# 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 1.26 2007/04/25 17:50:36 bm Exp $



## Überblick

- *PRP* (Pseudo-Random Permutation) *als PRF* (Pseudo-Random Function)
- ... und sichere *Einmalverschlüsselung* damit (RoR-OTCPA, LoR-OTCPA)
- ... und sichere Verschlüsselung auch für Mehrfachnutzung (*RoR-CPA*, *LoR-CPA*)!

# PRP als PRF

Warum *Pseudo-Random Permutation* als *Pseudo-Random Function* einsetzen?

- Wir haben effiziente Blockchiffren wie AES.
  Die Blockverschlüsselung liefert Permutationen $E_K\colon \{0,1\}^\ell \to \{0,1\}^\ell$,
  die sich bei unbekanntem Schlüssel „wie zufällig“ verhalten sollen
  $\to$ PRP als Primitive verfügbar (PRP-Sicherheit wird ohne Beweis vermutet)

- Oft nützlich ist aber ein PRF:
  siehe die Konstruktion eines PRG aus einer PRF letzte Woche,
  Verschlüsselung aus einem PRG in Aufgabe 1.2

- PRF ist sehr ähnlich wie PRP:
  allgemeine Funktion $\{0,1\}^\ell \to \{0,1\}^\ell$
  statt Bijektion $\{0,1\}^\ell \to \{0,1\}^\ell$



# PRP als PRF (Forts.)

- Um die *Sicherheit von PRP und PRF* zu „messen“,
  hatten wir folgende *Vorteile* verwendet:

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

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

  $\mathrm{Func}(\{0,1\}^\ell)$ ist die Menge aller Abbildungen $\{0,1\}^\ell \to \{0,1\}^\ell$,
  $\mathrm{Perm}(\{0,1\}^\ell) \subseteq \mathrm{Func}(\{0,1\}^\ell)$ sind die Bijektionen.

  Schreiben wir kürzer

$$\begin{aligned}
\Pr{}_K[\ldots] \quad &\text{für} \quad \Pr{}_{K\in_\$\mathcal{K}}[\ldots],\\
\Pr{}_\pi[\ldots] \quad &\text{für} \quad \Pr{}_{\pi\in_\$\mathrm{Perm}(\{0,1\}^\ell)}[\ldots],\\
\Pr{}_f[\ldots] \quad &\text{für} \quad \Pr{}_{f\in_\$\mathrm{Func}(\{0,1\}^\ell)}[\ldots].
\end{aligned}$$

## PRP als PRF (Forts.)

- Wir gehen von PRP-Sicherheit aus und wollen PRF-Sicherheit zeigen ...
- ... also beweisen: Gibt es einen erfolgreichen PRF-Angreifer, so haben wir damit auch einen erfolgreichen PRP-Angreifer.
- Diesmal müssen wir den Angreifer nicht speziell konstruieren, sondern setzen den PRF-Angreifer $\boldsymbol{A}$ direkt als PRP-Angreifer ein!
- Auf Gleichheit $\mathrm{Adv}^{\mathsf{PRP}}_{E,\boldsymbol{A}} = \mathrm{Adv}^{\mathsf{PRF}}_{E,\boldsymbol{A}}$ können wir i. a. nicht hoffen. Unser Ziel: Zeigen, dass $\left|\mathrm{Adv}^{\mathsf{PRP}}_{E,\boldsymbol{A}} - \mathrm{Adv}^{\mathsf{PRF}}_{E,\boldsymbol{A}}\right|$ klein sein muss!



## PRP als PRF (Forts.)

- Unser Ziel: Zeigen, dass $\left|\mathrm{Adv}^{\mathsf{PRP}}_{E,\boldsymbol{A}} - \mathrm{Adv}^{\mathsf{PRF}}_{E,\boldsymbol{A}}\right|$ klein sein muss!
- Es ist

$$\begin{aligned}\mathrm{Adv}^{\mathsf{PRP}}_{E,\boldsymbol{A}} - \mathrm{Adv}^{\mathsf{PRF}}_{E,\boldsymbol{A}} &= \Big(\Pr_K\big[\boldsymbol{A}^{E_K(\cdot)} \Rightarrow 1\big] - \Pr_\pi\big[\boldsymbol{A}^{\pi(\cdot)} \Rightarrow 1\big]\Big) \\ &\quad - \Big(\Pr_K\big[\boldsymbol{A}^{E_K(\cdot)} \Rightarrow 1\big] - \Pr_f\big[\boldsymbol{A}^{f(\cdot)} \Rightarrow 1\big]\Big) \\ &= \Pr_f\big[\boldsymbol{A}^{f(\cdot)} \Rightarrow 1\big] - \Pr_\pi\big[\boldsymbol{A}^{\pi(\cdot)} \Rightarrow 1\big],\end{aligned}$$

  also bleibt nur zu zeigen, dass

$$\left|\Pr_f\big[\boldsymbol{A}^{f(\cdot)} \Rightarrow 1\big] - \Pr_\pi\big[\boldsymbol{A}^{\pi(\cdot)} \Rightarrow 1\big]\right|$$

  klein ist.
- Um welches konkrete $E_K$ es geht, ist hier also egal!

## PRP als PRF (Forts.)

- Unsere Aufgabe lautet also: Untersuche

$$\left|\Pr_{f\in_{\$}\mathrm{Func}(\{0,1\}^\ell)}\left[\boldsymbol{A}^{f(\cdot)}\Rightarrow 1\right]-\Pr_{\pi\in_{\$}\mathrm{Perm}(\{0,1\}^\ell)}\left[\boldsymbol{A}^{\pi(\cdot)}\Rightarrow 1\right]\right|$$

- Auch das können wir als „Vorteil“ auffassen:
  Wie gut kann $\boldsymbol{A}$ zufällige Abbildungen $\{0,1\}^\ell \to \{0,1\}^\ell$
  von zufälligen Bijektionen $\{0,1\}^\ell \to \{0,1\}^\ell$ unterscheiden?

- Idee, damit $\boldsymbol{A}$ hier einen Erfolg erzielen kann:
  Einen Unterschied von allgemeinen Abbildungen gegenüber
  Bijektionen gibt es nur bei $x \neq y$ mit $f(x) = f(y)$

- Weil gleichverteilt *alle* Abbildungen bzw. Bijektionen betrachtet werden,
  sind keine bestimmten $x, y$ von vornherein besser als andere



## PRP als PRF (Forts.)

- Um allgemein Abbildungen und Bijektionen zu unterscheiden, kann $\boldsymbol{A}^{E(\cdot)}$
  verschiedene Werte durchprobieren und etwa folgendes abfragen:

$$\begin{gathered}E(00\ldots0000),\\ E(00\ldots0001),\\ E(00\ldots0010),\\ E(00\ldots0011),\\ E(00\ldots0100),\\ E(00\ldots0101),\\ \ldots\end{gathered}$$

  Gibt es irgendwann eine *Kollision* (nämlich $x \neq y$ mit $E(x) = E(y)$),
  so liegt keine Bijektion vor; andernfalls könnte es beides sein (Bijektion,
  allgemeine Abbildung).

- Erst nach Abfragen *aller* Werte $E(x)$, $x \in \{0,1\}^\ell$ könnte $\boldsymbol{A}^{E(\cdot)}$
  Bijektionen und allgemeine Abbildungen völlig zuverlässig unterscheiden.
  Aber das benötigt $2^\ell$ Orakel-Anfragen (nur bei sehr kleinem $\ell$ realistisch).

## PRP als PRF (Forts.)

- Um $\left|\Pr_f\left[\boldsymbol{A}^{f(\cdot)} \Rightarrow 1\right] - \Pr_\pi\left[\boldsymbol{A}^{\pi(\cdot)} \Rightarrow 1\right]\right|$ abzuschätzen, müssen wir also die Anzahl $q$ der Anfragen an das Orakel berücksichtigen.
- Von der Beschränkung durch $q$ abgesehen lassen wir hier beliebiges $\boldsymbol{A}$ zu (sonst keine Ressourcenbeschränkung!)
- Bis jetzt haben wir getrennte Wahrscheinlichkeitsräume: einerseits $\Pr_{f \in_\$ \mathrm{Func}(\{0,1\}^\ell)[\ldots]}$, andererseits $\Pr_{\pi \in_\$ \mathrm{Perm}(\{0,1\}^\ell)[\ldots]}$
- Wir wollen eine gemeinsame Darstellung finden: zwei Varianten *eines* Spiels mit klarem Zusammenhang
- Also konstruiere Orakel $E_{\mathrm{Func}}(\cdot)$ und $E_{\mathrm{Perm}}(\cdot)$, die sich verhalten wie oben, und betrachte dann $\left|\Pr\left[\boldsymbol{A}^{E_{\mathrm{Func}}(\cdot)} \Rightarrow 1\right] - \Pr\left[\boldsymbol{A}^{E_{\mathrm{Perm}}(\cdot)} \Rightarrow 1\right]\right|$



## PRP als PRF (Forts.)

Zuerst $E_{\mathrm{Func}}(\cdot)$:

**Initialisierung**

Für jedes $x \in \{0,1\}^\ell$:
$F[x] \leftarrow \perp$

**Orakelfunktionalität:** Wenn $\boldsymbol{A}$ eine Frage $x$ sendet ...

Falls $F[x] = \perp$, dann
$c \xleftarrow{\$} \{0,1\}^\ell$
$F[x] \leftarrow c$
Gib $F[x]$ zurück als Orakelantwort

Für $\boldsymbol{A}$ kein Unterschied zwischen $\boldsymbol{A}^{E_{\mathrm{Func}}(\cdot)}$ und $\boldsymbol{A}^{f(\cdot)}, f \in_\$ \mathrm{Func}(\{0,1\}^\ell)$!

## PRP als PRF (Forts.)

Dann $E_{\mathrm{Perm}}(\cdot)$:

**Initialisierung**

Für jedes $x \in \{0,1\}^\ell$:
$F[x] \leftarrow \perp$

**Orakelfunktionalität:** Wenn $\boldsymbol{A}$ eine Frage $x$ sendet ...

Falls $F[x] = \perp$, dann
$c \xleftarrow{\$} \{0,1\}^\ell \setminus \bigcup_{x \in \{0,1\}^\ell} \{F[x]\}$
$F[x] \leftarrow c$
Gib $F[x]$ zurück als Orakelantwort

Für $\boldsymbol{A}$ kein Unterschied zwischen $\boldsymbol{A}^{E_{\mathrm{Perm}}(\cdot)}$ und $\boldsymbol{A}^{\pi(\cdot)}, \pi \in_{\$} \mathrm{Perm}(\{0,1\}^\ell)$!



## PRP als PRF (Forts.)

$E_{\mathrm{Perm}}(\cdot)$ sieht so aber noch recht anders aus als $E_{\mathrm{Func}}(\cdot)$.

Wir können $E_{\mathrm{Perm}}(\cdot)$ auch so beschreiben:

**Initialisierung**

Für jedes $x \in \{0,1\}^\ell$:
$F[x] \leftarrow \perp$

**Orakelfunktionalität:** Wenn $\boldsymbol{A}$ eine Frage $x$ sendet ...

Falls $F[x] = \perp$, dann
$c \xleftarrow{\$} \{0,1\}^\ell$
Falls $c \in \bigcup_{x \in \{0,1\}^\ell} \{F[x]\}$, dann
$c \xleftarrow{\$} \{0,1\}^\ell \setminus \bigcup_{x \in \{0,1\}^\ell} \{F[x]\}$
$F[x] \leftarrow c$
Gib $F[x]$ zurück als Orakelantwort

Jetzt stimmt der innere Ablauf von $E_{\mathrm{Func}}(\cdot)$ und $E_{\mathrm{Perm}}(\cdot)$ weitergehend überein.

Noch eine Änderung, um den Unterschied „messen“ zu können ...

## PRP als PRF (Forts.)

Wir führen ein Flag $bad$ ein, das bei der Abweichung gesetzt wird.

Neue Beschreibung für $E_{\mathrm{Perm}}(\cdot)$:

**Initialisierung**

Für jedes $x \in \{0,1\}^\ell$:
$F[x] \leftarrow \perp$
$bad \leftarrow$ false

**Orakelfunktionalität:** Wenn $\boldsymbol{A}$ eine Frage $x$ sendet ...

Falls $F[x] = \perp$, dann
$c \xleftarrow{\$} \{0,1\}^\ell$
Falls $c \in \bigcup_{x \in \{0,1\}^\ell} \{F[x]\}$, dann
$bad \leftarrow$ true
$c \xleftarrow{\$} \{0,1\}^\ell \setminus \bigcup_{x \in \{0,1\}^\ell} \{F[x]\}$
$F[x] \leftarrow c$
Gib $F[x]$ zurück als Orakelantwort



## PRP als PRF (Forts.)

*Gemeinsame* Beschreibung für $E_{\mathrm{Func}}(\cdot)$ und $E_{\mathrm{Perm}}(\cdot)$:

**Initialisierung**

Für jedes $x \in \{0,1\}^\ell$:
$F[x] \leftarrow \perp$
$bad \leftarrow$ false

**Orakelfunktionalität:** Wenn $\boldsymbol{A}$ eine Frage $x$ sendet ...

Falls $F[x] = \perp$, dann
$c \xleftarrow{\$} \{0,1\}^\ell$
Falls $c \in \bigcup_{x \in \{0,1\}^\ell} \{F[x]\}$, dann
$bad \leftarrow$ true
Im Fall von $E_{\mathrm{Perm}}(\cdot)$:
$c \xleftarrow{\$} \{0,1\}^\ell \setminus \bigcup_{x \in \{0,1\}^\ell} \{F[x]\}$
$F[x] \leftarrow c$
Gib $F[x]$ zurück als Orakelantwort

Verhaltensunterschied zwischen $E_{\mathrm{Func}}(\cdot)$ und $E_{\mathrm{Perm}}(\cdot)$ nur möglich, wenn $bad$ gesetzt wird!

## PRP als PRF (Forts.)

Verhaltensunterschied zwischen $E_{\mathrm{Func}}(\cdot)$ und $E_{\mathrm{Perm}}(\cdot)$ nur möglich, wenn $bad$ gesetzt wird!

Sei "Bad" das Ereignis, das im Spielablauf irgendwann $bad \leftarrow$ true gesetzt wird.

Also:

$$\Pr\left[\overline{\mathsf{Bad}} \wedge \left(\boldsymbol{A}^{E_{\mathrm{Func}}(\cdot)} \Rightarrow 1\right)\right] = \Pr\left[\overline{\mathsf{Bad}} \wedge \left(\boldsymbol{A}^{E_{\mathrm{Perm}}(\cdot)} \Rightarrow 1\right)\right]$$

Wir interessieren uns für

$$\left|\Pr\left[\boldsymbol{A}^{E_{\mathrm{Func}}(\cdot)} \Rightarrow 1\right] - \Pr\left[\boldsymbol{A}^{E_{\mathrm{Perm}}(\cdot)} \Rightarrow 1\right]\right|,$$

also zerlegen wir die Ereignisse passend ...:



## PRP als PRF (Forts.)

Bekannt: $\Pr\left[\overline{\mathsf{Bad}} \wedge (\boldsymbol{A}^{E_{\mathrm{Func}}(\cdot)} \Rightarrow 1)\right] = \Pr\left[\overline{\mathsf{Bad}} \wedge (\boldsymbol{A}^{E_{\mathrm{Perm}}(\cdot)} \Rightarrow 1)\right]$

Zu untersuchen: $\left|\Pr\left[\boldsymbol{A}^{E_{\mathrm{Func}}(\cdot)} \Rightarrow 1\right] - \Pr\left[\boldsymbol{A}^{E_{\mathrm{Perm}}(\cdot)} \Rightarrow 1\right]\right|$

$$\begin{aligned}
&\Pr\left[\boldsymbol{A}^{E_{\mathrm{Func}}(\cdot)} \Rightarrow 1\right] - \Pr\left[\boldsymbol{A}^{E_{\mathrm{Perm}}(\cdot)} \Rightarrow 1\right] \\
&\quad = \Pr\left[\mathsf{Bad} \wedge \left(\boldsymbol{A}^{E_{\mathrm{Func}}(\cdot)} \Rightarrow 1\right)\right] + \Pr\left[\overline{\mathsf{Bad}} \wedge \left(\boldsymbol{A}^{E_{\mathrm{Func}}(\cdot)} \Rightarrow 1\right)\right] \\
&\qquad - \Pr\left[\mathsf{Bad} \wedge \left(\boldsymbol{A}^{E_{\mathrm{Perm}}(\cdot)} \Rightarrow 1\right)\right] - \Pr\left[\overline{\mathsf{Bad}} \wedge \left(\boldsymbol{A}^{E_{\mathrm{Perm}}(\cdot)} \Rightarrow 1\right)\right] \\
&\quad = \Pr\left[\mathsf{Bad} \wedge \left(\boldsymbol{A}^{E_{\mathrm{Func}}(\cdot)} \Rightarrow 1\right)\right] - \Pr\left[\mathsf{Bad} \wedge \left(\boldsymbol{A}^{E_{\mathrm{Perm}}(\cdot)} \Rightarrow 1\right)\right] \\
&\quad \leq \Pr\left[\mathsf{Bad} \wedge \left(\boldsymbol{A}^{E_{\mathrm{Func}}(\cdot)} \Rightarrow 1\right)\right] \\
&\quad \leq \Pr\left[\mathsf{Bad}\right]
\end{aligned}$$

## PRP als PRF (Forts.)

Völlig analog zu

$$\Pr\left[\boldsymbol{A}^{E_{\mathrm{Func}}(\cdot)} \Rightarrow 1\right] - \Pr\left[\boldsymbol{A}^{E_{\mathrm{Perm}}(\cdot)} \Rightarrow 1\right] \leq \Pr\left[\mathsf{Bad}\right]$$

lässt sich auch zeigen

$$\Pr\left[\boldsymbol{A}^{E_{\mathrm{Perm}}(\cdot)} \Rightarrow 1\right] - \Pr\left[\boldsymbol{A}^{E_{\mathrm{Func}}(\cdot)} \Rightarrow 1\right] \leq \Pr\left[\mathsf{Bad}\right],$$

also insgesamt

$$\left|\Pr\left[\boldsymbol{A}^{E_{\mathrm{Func}}(\cdot)} \Rightarrow 1\right] - \Pr\left[\boldsymbol{A}^{E_{\mathrm{Perm}}(\cdot)} \Rightarrow 1\right]\right| \leq \Pr\left[\mathsf{Bad}\right].$$

Es bleibt, $\Pr\left[\mathsf{Bad}\right]$ nach oben abzuschätzen.



## PRP als PRF (Forts.)

$\Pr\left[\mathsf{Bad}\right]$ ist die Wahrscheinlichkeit, dass hier jemals $bad \leftarrow$ true gesetzt wird:

**Initialisierung**

Für jedes $x \in \{0,1\}^\ell$:
  $F[x] \leftarrow \perp$
$bad \leftarrow$ false

**Orakelfunktionalität:** Wenn $\boldsymbol{A}$ eine Frage $x$ sendet ...

Falls $F[x] = \perp$, dann
  $c \xleftarrow{\$} \{0,1\}^\ell$
    Falls $c \in \bigcup_{x \in \{0,1\}^\ell} \{F[x]\}$, dann
      $bad \leftarrow$ true
      ...
  $F[x] \leftarrow c$
Gib $F[x]$ zurück als Orakelantwort

Ganz klar abhängig von $q$, der (maximalen) Anzahl der Aufrufe des Orakels durch $\boldsymbol{A}$ ...

## PRP als PRF (Forts.)

$$
\begin{aligned}
q = 0 \quad &\Rightarrow \quad \Pr[\mathsf{Bad}] = 0 \\
q = 1 \quad &\Rightarrow \quad \Pr[\mathsf{Bad}] = 0 \\
q = 2 \quad &\Rightarrow \quad \Pr[\mathsf{Bad}] \leq \frac{1}{2^\ell} \\
q = 3 \quad &\Rightarrow \quad \Pr[\mathsf{Bad}] \leq \frac{1}{2^\ell} + \frac{2}{2^\ell} \\
q = 4 \quad &\Rightarrow \quad \Pr[\mathsf{Bad}] \leq \frac{1}{2^\ell} + \frac{2}{2^\ell} + \frac{3}{2^\ell} \\
\ldots \quad &\qquad \ldots
\end{aligned}
$$

und allgemein

$$\Pr[\mathsf{Bad}] \;\leq\; \frac{1}{2^\ell} + \frac{2}{2^\ell} + \ldots + \frac{q-1}{2^\ell} \;=\; \frac{q(q-1)}{2^{\ell+1}}$$



## PRP als PRF (Forts.)

Es folgt also

$$\left|\Pr\left[\boldsymbol{A}^{E_{\mathrm{Func}}(\cdot)} \Rightarrow 1\right] - \Pr\left[\boldsymbol{A}^{E_{\mathrm{Perm}}(\cdot)} \Rightarrow 1\right]\right| \leq \frac{q(q-1)}{2^{\ell+1}}$$

und damit

$$\left|\mathrm{Adv}^{\mathsf{PRP}}_{E,\boldsymbol{A}} - \mathrm{Adv}^{\mathsf{PRF}}_{E,\boldsymbol{A}}\right| \leq \frac{q(q-1)}{2^{\ell+1}}.$$

Das ist das sogenannte *PRP/PRF Switching Lemma*.

Es besagt: Solange $q$ genügend klein bleibt, sind PRP-Sicherheit und PRF-Sicherheit ungefähr das gleiche.

(Spätestens um $q \approx 2^{\ell/2}$ herum wird es völlig nutzlos!
Dort sagt es nur noch $\left|\mathrm{Adv}^{\mathsf{PRP}}_{E,\boldsymbol{A}} - \mathrm{Adv}^{\mathsf{PRF}}_{E,\boldsymbol{A}}\right| \leq \frac{1}{2}$.)

## Einmalverschlüsselung mit dem Counter Mode

- Wir haben gerade gesehen: Ein PRP (z. B. eine Blockchiffre) ist auch ein PRF.
- Letzte Woche: Aus einem PRF können wir einen PRG konstruieren – verwende Präfixe von $E_K(00\ldots0000) \parallel E_K(00\ldots0001) \parallel E_K(00\ldots0010) \parallel \ldots$
- In Aufgabe 1.2: Mit einem PRG können wir verschlüsseln (sicher für Einmalverschlüsselung – RoR-OTCPA, LoR-OTCPA) durch XOR mit PRG-Wert der passenden Länge
- Das so von einer Blockchiffre abgeleitete Verschlüsselungsschema nennt sich *Counter Mode,* oft auch abgekürzt *CTR Mode.*
- Quantitative Sicherheit: *RoR-OTCPA-Vorteil* bei Verschlüsselung von bis zu $q \cdot \ell$ Bits? → Übungsaufgabe 2.4!



## Mehrfachverschlüsselung mit dem Counter Mode

- XOR mit einem Präfix von
$$E_K(00\ldots0000) \parallel E_K(00\ldots0001) \parallel E_K(00\ldots0010) \parallel \ldots$$
ist sicher für Einmalverschlüsselung (RoR-OTCPA, LoR-OTCPA).
- Sicherheit für *mehrfache* Verschlüsselung (RoR-CPA, LoR-CPA) ist leicht herzustellen!
- Nehmen wir an, $\ell$ ist gerade. Ist $iv \in \{0,1\}^{\ell/2}$, können wir XOR mit einem Präfix von
$$E_K(iv \parallel 00\ldots0000) \parallel E_K(iv \parallel 00\ldots0001) \parallel E_K(iv \parallel 00\ldots0010)$$
verwenden ($\ell/2$ Bits für $iv$, die verbleibenden $\ell/2$ Bits für den Zähler).
- Wählen wir $iv \in_\$ \{0,1\}^{\ell/2}$ *stets neu* im Verschlüsselungsalgorithmus (als *Initialization Vector*), so haben wir ein Verschlüsselungsschema für Mehrfachverschlüsselung!
- Beschreibung des Verschlüsselungsschemas: → Aufgabe 2.3
- Sicherheit quantitativ? → Aufgabe 2.5