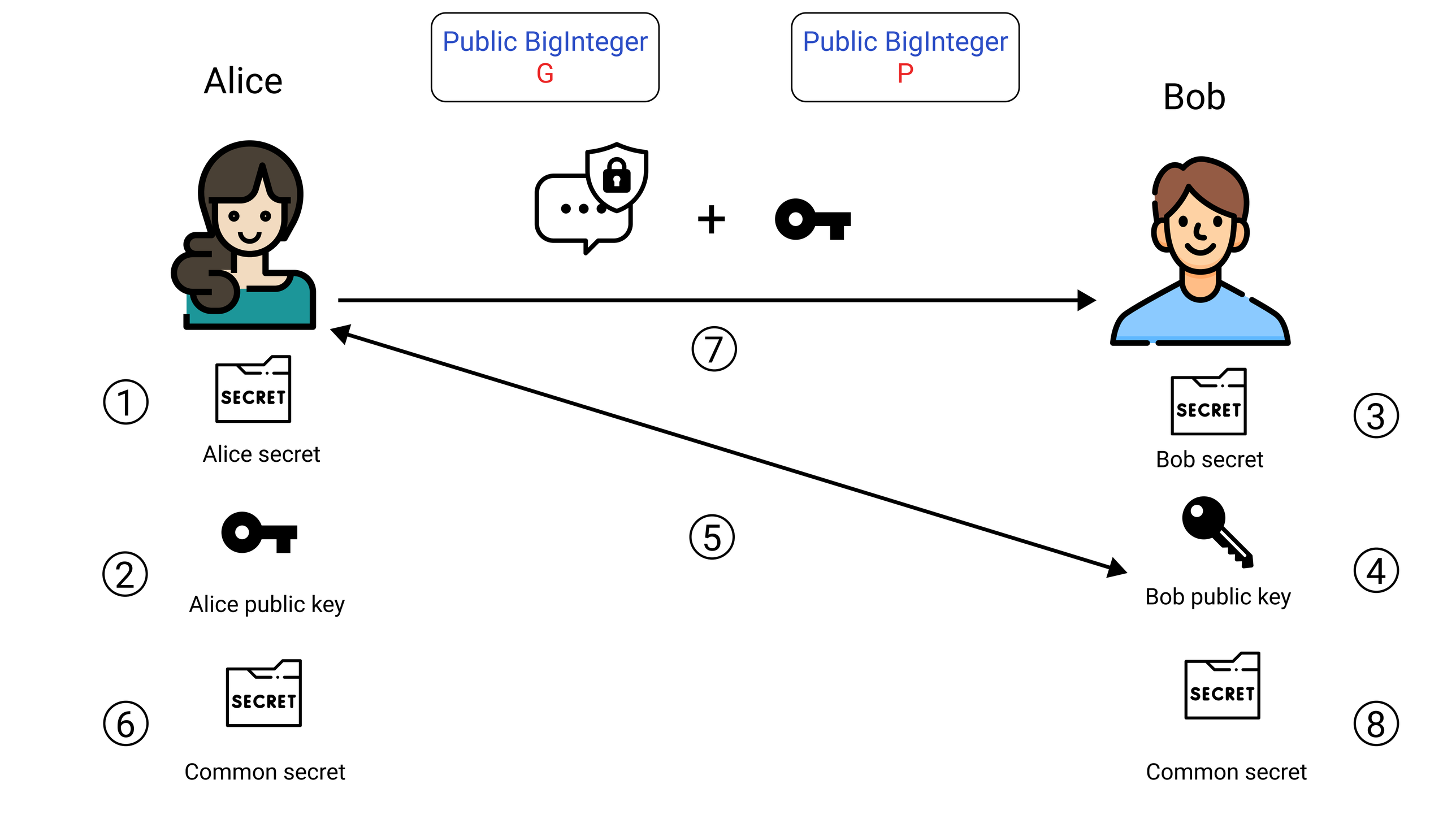
Public BigInteger
G
Public BigInteger
P
Alice
Bob
+
7
SECRET
1
Alice secret
SECRET
3
Bob secret
2
Alice public key
5
4
Bob public key
SECRET
6
Common secret
SECRET
8
Common secret