

Table 1: Detailed results for ISO 9798-2-6 - Nonces, keys, randomized primitives - NR-A2/Messleak

Case	Nonce	IA_A	IA_B	NIA_A	NIA_B
Reuse Always	n_1	X	X	X	X
Reuse Always	n_2	X	X	X	X
Reuse Once	$n_1 = n_1$	X	X	X	X
Reuse Once	$n_2 = n_2$	X	X	X	X