Beweisbar sichere Verschlüsselung

ITS-Wahlpflichtvorlesung

Dr. Bodo Möller
Ruhr-Universität Bochum
Horst-Görtz-Institut für IT-Sicherheit
Lehrstuhl für Kommunikationssicherheit
bmoeller@crypto.rub.de

$Id: bsv.ltx,v 1.17 2007/04/18 15:49:11 bm Exp $

Überblick

- Wann sind Krypto-Verfahren *„sicher“*?

  → brauchen *genaue Beschreibungen* der gewünschten Eigenschaften
  → (z. B.) formalisierte *Angriffsspiele*

- *Verschiedene Sicherheitsbegriffe* stehen zur Auswahl:
  nicht „X ist sicher“, sondern „X ist sicher im Sinne von Y“

- Aber wirklich *beweisbar sicher* ist fast nichts

- Oft möglich ist *Sicherheitsbeweis durch Reduktion*:

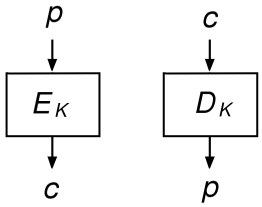
  Setze Sicherheit voraus für kryptographische *„Primitive“*,
  folgere Sicherheit für eine Konstruktion

Überblick (Forts.)

- *„Beweisbar sicher“* heißt fast immer:
  Beweis durch Reduktion mit (hoffentlich) vernünftigen Annahmen
- Möglichst einfache Annahmen!
- Ad-hoc-Konstruktionen ohne Beweis sind oft problematisch

Überblick (Forts.)

Beispiel: *Blockchiffre* (AES u. a.) als Primitive



$K \in \{0,1\}^k$

$E_K \colon \{0,1\}^\ell \to \{0,1\}^\ell$ (Verschlüsselung)
$D_K \colon \{0,1\}^\ell \to \{0,1\}^\ell$ (Entschlüsselung)

$D_K\big(E_K(p)\big) = p$ für alle $K \in \{0,1\}^k$, $p \in \{0,1\}^\ell$

Grundlegende Sicherheitseigenschaft (informell):
Ist K unbekannt, soll sich E_K *„wie zufällig“* verhalten

Überblick (Forts.)

Inhalte der Vorlesung:

- Konzepte und Techniken für beweisbare Sicherheit in der Kryptographie
- Sicherheitsbegriffe für Verschlüsselung
- Grundlegende Konstruktionen

Voraussetzungen:

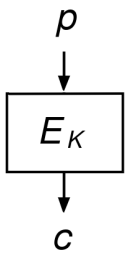
- Grundkenntnisse Kryptographie
- Rechnen mit Wahrscheinlichkeiten

Zum Vorgehen

- Folien und Aufgabenblätter:
  `http://www.crypto.rub.de/bewsich.html`
- *Übungen*: Mo 10–11 (IC 1/161) ab **16. 4. 2007**
- Lösen der Übungsblätter *teilweise* bewertet
  (... es steht vorher fest, welche!)
- Ergänzende *Literaturempfehlung* (mit zuviel Inhalt für 2+1 SWS ...):

  Mihir Bellare, Phillip Rogaway, "Introduction to Modern Cryptography"
  `http://www-cse.ucsd.edu/users/mihir/cse207/classnotes.html`

Sicherheit einer Blockchiffre



$K \in \{0,1\}^k =: \mathcal{K}$

$E_K \colon \{0,1\}^\ell \to \{0,1\}^\ell$

Jedes E_K ist eine *Permutation,* also injektiv: $E_K(p_1) \neq E_K(p_2)$ für $p_1 \neq p_2$

Grundlegende Sicherheitseigenschaft: E_K soll „wie zufällig aussehen“

Sicherheit einer Blockchiffre (Forts.)

Formalisierung durch ein *Angriffsspiel:*
Betrachte einen *Angreifer* (Gegner, *adversary*) $\boldsymbol{A}$

- $\boldsymbol{A}$ ist probabilistischer Algorithmus (d. h. mit Zufallszahlengenerator), interagiert mit einer Funktion $f \colon \{0,1\}^\ell \to \{0,1\}^\ell$
- f ist “black box” für $\boldsymbol{A}$:
  $\boldsymbol{A}$ kann Anfragen p senden und erhält jeweils $f(p)$;
  kein anderer Zugriff auf f
- Wir sagen auch: $\boldsymbol{A}$ hat *„Orakel-Zugriff“* auf f
  ... oder auch: auf $f(\cdot)$
- Wir schreiben auch: $\boldsymbol{A}^{f(\cdot)}$
- Schließlich gibt $\boldsymbol{A}$ ein Bit aus (0 oder 1).
  Wir schreiben $\boldsymbol{A}^{f(\cdot)} \Rightarrow 0$ oder $\boldsymbol{A}^{f(\cdot)} \Rightarrow 1$.

Sicherheit einer Blockchiffre (Forts.)

- Für $f(\cdot)$ können wir z. B. E_K einsetzen (mit $K \in \mathcal{K}$):
  $$\boldsymbol{A}^{E_K(\cdot)}$$
- $K \in_\$ \mathcal{K}$ heiße: K wird mit Gleichverteilung zufällig gewählt.
  Dann können wir betrachten:
  $$\Pr_{K \in_\$ \mathcal{K}}\left[\boldsymbol{A}^{E_K(\cdot)} \Rightarrow 1\right]$$
  Das ist eine Zahl irgendwo zwischen 0 (z. B., wenn $\boldsymbol{A}$ *immer* 0 ausgibt) und 1 (z. B., wenn $\boldsymbol{A}$ *immer* 1 ausgibt).
- Oder wähle eine zufällige Permutation (d. h. Bijektion) $\pi\colon \{0,1\}^\ell \to \{0,1\}^\ell$; wir schreiben $\pi \in \mathrm{Perm}(\{0,1\}^\ell)$.
  Wir können betrachten:
  $$\Pr_{\pi \in_\$ \mathrm{Perm}(\{0,1\}^\ell)}\left[\boldsymbol{A}^{\pi(\cdot)} \Rightarrow 1\right]$$

Sicherheit einer Blockchiffre (Forts.)

- Für *Vergleich* von E_K (Blockchiffre) mit Zufallspermutation betrachte
  $$\mathrm{Adv}^{\mathrm{PRP}}_{E,\boldsymbol{A}} := \Pr_{K \in_\$ \mathcal{K}}\left[\boldsymbol{A}^{E_K(\cdot)} \Rightarrow 1\right] - \Pr_{\pi \in_\$ \mathrm{Perm}(\{0,1\}^\ell)}\left[\boldsymbol{A}^{\pi(\cdot)} \Rightarrow 1\right]$$
- Das ist eine Zahl zwischen -1 und 1
- Wir nennen sie den *Vorteil* (*advantage*) von $\boldsymbol{A}$ gegen die Blockchiffre, genauer: *PRP-Vorteil* ("PRP" = *pseudo-random permutation*)
- Was besagt die Zahl $\mathrm{Adv}^{\mathrm{PRP}}_{E,\boldsymbol{A}}$?
  Ein „ausgeschmücktes" Angriffsspiel macht's deutlicher ...

Sicherheit einer Blockchiffre (Forts.)

Neuer Ablauf des Angriffsspiels:

- Wähle $b \in_\$ \{0,1\}$
- Falls $b = 1$, lass $\boldsymbol{A}^{E_K(\cdot)}$ ablaufen mit $K \in_\$ \mathcal{K}$;
  falls $b = 0$, lass $\boldsymbol{A}^{\pi(\cdot)}$ ablaufen mit $\pi \in_\$ \mathrm{Perm}(\{0,1\}^\ell)$.
- Die Ausgabe von $\boldsymbol{A}$ nennen wir $\widetilde{b}$

Interpretation: $\boldsymbol{A}$ versucht, mit $\widetilde{b}$ das versteckte Bit b zu erraten

Setze

$$\mathrm{Adv}'_{E,\boldsymbol{A}} = 2\Big(\Pr[\widetilde{b} = b] - \frac{1}{2}\Big).$$

Sicherheit einer Blockchiffre (Forts.)

$$\mathrm{Adv}'_{E,\boldsymbol{A}} = 2\Big(\Pr[\widetilde{b} = b] - \frac{1}{2}\Big)$$

Das ist eine Zahl zwischen -1 und 1.

- Wert 1 heißt: $\boldsymbol{A}$ rät immer richtig.
- Wert 0 heißt: $\boldsymbol{A}$ ist nicht besser als zufällig.

... deshalb *„Vorteil“* (*advantage*)!

- Wert -1 heißt: „Umgedrehtes“ $\boldsymbol{A}$ rät immer richtig!
  (Gib 1 aus gdw. $\boldsymbol{A} \Rightarrow 0$)

Sicherheit einer Blockchiffre (Forts.)

$$
\begin{aligned}
\mathrm{Adv}^{\mathsf{PRP}}_{E,\boldsymbol{A}} &= \Pr{}_{K\in_{\$}\mathcal{K}}\big[\boldsymbol{A}^{E_K(\cdot)} \Rightarrow 1\big] - \Pr{}_{\pi\in_{\$}\mathrm{Perm}(\{0,1\}^\ell)}\big[\boldsymbol{A}^{\pi(\cdot)} \Rightarrow 1\big] \\
&= \Pr\big[\widetilde{b} = 1 \mid b = 1\big] - \Pr\big[\widetilde{b} = 1 \mid b = 0\big] \\
&= \Pr\big[\widetilde{b} = 1 \mid b = 1\big] - \Big(1 - \Pr\big[\widetilde{b} = 0 \mid b = 0\big]\Big) \\
&= \Big(\Pr\big[\widetilde{b} = 1 \mid b = 1\big] + \Pr\big[\widetilde{b} = 0 \mid b = 0\big]\Big) - 1 \\
&= \left(\frac{\Pr\big[\widetilde{b} = 1 \wedge b = 1\big]}{\Pr\big[b = 1\big]} + \frac{\Pr\big[\widetilde{b} = 0 \wedge b = 0\big]}{\Pr\big[b = 0\big]}\right) - 1 \\
&= \left(\frac{\Pr\big[\widetilde{b} = 1 \wedge b = 1\big]}{\frac{1}{2}} + \frac{\Pr\big[\widetilde{b} = 0 \wedge b = 0\big]}{\frac{1}{2}}\right) - 1 \\
&= 2\Big(\Pr\big[\widetilde{b} = 1 \wedge b = 1\big] + \Pr\big[\widetilde{b} = 0 \wedge b = 0\big]\Big) - 1 \\
&= 2\big(\Pr\big[\widetilde{b} = b\big]\big) - 1 \;=\; 2\Big(\Pr\big[\widetilde{b} = b\big] - \frac{1}{2}\Big) \;=\; \mathrm{Adv}'_{E,\boldsymbol{A}}
\end{aligned}
$$

Sicherheit einer Blockchiffre (Forts.)

Wir haben also zwei Formulierungen für die gleiche Größe:

$$\mathrm{Adv}^{\mathsf{PRP}}_{E,\boldsymbol{A}} = \Pr{}_{K\in_{\$}\mathcal{K}}\big[\boldsymbol{A}^{E_K(\cdot)} \Rightarrow 1\big] - \Pr{}_{\pi\in_{\$}\mathrm{Perm}(\{0,1\}^\ell)}\big[\boldsymbol{A}^{\pi(\cdot)} \Rightarrow 1\big]$$

und (im „ausgeschmückten“ Angriffsspiel)

$$\mathrm{Adv}^{\mathsf{PRP}}_{E,\boldsymbol{A}} = 2\big(\Pr\big[\widetilde{b} = b\big] - \tfrac{1}{2}\big).$$

Wir nennen E *sicher* (hier speziell: *PRP-sicher*),
wenn der Vorteil $\mathrm{Adv}^{\mathsf{PRP}}_{E,\boldsymbol{A}}$ für jeden denkbaren Angreifer $\boldsymbol{A}$
verschwindend gering bleibt.

Sicherheit einer Blockchiffre (Forts.)

Wir nennen E *sicher* (hier speziell: *PRP-sicher*),
wenn der Vorteil $\mathrm{Adv}^{\mathrm{PRP}}_{E,\boldsymbol{A}}$ für jeden denkbaren Angreifer $\boldsymbol{A}$
verschwindend gering bleibt.

Beides sind bewusst schwammige Kriterien!

- Welche Angreifer sind „denkbar“? (Begrenzte Ressourcen, insbesondere Zeit)
- Welcher Vorteil gilt noch als „verschwindend gering“?

Für Beweise *durch Reduktion* muss man diese Fragen oft nicht beantworten:
beliebige quantitative Annahmen ergeben entsprechende Folgerungen.

Rückblick

- „Beweisbar sichere“ Kryptographie ist selten vollständig beweisbar sicher
- Sicherheitsbeweise brauchen Voraussetzungen für *Primitive*
- ... z. B. AES als PRP-sicher (Details von AES bleiben hier außen vor!)
- Hantieren mit formalen Sicherheitsbegriffen erfordert Stochastik
  (bedingte Wahrscheinlichkeiten)

Vorschau

- Sicherheitsbegriffe für Einmal-Verschlüsselung
- Sicherheitsbegriffe für symmetrische Verschlüsselung