SIGMA

$\hat{A}(a, A)_{ID_A}$ $\hat{B}(b, B)_{ID_B}$

S - session ID

S, $x \leftarrow_R Z_q$

g^x

$S, g^x \rightarrow$

1. $y \leftarrow_R Z_q$
2. $K \leftarrow g^{xy}$
3. $\sigma_B = Sig("1", S, g^x, g^y)$ uses b to sign
4. $K_0 \leftarrow PRF(K, 0)$
5. $K_1 \leftarrow PRF(K, 1)$
6. $M_B = MAC_{K1}("1", S, ID_B)$

$\leftarrow S, g^y, \sigma_B, M_B, ID_B$

1. $K = (g^y)^x = g^{yx}$
2. $\sigma_A = Sig_A("0", S, g^y, g^x)$
3. $K_0 \leftarrow PRF(K, 0)$
4. $K_1 \leftarrow PRF(K, 1)$
5. $M_A = MAC_{K1}("0", S, ID_A)$

$S, ID_A, M_A, \sigma_A \rightarrow$

First of all $\hat{A}$ sends s and public ephemeral key $\rightarrow g^x$. Then $\hat{B}$ uses g^x to compute K. Having K, $\hat{B}$ computes two keys $\rightarrow K_0, K_1$. Then it removes K and y from memory. Now $\hat{B}$ sends those values to $\hat{A}$. $\hat{A}$ computes K and K_0, K_1 and removes x and K from memory. Then verifies M_B checks Sig_B with B (by deriving from ID_B). After that it sends what is needed to $\hat{B}$. $\hat{B}$ verifies M_A, retrieves public key A and verifies Sig_A. If something is wrong, then session is aborted.

SIGMA is secure if: (under DDH)

1. Two parties accomplished the protocol and are sure that they were communicating with each other.
2. The session key of two parties is the same.
3. Session key is known only by two parties that communicate with each other.

We need to prove:

$\Pi(\mathcal{S}, R) - K_{\mathcal{S}}$

$\mathcal{A}$ plays with challenger C

$b \leftarrow_R \{0,1\}$ — C toss at random 0 or 1, (to feed it or to send him real session key)

if $b = 0$

$K \leftarrow K_{real}$

else

$K \leftarrow K_{random} \leftarrow_R \{0,1\}$

$$\left| Pr[\mathcal{A}(K_{real}) \rightarrow 0] - Pr[\mathcal{A}(K_{random}) \rightarrow 0] \right| < \varepsilon$$

Proof:

SoG

G.0 → original game (protocol) $K_0 \leftarrow PRF_{g^{xy}}(0)$ $K_1 \leftarrow PRF_{g^{xy}}(1)$

G.1 $K_0 \leftarrow PRF_K(0)$ $K_1 \leftarrow PRF_K(1)$ $K \leftarrow rand()$

G 2 $K_0 \leftarrow rand()$ $K_1 \leftarrow rand()$

G3 $K_0 \leftarrow rand()$ $K_1 \leftarrow PRF_K(1)$ $K \leftarrow rand()$

G4 $K_0 \leftarrow rand()$ $K_1 \rightarrow PRF_{g^{xy}}(1)$

$|Pr[D(G0) \rightarrow 1] - Pr[D(G1) \rightarrow 1]| \leq \varepsilon_{DDH}$

$|Pr[D(G1) \rightarrow 1] - Pr[D(G2) \rightarrow 1]| \leq \varepsilon_{PRF}$

$|Pr[D(G2) \rightarrow 1] - Pr[D(G3) \rightarrow 1]| \leq \varepsilon_{PRF}$

$|Pr[D(G3) \rightarrow 1] - Pr[D(G4) \rightarrow 1]| \leq \varepsilon_{DDH}$

$|Pr[D(G0) \rightarrow 1] - Pr[D(G4) \rightarrow 1]| \leq 2(\varepsilon_{PRF} + \varepsilon_{DDH})$

It means that $\mathcal{A}$ doesn't know when he is fooled.