A Novel Approach to RFID Authentication: The Vera M4H “Unclonable” RFID IC

Presenter:
Vivek Khandelwal,
Vice President of Marketing & Business Development
Agenda

» Company Overview
» PUF Technology Overview
» Unclonable RFIDs
» Summary
Verayo
Verayo

» Focus: Authentication & Security Technology

» Core Technology: “Silicon Biometrics” Technology – Physical Unclonable Functions

» Products: Unclonable RFIDs, Soft PUFs in FPGAs, Secure Processors

» Investors: Khosla Ventures

» Location: San Jose, CA, USA
History

2005 - 2006
- Professor Srini Devadas and Tom Ziola founded PUFCO
- PUFCO gains exclusive license to PUF technology from MIT
- Awarded contract by DARPA
- Funded by Khosla Ventures

2007 - 2008
- Awarded contracts by US DoD Agencies (DTO, US Missile Defense)
- Company renamed as Verayo
- Launched the world’s first unclonable chip – Vera X512H RFID IC

2009 - Now
- Awarded contracts by US DoD (DARPA, AFRL)
- Launched the second unclonable chip – Vera M4H RFID IC
Verayo In The News

Wall Street Journal Tech Innovation Awards 2009

Verayo awarded First Runners-Up in Semiconductor Category

Verayo named “Cool Vendor” in Supply Chain Category

Verayo CTO named in Top 25 CTO’s list by InfoWorld
PUF Technology
**Physical Unclonable Functions (PUF)**

A “silicon biometrics” technology that makes silicon chips “unclonable.”

> Identifies and authenticates **each and every** chip

> Dynamically **generates** unique volatile keys for each chip
Semiconductor chip fabrication process has unavoidable variations. These variations are:

- Unpredictable
- Permanent
- Effectively impossible to clone, even by chip manufacturers

PUFs are tiny electric circuits that exploit these variations to uniquely characterize each chip.

Unique characteristics = “silicon biometrics”

- Used to authenticate chips, generate crypto keys
How PUFs Work

PUF Circuit
Output = function of unique & random silicon fabrication process variations

Input Challenge
(random number)

Output Response = \textit{puf} (challenge, fab. process variations)

» Each PUF generates virtually unlimited number of challenge response pairs that are
  • Unique – same challenge results in different responses from different chips
  • Consistent – same challenge consistently generates a “very similar” response from the same chip

» Unique challenge response pairs = “silicon biometrics” used for authentication
“Unclonable” RFIDs
Vera X512H: World’s First “Unclonable” RFID IC

- PUF Technology
- Networked Authentication
- Pre-Configured Authentication Events
- ISO/IEC 14443-A, 13.56 Mhz
- 56-bit Tag ID
- 512 bit OTP
- Operating Temperature: -25 °C to +85 °C

Launched in Sept 2008
Vera X512H Authentication – Concept

Store “electronic dna samples” of Vera X512H IC in a secure online DB

Scan and compare the IC’s “electronic dna samples” against the ones stored in the database

Online Authentication Service
Vera X512H Product Authentication

Create the Challenge-Response Pair Database

<table>
<thead>
<tr>
<th>Serial # 5789256781</th>
<th>RFID Tag # 48793570</th>
</tr>
</thead>
<tbody>
<tr>
<td>Challenge</td>
<td>Response</td>
</tr>
<tr>
<td>11028490</td>
<td>89532973</td>
</tr>
<tr>
<td>46298504</td>
<td>34769145</td>
</tr>
<tr>
<td>….</td>
<td>….</td>
</tr>
</tbody>
</table>

Compare Response Against Challenge-Response Pairs in DB

Get Response for the Challenge from PUF on RFID Tag

Challenge = 11028490

Response

Result
Vera M4H:
Next Gen “Unclonable” RFID IC

- PUF Technology
- Local (Standalone) Authentication
- Unlimited Authentication Events
- ISO/IEC 14443-A, 13.56 Mhz
- 56-bit Tag ID
- 2K bit OTP User Memory
- Operating Temperature: -25 °C to +85 °C
Vera M4H RFID IC – A Novel Approach to RFID Authentication

Extract, encrypt and store the “genetic code” of the Vera M4H IC on the IC itself

Reader decrypts the “genetic code” of Vera M4H IC, interrogates the IC to prove it is authentic

“genetic code” = information on chip’s unique, unclonable fabrication variations

Based on “silicon biometrics”, a low cost alternative to cryptography based solutions
Vera M4H Provisioning

1. Chip-unique PUF parameters – information on each chip’s unique fabrication process variations – are extracted. Chip is disabled from emitting these parameters again.

2. On an external PC or server, PUF parameters are encrypted using user’s key.

3. Encrypted PUF parameters are stored back on the chip’s memory (OTP).

At a Trusted Location:
On wafer (on tester) or RFID tag provisioning
Vera M4 Authentication
Unlimited Local (Offline) Authentication Events

Vera M4H Based Ticket

1. Send encrypted PUF parameters
2. Send $Q_R = PUF(N_R)$ to reader

Secure RFID Reader

1. Decrypt PUF parameters
2. Send nonce $N_R$ to M4H IC
3. Calculate $Q_R = f(N_R, PUF$ data)
4. Compare $Q_R$ from M4H IC to authenticate

Encrypted PUF Parameters

Nonce $N_R$
How is it Unclonable?

Copy one chip's data to another

Ghost device

Response 75407896

Challenge 14703455

RF Front End

PUF

TID: 12345678

PUF Pams

User Memory

Response ?????

Challenge 14703455

RF Front End

PUF

TID: 12345678

PUF Pams

User Memory

Copy one chip's data to another

Ghost device
Comparison with Crypto Authentication

» **PUF Based RFIDs**
  - Unclonable – effectively impossible to create clone
  - Root of trust – the silicon
  - Authentication logic – tiny PUF circuit, no secure memory – simple/inexpensive

» **Crypto RFIDs**
  - Anti-cloning – depends on security of the stored key
  - Root of trust – stored key
  - Authentication logic - crypto logic, secure memory – complex/expensive
Verayo RFID Advantages

<table>
<thead>
<tr>
<th>Advantage</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unclonable</td>
<td>Effectively impossible to clone the RFID chip</td>
</tr>
<tr>
<td>Strong &amp; Robust Authentication</td>
<td>Authentication based on silicon signatures</td>
</tr>
<tr>
<td>Low Cost</td>
<td>Tiny PUF circuit consumes small die area</td>
</tr>
<tr>
<td>Low Power Consumption</td>
<td>Requires no crypto computation</td>
</tr>
</tbody>
</table>
New RFID Technology Landscape

- **Verayo RFIDs**
  - Authentication Strength: High
  - Cost & Complexity: Low

- **Crypto RFIDs**
  - Authentication Strength: Low
  - Cost & Complexity: High
## “Unclonable” RFID Product Roadmap

<table>
<thead>
<tr>
<th></th>
<th>Features</th>
<th>X512H</th>
<th>M4H</th>
<th>M1HW</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>RF Interface</td>
<td>HF</td>
<td>HF</td>
<td>HF</td>
</tr>
<tr>
<td>2</td>
<td>Standard</td>
<td>ISO 14443-A</td>
<td>ISO 14443-A</td>
<td>ISO 14443-A</td>
</tr>
<tr>
<td>3</td>
<td>Tag ID (or UID)</td>
<td>56b</td>
<td>56b</td>
<td>56b</td>
</tr>
<tr>
<td>4</td>
<td>User Memory</td>
<td>512b OTP</td>
<td>2K OTP</td>
<td>1K RW</td>
</tr>
<tr>
<td>5</td>
<td>Number of Authentication Events</td>
<td>Pre- Provisioned</td>
<td>Unlimited</td>
<td>Unlimited</td>
</tr>
<tr>
<td>6</td>
<td>Type of Authentication</td>
<td>IC only</td>
<td>IC only</td>
<td>Mutual</td>
</tr>
<tr>
<td>7</td>
<td>Mode of Operation</td>
<td>Networked</td>
<td>Standalone/ Networked</td>
<td>Standalone/ Networked</td>
</tr>
</tbody>
</table>
# PUF Based RFID Use Cases

<table>
<thead>
<tr>
<th>#</th>
<th>Applications</th>
<th>X512H</th>
<th>M4H</th>
<th>M1HW</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Product Authentication</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>2</td>
<td>Access Control</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>3</td>
<td>Transit – Daily Tickets</td>
<td></td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>4</td>
<td>Transit – Month/Year Passes</td>
<td></td>
<td></td>
<td>✔</td>
</tr>
<tr>
<td>5</td>
<td>Payment Cards</td>
<td></td>
<td></td>
<td>✔</td>
</tr>
<tr>
<td>6</td>
<td>Secure IDs</td>
<td></td>
<td></td>
<td>✔</td>
</tr>
<tr>
<td>7</td>
<td>Supply Chain Applications</td>
<td></td>
<td></td>
<td>✔</td>
</tr>
</tbody>
</table>
Summary
Summary

PUFs enable “silicon biometrics” based RFID Authentication

PUF based RFID:

» Secure & Reliable
  • Based on unclonable silicon signatures

» Simple & Efficient
  • Strong authentication protocol

» Low Cost, Consume Low Power
  • Smaller chip die area
Thank You!

Contact the Verayo team
» Email: vkhandelwal@verayo.com
» Web: www.verayo.com