NSFSaTC-BSF: TWC: Small: Practical Plausibly Deniable Encryption through Low-Level Storage Device Behavior

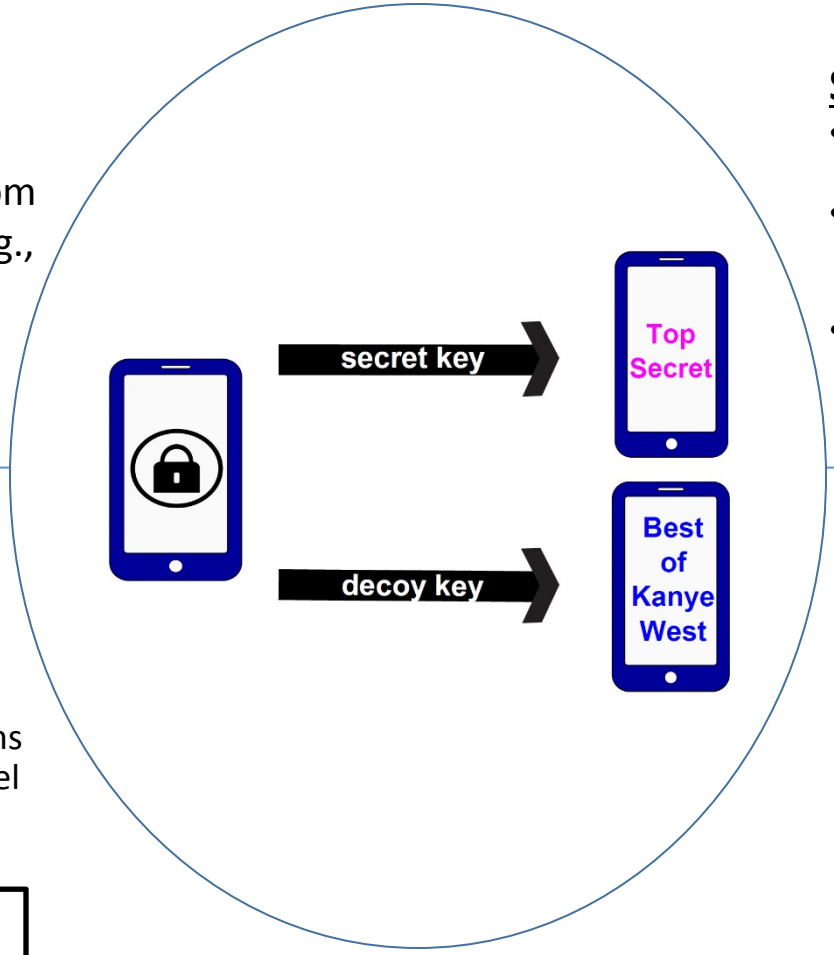
National Security Institute

Stony Brook University

UNC COLLEGE OF ARTS & SCIENCES

Challenge:

Protect sensitive data from malicious adversaries (e.g., human rights activist in oppressive regimes)



Scientific Impact:

- First theoretical foundations for plausible deniability.
- Encoding techniques for hiding information in flash storage
- Practical mechanisms for plausible deniability safe against multi-snapshot adversaries.

Solution:

- Fastest plausibly deniable storage to date.
- Fastest Write-Only ORAM
- New encoding mechanisms for SSDs using voltage level manipulation

Broader Impact:

- Protect Freedom of Speech and Human Rights Activism
- Project resulted in practical open-source tools and mechanisms

SATC Award 1526707, Radu Sion, sion@cs.stonybrook.edu (Principal Investigator, Stony Brook University), Donald Porter, porter@cs.unc.edu (Principal Investigator, University of North Carolina at Chapel Hill), collaboration with Dan Tsafrir, Technion, Israel.