PEARL: Plausibly-Deniable Flash Translation Layer

Chen Chen
Stony Brook University

Anrin Chakraborti
Duke University

Radu Sion
Stony Brook University

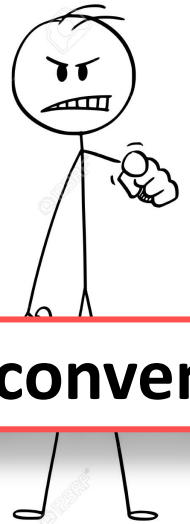
Stony Brook University
Computer Science Department

National Science Foundation
WHERE DISCOVERIES BEGIN

Privacy Against Coercive Adversaries

Increasingly Intrusive Privacy Laws

“ The United Kingdom's Regulation of Investigatory Powers Act makes it a crime to not surrender encryption keys on demand from a government official authorized by the act”



Oppressive Regimes

“Kazakhstan police detained an activist in Astana on suspicion of inciting social discord … **police confiscated a computer, a laptop, a mobile telephone, an iPod and documents. The authorities have not issued a record detailing the search and confiscation of items from Blyalov’s home, as they are required to do under Kazakh law” … Human Rights Watch (2015)**

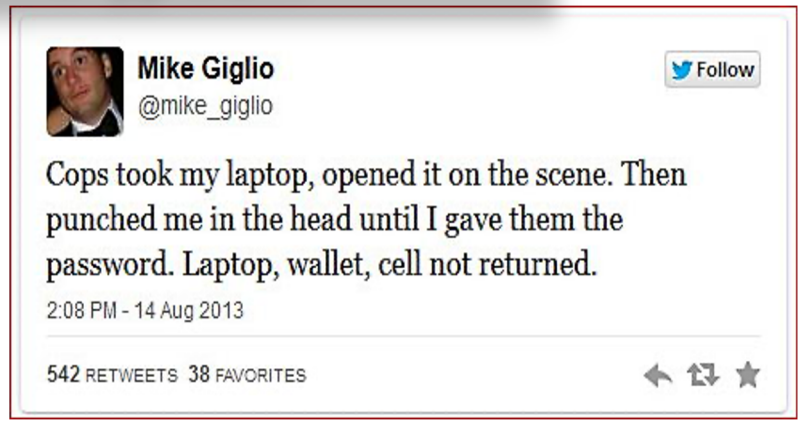
Need more than conventional encryption

hy

Unlawful Detention & Searches

Egypt: An opposition in exile whose loved ones pay the price

Authorities in Egypt have targeted relatives of activists who live abroad in an attempt to further stifle dissent.

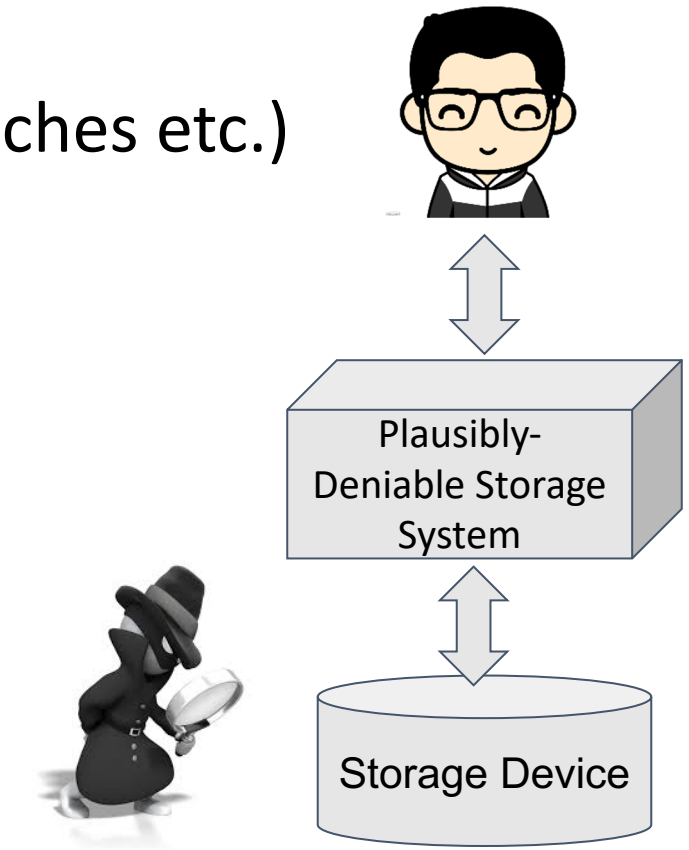


Plausible Deniability

"Security property of a mechanism that allows parties to claim to others (e.g., an officer in an oppressive regime) that some information is not in their possession or that some transaction has not taken place" – StegFS (1998), McDonald *et al.*

Threat Model

- Observe (multiple) snapshots of storage device
- Cannot observe device at runtime (memory, caches etc.)
- No system compromise
- Coerce users for key(s)
- Rational



Deployment

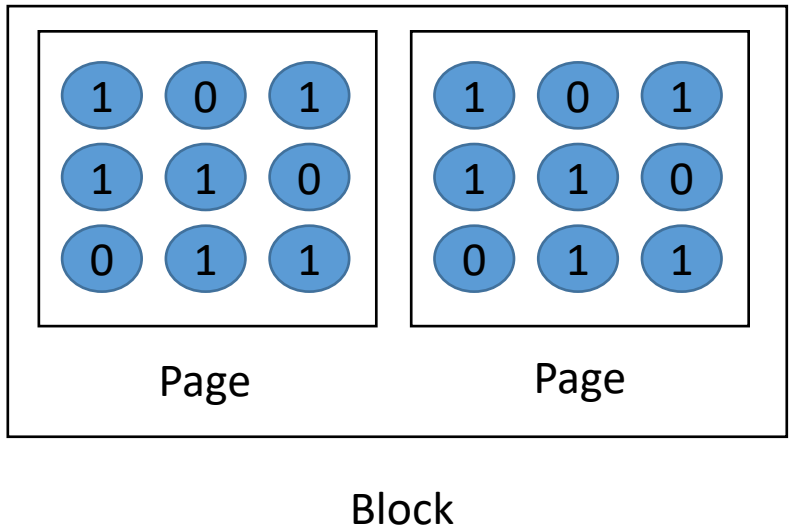

Hand over your phone.
You have encrypted data, hand over your key.
Public data
Fine, my data is encrypted.
Public key
Hidden key
Fine, I will give up the public key.

Plausibly-Deniable Storage Systems

- Steganographic Filesystems:
  - StegFS* [Anderson et al. IH '98], [McDonald et al. IH'99] [Pang et al. ICDE '03]
  - DEFY [Peters et al. NDSS '15], INFUSE [Chen et al. PETS '20]
  - …
- Hidden volumes:
  - TrueCrypt, HIVE [Blass et al. CCS '15], DataLair [Chakraborti et al. PETS '17], PD-DM [Chen et al. PETS '19]
  - …
- Flash-Based:
  - DEFTL [Jia et al. CCS '17]
  - ?

What Makes Flash Devices Different?

- Cells are basic unit of storage
- Group of cells make up a page
- Group of pages make up a block
- Page-level programming
  - 0 → 1, 1 ✗→ 0
- Block-level erase before write
  - Slow
  - Wear from P/E cycles



Flash Translation Layer (FTL)

- Interface between FS and raw flash
- Maps logical address to physical address space
- Wear levelling
- Garbage collection

FTL conflicts with upper layer deniability

PEARL: FTL with Plausible Deniability

- Deniability logic implement in FTL
- DEFTL [Jia CCS '17]: Single-snapshot deniability
- Multi-snapshot resistant → All changes due to "public data"

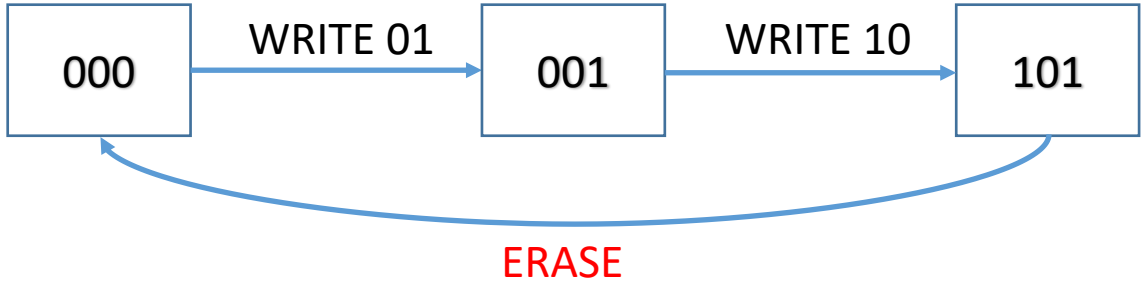
A data encoding scheme where
public + hidden data = plausible public data?

Write-Once-Memory (WOM) Code

- Write-once-memory: 0 → 1, 1 ~~→~~ 0
- More writes before erase
  - reduce wear, P/E cycles

(2,3) WOM Code

data	1st write	2nd write
00	000	111
01	001	110
10	010	101
11	100	011



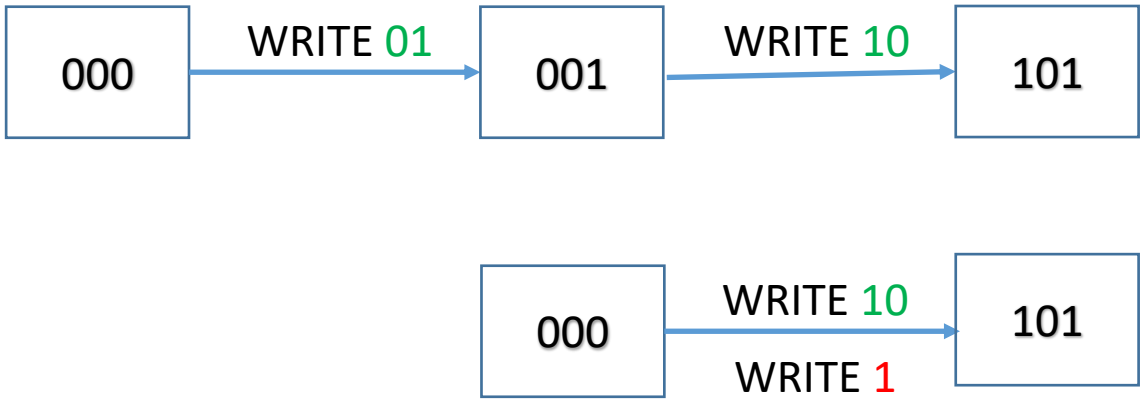
WOM Codes with Hidden Bits

- Additional capacity for a hidden bit
- 2 public writes = public + hidden write

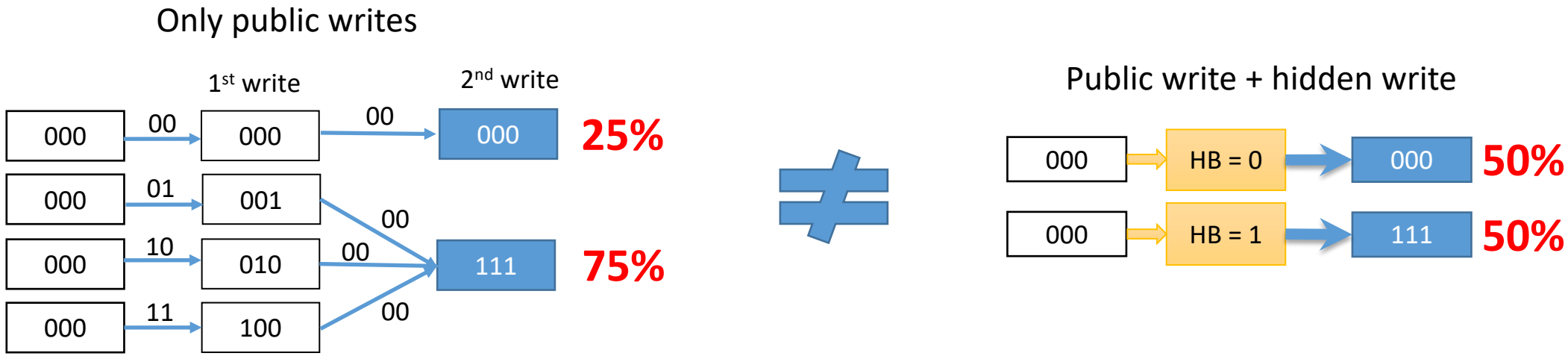
(2,3) WOM Code + 1 Bit Hidden

data	1st write	2nd write	
		HB = 0	HB = 1
00	000	000	111
01	001	001	110
10	010	010	101
11	100	100	011

Hidden bit decides
Codeword for public



Not all WOM Codes work!



Distribution of public only codewords = distribution of public + hidden codewords

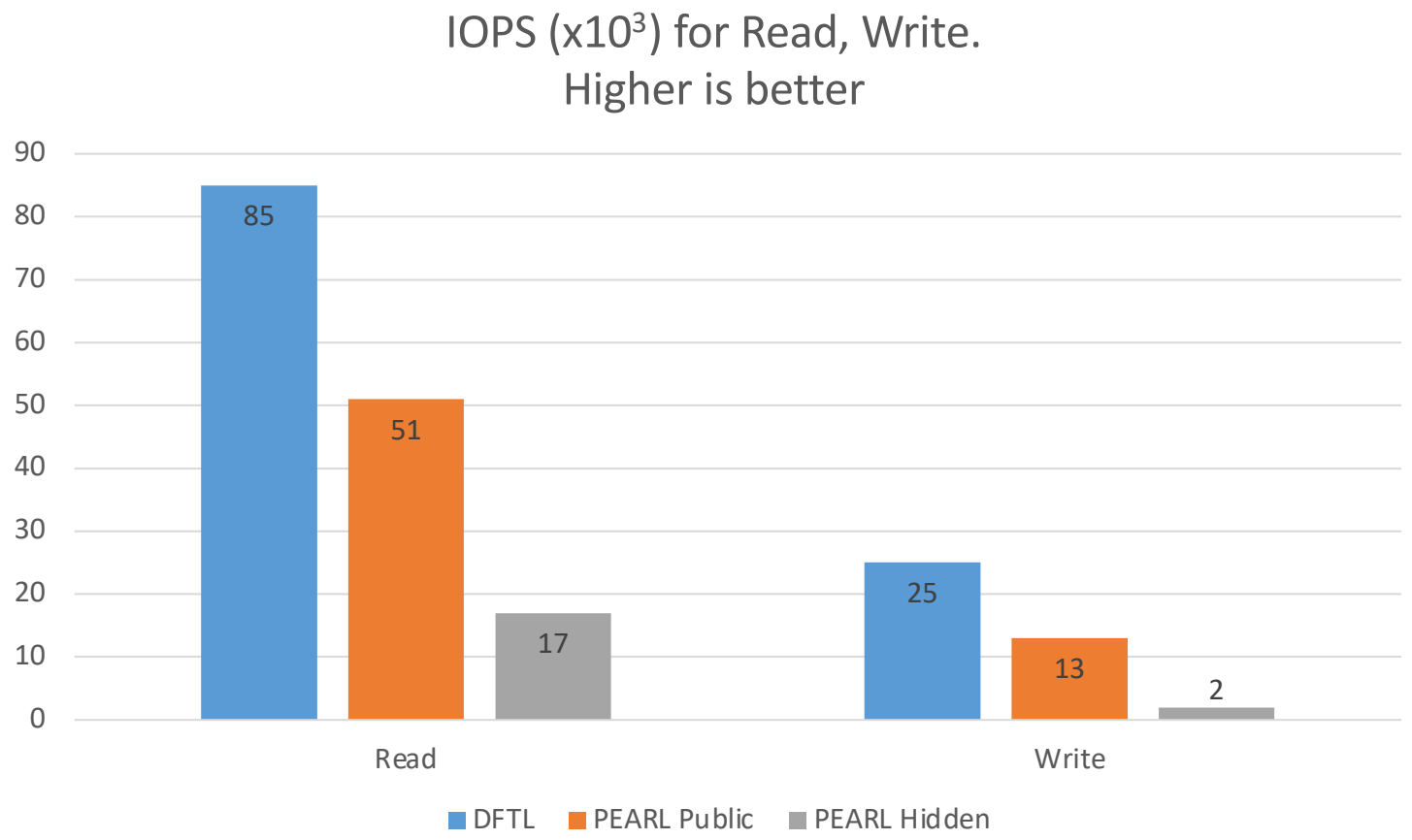
(3,5) WOM Code with Equal Partition

Public Data	First write	Second write	
000	00000	11110	10011
001	00001	11001	10110
010	00010	11010	10101
011	00100	11100	01111
100	01000	11111	01101
101	10000	11101	01110
110	11000	11000	10111
111	10100	11011	10100

More Challenges

- Page allocation & transition
- Garbage collection
- Wear Levelling
- …

Throughput


IOPS (x10³) for Read, Write.
Higher is better
90
80
70
60
50
40
30
20
10
0
85
51
17
25
13
2
Read
Write
DFTL
PEARL Public
PEARL Hidden

Conclusion

- FTL with plausible deniability
- WOM codes for multi-snapshot resilience
- Practical

Questions?