NIZKs with an untrusted CRS: Security in the face of parameter subversion

Mihir Bellare

Georg Fuchsbauer

Alessandra Scafuro

Asiacrypt 2016

Motivation

- 2013

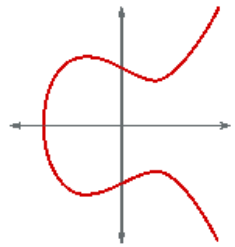
- compromised security not covered by standard model
- here: **parameter subversion**

Motivation

- 2013

- compromised security not covered by standard model
- here: **parameter subversion**

- example: *Dual EC* RNG



  - "trusted" parameters P, Q
  - int'l standard; NSA paid RSA $10 million
  - knowledge of $\log_Q P \Rightarrow$ predictable [ShuFer07]
    $\Rightarrow$ break TLS [CFN+14]

Motivation

- 2013

- compromised security not covered by standard model
- here: **parameter subversion**

- goal: **subversion resistance**
- this work: NIZK, relies on common reference string (CRS)
- example: zk-SNARK parameters
  for Zerocash (ZCASH) [BCG+14]

Related work

NIZK

- 2-move ZK protocols [BLV03, Pass03, BP04, BCPR14]
- NIZK in bare PK model [Wee07]
- CRS via multiparty computation [KKZZ14, BSCG$^+$15]
- UC w/ adv. CRS [CPs07], multiple CRSs [GO07, GGJS11]

Related work

NIZK

- 2-move ZK protocols [BLV03, Pass03, BP04, BCPR14]
- NIZK in bare PK model [Wee07]
- CRS via multiparty computation [KKZZ14, BSCG$^+$15]
- UC w/ adv. CRS [CPs07], multiple CRSs [GO07, GGJS11]

Subversion

- Algorithm-substitution attacks [BPR14, AMV15]
- Kleptography [YY96, YY97], cliptography [RTYZ16]
- Backdoored blockciphers [RP97, PG97, Pat99]

Non-interactive proofs

- let $L \in \mathcal{NP}$
- prove $x \in L$

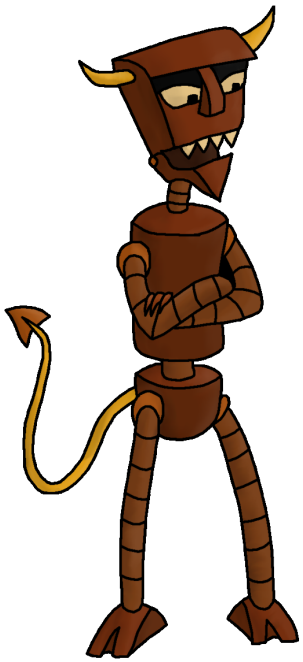
π

✓ / ×

Prover: x, w

Verifier: x

Non-interactive proofs



π

Soundness:

$\pi \checkmark \Rightarrow x \in L$

Prover: x, w

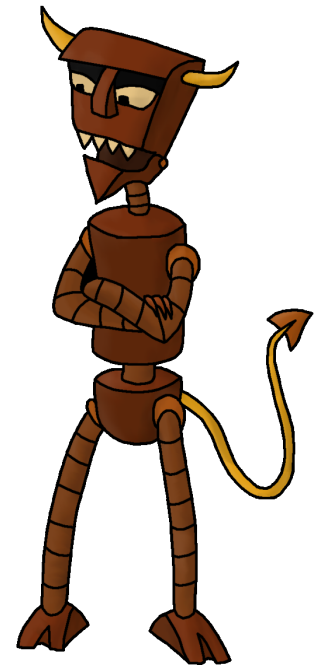
Verifier: x

Non-interactive proofs

π

Witness-indistinguishability:

$$\pi[w] \approx_c \pi[w']$$

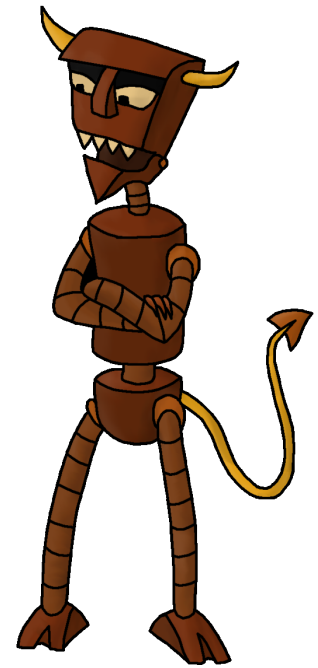


Prover: x, w

Verifier: x

Non-interactive proofs

π



Zero-knowledge:

crs'

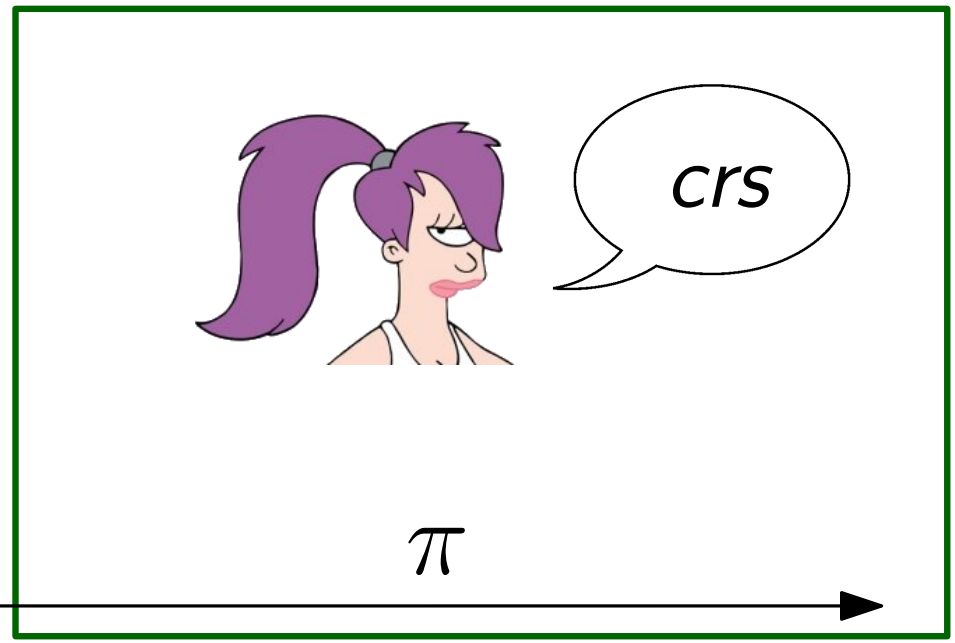
π'

Simulator: $x, \not{w}$

Prover: x, w

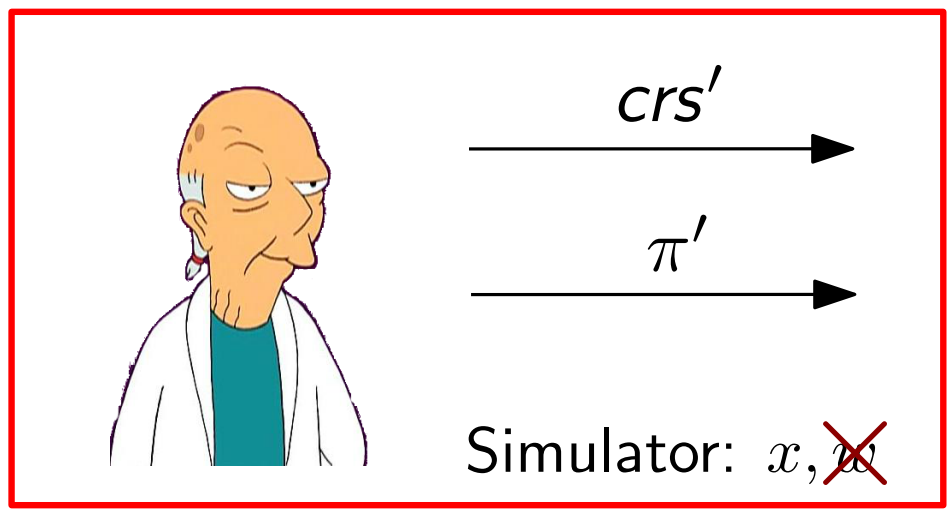
Verifier: x

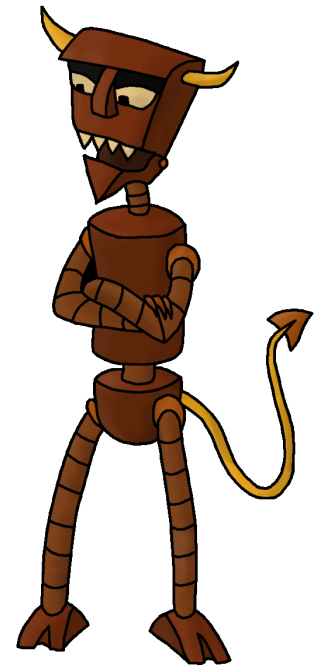
Non-interactive proofs



Prover: x, w

Zero-knowledge: $\approx_s$





Verifier: x

Subversion-resistant NI proofs

crs

π

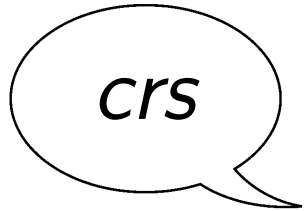
Subversion Soundness:

$\pi \checkmark \Rightarrow x \in L$

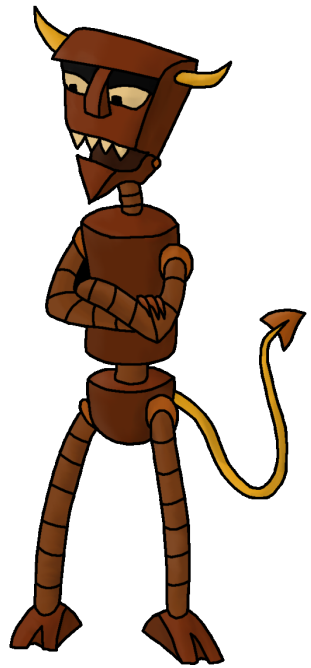
Prover: x, w

Verifier: x

Subversion-resistant NI proofs



π



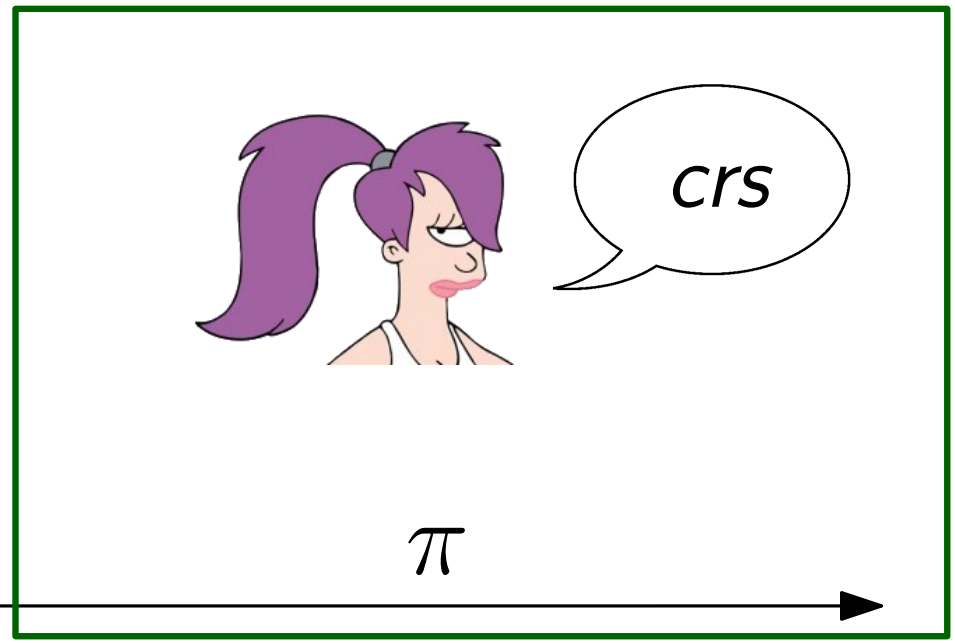
Subversion WI:

$$\pi[w] \approx_c \pi[w']$$

Prover: x, w

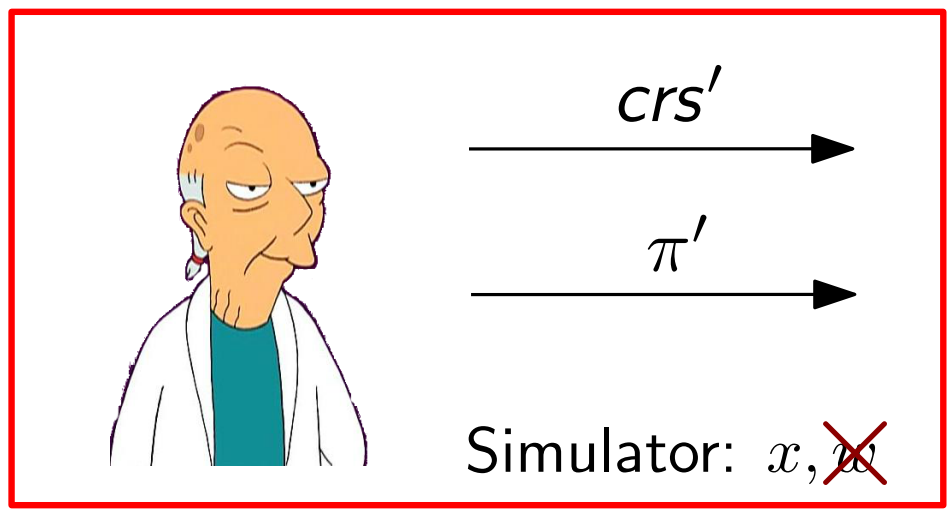
Verifier: x

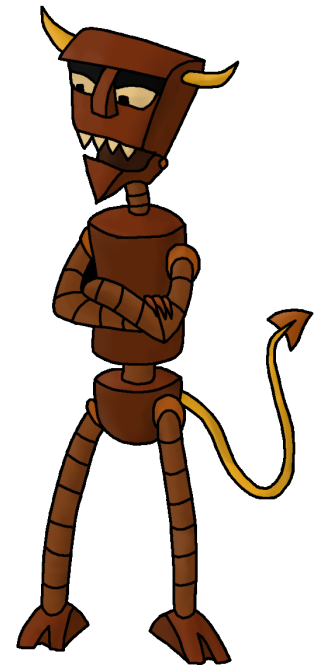
Non-interactive proofs



Prover: x, w

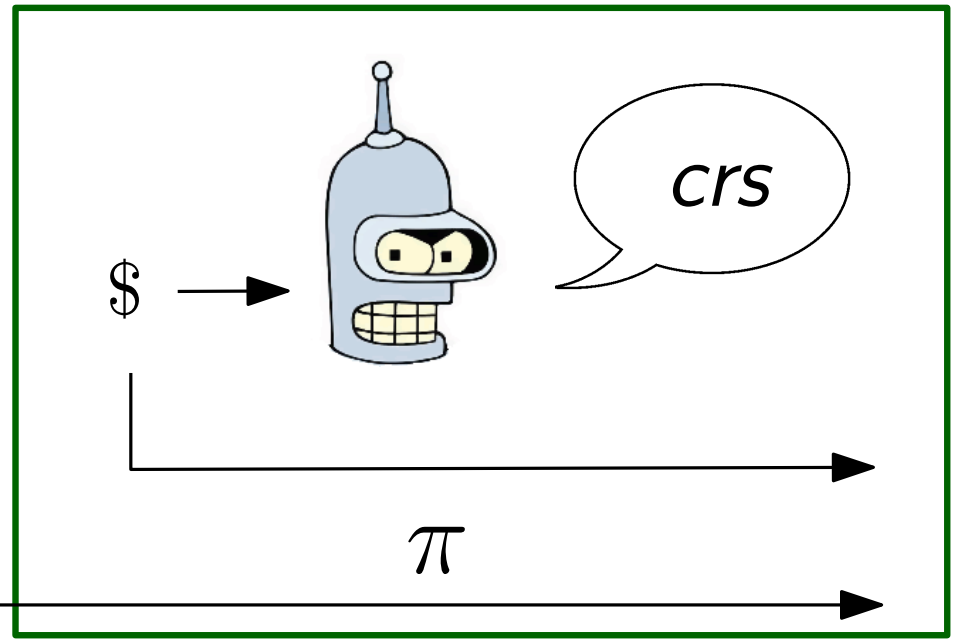
Zero-knowledge: $\approx_s$





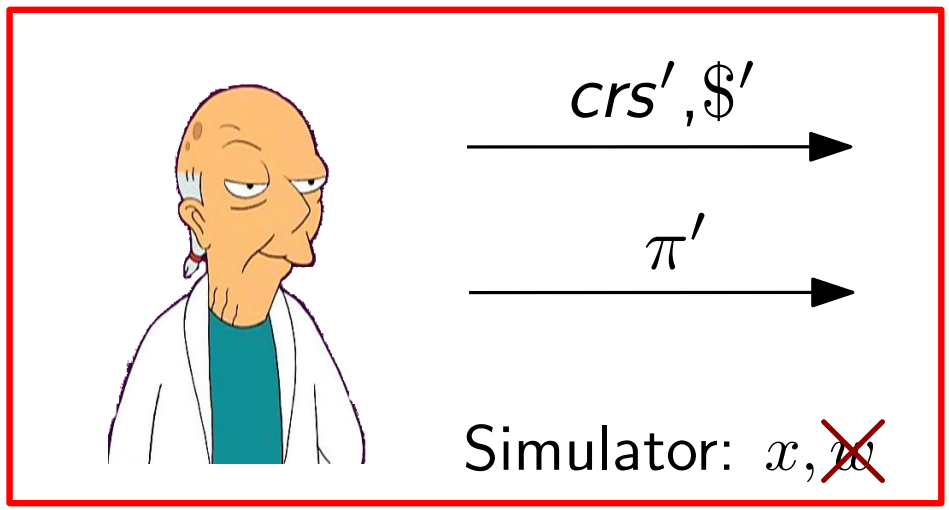
Verifier: x

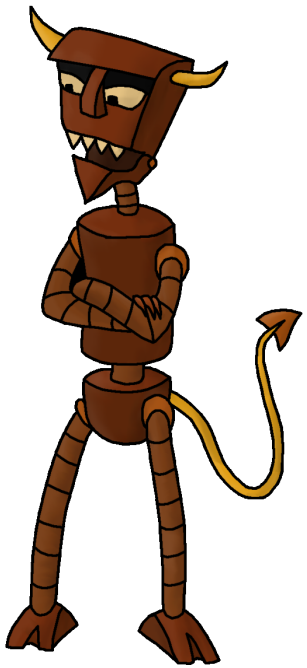
Subversion-resistant NI proofs



Prover: x, w

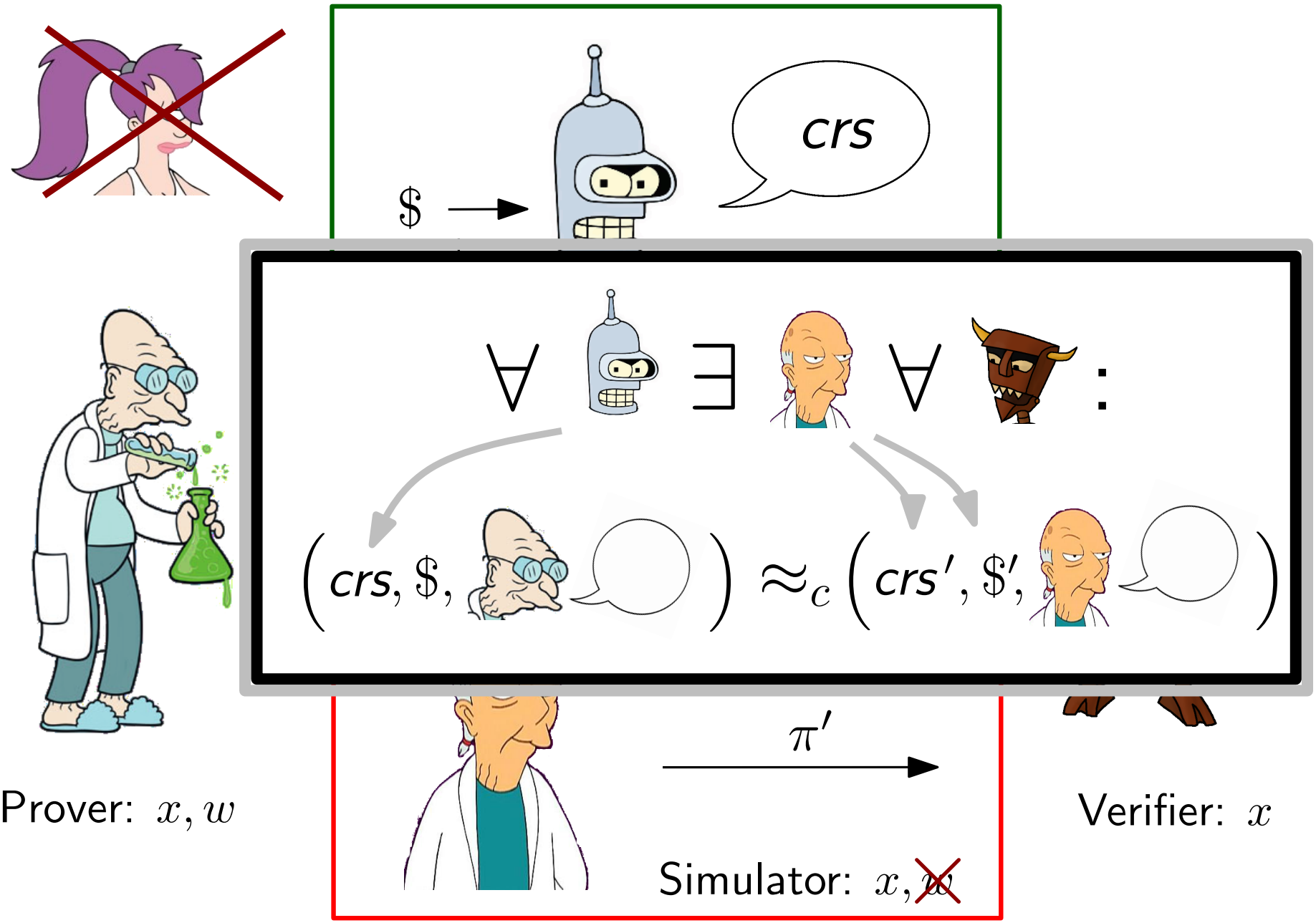
Subversion ZK: $\approx_s$



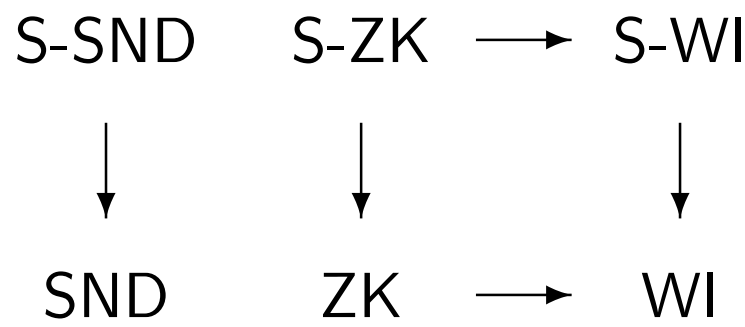


Verifier: x

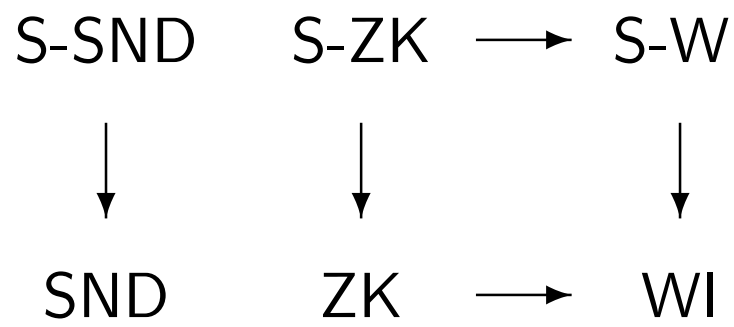
Subversion-resistant NI proofs



Our results



Our results



Our results

Standard			Subversion-resistant			Possible?	Assumpt's:
SND	ZK	WI	S-SND	S-ZK	S-WI		

Our results

Standard			Subversion-resistant			Possible?	Assumpt's:
SND	ZK	WI	S-SND	S-ZK	S-WI		
				•		✓	—

$\mathcal{E}$

✓

Prover: x, w

Verifier: x

Our results

Standard			Subversion-resistant			Possible?	Assumpt's:
SND	ZK	WI	S-SND	S-ZK	S-WI		
			•			✓	—

w

w witness for x?

Prover: x, w

Verifier: x

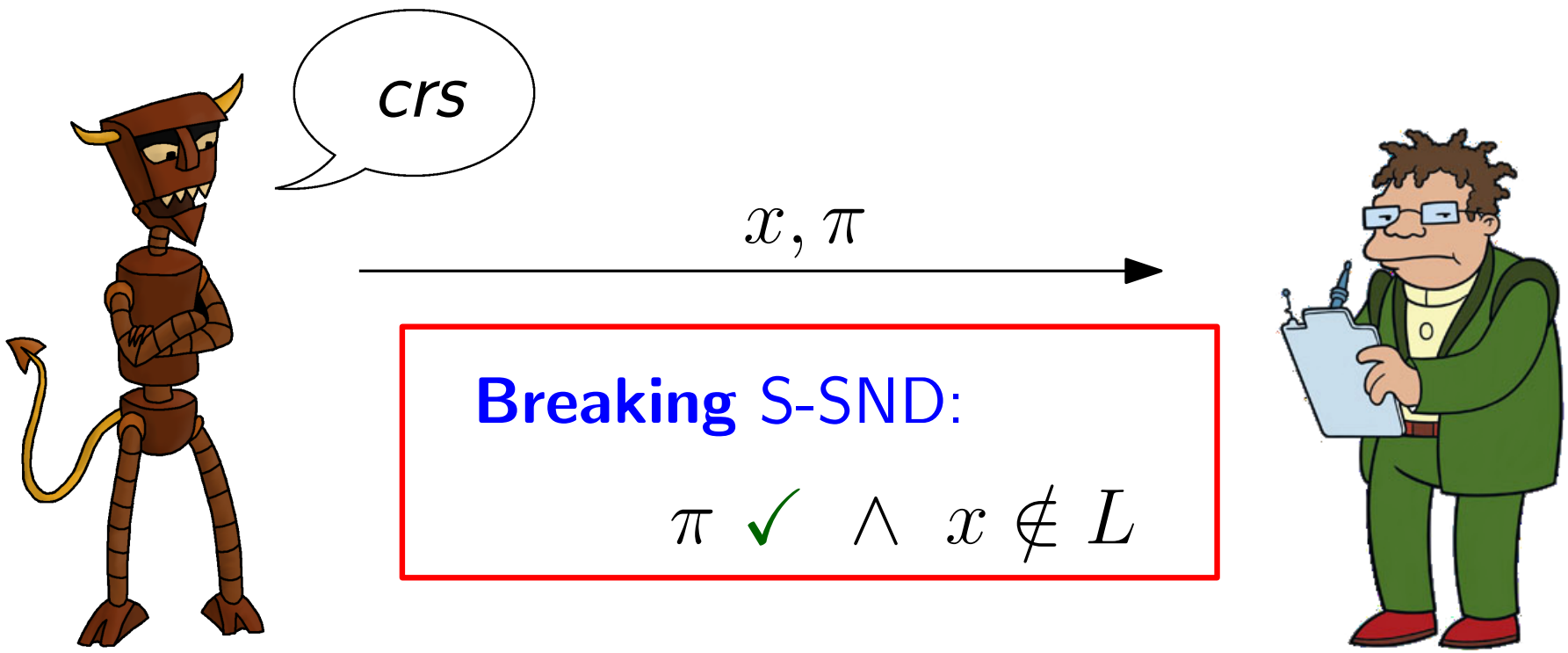
Our results

Standard			Subversion-resistant			Possible?	Assumpt's:
SND	ZK	WI	S-SND	S-ZK	S-WI		
•	•	•	**?**	**?**	**?**		

Our results

Standard			Subversion-resistant			Possible?	Assumpt's:
SND	ZK	WI	S-SND	S-ZK	S-WI		
	•		•			✗	

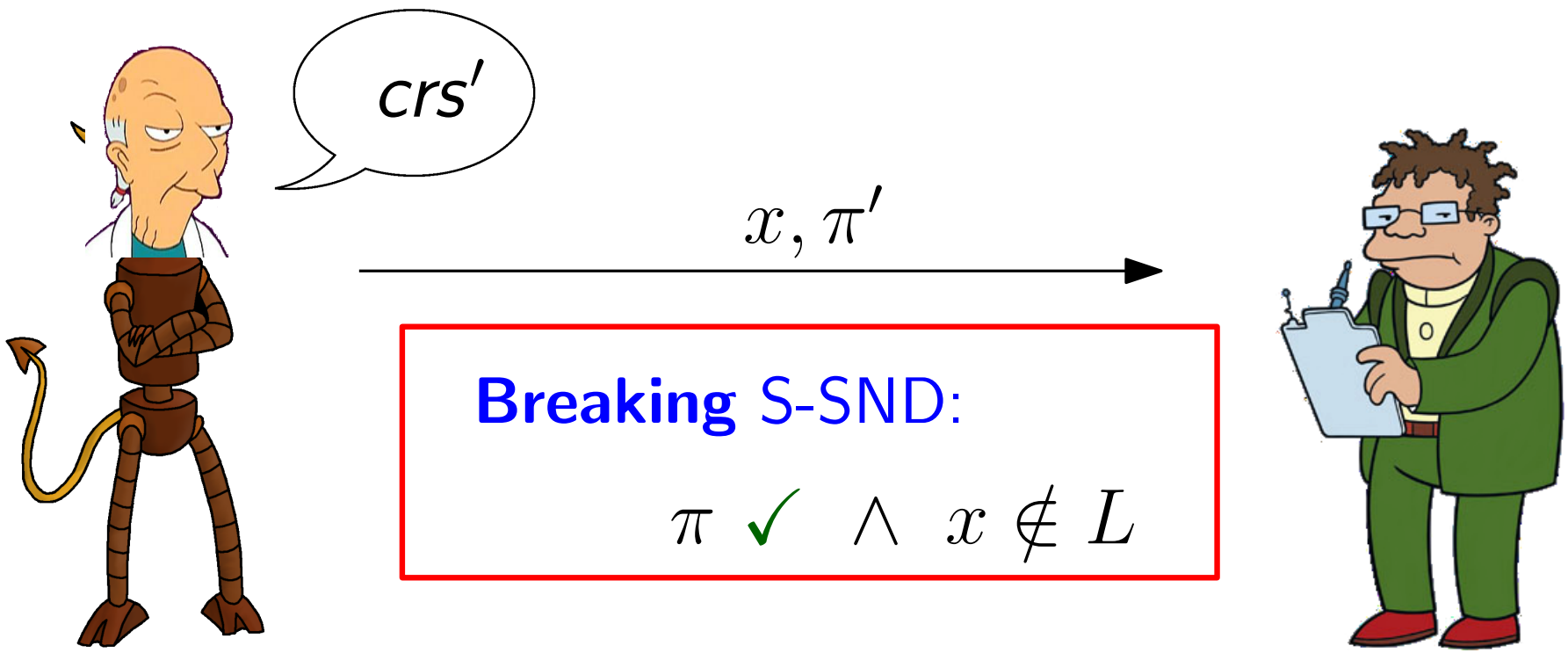
(if L is non-trivial)



Our results

Standard			Subversion-resistant			Possible?	Assumpt's:
SND	ZK	WI	S-SND	S-ZK	S-WI		
	•		•			✗	

(if L is non-trivial)



Our results

Standard			Subversion-resistant			Possible?	Assumpt's:
SND	ZK	WI	S-SND	S-ZK	S-WI		
	•		•			×	
•		•	•		•	?	

Our results

Standard			Subversion-resistant			Possible?	Assumpt's:
SND	ZK	WI	S-SND	S-ZK	S-WI		
	•		•			✗	
•		•	•		•	✓	DLin

Non-interactive Zaps [GOS06]

- NI WI proofs
- without CRS

No CRS $\Rightarrow$ subversion-resistant

Our results

Standard			Subversion-resistant			Possible?	Assumpt's:
SND	ZK	WI	S-SND	S-ZK	S-WI		
	•		•			✗	
•		•	•		•	✓	DLin
•	•	•		•	•	?	

Our results

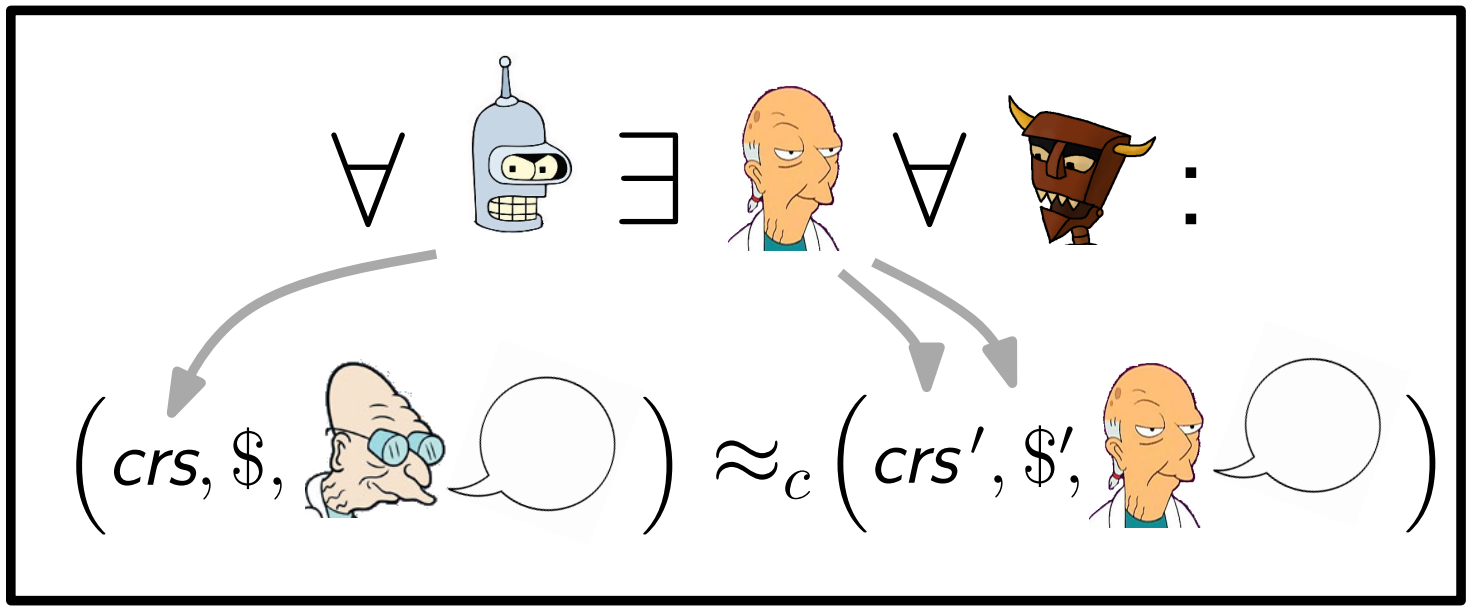
Standard			Subversion-resistant			Possible?	Assumpt's:
SND	ZK	WI	S-SND	S-ZK	S-WI		
	•		•			✗	
•		•	•		•	✓	DLin
•	•	•		•	•	?	

- implies 2-move ZK (verifier chooses CRS)

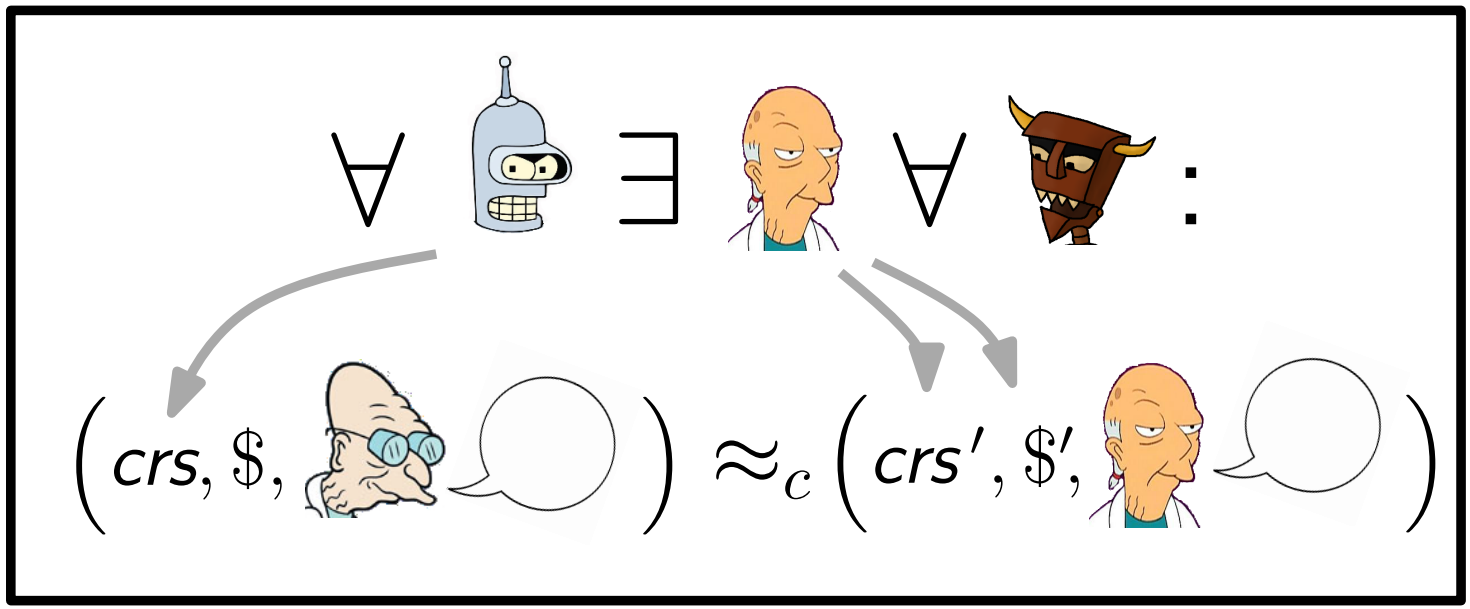
  $\Rightarrow$ only achieved under extractability assumpt's [BCPR14]

- construction under new *knowledge of exponent* assumption

Achieving SND + S-ZK

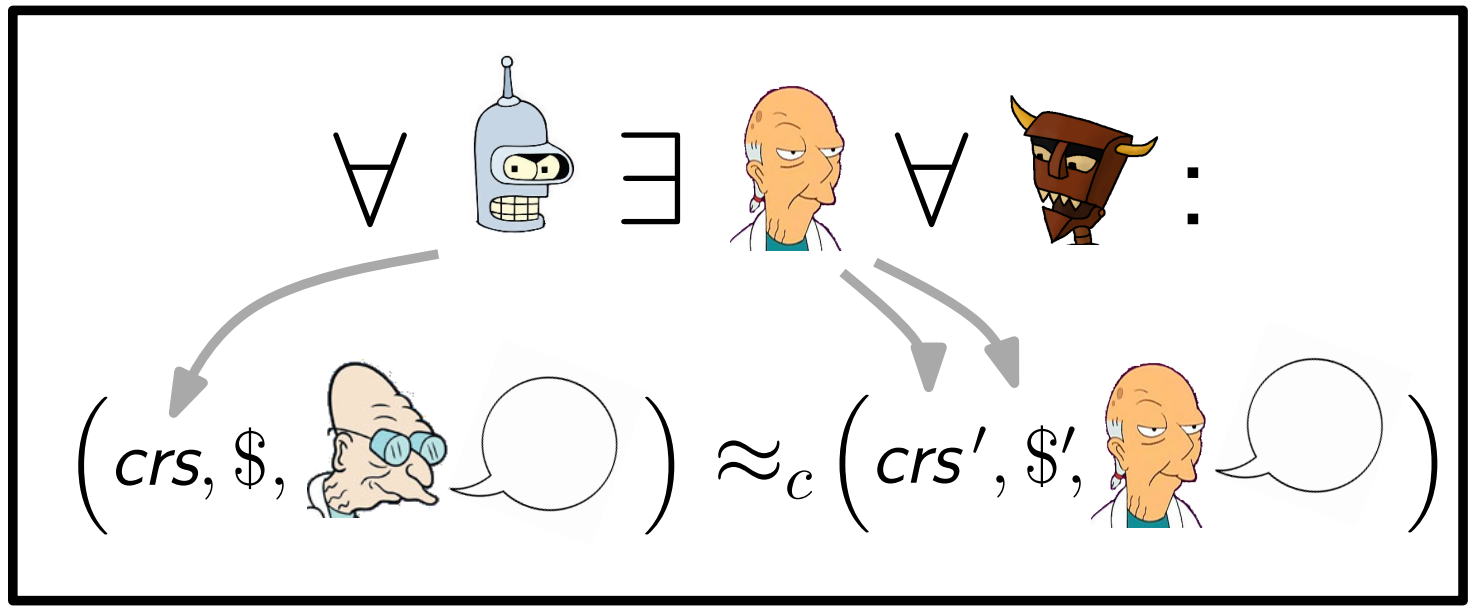


Achieving SND + S-ZK



KEA: $\forall$ $(g, h) \rightarrow$ $\rightarrow (g^s, h^s)$

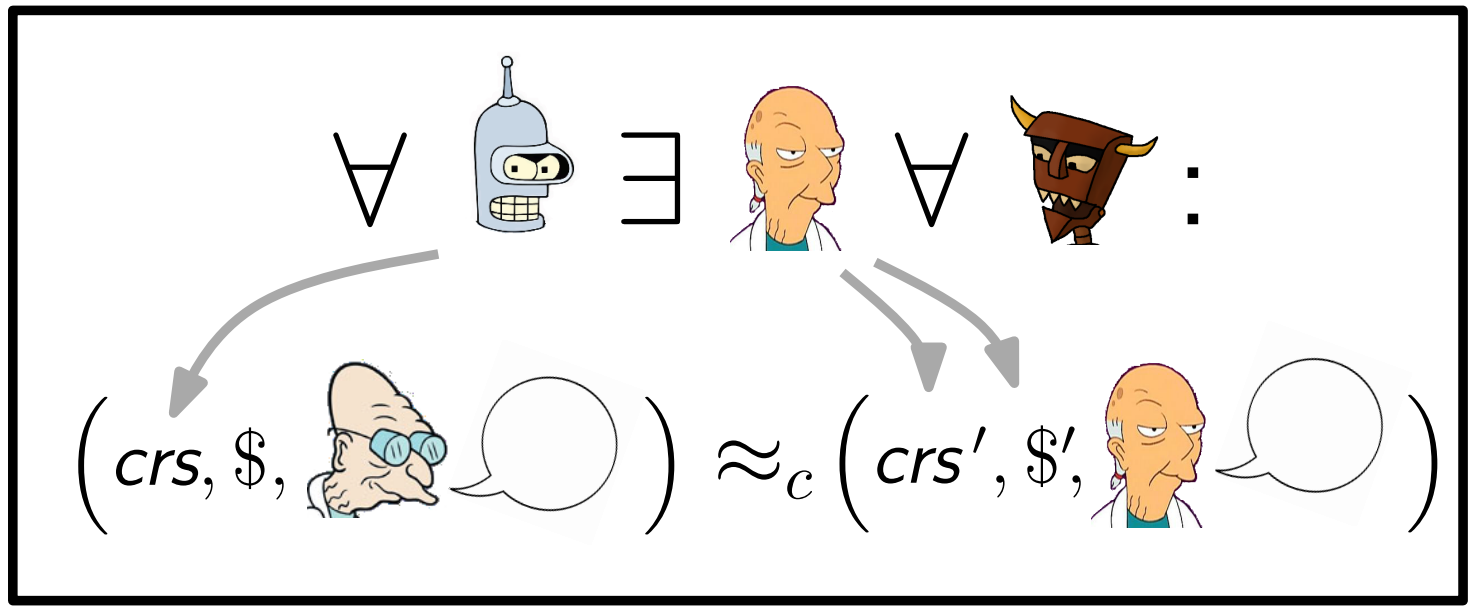
Achieving SND + S-ZK



KEA: $\forall$ $(g, h) \rightarrow$ $\rightarrow (g^s, h^s)$

$\exists$ $\hookrightarrow$ $\rightarrow s$

Achieving SND + S-ZK



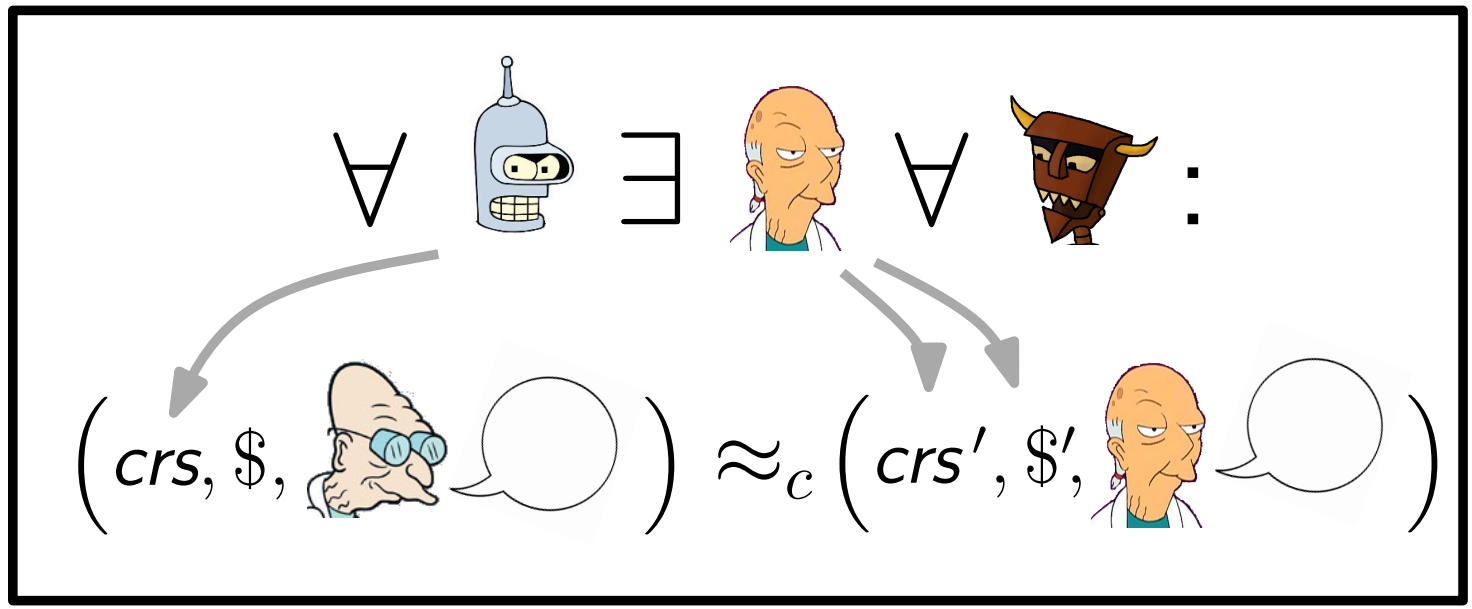
KEA: $\forall$ $(g, h) \rightarrow$ $\rightarrow (g^s, h^s)$

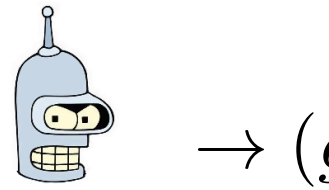
$\exists$ $\rightarrow$ $\rightarrow s$

idea:

- *crs*
- trapdoor

Achieving SND + S-ZK





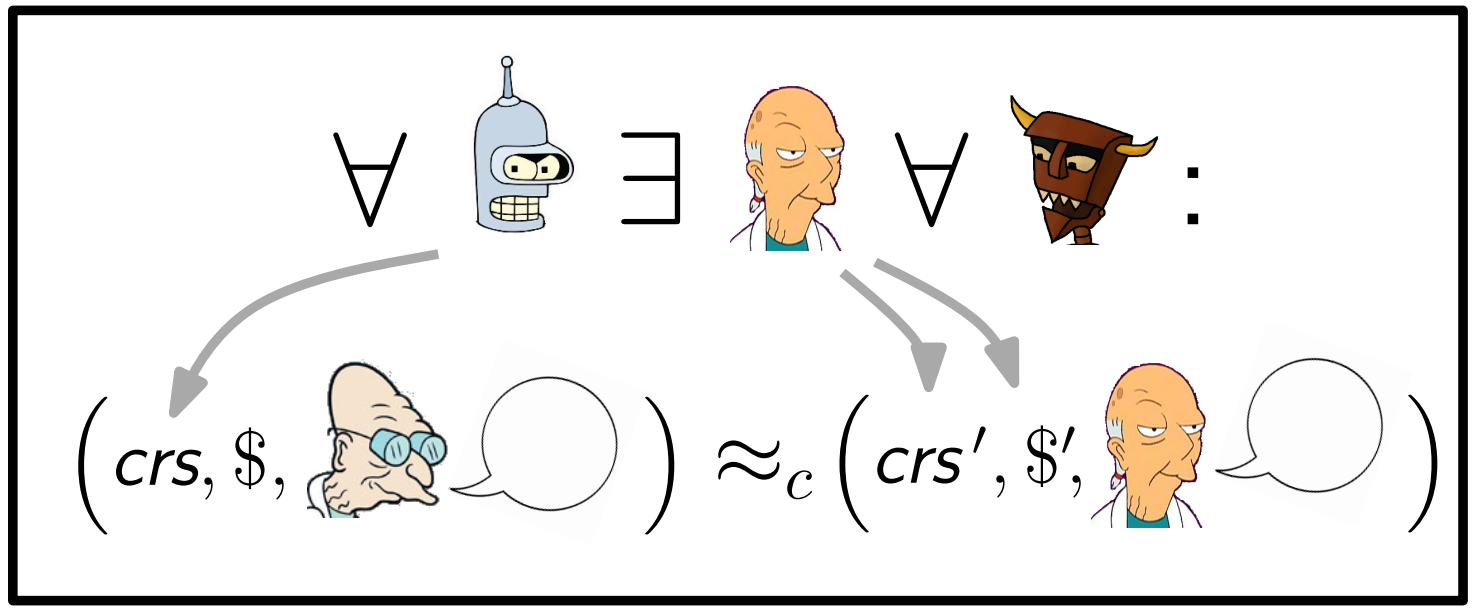
idea:

crs

trapdoor

Prove: $x \in L \vee$ "I know s"

Achieving SND + S-ZK



KEA: $\forall$ $(g, h) \rightarrow$ $\rightarrow (g^s, h^s)$

$\exists$ $\rightarrow s$

who chooses h?

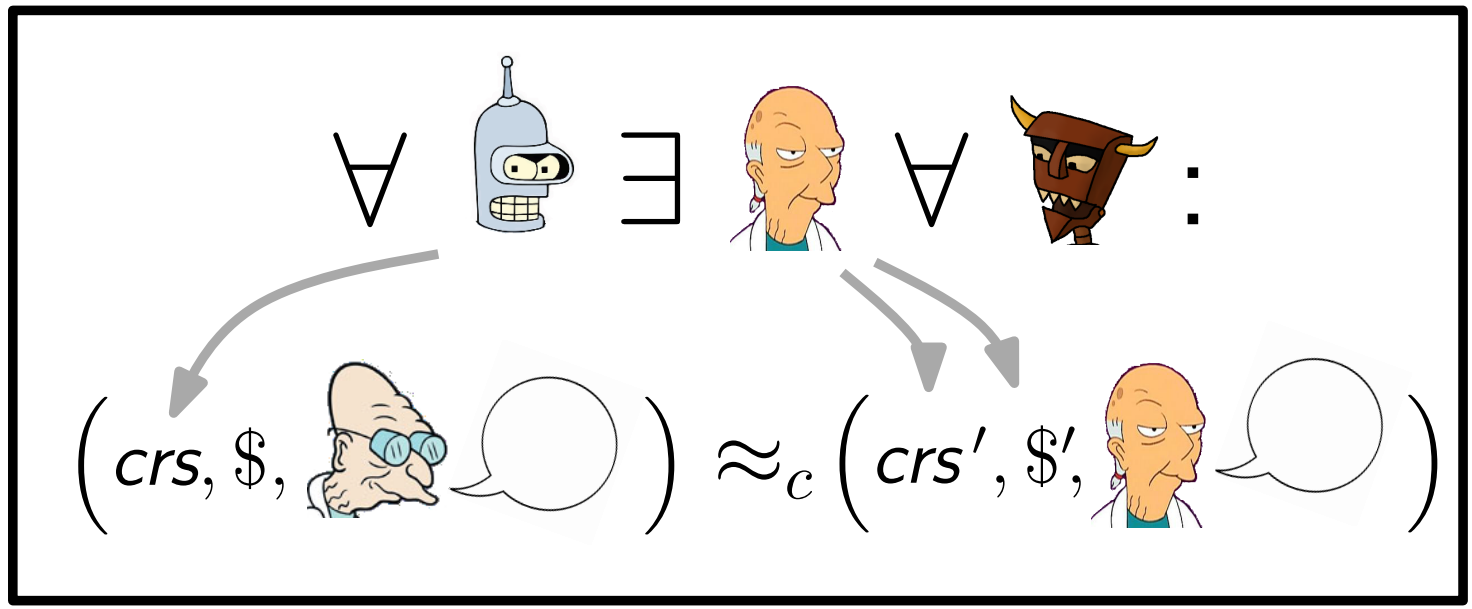
idea:

crs

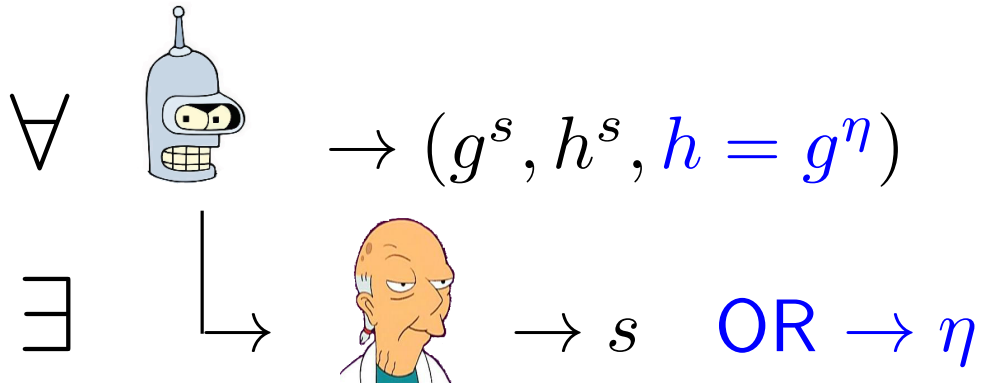
trapdoor

Prove: $x \in L \vee$ "I know s"

Achieving SND + S-ZK

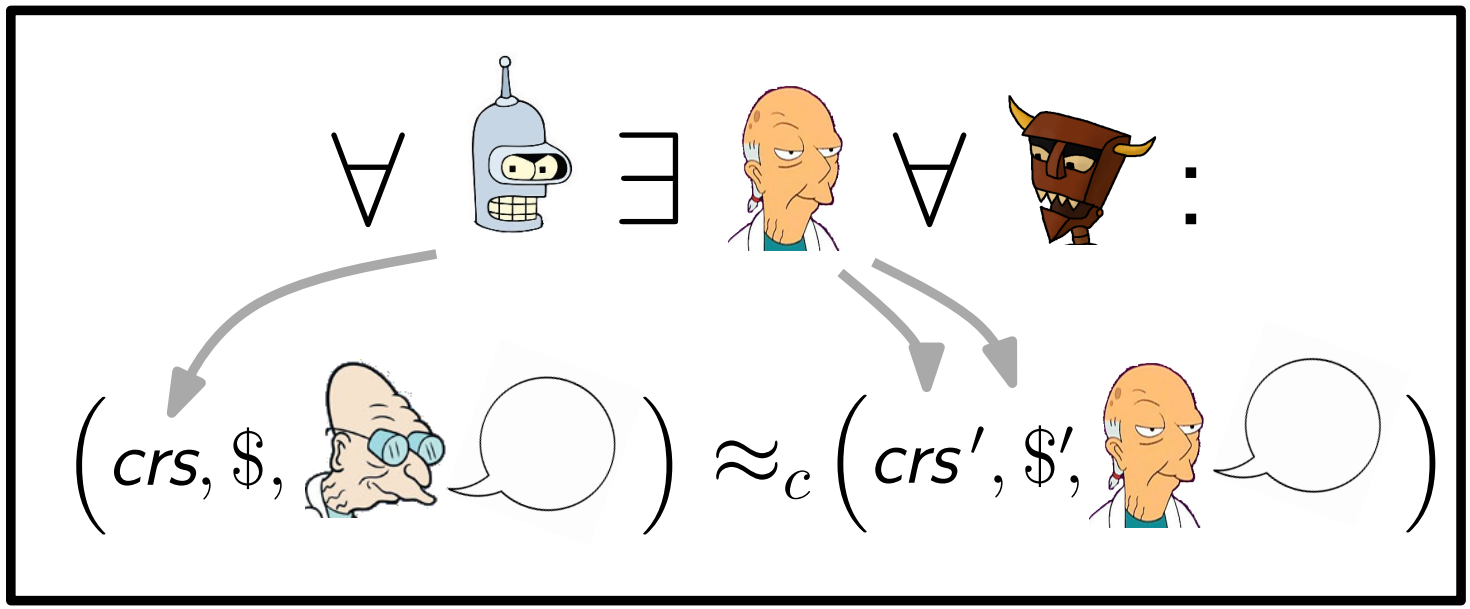


DH-KEA:



Prove: $x \in L \vee$ "I know s or η"

Achieving SND + S-ZK

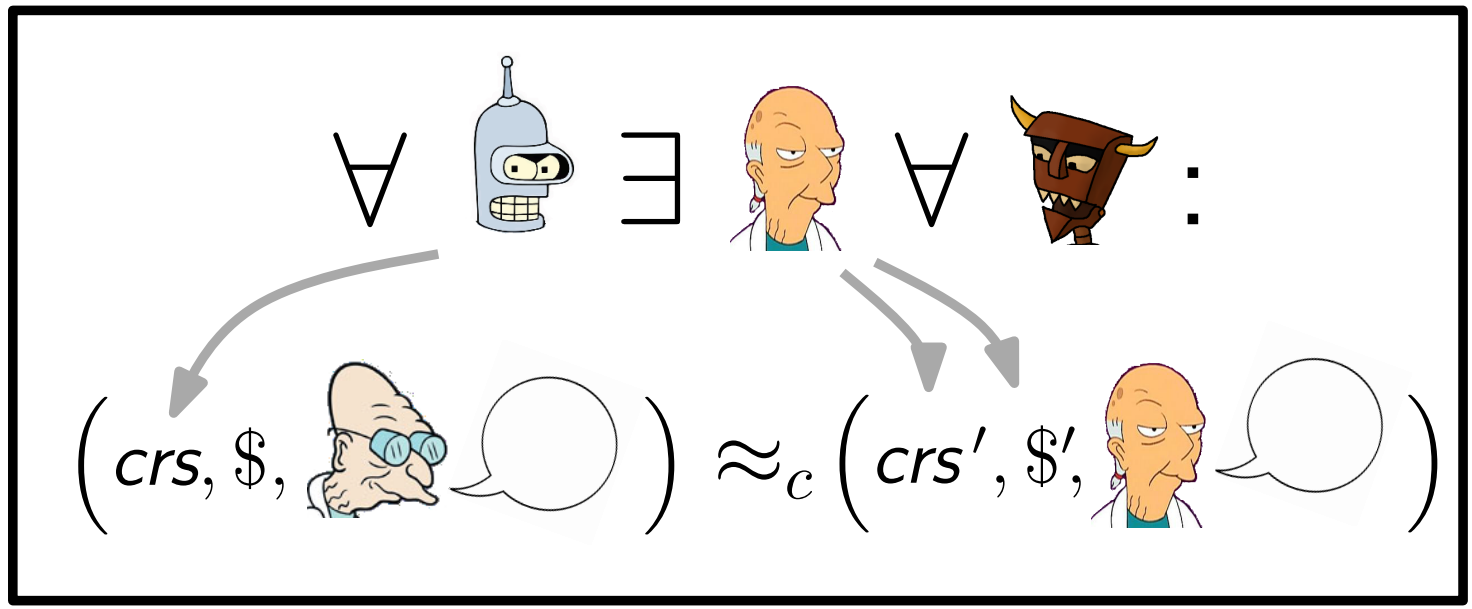


$$crs = (g^s, h^s, h = g^\eta)$$

prove knowledge how?

Prove: $x \in L \vee$ "I know s or η"

Achieving SND + S-ZK



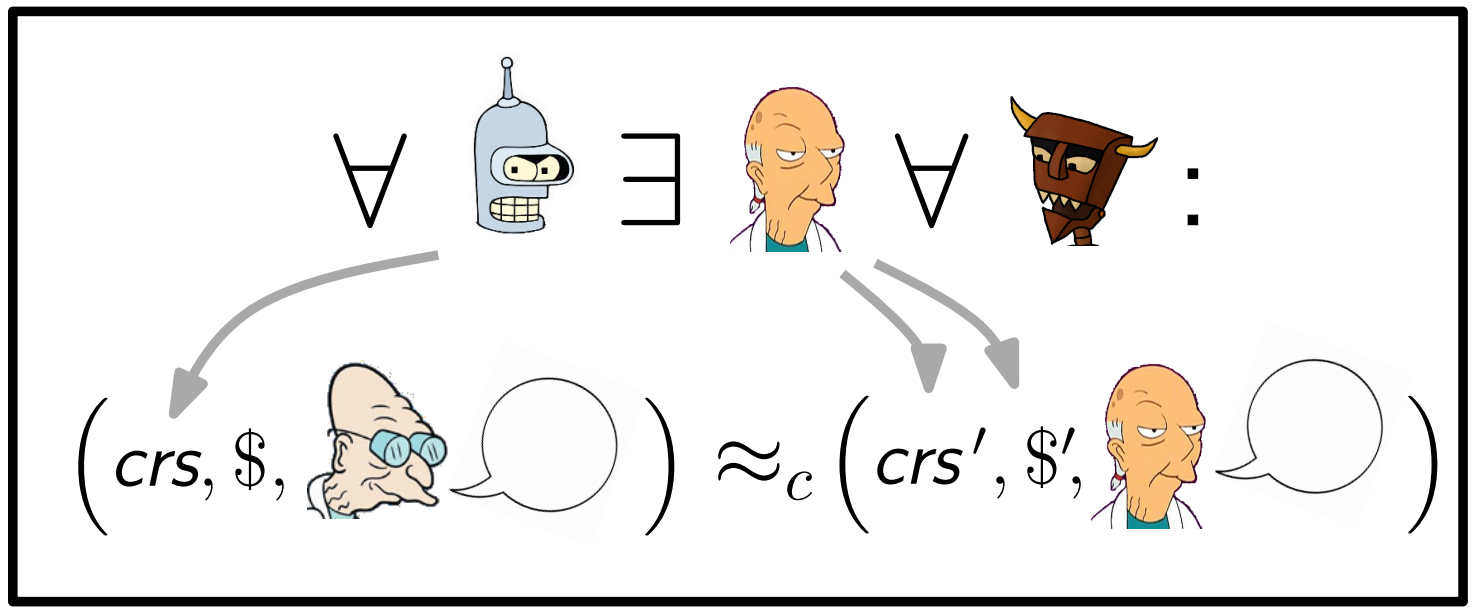
$$crs = (g^s, h^s, h = g^\eta)$$

$\mathsf{Enc}(pk, s)$

prove knowledge how?

Prove: $x \in L \vee$ "I know s or η"

Achieving SND + S-ZK



?

$crs = (g^s, h^s, h = g^\eta)$

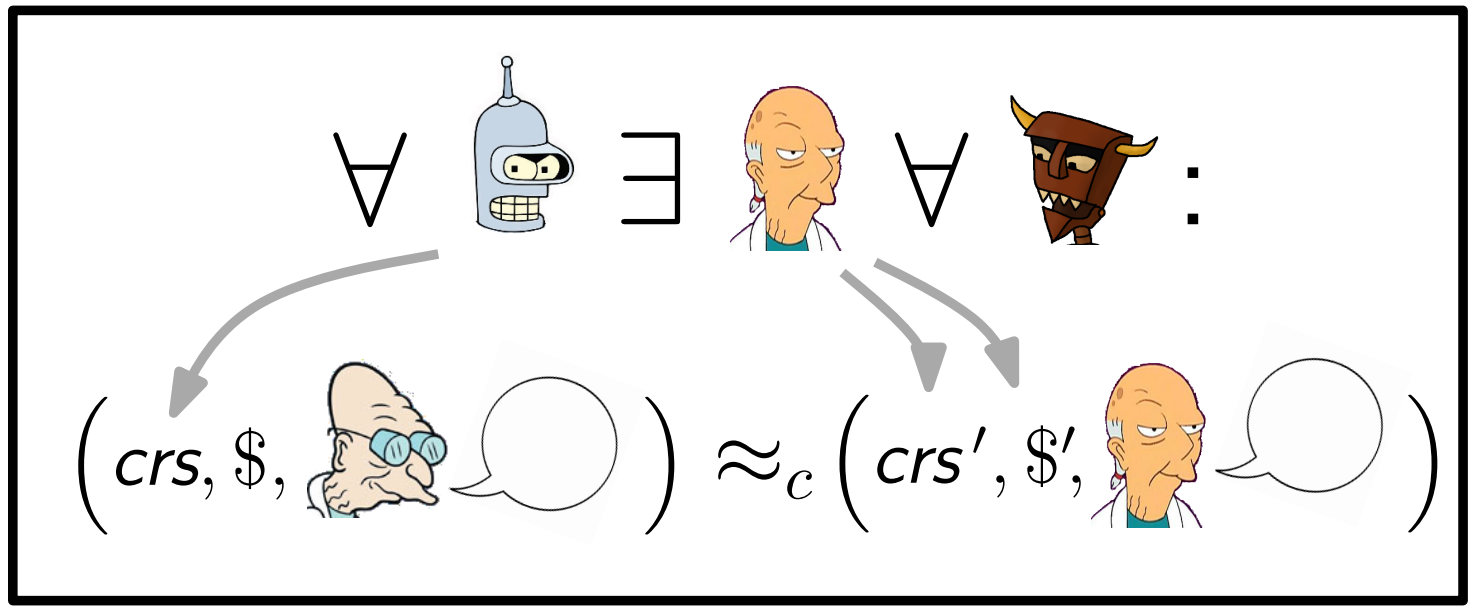
pk

$\mathsf{Enc}(pk, s)$

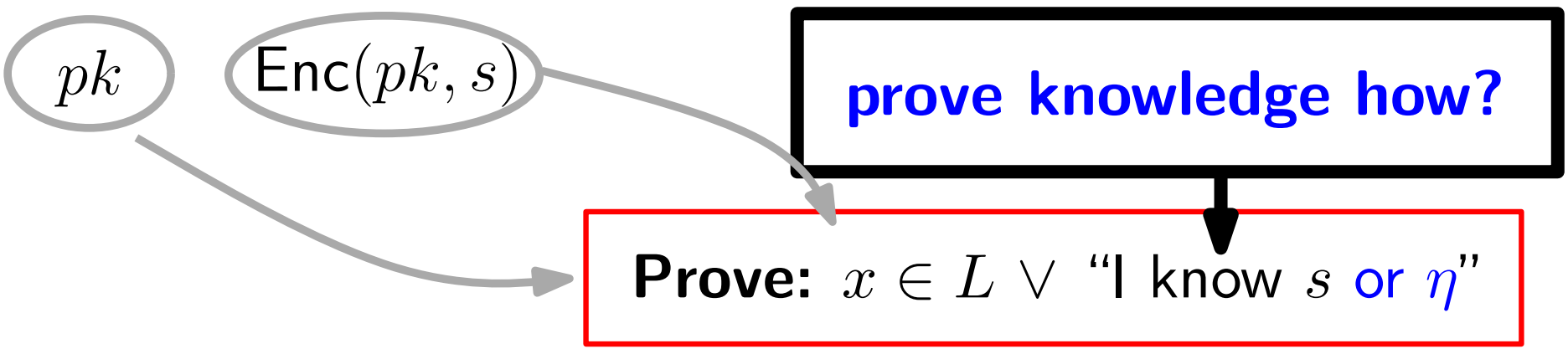
prove knowledge how?

Prove: $x \in L \vee$ "I know s or η"

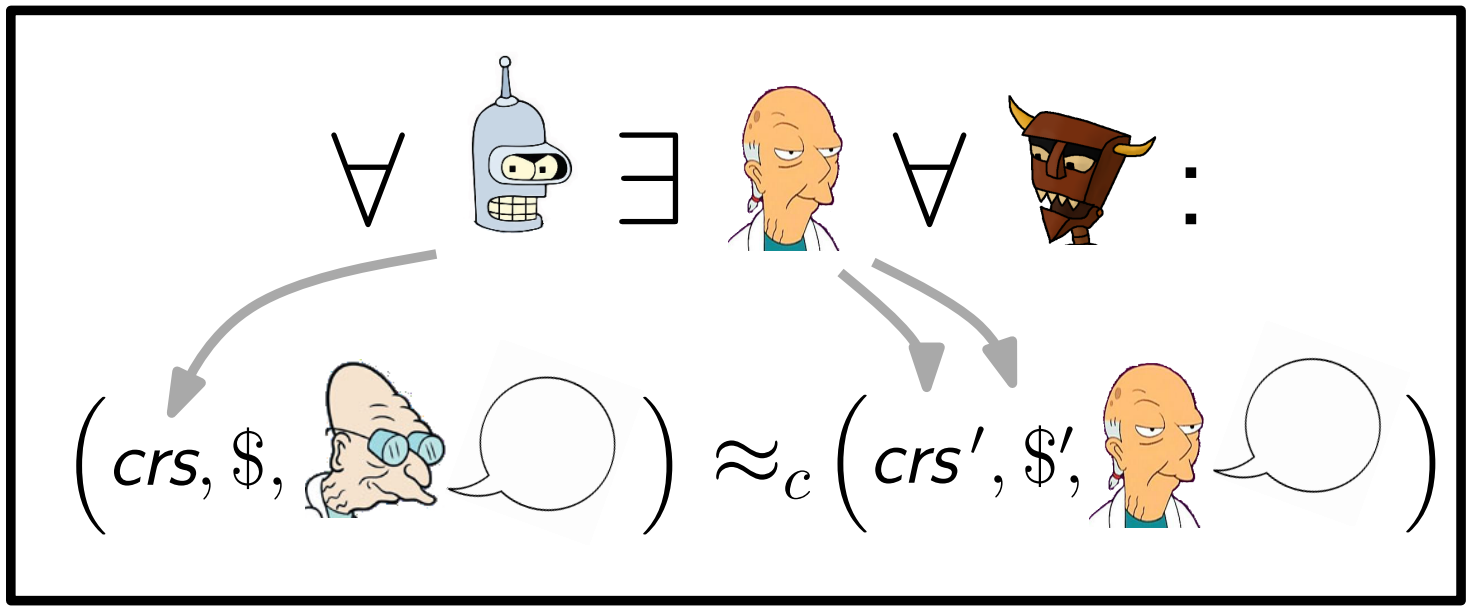
Achieving SND + S-ZK



$$crs = (g^s, h^s, h = g^\eta)$$



Achieving SND + S-ZK



$$crs = (g^s, h^s, h = g^\eta)$$

pk

$\mathsf{Enc}(pk, s)$

$+$ KEA-proof of sk

prove knowledge how?

Prove: $x \in L \vee$ "I know s or η"

Our results

Standard			Subversion-resistant			Possible?	Assumpt's:
SND	ZK	WI	S-SND	S-ZK	S-WI		
	•		•			✗	
•		•	•		•	✓	DLin
•	•	•		•	•	✓	DH-KEA

Our results

Standard			Subversion-resistant			Possible?	Assumpt's:
SND	ZK	WI	S-SND	S-ZK	S-WI		
	•		•			✗	
•		•	•		•	✓	DLin
•	•	•		•	•	✓	DH-KEA
•	•	•			•	✓	NIZK

Our results

Standard			Subversion-resistant			Possible?	Assumpt's:
SND	ZK	WI	S-SND	S-ZK	S-WI		
	•		•			✗	
•		•	•		•	✓	DLin
•	•	•		•	•	✓	DH-KEA
•	•	•			•	✓	NIZK

THANK YOU!

QUESTIONS?