Beweisbar sichere Verschlüsselung

ITS-Wahlpflichtvorlesung

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

Semantische Sicherheit

- Sicherheit von Verschlüsselungsschemen haben wir beschrieben durch "Real-or-Random"-, "Left-or-Right"- und "Find-then-Guess"-Angriffsspiele
- *„Sicher"* für RoR-OTCPA, LoR-OTCPA, RoR-CPA, LoR-CPA, FtG-CPA, wenn der *Vorteil* für jeden denkbaren Angreifer klein bleibt
- Anscheinend brauchbare Sicherheitsbegriffe – sehen aber doch willkürlich aus
- Was sollten wir von „sicherer" Verschlüsselung eigentlich verlangen ...?

Semantische Sicherheit (Forts.)

- Sichere Verschlüsselung *intuitiv:*
  Dem *Ciphertext* soll *nichts über den Plaintext* anzusehen sein
  (außer der Länge)
- *Formalisierung* als *semantische Sicherheit*
- Wir werden sehen: Auch das ist *äquivalent* zu den schon bekannten Begriffen!
- Aber schwerer zu handhaben: Gut vor allem für zusätzliches Verständnis,
  nicht zum Anwenden bei Sicherheitsbeweisen!
- In der Literatur im Detail große Unterschiede bei der Formalisierung
  der semantischen Sicherheit
- Hier nur ein Ansatz als Einblick (ohne die letzten Details)

Semantische Sicherheit (Forts.)

- *Angreifer* und *Vorteil* auch hier, aber etwas anders als bisher!
- *Bisher:* Vorteil *eines Angreifers*
- *Hier:* Vorteil betrachtet Angreifer *mit „Simulator“ zusammen*;
  „sicher“, wenn es *zu jedem Angreifer* einen *Simulator* gibt,
  so dass der Vorteil gering ist
- Vorteil soll hier beschreiben, was der Angreifer dem Ciphertext ansehen kann
- *Simulator* arbeitet ähnlich wie der Angreifer – aber *ohne Ciphertext!*
- Idee: Wenn ein solcher Simulator den Angreifer gut nachbilden kann,
  konnte der Angreifer dem Ciphertext nichts Brauchbares ansehen

Semantische Sicherheit für Einmalverschlüsselung

- Definition hier für Einmalverschlüsselung: *"Sem-OTCPA"*
  (semantic security under one-time chosen plaintext attack)
- *Angreifer* $\boldsymbol{A}$ ist wieder ein probabilistischer *Algorithmus*
  mit Zugriff auf ein *Orakel* $C(\cdot)$
- ... das ist eine Art Verschlüsselungsorakel,
  wieder mit einem geheimen Schlüssel $K \xleftarrow{\$} \mathcal{K}$,
  aber *etwas anders* als bisher!
- $\boldsymbol{A}$ übergibt dem Orakel $C(\cdot)$ die *Beschreibung einer Plaintext-Verteilung*
  als *probabilistischen Algorithmus* („Programm") $\mathfrak{M}$,
  das Orakel lässt $m \xleftarrow{\$} \mathfrak{M}$ laufen und verschlüsselt m:
  $c \xleftarrow{\$} \mathcal{E}_K(m)$, und c geht als Orakelantwort zurück an $\boldsymbol{A}$

Semantische Sicherheit für Einmalverschlüsselung (Forts.)

- $\boldsymbol{A}$ übergibt dem Orakel $C(\cdot)$ die *Beschreibung einer Plaintext-Verteilung*
  als *probabilistischen Algorithmus* („Programm") $\mathfrak{M}$,
  das Orakel lässt $m \xleftarrow{\$} \mathfrak{M}$ laufen und verschlüsselt m:
  $c \xleftarrow{\$} \mathcal{E}_K(m)$, und c geht als Orakelantwort zurück an $\boldsymbol{A}$
- *Einschränkung* dabei: Alle Ausgaben von $\mathfrak{M}$ müssen die gleiche Länge haben
  (denn nur für gleiche Längen erwarten wir sichere Verschlüsselung)
- $\boldsymbol{A}$ versucht sozusagen, dem Ciphertext c etwas über m anzusehen
- *Ausgaben* von $\boldsymbol{A}$: eine Funktionsbeschreibung $\mathfrak{f}$ und ein Wert y
- Test am Ende: Gilt $\mathfrak{f}(m) = y$?
- Soweit noch keine Aussage über Sicherheit möglich!
  $\boldsymbol{A}$ kann $\mathfrak{M}$ und $\mathfrak{f}$ so wählen, dass sich $\mathfrak{f}(m)$ trivial vorhersagen lässt
- Deshalb kommt der *Simulator* $\boldsymbol{S}$ ins Spiel ...

Semantische Sicherheit für Einmalverschlüsselung (Forts.)

- Simulator $\boldsymbol{S}$ ist wie $\boldsymbol{A}$ ein probabilistischer Algorithmus, soll $\boldsymbol{A}$ „simulieren“ – *ohne* Zugriff auf c!
- Dafür Orakel-Variante $\overline{C}(\cdot)$: nimmt $\mathfrak{M}$ entgegen und legt fest $m \xleftarrow{\$} \mathfrak{M}$, gibt aber nichts zurück (c bleibt unbekannt)
- $\boldsymbol{S}$ ist *gültiger Simulator* für $\boldsymbol{A}$, wenn seine Anfrage $\mathfrak{M}$ an $\overline{C}(\cdot)$ die gleiche Verteilung hat wie die Anfrage $\mathfrak{M}$ an $C(\cdot)$ bei $\boldsymbol{A}$ und auch $\mathfrak{f}$ die gleiche Verteilung hat wie bei $\boldsymbol{A}$
- Das Verschlüsselungsschema $(\mathcal{K}, \mathcal{E}, \mathcal{D})$ heißt *semantisch sicher* (unter OTCPA = one-time chosen plaintext attack),
  wenn es *zu jedem Angreifer* $\boldsymbol{A}$ einen gültigen *Simulator* $\boldsymbol{S}$ gibt, so dass der *Vorteil*

$$\mathrm{Adv}^{\text{Sem-OTCPA}}_{(\mathcal{K},\mathcal{E},\mathcal{D}),\boldsymbol{A},\boldsymbol{S}} = \Pr_{(\mathfrak{f},y)\xleftarrow{\$}\boldsymbol{A}^{C(\cdot)}}\Big[\mathfrak{f}(m) = y\Big] - \Pr_{(\mathfrak{f},y)\xleftarrow{\$}\boldsymbol{S}^{\overline{C}(\cdot)}}\Big[\mathfrak{f}(m) = y\Big]$$

  verschwindend gering ist!
  (Darin ist m der von $C(\cdot)$ bzw. $\overline{C}(\cdot)$ gewählte Plaintext wie oben beschrieben.)

Semantische Sicherheit für Einmalverschlüsselung (Forts.)

- Das Verschlüsselungsschema $(\mathcal{K}, \mathcal{E}, \mathcal{D})$ heißt *semantisch sicher* (unter OTCPA = one-time chosen plaintext attack),
  wenn es *zu jedem Angreifer* $\boldsymbol{A}$ einen gültigen *Simulator* $\boldsymbol{S}$ gibt, so dass der *Vorteil*

$$\mathrm{Adv}^{\text{Sem-OTCPA}}_{(\mathcal{K},\mathcal{E},\mathcal{D}),\boldsymbol{A},\boldsymbol{S}} = \Pr_{(\mathfrak{f},y)\xleftarrow{\$}\boldsymbol{A}^{C(\cdot)}}\Big[\mathfrak{f}(m) = y\Big] - \Pr_{(\mathfrak{f},y)\xleftarrow{\$}\boldsymbol{S}^{\overline{C}(\cdot)}}\Big[\mathfrak{f}(m) = y\Big]$$

  verschwindend gering ist

- Das bedeutet (wie gewünscht): $\boldsymbol{A}$ kann nichts Konkretes sagen über den unbekannten Plaintext m hinter der Orakelantwort $C(\cdot)$;
  denn alles, was $\boldsymbol{A}$ weiß, weiß $\boldsymbol{S}$ schon ohne die Orakelantwort!

Sem-OTCPA und LoR-OTCPA

- Wir wollen zeigen, dass unsere bisherigen Sicherheitsbegriffe äquivalent sind zu semantischer Sicherheit.

  (→ Zusätzliche Gewissheit, dass wir bisher schon die „richtigen“ Sicherheitsbegriffe verwendet haben.)

- Also zeigen wir: *Sem-OTCPA-Sicherheit impliziert LoR-OTCPA-Sicherheit*

  oder gleichbedeutend:
  LoR-OTCPA-*Unsicherheit* impliziert Sem-OTCPA-*Unsicherheit*

- Und: *LoR-OTCPA-Sicherheit impliziert Sem-OTCPA-Sicherheit*

  oder gleichbedeutend:
  Sem-OTCPA-*Unsicherheit* impliziert LoR-OTCPA-*Unsicherheit*

Sem-OTCPA und LoR-OTCPA (Forts.)

1. Ziel: *LoR-OTCPA-Unsicherheit impliziert Sem-OTCPA-Unsicherheit*

- Sei (erfolgreicher) LoR-OTCPA-Angreifer $\boldsymbol{A}$ gegeben
- Wir konstruieren einen (erfolgreichen) Sem-OTCPA-Angreifer $\boldsymbol{B}$, also einen Angreifer, der sich nicht gut simulieren lässt
- *Idee der Konstruktion:* Beschreibe den LoR-Angriff mit den Mitteln, die das Modell der semantischen Sicherheit bietet
- Annahme: Wenn $\boldsymbol{A}$ eine Anfrage (m_1, m_0) an sein LoR-Orakel stellt, sei stets $m_1 \neq m_0$ (andere Anfragen sind für $\boldsymbol{A}$ nutzlos – könnte irgendetwas statt dessen fragen)

Sem-OTCPA und LoR-OTCPA (Forts.)

Sei (erfolgreicher) LoR-OTCPA-Angreifer $\boldsymbol{A}$ gegeben.
Wir konstruieren einen (erfolgreichen) Sem-OTCPA-Angreifer $\boldsymbol{B}$,
also einen Angreifer, der sich nicht gut simulieren lässt

- Wenn $\boldsymbol{A}$ eine Anfrage (m_1, m_0) an sein LoR-Orakel stellt, lass $\boldsymbol{B}$ in $\mathfrak{M}$ die Gleichverteilung auf $\{m_1, m_0\}$ beschreiben
- ... und lass $\boldsymbol{B}$ die Funktion $\mathfrak{f}$ so definieren, dass $\mathfrak{f}(m) = 1$ für $m = m_1$ und $\mathfrak{f}(m) = 0$ sonst
- ... und lass $\boldsymbol{B}$ als y das Ausgabebit von $\boldsymbol{A}$ übernehmen.
- $\mathfrak{f}(m) = 1$ ist für $\boldsymbol{A}$ eine „Linksverschlüsselung“, $\mathfrak{f}(m) = 0$ eine „Rechtsverschlüsselung“
- $\boldsymbol{B}$ beschreibt also genau den LoR-Angriff von $\boldsymbol{A}$:
  ...

Sem-OTCPA und LoR-OTCPA (Forts.)

- $\boldsymbol{B}$ beschreibt genau den LoR-Angriff von $\boldsymbol{A}$:

  $$\Pr_{(\mathfrak{f},y)\xleftarrow{\$}\boldsymbol{B}^{C(\cdot)}}\Big[\mathfrak{f}(m) = y\Big]$$

  ist also unser

  $$\Pr_{b\in_\$\{0,1\}}\big[\boldsymbol{A}^{E_b(\cdot,\cdot)} \Rightarrow b\big]$$

  von früher (Folie 2.11 zu LoR-OTCPA)

- Aus dieser Gleichheit folgt

  $$\Pr_{(\mathfrak{f},y)\xleftarrow{\$}\boldsymbol{B}^{C(\cdot)}}\big[\mathfrak{f}(m) = y\big] \;=\; \frac{1}{2}\cdot \mathrm{Adv}^{\text{LoR-OTCPA}}_{(\mathcal{K},\mathcal{E},\mathcal{D}),\boldsymbol{A}} + \frac{1}{2},$$

  denn (siehe Folie 2.11)

  $$\mathrm{Adv}^{\text{LoR-OTCPA}}_{(\mathcal{K},\mathcal{E},\mathcal{D}),\boldsymbol{A}} \;=\; 2\cdot \Pr_{b\in_\$\{0,1\}}\big[\boldsymbol{A}^{E_b(\cdot,\cdot)} \Rightarrow b\big] - 1$$

Sem-OTCPA und LoR-OTCPA (Forts.)

- Wir haben also
$$\Pr_{(\mathfrak{f},y)\xleftarrow{\$}\boldsymbol{B}^{C(\cdot)}}\left[\mathfrak{f}(m)=y\right]$$
bestimmt; für $\mathrm{Adv}^{\text{Sem-OTCPA}}_{(\mathcal{K},\mathcal{E},\mathcal{D}),\boldsymbol{A},\boldsymbol{S}}$ fehlt noch
$$\Pr_{(\mathfrak{f},y)\xleftarrow{\$}\boldsymbol{S}^{\overline{C}(\cdot)}}\left[\mathfrak{f}(m)=y\right]$$
- Für jeden gültigen Simulator $\boldsymbol{S}$ zu unserem $\boldsymbol{B}$ muss gelten
$$\Pr_{(\mathfrak{f},y)\xleftarrow{\$}\boldsymbol{S}^{\overline{C}(\cdot)}}\left[\mathfrak{f}(m)=y\right]=\frac{1}{2},$$
denn $\mathfrak{f}(m)$ ist hier (beim „nachgebauten“ LoR) gleichverteilt auf $\{0,1\}$ und $\boldsymbol{S}$ erhält keinerlei Hinweis darauf!

Sem-OTCPA und LoR-OTCPA (Forts.)

- Also
$$\begin{aligned}\mathrm{Adv}^{\text{Sem-OTCPA}}_{(\mathcal{K},\mathcal{E},\mathcal{D}),\boldsymbol{A},\boldsymbol{S}} &= \Pr_{(\mathfrak{f},y)\xleftarrow{\$}\boldsymbol{A}^{C(\cdot)}}\left[\mathfrak{f}(m)=y\right]-\Pr_{(\mathfrak{f},y)\xleftarrow{\$}\boldsymbol{S}^{\overline{C}(\cdot)}}\left[\mathfrak{f}(m)=y\right]\\ &= \frac{1}{2}\cdot\mathrm{Adv}^{\text{LoR-OTCPA}}_{(\mathcal{K},\mathcal{E},\mathcal{D}),\boldsymbol{A}}+\frac{1}{2}-\frac{1}{2}\\ &= \frac{1}{2}\cdot\mathrm{Adv}^{\text{LoR-OTCPA}}_{(\mathcal{K},\mathcal{E},\mathcal{D}),\boldsymbol{A}},\end{aligned}$$
und das für *jeden* gültigen Simulator $\boldsymbol{S}$ zu $\boldsymbol{B}$.

→ Ist $\boldsymbol{A}$ erfolgreich und das Verschlüsselungsschema *LoR-OTCPA-unsicher,* so ist $\mathrm{Adv}^{\text{Sem-OTCPA}}_{(\mathcal{K},\mathcal{E},\mathcal{D}),\boldsymbol{A},\boldsymbol{S}}$ *nicht verschwindend gering,* das Verschlüsselungsverfahren also auch *Sem-OTCPA-unsicher,* q.e.d.!

- Damit haben wir gezeigt (Kontraposition):
Sem-OTCPA-Sicherheit impliziert *LoR-OTCPA-Sicherheit.*

Sem-OTCPA und LoR-OTCPA (Forts.)

2. Ziel: *Sem-OTCPA-Unsicherheit impliziert LoR-OTCPA-Unsicherheit*

- Sei $(\mathcal{K}, \mathcal{E}, \mathcal{D})$ *nicht* sicher im Sinne von Sem-OTCPA,
  es gebe also einen Angreifer $\boldsymbol{A}$, zu dem der Vorteil $\mathrm{Adv}^{\text{Sem-OTCPA}}_{(\mathcal{K},\mathcal{E},\mathcal{D}),\boldsymbol{A},\boldsymbol{S}}$
  für *keinen* gültigen Simulator $\boldsymbol{S}$ verschwindend gering ist.

- Wir nehmen ein gegebenes $\boldsymbol{A}$ und geben dazu ein $\boldsymbol{S}$ an.
  Laut Voraussetzung ist der Vorteil zwangsläufig „groß“
  (genauer: nicht verschwindend gering), egal, wie wir $\boldsymbol{S}$ konstruieren,
  solange es nur ein gültiger Simulator zu $\boldsymbol{A}$ ist!

Sem-OTCPA und LoR-OTCPA (Forts.)

- Wir nehmen ein gegebenes $\boldsymbol{A}$ und geben dazu ein $\boldsymbol{S}$ an.
  Laut Voraussetzung ist der Vorteil zwangsläufig „groß“

- $\boldsymbol{S}$ baut auf $\boldsymbol{A}$ auf:

  lässt $\boldsymbol{A}$ dessen gewünschte Plaintextverteilung $\mathfrak{M}$ wählen;
  schickt $\mathfrak{M}$ an das eigene „Orakel“ $\overline{C}(\cdot)$ (das nie etwas antwortet);
  erzeugt *selbst* $K' \xleftarrow{\$} \mathcal{K}$ und $m_0 \xleftarrow{\$} \mathfrak{M}$;
  setzt $c \xleftarrow{\$} \mathcal{E}_{K'}(m_0)$ und gibt c als Orakelantwort an $\boldsymbol{A}$ zurück;
  übernimmt schließlich die Ausgabe $(\mathfrak{f}, y)$ von $\boldsymbol{A}$.

- Das ist ein gültiger Simulator!
  (Nämlich gleiche Verteilung von $\mathfrak{M}$ und $\mathfrak{f}$ wie $\boldsymbol{A}$.)

- Den Vorteil

$$\mathrm{Adv}^{\text{Sem-OTCPA}}_{(\mathcal{K},\mathcal{E},\mathcal{D}),\boldsymbol{A},\boldsymbol{S}} = \Pr_{(\mathfrak{f},y)\xleftarrow{\$}\boldsymbol{A}^{C(\cdot)}}\left[\mathfrak{f}(m) = y\right] - \Pr_{(\mathfrak{f},y)\xleftarrow{\$}\boldsymbol{S}^{\overline{C}(\cdot)}}\left[\mathfrak{f}(m) = y\right]$$

  können wir hier umdeuten: ...

Sem-OTCPA und LoR-OTCPA (Forts.)

- Den Vorteil

$$\mathrm{Adv}^{\text{Sem-OTCPA}}_{(\mathcal{K},\mathcal{E},\mathcal{D}),\boldsymbol{A},\boldsymbol{S}} = \Pr_{(\mathfrak{f},y)\xleftarrow{\$}\boldsymbol{A}^{C(\cdot)}}\Big[\mathfrak{f}(m)=y\Big] - \Pr_{(\mathfrak{f},y)\xleftarrow{\$}\boldsymbol{S}^{\overline{C}(\cdot)}}\Big[\mathfrak{f}(m)=y\Big]$$

  können wir hier umdeuten:
  Bau aus $\boldsymbol{A}$ einen LoR-OTCPA-Angreifer $\boldsymbol{B}$, der (m_1, m_0) beide gemäß $\mathfrak{M}$ wählt und der schließlich 1 ausgibt, falls $\mathfrak{f}(m_1) = y$ (und 0 sonst).

  Wahrscheinlichkeit, dass $\boldsymbol{B}$ im "Left"-Fall 1 ausgibt: $\Pr_{(\mathfrak{f},y)\xleftarrow{\$}\boldsymbol{A}^{C(\cdot)}}\Big[\mathfrak{f}(m)=y\Big]$

  Wahrscheinlichkeit, dass $\boldsymbol{B}$ im "Right"-Fall 1 ausgibt: $\Pr_{(\mathfrak{f},y)\xleftarrow{\$}\boldsymbol{S}^{\overline{C}(\cdot)}}\Big[\mathfrak{f}(m)=y\Big]$

  Also

$$\begin{aligned}\mathrm{Adv}^{\text{Sem-OTCPA}}_{(\mathcal{K},\mathcal{E},\mathcal{D}),\boldsymbol{A},\boldsymbol{S}} &= \Pr\left[\boldsymbol{B}^{E_1(\cdot,\cdot)}\Rightarrow 1\right] - \Pr\left[\boldsymbol{B}^{E_0(\cdot,\cdot)}\Rightarrow 1\right]\\ &= \mathrm{Adv}^{\text{LoR-OTCPA}}_{(\mathcal{K},\mathcal{E},\mathcal{D}),\boldsymbol{B}}\end{aligned}$$

Sem-OTCPA und LoR-OTCPA (Forts.)

- Wir haben erhalten: $\mathrm{Adv}^{\text{Sem-OTCPA}}_{(\mathcal{K},\mathcal{E},\mathcal{D}),\boldsymbol{A},\boldsymbol{S}} = \mathrm{Adv}^{\text{LoR-OTCPA}}_{(\mathcal{K},\mathcal{E},\mathcal{D}),\boldsymbol{B}}$
- Laut Voraussetzung (Verschlüsselungsschema ist *Sem-OTCPA-unsicher*) ist der Sem-OTCPA-Vorteil nicht verschwindend gering, also ist der LoR-OTCPA-Vorteil nicht verschwinden gering d.h., das Verschlüsselungsschema ist *LoR-OTCPA-unsicher;* q.e.d.!
- Damit haben wir gezeigt (Kontraposition): *LoR-OTCPA-Sicherheit* impliziert *Sem-OTCPA-Sicherheit.*

Semantische Sicherheit für Mehrfachverschlüsselung

- *Semantische Sicherheit* kann man ganz ähnlich auch für *Mehrfachverschlüsselung* definieren:

$$\mathrm{Adv}^{\text{Sem-CPA}}_{(\mathcal{K},\mathcal{E},\mathcal{D}),\boldsymbol{A},\boldsymbol{S}}$$

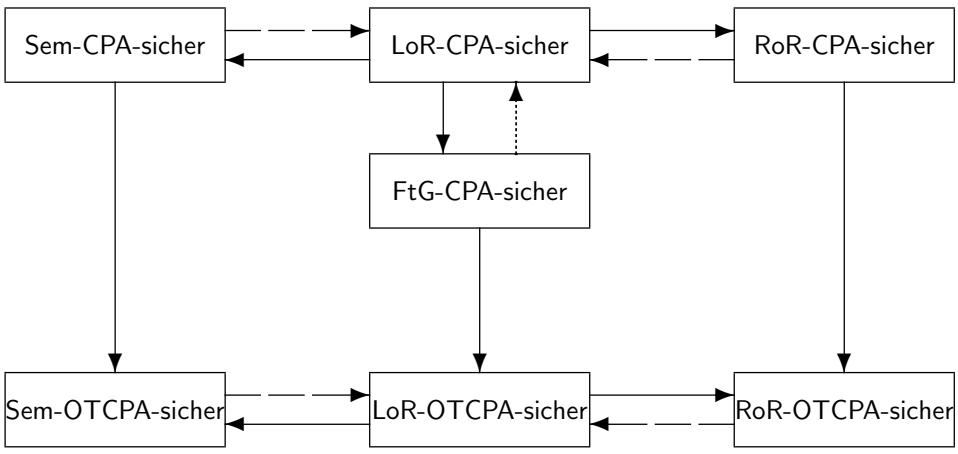
  „Sicher“, wenn es zu jedem $\boldsymbol{A}$ einen gültigen Simulator $\boldsymbol{S}$ gibt, für den dieser Vorteil verschwindend gering ist

- ... aber sehr viele Details in der formalen Darstellung (lassen wir hier aus)

- Ohne Beweis halten wir fest:
  Auch *Sem-CPA und LoR-CPA sind äquivalent* zueinander!

Sicherheitsbegriffe für symmetrische Verschlüsselung

Die Sicherheitsbegriffe mit *passivem Angreifer* im Überblick:



zu Aufgabe 2.5

Erster Schritt zur Lösung:

Blockchiffre E_K komplett ersetzen durch *gleichverteilt zufällige Abbildung* $f\colon \{0,1\}^\ell \to \{0,1\}^\ell$.

Welche *obere Schranke* für den *RoR-CPA-Vorteil beliebiger Angreifer* können wir dann angeben (abhängig von $q_\#$ und q_B)?