J Autom Reasoning (2012) 48:159–195
DOI 10.1007/s10817-010-9202-1

State and Progress in Strand Spaces: Proving Fair Exchange

Joshua D. Guttman

Received: 13 August 2010 / Accepted: 16 August 2010 / Published online: 27 August 2010

Abstract Many cryptographic protocols are intended to *coordinate state changes* among principals. Exchange protocols, for instance, coordinate delivery of new values to the participants, i.e. additions to the set of values they possess. An exchange protocol is *fair* if it ensures that delivery of new values is balanced: If one participant obtains a new possession via the protocol, then all other participants will, too. Understanding this balanced coordination of different principals in a distributed system requires relating (long-term) *state* to (short-term) protocol activities. Fair exchange also requires *progress* assumptions. In this paper we adapt the strand space framework to protocols, such as fair exchange, that coordinate state changes. We regard the *state* as a multiset of facts, and we allow protocol actions to cause local changes in this state via multiset rewriting. Second, *progress* assumptions stipulate that some channels are resilient—and guaranteed to deliver messages—and some principals will not stop at critical steps. Our proofs of correctness cleanly separate protocol properties, such as authentication and confidentiality, from properties about progress and state evolution. G. Wang's recent fair exchange protocol illustrates the approach.

Keywords Cryptographic protocol analysis • Strand spaces • Verification • Fair exchange

Funded in part by MITRE-Sponsored Research, and in part by National Science Foundation grant number CNS-0952287.

J. D. Guttman (✉)
Worcester Polytechnic Institute, Worcester, MA, USA
e-mail: guttman@wpi.edu

J. D. Guttman
The MITRE Corporation, Bedford, MA, USA