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

| | | Assumptions[a] | | | | |
|---|---|---|---|---|---|---|
| | Rounds / Flows | ROM | ICM | AAM | | Time[c] |
| J-PAKE with Schnorr [24] | 2 / 4 or 3 / 3 | ✗ | | ✗ | DSDH or<br>(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 |