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

Noise-based informatics

Laszlo B. Kish

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

Noise-based informatics is a field where the information (sensing, communication, or computation) is carried by the statistical properties of noises (stochastic processes with zero mean), and/or the coincidences of their instantaneous amplitudes with those of reference processes.

Fluctuation-Enhanced Sensing utilizes the statistical processes of the noise in the signal of sensors to serve with extra information about the dynamics of the interaction between the sensor and its environment.

The research on unconditional security began with stealth communication (zero-power communications) where the transmitter does not emit energy into the information channel but modulates the inherent noises there. Such system is not necessarily secure. On the other hand, the Kirchhoff-law-Johnson-noise (KLJN) key exchange is unconditionally secure and can run in stealth mode, too. It is the classical physical alternative of quantum key distribution.

Noise-based logic (NBL) utilizes a reference system of orthogonal noises to generate the logic signals. Several different NBL types exist. The quantum-mimic system uses the product of the reference noises to generate strings and it utilizes the superposition of these strings to achieve an exponentially large logic space with polynomial hardware and time complexity: the same features that quantum computers are promising to exploit.

The seminar gives a brief outline of the field. More details and papers can be found here:

https://noise.ece.tamu.edu/research_files/research_FES.htm
https://noise.ece.tamu.edu/research_files/research_secure.htm
https://noise.ece.tamu.edu/research_files/noise_based_logic.htm

Texas A&M University, its central campus is in College Station

Texas A&M University: The George Bush Library and Museum; The Bush School

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

Notable faculty:

Jack Kilby, inventor of the chip (Nobel Prize winner)

J.R. (Bob) Biard, inventor of LED, ROM, etc. (National Academy member)

Kandó Technical College, 1981...

Self-introduction (until 1998: L.B. Kiss), main research topics:

Measurements, simulations, concepts, models, theories, unsolved problems and applications of stochastic and/or dynamic phenomena.

- 1/f noise (1982-1989), Szeged-Hungary; Eindhoven-Holland (1986); Cologne-Germany (1989).
- Oxidation dynamics of CO2 laser-irradiated metals (1985-86), Szeged-Hungary.
- Theory of UV laser ablation (1986-88), Szeged-Hungary
- Self-organized criticality (1989-90), Cologne-Germany, Szeged-Hungary.
- Stochastic resonance (1990-2004), Szeged, Uppsala, Texas
- Noise in high-temperature superconductors (1988-1995), Uppsala-Sweden.
- Biased percolation and progressive degradation of devices (1995-1998), Szeged, Uppsala.
- Fabrication, experiments and theories of nanostructures; lognormality; etc, (1997-2001) Uppsala-Sweden.
- **Fluctuation-enhanced sensing** (1998 – present), Uppsala-Sweden, Texas.
- Energy dissipation of classical and quantum computing, critical approach (2003 – present), Texas.
- **Unconditional security with the noise-based KLJN key exchange protocol** (2005 – present), Texas.
- **Noise-based logic and computing** (2009 – present), Texas
- Thermal noise in the quantum limit - unsolved problem (1988, 2015-16), Szeged-Hungary, Texas.
- Criticisms, e.g. dissipation, memristor theory, information entropy, noise models: *always/everywhere*

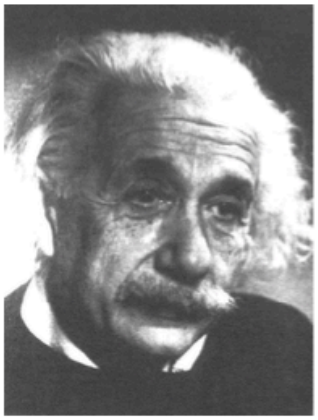
Noise

Deterministic laws of physics break down at small sizes.

Robert Brown
(1773 - 1858)

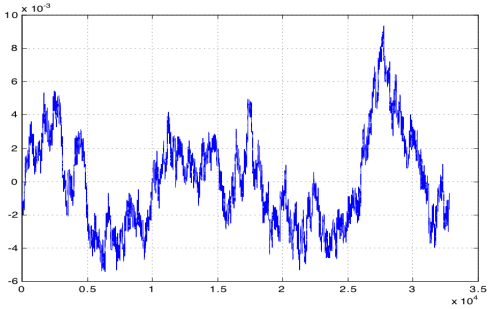
Ludwig Boltzmann
(1844-1906)

James Clerk Maxwell
(1831-1879)



Albert Einstein
(1879-1955)

Noise: stochastic signal



Noise-based informatics:

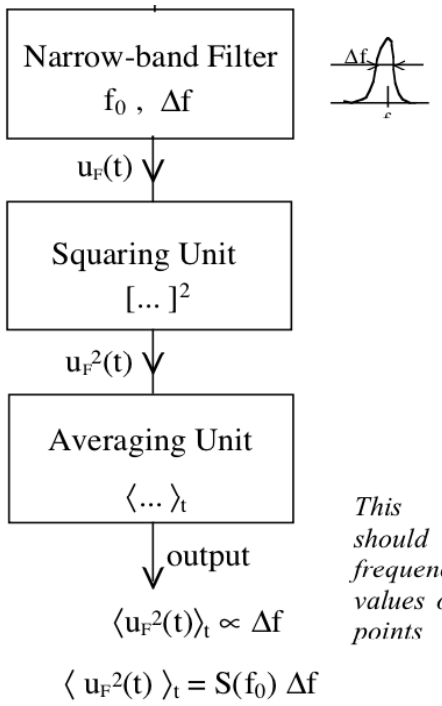
1. **Sensory information (Fluctuation-Enhanced Sensing)**
2. **Communications (stealth and secure)**
3. **Logic and computing**

Noise: stochastic signal

Noise-based informatics:

1. **Sensory information (Fluctuation-Enhanced Sensing)**
2. **Communications (stealth and secure)**
3. **Logic and computing**

Noise: stochastic signal



This measurement process should be repeated for each frequency of interest to get the values of the spectrum at those points

$$S(f_0) = \lim_{\Delta f \to 0} \frac{\langle u_F^2(t) \rangle}{\Delta f}$$

$$u_{\text{eff}}^2(f_{\text{low}}, f_{\text{high}}) = \int_{f_{\text{low}}}^{f_{\text{high}}} S(f)\,df$$

Our patents about Fluctuation-Enhanced Sensing (FES)

G. Schmera, L.B. Kish, "Bacteria Identification by Phage Induced Impedance Fluctuation Analysis, BIPIF", US Patent US9645101B2 (granted May 9, 2017). https://patents.google.com/patent/US9645101B2

L.B. Kish, M. Cheng, R. Young, M. King, S. Bezrukov, "Sensing Phage-Triggered Ion Cascade (SEPTIC)", November 24, 2004. US Patent # US7229754B2. https://patents.google.com/patent/US7229754

J. Smulko, L.B. Kish, G. Schmera, "System and Method for Gas Recognition by Analysis of Bispectrum Function", US Patent # US7680607B1 , https://patents.google.com/patent/US7680607B1/en?oq=US7680607B1

G. Schmera, L.B. Kish, ""System and Method of Molecule Counting Using Fluctuation Enhanced Sensors", US Patent # US7524460B1 (April 28, 2009). https://patents.google.com/patent/US7524460B1

G. Schmera and L.B. Kish, " System and method of fluctuation enhanced gas-sensing using saw devices ", US Patent, US Patent US7286942B1 (May 2003). https://patents.google.com/patent/US7286942B1

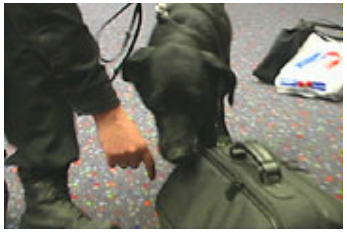
L.B. Kish, C.G. Granqvist and R. Vajtai (1999), "Sampling-and-Hold Chemical Sensing by Noise Measurements for Electronic Nose Applications", Swedish patent #SE 9904209-5 (now, public) http://was.prv.se/spd/pdf/RdizounvzhfWS3oljenFlQ/SE515249.C2.pdf

L.B. Kiss, C.G. Granqvist, J. Söderlund (1998), "Particle size determination", Swedish patent, # SE 9803320–2; Publ. No.: SE 513194 (now, public).
http://was.prv.se/spd/pdf/FngdBYlMdpXWS3oljenFlQ/SE513194.C2.pdf

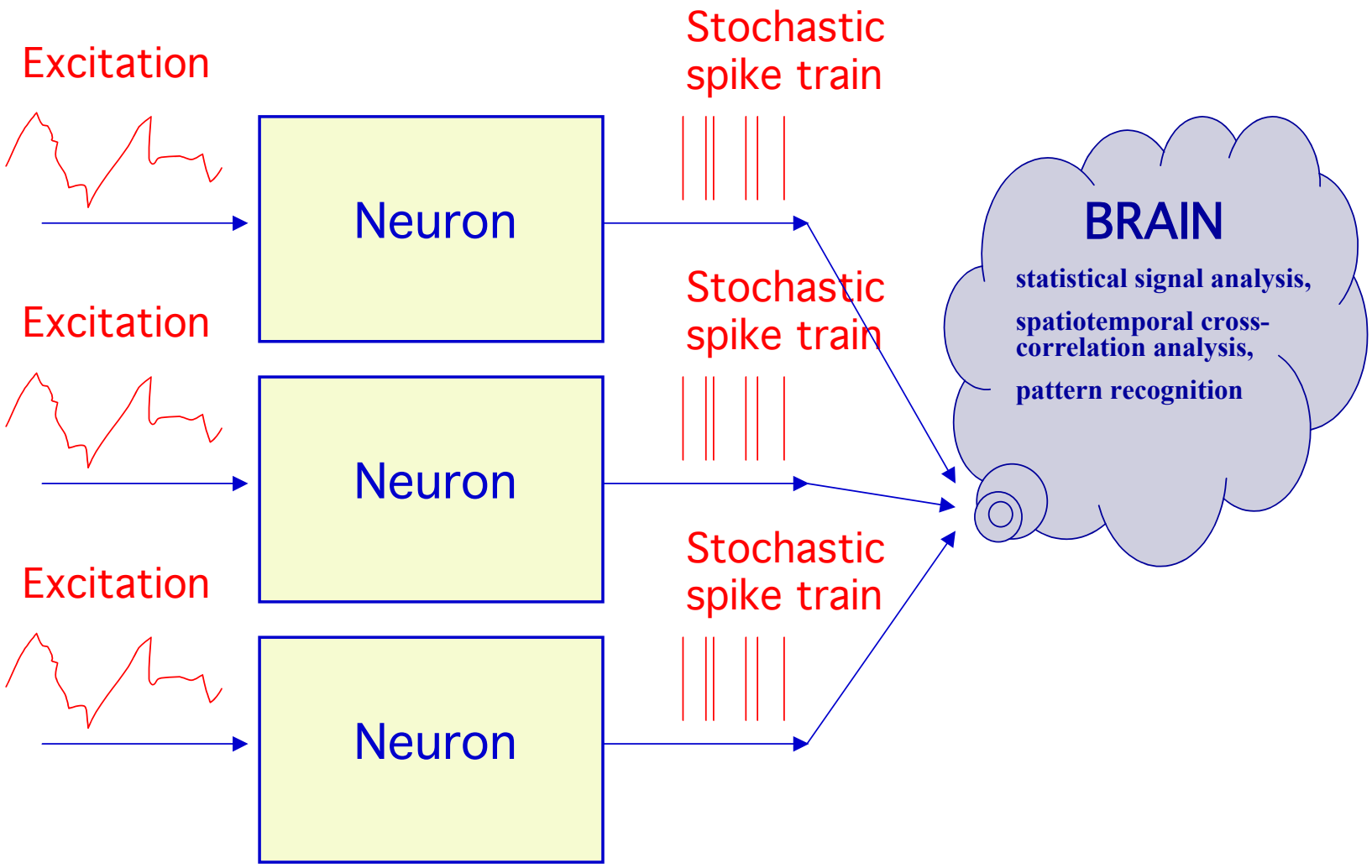
L.B. Kiss, C.G. Granqvist, J. Söderlund, "Detection of chemicals based on resistance fluctuation-spectroscopy", Swedish patent, # SE 9803019-0; Publ. No.: 513148 (now, public) http://was.prv.se/spd/pdf/8V-xToJGAh7WS3oljenFlQ/SE513148.C2.pdf

The best chemical and bio sensor have been developed by nature.

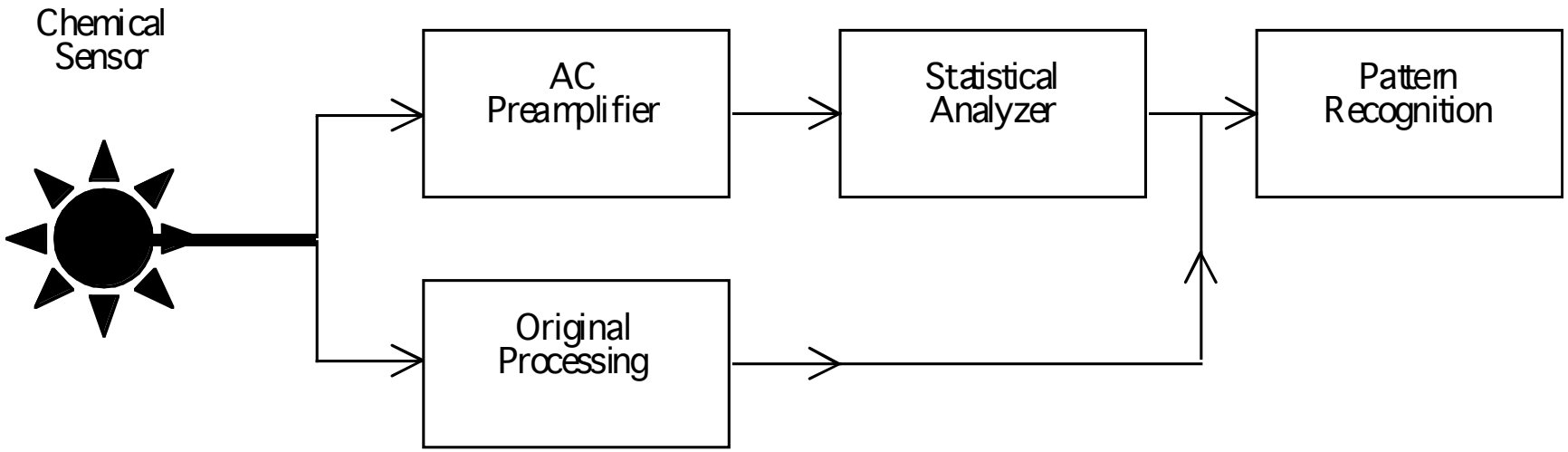
For example, *animal noses,* which produce *stochastic signals* (neural spikes) for the animal brain.



Fluctuation-Enhanced Sensing is strongly bio-mimic !

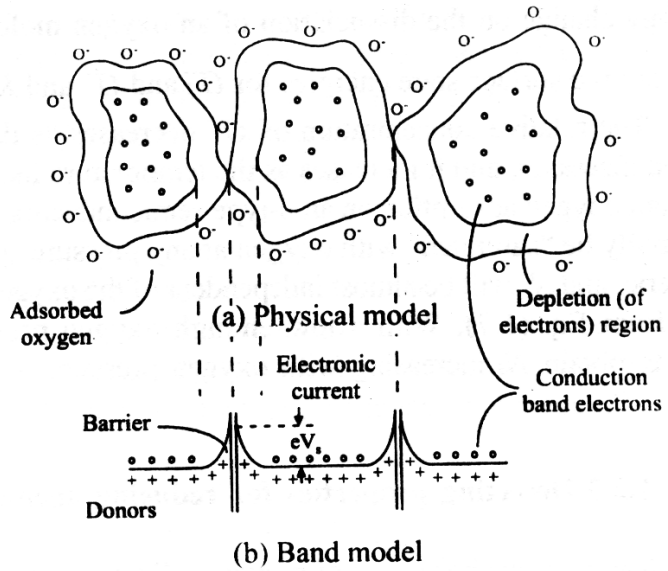


Fluctuation-enhanced chemical sensing.



Example: Taguchi gas sensors.

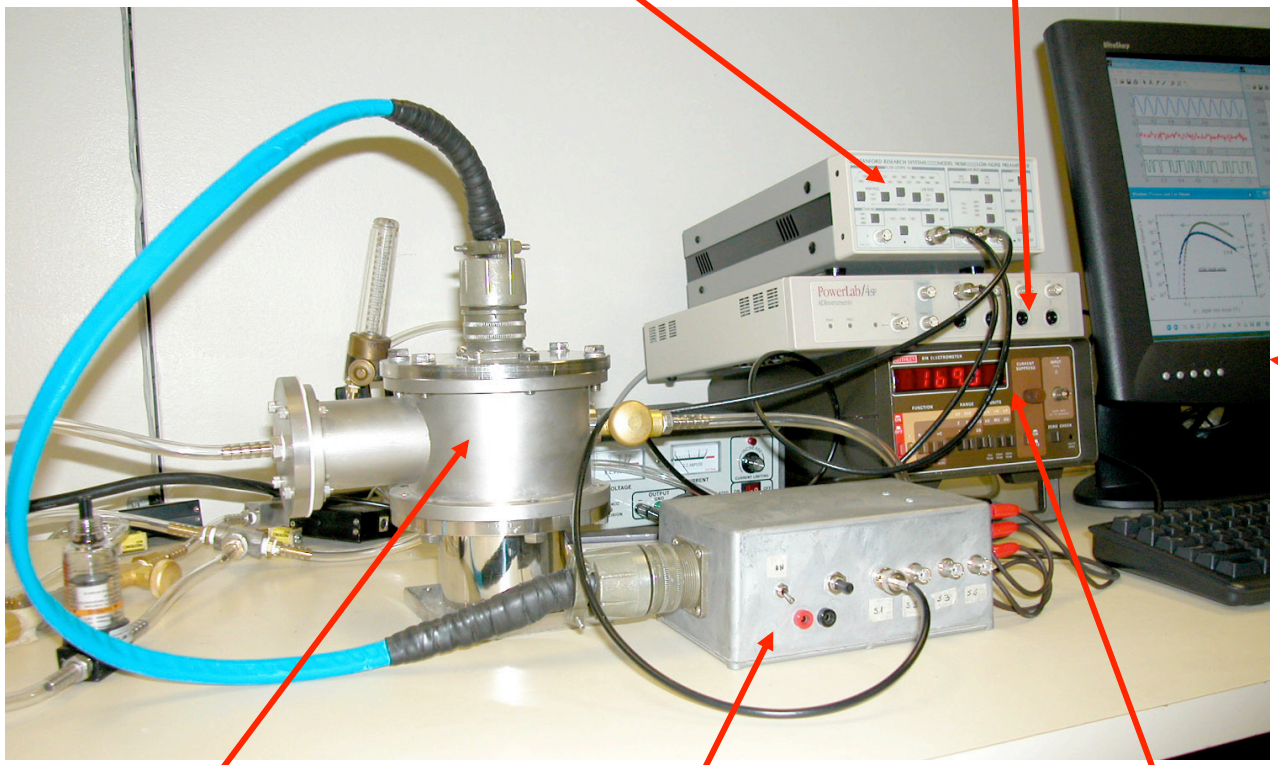
Taguchi sensors are heated semiconductor-oxide films where the resistance of the inter-grain junctions is modulated by the adsorbed agent which act as doping.

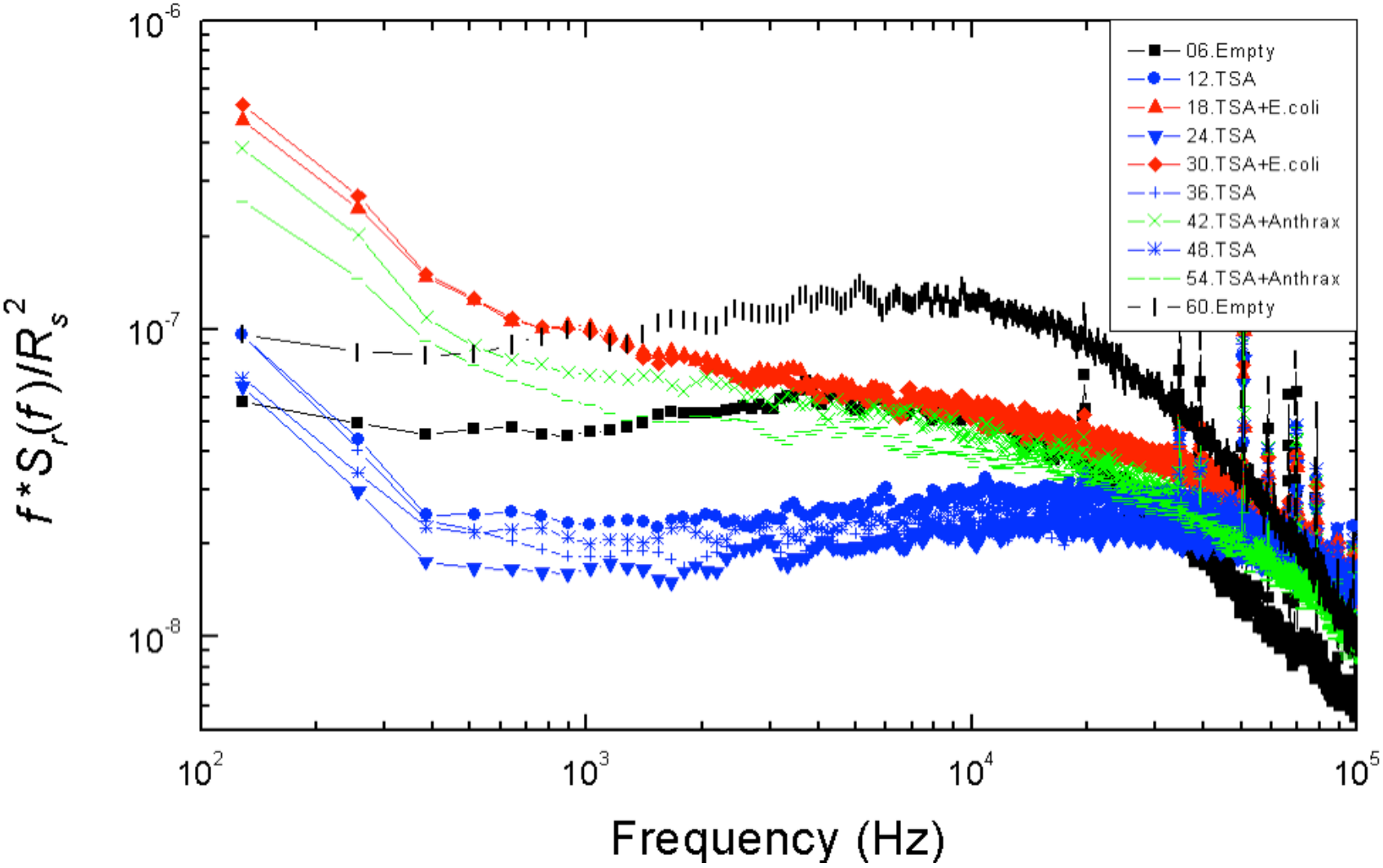


Stochastic microscopic fluctuations are generated in the junction resistance due to the diffusion of agents along the grain boundaries.

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

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

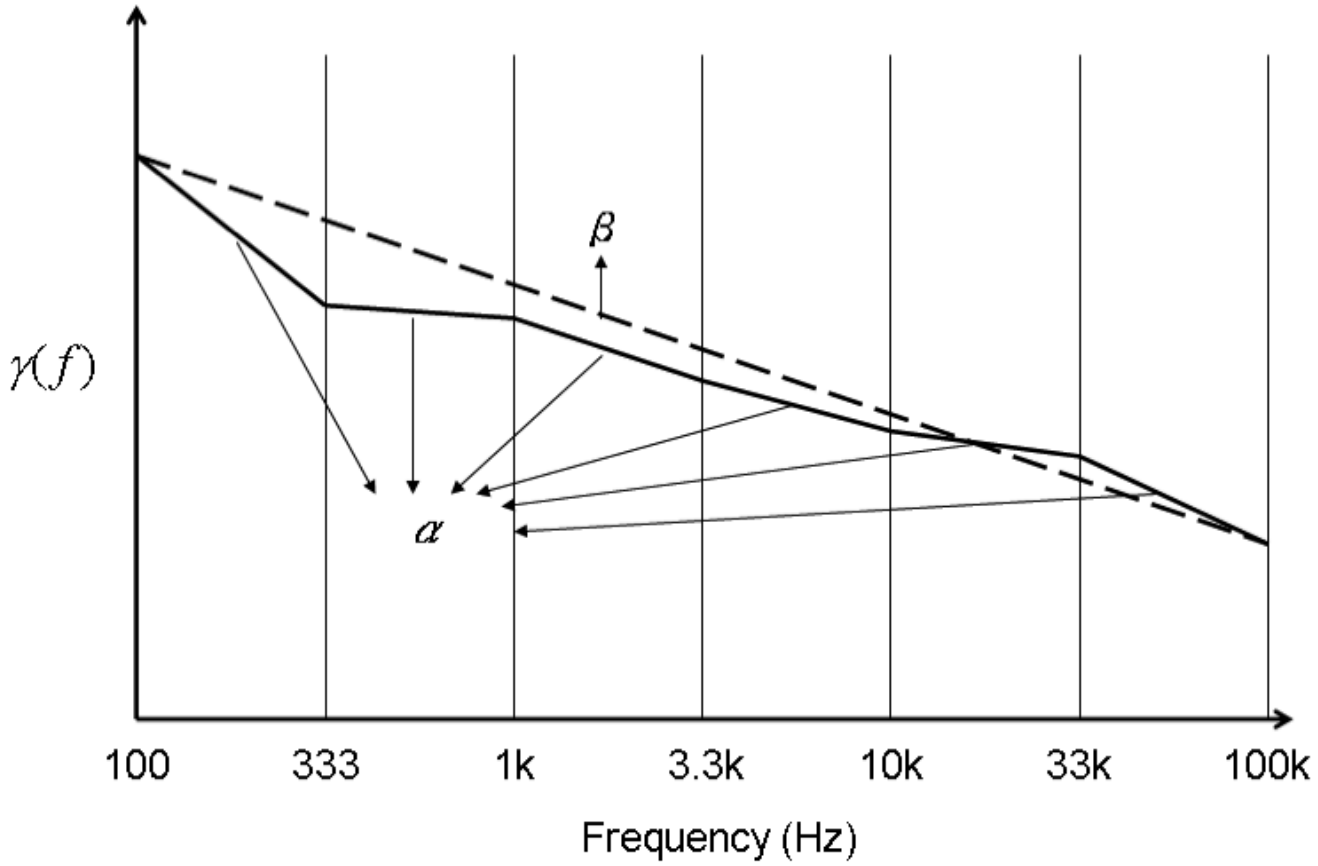




Normalized power spectra of the Taguchi sensor SP11 in sampling-and-hold-mode. The alias "Anthrax" stands for anthrax surrogate *Bacillus subtilis*.

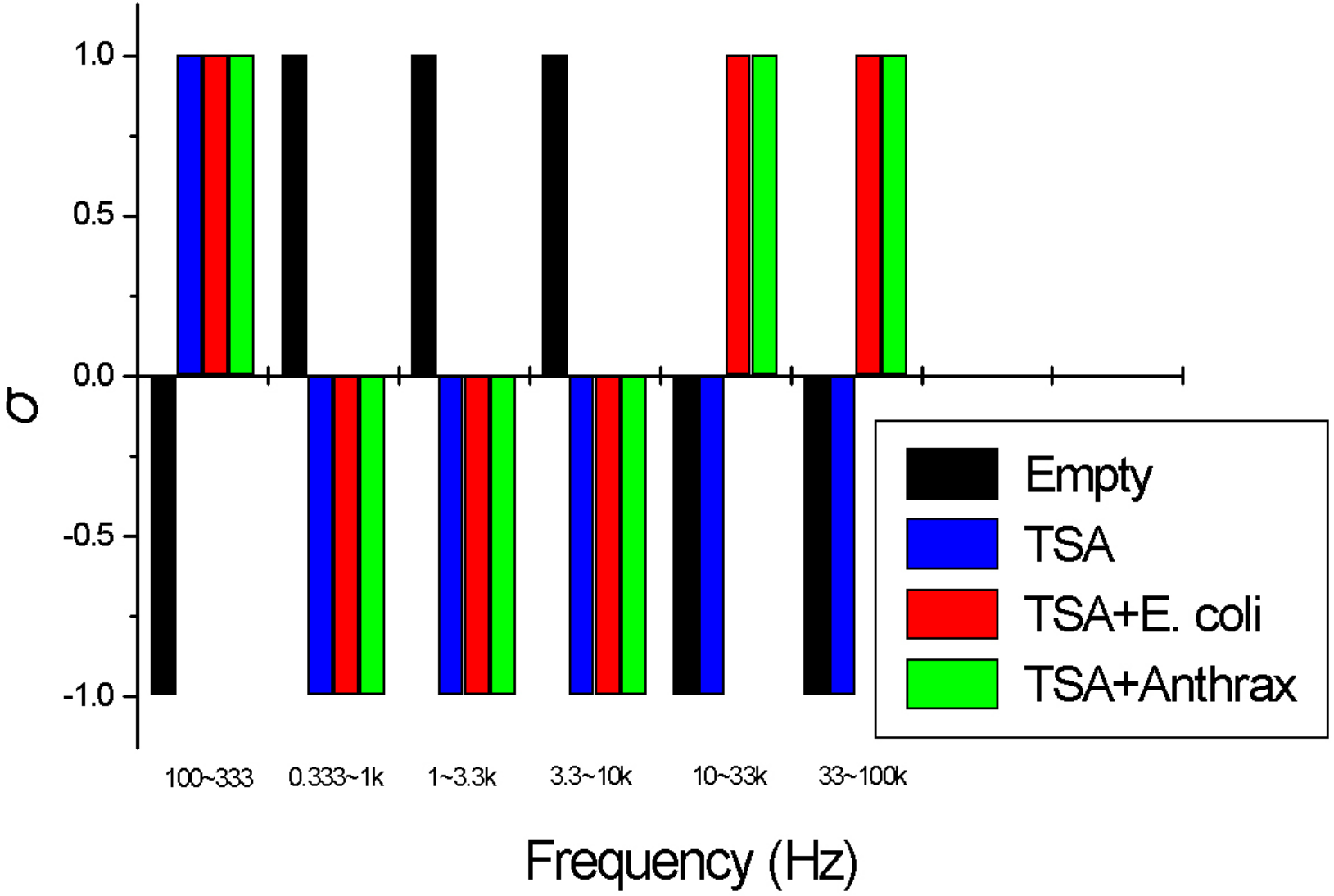
H.C. Chang, L.B. Kish, M.D. King, C. Kwan, "Binary Fingerprints at Fluctuation-Enhanced Sensing", *Sensors* **10** (2010) 361-373; Open Access, http://www.mdpi.com/1424-8220/10/1/361

simple way of binary and analog pattern generation

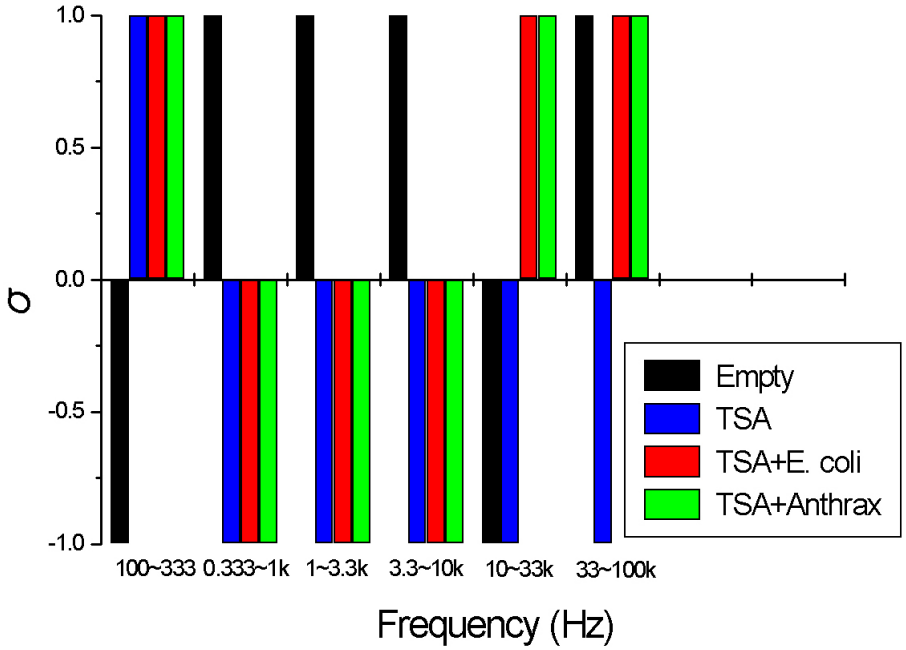


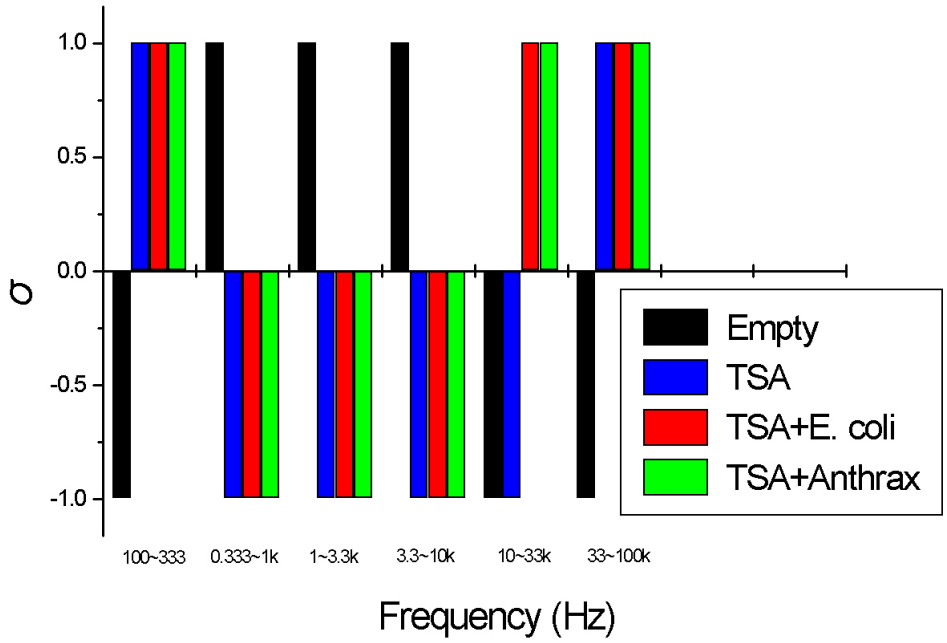
$$\gamma(f) = f\frac{S_r(f)}{R_s^2} \qquad \Delta = \alpha - \beta \qquad \sigma = \frac{\Delta}{|\Delta|} \qquad \Delta_n = \log\left|\frac{\Delta}{\beta}\right|$$

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



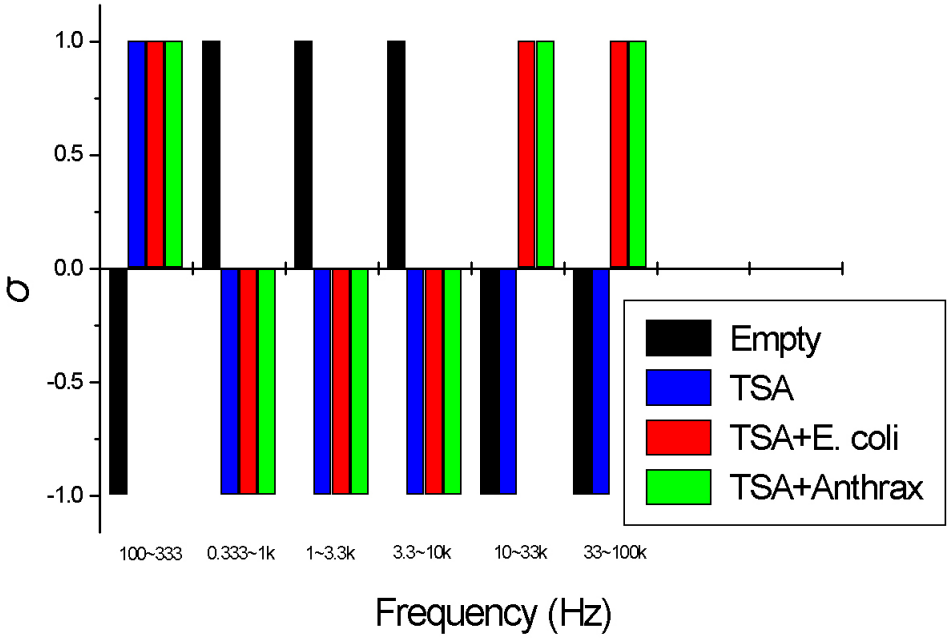
H.C. Chang, L.B. Kish, M.D. King, C. Kwan, "Binary Fingerprints at Fluctuation-Enhanced Sensing", *Sensors* **10** (2010) 361-373; Open Access, http://www.mdpi.com/1424-8220/10/1/361



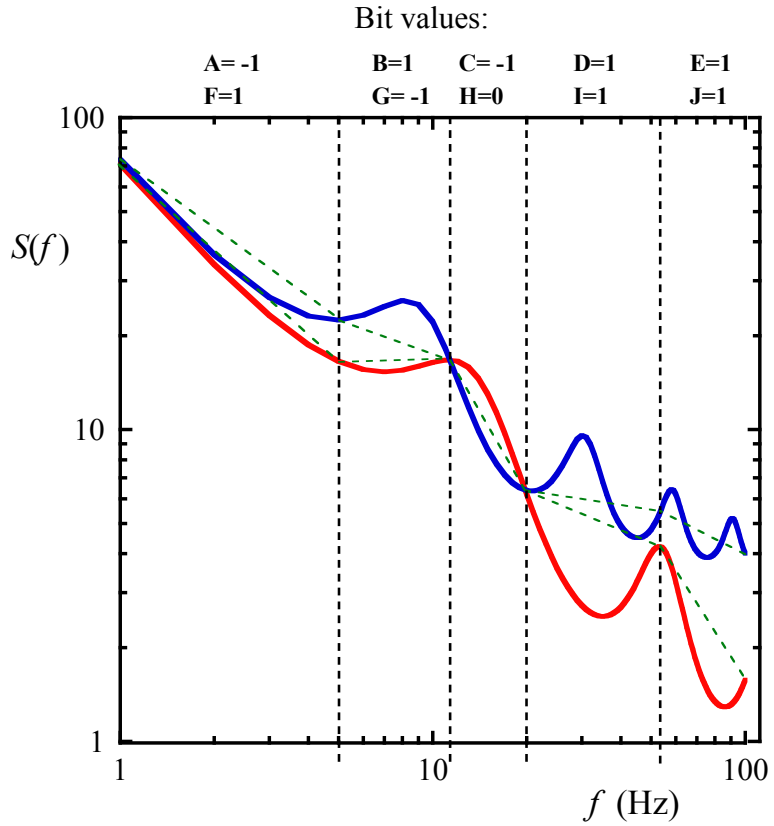


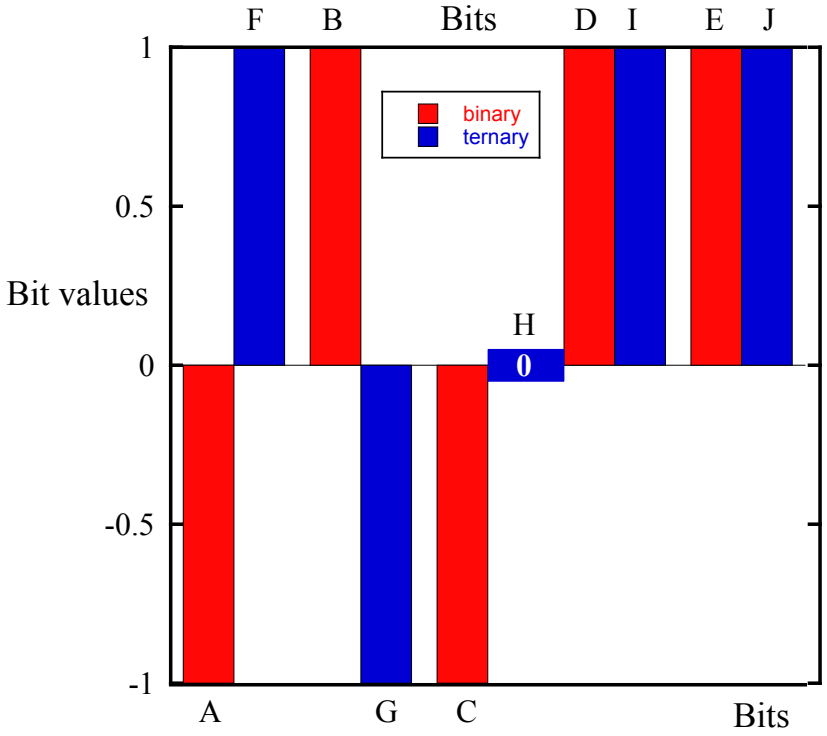
Reproducibility of the bacterial fingerprints (sampling-and-hold, SP11).

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



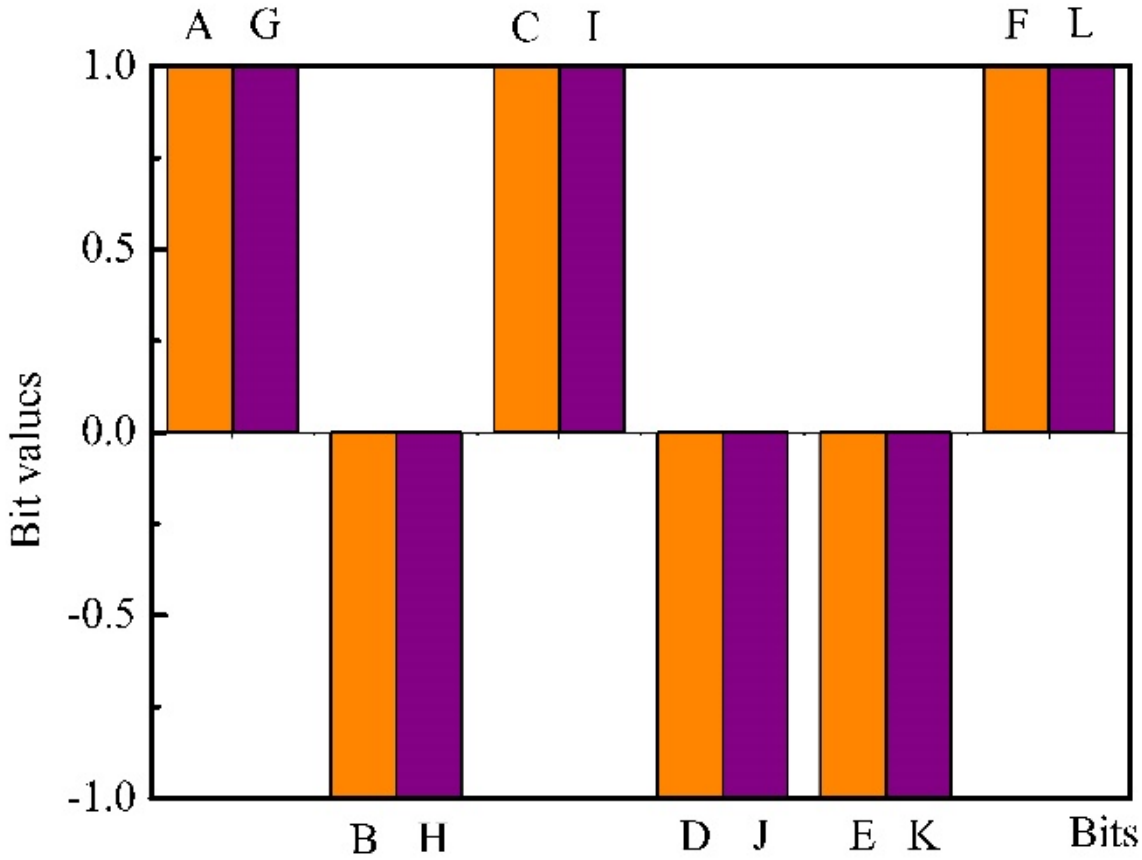
X. Yu, L.B. Kish, J.-L. Seguin, M.D. King:
Ternary Fingerprints with Reference Odor for Fluctuation-Enhanced Sensing
Biosensors 2020, 10, 93; doi:10.3390/bios10080093





Cow manure: It has different smell when the cow is sick

Cow manure: Ternary, reproducibility

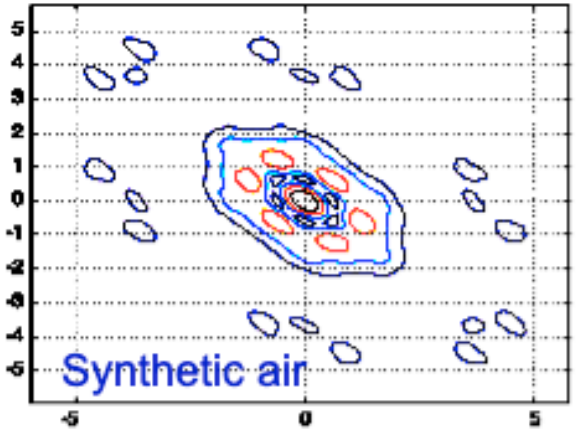


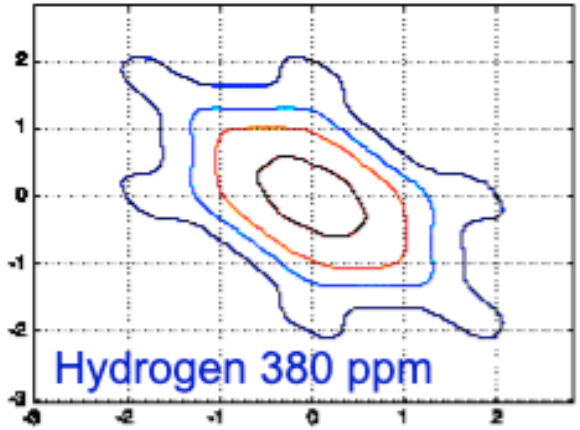
Orange: measurement-1; maroon: measurement-2 (of the same manure sample)

X. Yu, L.B. Kish, J.L. Seguin, M.D. King, "Ternary Fingerprints with Reference Odor for Fluctuation-Enhanced Sensing", *Biosensors* **10** (2020) 93; open access: https://doi.org/10.3390/bios10080093

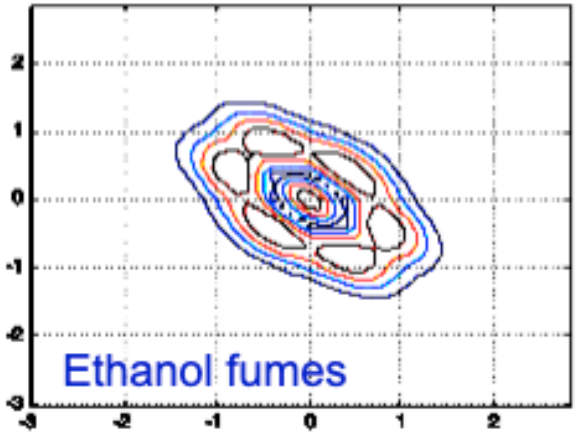
Bispectrum. COTS sensors. More sophisticated and powerful tool. This information which is hidden when using classical power density spectra. J.M. Smulko, L.B. Kish, "Higher-Order Statistics for Fluctuation-Enhanced Gas-Sensing", *Sensors and Materials* **16** (2004) 291-299

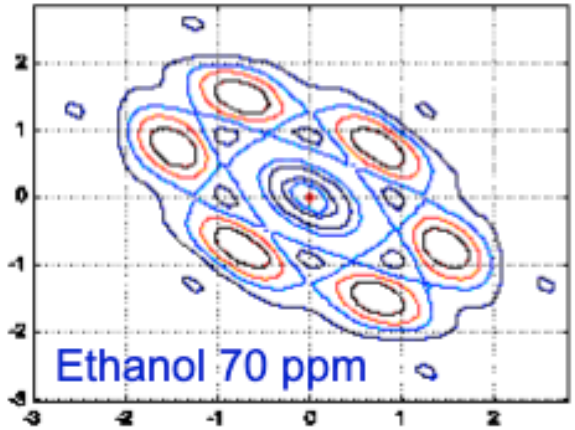
$$B(f_1, f_2) = \langle F(f_1)F(f_2)F(f_1 + f_2) \rangle$$





Note: all figures are generated by the same, single COTS sensor (NO_x sensor) !





SEnsing of Phage Triggered Ion Cascades: SEPTIC (feature in the Economist)

with Maria King and Ryland Young

Science and Technology: Screening for screams; Bacteriology

The Economist. London: Apr 16, 2005.Vol.375, Iss. 8422; pg. 81

The Economist

Section: *Science and Technology*
Publication title: The Economist. London: Apr 16, 2005. Vol. 375, Iss. 8422; pg. 81
Source type: Periodical
ISSN/ISBN: 00130613
ProQuest document ID: 822698581
Text Word Count 643

Full Text (643 words)

A rapid method of identifying dangerous bacteria

AT THE moment, identifying bacteria is a time-consuming business that involves taking a sample, adding nutrients, incubating the result and waiting until there is a large enough colony to test chemically. This can take hours. It would help patients (and, if it came to a terrorist attack involving bacteria, it would help the authorities, too) if this process could be speeded up. According to Laszlo Kish and Maria King, of Texas A&M University, it can be. Using a combination of virology and, surprisingly, microelectronics, they have devised a technique for identifying small quantities of bacteria in minutes.

The virological part of the test involves bacteriophages. Phages are viruses that attack bacteria with the same verve that some other viral species attack people. But phages are choosy about their prey. Most species can parasitise only a single sort of bacterium. In the past, bacteria-detection researchers have tried to exploit this specificity using conventional techniques: culturing samples, infecting them, and then testing for by-products of bacterial death. Though the results are often clearer than for ordinary assays, they still take a long time to arrive--too long for some patients.

That is where the second prong of Dr Kish's and Dr King's research kicks in. They realised that you do not have to wait until the bacteria die before you can tell whether they have been infected. Phages start their attack by injecting DNA into their victims. When this happens, there is a short-lived flow of ions (electrically charged atoms and molecules) out of the bacterium. This phenomenon, whimsically described as the bacterium "bleeding" or "screaming", is the first proof that the phage has found its target. Detect the scream and you know what type of bacterium you are dealing with.

The problem is "hearing" the scream. The signal created by the liberated ions would be hard enough to detect if all those ions were flowing in the same direction, and thus producing an electric current. But since they move off at random, even that minuscule current quickly vanishes.

The solution Dr Kish and Dr King have come up with is a device that can detect activity over a small enough distance for the current not to have vanished. It is called, with that delight in creating forced acronyms that plagues many branches of science, "sensing of phage-triggered ion cascade", or SEPTIC. It consists of a so-called nano-well into which the sample is decanted and which contains a capacitor with a gap of just 150 nanometres (billionths of a metre) between its plates.

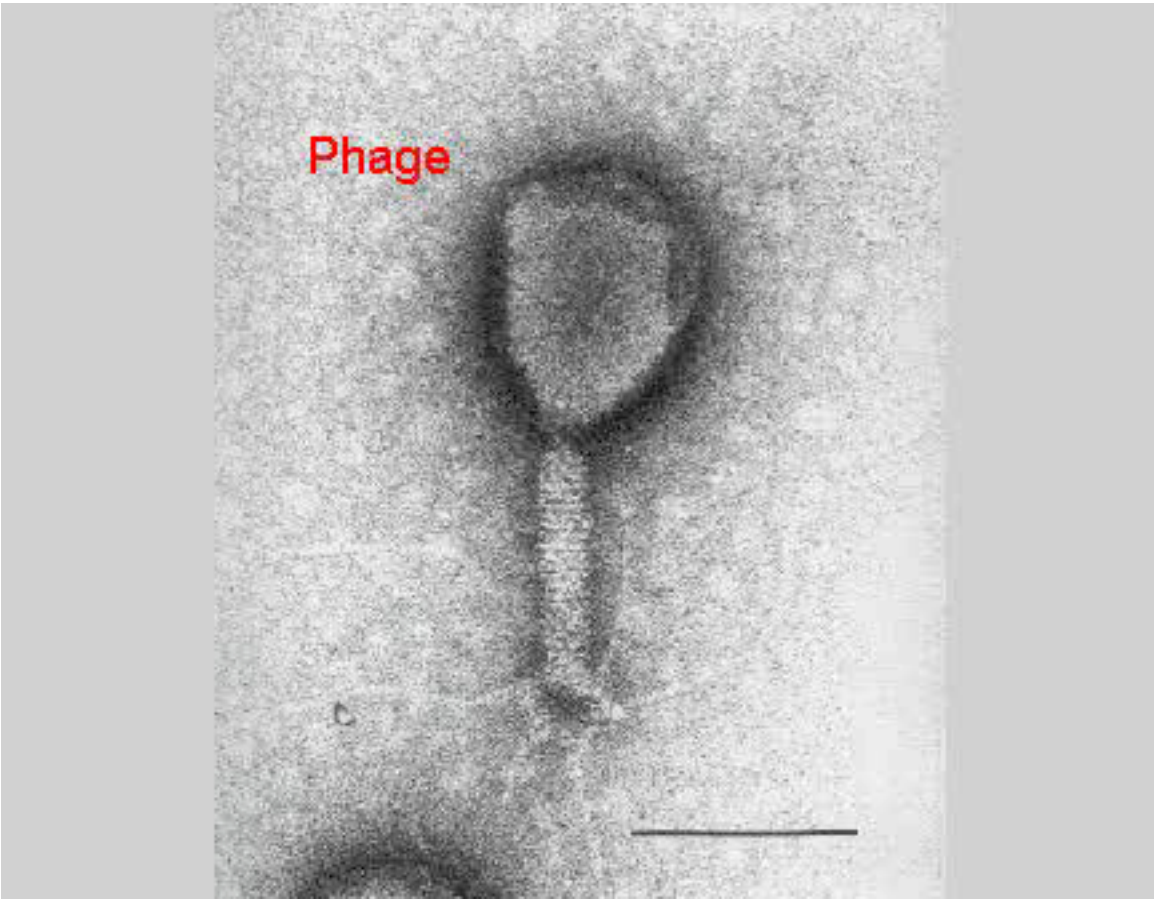
A capacitor is a routine electronic component, and capacitors of such minute dimensions are found by the zillion in computer chips. They consist of two electrodes known, by historical analogy with the structure of their ancient macroscopic ancestors, as plates. The plates are separated by an insulator, and if a positive charge is put on one plate and a negative charge on the other, the whole arrangement can act as a temporary electrical store.

If a drop of liquid containing the phage-infected sample is put between the plates, though, it will change the properties of the capacitor by changing the voltage between the plates. Any ions released into the liquid will change things further. And such changes can be detected in the electrical circuitry attached to the capacitor.

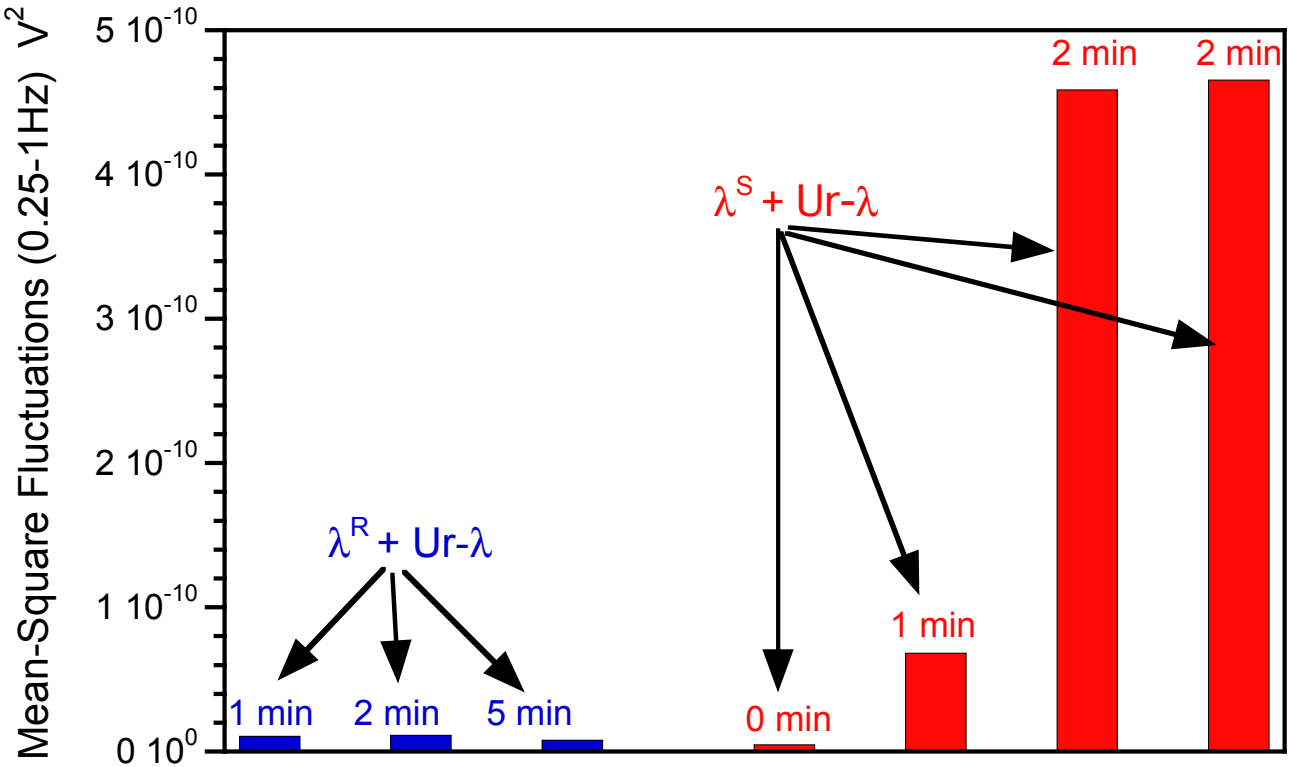
Initial tests of SEPTIC on that workhorse of all bacteriologists, E. coli, show that it works, and the team seems confident that similar results will be found with anthrax, plague, botulism and shigella. So next time an envelope containing white powder turns up in the post room, you will not have to wait long to find out whether it is dangerous. Better still, doctors will be sure from almost the outset that they are giving the correct antibiotic to infected patients. That should greatly improve the medicine's usefulness.

Animation movie about SEnsing of Phage Triggered Ion Cascades: SEPTIC

The specificity is given by the phages, the sensitivity by the "nanowell"



EXAMPLE: positive and negative experimental results versus incubation time with "ecoli" bacterium and its "lambda" phages



Noise-based informatics:

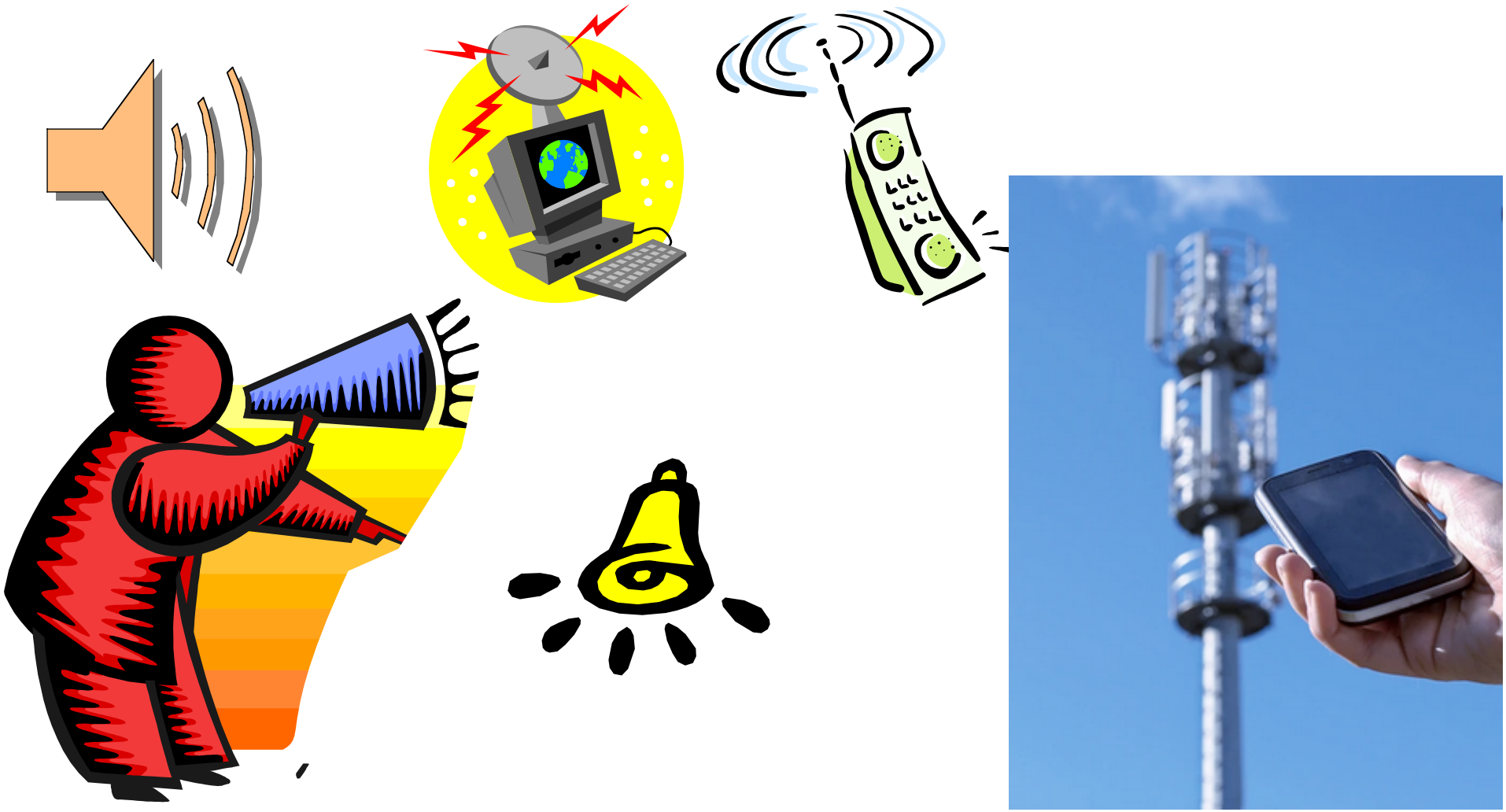
1. **Sensory information (Fluctuation-Enhanced Sensing)**
2. **Communications (stealth and secure)**
3. **Logic and computing**

Noise: stochastic signal

Introduction:

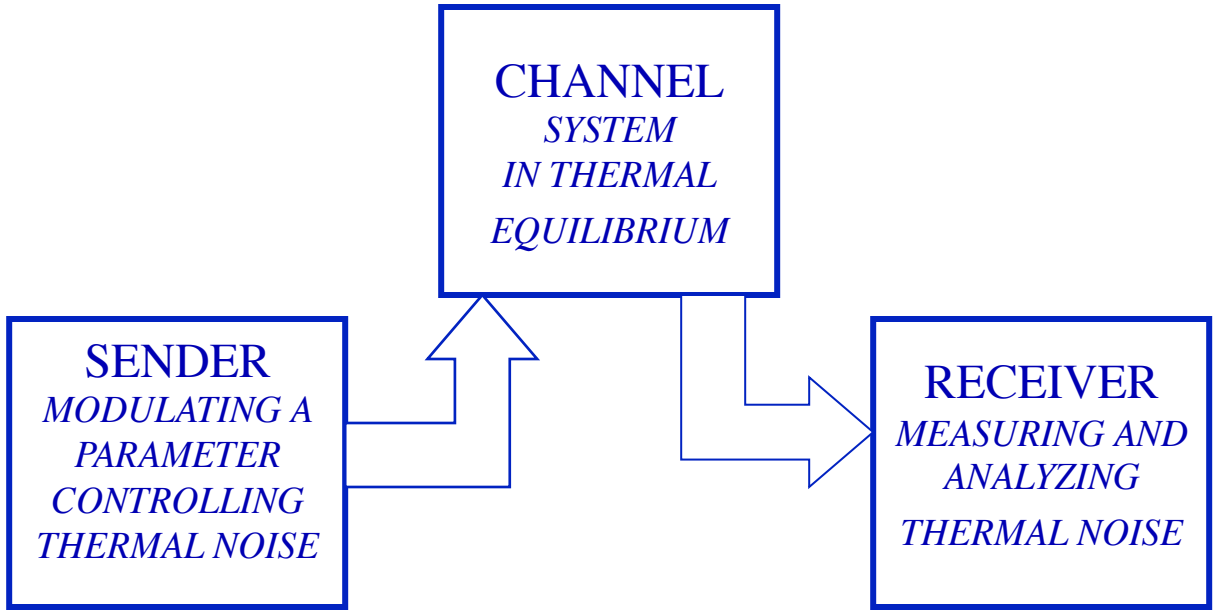
"Stealth communication: Zero-power classical communication, zero-quantum quantum communication and environmental-noise communication", *Applied Physics Lett.* **87** (December 2005), Art. No. 234109

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



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

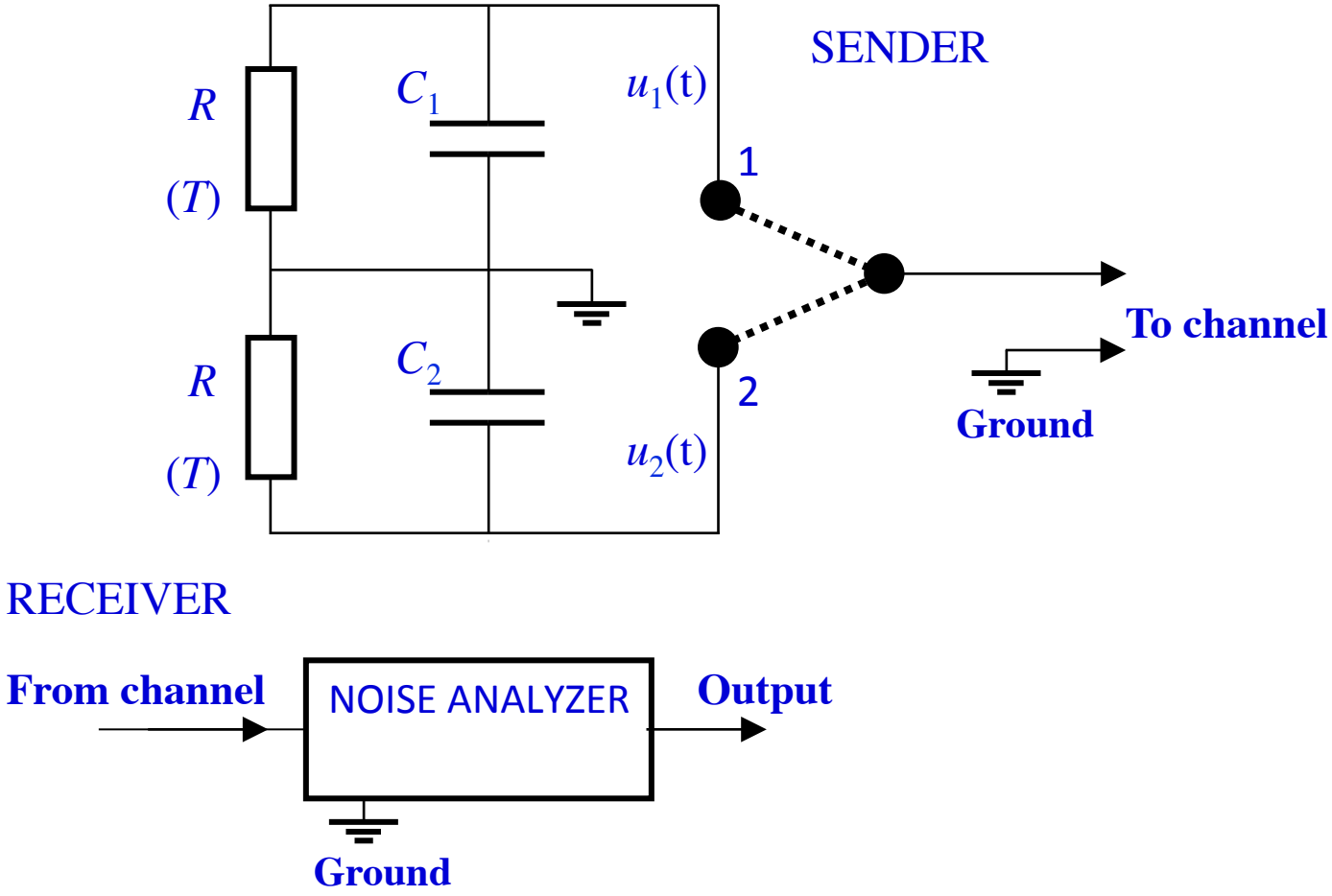
Zero-Signal-Power Classical Communication



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

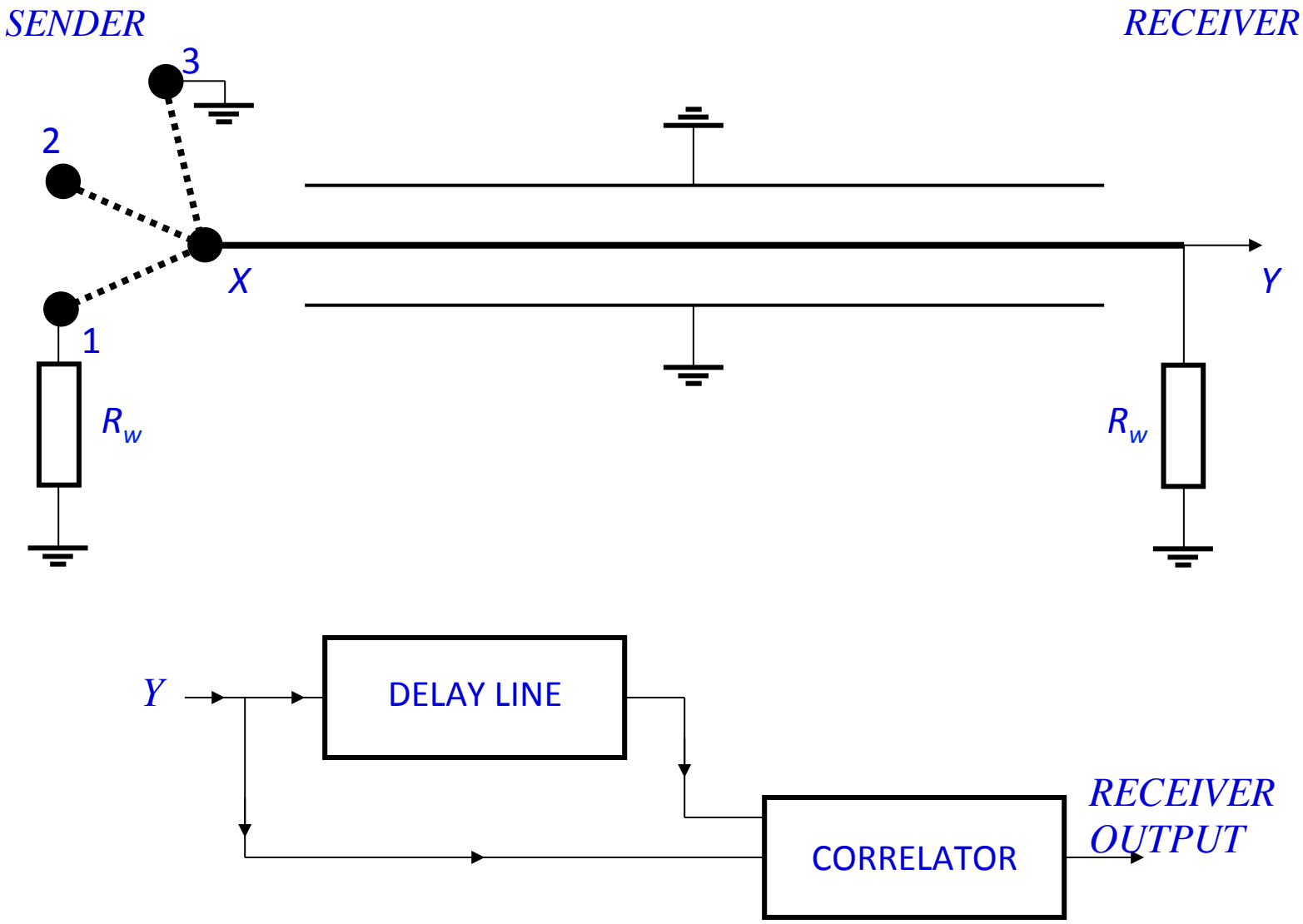
Bandwidth-based method (for wires)

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

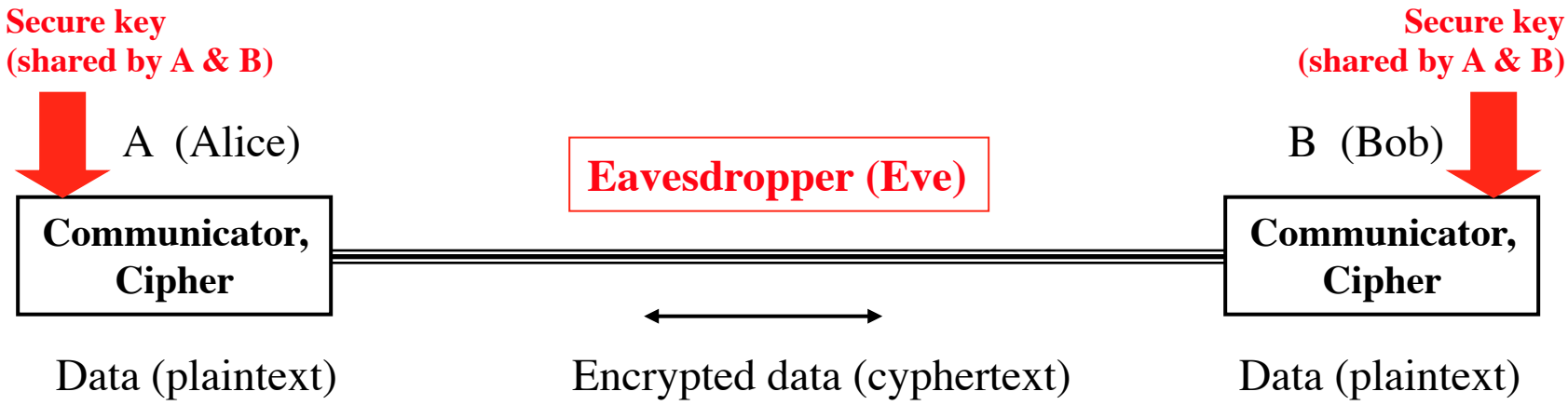


L.B. Kish, "Stealth communication: Zero-power classical communication, zero-quantum quantum communication and environmental-noise communication", *Applied Physics Lett.* **87** (2005), Art. No. 234109

Reflection-based method (for waves)



Secure communication via the internet by encryption

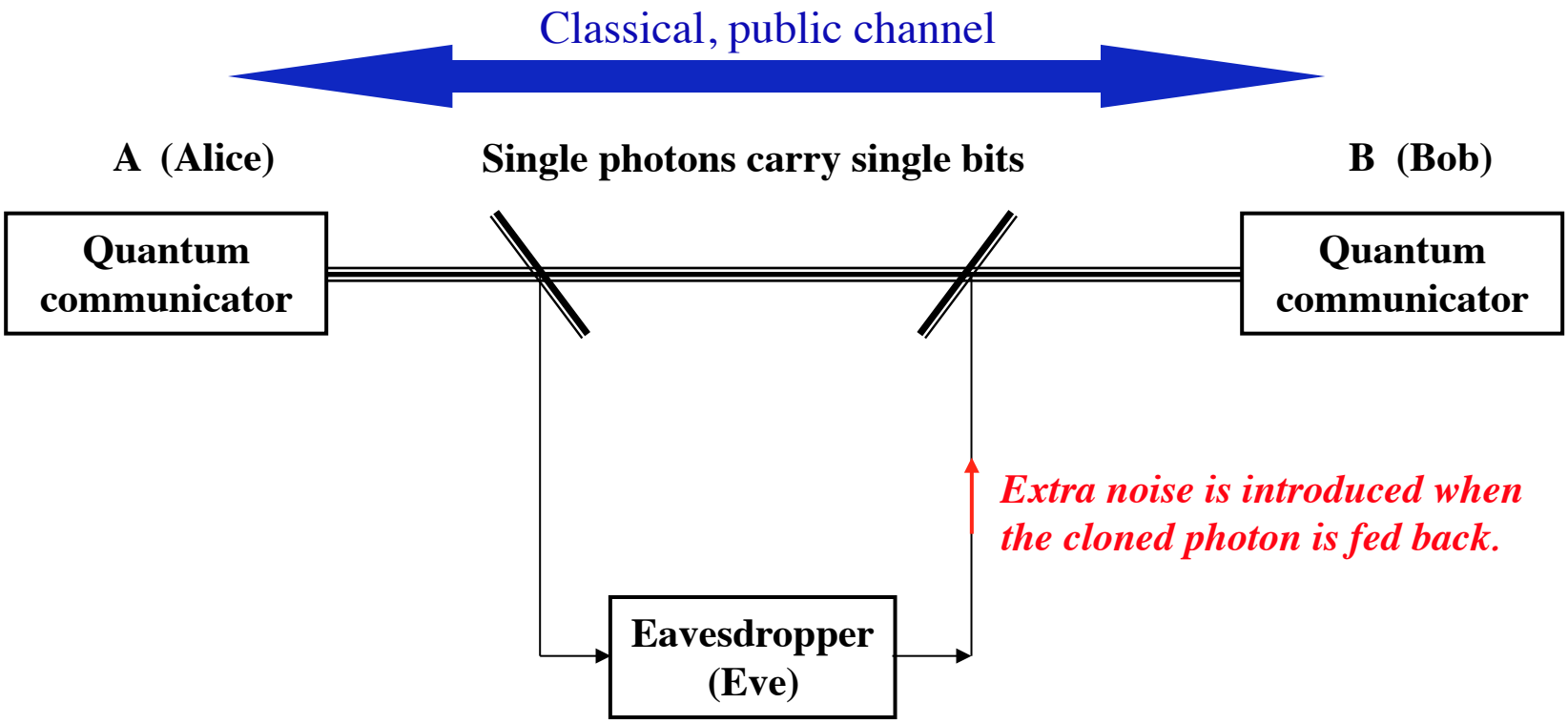


The eavesdropper (Eve) does not have the secure key thus she is unable to decrypt the information.

- ***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)

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.



Ongoing debates about and fully cracking the security of quantum key distribution (QK

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

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.

Heretic question back in 2005

Is it possible to do unconditionally secure key exchange with classical information, such as: voltage and current in a wire?

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

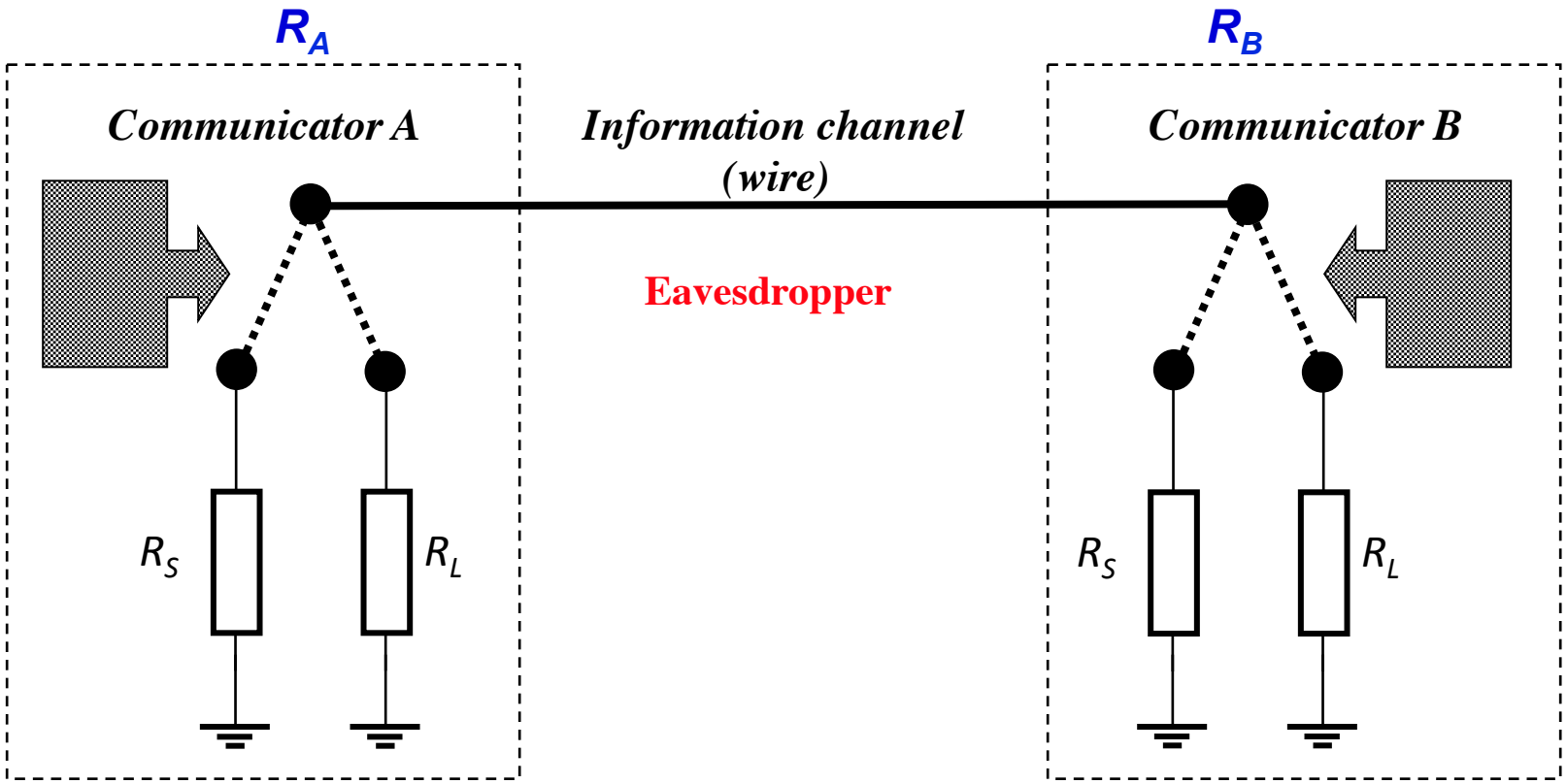
Basic idea: resistor loop (Kirchhoff loop): secure key generation and sharing

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:

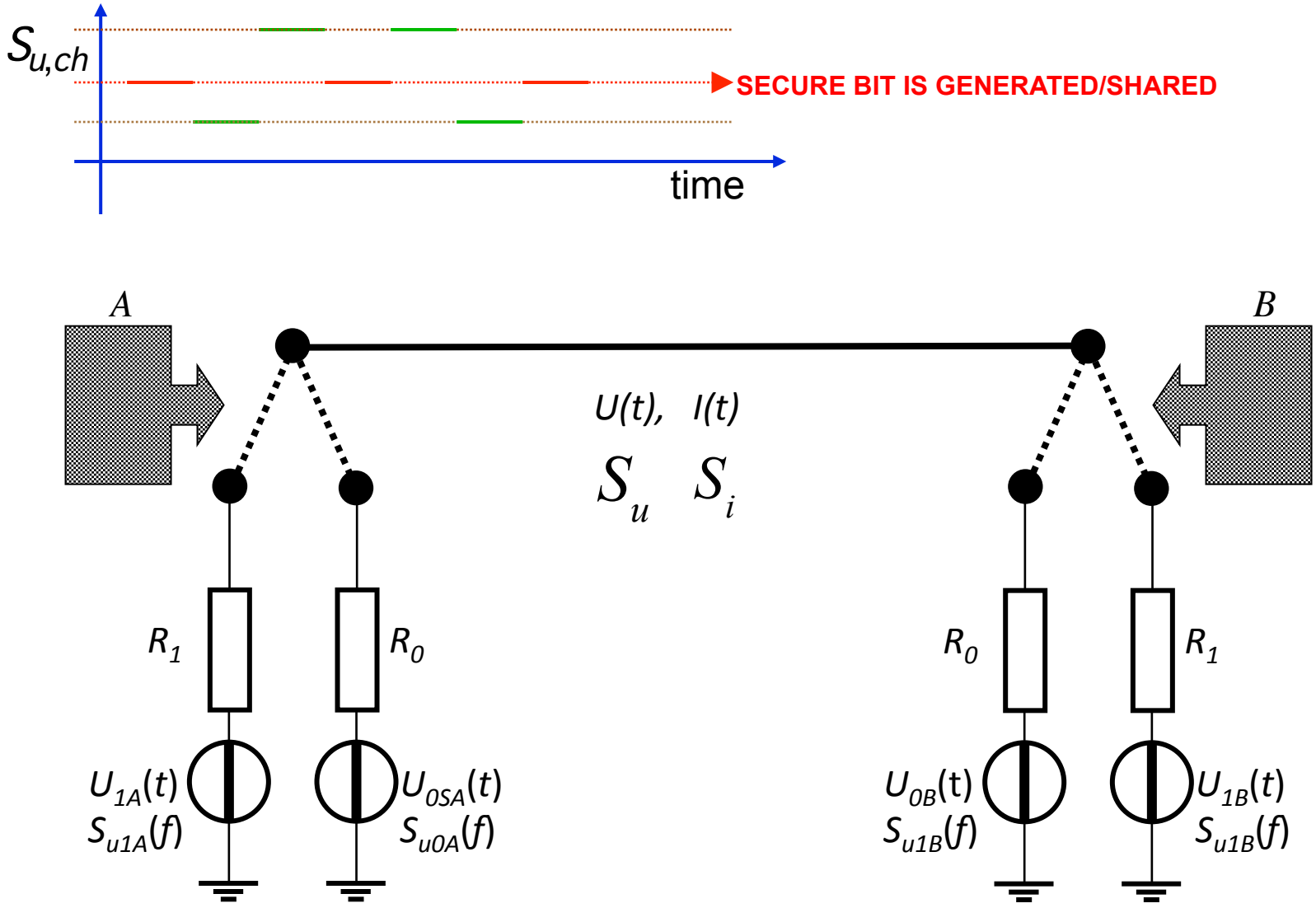
$$R_B = R_{loop} - R_A \;;\; R_A = R_{loop} - R_B$$

Who is feeding the cat? She, me, or both of us?



SECURE KEY GENERATION AND EXCHANGE BY VOLTAGE MEASUREMENTS

Who is feeding the cat? She, me, or both of us? Secure bit: when *either* she does it or me!

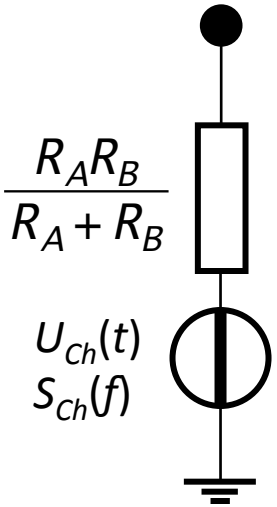


The loop resistance can be evaluated in two different ways

Johnson-Nyquist formulas for this Kirchhoff loop:

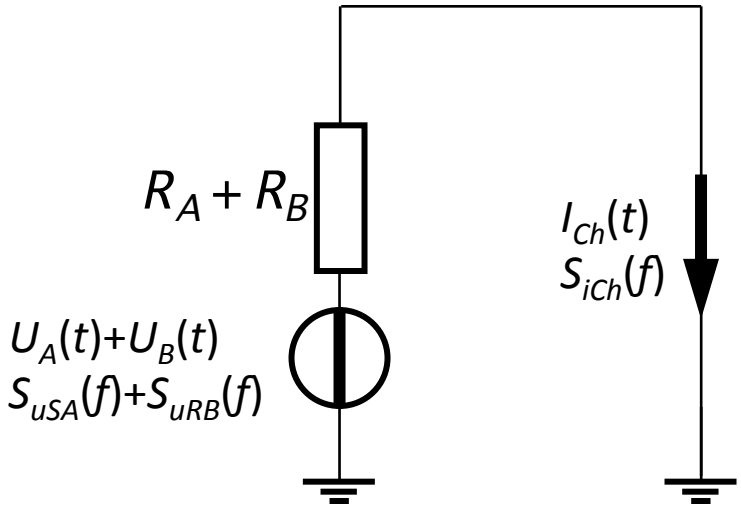
$$S_{u,R||}(f) = 4kT\frac{R_A R_B}{R_A + R_B}$$

(a)



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

(b)

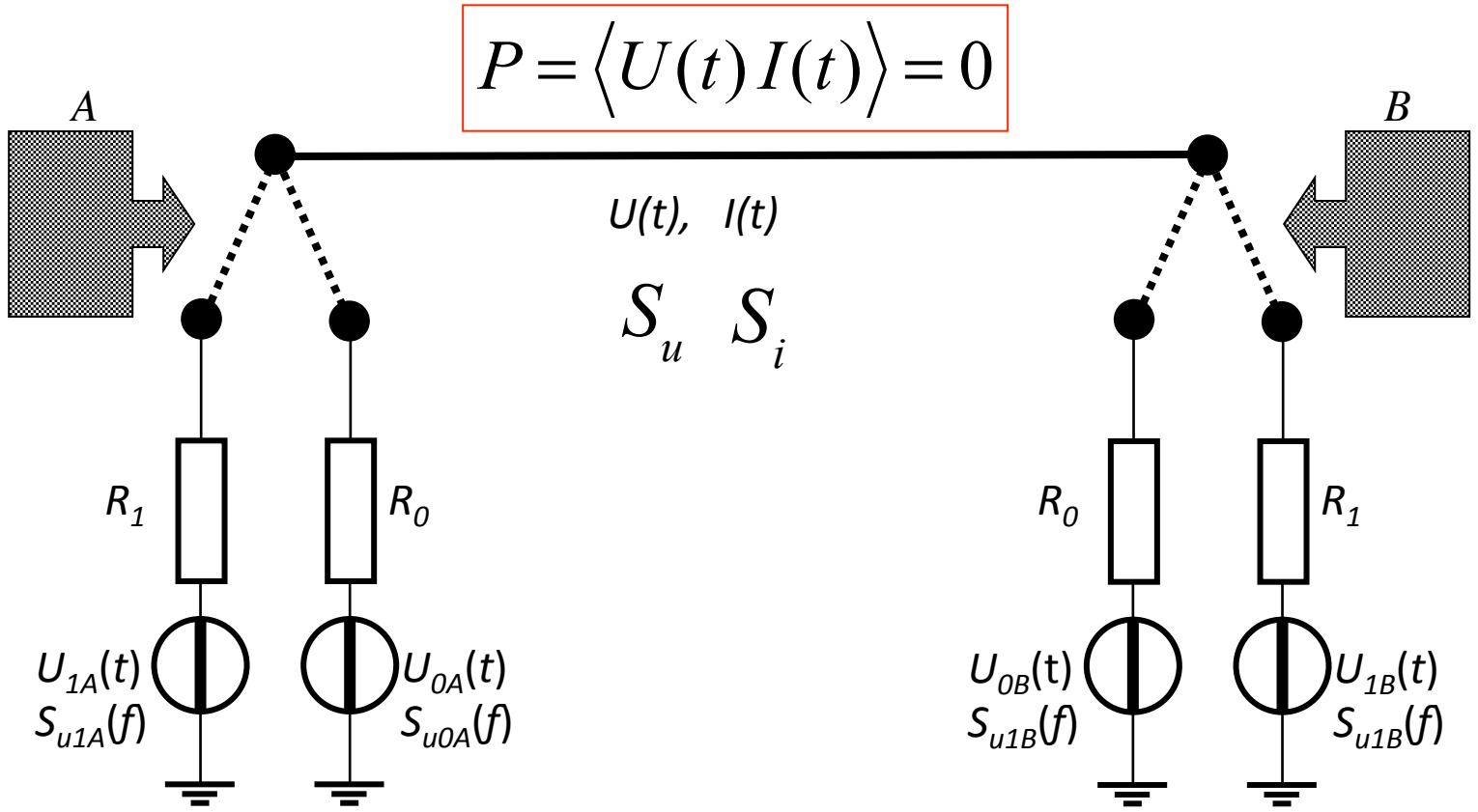


Eavesdropper's *Passively* Observed/Extracted Information: Resistance values but *not their locations*.

Gaussian processes **allow distribution functions** ***up to the second order only*****. But the net power flow is zero because of the** ***Second Law of Thermodynamics*****. It has been proven by multiple papers that the zero power flow is essential to perfect security; the most recent one is:**

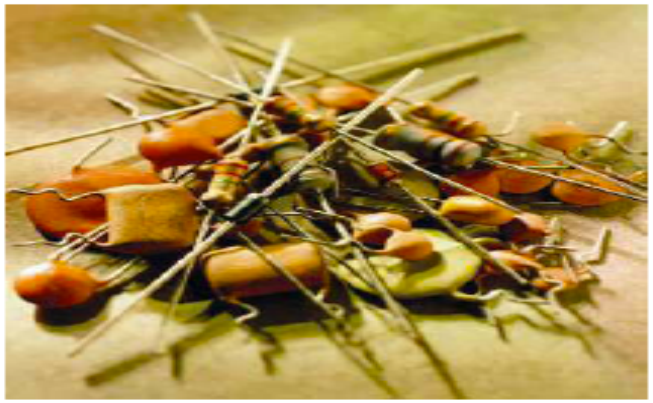
C. Chamon, L.B. Kish, "Perspective - On the thermodynamics of perfect unconditional security", *Appl. Phys. Lett.* **119**, (2021) 010501

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



Unconditional security over the wire: the KLJN hardware and protocol, some media features

Science Magazine, 2005 featuring the unpublished preprint

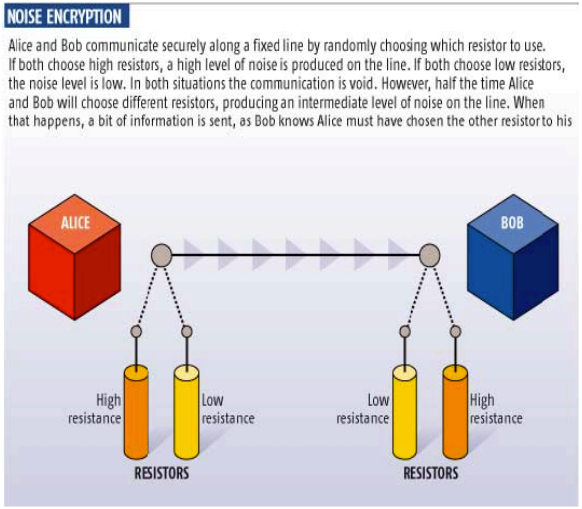


Stealth technology. A simple wire and resistors may send data securely.

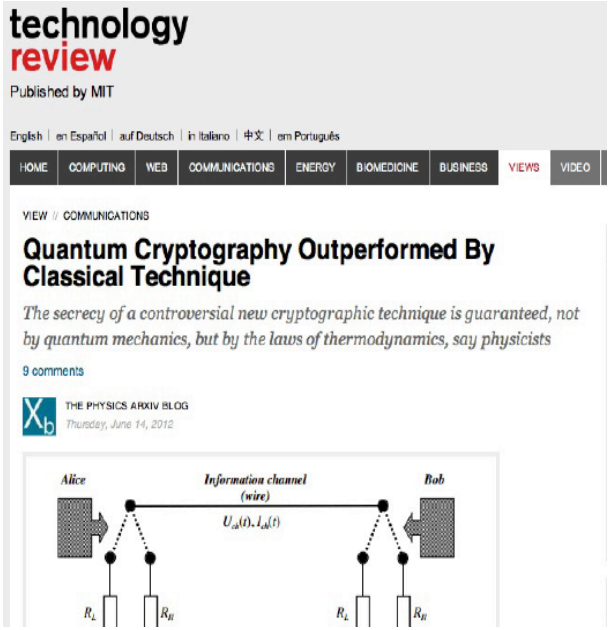
General security proof:
L.B. Kish, C.G. Granqvist, *Quantum Information Processing* **13** (2014) pp. 2213-2219.

http://www.scholarpedia.org/article/Secure_communications_using_the_KLJN_scheme

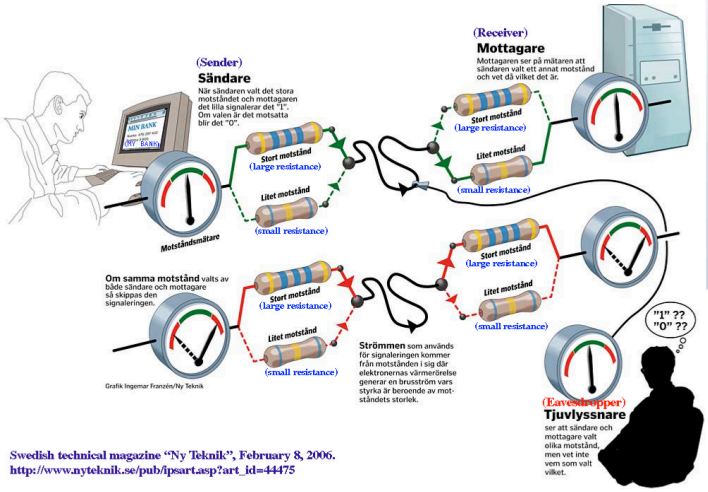
New Scientist magazine, 2007



MIT Tech Review 2012

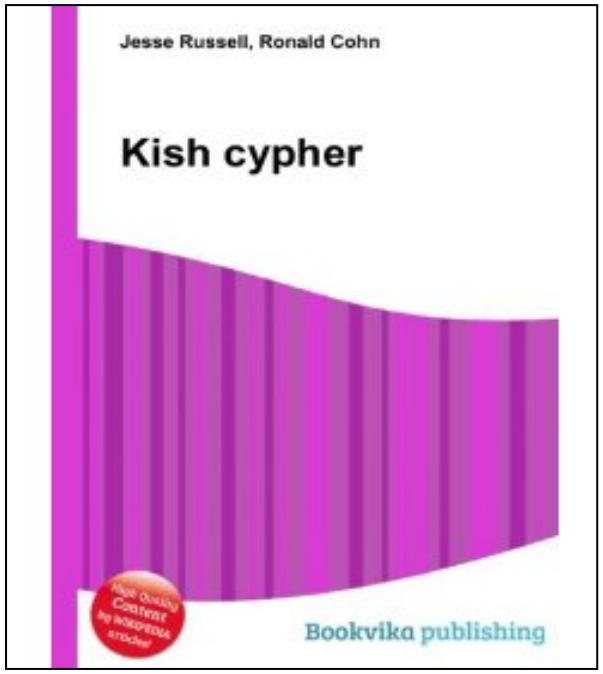


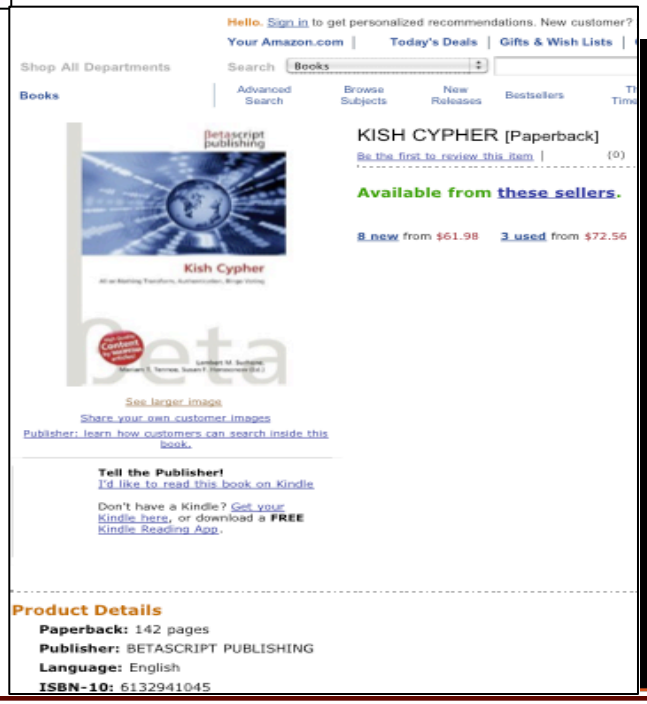
Ny Teknik magazine, Sweden, 2005



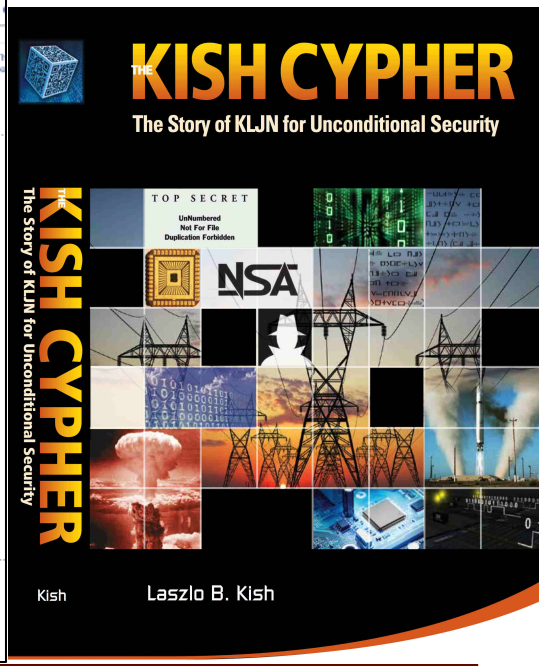
Swedish technical magazine "Ny Teknik", February 8, 2006.
http://www.nyteknik.se/pub/ipsart.asp?art_id=44475

Books by others (very bad ones)





My own book, 2017



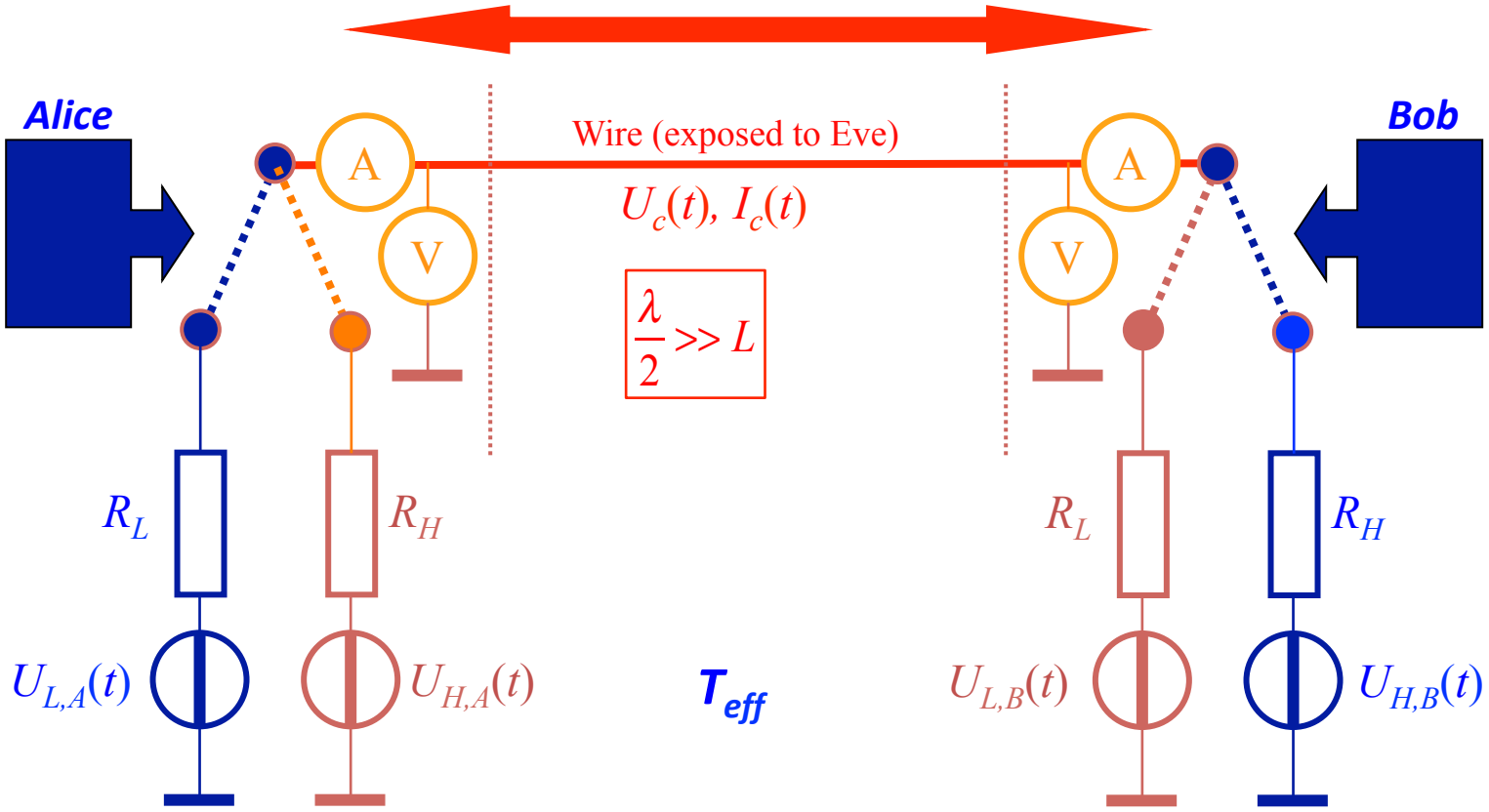
KLJN secure key exchanger, fully protected against passive and active (invasive) attacks

At active attacks, Eve modifies the system to extract information. Standard defense method is the current/voltage comparison providing unconditional security. Advanced models use a whole-cable simulator and random checking of integrity, too.

All these tools are possible because it is classical physics, not quantum. Safe against the classes of methods that cracked quantum communicators

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



Some of the potential applications:

Chip (integrability)

Credit cards

Securing computers, laptops, instruments, videogames

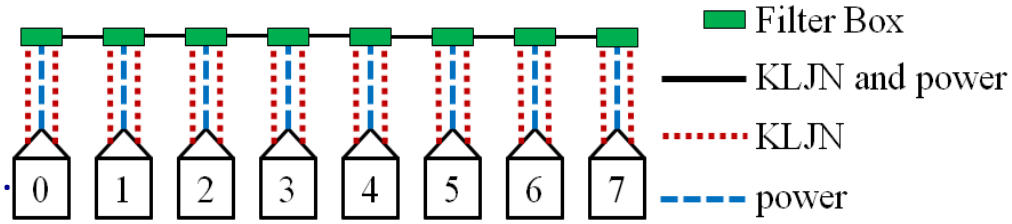
Powerlines

Autonomous vehicle systems (Vehicle ad hoc networks – VANET)

Some of the applications of KLJN:

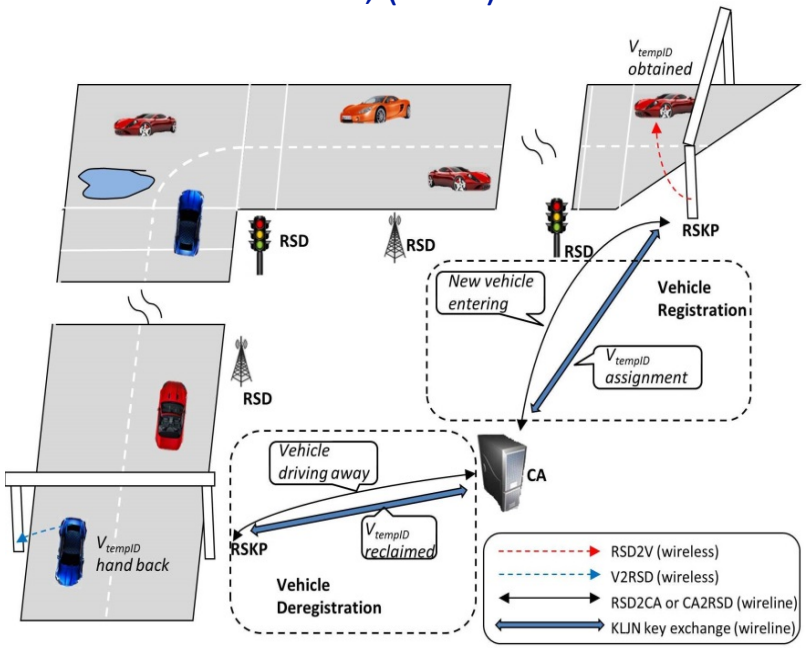
Unconditionally secure smart power grid

Patent: E. Gonzalez, L.B. Kish, R. Balog,
U.S. Patent US9270448 B2 (granted 2/2016).



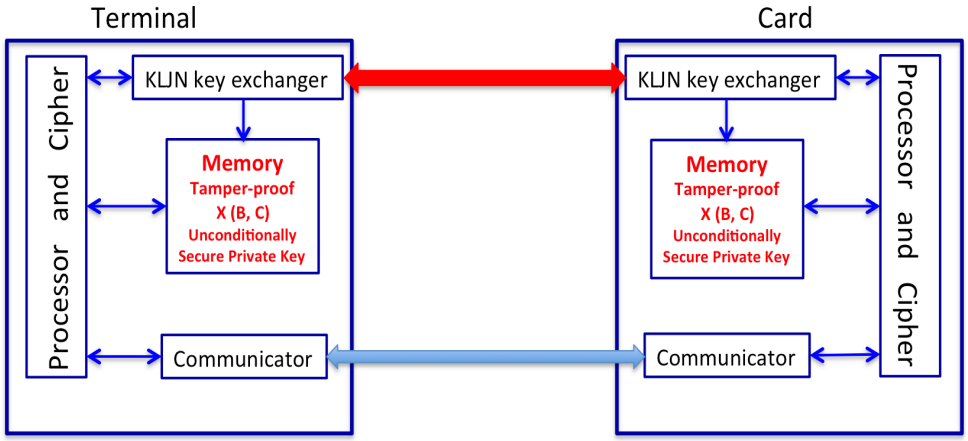
Unconditionally secure autonomous vehicle system

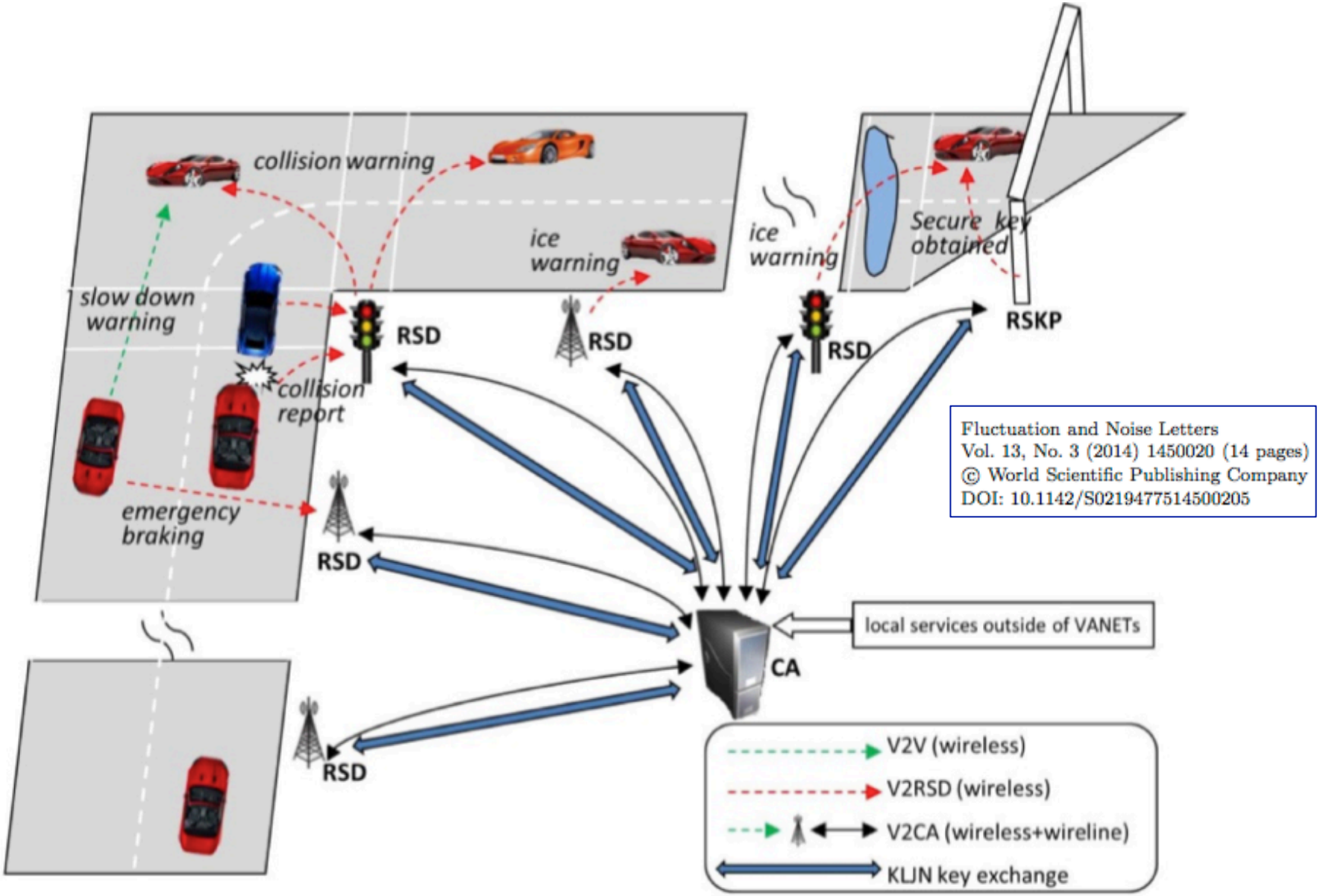
Fluct. Noise Lett. **14**, (2015) 1550008



Unconditionally secure credit and debit cards

Fluct. Noise. Lett. **16** (2017) 1750002





Fluctuation and Noise Letters
Vol. 13, No. 3 (2014) 1450020 (14 pages)

DOI: 10.1142/S0219477514500205

Fig. 3. VANET with unconditional secure key exchange. ¶

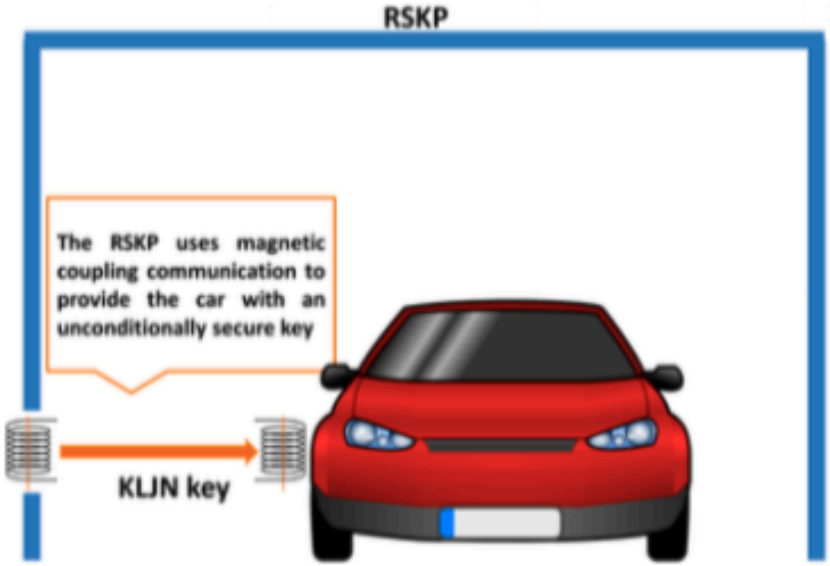


Fig. 5. Abstract illustration of RSKP delivering an unconditionally secure key to the vehicle via near field magnetic communication. Similar to the transformer principle, the magnetic near-field of two conductor coils is used to couple the initiator device (located at the RSKP) and listening device (located at the vehicle) [33]. Modulation schemes used include: amplitude on/off keying (OOK) with different modulation depth (100% or 10%) and binary phase-shift keying (BPSK) [33].

Fluctuation and Noise Letters
Vol. 14, No. 1 (2015) 1550008 (11 pages)

DOI: 10.1142/S021947751550008X

Fig. 6. Key donation with RSKP equipment embedded in the pavement. RSKPs are located underground of each lane.

If the length of the KLJN key is defined as N_k, then by combining Eqs. (1)–(4), we find that the lifetime of the KLJN key in vehicular communication networks is:

$$\tau_k = \frac{N_k}{f_c} = \frac{2N_k n_c \gamma L}{\Theta c}. \tag{5}$$

Note that this result represents a pessimistic estimation for inhomogeneous vehicular communication networks when n_c is the upper limit of the number of cars any RSD is handling. Thus, Eq. (5) gives an upper limit of the lifetime of the KLJN key in vehicular communication networks. To demonstrate the results, we assign possible practical values to the parameters. Let $L = 1000\,\mathrm{m}$, $c = 2{*}10^8\,\mathrm{m/s}$, $\gamma = 100$ (since $\gamma = \frac{B_{\mathrm{KLJN}}}{f_B}$, where $f_B \approx \frac{1}{\tau}$ should be low enough compared to B_{KLJN}, [30, 31]), $N_k = 100\,\mathrm{bits}$, $n_c = 1000$ vehicles, and $\Theta = 0.1$ (in order to satisfy $B_{\mathrm{KLJN}} \ll \frac{c}{L}$, that is the no-wave limit condition [22]). Then the lifetime of KLJN key is $\tau_k = 10^3\,\mathrm{s}$.

Techniques such as building parallel channels by using chip and multi-wire cables can be used to enhance the speed of the KLJN scheme and to decrease τ_k [19]. There is also a possibility to increase the security of physically exchanged keys in the case of repeated usage [33].

Noise-based informatics:

1. **Sensory information**
2. **Communications**
3. **Logic and computing**

Noise: stochastic signal

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

Motives

1. To reduce power dissipation and the related heat.

2. To use superpositions for multi-valued logic.

3. To utilize the noise products for exponential logic hyperspace: 2^N bits [2^(2^*N*) logic values] in a single wire, like in a quantum computer, for ***special-purpose***, exponentially large, parallel operations with polynomial hardware/time complexity.

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

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

"noise-based logic is one of the most ambitious atte

Sergey Bezrukov (NIH): brain logic, etc.

Walter Daugherity (CS, TAMU): CNOT and phonebook search on exponentially large superpositions, etc.

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

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

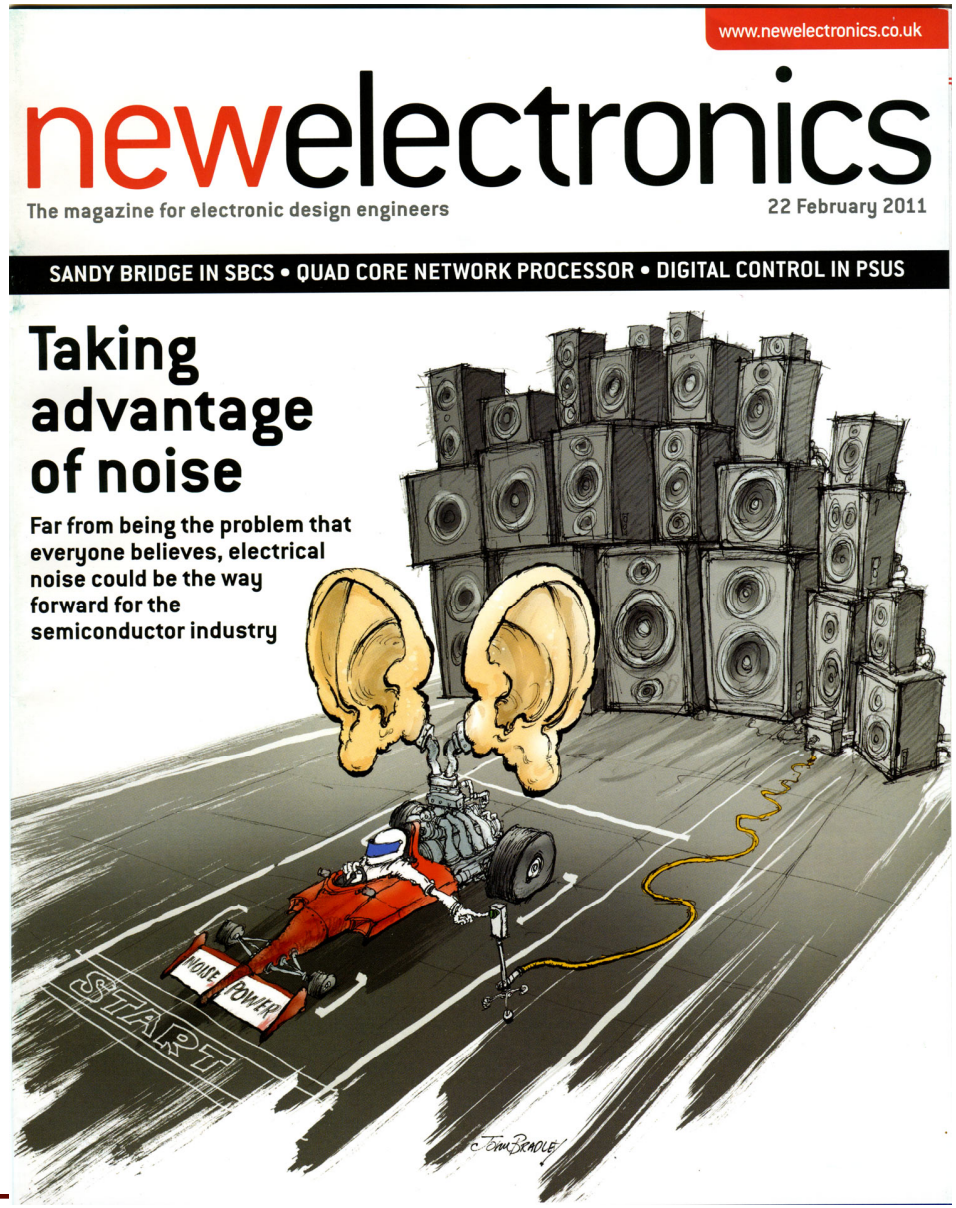
Sunil Khatri, (computer engineering faculty, TAMU): hyperspace, squeezed instantaneous logic, etc

Andreas Klappenecker (CS, TAMU): some of the quantum computing efforts, etc.

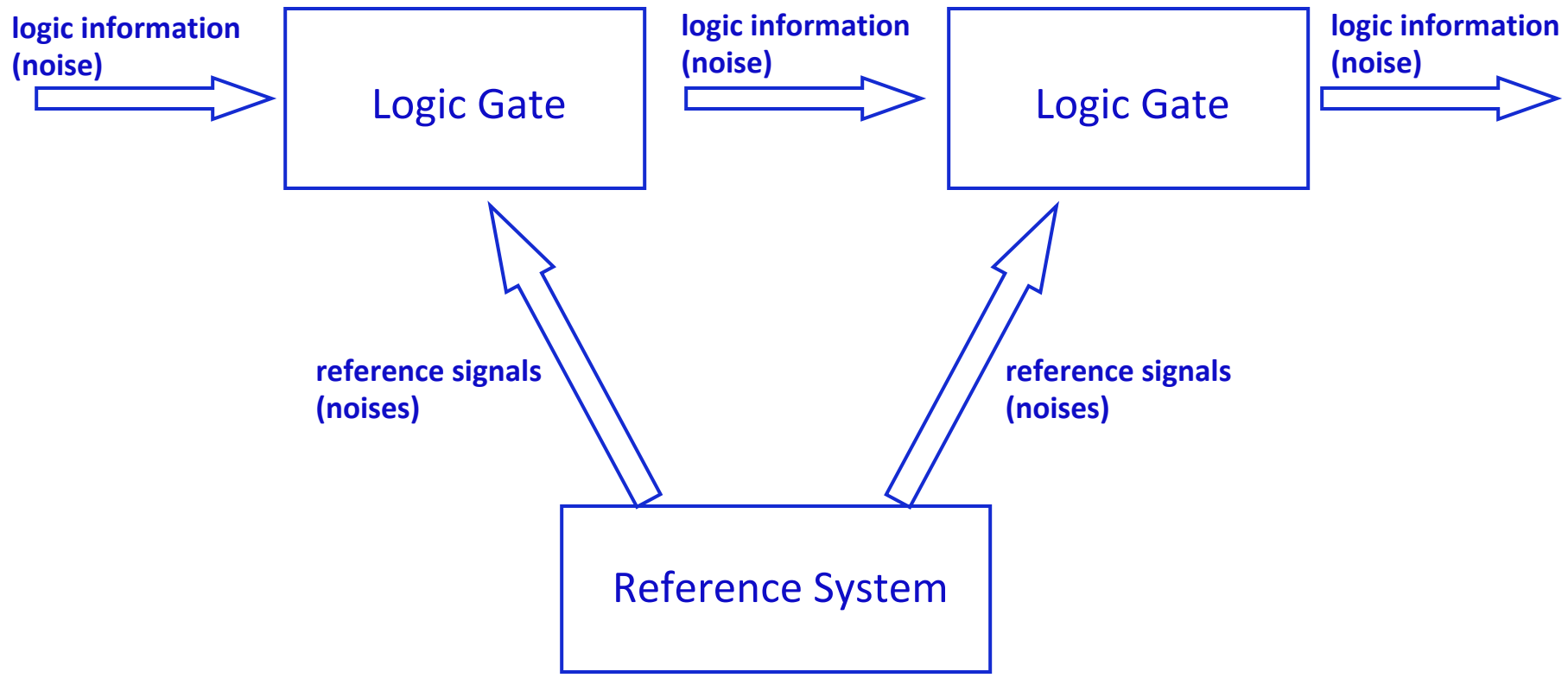
Ferdinand Peper (Kobe Research Center, Japan): squeezed and non-squeezed instantaneous logic, etc.

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

He Wen (Hunan University; former visiting scientist at TAMU): why noise?, problems with zeros, etc.



Generic noise-based logic outline

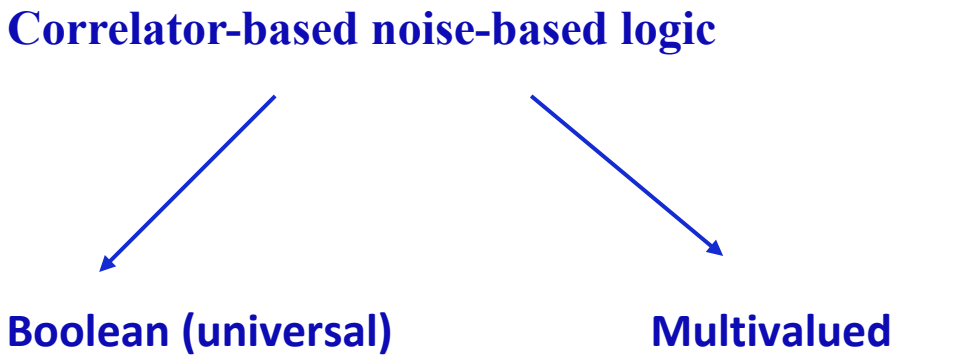


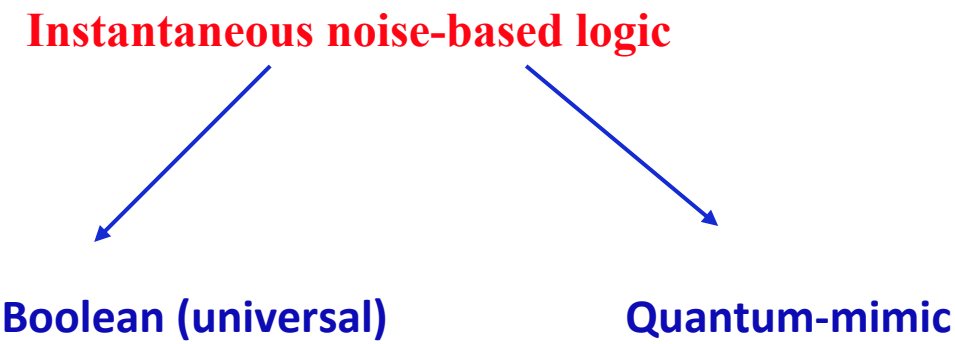
To identify and manipulate (gates) of the logic states (stochastic processes):

- **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:

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.***

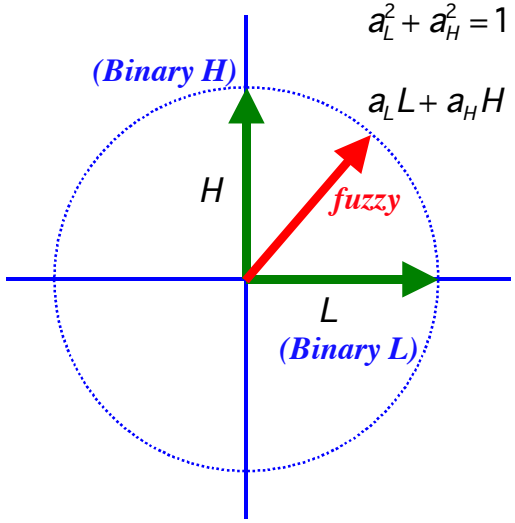
Examples: thermal noises of different resistors or current noises of different transistors: $V_k(t)$

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:

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



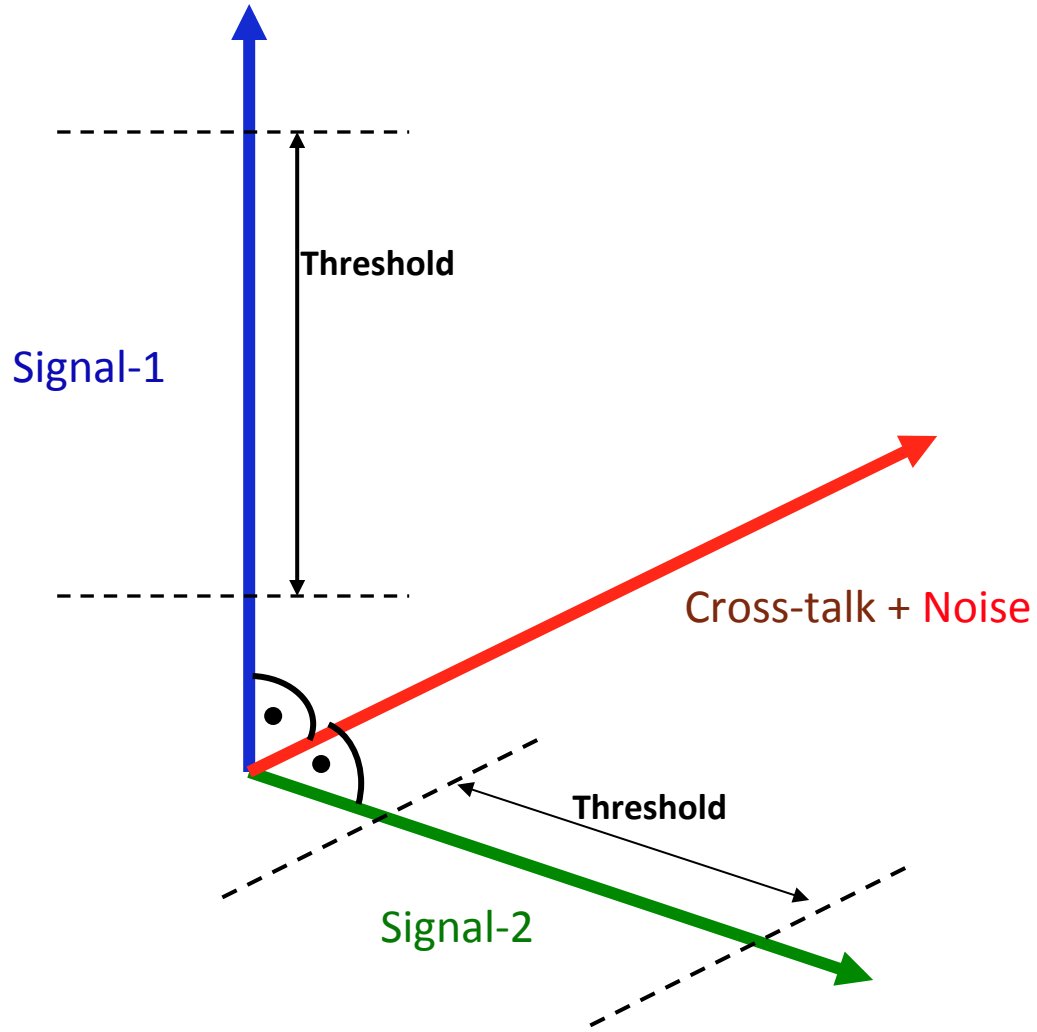
For example, a binary logic base is:

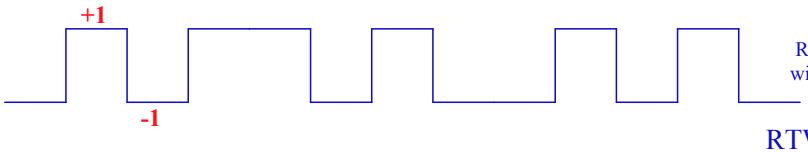
$$\langle L^2(t)\rangle = 1 \qquad \langle H^2(t)\rangle = 1 \qquad \langle H(t)L(t)\rangle = 0$$

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.





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

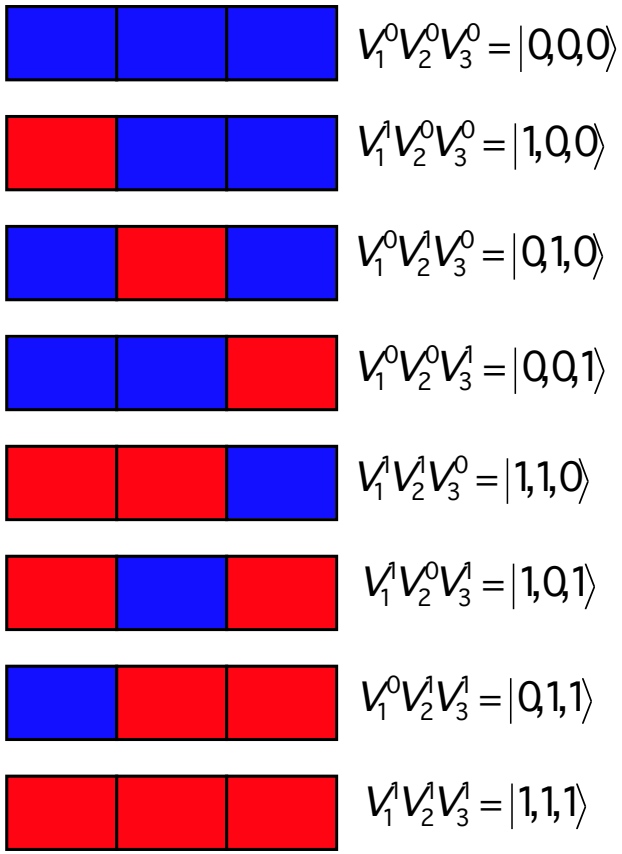
$(RTW_0 * RTW_1) * RTW_1 = RTW_0$

$(RTW_0 * RTW_1) * RTW_0 = RTW_1$

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



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

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

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

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

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

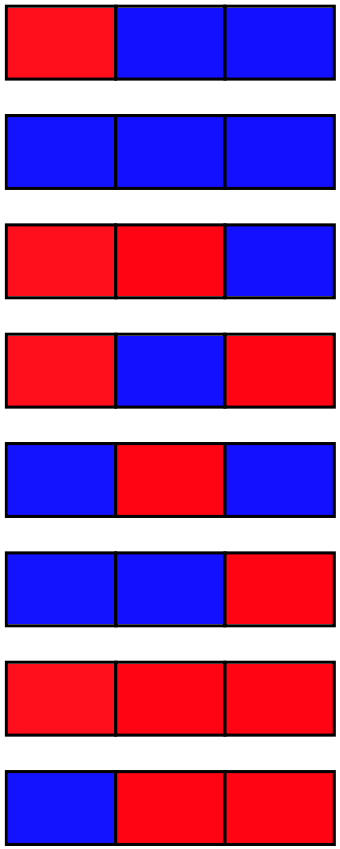
$V_1^1 V_2^0 V_3^1 = |1,0,1\rangle$

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

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

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

Single wire



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

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

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

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

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

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

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

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

Watch (next page) quantum-mimic instantaneous noise-based logic animation

by He Wen (music: Shankar Bhattacharyya)