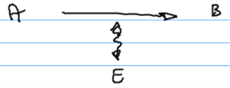
CRYPTOGRAPHY

N&C 12.6

Gisin et al. RMP '02

goal:



Private key crypt. (class.)

n-bit message, A → B
n-bit key, shared by A & B

A

$s_i = k_i \oplus m_i$

m 0101
k 1001 } s 1100

B

$m_i = s_i \oplus k_i$

m = 1100 / 1001 = 0101

- one-time path → provably secure
- E can at best jam comm.
- not secure if key is reused / stolen (copied)

Public key crypt. (class.)

A has private key (part)
announces public key (part)

B encrypts using public key, sends enc. mess. to A

A decode using private key

- e.g. RSA, based on prime numbers
- pretty secure, but not proven
- slow, key distribution

Quantum crypt.

→ create private key via public q. channel

idea: cannot distinguish non-orthogonal states without disturbing them

$|\psi\rangle, |\varphi\rangle \qquad \langle\psi|\varphi\rangle \neq 0$

most general q. process that doesn't disturb them

$$|\psi\rangle|u\rangle \xrightarrow{U} |\psi\rangle|v\rangle$$
$$|\varphi\rangle|u\rangle \longrightarrow |\varphi\rangle|v'\rangle$$

$$\langle\psi|\varphi\rangle\underbrace{\langle u|u\rangle}_{=1} = \langle\psi|\varphi\rangle\langle v|v'\rangle$$

BB 84 (Bennett & Brassard, 1984)

A sends $|\updownarrow\rangle$ OR $|\nearrow\rangle$ → "0"   random
$|\leftrightarrow\rangle$ OR $|\nwarrow\rangle$ → "1"   basis

B measures in $\{\updownarrow, \leftrightarrow\}$ OR $\{\swarrow, \nwarrow\}$ random

if send & meas. basis are same → correll.
≠ → un corr.

A & B announce basis they used; keep bits
if basis was same
→ 50% useful bits

E intercept & resend

50% unnoticed
50% causes errors
} E learns 50% inf.
causes 25% error rate

E can intercept/resend only fraction of bits
→ E learns less, perturbs less.

Error correction

- errors in source, channel, detector
- errors from E

$\Rightarrow$ A & B share bits, but with mistakes

e.g. A & B compare XOR of pairs of bits

Privacy amplification

$\rightarrow$ to lower bound on what E knows

e.g. A & B pick random pair of bits,
use XOR of these bits.

if E knows 60% of each bit

$\rightarrow$ $0.6^2 + 0.4^2$ of XOR

$= 52\%$

EPR protocol (Ekert 91)

$\frac{|00\rangle + |11\rangle}{\sqrt{2}}$ shared by A & B

- A & B each measure 1 qbit in random basis
- if basis same → correll.
  ≠ → no corr.

- EPR can be created by A, B, C

Security

- ideal
- realistic

- coherent attacks
- E can choose her meas. basis after A & B announced basis
- multiple photon pulses
- E improves equipment of A & B
- E could make equipment

In the end, E's knowledge bound ~ $2^{-\ell}$

- authentication