RISC-V Days Vietnam 2020

RISC-V Benefits and Security

September 18, 2020
Shumpei Kawasaki
SH Consulting KK
www.swhwc.com
RISC-V Association
riscv-association.jp

@risc_v
@riscv_a

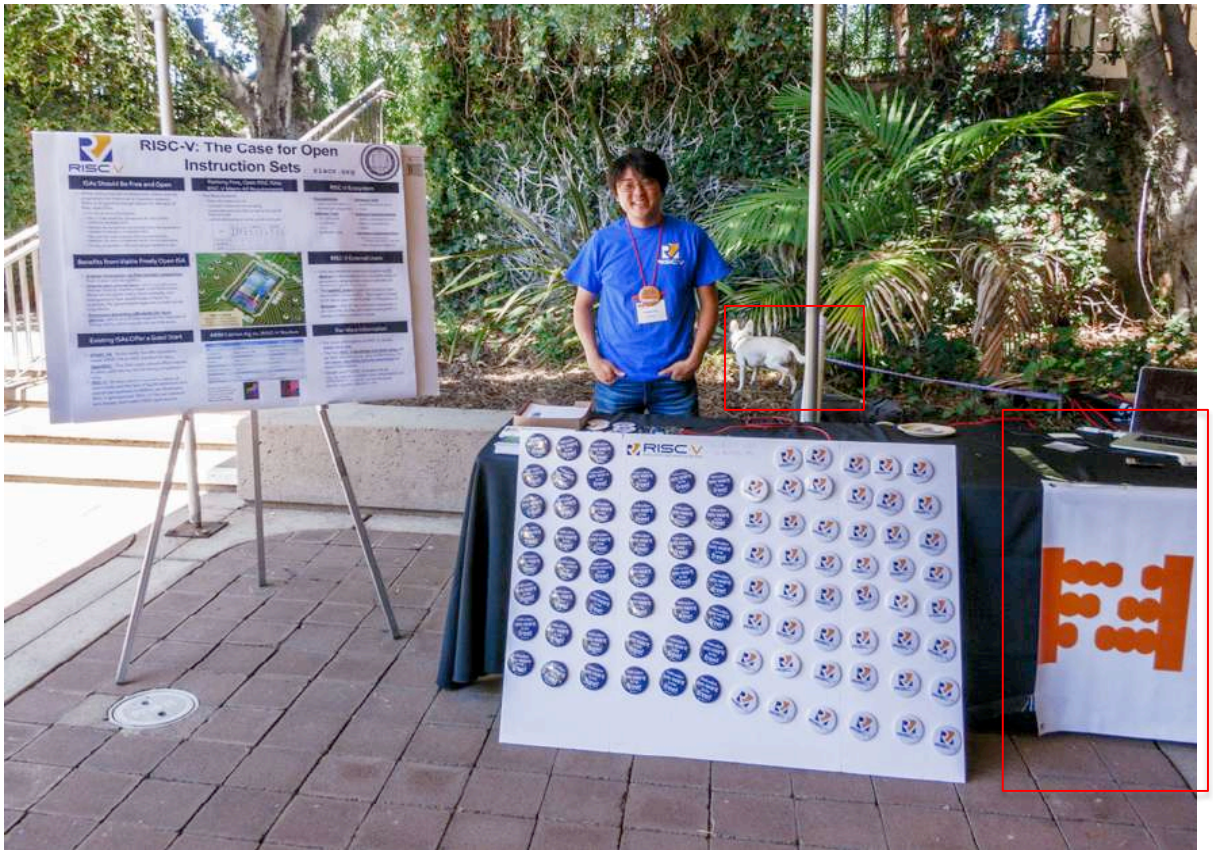
RISC-V 協会
RISC-V Association

発表内容

1. Background introduction
2. RISC-V Status
3. Open source security
4. Security architecture on smartphones, PCs and servers
5. RISC-V Security Trends
6. New Direction of Security
7. Summary

1. Background introduction

2014 Encounter with RISC-V



SH Microcomputer @ Hot Chip 26

SH microcomputer abolished in 2013

Captive IP

2545 ISA patent expired ISA license release

Open source SH-2

2nd announcement

2003 opencores.org

2014 0pf.org

2016 ~

2. RISC-V Status

RISC-V Feature 1: Modular instruction set 32/64/128 bit Covers all application areas

To make it a machine that can run Linux
(1) Register length (XLEN) = 64 bits.
(2) G (general-purpose instruction group) = as an instruction group
I (integer) + M (multiplication) + A (atomic)
+ F (single precision floating point)
+ D (double precision floating point)
+ Select C (compression instruction).
(3) Privilege mode configuration is
Select 3 levels (3).
M (machine level)
S (supervisor level) U (user level)
To support.

MXL	XLEN
1	32
2	64
3	128

①レジスタ長の指定

Table 3.1: Encoding of MXL field in `misa`

Level	Encoding	Name	Abbreviation
0	00	User/Application	U
1	01	Supervisor	S
2	10	*Reserved*	
3	11	Machine	M

特権モード定義

Table 1.1: RISC-V privilege levels.

Number of levels	Supported Modes	Intended Usage
1	M	Simple embedded systems
2	M, U	Secure embedded systems
3	M, S, U	Systems running Unix-like operating systems

④特権モード構成の指定

Table 1.2: Supported combinations of privilege modes.

Subset	Name
Standard General-Purpose ISA	
Integer	I
Integer Multiplication and Division	M
Atomics	A
Single-Precision Floating-Point	F
Double-Precision Floating-Point	D
General	G = IMAFD
Standard User-Level Extensions	
Quad-Precision Floating-Point	Q
Decimal Floating-Point	L
16-bit Compressed Instructions	C
Bit Manipulation	B
Dynamic Languages	J
Transactional Memory	T
Packed-SIMD Extensions	P
Vector Extensions	V
User-Level Interrupts	N
Non-Standard User-Level Extensions	
Non-standard extension "abc"	Xabc
Standard Supervisor-Level ISA	
Supervisor extension "def"	Sdef
Non-Standard Supervisor-Level Extensions	
Supervisor extension "ghi"	SXghi

汎用命令群G

圧縮命令C

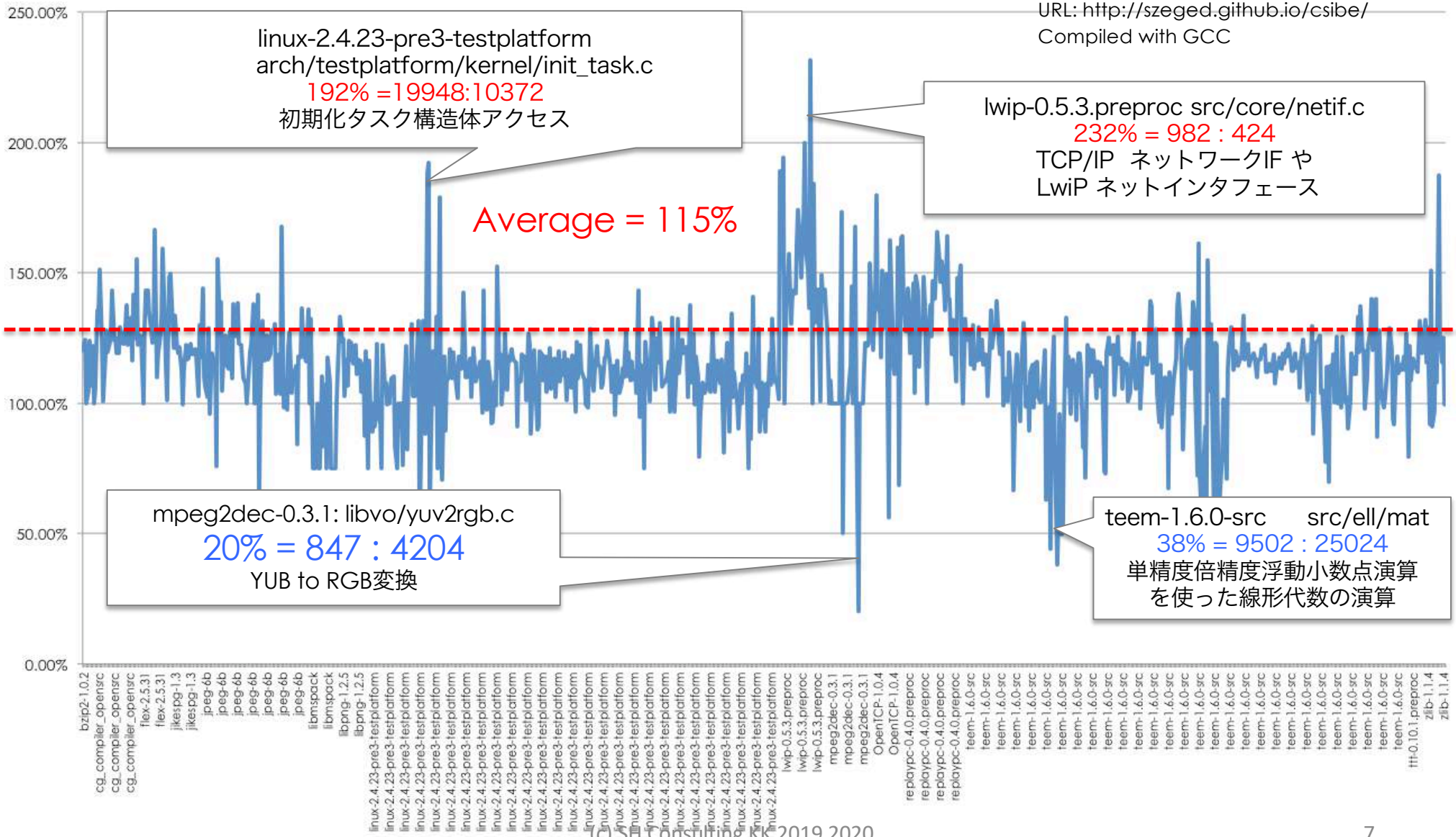
②命令群の指定

Table 22.1: Standard ISA subset names.

出展： SHC Poster Session Presentation at RISC-V Workshop 5 2016/11/29

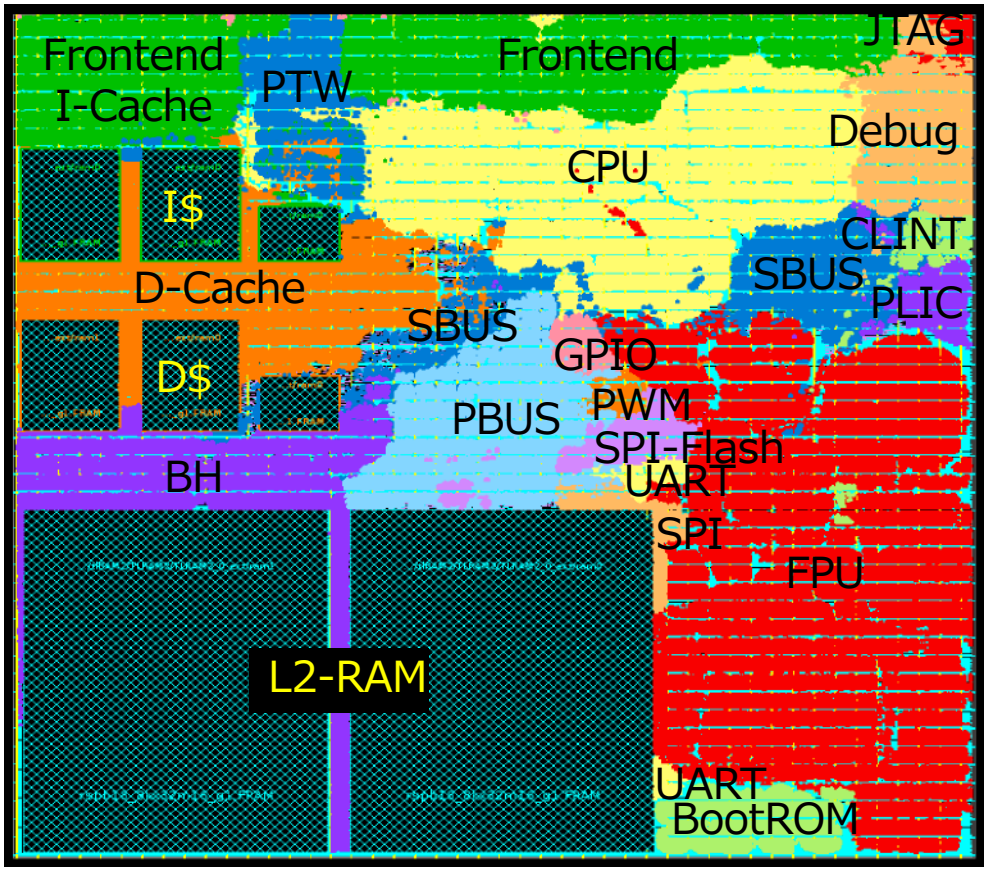
RISC-V Feature 2: Non-mode high density instruction RV64GC vs. ARM M0

CSiBE = Code Size Benchmark
URL: http://szeged.github.io/csibe/
Compiled with GCC



出展： SHC Poster Session Presentation at RISC-V Workshop 5 2016/11/29

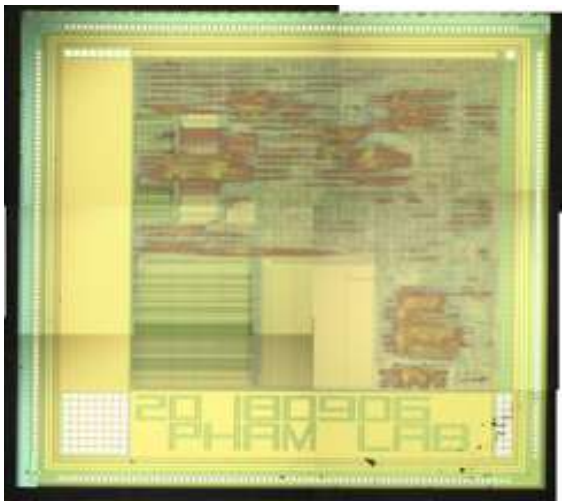
RISC-V Feature 3: RISC-V SoC Automatic Generation Tool



Exhibitors: University of Electro-Communications, University of Tokyo VDEC

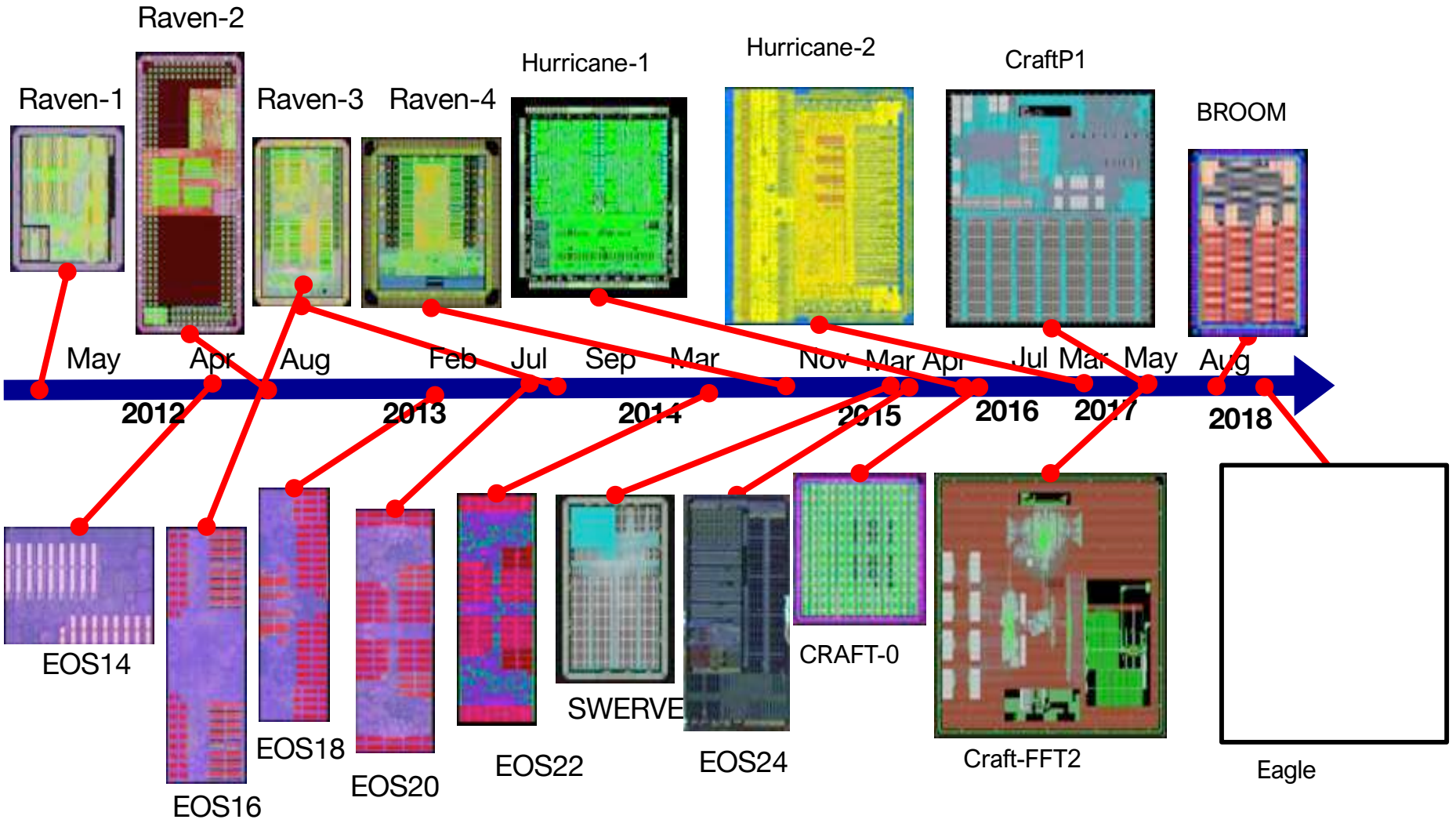
Remarks: Designed at weekend nights. The actual design is less than January.

Tip Complete: December 2018
Process: ROHM 180nm
Area: 3.75mm x 3.75mm
SRAM:
I $ + D $: 4KiB + 4KiB
L2-RAM: 64KiB
Logical scale: 302KG
(Usage rate: 53%)
Frequency: 80MHz @typ
(Not optimized)



5mm x 5mm (incl. I/O Pad)

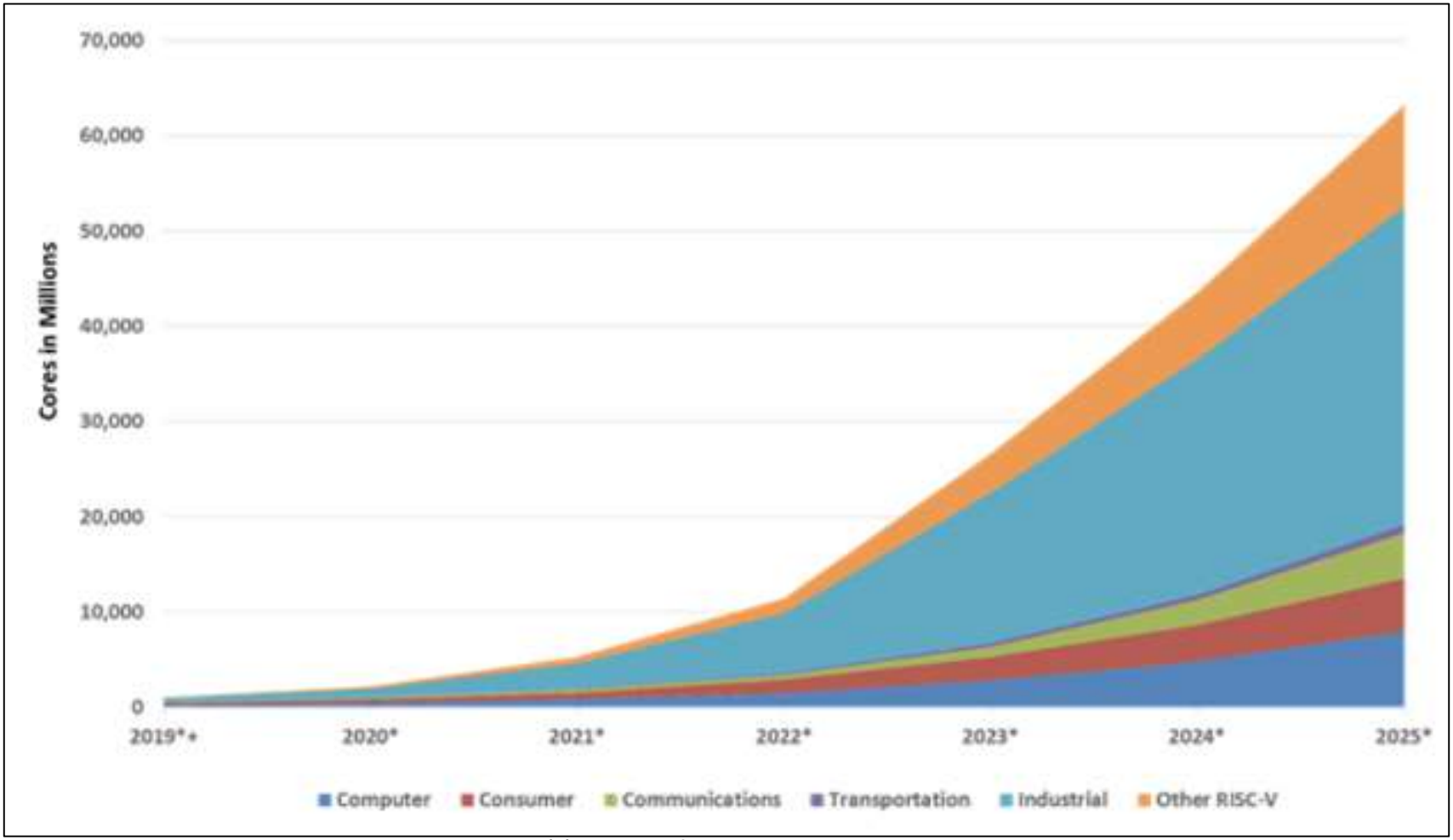
RISC-V Feature 4: Chip-mounted, software-mounted backed architecture release



IBM 45nm, ST 28nm FDOI, TSMC 28nm and 16nm FF, GF 14nmで設計

Application 1: Semico announced that RISC-V will become mainstream

- “For RISC-V adoption, we expect the market to consume a total of 62.4 billion RISC-V cores by 2025, and RISC-V will move towards mainstream adoption,” said Jim Ferdan. -President of Semico Research-



Application 2: RISC-V growth hotspot communication, etc., in-vehicle

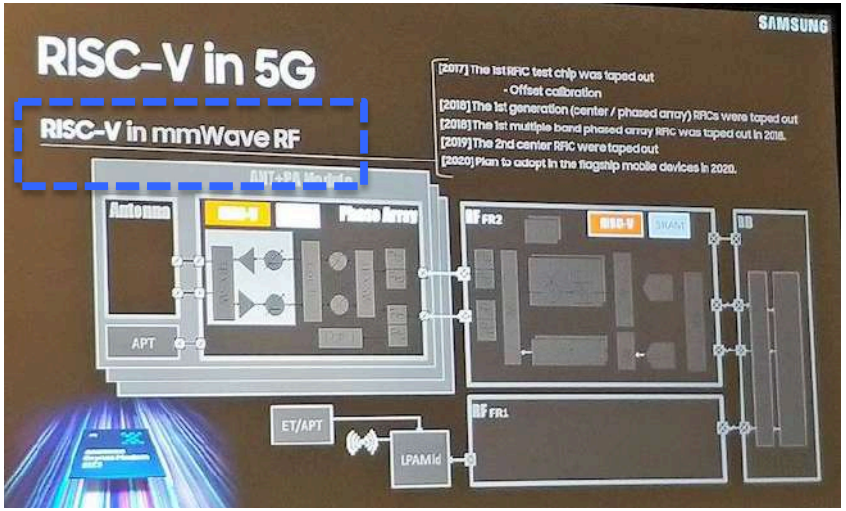
- 5G base stations and 5G terminals ： CAGR 209%
- IoT including wearable ： CAGR 185%
- In-vehicle, transportation CAGR 160%

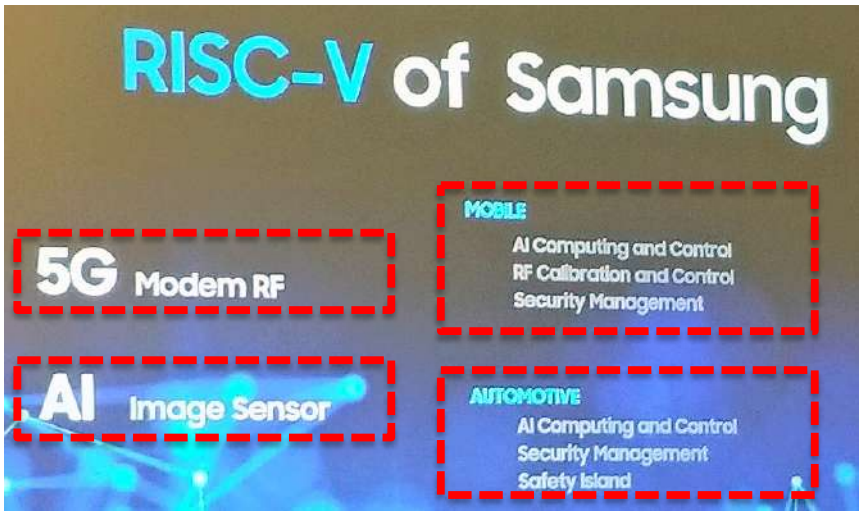
業界セクターおよびICの実装ごとのRISC-Vのコア出荷年間成長率。 出典：RISC-V Foundation。							
	コンピュータ	コンスーマ	通信	車載、運輸	工業	その他	合計
高性能型マルチコアSoC	60%	73%	224%	153%	106%	171%	144%
コストマルチコアSoC	60%	92%	222%	159%	122%	201%	177%
廉価SoC	63%	115%	217%	166%	127%	215%	190%
FPGA	62%	72%	190%	163%	102%	176%	149%
合計	61%	81%	209%	160%	110%	185%	159%

Application 3: Samsung uses SiFive RISC-V core for 5G applications

- Use RISC-V core for mmWave RF processing in 5G RF front-end modules.
- Applies to Samsung's flagship 5G smartphones in mass production in 2020.
- It was 2017 that the RISC-V core was incorporated. Repeated design for 3 years to complete mmWave RF processing on mobile.
- Samsung RISC-V Core Plan: (1) RF Calibration, (2) AI Image Sensor, (3) AI Computing Control, (4) Security Management, (5) Safety Island.
- Qualcomm has also been designing mmWave for some time.

Mass production mmWave RF Samsung RISC-V application field



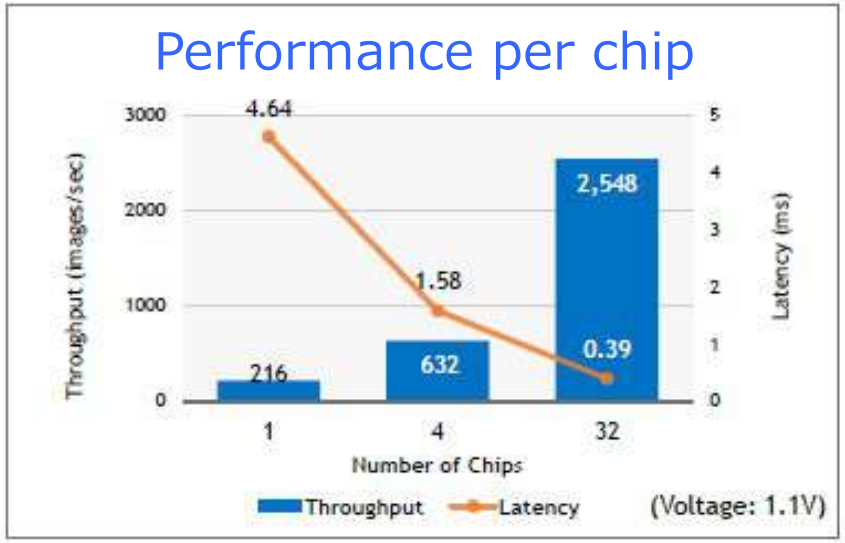


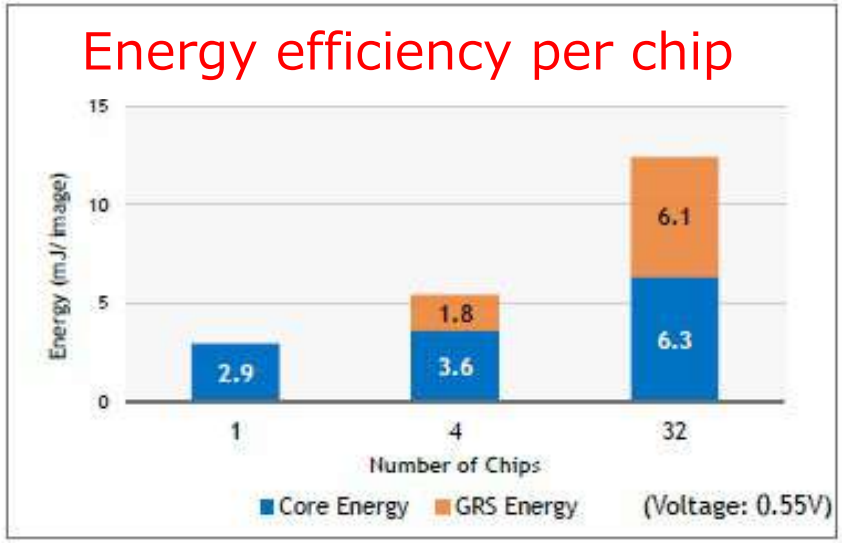
Application 4: NSIT EXE announces DR1000C RISC-V processor with vector function that meets ISO 26262 functional safety standard ASIL D level

The DR1000C is the world's first RISC-V-based processor that meets the ASIL D safety requirement level of the vehicle's ISO 26262 functional safety standard. A parallel processor optimally designed to offload the centralized computing load that a vehicle control microcomputer must perform with a multithreading mechanism and vector instructions. By incorporating the DR1000C, the vehicle control microcomputer supports advanced control algorithms such as model predictive control, and complies with stricter legal regulations.

Application 5: NVIDIA Disclosures RC18 Inference Chip Technology

- Reasoning does not yet have a dominant player compared to training.
- Pe has a RISC-V core for handling global PE and serial I / O functionality.
- A technology called Ground Reference Signaling as a signal technology for multi-chip modules on organic substrates → Doubles the bandwidth per millimeter of chip edges
- The RC18 inference engine chip fits in place of the Nvidia Deep Learning Accelerator.
- Fully coded in C ++ using high-level synthesis.
- Exploration tool to test the design space





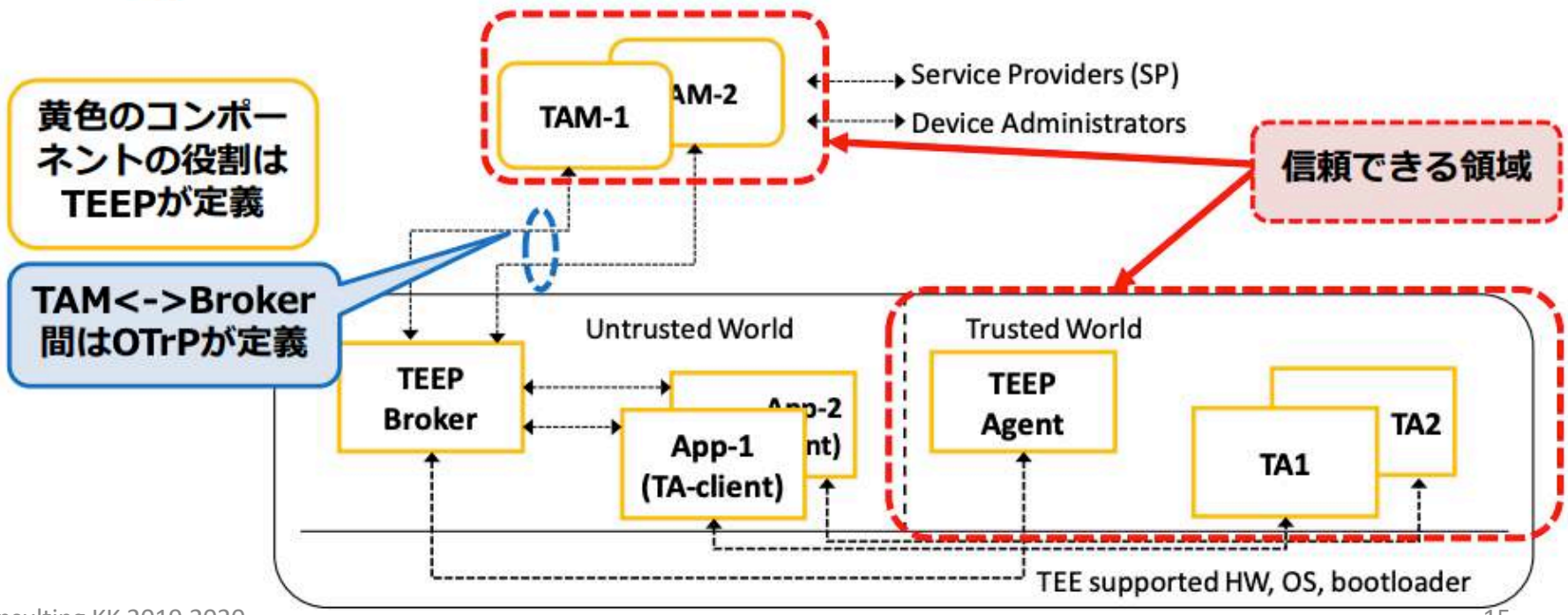
Scaling to 32 chips achieves 12X improvement in performance over 1 chip at Batch = 1.

Communication and synchronization overheads limit speed-up.

High energywith increasing number of chips.

Application 6: RISC-V TEE TEEP activity

- The AIST team is implementing TEEP on RISC-V. The IETF defines the Trusted Execution Environment Provisioning (TEEP) protocol, which remotely installs / updates / removes TAs (Trusted Applications) in the TEE (Trusted Execution Environment), which provides hardware isolation security for the CPU. TEEP is designed to be versatile across different CPU architectures. Currently the main activities are only Intel and ARM.
- TEEP consists of three software components: OS "TEEP Broker", TEE "TEEP Agent", and remote server "Trusted Application Manager (TAM)". I am thinking of using TEEP with RISC-V while maintaining the portability of existing TAs. This is a method to minimize necessary functions such as HTTP in TEE and Concise Binary Object Representation (CBOR) parser.



Application 7: RISC-V Quiet Server Deployment

- In June, the president of SiFive, a RISC-V company at the University of California spinout, declared that "the RISC-V server will be put into commercial operation within five years."

- Porting of container technology and microservices technology that guarantees resilience, operational rates and scalability.

- Language support is the foundation of the RISC-V instruction set (ISA). DARPA funding of LLVM / Clang, a new compiler for RISC-V, began in January, and RISC-V was upgraded to a Devian portable architecture in 2019. Construction of a foundation for a wide range of language support over Clang, OpenCL, and Rust has started. In May, the GNU Debugger (GDB) "GDB 8.3" implemented RISC-V support for the C, C ++, Ada, Go, and Rust languages. On September 3, Google announced that the server system language Go developed by Google will officially support RISC-V in the next release version 1.14.

- Instead of traditional collocations and virtual machines, server applications are shifting to highly abstract services such as microservices. The movement to make RISC-V compatible with this is steadily progressing as a pre-commercial stage. Software such as system operation infrastructure services (IaaS), application execution environment services (PaaS), and micro-function services (FaaS) are also being ported to RISC-V one after another. In the full-featured serverless RISC-V implementation of OpenFaaS, pull requests are being merged upstream.

- Under development of Open Titan as RoT for server

3. OPEN SOURCE SECURITY

High quality security technology

Offer as open source

⋯ I think what you are working on is important. I don‘t know of any open source high quality security solutions⋯

Andreas Olofsson, DARPA MTO

Kerckhoffs Principle (Exhibitor: Wikipedia)

Cryptography should still be secure, even if everything but the private key is known.

In cryptography, the Kerckhoffs principle is the principle proposed by Auguste Kerckhoffs in the 19th century:

Cryptography should still be secure, even if everything but the private key is known.

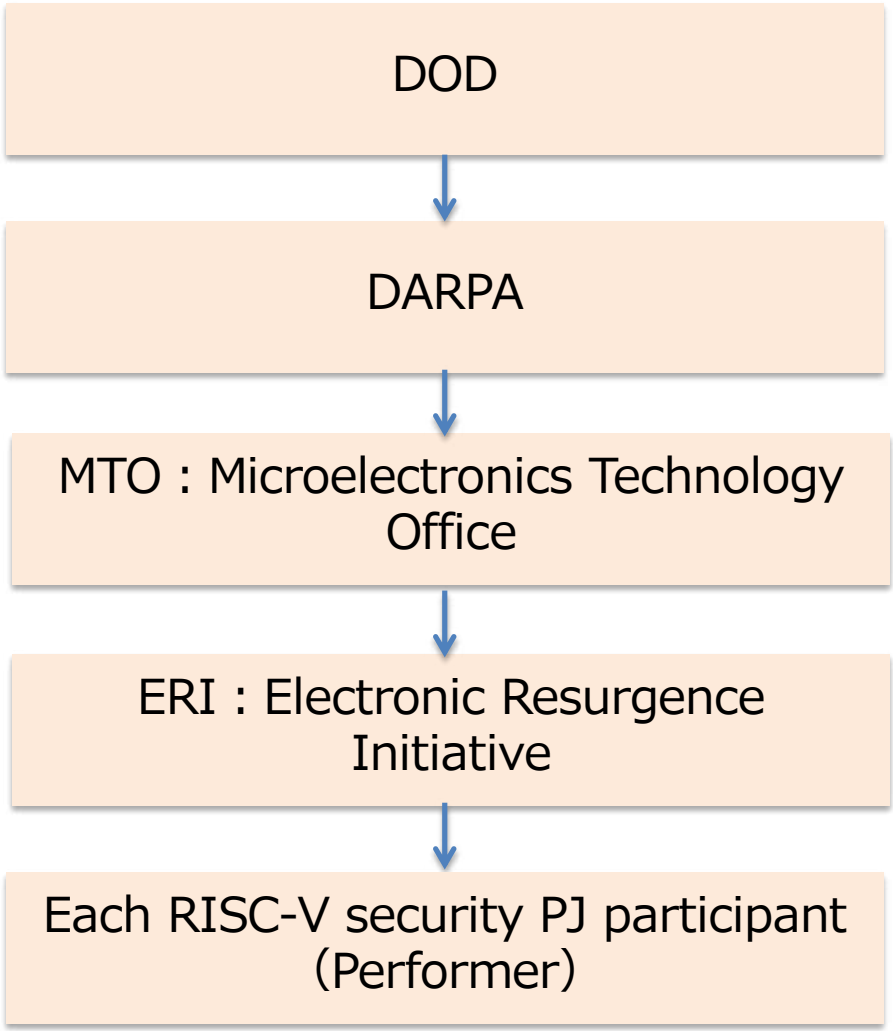
Many trust-based products (chips, IPs) do not have their implementation open to the public.

Even if the implementation configuration method is disclosed, secure implementation should be possible if the private key is protected.

Publication of cryptographic technology

In the 1970s, the US government banned cryptographic research. Diffie Whitfield thought the privately-developed Diffie-Hellman algorithm was a technology that protects individual rights. Announced "New Directions of Cryptography" with the slogan "Making Cryptography Available for the Masses!". I am convinced that the availability of public cryptography implementations, including PKI technology, will one day be useful to society. This is also related to the background that led to the release of the DES specification by the US government.

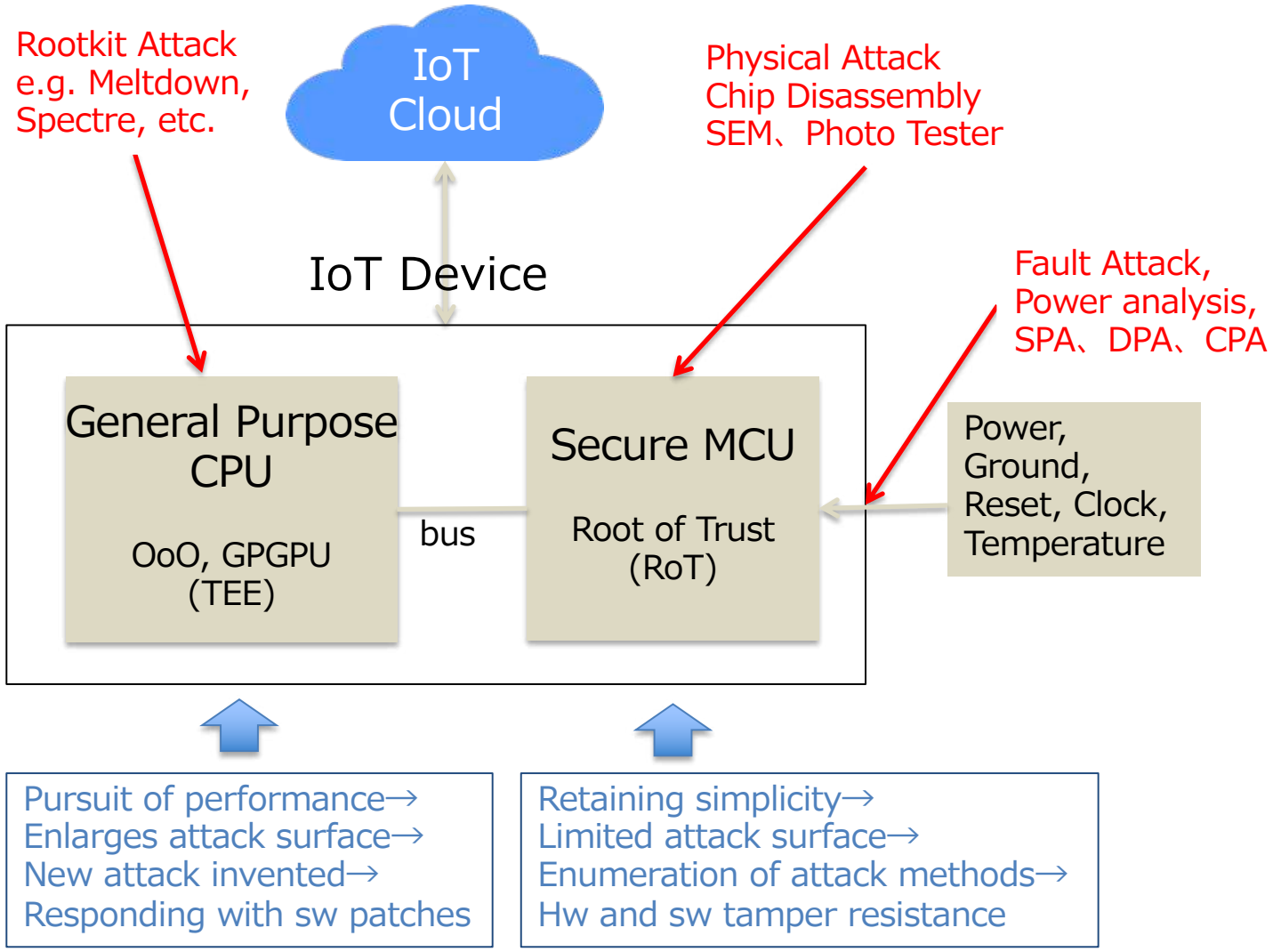
RISC-V Security and DARPA



- In 2017, US DARPA mandated that RISC-V be used as a CPU for security research as a funding condition.
- DARPA began funding the LLVM compiler for RISC-V in December 2018.

4. SECURITY ARCHITECTURE FOR SMARTPHONES, PCS, AND SERVERS

Secure MCU Protecting an IoT from Device Attacsk



- General-purpose processing CPU is complicated. Due to the complexity, the method of protection does not catch up.
- Separated trust origin. Protect a simple system in a variety of ways.
- Comprehensively analyze each attack method, build a defense method, and destroy each one.

メモリ管理

Attack cost vs. defense cost

- Attack cost example> $ 25K / device
- Defensive cost example <25 ¢ / device
- Categorify each attack method.
- Prioritize with attack costs
- ① Side channel attack
- = {Timing attack | Power analysis | Electromagnetic wave analysis} → Inexpensive
- ② Tip opening type
- = {Probe analysis | Light irradiation | Light emission analysis | FIB wiring editing
- | Protection circuit destruction | Test circuit restoration} → Expensive
- Leaked key detection on HSM server. Zero leaked keys 。

5. RISC-V SECURITY STATUS

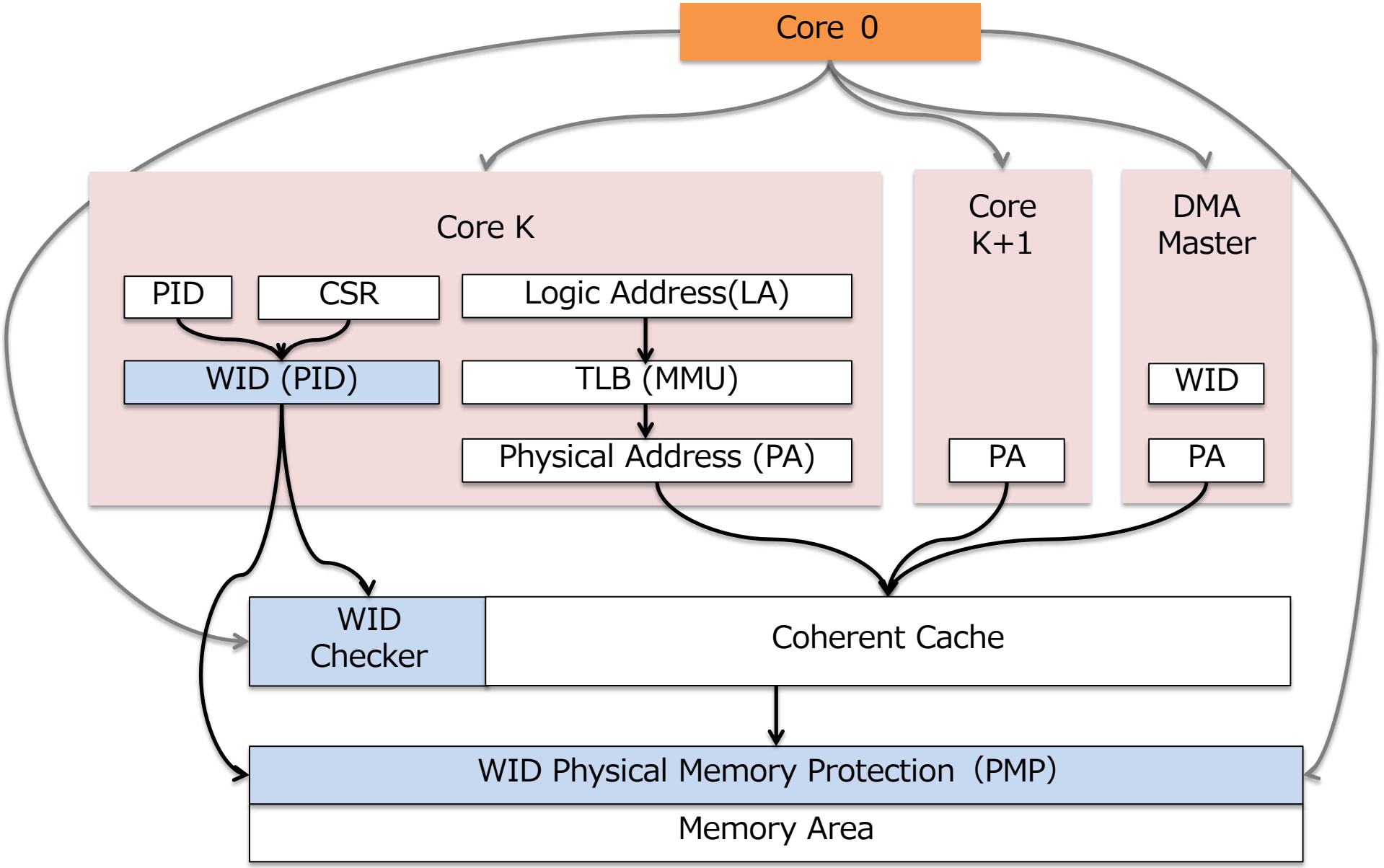
High quality security technology

Offer as open source

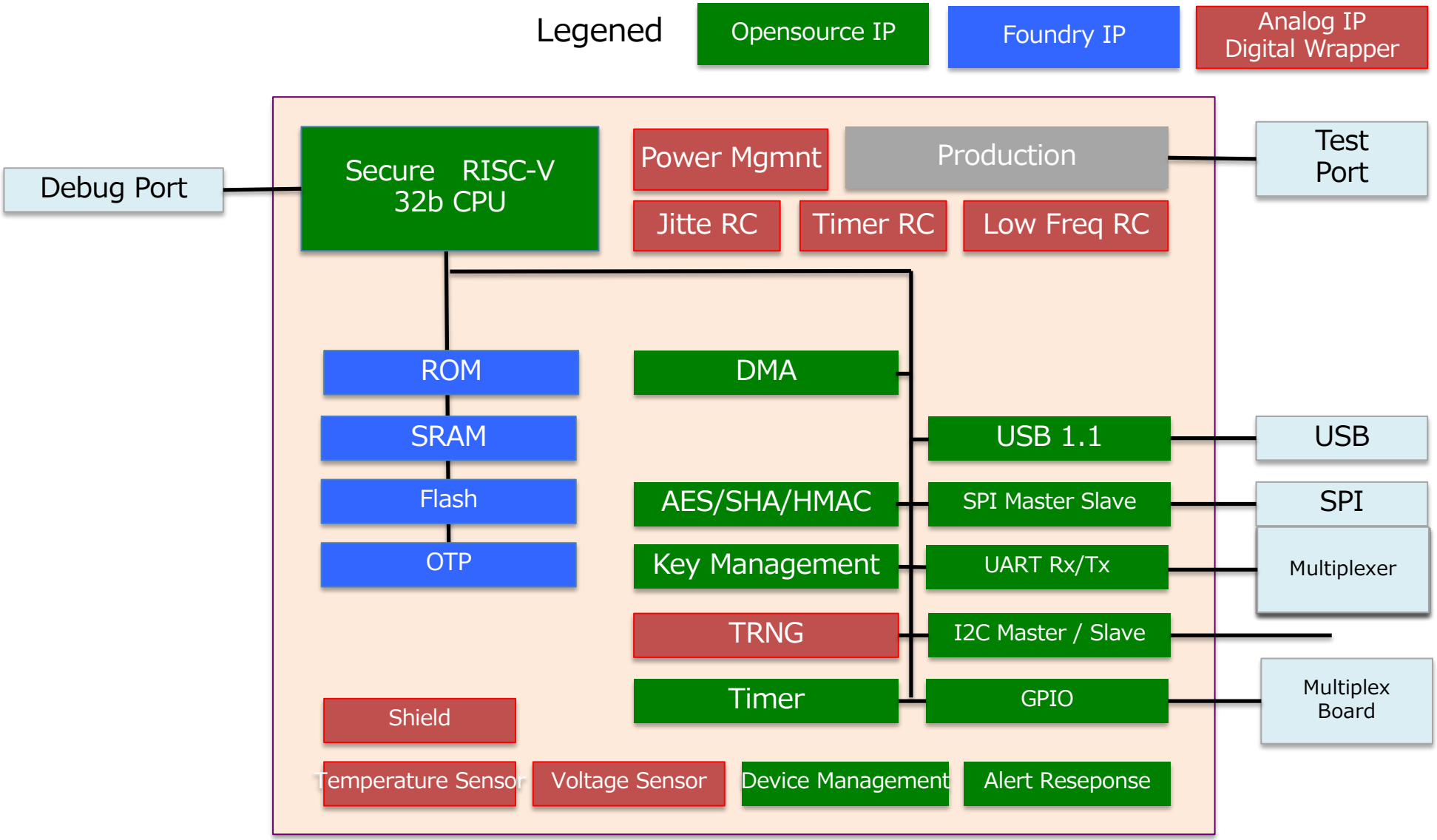
SiFive "Shield" "World Guard" announced on 10/23/2019

- Published as open source
- Both hardware and software are open source
- Reflected implementation in SPIKE, QEMU, Rocket
- Security that covers and surpasses the entire area of ARM-A TrustZone ™
- "Shield" = system name, "World Guard" = technical name
- TEE with WID, process isolation in multi-server application user mode
- Secured root of trust location as core 0 in RISC-V SoC
- Publish detailed security including memory, peripherals, bus master, DMA
- RISC-V IP Design Rules Reuse Past Architecture Technology
- ARM 2002 (expired in 2022) TrustZone ™ patent leading technology
- Virtual address → WID penetrating physical address Example: 68K function code

World ID operating principle



Open Titan Structure



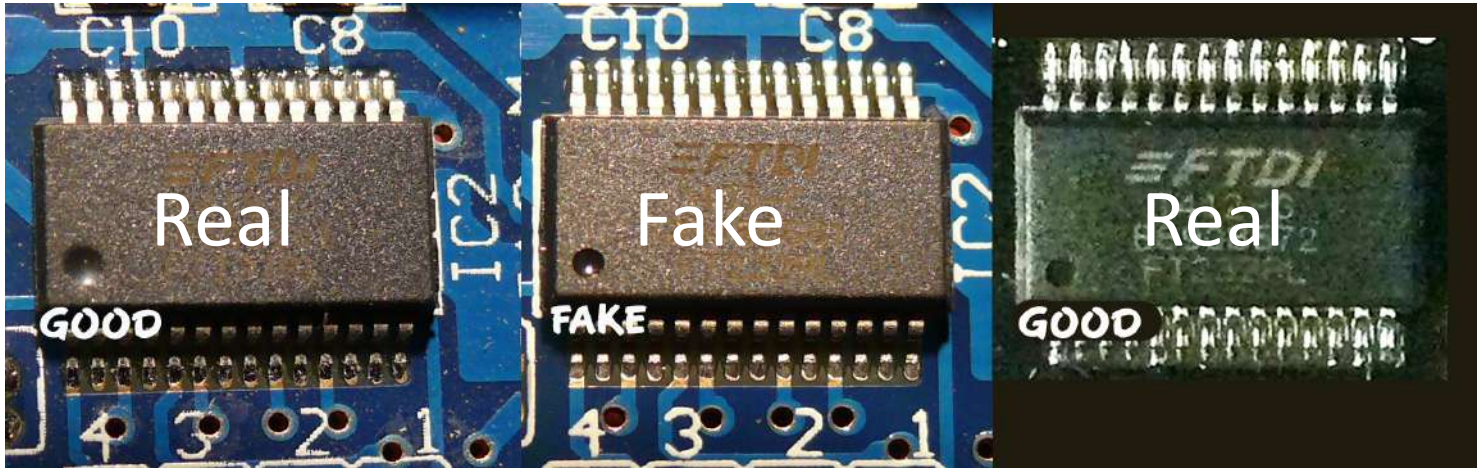
出展： Google

6.NEW DIRECTION OF SECURITY

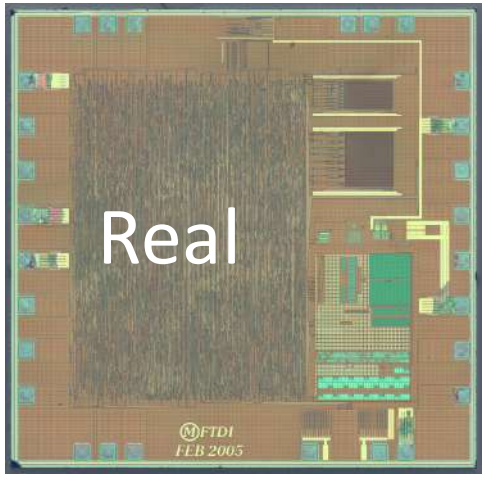
High quality security technology

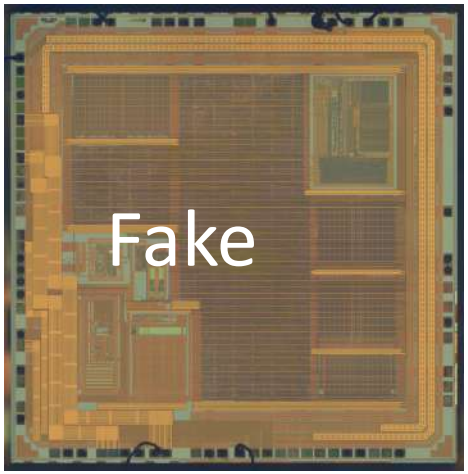
Offer as open source

Counterfeit chips are difficult to visually judge



Economic motivation for counterfeit manufacturing



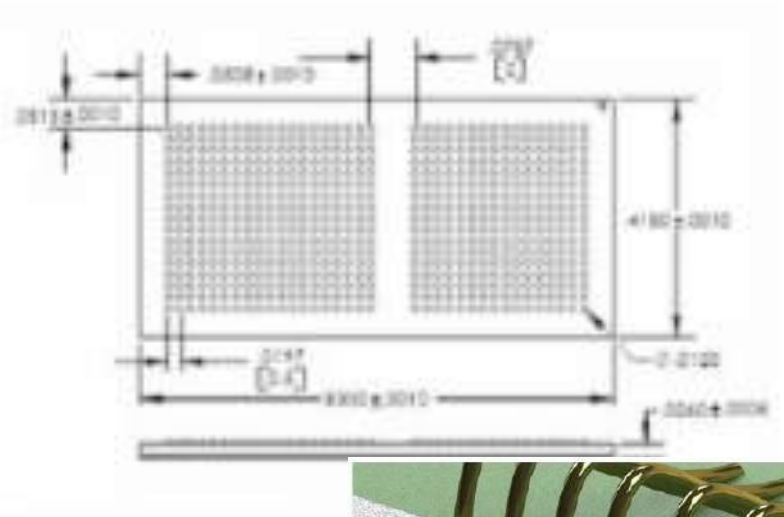


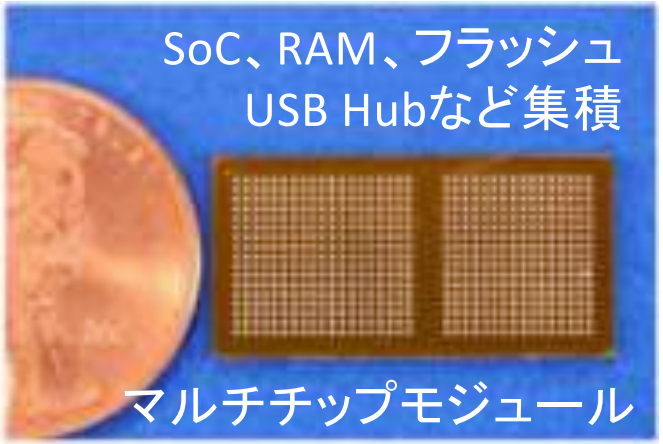
Chip Shows
"SR1107 2011-12
SUPEREAL"

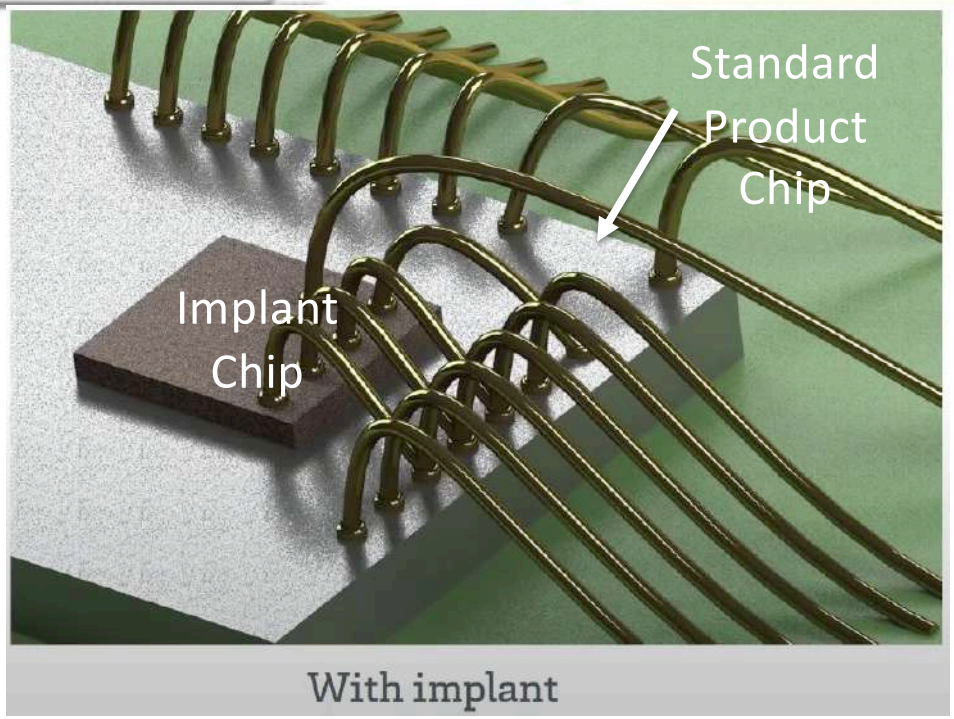
Table 1. Comparison of genuine and counterfeit technology

	Chip Size	Process	Cost	Estimated Selling Price
Real	3288x3209 µm	600-800nm	$1.00 (Software, Middleware)	$2.60
Fake	3489x3480 µm	500nm	$0.25	$0.50

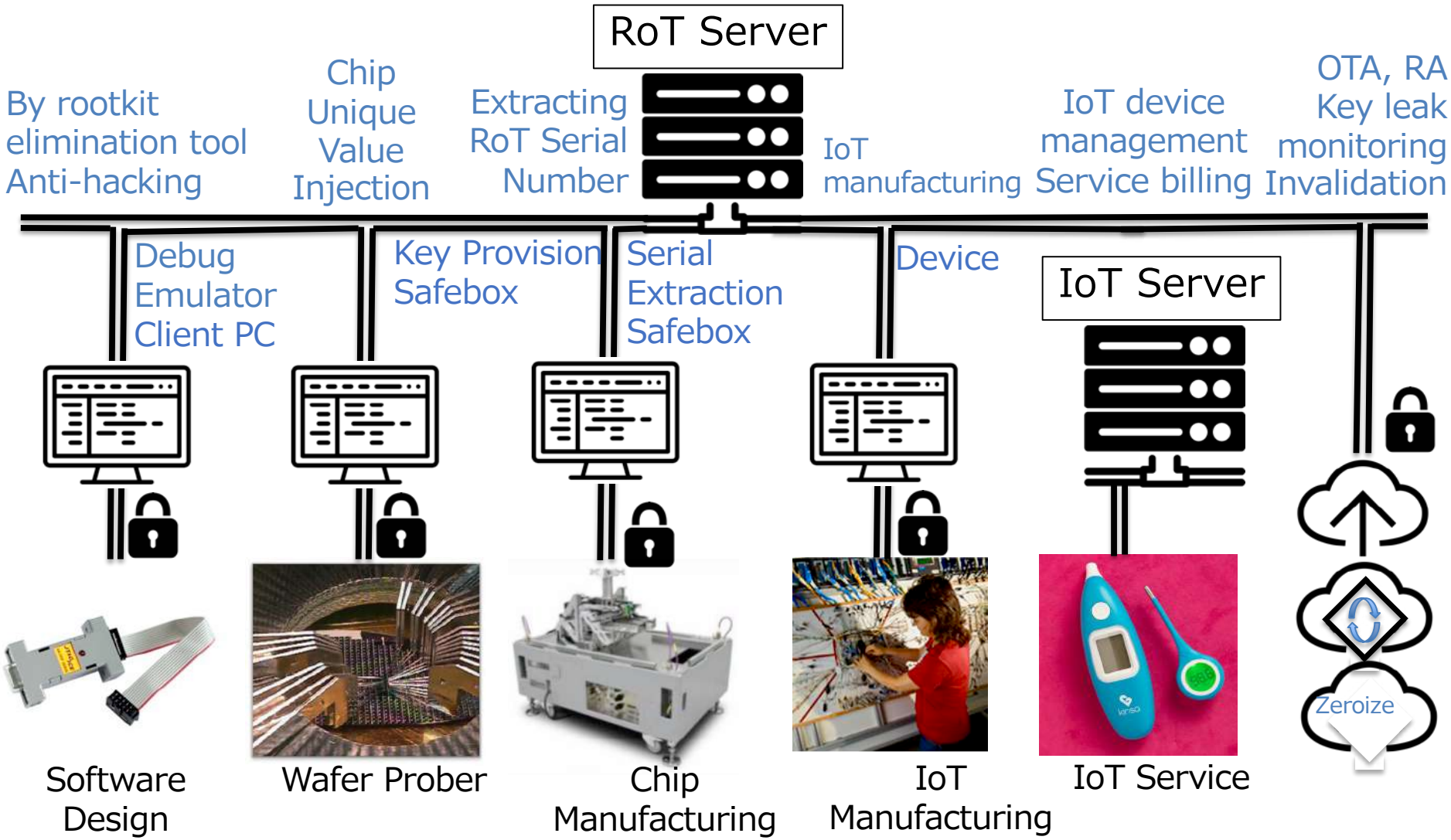
Implants are difficult to detect visually

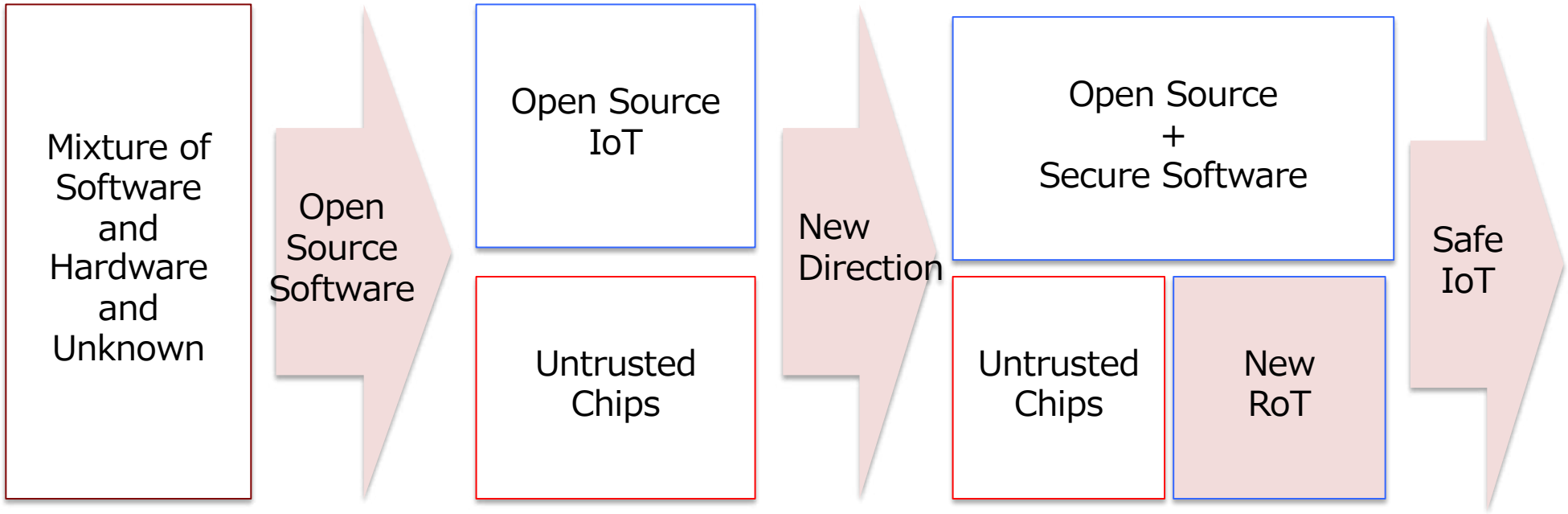




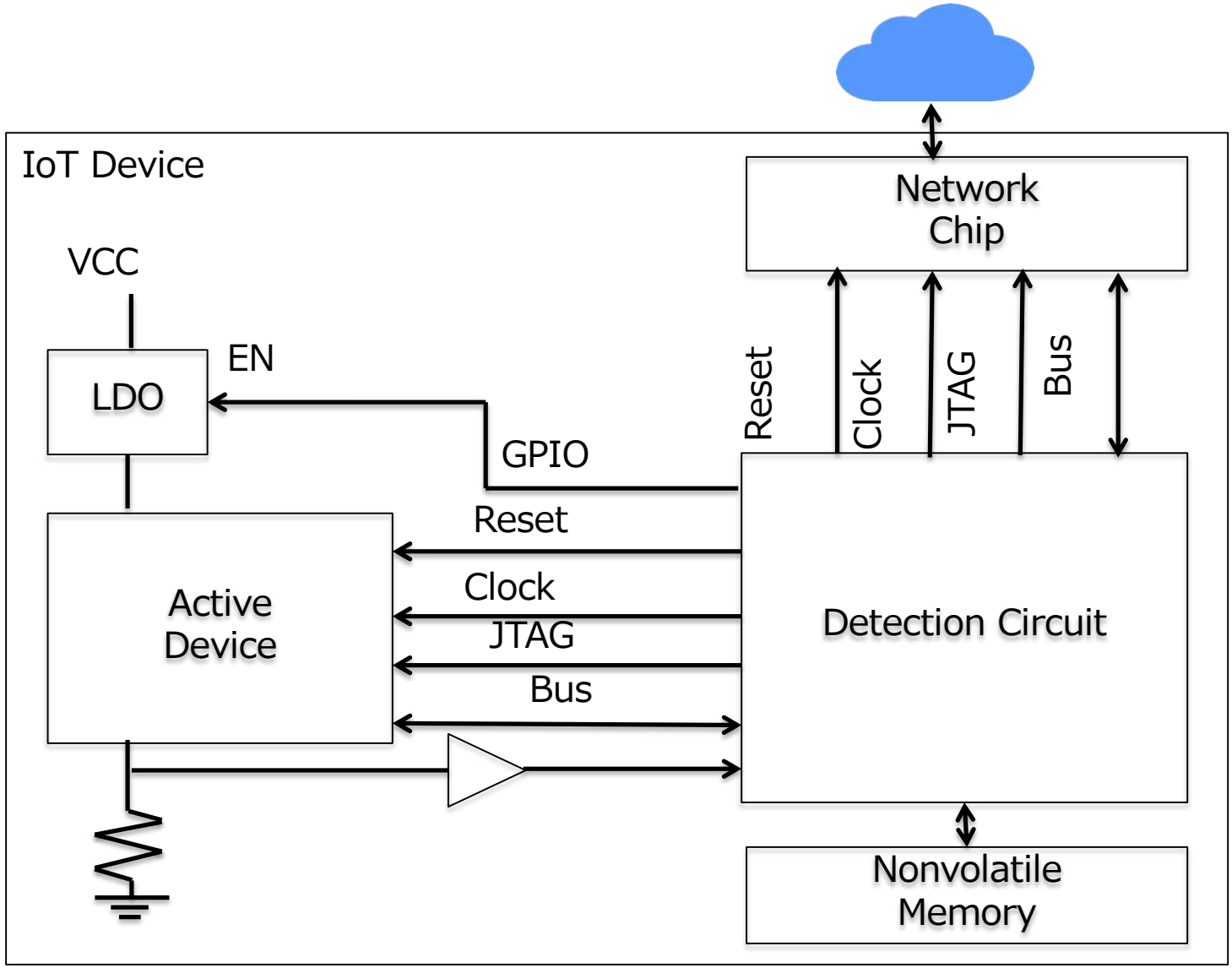


Chip supply chain and unique key infrastructure

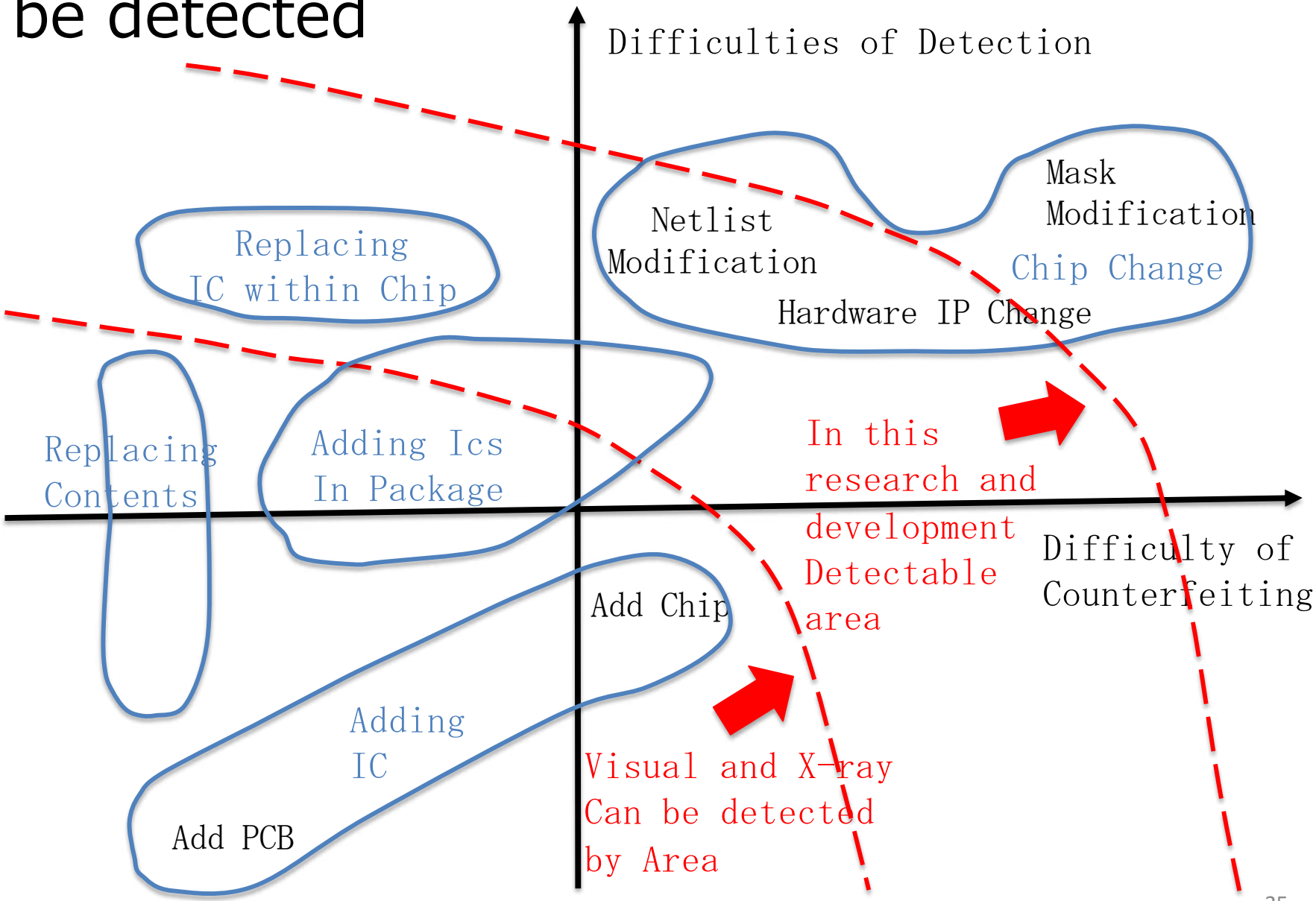




Separate and independent secure MCU to respond to IoT physical tampering



Scope of counterfeiting technology that can be detected



Credit: Bunny Huang

Summary

- RISC-V has made a huge progress both in technology and marketplace.
- As RISC-V security, open source security technology (eg Google, SiFive) and closed source technology (eg Rambus) are appearing one after another with the DARPA backing.
- RISC-V security will move further than RoT.

Part of this research is the National Research and Development Agency New Energy and Industrial Technology Development Organization (NEDO) "AI chip that enables high efficiency and high speed processing, next-generation computing technology development / innovative AI edge computing technology This was obtained as a result of the commissioned work of "Development / Secure Open Architecture Fundamental Technology and its AI Edge Applied Research and Development".