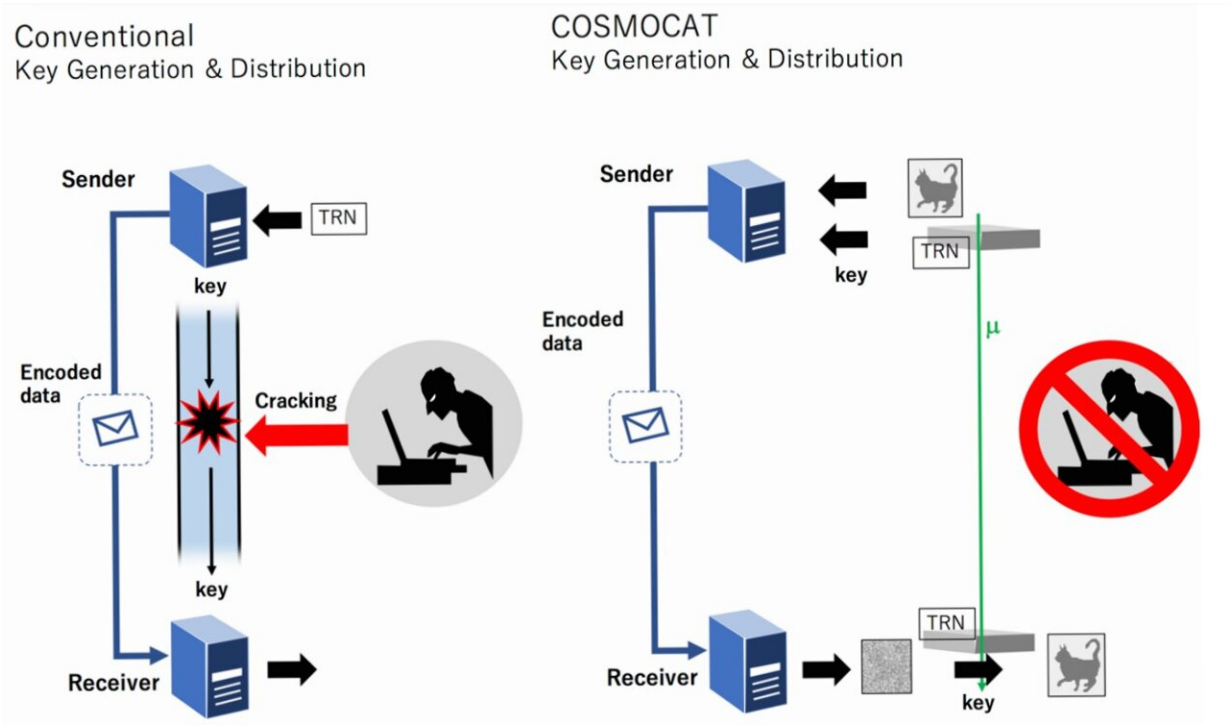
# Using cosmic rays to generate and distribute random numbers and boost security for local devices and networks

January 12 2023




When both sender and receiver have identical random numbers, they can share encrypted data without the need to share a key to decode it. This prevents so-called man-in-the-middle attacks. With COSMOCAT, muons (μ) arriving at the sender and receiver at the same time provide the source of the random number. Provided the devices are synchronized, the receiver can know which muon signal relates to which incoming message and can decode it accordingly. Credit: ©2022 Hiroyuki Tanaka

State-of-the-art methods of information security are likely to be compromised by emerging technologies such as quantum computers. One of the reasons they are vulnerable is that both encrypted messages and the keys to decrypt them must be sent from sender to receiver.

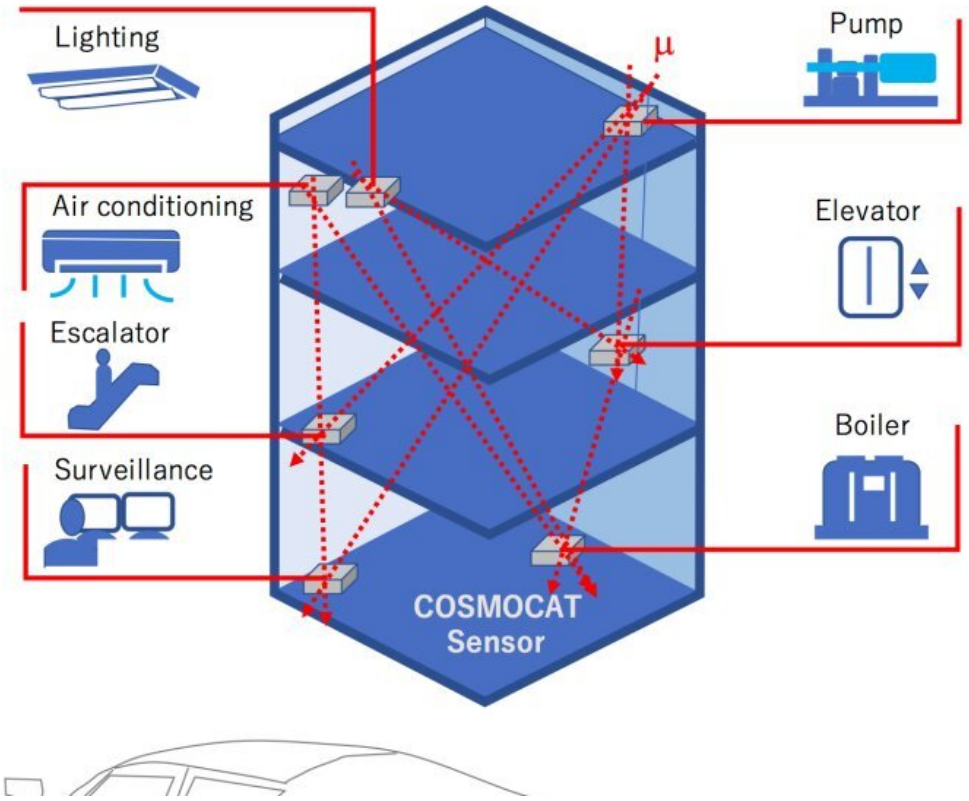
A new method—called COSMOCAT—is proposed and demonstrated, which removes the need to send a decryption key since cosmic rays transport it for us, meaning that even if messages are intercepted, they could not be read using any theorized approach. COSMOCAT could be useful in localized various bandwidth applications, as there are limitations to the effective distance between sender and receiver.

In the field of information communication technology, there is a perpetual arms race to find ever more secure ways to transfer data, and ever more sophisticated ways to break them. Even the first modern computers were essentially code-breaking machines used by the U.S. and European Allies during World War II. And this race is about to enter a new regime with the advent of quantum computers, capable of breaking current forms of security with ease. Even security methods which use quantum computers themselves might be susceptible to other quantum attacks.

"Basically, the problem with our current security paradigm is that it relies on encrypted information and keys to decrypt it both being sent along a network from sender to receiver," said Professor Hiroyuki Tanaka from Muographix at the University of Tokyo.

"Regardless of the way messages are encrypted, in theory someone eavesdropping could use the keys to decode the secure messages eventually. Quantum computers just make this process faster. If we dispense with this idea of sharing keys and could instead find some way of using unpredictable random numbers to encrypt information, then it should lead to a system immune to interception. And I happen to work

often with a source capable of generating truly random unpredictable numbers: cosmic rays from outer space."




Some use cases for COSMOCAT. As the distance is limited due to the nature of the muon shower arriving at the ground, COSMOCAT is best suited for networks within small areas such as buildings. Offices, data centers and buildings that make use of smart devices, and even electric-car charging stations, are some possible application areas. Credit: ©2022 Hiroyuki Tanaka

Various random number generators have been tried over time, but the problem is how to share these random numbers while avoiding interception. Cosmic rays may hold the answer, as one of their byproducts, muons, are statistically random in their arrival times at the

ground. Muons also travel close to the speed of light and penetrate solid matter easily.

This means that as long as we know the distance between the sender's detector and the receiver's detector, the time required for muons to travel from the sender to the receiver can be precisely calculated. And providing that a pair of devices are sufficiently synchronized, the muons' arrival time could serve as a secret key for both encoding and decoding a packet of data. But this key never has to leave the sender's device, as the receiving machine should automatically have it as well. This would plug the security hole presented by sending shared keys.

"I call the system Cosmic Coding and Transfer, or COSMOCAT," said Tanaka. "It could be used alongside or in place of current wireless communications technologies such as Wi-Fi, Bluetooth, near-field communication (NFC), and more. And it can exceed speeds possible with current encrypted Bluetooth standards. However, the distance it can be used at is limited; hence, it's ideally kept to small local networks, for example, within a building. I believe COSMOCAT is ready to be adopted by commercial applications."

At present, the muon-detecting apparatus are relatively large and require more power than other local wireless communication components. But as technology improves and the size of this apparatus can be reduced, it might soon be possible to install COSMOCAT in high-security offices, data centers and other local area networks.

The work is published in the journal *iScience*.

**More information:** Hiroyuki K.M. Tanaka, Cosmic Coding and Transfer (COSMOCAT) for Ultra High Security Near-Field Communications, *iScience* (2023). DOI: 10.1016/j.isci.2022.105897