2023-12-29

NVM的加密問題及效能優化

NVM encryption issues and performance optimization

第七組

CONTENTS

01

Introduction

Introduction

- **NVM Definition & Importance**: Non-Volatile Memory (NVM) such as PCM, ReRAM, and STT-MRAM, outperforms DRAM with higher density, lower power leakage, and faster reads. While useful for retaining data without power, it poses security challenges.
- **Security Challenges in Memory Technology**: NVMs like PCM, ReRAM, and STT-MRAM offer efficiency but have security vulnerabilities. Encryption is key but affects performance and durability.

Introduction

- **ROM**
  - **Basics**: ROM stores firmware and data that rarely changes.
  - **Use & Limits**: Widely used with update limitations.
- **Flash Memory**
  - **Basics**: Non-volatile with fast reads but limited writes.
  - **Use & Limits**: Great for data storage; requires encryption for security.
- **NVRAM**
  - **Basics**: Speed of RAM with flash persistence.
  - **Use & Limits**: Ideal for critical data retention; encryption is challenging.

02

Motivation

Motivation

- **Demand for High-Performance NVM Solutions**: Encryption enhances security but reduces performance and lifespan. Research focuses on improving encryption efficiency while maintaining security.
- **Research Scope & Purpose**: Addressing NVM's durability and enhancing performance and lifespan amidst encryption challenges.

03

Strategies for Performance Enhancement

Strategies for Performance Enhancement

Encryption Time Reduction

- **Efficient Algorithms**: Enhanced encryption methods like 3-level and 8-block split counter mode have shown to boost performance significantly.
- **Hardware Acceleration**: Logic-in-memory (LiM) technology reduces data transfer overheads and accelerates encryption by leveraging non-volatile device characteristics.

Strategies for Performance Enhancement

I/O Performance Optimization

- **Data Compression**: Techniques like Base Delta Immediate (BDI) compress data pre-encryption, lessening write operations to NVM.
- **Smart Caching**: Reducing re-encryption of unaltered words in cache lines diminishes write wear. BLE, for example, re-encrypts data only when a local modification counter is maxed out.

04

Challenges of Flash Memory Encryption

Challenges of Flash Memory Encryption

- Flash memory operates on a page basis for encryption and writing.
- Identifying clean and dirty lines doesn't reduce bit flips as entire pages need rewriting, not just altered data.
- Slower writing speeds compared to reading increase the performance cost of encryption.
- Limited lifespan of MLC types (around 10^6 write cycles).

05

Related Work and Experimental

Related Work and Experimental

Efficient In-Memory AES Encryption Implementation Using a General Memristive Logic

- **Methodology**: Utilizes logic-in-memory (LiM) technology, harnessing non-volatile device properties for efficient Boolean operations, integrating memristive logic with sense amplifier-based logic.
- **Experimental Results**: Demonstrated significant speed and energy efficiency gains. Encrypting 1 GB data showed 1.38 to 1.56 times speedup and 1.7 times energy efficiency over existing in-memory AES methods.

Related Work and Experimental

Efficient Split Counter Mode Encryption for NVM

- **Methodology**: Introduced 3-level and 8-block split counter mode encryption to optimize encryption efficiency in NVM.
- **Experimental Results**: Achieved up to 30% maximum and 8-9% average performance improvement compared to the original encryption method.

Related Work and Experimental

Enhance the Lifetime of PCM Memory by Reducing the Bit Flips

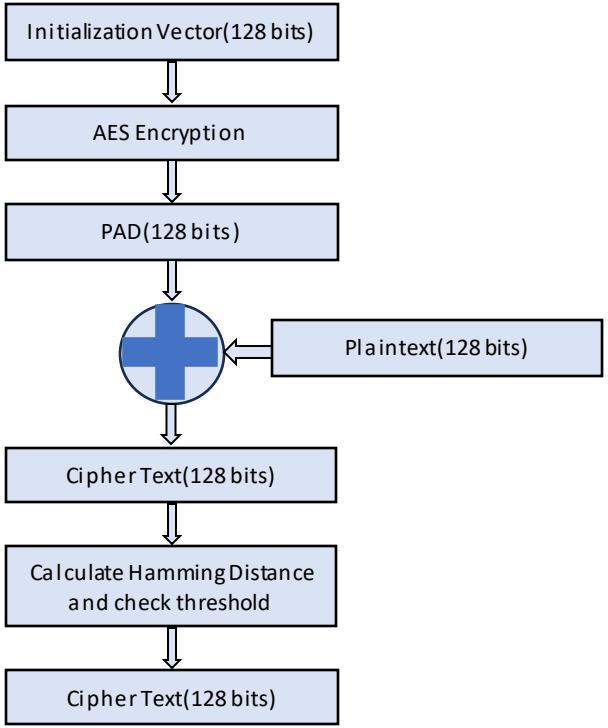
- **Methodology**: The study adopts the AES-CTR encryption algorithm, which strategically reduces bit transitions during the writing process to memory cells, thus aiming to curtail the rate of wear and extend memory longevity.
- **Experimental Results**: The results show a significant reduction in bit flips, leading to an enhanced PCM lifetime. The paper demonstrates the potential of this approach for improving PCM endurance.

06

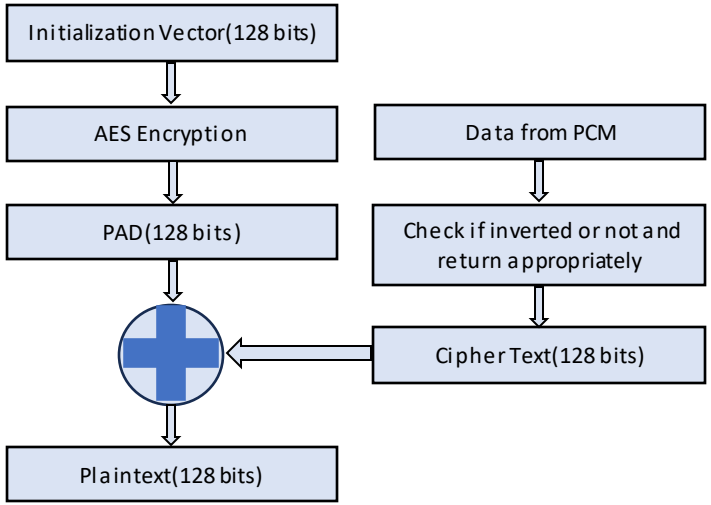
Methodology and Algorithms

Methodology and Algorithms

- **AES-CTR**



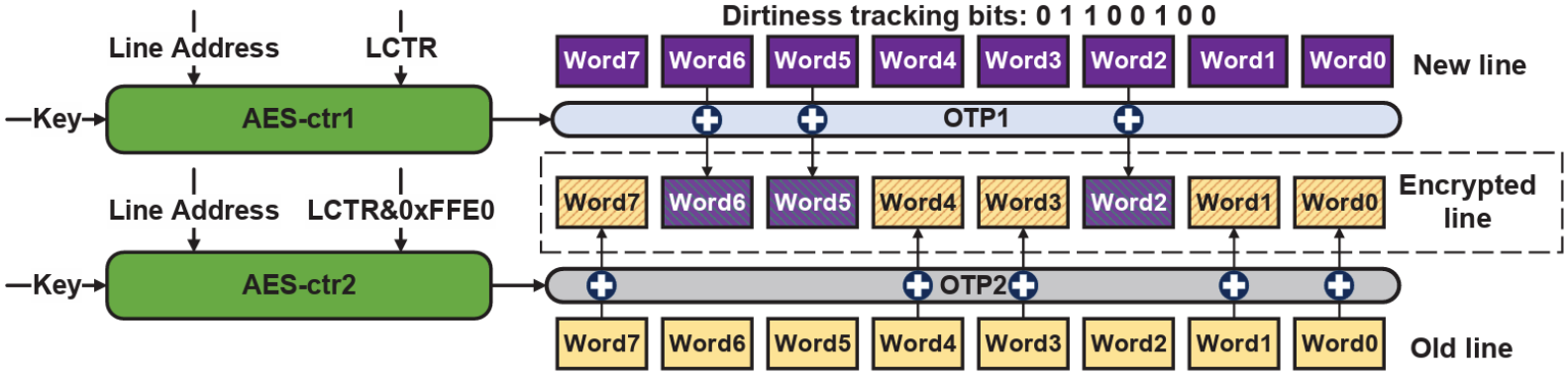
- Write Phase Block Diagram



- Read Phase Block Diagram

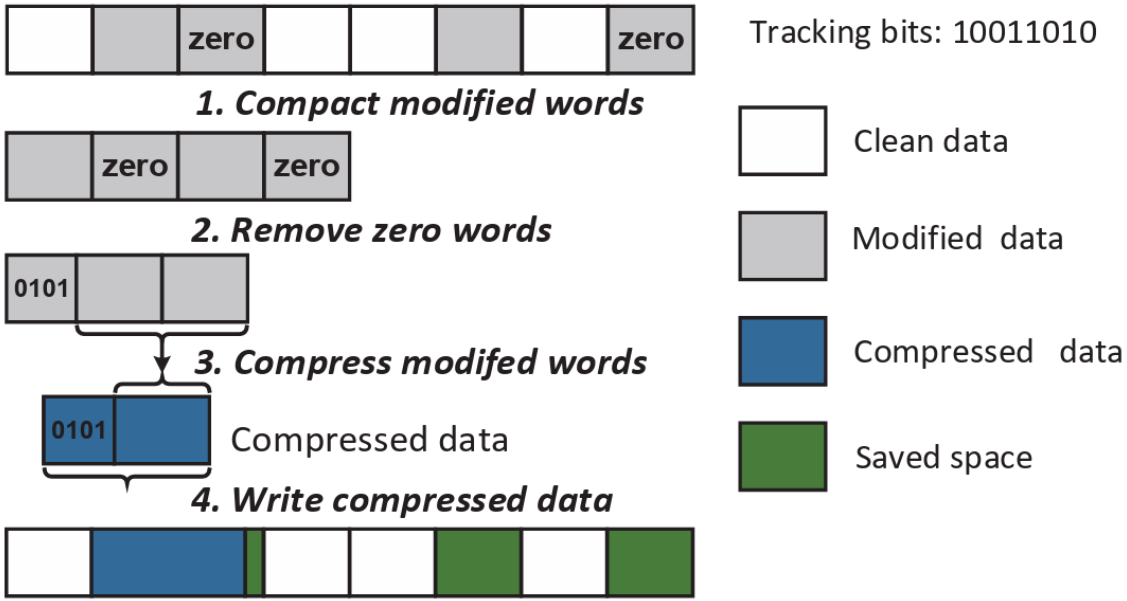
Methodology and Algorithms

- **DEUCE: Counter-Mode Encryption for Clean Word Write Prevention**



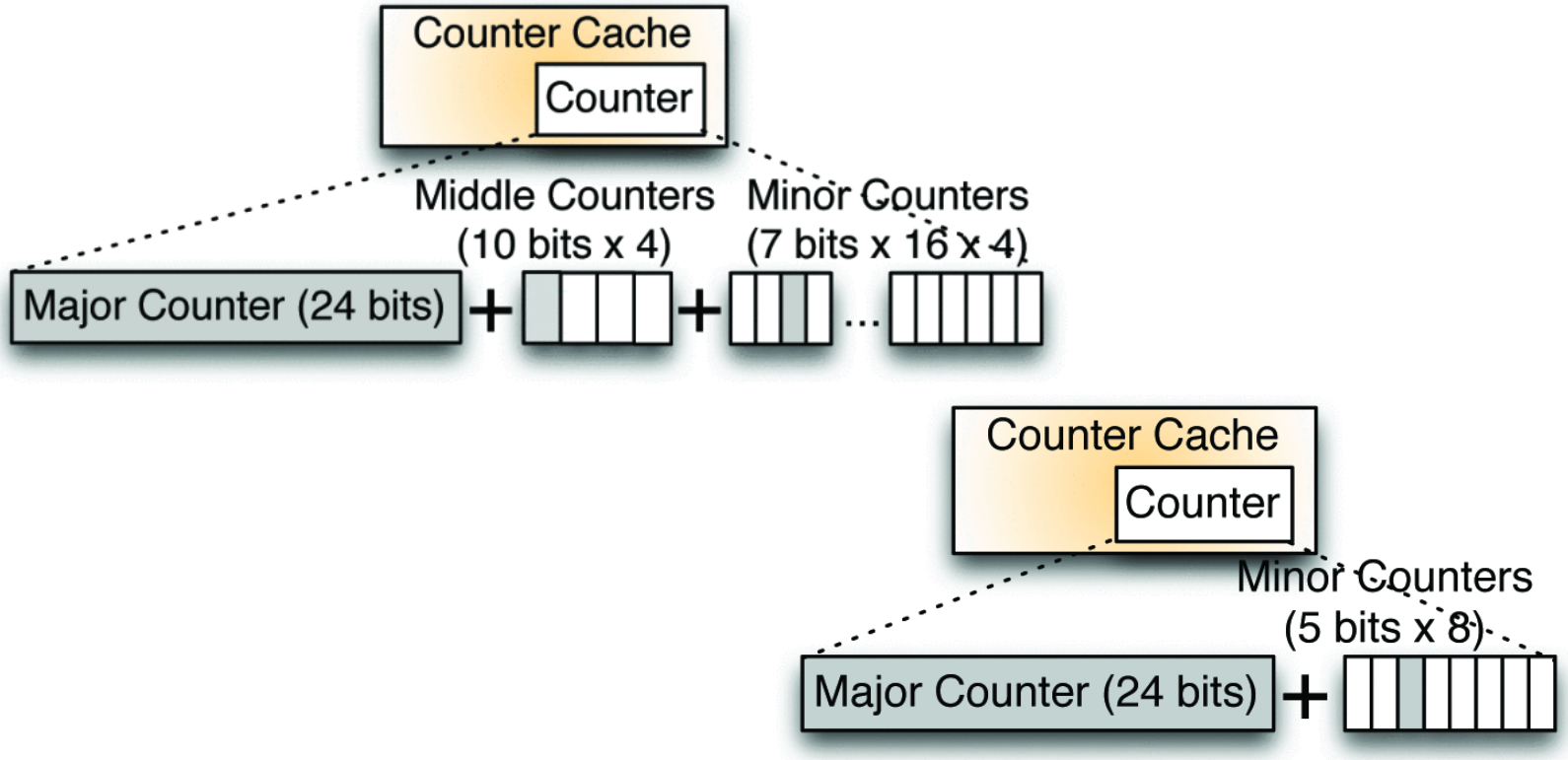
Methodology and Algorithms

- **MSE (Morphable Selective Encoding)**



Methodology and Algorithms

- **Split Counter Mode**



07

Conclusion and Future Prospects

Conclusion and Future Prospects

08

Reference

Reference

- Efficient In Memory AES Encryption Implementation Using a General Memristive Logic Surmounting the data movement bottleneck
- Efficient Split Counter Mode Encryption for NVM
- Enhance the Lifetime of PCM Memory by Reducing the Bit Flips
- Improving the Heavy Re-encryption Overhead of Split Counter Mode Encryption for NVM
- MORE2 Morphable Encryption and Encoding for Secure NVM

THE END

THANKS