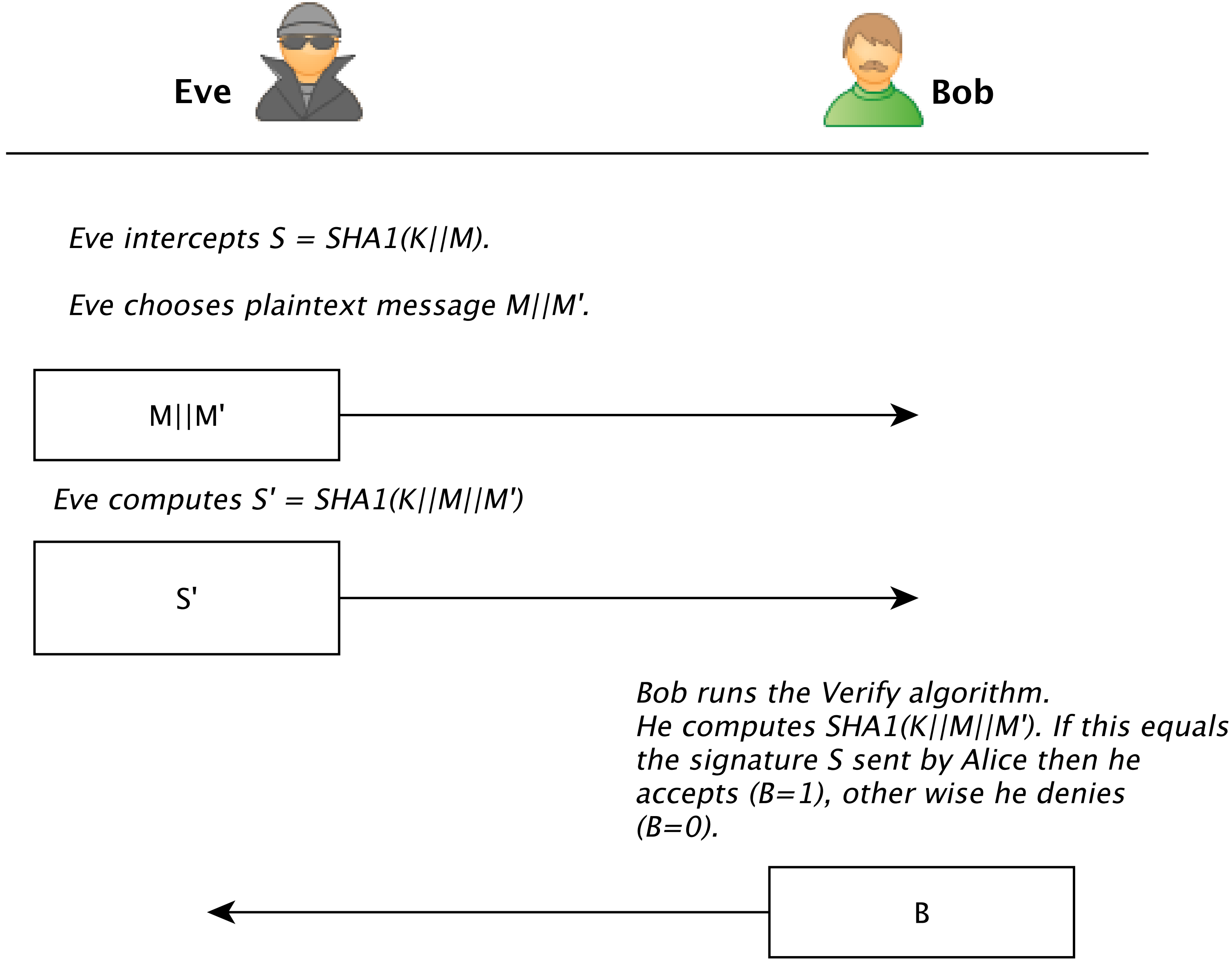

Eve

Bob

Eve intercepts S = SHA1(K||M).

Eve chooses plaintext message M||M'.

M||M'

Eve computes S' = SHA1(K||M||M')

S'

Bob runs the Verify algorithm.
He computes SHA1(K||M||M'). If this equals the signature S sent by Alice then he accepts (B=1), other wise he denies (B=0).

B