# A Bit of Secrecy for Gaussian Source Compression

Eva C. Song, Paul Cuff, H. Vincent Poor
{ CSONG, CUFF, POOR }@PRINCETON.EDU

PRINCETON UNIVERSITY

## Problem

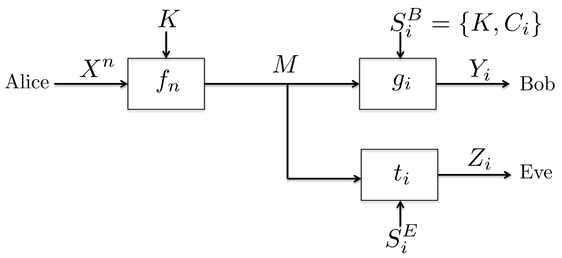
The compression of an i.i.d. Gaussian source sequence is studied in an unsecured network. Within a game theoretic setting for a three-party noiseless communication network (sender Alice, legitimate receiver Bob, and eavesdropper Eve), the problem of how to efficiently compress a Gaussian source with limited secret key in order to guarantee that Bob can reconstruct with high fidelity while preventing Eve from estimating an accurate reconstruction is investigated.

## Three cases

1. Weak eavesdropper $s_i^E = \{z^{i-1}\}$
2. Causal Source Awareness $s_i^E = \{x^{i-1}, z^{i-1}\}$
3. Causal General Awareness $s_i^E = \{x^{i-1}, y^{i-1}, z^{i-1}\}$

In all three cases, the SI of Bob is given by $k$ and $c_i = \{x^{i-1}, y^{i-1}, z^{i-1}\}$. It is sufficient to consider **only** $s_i^B = \{k\}$ which is independent of Bob's awareness of the eavesdropper.

## Problem Setup



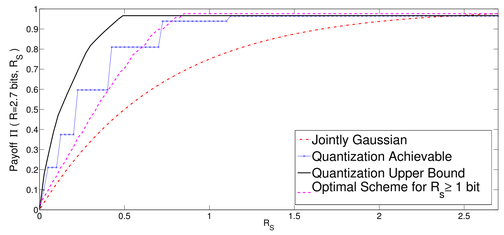

- $K \sim Unif[1 : 2^{nR_s}]$
- Encoder $f_n : \mathcal{X}^n \times \mathcal{K} \mapsto \mathcal{M}$
- Bob's decoder $\{g_i : \mathcal{M} \times \mathcal{S}_i^B \mapsto \mathcal{Y}\}_{i=1}^n$
- Eve's decoder $\{t_i : \mathcal{M} \times \mathcal{S}_i^E \mapsto \mathcal{Z}\}_{i=1}^n$
- Payoff $\pi(x, y, z) \triangleq \frac{1}{\sigma_0^2}[(z-x)^2 - (y-x)^2]$
- $\pi(x^n, y^n, z^n) \triangleq \frac{1}{n}\sum_{i=1}^n \pi(x_i, y_i, z_i)$

**Definition 1** *A secrecy rate-payoff triple* $(R, R_s, \Pi)$ *is achievable if* $K \in [1 : 2^{nR_s}]$, $M \in [1 : 2^{nR}]$, *and*

$$\lim_{n\to\infty} \sup_{\{f_n, \{g_i\}_{i=1}^n\}} \inf_{\{t_i\}_{i=1}^n} \mathbb{E}\pi(X^n, Y^n, Z^n) \geq \Pi.$$

## Numerical Computation

We numerically compare the payoffs under different schemes for the scenario of causal source awareness.




**Quantization achievable**:

$Y = nT$ and $U \triangleq n \mod N$. we greedily obtain an achievable lower bound by sequentially solving for the optimal $T$ that satisfies $R \geq I(X;U,Y)$ and the optimal $N$ that satisfies $R_s \geq I(X;Y|U)$.

**Scalar quantization upper bound**:

The quantization upper bound is numerically obtained by solving a linear programming problem.

## Results

**Theorem 1** *The secrecy rate-payoff triple* $(R, R_s, \Pi)$ *for a* ***weak eavesdropper*** *is achievable for an i.i.d. Gaussian source if and only if*

$$R_s > 0, \text{ and}$$

$$\Pi \leq 1 - \exp(-2R).$$

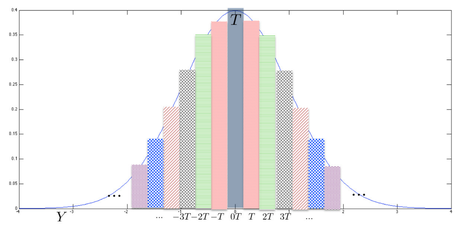
With **causal source awareness**, the general optimal payoff function

$$\Pi_{p_0}(R, R_s) = \max_{p(y,u|x)\in\mathcal{P}} \min_{z(u)} \mathbb{E}\pi(X, Y, z(U))$$

$$\mathcal{P} = \left\{ \begin{array}{l} p(y,u|x): \\ R_s \geq I(X;Y|U) \\ R \geq I(X;U,Y) \end{array} \right\}.$$

Jointly Gaussian does not do well here

$$\Pi_{p_0}(R, R_s) = 1 - \exp(-2\min(R_s, R)).$$




Gaussian Quantization

$$U = |Y|$$

$$H(Y) + \log T \to h(X), \text{ as } T \to 0$$

$$\Pi_{p_0}(R, R_s) \geq 1 - \tfrac{\pi e}{2} 2^{-2R} \text{ for } R_s \geq 1 \text{ bit}, R \to \infty.$$

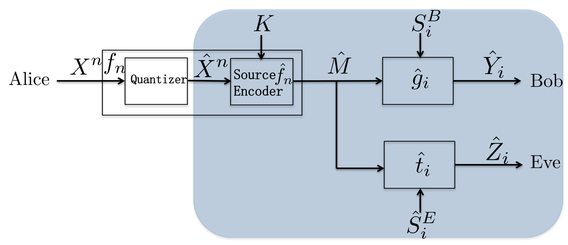
Achieving optimal payoff for $R_s \geq 1$ bit (Case 2 & 3)

**Theorem 2** *If the key rate* $R_s \geq 1$ *bit, the optimal secrecy rate-payoff function for an i.i.d. Gaussian source and* ***causal source awareness*** *is given by*

$$\Pi_{p_0}(R, R_s) = 1 - 2^{-2R}.$$

$Y$ is chosen such that $X$ and $Y$ are zero-mean jointly Gaussian. $U \triangleq |Y|$ and $V \triangleq sgn(Y)$.

## Special Case for Causal Source Awareness




$$\hat{X}_i = \mathbb{E}[X_i | \text{Quantization bin of } X_i]$$

$$\Pi_{p_0}^{\Delta}(R, R_s)$$

**Theorem 3** $\Pi_{p_0}^{\Delta}(R, R_s) = \frac{1}{\sigma_0^2} D_{\hat{p}_0}(R, R_s)$.

**Definition 2** *The rate-distortion triple* $(R, R_s, D)$ *is achievable if*

$$\mathbb{P}[\hat{Y}^n \neq \hat{X}^n] \to 0 \text{ as } n \to \infty, \text{ and}$$

$$\lim_{n\to\infty} \sup_{\{\hat{f}_n, \{\hat{g}_i\}_{i=1}^n\}} \inf_{\{\hat{t}_i(\hat{m}, \hat{s}_i^E)\}_{i=1}^n} \mathbb{E}\left[\frac{1}{n}\sum_{i=1}^n (\hat{Z}_i - \hat{X}_i)^2\right] \geq D.$$

$(R, R_s, D)$ is achievable iff $D \leq D_{\hat{p}_0}(R, R_s) \triangleq \max_{p(\hat{u}|\hat{x})\in\mathcal{Q}} \min_{\hat{z}(\hat{u})} \mathbb{E}[(\hat{z}(\hat{U}) - \hat{X})^2]$.

## References

[1] C. Schieler and P. Cuff, "Rate-distortion theory for secrecy systems," submitted to IEEE Trans. on Inf. Theory. http://arxiv.org/abs/1305.3905

[2] C. Schieler and P. Cuff, "Secrecy is cheap if the adversary must reconstruct," *ISIT*, Jul. 2012.

## Conclusion

For an eavesdropper that has causal information of Alice (and Bob), at most 1 bit of secret key is needed for each Gaussian source symbol to force maximum distortion to Eve while keeping the rate-distortion tradeoff at the same level as in point-to-point communication. Counter-intuitively, choosing the auxiliary random variable to be jointly Gaussian is not optimal.

## Acknowledgement

This work was supported by NSF Grants CCF-1116013 and CNS-09-05086, and AFOSR Grant FA9550-12-1-0196