

COMPARISON OF PRACTICAL DIFFIE-HELLMAN-BASED PAKE PROTOCOLS PROVEN SECURE IN THE BPR MODEL

	Rounds / Flows	Assumptions ^a				Time ^c
		CRS	ROM	ICM	AAM	
J-PAKE with Schnorr [24]	2 / 4 or 3 / 3		✗		✗	DSDH or (CSDH + DDH) 28 exp (12 exp + 8 mexp)
EKE [5], [7]	1 / 2			✗		CDH 4 exp + 2 memb + 2 enc
SPEKE [29], [35]	1 / 2		✗			DIDH ^d 4 exp + 2 memb
PPK [10]	2 / 2		✗			DDH 6 exp + 2 memb
SPAKE2 [3]	1 / 2		✗			CDH 4 exp + 2 memb