Tamarin prover basics: Green rectangular boxes represent rule instances. For a rule LHS - [ACT]-> RHS, the top line **Dependency Graphs** represents the LHS, the middle line the ACT, and the bottom line the RHS. The actions line also shows the Red arrows show the adversary learning a term from the network (through an Out fact) concrete timepoint variable Fr(~tvpA (here #vr.2) of this rule #vr 2 · A11 instance and the rule name (A1) **Ellipses** represent Out(<~tvpA, \$A, ~text1>) StA1(SA, ~tvpA) with the set of actions (if any). adversary actions (knowledge derivation, !KU(txt1)@#vk.12 #vk.2 : coerce[!KU(~tvpA)] sending, etc.) Fr(~kAT) Black arrows denote where a isend: adversary sending message to 'In' fact. #vr.1 : Setup[] produced fact is consumed by !KU: terms used during construction path SharedKey(\$A, 'T', ~kAT) coerce : start of construction path (after another rule. possible deconstruction path) !SharedKey(\$A, T Fr(~sesK) Fr(~tnT) Grey arrows show where a #vr.3 : T[Sent(\$A. \$A. ~sesK)] persistent fact/adversary Out(<-text4, senc(<-tvpA, ~sesK, \$A, ~text3>, ~kAT), senc(<-tnT, ~sesK, \$A, ~text2>, ~kAT, 1)> knowledge is used by another #vk : coerce[!KU(senc(<~tvpA, ~sesK, \$A, ~text3>, ~kAT))] time #vf.1 : isend vpA, ~sesK, \$A, ~text3> !SharedKey(\$A, 'T' Fr(~tnA) StA1(SA, ~tvpA) Fr(~text5) Fr(~text6) **Dotted arrows** indicate temporal ordering, i.e., #vr : A2[ALeams(\$A, \$A, ~sesK)] precedence. Out(<~text6, t3, senc(<~tnA, \$A, ~text5>, ~sesK)>) StA2(\$A,\$A,~tnA,~sesK #vk.1 : coerce[!KU(senc(<~tnA, \$A, ~text5>, ~sesK))] !KU(t1)@#vk.6 Grev ellipses indicate where the adversary chooses a term (here t1); ! KU is a specific In(<11, senc(<~tnA, \$A, ~text5>, ~sesK)>) StA2(SA, SA, ~tnA, ~sesK) case of K, i.e., learning # : A3[Done(\$A, \$A, ~sesK)] Slightly different shades of green are used to a term. distinguish between instances of different rules. Users can also choose to specify the color for each rule if they want to.

CC 05.09.2023 - Full details in the Tamarin manual