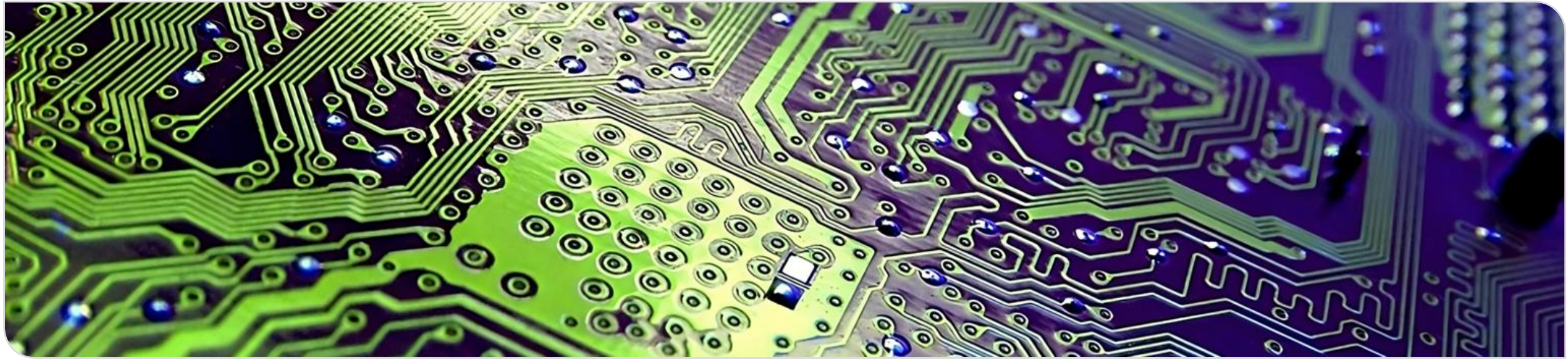
Karlsruhe Institute of Technology

30th Asia South Pacific Design Automation Conference ASP-DAC 2025

ASIA SOUTH PACIFIC DESIGN AUTOMATION CONFERENCE

Side-channel Collision Attacks on Hyper-Dimensional Computing Based on Emerging Resistive Memories

Brojogopal Sapui, Mehdi B. Tahoori



Outline

- Research Objective
- Background & Related Work
- Side Channel and Collision Analysis on CiM implemented HDC
- Countermeasure
- Results
- Conclusion

Research Objective

- **Key Focus:**
  - Side-channel attacks on computation-in-memory implemented HDC using emerging resistive memories.
- **Why This Matters?**
  - **HDC's Role**: Efficient and robust cognitive tasks in edge devices.
  - **Security Threat**: HDC model parameters at risk from physical attacks.
- **Core Objective:**
  - Collision analysis that works with minimal traces for SCA.
  - Propose a scalable countermeasure using hiding technique.

HDC: Hyper Dimensional Computing SCA: Side Channel Analysis

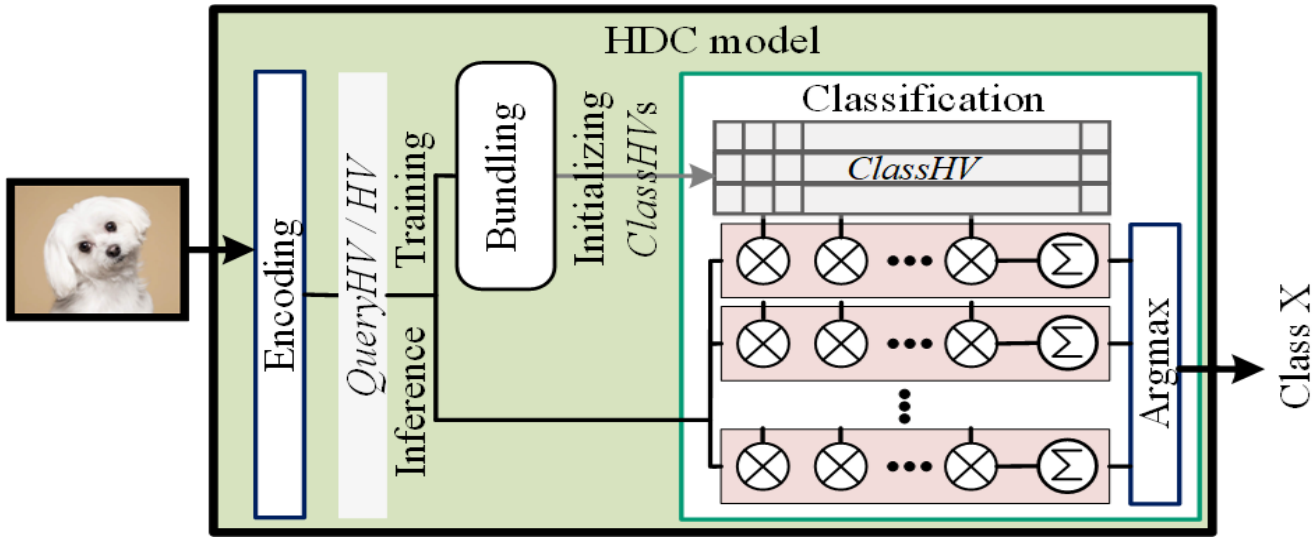
Background of HDC

- **What is HDC?**
  - Brain-inspired computational paradigm using high-dimensional hypervectors.

- **Core Features:**
  - Encodes data into hypervectors.
  - Similarity-based computations (e.g., addition, multiplication, permutation).
  - Associative Memory for inference.

- **Why HDC?**
  - Efficient: Low computational cost.
  - Resilient: Robust against noise.

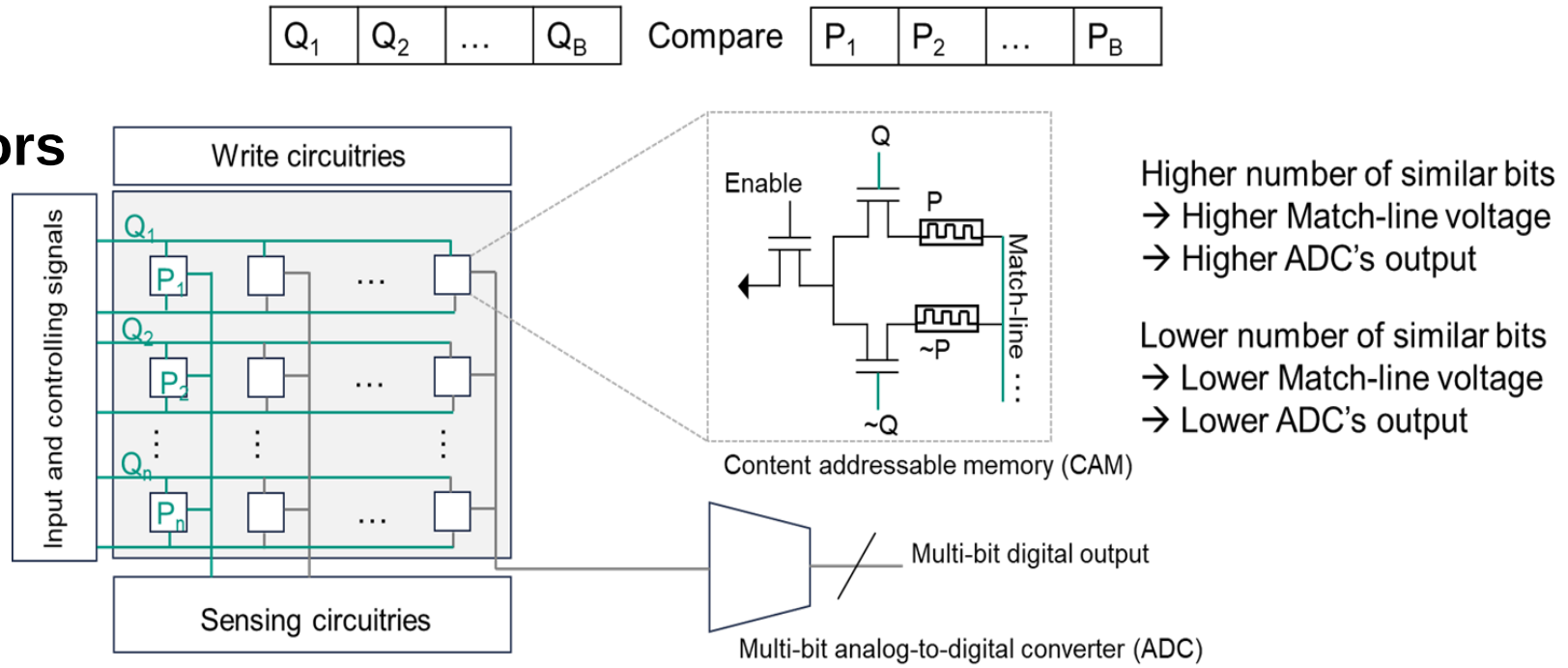
- **Applications:**
  - Image classification, language processing, and IoT edge devices.



Use of CAM in HDC

- **What is CAM?**
  - Memory architecture that retrieves data based on content rather than addresses.
  - Enables parallel search in cross arrays with memristive devices.

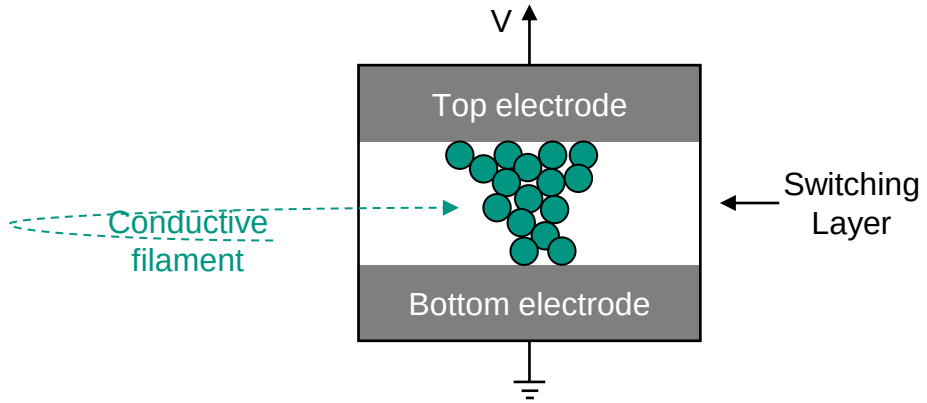
- **Role in HDC:**
  - Stores **class hypervectors** in memory.
  - Performs **similarity matching** between hypervectors.



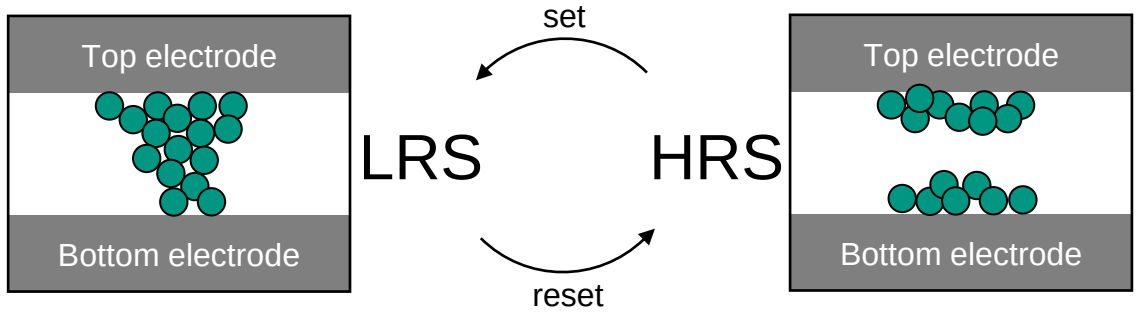
CAM: Content Addressable Memory

Resistive Random Access Memory (ReRAM)

- ReRAM is one of the most promising in memristive devices.
  - Simple structure
  - Very heigh storage density
  - Low power consumption
  - Compatible with CMOS

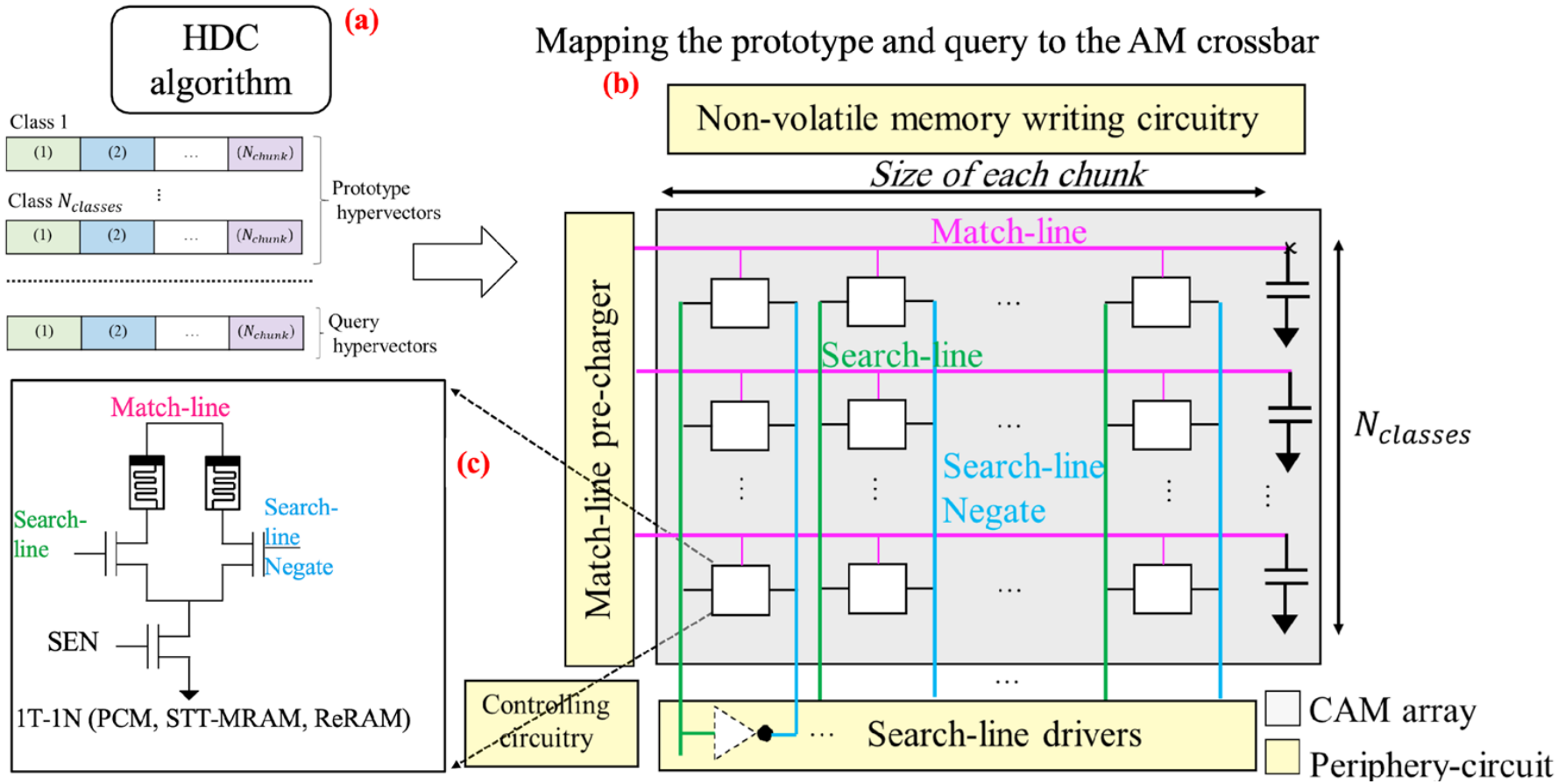


- Data is stored by changing the resistance of a solid dielectric material.
  - Set: conductive path is formed
    - Low Resistive State (LRS)
  - Reset: conductive path is broken
    - High Resistive State (HRS)

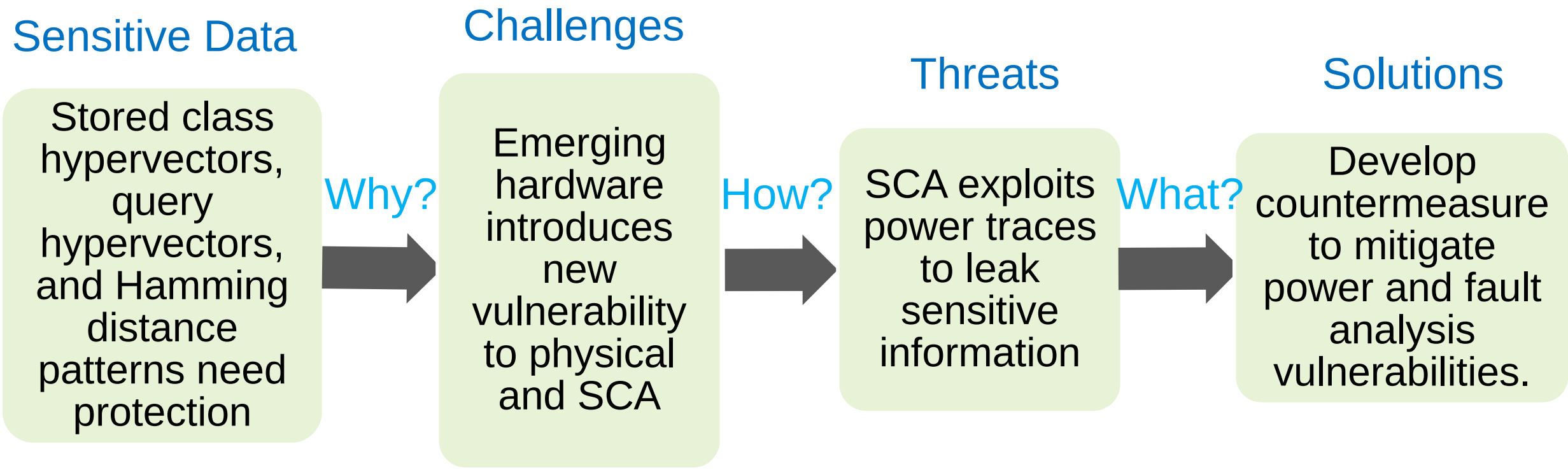


CiM Realization of HDC

- **HDC Framework**: Splits hypervectors for efficient similarity computation.
- **CAM Structure**: Uses memristive devices for storing and matching hypervectors.
- **Parallelism**: Enables simultaneous comparisons across multiple hypervectors.

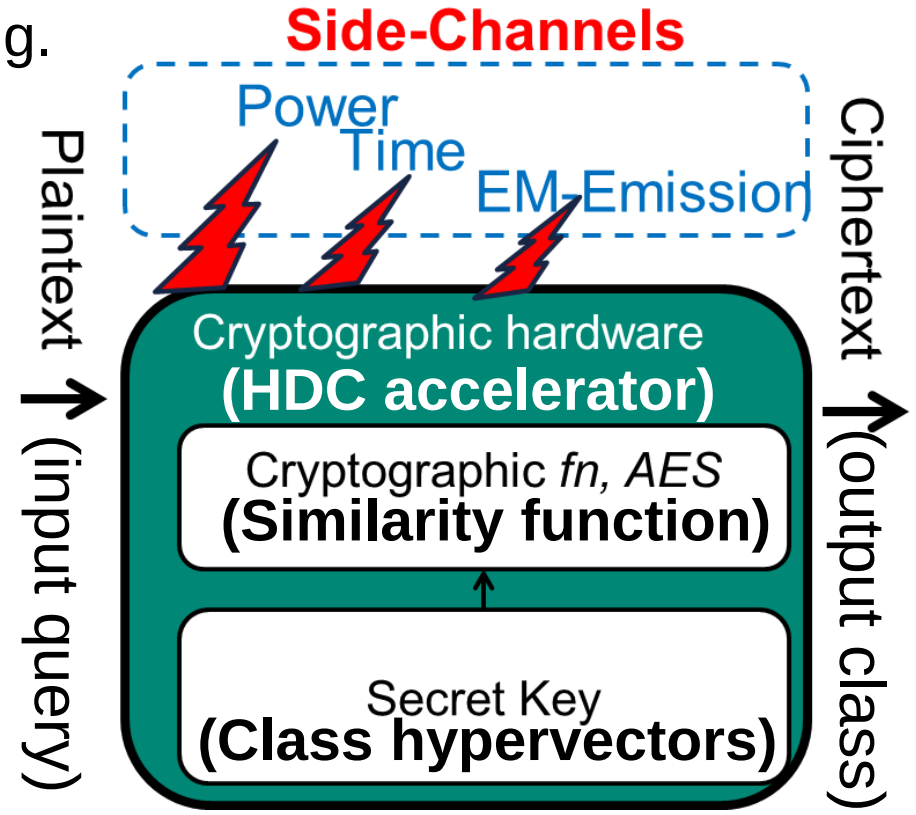


Motivation: Security?



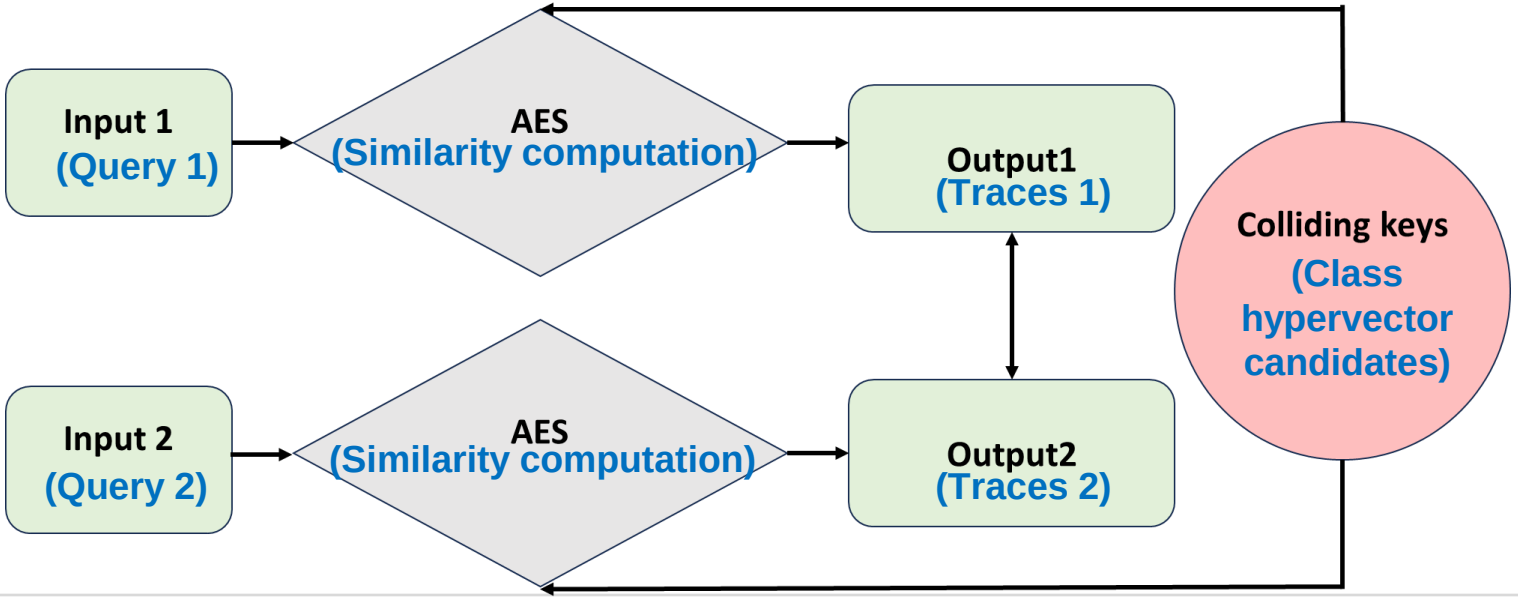
Side Channel Attacks

- **Concept of Side-Channels:**
  - Exploits unintended data leakage via power, timing.
- **HDC's Vulnerability:**
  - HDC operations leak data through power traces.
- **Power and Timing in CAM:**
  - Hamming distance-based operations create identifiable patterns.
- **Target for Sensitive Information:**
  - Analyze large number of power traces.
  - Aim to recover stored class hypervectors.



Collision Analysis

- **What is Collision Analysis?**
  - Technique identifying instances where multiple inputs result in identical outputs.
  - It narrows down the search space.
- **Key Role in HDC:**
  - Query hypervectors are applied to induce collisions.
  - Identifies query-class pairs with minimal Hamming distance.
  - Isolates the potential class hypervectors (the "good key").



Related Work

- **HDC Classifier Vulnerabilities**
  - Adversarial attacks manipulate prediction labels with minimal perturbations.
  - Risks of IP theft [1] from unprotected hypervectors, enabling model replication.

- **Collision Attacks in Cryptography:**
  - Early work focused on public key algorithms (e.g., doubling attacks).
  - Side-channel patterns used to reduce search space for sensitive data [2].

- **CiM using memristive device constraints for SCA:**
  - (HRS/LRS ratio, variability) increase vulnerabilities [3].

[1] Shijin Duan et al . 2022. Hdlock: Exploiting privileged encoding to protect hyperdimensional computing models against ip stealing. DAC. 679–684
[2] Glowacz et al. 2019. "Optimal collision side-channel attacks." *CARDIS 11–13*
[3] Brojogopal Sapui et al. 2023. Power Side-Channel Attacks and Countermeasures on Computation-in-Memory Architectures and Technologies. ETS. 1-6

Threat Model

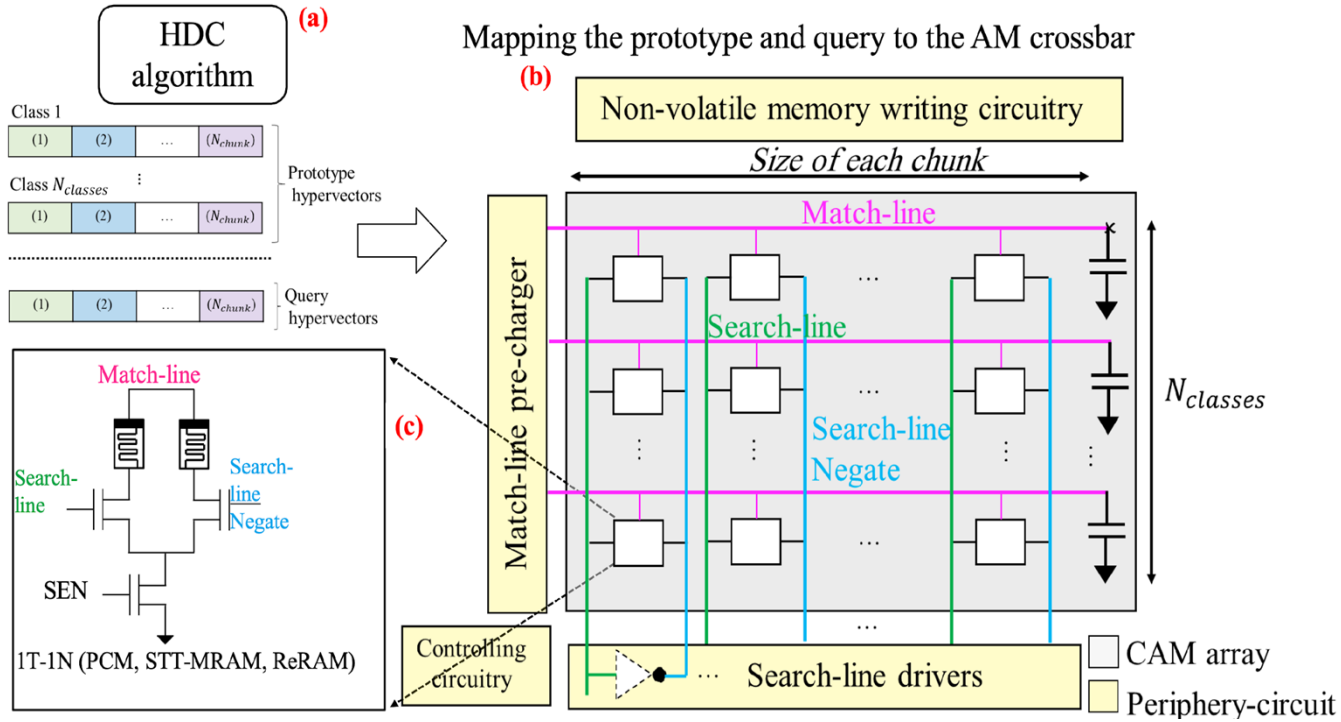
- **Restricted Access:** Sensitive parameters or training datasets.
- **Query Observation**: Input-output pairs and prediction labels.
- **Input Crafting**: Create specific query vectors if encoding is known.
- **Noise Injection**: Introduce noise into input images.
- **Power Measurement**: Total power but not submodule-specific.

- Approximate recovery of hypervectors suffices due to distributed information and bit-flip tolerance [4].

[4] Lulu Ge and Keshab K Parhi. 2020. Classification using hyperdimensional computing: A review. IEEE Circuits and Systems Magazine 20, 30–47.

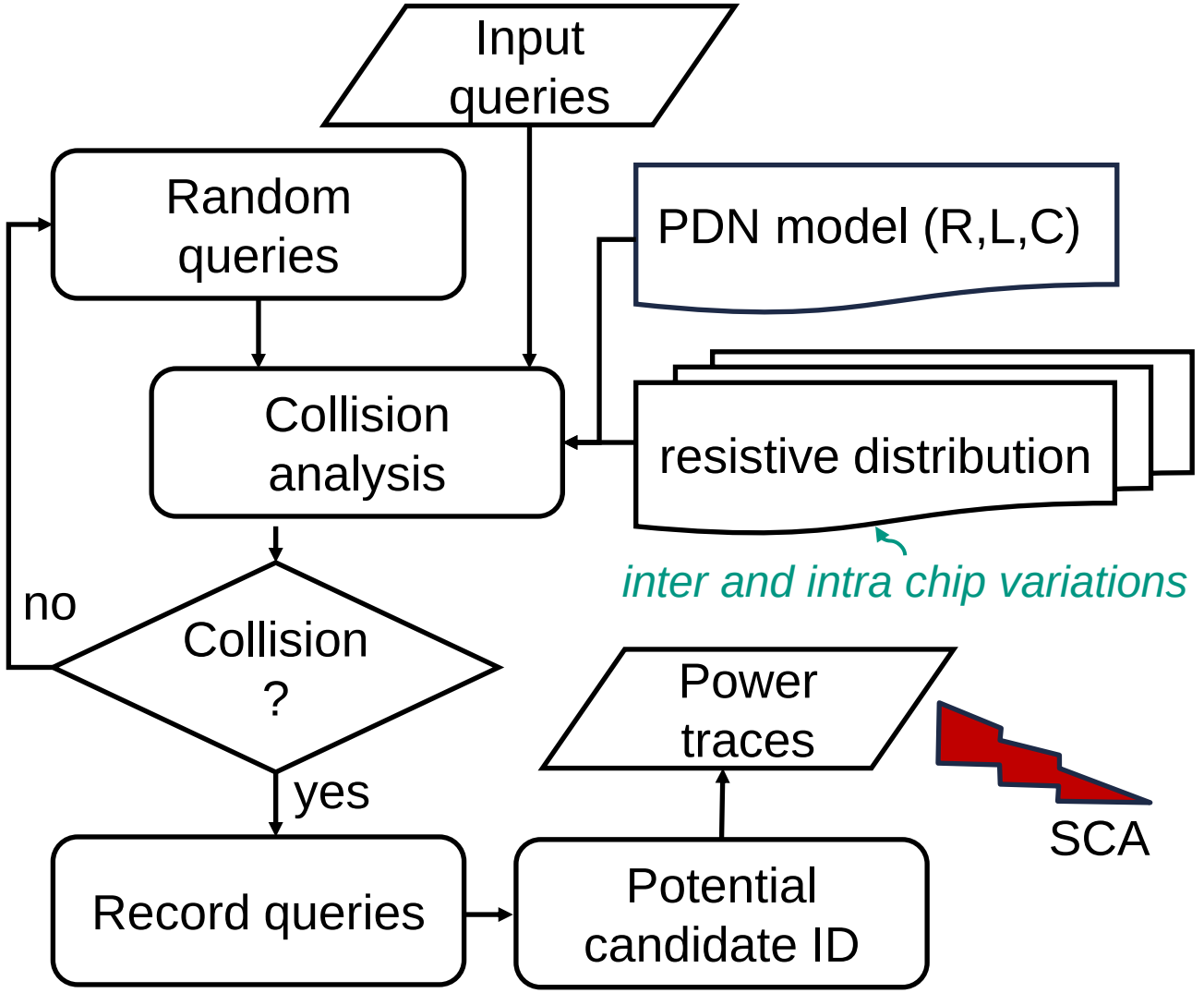
Design under Attack

- **Vulnerable Components**
  - **Search-Line Drivers**: Generate power
  - **Match-Lines**: Emit detectable patterns
- **Impact of Process Variations**
  - Resistive states exploit power variations.
- **Side-Channel Attack Flow**
  - Reducing search space by collision.
  - Power traces during query evaluations.
- **Target of the Attack**
  - Class hypervectors stored in CAM.
  - Query responses revealing data-dependent power.



Attack flow

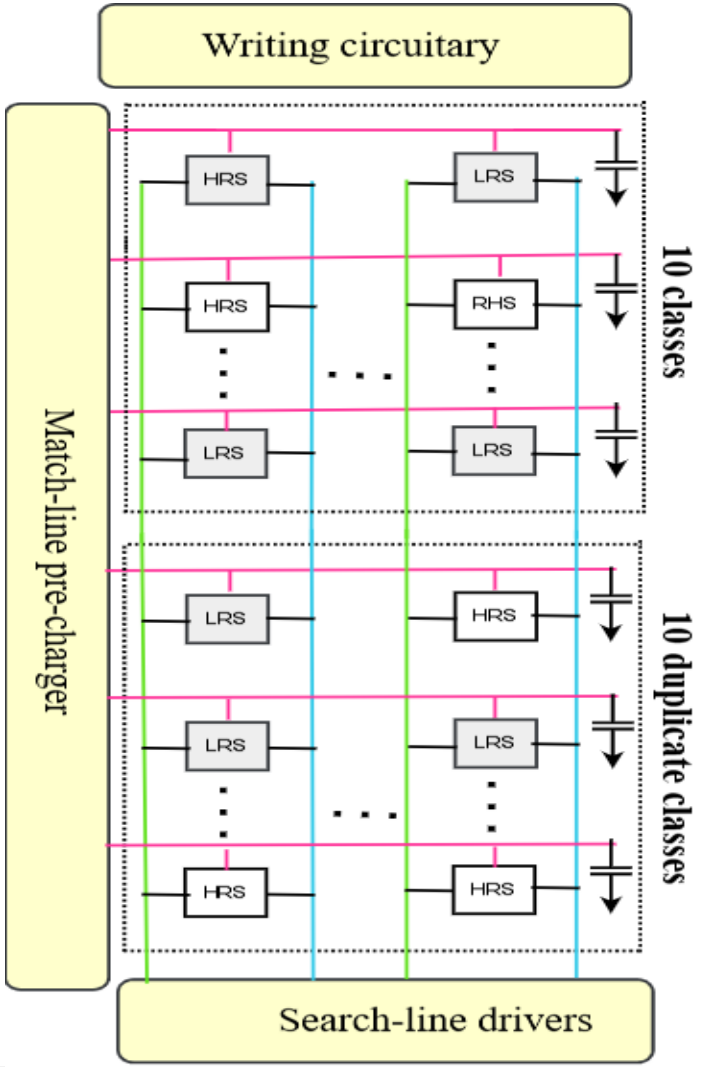
- **Collision Analysis:**
  - Narrow down candidate class hypervectors by analyzing query-class relationships.
- **Trace collection (simulations):**
  - Collect power traces during HDC operations.
  - Reveals potential class-dependent power traces.
- **Side channel attack:**
  - Use reduced traces to reveal actual class hypervectors.



[3] Brojogopal Sapui et al. 2023. Power Side-Channel Attacks and Countermeasures on Computation-in-Memory Architectures and Technologies. ETS. 1-6

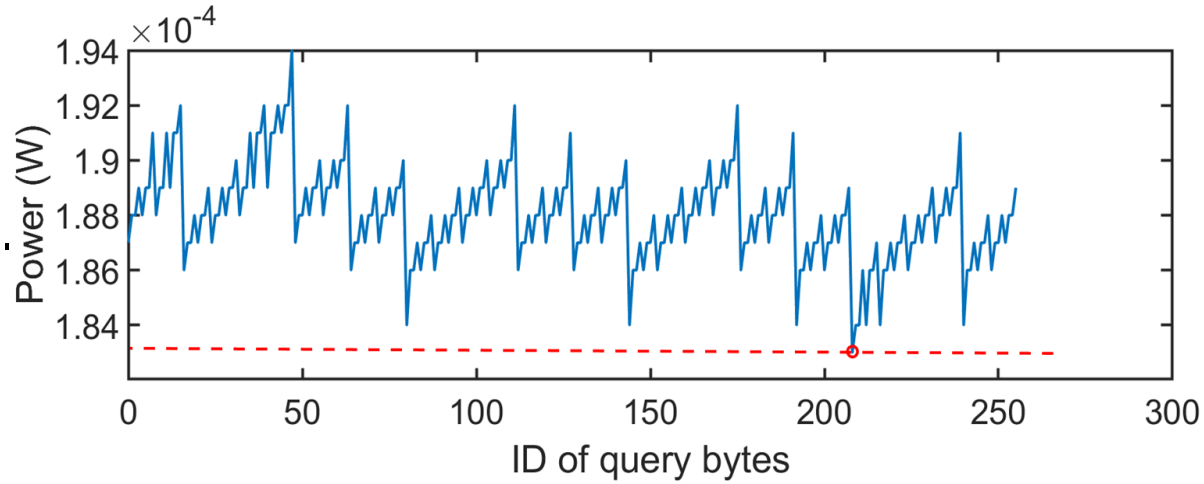
Countermeasure: balancing power

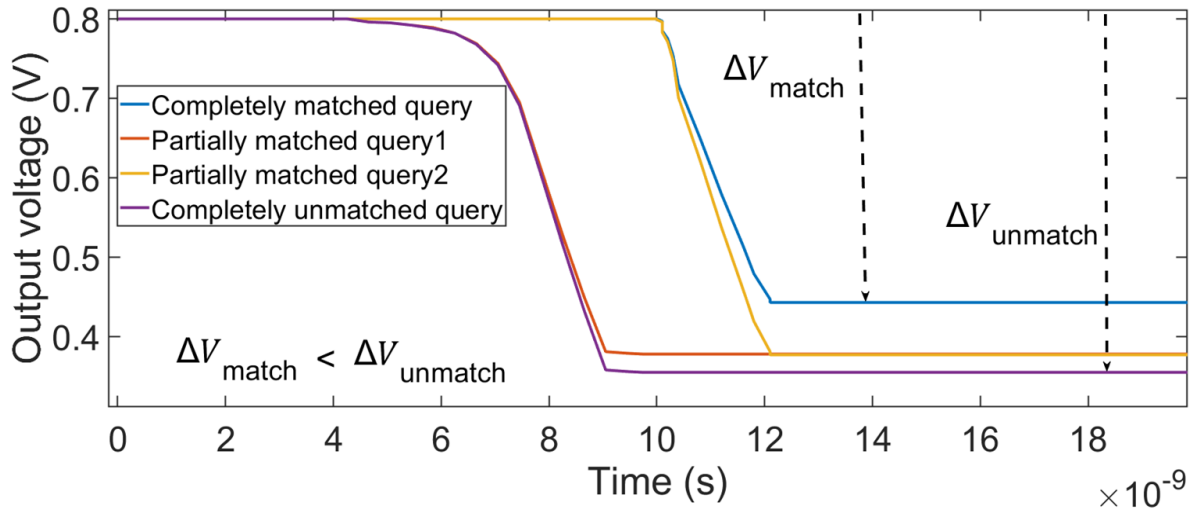
- **Dual-Rail Hiding Technique:**
  - Equalizes power consumption.
  - Reduces data-dependent variations in power profile.
- **Extension of CAM Array:**
  - Duplicates crossbar to store complementary hypervectors.
  - Each bit is paired with its complement.
- **Impact on Security:**
  - Masks data-dependent power signatures.
  - Power analysis ineffective for inferring class hypervectors.
- **Trade-Offs:**
  - Increases area (~87%) and power (~74%) overhead.
  - Scalable with constant overhead for varying array sizes.



Attack in HDC of 1-byte Query

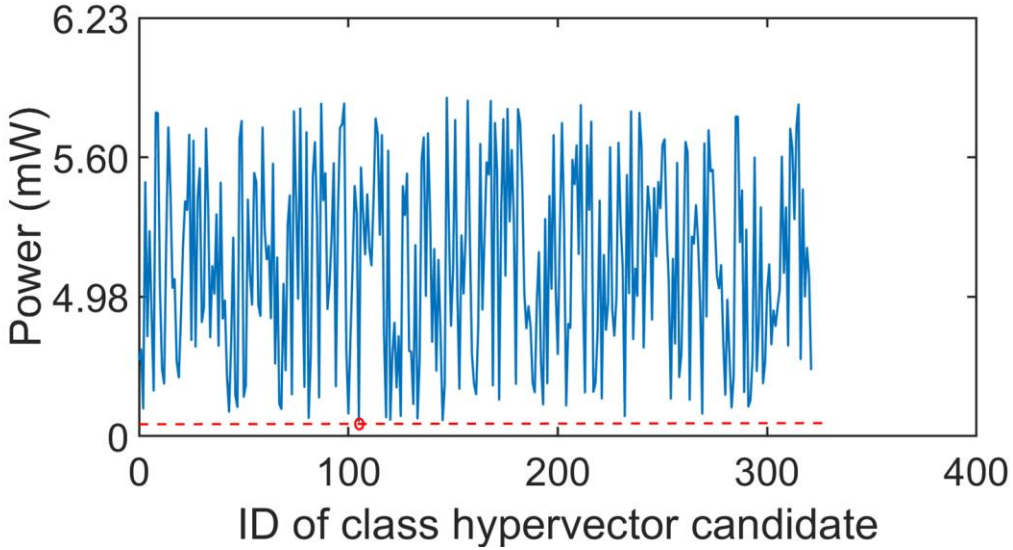
- **Power Variation Across Queries:**
  - Power variation reveals data-dependency.
  - Red line power for exactly matched queries.
- **Voltage Dynamics:**
  - Completely matched queries show lowest voltage transitions.
- **Implication for SCA:**
  - Query matching leaves observable power and voltage footprints.
  - Aiding side-channel attacks.

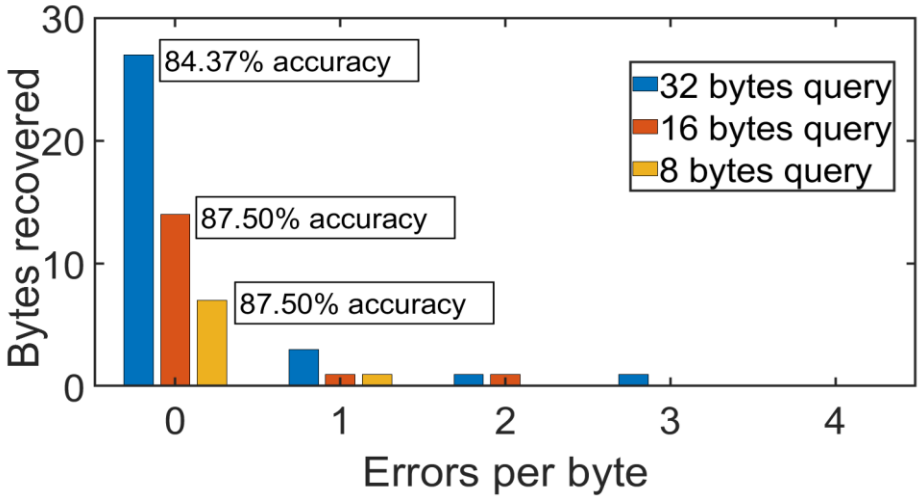




Attack in Unprotected Design: 32-byte Query

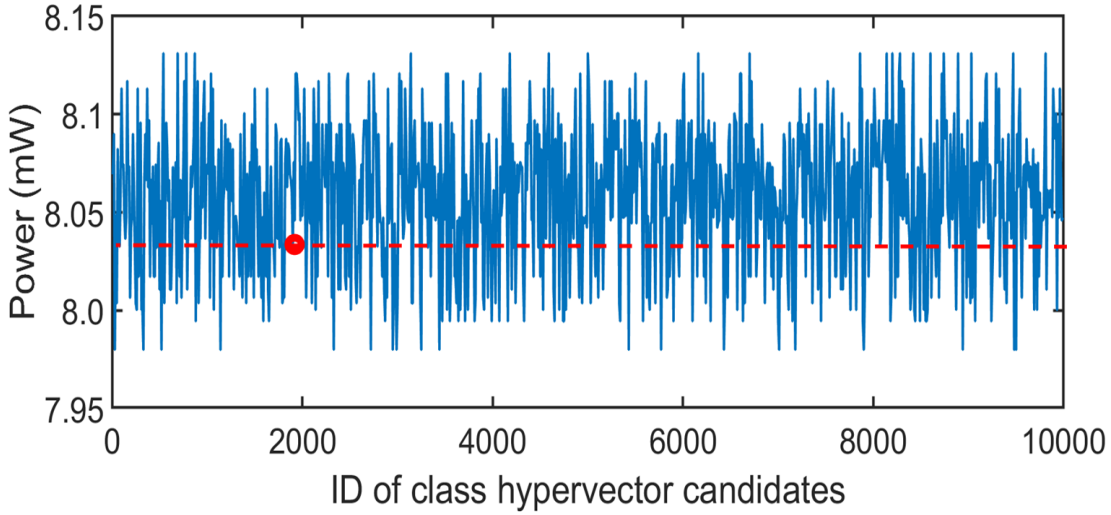
- **Power Analysis:**
  - Reveal variations across 338 hypervector candidates for class-4 in MNIST.
  - Most probable candidates align with the observed power patterns.
- **Efficiency of Attack:**
  - Requires only **338** traces for successful recovery.
  - Feasibility of attacks with few power traces.
- **Byte Recovery Accuracy:**
  - 32-byte queries recovered with **84.37% accuracy.**
  - 16-byte and 8-byte queries show **87.50% accuracy.**





Security Evaluation in Protected Design

- **Unsuccessful Collision Attack:**
  - Correct candidate class-hypervector is indistinguishable from others.
  - SCA fails in protected designs.
- **Power Profile:**
  - Uniform power distribution across all candidates prevents leakage.
- **Impact of Protection:**
  - Effectiveness of countermeasures in concealing power variations.



Countermeasure Impact and Future Goal

- **Overheads:**
  - **Power**: ~ **87% increase**.
  - **Area**: ~ **74% increase**.

- **Future Goal:**
  - Develop countermeasures with **reduced overhead**.
  - Maintain **system performance and efficiency** without significant compromises.

Conclusion

- **Key Contributions:**
- Demonstrated the vulnerability of CAM-based HDC to SCA.
- Proposed collision analysis to significantly reduce the traces.

- **Findings:**
- Unprotected designs leak information through **power traces** and voltage differences.
- Hiding can effectively prevent attacks but with **high power and area overheads**.

- **Future Directions:**
- Explore **low-overhead countermeasures** to balance security and system efficiency.
- Investigate advanced techniques to enhance **robustness**.

Thank you for your attention!
Any Question?

For any further questions contact:

brojogopal.sapui@kit.edu