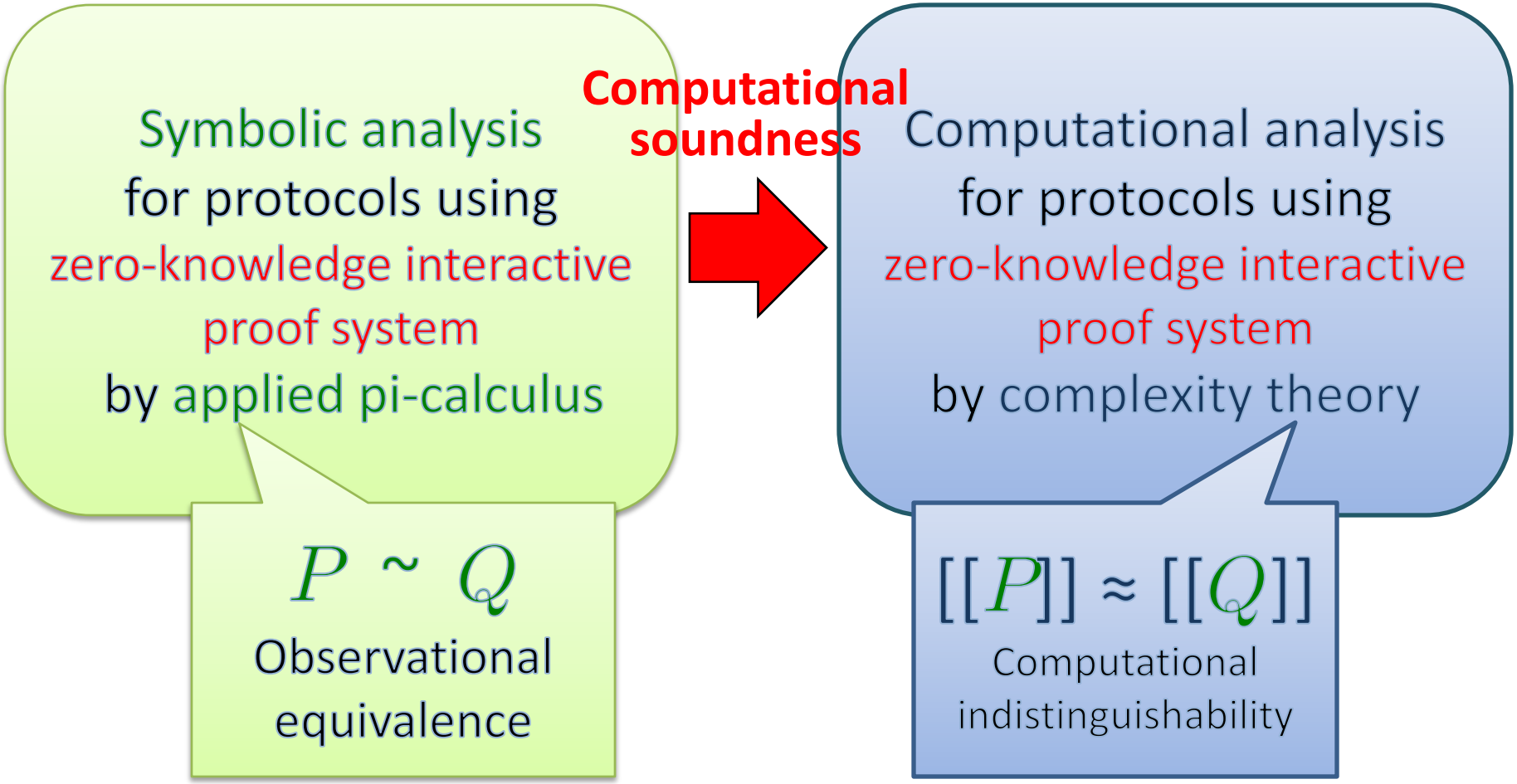
Computational Soundness of (Interactive) Zero-Knowledge Proof Systems in the Presence of Active Adversaries

Yusuke Kawamoto[1]

(Jointly with Gergei Bana[2] and Hideki Sakurada[3])

[1] University of Tokyo
[2] Technical University of Lisbon
[3] NTT Communication Science Labs.

Computational Soundness



Our Contributions

- Applied pi-calculus for protocols using Interactive Zero-Knowledge as sub-protocols
- Soundness of the observational equivalence of the applied pi-calculus (ongoing)
  - Active & adaptive adversary
  - Interpretation (i.e. the way of relating symbolic process with computational process) differs from previous work.
  - Mapping soundness + Tree soundness

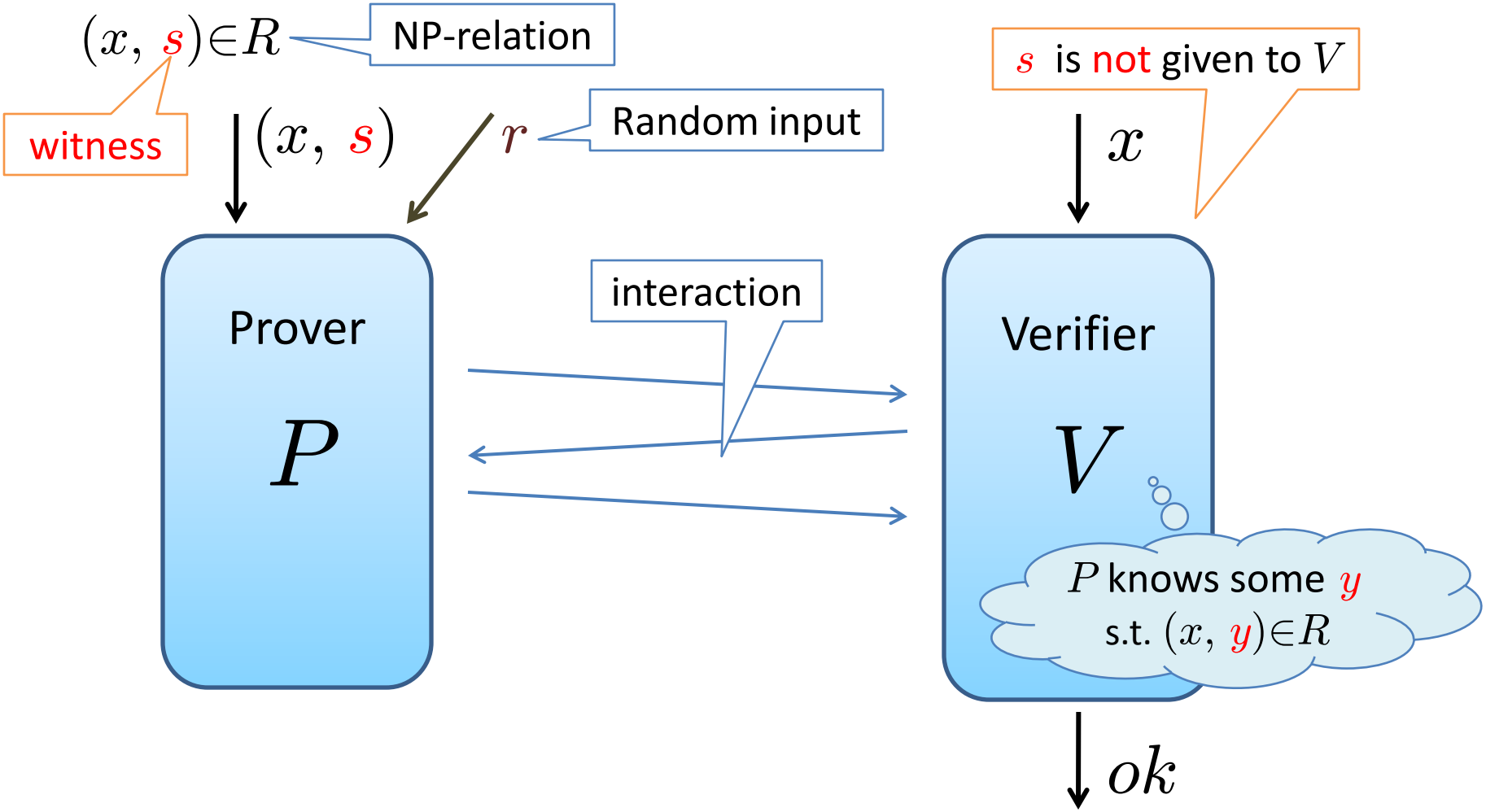
The proof of soundness is similar to [Comon & Cortier'08]

Similar results on mapping soundness for Non-Interactive Zero-Knowledge [Backes & Unruh'08]

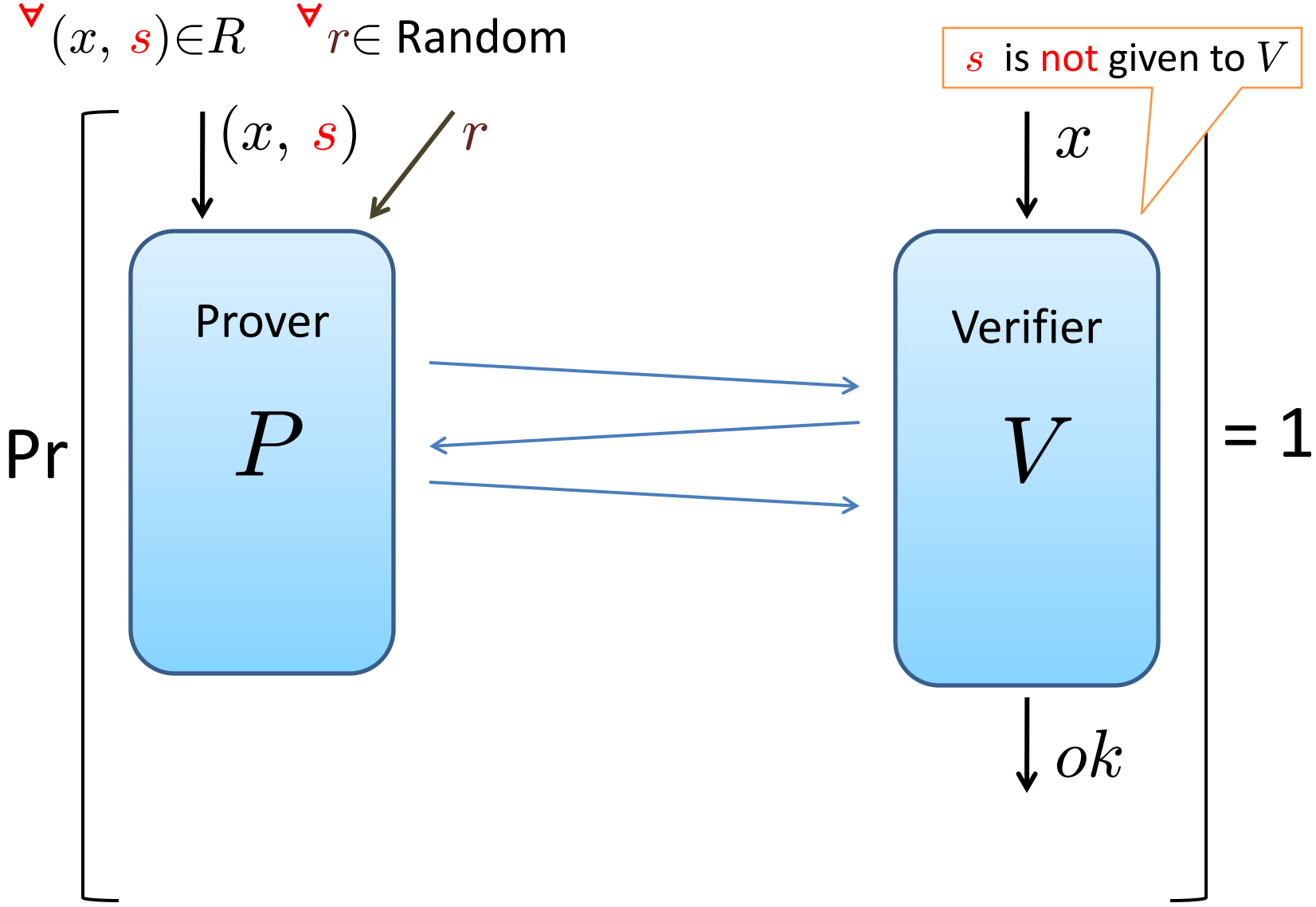
Overview

- Zero-Knowledge Interactive Proof System
- Symbolic model (applied pi-calculus)
- Computational Soundness
- Conclusion & Discussion

PoK (Proof of Knowledge) for R



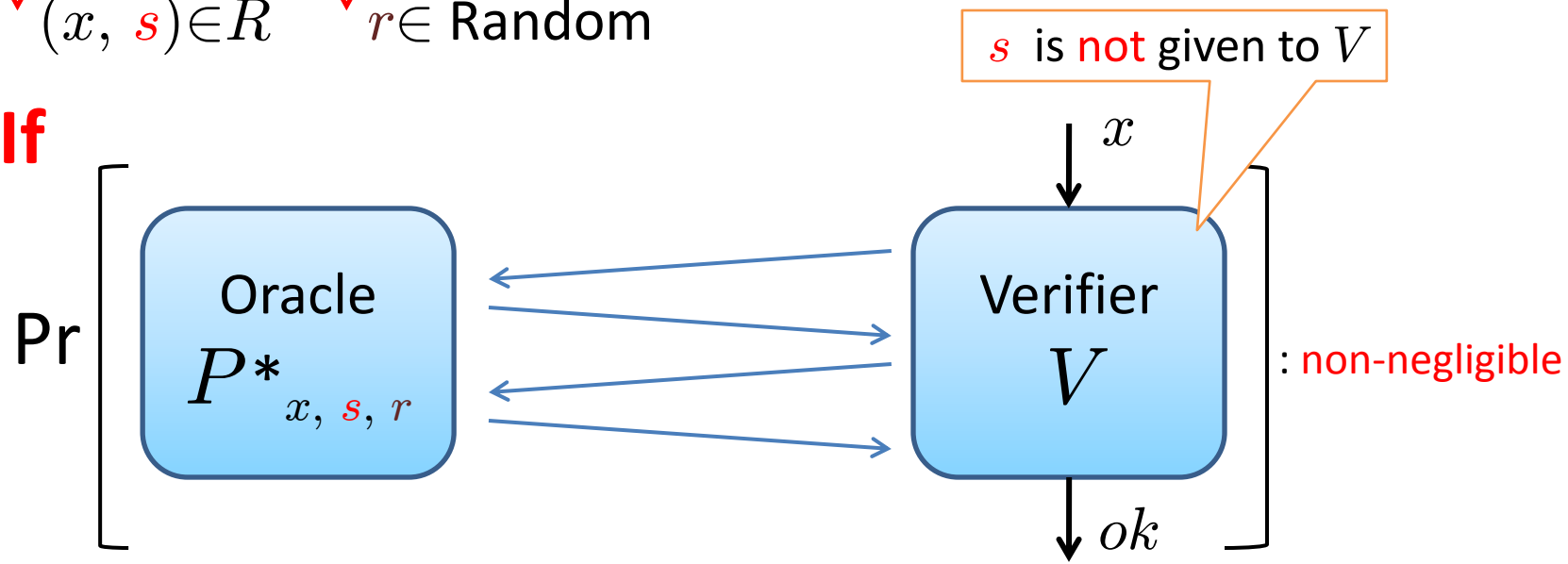
Non-triviality of PoK



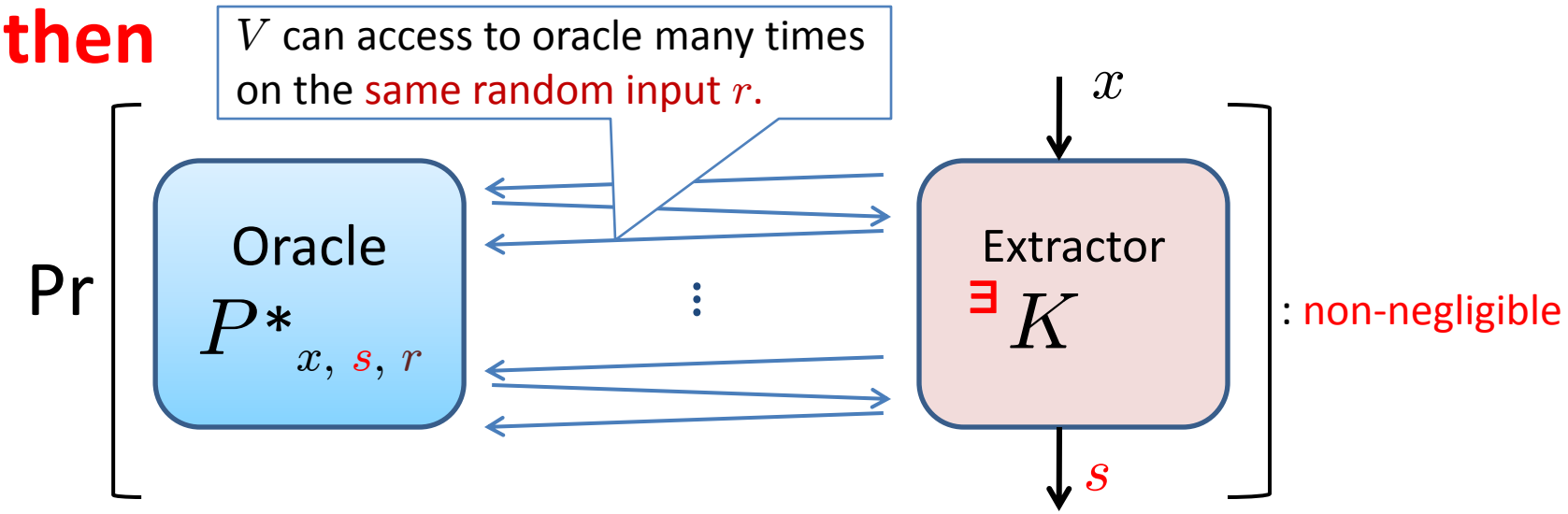
Validity of PoK

$\forall (x, s) \in R$ $\forall r \in$ Random

If

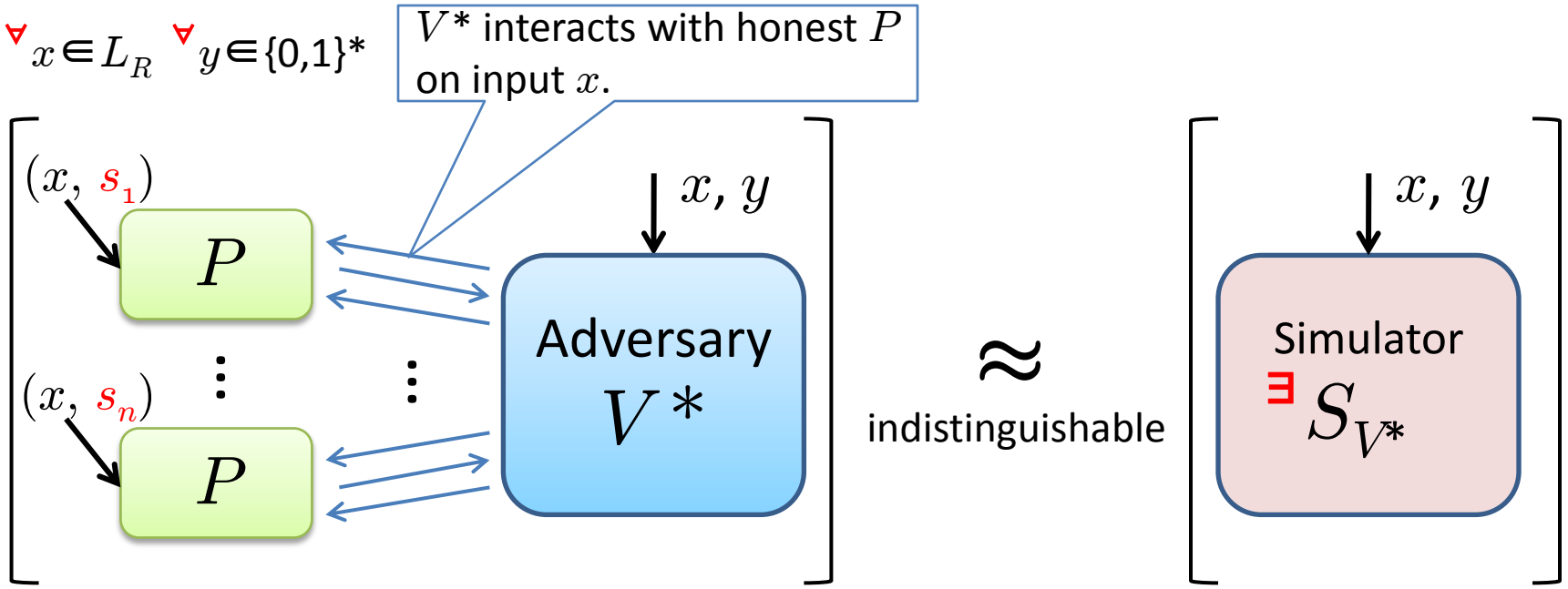


then



(**Concurrent**) **Zero-Knowledge** of PoK

- Adversary cannot obtain any information of the witness from provers running concurrently.
- Formally, for any PPT adversary V^*, there is PPT S_{V^*} s.t. V^* 's view and its simulation are indistinguishable.



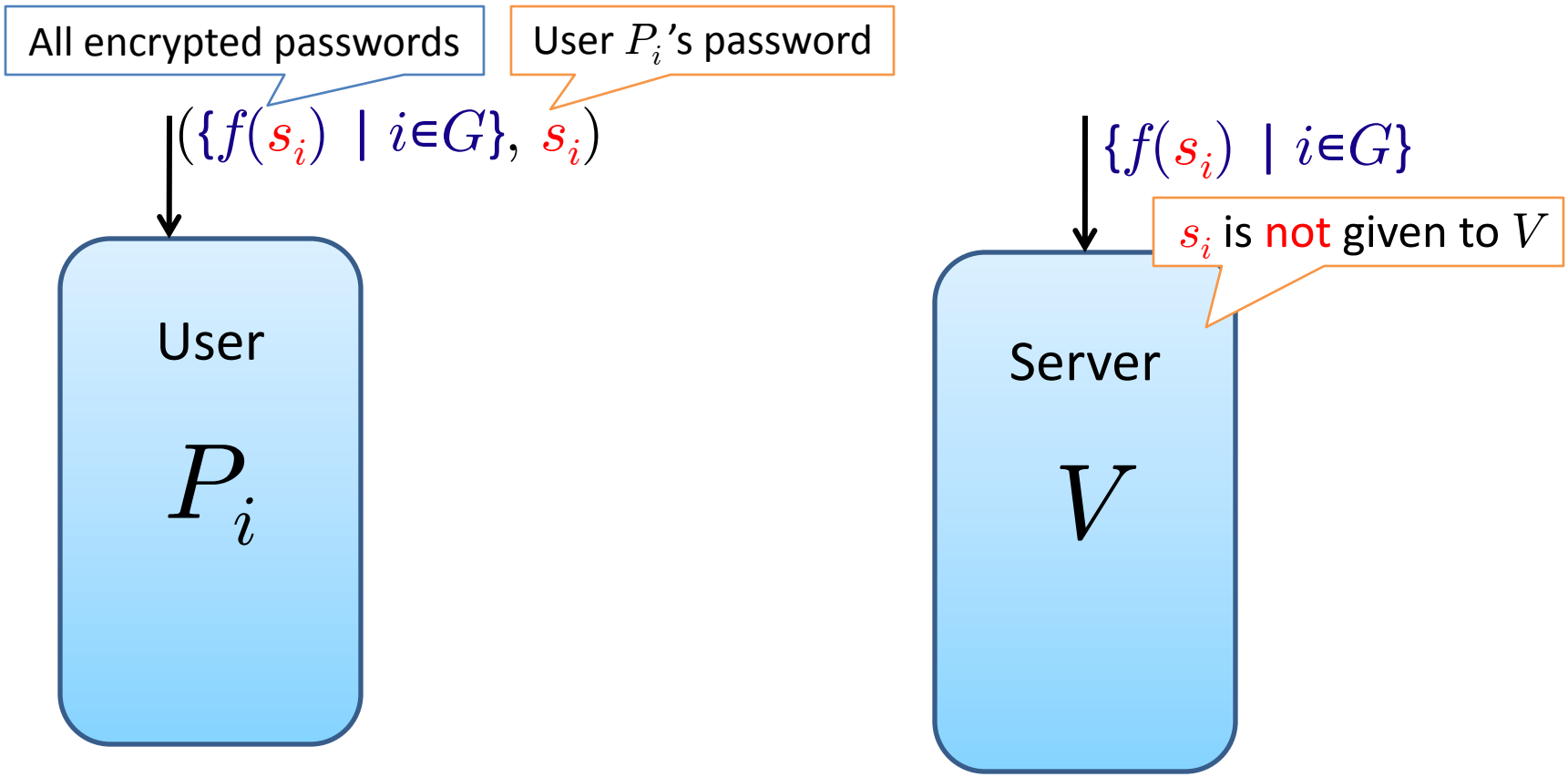
Our Computational Model

- Zero-Knowledge PoK (Proof of Knowledge)
  - Assume Non-triviality, Validity & Concurrent Zero-Knowledge
- One-way collision-free function f
- Each agent transmits bit strings:
  - Messages in PoK are explicitly transmitted.
- Adversary is probabilistic polynomial-time.

Example: Group Identification Protocol

PoK for $R=\{(x, s) \mid x \ni f(s)\}$

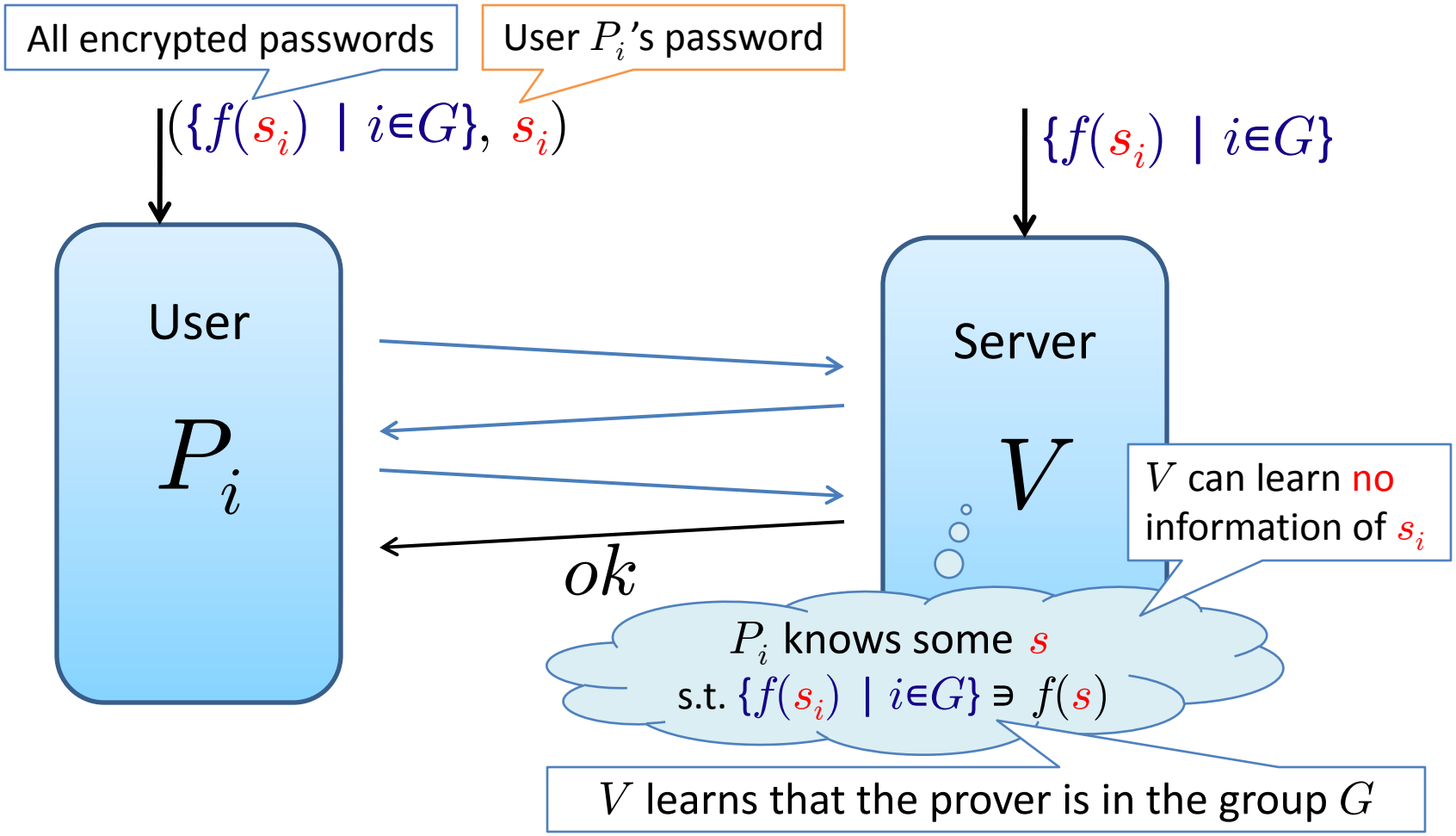
One-way collision-free function
No one can derive x from $f(x)$.



Example: Group Identification Protocol

PoK for $R=\{(x, s) \mid x \ni f(s)\}$

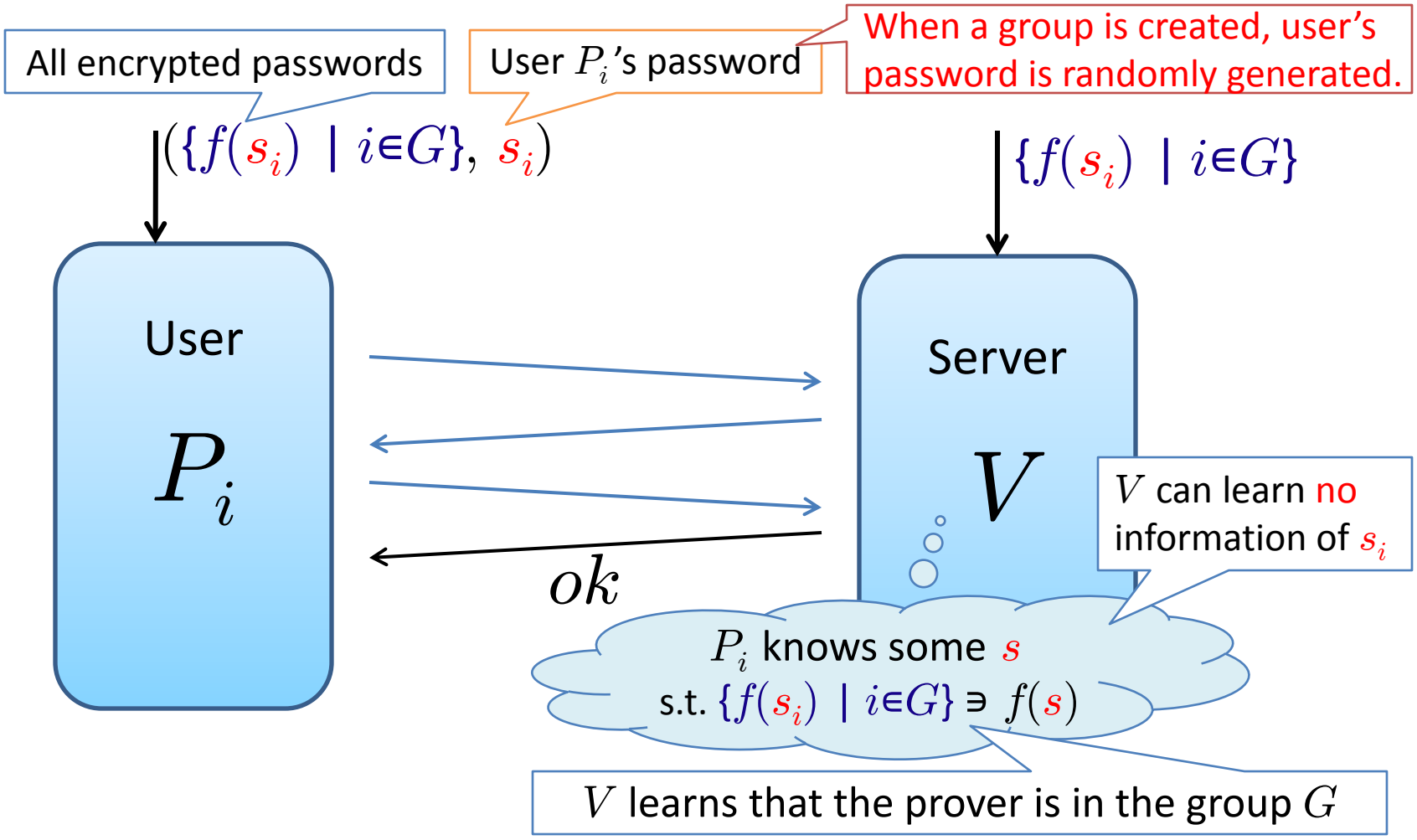
One-way collision-free function
No one can derive x from $f(x)$.



Example: Group Identification Protocol

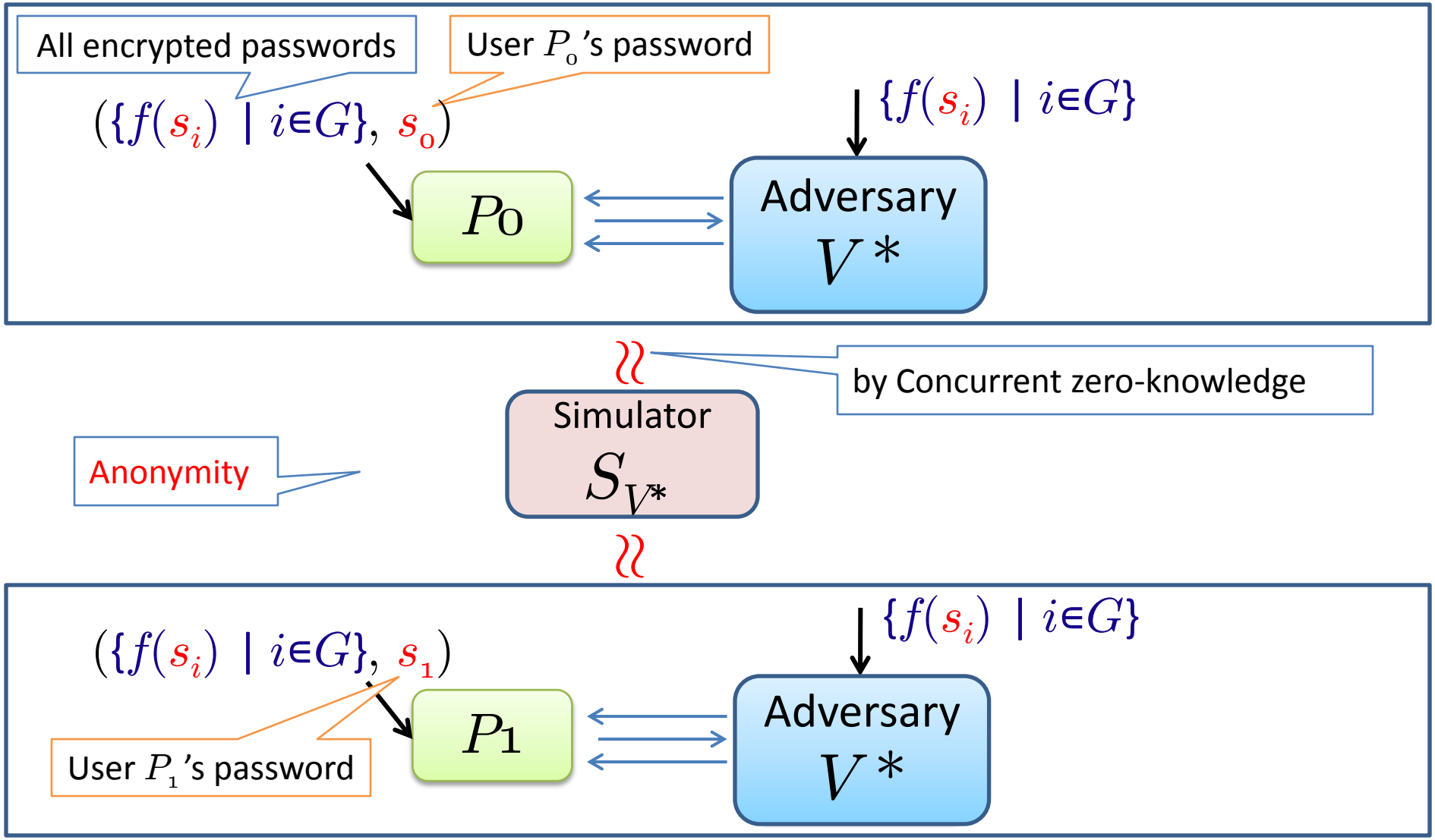
PoK for $R=\{(x, s) \mid x \ni f(s)\}$

One-way collision-free function
No one can derive x from $f(x)$.



Example: Group Identification Protocol

PoK for $R=\{(x, s) \mid x \ni f(s)\}$



Overview

- Zero-Knowledge Interactive Proof System
- Symbolic model (applied pi-calculus)
- Computational Soundness
- Conclusion & Discussion

Terms

- Agents transmit symbolic messages (Dolev-Yao terms).
- We introduce terms that abstracts ZKIP.

Term ::= Name | f(Name) | { Term, Term } | π_1(Term) | π_2(Term) | ok | $\perp$ | v(Term) | w(Term , Term, Term)

Password

One-way collision-free function
No one can derive x from f(x).

These terms abstracting ZKIP correspond to a lot of messages in interactive proofs in computational setting.

Conditions

- Agents & adversary can use the condition tests:

Φ ::= *M*(Term) — Well-formedness of terms

| *EQ*(Term, Term) — Equality as bit strings

| *Verify*(Term , Term, Term)

| $\Phi \wedge \Phi$ | $\Phi \vee \Phi$ — No negation

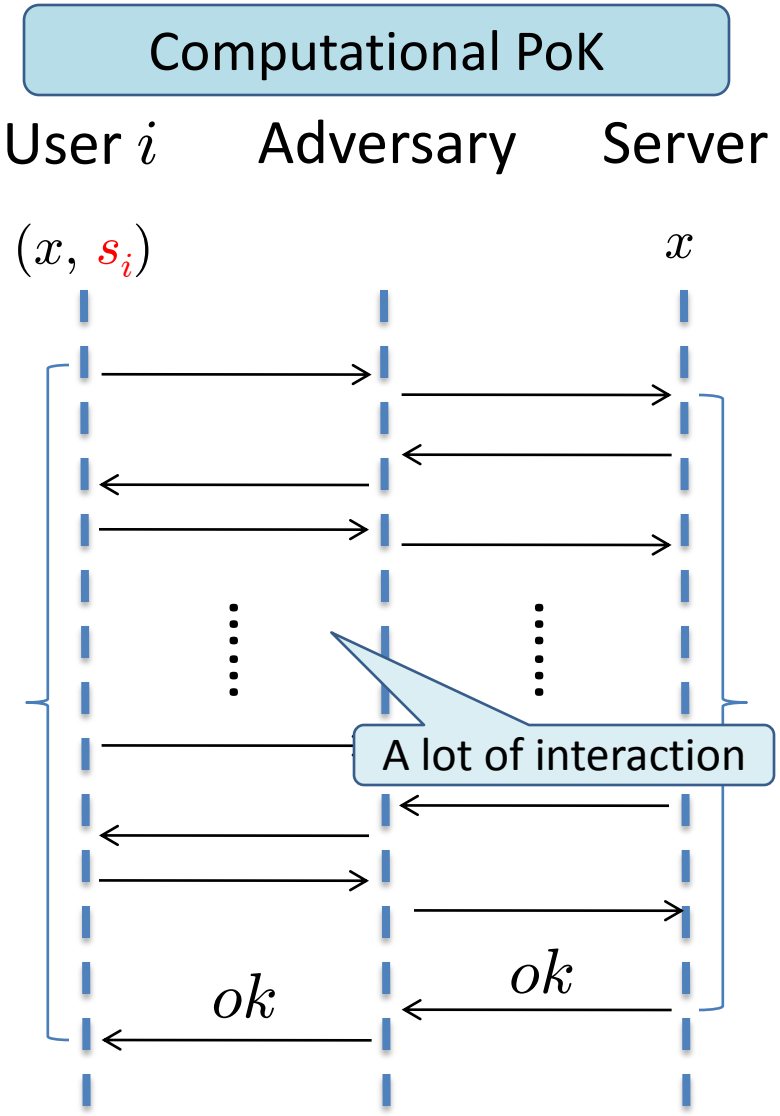
Check whether the interactive proof is true or not.

Symbolic Process

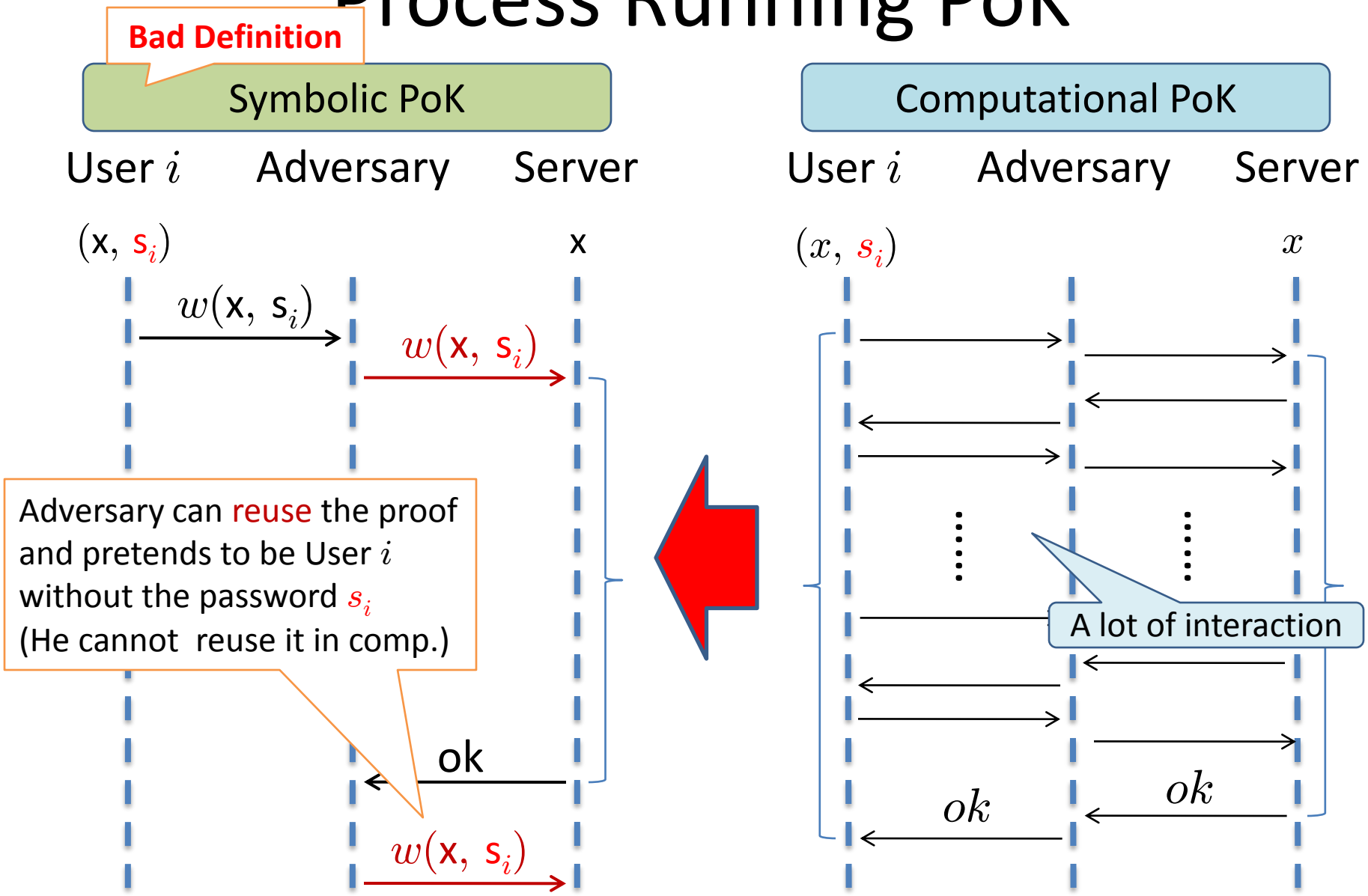
- General definition of Process (similar to [Comon & Coriter'08])

P, Q	::=	$\mathbf{c}(x).P$	input
	|	$\overline{\mathbf{c}}(u).P$	output
	|	$\mathbf{0}$	terminated process
	|	$P \parallel Q$	parallel composition
	|	$!P$	replication
	|	$(\nu\alpha)P$	restriction
	|	$\texttt{if}\ \Phi\ \texttt{then}\ P\ \texttt{else}\ \overline{\mathbf{c}}(\bot).\mathbf{0}$	condition

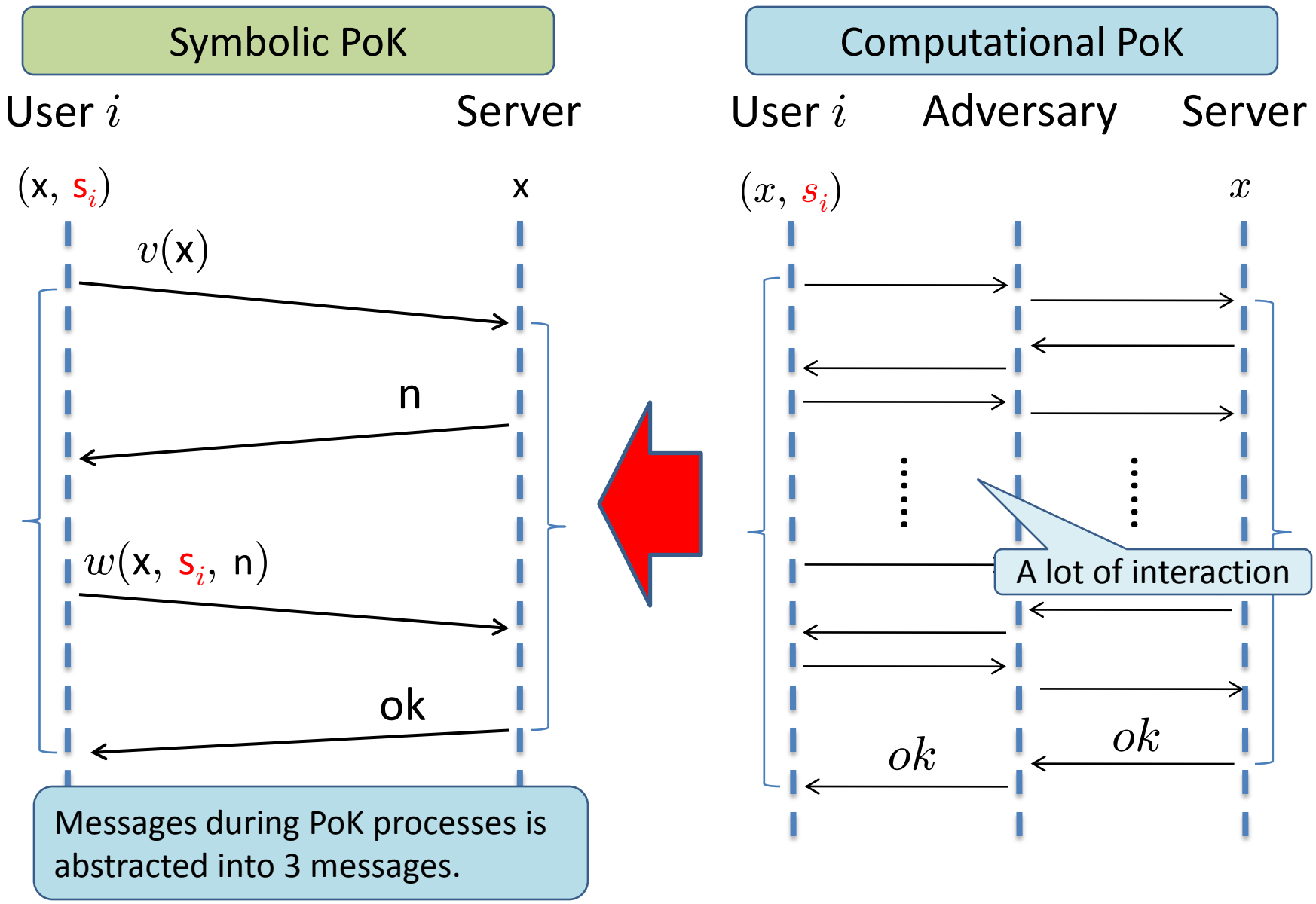
Process Running PoK



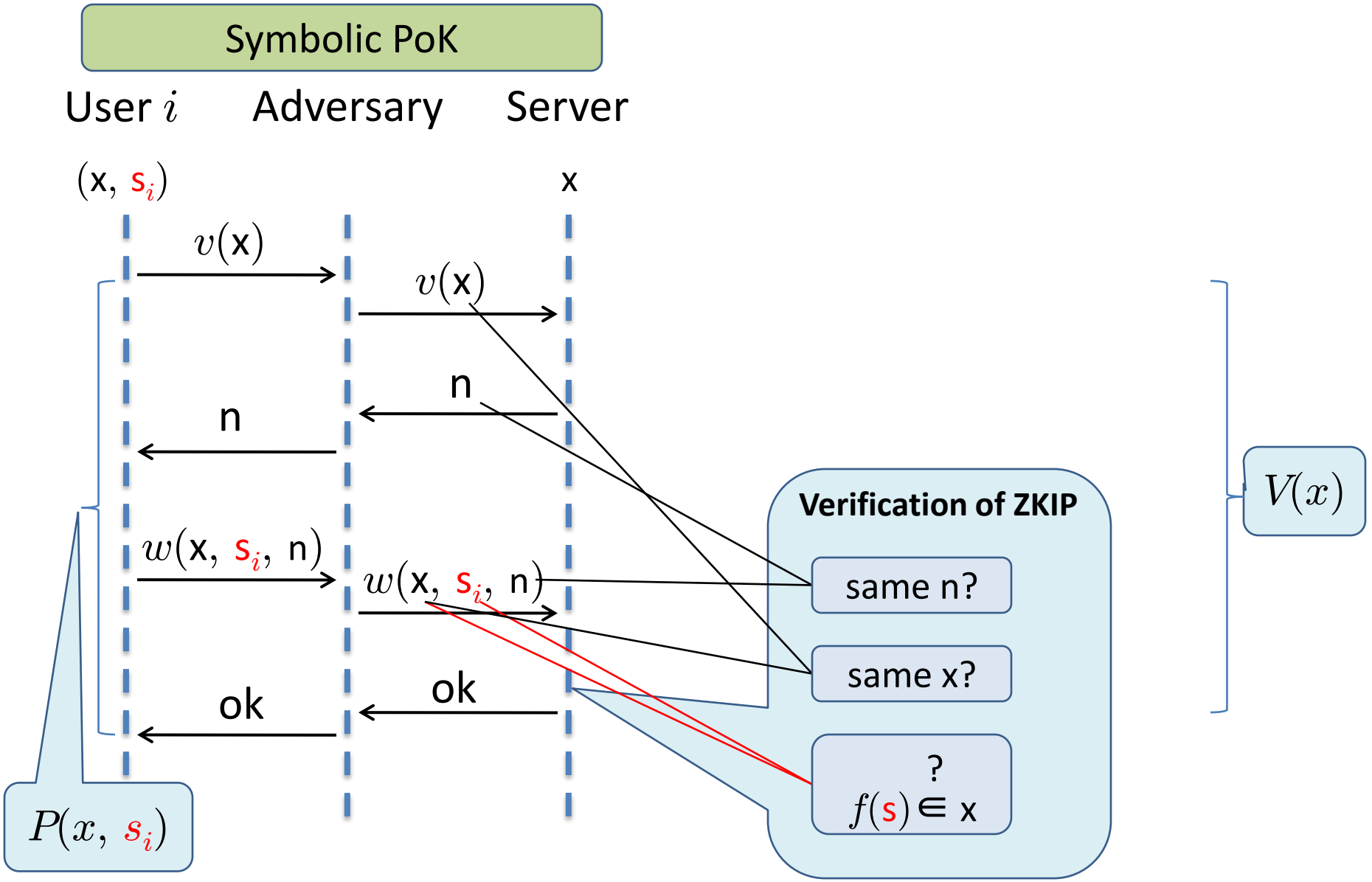
Process Running PoK



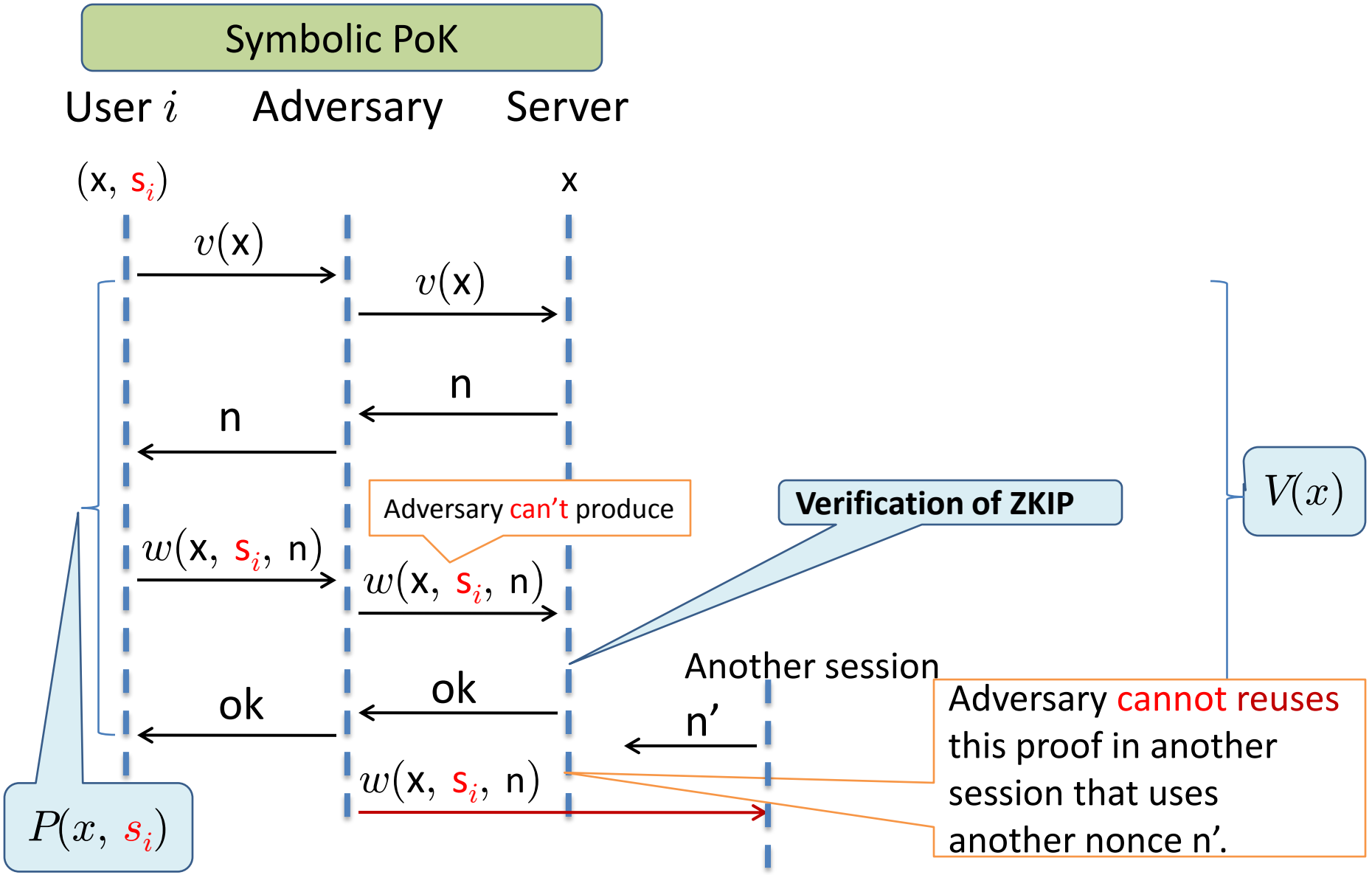
Process Running PoK



Process Running PoK



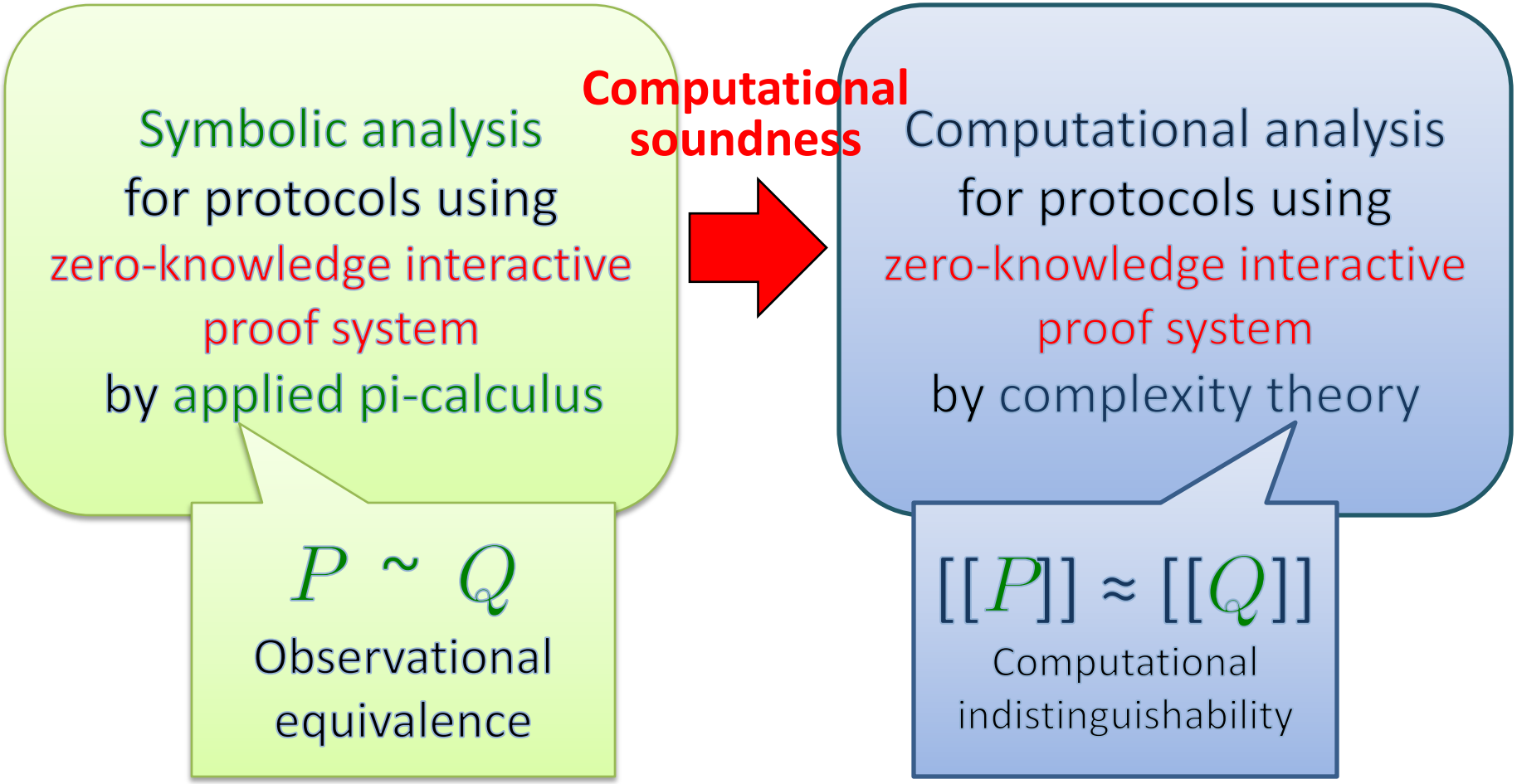
Process Running PoK



Overview

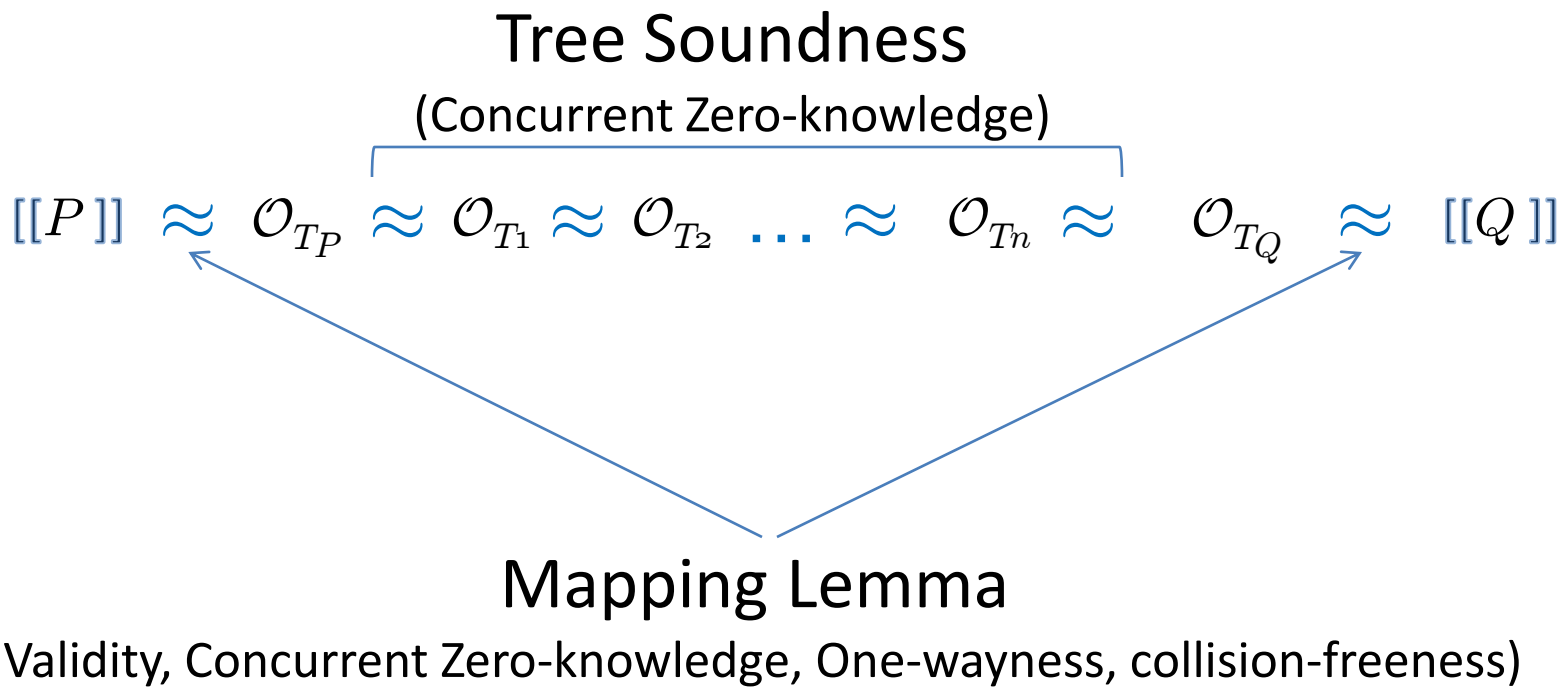
- Zero-Knowledge Interactive Proof System
- Symbolic model (applied pi-calculus)
- Computational Soundness
- Conclusion & Discussion

Computational Soundness



Outline of Proof

The proof of soundness is similar to [Comon & Cortier'08]



Conclusion

- Applied pi-calculus for protocols using Interactive Zero-Knowledge (of knowledge)

- Soundness of the observational equivalence of the applied pi-calculus (ongoing)
  - Active & adaptive adversary
  - Interpretation differs from previous work.
  - Mapping soundness + Tree soundness

Related Work

- Soundness of symbolic Non-Interactive ZK [Backes and Unruh]
  - Our work deal with interactive ZK.
    - In their symbolic model, a prover sends a proof term.
    - In our model, Messages during PoK processes is abstracted into 3 messages.
  - Our work includes not only mapping but also tree soundness.
  - Assumption on ZK
    - They assumed Non-malleability of ZK proofs.
    - Our work does not assume it, and restricts the class of protocols.

- Universally composable ZK
  - Universally composable ZK requires CRS model.
  - Our work deals with Concurrent ZK that is weaker than Universal Composable ZK.
  - Composition of soundness result is our future work.

Thank you for your attention.