

Startup company Verayo is marketing a passive 13.56 MHz RFID chip that prevents cloning by enabling users to verify its authenticity before selling a product to which it's attached.

By Claire Swedberg

Sept. 4, 2008—[Verayo](#), a Silicon Valley startup company formed by [MIT](#) researchers, has begun offering a commercialized version of its anti-cloning invention as a security solution for radio frequency identification. The system exploits the unique physical characteristics of the silicon and variations in the IC manufacturing process to identify each silicon chip and determine its authenticity, without requiring encryption keys or encryption storage.

Verayo's core technology—Physical Unclonable Functions (PUF)—is based on work conducted at MIT by a team of researchers headed by Professor Srinu Devadas. In 2005, Devadas joined with Anant Agrawal, former VP resident of [Sun Microsystems](#), to form a company called PUFACO, which obtained an exclusive license to MIT's rights in the core technology. The company began testing the technology for use with RFID in 2007, then changed its name to Verayo in May of this year.



Vivek Khandelwal

Verayo's first product is the Vera X512H, a passive 13.56 MHz RFID chip that offers 512 bits of memory and is based on the ISO 14443-A standard. The system capitalizes on a quirk of the chip-making process, says Vivek Khandelwal, the firm's marketing director. Like a person's fingerprints, each RFID chip possesses subtle but unique physical characteristics that distinguish it from all other RFID chips. Despite manufacturers' efforts to make chips that are exactly the same, he says, no two chips are exactly alike.

To create its PUF-enabled Vera X512H chip, Verayo developed an RFID chip containing a tiny electric circuit designed to transmit a "challenge," or string of numbers and letters, to the chip. When it receives this challenge, the chip then responds with its unique digital signal that can be translated into its own string of letters and numbers. That response is what makes it possible for Verayo to develop and market a system that utilizes this circuit to recognize and authenticate a chip, and to reject any IC that fails to respond to a challenge in the expected manner. "Because of the variation in the chip," Khandelwal says, "the responses you get are unique to each chip."

Here's how it works: An RFID tag is attached to a product or embedded in an ID card, such as a driver's license. Any high-frequency (HF) RFID interrogator that can read passive ISO 14443-A tags can be used to send a "write" command to the tag, thereby instructing the PUF circuit to issue a challenge to the chip, which then transmits its digital signature, along with a unique tag ID (TID) number programmed to the chip during manufacture. The interrogator receives the chip's digital signature, and the system compares it with the expected response for the chip with that specific TID. With a firmware update, the reader can also send custom commands, such as optimizing the challenge and response

exchange.

Either way, the interrogator's transmission to the chip activates the PUF circuit that issues a challenge, and the chip responds by transmitting a signal containing its unique digital signature. In most cases, the reader instructs the chip—via the PUF circuit—to perform this action several times, with multiple challenges, to verify its digital signature. The chip's resulting response is then transmitted to the user's back-end system.

When a retailer sells a tagged product, it can transmit a request to the item's manufacturer and obtain a list of challenges. An interrogator can then issue several different challenges (strings of numbers), each eliciting a digital signature that differs from those elicited by the other challenges. The reader will instruct the PUF circuit to send a challenge when prompted, and the chip will respond with the expected string of corresponding numbers and letters, indicating its authenticity, or with a separate set of numbers and letters signifying that it is counterfeit.

The response from an authentic chip will typically have a few variations of digits—up to 25 percent, Khandelwal says. If there are more than that figure, the chip is determined to be fraudulent—in other words, a cloned copy of an authentic chip. If there is any doubt, the reader operator can attempt another challenge and compare the results.

The PUF system, Khandelwal says, could be adapted for use with any RFID chip or tag, passive or active, and regardless of radio frequency and air-interface protocol. Because the PUF circuit is so small, and since no extra information needs to be stored on the chip (such as encryption data), the tag's power consumption remains unaffected. The addition of the PUF circuit adds only a slight increase to the tag's cost.

Verayo is presently working with [RSIID Technologies](#) to create the labels and tags in which the Verayo chips will be incorporated. Those labels and tags are commercially available now.

The RFID industry currently uses encryption algorithms to verify the authenticity of certain RFID ICs, such as [NXP's](#) Mifare passive 13.56 MHz chips. But this requires that the chip store encryption data, and that the reader and tag transmit via an encrypted signal. The EPC Gen 2 standard, however, does not support encryption, which means most passive UHF EPC Gen 2 tags presently on the market are vulnerable to cloning.

At the current time, Khandelwal says, Verayo is focusing on marketing the Vera X512H chip to the luxury products and ID cards market, where there is a high risk of tag counterfeiting. However, he notes, PUF-enabled tags could also be employed for other high-crime-risk industries, such as pharmaceutical products, sports memorabilia or airline cargo. Although Verayo is selling its own PUF-enabled RFID chips, any chip vendor could incorporate the PUF circuit into the chips it fabricates as well. Verayo is open to licensing agreements with RFID label makers, Khandelwal says.

On Sept. 17, *RFID Journal* will host a webinar during which Verayo will explain how its technology works, and how it can be employed to fight counterfeiting. For more information, or to register, [click here](#).