

Table 1: Detailed results for Four-Way Handshake - Static PSK - Nonces

Case	Nonce	IA_AP	IA_C	NIA_AP	NIA_C	IAK_AP	IAK_C	NIAK_AP	NIAK_C	S_AP	S_C	KF_AP	KF_C
No misgeneration	N/A	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Leak Always	$N_A$	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Leak Always	$N_S$	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Reuse Always	$N_A$	✗	✓	✓	✓	✗	✓	✓	✓	✓	✓	✗	✓
Reuse Always	$N_S$	✓	✗	✓	✓	✓	✗	✓	✓	✓	✓	✓	✗
Reuse Once	$N_A = N_A$	✗	✓	✓	✓	✗	✓	✓	✓	✓	✓	✗	✓
Reuse Once	$N_A = N_S$	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Reuse Once	$N_S = N_S$	✓	✗	✓	✓	✓	✗	✓	✓	✓	✓	✓	✗