Aktueller Überblick

§0 Einführende Worte (✓)

§1 Geschichtlicher Überblick (✓)

§2 Zufall (✓)

§3 Perfekte Sicherheit und ihre Grenzen

§4 Angriffsszenarien

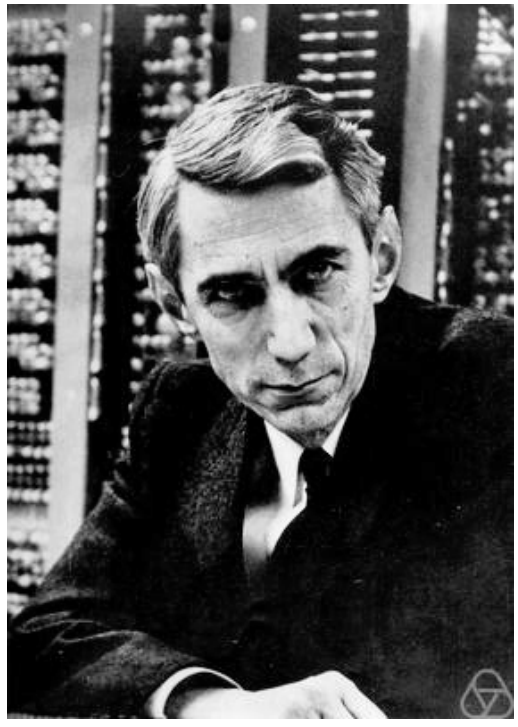
§5 Der komplexitätstheoretische Ansatz

§6 Pseudozufallsgeneratoren und Stromchiffren

§7 Pseudozufallsfunktionen und Blockchiffren

§3 Perfekte Sicherheit und ihre Grenzen

Claude Shannon ($*$ 1916, † 2001)



Quelle. Konrad Jacobs, Copyright: MFO

A Mathematical Theory of Communication, 1948

Communication Theory of Secrecy Systems, 1949

Shannon ist der Begründer der Informationstheorie.

(Behandeln wir hier nicht.)

Modell eines Chiffriersystems

Wir modellieren ein Chiffriersystem. Wir postulieren:

- Eine endliche Menge von (potentiellen) Nachrichten oder Klartexten / den Nachrichtenraum $\mathcal{M}$. Elemente / Nachrichten (=messages): $m^{(0)}, \ldots$
- Eine endliche Menge von (potentiellen) Chiffriertexten / den Chiffriertextraum $\mathcal{C}$. Elemente / Chiffriertexte: $c^{(0)}, \ldots$.
- Eine endliche Menge von (potentiellen) Schlüsseln / den Schlüsselraum $\mathcal{K}$. Elemente / Schlüssel: $k^{(0)}, \ldots$.

Modell eines Chiffriersystems

- Ein (möglicherweise) randomisiertes Verschlüsselungsverfahren / ein Verschlüsselungsalgorithmus $\mathcal{E}nc$ mit:

  Eingabe. $(k^{(0)}, m^{(0)}) \in \mathcal{K} \times \mathcal{M}$

  Ausgabe. Ein zufälliger Chiffriertext $\mathcal{E}nc_{k^{(0)}}(m^{(0)}) =$ eine Zufallsvariable mit Werten in $\mathcal{C}$
- Ein bezüglich Ein- und Ausgabe deterministisches Entschlüsselungsverfahren $\mathcal{D}ec$

  Eingabe. $(k^{(0)}, c^{(0)}) \in \mathcal{K} \times \mathcal{C}$

  Ausgabe. $\mathcal{D}ec_{k^{(0)}}(c^{(0)}) \in \mathcal{M}$
- mit: $\mathcal{D}ec_{k^{(0)}}(\mathcal{E}nc_{k^{(0)}}(m^{(0)})) = m^0$ mit Wahrscheinlichkeit 1 für alle $(k^{(0)}, m^{(0)}) \in \mathcal{K} \times \mathcal{M}$.

  (Hier wird für jedes Tupel $(k^{(0)}, m^{(0)})$ die Wahrscheinlichkeit bezüglich der Randomisierung in $\mathcal{E}nc$ betrahtet.)

Bemerkungen zu Algorithmen und Funktionen

Für einen Algorithmus $\mathcal{A}$ bezeichnen wir die Ausgabe unter einer Eingabe wie bei einer Funktion, z.B.:

- Eingabe. $x^{(0)}$
  Ausgabe. $\mathcal{A}(x^{(0)})$
  Allgemeiner Zusammenhang. $\mathcal{A}(x)$
- Eingabe. $(k^{(0)}, x^{(0)})$
  Ausgabe. $\mathcal{A}_{k^{(0)}}(x^{(0)})$
  Allgemeiner Zusammenhang. $\mathcal{A}_k(x)$

(Hier sind sowieso die "inneren Aspekte" irrelevant. Später werden auch Laufzeiten relevant und ansonsten sind wieder die "inneren Aspekte" irrelevant.)

Modell eines Chiffriersystems

Letztes Datum:

- Ein randomisierter Schlüsselerzeugungsalgorithmus $\mathcal{G}en$.
  Eingabe. nichts
  Ausgabe. ein zufälliger Schlüssel k (eine Zufallsvariable mit Werten in $\mathcal{K}$

Modell eines Chiffriersystems

Wir fixieren eine Nachricht $m^{(0)}$.

Wir haben

- die Randomisierung im Schlüsselerzeugungsalgorithmus / den zufälligen Schlüssel $k = \mathcal{G}en()$.
- die Randomisierung im Verschlüsselungsalgorithmus

Wir kombinieren dies (unabhängig) und erhalten eine Zufallsvariable $\mathcal{E}nc_k(m^{(0)})$.

Diese erfüllt:

$$\mathbf{P}[\mathcal{E}nc_k(m^{(0)}) = c^{(0)} \mid k = k^{(0)}]$$

$$= \mathbf{P}[\mathcal{E}nc_{k^{(0)}}(m^{(0)}) = c^{(0)}]$$

Also:

$$\mathbf{P}[\mathcal{E}nc_k(m^{(0)}) = c^{(0)}] = \sum_{k^{(0)} \in \mathcal{K}} \mathbf{P}[k = k^{(0)}] \cdot \mathbf{P}[\mathcal{E}nc_{k^{(0)}}(m^{(0)}) = c^{(0)}]$$

Analyse des Systems

Wir betrachten nun eine zufällige Nachricht (=Klartext) (= eine Zufallsvariable mit Werten auf $\mathcal{M}$) / irgendeine Wahrscheinlichkeitsverteilung auf $\mathcal{M}$.

Idee. Der Angreifer hat eine Vermutung über die versandten Nachrichten.

Wir haben nun diese Randomisierungen:

- die Randomisierung im Schlüsselerzeugungsalgorithmus / den zufälligen Schlüssel
- die Randomisierung im Verschlüsselungsalgorithmus
- die zufällige Nachricht.

Wir kombinieren dies alles unabhängig.

Wir erhalten:

$$\mathbf{P}[\mathcal{E}nc_k(m) = c^{(0)} \mid m = m^{(0)}] = \mathbf{P}[\mathcal{E}nc_k(m^{(0)}) = c^{(0)}]$$

Analyse des Systems

$$\mathbf{P}[\mathcal{E}nc_k(m) = c^{(0)} \mid m = m^{(0)}] = \mathbf{P}[\mathcal{E}nc_k(m^{(0)}) = c^{(0)}]$$

Es sei $c := \mathcal{E}nc_k(m)$. Dann:

$$\mathbf{P}[c = c^{(0)} \mid m = m^{(0)}] = \mathbf{P}[\mathcal{E}nc_k(m^{(0)}) = c^{(0)}]$$

Es sind äquivalent:

i) m und c sind unabhängig.

ii) Für alle Nachrichten $m^{(0)}$ und alle Chiffriertexte $c^{(0)}$ mit $\mathbf{P}[c = c^{(0)}] > 0$ ist

$$\mathbf{P}[m = m^{(0)} \mid c = c^{(0)}] = \mathbf{P}[m = m^{(0)}]$$

iii) Für alle Nachrichten $m^{(1)}, m^{(2)}$ mit $\mathbf{P}[m = m^{(1)}] > 0, \mathbf{P}[m = m^{(2)}] > 0$ und alle Chiffriertexte $c^{(0)}$ ist

$$\mathbf{P}[\mathcal{E}nc_k(m^{(1)}) = c^{(0)}] = \mathbf{P}[\mathcal{E}nc_k(m^{(2)}) = c^{(0)}] \,.$$

Analyse des Systems

Es sei $c := \mathcal{E}nc_k(m)$. Dann:

$$\mathbf{P}[c = c^{(0)} \mid m = m^{(0)}] = \mathbf{P}[\mathcal{E}nc_k(m^{(0)}) = c^{(0)}]$$

Es sind äquivalent:

i) m und c sind unabhängig.

ii) Für alle Nachrichten $m^{(0)}$ und alle Chiffriertexte $c^{(0)}$ mit $\mathbf{P}[c = c^{(0)}] > 0$ ist

$$\mathbf{P}[m = m^{(0)} \mid c = c^{(0)}] = \mathbf{P}[m = m^{(0)}]$$

iii) Für alle Nachrichten $m^{(1)}, m^{(2)}$ mit $\mathbf{P}[m = m^{(1)}] > 0, \mathbf{P}[m = m^{(2)}] > 0$ und alle Chiffriertexte $c^{(0)}$ ist

$$\mathbf{P}[\mathcal{E}nc_k(m^{(1)}) = c^{(0)}] = \mathbf{P}[\mathcal{E}nc_k(m^{(2)}) = c^{(0)}] \,.$$

Definition. Wenn diese Bedingungen für alle Verteilungen auf $\mathcal{M}$ (man kann sagen: für alle zufälligen Nachrichten) gelten, heißt das System perfekt sicher oder perfekt geheim.

Perfekte Sicherheit

Es gelte dies. D.h. für alle zufälligen Nachrichten / für alle Verteilungen auf $\mathcal{M}$ gelte:

iii) Für alle Nachrichten $m^{(1)}, m^{(2)}$ mit $\mathbf{P}[m = m^{(1)}] > 0, \mathbf{P}[m = m^{(2)}] > 0$ und alle Chiffriertexte $c^{(0)}$ ist

$$\mathbf{P}[\mathcal{E}nc_k(m^{(1)}) = c^{(0)}] = \mathbf{P}[\mathcal{E}nc_k(m^{(2)}) = c^{(0)}] \,.$$

Es seien $m^{(1)}, m^{(2)}$ Nachrichten.

Dann kann man die Verteilung / die zufällige Nachricht (Zufallsvariable) m auch so wählen, dass $\mathbf{P}[m = m^{(1)}] > 0$, $\mathbf{P}[m = m^{(2)}] > 0$.

Damit gilt:

vi) Für alle Nachrichten $m^{(1)}, m^{(2)}$ und alle Chiffriertexte $c^{(0)}$ ist

$$\mathbf{P}[\mathcal{E}nc_k(m^{(1)}) = c^{(0)}] = \mathbf{P}[\mathcal{E}nc_k(m^{(2)}) = c^{(0)}] \,.$$

Hier kommt gar keine Verteilung auf $\mathcal{M}$ vor!

Perfekte Sicherheit

Es gelte dies. D.h. für alle zufälligen Nachrichten / für alle Verteilungen auf $\mathcal{M}$ gelte:

iii) Für alle Nachrichten $m^{(1)}, m^{(2)}$ mit $\mathbf{P}[m = m^{(1)}] > 0, \mathbf{P}[m = m^{(2)}] > 0$ und alle Chiffriertexte $c^{(0)}$ ist

$$\mathbf{P}[\mathcal{E}nc_k(m^{(1)}) = c^{(0)}] = \mathbf{P}[\mathcal{E}nc_k(m^{(2)}) = c^{(0)}] \,.$$

Es seien $m^{(1)}, m^{(2)}$ Nachrichten.

Damit gilt:

vi) Für alle Nachrichten $m^{(1)}, m^{(2)}$ und alle Chiffriertexte $c^{(0)}$ ist

$$\mathbf{P}[\mathcal{E}nc_k(m^{(1)}) = c^{(0)}] = \mathbf{P}[\mathcal{E}nc_k(m^{(2)}) = c^{(0)}] \,.$$

Hier kommt gar keine Verteilung auf $\mathcal{M}$ vor!

Umgekehrt: Wenn dies gilt, dann gilt auch iii) mit belieber Verteilung auf $\mathcal{M}$.

Perfekte Sicherheit

Satz und Definition. Es sind äquivalent:

i) Es sei m eine zufällige Nachricht und $c := \mathcal{E}nc_k(m)$. Dann sind m und c unabhängig.

ii) Es sei m eine zufällige Nachricht und $c := \mathcal{E}nc_k(m)$. Dann gilt für alle Nachrichten $m^{(0)}$ und alle Chiffriertexte $c^{(0)}$ mit $\mathbf{P}[c = c^{(0)}] > 0$

$$\mathbf{P}[m = m^{(0)} \mid c = c^{(0)}] = \mathbf{P}[m = m^{(0)}] \,.$$

iv) Für alle Nachrichten $m^{(1)}, m^{(2)}$ und alle Chiffriertexte $c^{(0)}$ ist

$$\mathbf{P}[\mathcal{E}nc_k(m^{(1)}) = c^{(0)}] = \mathbf{P}[\mathcal{E}nc_k(m^{(2)}) = c^{(0)}] \,.$$

Wenn dies der Fall ist, heißt das Verfahren perfekt sicher oder perfekt geheim.

Perfekte Sicherheit

Satz und Definition. Es sind äquivalent:

i) Für alle zufälligen Nachrichten m gilt mit $c := \mathcal{E}nc_k(m)$: m und c unabhängig.

ii) Für alle zufälligen Nachrichten m gilt mit $c := \mathcal{E}nc_k(m)$: Für alle Nachrichten $m^{(0)}$ und alle Chiffriertexte $c^{(0)}$ mit $\mathbf{P}[c = c^{(0)}] > 0$

$$\mathbf{P}[m = m^{(0)} \mid c = c^{(0)}] = \mathbf{P}[m = m^{(0)}] \,.$$

iv) Für alle Nachrichten $m^{(1)}, m^{(2)}$ und alle Chiffriertexte $c^{(0)}$ ist

$$\mathbf{P}[\mathcal{E}nc_k(m^{(1)}) = c^{(0)}] = \mathbf{P}[\mathcal{E}nc_k(m^{(2)}) = c^{(0)}] \,.$$

Wenn dies der Fall ist, heißt das Verfahren perfekt sicher oder perfekt geheim.

Ein perfekt sicheres Verfahren

Sei $\mathcal{M} = \mathcal{C} = \mathcal{K} = \mathbf{Z}/N\mathbf{Z}$.

$\mathcal{G}en$. Wähle $k \in \mathcal{K} = \mathbf{Z}/N\mathbf{Z}$ uniform zufällig.

$\mathcal{E}en$. Eingabe: $(k^{(0)}, m^{(0)})$. Ausgabe: $m^{(0)} + k^{(0)}$.

$\mathcal{D}ec$. Eingabe: $(k^{(0)}, c^{(0)})$. Ausgabe: $c^{(0)} - k^{(0)}$.

Für alle $(m^{(0)}, c^{(0)})$ ist

$$\mathbf{P}[\mathcal{E}nc_{k^{(0)}}(m^{(0)}) = c^{(0)}] = \frac{1}{N} .$$

Das one-time-pad

Sei $n > 0$, $\mathcal{M} = \mathcal{C} = \mathcal{K} = (\mathbf{Z}/2\mathbf{Z})^{\ell}$.

$\mathcal{G}en$. Wähle Bits $k_1, \ldots, k_n$ unabhängig uniform zufällig, erhalte $k = (k_1, \ldots, k_\ell)$.

$\mathcal{E}en$. Eingabe: $(k^{(0)}, m^{(0)})$. Ausgabe: $m^{(0)} \oplus k^{(0)}$.

$\mathcal{D}ec$. Eingabe: $(k^{(0)}, c^{(0)})$. Ausgabe: $c^{(0)} \oplus k^{(0)}$.

Das Verfahren ist involutorisch.

Für alle $(m^{(0)}, c^{(0)})$ ist

$$\mathbf{P}[\mathcal{E}nc_k(m^{(0)}) = c^{(0)}] = \frac{1}{2^n} .$$

Das Verfahren ist perfekt sicher.

Grenzen der perfekten Sicherheit

Satz (Shannon) Für ein perfekt sicheres Chiffrierverfahren mit Nachrichtenraum $\mathcal{M}$ und Schlüsselraum $\mathcal{K}$ gilt $\#\mathcal{K} \geq \#\mathcal{M}$.

Grenzen der perfekten Sicherheit

Beweis

Es sei ein Verfahren $(\mathcal{G}en, \mathcal{E}nc, \mathcal{D}ec)$ gegeben.

Es gelte $\#\mathcal{K} < \#\mathcal{M}$.

z.z.: Das Verfahren ist nicht perfekt sicher.

Fixiere irgendeine Nachricht $m^{(0)}$ und hierzu einen Chiffriertext $c^{(0)}$ mit

$$\mathbf{P}[\mathcal{E}nc_k(m^{(0)}) = c^{(0)}] > 0\,. \quad (k = \mathcal{G}en())$$

Nun ist $\mathcal{D}ec$ deterministisch und

$$\#\{\mathcal{D}ec_{k^{(0)}}(c^{(0)}) \mid k^{(0)} \in \mathcal{K}\} \leq \#\mathcal{K}\,.$$

Es gibt eine Nachricht $m^{(1)}$, die kein Ergebnis der Anwendung von $\mathcal{D}ec$ auf $c^{(0)}$ und irgendeinen Schlüssel ist.

Es gilt dann $\mathbf{P}[\mathcal{E}nc_k(m^{(1)}) = c^{(0)}] = 0$.

Das Verfahren ist nicht perfekt sicher.

Grenzen der perfekten Sicherheit

Satz (Shannon) Für ein perfekt sicheres Chiffrierverfahren mit Nachrichtenraum $\mathcal{M}$ und Schlüsselraum $\mathcal{K}$ gilt $\#\mathcal{K} \geq \#\mathcal{M}$.