Initiator (sk_I, pk_I)		Responder (sk_R, pk_R)

IKE_SA_INIT

$\mathsf{spi_I} \xleftarrow{\$} \{0,1\}^{64}$
$x \xleftarrow{\$} \{0,1\}^{\lambda}, X \leftarrow g^x,$
$n_I \xleftarrow{\$} \{0,1\}^{\mu},$
$m_1 = (\overrightarrow{SA}, X, n_I)$

$\xrightarrow{\mathsf{spi_I}|0, m_1}$

$\mathsf{spi_R} \xleftarrow{\$} \{0,1\}^{64}$
$y \xleftarrow{\$} \{0,1\}^{\lambda}, Y \leftarrow g^y$
$n_R \xleftarrow{\$} \{0,1\}^{\mu},$
$m_2 = (SA, Y, n_R, [CREQ])$

$\xleftarrow{\mathsf{spi_I}|\mathsf{spi_R}, m_2}$

Key Derivation IKEv2

$$s \leftarrow \mathsf{PRF}_{n_I|n_R}(g^{xy})$$

$$T_1|T_2|T_3|... \leftarrow \mathsf{IPRF}_s(data);\ T_1 \leftarrow \mathsf{PRF}_s(data|1);$$
$$T_{i+1} \leftarrow \mathsf{PRF}_s(T_i|data|i+1)$$

$$k_d|k_{ai}|k_{ar}|k_{ei}|k_{er}|k_{pi}|k_{pr} \leftarrow \mathsf{IPRF}_s(n_i|n_r|\mathsf{spi_I}|\mathsf{spi_R})$$

IKE_AUTH

$mac_i \leftarrow \mathsf{PRF}_{k_{pi}}(ID_I)$
$\sigma_i \leftarrow$
$\mathsf{Sign}_{sk_I}(\mathsf{spi_I}|0|m_1|n_R|mac_i)$
$m_3 = (ID_I, \sigma_i, \overrightarrow{SA_2}, \overrightarrow{TS})$
$c_3' \leftarrow \mathsf{Enc}_{k_{ei}}(m_3)$
$c_3 = (c_3', \mathsf{MAC}_{k_{ai}}(c_3'))$

$\xrightarrow{\mathsf{spi_I}|\mathsf{spi_R}, c_3}$

$mac_r \leftarrow \mathsf{PRF}_{k_{pr}}(ID_R)$
$\sigma_r \leftarrow$
$\mathsf{Sign}_{sk_R}(\mathsf{spi_I}|\mathsf{spi_R}|m_2|n_I|mac_r)$
$m_4 := (ID_R, \sigma_r, SA_2, \overrightarrow{TS})$
$c_4' \leftarrow \mathsf{Enc}_{k_{er}}(m_4)$
$c_4 = (c_3', \mathsf{MAC}_{k_{ar}}(c_4'))$

$\xleftarrow{\mathsf{spi_I}|\mathsf{spi_R}, c_4}$

Key Derivation ESP/AH

$$k'_{ei}|k'_{ai}|k'_{er}|k'_{ar} \leftarrow \mathsf{IPRF}_{k_d}(n_i|n_r)$$