On the Impossibility of Three-Move Blind Signature Schemes

Marc Fischlin Dominique Schröder

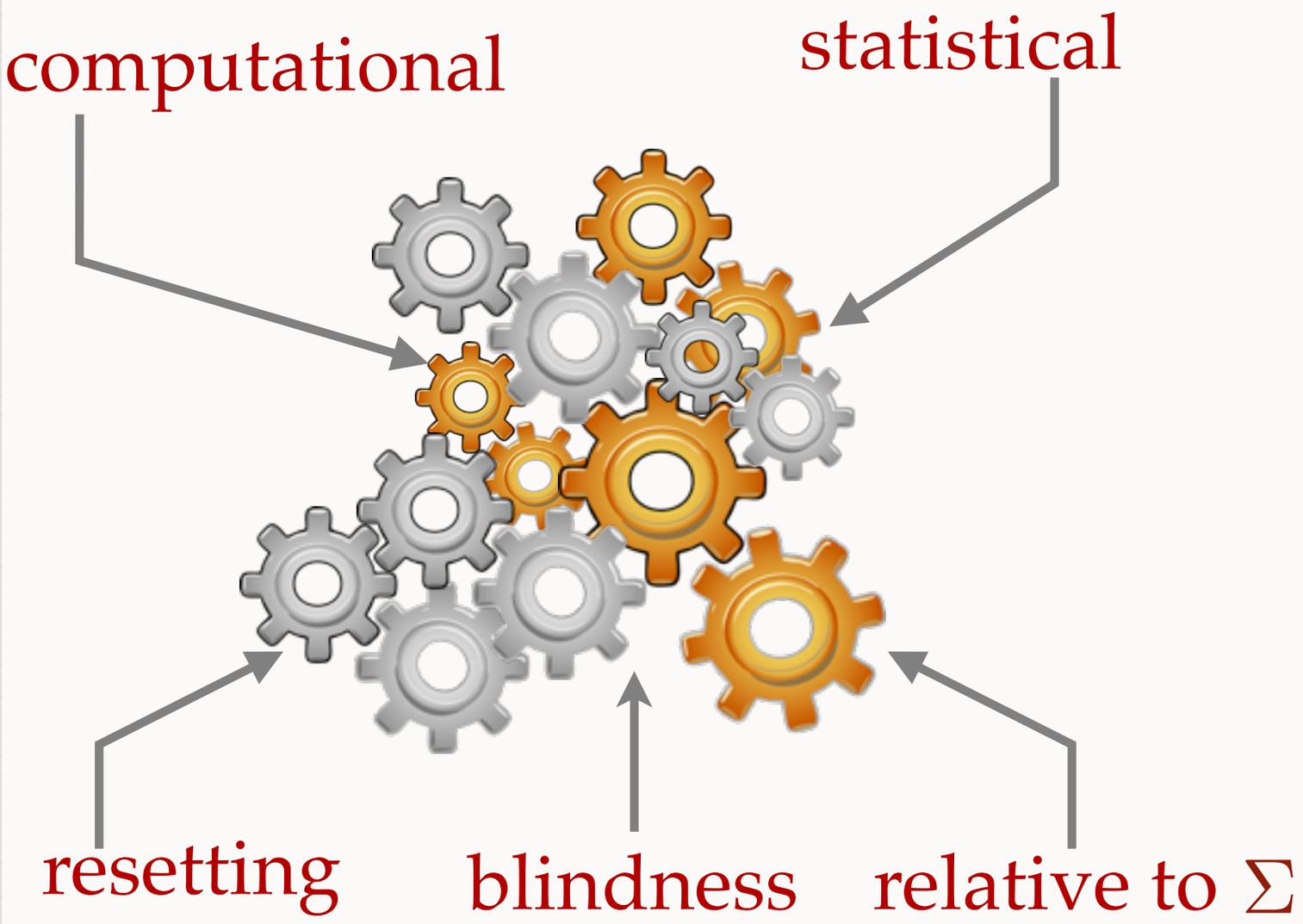
TU Darmstadt

www.dominique-schroeder.de

Eurocrypt 2010

DISCLAIMER

- Paper
- Talk



simplified
for exposition!

There exists

no three-move

blind signature scheme

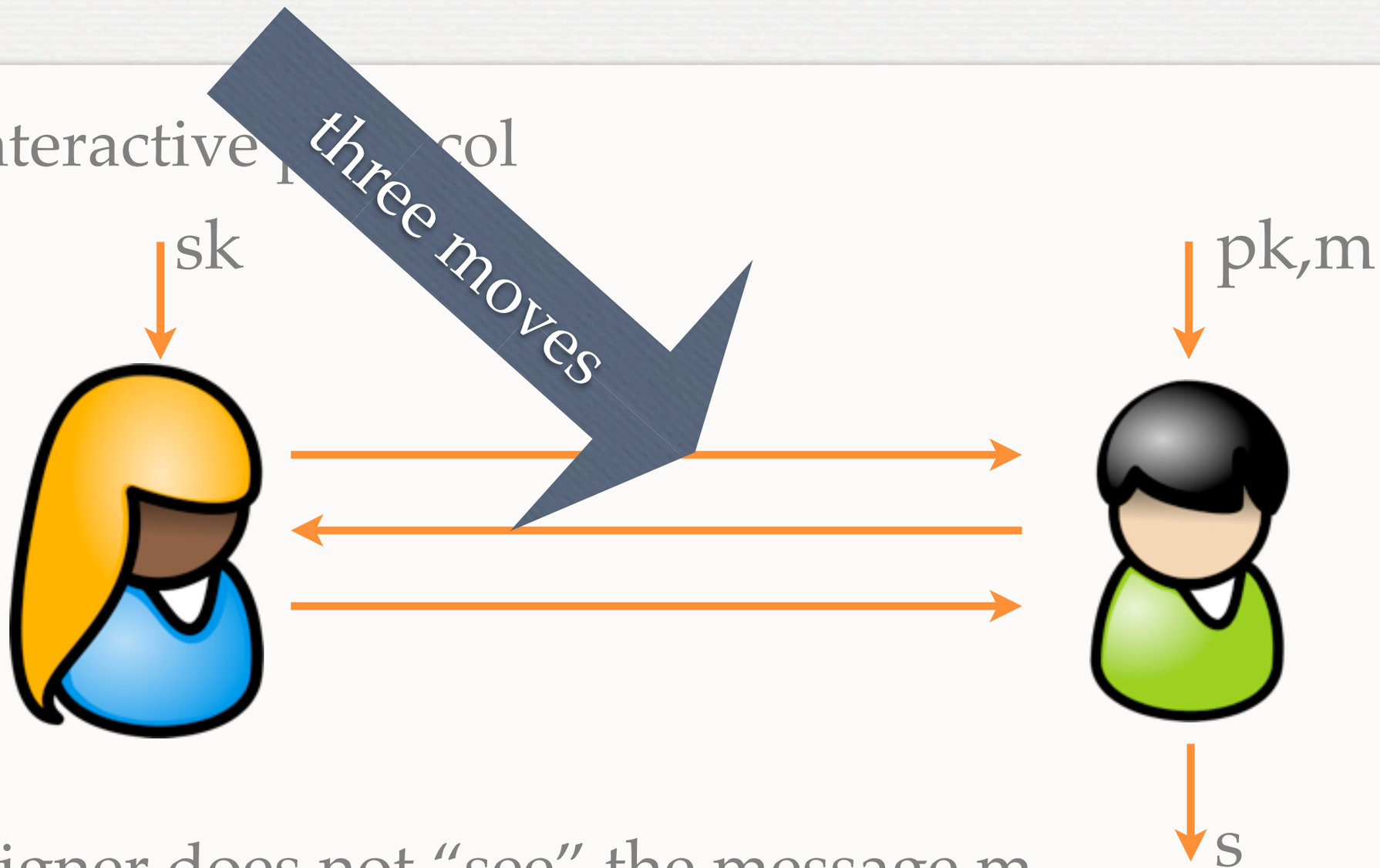
in the standard model!

THANKS FOR YOUR ATTENTION!

OUTLINE

BLIND SIGNATURE

- Interactive protocol

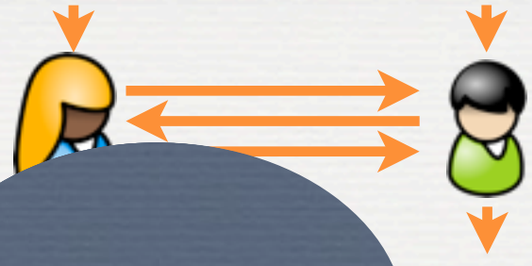


- Signer does not “see” the message m
- User cannot produce more signatures then # interactions

APPLICATIONS

- eVoting: FIFA world soccer cup selected in 2002 Most Valuable Player using Votopia

- unique blind signature => Oblivious Transfer



THREE MOVES???

ROM

Cha

PS
JLO

ABE,
BNPS

BOL

CKW KiaZ

Fis,
Oka

HKKL

standard model

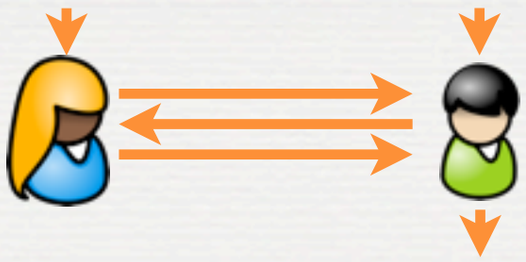
1983 96,97 01 04 05 06 08

CRS

interactive assumptions

STANDARD MODEL

CamKopWar	KiaZhou	Okamoto
5 moves	4 moves	4 moves
strong RSA	interactive	non-interactive
	CRS (concurrent)	



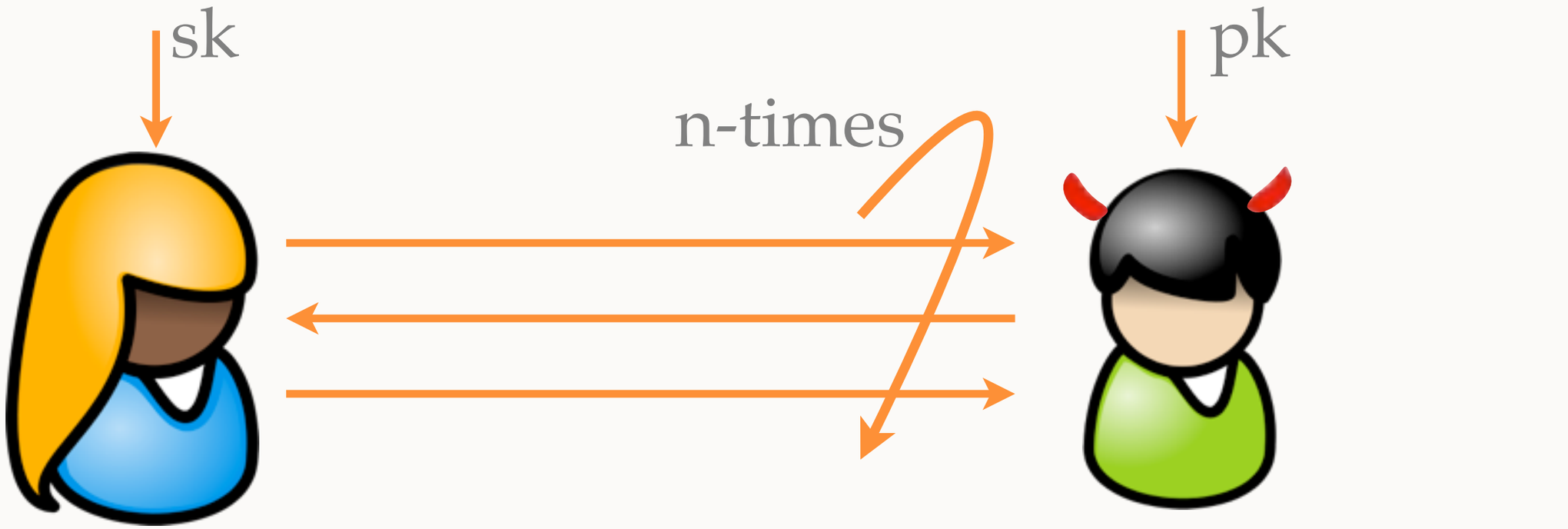
THREE MOVES???

27 years of research:
why can't we do better?

WHAT'S NEXT?

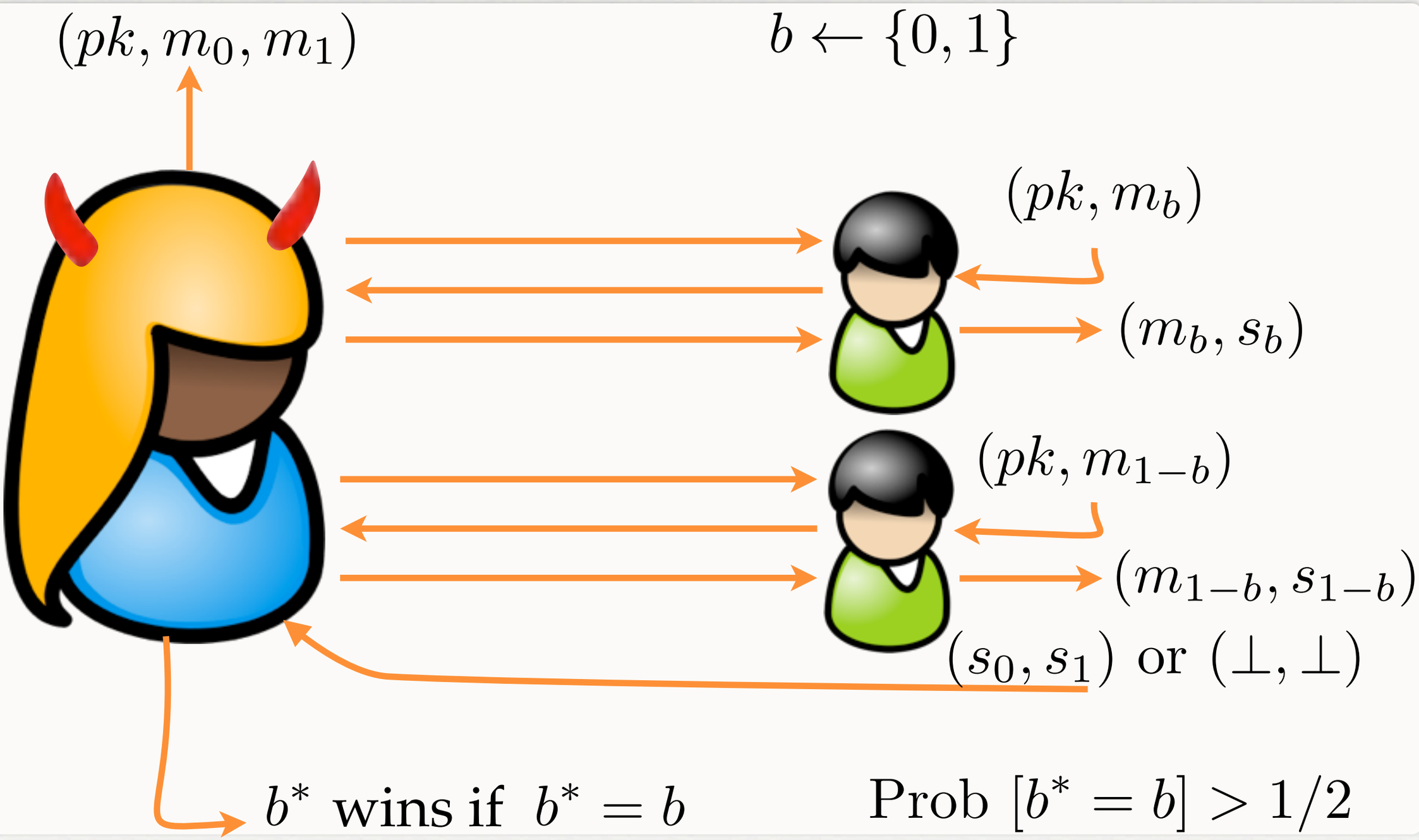
- Unforgeability
- Blindness
- Signature derivation checks
- Non-interactive computational problems
- Black-box reductions
- Meta-reductions

UNFORGEABILITY

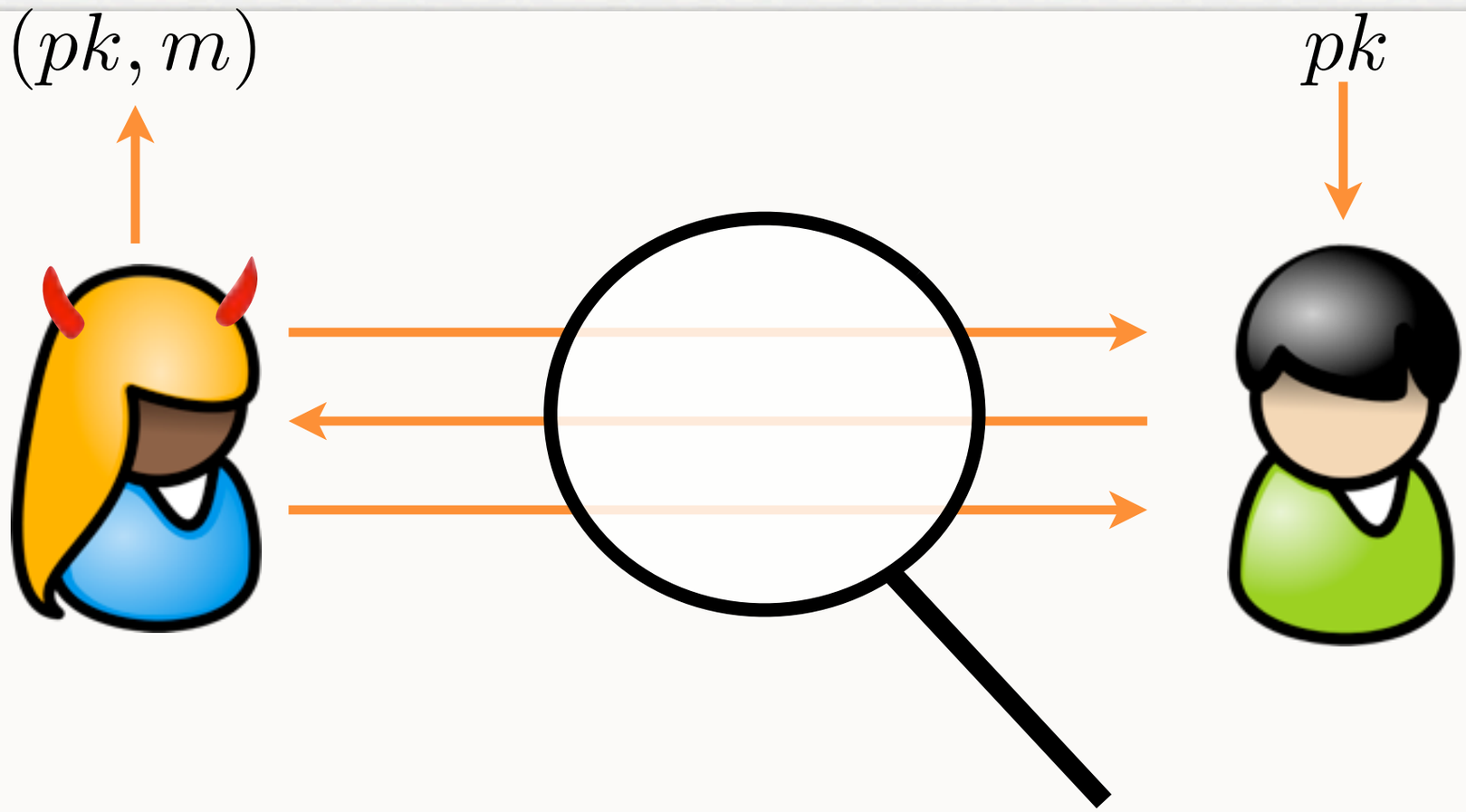


$$(m_1, s_1), \ldots, (m_{n+1}, s_{n+1})$$

BLINDNESS


(pk, m_0, m_1)
$b \leftarrow \{0,1\}$
(pk, m_b)
(m_b, s_b)
(pk, m_{1-b})
(m_{1-b}, s_{1-b})
(s_0, s_1) or $(\perp, \perp)$
b^* wins if $b^* = b$
Prob $[b^* = b] > 1/2$

SIGNATURE DERIVATION CHECKS

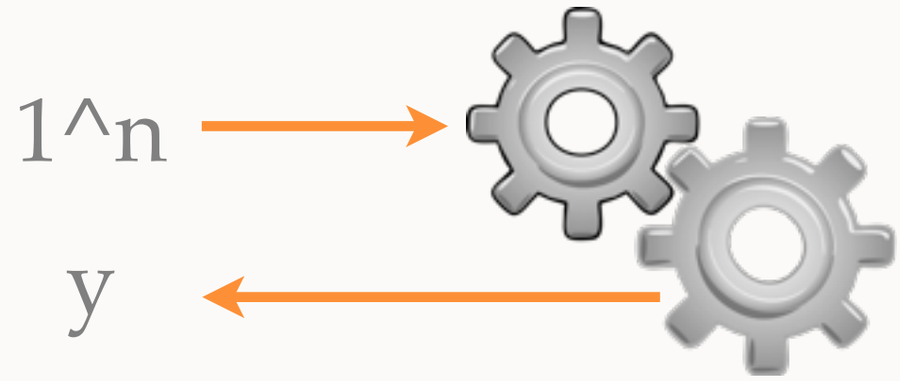


user able to compute a valid signature?

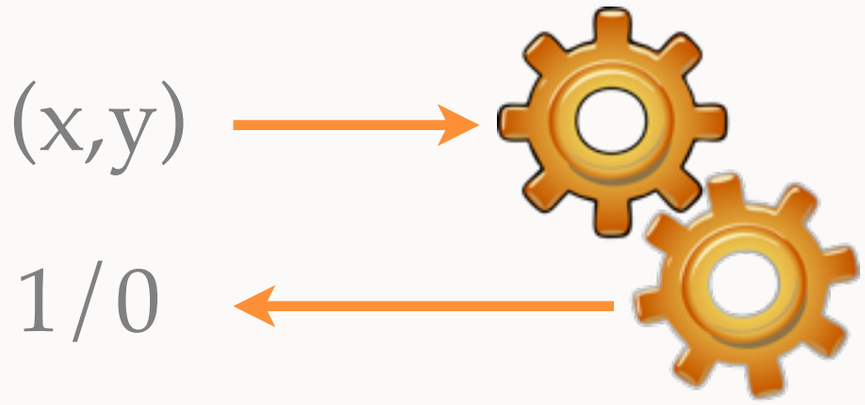
widely supported:
Chaum, Pointcheveal and Stern, Fischlin, ...

NON-INTERACTIVE PROBLEM

- Instance generator I



- Verification V



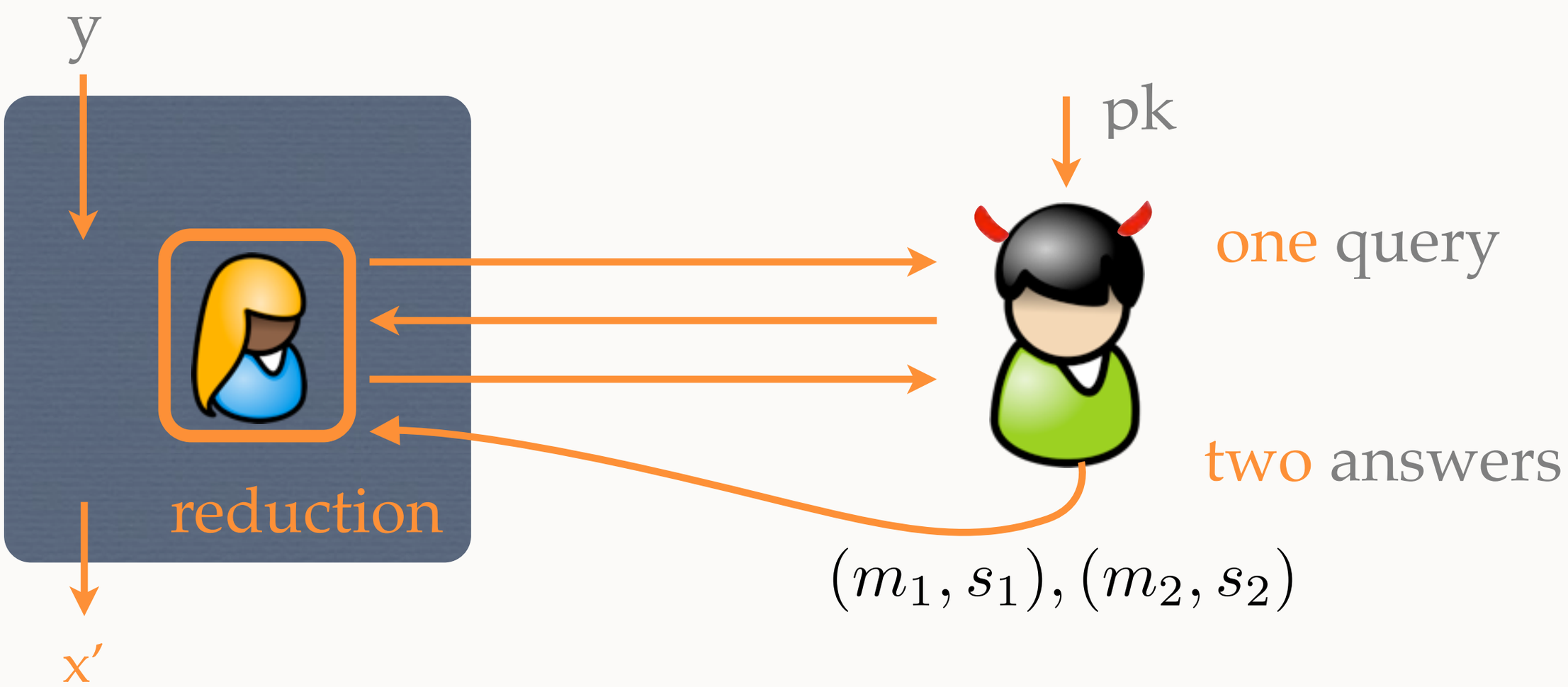
hard if probability that

x′ s.t. V(x′,y)=1

is negligible

BB-REDUCTION

- reduce unforgeability to a non-interactive problem



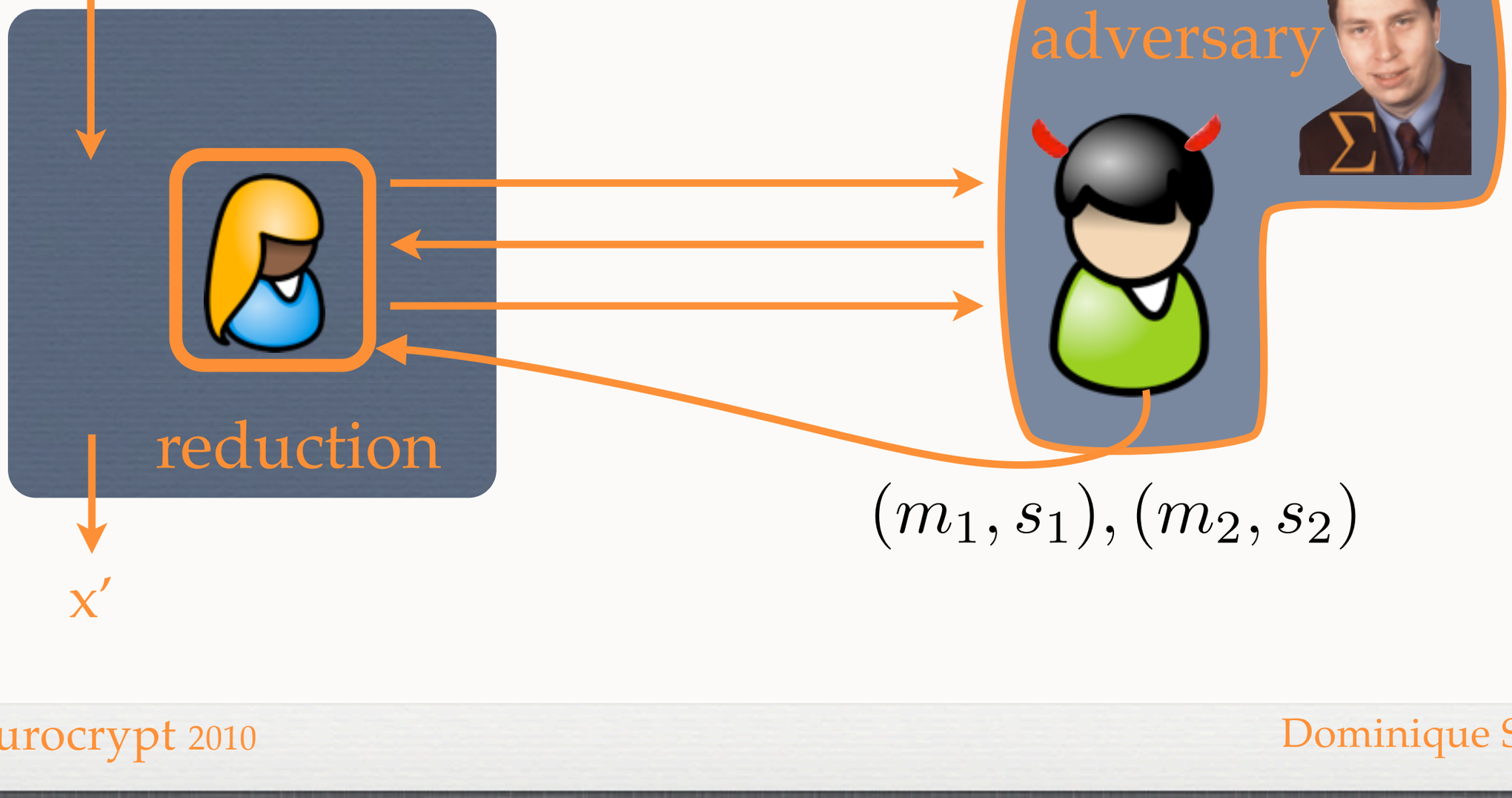
*Actual results may vary. See talk and proceedings for details.

BB$^{\Sigma}$-REDUCTION

- reduce unf…on-interactive problem

unlimited power

y

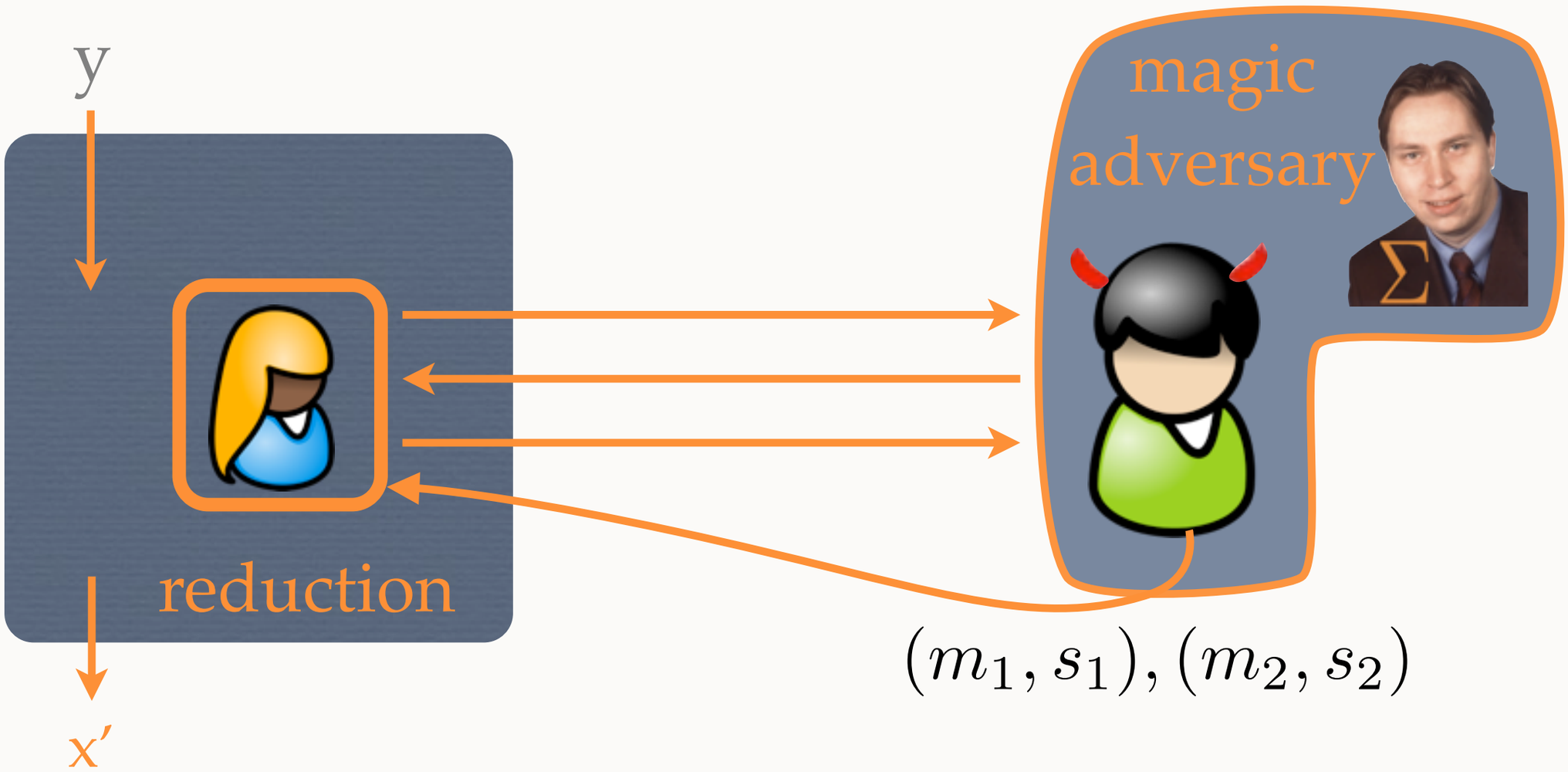


META-REDUCTION

- Meta-reduction ("reduction against the reduction")
  - Suppose that there exists a reduction that has black-box access to an adversary and reduces property X to an assumption Y.
- Then there exists a meta-reduction that
  - has black-box access to the reduction, and
  - simulates the adversary s.t. both algorithm solve the assumption Y directly.

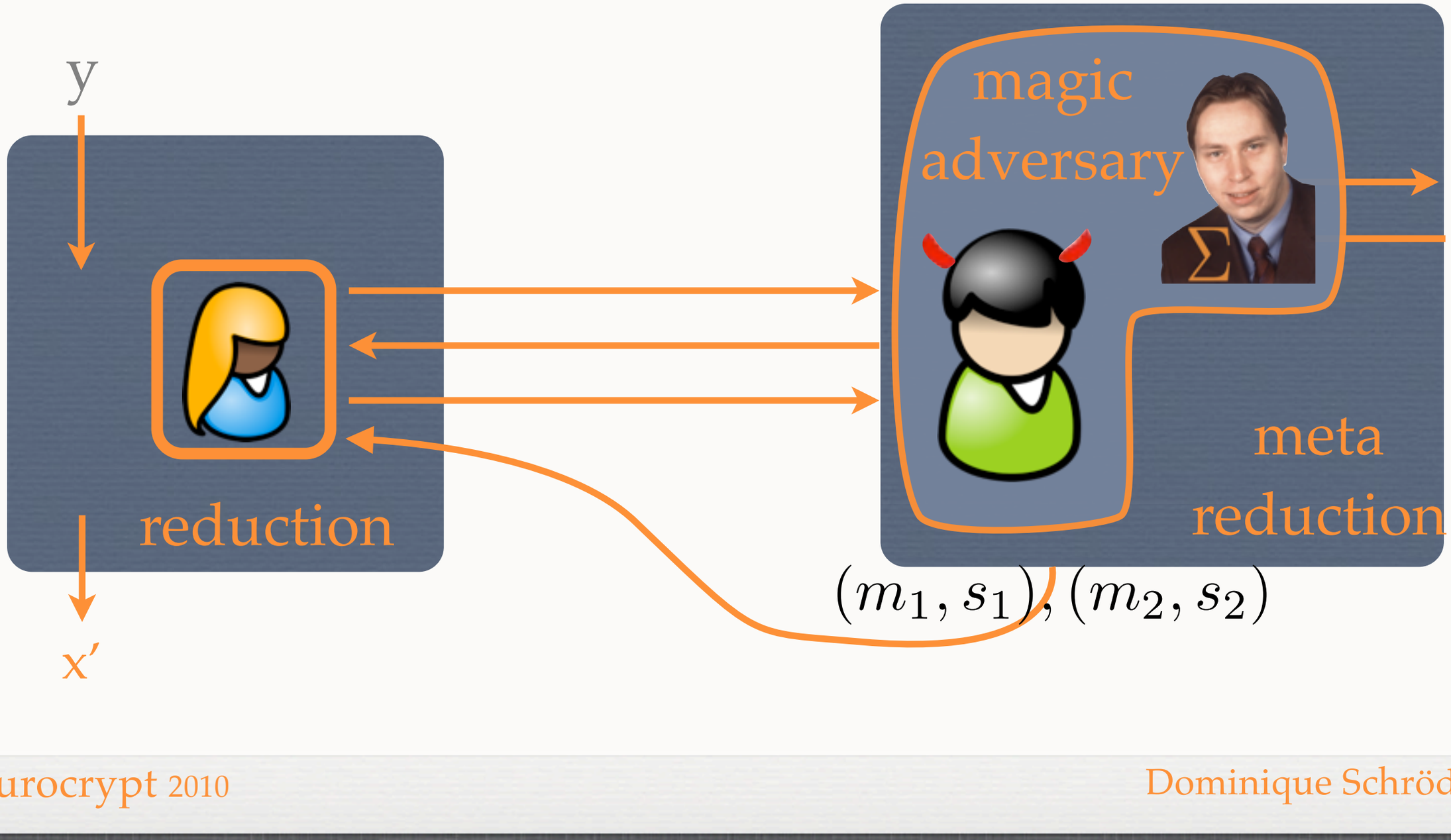
META-REDUCTION

- reduce unforgeability to a non-interactive problem



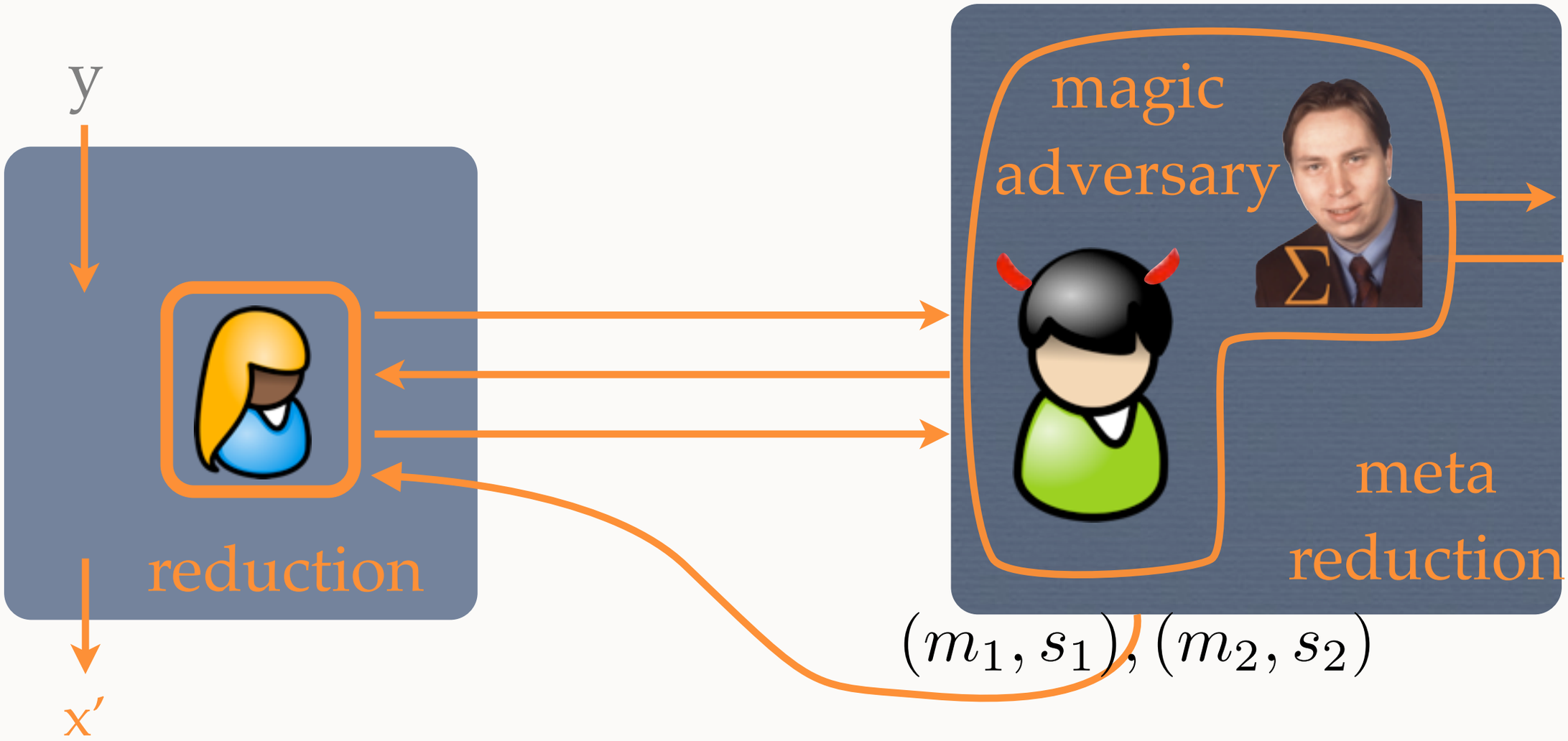
META-REDUCTION

- reduce unforgeability to a non-interactive problem



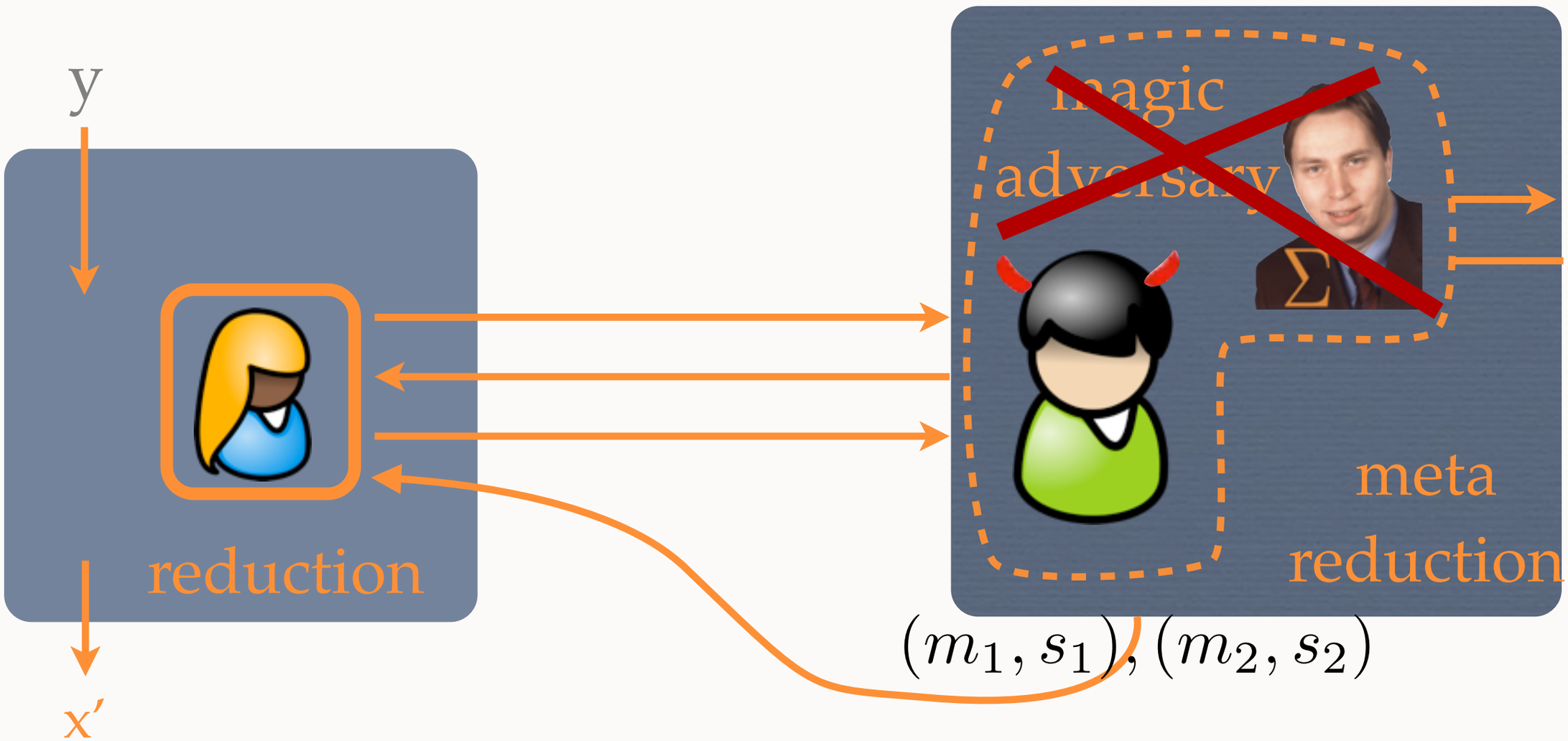
META-REDUCTION

- reduce unforgeability to a non-interactive problem



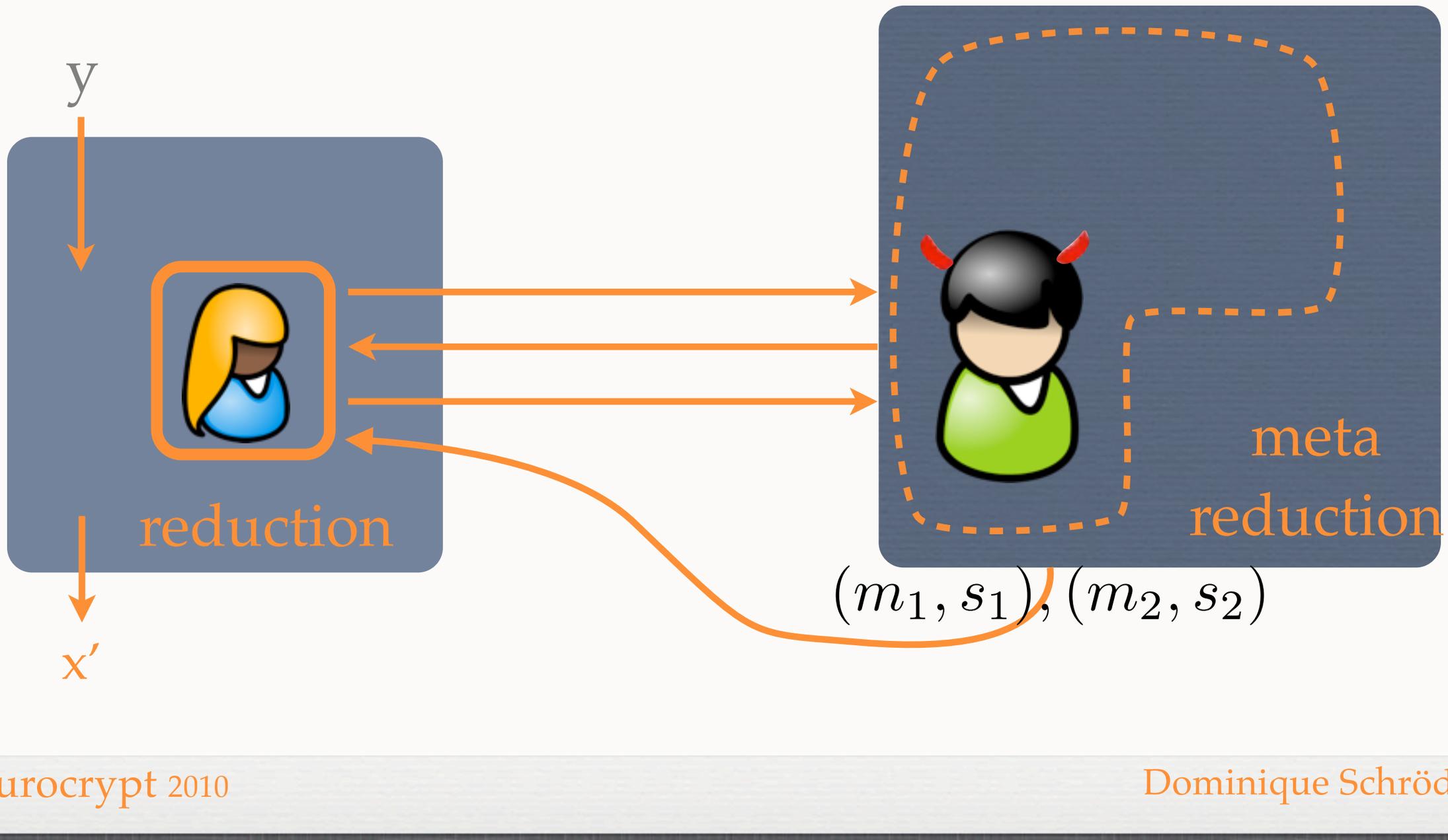
META-REDUCTION

- reduce unforgeability to a non-interactive problem



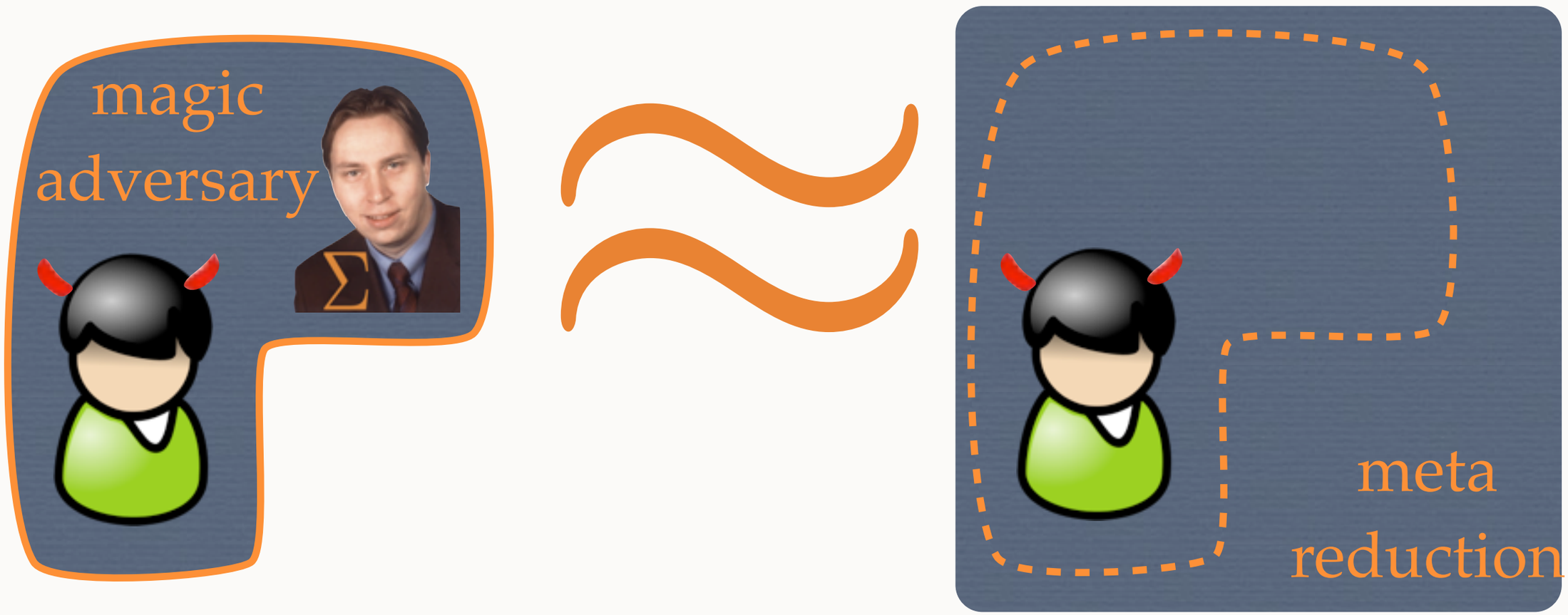
META-REDUCTION

- reduce unforgeability to a non-interactive problem



META-REDUCTION

- blindness??



VANILLA-REDUCTION 1/3

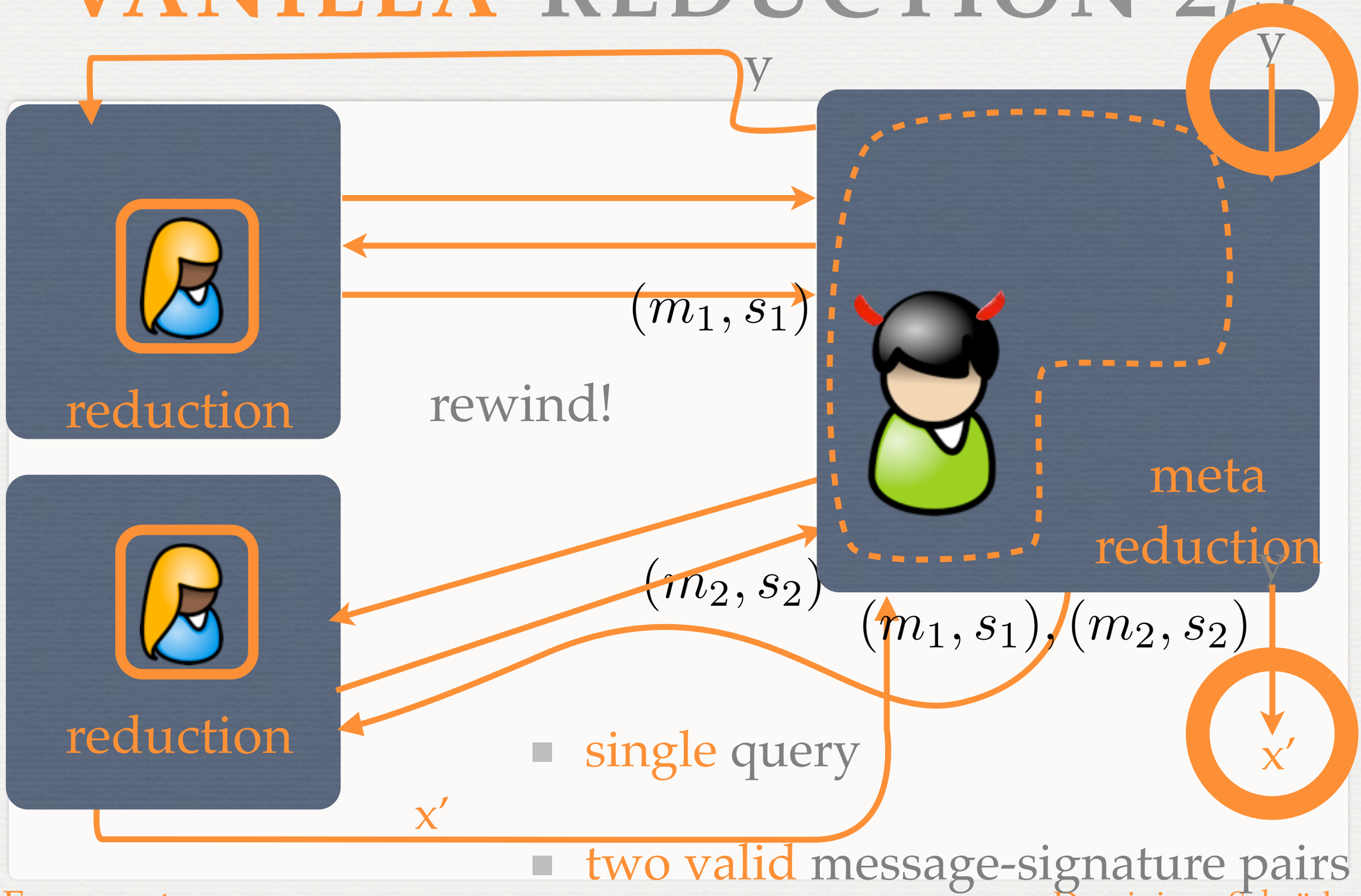
starting point

- does neither rewind nor reset the attacker
- succeeds with probability 1

we provide adversary

- asks a single query
- returns two message-signature pairs

VANILLA-REDUCTION 2/3

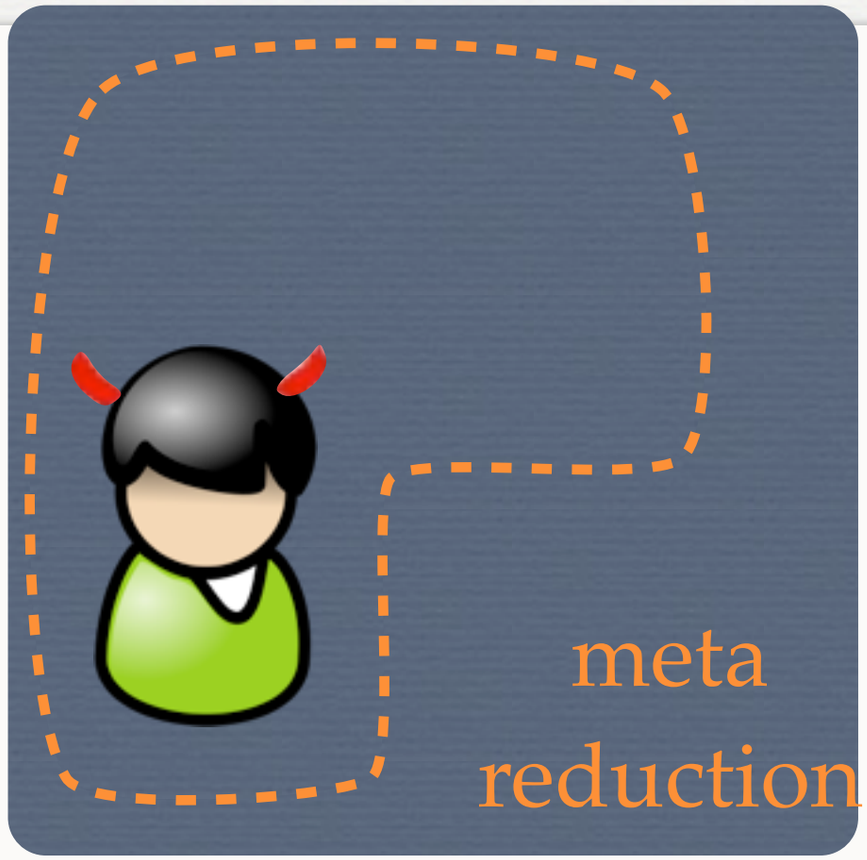


- single query
- two valid message-signature pairs

VANILLA-REDUCTION 3/3

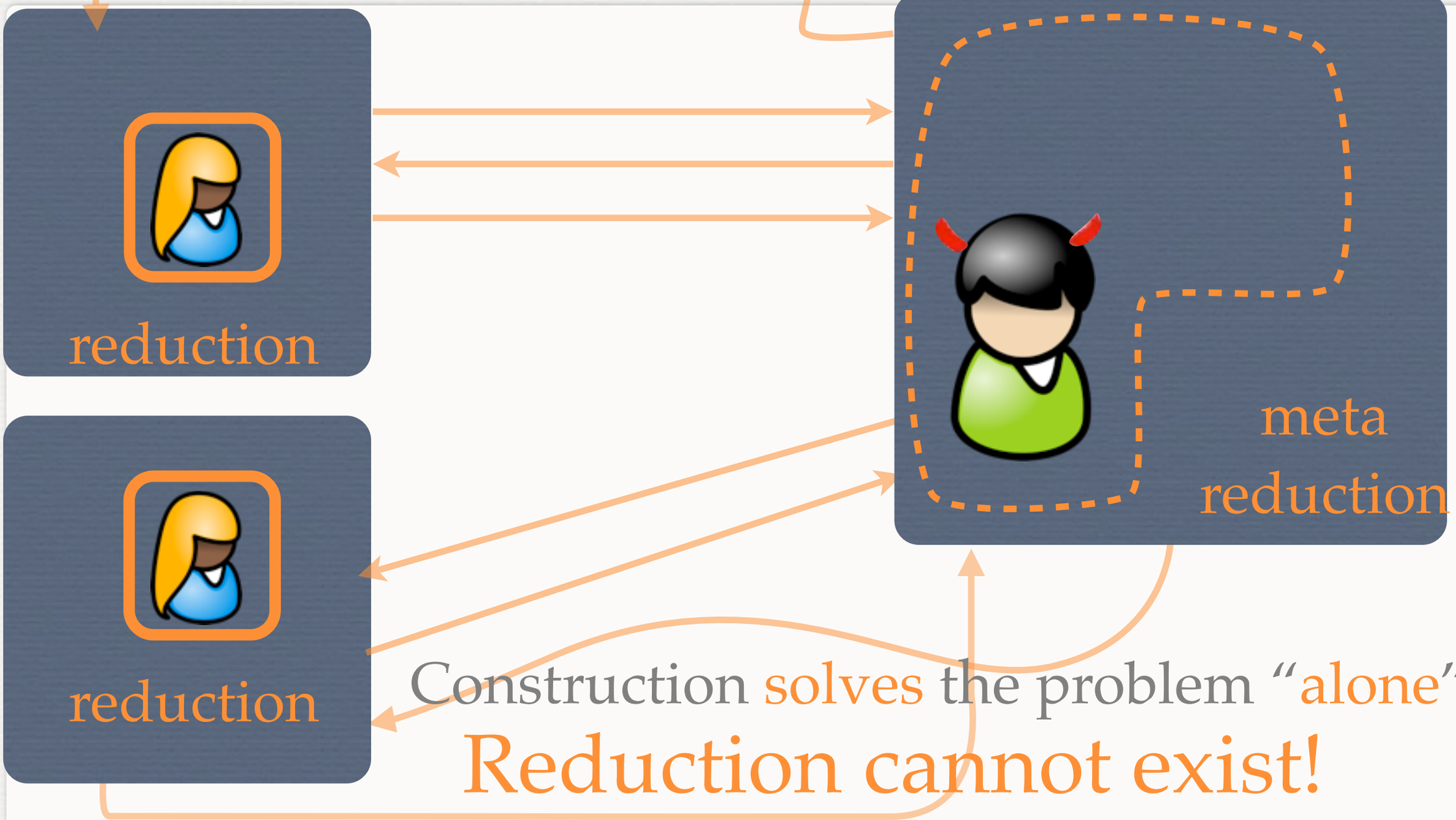
- blindness!!

$\approx$



Otherwise: build an attacker against blindness

VANILLA-REDUCTION



Construction solves the problem “alone”

Reduction cannot exist!

REMARKS

- Impossibility result extremely strong!
  - No reduction to an arbitrary non-interactive problem
    - dlog + col-res + one-way + ...
  - NOT obvious that this also holds for oracle separation techniques!
- Chaum's scheme: NO proof without ROM (H is instantiated with a non-interactive assumption)!

CONCLUSION

- 3 moves, standard model, non-interactive assumption, black-box, signature-derivation check, not possible
- 4 moves standard model (Okamoto)
- 2 moves CRS (Fischlin)
- 3 moves ROM (Pointcheval and Stern)
- 2 moves ROM (Chaum, Boldyreva -interactive assumption)

OUTLINE 2

THANKS

FOR YOUR ATTENTION!

Emmy Noether-Programm
Deutsche Forschungsgemeinschaft
DFG

CASED