Hausaufgabe

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

§4 Angriffsszenarien

Ein Spiel

Idee eines Spiels

Ein Angreifer sagt:

Ich kann das System durch Lauschen brechen.

Idee eines Spiels

Ein Herausforder antwortet:

Beweis es mir!

Wir machen ein Spiel.

Ich mach's Dir auf jeden Fall leicht:

Zu Beginn wähle ich einen Schlüssel.

Du schickst mir zwei Nachrichten Deiner Wahl.

Ich wähle eine aus, verschlüssele sie und schicke sie an Dich.

Du musst mir nur sagen, welche ich verschlüsselt habe.

Wenn Du mit Wahrscheinlichkeit $> \frac{1}{2}$ *gewinnst, glaub ich's Dir.*

Das Ununterscheidbarkeits-Spiel zum Lauscher-Angriff

Gegeben: $\mathcal{M}, \mathcal{C}, \mathcal{K}; \mathcal{G}en, \mathcal{E}nc, \mathcal{D}ec$.

1. Der Herausforderer erzeugt einen Schlüssel $k := \mathcal{G}en()$.
2. Der Angreifer wählt zwei verschiedene Nachrichten m_1, m_2.
   Er schickt diese an den Herausforderer.
3. Der Herausforderer wählt $i \in \{1, 2\}$ uniform (und unabhängig vom Bisherigen).
   Er berechnet $c := \mathcal{E}nc_k(m_i)$ und schickt c an den Angreifer.
4. Der Angreifer entscheidet sich für $j \in \{1, 2\}$.

Der Angreifer hat gewonnen, wenn $i = j$ ist.

Wir definieren den (signierten) Vorteil oder Erfolg des Angreifers als

$$2 \cdot (\mathbf{P}[\mathcal{A} \text{ gewinnt}] - \frac{1}{2}) \, .$$

Der Vorteil oder Erfolg

Wir definieren den (signierten) Vorteil oder Erfolg des Angreifers als

$$2 \cdot (\mathbf{P}[\mathcal{A} \text{ gewinnt}] - \frac{1}{2}) \, .$$

- Dieser Vorteil / Erfolg liegt zwischen -1 und 1 einschließlich.
- Der Faktor "2" wird oft weggelassen.
- Es wird in der Regel der Absolutbetrag als Vorteil / Erfolg definiert.
- Aber das ist nicht so wichtig ...

Vorteil / Erfolg

Es sei $\mathcal{A}$ ein Angreifer.

Betrachte nun den Angreifer $\mathcal{A}'$ mit vertauschter Ausgabe:

$\mathcal{A}'$:

Falls Ausgabe von $\mathcal{A}$ gleich 1: Ausgabe von $\mathcal{A}'$ gleich 2

Falls Ausgabe von $\mathcal{A}$ gleich 2: Ausgabe von $\mathcal{A}'$ gleich 1

Der Vorteil / Erfolg von $\mathcal{A}'$ ist:

$$2 \cdot (\mathbf{P}[\mathcal{A}' \text{ gewinnt}] - \tfrac{1}{2}) =$$

$$2 \cdot (\mathbf{P}[\mathcal{A} \text{ verliert}] - \tfrac{1}{2}) =$$

$$2 \cdot (1 - \mathbf{P}[\mathcal{A} \text{ gewinnt}] - \tfrac{1}{2}) =$$

$$2 \cdot (\tfrac{1}{2} - \mathbf{P}[\mathcal{A} \text{ gewinnt}]) =$$

$$= -\text{Vorteil / Erfolg von } \mathcal{A}'$$

Der Vorteil / Erfolg

Wir betrachten einen Angreifer $\mathcal{A}$, der c ignoriert.

Die Ausgabe j des Angreifers ist unabhängig von der Wahl i des Herausforders.

Der Erfolg ist 0:

$$\mathbf{P}[\mathcal{A} \text{ gewinnt} \mid j = 1] = \mathbf{P}[i = 1 \mid j = 1] = \mathbf{P}[i = 1] = \frac{1}{2}$$

$$\mathbf{P}[\mathcal{A} \text{ gewinnt} \mid j = 0] = \mathbf{P}[i = 1 \mid j = 0] = \mathbf{P}[i = 1] = \frac{1}{2}$$

Insgesamt:

$$\mathbf{P}[\mathcal{A} \text{ gewinnt}] = \frac{1}{2}$$

Spiele oder Tests ?

Alternative Formulierungen

"Spiel" ist nur eine Geschichte.

Übliche Alternative:

Das Angriff wird von einer Testumgebung durchgeführt.

Sowohl das Verfahren als auch $\mathcal{A}$ "kommen in die Testumgebung".

Auch möglich wäre: Test-Automat statt Testumgebung.

Aber "Automat" ist später schlecht, weil wir Algorithmen mit unendlich vielen Eingaben betrachten werden und "Automat" schon definiert ist.

Ununterscheidbarkeits-Test für Lauscher-Angriffe

Gegeben: $\mathcal{M}, \mathcal{C}, \mathcal{K}; \mathcal{G}en, \mathcal{E}nc, \mathcal{D}ec$.

1. Die Umgebung erzeugt einen Schlüssel $k := \mathcal{G}en()$.
2. Der Angreifer wählt zwei verschiedene Nachrichten m_1, m_2 gleicher Länge. Er schickt diese an die Umgebung.
3. Die Umgebung wählt $i \in \{1, 2\}$ uniform. Sie berechnet $c := \mathcal{E}nc_k(m_i)$ und schickt c an den Angreifer.
4. Der Angreifer entscheidet sich für $j \in \{1, 2\}$.
5. Die Umgebung gibt aus:
   1 (= "Der Angreifer hat gewonnen"), falls $i = j$
   0 (= "Der Angreifer hat verloren"), falls $i \neq j$

Ununterscheidbarkeits-Test für Lauscher-Angriffe

Oder “nur passiver Sprachgebrauch” für die Umgebung:

Ununterscheidbarkeits-Test für Lauscher-Angriffe

Gegeben: $\mathcal{M}, \mathcal{C}, \mathcal{K}; \mathcal{G}en, \mathcal{E}nc, \mathcal{D}ec$.

1. Es wird ein Schlüssel $k := \mathcal{G}en()$ erzeugt.
2. Der Angreifer wählt zwei verschiedene Nachrichten m_1, m_2 gleicher Länge.
3. Es werden $i \in \{1, 2\}$ uniform (und unabhängig vom Bisherigen) gewählt. Es wird $c := \mathcal{E}nc_k(m_i)$ berechnet und an den Angreifer gegeben.
4. Der Angreifer entscheidet sich für $j \in \{1, 2\}$.
5. Es wird ausgegeben:
   0, falls $i \neq j$
   1, falls $i = j$

Ununterscheidbarkeits-Test für Lauscher-Angriffe

Notation im Buch von Katz & Lindell:

$$\Pi = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$$

Ergebnis des Algorithmus:

$$\mathsf{PrivK}^{\mathsf{eav}}_{\mathcal{A},\Pi}$$

Damit der Erfolg des Angreifers $\mathcal{A}$:

$$2 \cdot (\mathbf{P}[\mathsf{PrivK}^{\mathsf{eav}}_{\mathcal{A},\Pi} = 1] - \frac{1}{2})$$

Perfekte Sicherheit und das Ununterscheidbarkeits-Spiel

Perfekte Sicherheit und das Spiel

Satz. Das Verfahren ist genau dann perfekt sicher, wenn im Ununterscheidbarkeitsspiel für Lauscher-Angriffe kein Angreifer einen Vorteil / Erfolg erzielen kann.

(D.h. der Vorteil / Erfolg ist stets 0.)

Perfekte Sicherheit und das Spiel

Vorbemerkung

Die Nachrichten m_1, m_2 können auch zufällig sein.

Die Entscheidung $i = 1/2$ des Herausforderers ist unabhängig von der Wahl von m_1, m_2.

"Perfekt sicher" $\longrightarrow$ "kein Angreifer mit Erfolg"

Das Verfahren sei perfekt sicher. Die Chiffriertexte $\mathcal{E}nc_k(m_i)$ sind identisch verteilt.

Der vom Herausforderer gesendete Text $c = \mathcal{E}nc_k(m_i)$ (mit Wahl von i) ist unabhängig von der Wahl von i.

Die Ausgabe des Angreifers ist unabhängig von der Wahl des Herausforderers.

Der Vorteil / Erfolg ist 0.

Perfekte Sicherheit und das Spiel

“Nicht perfekt sicher” $\longrightarrow$ “ein Angreifer mit Erfolg”

Das Verfahren sei nicht perfekt sicher.

Wir haben (feste) Nachrichten $m^{(1)}, m^{(2)}$ und einen Chiffriertext $c^{(0)}$ mit

$$\mathbf{P}[c = c^{(0)}] > 0 \,,$$

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

Definition von $\mathcal{A}$:

- Sende m_1 und m_2.

Nach Empfang von c:

- Wenn $c = c^{(0)}$: Wähle $j = 1$.
- Wenn $c \neq c^{(0)}$: Wähle $j \in \{1, 2\}$ uniform zufällig.

Perfekte Sicherheit und das Spiel

$$\mathbf{P}[\mathcal{A} \text{ gewinnt}] =$$

$$\mathbf{P}[\mathcal{A} \text{ gewinnt} \mid c = c^{(0)}] \cdot \mathbf{P}[c = c^{(0)}]$$
$$+ \mathbf{P}[\mathcal{A} \text{ gewinnt} \mid c \neq c^{(0)}] \cdot \mathbf{P}[c \neq c^{(0)}]$$

Zunächst:

$$\mathbf{P}[\mathcal{A} \text{ gewinnt} \mid c \neq c^{(0)}] = \frac{1}{2}$$

Nun:

$$\mathbf{P}[\mathcal{A} \text{ gewinnt} \mid c = c^{(0)}] \cdot \mathbf{P}[c = c^{(0)}] =$$

$$\mathbf{P}[i = 1 \mid c = c^{(0)}] \cdot \mathbf{P}[c = c^{(0)}] =$$

$$\mathbf{P}[i = 1 \, , c = c^{(0)}] =$$

$$\mathbf{P}[c = c^{(0)} \mid i = 1] \cdot \mathbf{P}[i = 1] =$$

$$\mathbf{P}[\mathcal{E}nc_k(m_1) = c^{(0)}] \cdot \tfrac{1}{2} >$$

Hausaufgabe

Aufgabe 1

Wir betrachten das Ununterscheidbarkeits-Spiel, das genau so beschrieben wird:

1. Der Herausforderer wählt $k \in \mathcal{K}$ "nach Vorschrift".
2. Der Angreifer wählt zwei verschiedene Nachrichten $m_1, m_2 \in \mathcal{M}$. (Das kann stochastisch sein.) Er schickt diese an den Herausforderer.
3. Der Herausforderer wählt $i \in \{1, 2\}$ gleichverteilt und schickt $c := \mathcal{E}nc_k(m_i)$ an den Angreifer.
4. Der Angreifer wählt $j \in \{1, 2\}$ und gibt dies bekannt.

Der Angreifer gewinnt, wenn $i = j$ ist.

Aufgabe 1

a) Kann man Schritte im Ablauf des Spiels vertauschen, ohne dass man "irgendwas Relevantes ändert"? Das heißt konkret: ohne, dass es Angreifer mit besserer oder schlechterer Gewinnwahrscheinlichkeit gibt. Wenn ja, dann welche Schritte?

b) Ist es relevant, dass der Angreifer m_1 und m_2 stochastisch wählen kann, oder könnte man auch "ohne relevante Änderung" verlangen, dass diese Wahl deterministisch zu erfolgen hat?

Aufgabe 1

c) Der Angreifer wähle $i \in \{1, 2\}$ nicht mehr gleichverteilt, sondern mit einer festen Wahrscheinlichkeit wie – sagen wir – $2/3$ zu $1/3$. Dann gibt es einen trivialen Angreifer mit Gewinnwahrscheinlichkeit $2/3$, stimmt's? Also sollten wir dann für den Erfolg eines Angreifers $\mathcal{A}$ definieren als $\mathbb{P}[\mathcal{A} \text{ gewinnt}] - \frac{2}{3}$.
Sagen wir, wir machen dies so. Können wir dann die Aussagen über perfekte Sicherheit etc. übertragen oder erhalten wir substantiell andere Aussagen?

Semantische Sicherheit

Semantische Sicherheit

Idee. Alles, was man aus einem Chiffriertext einer Nachricht und weiteren Daten über die Nachricht selbst erfahren kann, kann man auch ohne den Chiffriertext berechnen.

Was bedeutet "alles"?

Das könnte z.B. ein bestimmtes Bit sein.

Oder die Summe von zwei bestimmten Bits.

Oder (1. Bit + 2. Bit) $\cdot$ 5. Bit

$\vdots$

Also: Für irgendeine Funktion $f : \mathcal{M} \longrightarrow \{0,1\}^*$: $f(m)$

"Daten über die Nachricht" entsprechend:

Für irgendeine Funktion $h : \mathcal{M} \longrightarrow \{0,1\}^*$: $h(m)$.

Semantische Sicherheit

Es sei ein Chiffierverfahren mit $\mathcal{M}, \mathcal{C}, \mathcal{K}; \mathcal{G}en, \mathcal{E}nc, \mathcal{D}ec$ gegeben.

Definition. Das Verfahren ist perfekt semantisch sicher, wenn gilt:

Für alle Algorithmen $\mathcal{A}$ mit Eingabe $(c, \textbf{Zusatz}) \in \mathcal{C} \times \{0,1\}^*$ gibt es einen Algorithmus $\mathcal{A}'$ mit Eingabe $\textbf{Zusatz} \in \{0,1\}^*$ mit:

Für alle Funktionen $h : \mathcal{M} \longrightarrow \{0,1\}^*$ und $f : \mathcal{M} \longrightarrow \{0,1\}^*$ und alle zufälligen Nachrichten m:

$$\mathbf{P}[\mathcal{A}(\mathcal{E}nc_k(m), h(m)) = f(m)] = \mathbf{P}[\mathcal{A}'(h(m)) = f(m)]$$

Bemerkung. Diese genaue Definition ist von mir. Den Begriff "perfekt semantisch sicher" gibt es normalerweise nicht. Später mehr zu "semantisch sicher".

Semantische Sicherheit

Satz. Das Verfahren ist genau dann perfekt sicher, wenn es perfekt semantisch sicher ist.

Semantische Sicherheit

"**perfekt sicher**" $\longrightarrow$ "**perfekt semantisch sicher**"

Gegeben sei $\mathcal{A}$. Das Verfahren sei perfekt sicher.

Es sei m eine zufällige Nachricht.

Dann sind m und $c := \mathcal{E}nc_k(m)$ stochastisch unabhängig.

Idee. Der Algorithmus kann sich c auch selbst wählen.

Genauer. Für irgendeine feste Nachricht $m^{(0)}$ ist $\mathcal{E}nc_k(m^{(0)})$ genauso verteilt wie c und unabhängig von den anderen Wahlen.

Semantische Sicherheit

Definition von $\mathcal{A}'$

Verfahre genau wie $\mathcal{A}$ außer:

Wähle c selbst mit: $c := \mathcal{E}nc_k(m^{(0)})$ für eine feste Nachricht $m^{(0)}$.

Beachte: Die Verteilung von m wird nicht berücksichtigt.

Die Ausgaben der Algorithmen $\mathcal{A}$ und $\mathcal{A}'$ sind identisch verteilt.

Sematische Sicherheit

"**perfekt semantisch sicher**" $\longrightarrow$ "**perfekt sicher**"

Wir können für f, h Beliebiges wählen.

Wir wählen: $f(m) = m$, $h(m) =$ "nichts".

Wir haben:

Zu jeden Algorithmus $\mathcal{A}$ mit Eingabe $c \in \mathcal{C}$

gibt es einen Algorithmus $\mathcal{A}'$ ohne Eingabe mit

$$\mathbf{P}[\mathcal{A}(\mathcal{E}nc_k(m)) = m] = \mathbf{P}[\mathcal{A}'() = m]$$

für jede zufällige Nachricht m.

Semantische Sicherheit

Wir wählen zwei verschiedene Nachrichten $m^{(1)}$ und $m^{(2)}$, $i = \{1, 2\}$ unform, betrachten $m = m^{(i)}$.

Es ist

$$\mathbf{P}[\mathcal{A}(\mathcal{E}nc_k(m^{(i)})) = m^{(i)}] = \mathbf{P}[\mathcal{A}'() = m^{(i)}] \leq \frac{1}{2} .$$

Somit: Kein Spieler Unterscheidbarkeits-Spiel (mit deterministischer Wahl von zwei verschiedenen Nachrichten $m^{(1)}, m^{(2)}$) hat einen positiven Erfolg.

$\Longrightarrow$ (s.o.) Das Verfahren ist perfekt sicher.

Weitere Spiele

Das Spiel zum CPA

Gegeben: $\mathcal{M}, \mathcal{C}, \mathcal{K}; \mathcal{G}en, \mathcal{E}nc, \mathcal{D}ec$.

1. Der Herausforderer erzeugt einen Schlüssel $k := \mathcal{G}en()$.
2. Der Angreifer kann beliebige Nachrichten m mit dem Schlüssel k verschlüsseln lassen (d.h. $\mathcal{E}nc_k(m)$ berechnen lassen).
3. Der Angreifer wählt zwei verschiedene Nachrichten m_1, m_2. Er schickt diese an den Herausforderer.
4. Der Herausforderer wählt $i \in \{1, 2\}$ uniform. Er berechnet $c := \mathcal{E}nc_k(m_i)$ und schickt c an den Angreifer.
5. Der Angreifer kann beliebige (!) Nachrichten mit dem Schlüssel k verschlüsseln lassen.
6. Der Angreifer entscheidet sich für $j \in \{1, 2\}$.

Der Angreifer hat gewonnen, wenn $i = j$ ist.

Das Spiel zum nicht-adaptiven CCA

Gegeben: $\mathcal{M}, \mathcal{C}, \mathcal{K}; \mathcal{G}en, \mathcal{E}nc, \mathcal{D}ec$.

1. Der Herausforderer erzeugt einen Schlüssel $k := \mathcal{G}en()$.
2. Der Angreifer kann beliebige Texte ver- und entschlüsseln lassen.
3. Der Angreifer wählt zwei verschiedene Nachrichten m_1, m_2. Er schickt diese an den Herausforderer.
4. Der Herausforderer wählt $i \in \{1, 2\}$ uniform. Er berechnet $c := \mathcal{E}nc_k(m_i)$ und schickt c an den Angreifer.
5. Der Angreifer kann beliebige Nachrichten verschlüsseln lassen.
6. Der Angreifer entscheidet sich für $j \in \{1, 2\}$.

Der Angreifer hat gewonnen, wenn $i = j$ ist.

Das Spiel zum adaptiven CCA (CCA2)

Gegeben: $\mathcal{M}, \mathcal{C}, \mathcal{K}; \mathcal{G}en, \mathcal{E}nc, \mathcal{D}ec$.

1. Der Angreifer kann beliebige Texte ver- und entschlüsseln lassen.
2. Der Angreifer wählt zwei verschiedene Nachrichten m_1, m_2. Er schickt diese an den Herausforderer.
3. Der Herausforderer wählt $i \in \{1, 2\}$ uniform. Er berechnet $c := \mathcal{E}nc_k(m_i)$ und schickt c an den Angreifer.
4. Der Angreifer kann beliebige Nachrichten verschlüsseln lassen und Chiffriertexte verschieden von c entschlüsseln lassen.
5. Der Angreifer entscheidet sich für $j \in \{1, 2\}$.

Der Angreifer hat gewonnen, wenn $i = j$ ist.

Notwendige Randomisierung

Wir betrachten Angriffe mit gewählten Klartext (chosen plaintext attacks)

D.h. wir betrachten Angreifer im entsprechenden Spiel.

Für ein determinisistisches Verschlüsselungsverfahren gibt es immer einen trivialen Angriff (CPA) mit Erfolg 1:

Einfach die gewählten Nachrichten verschlüsseln lassen und nachschauen.

Dies motiviert, randomisierte Verfahren zu betrachten.

Notwendige Randomisierung

Verständnisfrage. Und was ist mit dem one-time-Pad? Ist das nicht "vollkommen sicher", wenn man nicht "Strahlung" beachtet? (Also auch CPA, CCA, CCA2-sicher?)

Antwort. Nein nach Definition, denn man würde immer wieder "zurückspulen".

Ja, wenn man auch den Zustand modelliert.

Wichtig. Laut Definition sind die betrachteten Verfahren zustandslos.

Hin zu einem komplexitätstheoreitschen Ansatz

Wir haben gesehen:

Ein gegenüber Lauschern sicheres Verfahren braucht einen Schlüsselraum, der mindestens so groß ist wie der Nachrichtenraum.

Aber immerhin haben wir das one-time-Pad ....

Frage. Gibt es überhaupt ein (zustandsloses) Verfahren, das "perfekt sicher gegenüber Angriffen mit gewähltem Klartext" ist?

(Achtung: "perfekt sicher" ist schon definiert, wir weichen hier für den Moment ab.)

Antwort. Nein

Angriff

- Wähle zwei verschiedene Nachrichten $m^{(1)}, m^{(2)}$.
- Nach Erhalt von $c = \mathcal{E}nc_k(m^{(i)})$:
  Lasse immer wieder $m^{(1)}, m^{(2)}$ verschlüsseln, bis
  $c = \mathcal{E}nc_k(m^{(j)})$.
  Wähle j.

Der Erfolg ist wieder 1.

Hin zum komplexitätstheoretischen Ansatz

Man sollte einen gewissen Erfolg zulassen

und gleichzeitig die Laufzeit in gewisser Weise beschränken.