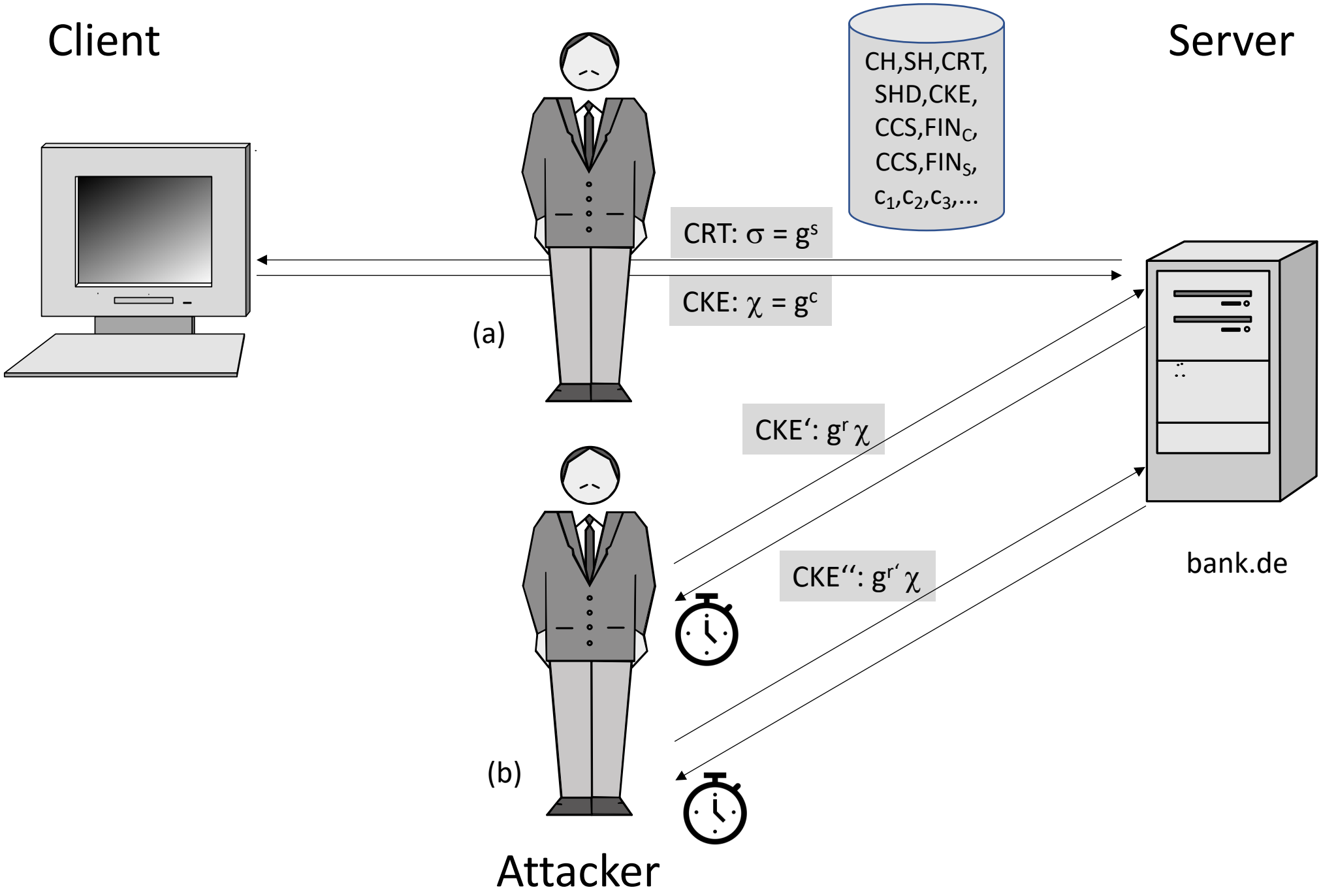
Client
Server
CH,SH,CRT,
SHD,CKE,
CCS,FIN$_C$,
CCS,FIN$_S$,
$c_1,c_2,c_3,\ldots$
CRT: $\sigma = g^s$
CKE: $\chi = g^c$
(a)
CKE‘: $g^r \chi$
CKE‘‘: $g^{r'} \chi$
bank.de
(b)
Attacker