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 1.109 2007/07/20 13:14:15 bm Exp $

Rückblick auf die Vorlesung

Wesentliche Gebiete:

- *Konzepte und Techniken*
- *Sicherheitsbegriffe*
- *Konstruktionen*

Konzepte und Techniken

- Formalisierung der (Un-)Sicherheit: *Angriffsspiele, Vorteile*
- Der *Vorteil* eines Angreifers ist
  - ... *manchmal* eine *Erfolgswahrscheinlichkeit*
  - ... *oft* ein Maß dafür, wie gut er *zwischen zwei Szenarien unterscheiden* kann:

$$\begin{aligned}\mathrm{Adv}^{\text{Sicherheitsbegriff}}_{\ldots,\boldsymbol{A}} &= \Pr_{\text{Welt 1}}\left[\boldsymbol{A}^{\text{Orakel in Welt 1}} \Rightarrow 1\right] - \Pr_{\text{Welt 0}}\left[\boldsymbol{A}^{\text{Orakel in Welt 0}} \Rightarrow 1\right] \\ &= 2\Big(\Pr\left[A^{\text{Orakel in Welt } b} \Rightarrow b\right] - \frac{1}{2}\Big)\end{aligned}$$

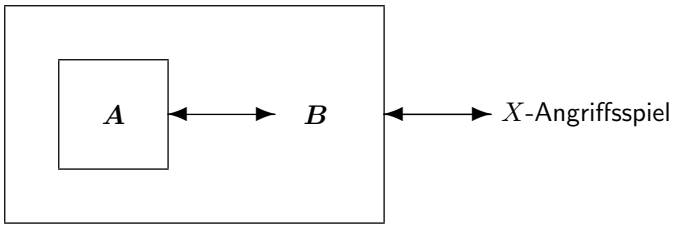
  Die zweite Zeile setzt voraus, dass

$$\Pr[\text{Welt 1}] = \Pr[\text{Welt 0}] = 1/2.$$

  [1.9 ff., 1.13]
- Beweise durch *Reduktion* [7.1 ff.]: ...

Konzepte und Techniken (Forts.)

- Beweise durch *Reduktion* [7.1 ff.]:
  - Informelle Aussage „S ist *X-sicher* $\Rightarrow$ T ist *Y-sicher*“
    (oft mehrere Voraussetzungen: S_1 ist X_1-sicher, S_2 ist X_2-sicher, ...)
  - *Beweisansatz*: Es gibt einen Y-Angreifer $\boldsymbol{A}$ auf T *mit Vorteil* $\mathrm{Adv}^{Y}_{T,\boldsymbol{A}}$
    $\Rightarrow$ Es gibt einen X-Angreifer $\boldsymbol{B}$ auf S *mit Vorteil* $\mathrm{Adv}^{X}_{S,\boldsymbol{B}}$
    ... und aus $\mathrm{Adv}^{Y}_{T,\boldsymbol{A}}$ ergibt sich eine *untere Schranke* für $\mathrm{Adv}^{X}_{S,\boldsymbol{B}}$:
    Es gibt ein sehr kleines ϵ und ein nicht allzu kleines α, so dass $\mathrm{Adv}^{X}_{S,\boldsymbol{B}} \geq \alpha \cdot \mathrm{Adv}^{Y}_{T,\boldsymbol{A}} - \epsilon$
  - Häufige *Beweistechnik*: Konstruiere $\boldsymbol{B}$ aus $\boldsymbol{A}$



Sicherheitsbegriffe

- *Pseudo-Random Function*, PRF [2.18; Aufgabenblatt 4; Lösungen zu Aufgabenblatt 7]
- *Pseudo-Random Permutation*, PRP, Blockchiffre
  [1.6 ff und 2.18; Lösungen zu Aufgabenblatt 3]
- *PRP/PRF Switching Lemma*, PRP als PRF [4.2–4.19]:
  $$\left|\mathrm{Adv}^{\mathrm{PRP}}_{E,\boldsymbol{A}} - \mathrm{Adv}^{\mathrm{PRF}}_{E,\boldsymbol{A}}\right| \leq \frac{q(q-1)}{2^{\ell+1}}$$
- *Pseudo-Random Generator*, PRG [2.19]
- *Message Authentication Code*, MAC [11.6 ff.]
- Sicherheitsbegriffe für *symmetrische Verschlüsselung*: ...

Sicherheitsbegriffe (Forts.)

- Sicherheitsbegriffe für *symmetrische Verschlüsselung*:
  - *Real-or-Random*, *Left-or-Right*, (*One-Time*) *Chosen Plaintext Attack*:

    RoR-OTCPA [2.7–2.10], LoR-OTCPA [2.11], RoR-CPA [2.22], LoR-CPA [2.23]
    [siehe auch Lösungen zu Aufgaben 1.1, 1.4, 1.5]

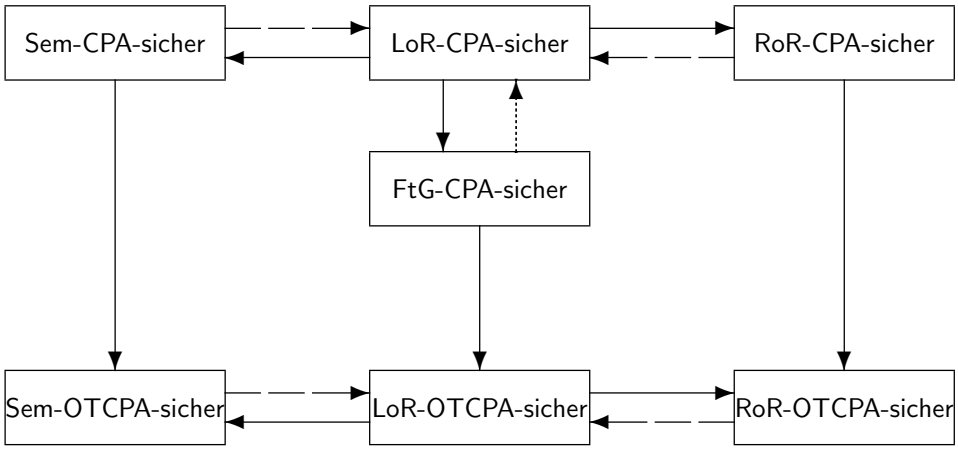
    Äquivalenzen RoR/LoR [2.12–2.17, 2.24, 10.7 ff.]
  - *Find-then-Guess*: FtG-CPA [5.3 ff.]

    Zusammenhänge LoR-CPA und FtG-CPA [5.7 ff.]
  - Aktive Angreifer: *Chosen Ciphertext Attack*;

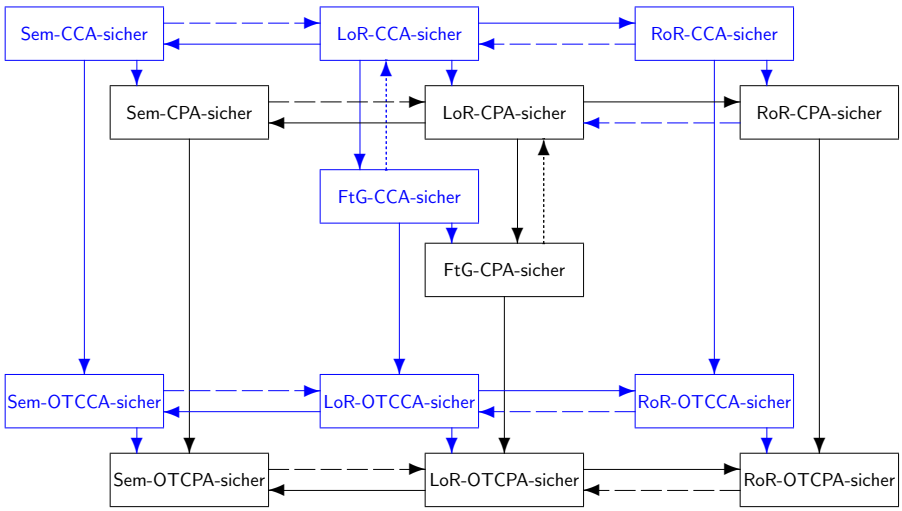
    "CCA"-Version von jedem "CPA"-Sicherheitsbegriff [9.1 ff.];
    $\cdots$ CCA-Sicherheit $\Rightarrow$ $\cdots$ CPA-Sicherheit
  - *Integrity of Ciphertexts*: INT-CTXT [10.22 f.];

    INT-CTXT-Sicherheit und (OT)CPA-Sicherheit zusammen
    $\Rightarrow$ (OT)CCA-Sicherheit [10.24 ff.]
  - *Semantische Sicherheit* (Sem-OTCPA, Sem-CPA) [6.1 ff.]:
    Für die Prüfung *keine Details*! Aber Zusammenhänge [6.19]: ...

Sicherheitsbegriffe (Forts.)

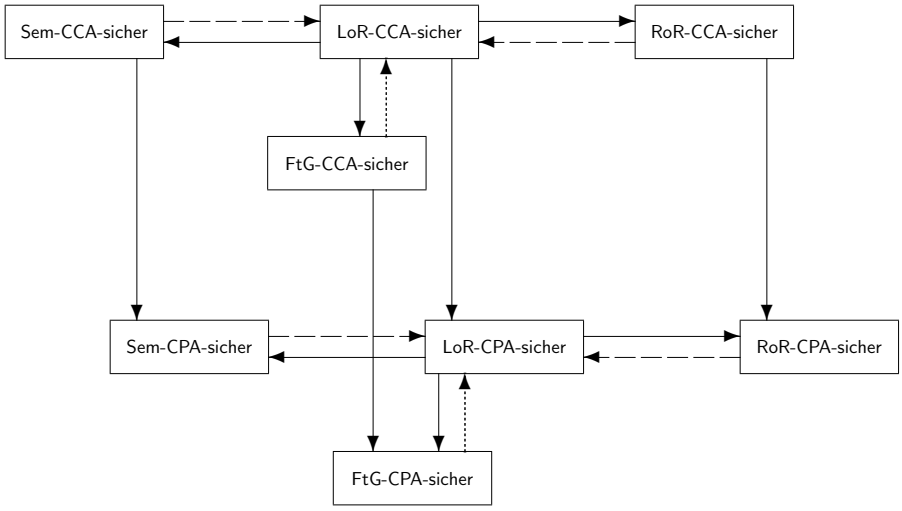


Sicherheitsbegriffe (Forts.)



Sicherheitsbegriffe (Forts.)

Analoge Sicherheitsbegriffe für *Public-Key-Verschlüsselung* [13.2 ff.]:



INT-CTXT-Sicherheit und Sicherheit als One-Time-Verschlüsselung sind hier nicht relevant!

Konstruktionen

- *Stream Cipher*: Verschlüsselungsschema aus PRG
  [2.19 f.; Lösungen zu Aufgaben 1.2, 1.3]
- *Counter Mode*, CTR Mode [Lösungen zu Aufgabenblatt 2, Aufgabenblatt 5]:
  - PRP/PRF Switching Lemma [4.2–4.19]
  - Konstruktion *PRG aus PRF* [3.3 ff.]
  - Verschlüsselungsschema aus PRG [4.20 f., 7.6 ff.]
- *Cipher Block Chaining*, CBC [8.1 ff., Aufgabenblatt 6]
- *PRF als MAC* [Lösung zu Aufgabenblatt 7]
- *Encrypt-then-MAC* [11.8 ff.]
- Public-Key-Verschlüsselung: *Hybride Verschlüsselung* [13.9 ff.]