Comparison of practical Diffie-Hellman-based PAKE protocols proven secure in the BPR model [5]

		Assumptions[a]					Complexity	
	Rounds / Flows	CRS	ROM	ICM	AAM		Communication[b]	Time[c]
J-PAKE with Schnorr [24]	2 / 4 or 3 / 3		✗		✗	DSDH or (CSDH + DDH)	$12 \times G + 6 \times \mathbb{Z}_p$	28 exp (12 exp + 8 mexp)
EKE [5], [7]	1 / 2			✗		CDH	$2 \times G$	4 exp + 2 memb + 2 enc
SPEKE [29], [35]	1 / 2		✗			DIDH[d]	$2 \times G$	4 exp + 2 memb
PPK [10]	2 / 2		✗			DDH	$2 \times G$	6 exp + 2 memb
SPAKE2 [3]	1 / 2		✗			CDH	$2 \times G$	4 exp + 2 memb
GK-SPOKE [1], [21], [30]	2 / 2	✗				DDH + PRG[e]	$6 \times G$	17 exp (4 exp + 7 mexp) + 6 memb
GL-SPOKE [1], [18], [32]	2 / 2	✗				DDH	$7 \times G$	21 exp (4 exp + 7 mexp) + 7 memb
KV-SPOKE [1], [33]	1 / 2	✗				DDH	$10 \times G$	30 exp (2 exp + 12 mexp) + 10 memb

[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; *mexp*: number of multi-exponentiations; *memb*: verification of the membership of a group element to the cyclic group G. For elliptic curve with small co-factor, this only costs a small number of additions on the curve, but for subgroups of $\mathbb{Z}_q$ (q being a prime larger than p, the order of the group G), this costs an exponentiation (with exponent $p - 1$); *enc*: encryption with the ideal cipher; multiplications, hash evaluations, and PRG evaluations are omitted;
[d] *DIDH*: decision inverted-additive Diffie-Hellman assumption [35] (see Fig. 2 and the Appendix);
[e] *PRG*: pseudo-random generator.