

## 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

The screenshot displays the Tamarin Prover interface. The left pane shows the 'Proof scripts' for a theory named 'FirstExample'. It includes a 'Message theory' section with multiset rewriting rules and tactics, followed by 'Raw sources' and 'Refined sources'. The 'Refined sources' section contains a lemma 'Client\_session\_key\_secret' with a proof script that uses tactics like 'all-traces', 'simplify', 'solve', 'case', and 'by contradiction' to prove the property. The right pane shows the 'Case: Reveal\_itk' with applicable proof methods and a list of goals. Below the goals, a 'Constraint system' diagram is shown, illustrating the relationships between various terms and constraints, such as  $PK(K^{-1}) \oplus PK(2)$  and  $PK(1) : \text{correl}(KX, \neg B)$ .

**Interactive mode**  
Inspect partial proof