# CS 5472 - Advanced Topics in Computer Security

## Topic 5: Deniable Encryption (2)

Spring 2018 Semester

Instructor: Bo Chen

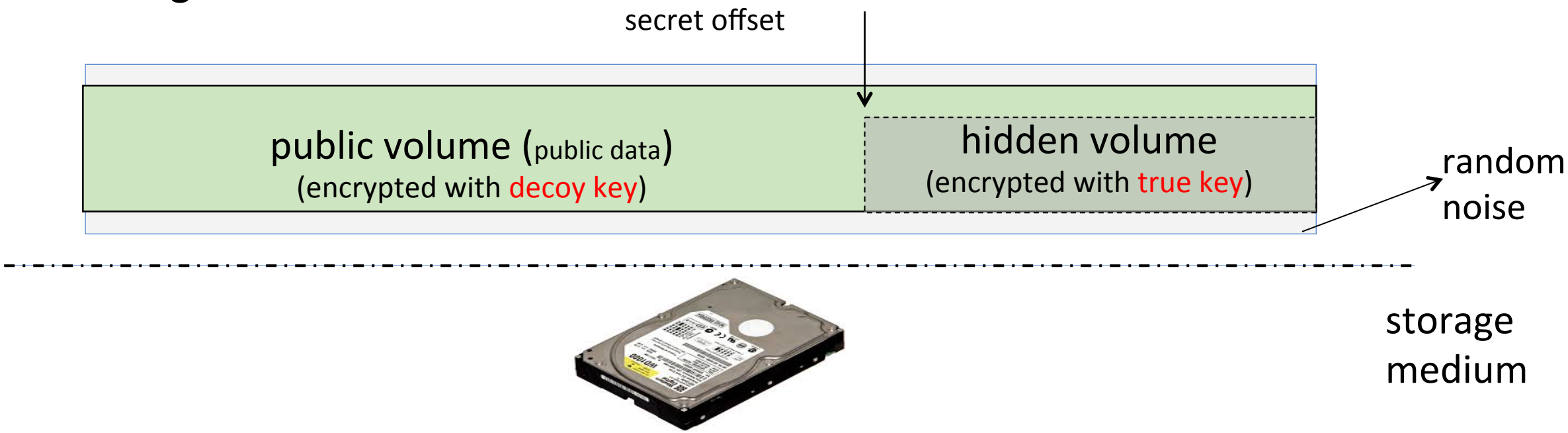
bchen@mtu.edu

http://cs.mtu.edu/~bchen

# Use Hidden Volume to Mitigate Coercive Attacks

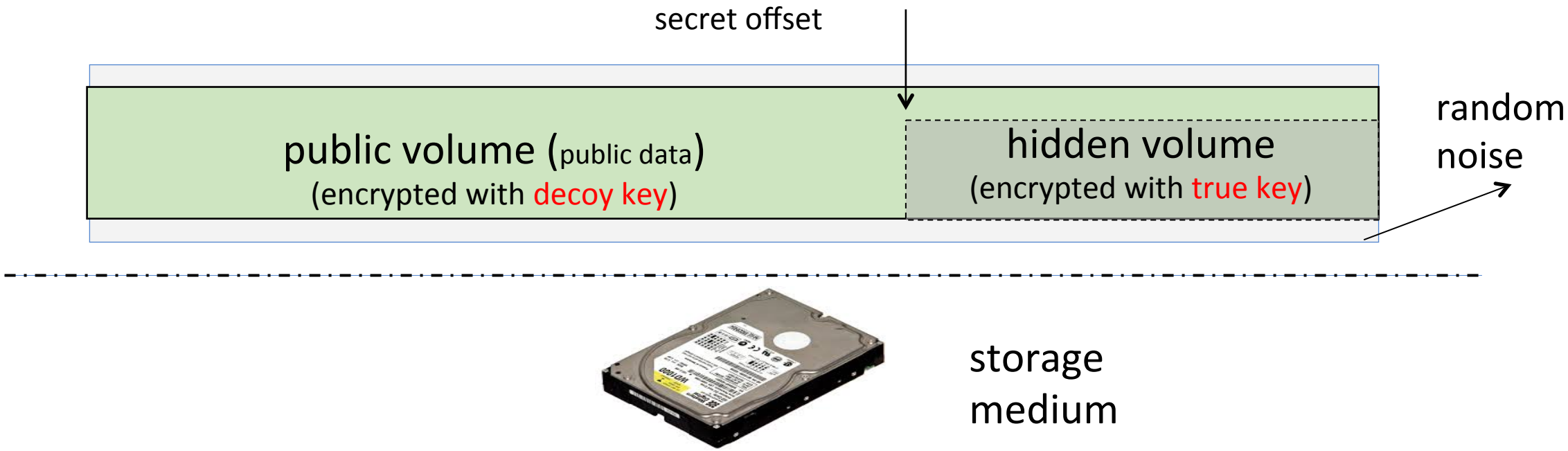
- A coercive attacker can enforce the victim to disclose the decryption key

- A hidden volume-based PDE system can be used to mitigate coercive attacks

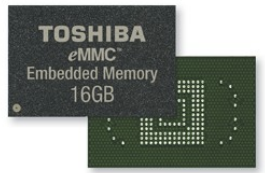
# The Hidden Volume Solution cannot Defend against a Multiple-snapshot Adversary

- By having multiple snapshots on the storage medium, the attacker can compromise deniability
  - Compare different snapshots and can observe the changes/modifications over the hidden volume, which was not supposed to happen
  - **Hidden volume is hidden in the empty space of the public volume**



# Any Other Deniability Compromises?

- Yes, from the underlying storage media
  - Mobile devices usually use flash memory as the underlying storage media, rather than mechanical hard disks
    - eMMC cards
    - miniSD cards
    - MicroSD cards

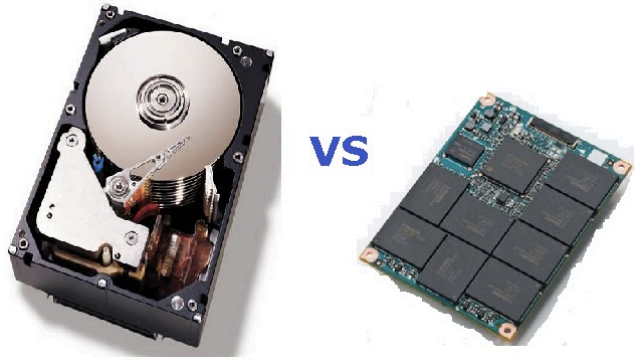


eMMC Chip


MMC Card

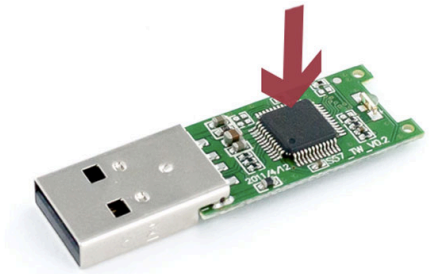


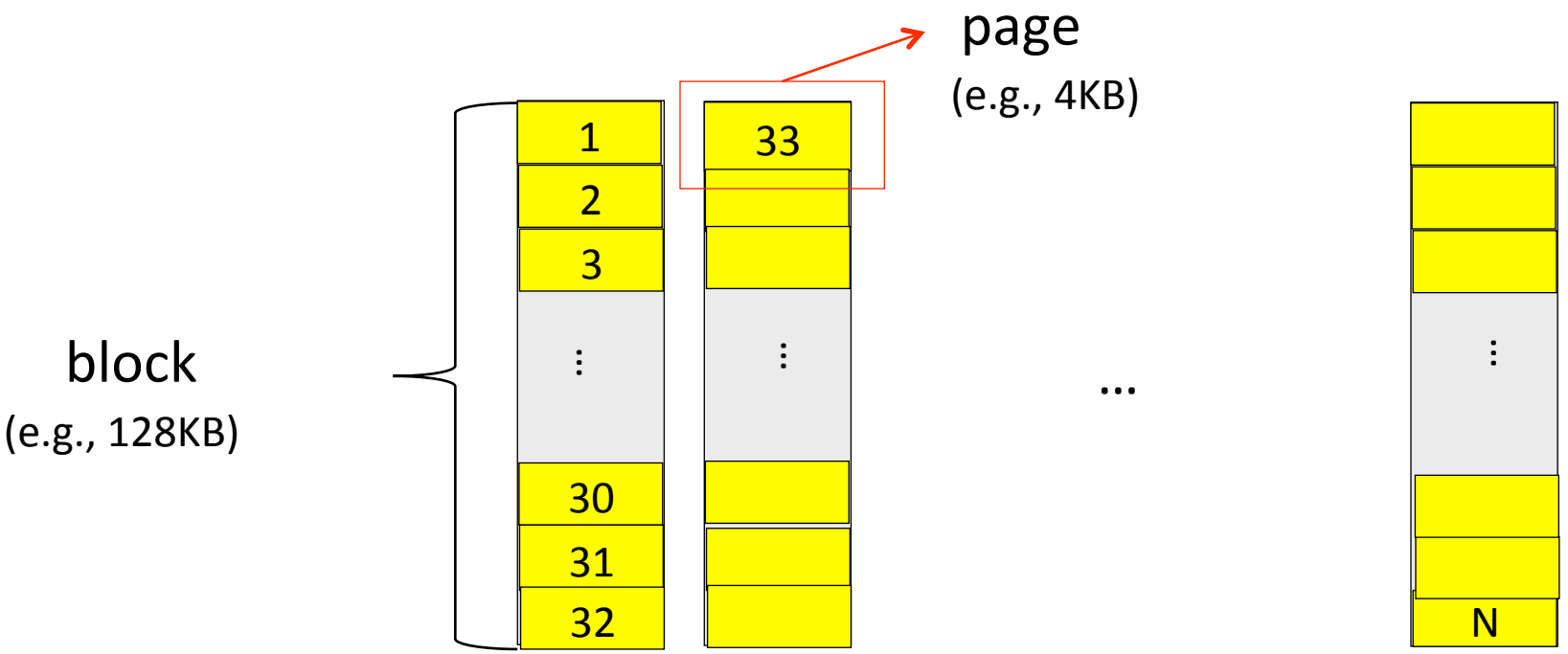
  - **Flash memory has significantly different physical nature compared to mechanical disk drives**, which may cause deniability compromise



# NAND Flash is Usually Used as Storage Media

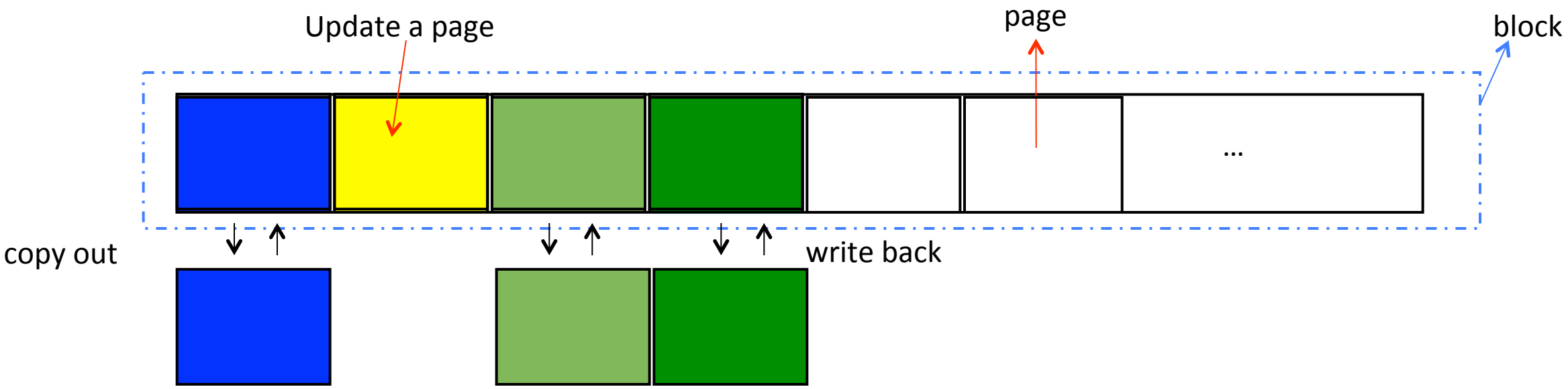
- NAND flash
  - USB sticks
  - Solid state drives (SSD)
  - SD/miniSD/microSD/eMMC





# Special Characteristics of NAND Flash

- Update unfriendly
  - Over-writing a page requires first erasing the entire block
  - Write is performed in pages (e.g., 4KB), but erase is performed in blocks (e.g., 128KB)




  - Over-write may cause significant write amplification

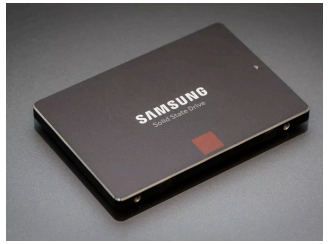
# Special Characteristics of NAND Flash (cont.)

- Support a finite number of program-erase (P/E) cycles
  - Each flash block can only be programmed/erased for a limited number of times (e.g., 10K)
  - Data should be placed evenly across flash (wear leveling)

# How to Manage NAND Flash

- Flash-specific file systems, which can handle the special characteristics of NDND flash
  - YAFFS/YAFFS2, UBIFS, F2FS, JFFS/JFFS2

- Flash translation layer (FTL) – a flash firmware embedded into the flash storage device, which can handle the special characteristics of NAND flash and emulate the flash storage as a regular block device
  - SSD
  - USB
  - SD




# A New Design Goal of PDE Systems for Mobile Devices

- Can defend against a multiple-snapshot adversary

- Accommodate the special nature of flash memory to prevent deniability compromise

# Paper Presentation

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

- Presented by Ryan Olson