Fully Leakage-Resilient Signatures

Elette Boyle
MIT

Gil Segev
Weizmann Institute → MSR SVC

Daniel Wichs
NYU

Really, Really Leakage-Resilient Signatures

Elette Boyle
MIT

Gil Segev
Weizmann Institute → MSR SVC

Daniel Wichs
NYU

Cryptographic Leakage

[Encrypted message]

- Leakage-resilient encryption

  [DP08, P09, AGV09, NS09, AARDVARK09, DKL09, ADW09, DGKPV10, BG10, BKKV10,…]

Cryptographic Leakage

Very important declaration. *Bob*

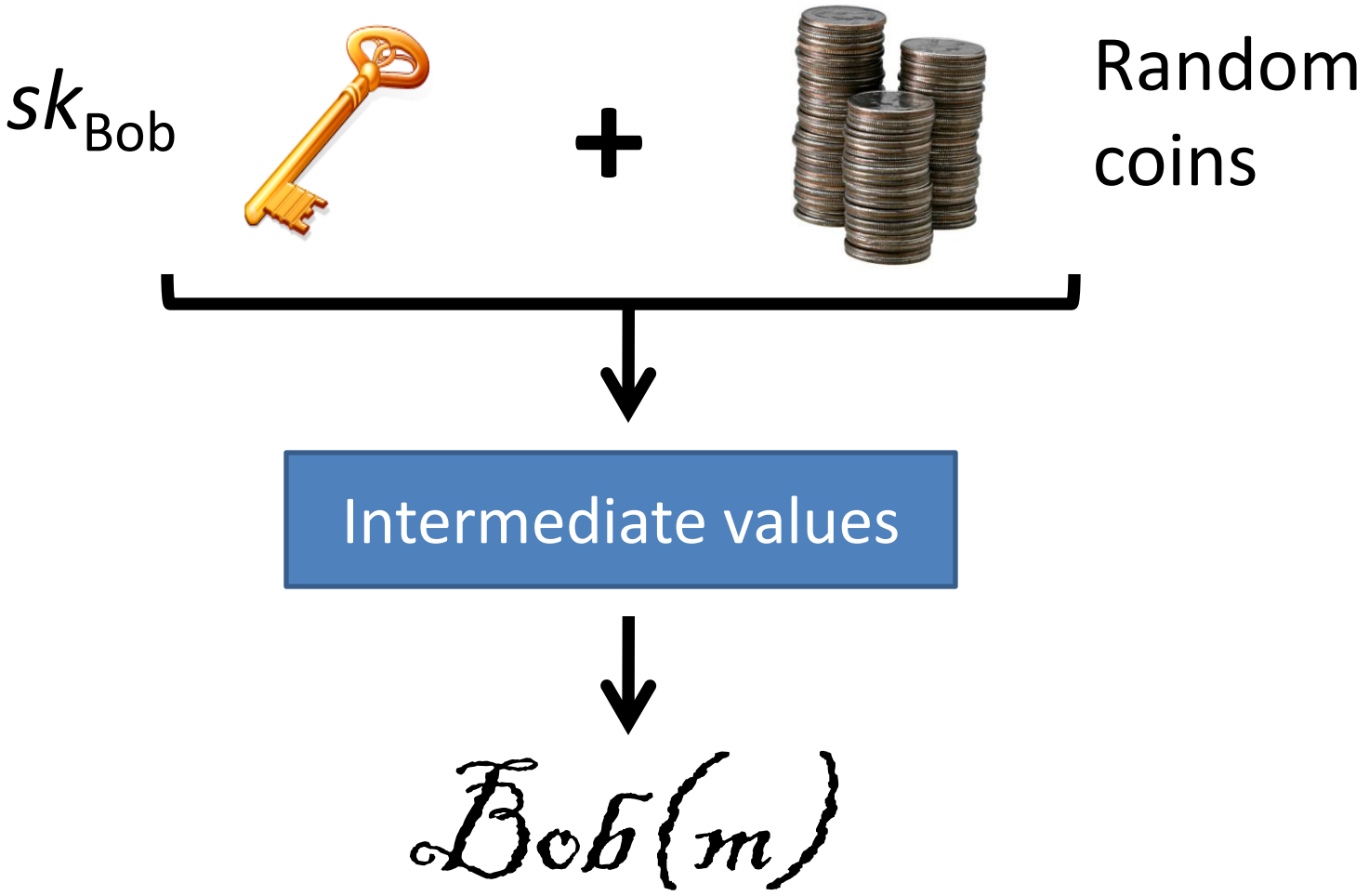
- Leakage-resilient encryption

  [DP08, P09, AGV09, NS09, AARDVARK09, DKL09, ADW09, DGKPV10, BG10, BKKV10,…]

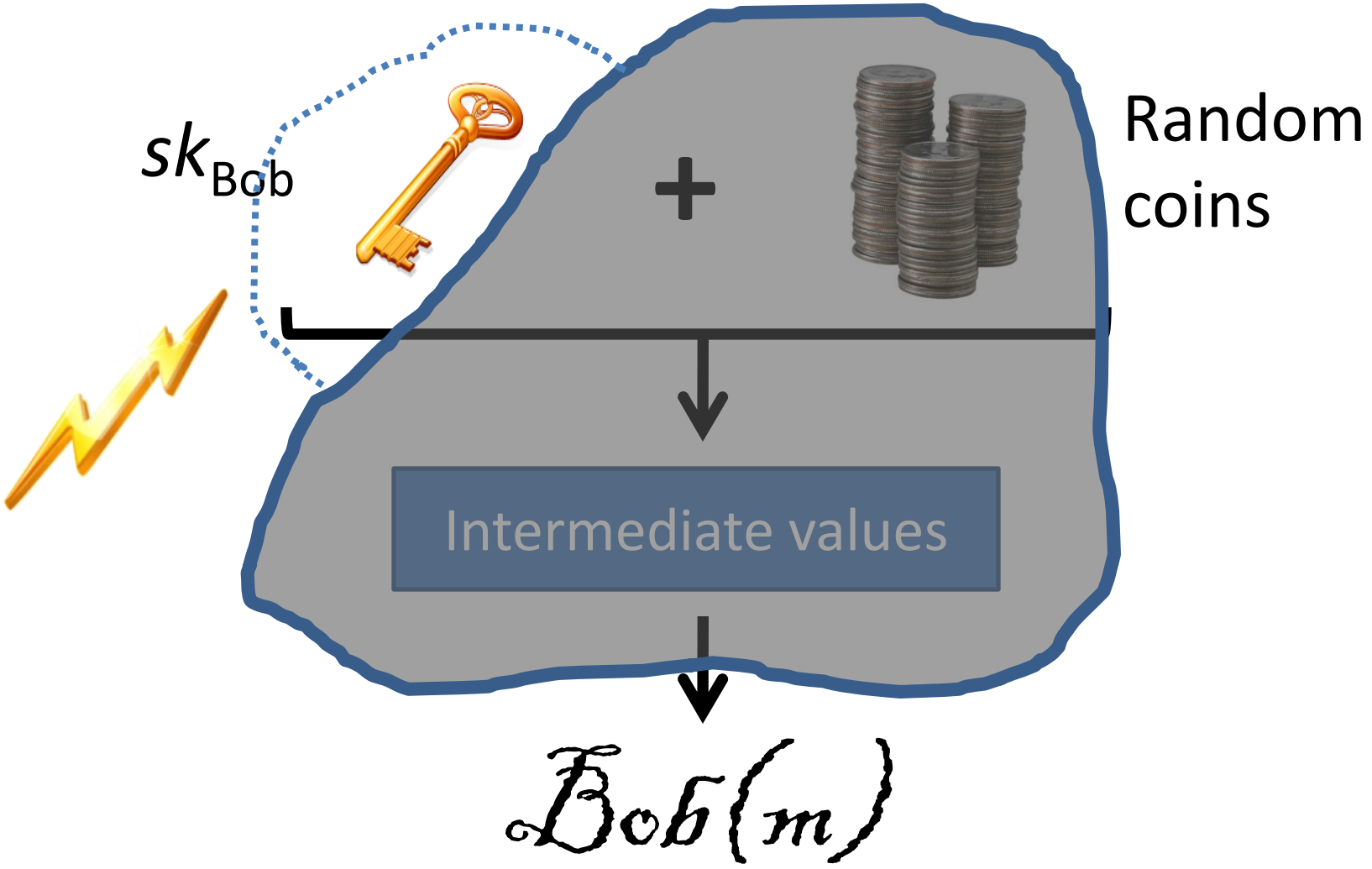
- Leakage-resilient signatures

  [KV09, ADW09, FKPR10, DHLW10, BKKV10]

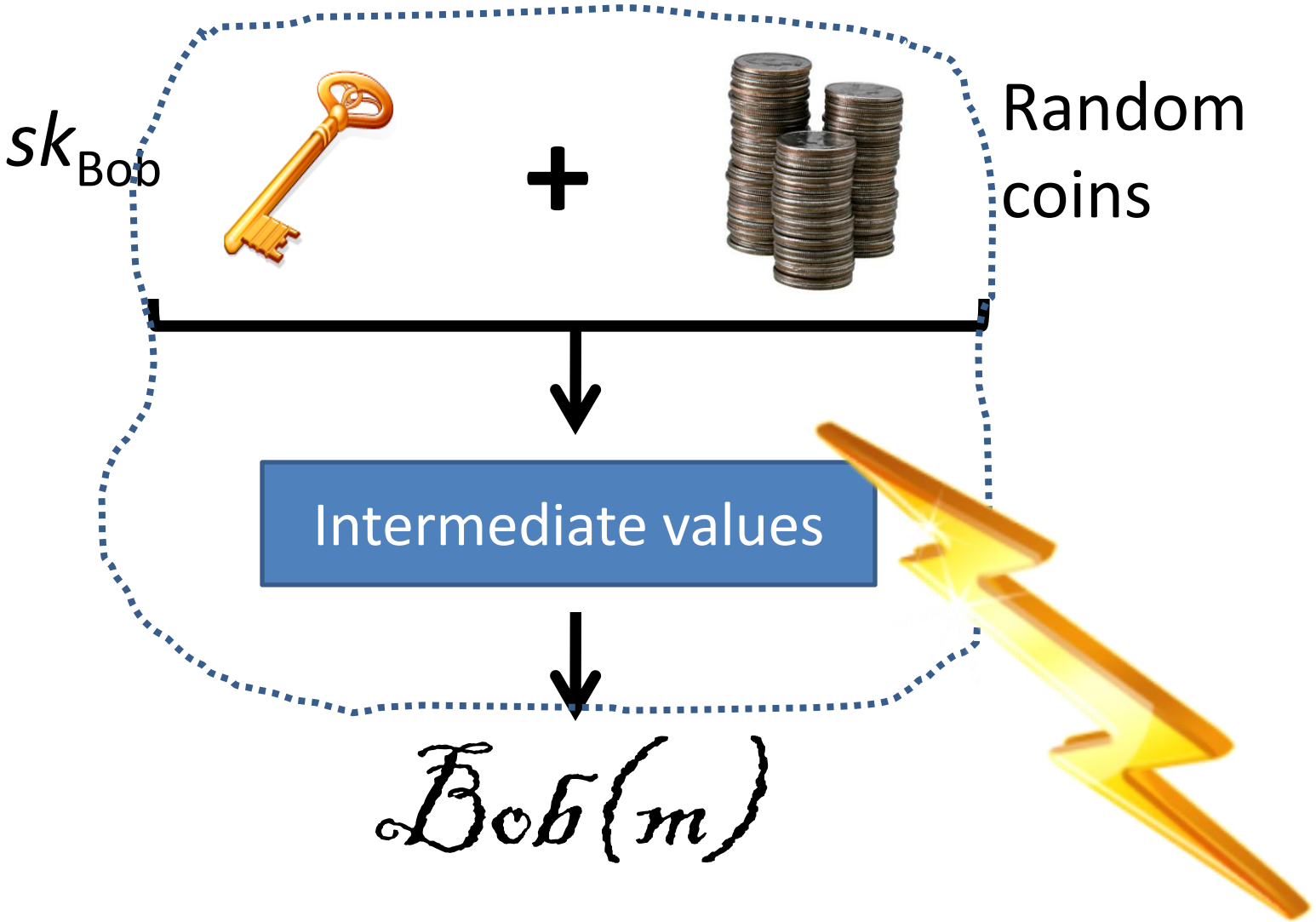
Modeling Signatures



Modeling Leaky Signatures



Modeling *Really* Leaky Signatures

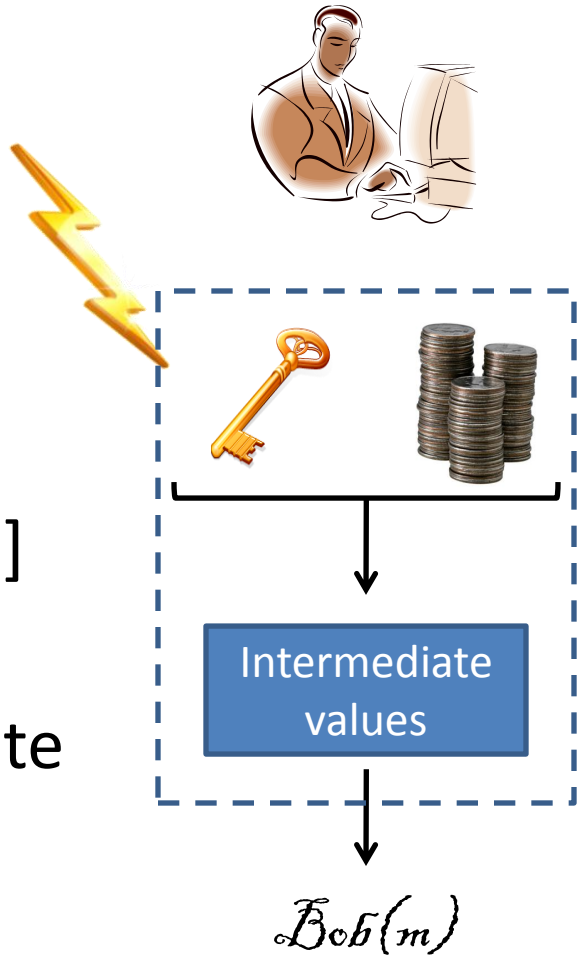


Previous Work

- **Fully** leakage-resilient
  - One-time signature [KV09]
  - Random oracles

    [KV09,ADW09,DHLW10,BKKV10]

** Leakage < L/2 or require key update every couple sigs **



Our Results

First fully leakage-resilient signatures in standard model

- Generic construction, efficient instantiation based on Linear Assumption
- Bounded-Leakage Model: up to $(1\text{-}o(1)) \cdot |sk|$
- Continual-Leakage Model: $(1\text{-}o(1)) \cdot |sk|$ per key update