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

Leak Always

Reuse Always
Reuse Always

Reuse Once

Reuse Once

 N_S

 $\frac{N_S}{N_A = N_A}$

 $N_A = N_S$

 $N_S = N_S$

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