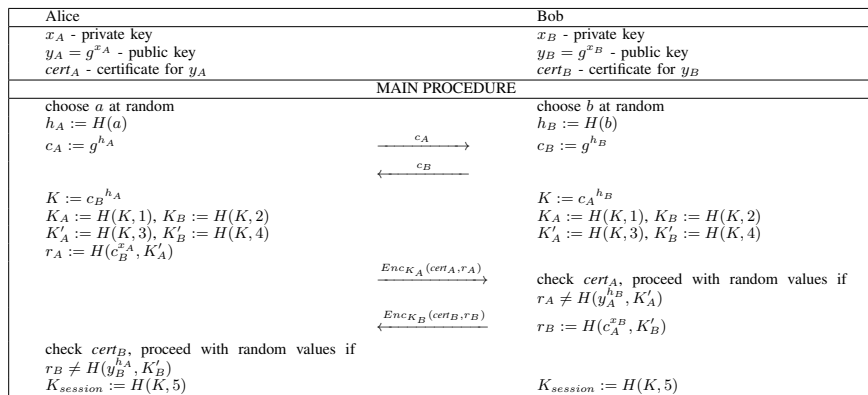
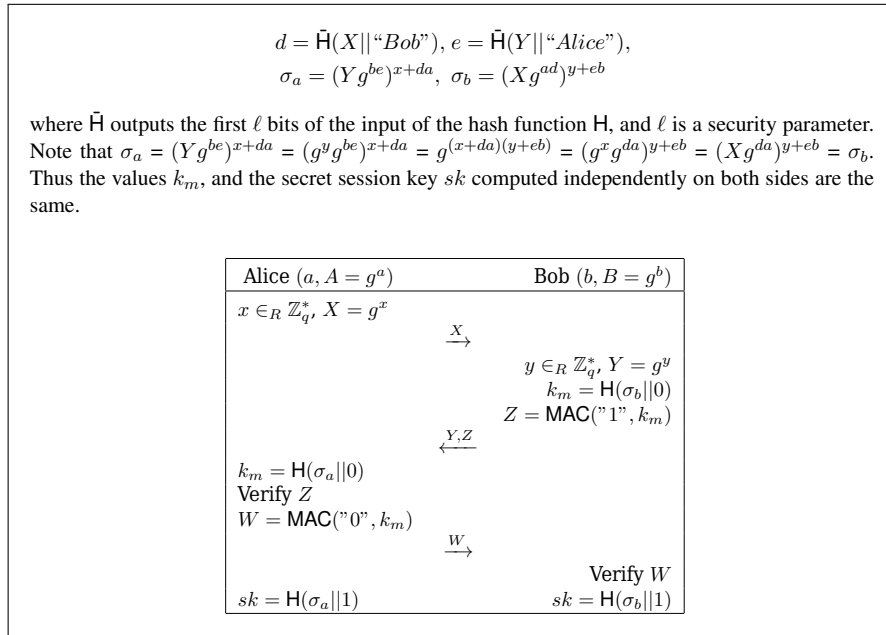
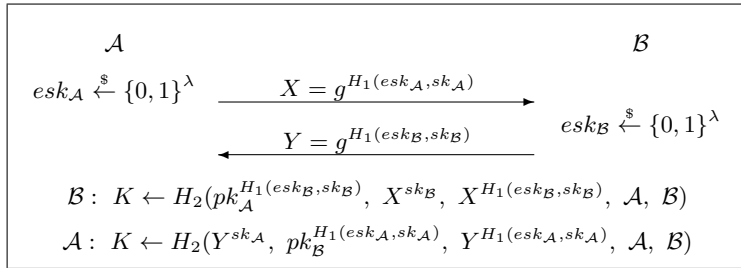


Assume the adversary has access to various oracles revealing, long term keys, ephemeral keys, variable states, etc. Question: Are then the following AKE schemes secure? If not - show the attack. If yes - show the intuition why.





Alice	Bob
$x_A$ - private key	$x_B$ - private key
$y_A = g^{x_A}$ - public key	$y_B = g^{x_B}$ - public key
$cert_A$ - certificate for $y_A$	$cert_B$ - certificate for $y_B$
OPTIONAL SETUP	
recompute $g$	recompute $g$
$y_A := g^{x_A}$ - set public key	$y_B := g^{x_B}$ - set public key
fetch $cert_A$ and check $y_A$	fetch $cert_B$ and check $y_B$
MAIN PROCEDURE	
choose $a$ at random	choose $b$ at random
$h_A := H(a 0)$	$h_B := H(b 0)$
$c_A := y_A^{h_A}$	$c_B := y_B^{h_B}$
$\xrightarrow{c_A}$	$\xleftarrow{c_B}$
$K := c_B^{x_A h_A}$	$K := c_A^{x_B h_B}$
$K_A := H(K 1), K_B := H(K 2)$	$K_A := H(K 1), K_B := H(K 2)$
	reject if $c_A \neq y_A^{H(a 0)}$ or $cert_A$ invalid
reject if $c_B \neq y_B^{H(b 0)}$ or $cert_B$ invalid	$\xleftarrow{Enc_{K_B}(b, cert_B)}$
$K_s := H(K 3)$	$K_s := H(K 3)$

