Kryptographie
Seminar

Shannons Theorie

Roland Brackmann

HASSO - PLATTNER - INSTITUT
an der Universität Potsdam

Übersicht

1. Einführung
2. Sicherheit in Kryptosystemen
3. Entropie
4. Redundanz
5. Mögliche Schlüsselkandidaten
6. Produkte von Kryptosystemen

Claude E. Shannon

- Claude E. Shannon (1916 - 2001)
  - Amerikanischer Mathematiker
  - Doktor am MIT mit 24
  - Begründer der Informationstheorie
- Wichtigsten Publikationen
  - A Mathematical Theory of Communication (1948)
  - Communication Theory of Secrecy Systems (1949)
- Einheit: das Shannon (sh)
  - Informationsgehalt einer Nachricht

Definition eines Kryptosystems

- Ein Kryptosystem S besteht aus dem Quintupel (*P,C,K,E,D*), wobei:
  - *P* – Klartexte (plaintexts)
  - *C* – Geheimtexte (ciphertexts)
  - *K* – Schlüssel (keys)
  - *E* – Verschlüsselungsfunktionen (encryption functions)
  - *D* – Entschlüsselungsfunktionen (decryption functions)
- Beispiel:

$$P=\{a,b\} \quad C=\{1,2,3,4\} \quad K=\{k_1,k_2,k_3\}$$
$$E:\{a,b\}\rightarrow\{1,2,3,4\} \quad D:\{1,2,3,4\}\rightarrow\{a,b\}$$

K \ P	a	b
k_1	1	2
k_2	2	3
k_3	3	4

E(b)

Was können wir über ein Kryptosystem erfahren?

- Die Wkt. mit der ein Geheimtext c auftritt, wird bestimmt durch:

$$P(c) = \sum_{p=d_k(c)} P(k) \cdot P(p)$$

- Wie hoch ist die Wkt., dass c = 2 als Geheimtext auftritt?

$$Wissen: \quad P(k_1) = \frac{1}{2} \quad P(k_2) = \frac{1}{4} \quad P(k_3) = \frac{1}{4} \qquad P(a) = \frac{1}{4} \quad P(b) = \frac{3}{4}$$

$$P_c(2) = P(k_1) \cdot P(b) + P(k_2) \cdot P(a)$$

$$P_c(2) = \frac{1}{2} \cdot \frac{3}{4} + \frac{1}{4} \cdot \frac{1}{4} = \frac{7}{16} = 43{,}75\%$$

K \ P	a	b
k_1	1	(2)
k_2	(2)	3
k_3	3	4

Satz von Bayes

- Satz von Bayes $$P(A \mid B) = \frac{P(B \mid A) \cdot P(A)}{P(B)}$$
  - Wahrscheinlichkeit des Eintretens eines Ereignisses A unter der Bedingung, dass ein Ereignis B bereits vorher eingetreten ist.
- Beispiel:
  - P(Düsseldorfer|Kölschtr.) = ?
  - P(Kölschtr.|Düsseldorfer) = 0,4
  - P(Düsseldorfer) = 0,2
  - P(Kölschtr.) = 0,8 * 0,9 + 0,2 * 0,4 = 0,8

	Kölner	Düsseldorfer
Anteil der rheinländischen Bevölkerung in %	80	20
davon Kölschtrinker in %	90	40

$$P(Düssel. \mid Kölschtr.) = \frac{P(Kölschtr. \mid Düssel.) \cdot P(Düssel.)}{P(Kölschtr.)} = \frac{0{,}4 \cdot 0{,}2}{0{,}8} = 10\%$$

  - Jemand trinkt Kölsch, zu 10 % ein Düsseldorfer!

Bedingte Wahrscheinlichkeiten

- P(c|p) ist die bedingte Wahrscheinlichkeit, dass der Geheimtext gleich c ist, unter der Voraussetzung, dass der Klartext gleich p ist:

$$P(c|p) = \sum_{p=d_k(c)} P(k) \qquad P(2\,|\,b) = P(k_1) = \frac{1}{2}$$

- P(p|c) ist die bedingte Wahrscheinlichkeit, dass der Klartext gleich p ist, unter der Voraussetzung, dass der Geheimtext gleich c ist (Satz von Bayes).

$$P(p|c) = \frac{P(p) \cdot P(c|p)}{P(c)}$$

- Bsp: Wie groß ist die Wkt., dass der Klartext b zu Geheimtext 2 verschlüsselt wurde?

$Suchen: \; P(b|2)$

$Kennen: P(2) = \frac{7}{16} \quad P(b) = \frac{3}{4}$

K \ P	a	b
k_1	1	2
k_2	2	3
k_3	3	4

$$P(b|2) = \frac{P(b) \cdot P(2|b)}{P(2)}$$

$$P(b|2) = \frac{\frac{3}{4} \cdot \frac{1}{2}}{\frac{7}{16}} = \frac{6}{7} = 85{,}7\ \%$$

Sicherheit von Kryptosystemen

- Berechenbare Sicherheit (computational security)
  - Der beste bekannte Algorithmus, um ein Kryptosystem zu knacken, muss mehr als X Schritte benötigen, wobei X groß.
  - Berechenbare Sicherheit ist eingeschränkt auf bestimmte Attacken.
- Beweisbare Sicherheit (provable security)
  - Reduzierung auf ein bekanntes Problem (z.B. NP-Vollständigkeit).
  - Beweis ist relativ zu bekanntem Problem, kein absoluter Beweis von Sicherheit.
- Unbedingte Sicherheit (unconditional security)
  - Ein Kryptosystem ist nicht zu lösen, selbst bei unbegrenzt verfügbarer Rechenleistung
  - Ein solches Kryptosystem wird als perfekt sicher bezeichnet.

Perfekte Sicherheit

- Ein Kryptosystem besitzt perfekte Sicherheit, wenn gilt:

  $P(p|c) = P(p) \quad \forall\, p \in P, c \in C$ nur bei Unabhängigkeit von p und c

- Perfekte Sicherheit bedeutet, dass durch Kenntnis des Geheimtexts keine Informationen über den Klartext bekannt werden.
- Ein System mit perfekter Sicherheit ist theoretisch unangreifbar.
- Besitzt unser Beispiel für den Geheimtext 2 und Klartext b perfekte Sicherheit?

$$P(b|2) = \frac{6}{7} \quad P(b) = \frac{3}{4}$$
$$P(b|2) \neq P(b) \quad \text{nein!}$$

Perfekte Sicherheit 2

- Seien für ein Kryptosystem (P,C,K,E,D) die Bedingungen

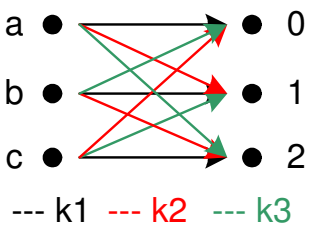
  $|K| = |C| = |P| \;:\; P(k_i) = \frac{1}{|K|}$ erfüllt,

  dann besitzt es perfekte Sicherheit, wenn für jedes $p \in P$ und $c \in C$ ein einzigartiger Schlüssel $d_K(c) = p$ existiert.

- Beispiel:

P / K	a	b	c
k_1	0	1	2
k_2	1	2	0
k_3	2	0	1

$$|K| = |k_1, k_2, k_3| = 3$$
$$|P| = |a,b,c| = 3$$
$$|C| = |0,1,2| = 3$$
$$P(k_i) = \frac{1}{3} : i = \{1,2,3\}$$



- Durch minimale Änderung verliert das System seine perfekte Sicherheit.

Kryptosystem mit perfekter Sicherheit

- One-Time Pad
  - Ein 1917 von Gilbert Vernam entwickelter Stromchiffre.
  - Galt als unangreifbar, jedoch fehlte der Beweis.
  - Konzept der perfekten Sicherheit von Shannon brachte den Beweis.

Klartexte	0	1	0	1	1	1	0
Schlüssel	1	0	1	1	1	0	1
Geheimtexte	1	1	1	0	0	1	1

$\oplus$	0	1
0	0	1
1	1	0

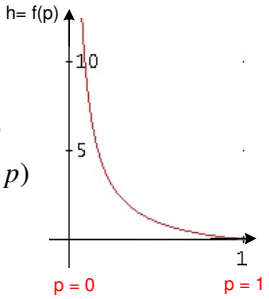
$$|P| = |K| = |C| = (Z_2)^n$$

- Bei perfekter Sicherheit ist |K| mindestens genau so groß wie |P|
  - Schlüsselverteilung ist das Hauptproblem!

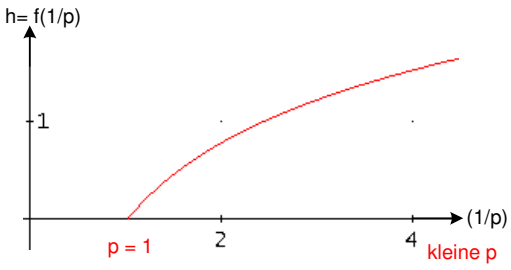
Herleitung des Informationsgehalts

- Wie kann man den Informationsgehalt einer Nachricht bestimmen?
  - Empfänger erwartet Nachricht → geringer Informationsgehalt
  - Empfänger erwartet Nachricht nicht → hoher Informationsgehalt

1. *Idee*:
$X - Achse = p$
$Y - Achse = h(p)$



2. *Idee*:
$X - Achse = \frac{1}{p}$
$Y - Achse = h(\frac{1}{p})$



- Additionssatz:

$$P(a) + P(b) = P(a \cap b) \quad a \text{ und } b \text{ sind unabhängig}$$

$$Würfel: \quad P(1) = \frac{1}{6} \quad P(6) = \frac{1}{6} \quad P(a \cup b) = \frac{1}{3}$$

Herleitung des Informationsgehalts 2

- Shannon benötigte eine Funktion für die der Additionssatz galt:
  - Für logarithmische Funktionen: log(x) + log(y) = log(x*y)
  - Wahl des logarithmus dualis aufgrund der Möglichkeit Daten binär darzustellen
- Informationsgehalt

$$h = \log_2\left(\frac{1}{p}\right) = \log_2(p^{-1})$$

$$Wissen: \quad \log_2(a^b) = b \cdot \log_2(a)$$

$$\mathbf{h = -\log_2(p) \quad [sh]}$$

- Beispiel:
  - Übertragung einer Dezimalziffer (bei Gleichverteilung p = 1/10)
  - Informationsgehalt: $-\log_2(0{,}1) = 3.32$ sh

Entropie

- Entropie ist der Mittelwert des Informationsgehaltes, der in einer Nachricht enthalten ist.

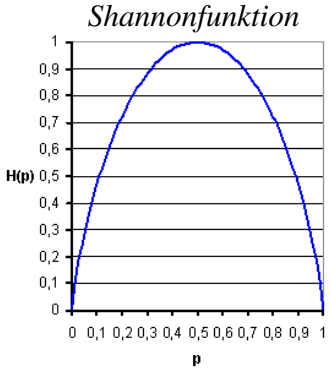
$$H(X) = -\sum_{i=1}^{n} P(X = x_i) \cdot \log_2 P(X = x_i) \quad [sh]$$

- Bsp: Ein Sender verschickt die Werte 0 und 1 mit gleichgroßer Wahrscheinlichkeit. Wie groß ist die Entropie?

$$H(X) = -\left(\frac{1}{2} \cdot \log_2\left(\frac{1}{2}\right)\right) - \left(\frac{1}{2} \cdot \log_2\left(\frac{1}{2}\right)\right) = -2 \cdot -\frac{1}{2} = 1 \ sh$$

- Shannonfunktion:

$$H(p) = -p \cdot \log_2 p - (1-p) \cdot \log_2(1-p) \quad sh$$



Entropie

- Eigenschaft der Entropie

$$H(X) \leq \log_2 n \quad \textit{mit Gleichheit bei } p_i = \frac{1}{n}$$

- Schlüsselbedeutung (key equivocation)

$$\textit{Für ein Kyptosystem } (P,C,K,E,D) \textit{ gilt}:$$
$$H(K|C) = H(K) + H(P) - H(C)$$

- Beispiel:

$$H(K) = -\frac{1}{2}\cdot\log_2\frac{1}{2} \quad -\frac{1}{4}\cdot\log_2\frac{1}{4} \quad -\frac{1}{4}\cdot\log_2\frac{1}{4} = 0{,}5 + 0{,}5 + 0{,}5 = 1{,}5\ sh$$

K \ P	a	b
k_1	1	2
k_2	2	3
k_3	3	4

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

Bedingte Entropie

- Bedingte Entropie misst den durchschnittlichen Informationsgehalt von X, bei Eintreten von Y.

$$H(X \mid Y) = -\sum_{y \in Y}\sum_{x \in X} P(y)\cdot P(x \mid y)\cdot \log_2 P(x \mid y) \quad [sh]$$

- Schlüsselbedeutung (aufwendig)

$$H(K \mid C) = -\sum_{c \in C}\sum_{k \in K} P(c)\cdot P(k \mid c)\cdot \log_2 P(k \mid c) \quad [sh]$$

$$H(K \mid C) = -\sum_{c \in C} \underbrace{P(1)\cdot P(k_1 \mid 1)\cdot \log_2 P(k_2 \mid 1)}_{k=k_1} + \underbrace{P(1)\cdot P(k_2 \mid 1)\cdot \log_2 P(k_2 \mid 1)}_{k=k_2} + \underbrace{P(1)\cdot P(k_3 \mid 1)\cdot \log_2 P(k_3 \mid 1)}_{k=k_3}$$

$$H(K \mid C) = 0{,}46\ sh$$

Sprache und ihre Entropie

- Mit H_L wird die Entropie einer Sprache beschrieben, d.h. H_L ist der durchschnittliche Informationsgehalt pro Buchstabe bzgl. aller Wörter
- Häufigkeiten
  - Buchstaben (e = 12,7 %, q = 0,1 %) $H_{L-letter} = H(P) \approx 4{,}19\ sh$
  - Digramme (th = 3.21 %, he = 3.05 %) $H_{L-digram} = \frac{H(P^2)}{2} \approx 3{,}9\ sh$
  - N-gramme (alle englischen Wörter) $H_L = \lim_{n\to\infty} \frac{H(P^n)}{n} = 1{,}0 \text{ bis } 1{,}5\ sh$

- Wie viele Bit werden zur Codierung des Alphabets benötigt?
  - $\log_2(26) \sim 4{,}7$ bit

Redundanz

- Redundanz ist der Informationsgehalt einer Nachricht, der überflüssig ist, da er explizit oder implizit schon in der Nachricht vorhanden ist.
- Redundanz der Sprache L:

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

- Beispiel:
  - Wissen, dass für die englische Sprache gilt:
    H_L = 1,0 bis 1,5 ~ 1,25 sh und Codierungsmenge = 4,7 bit

$$R_{engl} = 1 - \frac{1{,}25}{4{,}7} \approx 73{,}4\%$$

  - **Ca. 75% der engl. Sprache sind redundant**, d.h. man könnte ein Buch mit der richtigen Codierung auf ein Viertel seiner Größe schrumpfen.

Mögliche Schlüsselkandidaten (spurious keys)

- Es können bestimmte Schlüssel aussortiert werden, die verbleibenden Schlüssel nennt man *mögliche Schlüsselkandidaten*.
- Der richtige Schlüssel gehört nicht zu den *möglichen Schlüsselkandidaten.*
- Beispiel:
  - Geheimtext *WNAJW* wird abgefangen.
  - Wissen, dass Klartext in Englisch geschrieben wurde und ein Verschiebungschiffre zur Verschlüsselung benutzt wurde.
  - Nach ausrechnen aller Möglichkeiten, ergeben sich zwei sinnvolle Klartexte: *Arena* und *River*.
  - Somit zwei Schlüssel möglich: F und W.
  - Einer der beiden ist der richtige Schlüssel und einer der **mögliche Schlüsselkandidat**.

Abschätzung der möglichen Schlüsselkandidaten

- Sei S ein Kryptosystem (*P,C,K,E,D*)
  - mit $|C|=|P|$,
  - Gleichverteilung der Schlüssel *K,*
  - und einem Geheimtext der Länge n.
- Anzahl der möglichen Schlüsselkandidaten s_n:

$$s_n \geq \frac{|K|}{|P|^{n \cdot R_L}} - 1$$

- Um eine gute Schätzung zu bekommen, muss n entsprechend groß sein.

Unicity distance

- Die unicity distance eines Kryptosystems S ist die Anzahl der benötigten Buchstaben, um ein Kryptosystem zu knacken.
- Die Formel läßt sich von s_n ableiten, indem man $s_n = 0$ setzt und für n umstellt:

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

- Beispiel für den Substitutionschiffre:
  - |P| = 26
  - $|K| = 26! \sim 2^{88,4}$
  - $R_{engl} = 0,75$

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

- Für den Substitutionschiffre gilt, dass eine eindeutige Entschlüsselung möglich ist, wenn der Geheimtext mehr als 25 Zeichen enthält.

Verknüpfen von Kryptosystemen

- Produkt zweier Kryptosysteme
  - Ziel ist die Erhöhung der Sicherheit.
  - Hat grundlegende Bedeutung in der heutigen Kryptographie, z.B. im AES-Verfahren.
- Voraussetzung
  - Kryptosysteme müssen endomorph sein, d.h. Geheimtexte = Klartexte.
  - $S_1 = (P,P,K_1,E_1,D_1)$ und $S_2 = (P,P,K_2,E_2,D_2)$.
- Eigenschaften
  - Kommutation: Zwei Kryptosysteme kommutieren, wenn $S_1 * S_2 = S_2 * S_1$.
  - Assoziativität: $(S_1 * S_2) * S_3 = S_1 * (S_2 * S_3)$.
  - Idempotent: Kryptosystem ist idempotent, wenn: $S^2 = S * S = S$.

Literaturhinweise

1. *Stinson, Douglas: Cryptography Theory and Practice, Kapitel 2*
http://www.cs.ucla.edu/~jkong/research/security/Stinson-chap2.pdf
2. *Singh, Simon: Codes – Die Kunst der Verschlüsselung, März 2004*
3. *Handbook of Cryptography: http://www.cacr.math.uwaterloo.ca/hac/*
4. *Shannon, Claude: Communication Theory of Secrecy Systems*
http://www.cs.ucla.edu/~jkong/research/security/shannon1949.pdf
5. *http://www.ifi.unizh.ch/ee/teaching/ws03_04/informatikI/Information&Programmierung.pdf*
6. *Wagstaff, Samuel S.*: Cryptanalysis of number theoretic ciphers, 2003
7. *Beutelsbacher, Albrecht*: Kryptologie, Juli 2002

HASSO - PLATTNER - INSTITUT
an der Universität Potsdam

Vielen Dank für die Aufmerksamkeit!

Fragen …

roland.brackmann@hpi.uni-potsdam.de
www.hpi.uni-potsdam.de