Question: Let $(sk, pk) = (a, A) = (a, g^a)$ are secret/public keys in a well defined group with parameters (g, p, q), where assumptions: DLP, CDH, DDH hold. Let m, σ denote a message and its signature. Are the following signature schemes secure? If not - show the most *devastating* attack. If yes - show the intuition why.

$Sign(a, m)$	$Verify(A, m, \sigma)$
$r \in_R \mathbb{Z}_q^*$, $R = g^r$ $h = \mathcal{H}(m)$ $s = r + ah$ $\sigma = (R, s)$	$h = \mathcal{H}(m)$ Accept iff $g^s = RA^h$

$Sign(a, m)$	$Verify(A, m, \sigma)$
$r \in_R \mathbb{Z}_q^*$, $R = g^r$ $h = m + R$ $s = r + ah$ $\sigma = (R, s)$	$h = m + R$ Accept iff $g^s = RA^h$

$Sign(a, m)$	$Verify(A, m, \sigma)$
$r \in_R \mathbb{Z}_q^*$, $R = g^r$ $h = mR$ $s = r + ah$ $\sigma = (R, s)$	$h = mR$ Accept iff $g^s = RA^h$

$Sign(a, m)$	$Verify(A, m, \sigma)$
$r \in_R \mathbb{Z}_q^*$, $R = g^r$ $h = m \otimes R$ $s = r + ah$ $\sigma = (R, s)$	$h = m \otimes R$ Accept iff $g^s = RA^h$

$Sign(a, m)$	$Verify(A, m, \sigma)$
$r \in_R \mathbb{Z}_q^*$, $R = g^r$ $X = g^{ar}$ $h = \mathcal{H}(m, R)$ $s = h + ra$ $\sigma = (R, s, X)$	$h = \mathcal{H}(m, R)$ Accept iff $g^s = g^h X$

$Sign(a, m)$	$Verify(A, m, \sigma)$
$r \in_R \mathbb{Z}_q^*$, $R = g^r$ $X = g^{ar}$ $h = \mathcal{H}(m, R, X)$ $s = h + ra$ $\sigma = (R, s, X)$	$h = \mathcal{H}(m, R, X)$ Accept iff $g^s = g^h X$