

Secure Identification with RFID Chips/PUFs

Ivan Visconti
Univ. of Salerno - ITALY

joint work with:

Carlo Blundo
Univ. of Salerno
ITALY

Giuseppe Persiano
Univ. of Salerno
ITALY

Ahmad-Reza Sadeghi
Ruhr-Univ. Bochum
GERMANY

Christian Wachsmann
Ruhr-Univ. Bochum
GERMANY

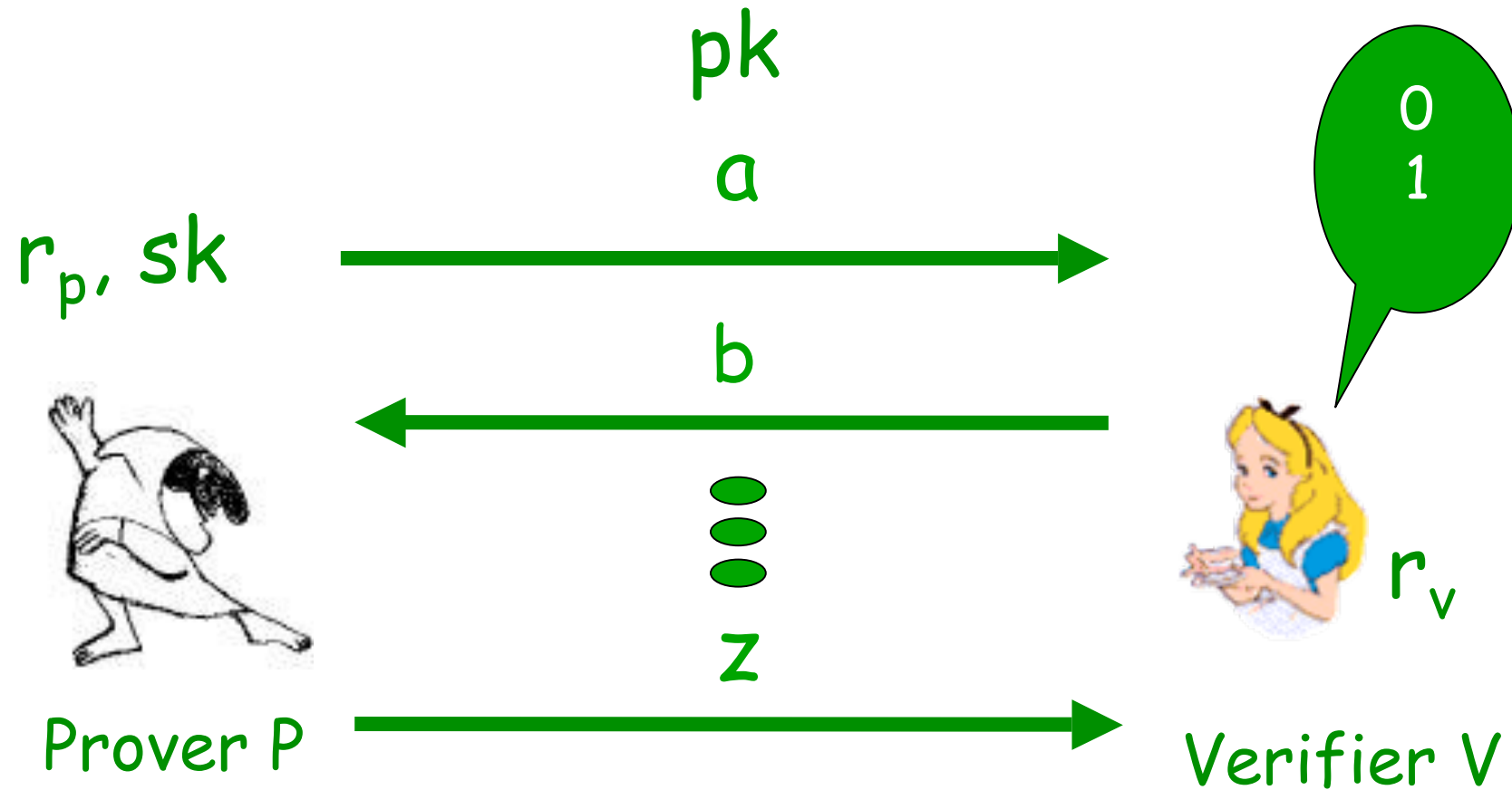
Security HW in Theory and Practice

- * Hardware considered in this talk:
 - RFID chips
 - Isolators
 - PUFs
- * Security properties that we will consider:
 - Non-Transferability in Identification
 - Resettability
 - Privacy and Unclonability

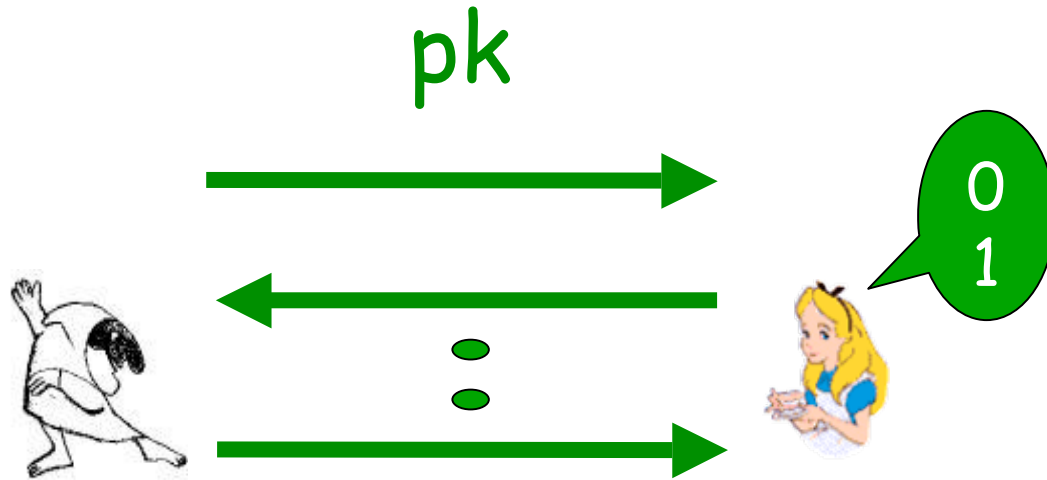
Outline

- Identification protocols
- MiM attacks
 - on-line vs off-line
 - Designated-verifier approach
- Reset attacks
- Transferability of some known proposals
- New Protocol
- Cheaper Identification

Identification Protocol (IDP)



IDP - Requirements



basic properties:

completeness: if P knows sk then V outputs 1

soundness: if P does not know sk then V outputs 0

Motivation: IDP for e-Passports

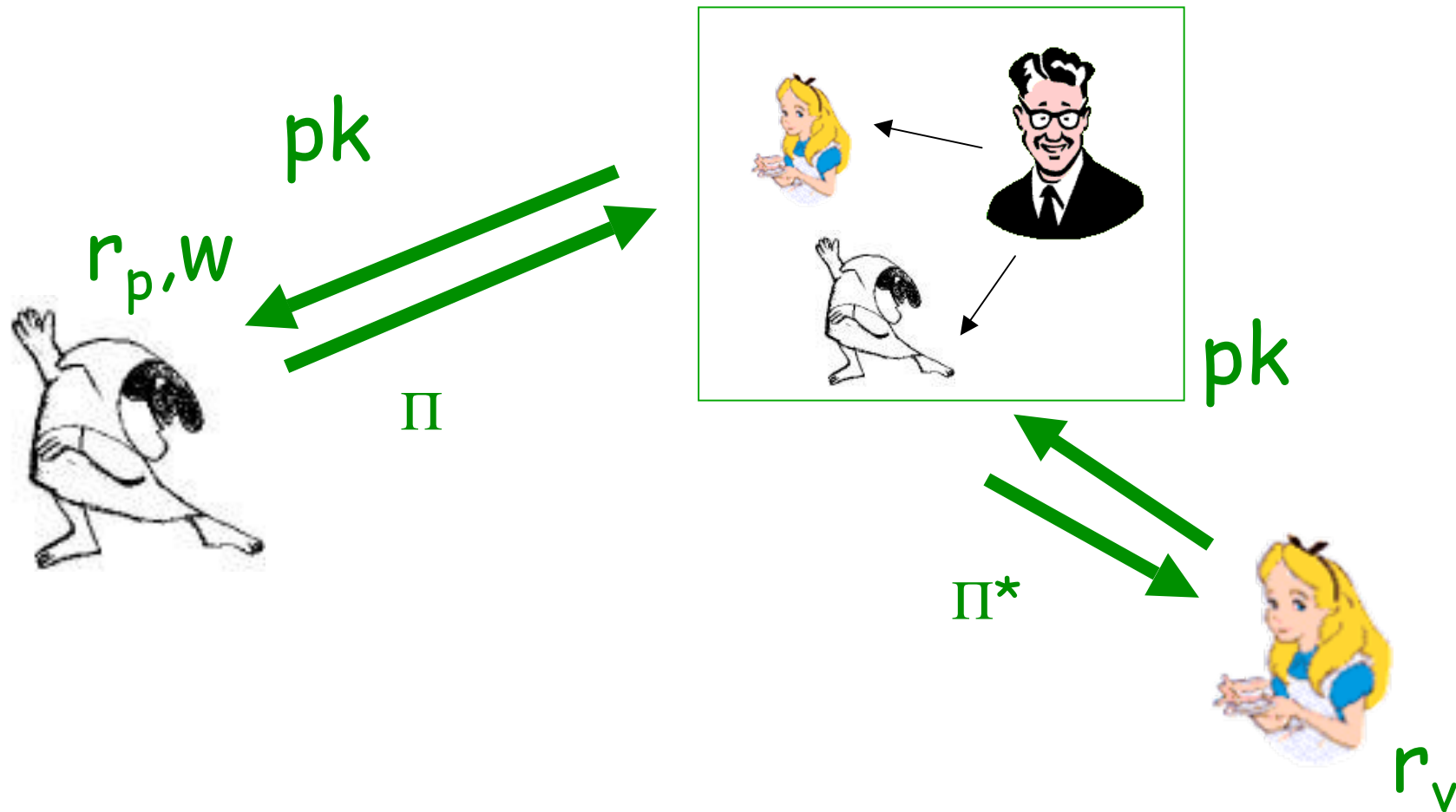
- ★ **RFID** Communication between secure chip and reader
- ★ Stored data on chip
 - Name, Passport No, Date of birth, Date of expiry
 - Biometrical data (facial Image, fingerprint, ...)
- ★ Main cryptographic protocols
 - Passive Authentication (mandatory)
uses digital signature by issuer (data signed)
 - Active Authentication (optional)
deployed against anti-cloning (signature of a challenge)
 - Basic Access Control (BAC) (optional) for secure communication
 - Extended Access Control (next generation of E-Passport)
chip and terminal authentication
 - ★ At the border control, E-Passports will play an Identification Protocol



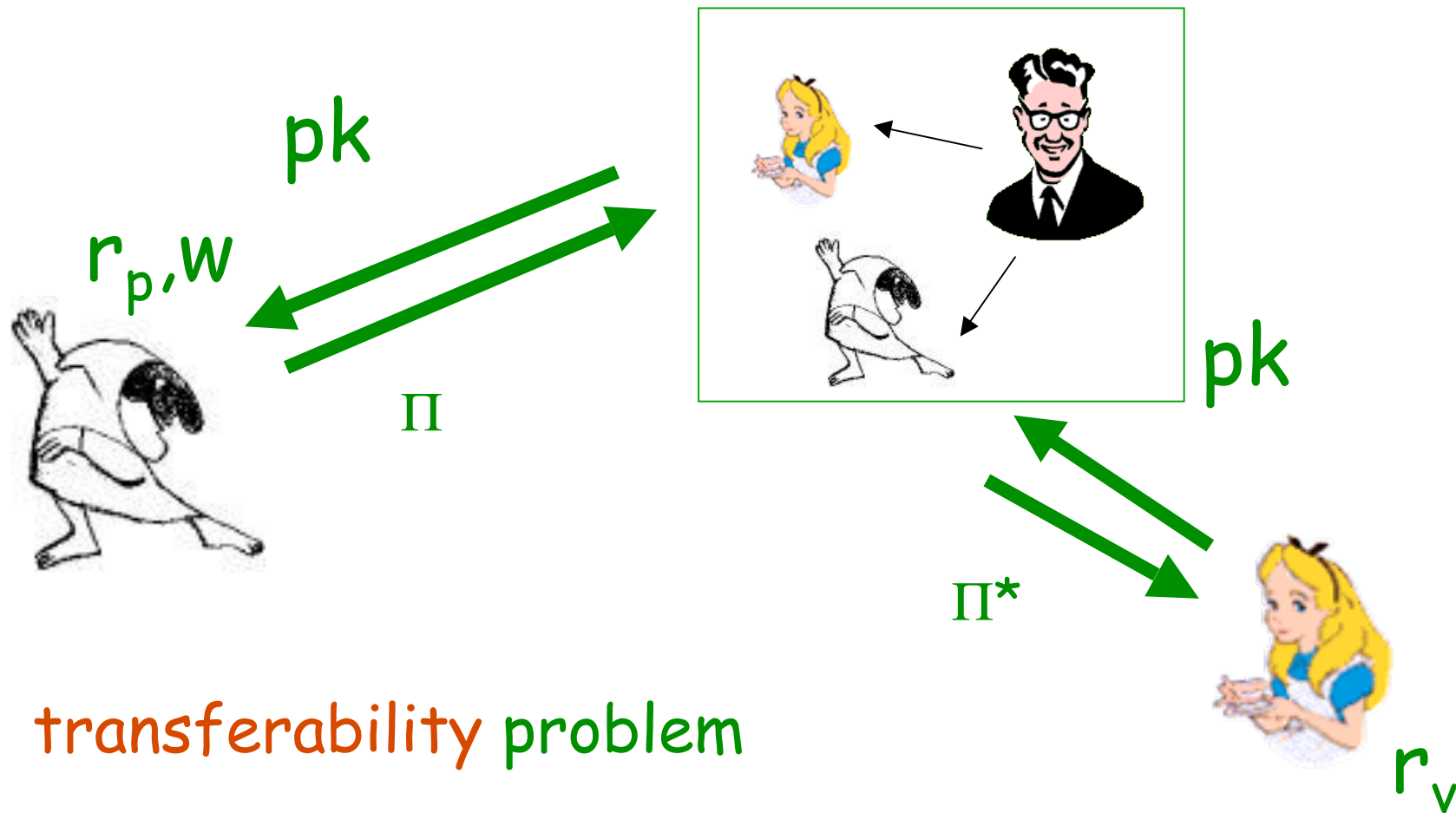
Outline

- Identification protocols
- **MiM attacks**
 - on-line vs off-line
 - Designated-verifier approach
- Reset attacks
- Transferability of some known proposals
- New Protocol
- Cheaper Identification

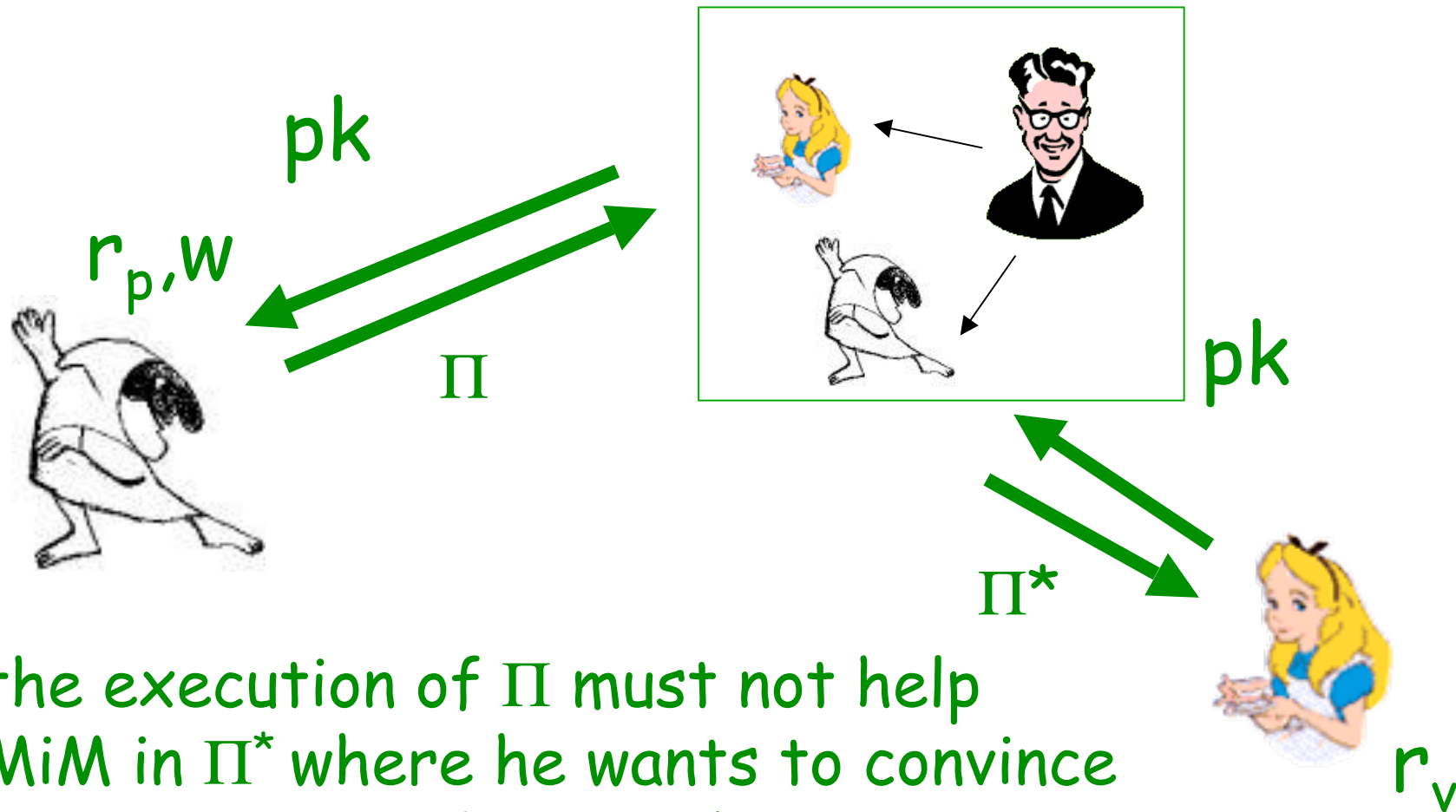
Man-in-the-Middle (MiM) Attack



Man-in-the-Middle (MiM) Attack

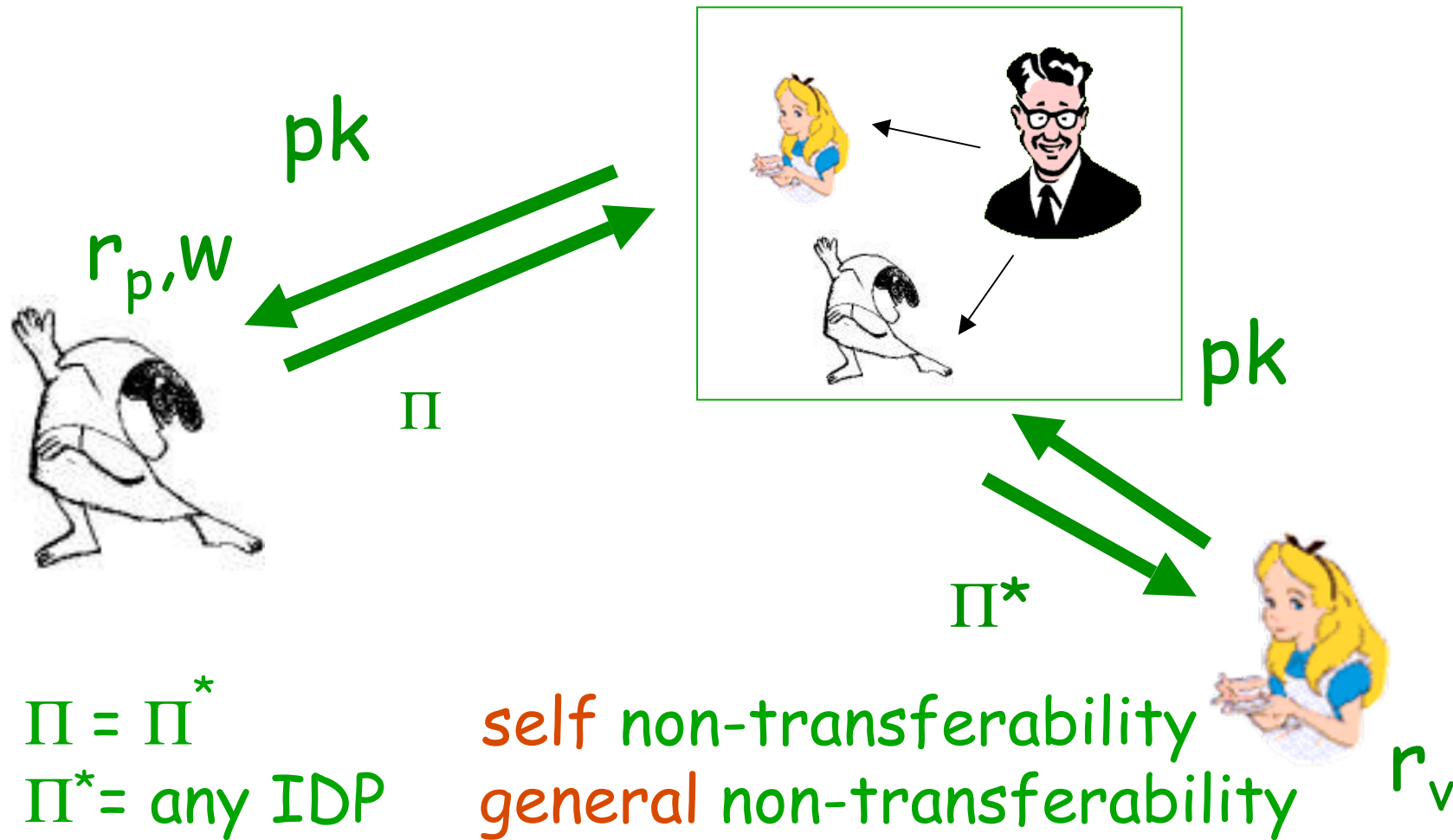


Non-Transferable Identification

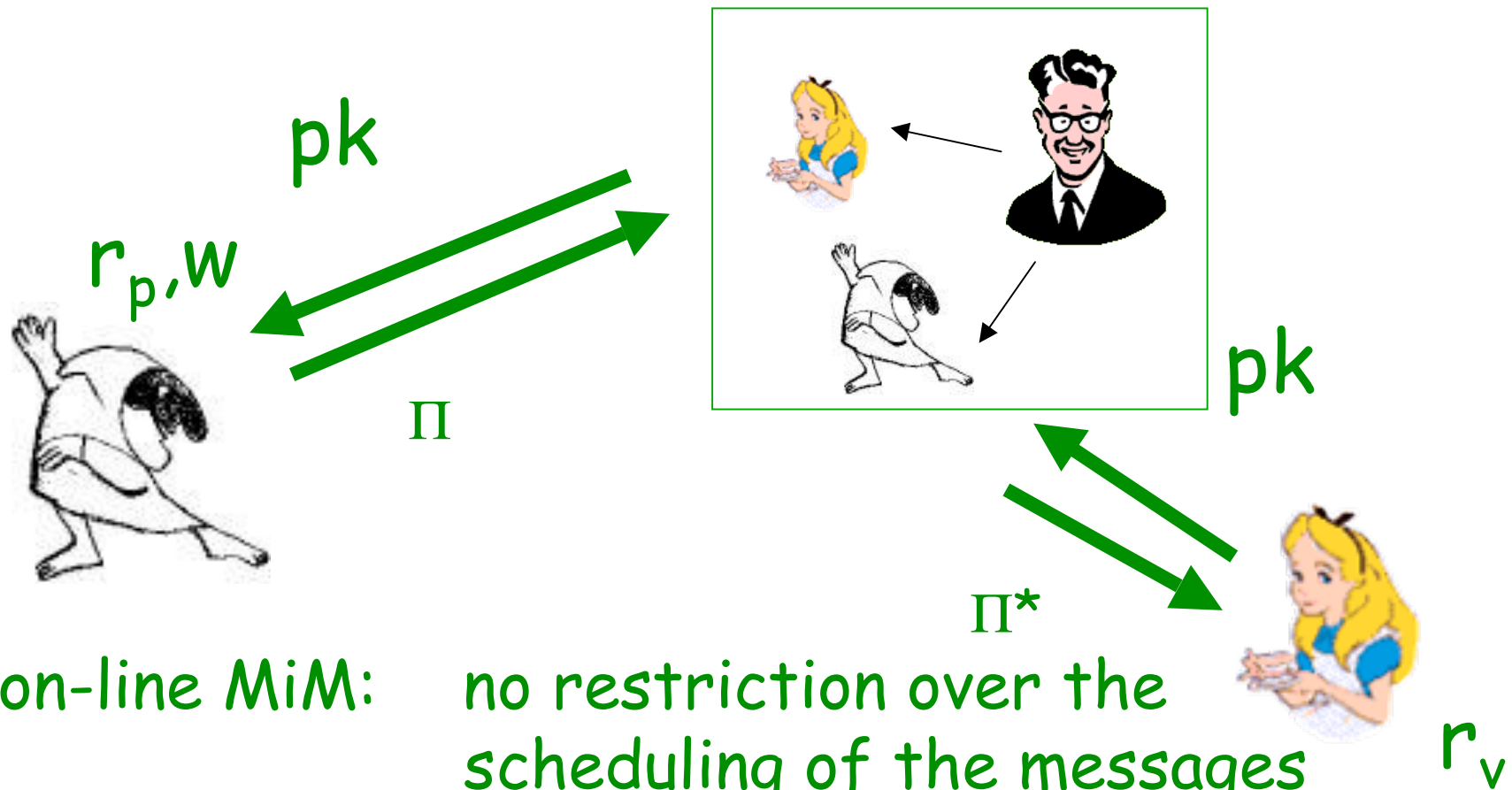


the execution of Π must not help
MiM in Π^* where he wants to convince
honest V over identity pk

Non-Transferable Identification



Man-in-the-Middle (MiM) Attack

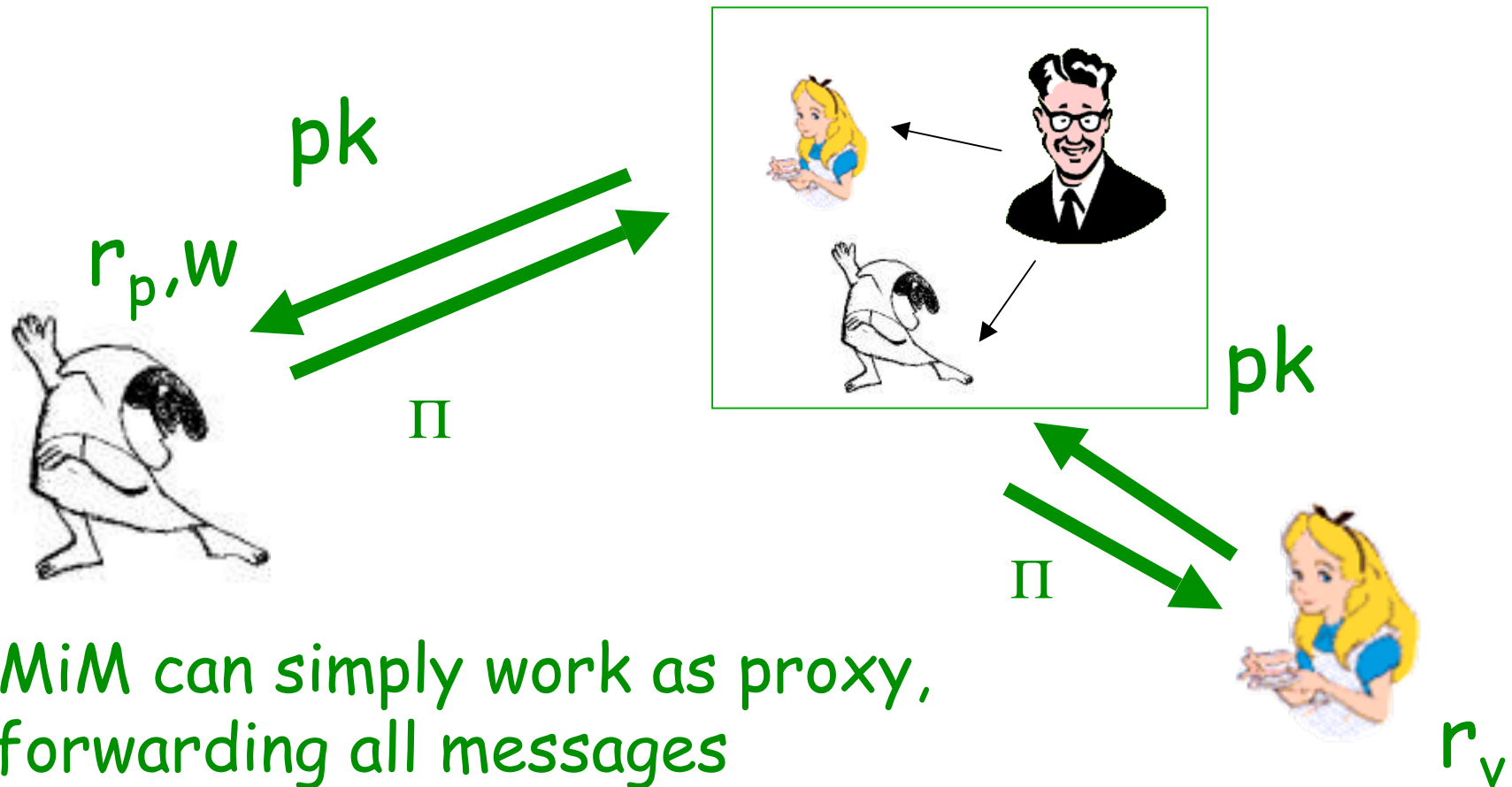


- on-line MiM: no restriction over the scheduling of the messages
- off-line MiM: Π is executed in isolation

Outline

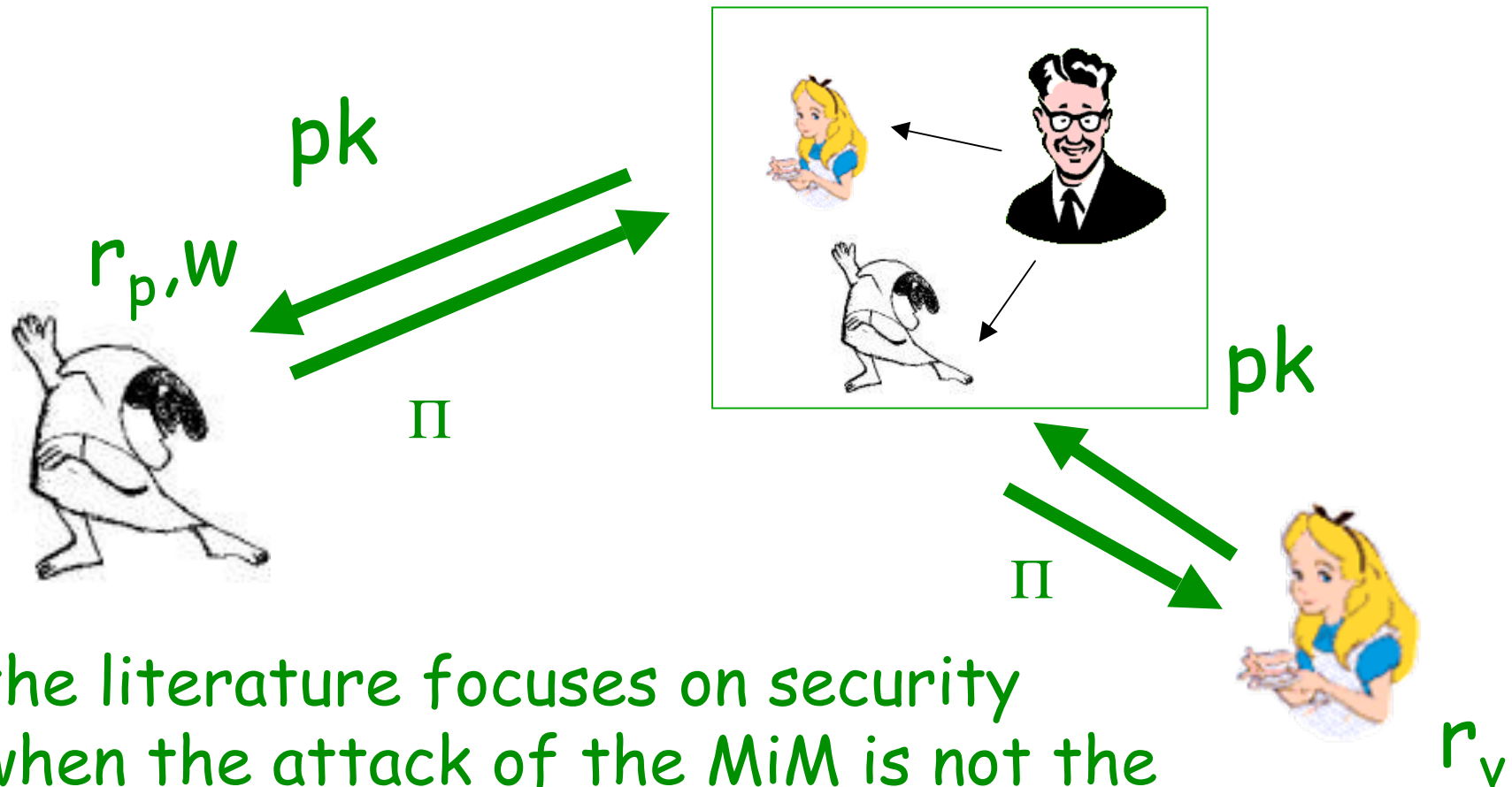
- Identification protocols
- MiM attacks
 - on-line vs off-line
 - Designated-verifier approach
- Reset attacks
- Transferability of some known proposals
- New Protocol
- Cheaper Identification

On-Line MiM Kills any IDP



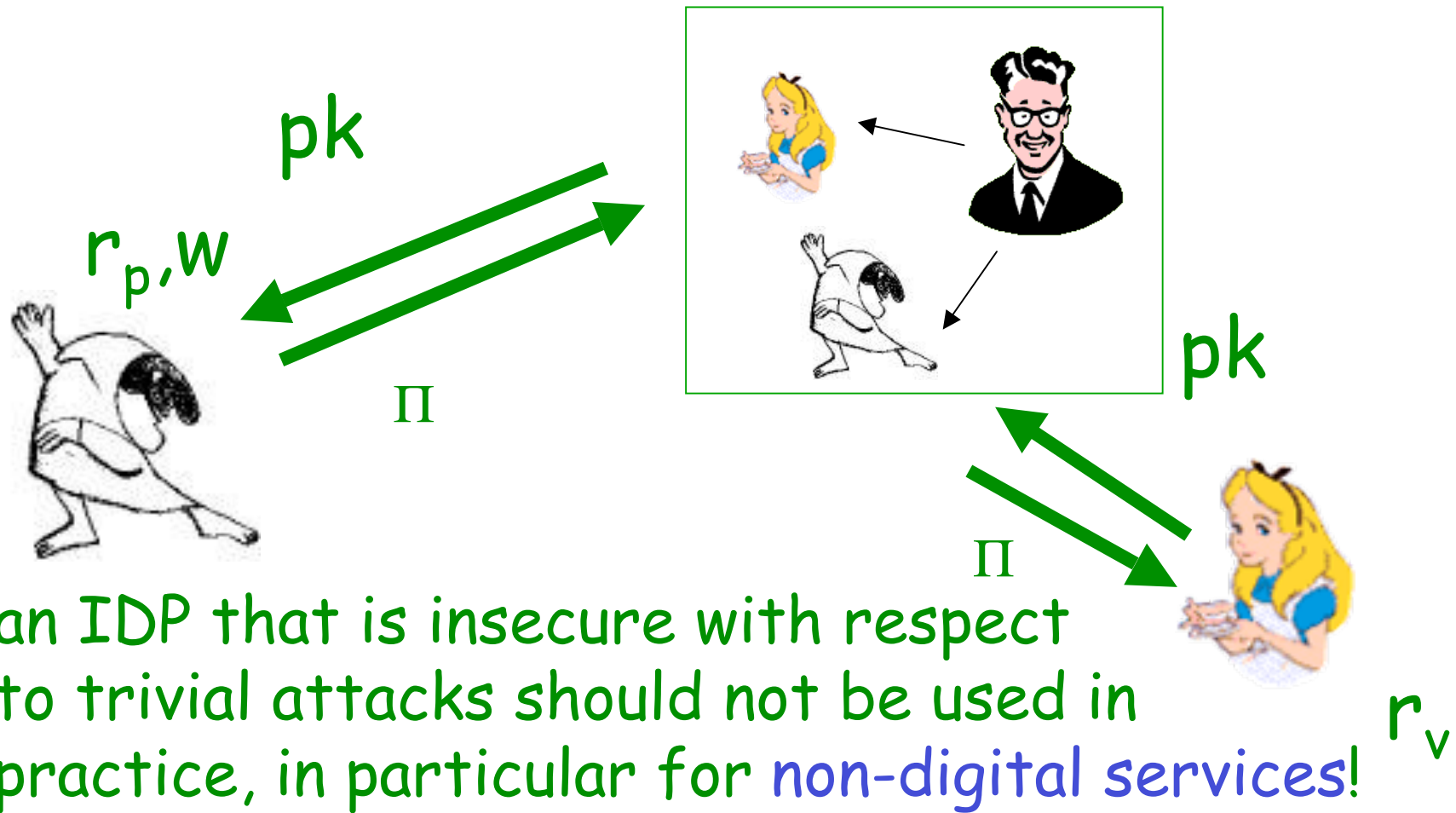
- MiM can simply work as proxy, forwarding all messages
- non-transferability is clearly impossible to achieve

On-Line MiM Kills any IDP

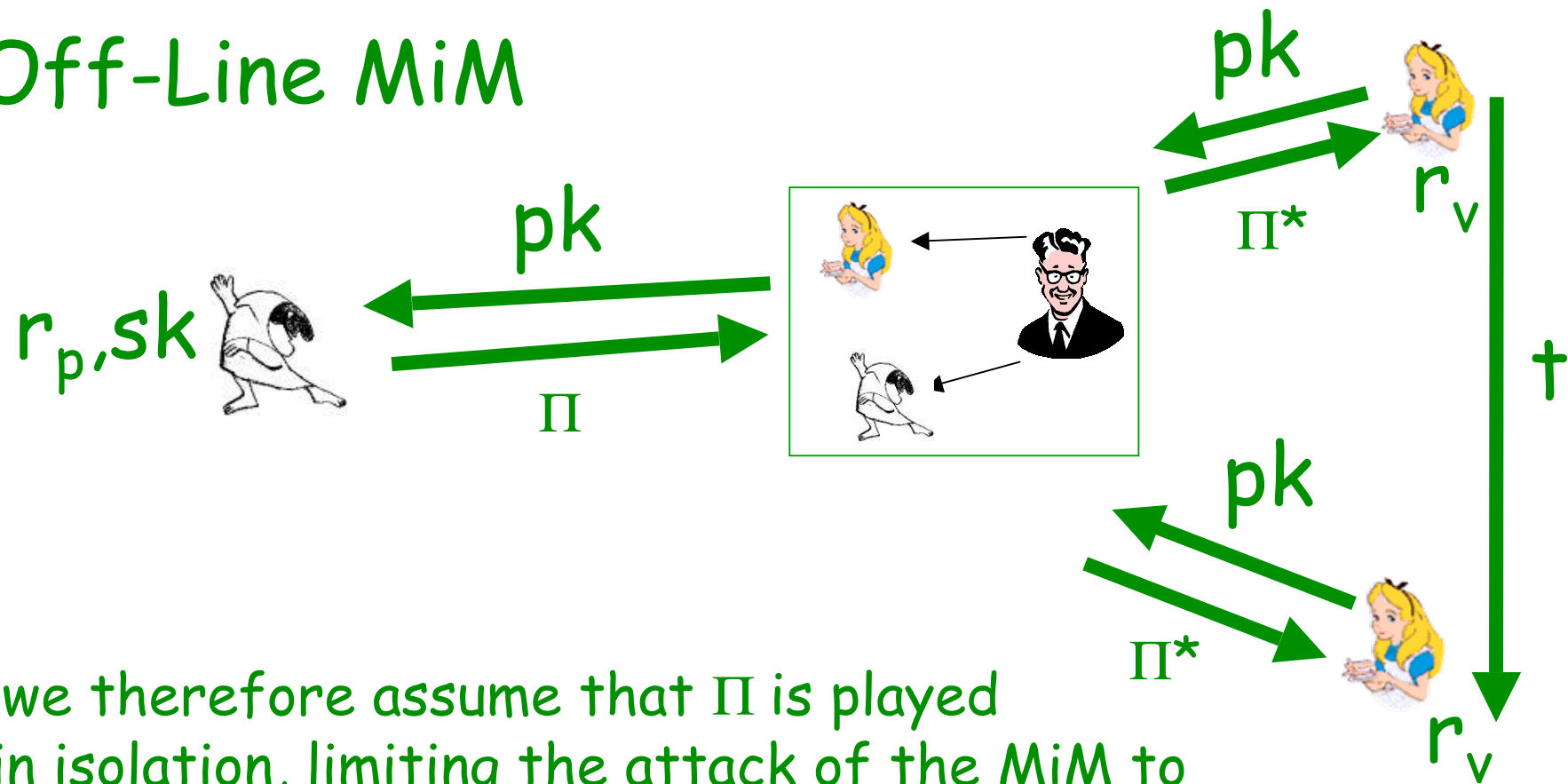


the literature focuses on security when the attack of the MiM is not the trivial one

On-Line MiM Kills any IDP



Off-Line MiM



- we therefore assume that Π is played in isolation, limiting the attack of the MiM to the off-line setting
- this is doable in practice by running Π in isolation
 - techniques as distance bounding can be used but area definitively deserves more research

Summing up

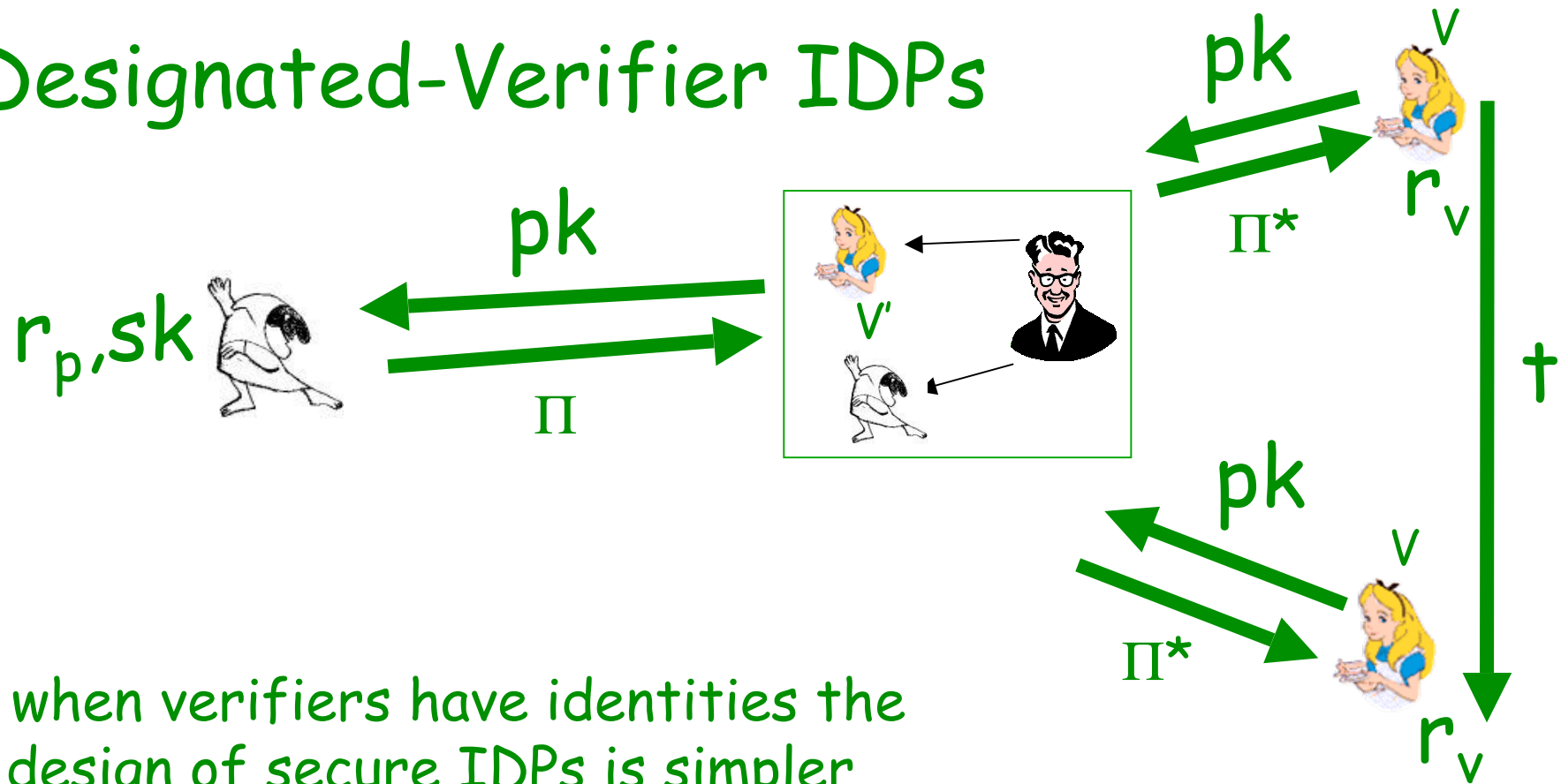
we are considering MiM attacks to IDPs
where:

- we want to avoid the transferability problem
- with $\Pi = \Pi^*$ we have self-security
- with $\Pi \leftrightarrow \Pi^*$ we have general-security
- we do not consider on-line MiM attacks
(impossibility...)
- in the off-line MiM attack Π is played in one shot

Outline

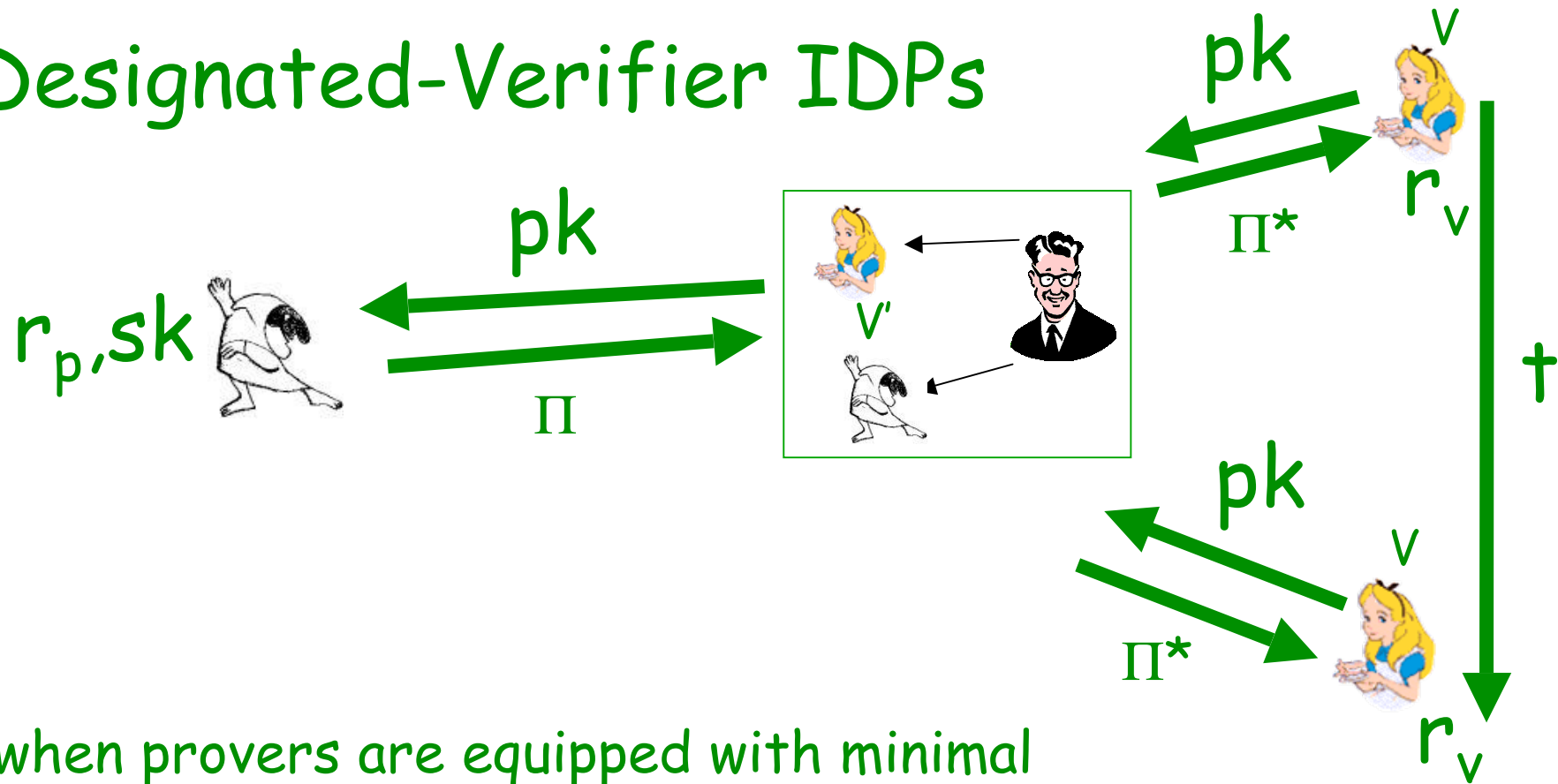
- Identification protocols
- MiM attacks
 - on-line vs off-line
 - Designated-verifier approach
- Reset attacks
- Transferability of some known proposals
- New Protocol
- Cheaper Identification

Designated-Verifier IDPs



- when verifiers have identities the design of secure IDPs is simpler
- it requires the management of a PKI for verifiers identities (revocations and enrolments)

Designated-Verifier IDPs



when provers are equipped with minimal resources (e.g., read-only permanent memory, no permanent network connection), the designated-verifier approach is not applicable

Outline

- Identification protocols
- MiM attacks
 - on-line vs off-line
 - Designated-verifier approach
- **Reset attacks**
- Transferability of some known proposals
- New Protocol
- Cheaper Identification

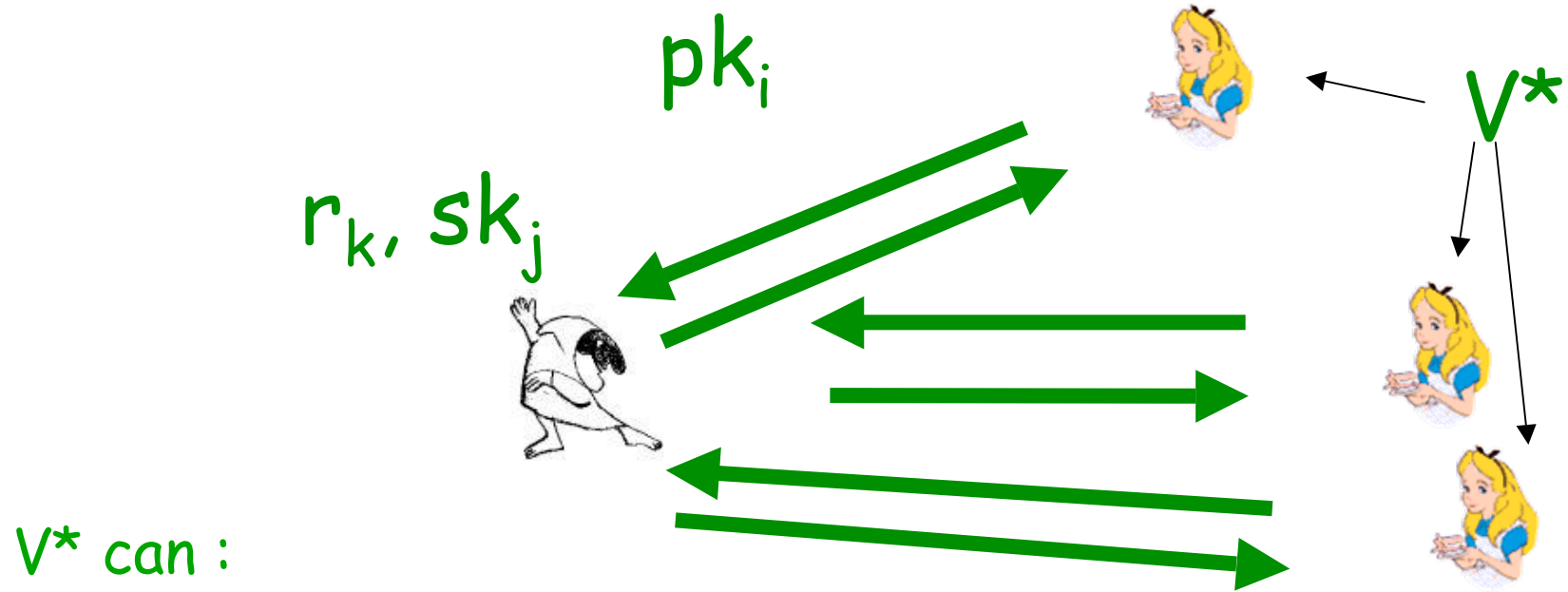
Reset Attacks

- there exist devices that when disconnected from their batteries go back to their initial state

[CGGM00]



- IDPs should consider these attacks to, hopefully preserving their efficiency

Reset Attacks



V^* can :

- reset the prover to a previous state (incarnation)
- concurrently interact with the incarnations of P

V^*   $P_{(i,k)} = P(pk_i, sk_i, r_k)$

Summing up

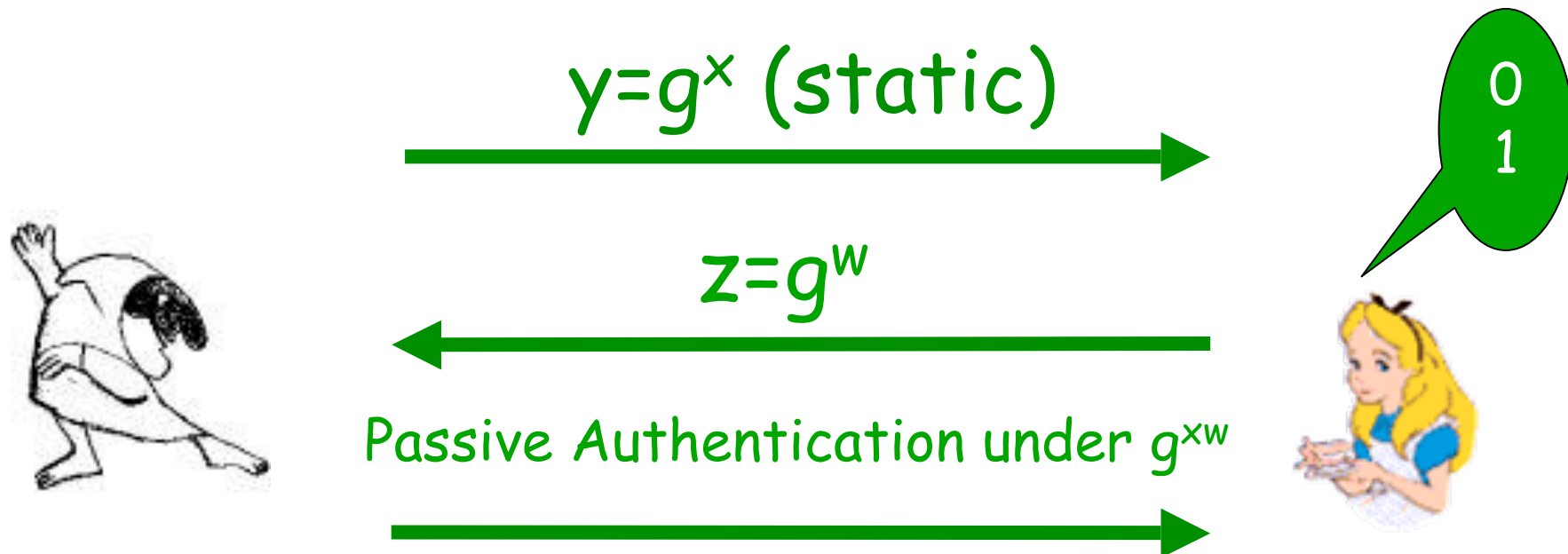
we are considering MiM attacks to IDPs
where:

- we want to avoid the transferability problem
- with $\Pi = \Pi^*$ we have self-security
- with $\Pi \leftrightarrow \Pi^*$ we have general-security
- we do not consider on-line MiM attacks
(impossibility...)
- in the off-line MiM attack Π is played in one shot
- we do not want identities for verifier
- we care about resettably-secure IDPs

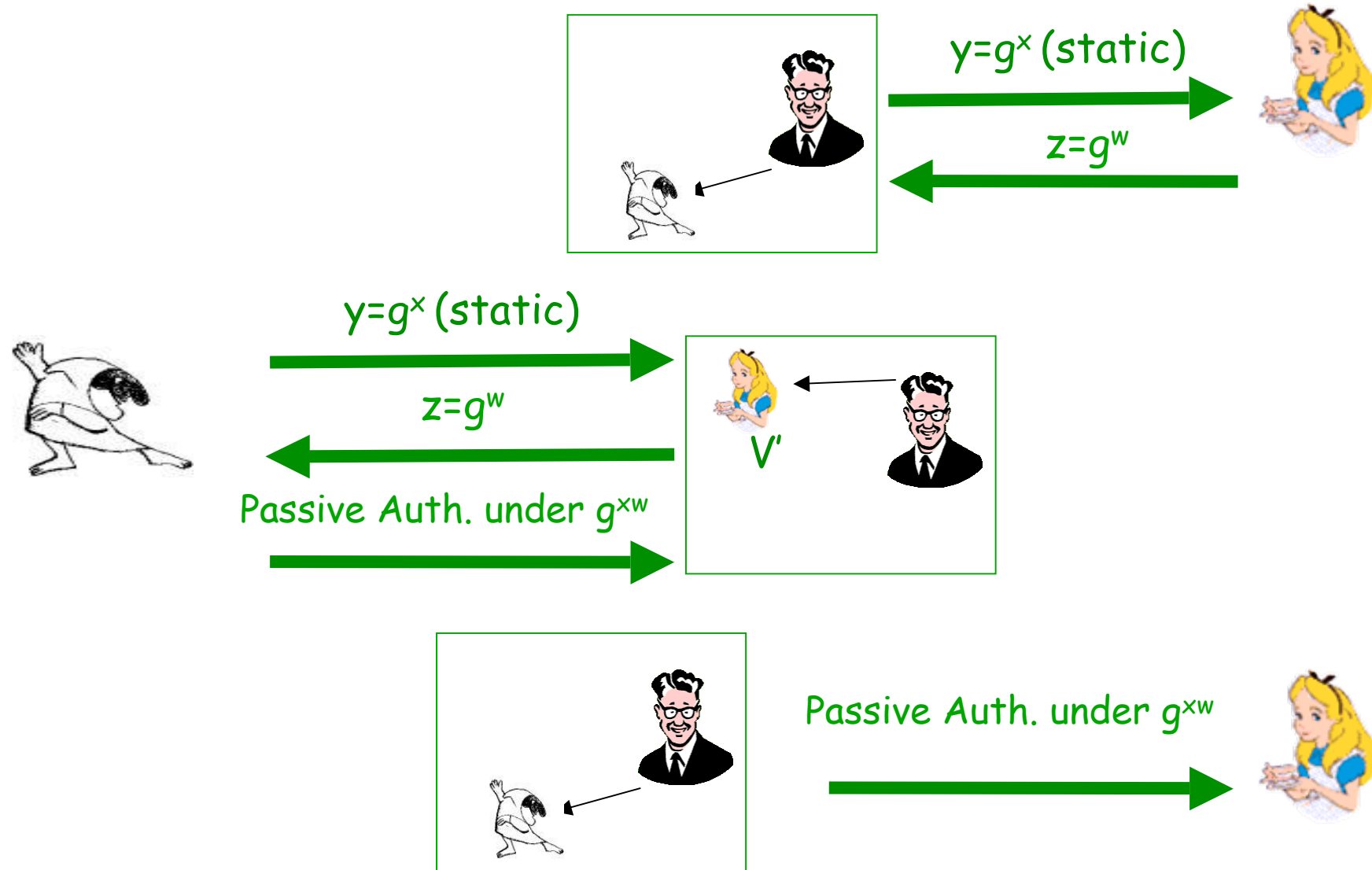
Outline

- Identification protocols
- MiM attacks
 - on-line vs off-line
 - Designated-verifier approach
- Reset attacks
- Transferability of some known proposals
- New Protocol
- Cheaper Identification

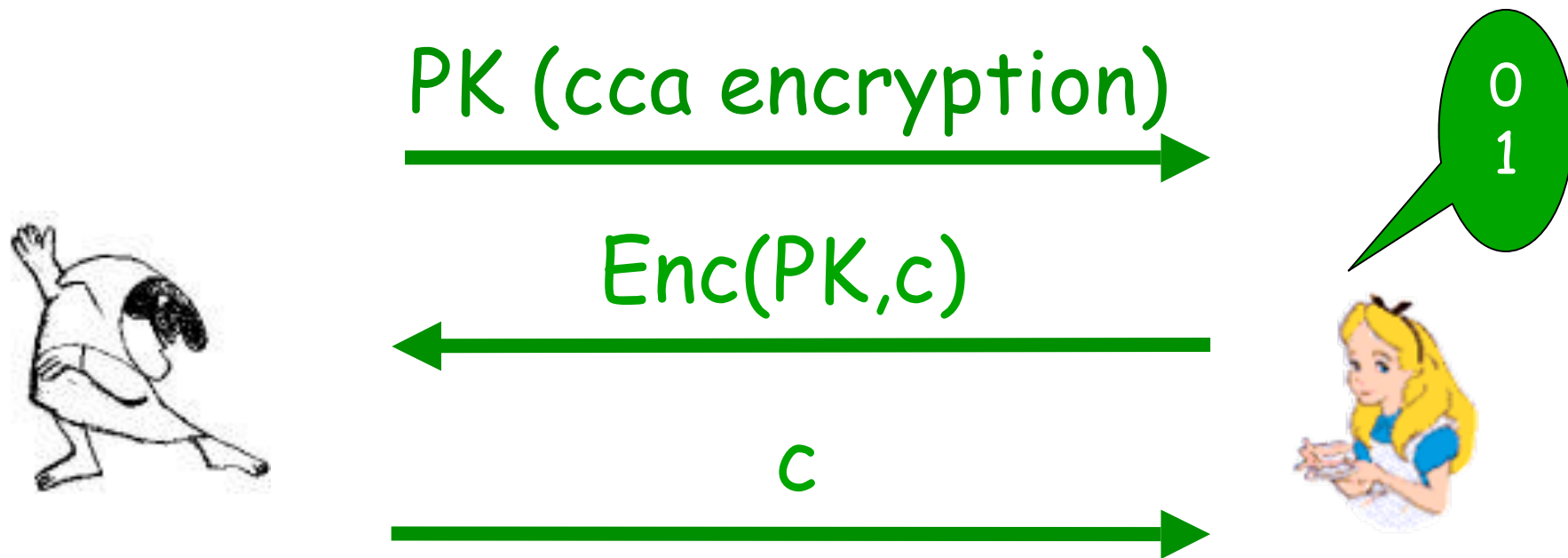
BSI Chip Authentication for E-Passports



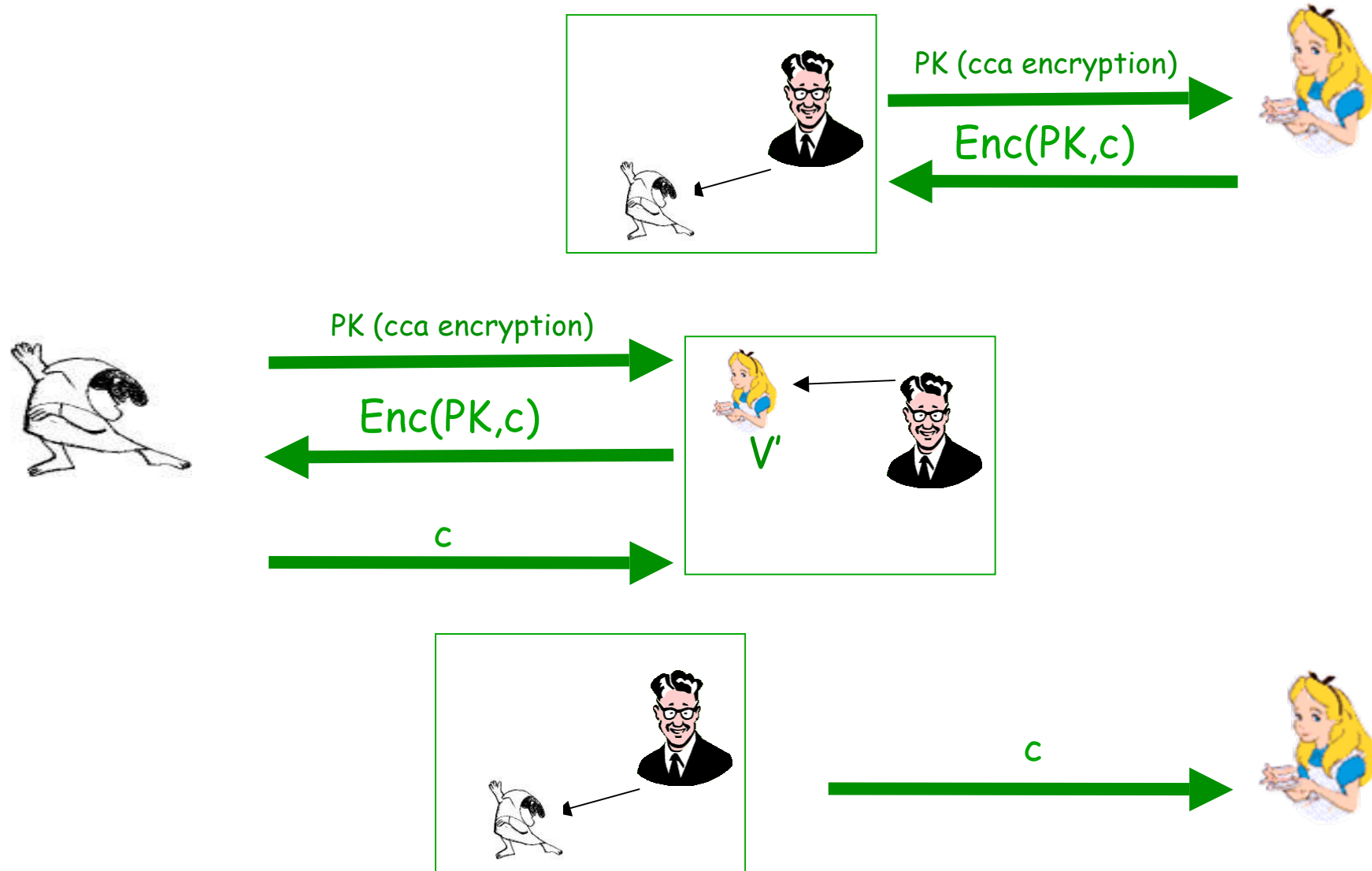
BSI Chip Authentication for E-Passports



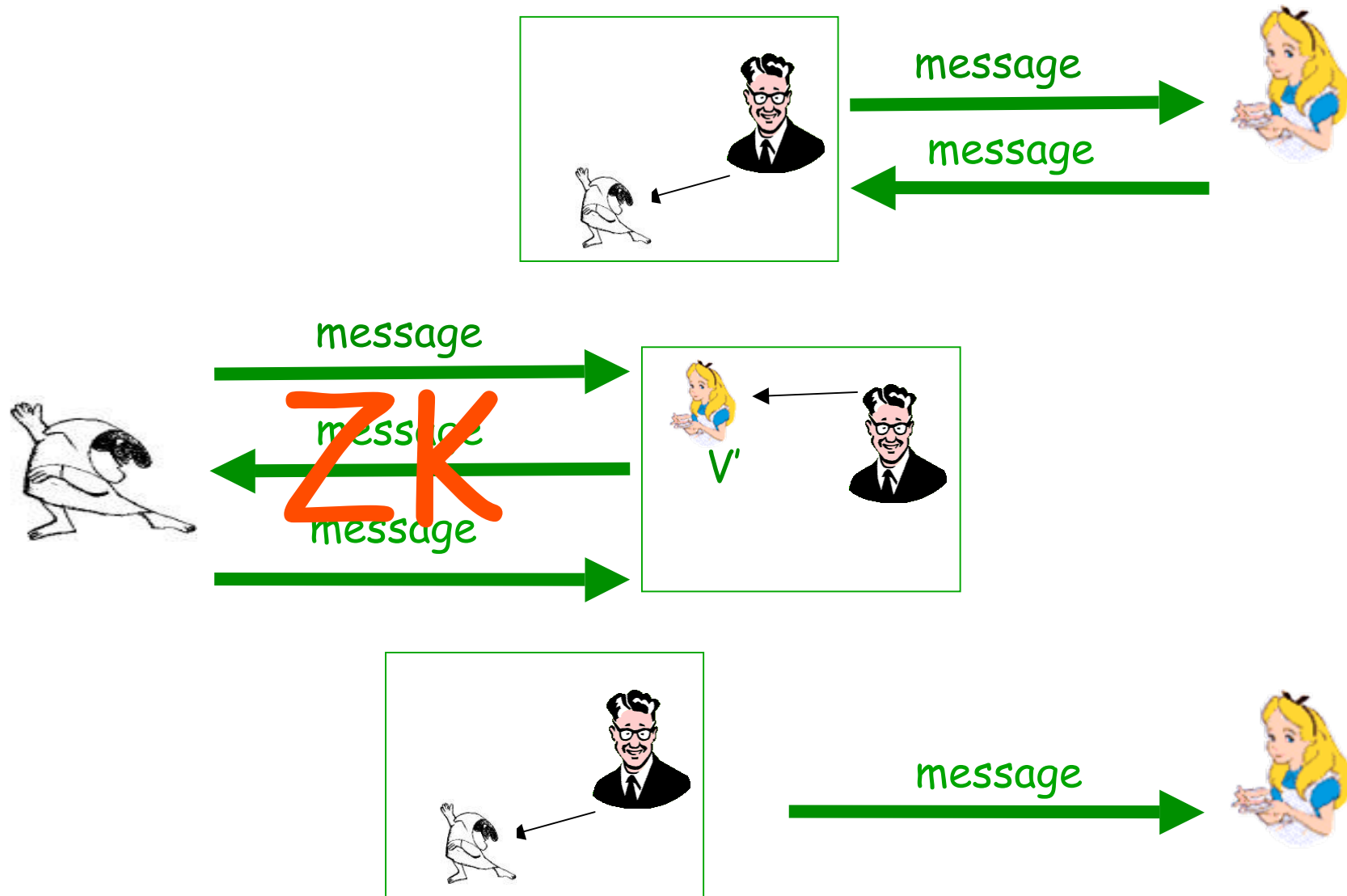
[BFGM01] Resetably-Secure Identification



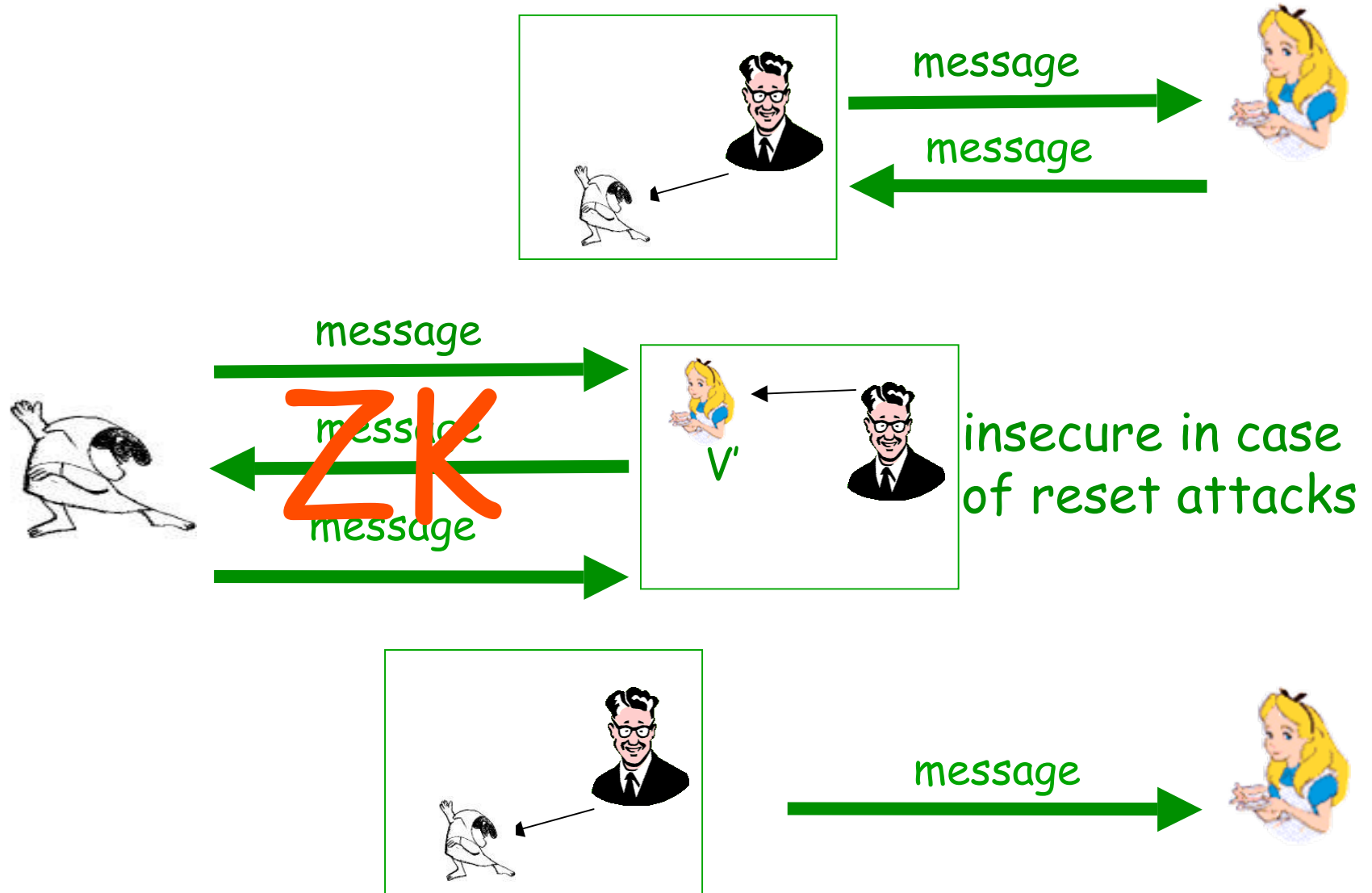
[BFGM01] Resettable-Secure Identification



[MVV] ZK Identification



[MVV] ZK Identification



Outline

- Identification protocols
- MiM attacks
 - on-line vs off-line
 - Designated-verifier approach
- Reset attacks
- Transferability of some known proposals
- **New Protocol**
- Cheaper Identification

Commitment Schemes



Properties:

- Binding: after giving the safe to Alice, Bob cannot alter the message m written inside
- Hiding: Alice cannot determine m until she learns the code
- Trapdooriness: a simulator computes a *simulated* safe that can be later opened as both m and $m' \langle \rangle m$

Schnorr's PoK of a Discrete Logarithm

$$p=2q+1, g, |\langle g \rangle|=q, y=g^x$$



$$a=g^s \text{ mod } p$$

$$c$$

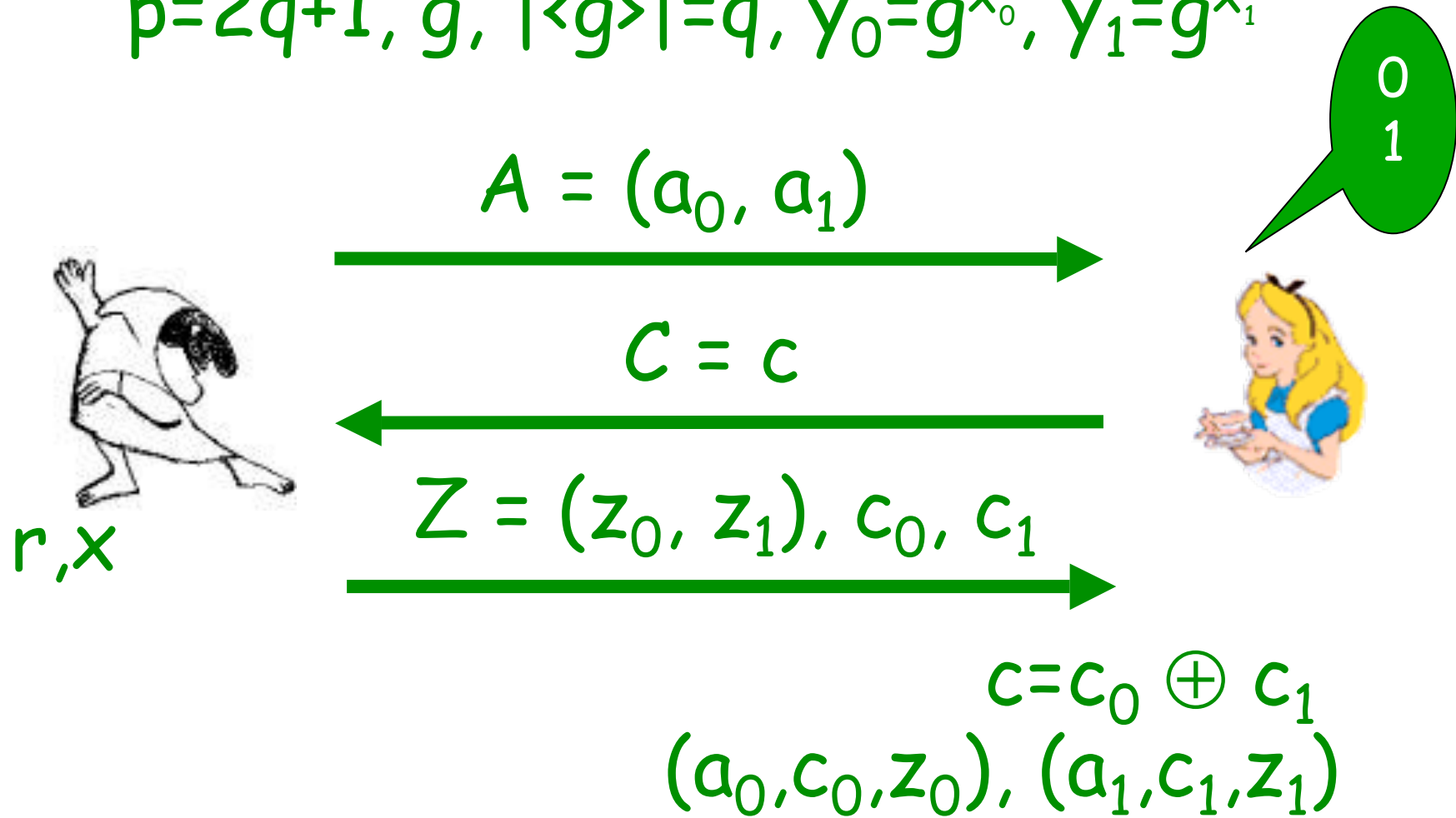
$$z=s+cx \text{ mod } q$$



$$g^s = ? = ay^c \text{ mod } p$$

Schnorr's PoK of a DL OR another DL

$$p=2q+1, g, |\langle g \rangle|=q, y_0=g^{x_0}, y_1=g^{x_1}$$



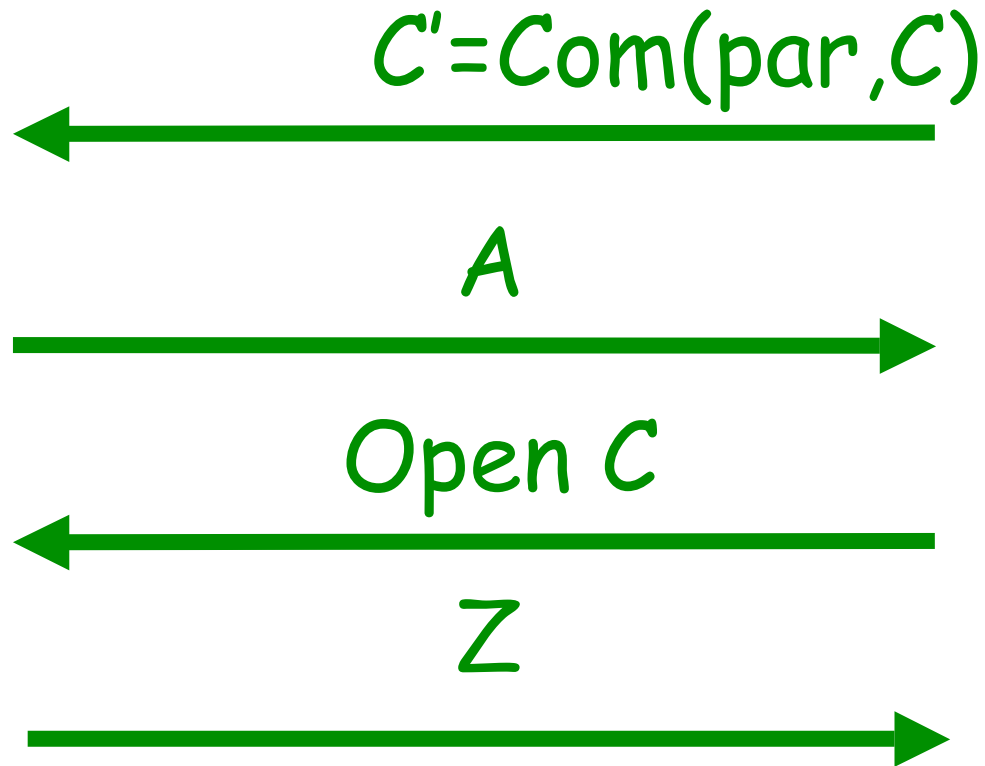
rNT Chip Authentication

$y = g^x$
par
$y' = g^{x'}$

compute $r = f(s, C')$
and use r
as randomness

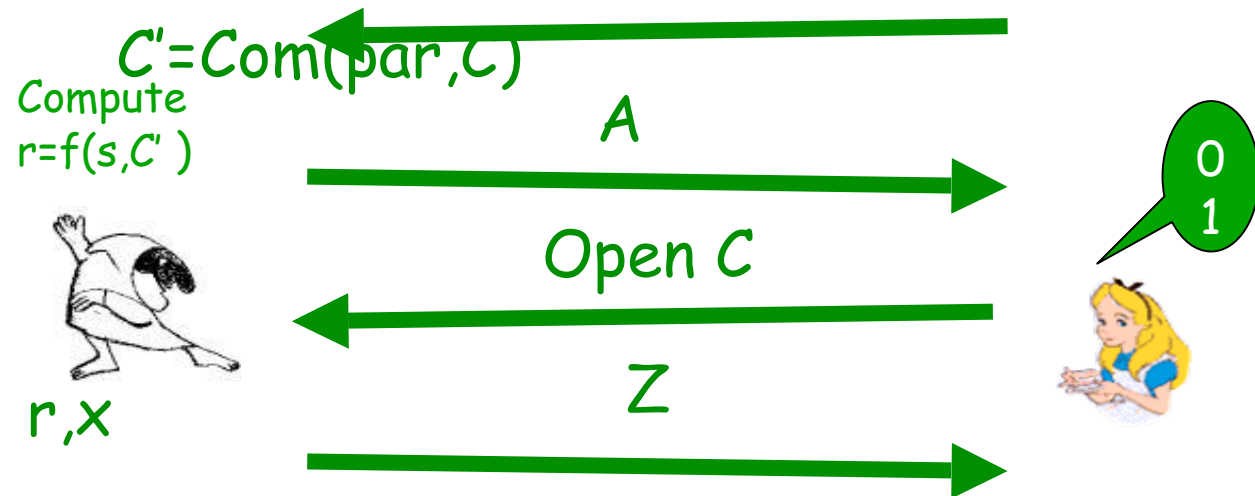


r, x



Analysis

$y = g^x$
par
$y' = g^{x'}$



Properties:

- Efficiency: 3 times slower than BSI chip authentication
- Transferability: we can prove that a successful MiM can be used to break the DLOG assumption
- Resettability: the protocol follows the [CGGM00] paradigm and is actually rZK (though rWI would suffice)

Outline

- Identification protocols
- MiM attacks
 - on-line vs off-line
 - Designated-verifier approach
- Reset attacks
- Transferability of some known proposals
- New Protocol
- Cheaper Identification

Suggestions

- Chip producers should certify the resilience of the chip with respect to reset attacks
 - good practice: plug in a tamper proof area a randomly chosen seed and a circuit for evaluating a pseudorandom function
- Protocol designers should consider the certified non-resettability
 - good practice: use [CGGM00] paradigm (when possible)

Cheaper Identification

- Applications of RFID as transport tickets require much cheaper tags (no public-key crypto)
 - Use private-key crypto
- User privacy is a main issue
 - Use rerandomizable encryption (but prevent DoS attacks)
- Ticket unclonability is fundamental as well
 - Use PUFs

Wait...

rerandomizable public-key encryption ??

no DoS ?

PUFs and privacy ??

Cheaper Identification

- Store on a tag
 - $K=f(s,t)$ where
 - s is a secret seed known to the tag producer
 - f is a pseudorandom function
 - t is the value of the PUF
 - a (public-key rerandomizable) encryption c of t
- The reader decrypts c thus obtaining t , then computes $f(s,t)$ thus obtaining K ,
- the reader and tag can now continue with symmetric key crypto
- Use an optical PUF for punishment and DoS!

Conclusion

- More gadgets, more fun... in theory
(more bugs in practice)
- Theory and Practice should talk to each other
before getting married
- Questions ?