Error-Free Perfect-Secrecy Systems

Siu-Wai Ho

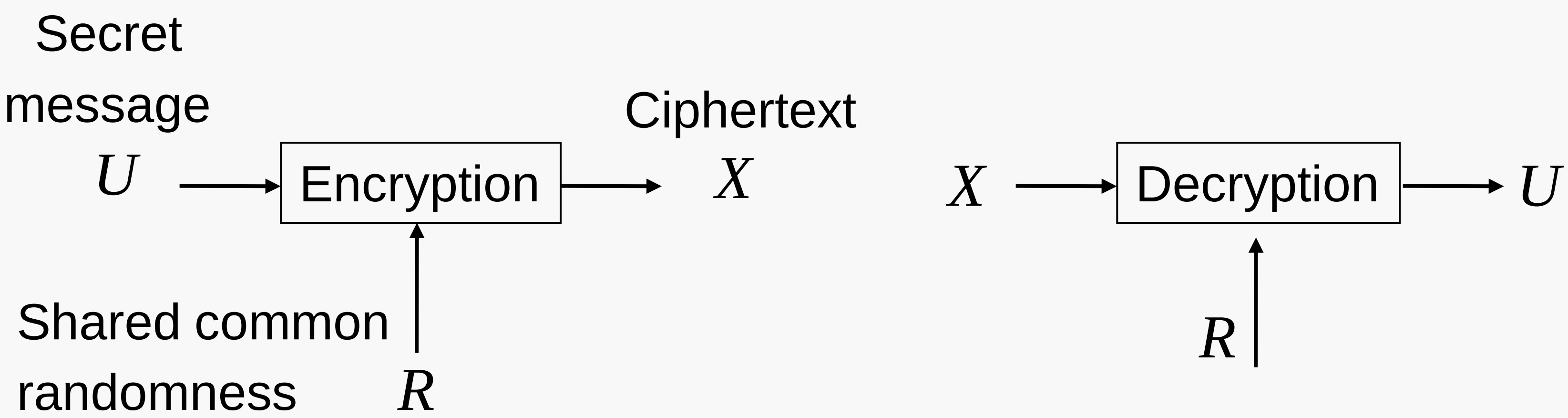
Institute for Telecommunications Research

University of South Australia

collaborated with Terence Chan, Chinthani Uduwerelle, and Alex Grant

Apr 13 2011

Introduction



- A system satisfies perfect secrecy if $I(U; X) = 0$.

$$I(U;X) = D(P_{UX} \,\|\, P_U P_X) = \sum_{ux} P_{UX}(ux) \log \frac{P_{UX}(ux)}{P_U(u) P_X(x)} = 0$$

$$\Leftrightarrow \quad P_{UX}(ux) = P_U(u) P_X(x) \quad \forall u, x$$

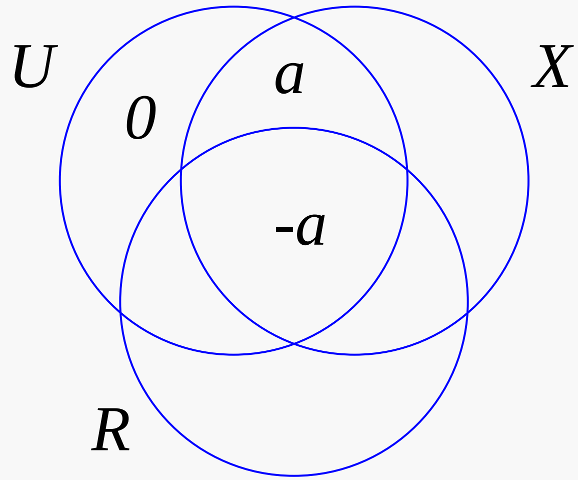
- Error-free means $H(U|XR) = 0$, i.e., $U = g(X, R)$.

Introduction

- Perfect secrecy was studied in [Shannon1949] [Massey 1988].

- Theorem [Shannon's perfect secrecy theorem]
- If $I(U; X) = 0$ and $H(U \mid RX) = 0$, then

$$H(R) \geq H(U)$$



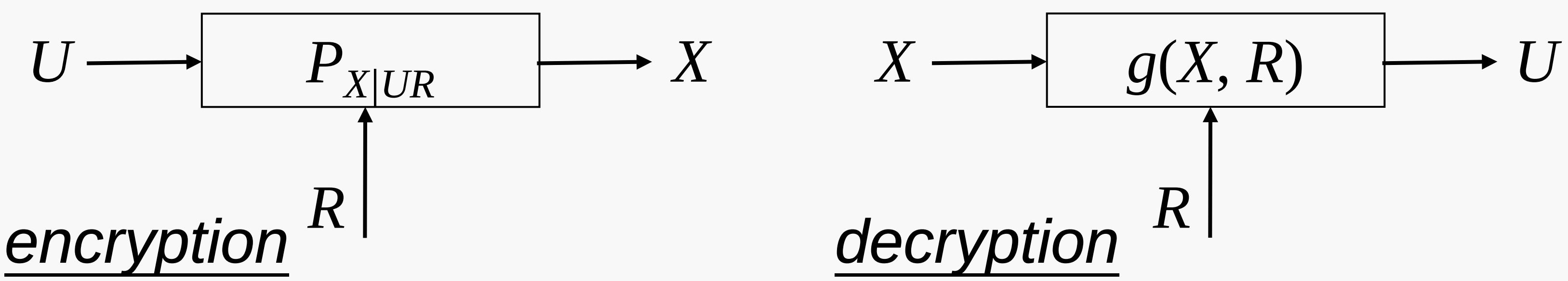
Introduction

- Definition 1 A cipher system is called an *Error-free Perfect-Secrecy (EPS)* system if

$$H(U|RX) = 0 \qquad \textit{zero decoding error}$$

$$I(U;X) = 0 \qquad \textit{perfect secrecy}$$

$$I(U;R) = 0 \qquad \textit{no side information}$$



Lower Bounds on Resources

- Theorem 1 Let $\mathcal{U}$ be the support of U. For an EPS system $\{R, U, X\}$,

$$\max_x P_X(x) \le |\mathcal{U}|^{-1},$$

and

$$\max_r P_R(r) \le |\mathcal{U}|^{-1}.$$

- Consequently,

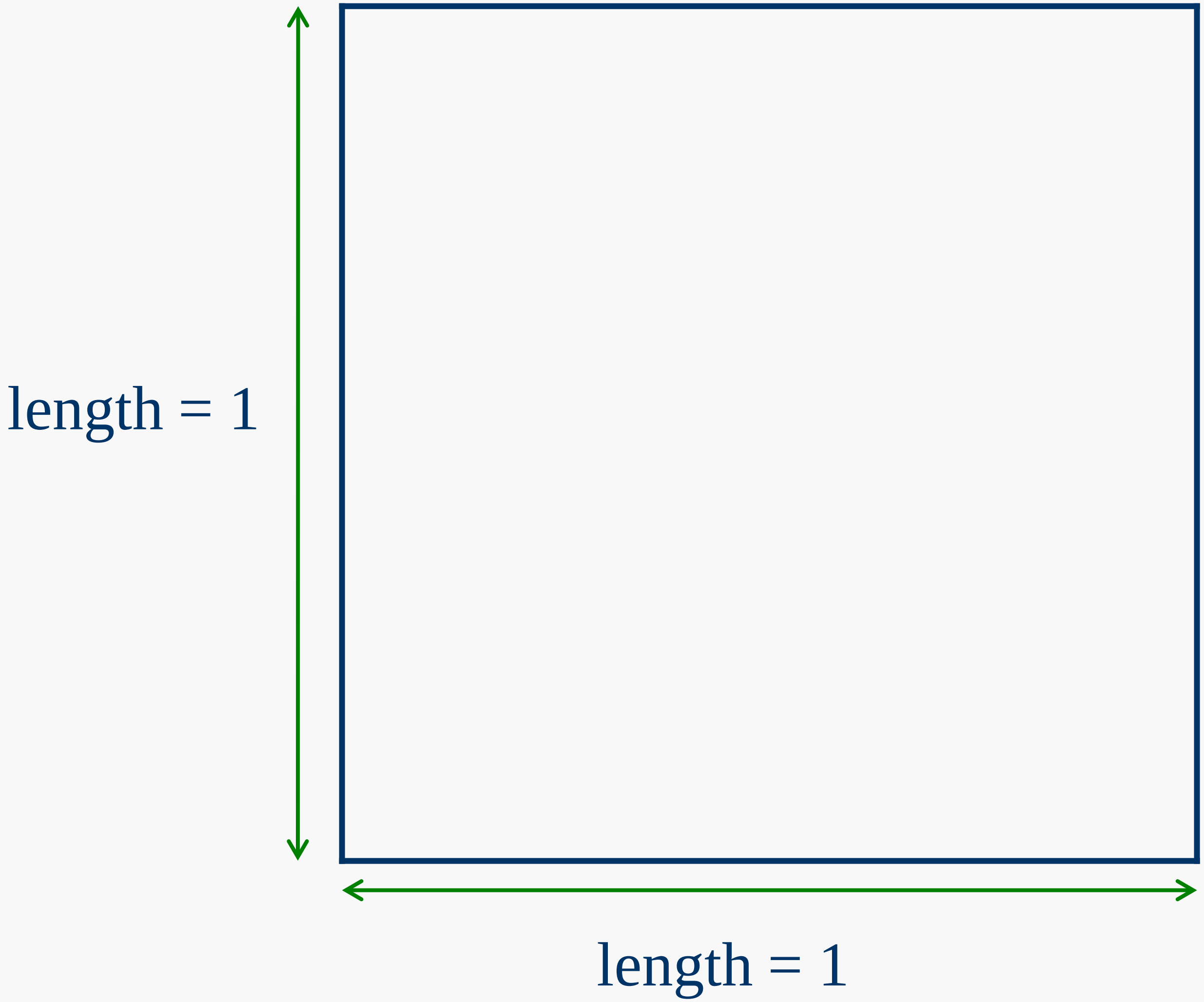
$$H(X) \ge \log |\mathcal{U}|,$$

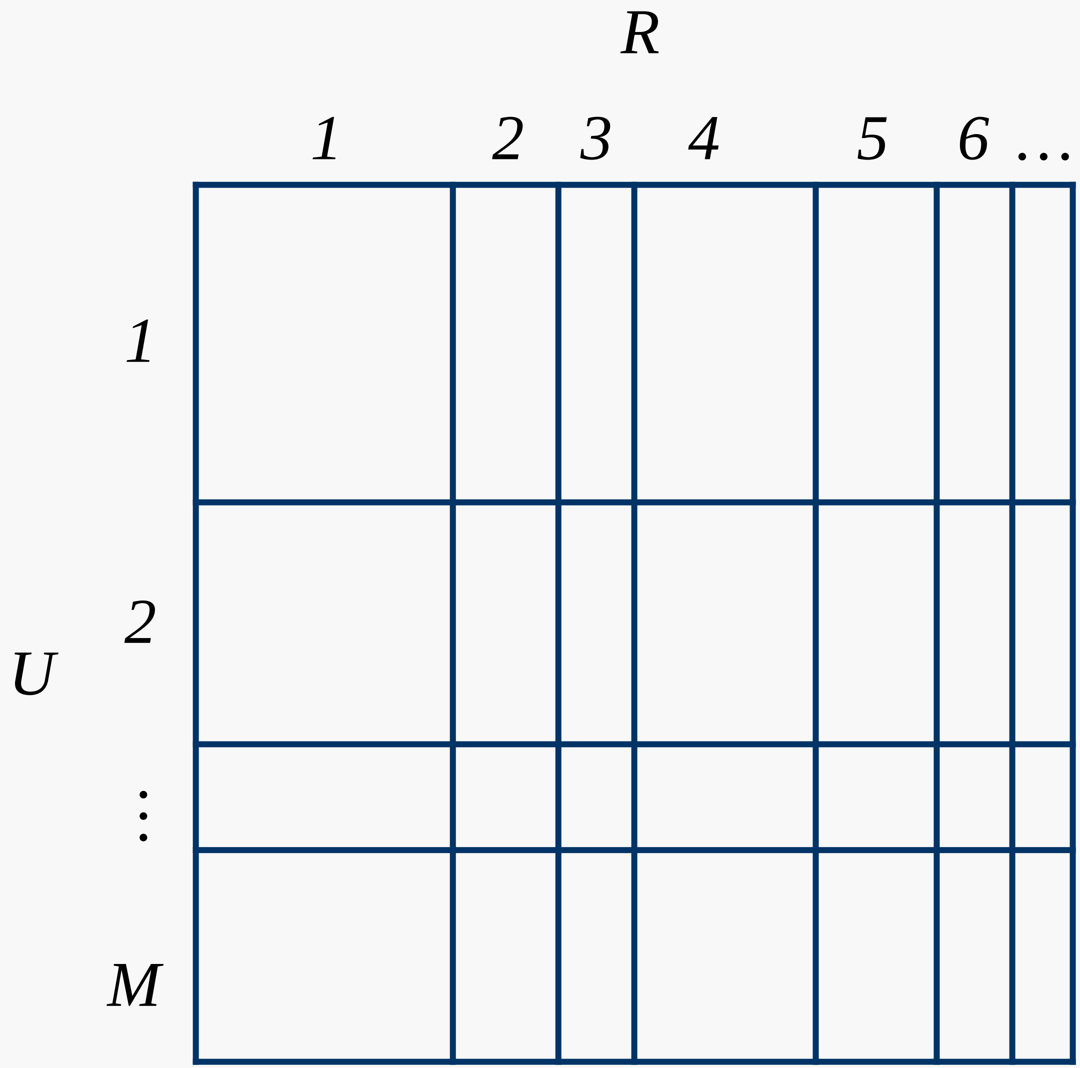
and

$$H(R) \ge \log |\mathcal{U}|.$$

- If the source is not uniform, $\log |\mathcal{U}| > H(U)$ and hence, $H(R) > H(U)$

Proof:

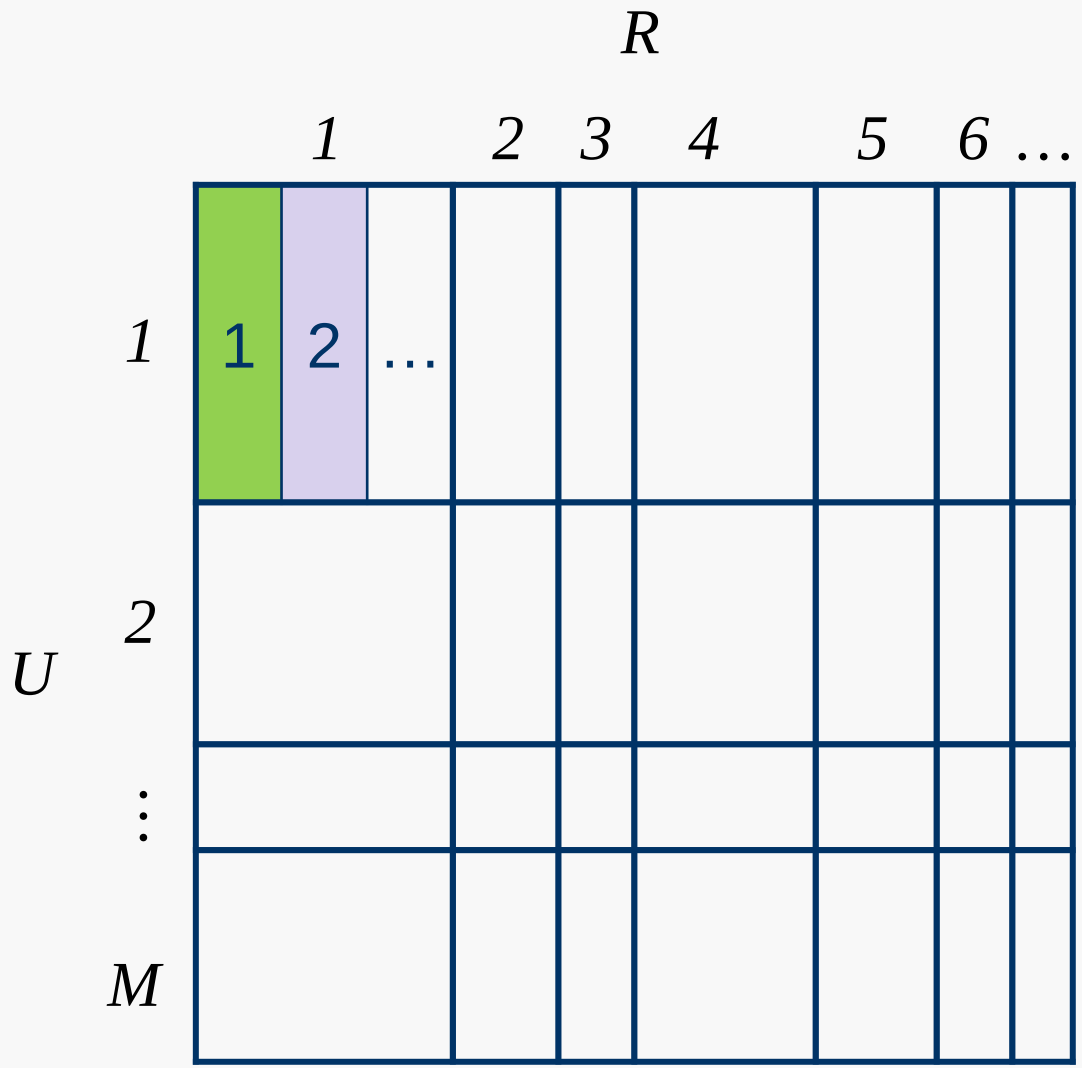




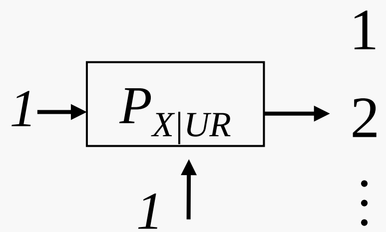
The height of each cell = P_U(u)

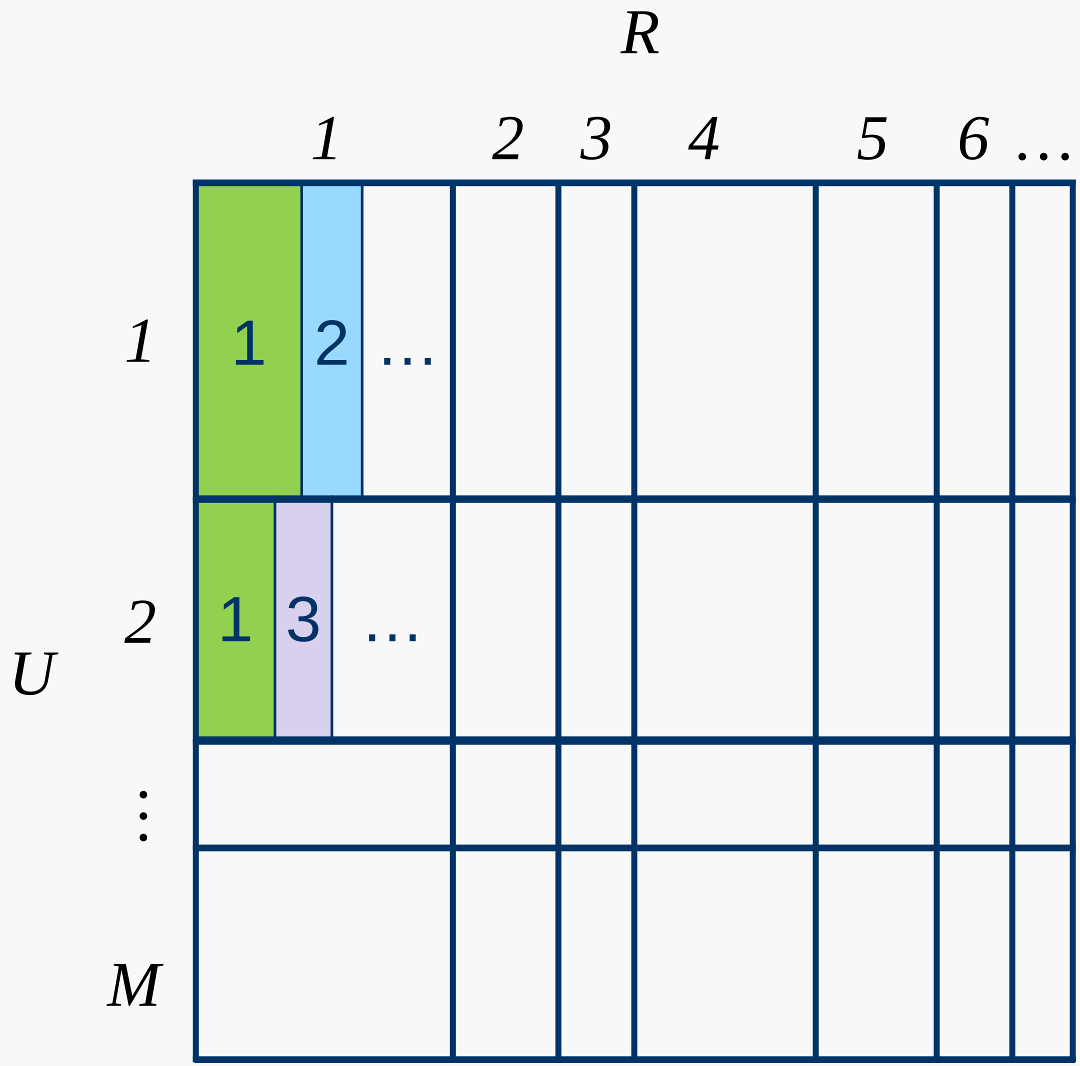
The width of each cell = $P_R(r)$

Due to $I(U;R) = 0$, the area of each cell = $P_U(u)\, P_R(r) = P_{UR}(u, r)$

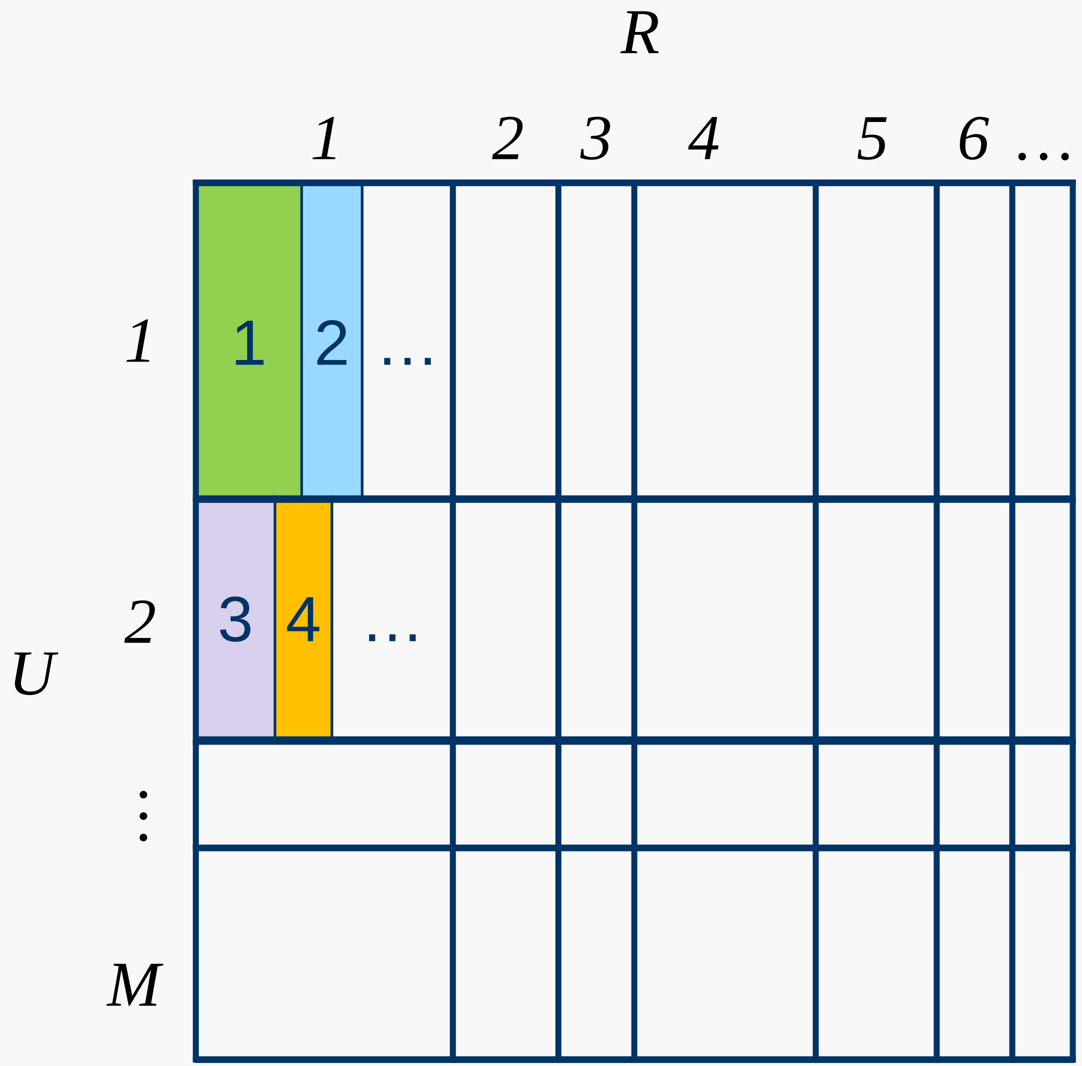


Each cell can have more than one values

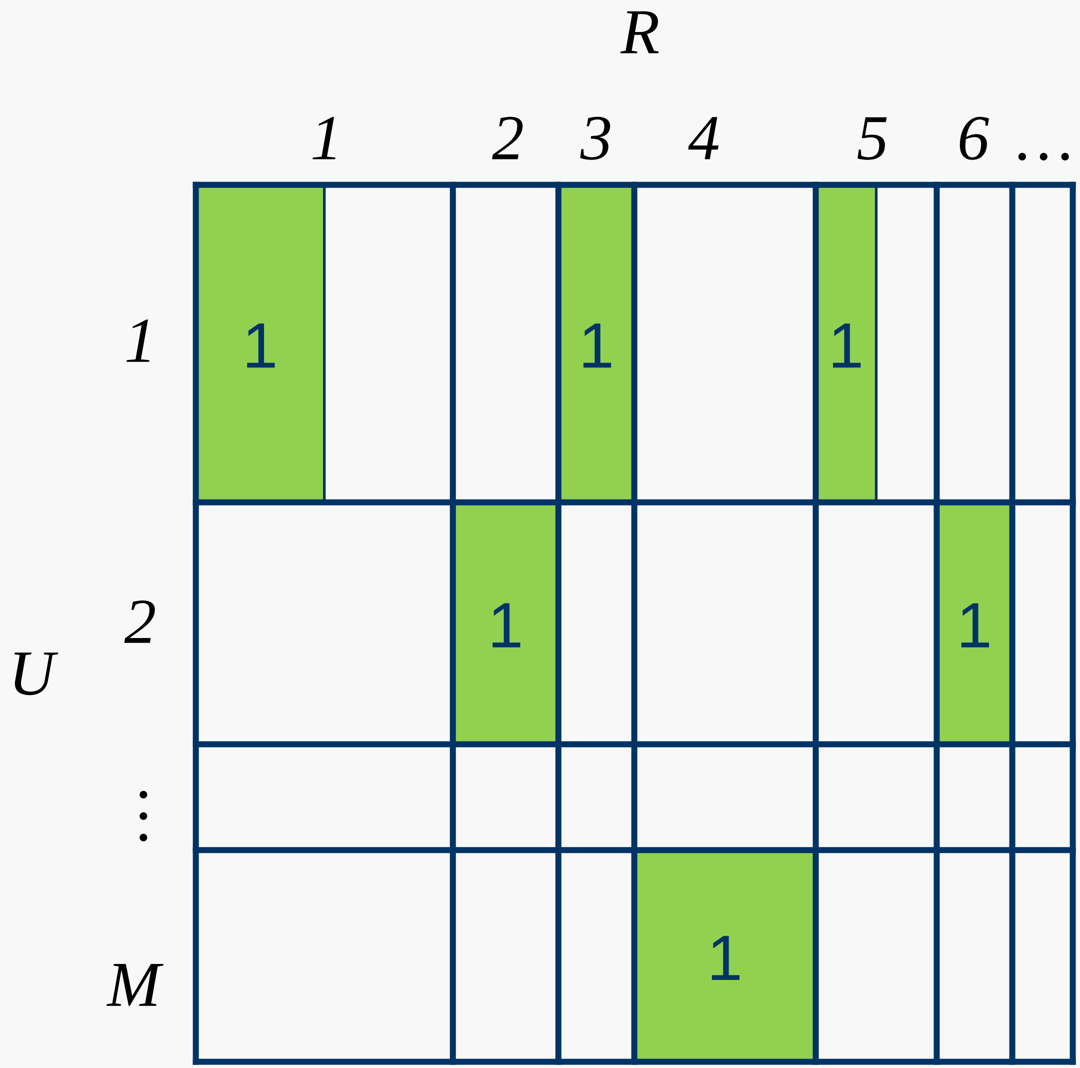




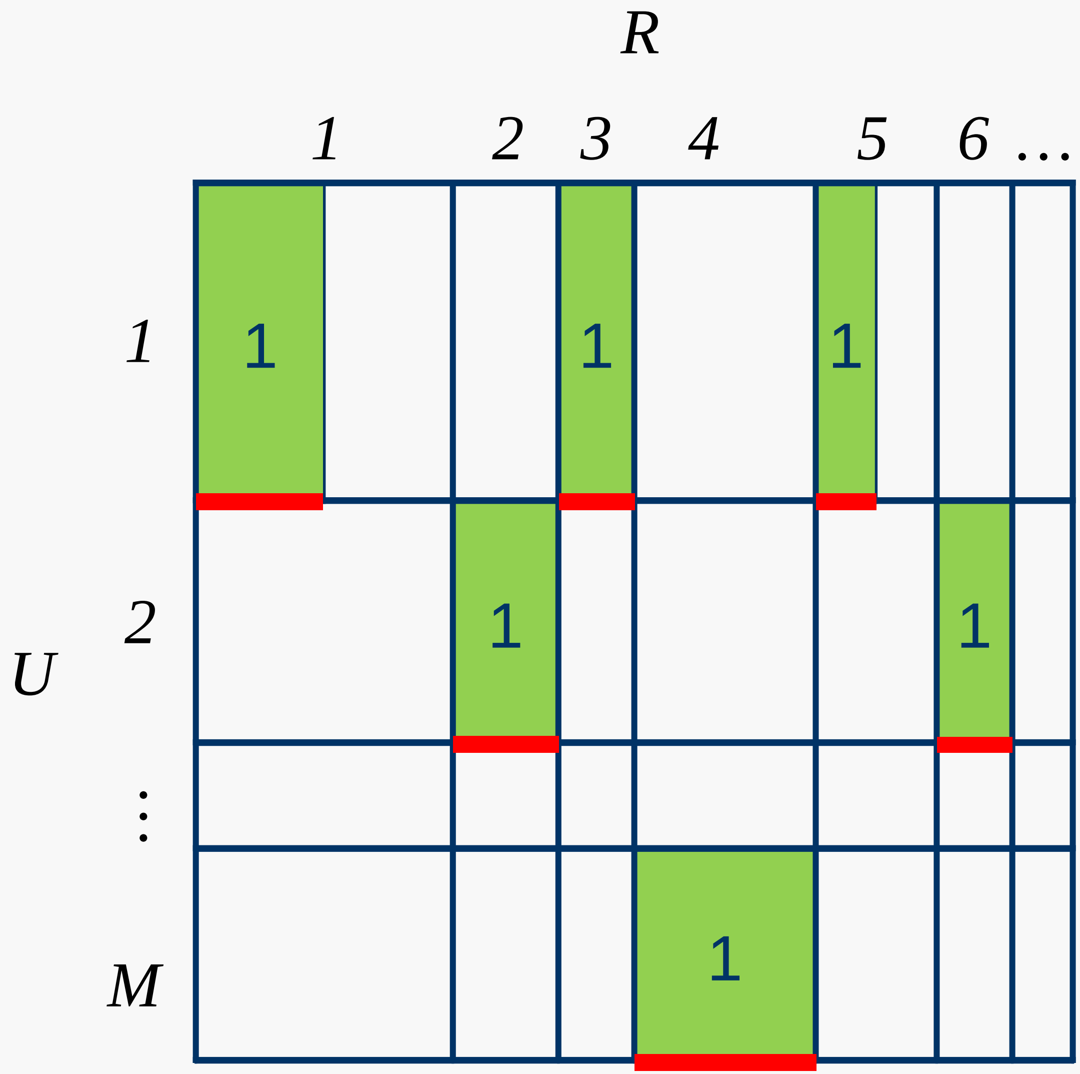
Due to $H(U|XR) = 0$, the same value of X cannot be assigned to the same column.



Due to $H(U|XR) = 0$, the same value of X cannot be assigned to the same column.



Consider $X = 1$.



For $1 \le i \le M$, the total green area in Row i is $P_{XU}(1,i)$.

The total length of the red lines in Row i is $P_{XU}(1,i) \,/\, P_U(i)$ $= P_{X|U}(1|i)$ $= P_X(1)$ due to $I(U;X)=0$

Since the total length of all red lines is less or equal to 1, $M\,P_X(1) \le 1$, and hence $P_X(1) \le M^{-1}$

Lower Bounds on Resources

- Theorem 1 Let $\mathcal{U}$ be the support of U.

$$\left.\begin{array}{r} H(U \mid RX)=0 \\ I(U;X)=0 \\ I(U;R)=0 \end{array}\right\} \Rightarrow \begin{array}{c} \max_x P_X(x) \le |\mathcal{U}|^{-1} \\ \max_r P_R(r) \le |\mathcal{U}|^{-1} \end{array} \Rightarrow \begin{array}{c} H(X) \ge \log|\mathcal{U}| \\ H(R) \ge \log|\mathcal{U}| \end{array}$$

- $H(R)$ measures the initial key requirement
- $H(X)$ measures the number of channel use
- Data compression cannot help to reduce $H(X)$
- These are constrained non-Shannon type inequalities

Countably Infinite $\mathcal{U}$

- Theorem 2 No EPS system can be constructed for $|\mathcal{U}| = \infty$, i.e., U is defined on a countably infinite support or a support with unbounded size.
  - Theorem 1 shows that $H(R)$ and $H(X)$ is large if the cardinality of the support of U is large regardless how small $H(U)$ is.
  - If $|\mathcal{U}| = \infty$, at least one of the following assumptions has to be dropped.

$$H(U|RX) = 0 \qquad \textit{zero decoding error}$$

$$I(U;X) = 0 \qquad \textit{perfect secrecy}$$

$$I(U;R) = 0 \qquad \textit{no side information}$$

Achievablity Part

- Theorem 3 If $|\mathcal{U}| < \infty$, there exists an EPS system such that $H(X) = H(R) = \log |\mathcal{U}|$.

- Proof: One-time pad.
- Let $M = |\mathcal{U}|$.
- Let R be uniformly distributed in $\{1, 2, \ldots, M\}$.
- Let $X = (U + R) \bmod M$.

Constrained non-Shannon Type Inequality

- Corollary 4 If $H(U|RX) = I(U;X) = I(U;R) = 0$, then

$$\left\lceil a^{H(U)} \right\rceil \le a^{H(X)}$$

where logarithms are with respect to base a.

- Proof: By Theorem 1,

$$H(U) \le \log|\mathcal{U}| \le H(X).$$

- Therefore,

$$a^{H(U)} \le |\mathcal{U}| \le a^{H(X)}.$$

- Remark: Corollary 4 generalizes Theorem 1 in [Matúš 2006], which has an extra assumption $H(X|UR) = H(R|UX) = 0$.

Example

- Suppose the sender and the receiver share a secret key $R = \{B_1, B_2, \ldots, B_n\}$, where B_i are i.i.d. with distribution P_B such that $P_B(0) = P_B(1) = 0.5$.
- Let $P_U(0) = 0.5$ and $P_U(1) = P_U(2) = 0.25$.
- Let

$$P_{B_{n+1}} = P_B$$

$$(U'_1, U'_2) = \begin{cases} (0, B_{n+1}) & \text{if } U = 0 \\ (1,0) & \text{if } U = 1 \\ (1,1) & \text{if } U = 2 \end{cases}$$

- Let $X = (U'_1 \oplus B_1, U'_2 \oplus B_2)$.
- The receiver can decode (U'_1, U'_2) from X and R.

Example (cont')

- $P_U(0) = 0.5$ and $P_U(1) = P_U(2) = 0.25$.

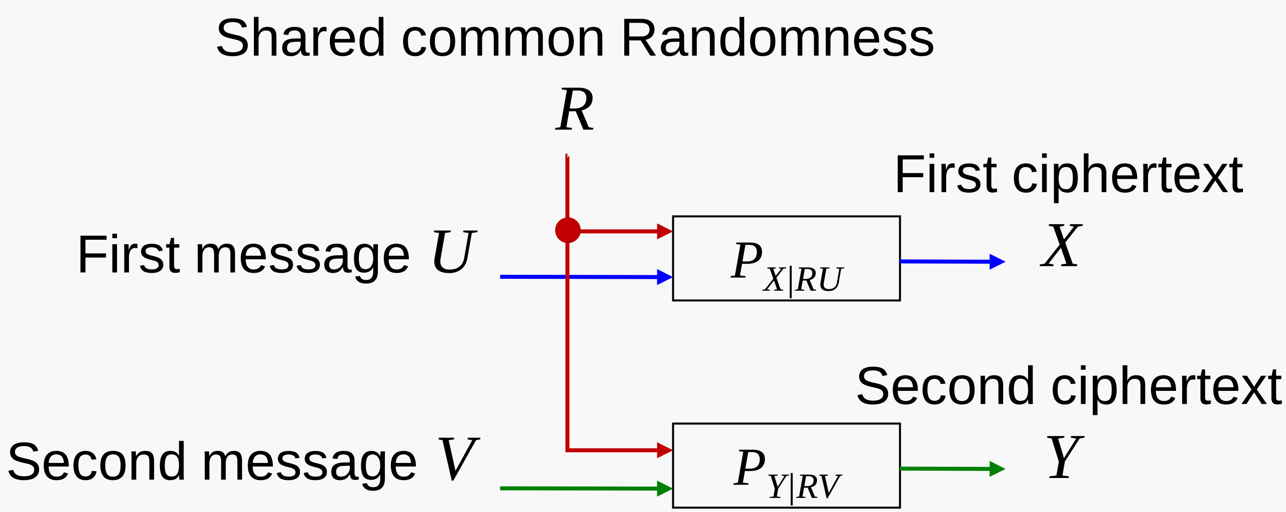
$$R' = \begin{cases} (B_3, B_4, \ldots, B_n, B_{n+1}) & \text{if } U = 0 \\ (B_3, B_4, \ldots, B_n) & \text{if } U = 1 \text{ or } 2 \end{cases}$$

- The expected key consumption:

$$\begin{aligned} P_U(0) \cdot 1 + P_U(1) \cdot 2 + P_U(2) \cdot 2 &= 1.5 \\ &= H(U) \\ &\boxed{= I(R;UX)} \end{aligned}$$

- The residual R' can be used in the next round.

Multiple Use



- The system satisfies

$$H(U \mid RX) = 0 \qquad H(V \mid RXY) = 0$$

$$I(U;X) = 0 \qquad I(UV;XY) = 0$$

$$I(U;R) = 0 \qquad I(V;R) = 0$$

Multiple Use (Justification 1)

- Theorem 5 If $I(UV;XY) = H(U \mid RX) = H(V \mid RXY) = 0$

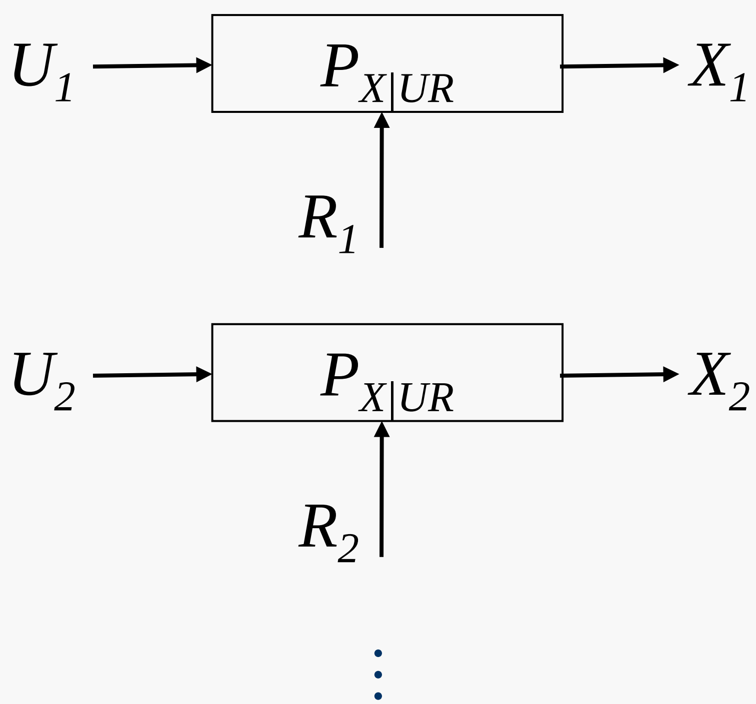
  and $$I(U;R) = I(V;R) = 0,$$

  then $$H(V \mid U) \le H(R \mid U, X)$$

  Proof: Constrained Shannon type inequality

- After the first transmission, the maximum amount of information that can still be transmitted secretly will be upper bounded by $H(R \mid UX) = H(R) - I(R;UX)$
- $H(R)$ is the size of the key shared at the beginning.
- $I(R; UX)$ seems to be the "amount of key" that has been consumed during the first transmission.

Multiple Use (Justification 2)



- Suppose an EPS system (U_i, R_i, X_i) is continuously and independently used.
- Both the sender and the receiver know $\{(U_i, R_i, X_i), i = 1, 2, \ldots\}$
- Suppose the sender and the receiver aims to generate a new common secret key $S^m = (S_1, \ldots, S_m)$

Multiple Use (Justification 2)

- The new common secret key $S^m = (S_1, \ldots, S_m)$.
- Suppose S_i are i.i.d. with generic random variable S.
- We require

$$I(S^m; U^j, X^j) = 0 \quad \text{for all } j$$
$$H(S^m \mid R^j, X^j) = 0 \quad \text{for sufficiently large } j$$

- Using S^m will not disclose any information about the previous system uses
- Both sender and the receiver can generate the same S^m without any error.

Multiple Use (Justification 2)

- Let N_m be a random variable such that

$$H(S^m | R^{N_m}, X^{N_m}) = 0$$

where $R^{N_m} = (R_1, \ldots, R_{N_m})$ and $X^{N_m} = (X_1, \ldots, X_{N_m})$.

- It is sufficient to use the EPS system N_m times to generate S^m.
- N_m is random because the realization of N_m depends on the realizations of $\{(U_i, R_i, X_i), i = 1, 2, \ldots\}$.
- We are interested to know $\dfrac{H(S^m)}{\mathbf{E}[N_m]}$
- Roughly speaking, this is the expected rate of generating a new key per system use.

Multiple Use (Justification 2)

- Theorem 6 Consider a sequence of i.i.d. EPS system $\{(U_i, R_i, X_i), i = 1, 2, \ldots\}$ with generic random variables (U, R, X). For any given P_S and positive integer m, we can construct S^m from N_m system uses such that

$$I(S^m; U^j, X^j) = 0 \quad \text{for all } j$$

$$H(S^m \mid R^{N_m}, X^{N_m}) = 0$$

- Then

$$\lim_{m\to\infty} \frac{H(S^m)}{\mathbf{E}[N_m]} \geq H(R \mid UX).$$

- Furthermore,

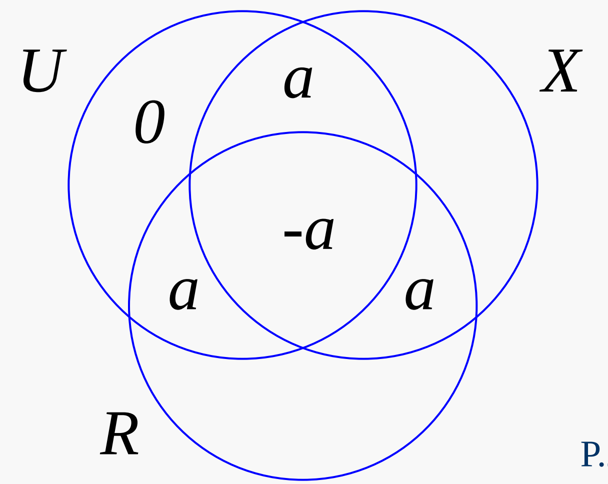
$$H(R \mid UX) \geq \frac{H(S^m)}{\mathbf{E}[N_m]}$$

Multiple Use (Justification 3)

- $H(R \mid X, U)$ is the amount of key that can be extracted after each use of the system
- $I(R;XU)$ is the expected key consumption in every use of an EPS system
- Theorem 7 For any EPS system,

$$I(R;UX) = H(R) - H(R \mid X, U) \geq H(U)$$

$$I(R;UX) = H(U) \quad \Leftrightarrow \quad I(R;X) = 0$$



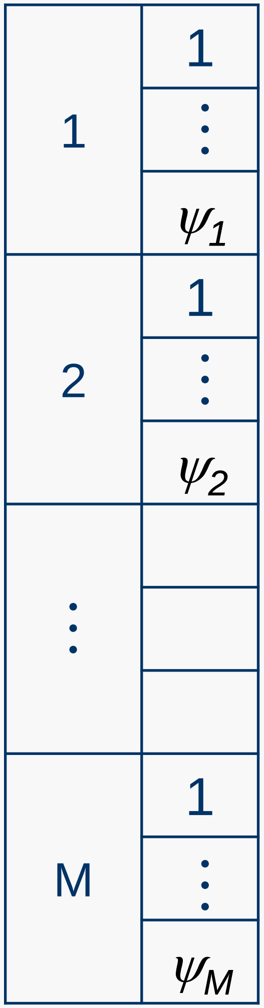
Min. Expected Key Consumption

- Example 2 Suppose U and R are independent and both uniformly distributed on sets $\{0, 1, \ldots, 2^i - 1\}$ and $\{0, 1, \ldots, 2^j - 1\}$, respectively, where $i \leq j$.
- R' is i random bits extracted from R
- $X = U \oplus R'$.
- $I(R;UX) = H(R) - H(R|UX) = H(R) - H(R|R') = j - (j - i)$
  $= H(U)$

Partition Code

- Let $M = |\mathcal{U}|$ and assume $M < \infty$.
- Let $\Psi = (\psi_1, \ldots, \psi_M) \in \mathcal{N}^M$ and $\theta = \sum_{i=1}^{M} \psi_i$
- Definition 2 A partition code $C(\Psi)$ encodes U as follows.
- Set $i = U$.
- A' is randomly picked from the set $\{1, \ldots, \psi_i\}$ with a uniform distribution.
- Let $A = \sum_{j=1}^{i-1} \psi_j + A' - 1$,

  R be uniformly distributed on the set $\{0, 1, \ldots, \theta - 1\}$ and $X = (A + R) \bmod \theta$.



Partition Code

- Partition code satisfies all the constraints in an EPS system.
- Furthermore,

$$H(X) = H(R) = \log\theta$$

and

$$I(R;U,X) = \sum_{i=1}^{M} P_U(i)\log\frac{\theta}{\psi_i} = H(U) + D(P_U \| Q_U),$$

where $Q_U(i) = \theta^{-1}\psi_i$

Min. Expected Key Consumption

- Theorem 8 Suppose $P_U(u)$ is rational for all u. Let θ be an integer such that $\theta \cdot P_U(u)$ is an integer for all u. Let $\Psi = (\psi_i)$ with $\psi_i = \theta \cdot P_U(u)$. Then the partition code $C(\Psi)$ achieves the minimum expected key consumption, i.e., $I(R; U, X) = H(U)$.

- $H(X)$ represents the number of channel uses to convey the ciphertext X.
- In addition to minimizing $I(R; U, X)$, we want to minimize $H(X)$ simultaneously

Min. Expected Key Consumption

- Theorem 9 Let $\mathcal{X}$, $\mathcal{R}$, and $\mathcal{U}$ be the supports of X, R, and U, respectively.

$$\left.\begin{array}{c} H(U \mid RX) = 0 \\ I(U;X) = 0 \\ I(U;R) = 0 \\ \underline{I(R;X) = 0} \end{array}\right\} \Rightarrow \begin{array}{c} \max_x P_X(x) \le \inf_{u\in\mathcal{U}} P_U(u) \\ \max_r P_R(r) \le \inf_{u\in\mathcal{U}} P_U(u) \end{array}$$

- Note that $\inf_{u\in\mathcal{U}} P_U(u) \le |\mathcal{U}|^{-1}$ where equality holds if and only if P_U is a uniform distribution.

Min. Expected Key Consumption

- Corollary 10 Suppose $\{R_n, U_n, X_n\}$ satisfy

  $$H(U_n \mid R_n X_n) = I(U_n; X_n) = I(U_n; R_n) = I(R_n; X_n) = 0$$

  and $H(U_n) > 0$ for all n. Then

$$\lim_{n\to\infty} H(U_n) = 0 \quad \Rightarrow \quad \lim_{n\to\infty} H(R_n) = \lim_{n\to\infty} H(X_n) = \infty$$

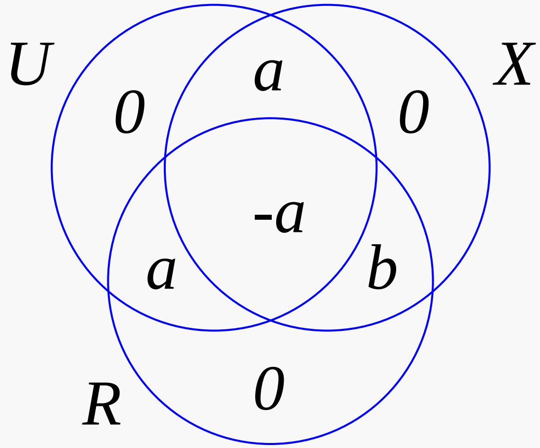
- Theorem 11 Suppose $\{R, U, X\}$ satisfy

  $$H(U \mid RX) = I(U; X) = I(U; R) = I(R; X) = 0.$$

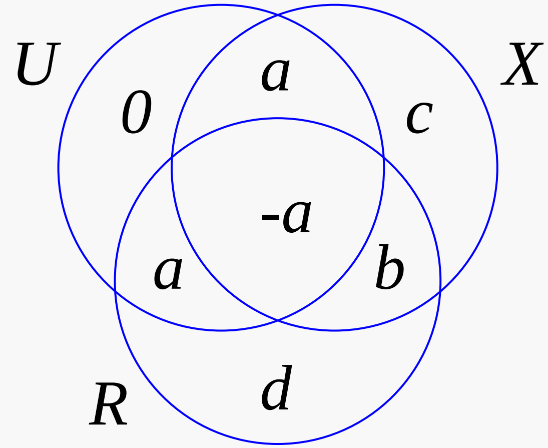
  If $P_U(u)$ is irrational for any $u \in \mathcal{U}$, then

  $$|\mathcal{X}| = |\mathcal{R}| = \infty.$$

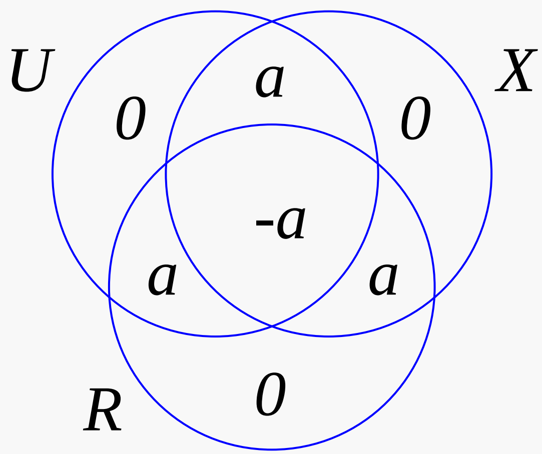
Constrained non-Shannon Type Inequalities



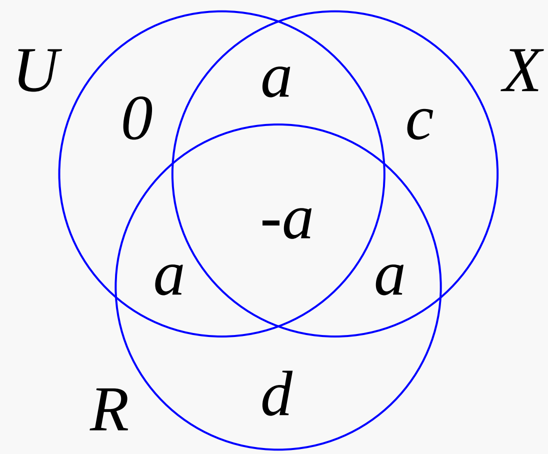
Thm. 1 in [Matúš 2006]



Thm. 1-3, Cor. 4



Ch. 15 in [Yeung 2008]



Thm. 9, Cor. 10, Thm. 11

Min. Number of Channel Uses

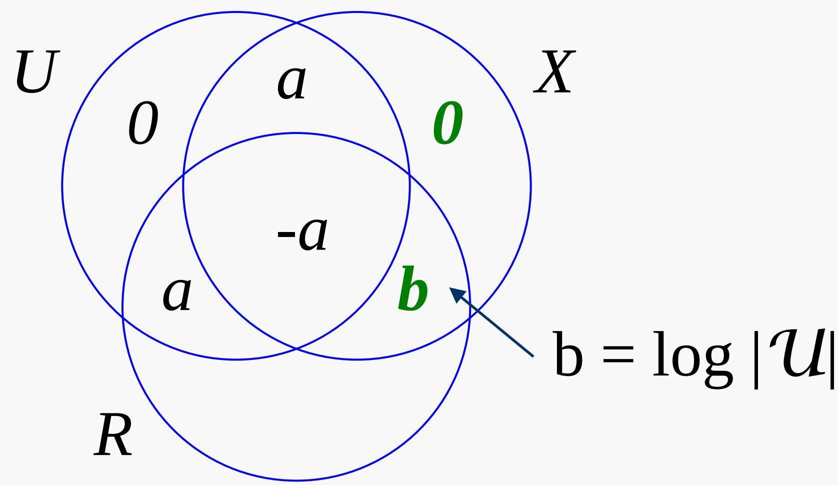
- Theorem 1 tells that $H(X) \geq \log |\mathcal{U}|$.
- We aim to minimize $I(R; XU)$ subject to $H(X) = \log |\mathcal{U}|$.

- If one-time pad is used,

  $H(U) \leq \log |\mathcal{U}| = H(X) = H(R) = I(R; XU)$.
- The effective key consumption $I(R; XU)$ is not minimal when the source U is not uniform.

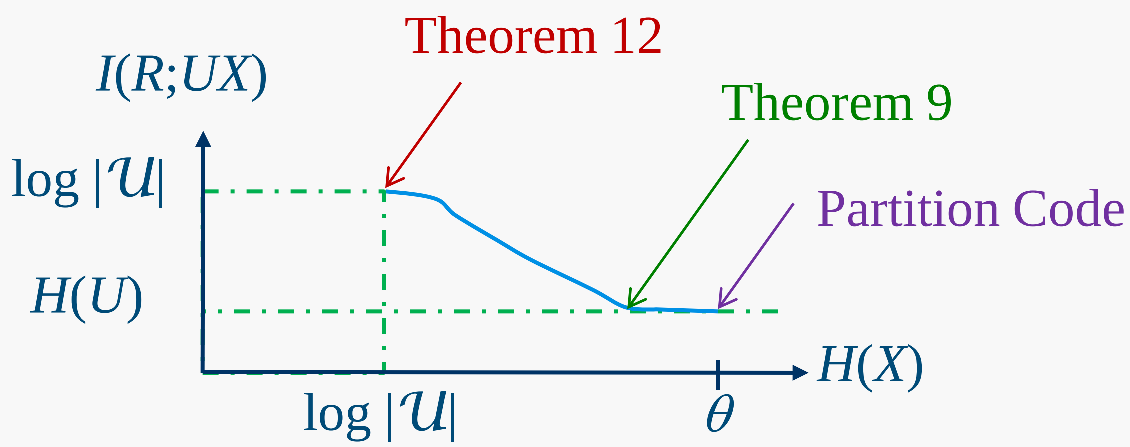
Min. Number of Channel Uses

- Theorem 12 For an EPS system, if $H(X) = \log |\mathcal{U}|$, then $I(R; UX) = \log |\mathcal{U}|$ and $H(X|RU) = 0$.



A Fundamental Tradeoff

- The minimum expected key consumption and the minimum number of channel use cannot be achieved simultaneously.



Conclusion

- We have studied perfect-secrecy systems with the assumption that the message and the secret key are independent.
- Under this setup, we have shown a new bound $\log|\mathcal{U}| \leq H(R)$ which is tighter than the one $H(U) \leq H(R)$.
- If $|\mathcal{U}| = \infty$, no security system can simultaneously achieve: i) perfect secrecy, ii) zero decoding error, iii) no side information.
- A new notion called effective key consumption $I(R;UX)$ is defined. It measures the amount of key used in an EPS system.
- If P_U is not uniform, the expected key consumption and the number of channel use cannot be minimized at the same time.
- There exists a fundamental tradeoff between these two parameters.

Q & A