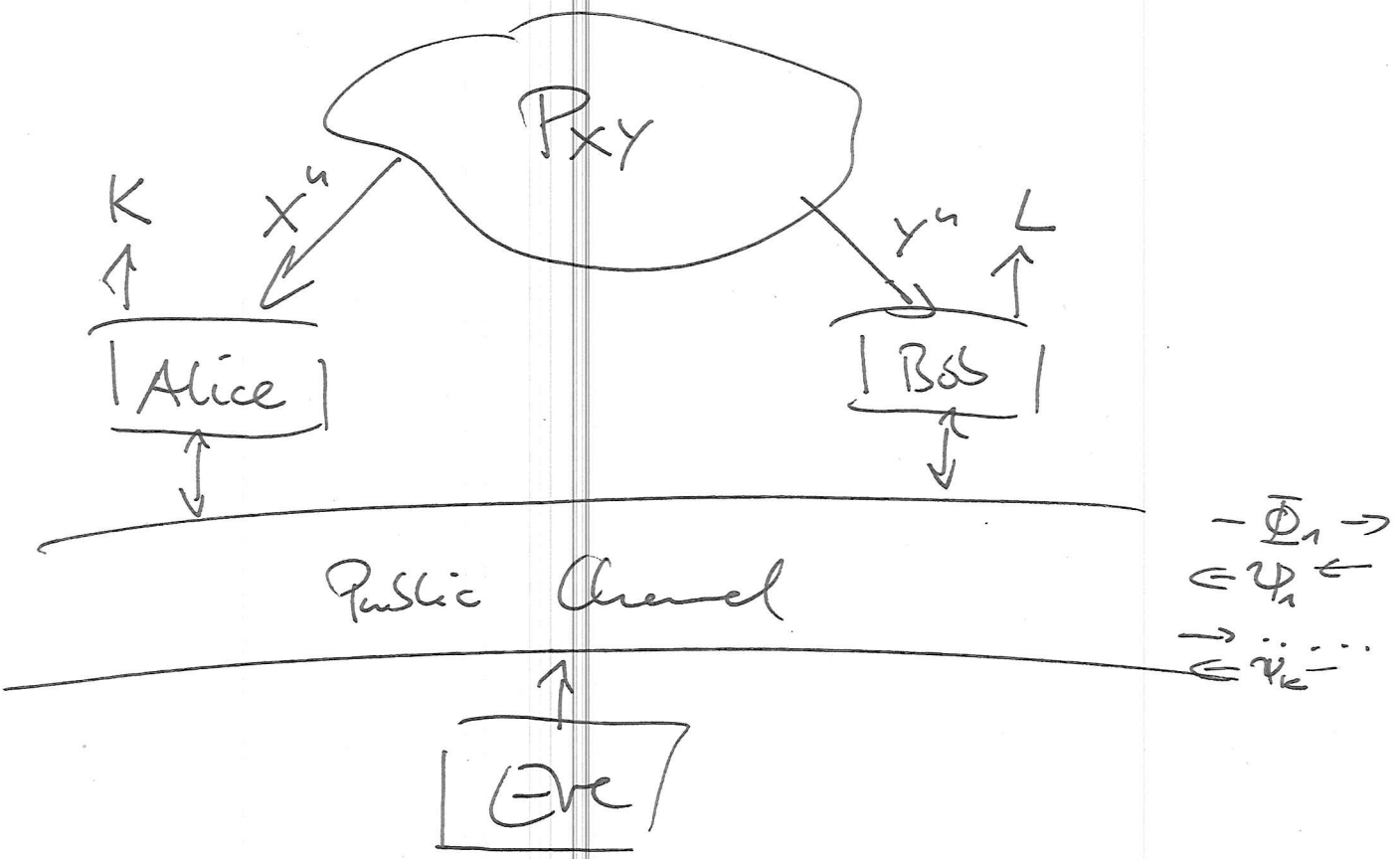
Secret Key Generation



. Alice & Bob have access to DMS P_{XY}
A observes X^n
B observes Y^n
They want to generate a common secret key
by exchanging messages $\underset{\text{(forward)}}{\Phi_i}$ and $\underset{\text{(backward)}}{\Psi_i}$ $i = 1, \ldots, k$

To include randomized strategies, both A & B can generate independent RVs M_x and M_y.

Secret-key generation protocol:

1. Initialization:
   A & B generate RVs M_x and M_y such that M_x, M_y and X^n, Y^n are mutually independent

2. First exchange:
   Both A&B exchange messages $\overline{\Phi}_1 = \overline{\Phi}_1(M_x, X^n)$ and $\overline{\Psi}_1 = \overline{\Psi}_1(M_y, Y^n)$

3. i-th exchange:
   $\overline{\Phi}_i = \overline{\Phi}_i(M_x, X^n, \overline{\Psi}^{i-1})$
   $\overline{\Psi}_i = \overline{\Psi}_i(M_y, Y^n, \overline{\Phi}^{i-1})$

4. after k exchanges:
   Compute secret key based on the protocol (by using so-called hash-functions) as
   $K = K(M_x, X^n, \overline{\Psi}^k)$
   $L = L(M_y, Y^n, \overline{\Phi}^k)$

Def: A SK rate R_{key} is achievable if for any $\varepsilon > 0$ and sufficiently large n there is a permissible SK generation protocol such that K and L satisfy

$$P\{K \neq L\} < \varepsilon \qquad \text{(same key)}$$

$$I(\Phi^n, \Psi^n; K) < \varepsilon \qquad \text{(secrecy)}$$

$$\frac{1}{n} H(K) > R_{key} - \varepsilon$$

$$\frac{1}{n} \log |\mathcal{K}^n| < \frac{1}{n} H(K) + \varepsilon \qquad \text{(nearly uniform)}$$

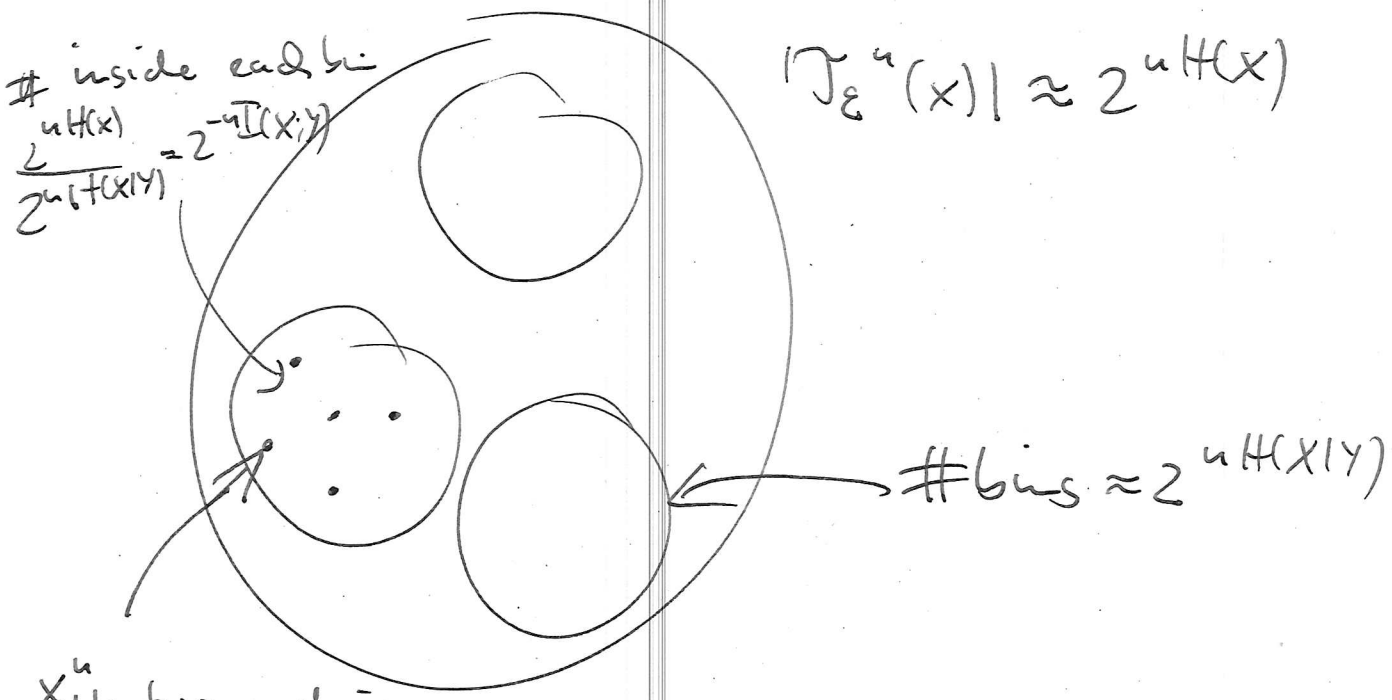
Theorem:
The SK capacity of the source model is

$$C_{key} = I(X;Y)$$

and is achievable by using a single forward or backward transmission only.

Proof:
- Achievability is based on Slepian-Wolf coding.
- all typical sequences x^n are allocated randomly & uniformly into $2^{nH(X|Y)}$ bins
- each bin has $\sim 2^{nI(X;Y)}$ elements
- Alice sends the bin number of X^n to Bob and Bob reconstructs x^n with its side information y^n (SW coding)

- public communication involves only the bin index, which is independent of the key index inside the bin → Eve cannot learn anything about the key!



X_{bk}^n two indices:

b: bin index (sent over public channel)

k: actual key index

- Now for the converse--

Lemma:

Let U and V be arbitrary RVs, and let $\Phi_1, \ldots, \Phi_k$ and $\psi_1, \ldots, \psi_k$ be such that for every $i \le k$ Φ_i is a function of U and ψ^{i-1} and ψ_i is a function of V and Φ^{i-1}. Then

$$I(U; V \mid \Phi^k, \psi^k) \le I(U; V)$$

Proof:

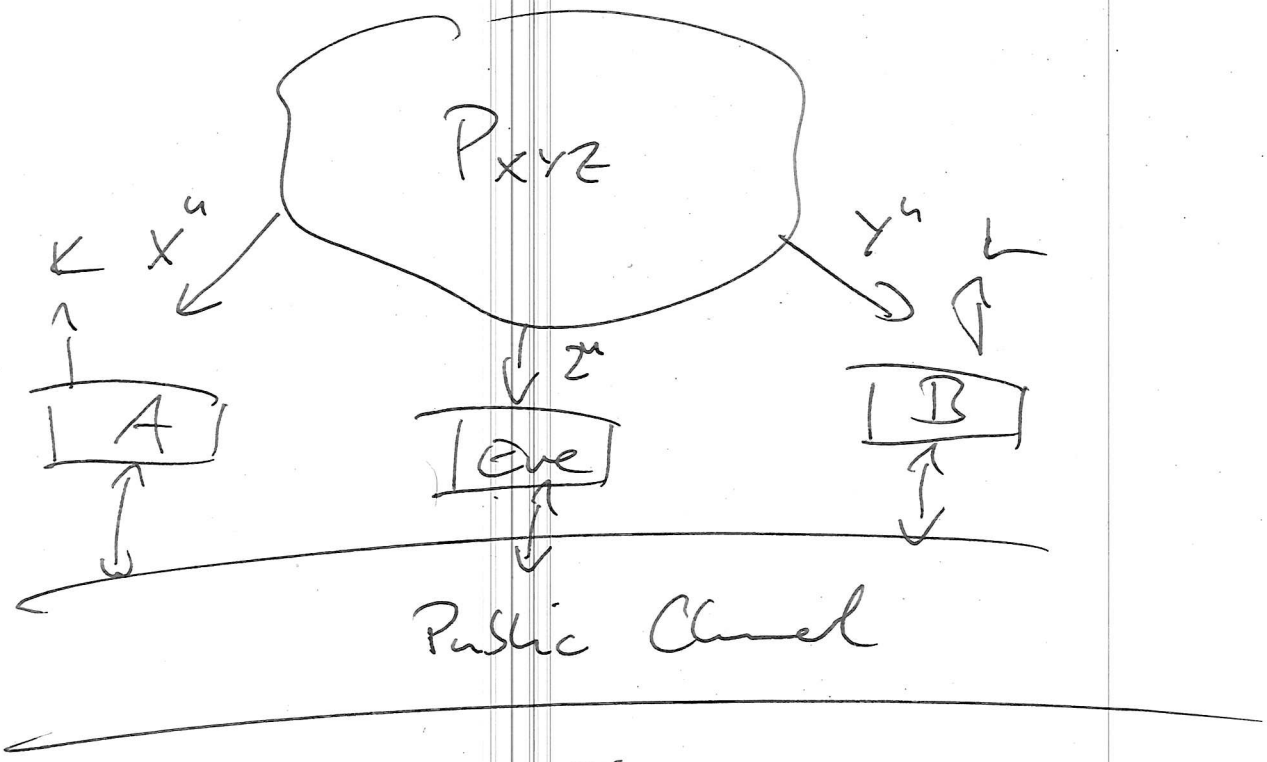
$$\begin{aligned} I(U; V \mid \Phi^k \psi^k) &= I(U; V \mid \Phi^{k-1} \Phi_k \psi^{k-1} \psi_k) \\ &\le I(U \Phi_k ; V \mid \Phi^{k-1}, \psi^{k-1}, \psi_k) \\ &\le I(U \Phi_k ; V \psi_k \mid \Phi^{k-1} \psi^{k-1}) \\ &= I(U; V \mid \Phi^{k-1}, \psi^{k-1}) \end{aligned}$$

where the last step follows from the assumption that Φ_k is a function of (U, ψ^{k-1}) and ψ_k a function of (V, Φ^{k-1}).

Back to the converse

$$\begin{aligned} n_k H(K) &= n_k I(K; L) + \underbrace{n_k H(K \mid L)}_{\le \varepsilon \text{ (Fano)}} \\ &\le n_k I(K; L \Phi^k \psi^k) \\ &\le n_k I(K; L \mid \Phi^k \psi^k) + I(K; \Phi^k \psi^k) \\ &\le n_k I(K; L \mid \Phi^k \psi^k) \\ &\le n_k I(M_X, X^n; M_Y Y^n \mid \Phi^k \psi^k) && \text{since } K = (M_X, X^n, \Phi^k) \\ &\le n_k I(M_X X^n; M_Y Y^n \mid) && \text{(Lemma above)} \\ &= n_k I(X^n; Y^n) = n I(X; Y) && \text{(independence)} \end{aligned}$$

Extension SW (source coding)



secrecy becomes: $I(\Phi^\xi, \Psi^\xi, Z^n; K) < \varepsilon$

Theorem:
An achievable SK rate for the SW model is

$$I(X;Y) - I(X;Z) \qquad \text{(forward)}$$

or

$$I(X;Y) - I(Y;Z) \qquad \text{(backward)}$$

Proof:
same ideas as for S but using a wiretap code inside each bin: