Deciding trace equivalence for protocols with asymmetric operations

Véronique Cortier, Stéphanie Delaune, Vaishnavi Sundararajan

---

**Theorem**

For simple, type-compliant protocols with acyclic dependency graphs, trace equivalence is decidable.

---

**Diagram:**

- Denning-Sacco with signature (DS protocol)
- Acyclic graph (DS Protocol)
- Simple Protocols
  - Each process operates on a distinct channel
- Type Compliance
  - Unifiable "encrypted" subterms get same type
  - Achievable via tagging
  - Extension to handle asymmetric primitives
- Acyclic dependency graph
  - Sequential dependencies
  - Data dependencies
  - Constructed using types

---

**Result**

<table>
<thead>
<tr>
<th>Asymmetric Primitives</th>
<th>Cipher text forwarding</th>
<th>Property</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lowe 98</td>
<td>✓</td>
<td>Secrecy</td>
</tr>
<tr>
<td>Ramanujam, Suresh 03</td>
<td>✓</td>
<td>Leakiness</td>
</tr>
<tr>
<td>Fröschle 15</td>
<td>✓</td>
<td>Leakiness</td>
</tr>
<tr>
<td>Chrétien et al 15</td>
<td>✓</td>
<td>Equivalence</td>
</tr>
<tr>
<td>This work</td>
<td>✓</td>
<td>Equivalence</td>
</tr>
</tbody>
</table>

---

**References:**