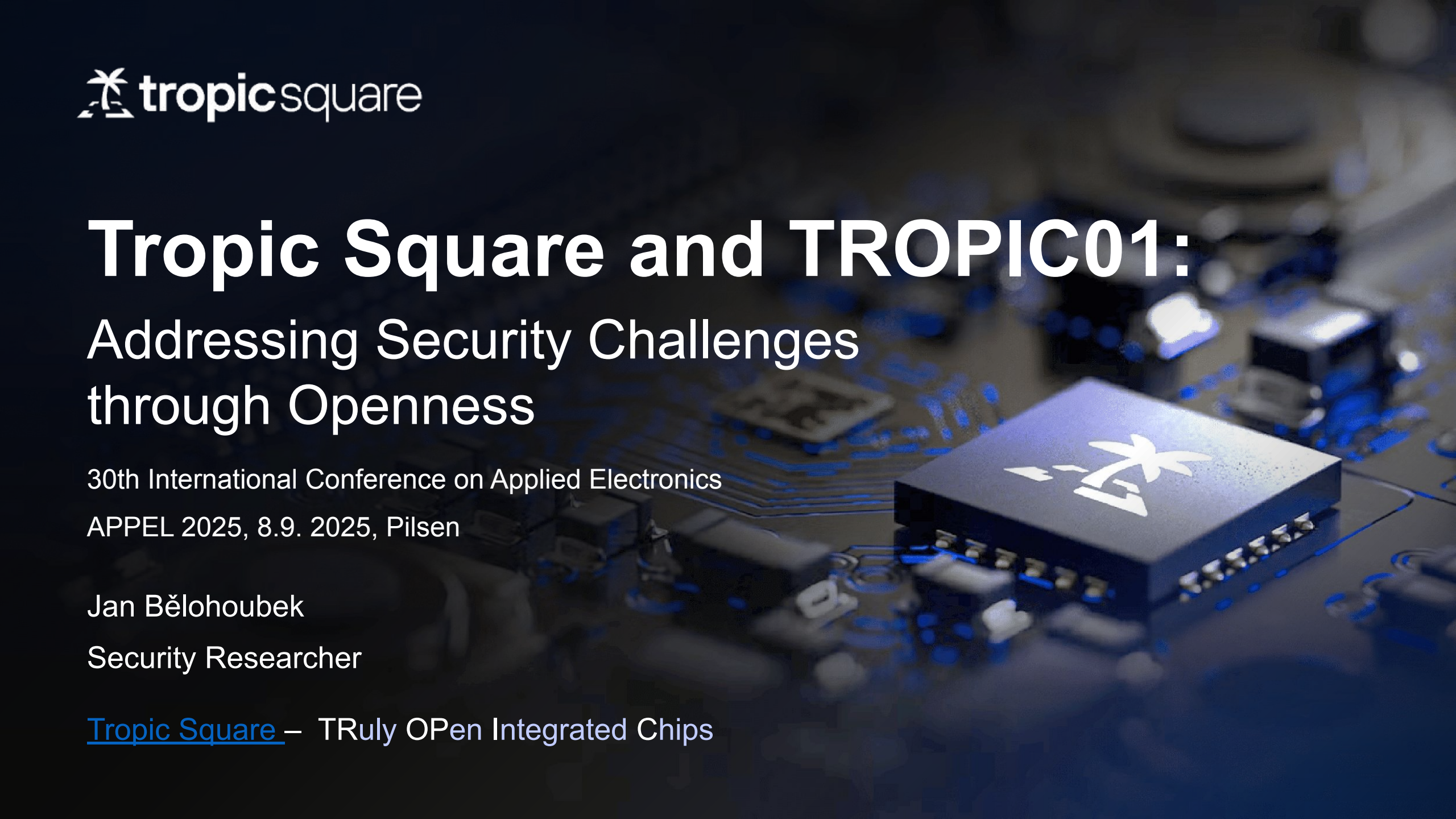
tropicsquare

Tropic Square and TROPIC01:

Addressing Security Challenges through Openness



30th International Conference on Applied Electronics

APPEL 2025, 8.9. 2025, Pilsen

Jan Bělohoubek

Security Researcher

Tropic Square – TRuly OPen Integrated Chips

Speaker & Context Introduction

Jan Bělohoubek
Security Researcher, Tropic Square and CTU

- Bc. FAV UWB in Pilsen; Ing., and Ph.D. CTU FIT in Prague
- Embedded HW and Software Development, HW verification
- Teaching HW and Security-related topics
- Side-Channel-related Security Research

- IEEE member and volunteer
- ASICentrum s.r.o., FIT CTU, FEE UWB

https://orcid.org/0000-0003-4312-9931

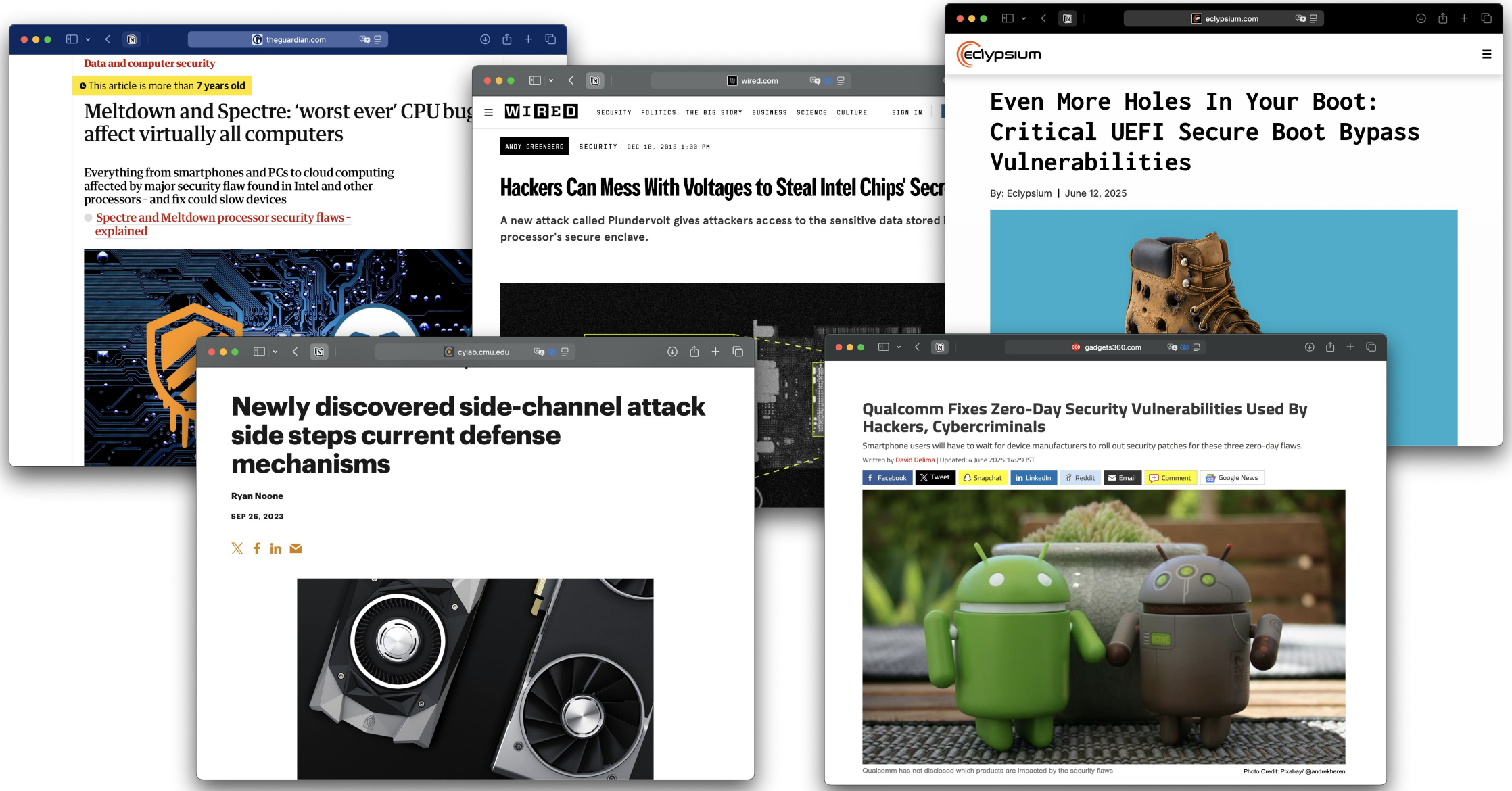
TROPIC – TRuly OPen IC

- **Tropic Square** is **fabless** semiconductor design house based in **Prague, Czech Republic**
- Founded to build **secure auditable chip** - alternative to status quo black box based secure chips
- Pioneering **open architecture and auditable design** since 2020
- Started before OpenTitan was published - fully independent genesis
- Currently a single-product company - TROPIC01 SE

Why do we care about security?

… and you should as well

Your Data, Devices and Services are in Danger



Trust, Security, and Auditability

TRUST

Assurance that an IC will function as intended throughout its lifecycle

- Correct functionality within specs. - RAMS+
  - Reliability
  - Availability
  - Maintainability
  - Safety
  - **Security - CIA Triad**

SECURITY

CIA Triad - IC and Data C+I+A

- Confidentiality
  - Security by Design
  - Encryption, no data leaks, …
- Integrity
  - IC does not suffer from **the supply chain vulnerabilities**
  - IC **as intended by designer**
  - **device integrity**, tamper resistance
- Availability
  - IC is reliable
  - IC is free of **backdoors or trojans**
  - IC is free of known **vulnerabilities**

You need to TRUST what is promised by your supply chain

Trust, Security, and Auditability

TRUST

Assurance that an IC will function as intended throughout its lifecycle

- Correct functionality within specs. - RAMS+
  - Reliability
  - Availability
  - Maintainability
  - Safety
  - **Security - CIA Triad**

SECURITY

CIA Triad - IC and Data C+I+A

- Confidentiality
  - Security by Design
  - Encryption, no data leaks, …
- Integrity
  - IC does not suffer from **the supply chain vulnerabilities**
  - IC **as intended by designer**
  - **device integrity**, tamper resistance
- Availability
  - IC is reliable
  - IC is free of **backdoors or trojans**
  - IC is free of known **vulnerabilities**

AUDITABILITY is the ability to VERIFY

Security is tricky

Security Challenges

Secure Chips are a Young Field … Security Applied to Anybody

Secure chips and silicon level security industry is in early days

- 1985 Wim van Eck - CRT screen reconstruction
  - Remotely displaying the contents of a Cathode Ray Tube (CRT) monitor by detecting its electromagnetic emissions.
- 1995 Paul Kocher - first papers about side channel attack
  - Concept of side-channel attacks, simple power analysis
- 2000s Prominent examples of reverse engineering
  - Gaming consoles, Printer cartridges
  - …
- 2010s Secure element chips, Root-of-Trust
  - Banking cards
  - Mobile phones, PCs
- 2025 Security still not a commodity solution
  - Coming Cyber Resilience Act (CRA) - enforcing security in many areas

Security Challenges

Evolving Threat Landscape: new vulnerabilities and exploits are continuously emerging
- attack vectors unknown at the design time
- running device out-of-spect

Usability and Innovation: security measures may
- slow down the time-to-market
- affect the design size or consumption
- affect the user experience

Complexity: complexity of ICs leads to
- lack of visibility and control over side effects
- race conditions
- privilege control issues

Resource Constraints
- lack of skilled engineers
- lack of budget
- time-to-market pressures

Supply Chain Issues
- globalization - and geopolitics
- trust in the supply chain

Business Objectives
- lack of understanding in business and management

Security as Excuse for Vendor-lock-in
- vendors arguing that closed systems offer superior protection compared to open/multi-vendor environments

Legislation Compliance - CRA

Security is tricky:

AUDITABILITY

- is the ability to VERIFY
- is a way to gain TRUST

BUT

Security is HARD to VERIFY

Achieving Trust: Reputation, Trust Transfer, and Openness

Reputation

"Trust me; I'm an established manufacturer with a long history."

Internal Audit

"Trust me; I applied this long list of measures and tests. Here are the results … "
"Trust me; I have a verification team."

(Reputation still required)

External Audit

"Trust me, this **independent** body proved, that I do not lie."

(Reputation and true independence of the external auditor required)

Openness

"Trust me, because **anybody can verify.**"

(Internal verification still required)

AUDITABILITY is the ability to VERIFY

The IC Industry Status Quo, The Security Perspective

Security by Obscurity

Implementation details are kept secret

Once secrecy is broken, security properties are affected

Attacker starting position is, in theory, hard

- **Opposed in 19th century by Auguste Kerckhoff!**
- Reverse Engineering and **Implementation Attacks**

Security by Design

Design should remain safe even implementation is known

It does not contradict Security by Obscurity, but it is fundamentally different approach

- they can **stack-up**

Design security **does not rely on secrecy**

Cryptosystem security should only rely on secrecy of keys

- **Kerckhoffs's Principle, 19th century**

Secrecy ONLY is NOT LEGITIMATE for Achieving Security

The IC Industry Status Quo, The Security Perspective

State of the Art: Combination of Security by Obscurity and Security by Design

Security by Obscurity

Secrecy Applied to Implementation

- Example:
  AES implementation details are kept secret

Security by Design

Security by Design Applied to Algorithm

- Example:
  AES algorithm security is proven

Consequences of Implementation Secrecy

Hiding design issues:

- Design-time security compromises
- Implementation quality
- Discovered weaknesses

To compromise the whole design, one weakness is enough

Verification/Auditability requires **full access to discover any weakness**

Secrecy Erodes TRUST

The IC Industry Status Quo, The Security Perspective

Fixing Eroded Trust - the Best Case under the IC Industry Status Quo

Prove of Quality

Reputed supplier open to independent audits by respected bodies.

Transparent Communication of Issues through the Life Cycle

Reputed supplier with transparent communication culture.

“Responsible disclosure” process.

Design Secrecy IS LEGITIMATE for IP Protection

Everybody declares Transparency, but experience shows it is NOT (yet) trustworthy.

The chips inside our devices are black boxes!

We don't know what they're doing.

Challenging the Status Quo of the IC Industry

Demanding Openness

Secrecy ONLY is NOT LEGITIMATE for achieving Security

Secrecy erodes TRUST

Design Secrecy IS LEGITIMATE for IP Protection

This is How the Business Model Works

Declared Transparency cannot fix eroded TRUST (completely)

- Unknown design-time security compromises
- Unknown implementation quality issues
- Inappropriate reaction to discovered weaknesses

Sense of security is just an illusion?!

Tropic Square Approach

Industry Position and Future Directions

Past & Present

- Cybercrime exploits undocumented features & vulnerabilities **despite obscurity (secrecy)**
- Semiconductor industry not innovating fast enough to deploy security at scale
- Cryptographers, security experts, academia demand transparency and auditability

Security by obscurity is obsolete.

Tropic Square Approach

Current Industry Position and Future Directions

Past & Present

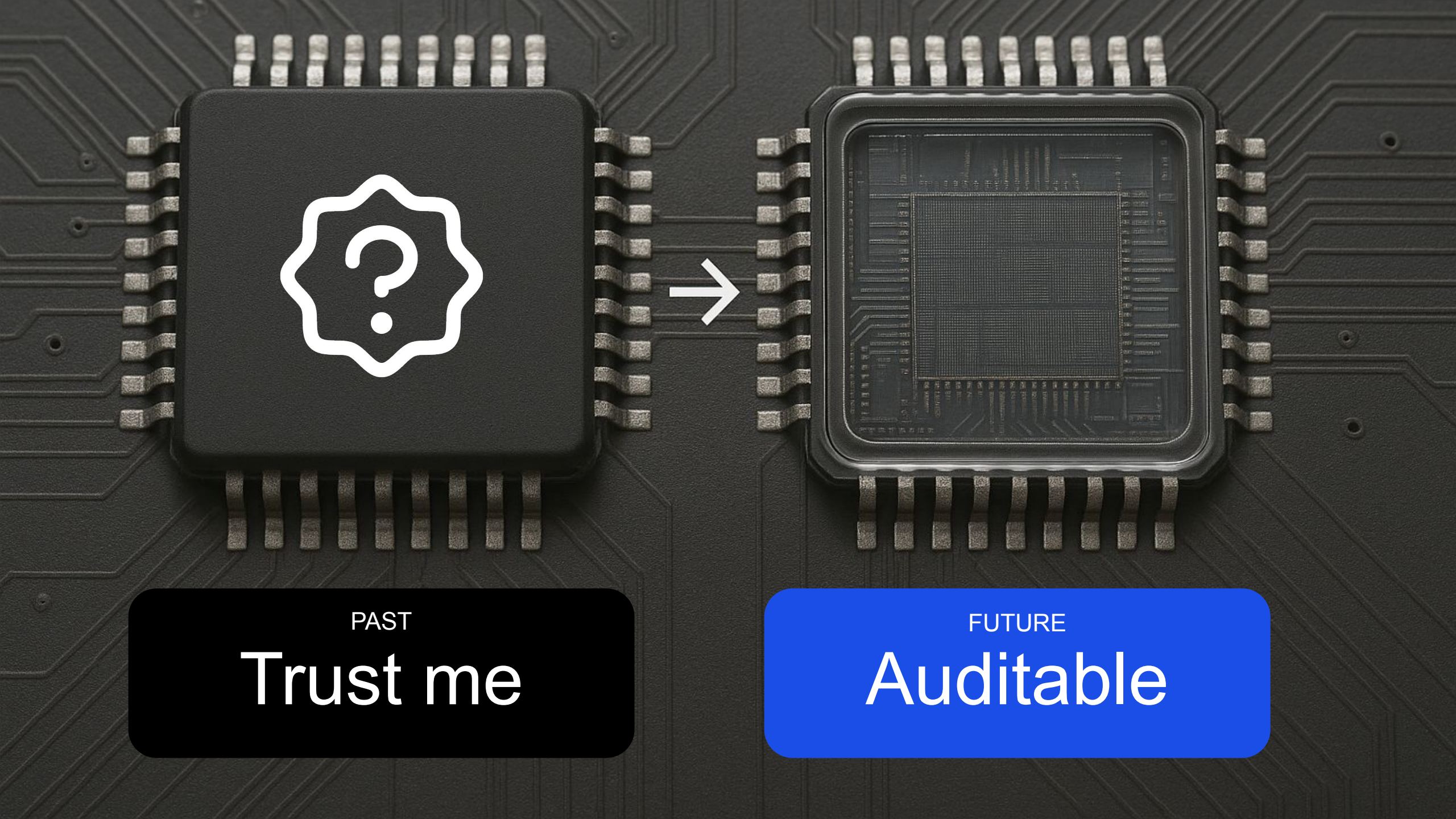
- Cybercrime exploits undocumented features & vulnerabilities despite obscurity
- Semiconductor industry not innovating fast enough to deploy security at scale
- Cryptographers, security experts, academia demand transparency and auditability

Security by obscurity is obsolete.

Future innovation, disruption

- **open architecture, auditable** secure chips and building blocks (IP cores)
- Side channel & physical attack resistance, continues evaluation - hacker's scenarios
  Do not trust, Verify!
- No back doors or undocumented features weakening security
- Transparent processes, more people reviewing

Auditable silicon, utilizing open source & RISC-V to enable verifiable security by design.


PAST
Trust me
FUTURE
Auditable

Tropic Square Approach

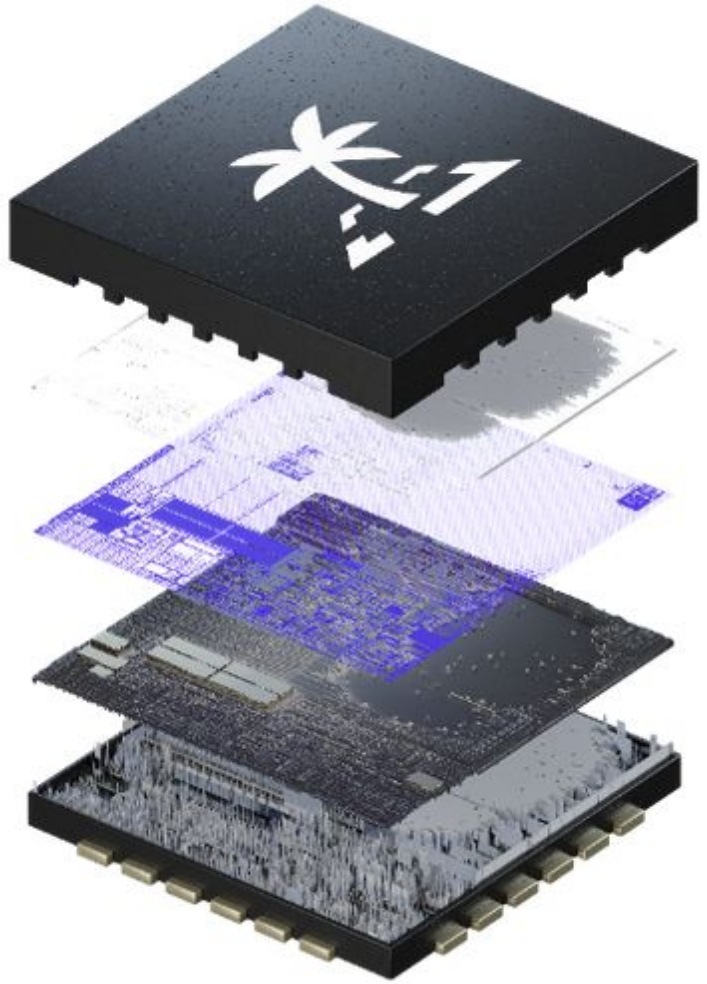
Security is Infinite Game

- Extra effort means, extra cost **security is NOT for free**
  - Area, effort, time cost
  - Customers don’t ask for security
  - Physics of silicon - not secure without extra effort
  - **IP blocks under NDA**

- **open != for free** - Tropic Square does not follow strict open-source definitions (not RMS compatible, not “Free as in Freedom”)

- **open != secure, but auditable**
  - need proof of work, security analysis, reviews, sharing traces, bug bounty incentives
  - influence of certification and becoming compatible with it

- Balance is a challenge - **absolute security is impossible**
- Security is an infinite game. How can it be implemented in “fixed hardware”?
- We need a viable business model.



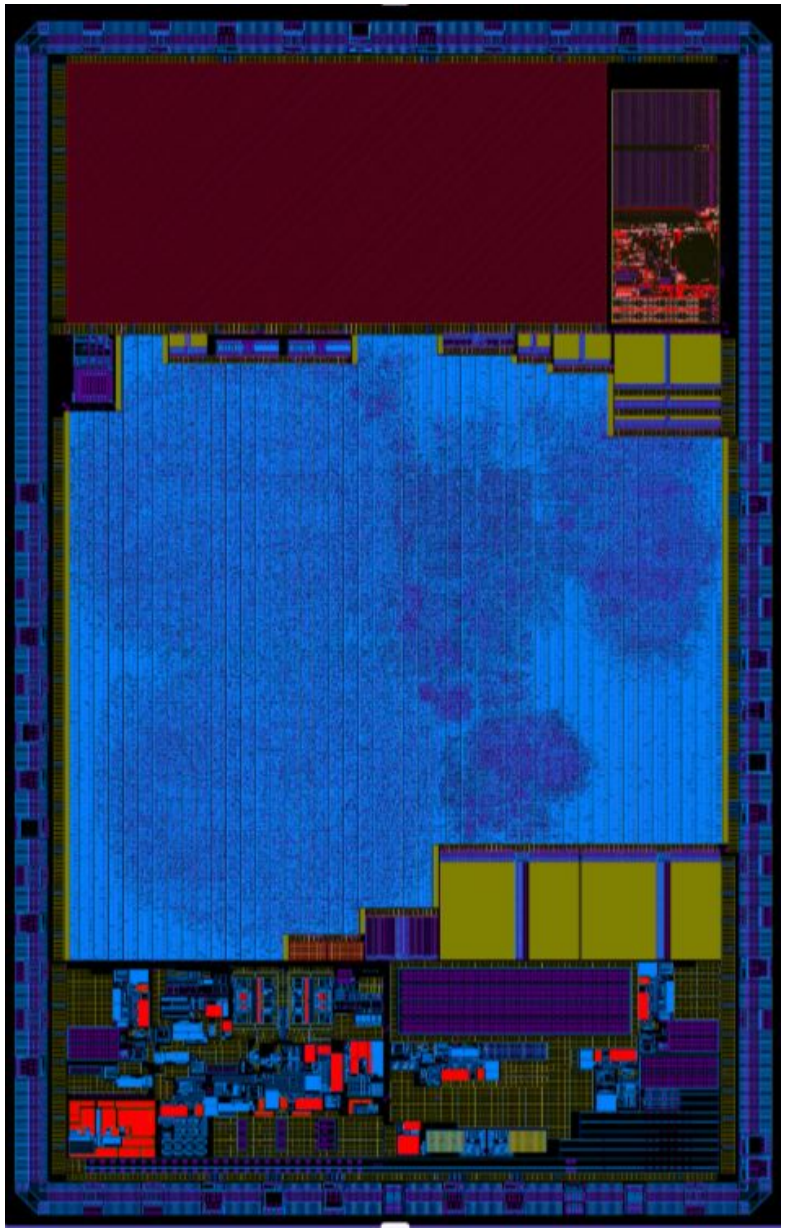
Tropic Square Approach

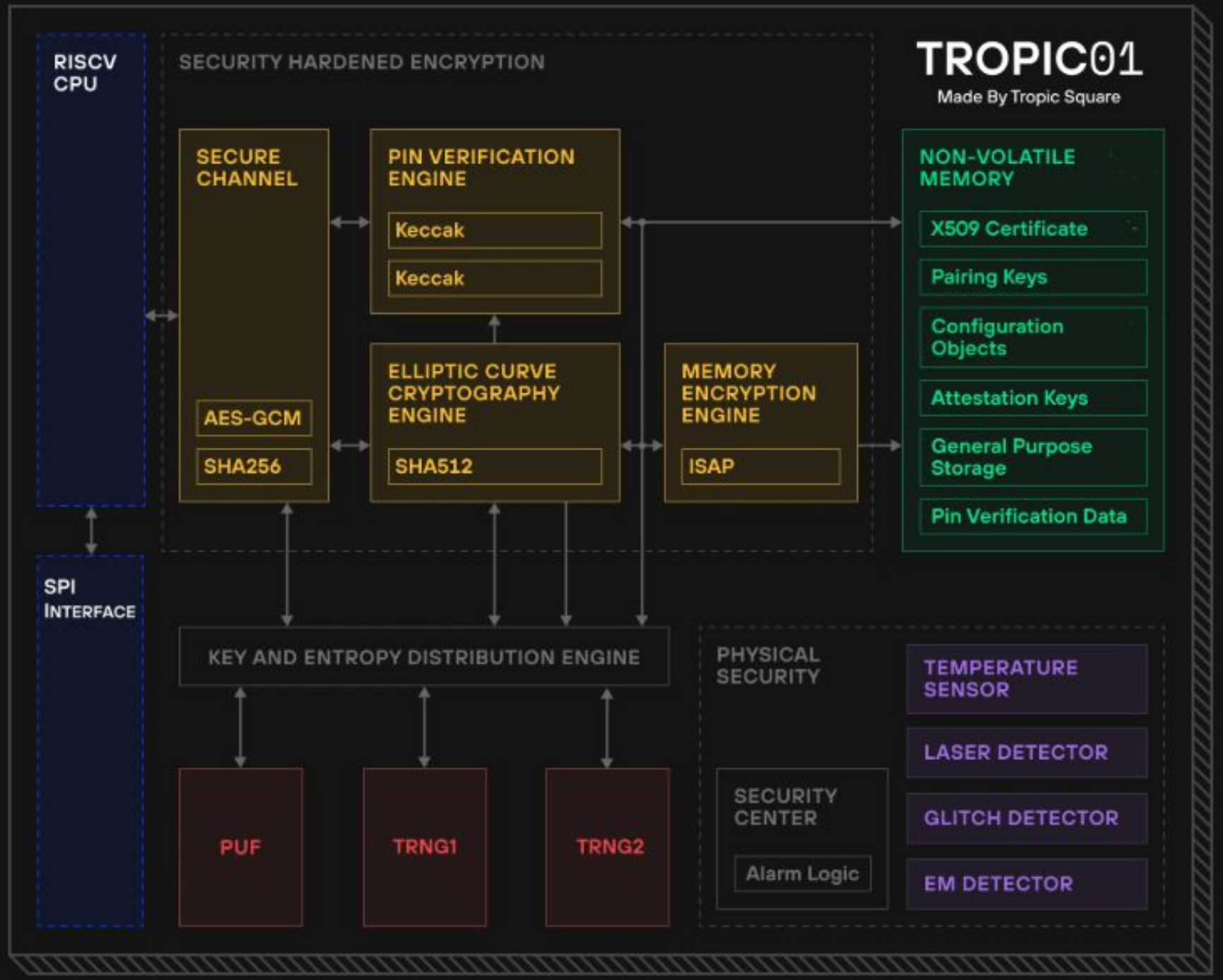
TROPIC01

- Designed in UMC55
- Designed predominantly using the standard, commercial industry toolchain

- Developers resources on github
  - https://github.com/tropicsquare
  - https://github.com/tropicsquare/tropic01

- Embedded World 2025
  - Embedded Computing Design - Best in show WINNER
  - Safety & Security WINNER





No Undocumented Features

FW Source Code

Threat Model

Test Results

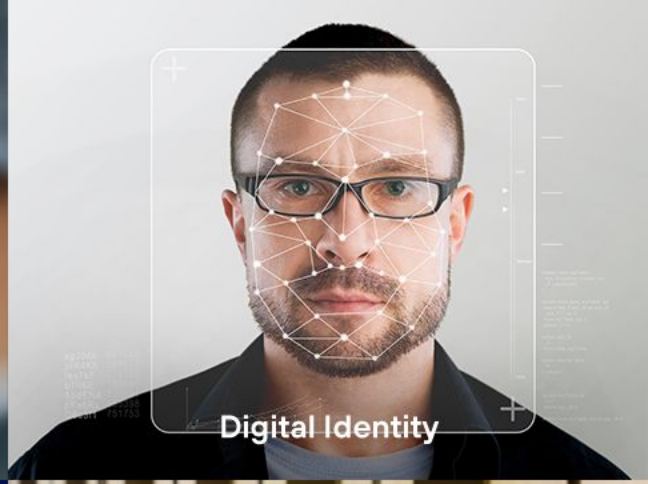
RTL for Audit

Tropic Square Approach

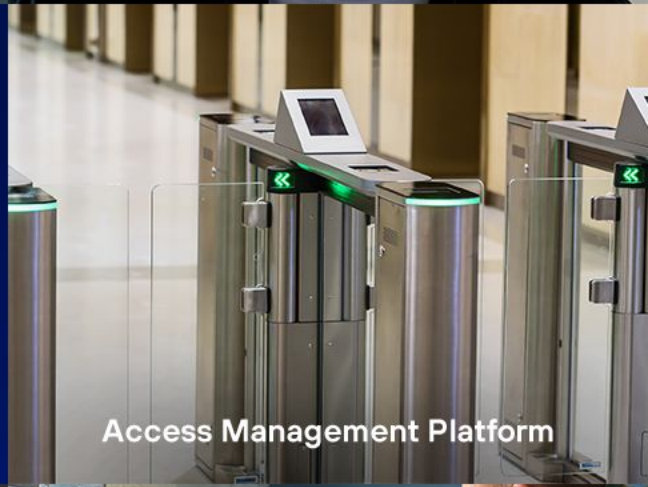
Beyond the Current Industry Position: The Real, Proven Transparency

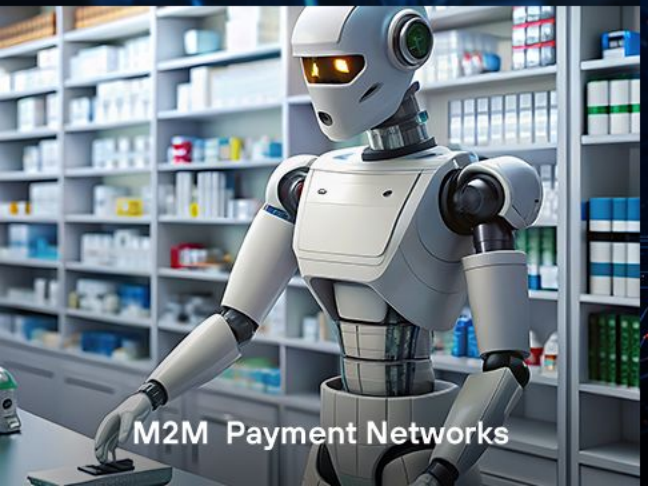
- **Security by Design**
- **Proved Transparency (Work-in-Progress)**
  - all materials we can provide to not violate **3rd party NDAs**, and **to stay profitable**

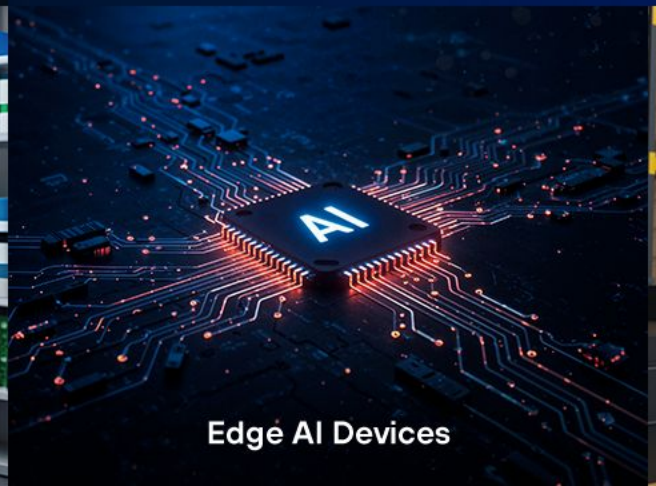
Feature	Current IC Industry Standard	Tropic Square Approach
Undocumented Features	Cannot be Verified	No, Auditable
SW Source Code	Some Vendors	Yes
FW Source Code	Few Vendors	Yes
Threat Model	Some Vendors or under NDA	Yes, Work-in-Progress
Audit Results	Some Vendors or under NDA	Yes, Running Audits
RTL	No (rarely under NDA)	Yes, under restricted License (no manf.)
Physical Implementation (GDSII)	No	No
Supply Chain Issues	???	???, Auditable

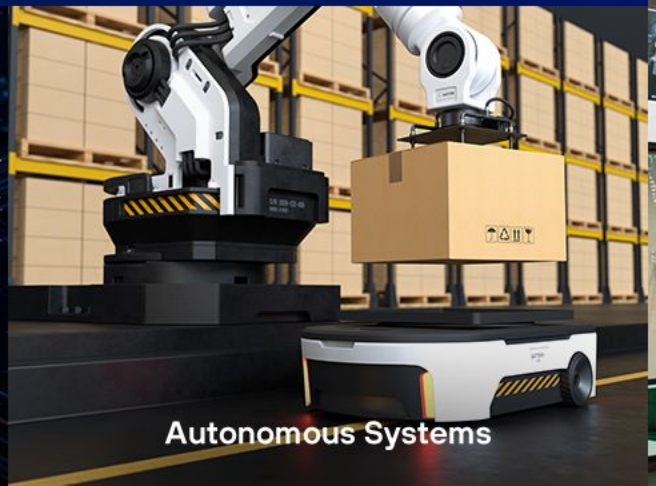


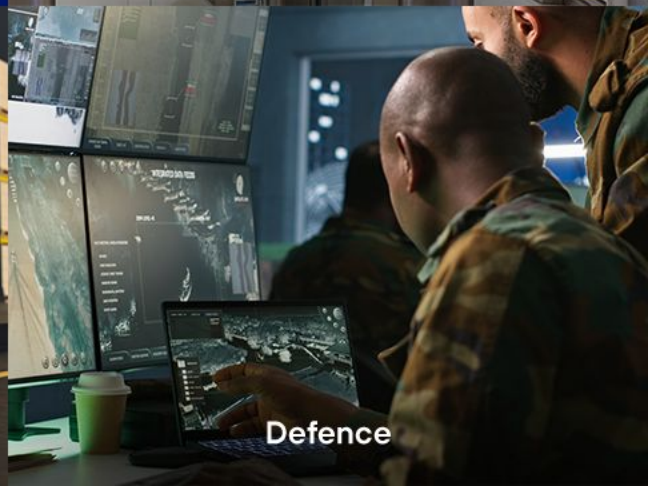
Market Segments & Applications











Future Open IC Design

Open IC Toolchains and PDKs

Open IC Tools

Implementation details are kept secret

- **The OpenROAD Project** (RTL2GDS)
- OpenLane (Verilog2GDS)
- Qflow - deprecated (Verilog2GDS)
- **ngSPICE**, **Verilator**, ghdl, Magic, **KLayout**, …

Why not used for TROPIC01?

- We **use some of them**, and we experiment with most of them!
- Lack of UMC55 PDK support
- Lack of industrial-grade support

Open PDKs

Skywatter Sky130

- The first open PDK
- US Foundry

IHP130

- European Foundry, Frankfurt (Oder)

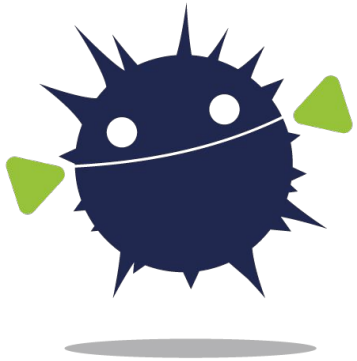
Why not used for TROPIC01?

- Not available 4 years back
- Security-related IPs not available
- (130nm technology)
- Considering for future designs (supply chain risk mitigation)

Open IC Design Already Mature for some Applications

Future Open IC Design

The ORSHIN Project: Pushing Open-Source Hardware Forward



Project Areas

Main project outcomes:

- Trusted Life Cycle Methodology
- Formal Verification
- Effective Security Audits
- Secure Communication Protocols

https://horizon-orshin.eu/
https://summer-school.info/
ORSHIN and Tropic Square at CHES

Applicability

Tropic Square is one of Industrial Partners:

- An academic paper is just a starting point
- There are challenges to replicating academic results - tooling etc.
- We are moving towards public executable, documented examples

Available at the end of September:

- https://github.com/tropicsquare/orshin-demo/
- https://github.com/tropicsquare/orshin-public-assets

Funded by the European Union under grant agreement no. 101070008. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union. Neither the European Union nor the granting authority can be held responsible for them.

Thank You for your feedback & Happy to answer your burning questions.

Jan Bělohoubek

Security Researcher

jan.belohoubek@tropicsquare.com

www.tropicsquare.com

welcome@tropicsquare.com

linkedin.com/company/tropicsquare-s-r-o

https://github.com/tropicsquare

https://x.com/tropicsquare