



ELSEVIER

Available online at www.sciencedirect.com



Electronic Notes in Theoretical Computer Science

**Electronic Notes in
Theoretical Computer
Science**

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 channels. Creation of fresh groups has the effect of statically preventing certain communications, and can block the 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.
