DEFY: A Deniable, Encrypted File System for Log-Structured Storage.

Timothy M. Peters, Mark A. Gondree, and Zachary N. J. Peterson. In NDSS'15

Presented by Fengwei Zhang

Introduction

- In 2012, a videographer smuggled evidence of human rights violations out of Syria. He lacked any data protection mechanisms and instead hid a micro-SD card in a wound on his arm

- Human rights group, ND-Burma, collects data on hundreds of thousands of human rights violations by the Burmese government. ND-Burma activists carry data on mobile devices, risking exposure at checkpoints and border crossings

Introduction

- Traditional encryption may not work when an adversary is able to coerce device owners into revealing their encrypted content

- Plausibly Deniable Encryption (PDE)

Related Work

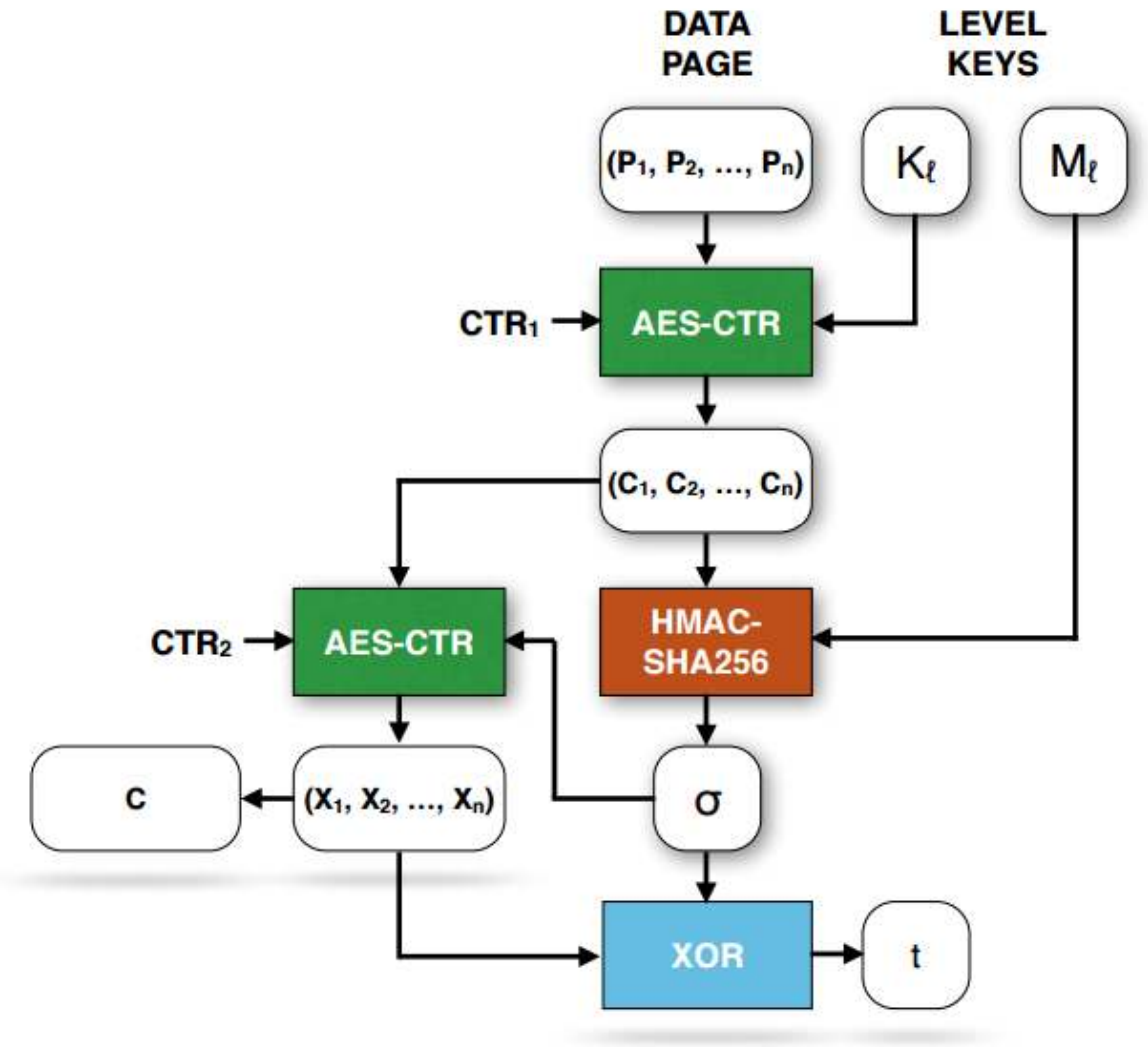
- Steganography-based
  - StegFS [1] hides blocks within random data and it works on Ext2 file system. However, the existence of the modified Ext2 driver and the external block table may make the system suspicious.
- Hidden volumes-based
  - Mobiflage [2], MobiPluto [3]

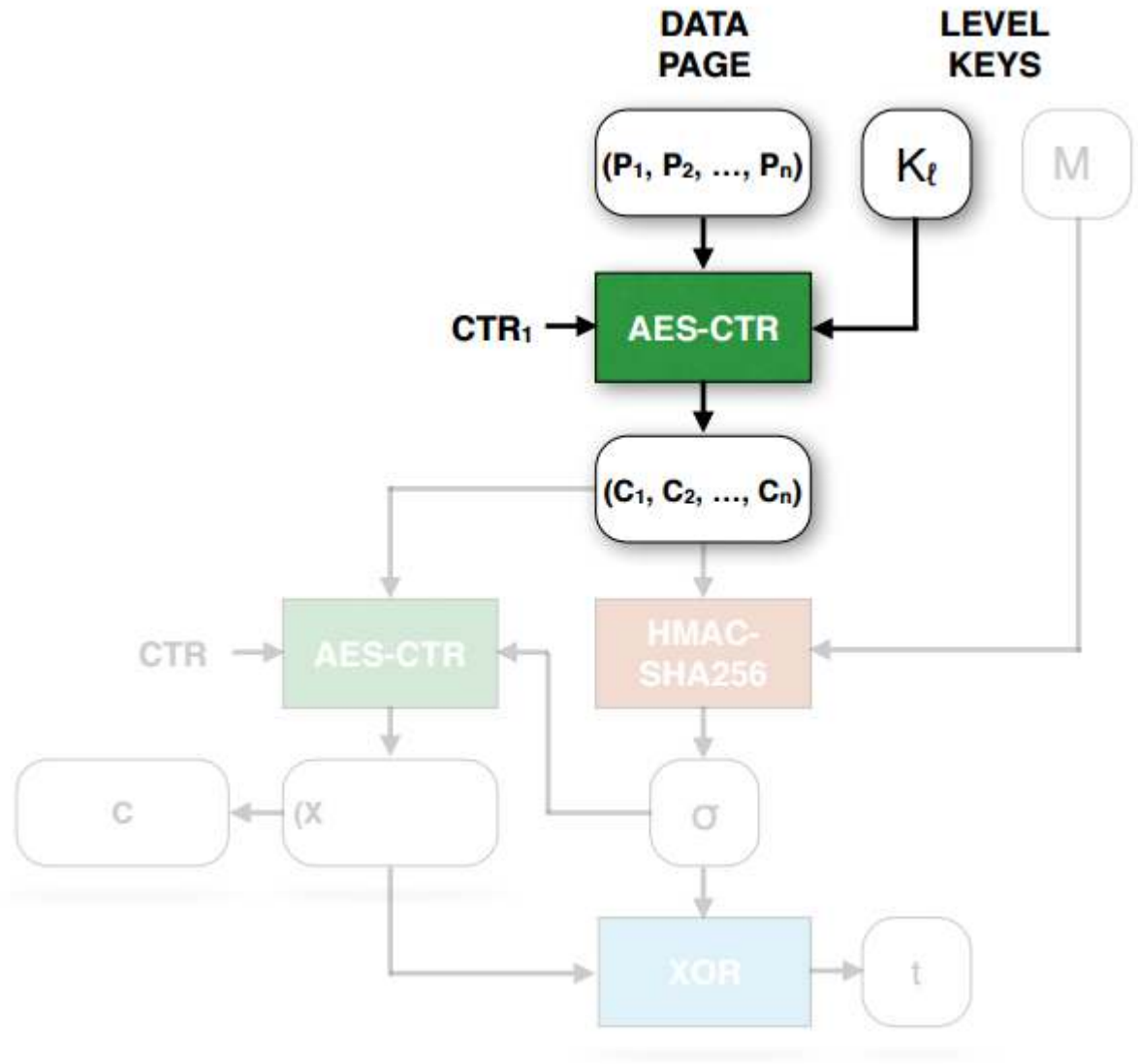
DEFY

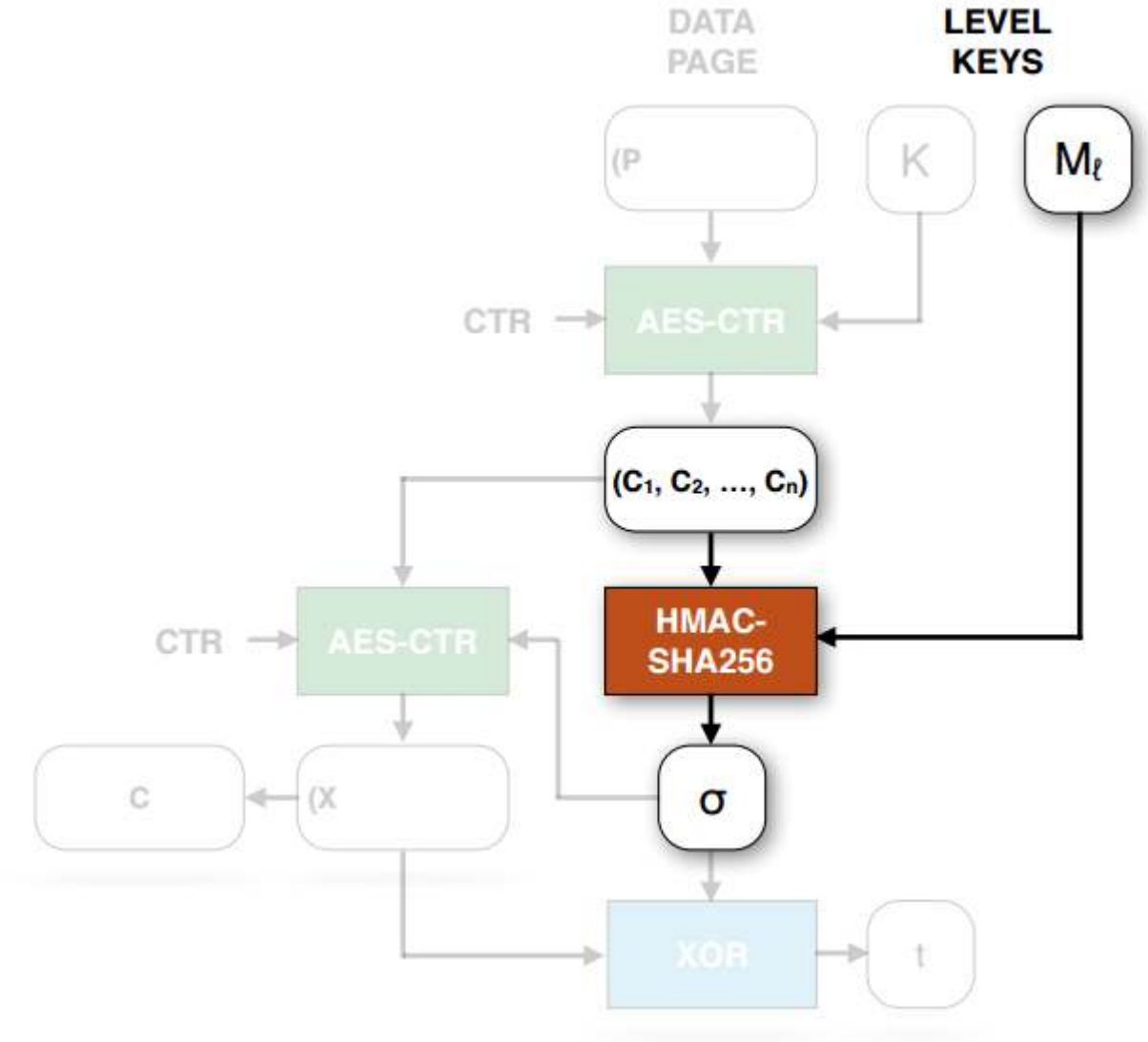
- DEFY, the Deniable Encrypted File System from YAFFS
- File-system, Flash-based
- Resistant against the most powerful adversary considered by prior work, a snapshotting adversary

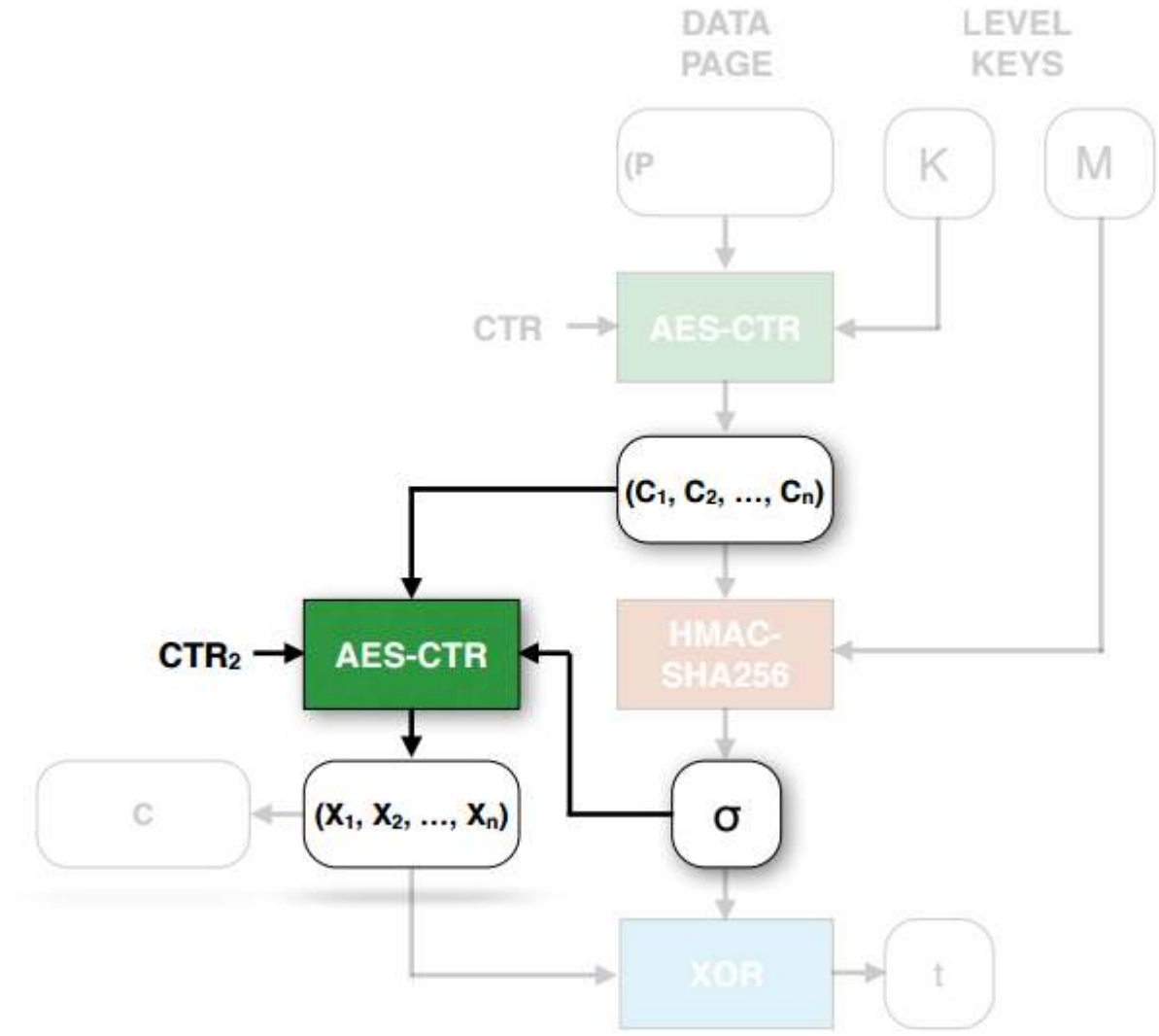
YAFFS

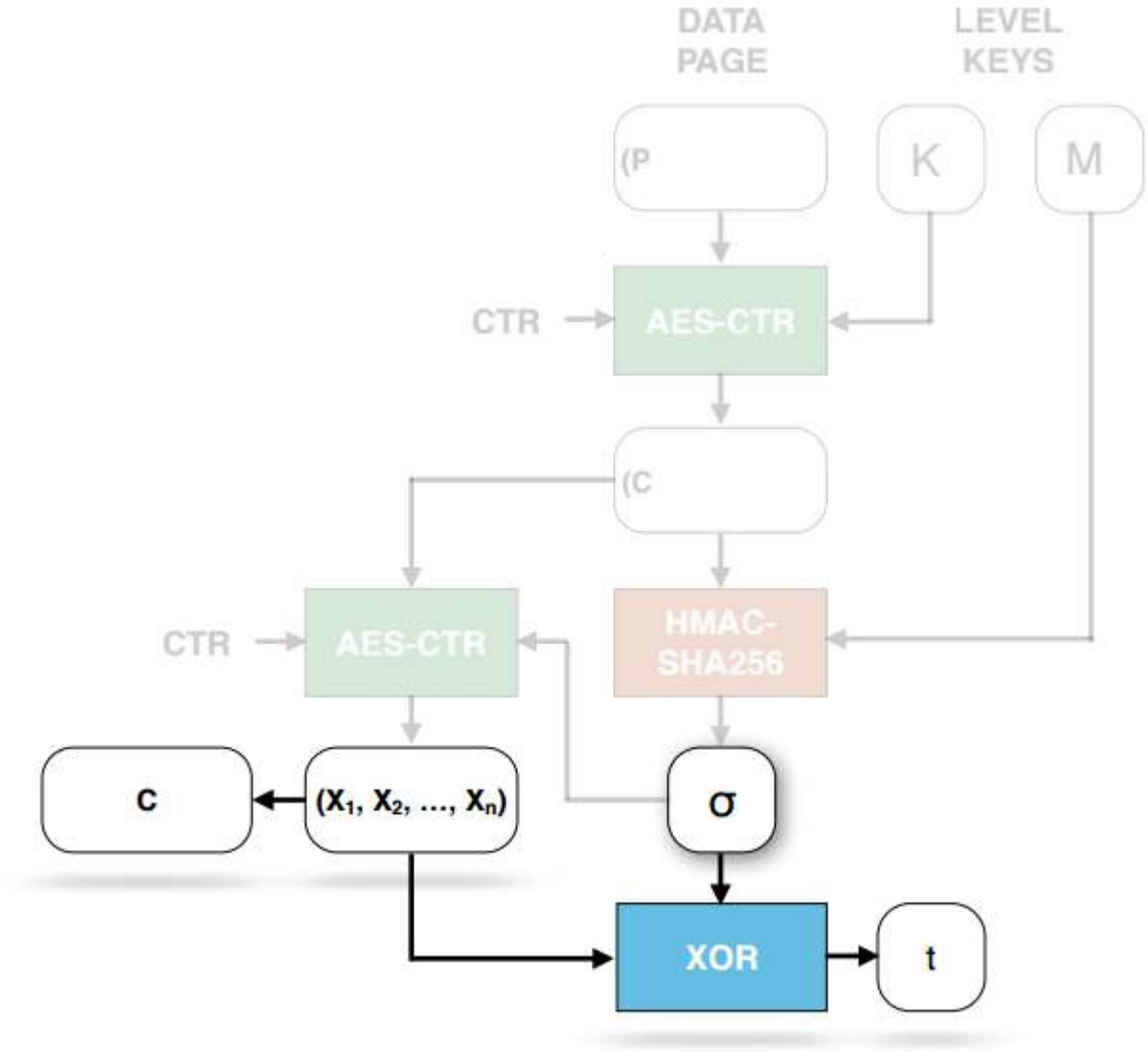
- File system designed for use with NAND flash
- Log-structured file system in that write requests are allocated sequentially
- Read/write at the page level (e.g., page size 4KB) and erasure occurs at the block level (e.g., block size 256KB)
- YAFFS1 vs. YAFFS2

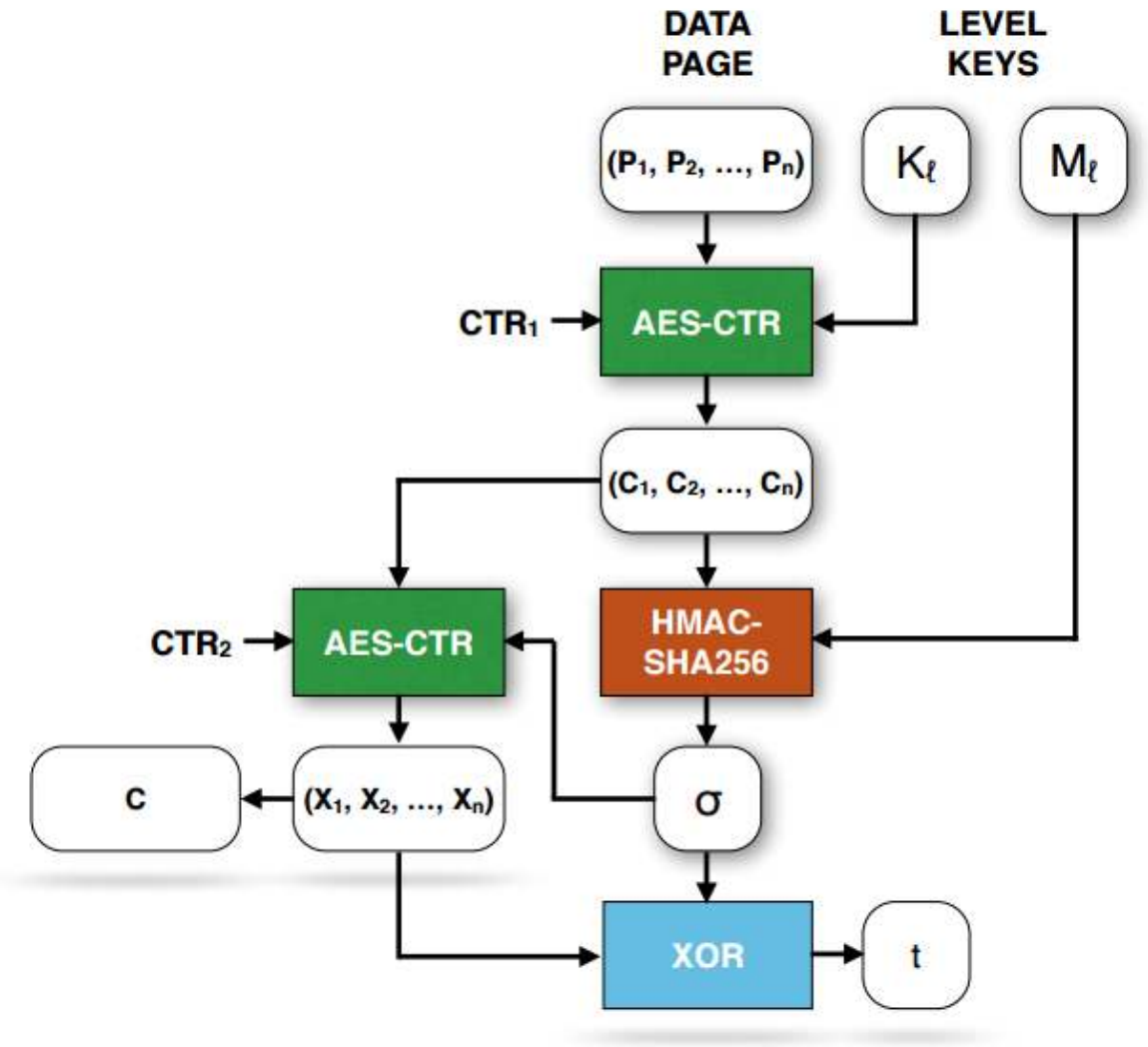

DATA PAGE
LEVEL KEYS
$(P_1, P_2, \ldots, P_n)$
K_ℓ
M_ℓ
CTR_1
AES-CTR
$(C_1, C_2, \ldots, C_n)$
CTR_2
AES-CTR
HMAC-SHA256
C
$(X_1, X_2, \ldots, X_n)$
σ
XOR
t


DATA PAGE
LEVEL KEYS
(P1, P2, …, Pn)
Kℓ
M
CTR1
AES-CTR
(C1, C2, …, Cn)
CTR
AES-CTR
HMAC-SHA256
C
X
σ
XOR
t


DATA PAGE
LEVEL KEYS
(P
K
M_ℓ
CTR
AES-CTR
$(C_1, C_2, \ldots, C_n)$
CTR
AES-CTR
HMAC-SHA256
C
(X
σ
XOR
t


DATA PAGE
LEVEL KEYS
(P
K
M
CTR
AES-CTR
$(C_1, C_2, \ldots, C_n)$
CTR_2
AES-CTR
HMAC-SHA256
C
$(X_1, X_2, \ldots, X_n)$
σ
XOR
t


DATA PAGE
LEVEL KEYS
(P
K
M
CTR
AES-CTR
(C
CTR
AES-CTR
HMAC-SHA256
C
(X1, X2, …, Xn)
σ
XOR
t


DATA PAGE
LEVEL KEYS
(P1, P2, …, Pn)
Kℓ
Mℓ
CTR1
AES-CTR
(C1, C2, …, Cn)
CTR2
AES-CTR
HMAC-SHA256
C
(X1, X2, …, Xn)
σ
XOR
t

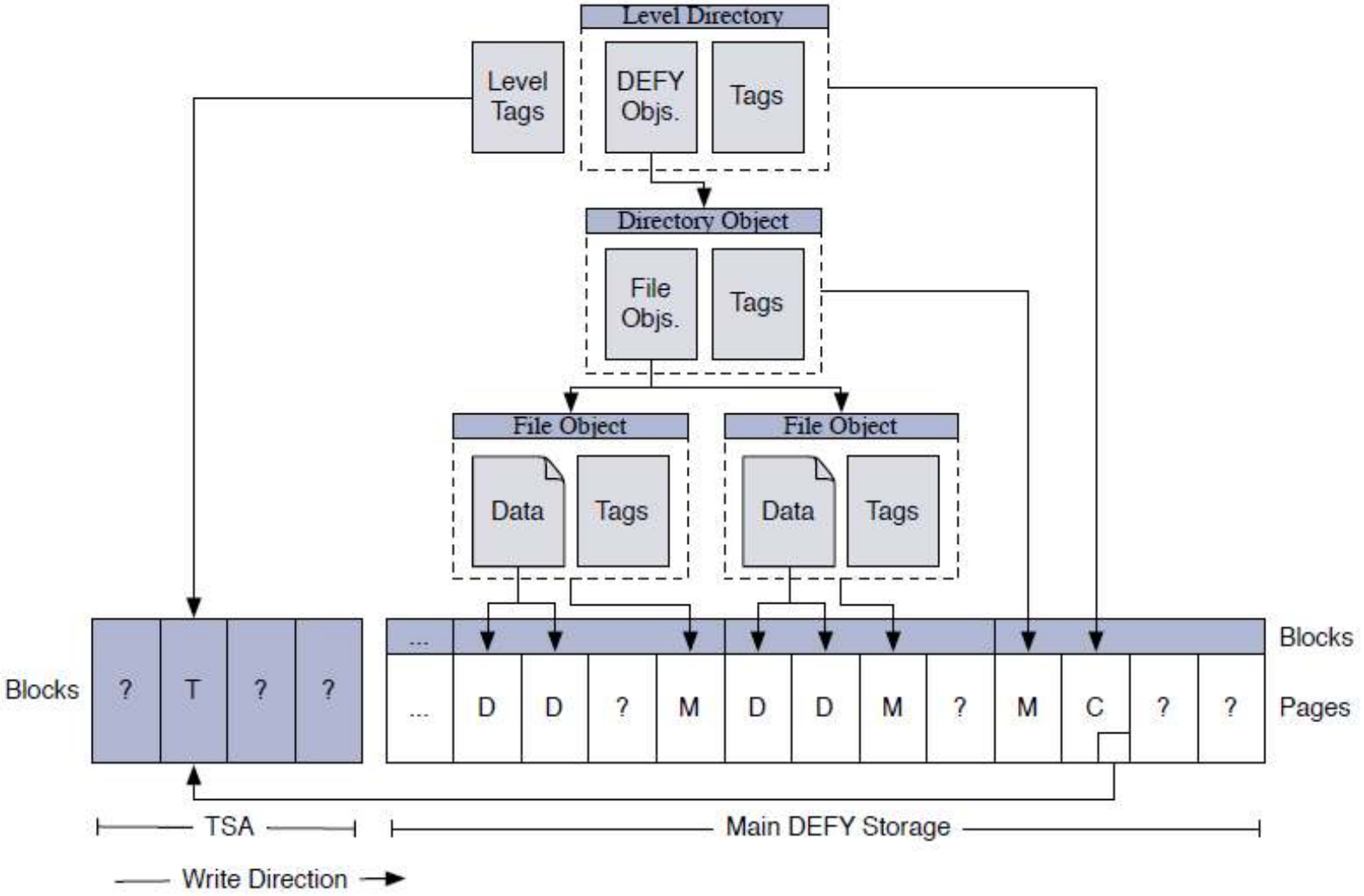


Fig. 2: An overview of the hierarchical structure of DEFY's metadata.

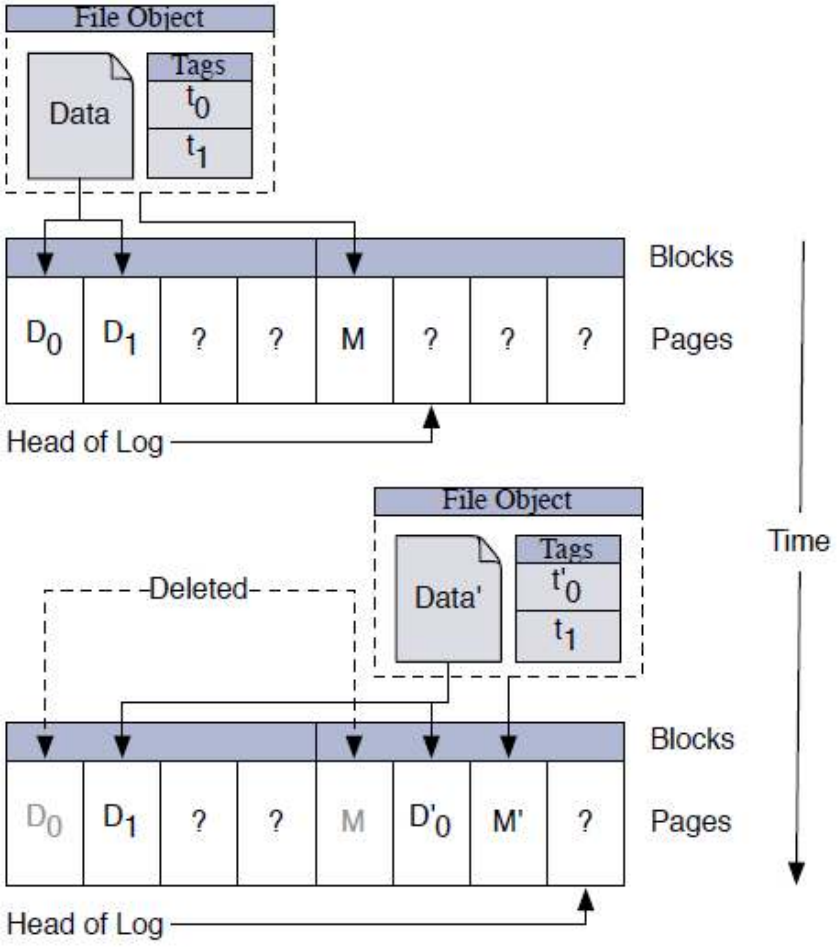


Fig. 3: A page-level view of a file being updated. In this example, the first logical page of the file is updated. This results in the replacement of the prior tag (t_0) with a new tag (t'_0), effectively deleting the prior version of the data page (D_0). A new file object is re-written (M') and a new tag for that object is stored in its parent object, effectively deleting the previous object (M).

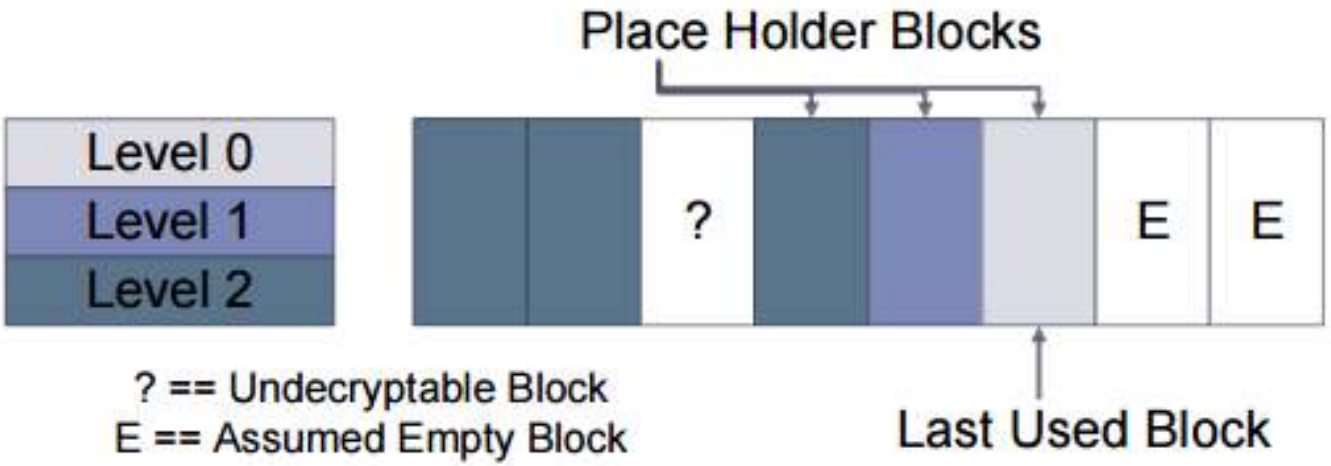
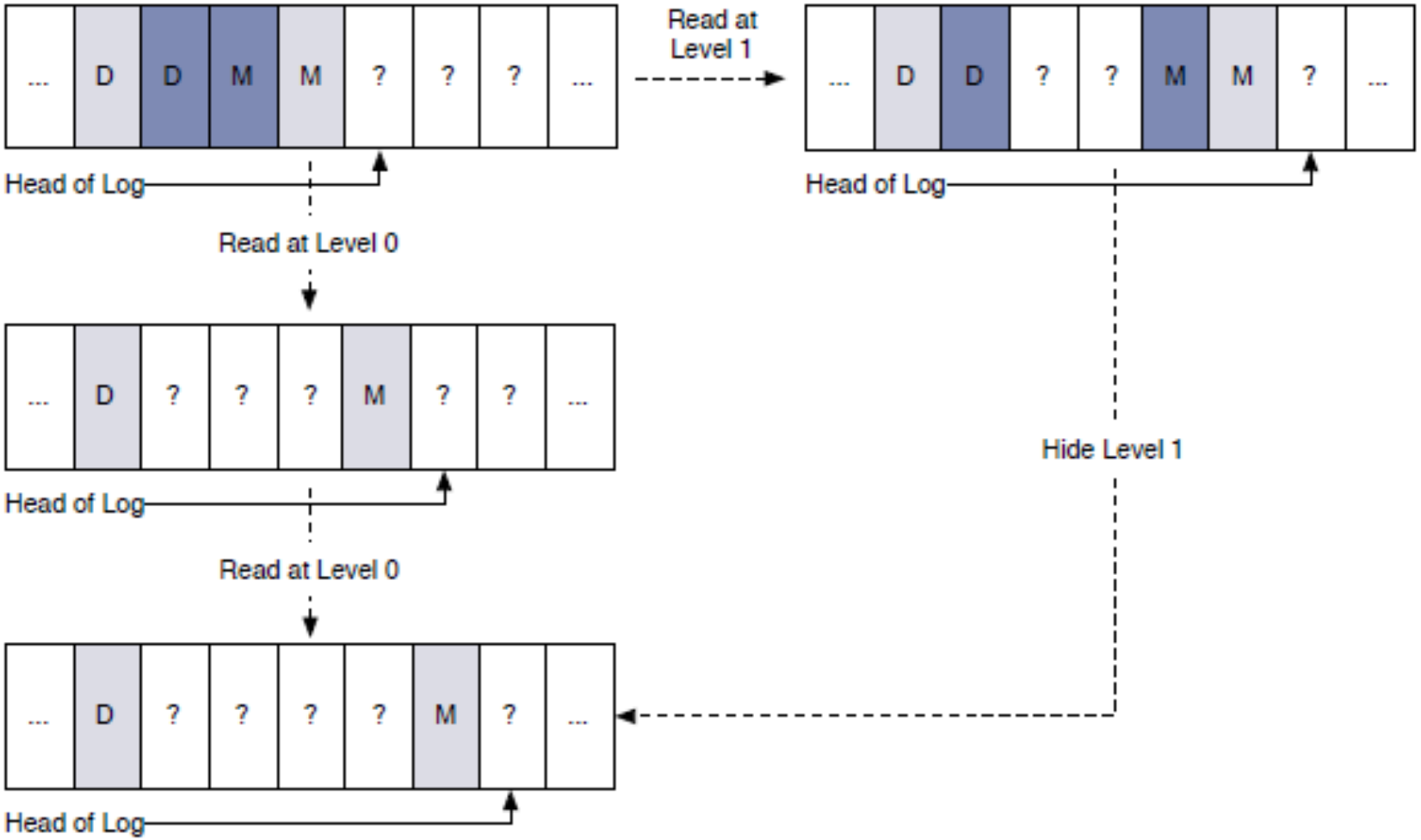
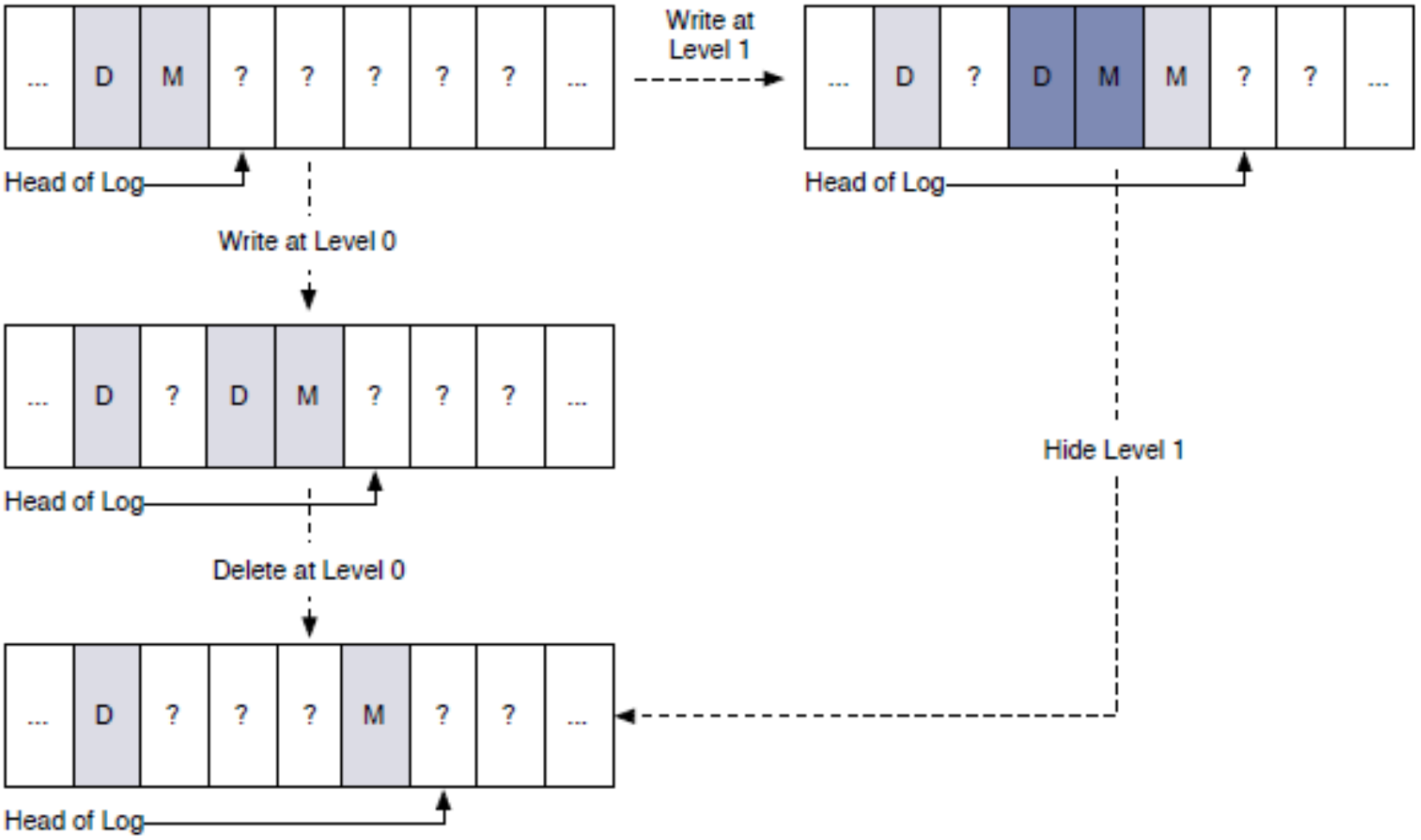


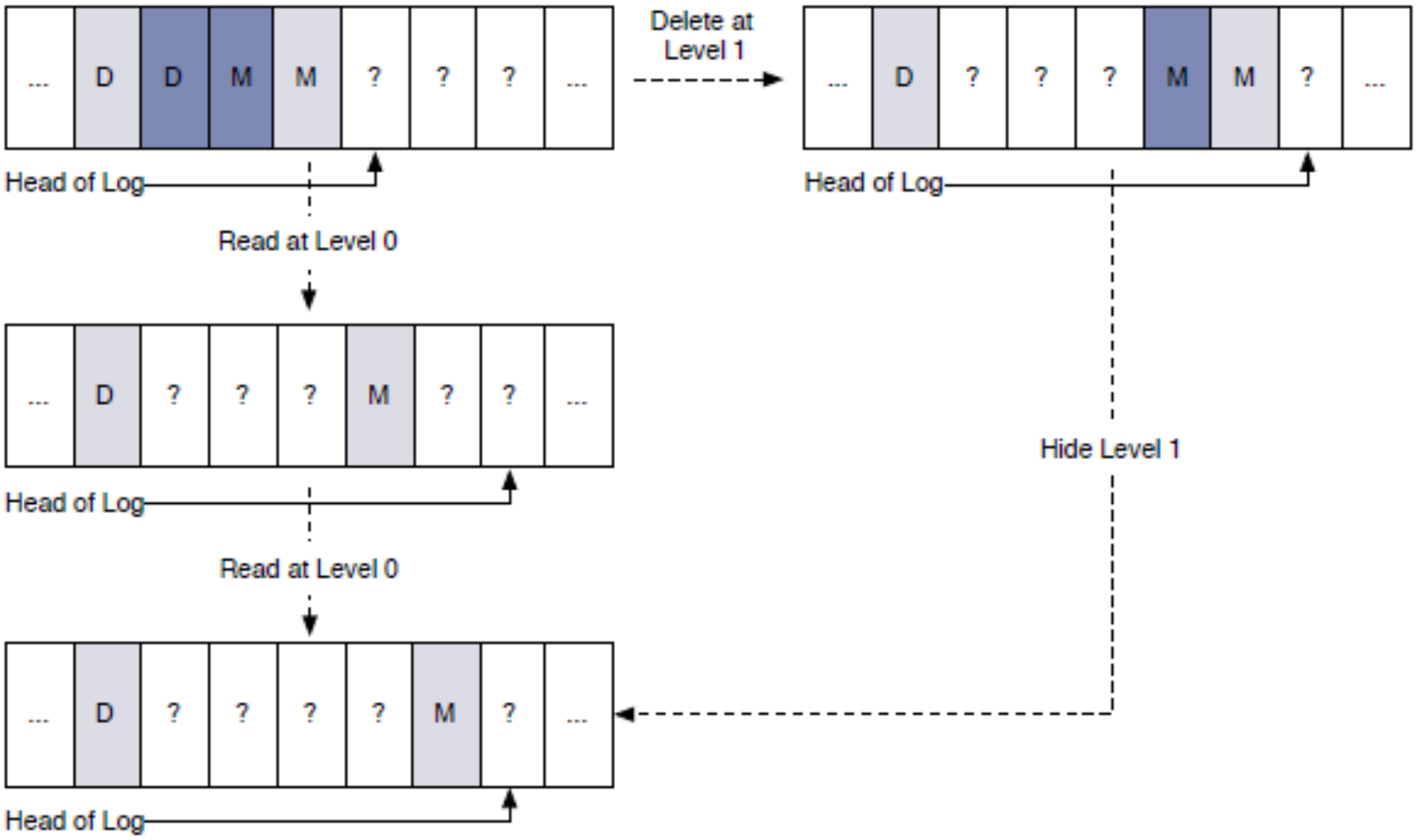
Figure 4.4: A multi-level view of the placeholder block order. The highest privilege level's block is written first and the lowest privilege level's block is written last.



(a) Reading a block.



(b) Writing a new block.



(c) Deleting a block.

Limitations of DEFY

- Information Leakage
  - Disk Level
    - Recent open files in geditor
    - Microsoft Word backup function
  - Memory Level
    - Cold boot attack
    - Scan memory to extract keys

References

1. A. D. McDonald and M. G. Kuhn. StegFS: A steganographic file system for Linux. In Information Hiding, pages 463–477. Springer, 2000.

2. A. Skillen and M. Mannan. On implementing deniable storage encryption for mobile devices. In 20th Annual Network and Distributed System Security Symposium, NDSS 2013, San Diego, California, USA, February 24-27, 2013

3. Bing Chang, Zhan Wang, Bo Chen, and Fengwei Zhang. MobiPluto: File System Friendly Deniable Storage for Mobile Devices, In Proceedings of The 2015 Annual Computer Security Applications Conference (ACSAC'15), Los Angeles, CA, December 2015.

Term Project Presentations

- Classes on Wednesday, Dec 09 and Monday, Dec 14

- 11:00am -13:40pm on Tuesday, Dec 15?