

Alice

Eve

pizza.de  
(TLS server)    pizza.de  
(application)

handshake<sub>AB</sub>



delayed by Eve

handshake<sub>EB</sub>



record layer<sub>EB</sub>

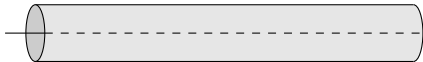
$m_0$



$m_0$

record layer<sub>AB</sub>

$m_1$



$m_1$

$m_0 || m_1$