Bitter Cryptography

Seung Geol Choi
Aggelos Kiayias
Tal Malkin

BiTR Cryptography

Seung Geol Choi
Aggelos Kiayias
Tal Malkin

Built-in Tamper Resilient Cryptography

Seung Geol Choi

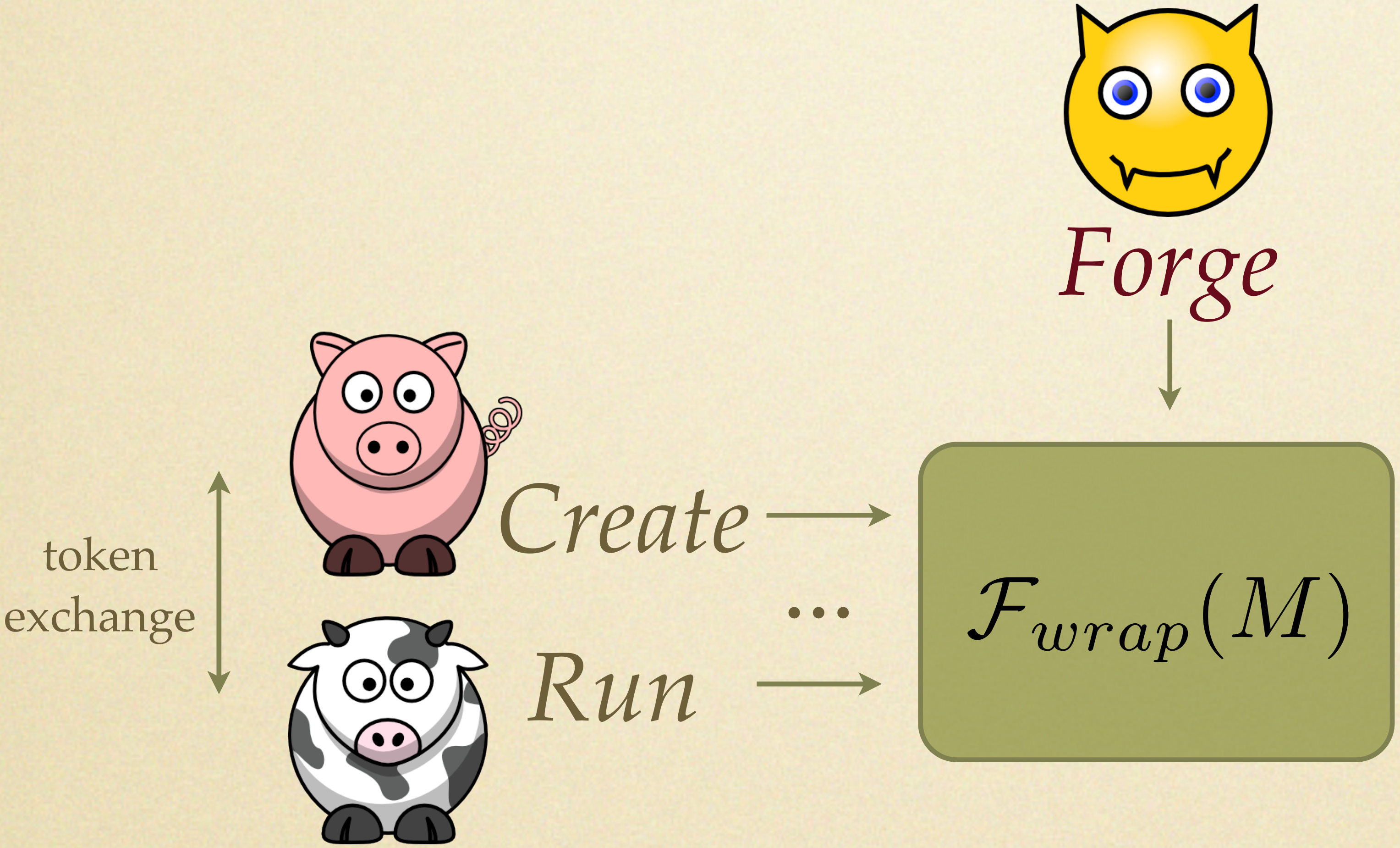
Aggelos Kiayias

Tal Malkin

disclaimer:
this talk is not
intentionally
funny*

*unless you find public
domain animal clipart funny.

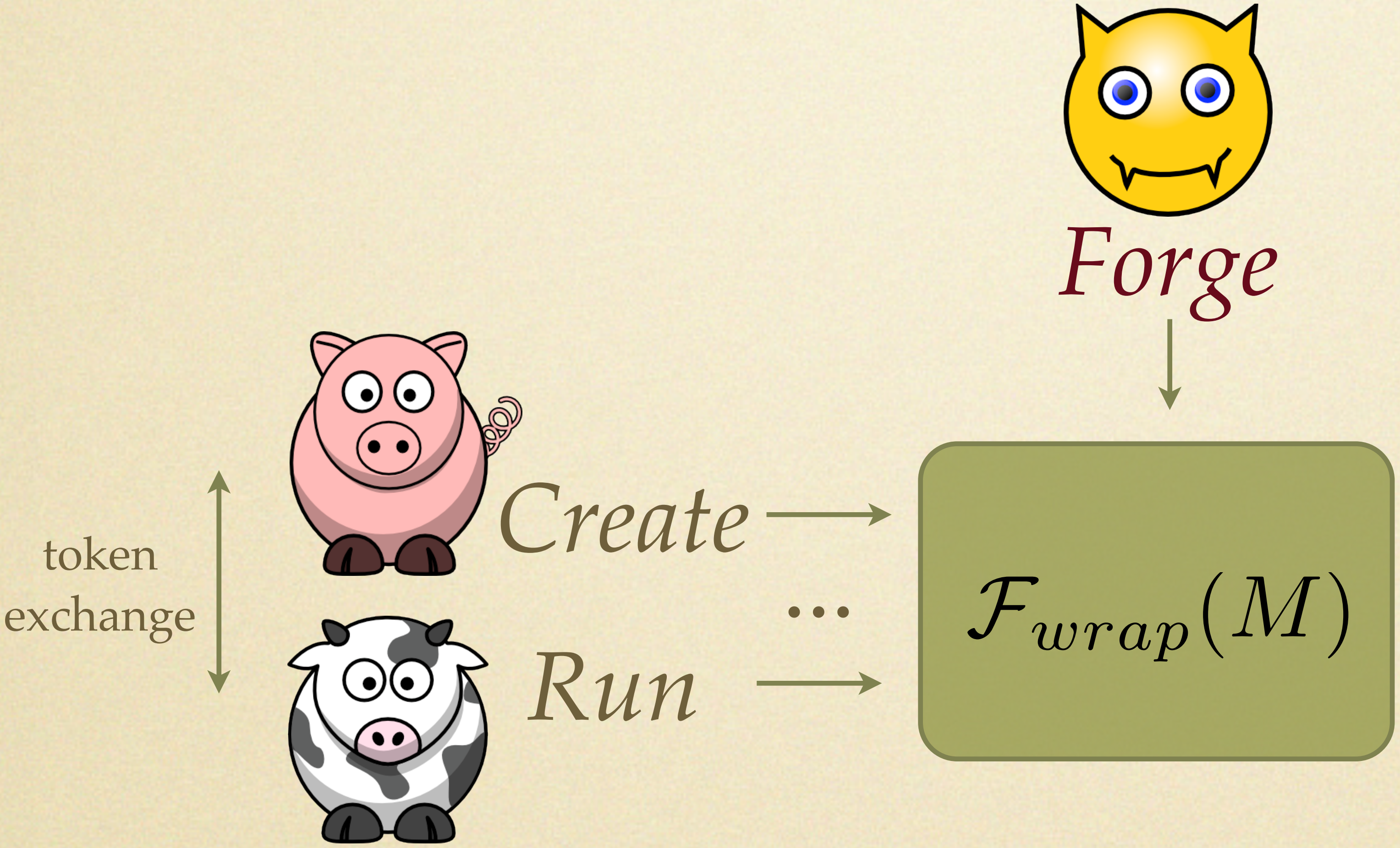
Crypto w/ Hardware Tokens



What cryptography exists in the $\mathcal{F}_{wrap}(\cdot)$ hybrid world ? ... *plenty*

[Katz07,MS08,CGS08,DNW08,GIS+10,K10,GIMS10]

Crypto w/ Hardware Tokens



Forge

Create

…

Run

token exchange

$\mathcal{F}_{wrap}(M)$

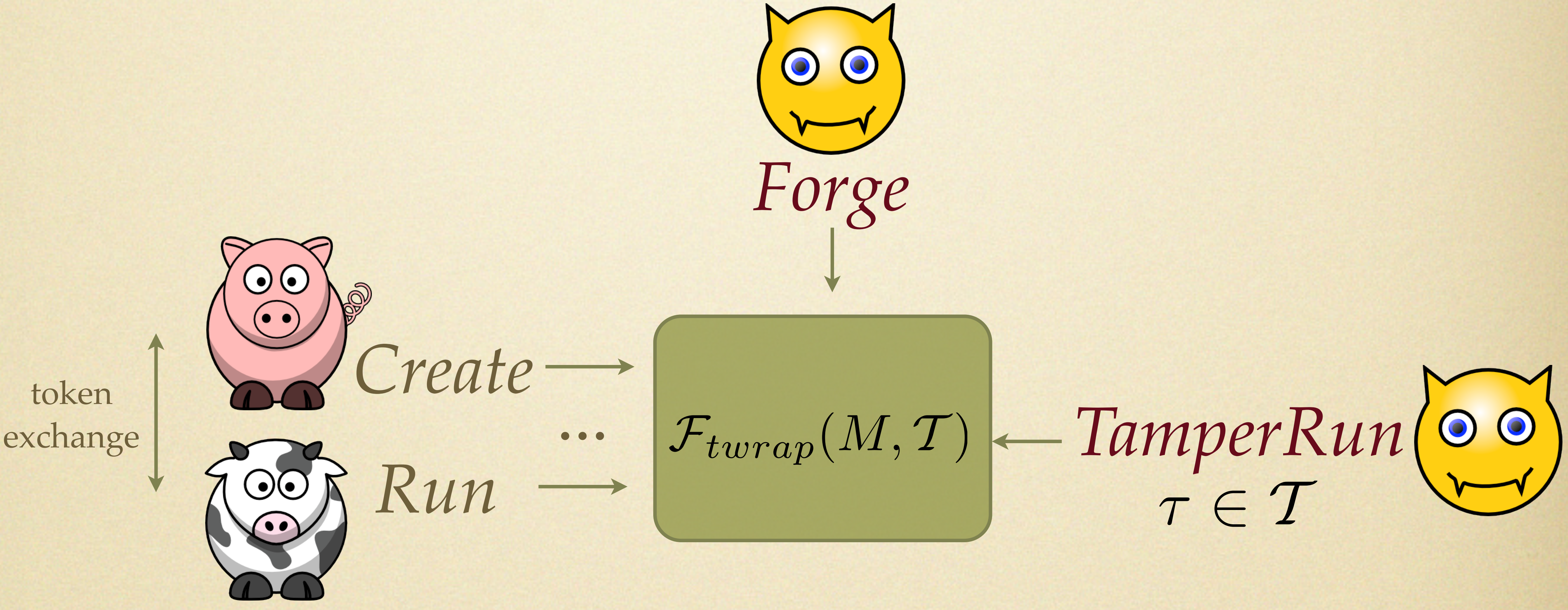
What cryptography exists in the $\mathcal{F}_{wrap}(\cdot)$ hybrid world ? ... *plenty*

[Katz07,MS08,CGS08,DNW08,GIS+10,K10,GIMS10]

Realistic?

- Attacks beyond the standard cryptographic model.
  - leaking.
  - tampering.
  - blah-blah.

Tamperable Tokens



Forge

token exchange

Create

Run

…

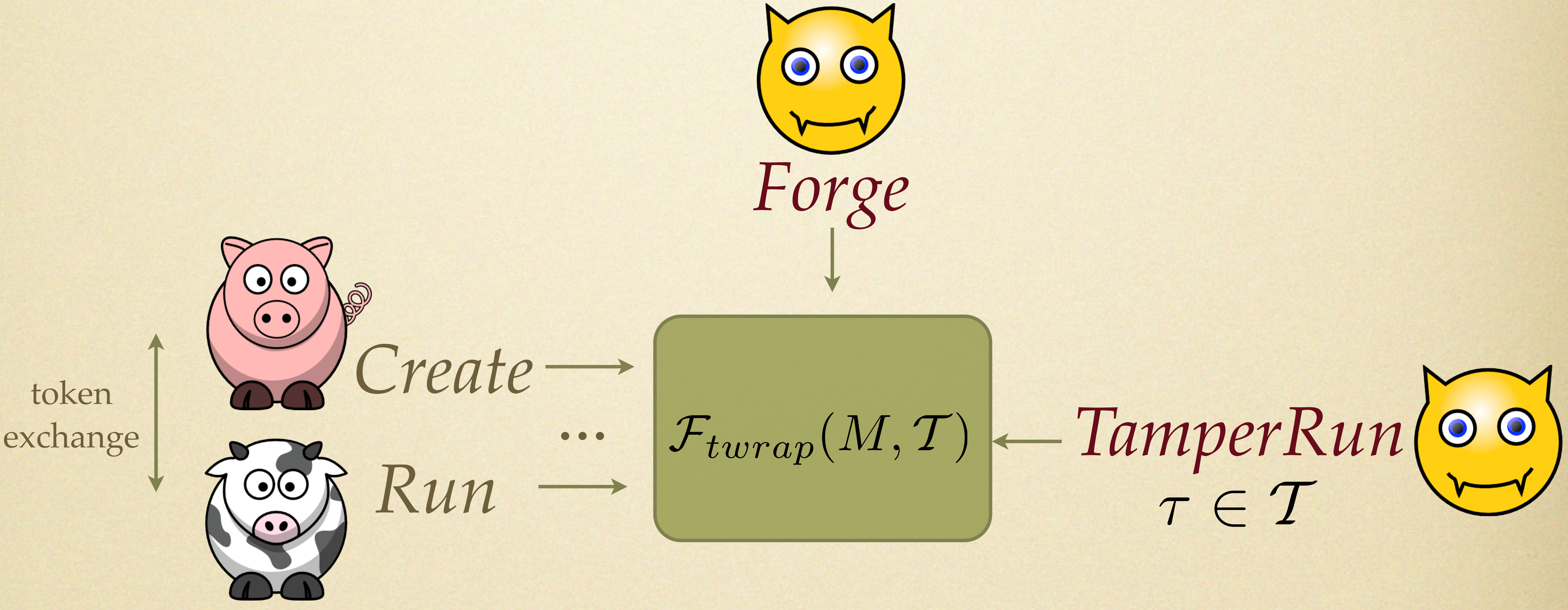
$\mathcal{F}_{twrap}(M, \mathcal{T})$

TamperRun

$\tau \in \mathcal{T}$

What cryptography exists in the $\mathcal{F}_{twrap}(\cdot)$ hybrid world ?

Tamperable Tokens



Forge

token exchange

Create

…

Run

$\mathcal{F}_{twrap}(M, \mathcal{T})$

TamperRun

$\tau \in \mathcal{T}$

What cryptography exists in the $\mathcal{F}_{twrap}(\cdot)$ hybrid world ?

This work

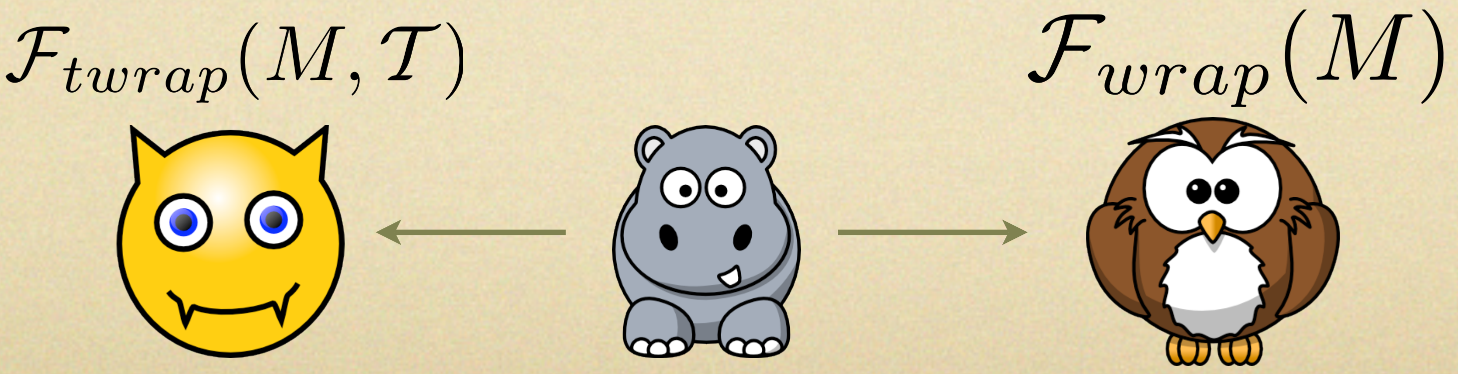
- defines the BiTR framework :

Built-in Tamper Resilience
(BiTR)

a property of *M : no matter the environment*
M is deployed as a token, tampering gives no advantage

Definition.

$\forall$ $\exists$ $\forall$ *s.t.*



$\mathcal{F}_{twrap}(M,\mathcal{T})$

$\mathcal{F}_{wrap}(M)$

indistinguishable

Built-in Tamper Resilience

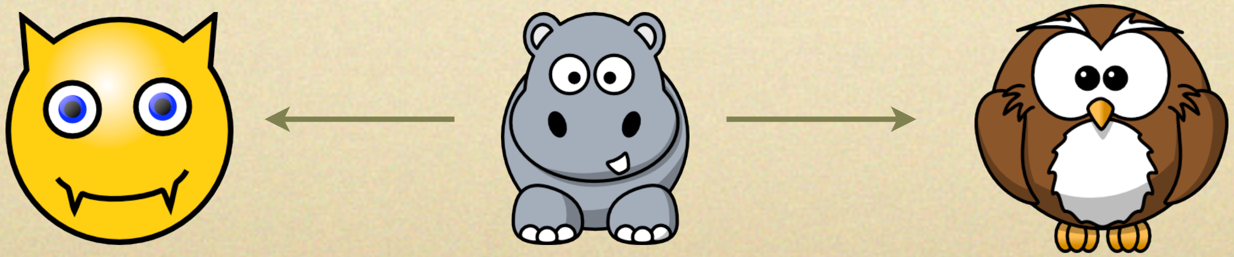
(BiTR)

a property of *M : no matter the environment M is deployed as a token, tampering gives no advantage*

Definition.

$\forall$ $\exists$ $\forall$ *s.t.*

$\mathcal{F}_{twrap}(M, \mathcal{T})$ $\mathcal{F}_{wrap}(M)$



indistinguishable

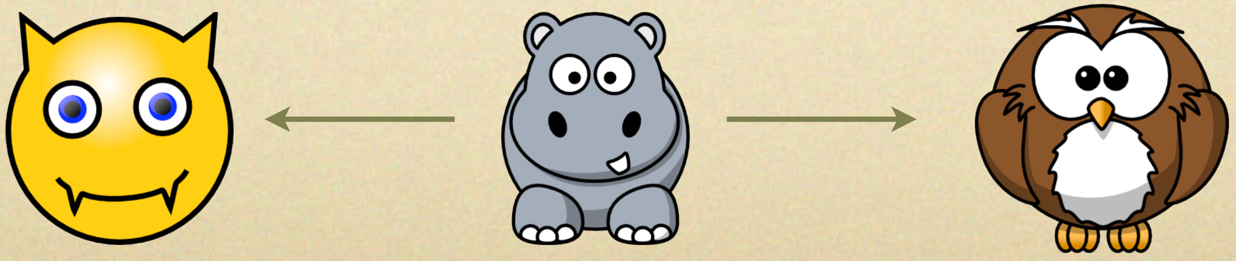
Built-in Tamper Resilience

(BiTR)

a property of M : *no matter the environment*
M is deployed as a token, tampering gives no advantage

Definition.

$\forall$ $\exists$ $\forall$ *s.t.*

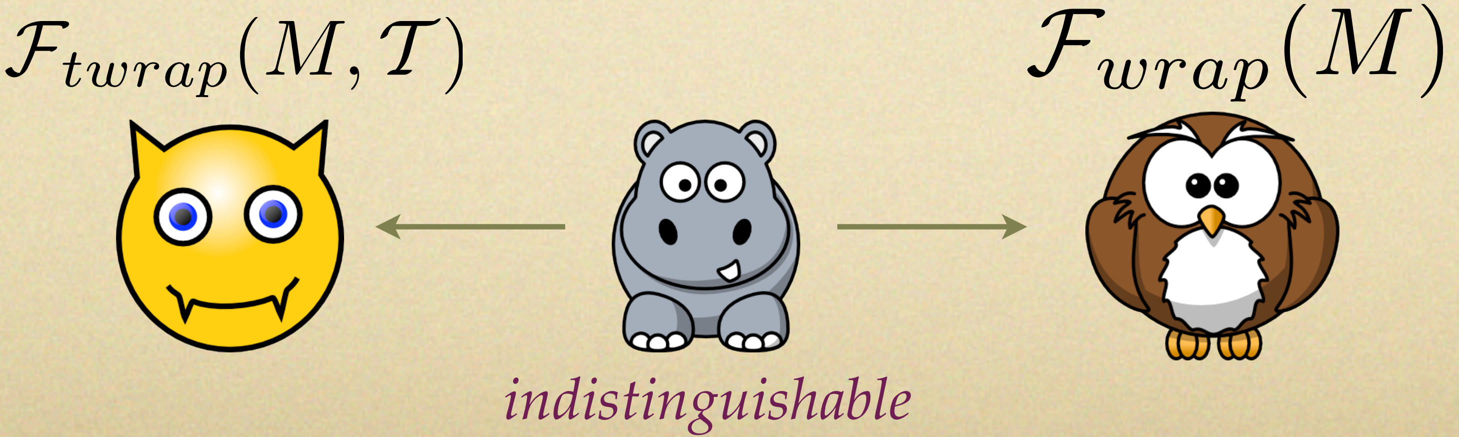


Built-in Tamper Resilience
(BiTR)

a property of *M : no matter the environment M is deployed as a token, tampering gives no advantage*

Definition.

$\forall$ $\exists$ $\forall$ *s.t.*



$\mathcal{F}_{twrap}(M,\mathcal{T})$

$\mathcal{F}_{wrap}(M)$

indistinguishable

This work

- questions
  - Are there efficient BiTR protocols?
  - Is the composition of BiTR protocols also BiTR?

This work

- answers
    - Are there efficient BiTR protocols? **yes!**

      (1) for restricted tampering functions - no encodings.

      tampering => affine transformations

      for signatures, identification, UC two-party SFE

      (2) for any given tampering functions - we can construct deterministic encodings if they exist.

- Is the composition of BiTR protocols also BiTR?

  sometimes! under suitable constraints...

Summary

- results : the BiTR framework and ...
  - Is the composition of BiTR protocols also BiTR?

    ... BiTR Composition Theorem.
  - Are there efficient BiTR protocols?

    ... we show all these people are BiTR :

Okamoto

Schnorr

Katz

Canetti

and pretty
much everybody is
somewhat BiTR