

Alice

Bob

g^x

$g^y, B, \text{SIG}_B(g^x, g^y), \text{MAC}_{K_m}(B)$

$A, \text{SIG}_A(g^y, g^x), \text{MAC}_{K_m}(A)$

Sigma protocol is defined in <http://webee.technion.ac.il/~hugo/sigma-pdf.pdf> p17