## Tamarin basics: Green rectangular boxes represent rule instances. For a rule LHS -[ ACT ]-> RHS, the top line represents the **Dependency Graphs** 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 concrete timepoint variable (here from the network (through an Out fact) Fr(~tvpA) Er/ --toyt1 #vr.2) of this rule instance and #vr.2 : A1 the rule name (A1) with the set of Out( <~tvpA, \$A, ~text1> ) StA1( \$A. ~tvpA) actions (if any). **Ellipses** represent adversary #vk.2 : coerce[!KU( ~tvpA )] !KU(txt1)@#vk.12 actions (knowledge derivation, sending, etc.) Fr(~kAT) Black arrows denote where a #vr.1 : Setup∏ produced fact is consumed by SharedKey(\$A, 'T', ~kAT) another rule. In( <~tvpA, \$A, txt1 !SharedKey(\$A, 'T', !SharedKey(\$A, 'T' Er(~tevt2) Fr(~text3) Fr(~text4) 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) )] #vf.1: isend !SharedKey(\$A, 'T' StA1(\$A, ~tvpA) Fr(~text5) Fr( ~text6 ) Fr(~tnA) **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 Grey ellipses indicate where the adversary chooses a term (here t1); !KU is a specific StA2(\$A,\$A,~tnA,~sesK) In( <11, senc(<~tnA, \$A, ~text5>, ~sesK)> ) case of K, i.e., learning #i : A3[Done( \$A, \$A, ~sesK )] a term. Slightly different shades of green are used to

distinguish between instances of different rules. Users can also choose to specify the color for

each rule if they want to.

