How Nanotech Can Foil Counterfeiters

2021-06-03

These tiny mechanical ID tags are unclonable, cheap, and invisible.

What’s the largest criminal enterprise in the world? Narcotics? Gambling? Human trafficking?

Nope. The biggest racket is the production and trade of counterfeit goods, which is expected to exceed US $1 trillion next year. You’ve probably suffered from it more than once yourself, purchasing on Amazon or eBay what you thought was a brand-name item only to discover that it was an inferior-quality counterfeit.

It’s an all-too-common ploy, and legitimate manufacturing companies and distributors suffer mightily as a result of it. But the danger runs much deeper than getting ripped off when you were seeking a bargain. When purchasing pharmaceuticals, for example, you’d be putting your health in jeopardy if you didn’t receive the bona fide medicine that was prescribed. Yet for much of the world, getting duped in this way when purchasing medicine is sadly the norm. Even people in developed nations are susceptible to being treated with fake or substandard medicines.

Tiny mechanical resonators produced the same way microchips are made [bottom] can serve to authenticate various goods. Being less than 1 micrometer across and transparent, these tags are essentially invisible.

Counterfeit electronics are also a threat, because they can reduce the reliability of safety-critical systems and can make even ordinary consumer electronics dangerous. Cellphones and e-cigarettes, for example, have been known to blow up in the

user’s face because of the counterfeit batteries inside them.

It would be no exaggeration to liken the proliferation of counterfeit goods to an infection of the global economy system—a pandemic of a different sort, one that has grown 100 fold over the past two decades, according to the International AntiCounterfeiting Coalition. So it’s no wonder that many people in industry have long been working on ways to battle this scourge.

The traditional strategy to thwart counterfeiters is to apply some sort of authentication marker to the genuine article. These efforts include the display of Universal Product Codes (UPC) and Quick Response (QR) patterns, and sometimes the inclusion of radio-frequency identification (RFID) tags. But UPC and QR codes must be apparent so that they are accessible for optical scanning. This makes them susceptible to removal, cloning, and reapplication to counterfeit products. RFID tags aren’t as easy to clone, but they typically require relatively large antennas, which makes it hard to label an item imperceptibly with them. And depending on what they are used for, they can be too costly.

We’ve come up with a different solution, one based on radio-frequency (RF) nanoelectromechanical systems (NEMS). Like RFID tags, our RF NEMS devices don’t have to be visible to be scanned. That, their tiny size, and the nature of their constituents, make these tags largely immune to physical tampering or cloning. And they cost just a few pennies each at most.

Unseen NEMS tags could become a powerful weapon in the global battle against counterfeit products, even counterfeit bills. Intrigued? Here’s a description of the physical principles on which these devices are based and a brief overview of what would be involved in their production and operation.

You can think of an RF NEMS tag as a tiny sandwich. The slices of bread are two 50-nanometer-thick conductive layers of indium tin oxide, a material commonly used to make transparent electrodes, such as those for the touch screen on your phone. The filling is a 100-nm-thick piezoelectric film composed of a scandium-doped aluminum nitride, which is similarly transparent. With lithographic techniques similar to those used to fabricate

integrated circuits, we etch a pattern in the sandwich that includes a ring in the middle suspended by four slender arms. That design leaves the circular surface free to vibrate.

The material making up the piezoelectric film is, of course, subject to the piezoelectric effect: When mechanically deformed, the material generates an electric voltage across it. More important here is that such materials also experience what is known as the converse piezoelectric effect—an applied voltage induces mechanical deformation. We take advantage of that phenomenon to induce oscillations in the flexible part of the tag.

To accomplish this, we use lithography to fabricate a coil on the perimeter of the tag. This coil is connected at one end to the top conductive layer and on the other end to the bottom conductive layer. Subjecting the tag to an oscillating magnetic field creates an oscillating voltage across the piezoelectric layer, as dictated by Faraday's law of electromagnetic induction. The resulting mechanical deformation of the piezo film in turn causes the flexible parts of the tag to vibrate.

This vibration will become most intense when the frequency of excitation matches the natural frequency of the tiny mechanical oscillator. This is simple resonance, the phenomenon that allows an opera singer's voice to shatter a wine glass when the right note is hit (and if the singer tries really, really hard). It's also what famously triggered the collapse of the Broughton suspension bridge near Manchester, England, in 1831, when 74 members of the 60th Rifle Corps marched across it with their footsteps landing in time with the natural mechanical resonance of the bridge. (After that incident, British soldiers were instructed to break step when they marched across bridges!) In our case, the relevant excitation is the oscillation of the magnetic field applied by a scanner, which induces the highest amplitude vibration when it matches the frequency of mechanical resonance of the flexible part of the tag.

These electron micrographs show some of the tags the authors have fabricated, which can take various forms. The preferred geometry [top] is a circular tag containing a piezoelectric ring suspended by four beams. It includes a coil [lighter shade], which connects with electrode layers on the top and bottom of the

ring. Voltages induced in this coil by an external scanner set up mechanical oscillations in the ring.

In truth, the situation is more complicated than this. The flexible portion of the tag doesn't have just one resonant frequency—it has many. It's like the membrane on a drum, which can oscillate in various ways. The left side might go up as the right side goes down, and vice versa. Or the middle might be rising as the perimeter shifts downward. Indeed, there are all sorts of ways that the membrane of a drum deforms when it is struck. And each of those oscillation patterns has its own resonant frequency.

We designed our nanometer-scale tags to vibrate like tiny drumheads, with many possible modes of oscillation. The tags are so tiny—just a few micrometers across—that their vibrations take place at radio frequencies in the range of 80 to 90 megahertz. At this scale, more than the geometry of the tag matters: the vagaries of manufacturing also come into play.

For example, the thickness of the sandwich, which is nominally around 200 nm, will vary slightly from place to place. The diameter or the circularity of the ring-shaped portion is also not going to be identical from sample to sample. These subtle manufacturing variations will affect the mechanical properties of the device, including its resonant frequencies.

In addition, at this scale the materials used to make the device are not perfectly homogeneous. In particular, in the piezoelectric layer there are intrinsic variations in the crystal structure. Because of the ample amount of scandium doping, conical clusters of cubic crystals form randomly within the matrix of hexagonal crystals that make up the aluminum nitride grains. The random positioning of those tiny cones creates significant differences in the resonances that arise in seemingly identical tags.

Random variations like these can give rise to troublesome defects in the manufacture of some microelectronic devices. Here, though, random variation is not a bug—it's a feature! It allows each tag that is fabricated to serve as a unique marker. That is, while the resonances exhibited by a tag are controlled in a general way by its geometry, the exact frequencies,

amplitudes, and sharpness of each of its resonances are the result of random variations. That makes each of these items unique and prevents a tag from being cloned, counterfeited, or otherwise manufactured in a way that would reproduce all the properties of the resonances seen in the original.

An RF NEMS tag is an example of what security experts call a physical unclonable function. For discretely labeling something like a batch of medicine to document its provenance and prove its authenticity, it’s just what the doctor ordered.

You might be wondering at this point how we can detect and characterize the unique characteristics of the oscillations taking place within these tiny tags. One way, in principle, would be to put the device under a vibrometer microscope and look at it move. While that’s possible—and we’ve done it in the course of our laboratory studies—this strategy wouldn’t be practical or effective in commercial applications.

But it turns out that measuring the resonances of these tags isn’t at all difficult. That’s because the electronic scanner that excites vibrations in the tag has to supply the energy that maintains those vibrations. And it’s straightforward for the electronic scanner to determine the frequencies at which energy is being sapped in this way.

The authors directly measured the surface topography of a tag using a digital holographic microscope, which is able to scan reflective surfaces and precisely measure their heights [top]. The authors also modeled various modes of oscillation of the flexible parts of such a tag [bottom]. Each mode has a characteristic resonant frequency, which varies with both the geometry of the tag and its physical composition.

The scanner we are using at the moment is just a standard piece of electronic test equipment called a network analyzer. (The word network here refers to the network of electrical components—resistors, and capacitors, and inductors—in the circuit being tested, not to a computer network like the Internet.) The sensor we attach to the network analyzer is just a

tiny coil, which is positioned within a couple of millimeters of the tag.

With this gear, we can readily measure the unique resonances of an individual tag. We record that signature by measuring how much the various resonant-frequency peaks are offset from those of an ideal tag of the relevant geometry. We translate each of those frequency offsets into a binary number and string all those bits together to construct a digital signature unique to each tag. The scheme that we are currently using produces 31-bit-long identifiers, which means that more than 2 billion different binary signatures are possible—enough to uniquely tag just about any product you can think of that might need to be authenticated.

Relying on subtle physical properties of a tag to define its unique signature prevents cloning but it does raise a different concern: Those properties could change.

For example, in a humid environment, a tag might adsorb some moisture from the air, which would change the properties of its resonances. That possibility is easy enough to protect against by covering the tag with a thin protective layer, say of some transparent polymer, which can be done without interfering with the tag’s vibrations.

But we also need to recognize that the frequencies of its resonances will vary as the tag changes temperature. We can get around that complication, though. Instead of characterizing a tag according to the absolute frequency of its oscillation modes, we instead measure the relationships between the frequencies of different resonances, which all shift in frequency by similar relative amounts when the temperature of the tag changes. This procedure ensures that the measured characteristics will translate to the same 31-bit number, whether the tag is hot or cold. We’ve tested this strategy over quite a large temperature range (from 0 to 200 °C.) and have found it to be quite robust.

A tag is characterized by the differences between its measured resonant frequencies [dips in red line] and the corresponding frequencies for an ideal tag [dips in black line]. These differences are encoded as short binary strings, padded to a standard length, with one bit signifying whether the frequency offset of positive

or negative [right]. Concatenated, these strings provide a unique digital fingerprint for the tag [bottom]

The RF network analyzer we're using as a scanner is a pricey piece of equipment, and the tiny coil sensor attached to it needs to be placed right up against the tag. While in some applications the location of the tag on the product could be standardized (say, for authenticating credit cards), in other situations the person scanning a product might have no idea where on the item the tag is positioned. So we are working now to create a smaller, cheaper scanning unit, one with a sensor that doesn't have to be positioned right on top of the tag.

We are also exploring the feasibility of modifying the resonances of a tag after it is fabricated. That possibility arises from a bit of serendipity in our research. You see, the material we chose for the piezoelectric layer in our tags is kind of unusual. Piezoelectric devices, like some of the filters in our cellphones, are commonly made from aluminum nitride. But the material we adopted includes large amounts of scandium dopant, which enhances its piezoelectric properties.

Unknown to us when we decided to use this more exotic formulation was a second quality it imparts: It makes the material into a ferroelectric, meaning that it can be electrically polarized by applying a voltage to it, and that polarization remains even after the applied voltage is removed. That's relevant to our application, because the polarization of the material influences its electrical and mechanical properties. Imparting a particular polarization pattern on a tag, which could be done after it is manufactured, would alter the frequencies of its resonances and their relative amplitudes. This approach offers a strategy by which low-volume manufacturers, or even end users, could "burn" a signature into these tags.

Our research on RF NEMS tags has been funded in part by Discover Financial Services, the company behind the popular Discover credit card. But the applications of the tiny tags we've been working on will surely be of interest to many other types of companies as well. Even governments might one day adopt nanomechanical tags to authenticate paper money.

Just how broadly useful these tags will be depends, of course, on how successful we are in engineering a handheld scanner—which might even be a simple add-on for a smartphone—and whether our surmise is correct that these tags can be customized after manufacture. But we are certainly excited to be exploring all these possibilities as we take our first tentative steps toward commercialization of a technology that might one day help to stymie the world's most widespread form of criminal activity.

This article appears in the June 2021 print issue as "The Hidden Authenticators."

Read the original article on IEEE Spectrum.