Amoeba: An Autonomous Backup and Recovery SSD for Ransomware Attack Defense

Donghyun Min[1], Donggyu Park[1], Jinwoo Ahn[1],
Ryan Walker[2], Junghee Lee[2], Sungyong Park[1], Youngjae Kim[1]

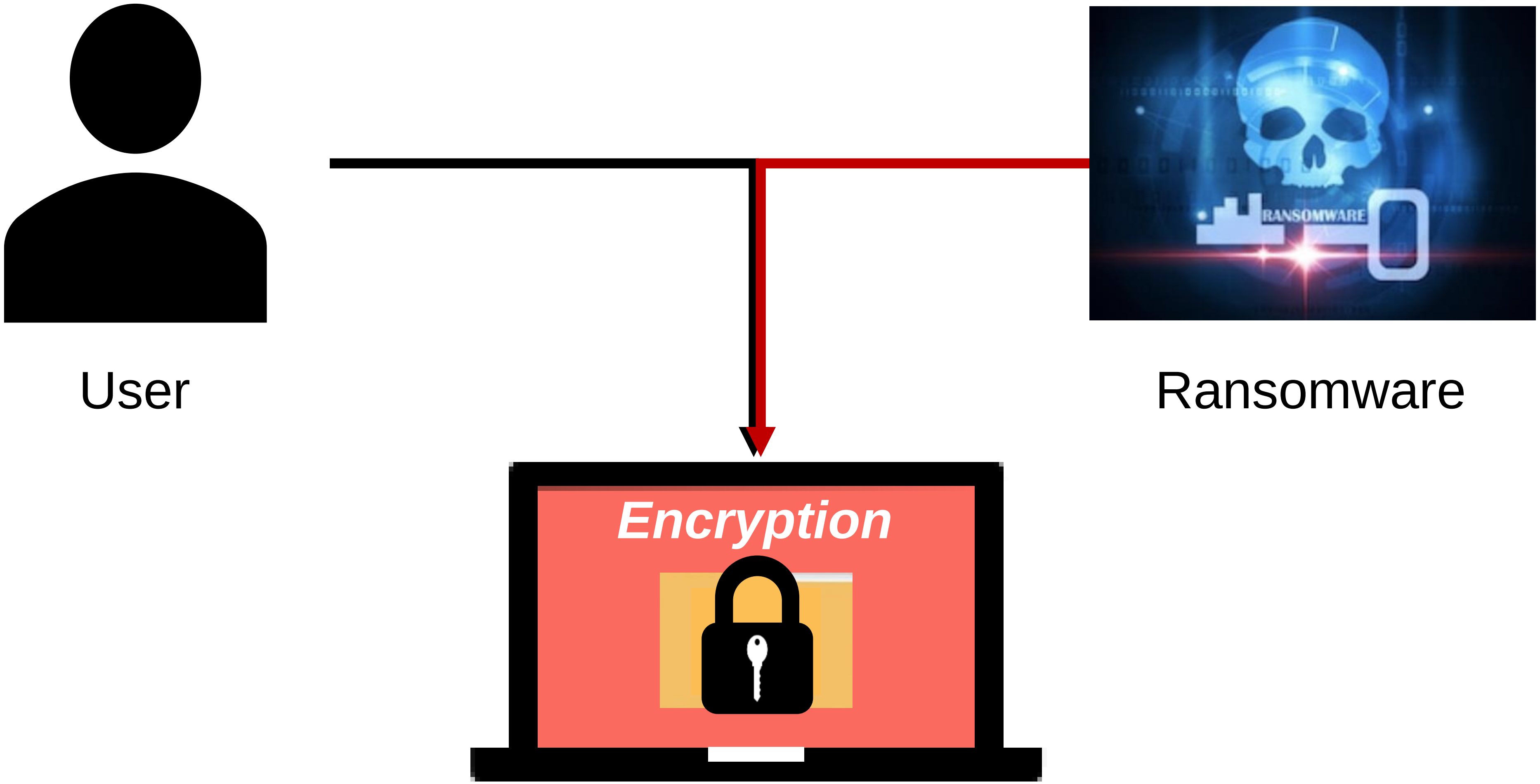
Presenter: Donghyun Min

Feb 19, 2019 @ HPCA'19

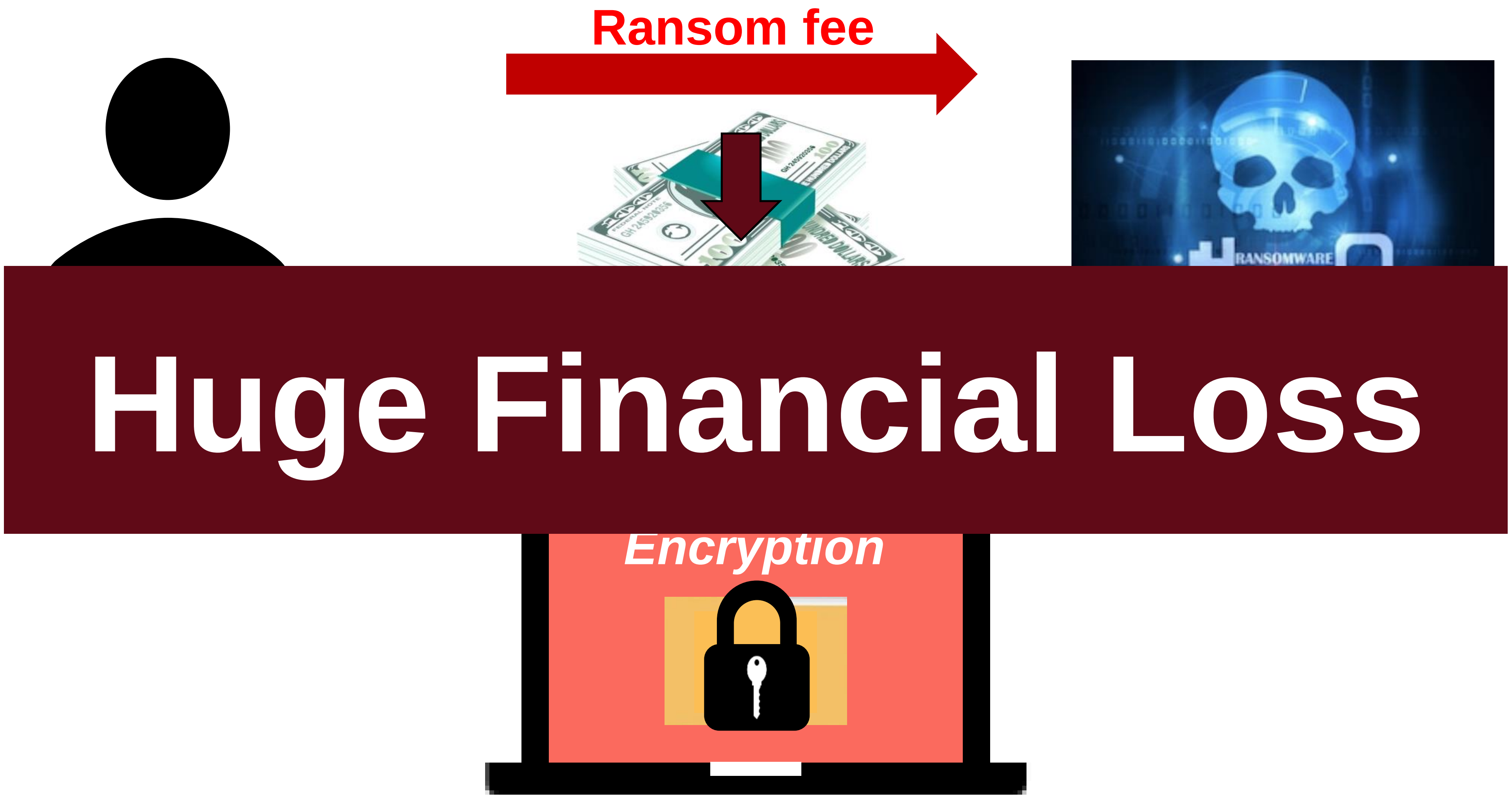
1 SOGANG UNIVERSITY

2 UTSA

Ransomware

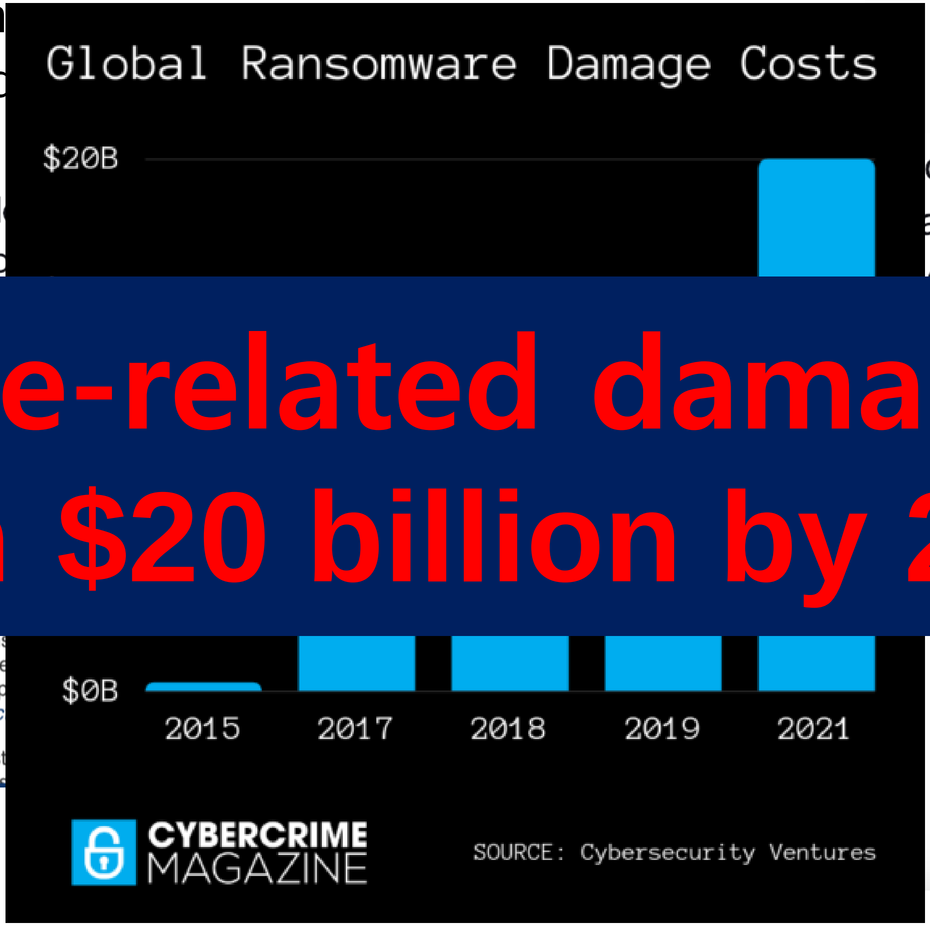


Ransomware



Damage of Ransomware Attack

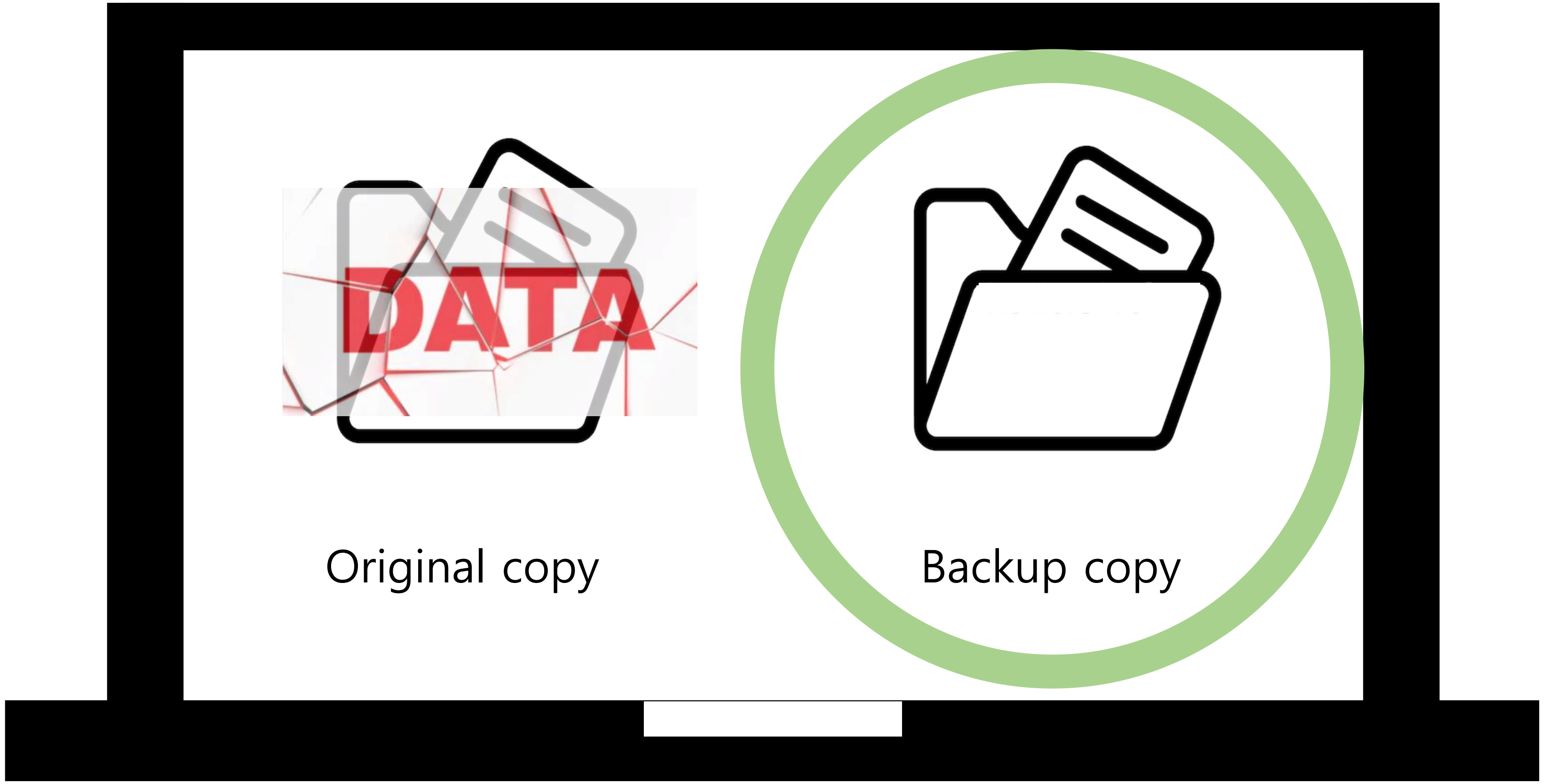
- Many areas are suffering from damage
  - Public institution
  - Government, inc



Ransomware-related damage cost will reach $20 billion by 2021!

How to Defend against Ransomware Attack

- Backup method



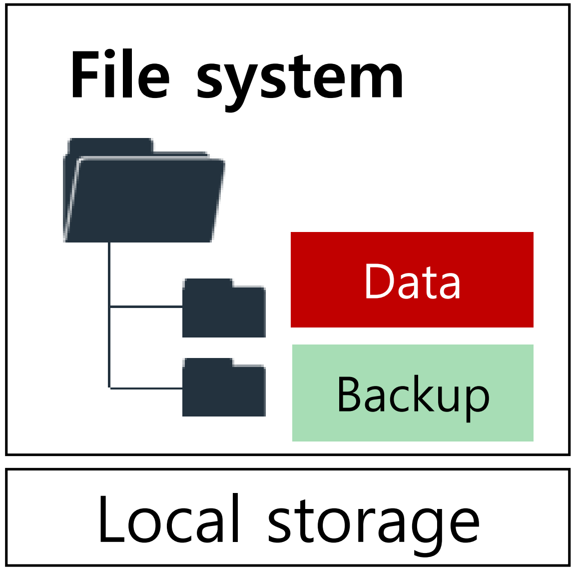
How to Defend against Ransomware Attack

- Approach 1: Host-level backup
  - Backup on Local File system
  - Backup on Remote machine

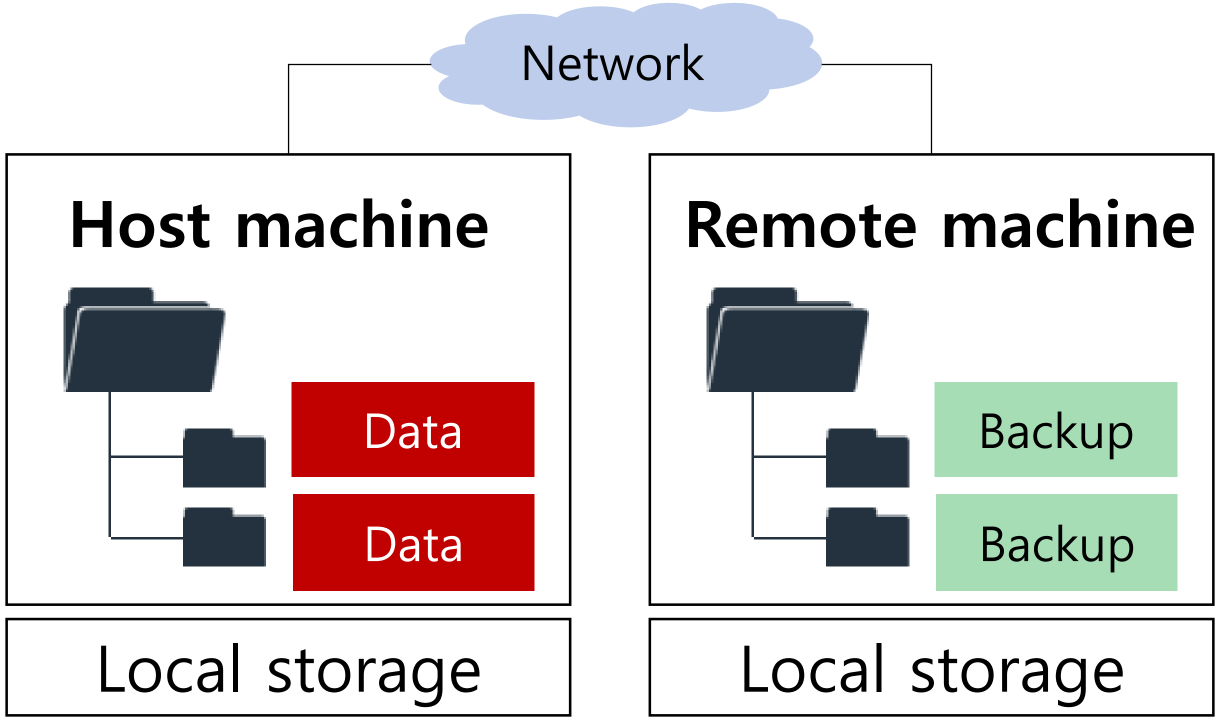
- Approach 2: Device-level backup
  - FlashGuard [CCS'17]
  - SSD-Insider [ICDCS'18]
  - Amoeba [CAL'18]

Approach 1: Host-level Backup

- Backup inside File system



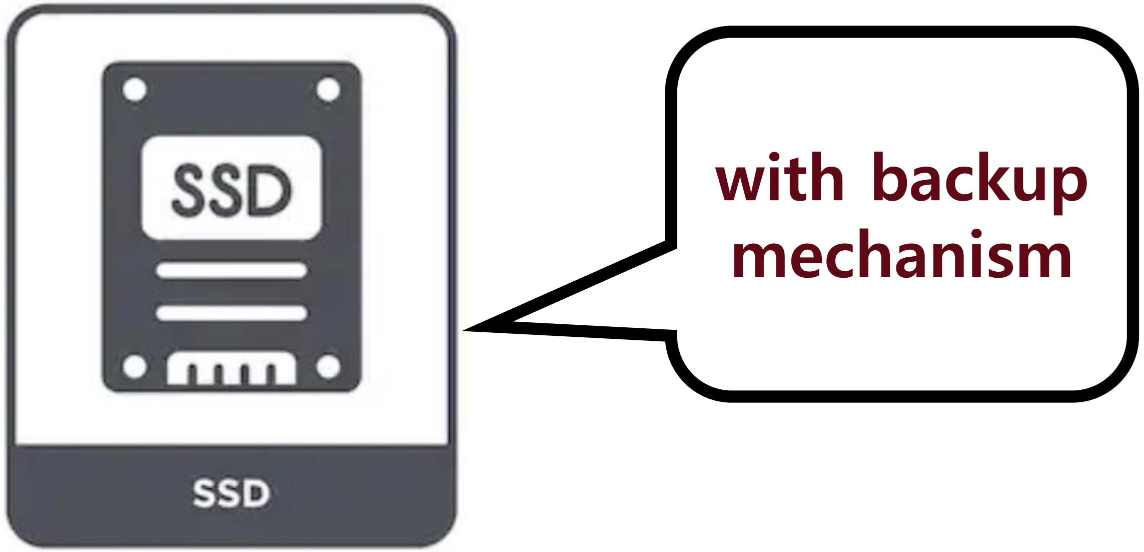
- Backup on Remote-machine



1. **Extra storage space is required.**
2. **Ransomware with kernel privilege can disable backup process.**

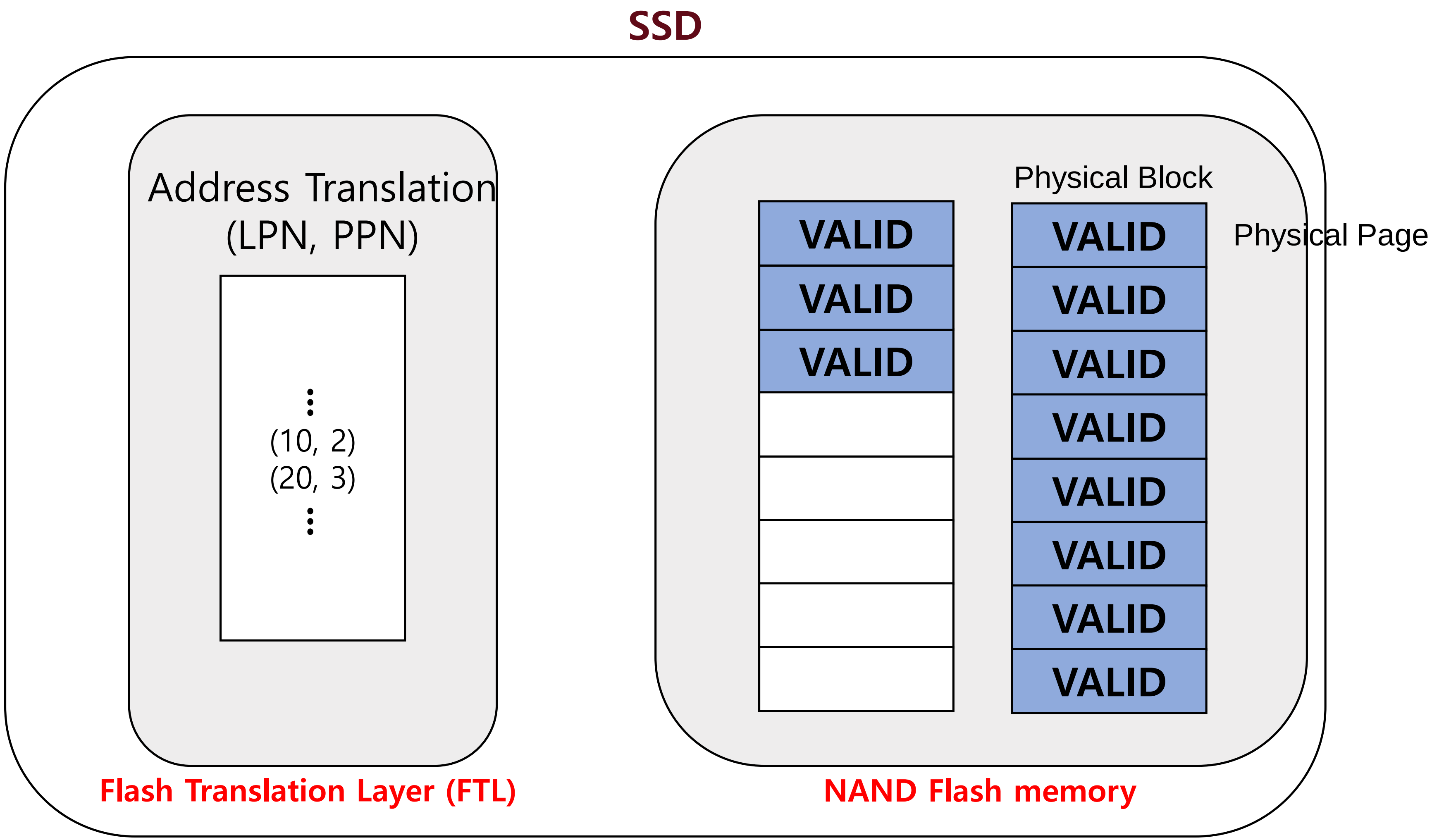
Approach 2: Device-level Backup

- FlashGuard [CCS'17]
- SSD-Insider [ICDCS'18]



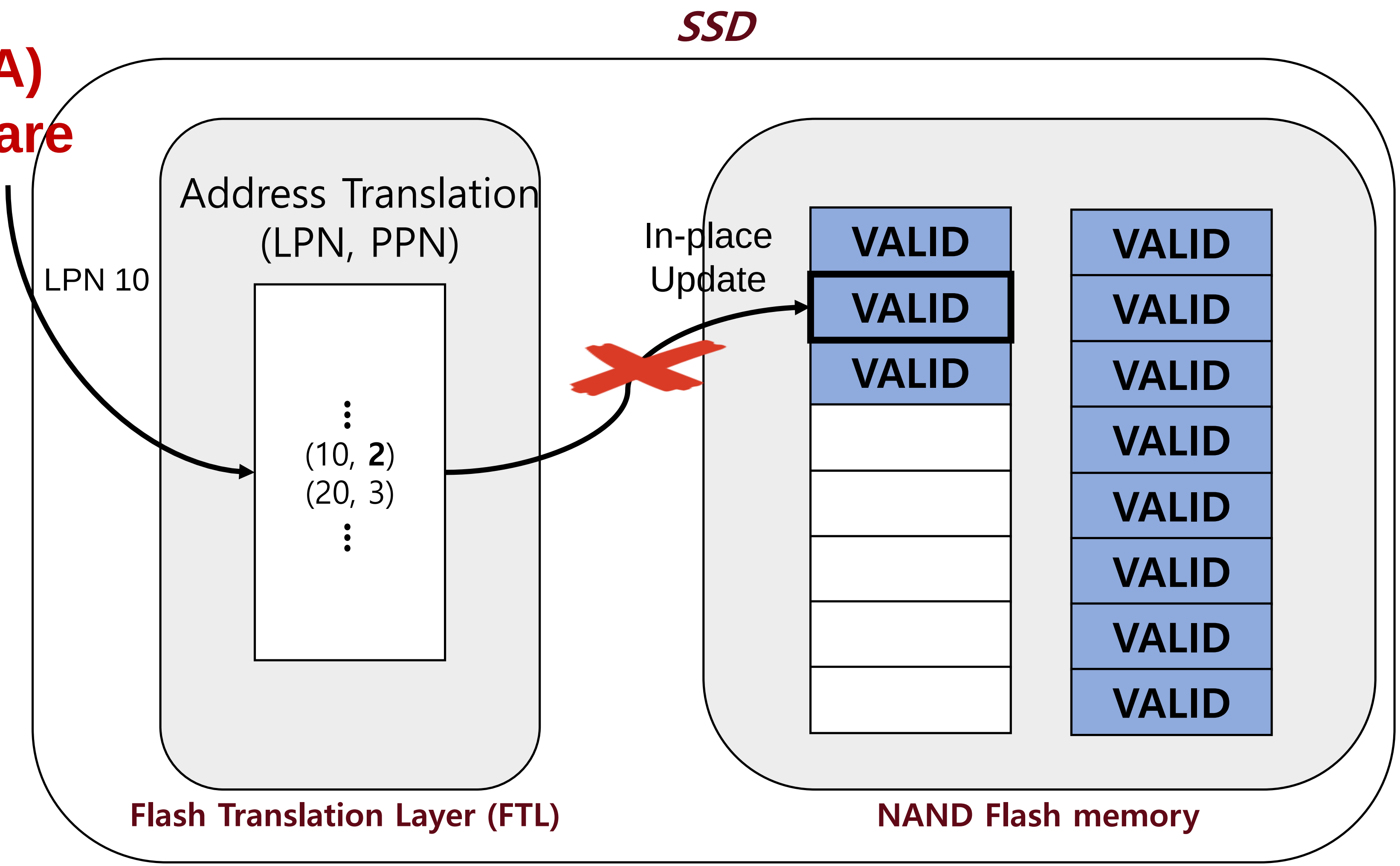
Out-of-place update

Opportunities: Out-of-Place Update in an SSD

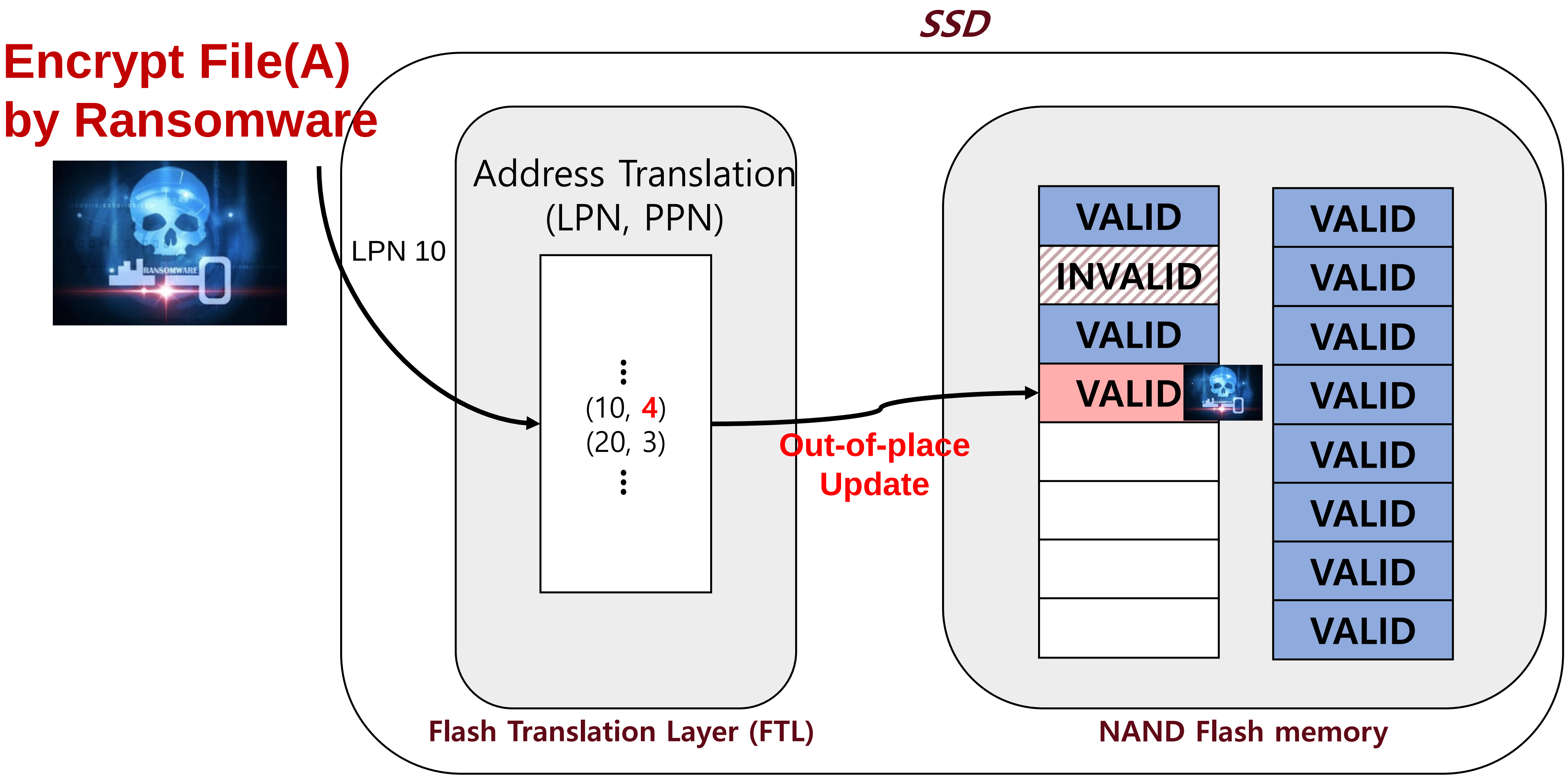


Opportunities: Out-of-Place Update in an SSD

Encrypt File(A)
by Ransomware



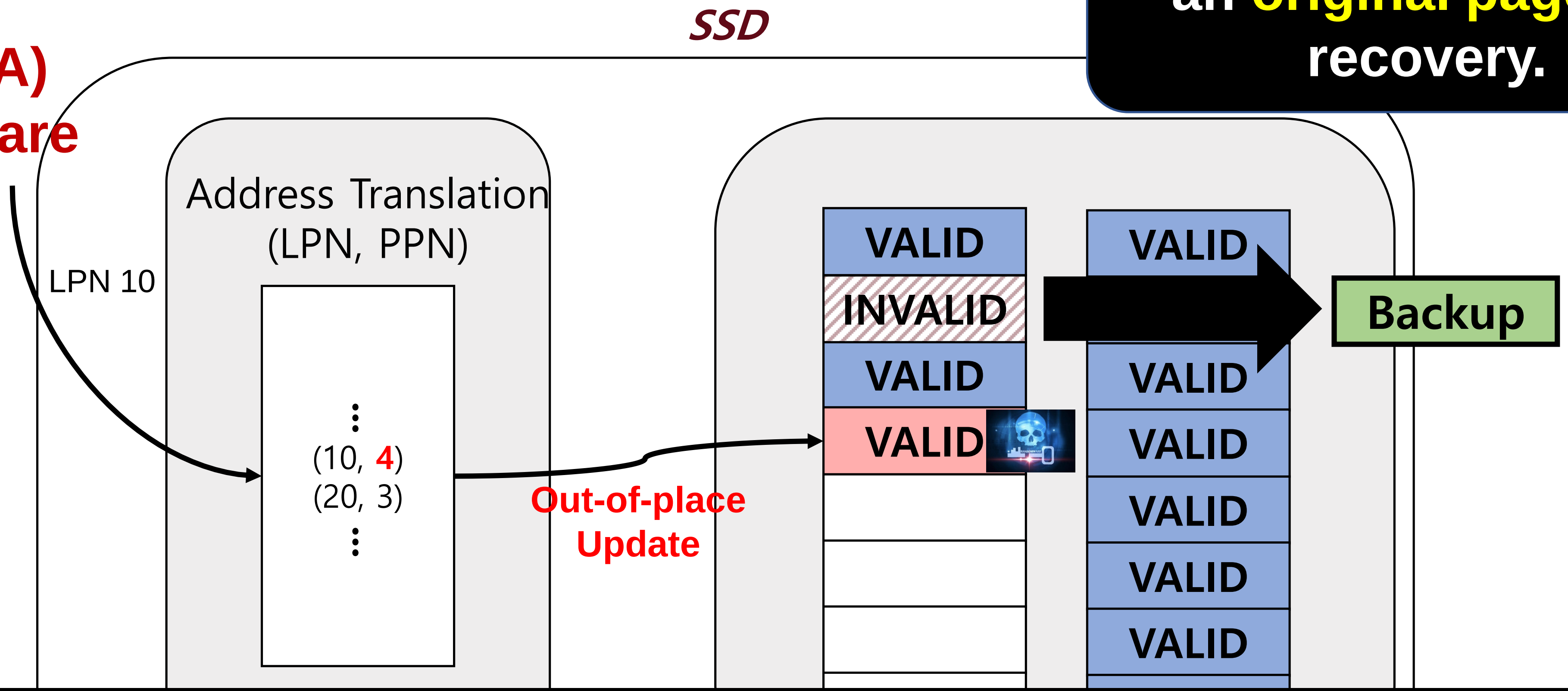
Opportunities: Out-of-Place Update in an SSD



Opportunities: Out-of-Place Update in an SSD

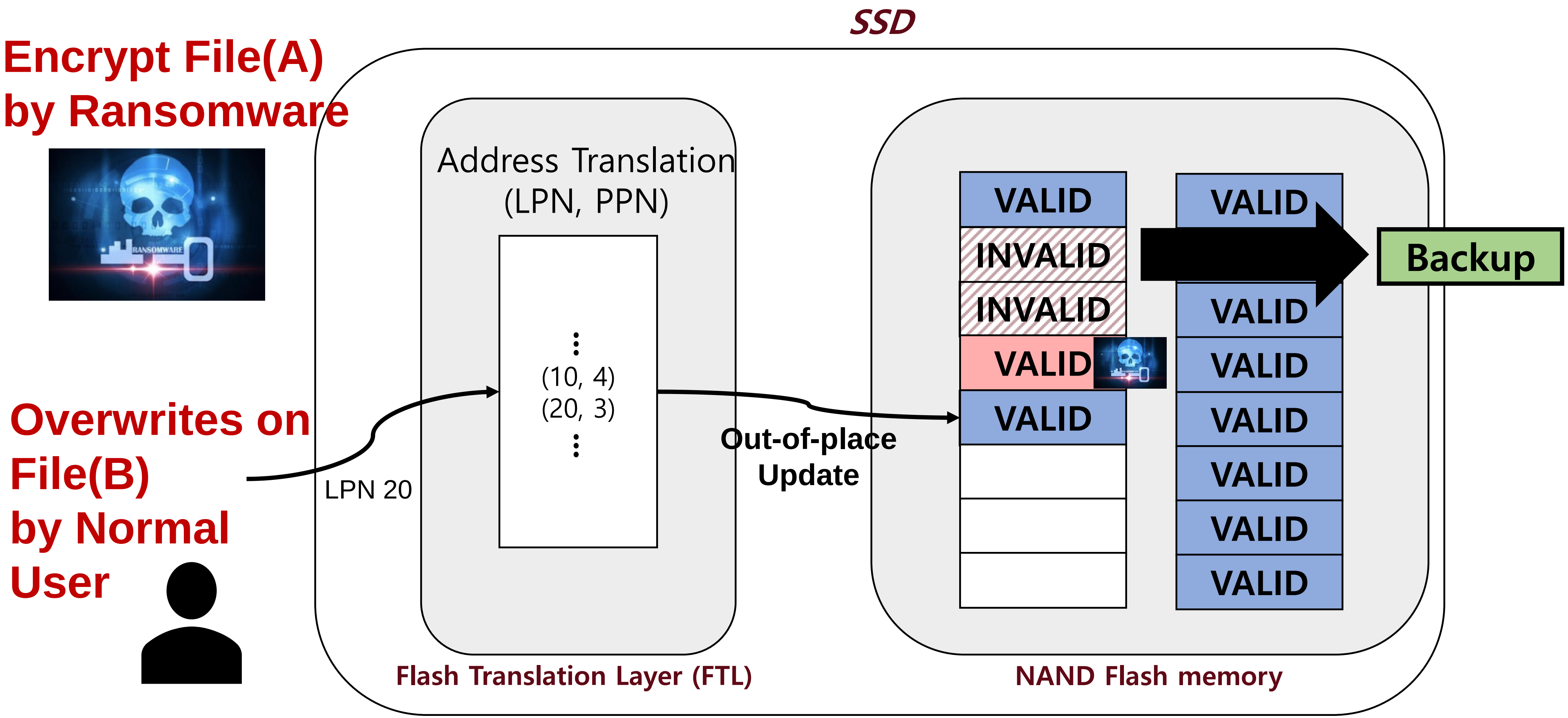
Invalid page is actually an **original page** for recovery.

Encrypt File(A) by Ransomware



1. We can save storage space for backup because **additional backup space is not required.**
2. Device-level backup can become more secure because **backup copy cannot be seen from ransomware application.**

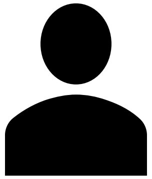
Challenges

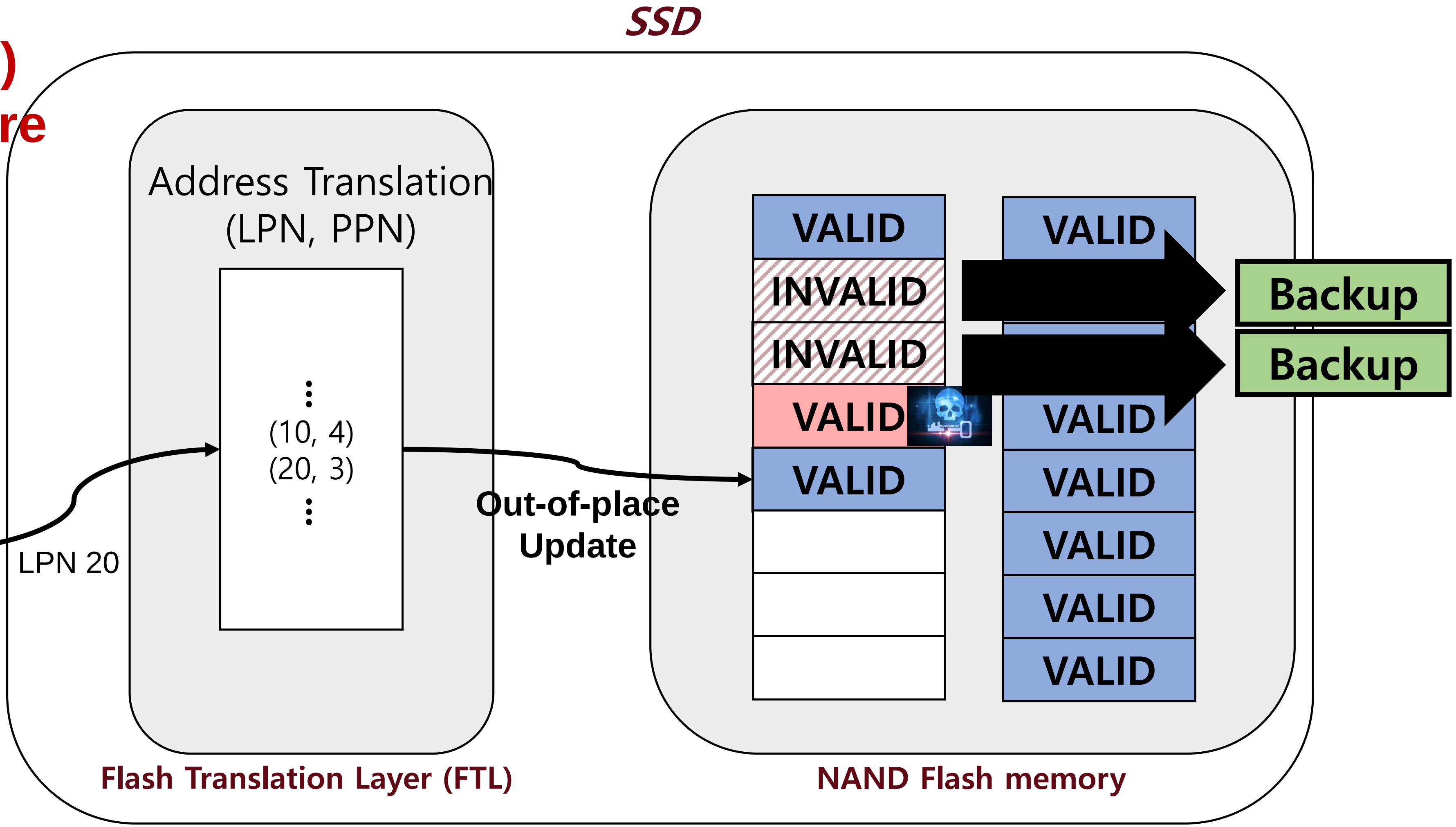

SSD
Encrypt File(A)
by Ransomware
Address Translation
(LPN, PPN)
(10, 4)
(20, 3)
VALID
INVALID
INVALID
VALID
VALID
VALID
VALID
VALID
VALID
VALID
VALID
VALID
Backup
Overwrites on
File(B)
by Normal
User
LPN 20
Out-of-place
Update
Flash Translation Layer (FTL)
NAND Flash memory

Challenges

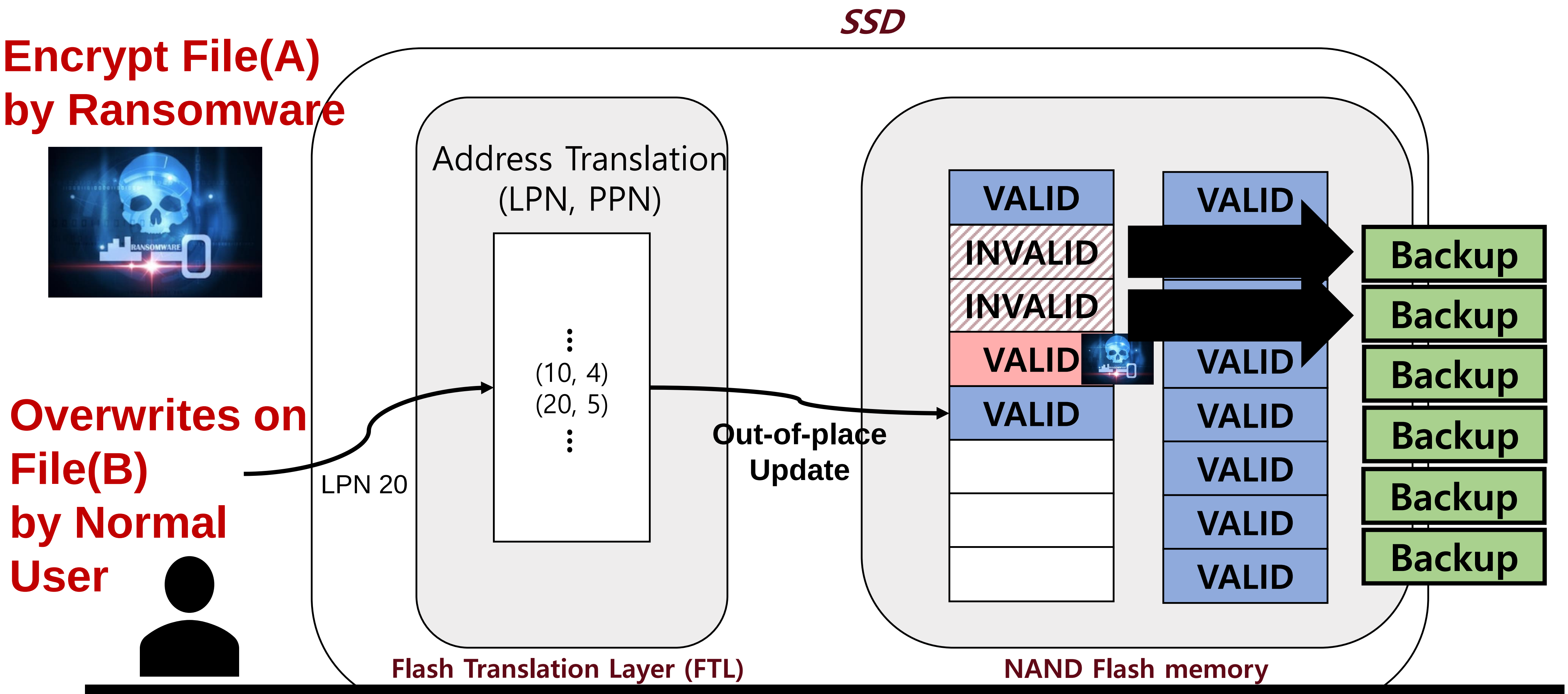
Encrypt File(A) by Ransomware

Overwrites on File(B) by Normal User





Challenges



SSD should keep invalid pages as backup only for updates by ransomware.

Summary: Limitations of Previous Works [CCS'17, ICDCS'18]

1. Lack of accurate ransomware detection algorithms

- Detection solely relies on I/O access pattern (e.g., Write Intensity)

➔ *False Positive (FP)* ➔ *GC overhead*

➔ *False Negative (FN)* ➔ *Recovery failure*

Summary: Limitations of Previous Works [CCS'17, ICDCS'18]

1. Lack of accurate ransomware detection algorithms

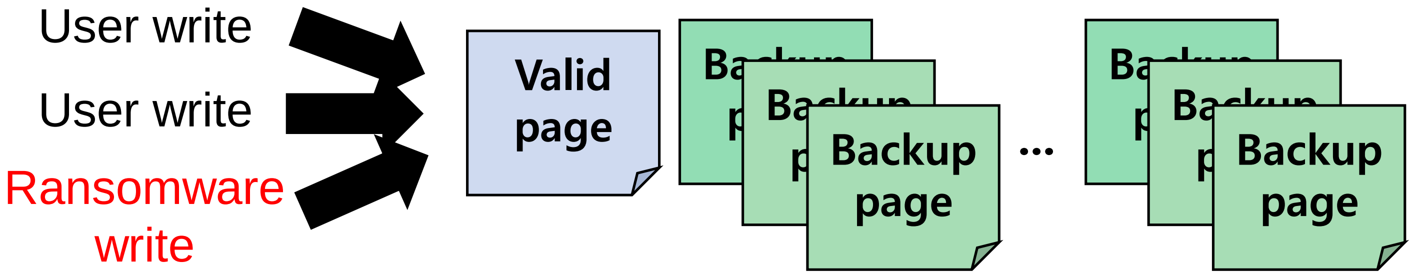
- Detection solely relies on I/O access pattern (e.g., Write Intensity)

➔ *False Positive (FP)* ➔ *GC overhead*

➔ *False Negative (FN)* ➔ *Recovery failure*

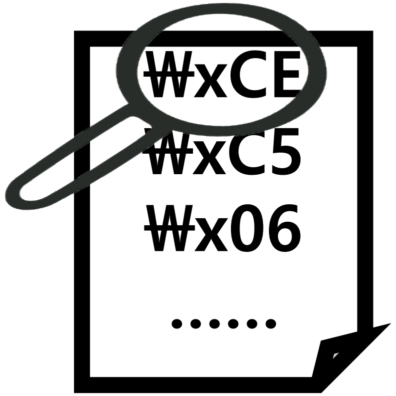
2. High unnecessary space overhead due to lack of intelligent backup mechanisms

- Unnecessary backup pages increase GC overhead.



Our Approach [Amoeba, CAL'18]

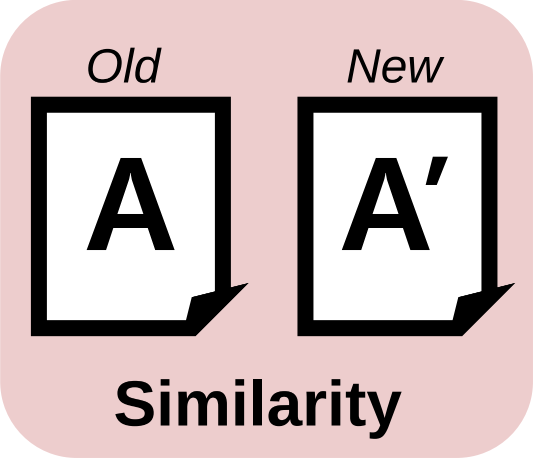
1. We use a content-based detection technique for high ransomware detection rate.

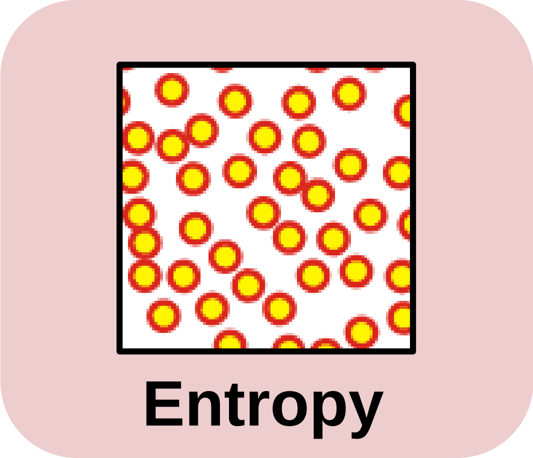


2. We implement an intelligent backup management mechanism to minimize space overhead for backup pages.

Challenge 1: How to Apply Content-based Detection at High Speed

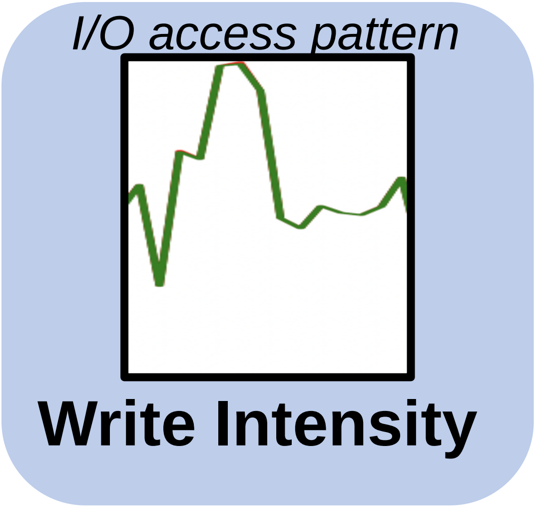
- Content-based detection offers high ransomware detection rate, but, it is highly time-consuming because it requires huge computation power for old and new comparison for similarity and entropy computation.

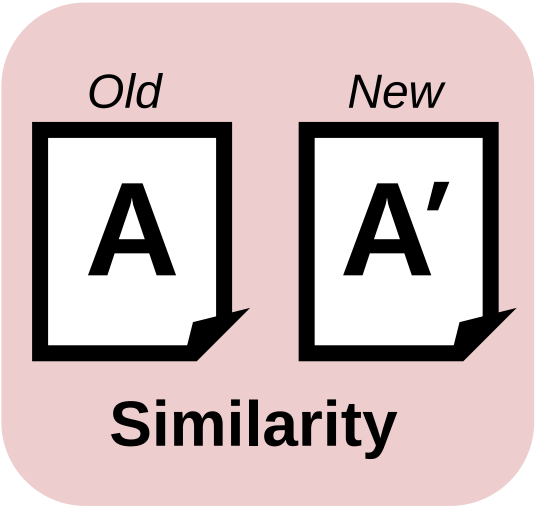


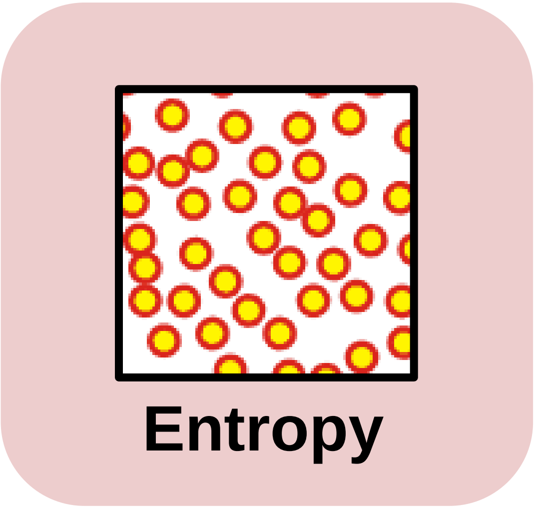


Challenge 2: How Accurately Detect Ransomware Attack

- Ransomware detection algorithm needs to be developed by considering three indicators all together should be required for high detection rate.



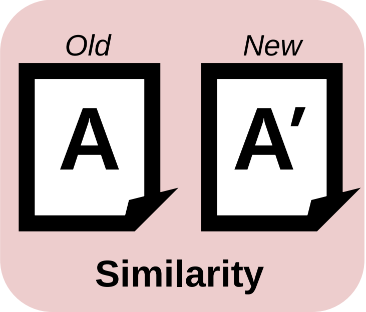


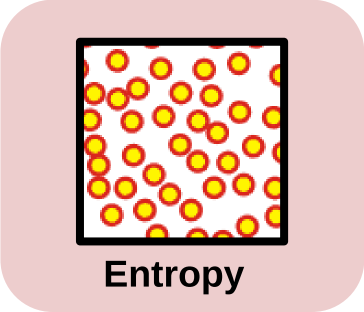


Challenge 2: How Accurately Detect Ransomware Attack

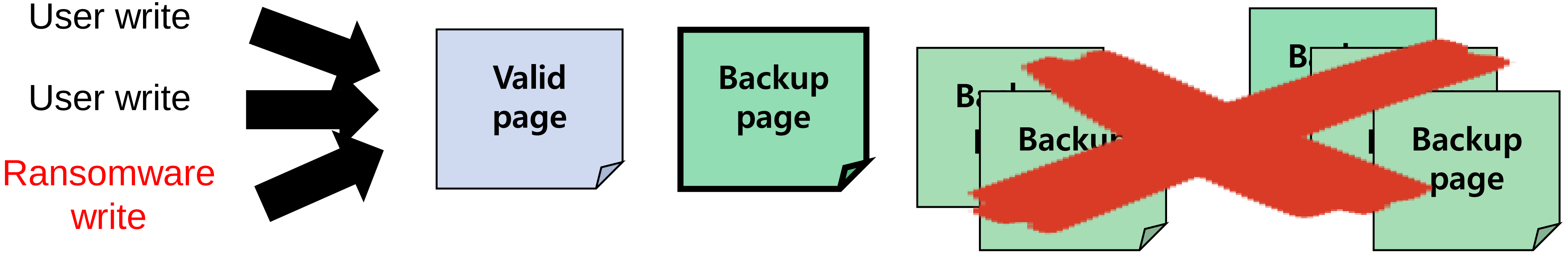
- If only Write Intensity is used, it often misjudge normal requests and ransomware attacks.

- If only Similarity and Entropy are used, it cannot distinguish legitimate encryption applications using compression and PGP cryptographic library from ransomware attacks.





Challenge 3: How to Minimize Backup Space Overhead

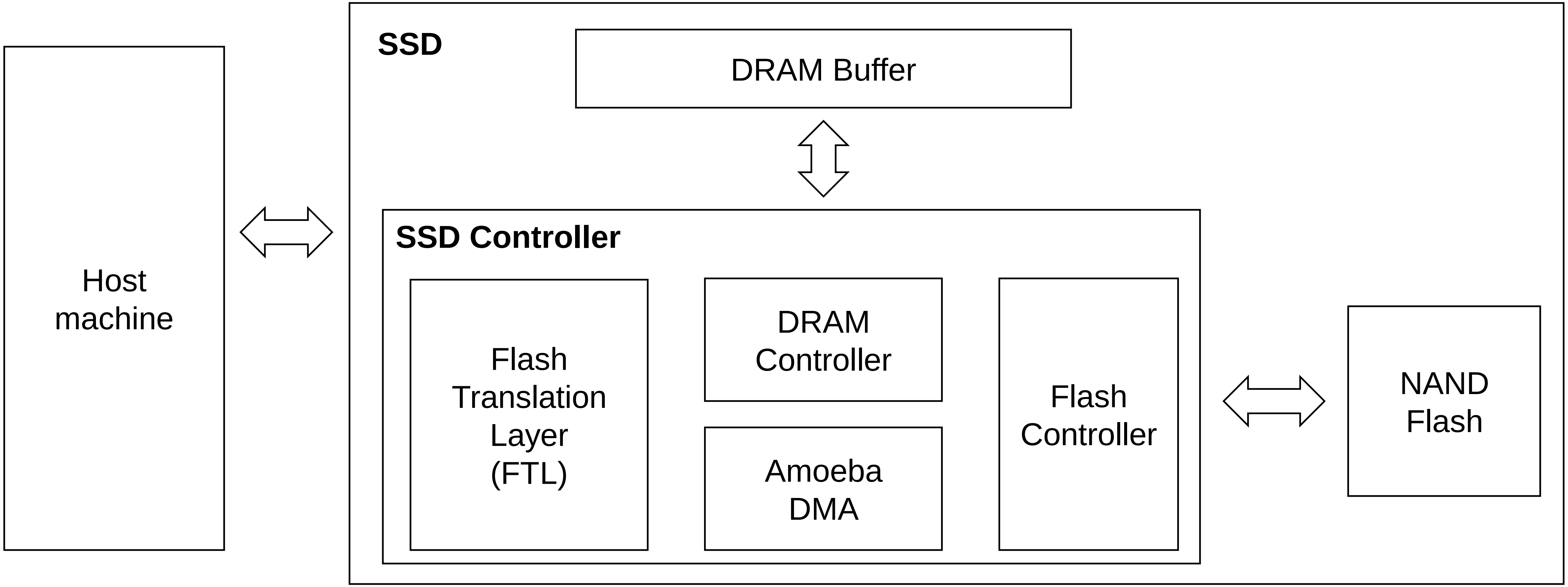


We should be able to identify only necessary backup pages for recovery among backup pages.

Amoeba:

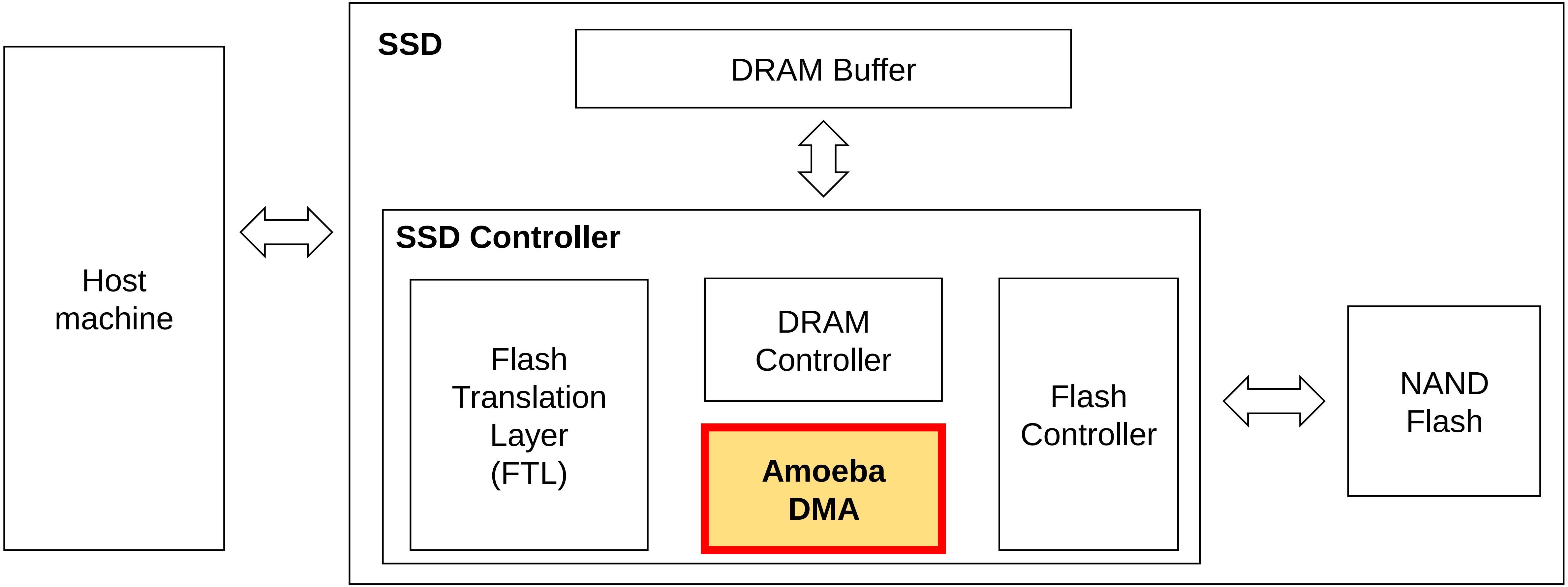
An Autonomous Backup and Recovery SSD for Ransomware Attack Defense

Amoeba System Architecture



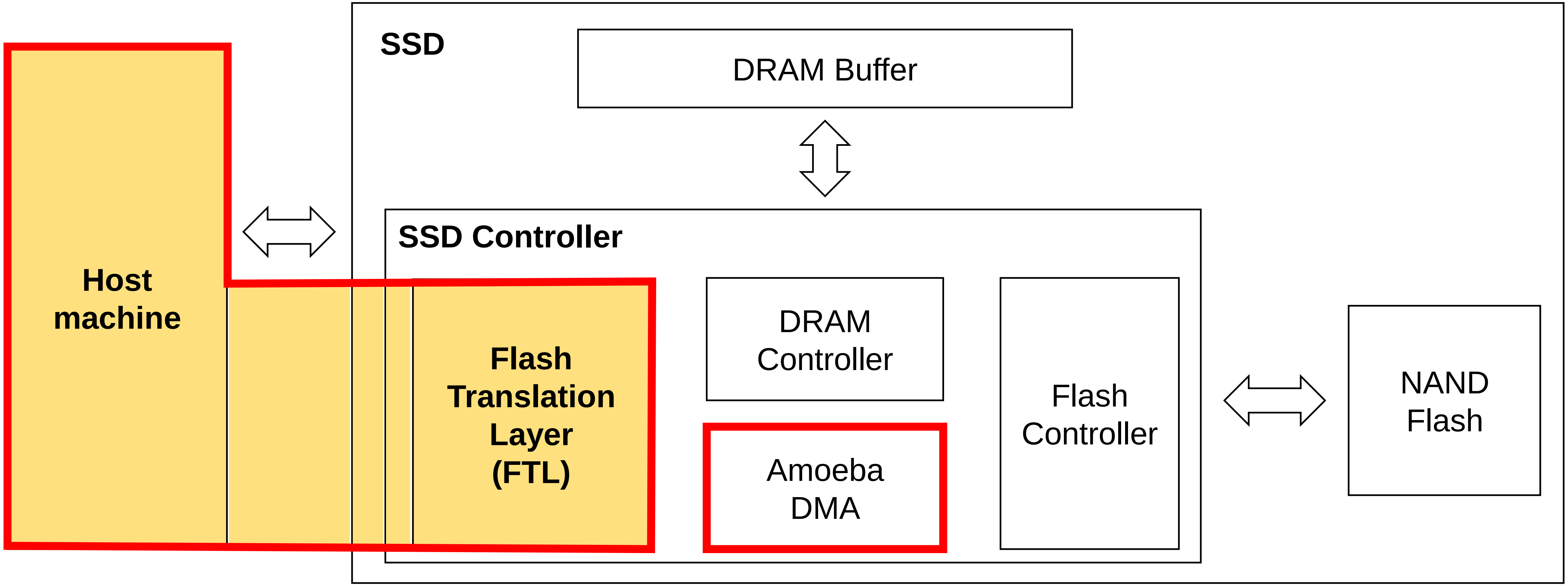
Amoeba System Architecture

- Amoeba DMA



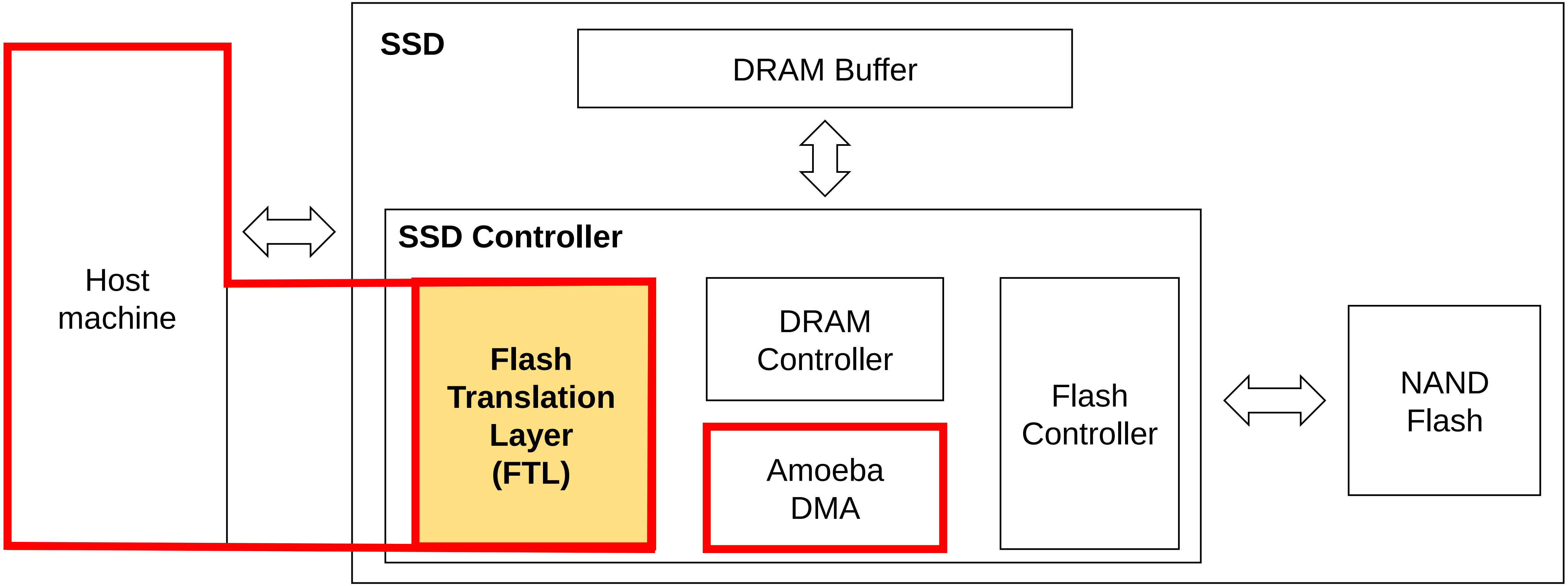
Amoeba System Architecture

- Ransomware Attack Risk Indicator (RARI)



Amoeba System Architecture

- Intelligent Backup Mechanism

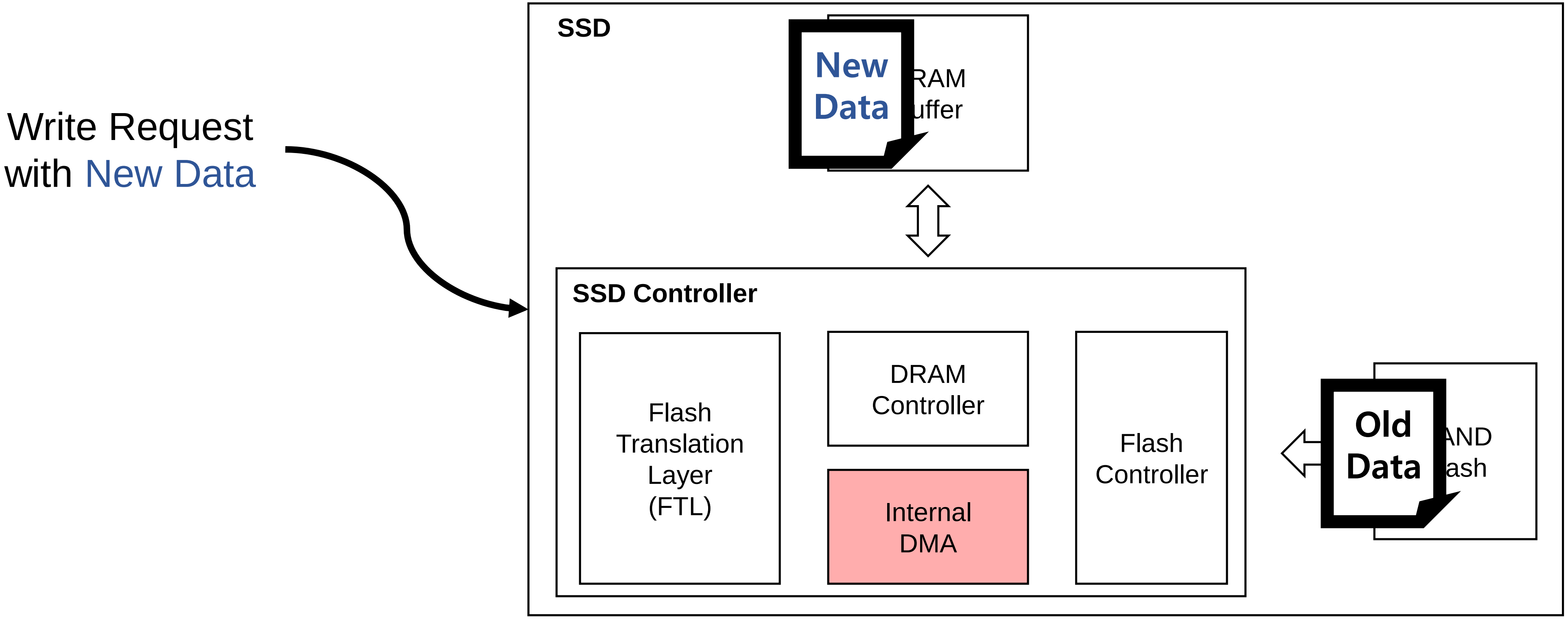


1. Amoeba DMA Engine

- Amoeba DMA engine for computing similarity, entropy

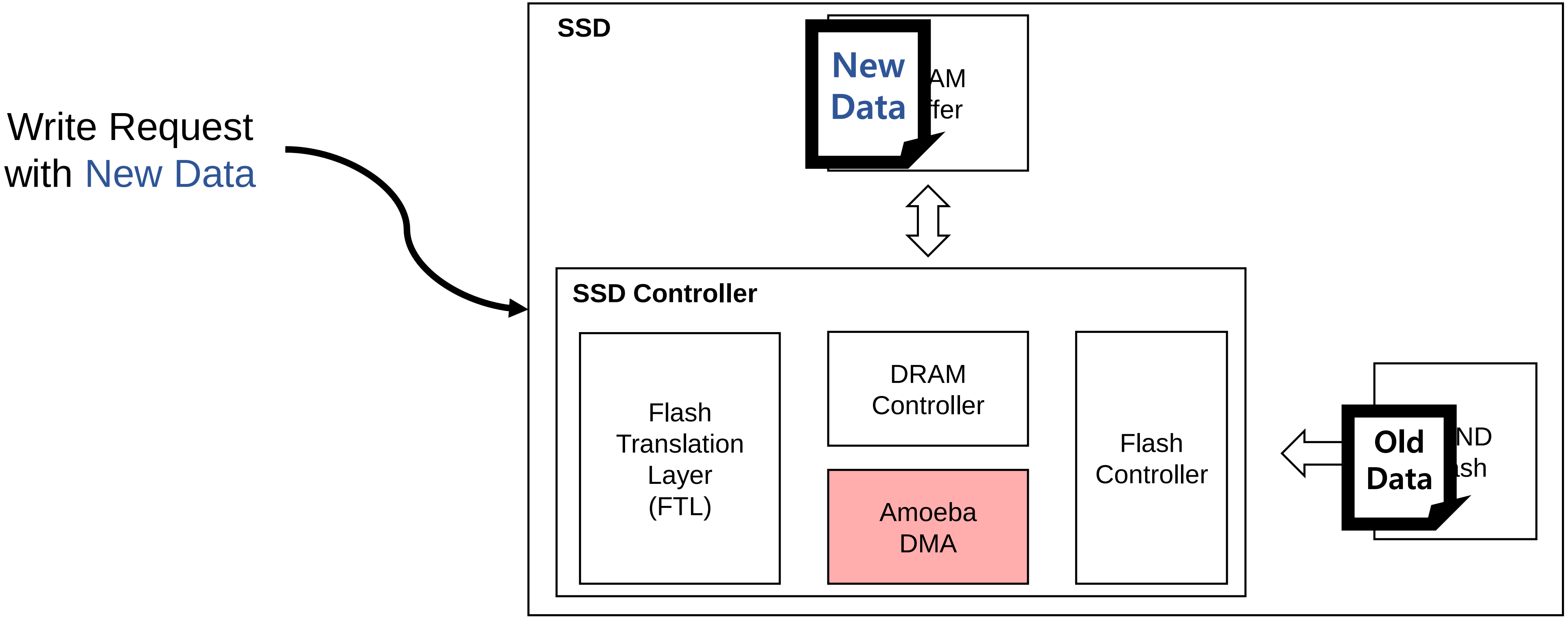
1. Amoeba DMA Engine

- Amoeba DMA engine for computing similarity, entropy
  - Basic DMA (Existing DMA)



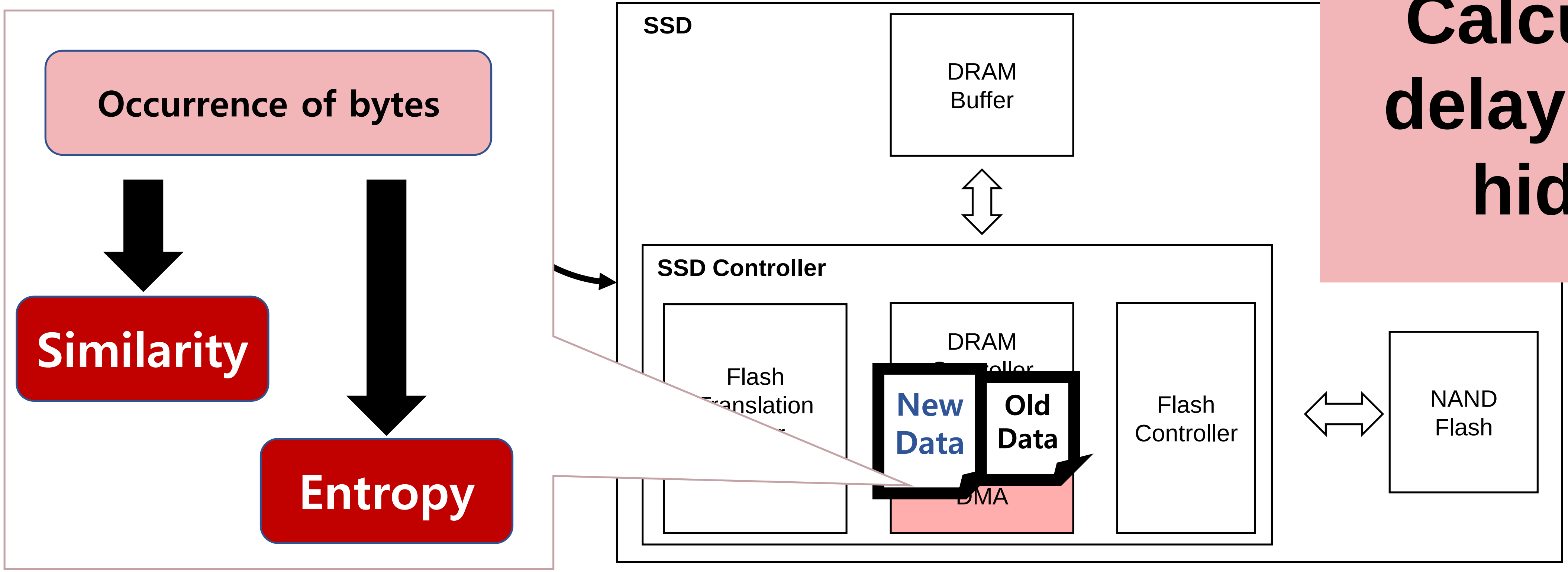
1. Amoeba DMA Engine

- Amoeba DMA engine for computing similarity, entropy
  - Basic DMA (Existing DMA)
  - Amoeba DMA



1. Amoeba DMA Engine

- Amoeba DMA engine for computing similarity, entropy
  - Basic DMA (Existing DMA)
  - Amoeba DMA



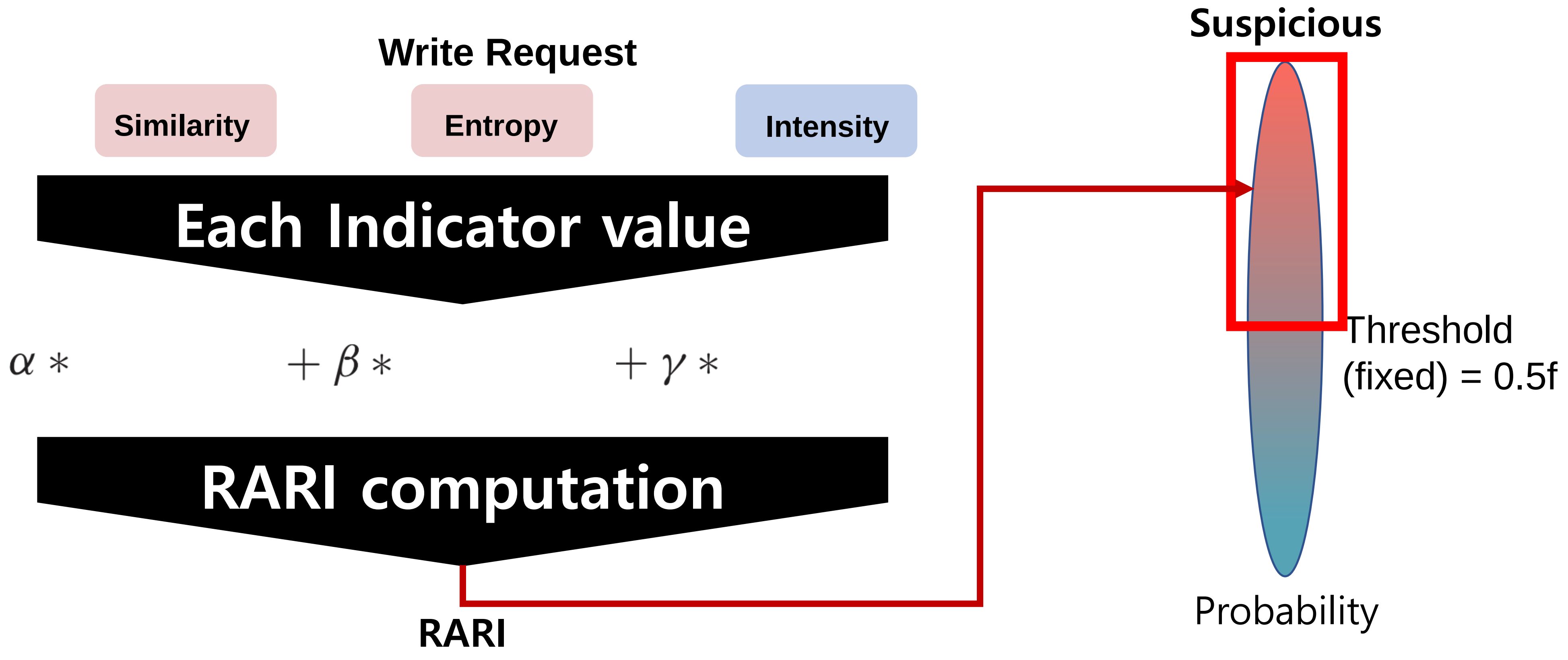
Calculation delay can be hidden.

2. Ransomware Attack Risk Indicator (RARI)

- We establish a model that combines three indicators (write intensity, similarity, and entropy) to form a RARI value.

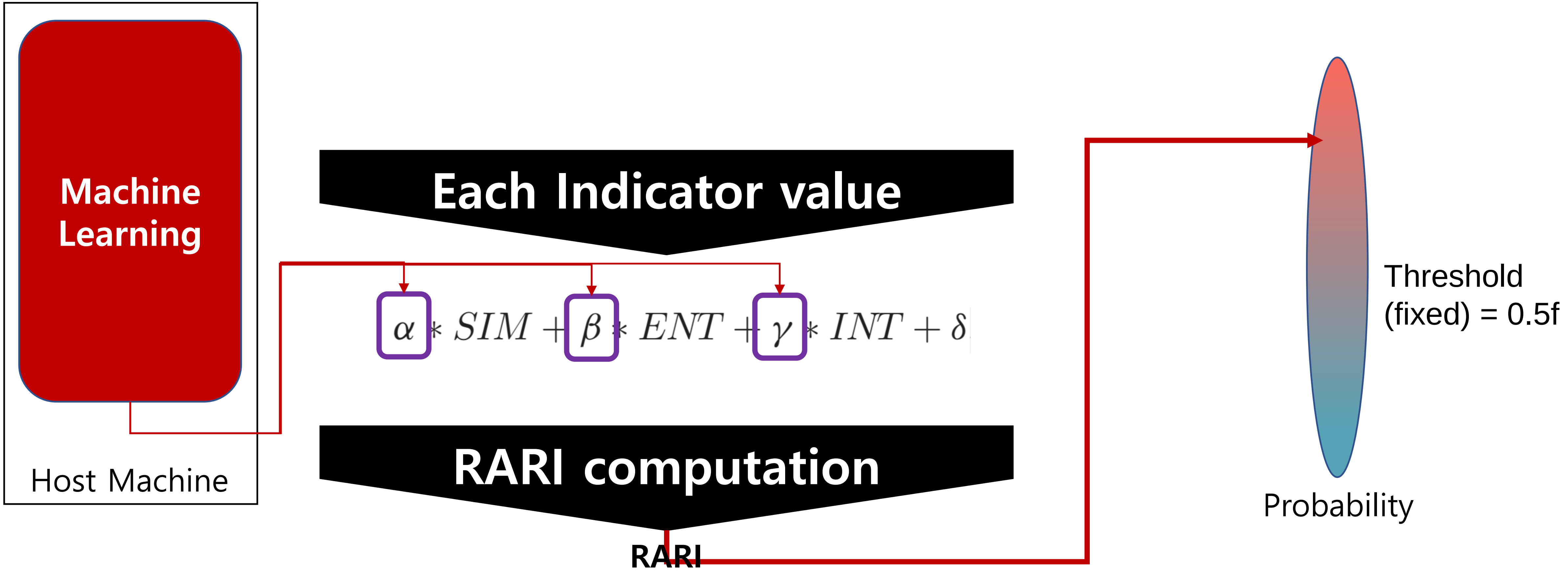
2. Ransomware Attack Risk Indicator (RARI)

- We establish a model that combines three indicators (write intensity, similarity, and entropy) to form a RARI value.



2. Ransomware Attack Risk Indicator (RARI)

- We establish a model that combines three indicators (write intensity, similarity, and entropy) to form a RARI value.

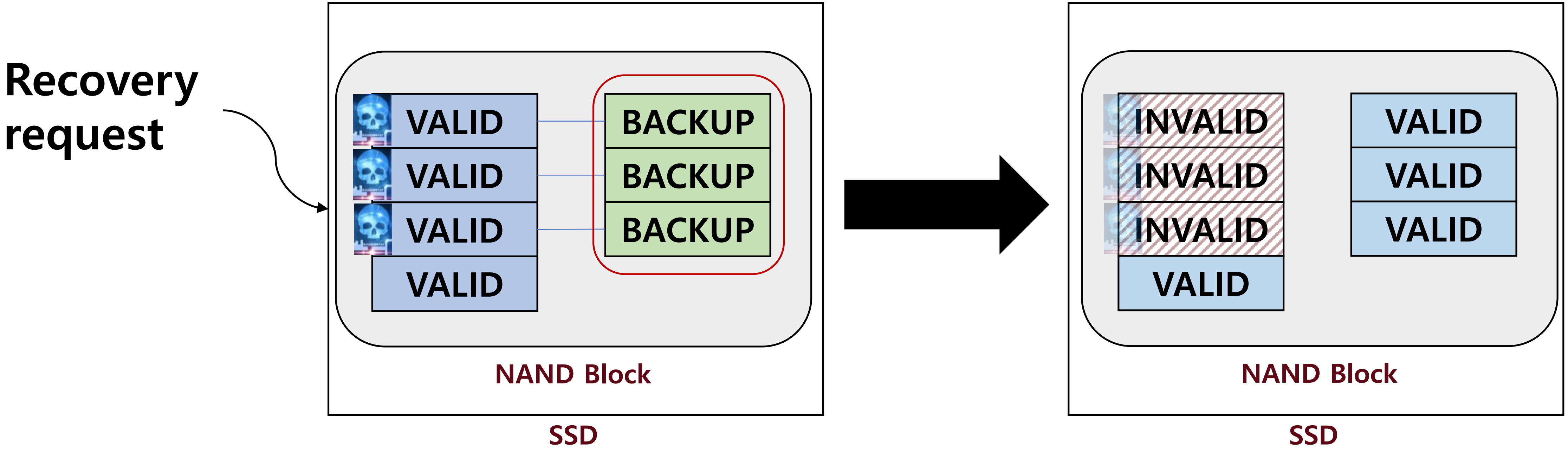


3. Intelligent Backup Control Mechanism

- We can accurately detect backup pages using RARI values. Thus, we can only maintain a backup page per logical page.

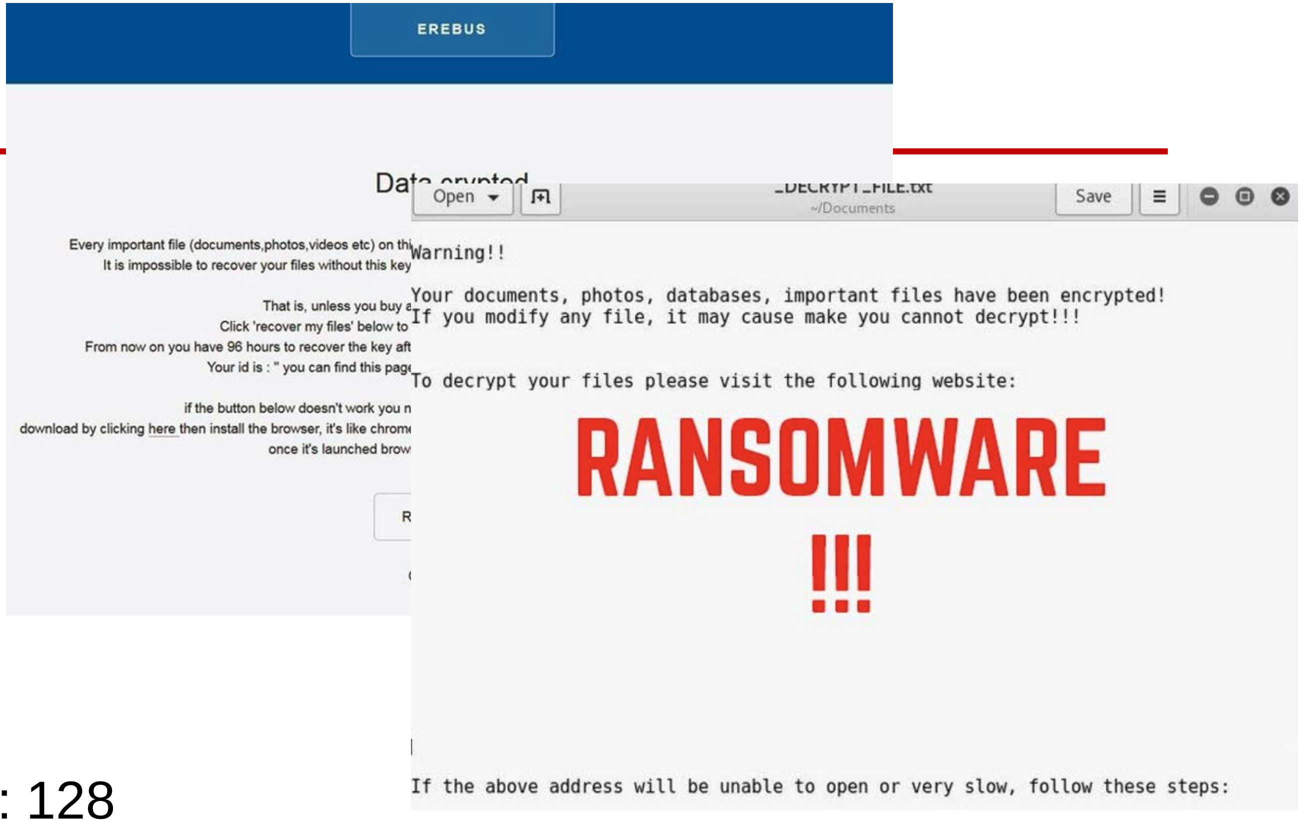
We can completely go away unnecessary backup pages in an SSD.

- Recovery Procedure

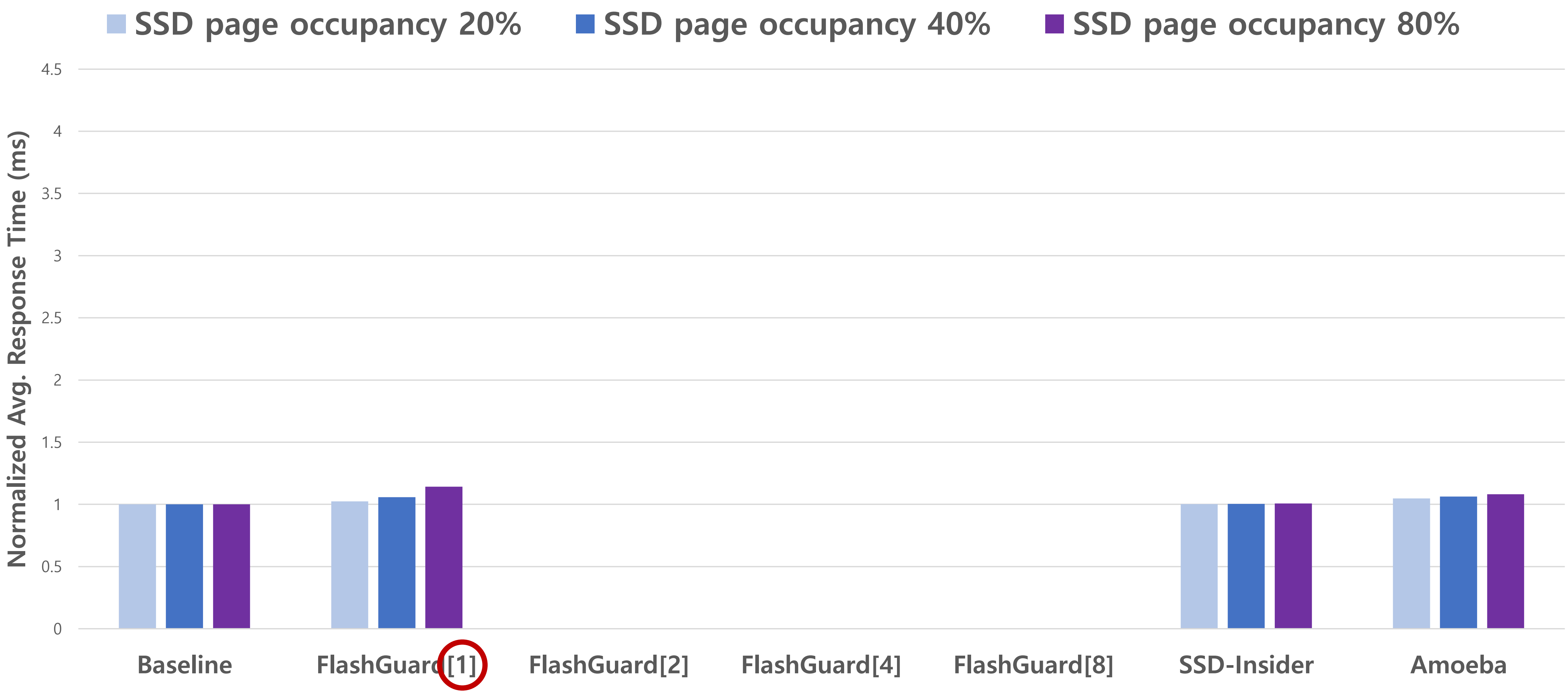


Evaluation Methodology

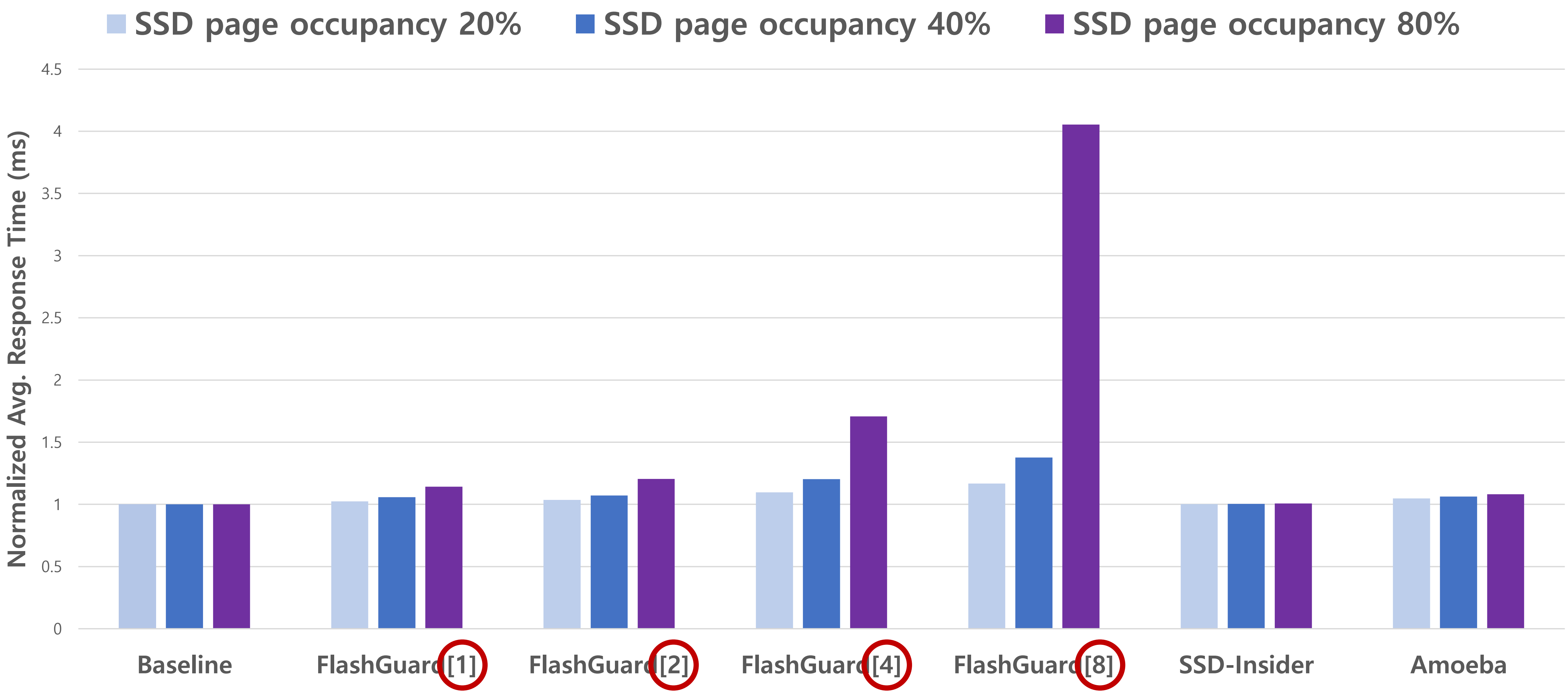
- MSR Disksim SSD Simulator
- Workload
  - Linux Erebus ransomware
  - User’s normal I/O
- Simulation setup
  - SSD Occupancy: 20%, 40%, 80%
  - Page Size: 8 KB, # of page per block: 128
- Comparison
  - Baseline: SSD without backup mechanism
  - FlashGuard
  - SSD-Insider
  - Amoeba



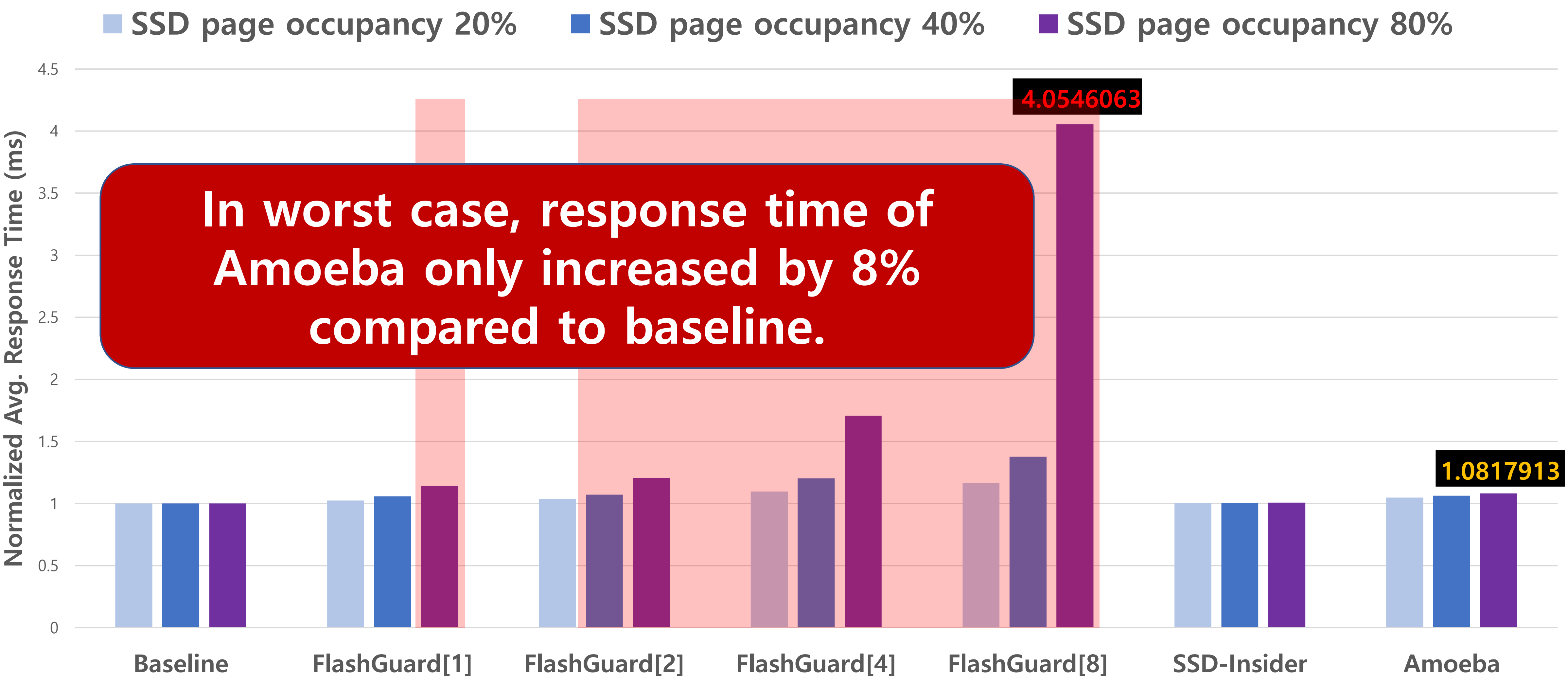
Result 1: Average Response Time



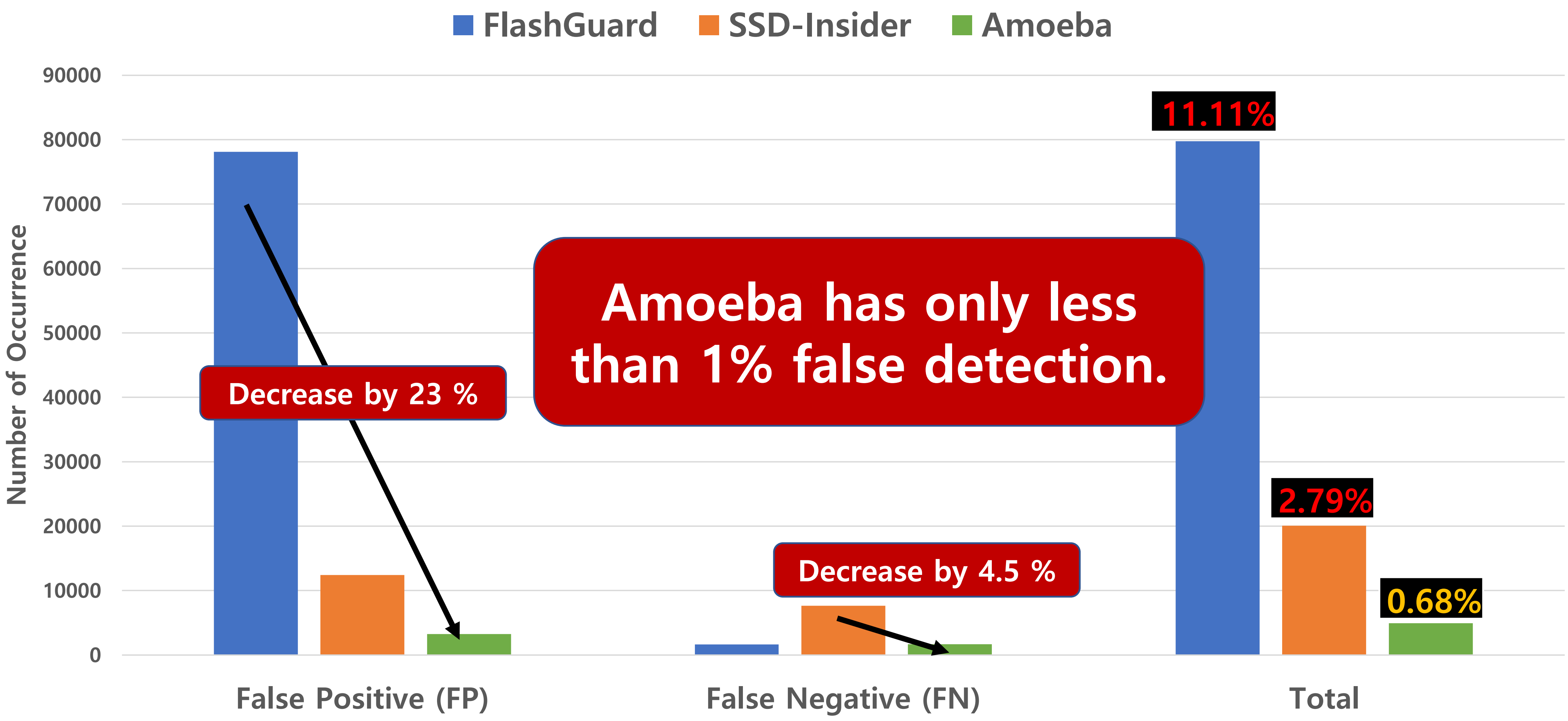
Result 1: Average Response Time



Result 1: Average Response Time

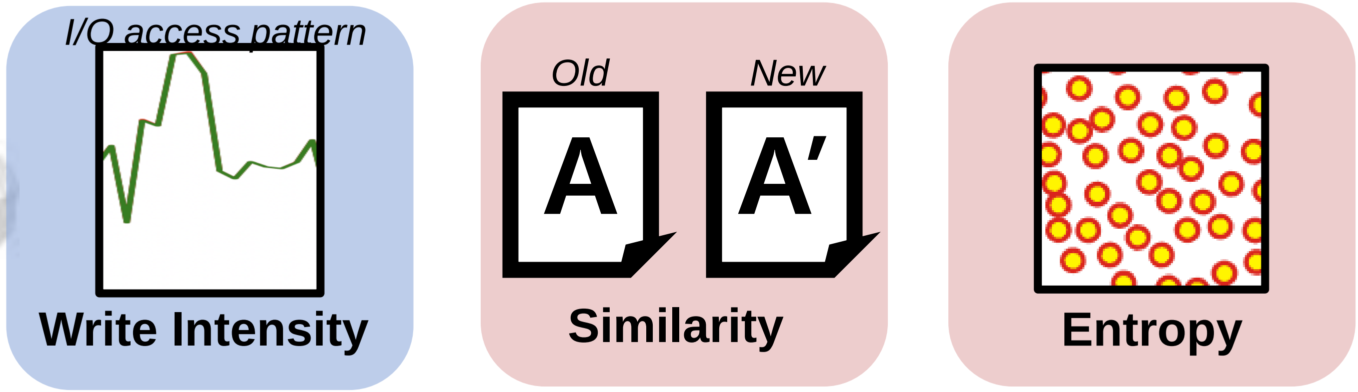


Result 2: Detection Accuracy



Conclusion

- We presented Amoeba: An Autonomous Backup and Recovery SSD for Ransomware Attack Defense.
  - Implemented Amoeba DMA Hardware engine to compute content-based detection algorithm.
  - Proposed a Ransomware Attack Risk Indicator (RARI) metric.
  - Provided Intelligent Backup and Recovery mechanism.



Thank you
Q & A

Donghyun Min

mdh38112@sogang.ac.kr

Sogang University, South Korea

Backup slides 1: GC Calls