

Universität Potsdam – Institut für Informatik
Seminar Kryptographie und Datensicherheit

Datensicherheit und Shannons Theorie

Marco Michael

2. November 2006

Sicherheit?
Wahrscheinlichkeitstheorie
Perfekte Sicherheit
Entropie
Gute Schlüssel
Literatur

Inhalt

Sicherheit?

Wahrscheinlichkeitstheorie

Perfekte Sicherheit

Entropie

Gute Schlüssel

Literatur

Sicherheit?

- Definitionsansätze

Wahrscheinlichkeitstheorie

Perfekte Sicherheit

Entropie

Gute Schlüssel

Literatur

Sicherheit?

Definitionsansätze für Sicherheit von Kryptosystemen

Sicherheit?

- Definitionsansätze

Wahrscheinlichkeitstheorie

Perfekte Sicherheit

Entropie

Gute Schlüssel

Literatur

Kryptosysteme haben ...

- rechenbetonte Sicherheit (*computational security*)
 - Mindestens N Rechenoperationen notwendig (N sehr groß)
 - Kann nur auf spezifische Attacken gezeigt werden
- beweisbare Sicherheit (*provable security*)
 - Reduzierung auf gut untersuchtes schweres Problem
 - Kein direkter Beweis für Sicherheit, da nur relativ zu einem anderen Problem
- unbedingte Sicherheit (*unconditional security*)
 - Keine Bedingung an Rechenoperationen
 - Selbst mit unbegrenzter Rechenkapazität nicht zu knacken

Untersuchung von Kryptosystemen auf unbedingte Sicherheit → Wahrscheinlichkeitstheorie

Sicherheit?

Wahrscheinlichkeitstheorie

- Einführung
- Satz von Bayes

Perfekte Sicherheit

Entropie

Gute Schlüssel

Literatur

Wahrscheinlichkeitstheorie

Sicherheit?

Wahrscheinlichkeitstheorie

• Einführung

• Satz von Bayes

Perfekte Sicherheit

Entropie

Gute Schlüssel

Literatur

Einführung

Definition 1: Eine *diskrete Zufallsgröße \mathbf{X}* besteht aus einer endlichen Menge X und einer auf X definierten *Wahrscheinlichkeitsverteilung*. Die Wahrscheinlichkeit, dass die Zufallsgröße \mathbf{X} den Wert x annimmt wird mit $\Pr[\mathbf{X} = x]$ bezeichnet (kurz $\Pr[x]$, falls \mathbf{X} fest). Weiterhin muss gelten $0 \leq \Pr[x], \forall x \in X$, und $\sum_{x \in X} \Pr[x] = 1$.

Definition 2: Sei \mathbf{X} eine Zufallsgröße definiert auf X . Dann heißt $E \subseteq X$ *Ereignis*. Die Wahrscheinlichkeit, dass \mathbf{X} einen Wert aus E annimmt, berechnet sich durch $\sum_{x \in E} \Pr[x]$.

Definition 3: Seien \mathbf{X} und \mathbf{Y} Zufallsgrößen auf den Mengen X bzw. Y . Die *Verbundwahrscheinlichkeit* $\Pr[x, y]$ (oder $\Pr[x \cap y]$) ist die Wahrscheinlichkeit, dass \mathbf{X} den Wert x annimmt und \mathbf{Y} den Wert y . Die *bedingte Wahrscheinlichkeit* $\Pr[x|y]$ bezeichnet die Wahrscheinlichkeit, dass \mathbf{X} den Wert x annimmt unter der Voraussetzung, dass \mathbf{Y} den Wert y hat.
Die Zufallsgrößen \mathbf{X} und \mathbf{Y} heißen *unabhängig*, falls $\Pr[x, y] = \Pr[x]\Pr[y]$ für alle $x \in X, y \in Y$.

Sicherheit?

Wahrscheinlichkeitstheorie

• Einführung

• Satz von Bayes

Perfekte Sicherheit

Entropie

Gute Schlüssel

Literatur

Beispiel – Wurf mit 2 Würfeln

Zufallsgröße Z definiert auf $Z = \{1, 2, 3, 4, 5, 6\} \times \{1, 2, 3, 4, 5, 6\}$

↪ $\Pr[(i, j)] = \frac{1}{36}$ für alle $(i, j) \in Z$

Betrachte Ereignis „Summe der Augenzahlen ist 4“

↪ $S_4 = \{(1, 3), (2, 2), (3, 1)\}$ dann ist $\Pr[S_4] = \frac{3}{36} = \frac{1}{12}$

i	$S_{2,12}$	$S_{3,11}$	$S_{4,10}$	$S_{5,9}$	$S_{6,8}$	S_7
$\Pr[S_i]$	$\frac{1}{36}$	$\frac{1}{18}$	$\frac{1}{12}$	$\frac{1}{9}$	$\frac{5}{36}$	$\frac{1}{6}$

Tabelle 1: Verteilung der Summen

Neue Zufallsgröße Y für Pasch oder Kein Pasch

↪ $\Pr[P] = \frac{1}{6}$ und $\Pr[K] = \frac{5}{6}$

↪ $\Pr[P, 4] = \Pr[4, P] = \frac{1}{36}$

↪ $\Pr[P|4] = \frac{1}{3}$ und $\Pr[4|P] = \frac{1}{6}$

Satz von Bayes

Sicherheit?

Wahrscheinlichkeitstheorie

• Einführung

• Satz von Bayes

Perfekte Sicherheit

Entropie

Gute Schlüssel

Literatur

- Frage: Zusammenhang zwischen Verbund- und bedingter Wahrscheinlichkeit?
- Antwort: Ja:

$$\Pr[x, y] = \Pr[x|y]\Pr[y] \text{ bzw. } \Pr[x, y] = \Pr[y|x]\Pr[x]$$

- Durch Umformung der Gleichungen erhält man

Satz von Bayes: Falls $\Pr[y] > 0$, dann

$$\Pr[x|y] = \frac{\Pr[x]\Pr[y|x]}{\Pr[y]}.$$

[Sicherheit?](#)

[Wahrscheinlichkeitstheorie](#)

[**Perfekte Sicherheit**](#)

- Annahmen
- Beispiel
- Definition
- Beispielsysteme

[Entropie](#)

[Gute Schlüssel](#)

[Literatur](#)

Perfekte Sicherheit

Sicherheit?

Wahrscheinlichkeitstheorie

Perfekte Sicherheit

• Annahmen

• Beispiel

• Definition

• Beispielsysteme

Entropie

Gute Schlüssel

Literatur

Annahmen

- Kryptosystem $(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$, gewählter Schlüssel $K \in \mathcal{K}$ nur für *eine* Verschlüsselung
- Wahrscheinlichkeitsverteilung auf \mathcal{P} mit Zufallsgröße \mathbf{x} , *a-priori*-Wahrscheinlichkeit dass Klartext x auftritt $\Pr[\mathbf{x} = x]$
- Schlüssel K nach fester Wahrscheinlichkeit ausgewählt, also Zufallsgröße \mathbf{K} und Wahrscheinlichkeit, dass Schlüssel K ausgewählt wurde $\Pr[\mathbf{K} = K]$
- \mathbf{x} und \mathbf{K} unabhängige Zufallsgrößen
- Zufallsgröße \mathbf{y} auf \mathcal{C} mit $\Pr[\mathbf{y} = y]$:
 - Menge möglicher Chiffrentexte, wenn K Schlüssel:

$$C(K) = \{e_K(x) | x \in \mathcal{P}\}$$

- Für alle $y \in \mathcal{C}$ gilt

$$\Pr[\mathbf{y} = y] = \sum_{\{K | y \in C(K)\}} \Pr[\mathbf{K} = K] \Pr[\mathbf{x} = d_K(y)]$$

Annahmen

Es lassen sich nun folgende bedingte Wahrscheinlichkeiten für jedes $y \in \mathcal{C}$ und $x \in \mathcal{P}$ berechnen:

- $\Pr[\mathbf{y} = y | \mathbf{x} = x]$:

$$\Pr[\mathbf{y} = y | \mathbf{x} = x] = \sum_{\{K | x = d_K(y)\}} \Pr[\mathbf{K} = K]$$

- $\Pr[\mathbf{x} = x | \mathbf{y} = y]$ (mittels Satz von Bayes):

$$\Pr[\mathbf{x} = x | \mathbf{y} = y] = \frac{\Pr[\mathbf{x} = x] \times \Pr[\mathbf{y} = y | \mathbf{x} = x]}{\Pr[\mathbf{y} = y]}$$

... oder ausführlicher ...

$$\Pr[\mathbf{x} = x | \mathbf{y} = y] = \frac{\Pr[\mathbf{x} = x] \times \sum_{\{K | x = d_K(y)\}} \Pr[\mathbf{K} = K]}{\sum_{\{K | y \in C(K)\}} \Pr[\mathbf{K} = K] \Pr[\mathbf{x} = d_K(y)]}$$

- [Sicherheit?](#)
- [Wahrscheinlichkeitstheorie](#)
- [Perfekte Sicherheit](#)
- Annahmen
- Beispiel
- Definition
- Beispielsysteme
- [Entropie](#)
- [Gute Schlüssel](#)
- [Literatur](#)

Beispiel

$$\mathcal{P} = \{a, b\} \text{ mit } \Pr[a] = \frac{1}{4}, \Pr[b] = \frac{3}{4}$$

$$\mathcal{K} = \{K_1, K_2, K_3\} \text{ mit } \Pr[K_1] = \frac{1}{2}, \Pr[K_2] = \Pr[K_3] = \frac{1}{4}$$

$\mathcal{C} = \{1, 2, 3, 4\}$ und die e_{K_i} gegeben durch die Matrix

	a	b
K_1	1	2
K_2	2	3
K_3	3	4

Die

Wahrscheinlichkeitsverteilung auf \mathcal{C} ist daher:

$$\Pr[1] = \frac{1}{8} \quad \Pr[2] = \frac{3}{8} + \frac{1}{16} = \frac{7}{16}$$

$$\Pr[3] = \frac{3}{16} + \frac{1}{16} = \frac{1}{4} \quad \Pr[4] = \frac{3}{16}$$

... nun lässt sich $\Pr[x = x | y = y]$ bestimmen

$$\Pr[a|1] = 1 \quad \Pr[b|1] = 0$$

$$\Pr[a|2] = \frac{1}{7} \quad \Pr[b|2] = \frac{6}{7}$$

$$\Pr[a|3] = \frac{1}{4} \quad \Pr[b|3] = \frac{3}{4}$$

$$\Pr[a|4] = 0 \quad \Pr[b|4] = 1$$

Sicherheit?
Wahrscheinlichkeitstheorie
Perfekte Sicherheit
• Annahmen
• Beispiel
• Definition
• Beispielsysteme
Entropie
Gute Schlüssel
Literatur

Definition

Definition: Ein Kryptosystem hat *perfekte Sicherheit*, falls $\Pr[x|y] = \Pr[x]$ für alle $x \in \mathcal{P}, y \in \mathcal{C}$.

Am Beispiel:

$$\begin{array}{ll} \Pr[a|1] = 1 \neq \Pr[a] = \frac{1}{4} & \Pr[b|1] = 0 \neq \Pr[b] = \frac{3}{4} \\ \Pr[a|2] = \frac{1}{7} \neq \Pr[a] = \frac{1}{4} & \Pr[b|2] = \frac{6}{7} \neq \Pr[b] = \frac{3}{4} \\ \Pr[a|3] = \frac{1}{4} = \Pr[a] = \frac{1}{4} & \Pr[b|3] = \frac{3}{4} = \Pr[b] = \frac{3}{4} \\ \Pr[a|4] = 0 \neq \Pr[a] = \frac{1}{4} & \Pr[b|4] = 1 \neq \Pr[b] = \frac{3}{4} \end{array}$$

→ Dieses Kryptosystem erfüllt die Voraussetzung für perfekte Sicherheit nur für den Chiffretext $y = 3$, daher insgesamt keine perfekte Sicherheit.

Satz: Sei $(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$ ein Kryptosystem mit $|\mathcal{K}| = |\mathcal{C}| = |\mathcal{P}|$. Dann bietet es perfekte Sicherheit, gdw. jeder Schlüssel mit gleicher Wahrscheinlichkeit $\frac{1}{|\mathcal{K}|}$ benutzt wird und $\forall x \in \mathcal{P}, y \in \mathcal{C}$ ein eindeutiger Schlüssel K existiert, so dass $e_K(x) = y$.

Beispiele für perfekt sichere Kryptosysteme

Sicherheit?

Wahrscheinlichkeitstheorie

Perfekte Sicherheit

- Annahmen
- Beispiel
- Definition
- Beispielsysteme

Entropie

Gute Schlüssel

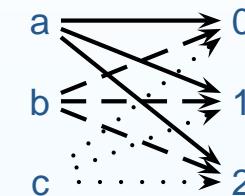
Literatur

1. Exemplarisch (nach [1])

	a	b	c
K_1	0	1	2
K_2	1	2	0
K_3	2	0	1

$$|\mathcal{K}| = |\mathcal{C}| = |\mathcal{P}| = 3$$

$$\Pr[K_i] = \frac{1}{3}$$



2. One-Time Pad (Beispielrealisierung)

- $n \in \mathbb{Z}, n \geq 1$ und $\mathcal{P} = \mathcal{C} = \mathcal{K} = (\mathbb{Z}_2)^n$
- $x = (x_1, \dots, x_n), K = (K_1, \dots, K_n), y = (y_1, \dots, y_n)$
- $e_K(x) = (x_1 + K_1, \dots, x_n + K_n) \bmod 2$ (entspricht \otimes)
- $d_K(y) = (y_1 + K_1, \dots, y_n + K_n) \bmod 2$ (entspricht \otimes)
- Sicherheit begründet durch:
 - Zufälligkeit (unvorhersagbar!) der Schlüssel
 - Geheimhaltung der Schlüssel
 - Schlüssel nur *einmal* benutzen

One-Time Pad – Beispiel

Sicherheit?

Wahrscheinlichkeitstheorie

Perfekte Sicherheit

- Annahmen
- Beispiel
- Definition
- Beispielsysteme

Entropie

Gute Schlüssel

Literatur

Klartext	0	1	1	1	0	0	1	0
Schlüssel	1	1	1	0	1	0	1	0
Chiffretext	1	0	0	1	1	0	0	0
Schlüssel	1	1	1	0	1	0	1	0
Klartext	0	1	1	1	0	0	1	0

- Angriffsmöglichkeiten:
 - Ausspähen des Schlüssels bei nicht geheimen Schlüsselaustausch
 - Kein ausreichend zufälliger Schlüssel
 - Mehrfachverwendung des Schlüssels (Differenz der Chiffretexte = Differenz der Klartexte)
- Nachteile:
 - Schlüssellänge und -anzahl
 - Zufälligkeit der Schlüssel
 - Synchronisationsproblem bei verschollenen Nachrichten
 - Kollisionssproblem bei gleichzeitigen Nachrichten A↔B

Sicherheit?

Wahrscheinlichkeitstheorie

Perfekte Sicherheit

Entropie

- Definition
- Beispiel
- Eigenschaften

Gute Schlüssel

Literatur

Entropie

Sicherheit?
Wahrscheinlichkeitstheorie
Perfekte Sicherheit
Entropie
• Definition
• Beispiel
• Eigenschaften
Gute Schlüssel
Literatur

Definition

- Ursprung in der Thermodynamik, Bedeutung Unordnungsgrad $\hat{=}$ große Unordnung = hohe Entropie
- Informationstheorie: Ungewissheit über einen Versuchsausgang, (mittlerer) Informationsgehalt einer Nachricht

Definition: Sei \mathbf{X} eine diskrete Zufallsgröße, die die Werte einer endlichen Menge X annimmt. Dann ist die *Entropie* von \mathbf{X} definiert als die Größe

$$H(\mathbf{X}) = - \sum_{x \in X} \Pr[x] \log_2 \Pr[x]$$

Anmerkung 1: Da $\log_2 y$ undefiniert für $y = 0$, aber $\lim_{y \rightarrow \infty} y \log_2 y = 0$ kann $\Pr[x] = 0$ für einige x angenommen werden.

Anmerkung 2: Wenn $|X| = n$ und $\Pr[x] = \frac{1}{n}, \forall n \in X$, dann ist $H(\mathbf{X}) = \log_2 n$.

Sicherheit?

Wahrscheinlichkeitstheorie

Perfekte Sicherheit

Entropie

- Definition

- Beispiel

- Eigenschaften

Gute Schlüssel

Literatur

Beispiel

$$\mathcal{P} = \{a, b\} \text{ mit } \Pr[a] = \frac{1}{4}, \Pr[b] = \frac{3}{4}$$

$$\mathcal{K} = \{K_1, K_2, K_3\} \text{ mit } \Pr[K_1] = \frac{1}{2}, \Pr[K_2] = \Pr[K_3] = \frac{1}{4}$$

$$\mathcal{C} = \{1, 2, 3, 4\} \text{ mit } \Pr[1] = \frac{1}{8}, \Pr[2] = \frac{7}{16}, \Pr[3] = \frac{1}{4}, \Pr[4] = \frac{3}{16}$$

$$H(\mathbf{X}) = - \sum_{x \in X} \Pr[x] \log_2 \Pr[x]$$

$$H(\mathbf{P}) = - \left(\frac{1}{4} \log_2 \frac{1}{4} + \frac{3}{4} \log_2 \frac{3}{4} \right)$$

$$H(\mathbf{P}) \approx 0,81$$

$$H(\mathbf{K}) = 1,5$$

$$H(\mathbf{C}) \approx 1,85$$

Sicherheit?
Wahrscheinlichkeitstheorie
Perfekte Sicherheit
Entropie
• Definition
• Beispiel
• Eigenschaften
Gute Schlüssel
Literatur

Entropieeigenschaften I

Satz: Sei \mathbf{X} eine Zufallsgröße mit einer Wahrscheinlichkeitsverteilung, die die Werte p_1, \dots, p_n ($p_i > 0, 1 \leq i \leq n$) annimmt. Dann gilt $H(\mathbf{X}) \leq \log_2 n$ mit Gleichheit gdw. $p_i = \frac{1}{n}, 1 \leq i \leq n$.

Folgerung: Die *maximale Entropie* $H(\mathbf{X})$ beträgt $\log_2 n$.

Satz: $H(\mathbf{X}, \mathbf{Y}) \leq H(\mathbf{X}) + H(\mathbf{Y})$, mit Gleichheit gdw. \mathbf{X} und \mathbf{Y} unabhängige Zufallsgrößen sind.

Definition (a): Seien \mathbf{X} und \mathbf{Y} zwei Zufallsgrößen. Dann erhält man für jeden Wert y aus \mathbf{Y} eine (bedingte) Wahrscheinlichkeitsverteilung auf X . Die zugehörige Zufallsgröße wird mit $(\mathbf{X}|y)$ bezeichnet. Offensichtlich gilt

$$H(\mathbf{X}|y) = - \sum_x \Pr[x|y] \log_2 \Pr[x|y]$$

Entropieeigenschaften II

Definition (b): Die *bedingte Entropie* $H(\mathbf{X}|\mathbf{Y})$ ist das gewichtete Mittel (bezüglich der Wahrscheinlichkeiten der $\Pr[y]$) der Entropien $(\mathbf{X}|y)$ über allen möglichen Werten von y . Sie wird wie folgt berechnet

$$H(\mathbf{X}|\mathbf{Y}) = - \sum_y \sum_x \Pr[y] \Pr[x|y] \log_2 \Pr[x|y]$$

Satz: $H(\mathbf{X}, \mathbf{Y}) = H(\mathbf{Y}) + H(\mathbf{X}|\mathbf{Y})$

Folgerung: $H(\mathbf{X}|\mathbf{Y}) \leq H(\mathbf{X})$ mit Gleichheit gdw. \mathbf{X} und \mathbf{Y} unabhängig.

[Sicherheit?](#)

[Wahrscheinlichkeitstheorie](#)

[Perfekte Sicherheit](#)

[Entropie](#)

[Gute Schlüssel](#)

- Schlüsselmehrdeutigkeit
- Schlüsselkandidaten
- Spracheigenschaften
- Eliminierung falscher Schlüssel
- Produktkryptosysteme

[Literatur](#)

Gute Schlüssel

Sicherheit?
Wahrscheinlichkeitstheorie
Perfekte Sicherheit
Entropie
Gute Schlüssel
● Schlüsselmehrdeutigkeit
● Schlüsselkandidaten
● Spracheigenschaften
● Eliminierung falscher Schlüssel
● Produktkryptosysteme
Literatur

Schlüsselmehrdeutigkeit

Es existiert ein fundamentaler Zusammenhang zwischen den Entropien der einzelnen Komponenten eines Kryptosystems. Die bedingte Entropie $H(\mathbf{K}|\mathbf{C})$ heißt **Schlüsselmehrdeutigkeit** (key equivocation) und ist ein Maß dafür, wieviel Information über den Schlüssel durch den Chiffertext offengelegt wird. Es gilt hierbei folgender

Satz: Sei $(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$ ein Kryptosystem. Dann gilt

$$H(\mathbf{K}|\mathbf{C}) = H(\mathbf{K}) + H(\mathbf{P}) - H(\mathbf{C})$$

Am Beispiel:

$$H(\mathbf{K}) = 1,5 \quad , \quad H(\mathbf{P}) \approx 0,81 \quad , \quad H(\mathbf{C}) \approx 1,85$$

$$H(\mathbf{K}|\mathbf{C}) = 1,5 + 0,81 - 1,85 = 0,46$$

Sicherheit?
Wahrscheinlichkeitstheorie
Perfekte Sicherheit
Entropie
Gute Schlüssel
● Schlüsselmehrdeutigkeit
● Schlüsselkandidaten
● Spracheigenschaften
● Eliminierung falscher Schlüssel
● Produktkryptosysteme
Literatur

Schlüsselkandidaten

- Annahmen: Eve
 - hört Chiffertext ab
 - weiß, dass Klartext eine „natürliche“ Sprache
 - hat Wissen um Verschlüsselungsmethode
 - hat unbegrenzte Rechenressourcen
- Eve kann einige Schlüssel verwerfen (Klartext ist unbrauchbar)
- Verbleibende „mögliche“ Schlüssel unterteilt in
 - Korrekter Schlüssel
 - Falsche Schlüssel

Beispiel:

- Sprache Englisch, Chiffertext *WNAJW*, Methode Verschiebungschiffre
- nur zwei „sinnvolle“ Klartexte möglich: *RIVER* und *ARENA*
 - mögliche Schlüssel *F* (5) und *W* (22)

Untersuchung von Spracheigenschaften

Sicherheit?

Wahrscheinlichkeitstheorie

Perfekte Sicherheit

Entropie

Gute Schlüssel

- Schlüsselmehrdeutigkeit

- Schlüsselkandidaten

- Spracheigenschaften

- Eliminierung falscher
Schlüssel

- Produktkryptosysteme

Literatur

Ziel: Anzahl falscher Schlüssel eingrenzen

- Entropie (pro Buchstabe) einer natürlichen Sprache (H_L) misst die durchschnittliche Information pro Buchstabe in einem „sinnvollen“ natürlichsprachigem Text
- n -Gram: Wort der Länge n über einem Alphabet, \mathbf{P}^n Zufallsgröße mit Wahrscheinlichkeitsverteilung aller n -Gramme eines Klartextes

Definition: Sei L eine natürliche Sprache. Die *Entropie* von L ist definiert als die Größe

$$H_L = \lim_{n \rightarrow \infty} \frac{H(\mathbf{P}^n)}{n}$$

und die *Redundanz* von L ist definiert durch

$$R_L = 1 - \frac{H_L}{\log_2 |\mathcal{P}|}$$

Beispiel

- L ist englische Sprache
- Durch Untersuchungen: $1,0 \leq H_L \leq 1,5$ also rund 1,25
- Redundanz:

$$R_L = 1 - \frac{1,25}{\log_2 26} \approx 0,734$$

→ ca. 75% der englischen Sprache redundant

Sicherheit?

Wahrscheinlichkeitstheorie

Perfekte Sicherheit

Entropie

Gute Schlüssel

- Schlüsselmehrdeutigkeit
- Schlüsselkandidaten
- Spracheigenschaften
- Eliminierung falscher Schlüssel
- Produktkryptosysteme

Literatur

Eliminierung falscher Schlüssel

- Sicherheit?
- Wahrscheinlichkeitstheorie
- Perfekte Sicherheit
- Entropie
- Gute Schlüssel
 - Schlüsselmehrdeutigkeit
 - Schlüsselkandidaten
 - Spracheigenschaften
 - Eliminierung falscher Schlüssel
 - Produktkryptosysteme
- Literatur

Redundanz

- gibt Aufschluss über effektive Codierungsmöglichkeit
- erlaubt Anzahl falscher Schlüsse zu minimieren

Satz: Sei $(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$ ein Kryptosystem mit $|\mathcal{C}| = |\mathcal{P}|$ und gleichwahrscheinlicher Schlüsselverteilung. R_L sei die Redundanz der zu Grunde liegenden Sprache. Mit gegebenen Chiffretext der Länge n , mit n hinreichend groß, erfüllt die erwartete Anzahl falscher Schlüssel \bar{s}_n die Formel

$$\bar{s}_n \geq \frac{|\mathcal{K}|}{|\mathcal{P}|^{nR_L}} - 1$$

Definition: Die *Eindeutigkeitsdistanz* eines Kryptosystems ist definiert durch den Wert n , bezeichnet als n_0 , bei dem die Anzahl erwarteter falscher Schlüssel Null wird. D.h. die durchschnittliche Menge an Chiffretext, die ein Angreifer benötigt, um den Schlüssel eindeutig zu bestimmen.

Eindeutigkeitsdistanz – Beispiel

Sicherheit?

Wahrscheinlichkeitstheorie

Perfekte Sicherheit

Entropie

Gute Schlüssel

- Schlüsselmehrdeutigkeit

- Schlüsselkandidaten

- Spracheigenschaften

- Eliminierung falscher
Schlüssel

- Produktkryptosysteme

Literatur

- $\bar{s}_n = 0$ in Gleichung (letzter Satz) setzen und nach n umformen ergibt

$$n_0 \approx \frac{\log_2 |\mathcal{K}|}{R_L \log_2 |\mathcal{P}|}$$

- Kryptosystem *Substitutions-Chiffre*: $|\mathcal{P}| = 26$ und $|\mathcal{K}| = 26!$, $R_L = 0,75$

$$n_0 \approx \frac{88,4}{0,75 \cdot 4,7} \approx 25$$

→ Ein Chiffrentext der Länge 25 ermöglicht (normalerweise) eine eindeutige Entschlüsselung.

Produktkryptosysteme

Sicherheit?

Wahrscheinlichkeitstheorie

Perfekte Sicherheit

Entropie

Gute Schlüssel

- Schlüsselmehrdeutigkeit
- Schlüsselkandidaten
- Spracheigenschaften
- Eliminierung falscher Schlüssel

● **Produktkryptosysteme**

Literatur

- Idee: Verknüpfen zweier Kryptosysteme zur Erhöhung der Sicherheit
- *endomorphe* Kryptosysteme notwendig ($\mathcal{P} = \mathcal{C}$)

$$S_1 = (\mathcal{P}, \mathcal{P}, \mathcal{K}_1, \mathcal{E}_1, \mathcal{D}_1)$$

$$S_2 = (\mathcal{P}, \mathcal{P}, \mathcal{K}_2, \mathcal{E}_2, \mathcal{D}_2)$$

→ Produkt: $S_1 \times S_2 = (\mathcal{P}, \mathcal{P}, \mathcal{K}_1 \times \mathcal{K}_2, \mathcal{E}, \mathcal{D})$

- Schlüssel K hat die Form (K_1, K_2) mit $K_1 \in \mathcal{K}_1, K_2 \in \mathcal{K}_2$
- Verschlüsselungsfunktion: $d_{(K_1, K_2)}(y) = d_{K_1}(d_{K_2}(y))$
- Entschlüsselungsfunktion: $e_{(K_1, K_2)}(x) = e_{K_2}(e_{K_1}(x))$
- Beachte umgekehrte Schlüsselfolge:

$$\begin{aligned} d_{(K_1, K_2)}(e_{(K_1, K_2)}(x)) &= d_{(K_1, K_2)}(e_{K_2}(e_{K_1}(x))) \\ &= d_{K_1}(d_{K_2}(e_{K_2}(e_{K_1}(x)))) \\ &= d_{K_1}(e_{K_1}(x)) \\ &= x \end{aligned}$$

Eigenschaften von Produktkryptosystemen

Sicherheit?

Wahrscheinlichkeitstheorie

Perfekte Sicherheit

Entropie

Gute Schlüssel

- Schlüsselmehrdeutigkeit
- Schlüsselkandidaten
- Spracheigenschaften
- Eliminierung falscher Schlüssel

● **Produktkryptosysteme**

Literatur

- Assoziativität: $S_1 \times (S_2 \times S_3) = (S_1 \times S_2) \times S_3$ gilt für alle Kryptosysteme
- Kommutierende Kryptosysteme: $S_1 \times S_2 = S_2 \times S_1$ gilt nicht für alle Kryptosysteme
- Idempotenz: $S \times S = S^2 = S$
↪ falls nicht idempotent Chance für höhere Sicherheit durch multiple Iterationen ($\text{DES} = S^{16}$)
- Beachte: S_1, S_2 idempotent und kommutierend $\Rightarrow S_1 \times S_2$ ebenso

$$\begin{aligned}(S_1 \times S_2) \times (S_1 \times S_2) &= S_1 \times (S_2 \times S_1) \times S_2 \\&= S_1 \times (S_1 \times S_2) \times S_2 \\&= (S_1 \times S_1) \times (S_2 \times S_2) \\&= S_1 \times S_2\end{aligned}$$

Literatur

- [1] BRACKMANN, Roland. *Shannons Theorie*.
http://www.cs.uni-potsdam.de/ti/lehre/05-Kryptographie/slides/shannons_theorie_brackmann.pdf
- [2] HOPPE, Tobias. *Das One-Time-Pad und Chiffriermaschinen*.
<http://www-ivs.cs.uni-magdeburg.de/bs/lehre/wise0102/progb/vortraege/choppe/choppe.html>
- [3] MENEZES, Alfred J. ; VAN OORSCHOT, Paul C. ; VANSTONE, Scott A.: *Handbook of Applied Cryptography*. CRC Press, Inc., 1996. – ISBN 0849385237
- [4] SHANNON, Claude E. *Communication Theory of Secrecy Systems*.
<http://www.cs.ucla.edu/~jkong/research/security/shannon1949.pdf>
- [5] STINSON, Douglas R.: *Cryptography: Theory and Practice*. Second. CRC Press, Inc./Chapman&Hall, 2002. – ISBN 1584882069
- [6] WIKIPEDIA. *Bayestheorem*. <http://de.wikipedia.org/wiki/Bayestheorem>

Vielen Dank für Ihre Aufmerksamkeit