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.

$$d = \bar{\mathsf{H}}(X||\text{“}Bob\text{”}),\ e = \bar{\mathsf{H}}(Y||\text{“}Alice\text{”}),$$
$$\sigma_a = (Yg^{be})^{x+da},\ \sigma_b = (Xg^{ad})^{y+eb}$$

where $\bar{\mathsf{H}}$ outputs the first ℓ bits of the input of the hash function H, and ℓ is a security parameter. Note that $\sigma_a = (Yg^{be})^{x+da} = (g^y g^{be})^{x+da} = g^{(x+da)(y+eb)} = (g^x g^{da})^{y+eb} = (Xg^{da})^{y+eb} = \sigma_b$. Thus the values k_m, and the secret session key sk computed independently on both sides are the same.

Alice $(a, A = g^a)$		Bob $(b, B = g^b)$
$x \in_R \mathbb{Z}_q^*$, $X = g^x$		
	$\xrightarrow{X}$	
		$y \in_R \mathbb{Z}_q^*$, $Y = g^y$
		$k_m = \mathsf{H}(\sigma_b\|\|0)$
		$Z = \mathsf{MAC}(\text{"}1\text{"}, k_m)$
	$\xleftarrow{Y,Z}$	
$k_m = \mathsf{H}(\sigma_a\|\|0)$		
Verify Z		
$W = \mathsf{MAC}(\text{"}0\text{"}, k_m)$		
	$\xrightarrow{W}$	
		Verify W
$sk = \mathsf{H}(\sigma_a\|\|1)$		$sk = \mathsf{H}(\sigma_b\|\|1)$

Alice		Bob
x_A - private key $y_A = g^{x_A}$ - public key *cert*$_A$ - certificate for y_A		x_B - private key $y_B = g^{x_B}$ - public key *cert*$_B$ - certificate for y_B
	MAIN PROCEDURE	
choose a at random		choose b at random
$h_A := H(a)$		$h_B := H(b)$
$c_A := g^{h_A}$	$\xrightarrow{c_A}$	$c_B := g^{h_B}$
	$\xleftarrow{c_B}$	
$K := {c_B}^{h_A}$		$K := {c_A}^{h_B}$
$K_A := H(K,1)$, $K_B := H(K,2)$		$K_A := H(K,1)$, $K_B := H(K,2)$
$K'_A := H(K,3)$, $K'_B := H(K,4)$		$K'_A := H(K,3)$, $K'_B := H(K,4)$
$r_A := H(c_B^{x_A}, K'_A)$		
	$\xrightarrow{Enc_{K_A}(cert_A, r_A)}$	check *cert*$_A$, proceed with random values if $r_A \neq H(y_A^{h_B}, K'_A)$
	$\xleftarrow{Enc_{K_B}(cert_B, r_B)}$	$r_B := H(c_A^{x_B}, K'_B)$
check *cert*$_B$, proceed with random values if $r_B \neq H(y_B^{h_A}, K'_B)$		
$K_{session} := H(K,5)$		$K_{session} := H(K,5)$

$$
\begin{array}{ccc}
\mathcal{A} & & \mathcal{B} \\
esk_{\mathcal{A}} \xleftarrow{\$} \{0,1\}^{\lambda} & \xrightarrow{\quad X = g^{H_1(esk_{\mathcal{A}}, sk_{\mathcal{A}})} \quad} & \\
 & \xleftarrow{\quad Y = g^{H_1(esk_{\mathcal{B}}, sk_{\mathcal{B}})} \quad} & esk_{\mathcal{B}} \xleftarrow{\$} \{0,1\}^{\lambda}
\end{array}
$$

$$\mathcal{B}: \; K \leftarrow H_2(pk_{\mathcal{A}}^{H_1(esk_{\mathcal{B}}, sk_{\mathcal{B}})}, \; X^{sk_{\mathcal{B}}}, \; X^{H_1(esk_{\mathcal{B}}, sk_{\mathcal{B}})}, \; \mathcal{A}, \; \mathcal{B})$$

$$\mathcal{A}: \; K \leftarrow H_2(Y^{sk_{\mathcal{A}}}, \; pk_{\mathcal{B}}^{H_1(esk_{\mathcal{A}}, sk_{\mathcal{A}})}, \; Y^{H_1(esk_{\mathcal{A}}, sk_{\mathcal{A}})}, \; \mathcal{A}, \; \mathcal{B})$$

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

$$
\begin{array}{ccc}
\mathbb{A} & & \mathbb{B} \\
x & \xrightarrow{\quad g^x, \; SIG_{\mathbb{A}}(g^x, \mathbb{B}) \quad} & \\
 & \xleftarrow{\quad g^y, \; SIG_{\mathbb{B}}(g^y, \mathbb{A}) \quad} & y \\
K = g^{xy} & & K = g^{xy}
\end{array}
$$

$$
\begin{array}{ccc}
\mathbb{A}: \; a, g^a & & \mathbb{B}: \; b, g^b \\
x & \xrightarrow{\qquad g^x \qquad} & \\
 & \xleftarrow{\qquad g^y \qquad} & y \\
K = H(g^{ay}, g^{bx}, \mathbb{A}, \mathbb{B}) & & K = H(g^{ay}, g^{bx}, \mathbb{A}, \mathbb{B})
\end{array}
$$