Initiator		Responder
(sk_I, pk_I)		(sk_R, pk_R)
$(k_d, k_{ei}, k_{ai}, k_{er}, k_{ar})$		$(k_d, k_{ei}, k_{ai}, k_{er}, k_{ar})$
$(\mathsf{spi_I}, \mathsf{spi_R})$		$(\mathsf{spi_I}, \mathsf{spi_R})$

CREATE_CHILD

$[x' \xleftarrow{\$} \{0,1\}^\lambda, X' \leftarrow g^{x'}]$
$n'_I \xleftarrow{\$} \{0,1\}^\mu,$
$m'_1 = (\vec{SA}, n_I, [X'])$
$c'_1 \leftarrow \mathsf{Enc}_{k_{ei}}(m'_1)$
$c_1 = (c'_1, \mathsf{MAC}_{k_{ai}}(c'_1))$

$\mathsf{spi_I}|\mathsf{spi_R}, c_1 \longrightarrow$

$[y' \xleftarrow{\$} \{0,1\}^\lambda, Y' \leftarrow g^{y'}]$
$n'_R \xleftarrow{\$} \{0,1\}^\mu,$
$m'_2 = (SA, n'_R, [Y'])$
$c'_2 \leftarrow \mathsf{Enc}_{k_{er}}(m'_2)$
$c_2 = (c'_2, \mathsf{MAC}_{k_{ar}}(c'_2))$

$\mathsf{spi_I}|\mathsf{spi_R}, c_2 \longleftarrow$

Key Derivation

$$k'_{ei}|k'_{ai}|k'_{er}|k'_{ar} \leftarrow \mathsf{IPRF}_{k_d}([g^{x'y'}]|n'_I|n'_R)$$