Michael Backes
Saarland University, Germany
joint work with Birgit Pfitzmann and Michael Waidner

Secure Reactive Systems, Day 5:

Preservation Theorems for Dolev-Yao Models and Limits of Soundness

Tartu, 03/01/06

Recall the RS Framework

- Precise system model allowing cryptographic and abstract operations
- Reactive simulatability with composition theorem
- Preservation theorems for security properties
- Concrete pairs of idealizations and secure realizations
- Sound symbolic abstractions (Dolev-Yao models) that are suitable for tool support
- Sound security proofs of security protocols: NSL, Otway-Rees, iKP, etc.
- Detailed Proofs (Poly-time, cryptographic bisimulations with static information flow analysis, …)

Recall the RS Framework

- Precise system model allowing cryptographic and abstract operations
- Reactive simulatability with composition theorem
- **Preservation theorems for security properties**
- Concrete pairs of idealizations and secure realizations
- Sound symbolic abstractions (Dolev-Yao models) that are suitable for tool support
- **Sound security proofs of security protocols: NSL, Otway-Rees, iKP, etc.**
- Detailed Proofs (Poly-time, cryptographic bisimulations with static information flow analysis, …)
- **Limitations, …**

Proving the Needham-Schroeder-Lowe Protocol with the BPW Model

The NS Public-Key Protocol

- **Authentication protocol**

  $u \rightarrow v: E_{pk\_v}(N_u, u)$

  $v \rightarrow u: E_{pk\_u}(N_u, N_v)$

  $u \rightarrow v: E_{pk\_v}(N_v)$

- **Afterwards successfully terminating the protocol, v knows that u wanted to communicate with v.**

  Wrong!

The NSL Public-Key Protocol

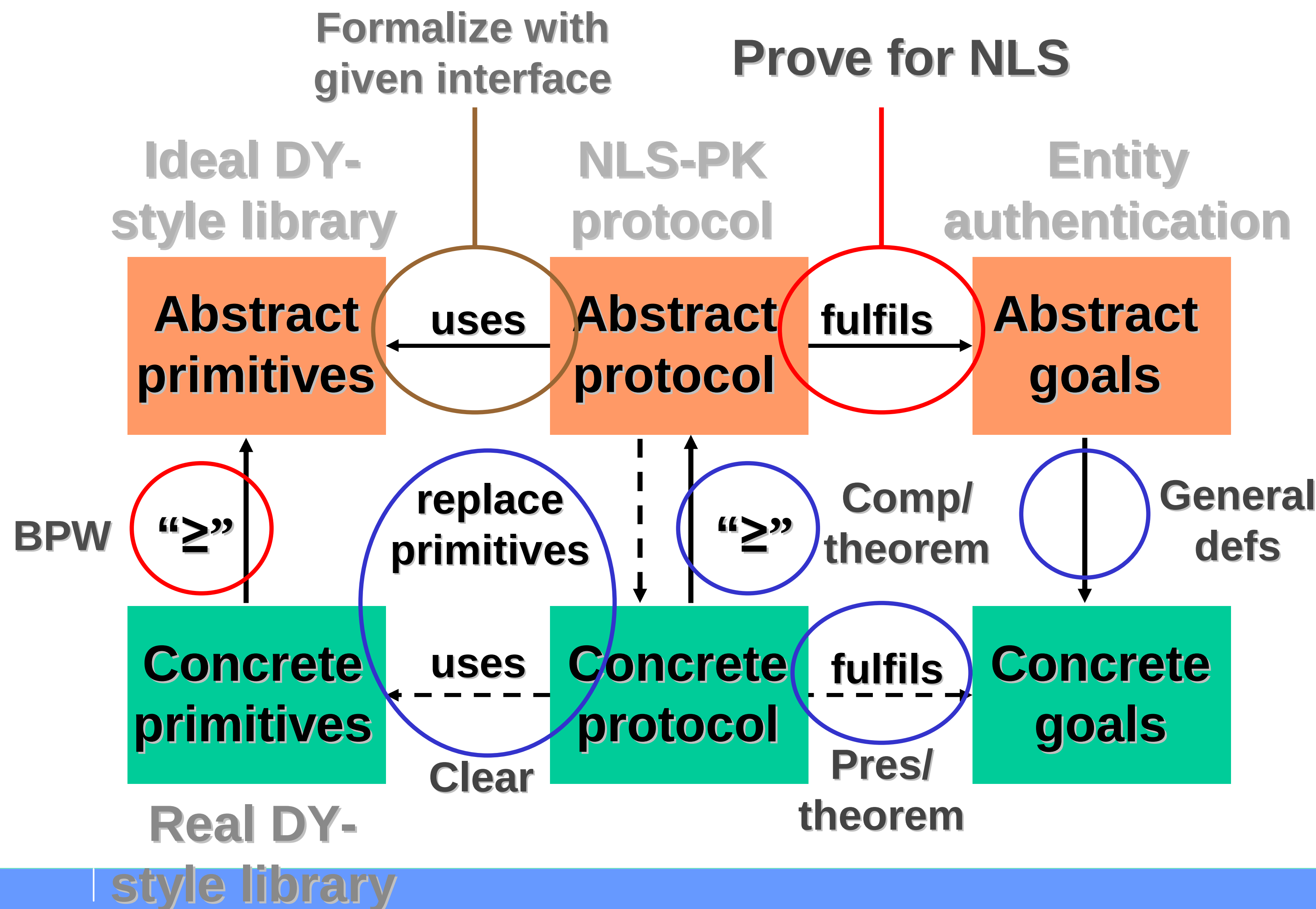
- **Originally Needham and Schroeder 78**
- **Modified by Lowe 95 after MITM attack**

  $u \rightarrow v: E_{pk\_v}(N_u, u)$

  $v \rightarrow u: E_{pk\_u}(N_u, N_v, v)$

  $u \rightarrow v: E_{pk\_v}(N_v)$
- **Multiple proofs over Dolev-Yao (Lowe, Meadows, Syverson, Schneider, …)**
- **No prior cryptographic proof; concurrently by Warinschi (directly cryptographic)**
- **All formal methods (and crypto) need refined protocol definition; sometimes automated**

Recall: Sound Abstract Protocol Proofs



Recall: Dolev-Yao Model

- Idea [DY81]
  - Abstraction as term algebras, e.g., $D_x(E_x(E_x(m)))$
  - Cancellation rules, e.g., $D_x E_x = \varepsilon$
- Well-developed proof theories
  - Abstract data types
  - Equational 1st-order logic
- Important for security proofs:
  - Inequalities! (Everything that cannot be derived.)
  - Known as “initial model”

Important goal: Justify or replace

Recall: BPW Model

U

V

$T_{u,4} \leftarrow$ encrypt($T_{u,1}$, $T_{u,3}$)
send(V, $T_{u,4}$)

received(U, $T_{v,2}$)

get_type($T_{v,2}$)
$T_{v,3}$:= decrypt(...)

	Term 1	Term 2	Term 3	Term 4
For U:	$T_{u,1}$	$T_{u,2}$	$T_{u,3}$	...
For V:	-	$T_{v,1}$	-	
For A:	-	$T_{a,1}$	-	

Term 1: pk

Term 2: E (pk, m)

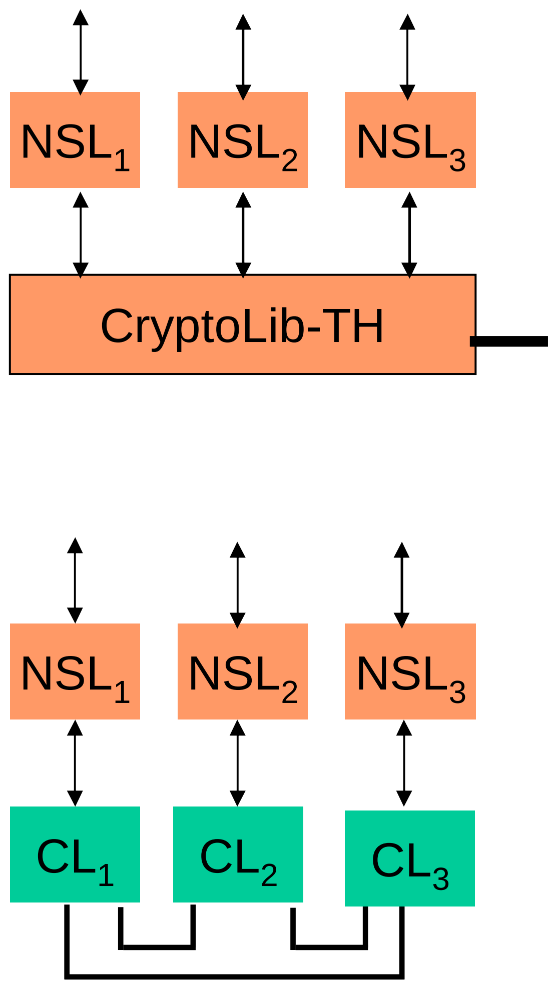
Term 3: E (pk, m)

Term 4: E (pk, E (pk, m))

TH

A

The NSL Protocol over BPW Model



Refining u → v: $E_{pk\_v}(N_u, u)$

For NLS_u:

1. $n_u^{hnd} \leftarrow$ gen_nonce();
2. $Nonce_{u,v} := Nonce_{u,v} \cup \{n_u^{hnd}\}$;
3. $u^{hnd} \leftarrow$ store(u);
4. $l^{hnd} \leftarrow$ list(n_u^{hnd}, u^{hnd});
5. $c^{hnd} \leftarrow$ encrypt($pke_{u,v}^{hnd}$, l^{hnd});
6. send_i(v, c^{hnd})

Informal Entity Authentication Property

- **“When v thinks it speaks with u, then it does.”**
- **“When v successfully terminates a session thinking to speak with u, then u indeed started a session with v.”**

Remarks:

  - **Entity authentication is weak: no session key, no time.**
  - **Mutual authentication and replay prevention possible.**

Entity Authentication in Our Model

- **Important for preservation theorem: Property expressed as user in-/outputs**
- **Here**
  - **"successful termination" as output for *v***
  - **"protocol start" as input from *u***

$$\exists t_1\text{: EA\_out}_v\text{!(ok, } u\text{)}$$

$$\Rightarrow \exists t_0 < t_1\text{: EA\_in}_u\text{?(new\_prot, } v\text{)}$$

Recall: Property Preservation

Preservation theorems over „≥ " for

- Integrity **properties**
- **Some confidentiality properties:**
  - Non-interference
  - Intransitive non-interference
  - Strong key and message secrecy (later)
- **„Polynomial** liveness**"**

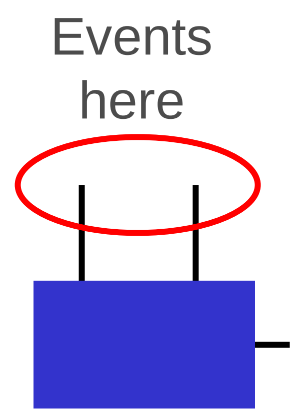
Authenticity is one of these

Recall: Integrity Preservation Theorem

- Integrity property: **Set of permitted traces at ports to the users**
  - **E.g., semantics of temporal logic**
- Cryptographic semantics
  - **Perfect / statistical / computational fulfillment**
  - **Poly: $\forall A \in PPT$: $P(run\lceil_{\text{ports to the user}} \notin I) \in NEGL$**
- Preservation Theorem:

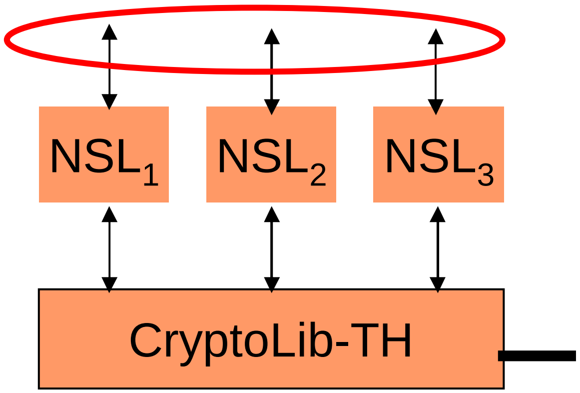
$(Sys_{real} \geq Sys_{ideal}) \wedge (Sys_{ideal}$ fulfills I)

$\wedge$ I poly testable $\Rightarrow$ (Sys_{real} fulfills I)



Proving that NSL Fulfills Entity Authentication

EA definition



Idea:

v terminates protocol with u

$\Rightarrow$ u sent 3rd message

$\Rightarrow$ u obtained 2nd message

$\Rightarrow$ v sent 2nd message

...

Proof via invariants.

E.g., nonce secrecy:

- ***Informal:*** **Honest *u* created N_u for honest *v***
  $\Rightarrow$ N_u only known to u and v
- ***Formal:***
  $D[\,j\,].\mathrm{hnd}_u \in Nonce_{u,v} \Rightarrow (D[\,j\,].\mathrm{hnd}_w = \downarrow \text{ for all } w \notin \{u,v\})$

The Other Invariants

- **Correct nonce owner ($Nonce_{u,v} \leftrightarrow$ handles)**
- **Unique nonce use**
- **Nonce list secrecy (List with N_u has handles for *u*, *v* only)**
- **Correct list creator (for the 3 protocol messages)**

1. u → v: $E_{pk\_v}(N_u,u)$
2. v → u: $E_{pk\_u}(N_u, N_v,v)$
3. u → v: $E_{pk\_v}(N_v)$

  - ***Msg 1:***

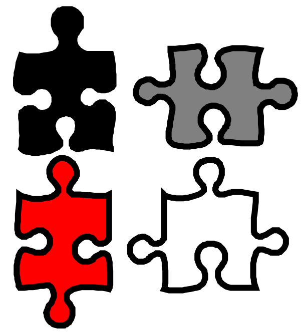
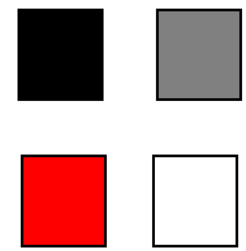
    If D[*j*].type = list:

    Let $x_i := D[\,j\,].arg[\,i\,]$ and $x_i^{hnd} := D[\,x_i\,].hnd_u$:

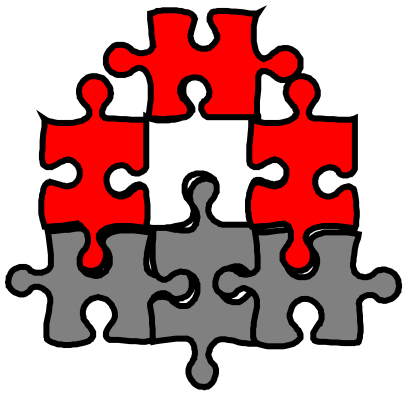
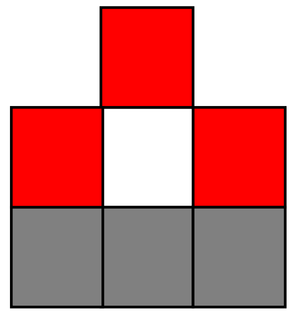
    If $x_1^{hnd} \in Nonce_{u,v}$ and $D[\,x_2\,]$.type = data then D[*j*] was created by user *u* in Step 4.

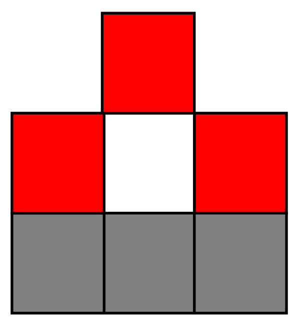
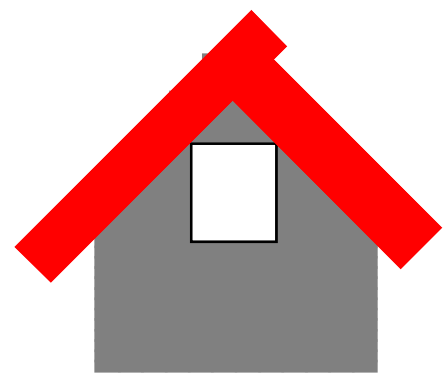
Relating Symbolic and Cryptographic Secrecy

Recall Prior Result

- “as secure as” (reactive simulatability)
- for certain versions of  and 

Specification Styles

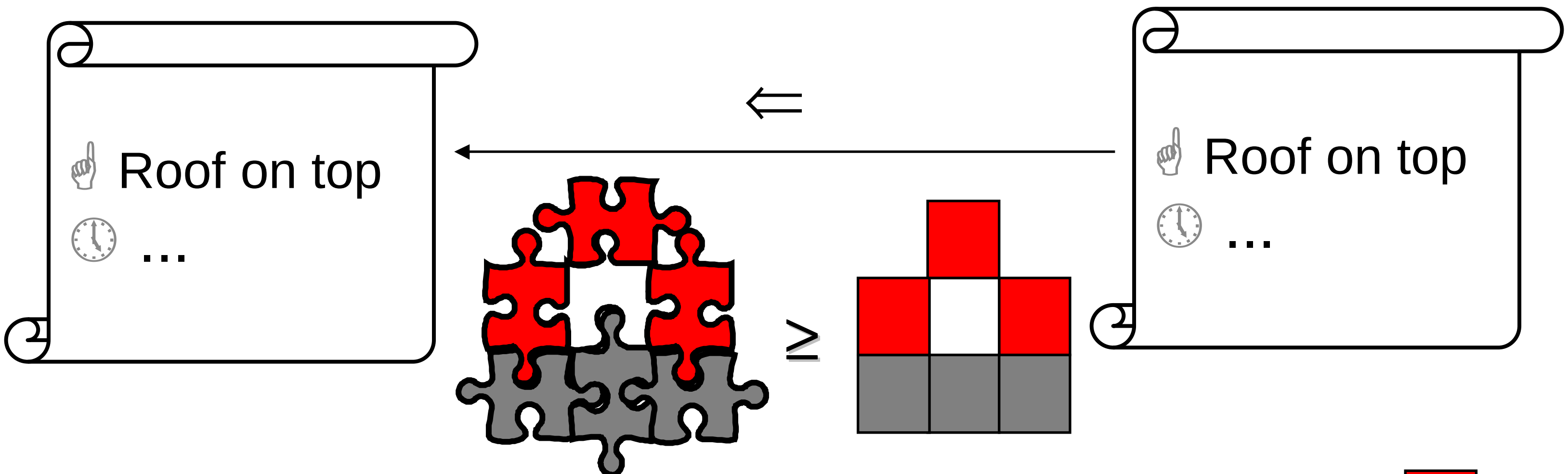
- Is  ≥  what people want?
- Often yes, in particular together with

 ≥ 

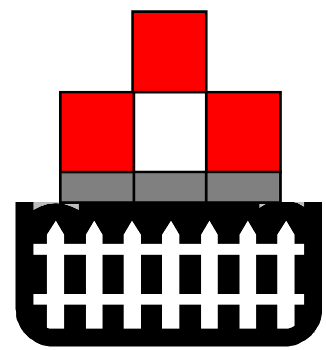
  - E.g., secure channels (see also spi calculus), certified mail
- But not always ...

Alternative: Property-based spec.

- **E.g., "I want a tight roof on top": integrity**
  - **Preserved by "≥":**

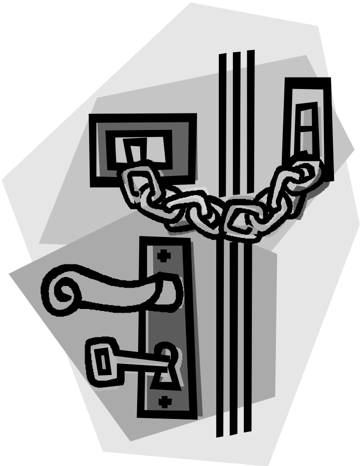


- **Also preserved:**
  - **Non-interference (info-flow secrecy, strong)**
  - **Liveness (poly ...)**

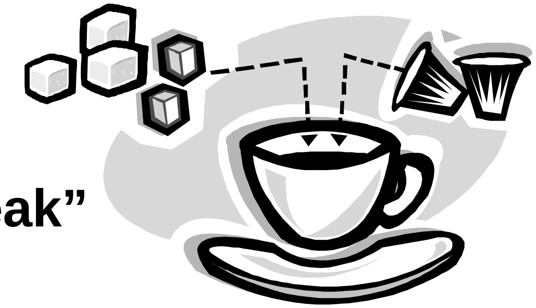


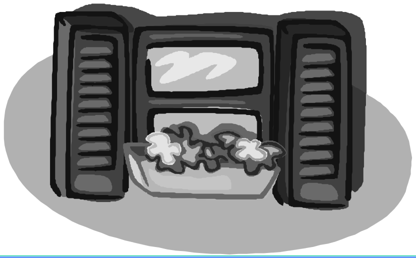
Secrecy of Individual Things or Actions

- “Keep my burglar alarms secret”
  - System-related secret
  - Pretty much doable by designer alone
  - Only simple rules for user



- “People shouldn’t see what I eat”
  - Secret of the user
  - Can’t be done by designer alone
  - Distinguish “user leak” from “system leak”





Key Secrecy

- **Standard symbolic definition: *k* does not get into A's knowledge set**
- **Standard cryptographic definition: *k* indistinguishable from random *r* given A's view**
- **We essentially show**

  k symb secret $\Rightarrow$ k crypt secret

- **One main exception: k must be**

  "symbolically unused":

  $\Leftrightarrow$ no term E(*k*, *m*) resp. MAC(*k*, *m*) in A's knowledge set

  (i.e., no such term has been constructed in the DY-model by any protocol).

Why Is "Symbolically Unused" Needed?

- **Example KX protocol:**

Sig(E(..., k)) →

... ←

(Confirm) MAC(k, 11111) →

- **Main protocol money transfer:**

... →

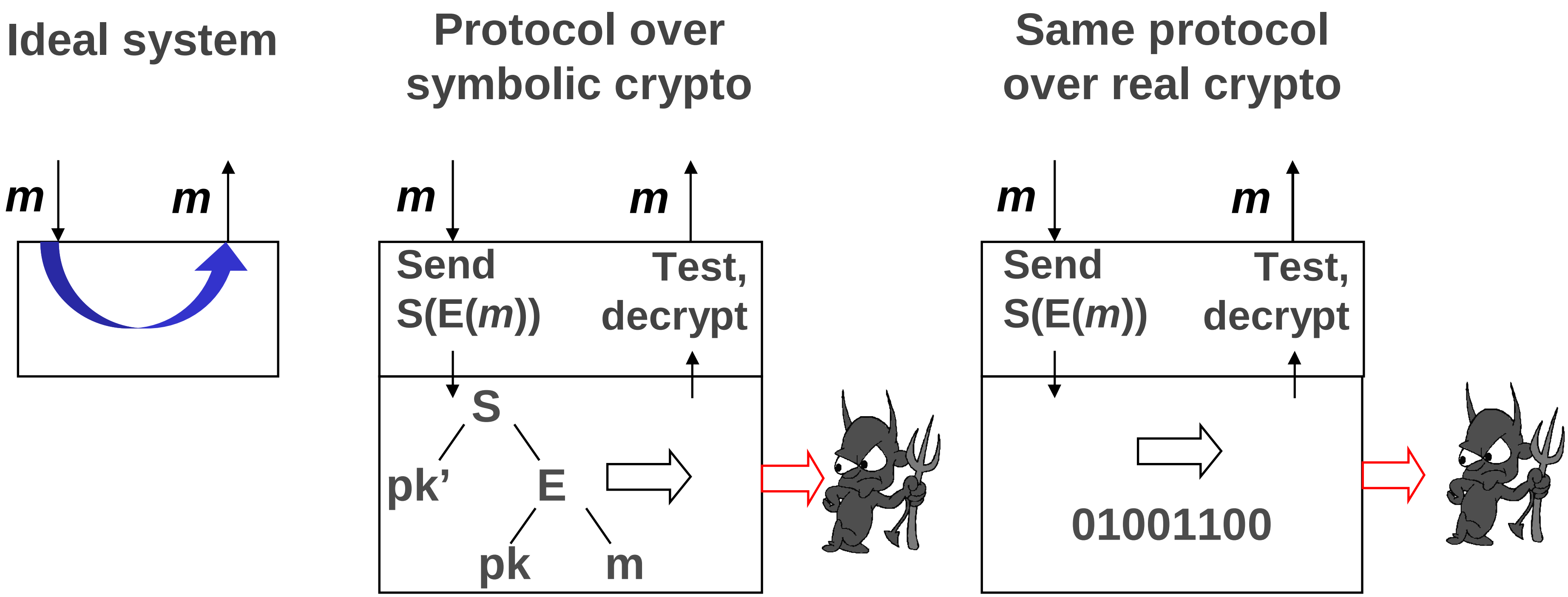
$ to transfer? ←

MAC(k, 1~~0)~~1111) →

- **Cryptographic definition was designed for arbitrary sequential composition and really needs this.**

Payload Secrecy – Definition Problems

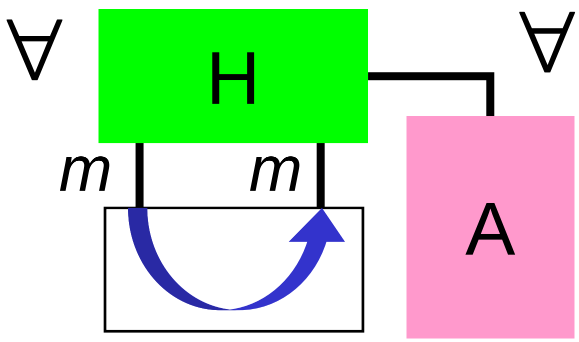
- **E.g., secure channel**



- **Is *m* secret? According to what definition?**
- **Should be true at least for this ideal system**

Is *m* Secret for Ideal Secure Channel?

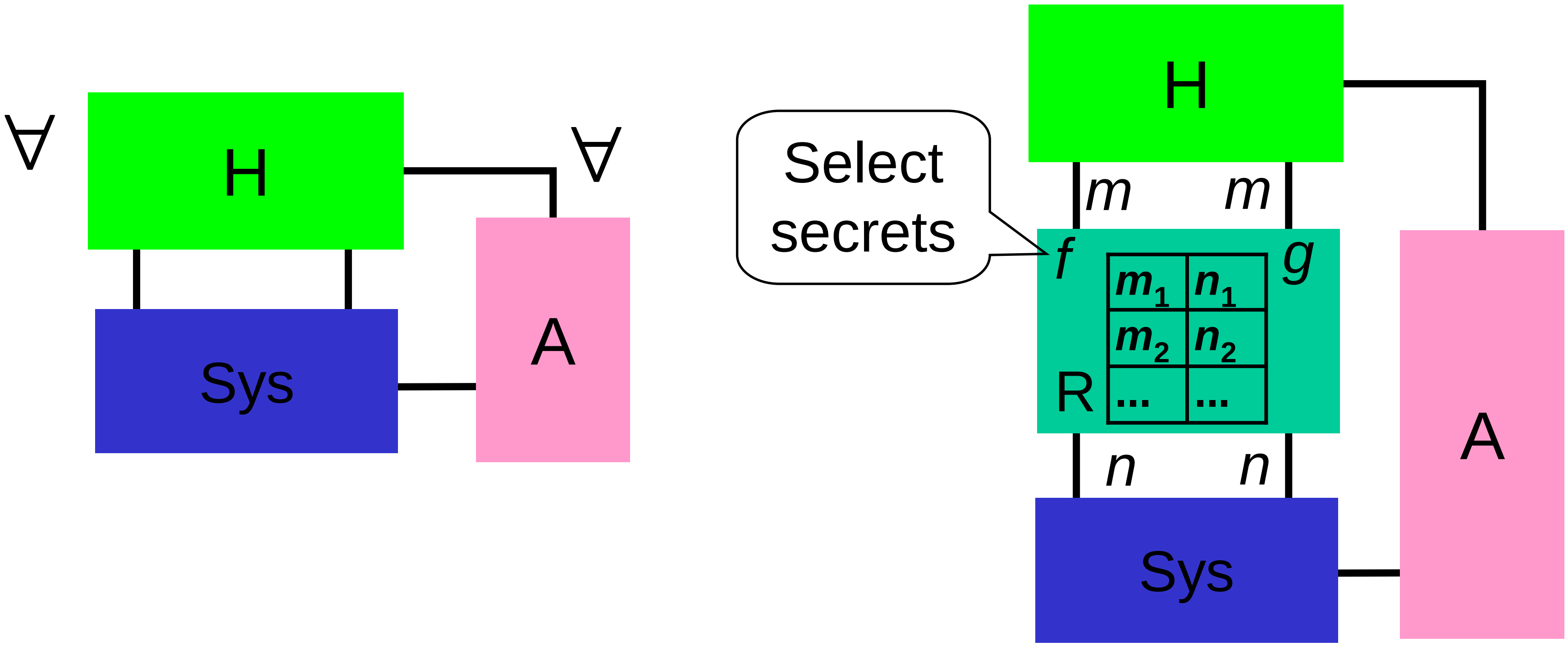
- **Not with the following strict definition (due to partial info and active attacks)**



m indistinguishable from random *r*

- **Main related cryptographic definition: For encryption:**
  - **Specific message-chooser**
  - **Specific condition that one ciphertext *c* is not decrypted.**
- **Other such specific def's exist, but no general one.**

Replacement Machine as Generalization



$$\text{view}_{\text{normal}}(\text{H}) \approx \text{view}_{\text{withR}}(\text{H})$$

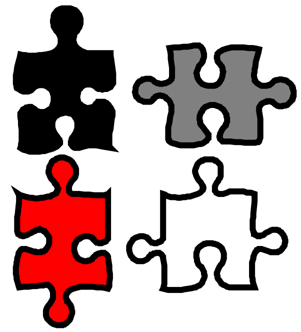
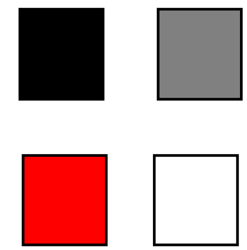
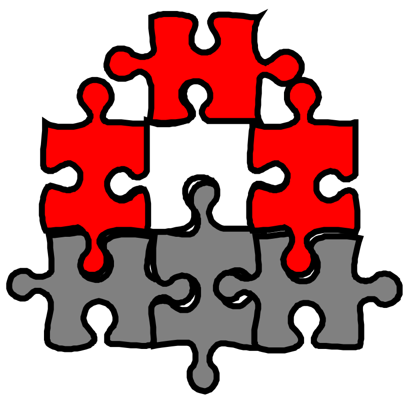
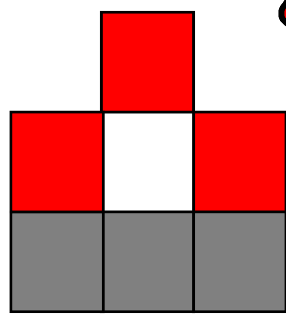
Idea: If system leak, A and thus H would notice that *n* used instead of *m*

Results on Payload Secrecy

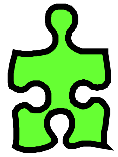
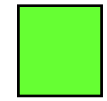
- Preservation **theorem for this cryptographic payload secrecy over “≥”.**
- Symbolic **payload secrecy**
  $\wedge$ **benign info flow of payload**
  $\Rightarrow$ cryptographic **payload secrecy**

Impossibility Results: Unsoundness of Symbolic XOR and Symbolic Hash functions

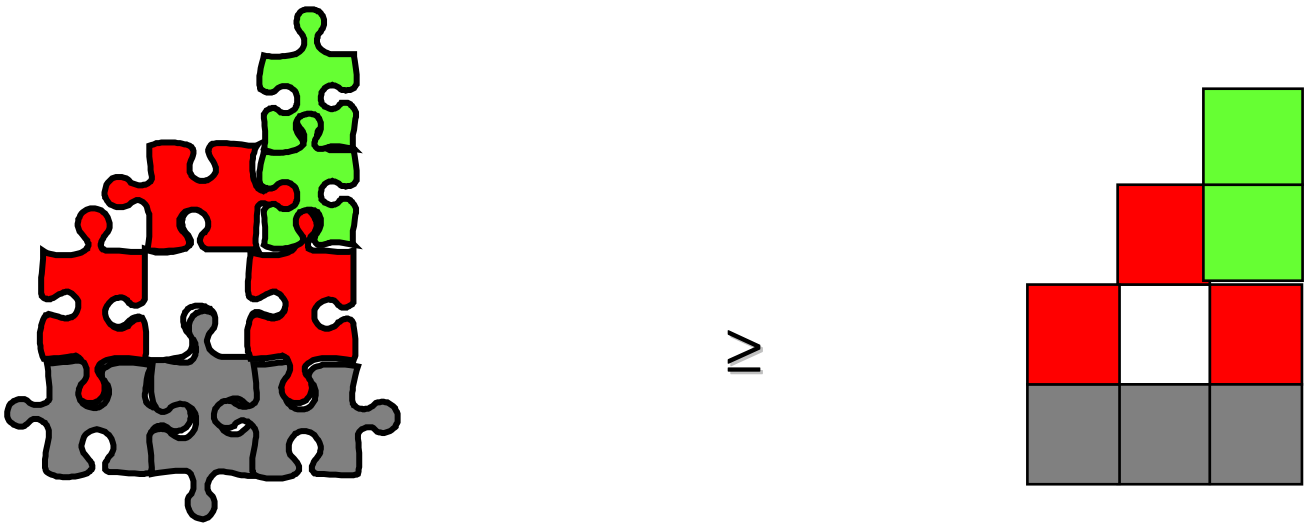
Recall Prior Result

- **“as secure as” (reactive simulatability)**
- **for certain versions of**  **and** 
-  ≥ 
- **What about abstract XOR (operator with algebraic properties) and hashes (no cancellation rules and no inverse)?**

Extension to XOR?

- **Given real XOR/Hash  and abstract XOR/Hash **

Secure?



Impossibility Results: Symbolic XOR

– **Symbolic XOR** not **securely realizable wrt. blackbox simulatability**

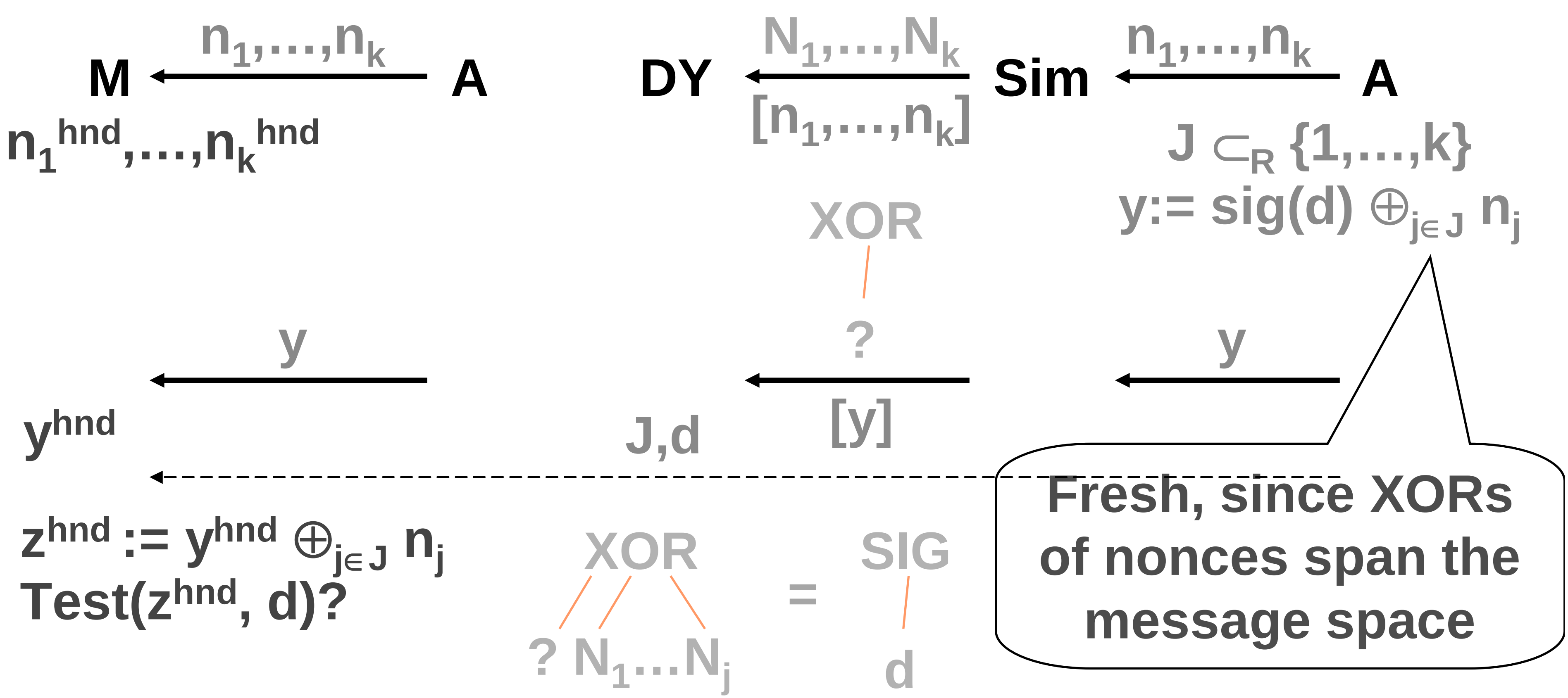
“*No Dolev-Yao style XOR can be securely realized wrt blackbox simulatability by any (moderately natural) implementation of XOR*”

- **“Meta-theorem”, hard to prove:**
  - **Reactive Simulatability reflexive**
  - **“Dolev-Yao style” difficult to capture formally**
  - **What is “natural implementation of XOR”?**

  $\longrightarrow$ **Series of concrete statements that can be verified**

\+ **Symbolic XOR sound under passive attacks**

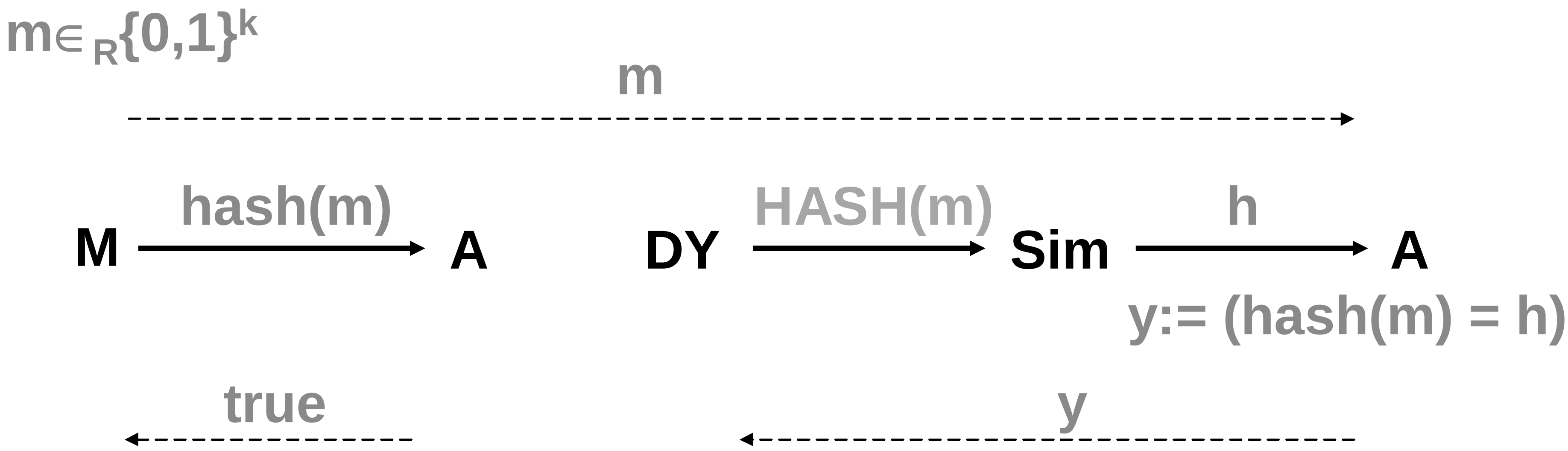
General Counterexample



Always true

- **Unsolvable on the term level**
- **Provably requires computing cryptographic test routine**

One Reason why Hash Functions fail



- **Needed:** **Pr[y = true] ≥ 1 – 1/poly(k)**
- **Properties of hash give:** **Pr[y = true] ≤ 1/poly(k)**

Summary of Secure Reactive Systems

- **Reactive simulatability: core definition to link cryptography and formal methods**
- **Justifying Dolev-Yao-style abstraction as the most important task (and this works for a lot of the common operations!)**
- **But also great for lots of other abstractions of various crypto primitives**
- **Composition and property preservation theorems enable usage**
- **First cryptographically sound proofs of Needham-Schroeder-Lowe, Otway-Rees, payment systems, etc.**
- **Now also limitations: Dolev-Yao-style Hash functions and XOR do not work**

More Information

- backes@cs.uni-sb.de
- http://www.zurich.ibm.com/security/models/
- Read just one paper?
  - ACM CCS 2003 (soundness)
  - ESORICS 2005 (impossibility)
- Read more? Oakland 2005, CSFW 2004, IEEE JSAC 2004, ESORICS 2003