新興記憶體儲存系統元件期中報告

GROUP 7

OUTLINE

- Background Introduction
- Related Work
- Motivation
- Problem and probably solution
- Reference

INTRODUCTION

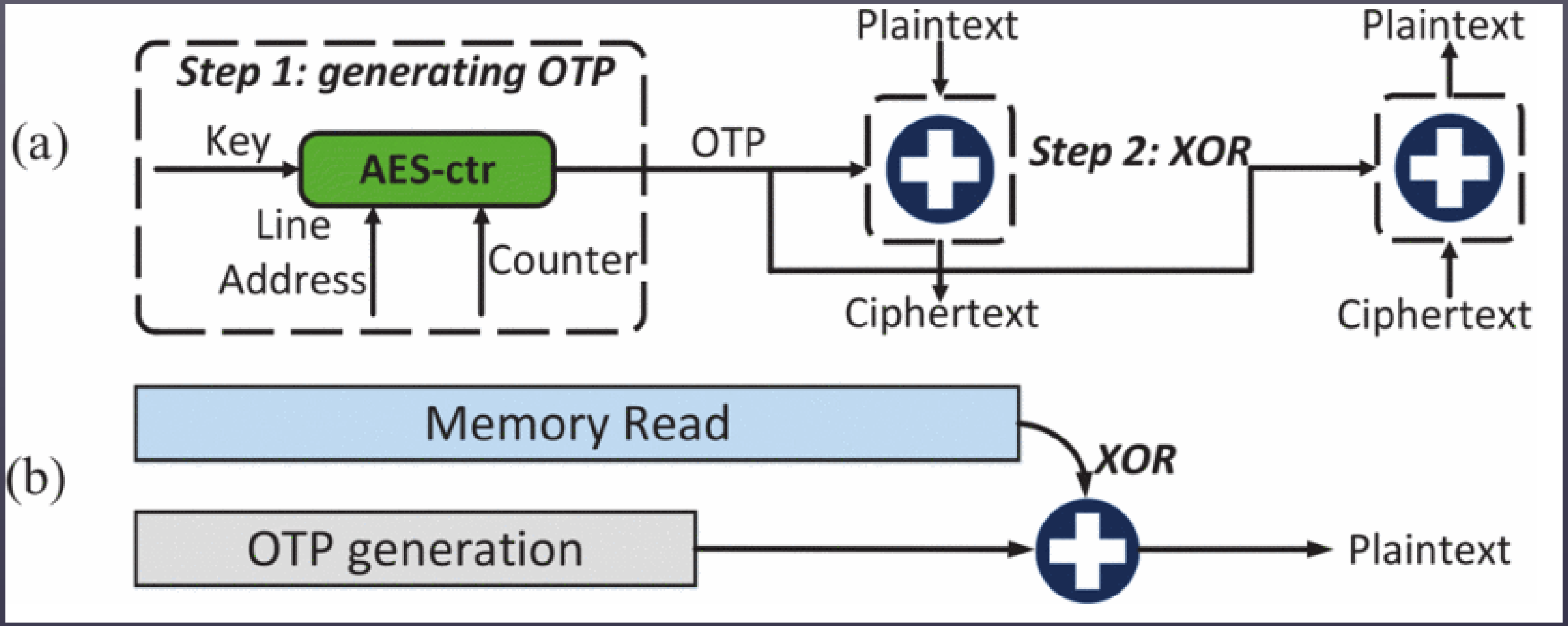
- Non-Volatile Memory (NVM):
  - Characteristics:
    - High Density: Provides higher storage density.
    - Fast Read Speed: Faster compared to traditional DRAM technology.
    - Non-Volatile Nature: Data persists even after power-off.
  - Various Types:
    - Flash Memory
    - Phase-Change Memory (PCM)
    - Resistive Random-Access Memory (ReRAM)

INTRODUCTION

- Non-Volatile Memory (NVM):
  - Security Challenges:
    - Data Persistence Risk: NVM's non-volatile nature increases security risks.
  - Endurance Challenges
    - NVM technologies, such as Flash memory, have limited write endurance, leading to potential degradation and failure after a certain number of write cycles.

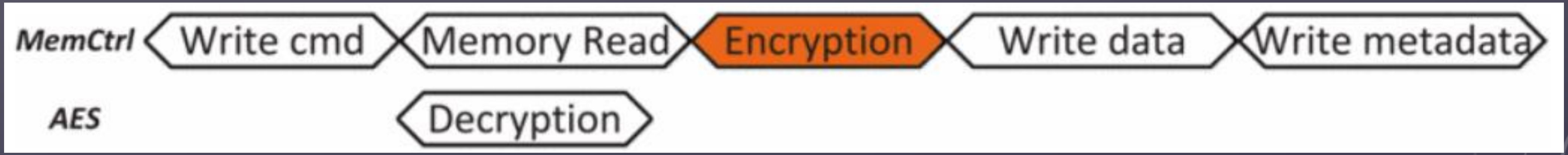
COUNTER MODE ENCRYPTION

Memory encryption



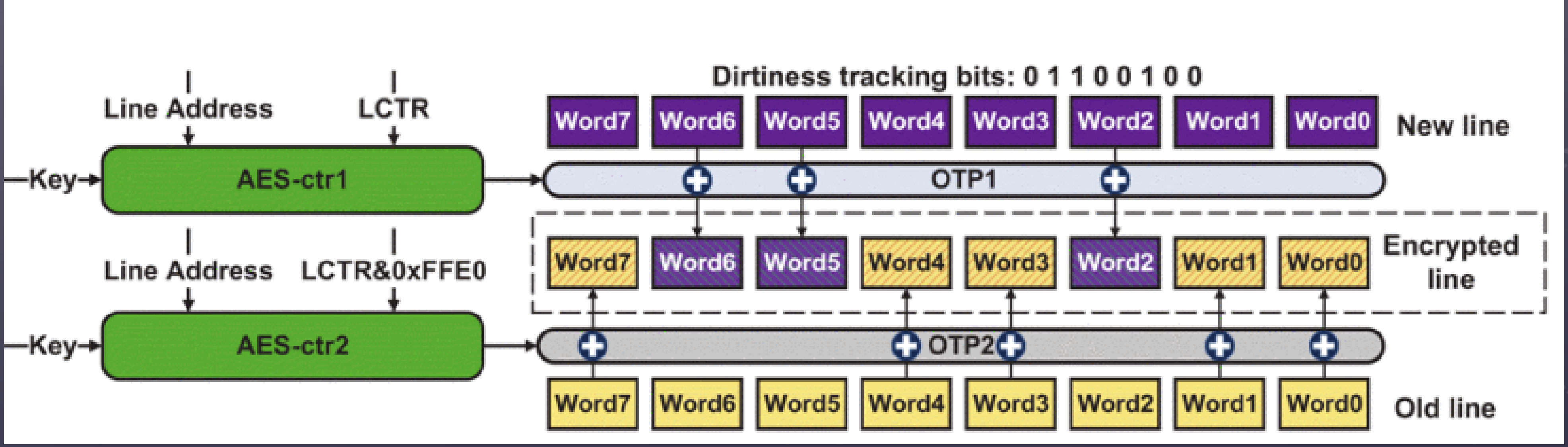
SERIAL ENCRYPTION

Serial encryption prolongs the write latency.



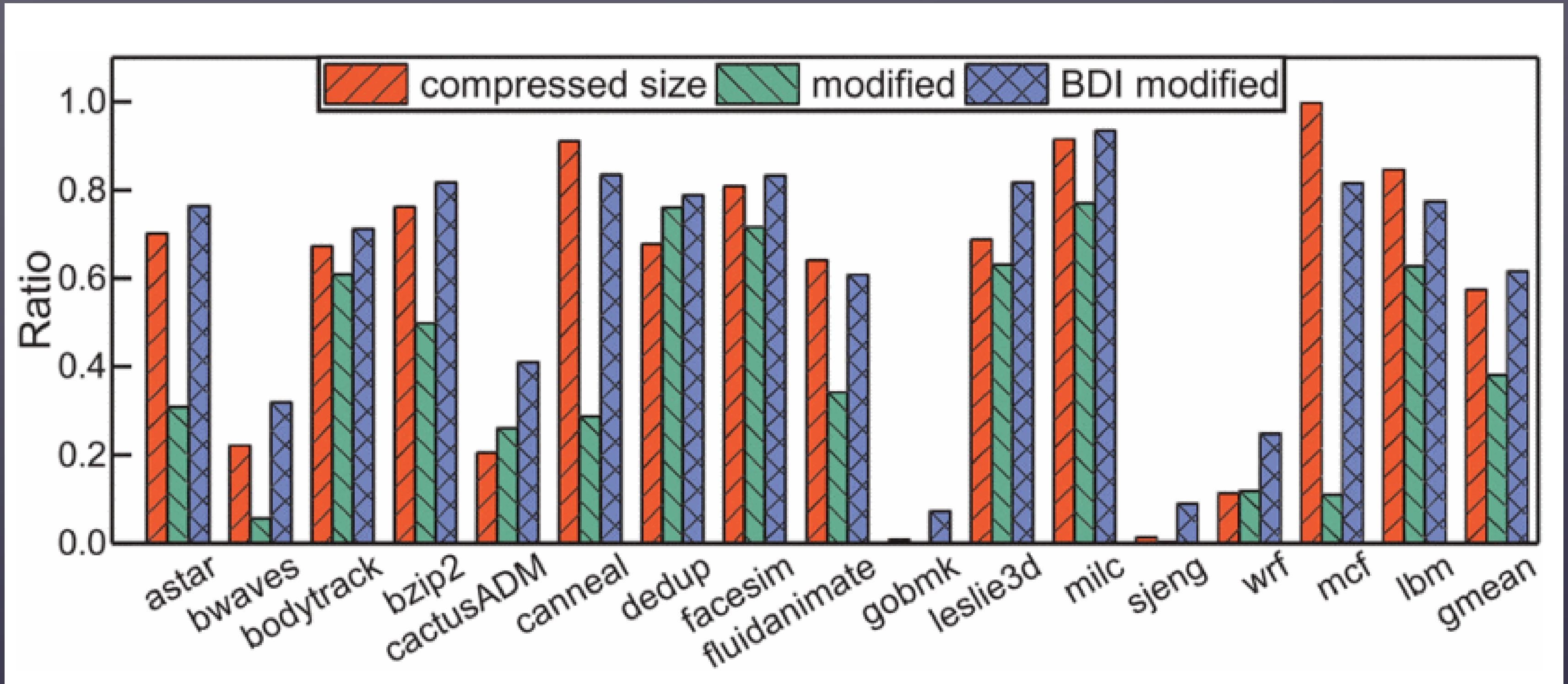
CLEAN WORD ENCRYPTION

DEUCE: Counter-Mode Encryption for Clean Word Write Prevention



COMPRESSION CHALLENGE

Using BDI compression



ISSUES

- Many Clean Words Still Encrypted:

  Despite the reduction in re-encryption of clean words by current encryption techniques like BLE, DEUCE, and SECRET, some clean words persist.

- Compression Techniques Increase Modified Words:

  Current compression techniques reduce encrypted data size but create many modified words.

MOTIVATION

- Challenges in Applying Encryption to NVM:
  - Extended encryption latency reduces system performance.
  - Encryption leads to increased bit writes, impacting endurance.
- Challenges in Encryption and Compression Techniques:
  - Insufficient Reduction of Clean Words Encryption
  - Impact of Compression Techniques on Clean Words

PROBLEM

- Defending against attacks on NVM's non-volatile characteristics
- **Encryption and Performance:**
    - Encryption method choice is intertwined with performance.
    - Inappropriate methods impact both performance and memory lifespan.
- **Crucial Question:**
    - How to efficiently and securely encrypt data in NVM?
    - Emphasis on safeguarding non-volatile data.

PROBLEM—PROBABLY SOLUTION

- Clean Row Prediction and Pre-encryption:

  Predict and pre-encrypt clean rows before data modification to reduce encryption latency.

- Advanced Data Compression:

  Improve data compression techniques to minimize the number of modified words and reduce encryption frequency.

- Counter Segmentation for Overflow Reduction:

  Segment large counters into smaller ones to decrease the likelihood of overflow, reducing the need for re-encryption.

REFERENCE

- MORE2: Morphable Encryption and Encoding for Secure NVM
- Efficient In-Memory AES Encryption Implementation Using a General Memristive Logic: Surmounting the data movement bottleneck
- Efficient Split Counter Mode Encryption for NVM
- NVCool: When Non-Volatile Caches Meet Cold Boot Attacks

Q&A