Achieving Leakage Resilience through Dual System Encryption

Allison Lewko, Yannis Rouselakis,
Brent Waters

THE UNIVERSITY OF
TEXAS
AT AUSTIN

Leakage Resilience

Exploding Field: [ISW03, MR04, HSHCPCFAF08, DP08, P09, AGV09, DKL09, NS09, ADW09, KV09, FKPR10, ADNSWW10, BG10, DP10, JV10, GR10, CDRW10 …]

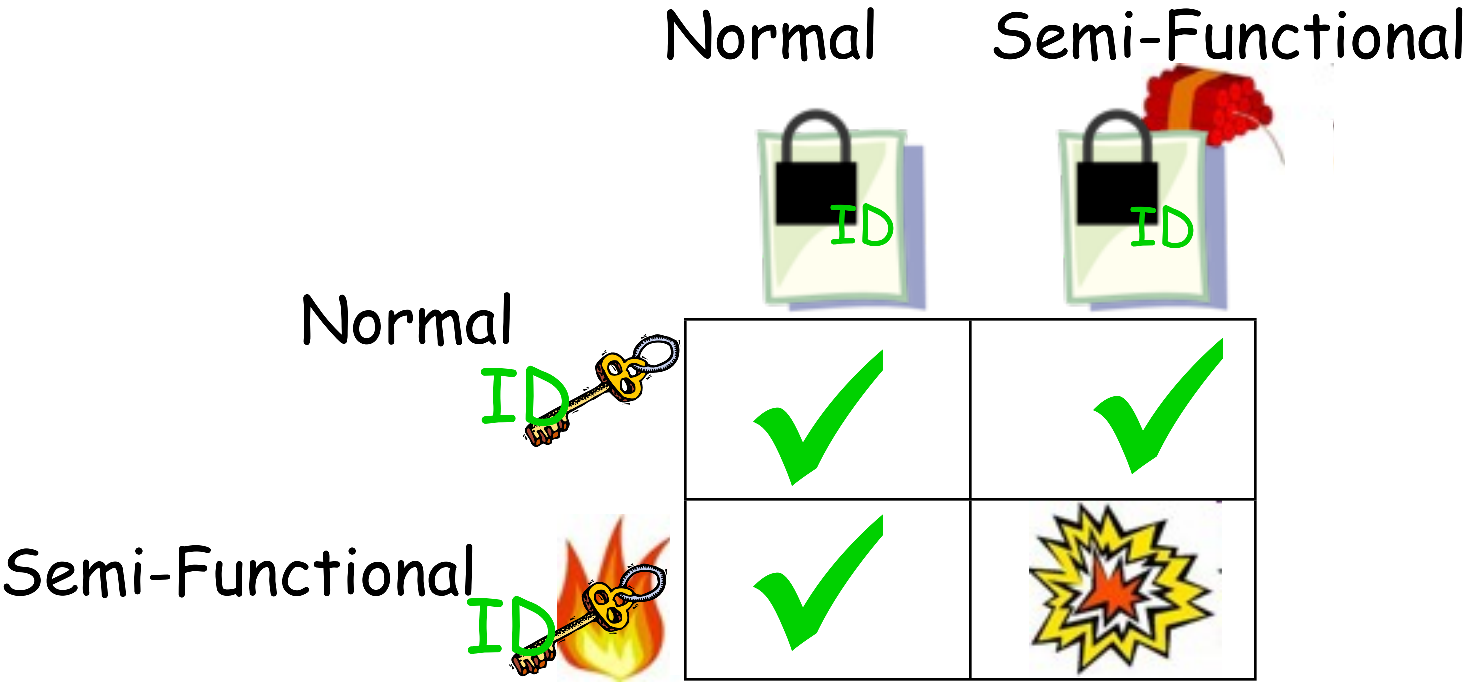
- Continual Leakage Model [BKKV10, DHLW10]
    - Signatures, PKE, Continual, IBE
    - "Tailored" subspace techniques for IBE
    - Limitations: Selective, Master Leakage, HIBE, ABE?

Can we leverage recent advances in IBE/ Functional Encryption?

Dual System Encryption

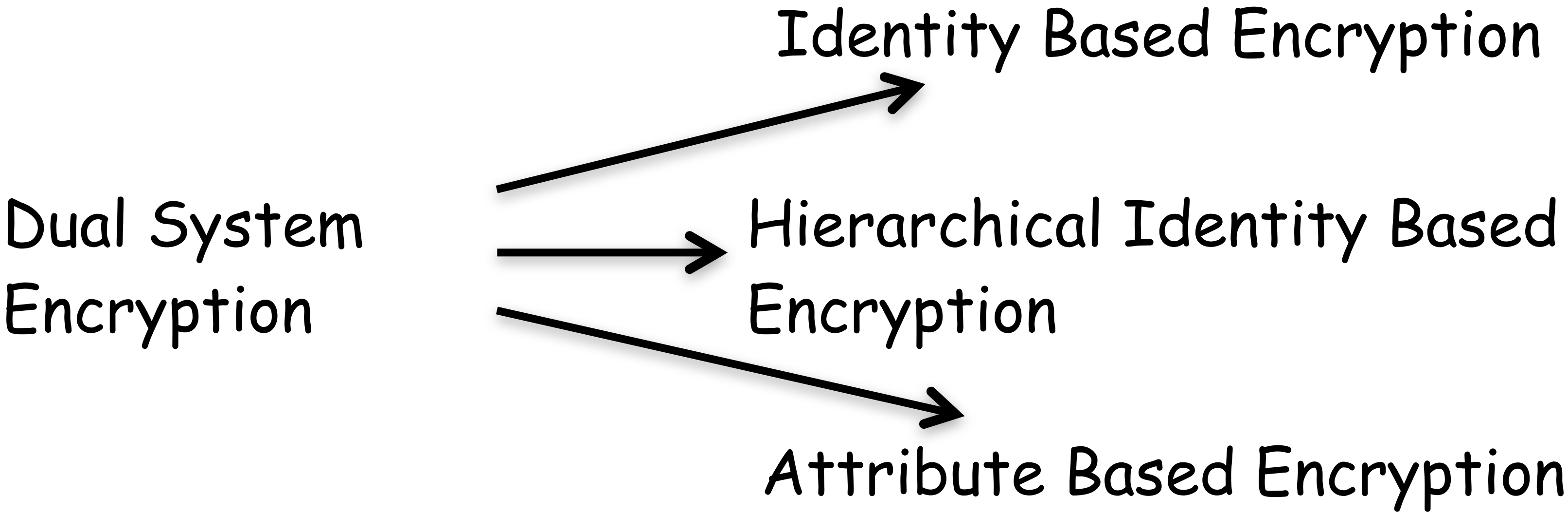
Two types of keys and ciphertexts:

Normal and Semi-functional



	Normal	Semi-Functional
Normal	✓	✓
Semi-Functional	✓	💥

Our Results



Dual System Encryption

Identity Based Encryption

Hierarchical Identity Based Encryption

Attribute Based Encryption

- Adaptive security
- Master key leakage