

Protocol Model

Property P

System S

Tamarin Prover

Constraint
from $\neg P$

Constraints
from S

Dedicated
constraint
solver

Solution exists:
ATTACK

No solution
exists: PROOF

Run out of time
or memory

Provide **hints**
for the prover

The screenshot displays the Tamarin Prover interface with two main panels. The left panel, titled 'Proof scripts', contains a script for a theory named 'FirstExample'. It defines a message theory, multiset rewriting rules, tactics, and raw sources. A lemma 'Client_session_key_secret' is stated, followed by a 'simplify' tactic and a 'solve' tactic. The right panel, titled 'Case: Reveal_itk', shows the applicable proof methods and a list of goals. Below this, a 'Constraint system' diagram is shown, illustrating the relationships between various terms and constraints. The diagram includes nodes like 'P1: (b)', 'P2: (b)', 'P3: (b)', 'P4: (b)', 'P5: (b)', 'P6: (b)', 'P7: (b)', 'P8: (b)', 'P9: (b)', 'P10: (b)', 'P11: (b)', 'P12: (b)', 'P13: (b)', 'P14: (b)', 'P15: (b)', 'P16: (b)', 'P17: (b)', 'P18: (b)', 'P19: (b)', 'P20: (b)', 'P21: (b)', 'P22: (b)', 'P23: (b)', 'P24: (b)', 'P25: (b)', 'P26: (b)', 'P27: (b)', 'P28: (b)', 'P29: (b)', 'P30: (b)', 'P31: (b)', 'P32: (b)', 'P33: (b)', 'P34: (b)', 'P35: (b)', 'P36: (b)', 'P37: (b)', 'P38: (b)', 'P39: (b)', 'P40: (b)', 'P41: (b)', 'P42: (b)', 'P43: (b)', 'P44: (b)', 'P45: (b)', 'P46: (b)', 'P47: (b)', 'P48: (b)', 'P49: (b)', 'P50: (b)', 'P51: (b)', 'P52: (b)', 'P53: (b)', 'P54: (b)', 'P55: (b)', 'P56: (b)', 'P57: (b)', 'P58: (b)', 'P59: (b)', 'P60: (b)', 'P61: (b)', 'P62: (b)', 'P63: (b)', 'P64: (b)', 'P65: (b)', 'P66: (b)', 'P67: (b)', 'P68: (b)', 'P69: (b)', 'P70: (b)', 'P71: (b)', 'P72: (b)', 'P73: (b)', 'P74: (b)', 'P75: (b)', 'P76: (b)', 'P77: (b)', 'P78: (b)', 'P79: (b)', 'P80: (b)', 'P81: (b)', 'P82: (b)', 'P83: (b)', 'P84: (b)', 'P85: (b)', 'P86: (b)', 'P87: (b)', 'P88: (b)', 'P89: (b)', 'P90: (b)', 'P91: (b)', 'P92: (b)', 'P93: (b)', 'P94: (b)', 'P95: (b)', 'P96: (b)', 'P97: (b)', 'P98: (b)', 'P99: (b)', 'P100: (b)'. The diagram shows how these constraints are derived from the proof script and the goal list.

Interactive mode
Inspect partial proof