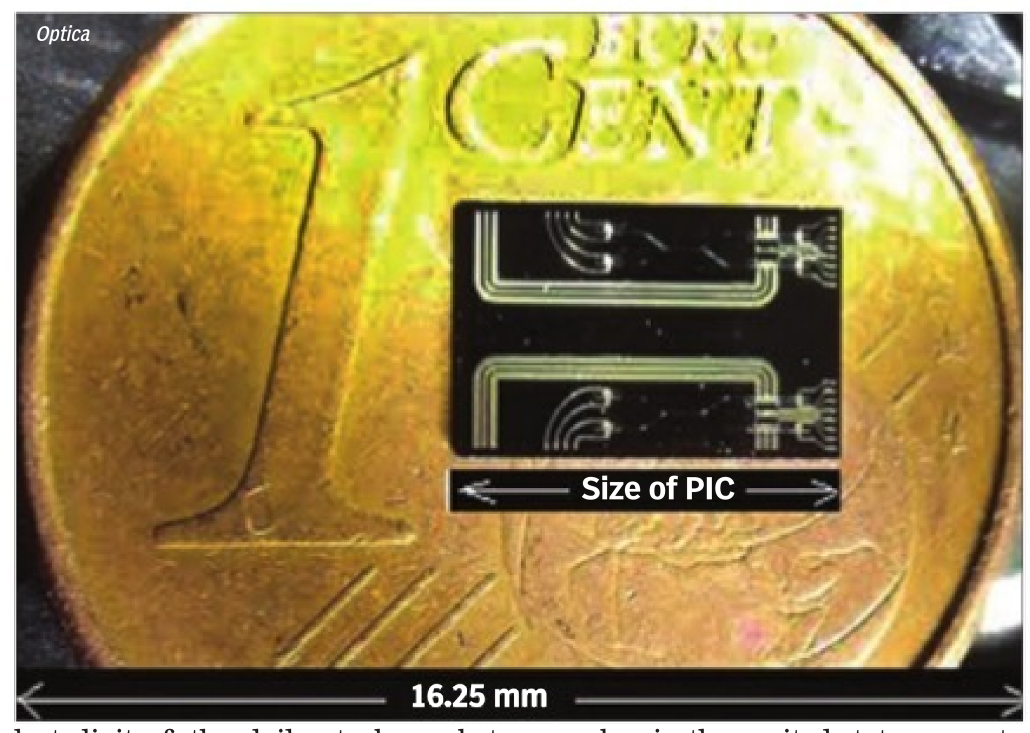
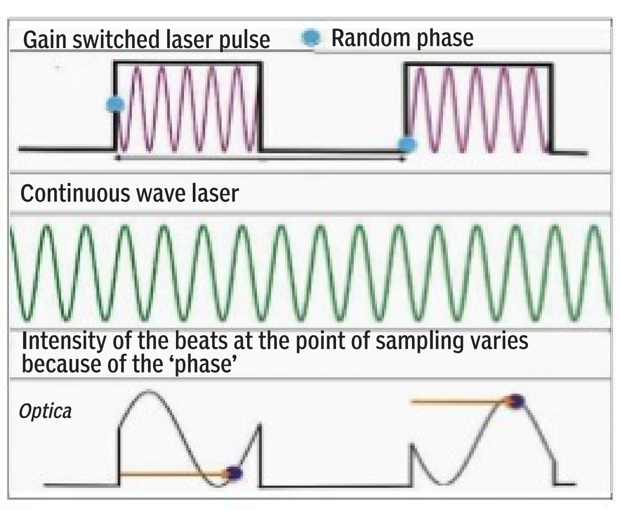
Quantum chip keeps you guessing

MINIATURE DEVICES CAN NOW CREATE REAL RANDOM NUMBERS, WRITES S ANANTHANARAYANAN

Random numbers have become important in daily life, given how they are at the heart of e-commerce and secure communications and also form the basis of statistical methods of solving problems in engineering and economics. And yet, truly random numbers are difficult to generate. A series of seemingly random numbers can still show patterns, and this can lead to frauds in e-commerce or errors in computations. Carlos Abellani, Waldimar Amaya, David Domenech, Pascual Munoz, Jose Capmany, Stefano Longhi, Morgan W Mitchell and Valerio Pruneri from the Institutes of Science and Technology and the Institute of Research and Advanced Studies at Barcelona, Polytechnic University and the firm, VLC Photonica, at Valencia and the Institute of Photonics and Nanotechnology at Milan, describe in the Optical Society's journal, *Optica*, a method of using quantum effects to generate truly random numbers with the help of a miniature device that can be embedded in a mobile phone.The operative quality of random numbers is that those in a series cannot be predicted from the preceding ones, nor even any of the digits that appear in them.

Once a random number has been exchanged by a pair of correspondents, they can base a code on this number and keep their exchanges confidential. Devices like computers, which handle e-commerce transactions, thus routinely generate hundreds of large random numbers. The numbers generated by a complex formula are based on a "seed" number to get started, and do pass many statistical tests of randomness. The numbers, however, are not truly random and if a third party should guess the "seed" that was used, he/she could work out the numbers and impersonate others in transactions.Real random numbers are created not by a formula but by physical processes, like the last digits of the number of grains in a handful of sand, the throw of honest dice or even the last digit of the daily stock market index. The trouble with these processes, however, is that creating a large random number with their help is time consuming and cannot serve the thousands of transactions every second in real applications (the stock market index is out of the question as it is not even secret!). The alternative has, hence, been to use quantum mechanical processes, which is the way that matter behaves at very small dimensions, to create random numbers. These processes are truly random and generating random numbers based on them, using light waves and electronics, can be very fast.





Quantum process A typical quantum process is that of a photon, or a particle of light, choosing one of two alternate paths. When photons in a beam traverse the paths without being observed, they behave like waves and appear to take both paths at the same time. When the photons are observed, or detected, however, they act like particles and take one or the other path, but randomly. The choice, which represents "0" or "1" of binary numbers, is truly unpredictable and a source of single photons and detectors can generate real random numbers, but not rapidly. A faster method is to make use of the decay of atoms in slightly long-lived excited states that which form the basis of lasers.

The atoms in a laser have this property that when they are excited to a higher state they pause a bit, just a very small fraction of a second, before they de-excite, which is with the emission of a photon. If a collection of such atoms is rapidly excited, the number in the excited state grows to be more than in the ground state.

The photon emitted by the chance decay of any atom is then likely to strike another excited atom, which would result in two photons, which are in the same phase of oscillation, being emitted together. These two photons could then stimulate further emission, and so on. If the process of creating excited atoms is continued, the process of decay progresses as a cascade, which becomes the continuous laser beam, of a "continuous wave" laser.

Another form of the laser is where the atoms are excited by repeated flashes of light, each flash resulting in a pulse of laser light. In this kind of laser, which is called a "gain switched" laser, each flash creates a population of excited atoms and the first chance decay of any of them becomes the "seed" for a cascade that creates each pulse of laser light. As this "seeding" photon arises at a random time, the phase of vibration of each pulse of laser light is random too.

Measuring the phase of the laser pulses would then be a source of real random numbers, and these would arise very fast, and could be processed equally fast by optics and electronics.

Miniaturisation
The materials used in these lasers are semiconductors, the stuff of transistors and electronic chips, and the act of "excitation" is knocking an electron out of a large number of the atoms in the semiconductor crystals. Laser light is then emitted when a free electron falls back into the space left by an electron knocked out, to emit the first photon, followed by the cascade. The trouble with even this arrangement, however, is that the components are separate and the assembly is large. In the advance reported in the journal *Optica*, however, the "gain switched" laser and another, "continuous wave" laser, which is to help detect the changes in phase of the pulses from the first laser, are built on a single chip of a special material, just over half a centimetre across. The technology, called a Photonic Integrated Circuit, combines electronics and optics and enables the components for generating optical signals as well as processing the signals to extract the phase of one of them, to be built into the same device.

The method used to extract the phase information is the same as is used in radio technology to extract data or sound information from the radio signal that comes to the receiver. The signals received at different frequencies of radio waves from different stations are brought down to a single frequency by combining the incoming signal with other frequencies generated at the receiver. The effect of combining two frequencies is to generate two new signals, of a fluctuation of the amplitude of the waves, at the sum and the difference of the two frequencies that we started with.

This is the effect used for tuning a guitar string, for instance, where the guitarist listens to the frequency of the rise and fall of the sound, which are called "beats", as the string is plucked and a standard tuning fork is sounded at the same time.In the same way, the two lasers on the PIC chip interfere and cause a rise and fall of amplitude of light in the pulses that emerge. As each pulse from the gain switched laser is "out of step" to a different extent because of the random phase, there is a corresponding variation in the nature of the "beats" and this can be processed to yield random numbers, one corresponding to each pulse. The instrumentation to detect and process the "beats" is also built into the PIC chip.The frequency of the pulses and, hence, the number of random digits can be in billions every second. Very large random numbers can therefore be created very fast.

The arrangement being on an electronic chip also allows it to be easily integrated with devices like computers and even cell phones.

This makes it possible to have very secure communications in a variety of situations and also a portable platform for other uses of random numbers.

THE WRITER CAN BE CONTACTED AT
RESPONSE@SIMPLESCIENCE.IN

Hacking the random number generator

When we log into the server of a secure service, like a bank, the server assigns us a unique code number to identify genuine requests or commands that we send. The code number is complex and random, like "335C66huYY94dw9f6…" so that it is difficult for others to guess the number and impersonate us.

The number is generated using a computer programme that uses some number as "seed" and generates a series of numbers that are largely unrelated and can be considered random for most purposes. The programme, however, will generate the same series every time it starts with the same "seed". Hence, to be as unpredictable as possible, the programme tries to take a random and secret number as "seed" each time it starts. In one case, the seed was taken as the time, correct to the millisecond, at which the server was switched on.

A hacker who has the random number generating programme uses some method to make the server crash. When this happens, it restarts in less than a minute and this gives the hacker a handle on the new "seed", as the time somewhere within that minute, or the 60,000 possible "seeds". The hacker now runs a programme to see which of these 60,000 "seeds" produces the random number that he/she has been assigned. This gives the hacker the "seed" being used and, hence, access to all the random numbers in use!

BETWEEN THE LAYERS

TAPAN KUMAR MAITRA EXPLAINS THE WAY PROTEINS ARE IDENTIFIED IN A MEMBRANE AND CHRONICLES THEIR TYPES

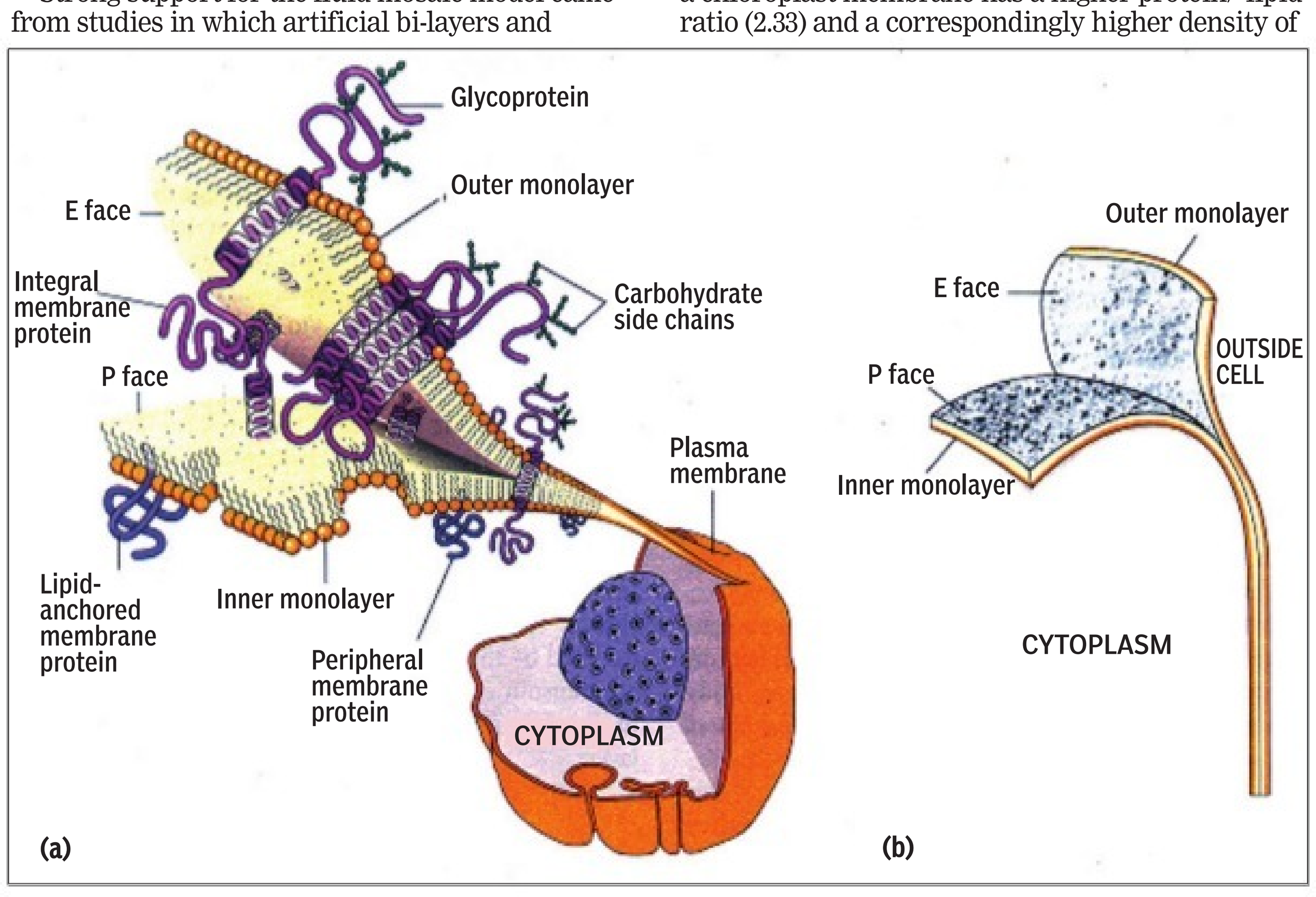
Having looked in some detail at the "fluid" aspect of the fluid mosaic model, let's address the "mosaic" part. That may include lipid rafts and other lipid domains, but the main components of the membrane mosaic are the many membrane proteins, as initially envisioned by Singer and Nicholson. Here's a look, first, at the confirming evidence that microscopists provided for the membrane as a mosaic of proteins and then, the major classes of membrane proteins.

Strong support for the fluid mosaic model came from studies in which artificial bi-layers and natural membranes were prepared for electron microscopy by freeze-fracturing. In this technique, a lipid bi-layer or a membrane (or a cell containing membranes) is frozen quickly and then subjected to a sharp blow from a diamond knife. The resulting fracture often follows the plane between the two layers of membrane lipid, because the non-polar interior of the bi-layer is the path of least resistance through the frozen specimen. As a result, the bi-layer is split into its inner and outer monolayers, revealing the inner surface of each.

Electron micrographs of membranes prepared in this way provide striking evidence that proteins are actually suspended within membranes. Whenever a fracture plane splits the membrane into its two layers, particles having the size and shape of globular proteins can be seen adhering to one or the other of the inner membrane surfaces, called the E (for exoplasmic) and P (for protoplasmic) faces.

Moreover, the abundance of such particles correlates well with the known protein content of the particular membrane under investigation. The electron micrographs illustrate this well – the erythrocyte plasma membrane has a rather low protein/lipid ratio and a rather low density of particles when subjected to freeze-fracture, whereas a chloroplast membrane has a higher protein/ lipid ratio (2.33) and a correspondingly higher density of intra-membranous particles, especially on the inner lipid layer.

Confirmation that the particles seen in this way really are proteins came from work by David Deamer and Daniel Branton, who used the freeze-fracture technique to examine artificial bi-layers with and without added protein. Bi-layers formed from pure phospholipids showed no evidence of particles on their interior surfaces. When proteins were added to the artificial bi-layers, however, particles similar to those seen in natural membranes were readily visible.



Sketch (a) of a freeze-fractured membrane in which the fracture plane has passed through the hydrophobic interior of the membrane, revealing the inner surfaces of the two monolayers. Hydrophobic segments of proteins are shown in light purple, hydrophilic segments in dark purple. Integral membrane proteins that remain with the outer monolayer are seen on the E (exoplasmic) face, whereas those that remain with the inner monolayer are seen on the P (protoplasmic) face; and sketch (b) of a freeze-fractured membrane with electron micrographs of the E and P faces from the plasma membrane of a mouse kidney tubule cell superimposed on the drawing.

THE WRITER IS ASSOCIATE PROFESSOR, HEAD, DEPARTMENT OF BOTANY, ANANDA MOHAN COLLEGE, KOLKATA, AND ALSO FELLOW, BOTANICAL SOCIETY OF BENGAL, AND CAN BE CONTACTED AT
tapanmaitra59@yahoo.co.in

Cosmic 'spaghettification'

SARAH KAPLAN REPORTS ON HOW SCIENTISTS CAUGHT BLACK HOLES SWALLOWING STARS – AND BURPING ENERGY BACK UP

For the first time, astronomers have clearly observed at infrared wavelengths what happens after a black hole eats a star: it burps back up a brilliant flare of light that echoes through space. Two studies published this week — one by scientists at thge National Aeronautics and Space Administration, the other by researchers at the University of Science and Technology of China — describe these "tidal disruption flares" using data from Nasa's Wide-field Infrared Survey Explorer, a space telescope that has photographed the entire sky in infrared light.

"This is the first time we have clearly seen the infrared light echoes from multiple tidal disruption events," Sjoert van Velzen, a postdoctoral fellow at Johns Hopkins University and lead author of the Nasa study, said in a statement. His study caught three black holes in the act of star swallowing; researchers in China documented a fourth.

The technical term for these celestial phenomena is "stellar tidal disruption events". When a star gets too close to a black hole's event horizon (the "point of no return", at which not even light can escape), it gets stretched and torn apart by variations in the black hole's gravitational pull. Scientists call the process "spaghettification" for the way that it elongates everything that has the misfortune of enduring it.

As it devours the star, the black hole emits an enormous amount of energy, including ultraviolet and X-ray light, that destroys everything in its immediate neighbourhood.

"It's as though the black hole has cleaned its room by throwing flames," van Velzen said.

But beyond the reach of the most intense radiation, a patchy web of dust swirls. At this distance — a few trillion miles from the black hole — the dust particles can absorb the light released during the death of the star without being destroyed by it. The particles then re-emit the light at longer, infrared wavelengths. Scientists recently detected several X-ray emissions from black holes that seemed to be signatures of this phenomenon, but the new studies are the first to catch the event in infrared.

The Wise telescope, which is attuned to infrared radiation, can capture these "echoes" of the star's destruction; by measuring the delay between the original light flare and the subsequent echoes, scientists on the ground can figure out how much energy was released as the star got consumed.

The studies also let astronomers figure out the exact location of the dust web and understand some of its most basic characteristics.

This material isn't only the outskirts of black hole — it represents the nucleus of the galaxy for which the black hole forms the centre. That makes observations of tidal disruption flares doubly interesting: They can help scientists understand not just the dark, dense mysteries of black holes, but also the bright, swirling places that surround them.

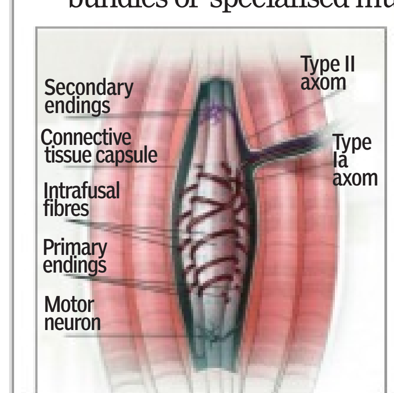
WASHINGTON POST

An illustration of a supermassive black hole feasting on its surroundings. The central hole is hidden from view by gas and dust.

PLUS POINTS

Muscle spindles

Scattered throughout skeletal muscle, the muscle spindles are composed of connective tissue capsules containing bundles of specialised muscle fibres called intrafusal fibres. Wrapped around the middle of these fibres are the spiral terminals of a large sensory neuron, the type Ia axon. To one side of these spiral terminals, collectively called the primary endings, are the secondary endings, the terminals of a smaller sensory neuron, the type II axon. Both types of nerve endings serve as stretch sensors that send feedback about muscle contraction and length changes to the brain.

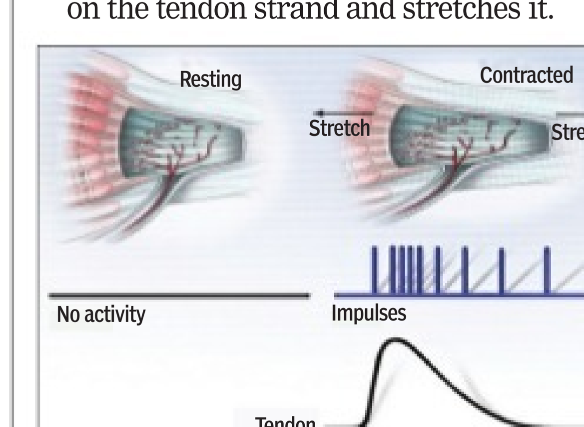


At rest, muscle spindles generate a trickle of nerve impulses. Stretching the muscle raises the number of nerve impulses from both the spindle's primary and secondary endings. Impulses in the primary endings signal both the rate of change in muscle length and the length change itself. Primary endings are therefore both movement and position sensors. This sensitivity to the rate of the stretch makes the primary endings responsive to muscle vibration. The secondary endings respond only to the length change, making them position sensors; they are vibration-insensitive.

Tendon organs

Tendons attach muscles to bones. At the junction between muscle fibres and tendons lie the tendon organs, small bundles of tendon strands enclosed within a connective tissue capsule, similar to that in muscle spindles. The axon of a large sensory neuron, the type Ib axon, penetrates the capsule and terminates on the collagen strands. Each strand is attached to a single muscle fibre. In a typical tendon organ there are 10-20 innervated tendon strands with attached muscle fibres.

Like muscle spindles, tendon organs are stretch sensors. They are particularly sensitive to muscle contraction. In the resting state, tendon organs are silent. When the muscle fibre contracts, it pulls on the tendon strand and stretches it.



This stretches the nerve ending of the Ib axon to generate nerve impulses. During a contraction, as muscle tension rises and then falls, the pattern of impulses increases and then decreases in frequency and number.

THE SCIENTIST

Skilled tool-users

A sacred crow driven to extinction on its native Hawaii has been found to be able to make and use highly effective tools in a discovery which could help conservationists reintroduce the bird into the wild later this year. According to traditional Hawaiian beliefs, the 'alala bird is a spirit guide that takes souls to a "Leaping Place" on their journey to the afterlife. Without the help of such a guide, souls may be forced to "drift forever through a twilight of ghosts".

The last 'alala disappeared from the wild in 2002, amid a widespread decline of native Hawaiian flora and fauna linked to the arrival of invasive species brought by humans. Its chicks were "very vulnerable" to rats and the adults were killed by cats, dogs and mongooses, according to the US Fish & Wildlife Service.

That left a total population of about 100 individuals in captivity. But conservationists plan to release a number of the birds back into native forest later this year in the hope that the species can re-establish itself. Ahead of the reintroduction programme, scientists have discovered the Hawaiian crow, as it is also known, has a genetic predisposition to use tools — usually long sticks designed to winkle out insects from holes in dead wood. Only a handful of bird species around the world — including the New Caledonian crow – have been found to display similar abilities.

Writing in the journal *Nature*, the researchers said, "The 'alala is a highly dextrous tool-user. During experimental trials, birds routinely selected tools of appropriate dimensions, replaced unsuitable tools, and transported non-supplied sticks to the log. Tool modification occurred frequently and we even observed tools being manufactured from plant materials."

To test whether genetics played a role in this behaviour, the scientists raised seven 'alala so that they were not able to observe adult tool-users. "All (seven) birds eventually used sticks and other objects in an attempt to reach hidden food during probe trials, and four were successful; a fifth subject later used tools successfully on the log task," *Nature* reported.

THE INDEPENDENT