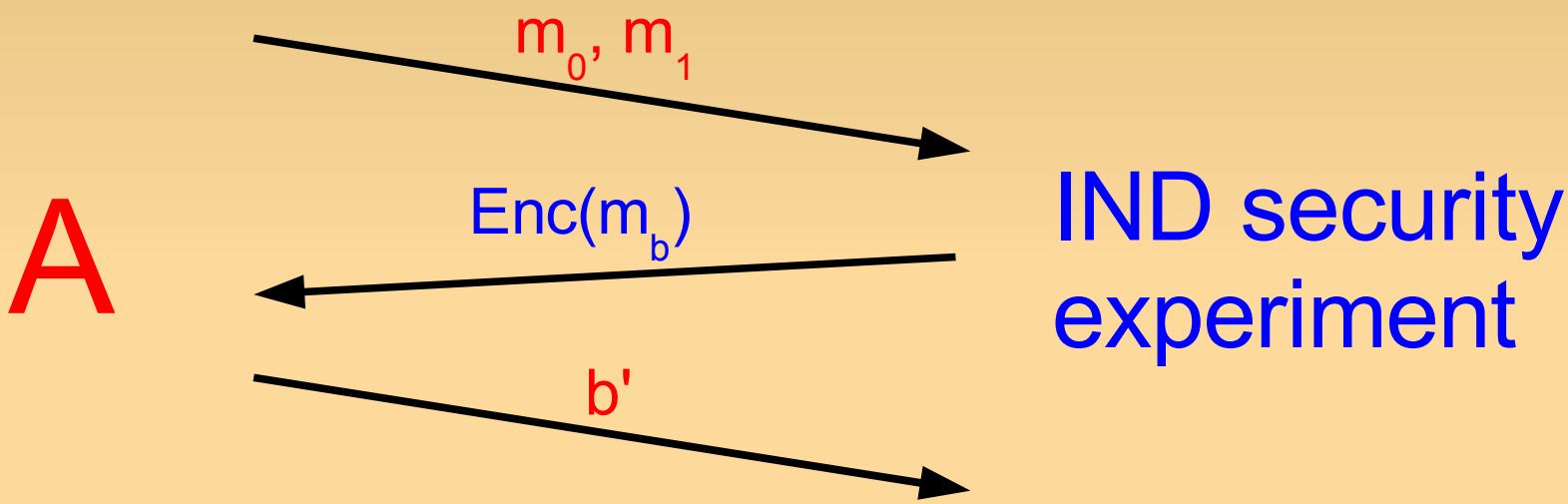
Towards Key-Dependent Message Security in the Standard Model

Dennis Hofheinz (CWI),
Dominique Unruh (Saarland University)

Encryption scheme security

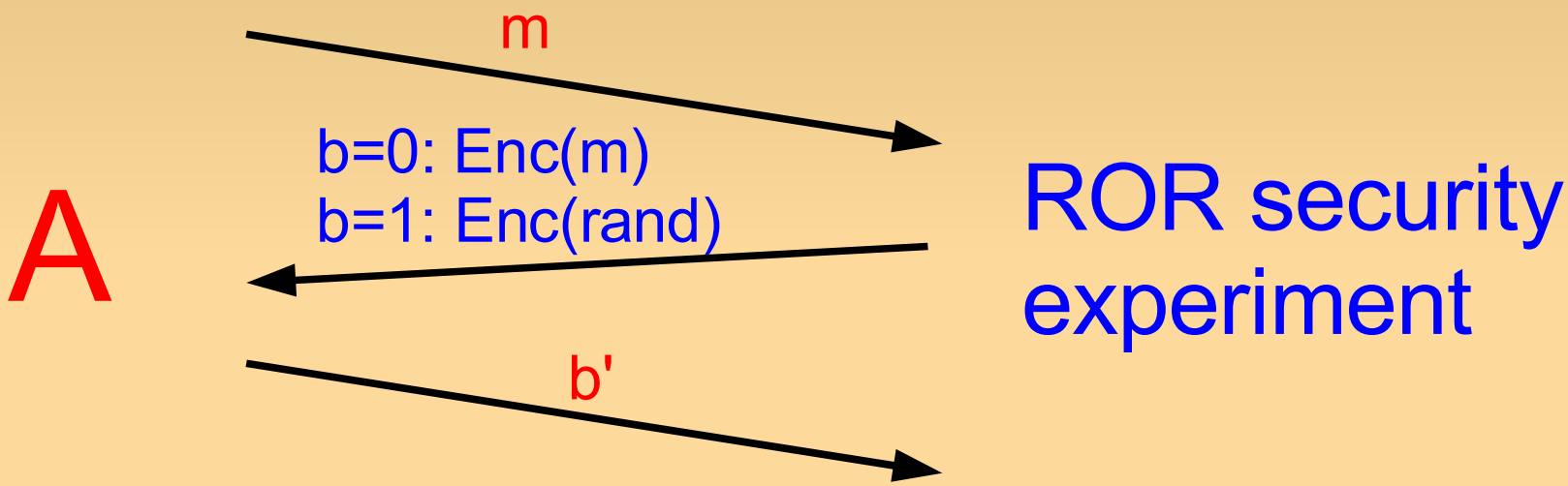
- Idea: two encryptions indistinguishable



- Scheme IND secure (IND-CPA/IND-CCA)
  ⇔ no A achieves Pr[b'=b]>1/2
- A also gets encryption oracle/public key

Encryption scheme security

- Equivalent to IND: ROR (real-or-random)



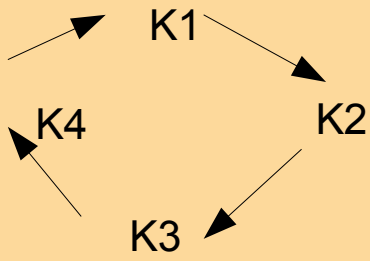
- Scheme ROR secure (ROR-CPA/ROR-CCA)
  ⇔ no A achieves Pr[b'=b]>1/2
- Multiple ROR queries allowed

Applications of IND/ROR

- IND/ROR-style definitions are elegant
  - Strict, reasonable, achievable, useful
- But: ...if you want to encrypt your hard drive?

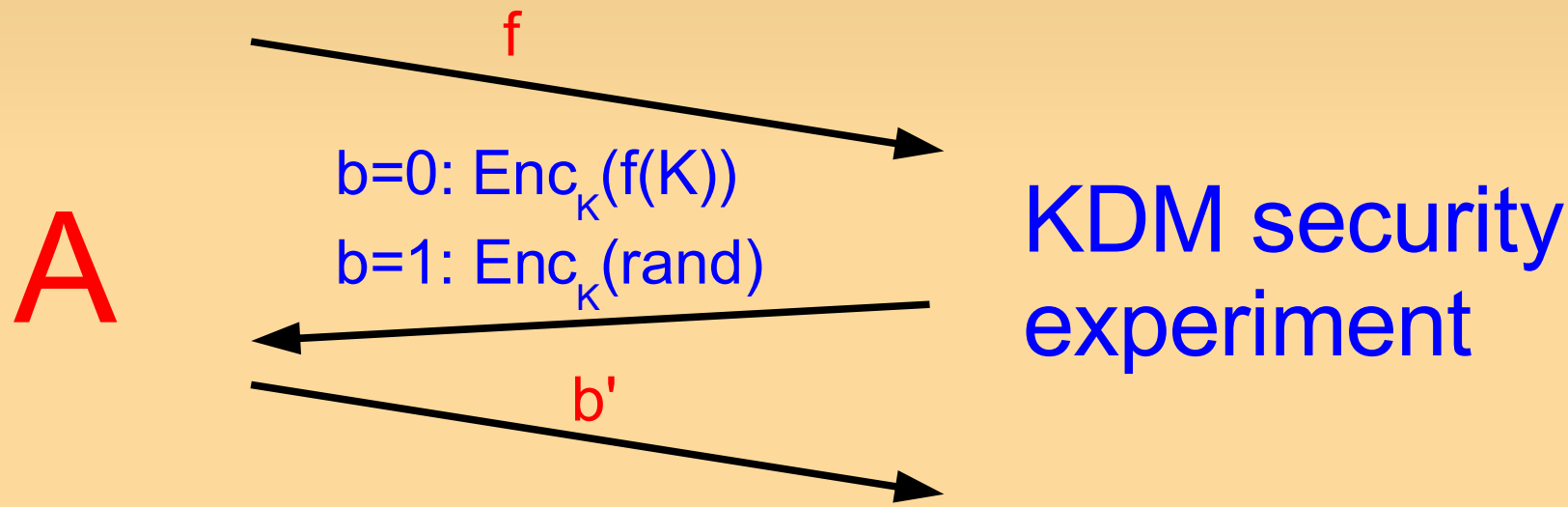
$$Enc_K(\ \text{  }\ )$$

- ...or your protocols have key cycles?
- IND-CCA does not help here!



Stronger: KDM security

- [Black, Rogaway, Shrimpton 2002]:
  - Reasonable to look at stronger notion:



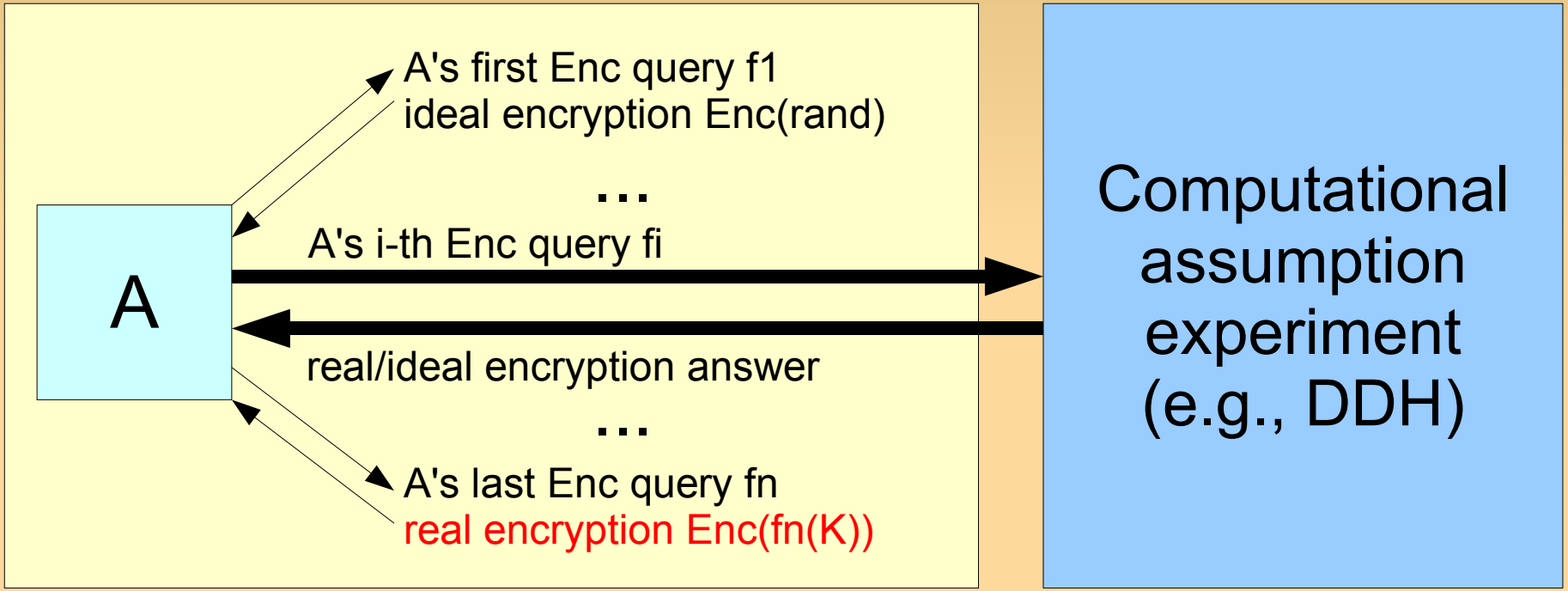
- A gets multiple queries
- Implies IND/ROR, good for use cases

KDM: previous work

- Soundness results (related assumptions)
  - Acyclicity assumptions (e.g. [Abadi, Rogaway 1998])
  - ...or security under key cycles (e.g. [Adao et al 2005])
- Key cycle security [Camenisch, Lysyanskaya 2001]
- KDM def/RO scheme [Black, Rogaway, Shrimpton 2002]
- Adaptive KDM [Backes, Pfitzmann, Scedrov 2006]
- Concurrent work: [Halevi, Krawczyk 2007]
  - Positive & negative results in **standard** model

KDM: hard to achieve

- Usual way hybrid arguments are done:

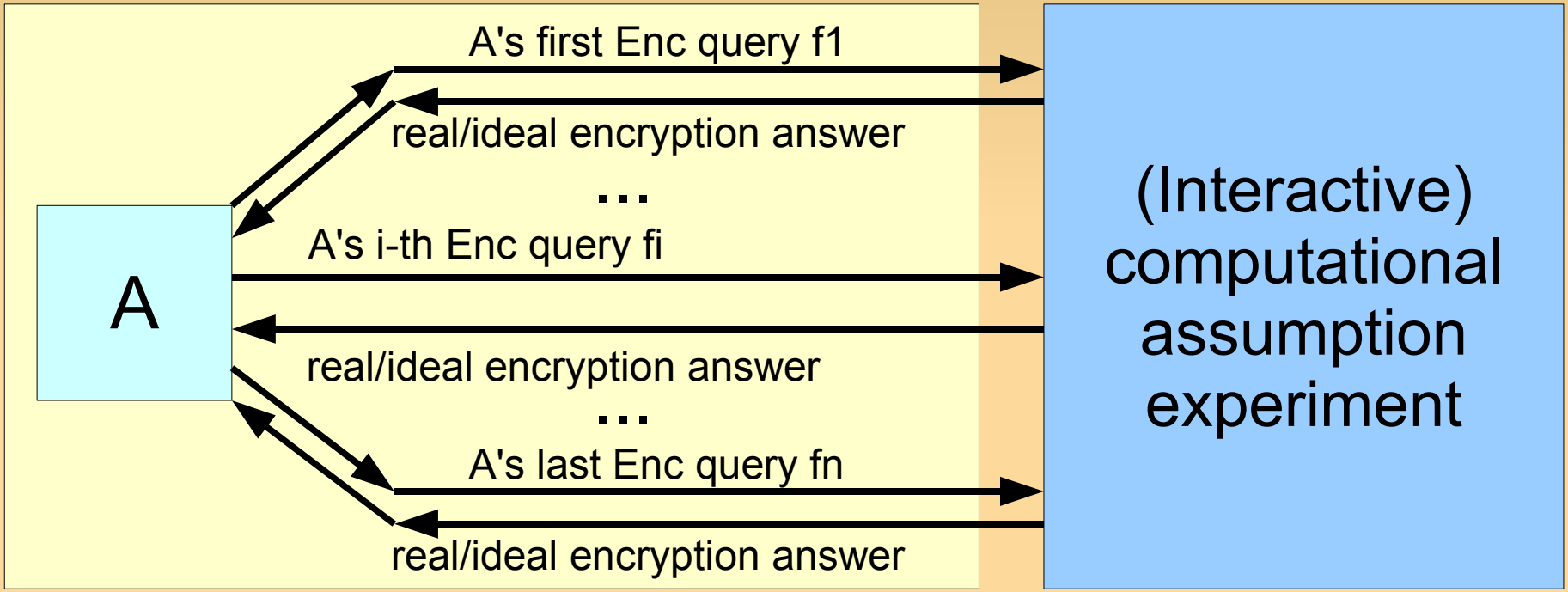


Reduced adversary B

- But: no way to simulate $Enc_K(f(K))$ in B

KDM in the standard model

- Possible but not interesting:



Reduced adversary B

- Security essentially **is** the assumption ☹

Weakening KDM

- KDM hard to achieve in standard model
- [BRS01] uses statistical RO properties
  - Analysis breaks down without independence of oracle queries
- Several weakenings of KDM imaginable
  - Smaller class of allowed dependencies (i.e., functions f) [Halevi, Krawczyk 2007]
  - Bound number of encryptions (this talk)
  - Or: consider stateful schemes (this talk)

Idea: bounded KDM security

- Setting: KDM with bounded # encryptions
  - Idea: if key is sufficiently bigger than **all** encryptions
    then key always contains enough entropy
    such that entropy smoothing works
  - Example scheme:

$$Enc_K(m) = (h, h(K) + m)$$

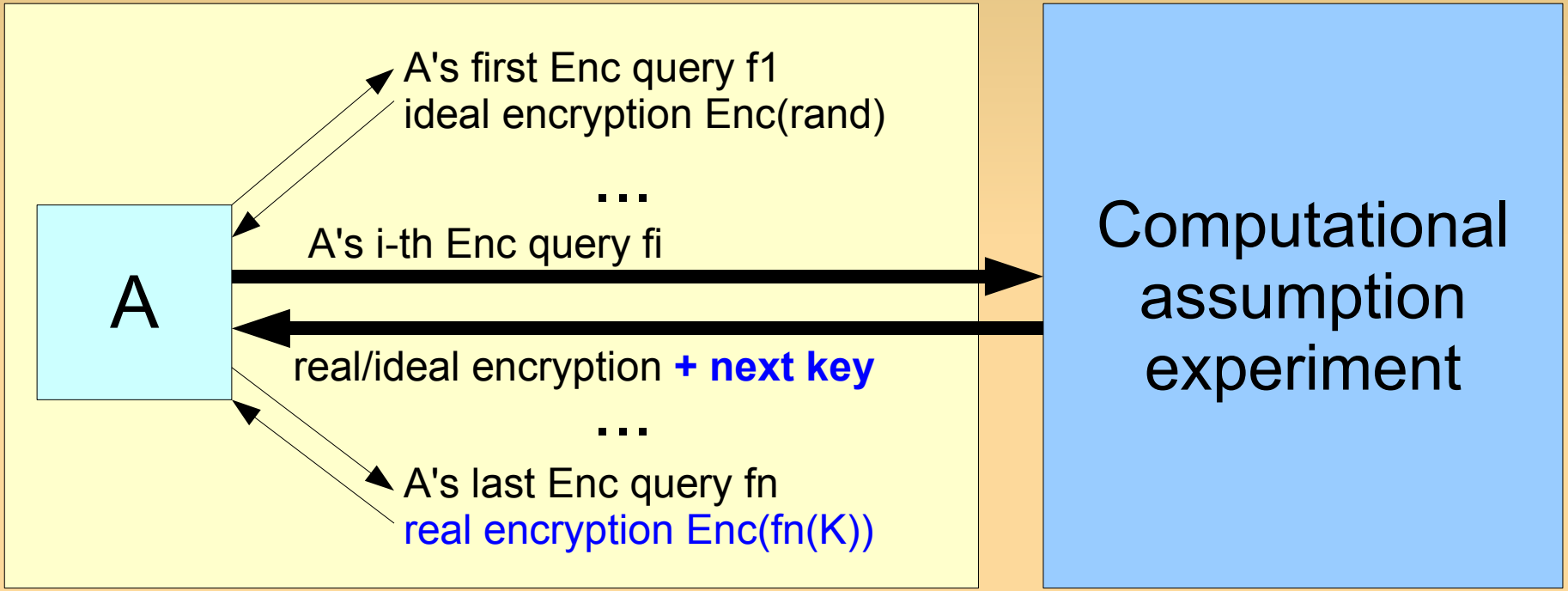
  - If $|K| > |m| (2n+3)$ (where n= # encryptions)
    then this scheme is KDM secure (statistically)

Idea: stateful schemes

- Intuition: update state after encryption
  - State/key before i-th encryption: K_i
- Two options:
  - Weak stateful KDM: trusted erasures ($f_i=f_i(K_i)$)
  - Strong stateful KDM: no erasures ($f_i=f_i(K_1,...,K_i)$)
  - No bound on # encryptions!
- We can achieve weak (but not strong)

Idea: stateful schemes

- Idea: weak stateful KDM allows hybrids:



Reduced adversary B

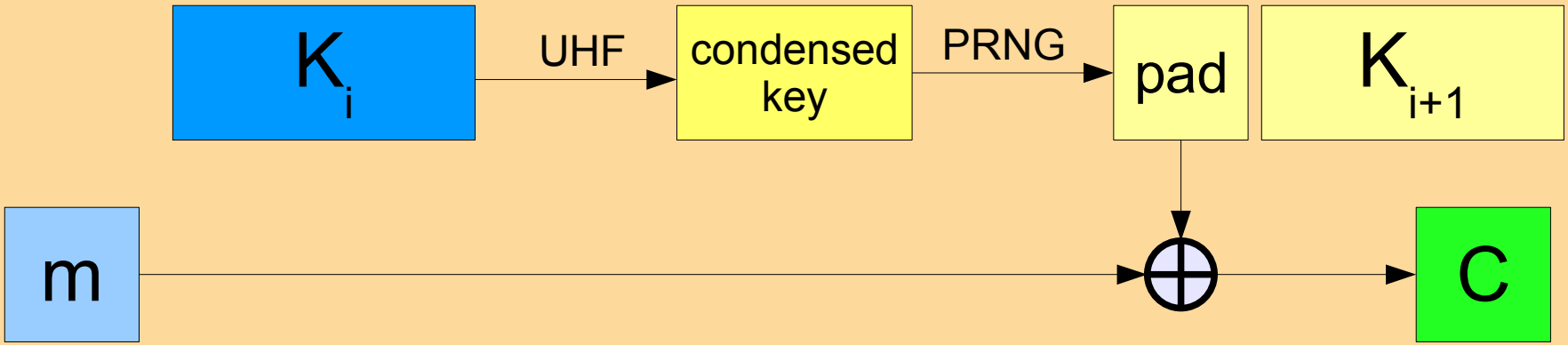
- ”Direction” of hybrid argument matters!

Idea: stateful schemes

- Scheme (entropy smoothing + PRNG):

$ENC_{K_i}(K_i,m)$:

1. randomly pick UHF h
2. condensed_key = $h(K_i)$
3. (pad,K_{i+1}) = PRNG(condensed_key)
4. C = (h , pad + m)



Strong stateful KDM security?

- Setting: message depends on all previous keys:

$$f_i = f_i(K_1, \ldots , K_i)$$

- Hybrid argument trick as before doesn't work
  - Reason: to produce any encryption, need K_1
- Still: very attractive goal (→ use cases)
  - Strong stateful KDM is weaker than full KDM...
  - ... but but for use cases, just as good

Conclusion

- KDM in standard model hard (but intriguing)
  - One-to-many encryptions/keys w/o hybrids
- Our approach: weaken security notion
  - Bounded # encryptions
  - Stateful schemes with trusted erasures
- Open: how to achieve full KDM security w/o RO
  - ...or strong stateful KDM security
  - ...or at least security in presence of key cycles
  - Different assumption? Impossibilities?