There is no free Trust ...

Pim Tuyls, CEO and Founder Intrinsic ID

June 1, 2017
Intrinsic ID Company Overview

• Corporate Identity
  • Spin-out of Philips security 2008
  • Sunnyvale HQ, Eindhoven R&D, sales in Seoul and Tokyo
  • Independent company with venture capital funding

• World-leading Authentication Company
  • Leader in SRAM PUF (Physical Unclonable Functions)
    • #1 in patents, #1 in design wins, #1 in deployed products
  • Most scalable, robust, and secure implementation of SRAM PUF
  • Most experienced SRAM PUF engineering team

2016 Winner EU Innovation Radar Prize
Intrinsic ID: Security Solutions for IoT

- **HW based Security** — In-line with the strategic principles for IoT of US Department of Homeland Security
- **Low Cost** — Low footprint SW and HW products fit into the smallest, resource constrained devices
- **Available** — Can be implemented on almost all MCUs, sensors, flash devices, …
- **Flexible** — Keys can be provisioned at any point in the supply chain
SRAM PUF Keys from Silicon Characteristics

1. **Process Variation**
   Deep sub-micron variations in the production process give every transistor slightly random electric properties.

2. **SRAM Start-up Values**
   When the SRAM is powered on, this randomness is expressed in the start-up values (0 or 1) of SRAM cells.

3. **Silicon Fingerprint**
   The start-up values create a highly random and repeatable pattern that is unique to each chip.

4. **SRAM PUF Key**
   The silicon fingerprint is turned into a secret key that builds the foundation of a security subsystem.

**SRAM PUF Benefits**
- Device-unique, unclonable fingerprint
- Leverages entropy of mfg. process
- No key material programmed
Leadership
SRAM PUF ≠ PUF

Intrinsic ID
- Based on standard 6T SRAM
- Little to no dependency on process
- Available
- Reliable

- Measures resistance in modified silicon
- Requires silicon change
- Susceptible to temperature/voltage

- Also called ring oscillator
- Requires silicon change
- Scalability challenges across mfg nodes
SRAM PUF Silicon Key Products

**CREATE. WRAP. MANAGE.**

**QUIDDIKEY**
- Hardware IP
- Delivered as RTL
- 12 - 50K Gates
- 500B - 1KB SRAM
- 100K Cycle Speed
- Embedded at Fab

**BROADKEY**
- Software IP
- Delivered as Libraries
- 8 - 25KB Code Size
- 500B - 1KB SRAM
- 500K Cycle Speed
- Portable Across MCUs
- In-field Retrofitting
CREATE. WRAP. MANAGE.
PUF-based secret keys

<table>
<thead>
<tr>
<th>Software IP</th>
<th>Key Entropy</th>
<th>Footprint</th>
<th>PUF SRAM</th>
<th>Reconstruction Speed</th>
</tr>
</thead>
<tbody>
<tr>
<td>BROADKEY - LIGHT</td>
<td>Device-unique key creation</td>
<td>128 bits 8 KB*</td>
<td>0.5 KB</td>
<td>0.5M Cycles</td>
</tr>
<tr>
<td></td>
<td></td>
<td>128 bits 15 KB</td>
<td>0.5 KB</td>
<td>0.5M Cycles</td>
</tr>
<tr>
<td></td>
<td></td>
<td>256 bits 15 KB</td>
<td>1.0 KB</td>
<td>0.6M Cycles</td>
</tr>
<tr>
<td>BROADKEY - FLEX</td>
<td>Device-unique key creation, derivation, wrapping and management</td>
<td>128 bits 20 KB</td>
<td>0.5 KB</td>
<td>0.6M Cycles</td>
</tr>
<tr>
<td></td>
<td></td>
<td>256 bits 20 KB</td>
<td>1.0 KB</td>
<td>0.7M Cycles</td>
</tr>
<tr>
<td>BROADKEY - FLEX-E</td>
<td>BROADKEY-Flex including elliptic curve private key generation</td>
<td>128 bits 25 KB</td>
<td>0.5 KB</td>
<td>0.7M Cycles</td>
</tr>
<tr>
<td></td>
<td></td>
<td>256 bits 25 KB</td>
<td>1.0 KB</td>
<td>0.8M Cycles</td>
</tr>
</tbody>
</table>

Software IP delivered as library compiled for specific target chip, including interface specification and user manual

* Trimmed down version, reconstruction only
Reference on ARM Cortex M3 in software, other optimizations possible
Behavior of SRAM PUF

Noise at Room Temp: typically 6%
Lifetime: 25+ Years!

- **High V, High T**
  - Noise increases up to 15%
  - Noise reduces below 10%
  - Start of anti-ageing
  - No anti-ageing applied
- **burn-in at high V and T**

© Intrinsic ID | Confidential
Today we launch ...
SRAM PUF-based Authentication solutions from Intrinsic ID
SPARTAN-CLOUD Authentication Protocol

- **MCU**
  - Application
  - MQTT client lib.
  - SPARTAN-CLOUD library
    - BROADKEY Flex-E
  - AC
  - Cert
  - TLS library
  - SRAM
  - OTP
  - PUF

- **Cloud Connection Service** (MQTT/TLS)
  - Public Key
  - Device Unique Certificate
  - Provisioning PC

Authenticate Everything © Intrinsic ID | Confidential
Authenticate Everything
It is happening ...
And Save the Date ...

Fall Security Summit
October 23, 2017
Silicon Valley
Thank You!

Pim Tuyls, CEO
Email@Intrinsic-ID.com
408.933.9980
www.intrinsic-id.com