INFORMATION THEORETIC NETWORK SECRET KEY GENERATION

Sirin Nitinawarat and Prakash Narayan
Jointly with A. Barg, C. Ye and A. Reznik

ISR @25 The Institute for Systems Research, A. JAMES CLARK SCHOOL OF ENGINEERING

Notions of Security

Computational Security

- Existing cryptosystems – public key as well as secret key – are based on the notion of computational security.
- This notion relies on the difficulty currently faced in solving a ``hard'' computational problem, e.g., the existence of ``one-way'' functions.
- Recent advances in computing may present theoretical challenges to currently implemented cryptosystems.

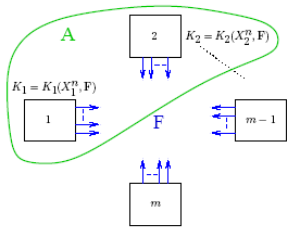
Information Theoretic Security

- 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.
- Benefits: Innate connections with multiterminal data compression and channel coding.
- Challeges: New algorithms for secret key construction.

Secret Key Generation by Public Communication

- Multiple user terminals observe separate but correlated signals, e.g., different noisy versions 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 secret key thereby generated can be used for encrypted communication.
- Application: Security with a one-time pad in a wireless network.

What is a Secret Key?



Secret Key (SK): K is a SK for A, achievable with communication $\mathbf{F}$ 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 $\mathbf{F}$, and is nearly uniformly distributed.

Objectives: (i) Determine the largest rate of such an achievable SK: SK capacity
(ii) Construct a SK of maximal rate.

Special Model I: Correlated Gaussian Signals

Let X_1 and X_2 be jointly Gaussian random variables with $X_1 \sim \mathcal{N}(0,\sigma_1^2)$, $X_2 \sim \mathcal{N}(0,\sigma_2^2)$, and $E[X_1X_2] = \rho\sigma_1\sigma_2, |\rho| < 1$. Then, the SK capacity is

$$C_S = I(X_1 \wedge X_2) = \frac{1}{2}\log\left(\frac{1}{1-\rho^2}\right).$$

Main Contributions:

(i) A new scheme for achieving the SK capacity C_S using structured codes: nested lattice codes and linear codes
(ii) A characterization of the optimum tradeoff between SK rate and quantization rate.

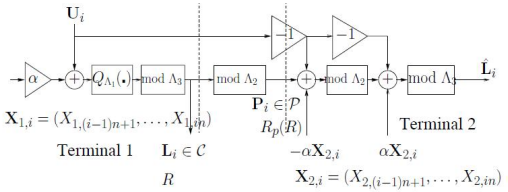
Special Model II: Pairwise Independent Network Model

- $X_1 = (X_{12}, \ldots, X_{1m})$
- $X_2 = (X_{21}, X_{23}, \ldots, X_{2m})$
- $X_m = (X_{m1}, \ldots, X_{m,m-1})$

- $X_i = (X_{ij}, j \in \{1,\ldots,m\}\backslash\{i\}),\ i = 1,\ldots,m.$
- X_{ij} is correlated with X_{ji}, $1 \le i \ne j \le m$.
- (X_{ij}, X_{ji}) independent across i, j.

Secret Key Generation Algorithm

For any fixed $R > 0$, both terminals agree on n-dim. nested lattice codes $\Lambda_1 \supset \Lambda_2 \supset \Lambda_3$ with a suitable selection of α as a function of $R, D, \sigma_X, \sigma_Y, \rho$.



Connection to Rate Distortion Theory

- $\mathbf{L}$ is approximately an optimum rate distortion codeword of $\mathbf{X}_1$ of rate R.
- $\mathbf{P}$ is approximately an optimum Wyner-Ziv codeword of $\mathbf{X}_1$ given $\mathbf{X}_2$ as side information, of rate

$$R_p(R) = \frac{1}{2}\log\left[\left(\left(e^{2R}-1\right)\left(1-\rho^2\right)+1\right)\right].$$

Tradeoff Between SK Rate and Quantization Rate

For any $R > 0$, there exist n-dimensional nested lattice codes $\Lambda_1 \supset \Lambda_2 \supset \Lambda_3$ such that the algorithm above produces a random variable $\mathbf{L}$ of rate arbitrarily close to R, from which a SK $K = \mathbf{L} - Q_{\Lambda_2}(\mathbf{L})$ can be constructed of rate

$$C(R) = \frac{1}{2}\log\left[\left(\left(1-\rho^2\right)+\rho^2 e^{-2R}\right)^{-1}\right].$$

Furthermore, $C(R)$ is optimum among all schemes with quantization at terminal 1 of rate R, followed by public communication based on the quantized signal at terminal 1.

Secret Key Capacity

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

Secret Key Generation Algorithm

1. Generate independent pairwise SKs. For *(i, j)*, best SK rate is

$$I(X_{ij}\wedge X_{ji}),\ 1 \le i \ne j \le m.$$

2. 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. Optimality: Using Nash-Williams and Tutte (1961), we show that our algorithms produces a SK of optimum rate.
6. Efficiency: Our algorithm has linear-time complexity in n.