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

Noise-Based Logic: Why Noise?

He Wen[1,2] and Laszlo B. Kish[1]

[1]*Department of Electrical and Computer Engineering, Texas A&M University, College Station*

[2]*Hunan University, College of Electrical and Information Engineering, Changsha, 410082, China*

Although noise-based logic shows potential advantages of reduced power dissipation and the ability of large parallel operations with low hardware and time complexity the question still persist: is randomness really needed out of orthogonality? In this talk after introducing noise-based logic we address this question.

A journal paper about this issue is coming out in the December issue of Fluctuation and Noise Letters
http://www.ece.tamu.edu/~noise/research_files/noise_based_logic.htm

Presented at: ICCAD 2012, SPECIAL SESSION: ***Computing in the Random Noise: The Bad, the Good, and the Amazing Grace***
November 5, 2012, San Jose, CA.

Our Noise-based Informatics efforts have much relevance:

1. **Sensory information: Fluctuation-Enhanced Sensing**
2. **Communications: Noise-based Secure Key Exchange, competitor of quantum encryption**
3. **Noise-based Logic and Computing**

"Spiritual" motivation to introduce and explore Noise-based Logic:

1. The evolution of microprocessor performance has slowed down

2. To understand how does the *brain works with noise*: neural signals.

3. *Myth-busting*: Quantum-informatics-mimics by classical physics.

   Exploring goals that quantum informatics hope to reach *within this century*.


EXTREMETECH

Top Searches: Apple • Android • Windows 8 • iPad   Trending: Windows 8 • Batteries • 3D • Automobiles

Computing | Mobile | Internet | Gaming | Electronics | Extreme

COMPUTING > MOVE OVER, QUANTUM CRYPTOGRAPHY: CLASSICAL PHYSICS CAN BE UNBREAKABLE TOO

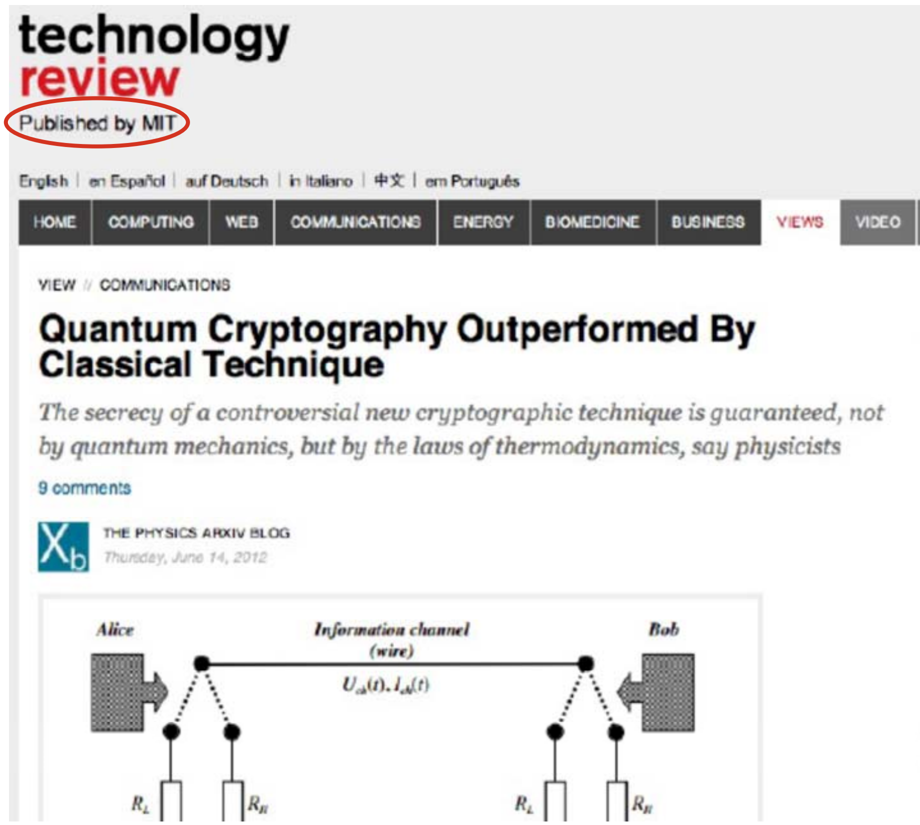
Move over, quantum cryptography: Classical physics can be unbreakable too

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

Share This Article

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

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


technology review

Published by MIT

English | en Español | auf Deutsch | in Italiano | 中文 | em Português

HOME | COMPUTING | WEB | COMMUNICATIONS | ENERGY | BIOMEDICINE | BUSINESS | VIEWS | VIDEO

VIEW // COMMUNICATIONS

Quantum Cryptography Outperformed By Classical Technique

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

9 comments

THE PHYSICS ARXIV BLOG

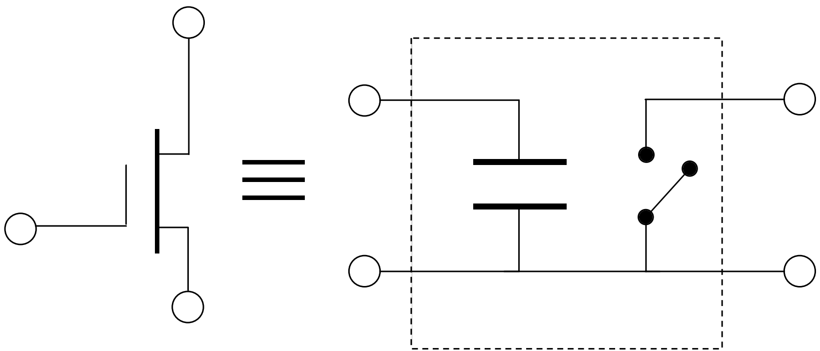
Thursday, June 14, 2012

The microprocessor problem

Speed-Error-Power **triangle**

Model-picture of speed and dissipation versus miniaturization (LK, *PLA*, 2002)

A switch is a potential barrier which
exists (*off position*) or not (*on position*).
To control/build the potential barrier we need energy.



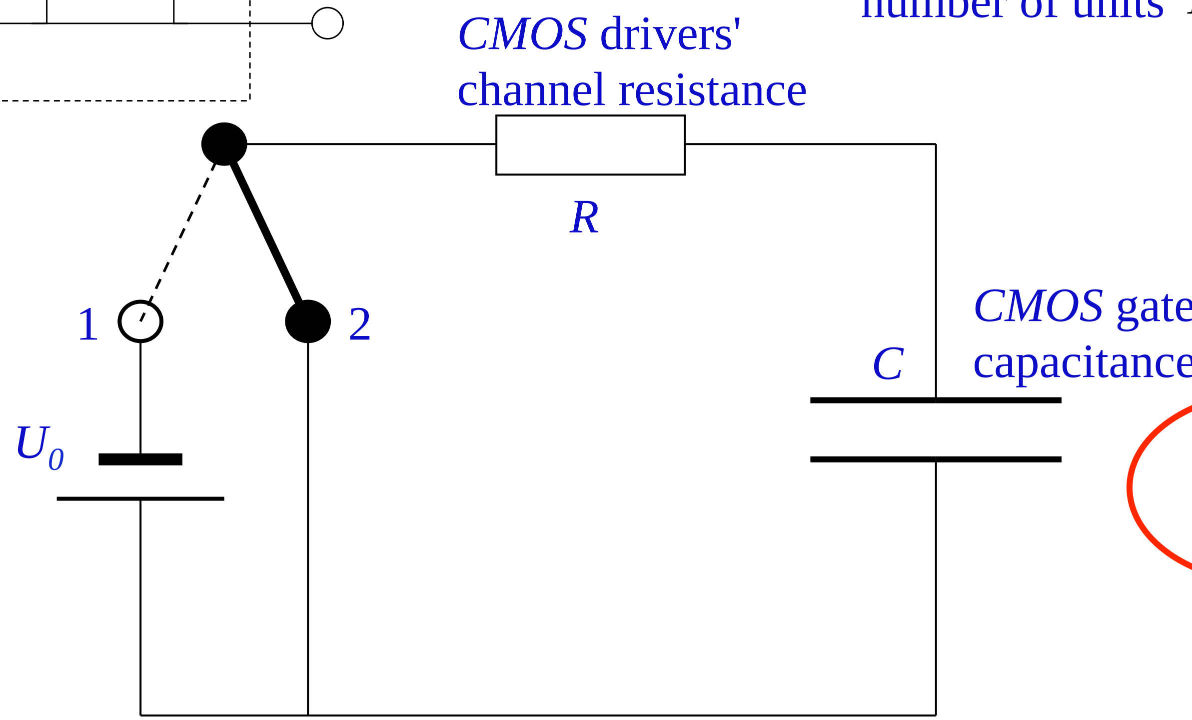
Maximal clock frequency $f_0 \cong (RC)^{-1}$

Dissipation by a single unit $P_1 \propto f_0 E_1 \propto (RC)^{-1} C U_0^2 \propto \dfrac{U_0^2}{R}$

Total dissipation by the chip $P_N \propto N U_0^2 / R \propto N U_0^2 \propto U_0^2 / s^2$

s : characteristic device size

number of units $N \propto \dfrac{1}{s^2}$

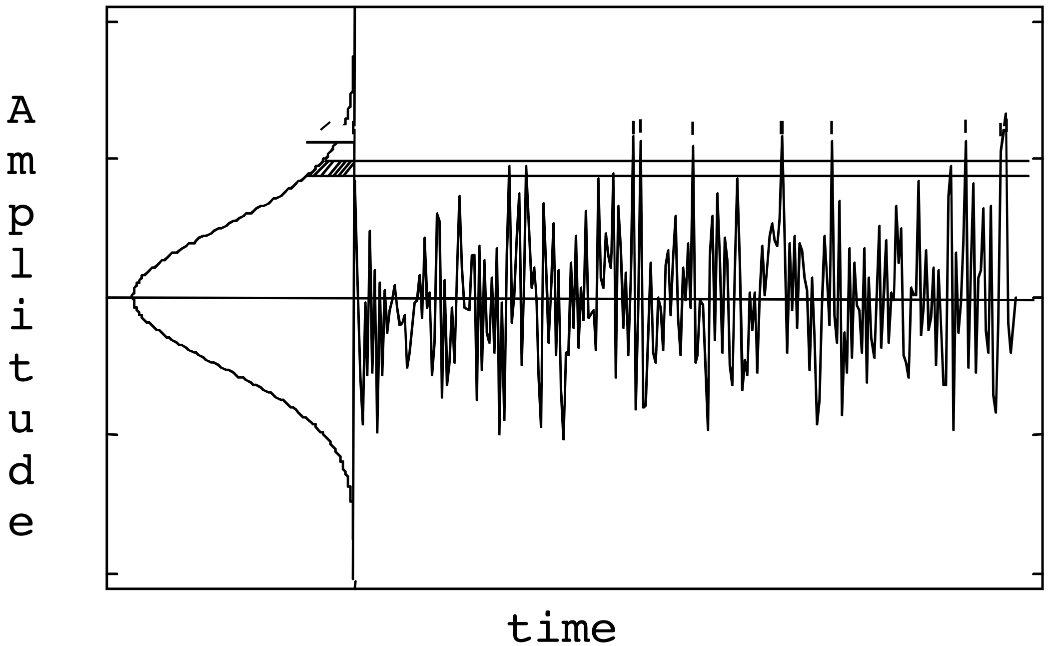


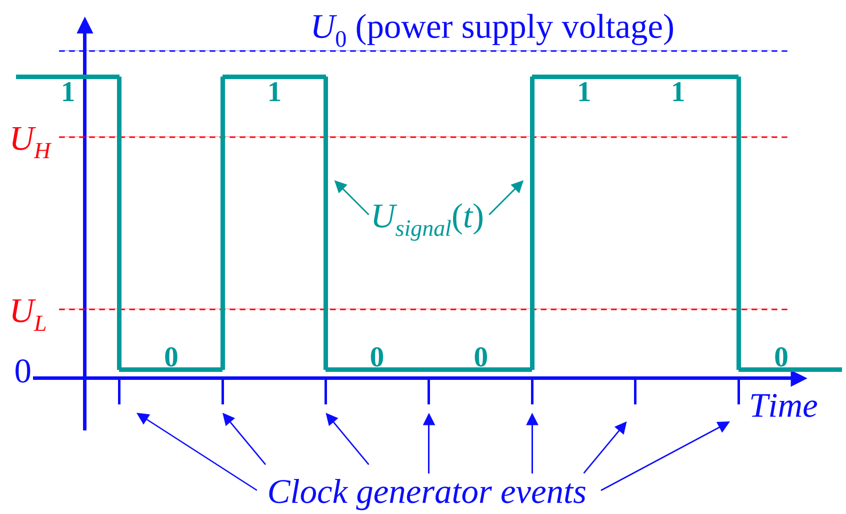
$C \propto s^2$

$C \propto s$

False bit flips. Gaussian noise can reach an arbitrarily great amplitude during a long-enough period of time and the *rms* noise voltage grows with miniaturization:

$$U_n = \sqrt{\frac{kT}{C}}$$





Same as the thermal activation formula, however, here we know the mean attempt frequency more accurately.

For band-limited white noise, frequency band (0, f_c), the *threshold crossing frequency* is:

$$\nu(U_{th}) = \frac{2}{\sqrt{3}} \exp\left(\frac{-U_{th}^2}{2U_n^2}\right) f_c \qquad \text{where} \qquad U_n = \sqrt{S(0) f_c}$$

L.B. Kish, "End of Moore's Law; Thermal (Noise) Death of Integration in Micro and Nano Electronics", Phys. Lett. A., 305 (2002) 144–149
L.B. Kish, "Moore's Law and the Energy Requirement of Computing versus Performance", IEE Proc. - Circ. Dev. Syst. 151 (2004) 190-194.

Energy dissipation of single logic operation at ε error probility:

$$E > kT \ln \frac{1}{\varepsilon}$$

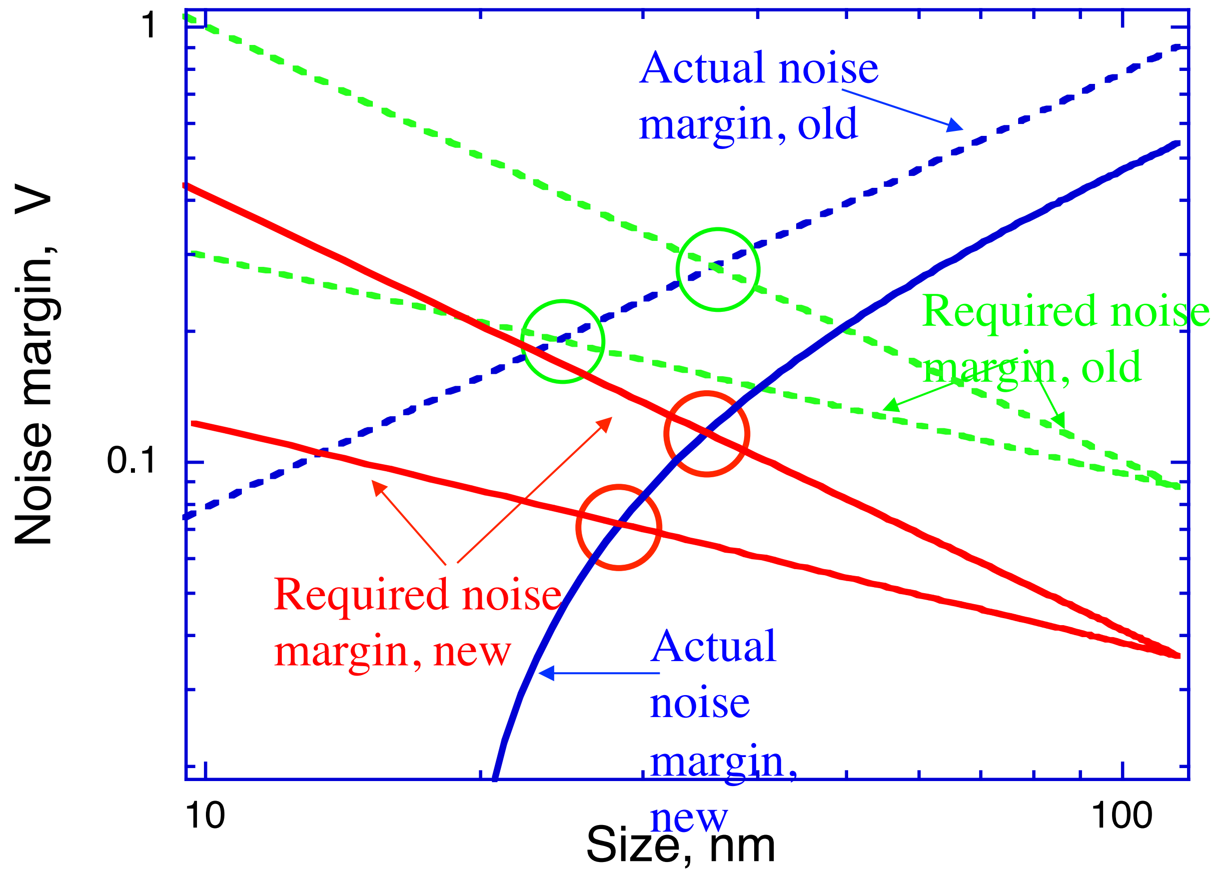
Speed-Error-Power

$$\varepsilon < 10^{-25} \Rightarrow E \approx 60kT$$

Practical situation is much worse; prediction in 2002-2003:

It was supposed that:

- *The bandwidth is utilized;*
- *The supply voltage is reduced proportionally with size (to control energy dissipation and avoid early failure due to hot electrons.*



ELSEVIER

November 2002

PHYSICS LETTERS A

Physics Letters A 305 (2002) 144–149

www.elsevier.com/locate/pla

End of Moore's law: thermal (noise) death of integration in micro and nano electronics

Laszlo B. Kish [1]

Texas A&M University, Department of Electrical Engineering, College Station, TX 77843-3128, USA

Received 16 July 2002; received in revised form 19 September 2002; accepted 19 September 2002

Communicated by C.R. Doering

Abstract

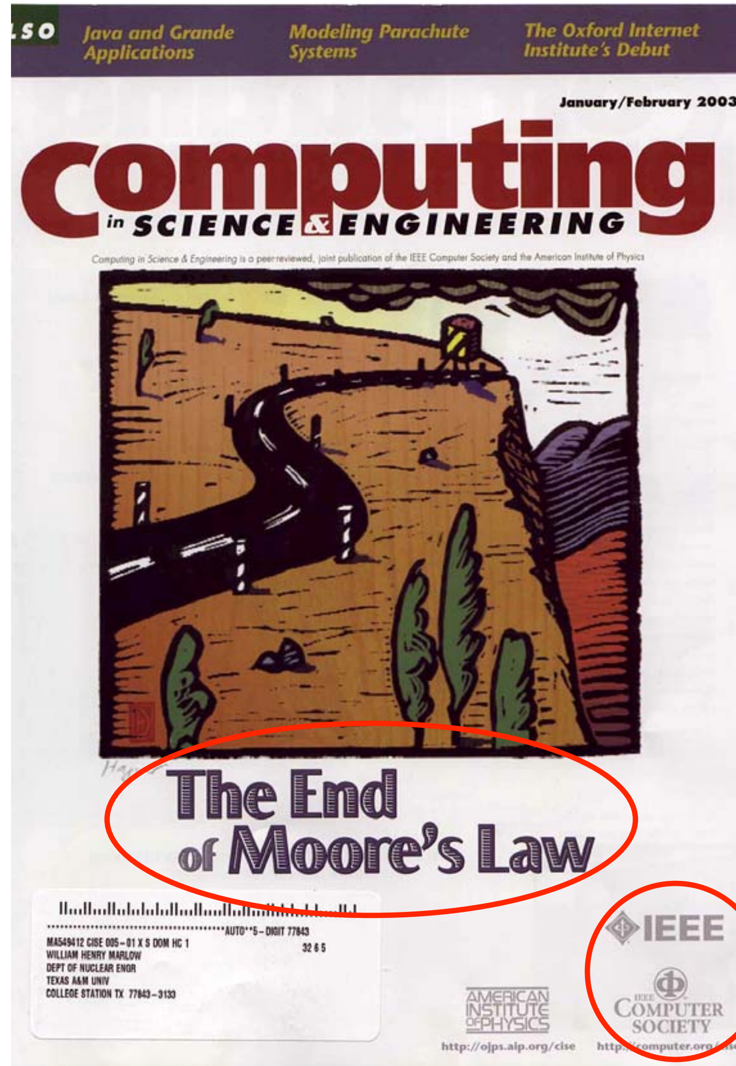
The exponential growth of memory size and clock frequency in computers has a great impact on everyday life. The growth is empirically described by Moore's law of miniaturization. Physical limitations of this growth would have a serious impact on technology and economy. A thermodynamical effect, the increasing thermal noise voltage (Johnson–Nyquist noise) on decreasing characteristic capacitances, together with the constrain of using lower supply voltages to keep power dissipation manageable on the contrary of increasing clock frequency, has the potential to break abruptly Moore's law within 6–8 years, or earlier.

Conclusion was (2002): ***if the miniaturization is continuing below 30-40 nm, then the clock frequency cannot be increased.***

No increase since 2003 ! Prophecy fulfilled much earlier!

Even though Moore's law has seemingly been followed, the speed of building elements are not utilized. Supply voltage has been kept high.

January 2003



The brain

dreams and reality

In the "Blade Runner" movie (made in 1982) in Los Angeles, at 2019,
the *Nexus-6* robots are *more intelligent* than average humans.

2019 is only 7 years from now **and nowadays we have been observing the** ***slowdown*** **of the** ***evolution*** **of computer chip performance.**

We are simply nowhere compared a Nexus-6.

Have we missed the noisy neural spikes in our computer developments???

Isaac Asimov (1950's): ***The Three Laws of Robotics:***

1. A robot may not injure a human being, or, through inaction, allow a human to come to harm.

2. A robot must obey orders given to him by human beings except where such orders would conflict with the First Law.

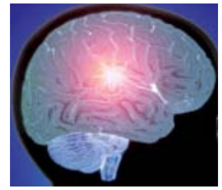
3. A robot must protect its own existence as long as such protection does not conflict with the First or Second Law.

Not even the best supercomputers are able to address such refined perception of situations!

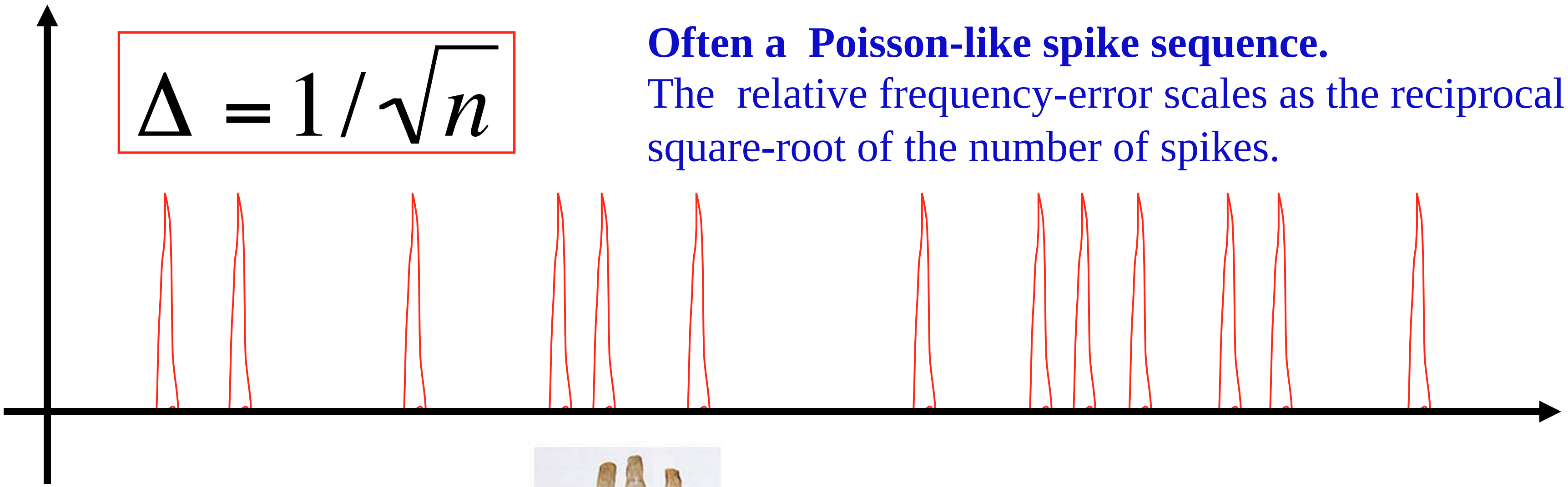
We have *great problems even with the most elementary necessities*, such as *recognition of natural speech* of arbitrary people or *speech in background noise*.

How does biology do it??? A quick comparison.

Note: Average power consumption of a supercomputer in the worldwide TOP-10 list (2012) is **1.32 million Watts**.



This Laptop	**Human Brain**
Power dissipation: about 12 W	**Brain dissipation: about 12 W**
Number of switches (transistors): 10^{13}	**Number of switches (neurons): 10^{11}**
Very high bandwidth (GHz range)	**Extremely low bandwidth (< 100 Hz)**
Signal: deterministic, binary voltage	**Signal: *stochastic spike train, noise***
Deterministic binary logic scheme, *general-purpose(?)*	**Unknown logic scheme, *special-purpose (???)***
Potential-well based, addressed memory	**Unknown, associative memory**
High speed of fast, primitive operations	**Slow but intelligent operations**
Low probability of errors	**High probability of errors, even with simple operations**
Sensitive for operational errors (freezing)	**Error robust (no freezing) (?)**



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

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

1 = flexor digitorium
2 = lumbrical

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 in a palmtop, 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 our palmtop computer!

Noise-based logic

Present and past collaborators on noise-based logic (Alphabetical order).

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

Khalyan Bollapalli (former computer engineering PhD student, TAMU): exploration of sinusoidal orthogonal logic

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

Tamas Horvath (Frauenhofer for Computer Science, Bonn, Germany): string verification, Hamilton coloring problem.

Sunil Khatri, (Computer Engineering, TAMU): hyperspace, squeezed instantaneous logic, etc.

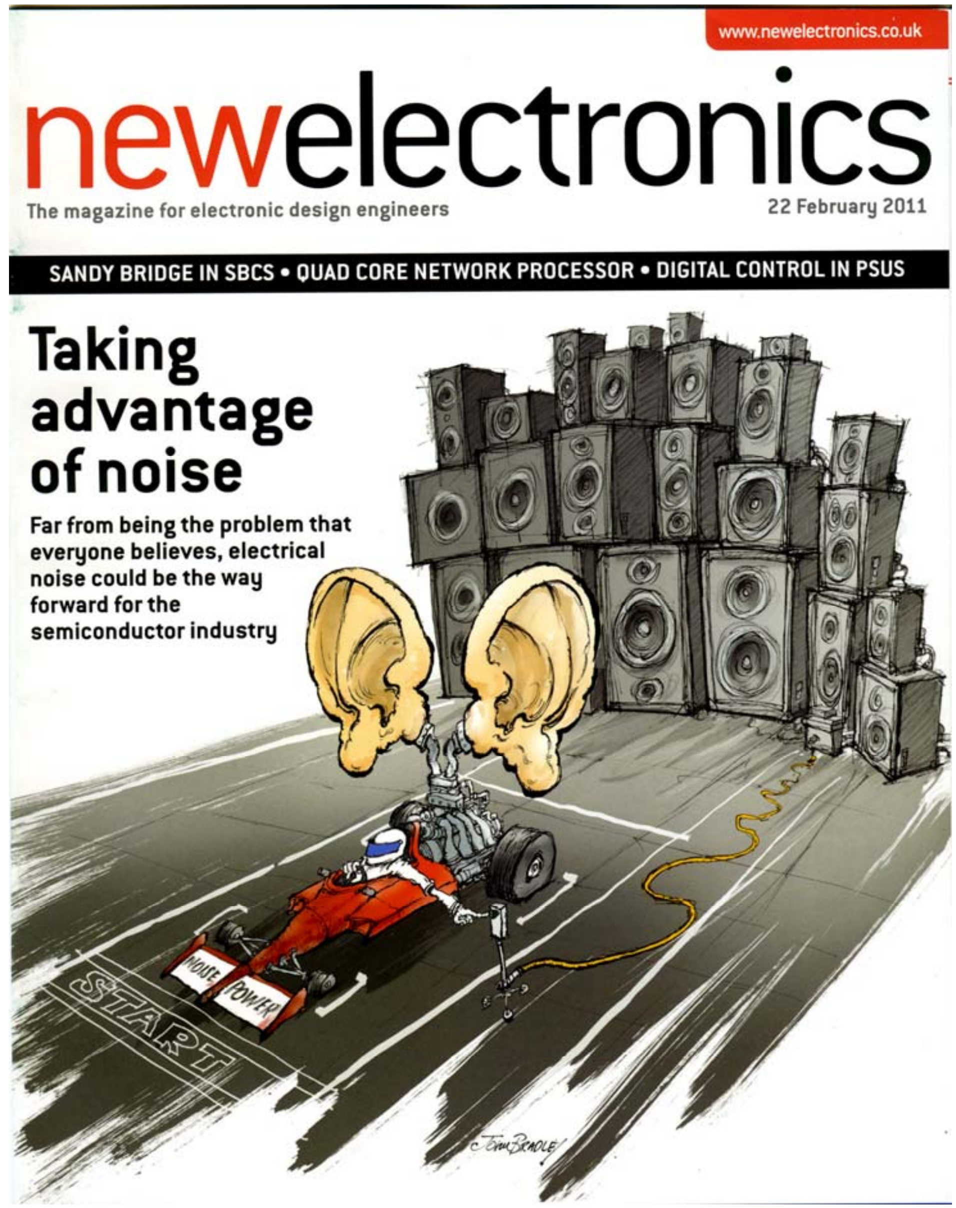
Andreas Klappenecker, (Computer Science, TAMU): quantum-mimicking, large complexity instantaneous parallel operations, etc.

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

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

He Wen (Electrical Engineering, TAMU; Visiting Scholar from Hunan University, China): large complexity instantaneous parallel operations; why noise; complex noise-based logic, etc.

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



What is Noise-based logic:

- ***Noise carries the logic information.***
- ***The logic base, which is a reference signal system, consists of uncorrelated (orthogonal) stochastic signals (noises). These are orthogonal vectors. Superpositions are possible: vector space.***
- ***This reference system is needed to identify these vectors in a deterministic way. Deterministic logic.***

What *noise-based logic* is certainly not: ***It is not noise-assisted signal transfer***, for example:

- ***It is not stochastic resonance***
- ***It is not dithering***
- ***It is not linearization by noise***

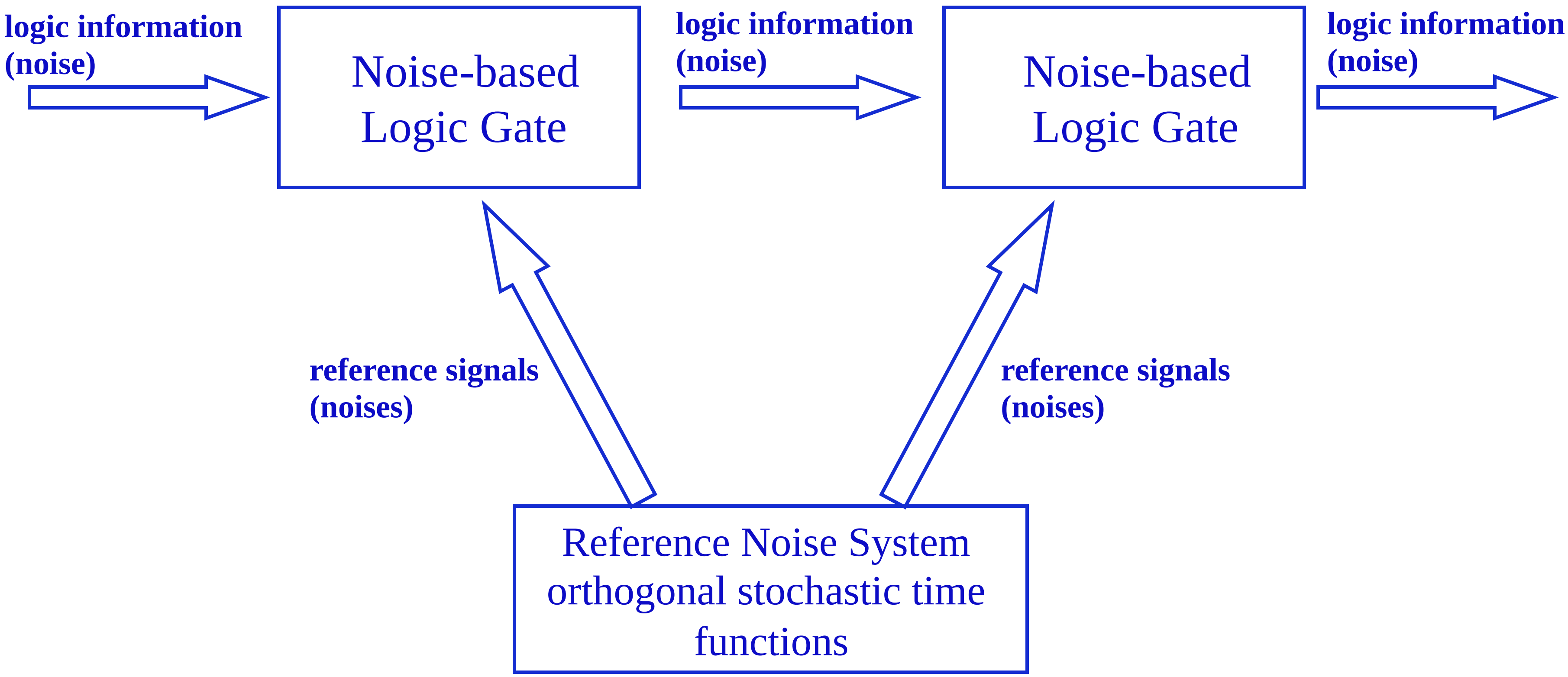
None of these schemes use the noise as information carrier.

Note: because noise-based logic is ***deterministic logic***:

- ***It is not stochastic computing***
- ***It is not randomized algorithm (even though it may utilize such)***

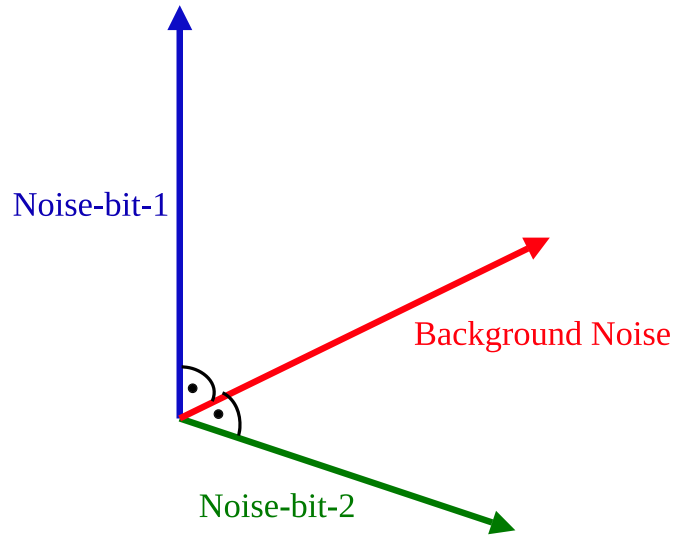
How does a noise-based logic hardware look like?

Generic noise-based logic outline



1. Logic signals are noises that are orthogonal on the noise. Base: *N* orthogonal noises: noise-bits.

2. Multivalued logic.



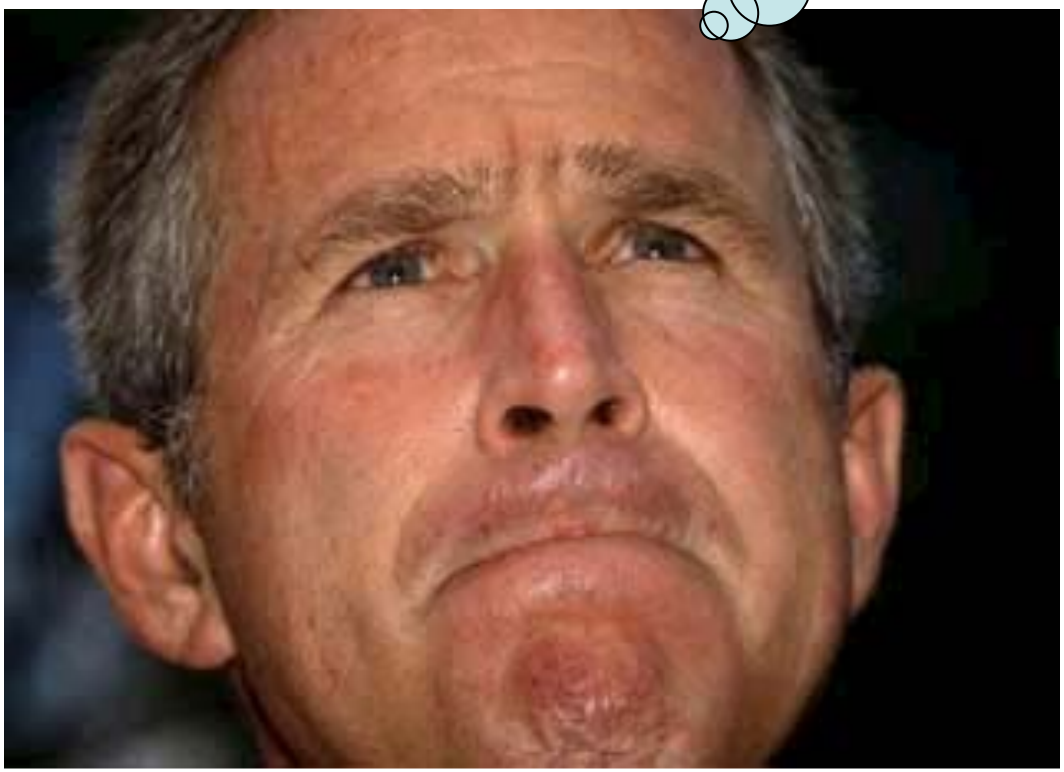
3. Superpositions. *N* noise-bits. *N* bits simultaneously in a single wire.

4. Hyperspace vectors. Product of two or more different base noises: orthogonal to each base noise. Their superpositions represent 2^N bits simultaneously in a single wire.

Quantum computers: *N* qubits represents 2^N classical bits

(Note: sinusoidal functions can also do this, see below, but there is a price)

But, periodic functions, like sinusoidals can also do this! ***Why noise ???***



But why noise?

At least three major aspects of noise compared to periodic:

- Physics: Entropy production (energy dissipation):

Simple wording: noise is freely available; generated by the system without power requirement.

Deeper: Brillouin's negentropy law. The deterministic signal has negative entropy (negentropy) due to its information entropy $\boldsymbol{I_s}$ (amplitude resolution; reduced relative uncertainty). Due to the Second Law of Thermodynamics, the entropy of the whole closed system cannot decrease thus, at least, the same amount if positive entropy (in this case, heat) will be produced. If a resonator circuit is used on the oscillator, this heat production will be repeated within the passive relaxation time (Q-times the period) of the resonator thus a continuous heating power will be generated:

$$P_{heat} = TS_s / \tau \geq \tau^{-1} \overbrace{kTI_s \ln(2)}^{\text{Brillouin}}$$

In a resonator-free oscillator the situation is worse because the same heat is produced at each period of oscillation, which means the dissipation is Q-times higher.

- Resilience of distinguishability of time series, compare periodic/stochastic.

- Computational complexity at certain (**quantum-mimics**) special-purpose operations.

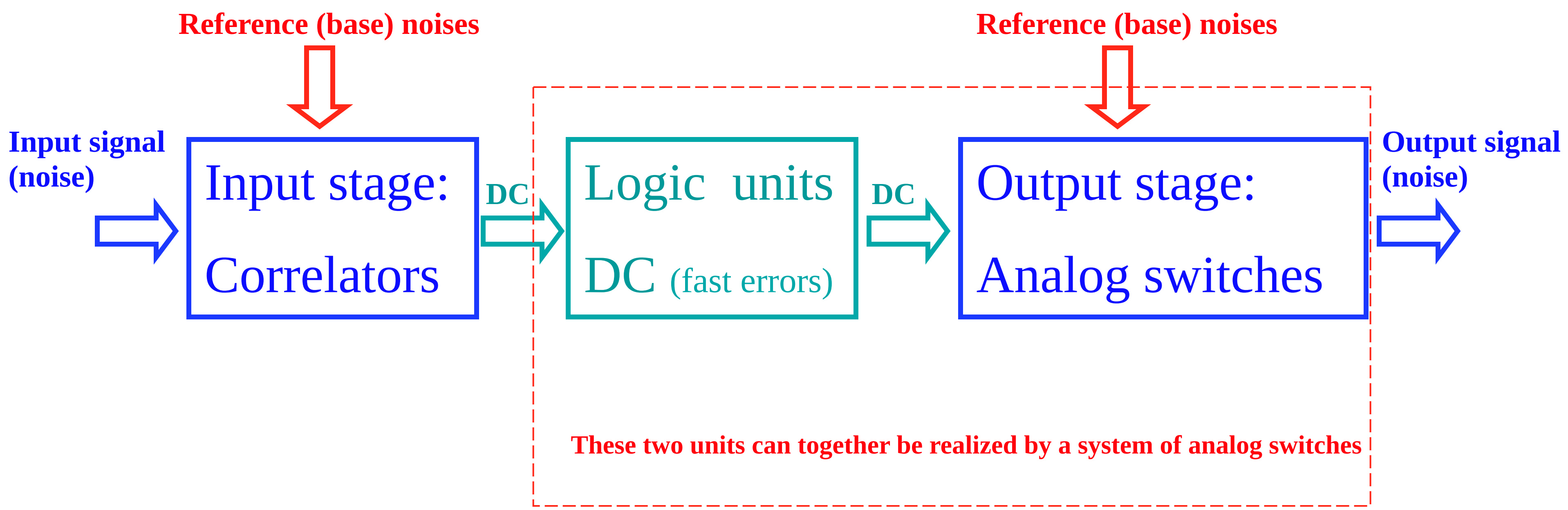
Example - 1 for entropy generation:

Correlator-based *noise-based logic*

Basic structure of correlator-based noise-based logic with continuum noises:

Theoretically much less power dissipation.
But that needs special devices (may not exist yet).
Slower: longer time.

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



Note: analog circuitry but *digital accuracy* due to the threshold operation in the DC part!

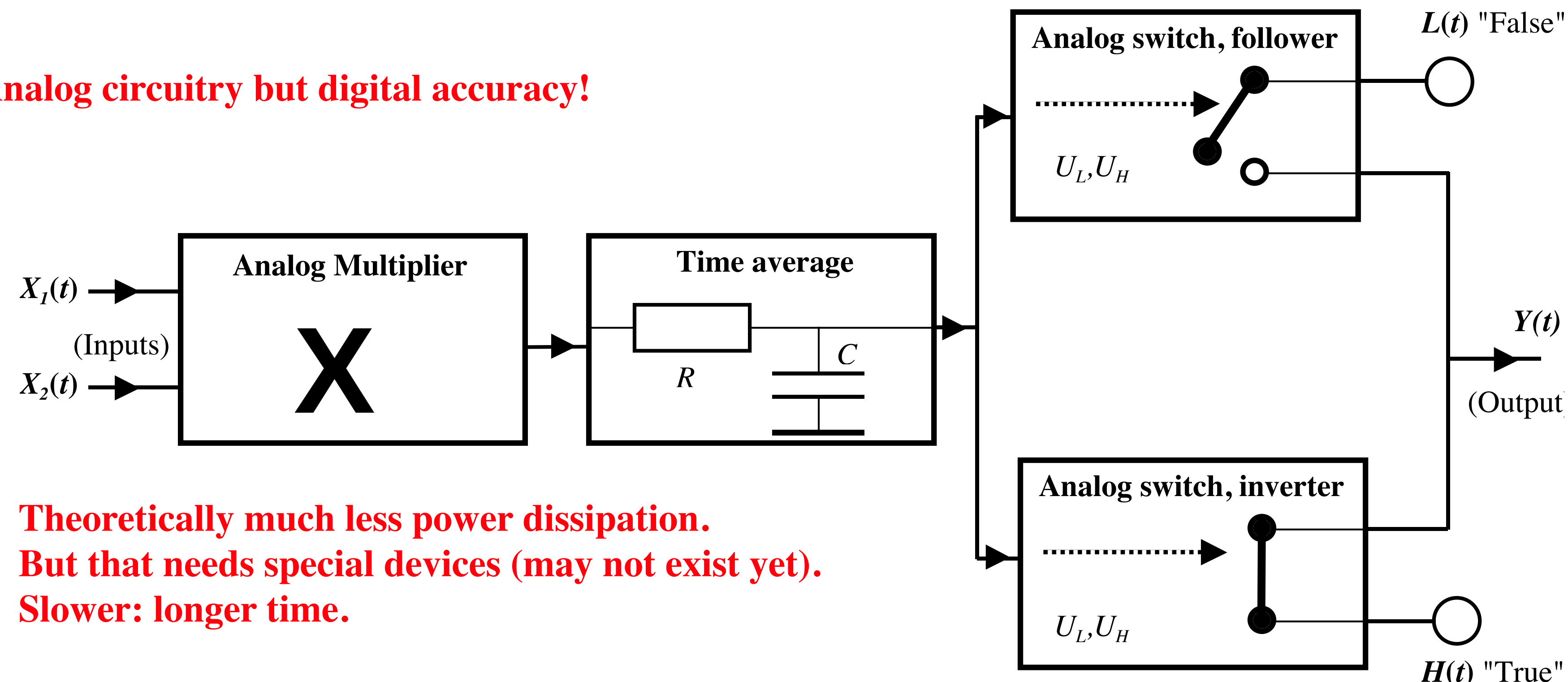
Example: XOR gate comparing two logic vectors in a space of arbitrary dimensions (binary, multi-value, etc), with binary output giving "True" value only when the two input vectors are orthogonal.

Even though the equation contains four multiplications, two saturation nonlinearities, one inverter, and two time averaging, the hardware realization is much simpler. It requires only one multiplier, one averaging unit and two analog switches. Realizations of the other gates also turns out to me simpler than their mathematical equations.

LK, *Physics Letters A* **373** (2009) 911-918

$$Y(t) = \underline{\overline{\overset{\otimes}{\langle X_1(t)X_2(t)\rangle}}}\, H(t) + \underline{\overline{\langle X_1(t)X_2(t)\rangle}}\, L(t)$$

Analog circuitry but digital accuracy!



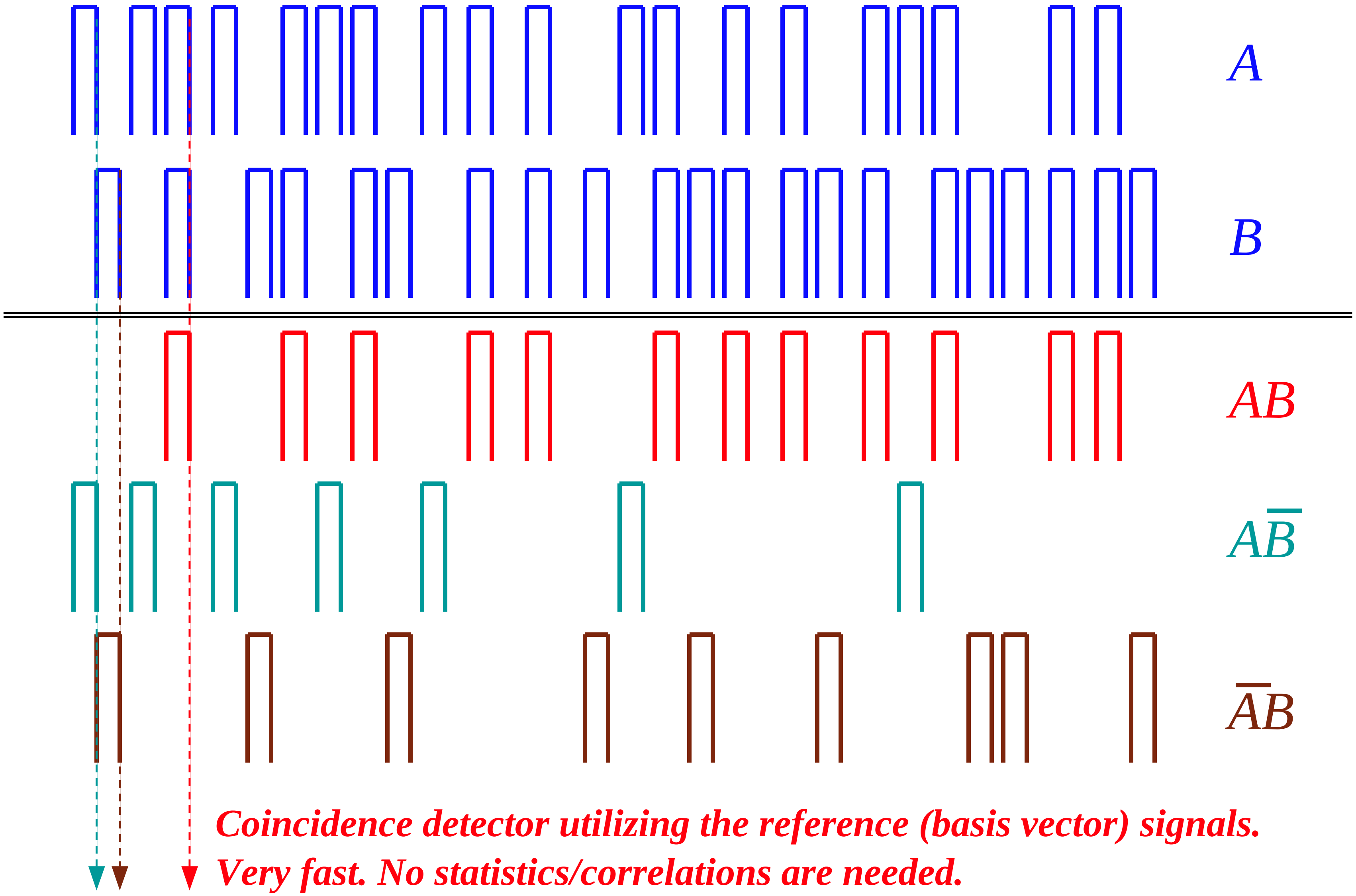
Theoretically much less power dissipation.
But that needs special devices (may not exist yet).
Slower: longer time.

The real potential would be due to multivalued aspects.

Example - 2 for resilience:

Brain: Random unipolar spike train based ***noise-based logic***

Brain signal scheme utilizing stochastic neural spikes, their superpositions and coincidence detection

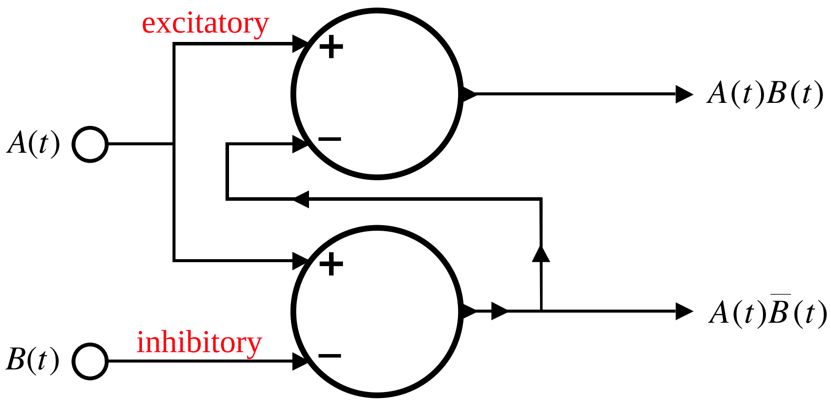


Coincidence detector utilizing the reference (basis vector) signals.
Very fast. No statistics/correlations are needed.

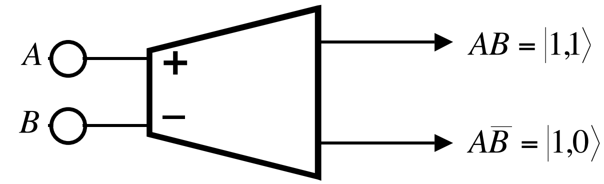
S.M. Bezrukov, L.B. Kish, *Physics Letters A* **373** (2009) 2338-2342

Neural circuitry utilizing coincidences of neural spikes.

The basic building element orthon (left) and its symbol (right).



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



ELSEVIER

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 firs
afferent types. First-spike tim
directional tuning curve, simil
with firing rates. However, fo
(FA-I and SA-I), the directio
first-spike latency did not co
with firing rates (derived
interval). Spike time and m
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

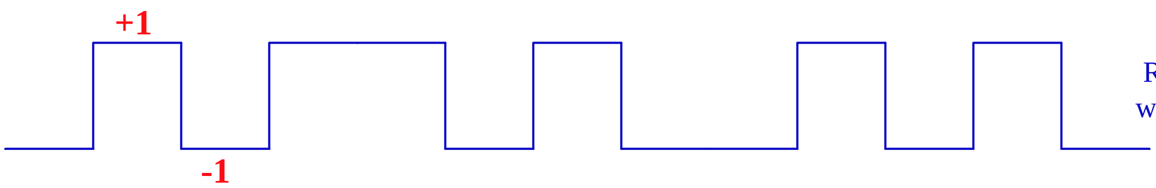
Neural Computation **17, 859–879** (2005)

Example - 3 for computational complexity:

Quantum mimic:

Hyperspace-based *instantaneous noise-based logic*

Instantaneous NBL. Example: Random Telegraph Waves. Their products: hyperspace



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

When the binary values of a bit are represented by waves V_0 and V_1

then the **NOT operator is multiplication by $V_0 * V_1$**

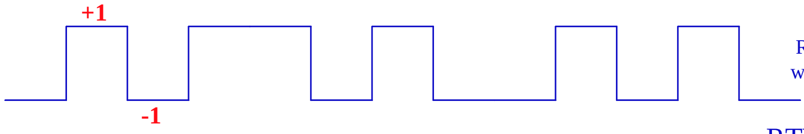
proof: $(V_0*V_1)*V_1=V_0$ $(V_0*V_1)*V_0=V_1$

Application example: string (-difference) verification **83 time steps for less than 10^{-25} error probability**

L.B. Kish, S. Khatri, T. Horvath, "Computation using Noise-based Logic: Efficient String Verification over a Slow Communication Channel", Eur. J. Phys. B 79 (2011) 85-90

Arbitrary *N*-long bit strings can be represented by 2*N* independent waves;
2 waves for each bit, to represent its 2 possible values
The actual string is represented by the product of the *N* waves that correspond to the bit values, for example:

$$\begin{matrix} 1 & & 0 & & 1 & & 1 & & 0 & & 1 \\ V_1^1 & * & V_2^0 & * & V_3^1 & * & V_4^1 & * & V_5^0 & * & V_6^1 \end{matrix}$$



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

$(V_0 * V_1) * V_1 = V_0$

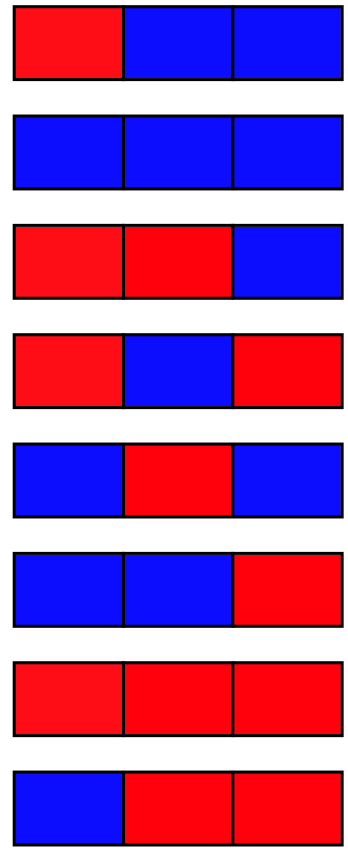
$(V_0 * V_1) * V_0 = V_1$

Example-2: Large, parallel operations in hyperspace

The second noise-bit in the superposition of 2^N binary numbers is inverted by an $O(N^0)$ hardware complexity class operation !

$$\left(V_2^0 * V_2^1\right) *$$

Single wire



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

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

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

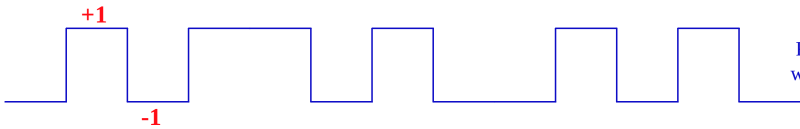
$V_1^1 V_2^0 V_3^1 = |1,0,1\rangle$

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

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

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

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



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

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

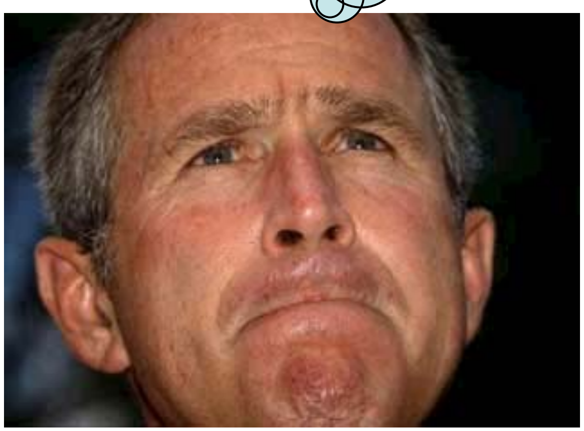
all orthogonal

$(V_0 * V_1) * V_1 = V_0$

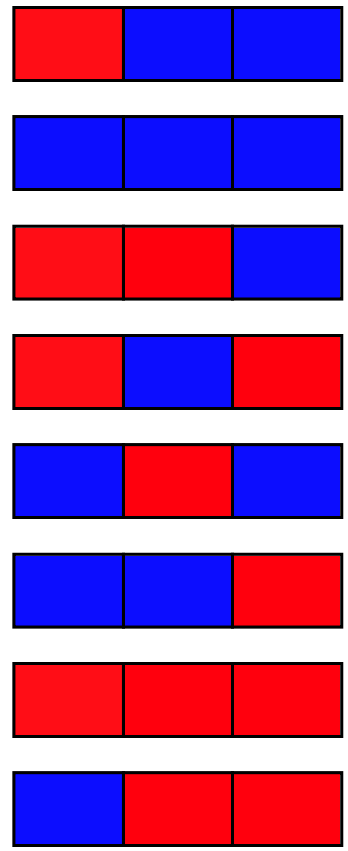
$(V_0 * V_1) * V_0 = V_1$

Example-2: Large, parallel operations in hyperspace

Can be done with sinusoidal signals, too! Isn't that better? Then a Fourier-series analysis over the base period would serve with the full result !



Single wire



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

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

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

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

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

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

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

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

The signal system with sinusoidals:

Linear vs Exponential harmonic (sinusoidal) bases:

$$L_r(t) = e^{j2\pi(2r-1)f_0 t}$$

$$H_r(t) = e^{j2\pi 2r f_0 t}$$

$$L_r(t) = e^{j2\pi 2^{2r-2} f_0 t}$$

$$H_r(t) = e^{j2\pi 2^{2r-1} f_0 t}$$

Time complexity: f_{max}/f_{min}

Bit	Logic Value	Frequency	
		Linear Representation	Exponential Representation
1st	L_1	f_0	f_0
	H_1	$2f_0$	$2f_0$
2nd	L_2	$3f_0$	$4f_0$
	H_2	$4f_0$	$8f_0$
...	...	...	...
Nth	L_N	$(2N\text{-}1)f_0$	$2^{2N\text{-}2}f_0$
	H_N	$2Nf_0$	$2^{2N\text{-}1}f_0$
		Degenerate example: $L_1H_2=H_1L_2$	***OK***

Hyperspace (product) vector, $\prod_{r=1}^{N} X_r$ **time complexity:** $O(N^2)$ $O(2^{2N})$

Conclusions (why noise)

- Orthogonal noises are a freely available logic signal system (e.g. N resistors).

- In the brain logic scheme noise provides extraordinary resilience compared to periodic spikes.

- In (quantum-mimic) setting up the instantaneous hyperspace a sinusoidal hyperspace requires $O(2^{2N})$ time complexity while the RTW-based scheme $O(1)$
- The FFT analysis of the sinusoidal hyperspace vector requires $O(2^{2N})$ time complexity while that of the RTW based noise-based logic will require an $O(N)$ time complexity.

- And a lot of open questions, including:

- Tamas Horvath (Fraunhofer, IAIS, Germany): "*The connection between the expressive power of NBL and that of probabilistic Turing machines is an interesting open question for further research*."

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

Noise-Based Logic: Why Noise?

He Wen[1,2] and Laszlo B. Kish[1]

[1]*Department of Electrical and Computer Engineering, Texas A&M University, College Station*

[2]*Hunan University, College of Electrical and Information Engineering, Changsha, 410082, China*

Although noise-based logic shows potential advantages of reduced power dissipation and the ability of large parallel operations with low hardware and time complexity the question still persist: is randomness really needed out of orthogonality? In this talk after introducing noise-based logic we address this question.

A journal paper about this issue is coming out in the December issue of Fluctuation and Noise Letters
http://www.ece.tamu.edu/~noise/research_files/noise_based_logic.htm

Presented at: ICCAD 2012, SPECIAL SESSION: ***Computing in the Random Noise: The Bad, the Good, and the Amazing Grace***
November 5, 2012, San Jose, CA.