	Jablon (hash)	Jablon (challenge)	IEEE P1363.2:D26 ISO/IEC 11770-4:2006	Hao&Shahandashti	ISO/IEC 11770-4:2017		Proof is based on…
Correctness	00:00:00.01	00:00:00.01	00:00:00.01	00:00:00.01	00:00:00.01	C	trace
Secrecy of password	00:00:01.15	00:00:03.83	00:02:56.60	00:44:45.54	03:11:01.40	PW	observational equivalence
Secrecy of session key	00:00:00.85	00:00:02.45	00:00:52.40	00:31:25.24	02:54:20.40	IKA	observational equivalence
Equality of exchanged key	00:00:00.31	00:00:00.56	00:00:00.31	00:00:00.12	00:00:00.11	EKA	event property
weak Perfect Forward Secrecy	00:00:00.01	00:00:00.01	00:00:00.01	00:00:00.01	00:00:00.01	wPFS	non-interference
Unilateral UKS resilience	00:00:00.02	00:00:00.04	00:00:00.05	00:00:00.08	00:00:00.09	UKS	event property
Bilateral UKS resilience	00:00:00.08	00:00:00.10	00:00:00.10	00:00:00.07	00:00:00.08		event property
Impersonation resilience	00:00:00.14	00:00:00.17	00:00:00.14	00:00:00.03	00:00:00.03	IMP	correspondences
Swap Sessions resilience	00:00:00.10	00:00:00.14	00:00:00.13	00:00:00.08	00:00:00.09	SS	event property
Weak Entity Agreement	00:00:00.20	00:00:00.31	00:00:00.22	00:00:00.13	00:00:00.14	WA	correspondences
Strong Entity Agreement	00:00:00.18	00:00:00.28	00:00:00.23	00:00:00.15	00:00:00.16	SA	correspondences
Non-malleability	00:00:01.11	00:00:10.23	00:00:14.11	00:01:57.02	00:02:48.87	MAL	event property
Total time	**00:00:04.15**	**00:00:18.11**	**00:04:04.30**	**01:18:08.47**	**06:08:11.39**	**07:30:46.42**