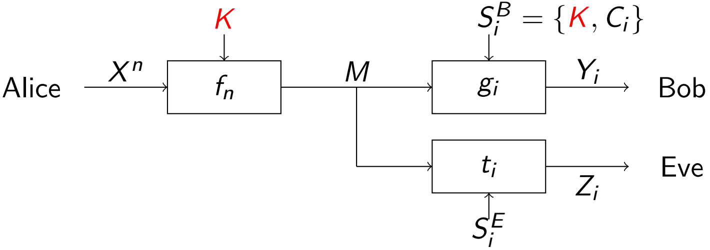
# A Bit of Secrecy for Gaussian Source Compression

Eva Song, Paul Cuff, and H. Vincent Poor

Department of Electrical Engineering
Princeton University

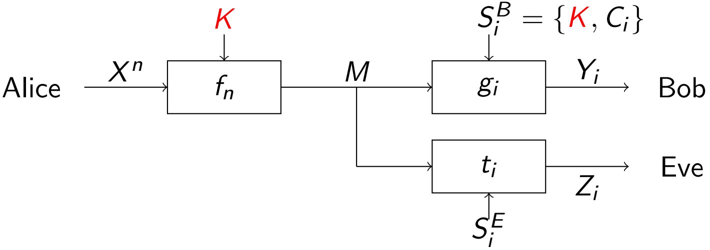
July 11, 2013

# Problem Setup



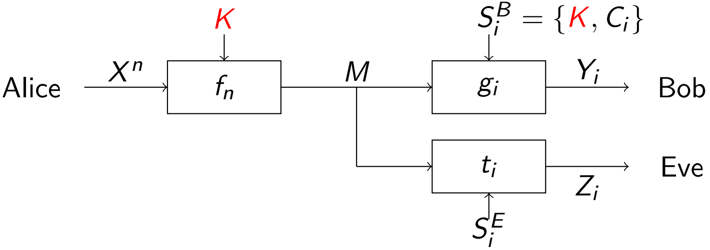

- $X^n$ i.i.d. with $X_i \sim \mathcal{N}(\mu_0, \sigma_0^2)$
- $K \sim Unif[1 : 2^{nR_s}]$

# Problem Setup



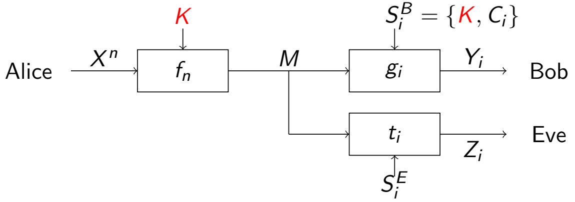

- $X^n$ i.i.d. with $X_i \sim \mathcal{N}(\mu_0, \sigma_0^2)$
- $K \sim Unif[1 : 2^{nR_s}]$
- Encoder $f_n : \mathcal{X}^n \times \mathcal{K} \mapsto \mathcal{M}$, $\mathcal{M} = [1 : 2^{nR}]$
- Bob's decoder $\{g_i : \mathcal{M} \times \mathcal{S}_i^B \mapsto \mathcal{Y}\}_{i=1}^n$, $C_i = \{X^{i-1}, Y^{i-1}, Z^{i-1}\}$
- Eve's decoder $\{t_i : \mathcal{M} \times \mathcal{S}_i^E \mapsto \mathcal{Z}\}_{i=1}^n$

# Problem Setup

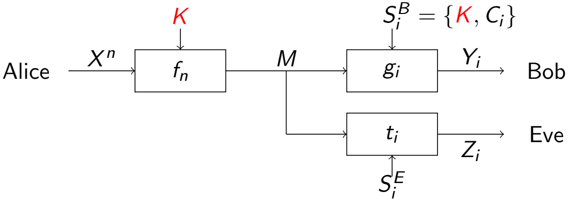



- $X^n$ i.i.d. with $X_i \sim \mathcal{N}(\mu_0, \sigma_0^2)$
- $K \sim Unif[1 : 2^{nR_s}]$
- Encoder $f_n : \mathcal{X}^n \times \mathcal{K} \mapsto \mathcal{M}$, $\mathcal{M} = [1 : 2^{nR}]$
- Bob's decoder $\{g_i : \mathcal{M} \times \mathcal{S}_i^B \mapsto \mathcal{Y}\}_{i=1}^n$, $C_i = \{X^{i-1}, Y^{i-1}, Z^{i-1}\}$
- Eve's decoder $\{t_i : \mathcal{M} \times \mathcal{S}_i^E \mapsto \mathcal{Z}\}_{i=1}^n$
- Payoff $\pi(x, y, z) \triangleq \frac{1}{\sigma_0^2}[(z - x)^2 - (y - x)^2]$
- $\pi(x^n, y^n, z^n) \triangleq \frac{1}{n}\sum_{i=1}^n \pi(x_i, y_i, z_i)$

# Three Cases

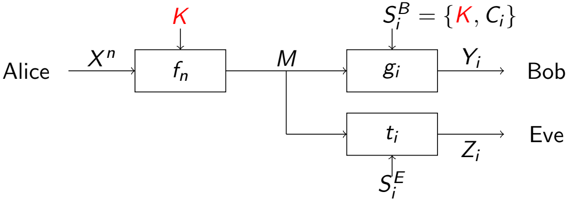


# Three Cases



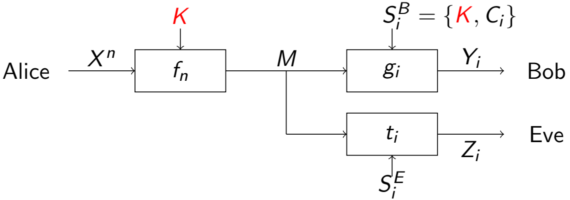

- Weak eavesdropper $s_i^E = \{z^{i-1}\}$

# Three Cases



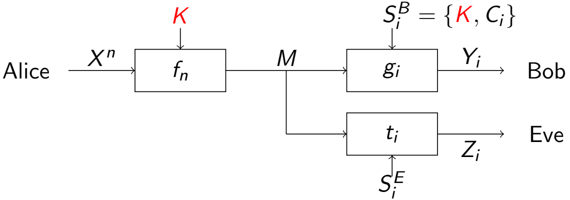

- Weak eavesdropper $s_i^E = \{z^{i-1}\}$
- Causal source awareness $s_i^E = \{x^{i-1}, z^{i-1}\}$

# Three Cases




- Weak eavesdropper $s_i^E = \{z^{i-1}\}$
- Causal source awareness $s_i^E = \{x^{i-1}, z^{i-1}\}$
- Causal general awareness $s_i^E = \{x^{i-1}, y^{i-1}, z^{i-1}\}$

# Three Cases




- Weak eavesdropper $s_i^E = \{z^{i-1}\}$
- Causal source awareness $s_i^E = \{x^{i-1}, z^{i-1}\}$
- Causal general awareness $s_i^E = \{x^{i-1}, y^{i-1}, z^{i-1}\}$

## Definition

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

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

# Overview

# Overview

- Weak eavesdropper
  - General source
  - General distortion measure
  - Lossless compression
  - ✓ $R_s > 0$, $R > H(X)$, $D_{\max} \triangleq \min_{\hat{x}} \mathbb{E} d(X, \hat{x})$ [Schieler & Cuff '12]

# Overview

- Weak eavesdropper
  - General source
  - General distortion measure
  - Lossless compression
  - ✓ $R_s > 0$, $R > H(X)$, $D_{\max} \triangleq \min_{\hat{x}} \mathbb{E} d(X, \hat{x})$ [Schieler & Cuff '12]
- Causal source/general awareness
  - General source
  - General payoff function
  - Lossy compression
  - ✓ $\Pi_{p_0}(R, R_s) = \max_{\mathcal{P}} \min_{z(u)} \mathbb{E}\pi(X, Y, z(U))$ [Cuff '10]

# Overview

- Weak eavesdropper
  - General source
  - General distortion measure
  - Lossless compression
  - ✓ $R_s > 0$, $R > H(X)$, $D_{\max} \triangleq \min_{\hat{x}} \mathbb{E} d(X, \hat{x})$ [Schieler & Cuff '12]
- Causal source/general awareness
  - General source
  - General payoff function
  - Lossy compression
  - ✓ $\Pi_{p_0}(R, R_s) = \max_{\mathcal{P}} \min_{z(u)} \mathbb{E}\pi(X, Y, z(U))$ [Cuff '10]
- Goal: optimize for Gaussian source

# Why do we consider this model?

- Gaussian source
- Tradeoff between lossy compression rate and secrecy
- Causal disclosure [Schieler & Cuff '13]

# Weak Eavesdropper

**Theorem**

*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*

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

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

- Maximum distortion between Alice and Eve
- Distortion-rate function for Gaussian source $R(D) = \frac{1}{2} \log \frac{\sigma_0^2}{D}$

# Causal Source Awareness

- General solution to any i.i.d. source sequence and payoff function:

$$
\begin{aligned}
\Pi_{p_0}(R, R_s) &= \max_{p(y,u|x)\in\mathcal{P}} \min_{z(u)} \mathbb{E}\pi(X, Y, z(U)) \\
\mathcal{P} &= \left\{ \begin{array}{l} p(y,u|x): \\ R_s \geq I(X; Y|U) \\ R \geq I(X; U, Y) \end{array} \right\}.
\end{aligned}
$$

# Causal Source Awareness

- General solution to any i.i.d. source sequence and payoff function:

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

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

- What $p(y, u|x)$ should we choose?

# Causal Source Awareness

- General solution to any i.i.d. source sequence and payoff function:

$$
\begin{aligned}
\Pi_{p_0}(R, R_s) &= \max_{p(y,u|x)\in\mathcal{P}} \min_{z(u)} \mathbb{E}\pi(X, Y, z(U)) \\
\mathcal{P} &= \left\{ \begin{array}{l} p(y, u|x) : \\ R_s \geq I(X; Y|U) \\ R \geq I(X; U, Y) \end{array} \right\}.
\end{aligned}
$$

- What $p(y, u|x)$ should we choose?

$$
\begin{aligned}
\Pi_{p_0}(R, R_s) &= \max_{p(y,u|x)\in\mathcal{P}} \min_{z(u)} \frac{1}{\sigma_0^2}\mathbb{E}[(z(U) - X)^2 - (Y - X)^2] \\
&= \frac{1}{\sigma_0^2} \max_{p(y,u|x)\in\mathcal{P}} \left[ \sum_{x,u} p(u|x)p_0(x)(x - \mathbb{E}[X|U = u])^2 \right. \\
&\quad \left. - \sum_{x,y} p(y|x)p_0(x)(y - x)^2 \right]
\end{aligned}
$$

# Why Is Jointly Gaussian Bad?

# Why Is Jointly Gaussian Bad?

If constraining $p(x, y, u)$ to be jointly Gaussian,

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

# Why Is Jointly Gaussian Bad?

If constraining $p(x, y, u)$ to be jointly Gaussian,

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

- Achievability:
  - $p(y|x)$ s.t. $X$ and $Y$ are jointly Gaussian
  - $I(X; Y) \leq \min(R_s, R)$
  - $U \perp X, Y$

# Why Is Jointly Gaussian Bad?

If constraining $p(x, y, u)$ to be jointly Gaussian,

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

- Achievability:
  - $p(y|x)$ s.t. $X$ and $Y$ are jointly Gaussian
  - $I(X; Y) \leq \min(R_s, R)$
  - $U \perp X, Y$
- Converse:
  - Fix $p(x, y, u)$ to be jointly Gaussian with correlations $\rho_{xy}$, $\rho_{xu}$ and $\rho_{yu}$

# Why Is Jointly Gaussian Bad?

If constraining $p(x, y, u)$ to be jointly Gaussian,

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

- Achievability:
  - $p(y|x)$ s.t. $X$ and $Y$ are jointly Gaussian
  - $I(X; Y) \leq \min(R_s, R)$
  - $U \perp X, Y$
- Converse:
  - Fix $p(x, y, u)$ to be jointly Gaussian with correlations $\rho_{xy}$, $\rho_{xu}$ and $\rho_{yu}$
  - Equivalent to $\max \rho_{xy}^2 - \rho_{xu}^2$

# Why Is Jointly Gaussian Bad?

If constraining $p(x, y, u)$ to be jointly Gaussian,

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

- Achievability:
  - $p(y|x)$ s.t. $X$ and $Y$ are jointly Gaussian
  - $I(X; Y) \leq \min(R_s, R)$
  - $U \perp X, Y$
- Converse:
  - Fix $p(x, y, u)$ to be jointly Gaussian with correlations $\rho_{xy}$, $\rho_{xu}$ and $\rho_{yu}$
  - Equivalent to $\max \rho_{xy}^2 - \rho_{xu}^2$
  - $R_s \geq \frac{1}{2}\log\frac{(1-\rho_{xu}^2)(1-\rho_{yu}^2)}{1-\rho_{xy}^2-\rho_{xu}^2-\rho_{yu}^2+2\rho_{xy}\rho_{xu}\rho_{yu}} \Rightarrow \rho_{xy}^2 - \rho_{xu}^2 \leq 1 - \exp(-2R_s)$

# Why Is Jointly Gaussian Bad?

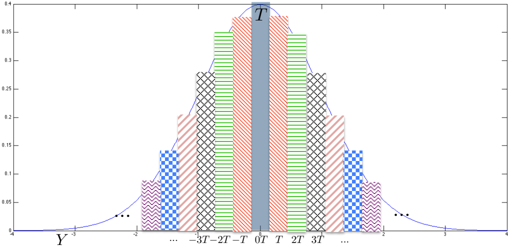
If constraining $p(x, y, u)$ to be jointly Gaussian,

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

- Achievability:
  - $p(y|x)$ s.t. $X$ and $Y$ are jointly Gaussian
  - $I(X;Y) \leq \min(R_s, R)$
  - $U \perp X, Y$
- Converse:
  - Fix $p(x, y, u)$ to be jointly Gaussian with correlations $\rho_{xy}$, $\rho_{xu}$ and $\rho_{yu}$
  - Equivalent to max $\rho_{xy}^2 - \rho_{xu}^2$
  - $R_s \geq \frac{1}{2}\log\frac{(1-\rho_{xu}^2)(1-\rho_{yu}^2)}{1-\rho_{xy}^2-\rho_{xu}^2-\rho_{yu}^2+2\rho_{xy}\rho_{xu}\rho_{yu}} \Rightarrow \rho_{xy}^2 - \rho_{xu}^2 \leq 1 - \exp(-2R_s)$
  - $R \geq \frac{1}{2}\log\frac{(1-\rho_{yu}^2)}{1-\rho_{xy}^2-\rho_{xu}^2-\rho_{yu}^2+2\rho_{xy}\rho_{xu}\rho_{yu}} \Rightarrow \rho_{xy}^2 - \rho_{xu}^2 \leq 1 - \exp(-2R)$

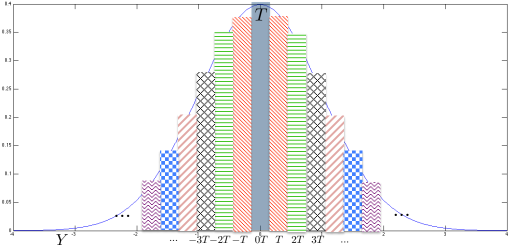
# Example: Gaussian Quantization

# Example: Gaussian Quantization



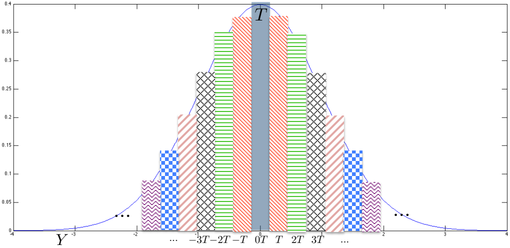

- $Y \triangleq nT$
- $U = |Y|$

# Example: Gaussian Quantization



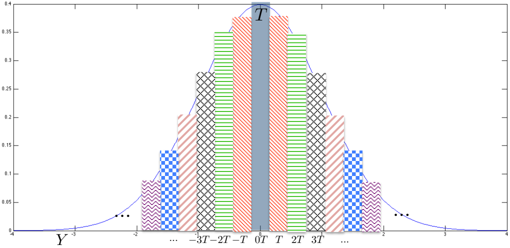

- $Y \triangleq nT$
- $U = |Y|$
- $X - \square - Y - \square - U$
- $\mathbb{E}[X|U = u] = 0$, for all $u$

# Example: Gaussian Quantization




- $Y \triangleq nT$
- $U = |Y|$
- $X - \square - Y - \square - U$
- $\mathbb{E}[X|U = u] = 0$, for all $u$
- $R_s \geq I(X; Y|U) = H(Y|U)$
  less than 1 bit
- $R \geq I(X; U, Y) = H(Y)$

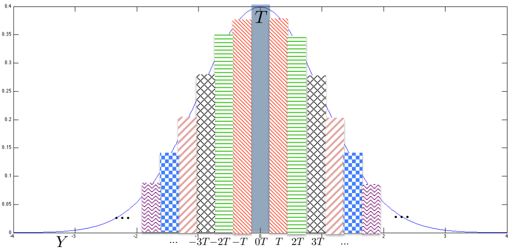
# Example: Gaussian Quantization




- $Y \triangleq nT$
- $U = |Y|$
- $X - \square - Y - \square - U$
- $\mathbb{E}[X|U = u] = 0$, for all $u$
- $R_s \geq I(X; Y|U) = H(Y|U)$
  less than 1 bit
- $R \geq I(X; U, Y) = H(Y)$

- $H(Y) + \log T \to h(X)$, as $T \to 0$
- Sufficient condition:
  $T \geq \sqrt{2\pi e}\sigma_0 2^{-R}$, for $R \to \infty$

# Example: Gaussian Quantization




- $Y \triangleq nT$
- $U = |Y|$
- $X - \square - Y - \square - U$
- $\mathbb{E}[X|U = u] = 0$, for all $u$
- $R_s \geq I(X; Y|U) = H(Y|U)$
  less than 1 bit
- $R \geq I(X; U, Y) = H(Y)$

- $H(Y) + \log T \to h(X)$, as $T \to 0$
- Sufficient condition:
  $T \geq \sqrt{2\pi e}\sigma_0 2^{-R}$, for $R \to \infty$
- Summarizing:
  $\Pi_{p_0}(R, R_s) \geq 1 - \frac{\pi e}{2} 2^{-2R}$
  for $R_s \geq 1$ bit and $R \to \infty$.

# Optimal Payoff for $R_s \geq 1$ bit

**Theorem**

*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*

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

# Converse

# Converse

- Recall:
  - $\frac{1}{\sigma_0^2} \max_{p(y,u|x)\in\mathcal{P}} \Big[ \sum_{x,u} p(u|x)p_0(x)(x - \mathbb{E}[X|U=u])^2$
    $- \sum_{x,y} p(y|x)p_0(x)(y-x)^2 \Big]$
  - $R_s \geq I(X;Y|U)$
  - $R \geq I(X;U,Y)$

# Converse

- Recall:
  - $\frac{1}{\sigma_0^2} \max_{p(y,u|x)\in\mathcal{P}} \Big[ \sum_{x,u} p(u|x)p_0(x)(x - \mathbb{E}[X|U=u])^2$
    $- \sum_{x,y} p(y|x)p_0(x)(y-x)^2 \Big]$
  - $R_s \geq I(X;Y|U)$
  - $R \geq I(X;U,Y)$
- Relax constraints on rates $R$ and $R_s$
- $\max_{p(y,u|x)} \sum_{u,x} p(u|x)p_0(x)(x - \mathbb{E}[X|U=u])^2 = \sigma_0^2$
- $\min_{p(y,u|x):I(X;Y)\leq R} \sum_{x,y} p(y|x)p_0(x)(y-x)^2 = \sigma_0^2 2^{-2R}$

# Achievability

# Achievability

Choose $p(y, u|x)$ s.t.

- $X$ and $Y$ are zero-mean jointly Gaussian

# Achievability

Choose $p(y, u|x)$ s.t.

- $X$ and $Y$ are zero-mean jointly Gaussian
- $U \triangleq |Y|$
- $V \triangleq sgn(Y)$
- $(U, V) \Leftrightarrow Y$

# Achievability

Choose $p(y, u|x)$ s.t.

- $X$ and $Y$ are zero-mean jointly Gaussian
- $U \triangleq |Y|$
- $V \triangleq sgn(Y)$
- $(U, V) \Leftrightarrow Y$
- Constraint on $R$: $I(X; Y, U) = I(X; Y)$
- Constraint on $R_s$: $I(X; Y|U) = I(X; V|U) < 1$ bit
- $\mathbb{E}[X|U = u] = \frac{1}{2}\mathbb{E}[X|Y = u] + \frac{1}{2}\mathbb{E}[X|Y = -u] = 0$, for all $u$

$\Rightarrow \Pi_{p_0}(R, R_s) = 1 - 2^{-2R}$ for $R_s \geq 1$ bit

# Causal General Awareness

- General solution to any i.i.d. source sequence and payoff function:

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

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

# Causal General Awareness

- General solution to any i.i.d. source sequence and payoff function:

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

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

**Theorem**

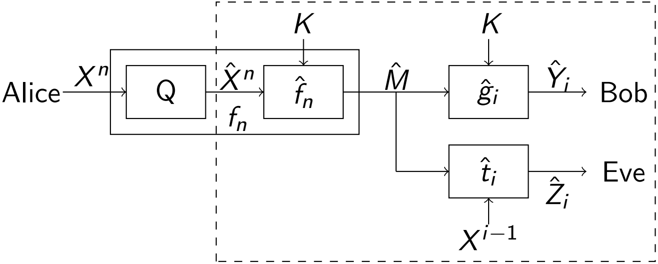
*If the key rate $R_s \geq 1$ bit, the optimal secrecy rate-payoff function for an i.i.d. Gaussian source and* **causal general awareness** *is given by*

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

# What do we do for $R_s < 1$ bit?

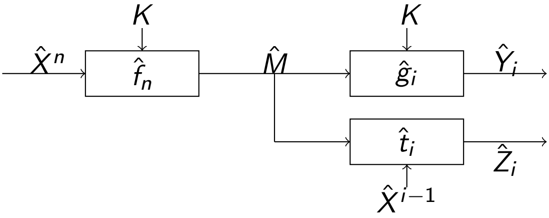
- Optimization too hard
- What if we quantize the source sequence symbol-by-symbol?

# Quantization Special Case for Causal Source Awareness




- Alice quantizes $X^n$ symbol-by-symbol $\hat{X}^n$ before transmission
- Bob reproduces the scalar quantization version $\hat{X}^n$
- $\hat{X}_i = \mathbb{E}[X_i|\text{Quantization bin of } X_i]$
- What is the optimal payoff function $\Pi^{\Delta}_{p_0}(R, R_s)$?

# Lossless Compression




## Definition

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

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

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

# Lossless Compression Rate Distortion

- $\hat{X} \sim \hat{p}_0$
- $\mathcal{Q} = \{p(\hat{u}|\hat{x}) : R \geq H(\hat{X}), R_s \geq H(\hat{X}|\hat{U})\}$
- $D_{\hat{p}_0}(R, R_s) \triangleq \max_{p(\hat{u}|\hat{x}) \in \mathcal{Q}} \min_{\hat{z}(\hat{u})} \mathbb{E}[(\hat{z}(\hat{U}) - \hat{X})^2]$

**Theorem 4.1 [Cuff '10]**

*$(R, R_s, D)$ is achievable iff*

$$D \leq D_{\hat{p}_0}(R, R_s)$$

# Applying Result from Lossless Compression

# Applying Result from Lossless Compression

**Lemma**

$X_i - \square - (\hat{M}, \hat{X}^{i-1}) - \square - X^{i-1}$ *for all* $i = 1, ..., n$

# Applying Result from Lossless Compression

**Lemma**

$X_i - \square - (\hat{M}, \hat{X}^{i-1}) - \square - X^{i-1}$ *for all* $i = 1, ..., n$

**Theorem**

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

- $D_{\hat{p}_0}(R, R_s)$ can be calculated as a linear program.

# Numerical Result for Causal Source Awareness

# Numerical Result for Causal Source Awareness

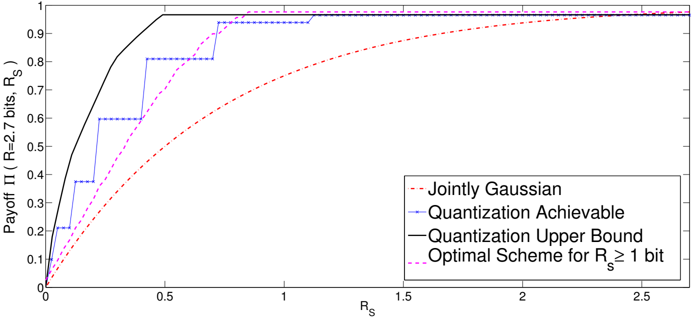
A simple quantization scheme

- Given $T$ and $N$
- $Y \triangleq nT$
- $U \triangleq n \bmod N$
- Greedily solve for optimal $T$ s.t. $R \geq I(X; U, Y)$
- Solve for optimal $N$ s.t. $R_s \geq I(X; Y|U)$

# Numerical Result for Causal Source Awareness

A simple quantization scheme

- Given $T$ and $N$
- $Y \triangleq nT$
- $U \triangleq n \bmod N$
- Greedily solve for optimal $T$ s.t. $R \geq I(X; U, Y)$
- Solve for optimal $N$ s.t. $R_s \geq I(X; Y|U)$



# Conclusion

- Weak eavesdropper ✓
  - $R_s > 0$
  - Bob: Rate-distortion
  - Eve: Maximum distortion
- Causal source awareness
  - Jointly Gaussian sub-optimal
  - $R_s \geq 1$ bit ✓
  - $R_s < 1$ bit symbol-by-symbol
- Causal general awareness
  - Jointly Gaussian sub-optimal
  - $R_s \geq 1$ bit ✓