

# Steganographie als informationstheoretisches Modell

Martin Bober

Hauptseminar Theoretische Nachrichtentechnik

14. Januar 2009

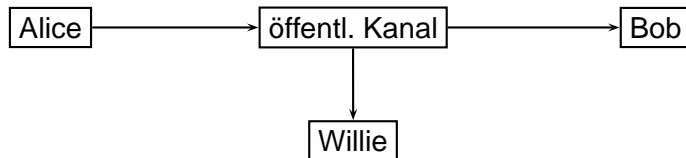
## 1 Einführung

- Prisoner's Problem
  - Variationen
  - Erweiterung des Szenarios
- Implementierung von Steganographie
  - Binäre Daten als Trägernachrichten
  - Texte als Trägernachrichten

## 2 Informationstheoretisches Modell

- Kodierung
- Willies Detektionsproblem
- Steganographische Sicherheit

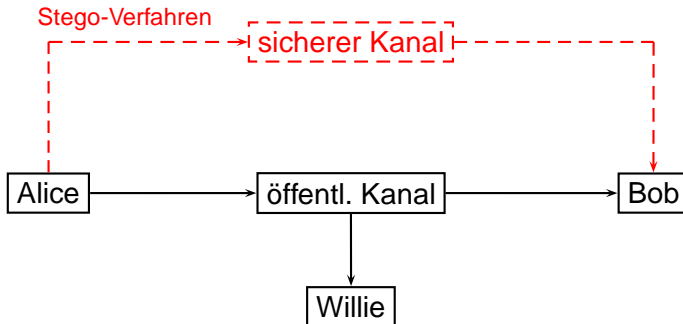
# Prisoner's Problem mit passivem Warter



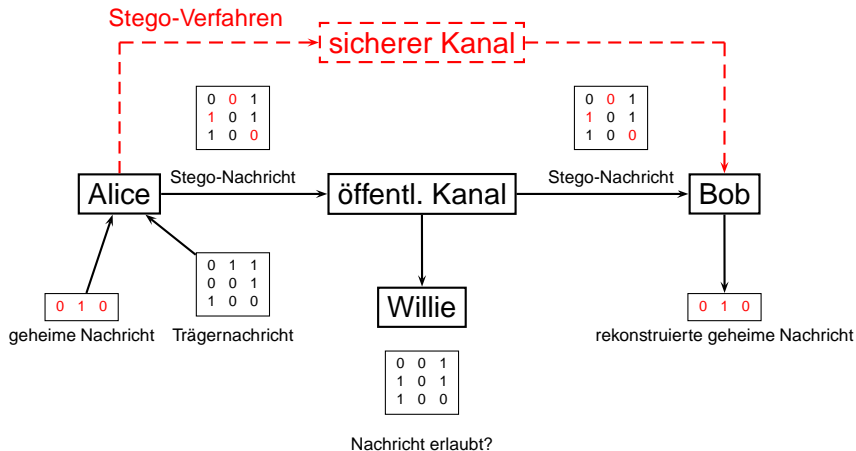
# Prisoner's Problem mit aktivem Warter



# Erweitertes Gefängnis-Szenario



# Lösung des Prisoner's Problem



# Bild als Trägernachricht - Beispiel 1

Das rechte Bild enthält den  $\text{\LaTeX}$ -Quelltext dieser Präsentation.



Stego-Parameter: Significance = 2, Distance = 9, Offset= 1

# Bild als Trägernachricht - Beispiel 2

Das rechte Bild enthält das Skript als PDF (ca 100kB).



Stego-Parameter: Significance = 4, Distance = 3, Offset= 0

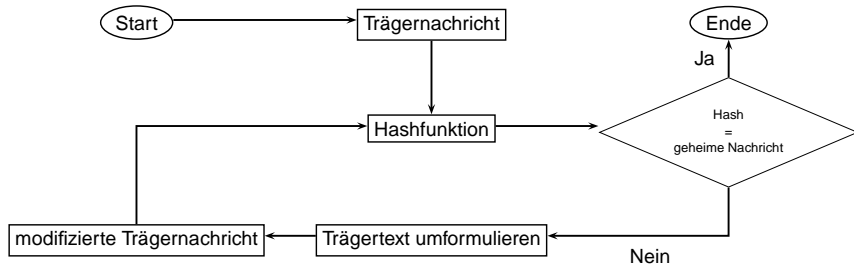
# Bild als Trägernachricht - Beispiel 2

Das rechte Bild enthält das Skript als PDF (ca 100kB).



Stego-Parameter: Significance = 8, Distance = 3, Offset= 0

# Texte als Trägernachrichten



- Trägernachricht:  $c \in \mathcal{C}$  mit Verteilung  $C$

- Trägernachricht:  $c \in \mathcal{C}$  mit Verteilung  $C$
- Geheime Nachricht:  $e \in \mathcal{E}$  mit Verteilung  $E$

- Trägernachricht:  $c \in \mathcal{C}$  mit Verteilung  $C$
- Geheime Nachricht:  $e \in \mathcal{E}$  mit Verteilung  $E$
- Stegonachricht:  $s \in \mathcal{S}$  mit Verteilung  $S$

- Trägernachricht:  $c \in \mathcal{C}$  mit Verteilung  $C$
- Geheime Nachricht:  $e \in \mathcal{E}$  mit Verteilung  $E$
- Stegonachricht:  $s \in \mathcal{S}$  mit Verteilung  $S$
- Stegoschlüssel:  $k \in \mathcal{K}$  mit Verteilung  $K$

- Trägernachricht:  $c \in \mathcal{C}$  mit Verteilung  $C$
- Geheime Nachricht:  $e \in \mathcal{E}$  mit Verteilung  $E$
- Stegonachricht:  $s \in \mathcal{S}$  mit Verteilung  $S$
- Stegoschlüssel:  $k \in \mathcal{K}$  mit Verteilung  $K$
- 1-Bit gleichverteilte Zufallsgröße:  $r \in \mathcal{R} = \mathbb{B}$  mit Verteilung  $R$

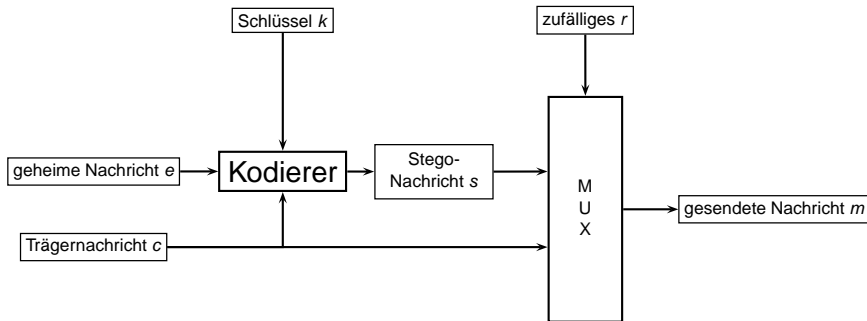
- Trägernachricht:  $c \in \mathcal{C}$  mit Verteilung  $C$
- Geheime Nachricht:  $e \in \mathcal{E}$  mit Verteilung  $E$
- Stegonachricht:  $s \in \mathcal{S}$  mit Verteilung  $S$
- Stegoschlüssel:  $k \in \mathcal{K}$  mit Verteilung  $K$
- 1-Bit gleichverteilte Zufallsgröße:  $r \in \mathcal{R} = \mathbb{B}$  mit Verteilung  $R$
- gesendete Nachricht:  $m \in \mathcal{M} = \mathcal{C} \cup \mathcal{S}$  mit Verteilung  $M$

- Trägernachricht:  $c \in \mathcal{C}$  mit Verteilung  $C$
- Geheime Nachricht:  $e \in \mathcal{E}$  mit Verteilung  $E$
- Stegonachricht:  $s \in \mathcal{S}$  mit Verteilung  $S$
- Stegoschlüssel:  $k \in \mathcal{K}$  mit Verteilung  $K$
- 1-Bit gleichverteilte Zufallsgröße:  $r \in \mathcal{R} = \mathbb{B}$  mit Verteilung  $R$
- gesendete Nachricht:  $m \in \mathcal{M} = \mathcal{C} \cup \mathcal{S}$  mit Verteilung  $M$
- Falls nicht anders angegeben, sind alle Logarithmen auf Basis 2 bezogen.

- 1  $H(M|C, E, K, R) = 0$ : Was Alice sendet wird ausschließlich von den Zufallsvariablen  $C$ ,  $E$ ,  $K$  und  $R$  bestimmt.

- 1  $H(M|C, E, K, R) = 0$ : Was Alice sendet wird ausschließlich von den Zufallsvariablen  $C$ ,  $E$ ,  $K$  und  $R$  bestimmt.
- 2  $H(E) > 0$ : Der Inhalt der geheimen Nachricht ist nicht determiniert.

- 1  $H(M|C, E, K, R) = 0$ : Was Alice sendet wird ausschließlich von den Zufallsvariablen  $C$ ,  $E$ ,  $K$  und  $R$  bestimmt.
- 2  $H(E) > 0$ : Der Inhalt der geheimen Nachricht ist nicht determiniert.
- 3  $H(E|S, K) = 0$ : Die geheime Nachricht muss von Bob unter Kenntnis von  $s$  und  $k$  dekodierbar sein.



- $\mathcal{H}_C$ :  $m$  ist eine reine Trägernachricht und wurde von der Verteilung  $C$  erzeugt.
- $\mathcal{H}_S$ :  $m$  ist eine Stego-Nachricht und wurde von der Verteilung  $S$  erzeugt.

# Mögliche Fehler beim Detektieren

- Typ I Fehler (Falschalarm) mit Wahrscheinlichkeit  $\alpha$
- Typ II Fehler (Detektionsversagen) mit Wahrscheinlichkeit  $\beta$

Optimale Detektionsregel:

$$\Lambda(m) = \log \frac{P_C(m)}{P_S(m)} \underset{\eta_S}{\overset{\eta_C}{\geq}} T \quad (1)$$

mit:

$\Lambda$  *log likelihood ratio*

$T$  Schwellwert für Entscheidung

Durch Detektionsentscheidung lassen sich zwei Verteilungen  $M_C$  und  $M_S$  über der Menge  $\mathcal{M}$  definieren:

$$P_{M_S}(m) = \begin{cases} 1 - \alpha & \text{für } m \in \mathcal{S} \\ \alpha & \text{für } m \in \mathcal{C} \end{cases}$$
$$P_{M_C}(m) = \begin{cases} 1 - \beta & \text{für } m \in \mathcal{C} \\ \beta & \text{für } m \in \mathcal{S} \end{cases}$$

Allgemein:

$$D(X||Y) = \sum_{x \in \mathcal{X}} P_X(x) \log \frac{P_X(x)}{P_Y(x)}$$

Speziell für binäre  $X, Y$ :

$$d(\alpha, \beta) = \alpha \log \frac{\alpha}{1 - \beta} + (1 - \alpha) \log \frac{1 - \alpha}{\beta}$$

Abschätzung für relative Entropie von  $C, S$  nach [2]:

$$D(M_C || M_S) \leq D(C || S) \quad (2)$$

Mit Kenntnis von  $M_C, M_S$ :

$$d(\alpha, \beta) \leq D(C || S) \quad (3)$$

Falls obere Schranke  $D(C||S) \leq \varepsilon$  existiert:

- obere Schranke für  $d(\alpha, \beta)$
- oft Vorgabe für  $\alpha$  (Bsp,  $\alpha = 0$ )
  - dann existiert untere Schranke für  $\beta \geq 2^{-\varepsilon}$
  - obere Schranke für Wahrscheinlichkeit, dass geheime Nachricht entdeckt wird:  $\gamma \leq 1 - 2^{-\varepsilon}$

## Definition: $\varepsilon$ -Sicherheit

Ein steganographisches System mit der Trägernachrichtenverteilung  $C$  und der Stegonachrichtenverteilung  $S$  heißt  $\varepsilon$ -*sicher* gegen passive Angreifer, wenn ein  $\varepsilon$  existiert, so dass für die relative Entropie  $D(C||S)$  gilt:

$$D(C||S) \leq \varepsilon \quad (4)$$

Für  $\varepsilon = 0$  heißt das System *absolut sicher*.

Es existieren Systeme, die nach obiger Definition sicher sind. Zwei Beispiele:

- One Time Pad
- Partitionierung von  $\mathcal{C}$

# One Time Pad (OTP)

$C$ : Gleichverteilung über  $\mathcal{B}^n$ ;  $k \in \mathbb{B}^n$

- Kodierung:  $s = e \oplus k$
- Dekodierung:  $e = s \oplus k$
- Durch OTP-Kodierung ist  $S$  ebenfalls eine Gleichverteilung.  
→  $D(C||S) = 0$

# Partitionierung von $\mathcal{C}$

Partitionierung von  $\mathcal{C}$  in Untermengen  $\mathcal{C}_0$  und  $\mathcal{C}_1$ , so dass  $\mathcal{C}$  über beide möglichst gleichverteilt ist:

$$\mathcal{C}_0 = \min_{\mathcal{C}' \subseteq \mathcal{C}} \left| \sum_{c \in \mathcal{C}'} P_{\mathcal{C}}(c) - \sum_{c \notin \mathcal{C}'} P_{\mathcal{C}}(c) \right| \quad \text{und} \quad \mathcal{C}_1 = \mathcal{C} \setminus \mathcal{C}_0$$

Senden von Nachricht  $m \in \mathcal{C}_{e \oplus k}$ .

Sei  $\delta = P(\mathbf{c} \in \mathcal{C}_0) - P(\mathbf{c} \in \mathcal{C}_1)$ .



$$P_S(\mathbf{c}) = \begin{cases} \frac{P_{\mathbf{C}}(\mathbf{c})}{1+\delta} & \text{für } \mathbf{c} \in \mathcal{C}_0 \\ \frac{P_{\mathbf{C}}(\mathbf{c})}{1-\delta} & \text{für } \mathbf{c} \in \mathcal{C}_1 \end{cases}$$

# Herleitung der Sicherheit II

Mit Hilfe von  $\log(1 + x) \leq \frac{x}{\ln 2}$ :

$$\begin{aligned} D(C||S) &= \sum_{c \in \mathcal{C}} P_C(c) \log \frac{P_C(c)}{P_S(c)} \\ &= \sum_{c \in \mathcal{C}_0} P_C(c) \log(1 + \delta) + \sum_{c \in \mathcal{C}_1} P_C(c) \log(1 - \delta) \\ &= \frac{1 + \delta}{2} \cdot \log(1 + \delta) + \frac{1 - \delta}{2} \cdot \log(1 - \delta) \\ &\leq \frac{1 + \delta}{2} \cdot \frac{\delta}{\ln 2} + \frac{1 - \delta}{2} \cdot \frac{-\delta}{\ln 2} = \frac{\delta^2}{\ln 2} = \epsilon \end{aligned}$$

Für gleichmäßige Partitionierung von  $\mathcal{C}$  ( $\delta = 0$ ) ist das System absolut sicher

-  ANDERSON, ROSS J. und FABIEN A.P. PETITCOLAS: *On The Limits Of Steganography*, 1997.
-  CACHIN, CHRISTIAN: *An Information-Theoretic Model for Steganography*.  
In: *Proceedings of 2nd Workshop on Information Hiding*.