An Unconditional Secure Key-Exchange

If we use in a one-time pad as message and key a true pure random string, we can prove this is an unconditional secure key-exchange using the key as a fixed key and the message as a one-time key.

Proof

Definitions:

X = Message (this is a true pure random string which is the one-time key)
Y = Ciphertext (this is the encrypted true pure random string which is the one-time encrypted key)
Z = Key (this is a true pure random string which is used as a fixed key)

For a general cipher following information-theoretic equalities hold:

$H(X|Y,Z)=0$, X can be recovered from Y and Z
$H(Y|X,Z)=0$, the cipher text is a function of the plain text and the key
$I(X,A;Z)=0$, the plain texts and the key are independent

For the XOR of the one-time pad following information-theoretic equalities hold:

$H(Y|X,Z)=0$
$H(X|Y,Z)=0$
$H(Z|X,Y)=0$

The XOR of 2 pure random sequences is a pure random sequence, because XOR is both an injective and surjective function. Because $Y=XOR(Z,X)$ and Z and X are independent pure true random strings, following information-theoretic equalities hold:

$H(Y)=H(X)$
$H(Y)=H(Z)$

If we do the one time pad again with a different message A and the same key Z:

$H(A|B,Z)=0$, A can be recovered from B and Z
$H(B|A,Z)=0$, the cipher text is a function of the plain text and the key
$I(A,X;Z)=0$, the plain texts and the key are independent

Equalities for the XOR:

$H(B|A,Z)=0$
$H(A|B,Z)=0$
$H(Z|A,B)=0$

Equalities for the pure random strings:

$H(B)=H(A)$
$H(B)=H(Z)$

In general, the plain texts are independent:

$I(A;X)=0$

Given the information-theoretic equalities above we can use an information-theoretic inequality prover ([1],[2]) to prove the following information-theoretic equations:

$I(X;Y,B)=0$ and $I(A;Y,B)=0$ so the key-exchange is perfectly secure.
$I(Z;Y,B)=0$, so an attacker knowing only B and Y learns nothing of Z.

So this Key-Exchange is unconditional secure!

References

[1] xitip.epfl.ch
[2] Information Theory and Network Coding, Raymond Yeung