Hide-and-Seek: Hiding Secrets in Threshold Voltage Distributions of NAND Flash Memory Cells

Md Raquibuzzaman, Aleksandar Milenkovic, Biswajit Ray

The University of Alabama in Huntsville

mr0068@uah.edu, milenka@uah.edu biswajit.ray@uah.edu

This work was supported in part by the National Science Foundation under Grants #2145311 and #2007403

Outline

- Motivation and background
- Proposed data hiding scheme
- Experimental evaluation
- Conclusion and future work

Motivation

- **Stolen or lost personal electronic devices:** Stolen or lost devices may lead to data leakage. Cryptographically encoded data typically appears unrecognizable; however, it is advantageous to hide the very presence of any hidden secret.

- **Coercive adversary**: Conventional encryption cannot defend against a coercive attacker who can find ways to force the device owner into disclosing the decryption key.

State-of-the-art solutions

Plausibly Deniable Encryption (PDE):

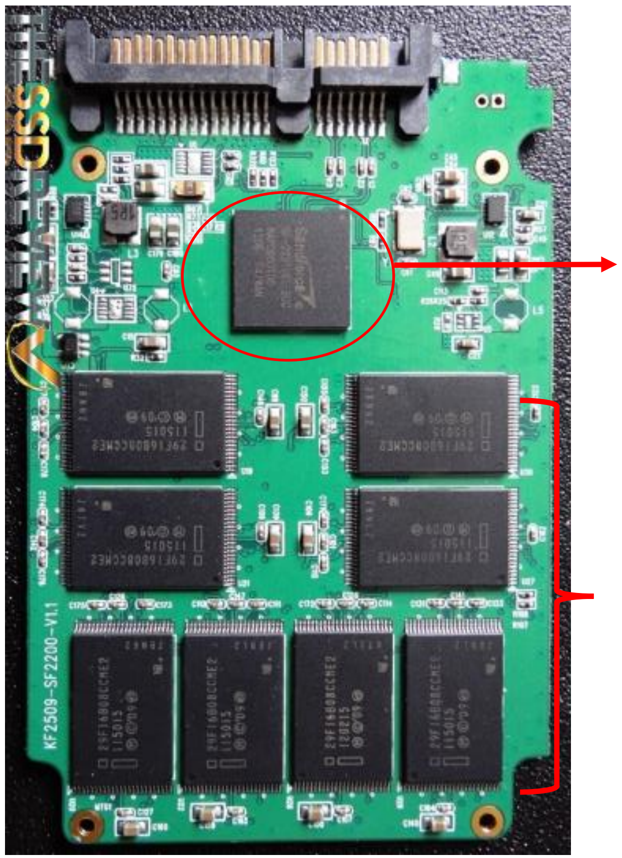
- Involves a decoy key (for innocuous plain text) and a true key (for original sensitive data)
- Digital steganography and steganographic file system
- Typically developed for PC platforms, e.g., TrueCrypt, HIVE

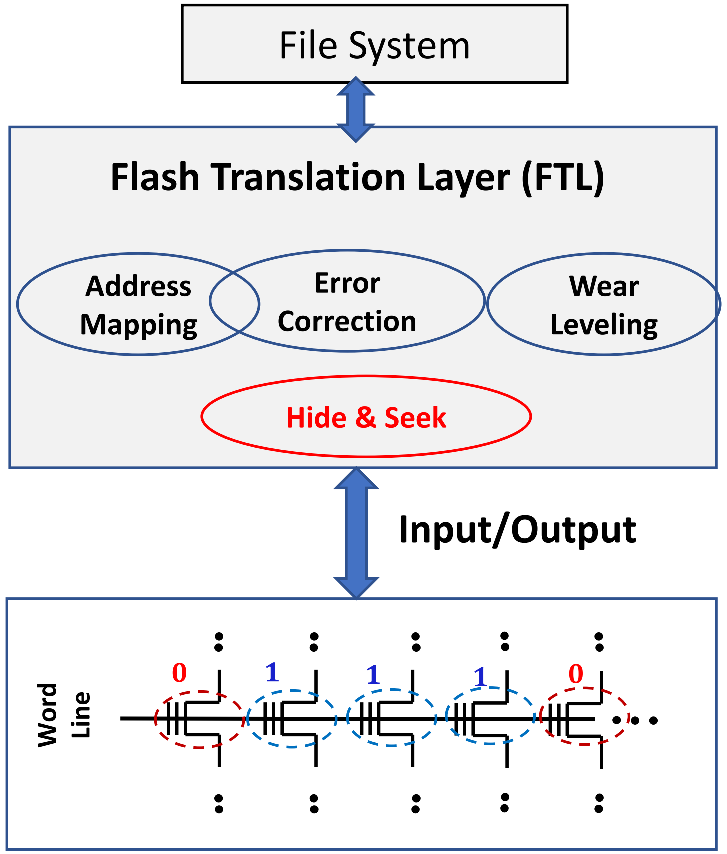
Challenges:

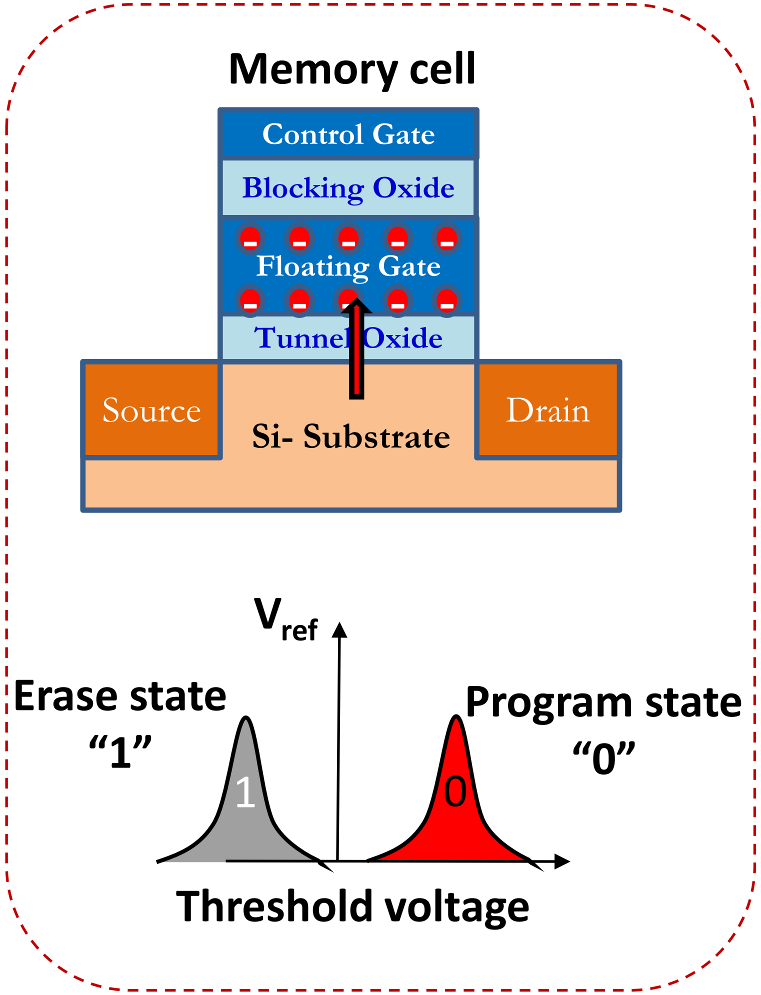
- Mobile platform are resource-limited and hence PDE solutions developed for PC platforms are not directly applicable
- Mobile platforms typically use flash storage which has different constraints than hard-disk-drives

Background: System view of flash storage

Internal of an SSD



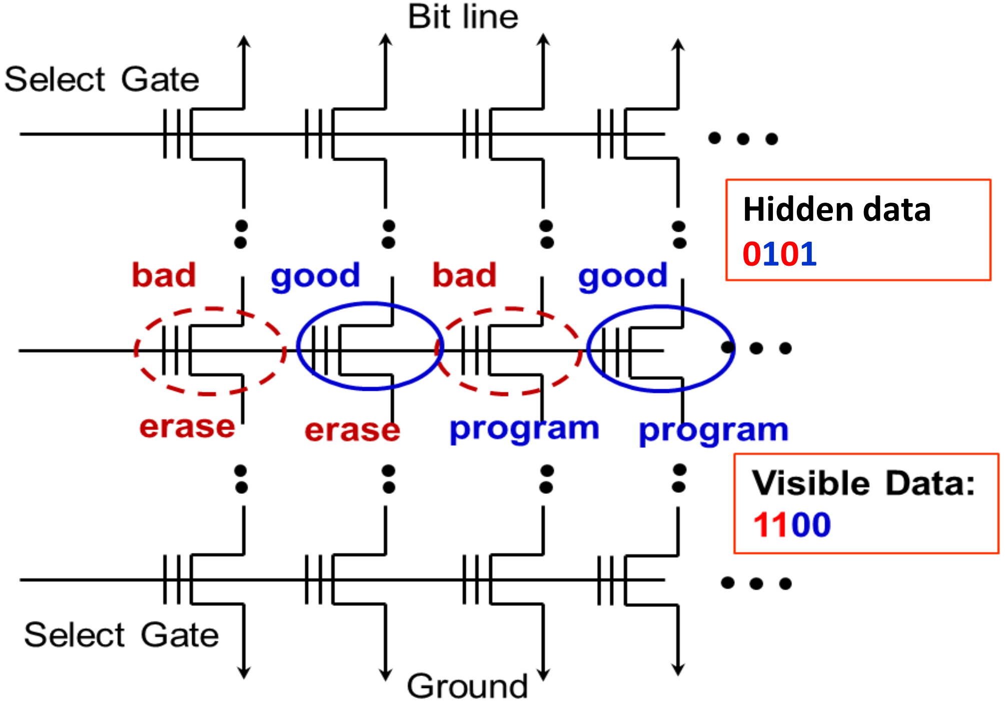




Hide & Seek can be implemented as a new function in the FTL

Literature: Data hiding using physical properties of flash memory

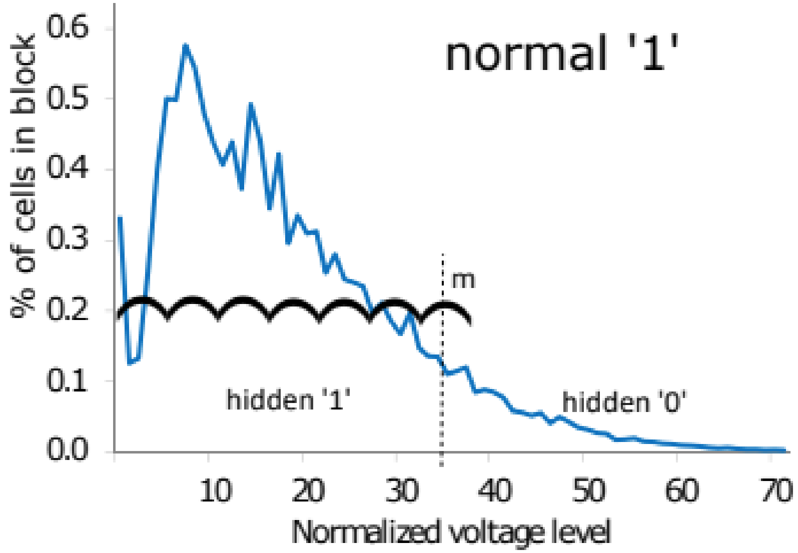
Wang et. al., IEEE S&P 2013 [1]



Key Points

- **Repeated Program/Erase cycle is employed to change the physical properties**
- **Cell program time variation is used to hide data**

Zuck et. al., FAST 2018 [2]

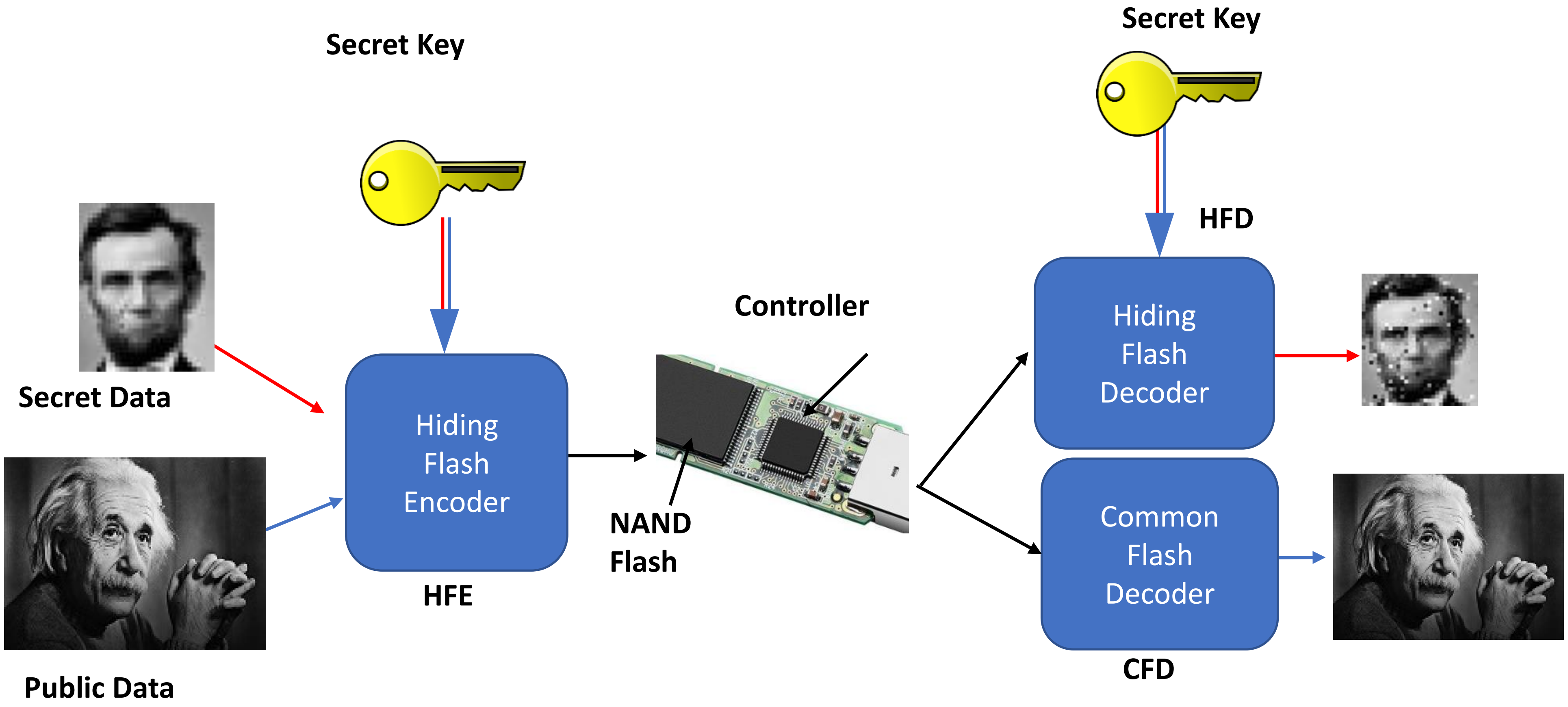


Key Points

- **Hides information in erased state; requires privileged commands**
- **Erase states suffer from NAND reliability issues**

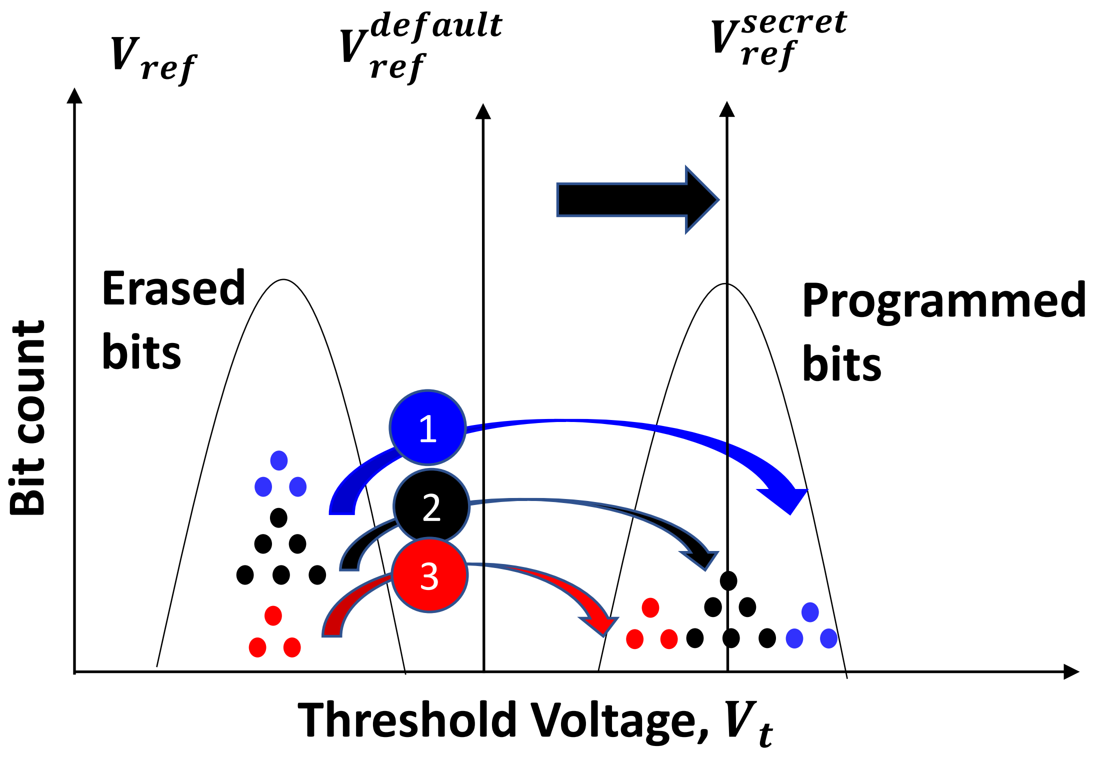
1. Wang, Y., Yu, W.-k., Xu, S. Q., Kan, E., and Suh, G. E. Hiding information in flash memory. In *2013 IEEE Symposium on Security and Privacy* (2013), pp. 271–285
2. Zuck, A., Li, Y., Bruck, J., Porter, D. E., and Tsafrir, D. Stash in a flash. In *16th USENIX Conference on File and Storage Technologies (FAST 18)* (Oakland, CA, Feb. 2018), USENIX Association, pp. 169–188

System view of the proposed method



Proposed data hiding method

Hide & Seek stores secret data in a subset of programmed bits of the public data by manipulating their threshold voltages. The encoding involves 3-step programming sequence:



1 Program the **blue cells**. They are the zeros of hidden data. Neighbor word line interference effects are used to boost up blue cell V_t

2 Program the **black cells**. They are the majority bits in the program distribution of the public data (not holding secret data)

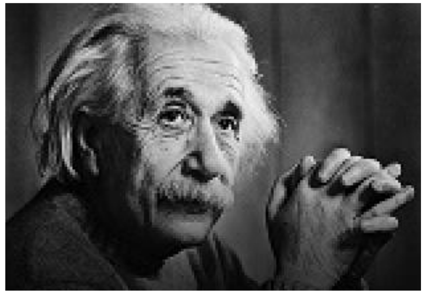
3 Program the **red cells** using a partial program operation. They are the one bits of hidden data

Example: Illustration of data hiding scheme

Secret image

Binary value: 1010110....

Visible image

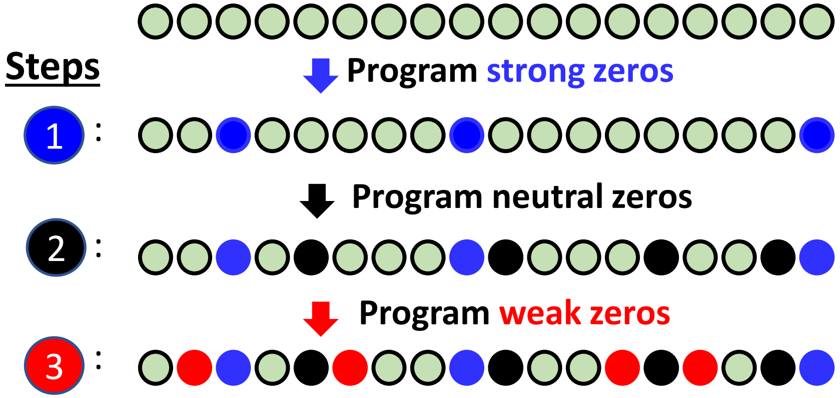


Binary : 100100110011000100....

Secret data: 1 0 1 0 1 1 0....

Public Data: 1 0 0 1 0 0 1 1 0 0 1 1 0 0 0 1 0 0

Steps



● : Strong zeros

● : Neutral zeros

● : Weak zeros

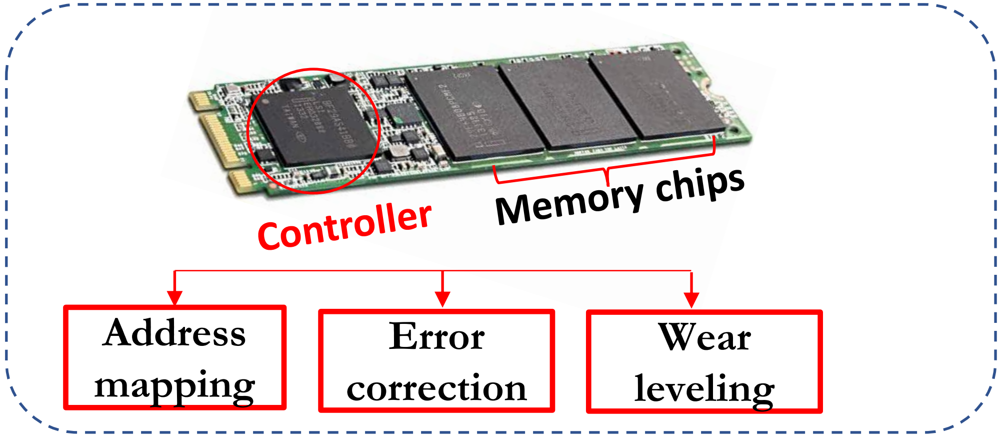
● : Ones of public data

Key Points

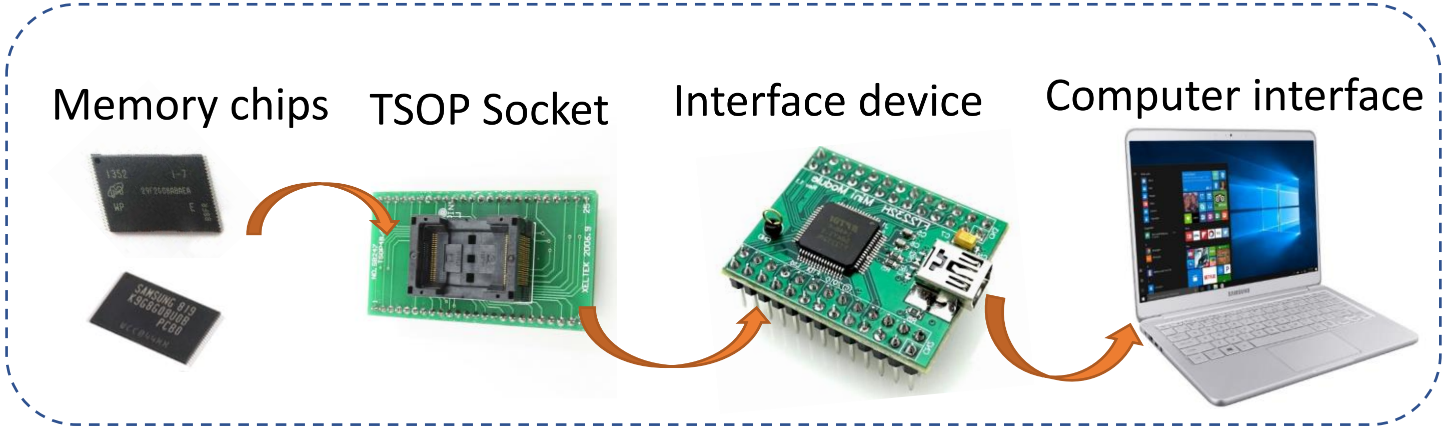
- Strong zeros are created using word line interference effects
- Weak zeros are created using partial program operation

Experimental set-up: Interfacing COTS memory chips

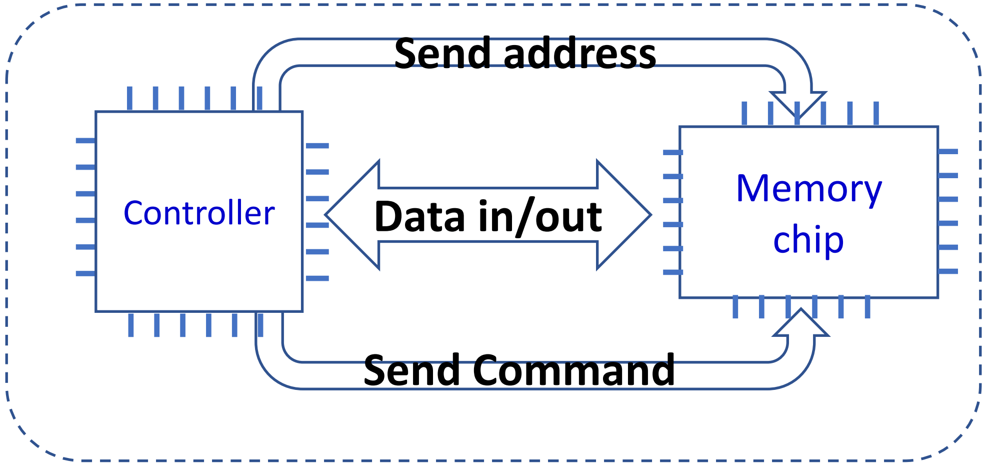
A typical storage system

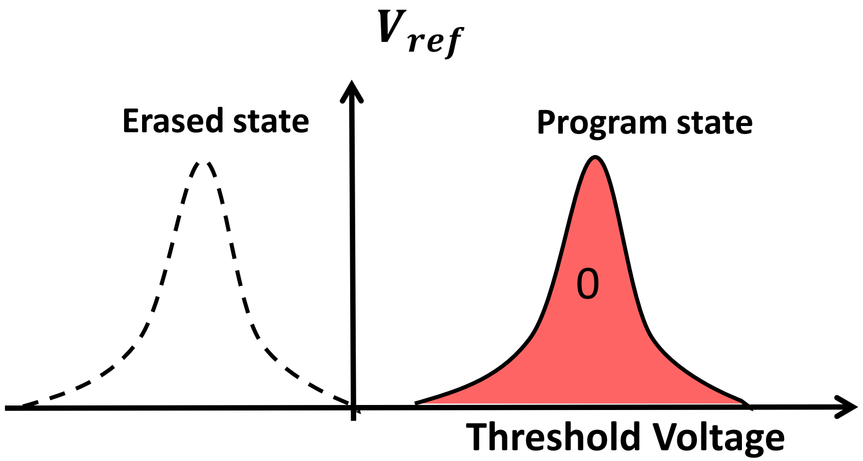


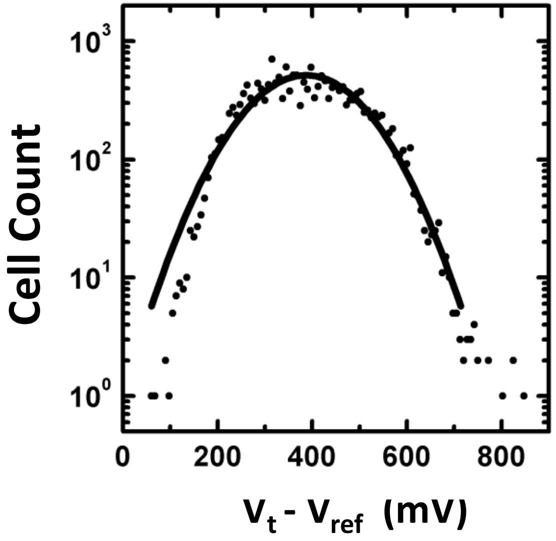
Experimental Set-up



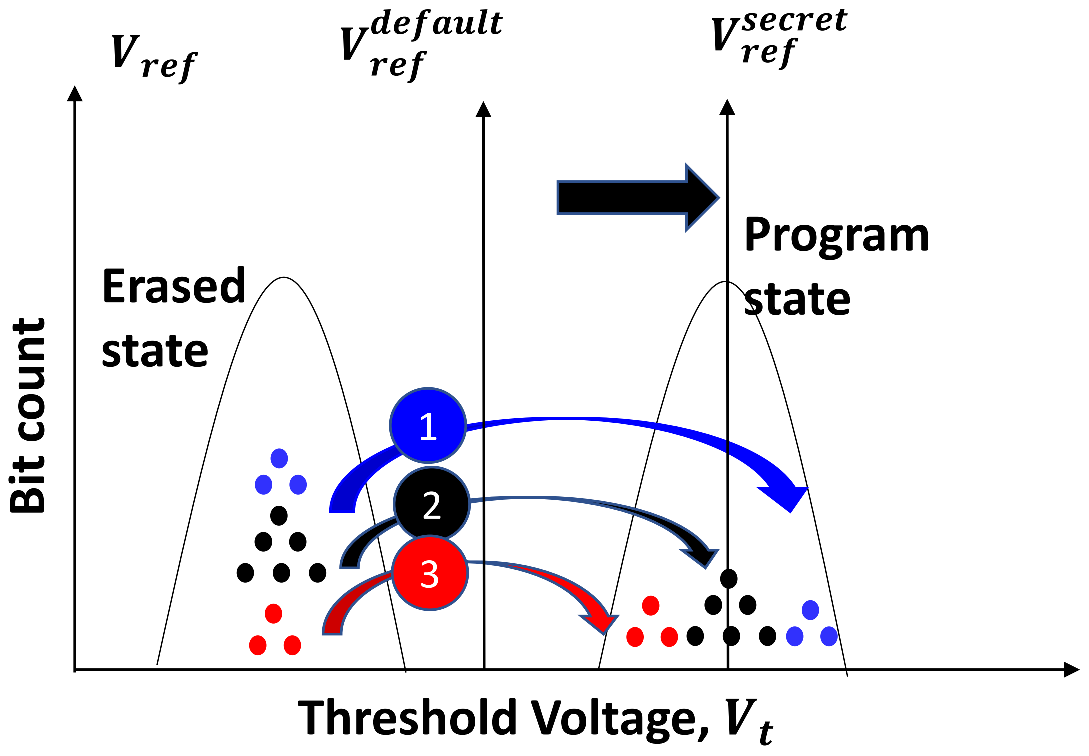
Interfacing framework

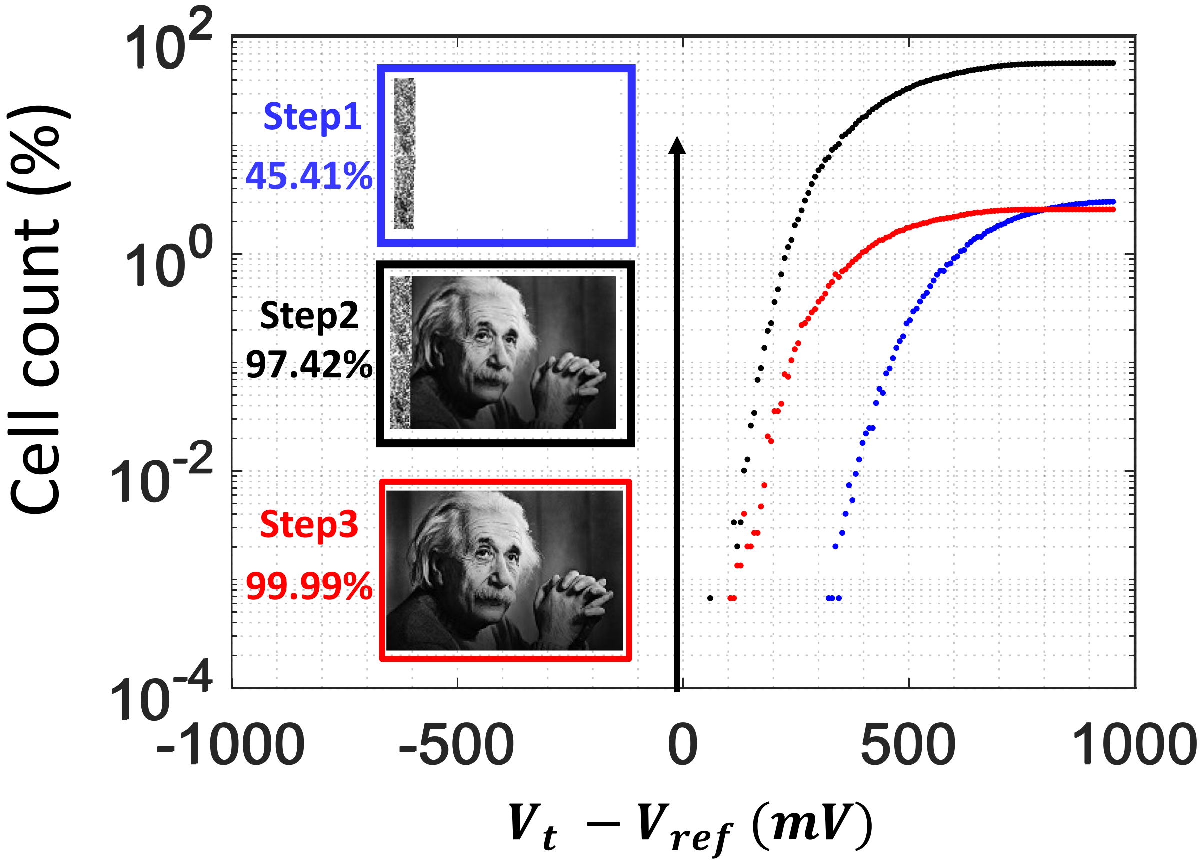






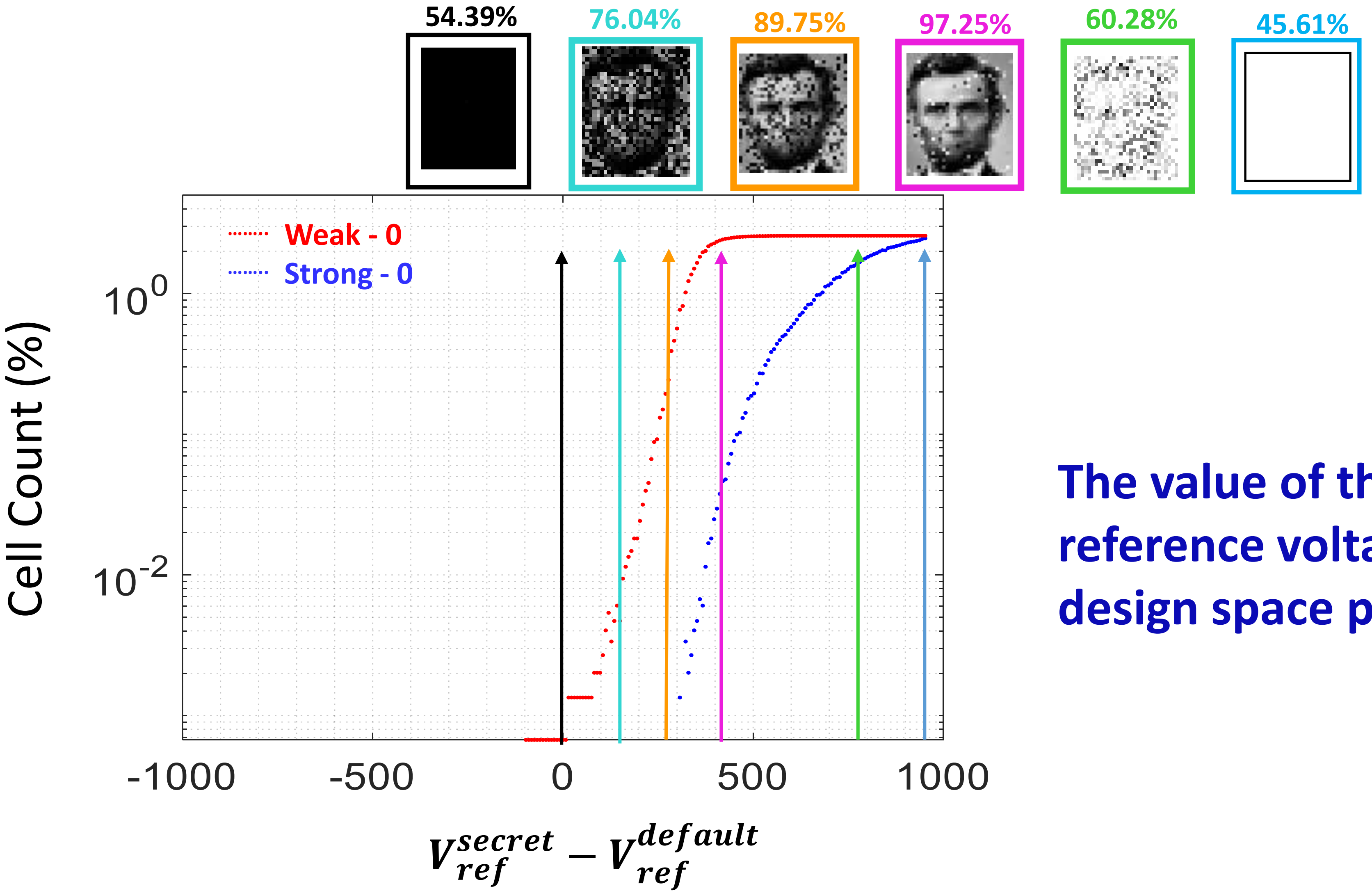
Experimental evaluation of write operation





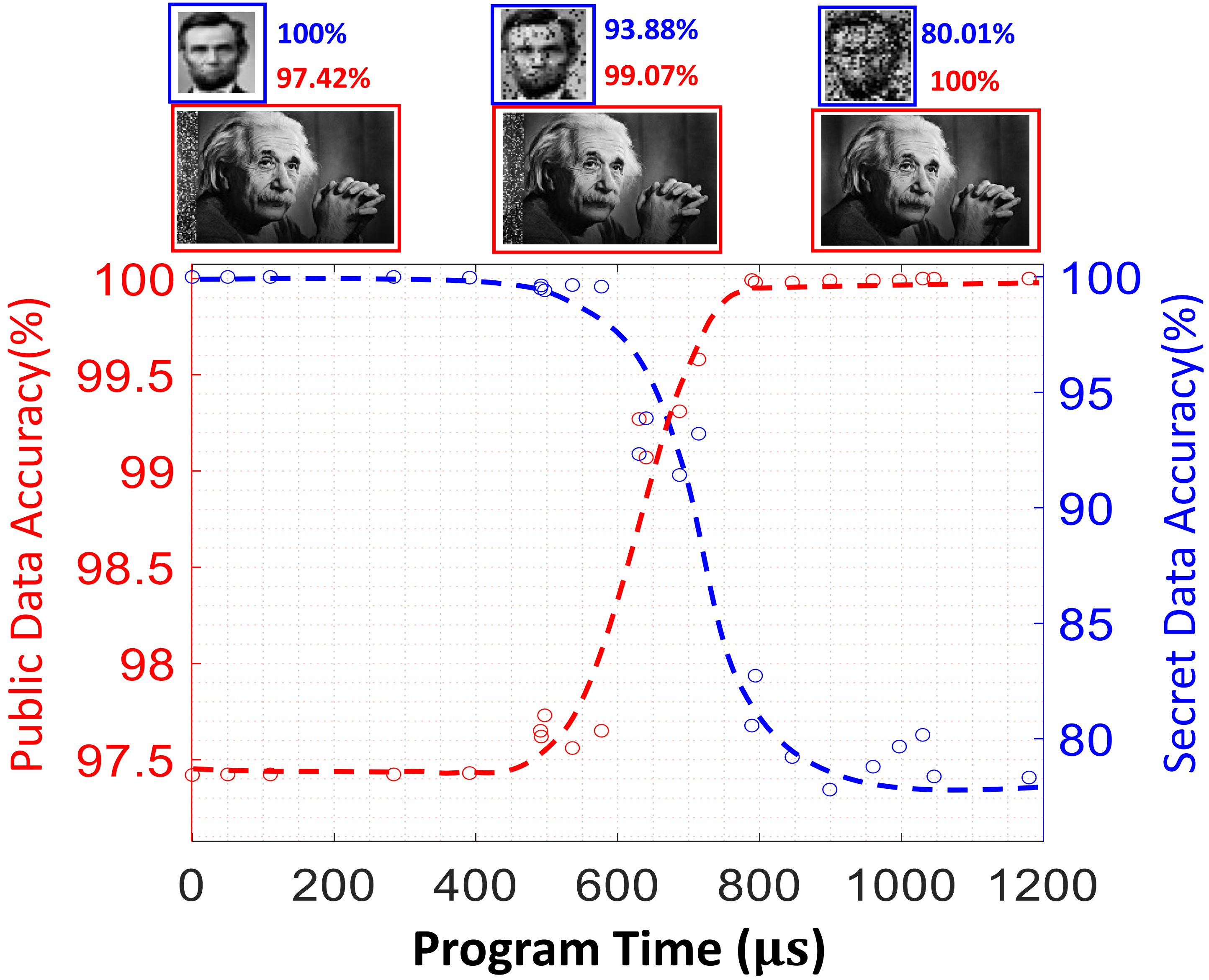
Accuracy of the public image is not significantly affected by the hiding operation

Experimental evaluation of read operation

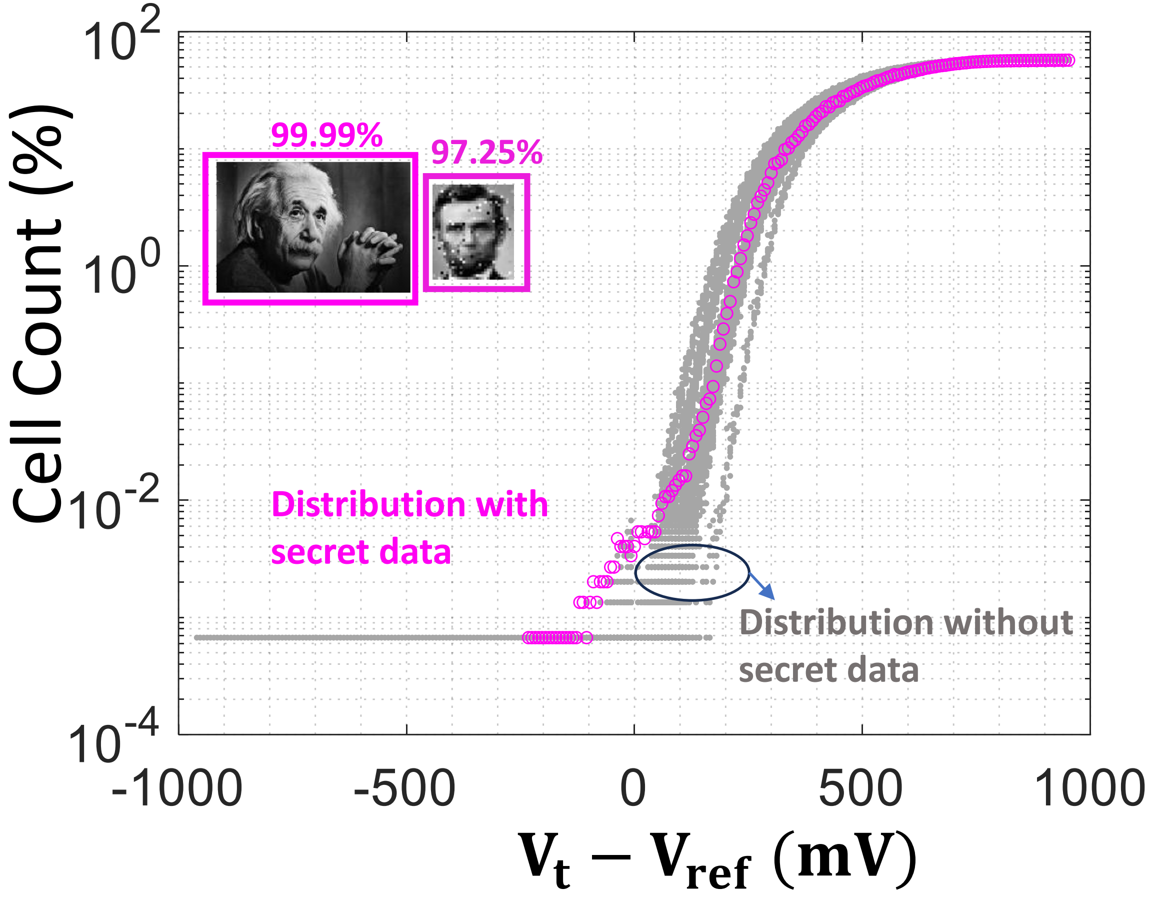


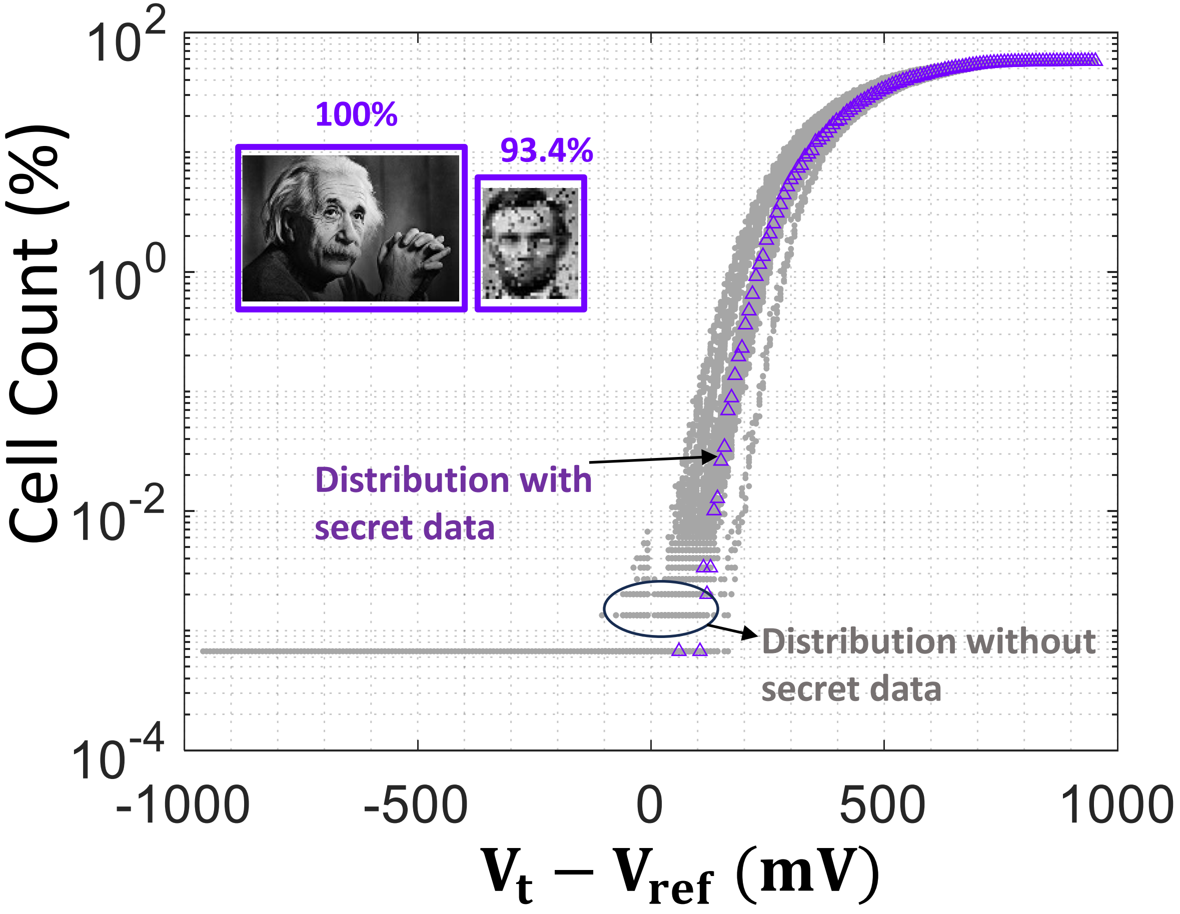
The value of the secret read reference voltage is another design space parameter

Impact of partial program time on accuracy



Accuracy and detectability trade-off





- **NAND flash memory has significant V_t variation due to process variation**
- **Accuracy of the secret image can be tuned with partial program operation**

Conclusions and Future Work

- We have experimentally demonstrated the feasibility of hiding information in the program state of the COTS 3D NAND flash memory chips

- The method provides several design space variable to tune the accuracy, and detectability of the secret image

- The method is universally applicable to all NAND flash chips from any manufacturer without requiring any hardware modification or privileged commands

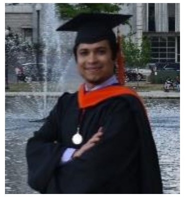
- Implementation of the proposed concept in the FTL with performance trade-off evaluation remains to be evaluated

Thank You

email: biswajit.025@gmail.com

Research Group

Raquib



Umesh

Matchima

Horace

Anik

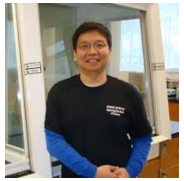
Farzana

Recent Graduates

Dr. Kumari

Dr. Sakib

Dr. Huang



Mr. Hasan