Development of a Verification Tool for Composable Security

Itsuki SUZUKI, Yoshiki KAMANO,
Maki YOSHIDA, Toru FUJIWARA

Osaka University

Outline

- Background
- UC framework and previous verification
- Our symbolic model and results
- Conclusion and future work

Composable Security

- Protocols are required to satisfy composable security
  - Maintained under a general protocol composition operation

⇒Such a security is provided by various frameworks

  - Universally composable (UC) framework
  - Reactive simulatability (RSIM) framework
  - Probabilistic polynomial-time process calculus (PPC)
  - Task-structured probabilistic I/O automata (task-PIOA) framework

- Proving security is difficult and error-prone

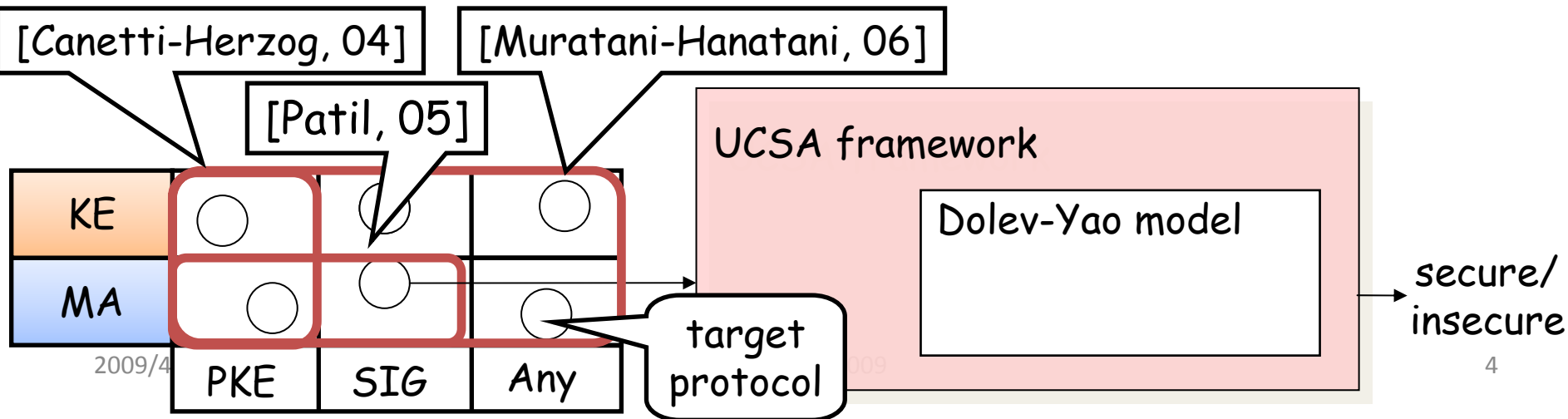
⇒Formal verification methods for these security were provided

UC framework is used for formulating and analyzing the security of many cryptographic protocols

Our goal is to develop a verification method for UC security

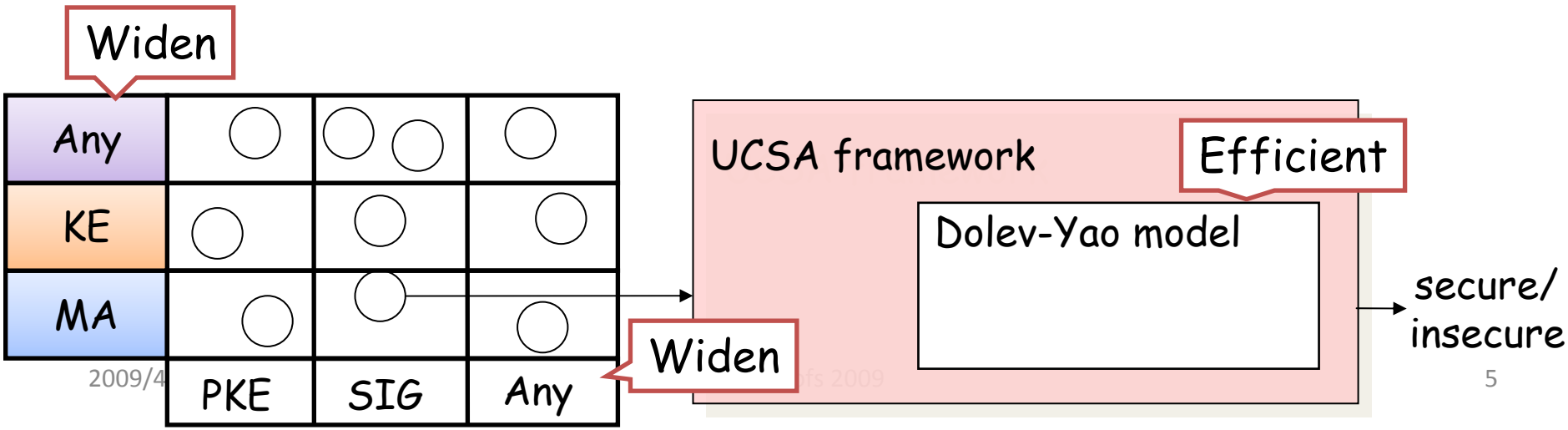
Formal Verification for UC Security

- [Canetti-Herzog, 04]
  - Proposed a universally composable symbolic analysis framework (UCSA) based on the Dolev-Yao model
  - Concentrated on mutual authentication (MA) and key exchange (KE) protocols that use public key encryption (PKE)
  - Verified the UC security of Needham- Schroeder-Lowe protocol by ProVerif
- [Patil, 05]
  - Expanded UCSA to include MA protocols that also use digital signatures (SIG)
- [Muratani-Hanatani, 06]
  - Presented a general approach to allow MA and KE protocols to use any cryptographic primitives



Future Work [Canetti, 08]

- Widen the range of cryptographic primitives that can be modeled in an abstract, symbolic, and composable way
- Widen the range of security properties and tasks that can be asserted symbolically
- Construct new tools to allow for efficient automated security analysis, capitalizing on the composable approach
- Formulate and assert the composability of security properties directly in a symbolic model



Brief Objective, Method, Results

- Objective
  - Further development of UCSA
- Method
  - Extend our symbolic model so that it can symbolically define notions in the UC framework
- Results
  - Demonstrate that our symbolic model can be used to verify the UC security of same protocols as [Patil, 05]
    - MA protocols using PKE and SIG
  - Symbolically define some notions in the UC framework for KE protocols that use PKE and SIG

Features of Our Symbolic Model

- Comparing with the method of ProVerif

	ProVerif	ASV
Handling primitives	Shared and public key encryption, signatures, one-way hash functions, and DH key agreements	
Running environment	Unbounded number of sessions of the protocol	
termination	Protocols that satisfy sufficient condition	
Reconstruction of attack	enable	

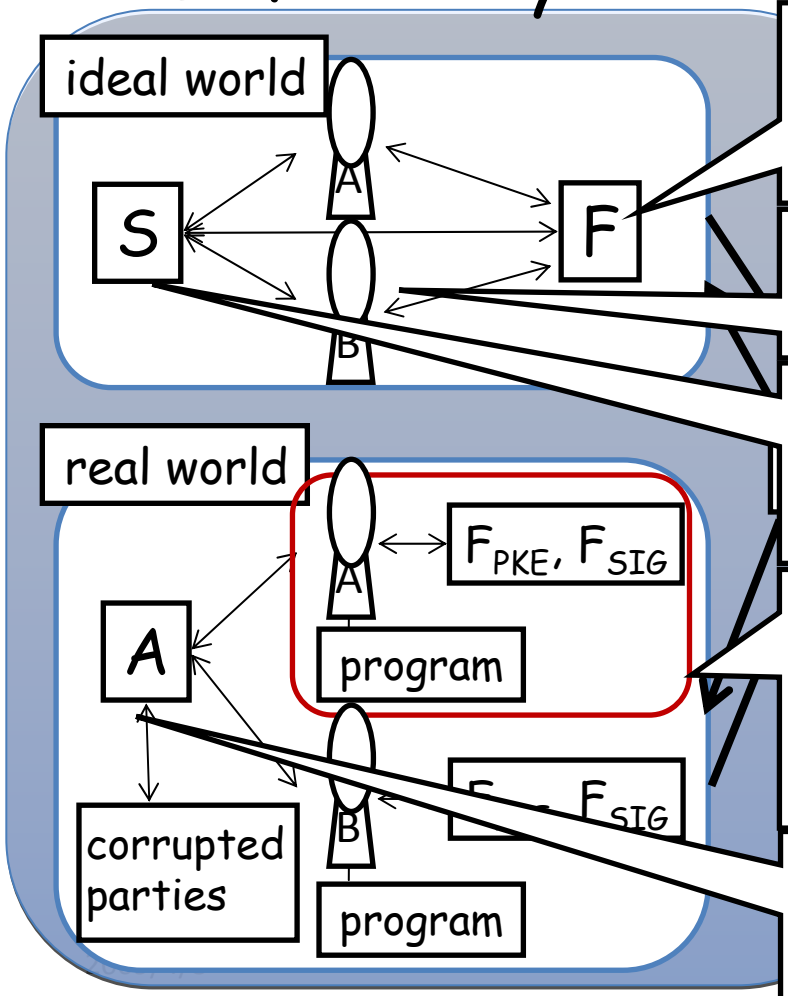
Application to showing the computational soundness	UC security [Canneti-Herzog,04],[Patil, 05], [Muratani-Hanatani, 06] Zero-knowledge proofs [Backes-Unruh,08] Observational equivalence [Comon-Lundh-Cortier,08]	UC security [Suzuki et al.,SCIS09], [Suzuki et al.,FAIS09]

Outline

- Background
- UC framework and previous verification
- Our symbolic model and results
- Conclusion and future works

UC Framework
Model (1/2)

- Defined by two world and environment



Ideal functionality
- describe a cryptographic task as an incorruptible trusted party

Dummy party
- only interact with the ideal functionality

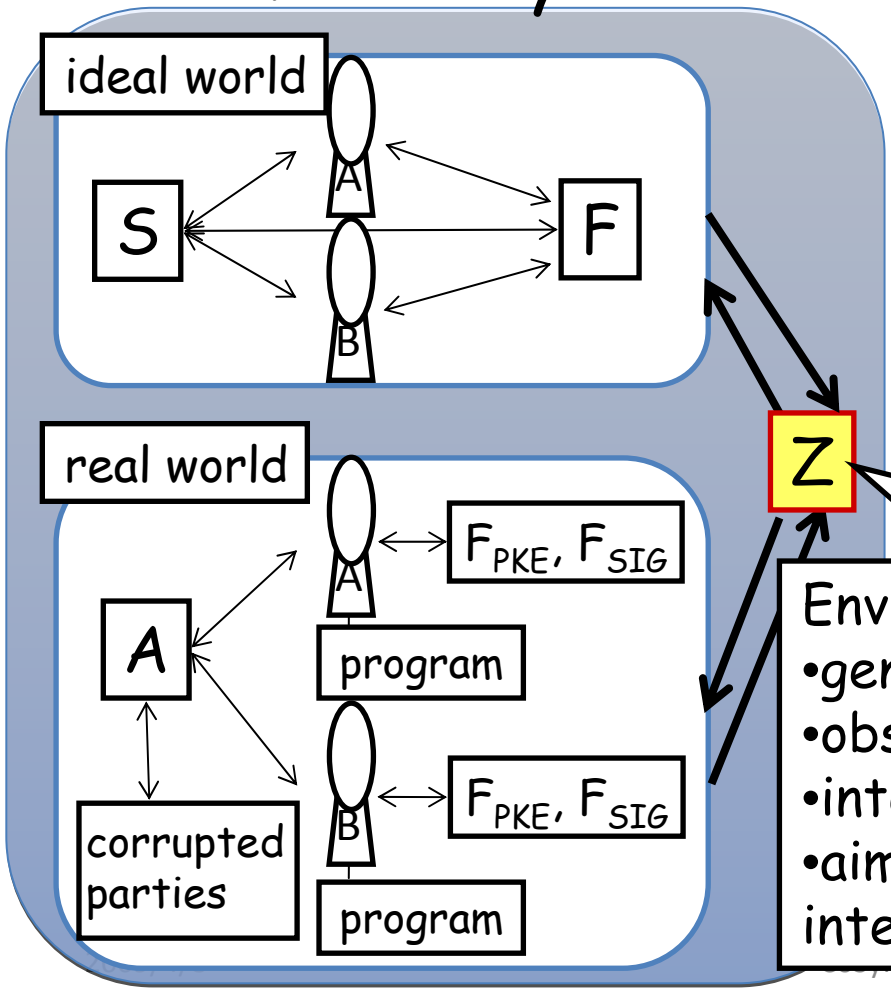
Adversary (Simulator, S)
- manipulate the adversary and parties in the real world

Party
- run program in a network
- have party ID(PID) and session ID(SID)
- can call ideal functionalities

Adversary (A)
- control the interaction between parties, and the internal actions of the corrupted parties

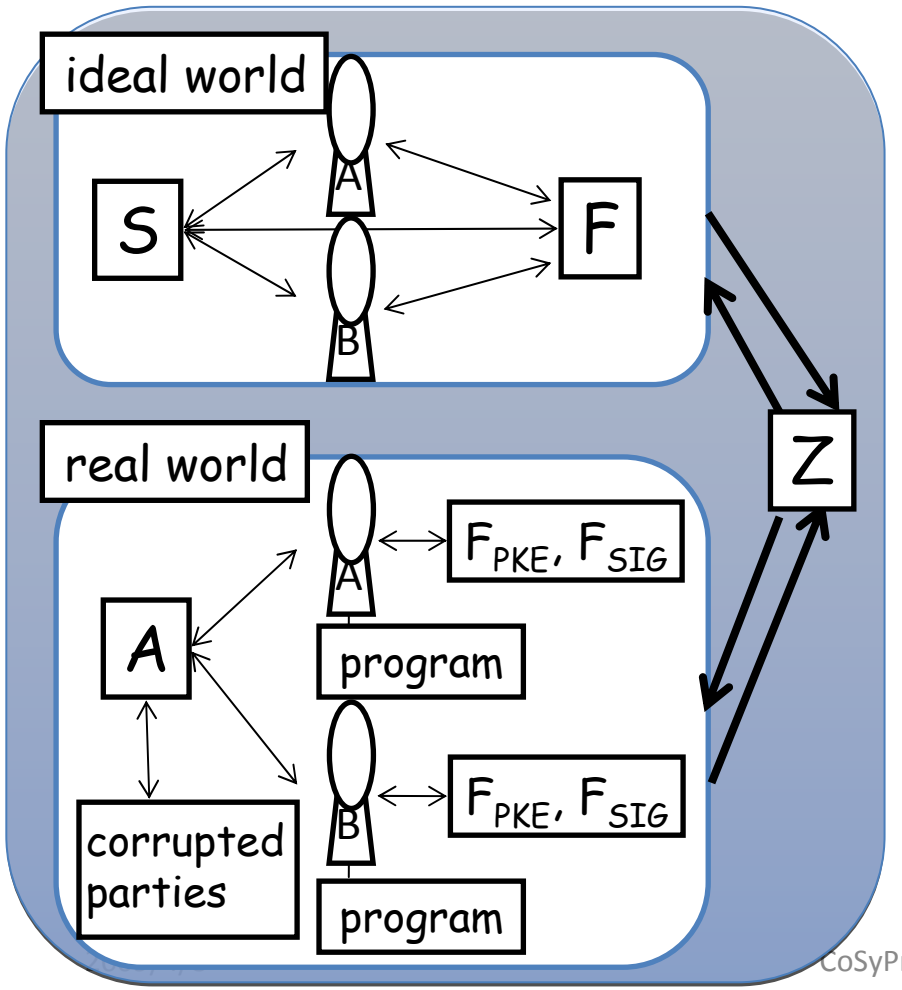
UC Framework
Model (2/2)

- Defined by two world and environment



Environment (Z)
- generate the inputs to all parties
- observes all outputs of parties
- interact with adversary
- aim to distinguish whether it is interacting with A or S

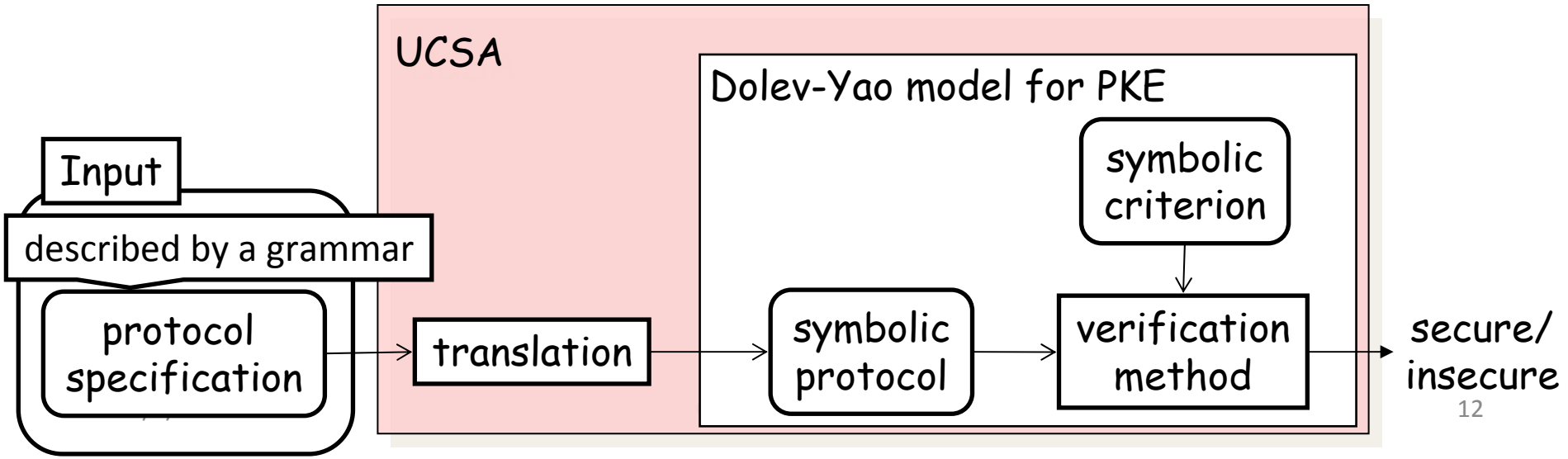
UC Framework
Security Definition



- Protocol is said to be UC secure if
  ∀ adversary.
  ∃ simulator.
  ∀ environment.
  probability that the environment can distinguish weather it is interacting with the adversary or the simulator on any input is negligible

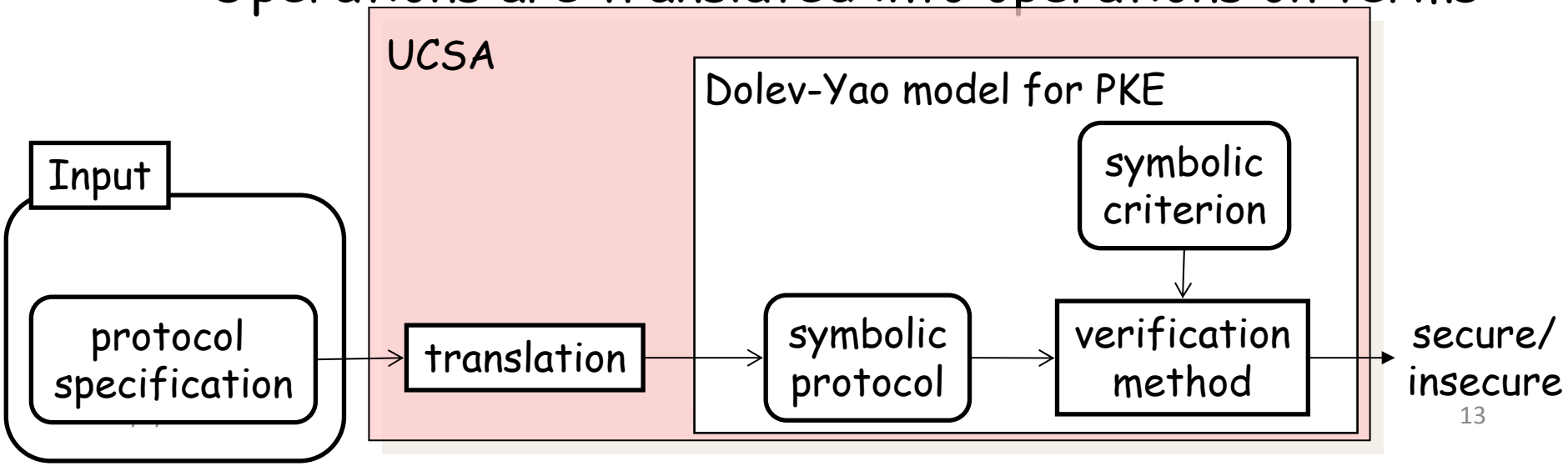
Results in [Canetti-Herzog, 04]

- Proposed the grammar of protocol specification
  - Concentrated on MA and KE protocols that use PKE
- Presented translation from concrete protocol into symbolic protocol in the Dolev-Yao model
- Provided symbolic criteria for MA and KE
  - Symbolic criterion for MA is similar to the traditional criterion
  - Symbolic criterion for KE is a new adequate criterion
- Proved the soundness the symbolic criterion
  - Protocol is UC secure if corresponding protocol is symbolically secure



Basic Idea of Translation

- From concrete protocol specification into symbolic protocol
  - Values are translated into a symbol (Dolev-Yao term)
  - Call of ideal functionalities are translated into symbolic primitives defined in advance
  - Operations are translated into operations on terms



Outline

- Background
- UC framework and previous framework
- Our symbolic model and results
- Conclusion and future works

Previous Work in Our Group

'82 First symbolic verification for specific protocols

Dolev-Yao model [Dolev-Yao,83]

'85 Proposal of symbolic model

- aim to verify secrecy

'88 Extension of the model

- allow to verification of unforgeability, but restrict functions to a single argument

'97 Extension of the model

- include polyad functions

computational soundness of formal encryption [Abadi-Rogaway,00]

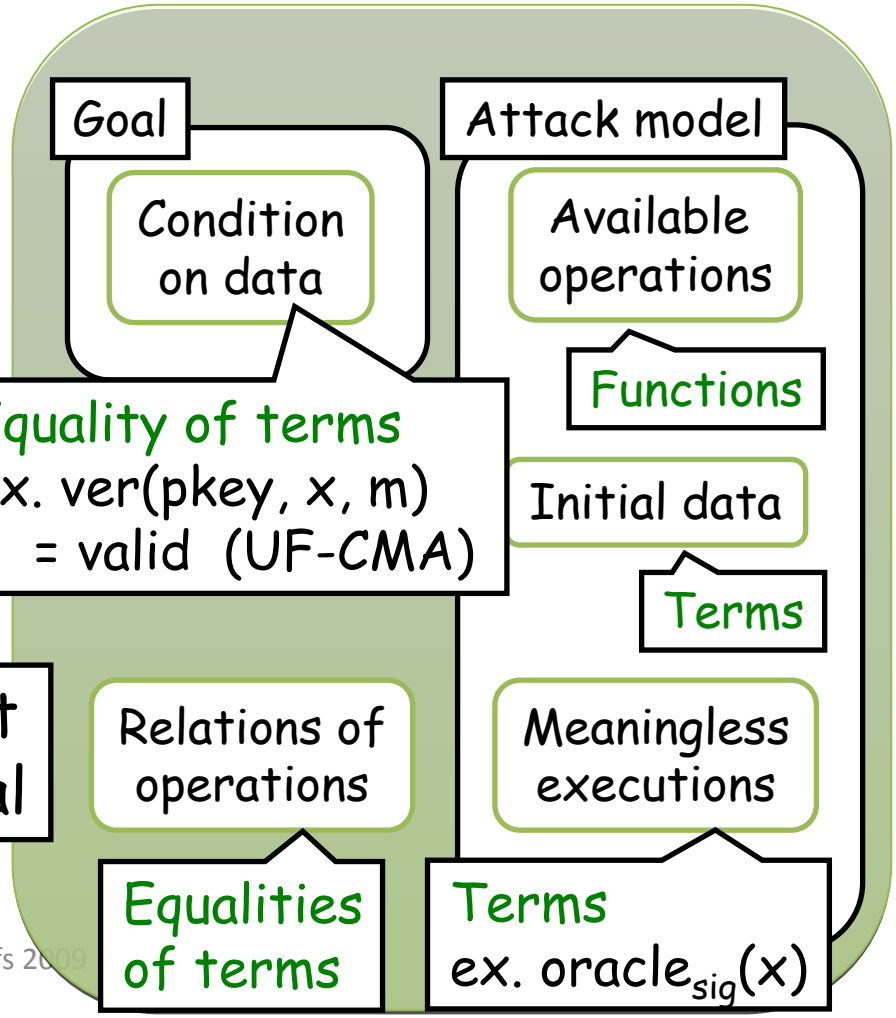
'03 Application to secure information flow

'04 Proposal of algorithm to reconstruct attack

'09 Application to verifying UC security

Our Symbolic Model
Protocol Specification

- Operations : function symbols
  - ex. sig, ver, $oracle_{sig}$, pkey, skey, m
- Data : terms
  - ex. sig (skey, m)
- Relations between operations : axioms (equalities of terms)
  - ex. ver(pkey, sig(skey, x), x) = valid, $oracle_{sig}(x)$ = sig(skey, x)
- Similar to classic security notion
  - Attack model and adversary's goal (ex. UF-CMA, OW-CCA)

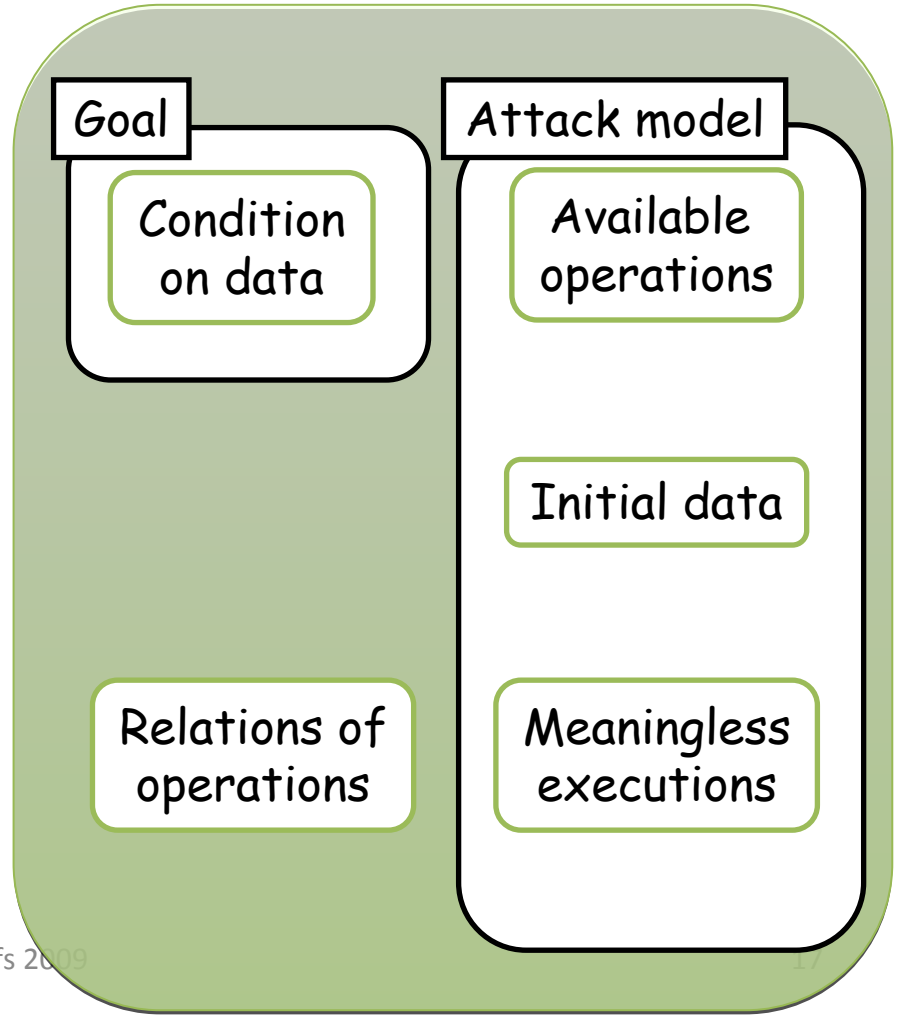


Adversary aims to construct a term that satisfies his goal

goal term

Our Symbolic Model
Security Definition

- Protocol is said to be axiomatically secure if a goal term is included in the set of terms that adversary can construct by executing operations on the initial data without doing any meaningless executions



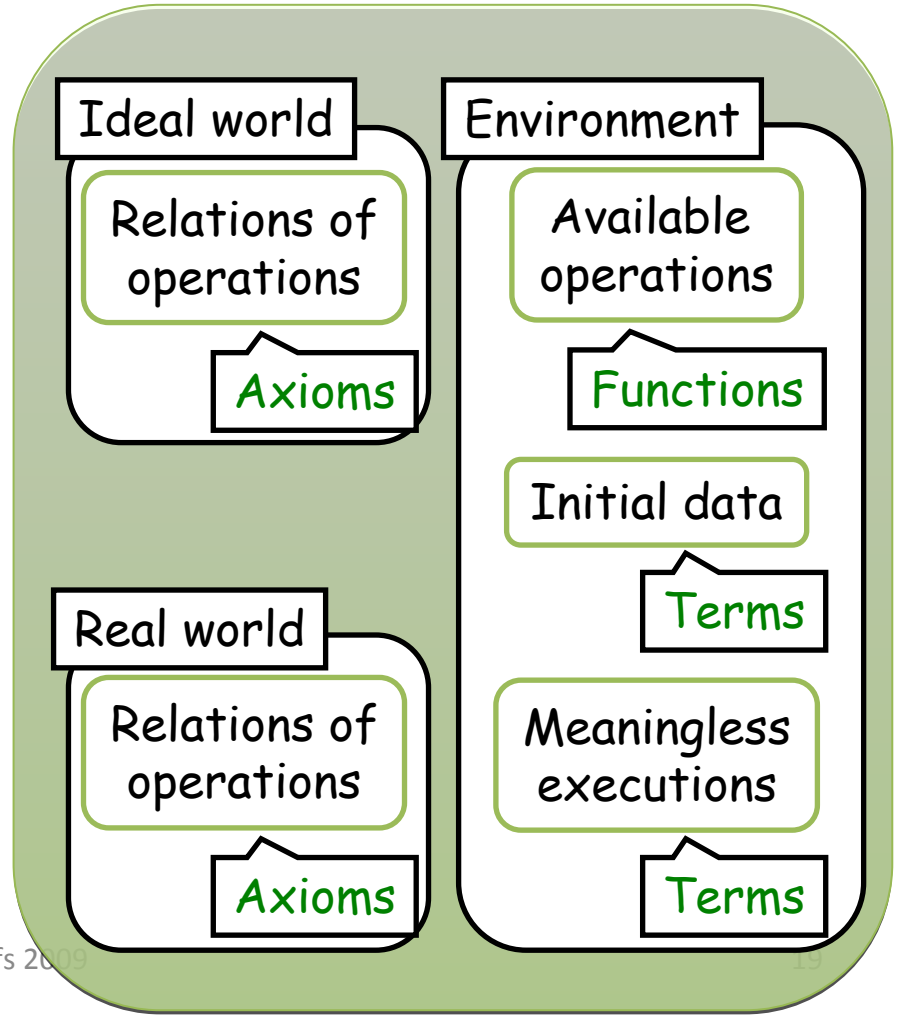
Use of Our Symbolic Model in UCSA

- Need of corresponding translation and symbolic criterion

- Approach for MA protocols
  - Use the original model same as [Patil, 05]
- Approach for KE protocols
  - Extend our model in order to symbolically define notions in the UC framework
    - Symbolic environment, ideal world, and real world
    - Symbolic indistinguishability
  - Define symbolic criterion based on new symbolic notions
    - Similar criterion to previous one (real or random secrecy)

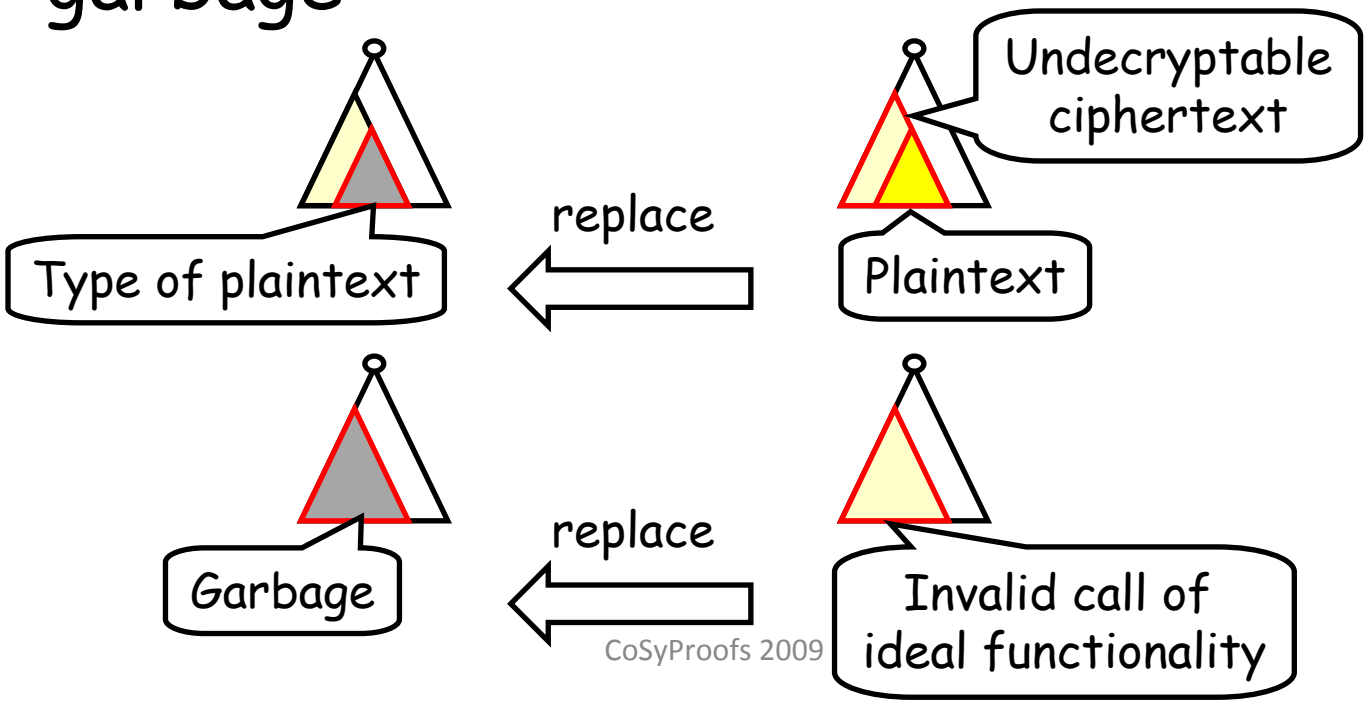
Symbolic Definition

- Environment
  - Defined by initial data, available operations, meaningless executions
- Ideal world and real world
  - Defined by relations between operations
- Environment's view
  - Defined for terms constructed by environment
- Indistinguishability
  - Environment's view of the interaction with real world is identical to its view of the interaction with ideal world



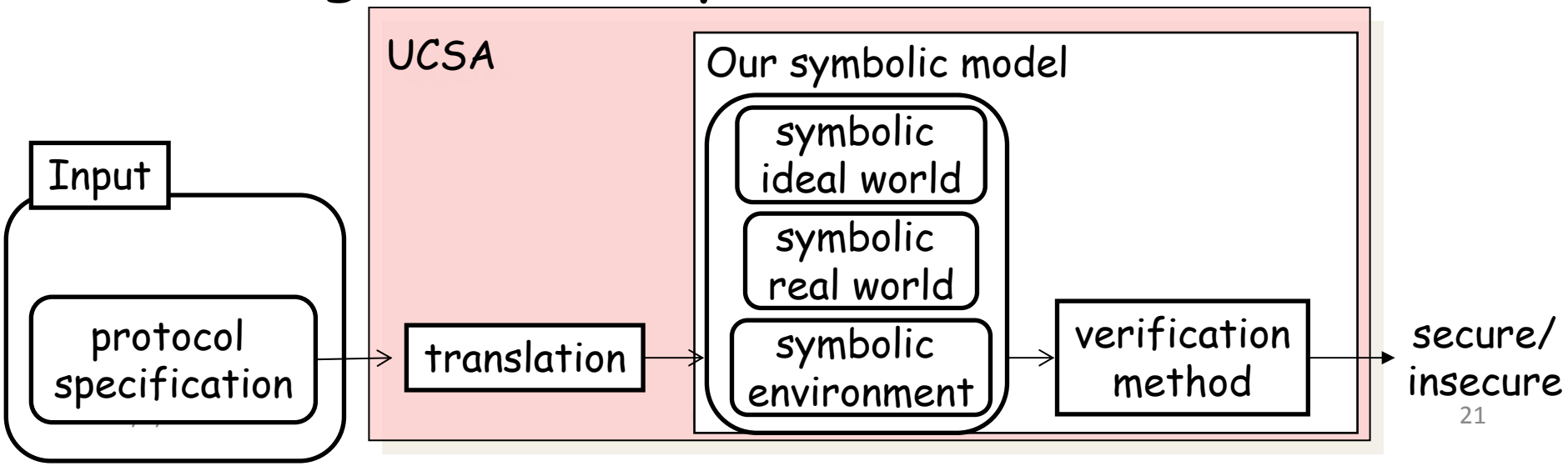
Environment's View

- Represent information that environment can deduce from a term
- Defined by terms replaced sub term with another term that represents type of data or garbage



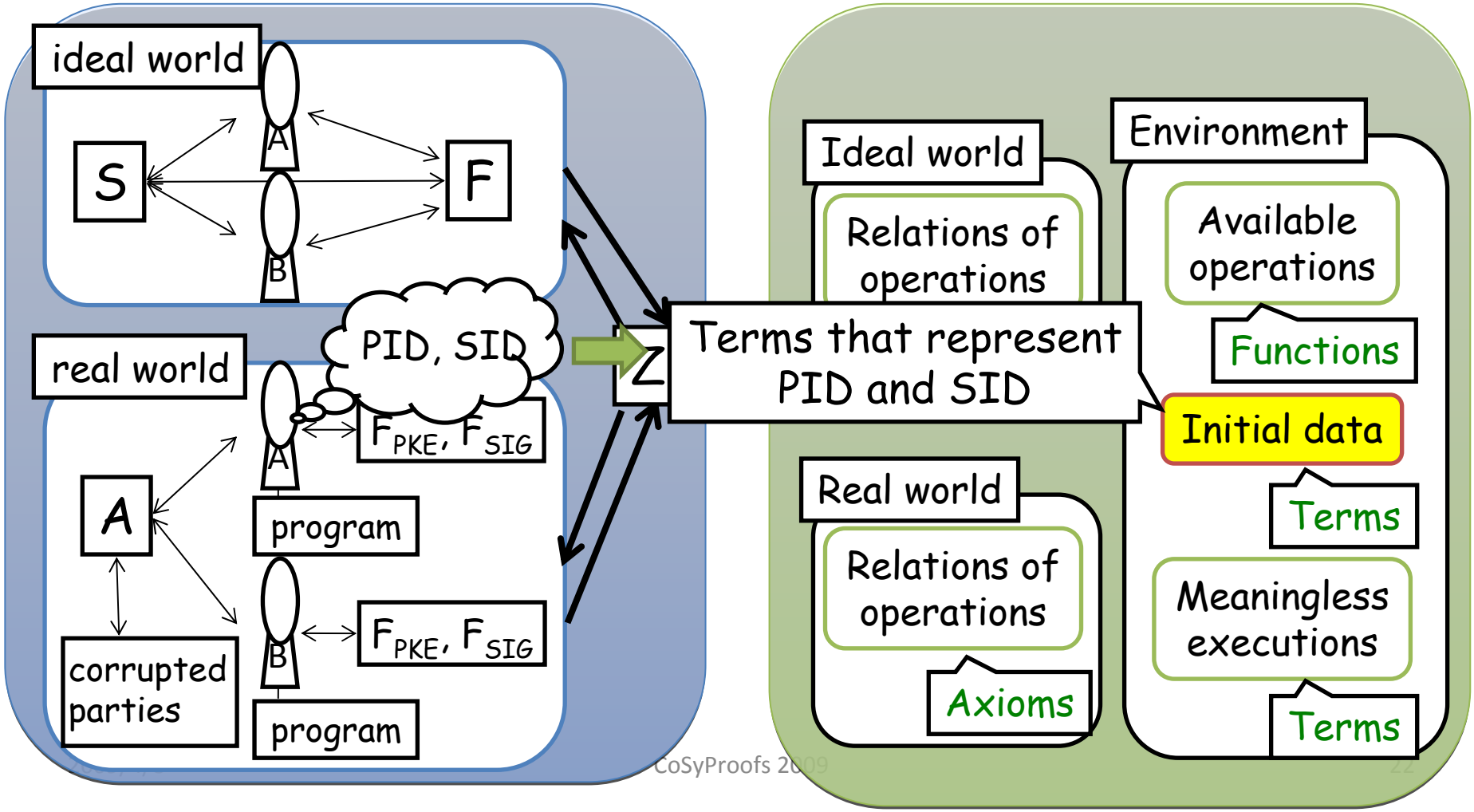
Overview of Verification for KE

- Translate concrete protocol into symbolic environment, symbolic real world, and real world
- Determine whether environment can distinguish two symbolic world



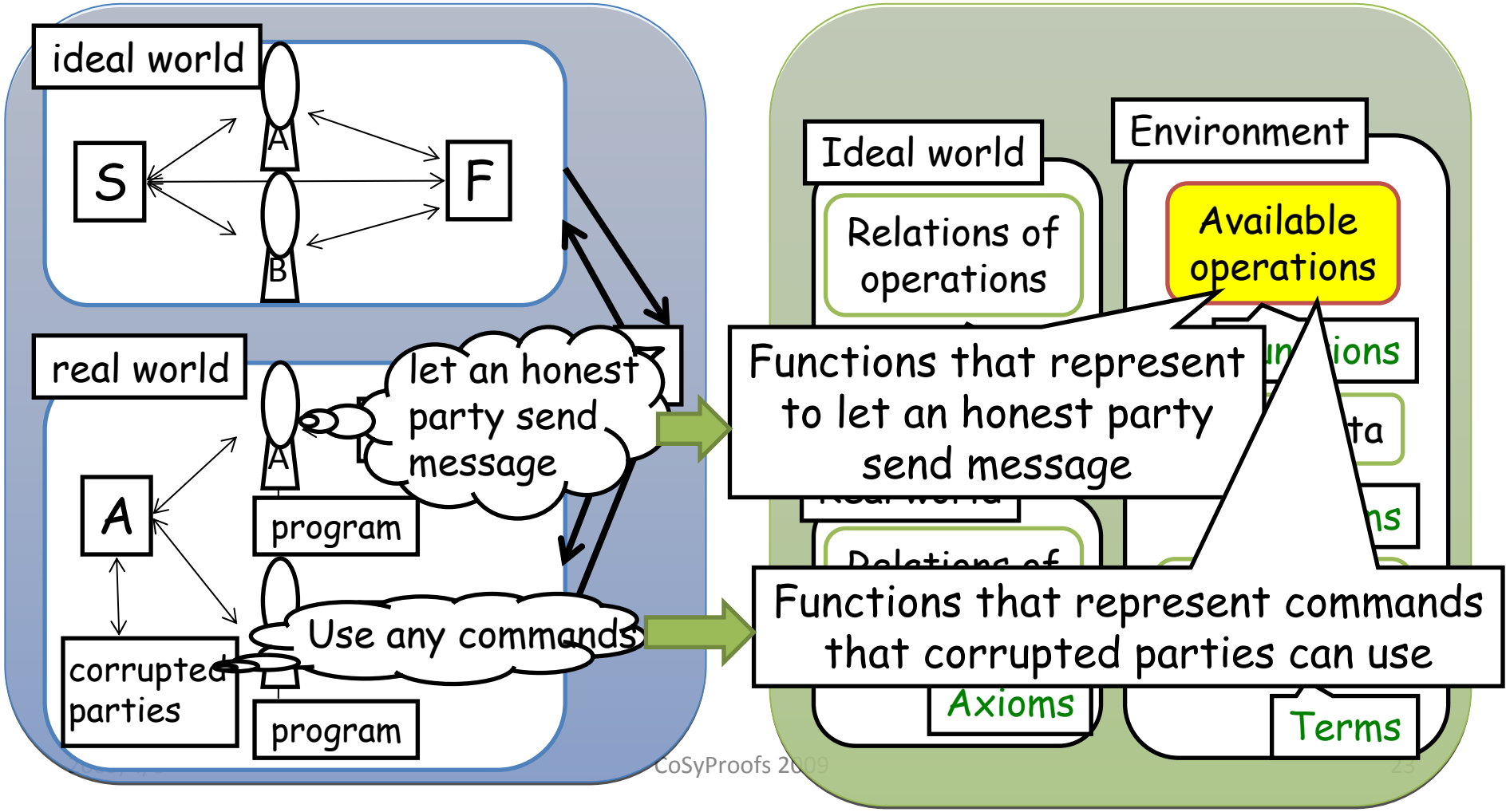
Basic Idea of Translation (1/2)

- Initial data, available operations and meaningless executions



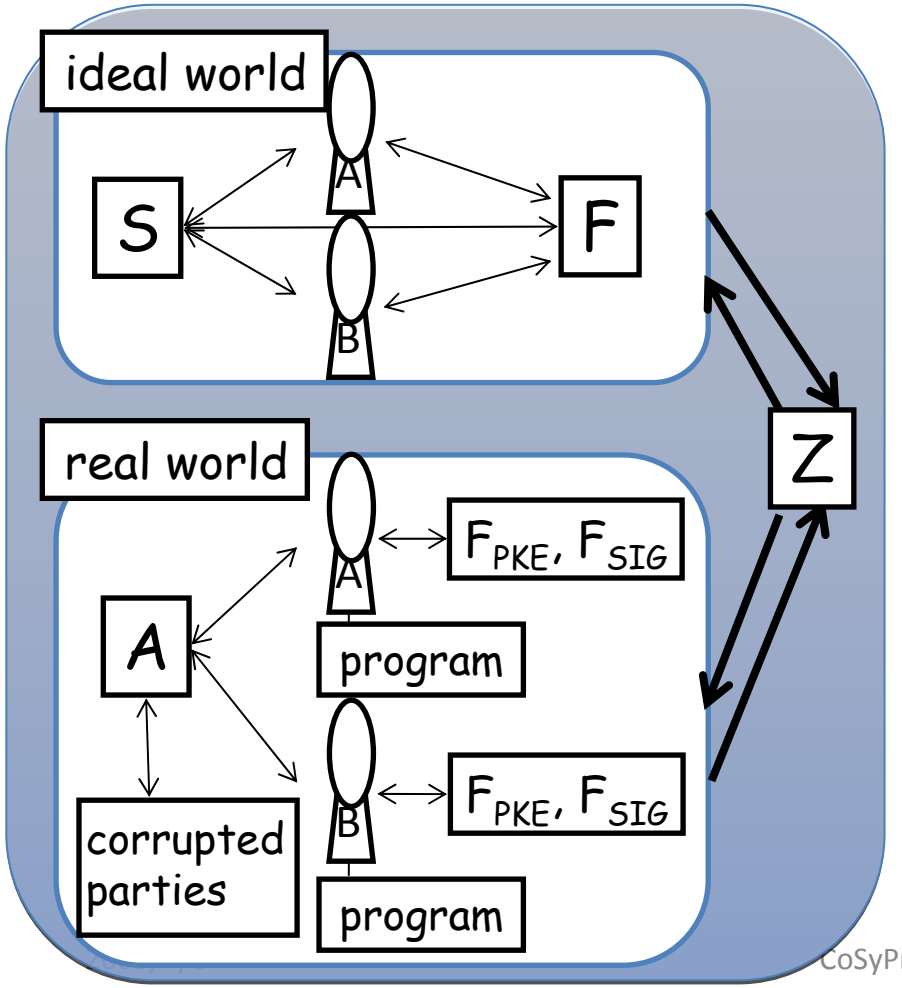
Basic Idea of Translation (1/2)

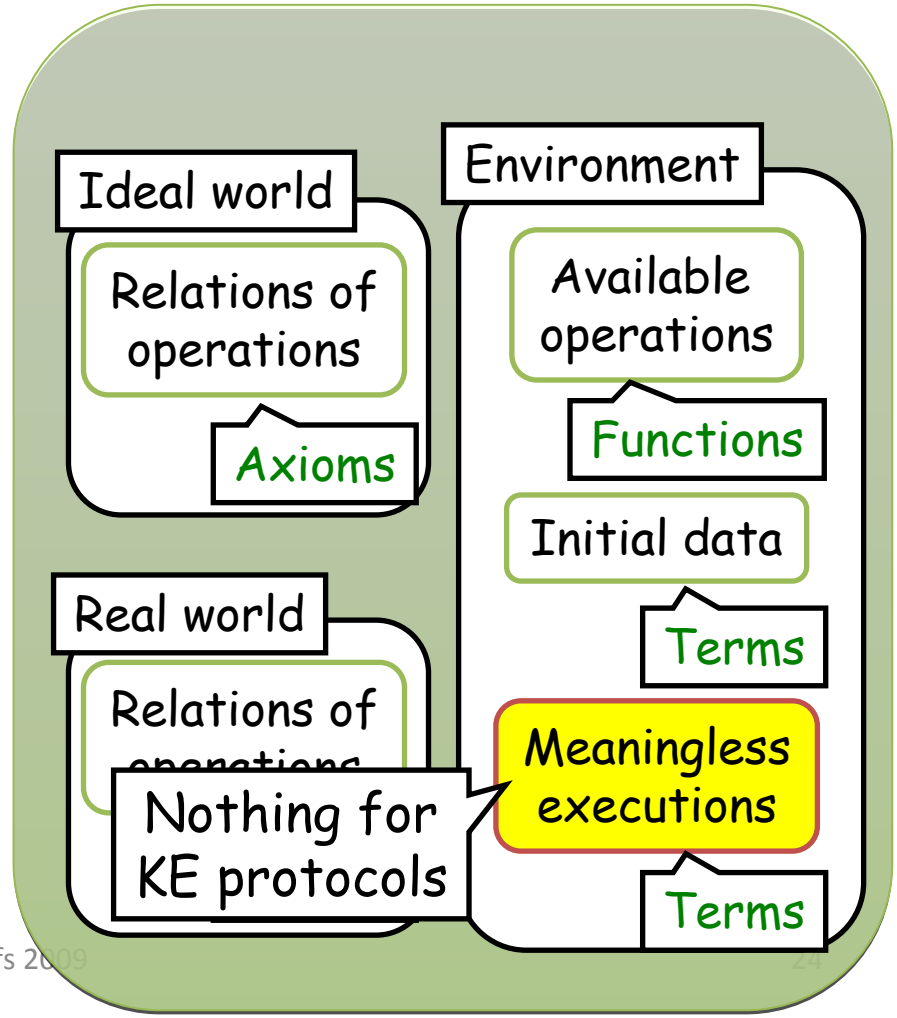
- Initial data, available operations and meaningless executions



Basic Idea of Translation (1/2)

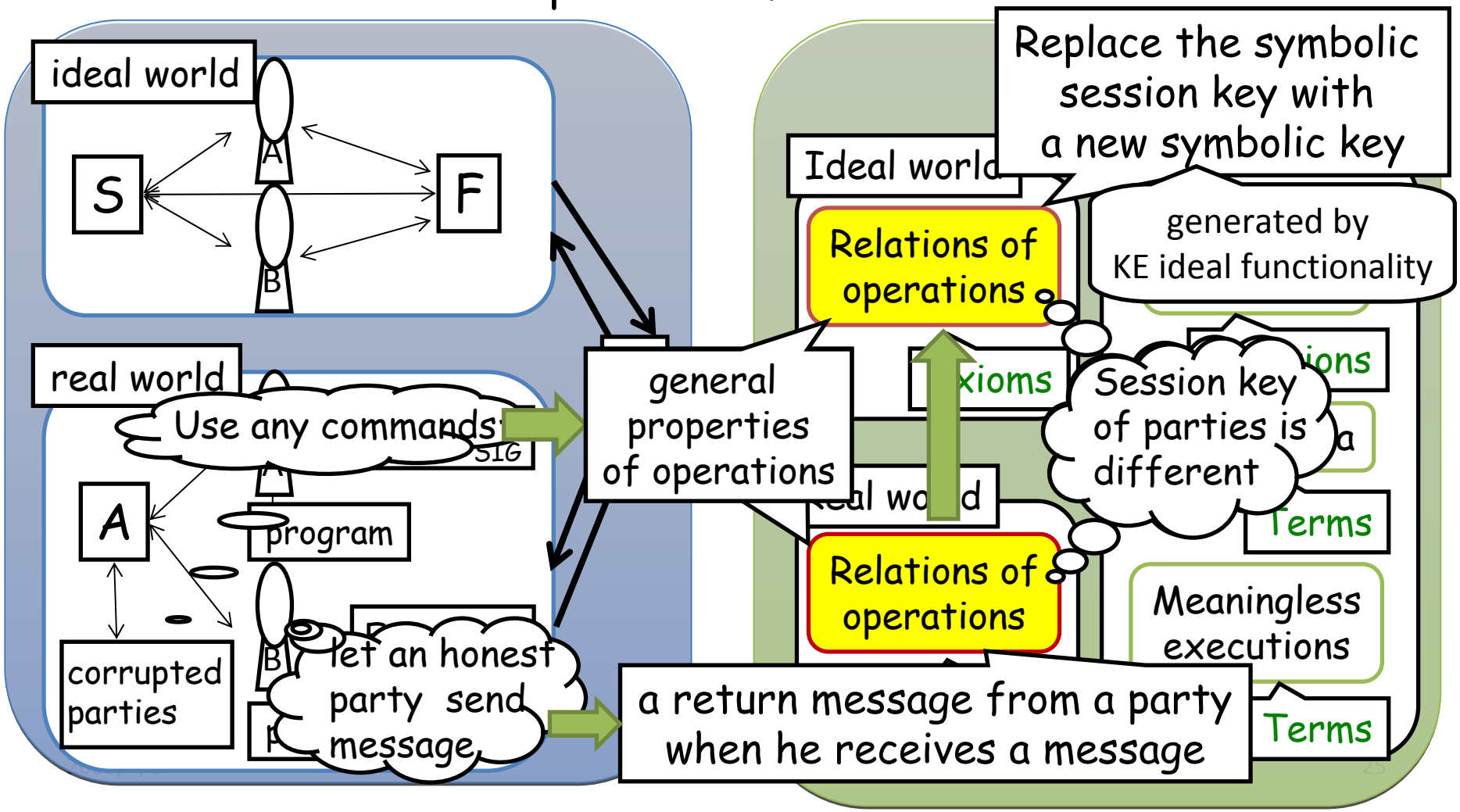
- Initial data, available operations and meaningless executions





Basic Idea of Translation (2/2)

- Relations between operations for real world and ideal world



Conclusion

- Propose UCSA based on our symbolic model
  - Concentrate on MA and KE protocols that use PKE and SIG
  - For MA, same approach to previous work
  - For KE, expand our symbolic model to symbolically define notions in UC framework
- Future work
  - Widen the range of verifiable protocols
  - Provide algorithm to generate symbolic ideal world from specification of ideal functionality
    - Need of grammar for ideal functionality ?

References (1/2)

- [Abadi-Rogaway,00] M. Abadi and P. Rogaway, ``Reconciling Two Views of Cryptography (the Computational Soundness of Formal Encryption),'' IFIP TCS 2000, LNCS vol.1872, pp.3-22, 2000.
- [Backes et al.,08] M. Backes, M. Maffei, and D. Unruh, ``Zero-Knowledge in the Applied Pi-calculus and Automated Verification of the Direct Anonymous Attestation Protocol,'' In Proc. of 29th IEEE Symp. on Security and Privacy (S&P 2008), pp.202-215, 2008.
- [Canetti-Herzog, 04] R. Canetti and J. Herzog, ``Universally Composable Symbolic Analysis of Cryptographic Protocols (The Case of Encryption-Based Mutual Authentication and Key Exchange),'' IACR Cryptology ePrint Archive, Report 2004/334, 2004.
- [Comon-Lundh-Cortier.,08] H. Common-Lundh and V. Cortier, ``Computational soundness of observational equivalence,'' In Proc. of 15th ACM conf. on Computer and communications security, pp.109-118, 2008.
- [Dolev-Yao,83] D. Dolev and A .C. Yao, ``On the Security of Public-Key Protocols,'' IEEE Trans. Info. Theory, vol.29, pp.198-208, 1983.

References (2/2)

- [Muratani-Hanatani, 06] H. Muratani, Y. Hanatani, ``Computationally Sound Symbolic Criteria for UC-secure Multi-Party Mutual Authentication and Key Exchange Protocols,'' IEICE Tech. Rep., ISEC06-150, vol.106, no.597, pp.59-64, 2007 (in Japanese).
- [Patil, 05] A. Patil, ``On Symbolic Analysis of Cryptographic Protocols.'' Master's Thesis, Massachusetts Institute of Technology, 2005.
- [Suzuki et al.,SCIS09] I. Suzuki, M. Yoshida, and T. Fujiwara, ``Formal Method for Universally Composable Security Analysis of Mutual Authentication,'' SCIS 2009, 4C2-4, 2009 (in Japanese).
- [Suzuki et al.,SCIS09] I. Suzuki, M. Yoshida, and T. Fujiwara, `` Formal Verification for Universally Composable Key Agreement, '' FAIS 2009 (oral presentation).