Information Theoretic Network Secret Key Generation

Sirin Nitinawarat*, Chunxuan Ye, Prakash Narayan,
Alexander Barg and Alex Reznik

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

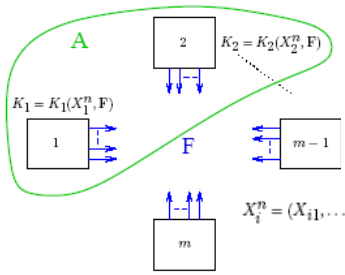
A complementary approach for secret key cryptosystems

- 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?



Secret Key (SK): A rv K is a SK, achievable with communication **F** if

- $Pr\{K = K_i, i \in A\} \cong 1$ ("common randomness")
- $I(K \wedge \mathbf{F}) \cong 0$ ("secrecy")
- $H(K) \cong \log(\text{cardinality of key space})$. ("uniformity")

Thus, a secret key, shared by the terminals in A, is effectively concealed from an eavesdropper with access to **F**, and is nearly uniformly distributed.

Objectives: (i) Determine the *larget 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

- $X_1 = (X_{12}, \ldots, X_{1m})$
- $X_2 = (X_{21}, X_{23}, \ldots, X_{2m})$
- $X_m = (X_{m1}, \ldots, X_{m,m-1})$
- $X_i = (X_{ij}, j \in \{1, \ldots, m\} \backslash \{i\}),\ i = 1, \ldots, m.$
- X_{ij} is correlated with X_{ji}, $1 \le i \ne j \le m$.
- (X_{ij}, X_{ji}) independent across i, j.

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

- By Csiszár-Narayan (2004):

$$\begin{aligned} C_S &= H(X_1, \ldots, X_m) - \max_{\lambda} \sum_B \lambda_B H(X_B | X_{B^c}) \\ &= \sum_{\substack{i \le i \ne j \le m \\ i<j}} H(X_{ij}, X_{ji}) \\ &\quad - \max_{\lambda} \sum_B \lambda_B \left[\sum_{i \in B,\, j \in B^c} H(X_{ij}|X_{ji}) + \sum_{\substack{i \in B,\, j \in B \\ i<j}} H(X_{ij}, X_{ji}) \right]. \end{aligned}$$

- Also, $C_S \le C_S^{ub}$, where

$$C_S^{ub} = \min_{2 \le k \le m} \min_{\substack{k-\text{partitions} \\ \{B_1, \ldots, B_k\}}} \frac{1}{k-1} \sum_{l=1}^{k-1} \left[\sum_{i \in B_l} \sum_{j \in \cup_{l'=l+1}^{k} B_{l'}} I(X_{ij} \wedge X_{ji}) \right].$$

- *Remark:* Shall see that $C_S = C_S^{ub}$.

Secret Key Generation

1. Generate independent pairwise SKs. For *(i, j)*, bet SK rate is $I(X_{ij} \wedge X_{ji}),\ 1 \le i \ne j \le m.$
2. W.l.o.g., can assume all such SKs to consist of an integer number of bits.
3. Consider a *complete* multigraph, with no. of edges between a pair of nodes = lengths of SK (bits).
4. An achievable common SK length = max no. of edge-disjoint spanning trees which can be packed in this multigraph.
5. Consider N such edge-disjoint spanning trees Let $T_1, \ldots, T_N$. be $\mathcal{B} = \{B_1, \ldots, B_k\}$, ..., $m\}$. Then

$$\begin{aligned} \text{No. of cross edges across } \mathcal{B} &\le \sum_{i=1}^{N} (\text{No. of cross edges of } T_i \text{ across } \mathcal{B}) \\ &\ge N(k-1), \end{aligned}$$

so that $N \le \frac{1}{k-1}$ (No. of cross edges across $\mathcal{B}$). Hence: max no. of edge-disjoint spanning trees

$$\le \min_{2 \le k \le m} \min_{\mathcal{B} = \{B_1, \ldots, B_k\}} \frac{1}{k-1} (\text{No. of cross edges across } \mathcal{B}) \qquad (*)$$

6. By Nash-Williams and Tutte (1961): there exists a collection edge-disjoint spanning trees whose size = (*) above.
7. Finally we observe that (*) = nC_S^{ub}.

Spanning Tree Packing and Secret Key Capacity

We note that for a multigraph M with nodes *1, … , 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 $\le C_S$.
In the present case, equality holds.

Poly-time Alg. Achieiving

H. N. Gabow and H. H. Westermainn,``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 $I(X_{ij} \wedge X_{ji}),\ 1 \le i \ne j \le m.$
  - For every Steiner tree, we can generate 1 bit of SK for A.
  - Max. no. of Steiner trees that can be packed in M $\le C_S(A)$.
- Remarks:
  - Packing edge-disjoint Steiner trees may not achieve $C_S(A)$.