Lecture 4

Thursday, 16 February 2023 10:47

ProVerif needs

- protocol
- usage needs
- attacker model
- goals

inp net (A, =B, x) is ProVerif syntax for inp net y; split y is (y_1, y_2, x); if B = y_2 then stop

Compromised participant is modeled as a spy; a process which outputs all (secret) information it gets to the network

you can encode public-key encryption by having

a private function to retrieve the private key of an agent

a (public) function to retrieve the public key of an agent

private free k is the same as process new k; ...