

Aritra Dhar

Building Trust in Modern Computing Platforms



Diss. ETH No. 27668