ITRI
Industrial Technology
Research Institute

How Post-Quantum Cryptography and AI Are Changing the Security Landscape

Ensuring Integrity and Trust in a Highly Automated Digital World

Dr. Wei-Chung Hwang
Deputy General Director, Industrial Technology Research Institute (ITRI)

Dr. Wei-Bin Lee, Convener
Post-Quantum Cryptography Cybersecurity Industry Alliance (PQC-CIA)

2025/8/5

Evolvement of IT Technologies

Digital
Internet
Social
Mobile

Intelligence
Discriminate,
Generative,
Agentic,
Physical

Quantum
Communication,
Sensing,
Computing

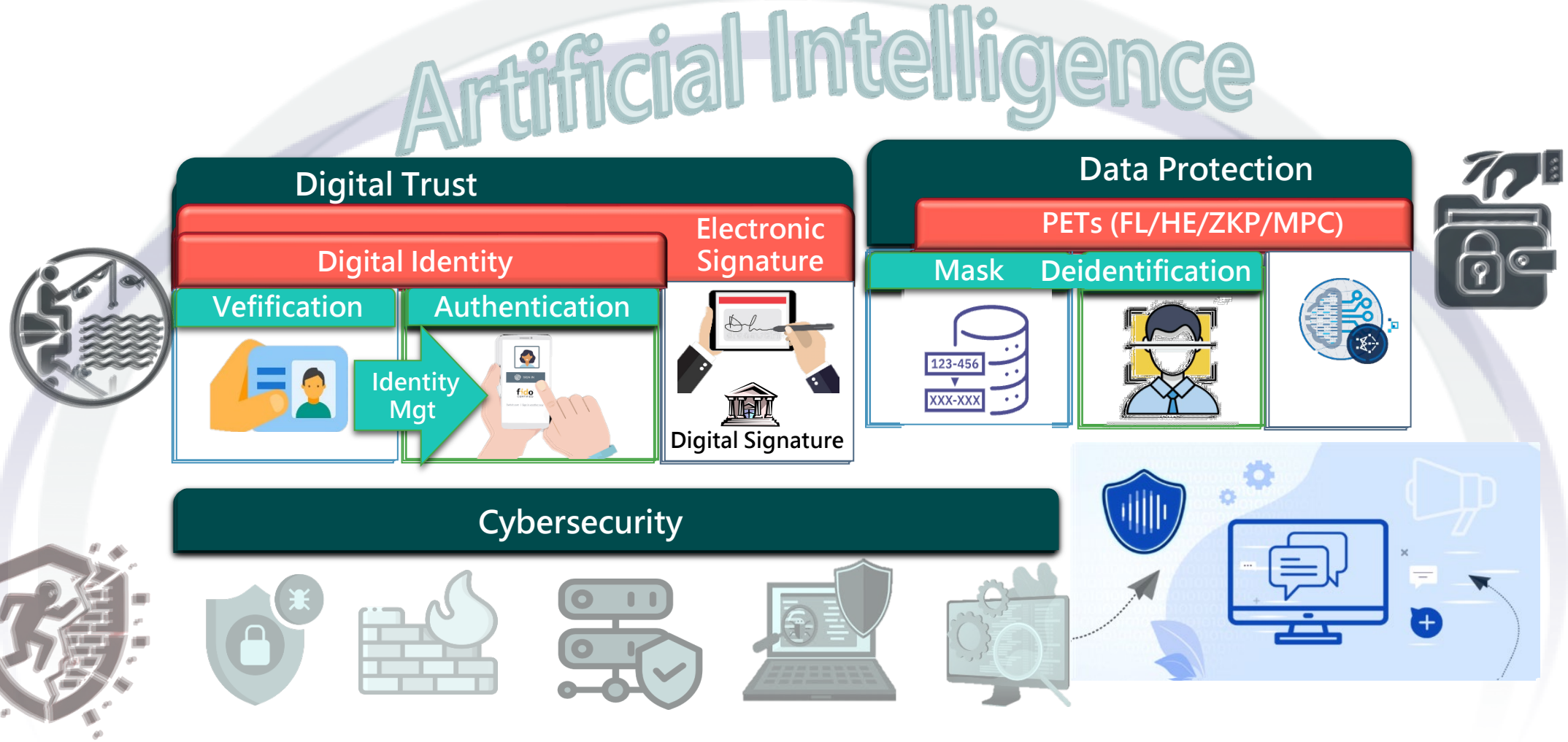
Support

Threat

Trustworthy: Identity, Signature, Data, Security

ITRI
Industrial Technology Research Institute

Foundations of Trustworthy Digital Society



ITRI Industrial Technology Research Institute

Frameworks of Digital Trust

Multi-Factor Authentication

Biometrics

Hardware

OTP & Password

Wallet

Authenticator

User (Receiver)

Relying Party (Verifier)

Certificate Authority

Identity Provider (Issuer)

Distributed Ledger

SSI/DID

fido ALLIANCE

PKI

Public Key Cryptography (PKC)

Post Quantum Cryptography (PQC)

Cryptography

Identity Management

Certification & Compliance

Governance

Highly regulated

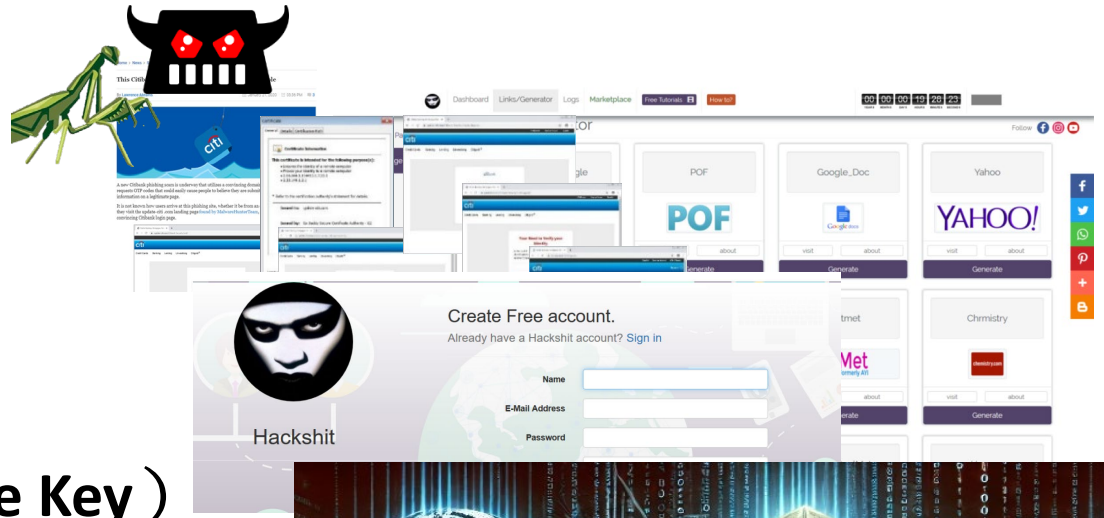
Market oriented

Technology neutrality

ITRI Industrial Technology Research Institute

Challenge One: Out-of-date cryptography

- ~~One-time Password~~
- **Symmetric cryptography（Private Key）**
  - ~~DES~~, ~~RC2~~, ~~RC4~~, ~~3DES~~, AES
- **Asymmetric encryption （Public/private Key）**
  - RSA, DSA, ECC, **PQC, PKD**
- **Data validation, hash functions**
  - HMAC, ~~MD5~~, SHA



Source: DALL·E 2024-11-10

Challenge 2: AI as Spear or Shield

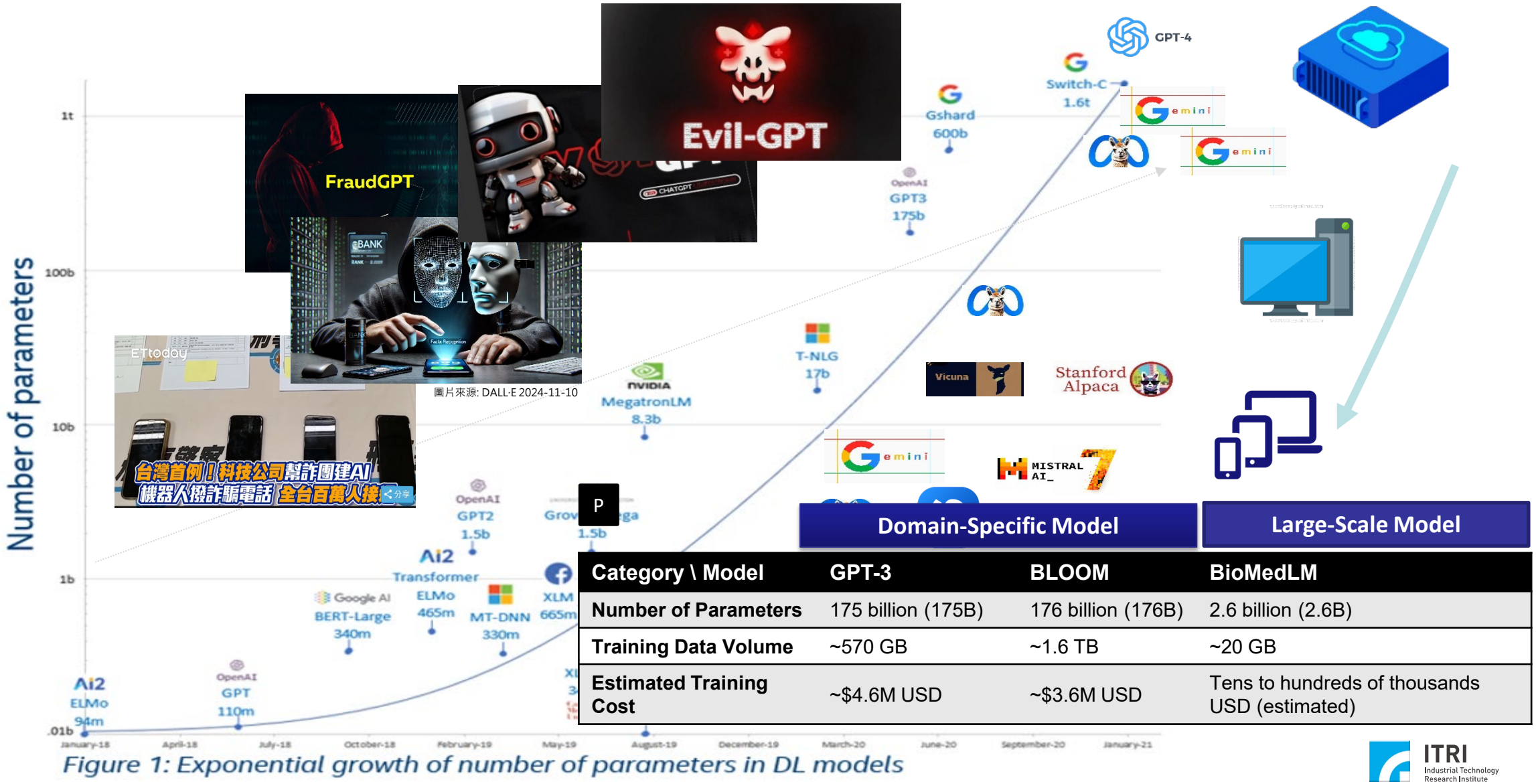


Figure 1: Exponential growth of number of parameters in DL models

Category \ Model	GPT-3	BLOOM	BioMedLM
	Large-Scale Model		Domain-Specific Model
Number of Parameters	175 billion (175B)	176 billion (176B)	2.6 billion (2.6B)
Training Data Volume	~570 GB	~1.6 TB	~20 GB
Estimated Training Cost	~$4.6M USD	~$3.6M USD	Tens to hundreds of thousands USD (estimated)

ITRI Industrial Technology Research Institute

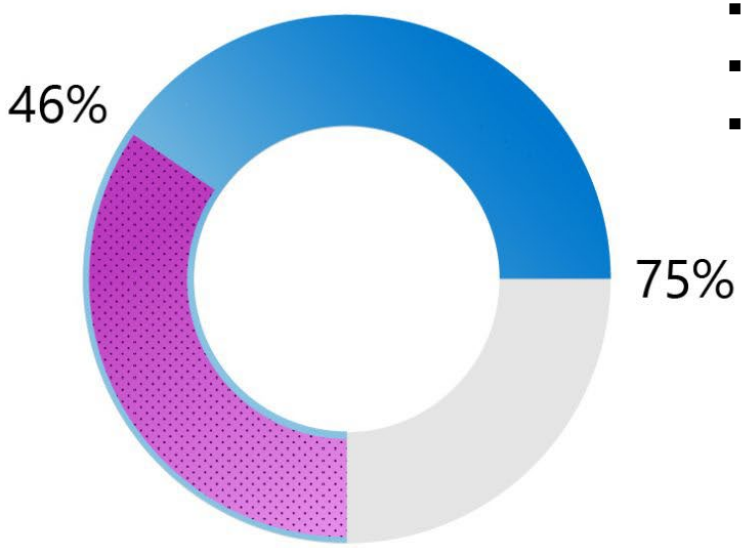
Dawn of the AI Era

Three Out of Four People Use AI at Work

Usage nearly doubled within the last six months.

75% of people are already using AI at work

46% of them started using it less than 6 months ago



Employee Perception of AI Benefits:

- Saves time (90%)
- Focuses on important work (85%)
- Enhances creativity (84%)
- Increases job enjoyment (83%)

Source: Work Trend Index Report, May 2024

Survey questions:
How often do you use generative artificial intelligence (AI) for your work?
How long have you been using generative artificial intelligence (AI) at work?

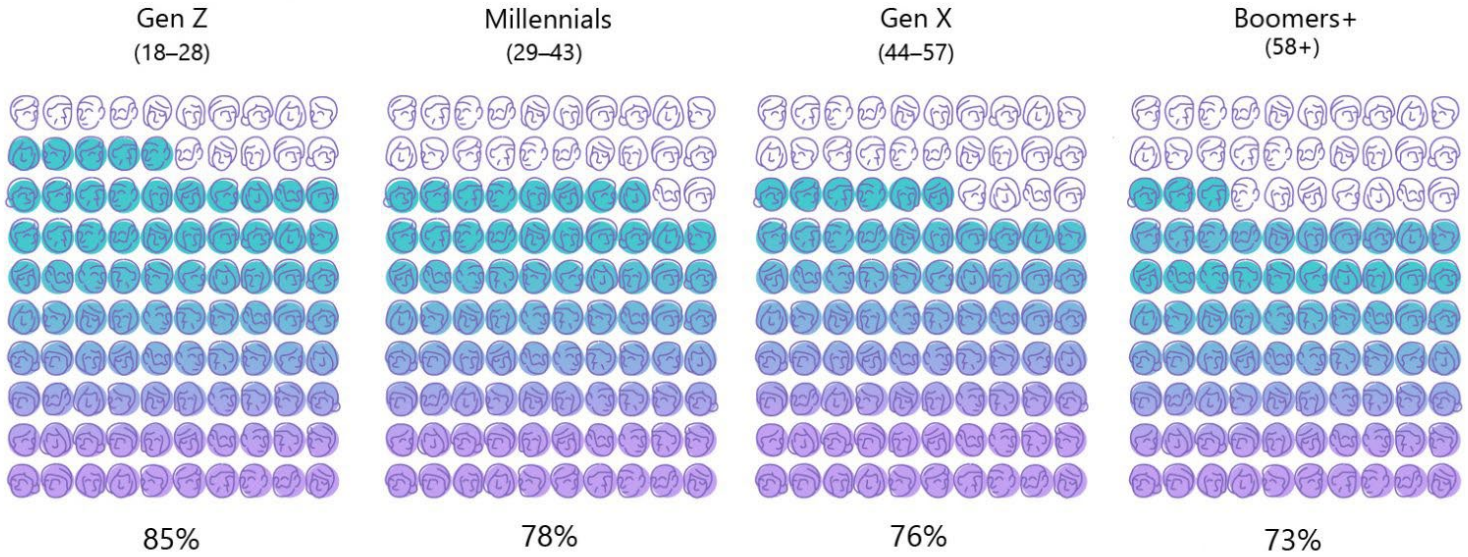
ITRI Industrial Technology Research Institute

Looming Cybersecurity Threat

However, BYOAI (Bring Your Own AI) poses cybersecurity, compliance, and operational risks for enterprises

BYOAI Is Not Just for Gen Z

Employees across every age group are bringing their own AI tools to work.



Share of survey respondents who have used AI tools at work not provided by their organization

Source: Work Trend Index Report, May 2024

ITRI Industrial Technology Research Institute

Future of Trustworthy Digital Societty

③ Collaboration & Partnership

② Intelligence & Affordability

① Alignment & Agility

ITRI
Industrial Technology Research Institute

Post-Quantum Cryptography Enable Digital Trust

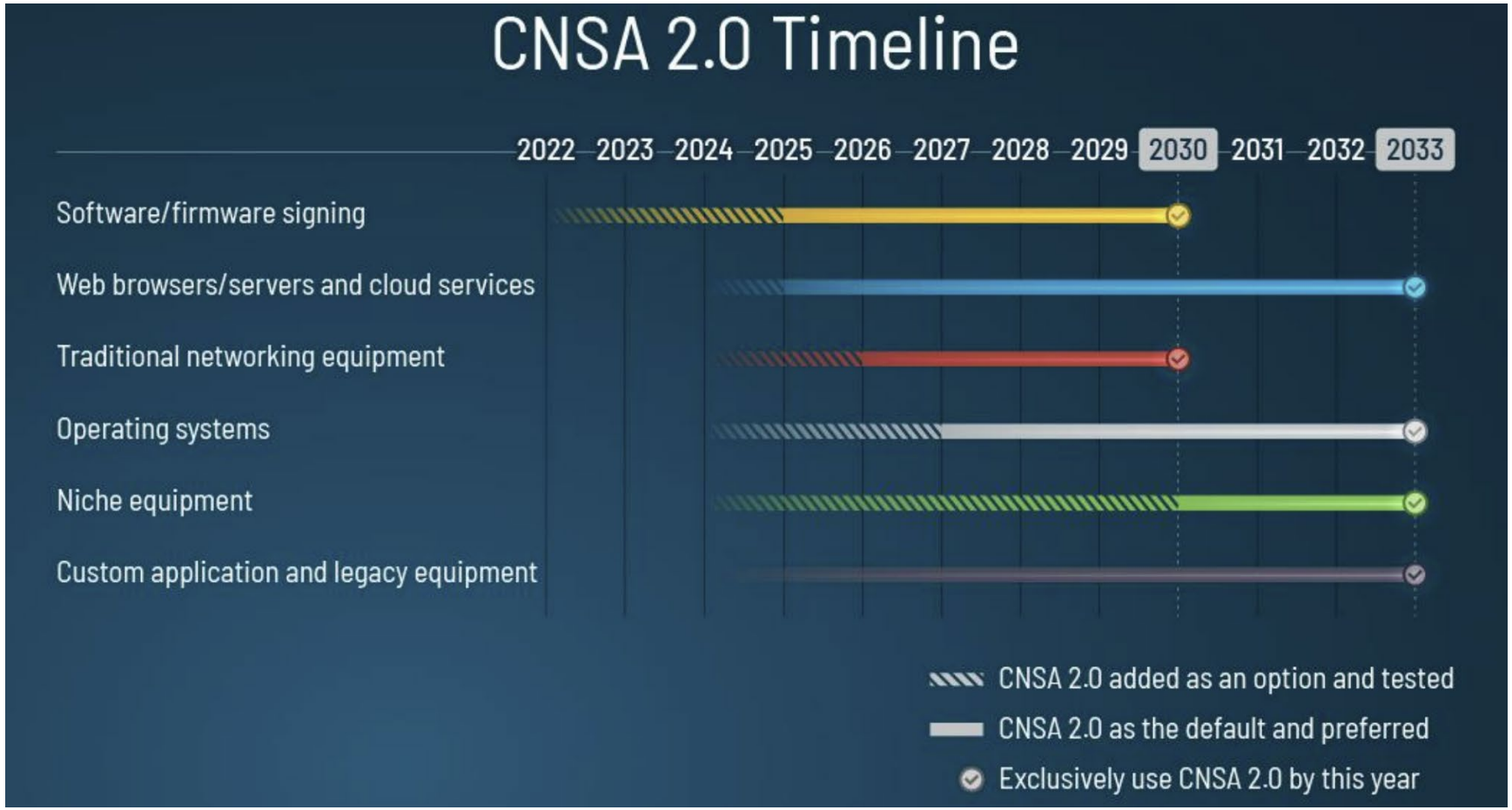
Dr. Wei-Bin Lee, Convener

Post-Quantum Cryptography Cybersecurity Industry Alliance (PQC-CIA)

PQC-CIA
PQC Cybersecurity Industry Alliance

Year to Quantum is Cybersecurity Threat

- **NSA's Cybersecurity Advisory (CSA) released CNSA 2.0(Commercial National Security Algorithm Suite 2.0), mandating that quantum-resistant algorithms be fully adopted by 2035**



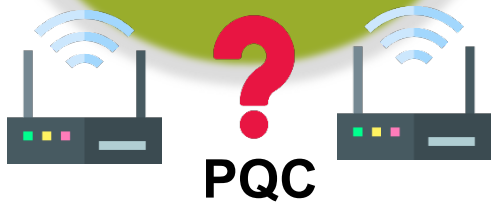
Source: https://media.defense.gov/2025/May/30/2003728741/-1/-1/0/CSA_CNSA_2.0_ALGORITHMS.PDF

PQC-CIA
PQC Cybersecurity Industry Alliance

Challenges of PQC Development & Migration

PQC Algorithm is Difficult

Inter-operability Testing



No idea for migration

Budget & Priority

Industry Alliance for Quantum Resilience

PQC-CIA
PQC Cybersecurity Industry Alliance

MISSION

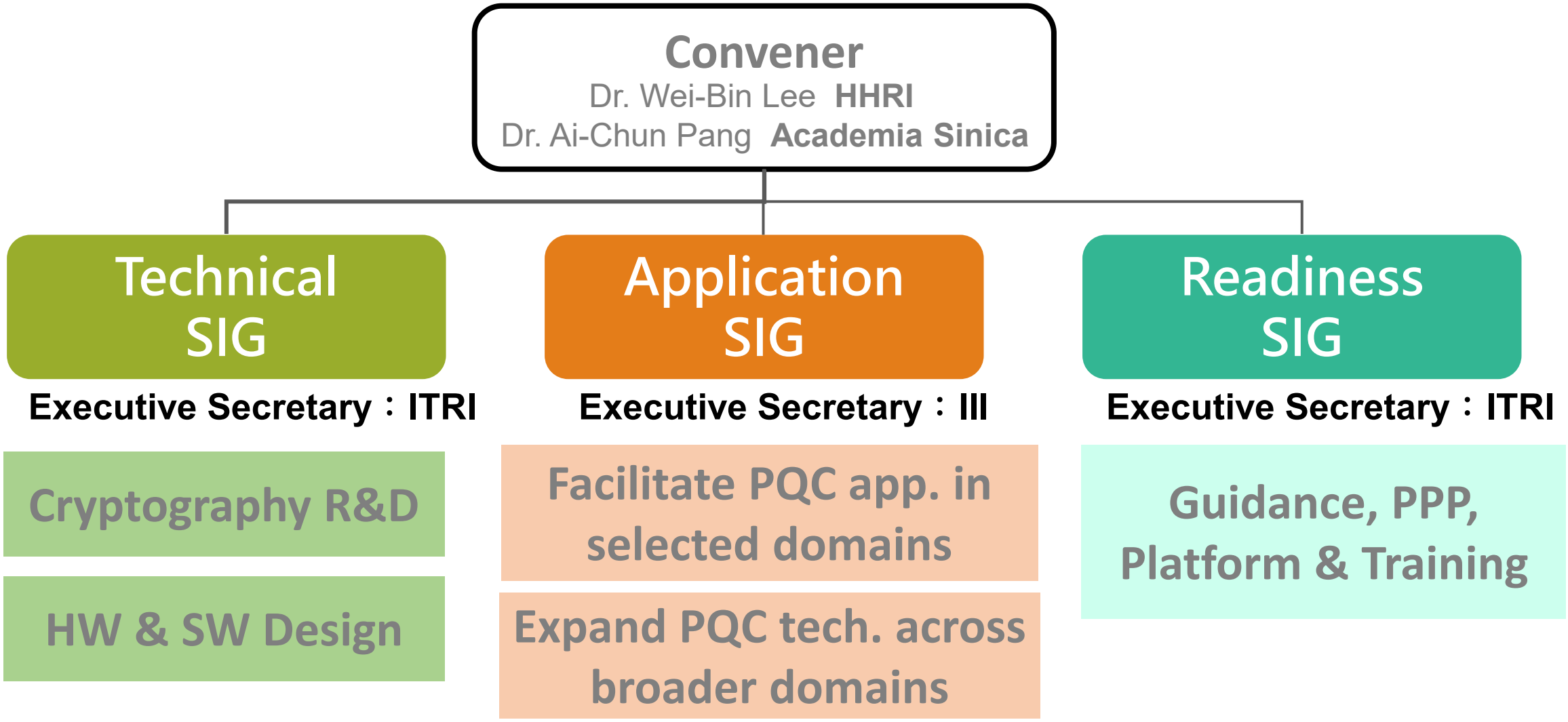
To promote robust public-private partnerships

To accelerate the growth of post-quantum industries

To take action to ensure that Taiwan is PQC ready

PQC-CIA
PQC Cybersecurity Industry Alliance

Organization



PQC-CIA：Three Focuses

PQC-CIA
PQC Cybersecurity Industry Alliance

Application

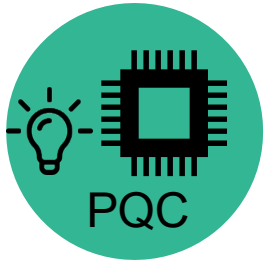
PQC-Ready Solutions

- ✓ Enhance data security
- ✓ Enhance user trust
- ✓ Optimize investment returns

Industry

PQC Ecosystem

- ✓ Enhance global competitiveness
- ✓ Seize new business opportunities
- ✓ Accelerate market entry timing



Innovation

New Application

- ✓ Promote product innovation
- ✓ Expand the global market
- ✓ Create added value for products

PQC-CIA
PQC Cybersecurity Industry Alliance

Public-Private Partnerships as Bridge

Public Sector

We urge the government
(1) to pay attention to the issue of quantum migration.
(2) As the early buyer (demand side)

Private Sector

We provide
(1)talent cultivation
(2) Quickly validate market demand to shorten the product development cycle
(3) Save R&D costs and quickly achieve product innovation

- **Empower Taiwan's PQC Industries**
- **Promote the demand side to adapt PQC-ready solutions**
- **As a platform for PoC and Interoperability Testing: PKI, E-Signature solutions**

Official Launch of TAIWAN PQC Migration Guidelines

- The Administration for Digital Industries, in collaboration with the Post-Quantum Cybersecurity Industry Alliance, released the “ TAIWAN PQC Migration Guidelines” at CYBERSEC 2025.
- Representatives from the Ministry of the Interior, Financial Supervisory Commission, and Ministry of Economic Affairs were invited to join the PQC Migration Panel Discussion to explore strategies and the national roadmap for PQC migration.

中華民國 內政部
MINISTRY OF THE INTERIOR, R.O.C (TAIWAN)

經濟部
Ministry of Economic Affairs

數位發展部 數位產業署
Administration for Digital Industries, moda

金融監督管理委員會
Financial Supervisory Commission R.O.C. (Taiwan)

Common Platform as Joint Result

The PQC Common Platform Solution includes four key components：
(1) PQC Silicon Intellectual Property, (2)PQC Software and Firmware, (3) PQC Chip Design and Verification Environment, and (4) PQC Application Reference Examples.

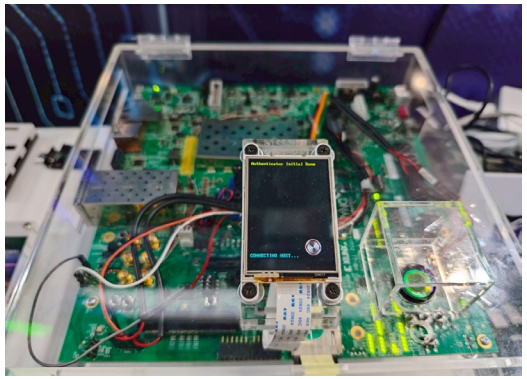
PQC Application Reference Examples.
(Identification、Digital Signature)

PQC Chip Common Platform for Product Design and Verification Environment (FPGA)

PQC IP
ML-KEM 、ML-DSA、SLH-DSA

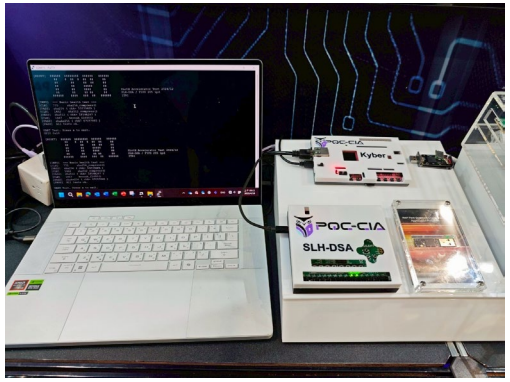
PQC SW/FW
ARM、RISC-V、X86 、...

All of the above are ready for collaboration

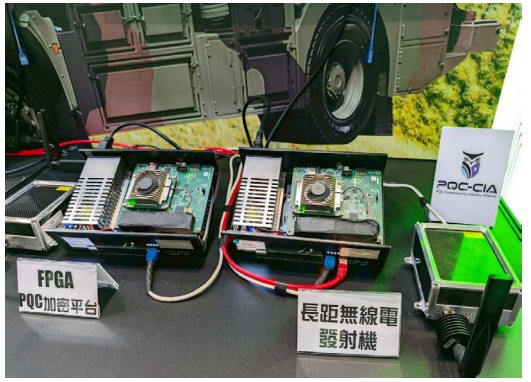


Identification

Digital Signature



PQC IP & PQC SW/FW



PQC Chip Common Platform

PQC-CIA

PQC Cybersecurity Industry Alliance

Public-Private Partnership for Better Digital World

指導單位：數位發展部 數位產業署 Administration for Digital Industries, moda

秘書處：工業技術研究院 Industrial Technology Research Institute

財團法人資訊工業策進會 INSTITUTE FOR INFORMATION INDUSTRY