











Learner statistics for learned state machines of SSH server implementations. For each implementation and key exchange, the table lists the required number of iterations of the learner, the number of queries answered by the SUL, the time in seconds required to learn the state machine, and the number of states and transitions in the resulting state machine. Note that an increased number of iterations indicates one or multiple cache conflicts. The number of queries does not include queries answered by the cache without querying the SUL directly. The number of transitions lists both, total and distinct transitions, where a distinct transition resembles all transitions with the same input and output state but different input and output symbols. Rows in gray represent learning attempts that were terminated due to repeated cache conflicts after an hour of learning time. In these cases, the number of states and transitions refers to the last hypothesis before termination.

Implementation	Version	OS	KEX	# Iterations	# Queries		Time [s]	# States	# Transitions	
					Learn.	Equiv.			Total	Distinct
AsyncSSH	2.20.0		DH	6	1,506	2,088	372	14	1,316	41
			DHGEX	7	1,296	2,297	356	14	1,316	40
			ECDH	6	816	2,084	285	10	940	29
			PQ-Hybrid	6	1,685	2,081	448	13	1,222	36
			RSA	14	881	2,152	338	10	940	29
Bitwise SSH	9.43		DH	7	1,256	6,768	495	11	1,023	29
			DHGEX	38	1,990	6,847	708	18	1,674	56
			ECDH	5	1,058	6,762	557	9	837	22
Dropbear	2025.87		DH	13	1,280	5,488	1,457	10	940	29
			ECDH	6	1,001	5,579	2,789	9	846	25
			PQ-Hybrid	6	1,030	5,958	1,519	9	846	25
Erlang SSH	5.2.8		DH	14	3,582	8,049	753	16	1,504	58
			DHGEX	8	3,411	6,686	708	14	1,316	43
			ECDH	20	3,013	6,680	619	11	1,034	35
LANCOM LCOS	10.90.0126 Rel		DH				> 3,600	57	5,358	458
			DHGEX				> 3,600	35	3,290	213
			ECDH				> 3,600	14	1,316	75
			PQ-Hybrid				> 3,600	26	2,444	151
Golang x/crypto/ssh	0.37.0		DH	5	309	1,283	141	8	744	21
			ECDH	5	304	1,286	138	8	744	20
libssh	0.11.1		DH	4	1,462	10,675	698	10	940	28
			DHGEX				> 3,600	19	1,786	84
OpenSSH	9.9p2		ECDH	4	1,355	10,639	688	9	846	23
			DH	52	4,036	11,704	929	13	1,222	37
			DHGEX	6	3,085	10,570	915	13	1,222	35
			ECDH	6	1,960	10,592	840	10	940	26
Tectia SSH	6.6.5.353		PQ-Hybrid	13	2,495	11,454	815	10	940	26
			DH				> 3,600	37	3,478	172
			DHGEX				> 3,600	46	4,324	214
			ECDH				> 3,600	20	1,880	70
TinySSH	20250201		PQ-Hybrid				> 3,600	19	1,786	84
			ECDH	5	819	1,146	139	7	658	16
			PQ-Hybrid	5	819	1,135	129	7	658	16