

Normalized Derivations

If **B** represents some set of information that is known by a principal, then the principal also knows (can generate) all the information in **B**'s clousre, which in general is an infinite set; however, we usually are not interested in the set of everything that a principal knows, but instead whether or not a specific message $x \in M$ can be generated by a principal.

Let $x \in \overline{B}$ be a message, A derivation of x from B is an alternating sequence of sets of messages and rule instances written as follows:

$$\mathbf{B}_0 \xrightarrow{R_0} B_1 \xrightarrow{R_1} \cdots B_{k-1} \xrightarrow{R_{k-1}} B_k$$

where

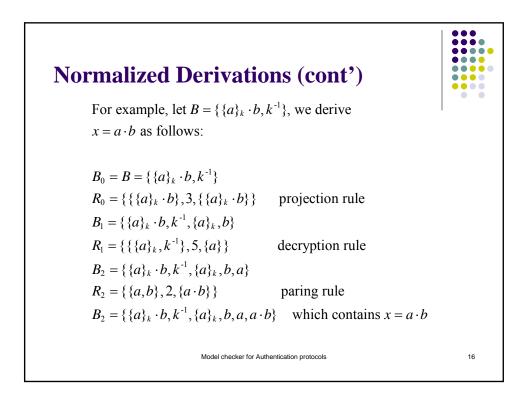
and each rule instance Ri is written as $\langle I_i, N_i, O_i \rangle$ where

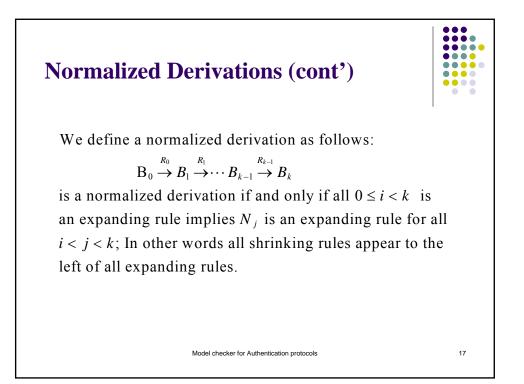
• $I_i \subseteq B_i$, $B_{i+1} = B_i \cup O_i$

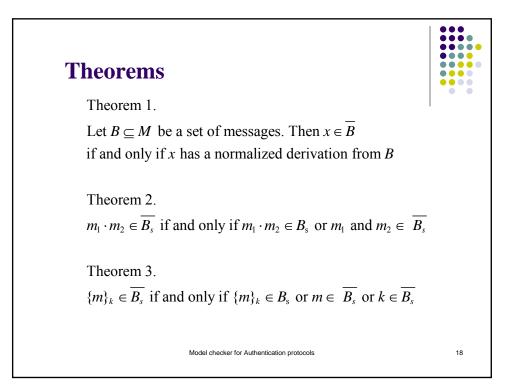
 $B = B_0, x \in B_k$

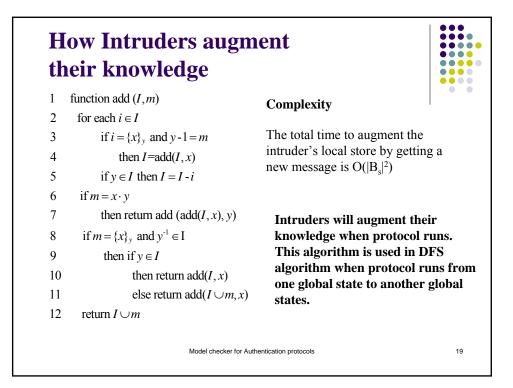
• N_i is one of the clore rules for \overline{B} such that I_i satisfies the premise of the rule and O_i is the corresponding conclusion Model checker for Authentication protocols

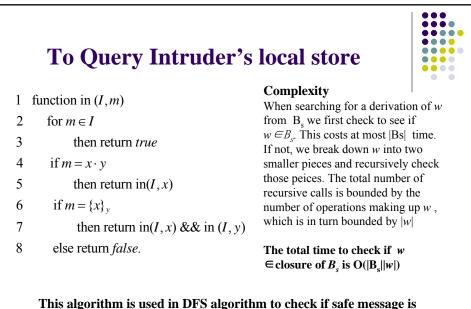
15











This algorithm is used in DFS algorithm to check if safe messag known by Intruder

Model checker for Authentication protocols

20

