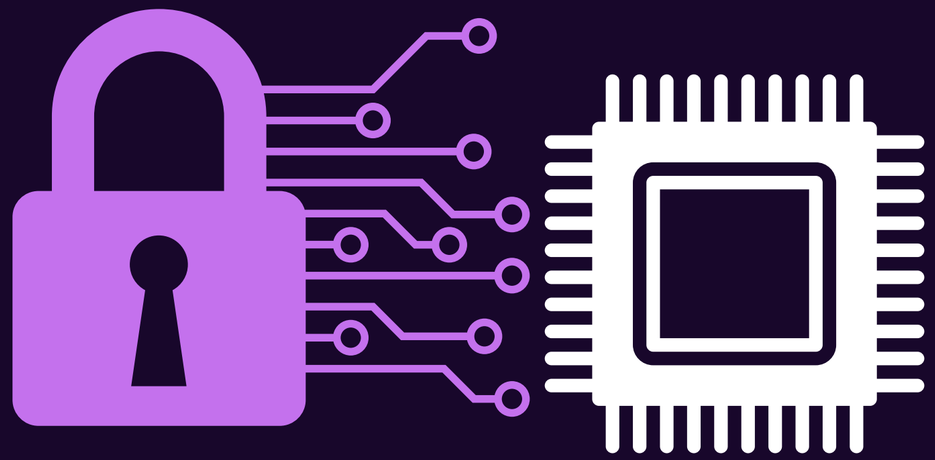
FUTURE OF CYBERSECURITY (THE SCILICON CHIPS)



Host: Prof. Dr. M M Alam

Guest: Sidra Saleem

23RD JULY 2023

Silicon Tech And Cyber Security

- Silicon technology continues to evolve, with innovations like hardware-based machine learning for anomaly detection and threat identification.
- As cybersecurity threats become more sophisticated, leveraging silicon tech for robust hardware-based security measures is essential to protect digital systems, networks, and data from potential attacks.
- Innovations like the application of AI and ML directly onto silicon chips - also known as edge AI - are driving advancements in this area.
- For example, Google's Edge TPU (Tensor Processing Unit) is designed to run TensorFlow Lite ML models at the edge of the network, enabling secure, low-latency, and efficient processing.

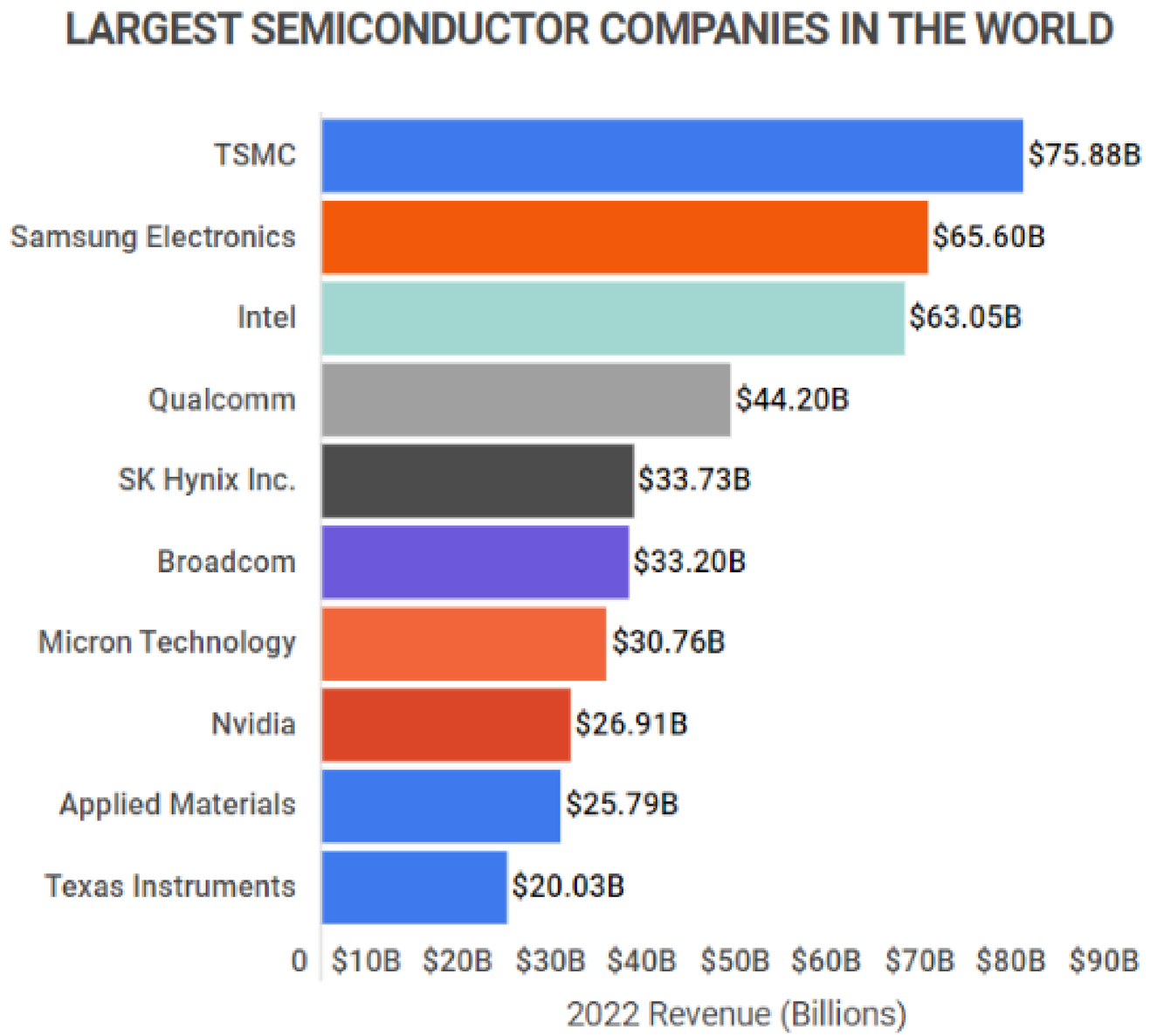
Semiconductors In AI

The crucial role semiconductors play in AI computations.

- Efficient Computation
- Data Processing
- Edge AI

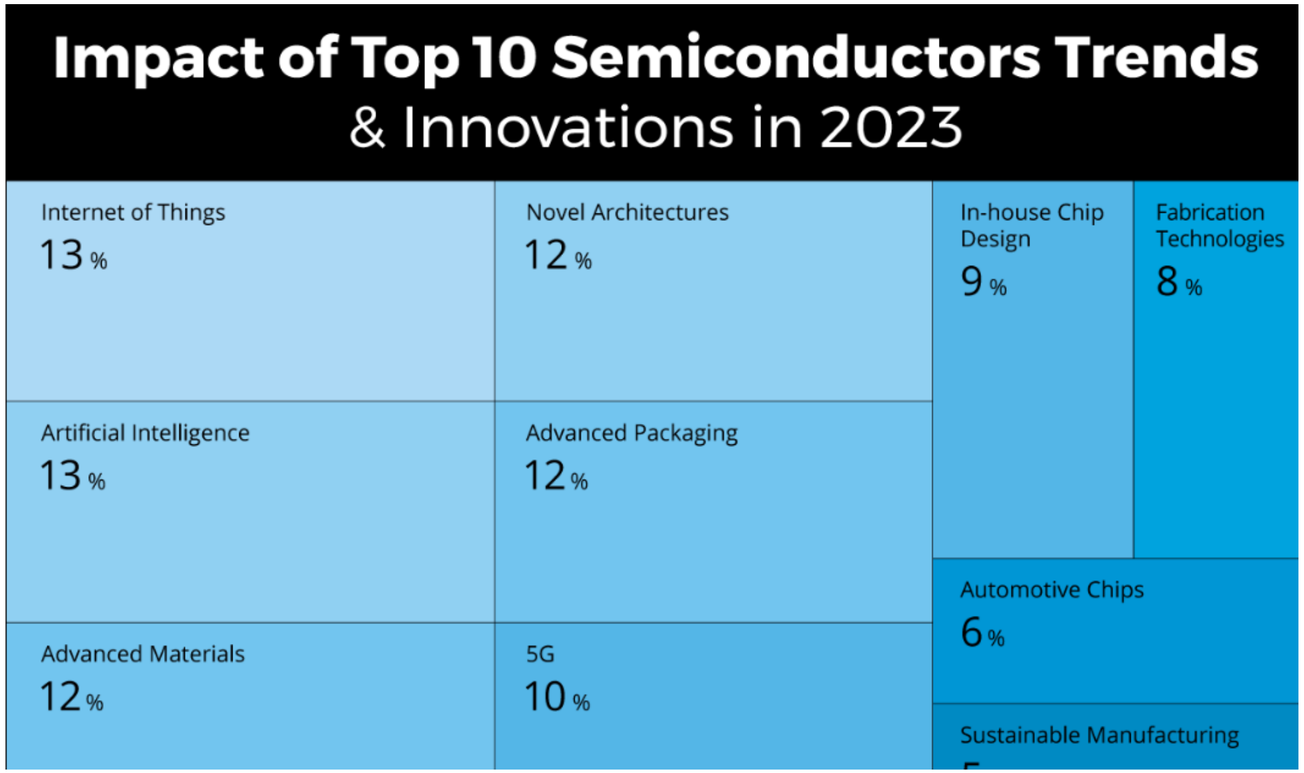
The advancements in AI-driven cybersecurity made possible by semiconductors.

- Anomaly Detection
- Secure Hardware



Trends and future directions in semiconductor technology for AI applications

- Custom Chips for AI
- Hardware for Quantum Computing
- Nanotechnology and Semiconductors
- Neuromorphic Chips



Smart Dust in AI Cybersecurity

Potential applications of Smart Dust in enhancing device security and AI-driven cybersecurity:

- Monitoring Physical Environments
- Network Security
- Data Authentication
- AI Integration

Considerations and challenges in implementing Smart Dust technology.

- Power Supply
- Data Privacy
- Security
- Interference
- Scale

Elon Musk's New AI Venture, xAI

- Overview of Elon Musk's new venture xAI.
- How xAI aligns with Musk's vision for AI.
- Expected contributions of xAI to the field of AI.

Dojo Supercomputers

- The role of the Dojo Supercomputer in training AI for autonomous driving.
- The power and architecture of the Dojo Supercomputer.
- Tesla's vision for the future of AI and autonomous driving.

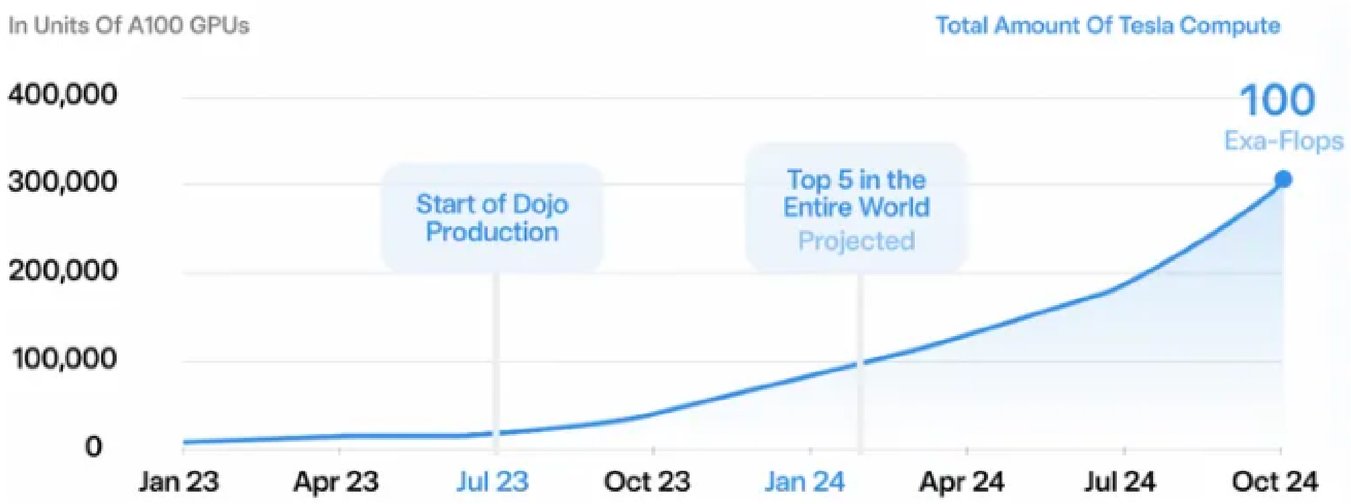
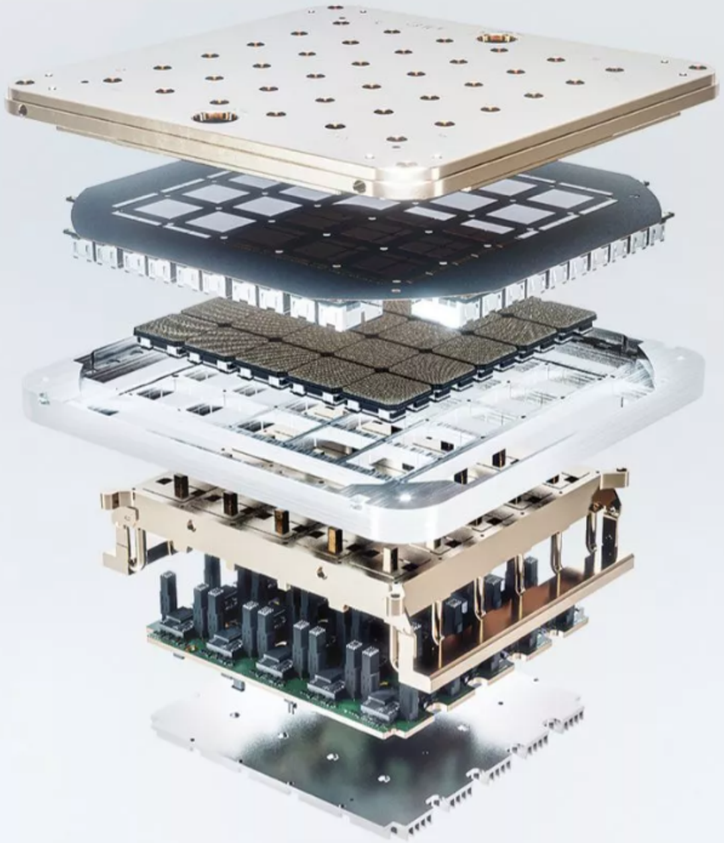


Image: Tesla

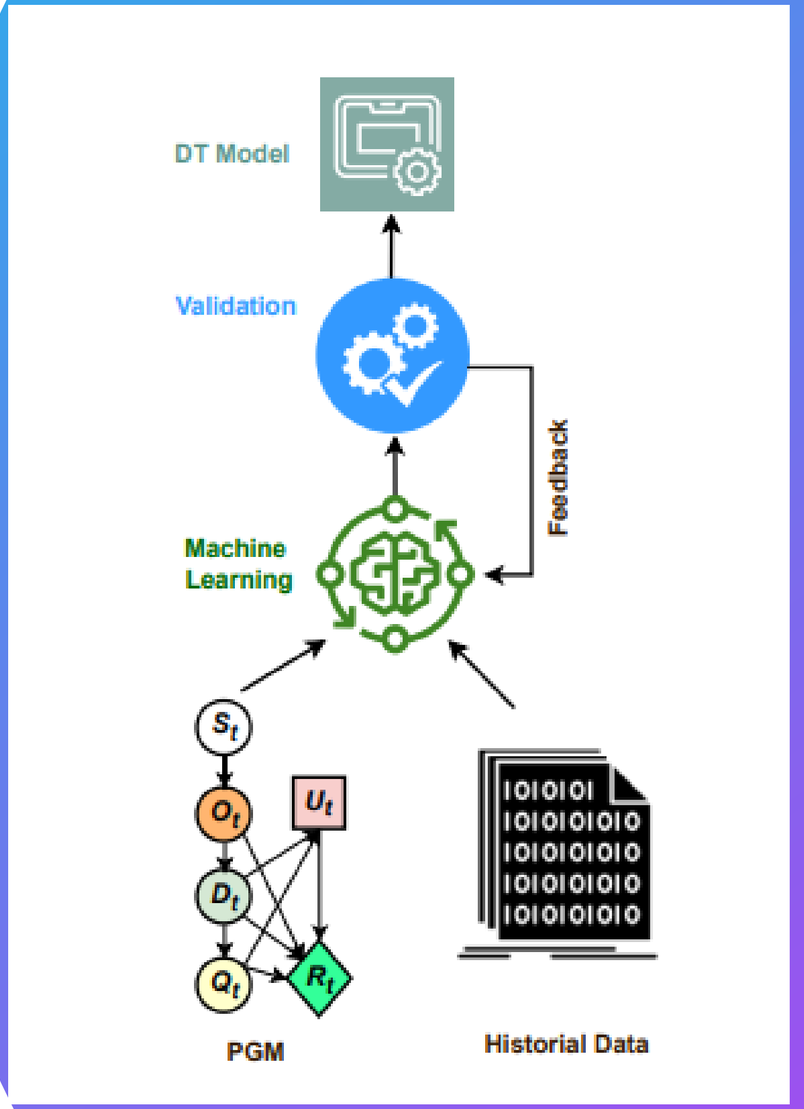
D1 Chip

- The D1 chip's role in powering the Dojo Supercomputer.
- Technical specifications and innovations introduced in the D1 chip.
- Importance of D1 chip in the larger context of semiconductor technology evolution.
- The D1 chip, and the Dojo system as a whole, represent a significant development in the field of AI hardware.
- They could potentially lead to more efficient and powerful AI systems, particularly for tasks that require processing large amounts of data, such as autonomous driving.

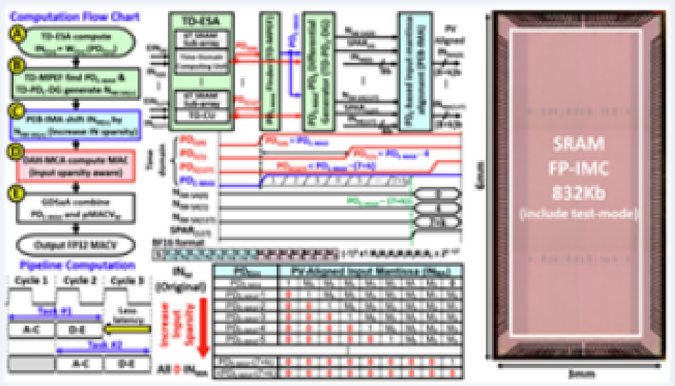


Digital Twin and AI Chip

- DT could provide the estimated states of edge servers and training data to a centralized base station, which could then derive an optimal offloading solution .
- The framework aims to overcome challenges such as communication reliability, resource constraints, device heterogeneity, and the dynamic nature of the edge computing environment.
- By leveraging AI algorithms on AI chips, it's possible to create predictive DT models that can accurately estimate the states of physical entities. These DT models are developed using machine learning (ML) and probabilistic graphical models (PGMs).

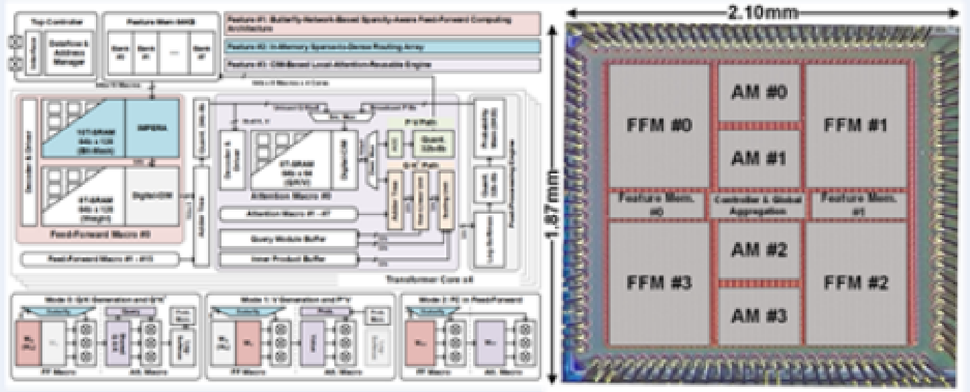


New Trends on ISSCC 2023 Machine Learning Chips



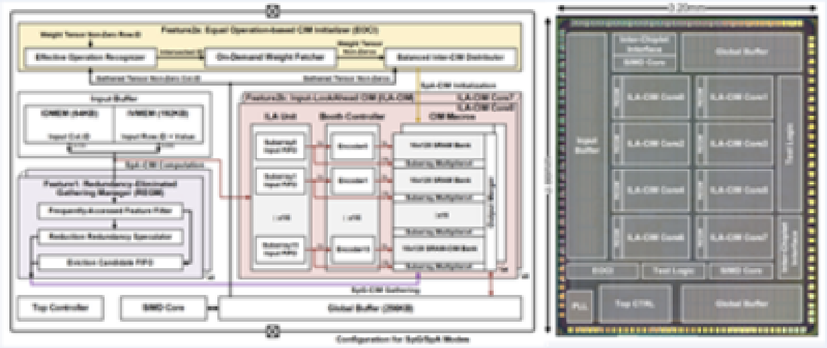
(P. Wu, *et al. ISSCC*, pp. 126–128, IEEE, 2023)

Floating-Point SRAM CIM Macro



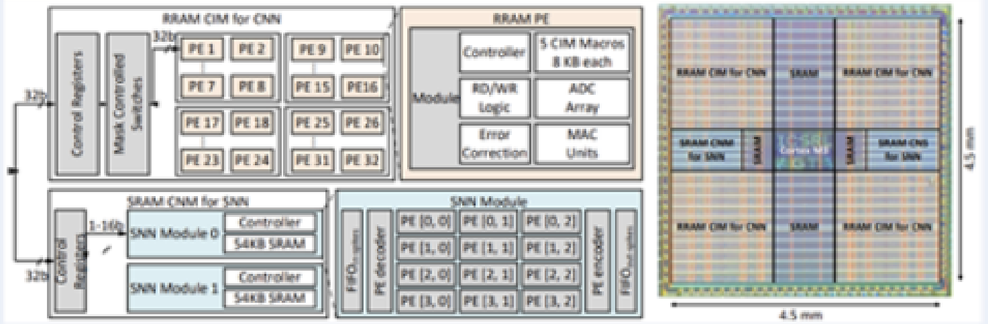
(S. Liu, *et al. ISSCC*, pp. 250–252, IEEE, 2023)

BFLY-CIM-Transformer Accelerator



(F. Tu, *et al. ISSCC*, pp. 254–256, IEEE, 2023)

Chiplet Digital-CIM Tensor Processor



(A. Lele, *et al. ISSCC*, pp. 426–428, IEEE, 2023)

Heterogeneous SoC for Hybrid SNN/CNN Network

HAILO Chip

- The Hailo-8 is designed to fit into smart devices in industries such as automotive, smart cities, retail, and manufacturing, among others.
- In smart city applications, the Hailo-8 can be used in CCTV cameras to improve security, manage traffic flow, and even assist in spotting and addressing infrastructure issues.

Google DeepMind's Use of AI

- Overview of Google DeepMind's use of AI in designing specialized semiconductors.
- The interplay and mutual benefits between AI and semiconductor technology.
- Google DeepMind's contributions and future direction in AI and semiconductor research.

Intel's Silicon Tech in Cyber

- Intel's new silicon-level cybersecurity technology, the "Intel Threat Detection Technology (Intel TDT)" and "Intel Security Essentials", are security measures built directly into their chips.
- These are not separate hardware devices, but rather software and hardware design features that are integrated into the Intel processors to make them inherently more secure against cyber threats.

The Impact of Quantum Computing on Cybersecurity

- Overview of how quantum computing can impact cybersecurity.
- Specific threats posed by quantum computing to existing cybersecurity measures.
- The opportunities quantum computing presents for enhanced cybersecurity.

Cryptographic algorithm	After quantum computing
AES-256	Secure but weakened
SHA-256	Secure but weakened
RSA	No longer secure
ECDSA	No longer secure
DSA	No longer secure

USEFUL LINKS

https://research.aimultiple.com/ai-chip-makers/
https://research.ibm.com/blog/ibm-semiconductors-research
https://www.orfonline.org/research/the-future-of-cybersecurity-is-in-silicon/
https://www.uscybersecurity.net/ai-chip/
https://www.claws.in/quantum-computing-empowering-national-security-for-a-secure-future/