www.ccs.neu.edu/theory

Algorithms, Complexity, and Cryptography

Rajmohan Rajaraman

Ravi Sundaram

Emanuele Viola

Daniel Wichs

Visitor Yevgeniy Dodis (from NYU)

Spring 2013 Ph.D. cryptography class

Postdoc Chinmoy Dutta

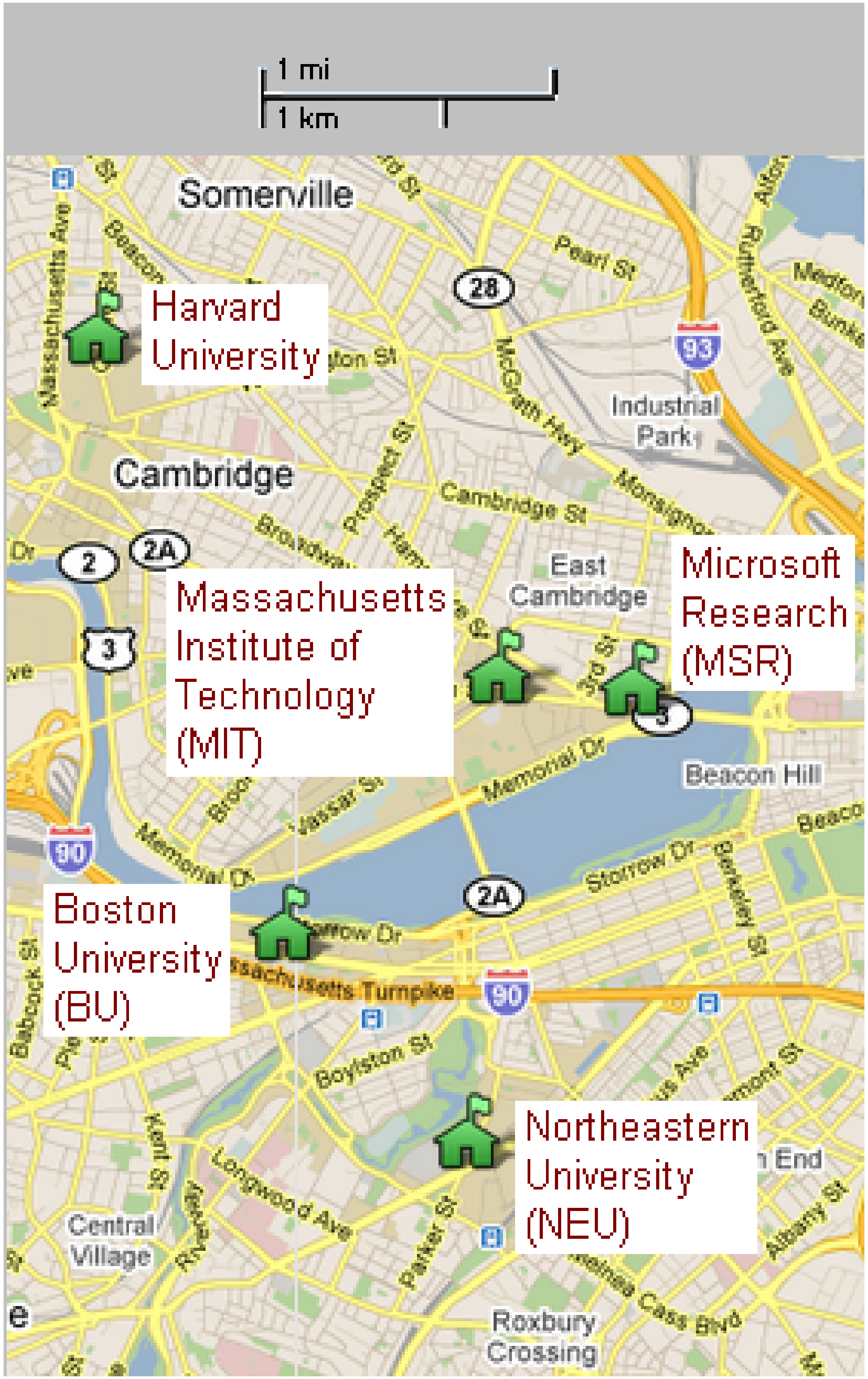
6 Ph.D. students

Theory in the Boston area

Overwhelming number of
talks,
seminars,
classes.

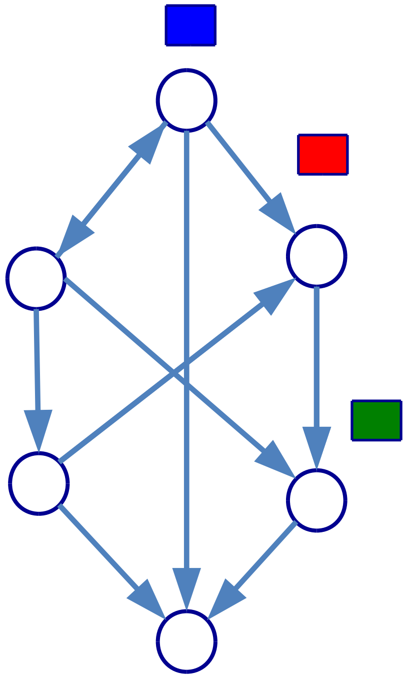
Students from other institutions come to NEU talks, classes

NEU students go there



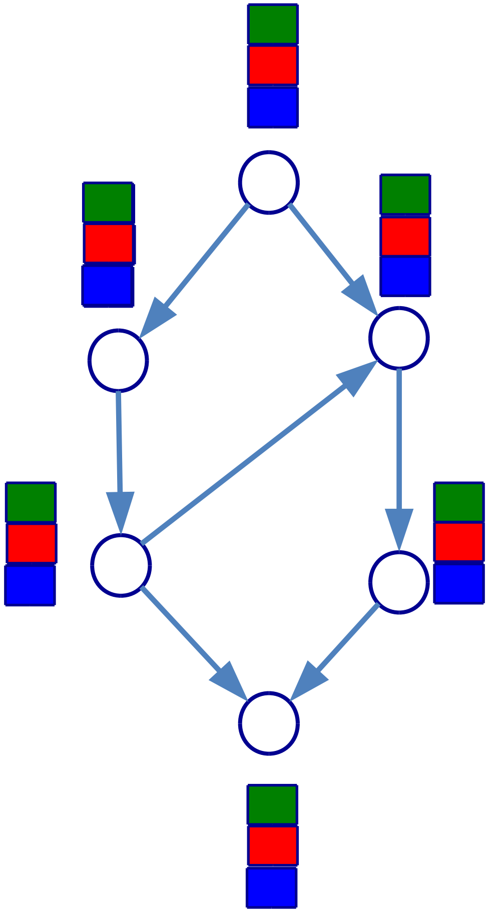
Some recent work done at NEU

Spreading in Dynamic Networks



Goal: Spread tokens 🟩🟥🟦 to all nodes of network

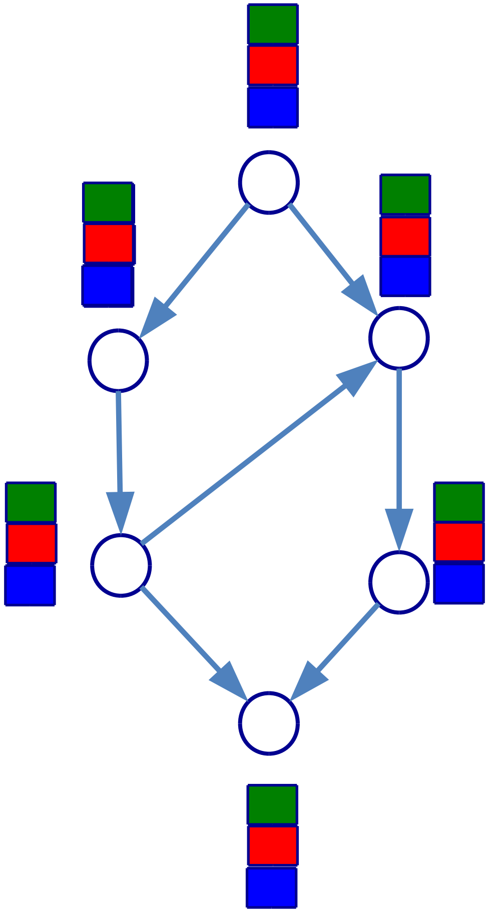
Spreading in Dynamic Networks



Goal: Spread tokens 🟩🟥🟦 to all nodes of network

- Dynamic setting: network changes every step

Spreading in Dynamic Networks

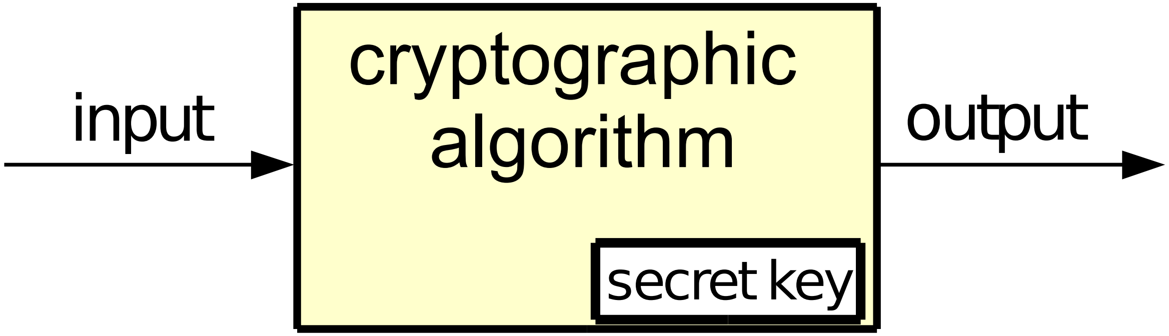


[Chinmoy Dutta
Gopal Pandurangan
Rajmohan Rajaraman
Emanuele Viola
Zhifeng Sun
SODA 2013]:

SYMM-DIFF algorithm for mixed token distribution.

Conjecture: works in general

Ideal crypto model: **black-box**



input

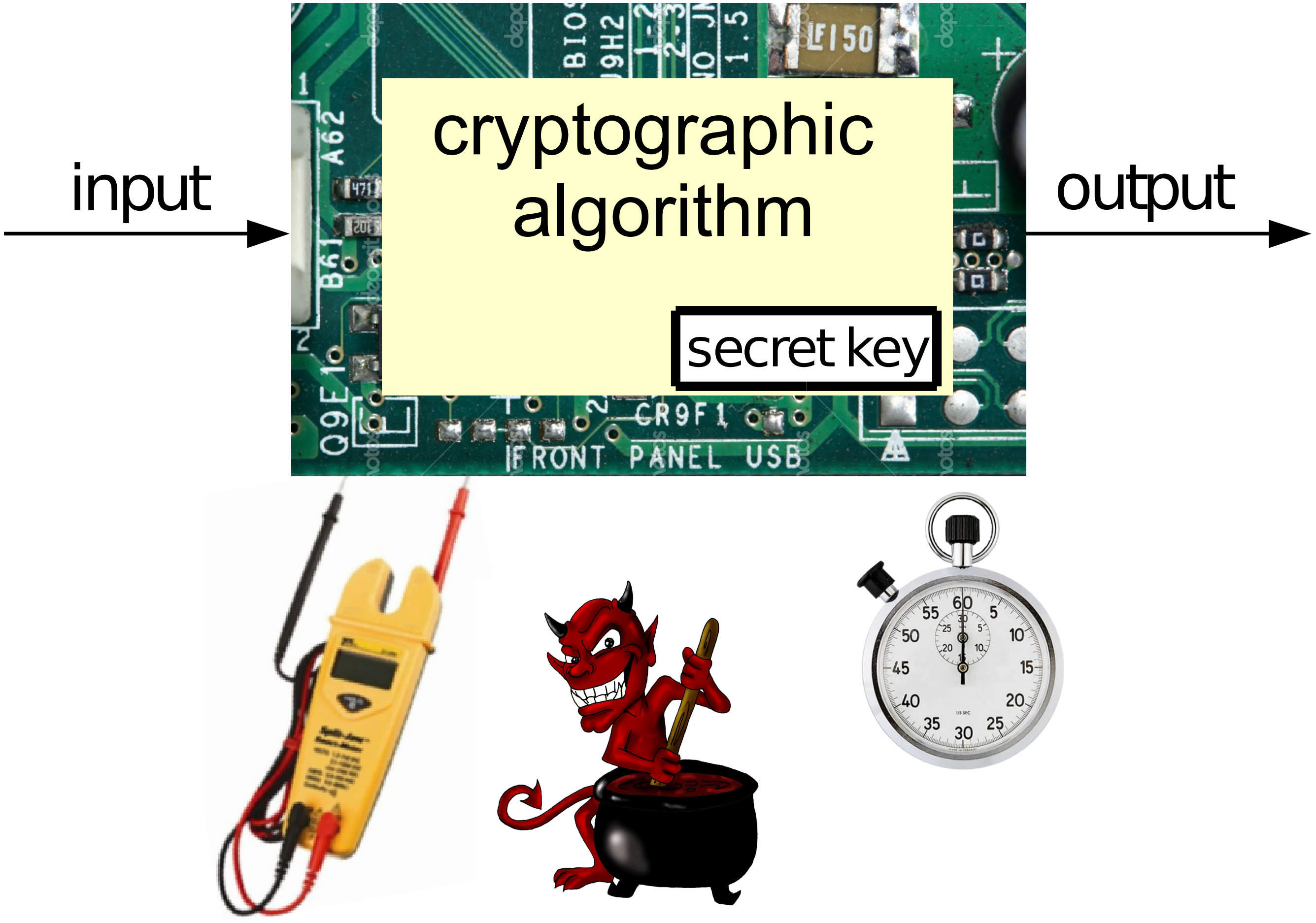
cryptographic algorithm

secret key

output

- adversary sees inputs/outputs
- but nothing more

Reality: algorithms run on hardware



input

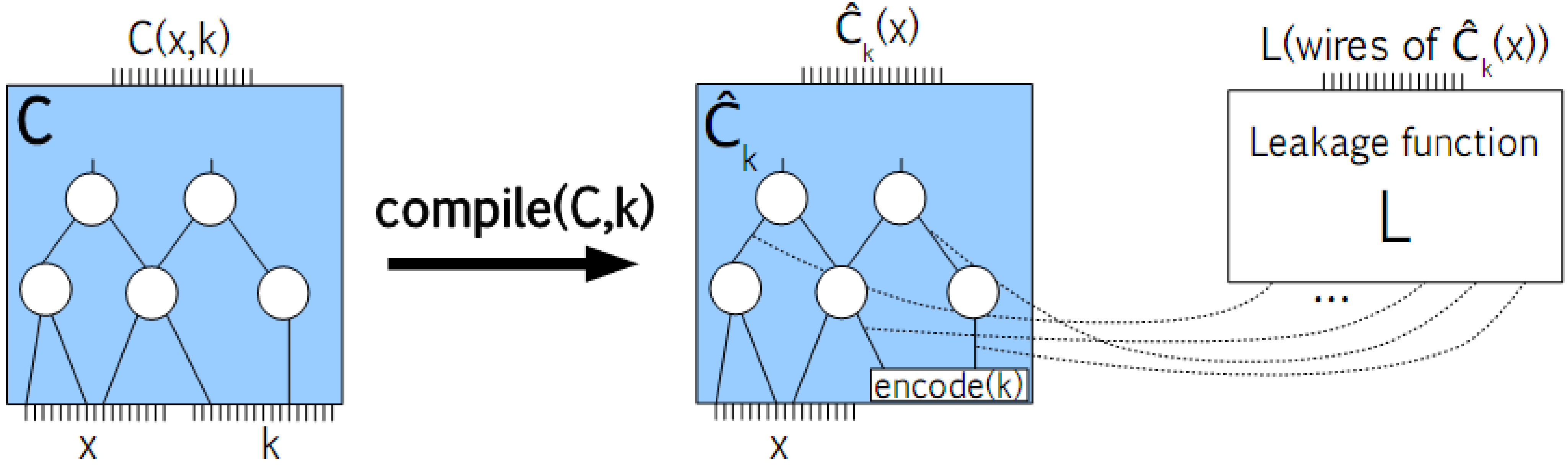
cryptographic algorithm

secret key

output

- hardware **leaks** information (side-channels)
- power consumption [Kocher-Jaffe-Jun '99], timing [Kocher '96], acoustics [Asonov-Agrawal '04], …

Leakage model



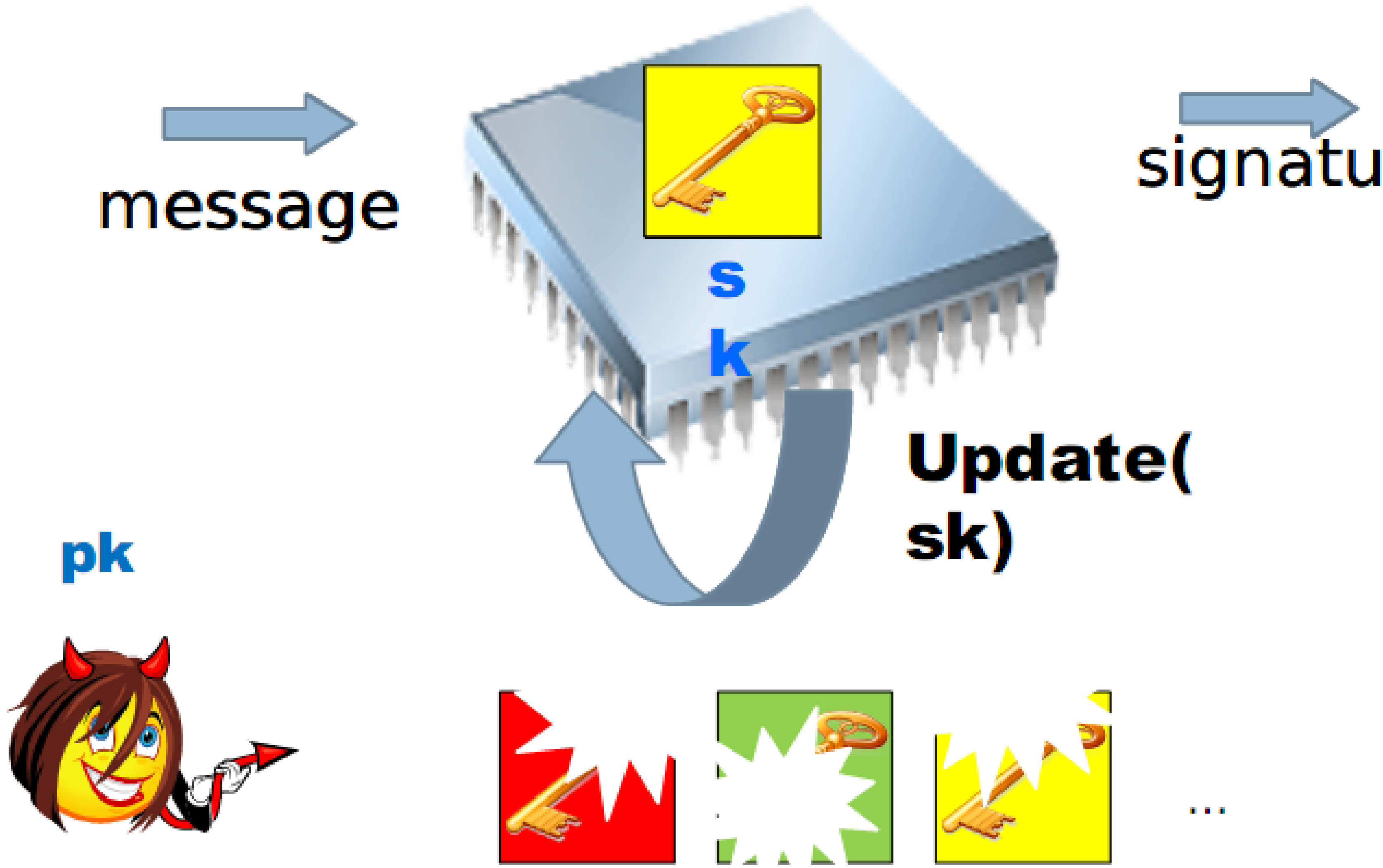
- <u>Adversary chooses</u>: x, L : $\{0,1\}^{|\hat{C}|} \rightarrow \{0,1\}^*$
- <u>Adversary sees</u>: C, $\hat{C}_k(x)$, L(wires of $\hat{C}_k(x)$)
- <u>Security goal</u>: leakage L “doesn't help”

$\exists$ simulator S, $\forall$x,k: $\Delta(L(\text{wires}), L(S(C, x, \hat{C}_k(x)))) \leq \text{negl}$
(Δ over compiler and simulator)

Continual Leakage

[Dodis Haralembiev Lopez Wichs FOCS10]

Signature Scheme



message

signature

sk

Update(sk)

pk

…

- [Miles Viola; STOC 2013]

State-of-the-art leakage resistance, for “one-shot”

- We construct circuits over a **group** G.
  - wires carry group elements
  - gates: mult. & inversion in G

- Main setting: **$G = A_5$**
  - elements: even permutations of {1, …, 5}