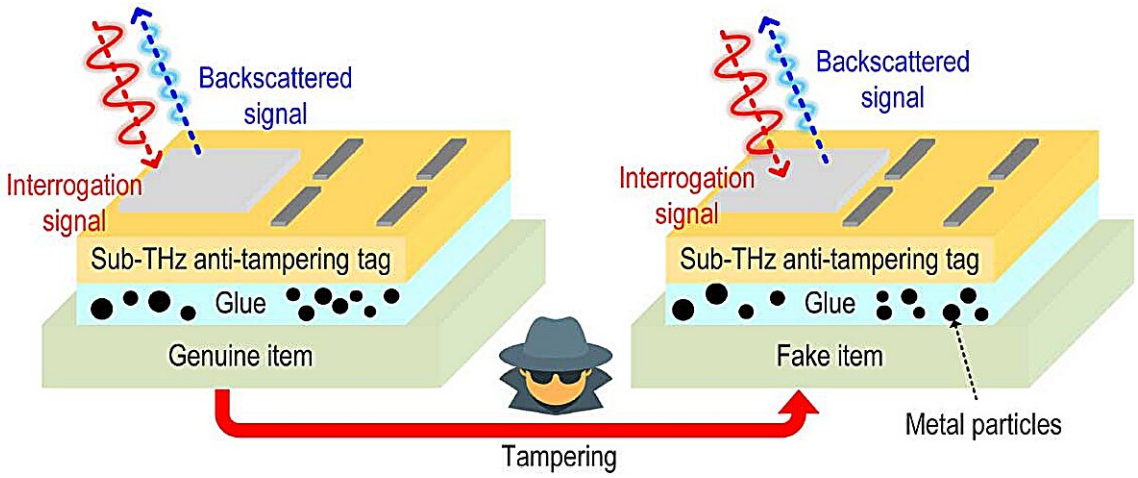
This tiny, tamper-proof ID tag can authenticate almost anything

February 18 2024



After passing through the tag and striking the object's surface, terahertz waves are reflected, or backscattered, to a receiver for authentication. Credit: Ruonan Han, Eunseok Lee, et al

A few years ago, MIT researchers invented a cryptographic ID tag that is several times smaller and significantly cheaper than the traditional radio frequency tags (RFIDs) that are often affixed to products to verify their authenticity.

This tiny tag, which offers improved security over RFIDs, utilizes terahertz waves, which are smaller and travel much faster than radio waves. But this terahertz tag shared a major security vulnerability with

traditional RFIDs: A counterfeiter could peel the tag off a genuine item and reattach it to a fake, and the authentication system would be none the wiser.

The researchers have now surmounted this security vulnerability by leveraging terahertz waves to develop an antitampering ID tag that still offers the benefits of being tiny, cheap, and secure.

They mix microscopic metal particles into the glue that sticks the tag to an object and then use terahertz waves to detect the unique pattern those particles form on the item's surface. Akin to a fingerprint, this random glue pattern is used to authenticate the item, explains Eunseok Lee, an electrical engineering and computer science (EECS) graduate student and lead author of a paper on the antitampering tag.

"These metal particles are essentially like mirrors for terahertz waves. If I spread a bunch of mirror pieces onto a surface and then shine a light on that, depending on the orientation, size, and location of those mirrors, I would get a different reflected pattern. But if you peel the chip off and reattach it, you destroy that pattern," adds Ruonan Han, an associate professor in EECS, who leads the Terahertz Integrated Electronics Group in the Research Laboratory of Electronics.

The researchers produced a light-powered antitampering tag that is about 4 square millimeters in size. They also demonstrated a machine-learning model that helps detect tampering by identifying similar glue pattern fingerprints with more than 99 percent accuracy.

Because the terahertz tag is so cheap to produce, it could be implemented throughout a massive supply chain. Its tiny size enables the tag to attach to items too small for traditional RFIDs, such as certain medical devices.

The paper, which will be presented at the IEEE Solid State Circuits Conference, is a collaboration between Han's group and the Energy-Efficient Circuits and Systems Group of Anantha P. Chandrakasan, MIT's chief innovation and strategy officer, dean of the MIT School of Engineering, and the Vannevar Bush Professor of EECS. Co-authors include EECS graduate students Xibi Chen, Maitryi Ashok, and Jaeyeon Won.

Preventing tampering

This research project was partly inspired by Han's favorite car wash. The business stuck an RFID tag onto his windshield to authenticate his car wash membership. For added security, the tag was made from fragile paper so it would be destroyed if a less-than-honest customer tried to peel it off and stick it on a different windshield.

But that is not a terribly reliable way to prevent tampering. For instance, someone could use a solution to dissolve the glue and safely remove the fragile tag.

Rather than authenticating the tag, a better security solution is to authenticate the item itself, Han says. To achieve this, the researchers targeted the glue at the interface between the tag and the item's surface.

Their antitampering tag contains a series of minuscule slots that enable terahertz waves to pass through the tag and strike microscopic metal particles that have been mixed into the glue.

Terahertz waves are small enough to detect the particles, whereas larger radio waves would not have enough sensitivity to see them. Also, using terahertz waves with a 1-millimeter wavelength allowed the researchers to make a chip that does not need a larger, off-chip antenna.

After passing through the tag and striking the object's surface, terahertz waves are reflected or backscattered to a receiver for authentication. How those waves are backscattered depends on the distribution of metal particles that reflect them.

The researchers put multiple slots onto the chip so waves can strike different points on the object's surface, capturing more information on the random distribution of particles.

"These responses are impossible to duplicate, as long as the glue interface is destroyed by a counterfeiter," Han says.

A vendor would take an initial reading of the antitampering tag once it was stuck onto an item and then store those data in the cloud, using them later for verification.

AI for authentication

But when it came time to test the antitampering tag, Lee ran into a problem: It was very difficult and time-consuming to take precise enough measurements to determine whether two glue patterns were a match.

He reached out to a friend in the MIT Computer Science and Artificial Intelligence Laboratory (CSAIL), and together, they tackled the problem using AI. They trained a machine-learning model that could compare glue patterns and calculate their similarity with more than 99 percent accuracy.

"One drawback is that we had a limited data sample for this demonstration, but we could improve the neural network in the future if a large number of these tags were deployed in a supply chain, giving us a lot more data samples," Lee says.

The authentication system is also limited by the fact that terahertz waves suffer from high levels of loss during transmission, so the sensor can only be about 4 centimeters from the tag to get an accurate reading. This distance wouldn't be an issue for an application like barcode scanning, but it would be too short for some potential uses, such as in an automated highway toll booth. Also, the angle between the sensor and tag needs to be less than 10 degrees, or the terahertz signal will degrade too much.

They plan to address these limitations in future work and hope to inspire other researchers to be more optimistic about what can be accomplished with terahertz waves despite the many technical challenges, says Han.

"One thing we really want to show here is that the application of the terahertz spectrum can go well beyond broadband wireless. In this case, you can use terahertz for ID, security, and authentication. There are a lot of possibilities out there," he adds.

More information: Ruonan Han et al, "A Packageless Anti-Tampering Tag Utilizing Unclonable Sub-THz Wave Scattering at the Chip-Item Interface," *IEEE Solid State Circuits Conference* (2024). www.isscc.org/

This story is republished courtesy of MIT News (web.mit.edu/newsoffice/), a popular site that covers news about MIT research, innovation and teaching.

Provided by Massachusetts Institute of Technology