Lemma	Scenario	**models/lake-edhoc**	**models/lake-edhoc-KEM**
auth-IR-unique	Sig$^{↯}$-proof, SessKey$^{↯}$, AEAD$^{↯}$, $\oplus^{↯}$, DHShare$^{↯}$	🕓^{P}	✓^{P} (41) ✓^{T} (1272)
	Sig$^{↯}$-proof, SessKey$^{↯}$, AEAD$^{↯}$, $\oplus^{↯}$, DH$^{↯}$	✓^{P} (615) 🕓^{T}	∅
auth-RI-unique	Sig$^{↯}$-proof, SessKey$^{↯}$, AEAD$^{↯}$, $\oplus^{↯}$, DHShare$^{↯}$	🕓^{P}	✓^{P} (32) ✓^{T} (1630)
	Sig$^{↯}$-proof, SessKey$^{↯}$, AEAD$^{↯}$, $\oplus^{↯}$, DH$^{↯}$	✓^{P} (585) 🕓^{T}	∅
data-authentication-IR	$\oplus^{↯}$	✗^{P} (23)	✗^{P} (2)
	Sig$^{↯}$-proof, DHShare$^{↯}$	🕓^{P}	✗^{P} (4)
	Sig$^{↯}$-proof, SessKey$^{↯}$, AEAD$^{↯}$	✓^{P} (⇒) 🕓^{T}	✓^{P} (3) 🕓^{T}
	Sig$^{↯}$, SessKey$^{↯}$, AEAD$^{↯}$, DHShare$^{↯}$	🕓^{P}	✓^{P} (3) ✓^{T} (1347)
	Sig$^{↯}$-proof, SessKey$^{↯}$, AEAD$^{↯}$, DH$^{↯}$	✓^{P} (46) 🕓^{T}	∅
data-authentication-RI	$\oplus^{↯}$, DHShare$^{↯}$	🕓^{P}	✗^{P} (21)
	Sig$^{↯}$-proof, DHShare$^{↯}$	🕓^{P}	✗^{P} (23)
	Sig$^{↯}$, SessKey$^{↯}$, AEAD$^{↯}$, DHShare$^{↯}$	🕓^{P}	✓^{P} (6) ✓^{T} (1647)
	Sig$^{↯}$-proof, SessKey$^{↯}$, AEAD$^{↯}$, $\oplus^{↯}$	✓^{P} (⇒) 🕓^{T}	✓^{P} (25) 🕓^{T}
	Sig$^{↯}$-proof, SessKey$^{↯}$, AEAD$^{↯}$, $\oplus^{↯}$, DH$^{↯}$	✓^{P} (933) 🕓^{T}	∅
honest-auth-RI-non-inj	Sig$^{↯}$-proof, SessKey$^{↯}$, AEAD$^{↯}$, $\oplus^{↯}$, DHShare$^{↯}$	🕓^{P}	✓^{P} (57) 🕓^{T}
	Sig$^{↯}$-proof, SessKey$^{↯}$, AEAD$^{↯}$, $\oplus^{↯}$, DH$^{↯}$	✓^{P} (742) 🕓^{T}	∅
honest-auth-RI-unique	Sig$^{↯}$-proof, SessKey$^{↯}$, AEAD$^{↯}$, $\oplus^{↯}$, DHShare$^{↯}$	🕓^{P}	✓^{P} (50) ✓^{T} (1319)
	Sig$^{↯}$-proof, SessKey$^{↯}$, AEAD$^{↯}$, $\oplus^{↯}$, DH$^{↯}$	✓^{P} (598) 🕓^{T}	∅
secretI	Sig$^{↯}$-proof, SessKey$^{↯}$, AEAD$^{↯}$, $\oplus^{↯}$, DHShare$^{↯}$	🕓^{P}	✓^{P} (143) 🕓^{T}
	Sig$^{↯}$-proof, SessKey$^{↯}$, AEAD$^{↯}$, $\oplus^{↯}$, DH$^{↯}$	✓^{P} (1891) 🕓^{T}	∅
secretR	Sig$^{↯}$-proof, SessKey$^{↯}$, AEAD$^{↯}$, $\oplus^{↯}$, DHShare$^{↯}$	🕓^{P}	✓^{P} (232) 🕓^{T}
	Sig$^{↯}$-proof, SessKey$^{↯}$, AEAD$^{↯}$, $\oplus^{↯}$, DH$^{↯}$	✓^{P} (1181) 🕓^{T}	∅
honest-auth-IR-non-inj	Sig$^{↯}$-proof, SessKey$^{↯}$, AEAD$^{↯}$, $\oplus^{↯}$, DHShare$^{↯}$	🕓^{P}	✓^{P} (30) 🕓^{T}
	Sig$^{↯}$-proof, SessKey$^{↯}$, AEAD$^{↯}$, $\oplus^{↯}$, DH$^{↯}$	✓^{P} (504) 🕓^{T}	∅
honest-auth-IR-unique	Sig$^{↯}$-proof, SessKey$^{↯}$, AEAD$^{↯}$, $\oplus^{↯}$, DHShare$^{↯}$	🕓^{P}	✓^{P} (40) ✓^{T} (1468)
	Sig$^{↯}$-proof, SessKey$^{↯}$, AEAD$^{↯}$, $\oplus^{↯}$, DH$^{↯}$	✓^{P} (619) 🕓^{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)