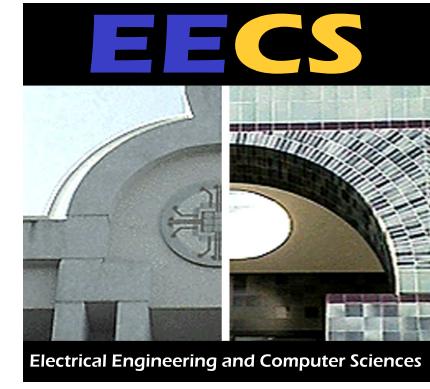


Secure Communication using an Untrusted Relay via Sources and Channels



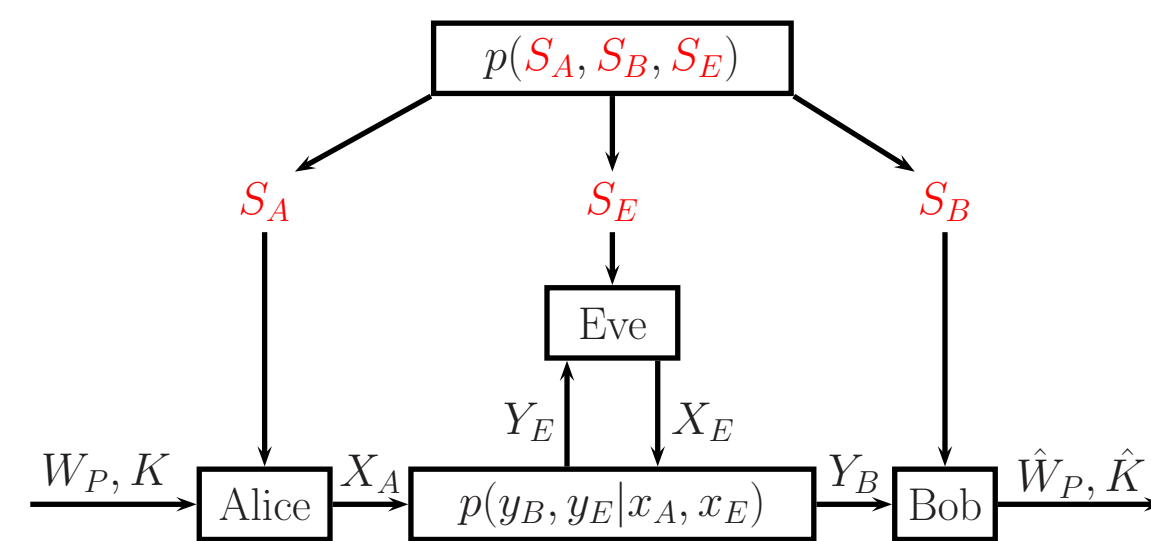
Nebojsa Milosavljevic, Michael Gastpar and Kannan Ramchandran

Department of Electrical Engineering and Computer Sciences, University of California, Berkeley

Problem Setup

Resources available:

- Relay channel
- Distributed sources with observations independent of the channel



Goal:

- Alice and Bob to agree on a secret key K which is perfectly secret from Eve
- Bob to decode private message W_P which is perfectly secret from Eve

Secret key $K = g(S_A^n)$ has to satisfy:

- Secrecy: $\frac{1}{n}I(K; Y_E^n, S_E^n) \rightarrow 0$ as $n \rightarrow \infty$
- Uniformity: $\frac{1}{n}H(K) \rightarrow \frac{1}{n} \log |\mathcal{K}|$ as $n \rightarrow \infty$
- Recoverability: $\frac{1}{n}H(K|Y_B^n, S_B^n) \rightarrow 0$ as $n \rightarrow \infty$

Private message W_P has to satisfy:

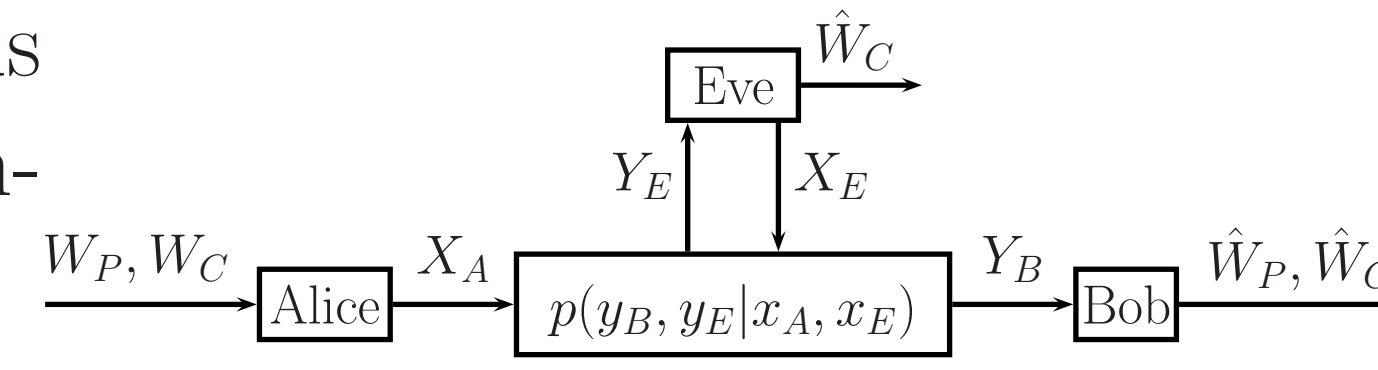
- Secrecy: $\frac{1}{n}I(W_P; Y_E^n, S_E^n) \rightarrow 0$ as $n \rightarrow \infty$
- Recoverability: $\frac{1}{n}H(W_P|Y_B^n, S_B^n) \rightarrow \infty$ as $n \rightarrow \infty$

An Achievable Strategy

1. Convert channel into public and private bit pipes.
 - Use private bit pipe to send part of the private message
2. Use part of public bit pipe and distributed sources to generate secret key
3. Use part of the secret key as one-time pad for remainder of public bit pipe

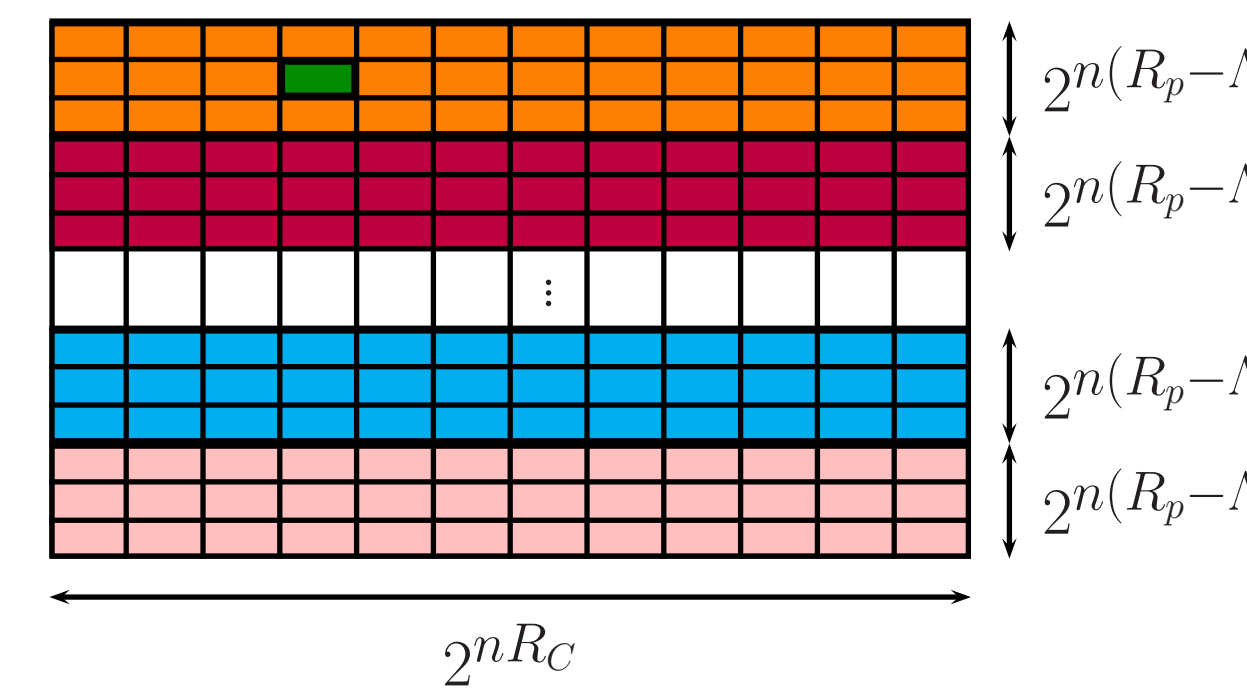
Converting Channel into Public and Private Bit Pipes

- Each cell corresponds to input X_A^n to channel



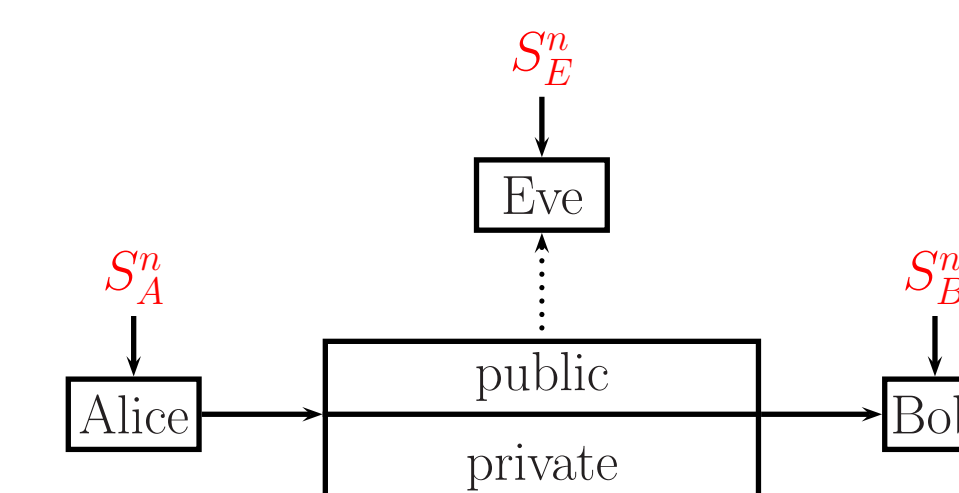
$$R_{private} = R_P - \Lambda$$

$$R_{public} = R_C + \Lambda$$



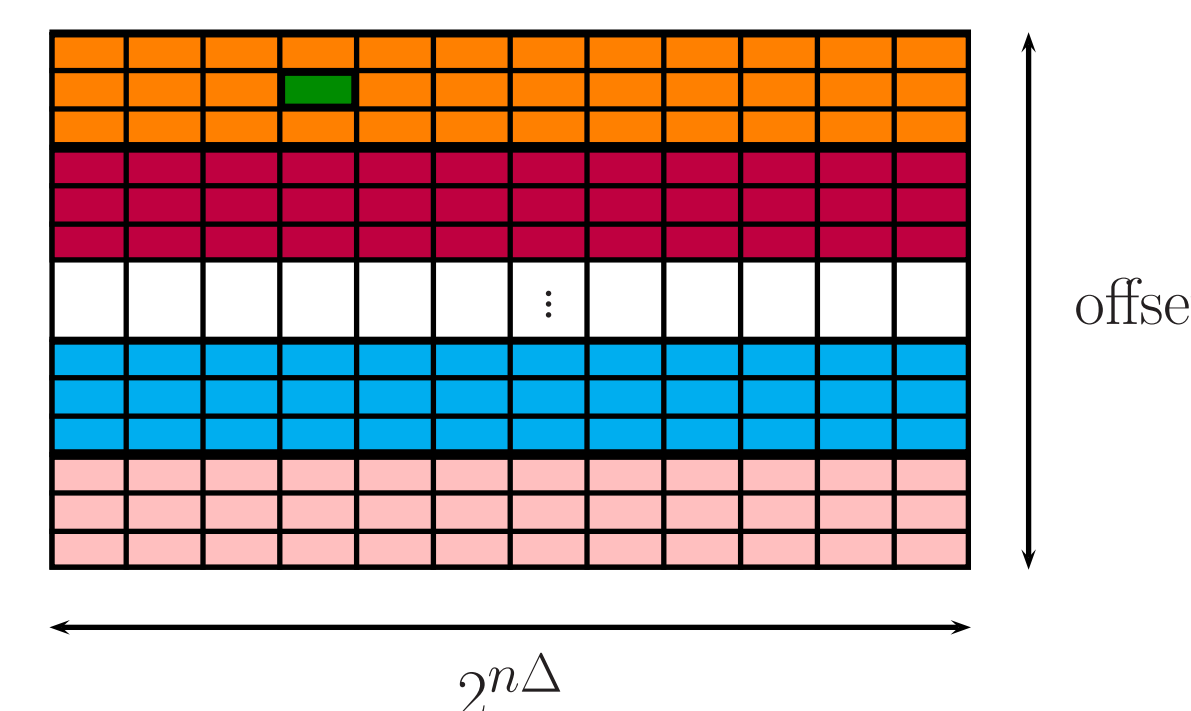
Secret Key Generation

(Csiszár-Narayan 00)



Construction:

- Quantize S_A^n and place in Wyner-Ziv bin
- **Secret key** represented by the **color** of the offset



An Achievable Strategy

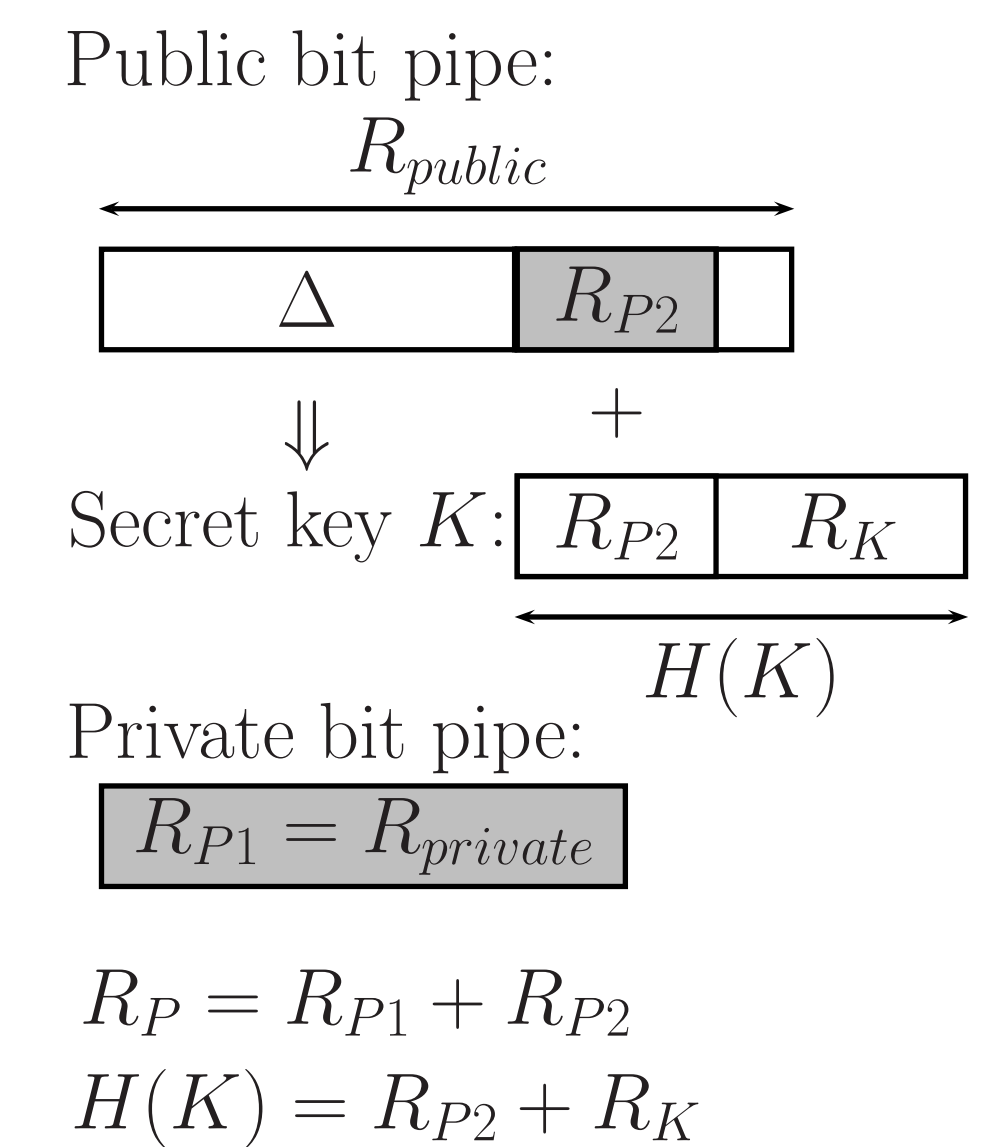
Combining these three steps we can show:

$$R_P \leq R_{public} + R_{private} - \Delta$$

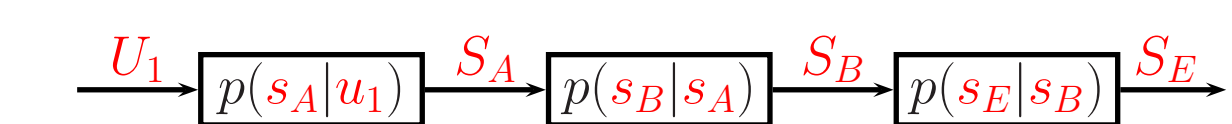
$$R_P + R_K \leq R_{private} + H(K)$$

Using Secret Key as One Time Pad

- Use distributed sources and public bit pipe to generate key of size $H(K)$ by sending Wyner-Ziv bin index at rate Δ across the channel.
- One-time pad the message sent over the public bit pipe with a key of equal size



Sum Rate Optimality



Reversely degraded channel:

$$R_P + R_K \leq I(X_A; Y_B|X_E) - I(X_A; Y_E|X_E) + I(U_1; S_B) - I(U_1; S_E)$$

Degraded channel:

$$R_P + R_K \leq I(U_1; S_B) - I(U_1; S_E)$$

Gaussian Example

- What is the benefit of having distributed observations at Alice and Bob?

