A microscopic RF Authentication IC for Preventing Counterfeit Electronics

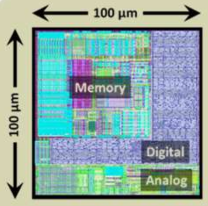
Michael Kane (SRI PI), Alan Braun (SRI), Rich Sita (SRI) Bayard Gardineer (SRI), John Armer (Incyte),
Arne Knudsen (Kyocera), Isaac Potoczny-Jones (Tozny), Siva Narendra (Tyfone)

Driving Applications: Supply Chain Hardware Integrity for Electronics Defense (SHIELD)

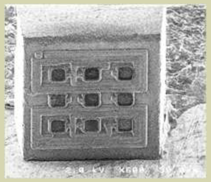
Purpose of this Work

Electronic systems that are relied upon for national security depend on the performance and reliability of highly sophisticated electronic components. However, counterfeit electronics entering the DoD supply chain place our military personnel and our country at risk.

Under DARPA's SHIELD (Supply chain Hardware Integrity for Electronics Defense) Program, SRI International has developed a novel end-to-end solution to secure the electronic component supply chain by using a low-cost identification chip embedded in microelectronic circuit packaging.

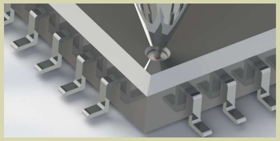


Layout of SHIELD dielet

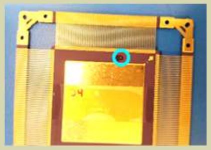


SEM micrograph of dielet

Dielet on nose of Lincoln penny



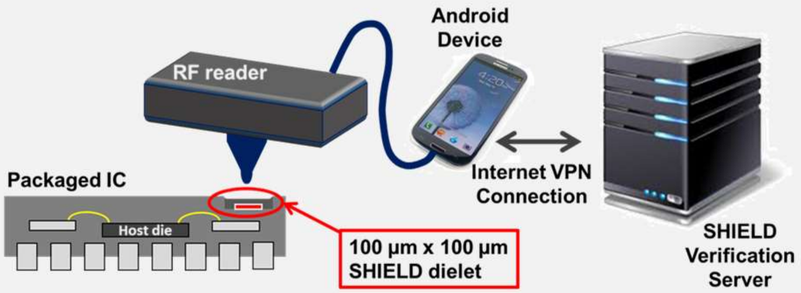
Computer-generated image of dielet being placed into well in QFP package



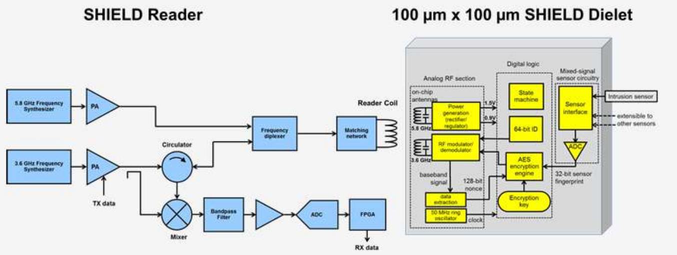
Xilinx FPGA in Kyocera 228-lead QFP package with embedded SHIELD dielet

The SHIELD Dielet:

- Is a passive radio-frequency tag, deriving power from the reader during authentication.
- Uses two on-chip antennas, unlike an conventional radio-frequency ID (RFID) chip, which is attached to an external antenna for power and communication. This allows the dielet to easily be embedded in a host package.
- For unclonability, each dielet has a unique 256-bit secret key and 64-bit ID, programmed into nonvolatile memory at wafer probe, and also enrolled with the remote SHIELD Verification Server.
- Has a full Advanced Encryption Standard (AES) encryption engine for the secure challenge-response transaction.

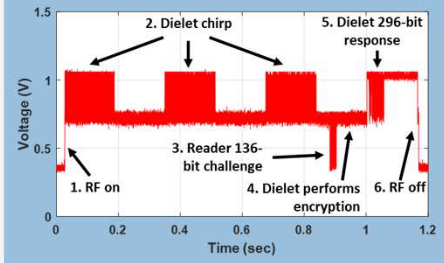


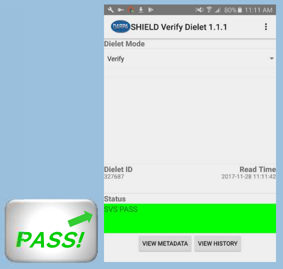
Block Diagram of SHIELD Reader and Dielet



The SHIELD ID chip is referred to as a "dielet" because it is only 100 µm square, smaller than a grain of fine sand. It can be authenticated wirelessly via an RF reader communicating securely over the internet with a remote SHIELD Verification Server, providing a hardware root-of-trust, thus guaranteeing the authenticity of the host IC by making counterfeiting very difficult and prohibitively expensive.

A SHIELD Authentication Transaction





SHIELD Verify Dielet 1.1.1

Dielet Mode
Verify

Dielet ID
327687

Read Time
2017-11-28 11:11:42

Status
SVS PASS

A complete SHIELD authentication transaction, including internet latency, takes only 1-2 seconds.

Analog output of reader demodulator and Android device screenshot during a successful dielet authentication

Contact: michael.kane@sri.com

This research was developed with funding from the Defense Advanced Research Projects Agency (DARPA). The views, opinions and/or findings expressed are those of the author and should not be interpreted as representing the official views or policies of the Department of Defense or the U.S. Government.

Distribution Statement A – Approved for Public Release, Distribution Unlimited

THE ELECTRONICS RESURGENCE INITIATIVE