

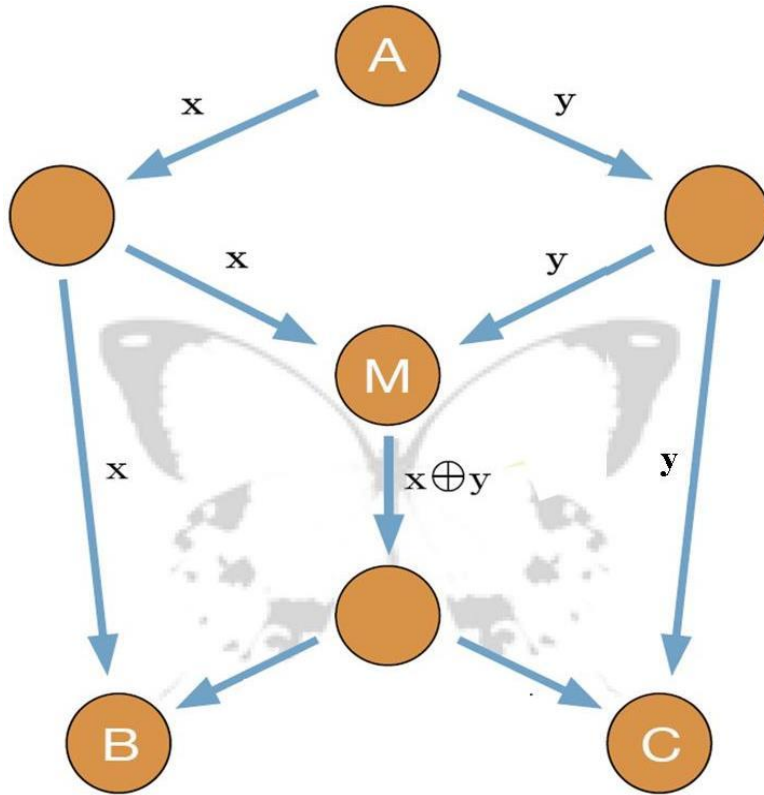
Performance Bounds in Secure Network Coding

Fan CHENG and Raymond W. YEUNG

Department of Information Engineering
The Chinese University of Hong Kong



Our Problem

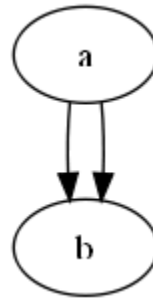


- Multicast message M from Source node (A) to destination nodes (B and C)
- Wiretappers can access the information on some edges
- How to keep the Perfect Secrecy of M?
- Strategy: Mix M with a random key K
- Question: max $H(M)$ and min $H(K)$?

Outline

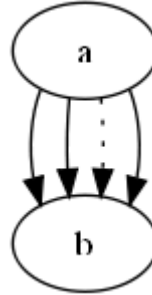
- Introduction
- Problem Formulation
- Our results
 - Upper bound on $H(M)$
 - Lower Bound on $H(K)$
 - An algorithm to compute the lower bound
 - Tightness of the lower bound

Perfect Secrecy



- Studied by Shannon (1949)
- A secure channel: private key (The key K)
- A public channel: the ciphertext ($M + K$)
- Conclusion: $H(K) \geq H(M)$ (One-time pad)

Wiretap Channel II



- Studied in Ozarow and Wyner (1984)
- A special case of secret sharing Shamir (1979)
- Binary data sequence S^K is transmitted as a N -bit binary data sequence S^N
- An intruder can intercept a subset of size r of the transmitted symbols
- Conclusion:
$$H(K) \geq \frac{r}{N-r} H(M)$$

Secure Network Coding over a Wiretap Network

- Wiretap Network Model (G, s, U, A)
 - Studied in Cai & Yeung (2002, 2010)
 - $G = (V, E)$, a directed acyclic graph (DAG)
 - For each pair of nodes (u, v) , there may be multiple edges with unit capacity
 - Source node s , M and K are generated here
 - Set of user nodes U , M is recovered at each user node u
 - Wiretap sets A , all the r -subset of E
- Admissible code
 - Satisfy the security condition
 - On each user node, M can be recovered

Secure Network Coding over a Wiretap Network

- Conclusion: Let q be the size of the alphabet and $n = \min_u \min cut(s, u)$
 - $H(M) : H(M) \leq (n - r) \log q$
 - $H(K) : H(K) \geq \frac{r}{n - r} H(M)$
- The bounds are tight and can be achieved by linear network coding.

Our Problem Setting

Wiretap Network (G, s, U, A)

- $G = (V, E)$: A directed acyclic graph (DAG)
- For each pair of nodes (u, v) , there may be multiple edges with unit capacity
- Source node s : M and K are generated here
- Set of user nodes U : Recover M at each user node u
- Wiretap sets A : **arbitrary subsets of E**

A Universal Approach for the Lower Bound on $H(K)$

- Objective: $\min \frac{H(K)}{H(M)}$
 - Source node s : $H(X_{(e_i: e_i \in \text{Out}(s))} | M, K) = 0$
 - Intermediate node v : $H(X_{(e_i: e_i \in \text{Out}(v))} | X_{(e_i: e_i \in \text{In}(v))}) = 0$
 - Destination node u : $H(M | X_{(e_i: e_i \in \text{In}(v))}) = 0$
 - Secure Condition: for each wiretap set l , $I(Y_l; M) = 0$
- A lower bound by invoking all the Shannon-type inequalities
 - Time complexity is exponential
 - The lower bound doesn't give much insight into the problem

Fractional Packing and Fractional Covering

$[n]: \{1, 2, \dots, n\}$

Fractional covering and Fractional packing

Given a collection C (hyper-graph) of subsets of $[n]$, a function $\alpha: C \rightarrow R^+$, is called a *fractional covering*, if for each $i \in [n]$, we have $\sum_{s \in C: i \in s} \alpha(s) \geq 1$.

Given C , a function $\beta: C \rightarrow R^+$ is a *fractional packing*, if for each $i \in [n]$, we have $\sum_{s \in C: i \in s} \beta(s) \leq 1$.

If $\gamma: C \rightarrow R^+$ is both a fractional covering and a fractional packing, we call γ a *fractional partition*.

Fractional Packing and Fractional Covering

Example

- Let $n=3$, $C=\{\{1,2\}, \{2,3\}, \{3,1\}\}$, $\{f_1, f_2, f_3\}$

	C_1	C_2	C_3	
1	f_1		f_3	f_1+f_3
2	f_1	f_2		f_1+f_2
3		f_2	f_3	f_2+f_3

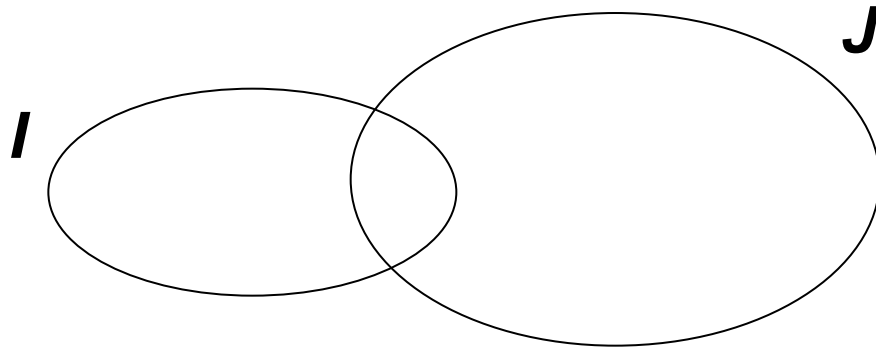
– fractional covering: $f_1 + f_3 \geq 1$, $f_1 + f_2 \geq 1$, $f_2 + f_3 \geq 1$;

– fractional packing: $f_1 + f_3 \leq 1$, $f_1 + f_2 \leq 1$, $f_2 + f_3 \leq 1$;

An Upper Bound on $H(M)$

- Let the size of the transmission alphabet F be q . Let J be a cut-set and I be a wiretap set. For any admissible code on G ,

$$H(M) \leq \min_{J,I} |J \setminus I| \log q$$



Madiman & Tetali's Inequality (2010)

- For any collection C of subsets of $[n]$, any fractional covering α and any fractional packing β ,

$$\sum_{s \in C} \beta(s) H(X_s | X_{s^c}) \leq H(X_{[n]}) \leq \sum_{s \in C} \alpha(s) H(X_s)$$

- Subsumes Han's inequalities (1978).

Lower Bounds on $H(K)$

- Fractional packing bound

Fix a cut-set J and let β be a fractional packing of $\{J \setminus I\}$, then

$$H(K) \geq \max_{\beta} \left(\sum_I \beta(J \setminus I) - 1 \right) H(M)$$

- Fractional covering bound

Fix a cut-set J and let α be a fractional covering of $\{I \cap J\}$, then

$$H(K) \geq \max_{\alpha} \frac{1}{\sum_I \alpha(I \cap J) - 1} H(M)$$

Lower Bounds on H(K)

The equivalence of these two bounds

Given a cut-set J , then

$$\max_{\beta} \left(\sum_I \beta(J \setminus I) - 1 \right) = \frac{1}{\min_{\alpha} \sum_I \alpha(I \cap J) - 1},$$

where α is a fractional covering of $\{I \cap J\}$ and β is a fractional packing of $\{J \setminus I\}$.

- ◆ Devise an algorithm whose time Complexity is $O(|E|^d (|V| + |E|))$, which is polynomial when d is a constant
- ◆ In general, the bound is not tight
- ◆ In the point to point communication system, the lower bound is tight.

Reference

- [1] C. E. Shannon, "Communication theory of secrecy systems," 1949.
- [2] A. Shamir, "How to share a secret," Communications of the ACM, 1979.
- [3] L. Ozarow and A. Wyner, "Wire-tap channel II," EUROCRYPT 84-A Workshop on the Theory and Application of Cryptographic Techniques, 1984.
- [4] N. Cai and R. W. Yeung, "Secure network coding," ISIT 2002 & IEEE IT 2010.
- [5] M. Madiman and P. Tetali, "Information inequalities for joint distribution, with interpretations and applications," IEEE IT 2010.