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 1.99 2007/07/11 10:16:09 bm Exp $

Übungsaufgaben

- Aufgabe 2.3, Counter Mode:
  heute
- Aufgaben *2.1 und 2.2*, Electronic Codebook Mode (ECB):
  zu Montag (7. Mai) als *bewertete Aufgaben!*
- Aufgaben 2.4 und 2.5, Counter Mode:
  Montag

Überblick

Wir bleiben noch bei einem passiven Angreifer,
also "CPA" (chosen-plaintext attack).

Weitere Sicherheitsbegriffe für Verschlüsselung neben RoR und LoR:

- *Find-then-Guess* (heute)
- *semantische Sicherheit* (nächste Woche)

Find-then-Guess-Sicherheit

- Bekannt: *Left-or-right-Angriffsspiel* (LoR-CPA)
  mit Linksverschlüsselungsorakel $E_1(\cdot,\cdot)$, Rechtsverschlüsselungsorakel $E_0(\cdot,\cdot)$
- Dort *durchgängig* Links- oder Rechtsverschlüsselung
- *Variante davon:* Angreifer bekommt (*echtes*) Verschlüsselungsorakel $E(\cdot)$
  und *Einmal*-Links-oder-rechts-Verschlüsselungsorakel $E_b(\cdot,\cdot)$
  ($b = 1$ für links oder $b = 0$ für rechts)
- ... mit folgendem Ablauf:

  Angreifer stellt Anfragen an $E(\cdot)$ (*Find*),
  stellt *eine* Anfrage an $E_b(\cdot,\cdot)$,
  stellt weitere Anfragen an $E(\cdot)$
  und gibt schließlich ein Bit $\widetilde{b}$ aus (*Guess*)

Find-then-Guess-Sicherheit (Forts.)

Das *FtG-CPA-Angriffsspiel* mit den Fällen $b = 1$, $b = 0$ sieht also wie folgt aus für ein Verschlüsselungsschema $(\mathcal{K}, \mathcal{E}, \mathcal{D})$ mit Plaintextmenge $\mathcal{M}$.

- $K \xleftarrow{\$} \mathcal{K}$ wird (für den Angreifer geheim) festgelegt.
- Angreifer $\boldsymbol{A}$ hat Orakelzugriff auf ein Verschlüsselungsorakel $E(\cdot)$.
  Dieses Orakel gibt $\mathcal{E}_K(m)$ zurück (zur Anfrage $m \in \mathcal{M}$).
- Angreifer $\boldsymbol{A}$ hat außerdem Orakelzugriff auf $E_b(\cdot,\cdot)$, aber *nur einmal;*
  die Anfrage (m_1, m_0) muss erfüllen $|m_1| = |m_0|$ und $m_1, m_0 \in \mathcal{M}$.
  Dieses Orakel gibt $\mathcal{E}_K(m_b)$ zurück.
- $\boldsymbol{A}$ gibt schließlich ein Bit $\widetilde{b}$ aus.

Der *FtG-CPA-Vorteil* folgt dem gewohnten Muster:

$$\mathrm{Adv}^{\text{FtG-CPA}}_{(\mathcal{K},\mathcal{E},\mathcal{D}),\boldsymbol{A}} \;=\; \Pr\left[\boldsymbol{A}^{E(\cdot),E_1(\cdot,\cdot)} \Rightarrow 1\right] - \Pr\left[\boldsymbol{A}^{E(\cdot),E_0(\cdot,\cdot)} \Rightarrow 1\right]$$

Find-then-Guess-Sicherheit (Forts.)

- Ein "FtG-OTCPA" brauchen wir nicht zu betrachten!
  (Bei Einmalverschlüsselung hat das zweite Orakel in FtG-CPA keinen Platz, also quasi FtG-OTCPA = LoR-OTCPA.)
- *FtG-CPA* nennt sich oft auch *IND-CPA*
  für *indistinguishability of encryption* ...
- ... aber "IND-CPA" ist *nicht eindeutig:*
  oft ist FtG-CPA gemeint, manchmal LoR-CPA!
  Mit ausdrücklichem "FtG" und "LoR" vermeiden wir Verwechslungen.

Find-then-Guess-Sicherheit (Forts.)

Wie ordnet sich der neue Sicherheitsbegriff ein?

- Aus LoR-CPA-Sicherheit folgt FtG-CPA-Sicherheit
- Aus FtG-CPA-Sicherheit folgt LoR-CPA-Sicherheit,
  aber i. a quantitativ schwächer (LoR-CPA-Vorteil kann größer sein)

Details und Beweise folgen ...

Find-then-Guess-Sicherheit (Forts.)

Behauptung (informell): *Aus LoR-CPA-Sicherheit folgt FtG-CPA-Sicherheit*

Beweis:

Zu FtG-CPA-Angreifer $\boldsymbol{A}$ konstruieren wir LoR-CPA-Angreifer $\boldsymbol{B}$
mit im wesentlichen gleicher Laufzeit und

$$\mathrm{Adv}^{\text{LoR-CPA}}_{(\mathcal{K},\mathcal{E},\mathcal{D}),\boldsymbol{B}} = \mathrm{Adv}^{\text{FtG-CPA}}_{(\mathcal{K},\mathcal{E},\mathcal{D}),\boldsymbol{A}}$$

(gibt es keinen erfolgreichen LoR-CPA-Angreifer, kann es also auch
keinen erfolgreichen FtG-CPA-Angreifer geben).

...

Find-then-Guess-Sicherheit (Forts.)

Zu FtG-CPA-Angreifer $\boldsymbol{A}$ konstruieren wir LoR-CPA-Angreifer $\boldsymbol{B}$ mit im wesentlichen gleicher Laufzeit und $\mathrm{Adv}^{\text{LoR-CPA}}_{(\mathcal{K},\mathcal{E},\mathcal{D}),\boldsymbol{B}} = \mathrm{Adv}^{\text{FtG-CPA}}_{(\mathcal{K},\mathcal{E},\mathcal{D}),\boldsymbol{A}}$

$\boldsymbol{A}$ erwartet ein (echtes) Verschlüsselungsorakel und ein Einmal-LoR-Verschlüsselungsorakel.

$\boldsymbol{B}$ hat LoR-Verschlüsselungsorakel zur Verfügung

Das Einmal-LoR-Verschlüsselungsorakel $E_b(\cdot,\cdot)$ für $\boldsymbol{A}$ ist also kein Problem: Verwende das Orakel von $\boldsymbol{B}$.

Das Verschlüsselungsorakel $E(\cdot)$ für $\boldsymbol{A}$ ist auch problemlos „nachzubauen“! Für Anfrage m verwende das Orakel von $\boldsymbol{B}$ mit Anfrage (m,m).

So konstruiert, hat $\boldsymbol{B}$ genau den gleichen Ablauf wie $\boldsymbol{A}$:

$$\Pr\left[\boldsymbol{B}^{E_1(\cdot,\cdot)} \Rightarrow 1\right] = \Pr\left[\boldsymbol{A}^{E(\cdot),E_1(\cdot,\cdot)} \Rightarrow 1\right]$$
$$\Pr\left[\boldsymbol{B}^{E_0(\cdot,\cdot)} \Rightarrow 1\right] = \Pr\left[\boldsymbol{A}^{E(\cdot),E_0(\cdot,\cdot)} \Rightarrow 1\right]$$

Also gleicher Vorteil, q.e.d.!

Find-then-Guess-Sicherheit (Forts.)

Behauptung (informell):

Aus FtG-CPA-Sicherheit folgt LoR-CPA-Sicherheit in einem schwächeren Sinn,
nämlich bei bis zu q-facher Zunahme des Vorteils,
wenn die Orakel bis zu q-mal benutzt werden

Beweis:

Zu LoR-CPA-Angreifer $\boldsymbol{A}$ konstruieren wir FtG-CPA-Angreifer $\boldsymbol{B}$
mit im wesentlichen gleicher Laufzeit und

$$\mathrm{Adv}^{\text{FtG-CPA}}_{(\mathcal{K},\mathcal{E},\mathcal{D}),\boldsymbol{B}} = \frac{1}{q} \cdot \mathrm{Adv}^{\text{LoR-CPA}}_{(\mathcal{K},\mathcal{E},\mathcal{D}),\boldsymbol{A}}$$

...

Find-then-Guess-Sicherheit (Forts.)

Zu LoR-CPA-Angreifer $\boldsymbol{A}$ konstruieren wir FtG-CPA-Angreifer $\boldsymbol{B}$ mit im wesentlichen gleicher Laufzeit und $\mathrm{Adv}^{\text{FtG-CPA}}_{(\mathcal{K},\mathcal{E},\mathcal{D}),\boldsymbol{B}} = \frac{1}{q} \cdot \mathrm{Adv}^{\text{LoR-CPA}}_{(\mathcal{K},\mathcal{E},\mathcal{D}),\boldsymbol{A}}$

$\boldsymbol{A}$ erwartet LoR-Verschlüsselungsorakel $E_{\boldsymbol{A}}(\cdot,\cdot)$,
$\boldsymbol{B}$ hat Verschlüsselungsorakel $E(\cdot)$ und Einmal-LoR-Verschlüsselungsorakel $E(\cdot,\cdot)$

Für $i = 1, \ldots, q$ konstruieren wir aus $\boldsymbol{A}$ einen FtG-CPA-Angreifer $\boldsymbol{B}_i$:

- Für die ersten $i-1$ Anfragen $E_{\boldsymbol{A}}(m_1, m_0)$: gib $\boldsymbol{A}$ die Orakelantwort $E(m_1)$
- Für die i-te Anfrage $E_{\boldsymbol{A}}(m_1, m_0)$: gib $\boldsymbol{A}$ die Orakelantwort $E(m_1, m_0)$
- Für spätere Anfragen $E_{\boldsymbol{A}}(m_1, m_0)$: gib $\boldsymbol{A}$ die Orakelantwort $E(m_0)$

Beobachtungen:

$\boldsymbol{B}_q^{E(\cdot),E_1(\cdot,\cdot)}$ (also $\boldsymbol{B}_q$ in einer Umgebung mit Linksverschlüsselung)
bietet $\boldsymbol{A}$ durchgehend ein Linksverschlüsselungsorakel.

$\boldsymbol{B}_1^{E(\cdot),E_0(\cdot,\cdot)}$ (also $\boldsymbol{B}_1$ in einer Umgebung mit Rechtsverschlüsselung)
bietet $\boldsymbol{A}$ durchgehend ein Rechtsverschlüsselungsorakel.

$\boldsymbol{B}_i^{E(\cdot),E_1(\cdot,\cdot)}$ entspricht exakt $\boldsymbol{B}_{i+1}^{E(\cdot),E_0(\cdot,\cdot)}$ (i-malig links, danach rechts).

Find-then-Guess-Sicherheit (Forts.)

$\boldsymbol{B}_q^{E_1(\cdot,\cdot)}$ bietet $\boldsymbol{A}$ durchgehend ein Linksverschlüsselungsorakel,
$\boldsymbol{B}_1^{E_0(\cdot,\cdot)}$ bietet $\boldsymbol{A}$ durchgehend ein Rechtsverschlüsselungsorakel,
$\boldsymbol{B}_i^{E(\cdot),E_1(\cdot,\cdot)}$ entspricht exakt $\boldsymbol{B}_{i+1}^{E(\cdot),E_0(\cdot,\cdot)}$

$$
\begin{aligned}
\mathrm{Adv}^{\text{LoR-CPA}}_{(\mathcal{K},\mathcal{E},\mathcal{D}),\boldsymbol{A}} &= \Pr\left[\boldsymbol{A}^{E_{\boldsymbol{A},1}(\cdot,\cdot)} \Rightarrow 1\right] - \Pr\left[\boldsymbol{A}^{E_{\boldsymbol{A},0}(\cdot,\cdot)} \Rightarrow 1\right] \\
&= \Pr\left[\boldsymbol{B}_q^{E(\cdot),E_1(\cdot,\cdot)} \Rightarrow 1\right] - \Pr\left[\boldsymbol{B}_1^{E(\cdot),E_0(\cdot,\cdot)} \Rightarrow 1\right] \\
&\quad + \sum_{1 \le i < q} \Big(\underbrace{\Pr\left[\boldsymbol{B}_i^{E(\cdot),E_1(\cdot,\cdot)} \Rightarrow 1\right] - \Pr\left[\boldsymbol{B}_{i+1}^{E(\cdot),E_0(\cdot,\cdot)} \Rightarrow 1\right]}_{0} \Big) \\
&= \sum_{1 \le i \le q} \Big(\Pr\left[\boldsymbol{B}_i^{E(\cdot),E_1(\cdot,\cdot)} \Rightarrow 1\right] - \Pr\left[\boldsymbol{B}_i^{E(\cdot),E_0(\cdot,\cdot)} \Rightarrow 1\right] \Big) \\
&= \sum_{1 \le i \le q} \mathrm{Adv}^{\text{FtG-CPA}}_{(\mathcal{K},\mathcal{E},\mathcal{D}),\boldsymbol{B}_i}
\end{aligned}
$$

Find-then-Guess-Sicherheit (Forts.)

$$\mathrm{Adv}^{\text{LoR-CPA}}_{(\mathcal{K},\mathcal{E},\mathcal{D}),\boldsymbol{A}} = \sum_{1\le i\le q} \mathrm{Adv}^{\text{FtG-CPA}}_{(\mathcal{K},\mathcal{E},\mathcal{D}),\boldsymbol{B}_i}$$

Konstruiere $\boldsymbol{B}$ aus den $\boldsymbol{B}_i$:
Wähle $i \xleftarrow{\$} \{1,\ldots,q\}$ und greif dann genau wie $\boldsymbol{B}_i$ an. Dann

$$\begin{aligned}
\mathrm{Adv}^{\text{FtG-CPA}}_{(\mathcal{K},\mathcal{E},\mathcal{D}),\boldsymbol{B}} &= \Pr\left[\boldsymbol{B}^{E(\cdot),E_1(\cdot,\cdot)} \Rightarrow 1\right] - \Pr\left[\boldsymbol{B}^{E(\cdot),E_0(\cdot,\cdot)} \Rightarrow 1\right] \\
&= \frac{1}{q} \cdot \sum_{1\le i\le q} \Pr\left[\boldsymbol{B}_i^{E(\cdot),E_1(\cdot,\cdot)} \Rightarrow 1\right] \\
&\quad - \frac{1}{q} \cdot \sum_{1\le i\le q} \Pr\left[\boldsymbol{B}_i^{E(\cdot),E_0(\cdot,\cdot)} \Rightarrow 1\right] \\
&= \frac{1}{q} \cdot \sum_{1\le i\le q} \mathrm{Adv}^{\text{FtG-CPA}}_{(\mathcal{K},\mathcal{E},\mathcal{D}),\boldsymbol{B}_i} \\
&= \frac{1}{q} \cdot \mathrm{Adv}^{\text{LoR-CPA}}_{(\mathcal{K},\mathcal{E},\mathcal{D}),\boldsymbol{A}}.
\end{aligned}$$

Q.e.d.!

Find-then-Guess-Sicherheit (Forts.)

Zusammenfassung: Sicherheit im Sinne von FtG-CPA

- entspricht *qualitativ* Sicherheit im Sinne von LoR-CPA (und damit auch RoR-CPA),
- ist dabei aber *quantitativ* schwächer.

Warum dann überhaupt Find-then-Guess?

Bei FtG haben wir nur einmal ein „seltsames“ Orakel (das LoR-Orakel), sonst ein echtes Verschlüsselungsorakel.

Damit ist FtG-Sicherheit in Beweisen oft einfacher handzuhaben als RoR oder LoR.