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 1.107 2007/07/20 13:01:54 bm Exp $

Zu Aufgabenblatt 1

- Aufgaben 1.1 bis 1.5 behandeln die bis jetzt vorgestellten Sicherheitsbegriffe für Verschlüsselung:

  RoR-OTCPA LoR-OTCPA
  RoR-CPA LoR-CPA

- Lösung zu Aufgabe 1.1:
  http://www.crypto.rub.de/bewsich.html

- Aufgabe 1.2 behandelt einen Zusammenhang zwischen Verschlüsselung (Sicherheitsbegriff RoR-OTCPA) und Pseudo-Random Generator (PRG).
  Dort PRG als „Primitive“, Verschlüsselung als Konstruktion

Sicherheitsbegriffe bis jetzt

- RoR-OTCPA [2.8 f.], LoR-OTCPA [2.11], RoR-CPA [2.22], LoR-CPA [2.23] für *Verschlüsselungsschema* $(\mathcal{K}, \mathcal{E}, \mathcal{D})$
- *Pseudo-random permutation* (PRP, [1.6 ff., 2.18]) für Bijektionen $E_K \colon \{0,1\}^\ell \to \{0,1\}^\ell$ mit Schlüssel $K \in \mathcal{K}$ (entspricht Blockchiffre)
- *Pseudo-random function* (PRF, [2.18]) für (allgemeine) Abbildungen $E_K \colon \{0,1\}^\ell \to \{0,1\}^\ell$ mit Schlüssel $K \in \mathcal{K}$
- *Pseudo-random generator* (PRG, [2.19]):
  g_K erzeugt beliebig langen Bitstring zu Schlüssel $K \in \mathcal{K}$
  ($g_K(\ell')$ ist Präfix von $g_K(\ell)$ für $\ell' \leq \ell$)

Jeweils *Vorteil* durch Unterschied zweier Varianten eines Angriffsspiels definiert:

- oft: echtes oder ideales Orakel
- bei "LoR": Links- oder Rechtsverschlüsselungsorakel

Konstruktion eines PRG

- Aufgabe 1.2: Verwende PRG (pseudo-random generator) in Konstruktion für Einmal-Verschlüsselung
- *Jetzt:* Verwende PRF (pseudo-random function) in Konstruktion eines PRG
- Später: Verwende PRP (pseudo-random permutation) als PRF

Alles in allem: Einmal-Verschlüsselung aus einer PRP
(also aus einer Blockchiffre, z. B. AES)

Konstruktion eines PRG (Forts.)

Idee: Verwende einen λ-Bit-Zähler

$$\begin{aligned} p_0 &= 00...0000 \\ p_1 &= 00...0001 \\ p_2 &= 00...0010 \\ p_3 &= 00...0011 \\ p_4 &= 00...0100 \\ \ldots &= \ldots \end{aligned}$$

... und wende PRF $E_K \colon \{0,1\}^\lambda \to \{0,1\}^\lambda$ an:

$$\begin{aligned} c_0 &= E_K(p_0) \\ c_1 &= E_K(p_1) \\ c_2 &= E_K(p_2) \\ \ldots &= \ldots \end{aligned}$$

Konstruktion eines PRG (Forts.)

$g_K(\ell)$ sei ℓ-Bit-Präfix von

$$c_0 \parallel c_1 \parallel c_2 \parallel \ldots = E_K(00...0000) \parallel E_K(00...0001) \parallel E_K(00...0010) \parallel \ldots$$

Klar ist:
Für $\ell' \leq \ell$ ist $g_K(\ell')$ Präfix von $g_K(\ell)$ (wie gewünscht),
g erfüllt also die formale Anforderung für einen PRG.

Wie sieht es mit der Sicherheit aus?

Konstruktion eines PRG (Forts.)

Sicherheit des PRG wird bekanntlich quantifiziert durch möglichen PRG-Vorteil eines Angreifers $\boldsymbol{A}$:

$$\mathrm{Adv}^{\mathsf{PRG}}_{g,\boldsymbol{A}} \;=\; \Pr{}_{K\in_{\$}\mathcal{K}}\big[\boldsymbol{A}^{g_K(\cdot)} \Rightarrow 1\big] - \Pr{}_{S\in_{\$}\{0,1\}^L}\big[\boldsymbol{A}^{S(\cdot)} \Rightarrow 1\big]$$

(L als obere Schranke laut der erlaubten Laufzeit von $\boldsymbol{A}$.)

Beweisidee: Angriff auf PRG lässt sich „umbiegen“ in Angriff auf PRF!

Angreifer $\boldsymbol{B}$ auf PRF:

Sende nacheinander $p_0, p_1, p_2, \ldots$ (soweit benötigt) an Orakel E,
bilde aus den Antworten den Bitstring der von $\boldsymbol{A}$ gewünschten Länge.

Konstruktion eines PRG (Forts.)

Angreifer $\boldsymbol{B}$ auf PRF:

Sende nacheinander $p_0, p_1, p_2, \ldots$ (soweit benötigt) an Orakel E,
bilde aus den Antworten den Bitstring der von $\boldsymbol{A}$ gewünschten Länge.

Interaktion von $\boldsymbol{A}$ mit Orakel g_K ergibt Interaktion von $\boldsymbol{B}$ mit E_K.

Interaktion von $\boldsymbol{A}$ mit $S \in_{\$} \{0,1\}^L$ (idealer Fall) ergibt Interaktion von $\boldsymbol{B}$ mit $f \in_{\$} \mathrm{Func}(\{0,1\}^\lambda)$;
vorausgesetzt, $L \leq \lambda \cdot 2^\lambda$.

Also

$$\mathrm{Adv}^{\mathsf{PRG}}_{g,\boldsymbol{A}} = \mathrm{Adv}^{\mathsf{PRF}}_{E,\boldsymbol{B}}$$

unter der Voraussetzung, dass L genügend klein bleibt.

($\rightarrow$ Beschränkung der Laufzeit von $\boldsymbol{A}$!)

Das heißt, g ist sicher als PRG, wenn E_K sicher ist als PRF.