Four-Round Black-Box Non-Malleable Commitments from One-Way Permutations

Michele Ciampi
The University of Edinburgh

Emmanuela Orsini
imec-COSIC, KU Leuven

Luisa Siniscalchi
Danish Technical University

Commitment scheme

Commitment scheme

Commitment scheme

Commitment scheme

Commitment scheme

Commitment scheme

- Binding

Commitment scheme

- Binding
- Hiding

Non-malleable commitment

w.r.t. commitment

Man In the Middle

Non-malleable commitment

w.r.t. commitment

Man In the Middle

Non-malleable commitment

w.r.t. commitment

Man In the Middle

Non-malleable commitment

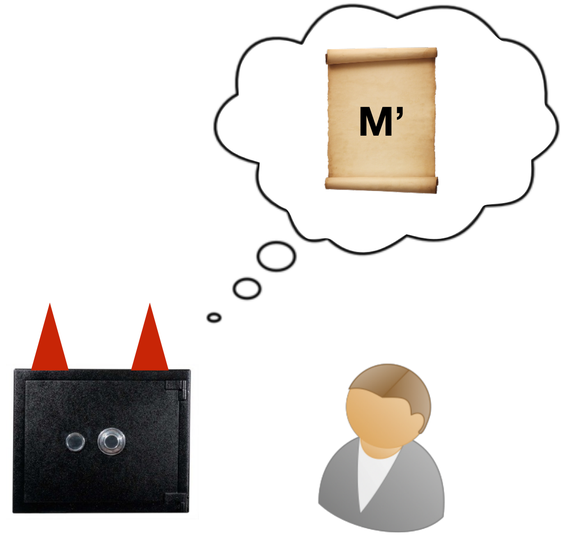
w.r.t. commitment

Man In the Middle

Non-malleable commitment

w.r.t. commitment

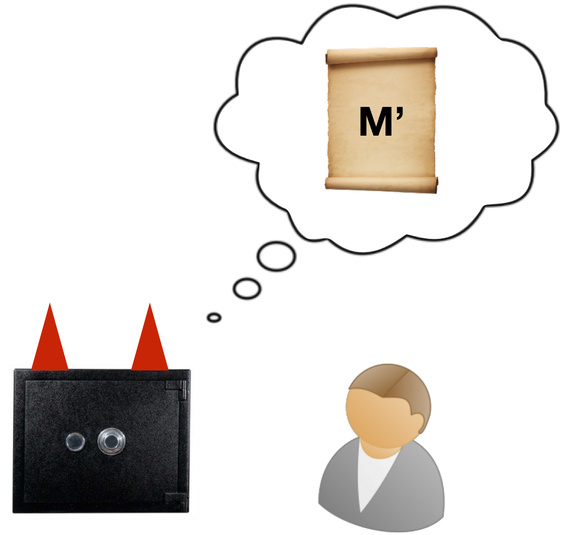
Man In the Middle



Non-malleable commitment

w.r.t. commitment

Man In the Middle



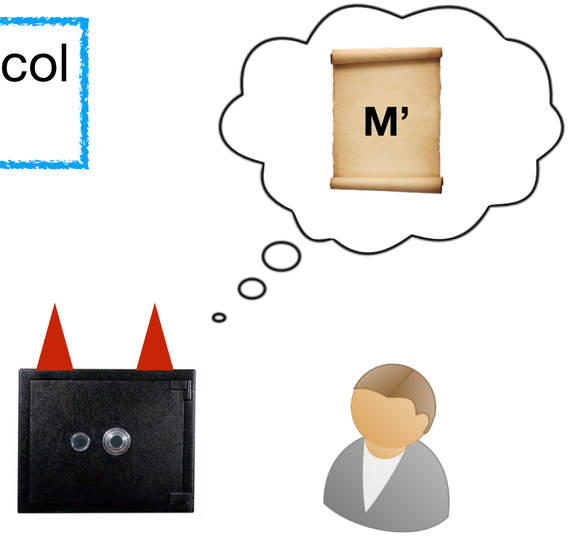
No relation between **M** and **M'**

Non-malleable commitment

w.r.t. commitment

Crucial for constructing MPC protocol with minimal round complexity

Man In the Middle



No relation between **M** and **M'**

State of the art on non-malleable commitments

(Plain model, polynomial-time assumptions)

*one-to-one OWFs

State of the art on non-malleable commitments

(Plain model, polynomial-time assumptions)

Result	Number of rounds	Assumptions	BB use of adversary	BB use of primitives
[DDN, STOC91]	Logarithmic	OWFs	Yes	**No**
[Bar, FOCS02]	Constant	CHRFs + TPs	No	**No**
[PR, FOCS05]	Constant	Claw-Free Perm	No	**No**
[PW, EUROCRYPT10]	Constant	Sub-esponenial OWFs	Yes	**No**
[Goy11/LP11, STOC11]	Constant	OWFs	Yes	**No**
[GLOV, FOCS12]	Constant	BB OWFs	Yes	**Yes**

*one-to-one OWFs

State of the art on non-malleable commitments

(Plain model, polynomial-time assumptions)

Result	Number of rounds	Assumptions	BB use of adversary	BB use of primitives
[DDN, STOC91]	Logarithmic	OWFs	Yes	**No**
[Bar, FOCS02]	Constant	CHRFs + TPs	No	**No**
[PR, FOCS05]	Constant	Claw-Free Perm	No	**No**
[PW, EUROCRYPT10]	Constant	Sub-esponenial OWFs	Yes	**No**
[Goy11/LP11, STOC11]	Constant	OWFs	Yes	**No**
[GLOV, FOCS12]	Constant	BB OWFs	Yes	**Yes**
[GRRV, FOCS14]	4	OWFs	Yes	**No**
[COSV, CRYPTO17]	4	OWFs*	Yes	**No**
[Khu, TCC17]	3	DDH	Yes	**No**
[GR19, FOCS19]	3	OWFs*	Yes	**No**

Three-round lower bound [Pas,TCC13]

*one-to-one OWFs

State of the art on non-malleable commitments

(Plain model, polynomial-time assumptions)

Result	Number of rounds	Assumptions	BB use of adversary	BB use of primitives
[DDN, STOC91]	Logarithmic	OWFs	Yes	**No**
[Bar, FOCS02]	Constant	CHRFs + TPs	No	**No**
[PR, FOCS05]	Constant	Claw-Free Perm	No	**No**
[PW, EUROCRYPT10]	Constant	Sub-esponenial OWFs	Yes	**No**
[Goy11/LP11, STOC11]	Constant	OWFs	Yes	**No**
[GLOV, FOCS12]	Constant	BB OWFs	Yes	**Yes**
[GRRV, FOCS14]	4	OWFs	Yes	**No**
[COSV, CRYPTO17]	4	OWFs*	Yes	**No**
[Khu, TCC17]	3	DDH	Yes	**No**
[GR19, FOCS19]	3	OWFs*	Yes	**No**

Three-round lower bound [Pas,TCC13]

*one-to-one OWFs

State of the art on non-malleable commitments

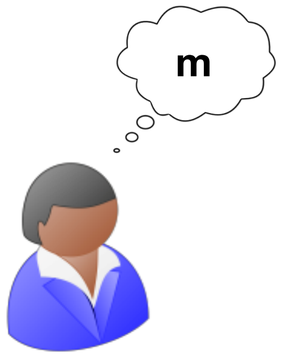
(Plain model, polynomial-time assumptions)

Result	Number of rounds	Assumptions	BB use of adversary	BB use of primitives
[DDN, STOC91]	Logarithmic	OWFs	Yes	**No**
[Bar, FOCS02]	Constant	CHRFs + TPs	No	**No**
[PR, FOCS05]	Constant	Claw-Free Perm	No	**No**
[PW, EUROCRYPT10]	Constant	Sub-esponenial OWFs	Yes	**No**
[Goy11/LP11, STOC11]	Constant	OWFs	Yes	**No**
[GLOV, FOCS12]	Constant	BB OWFs	Yes	**Yes**
[GRRV, FOCS14]	4	OWFs	Yes	**No**
[COSV, CRYPTO17]	4	OWFs*	Yes	**No**
[Khu, TCC17]	3	DDH	Yes	**No**
[GR19, FOCS19]	3	OWFs*	Yes	**No**
This work	**4**	**OWFs***	**Yes**	**Yes**

Three-round lower bound [Pas,TCC13]

*one-to-one OWFs

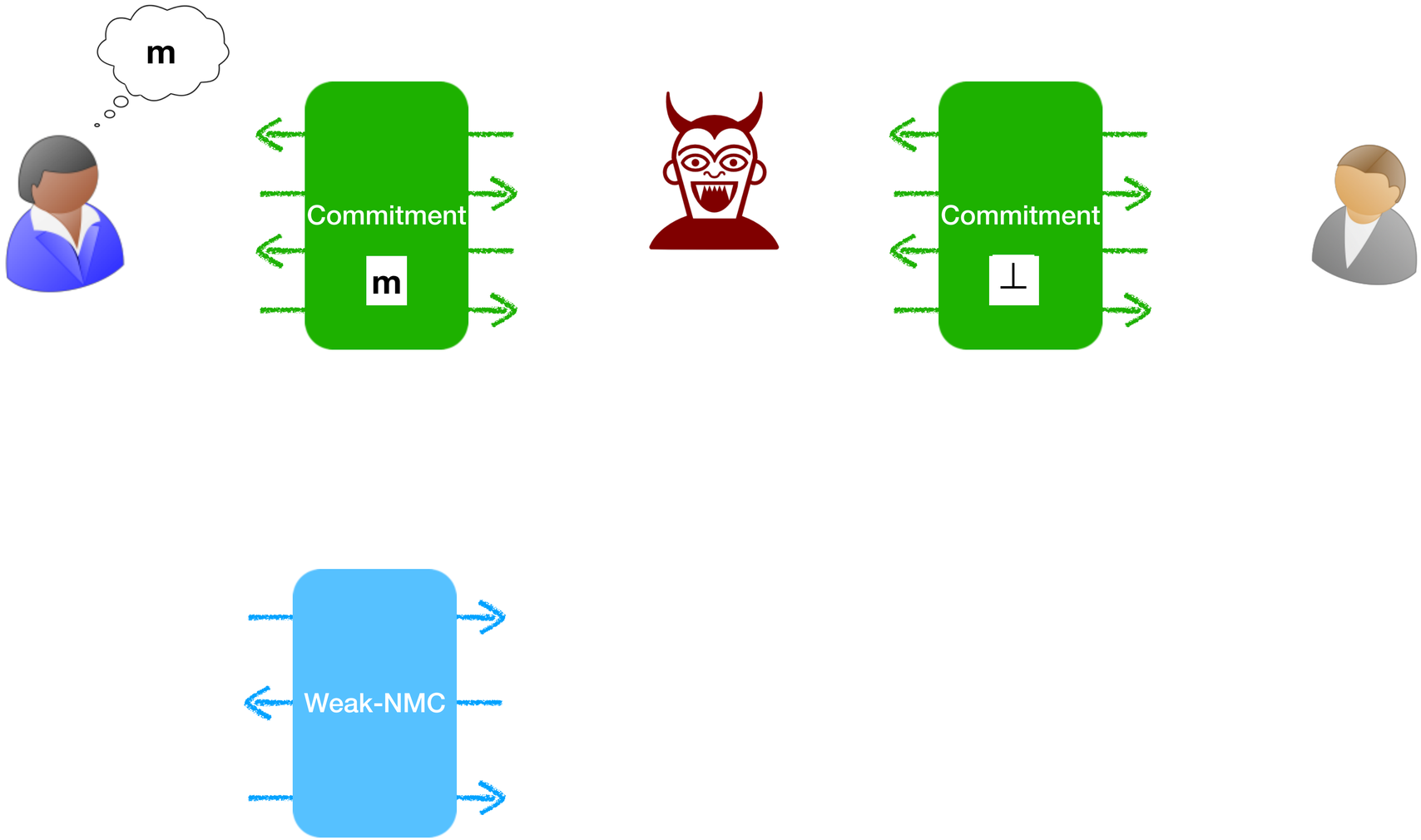
Weak Non-Malleable Commitments



Weak Non-Malleable Commitments

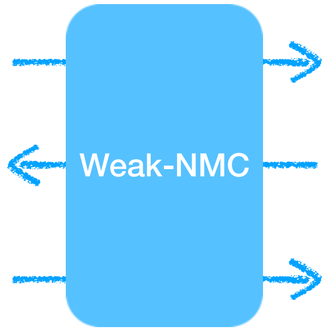
Weak Non-Malleable Commitments

Weak Non-Malleable Commitments



[GRRV14] Vipul Goyal, Silas Richelson, Alon Rosen, and Margarita Vald. FOCS 2014

Weak Non-Malleable Commitments

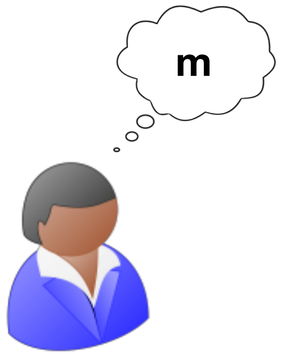


[GRRV14, Lemma] Weak-non-malleable commitment

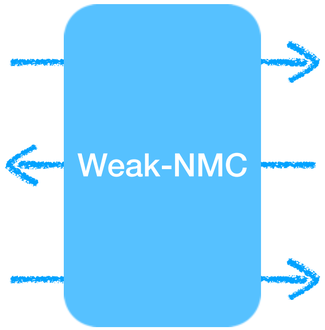
Has an extractor

[GRRV14] Vipul Goyal, Silas Richelson, Alon Rosen, and Margarita Vald. FOCS 2014

Weak Non-Malleable Commitments



Weak MiM

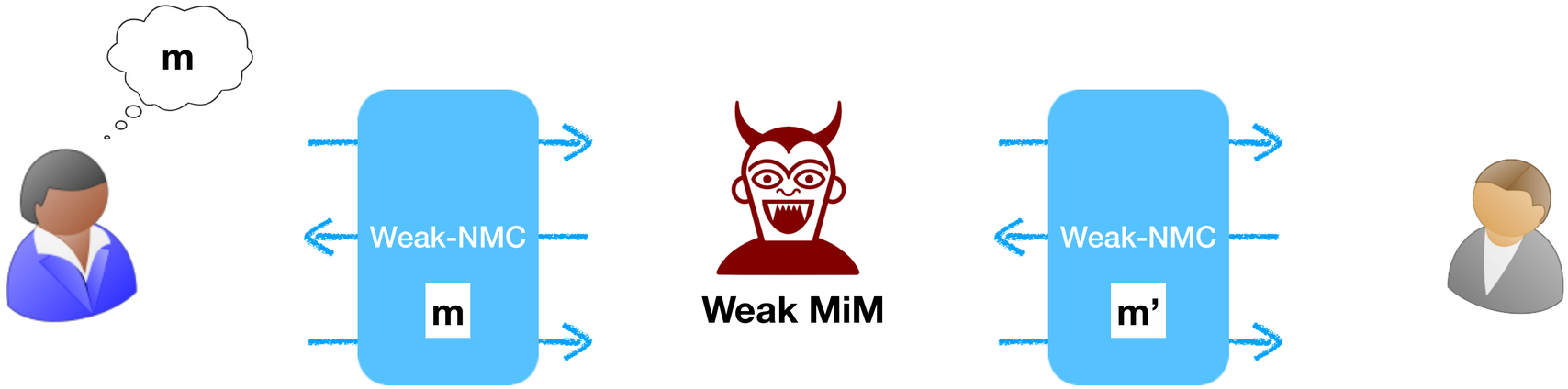


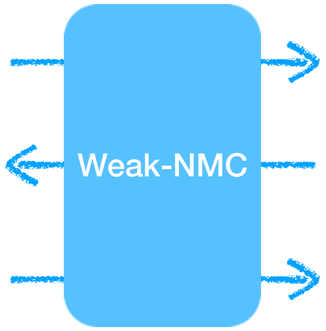
[GRRV14, Lemma] Weak-non-malleable commitment

Has an extractor

Vipul Goyal, Silas Richelson, Alon Rosen, and Margarita Vald. FOCS 2014

Weak Non-Malleable Commitments



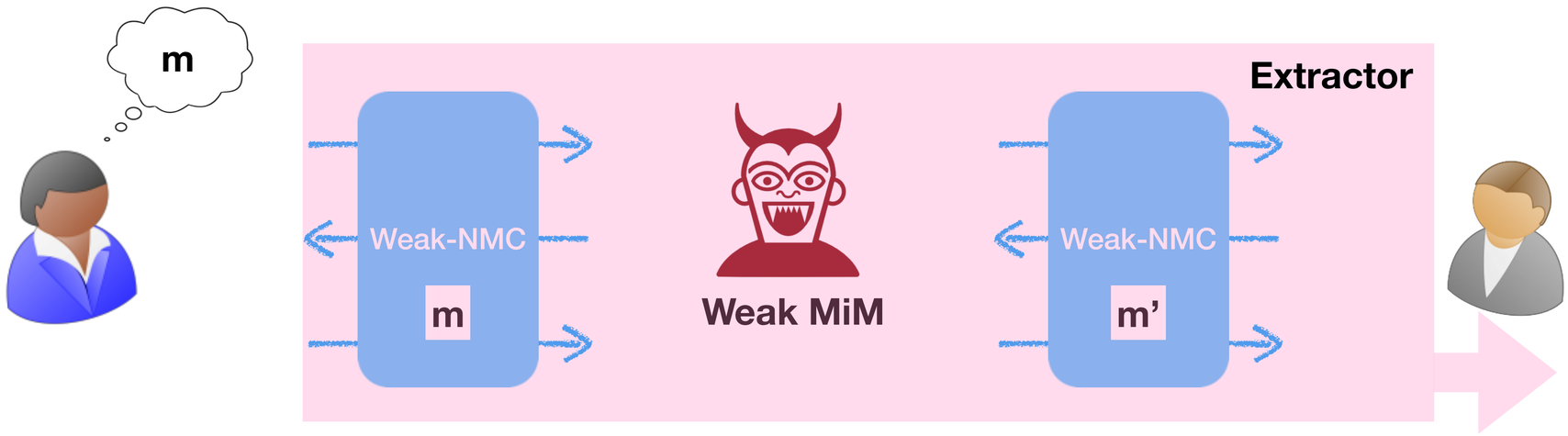


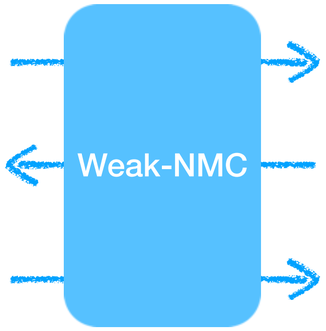
[GRRV14, Lemma] Weak-non-malleable commitment

Has an extractor

Vipul Goyal, Silas Richelson, Alon Rosen, and Margarita Vald. FOCS 2014

Weak Non-Malleable Commitments



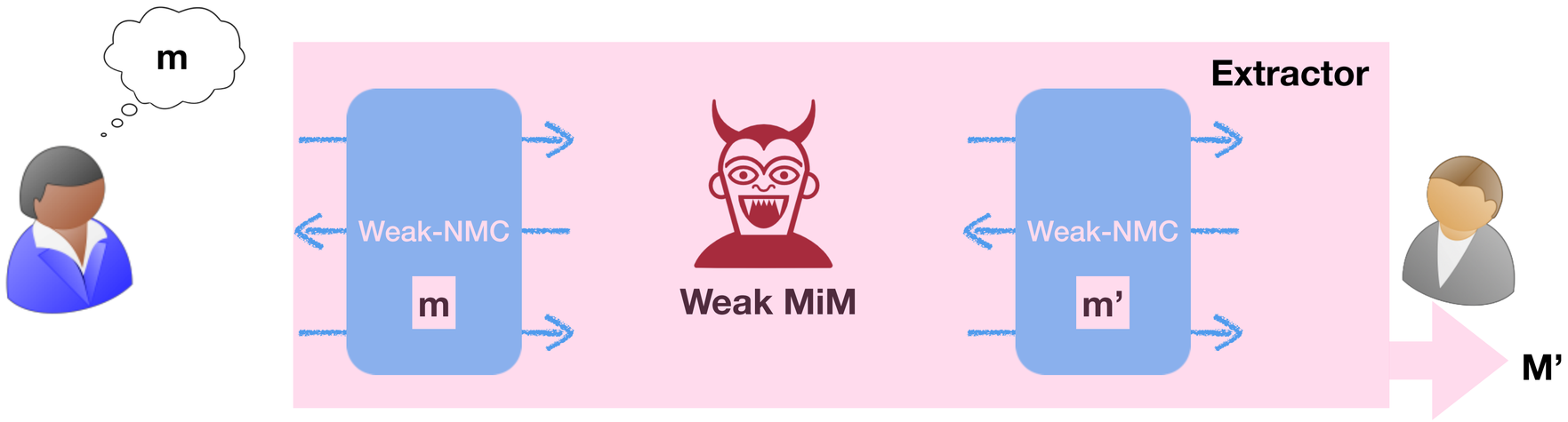


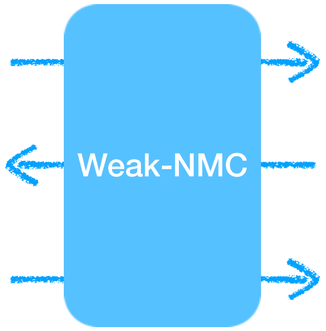
[GRRV14, Lemma] Weak-non-malleable commitment

Has an extractor

Vipul Goyal, Silas Richelson, Alon Rosen, and Margarita Vald. FOCS 2014

Weak Non-Malleable Commitments





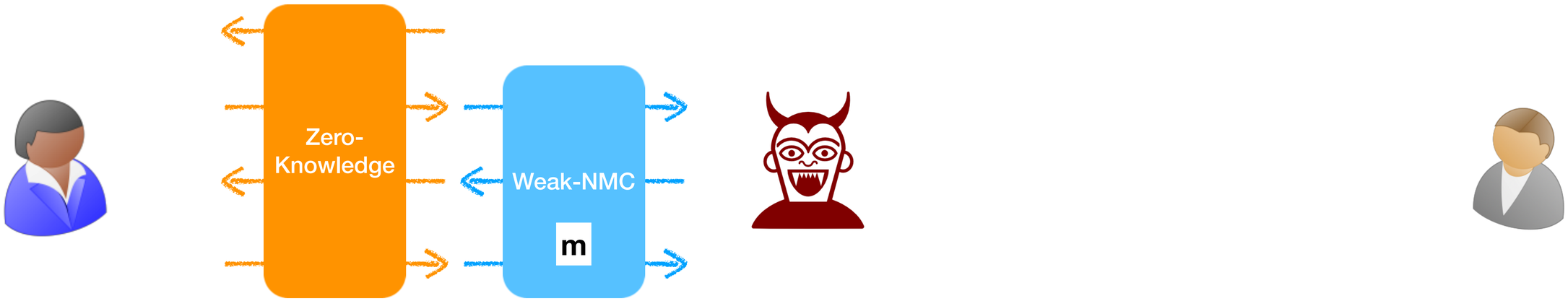
[GRRV14, Lemma] Weak-non-malleable commitment

Has an extractor

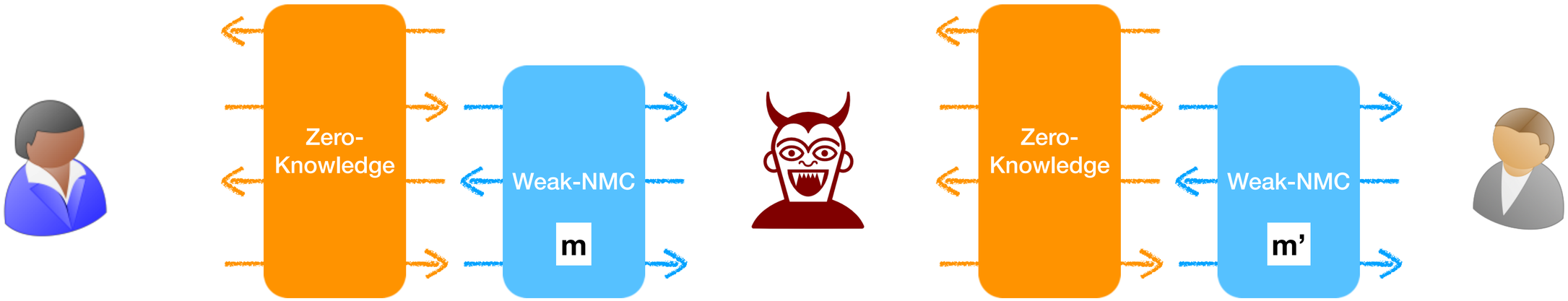
Vipul Goyal, Silas Richelson, Alon Rosen, and Margarita Vald. FOCS 2014

A candidate approach

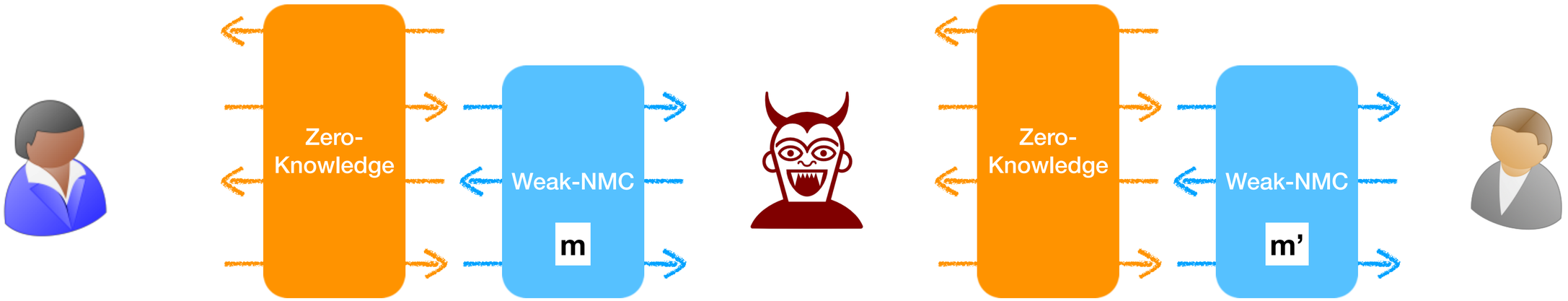
A candidate approach

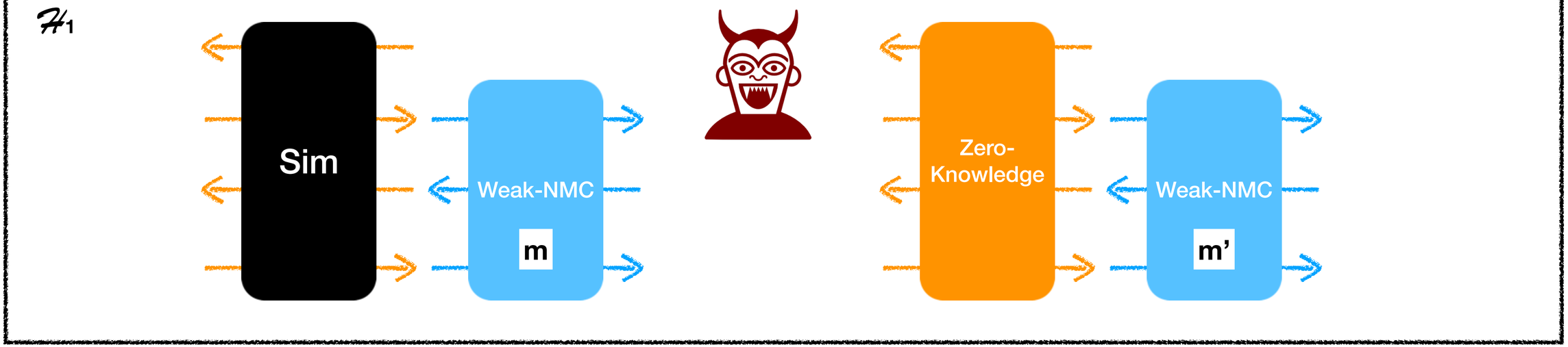


A candidate approach

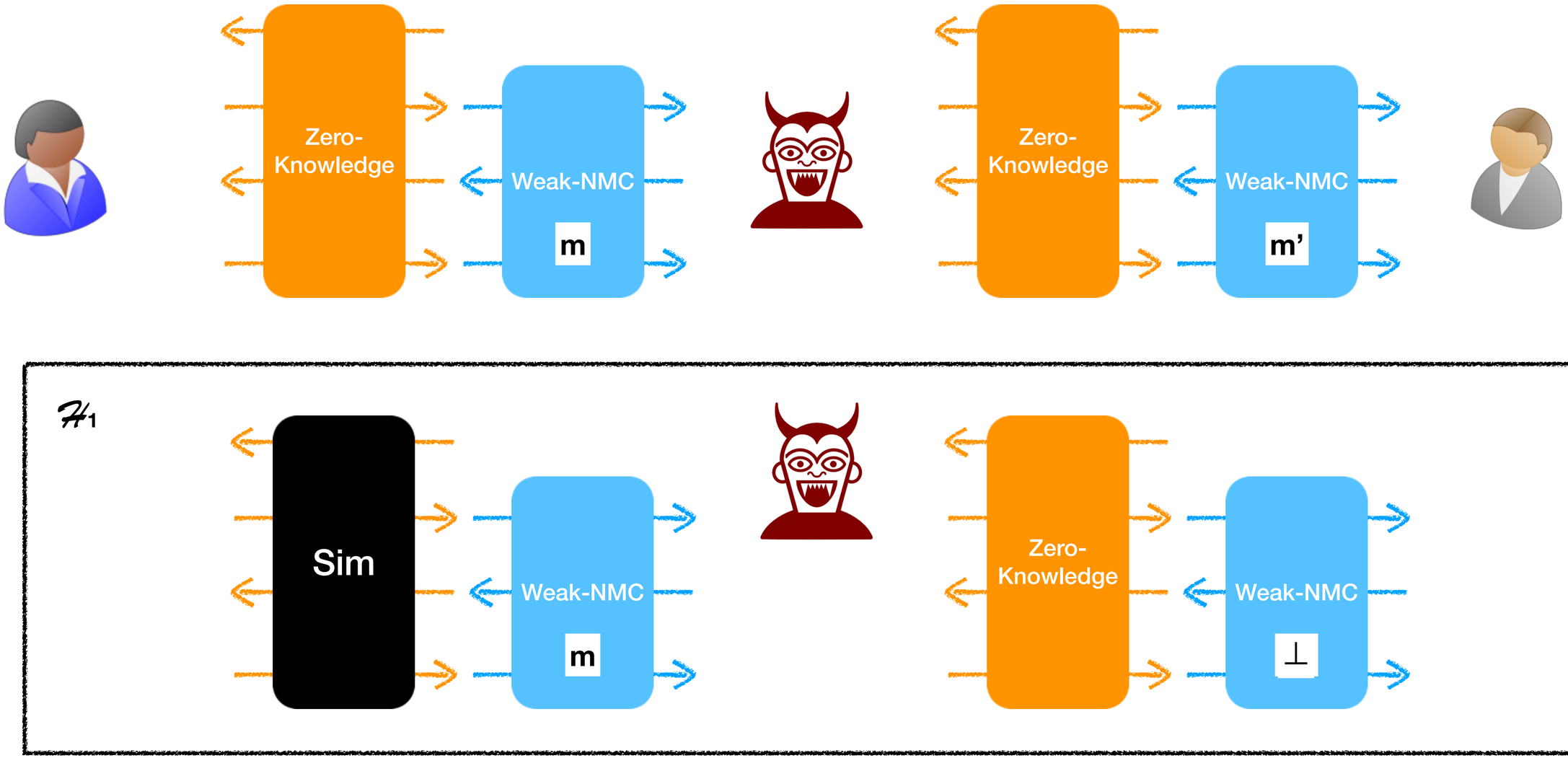


A candidate approach

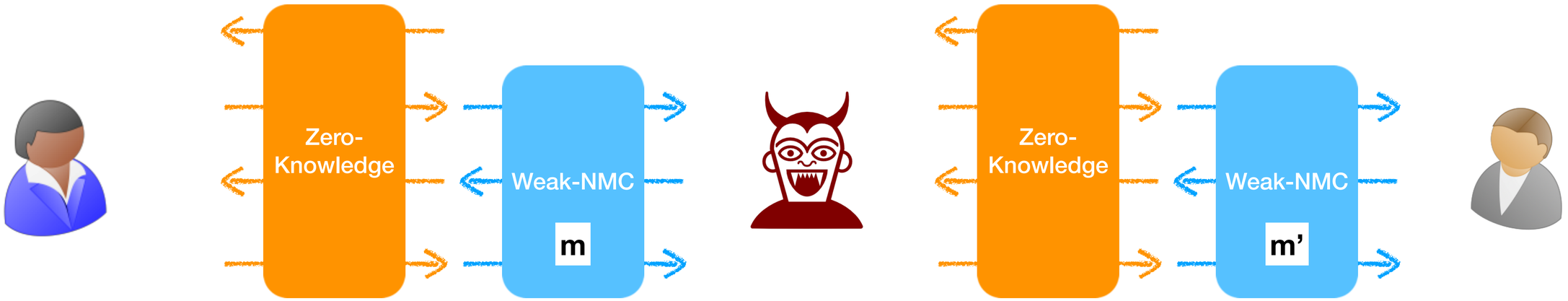


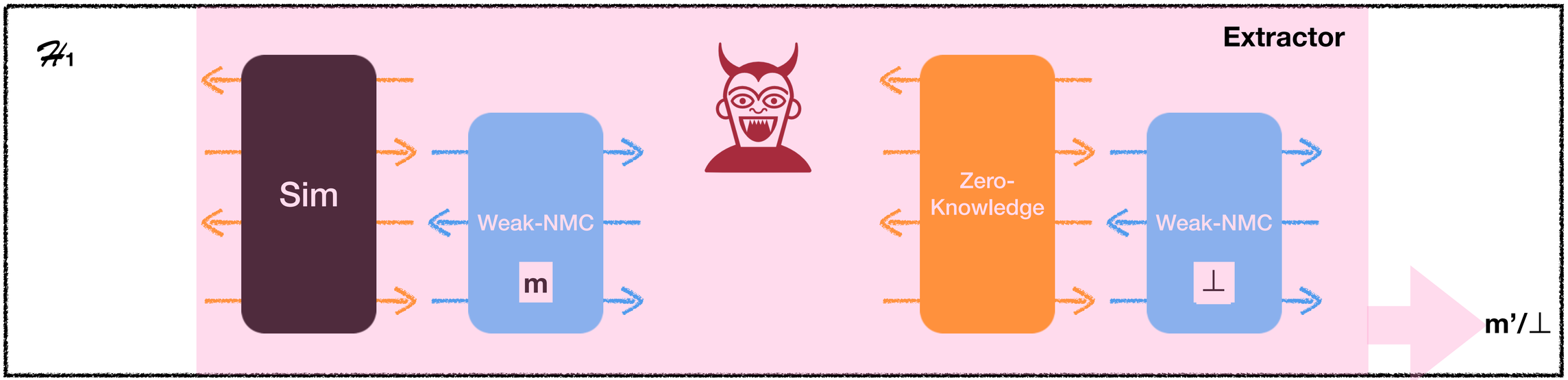


A candidate approach

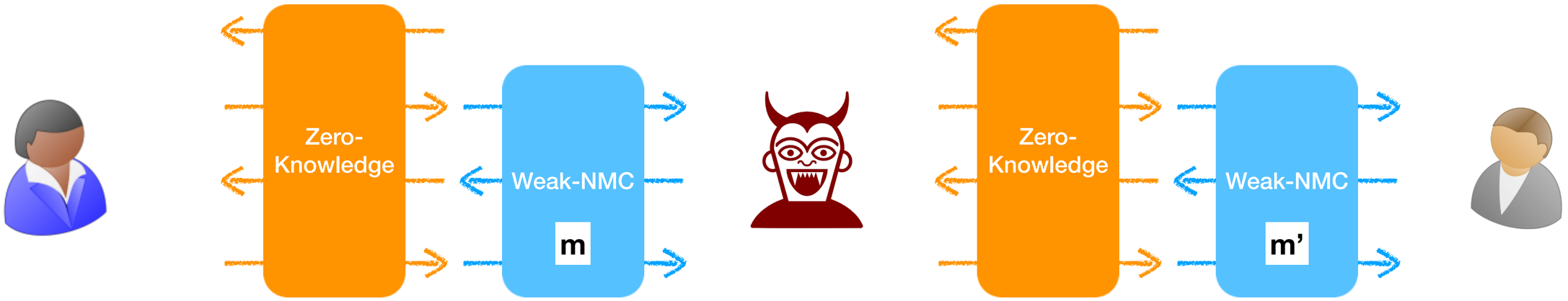


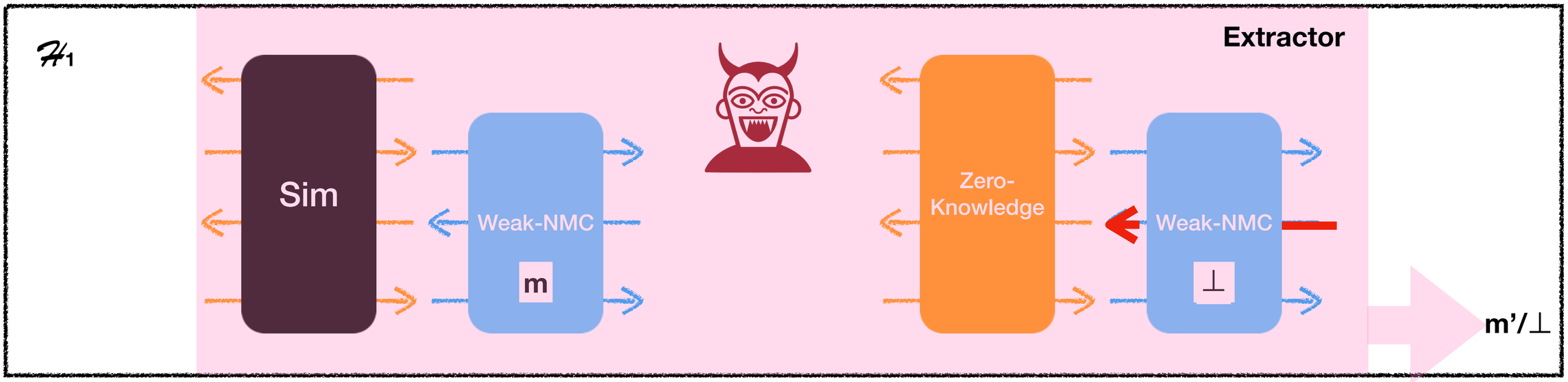
A candidate approach



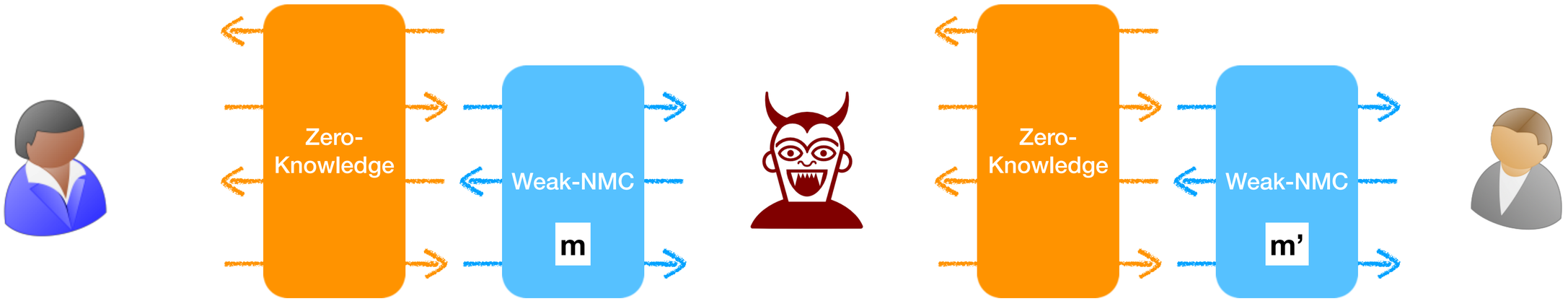


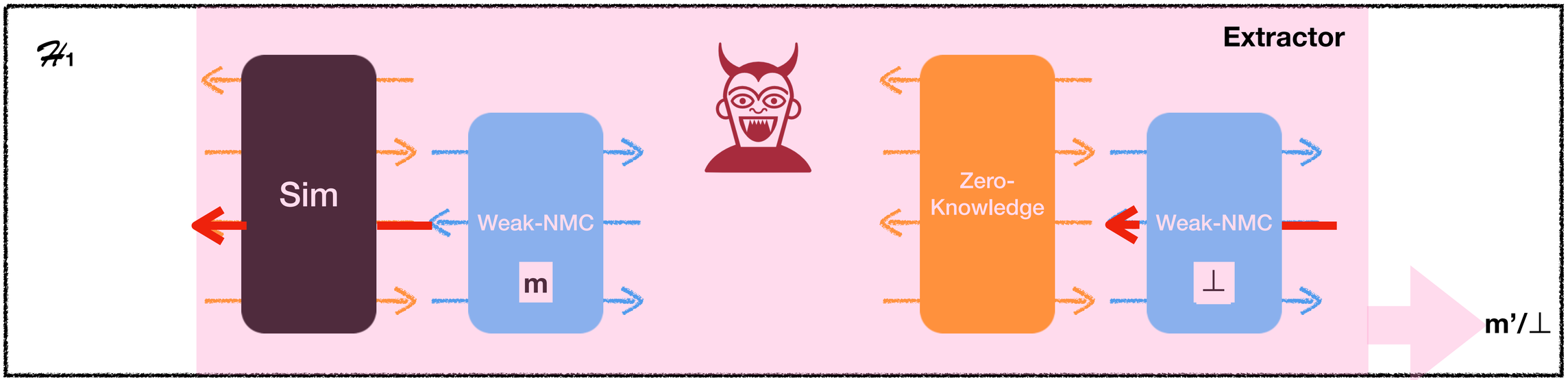
A candidate approach



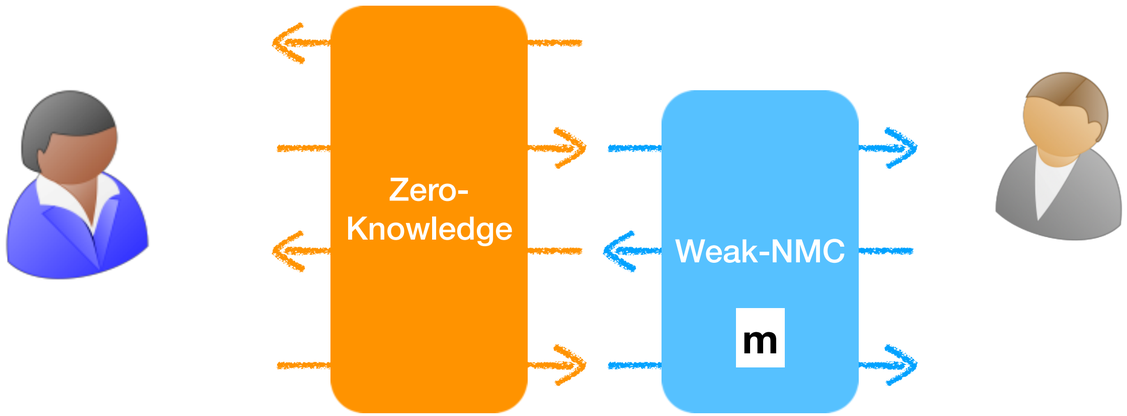


A candidate approach



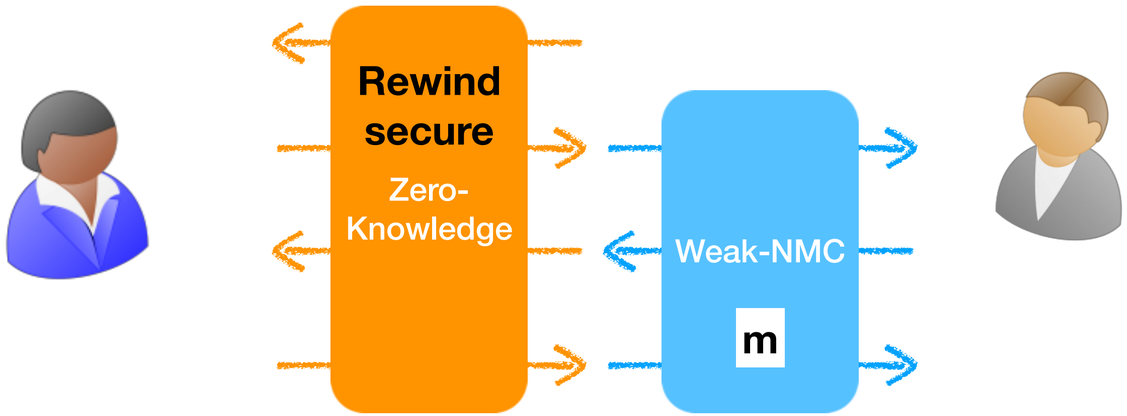


The [GRRV14] approach



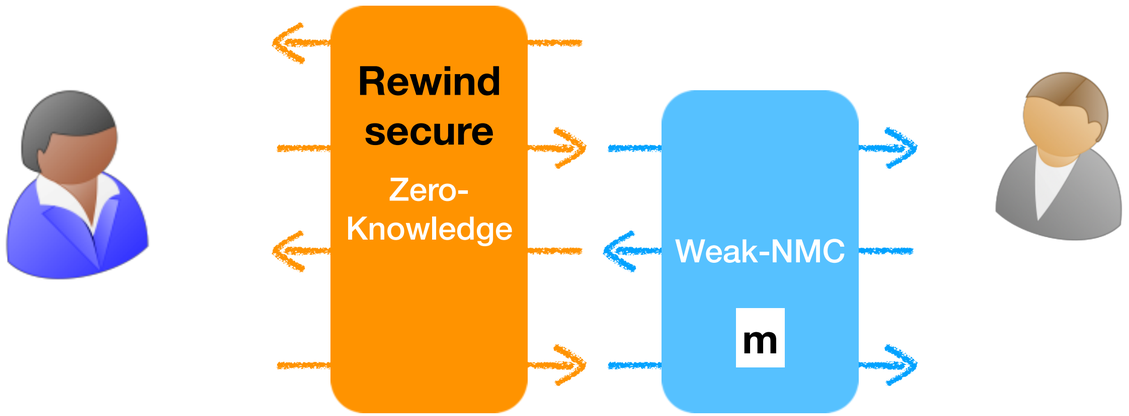
Vipul Goyal, Silas Richelson, Alon Rosen, and Margarita Vald. FOCS 2014

The [GRRV14] approach



Vipul Goyal, Silas Richelson, Alon Rosen, and Margarita Vald. FOCS 2014

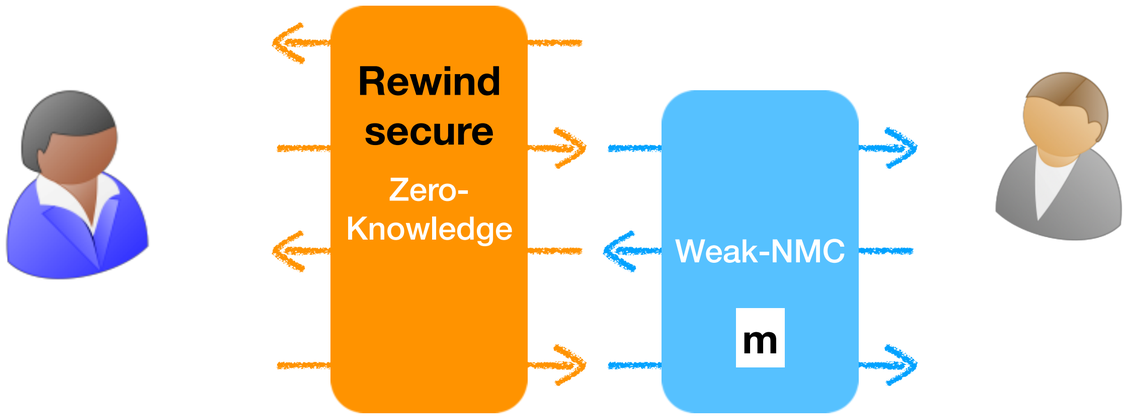
The [GRRV14] approach



4-round non-malleable commitment

Vipul Goyal, Silas Richelson, Alon Rosen, and Margarita Vald. FOCS 2014

The [GRRV14] approach

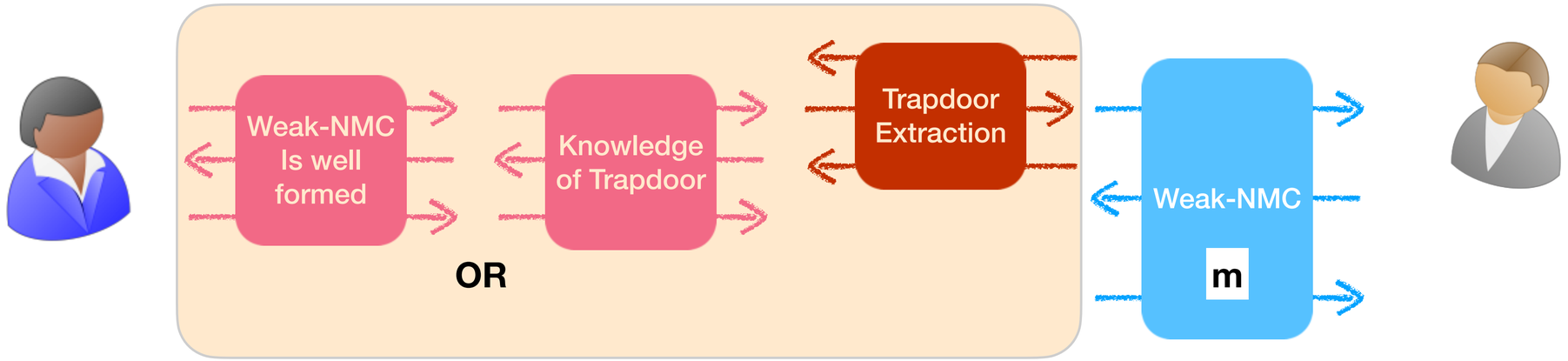


4-round non-malleable commitment

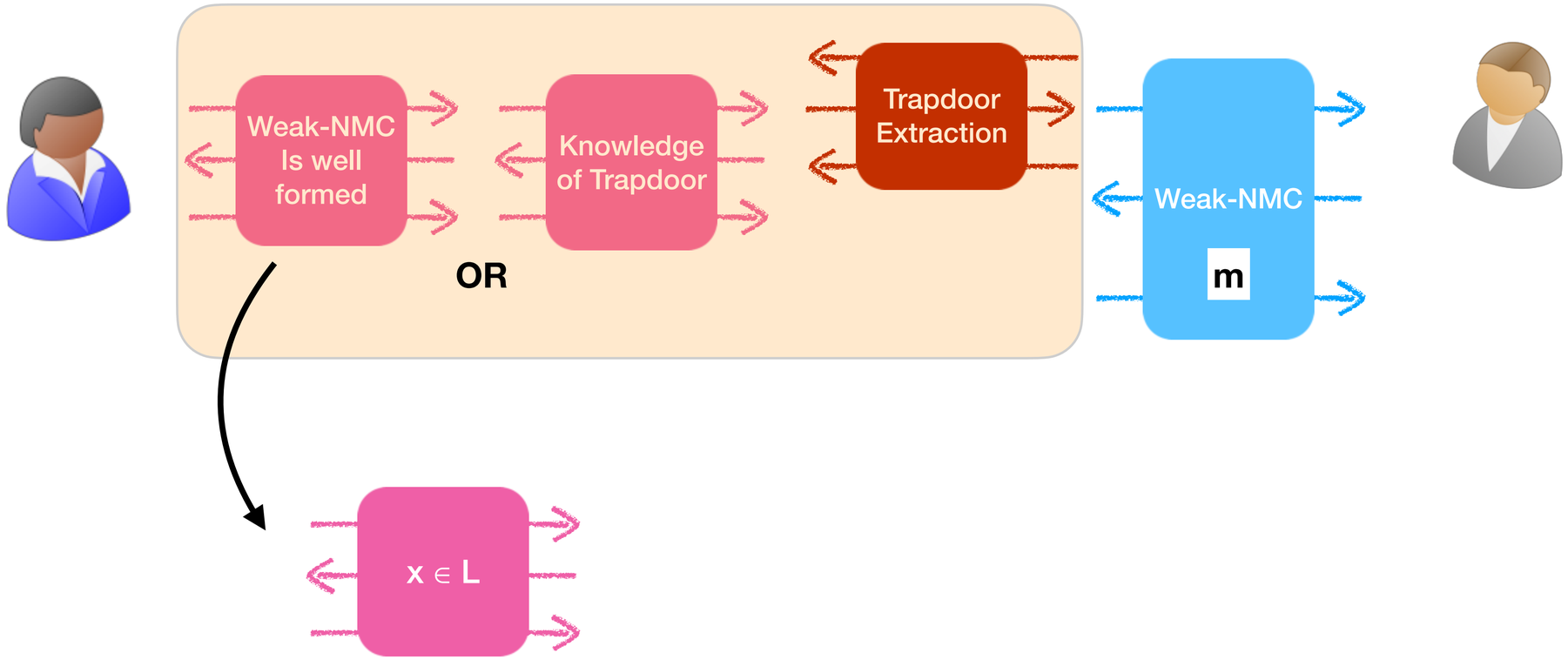
ZK is non-black box and it makes non-black-box use of the Weak-NMC

Vipul Goyal, Silas Richelson, Alon Rosen, and Margarita Vald. FOCS 2014

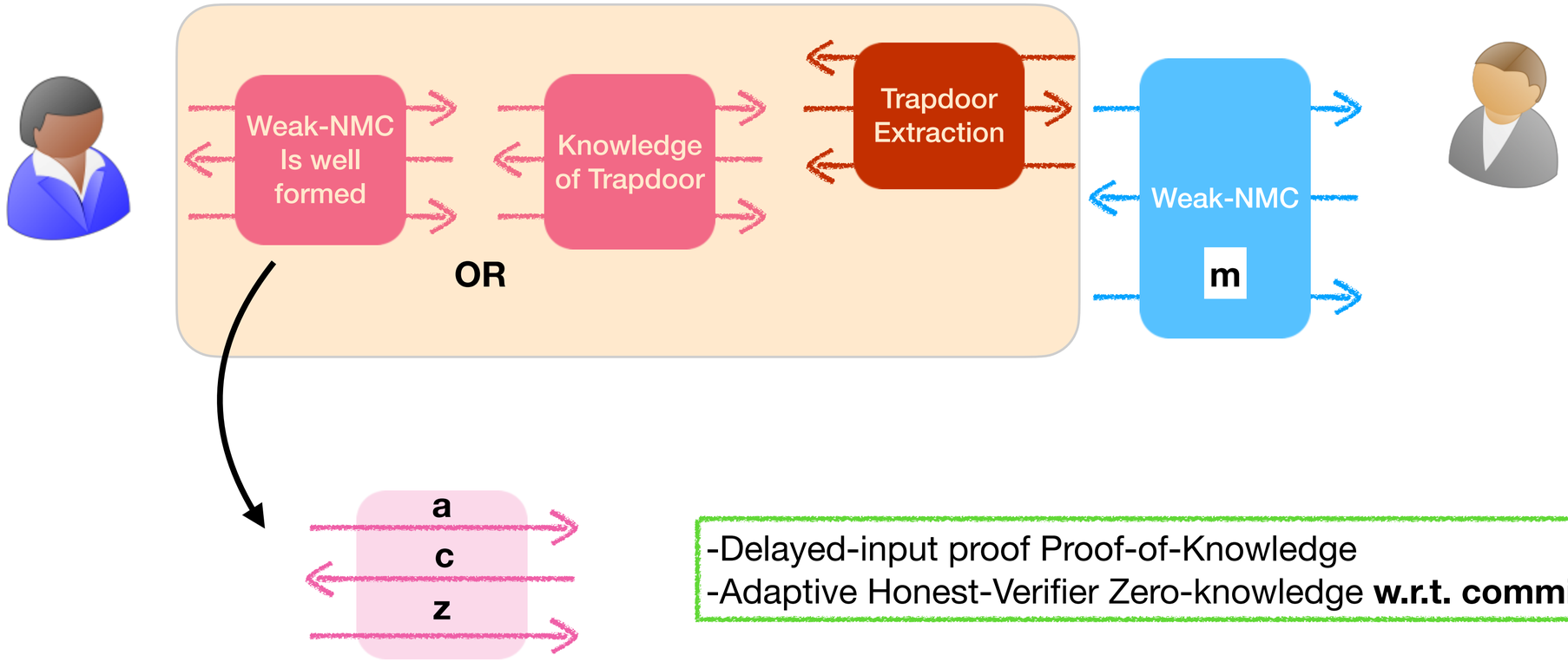
Our Approach



Our Approach



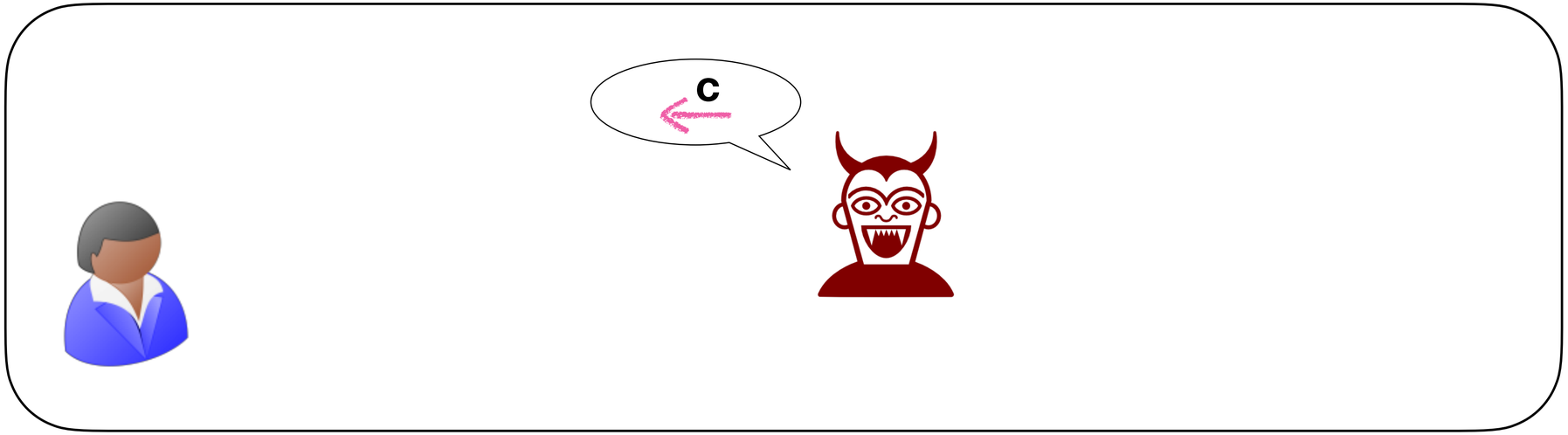
Our Approach



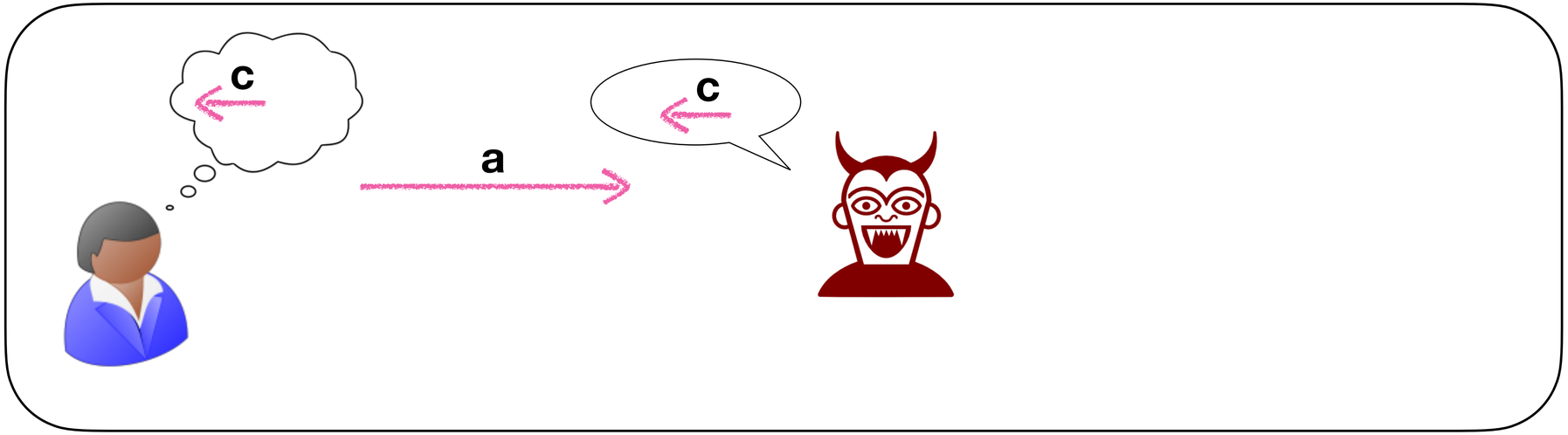
-Delayed-input proof Proof-of-Knowledge
-Adaptive Honest-Verifier Zero-knowledge **w.r.t. commitment**

Honest verifier zero-knowledge with respect to commitments (HVZK**C**)

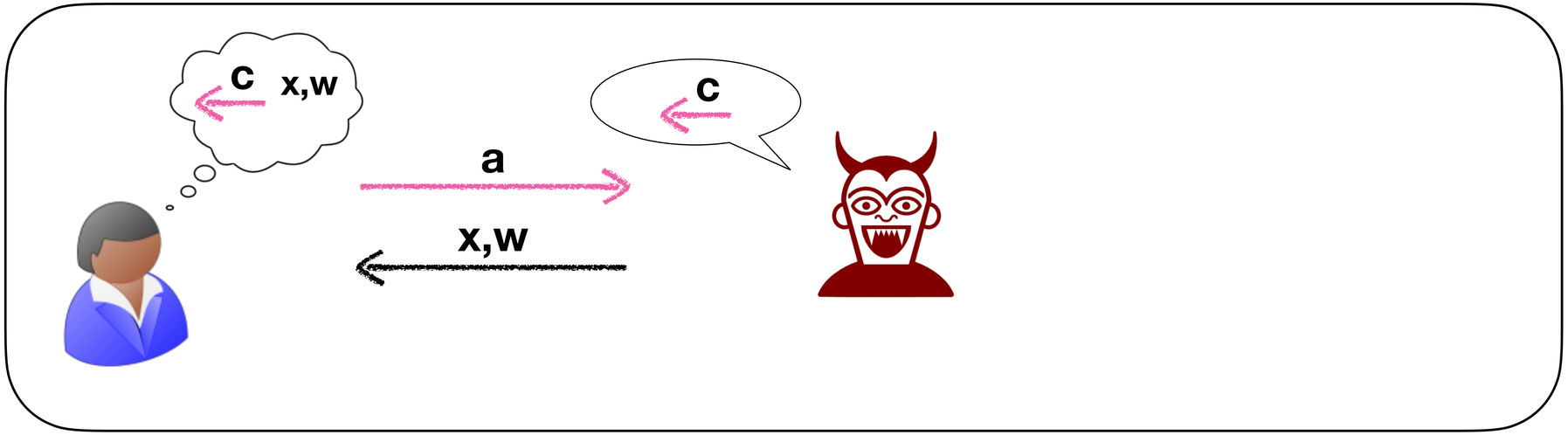
Honest verifier zero-knowledge with respect to commitments (HVZK**C**)



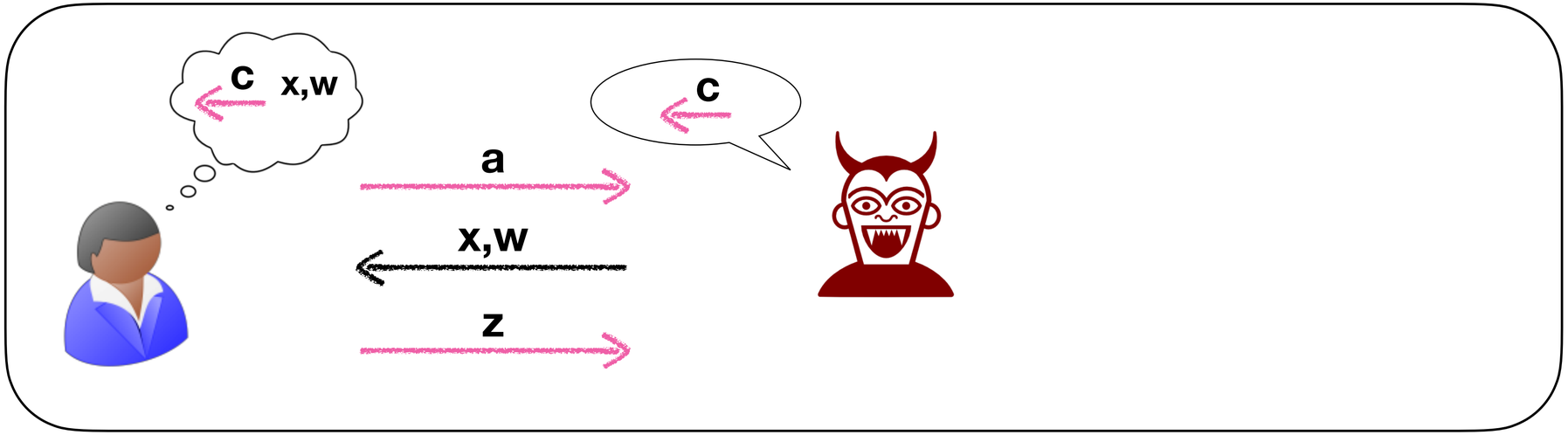
Honest verifier zero-knowledge with respect to commitments (HVZK**C**)



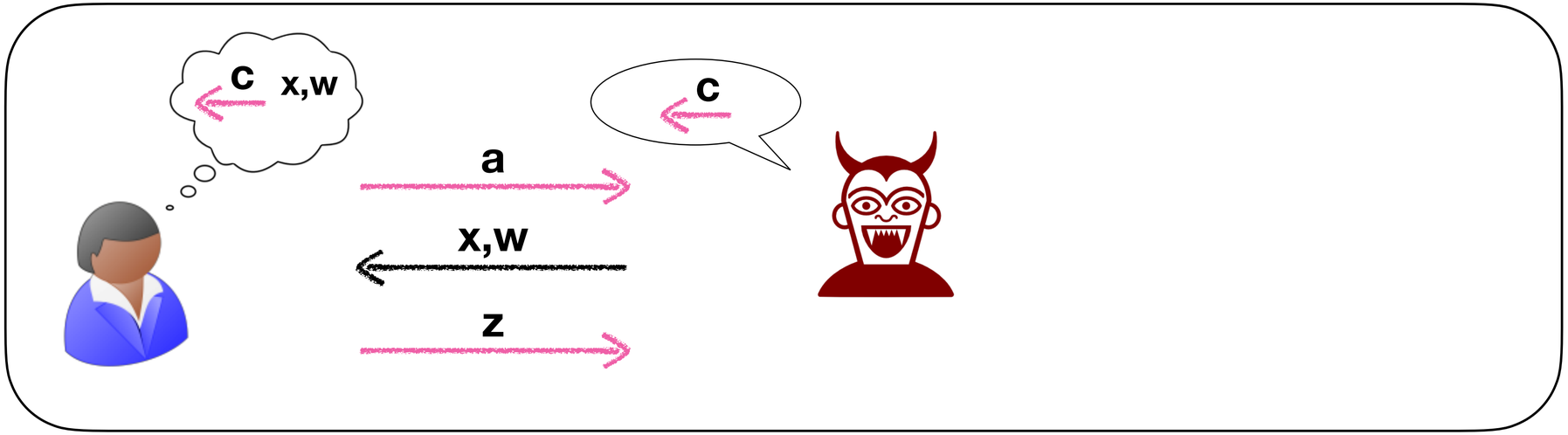
Honest verifier zero-knowledge with respect to commitments (HVZK**C**)

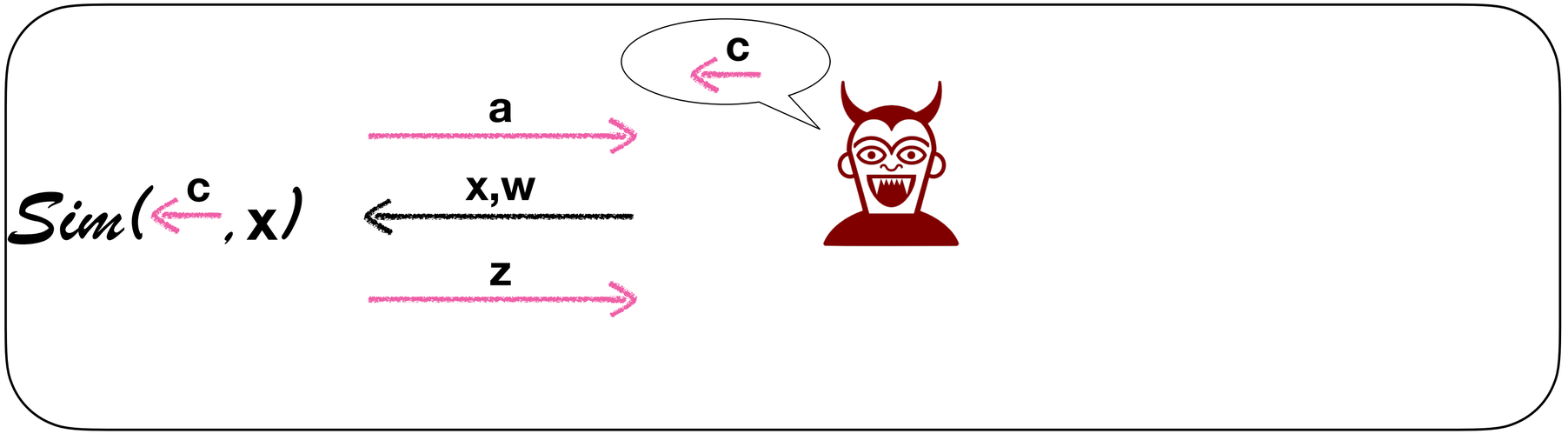


Honest verifier zero-knowledge with respect to commitments (HVZK**C**)

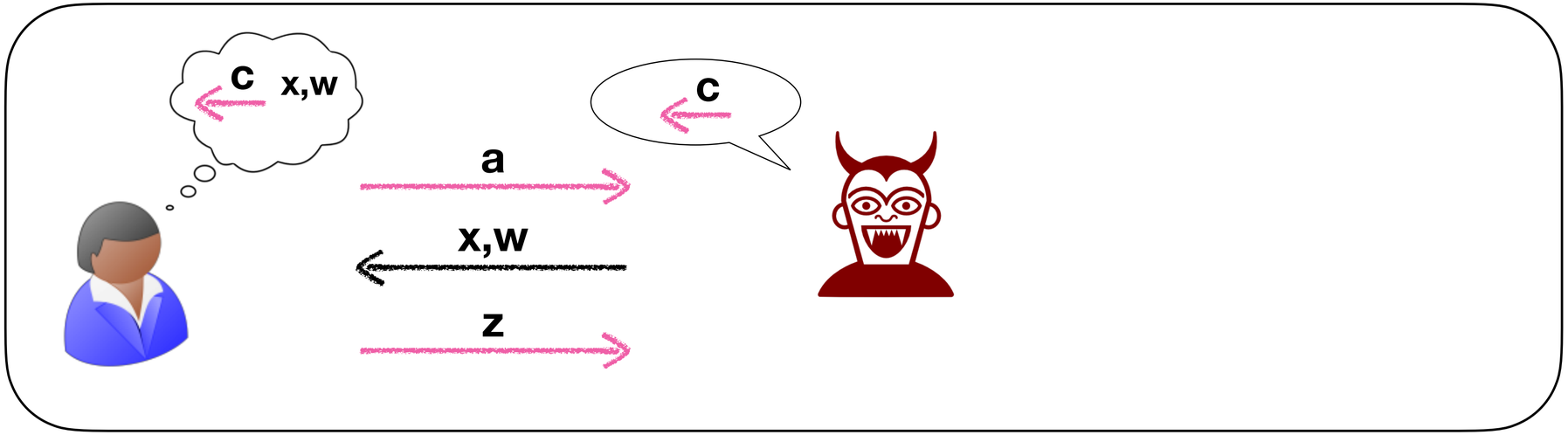


Honest verifier zero-knowledge with respect to commitments (HVZK**C**)



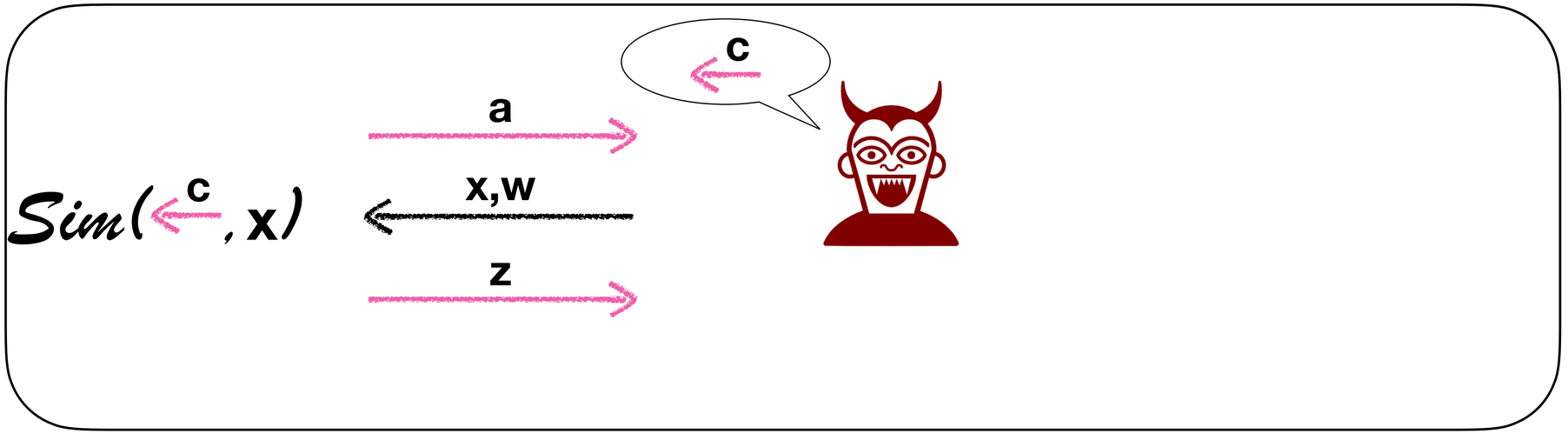


Honest verifier zero-knowledge with respect to commitments (HVZK**C**)

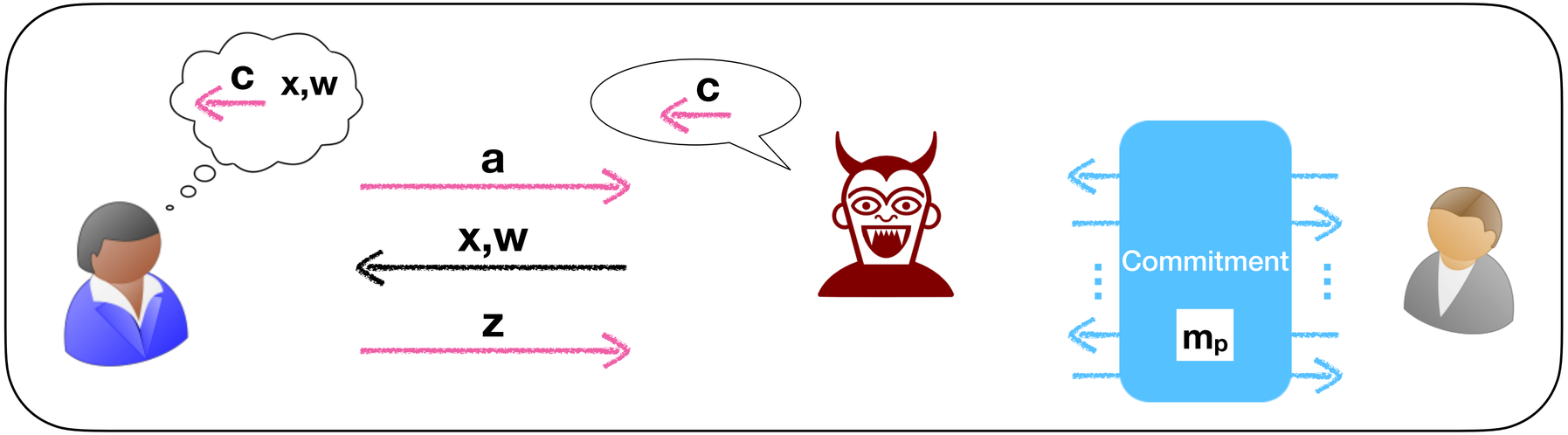


$\approx$

$D_{HVZK}(view)$

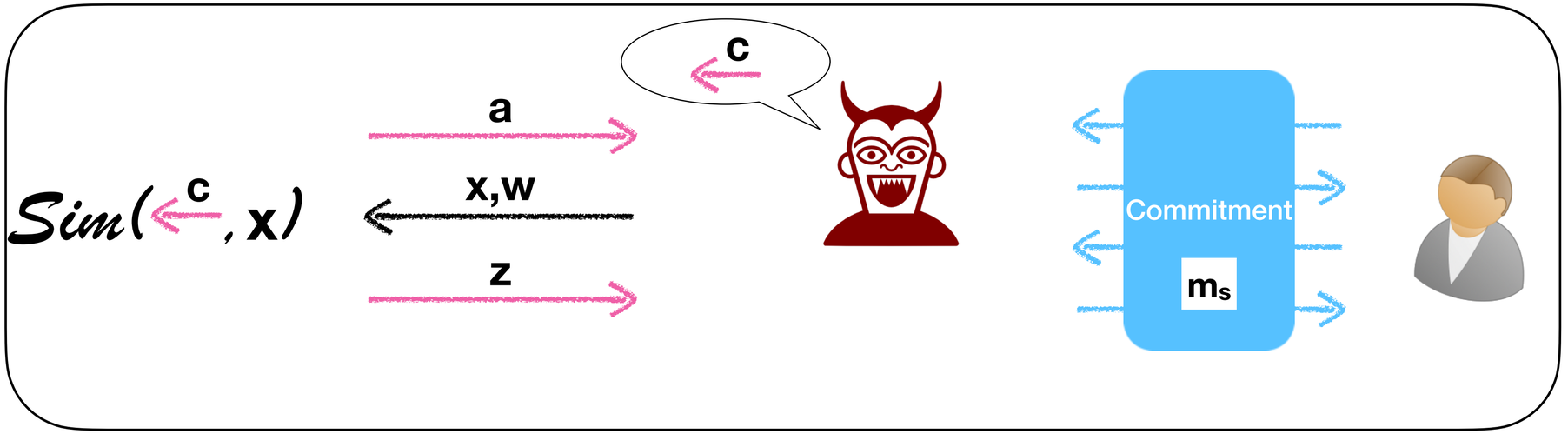


Honest verifier zero-knowledge with respect to commitments (HVZK**C**)



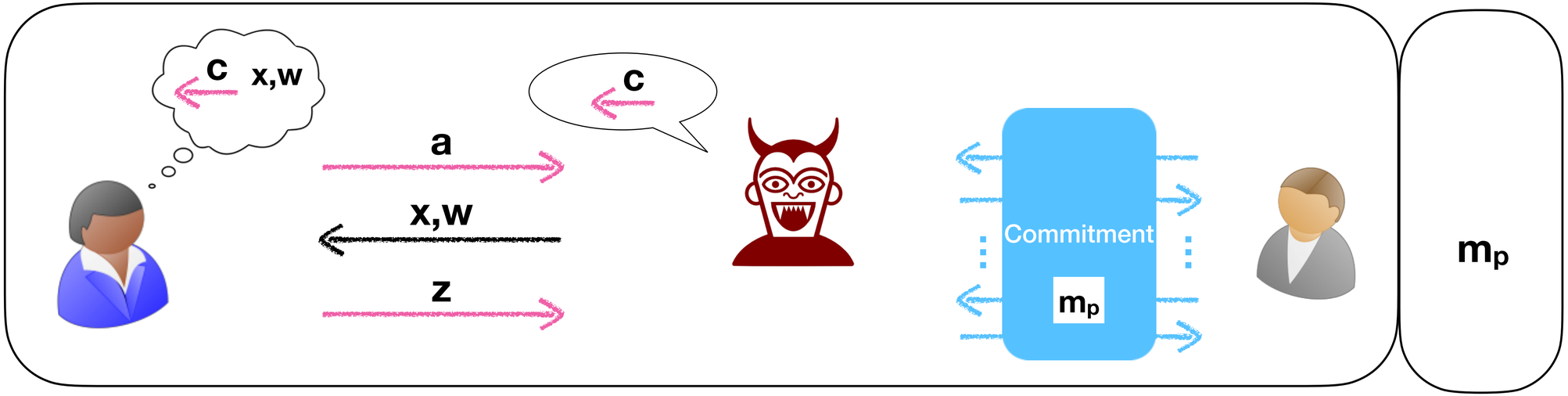
$\approx$

$\mathcal{D}_{HVZK}(view)$



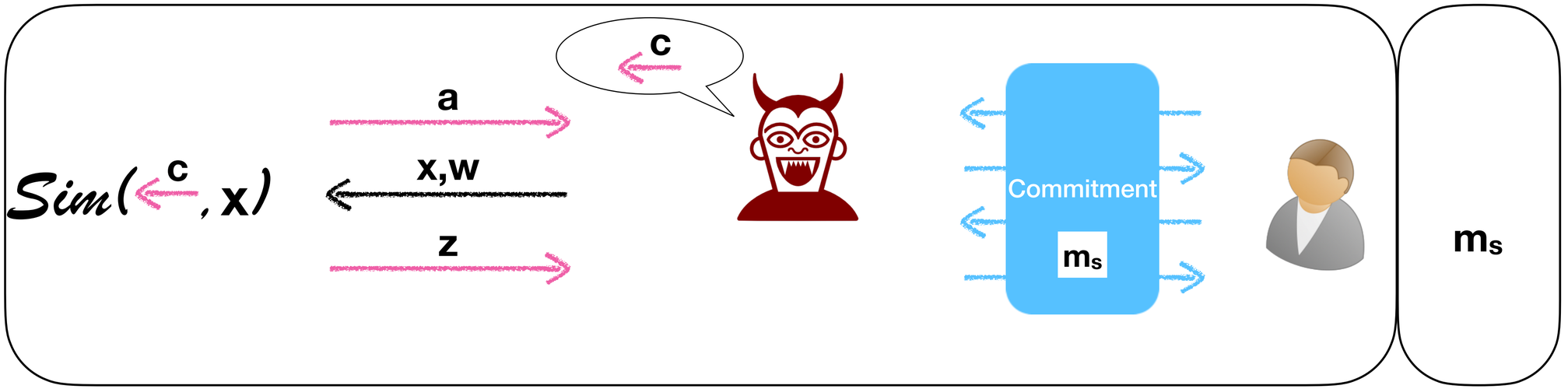
$Sim(\overleftarrow{c}, x)$

Honest verifier zero-knowledge with respect to commitments (HVZK**C**)

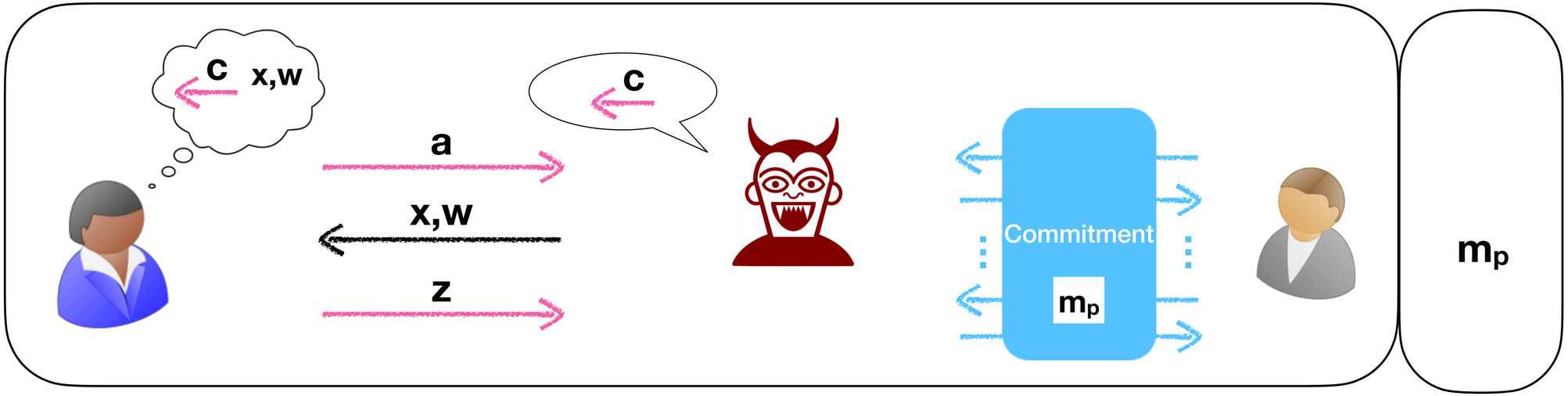


$\approx$

$\mathcal{D}_{\text{HVZK}}(\text{view})$



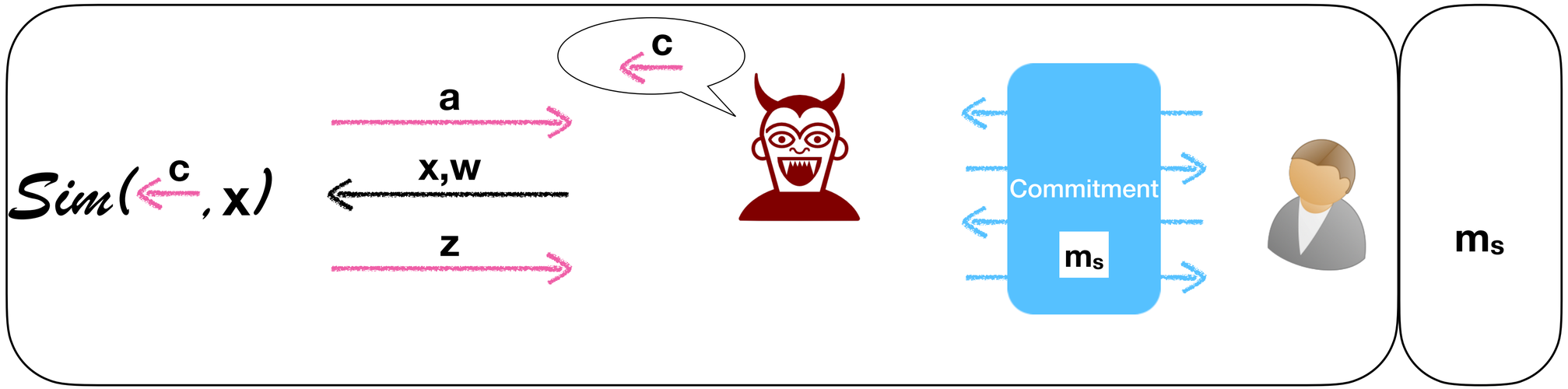
Honest verifier zero-knowledge with respect to commitments (HVZK**C**)



≈

$\mathcal{D}_{HVZK}(view)$

$\mathcal{D}_{HVZKC}(view,m)$



HVZK**C** is Not Implied by Honest verifier zero-knowledge

HVZK**C** is Not Implied by Honest verifier zero-knowledge

- Our work: HVZK with respect to *extractable commitments*

HVZK**C** is Not Implied by Honest verifier zero-knowledge

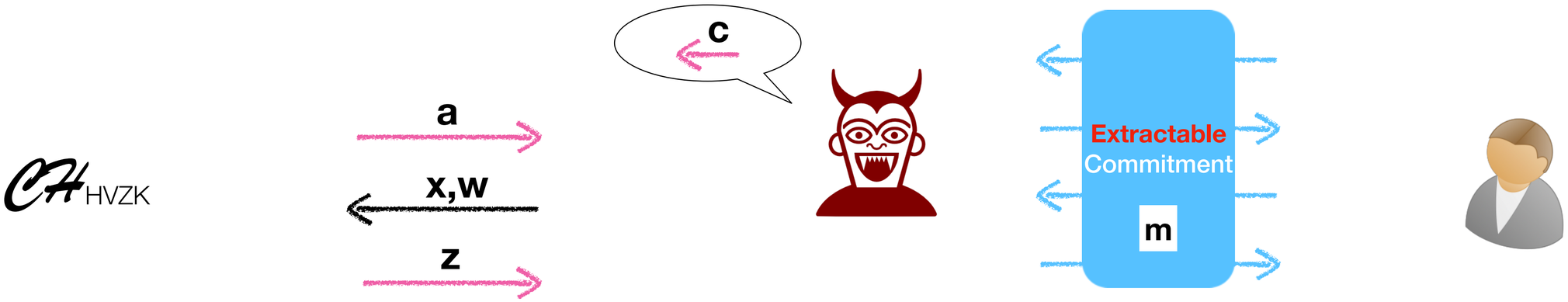
- Our work: HVZK with respect to *extractable commitments*
- If we have an adversary that breaks HVZK**C** then we can construct an adversary that breaks HVZK

HVZK**C** is Not Implied by Honest verifier zero-knowledge

- Our work: HVZK with respect to *extractable commitments*
- If we have an adversary that breaks HVZK**C** then we can construct an adversary that breaks HVZK
- $\mathcal{CH}_{\text{HVZK}}$: generates a transcript either using the prover procedure or using the simulator

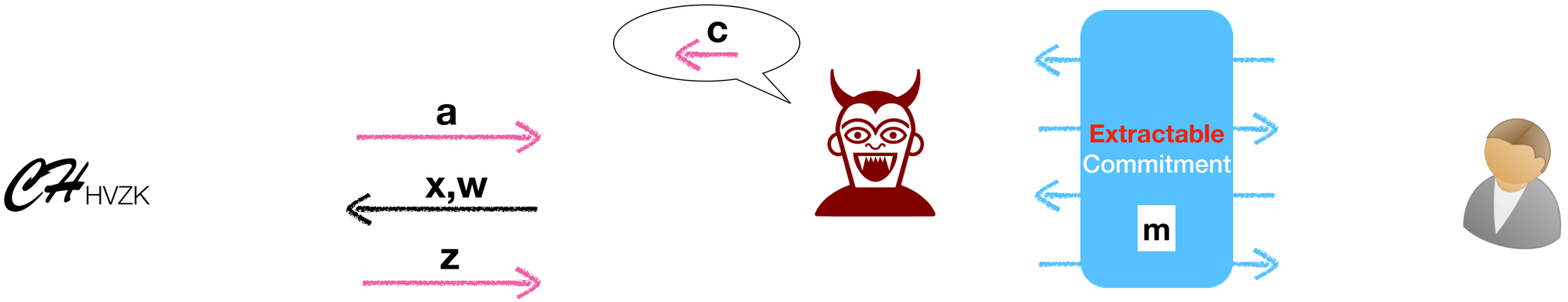
HVZK**C** is Not Implied by Honest verifier zero-knowledge

- Our work: HVZK with respect to *extractable commitments*
- If we have an adversary that breaks HVZK**C** then we can construct an adversary that breaks HVZK
- $\mathcal{CH}_{\text{HVZK}}$: generates a transcript either using the prover procedure or using the simulator



HVZK**C** is Not Implied by Honest verifier zero-knowledge

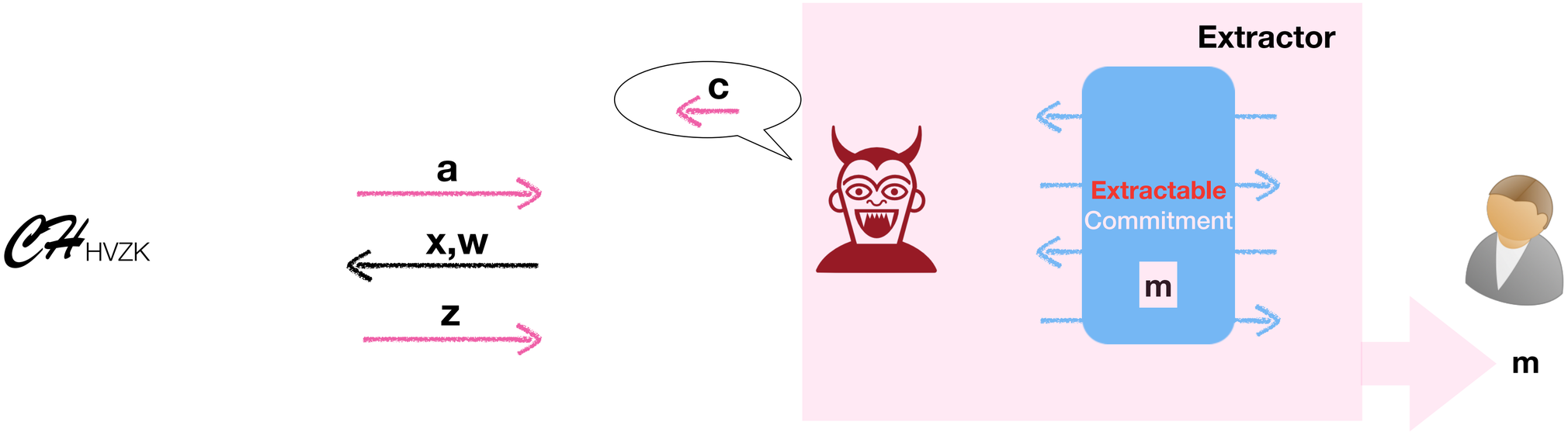
- Our work: HVZK with respect to *extractable commitments*
- If we have an adversary that breaks HVZK**C** then we can construct an adversary that breaks HVZK
- $\mathcal{CH}_{\text{HVZK}}$: generates a transcript either using the prover procedure or using the simulator



$\mathcal{D}_{\text{HVZK}\mathbf{C}}(\text{view},?)$

HVZK**C** is Not Implied by Honest verifier zero-knowledge

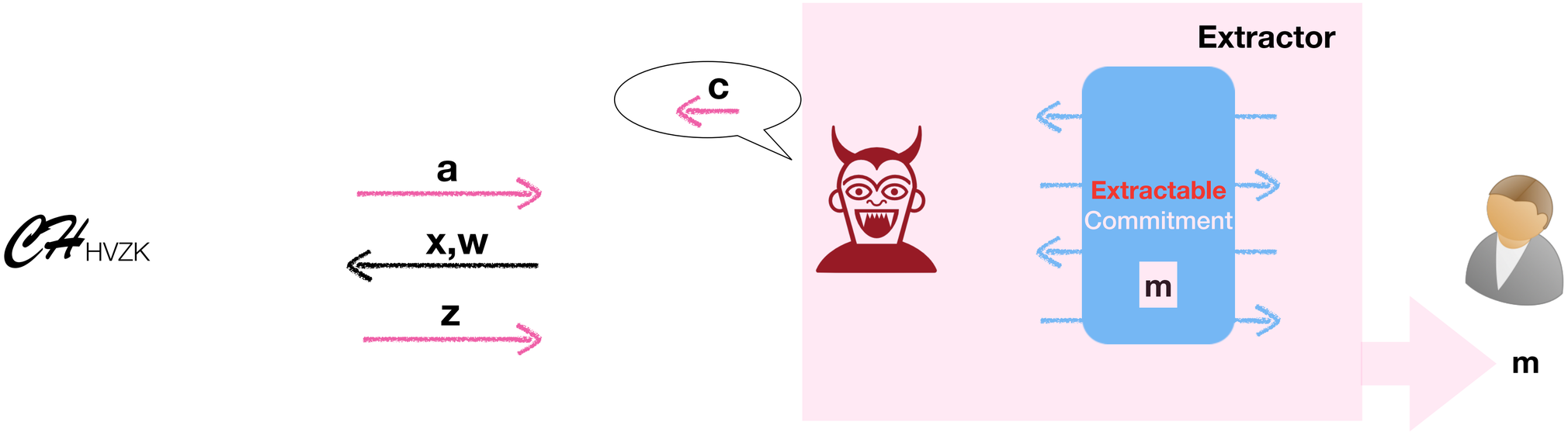
- Our work: HVZK with respect to *extractable commitments*
- If we have an adversary that breaks HVZK**C** then we can construct an adversary that breaks HVZK
- $\mathcal{CH}_{\text{HVZK}}$: generates a transcript either using the prover procedure or using the simulator



$\mathcal{D}_{\text{HVZK}\mathbf{C}}(\text{view},?)$

HVZK**C** is Not Implied by Honest verifier zero-knowledge

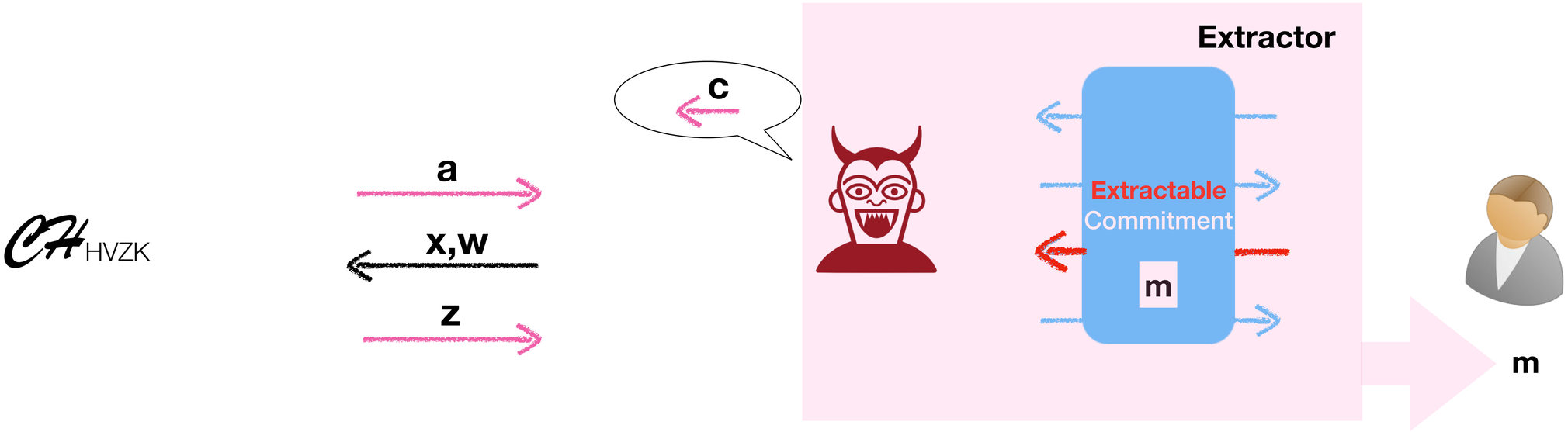
- Our work: HVZK with respect to *extractable commitments*
- If we have an adversary that breaks HVZK**C** then we can construct an adversary that breaks HVZK
- $\mathcal{CH}_{\text{HVZK}}$: generates a transcript either using the prover procedure or using the simulator



$\mathcal{D}_{\text{HVZKC}}(\text{view}, \mathbf{m})$

HVZK**C** is Not Implied by Honest verifier zero-knowledge

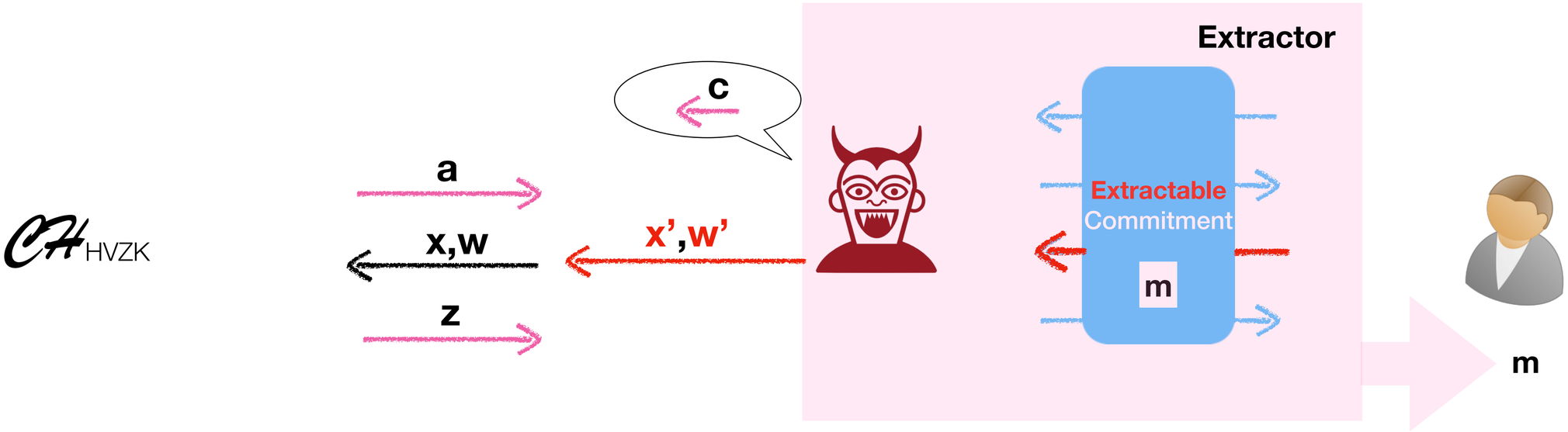
- Our work: HVZK with respect to *extractable commitments*
- If we have an adversary that breaks HVZK**C** then we can construct an adversary that breaks HVZK
- $\mathcal{CH}_{\text{HVZK}}$: generates a transcript either using the prover procedure or using the simulator



$\mathcal{D}_{\text{HVZK}^{\mathbf{C}}}(\text{view}, \mathbf{m})$

HVZK**C** is Not Implied by Honest verifier zero-knowledge

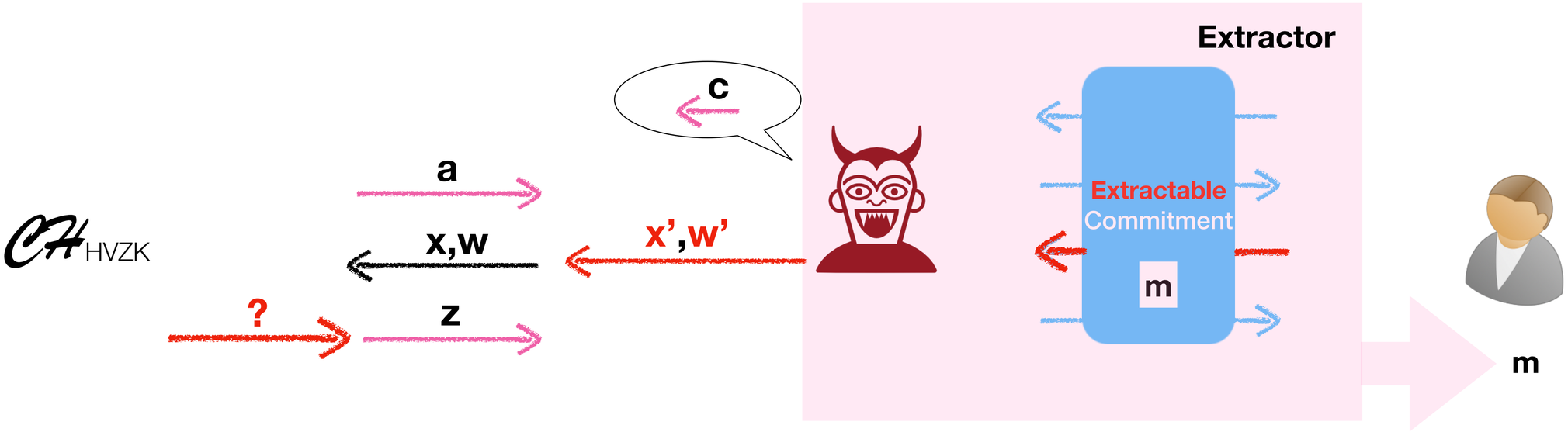
- Our work: HVZK with respect to *extractable commitments*
- If we have an adversary that breaks HVZK**C** then we can construct an adversary that breaks HVZK
- $\mathcal{CH}_{\text{HVZK}}$: generates a transcript either using the prover procedure or using the simulator



$\mathcal{D}_{\text{HVZKC}}(\text{view}, \mathbf{m})$

HVZK**C** is Not Implied by Honest verifier zero-knowledge

- Our work: HVZK with respect to *extractable commitments*
- If we have an adversary that breaks HVZK**C** then we can construct an adversary that breaks HVZK
- $\mathcal{CH}_{\text{HVZK}}$: generates a transcript either using the prover procedure or using the simulator



$\mathcal{D}_{\text{HVZKC}}(\text{view}, \mathbf{m})$

Our HVZK**C** Scheme

[BMR90]

MPC

Preprocessing

Online phase

[BMR90] Donald Beaver, Silvio Micali, and Phillip Rogaway. STOC 1990

Our HVZK**C** Scheme

[BMR90]

MPC

Preprocessing

Online phase

+

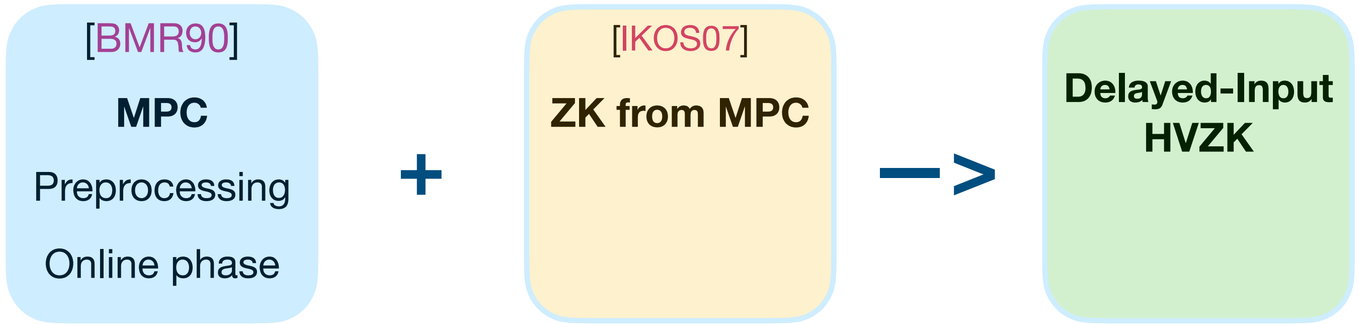
[IKOS07]

ZK from MPC

[BMR90] Donald Beaver, Silvio Micali, and Phillip Rogaway. STOC 1990

[IKOS07] Yuval Ishai, Eyal Kushilevitz, Rafail Ostrovsky, and Amit Sahai. STOC 2007

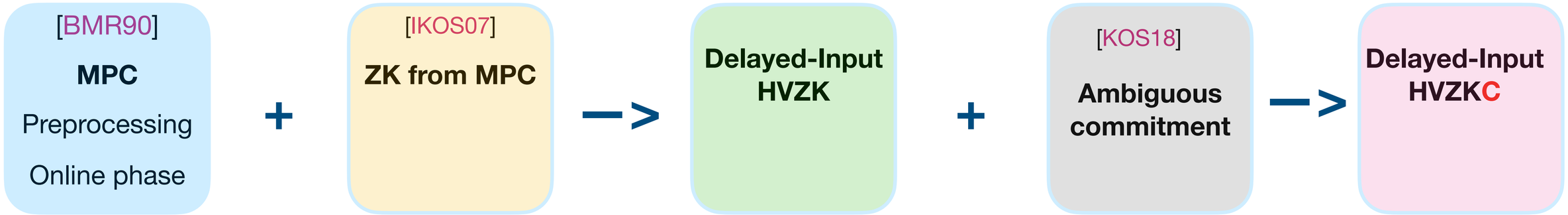
Our HVZK**C** Scheme



[BMR90] Donald Beaver, Silvio Micali, and Phillip Rogaway. STOC 1990

[IKOS07] Yuval Ishai, Eyal Kushilevitz, Rafail Ostrovsky, and Amit Sahai. STOC 2007

Our HVZKC Scheme



[BMR90] Donald Beaver, Silvio Micali, and Phillip Rogaway. STOC 1990

[IKOS07] Yuval Ishai, Eyal Kushilevitz, Rafail Ostrovsky, and Amit Sahai. STOC 2007

[KOS18] Dakshita Khurana, Rafail Ostrovsky, and Akshayaram Srinivasan. TCC 2018

Conclusions and Open Questions

Conclusions and Open Questions

- Delayed-input BB HVZK**C** from the BMR protocol
- The weak-non-malleable commitment needs to be modified
- Rewind security may be unnecessarily strong for some applications

Conclusions and Open Questions

- Delayed-input BB HVZK**C** from the BMR protocol
- The weak-non-malleable commitment needs to be modified
- Rewind security may be unnecessarily strong for some applications
- Open problems
  - Concrete efficiency using OWFs
  - 3-round non-malleable commitments with BB use of OWFs
  - Extension to the many-many setting

Thanks

https://ia.cr/2022/1543