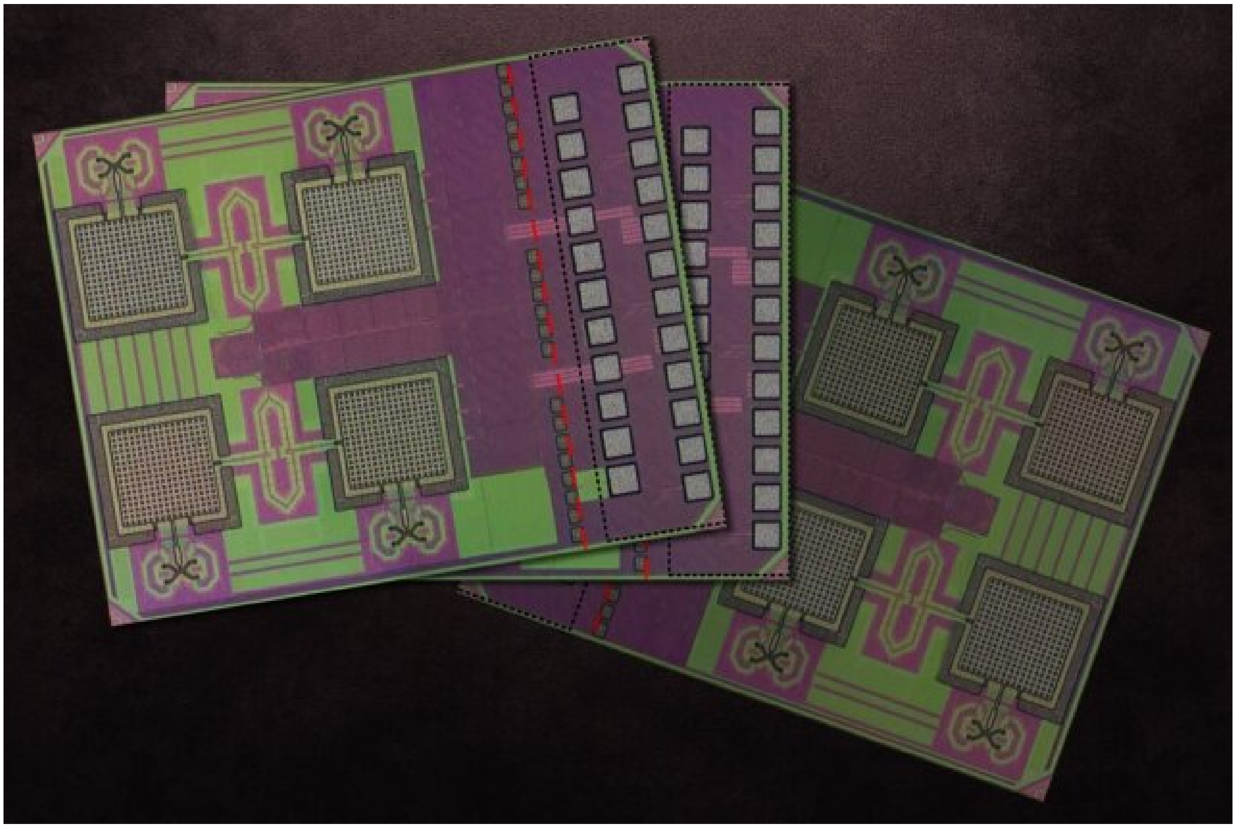
Tiny, battery-free ID chip can help combat losses to counterfeiting

February 20 2020, by Rob Matheson



MIT researchers' millimeter-sized ID chip integrates a cryptographic processor, an antenna array that transmits data in the high terahertz range, and photovoltaic diodes for power. Credit: MIT News

To combat supply chain counterfeiting, which can cost companies billions of dollars annually, MIT researchers have invented a cryptographic ID tag that's small enough to fit on virtually any product and verify its authenticity.

A 2018 report from the Organization for Economic Co-operation and Development estimates about $2 trillion worth of counterfeit goods will be sold worldwide in 2020. That's bad news for consumers and companies that order parts from different sources worldwide to build products.

Counterfeiters tend to use complex routes that include many checkpoints, making it challenging to verifying their origins and authenticity. Consequently, companies can end up with imitation parts. Wireless ID tags are becoming increasingly popular for authenticating assets as they change hands at each checkpoint. But these tags come with various size, cost, energy, and security tradeoffs that limit their potential.

Popular radio-frequency identification (RFID) tags, for instance, are too large to fit on tiny objects such as medical and industrial components, automotive parts, or silicon chips. RFID tags also contain no tough security measures. Some tags are built with encryption schemes to protect against cloning and ward off hackers, but they're large and power hungry. Shrinking the tags means giving up both the antenna package—which enables radio-frequency communication—and the ability to run strong encryption.

In a paper presented yesterday at the IEEE International Solid-State Circuits Conference (ISSCC), the researchers describe an ID chip that navigates all those tradeoffs. It's millimeter-sized and runs on relatively low levels of power supplied by photovoltaic diodes. It also transmits data at far ranges, using a power-free "backscatter" technique that operates at a frequency hundreds of times higher than RFIDs. Algorithm optimization techniques also enable the chip to run a popular cryptography scheme that guarantees secure communications using extremely low energy.

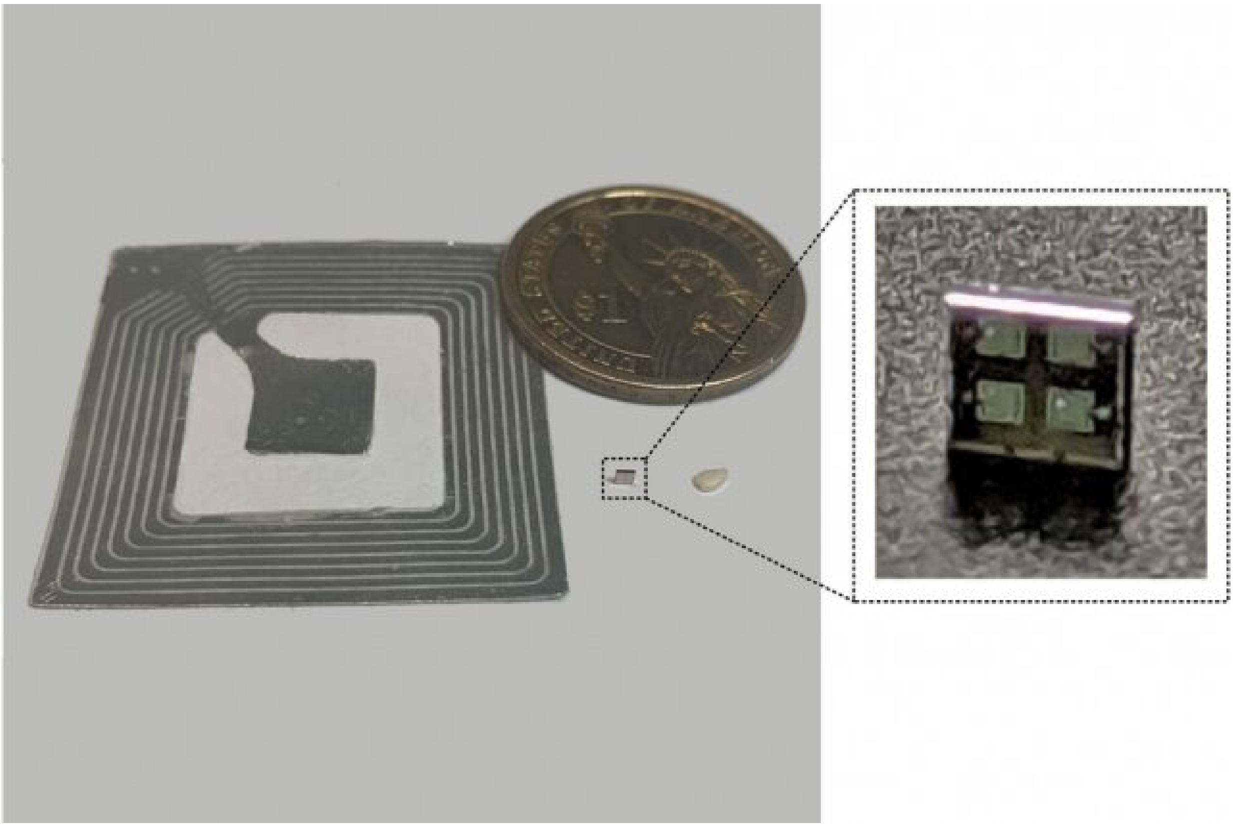
"We call it the 'tag of everything." And everything should mean everything," says co-author Ruonan Han, an associate professor in the Department of Electrical Engineering and Computer Science and head of the Terahertz Integrated Electronics Group in the Microsystems Technology Laboratories (MTL). "If I want to track the logistics of, say, a single bolt or tooth implant or silicon chip, current RFID tags don't enable that. We built a low-cost, tiny chip without packaging, batteries, or other external components, that stores and transmits sensitive data."

Joining Han on the paper are: graduate students Mohamed I. Ibrahim, Muhammad Ibrahim Wasiq Khan, and Chiraag S. Juvekar; former postdoc associate Wanyeong Jung; former postdoc Rabia Tugce Yazicigil; and Anantha P. Chandrakasan, who is the dean of the MIT School of Engineering and the Vannevar Bush Professor of Electrical Engineering and Computer Science.

System integration

The work began as a means of creating better RFID tags. The team wanted to do away with packaging, which makes the tags bulky and increases manufacturing cost. They also wanted communication in the high terahertz frequency between microwave and infrared radiation—around 100 gigahertz and 10 terahertz—that enables chip integration of an antenna array and wireless communications at greater reader distances. Finally, they wanted cryptographic protocols because RFID tags can be scanned by essentially any reader and transmit their data indiscriminately.

But including all those functions would normally require building a fairly large chip. Instead, the researchers came up with "a pretty big system integration," Ibrahim says, that enabled putting everything on a monolithic—meaning, not layered—silicon chip that was only about 1.6 square millimeters.



Even though it’s the size of a sesame seed, the ID tag (zoomed in, right) can send wireless communications at greater reader distances than much larger RFID tags (left) and can run cryptographic algorithms to help secure nearly any product in the supply chain. Credit: Massachusetts Institute of Technology

One innovation is an array of small antennas that transmit data back and forth via backscattering between the tag and reader. Backscatter, used commonly in RFID technologies, happens when a tag reflects an input signal back to a reader with slight modulations that correspond to data transmitted. In the researchers' system, the antennas use some signal splitting and mixing techniques to backscatter signals in the terahertz range. Those signals first connect with the reader and then send data for encryption.

Implemented into the antenna array is a "beam steering" function, where the antennas focus signals toward a reader, making them more efficient, increasing signal strength and range, and reducing interference. This is the first demonstration of beam steering by a backscattering tag, according to the researchers.

Tiny holes in the antennas allow light from the reader to pass through to photodiodes underneath that convert the light into about 1 volt of electricity. That powers up the chip's processor, which runs the chip's "elliptic-curve-cryptography" (ECC) scheme. ECC uses a combination of private keys (known only to a user) and public keys (disseminated widely) to keep communications private. In the researchers' system, the tag uses a private key and a reader's public key to identify itself only to valid readers. That means any eavesdropper who doesn't possess the reader's private key should not be able to identify which tag is part of the protocol by monitoring just the wireless link.

Optimizing the cryptographic code and hardware lets the scheme run on an energy-efficient and small processor, Yazicigil says. "It's always a tradeoff," she says. "If you tolerate a higher-power budget and larger size, you can include cryptography. But the challenge is having security in such a small tag with a low-power budget."

Pushing the limits

Currently, the signal range sits around 5 centimeters, which is considered a far-field range—and allows for convenient use of a portable tag scanner. Next, the researchers hope to "push the limits" of the range even further, Ibrahim says. Eventually, they'd like many of the tags to ping one reader positioned somewhere far away in, say, a receiving room at a supply chain checkpoint. Many assets could then be verified rapidly.

"We think we can have a reader as a central hub that doesn't have to come close to the tag, and all these chips can beam steer their signals to talk to that one reader," Ibrahim says.

The researchers also hope to fully power the chip through the terahertz signals themselves, eliminating any need for photodiodes.

The chips are so small, easy to make, and inexpensive that they can also be embedded into larger silicon computer chips, which are especially popular targets for counterfeiting.

"The U.S. semiconductor industry suffered $7 billion to $10 billion in losses annually because of counterfeit chips," Wasiq Khan says. "Our chip can be seamlessly integrated into other electronic chips for security purposes, so it could have huge impact on industry. Our chips cost a few cents each, but the technology is priceless," he quipped.

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

Citation: Tiny, battery-free ID chip can help combat losses to counterfeiting (2020, February 20) retrieved 27 April 2024 from https://techxplore.com/news/2020-02-tiny-battery-free-id-chip-combat.html