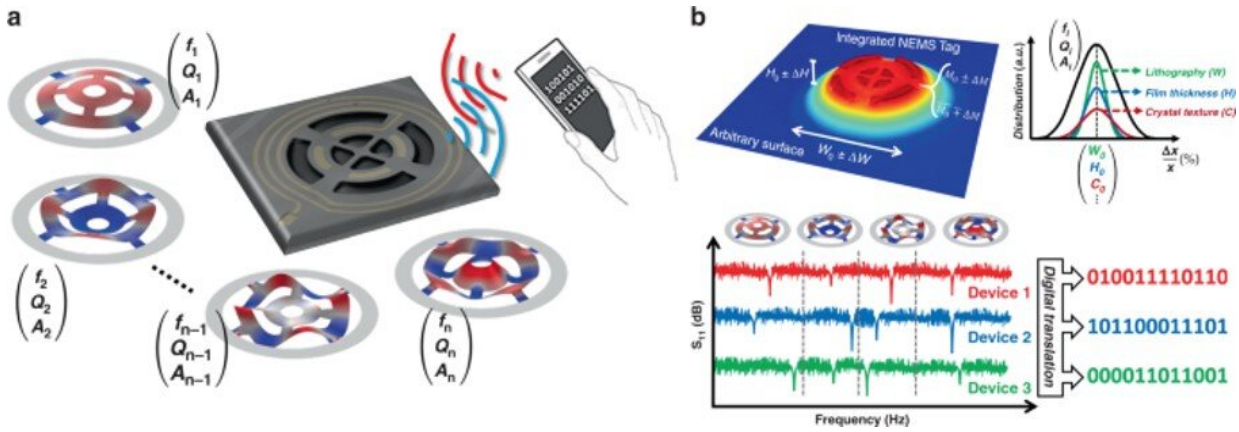
Nanoelectromechanical tags for tamper-proof product identification and authentication

December 8 2020, by Thamarasee Jeewandara



Conceptual demonstration of the NEMS tag concept. (a) a set of mechanical resonance modes with different frequencies (fi), quality factors (Qi), and vibration amplitudes (Ai) are excited upon wireless interrogation. The resulting spectral signature is translated into a digital string. (b) The topography of a fabricated NEMS tag, integrated on a glass substrate. The fabrication uncertainties, including film thickness variation, lithographical errors, and randomized crystal polymorphism, induce inhomogeneous variations in the spectral signature of NEMS tags and result in the realization of digital strings unique to each tag. Credit: Microsystems & Nanoengineering, doi: 10.1038/s41378-020-00213-2

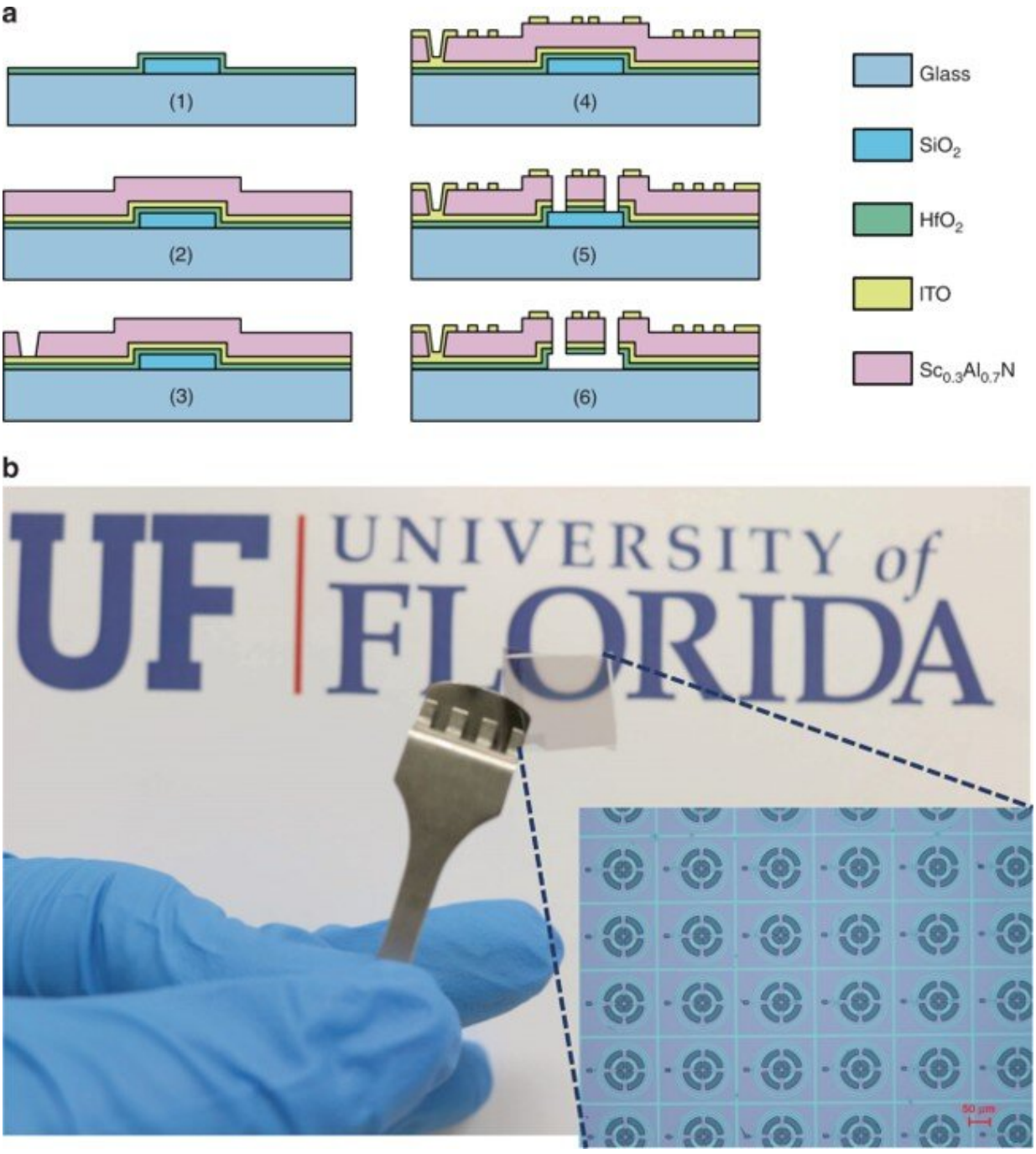
Researchers in cybersecurity aim to realize truly unclonable identification and authentication tags to defend global systems from ever-increasing counterfeit attacks. In a new report now published on *Nature:*

Microsystems & Nanoengineering, Sushant Rassay and a team of researchers in electrical and computer engineering at the University of Florida, U.S., demonstrated nanoscale tags to explore an electromechanical spectral signature as a fingerprint based on the inherent randomness of the fabrication process. The ultraminiature size and transparent constituents of the nanoelectromechanical (NEMS) tags provided substantial immunity to physical tampering and cloning efforts. The NEMS can typically convert forms of mechanical and vibrational energy from the environment into electric power by developing reliable power sources for ultralow power wireless electronic devices. The team also developed adaptive algorithms to digitally translate the spectral signature into binary fingerprints. The experiments highlighted the potential of clandestine (stealthy) NEMS to secure identification and authentication across a range of products and consumer goods.

Developing technologies to fight counterfeit trade

The emergence of counterfeit trade can significantly impact the global economic system, while escalating to impose broad social damage and pose international security threats as a source of white-collar crime. Counterfeit trade is conventionally fought using physical tags to identify, authenticate, and track genuine items by generating digital fingerprints or watermarks. The effectiveness of a physical tag can be defined by its applicability to diverse goods ranging from edibles to electronics, its perseverance to cloning alongside the associated cost of production. Researchers have developed a variety of general-purpose physical tag technologies, including quick response (QR) patterns, universal product code (UPC) and radiofrequency identification (RFID) tags. However, such techniques are limited and therefore pose security risks. Scientists had therefore recently developed nanoscale physical unclonable functions or nanophysical unclonable functions (PUFs) to identify substantial limits of identification and authentication tags. In this study, Rassay et al. presented a radically different approach using

nanoelectromechanical systems (NEMS) to realize stealthy physical tags. The constructs maintained substantial immunity to tampering and cloning with generic applicability across a range of products.

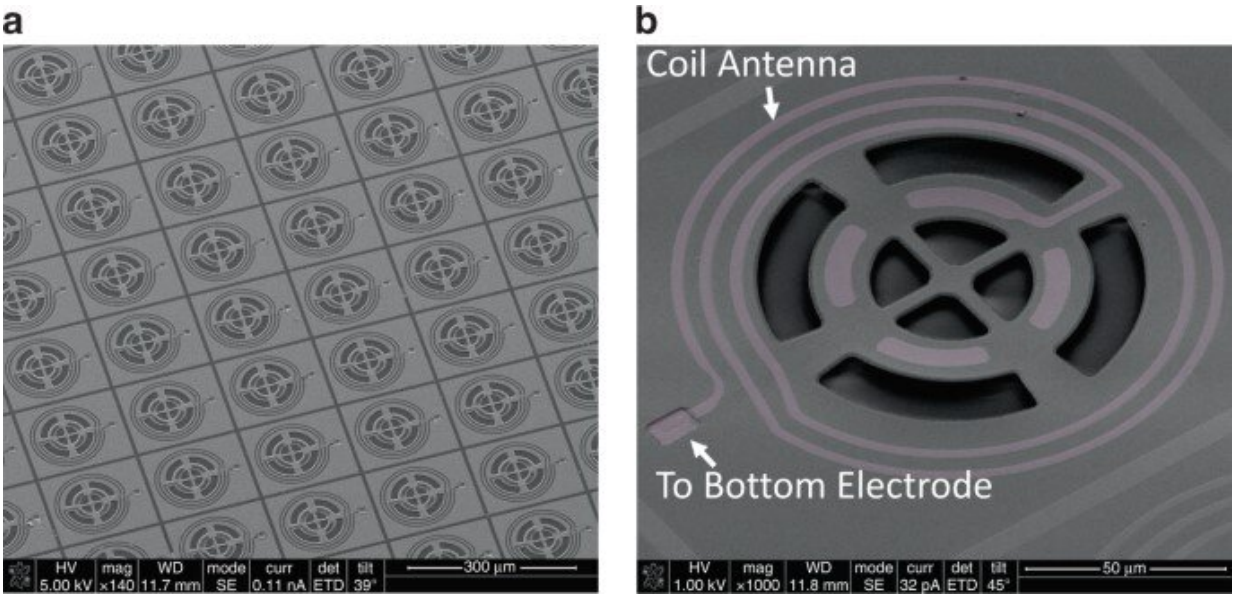


Fabrication of the clandestine NEMS tags. a the fabrication process for the implementation of clandestine NEMS tags on a glass substrate: (1) deposition and patterning of a sacrificial SiO2 layer on the glass substrate and the ALD of 10-nm HfO2, (2) sputtering and patterning of 50-nm ITO (bottom electrode) and 100-nm Sc0.3Al0.7N, (3) patterning of the Sc0.3Al0.7N layer to access the bottom ITO electrode, (4) deposition and patterning of the top ITO electrodes and the coil, (5) etching of trenches in the transducer stack to define the NEMS tag geometry, and (6) releasing of the NEMS tag by etching sacrificial SiO2. b A 1-cm×1-cm glass substrate with very-large-scale-integrated array of NEMS tags featuring optical transparency. The inset shows an enlargement of the optical image, highlighting an array of NEMS tags with identical layouts. Credit: Microsystems & Nanoengineering, doi: 10.1038/s41378-020-00213-2

Nanoelectromechanical systems (NEMS) tags

The NEMS tags showed an electromechanical spectral signature composed of a large set of high-quality-factor (Q) resonance peaks. In general, the Q-factor describes the properties of an oscillator or resonator and the nature of the stored energy of the resonator, where a higher Q indicates that oscillations disperse slowly to cause a lower rate of energy loss relative to the stored energy of the resonator. These physical characteristics coupled to their ultraminiature size and transparent constituents ensured the immunity of NEMS tags towards physical tampering and cloning efforts. The cost-effective tags can be used in cluttered environments with large background noise and interference. To create the NEMS tags, Rassay et al. sandwiched a thin piezoelectric film between two metallic layers and enhanced the tag by choosing transparent materials to form constituent layers, then implemented the tags on a glass substrate to evaluate their transparency. The constituents provided a large electromechanical coupling coefficient to allow excitation of the mechanical resonance modes with miniscule magnetic powers. The team ultimately patterned the NEMS tag and

observed the product using scanning electron microscopy (SEM) to highlight its optical transparency.



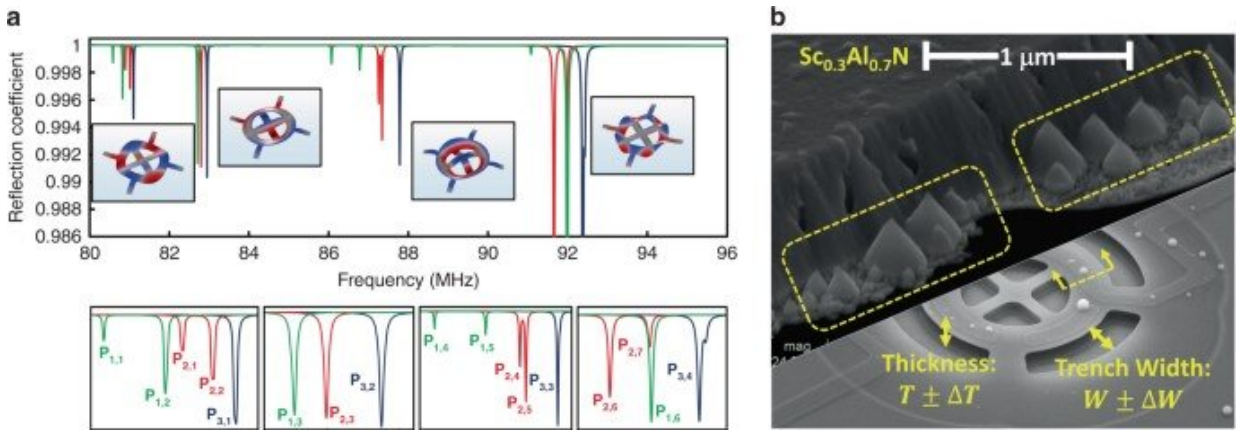
SEM images of the clandestine NEMS tags. (a) an array of NEMS tags with the same layouts implemented in the same batch on a glass substrate; (b) an individual NEMS tag with an integrated coil antenna enabling wireless interrogation of the spectral signature through magnetic coupling. Credit: Microsystems & Nanoengineering, doi: 10.1038/s41378-020-00213-2

Principle-of-action and digital translation

During the development of the NEMS tags, the scientists delved into the properties of the electromechanical spectral signature to facilitate identification. The team designed the lateral geometry of the NEMS tags to create a large set of high-Q mechanical resonance modes across a small frequency range of interest (80-90 MHz). Based on the varying characteristics of the corresponding peaks to the resonance modes,

Rassay et al. assigned a binary string to the NEMS tags.

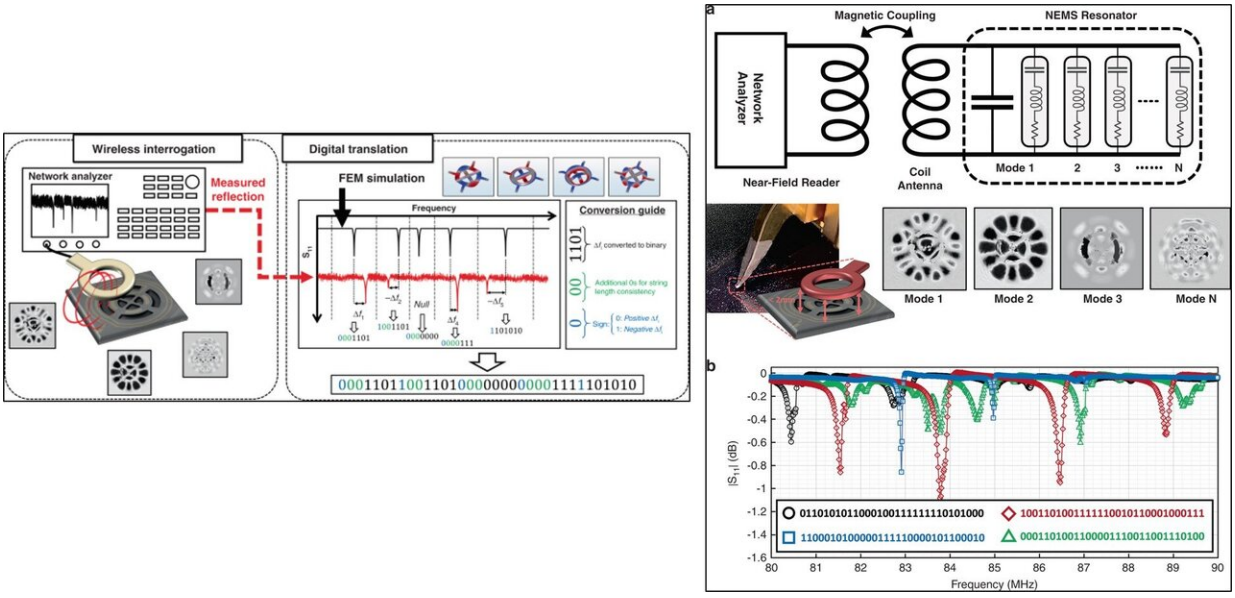
The random nature of the material distribution allowed them to create visually identical NEMS tags with unique digital fingerprints that were only reflected in their spectral signature, and therefore nearly impossible to reverse engineer. The random and intrinsic uncertainties of the label constituents were desirable as it provided two distinct security benefits; first, it allowed the team to create unique identifiers or fingerprints for each of the batch-fabricated devices. Second, the material-based intrinsic randomness was advantageous to protect the information during its manufacture, thereby preventing counterfeit products. The translation procedure contained wireless interrogation and digital translation components, where the team implemented a series of elaborate steps to generate a unique binary string designated to each NEMS tag.



Simulation of NEMS tag spectral signature subjected to randomized structural variations. (a) the large-span simulated spectral signature of the NEMS tags, with randomized variations in their thickness, lateral dimension, and crystalline profiles, and the short-span signature over each resonance peak in the spectral response, highlighting the effect of the nanofabrication uncertainties. (b) An SEM image of the NEMS tag cross section, highlighting the fact that the cubic cones formed randomly during the Sc0.3Al0.7N growth. Credit: Microsystems & Nanoengineering, doi: 10.1038/s41378-020-00213-2

Characterizing the NEMS tag

To measure the spectral signature tags, Rassay et al. used near-field wireless interrogation across the frequency span of 80 to 90 MHz. To accomplish this, they positioned an intelligent character recognition (ICR) magnetic near-field microprobe with a coil radius of 50 µm for wireless interrogation through magnetic coupling. The team positioned the microprobe at a sub-2-mm vertical distance from the label, connected to a network analyzer to measure the reflection response across the frequency spectrum. The team then compared the spectral signatures of four NEMS labels, which they randomly picked from the array. For example, the 31-bit string assigned to the spectral signature fingerprints highlighted the entropy of the clandestine NEMS technology. As proof of concept, the team quantified the entropy under different temperature ranges for ten NEMS tags with identical designs using the interdevice Hamming distance (a metric to compare two binary data strings) to measure the uniqueness of the binary strings corresponding to the spectral signatures.



LEFT: Schematic diagram of the digital translation procedure used to designate unique binary tags to the NEMS labels: the measured spectral signature of a tag is compared with the reference signature extracted from COMSOL simulations. The reference signature is divided into intervals with borders defined by the average of the frequencies of adjacent peaks. In each interval, the measured peak with the highest magnitude is identified, and its frequency is subtracted from the reference peak. The resulting decimal value is converted to a binary substring. A conversion guide is used to assign the leftmost bit to the sign of the subtraction, additional zeros to ensure consistent length of the substrings, regardless of the relative frequency offset of the measurements and reference in each interval, and all zeros when no measured peak exists in an interval. Finally, the substrings are cascaded to create the designated binary tag for the NEMS label. RIGHT: Wireless spectral interrogation of the NEMS tags. (a) the near-field wireless interrogation setup used for extraction of the spectral signature of the NEMS tags. The inset shows various mechanical vibration patterns corresponding to resonance modes in the spectral signature, measured by the holographic microscope. (b) The measured spectral signature of three NEMS tags with identical designs and fabricated in the same batch. The inset shows the 31-bit binary strings extracted for each tag. Credit: Microsystems & Nanoengineering, doi: 10.1038/s41378-020-00213-2

Outlook of the anti-counterfeiting stealth technology

In this way, Sushant Rassay and colleagues showed a new physical tag technology to identify and authenticate the use of the electromechanical spectral signatures of clandestine nanoelectromechanical (NEMS) tags. The ultraminiature device provided an optically transparent and visually undetectable indirect method for information storage. They engineered the spectral signature of the NEMS tag to have a large number of high-Q mechanical resonance peaks. The team obtained distinct fingerprints for the NEMS tags due to intrinsic variations of the material properties and

extrinsic variations of the fabrication process. The scientists also developed a translation algorithm to designate a binary string to the spectral signature of each tag. The resulting large entropy and robustness of the NEMS tags highlighted the potential of the technology to identify and authenticate products.

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

Yansong Gao et al. Emerging Physical Unclonable Functions With Nanotechnology, *IEEE Access* (2016). DOI: 10.1109/ACCESS.2015.2503432

Riikka Arppe et al. Physical unclonable functions generated through chemical methods for anti-counterfeiting, *Nature Reviews Chemistry* (2017). DOI: 10.1038/s41570-017-0031