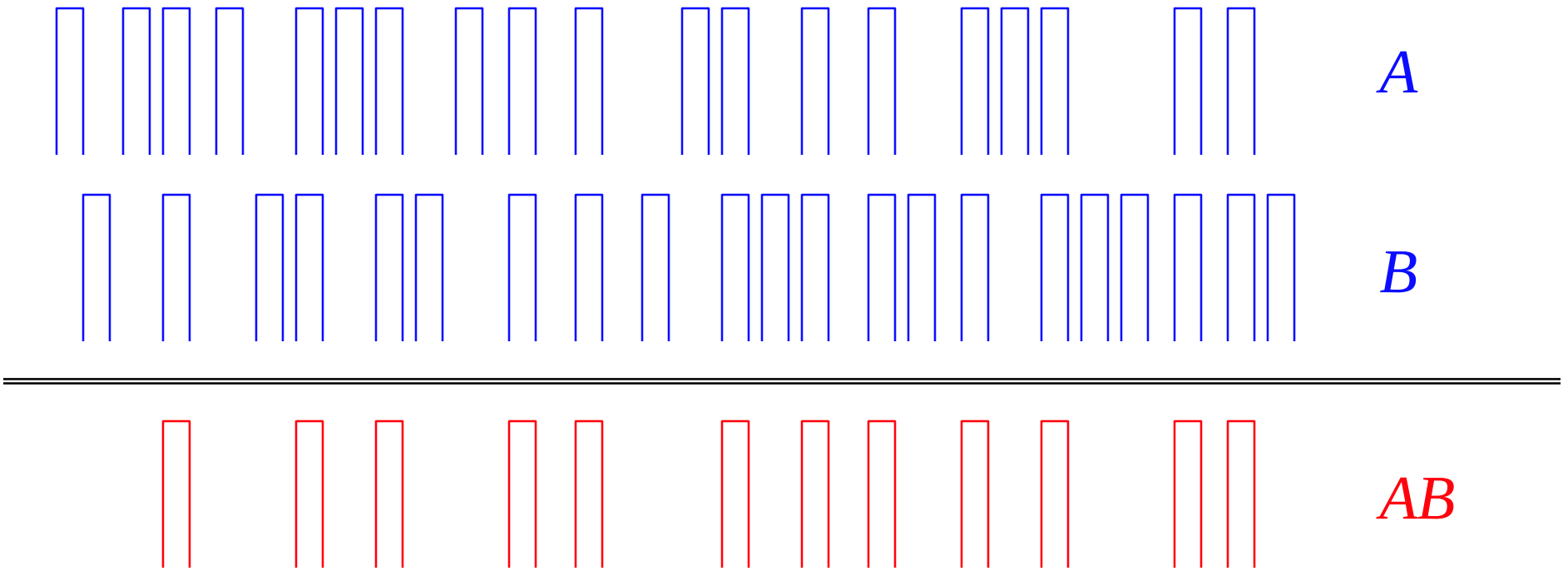
Supposing the maximal frequency, 100 Hz, of spike trains, 1% error needs to count 10^4 spikes, which is 100 seconds of averaging!

Pianist playing with 10 Hz hit rate would have 30% error in the rhythm at the point of brain control. Parallel channels needed, at least 100 of them.
(Note: controlling the actual muscles is also a problem of negative feedback but we need an accurate reference signal).

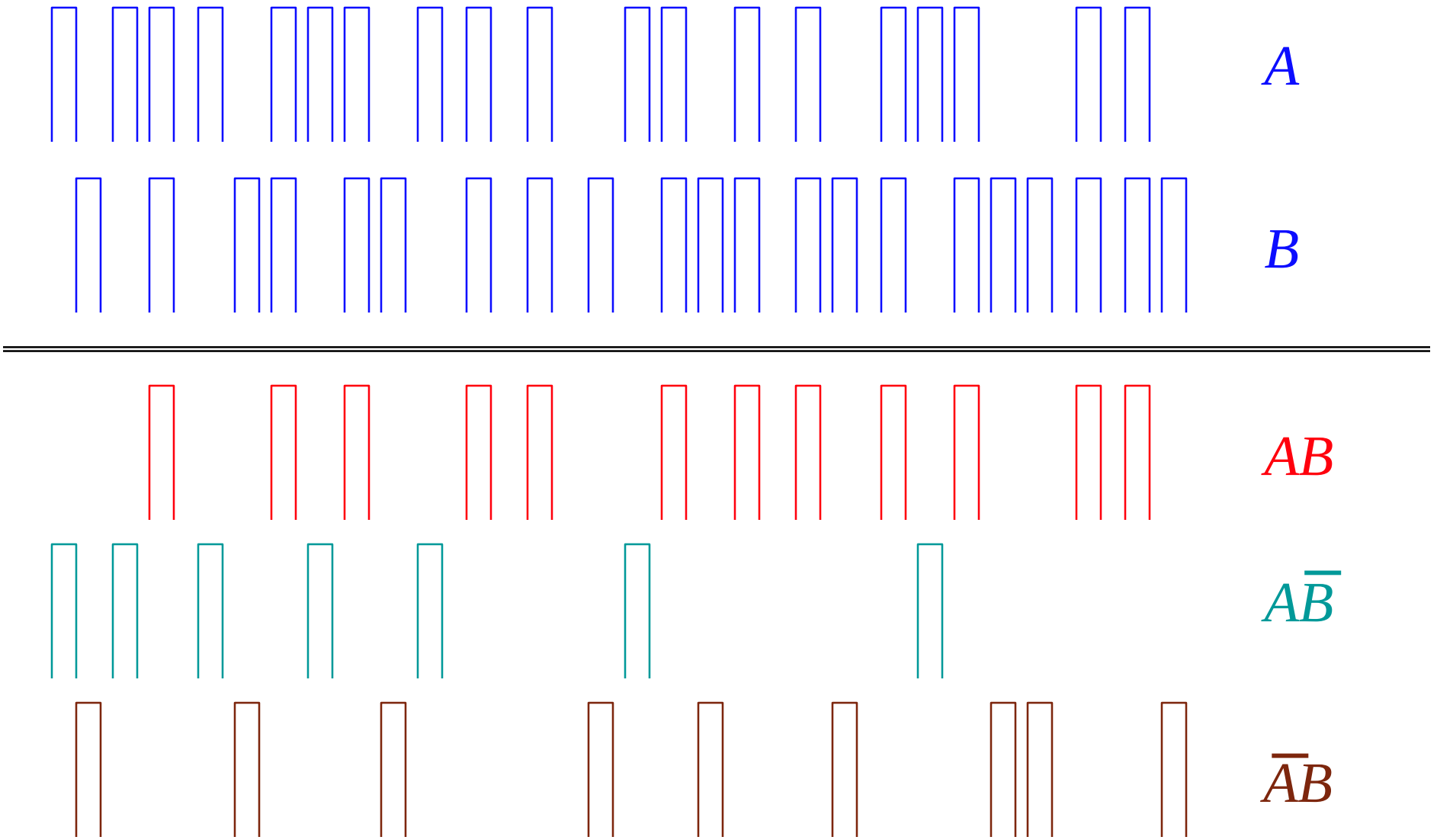
Let's do the naive math: similar number of neurons and transistors, but 30 million times slower clock; plus a factor of 10^4 slowing down due to averaging needed by the stochastics.
The brain should perform about 300 billion times slower than a computer!


A
B

S.M. Bezrukov, L.B. Kish, *Physics Letters A* **373** (2009) 2338-2342

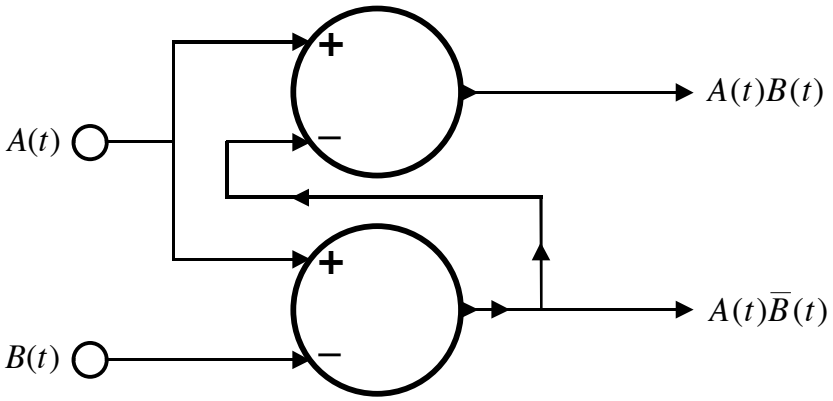


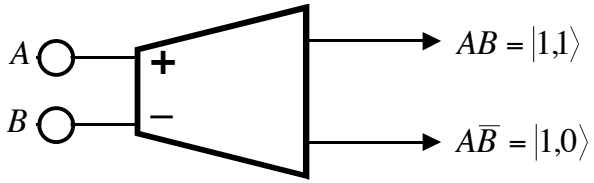
Brain logic scheme and its signals. S.M. Bezrukov, L.B. Kish, *Physics Letters A* **373** (2009) 2338-2342

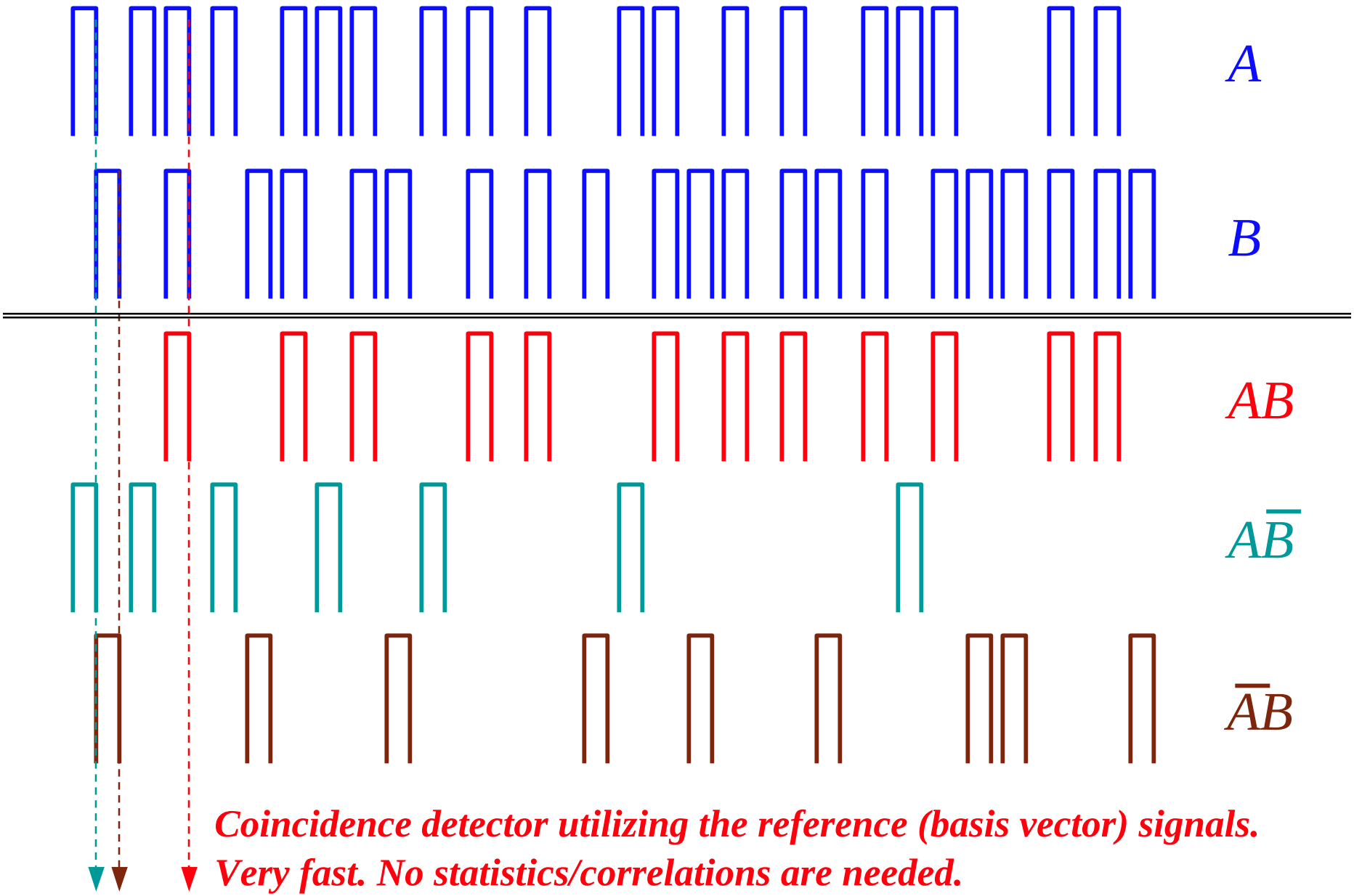


Neural circuitry. The orthon building element and its symbol.

(Bezrukov, Kish, *Physics Letters A* **373** (2009) 2338-2342)







Coincidence detector utilizing the reference (basis vector) signals.

Very fast. No statistics/correlations are needed.

S.M. Bezrukov, L.B. Kish, *Physics Letters A* **373** (2009) 2338-2342

A similar characteristics has recently been observed indicating the importance of timing of single spikes.

Update TRENDS in Neurosciences Vol.28 No.1 January 2005

Research Focus

Spike times make sense

Rufin VanRullen, Rudy Guyonneau and Simon J. Thorpe

Centre de Recherche Cerveau et Cognition, 133 Route de Narbonne, 31062 Toulouse Cedex, France

Many behavioral responses are completed too quickly for the underlying sensory processes to rely on estimation of neural firing rates over extended time windows. Theoretically, first-spike times could underlie such rapid responses, but direct evidence has been lacking. Such evidence has now been uncovered in the human somatosensory system. We discuss these findings and their potential generalization to other sensory modalities, and we consider some future challenges for the neuroscientific community.

systematically influenced first
afferent types. First-spike tim
directional tuning curve, simil
with firing rates. However, f
(FA-I and SA-I), the directio
first-spike latency did not co
with firing rates (derived
interval). Spike time and r
thus be used independently to
of a stimulus variable.

LETTER Communicated by Laurence Abbott

Neurons Tune to the Earliest Spikes Through STDP

Rudy Guyonneau
rudy.guyonneau@cerco.ups-tlse.fr
Centre de Recherche "Cerveau et Cognition," Toulouse 31000, France, and Spikenet Technology, Revel, France

Rufin VanRullen
Rufin.vanrullen@cerco.ups-tlse.fr
Centre de Recherche "Cerveau et Cognition," Toulouse 31000, France

Simon J. Thorpe
Simon.Thorpe@cerco.ups-tlse.fr
Centre de Recherche "Cerveau et Cognition, Toulouse 31000, France, and Spikenet Technology, Revel 31250, France

Neural Computation **17, 859–879** (2005)

Conclusion:

•Fluctuation-enhanced sensing work but it is a rather empirical approach when the sensors are not well defined regarding stochastics such as commercial sensors.

•The noise-based secure communication is feasible and provides higher security with stronger robustness and much lower price than quantum communicators do.

•Noise-based logic and computing shows some interesting features but there are still a lot of open questions to answer before we can see it it can beat quantum computing. (Of course yet to see if quantum computers will ever be built or if they are feasible).

•In any case, noise-based logic offers a deterministic multivalued logic system for the brain.

END OF TALK