Table 1: Detailed results for ISO 9798-2-6 - Nonces, keys, randomized primitives - NR-A1/Keyleak

Case	Nonce	IA_A	IA_B	NIA_A	NIA_B
No misgeneration	N/A	✓	✓	✓	✓
Leak Always	R_B	✓	✓	✓	✓
Leak Always	R_A	✓	✓	✓	✓
Leak Always	k_{AB}	✗	✗	✗	✗
Leak Always	n_1	✓	✓	✓	✓
Leak Always	n_2	✓	✓	✓	✓
Leak Always	R_{A2}	✓	✓	✓	✓
Leak Always	n_3	✓	✓	✓	✓
Leak Always	n_4	✓	✓	✓	✓
Reuse Always	R_B	✓	✗	✓	✓
Reuse Always	R_A	✓	✓	✓	✓
Reuse Always	k_{AB}	✗	✗	✗	✗
Reuse Always	n_1	✗	✗	✗	✗
Reuse Always	n_2	✗	✗	✗	✗
Reuse Always	R_{A2}	✓	✓	✓	✓
Reuse Always	n_3	✓	✓	✓	✓
Reuse Always	n_4	✓	✓	✓	✓
Reuse Once	$R_B = R_B$	✓	✗	✓	✓
Reuse Once	$R_B = R_A$	✓	✓	✓	✓
Reuse Once	$R_B = k_{AB}$	✗	✗	✗	✗
Reuse Once	$R_B = n_1$	✓	✓	✓	✓
Reuse Once	$R_B = n_2$	✓	✓	✓	✓
Reuse Once	$R_B = R_{A2}$	✓	✓	✓	✓
Reuse Once	$R_B = n_3$	✓	✓	✓	✓
Reuse Once	$R_B = n_4$	✓	✓	✓	✓
Reuse Once	$R_A = R_A$	✓	✓	✓	✓
Reuse Once	$R_A = k_{AB}$	✗	✗	✗	✗
Reuse Once	$R_A = n_1$	✓	✓	✓	✓
Reuse Once	$R_A = n_2$	✓	✓	✓	✓
Reuse Once	$R_A = R_{A2}$	✓	✓	✓	✓
Reuse Once	$R_A = n_3$	✓	✓	✓	✓
Reuse Once	$R_A = n_4$	✓	✓	✓	✓
Reuse Once	$k_{AB} = k_{AB}$	✗	✗	✗	✗
Reuse Once	$k_{AB} = n_1$	✗	✗	✗	✗
Reuse Once	$k_{AB} = n_2$	✗	✗	✗	✗
Reuse Once	$k_{AB} = R_{A2}$	✗	✗	✗	✗
Reuse Once	$k_{AB} = n_3$	✗	✗	✗	✗
Reuse Once	$k_{AB} = n_4$	✗	✗	✗	✗
Reuse Once	$n_1 = n_1$	✗	✗	✗	✗
Reuse Once	$n_1 = n_2$	✓	✓	✓	✓
Reuse Once	$n_1 = R_{A2}$	✓	✓	✓	✓
Reuse Once	$n_1 = n_3$	✓	✓	✓	✓
Reuse Once	$n_1 = n_4$	✓	✓	✓	✓
Reuse Once	$n_2 = n_2$	✗	✗	✗	✗
Reuse Once	$n_2 = R_{A2}$	✓	✓	✓	✓
Reuse Once	$n_2 = n_3$	✓	✓	✓	✓
Reuse Once	$n_2 = n_4$	✓	✓	✓	✓
Reuse Once	$R_{A2} = R_{A2}$	✓	✓	✓	✓
Reuse Once	$R_{A2} = n_3$	✓	✓	✓	✓
Reuse Once	$R_{A2} = n_4$	✓	✓	✓	✓
Reuse Once	$n_3 = n_3$	✓	✓	✓	✓
Reuse Once	$n_3 = n_4$	✓	✓	✓	✓
Reuse Once	$n_4 = n_4$	✓	✓	✓	✓