



Notions of Security

Computational Security

- Existing cryptosystems – public key as well as private key – are based on the notion of **computational security** or **complexity theoretic security**.
- Rely on the difficulty currently faced in solving a “hard” computational problem, e.g., the existence of “one-way” function.
- Recent advances in computing may present theoretical challenges to currently implemented cryptosystems.

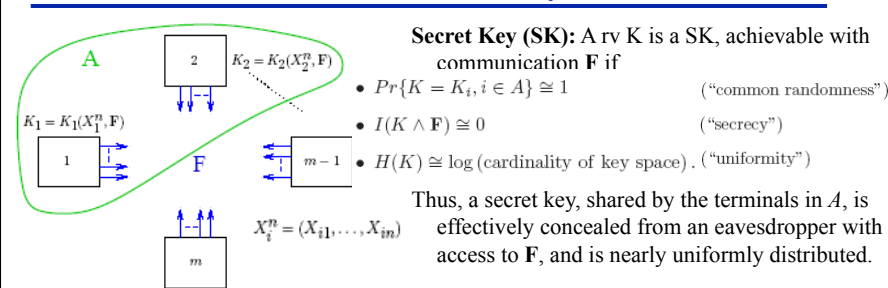
Information Theoretic Security

- A complementary approach for secret key cryptosystems
- Unconditional Security:** A **quantifiable and provable** notion of security, with no assumption of “one-way” functions and no restrictions on the computational power of adversary.
 - ? New insights: **Innate connections with multiterminal data compression.**
 - ??? New algorithms: **Potential rests on advances in algorithms for multiterminal data compression.**

Secret Key Generation

- Multiple terminals observe separate but correlated signals, e.g., different noisy version of a common broadcast signal or measurements of a parameter of the environment.
- The terminals wish to generate a **secret key**, to which end they then communicate publicly over a noiseless channel. A secret key is common randomness generated at each terminal which is **effectively concealed** from an eavesdropper with access to the public communication.
- The key generation procedure exploits the correlated nature of the observed signals.
- The secret key thereby generated can be used for encrypted communication.

What is Secret Key?



- Objectives:** (i) Determine the *largest entropy rate* of such a SK which can be achieved with suitable communication: **SK capacity** $C_S(A)$.
(ii) Generate such a SK of maximal rate.

The Model: Pairwise Reciprocal Channels

- $X_1 = (X_{12}, \dots, X_{1m})$
- $X_2 = (X_{21}, X_{23}, \dots, X_{2m})$
- $X_m = (X_{m1}, \dots, X_{m,m-1})$
- $X_i = (X_{ij}, j \in \{1, \dots, m\} \setminus \{i\}), i = 1, \dots, m.$
- X_{ij} is correlated with $X_{ji}, 1 \leq i \neq j \leq m.$
- (X_{ij}, X_{jk}) independent across $i, j.$

Secret Key Capacity for $A = \{1, \dots, m\}$

- By Csiszár-Narayan (2004):

$$C_S = H(X_1, \dots, X_m) - \max_{\lambda} \sum_B \lambda_B H(X_B | X_{B^c})$$

$$= \sum_{1 \leq i \neq j \leq m} H(X_{ij}, X_{ji}) - \max_{\lambda} \sum_B \lambda_B \left[\sum_{i \in B, j \in B^c} H(X_{ij} | X_{ji}) + \sum_{i \in B^c, j \in B} H(X_{ij}, X_{ji}) \right]$$
- Also, $C_S \leq C_S^{ub}$, where

$$C_S^{ub} = \min_{2 \leq k \leq m} \min_{\{B_1, \dots, B_k\} \text{ k-partition of } A} \frac{1}{k-1} \sum_{l=1}^{k-1} \sum_{i \in B_l, j \in \cup_{t=l+1}^k B_t} I(X_{ij} \wedge X_{ji})$$
- Remark:** Shall see that $C_S = C_S^{ub}$.

Secret Key Generation

- Generate independent pairwise SKs. For (i, j) , bet SK rate is $I(X_{ij} \wedge X_{ji}), 1 \leq i \neq j \leq m.$
- W.l.o.g., can assume all such SKs to consist of an integer number of bits.
- Consider a *complete* multigraph, with no. of edges between a pair of nodes = lengths of SK (bits).
- An achievable common SK length = max no. of edge-disjoint spanning trees which can be packed in this multigraph.
- Consider N such edge-disjoint spanning trees Let T_1, \dots, T_N . be $B = \{B_1, \dots, B_k\}, \dots, m\}$. Then
No. of cross edges across $B \leq \sum_{l=1}^N (\text{No. of cross edges of } T_l \text{ across } B) \geq N(k-1),$
so that $N \leq \frac{1}{k-1} (\text{No. of cross edges across } B).$
Hence: max no. of edge-disjoint spanning trees $\leq \frac{\min_{2 \leq k \leq m} \min_{B=\{B_1, \dots, B_k\}} \frac{1}{k-1} (\text{No. of cross edges across } B)}{1}$ (*)
- By Nash-Williams and Tutte (1961): there exists a collection edge-disjoint spanning trees whose size = (*) above.
- Finally we observe that (*) = nC_S^{ub} .

Spanning Tree Packing and Secret Key Capacity

We note that for a multigraph M with nodes $1, \dots, m$, such that for every pair of node i, j , the number of edges between node i and j in M equals
max. no. of edge-disjoint spanning trees that can be packed in $M \leq C_S.$
In the present case, equality holds.

Poly-time Alg. Achieving

H. N. Gabow and H. H. Westermann, “Forests, Frames and Games: Algorithms for Matroid Sums and Applications,” *Algorithmica* 7 (1992)

Steiner Tree Packing and Secret Key Generation

- Given A , a Steiner tree (for A) is a tree that covers A .
- Connection with $C_S(A)$:
 - Let no. of edges between i and j be $I(X_{ij} \wedge X_{ji}), 1 \leq i \neq j \leq m.$
 - For every Steiner tree, we can generate 1 bit of SK for A .
 - Max. no. of Steiner trees that can be packed in $M \leq C_S(A).$
- Remarks:
 - Packing edge-disjoint Steiner trees may not achieve $C_S(A).$