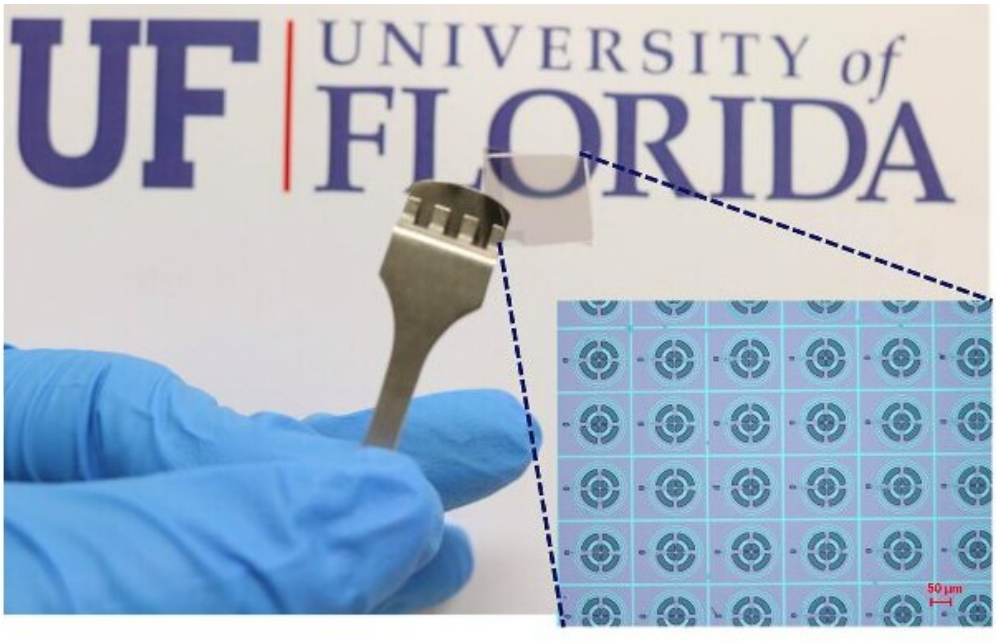
NEMS IDs: Secure nanoelectromechanical tags for identification and authentication

January 7 2021, by Ingrid Fadelli



A glass die having an array of NEMS tags integrated on it: the diel is hold in front of the logo to highlight the optical transparency of the NEMS tags.

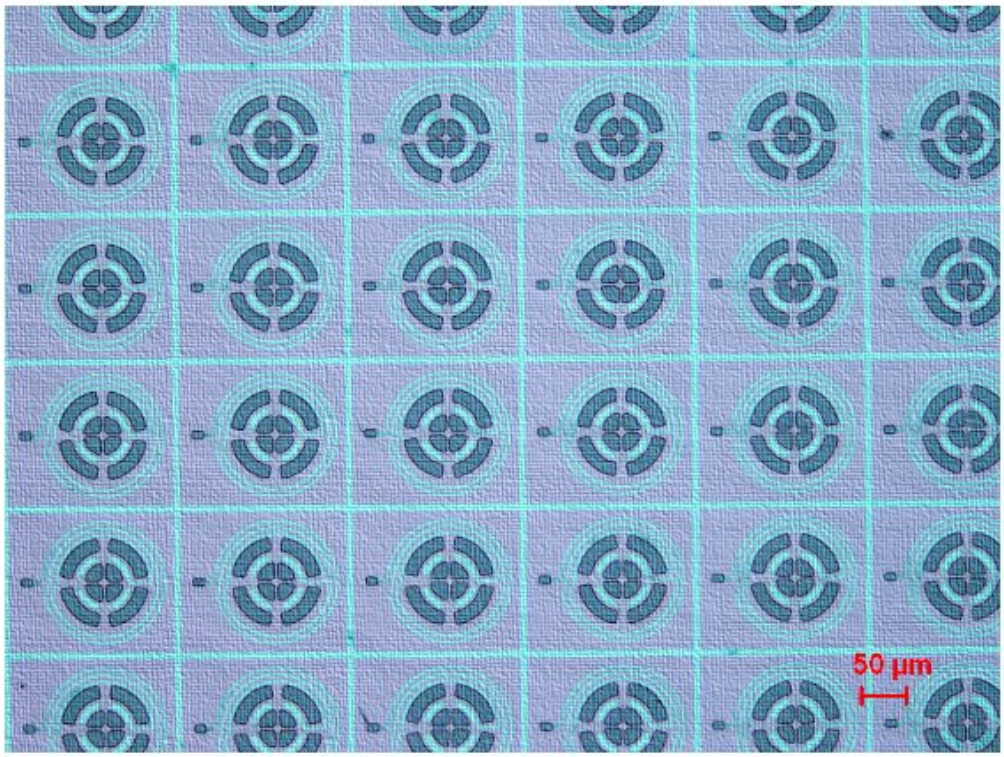
Credit: Rassay et al.

In recent years, hackers have become increasingly good at counterfeiting identification and authentication tags. This has led to an increase in cases of identity theft, fraud, security breaches and other concerning privacy or security related incidents.

Researchers at University of Florida have recently created NEMS IDs, a system that could reduce the probability of these attacks being successful. This system, presented in a paper published in *Nature Microsystems & Nanoengineering*, is based on the use of clandestine nanoelectromechanical tags that are far more resistant to physical tampering and cloning that most identification tags used today.

"The infectious effects of counterfeiting now extend far beyond economic aspects, and target social health and international security," Roozbeh Tabrizian, one of the researchers who carried out the study, told TechXplore. "Over the past few years, counterfeiting was clearly identified as a major promoter and sponsor of organized crime and terrorism, forced or child labor and identity theft or fraud. Hence, there is a critical need for identification and authentication technologies that enable traceability of genuine products and identify their fake counterparts."

Most identification systems used today, including those based on universal product code (UPC) barcodes, quick response (QR) codes and radio-frequency identification tags (RFID) have been quite successful in reducing the risk of counterfeit-based breaches or attacks. Unfortunately, however, all of these systems have significant limitations. For instance, most of these technologies are too large (i.e., easy to reproduce), need to be in the line of sight to be analyzed and can be easily stolen or recycled.



An array of wireless NEMS tags integrated on a single glass die.

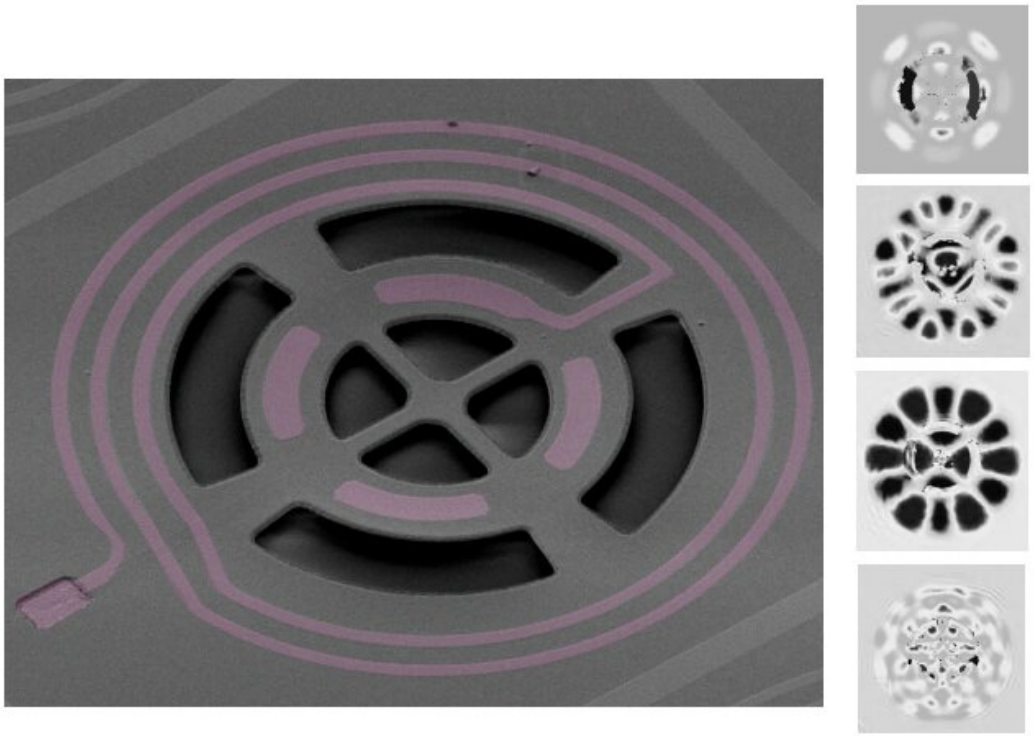
Credit: Rassay et al.

Researchers have also developed more sophisticated alternatives, such as nano-PUFs, DNA-based data storage schemes and optical ID labels, all of which can improve the security of tags by increasing the complexity of information storage mediums and the operation physics. Tampering with these systems or cloning them is thus far more challenging and expensive.

While many of these systems have been found to be more secure than basic identification approaches, they are difficult to implement on a

large scale and in a variety of contexts. In fact, nano-PUFs, DNA-based data storage schemes and optical ID labels generally need to be customized to meet the sizes and characteristics of specific goods or products. They are also very expensive to produce and require highly sophisticated read out systems.

"Our team's main goal was to develop an ID tag technology that simultaneously provides three substantial advantages: (a) the user interface remains simple, low-cost, and widely applicable to arbitrary hosts; (b) operation physics complex enough to avoid tampering; and (c) performance (i.e., entropy, reliability, robustness, etc.) better or at least on a par with available technologies," Tabrizian explained. "For this purpose, we came up with the Nano-Electro-Mechanical System Identification tags (NEMS IDs)."



(left) The wireless NEMS tag: a coil integrated around the NEMS enables wireless interrogation of the spectral signature through magnetic coupling. (right) the vibration pattern of the NEMS tag, captured using a digital holographic microscope.

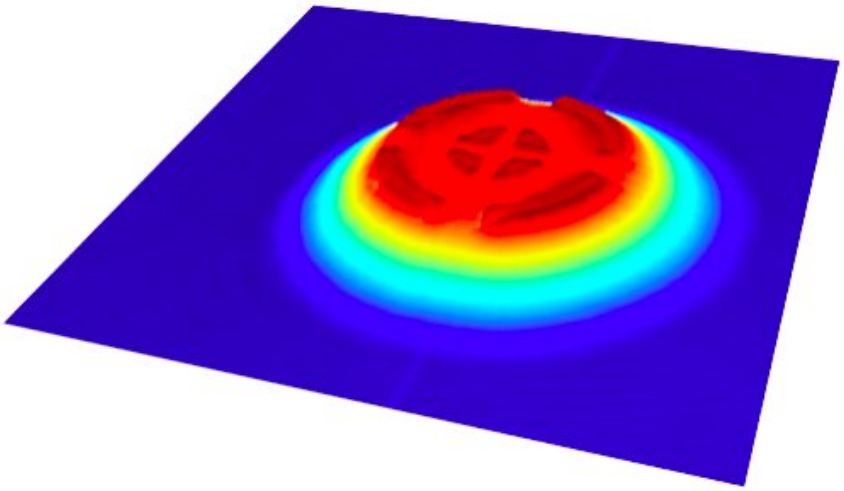
Credit: Rassay et al.

The identification tags developed by Tabrizian and his colleagues exploit the spectral signature of transparent and wireless NEMS, which is a tamper-proof and unclonable information storage medium with ultra-high entropy. These spectral signatures are translated into binary fingerprints by adaptive algorithms. The ID tags can be read out using simple wireless readout instruments, which are widely available.

"NEMS IDs can be created en masse via semiconductor batch manufacturing, which makes them very low cost," Tabrizian said. "In

addition, using the spectral signature, engineered to have several mechanical resonance peaks, not only enables information storage within an unseeable/indirect approach, but also enables low-power interrogation of the tag, thanks to the very high quality factor of the mechanical resonance modes."

The ID tags have advantageous structural characteristics, as they are extremely small and transparent. This means that they are almost impossible to see and locate, which greatly reduces the risk that they will be tampered with.

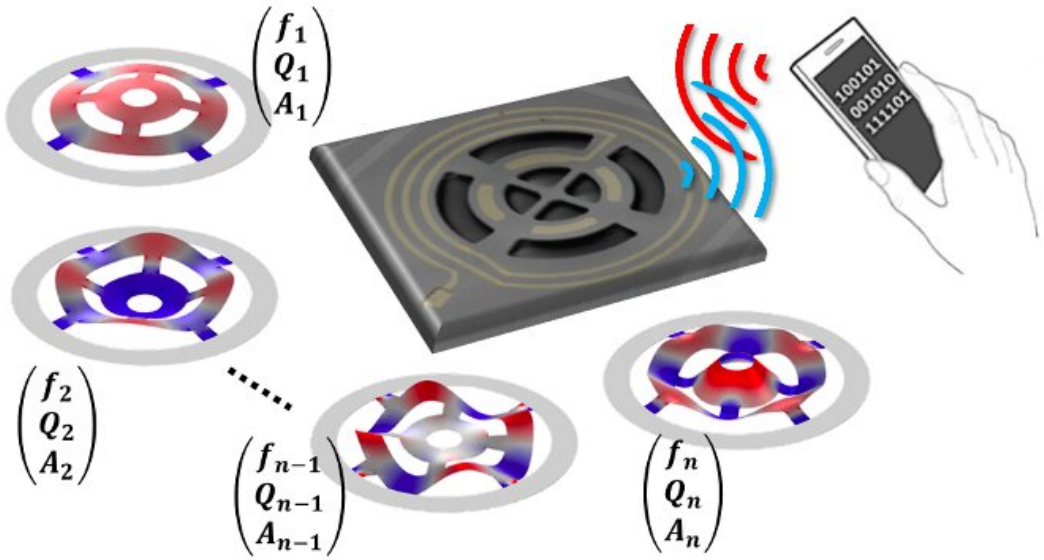


Topographic image of a NEMS tag integrated on a glass substrate, captured using a digital holographic microscope.

Credit: Rassay et al.

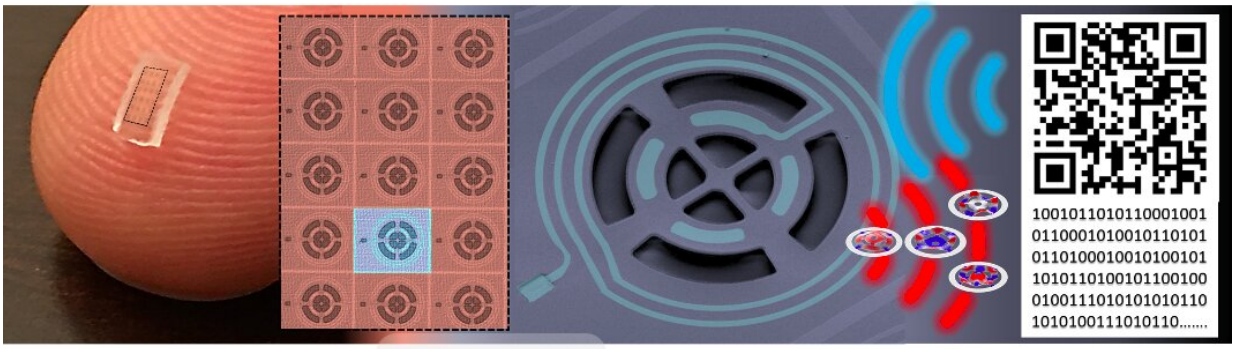
In initial tests, the NEMS ID system proved to be highly promising and reliable. Moreover, the fingerprints it derived were found to be consistent and easy to identify using common wireless read out tools.

"The demonstration of the potential of NEMS spectral signatures to serve as a high-density information carrier medium is very exciting," Tabrizian said. "This is conceptually similar to the very essence of material science: The phonon spectrum of the material (i.e., the spectral distribution of the collective atomic vibrations) is a unique fingerprint of the material and governs a wide range of its fundamental properties. Our system does something similar, as it stores information in the spectral signature (i.e., a finite set of mechanical vibration modes) of a nanostructure."



Conceptual demonstration of the wireless NEMS tag operation: Wireless interrogation of the device excites mechanical vibration modes with different frequency, quality factor and amplitude. The information of these vibration modes is then translated to a digital string and serve as the fingerprint.

Credit: Rassay et al.



(left) A die with an array of NEMS tags integrated on the surface. (right) Schematic demonstration of the mechanical vibration modes of the NEMS tag. The frequency of these modes are used, along with a translation procedure, to designate the binary sting to the NEMS tag.

Credit: Rassay et al.

In their recent paper, the researchers primarily discuss the use of NEMS IDs as fingerprints. However, in the future, the system they developed could also be adapted to act as a tamper-proof storage platform for rewritable data, which could turn out to be more secure than most existing storage technologies. Tabrizian and his colleagues are currently investigating possible attacks targeting the system they developed in order to identify ways to further enhance their security.

"On the application side of things, we now also aim to optimize NEMS IDs to enable their integration on popular host materials, such as different types of paper and plastic, and we are also exploring their use in edible and liquid products," Tabrizian said. "From a physics

perspective, on the other hand, we are investigating spectral configuration approaches, using material and device level engineering, to enable non-volatile information storage in NEMS IDs."

More information: Clandestine nanoelectromechanical tags for identification and authentication. *Microsystems & Nanoengineering*(2020). DOI: 10.1038/s41378-020-00213-2.