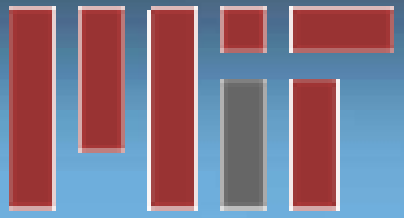


CRYPTO'09 rump session
August 18, 2009

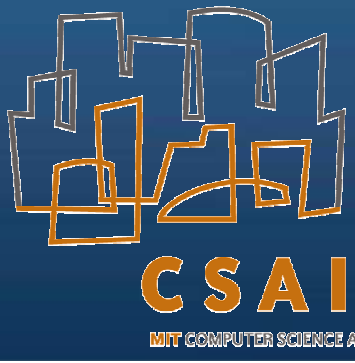
Protecting Circuits from Computationally-Bounded Leakage

Eran Tromer MIT

Joint work with

Sebastian Faust K.U. Leuven

Leo Reyzin Boston University



Motivation

The great tragedy of Crypto –

the slaying of a provably secure scheme

by an ugly side channel.

Engineering approach

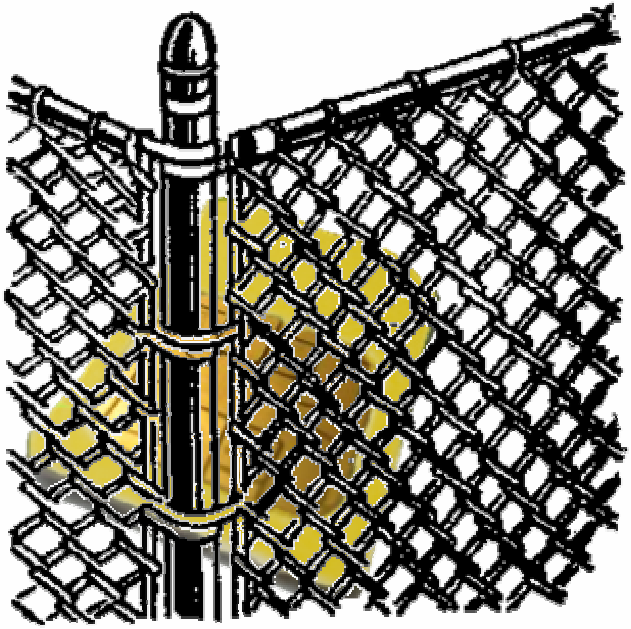
Try preventing side-channel leakage.

Engineering approach

Try preventing side-channel leakage.

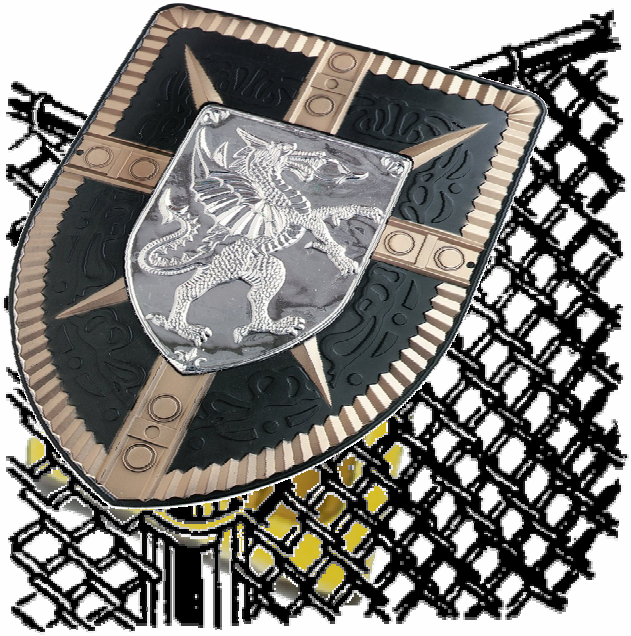
Engineering approach

Try preventing side-channel leakage.



Engineering approach

Try preventing side-channel leakage.

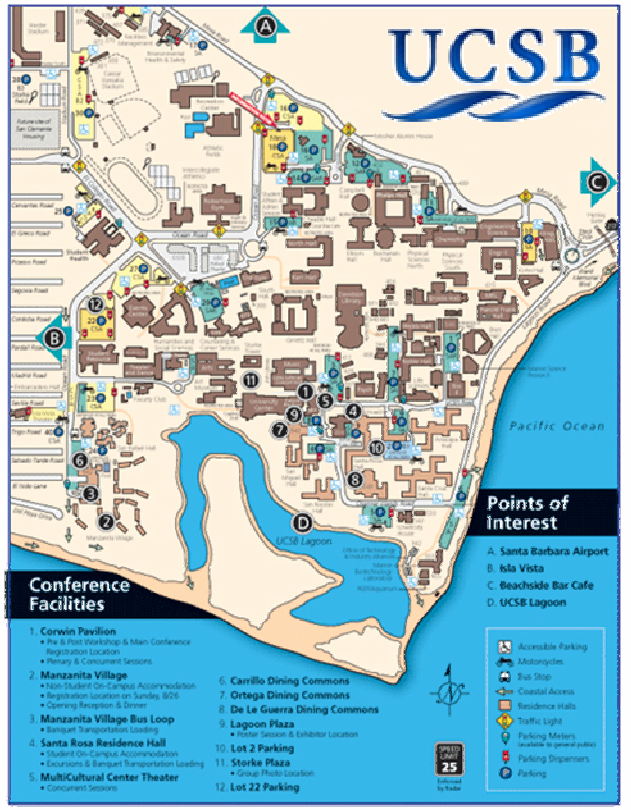


Good luck…

Cryptographic approach

Leakage is a *given*,
modeled by an adversarial
observer.

The device should
protect itself against it.



Related Work

[CDHKS00]: Canetti, Dodis, Halevi, Kushilevitz, Sahai: Exposure-Resilient Functions and All-Or-Nothing Transforms

[ISW03]: Ishai, Sahai, Wagner: Private Circuits: Securing Hardware against Probing Attacks

[MR04]: Micali, Reyzin: Physically Observable Cryptography

[GTR08]: Goldwasser, Tauman-Kalai, Rothblum: One-Time Programs

[DP08]: Dziembowski, Pietrzak: Leakage-Resilient Cryptography in the Standard Model

[Pie09]: Pietrzak: A leakage-resilient mode of operation

[AGV09]: Akavia, Goldwasser, Vaikuntanathan: Simultaneous Hardcore Bits and Cryptography against Memory Attacks

[ADW09]: Alwen, Dodis, Wichs: Leakage-Resilient Public-Key Cryptography in the Bounded Retrieval Model

[FKPR09]: Faust, Kiltz, Pietrzak, Rothblum: Leakage-Resilient Signatures

[DHT09]: Dodis, Lovett, Tauman-Kalai: On Cryptography with Auxiliary Input

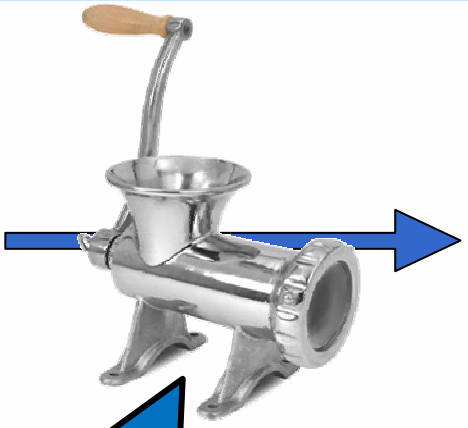
[SMY09]: Standaert, Malkin, Yung: A Unified Framework for the Analysis of Side-Channel Key-Recovery Attacks

...

Model

[Ishai Sahai Wagner '03]

Any boolean circuit

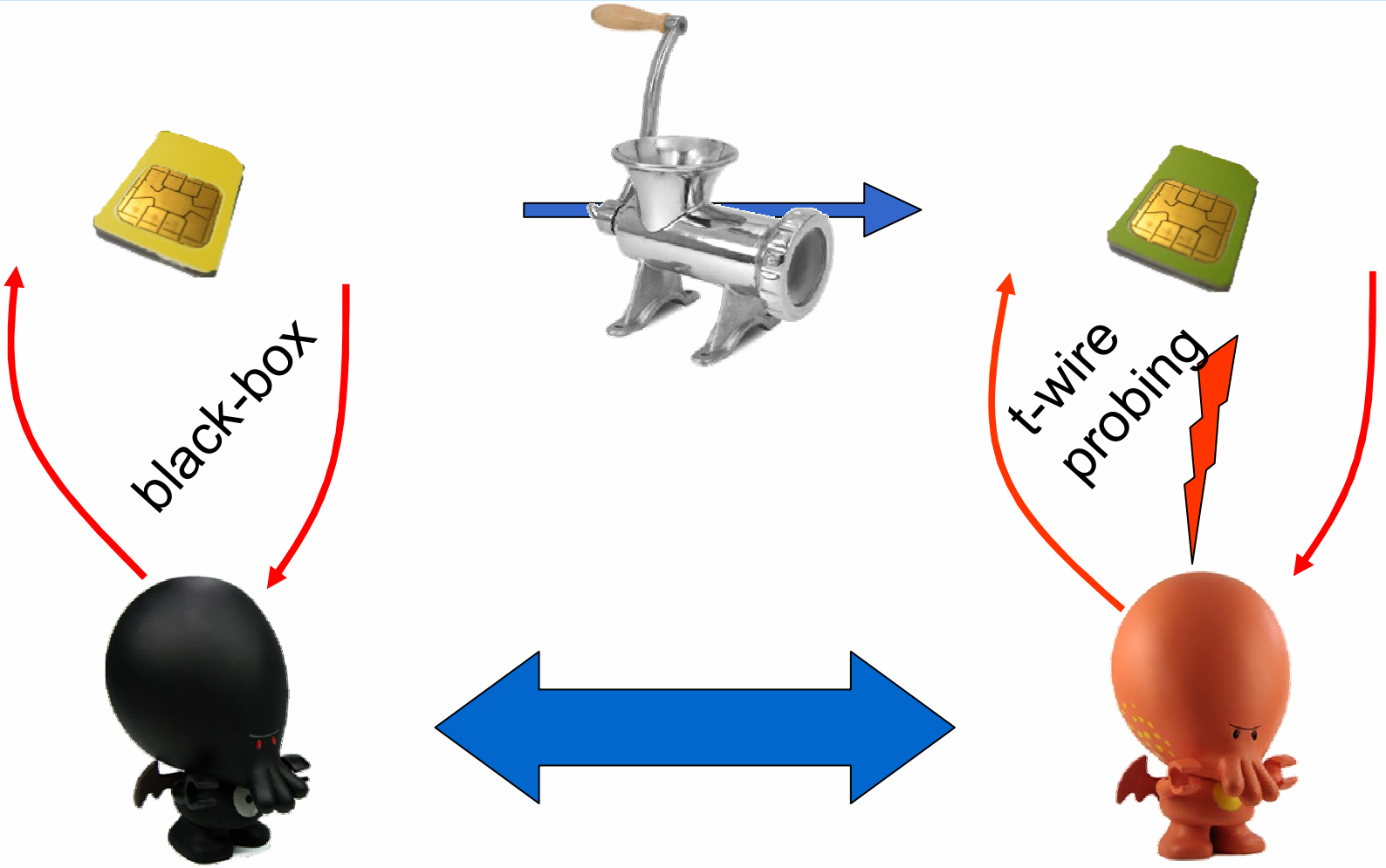


Circuit transformation

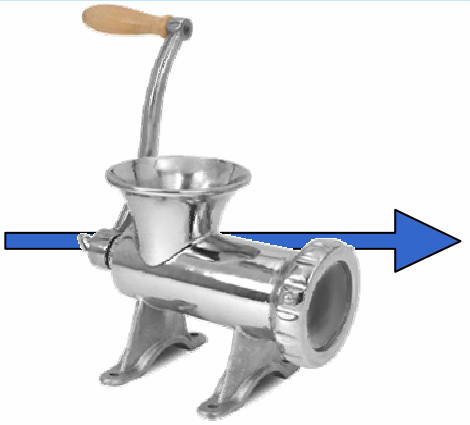
Transformed circuit

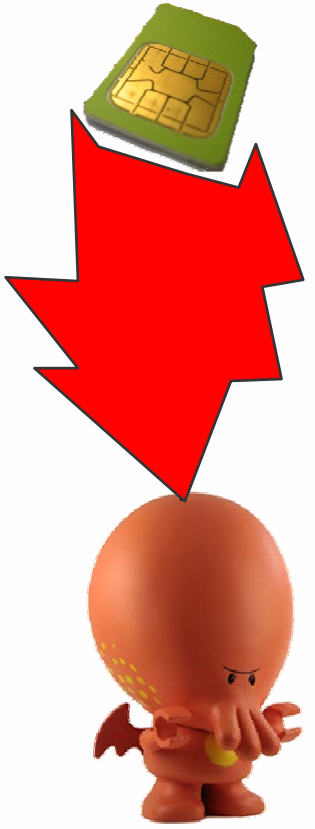
Model

[Ishai Sahai Wagner '03]



Our goal

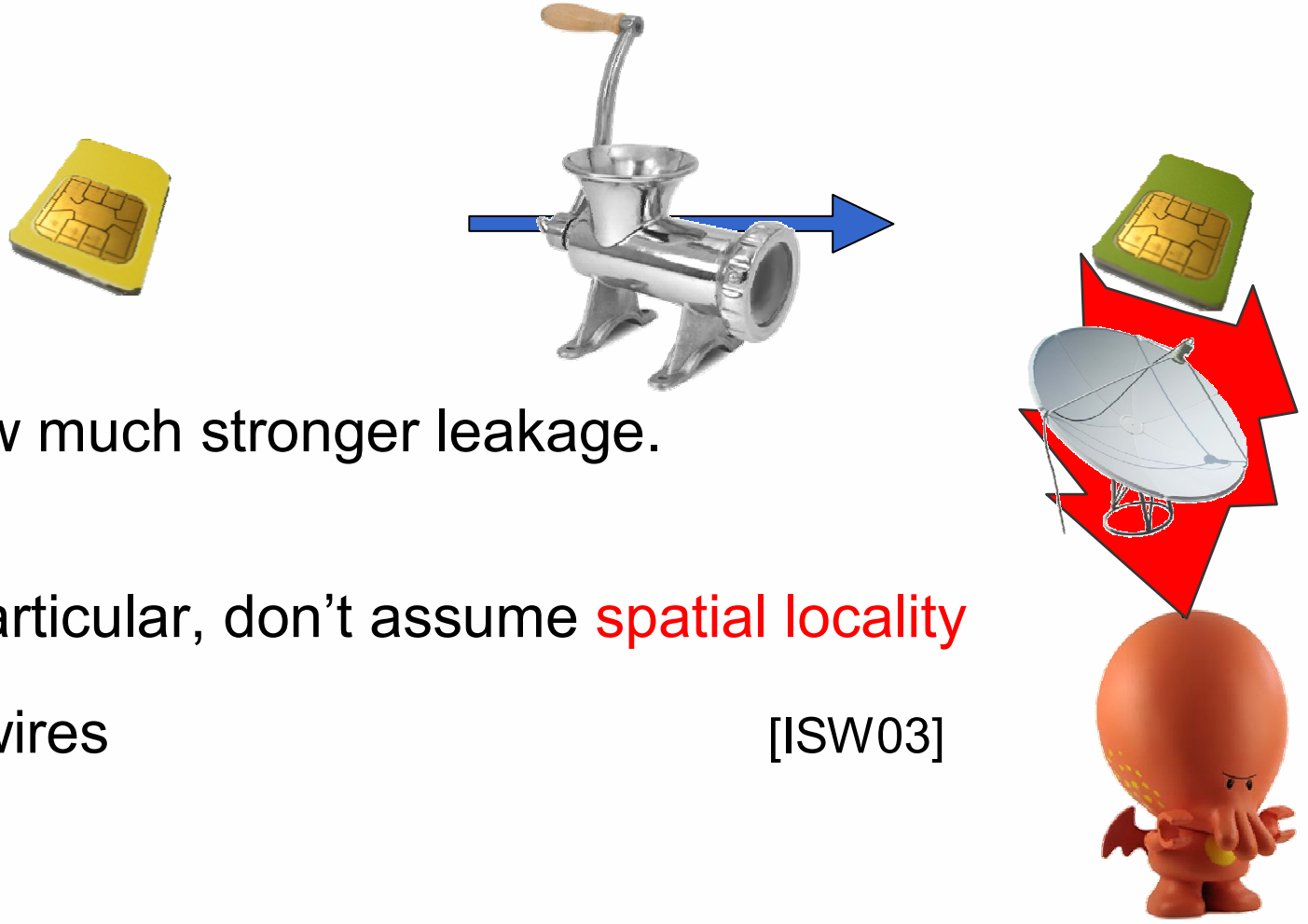




Allow much stronger leakage.

In particular, don't assume spatial locality

Our goal

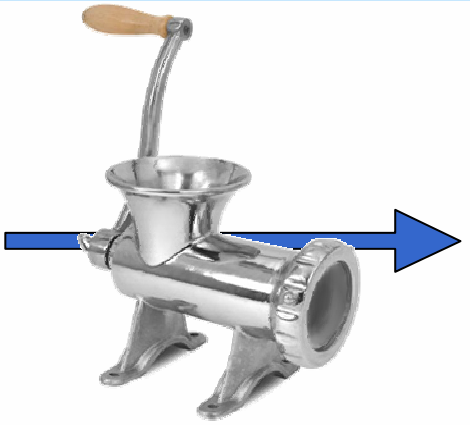


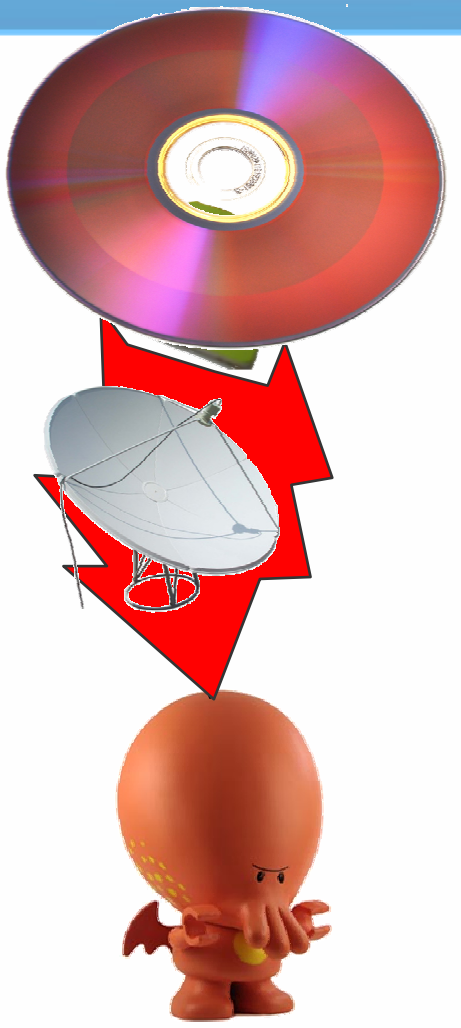
Allow much stronger leakage.

In particular, don't assume spatial locality

- t wires [ISW03]

Our goal



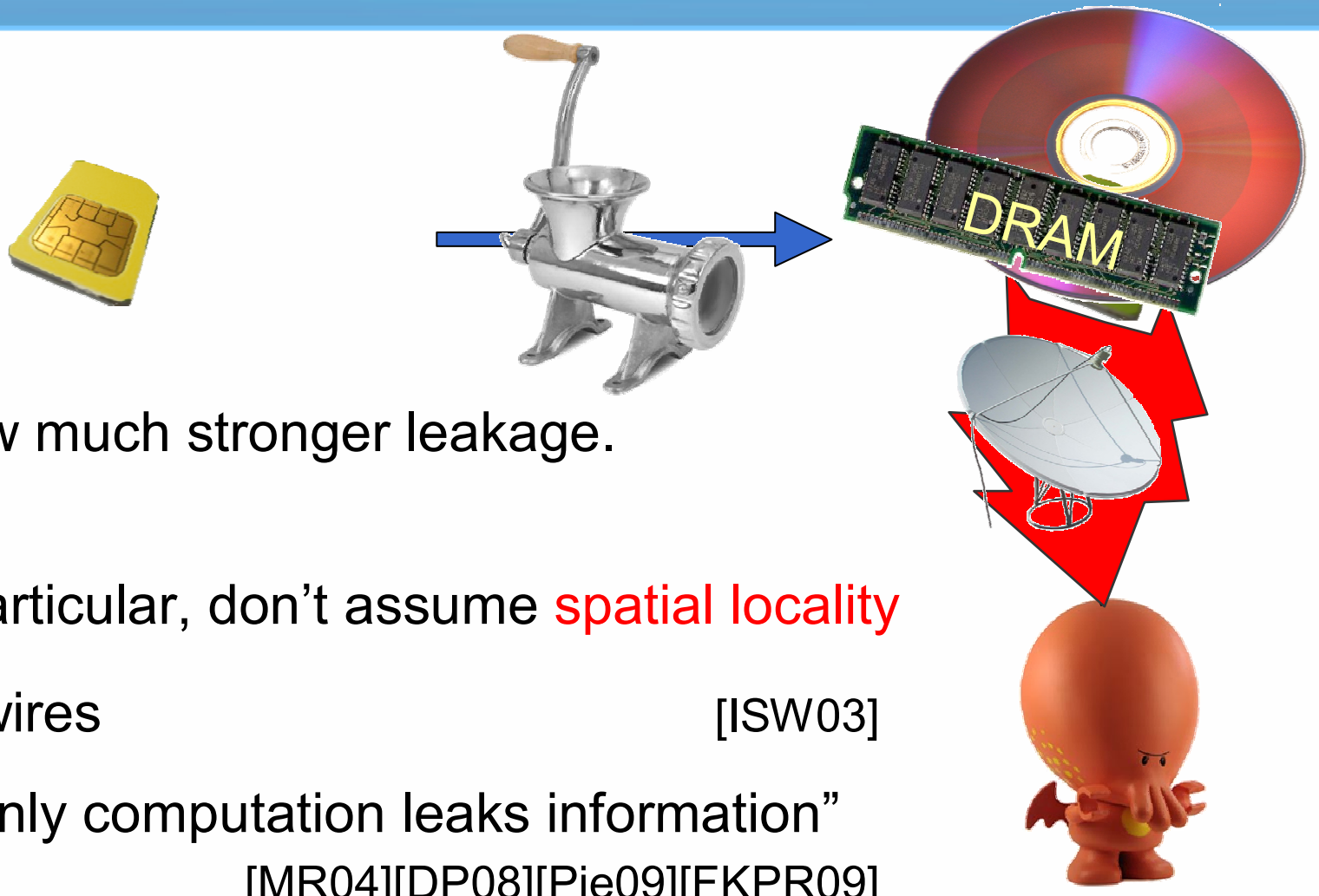


Allow much stronger leakage.

In particular, don't assume spatial locality

- t wires [ISW03]
- "Only computation leaks information" [MR04][DP08][Pie09][FKPR09]

Our goal



Allow much stronger leakage.

In particular, don't assume spatial locality

- t wires [ISW03]
- "Only computation leaks information" [MR04][DP08][Pie09][FKPR09]

Our main construction

A transformation that makes **any circuit** resilient against

- **Global adaptive leakage**
  May depend on whole state and intermediate results, and chosen adaptively by a powerful on-line adversary.
- **Arbitrary total leakage**
  Bounded just per observation. [DP08]

But we must assume something:

- **Leakage function is computationally weak** [∈MR04]
- **A simple leak-free component** [∈MR04]

Computationally-weak leakage

Computationally-weak leakage

Computationally-weak leakage

computationally weak

can be powerful

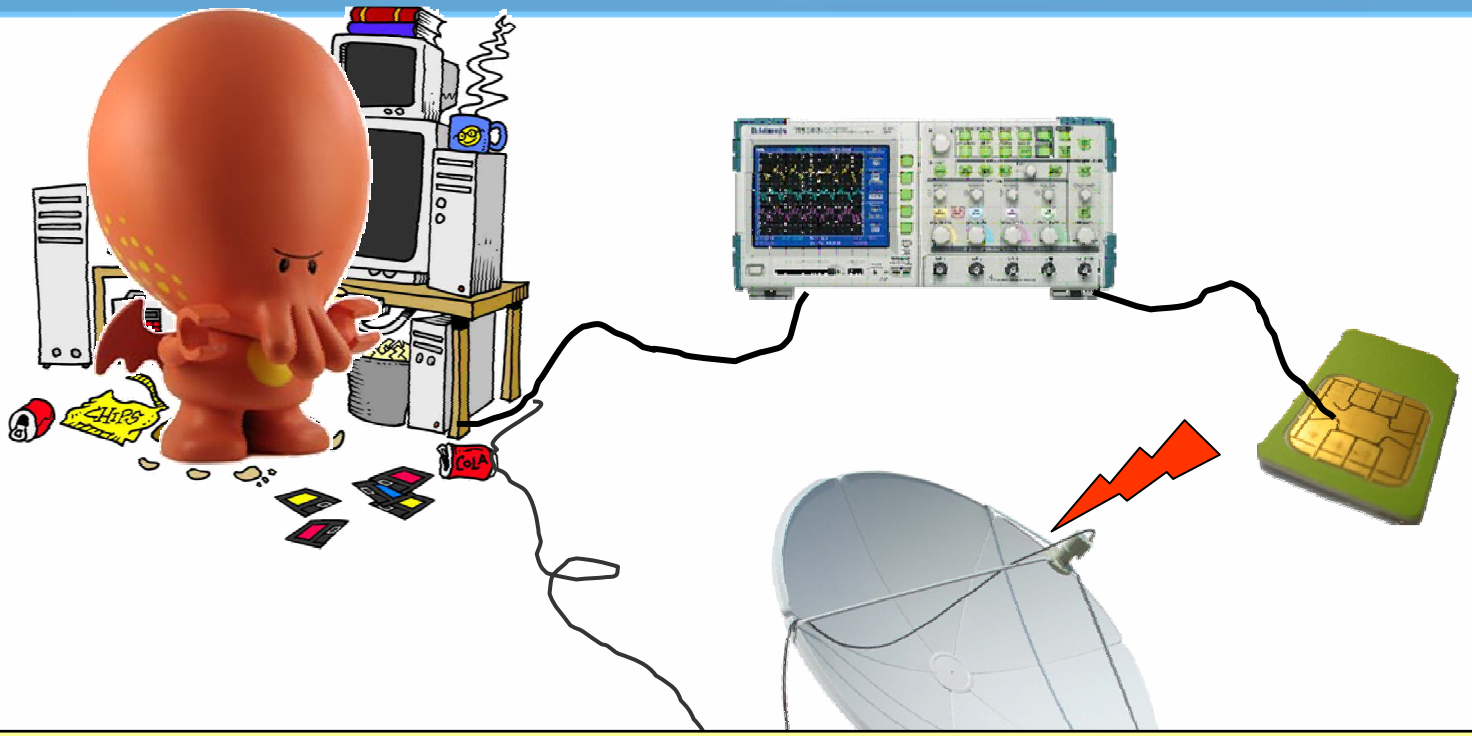
Computationally-weak leakage

computationally weak

can be powerful

“antennas are dumb”

Computationally-weak leakage

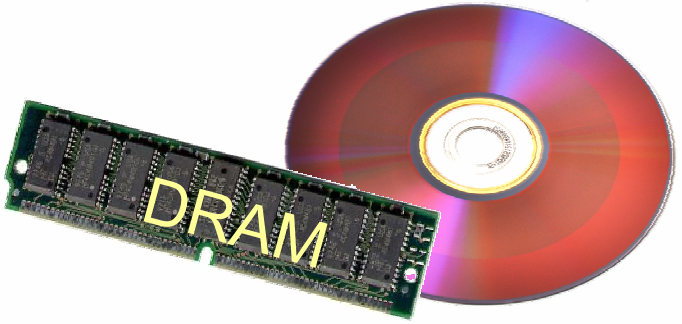


Assumption: the observed leakage is a computationally-weak function of the device's internal wires.

Leak-free components

- **Secure memory**

[MR04][DP08][Pie09][FKPR09]

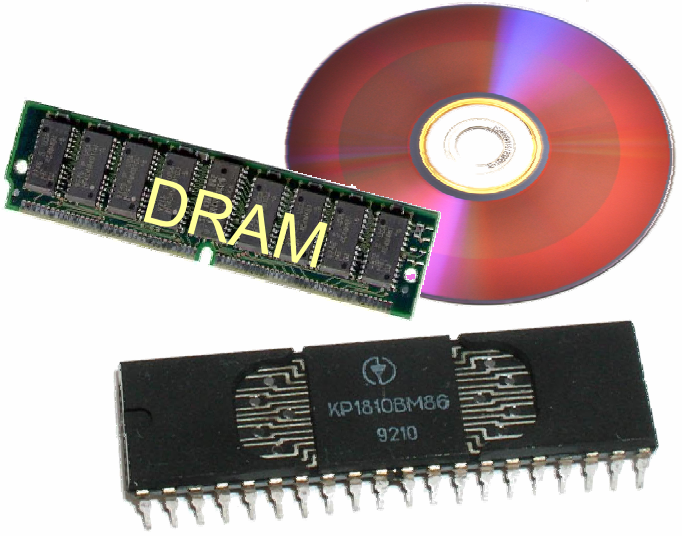


Leak-free components

- **Secure memory**

  [MR04][DP08][Pie09][FKPR09]

- **Secure processor** [G89][GO95]

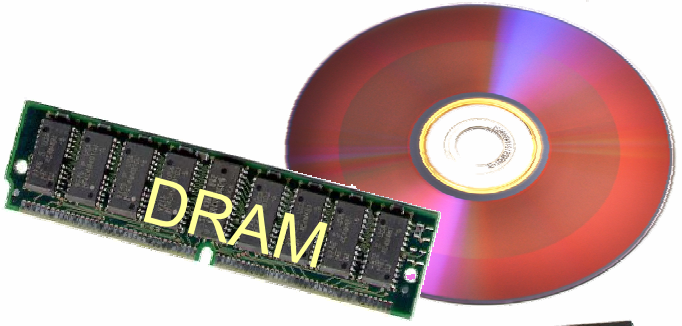


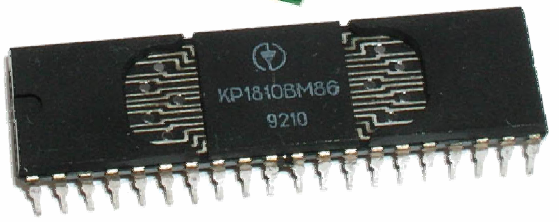
Leak-free components

- **Secure memory**

  [MR04][DP08][Pie09][FKPR09]

- **Secure processor** [G89][GO95]





- Here: simple component that samples from a fixed distribution, e.g: **draw strings with parity 0**.
  - No stored secrets or state
  - No input

    → consumable leak-free “tape roll”

Results

- Constructions for generic circuit transformation using linear secret sharing schemes.
  - Example: unconditional security against AC^0 leakge.
- Argue necessity of leak-free components
  (for "natural" constructions)
  by complexity-theoretic bounds/conjectures.
- General proof technique + additional applications.

http://eprint.iacr.org/2009/341