Computationally Sound Symbolic Analysis of anonymity in presence of active adversaries

Hideki Sakurada

Joint work with H. Comon-Lundh,

Y. Kawamoto and M. Hagiya

Summary

- We prove the computational soundness:

$$P \sim Q \quad \Rightarrow \quad [\![P]\!] \approx [\![Q]\!]$$

Observational equivalence Computational indistinguishability

- For protocols with PKE and ring signatures, e.g. anonymous voting protocols,

$$P(\text{voter}_1, \text{vote}_1, \text{voter}_2, \text{vote}_2) \sim P(\text{voter}_2, \text{vote}_1, \text{voter}_1, \text{vote}_2)$$

- Without assuming polynomially-computable parsing functions.

Previous soundness results

- Abadi and Rogaway: term equivalence, passive adversary,
- Micciancio and Warinschi: trace properties, active adversary, assume parsing
- Comon-Lundh and Cortier: process equivalence, simple processes, symmetric encryption, active adversary, assume parsing
- Kawamoto et al.: process equivalence, ring signatures, active adversary, assume parsing, bounded # of sessions
- Backes et al.: trace properties, active adversary, restricted class of protocols?, assume parsing

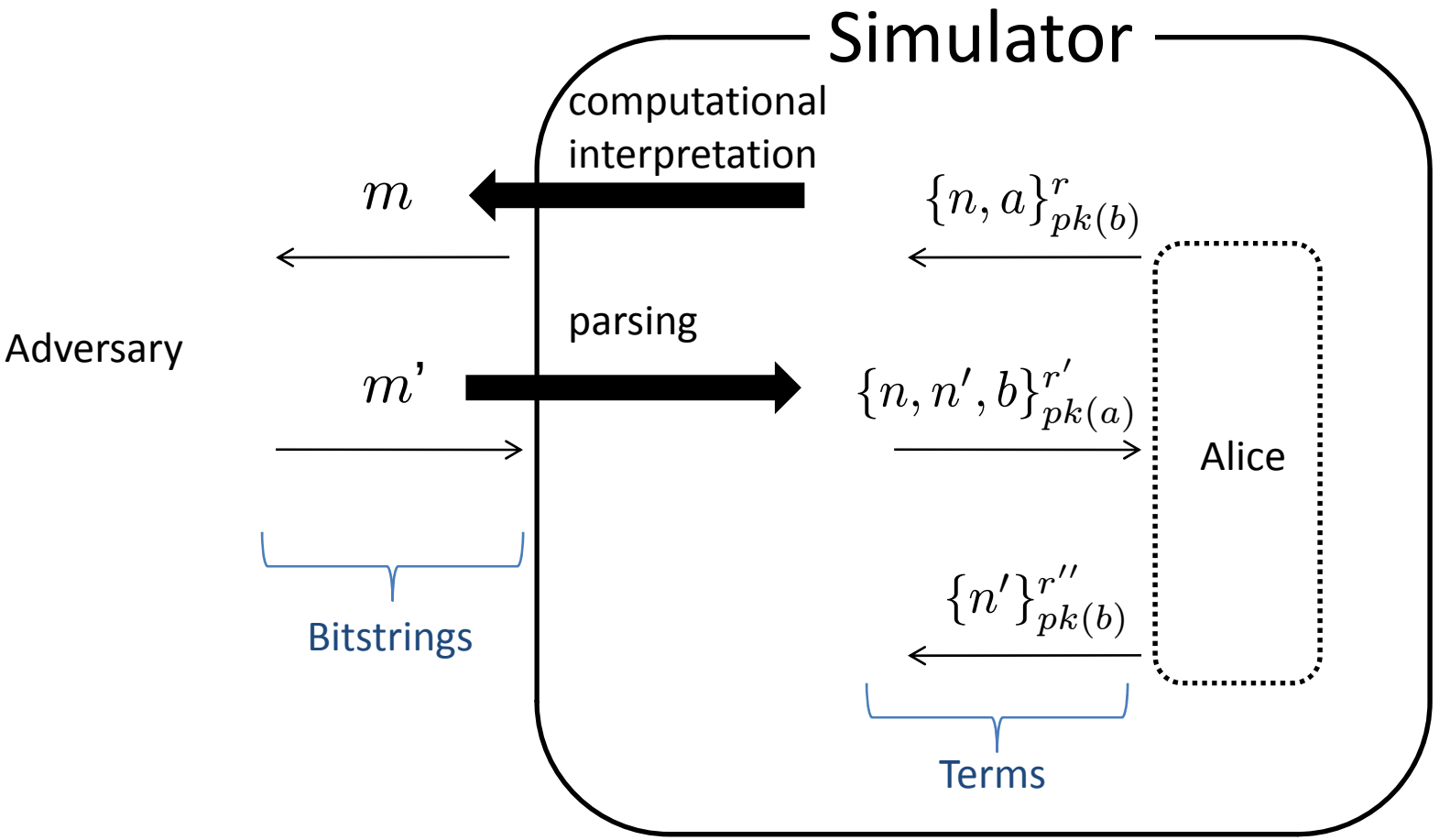
Our result

- We prove the computational soundness:
  - Process equivalence
  - Larger class of protocols
  - More primitives (PKE and ring signatures)
  - Active adversary
  - Unbounded number of sessions
  - *Without assuming parsing*

Simulator's parsing

- In the proof of mapping lemma [Micciancio and Warinschi] , the simulator simulates agents by interpreting terms and parsing bitstrings.
- If a message sent by the adversary is parsed into a term symbolically impossible to be produced, the simulator break, e.g., IND-CCA.
- Parsing must be polynomially computable.

Simulator's parsing



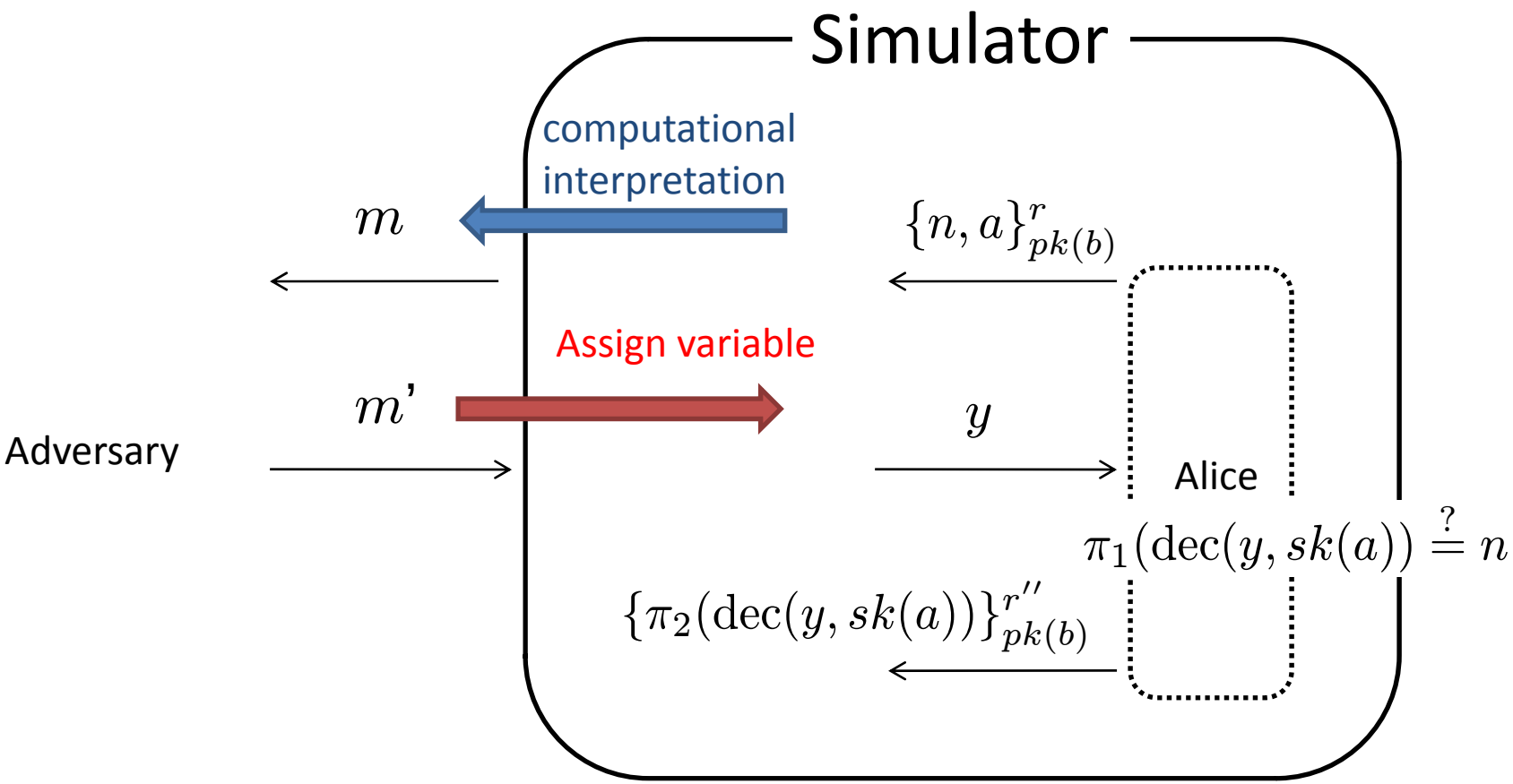
In order to make parsing polynomially computable,
Previous work doesn't allow a ciphertext by an unknown key.

Our Approach

- Simulator doesn't parse messages, but only simulates participants.

  (It doesn't touch messages until participants do)
- If the simulator goes down to a branch (of *if-then-else* statement) that is symbolically impossible, we break, e.g., IND-CCA.

Our approach



The simulator does not touch received messages until the participants do in a condition or a reply message.

Processes (Applied pi-calculus)

Processes

$$
\begin{aligned}
P, Q ::= \quad & P \parallel Q \\
& !P \\
& \nu n.P \\
& c(x).P \qquad \text{Receiving of term} \\
& \overline{c}(M).P \qquad \text{Sending of term M} \\
& \text{if } C \text{ then } P \text{ else } Q
\end{aligned}
$$

Terms

$$
\begin{aligned}
M ::= \quad & n, r \\
& \{M, M'\} \\
& \pi_i(M) \\
& \{M\}^r_{M'} \\
& \mathrm{dec}(M, M') \\
& [M]^r_{M', VK} \\
& \mathrm{check}(M, VK)
\end{aligned}
$$

Communication

$$c(x).P \parallel \overline{c}(M).Q \rightarrow P\{x \mapsto M\} \parallel Q$$

Observational equivalence (P and Q behaves same under any process A)

$$P \sim Q \quad \Longleftrightarrow \forall A.((P \parallel A) \downarrow_c \Leftrightarrow (Q \parallel A) \downarrow_c)$$

Outline of the soundness proof

[Comon-Lundh and Cortier]

$$P \sim Q$$

Observational equivalence is characterized by equivalence (bisimilarity) of computation tree

$$T_P \sim T_Q$$

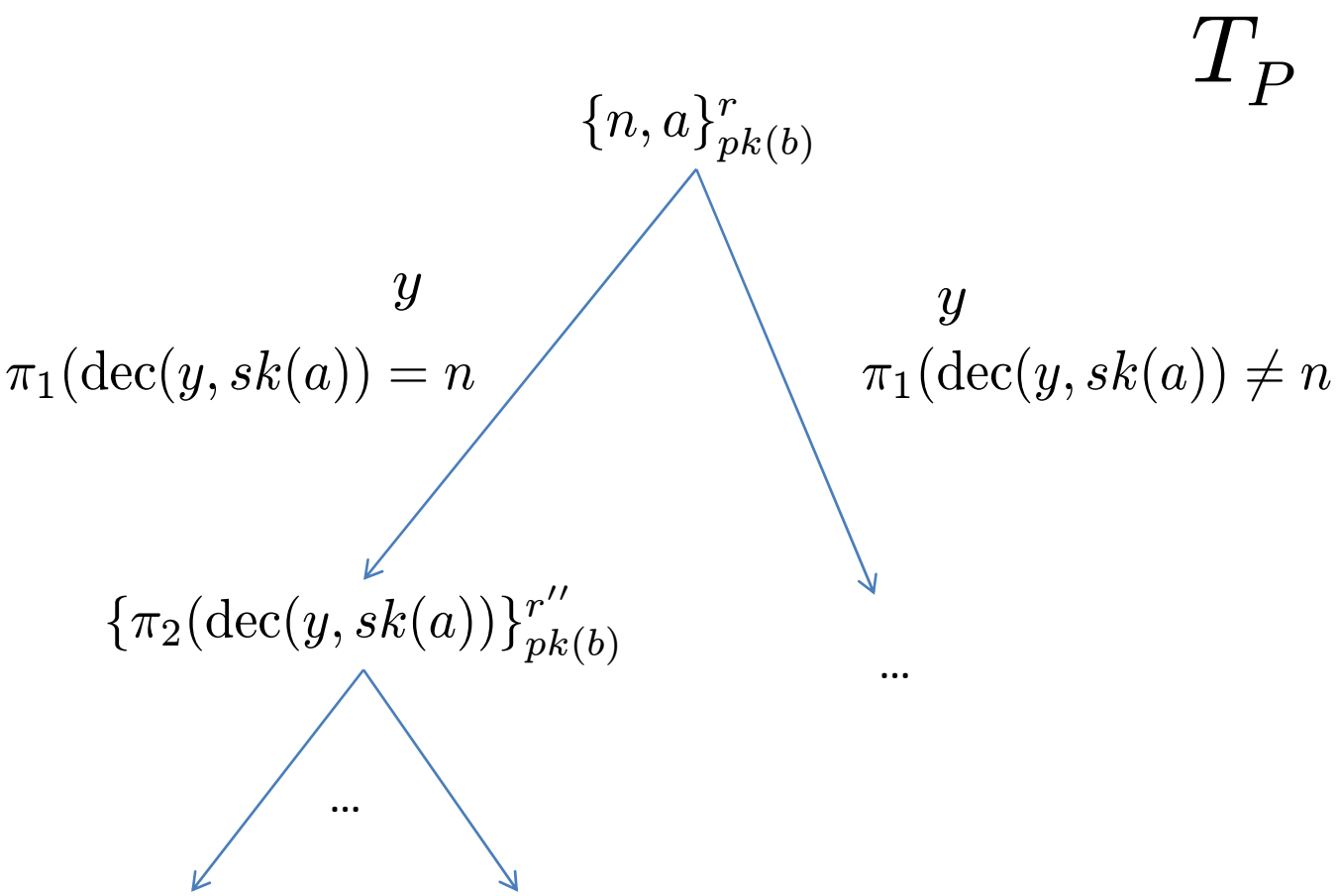
Generalization of [Abadi and Rogaway] into trees

$$\mathcal{O}_{T_P} \approx \mathcal{O}_{T_Q}$$

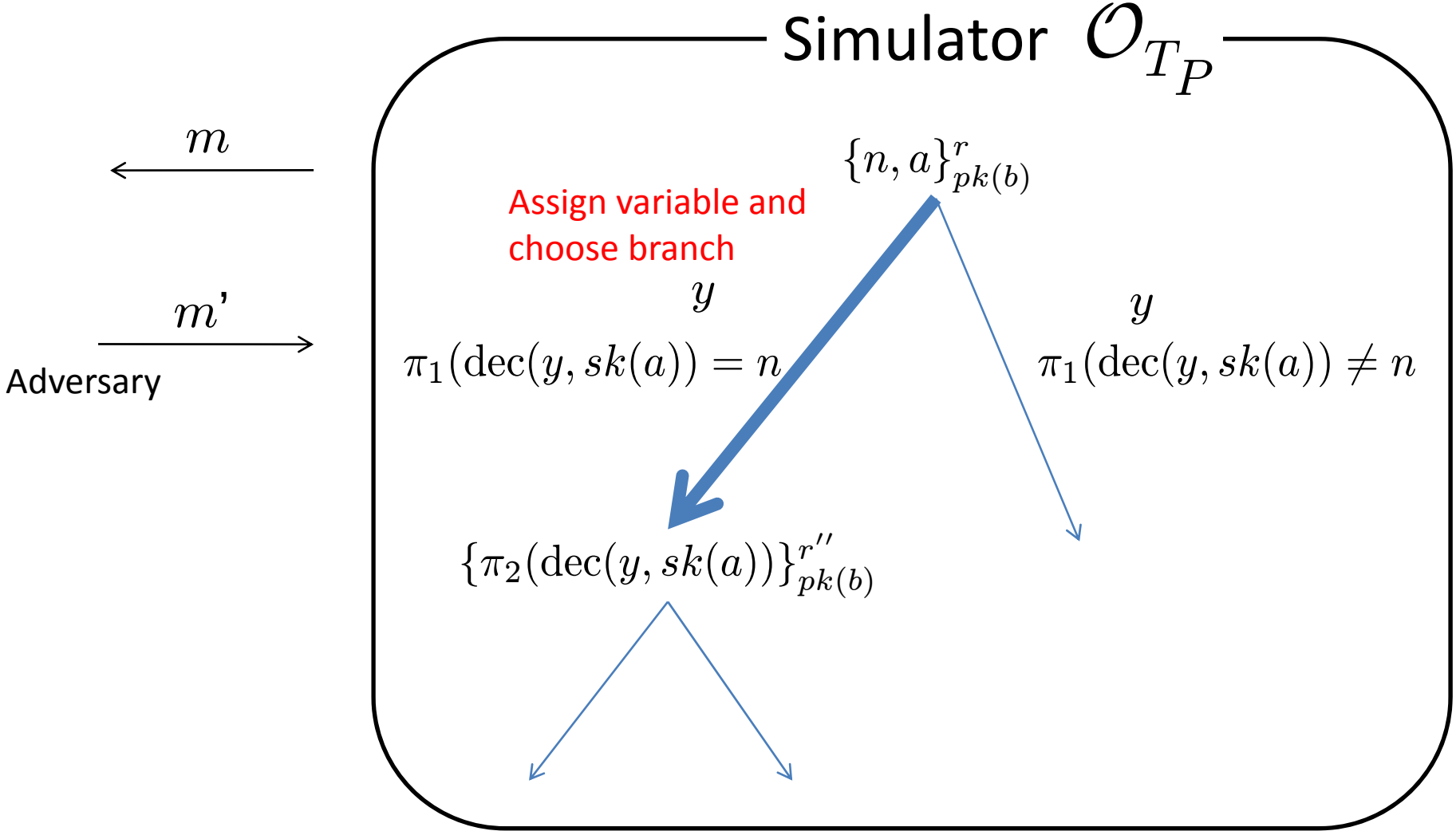
Mapping Lemma
[Micciancio and Warinschi]

$$[\![P]\!] \approx [\![Q]\!]$$

Our Computation Tree

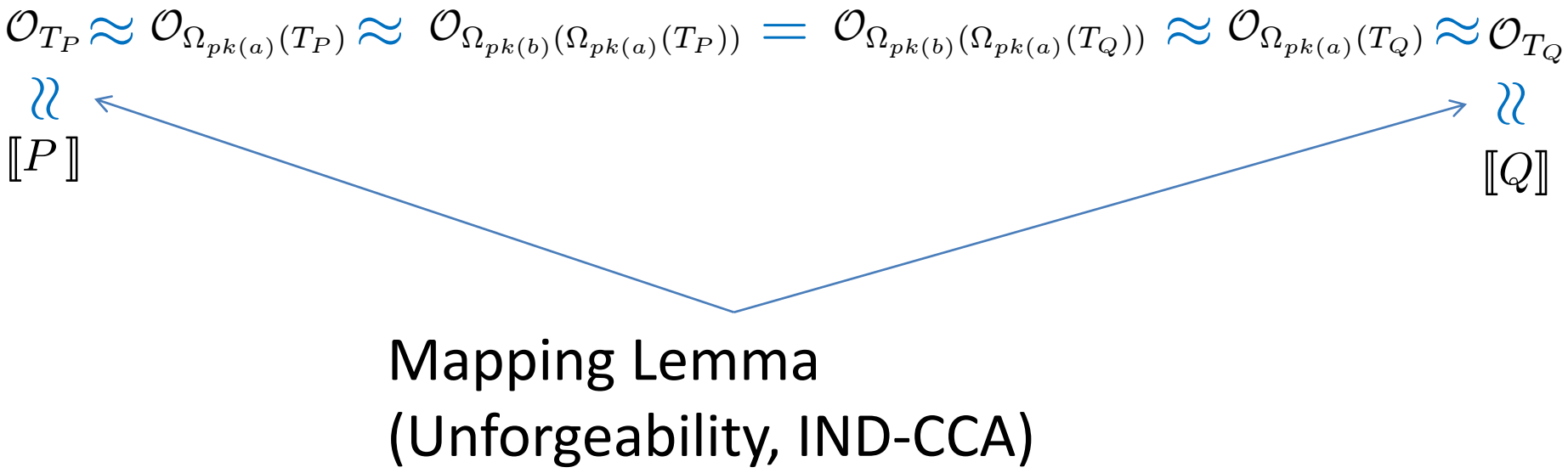


Simulator


Simulator $\mathcal{O}_{T_P}$
m
m'
Adversary
$\{n, a\}^r_{pk(b)}$
Assign variable and choose branch
y
$\pi_1(\mathrm{dec}(y, sk(a)) = n$
y
$\pi_1(\mathrm{dec}(y, sk(a)) \neq n$
$\{\pi_2(\mathrm{dec}(y, sk(a))\}^{r''}_{pk(b)}$

More details

Successive game transformations
(IND-CCA, anonymity of ring signatures)



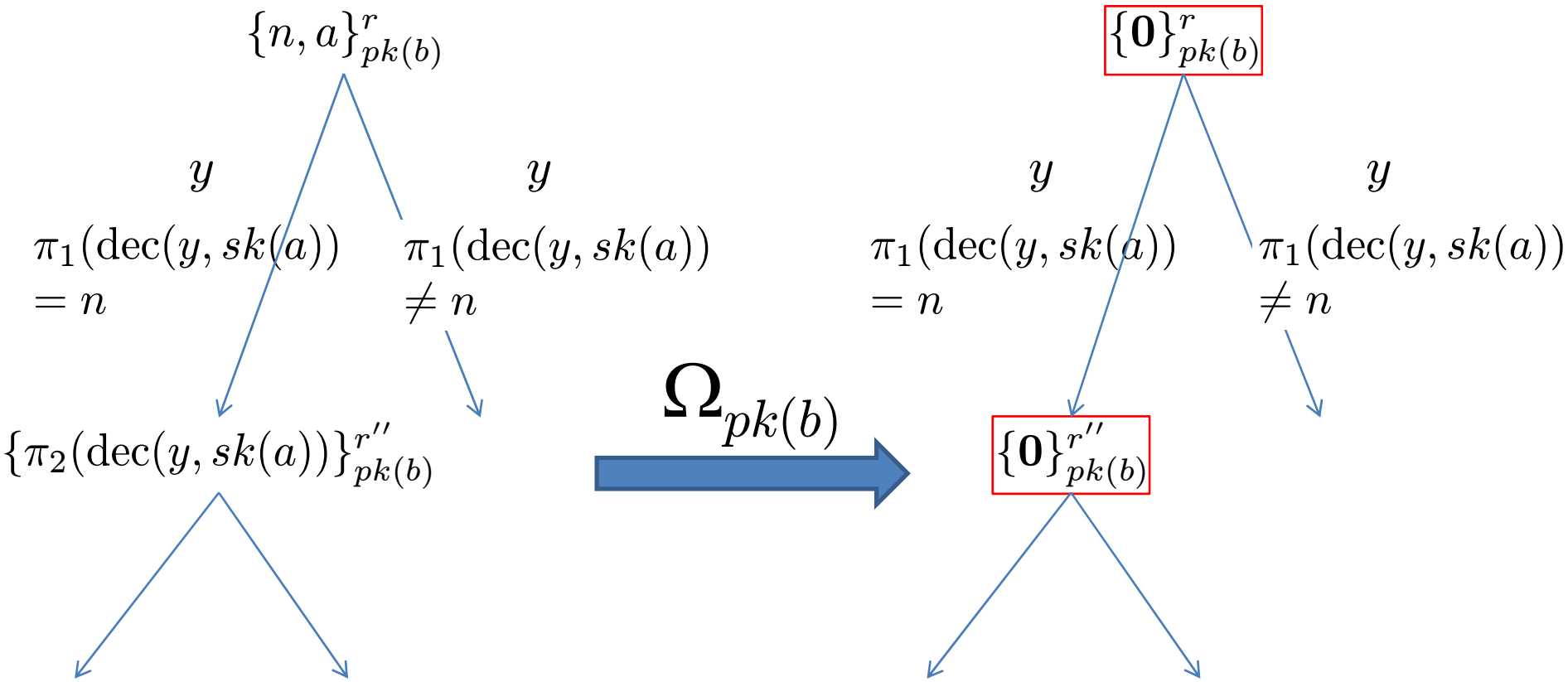
Mapping Lemma
(Unforgeability, IND-CCA)

Computational assumptions

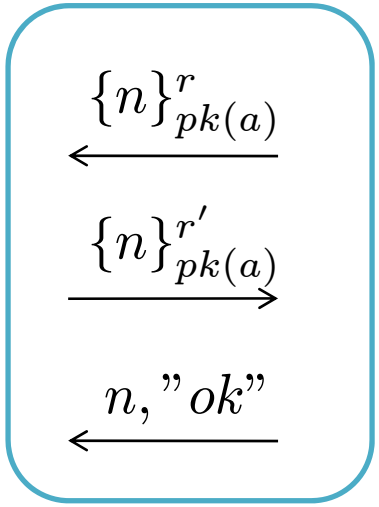
- Public-key encryption: IND-CCA
- Ring signatures:
  - Unforgeability: signatures cannot be produced without signing keys
  - Anonymity: signers of a group are indistinguishable from their signatures

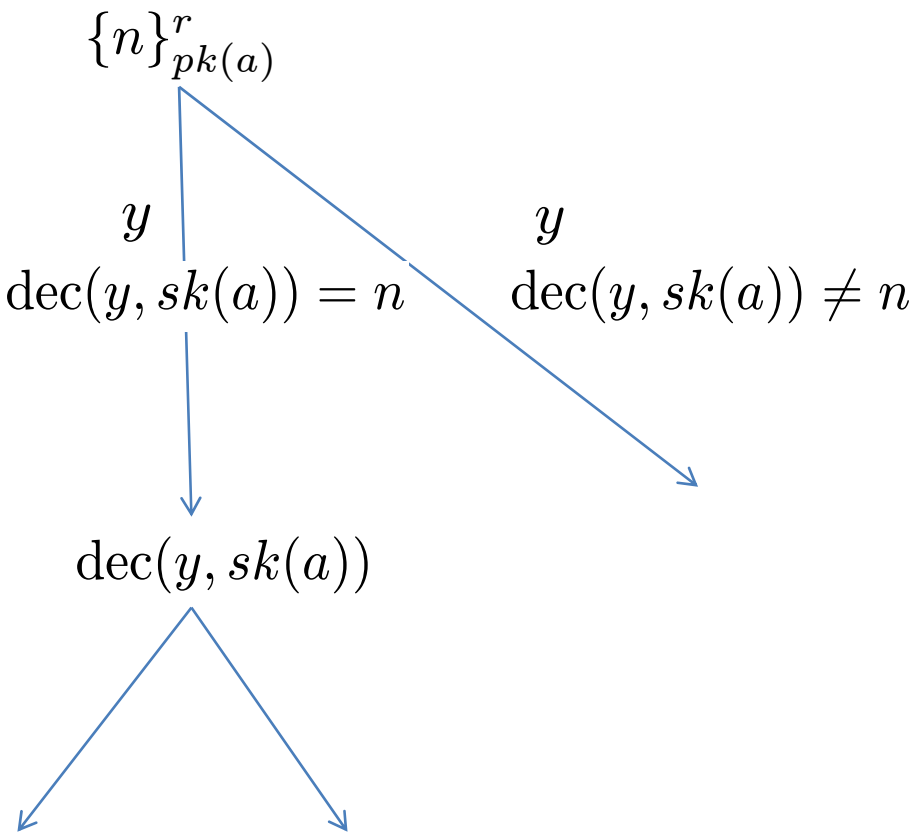
$$[m]^r_{sk_0,\{vk_0,vk_1,vk_2\}} \approx [m]^r_{sk_1,\{vk_0,vk_1,vk_2\}}$$

Transformation by IND-CCA: Easy case

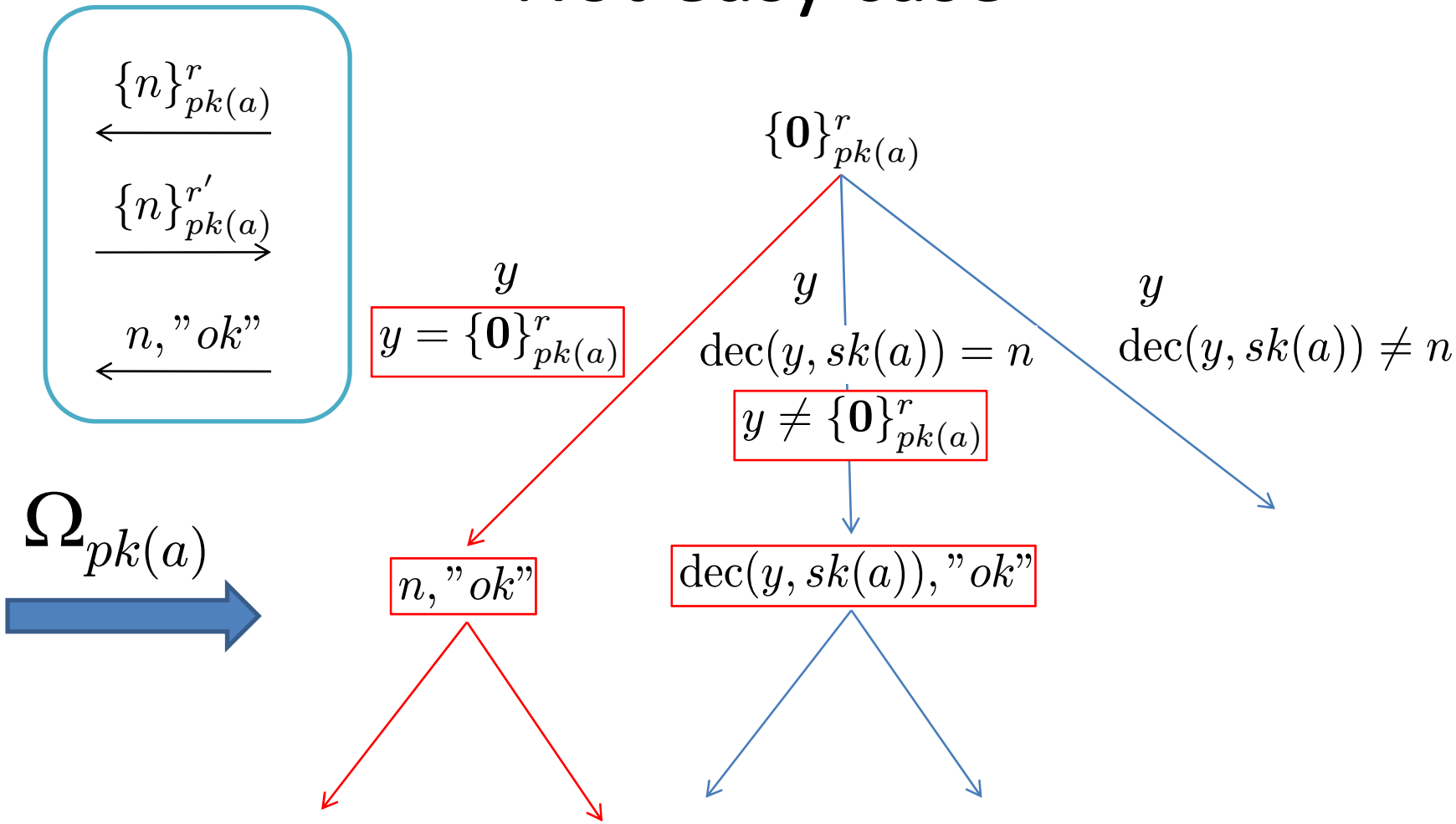


Transformation by IND-CCA: Not easy case





Transformation by IND-CCA: Not easy case



Conclusion

- We prove the computational soundness:

$$P \sim Q \quad \Rightarrow \quad [\![P]\!] \approx [\![Q]\!]$$

Observational equivalence — Computational indistinguishability

  - Larger class of protocols
  - More primitives (PKE and ring signatures)
  - Active adversary
  - Unbounded number of sessions
  - *Without assuming parsing*