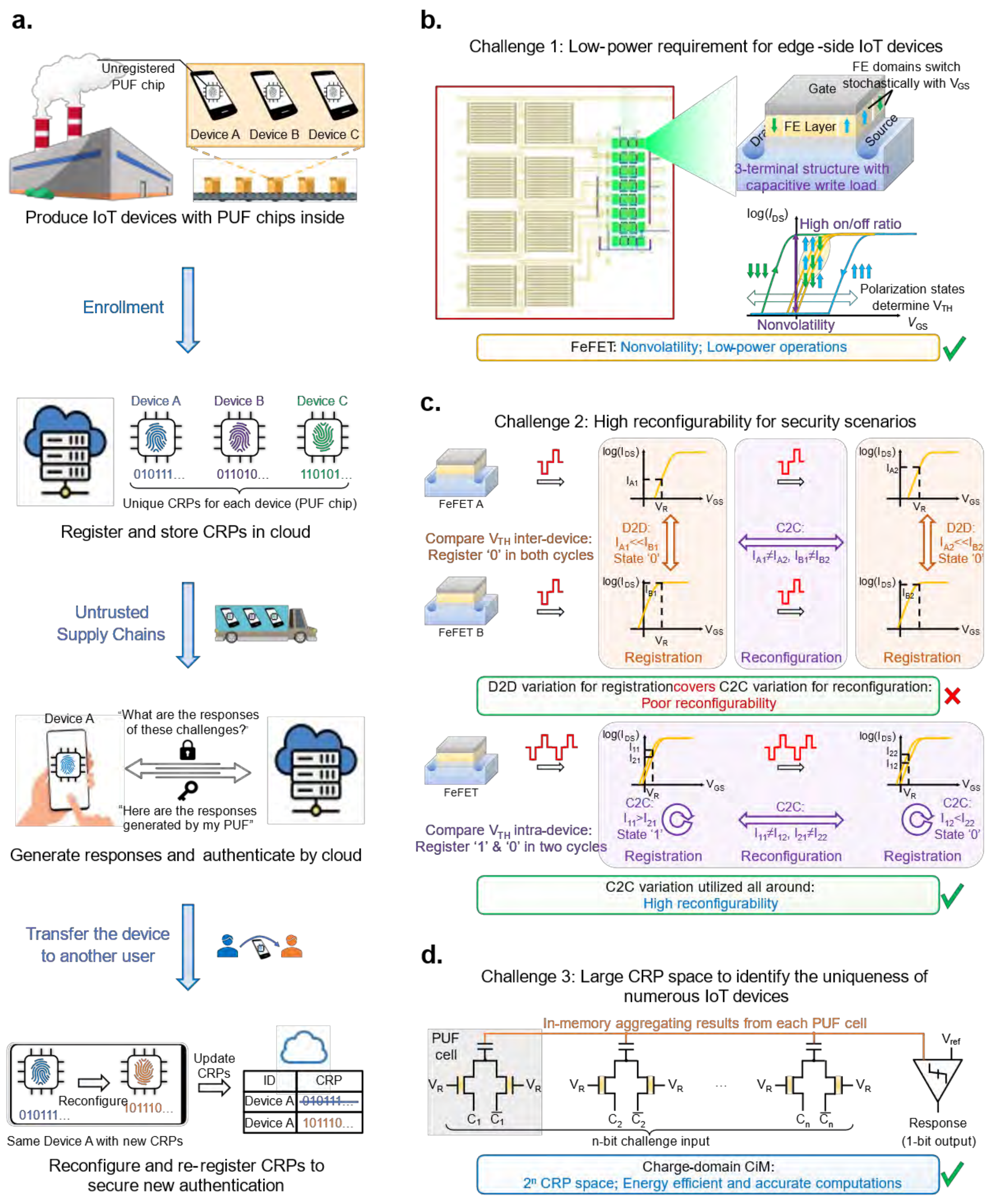
moduleqnc
quantum & neuromorphic computing

Hardware security and Brain-inspired computing

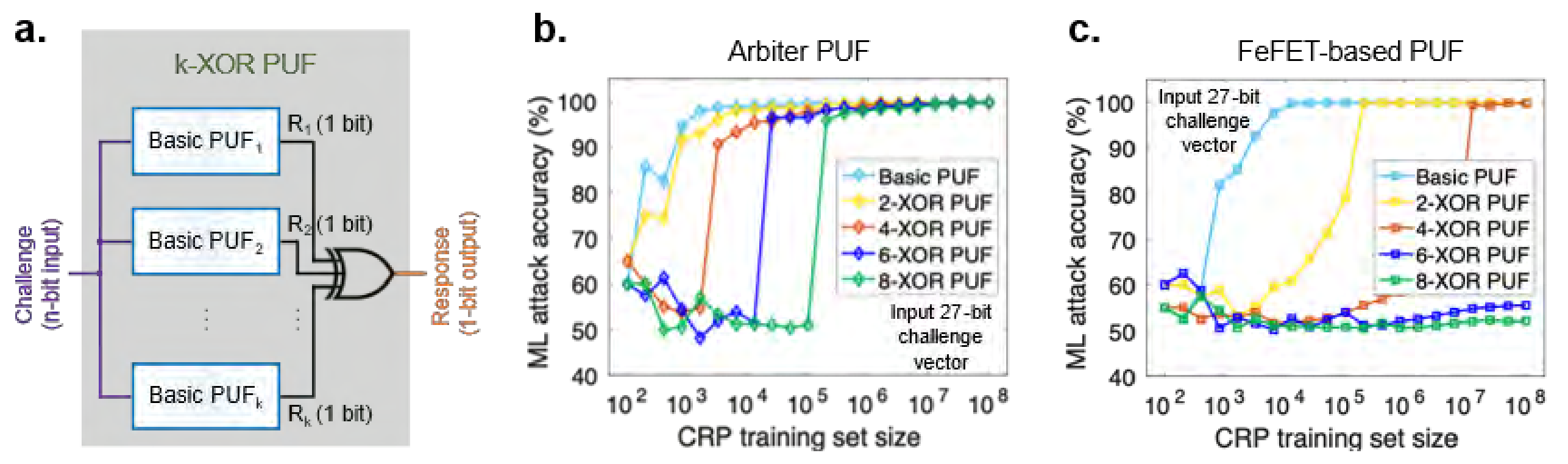
Memristors for safe and high-scale neuromorphic systems

1 Physically uncloneable functions

Application: Secure compute-in-memory systems by encrypting the neuromorphic system through keys generated by physically unclonable functions (PUFs) using 450nmx450nm ferroelectric field-effect technology with Machine Learning Attack Robustness


a.
Unregistered PUF chip
Device A Device B Device C
Produce IoT devices with PUF chips inside
Enrollment
Device A Device B Device C
010111... 011010... 110101...
Unique CRPs for each device (PUF chip)
Register and store CRPs in cloud
Untrusted Supply Chains
Device A
"What are the responses of these challenges?"
"Here are the responses generated by my PUF"
Generate responses and authenticate by cloud
Transfer the device to another user
010111... Reconfigure 101110...
Update CRPs
ID CRP
Device A ~~010111...~~
Device A 101110...
Same Device A with new CRPs
Reconfigure and re-register CRPs to secure new authentication
b.
Challenge 1: Low-power requirement for edge-side IoT devices
FE domains switch stochastically with V_{GS}
Gate
FE Layer
Drain
Source
3-terminal structure with capacitive write load
$\log(I_{DS})$
High on/off ratio
Polarization states determine V_{TH}
Nonvolatility
V_{GS}
FeFET: Nonvolatility; Low-power operations
c.
Challenge 2: High reconfigurability for security scenarios
FeFET A
FeFET B
Compare V_{TH} inter-device: Register '0' in both cycles
D2D: $I_{A1} \ll I_{B1}$ State '0'
C2C: $I_{A1} \neq I_{A2}$, $I_{B1} \neq I_{B2}$
D2D: $I_{A2} \ll I_{B2}$ State '0'
Registration
Reconfiguration
Registration
D2D variation for registration covers C2C variation for reconfiguration: Poor reconfigurability
FeFET
Compare V_{TH} intra-device: Register '1' & '0' in two cycles
C2C: $I_{11} > I_{21}$ State '1'
C2C: $I_{11} \neq I_{12}$, $I_{21} \neq I_{22}$
C2C: $I_{12} < I_{22}$ State '0'
C2C variation utilized all around: High reconfigurability
d.
Challenge 3: Large CRP space to identify the uniqueness of numerous IoT devices
In-memory aggregating results from each PUF cell
PUF cell
V_R
C_1 $\bar{C}_1$
C_2 $\bar{C}_2$
C_n $\bar{C}_n$
n-bit challenge input
V_{ref}
Response (1-bit output)
Charge-domain CiM: 2^n CRP space; Energy efficient and accurate computations

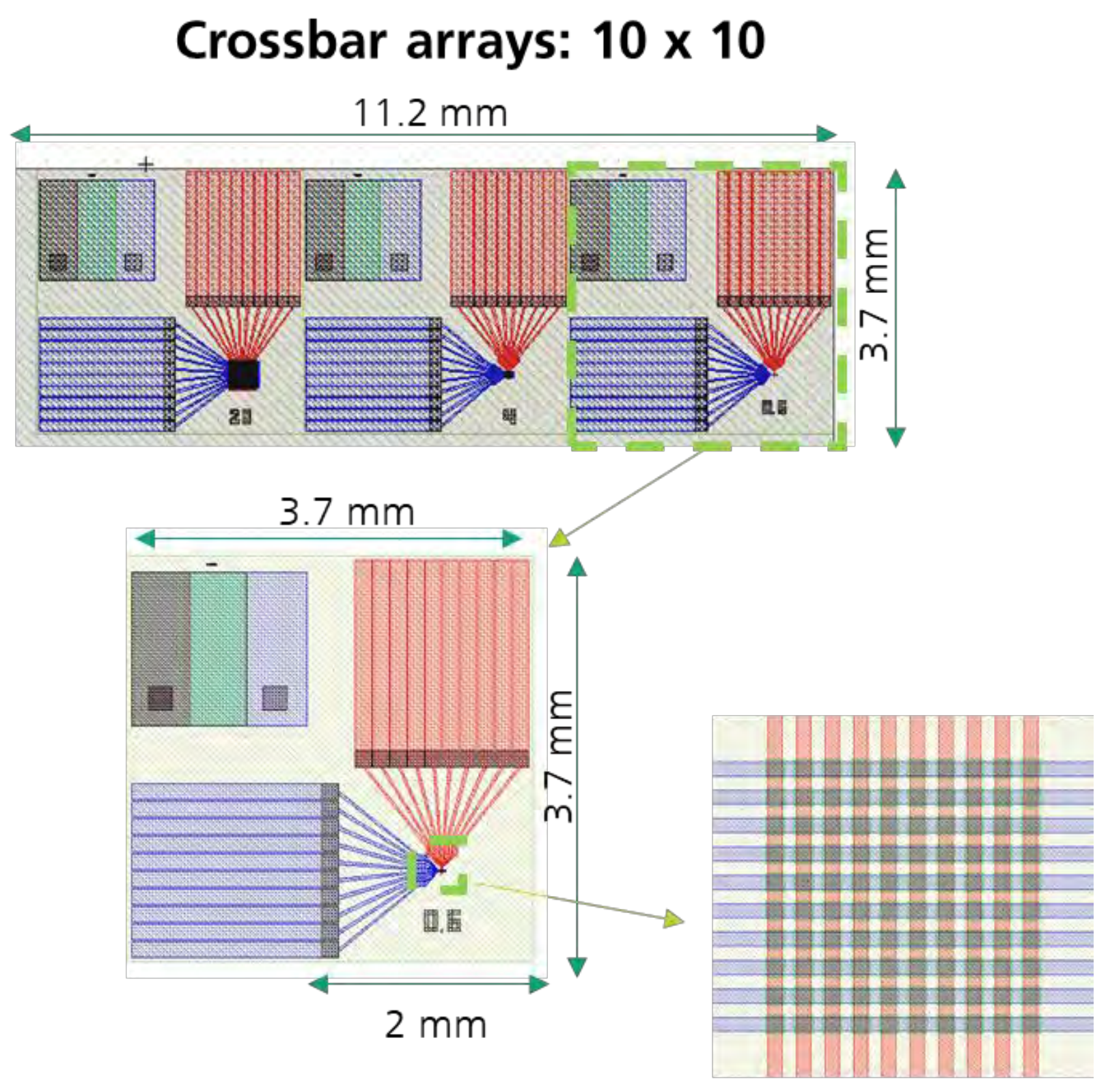
FeFET-based strong PUF overview. a. Conceptual workflow of the PUF-based IoT device authentication. b. For the low-power requirements of IoT devices, nonvolatile FeFETs integrated with capacitors are utilized c. For high reconfigurability in security scenarios, the FeFET C2C variation is exploited. d. To provide massive CRP space for billions of IoT devices, the 2FeFET-1C PUF cell is proposed with charge-domain CiM to provide exponential CRP space as well as low-power and accurate computations.



Proof of ML attack robustness tested for large range of network types

2 Memristive Crossbar-Arrays

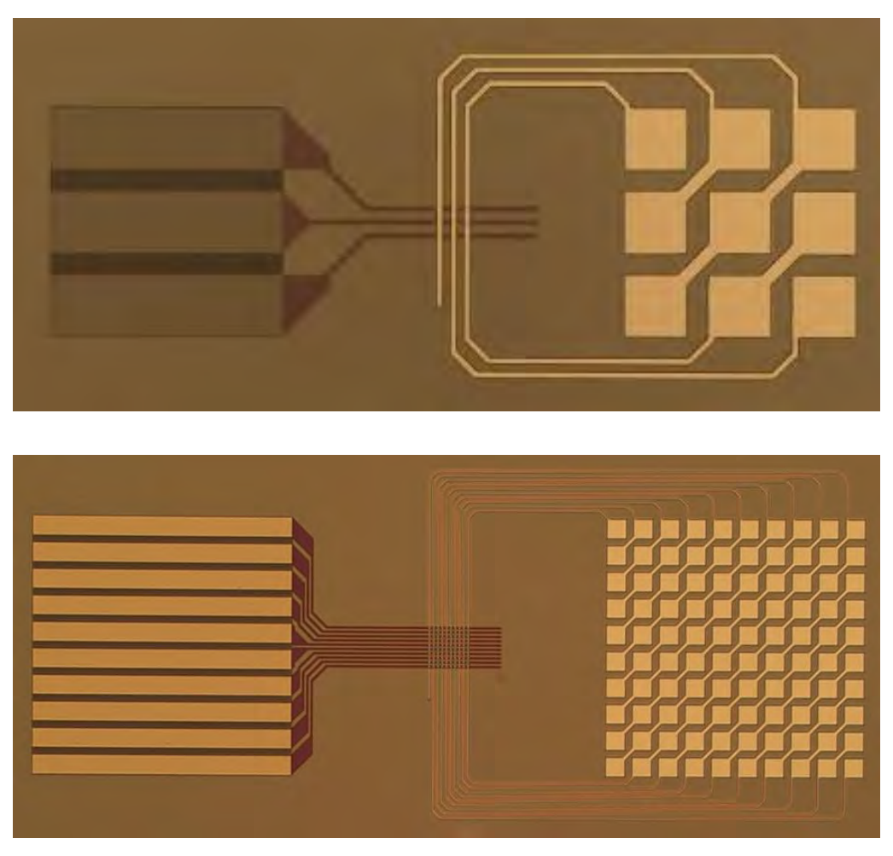
Application: High-density crossbar structures for neuromorphic computing and in-memory computing, optionally with different memristive materials and layer systems



Crossbar dimension with different distances: 20/4/0.6 µm

Typical layouts for memristive crossbar arrays
current status: 1000 cells with a minimum cell size of 600 nm

Components for neuromorphic computing at wafer scale



Memristive crossbar structures with 9 (top) and 100 cells (bottom)

3 Benchmark

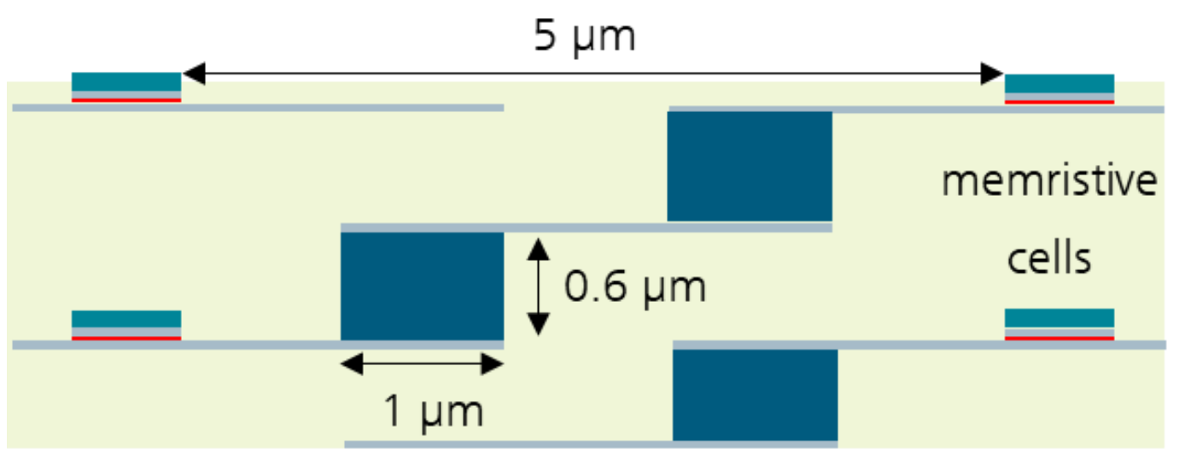
Unique selling points and special features

- Strong PUF with FeFET Technology
- 50.00 % Uniformity, NIST Test Pass
- 49.98 % Uniqueness, 50.02% Reconfigurability
- 4 fJ/bit Power consumption,
- Robustness against various ML attacks
- Crossbar structures with freely selectable materials and multi-layer systems
- Customizable electrode materials and geometries

4 Outlook

Further developments as part of FMD-QNC

- Offer of secure in-memory computing systems and encrypted memories with personalized keys
- Continuous increase in the number of cells up to several 10,000 cells with a simultaneous reduction in cell size.
- Integration of new material systems and multilayers with improved performance and increased reliability.
- Technology for 3D stacking of crossbar matrices for the production of neural networks with several hidden layers.



GEFÖRDERT VOM
Bundesministerium für Bildung und Forschung