Table 1: Detailed results for ISO 9798-2-4 - 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	n_1	✓	✓	✓	✓
Leak Always	n_2	✓	✓	✓	✓
Leak Always	n_2	✓	✓	✓	✓
Leak Always	n_2	✓	✓	✓	✓
Leak Always	n_2	✓	✓	✓	✓
Leak Always	n_2	✓	✓	✓	✓
Reuse Always	R_B	✓	✗	✓	✓
Reuse Always	R_A	✗	✓	✗	✓
Reuse Always	n_1	✗	✗	✗	✗
Reuse Always	n_2	✗	✗	✗	✗
Reuse Once	$R_B = R_B$	✓	✗	✓	✓
Reuse Once	$R_B = R_A$	✓	✓	✓	✓
Reuse Once	$R_B = n_1$	✓	✓	✓	✓
Reuse Once	$R_B = n_2$	✓	✓	✓	✓
Reuse Once	$R_A = R_A$	✗	✓	✗	✓
Reuse Once	$R_A = n_1$	✓	✓	✓	✓
Reuse Once	$R_A = n_2$	✓	✓	✓	✓
Reuse Once	$n_1 = n_1$	✗	✗	✗	✗
Reuse Once	$n_1 = n_2$	✗	✗	✗	✗
Reuse Once	$n_2 = n_2$	✗	✗	✗	✗