Black-Box (and Fast) Non-Malleable Zero Knowledge

Vincenzo Botta
Sapienza University

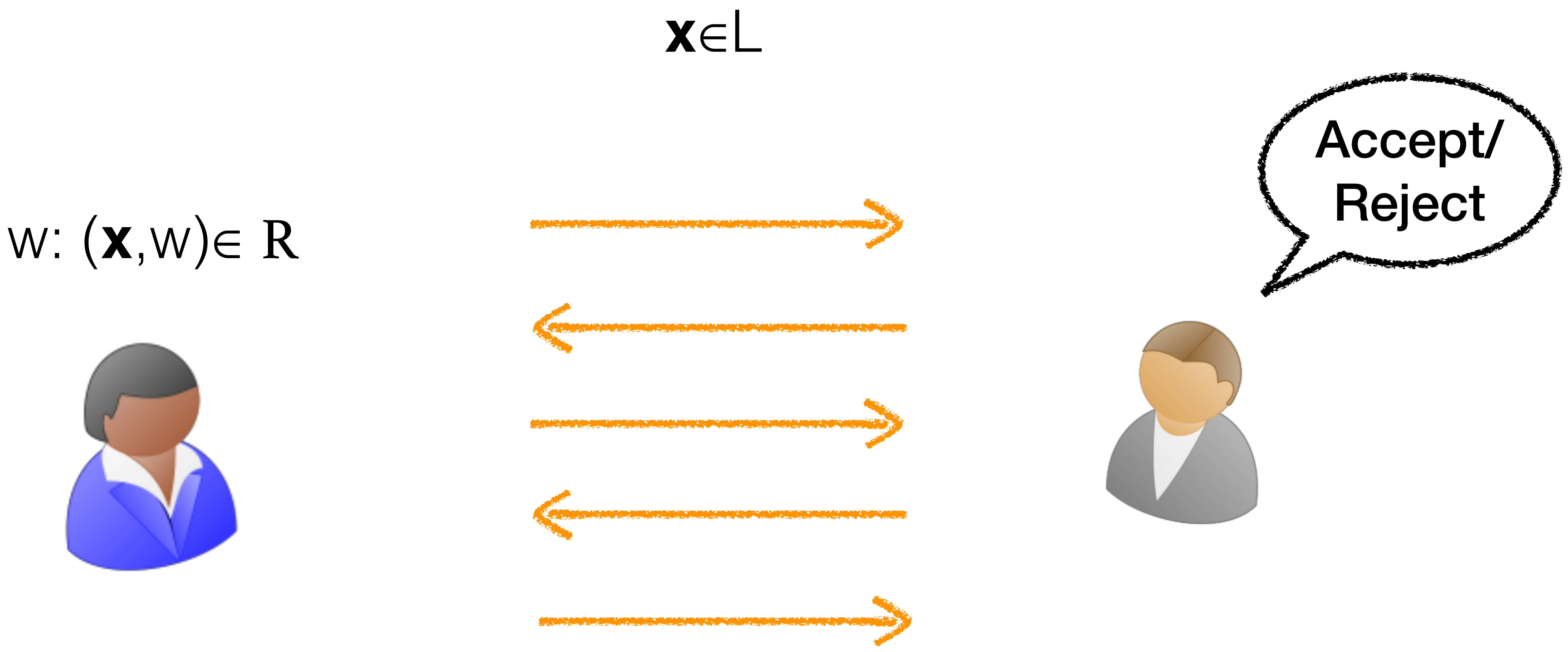
Emmanuela Orsini
Bocconi University

Ivan Visconti
University of Salerno

Michele Ciampi
The University of Edinburgh

Luisa Siniscalchi
Danish Technical University

Zero-knowledge proofs

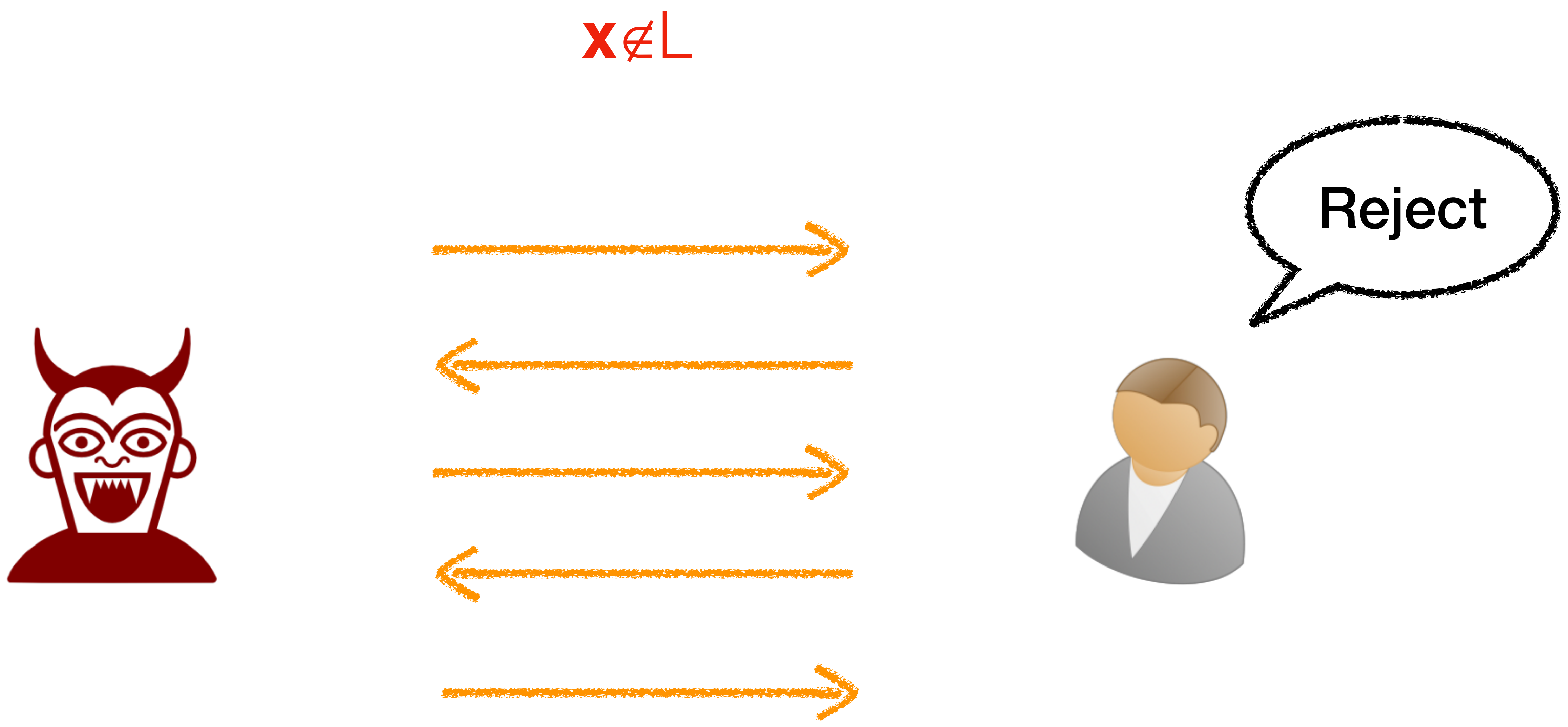


Completeness

Soundness

Zero-knowledge

Zero-knowledge proofs



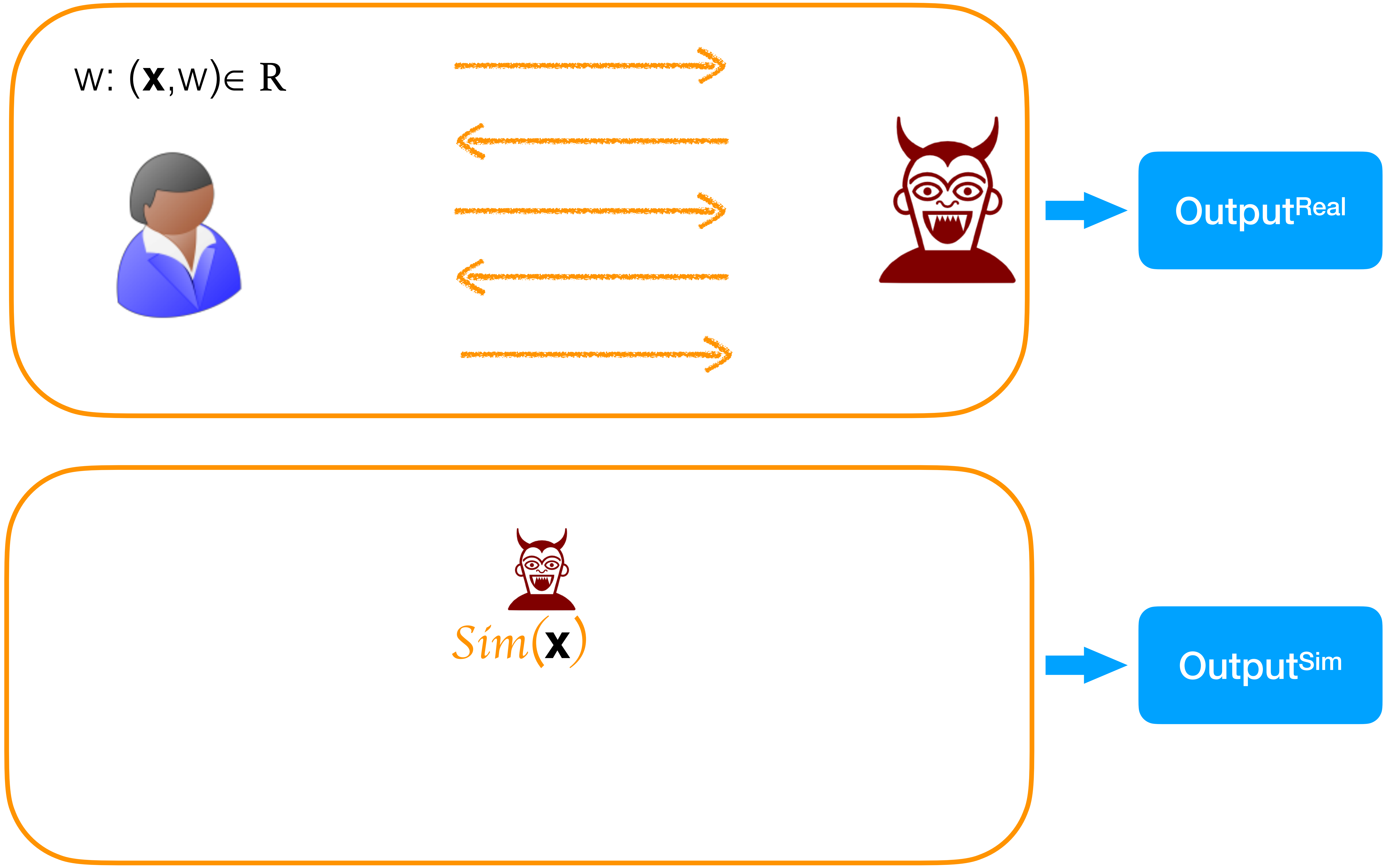
Completeness

Soundness

Zero-knowledge

Zero-knowledge proofs

$\mathbf{x} \in L$

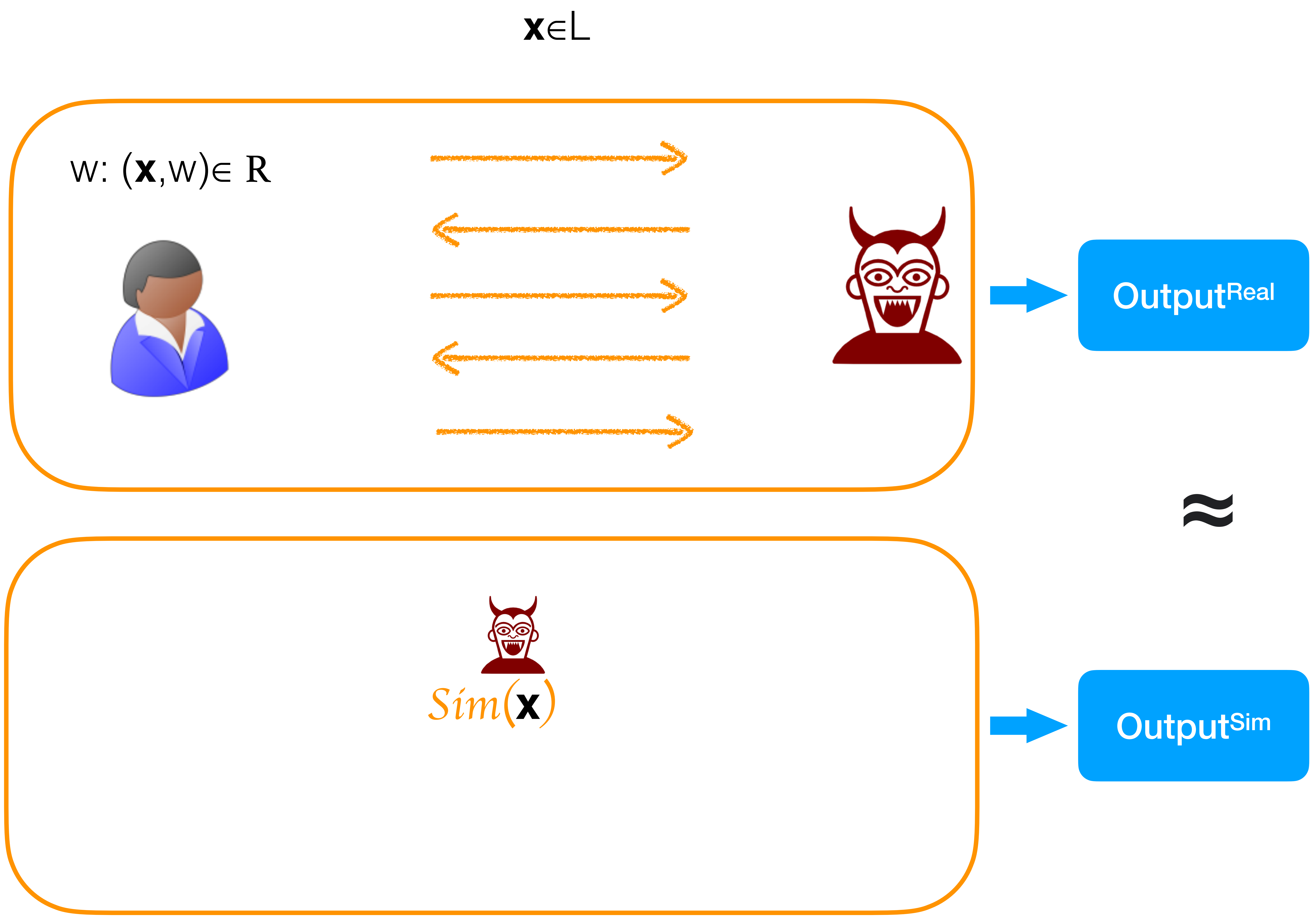


Completeness

Soundness

Zero-knowledge

Zero-knowledge proofs



Completeness

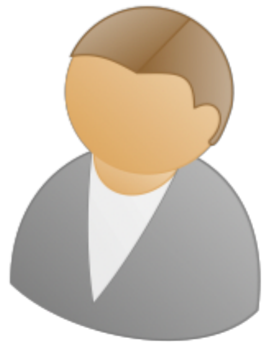
Soundness

Zero-knowledge

Non-malleable zero-knowledge

$\mathbf{x} \in L$ $\mathbf{x'} \in L$

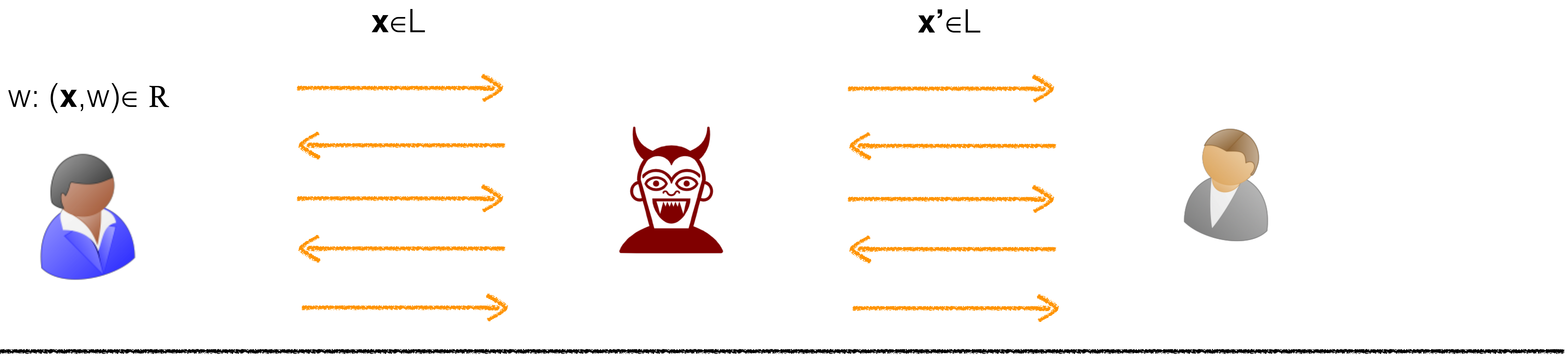
w: $(\mathbf{x}, w) \in R$



Non-malleable zero-knowledge

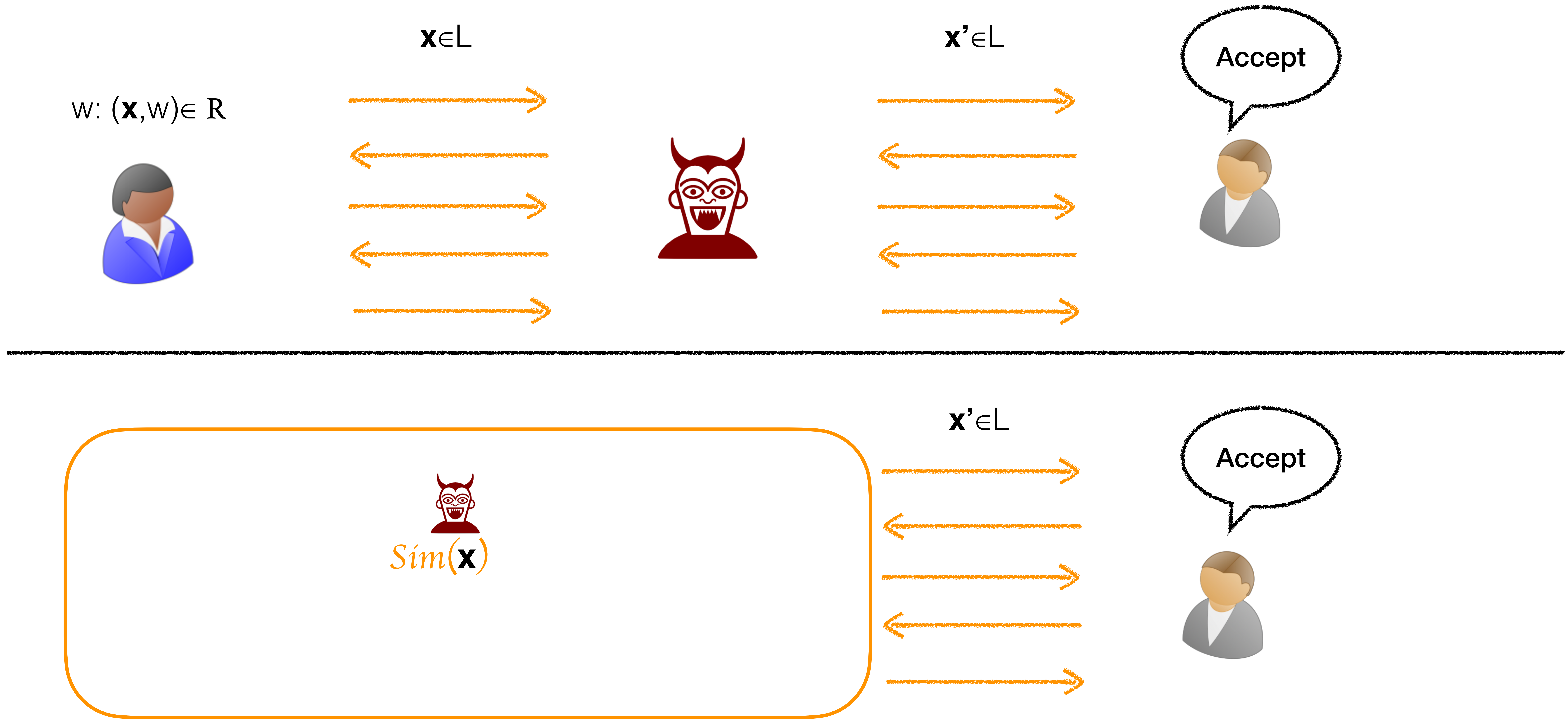
Non-malleable zero-knowledge

Non-malleable zero-knowledge



Non-malleable zero-knowledge

Non-malleable zero-knowledge



State of the art

Black-box simulation
Plain model (no RO, no setup)
Minicrypt
Constant-round
Black-box use of primitives

Constant round NMZK from one-way functions

State of the art

Black-box simulation
Plain model (no RO, no setup)
Minicrypt
Constant-round
Black-box use of primitives

Constant round NMZK from one-way functions

Theoretical

[DDN91] Danny Dolev, Cynthia Dwork, and Moni Naor. Non-malleable cryptography (extended abstract). STOC 1991.
[Bar02] Boaz Barak. Constant-round coin-tossing with a man in the middle or realizing the shared random string model. FOCS 2002
[PR05] Rafael Pass and Alon Rosen. New and improved constructions of non-malleable cryptographic protocols. STOC 2005
[Wee10] Hoeteck Wee. Black-box, round-efficient secure computation via non-malleability amplification. FOCS 2010.
[LP11] Huijia Lin and Rafael Pass. Constant-round non-malleable commitments from any one-way function. STOC 2011.
[Goy11] Constant round non-malleable protocols using one-way functions. STOC 2011.
[GRRV14] Vipul Goyal, Silas Richelson, Alon Rosen, and Margarita Vald. An algebraic approach to non-malleability. FOCS 2014.

State of the art

Black-box simulation
Plain model (no RO, no setup)
Minicrypt
Constant-round
Black-box use of primitives

Constant round NMZK from one-way functions

Theoretical

[DDN91] Danny Dolev, Cynthia Dwork, and Moni Naor. Non-malleable cryptography (extended abstract). STOC 1991.
[Bar02] Boaz Barak. Constant-round coin-tossing with a man in the middle or realizing the shared random string model. FOCS 2002
[PR05] Rafael Pass and Alon Rosen. New and improved constructions of non-malleable cryptographic protocols. STOC 2005
[Wee10] Hoeteck Wee. Black-box, round-efficient secure computation via non-malleability amplification. FOCS 2010.
[LP11] Huijia Lin and Rafael Pass. Constant-round non-malleable commitments from any one-way function. STOC 2011.
[Goy11] Constant round non-malleable protocols using one-way functions. STOC 2011.
[GRRV14] Vipul Goyal, Silas Richelson, Alon Rosen, and Margarita Vald. An algebraic approach to non-malleability. FOCS 2014.

Non-BB protocols

State of the art

Black-box simulation
Plain model (no RO, no setup)
Minicrypt
Constant-round
Black-box use of primitives

Constant round NMZK from one-way functions

Theoretical

[DDN91] Danny Dolev, Cynthia Dwork, and Moni Naor. Non-malleable cryptography (extended abstract). STOC 1991.
[Bar02] Boaz Barak. Constant-round coin-tossing with a man in the middle or realizing the shared random string model. FOCS 2002
[PR05] Rafael Pass and Alon Rosen. New and improved constructions of non-malleable cryptographic protocols. STOC 2005
[Wee10] Hoeteck Wee. Black-box, round-efficient secure computation via non-malleability amplification. FOCS 2010.
[LP11] Huijia Lin and Rafael Pass. Constant-round non-malleable commitments from any one-way function. STOC 2011.
[Goy11] Constant round non-malleable protocols using one-way functions. STOC 2011.
[GRRV14] Vipul Goyal, Silas Richelson, Alon Rosen, and Margarita Vald. An algebraic approach to non-malleability. FOCS 2014.

Non-BB protocols

Practical

[KLP22] Allen Kim, Xiao Liang, and Omkant Pandey. A new approach to efficient non-malleable zero-knowledge. CRYPTO 2022

	Rounds	BB use of primitives	SHA-256 preimage Computation	SHA-256 preimage Communication
[KLP22]	>20	non-BB	1680ms	20MB

State of the art

Black-box simulation
Plain model (no RO, no setup)
Minicrypt
Constant-round
Black-box use of primitives

Constant round NMZK from one-way functions

Theoretical

[DDN91] Danny Dolev, Cynthia Dwork, and Moni Naor. Non-malleable cryptography (extended abstract). STOC 1991.
[Bar02] Boaz Barak. Constant-round coin-tossing with a man in the middle or realizing the shared random string model. FOCS 2002
[PR05] Rafael Pass and Alon Rosen. New and improved constructions of non-malleable cryptographic protocols. STOC 2005
[Wee10] Hoeteck Wee. Black-box, round-efficient secure computation via non-malleability amplification. FOCS 2010.
[LP11] Huijia Lin and Rafael Pass. Constant-round non-malleable commitments from any one-way function. STOC 2011.
[Goy11] Constant round non-malleable protocols using one-way functions. STOC 2011.
[GRRV14] Vipul Goyal, Silas Richelson, Alon Rosen, and Margarita Vald. An algebraic approach to non-malleability. FOCS 2014.

Non-BB protocols

Practical

[KLP22] Allen Kim, Xiao Liang, and Omkant Pandey. A new approach to efficient non-malleable zero-knowledge. CRYPTO 2022

	Rounds	BB use of primitives	SHA-256 preimage	
			Computation	Communication
[KLP22]	>20	non-BB	1680ms	20MB
This work	**9**	**BB**	**100ms**	**5MB**

State of the art

Black-box simulation
Plain model (no RO, no setup)
Minicrypt
Constant-round
Black-box use of primitives

Constant round NMZK from one-way functions

Theoretical

[DDN91] Danny Dolev, Cynthia Dwork, and Moni Naor. Non-malleable cryptography (extended abstract). STOC 1991.
[Bar02] Boaz Barak. Constant-round coin-tossing with a man in the middle or realizing the shared random string model. FOCS 2002
[PR05] Rafael Pass and Alon Rosen. New and improved constructions of non-malleable cryptographic protocols. STOC 2005
[Wee10] Hoeteck Wee. Black-box, round-efficient secure computation via non-malleability amplification. FOCS 2010.
[LP11] Huijia Lin and Rafael Pass. Constant-round non-malleable commitments from any one-way function. STOC 2011.
[Goy11] Constant round non-malleable protocols using one-way functions. STOC 2011.
[GRRV14] Vipul Goyal, Silas Richelson, Alon Rosen, and Margarita Vald. An algebraic approach to non-malleability. FOCS 2014.

Non-BB protocols

Practical

[KLP22] Allen Kim, Xiao Liang, and Omkant Pandey. A new approach to efficient non-malleable zero-knowledge. CRYPTO 2022

	Rounds	BB use of primitives	SHA-256 preimage Computation	SHA-256 preimage Communication
[KLP22]	>20	non-BB	1680ms	20MB
This work	**9**	**BB**	**100ms**	**5MB**

The first BB protocol

Non-malleable commitment

w.r.t. commitment

Non-malleable commitment

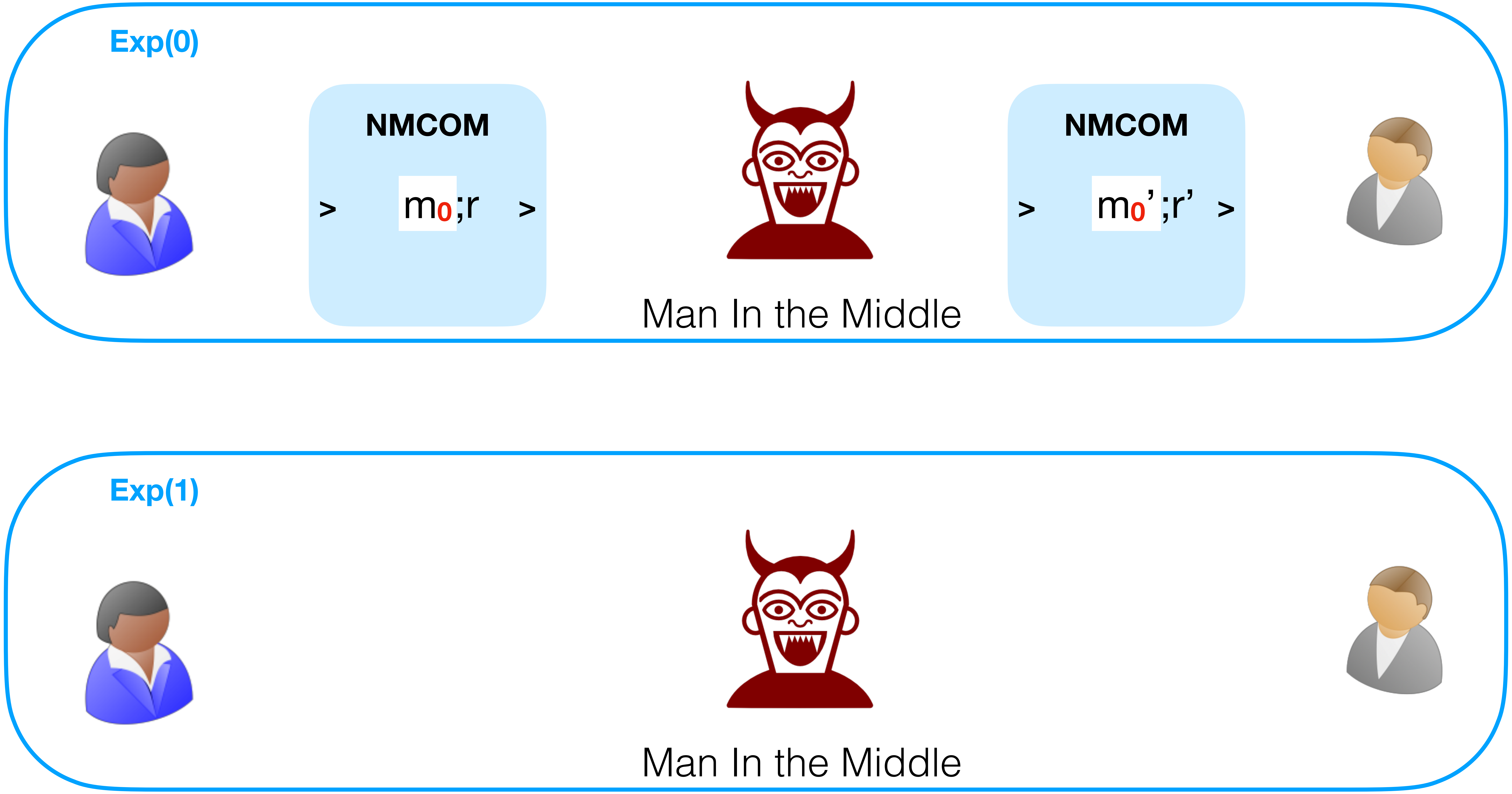
w.r.t. commitment

Non-malleable commitment

w.r.t. commitment

Non-malleable commitment

w.r.t. commitment



Non-malleable commitment

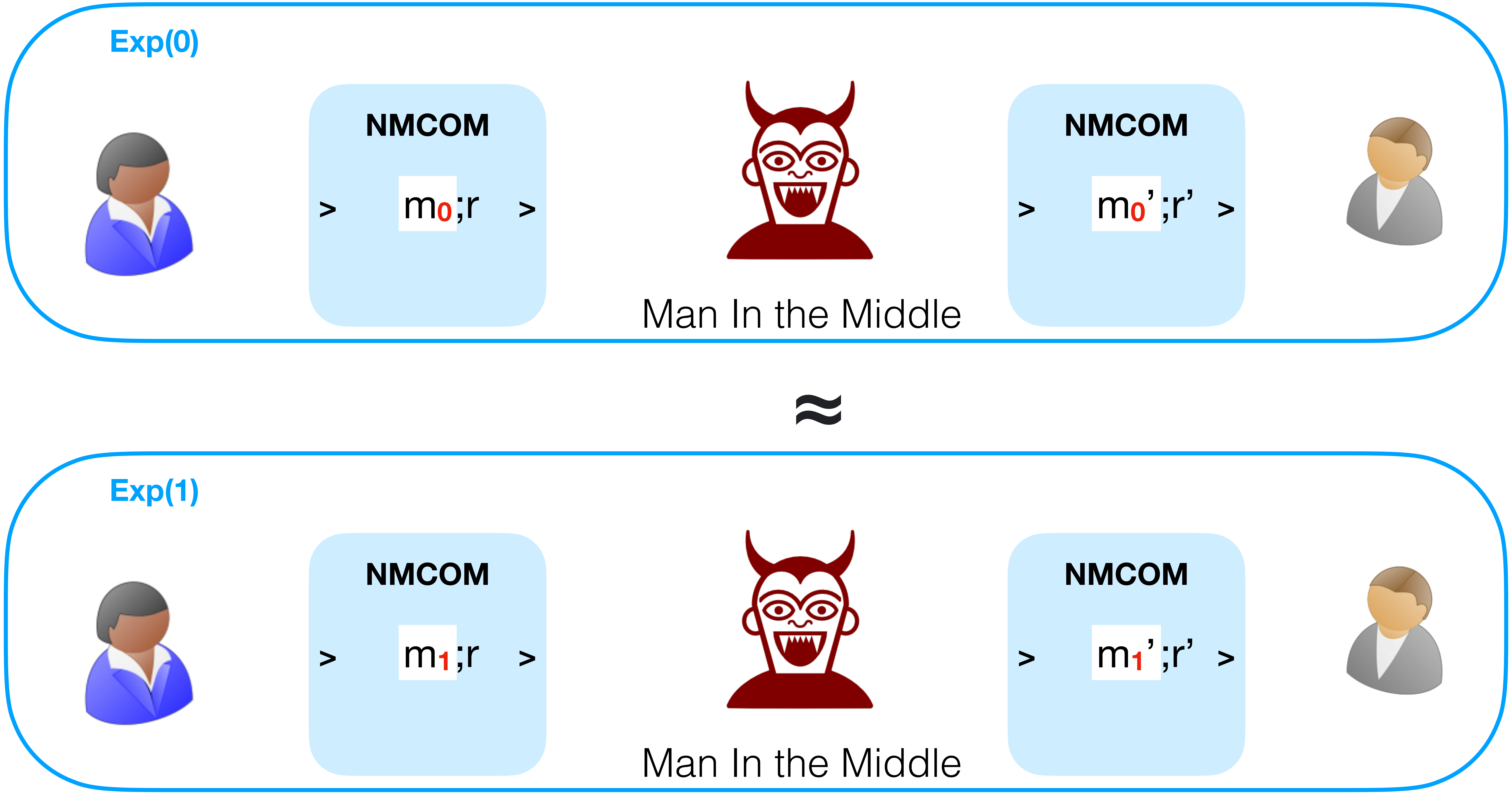
w.r.t. commitment

Non-malleable commitment

w.r.t. commitment

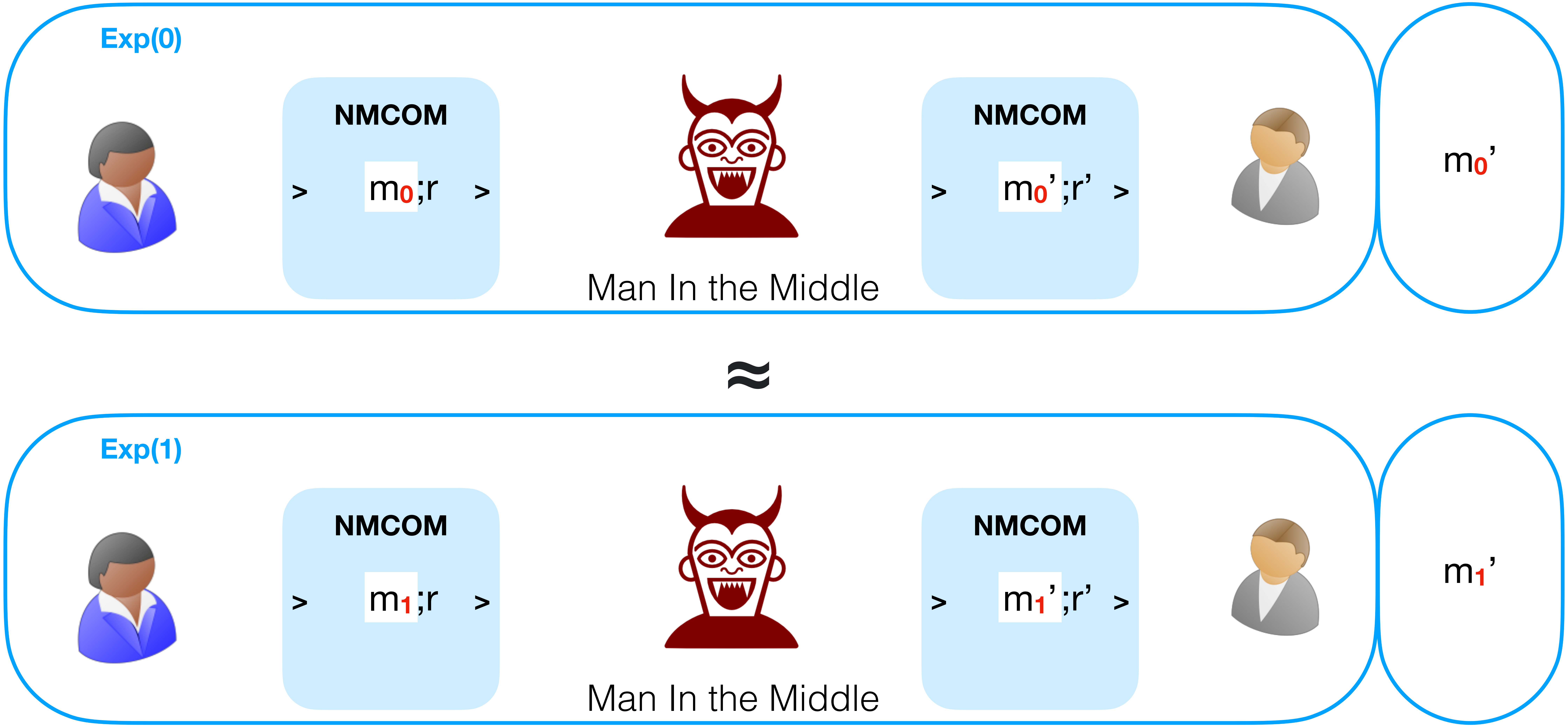
Non-malleable commitment

w.r.t. commitment

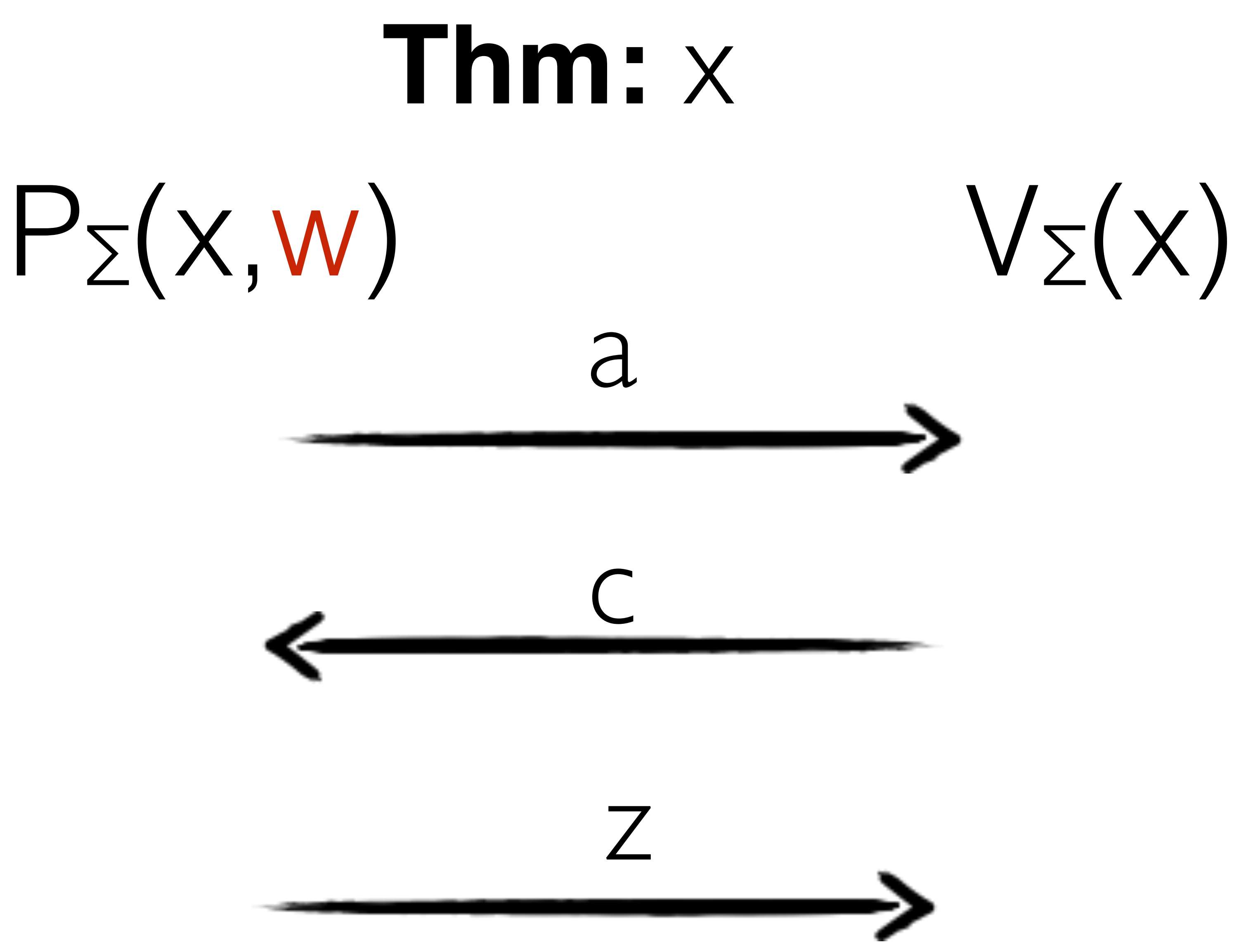


Non-malleable commitment

w.r.t. commitment

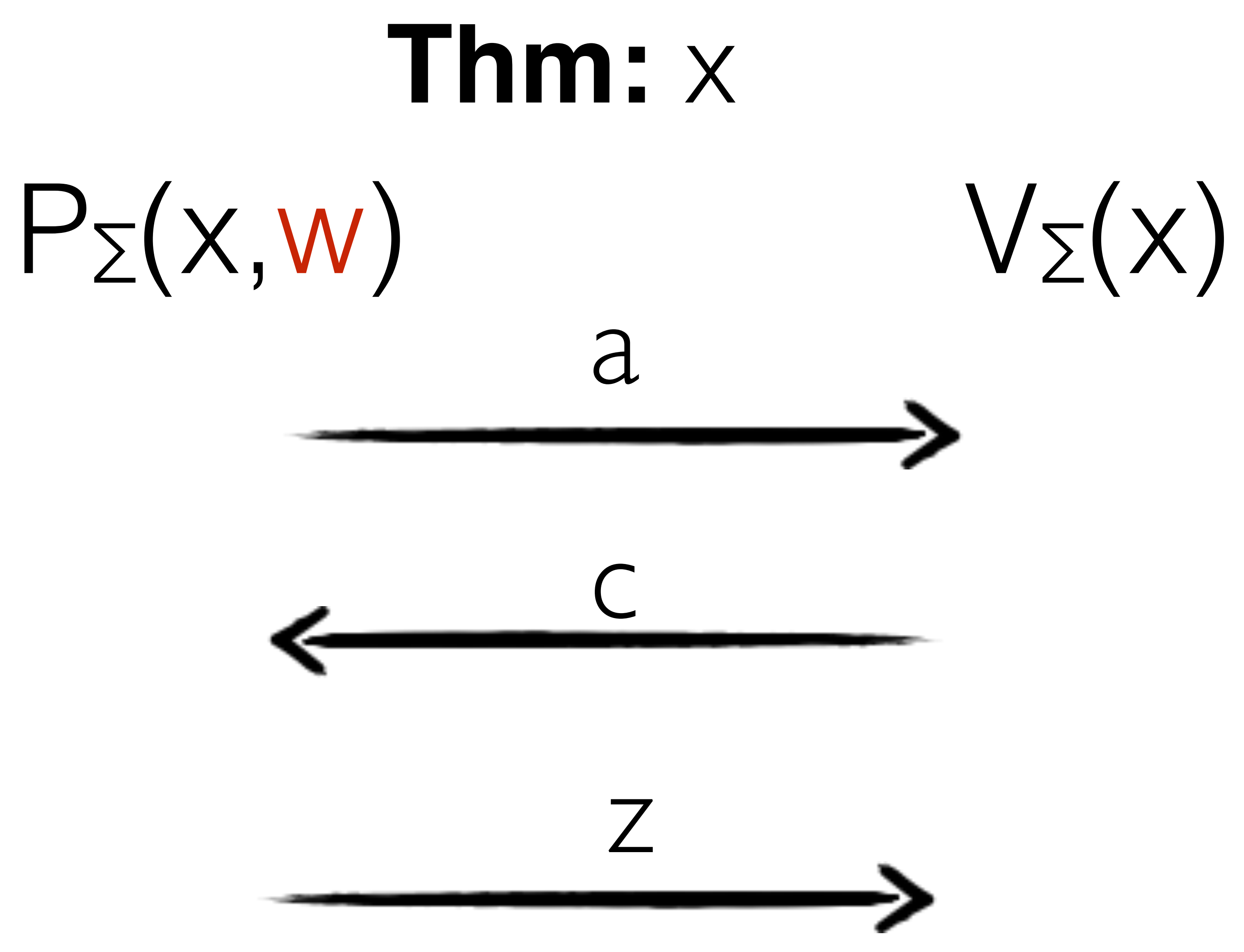


Sigma protocols



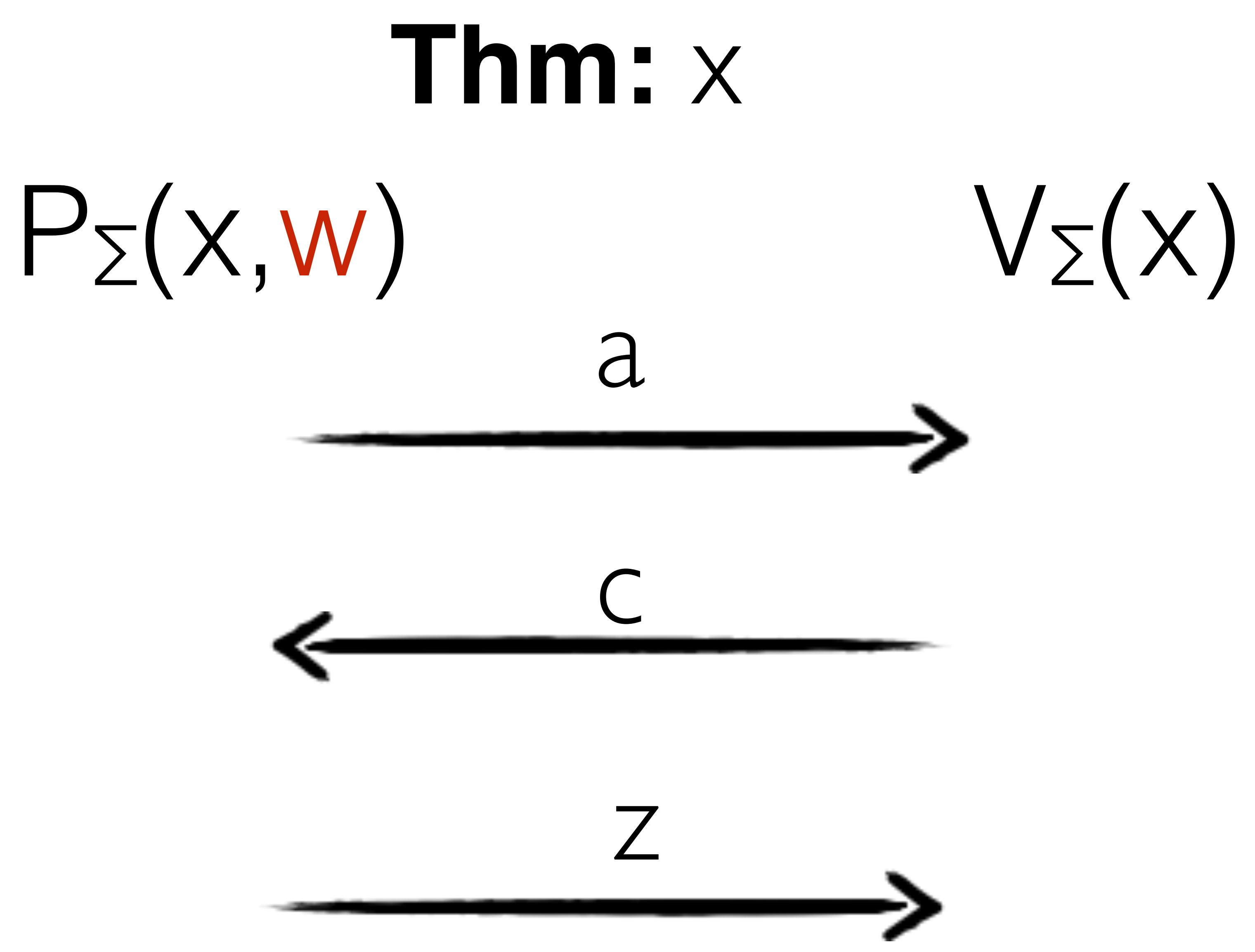
Sigma protocols

- Completeness



Sigma protocols

- Completeness
- Honest Verifier Zero-Knowledge $\mathcal{HVZK}_{Sim}(x) \Longrightarrow$



Sigma protocols

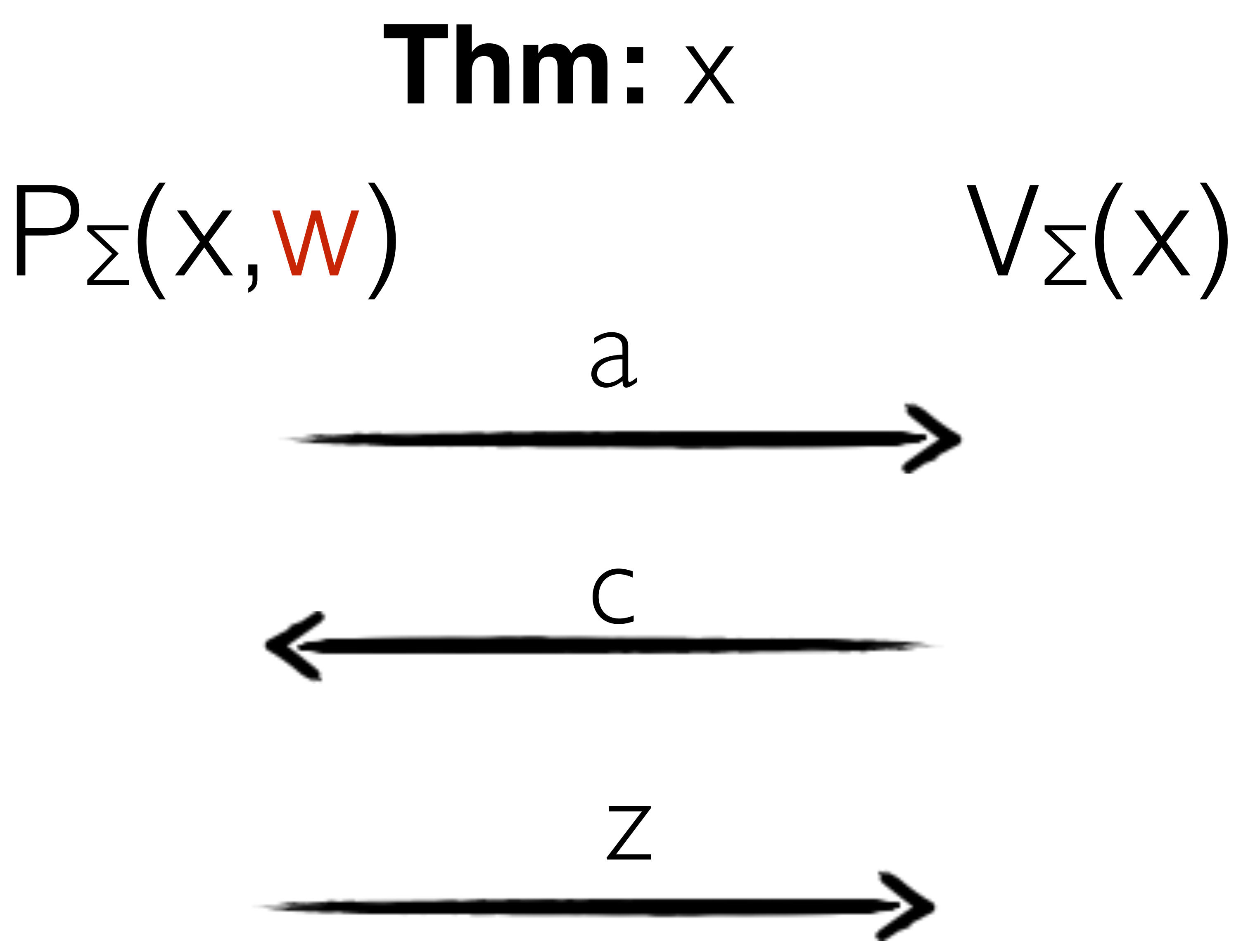
- Completeness

- Honest Verifier Zero-Knowledge $\mathcal{HVZK}_{Sim}(x) \Longrightarrow$

a'

c'

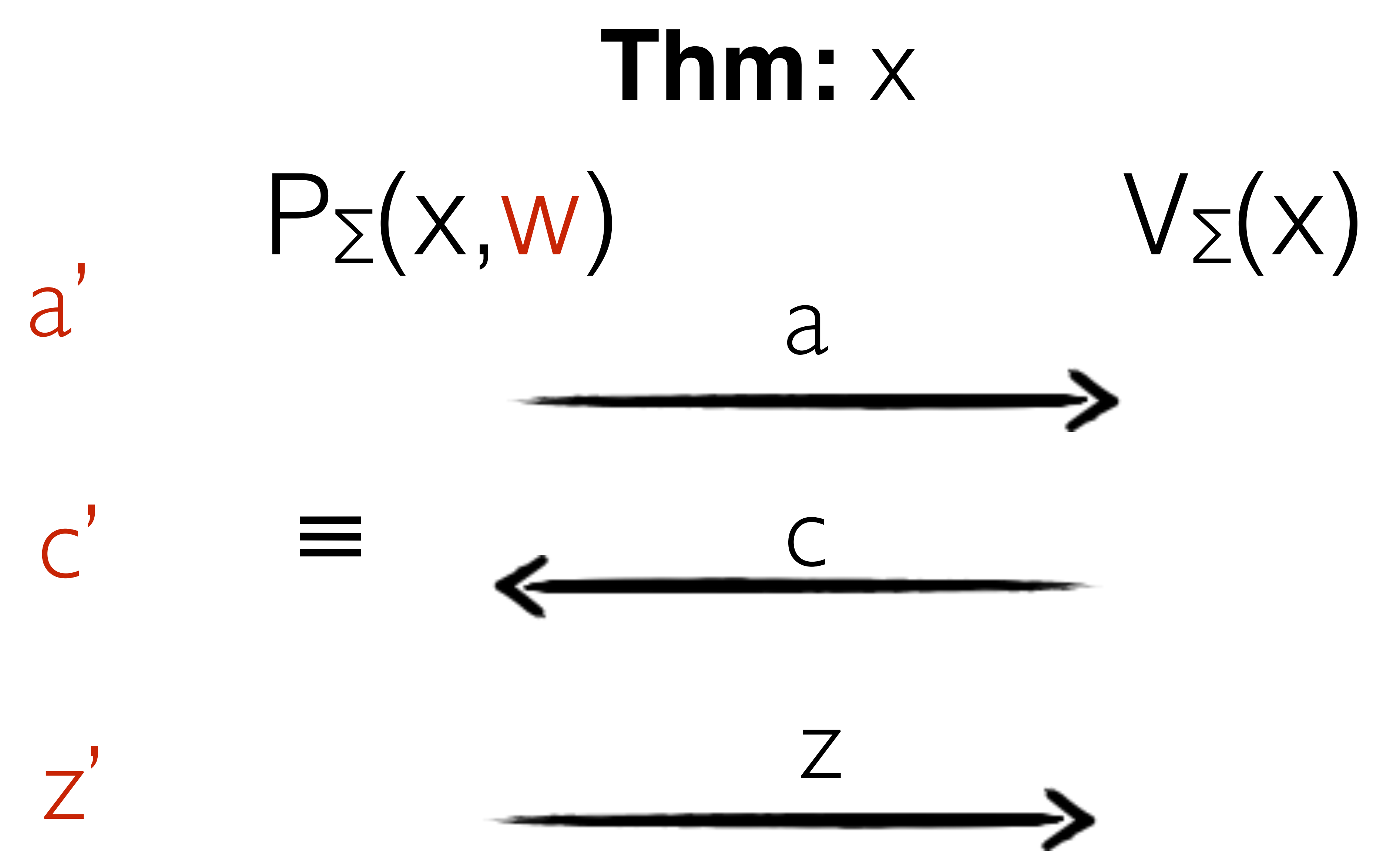
z'



Sigma protocols

- Completeness

- Honest Verifier Zero-Knowledge $\mathcal{HVZK}_{Sim}(x) \Longrightarrow$



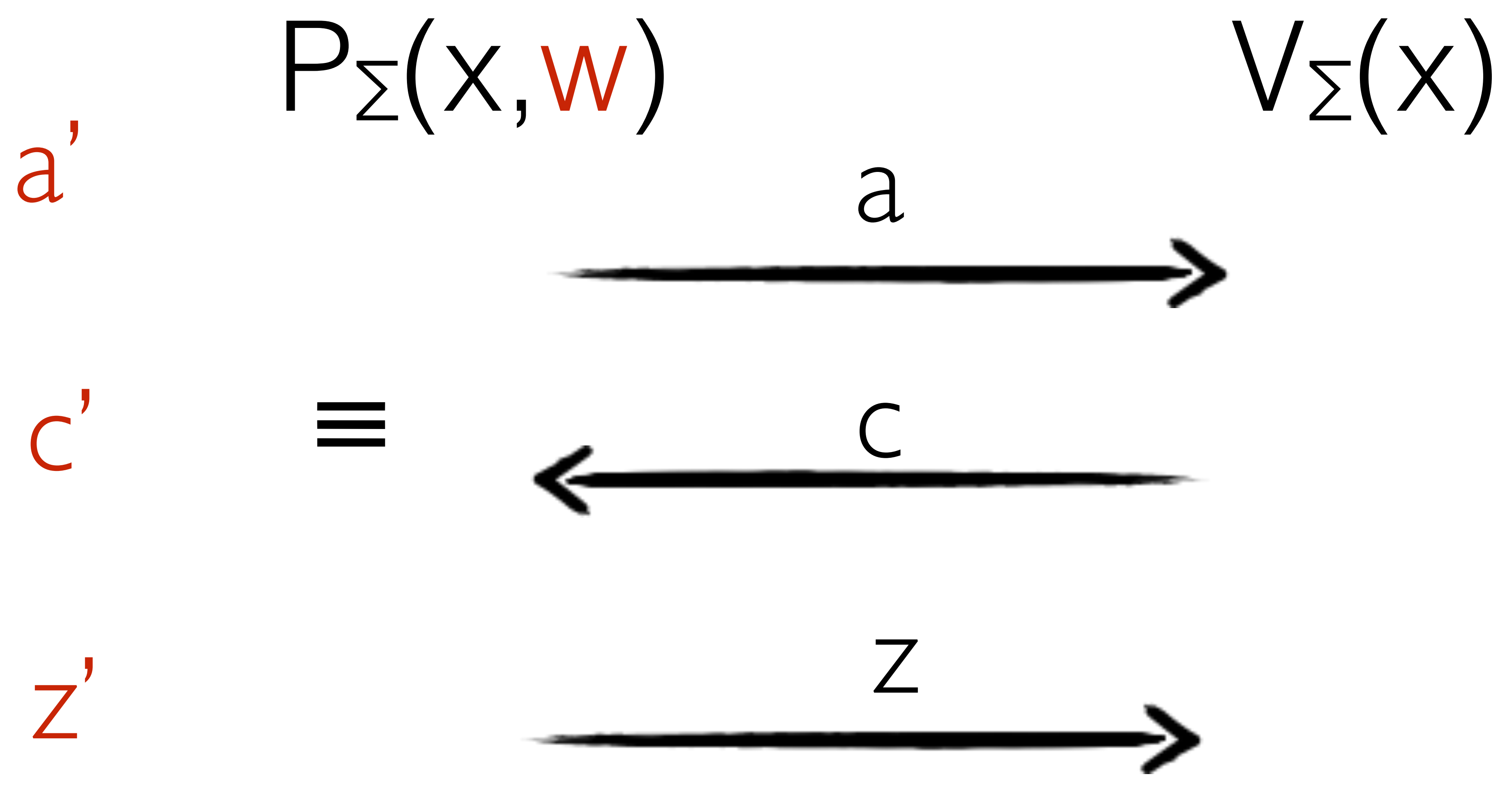
Sigma protocols

- Completeness

- Honest Verifier Zero-Knowledge $\mathcal{HVZK}_{Sim}(x) \Longrightarrow$

  Special Honest Verifier Zero-Knowledge $\mathcal{SHVZK}_{Sim}(x,c) \Rightarrow$ a',z'

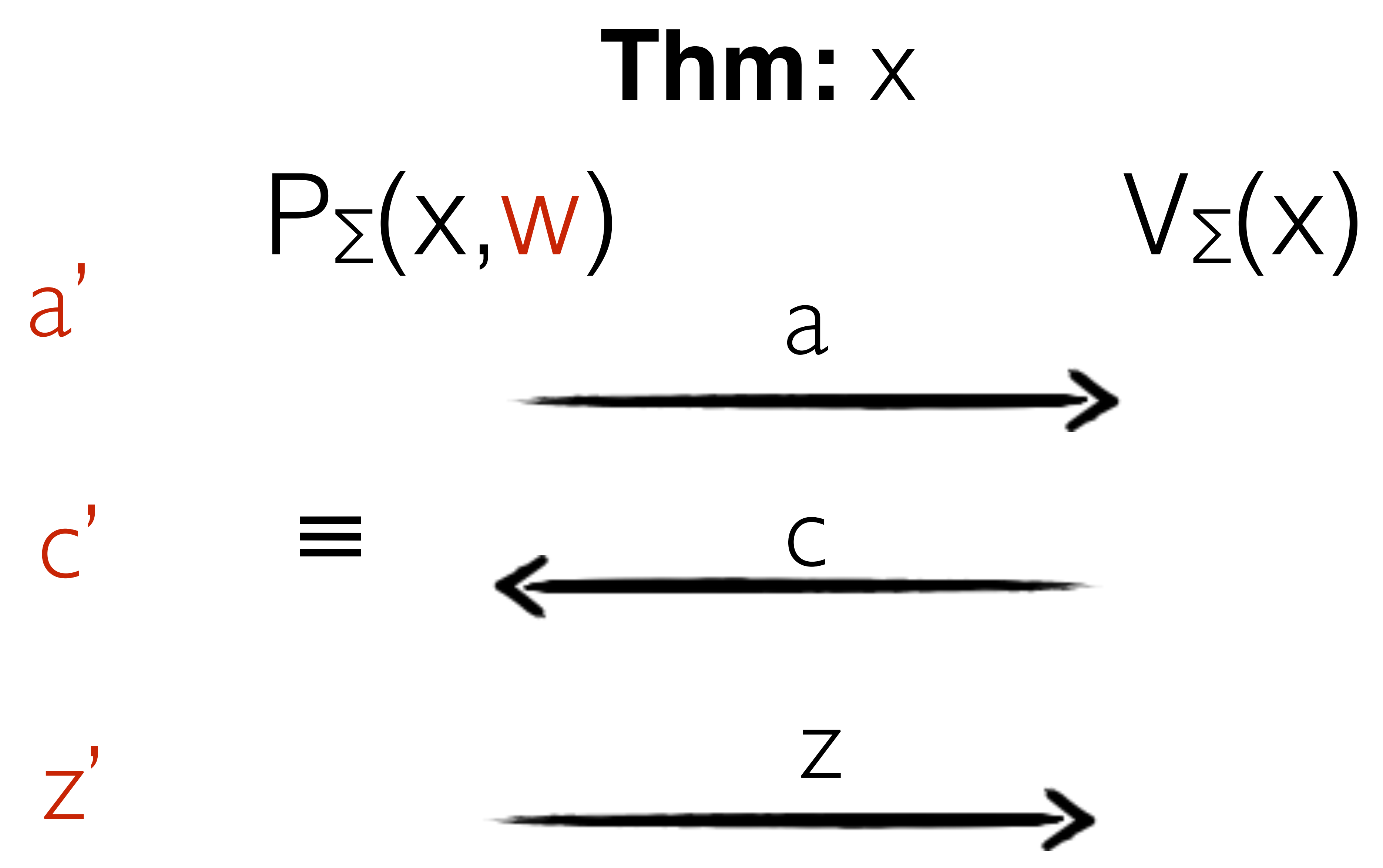
Thm: x



Sigma protocols

- Completeness
- Honest Verifier Zero-Knowledge $\mathcal{HVZK}_{Sim}(x) \Longrightarrow$

  Special Honest Verifier Zero-Knowledge $\mathcal{SHVZK}_{Sim}(x,c) \Rightarrow$ a',z'
- Special Soundness

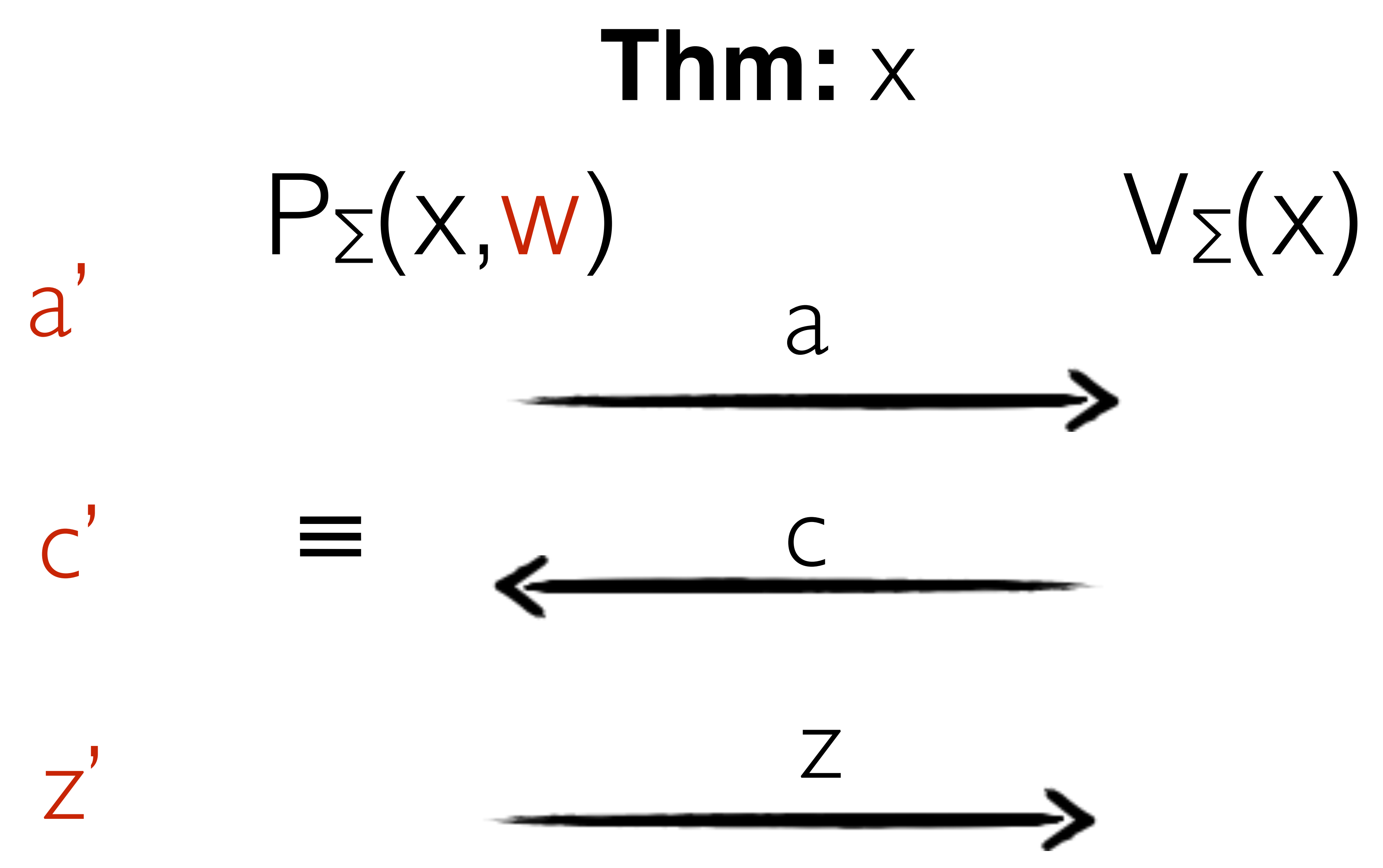


Sigma protocols

- Completeness
- Honest Verifier Zero-Knowledge $\mathcal{HVZK}_{Sim}(x) \Longrightarrow$

  Special Honest Verifier Zero-Knowledge $\mathcal{SHVZK}_{Sim}(x,c) \Rightarrow a', z'$

- Special Soundness



S-Sound Extractor

x, (**a** c z)

x, (**a** c' z')

$c \neq c'$ ⇒ w: (**x**,w)∈ R

Our NMZK Scheme*

$\mathbf{x} \in L$

*[JP14] Abhishek Jain and Omkant Pandey. Non-malleable zero knowledge: Black-box constructions and definitional relationships. SCN 2014

Our NMZK Scheme*

$\mathbf{x} \in L$

$\mathbf{a} \longleftarrow P_{\Sigma}(\mathbf{x}, w)$

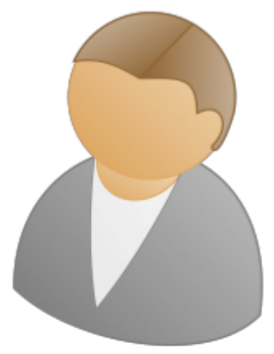
*[JP14] Abhishek Jain and Omkant Pandey. Non-malleable zero knowledge: Black-box constructions and definitional relationships. SCN 2014

Our NMZK Scheme*

$\mathbf{x} \in L$

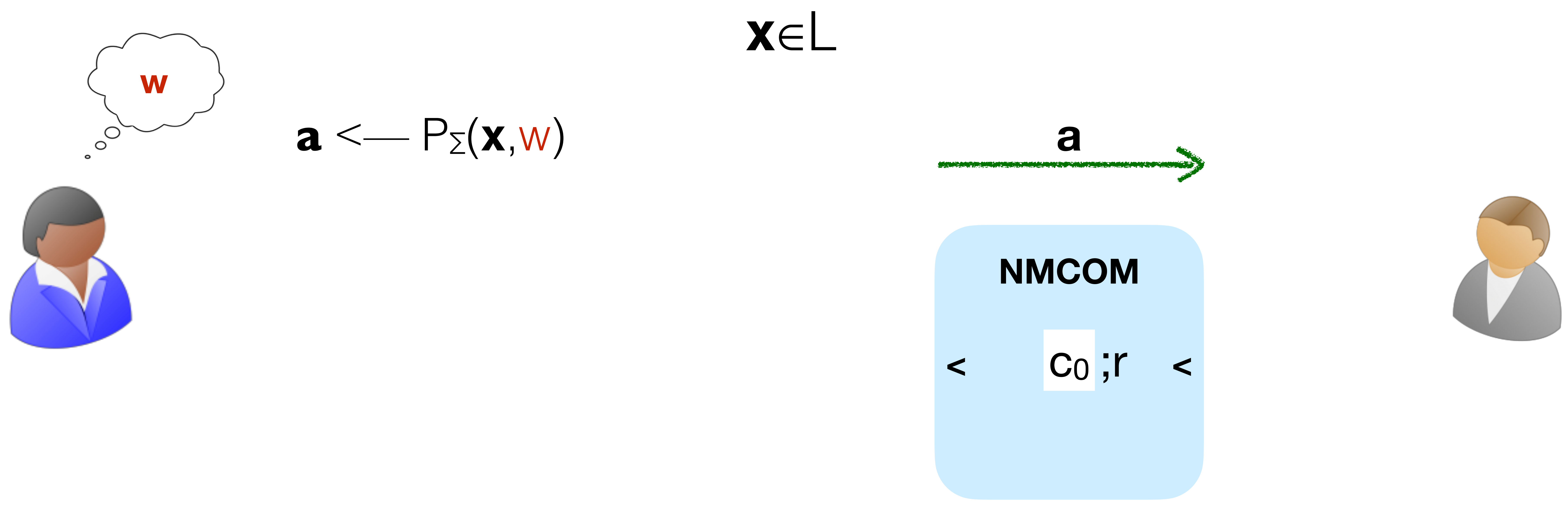
$\mathbf{a} \leftarrow P_{\Sigma}(\mathbf{x}, w)$

$\xrightarrow{\mathbf{a}}$



*[JP14] Abhishek Jain and Omkant Pandey. Non-malleable zero knowledge: Black-box constructions and definitional relationships. SCN 2014

Our NMZK Scheme*



*[JP14] Abhishek Jain and Omkant Pandey. Non-malleable zero knowledge: Black-box constructions and definitional relationships. SCN 2014

Our NMZK Scheme*

$\mathbf{x} \in L$

$\mathbf{a} \longleftarrow P_{\Sigma}(\mathbf{x}, w)$

$\mathbf{a}$ →

NMCOM

< c_0 ;r <

c_1 →

*[JP14] Abhishek Jain and Omkant Pandey. Non-malleable zero knowledge: Black-box constructions and definitional relationships. SCN 2014

Our NMZK Scheme*

$\mathbf{x} \in L$

$\mathbf{a} \longleftarrow P_{\Sigma}(\mathbf{x}, w)$

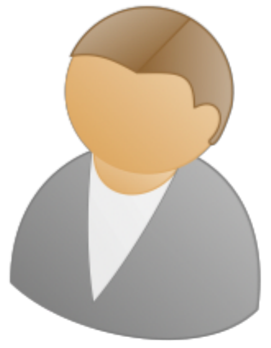
a →

NMCOM

< c_0 ;r <

c_1 →

← c_0, r



*[JP14] Abhishek Jain and Omkant Pandey. Non-malleable zero knowledge: Black-box constructions and definitional relationships. SCN 2014

Our NMZK Scheme*

$\mathbf{x} \in L$

$\mathbf{a} \leftarrow P_\Sigma(\mathbf{x}, w)$

$\mathbf{a}$ →

NMCOM

< c_0 ;r <

If (c_0, r) is a valid opening

c_1 →

c_0, r ←

$\mathbf{c} = \mathbf{c_0} \oplus \mathbf{c_1}$

$z \leftarrow P_\Sigma(x, w, \mathbf{c})$

*[JP14] Abhishek Jain and Omkant Pandey. Non-malleable zero knowledge: Black-box constructions and definitional relationships. SCN 2014

Our NMZK Scheme*

$\mathbf{x} \in L$

$\mathbf{a}$ <— $P_\Sigma(\mathbf{x}, w)$

a →

NMCOM

< c_0 ;r <

If (c_0, r) is a valid opening

$\mathbf{c} = \mathbf{c_0} \oplus \mathbf{c_1}$

z <— $P_\Sigma(x, w, \mathbf{c})$

c_1 →

c_0, r ←

z →

*[JP14] Abhishek Jain and Omkant Pandey. Non-malleable zero knowledge: Black-box constructions and definitional relationships. SCN 2014

Our NMZK Scheme*

$\mathbf{x} \in L$

$\mathbf{a} \leftarrow P_\Sigma(\mathbf{x}, w)$

$\xrightarrow{\mathbf{a}}$

NMCOM

< c_0 ;r <

If (c_0, r) is a valid opening

$\xrightarrow{c_1}$

$\mathbf{c = c_0 \oplus c_1}$

$\xleftarrow{c_0,\ r}$

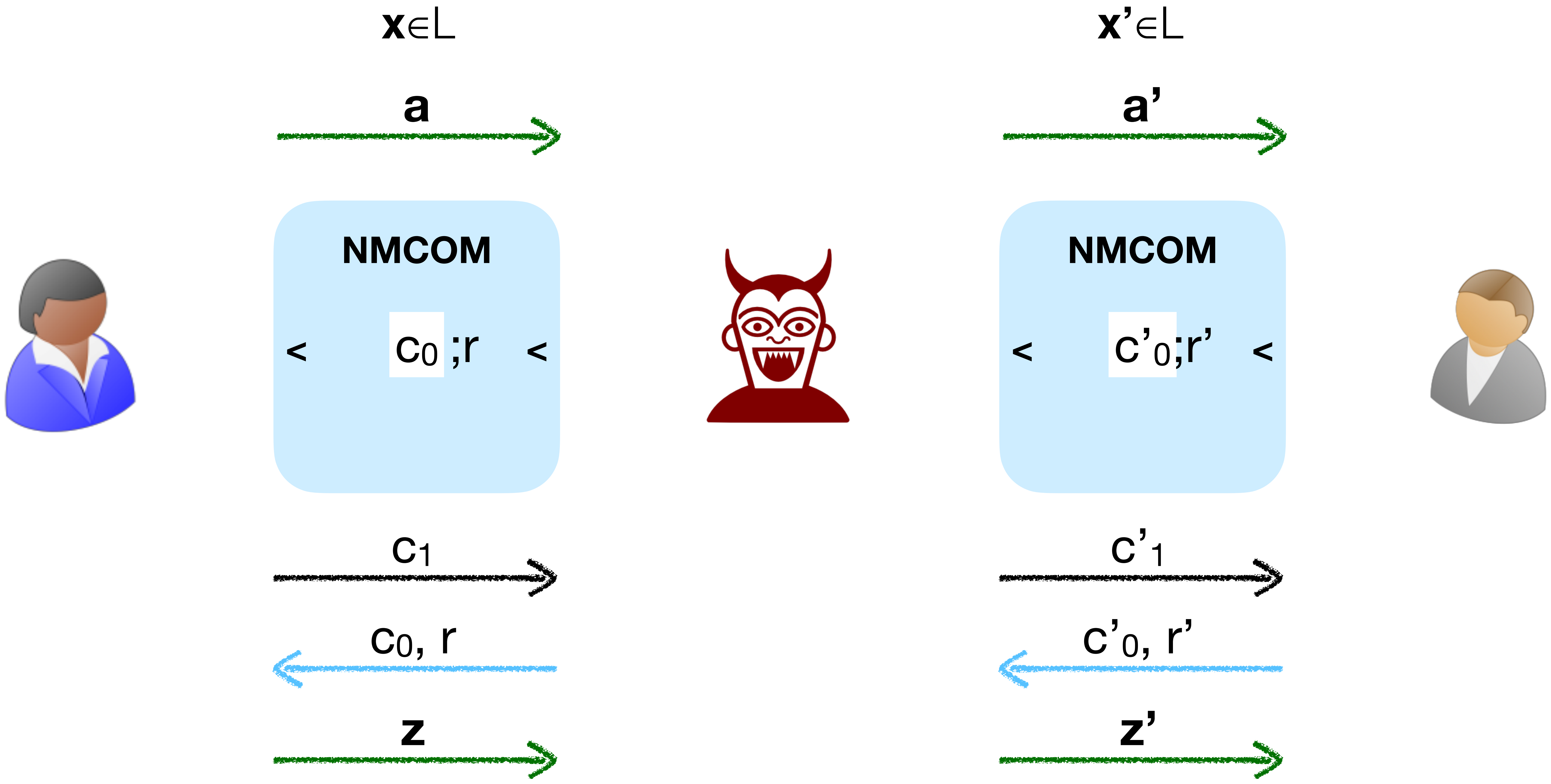
$z \leftarrow P_\Sigma(x, w, \mathbf{c})$

$\xrightarrow{\mathbf{z}}$

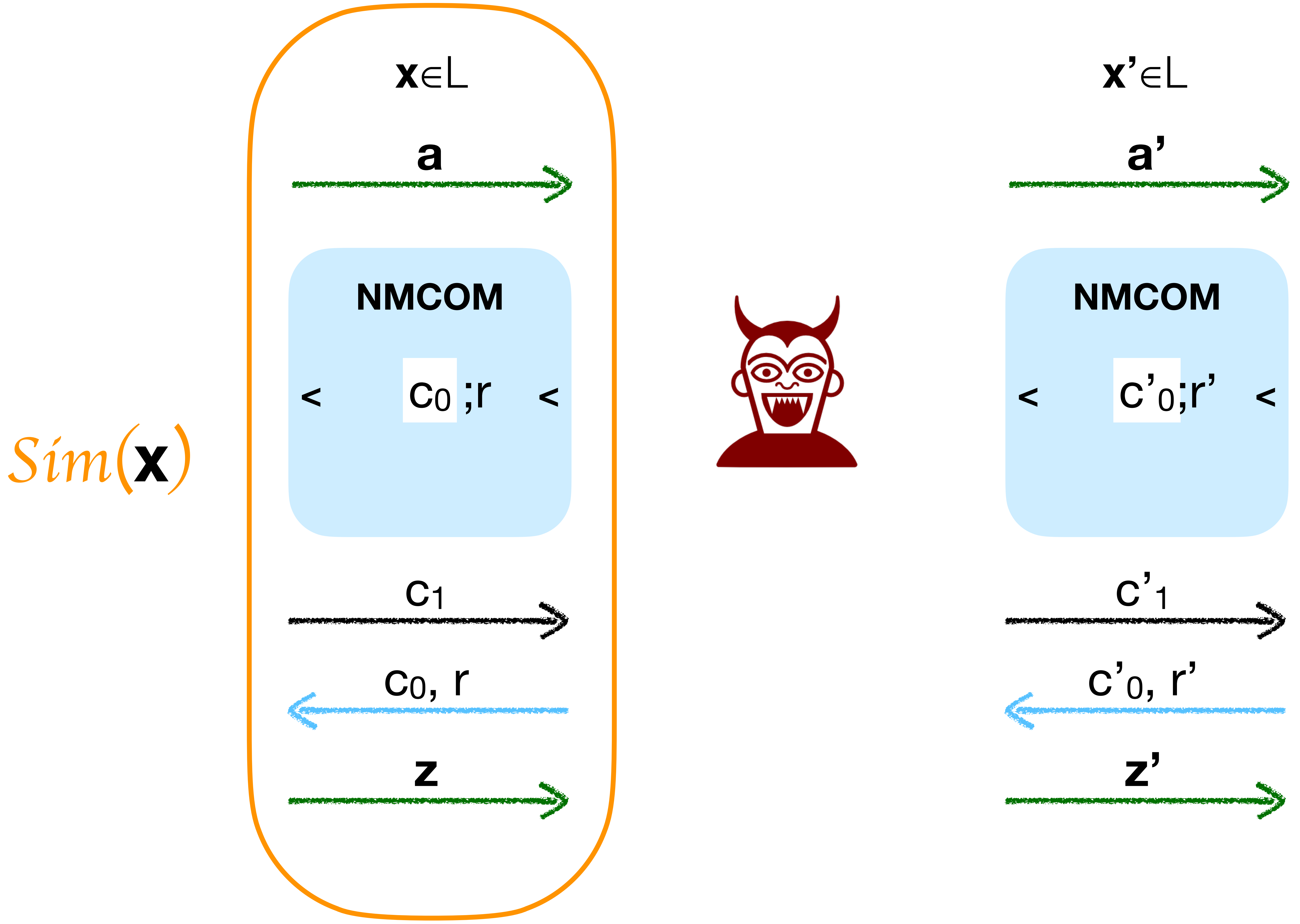
$V_\Sigma(x,a,c,z)=1$

*[JP14] Abhishek Jain and Omkant Pandey. Non-malleable zero knowledge: Black-box constructions and definitional relationships. SCN 2014

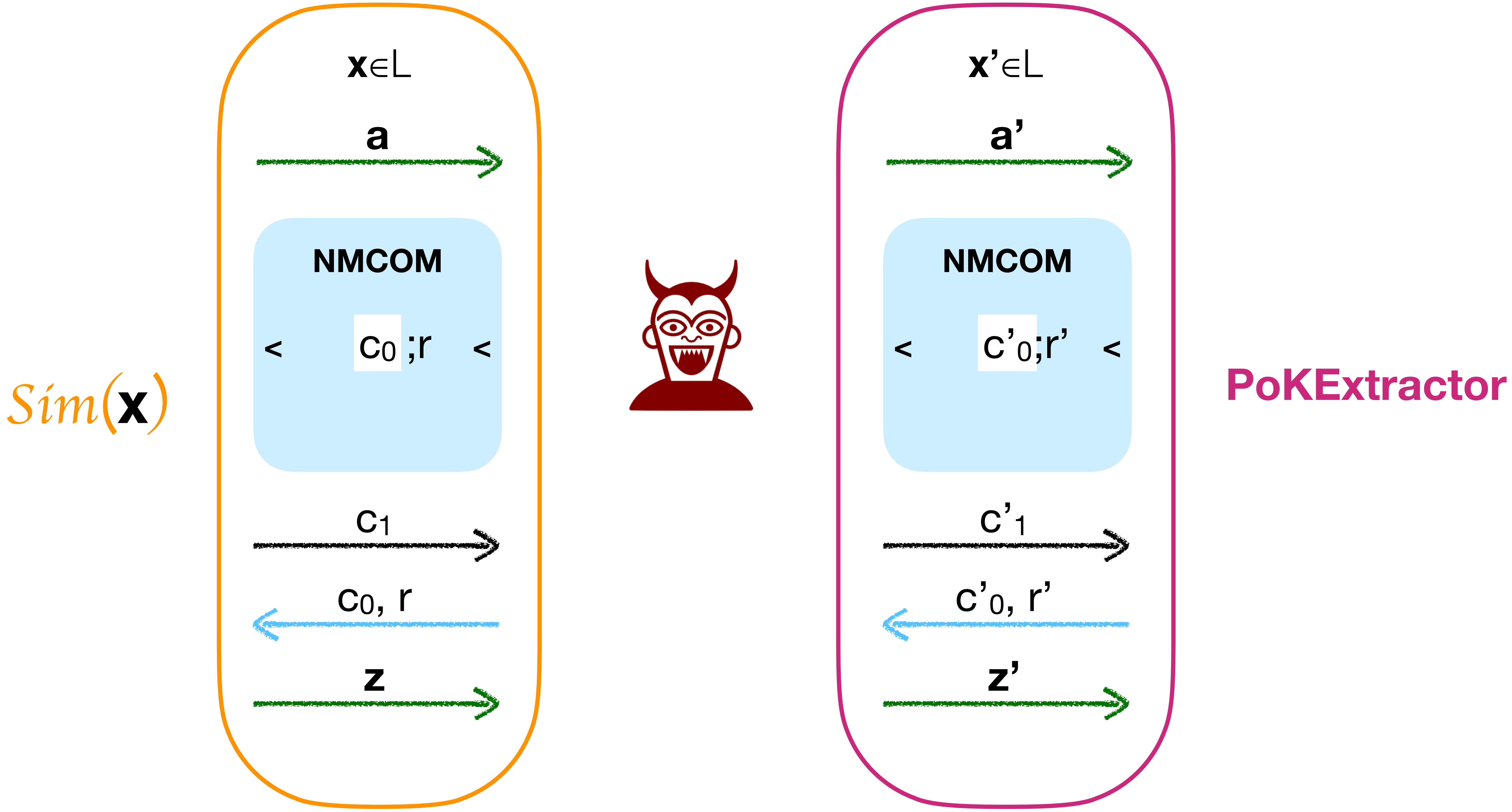
Proof approach



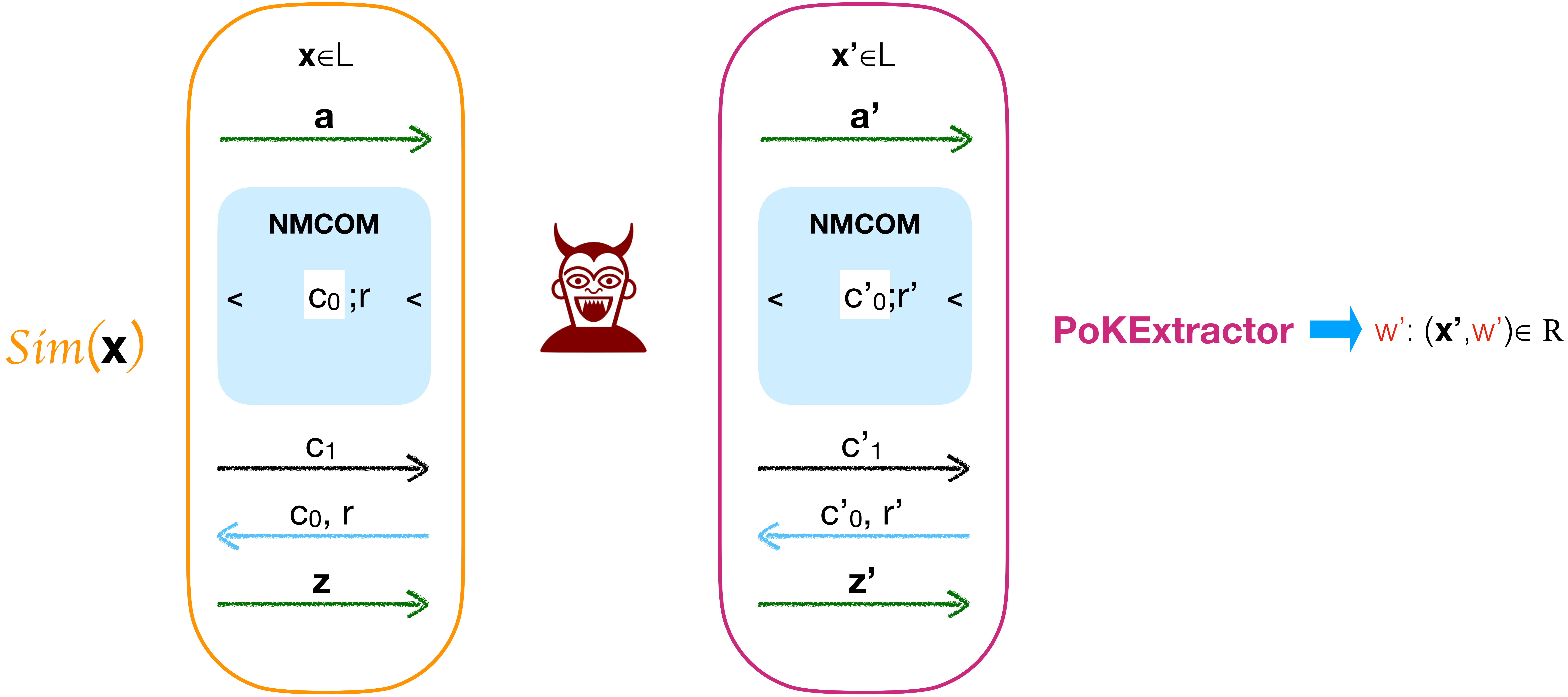
Proof approach



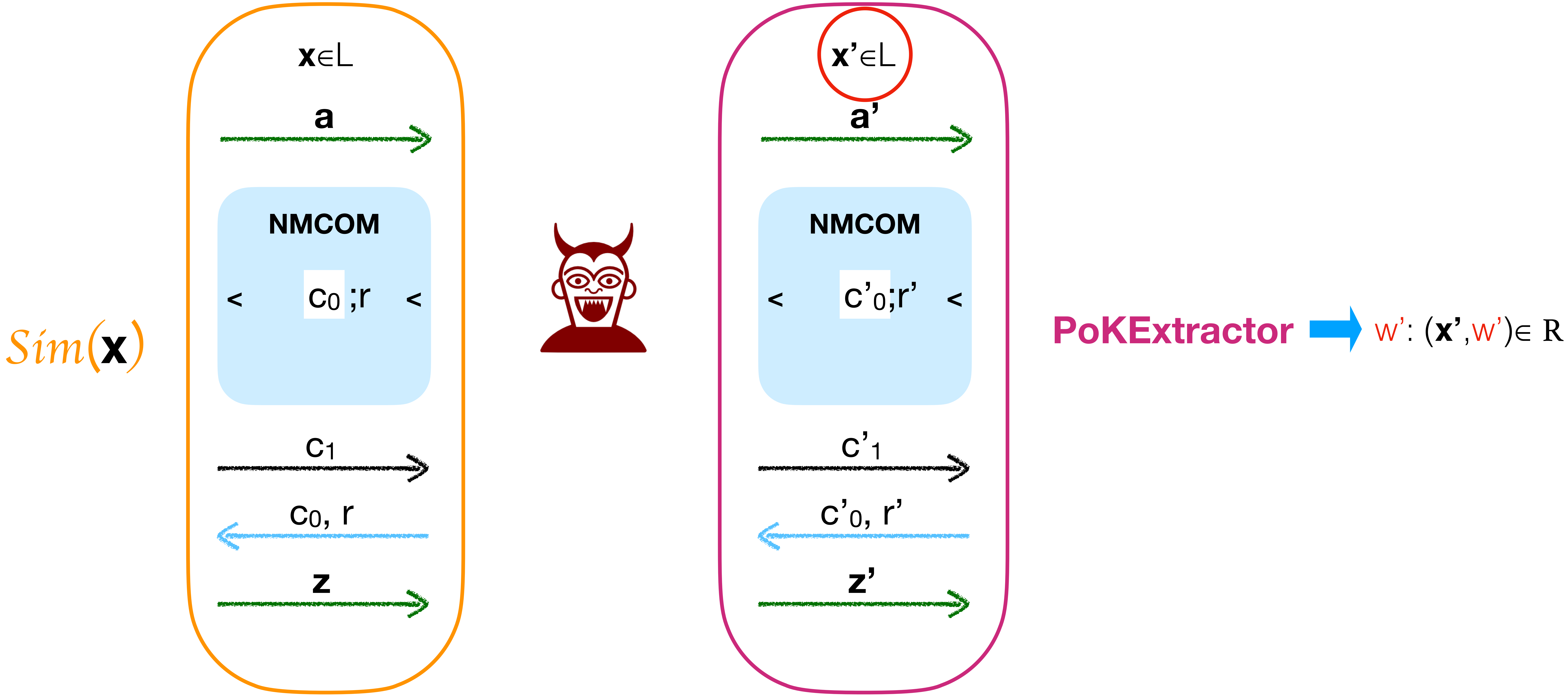
Proof approach



Proof approach



Proof approach



Zero-Knowledge

$Sim(\mathbf{x})$

Zero-Knowledge

$Sim(\mathbf{x})$

$\mathbf{a},\mathbf{c},\mathbf{z}$ <— $HVZK_{\Sigma}(\mathbf{x})$

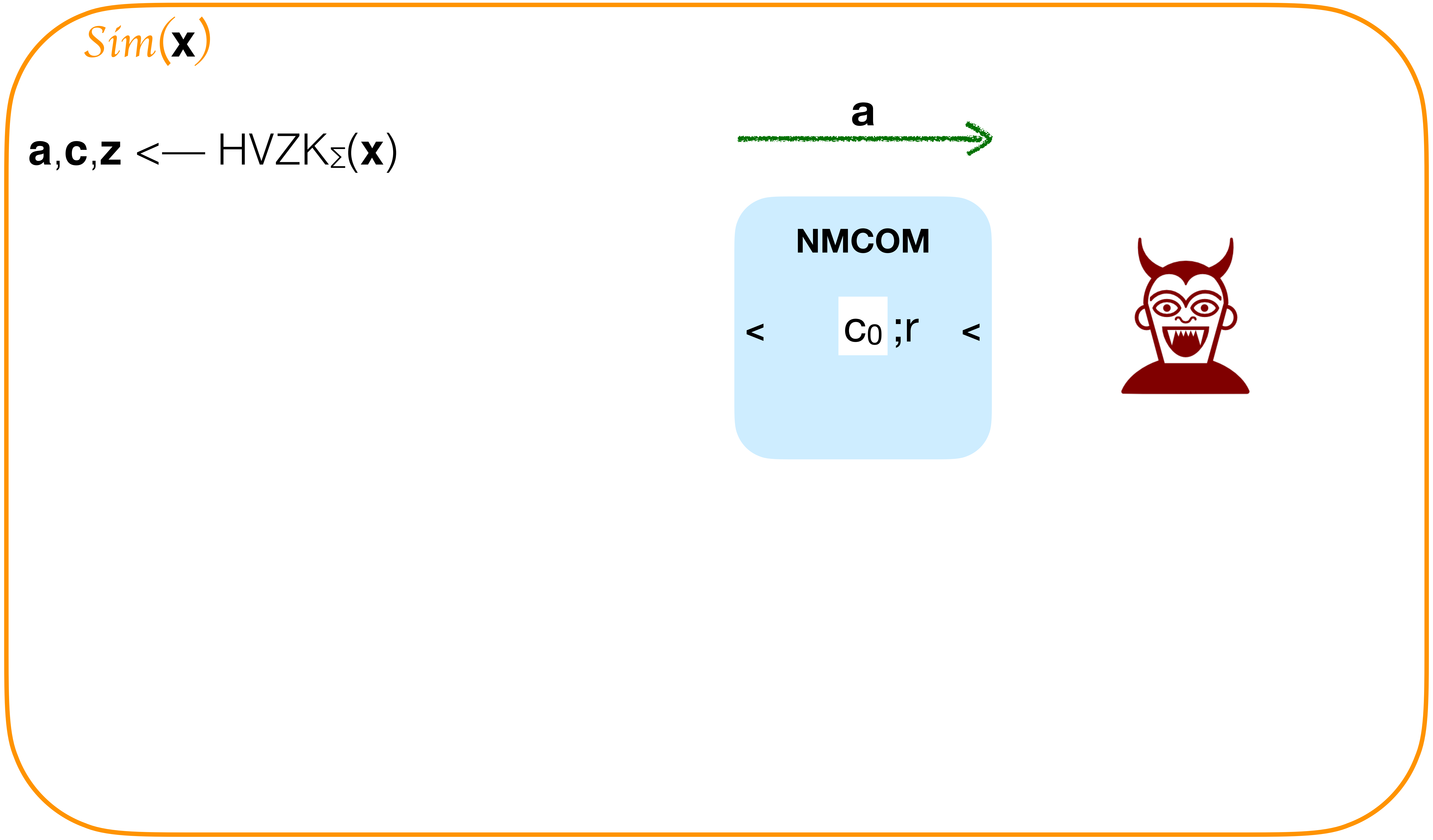
Zero-Knowledge

Sim(**x**)

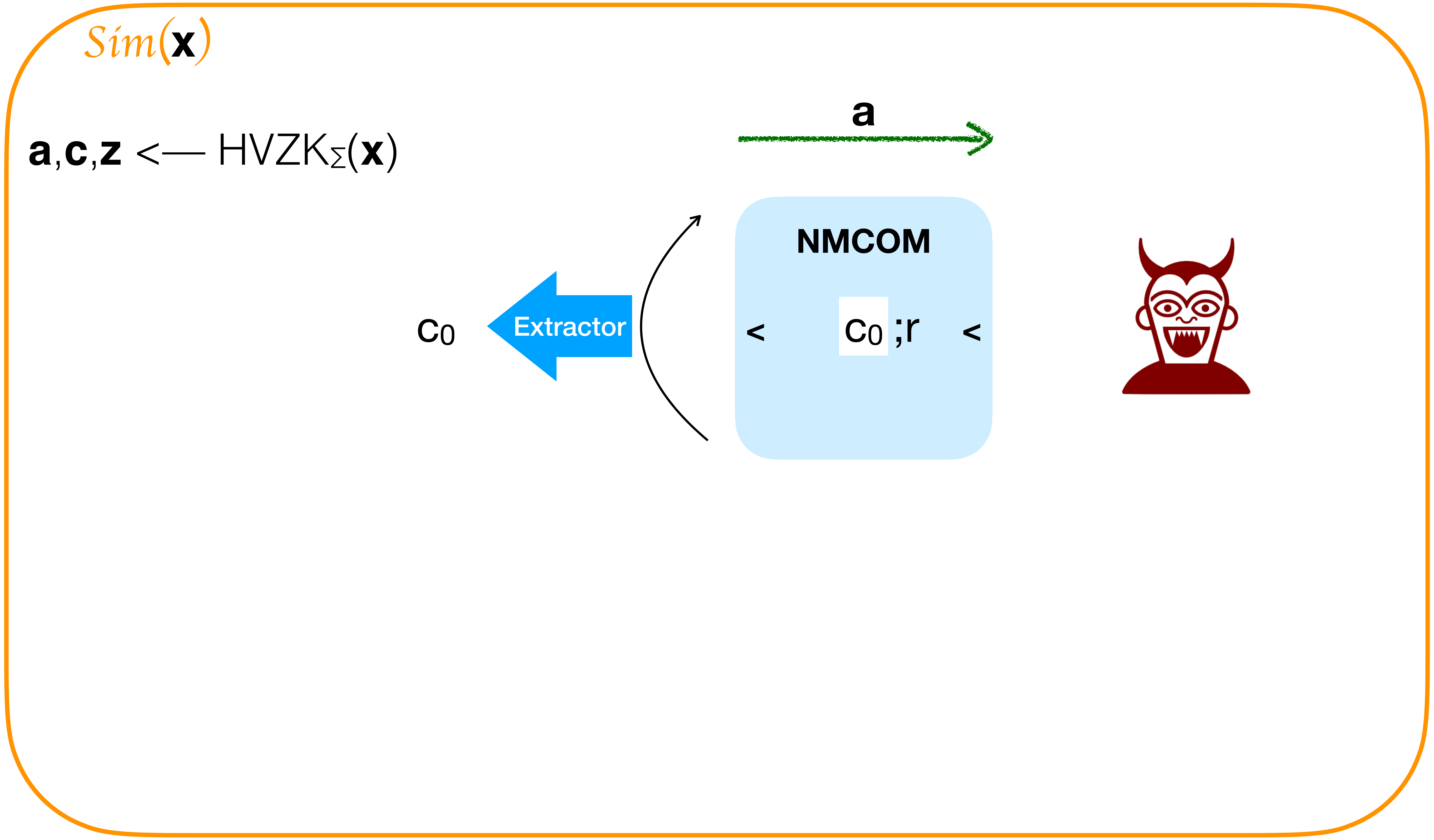
a,**c**,**z** <— $\mathrm{HVZK}_\Sigma(\mathbf{x})$

a →

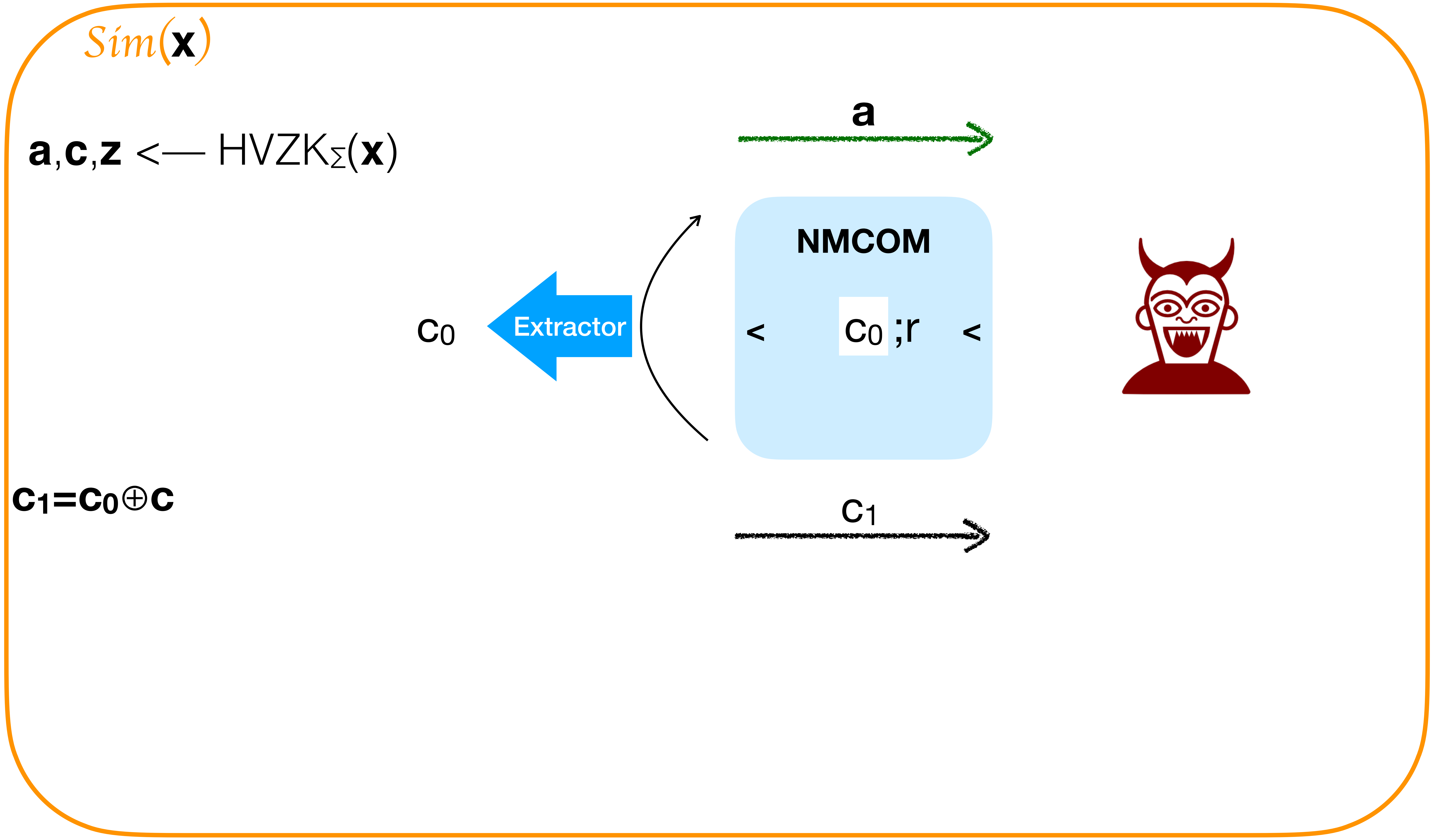
Zero-Knowledge



Zero-Knowledge



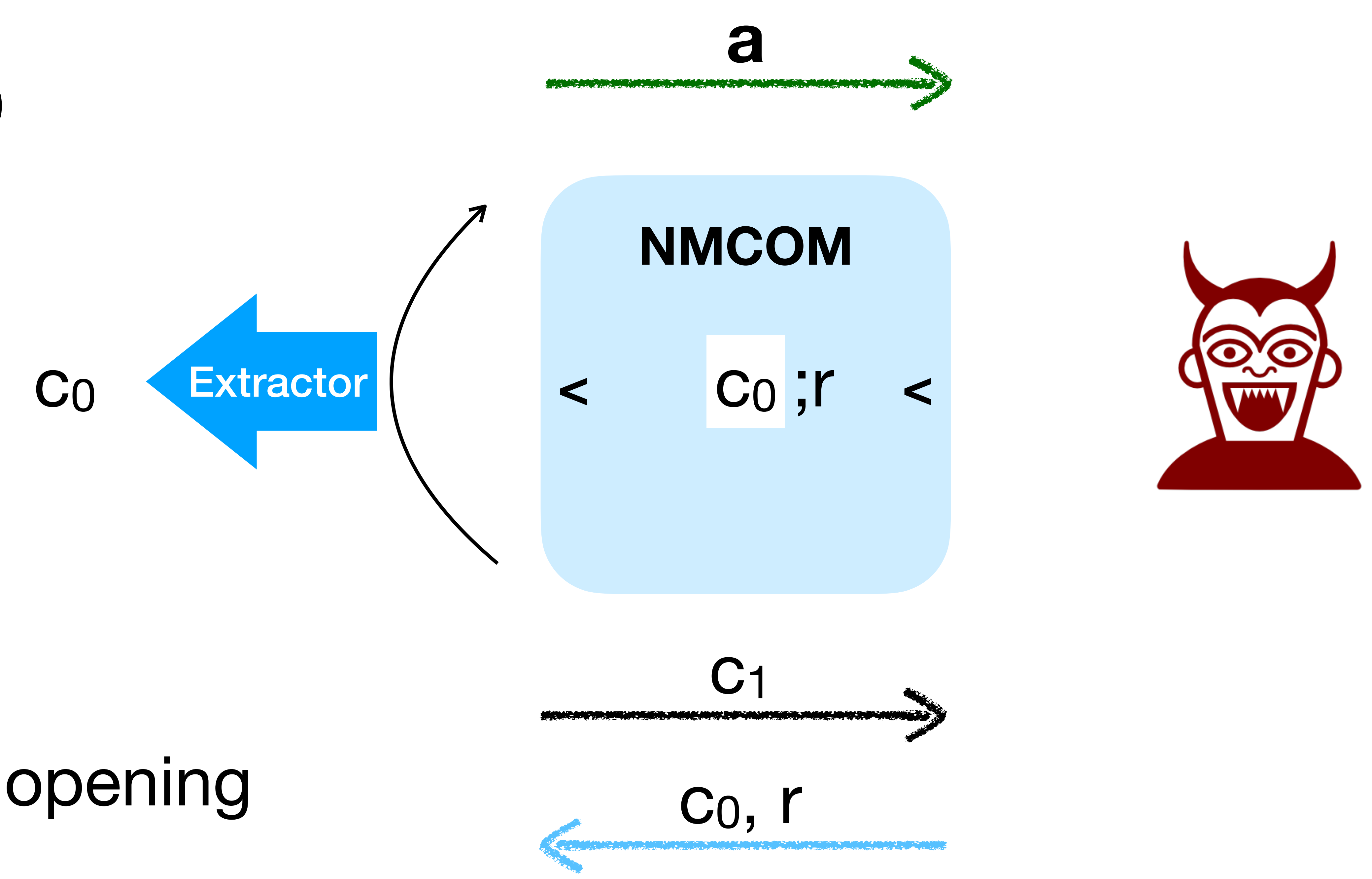
Zero-Knowledge



Zero-Knowledge

Sim(**x**)

$\mathbf{a},\mathbf{c},\mathbf{z} \longleftarrow HVZK_{\Sigma}(\mathbf{x})$



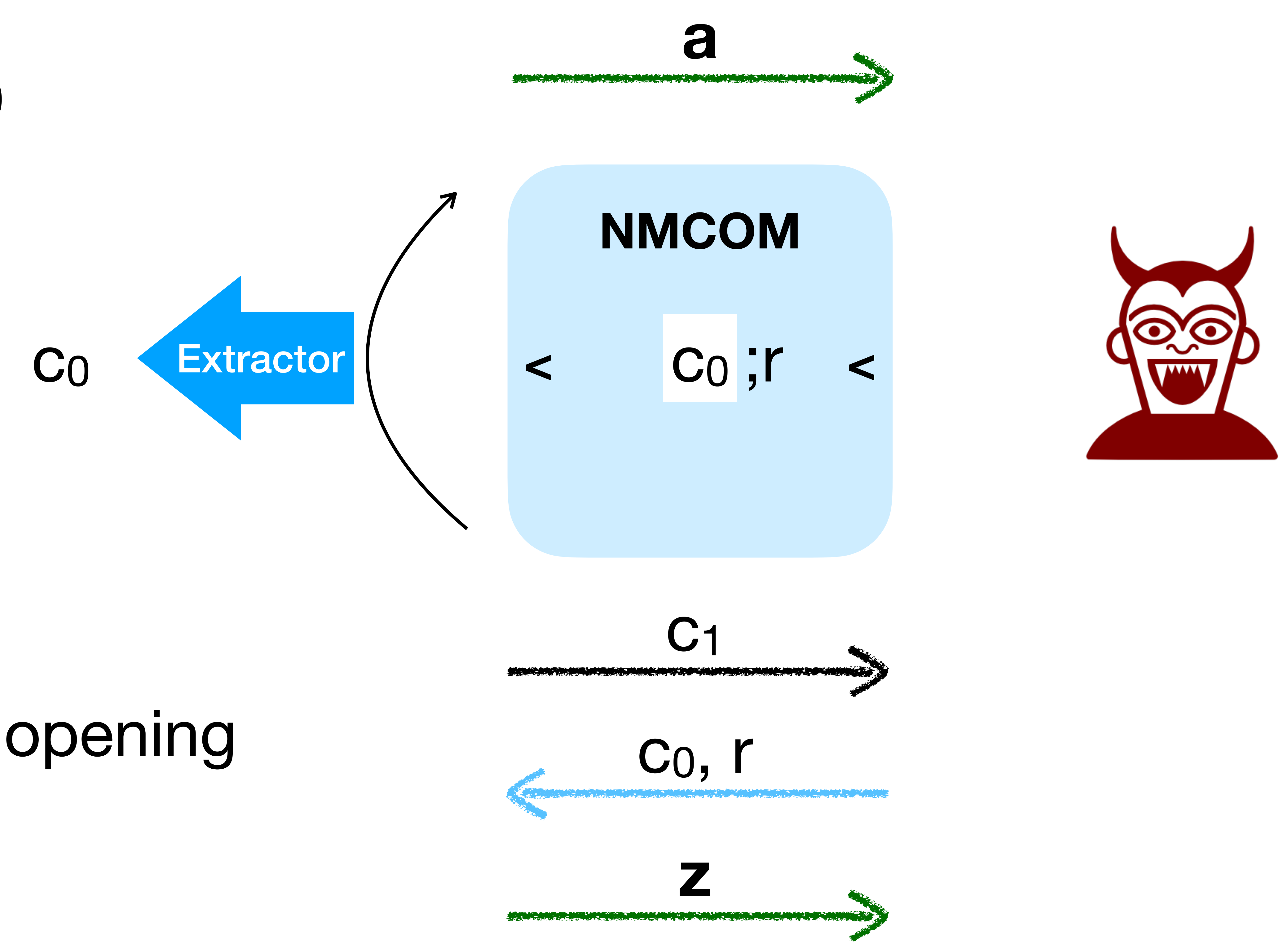
$\mathbf{c_1 = c_0 \oplus c}$

If (c_0, r) is a valid opening

Zero-Knowledge

Sim(**x**)

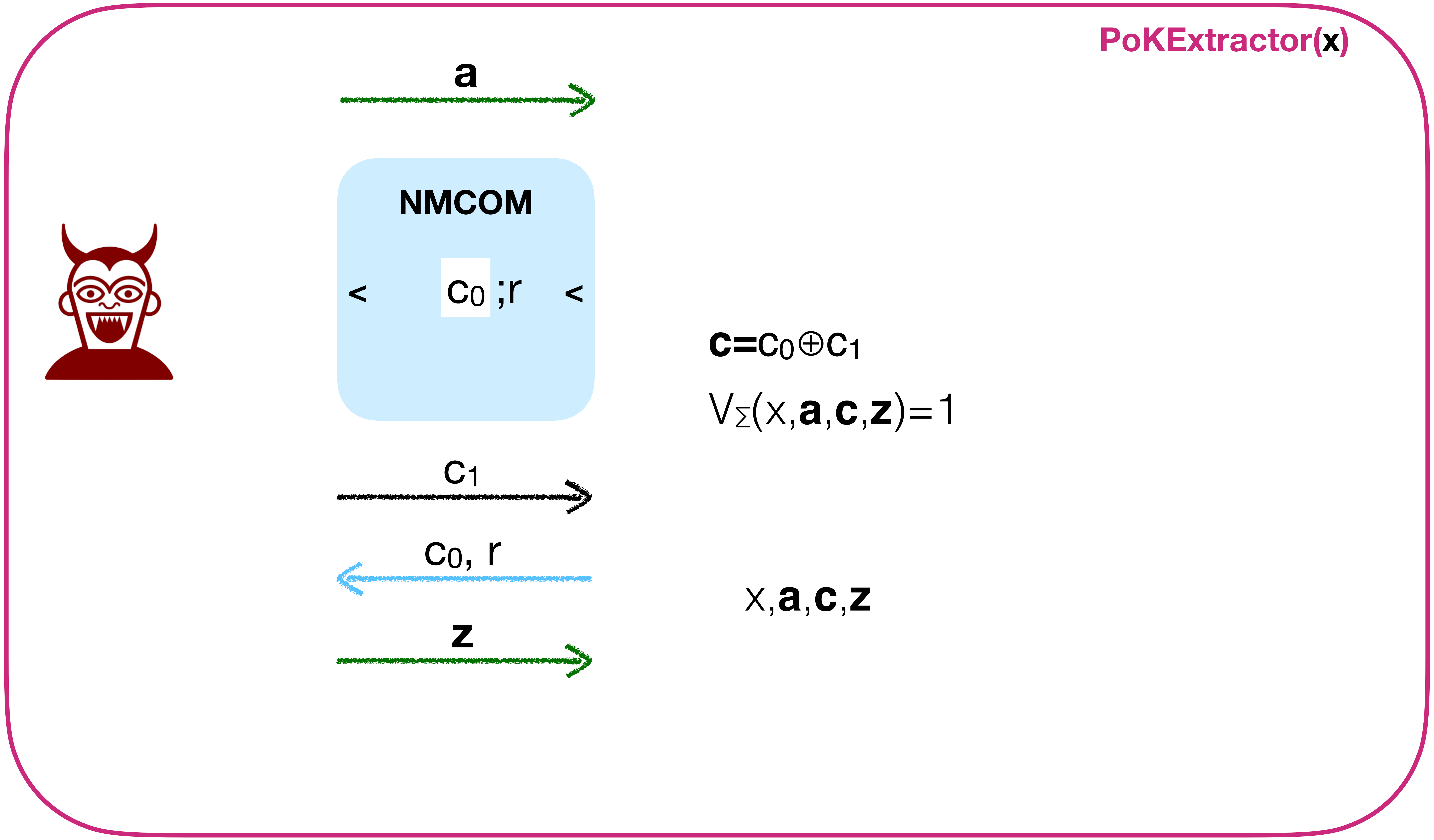
$\mathbf{a},\mathbf{c},\mathbf{z} \leftarrow HVZK_\Sigma(\mathbf{x})$



$\mathbf{c_1 = c_0 \oplus c}$

If (c_0, r) is a valid opening

Soundness (Via Extraction)



Soundness (Via Extraction)

PoKExtractor(x)

$\xrightarrow{\mathbf{a}}$

$\mathbf{c}=c_0 \oplus c_1$

$V_\Sigma(x,\mathbf{a},\mathbf{c},\mathbf{z})=1$

$x,\mathbf{a},\mathbf{c},\mathbf{z}$

Soundness (Via Extraction)

PoKExtractor(x)

a

NMCOM

< c^*_0 ;r^* <

$\mathbf{c} = c_0 \oplus c_1$

$V_\Sigma(x, \mathbf{a}, \mathbf{c}, \mathbf{z}) = 1$

$x, \mathbf{a}, \mathbf{c}, \mathbf{z}$

Soundness (Via Extraction)

PoKExtractor(x)

a

NMCOM

< c^*_0 ;r^* <

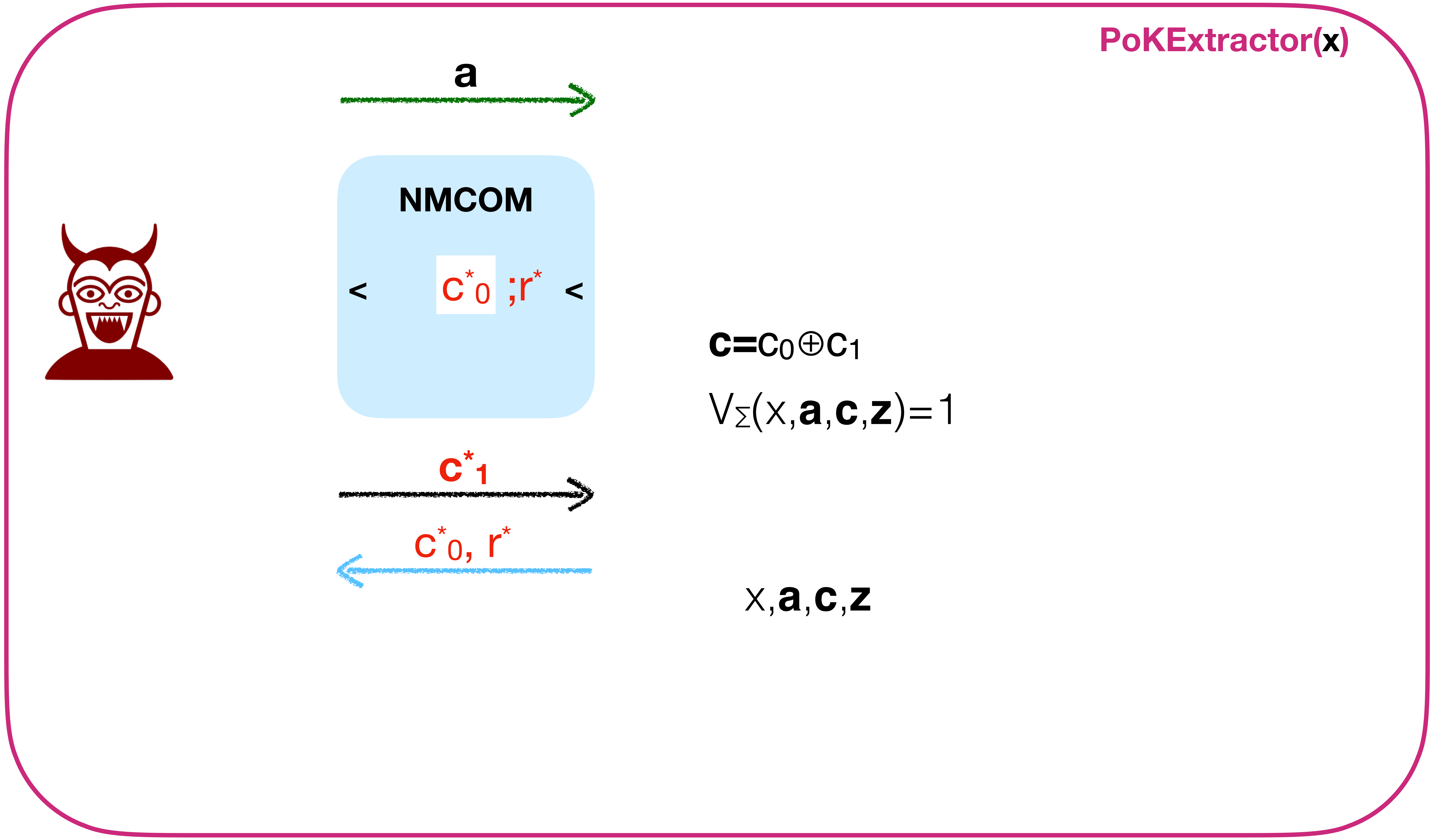
$\mathbf{c^*_1}$

$\mathbf{c}=c_0 \oplus c_1$

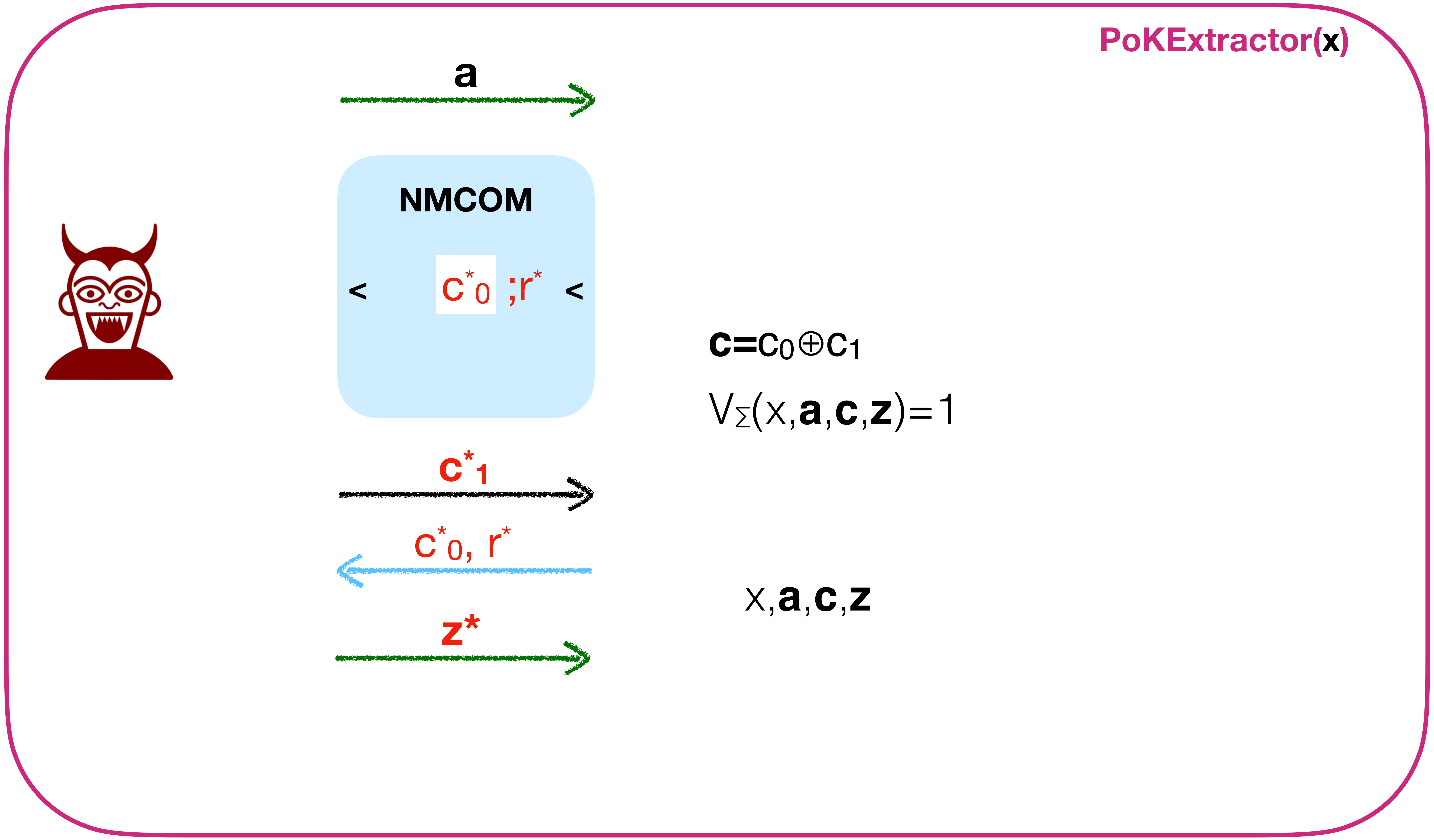
$V_\Sigma(x,\mathbf{a},\mathbf{c},\mathbf{z})=1$

$x,\mathbf{a},\mathbf{c},\mathbf{z}$

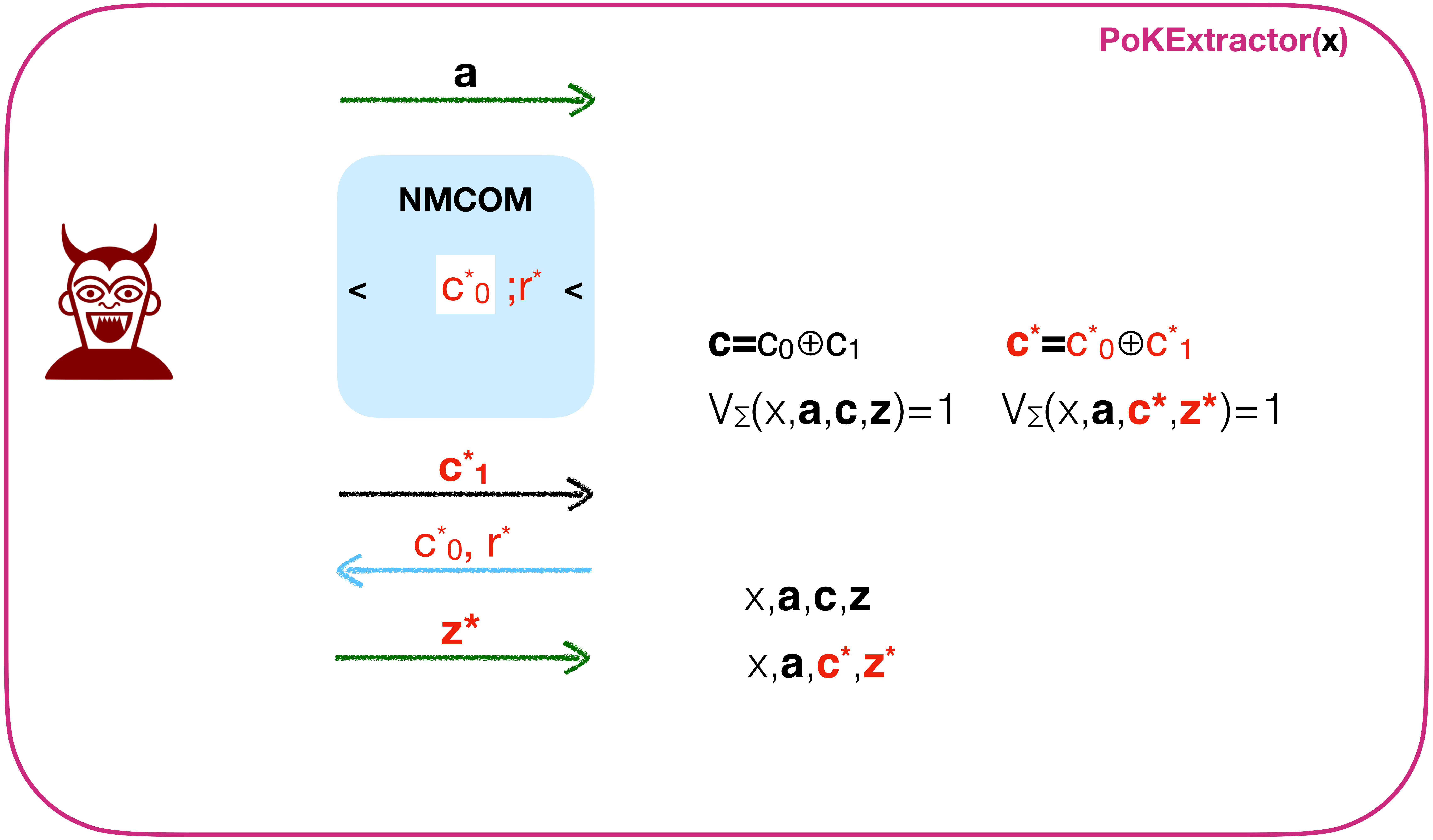
Soundness (Via Extraction)



Soundness (Via Extraction)



Soundness (Via Extraction)



Soundness (Via Extraction)

PoKExtractor(x)

a

NMCOM

< c^*_0 ;r^* <

$\mathbf{c}$=$c_0 \oplus c_1$ $\mathbf{c^*}$=$c^*_0 \oplus c^*_1$

$V_\Sigma(x,\mathbf{a},\mathbf{c},\mathbf{z})=1$ $V_\Sigma(x,\mathbf{a},\mathbf{c^*},\mathbf{z^*})=1$

$\mathbf{c^*_1}$

c^*_0, r^*

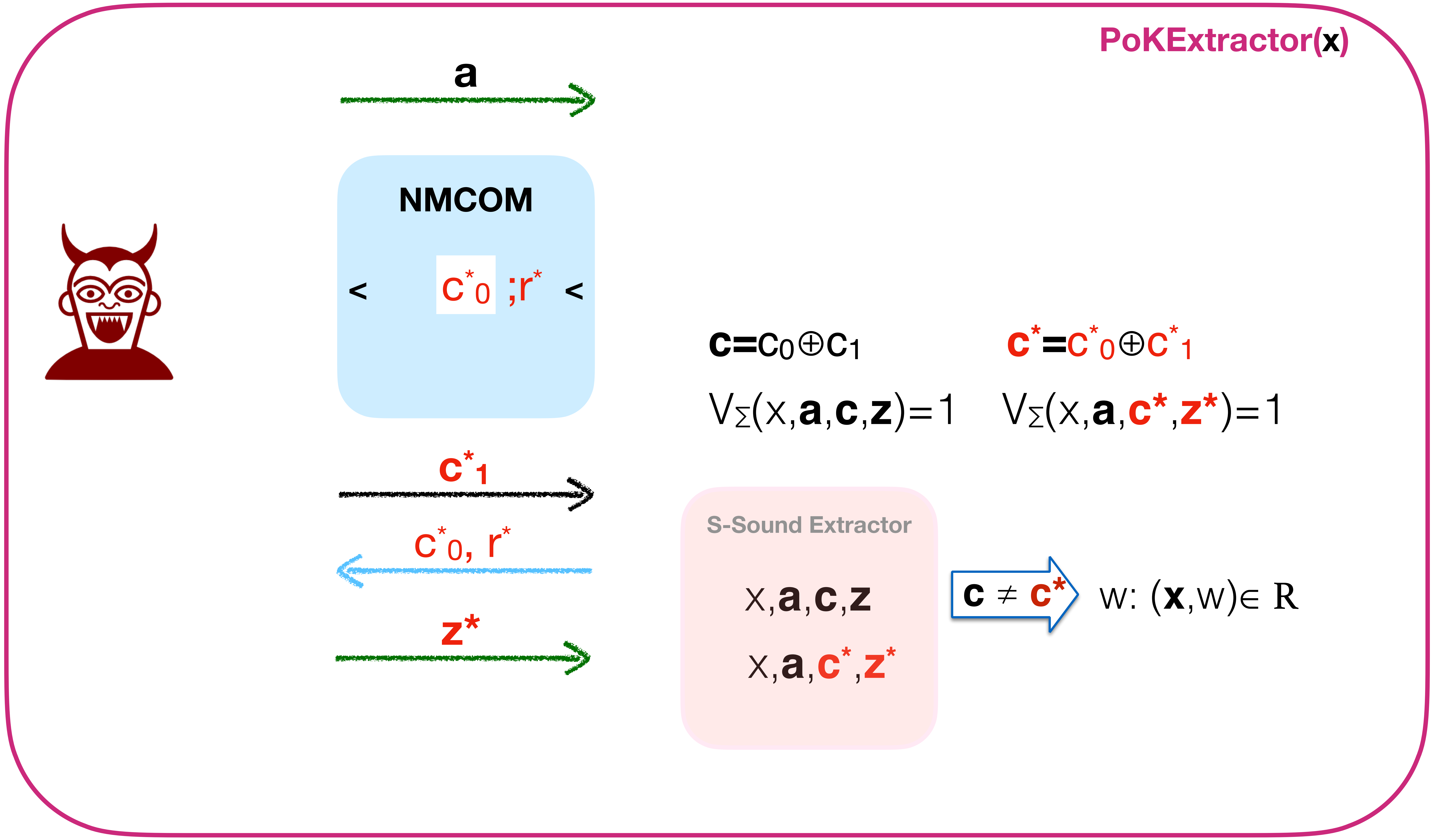
$\mathbf{z^*}$

$x,\mathbf{a},\mathbf{c},\mathbf{z}$

$x,\mathbf{a},\mathbf{c}^*,\mathbf{z}^*$

Hiding of NMCOM guarantees that c≠c*

Soundness (Via Extraction)



Hiding of NMCOM guarantees that $c \neq c^*$

Non-Malleability

x∈L

Sim(**x**)

a,**c**,**z** <— HVZK$_\Sigma$(**x**)

x'∈L

Non-Malleability

$\mathbf{x} \in L$

$\mathbf{x'} \in L$

Sim($\mathbf{x}$)

$\mathbf{a},\mathbf{c},\mathbf{z} \longleftarrow \mathrm{HVZK}_{\Sigma}(\mathbf{x})$

a →

Non-Malleability

$\mathbf{x} \in L$

$\mathbf{x'} \in L$

Sim($\mathbf{x}$)

$\mathbf{a},\mathbf{c},\mathbf{z}$ <— $\mathrm{HVZK}_{\Sigma}(\mathbf{x})$

a →

a' →

Non-Malleability

$\mathbf{x} \in L$

Sim($\mathbf{x}$)

$\mathbf{a},\mathbf{c},\mathbf{z} <\!\!-\!\!- HVZK_{\Sigma}(\mathbf{x})$

a

$\mathbf{x'} \in L$

a'

NMCOM

< $c'_0;r$ <

Non-Malleability

$\mathbf{x} \in L$

Sim($\mathbf{x}$)

$\mathbf{a},\mathbf{c},\mathbf{z}$ <— $\mathrm{HVZK}_{\Sigma}(\mathbf{x})$

a

NMCOM

$<$ c_0;r $<$

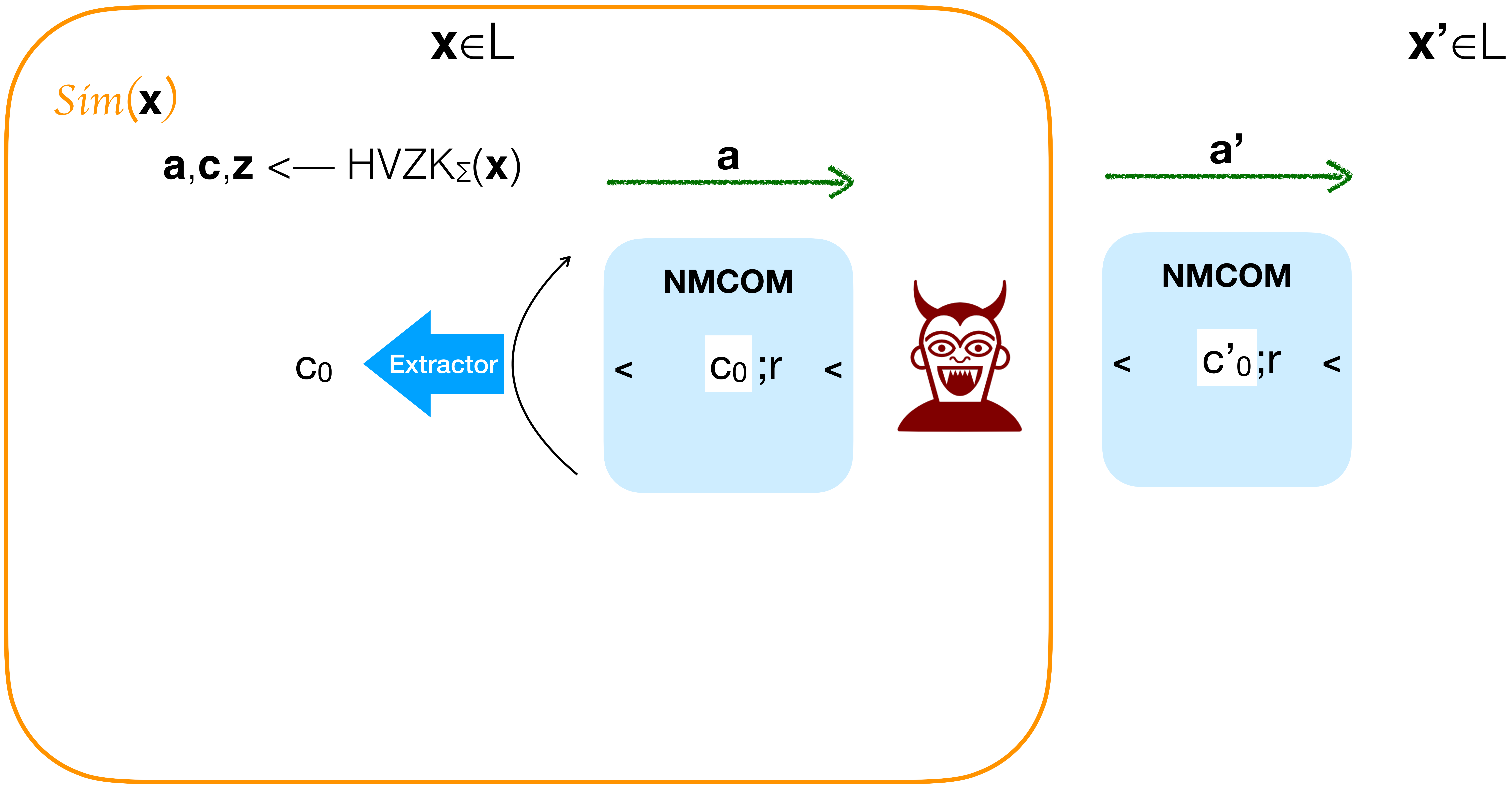
$\mathbf{x'} \in L$

a'

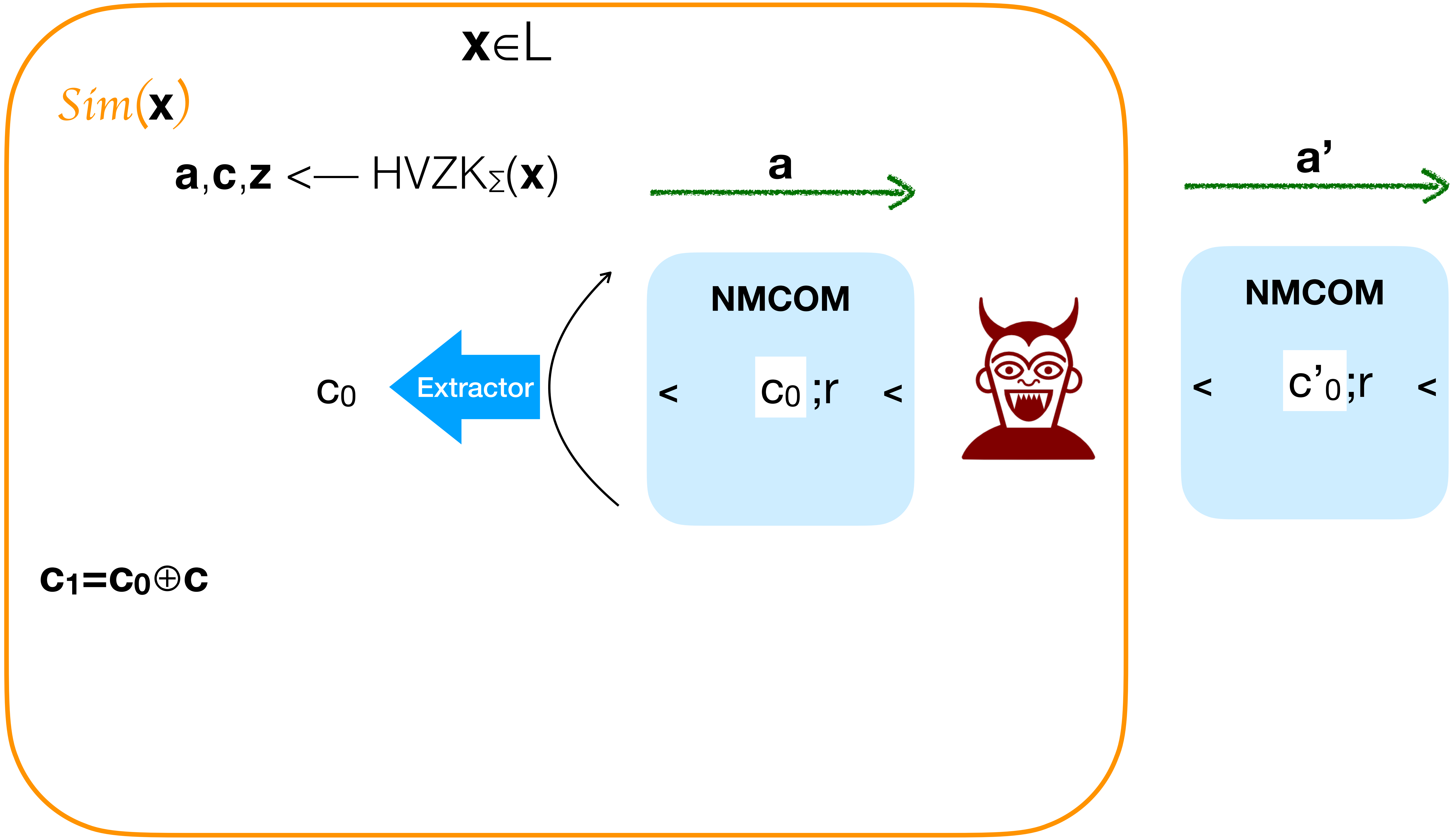
NMCOM

$<$ c'_0;r $<$

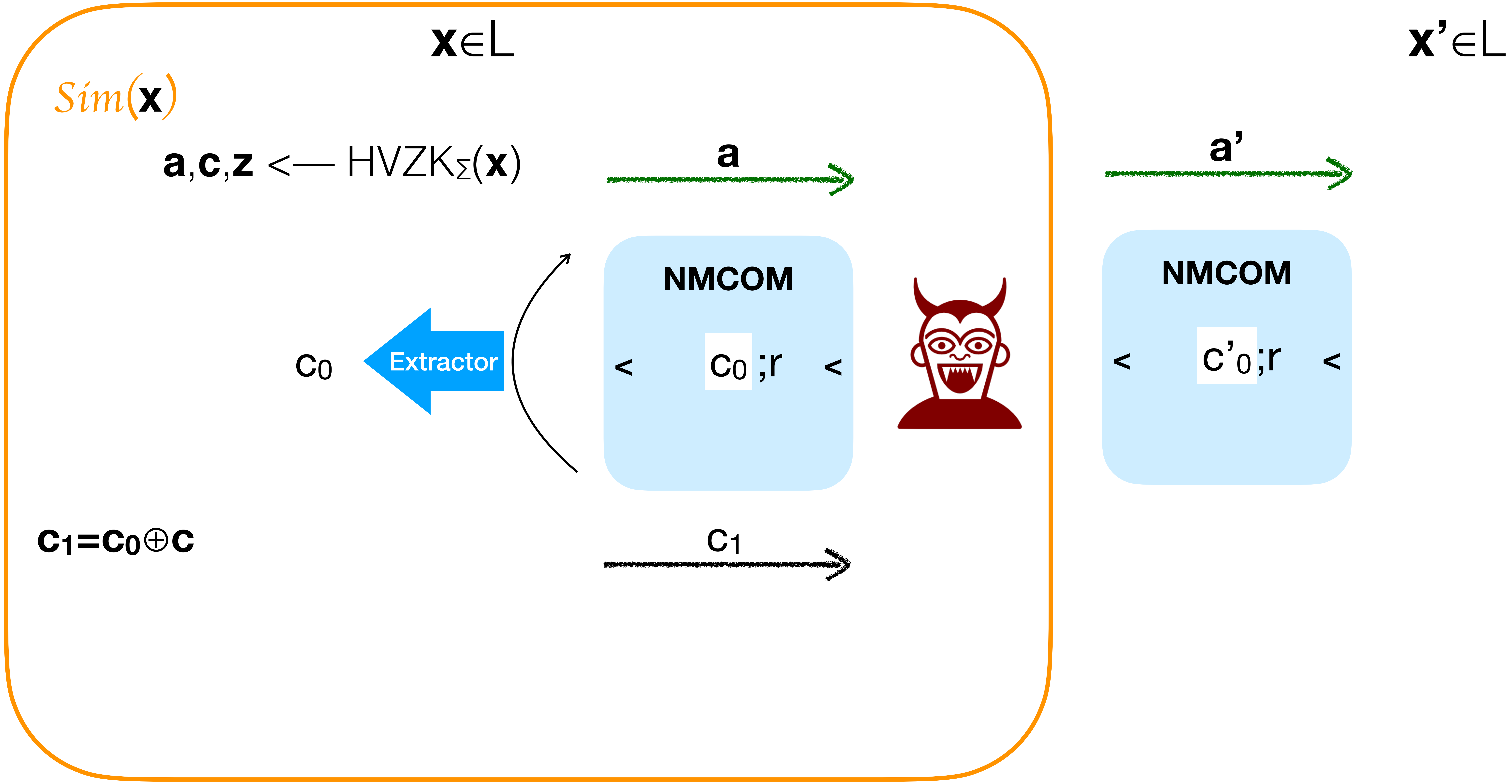
Non-Malleability



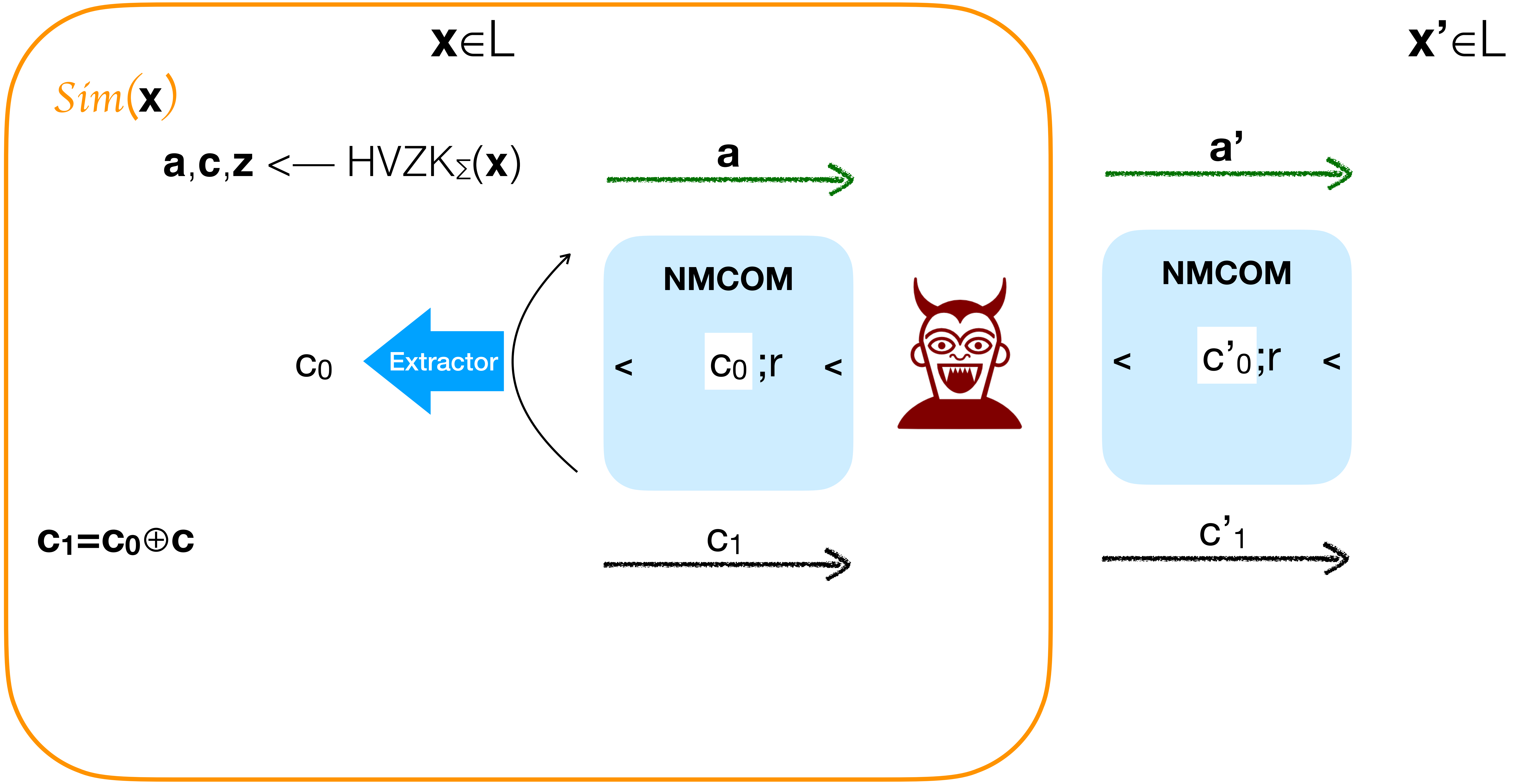
Non-Malleability



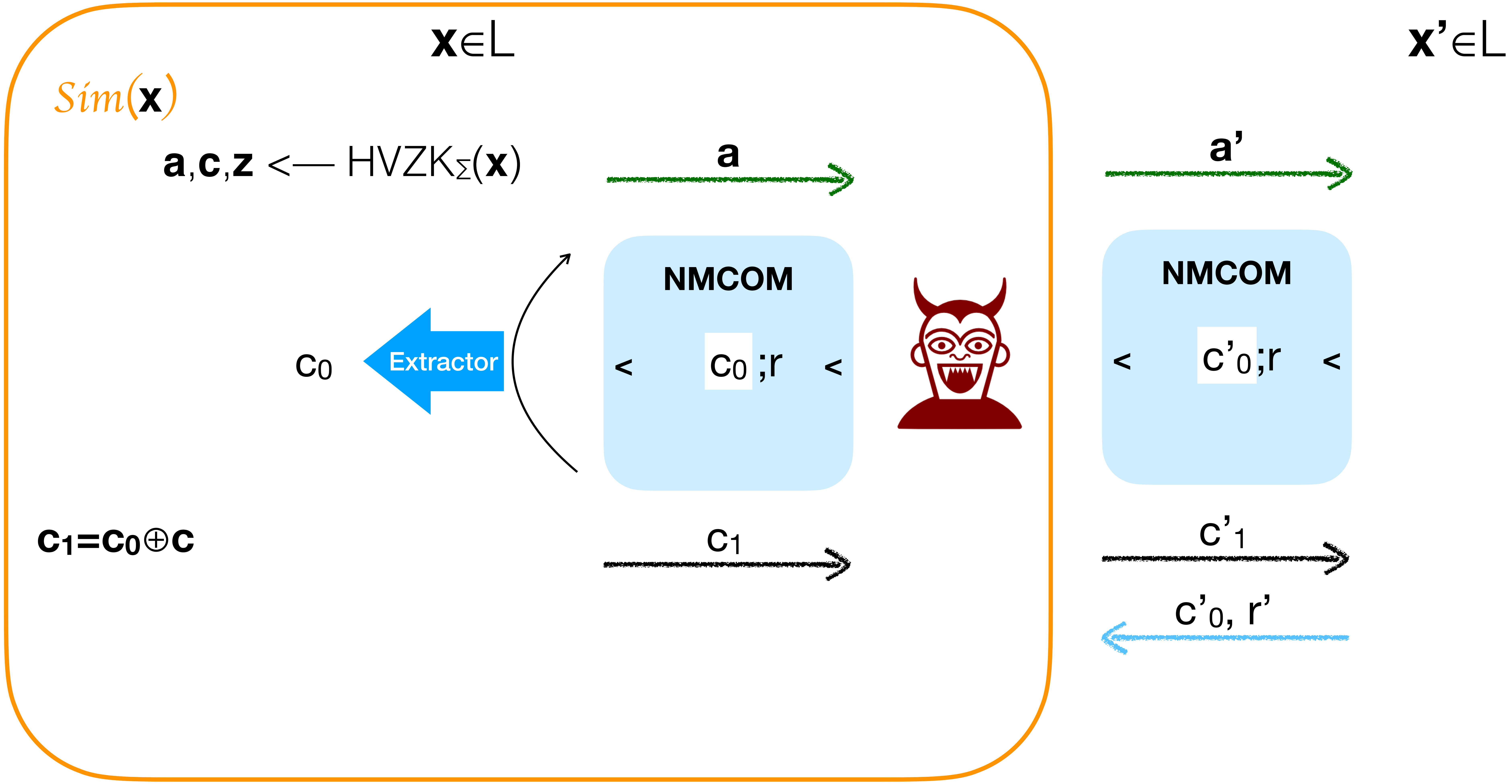
Non-Malleability



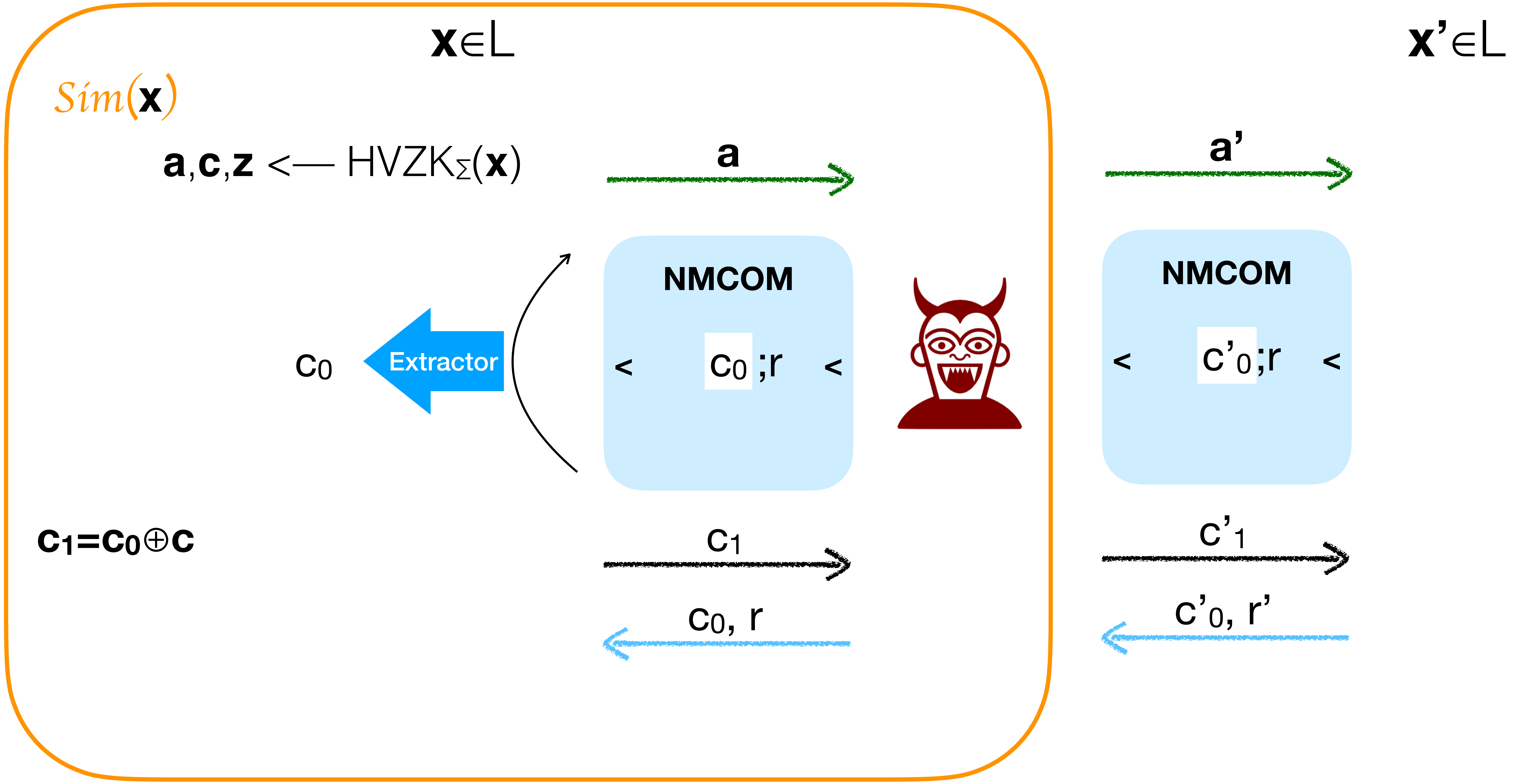
Non-Malleability



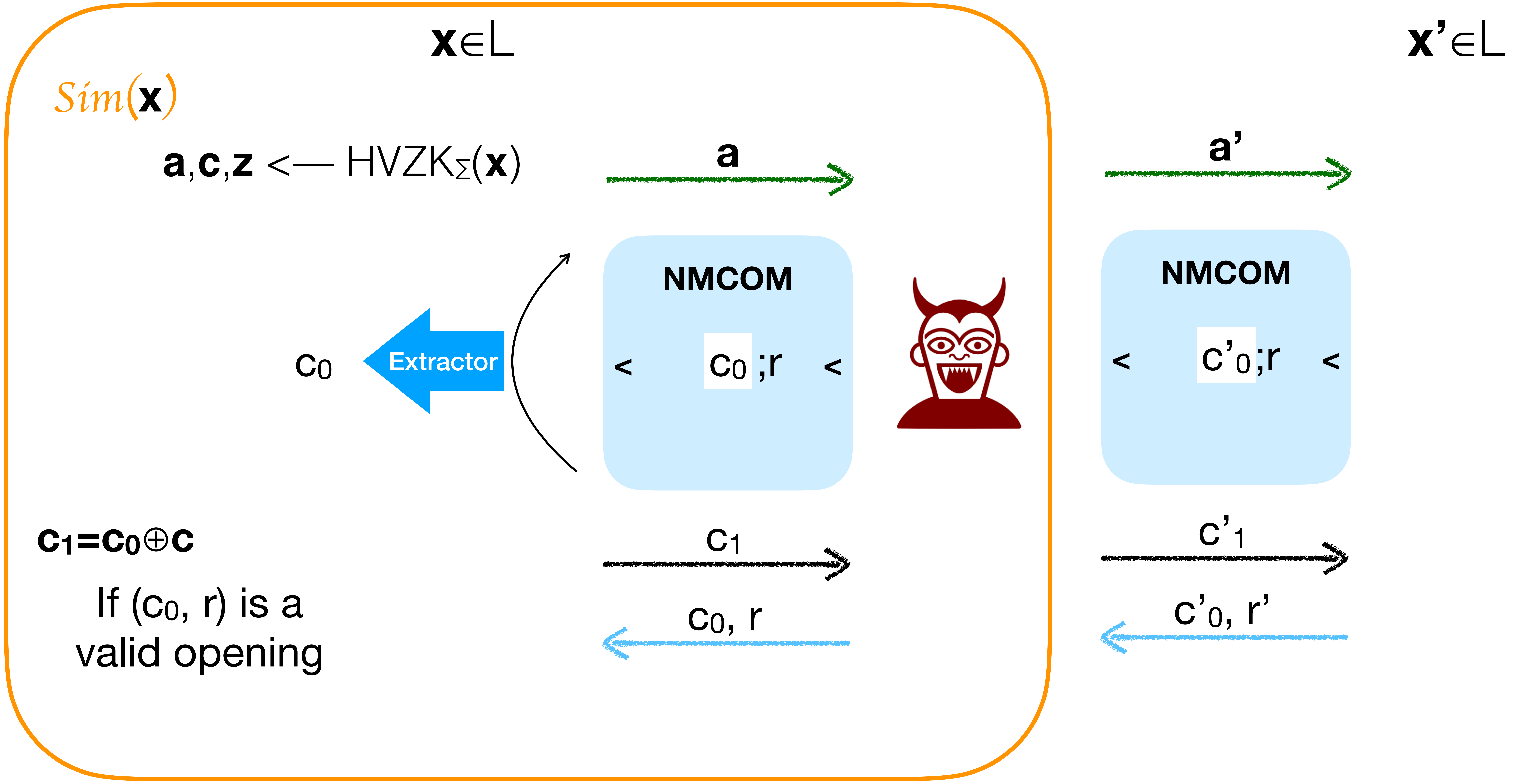
Non-Malleability



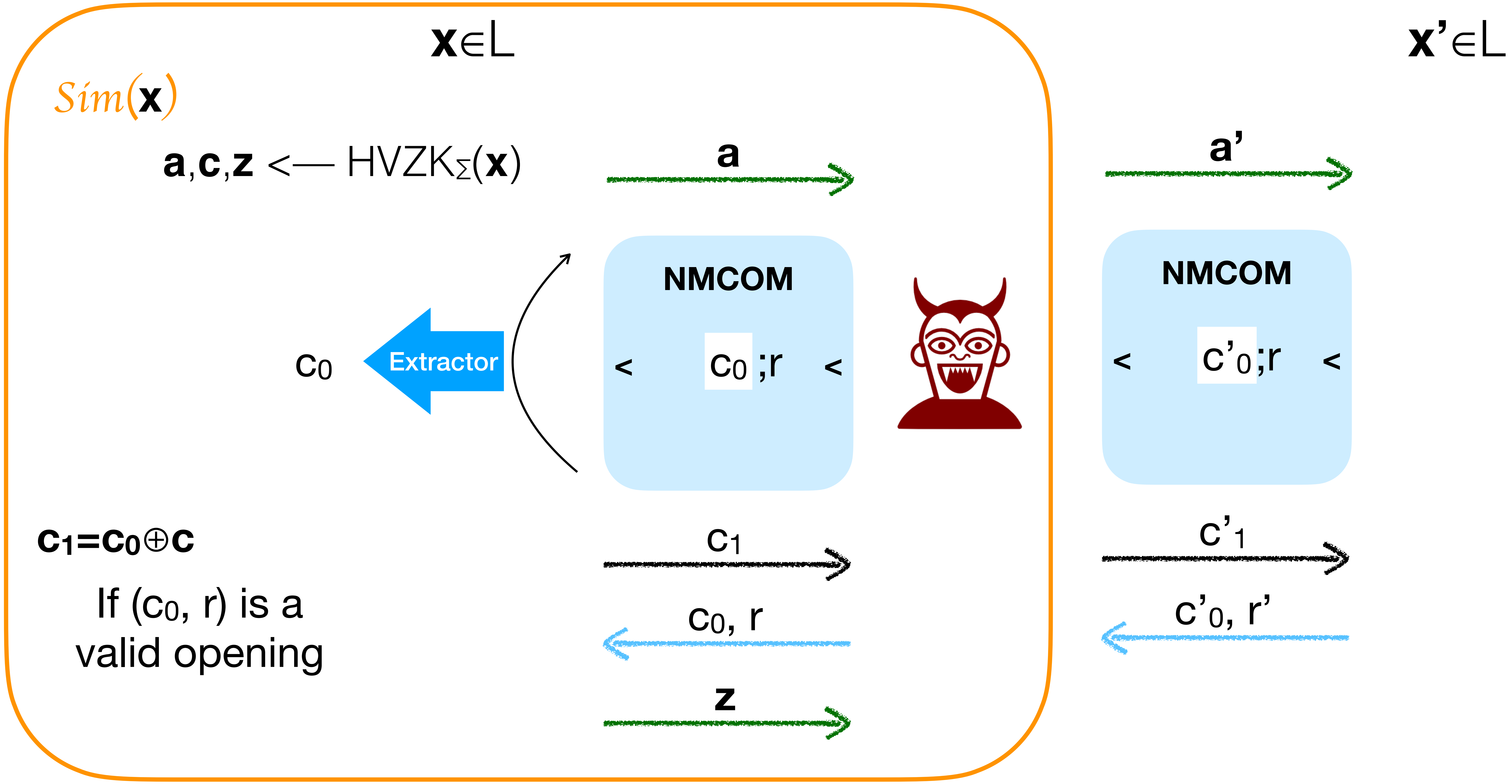
Non-Malleability



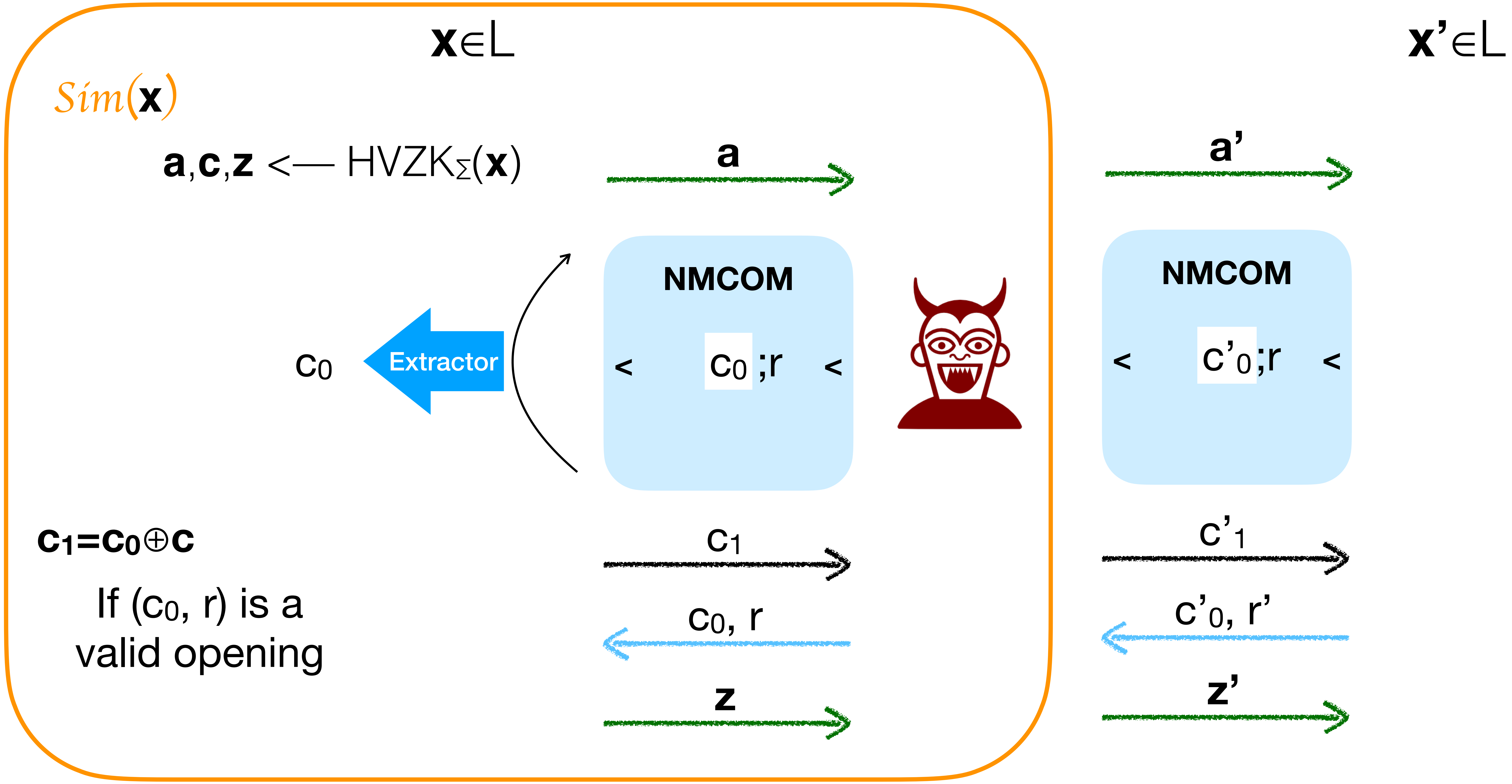
Non-Malleability



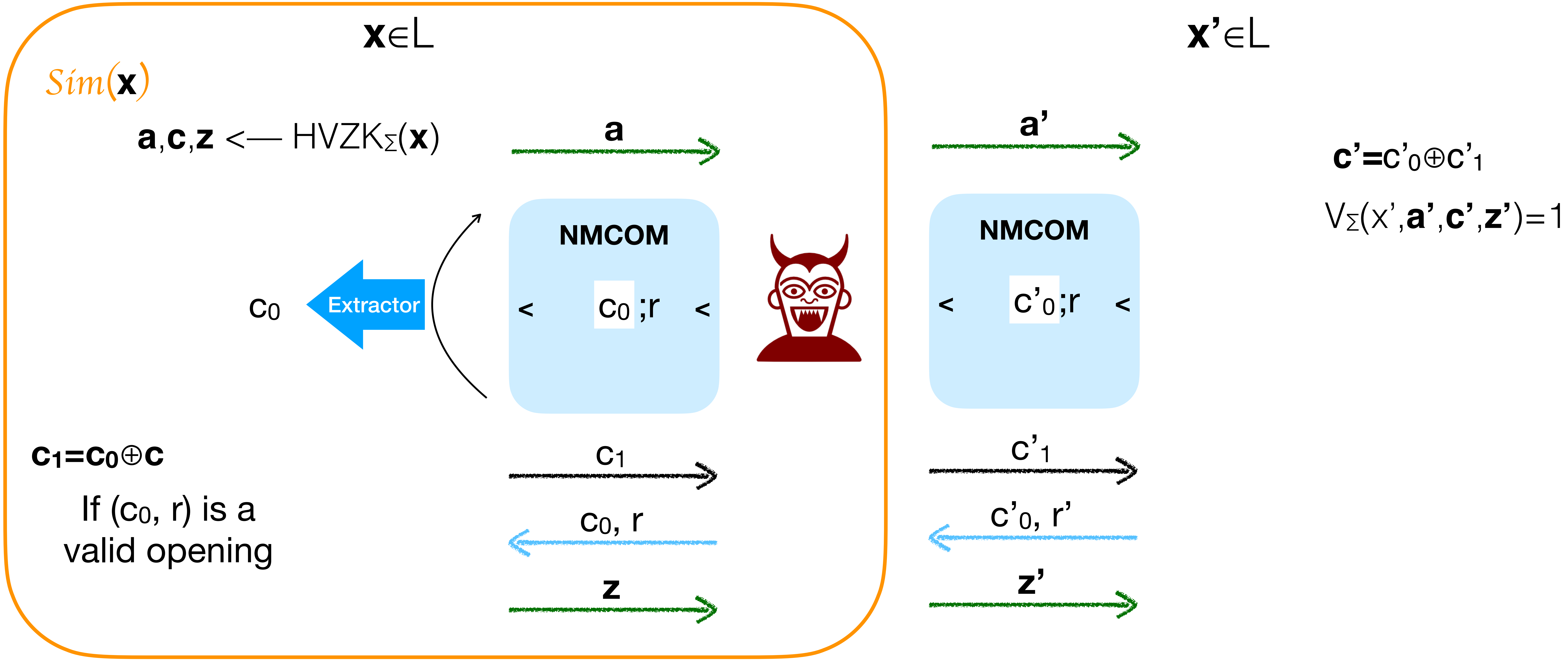
Non-Malleability



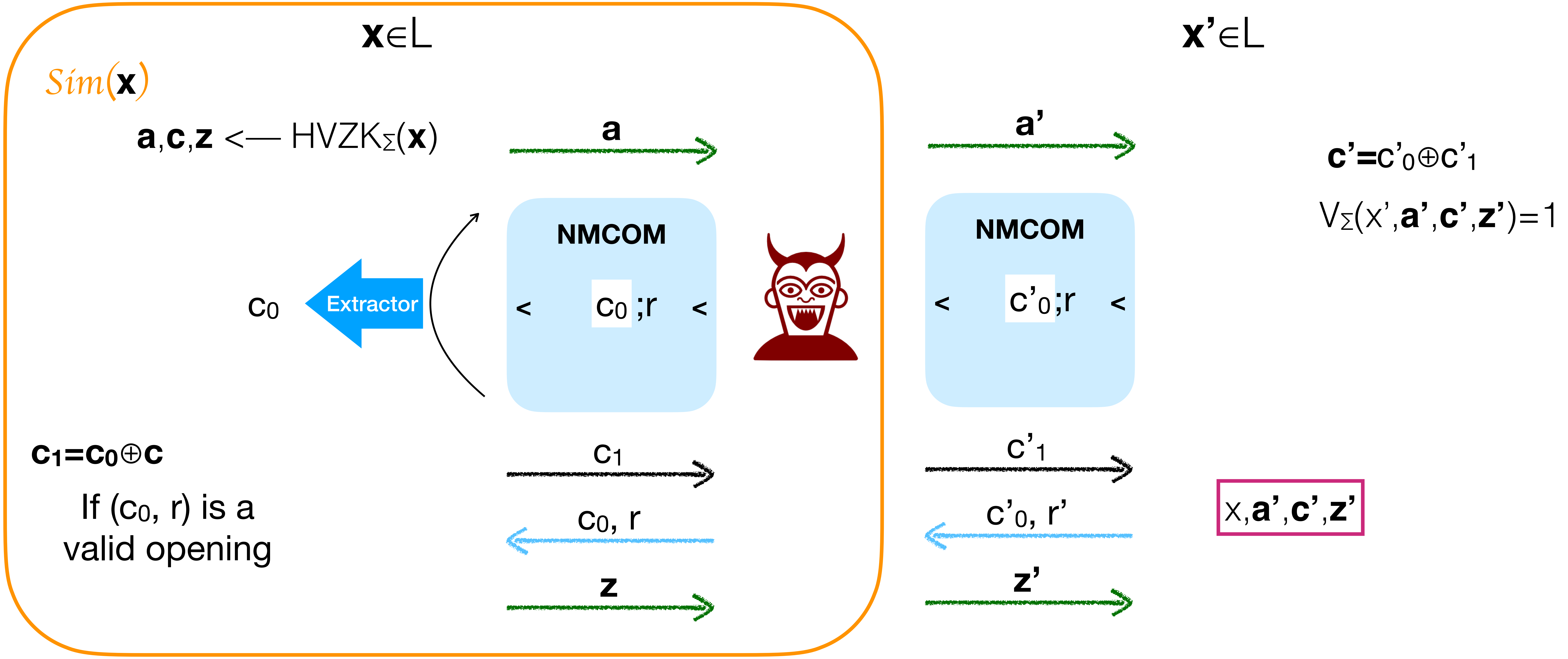
Non-Malleability



Non-Malleability



Non-Malleability



Non-Malleability

Non-Malleability

Non-Malleability

Non-Malleability

Non-Malleability

Non-Malleability

Non-Malleability

Non-Malleability

Non-Malleability

Non-Malleability

Non-Malleability

Non-Malleability

Non-Malleability

Non-Malleability

Non-Malleability

Hiding of NMCOM guarantees that c'≠c*

Non-Malleability

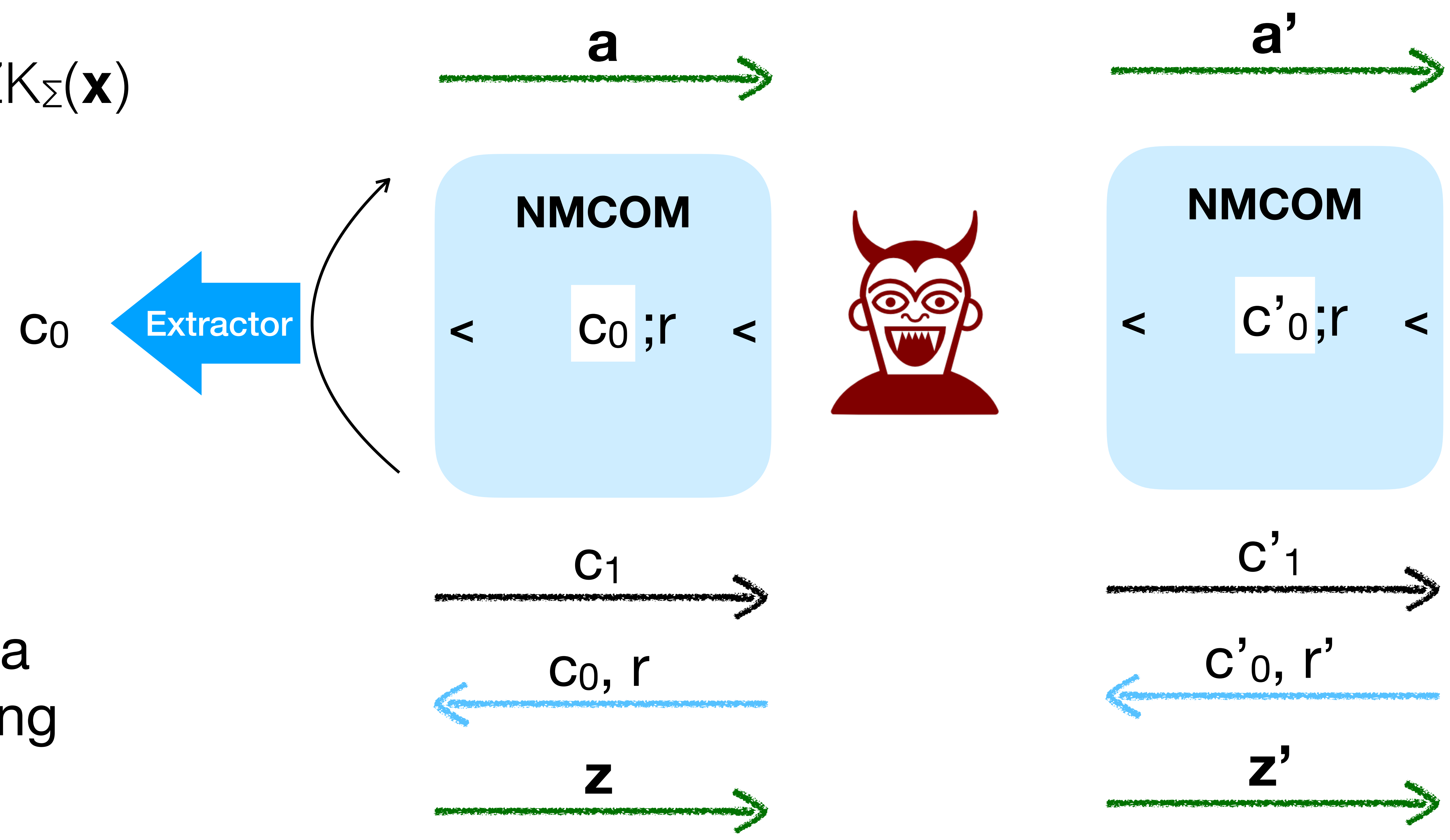
Hiding of NMCOM guarantees that $c' \neq c^*$

But we are running the extractor of NMCOM!

Reduction to non-malleability

$Sim(\mathbf{x})$

$\mathbf{a},\mathbf{c},\mathbf{z} \leftarrow HVZK_{\Sigma}(\mathbf{x})$



$\mathbf{c_1}=\mathbf{c_0}\oplus\mathbf{c}$

If (c_0, r) is a valid opening

$\mathbf{c'}=c'_0\oplus c'_1$

$V_{\Sigma}(x',\mathbf{a'},\mathbf{c'},\mathbf{z'})=1$

Reduction to non-malleability

$Sim(\mathbf{x})$

$\mathbf{a},\mathbf{c},\mathbf{z} \leftarrow \mathrm{HVZK}_{\Sigma}(\mathbf{x})$

a ⟶

a’ ⟶

$\mathbf{c'} = c'_0 \oplus c'_1$

$V_{\Sigma}(x', \mathbf{a'}, \mathbf{c'}, \mathbf{z'}) = 1$

Reduction to non-malleability

Sim(**x**)

a,**c**,**z** <— $HVZK_{\Sigma}$(**x**)

a

a'

Challenge messages

(m_0,m_1)

$\mathbf{c'} = c'_0 \oplus c'_1$

$V_{\Sigma}(x', \mathbf{a'}, \mathbf{c'}, \mathbf{z'}) = 1$

Reduction to non-malleability

Sim(**x**)

$\mathbf{a},\mathbf{c},\mathbf{z} <\!\!— HVZK_{\Sigma}(\mathbf{x})$

a

a'

NMCOM

< m_b ;r^* <

Challenge messages

(m_0,m_1)

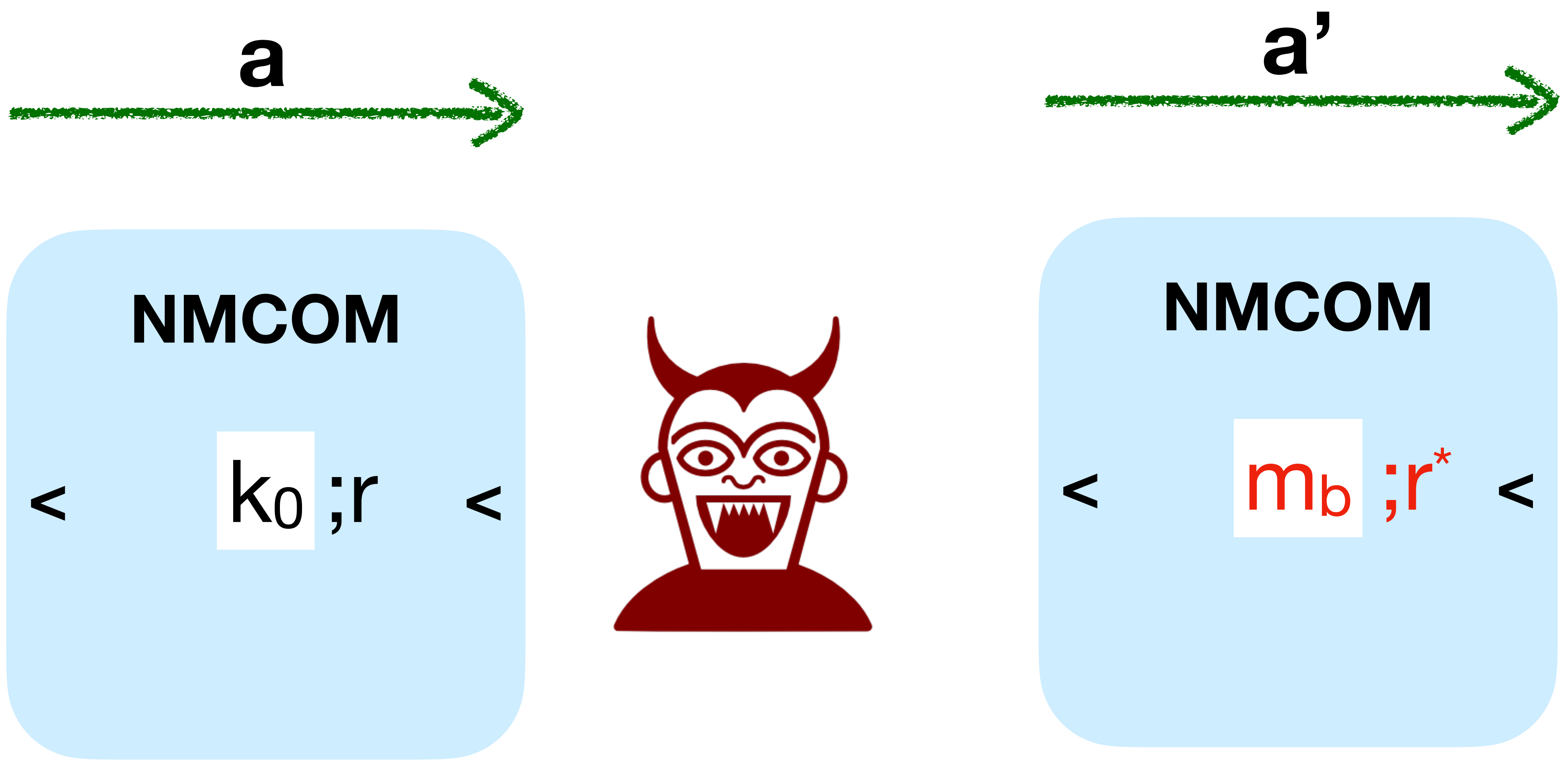
$\mathbf{c'}=c'_0 \oplus c'_1$

$V_{\Sigma}(x',\mathbf{a'},\mathbf{c'},\mathbf{z'})=1$

Reduction to non-malleability

Sim(**x**)

$\mathbf{a},\mathbf{c},\mathbf{z} \longleftarrow \mathrm{HVZK}_\Sigma(\mathbf{x})$



Challenge messages

(m_0,m_1)

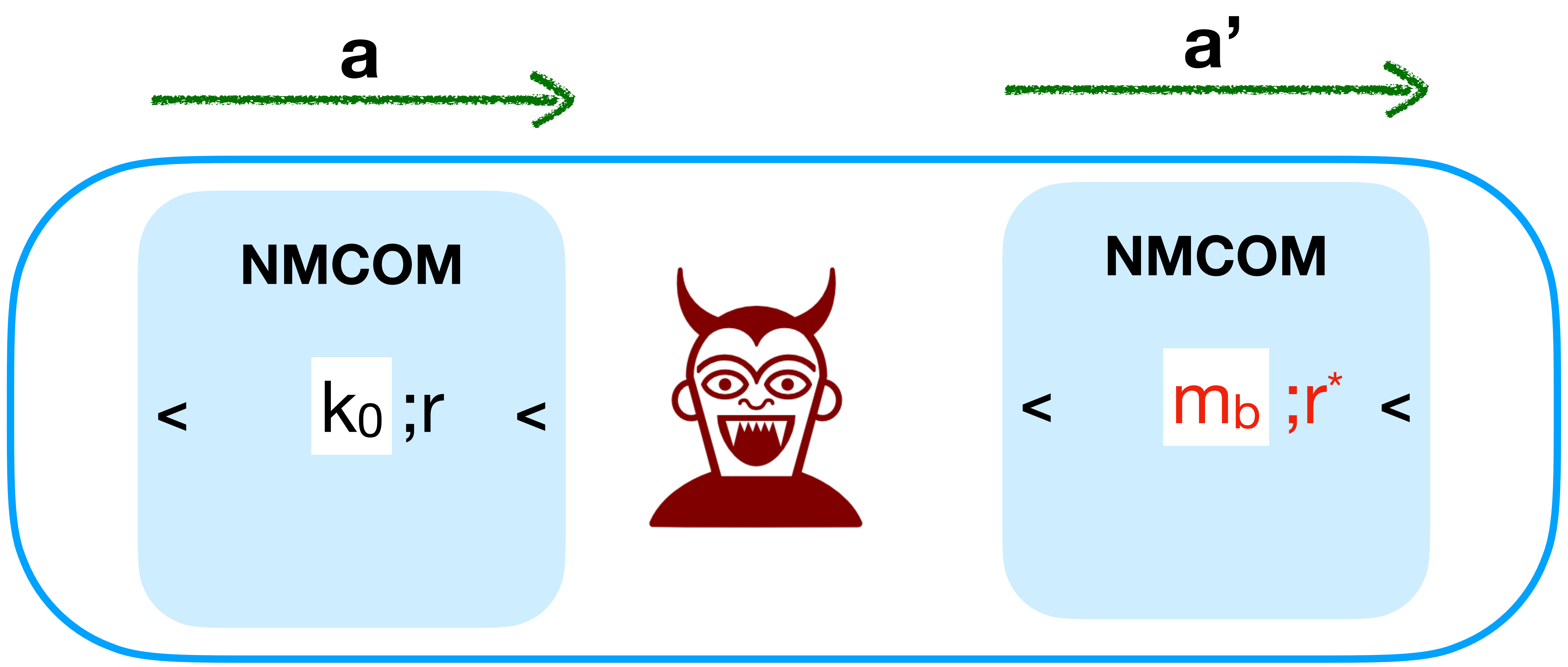
$\mathbf{c'} = c'_0 \oplus c'_1$

$V_\Sigma(x',\mathbf{a'},\mathbf{c'},\mathbf{z'})=1$

Reduction to non-malleability

Sim(**x**)

a,**c**,**z** <— HVZK$_\Sigma$(**x**)



Challenge messages

(m_0,m_1)

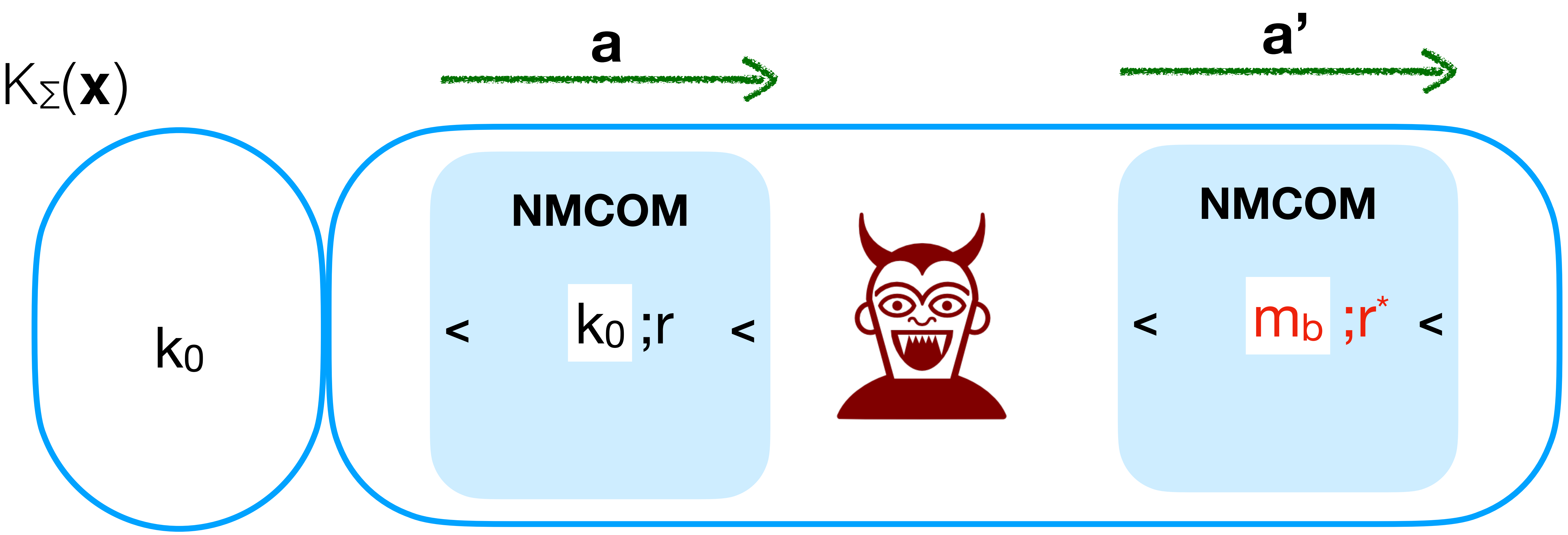
c'=c'$_0\oplus$c'$_1$

V$_\Sigma$(x',**a'**,**c'**,**z'**)=1

Reduction to non-malleability

$\mathit{Sim}(\mathbf{x})$

$\mathbf{a},\mathbf{c},\mathbf{z} \leftarrow \text{HVZK}_\Sigma(\mathbf{x})$



Challenge messages

(m_0,m_1)

$\mathbf{c'} = c'_0 \oplus c'_1$

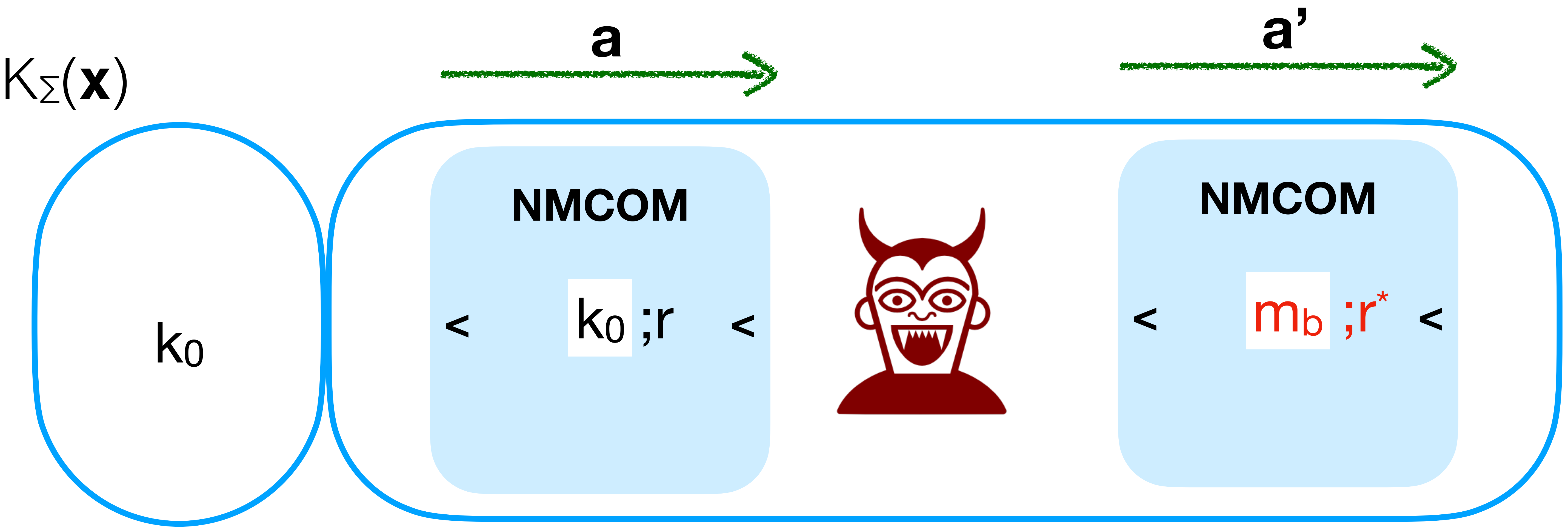
$V_\Sigma(x', \mathbf{a'}, \mathbf{c'}, \mathbf{z'}) = 1$

k_0 is an input to the distinguisher

Reduction to non-malleability

$\mathit{Sim}(\mathbf{x})$

$\mathbf{a},\mathbf{c},\mathbf{z} \longleftarrow \mathrm{HVZK}_{\Sigma}(\mathbf{x})$



$\mathbf{k_1=k_0 \oplus c}$

Challenge messages

(m_0,m_1)

$\mathbf{c'}=c'_0 \oplus c'_1$

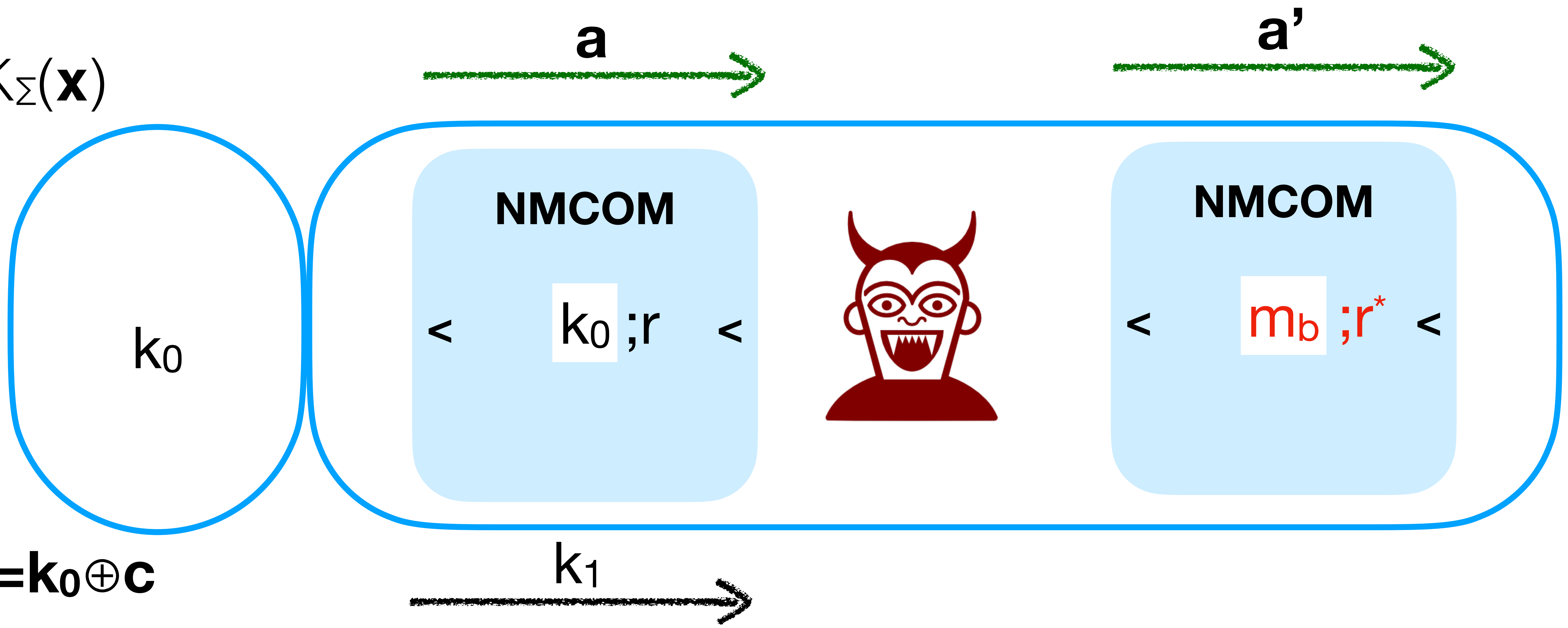
$V_{\Sigma}(x',\mathbf{a'},\mathbf{c'},\mathbf{z'})=1$

k_0 is an input to the distinguisher

Reduction to non-malleability

Sim(**x**)

$\mathbf{a},\mathbf{c},\mathbf{z} \leftarrow \mathrm{HVZK}_\Sigma(\mathbf{x})$



$\mathbf{k_1=k_0 \oplus c}$

Challenge messages

(m_0,m_1)

$\mathbf{c'}=c'_0 \oplus c'_1$

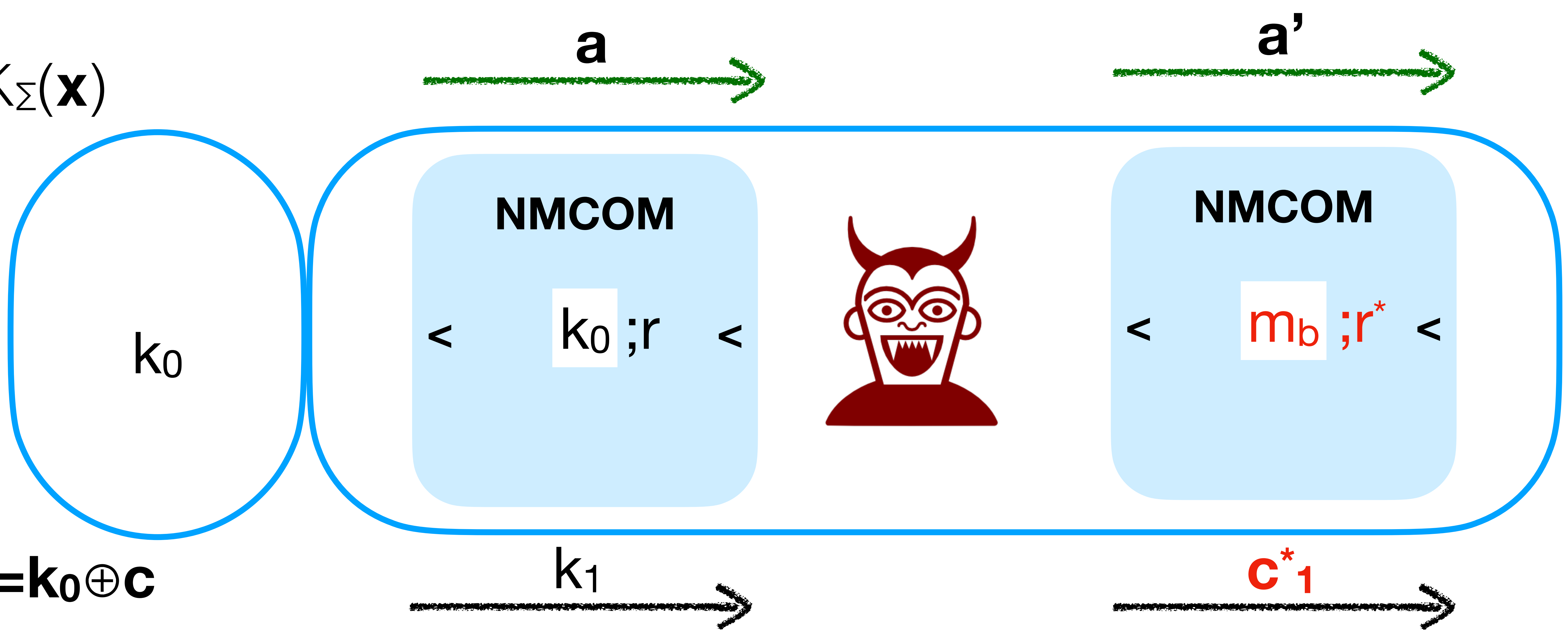
$V_\Sigma(x',\mathbf{a'},\mathbf{c'},\mathbf{z'})=1$

k_0 is an input to the distinguisher

Reduction to non-malleability

$\mathit{Sim}(\mathbf{x})$

$\mathbf{a},\mathbf{c},\mathbf{z} \leftarrow \text{HVZK}_\Sigma(\mathbf{x})$



Challenge messages

(m_0,m_1)

$\mathbf{k_1=k_0\oplus c}$

$\mathbf{c'}=c'_0\oplus c'_1$

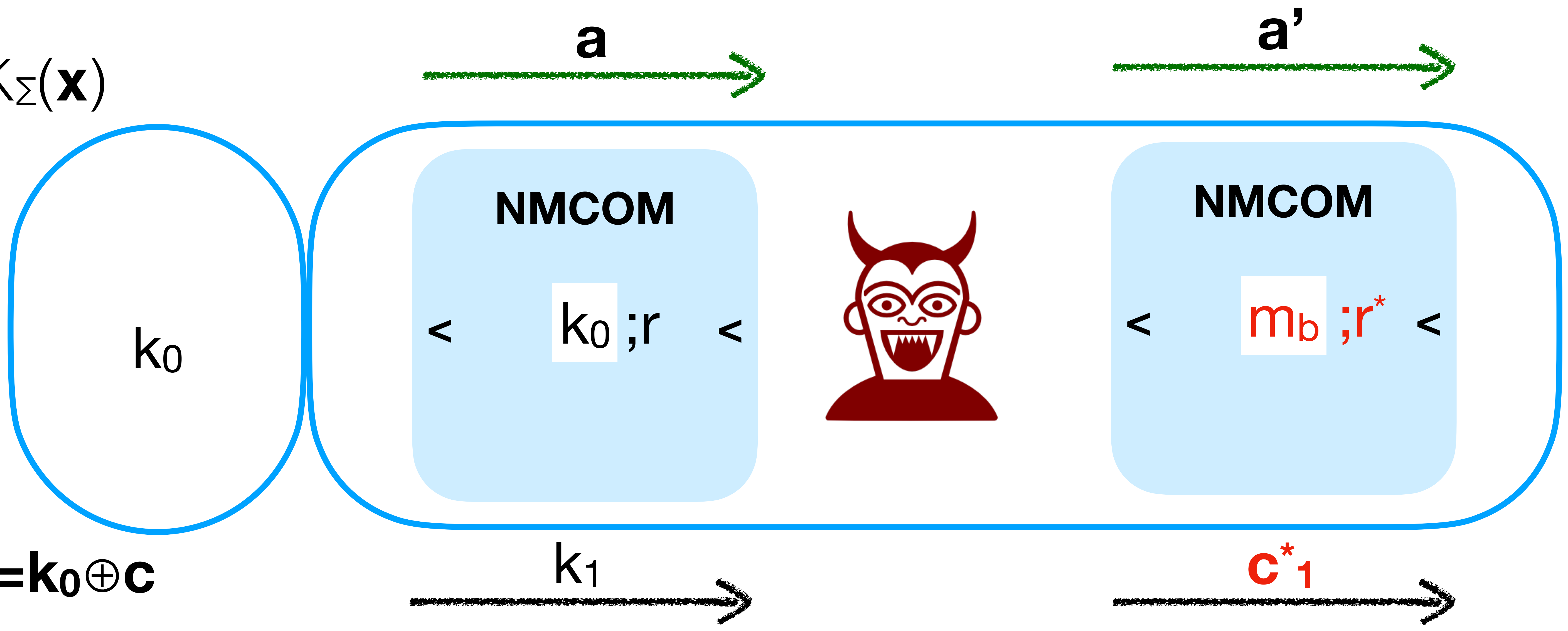
$V_\Sigma(x',\mathbf{a'},\mathbf{c'},\mathbf{z'})=1$

k_0 is an input to the distinguisher

Reduction to non-malleability

$Sim(\mathbf{x})$

$\mathbf{a},\mathbf{c},\mathbf{z} \leftarrow \mathrm{HVZK}_{\Sigma}(\mathbf{x})$



$\mathbf{k_1=k_0 \oplus c}$

Challenge messages

(m_0,m_1)

$\mathbf{c'}=c'_0 \oplus c'_1$

$V_{\Sigma}(x',\mathbf{a'},\mathbf{c'},\mathbf{z'})=1$

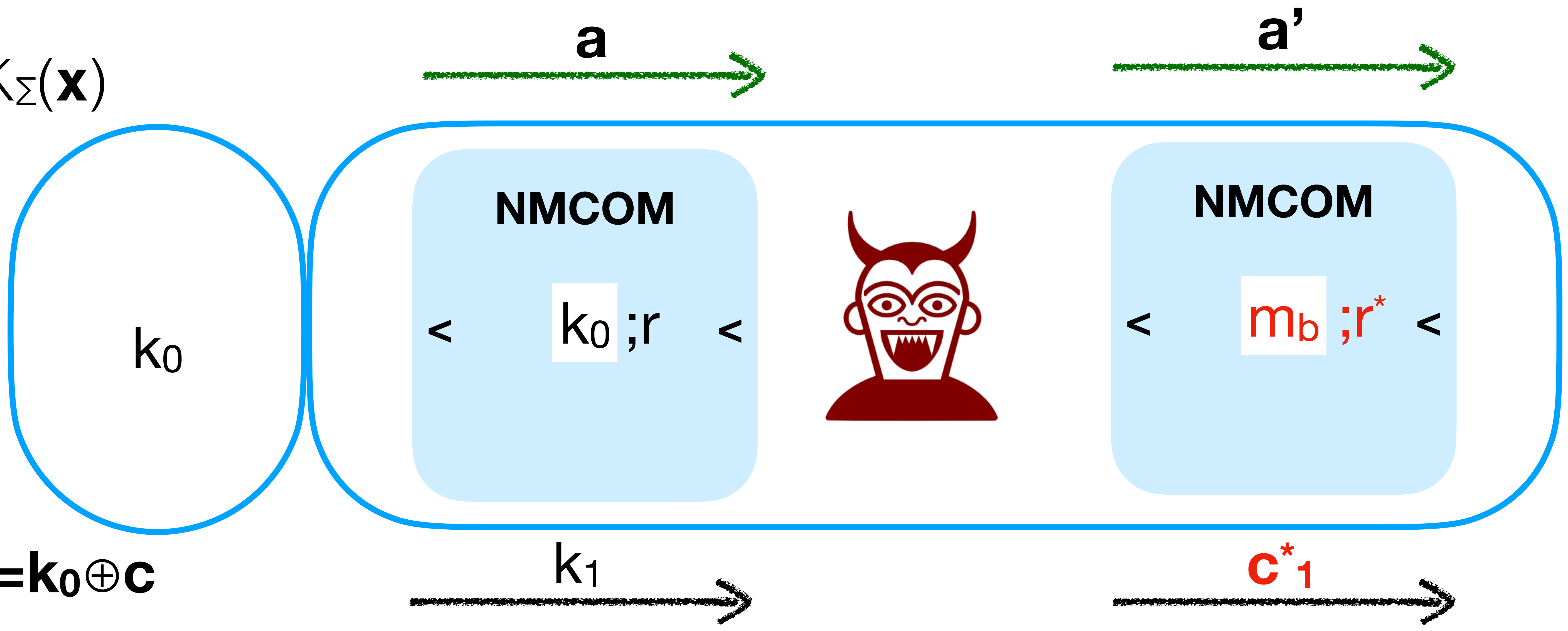
k_0 is an input to the distinguisher

With high probability $c'=c^*$ —>

Reduction to non-malleability

$\mathit{Sim}(\mathbf{x})$

$\mathbf{a},\mathbf{c},\mathbf{z} \leftarrow \text{HVZK}_\Sigma(\mathbf{x})$



$\mathbf{k_1=k_0\oplus c}$

Challenge messages

(m_0,m_1)

$\mathbf{c'}=c'_0\oplus c'_1$

$V_\Sigma(x',\mathbf{a'},\mathbf{c'},\mathbf{z'})=1$

k_0 is an input to the distinguisher

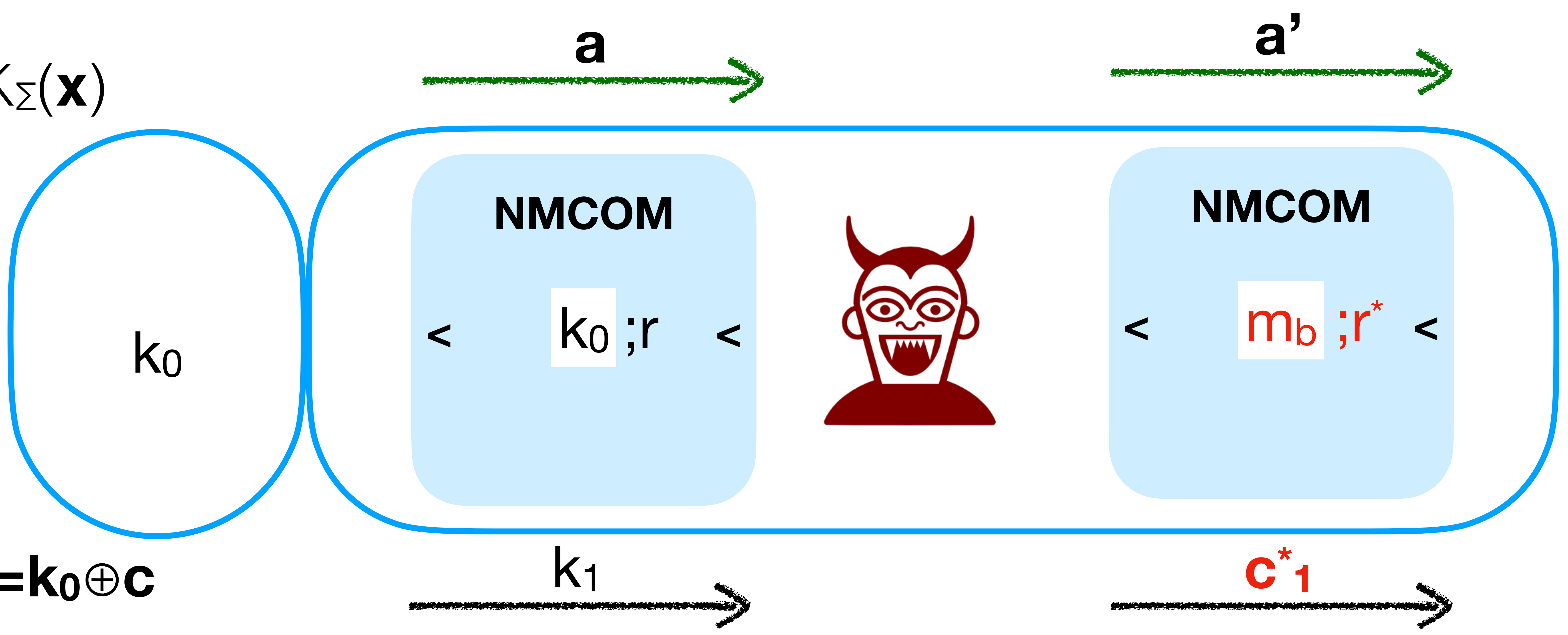
With high probability $c'=c^*$ —>

$c'_0\oplus c'_1=\mathbf{c'}=\mathbf{c^*}=m_b\oplus c^*_1$ —>

Reduction to non-malleability

$\mathit{Sim}(\mathbf{x})$

$\mathbf{a},\mathbf{c},\mathbf{z} \leftarrow \text{HVZK}_\Sigma(\mathbf{x})$



$\mathbf{k_1=k_0\oplus c}$

Challenge messages

(m_0,m_1)

$\mathbf{c'}=c'_0\oplus c'_1$

$V_\Sigma(x',\mathbf{a'},\mathbf{c'},\mathbf{z'})=1$

k_0 is an input to the distinguisher

With high probability $c'=c^*$ —>

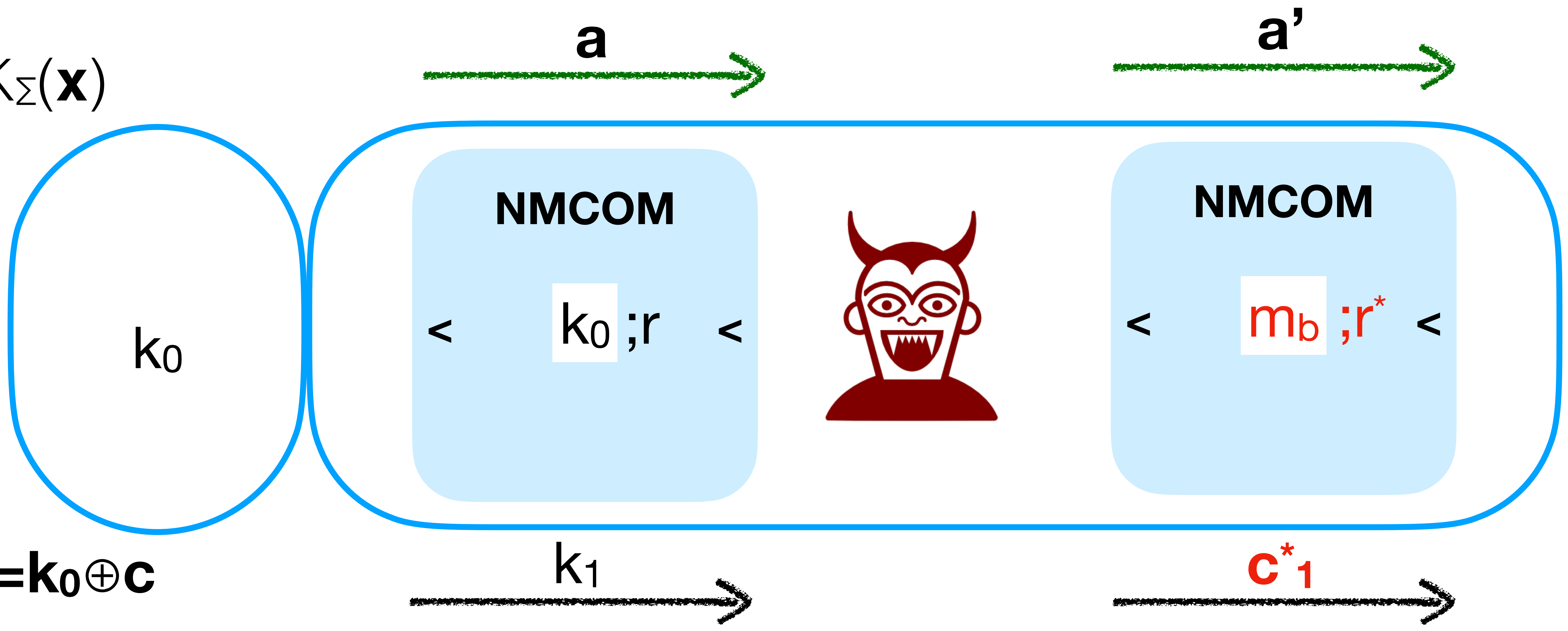
$c'_0\oplus c'_1=\mathbf{c'}=\mathbf{c^*}=m_b\oplus c^*_1$ —>

$c'_0\oplus c'_1=m_b\oplus c^*_1$ —>

Reduction to non-malleability

Sim(**x**)

a,**c**,**z** <— HVZK$_\Sigma$(**x**)



k_1=k_0⊕c

Challenge messages

(m_0,m_1)

c'=c'$_0$⊕c'$_1$

V$_\Sigma$(x',**a'**,**c'**,**z'**)=1

k_0 is an input to the distinguisher

With high probability c'=c^* —>

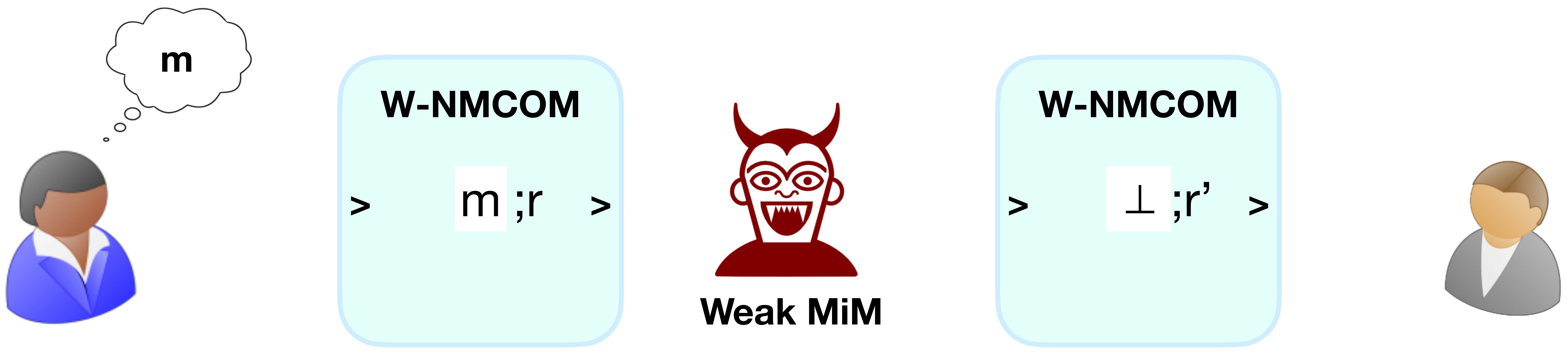
c'$_0$⊕c'$_1$=**c'**= **c^***=m_b⊕c^*_1 —>

c'$_0$⊕c'$_1$=m_b⊕c^*_1 —>

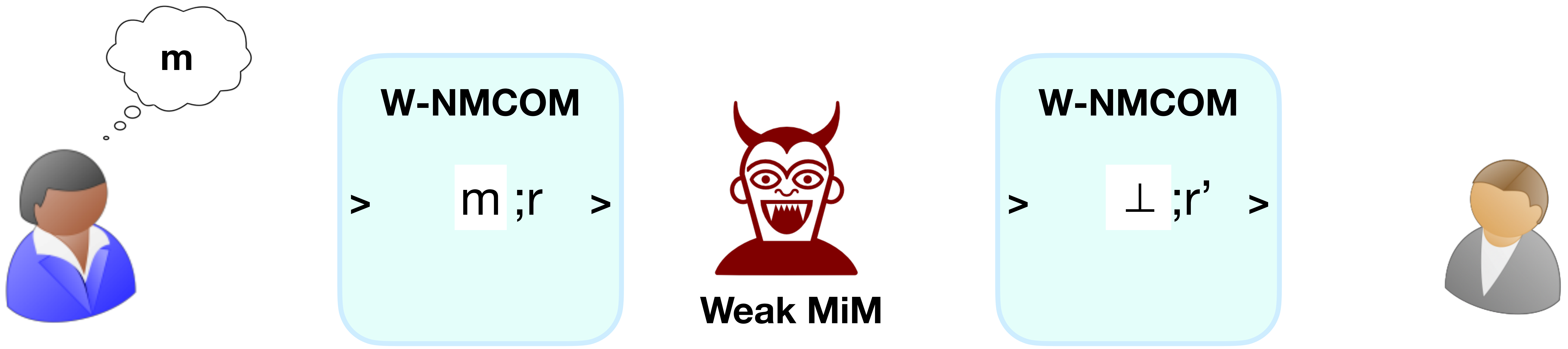
m_b=c'$_0$⊕c'$_1$⊕c^*_1

Weak Non-Malleable Commitments

Weak Non-Malleable Commitments



Weak Non-Malleable Commitments



[BGR+15] Hai Brenner, Vipul Goyal, Silas Richelson, Alon Rosen, and Margarita Vald. Fast non-malleable commitments. CCS 2015
[GRRV14] Vipul Goyal, Silas Richelson, Alon Rosen, and Margarita Vald. FOCS 2014

Weak non-malleability may suffice

$\mathbf{a} \leftarrow P_{\Sigma}(x,w)$

$\mathbf{a}$ →

NMCOM

< c_0 ;r <

If (c_0, r) is a valid opening

c_1 →

← c_0, r

$\mathbf{c = c_0 \oplus c_1}$

$z \leftarrow P_{\Sigma}(x,w,\mathbf{c})$

$\mathbf{z}$ →

$V_{\Sigma}(x,a,c,z)=1$

Weak non-malleability may suffice

$\mathbf{a} \longleftarrow P_{\Sigma}(x,w)$

$\mathbf{a}$ →

W-NMCOM

< c_0 ;r <

If (c_0, r) is a valid opening

c_1 →

← c_0, r

$\mathbf{c}=\mathbf{c}_0\oplus\mathbf{c}_1$

$z \longleftarrow P_{\Sigma}(x,w,\mathbf{c})$

$\mathbf{z}$ →

$V_{\Sigma}(x,a,c,z)=1$

Conclusions and Open Questions

Conclusions and Open Questions

- Black-box practical non-malleable zero-knowledge scheme

Conclusions and Open Questions

- Black-box practical non-malleable zero-knowledge scheme
- Minimal assumptions, and practical

Conclusions and Open Questions

- Black-box practical non-malleable zero-knowledge scheme
- Minimal assumptions, and practical
- Plug and play with any sigma-protocol*
  - Schnorr's protocol
  - ZKBoo/ZKB++ [GMO16, CDG+17]

[GMO16] Irene Giacomelli, Jesper Madsen, and Claudio Orlandi. ZKBoo: Faster zero-knowledge for Boolean circuits. USENIX 2016

[CDG+17] Melissa Chase, David Derler, Steven Goldfeder, Claudio Orlandi, Sebastian Ramacher, Christian Rechberger, Daniel Slamanig, and Greg Zaverucha. Post-quantum zero-knowledge and signatures from symmetric-key primitives. CCS 2017

Conclusions and Open Questions

- Black-box practical non-malleable zero-knowledge scheme
- Minimal assumptions, and practical
- Plug and play with any sigma-protocol*
  - Schnorr's protocol
  - ZKBoo/ZKB++ [GMO16, CDG+17]
- Can we match the lower bound (4 rounds) of BB zero-knowledge?

[GMO16] Irene Giacomelli, Jesper Madsen, and Claudio Orlandi. ZKBoo: Faster zero-knowledge for Boolean circuits. USENIX 2016

[CDG+17] Melissa Chase, David Derler, Steven Goldfeder, Claudio Orlandi, Sebastian Ramacher, Christian Rechberger, Daniel Slamanig, and Greg Zaverucha. Post-quantum zero-knowledge and signatures from symmetric-key primitives. CCS 2017

Conclusions and Open Questions

- Black-box practical non-malleable zero-knowledge scheme
- Minimal assumptions, and practical
- Plug and play with any sigma-protocol*
  - Schnorr's protocol
  - ZKBoo/ZKB++ [GMO16, CDG+17]
- Can we match the lower bound (4 rounds) of BB zero-knowledge?
- Adaptive input, parallel/concurrent composition

[GMO16] Irene Giacomelli, Jesper Madsen, and Claudio Orlandi. ZKBoo: Faster zero-knowledge for Boolean circuits. USENIX 2016

[CDG+17] Melissa Chase, David Derler, Steven Goldfeder, Claudio Orlandi, Sebastian Ramacher, Christian Rechberger, Daniel Slamanig, and Greg Zaverucha. Post-quantum zero-knowledge and signatures from symmetric-key primitives. CCS 2017

Thanks