

# Driving Security from the bottom of the Stack

**Software and Supply Chain  
Assurance Forum 2025**

**Reed Hinkel, Synopsys  
Emile Monette, Synopsys**

**September 10<sup>th</sup>, 2025**

# Driving Security from the bottom of the Stack

Securing the silicon supply chain as a foundation for securing the system and software supply chain



[Who is Synopsys?](#)

---

[Semiconductor History](#)

---

[Semiconductor Standards](#)

---

[Semiconductor Regulations](#)

---

[The Supply Chain for Semis](#)

---

[Safe & Secure Software](#)

---

[Q&A](#)

---

[Closing](#)

---

[Closing](#)

# Empowering Our Customers' INNOVATION

## PURPOSE

To power innovation today  
that ignites the ingenuity  
of tomorrow

## MISSION

Empower innovators  
to drive human  
advancement

## VALUE PROPOSITION

Maximize customers'  
R&D capabilities and multiply  
their productivity

# SYNOPSYS®

Our Technology, Your Innovation™

# CREATING THE LEADER in Engineering Solutions from Silicon to Systems

**SYNOPSYS**<sup>®</sup>

Leader in Silicon Design



**Ansys**

Leader in Simulation & Analysis

## PROVIDES

comprehensive solutions  
for the entire silicon design process  
including multi-die simulation & analysis

## EXTENDS

AI leadership in EDA  
and simulation to accelerate  
customers' innovation

## ACCELERATES

creation of intelligent products by  
bringing silicon expertise across  
systems verticals

# THE LEADER in Engineering Solutions from Silicon to Systems

**#1**

in EDA

**LEADER**

in advanced node designs

**PIONEER**

in AI-powered EDA

**#2**

in silicon IP

**LEADER**

in interface & foundation IP

**PIONEER**

in IP nodes & standards

**#1**

in simulation & analysis

**LEADER**

in multi-physics

**PIONEER**

in simulation-related AI & digital twin

**~\$9B**

Revenue (TTM)

**~28K**

Employees

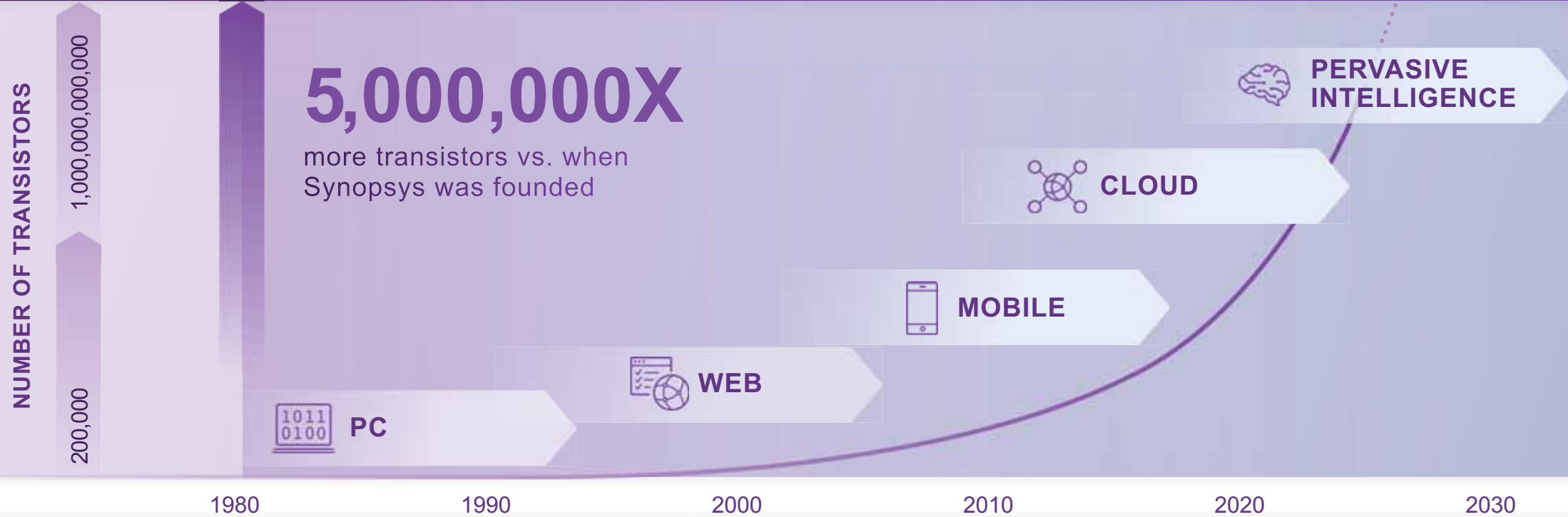
**>25%**

R&D Investment

**38**

Countries

# THE DRIVING FORCE of Transformative Technology



## SYSTEMS ANALYSIS & DESIGN

SLM<sup>1</sup>

Embedded SW Testing

eDT<sup>2</sup>

Physics simulation & Digital Engineering (Ansys acquisition)

## SILICON IP

Interface IP

Foundation IP & Processor IP

Security IP

## ELECTRONIC DESIGN AUTOMATION (EDA)

Pioneered Synthesis

Verification & Signoff

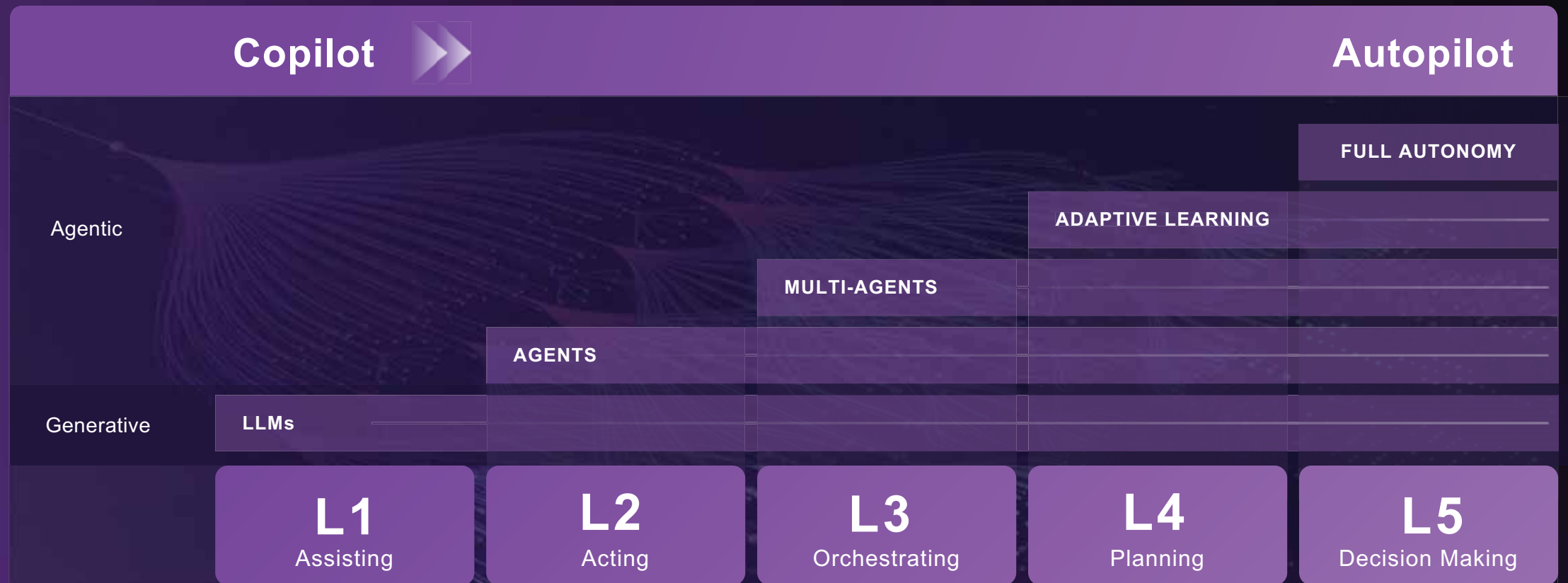
Place & Route

Emulation

AI-Powered EDA

1. "SLM" stands for "Silicon Lifecycle Management" 2. "eDT" stands for "Electronics Digital Twin"

# THE FUTURE of AI-Powered Engineering Workflows



# The Era of **PERVASIVE INTELLIGENCE**



**ARTIFICIAL  
INTELLIGENCE**



**SILICON  
PROLIFERATION**



**SOFTWARE-DEFINED  
SYSTEMS**

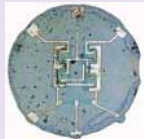
# The Birth of the Semiconductor and the first and second Era's



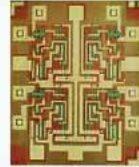
**Jack Kilby**  
Texas Instruments  
Filed March 1959  
First Integrated Circuit



**Robert Noyce**  
Fairchild Semi  
Filed July 1959  
First Planar IC



## Semiconductor device fabrication



### MOSFET scaling (process nodes)

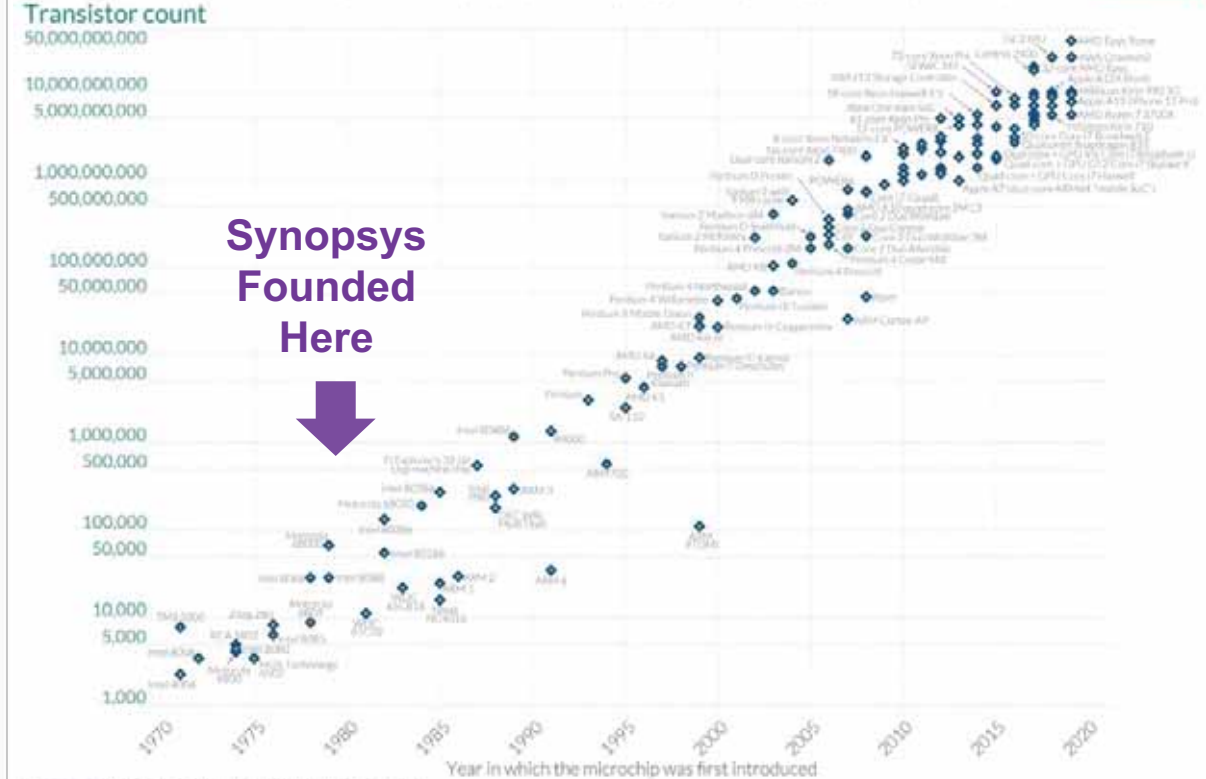
- 20 μm – 1968
- 10 μm – 1971
- 6 μm – 1974
- 3 μm – 1977
- 1.5 μm – 1981
- 1 μm – 1984
- 800 nm – 1987
- 600 nm – 1990
- 350 nm – 1993
- 250 nm – 1996
- 180 nm – 1999
- 130 nm – 2001
- 90 nm – 2003
- 65 nm – 2005
- 45 nm – 2007
- 32 nm – 2009
- 28 nm – 2010
- 22 nm – 2012
- 14 nm – 2014
- 10 nm – 2016
- 7 nm – 2018
- 5 nm – 2020
- 3 nm – 2022

- Future
- 2 nm ~ 2025
  - 1 nm ~ 2027

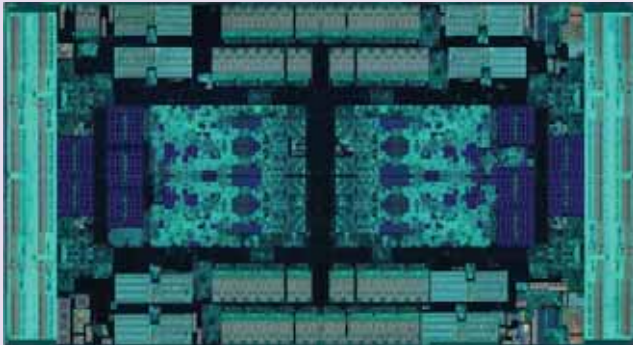
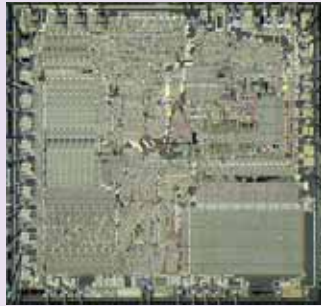
## Moore's Law: The number of transistors on microchips has doubled every two years

Our World in Data

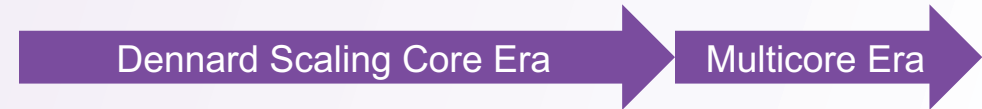
Moore's law describes the empirical regularity that the number of transistors on integrated circuits doubles approximately every two years. This advancement is important for other aspects of technological progress in computing – such as processing speed or the price of computers.



**Intel® 8088**  
1980  
29,000 Transistors  
3000nm Process Node



**AMD Epyc™ Rome**  
2019  
39.5B Transistors  
7nm Process Node



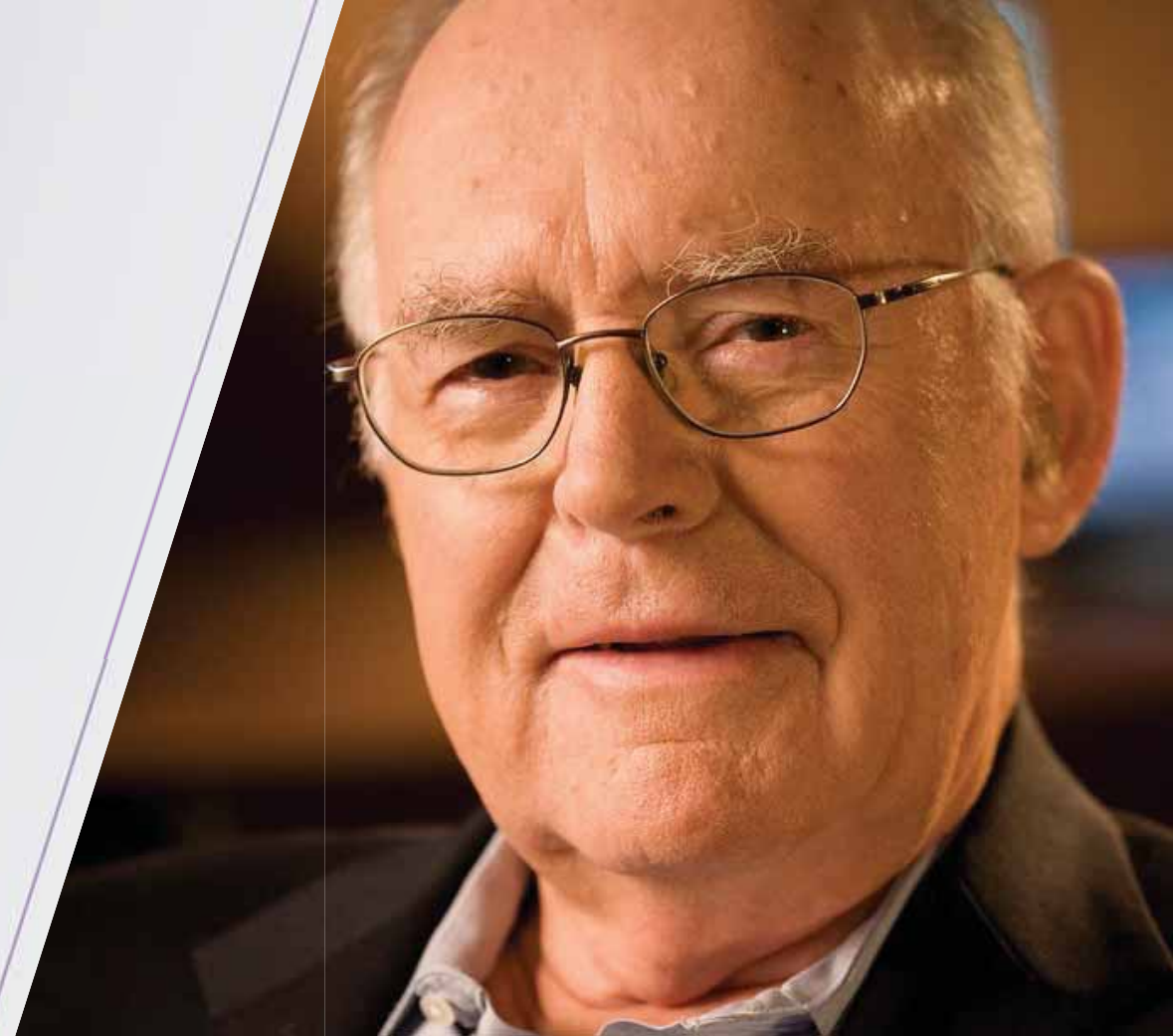
# “Day of Reckoning”

Predicted by Gordon Moore

“It may prove to be more economical to build large systems out of smaller functions, which are separately packaged and interconnected.”

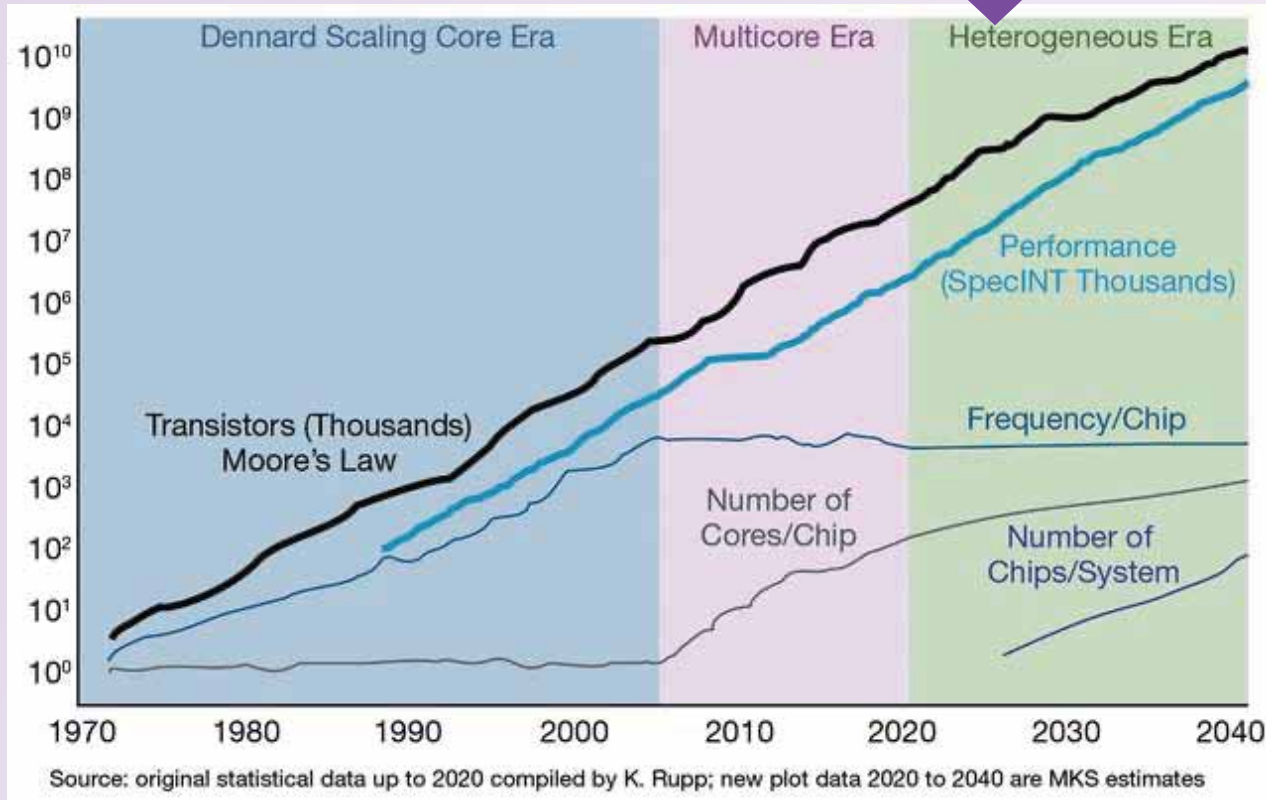
Courtesy Intel

Source: <https://newsroom.intel.com/wp-content/uploads/sites/11/2018/05/moores-law-electronics.pdf>

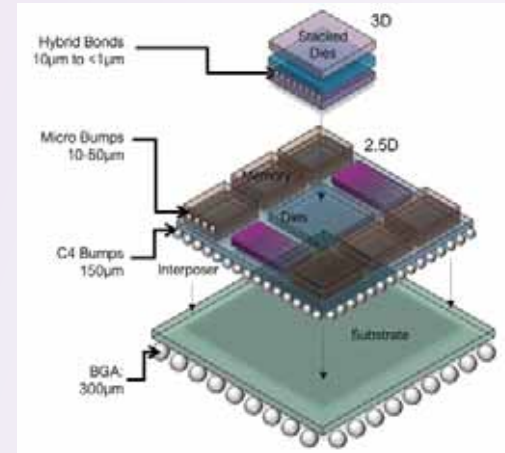


# Birth of the Heterogeneous Multi-die Era

We are here ↓

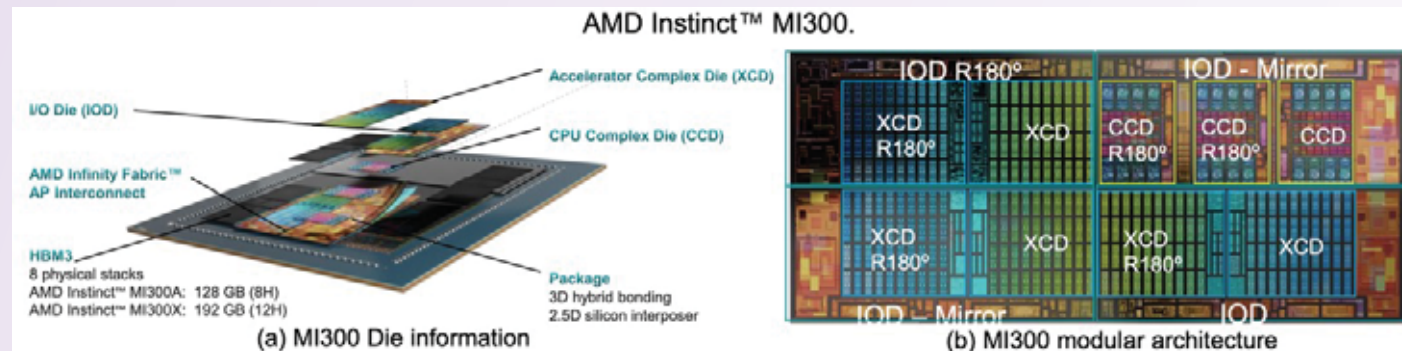
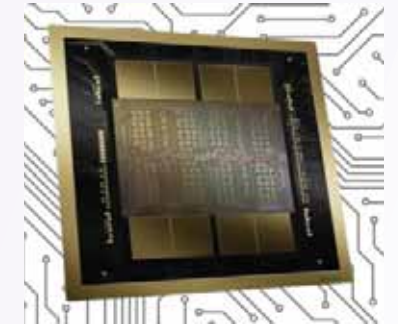


## Birth of "Chiplets" and 2.5D and 3D Array Assembly



## Nvidia Blackwell™ 2024

104B Transistors  
4nm Process Node – TSMC 4NP  
Hit the Silicon Reticule Limit so 2 Blackwell Die are packaged together in the final array for a total of 208B Transistors



2023  
146B Transistors for M1300A  
153B Transistors for M1300X  
5 & 6nm Process Nodes

# Innovations in Standardization for the Heterogenous Multi-Die Era

Growing Need for Chips and chiplets to be Compliant and interoperable

## Technology Standards Bodies



Existing standards need to adapt and extend to meet industry use case demands

## High Bandwidth Interconnect Specification Bodies



Critical innovations need to be achieved by teams of key market participants to develop solutions that will encourage market adoption through deployment of compliance testing and interoperability programs that assure different vendor implementations interoperate

## System Specifications Bodies



These are examples for the HPC and Data Center market that develop best practices and specifications with key system companies like Microsoft, Google, Dell and HPE

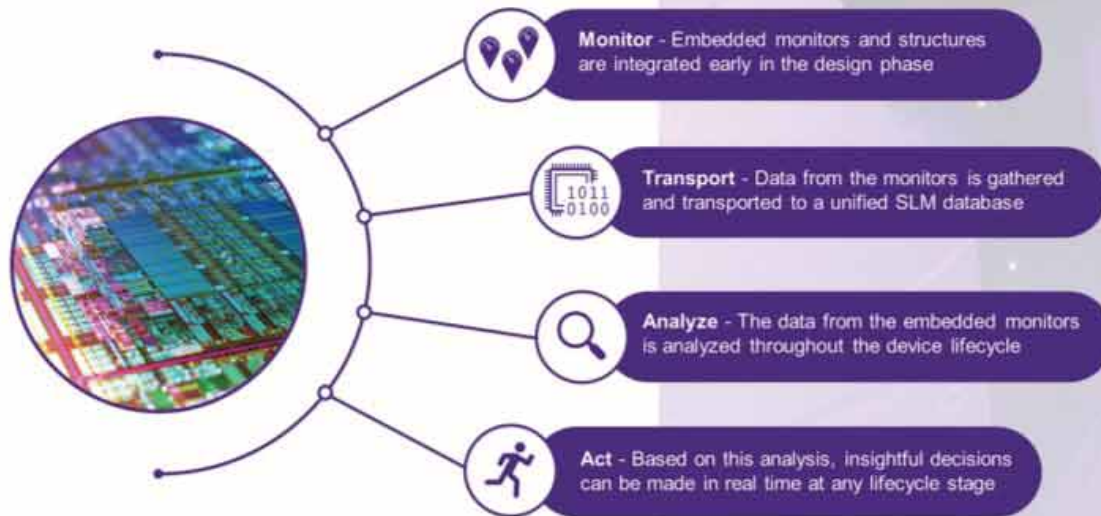
# Other Critical Innovations that have not yet been Standardized

## Silicon Lifecycle Management

- Enabling monitoring and maintainability over a devices lifetime
- Instrumental in developing digital twins of devices in operation

In-silicon visibility & insight is key

We can no longer afford to be blind to what is happening inside the chips ...



Silicon Lifecycle Management (SLM) enables optimizations at each stage of the semiconductor lifecycle

# Open Compute Project

## Moving HPC/Datacenter Industry Guidance and Specifications Forward



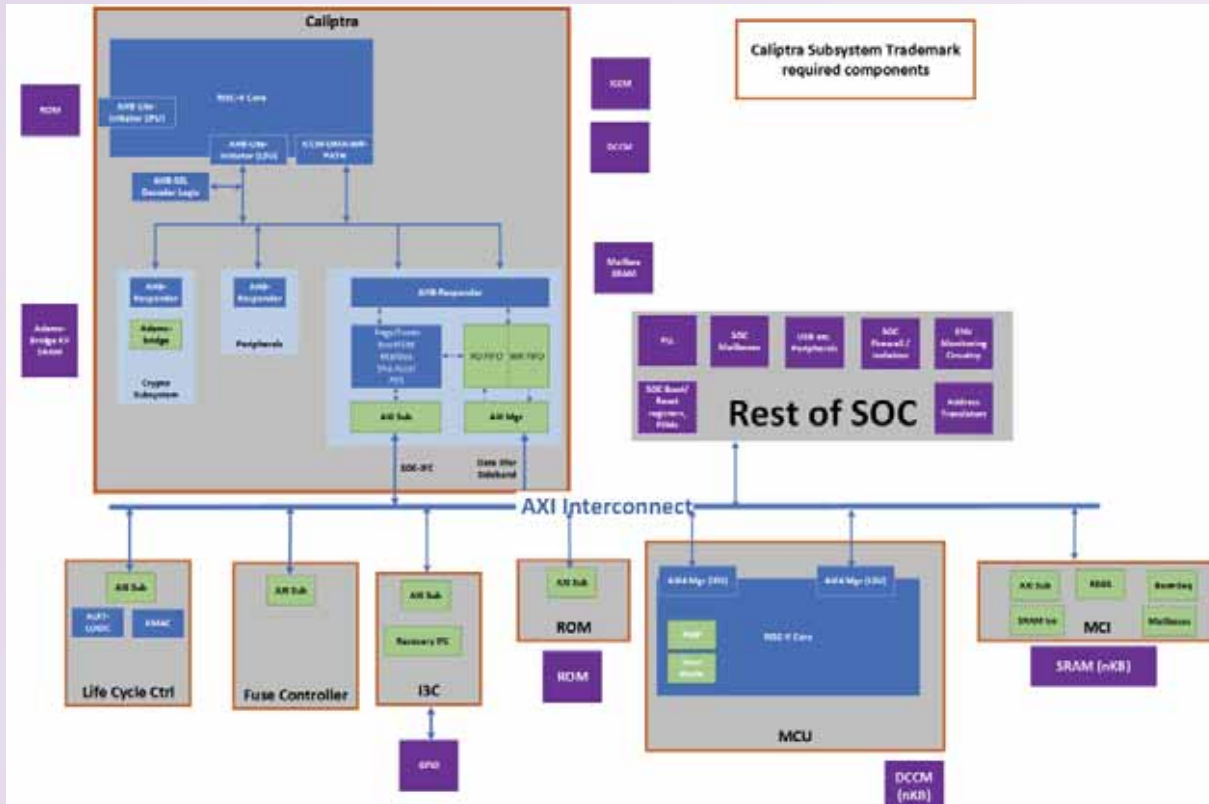
- The Open Compute Project (OCP) is a collaborative community focused on redesigning hardware technology to efficiently support the growing demands on compute infrastructure
- The OCP hosts a series of specifications, industry guidance, whitepapers, templates, and more based on a curated Contribution Model
- Key members include Microsoft, Google, Nvidia, Meta, Intel, AMD, Arm, Ampere, Seagate & Supermicro
- The focus is on solving the most pressing problems of the industry including several security topics including OCP SAFE and the Caliptra Specification.

## Open-Source Hardware Development



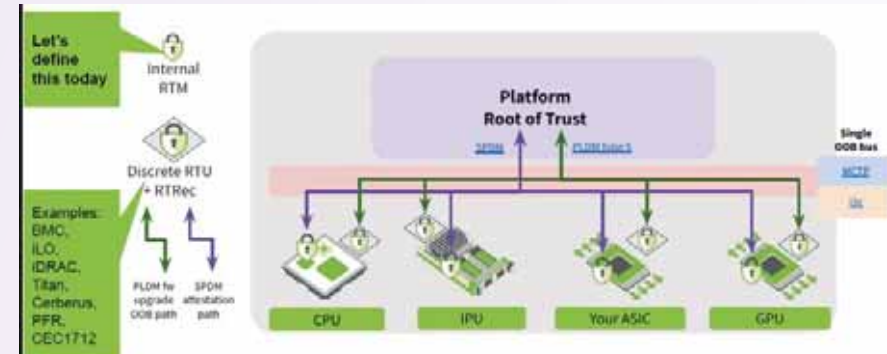
- CHIPS Alliance organized as the first Open Source for Semiconductor Hardware IP and EDA tools
- Hosted under the auspices of the Linux Foundation and follows all of the same Linux Foundation rules and procedures as the software projects that the Linux Foundation hosts including working groups like...
- The Caliptra project founders include Microsoft, Google, AMD & Nvidia who are the primary developers of the Caliptra opensource hardware and software for an Attestation Root of Trust based on code contributions from the founders and maintained by all of the member companies

# Caliptra – A Root-of-Trust for Attestation & Measurement



- Caliptra is an open-source hardware and software product jointly developed by the members of the Caliptra Working Group and the community that uses it contribute back their bug fixes, recommended patches, etc.
- The founders and primary Contributors are Microsoft, Google, Nvidia & AMD
- Over 20 different implementations have been developed into final semiconductor products from all of the member companies and many more
- Caliptra was spawned by the founders' desire to improve the security and quality of implementations in product that come from a diverse array of companies.
- It was a response to guidance from NIST 800-193
- It includes TCG DICE & SPDM 1.x Attestation in the overall architecture

	Detection	Protection	Recovery	Identity	Measurement	Lifecycle	Ownership	Attestation
	RTM : RoT for Measurement (a.k.a. RTD)	RTU : RoT for Update	RTRec	Manufacturer Identity aligned to TCG DICE	Code & configuration posture of the device.	Debug mode (ON/OFF), established at reset.	No stateful transfer. Vendor authored firmware only, with stateless Owner Authorization	Identity & Measurement reporting using DMTF SPDM v1.2+
	<b>Integrated Silicon RoT</b> <ul style="list-style-type: none"> <li>• Well and narrowly defined job</li> <li>• Measure, verify and attest</li> <li>• In package – best bet against physical attacks on integrity</li> <li>• Limited fuses</li> </ul>	<b>Discrete RoT Chip</b> <ul style="list-style-type: none"> <li>• Mitigate DoS at scale</li> <li>• RTU: reject random blobs pushed at scale</li> <li>• RTRec: automated recovery against buggy updates</li> <li>• OK to be a separate discrete element                             <ul style="list-style-type: none"> <li>• Physical attacks irrelevant to scalable DoS mitigation</li> </ul> </li> <li>• Integrated flash for unlimited renewability                             <ul style="list-style-type: none"> <li>• Enforce versions, owners, rotations</li> </ul> </li> </ul>						



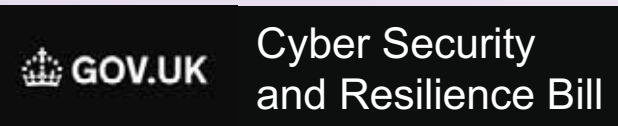
# Increasing Government Influence on the industry

In addition to compliance to industry standards Government Mandate by Legislation various Government Agencies have a growing interest in regulating silicon and systems aimed at increasing their cybersecurity and readiness to confront emerging threats in a dynamic world environment

## Representative Government Acts & Directives



IoT Cybersecurity Improvement Act



Cyber Security and Resilience Bill



## Representative Standards Agencies



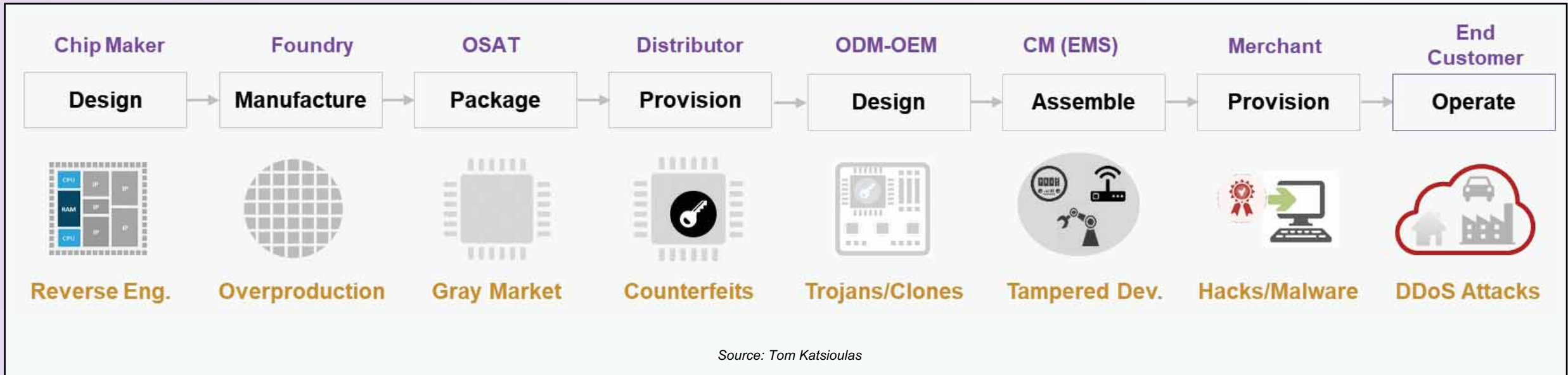
## Representative Regulatory Agencies



UNECE

# Growingly Complex and Untrusted Silicon Supply Chain

Leading to Many Potential Attack Points and Variety of Attacks in Production Process



USA  
Lower Threat  
WW  
High Threat

USA  
Lower Threat  
Taiwan  
High Threat

China/Malaysia  
Vietnam  
High Threat  
USA/EU for  
Advanced Packing  
Lower Threat

Taiwan/China  
Malaysia/Vietnam  
High Threat  
USA/EU  
Lower Threat

Taiwan/China  
Malaysia/Vietnam  
High Threat  
USA/EU  
Lower Threat

Taiwan/China  
Malaysia/Vietnam  
High Threat  
USA/EU  
Lower Threat

WW  
High Threat  
Assumed

WW  
High Threat  
Assumed

As the value of confidential IP or data related to AI increases the insider threats become greater

# Government & Industry acting on Semiconductor Supply Chain Standards

## Moving Industry Guidance Forward



- Hosting a series of Workshops on Semiconductor Traceability & Provenance aimed at determining what is needed in guidance and potential regulation
- Next workshop is in October 21<sup>st</sup> at NIST in Gaithersburg, MD
- Gathering insights to needs and requirements from industry
- Previous presentations from industry technology suppliers
- Next will be members of Hyperscaler industry like Microsoft, Google, Meta, IBM, Dell & HPE and Automotive industry like GM, Bosch & Stellantis, plus Government like DOD, DOC, DOE & DHS

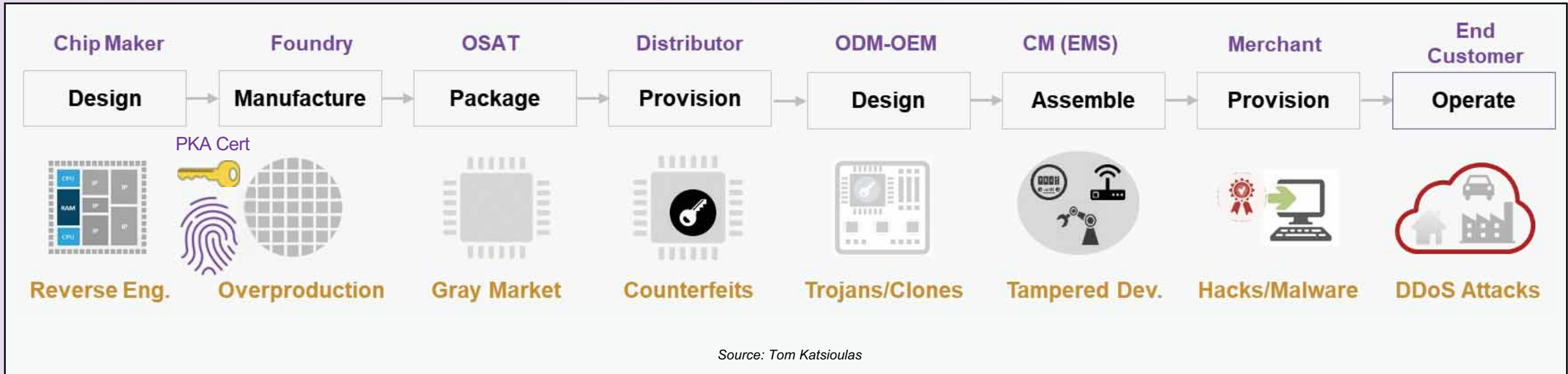
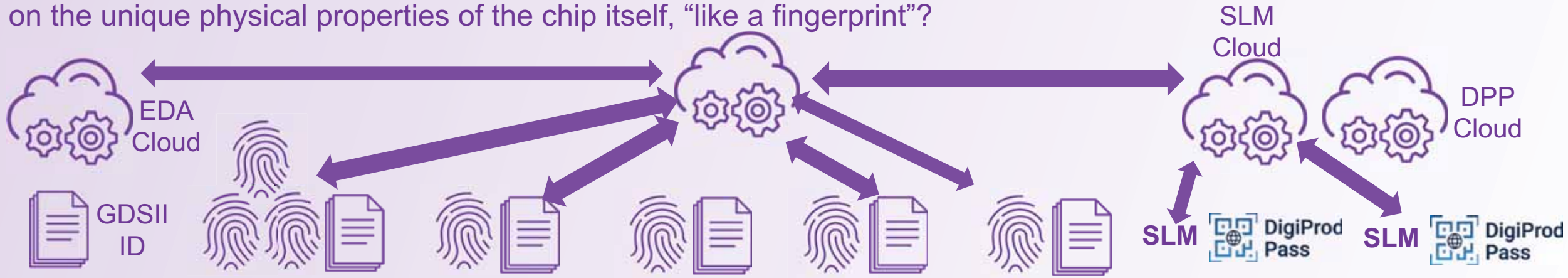
## Standardization being Explored



- Conducting a Semiconductor Traceability and Provenance Phase 0 exploration of the industry gaps & requirements to determine what standardization is possible and practical to deliver to the Semi industry
- Current participants in addition to Synopsys include NIST, IBM, Microsoft, Rambus, Cadence, Intel, AMD, Qualcomm, Micron, Stellantis, Airbus, Lockheed, Global Foundries & Samsung
- The working group will wrap up work by the end of 2025 and make recommendations on what is required
- Current stage of work is a survey of existing industry solutions

# Conceptual Solution to fill the gaps with a SRAM PUF "fingerprint"

There is presently a gap in the manufacturing where an individual identity does not exist for use to track the product through the earliest stages of processing until it can have an ID injected by test equipment. This has various weaknesses from a pedigree and provenance perspective, but what if we were to derive an intrinsic identity based on the unique physical properties of the chip itself, "like a fingerprint"?



Source: Tom Katsioulas

# Strong Security Starts in Hardware – Building it from the Ground Up

If You Don't Have a Root of Trust in Hardware, Software-Only Security Solutions are...

Easy  
to copy

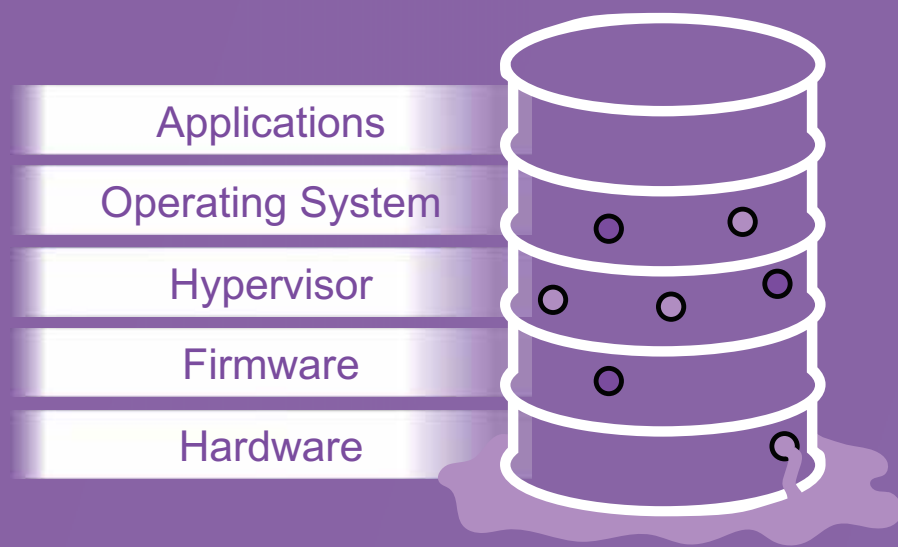
Easy to  
reverse engineer

Easy to debug  
(while running)

Easy(ier) to attack  
with side channels

Easy to  
tamper with

## Hardware Security is the foundation



## Software on unprotected hardware...



is a castle built on quicksand

# Complete Silicon Security Solution

## Market-Leading Toolbox of Configurable Cryptographic Building Blocks

**Crypto Cores:** Symmetric & asymmetric crypto engines, including the latest standards-compliant Post-Quantum Cryptography (PQC)

**Physical Unclonable Functions (PUFs):** Market-leading IP that generates keys from unique physical properties of SoCs and since keys are never stored, PUFs eliminate the risk of key extraction

**Random Number Generators:** Market-leading IP that generates random numbers that are required for most cryptographic functions

**Cryptography Software Library:** Comprehensive suite of encryption and certificate processing functions for embedded applications

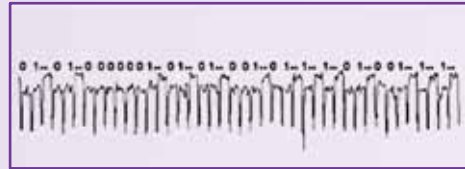
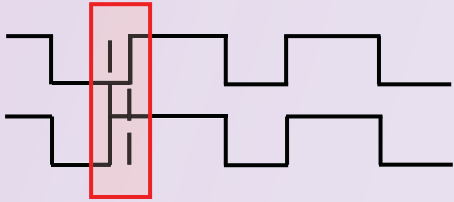
**Secure Boot SDK:** Allows developers to implement secure boot using software-only constructs or with Synopsys offload engines



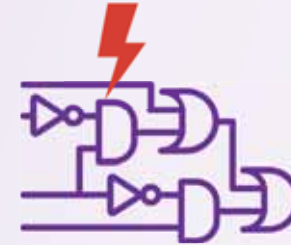
Proven in 1.5B+ Data Center, IoT, Consumer, Automotive & Mobile Chips

# Protecting Against Side-Channel Attacks

Side-Channel Countermeasures to Prevent Leaking Sensitive Information



Paul Kocher, Joshua Jaffe, and Benjamin Jun



## TIMING ANALYSIS

### Countermeasures:

- Constant-time algorithms
- Activity masking

## DIFFERENTIAL POWER ANALYSIS

### Countermeasures:

- Constant-weight codes
- Noise generation

## FAULT INJECTION

### Countermeasures:

- Constant-time algorithms
- Activity masking

There are more side-channel attacks...

... use a combination of different countermeasures

# What is Quantum Computing?

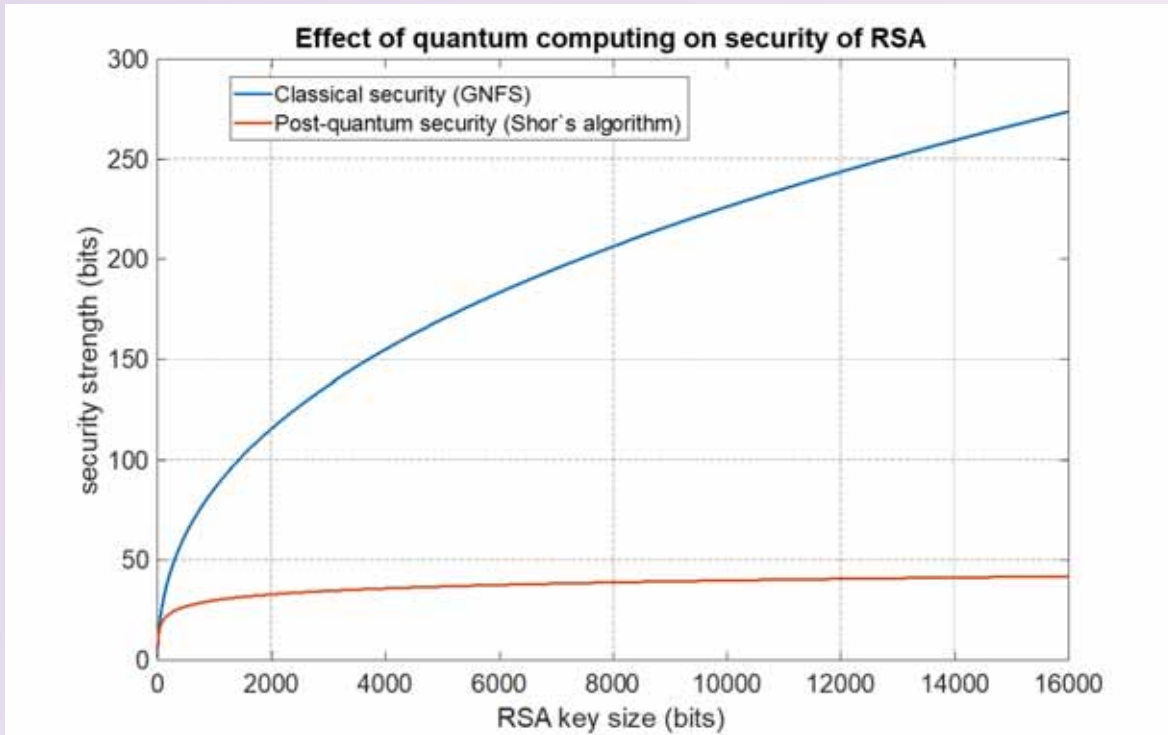
Quantum Computing is about building a computer and algorithms that exploit quantum phenomena, like superposition and entanglement (first computer: 1998)



Image source: IBM Q System One

Quantum algorithms have the potential to solve some difficult problems (e.g., factoring large numbers) much faster than an algorithm on a classical computer can

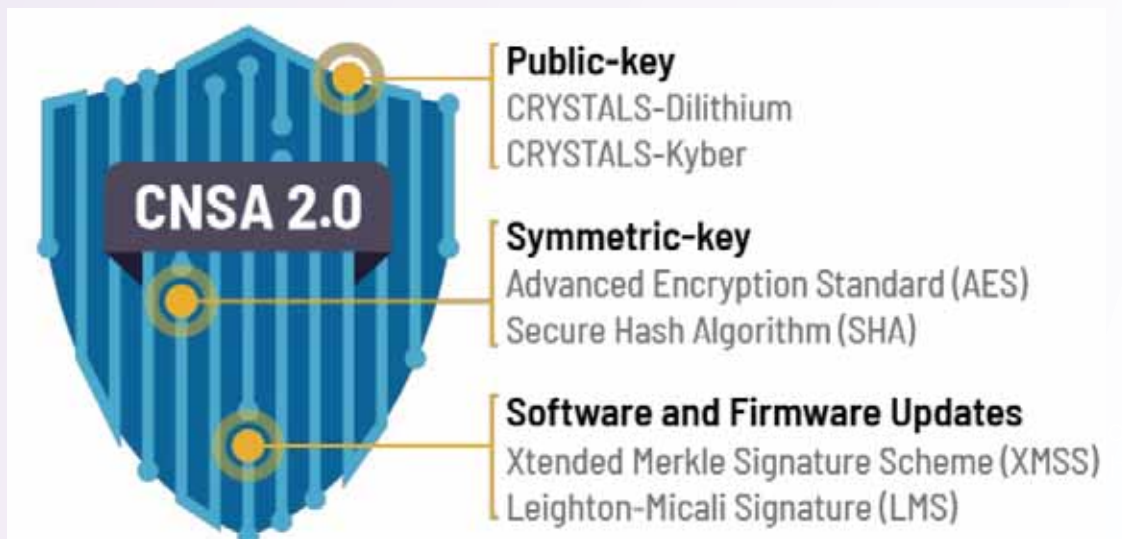
# Quantum Computing Attack Expectations



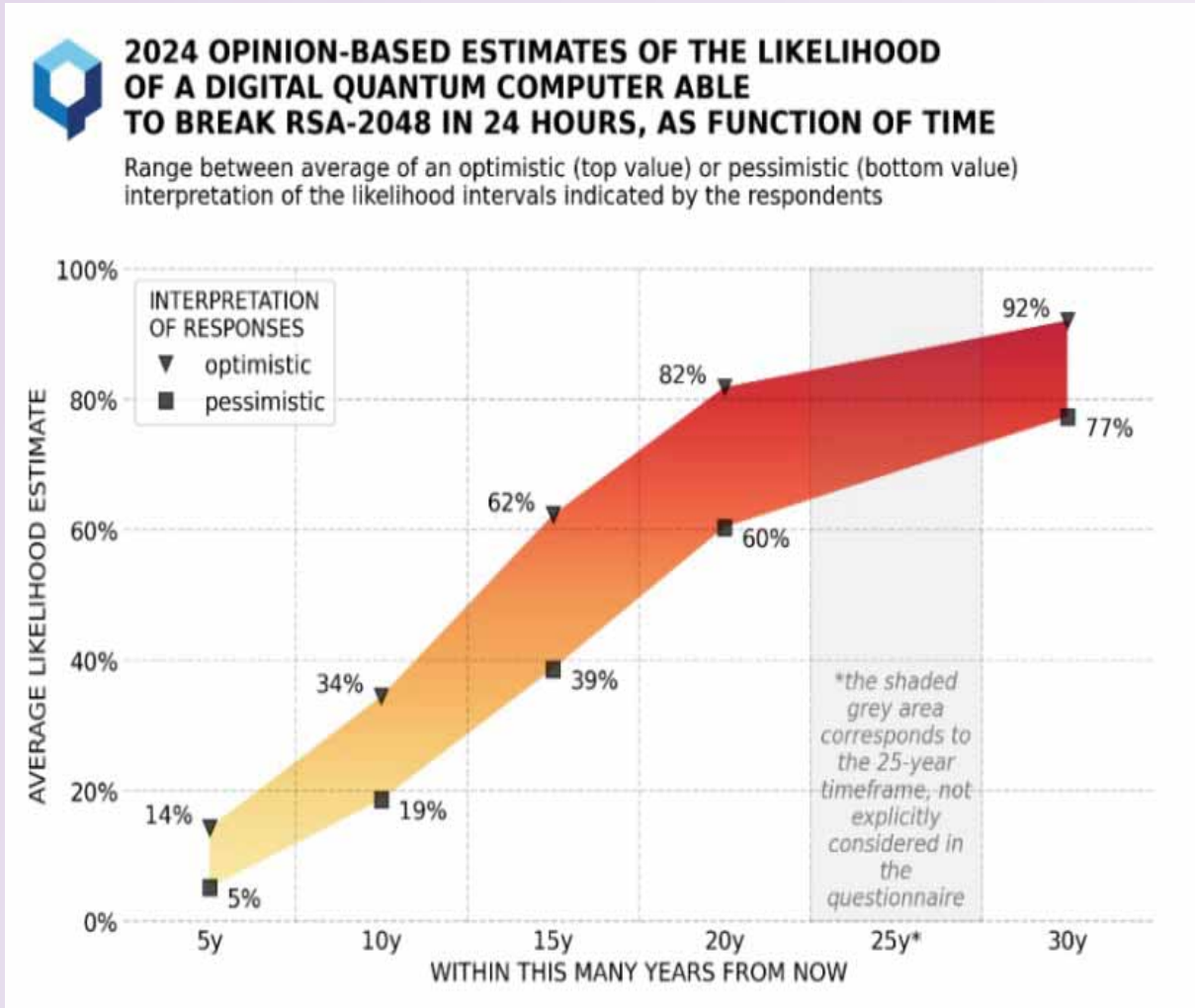
Classical Security Algorithms have limited defenses against Quantum attack causing the bit strength and therefore the processing cost of maintaining their use to skyrocket.

Table 1 - Impact of Quantum Computing on Common Cryptographic Algorithms

Cryptographic Algorithm	Type	Purpose	Impact from large-scale quantum computer
AES	Symmetric key	Encryption	Larger key sizes needed
SHA-2, SHA-3	-----	Hash functions	Larger output needed
RSA	Public key	Signatures, key establishment	No longer secure
ECDSA, ECDH (Elliptic Curve Cryptography)	Public key	Signatures, key exchange	No longer secure
DSA (Finite Field Cryptography)	Public key	Signatures, key exchange	No longer secure



# It's a Matter of Time...



Quantum Threat Timeline Report 2024,  
Global Risk Institute

Based on predictions, there is still time to prepare for Quantum Computing threat

However, there is another threat:  
**“Harvest now, decrypt later”**

# NIST Initiative on Post-Quantum Cryptography

## Moving Standardization Forward



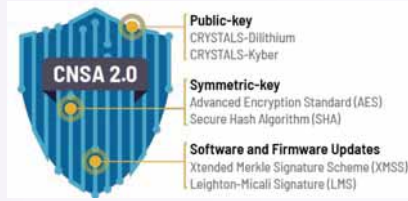
Post-quantum cryptography (PQC) are cryptographic algorithms designed to be secure against cryptanalytic attacks by quantum computers



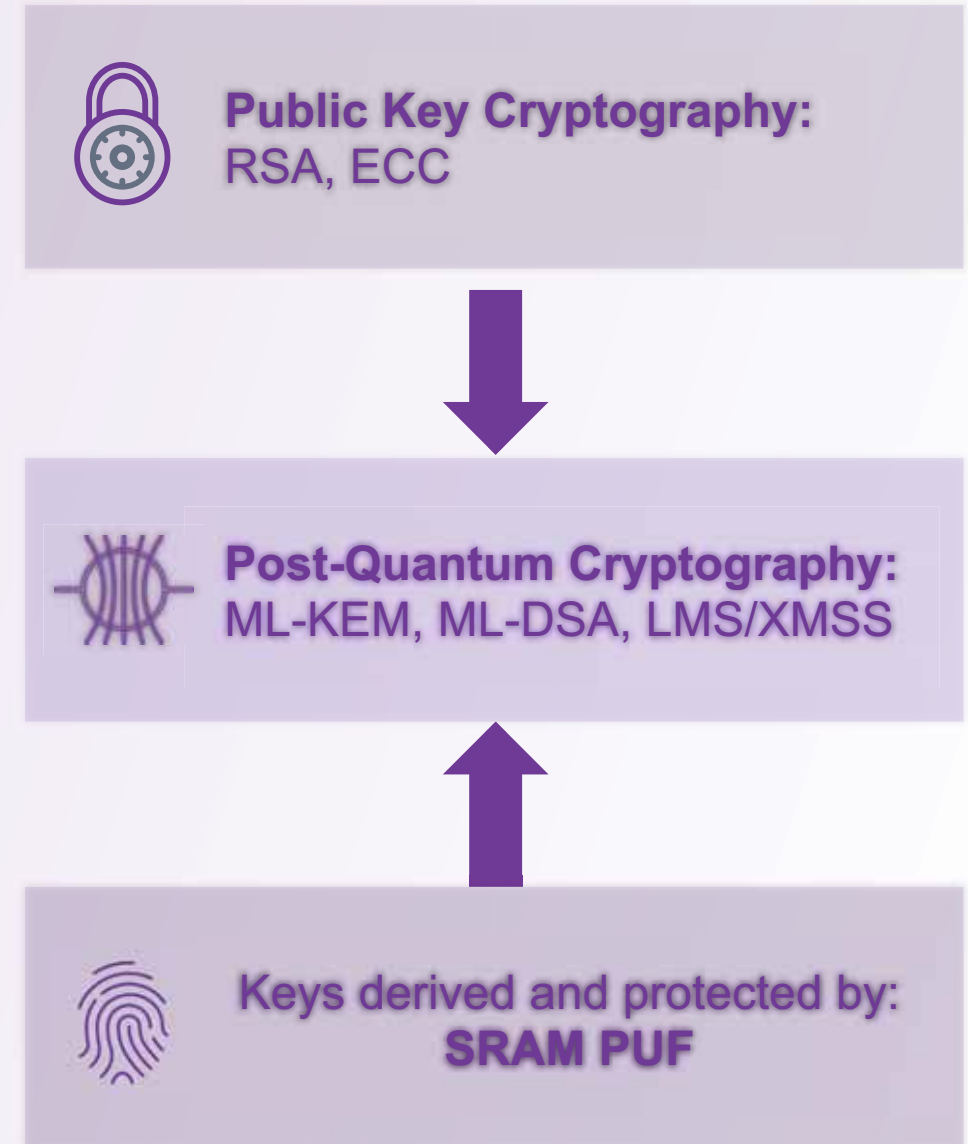
National Institute of Standards and Technology (NIST) is driving the standardization process for quantum-resistant public-key cryptographic algorithms

# Post-Quantum Cryptography – Migration Needs to Start Now

## CNSA v2.0: Quantum Resistant Commercial National Security Algorithm Suite



Algorithm	Specification	Parameters
<b>GENERAL PURPOSE ALGORITHMS</b>		
AES	FIPS 197	Use 256-bit keys
ML-KEM	FIPS 203	ML-KEM-1024
ML-DSA	FIPS 204	ML-DSA-87
SHA	FIPS 180-4	SHA-384 or SHA-512
<b>ALGORITHMS ALLOWED IN SPECIFIC APPLICATIONS</b>		
LMS	NIST SP 800-208	All parameters approved
XMSS	NIST SP 800-208	All parameters approved
SHA3	FIPS 202	SHA3-384 or SHA3-512



**All National Security Systems need to comply by 2035**

# NIST Proposed Timelines for PQC Transition



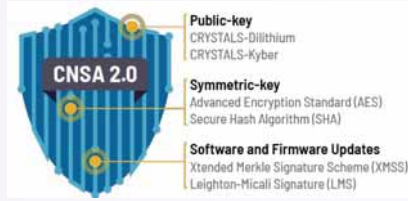
NIST IR 8547 Initial Public Draft (Nov 2024)

Algorithm Type	Name	Standard	Parameters	Deprecated	Disallowed
Key Establishment	Finite Field DH and MQV	SP 800-56A	112 bits of security strength	After 2030	After 2035
			$\geq 128$ bits of security strength		After 2035
	Elliptic Curve DH and MQC	SP 800-56A	112 bits of security strength	After 2030	After 2035
			$\geq 128$ bits of security strength		After 2035
	RSA	SP 800-56B	112 bits of security strength	After 2030	After 2035
			$\geq 128$ bits of security strength		After 2035
Digital Signature	ECDSA	FIPS 186	112 bits of security strength	After 2030	After 2035
			$\geq 128$ bits of security strength		After 2035
	EdDSA	FIPS 186	$\geq 128$ bits of security strength		After 2035
	RSA	FIPS 186	112 bits of security strength	After 2030	After 2035
			$\geq 128$ bits of security strength		After 2035

**The time to start preparing for PQC transition is now!**

# Expected Phased in approach of industry adoption

Be aware of that that systems we all maintain need to be Quantum Ready by 2030 and for some aspects required adoption has already started!



We are here ↓



**Make sure your supply chain is Quantum-Ready so you are safe from the threat !**



Questions & Answers

· ՇԱՆՐՀԱԿԱԼՈՒԹՅՈՒՆ · PAKKA PÉR FYRIR · शुक्रिया · K  
ERIM · KÖSZÖNÖMΒΒ · MAHALO · مشكراً لك · MERCI · ՇԱՆՐ  
TAKK SKAL DU HA · ありがとう · KÖSZÖNÖM · 고맙습니다  
· MAHALO · مشكراً لك · MERCI · ՇԱՆՐՀԱԿԱԼՈՒԹՅՈՒՆ · P

# THANK YOU

· ΤΩ · DZIĘKUJĘ CI · TERIMA KASIH · متشكر · 谢谢 · GRAZIE  
· ຂອບໃຈ · SALAMAT · TAKK SKAL DU HA · ありがとう · KO  
· DĚKUJU · ਤੁਹਾਡਾ ਧੰਨਵਾਦ · СПАСИБО · GRATIAS TIBI · थ  
YOU · TEŞEKKÜR EDERİM · KÖSZÖNÖMΒΒ · MAHALO · ك

**SYNOPSYS<sup>®</sup>**

Our Technology, Your Innovation™

# Backup

