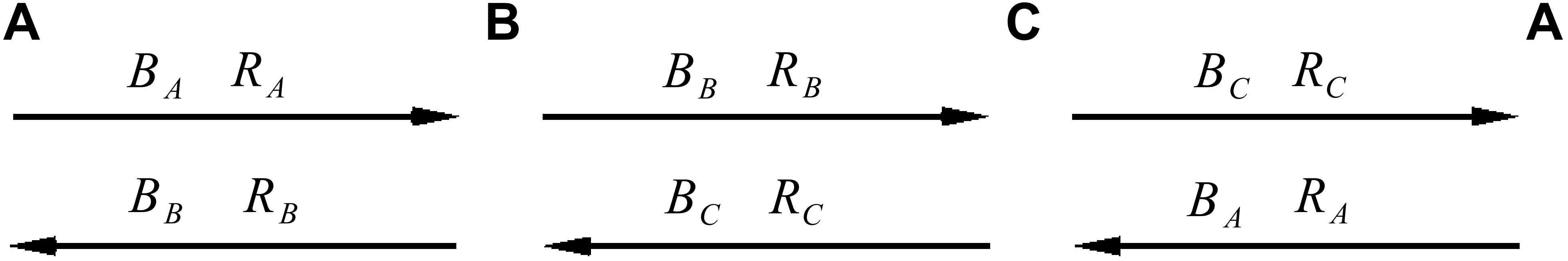
Authenticated BD Group Key Exchange

Each participant generates: $\left(\boldsymbol{b}_j, \boldsymbol{B}_j\right), \left(r_j, R_j\right), \left(h_j, H_j\right)$



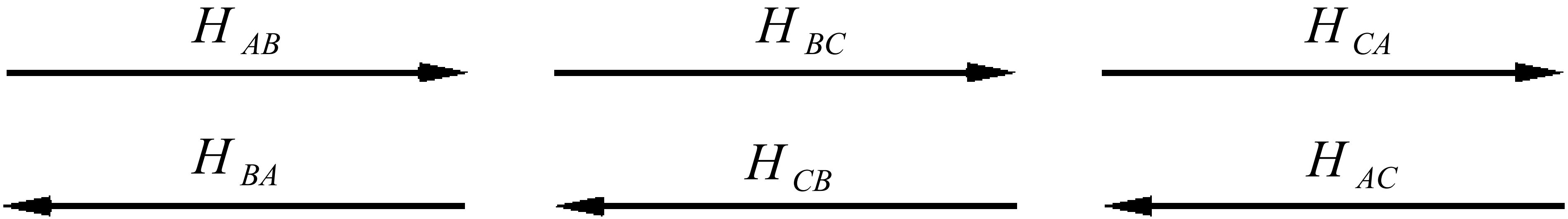
A **B** **C** **A**

B_A R_A B_B R_B B_C R_C

B_B R_B B_C R_C B_A R_A

Compute: $k_{ji} = \text{hash}\left(\text{ECDH}\left(b_j, R_i\right) \parallel \text{ECDH}\left(r_j, B_i\right) \parallel \text{ECDH}\left(r_j, R_i\right)\right)$

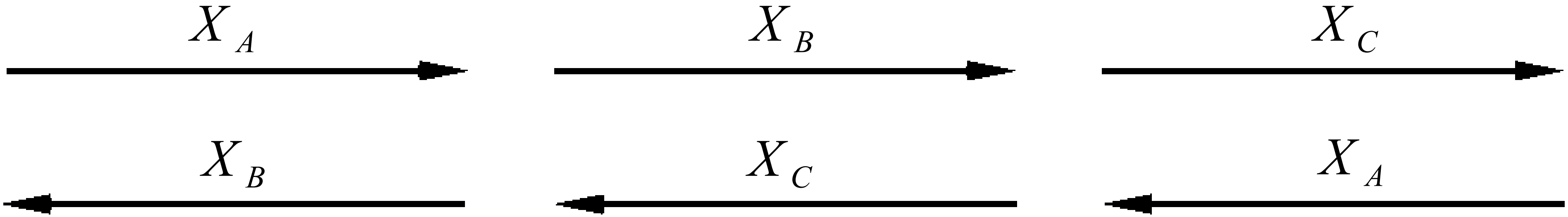
$H_{ji} = H_j \parallel \text{hmac}\left(k_{ji}, H_j\right)$



H_{AB} H_{BC} H_{CA}

H_{BA} H_{CB} H_{AC}

Compute: $X_j = BD_1\left(h_j, \left\{H_i\right\}\right)$



X_A X_B X_C

X_B X_C X_A

Compute: $\text{MK} = BD_2\left(h_j, \left\{X_i\right\}\right)$