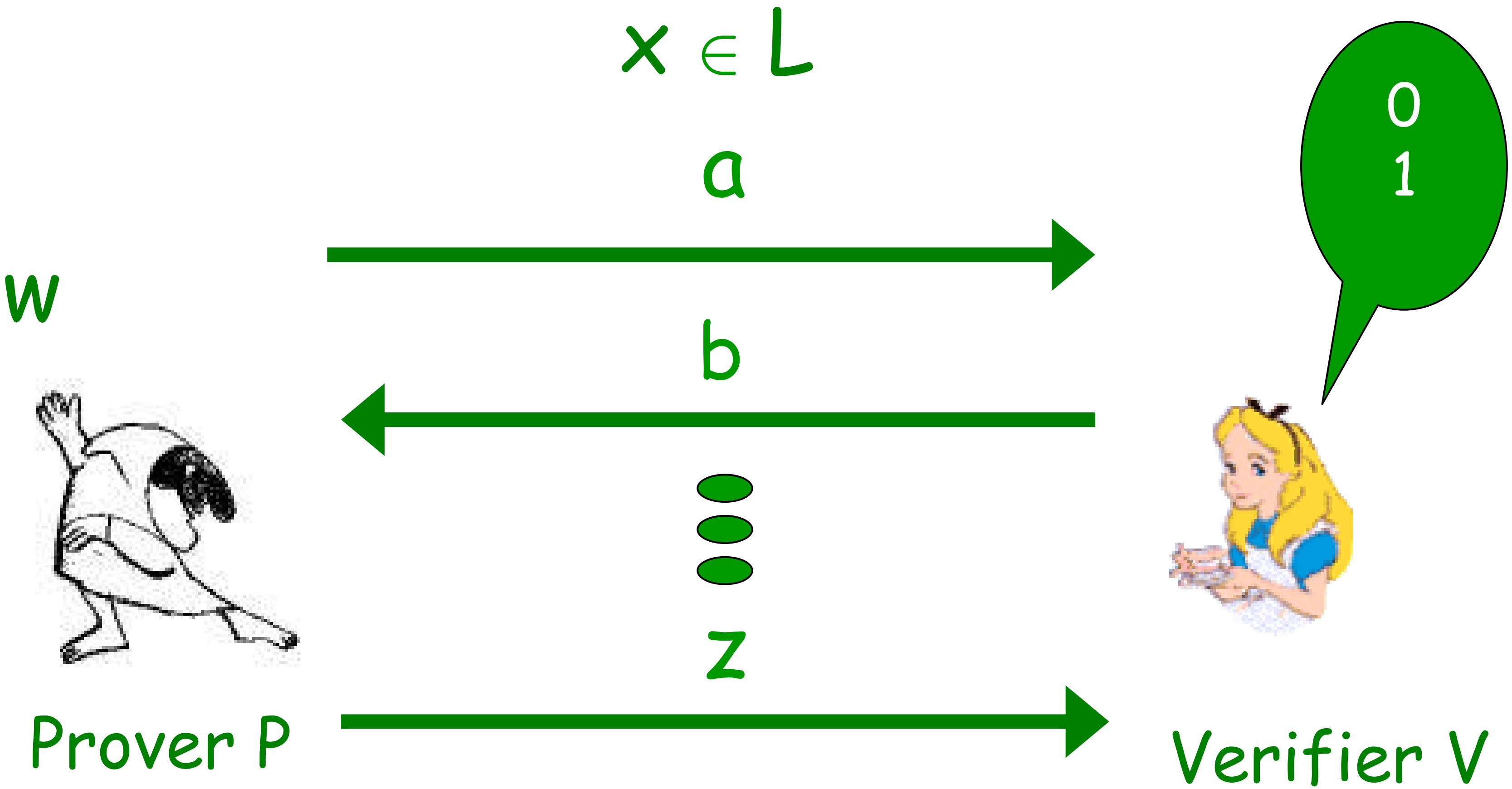
Concurrent Non-Malleable Witness Indistinguishability

Rafail Ostrovsky (UCLA, USA)
Giuseppe Persiano (Univ. Salerno - ITALY)
Ivan Visconti (Univ. Salerno - ITALY)

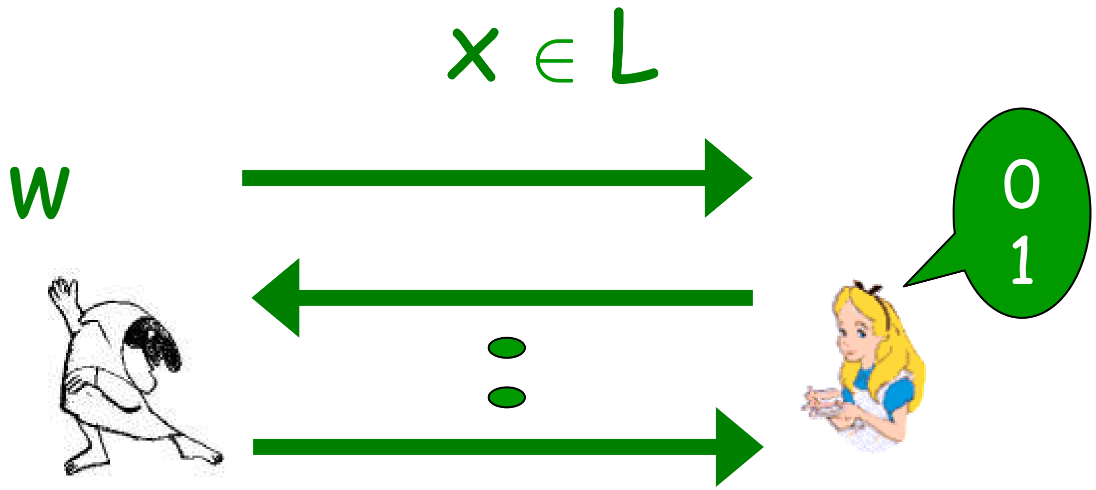
Outline

- Concurrent ZK, NMZK, Witness Indist.
- Non-Malleable Witness Indistinguishability
- Cnst-Rnd Concurrent NMWI in the plain model
- Cnst-Rnd Concurrent NMZK in the BPK Model
- UC with preprocessing

Interactive Proof System



Interactive Proof System

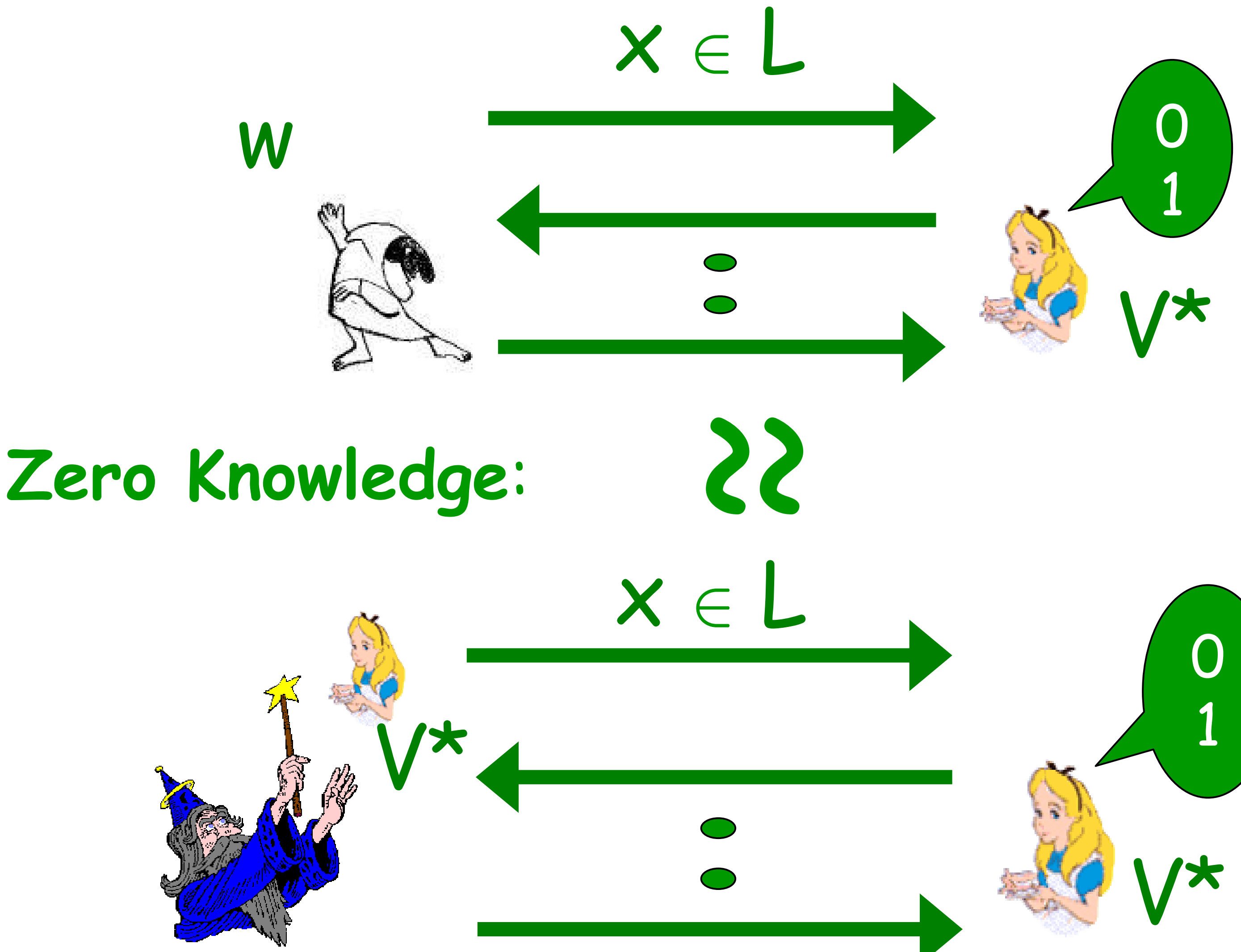


Properties:

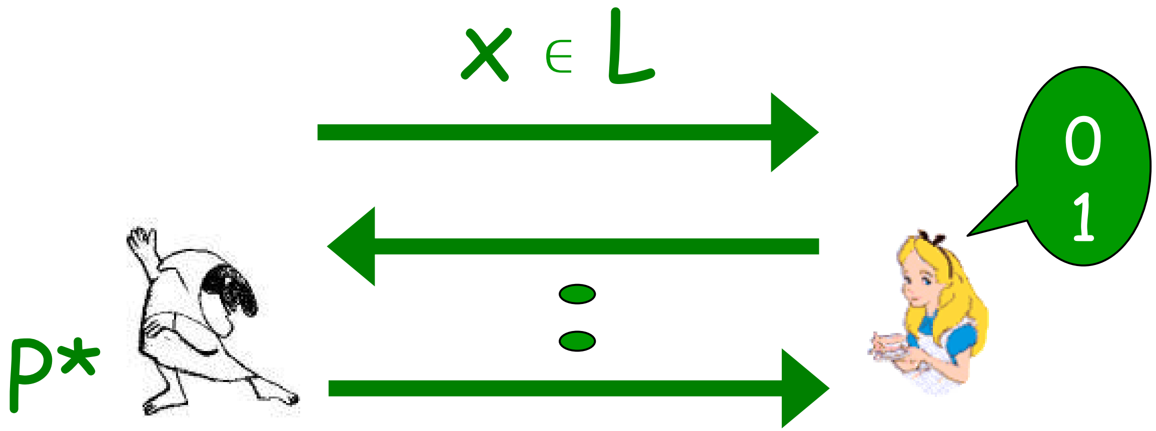
Completeness: if $x \in L$ then V outputs 1

Soundness: if NOT($x \in L$) then V outputs 0

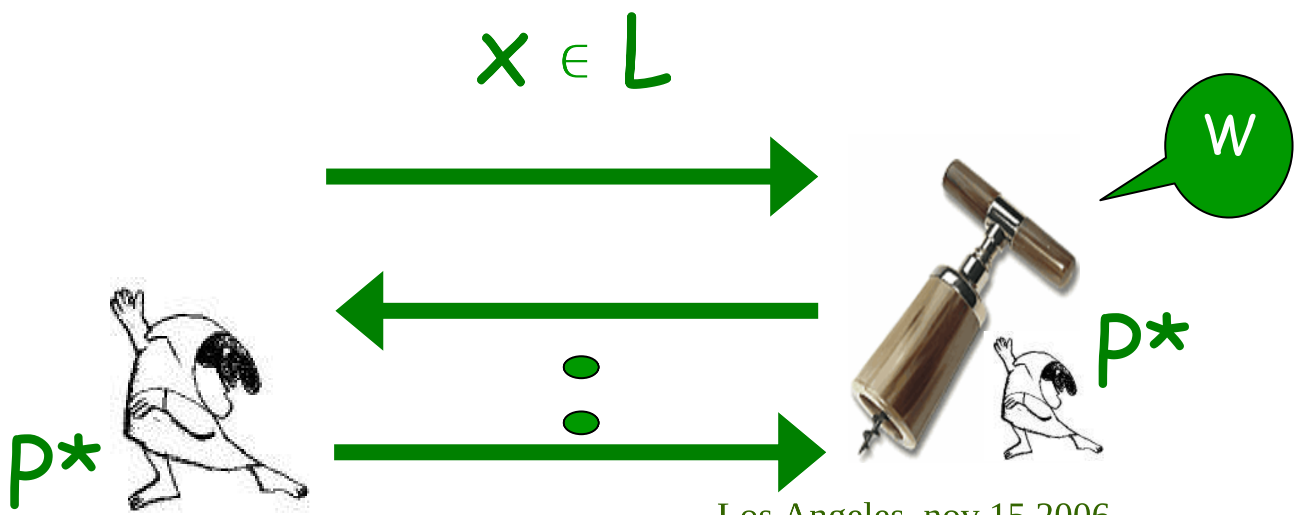
Interactive Zero-Knowledge Proofs



Interactive Proof of Knowledge



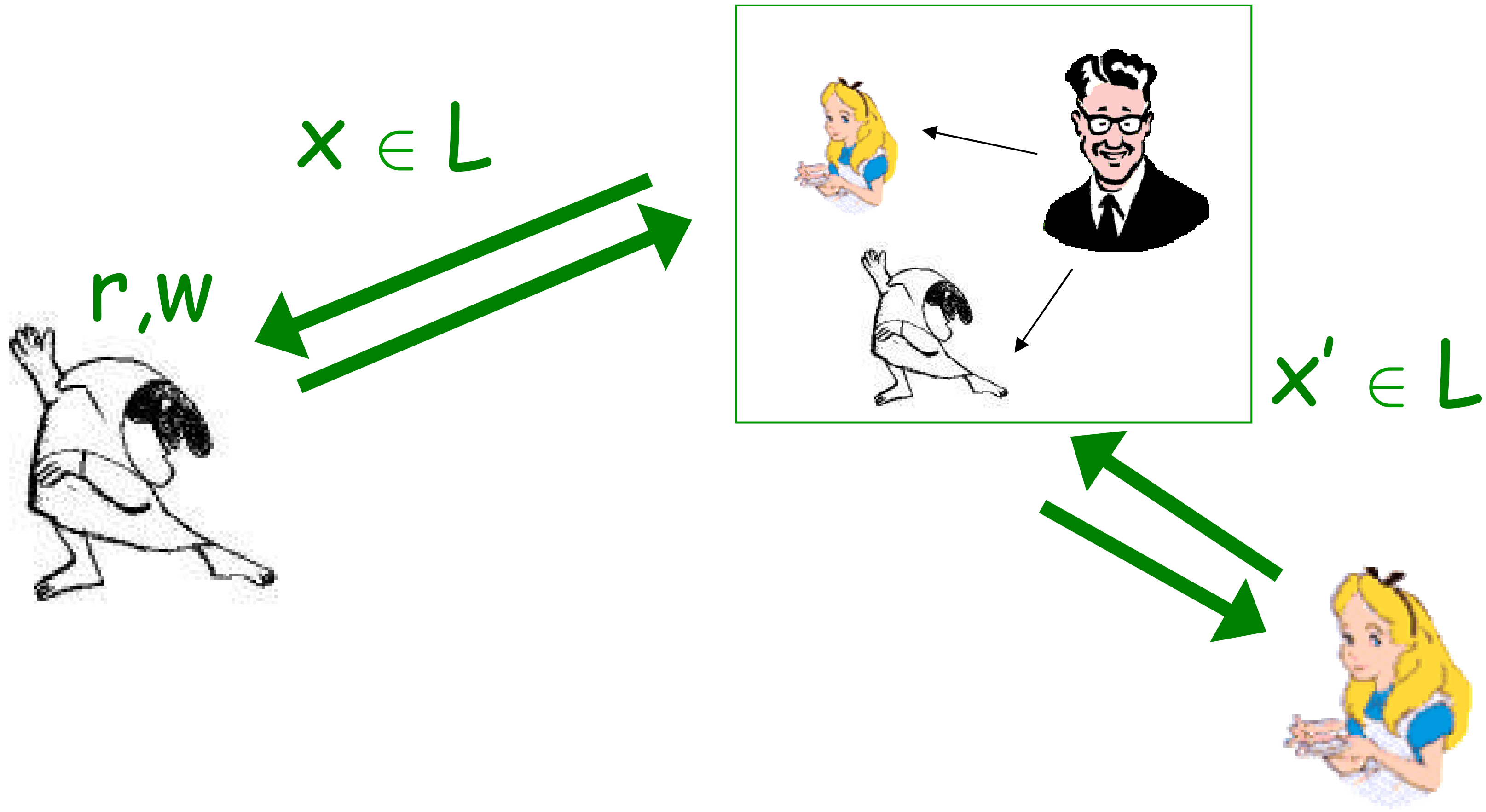
Witness Extraction:



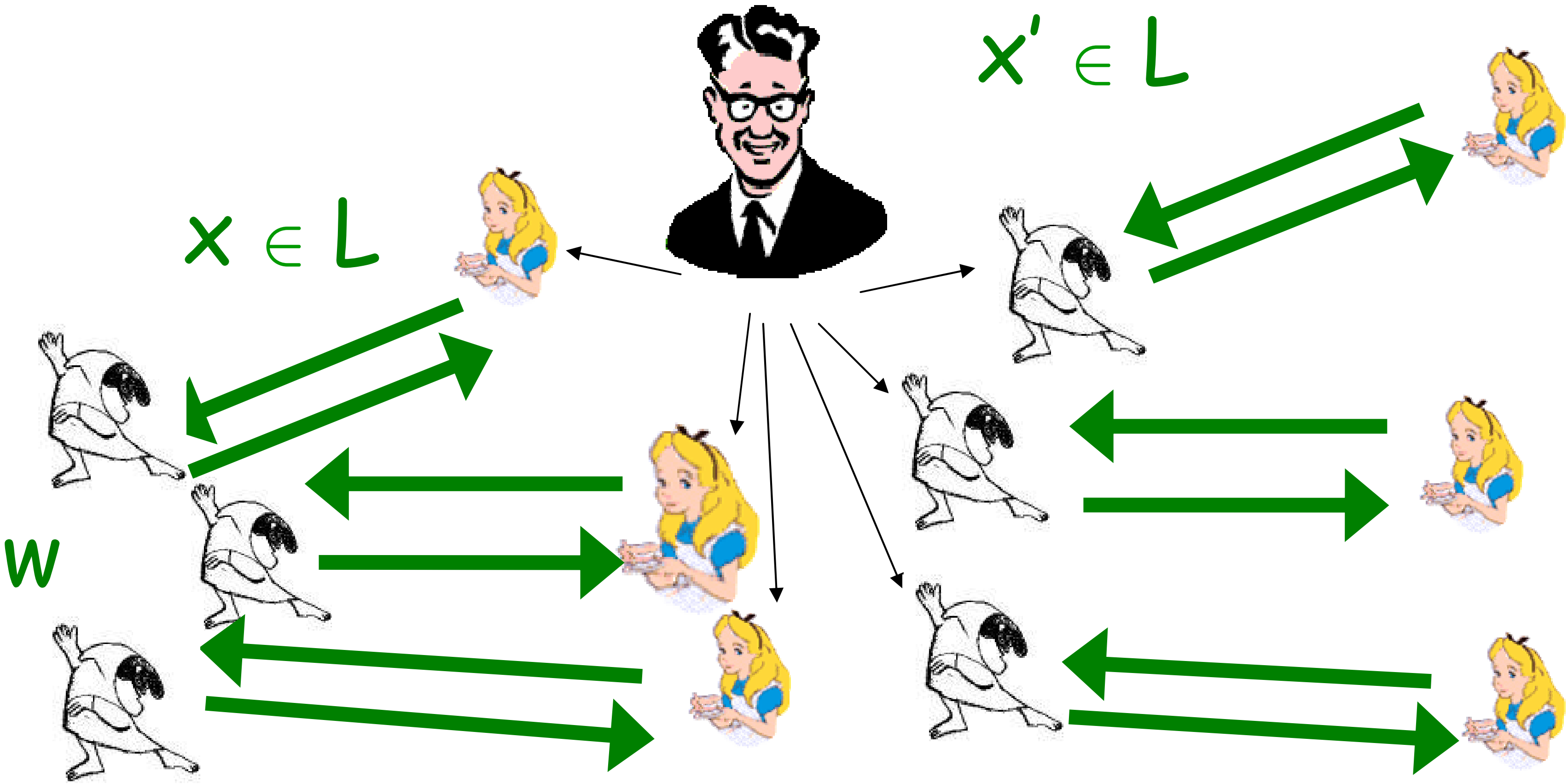
Outline

- Concurrent ZK, NMZK, Witness Indist.
- Non-Malleable Witness Indistinguishability
- Cnst-Rnd Concurrent NMWI in the plain model
- Cnst-Rnd Concurrent NMZK in the BPK Model
- UC with preprocessing

Man-in-the-Middle (MiM) Attack

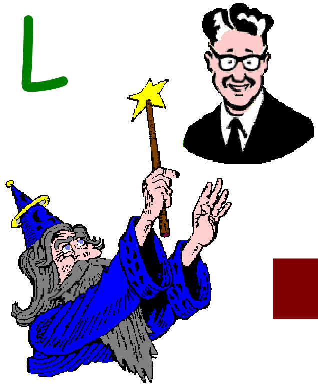


Concurrent MiM Attack



Concurrent NMZK

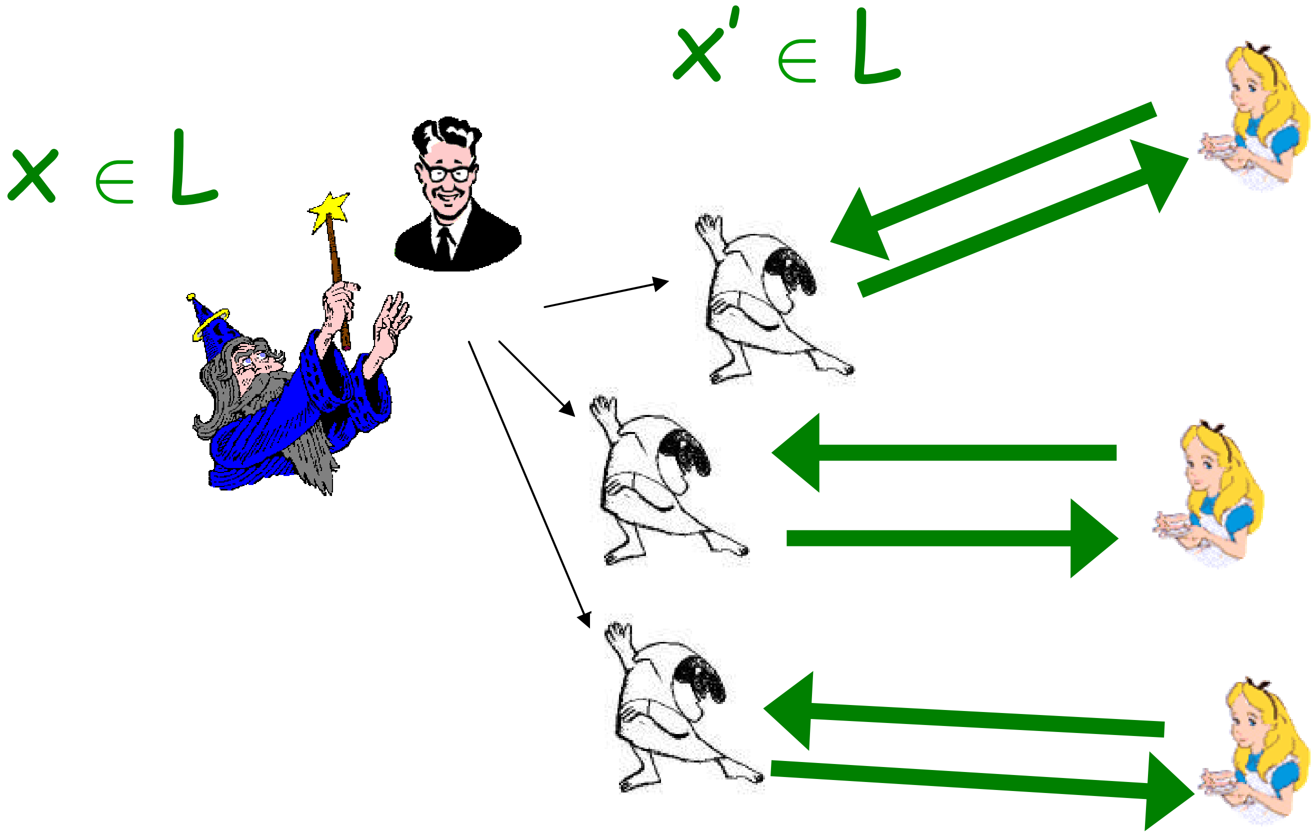
$x \in L$



$x' \in L$

$y' : (x', y') \in R_L$

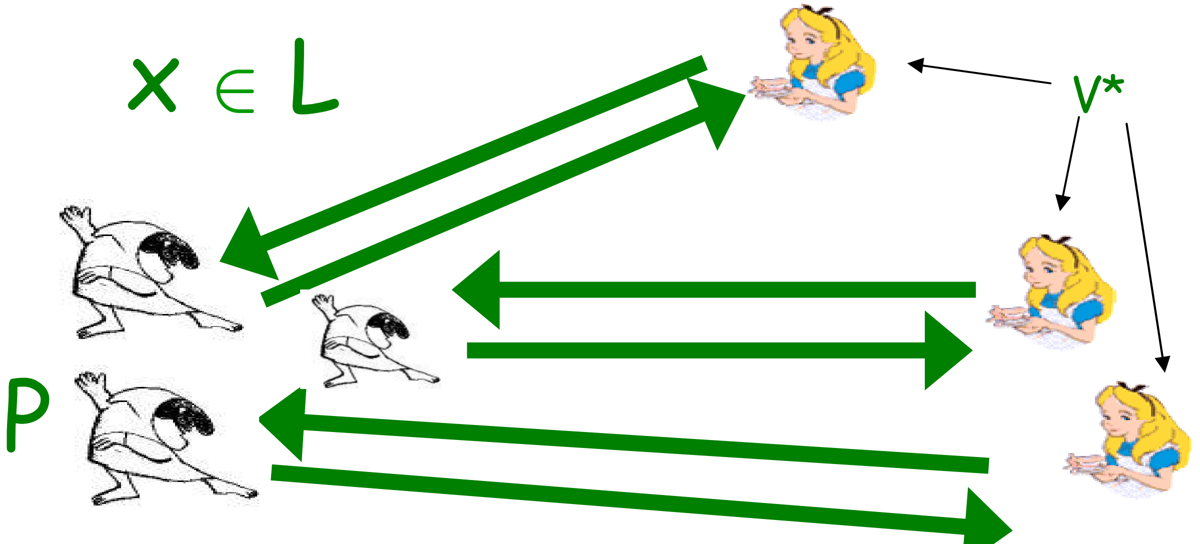
Concurrent NMZK



Outline

- Concurrent (ZK, NMZK), Witness Indist.
- Non-Malleable Witness Indistinguishability
- Cnst-Rnd Concurrent NMWI in the plain model
- Cnst-Rnd Concurrent NMZK in the BPK Model
- UC with preprocessing

Witness Indistinguishable Proofs



Witness Indistinguishability:

For all $x \in L$, for all pair (y,y') of valid witnesses for $x \in L$

ViewV*(P(y),x,y,y') $\approx$ ViewV*(P(y'),x,y,y') where

ZK implies WI

Witness Indistinguishability

ZK implies WI
but WI helps for the design of ZK protocols
(e.g., FLS-paradigm):
Non-Black-Box ZK
NIZK in the SRS model [FLS90,DDOPS01]

can we use a notion of WI secure against MiM attacks for the design of CNMZK protocols ?

Outline

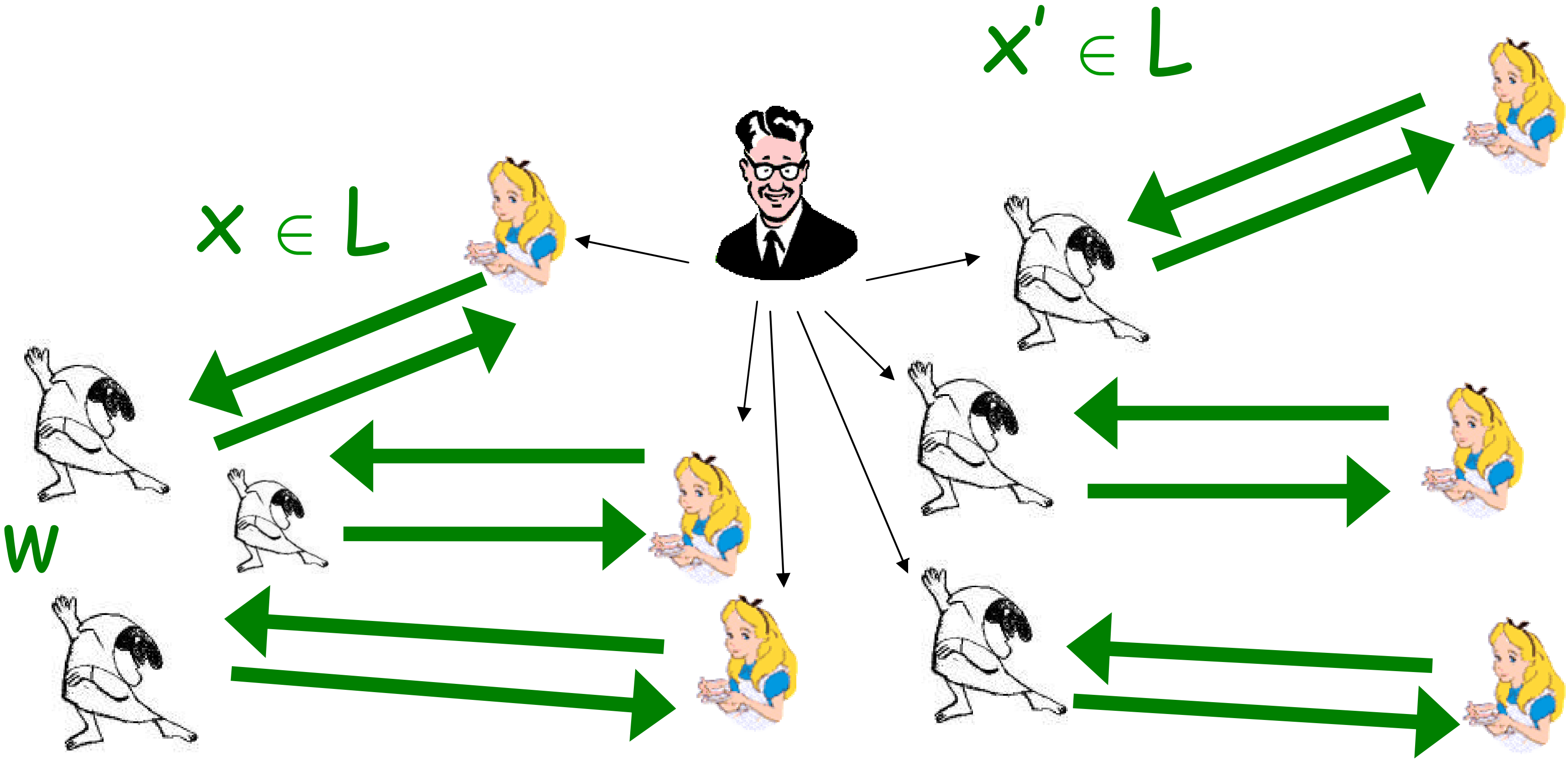
- Concurrent (ZK, NMZK), Witness Indist.
- Non-Malleable Witness Indistinguishability
- Cnst-Rnd Concurrent NMWI in the plain model
- Cnst-Rnd Concurrent NMZK in the BPK Model
- UC with preprocessing

Witness Encoded in a Proof

- we focus on commit-and-prove arguments where in the first message the prover commits to the witness by using a statistically binding (therefore we consider computational indistinguishability) commitment scheme (this message is the "witness encoded in the proof") and then proves that the committed message is an NP-witness for $x \in L$

- the goal of the MiM is to relate the witnesses encoded in the proofs he gives with the witnesses encoded in the proofs he receives

Concurrent MiM Attack



CNMWI, very informally

CNM Witness Indistinguishability:

“the distribution of the witnesses encoded in the proofs given by the man-in-the-middle is independent of the distribution of the witnesses encoded in the proofs given by the prover”

CNMWI, informally

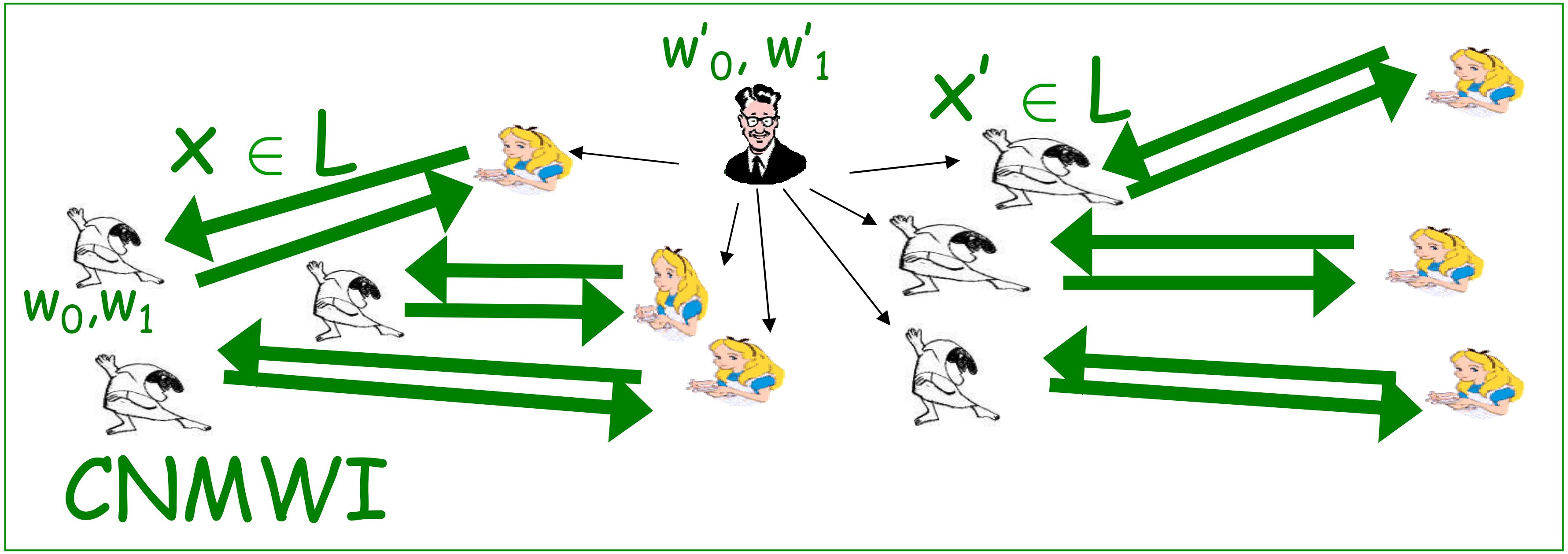
CNM Witness Indistinguishability:

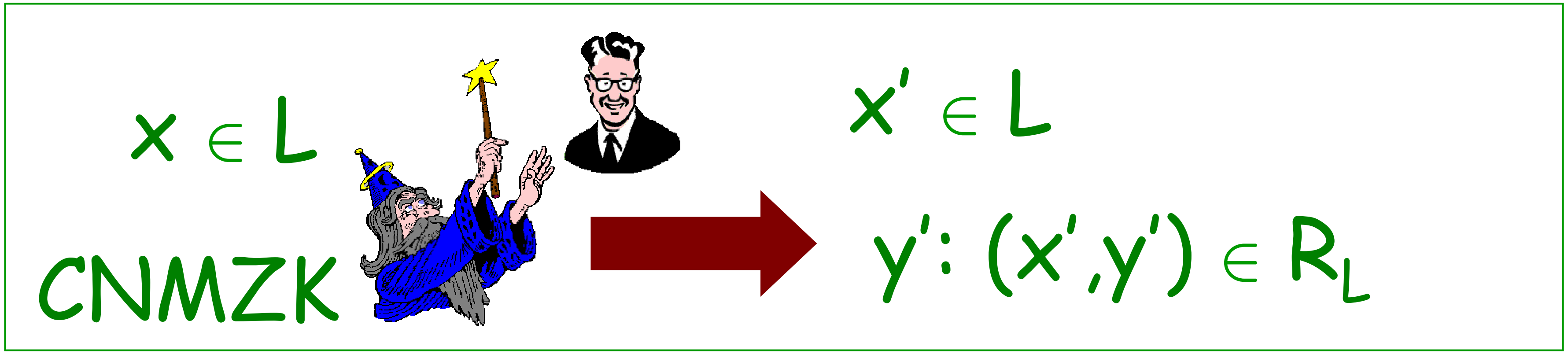
let $mim_{<x>}(<w>)$ the random variable that the describes the witnesses encoded in the proofs given by the mim when receiving proofs for $<x>$ from P with encoded witnesses $<w>$

CNMWI requires that the following distributions are comput. indistinguishable

$$\{mim_{<x>}(<w>)\}, \{mim_{<x>}(<w'>)\}$$

CNMZK vs CNMWI





CNMWI+ (informal)

CNMWI+ following the Simulation paradigm:

“for any PPT adversary *A* that in a MiM attack proves statements <x> to a honest verifier with proofs that encode witnesses <w>, there exists a ppt S that by accessing to *A* proves statements <x> to a honest verifier with proofs that encode witnesses_<w>”

this definition implies both the previous def. of CNMWI and that of CNMZK

CNM Commitments [PR05]

CNM Commitments:

"for any PPT adversary *A* that in a MiM attack commits to messages <w>, there exists a PPT S that by accessing to *A* outputs commitments to messages <w>"

Can CNM commitment schemes help for designing CNMWI argument systems ?

Outline

- Concurrent ZK, NMZK, Witness Indist.
- Non-Malleable Witness Indistinguishability
- Cnst-Rnd Concurrent NMWI in the plain model
- Cnst-Rnd Concurrent NMZK in the BPK Model
- UC with preprocessing

Constant Round CNMWI

P→V send a commitment of the witness w
P→V use the one-left many-right statistical concurrent non-malleable ZK argument of knowledge of [PR05a] for proving that w is a witness for $x \in L$

Remark: this protocol is a PoK and it is only a cosmetic variation of the one by [PR05b] for concurrent non-malleable commitments

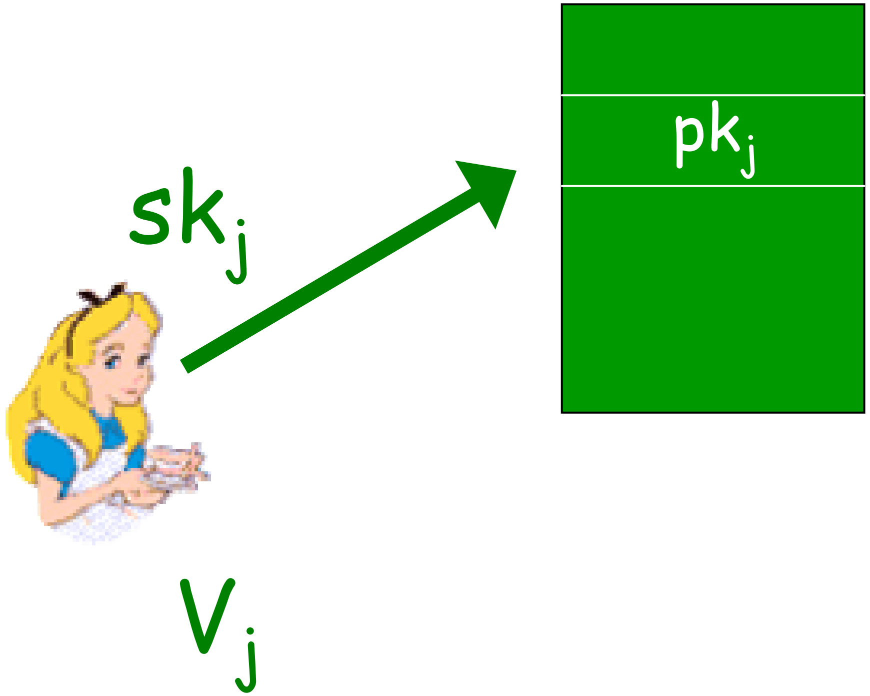
Outline

- Concurrent ZK, NMZK, Witness Indist.
- Non-Malleable Witness Indistinguishability
- Cnst-Rnd Concurrent NMWI in the plain model
- Cnst-Rnd Concurrent NMZK in the BPK Model
- UC with preprocessing

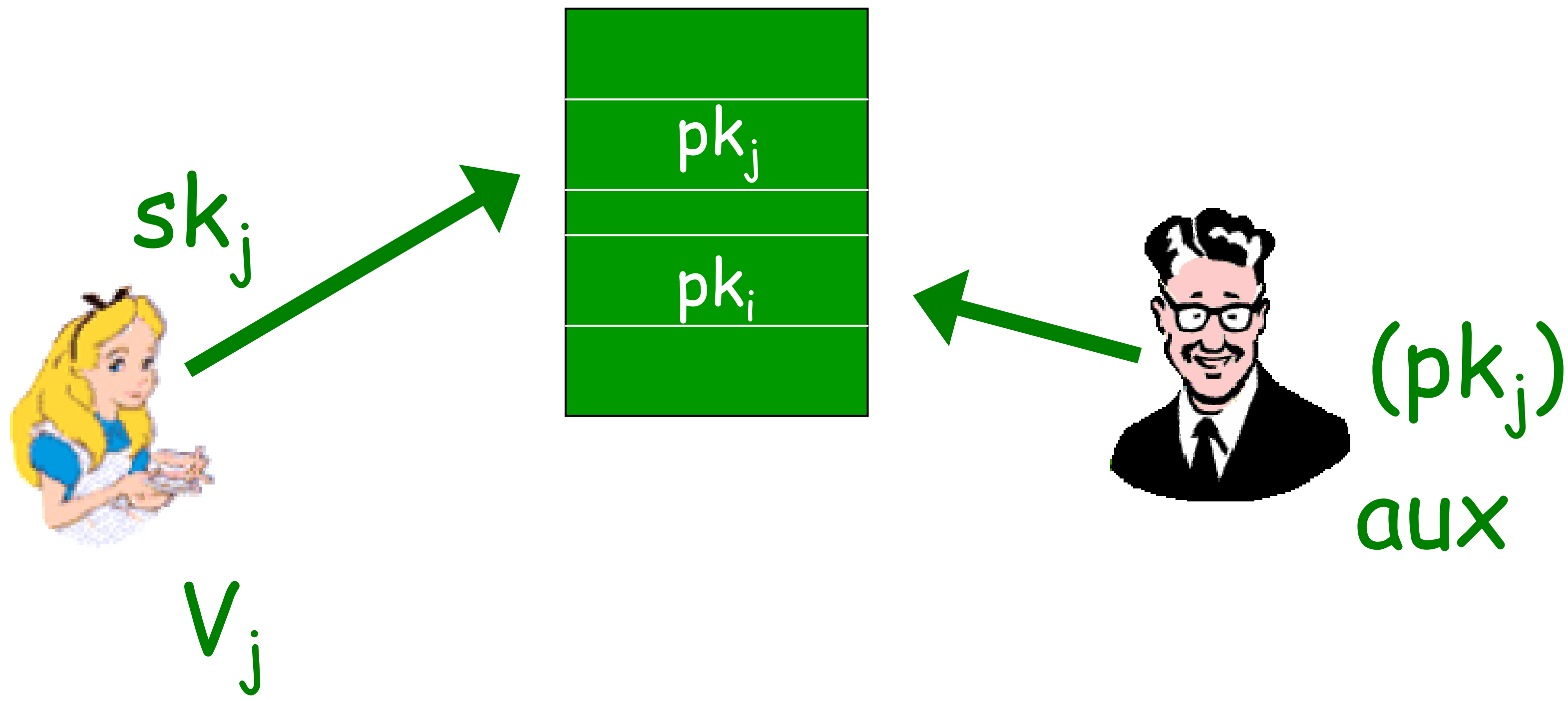
The Bare Public-Key (BPK) model (CGGM00)

- In a key-registration stage:
  - Each verifier (non-interactively) posts her public key on a public file, common to all parties
  - There is no bound on the power of the adversary that therefore can control the entire resulting file
- In the proof stage:
  - The same public file is part of the common input in all proofs and the verifiers can use their private keys
- BPK is a weaker version of the (PKI) model since
  - public keys do NOT need to be certified during the key-registration phase

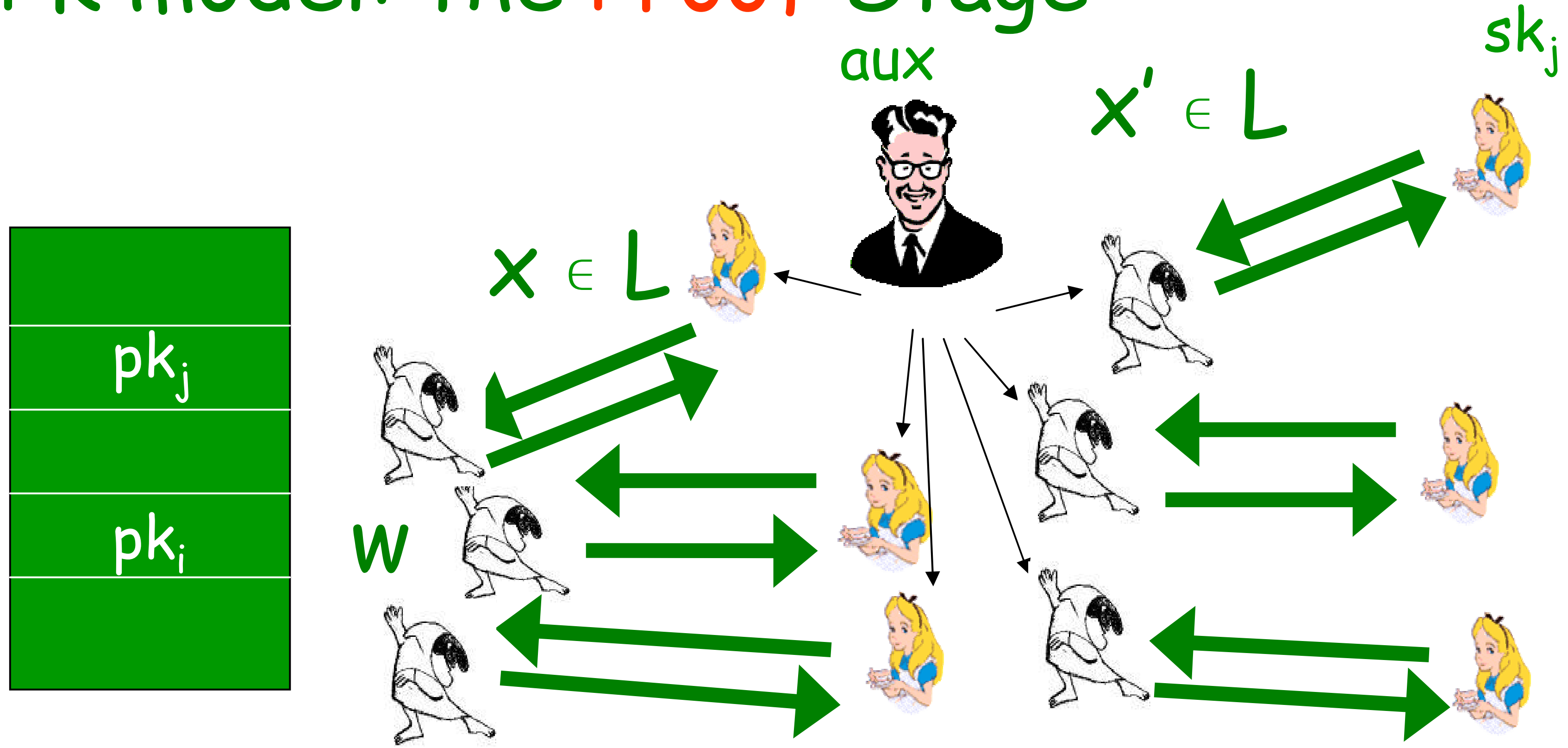
BPK model: the Key-Registration Stage



BPK model: first attack of the MiM



BPK model: the Proof Stage



CNMZK in the BPK model

y_{j0},$=f(sk_{j0})$, $y_{i1}=f(sk_{j1})$

y_{j0} y_{j1}

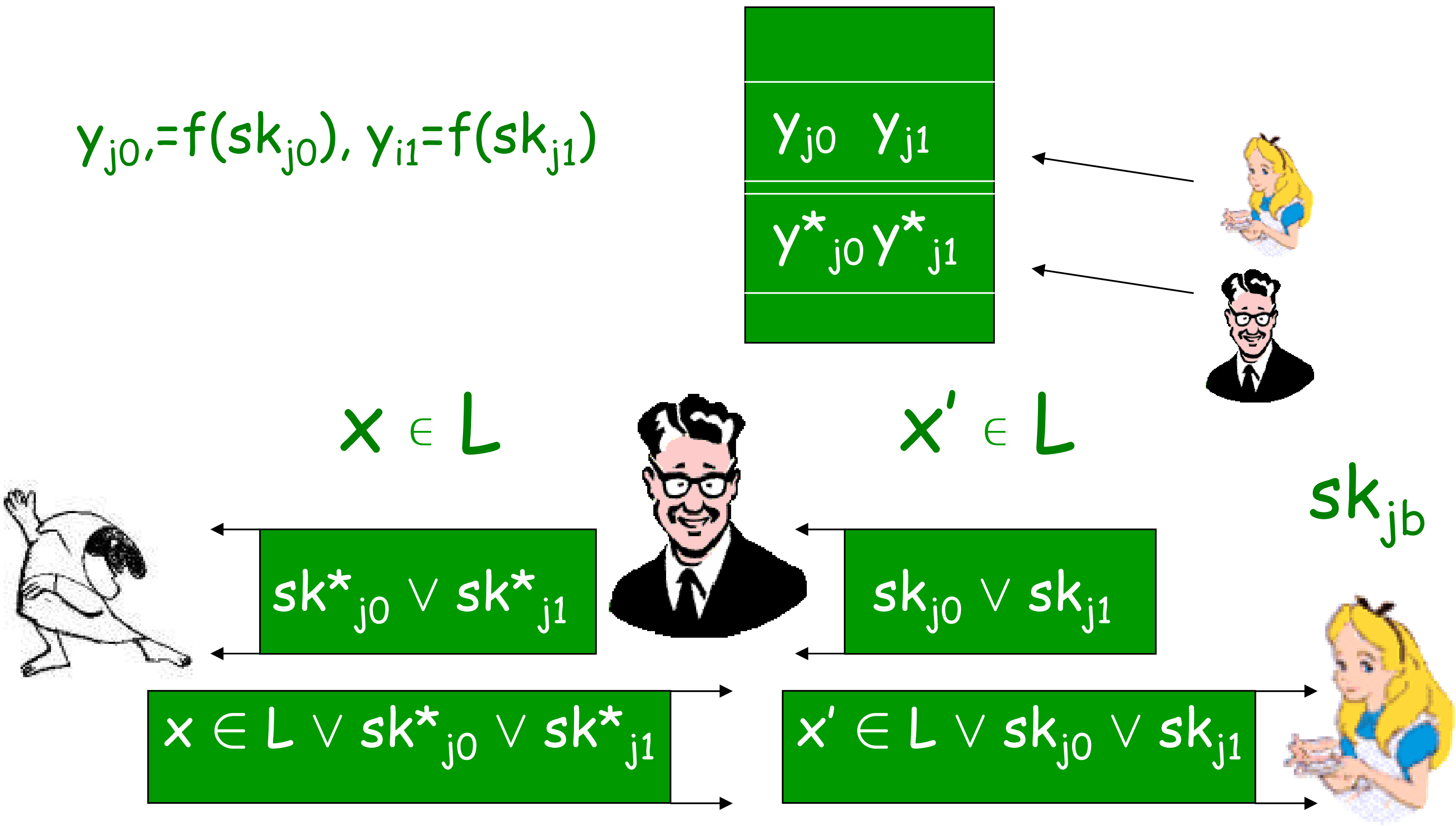
$x \in L$

CNMWIPoK $sk_{j0} \vee sk_{j1}$

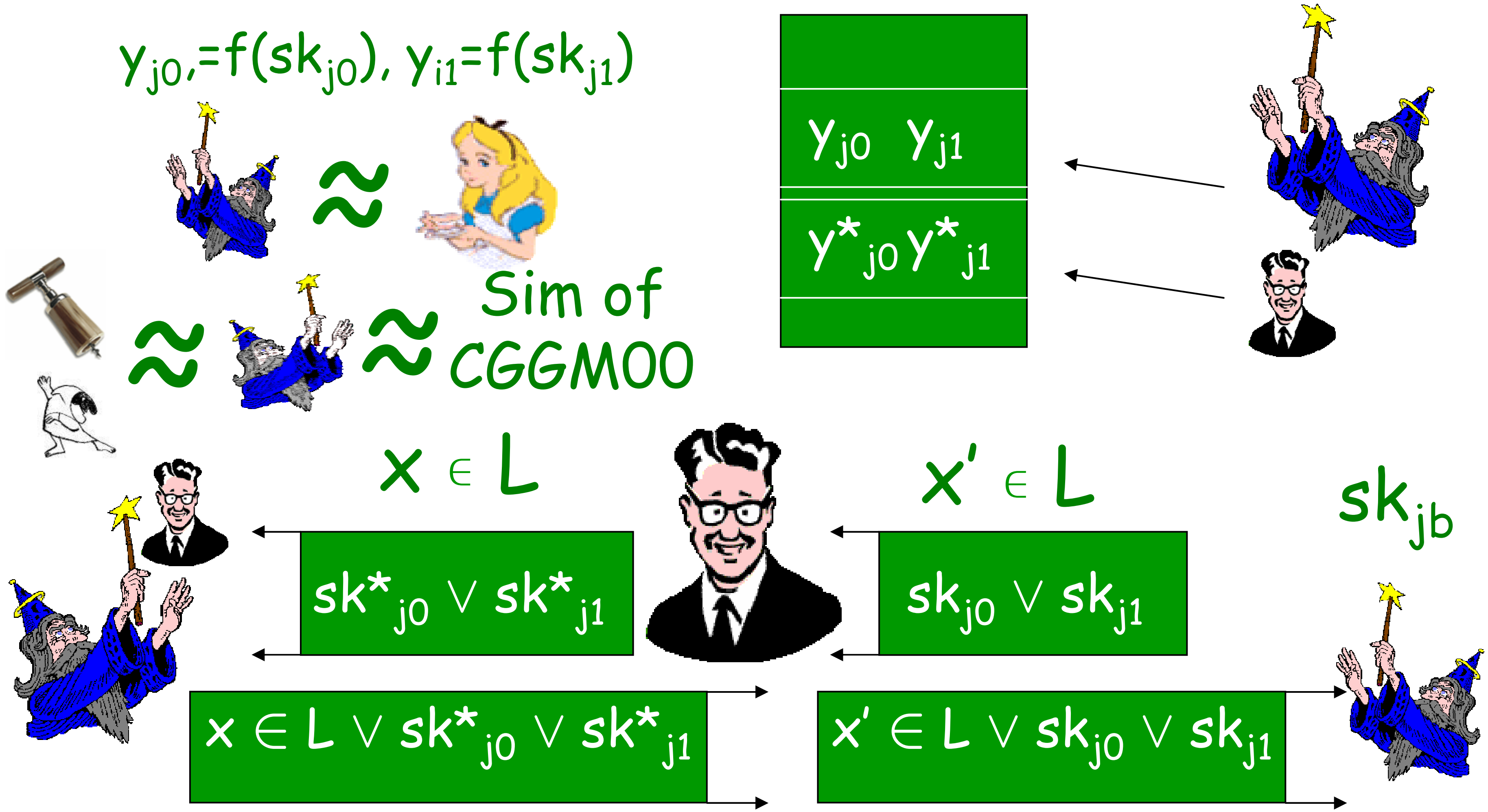
CNMWIPoK $x \in L \vee sk_{j0} \vee sk_{j1}$

sk_{jb}

Man-in-the-Middle Attack



Simulator for the MiM



Concurrent NMZK

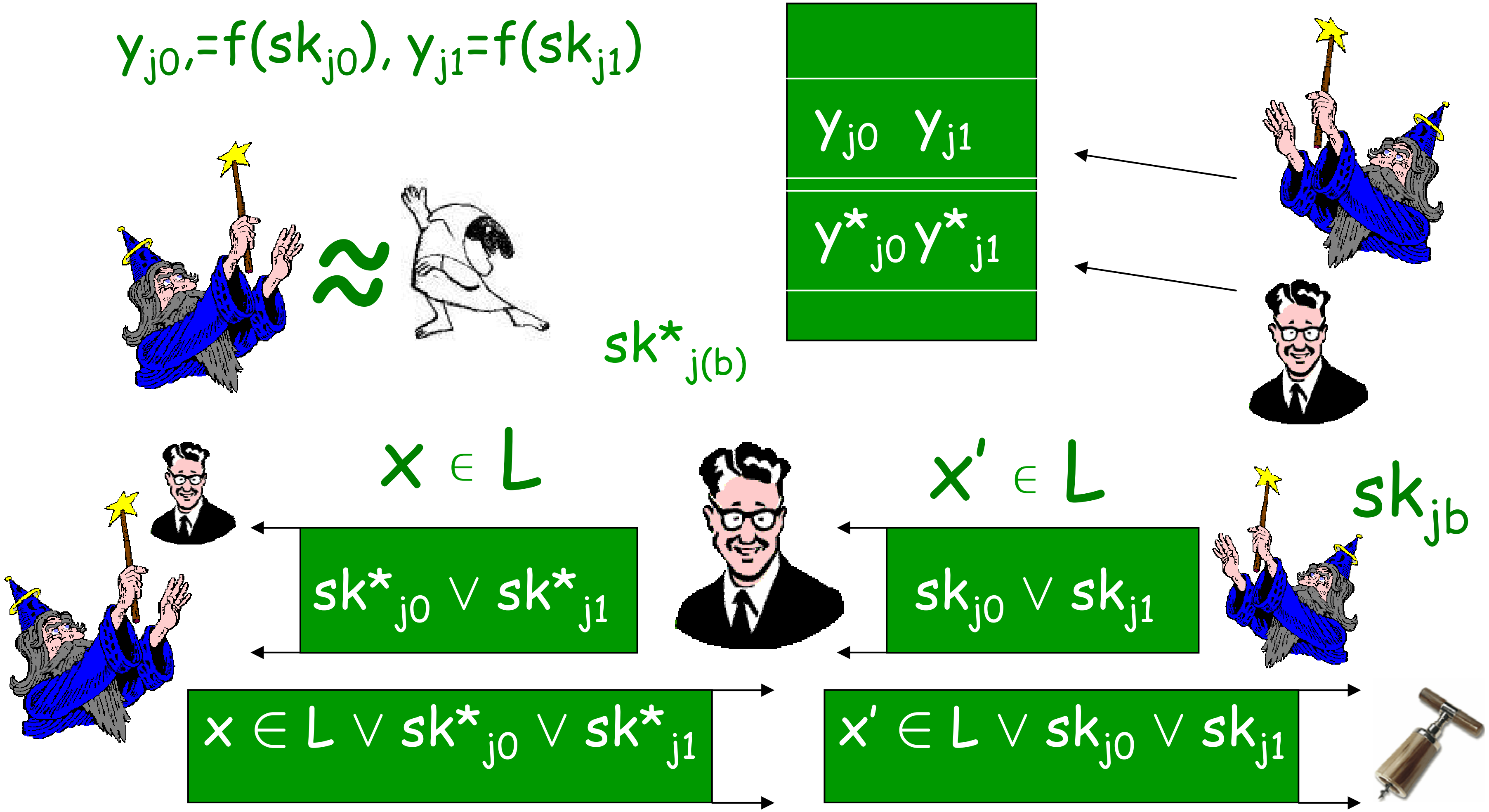
$x \in L$

$x' \in L$

$y' : (x', y') \in R_L$

Simulator for the MiM

$y_{j0}, = f(sk_{j0}),\ y_{j1} = f(sk_{j1})$



Concurrent NMZK

$x \in L$

$x' \in L$

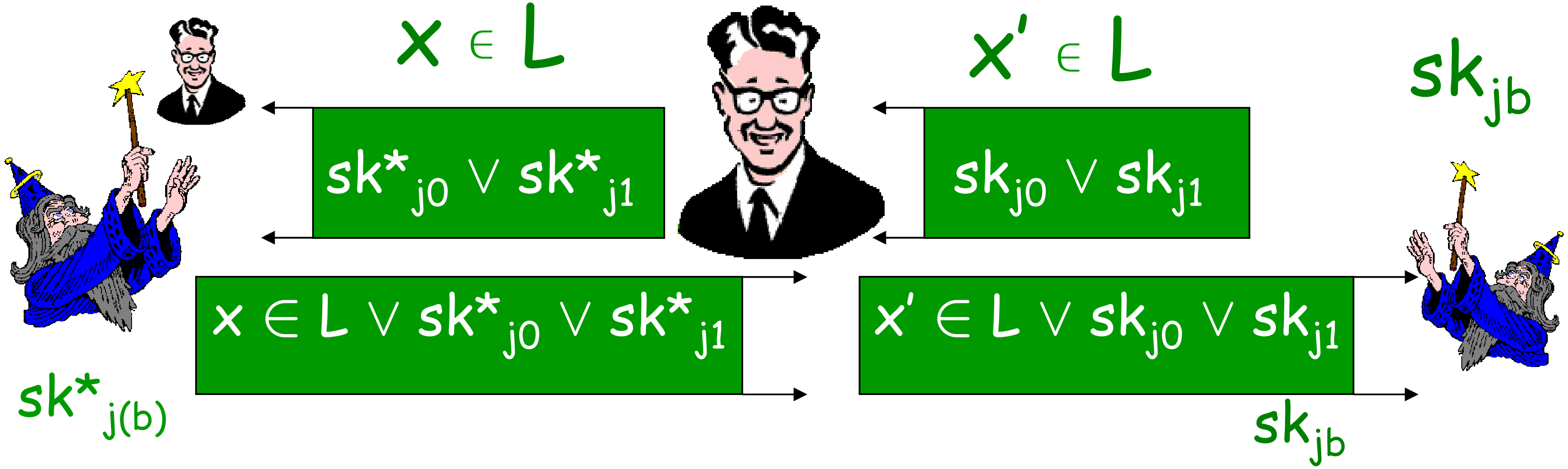
get $w \in \{y', sk_{j0}, sk_{j0}\}$

if $(w == y')$ ✓

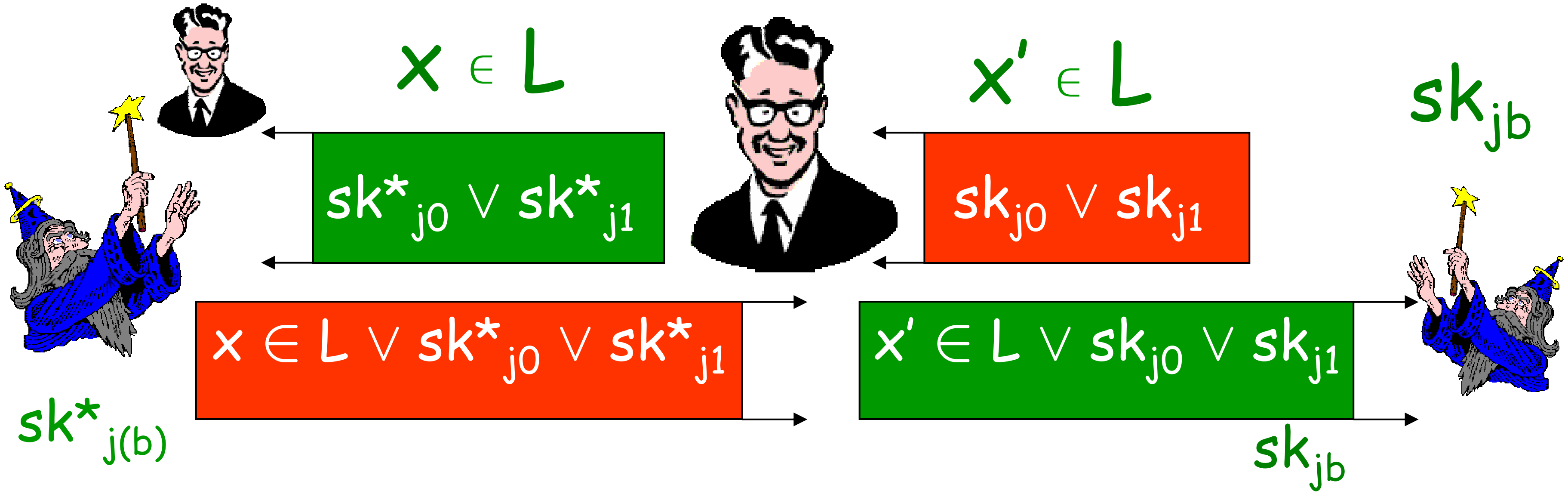
else if $(w == sk_{j(1-b)})$ ✓

else if $(w == sk_{jb})$??

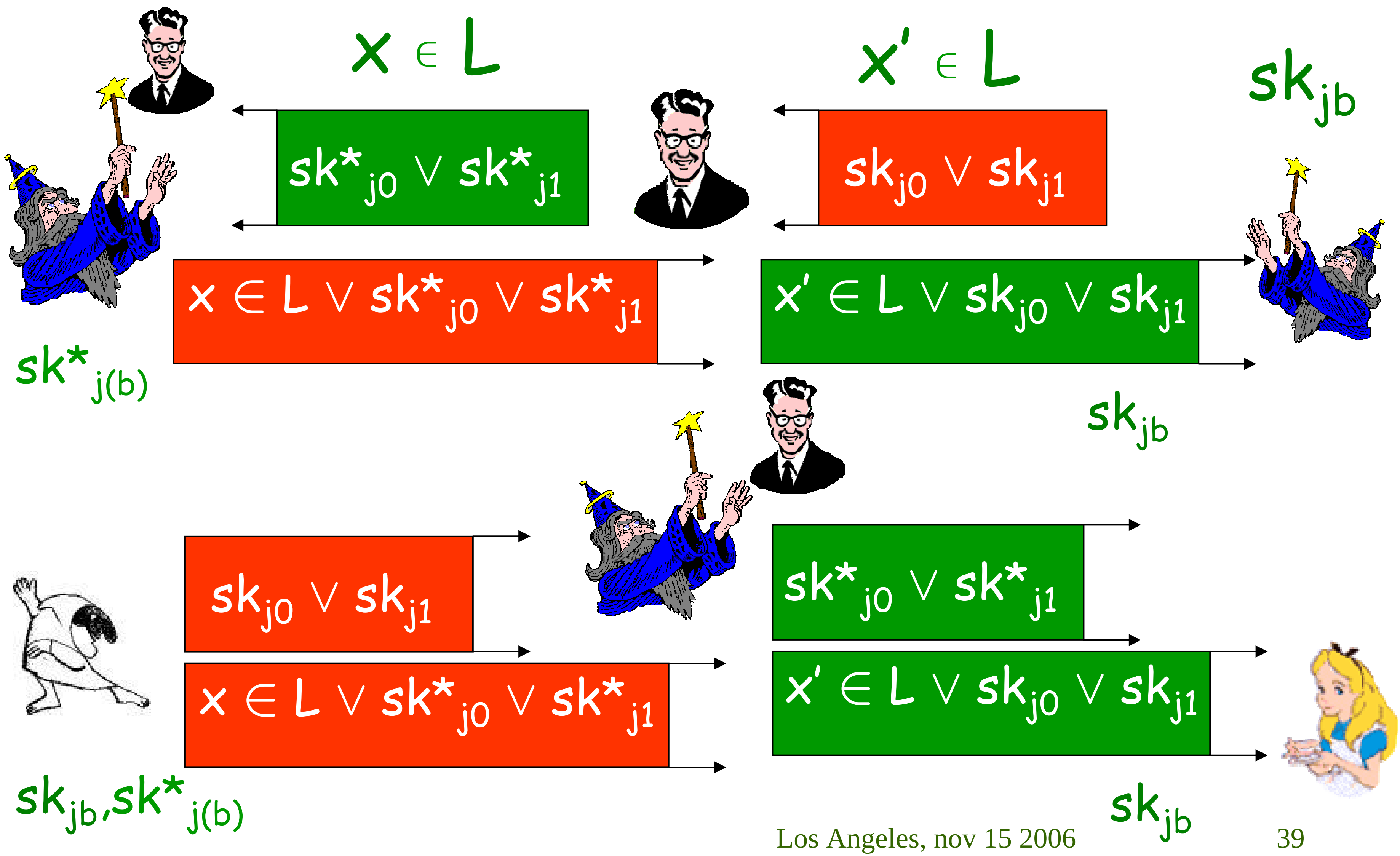
Simulator for the MiM



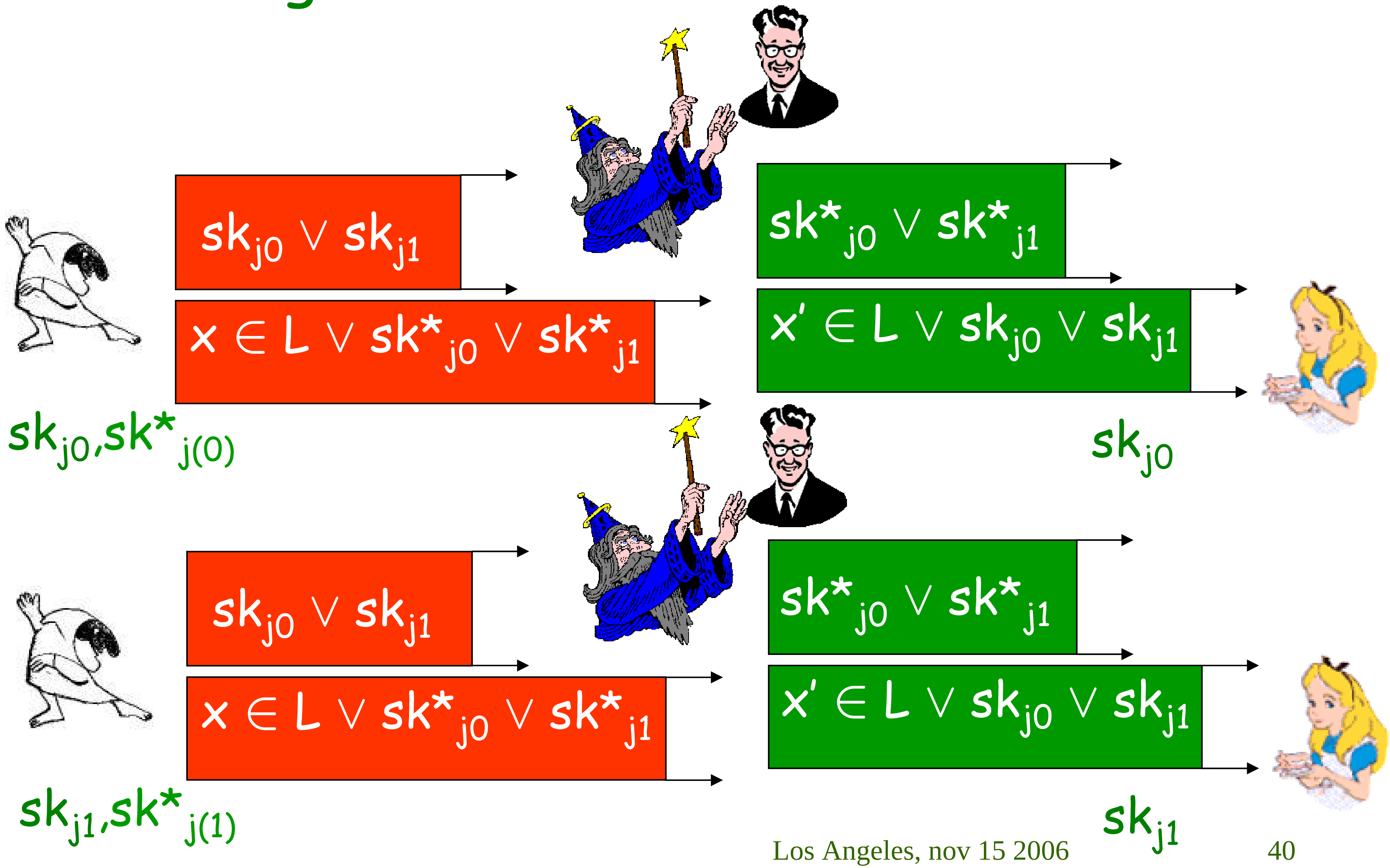
Simulator for the MiM



The MiM for CNMZK in BPK is reduced to a MiM for CNMWI in the plain model



Reducing the MiM to a MiM for CNMWI



Comparison with previous CNMZK

Paper	Model
DDOPS 01	Shared Random String
PS 04 / BS 05	Relaxed Security
KLP 05	Timing Assumption
PRS 06	Plain (polylog rounds)
This work	Bare Public Key

Outline

- Concurrent ZK, NMZK, Witness Indist.
- Non-Malleable Witness Indistinguishability
- Cnst-Rnd Concurrent NMWI in the plain model
- Cnst-Rnd Concurrent NMZK in the BPK Model
- UC with preprocessing

UC [Can01+CLOS02+BCNP04]

- [CLOS02] UC for any functionality can be reduced to realizing $\mathcal{F}_{mcom}$ (multi-instance commitment functionality)
- [BCNP04] $\mathcal{F}_{mcom}$ can be reduced to realizing $\mathcal{F}_{kr}$ (key registration funct.)

Key Registration Funct. [BCNP04]

- F_{kr} requires that the functionality can see each private key and guarantees that
  - each party has a well formed public key
  - the public keys of the honest parties are safe (private keys are not known by the adversary)

Key Registration Funct. [BCNP04]

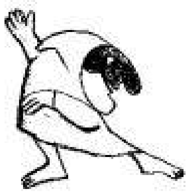
- F_{kr} is realized in BCNP04
  - assuming the existence of trusted third parties
    - with any F_{crs}
    - with a PKI-like registration service where the key authority generates public keys and gives the public keys to parties
    - with a PKI-like registration service where parties generates keys but have to the send both the public and secret keys to the authority
    - with semi-trusted authorities
  - assuming isolated stand-alone executions
    - each party generates a public key and gives a ZKPoK of the secret key to a trusted authority

UC with Preprocessing

- key-stage preprocessing (non-interactive):
  - run the key-stage of the CNMZK protocol in the BPK model; each party generates and posts also the additional public key PK used in BCNP04
- key-knowledge preprocessing (interactive):
  - each party interested in running protocols with other parties, runs the proof stage of the CNMZK protocol in the BPK model, proving knowledge of the secret key SK

Comparison with previous results

Paper	Model
CLOS 02	Common Reference String
BCNP 04	TTP or Isolated ZKPoK
PS 04 / BS 05	Relaxed Security
KLP 05	Timing Assumption
This work	Preprocessing (2 stages)



the prover

Thanks!

the verifier

the extractor

the simulator

the man-in-the-middle