A Constraint-Based Algorithm for Contract-Signing Protocols

Detlef Kähler

Kiel University

Joint work with Ralf Küsters

Overview

- Introduction / Motivation
- Formal model / Problem
- Constraint solving / Algorithm
- Conclusion

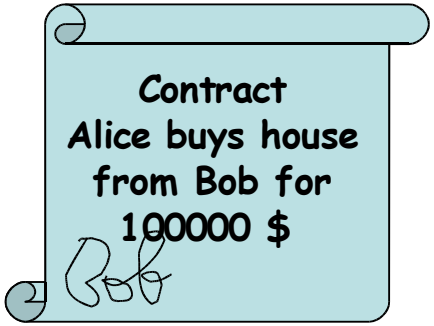
Contract signing

Example: Alice wants to buy a house from Bob

1) Parties agree upon contractual text
2) Both parties sign a copy
3) Parties exchange signed copies simultaneously

Alice

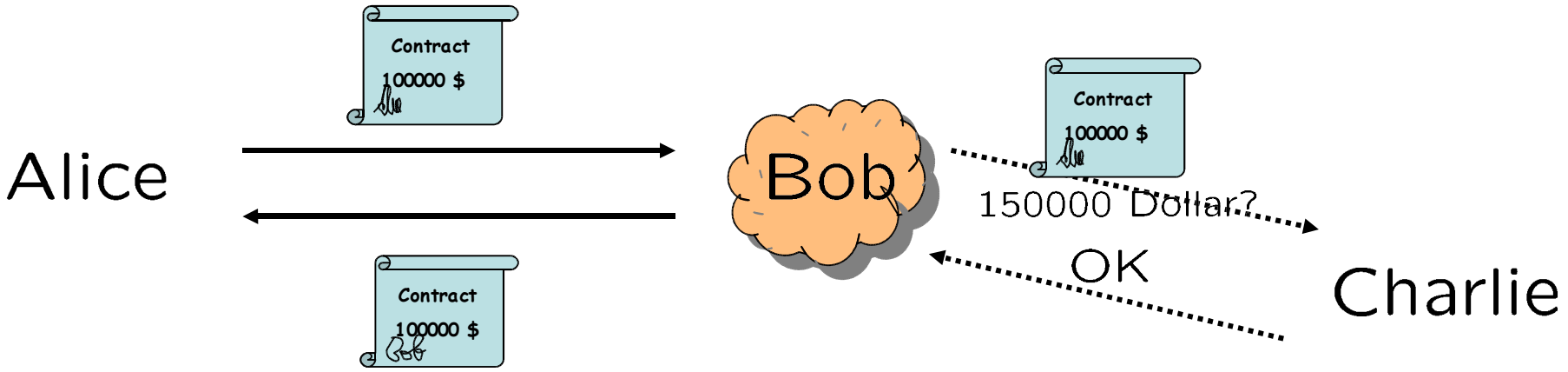
Bob



Contract signing over a network

How to do the exchange of signed copies?

Naïve approach

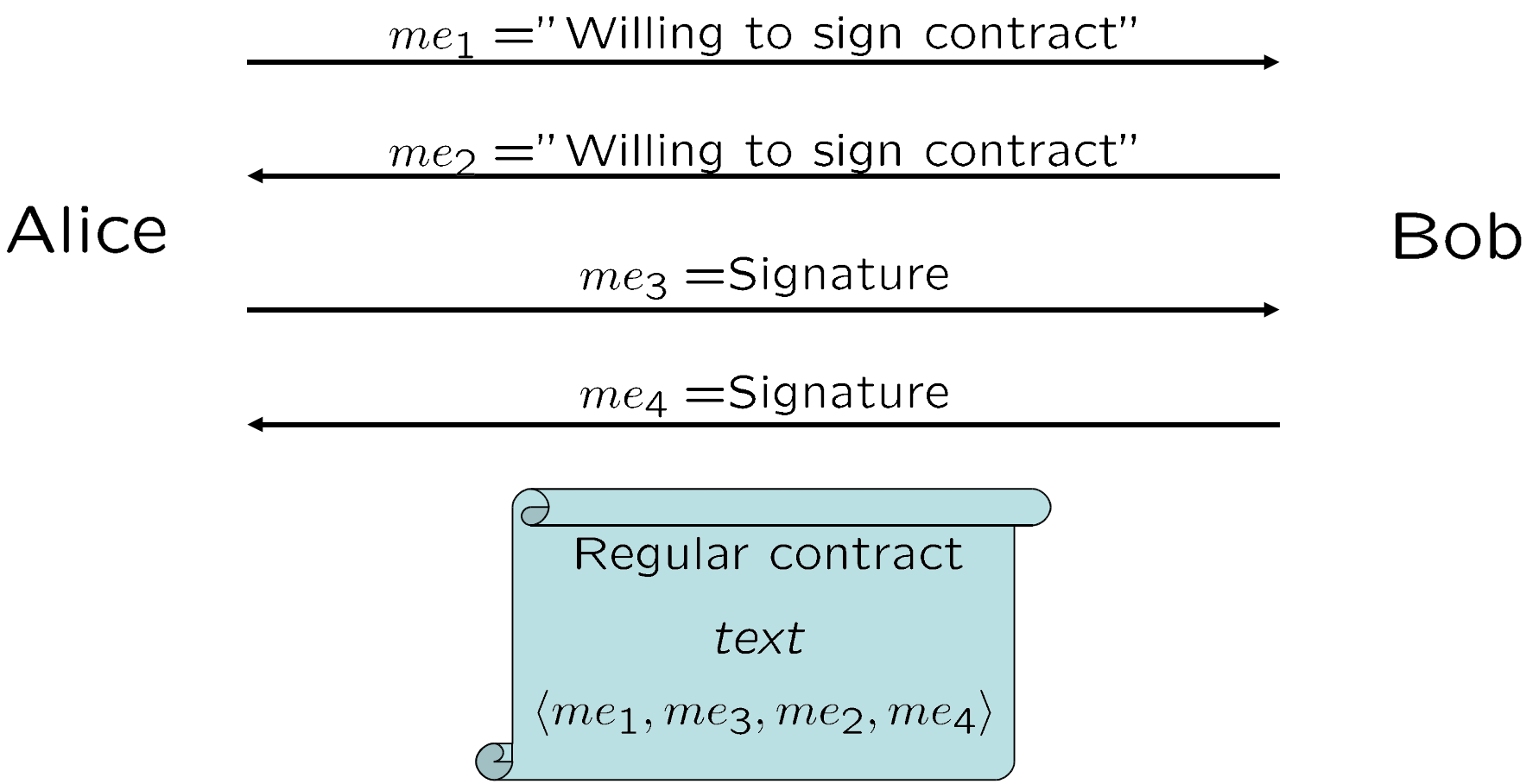


A contract-signing protocol is balanced for Alice if at no stage of the protocol execution Bob has both

- a strategy to obtain a valid contract, and
- a strategy to prevent Alice from getting a valid contract.

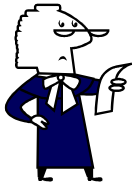
ASW-protocol

ASW-protocol: Optimistic two party contract-signing protocol



ASW-protocol

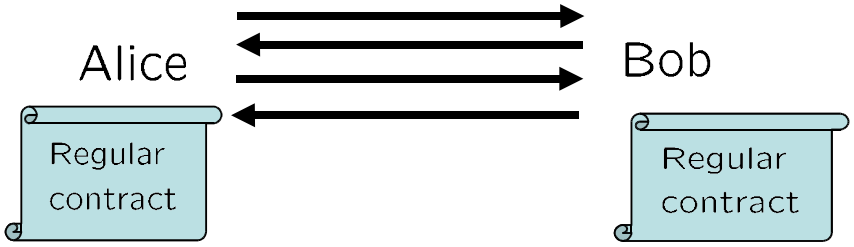
Abort subprotocol



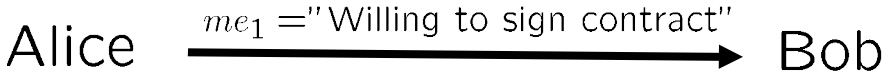
Alice $\xrightarrow{me_1 = \text{"Willing to sign contract"}}$ Bob

ASW-protocol

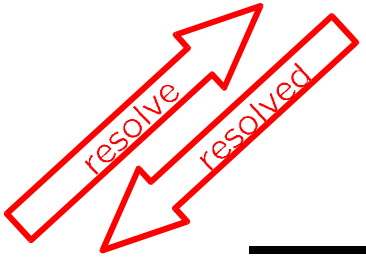
Main protocol

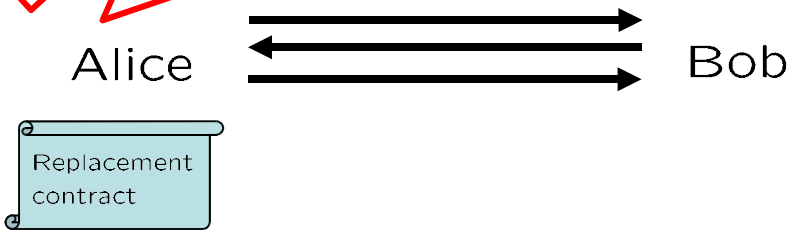


Abort subprotocol

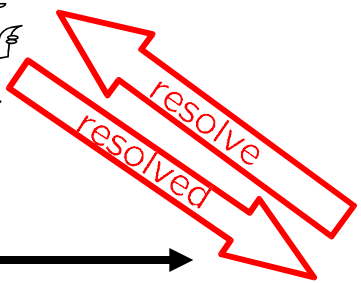


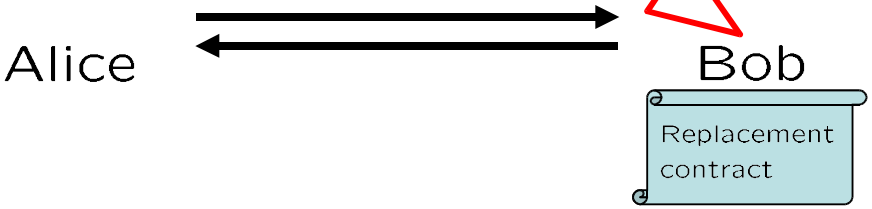
Resolve Subprotocol (Alice)



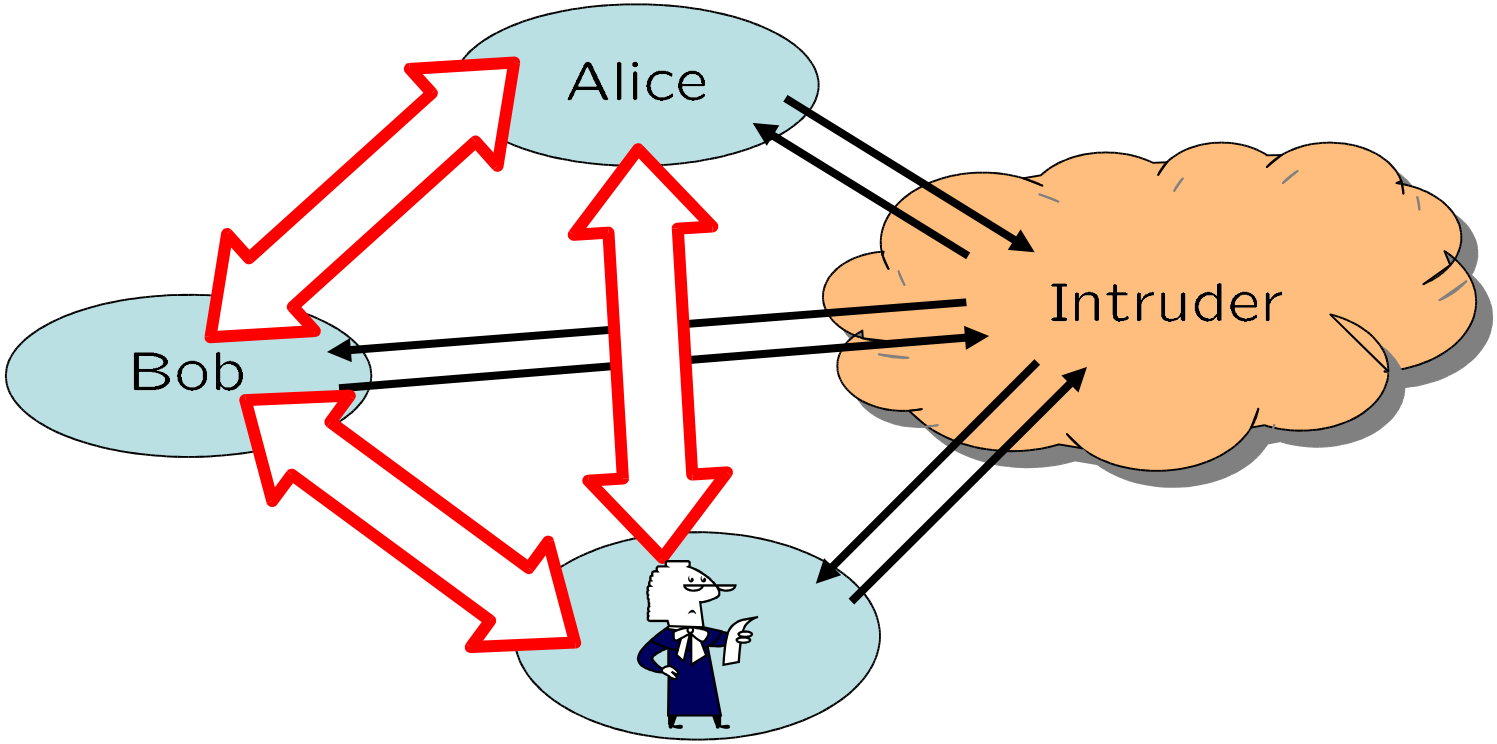


Resolve Subprotocol (Bob)





Communication model (extended Dolev-Yao)



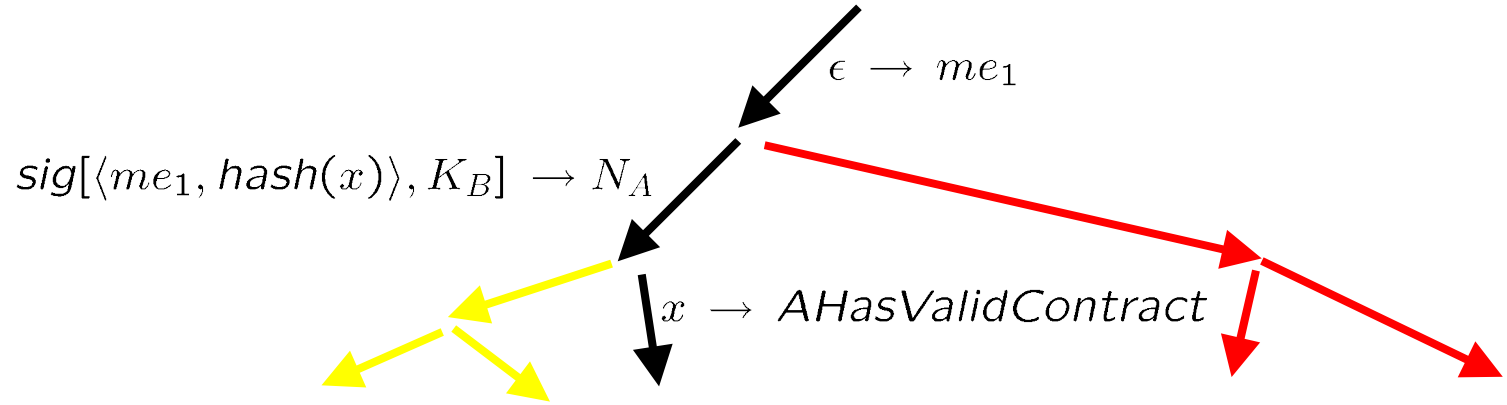
- The network is the intruder
- Secure channels

Finite-session model of a model proposed by Scedrov et al. [2001]

Formal model

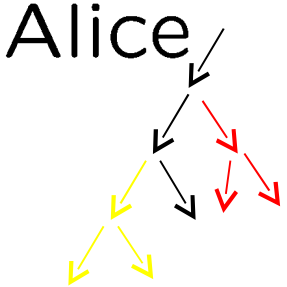
Participants are rule trees

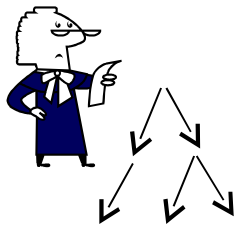
Alice (ASW-protocol) as rule tree $\prod_A$



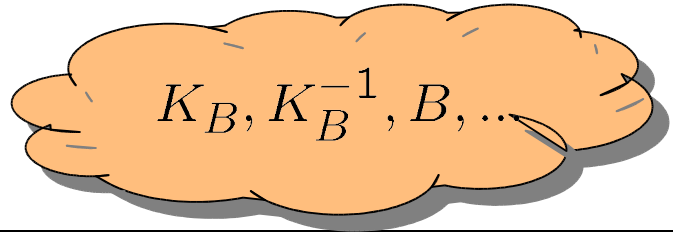
A protocol P consists of

a family of participants + initial intruder knowledge





$P = (\{\prod_i\}_i, K)$

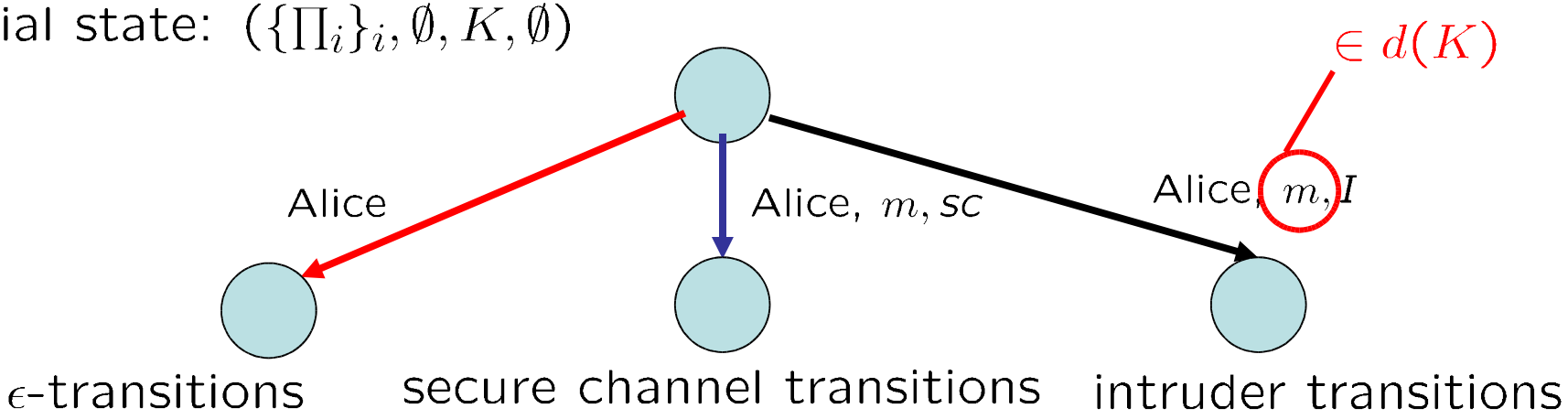


Protocol States

Given a protocol $P = (\{\prod_i\}_i, K)$.

State of protocol P: $(\{\prod'_i\}_i, \sigma, K', S)$

Initial state: $(\{\prod_i\}_i, \emptyset, K, \emptyset)$

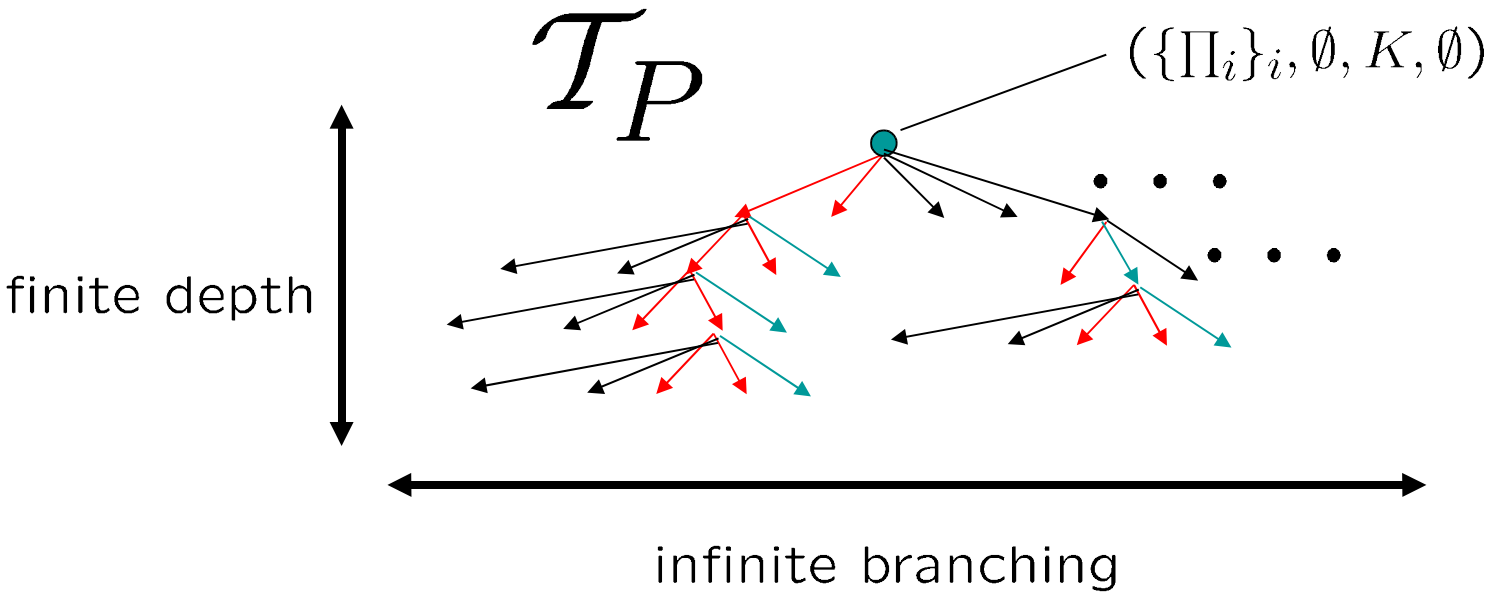


$d(K)$: set of messages constructable by the intruder

Transition tree

Given a protocol $P = (\{\prod_i\}_i, K)$.

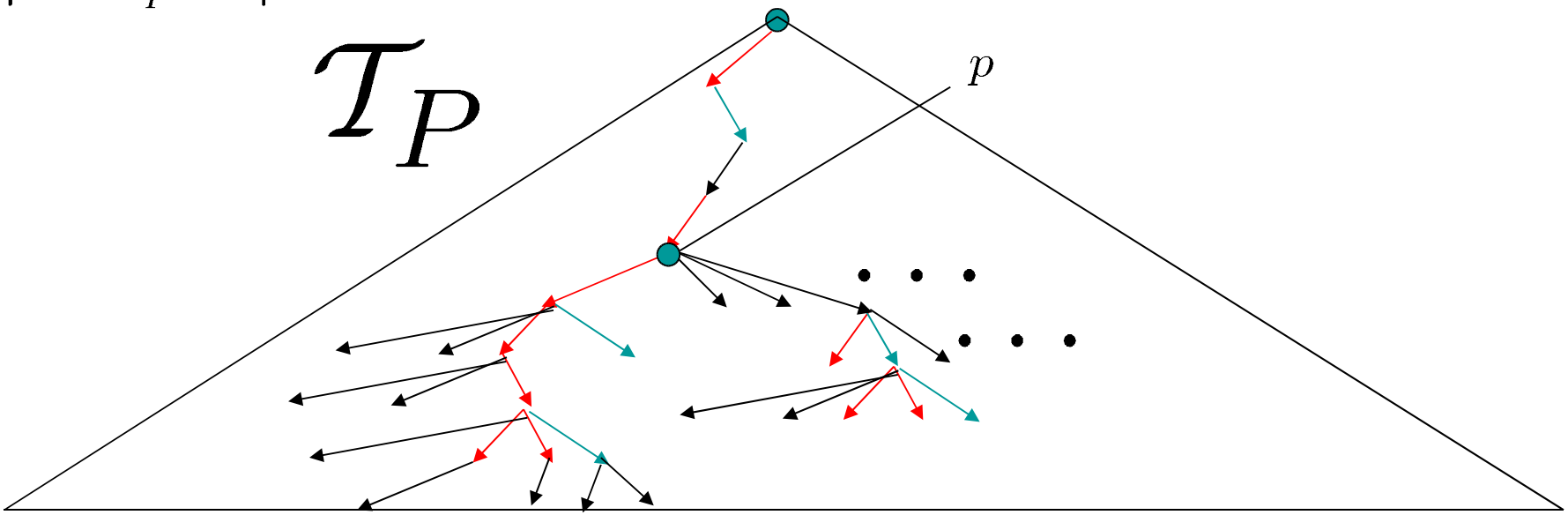
What is the execution of protocol P?



The set of runs can be thought of as a tree rooted at $(\{\prod_i\}_i, \emptyset, K, \emptyset)$

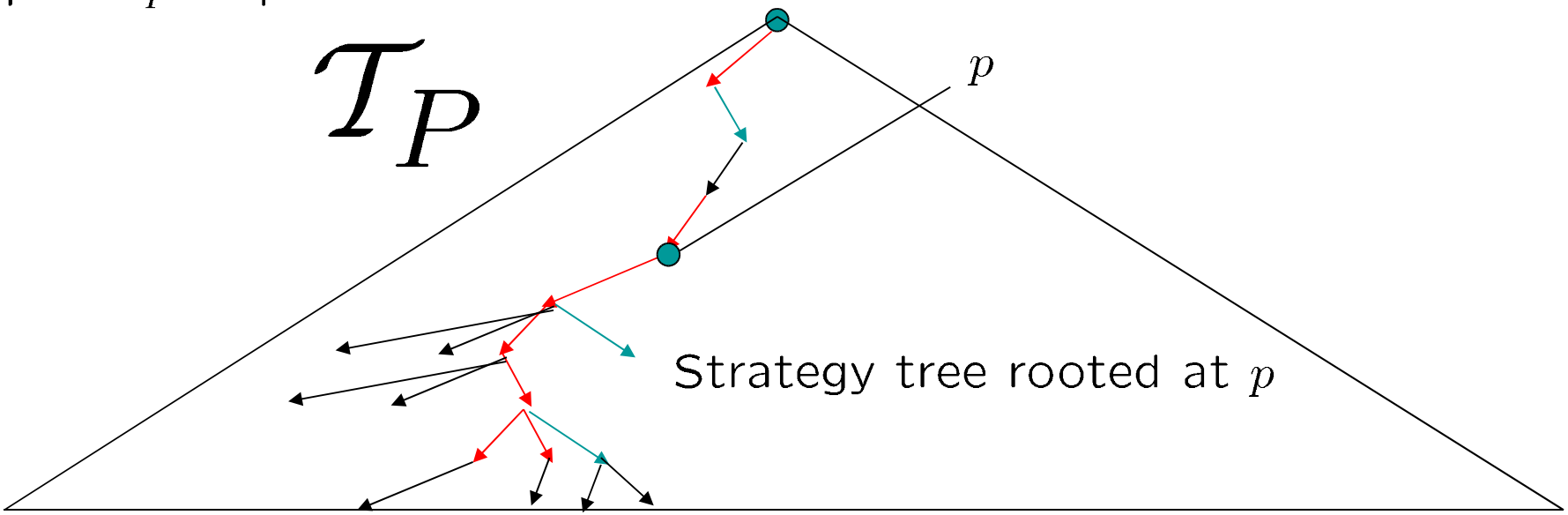
Intruder Strategies (1)

Balance talks about intruder strategies.
What is an intruder strategy at some point p of protocol execution?



Intruder Strategies (2)

Balance talks about intruder strategies.
What is an intruder strategy at some point p of protocol execution?



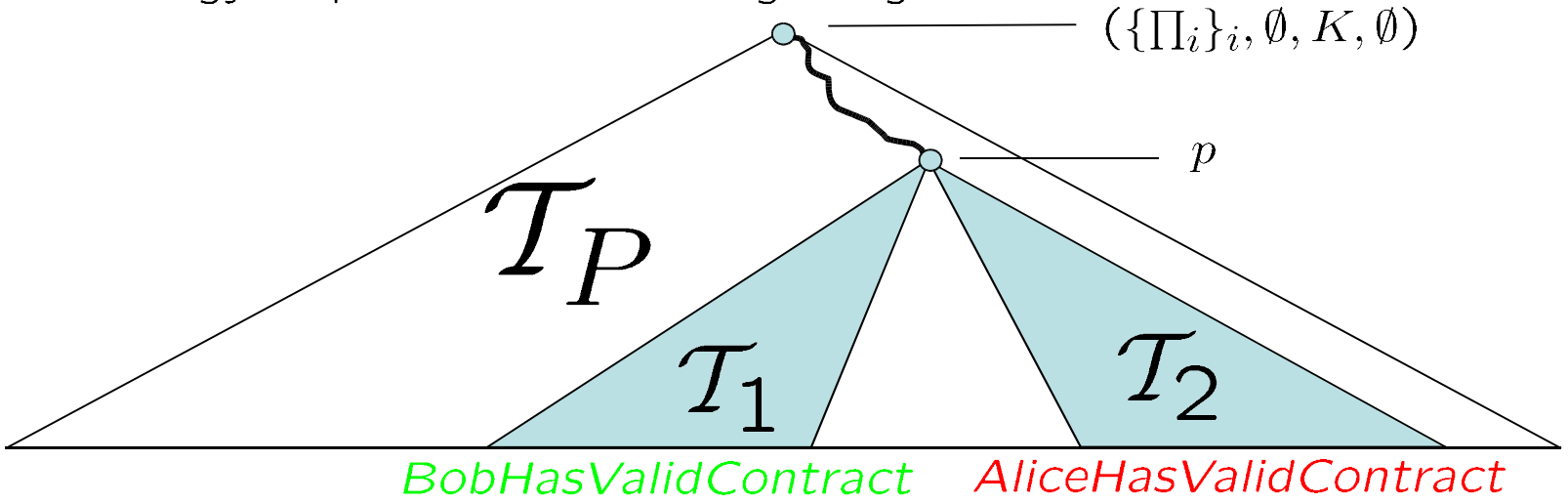
- Intruder may choose not to take some intruder transitions
- ε-transitions and secure channel transitions are not under control of the intruder

Strategy properties

How can we formulate game-theoretic security requirements?

A contract-signing protocol is unbalanced for Alice if
there exists a point in the protocol execution where Bob has both

- a strategy to obtain a valid contract, and
- a strategy to prevent Alice from getting a valid contract.



Problem:
Given a protocol P and a strategy property C
Is there a state $p \in \mathcal{T}_P$ that satisfies C?
Problem is decidable K., Küsters [2005]

Constraint solving

A constraint is of the form

$$m : T$$

where m is a term and T is a finite set of terms

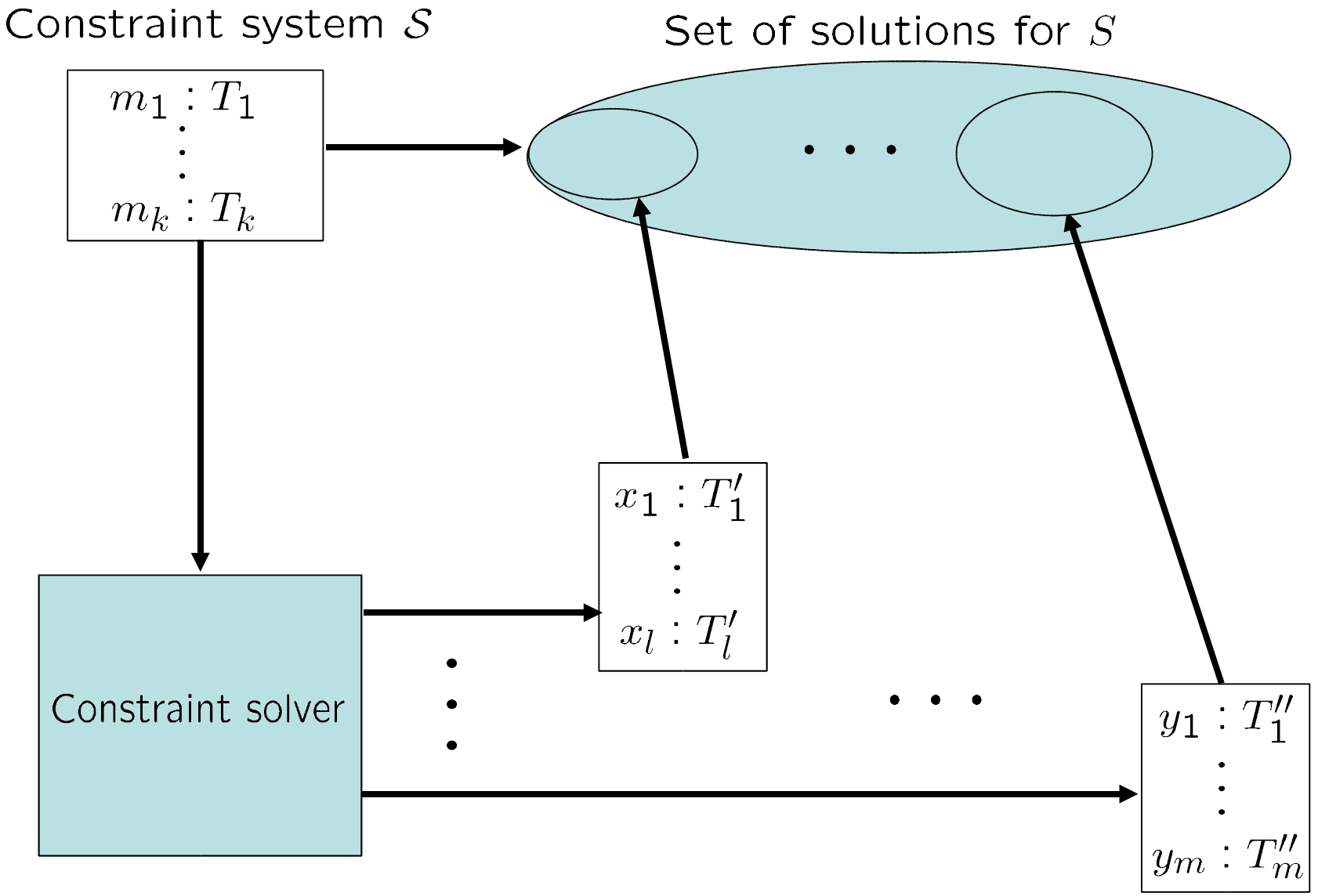
A constraint system is a sequence of constraints

$$\boxed{\begin{array}{l} m_1 : T_1 \\ m_2 : T_2 \\ \vdots \\ m_k : T_k \end{array}}$$

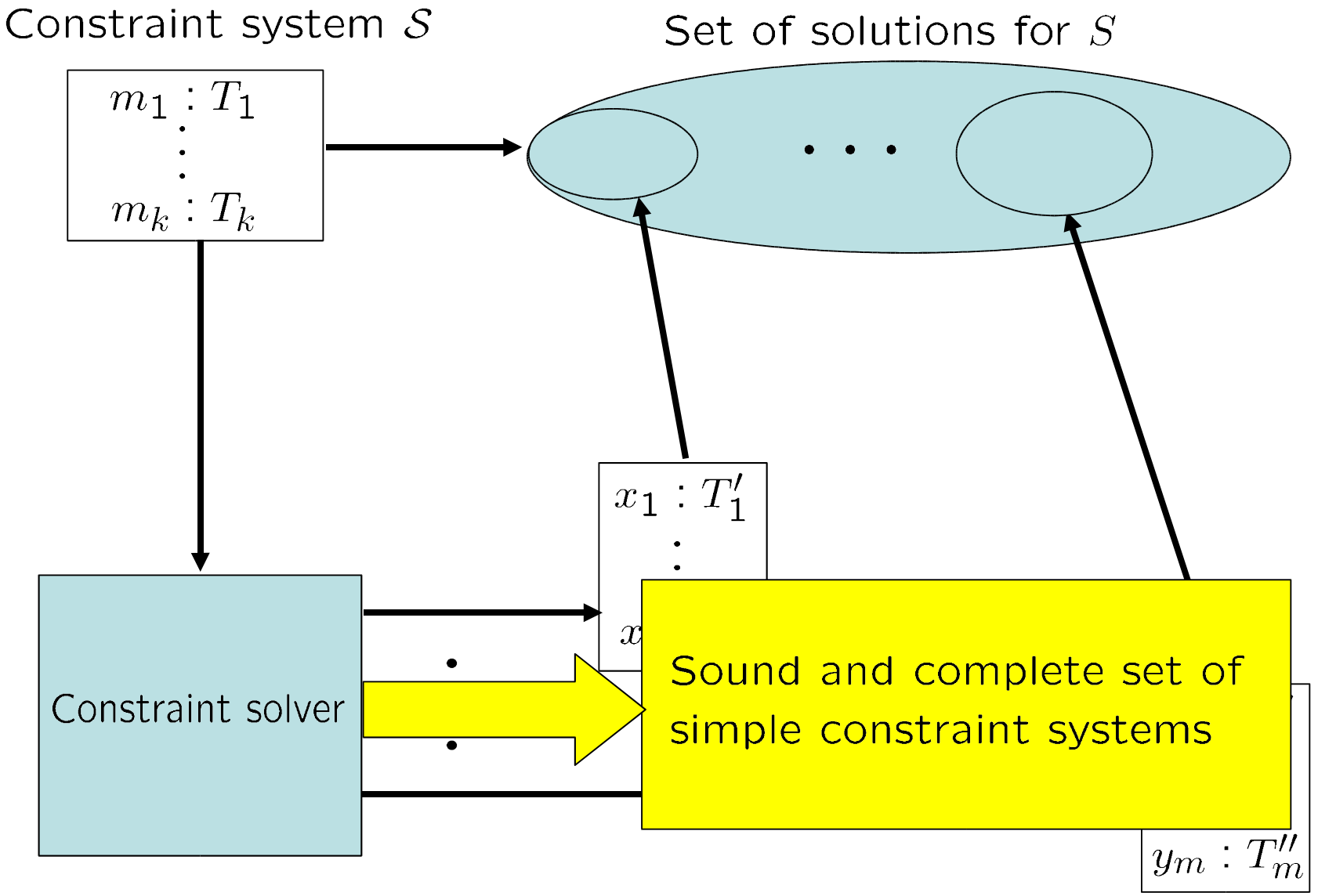
A solution of a constraint system $\mathbf{C}$ is a substitution σ of the variables in $\mathbf{C}$ by messages such that

$$\begin{array}{l} \sigma(m_1) \in d(\,\sigma(T_1)\,) \\ \sigma(m_2) \in d(\,\sigma(T_2)\,) \\ \vdots \\ \sigma(m_k) \in d(\,\sigma(T_k)\,) \end{array}$$

Constraint solver (1)

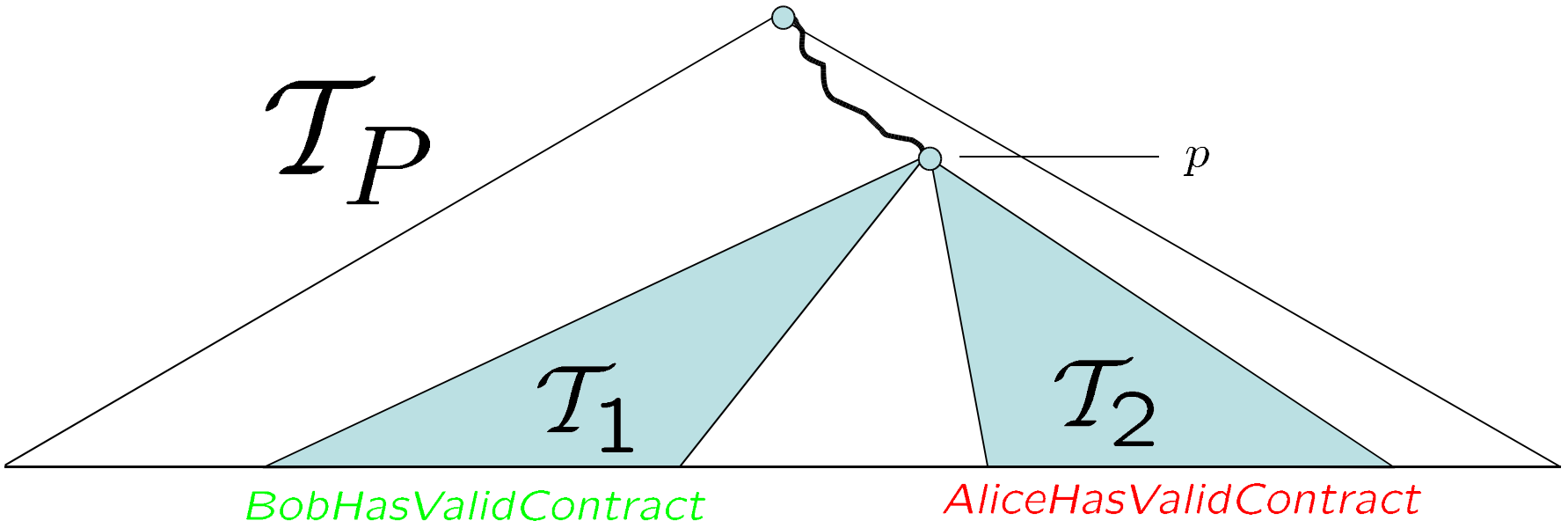


Constraint solver (2)



Algorithm

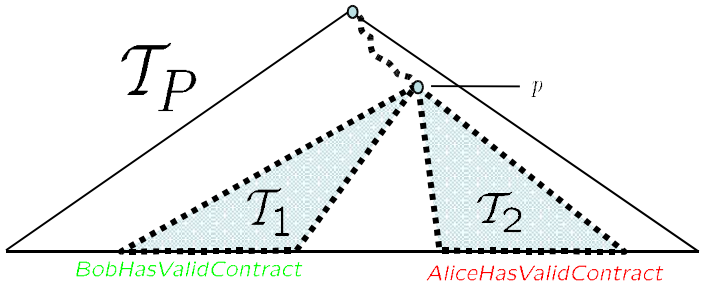
Given: Protocol P and a strategy property C
Is there a state $p \in \mathcal{T}_P$ that satisfies C?



Algorithm

Given: Protocol P and a strategy property C
Is there a state $p \in \mathcal{T}_P$ that satisfies C?

Guess symbolic attack



Construct and solve constraint system

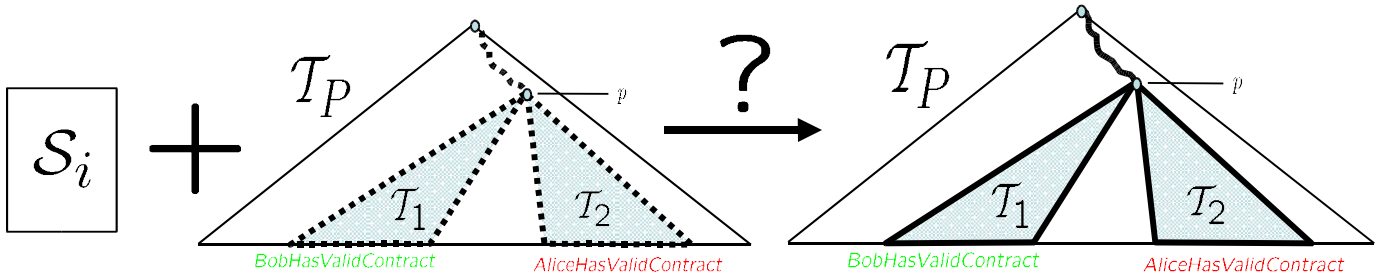
$m_1 : T_1$
$m_2 : T_2$
$m_{17} : T_{17}$

Constraint solver

sound and complete

$\mathcal{S}_1$ $\mathcal{S}_2$ $\cdots$ $\mathcal{S}_b$

Check solutions



Related work

- Contract-signing protocols
  Asokan, Shoup, and Waidner [1998]
  Garay, Jacobsson, and MacKenzie [1999]
  • • •
- Finite state analysis of contract-signing protocols
  Mitchell, Shmatikov [2001]
  Kremer, Raskin [2002]
  • • •
- Infinite state analysis
  Chadha, Kanovich, and Scedrov [2001]
  • • •
- Constraint solving
  Millen, Shmatikov [2001]
  • • •

Conclusions

- Studied game-theoretic properties of infinite transition graphs induced by cryptographic protocols.
- Showed that balance and related game-theoretic properties are decidable using constraint solving algorithm.
- Future work: implementation, complexity analysis