

EK

seed

EK_{vec}

CT

CT1

CT2