SPEKE (with strong password-only authentication)

Protocol Purpose

Strong Password-Only Authenticated Key Exchange

Definition Reference

http://citeseer.ist.psu.edu/jablon96strong.html

Model Authors

- Haykal Tej, Siemens CT IC 3, 2003
- Sebastian Mödersheim, ETH Zürich, December 2003

Alice&Bob style

```
A -> B : exp(S(A,B), Na)     |    key exchange part
B -> A : exp(S(A,B), Nb)     |

               both A and B compute
```

```
      State’:= 3

end role
```

sec_r_Ca,sec_r_Cb