Unconditionally Secure Universally Composable Commitments from Physical Assumptions

Ivan Damgård and Alessandra Scafuro

Wait...Isn't done yet?

Universally Composable

Wait...Isn't done yet?

Universally Composable

Statefull tokens [K07..]

Stateless tokens [CGS08..]

Trusted PUFs [BFSK11]

Malicious PUFs [OSVW13]

(trusted)
Signature card [HMQU11..]

Wait...Isn't done yet?

Universally Composable AND Unconditionally Secure

Statefull tokens [K07..]

Stateless tokens [CGS08..]

Trusted PUFs [BFSK11]

Malicious PUFs [OSVW13]

(trusted)
Signature card [HMQU11..]

Wait...Isn't done yet?

Universally Composable AND Unconditionally Secure

Statefull tokens [K07..]

Statefull tokens [MS08..]

Stateless tokens [CGS08..]

Trusted PUFs [BFSK11]

Malicious PUFs [OSVW13]

(trusted)
Signature card [HMQU11..]

Wait...Isn’t done yet?

Universally Composable AND Unconditionally Secure

Statefull tokens [K07..]

Stateless tokens [CGS08..]

Trusted PUFs [BFSK11]

Malicious PUFs [OSVW13]

(trusted)
Signature card [HMQU11..]

Statefull tokens [MS08..]

Trusted PUFs

Wait...Isn't done yet?

Universally Composable AND Unconditionally Secure

Statefull tokens [K07..]

Stateless tokens [CGS08..]

Trusted PUFs [BFSK11]

Malicious PUFs [OSVW13]

(trusted)
Signature card [HMQU11..]

Statefull tokens [MS08..]

this work

Trusted PUFs

this work

Unconditionally Secure

Universally Composable

Commitments

Unconditionally Secure

Universally Composable

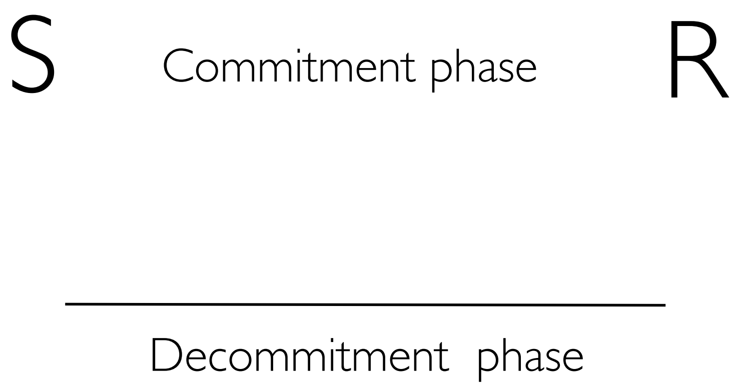
Commitments

S

R

Unconditionally Secure Universally Composable

Commitments



S

Commitment phase

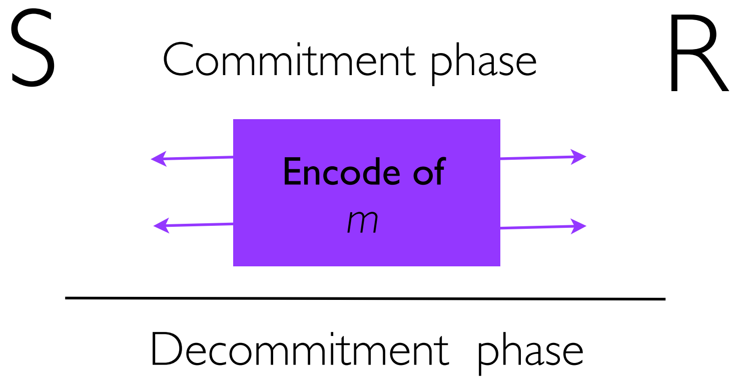
R

Decommitment phase

Unconditionally Secure

Universally Composable

Commitments



S

Commitment phase

R

Encode of *m*

Decommitment phase

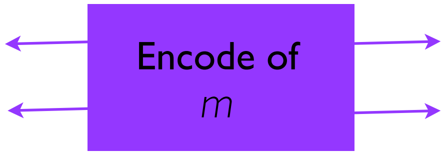
Unconditionally Secure

Universally Composable

Commitments

S

Commitment phase



Encode of
m

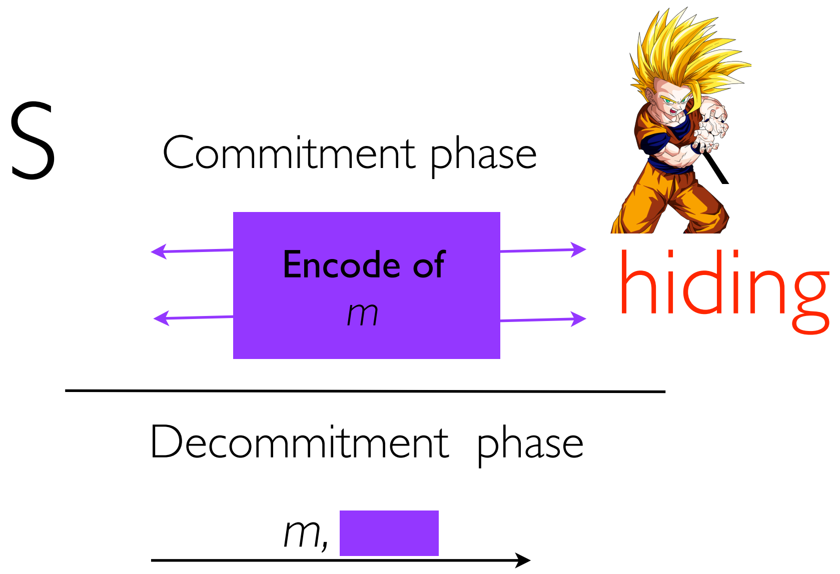
hiding

Decommitment phase

Unconditionally Secure

Universally Composable

Commitments



S

Commitment phase

Encode of *m*

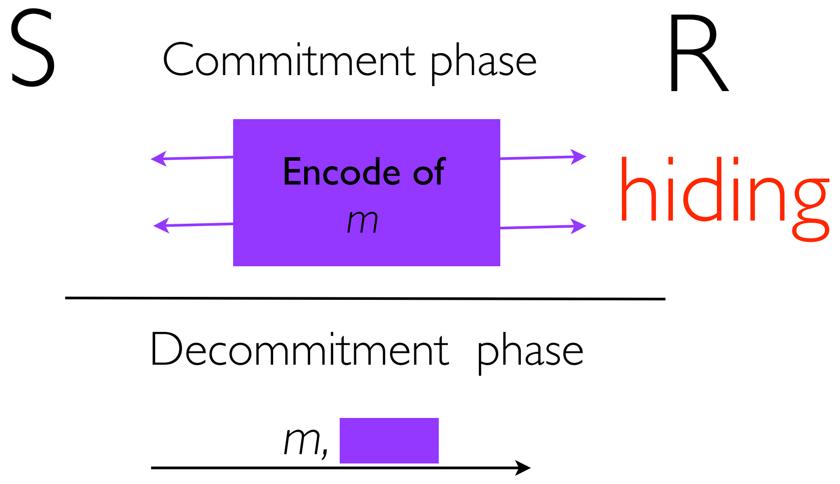
hiding

Decommitment phase

m,

Unconditionally Secure Universally Composable

Commitments



S

Commitment phase

R

Encode of *m*

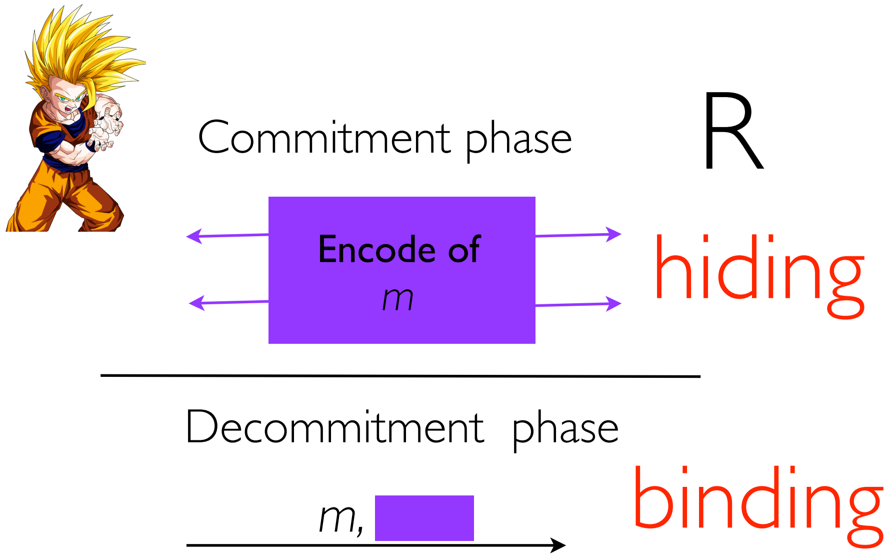
hiding

Decommitment phase

m,

Unconditionally Secure Universally Composable

Commitments



Commitment phase

R

Encode of m

hiding

Decommitment phase

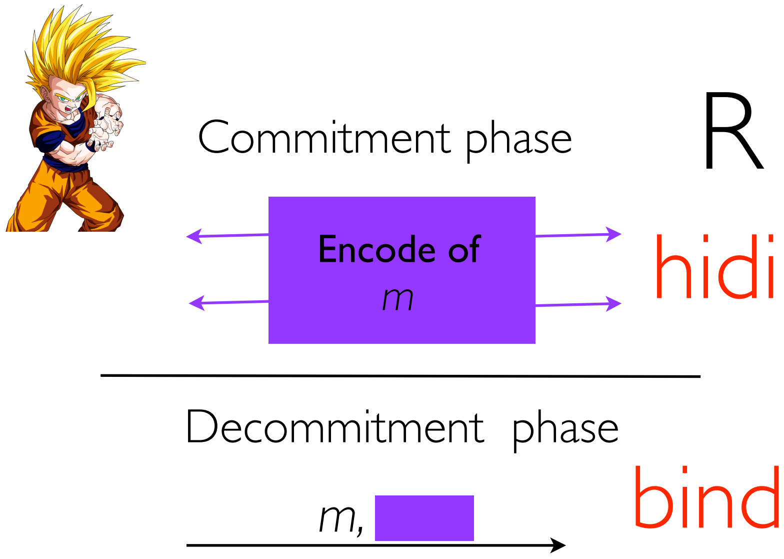
m,

binding

Unconditionally Secure

Universally Composable

Commitments



Commitment phase

R

Encode of *m*

hiding

Decommitment phase

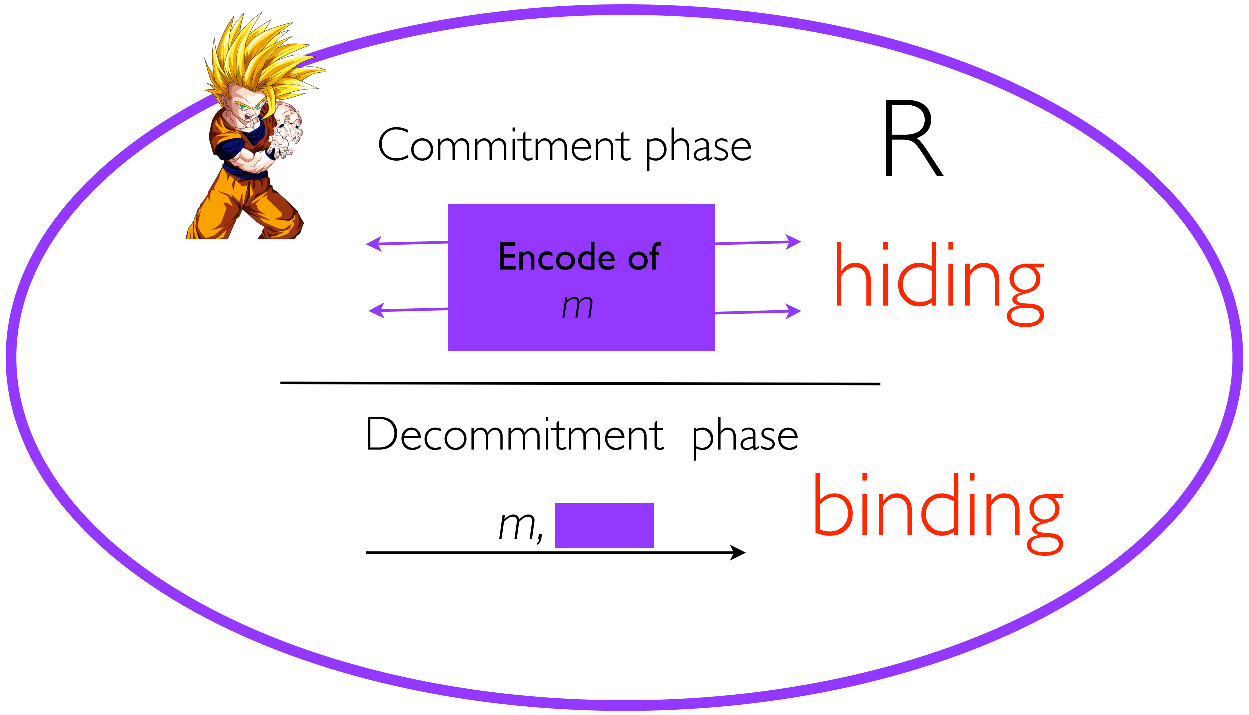
m, ▨

binding

Unconditionally Secure

Universally Composable

Commitments



Commitment phase

R

Encode of m

hiding

Decommitment phase

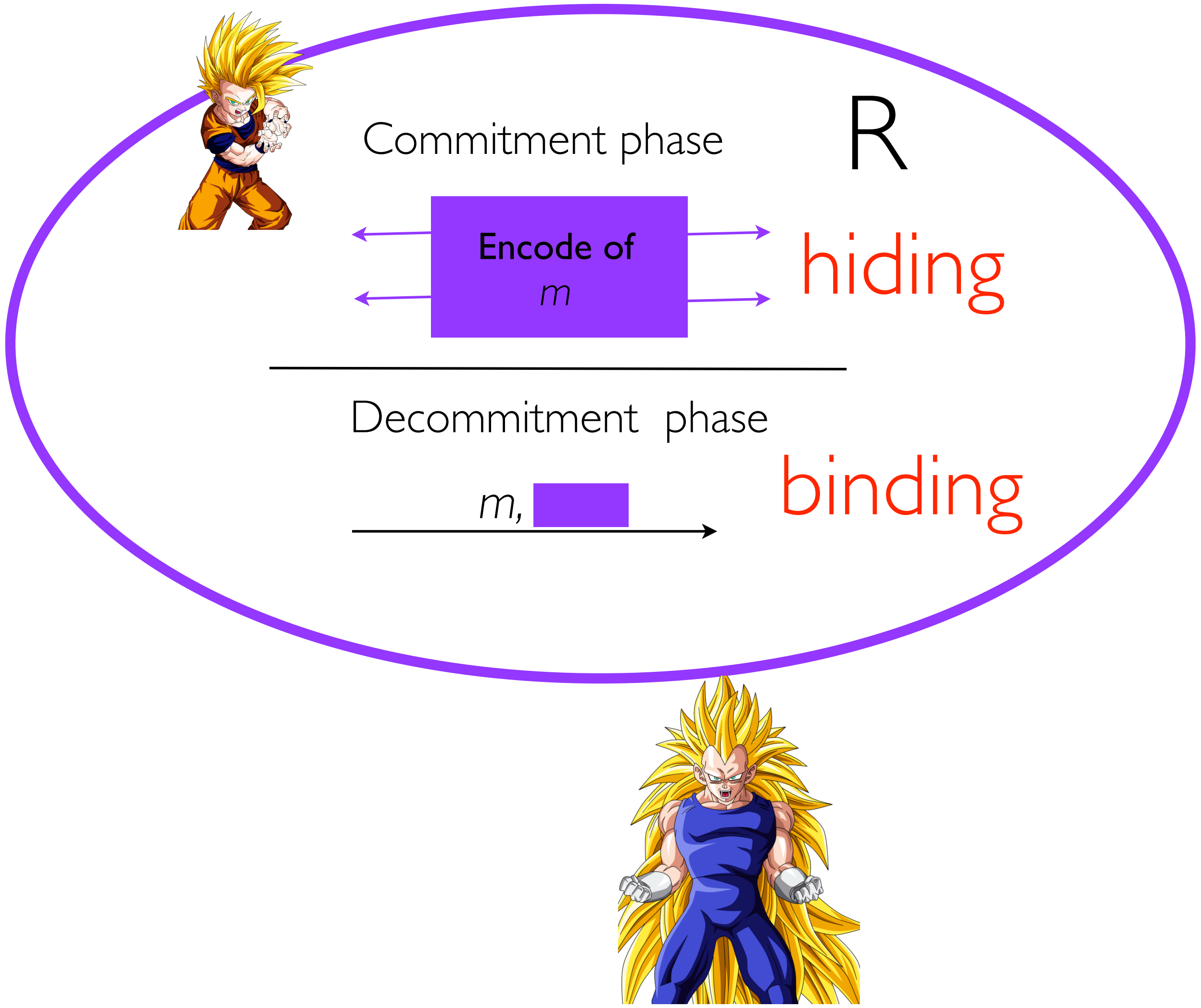
m,

binding

Unconditionally Secure

Universally Composable

Commitments



Commitment phase

R

Encode of *m*

hiding

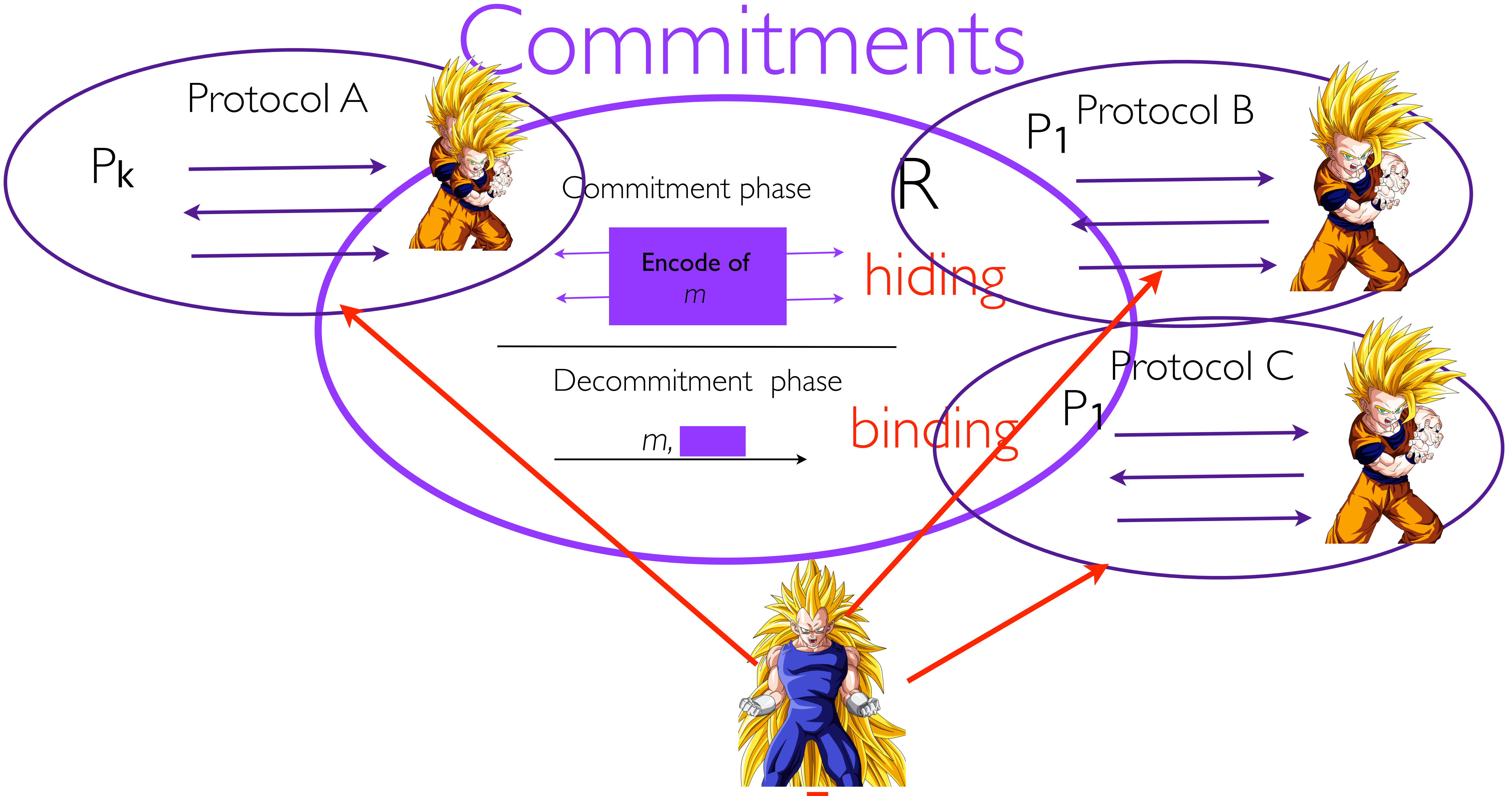
Decommitment phase

m,

binding

Unconditionally Secure

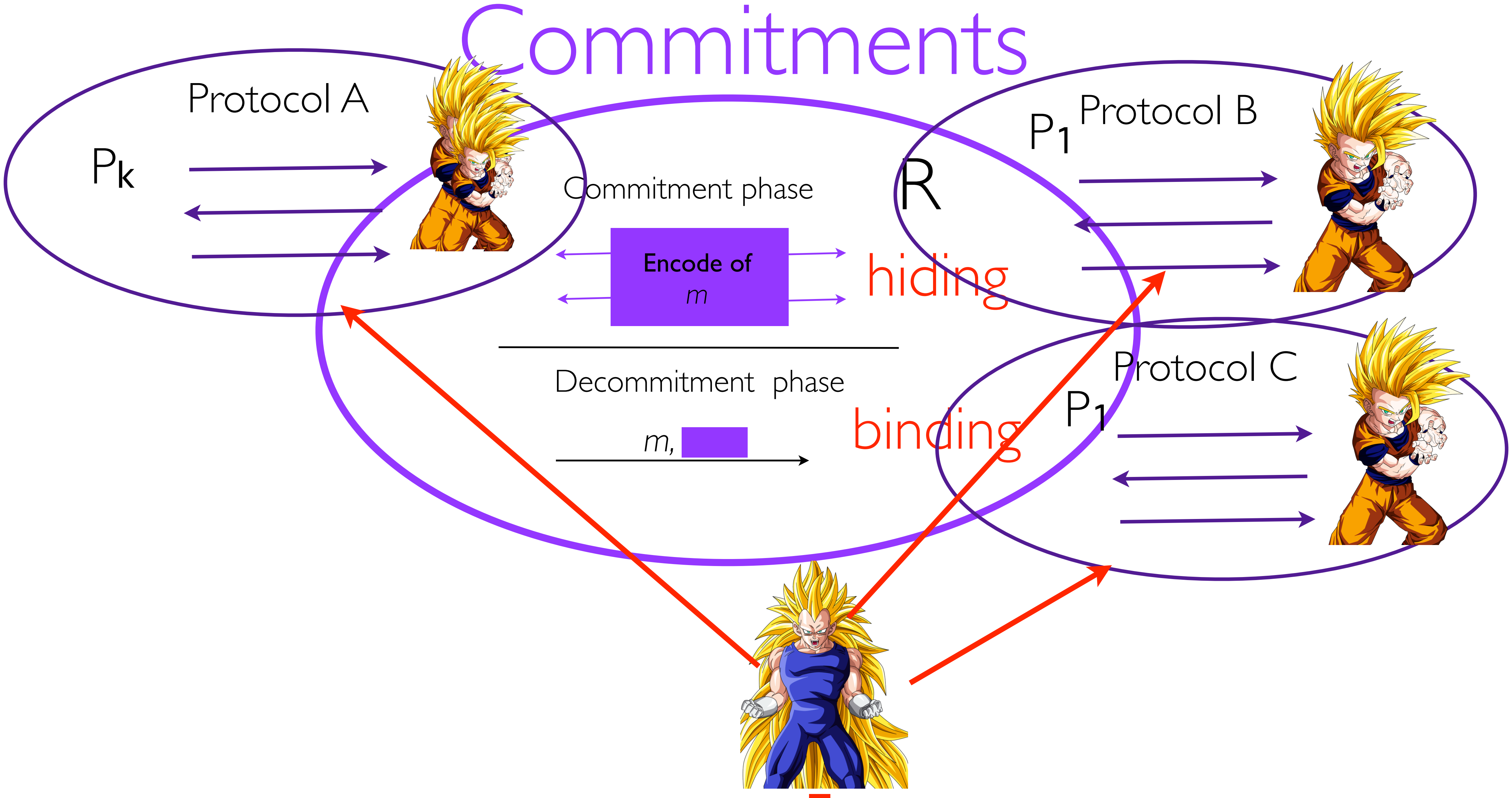
Universally Composable



[CKL03] Setup Assumptions

Unconditionally Secure

Universally Composable

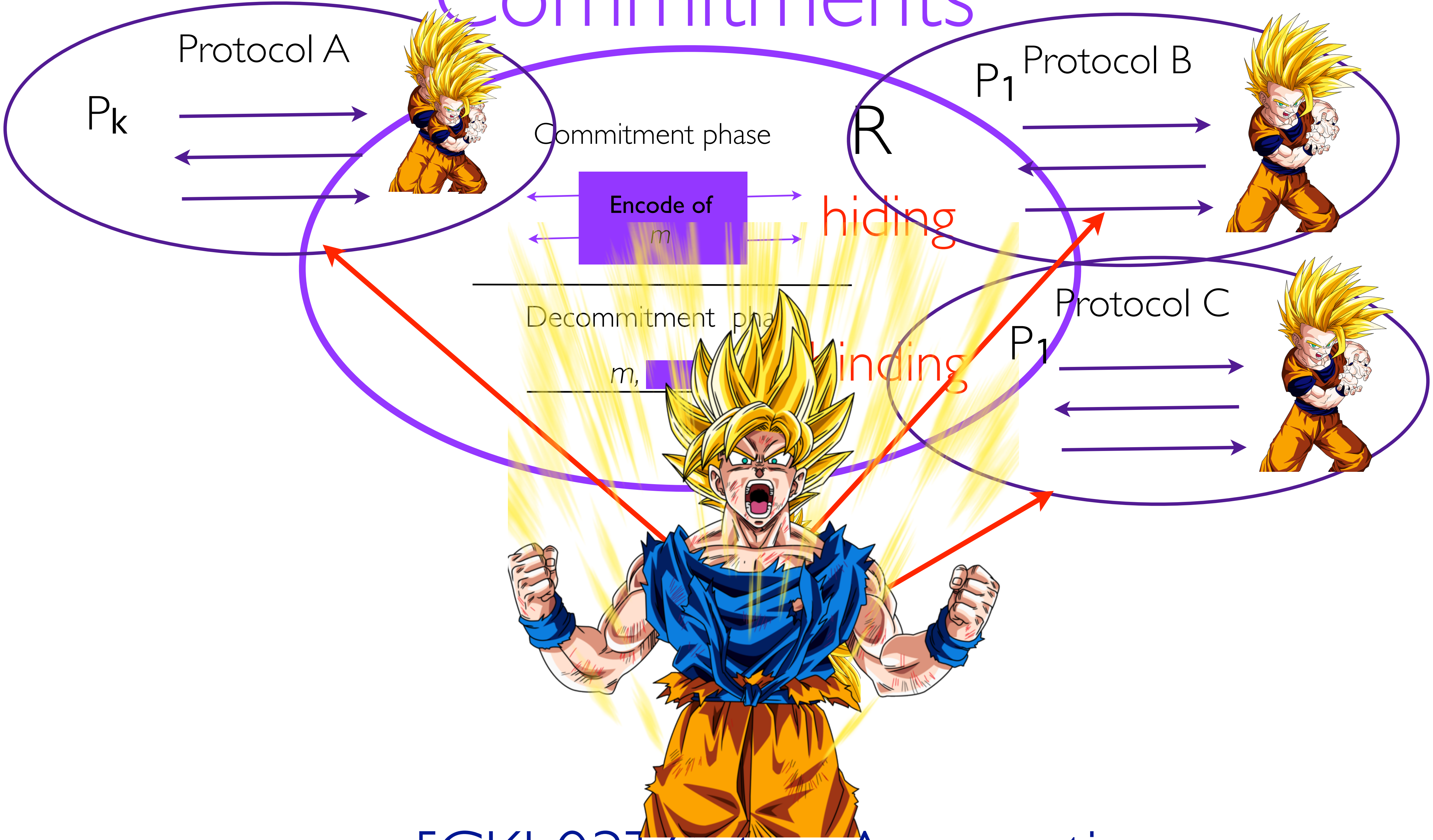


[CKL03] Setup Assumptions

Unconditionally Secure

Universally Composable

Commitments

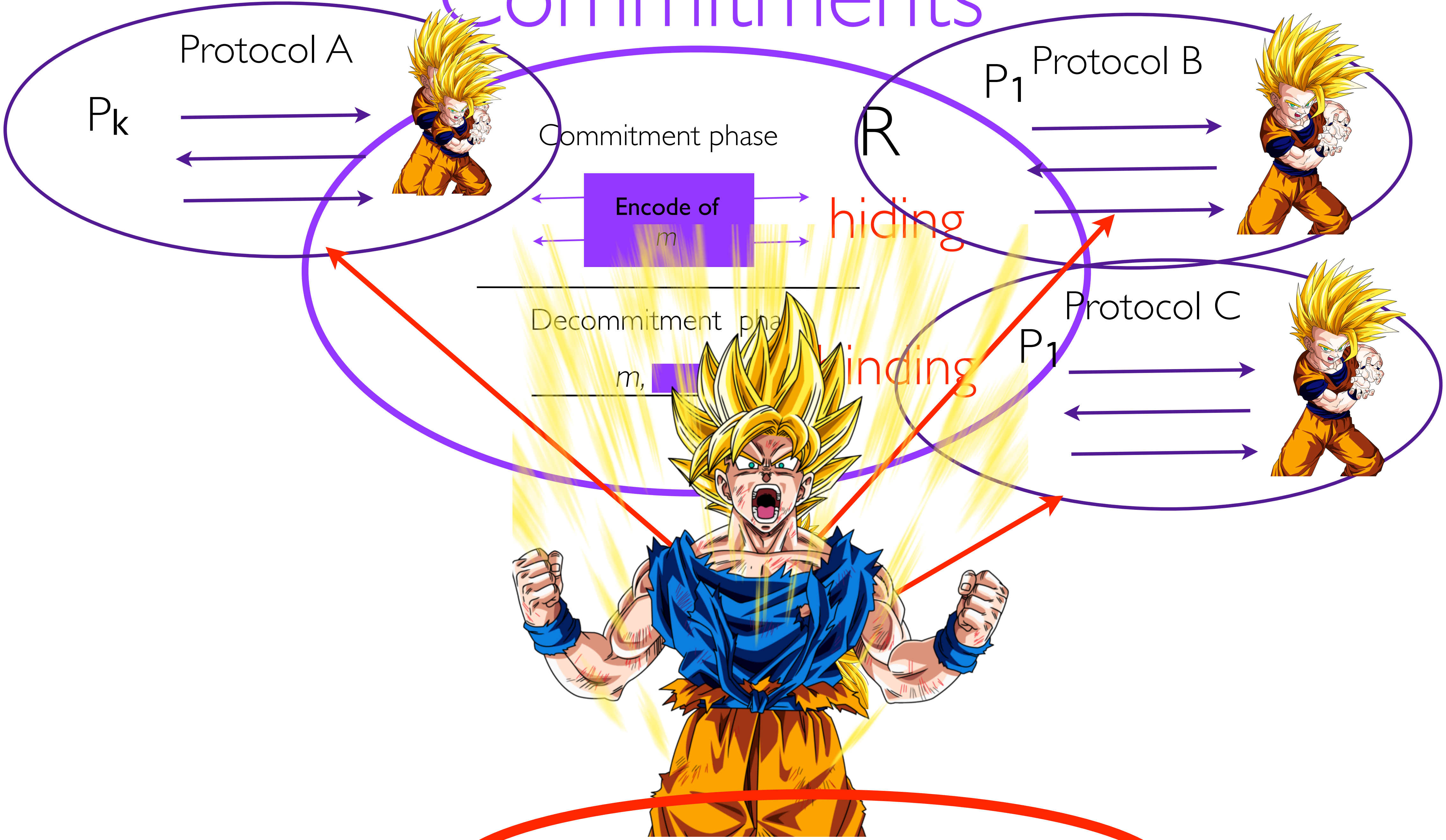


[CKL03] Setup Assumptions

Unconditionally Secure

Universally Composable

Commitments



Physical Assumptions

Physical Assumptions

Tamper-proof
hardware token

Physically Uncloneable Functions
PUFs

Physical Assumptions

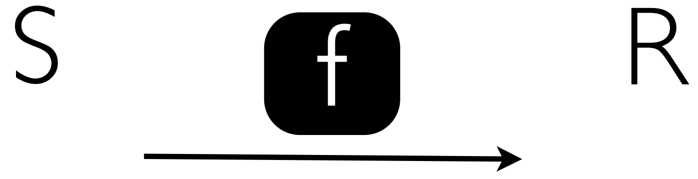
Tamper-proof
hardware token

S R

Physically Uncloneable Functions
PUFs

Physical Assumptions

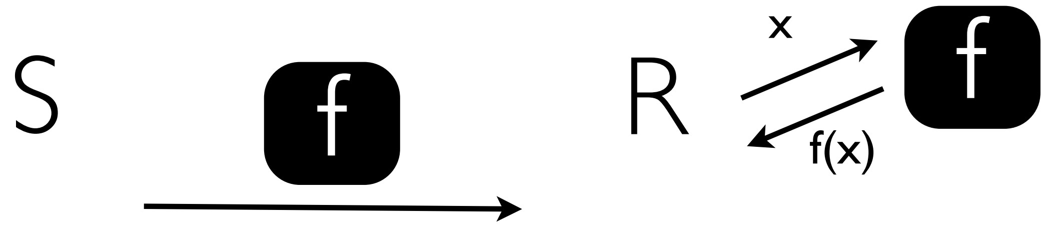
Tamper-proof
hardware token



Physically Uncloneable Functions
PUFs

Physical Assumptions

Tamper-proof
hardware token



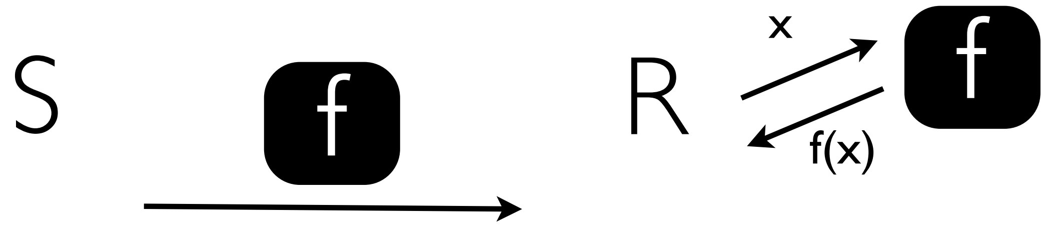
Physically Uncloneable Functions
PUFs

Physical Assumptions

Tamper-proof hardware token

Assumption: tamper-proof

R learns only f(x)



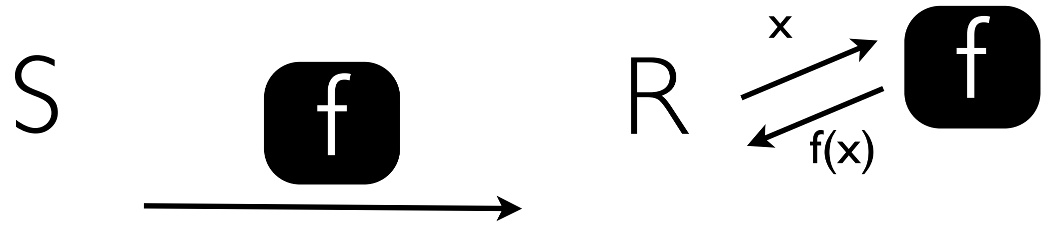
Physically Uncloneable Functions PUFs

Physical Assumptions

Tamper-proof
hardware token

Assumption: tamper-proof

R learns only f(x)



Stateful

- (tamper-proof) updatable memory
- reset attacks

Stateless

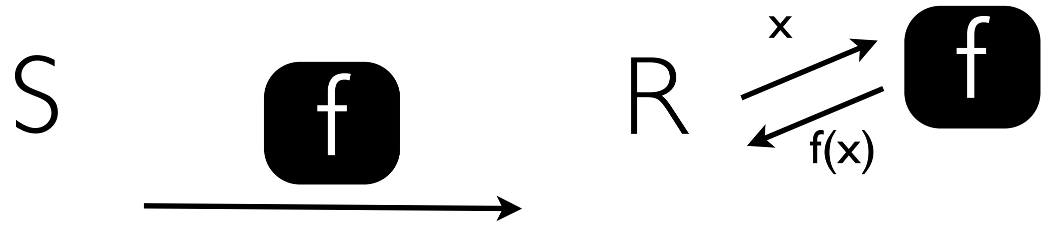
Physically Uncloneable Functions
PUFs

Physical Assumptions

Tamper-proof
hardware token

Assumption: tamper-proof

R learns only f(x)



Stateful

- (tamper-proof) updatable memory
- reset attacks

Stateless

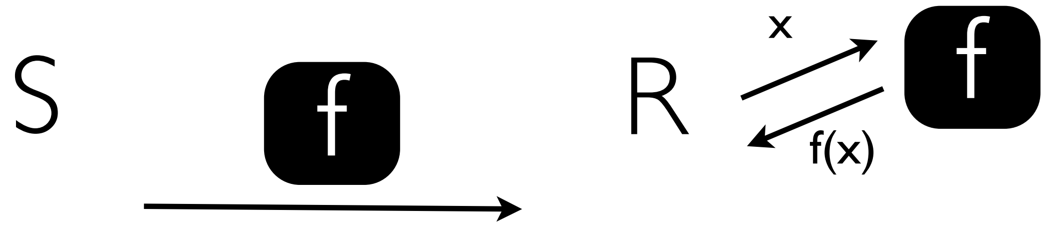
Physically Uncloneable Functions
PUFs

Physical Assumptions

Tamper-proof
hardware token

Assumption: tamper-proof

R learns only f(x)



Stateful

- (tamper-proof) updatable memory
- reset attacks

Stateless

Physically Uncloneable Functions
PUFs

S

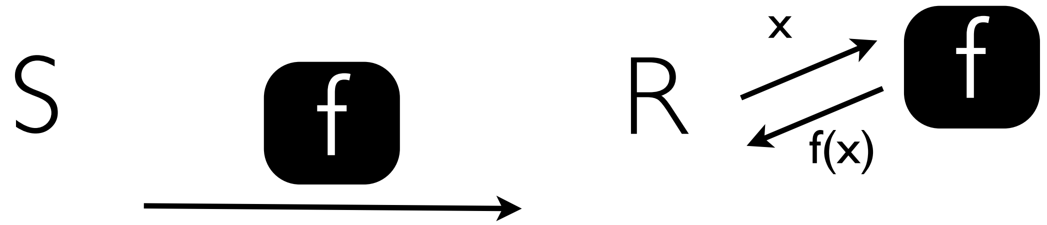
R

Physical Assumptions

Tamper-proof hardware token

Assumption: tamper-proof

R learns only f(x)

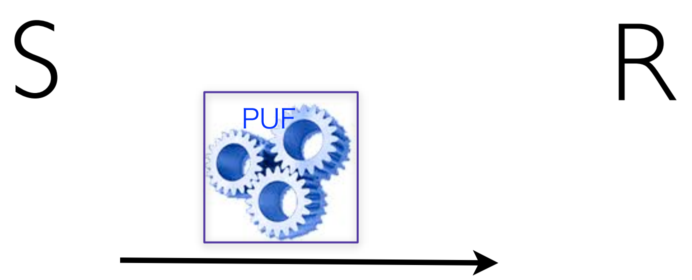


Stateful

- (tamper-proof) updatable memory
- reset attacks

Stateless

Physically Uncloneable Functions PUFs

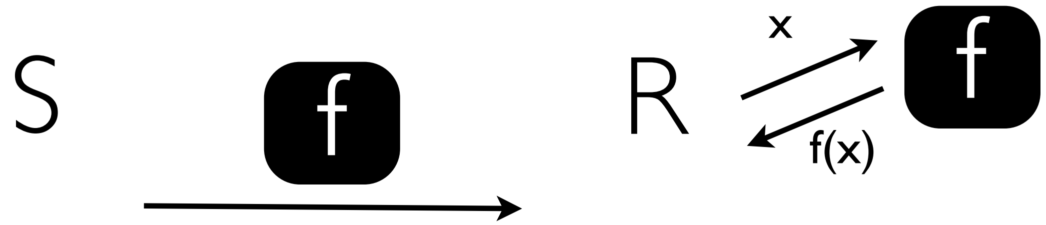


Physical Assumptions

Tamper-proof hardware token

Assumption: tamper-proof

R learns only f(x)

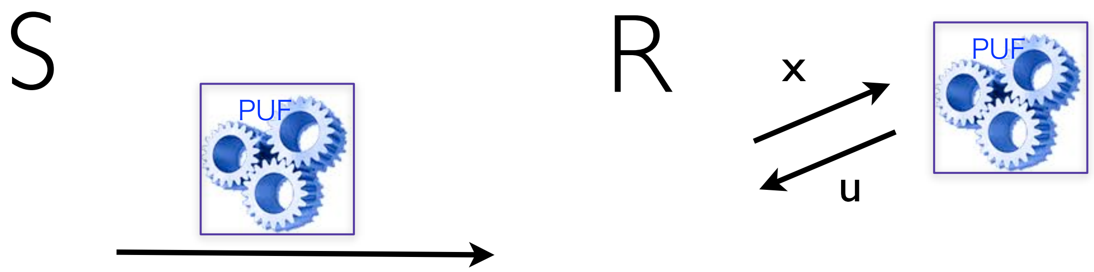


Stateful

- (tamper-proof) updatable memory
- reset attacks

Stateless

Physically Uncloneable Functions PUFs

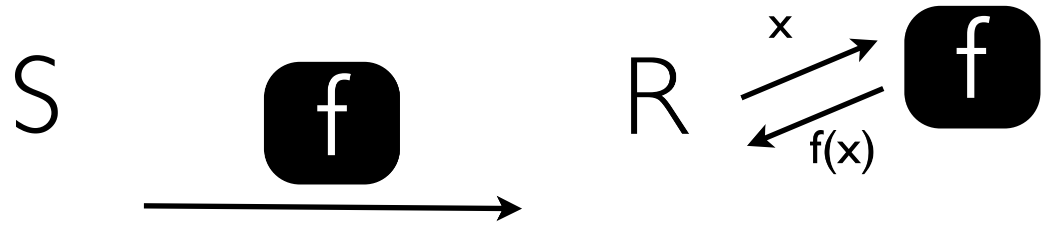


Physical Assumptions

Tamper-proof hardware token

Assumption: tamper-proof

R learns only f(x)



Stateful

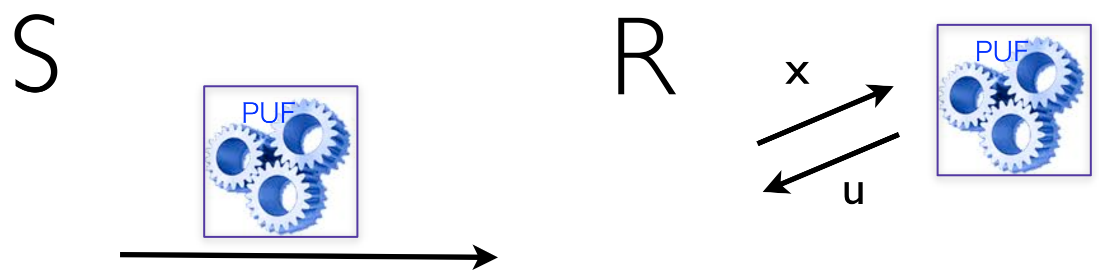
- (tamper-proof) updatable memory
- reset attacks

Stateless

Physically Uncloneable Functions PUFs

Assumption: unpredicatability

R cannot predict the answer on y != x (with y far from x)

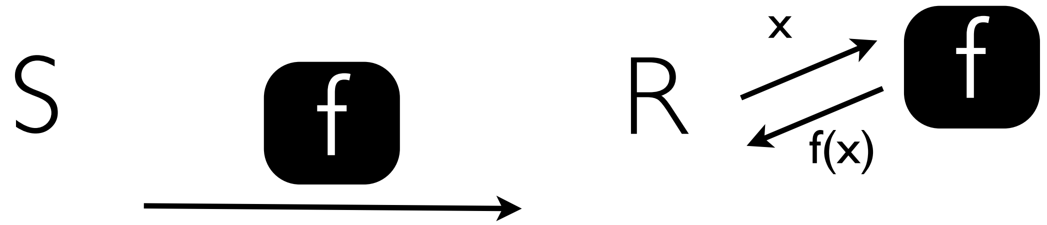


Physical Assumptions

Tamper-proof hardware token

Assumption: tamper-proof

R learns only f(x)



Stateful

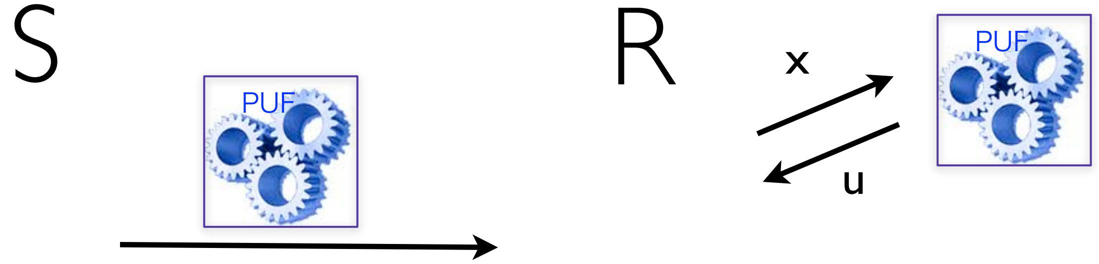
- (tamper-proof) updatable memory
- reset attacks

Stateless

Physically Uncloneable Functions PUFs

Assumption: unpredicatability

R cannot predict the answer on y != x (with y far from x)



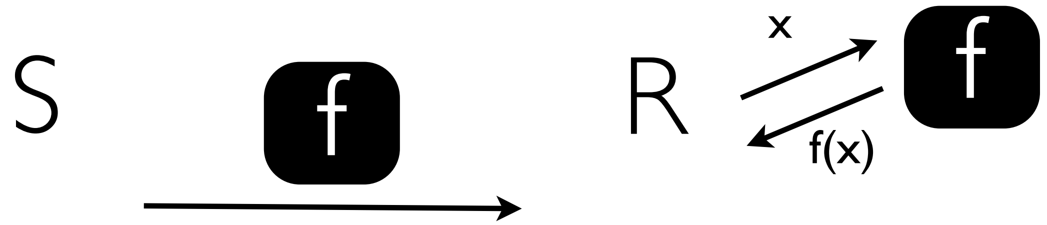
unpredictability holds for “far enough” challenges

Physical Assumptions

Tamper-proof hardware token

Assumption: tamper-proof

R learns only f(x)



Stateful

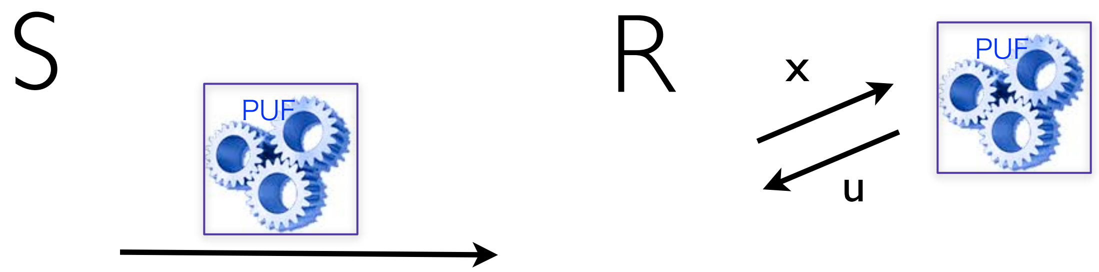
- (tamper-proof) updatable memory
- reset attacks

Stateless

Physically Uncloneable Functions PUFs

Assumption: unpredicatability

R cannot predict the answer on y != x (with y far from x)



unpredictability holds for “far enough” challenges

Assumption

physically uncloneable

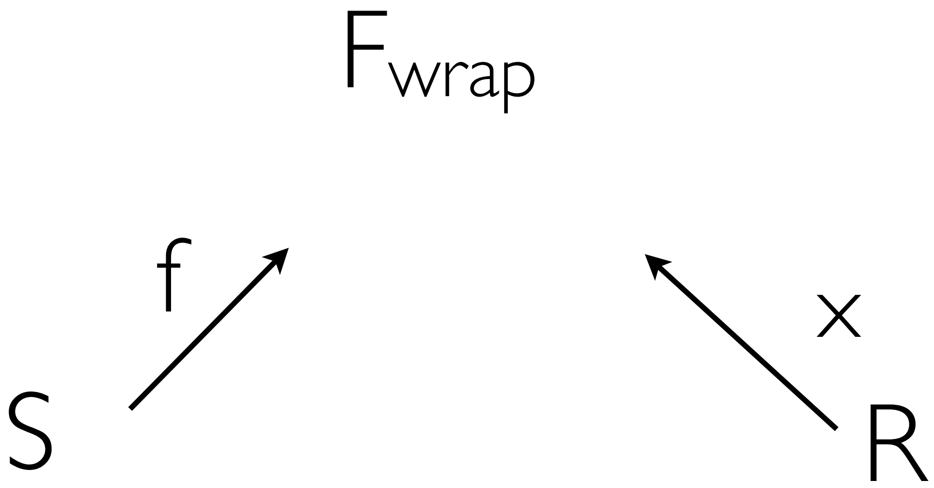
UC-Modeling Physical Assumptions

Tamper-proof Model
[Katz07]

(Malicious) PUF- Model
[BFKS11,OSVW13]

UC-Modeling Physical Assumptions

Tamper-proof Model
[Katz07]



F_{wrap}

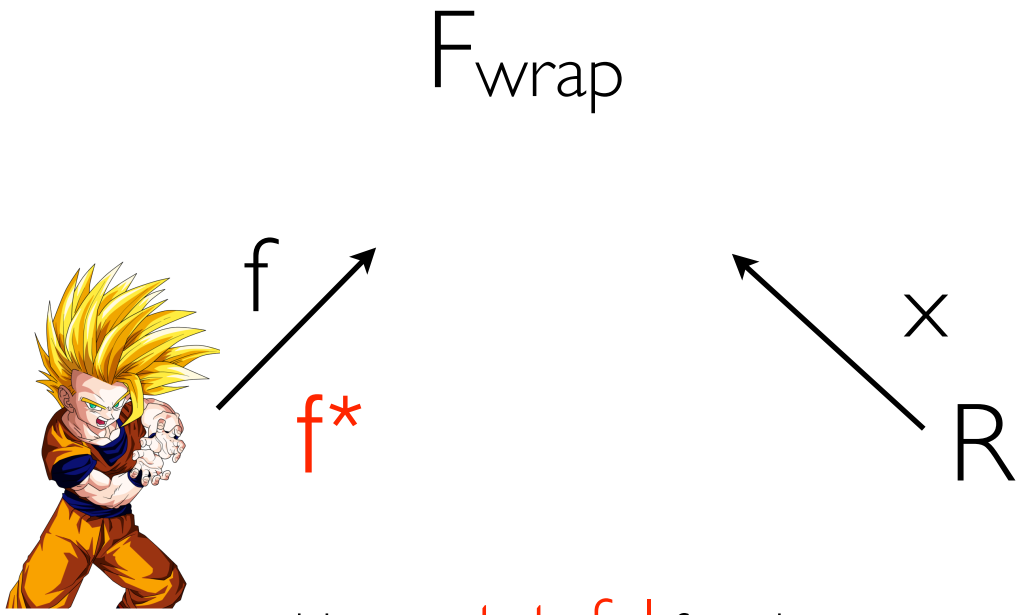
$S \xrightarrow{f}$

$\xleftarrow{x} R$

(Malicious) PUF- Model
[BFKS11,OSVW13]

UC-Modeling Physical Assumptions

Tamper-proof Model [Katz07]



F_{wrap}

f

f*

x

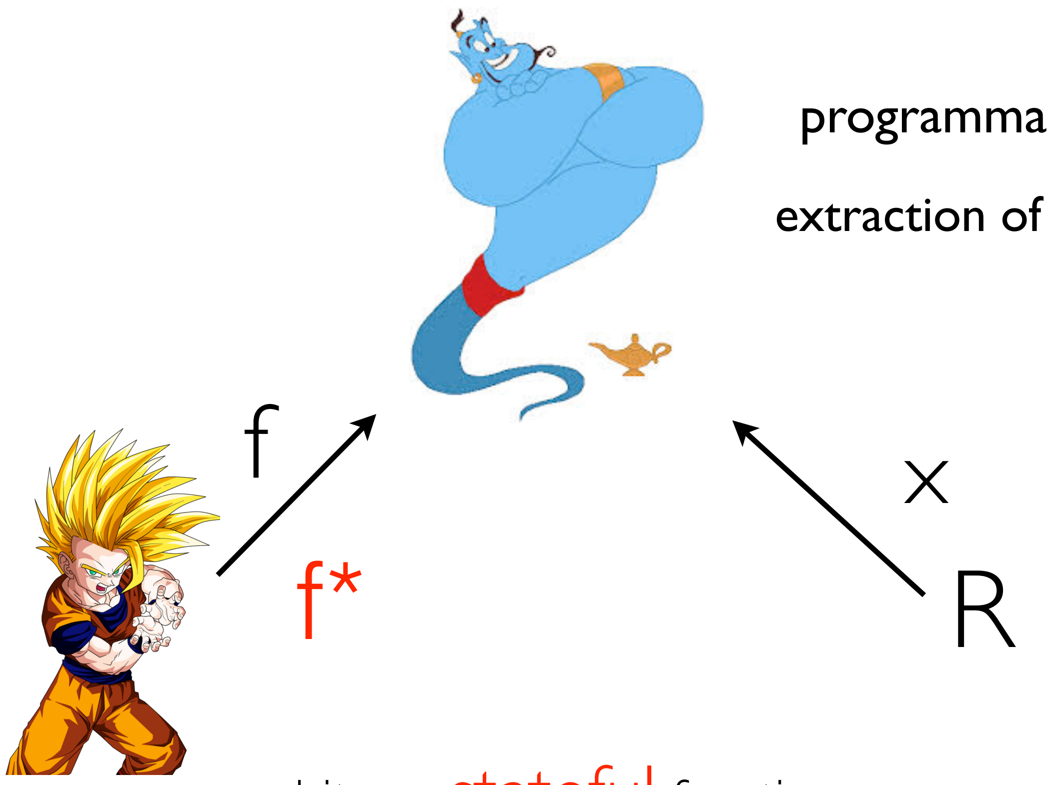
R

arbitrary stateful function

(Malicious) PUF- Model [BFKS11,OSVW13]

UC-Modeling Physical Assumptions

Tamper-proof Model [Katz07]



programmable

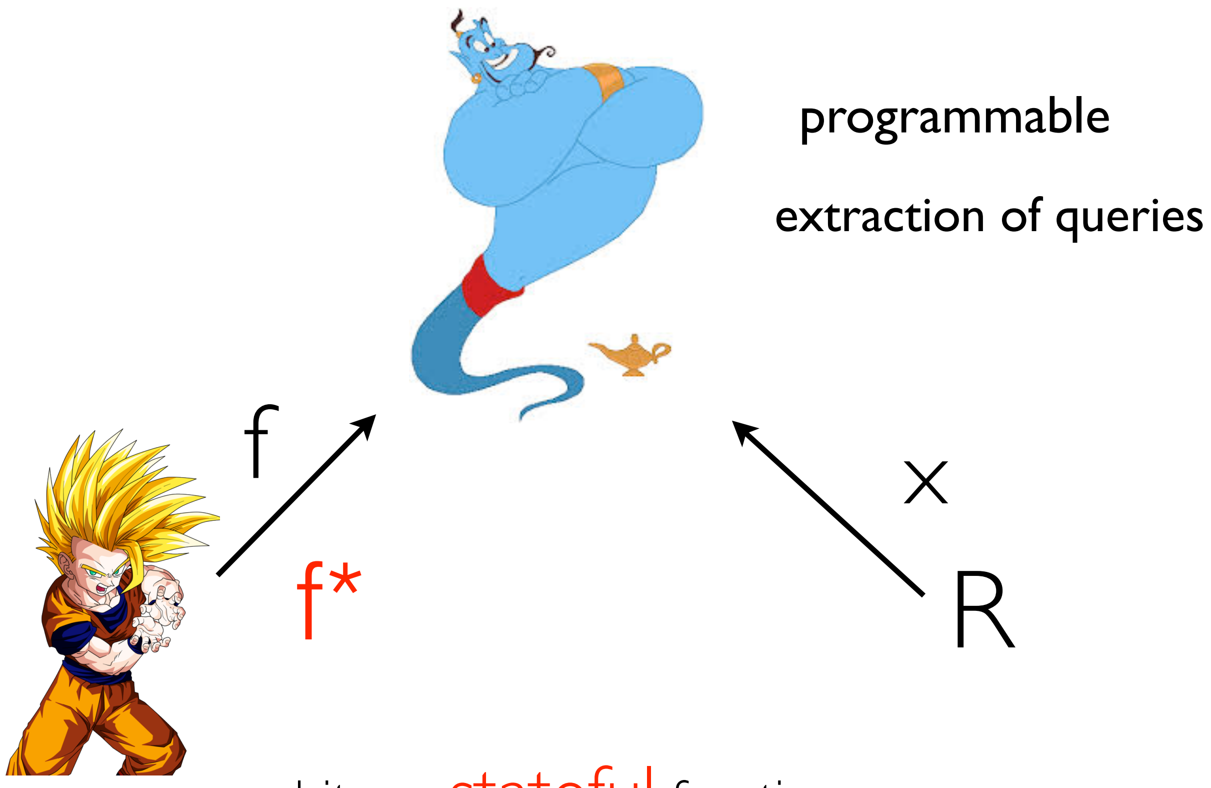
extraction of queries

arbitrary stateful function

(Malicious) PUF- Model [BFKS11,OSVW13]

UC-Modeling Physical Assumptions

Tamper-proof Model [Katz07]



programmable

extraction of queries

f

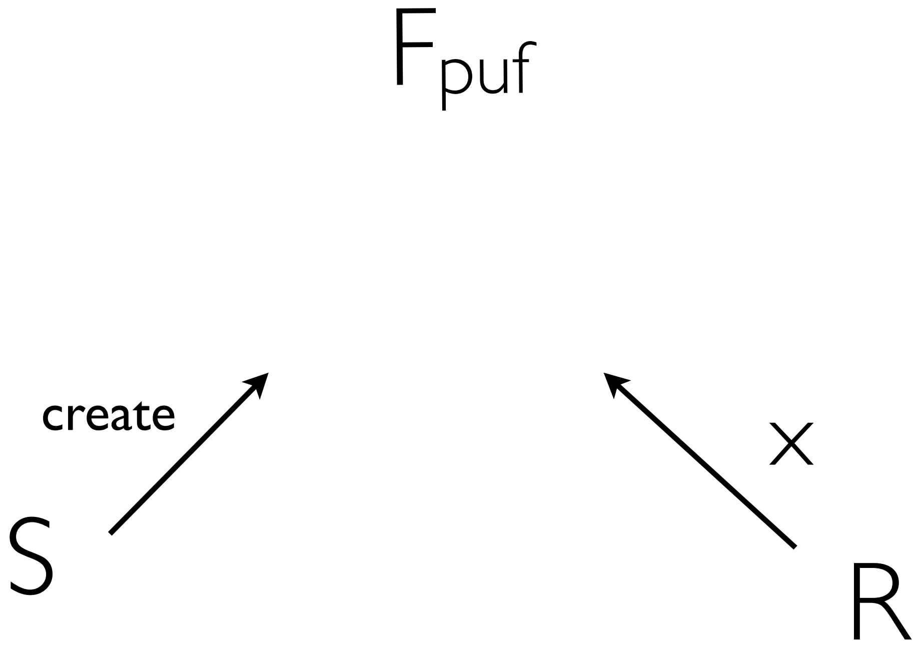
f*

x

R

arbitrary stateful function

(Malicious) PUF- Model [BFKS11,OSVW13]



F_{puf}

create

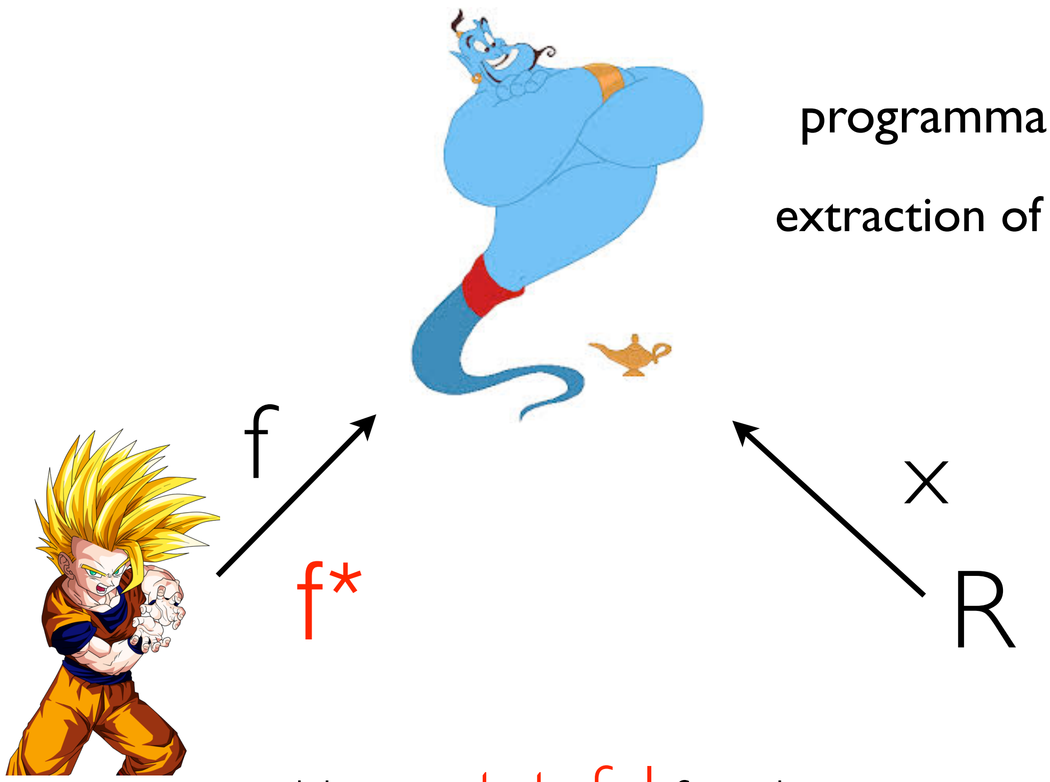
S

x

R

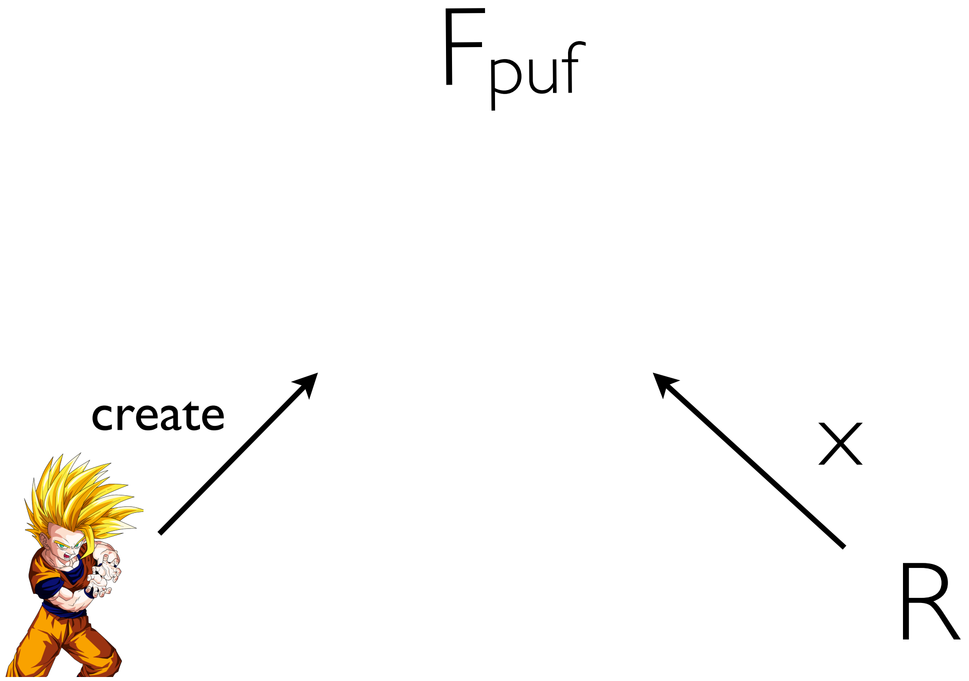
UC-Modeling Physical Assumptions

Tamper-proof Model [Katz07]



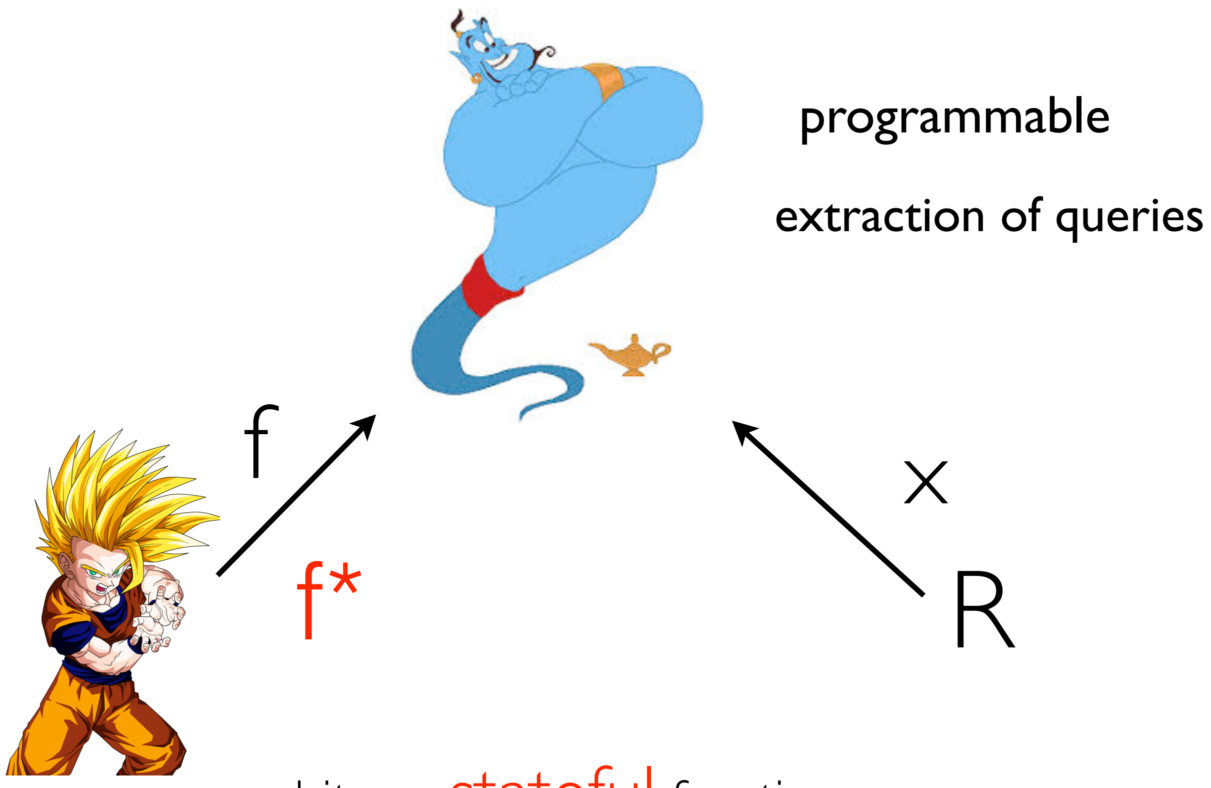
arbitrary stateful function

(Malicious) PUF- Model [BFKS11,OSVW13]



UC-Modeling Physical Assumptions

Tamper-proof Model [Katz07]



programmable

extraction of queries

f

f*

x

R

arbitrary stateful function

(Malicious) PUF- Model [BFKS11,OSVW13]

$F_{puf}^{p,p*}$

create

create*

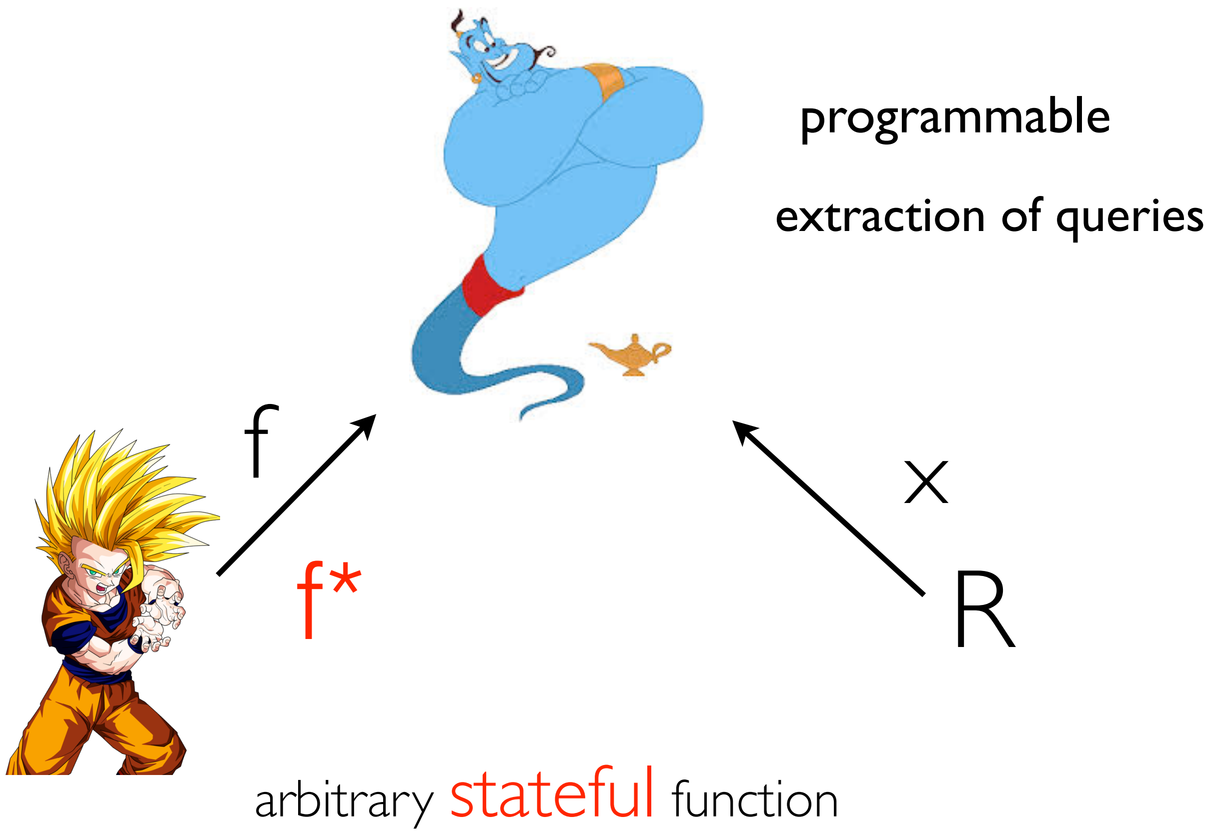
x

R

arbitrary stateful function

UC-Modeling Physical Assumptions

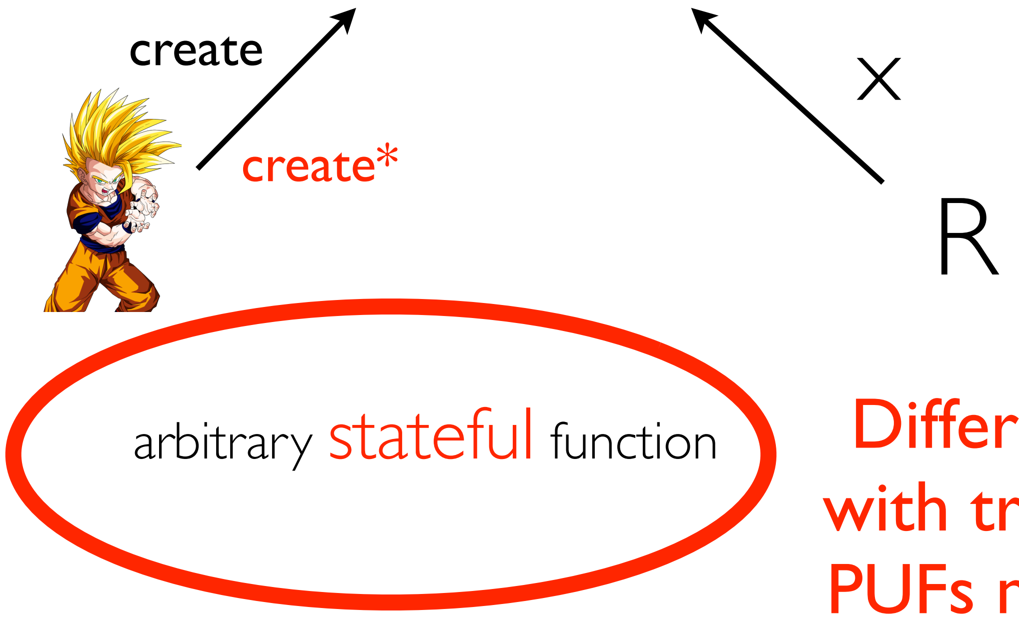
Tamper-proof Model [Katz07]



arbitrary stateful function

(Malicious) PUF- Model [BFKS11,OSVW13]

$F_{puf}^{p,p*}$

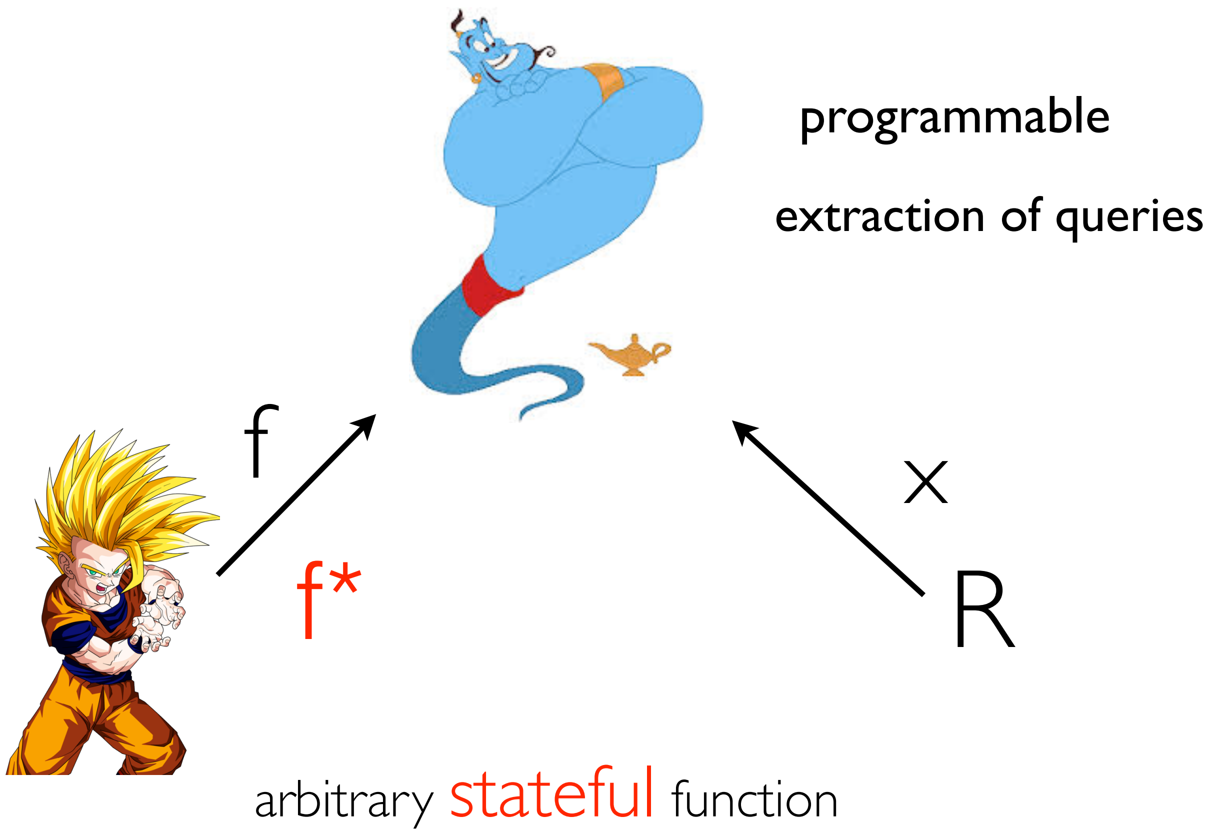


arbitrary stateful function

Difference with trusted PUFs model

UC-Modeling Physical Assumptions

Tamper-proof Model [Katz07]



programmable

extraction of queries

f

f*

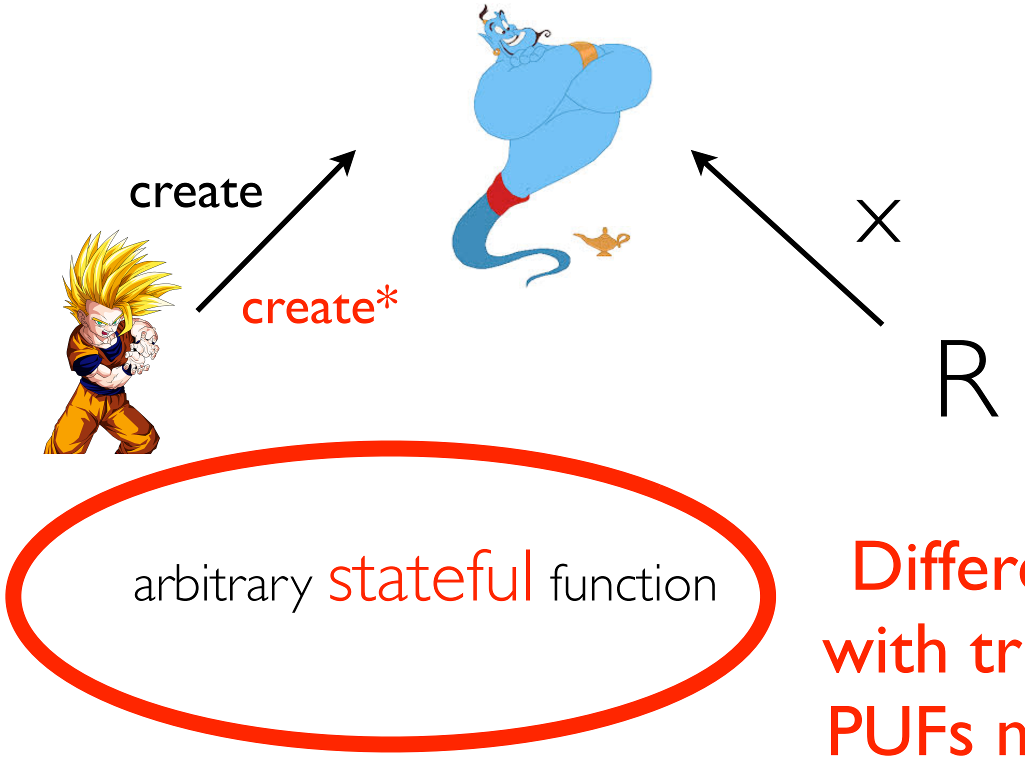
x

R

arbitrary stateful function

(Malicious) PUF- Model [BFKS11,OSVW13]

F_{puf}^{p,p^*}



create

create*

x

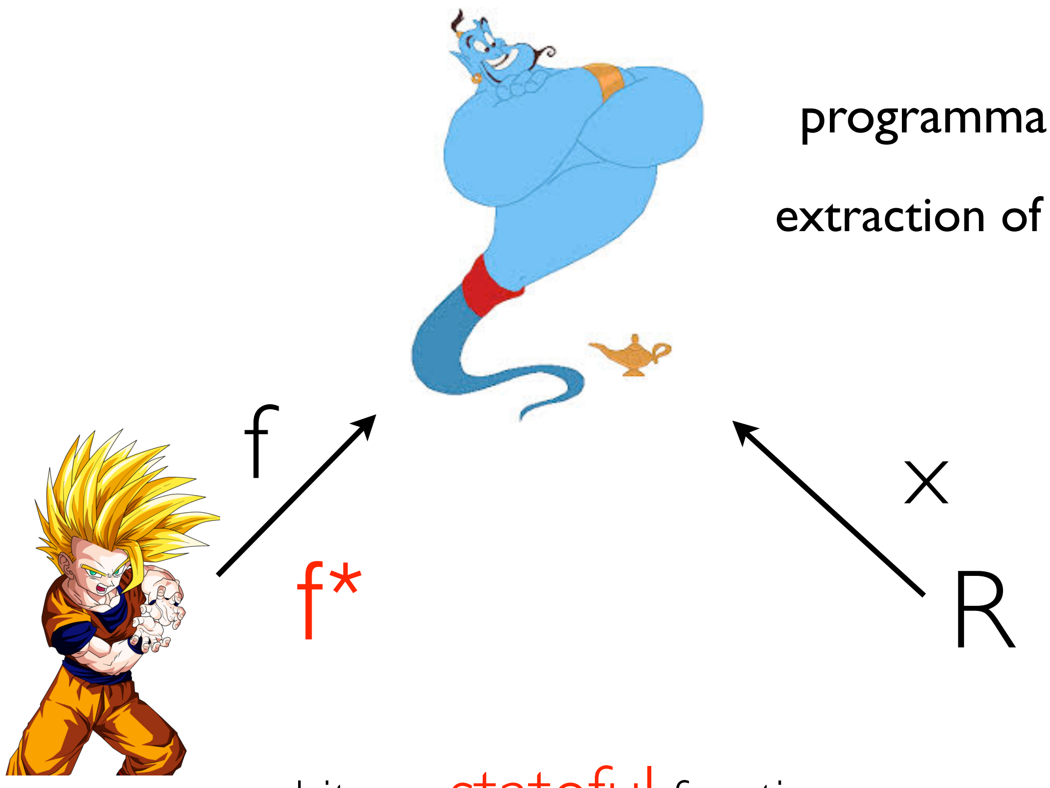
R

arbitrary stateful function

Difference with trusted PUFs model

UC-Modeling Physical Assumptions

Tamper-proof Model [Katz07]



f

f*

x

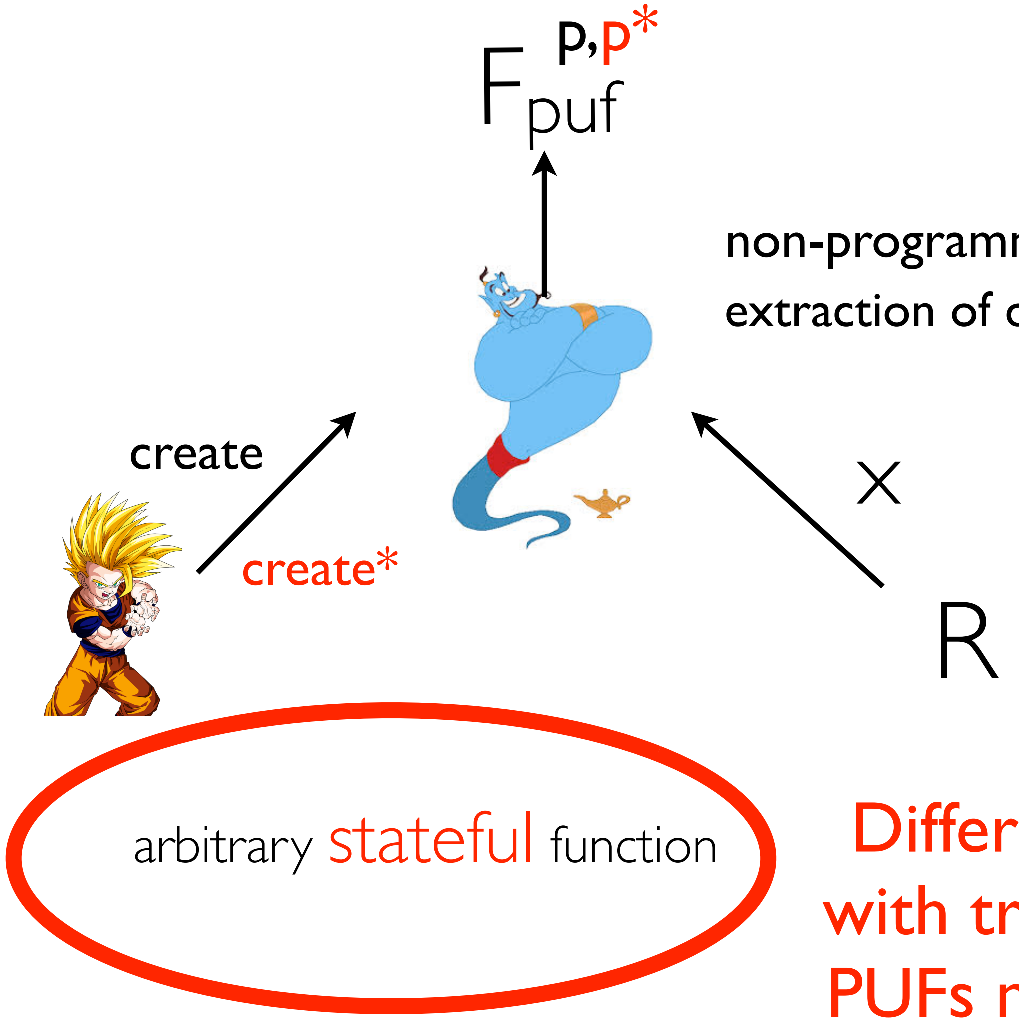
R

programmable

extraction of queries

arbitrary stateful function

(Malicious) PUF- Model [BFKS11,OSVW13]



$F_{puf}^{p,p*}$

non-programmable

extraction of queries

create

create*

x

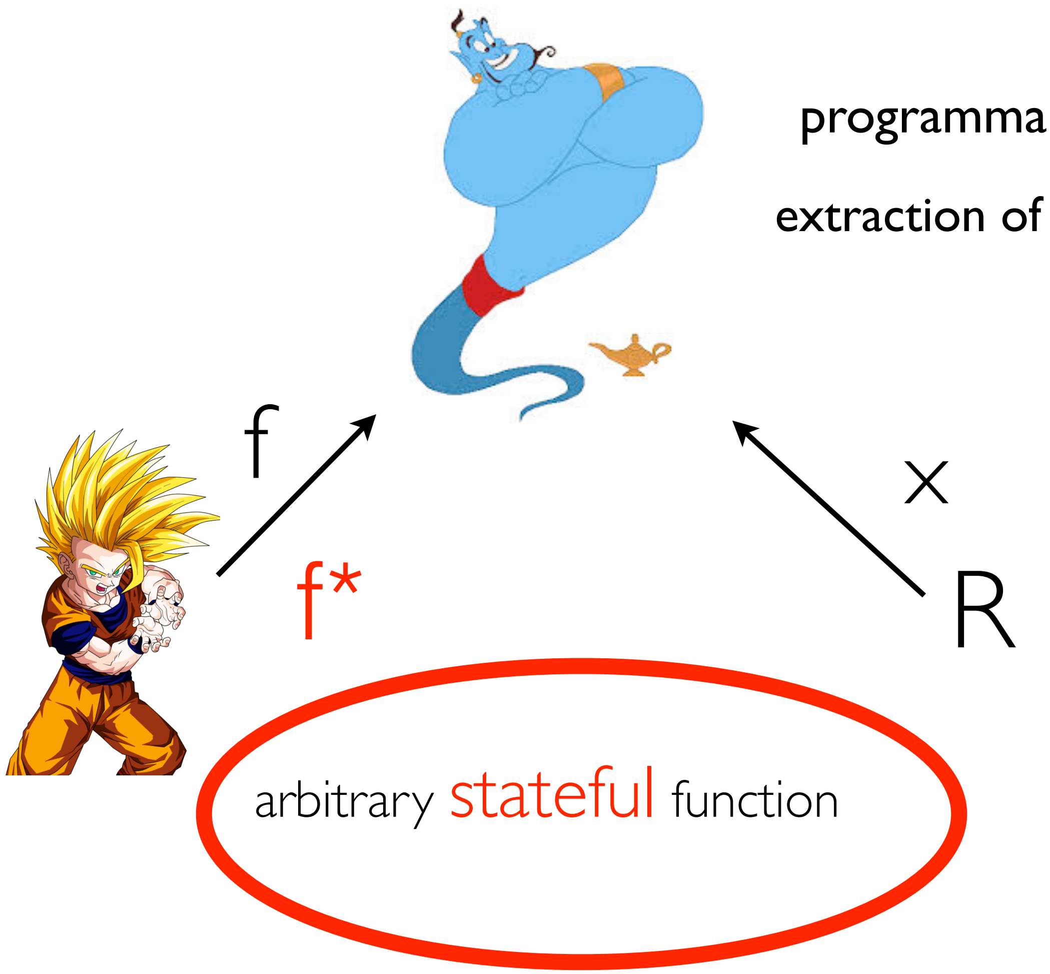
R

arbitrary stateful function

Difference with trusted PUFs model

UC-Modeling Physical Assumptions

Tamper-proof Model [Katz07]



programmable

extraction of queries

f

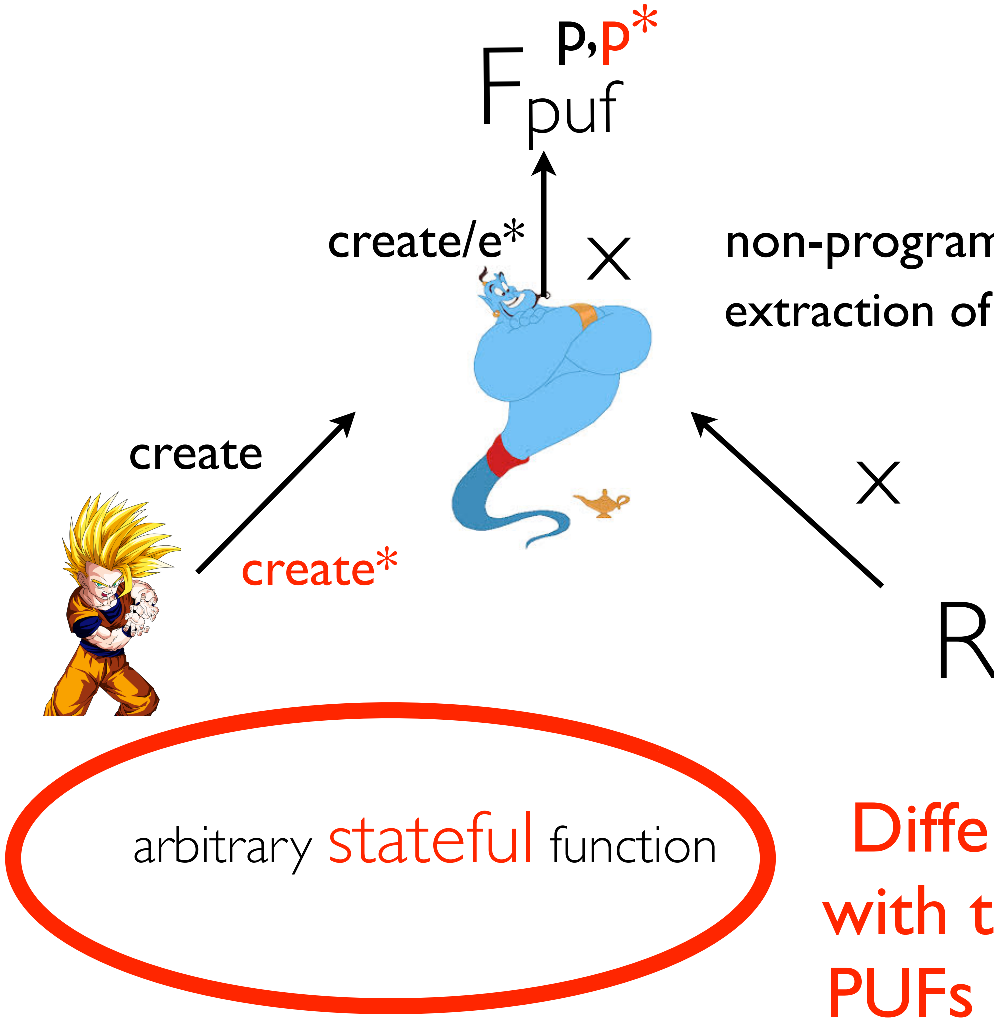
f*

×

R

arbitrary stateful function

(Malicious) PUF- Model [BFKS11,OSVW13]



F_{puf}^{P,P^*}

create/e*

×

non-programmable

extraction of queries

create

create*

×

R

arbitrary stateful function

Difference with trusted PUFs model

Crucial: the security of each party depends only on the "goodness" of its own hardware

State of the art

	Unconditional UC Oblivious Transfer	Unconditional UC Commitment
Stateless Tokens		
(Malicious) PUFs		

State of the art

	Unconditional UC Oblivious Transfer	Unconditional UC Commitment
Stateless Tokens	Impossible [GIMS10]	
(Malicious) PUFs		

State of the art

	Unconditional UC Oblivious Transfer	Unconditional UC Commitment
Stateless Tokens	Impossible [GIMS10]	stand-alone Com [GIMS10] restricted adversary
(Malicious) PUFs		

State of the art

	Unconditional UC Oblivious Transfer	Unconditional UC Commitment
Stateless Tokens	Impossible [GIMS10]	stand-alone Com [GIMS10] restricted adversary ?
(Malicious) PUFs		

State of the art

	Unconditional UC Oblivious Transfer	Unconditional UC Commitment
Stateless Tokens	Impossible [GIMS10]	stand-alone Com [GIMS10] restricted adversary ?
(Malicious) PUFs	?	

State of the art

	Unconditional UC Oblivious Transfer	Unconditional UC Commitment
Stateless Tokens	Impossible [GIMS10]	stand-alone Com [GIMS10] restricted adversary ?
(Malicious) PUFs	?	stand-alone Com [OSVW13]

State of the art

	Unconditional UC Oblivious Transfer	Unconditional UC Commitment
Stateless Tokens	Impossible [GIMS10]	stand-alone Com [GIMS10] restricted adversary ?
(Malicious) PUFs	?	stand-alone Com [OSVW13] ?

State of the art

	Unconditional UC Oblivious Transfer	Unconditional UC Commitment
Stateless Tokens	Impossible [GIMS10]	stand-alone Com [GIMS10] restricted adversary ?
(Malicious) PUFs	?	stand-alone Com [OSVW13] ?

Caveat: Adv allowed to only poly queries

In this paper

	Unconditional UC Oblivious Transfer	Unconditional UC Commitment
Stateless Tokens	Impossible [GIMS10]	stand-alone Com [GIMS10] restricted adversary ?
(Malicious) PUFs	?	stand-alone Com [OSVW13] ?

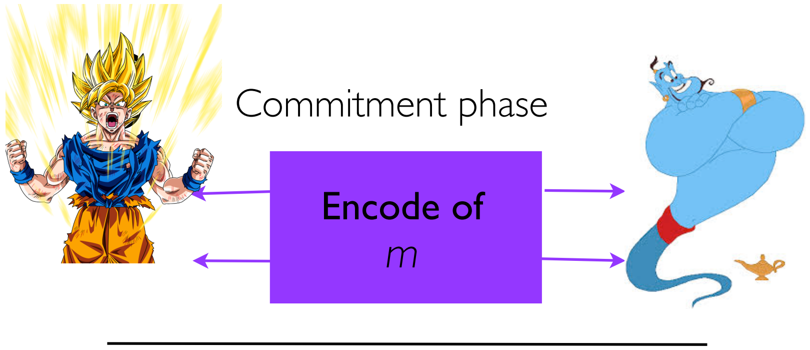
In this paper

	Unconditional UC Oblivious Transfer	Unconditional UC Commitment
Stateless Tokens	Impossible [GIMS10]	Yes
(Malicious) PUFs	?	stand-alone Com [OSVW13] ?

In this paper

	Unconditional UC Oblivious Transfer	Unconditional UC Commitment
Stateless Tokens	Impossible [GIMS10]	Yes
(Malicious) PUFs	?	Yes

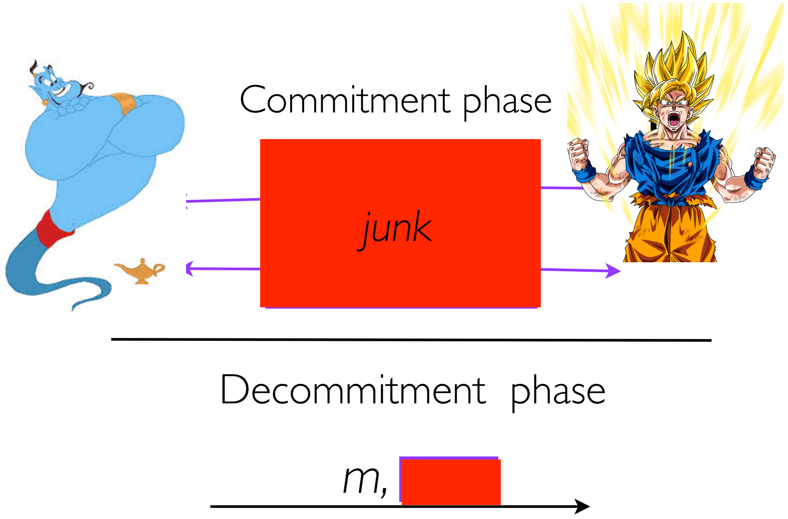
UC-Commitments with Physical Assumptions



Commitment phase

Encode of *m*

Straight-line extractable



Commitment phase

junk

Decommitment phase

m, 🟥

Straight-line equivocal

Our Technique

Our Technique

- Black-box Unconditional compiler

Our Technique

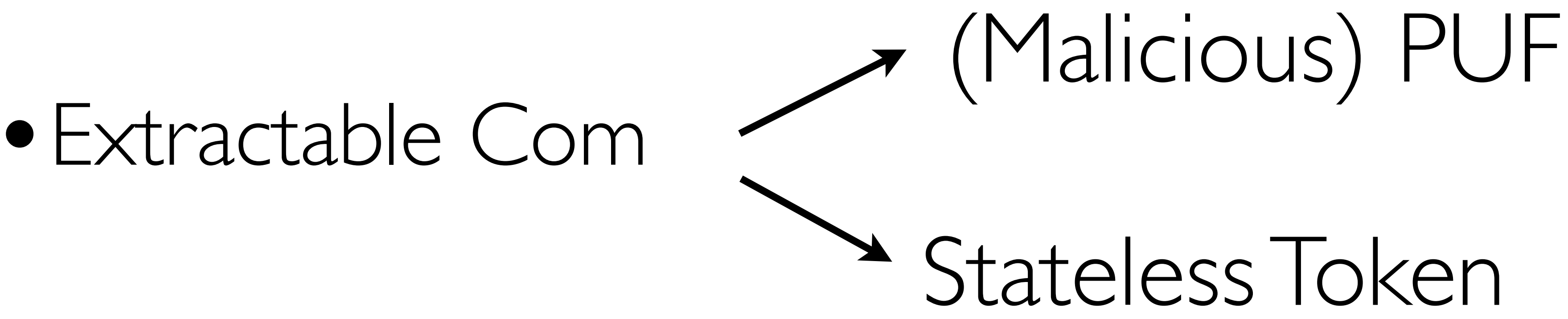
- Black-box Unconditional compiler

Extractable Com => Equivocal + Extractable Com

Our Technique

- Black-box Unconditional compiler

Extractable Com => Equivocal + Extractable Com



- Extractable Com

(Malicious) PUF

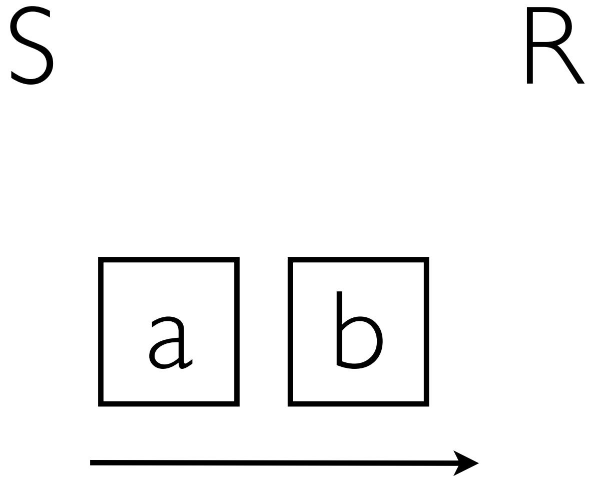
Stateless Token

Black-Box Compiler

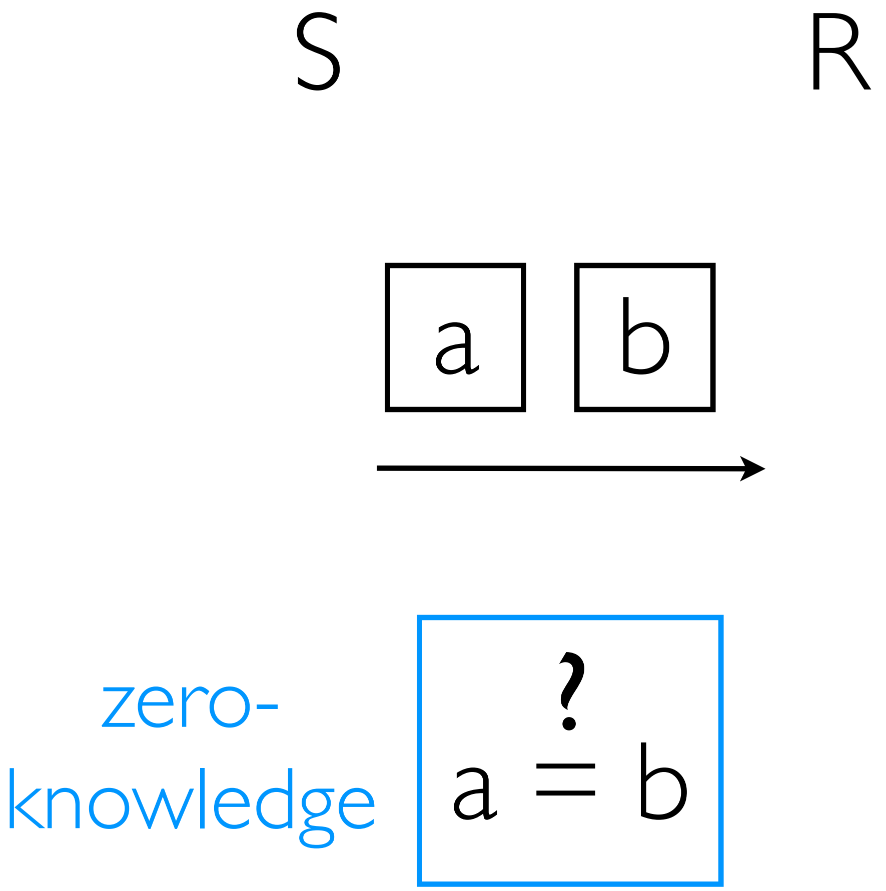
Black-box Proof of Equality of Commitments

S R

Black-box Proof of Equality of Commitments



Black-box Proof of Equality of Commitments



S

R

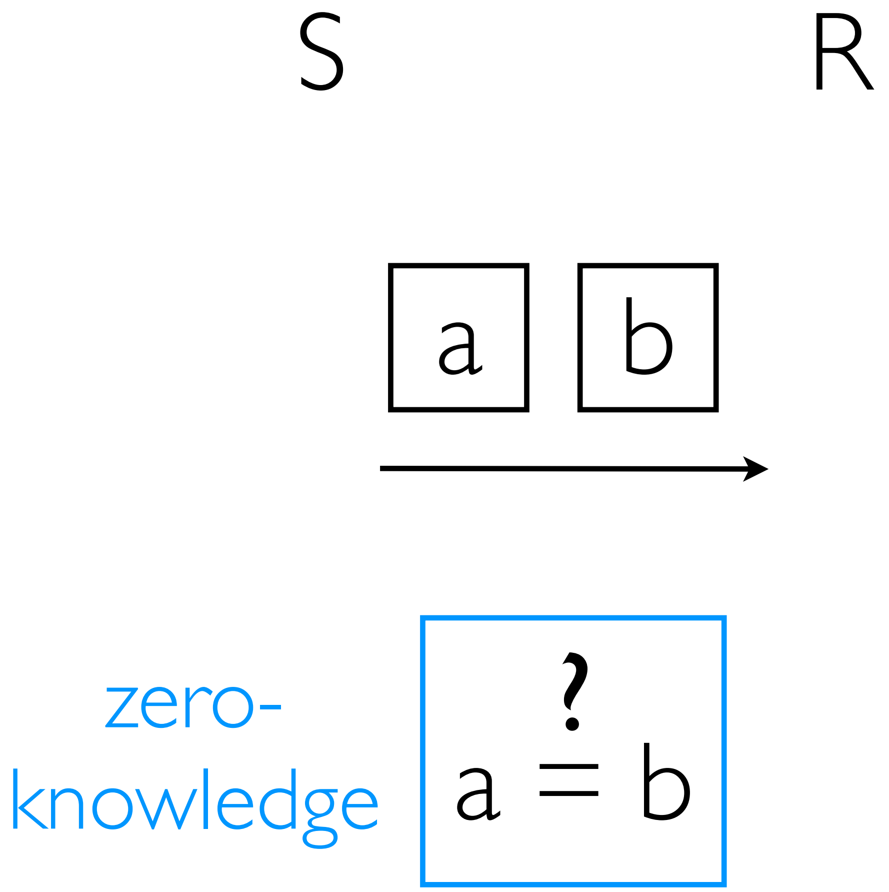
$\boxed{a}$ $\boxed{b}$

zero-knowledge

$a \overset{?}{=} b$

Black-box Proof of Equality of Commitments

Kilian 92



S

R

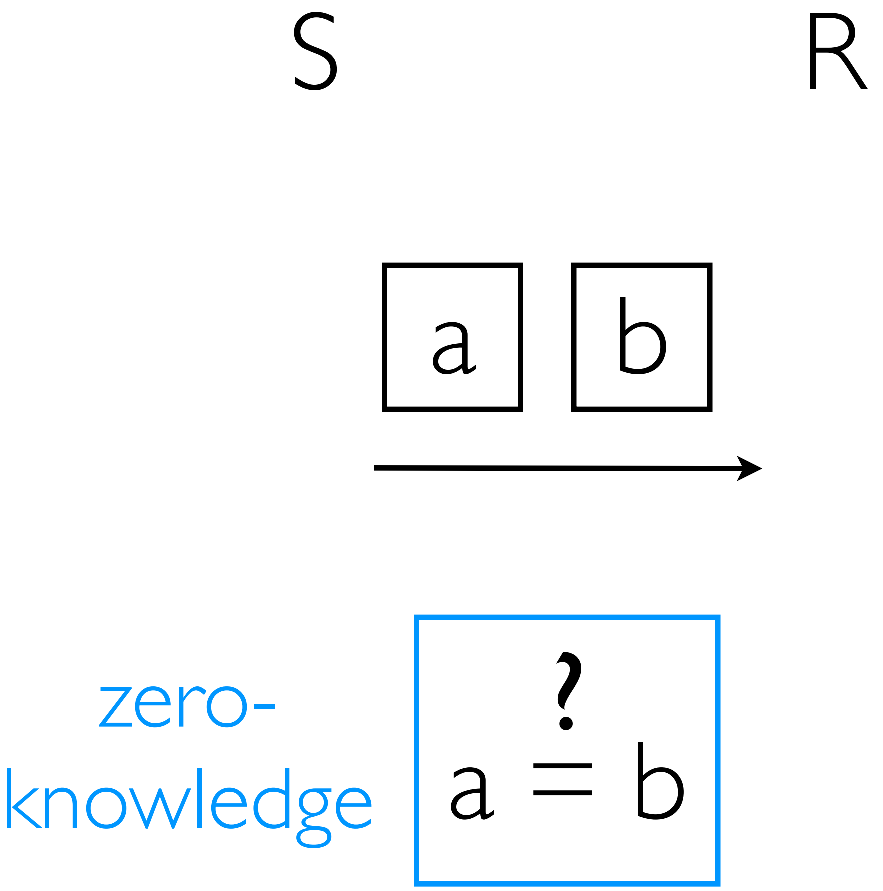
$\boxed{a}$ $\boxed{b}$

zero-knowledge

$a \overset{?}{=} b$

Black-box Proof of Equality of Commitments

Kilian 92



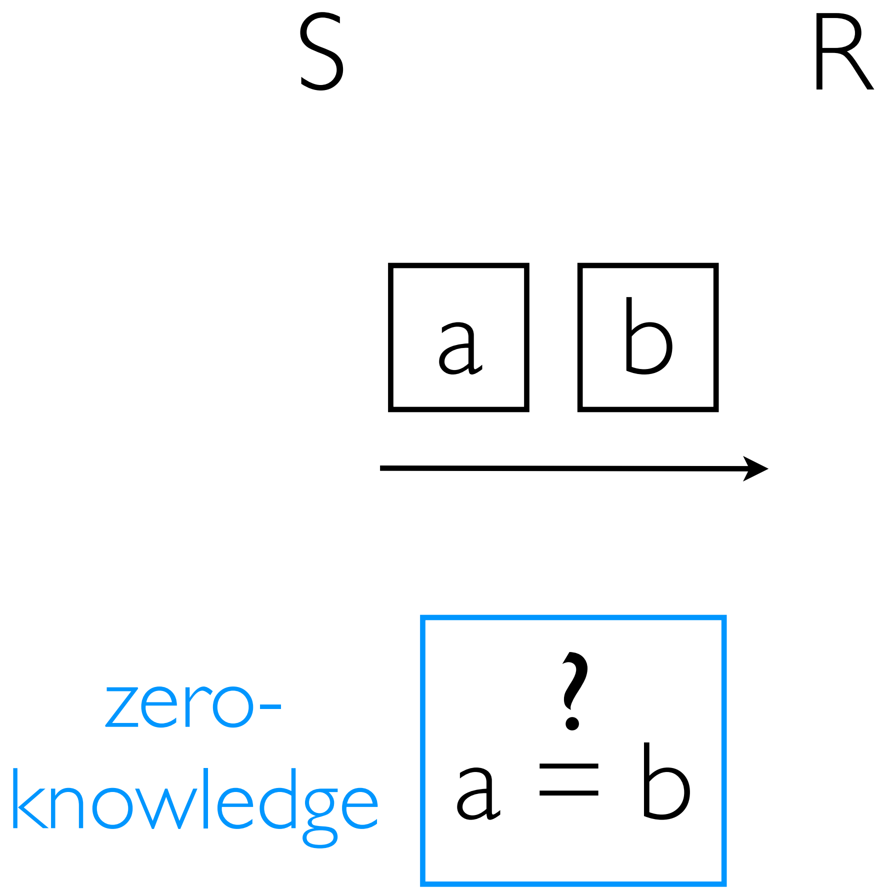
S R

$\boxed{a}$ $\boxed{b}$ $\xrightarrow{\qquad}$

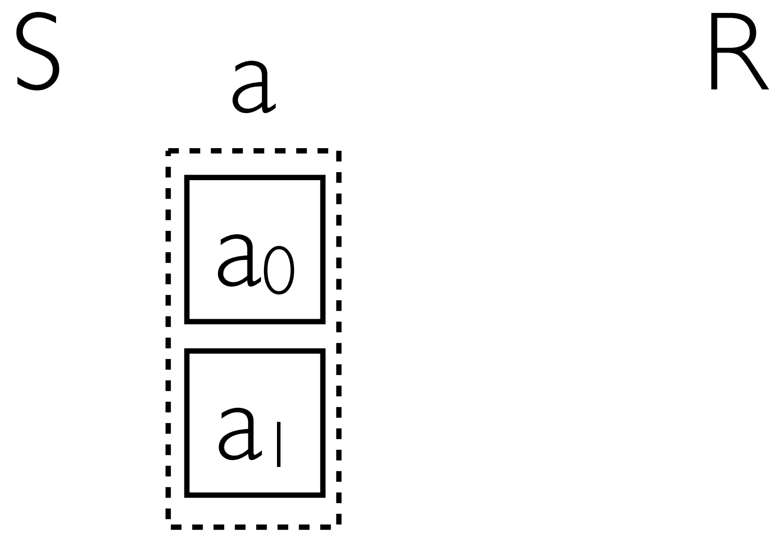
zero-knowledge $\boxed{a \overset{?}{=} b}$

S R

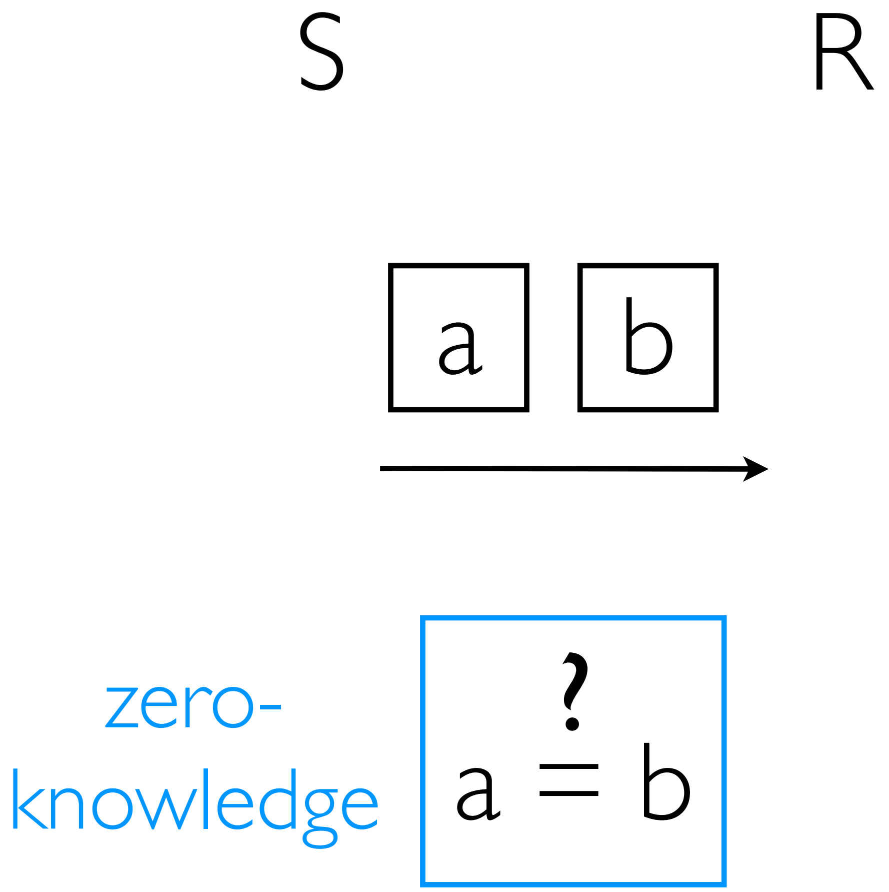
Black-box Proof of Equality of Commitments



Kilian 92



Black-box Proof of Equality of Commitments



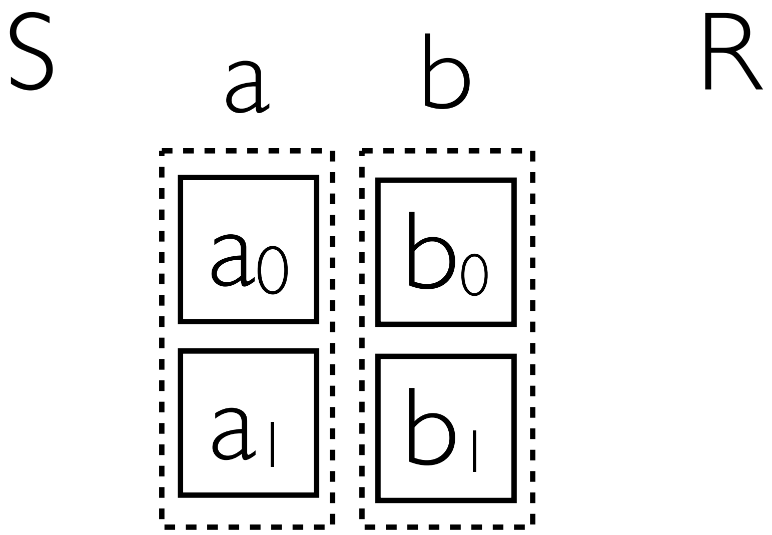
S R

$\boxed{a}$ $\boxed{b}$

zero-knowledge

$\boxed{a \overset{?}{=} b}$

Kilian 92

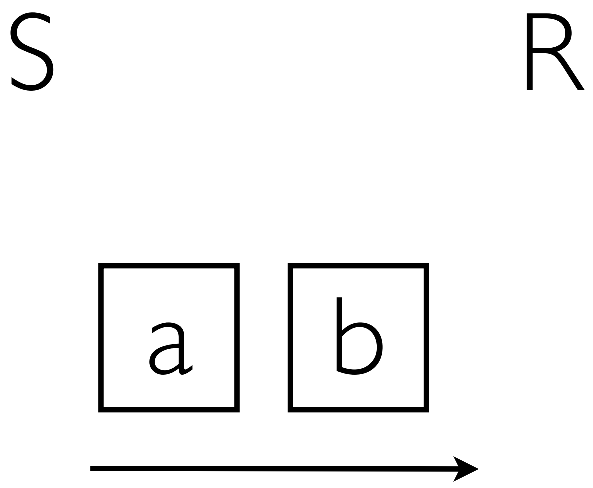


S a b R

$\boxed{a_0}$ $\boxed{b_0}$

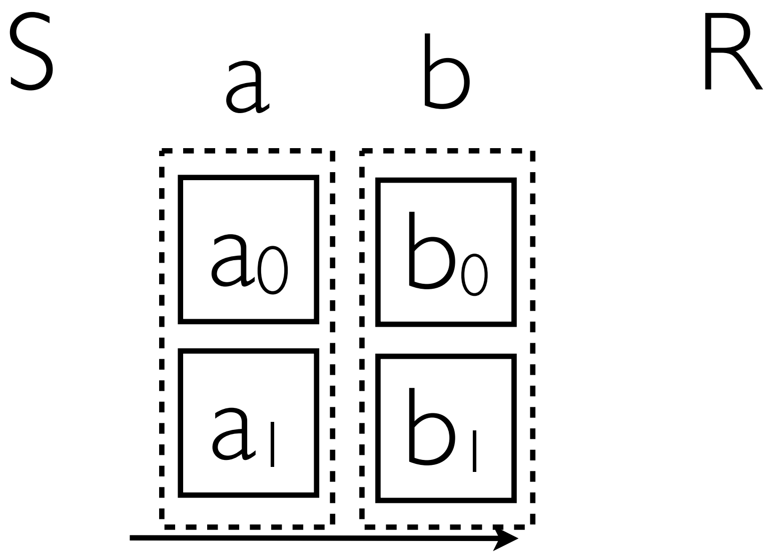
$\boxed{a_1}$ $\boxed{b_1}$

Black-box Proof of Equality of Commitments

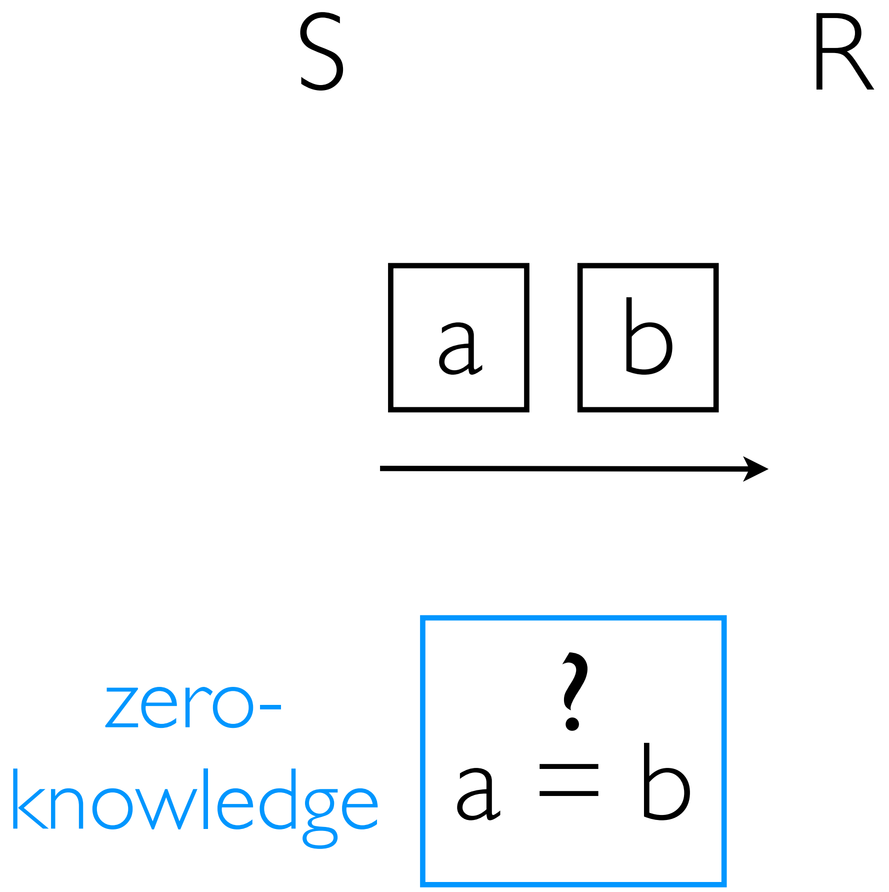


zero-knowledge $\boxed{a \overset{?}{=} b}$

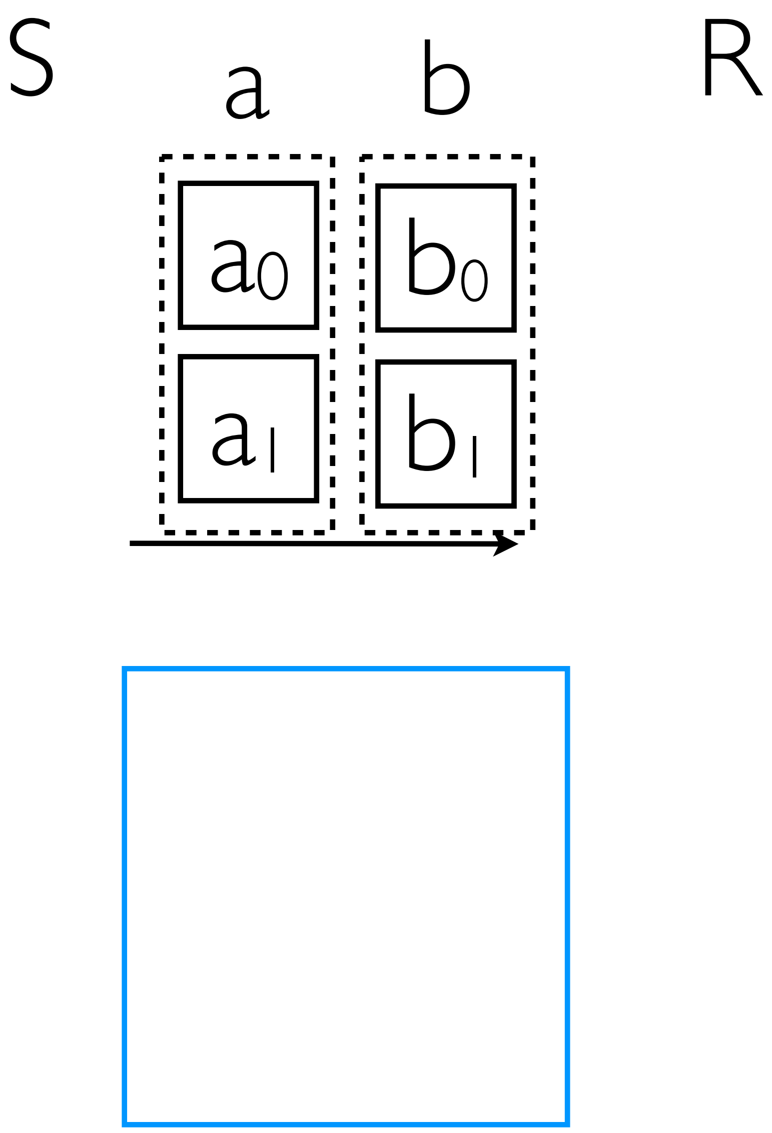
Kilian 92



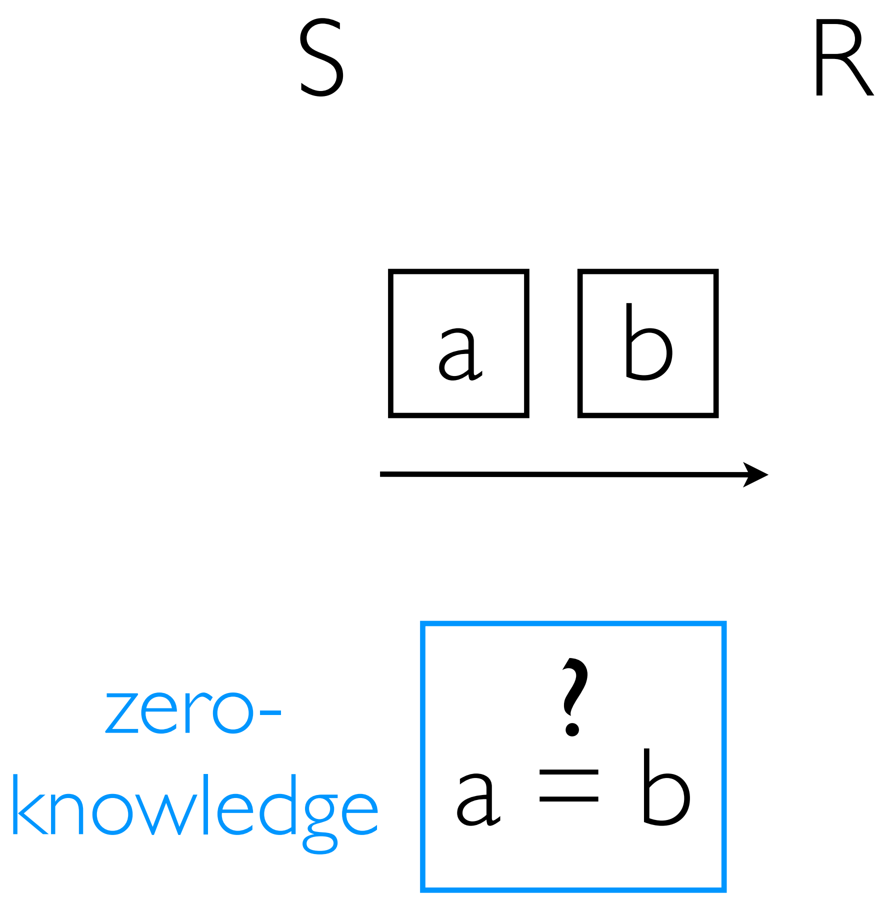
Black-box Proof of Equality of Commitments



Kilian 92



Black-box Proof of Equality of Commitments



S

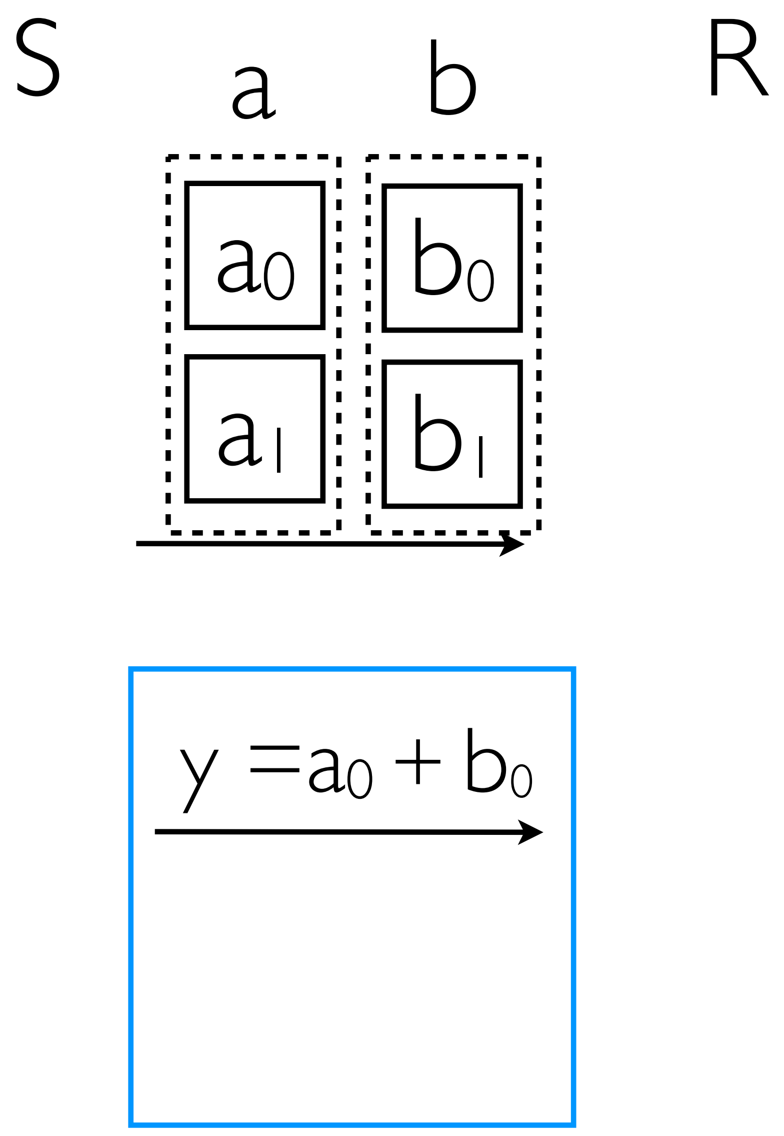
R

$\boxed{a}$ $\boxed{b}$

zero-knowledge

$a \overset{?}{=} b$

Kilian 92



S

a b

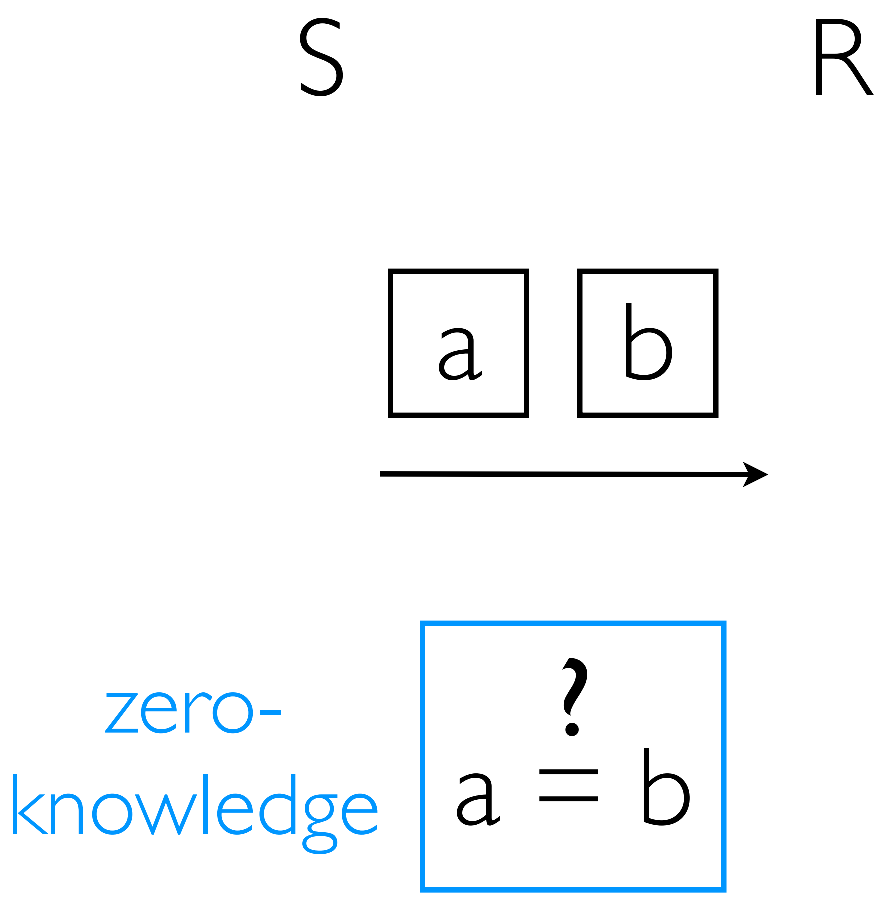
R

$\boxed{a_0}$ $\boxed{b_0}$

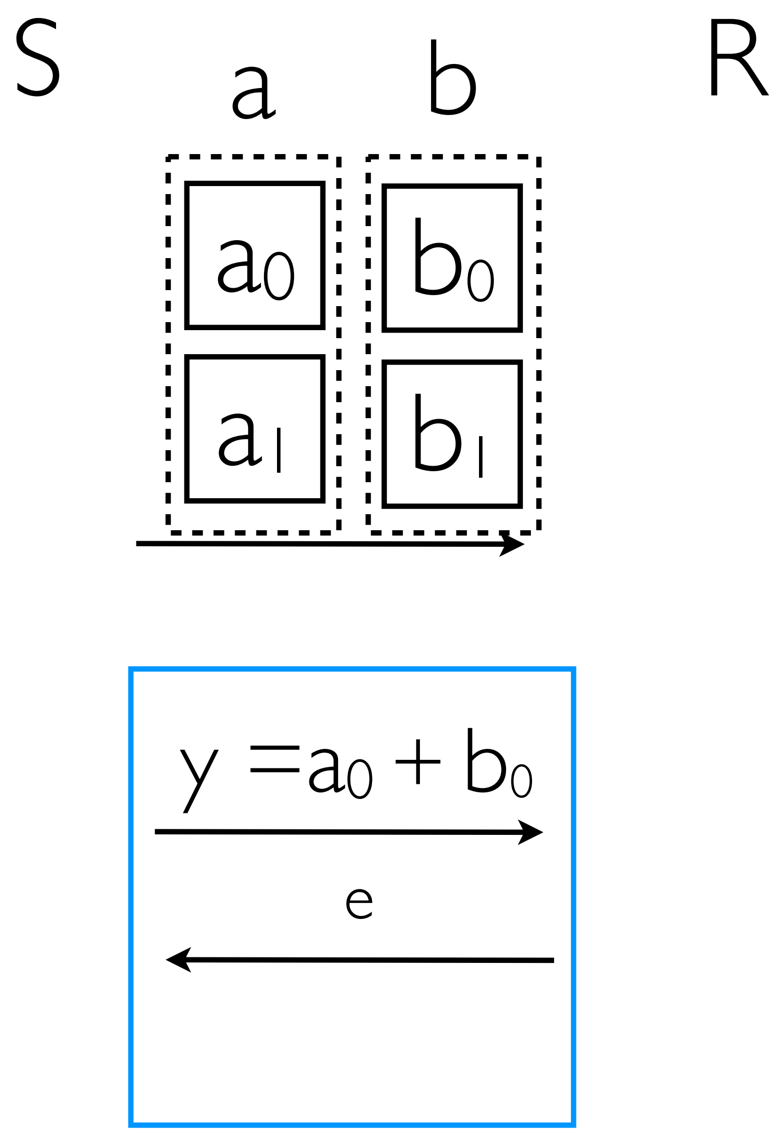
$\boxed{a_1}$ $\boxed{b_1}$

$y = a_0 + b_0$

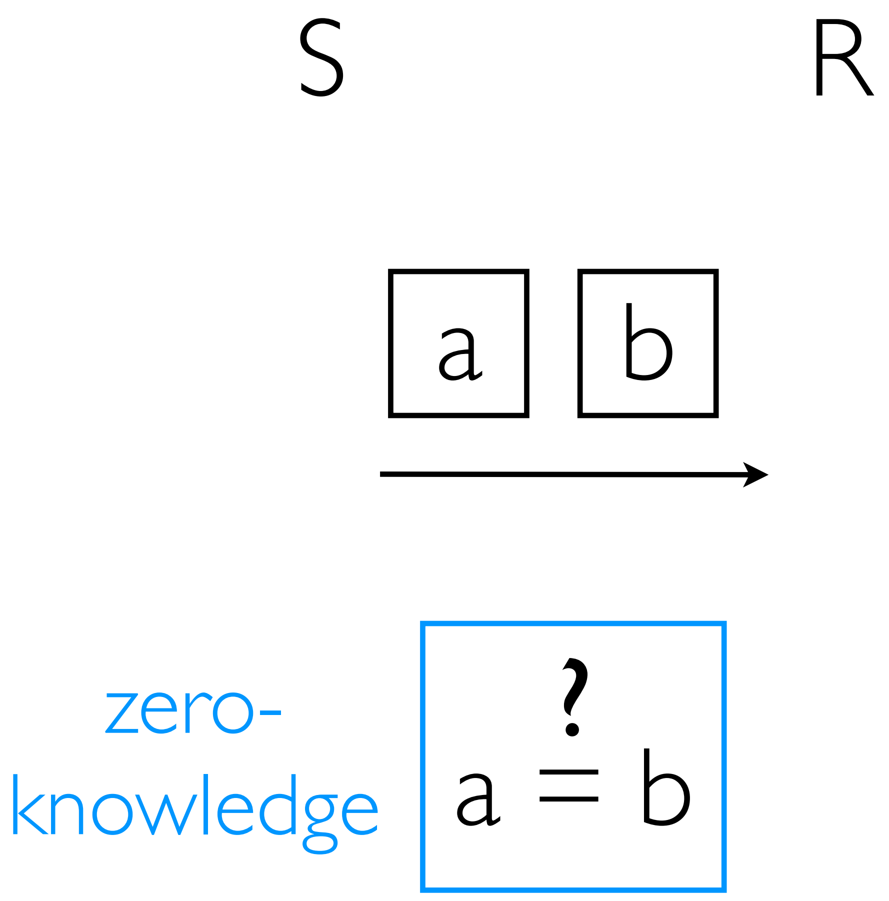
Black-box Proof of Equality of Commitments



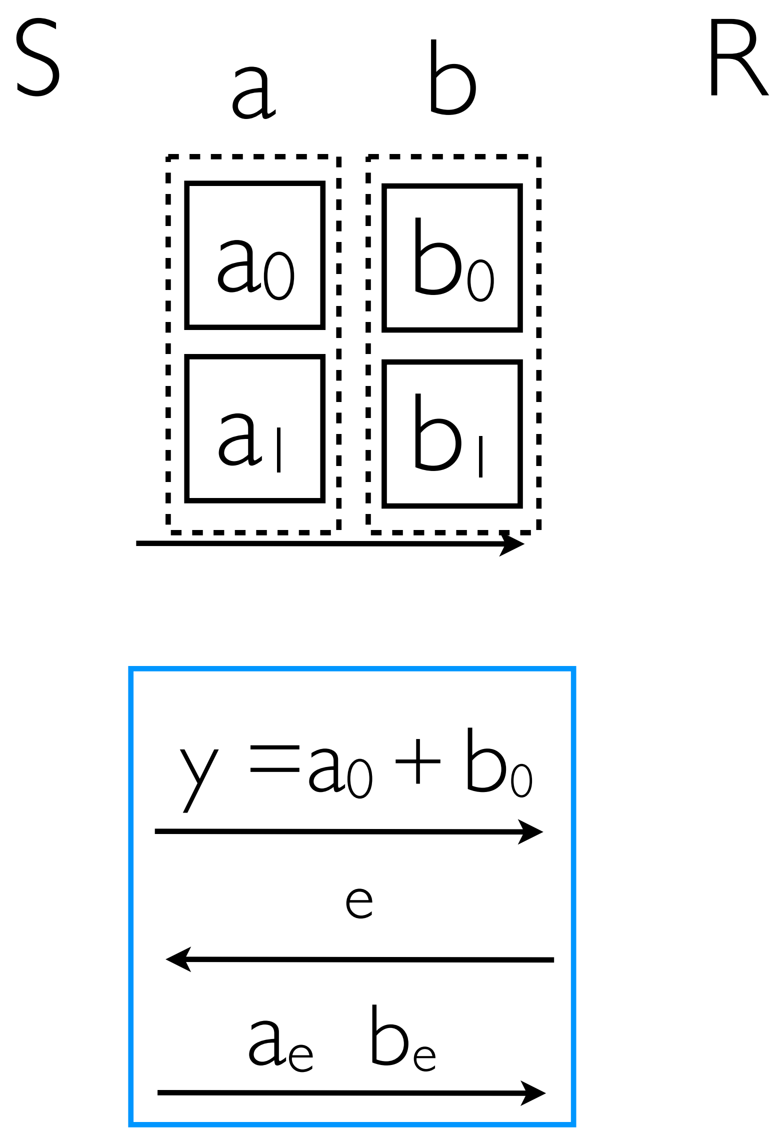
Kilian 92



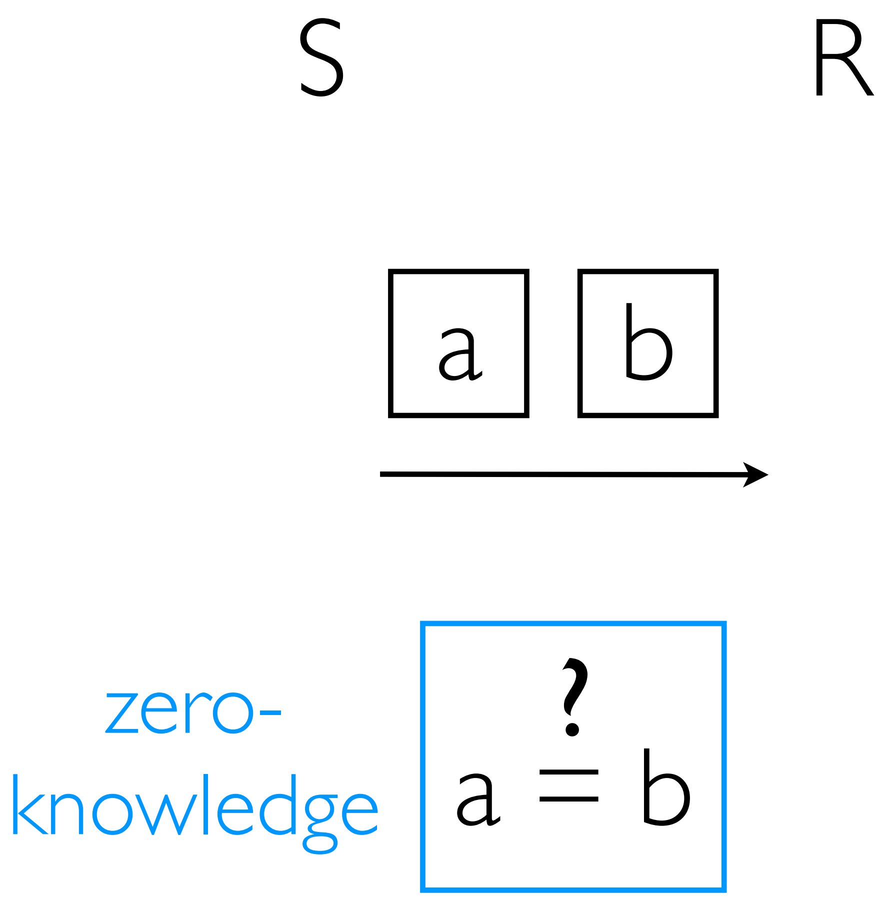
Black-box Proof of Equality of Commitments



Kilian 92



Black-box Proof of Equality of Commitments



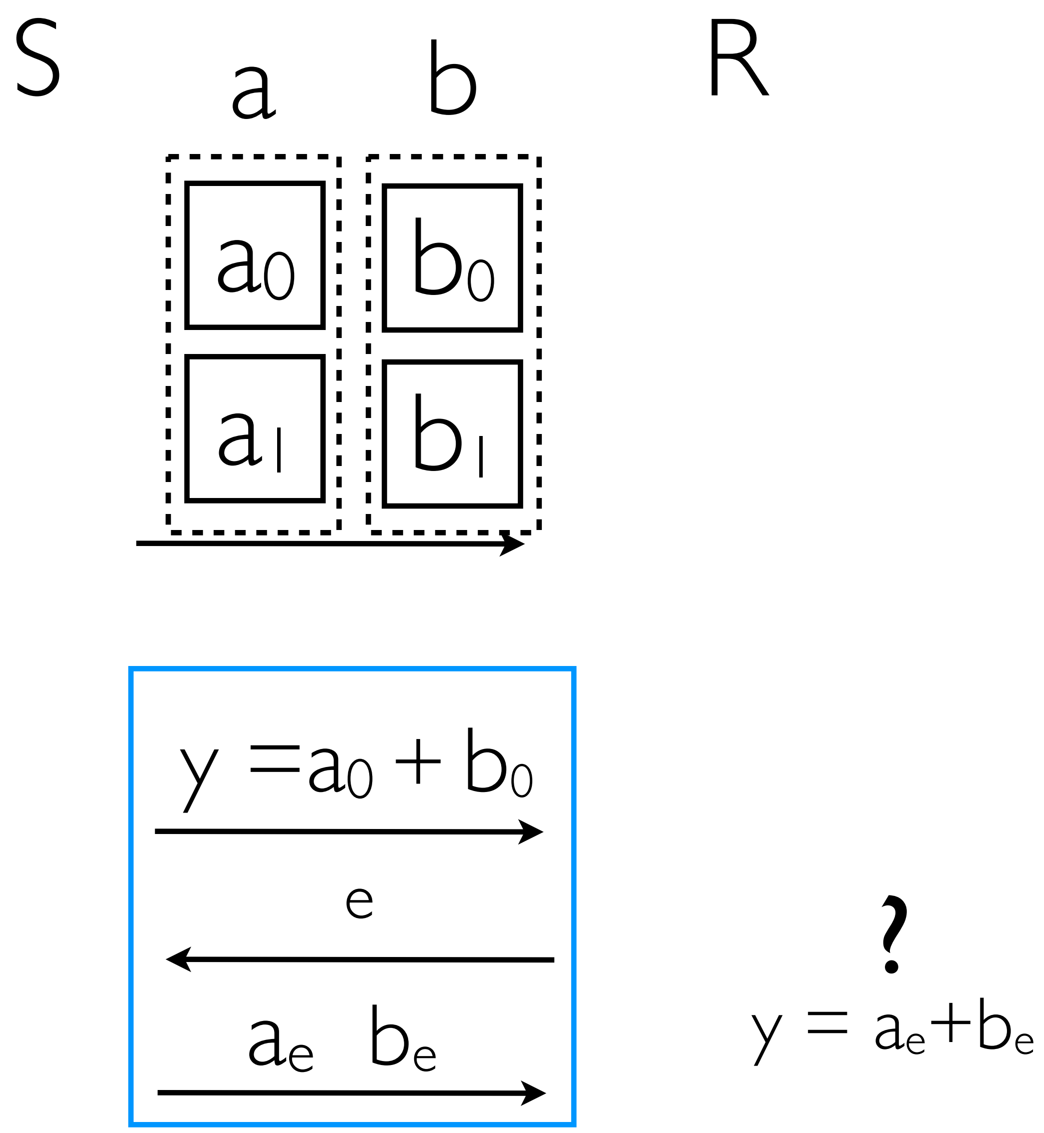
S R

$\boxed{a}$ $\boxed{b}$

zero-knowledge

$a \overset{?}{=} b$

Kilian 92



S a b R

$\boxed{a_0}$ $\boxed{b_0}$

$\boxed{a_1}$ $\boxed{b_1}$

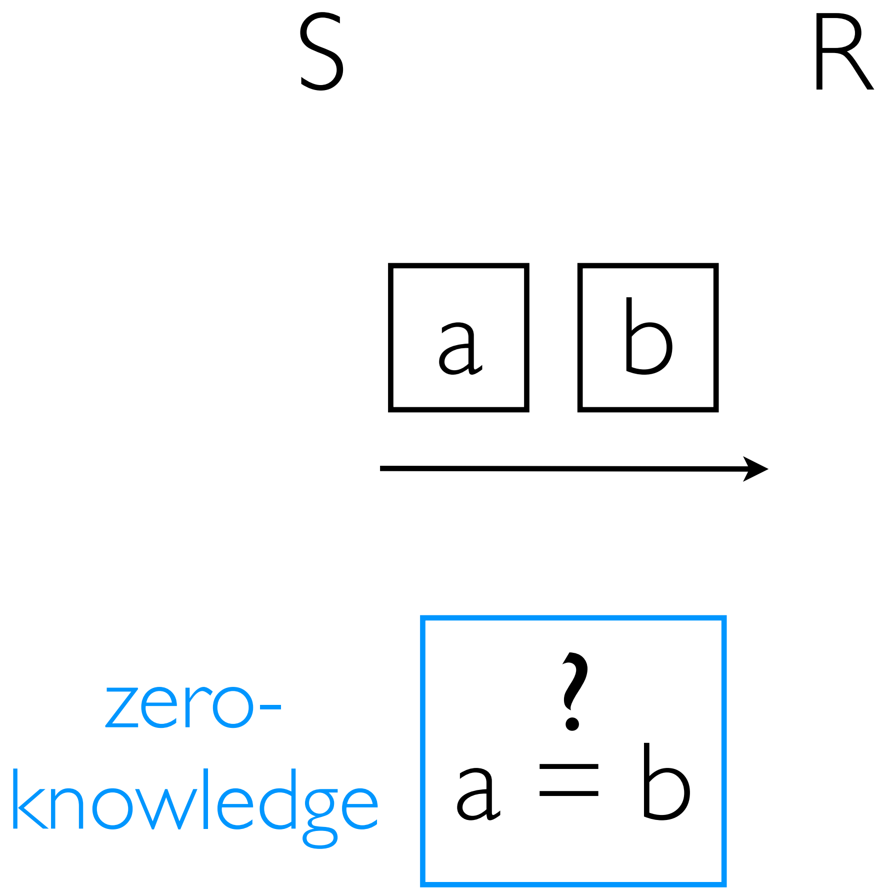
$y = a_0 + b_0$

e

$a_e \quad b_e$

$y \overset{?}{=} a_e + b_e$

Black-box Proof of Equality of Commitments



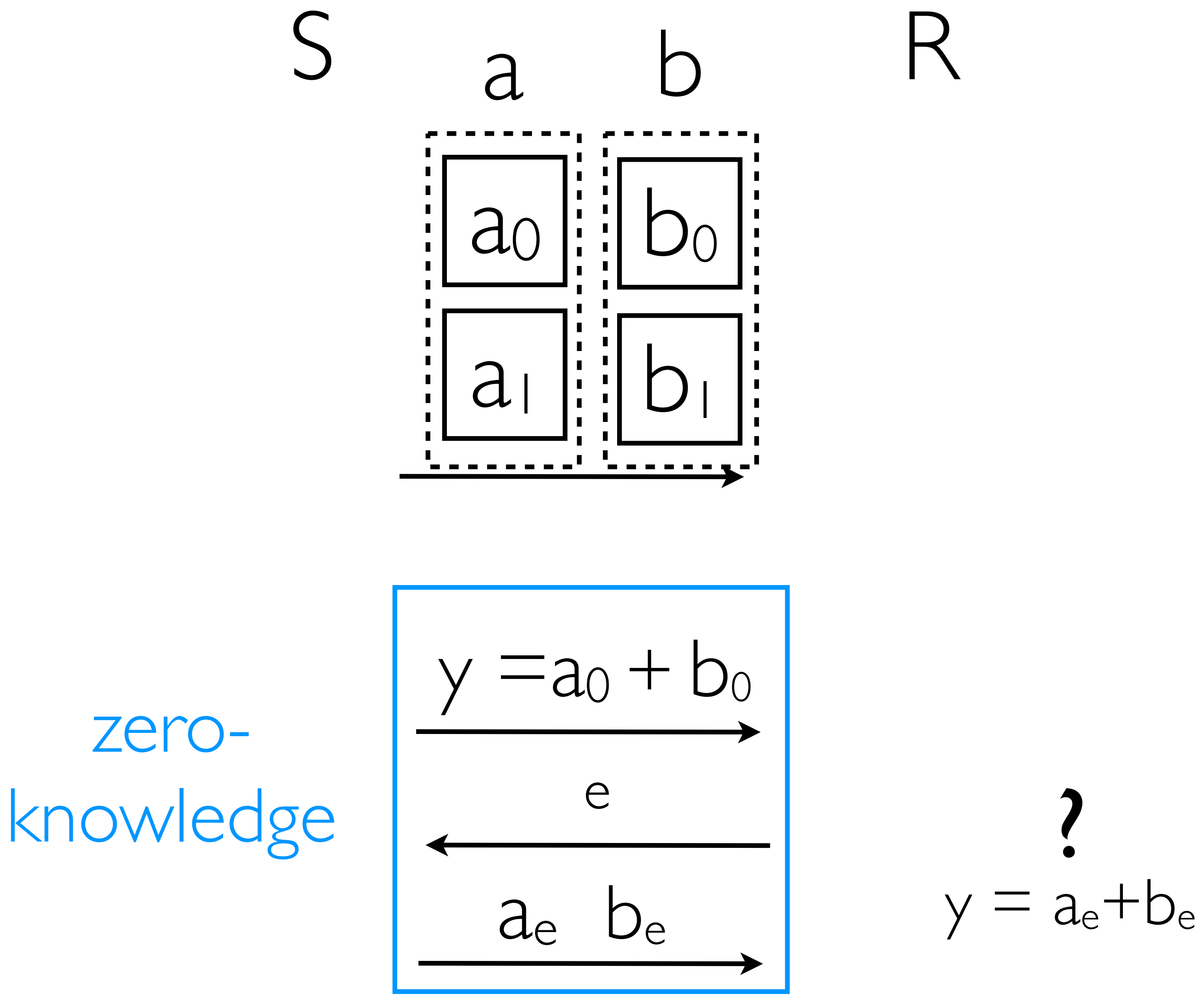
S R

$\boxed{a}$ $\boxed{b}$

zero-knowledge

$a \overset{?}{=} b$

Kilian 92



S R

a b

$\boxed{a_0}$ $\boxed{b_0}$

$\boxed{a_1}$ $\boxed{b_1}$

zero-knowledge

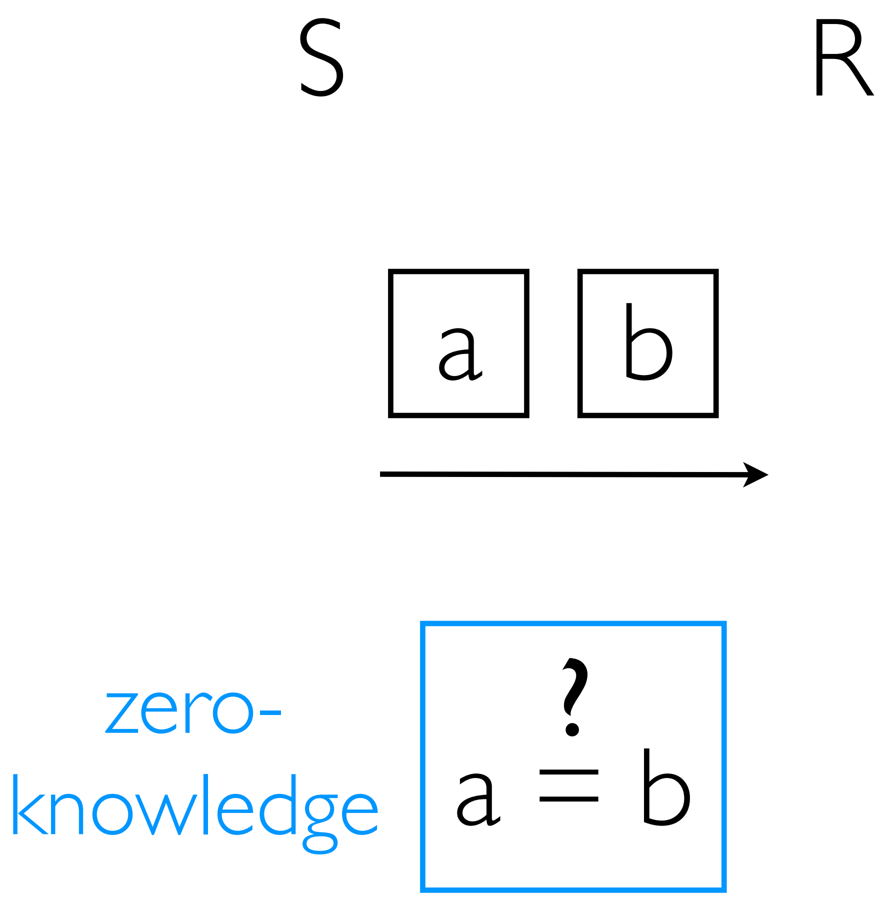
$y = a_0 + b_0$

e

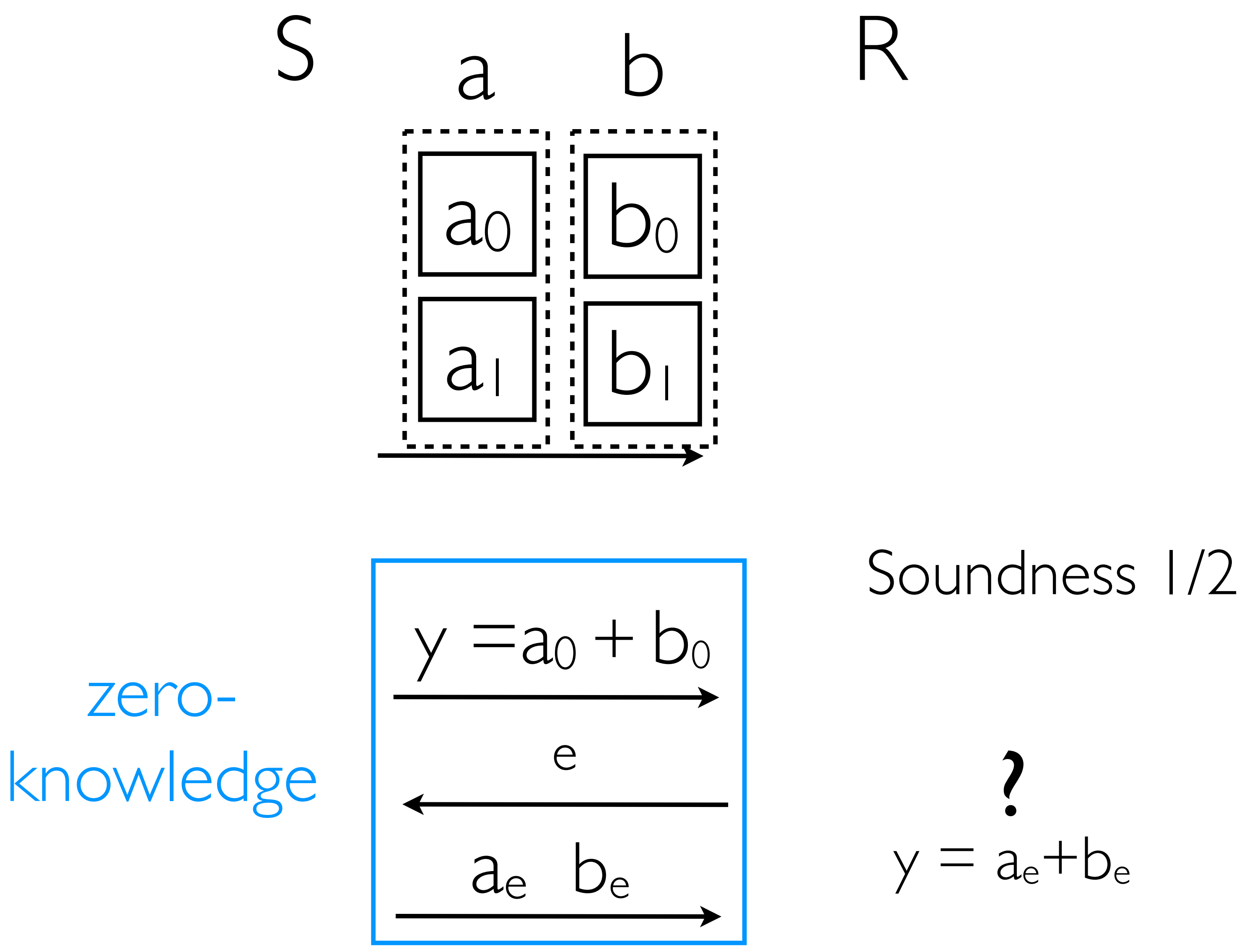
$a_e \quad b_e$

$y \overset{?}{=} a_e + b_e$

Black-box Proof of Equality of Commitments



Kilian 92



Straight-line ZK BB proof of equality

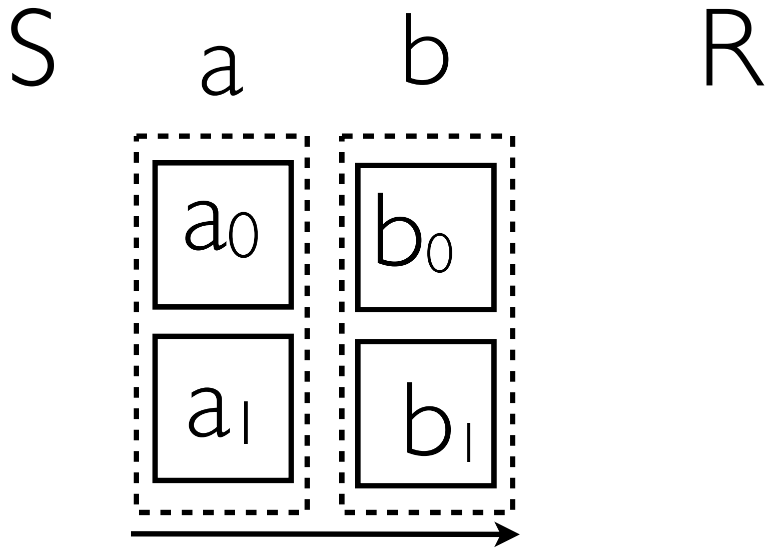
Straight-line ZK BB proof of equality

Assume boxes are

extractable

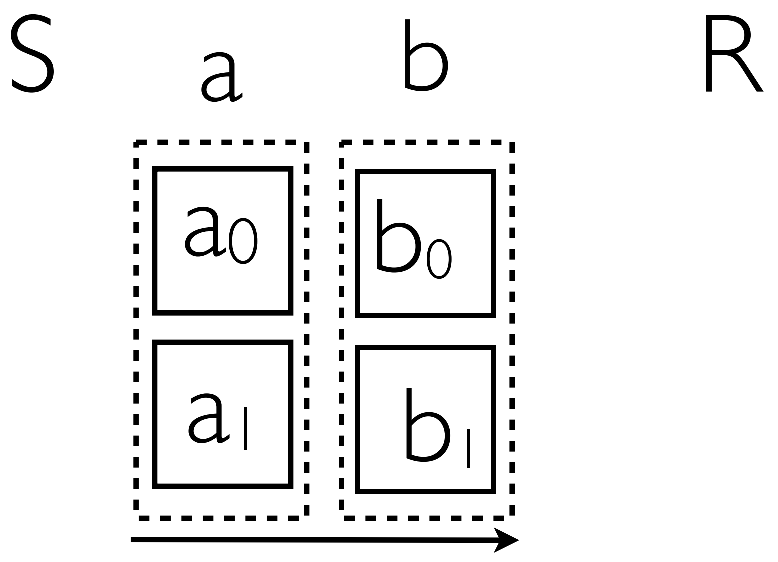
Straight-line ZK BB proof of equality

Assume boxes are
extractable



Straight-line ZK BB proof of equality

Assume boxes are extractable



zero-knowledge

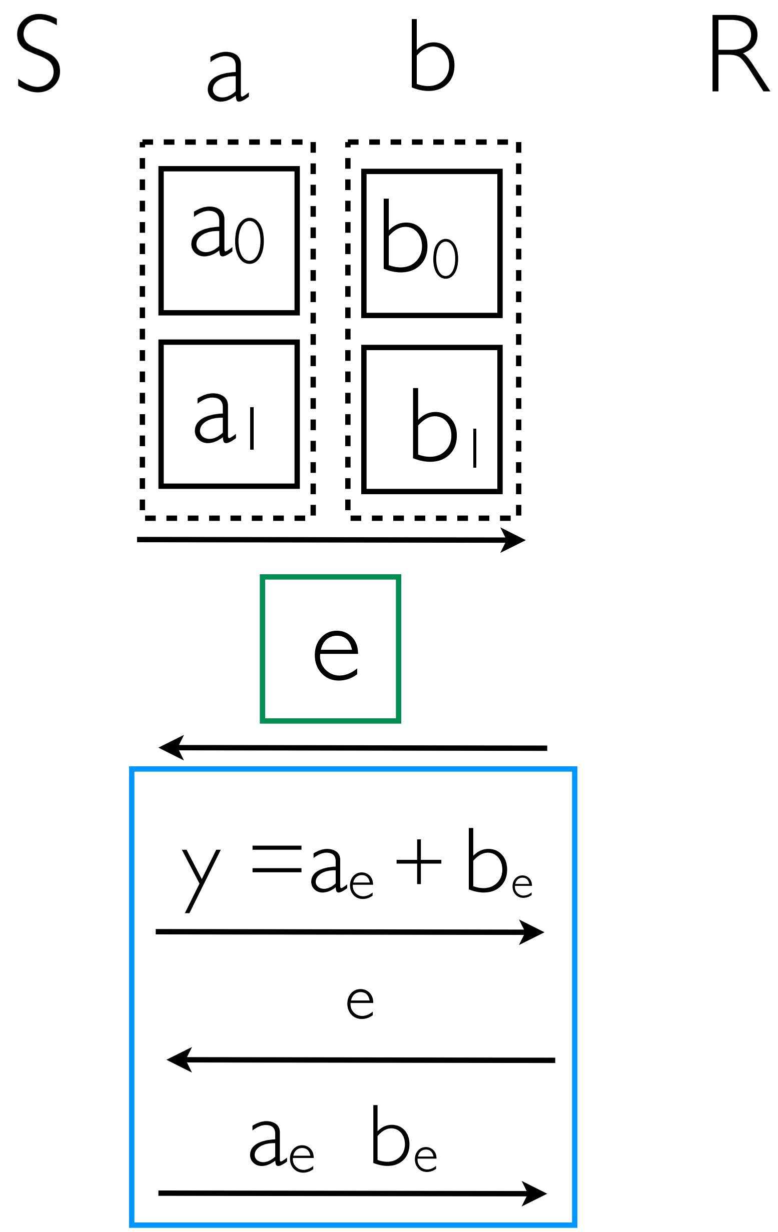
$$\xrightarrow{y = a_e + b_e}$$

$$\xleftarrow{e}$$

$$\xrightarrow{a_e \quad b_e}$$

Straight-line ZK BB proof of equality

Assume boxes are
extractable



S a b R

a_0 b_0

a_1 b_1

e

zero-knowledge

$y = a_e + b_e$

e

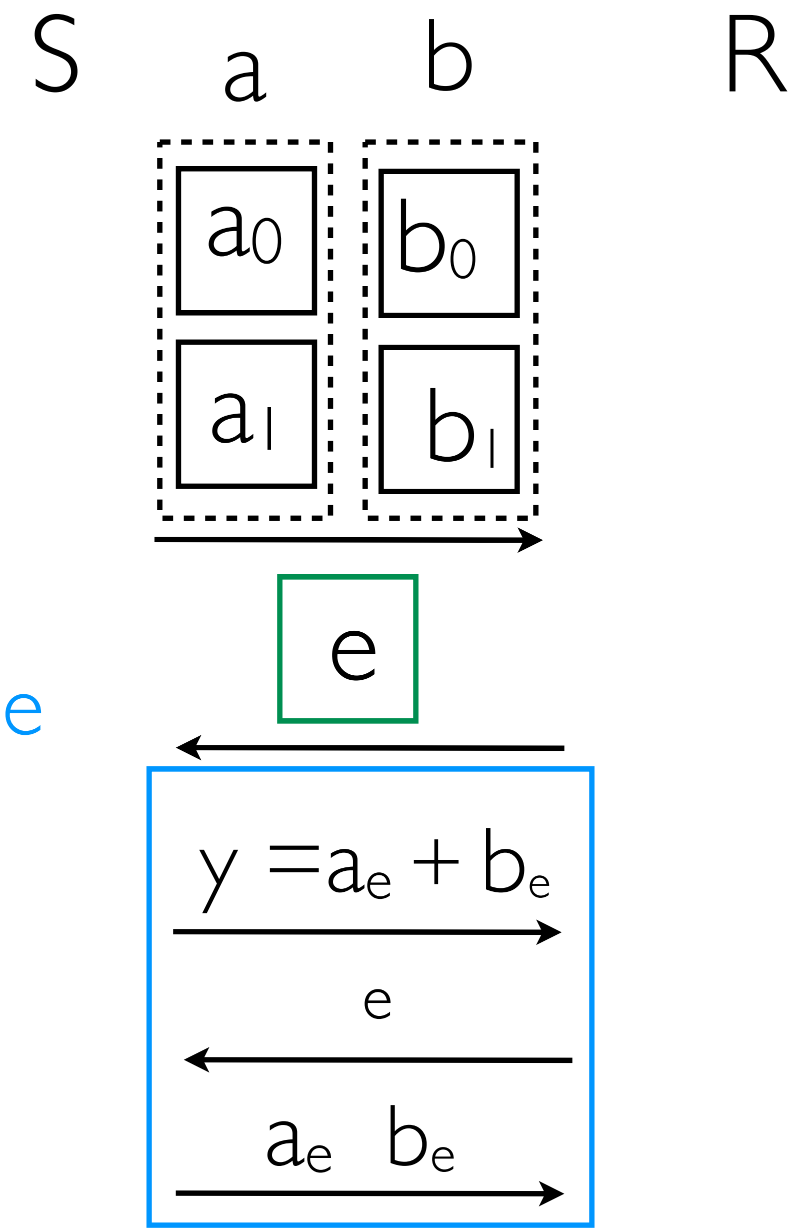
a_e b_e

Straight-line ZK BB proof of equality

Assume boxes are extractable

Straight-line

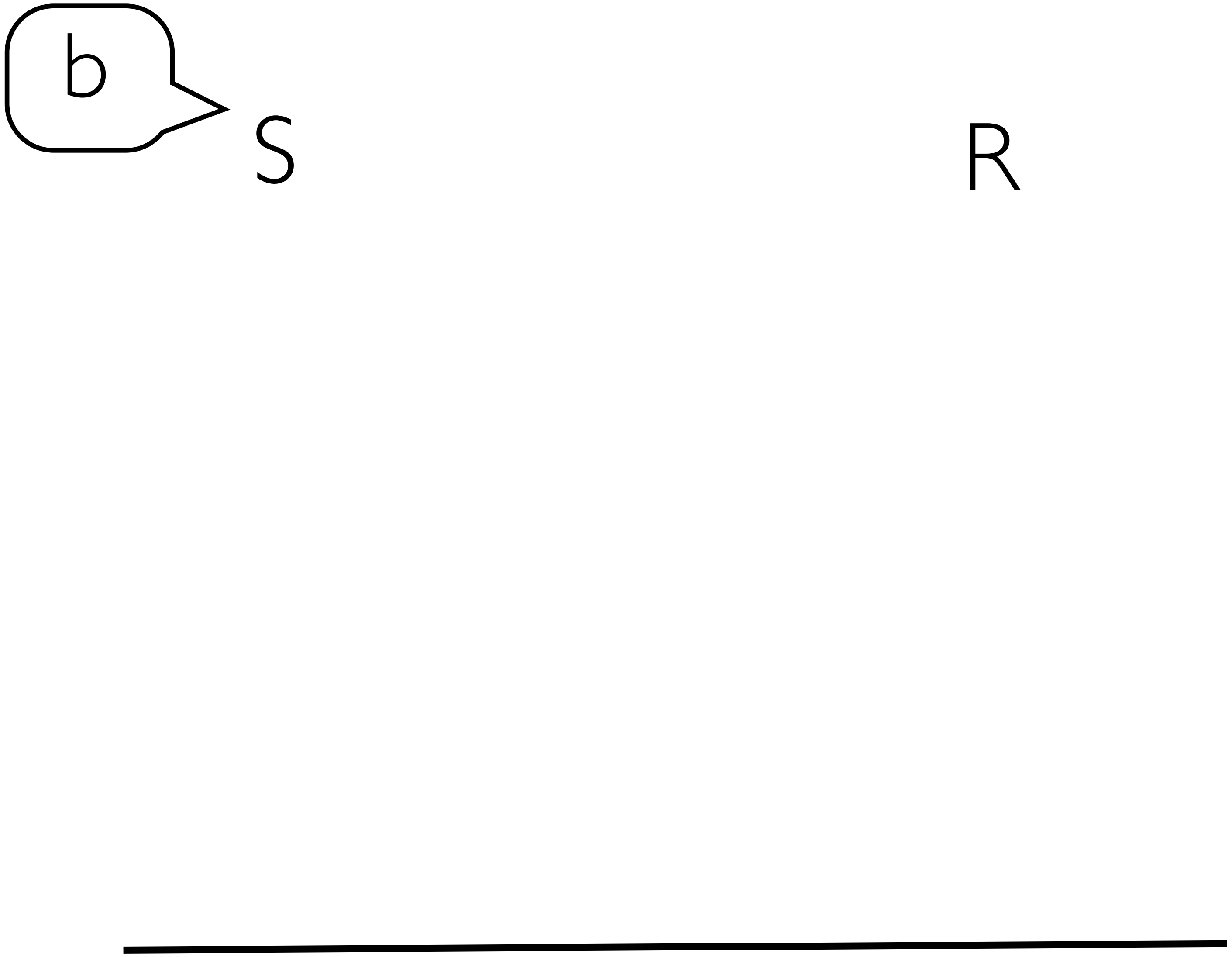
zero-knowledge



Compiler

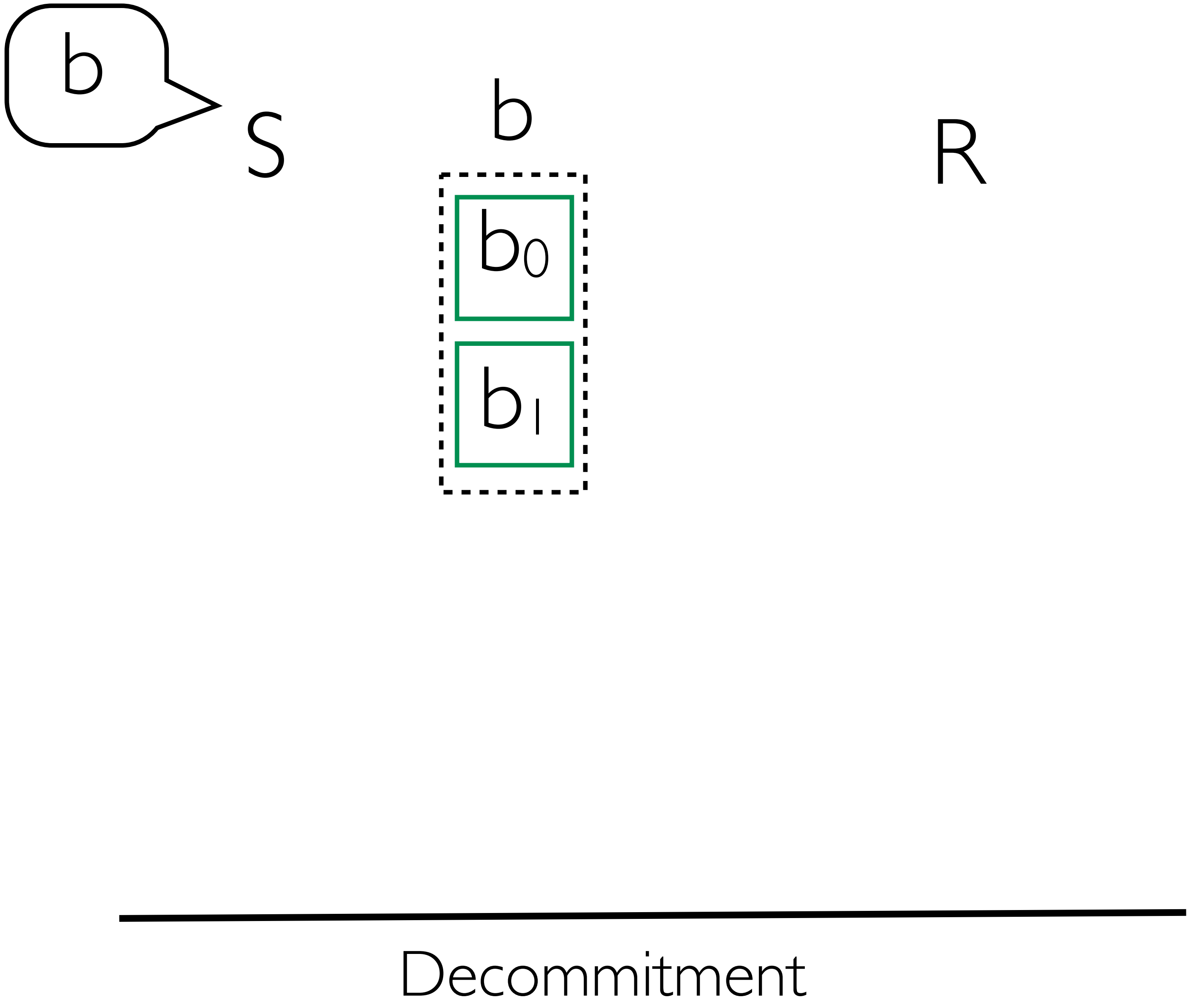
Extractable Commitment => Equivocal + Extractable

Compiler: Equivocal commitments from Extractable Commitments

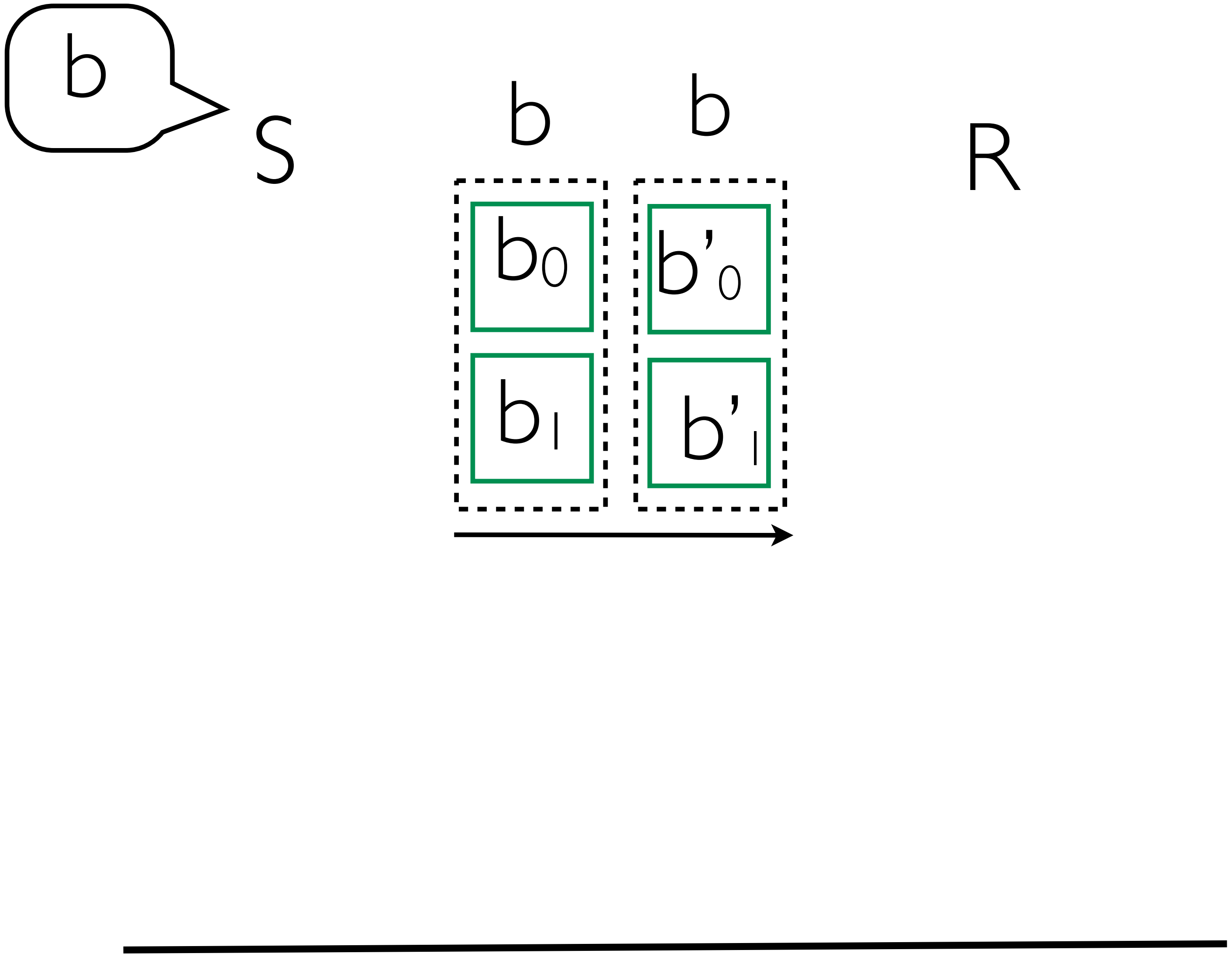


Decommitment

Compiler: Equivocal commitments from Extractable Commitments

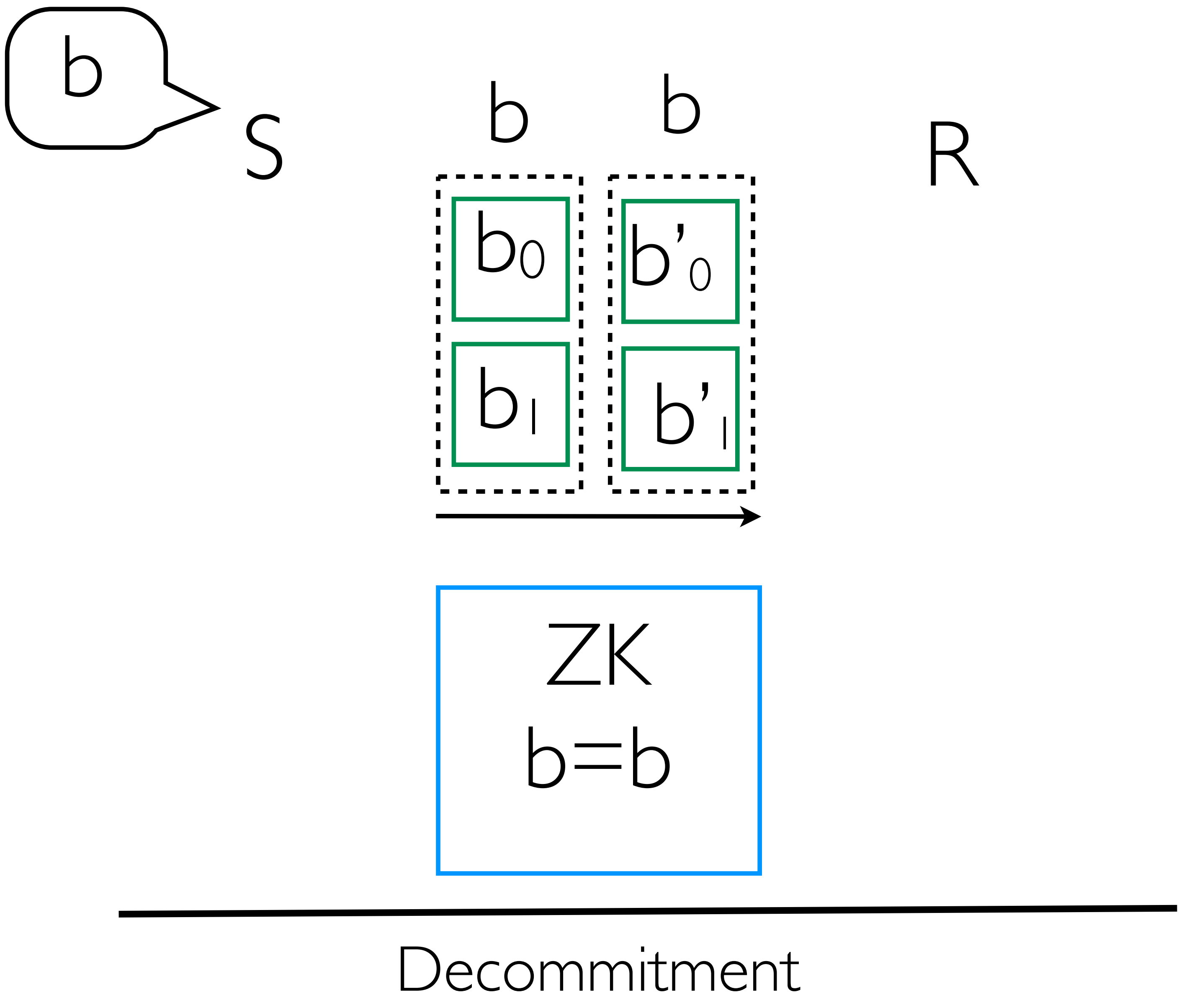


Compiler: Equivocal commitments from Extractable Commitments

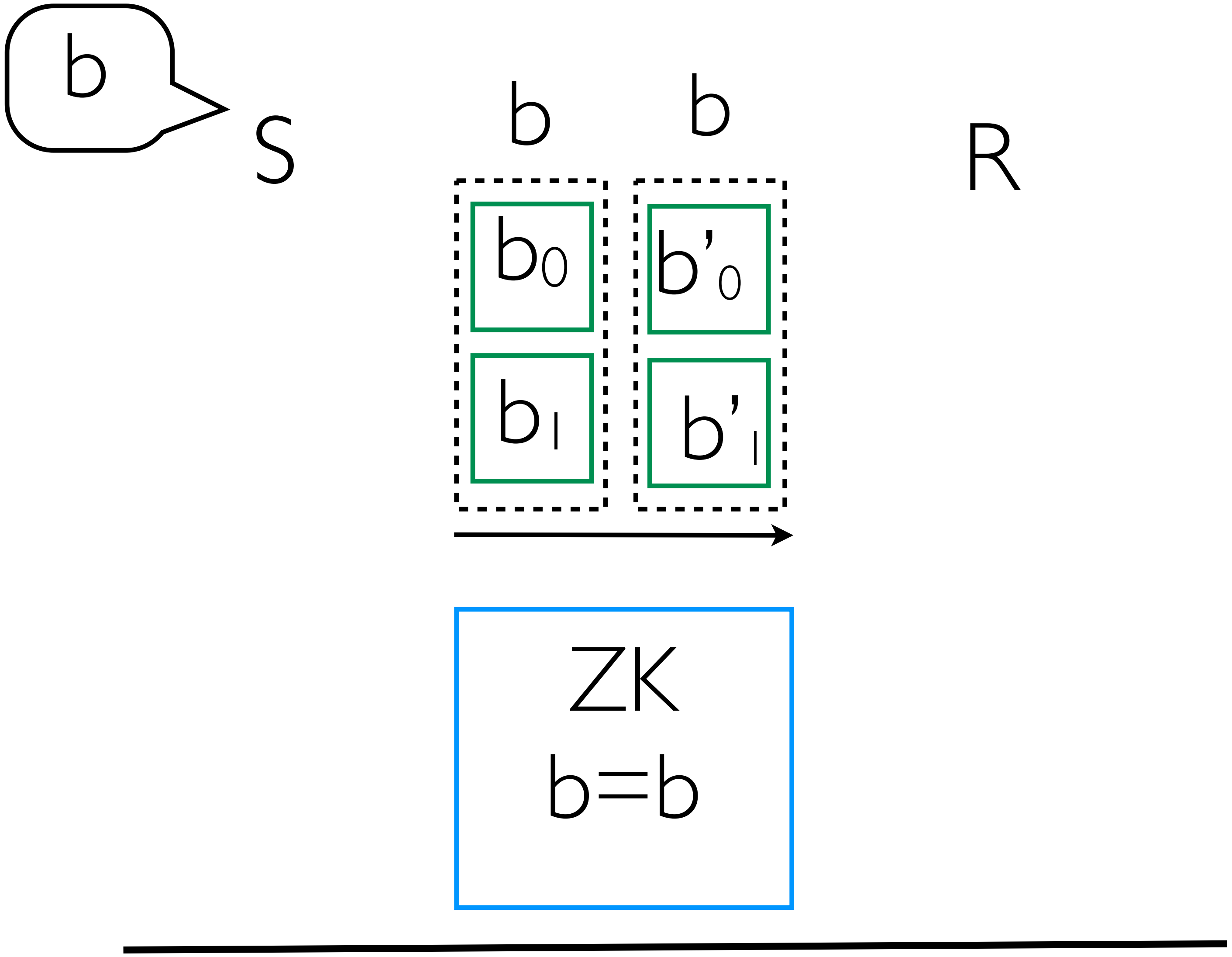


Decommitment

Compiler: Equivocal commitments from Extractable Commitments



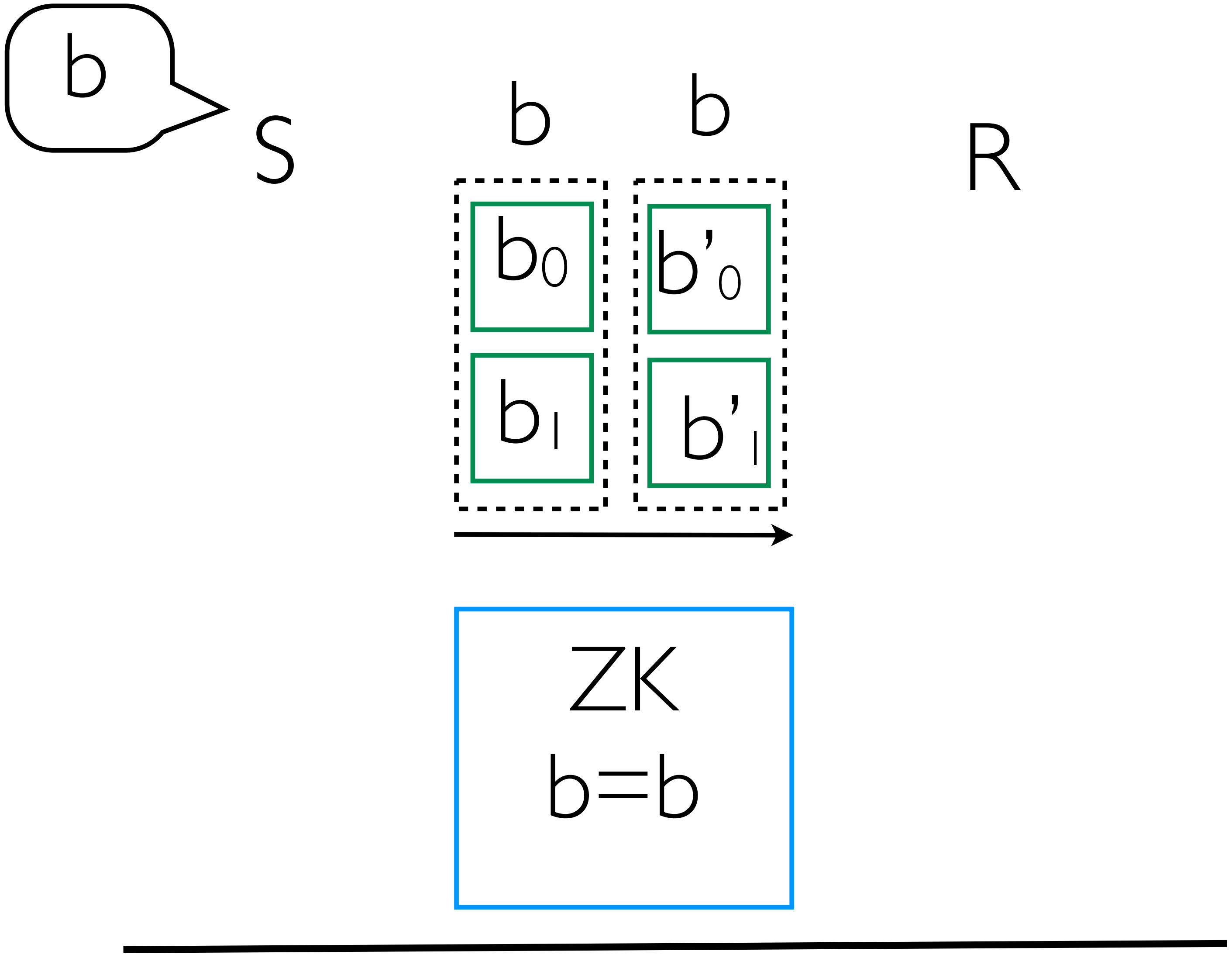
Compiler: Equivocal commitments from Extractable Commitments



Decommitment

open **either**
first or second com

Compiler: Equivocal commitments from Extractable Commitments



idea used in Hof11

Decommitment

open **either**
first or second com

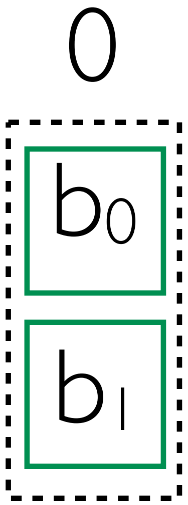
Equivocality

Straight-line equivocality

Decommitment

Equivocality

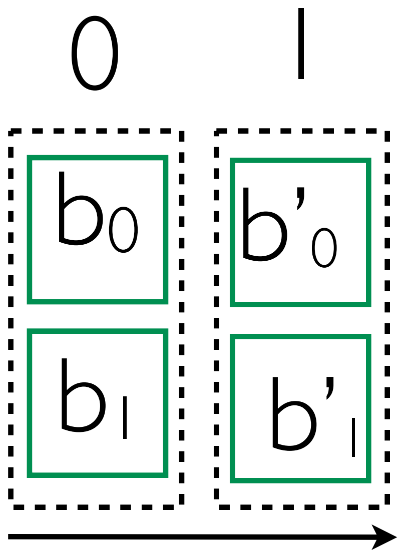
Straight-line equivocality



Decommitment

Equivocality

Straight-line equivocality



0 1

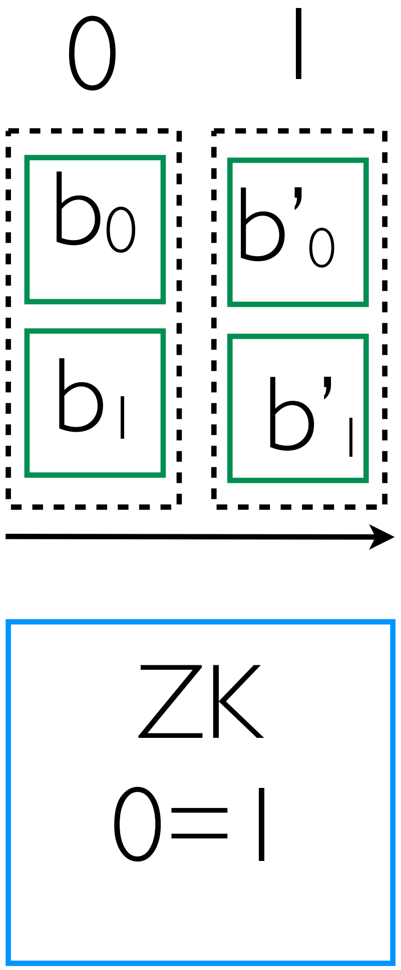
b_0 b'_0

b_1 b'_1

Decommitment

Equivocality

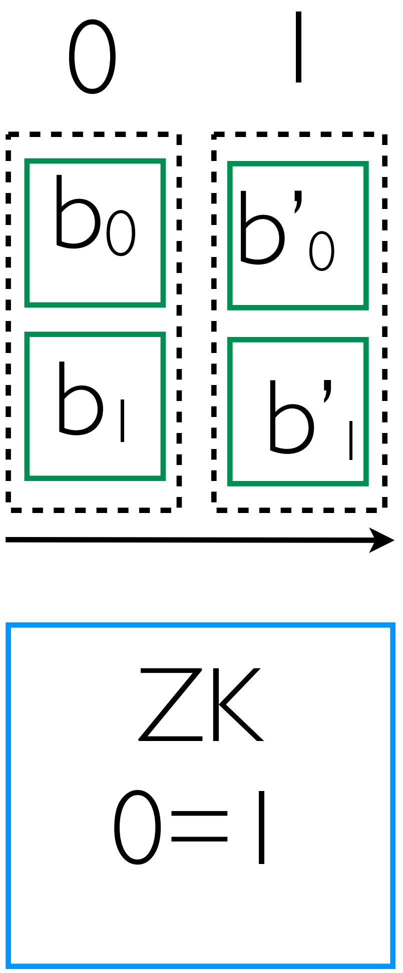
Straight-line equivocality



Decommitment

Equivocality

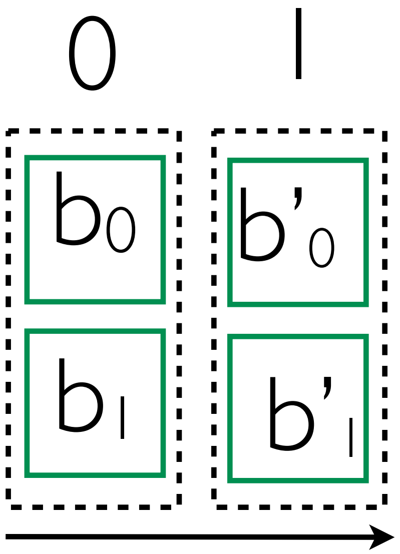
Straight-line equivocality



Decommitment

Equivocality

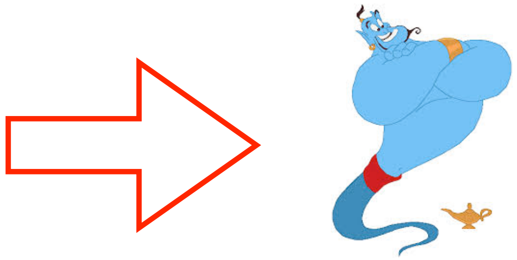
Straight-line equivocality



ZK

0=1

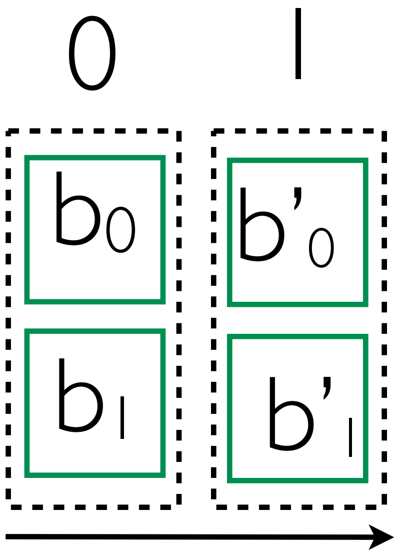
b



Decommitment

Equivocality

Straight-line
equivocality



0 1

b_0 b'_0

b_1 b'_1

ZK
0=1

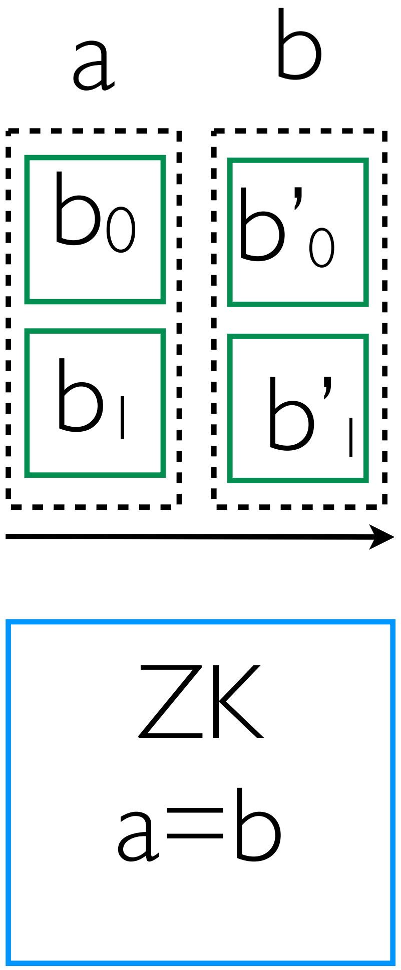
---

b

Decommitment

open **b**

Extractability



a b

b_0 b_1

b'_0 b'_1

ZK

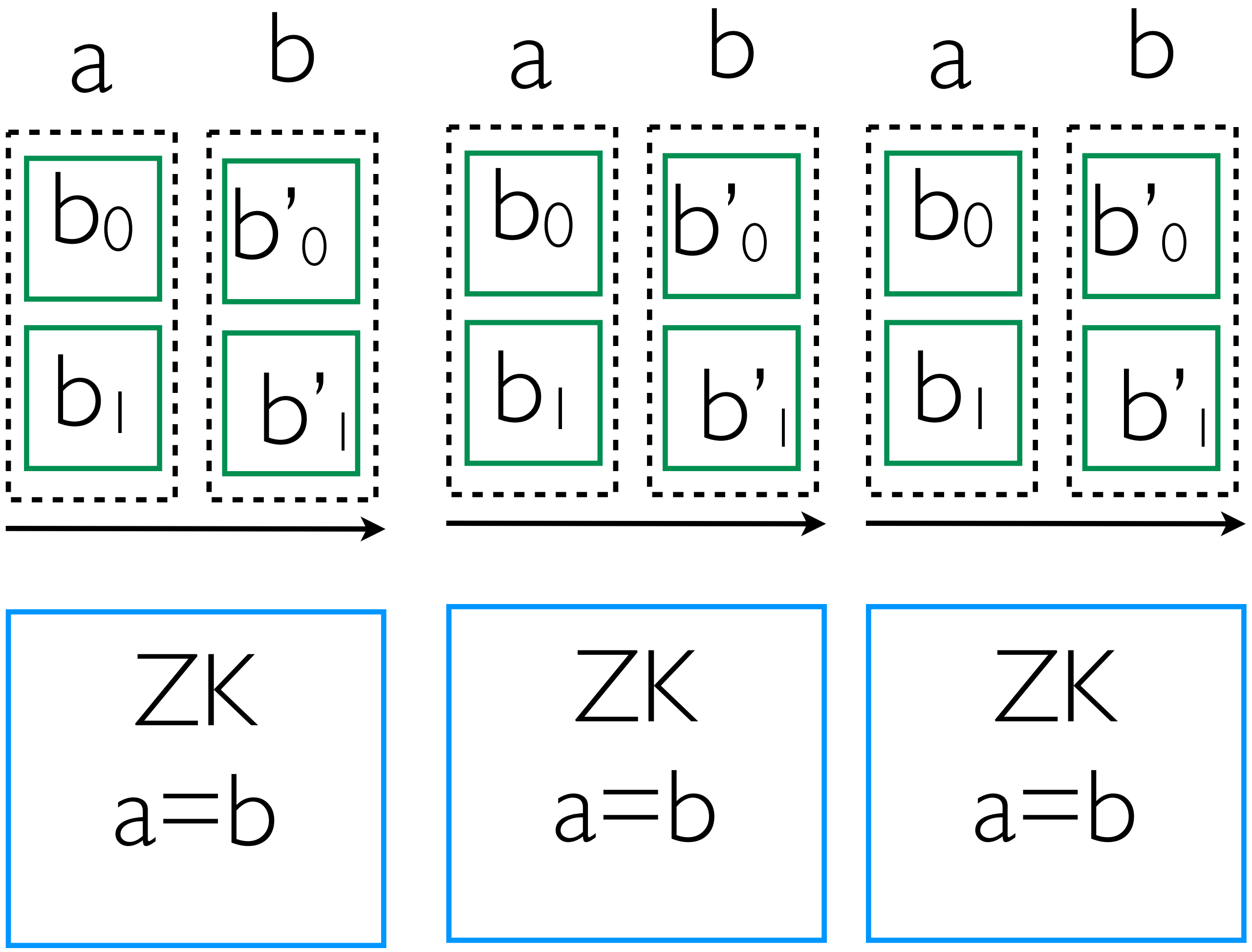
a=b

Straight-line extractability

Decommitment

open **either**
a or b

Extractability



a b a b a b

b_0 b'_0 b_0 b'_0 b_0 b'_0

b_1 b'_1 b_1 b'_1 b_1 b'_1

ZK a=b

ZK a=b

ZK a=b

Extractability

Decommitment

open **either** a or b

open **either** a or b

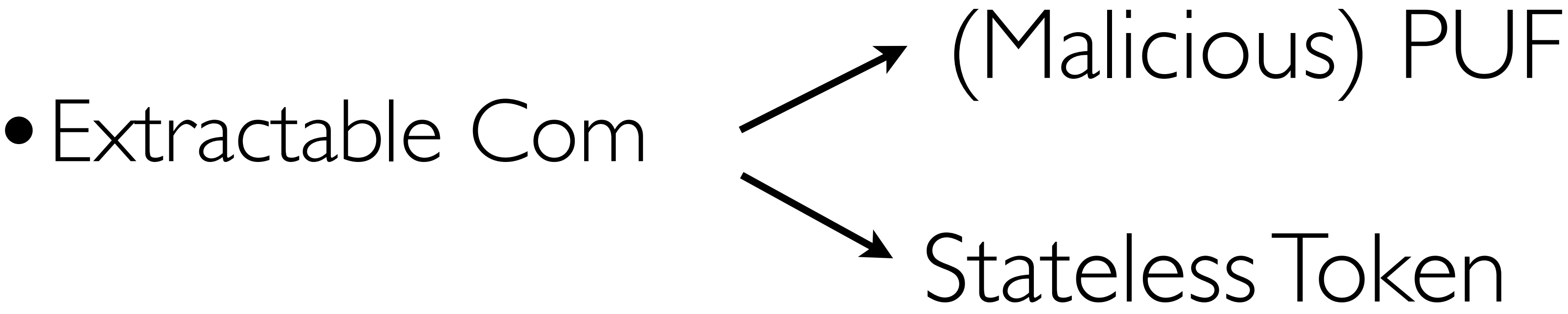
open **either** a or b

check that all open to the same bit

Our Technique

- Black-box compiler

Extractable Com => Equivocal + Extractable Com



- Extractable Com

(Malicious) PUF

Stateless Token

Extractable Commitment from (malicious) PUFs

Extractable Commitment from (malicious) PUFs

Extractable Commitment from (malicious) PUFs

for free: stand-alone
unconditional commitment
from [OSVW13]
PUF-Com

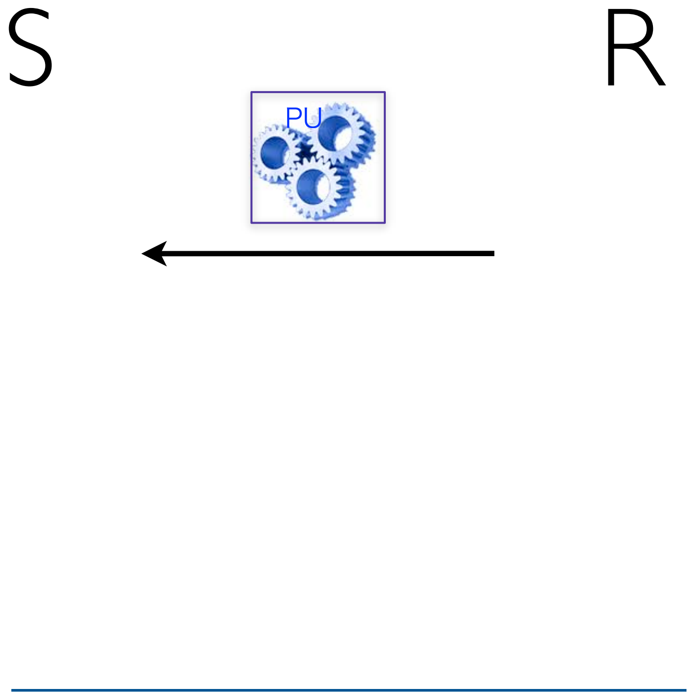
Extractable Commitment from (malicious) PUFs

S

R

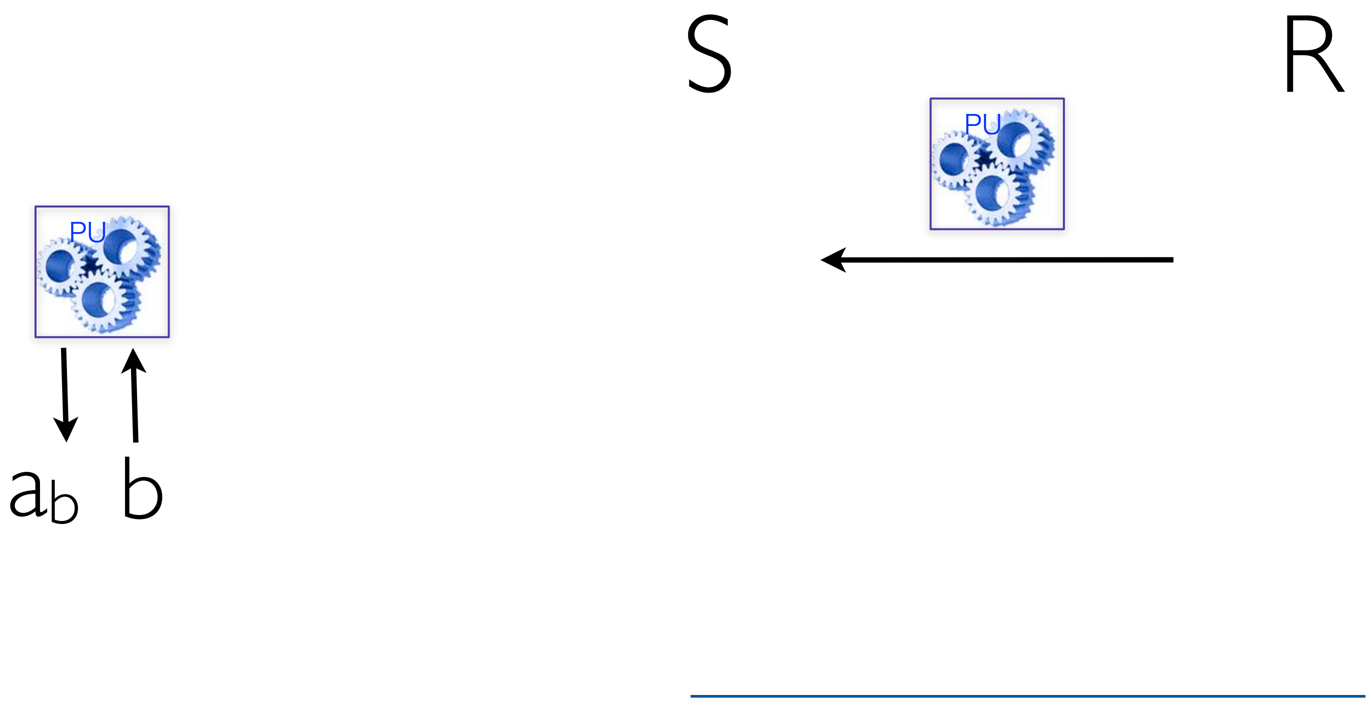
for free: stand-alone
unconditional commitment
from [OSVW13]
PUF-Com

Extractable Commitment from (malicious) PUFs



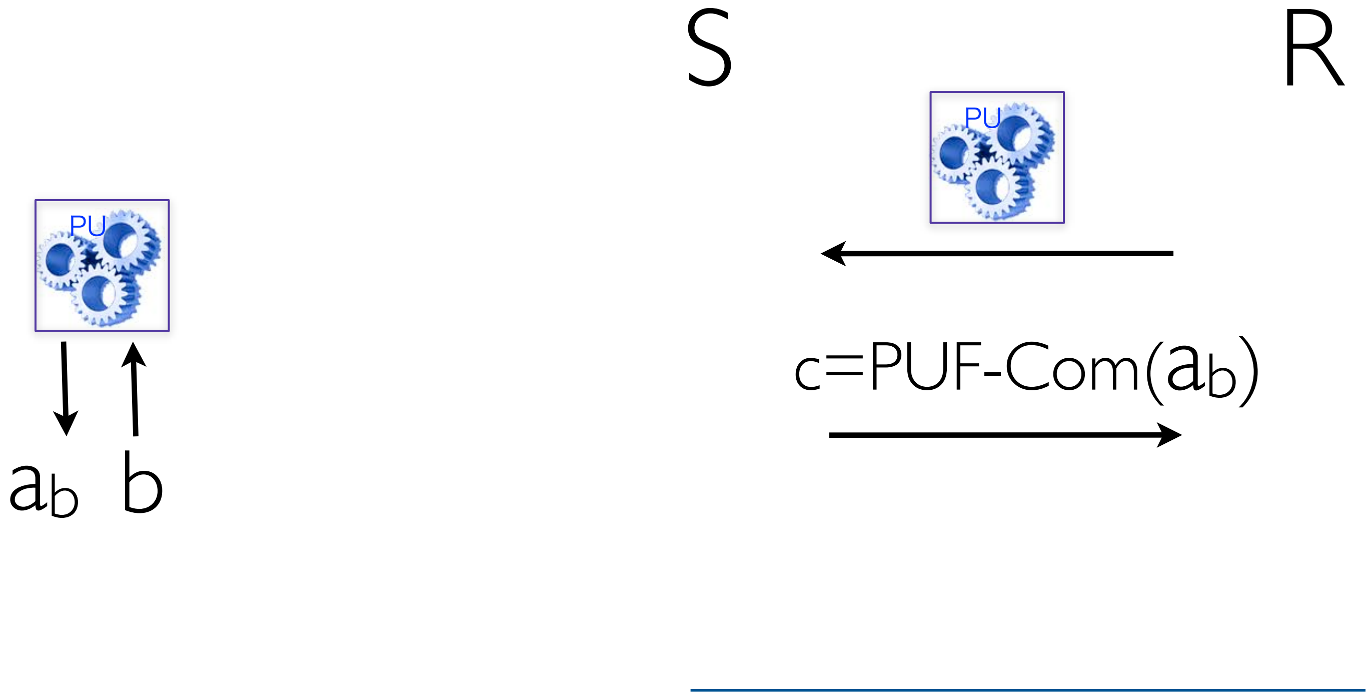
for free: stand-alone
unconditional commitment
from [OSVW13]
PUF-Com

Extractable Commitment from (malicious) PUFs



for free: stand-alone unconditional commitment from [OSVW13] PUF-Com

Extractable Commitment from (malicious) PUFs



S

R

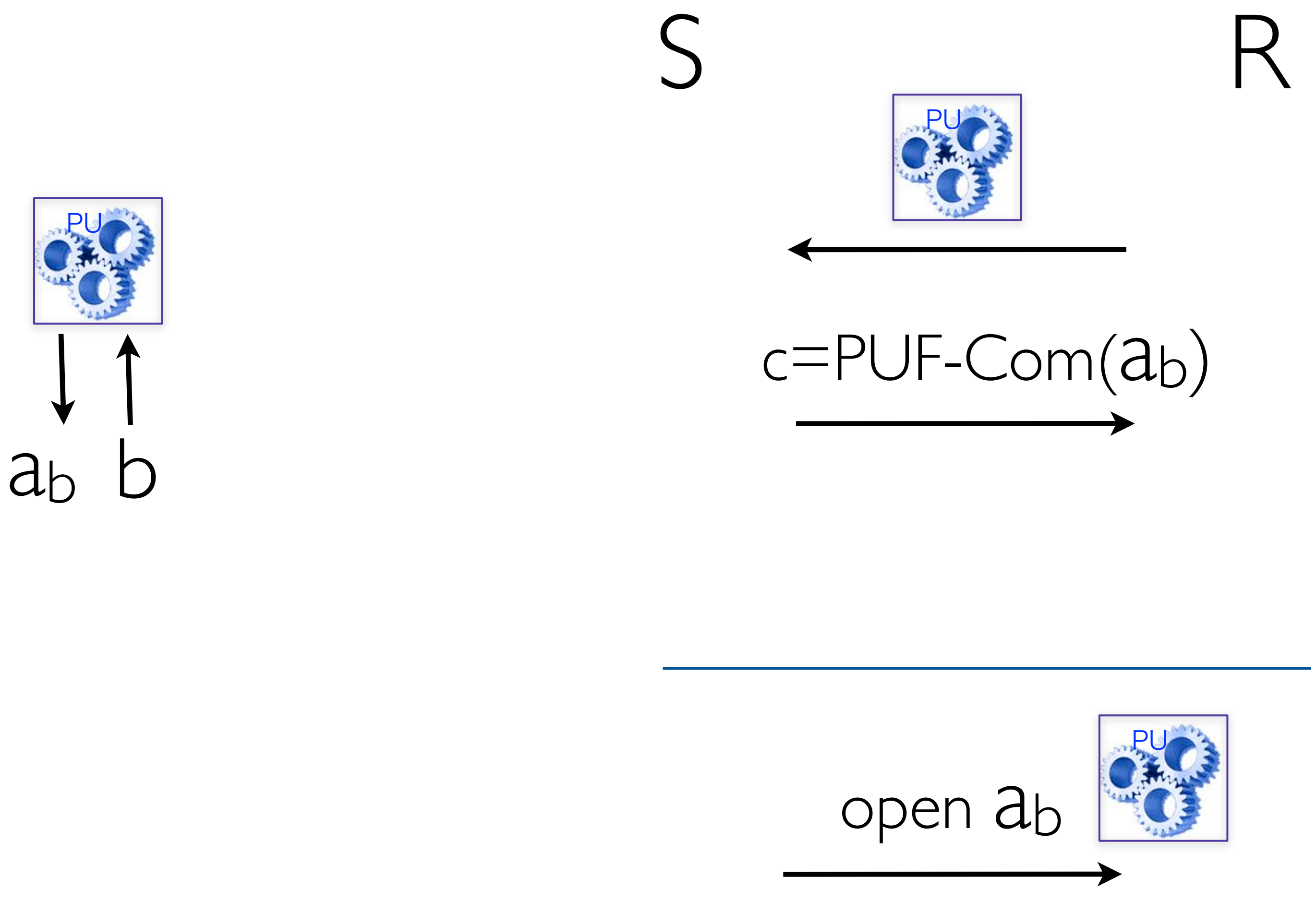
a_b b

c=PUF-Com(a_b)

for free: stand-alone
unconditional commitment
from [OSVW13]
PUF-Com

Extractable Commitment from (malicious) PUFs

for free: stand-alone
unconditional commitment
from [OSVW13]
PUF-Com



S

R

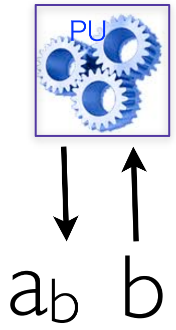
c=PUF-Com(a_b)

a_b b

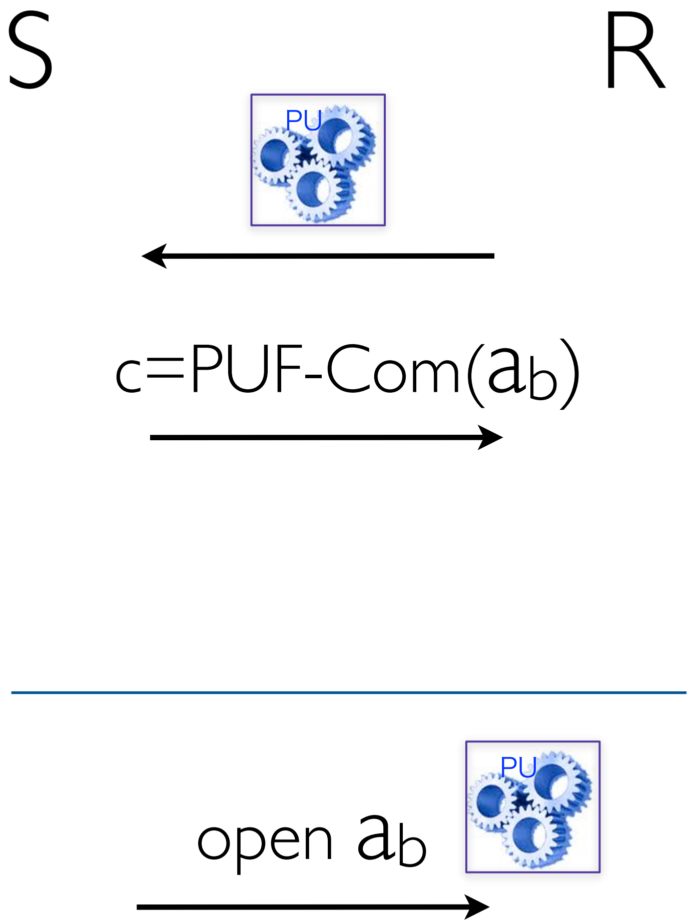
open a_b

Extractable Commitment from (malicious) PUFs

Problem 1: Adv can query with 0/1



a_b b



S R

c=PUF-Com(a_b)

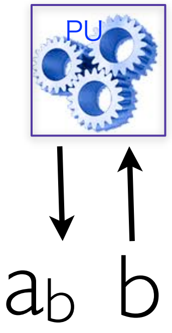
open a_b

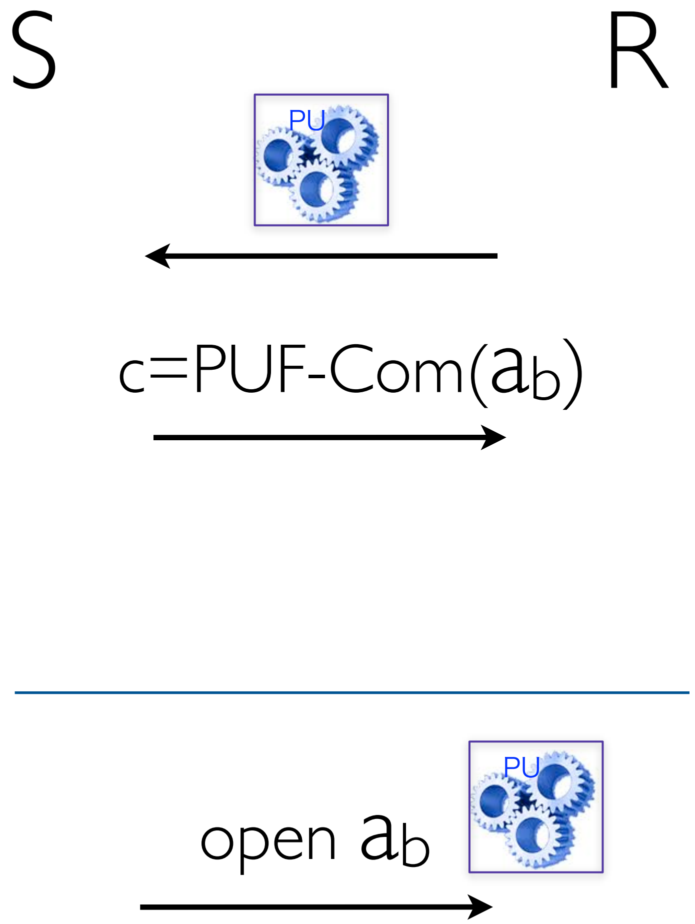
for free: stand-alone unconditional commitment from [OSVW13] PUF-Com

Extractable Commitment from (malicious) PUFs

Problem 1: Adv can query with 0/1

idea [MQU07,CGS08]





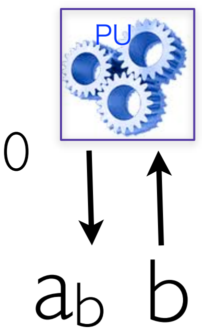
for free: stand-alone unconditional commitment from [OSVW13] PUF-Com

Extractable Commitment from (malicious) PUFs

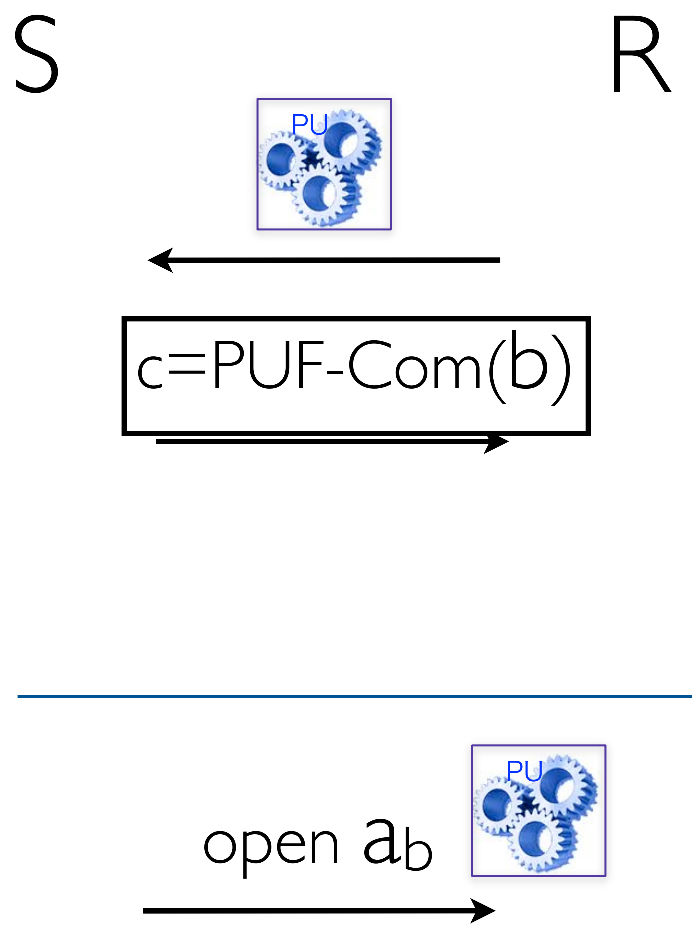
Problem 1: Adv can query with 0/1

for free: stand-alone unconditional commitment from [OSVW13] PUF-Com

idea [MQU07,CGS08]



a_b b



S

R

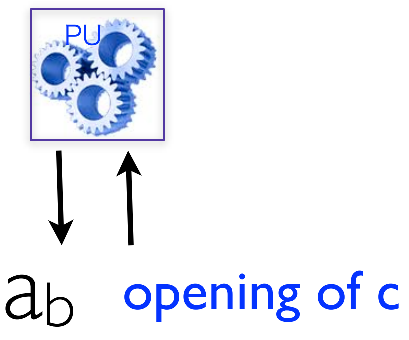
c=PUF-Com(b)

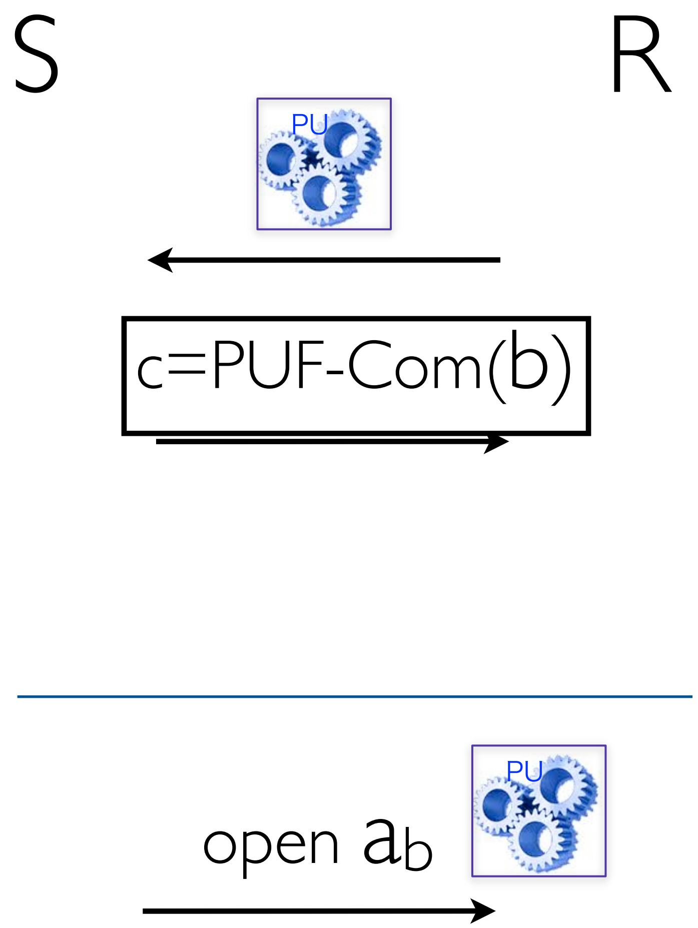
open a_b

Extractable Commitment from (malicious) PUFs

Problem 1: Adv can query with 0/1

idea [MQU07,CGS08]



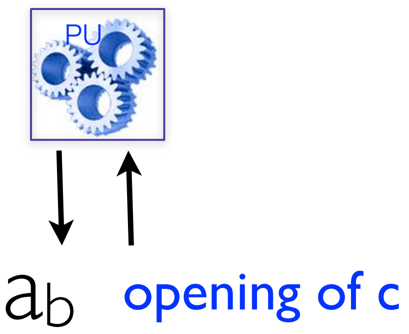


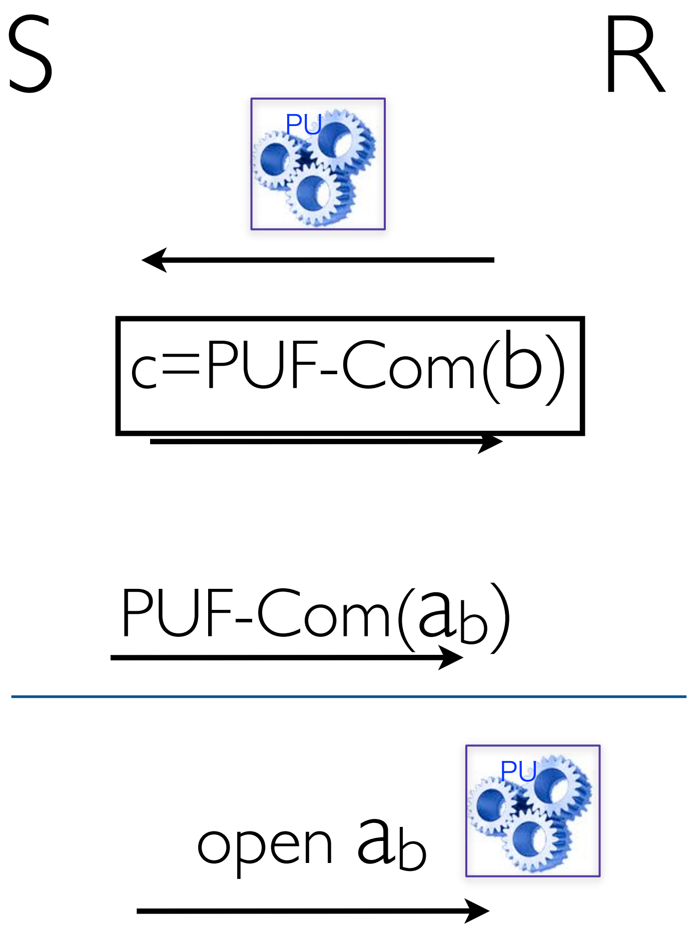
for free: stand-alone unconditional commitment from [OSVW13] PUF-Com

Extractable Commitment from (malicious) PUFs

Problem 1: Adv can query with 0/1

idea [MQU07,CGS08]



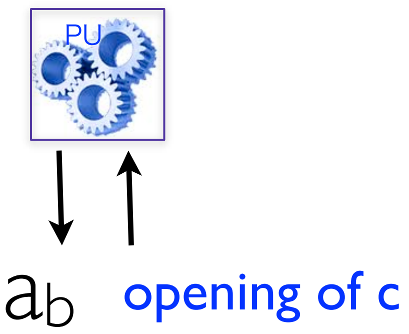


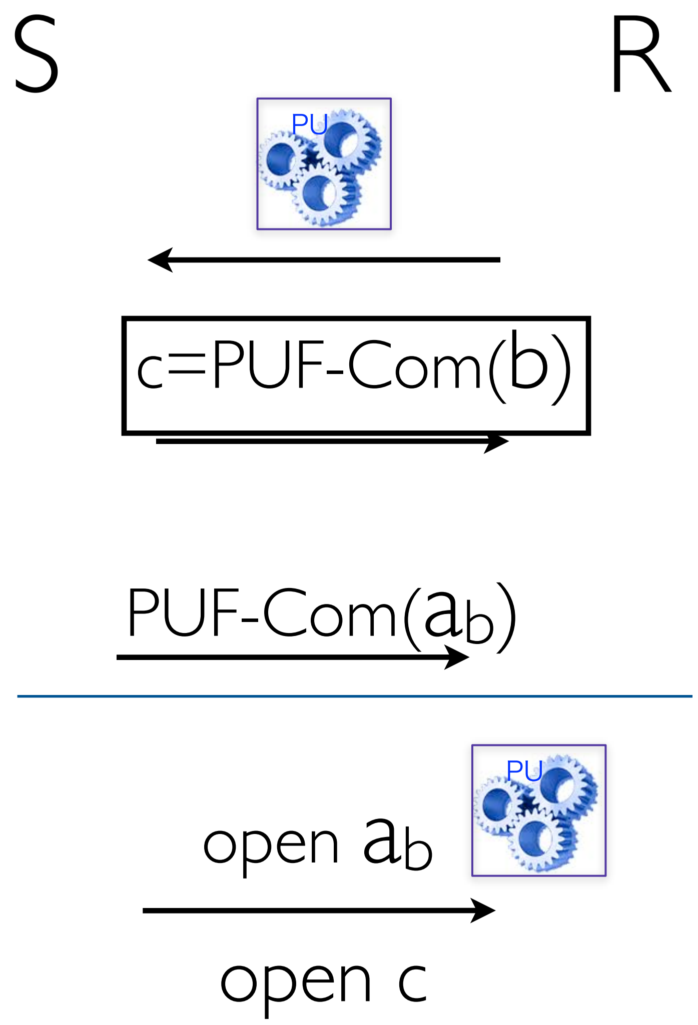
for free: stand-alone unconditional commitment from [OSVW13] PUF-Com

Extractable Commitment from (malicious) PUFs

Problem 1: Adv can query with 0/1

idea [MQU07,CGS08]



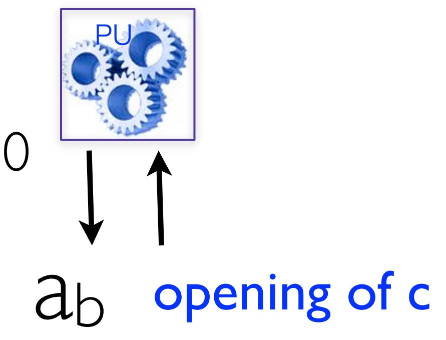


for free: stand-alone unconditional commitment from [OSVW13] PUF-Com

Extractable Commitment from (malicious) PUFs

Problem 1: Adv can query with 0/1

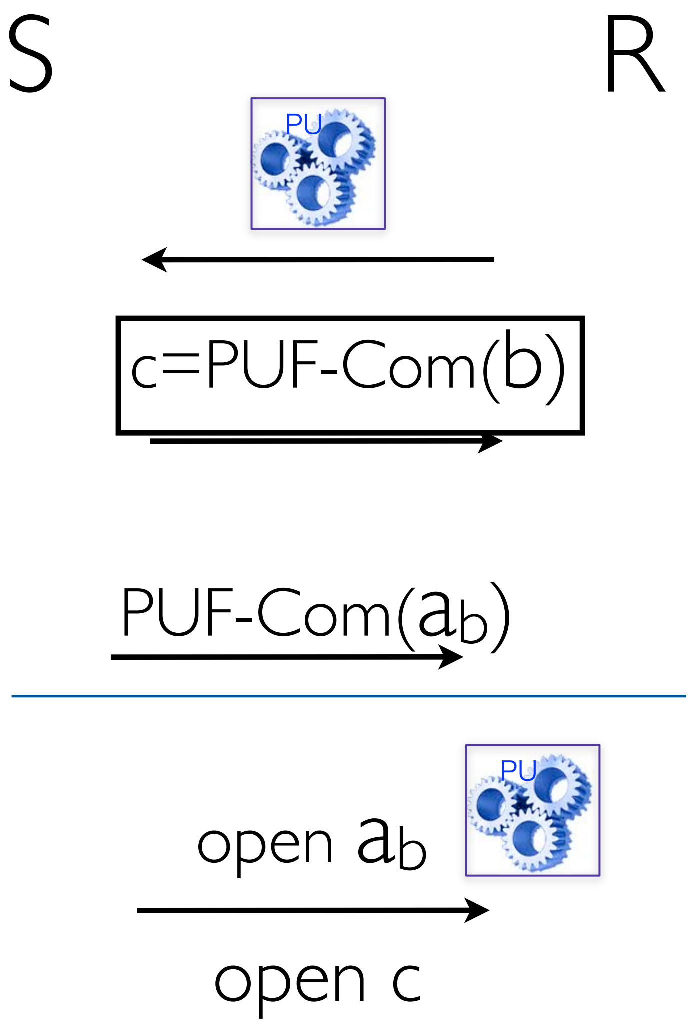
idea [MQU07,CGS08]



a_b opening of c

Problem 2: Adv queries with strings that are “close” to the actual opening

unpredictability does not hold for close queries



S

R

c=PUF-Com(b)

PUF-Com(a_b)

open a_b

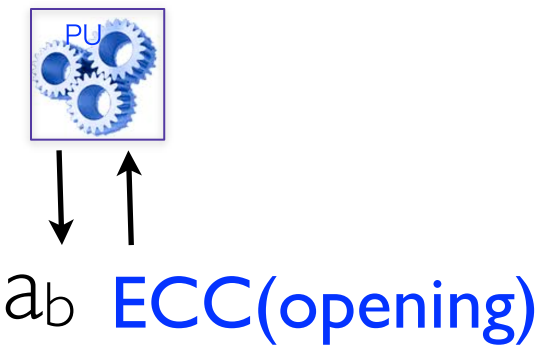
open c

for free: stand-alone unconditional commitment from [OSVW13] PUF-Com

Extractable Commitment from (malicious) PUFs

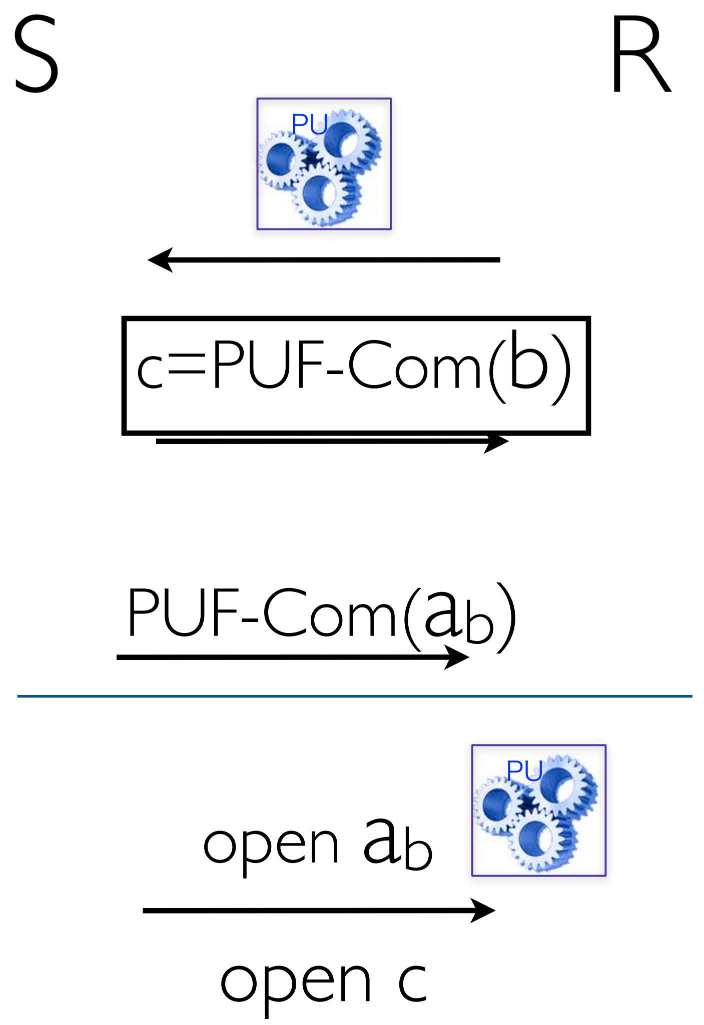
Problem 1: Adv can query with 0/1

idea [MQU07,CGS08]



PU

a_b **ECC(opening)**



S

R

PU

c=PUF-Com(b)

PUF-Com(a_b)

open a_b

PU

open c

for free: stand-alone unconditional commitment from [OSVW13] PUF-Com

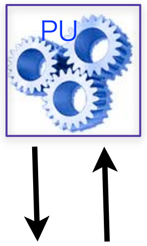
Problem 2: Adv queries with strings that are "close" to the actual opening

unpredictability does not hold for close queries

Extractable Commitment from (malicious) PUFs

Problem 1: Adv can query with 0/1

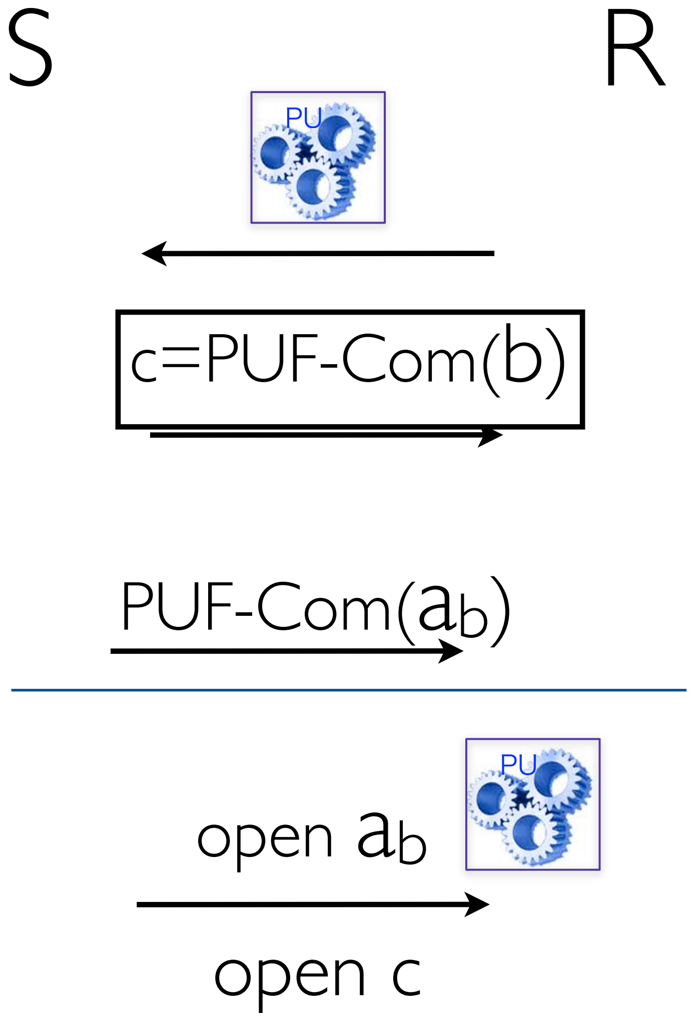
idea [MQU07,CGS08]



a_b **ECC(opening)**

Problem 2: Adv queries with strings that are "close" to the actual opening

unpredictability does not hold for close queries



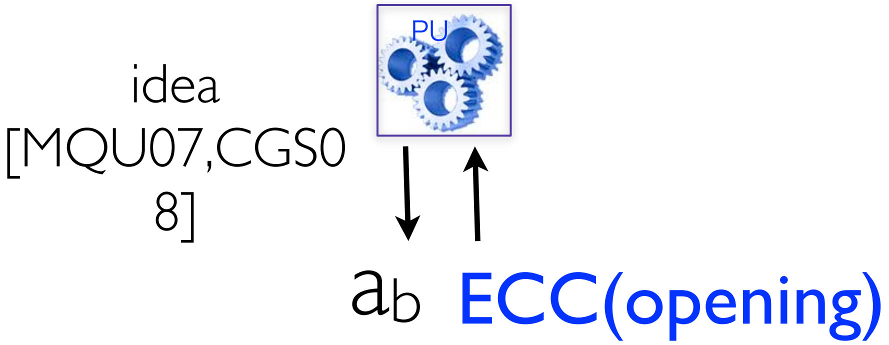
for free: stand-alone unconditional commitment from [OSVW13] PUF-Com

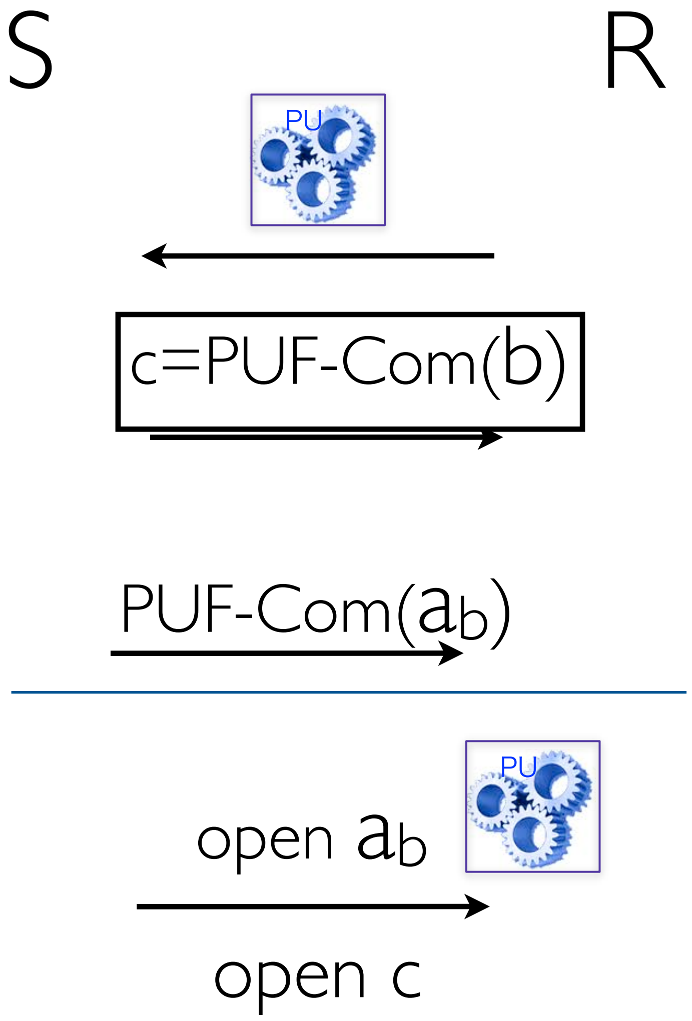
token

we construct: stand-alone unconditional commitment from malicious tokens

Extractable Commitment from (malicious) PUFs

Problem 1: Adv can query with 0/1





for free: stand-alone unconditional commitment from [OSVW13] PUF-Com

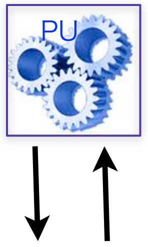
token

we construct: stand-alone unconditional commitment from malicious tokens

Extractable Commitment from (malicious) PUFs

Problem 1: Adv can query with 0/1

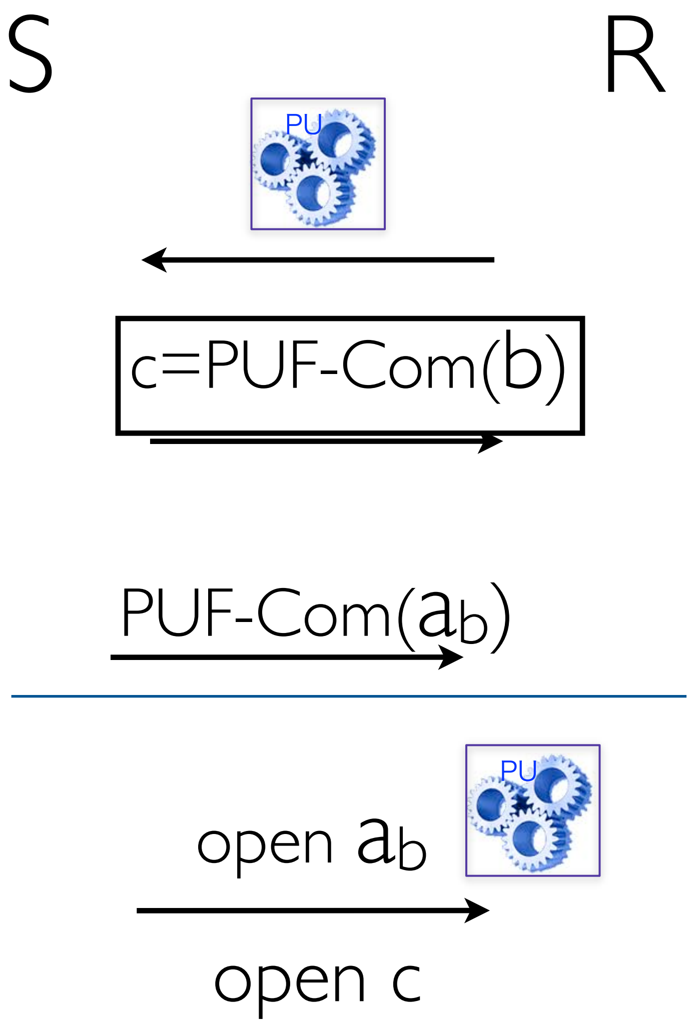
idea [MQU07,CGS08]



a_b **ECC(opening)**

token

no unconditional unpredictability for free: prevent uncontrolled access to the (stateless) token



for free: stand-alone unconditional commitment from [OSVW13] PUF-Com

token

we construct: stand-alone unconditional commitment from malicious tokens

Conclusion

- black-box compiler **any** extractable commitments => UC-commitments
- Extractable commitments from Malicious PUFs => the first unconditional UC-security with PUFs
- Extractable commitments from Stateless token admitting arbitrary malicious adversary => the first unc. UC-secure protocol with stateless tokens. Complete the picture of unconditional UC security with stateless tokens.
- Unconditional OT with malicious PUFs??

Thanks