

Verayo

Introduction to Verayo

Agenda

- » **Company Overview**
- » **PUF Technology Overview**
- » **Unclonable RFIDs**
- » **RFID PUF Test Results**
- » **Summary**

Company Overview

Verayo

Verayo is a Silicon Valley start-up bringing to market a range of security solutions based on a breakthrough technology, invented at MIT, called Physical Unclonable Functions (PUF). PUF is a “silicon biometrics” technology, a type of electronic DNA or fingerprinting technology for silicon chips.

Team

Executive Team	Anant Agrawal, CEO Former VP & GM of Sun's Microprocessor Division. Founding CEO of Insilica, a fabless semiconductor company.
	Dr. Srinivasa Devadas, Co-Founder & CTO Associate head of Electrical Engineering & Computer Science at MIT. Inventor of PUF technology. Research focus – computer architecture, security, VLSI.
Investor	Vinod Khosla – Khosla Ventures Founding CEO of Sun Microsystems. Partner at Kleiner Perkins Caufield & Byers. Leading investor in computer and green technology companies.
Advisors	Dr. Taher Elgamal Leading expert in computer security. Inventor of SSL, cryptography algorithms. CTO of Tumbleweed. Former CTO of Netscape.
	Fred Weber President & CEO of MetaRAM, a semiconductor start-up focused on memory subsystems. Former CTO of AMD, helped bring Athlon, Opteron processors to market.
	Tom Ziola, Co-Founder Former VP & GM of MSN-TV at Microsoft. Former EIR at Kleiner Perkins.

History

2005

- Srini and Tom found PUFCO. PUFCO gains exclusive license to PUF technology from MIT. Gets funded by Khosla Ventures.

2006

- Awarded Contract by DARPA.

2007

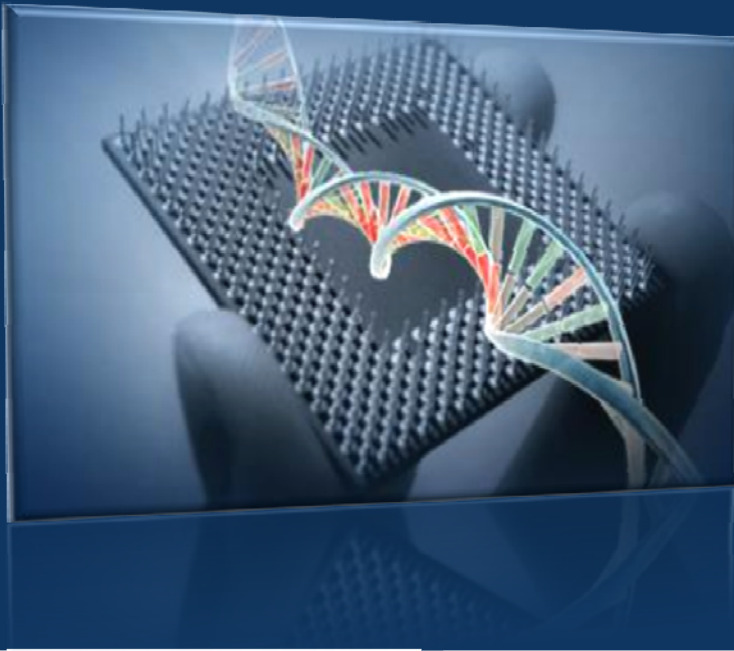
- Awarded Contracts by USDoD Agencies (DTO, US Missile Defense).
- Prototyped, Tested PUF-based RFID for Anti-Counterfeiting.

2008

- Company renamed as Verayo
- Developed PUF RFID for Commercial Markets

Technology Overview

Physical Unclonable Functions (PUF)



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

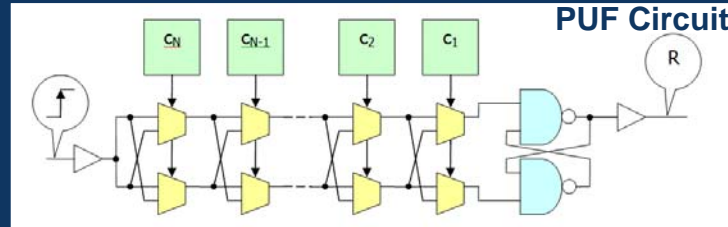
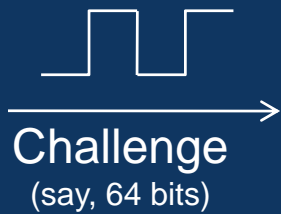
- » Identifies and authenticates each and every chip
- » Dynamically generates virtually unlimited number of unique volatile keys for each chip

Concept



- » 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



- » PUFs circuits are fabricated identically on all chips
- » 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 the same response from the same chip
- » Unique challenge response pairs = “electronic fingerprints” used for authentication, crypto key generation

PUF Products & Markets

Authentication

» **RFID PUFs (contactless)**

- Luxury Products
- Pharmaceutical Products
- DMV/Travel Cards
- Currency Notes
- Passports

» **Embedded PUFs (contact)**

- DMV Cards
- Computer, Networking, Electronic Gear

Crypto Platforms

» **CryptoPUF**

- Smart Cards
- NFC Cards
- GSM, WiMAX, LTE

» **Secure Processor**

- Servers/PC
- Mobile Platform

Unclonable RFIDs

Unclonable RFIDs

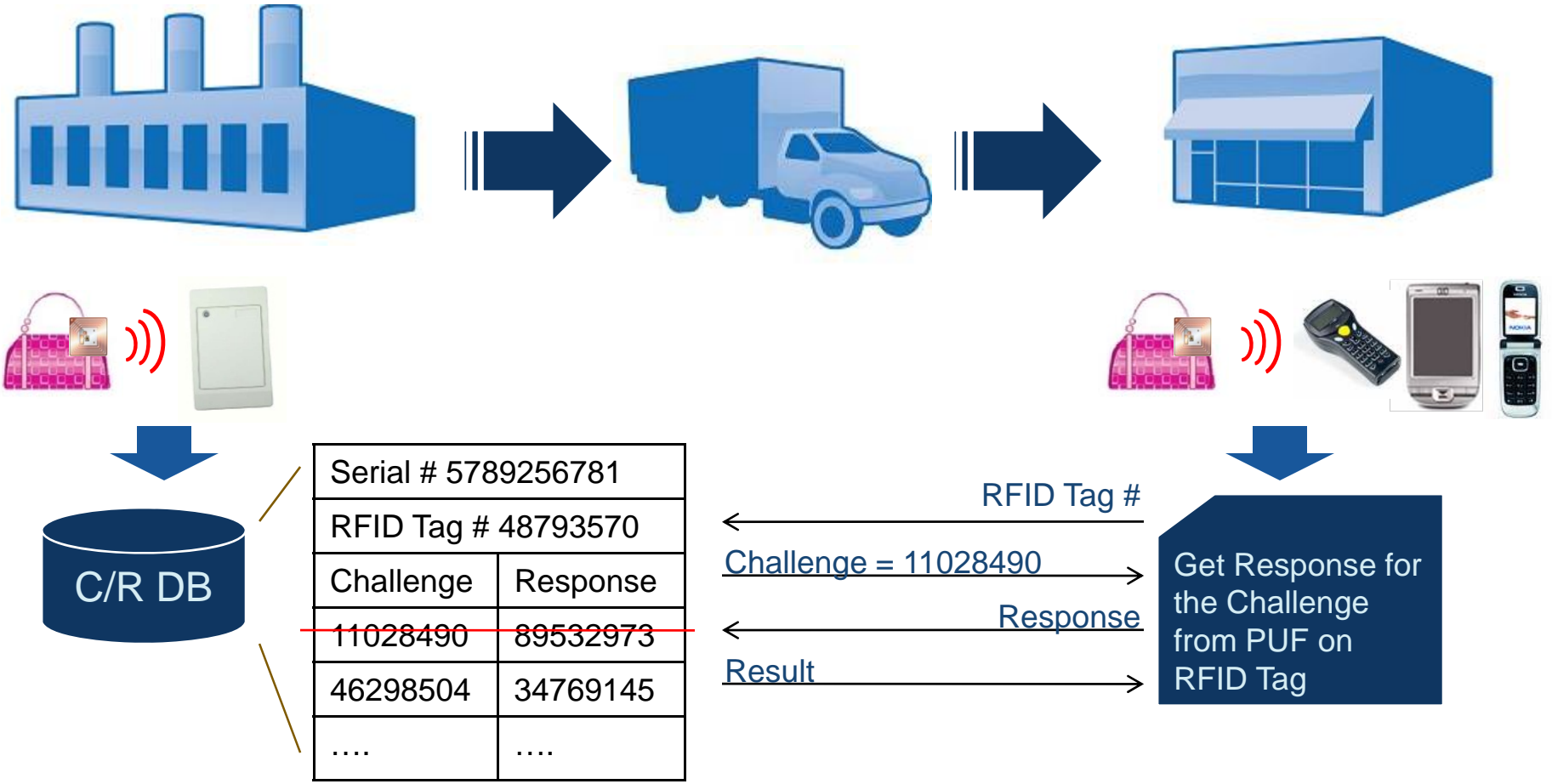
PUF



Passive: LF, HF, UHF
Semi-Passive
Active

- » Tiny PUF circuit is added to a regular RFID chip
 - Works like a standard RFID chip
 - PUF is activated only for authentication
- » PUF enhances regular RFIDs
 - Makes each RFID chip unique and unclonable
 - Enables a strong and robust authentication mechanism
- » Cost-effective security solution for
 - Anti-counterfeiting
 - Secure IDs and access cards

PUF based RFID Authentication



Create the Challenge-Response Pair Database

Compare Response Against Challenge-Response Pairs in DB

PUF RFID Advantages

Unclonable

- No one can clone the RFID chip

Strong & Robust Authentication

- Unlimited number of challenge-response pairs
- Each challenge response pair used once
- Prevents skimming and replay attacks




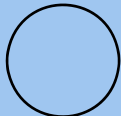





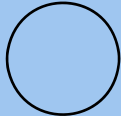


Low Cost

- Tiny PUF circuit consumes small die area

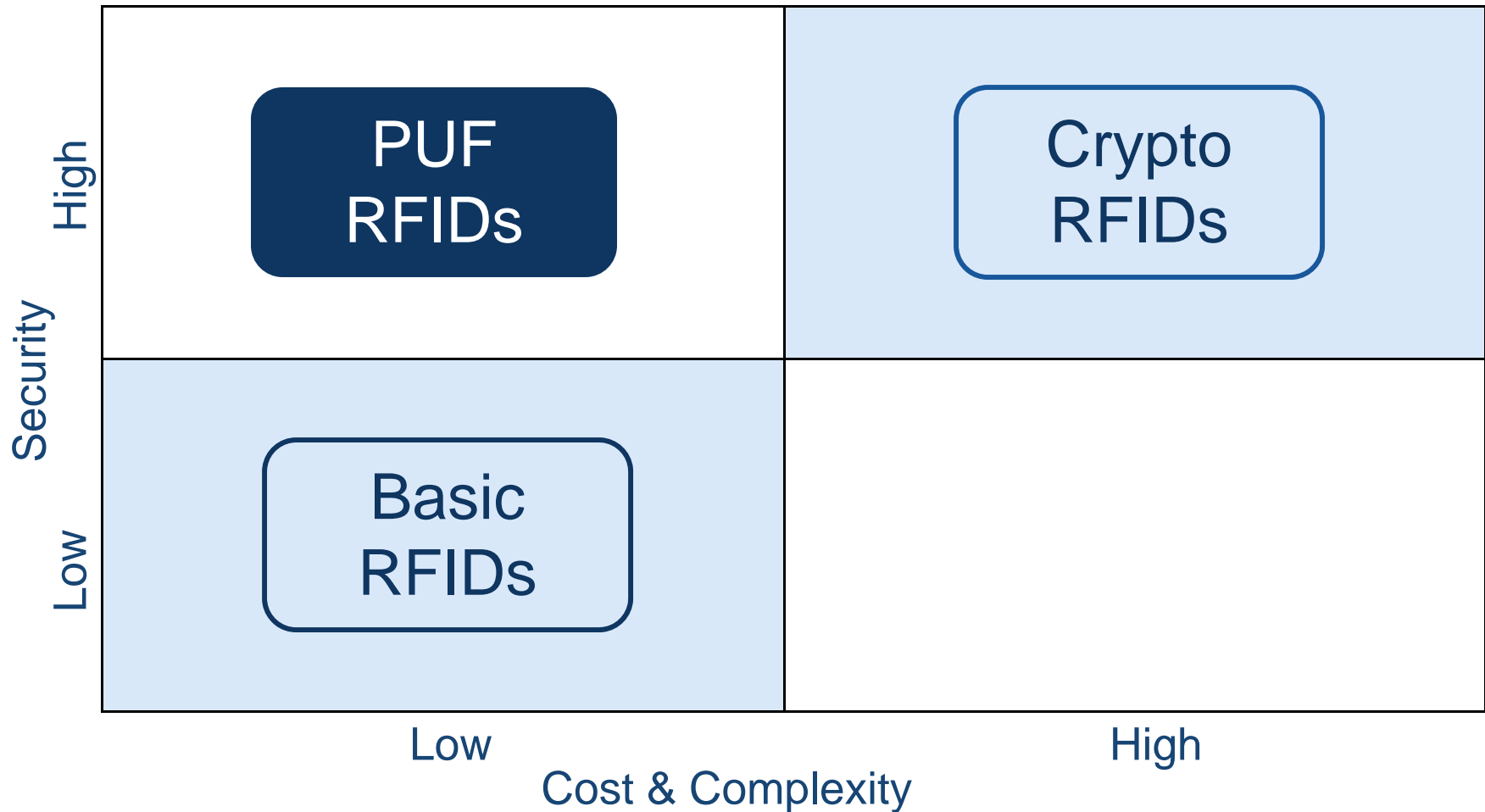
Low Power Consumption

- Requires no crypto computation

PUF RFIDs - Feature Comparisons

Feature	Basic RFIDs	PUF based RFIDs	Crypto RFIDs
Anti-Cloning			
Data Protection – Side channel, replay attacks			
Tag Authentication			
Secure Communication			

PUF RFIDs vs. Others



PUF Test Data & Results

RFID PUF Test – Parameters & Conditions

False Negative

Erroneous rejection of an authentic device
(Intra Chip Variations)

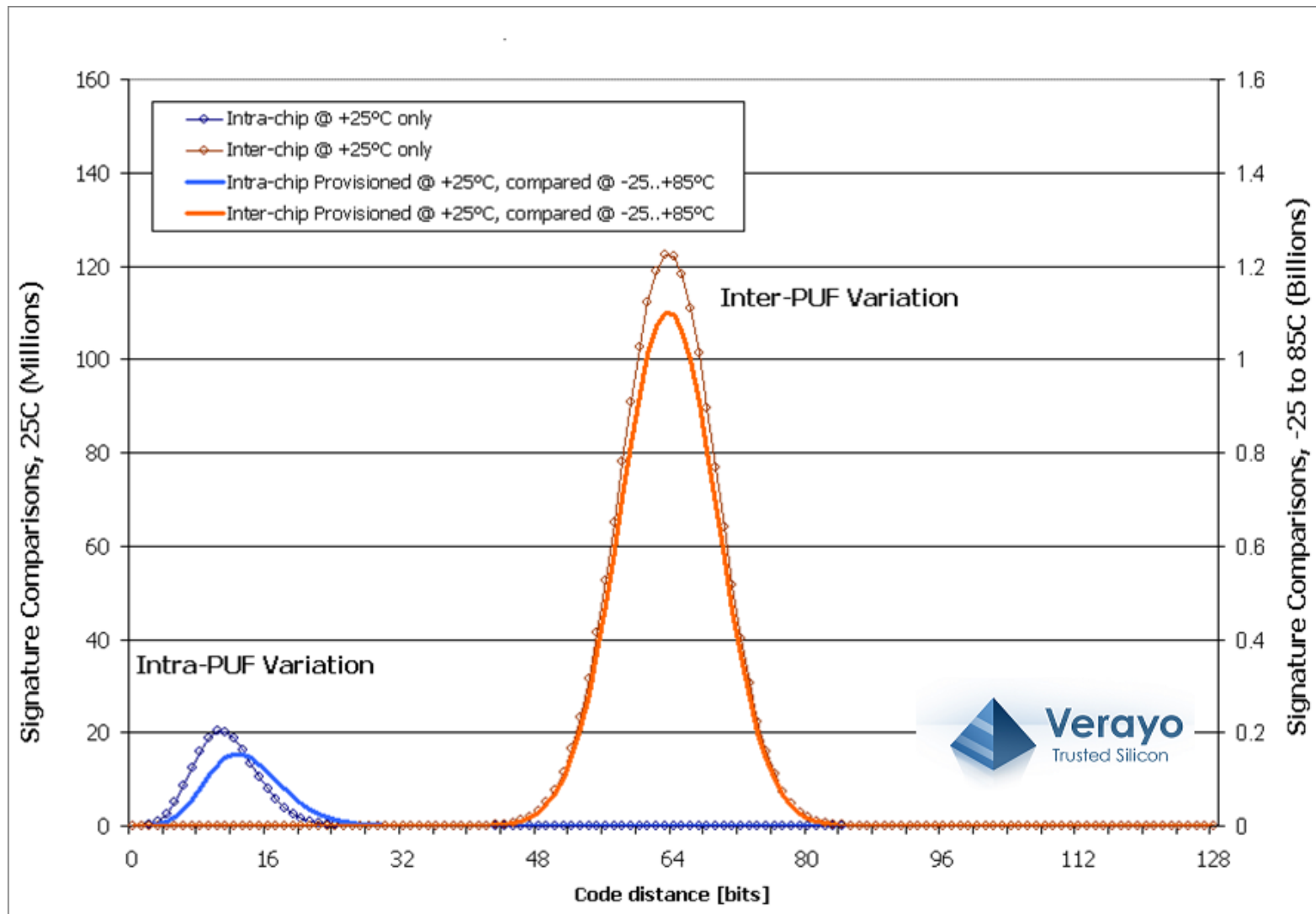
False Positive

Erroneous authentication of an imposture device
(Inter Chip Variations)

Temperature Range: -25°C to +85°C

- » C/R database created at different temperatures
- » C/R authentication done at different temperatures
- » Corner cases (low/high temp) included

Code Distance Characteristic



Summary

Summary

PUF – a breakthrough semiconductor security technology

PUFs make RFID chips

- » Unclonable
- » Enable a simple, strong and robust authentication scheme
- » Highly reliable across environmental conditions
- » Higher security at low cost, low power consumption

Thank You