

---

# Attacking Group Protocols by Refuting Inductive Conjectures

Graham Steel, Alan Bundy  
and Monika Maidl



School of  
**informatics**

---

## Introduction

- Automated Protocol Analysis
    - ‘much of the low-lying fruit has been picked’
  - Group protocols - Challenging:
    - Arbitrary number of agents increases search space
    - Non-atomic keys
    - More complex ‘control conditions’
  - **Hypothesis:** Formalisation in an inductive model, and use of the CORAL counterexample finder, is an effective means of tackling these challenges.
-

## A Group Protocol

1.  $M_n \rightarrow \text{ALL} : M_n, \{ E \}_P$
2.  $M_i \rightarrow M_n : M_i, \{ R_i, S_i \}_E, i = 1, \dots, n - 1$
3.  $M_n \rightarrow M_i : \{ \{ S_j, j = 1, \dots, n \} \}_{R_i}, i = 1, \dots, n - 1$
4.  $M_i \rightarrow M_n : M_i, \{ S_i, h(S_1, \dots, S_n) \}_K, \text{ some } i.$

(Asokan–Ginzboorg, 2000)

- $E$  fresh public key generated by  $M_n$
  - $R_i$  fresh symmetric keys
  - $S_i$  contributions to group key
  - New group key  $K = f(S_1, \dots, S_n)$
-

## Inductive Model

### Paulson and Bella

Protocols formalised in HOL as traces

A trace is a list of events like ‘Sends  $A$   $B$  Message’

Prove security properties by induction on traces, e.g.

‘If  $A$  receives message 3 with nonce  $N$ ,  
and he sent message 1 with nonce  $N$  to  $B$ ,  
then key  $K$  is not known to the spy.

Deal directly with arbitrary number of agents, nonces, keys,...  
and can model group protocols

**BUT:** No support for non-theorem detection

---

## CORAL

Uses a method borrowing theory from ‘Proof by Consistency’  
- a refutation complete method for proving inductive theorems

Developed by Musser (1980), Huet & Hullot (1982), Kapur &  
Musser (1987), Jouannaud & Kounalis (1986), Bachmair (1988),  
Ganzinger & Stuber (1993) and others.

Re-cast by Comon and Nieuwenhuis (1999)

Two stage approach: I-Axiomatisation + First-order consistency

---

## CORAL

Implemented on top of the SPASS prover

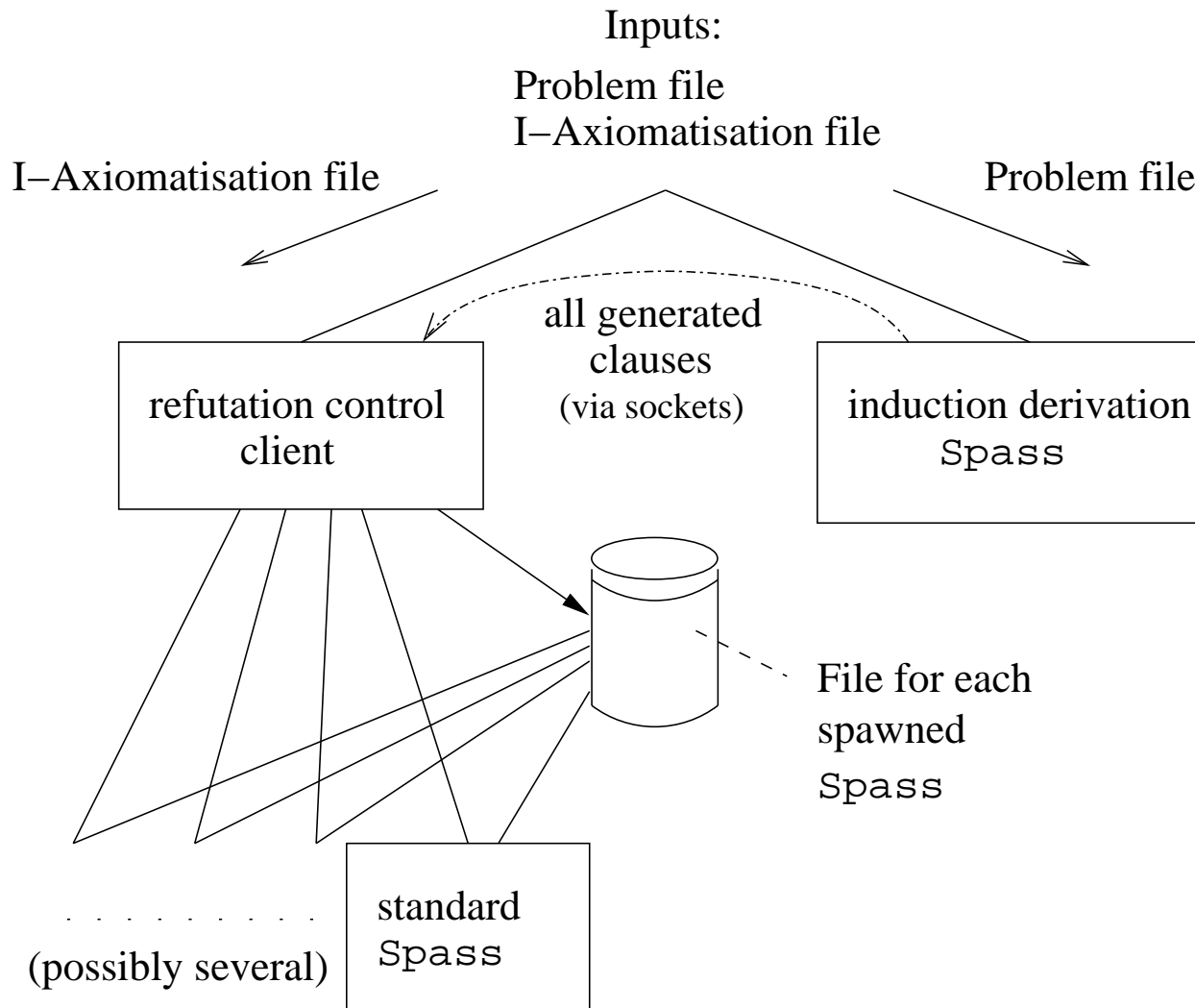
First-order version of Paulson model

Reductive definitions

By refuting a security property  $\forall trace.P(trace)$ , we obtain the attack as the instantiation of *trace*

Tested on several known attacks (from Clark-Jacob corpus)

---



## Heuristics

- Only plausible faked messages
  - Spy only expects plausible subterms
  - Occurs check of *parts* literals
  - Elimination of invalid terms
-

## Back to Asokan–Ginzboorg...

1.  $M_n \rightarrow \text{ALL} : M_n, \{E\}_P$
2.  $M_i \rightarrow M_n : M_i, \{R_i, S_i\}_E, i = 1, \dots, n - 1$
3.  $M_n \rightarrow M_i : \{ \{S_j, j = 1, \dots, n\} \}_{R_i}, i = 1, \dots, n - 1$
4.  $M_i \rightarrow M_n : M_i, \{S_i, h(S_1, \dots, S_n)\}_K, \text{ some } i.$

For  $n$  agent group,  $n - 1$  message 3s are sent simultaneously

---

## Security Properties

A+G claim protocol is “balanced” and resistant to “disruption attacks”.

Must convert these abstract properties to conjectures, e.g.

$$\begin{aligned}
 &eqagent(XI, spy) = false \wedge \\
 &member(sent(XI, XK, pair(principal(XI), \\
 &\quad encr(pair(nonce(SI), h(Package)), f(Package))))), Trace) = true \\
 &member(sent(MN, XJ, encr(Package, nonce(RJ))), Trace) = true \\
 &member(sent(MN, all, pair(principal(MN), encr(key(E), key(P))))), Trace) = true \\
 &member(nonce(SJ), Package) = true \\
 &member(sent(XJ, MN, pair(principal(XJ), encr(pair(nonce(RJ), nonce(SJ)), \\
 &\quad key(E))))), Trace) = false \rightarrow
 \end{aligned}$$


---

## Results

Disruption attacks: CORAL finds two counterexamples,  
corresponding to two attacks

First one on a group of size 3, then when this is fixed, another on  
a group of size 2

After that no more attacks (but no guarantee)

A conjecture about players agreeing on the *same* key also yields  
an attack, when the spy is in the room.

---

## Disruption Attack - Group size 3

1.  $M_1 \rightarrow \text{ALL} : M_1, \{ E \}_P$
2.  $M_2 \rightarrow M_1 : M_2, \{ R_{M_2}, S_{M_2} \}_E$
2.  $\text{spy} \rightarrow M_1 : M_3 \{ R_{M_2}, S_{M_2} \}_E$
3.  $M_1 \rightarrow M_2 : \{ S_{M_2}, S_{M_2}, S_{M_1} \}_{R_{M_2}}$
3.  $M_1 \rightarrow M_3 : \{ S_{M_2}, S_{M_2}, S_{M_1} \}_{R_{M_2}}$
4.  $M_2 \rightarrow M_1 : M_2, \{ S_{M_2}, h(S_{M_2}, S_{M_2}, S_{M_1}) \}_{f(S_{M_2}, S_{M_2}, S_{M_1})}$

## Search Performance

CORAL takes up to 3 hours to find these attacks

Much of this is due to the nature of the model we search in

May be room for more heuristics

Re-implementation, e.g. in Vampire

---

## Example 2 - Tanaka-Sato / Tagdhiri-Jackson

A protocol for maintaining a secure multicast key for a dynamic group

Originally proposed by Tanaka + Sato. T+J found flaws using Alloy + SAT checker, proposed improved protocol.

However, their model did not include an active attacker!

CORAL found an attack on the improved version

---

# Tanaka-Sato/Taghdiri-Jackson

Join:

1.  $M_i \rightarrow S : \{ \text{join} \}_{K_{M_i}}$
2.  $S \rightarrow M_i : \{ Ik_{M_i}, Gk(n) \}_{K_{M_i}}$

Send:

1.  $M_i \rightarrow S : \{ \text{send}(n) \}_{K_{M_i}}$
2.  $S \rightarrow M_i : \{ n', Gk(n') \}_{K_{M_i}}$

Leave:

1.  $M_i \rightarrow S : \{ \text{leave} \}_{K_{M_i}}$
2.  $S \rightarrow M_i : \{ \text{ack.leave} \}_{K_{M_i}}$   
(and generate new key)

Receive:

1.  $M_j \rightarrow S : \{ \text{read}(n) \}_{K_{M_j}}$
2.  $S \rightarrow M_j : \{ Gk(n') \}_{K_{M_j}}$

## CORAL on Tagdhiri–Jackson

Conjecture - there is no trace in which a player outside the group can read a message sent by an honest player from inside the group

CORAL finds a counterexample - spy leaves the group, then replays a key update

The other property T+J tried to fix also false in presence of an active attacker

– the attack is very similar

---

## Attack on Tagdhiri Jackon

$M_1 \rightarrow S : \{ send(sq) \}_{Ik(2)}$   
 $S \rightarrow M_2 : \{ sq', Gk(2) \}_{Ik(2)}$   
 $spy \rightarrow S : \{ send(sq'') \}_{Ik(1)}$   
 $S \rightarrow spy : \{ sq', Gk(2) \}_{Ik(1)}$   
 $spy \rightarrow S : \{ leave \}_{Ik(1)}$   
 $M_1 \rightarrow S : \{ send(sq') \}_{Ik(2)}$   
 $spy \rightarrow M_2 : \{ sq', Gk(2) \}_{Ik(2)}$

# Iolus

Join:

1.  $M_i \rightarrow S : \{ \text{join} \}_{K_{M_i}}$
2.  $S \rightarrow M_i : \{ Ik_{M_i}, Gk(n) \}_{K_{M_i}}$

Send:

1.  $M_i \rightarrow \text{ALL} : \{ \text{message} \}_{Gk(n)}$

Leave:

1.  $M_i \rightarrow S : \{ \text{leave} \}_{K_{M_i}}$
2.  $S \rightarrow \text{ALL} : [ \{ Gk_{n'} \}_{K_{M_j}} \dots ] \forall j \neq i, M_j \in \text{group}$

## Summary

**Hypothesis:** Formalisation in an inductive model, and use of the CORAL counterexample finder, is an effective means of tackling these challenges.

**Evidence:**

6 previously unknown attacks on 3 different protocols

Making conjectures becoming easier with experience

Re-use of features of the model (lists, auxiliary functions..)

---

## Further Work

- More group protocols, with Diffie-Hellman operations
- API attacks

More details

<http://homepages.inf.ed.ac.uk/s9808756/coral>

---