

DHIES

[Abdalla-Bellare-Rogaway 1997]

