

Electronic Notes in Theoretical Computer Science

[www.elsevier.com/locate/entcs](http://www.elsevier.com/locate/entcs)

Secrecy and Group Creation

Luca Cardelli, Andy Gordon and Giorgio Ghelli

**Abstract**

We add an operation of group creation to the typed pi-calculus, where a group is a type for chan- nels. Creation of fresh groups has the effect of statically preventing certain communications, and can blockthe accidental or malicious leakage of secrets. We adapt a notion of secrecy introduced by Abadi, and prove a preservation of secrecy property. When applied to the ambient calculus, the same notion of group creation can be used to create and preserve shared secrets among mobile agents.

1571-0661 *⃝*c Elsevier Ltd Open access under [CC BY-NC-ND license.](http://creativecommons.org/licenses/by-nc-nd/3.0/)

10.1016/S1571-0661(05)80034-9