Secret Communication under Plausible Deniability

FSU Theory Reading Group

Xiaoyu Cheng

Florida State University

Yonggyun (YG) Kim

Florida State University

Pak Hang (Michael) Tam

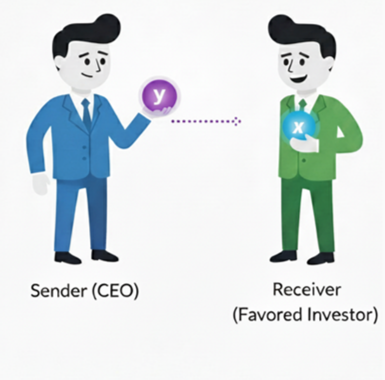
University of North Carolina, Chapel Hill

October 27, 2025

Motivation

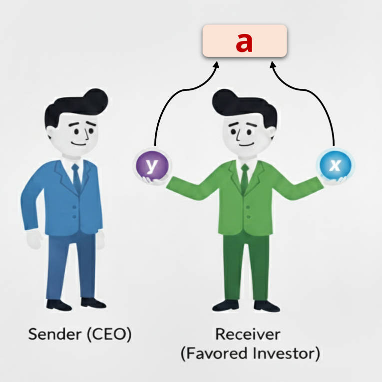
Motivation: Insider Trading

- A CEO wants to secretly pass a valuable "tip" to a favored investor, who already has his own private information.
- The investor uses *all* this information—his own & the CEO's tip—to make a decision.
  - The CEO wants to give the most helpful tip possible.
- An outside investigator may be watching.
  - How can CEO give a useful tip that is also "safe" and won't get them into trouble even if they are investigated?



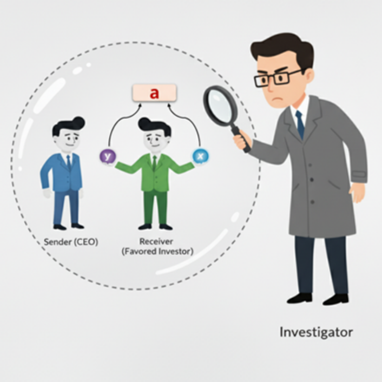
Motivation: Insider Trading

- A CEO wants to secretly pass a valuable "tip" to a favored investor, who already has his own private information.
- The investor uses *all* this information—his own & the CEO's tip—to make a decision.
  - The CEO wants to give the most helpful tip possible.
- An outside investigator may be watching.
  - How can CEO give a useful tip that is also "safe" and won't get them into trouble even if they are investigated?



Motivation: Insider Trading

- A CEO wants to secretly pass a valuable "tip" to a favored investor, who already has his own private information.
- The investor uses *all* this information—his own & the CEO's tip—to make a decision.
  - The CEO wants to give the most helpful tip possible.
- An outside investigator may be watching.
  - How can CEO give a useful tip that is also "safe" and won't get them into trouble even if they are investigated?



Motivation: What Makes Communication "Safe"?

- To avoid trouble, the Sender's tip must be defensible under investigation.
  1. **Secrecy**: The tip must be meaningless on its own. [Shannon, 1949]
     - An explicit message like "Buy the stock!" is not secret. The message itself is incriminating evidence.
  2. **Plausible Deniability**: The Receiver's final action must be justifiable without revealing the tip.
     - The investor must be able to claim, "Given what I already knew privately, my decision makes perfect sense." This creates a credible cover story.
- **Main Question:** What is the most informative signal the Sender can design under these constraints?

Motivation: What Makes Communication "Safe"?

- To avoid trouble, the Sender's tip must be defensible under investigation.
    1. **Secrecy**: The tip must be meaningless on its own. [Shannon, 1949]
        - An explicit message like "Buy the stock!" is not secret. The message itself is incriminating evidence.
    2. **Plausible Deniability**: The Receiver's final action must be justifiable without revealing the tip.
        - The investor must be able to claim, "Given what I already knew privately, my decision makes perfect sense." This creates a credible cover story.
- **Main Question:** What is the most informative signal the Sender can design under these constraints?

Motivation: What Makes Communication “Safe”?

- To avoid trouble, the Sender’s tip must be defensible under investigation.
  1. **Secrecy**: The tip must be meaningless on its own. [Shannon, 1949]
     - An explicit message like “Buy the stock!” is not secret. The message itself is incriminating evidence.
  2. **Plausible Deniability**: The Receiver’s final action must be justifiable without revealing the tip.
     - The investor must be able to claim, “Given what I already knew privately, my decision makes perfect sense.” This creates a credible cover story.
- **Main Question:** What is the most informative signal the Sender can design under these constraints?

Motivation: What Makes Communication "Safe"?

- To avoid trouble, the Sender's tip must be defensible under investigation.
  1. **Secrecy**: The tip must be meaningless on its own. [Shannon, 1949]
     - An explicit message like "Buy the stock!" is not secret. The message itself is incriminating evidence.
  2. **Plausible Deniability**: The Receiver's final action must be justifiable without revealing the tip.
     - The investor must be able to claim, "Given what I already knew privately, my decision makes perfect sense." This creates a credible cover story.
- **Main Question:** What is the most informative signal the Sender can design under these constraints?

Setup

Setup: Preliminaries

- Players: Sender, (informed) Receiver and (outside) Investigator
- The state of the world $\omega \in \Omega := \{\omega_1, \cdots, \omega_N\}$ with prior $\mu \in \Delta(\Omega)$
    - Assume that μ has full support.
- Receiver receives a signal x from a fixed information structure $f : \Omega \to \Delta(X)$ where $X = \{x_1, \cdots, x_J\}$
- Sender designs a joint information structure $h : \Omega \to \Delta(X \times Y)$, generating an additional signal $y \in Y$
    - The marginal distribution of X must correspond to f
    - The marginal distribution of Y is denoted as $g : \Omega \to \Delta(Y)$

Setup: Preliminaries

- Players: Sender, (informed) Receiver and (outside) Investigator
- The state of the world $\omega \in \Omega := \{\omega_1, \cdots, \omega_N\}$ with prior $\mu \in \Delta(\Omega)$
  - Assume that μ has full support.
- Receiver receives a signal x from a fixed information structure $f : \Omega \to \Delta(X)$ where $X = \{x_1, \cdots, x_J\}$
- Sender designs a joint information structure $h : \Omega \to \Delta(X \times Y)$, generating an additional signal $y \in Y$
  - The marginal distribution of X must correspond to f
  - The marginal distribution of Y is denoted as $g : \Omega \to \Delta(Y)$

Setup: Preliminaries

- Players: Sender, (informed) Receiver and (outside) Investigator
- The state of the world $\omega \in \Omega := \{\omega_1, \cdots, \omega_N\}$ with prior $\mu \in \Delta(\Omega)$
    - Assume that μ has full support.
- Receiver receives a signal x from a fixed information structure $f : \Omega \to \Delta(X)$ where $X = \{x_1, \cdots, x_J\}$
- Sender designs a joint information structure $h : \Omega \to \Delta(X \times Y)$, generating an additional signal $y \in Y$
    - The marginal distribution of X must correspond to f
    - The marginal distribution of Y is denoted as $g : \Omega \to \Delta(Y)$

Setup: Preliminaries

- Players: Sender, (informed) Receiver and (outside) Investigator
- The state of the world $\omega \in \Omega := \{\omega_1, \cdots, \omega_N\}$ with prior $\mu \in \Delta(\Omega)$
  - Assume that μ has full support.
- Receiver receives a signal x from a fixed information structure $f : \Omega \to \Delta(X)$ where $X = \{x_1, \cdots, x_J\}$
- Sender designs a joint information structure $h : \Omega \to \Delta(X \times Y)$, generating an additional signal $y \in Y$
  - The marginal distribution of X must correspond to f
  - The marginal distribution of Y is denoted as $g : \Omega \to \Delta(Y)$

Setup: Utility and Optimal Actions

- The set of actions (by Receiver) is an ordered set $A = \{a_1, \cdots, a_L\}$
- A utility function $u : A \times \Omega \to \mathbb{R}$ satisfies the *single-crossing* property if for any actions $a' > a$ and states $\omega' > \omega$:

$$u(a', \omega) \ \geq (>) \ u(a, \omega) \qquad \Longrightarrow \qquad u(a', \omega') \ \geq (>) \ u(a, \omega').$$

  Let $\mathcal{U}_{SC}$ denote the class of single-crossing utilities.

- Optimal actions given $u \in \mathcal{U}_{SC}$:
  - $a_{x,y}(u)$ given (x, y)
  - $a_x(u)$ $(a_y(u))$ given x (y)
  - $a_\emptyset(u)$ without any signal

Setup: Utility and Optimal Actions

- The set of actions (by Receiver) is an ordered set $A = \{a_1, \cdots, a_L\}$
- A utility function $u : A \times \Omega \to \mathbb{R}$ satisfies the *single-crossing* property if for any actions $a' > a$ and states $\omega' > \omega$:

$$u(a', \omega) \ \geq (>) \ u(a, \omega) \qquad \Longrightarrow \qquad u(a', \omega') \ \geq (>) \ u(a, \omega').$$

  Let $\mathcal{U}_{SC}$ denote the class of single-crossing utilities.

- Optimal actions given $u \in \mathcal{U}_{SC}$:
  - $a_{x,y}(u)$ given (x, y)
  - $a_x(u)$ $(a_y(u))$ given x (y)
  - $a_\emptyset(u)$ without any signal

Setup: Utility and Optimal Actions

- The set of actions (by Receiver) is an ordered set $A = \{a_1, \cdots, a_L\}$
- A utility function $u : A \times \Omega \to \mathbb{R}$ satisfies the *single-crossing* property if for any actions $a' > a$ and states $\omega' > \omega$:

$$u(a', \omega) \ \geq (>) \ u(a, \omega) \qquad \Longrightarrow \qquad u(a', \omega') \ \geq (>) \ u(a, \omega').$$

  Let $\mathcal{U}_{SC}$ denote the class of single-crossing utilities.

- Optimal actions given $u \in \mathcal{U}_{SC}$:
  - $a_{x,y}(u)$ given (x, y)
  - $a_x(u)$ $(a_y(u))$ given x (y)
  - $a_\emptyset(u)$ without any signal

Setup: Utility and Optimal Actions

- The set of actions (by Receiver) is an ordered set $A = \{a_1, \cdots, a_L\}$

- A utility function $u : A \times \Omega \to \mathbb{R}$ satisfies the *single-crossing* property if for any actions $a' > a$ and states $\omega' > \omega$:

$$u(a', \omega) \ \geq (>) \ u(a, \omega) \qquad \Longrightarrow \qquad u(a', \omega') \ \geq (>) \ u(a, \omega').$$

  Let $\mathcal{U}_{SC}$ denote the class of single-crossing utilities.

- Optimal actions given $u \in \mathcal{U}_{SC}$:
  - $a_{x,y}(u)$ given (x, y)
  - $a_x(u)$ $(a_y(u))$ given x (y)
  - $a_\emptyset(u)$ without any signal

Setup: Observable Information across Players

Receiver

$u \in \mathcal{U}_{SC}$

Sender & Receiver

$h : \Omega \to \Delta(X \times Y)$

Public Information

$\mathcal{U}_{SC}$

$f : \Omega \to \Delta(X)$

$A = \{a_1, \cdots, a_L\}$

$g : \Omega \to \Delta(Y)$

$x, \ y$

$\mu \in \Delta(\Omega)$

$a_{\emptyset}(u), \ a_{x,y}(u)$

Setup: Designing Information

The sender's objective is to design a joint information as informative as possible subject to constraints

1. $h : \Omega \to \Delta(X \times Y)$ satisfies **secrecy** iff for all $u \in \mathcal{U}_{SC}$ and $y \in Y$,

$$a_y(u) = a_\emptyset(u).$$

2. $h : \Omega \to \Delta(X \times Y)$ satisfies **plausible deniability** iff for all $u \in \mathcal{U}_{SC}$ and $(x, y) \in X \times Y$, there exists $\tilde{u} \in \mathcal{U}_{SC}$ such that

$$a_{x,y}(u) = a_x(\tilde{u}) \qquad \text{and} \qquad a_\emptyset(u) = a_\emptyset(\tilde{u}).$$

Setup: Designing Information

The sender's objective is to design a joint information as informative as possible subject to constraints

1. $h : \Omega \to \Delta(X \times Y)$ satisfies **secrecy** iff for all $u \in \mathcal{U}_{SC}$ and $y \in Y$,

$$a_y(u) = a_\emptyset(u).$$

2. $h : \Omega \to \Delta(X \times Y)$ satisfies **plausible deniability** iff for all $u \in \mathcal{U}_{SC}$ and $(x, y) \in X \times Y$, there exists $\tilde{u} \in \mathcal{U}_{SC}$ such that

$$a_{x,y}(u) = a_x(\tilde{u}) \qquad \text{and} \qquad a_\emptyset(u) = a_\emptyset(\tilde{u}).$$

Setup: Designing Information

The sender's objective is to design a joint information as informative as possible subject to constraints

1. $h : \Omega \to \Delta(X \times Y)$ satisfies **secrecy** iff for all $u \in \mathcal{U}_{SC}$ and $y \in Y$,

$$a_y(u) = a_\emptyset(u).$$

2. $h : \Omega \to \Delta(X \times Y)$ satisfies **plausible deniability** iff for all $u \in \mathcal{U}_{SC}$ and $(x, y) \in X \times Y$, there exists $\tilde{u} \in \mathcal{U}_{SC}$ such that

$$a_{x,y}(u) = a_x(\tilde{u}) \qquad \text{and} \qquad a_\emptyset(u) = a_\emptyset(\tilde{u}).$$

2 by 2 Example

2 by 2 Example: Optimal Secret Information (w/o PD)

- $\Omega = \{\omega_L, \omega_H\}$, $X = \{L, H\}$

	L	H
ω_L	.8	.2
ω_H	.2	.8

2 by 2 Example: Optimal Secret Information (w/o PD)

- $\Omega = \{\omega_L, \omega_H\}$, $X = \{L, H\}$, $Y = \{T, F\}$

	LT	HF	LF	HT
ω_L	.8	.2	0	0
ω_H	0	0	.2	.8

2 by 2 Example: Optimal Secret Information (w/o PD)

- $\Omega = \{\omega_L, \omega_H\}$, $X = \{L, H\}$, $Y = \{T, F\}$

	LT	HF	LF	HT
ω_L	.8	.2	0	0
ω_H	0	0	.2	.8

	T	F
ω_L	.8	.2
ω_H	.8	.2

- This joint information structure is most informative and satisfies *secrecy*,

2 by 2 Example: Optimal Secret Information (w/o PD)

- $\Omega = \{\omega_L, \omega_H\}$, $X = \{L, H\}$, $Y = \{T, F\}$

	LT	HF	LF	HT
ω_L	.8	.2	0	0
ω_H	0	0	.2	.8

	T	F
ω_L	.8	.2
ω_H	.8	.2

- This joint information structure is most informative and satisfies *secrecy*, but it violates the *plausible deniability*

2 by 2 Example: Optimal Secret Information w/ PD

- $\Omega = \{\omega_L, \omega_H\}$, $X = \{L, H\}$, $Y = \{T, M(eaningless)\}$

	LT	HM	LM	HT
ω_L	.6	.2	.2	0
ω_H	0	.2	.2	.6

2 by 2 Example: Optimal Secret Information w/ PD

- $\Omega = \{\omega_L, \omega_H\}$, $X = \{L, H\}$, $Y = \{T, M(eaningless)\}$

	LT	HM	LM	HT
ω_L	.6	.2	.2	0
ω_H	0	.2	.2	.6

	T	M
ω_L	.6	.4
ω_H	.6	.4

- This joint information structure satisfies secrecy and plausible deniability,

2 by 2 Example: Optimal Secret Information w/ PD

- $\Omega = \{\omega_L, \omega_H\}$, $X = \{L, H\}$, $Y = \{T, M(eaningless)\}$

	LT	HM	LM	HT
ω_L	.6	.2	.2	0
ω_H	0	.2	.2	.6

	T	M
ω_L	.6	.4
ω_H	.6	.4

- This joint information structure satisfies secrecy and plausible deniability, and it is shown to be Blackwell more informative than any joint information structures that satisfies two conditions

2 by 2 Case: Theorem

- $\Omega = \{\omega_L, \omega_H\}$, $X = \{L, H\}$, wlog $f_L \geq f_H$

$$f = \begin{array}{c|cc} & L & H \\ \hline \omega_L & f_L & 1 - f_L \\ \omega_H & f_H & 1 - f_H \end{array}$$

2 by 2 Case: Theorem

- $\Omega = \{\omega_L, \omega_H\}$, $X = \{L, H\}$, wlog $f_L \geq f_H$, $Y = \{T, M(eaningless)\}$

$$h^* = \begin{array}{c|cccc} & LT & LM & HM & HT \\ \hline \omega_L & f_L - f_H & f_H & 1 - f_L & 0 \\ \omega_H & 0 & f_H & 1 - f_L & f_L - f_H \end{array}$$

2 by 2 Case: Theorem

- $\Omega = \{\omega_L, \omega_H\}$, $X = \{L, H\}$, wlog $f_L \geq f_H$, $Y = \{T, M(eaningless)\}$

$$h^* = \begin{array}{c|cccc} & LT & LM & HM & HT \\ \hline \omega_L & f_L - f_H & f_H & 1 - f_L & 0 \\ \omega_H & 0 & f_H & 1 - f_L & f_L - f_H \end{array}$$

Theorem 1

Suppose that $|\Omega| = |X| = 2$. For any joint information structure h satisfying plausible deniability and secrecy, h^* is more Blackwell informative than h.

Binary State and Multiple Signals

Binary State and Multiple Signals

- $\Omega = \{\omega_L, \omega_H\}$, $X = \{x_1, \cdots, x_J\}$, $f_L^j \equiv f(x_j|\omega_L)$ and $f_H^j \equiv f(x_j|\omega_H)$
- Define

$$\mathcal{L} = \left\{x_j \in X \ : \ f_L^j \geq f_H^j\right\} \qquad \text{and} \qquad \mathcal{H} = \left\{x_j \in X \ : \ f_L^j < f_H^j\right\}$$

- Define $h^*(x_j, y|\omega)$ as follows:

	jT	jM
ω_L	$f_L^j - f_H^j$	f_H^j
ω_H	0	f_H^j

$x_j \in \mathcal{L}$

	jM	jT
ω_L	f_L^j	0
ω_H	f_L^j	$f_H^j - f_L^j$

$x_j \in \mathcal{H}$

Binary State and Multiple Signals

- $\Omega = \{\omega_L, \omega_H\}$, $X = \{x_1, \cdots, x_J\}$, $f_L^j \equiv f(x_j|\omega_L)$ and $f_H^j \equiv f(x_j|\omega_H)$
- Define

$$\mathcal{L} = \left\{x_j \in X \ : \ f_L^j \geq f_H^j\right\} \qquad \text{and} \qquad \mathcal{H} = \left\{x_j \in X \ : \ f_L^j < f_H^j\right\}$$

- Define $h^*(x_j, y|\omega)$ as follows:

	jT	jM
ω_L	$f_L^j - f_H^j$	f_H^j
ω_H	0	f_H^j

$x_j \in \mathcal{L}$

	jM	jT
ω_L	f_L^j	0
ω_H	f_L^j	$f_H^j - f_L^j$

$x_j \in \mathcal{H}$

Binary State and Multiple Signals

- $\Omega = \{\omega_L, \omega_H\}$, $X = \{x_1, \cdots, x_J\}$, $f_L^j \equiv f(x_j|\omega_L)$ and $f_H^j \equiv f(x_j|\omega_H)$
- Define

$$\mathcal{L} = \left\{x_j \in X \ : \ f_L^j \geq f_H^j\right\} \qquad \text{and} \qquad \mathcal{H} = \left\{x_j \in X \ : \ f_L^j < f_H^j\right\}$$

- Define $h^*(x_j, y|\omega)$ as follows:

	jT	jM
ω_L	$f_L^j - f_H^j$	f_H^j
ω_H	0	f_H^j

$x_j \in \mathcal{L}$

	jM	jT
ω_L	f_L^j	0
ω_H	f_L^j	$f_H^j - f_L^j$

$x_j \in \mathcal{H}$

Binary State and Multiple Signals

Theorem 2

Suppose that $|\Omega| = 2$. For any joint information structure h satisfying plausible deniability and secrecy, h^* is more Blackwell informative than h.

▸ Proof Sketch

Multiple States and Binary Signal

Multiple States and Binary Signal

- $\Omega = \{\omega_1, \cdots, \omega_n\}$, $X = \{L, H\}$, wlog MLRP holds:

$$f_1^L \geq \cdots \geq f_n^L \qquad \text{and} \qquad f_1^H \leq \cdots \leq f_n^H$$

- Construct h^{**} with a set of signals $Y = \{1, \cdots, n-1, M\}$: Details
  - Upon receiving $y = M$, the posterior is the same as the prior
  - $y = k$ serves as a cutoff signal together with x:

Multiple States and Binary Signal

- $\Omega = \{\omega_1, \cdots, \omega_n\}$, $X = \{L, H\}$, wlog MLRP holds:

$$f_1^L \geq \cdots \geq f_n^L \qquad \text{and} \qquad f_1^H \leq \cdots \leq f_n^H$$

- Construct h^{**} with a set of signals $Y = \{1, \cdots, n-1, M\}$: ▸ Details
  - Upon receiving $y = M$, the posterior is the same as the prior
  - $y = k$ serves as a cutoff signal together with x:

Multiple States and Binary Signal

- $\Omega = \{\omega_1, \cdots, \omega_n\}$, $X = \{L, H\}$, wlog MLRP holds:

$$f_1^L \geq \cdots \geq f_n^L \qquad \text{and} \qquad f_1^H \leq \cdots \leq f_n^H$$

- Construct h^{**} with a set of signals $Y = \{1, \cdots, n-1, M\}$: ▸ Details
  - Upon receiving $y = M$, the posterior is the same as the prior
  - $y = k$ serves as a cutoff signal together with x:

Multiple States and Binary Signal

- $\Omega = \{\omega_1, \cdots, \omega_n\}$, $X = \{L, H\}$, wlog MLRP holds:

$$f_1^L \geq \cdots \geq f_n^L \qquad \text{and} \qquad f_1^H \leq \cdots \leq f_n^H$$

- Construct h^{**} with a set of signals $Y = \{1, \cdots, n-1, M\}$: ▸ Details
  - Upon receiving $y = M$, the posterior is the same as the prior
  - $y = k$ serves as a cutoff signal together with x:

Multiple States and Binary Signal

- $\Omega = \{\omega_1, \cdots, \omega_n\}$, $X = \{L, H\}$, wlog MLRP holds:

$$f_1^L \geq \cdots \geq f_n^L \qquad \text{and} \qquad f_1^H \leq \cdots \leq f_n^H$$

- Construct h^{**} with a set of signals $Y = \{1, \cdots, n-1, M\}$: Details
  - Upon receiving $y = M$, the posterior is the same as the prior
  - $y = k$ serves as a cutoff signal together with x:
    Prior belief:

ω_1	$\cdots$	ω_k	ω_{k+1}	$\cdots$	ω_n
μ_1	$\cdots$	μ_k	μ_{k+1}	$\cdots$	μ_n

Multiple States and Binary Signal

- $\Omega = \{\omega_1, \cdots, \omega_n\}$, $X = \{L, H\}$, wlog MLRP holds:

$$f_1^L \geq \cdots \geq f_n^L \qquad \text{and} \qquad f_1^H \leq \cdots \leq f_n^H$$

- Construct h^{**} with a set of signals $Y = \{1, \cdots, n-1, M\}$: ▸ Details
  - Upon receiving $y = M$, the posterior is the same as the prior
  - $y = k$ serves as a cutoff signal together with x:
    Posterior belief with (L, k):

ω_1	$\cdots$	ω_k	ω_{k+1}	$\cdots$	ω_n
$\frac{\mu_1}{\sum_{i=1}^k \mu_i}$	$\cdots$	$\frac{\mu_k}{\sum_{i=1}^k \mu_i}$	0	$\cdots$	0

Multiple States and Binary Signal

- $\Omega = \{\omega_1, \cdots, \omega_n\}$, $X = \{L, H\}$, wlog MLRP holds:

$$f_1^L \geq \cdots \geq f_n^L \qquad \text{and} \qquad f_1^H \leq \cdots \leq f_n^H$$

- Construct h^{**} with a set of signals $Y = \{1, \cdots, n-1, M\}$: ▸ Details
    - Upon receiving $y = M$, the posterior is the same as the prior
    - $y = k$ serves as a cutoff signal together with x:
      Posterior belief with (H, k):

ω_1	$\cdots$	ω_k	ω_{k+1}	$\cdots$	ω_n
0	$\cdots$	0	$\frac{\mu_{k+1}}{\sum_{i=k+1}^{n} \mu_i}$	$\cdots$	$\frac{\mu_n}{\sum_{i=k+1}^{n} \mu_i}$

Multiple States and Binary Signal

- h^{**} satisfies
  1. **Secrecy**: w/o x, the posterior is the same as the prior
  2. **Plausible Deniability**: when $(x, y) = (L, k)$, the receiver can pretend that her utility does not differ much across actions for higher states greater than k

Theorem 3

Suppose that $|X| = 2$. For any joint information structure h satisfying plausible deniability and secrecy, h^{**} is more Blackwell informative than h.

Multiple States and Binary Signal

- h^{**} satisfies
  1. **Secrecy**: w/o x, the posterior is the same as the prior
  2. **Plausible Deniability**: when $(x, y) = (L, k)$, the receiver can pretend that her utility does not differ much across actions for higher states greater than k

Theorem 3

Suppose that $|X| = 2$. For any joint information structure h satisfying plausible deniability and secrecy, h^{**} is more Blackwell informative than h.

Multiple States and Binary Signal

- h^{**} satisfies
  1. **Secrecy**: w/o x, the posterior is the same as the prior
  2. **Plausible Deniability**: when $(x, y) = (L, k)$, the receiver can pretend that her utility does not differ much across actions for higher states greater than k

Theorem 3

Suppose that $|X| = 2$. For any joint information structure h satisfying plausible deniability and secrecy, h^{**} is more Blackwell informative than h.

Conclusion

Conclusion

- **Summary**
  - Introduced **secrecy** and **plausible deniability** as formal constraints for communication.
  - Characterized the *Blackwell-optimal* joint information structures under these constraints for several key cases (2×2, $2 \times N$, $N \times 2$).
- **Future Directions**
  - Characterize the optimal signal for the general $N \times J$ case (multiple states and multiple signals).
  - Explore concrete applications of this framework, e.g., in finance (insider trading) or political economy.

Conclusion

- **Summary**
  - Introduced **secrecy** and **plausible deniability** as formal constraints for communication.
  - Characterized the *Blackwell-optimal* joint information structures under these constraints for several key cases (2×2, $2 \times N$, $N \times 2$).
- **Future Directions**
  - Characterize the optimal signal for the general $N \times J$ case (multiple states and multiple signals).
  - Explore concrete applications of this framework, e.g., in finance (insider trading) or political economy.

Appendix

Theorem 1 & 2: Proof Sketch

1. If h satisfies plausible deniability, it satisfies:

$$\begin{cases} h_L^{jk} \leq h_H^{jk}, & \text{if } f_L^j \leq f_H^j, \\ h_L^{jk} \geq h_H^{jk}, & \text{if } f_L^j \geq f_H^j, \end{cases} \quad \forall\, j,\ k, \tag{$\star$}$$

   or equivalently, for all j, k,

$$\begin{cases} \Pr(\omega_H|x_j, y_k) \geq \mu(\omega_H), & \text{if } \Pr(\omega_H|x_j) \geq \mu(\omega_H), \\ \Pr(\omega_H|x_j, y_k) \leq \mu(\omega_H), & \text{if } \Pr(\omega_H|x_j) \leq \mu(\omega_H), \end{cases}$$

2. h^* Blackwell dominates any h satisfying ($\star$)
3. h^* satisfies plausible deniability and secrecy.

Go Back

Theorem 1 & 2: Proof Sketch

1. If h satisfies plausible deniability, it satisfies:

$$\begin{cases} h_L^{jk} \leq h_H^{jk}, & \text{if } f_L^j \leq f_H^j, \\ h_L^{jk} \geq h_H^{jk}, & \text{if } f_L^j \geq f_H^j, \end{cases} \quad \forall\, j,\ k, \tag{$\star$}$$

2. h^* Blackwell dominates any h satisfying $(\star)$
   - We show this by constructing a garbling.

3. h^* satisfies plausible deniability and secrecy.

Go Back

Theorem 1 & 2: Proof Sketch

1. If h satisfies plausible deniability, it satisfies:

$$\begin{cases} h_L^{jk} \leq h_H^{jk}, & \text{if } f_L^j \leq f_H^j, \\ h_L^{jk} \geq h_H^{jk}, & \text{if } f_L^j \geq f_H^j, \end{cases} \quad \forall\, j,\ k, \tag{$\star$}$$

2. h^* Blackwell dominates any h satisfying ($\star$)

3. h^* satisfies plausible deniability and secrecy.

Go Back

Formal Construction of h^{**}

$$
f = \begin{array}{c|cc}
 & L & H \\
\hline
\omega_1 & f_1 & 1 - f_1 \\
\omega_2 & f_2 & 1 - f_2 \\
\vdots & \vdots & \vdots \\
\omega_{n-1} & f_{n-1} & 1 - f_{n-1} \\
\omega_n & f_n & 1 - f_n
\end{array}
$$

Go Back

Formal Construction of h^{**}

$$h^{**} = \begin{array}{c|ccccc|ccccc}
 & L_1 & L_2 & \cdots & L_{n-1} & L_M & H_M & H_1 & H_2 & \cdots & H_{n-1} \\
\hline
\omega_1 & f_1 - f_2 & f_2 - f_3 & \cdots & f_{n-1} - f_n & f_n & 1 - f_1 & 0 & 0 & \cdots & 0 \\
\omega_2 & 0 & f_2 - f_3 & \cdots & f_{n-1} - f_n & f_n & 1 - f_1 & f_1 - f_2 & 0 & \cdots & 0 \\
\omega_3 & 0 & 0 & \cdots & f_{n-1} - f_n & f_n & 1 - f_1 & f_1 - f_2 & f_2 - f_3 & \cdots & 0 \\
\vdots & \vdots & \vdots & & \ddots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\
\omega_n & 0 & 0 & \cdots & 0 & f_n & 1 - f_1 & f_1 - f_2 & f_2 - f_3 & \cdots & f_{n-1} - f_n
\end{array}$$

Go Back