Andes and PUFsecurity Webinar

24 Feb 2022
Today’s Speakers

- **John Min** is Director of Field Application Engineering at Andes USA. He has extensive background in Processing – CPU, DSP and ASIC. Prior to Andes, John spent last 20 years in Processor companies like SiFive, MIPS and ARC in various technical roles. Prior to that, he worked in consumer electronics at LG and HP. John has multiple degrees from University of Southern California.
Andrew Intro

• **Andrew Irvin**, Chairman's office of eMemory and PUFsecurity

15+ years experience across three continents in Sales, Marketing, and Project Management. Originally from the United Kingdom and is a graduate from Edinburgh University. He is also licensed Architect and oversaw the design and construction of serval large building projects in China and Europe prior to moving into the semiconductor industry.
Andes Technology Corporation

Who We Are

- CPU: Pure-play CPU IP Vendor
- 16-year-old Public Company
- RISC-V Founding Premier Member
- RISC-V Ambassador Running Task Groups
- Board of Directors
- Major Open-Source Contributor/Maintainer

Quick Facts

- 100+ years
  CPU Experience in Silicon Valley
- 80+% Engineers
- 250+ Licensees
- 20K+ AndeSight IDE installations
- ~10B (Q4/21) Total shipment of Andes-Embedded™ SoC
- Global Presence
Large Range of Andes Processors

Application
Multicores

Application

DSP/
SIMD/
Vector

Controller

2-stage

5-stage

>3.53 Coremark/MHz

Memboost
Enhance memory

8-stage

>5.50 Coremark/MHz

AX25MP
A25MP
A25

AX25

AX27
A27

NX27V

D25F

NX25F

N22
N25F

AX45MP
A45MP
A45

AX45

D45F

NX45F

N45F

A25MP
AX25MP
A25MP
A25

AX25

AX27
A27

NX27V

D25F

NX25F

N22
N25F

AX45MP
A45MP
A45

AX45

D45F

NX45F

N45F

A25MP
AX25MP
A25MP
A25

AX25

AX27
A27

NX27V

D25F

NX25F

N22
N25F

AX45MP
A45MP
A45

AX45

D45F

NX45F

N45F

A25MP
AX25MP
A25MP
A25

AX25

AX27
A27

NX27V

D25F

NX25F

N22
N25F

AX45MP
A45MP
A45

AX45

D45F

NX45F

N45F

A25MP
AX25MP
A25MP
A25

AX25

AX27
A27

NX27V

D25F

NX25F

N22
N25F

AX45MP
A45MP
A45

AX45

D45F

NX45F

N45F

A25MP
AX25MP
A25MP
A25

AX25

AX27
A27

NX27V

D25F

NX25F

N22
N25F

AX45MP
A45MP
A45

AX45

D45F

NX45F

N45F

A25MP
AX25MP
A25MP
A25

AX25

AX27
A27

NX27V

D25F

NX25F

N22
N25F

AX45MP
A45MP
A45

AX45

D45F

NX45F

N45F

A25MP
AX25MP
A25MP
A25

AX25

AX27
A27

NX27V

D25F

NX25F

N22
N25F

AX45MP
A45MP
A45

AX45

D45F

NX45F

N45F

A25MP
AX25MP
A25MP
A25

AX25

AX27
A27

NX27V

D25F

NX25F

N22
N25F

AX45MP
A45MP
A45

AX45

D45F

NX45F

N45F

A25MP
AX25MP
A25MP
A25

AX25

AX27
A27

NX27V

D25F

NX25F

N22
N25F

AX45MP
A45MP
A45

AX45

D45F

NX45F

N45F

A25MP
AX25MP
A25MP
A25

AX25

AX27
A27

NX27V

D25F

NX25F

N22
N25F

AX45MP
A45MP
A45

AX45

D45F

NX45F

N45F
Andes RISC-V Adoption

Renesas: ASSP MCU with configurable V5 cores
- Scalable/configurable performance
- Selectable safety features
- Customization options
- Feature-rich AndeSight IDE

Telink: IoT and Wireless Audio with D25F embedded
- Strong integer/DSP performance
- Efficient small data processing
- Good development tools

Picocom: 5G Open RAN small cells

AI Accelerators for Servers with >10 NX27V Cores
- RVV with 512-bit VLEN/SIMD
- Custom instructions
- LLVM compiler
Securing Andes RISC-V with PUFsecurity
Agenda

1. Company Profile
2. Securing the Future of Computing
3. The Four Fundamentals of Chip Security
4. PUF-based Solutions with Andes RISC-V
World’s Largest Pure-Play eNVM Provider

**ememory**

- **22 Years**
  - In the IP business
  - Based in Taiwan

- **990+**
  - International
  - Patents Issued

- **5,850+**
  - Customer
  - Tape-Outs

- **1.8M+**
  - Wafers shipped quarterly

- **40M+**
  - Wafers shipped to date

Subsidiary Dedicated to PUF-based Security IP

**PUFsecurity**

- **300+**
  - Employee Pure IP Company

- **70%**
  - IP Developers

- **17 Years**
  - Consecutive Growth

- **$84M+**
  - Annual Revenue

- **12 Years**
  - Consecutive TSMC IP Partner Award

- **Consecutive Growth**

- **World’s Largest**
  - Pure-Play eNVM Provider

- **Subsidiary Dedicated to**
  - PUF-based Security IP

- **Customer Tape-Outs**

- **Wafers shipped quarterly**

- **Wafers shipped to date**

- **Based in Taiwan**

- **International Patents Issued**

- **Employee Pure IP Company**

- **Annual Revenue**

- **Consecutive TSMC IP Partner Award**
Quantum Tunneling PUF

Provides unique ID for each chip and the necessary hardware ‘Root of Trust’ to achieve high security solutions whilst also eliminating the need for additional processes.

Logic Non-Volatile Memory

Provides embedded logic NVM solutions, including both OTP and MTP to improves yield, performance, and flexibility in product development and production.

Unique Contribution to the Industry

Invention of Logic Non-volatile OTP Memory

Invention of Logic Non-volatile MTP Memory

Invention of Logic Chip Fingerprint Quantum Tunneling PUF

PUF

Physically Unclonable Function

A chip fingerprint for silicon
# Widely Available Security IPs

<table>
<thead>
<tr>
<th></th>
<th>0.15 μm</th>
<th>0.13 μm</th>
<th>0.11 μm</th>
<th>90 nm</th>
<th>80 nm</th>
<th>65 nm</th>
<th>55 nm</th>
<th>40 nm</th>
<th>28 nm</th>
<th>16 nm</th>
<th>14 nm</th>
<th>12 nm</th>
<th>7 nm</th>
<th>6 nm</th>
<th>5 nm</th>
<th>4 nm</th>
<th>3 nm</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>FinFET</strong></td>
<td>□</td>
<td></td>
<td></td>
<td>□</td>
<td></td>
<td>□</td>
<td></td>
<td>□</td>
<td></td>
<td>□</td>
<td></td>
<td>□</td>
<td>□</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>FDX/HPC/HPC+</strong></td>
<td>□</td>
<td></td>
<td></td>
<td>□</td>
<td></td>
<td>□</td>
<td></td>
<td>□</td>
<td></td>
<td>□</td>
<td></td>
<td>□</td>
<td>□</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Mixed Signal</strong></td>
<td>□</td>
<td></td>
<td></td>
<td>□</td>
<td></td>
<td>□</td>
<td></td>
<td>□</td>
<td></td>
<td>□</td>
<td></td>
<td>□</td>
<td>□</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Logic (Generic/LP)</strong></td>
<td>□</td>
<td></td>
<td></td>
<td>□</td>
<td></td>
<td>□</td>
<td></td>
<td>□</td>
<td></td>
<td>□</td>
<td></td>
<td>□</td>
<td>□</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>HV (Driver)</strong></td>
<td>□</td>
<td></td>
<td></td>
<td>□</td>
<td></td>
<td>□</td>
<td></td>
<td>□</td>
<td></td>
<td>□</td>
<td></td>
<td>□</td>
<td>□</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>BCD (PMIC)</strong></td>
<td>□</td>
<td></td>
<td></td>
<td>□</td>
<td></td>
<td>□</td>
<td></td>
<td>□</td>
<td></td>
<td>□</td>
<td></td>
<td>□</td>
<td>□</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>ULP/ULL</strong></td>
<td>□</td>
<td></td>
<td></td>
<td>□</td>
<td></td>
<td>□</td>
<td></td>
<td>□</td>
<td></td>
<td>□</td>
<td></td>
<td>□</td>
<td>□</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>eFlash (eFlash ULP)</strong></td>
<td>□</td>
<td></td>
<td></td>
<td>□</td>
<td></td>
<td>□</td>
<td></td>
<td>□</td>
<td></td>
<td>□</td>
<td></td>
<td>□</td>
<td>□</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Automotive</strong></td>
<td>□</td>
<td></td>
<td></td>
<td>□</td>
<td></td>
<td>□</td>
<td></td>
<td>□</td>
<td></td>
<td>□</td>
<td></td>
<td>□</td>
<td>□</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>DRAM</strong></td>
<td>□</td>
<td></td>
<td></td>
<td>□</td>
<td></td>
<td>□</td>
<td></td>
<td>□</td>
<td></td>
<td>□</td>
<td></td>
<td>□</td>
<td>□</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>CIS</strong></td>
<td>□</td>
<td></td>
<td></td>
<td>□</td>
<td></td>
<td>□</td>
<td></td>
<td>□</td>
<td></td>
<td>□</td>
<td></td>
<td>□</td>
<td>□</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- **Qualified/Production**
- **Verified/Developing**

Kickoff in 2022

- NeoPUF adopts the same technology, programming mechanism, and bit cell as NeoFuse
- Qualified NeoFuse stands for NeoPUF and PUF-based IPs readiness
Hackers Remotely Kill a Jeep on the Highway
Sparking a 1.4 million vehicle recall by Chrysler, marking the start of the age of hackable vehicles.

Link

IoT Security Camera hacking demonstration on YouTube
Step by step guides for hacking IoT devices are widely available online.

Link

Colonial Pipeline pay $4.4m to end ransomware attack
ending the massive shutdown of approximately half of the USA’s East Coast fuel supply

Link
Hardware Attacks are Today Reality

De-cap
E-fuse keys stolen

Fault Injection
Espressif WiFi-IoT Chip Hacked

Differential Power Analysis
STM MCU AES key found

- Secure Storage needed
- ESP32-S2 will ECO soon
- Countermeasures needed

Invisible OTP

Side Channel Attack Protection / Anti-Tampering Design
Securing the Future of Computing

AVERAGE LIFESPAN
(Chip Application by year)

Industrial
Automotive
Appliances
Servers
Smart Phones
Consumer Electronics

Source: https://semiengineering.com/making-chips-to-last-their-lifetime/

Privacy and safety need to be built into the metaverse from day one.

Mark Zuckerberg
Meta. 2021
### The Security Ecosystem’s Weakest Link

#### SECURITY SYSTEM BY COMPUTING LAYER
(and Example Protection Approach)

<table>
<thead>
<tr>
<th>Software</th>
<th>Hardware</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application</td>
<td>Cryptographic Engine</td>
</tr>
<tr>
<td>Operating System</td>
<td>- Ex. Hardware Crypto Engine, Secure BUS and Keys</td>
</tr>
<tr>
<td>Firmware</td>
<td>Root of Trust</td>
</tr>
<tr>
<td></td>
<td>- Unknown Key (PUF), Secure Storage (OTP)</td>
</tr>
</tbody>
</table>

#### Software
- https:// for Security
- Constantly needs upgrades
- Never know if it is booted from genuine firmware
- Can be Hardware Root of Trust when well designed

#### Hardware
- Software patches can be applied when being hacked
- Hardware tape-out needed when being hacked
How **Chips Boot Up** is Key to Security

1st Generation
Conventional Booting

- Flash (code)

2nd Generation
Improved Booting

- Flash (encrypted code)

3rd Generation
Secure Booting

- Flash (encrypted code)

System on Chip

- Injected Key (OTP/eFuse)

ROM code + OTP code + OTP key + Signing

Verify
Secure Boot Flow (Hardware and Software)

1. **ROM**
   - First Boot load normally in ROM code (security)
   - Regulations

2. **OTP**
   - Preferred in OTP code (flexibility, ~ few k Bytes)
   - Security

3. **Operating System**
   - Applications
     - Application 01
     - Application 02
     - Application 03
     - ... Application 99

4. **Unique Identity**
   - Authentication needed in SW application
   - Key Storage

- **Key Generation**
  - How is this Root Key Generated?

- **Isolation Encryption**

- **PUF-based** solution can solve all these 4 fundamental problems

- **ROM**
- **OTP**
- **Operating System**
- **Unique Identity**

- **Key Storage**: Where you store this Root Key?
- **Key Generation**: How is this Root Key Generated?

- **Verify**: Key ➔ Decrypt
- **Verify**: Key ➔ Decrypt
- **Verify**: Key ➔ Decrypt
The Four Fundamentals of Chip Security

1. OTP for Boot Code
2. Root Key Storage
3. Root Key Generation
4. Unique Unclonable Identification
Physical Invisibility Top View via SEM

**e-Fuse** (Electrical Fuse)

**anti-Fuse** (NeoFuse/NeoPUF)

**eFuse OTP**
No PUF-based Storage

- OTP address can be easily located

**Secure OTP**
With NeoPUF Protection

- Different Physical location for each chip
### Root Key Generation

#### Injected Root Key
(Serial Identification)

- Initial injection required
- Key Injection must be done during CP/FT
- Secure room (audit) needed
- Extra $0.5~$2 per unit cost

#### Inborn Root Key
(PUF-based Identification)

- Inborn, unique, unclonable ID
- Provides zero-touch / zero-trust
- Private key from PUF never exposed outside SOC

---

**Key Management**
- External Random Number Generator
- Key Database

**Automatic Test Equipment**

**Digital Key Injection**

**NVM**

**PUF**

**Injected Root Key**
(Serial Identification)

**Inborn Root Key**
(PUF-based Identification)
### Security Subsystem

<table>
<thead>
<tr>
<th>Analog Macro (process dependent)</th>
<th>Digital IP (process independent)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Anti-Tamper Design</td>
<td>Secure CPU</td>
</tr>
<tr>
<td>TRNG (entropy)</td>
<td>HASH Crypto</td>
</tr>
<tr>
<td>OTP (Secure Storage)</td>
<td>Symmetric Crypto</td>
</tr>
<tr>
<td>PUF (Chip Fingerprint)</td>
<td>Asymmetric Crypto</td>
</tr>
</tbody>
</table>

**Security systems rely on OTP Memory**

**Secure OTP is replacing eFuse**

**Crypto engines require TRNG**

**TRNG is digital + analog**

**External Key injection is expensive**

**PUF has zero-touch provisioning**

**PUF / OTP / TRNG / Anti-tampering combined into one single Hardware Root of Trust IP is Ideal**
**PUF-based Security Solutions for RISC-V**

**PUFrt**: Secure Storage (OTP) + Inborn ID / Key (PUF) + Randomness (TRNG) + Anti-Tampering + 3rd party security lab certification

**PUFcc**: PUFrt + Anti-tampering & NIST-certified Crypto Coprocessor + Secure Enclave (Boundary)
FPGA Demonstration
by integrating RISC-V (ANDES) and PUFcc (PUFsecurity)

- **On-chip Inborn HUK**: Saving provisioning cost
- **Secure boot using PUFcc**: Paired SoC and FW to protect from HW/SW counterfeiting
Total Solutions for Hardware Security

Secure OTP
for Key Storage & Boot code

PUF
inborn identity & saving key management flow

TRNG
SP800-90B compliant random number

NIST certified Crypto Engines
With encryption and anti-tamper
Thank You
Andes Advantage

- **Standard RISC-V ISA** with Andes Extensions
- **AndeStar V5 ISA** - Extensions to accelerate and secure computing
  - **StackSafe™**: HW supported stack protection
  - **PowerBrake**: Stalling pipeline to save power
  - **QuickNap™**: Fast power-down/wake-up support for caches
- **ACE** - Andes Custom Extensions
  - **Custom Instructions** – Accelerate Instruction
  - **Custom Memories** – Fast and local operands
  - **Custom Ports** – Accelerate, move, and secure – predictable bus
StackSafe™: Protect Stack Usage

- **Recording mode:**
  - Record the maximum usage of stack pointer

- **Protection mode:**
  - Allocate stack size and set its bound accordingly
  - When stack pointer grows over the bound → Generate an exception

---

Exception!
PowerBrake & QuickNap™: Power Management

- **PowerBrake**: to digitally adjust power (via stalling pipeline)
- **QuickNap™**: logic power-down and SRAM in retention
  - Put dirty bits in tag SRAM instead of flops
  - Eliminate the need to flush data cache

Power consumption vs. Performance (frequency)

- **Standby**
- **Dormant**
- **Shutdown**

SRAM power-down

Clock off

Performance (frequency) vs. PowerBrake (frequency scaling)

- **Maximum performance**
- **Minimum performance**
PowerBrake

Clock

Top clock

Pipeline stalling

MPFT_CTL.T_LEVEL = 0xA

IDLE the CPU

Top-Level Core Clock Gating

Performance Throttling
ACE for Performance and Security

- RISC-V ISA extension enables
  - New instructions
  - New coprocessors
  - New memory locations
- Andes eases extension with
  - ACE key words in System C framework
  - Rich semantics for new instructions
  - Fully automated COPILOT generator
    - Integrating acceleration & RISC-V core
    - Resource & data hazard protection
    - Simulator, compiler, assembler, etc.
    - Test vectors for verification

Vs Traditional Architecture.
Private Port for Data Isolation

A usage example

- HW engine: application-specific DMA and structured computations (e.g. CNN)
- ACE instructions: control HW engine, and load/store data to/from VRF

Advantages:

- HW engine is tightly-coupled
- Data accesses are more efficient
- Data accesses are isolated
Q&A
Thank you!