

Notions of Security

1

Computational Security

- Existing cryptosystems – public key as well as secret key – are based on the notion of **computational security** or **complexity theoretic security**.
- 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.
- ? New insights: **Innate connections with multiterminal data compression.**
- ??? New algorithms: **Potential rests on advances in algorithms for multiterminal data compression.**

Secret Key Generation

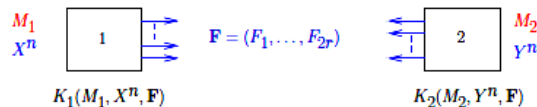
2

- Two terminals observe separate but correlated Gaussian signals arising from 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 key generation procedure exploits the correlation of the observed signals.
- The secret key thereby generated can be used for encrypted communication.
- Application: Security in a wireless environment.

What Is a Secret Key?

3

$\{(X_i, Y_i)\}_{i=1}^n \sim$ jointly Gaussian, i.i.d.



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

- $\Pr\{K = K_1 = K_2\} \cong 1$ (“common randomness”)
- mutual information $I(K \wedge F) \cong 0$ (“secrecy”)
- entropy $H(K) \cong \log(\text{size of key space})$. (“uniformity”)

Thus, a secret key, shared by the terminals 1 and 2, is effectively concealed from an eavesdropper with access to F , and is nearly uniformly distributed.

Objectives:

- Determine the *largest entropy rate of such a SK* which can be achieved with suitable communication: **SK capacity** C_S .
- Generate such a capacity-achieving SK using structured codes.

Secret Key Capacity

4

Theorem 1 : Let X, Y be jointly Gaussian \mathbb{R} -valued random variables with $X \sim \mathcal{N}(0, \sigma_x^2)$, $Y \sim \mathcal{N}(0, \sigma_y^2)$, and $E[XY] = \rho \sigma_x \sigma_y$, $\sigma_x^2 < \infty$, $\sigma_y^2 < \infty$, $|\rho| < 1$. Then, the SK capacity is

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

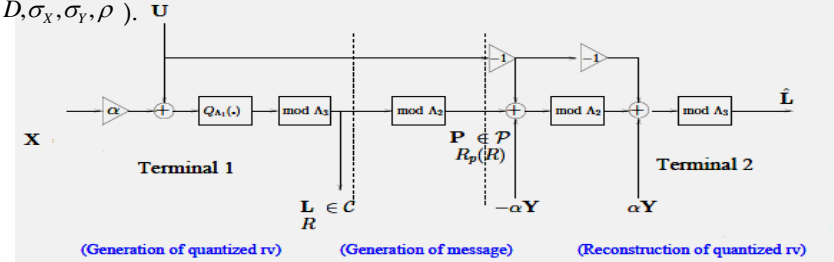
Main Contributions:

- A new scheme for achieving the SK capacity C_S using structured codes: nested lattice codes and linear codes
- A characterization of the associated tradeoff between SK rate and quantization rate.

Secret Key Generation Algorithm

5

For any fixed $R > 0$ and an arbitrary but fixed $D > 0$, let $\alpha = \left(\sqrt{D(e^{2R} - 1)} \right) \cdot (\sigma_x)^{-1}$. Both terminals agree on n -dim. nested lattice codes $\Lambda_1 \supset \Lambda_2 \supset \Lambda_3$ (selected according to $R, D, \sigma_x, \sigma_y, \rho$).



Connection to Rate Distortion Theory

- L is approximately an optimum rate distortion codeword of X of rate R .
- P is approximately an optimum Wyner-Ziv codeword of X given Y as side information, of rate $R_p(R) = \frac{1}{2} \log \left[\left((e^{2R} - 1)(1 - \rho^2) + 1 \right) \right]$.

Tradeoff Between SK Rate and Quantization Rate

6

Theorem 2 : For any $R > 0$, there exists n -dimensional nested lattice codes $\Lambda_1 \supset \Lambda_2 \supset \Lambda_3$ such that the algorithm above produces a random variable L of rate arbitrarily close to R , from which a SK $K = L - Q_{\Lambda_2}(L)$ can be generated of rate

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

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.

Summary

7

- Structured codes can achieve SK capacity.
- The optimum tradeoff between SK rate and quantization rate is characterized.
- The tradeoff is achievable by a SK generation scheme using structured codes that are optimum for certain lossy data compression problems.