Title: PSI 2018/2019 - Quantum Information Review - Lecture 13

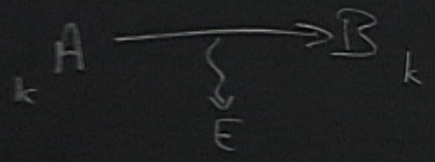
Speakers: Daniel Gottesman

Collection: PSI 2018/2019 - Quantum Information Review (Gottesman)

Date: March 20, 2019 - 11:30 AM

URL: http://pirsa.org/19030050

One-time pad



symmetric cryptosystem

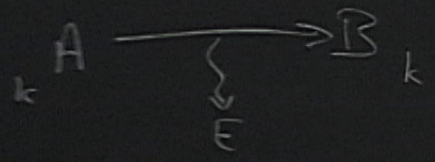
A&B share same private key k

Key k: n random bits, unknown to Eve

Encryption: A has message m (n bits long)

Ciphertext is $c = m \oplus k$, bitwise XOR

One-time pad



symmetric cryptosystem

A&B share same private key k

Key k: n random bits, unknown to Eve

Encryption: A has message m (n bits long)

Ciphertext is $e = m \oplus k$, bitwise XOR

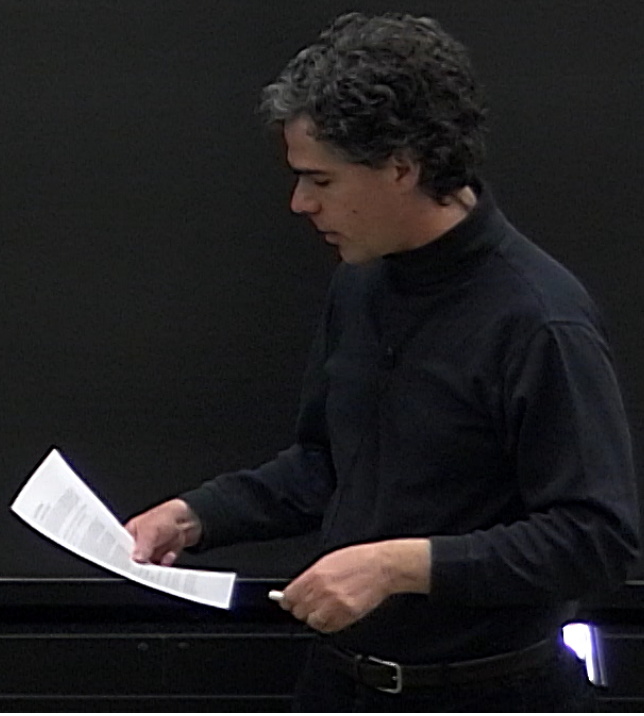
Decryption: $e \longmapsto e \oplus k = m$

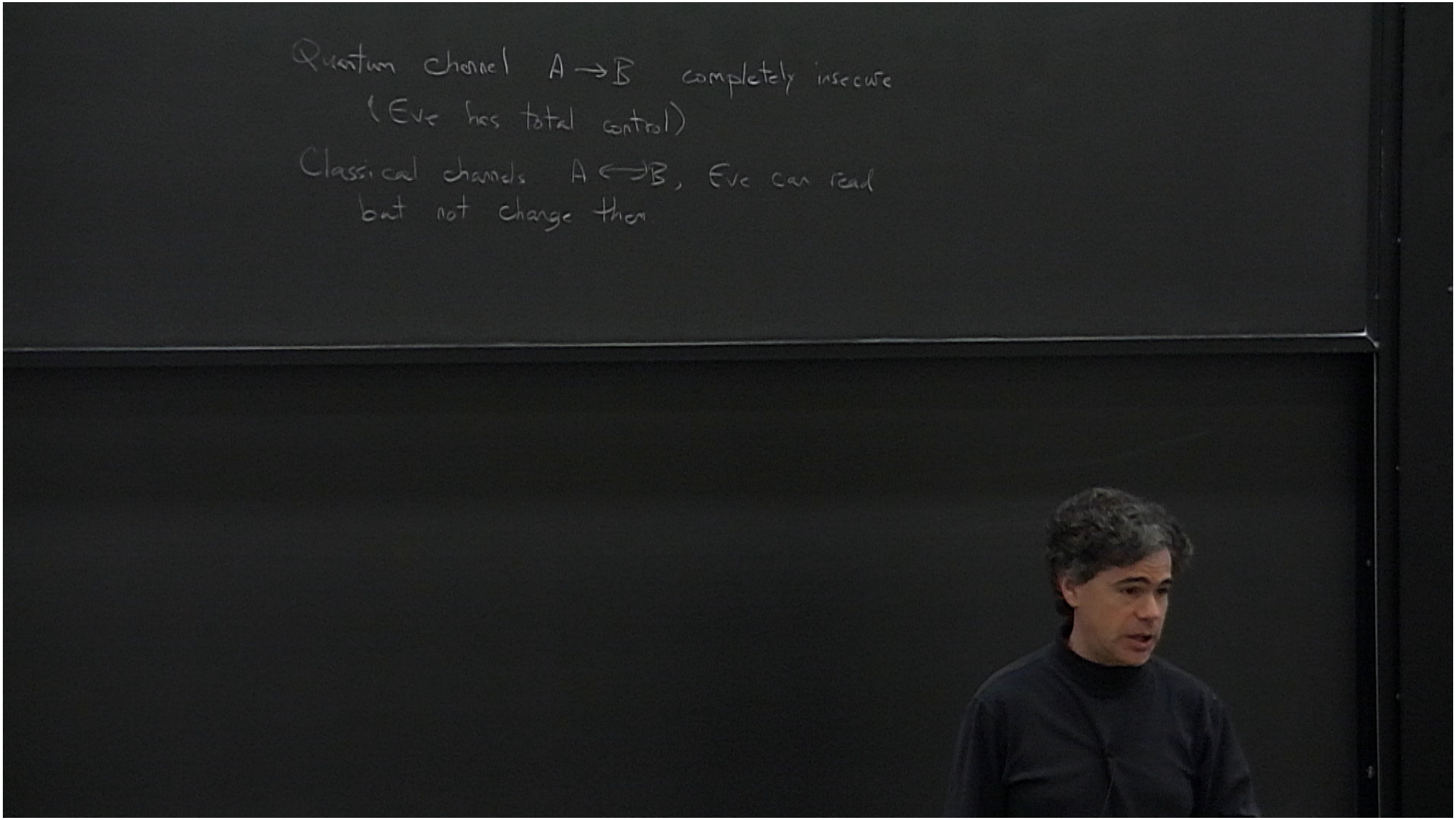
Quantum Key Distribution

BB 84 protocol:

1. Alice generates N random bit pairs (a_i, r_i).
2. Each pair specifies a quantum state. Alice creates these states & sends them to Bob over the quantum channel.

a_i	r_i	state
0	0	$\|0\rangle$
0	1	$\|1\rangle$
1	0	$\|+\rangle$
1	1	$\|-\rangle$

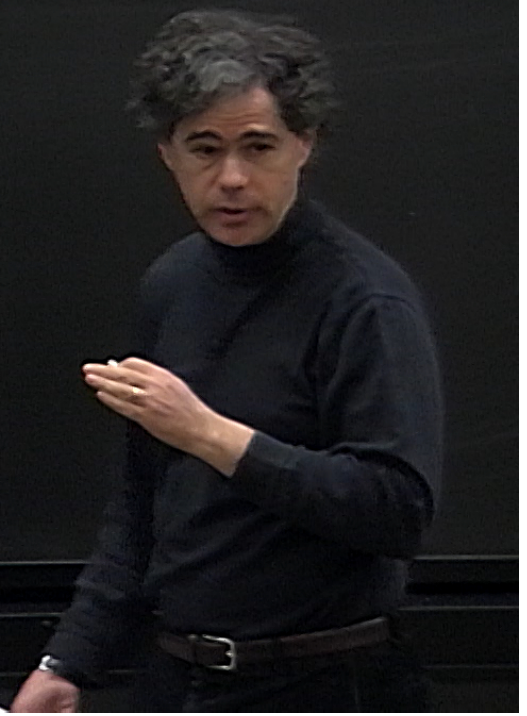



Quantum channel A → B completely insecure
(Eve has total control)
Classical channels A ⟷ B, Eve can read
but not change them

but not change them

3. Bob chooses N random bases b_i and measures qubit i in basis b_i, getting result s_i.

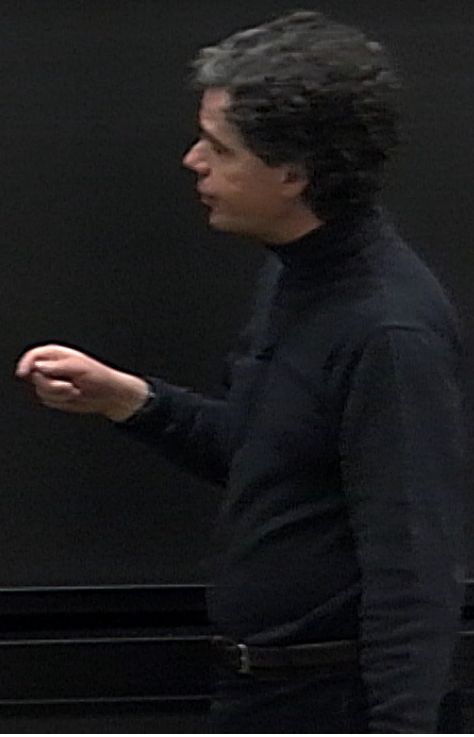
4. Alice & Bob announce a_i & b_i over the classical channel. They do <u>not</u> announce r_i & s_i.



but not change them.

3. Bob chooses N random bases b_i and measures qubit i in basis b_i, getting result s_i.

4. Alice & Bob announce a_i & b_i over the classical channel. They do not announce r_i & s_i. If $a_i = b_i$, they keep bit i. If $a_i \neq b_i$, they discard bit i. The bits r_i & s_i that they keep are called the raw key



N random bases b_i and

in basis b_i, getting result s_i.

announce a_i & b_i over the classical

announce r_i & s_i. If

If $a_i \neq b_i$, they

The bits r_i & s_i that they

raw key

5. Alice & Bob choose a random subset, say 50% of the raw key, & announce r_i and s_i over the classical channel. They compare & calculate the error rate. If it is too high,

N random bases b_i and

i in basis b_i, getting result s_i.

a_i & b_i over the classical

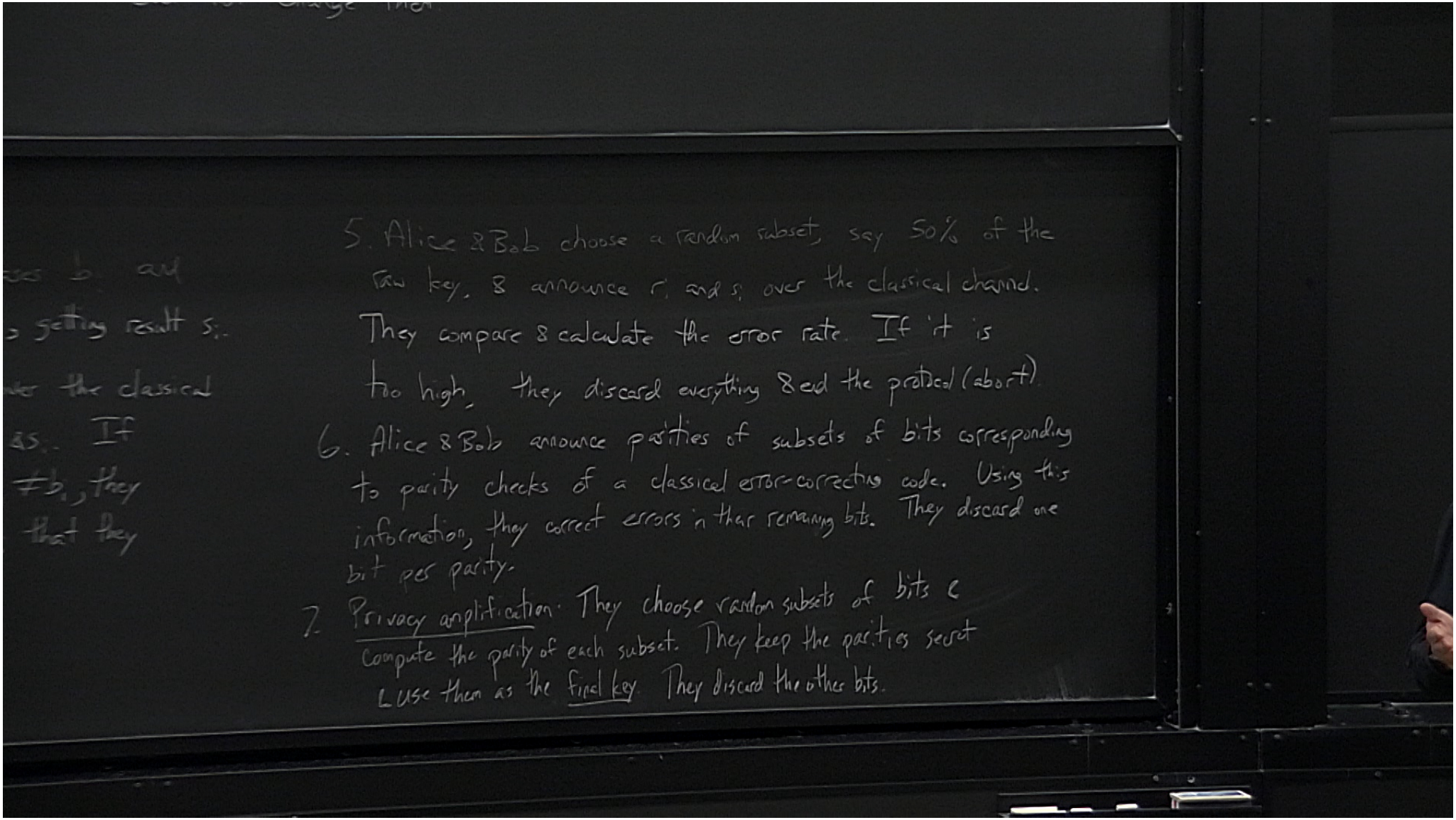
announce r_i & s_i. If

If $a_i \neq b_i$, they

The bits r_i & s_i that they

raw key

5. Alice & Bob choose a random subset, say 50% of the raw key, & announce r_i and s_i over the classical channel. They compare & calculate the error rate. If it is too high, they discard everything & end the protocol (abort).
6. Alice & Bob announce parities of subsets of bits corresponding to parity checks of a classical error-correcting code. Using this information, they correct errors in their remaining bits

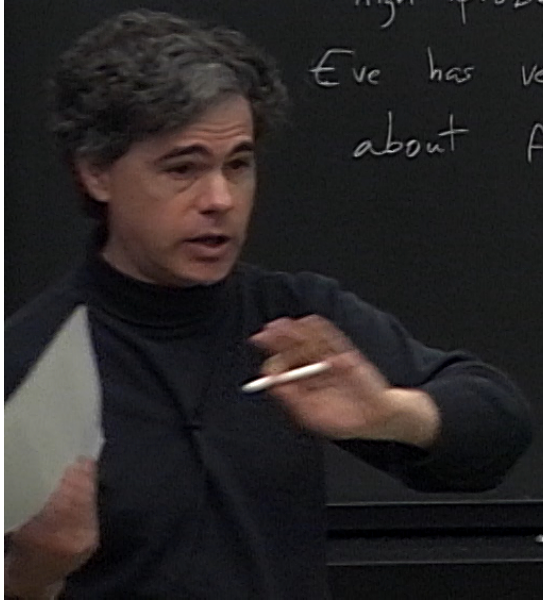

5. Alice & Bob choose a random subset, say 50% of the raw key, & announce r_i and s_i over the classical channel. They compare & calculate the error rate. If it is too high, they discard everything & end the protocol (abort).
6. Alice & Bob announce parities of subsets of bits corresponding to parity checks of a classical error-correcting code. Using this information, they correct errors in their remaining bits. They discard one bit per parity.
7. Privacy amplification: They choose random subsets of bits & compute the parity of each subset. They keep the parities as secret & use them as the final key. They discard the other bits.

0	1	$\|1\rangle$
1	0	$\|+\rangle$
1	1	$\|-\rangle$

Security condition

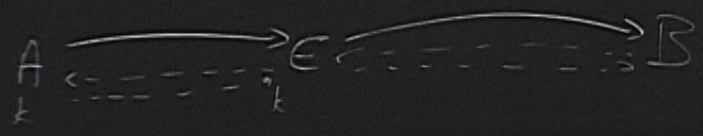
Either Alice & Bob reject the key w/ high probability $(1 - 2^{-s})$ or

Eve has very little information (2^{-s} bits) about Alice & Bob's key.



7. Privacy amplification. They choose random subsets of bits &
Compute the parity of each subset. They keep the parities secret
& use them as the final key. They discard the other bits.

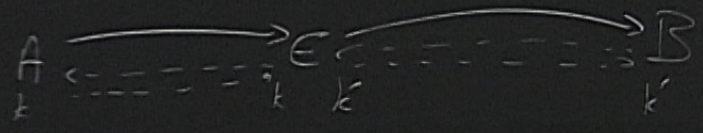
Suppose Eve could change classical channel:



"man-in-the-middle attack"

7. Privacy amplification. They choose random subsets of bits &
Compute the parity of each subset. They keep the parities secret
& use them as the final key. They discard the other bits.

Suppose Eve could change classical channel:



"Man-in-the-middle attack"

Authentication protocol.

Secret-key protocols w/
information-theoretic security.