Lemma	Scenario	lake-draft12/lake-edhoc	lake-draft12/lake-edhoc-KEM	lake-draft14/lake-edhoc	lake-draft14/lake-edhoc-KEM
no-reflection-attacks-RI		✗^{P} (18)	✗^{P} (0)	✗^{P} (21)	✗^{P} (0)
	DH-Check	✗^{P} (14)	∅	✗^{P} (16)	∅
	Sig$^{\not}$, AEAD$^{\not}$, $\oplus^{\not}$, DHShare$^{\not}$, Cred-Check	✓^{P} (2435) 🕓^{T}	✓^{P} (⇒) ✓^{T} (⇒)	✓^{P} (3083) 🕓^{T}	✓^{P} (⇒) ✓^{T} (⇒)
	Sig$^{\not}$-proof, AEAD$^{\not}$, $\oplus^{\not}$, DH$^{\not}$, Cred-Check	✓^{P} (1239) 🕓^{T}	∅	✓^{P} (⇒) 🕓^{T}	∅
	Sig$^{\not}$-proof, SessKey$^{\not}$, AEAD$^{\not}$, DH$^{\not}$, Cred-Check	✓^{P} (132) 🕓^{T}	∅	✓^{P} (⇒) 🕓^{T}	∅
	Sig$^{\not}$-proof, SessKey$^{\not}$, AEAD$^{\not}$, DHShare$^{\not}$, Cred-Check	✓^{P} (2199) 🕓^{T}	✓^{P} (⇒) ✓^{T} (6753)	✓^{P} (2132) 🕓^{T}	✓^{P} (⇒) ✓^{T} (⇒)
	Sig$^{\not}$-proof, SessKey$^{\not}$, AEAD$^{\not}$, $\oplus^{\not}$, Cred-Check	✓^{P} (1546) 🕓^{T}	✓^{P} (⇒) 🕓^{T}	✓^{P} (⇒) 🕓^{T}	✓^{P} (⇒) ✓^{T} (⇒)
	Sig$^{\not}$, SessKey$^{\not}$, AEAD$^{\not}$, $\oplus^{\not}$, DH$^{\not}$, Cred-Check	✓^{P} (1080) 🕓^{T}	∅	✓^{P} (⇒) 🕓^{T}	∅
	Sig$^{\not}$-proof, AEAD$^{\not}$, $\oplus^{\not}$, DH$^{\not}$, Cred-Check, DH-Check	✓^{P} (1308) 🕓^{T}	∅	✓^{P} (⇒) 🕓^{T}	∅
	Sig$^{\not}$-proof, AEAD$^{\not}$, $\oplus^{\not}$, DHShare$^{\not}$, Cred-Check, DH-Check	✓^{P} (1971) 🕓^{T}	∅	✓^{P} (⇒) 🕓^{T}	∅
	Sig$^{\not}$-proof, SessKey$^{\not}$, AEAD$^{\not}$, $\oplus^{\not}$, DH$^{\not}$, Cred-Check	🕓^{P}	∅	✓^{P} (1649) 🕓^{T}	∅
	Sig$^{\not}$-proof, SessKey$^{\not}$, AEAD$^{\not}$, $\oplus^{\not}$, DHShare$^{\not}$, Cred-Check	🕓^{P}	✓^{P} (809) 🕓^{T}	🕓^{P}	✓^{P} (134) ✓^{T} (5571)
	Sig$^{\not}$-proof, SessKey$^{\not}$, AEAD$^{\not}$, DH$^{\not}$, Cred-Check, DH-Check	✓^{P} (134) 🕓^{T}	∅	✓^{P} (⇒) 🕓^{T}	∅
	Sig$^{\not}$-proof, SessKey$^{\not}$, AEAD$^{\not}$, DHShare$^{\not}$, Cred-Check, DH-Check	✓^{P} (1419) 🕓^{T}	∅	✓^{P} (⇒) 🕓^{T}	∅
	Sig$^{\not}$-proof, SessKey$^{\not}$, AEAD$^{\not}$, $\oplus^{\not}$, Cred-Check, DH-Check	✓^{P} (1365) 🕓^{T}	∅	✓^{P} (⇒) 🕓^{T}	∅
	Sig$^{\not}$, SessKey$^{\not}$, AEAD$^{\not}$, $\oplus^{\not}$, DHShare$^{\not}$, Cred-Check, DH-Check	✓^{P} (2280) 🕓^{T}	∅	✓^{P} (⇒) 🕓^{T}	∅
	Sig$^{\not}$, SessKey$^{\not}$, AEAD$^{\not}$, $\oplus^{\not}$, DH$^{\not}$, Cred-Check, DH-Check	✓^{P} (1082) 🕓^{T}	∅	✓^{P} (⇒) 🕓^{T}	∅
	Sig$^{\not}$-proof, SessKey$^{\not}$, AEAD$^{\not}$, $\oplus^{\not}$, DH$^{\not}$, Cred-Check, DH-Check	🕓^{P}	∅	✓^{P} (1541) 🕓^{T}	∅
	Sig$^{\not}$-proof, SessKey$^{\not}$, AEAD$^{\not}$, $\oplus^{\not}$, DHShare$^{\not}$, Cred-Check, DH-Check	🕓^{P}	∅	✓^{P} (2242) 🕓^{T}	∅
auth-IR-unique		✗^{P} (12)	✗^{P} (0)	✓^{P} (⇒) ✓^{T} (2579)	✓^{P} (⇒) ✓^{T} (⇒)
	DHShare$^{\not}$, DH-Check	✗^{P} (240)	∅	✓^{P} (⇒) ✓^{T} (2433)	∅
	DH$^{\not}$, DH-Check	✗^{P} (41)	∅	✓^{P} (⇒) 🕓^{T}	∅
	Sig$^{\not}$-proof, SessKey$^{\not}$, AEAD$^{\not}$, DHShare$^{\not}$	✗^{P} (⇒)	✗^{P} (⇒)	✓^{P} (1705) 🕓^{T}	✓^{P} (⇒) ✓^{T} (⇒)
	Sig$^{\not}$, SessKey$^{\not}$, AEAD$^{\not}$, $\oplus^{\not}$, DHShare$^{\not}$	✗^{P} (⇒)	✗^{P} (⇒)	✓^{P} (3288) 🕓^{T}	✓^{P} (⇒) ✓^{T} (⇒)
	Sig$^{\not}$-proof, SessKey$^{\not}$, AEAD$^{\not}$, $\oplus^{\not}$, DHShare$^{\not}$	✗^{P} (⇒)	✗^{P} (⇒)	🕓^{P}	✓^{P} (115) ✓^{T} (1250)
	Sig$^{\not}$-proof, SessKey$^{\not}$, AEAD$^{\not}$, $\oplus^{\not}$, DH$^{\not}$	✗^{P} (⇒)	∅	✓^{P} (1260) 🕓^{T}	∅
	Sig$^{\not}$-proof, SessKey$^{\not}$, AEAD$^{\not}$, $\oplus^{\not}$, DH-Check	✓^{P} (709) 🕓^{T}	∅	✓^{P} (⇒) 🕓^{T}	∅
	Sig$^{\not}$-proof, SessKey$^{\not}$, AEAD$^{\not}$, $\oplus^{\not}$, DH$^{\not}$, DH-Check	✗^{P} (⇒)	∅	✓^{P} (1391) 🕓^{T}	∅
	Sig$^{\not}$-proof, SessKey$^{\not}$, AEAD$^{\not}$, $\oplus^{\not}$, DHShare$^{\not}$, DH-Check	✗^{P} (⇒)	∅	✓^{P} (2219) 🕓^{T}	∅
data-authentication-IR	DHShare$^{\not}$	✗^{P} (61)	✓^{P} (⇒) ✓^{T} (157)	✗^{P} (69)	✓^{P} (⇒) ✓^{T} (154)
	DHShare$^{\not}$, DH-Check	✗^{P} (51)	∅	✗^{P} (59)	∅
	Sig$^{\not}$-proof, SessKey$^{\not}$, AEAD$^{\not}$, $\oplus^{\not}$, DH$^{\not}$	✓^{P} (2853) 🕓^{T}	∅	✓^{P} (1426) 🕓^{T}	∅
	Sig$^{\not}$-proof, SessKey$^{\not}$, AEAD$^{\not}$, $\oplus^{\not}$, DHShare$^{\not}$	✗^{P} (⇒) 🕓^{T}	✓^{P} (277) 🕓^{T}	✗^{P} (⇒) 🕓^{T}	✓^{P} (107) 🕓^{T}
	Sig$^{\not}$-proof, SessKey$^{\not}$, AEAD$^{\not}$, $\oplus^{\not}$, DH$^{\not}$, DH-Check	✓^{P} (2759) 🕓^{T}	∅	✓^{P} (1417) 🕓^{T}	∅
data-authentication-RI	AEAD$^{\not}$	✗^{P} (37)	✗^{P} (2)	✓^{P} (⇒) 🕓^{T}	✓^{P} (⇒)
	DHShare$^{\not}$	✗^{P} (1358)	✗^{P} (7)	✓^{P} (⇒) 🕓^{T}	✓^{P} (⇒)
	SessKey$^{\not}$	✗^{P} (51)	✗^{P} (3)	✓^{P} (⇒) ✓^{T} (6587)	✓^{P} (⇒)
	$\oplus^{\not}$, DHShare$^{\not}$	✗^{P} (⇒) 🕓^{T}	✗^{P} (⇒)	🕓^{P}	✗^{P} (42)
	AEAD$^{\not}$, DH-Check	✗^{P} (24)	∅	✓^{P} (⇒) 🕓^{T}	∅
	DHShare$^{\not}$, DH-Check	✗^{P} (572)	∅	✓^{P} (⇒) 🕓^{T}	∅
	SessKey$^{\not}$, DH-Check	✗^{P} (42)	∅	✓^{P} (⇒) ✓^{T} (6210)	∅
	Sig$^{\not}$-proof, DHShare$^{\not}$	✗^{P} (⇒) 🕓^{T}	✗^{P} (⇒)	✗^{P} (2106)	✗^{P} (27)
	Sig$^{\not}$-proof, $\oplus^{\not}$	✓^{P} (⇒) 🕓^{T}	✓^{P} (57) ✓^{T} (1319)	✓^{P} (⇒) 🕓^{T}	✓^{P} (⇒)
	$\oplus^{\not}$, DHShare$^{\not}$, DH-Check	✗^{P} (⇒) 🕓^{T}	∅	✗^{P} (1986)	∅
	Sig$^{\not}$-proof, $\oplus^{\not}$, DH$^{\not}$	✓^{P} (1928) 🕓^{T}	∅	✓^{P} (⇒) 🕓^{T}	∅
	Sig$^{\not}$-proof, DHShare$^{\not}$, DH-Check	✗^{P} (⇒) 🕓^{T}	∅	✗^{P} (991)	∅
	Sig$^{\not}$, SessKey$^{\not}$, AEAD$^{\not}$, DHShare$^{\not}$	✗^{P} (⇒) 🕓^{T}	✗^{P} (⇒)	✓^{P} (1931) 🕓^{T}	✓^{P} (9) ✓^{T} (785)
	Sig$^{\not}$-proof, $\oplus^{\not}$, DH$^{\not}$, DH-Check	✓^{P} (1942) 🕓^{T}	∅	✓^{P} (⇒) 🕓^{T}	∅
	Sig$^{\not}$-proof, SessKey$^{\not}$, AEAD$^{\not}$, $\oplus^{\not}$	✗^{P} (⇒) 🕓^{T}	✗^{P} (⇒)	✓^{P} (⇒) 🕓^{T}	✓^{P} (47) 🕓^{T}
	Sig$^{\not}$, SessKey$^{\not}$, AEAD$^{\not}$, DHShare$^{\not}$, DH-Check	✗^{P} (⇒) 🕓^{T}	∅	✓^{P} (783) 🕓^{T}	∅
	Sig$^{\not}$-proof, SessKey$^{\not}$, AEAD$^{\not}$, $\oplus^{\not}$, DH$^{\not}$	✗^{P} (⇒) 🕓^{T}	∅	✓^{P} (2146) 🕓^{T}	∅
	Sig$^{\not}$-proof, SessKey$^{\not}$, AEAD$^{\not}$, $\oplus^{\not}$, DH$^{\not}$, DH-Check	✗^{P} (⇒) 🕓^{T}	∅	✓^{P} (2097) 🕓^{T}	∅
honest-auth-RI-non-inj	SessKey$^{\not}$, DHShare$^{\not}$	✗^{P} (1170)	✓^{P} (⇒) ✓^{T} (⇒)	✓^{P} (⇒) 🕓^{T}	✓^{P} (⇒) ✓^{T} (⇒)
	SessKey$^{\not}$, DHShare$^{\not}$, DH-Check	✗^{P} (509)	∅	✓^{P} (⇒) 🕓^{T}	∅
	Sig$^{\not}$-proof, AEAD$^{\not}$, DHShare$^{\not}$	✓^{P} (1117) 🕓^{T}	✓^{P} (⇒) ✓^{T} (⇒)	✓^{P} (⇒) 🕓^{T}	✓^{P} (⇒) ✓^{T} (⇒)
	Sig$^{\not}$, AEAD$^{\not}$, $\oplus^{\not}$, DHShare$^{\not}$	✓^{P} (2545) 🕓^{T}	✓^{P} (⇒) ✓^{T} (⇒)	✓^{P} (⇒) 🕓^{T}	✓^{P} (⇒) ✓^{T} (⇒)
	Sig$^{\not}$-proof, AEAD$^{\not}$, $\oplus^{\not}$, DH$^{\not}$	✓^{P} (1243) 🕓^{T}	∅	✓^{P} (⇒) 🕓^{T}	∅
	Sig$^{\not}$-proof, SessKey$^{\not}$, AEAD$^{\not}$, DHShare$^{\not}$	✗^{P} (⇒) 🕓^{T}	✓^{P} (⇒) ✓^{T} (6937)	✓^{P} (2012) 🕓^{T}	✓^{P} (⇒) ✓^{T} (⇒)
	Sig$^{\not}$-proof, SessKey$^{\not}$, AEAD$^{\not}$, DH$^{\not}$	✓^{P} (134) 🕓^{T}	∅	✓^{P} (⇒) 🕓^{T}	∅
	Sig$^{\not}$-proof, SessKey$^{\not}$, AEAD$^{\not}$, $\oplus^{\not}$	✓^{P} (1545) 🕓^{T}	✓^{P} (⇒) 🕓^{T}	✓^{P} (⇒) 🕓^{T}	✓^{P} (⇒) ✓^{T} (⇒)
	Sig$^{\not}$, SessKey$^{\not}$, AEAD$^{\not}$, $\oplus^{\not}$, DH$^{\not}$	✓^{P} (1059) 🕓^{T}	∅	✓^{P} (⇒) 🕓^{T}	∅
	Sig$^{\not}$, SessKey$^{\not}$, AEAD$^{\not}$, $\oplus^{\not}$, DHShare$^{\not}$	✗^{P} (⇒) 🕓^{T}	✓^{P} (⇒) ✓^{T} (2185)	✓^{P} (3529) 🕓^{T}	✓^{P} (⇒) ✓^{T} (⇒)
	Sig$^{\not}$-proof, AEAD$^{\not}$, $\oplus^{\not}$, DH$^{\not}$, DH-Check	✓^{P} (1251) 🕓^{T}	∅	✓^{P} (⇒) 🕓^{T}	∅
	Sig$^{\not}$-proof, AEAD$^{\not}$, $\oplus^{\not}$, DHShare$^{\not}$, DH-Check	✓^{P} (1931) 🕓^{T}	∅	✓^{P} (⇒) 🕓^{T}	∅
	Sig$^{\not}$-proof, SessKey$^{\not}$, AEAD$^{\not}$, $\oplus^{\not}$, DHShare$^{\not}$	✗^{P} (⇒) 🕓^{T}	✓^{P} (752) 🕓^{T}	🕓^{P}	✓^{P} (97) ✓^{T} (7030)
	Sig$^{\not}$-proof, SessKey$^{\not}$, AEAD$^{\not}$, $\oplus^{\not}$, DH$^{\not}$	🕓^{P}	∅	✓^{P} (1665) 🕓^{T}	∅
	Sig$^{\not}$-proof, SessKey$^{\not}$, AEAD$^{\not}$, DH$^{\not}$, DH-Check	✓^{P} (127) 🕓^{T}	∅	✓^{P} (⇒) 🕓^{T}	∅
	Sig$^{\not}$-proof, SessKey$^{\not}$, AEAD$^{\not}$, $\oplus^{\not}$, DH-Check	✓^{P} (1448) 🕓^{T}	∅	✓^{P} (⇒) 🕓^{T}	∅
	Sig$^{\not}$, SessKey$^{\not}$, AEAD$^{\not}$, $\oplus^{\not}$, DH$^{\not}$, DH-Check	✓^{P} (1062) 🕓^{T}	∅	✓^{P} (⇒) 🕓^{T}	∅
	Sig$^{\not}$-proof, SessKey$^{\not}$, AEAD$^{\not}$, $\oplus^{\not}$, DH$^{\not}$, DH-Check	🕓^{P}	∅	✓^{P} (1646) 🕓^{T}	∅
	Sig$^{\not}$-proof, SessKey$^{\not}$, AEAD$^{\not}$, $\oplus^{\not}$, DHShare$^{\not}$, DH-Check	✗^{P} (⇒) 🕓^{T}	∅	✓^{P} (2508) 🕓^{T}	∅
secretI	Sig$^{\not}$-proof, AEAD$^{\not}$, DHShare$^{\not}$	✓^{P} (1281) 🕓^{T}	✓^{P} (⇒) 🕓^{T}	🕓^{P}	✓^{P} (⇒) 🕓^{T}
	Sig$^{\not}$, AEAD$^{\not}$, $\oplus^{\not}$, DHShare$^{\not}$	✓^{P} (3417) 🕓^{T}	✓^{P} (⇒) 🕓^{T}	🕓^{P}	✓^{P} (⇒) 🕓^{T}
	Sig$^{\not}$, SessKey$^{\not}$, AEAD$^{\not}$, DHShare$^{\not}$	✓^{P} (1758) 🕓^{T}	✓^{P} (⇒) ✓^{T} (4832)	🕓^{P}	✓^{P} (⇒) 🕓^{T}
	Sig$^{\not}$-proof, AEAD$^{\not}$, $\oplus^{\not}$, DH$^{\not}$	✓^{P} (⇒) 🕓^{T}	∅	✓^{P} (3442) 🕓^{T}	∅
	Sig$^{\not}$-proof, $\oplus^{\not}$, DH$^{\not}$, DH-Check	✓^{P} (⇒) 🕓^{T}	∅	✓^{P} (3345) 🕓^{T}	∅
	Sig$^{\not}$-proof, SessKey$^{\not}$, AEAD$^{\not}$, DH$^{\not}$	✓^{P} (⇒) 🕓^{T}	∅	✓^{P} (336) 🕓^{T}	∅
	Sig$^{\not}$-proof, SessKey$^{\not}$, AEAD$^{\not}$, $\oplus^{\not}$	✓^{P} (⇒) 🕓^{T}	✓^{P} (⇒) 🕓^{T}	✓^{P} (1044) 🕓^{T}	✓^{P} (⇒) 🕓^{T}
	SessKey$^{\not}$, AEAD$^{\not}$, $\oplus^{\not}$, DH$^{\not}$, DH-Check	✓^{P} (⇒) 🕓^{T}	∅	✓^{P} (3340) 🕓^{T}	∅
	Sig$^{\not}$, AEAD$^{\not}$, $\oplus^{\not}$, DH$^{\not}$, DH-Check	✓^{P} (⇒) 🕓^{T}	∅	✓^{P} (2897) 🕓^{T}	∅
	Sig$^{\not}$, SessKey$^{\not}$, AEAD$^{\not}$, $\oplus^{\not}$, DH$^{\not}$	✓^{P} (⇒) 🕓^{T}	∅	✓^{P} (3249) 🕓^{T}	∅
	Sig$^{\not}$-proof, AEAD$^{\not}$, $\oplus^{\not}$, DHShare$^{\not}$, DH-Check	✓^{P} (2065) 🕓^{T}	∅	🕓^{P}	∅
	Sig$^{\not}$, SessKey$^{\not}$, $\oplus^{\not}$, DH$^{\not}$, DH-Check	✓^{P} (⇒) 🕓^{T}	∅	✓^{P} (3496) 🕓^{T}	∅
	Sig$^{\not}$-proof, SessKey$^{\not}$, AEAD$^{\not}$, $\oplus^{\not}$, DHShare$^{\not}$	🕓^{P}	✓^{P} (495) 🕓^{T}	🕓^{P}	✓^{P} (488) 🕓^{T}
	Sig$^{\not}$-proof, SessKey$^{\not}$, AEAD$^{\not}$, $\oplus^{\not}$, DH$^{\not}$	✓^{P} (3485) 🕓^{T}	∅	🕓^{P}	∅
	Sig$^{\not}$-proof, SessKey$^{\not}$, AEAD$^{\not}$, DH$^{\not}$, DH-Check	✓^{P} (⇒) 🕓^{T}	∅	✓^{P} (316) 🕓^{T}	∅
	Sig$^{\not}$-proof, SessKey$^{\not}$, AEAD$^{\not}$, DHShare$^{\not}$, DH-Check	✓^{P} (2779) 🕓^{T}	∅	🕓^{P}	∅
	Sig$^{\not}$-proof, SessKey$^{\not}$, AEAD$^{\not}$, $\oplus^{\not}$, DH-Check	✓^{P} (⇒) 🕓^{T}	∅	✓^{P} (792) 🕓^{T}	∅
	Sig$^{\not}$-proof, SessKey$^{\not}$, AEAD$^{\not}$, $\oplus^{\not}$, DH$^{\not}$, DH-Check	✓^{P} (3434) 🕓^{T}	∅	🕓^{P}	∅
secretR	Sig$^{\not}$, AEAD$^{\not}$, $\oplus^{\not}$, DHShare$^{\not}$	✓^{P} (2678) 🕓^{T}	✓^{P} (⇒) ✓^{T} (⇒)	🕓^{P}	✓^{P} (⇒) 🕓^{T}
	Sig$^{\not}$-proof, AEAD$^{\not}$, $\oplus^{\not}$, DH$^{\not}$	✓^{P} (1188) 🕓^{T}	∅	✓^{P} (⇒) 🕓^{T}	∅
	Sig$^{\not}$-proof, SessKey$^{\not}$, AEAD$^{\not}$, DHShare$^{\not}$	✓^{P} (3541) 🕓^{T}	✓^{P} (⇒) 🕓^{T}	🕓^{P}	✓^{P} (⇒) 🕓^{T}
	Sig$^{\not}$-proof, SessKey$^{\not}$, AEAD$^{\not}$, DH$^{\not}$	✓^{P} (128) 🕓^{T}	∅	✓^{P} (⇒) 🕓^{T}	∅
	Sig$^{\not}$-proof, SessKey$^{\not}$, AEAD$^{\not}$, $\oplus^{\not}$	✓^{P} (1622) 🕓^{T}	✓^{P} (⇒) ✓^{T} (3174)	✓^{P} (⇒) 🕓^{T}	✓^{P} (⇒) ✓^{T} (4635)
	Sig$^{\not}$, SessKey$^{\not}$, AEAD$^{\not}$, $\oplus^{\not}$, DH$^{\not}$	✓^{P} (968) 🕓^{T}	∅	✓^{P} (⇒) 🕓^{T}	∅
	Sig$^{\not}$-proof, AEAD$^{\not}$, $\oplus^{\not}$, DH$^{\not}$, DH-Check	✓^{P} (1174) 🕓^{T}	∅	✓^{P} (⇒) 🕓^{T}	∅
	Sig$^{\not}$-proof, AEAD$^{\not}$, $\oplus^{\not}$, DHShare$^{\not}$, DH-Check	✓^{P} (1850) 🕓^{T}	∅	🕓^{P}	∅
	Sig$^{\not}$-proof, SessKey$^{\not}$, AEAD$^{\not}$, $\oplus^{\not}$, DHShare$^{\not}$	🕓^{P}	✓^{P} (1093) 🕓^{T}	🕓^{P}	✓^{P} (424) 🕓^{T}
	Sig$^{\not}$-proof, SessKey$^{\not}$, AEAD$^{\not}$, $\oplus^{\not}$, DH$^{\not}$	🕓^{P}	∅	✓^{P} (2817) 🕓^{T}	∅
	Sig$^{\not}$-proof, SessKey$^{\not}$, AEAD$^{\not}$, DH$^{\not}$, DH-Check	✓^{P} (130) 🕓^{T}	∅	✓^{P} (⇒) 🕓^{T}	∅
	Sig$^{\not}$-proof, SessKey$^{\not}$, AEAD$^{\not}$, DHShare$^{\not}$, DH-Check	✓^{P} (2358) 🕓^{T}	∅	🕓^{P}	∅
	Sig$^{\not}$-proof, SessKey$^{\not}$, AEAD$^{\not}$, $\oplus^{\not}$, DH-Check	✓^{P} (1495) 🕓^{T}	∅	✓^{P} (⇒) 🕓^{T}	∅
	Sig$^{\not}$, SessKey$^{\not}$, AEAD$^{\not}$, $\oplus^{\not}$, DH$^{\not}$, DH-Check	✓^{P} (1012) 🕓^{T}	∅	✓^{P} (⇒) 🕓^{T}	∅
	Sig$^{\not}$, SessKey$^{\not}$, AEAD$^{\not}$, $\oplus^{\not}$, DHShare$^{\not}$, DH-Check	✓^{P} (3277) 🕓^{T}	∅	🕓^{P}	∅
	Sig$^{\not}$-proof, SessKey$^{\not}$, AEAD$^{\not}$, $\oplus^{\not}$, DH$^{\not}$, DH-Check	🕓^{P}	∅	✓^{P} (2860) 🕓^{T}	∅

Automated aggregation of results

For each lemma and each scenario, we display the result of the automated analysis based on Proverif and Tamarin.
We display all scenarios for which at least one of the protocol has a non trivial and non timeout result.

✗^{T} (x),✗^{P} (x): attack found with Tamarin (T) or Proverif (P) in x seconds
✓^{T} (x),✓^{P} (x): proof found with Tamarin (T) or Proverif (P) in x seconds
(⇒): means the result is implied by another displayed result
🕓^{T},🕓^{P}: timeout for Tamarin (T) or Proverif (P)
∅: the scenario is irrelevant for this protocol (e.g., DH weakness in KEM setting)