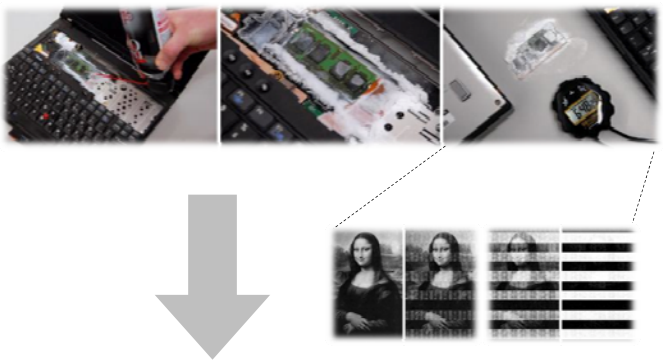
Leakage Resilient Cryptosystems

RUI ZHANG

A Gap between Theoretical Analysis and Practical Attacks

- Traditional theoretic analysis on security of cryptographic schemes usually assumes the implementation is perfect.
  - Deriving a proper mathematical model from the real systems;
  - Showing reductions from any attack to the target scheme to breaking underlying assumptions.
- This may be not always true in practice due to so-called "side-channel attack" (power consumption, computation time, electro-magnetic emission, acoustic cryptanalysis, etc.).
  - E.g.: the "cold boot attack"

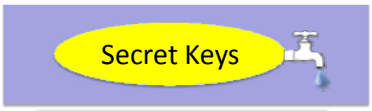
Cold Boot Attack



Secret keys in the memory

Image source: http://citp.princeton.edu/memory/media/

A New Study Considering Such Side Channels



New modeling and "proper" analysis

- Only the amount of information leakage is limited.
- The type of information leakage is not limited.

Secure schemes tolerating (partial) key leakage

Public Key Encryption

Digital Signature

Verifiable Pseudorandom Function (VRF)

The Main Tool:

(Hierarchical) ID-Based KEMs tolerating leakage in the master secret key

Reference:

Physically Observable Cryptography

- Micali-Reyzin [TCC 2004]