# 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 1.46 2007/05/16 17:59:22 bm Exp $



## Rückblick: Sicherheitsbeweise durch Reduktion

- Es geht uns um Aussagen der Form

  „$S$ ist *$X$-sicher* $\Rightarrow$ $T$ ist *$Y$-sicher*“

- *Konstruktiv* zeigen lässt sich nicht Sicherheit, sondern *Unsicherheit*

- Beweisrichtung deshalb umgekehrt (*Kontraposition*),
  denn $A \Rightarrow B$ ist gleichbedeutend mit $\overline{B} \Rightarrow \overline{A}$:

  „$T$ ist *nicht $Y$-sicher* $\Rightarrow$ $S$ ist *nicht $X$-sicher*“

- Genauer quantitativ (mit *Vorteil* als Maß für Unsicherheit):

  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* $\mathrm{Adv}^{X}_{S,\boldsymbol{B}}$,
  wobei $\mathrm{Adv}^{X}_{S,\boldsymbol{B}} \geq \alpha \cdot \mathrm{Adv}^{Y}_{T,\boldsymbol{A}} - \epsilon$

  Hier kann $\alpha < 1$ sein, aber nicht zu klein; $\epsilon$ soll verschwindend gering bleiben

## Rückblick: Sicherheitsbeweise durch Reduktion (Forts.)

- 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 $\mathrm{Adv}^X_{S,\boldsymbol{B}} \geq \alpha \cdot \mathrm{Adv}^Y_{T,\boldsymbol{A}} - \epsilon$
  $\alpha$ nicht zu klein, $\epsilon$ verschwindend gering

- Das Problem, $X$ im $S$-Angriffsspiel anzugreifen, wird *„reduziert“*
  auf das Problem, $Y$ im $T$-Angriffsspiel anzugreifen

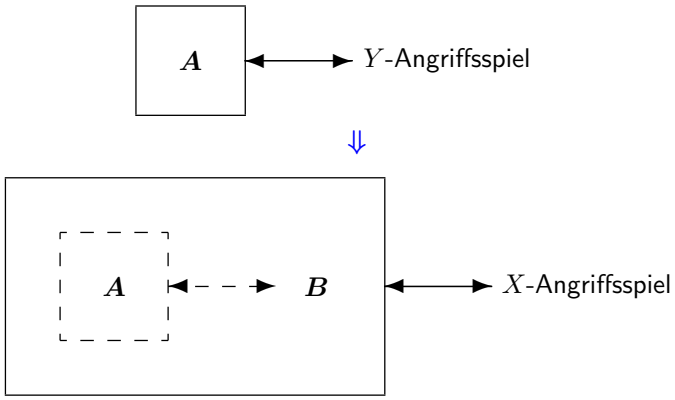
- Die Ungleichung
  $$\mathrm{Adv}^X_{S,\boldsymbol{B}} \geq \alpha \cdot \mathrm{Adv}^Y_{T,\boldsymbol{A}} - \epsilon$$
  entspricht wieder der *ursprünglichen Reihenfolge*
  $$\text{„}S \text{ ist } X\text{-sicher } \Rightarrow\ T \text{ ist } Y\text{-sicher“}$$
  (Ist nämlich laut Sicherheitsannahme $\mathrm{Adv}^X_{S,\boldsymbol{B}}$ klein,
  so ist laut Ungleichung auch $\mathrm{Adv}^Y_{T,\boldsymbol{A}} \leq \frac{1}{\alpha} \cdot \left(\mathrm{Adv}^X_{S,\boldsymbol{B}} + \epsilon\right)$ klein,
  wenn $\frac{1}{a}$ und $\epsilon$ im Rahmen bleiben)



## Rückblick: Sicherheitsbeweise durch Reduktion (Forts.)

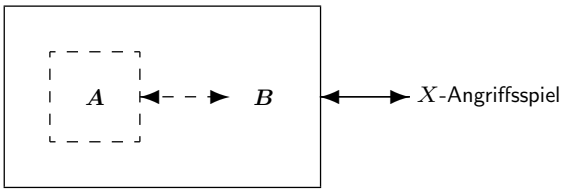
- Es gibt einen $Y$-Angreifer $\boldsymbol{A}$ auf $T$ mit Vorteil $\mathrm{Adv}^Y_{T,\boldsymbol{A}}$
  $\Rightarrow$ Es gibt einen $X$-Angreifer $\boldsymbol{B}$ auf $S$ mit Vorteil $\mathrm{Adv}^X_{S,\boldsymbol{B}} \geq \alpha \cdot \mathrm{Adv}^Y_{T,\boldsymbol{A}} - \epsilon$
  $\alpha$ nicht zu klein, $\epsilon$ verschwindend gering

- Häufige *Beweistechnik:* Konstruiere $\boldsymbol{B}$ aus $\boldsymbol{A}$



## Rückblick: Sicherheitsbeweise durch Reduktion (Forts.)

- Häufige *Beweistechnik:* Konstruiere $\boldsymbol{B}$ aus $\boldsymbol{A}$




- Wir erlauben *jeden denkbaren $Y$-Angreifer* $\boldsymbol{A}$ auf $T$ („gut“ oder „schlecht“), ohne konkret festzulegen, wie $\boldsymbol{A}$ vorgehen sollte!

  Denn wir wollen *beweisbare Sicherheit* – wir wollen nicht darauf angewiesen sein, dass uns alle denkbaren Angriffe einfallen

- $\boldsymbol{B}$ verwendet $\boldsymbol{A}$ als *“black box”:* stellt für $\boldsymbol{A}$ irgendwie ein $Y$-Angriffsspiel dar (wie $\boldsymbol{A}$ es in seiner „natürlichen Umgebung“ erwartet), agiert dabei selbst im $X$-Angriffsspiel;

  wir suchen einen Zusammenhang $\mathrm{Adv}^X_{S,\boldsymbol{B}} \geq \alpha \cdot \mathrm{Adv}^Y_{T,\boldsymbol{A}} - \epsilon$



## Rückblick: Sicherheitsbeweise durch Reduktion (Forts.)

- Mit Reduktionsbeweisen nach diesem Schema konnten wir vieles beweisen, z. B.
  - „$(\mathcal{K}, \mathcal{E}, \mathcal{D})$ ist LoR-CPA-sicher $\Rightarrow$ $(\mathcal{K}, \mathcal{E}, \mathcal{D})$ ist RoR-OTCPA-sicher“
  - „$(\mathcal{K}, \mathcal{E}, \mathcal{D})$ ist RoR-CPA-sicher $\Rightarrow$ $(\mathcal{K}, \mathcal{E}, \mathcal{D})$ ist LoR-CPA-sicher“
  - „$g$ ist PRG-sicher $\Rightarrow$ XOR-Verschlüsselung mit $g$ RoR-OTCPA-sicher“

  und anderes!

- Oft brauchen wir andere Varianten dieses Ansatzes ...

## Sicherheitsbeweis für den Counter Mode

**Aufgabe 2.5** Machen Sie eine Aussage über die Sicherheit der Counter-Mode-Verschlüsselung (Aufgabe 2.3) für Mehrfachverschlüsselung, ausgehend von der PRP-Sicherheit der verwendeten Blockchiffre!

Gesucht ist eine Ungleichung zu RoR-CPA-Vorteil und PRP-Vorteil, die die folgenden Parameter zu den Anfragen des Angreifers an das Verschlüsselungsorakel berücksichtigen sollte:

- Die maximale Anzahl $q_\#$ der Anfragen;
- die jeweilige Maximallänge $q_\mathrm{B}$ pro Anfrage, gerechnet in Blocks zu $\ell$ Bits.

- *Ansatz* laut *Anleitung zu Aufgabe 2.5:*
  Beweis zunächst für *gleichverteilt zufälliges* $f \in \mathrm{Func}(\{0,1\}^\ell)$
  (als „Gedankenexperiment“) statt für die konkrete Blockchiffre $E_K$

- Sei $(\mathcal{K}, \mathcal{E}, \mathcal{D})$ die Counter-Mode-Verschlüsselung mit $E_K$,
  $(\mathcal{K}', \mathcal{E}', \bot)$ mit $\mathcal{K}' = \mathrm{Func}(\{0,1\}^\ell)$ die Counter-Mode-Verschlüsselung mit $f$;
  die *Entschlüsselung* ist hier (OT-CPA-Sicherheit) *irrelevant!*



## Sicherheitsbeweis für den Counter Mode (Forts.)

- Sei $(\mathcal{K}, \mathcal{E}, \mathcal{D})$ die Counter-Mode-Verschlüsselung mit $E_K$,
  $(\mathcal{K}', \mathcal{E}', \bot)$ die Counter-Mode-Verschlüsselung mit $f$ ($\mathcal{K}' = \mathrm{Func}(\{0,1\}^\ell)$)

- Wir haben bei der Übung bereits gesehen (mit stochastischen Überlegungen):

$$\mathrm{Adv}^{\text{RoR-CPA}}_{(\mathcal{K}',\mathcal{E}',\bot),\boldsymbol{A}} \leq \frac{q_\#^2}{2^{\ell/2+1}}$$

  (nämlich $\mathrm{Adv}^{\text{RoR-CPA}}_{(\mathcal{K}',\mathcal{E}',\bot),\boldsymbol{A}} \leq \Pr[C]$, Ereignis $C$ bezeichnet eine *Kollision*
  zwischen den $iv \in_\$ \{0,1\}^{\ell/2}$ bei verschiedenen Verschlüsselungsvorgängen)

- Das gilt für *beliebige Angreifer* mit bis zu $q_\#$ Verschlüsselungsanfragen
  (sonst ohne Ressourcenbeschränkung)

- Was können wir nun über $\mathrm{Adv}^{\text{RoR-CPA}}_{(\mathcal{K},\mathcal{E},\mathcal{D}),\boldsymbol{A}}$ sagen?
  Wir wollen einen PRP-Vorteil verwenden
  (mit dem “Switching Lemma” reicht zunächst ein PRF-Vorteil)

## Sicherheitsbeweis für den Counter Mode (Forts.)

- Sei $(\mathcal{K}, \mathcal{E}, \mathcal{D})$ die Counter-Mode-Verschlüsselung mit $E_K$,
  $(\mathcal{K}', \mathcal{E}', \perp)$ die Counter-Mode-Verschlüsselung mit $f$ $(\mathcal{K}' = \mathrm{Func}(\{0,1\}^\ell)$
- Insgesamt *vier verschiedene Verschlüsselungsorakel:*
  - $E_1(\cdot)$, $E_0(\cdot)$ real, random bei $(\mathcal{K}, \mathcal{E}, \mathcal{D})$
  - $E'_1(\cdot)$, $E'_0(\cdot)$ real, random bei $(\mathcal{K}', \mathcal{E}', \perp)$
- Vorteile

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

  und

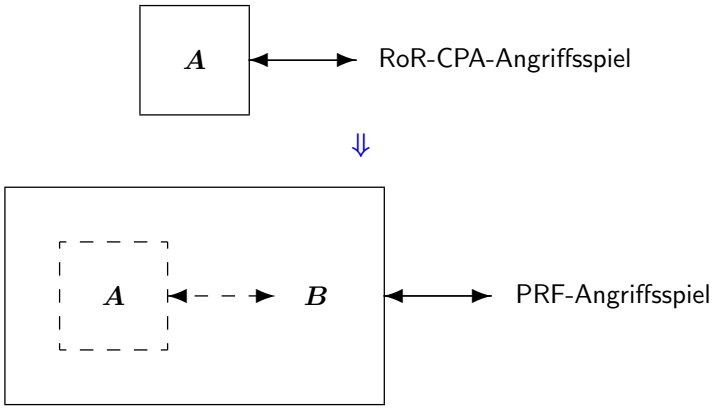
$$\mathrm{Adv}^{\text{RoR-CPA}}_{(\mathcal{K}',\mathcal{E}',\perp),\boldsymbol{A}} = \Pr\left[\boldsymbol{A}^{E'_1(\cdot)} \Rightarrow 1\right] - \Pr\left[\boldsymbol{A}^{E'_0(\cdot)} \Rightarrow 1\right]$$

- Kommen wir über solche Orakel $E(\cdot)$ irgendwie auf einen PRF-Angreifer?



## Sicherheitsbeweis für den Counter Mode (Forts.)

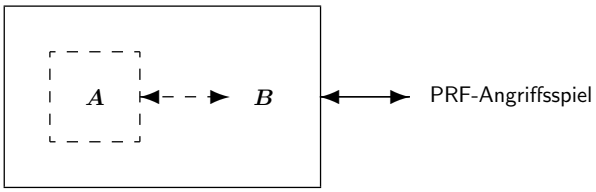
- Wir setzen die Black-Box-Technik hier ein:




- $\boldsymbol{B}$ implementiert als *Orakel für $\boldsymbol{A}$* die Counter-Mode-Verschlüsselung, aber *mit dem PRF-Orakel* anstelle von $E_K$ oder $f$

## Sicherheitsbeweis für den Counter Mode (Forts.)

- $\boldsymbol{B}$ implementiert als Orakel für $\boldsymbol{A}$ die Counter-Mode-Verschlüsselung mit dem PRF-Orakel anstelle von $E_K$ oder $f$




- Die Fälle des PRF-Angriffsspiels:
  $\boldsymbol{B}$ interagiert mit $E_K$ ($K \in_\$ \mathcal{K}$) oder mit $f$ ($f \in_\$ \mathrm{Func}(\{0,1\}^\ell)$ ...
- ... und mit $E_K$ ergibt sich für $\boldsymbol{A}$ genau $E_1(\cdot)$, also:

$$\Pr\left[\boldsymbol{A}^{E_1(\cdot)} \Rightarrow 1\right] = \Pr_{K\in_\$\mathcal{K}}\left[\boldsymbol{B}^{E_K(\cdot)} \Rightarrow 1\right]$$

- ... und mit $f$ ergibt sich für $\boldsymbol{A}$ genau $E'_1(\cdot)$, also:

$$\Pr\left[\boldsymbol{A}^{E'_1(\cdot)} \Rightarrow 1\right] = \Pr_{f\in_\$\mathrm{Func}(\{0,1\}^\ell}\left[\boldsymbol{B}^{f(\cdot)} \Rightarrow 1\right]$$

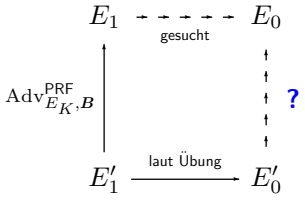


## Sicherheitsbeweis für den Counter Mode (Forts.)

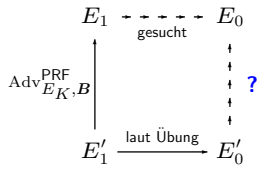
- $\Pr\left[\boldsymbol{A}^{E_1(\cdot)} \Rightarrow 1\right] = \Pr_{K\in_\$\mathcal{K}}\left[\boldsymbol{B}^{E_K(\cdot)} \Rightarrow 1\right]$,
  $\Pr\left[\boldsymbol{A}^{E'_1(\cdot)} \Rightarrow 1\right] = \Pr_{f\in_\$\mathrm{Func}(\{0,1\}^\ell}\left[\boldsymbol{B}^{f(\cdot)} \Rightarrow 1\right]$
- Es folgt

$$\begin{aligned}\mathrm{Adv}^{\mathsf{PRF}}_{E_K,\boldsymbol{B}} &= \Pr_{K\in_\$\mathcal{K}}\left[\boldsymbol{B}^{E_K(\cdot)} \Rightarrow 1\right] - \Pr_{f\in_\$\mathrm{Func}(\{0,1\}^\ell)}\left[\boldsymbol{B}^{f(\cdot)} \Rightarrow 1\right] \\ &= \Pr\left[\boldsymbol{A}^{E_1(\cdot)} \Rightarrow 1\right] - \Pr\left[\boldsymbol{A}^{E'_1(\cdot)} \Rightarrow 1\right],\end{aligned}$$

  der gesuchte Zusammenhang mit $\mathrm{Adv}^{\mathsf{PRF}}_{E_K,\boldsymbol{B}}$!
- Und was haben $E_1(\cdot)$ und $E'_1(\cdot)$ nun mit $\mathrm{Adv}^{\mathsf{RoR\text{-}CPA}}_{(\mathcal{K},\mathcal{E},\mathcal{D}),\boldsymbol{A}}$ zu tun ...?



# Sicherheitsbeweis für den Counter Mode (Forts.)

- 

- Also fehlt uns noch $\Pr\left[\boldsymbol{A}^{E_0(\cdot)} \Rightarrow 1\right] - \Pr\left[\boldsymbol{A}^{E'_0(\cdot)} \Rightarrow 1\right]$
- Das sind zwei "Random"-Verschlüsselungsorakel: einmal mit $E_K$, einmal mit $f$
- Man sieht leicht (anhand der Beschreibung des Verschlüsselungsalgorithmus): Welche Abbildung im Hintergrund ist, ist hier egal!
  (Die Ausgabe des "Random"-Verschlüsselungsorakel ist stets gleichverteilt.)
- Somit $\Pr\left[\boldsymbol{A}^{E_0(\cdot)} \Rightarrow 1\right] = \Pr\left[\boldsymbol{A}^{E'_0(\cdot)} \Rightarrow 1\right]$
- Nun können wir alles zusammensetzen ...



# Sicherheitsbeweis für den Counter Mode (Forts.)

- $\Pr\left[\boldsymbol{A}^{E_1(\cdot)} \Rightarrow 1\right] - \Pr\left[\boldsymbol{A}^{E'_1(\cdot)} \Rightarrow 1\right] = \mathrm{Adv}^{\mathsf{PRF}}_{E_K,\boldsymbol{B}}$
- $\Pr\left[\boldsymbol{A}^{E'_1(\cdot)} \Rightarrow 1\right] - \Pr\left[\boldsymbol{A}^{E'_0(\cdot)} \Rightarrow 1\right] = \mathrm{Adv}^{\mathsf{RoR\text{-}CPA}}_{(\mathcal{K}',\mathcal{E}',\perp),\boldsymbol{A}} \leq \frac{q_\#^2}{2^{\ell/2+1}}$
- $\Pr\left[\boldsymbol{A}^{E_0(\cdot)} \Rightarrow 1\right] - \Pr\left[\boldsymbol{A}^{E'_0(\cdot)} \Rightarrow 1\right] = 0$
- Es folgt

$$\begin{aligned}
\mathrm{Adv}^{\mathsf{RoR\text{-}CPA}}_{(\mathcal{K},\mathcal{E},\mathcal{D}),\boldsymbol{A}} &= \Pr\left[\boldsymbol{A}^{E_1(\cdot)} \Rightarrow 1\right] - \Pr\left[\boldsymbol{A}^{E_0(\cdot)} \Rightarrow 1\right] \\
&= \Pr\left[\boldsymbol{A}^{E_1(\cdot)} \Rightarrow 1\right] - \Pr\left[\boldsymbol{A}^{E'_1(\cdot)} \Rightarrow 1\right] \\
&\quad + \Pr\left[\boldsymbol{A}^{E'_1(\cdot)} \Rightarrow 1\right] - \Pr\left[\boldsymbol{A}^{E'_0(\cdot)} \Rightarrow 1\right] \\
&\quad + \Pr\left[\boldsymbol{A}^{E'_0(\cdot)} \Rightarrow 1\right] - \Pr\left[\boldsymbol{A}^{E_0(\cdot)} \Rightarrow 1\right] \\
&\leq \mathrm{Adv}^{\mathsf{PRF}}_{E_K,\boldsymbol{B}} + \frac{q_\#^2}{2^{\ell/2+1}}
\end{aligned}$$

## Sicherheitsbeweis für den Counter Mode (Forts.)

- Wir haben also

$$\mathrm{Adv}^{\text{RoR-CPA}}_{(\mathcal{K},\mathcal{E},\mathcal{D}),\boldsymbol{A}} \;\leq\; \mathrm{Adv}^{\text{PRF}}_{E_K,\boldsymbol{B}} + \frac{q_{\#}^2}{2^{\ell/2+1}},$$

  das heißt

$$\mathrm{Adv}^{\text{PRF}}_{E_K,\boldsymbol{B}} \;\geq\; \mathrm{Adv}^{\text{RoR-CPA}}_{(\mathcal{K},\mathcal{E},\mathcal{D}),\boldsymbol{A}} - \frac{q_{\#}^2}{2^{\ell/2+1}}$$

- Mit

$$\mathrm{Adv}^{\text{PRP}}_{E_K,\boldsymbol{B}} - \mathrm{Adv}^{\text{PRF}}_{E_K,\boldsymbol{B}} \;\leq\; \frac{q^2}{2^{\ell+1}}$$

  laut *PRP/PRF Switching Lemma* bei maximal $q$ Anfragen ans PRP- bzw. PRF-Orakel folgt

$$\mathrm{Adv}^{\text{PRP}}_{E_K,\boldsymbol{B}} \;\geq\; \mathrm{Adv}^{\text{RoR-CPA}}_{(\mathcal{K},\mathcal{E},\mathcal{D}),\boldsymbol{A}} - \frac{q_{\#}^2}{2^{\ell/2+1}} - \frac{q^2}{2^{\ell+1}}$$

  als Sicherheitsresultat für den Counter Mode!



## Sicherheitsbeweis für den Counter Mode (Forts.)

*Zusammenfassung*

- „$E_K$ ist *PRP-sicher* $\Rightarrow$
  *Counter-Mode-Verschlüsselung* mit $E_K$ ist *RoR-CPA-sicher*“
- ... nämlich genauer: zu jedem RoR-CPA-Angreifer $\boldsymbol{A}$ lässt sich ein PRP-Angreifer $\boldsymbol{B}$ angeben mit

$$\mathrm{Adv}^{\text{PRP}}_{E_K,\boldsymbol{B}} \;\geq\; \mathrm{Adv}^{\text{RoR-CPA}}_{(\mathcal{K},\mathcal{E},\mathcal{D}),\boldsymbol{A}} - \frac{q_{\#}^2}{2^{\ell/2+1}} - \frac{q^2}{2^{\ell+1}},$$

  wobei $q_{\#}$ die maximale Anzahl die Verschlüsselungsvorgäng bezeichnet und $q$ die maximale Anzahl der Blocks insgesamt.

  (Das gilt für den Counter Mode wie in der Lösung zu Aufgabe 2.3 beschrieben, nämlich mit $iv \in_{\$} \{0,1\}^{\ell/2}$.)

# Sicherheitsbeweis für den Counter Mode (Forts.)

- *Resultat zur Sicherheit:* $\mathrm{Adv}^{\mathsf{PRP}}_{E_K,\boldsymbol{B}} \geq \mathrm{Adv}^{\mathsf{RoR\text{-}CPA}}_{(\mathcal{K},\mathcal{E},\mathcal{D}),\boldsymbol{A}} - \frac{q_\#^2}{2^{\ell/2+1}} - \frac{q^2}{2^{\ell+1}}$
- Hier ist

$$\epsilon = \frac{q_\#^2}{2^{\ell/2+1}} + \frac{q^2}{2^{\ell+1}}$$

  „verschwindend gering“, solange $q_\#$ und $q$ genügend klein sind!
- Wie lange das so ist, hängt also von $\ell$ ab:
  Deshalb ist z. B. AES mit $\ell = 128$ *oft besser* als Blockchiffren mit $\ell = 64$
- Die Lösung zu Aufgabe 2.5 folgt mit $q = q_\# \cdot q_\mathrm{B}$:

$$\mathrm{Adv}^{\mathsf{PRP}}_{E_K,\boldsymbol{B}} \geq \mathrm{Adv}^{\mathsf{RoR\text{-}CPA}}_{(\mathcal{K},\mathcal{E},\mathcal{D}),\boldsymbol{A}} - \frac{q_\#^2}{2^{\ell/2+1}} - \frac{(q_\# q_B)^2}{2^{\ell+1}}$$

  ... z. B. für $q_\mathrm{B} = 2^{\ell/4}$ ergibt sich

$$\mathrm{Adv}^{\mathsf{PRP}}_{E_K,\boldsymbol{B}} \geq \mathrm{Adv}^{\mathsf{RoR\text{-}CPA}}_{(\mathcal{K},\mathcal{E},\mathcal{D}),\boldsymbol{A}} - \frac{q_\#^2}{2^{\ell/2}}$$