		Assumptions[a]			Complexity	
	Rounds / Flows	ROM	AAM		Communication[b]	Time[c]
J-PAKE with Schnorr	2 / 4 or 3 / 3	✗	✗	DSDH or (CSDH + DDH)	$12 \times G + 6 \times \mathbb{Z}_p$	28 exp
SPEKE	1 / 2	✗		DIDH[d]	$2 \times G$	8 exp
PPK	2 / 2	✗		DDH	$2 \times G$	6 exp

[a] *CRS*: common reference string, *ROM*: random-oracle model, *ICM*: ideal-cipher model, *AAM*: algebraic-adversary model;

[b] G: group elements, $\mathbb{Z}_p$: scalars;

[c] *exp*: number of exponentiations;

[d] *DIDH*: decision inverted-additive Diffie-Hellman assumption