Secret Key Agreement with Rate-Limited Communication Among Three Nodes

P. Cuff, J. Liu, S. Verdú

Setting

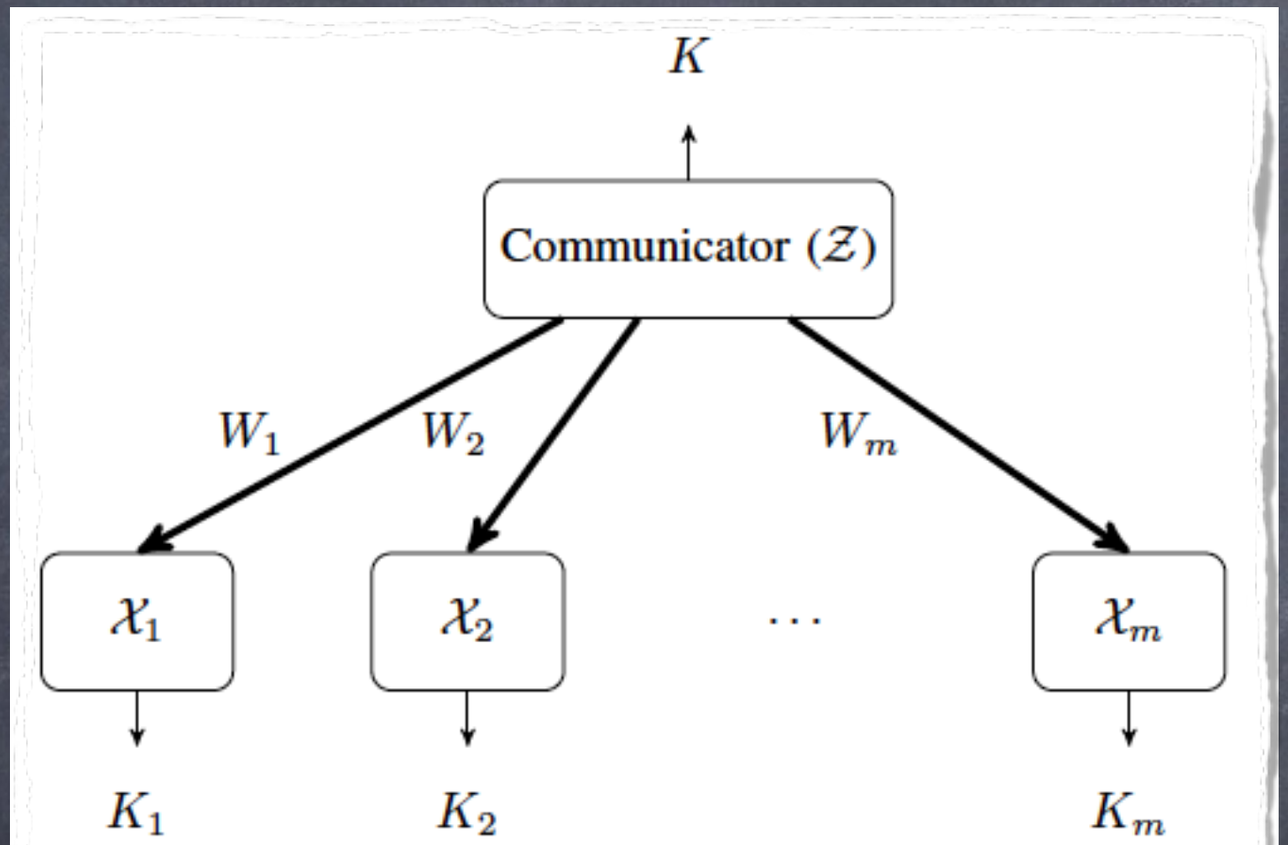


Figure 1: Key generation with one communicator

Quantum Key Exchange

[Bennett-Brassard '84]

Quantum Key Exchange

[Bennett-Brassard '84]

Theorem (2 nodes)

- [Ahlswede-Csiszár '93]
- R_k is key generation rate
- R is communication rate
- (X,Y) are correlated observations; Z is adversaries observation
- Necessary and sufficient conditions:
  - Exists random variables U and V:
  - (U,V)–X–(Y,Z) form Markov chain
  - $R_k \leq I(V;Y|U) - I(V;Z|U)$
  - $R \geq I(U,V;X) - I(U,V;Y)$

Scalar Gaussian

- [Watanabe-Oohama '10]
- $R(r) = 1/2 \log(1 + \beta - \beta 2^{-2r})$
- $\beta = (\rho_{xy}^2 - \rho_{xz}^2)/(1-\rho_{xy}^2)$

Interpretation

- Define Gaussian capacity function:
  - $C(x) = 1/2 \log(1 + x)$
- Recall:
  - $\beta = (\rho_{xy}^2 - \rho_{xz}^2)/(1-\rho_{xy}^2)$
- Notice that $C(\beta) = I(X;Y) - I(X;Z)$
- Interpret: β is a signal-to-noise ratio for key agreement with unlimited communication
- $R(r) = C(\beta(1-2^{-2r}))$

Vector Gaussian

- [Lui-Cuff-Verdú '14]
  - Jointly diagonalize (under certain conditions)
  - Water-filling

For (X^L, Y^L, Z^L) product Gaussian sources, $R(r)$ is parameterized as

$$r = \frac{1}{2} \sum_{i:\beta_i > \mu} \log \frac{\beta_i(\mu+1)}{(\beta_i+1)\mu}, \quad R = \frac{1}{2} \sum_{i:\beta_i > \mu} \log \frac{\beta_i+1}{\mu+1},$$

where $\mu > 0$ and $\beta_i := \frac{\rho^2_{X_iY_i} - \rho^2_{X_iZ_i}}{1-\rho^2_{X_iY_i}}$.

Stationary Gaussian

- Key Generation for non-i.i.d. Gaussian observations

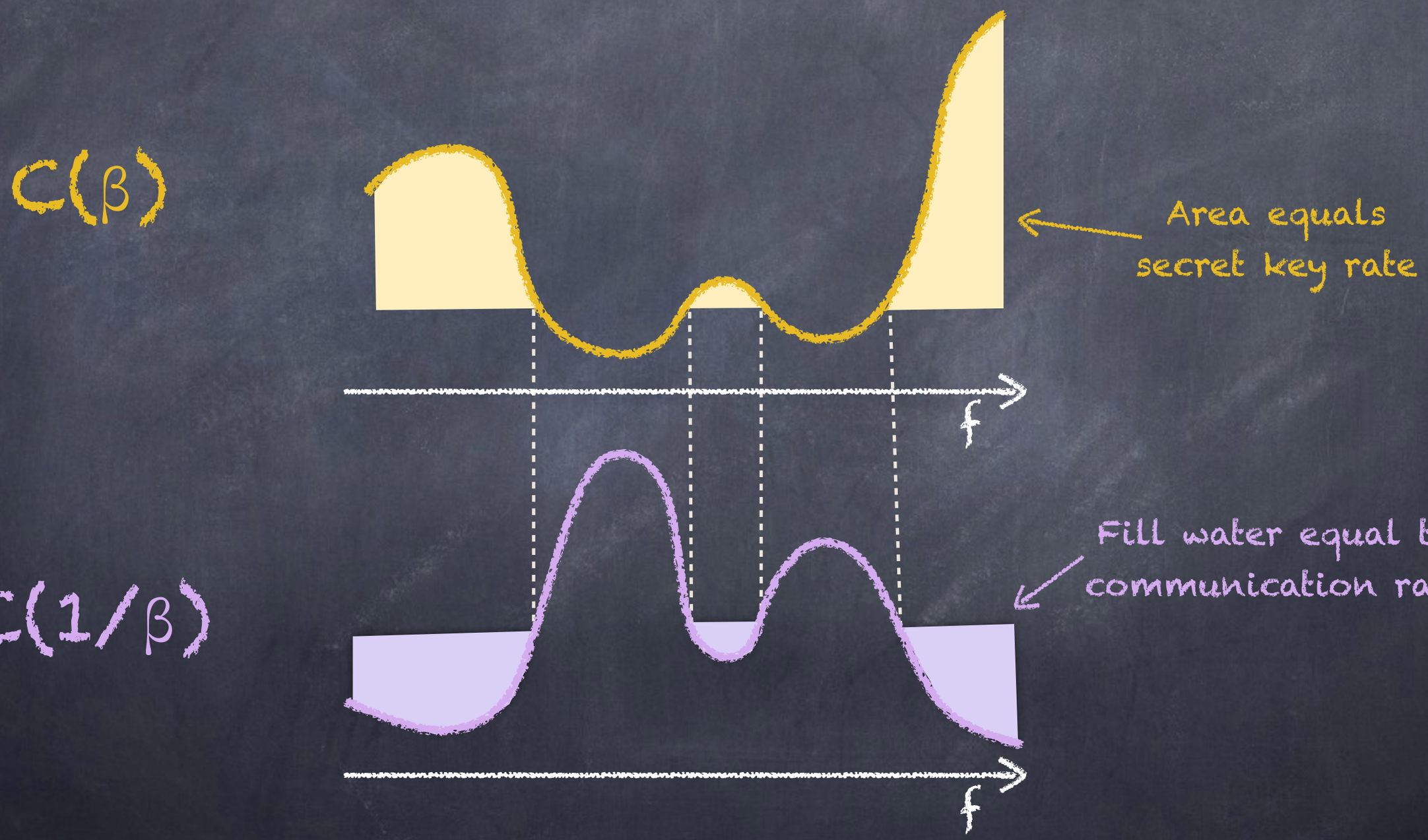
- Let $S(\omega)$ be power special density

$$r = \frac{1}{4\pi}\int_{\beta(\omega)>\mu} \log \frac{\beta(\omega)(\mu+1)}{(\beta(\omega)+1)\mu} \mathrm{d}\omega,$$

$$R = \frac{1}{4\pi}\int_{\beta(\omega)>\mu} \log \frac{\beta(\omega)+1}{\mu+1} \mathrm{d}\omega.$$

where $\beta(\omega) := \frac{|S_{XY}(\omega)|^2 S_Z(\omega) - |S_{XZ}(\omega)|^2 S_Y(\omega)}{S_X(\omega)S_Y(\omega)S_Z(\omega) - |S_{XY}(\omega)|^2 S_Z(\omega)}$ *depends only on the spectral densities.*

Water-filling



One Communicator, Many Nodes

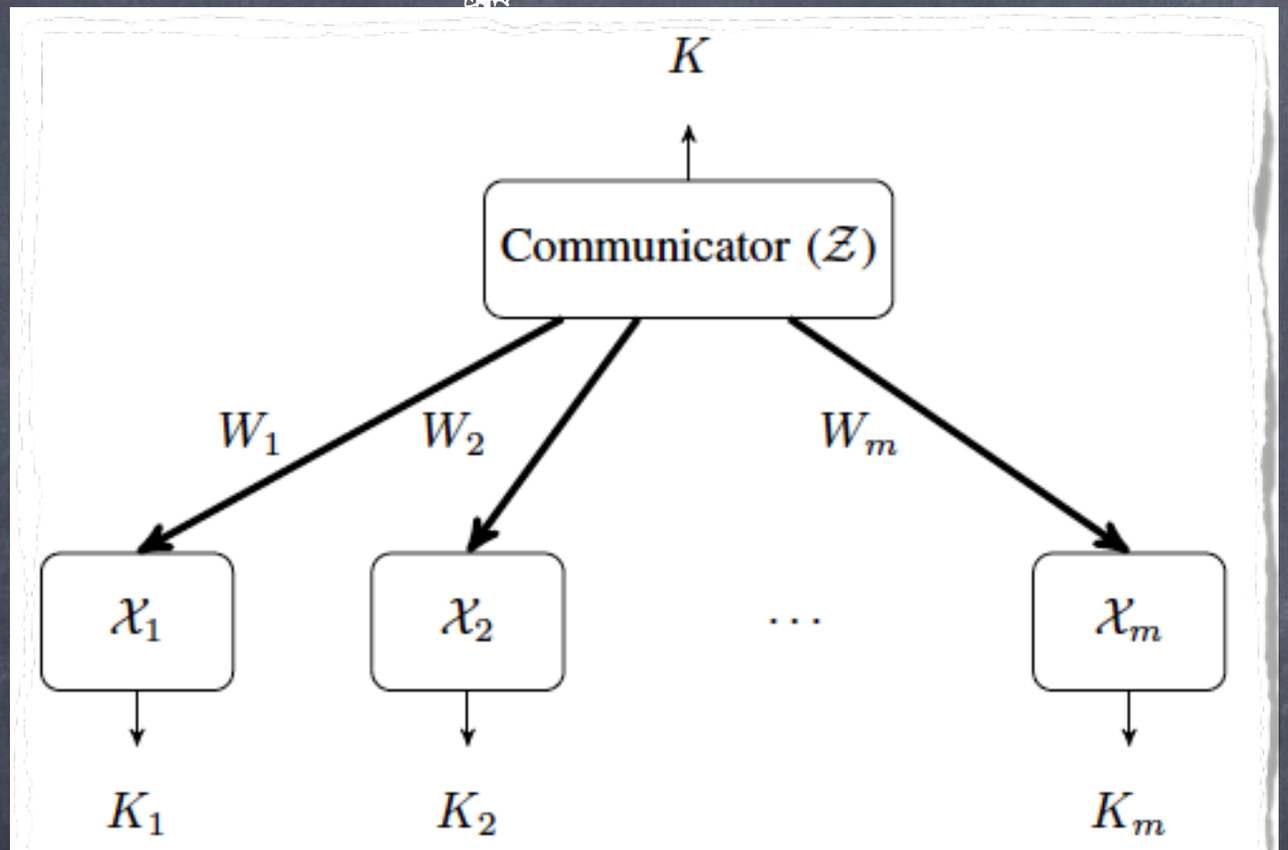


Figure 1: Key generation with one communicator

Related - Secret Key, Unlimited Communication

- [Csiszár-Narayan '04]
  - $R_K = \min_j I(Z;X_j)$

Related - Common Randomness Generation

- [Ahlswede-Csiszár '98]:
  - Exists R.V. U:
    - $U - Z - X^m$ form Markov chain
    - $R_0 \leq I(U;Z)$
    - $R_j \geq I(U;Z|X_j)$ for all j

Secret Key Generation

- Theorem
  - Exists R.V.s U, S_1, ..., S_m:
  - $(U,S^m)-Z-X^m$ form Markov chain
  - $R_k \leq I(U;Z)$
  - $R_k \leq \min_j I(U,S_j;X_j)$
  - $R_j \geq I(U,S_j;Z|X_j)$ for all j

Encoding

- Super-position:
  - U is bottom layer
  - Sj is upper layer
  - Only use binning on U
  - Sj helps to decode U
- Use Likelihood Encoder

"Omniscient Helper"

- Case where $Z = (X_1, \ldots, X_m)$
- Corollary:
  - Exists R.V. U:
  - $R_k \leq I(U;X^m)$
  - $R_k \leq \min_j H(X_j)$ ⟵ Only additional constraint (vs CR)
  - $R_j \geq I(U;X^m|X_j)$ for all j

ALL Message Secrecy

- Our result only gives "one message secrecy"
- Consider an example (m=3):
  - (X_1,X_2,X_3) binary and uniformly distributed such that $X_1 \oplus X_2 \oplus X_3 = 0$
  - $R_1=1$, $R_2=1$, $R_3=0$
  - Communicator is omniscient

Return to General Region

- Encoder implied by this region achieves "all message secrecy" for this example
  - Exists R.V.s $U, S_1, \ldots, S_m$: ← Set $S_1 = S_2 = X_1$
    - $(U,S^m)-Z-X^m$ form Markov chain
    - $R_k \leq I(U;Z)$
    - $R_k \leq \min_j I(U,S_j;X_j)$
    - $R_j \geq I(U,S_j;Z|X_j)$ for all j