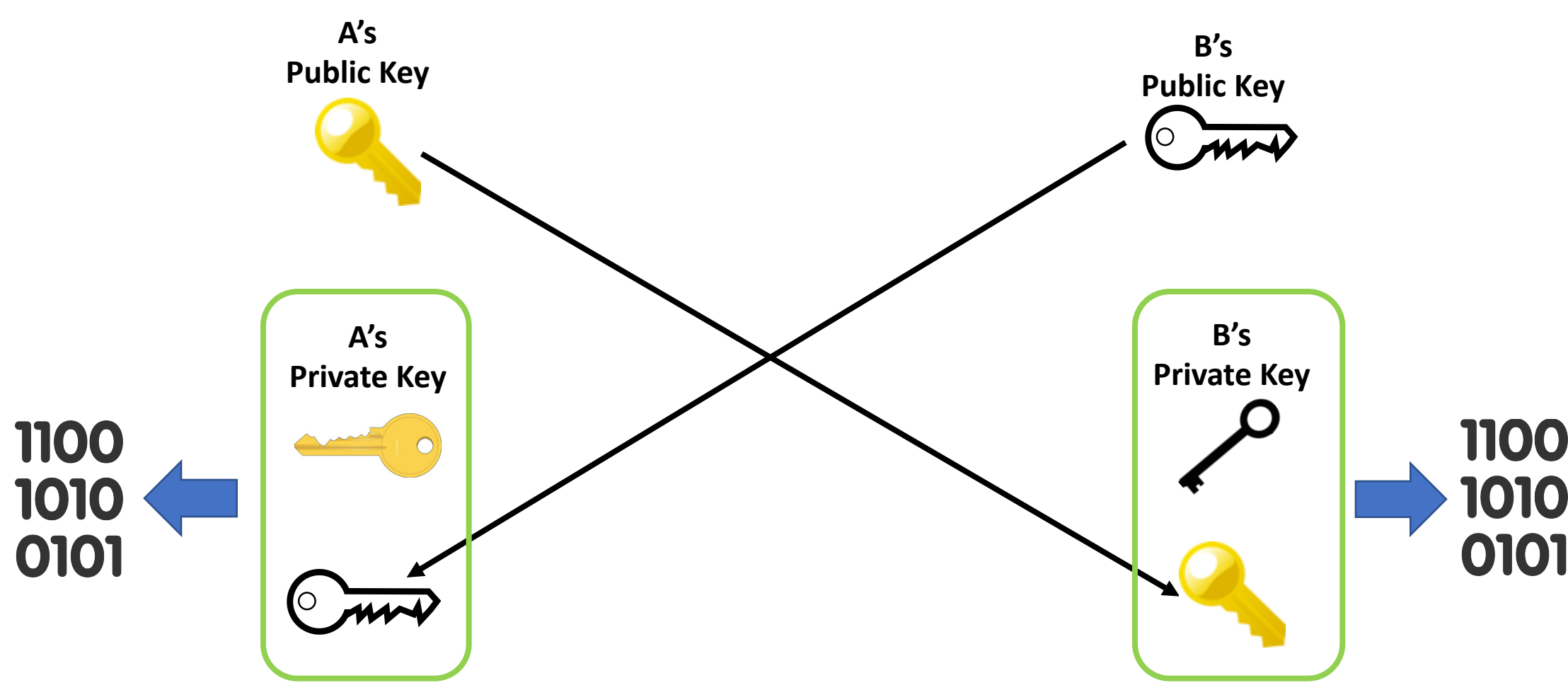

Just by simply exchange the public key each other, one can calculate the shared random bits from the other's public key and its own private key.