

Chapter 1

Secure State Machine Model

1.1 State Machines

1.1.1 Next-state Function

1.1.2 Next-output Function

1.1.3 Transition Commands

1.2 Secure State Machines

1.2.1 State Machine Versus Secure State Machine

1.2.2 Transition Types

1.2.3 Authentication

1.2.4 Authorization

1.3 Secure State Machines in HOL

1.3.1 Parameterizable Secure State Machine

1.3.2 Parameterization

1.3.3 Configurations: five parts

1.3.3.1 State Interpretation

1.3.3.2 Security context 2

1.3.3.3 Input stream

1.3.3.4 State

1.3.3.5 Output stream

1.3.4 Authentication