Hyperproperties in Security Protocols

Summary of a coffee-break discussion

Itsaka Rakotonirina
Security Protocols

Distributed program
Security Protocols

Distributed program

adversary
Reachability

possible execution trace

state S
Reachability

For all traces $T$, the final state $S$ of $T$ is "fine".

chosen local property on the final state
Indistinguishability

trace 1 ( ? = ♂ )  →  state S₁

trace 2 ( ? = ♂ )  →  state S₂
Indistinguishability

For all traces $T_1$, there exists a trace $T_2$, "$T_1 \sim T_2$"

Property

indistinguishable by adversarial tests
Effective callback freedom

trace 1 (with feature callback)

state $S_1$

trace 2 (without callback)

state $S_2$
Effective callback freedom

For all traces $T_1$, there exists a trace $T_2$ (without callback), $S_1 \approx S_2$
Front-Running Resistance

trace 1

state $S_1$

trace 2

state $S_2$
Front-Running Resistance

Property

For all traces $T_1$, for all traces $T_2$ that is a permutation of $T_1$, "$S_2 \approx S_1$"

equivalence relation on final states
Coalition Resistance

trace 1 ( ? = 🧵🧵🧵🧵 ) → state $S_1$

trace 2 ( ? = 🧵🧵🧵🧵 ) → state $S_2$
Impact of Coalition Resistance

For all traces $T_1$, for all traces $T_2$ involving a subset of $T_1$'s participants, "$S_2 \leq S_1$"

Property