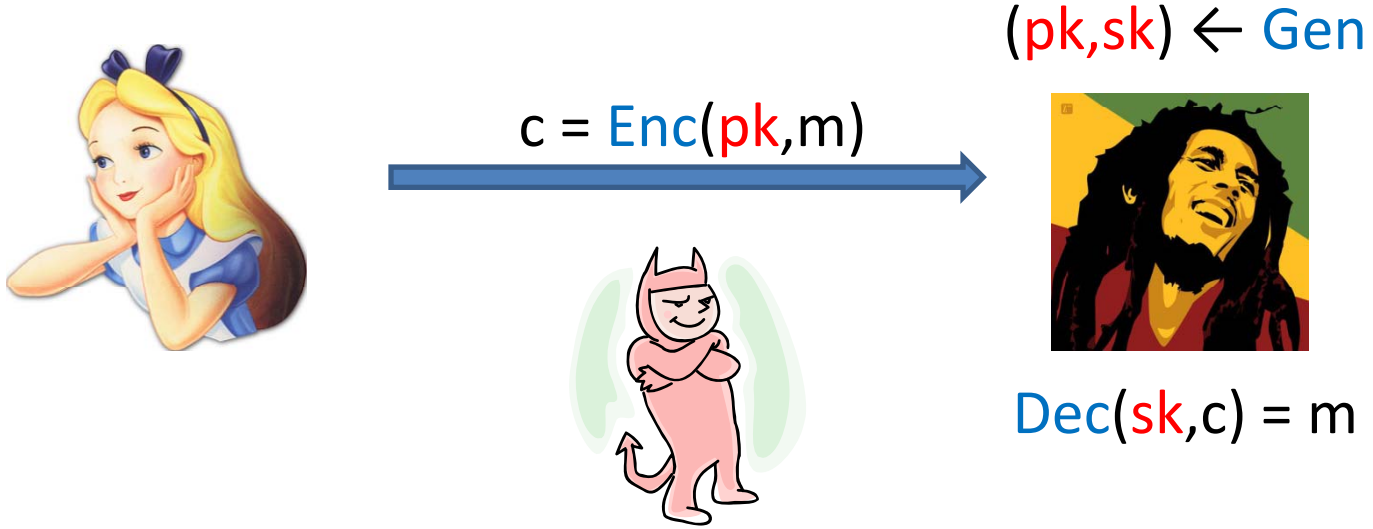
Cornell University

Randomness-Dependent Message Security

Eleanor Birrell Kai-Min Chung Rafael Pass Sidharth Telang

Public key Encryption

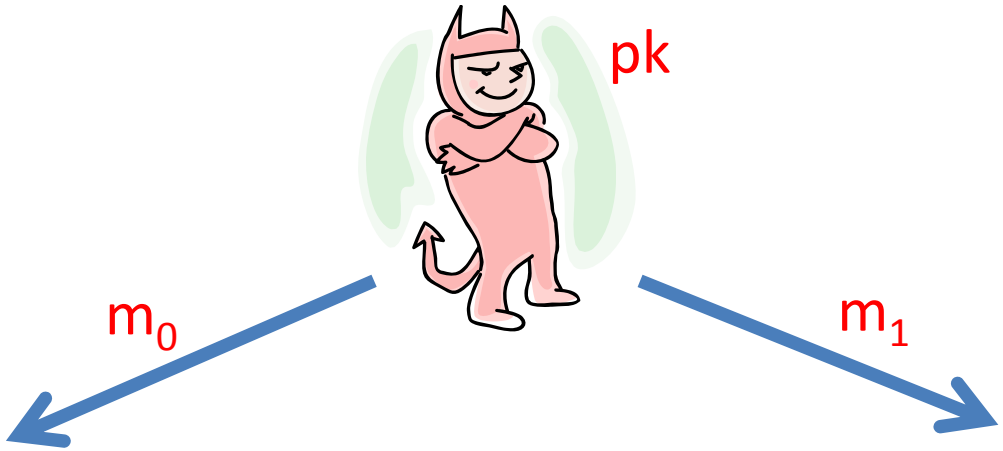
- Goal:



Encryption scheme (Gen, Enc, Dec)

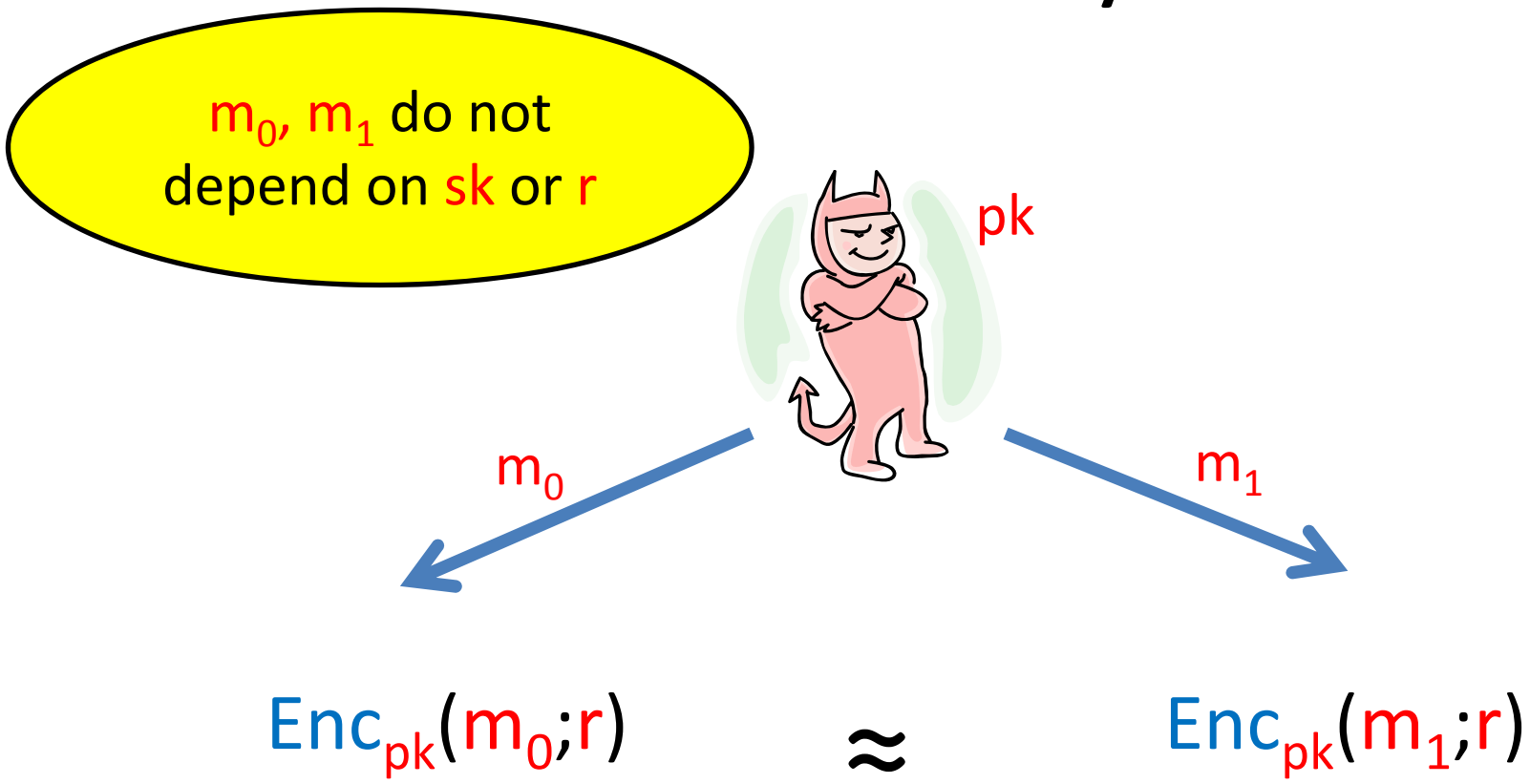
Formal security: CPA/CCA

CPA security



$$\mathrm{Enc}_{pk}(m_0;r) \approx \mathrm{Enc}_{pk}(m_1;r)$$

CPA security



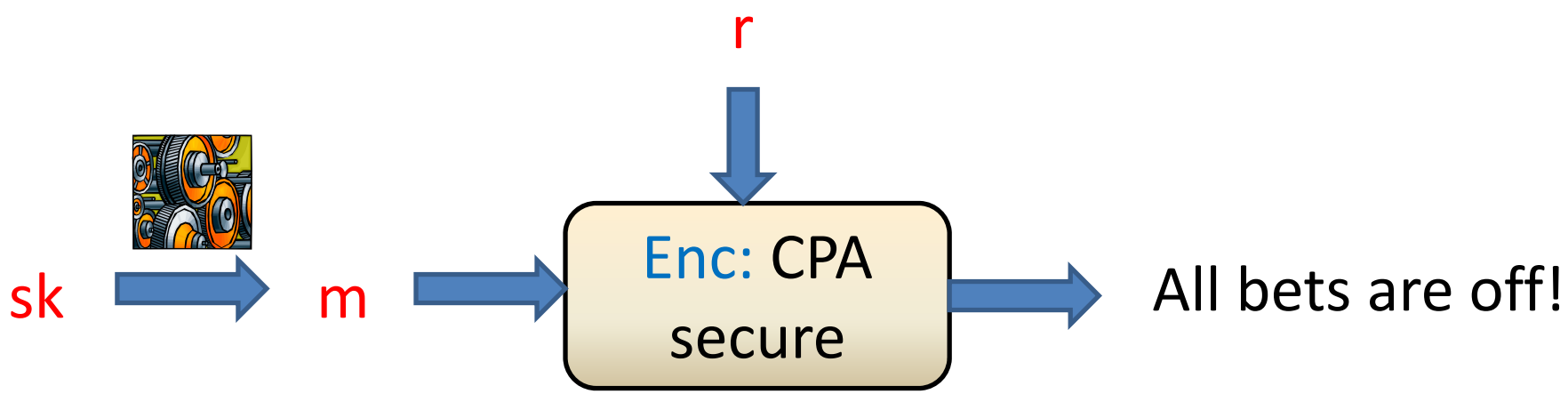
m_0, m_1 do not depend on sk or r

Good for many settings

Not good for some

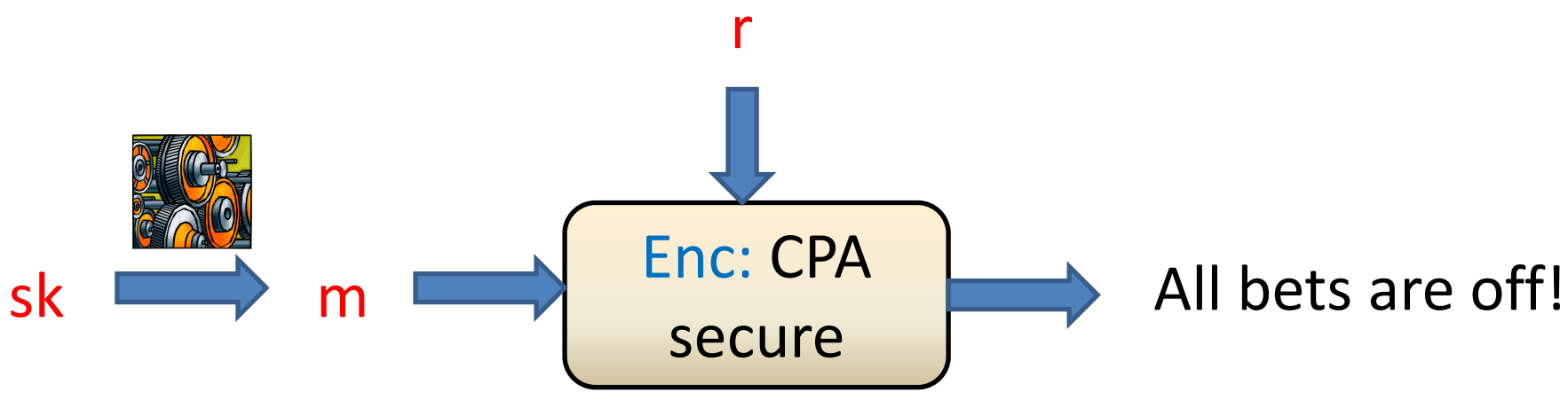
m_0, m_1 do not depend on sk or r

Good for many settings
Not good for some



m_0, m_1 do not depend on sk or r

Good for many settings
Not good for some



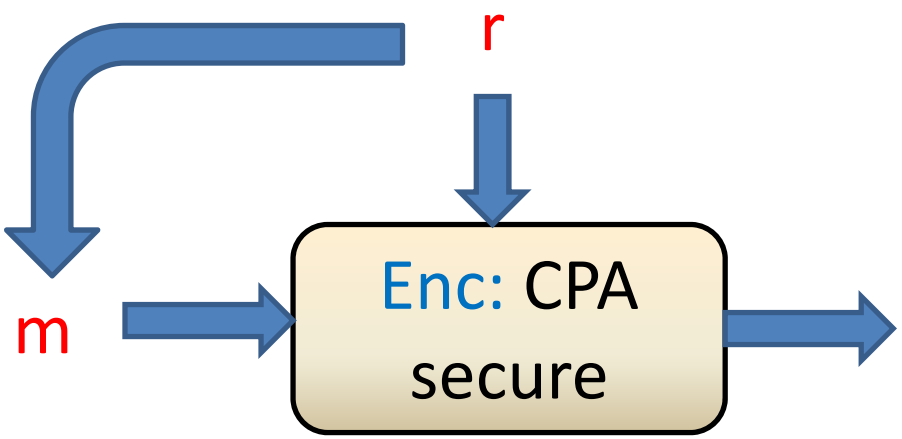
- but key dependent messages (KDM) are useful!

practically and theoretically ABBC, CKVW10, G09, BRS02,CL01, BPS08, BHHO08 etc.

- Intensely studied, lots of work…

m_0, m_1 do not depend on sk or r

Good for many settings
Not good for some



- randomness dependent messages (RDM)
  - implicit in MS09, HLW12, BBNRSSY09
    - explicit in HO10
      - much less studied

Why RDM?

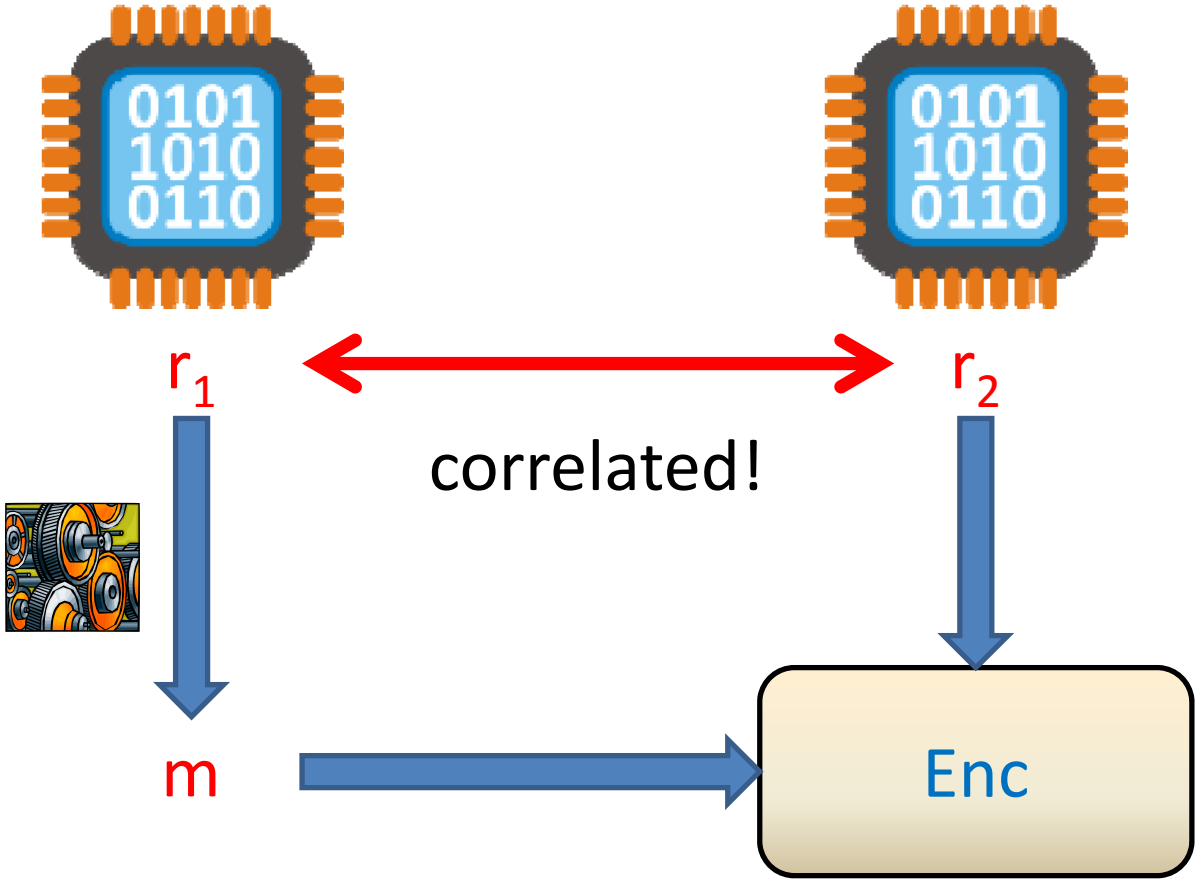
1) RDM happens! (involuntary attack)

correlated!

HDWH12

Why RDM?

1) RDM happens! (involuntary attack)



Why RDM?

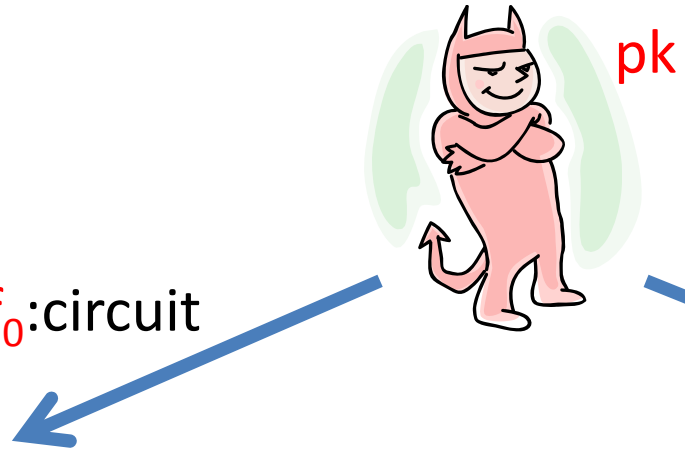
2) RDM is useful! (voluntary attack)

e.g.

- MS09, HLW12: 1-bit CCA2 => many-bit CCA2
- HO10: lossy encryption => inj. OW. TDF.

RDM security [HO10]

security against any RDM function



$\mathrm{Enc}_{pk}(f_0(r);r) \approx \mathrm{Enc}_{pk}(f_1(r);r)$

“weak” RDM security

f_0 and f_1 do not depend on pk

f_0:circuit

f_1:circuit

$Enc_{pk}(f_0(r);r)$ ≈ $Enc_{pk}(f_1(r);r)$

Hedged Encryption [BBNRSSY09] => weak RDM security

RDM security

pk

our focus: f_0 and f_1 depend on pk

f_0:circuit

f_1:circuit

$Enc_{pk}(f_0(r);r)$ ≈ $Enc_{pk}(f_1(r);r)$

2-circular RDM security

pk

f, g:circuits

$c_1 = Enc_{pk}(f(r_2);r_1)$

$c_2 = Enc_{pk}(g(r_1,c_1);r_2)$

k-circular RDM security

k=2

f, g:circuits

$c_1 = Enc_{pk}(f(r_2);r_1)$

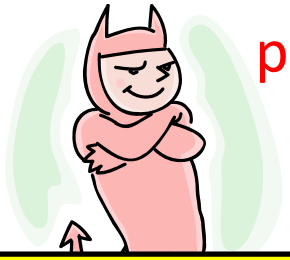
$c_2 = Enc_{pk}(g(r_1,c_1);r_2)$

≈

$c_1 = Enc_{pk}(0;r_1)$

$c_2 = Enc_{pk}(0;r_2)$

k-circular RDM security



pk

its

this work:
***k*-circular RDM security =>**
RDM security

$c_1 = En$ ... $r_1)$

$c_2 = Enc_{pk}(g(r_1, c_1); r_2)$

$c_2 = Enc_{pk}(0; r_2)$

Question: Can we get circular RDM, or even RDM security
i.e. security against any RDM function?

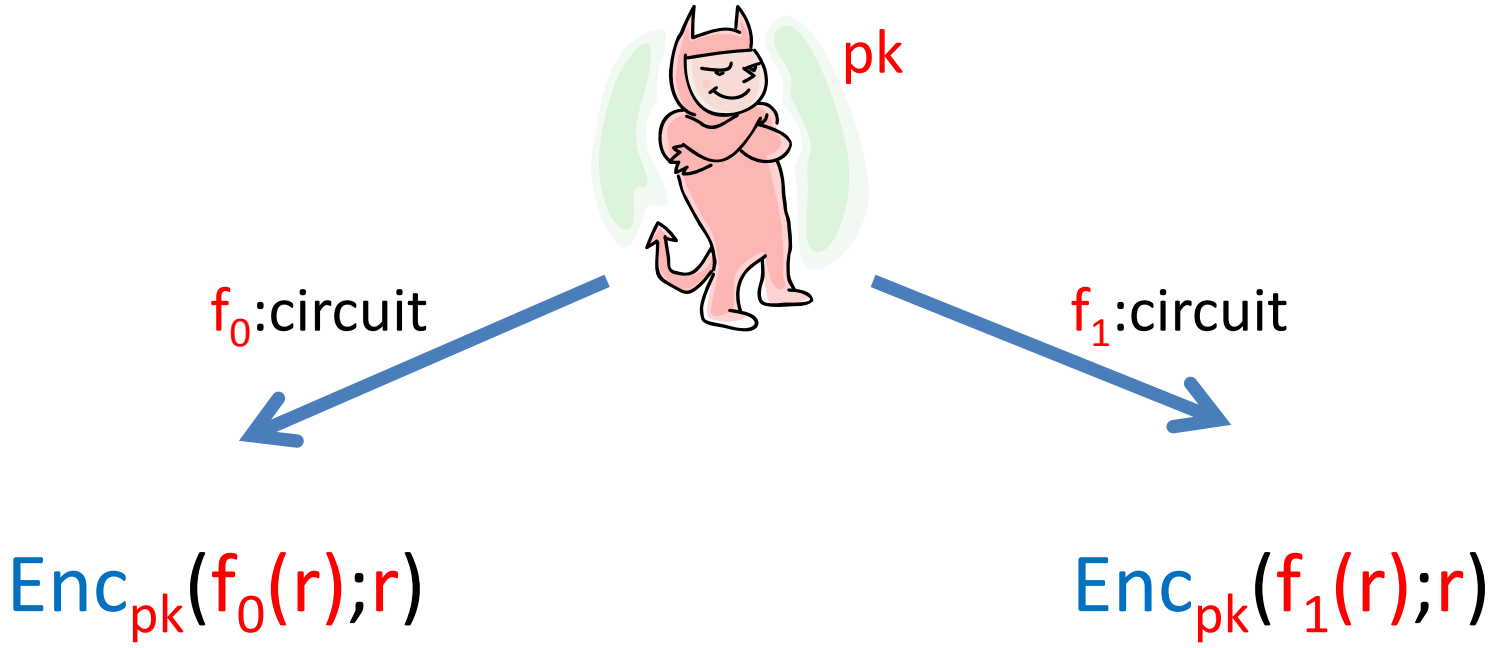
Our results

“Full” RDM security

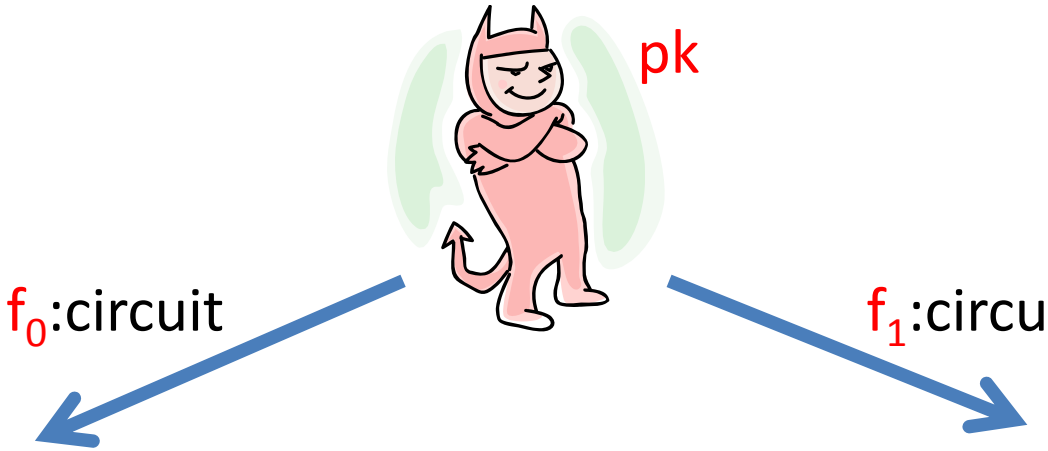
i.e. security against any RDM function

- Impossible in standard model
- => circular RDM impossible too

“Full” RDM is impossible



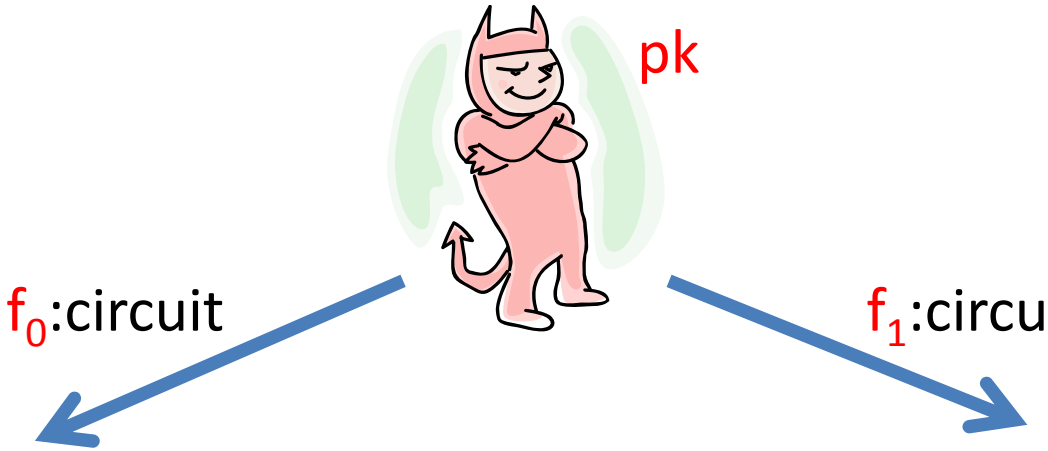
“Full” RDM is impossible



$f_0(r) = b'$ such that
$Enc_{pk}(b';r)$ “signals” 0

$f_1(r) = b'$ such that
$Enc_{pk}(b';r)$ “signals” 1

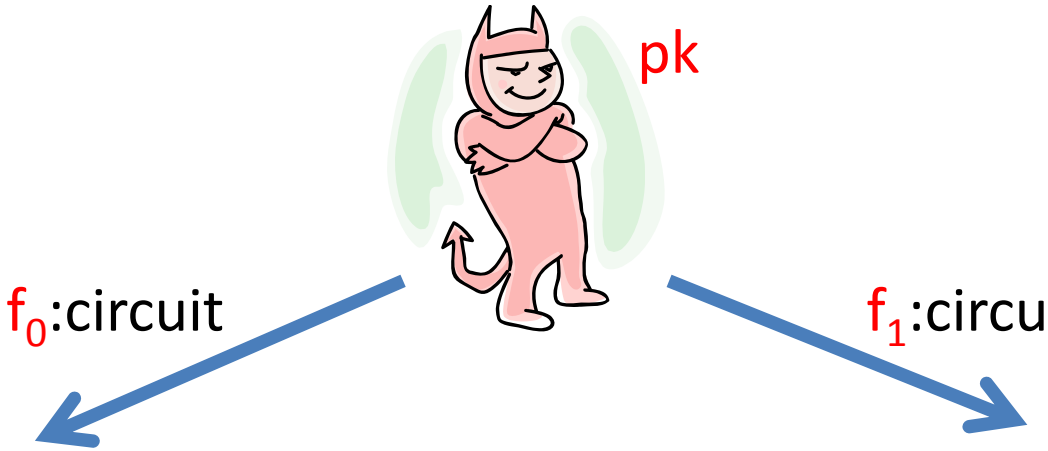
“Full” RDM is impossible



$f_0(r) = b'$ such that
$Enc_{pk}(b';r)$’s 1st bit is 0

$f_1(r) = b'$ such that
$Enc_{pk}(b';r)$’s 1st bit is 1

“Full” RDM is impossible



$f_0(r) = b'$ such that
$\mathrm{Enc}_{pk}(b';r)$’s 1st bit is 0

$f_1(r) = b'$ such that
$\mathrm{Enc}_{pk}(b';r)$’s 1st bit is 1

Use randomness extractor to get signal bit

Question: Can we get **bounded** RDM security?
i.e. security against *a priori* bounded size RDM functions?

Our results

Bounded circular RDM security

- **Theorem 1**: for any poly *s*, exists transformation s.t.

transformation: Enc(m ; preprocess(r))

- r needs to be “long”

We also show: black-box barriers for proving RDM security if r is shorter than m

Our results

Bounded circular RDM security with "short" randomness

- **Theorem 2**: For any poly *s,*

exists scheme that is circular secure against size *s* RDM functions

with arbitrary message and randomness length

assuming lossy trapdoor function [PW08]

Thm1: Bounded circular RDM security from CPA/CCA

Thm1: Bounded circular RDM security from CPA/CCA

- View RDM as indirect randomness leakage

- Idea:

  use CPA secure (Gen,Enc,Dec) and r “long” enough

$$\mathrm{Enc}_{pk}(m\ ;\ \mathrm{preprocess}(r)\ )$$

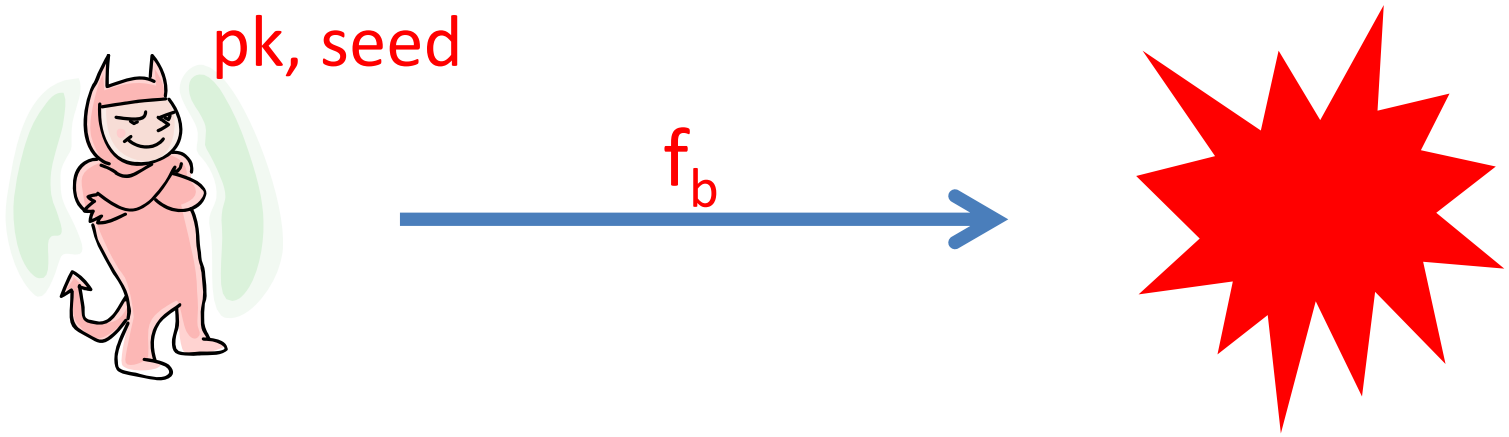
preprocess: randomness extraction

f_b: *s*-bounded leakage function

$r | f_b(r)$: *s*-"bounded leaked source"

$Enc_{pk}(m ; extr(seed,r))$

- Seeded extractors don't work
  require seed and source independence!

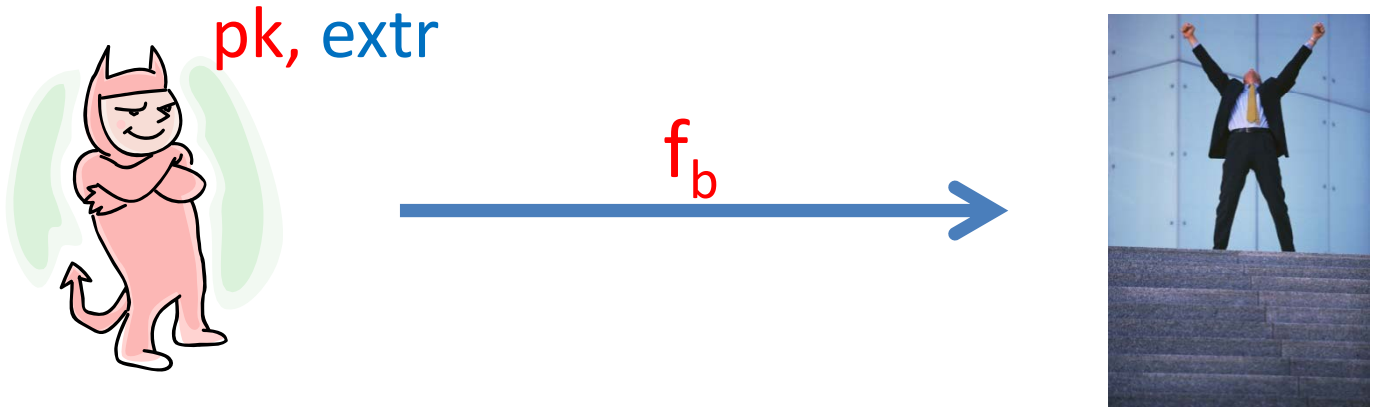


f_b: *s*-bounded leakage function

$r | f_b(r)$: *s*-"bounded leaked source"

$Enc_{pk}(m ; extr(r))$

- need deterministic extraction that works for **all** *s*-bounded leaked sources



f_b: *s*-bounded leakage function

$r|f_b(r)$: *s*-"bounded leaked source"

$Enc_{pk}(m ; extr(r))$

- need deterministic extraction that works for **all** *s*-bounded leaked sources

We show: Deterministic extraction Lemma for bounded leaked sources

w.h.p $h \leftarrow$ t-wise ind. hash,

for all *s*-bounded leaked sources with high min-entropy

$$f_b(r), h(r) \approx f_b(r), U$$

We show: Deterministic extraction Lemma for bounded leaked sources

w.h.p $h \leftarrow$ t-wise ind. hash,

for all s-bounded leaked sources with high min-entropy

$$f_b(r), h(r) \approx f_b(r), U$$

TV00: Deterministic extraction Lemma for bounded samplable sources

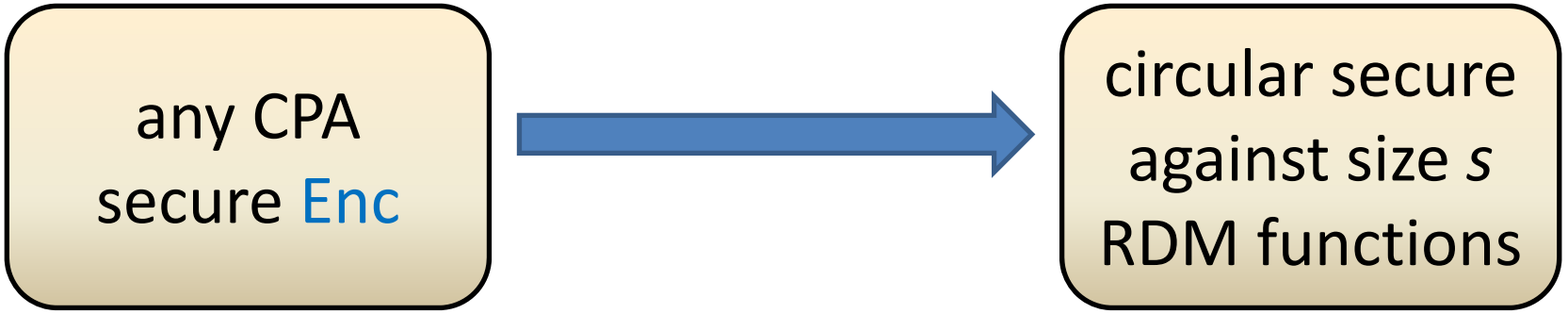
w.h.p $h \leftarrow$ t-wise ind. hash,

for all s-bounded samplable sources X with high min-entropy

$$h(X) \approx U$$

Bounded circular RDM security

- For any poly *s*



$$\mathrm{Enc}(m\ ;\ \mathrm{hash}_{\text{t-wise indep}}(r)\ )$$

- **In paper**: black-box barriers for proving RDM security on a falsifiable assumption if r is shorter than m

Bounded circular RDM security with “short” randomness?

Thm2: Bounded circular RDM security
with **arbitrary** message and randomness length
from lossy trapdoor function (LTDF)

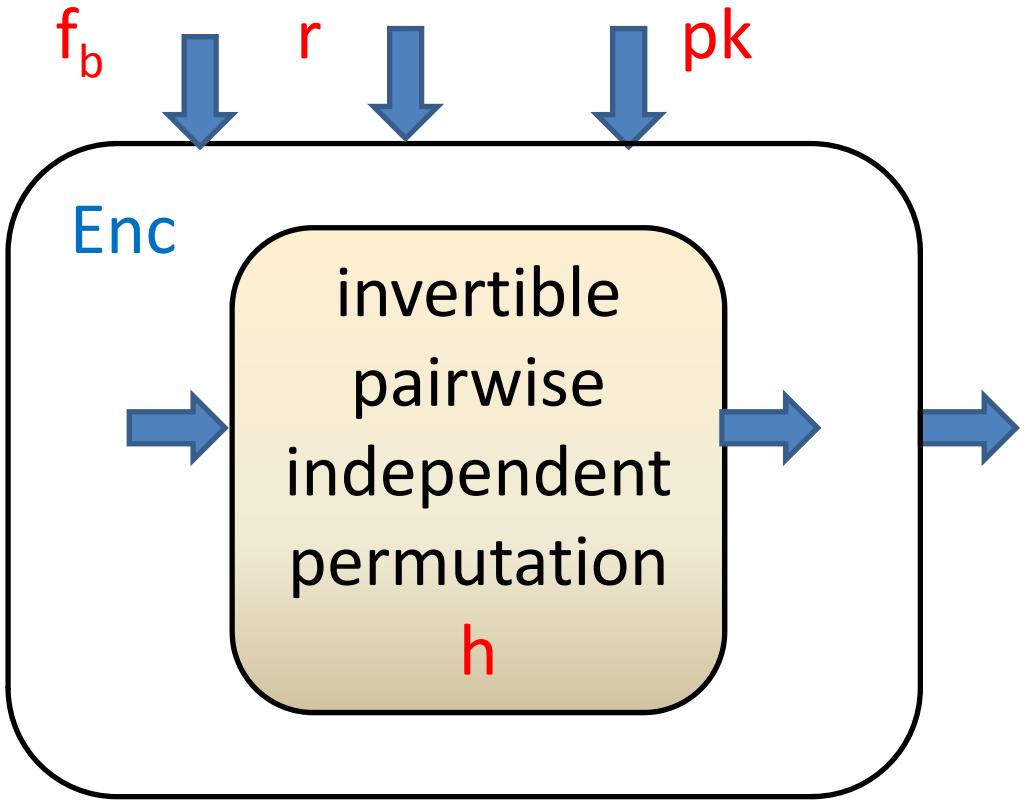
Hedged Encryption [BBNRSSY09]

secure w.r.t. RDM functions don't depend on pk

- from lossy trapdoor functions (LTDF)

crooked LHL [DS08]
For all sources X
with high min-entropy
and functions with
small range f
$f(h(X)) \approx f(U)$

works only when
X and h are
independent



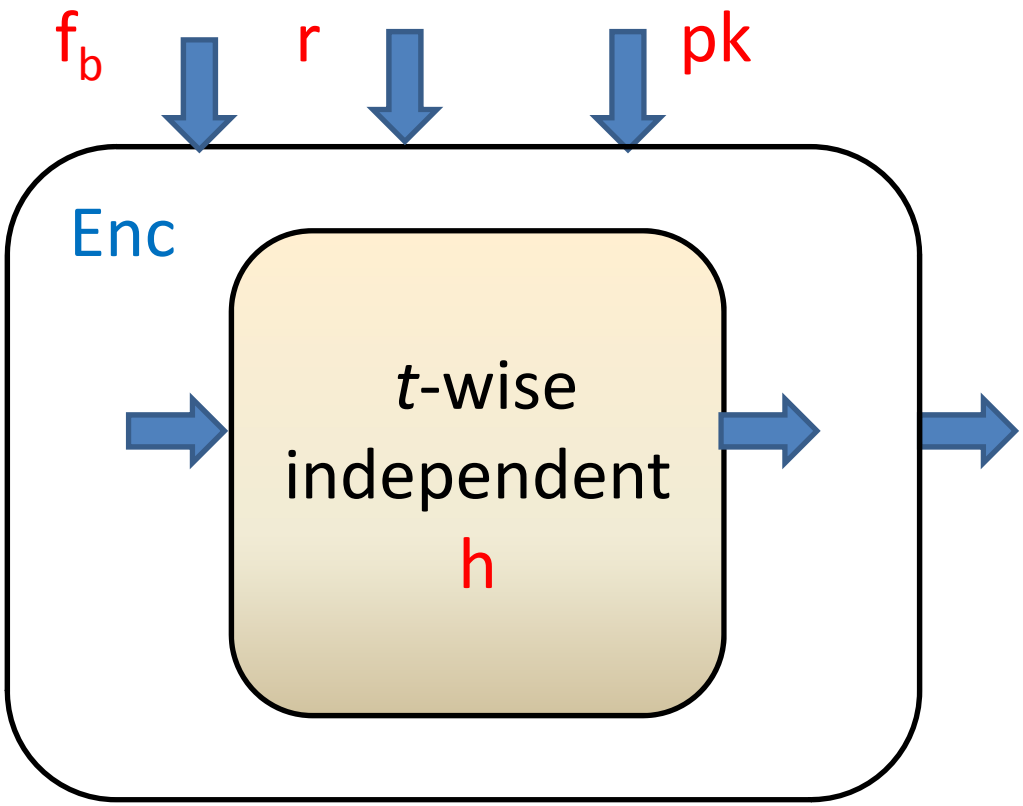
We show: Crooked det. ext. for bounded leaked sources

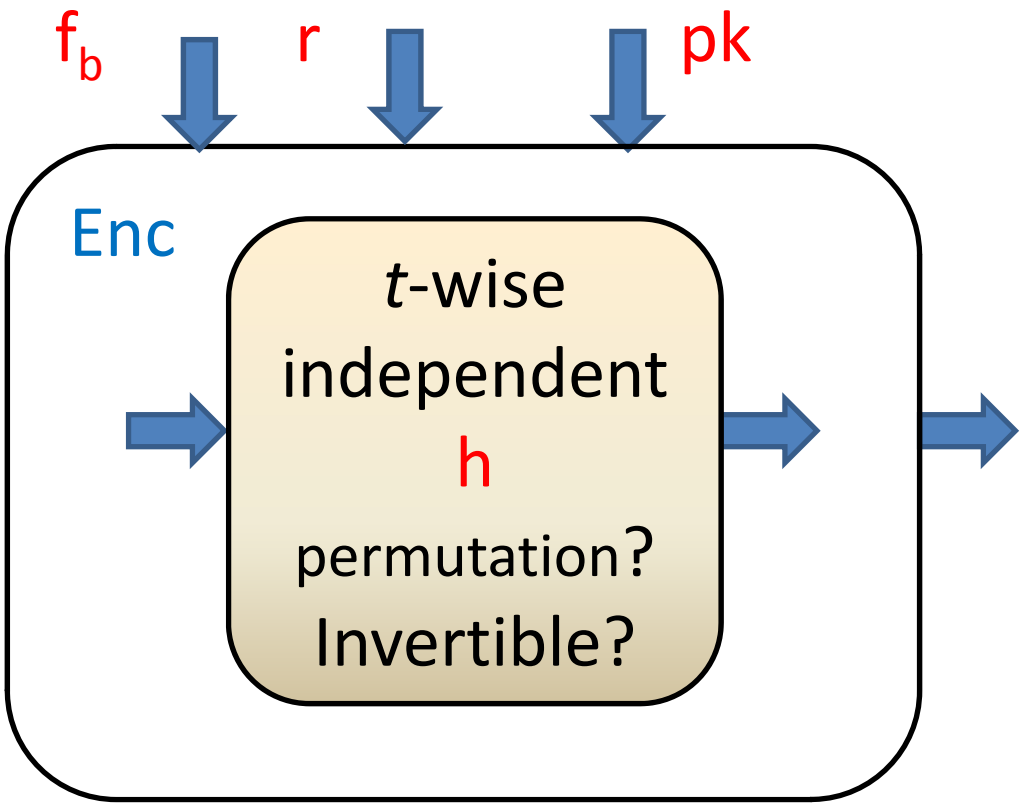
w.h.p $h \leftarrow$ t-wise ind. hash,

for all bounded leaked sources X with high min-entropy

and functions with small range f

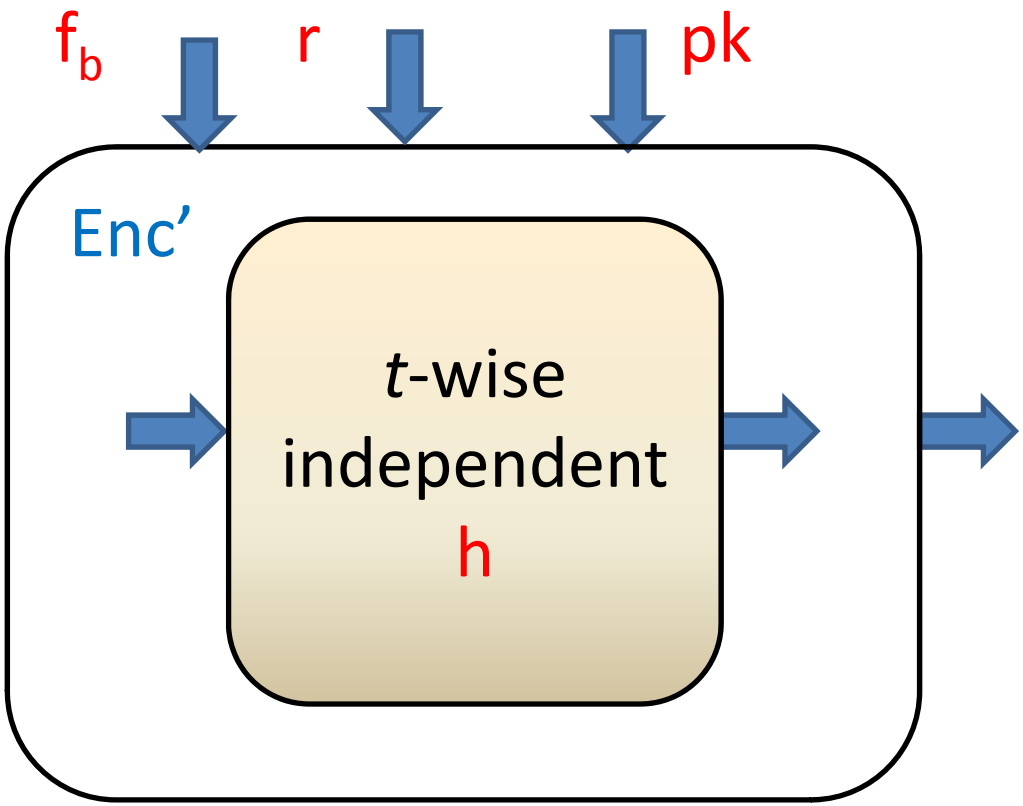
$f(h(X)) \approx f(U)$





open problem

Almost t-wise doesn't suffice



Instead we modify scheme so that we don't need permutation

=> can use standard polynomial construction, invert with Berlekamp algorithm

RDM (why? it happens and it's useful)

"Full" RDM security

i.e. security w.r.t. all RDM functions

- Impossible in standard model (rules out circular)
- Secure construction in "ultra-weak" RO model

(i.e. reduction neither programs oracle nor sees queries to it)

"Bounded" circular RDM security

i.e. security w.r.t. RDM functions of *a priori* bounded size

- From lossy trapdoor functions
- From CPA/CCA secure schemes
  - construction with "long" randomness
  - barriers for secure constructions with "short" randomness