Beweisbar sichere Verschlüsselung

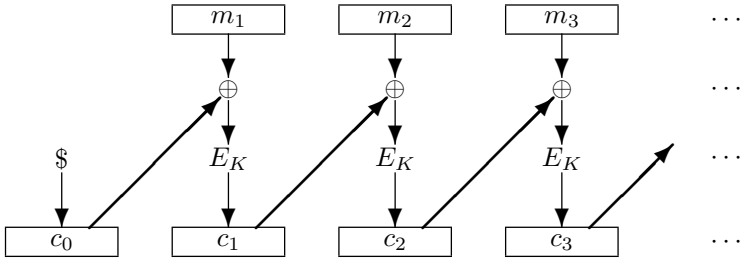
ITS-Wahlpflichtvorlesung

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

$Id: bsv.ltx,v 1.56 2007/05/23 16:45:20 bm Exp $

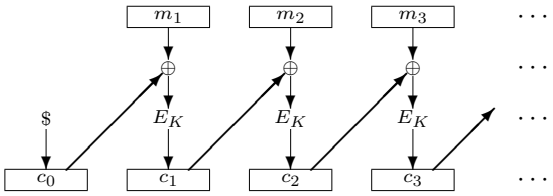
Cipher Block Chaining (CBC)

- *CBC* ist einer der ältesten Modes of Operation für Blockchiffren:
  FIPS PUB 81, *DES Modes of Operation,* NIST 1980
  (Federal Information Processing Standards Publication,
  National Institute of Standards and Technology, USA)
- ... wird verwendet für *beliebige Blockchiffren*:
  - Schlüsselmenge $\mathcal{K}$;
  - für $K \in \mathcal{K}$ Abbildungen $E_K, D_K \colon \{0,1\}^\ell \to \{0,1\}^\ell$;
  - $D_K = E_K^{-1}$ (das heißt $x = D_K\big(E_K(x)\big)$ für $x \in \{0,1\}^\ell$)
- *CBC-Verschlüsselung:*

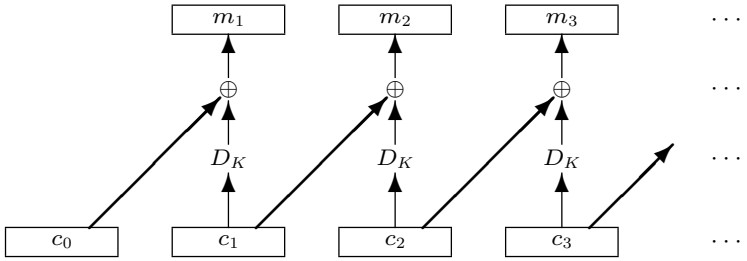


Cipher Block Chaining (CBC) (Forts.)

- CBC-Verschlüsselung:



- *CBC-Entschlüsselung:*

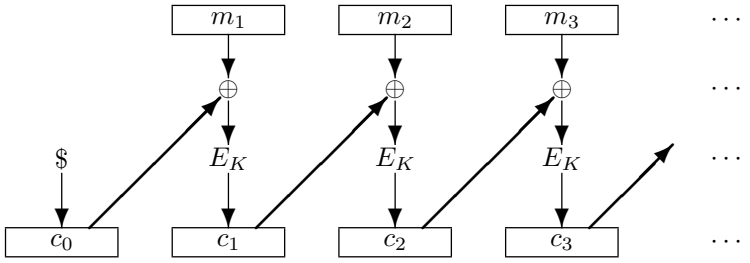


Cipher Block Chaining (CBC) (Forts.)

- *CBC* für eine ℓ-Bit-Blockchiffre *als Verschlüsselungsschema* $(\mathcal{K}, \mathcal{E}, \mathcal{D})$:
  - $\mathcal{K}$ (als *Schlüsselgenerierungsalgorithmus*):
    erzeugt gleichverteilt zufälligen Schlüssel aus der Menge $\mathcal{K}$
  - *Verschlüsselungsalgorithmus* $\mathcal{E}_K(m)$:
    funktioniert für alle Plaintexte m einer Länge $n \cdot \ell$,
    also für die Plaintextmenge $\mathcal{M} = \bigcup_{0 \leq i} \{0,1\}^{n \cdot \ell}$;
    - zerlegt $m = m_1 \parallel m_2 \parallel \ldots \parallel m_n$ (mit $|m_i| = \ell$ für jedes i)
    - setzt $c_0 \xleftarrow{\$} \{0,1\}^\ell$ (zufälliger *Initialization Vector*)
    - setzt $c_i \leftarrow E_K(c_{i-1} \oplus m_i)$ für $i = 1, \ldots, n$
    - gibt $c_0 \parallel c_1 \parallel c_2 \parallel \ldots \parallel c_n$ aus
  - *Entschlüsselungsalgorithmus* $\mathcal{D}_K(c)$ für Ciphertexte $c \in \{0,1\}^*$:
    - zerlegt $c = c_0 \parallel c_1 \parallel c_2 \parallel \ldots \parallel c_n$ (mit $|c_i| = \ell$ für jedes i);
      falls nicht möglich: Abbruch mit Ausgabewert $\perp$!
    - setzt $m_i \leftarrow c_{i-1} \oplus D_K(c_i)$ für $i = 1, \ldots, n$
    - gibt $m_1 \parallel m_2 \parallel \ldots \parallel m_n$ aus

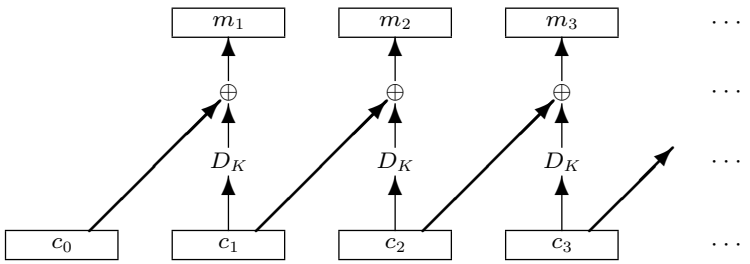
Cipher Block Chaining (CBC) (Forts.)

- Verschlüsselungsalgorithmus $\mathcal{E}_K(m)$ für die Plaintextmenge $\mathcal{M} = \bigcup_{0 \le i} \{0,1\}^{n \cdot \ell}$:
  - zerlegt $m = m_1 \parallel m_2 \parallel \ldots \parallel m_n$ (mit $|m_i| = \ell$ für jedes i)
  - setzt $c_0 \xleftarrow{\$} \{0,1\}^\ell$
  - setzt $c_i \leftarrow E_K(c_{i-1} \oplus m_i)$ für $i = 1, \ldots, n$
  - gibt $c_0 \parallel c_1 \parallel c_2 \parallel \ldots \parallel c_n$ aus
- ... als Diagramm zum Vergleich:



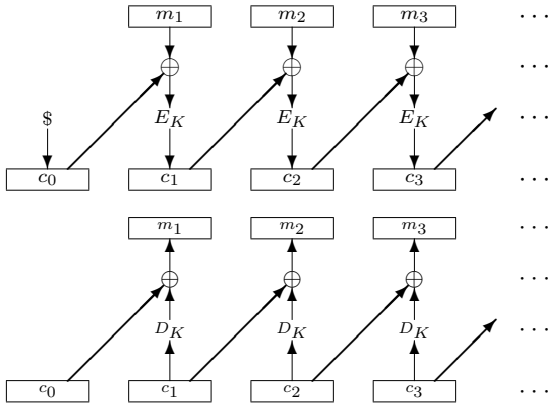
Cipher Block Chaining (CBC) (Forts.)

- Entschlüsselungsalgorithmus $\mathcal{D}_K(c)$ für Ciphertexte $c \in \{0,1\}^*$:
  - zerlegt $c = c_0 \parallel c_1 \parallel c_2 \parallel \ldots \parallel c_n$ (mit $|c_i| = \ell$ für jedes i);
    falls nicht möglich: Abbruch mit Ausgabewert $\perp$!
  - setzt $m_i \leftarrow c_{i-1} \oplus D_K(c_i)$ für $i = 1, \ldots, n$
  - gibt $m_1 \parallel m_2 \parallel \ldots \parallel m_n$ aus
- ... als Diagramm zum Vergleich:



Cipher Block Chaining (CBC) (Forts.)

- Erste Frage: Ist dieses *Verschlüsselungsschema korrekt?*
  Gilt also $\mathcal{D}_K\big(\mathcal{E}_K(m)\big) = m$ für $K \xleftarrow{\$} \mathcal{K}$, $m \in \mathcal{M}$?
- *Ja,* wegen $D_K\big(E_K(x_i)\big) = x_i$;
  die Korrektheit kann man in der Diagramm-Darstellung leicht nachprüfen:



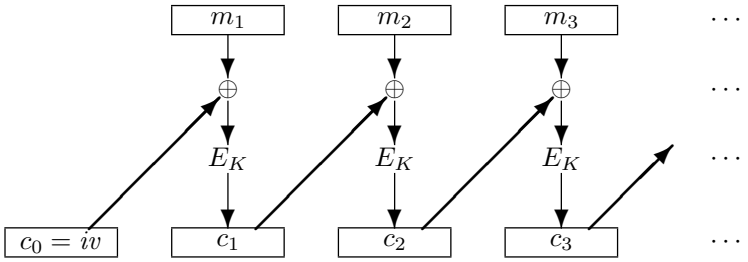
(Für $x_i = c_{i-1} \oplus m_i$ gilt $m_i = c_{i-1} \oplus x_i$.)

Cipher Block Chaining (CBC) (Forts.)

- Die Korrektheit ist geklärt – bleibt die Frage nach der *Sicherheit.*
- Wir nehmen weiter einen passiven Angreifer an (Chosen Plaintext Attack)
  und untersuchen die Sicherheit im Sinne von *RoR-CPA.*
- ... d. h. untersuchen die Aussichten des Angreifers,
  in einem "Real-or-Random"-Angriffsspiel
  zwischen CBC-Verschlüsselung $\mathcal{E}_K(\cdot)$ ("real")
  und der CBC-Verschlüsselung von Zufallsdaten ("random") zu unterscheiden.
- Vorweg *unsichere Varianten* von CBC: ...

Cipher Block Chaining (CBC) (Forts.)

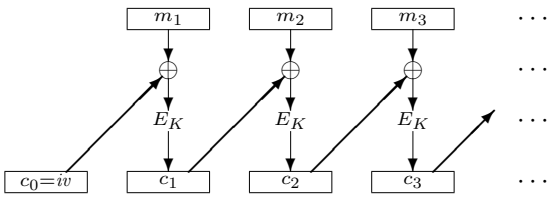
- CBC *mit konstantem Initialization Vector* iv (z. B. $iv = 0000\ldots0000$) ist bei Mehrfachverschlüsselung nicht sicher!



- Klar, denn wir haben schon gesehen:
  Deterministische Mehrfachverschlüsselung ist *immer unsicher.*

Cipher Block Chaining (CBC) (Forts.)

- Wie sieht es aus bei CBC *mit einem Zähler* als iv?
  (Erster Verschlüsselungsvorgang $iv = 0000\ldots0000$,
  zweiter Verschlüsselungsvorgang $iv = 0000\ldots0001$,
  dritter Verschlüsselungsvorgang $iv = 0000\ldots0010$, ...)



- Auch nicht sicher!

  Ein erfolgreicher Angriff: RoR-CPA-Angreifer stellt Anfragen der Länge ℓ $E(0000\ldots0000)$, $E(0000\ldots0001)$

  Im "Real"-Fall ergibt sich dann zweimal das gleiche c_1 $(= E_K(0000\ldots0000))$; im "Random"-Fall höchstwahrscheinlich nicht → *hoher Vorteil möglich*

Die Sicherheit von CBC

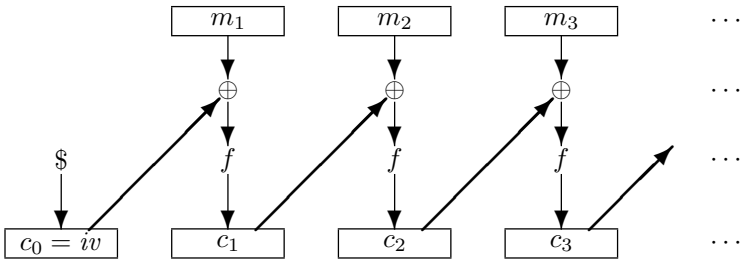
- Bei der *RoR-CPA-Sicherheit* betrachten wir zwei Orakel:
  - $E_1(\cdot)$ als *„echtes“ Verschlüsselungsorakel*
    (liefert $\mathcal{E}_K(\cdot)$ mit festem $K \xleftarrow{\$} \mathcal{K}$)
  - $E_0(\cdot)$ als *„zufälliges“ Verschlüsselungsorakel*
    (liefert $\mathcal{E}_K(m_0)$ mit festem $K \xleftarrow{\$} \mathcal{K}$
    für jeweils neu zufällig gewähltes m_0 der geforderten Länge)
- Gesucht: Eine Aussage über den RoR-CPA-Vorteil

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

  eines Angreifers $\boldsymbol{A}$
- Schon bei der Sicherheit des Counter Mode (CTR) erprobter Ansatz:
  zusätzliche Orakel $E'_1(\cdot)$, $E'_0(\cdot)$ analog zu $E_1(\cdot)$, $E_0(\cdot)$,
  aber auf Basis von $f \in_{\$} \mathrm{Func}(\{0,1\}^\ell)$ statt der konkreten Blockchiffre

Die Sicherheit von CBC (Forts.)

- Die idealisierte Verschlüsselung mit Orakel $E'_1(\cdot)$ geschieht also so
  ($f \in_{\$} \mathrm{Func}(\{0,1\}^\ell)$):



- $E'_0(\cdot)$ (als Pendant zum “Random”-Verschlüsselungsorakel $E_0(\cdot)$)
  analog dazu, aber mit zufälligem Plaintext

Die Sicherheit von CBC (Forts.)

- Wie beim Beweis der Sicherheit des Counter Mode wollen wir

$$\Pr\left[\boldsymbol{A}^{E_1(\cdot)} \Rightarrow 1\right] \qquad \Pr\left[\boldsymbol{A}^{E_0(\cdot)} \Rightarrow 1\right]$$
$$\Pr\left[\boldsymbol{A}^{E'_1(\cdot)} \Rightarrow 1\right] \qquad \Pr\left[\boldsymbol{A}^{E'_0(\cdot)} \Rightarrow 1\right]$$

  betrachten, um etwas über

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

  auszusagen:

  - $\Pr\left[\boldsymbol{A}^{E_1(\cdot)} \Rightarrow 1\right] - \Pr\left[\boldsymbol{A}^{E'_1(\cdot)} \Rightarrow 1\right]$ *?*
  - $\Pr\left[\boldsymbol{A}^{E'_1(\cdot)} \Rightarrow 1\right] - \Pr\left[\boldsymbol{A}^{E'_0(\cdot)} \Rightarrow 1\right]$ *?*
  - $\Pr\left[\boldsymbol{A}^{E'_0(\cdot)} \Rightarrow 1\right] - \Pr\left[\boldsymbol{A}^{E_0(\cdot)} \Rightarrow 1\right]$ *?*

Die Sicherheit von CBC (Forts.)

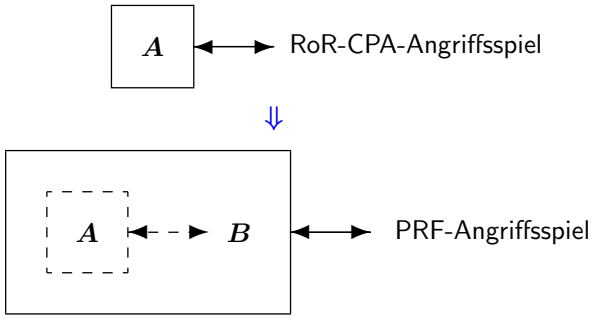
$$\Pr\left[\boldsymbol{A}^{E_1(\cdot)} \Rightarrow 1\right] - \Pr\left[\boldsymbol{A}^{E'_1(\cdot)} \Rightarrow 1\right] \textit{???}$$

$$\Pr\left[\boldsymbol{A}^{E'_1(\cdot)} \Rightarrow 1\right] - \Pr\left[\boldsymbol{A}^{E'_0(\cdot)} \Rightarrow 1\right] \textit{???}$$

$$\Pr\left[\boldsymbol{A}^{E'_0(\cdot)} \Rightarrow 1\right] - \Pr\left[\boldsymbol{A}^{E_0(\cdot)} \Rightarrow 1\right] \textit{???}$$

Die Sicherheit von CBC (Forts.)

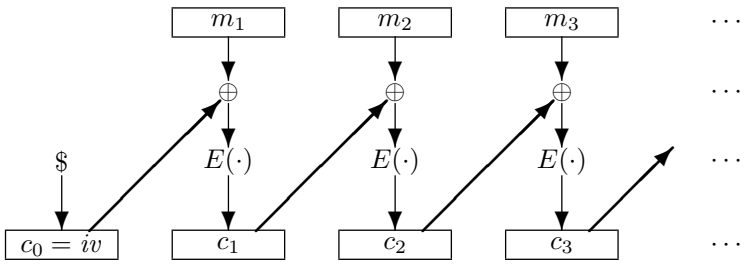
- $\Pr\left[\boldsymbol{A}^{E_1(\cdot)} \Rightarrow 1\right] - \Pr\left[\boldsymbol{A}^{E_1'(\cdot)} \Rightarrow 1\right]$?
- Ansatz: Konstruiere aus $\boldsymbol{A}$ (RoR-CPA-Angreifer gegen CBC) einen PRF-Angreifer $\boldsymbol{B}$



- $\boldsymbol{B}$ bietet für $\boldsymbol{A}$ CBC-Verschlüsselung auf Basis seines PRF-Orakels, übernimmt das Ausgabebit von $\boldsymbol{A}$ als eigene Ausgabe ...

Die Sicherheit von CBC (Forts.)

- Ansatz: Konstruiere aus $\boldsymbol{A}$ (RoR-CPA-Angreifer gegen CBC) einen PRF-Angreifer $\boldsymbol{B}$
- $\boldsymbol{B}$ bietet für $\boldsymbol{A}$ CBC-Verschlüsselung auf Basis seines PRF-Orakels, übernimmt das Ausgabebit von $\boldsymbol{A}$ als eigene Ausgabe
- $\boldsymbol{B}$ implementiert für $\boldsymbol{A}$ also folgende Variante von $\mathcal{E}_K(m)$:



Hier bezeichnet $E(\cdot)$ das PRF-Orakel

- Im Fall $E(\cdot) = E_K(\cdot)$ des PRF-Angriffsspiels ergibt sich so CBC mit E_K; genau wie bei $E_1(\cdot)$.
- ... und im Fall $E(\cdot) = f(\cdot)$ ergibt sich CBC mit f, genau wie bei $E_1'(\cdot)$.

Die Sicherheit von CBC (Forts.)

- Der Fall $E_K(\cdot)$ des PRF-Angriffsspiels ist wie $E_1(\cdot)$,
  der Fall $f(\cdot)$ ist wie $E'_1(\cdot)$
- $\boldsymbol{B}$ (auf Basis von $\boldsymbol{A}$ konstruiert) übernimmt hier dessen Ausgabe: Also

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

- Der PRF-Vorteil von $\boldsymbol{B}$ ist definiert als

$$\mathrm{Adv}^{\mathsf{PRF}}_{E_K,\boldsymbol{B}} = \Pr\left[\boldsymbol{B}^{E_K(\cdot)} \Rightarrow 1\right] - \Pr\left[\boldsymbol{B}^{f(\cdot)} \Rightarrow 1\right],$$

  also folgt

$$\Pr\left[\boldsymbol{A}^{E_1(\cdot)} \Rightarrow 1\right] - \Pr\left[\boldsymbol{A}^{E'_1(\cdot)} \Rightarrow 1\right] = \mathrm{Adv}^{\mathsf{PRF}}_{E_K,\boldsymbol{B}}$$

Die Sicherheit von CBC (Forts.)

- Diese Gleichung

$$\Pr\left[\boldsymbol{A}^{E_1(\cdot)} \Rightarrow 1\right] - \Pr\left[\boldsymbol{A}^{E'_1(\cdot)} \Rightarrow 1\right] = \mathrm{Adv}^{\mathsf{PRF}}_{E_K,\boldsymbol{B}}$$

  enthält einen PRF-Vorteil – für E_K (Blockchiffre) wäre PRP-Vorteil natürlicher
- Laut *PRF/PRP Switching Lemma:*
  Wenn $\boldsymbol{A}$ höchstens q Blöcke verschlüsseln lässt
  ($\rightarrow$ hier höchstens q Orakelanfragen für $\boldsymbol{B}$), gilt

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

- Also:

$$\Pr\left[\boldsymbol{A}^{E_1(\cdot)} \Rightarrow 1\right] - \Pr\left[\boldsymbol{A}^{E'_1(\cdot)} \Rightarrow 1\right] \leq \mathrm{Adv}^{\mathsf{PRP}}_{E_K,\boldsymbol{B}} + \frac{q^2}{2^{\ell+1}}$$

Die Sicherheit von CBC (Forts.)

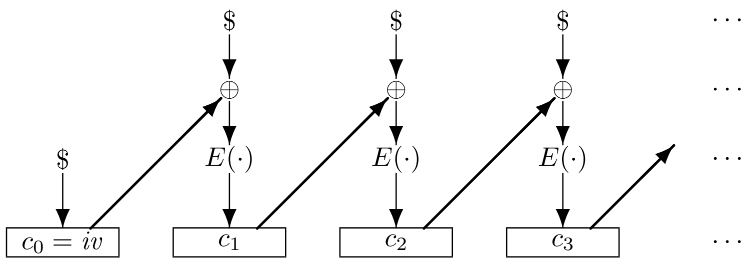
$$\Pr\left[A^{E_1(\cdot)} \Rightarrow 1\right] - \Pr\left[A^{E_1'(\cdot)} \Rightarrow 1\right] !$$

$$\Pr\left[A^{E_1'(\cdot)} \Rightarrow 1\right] - \Pr\left[A^{E_0'(\cdot)} \Rightarrow 1\right] ???$$

$$\Pr\left[A^{E_0'(\cdot)} \Rightarrow 1\right] - \Pr\left[A^{E_0(\cdot)} \Rightarrow 1\right] ???$$

Die Sicherheit von CBC (Forts.)

- $\Pr\left[A^{E_0'(\cdot)} \Rightarrow 1\right] - \Pr\left[A^{E_0(\cdot)} \Rightarrow 1\right]$?
- $E_0'(\cdot)$ und $E_0(\cdot)$ sind *"Random"-Verschlüsselungsorakel* nach diesem Schema:



„$E(\cdot)$“ hierin ist $f(\cdot)$ bzw. $E_K(\cdot)$

- Ganz ähnlich wie vorhin können wir einen PRF-Angreifer C konstruieren mit $\Pr\left[A^{E_0(\cdot)} \Rightarrow 1\right] = \Pr\left[C^{E_K(\cdot)} \Rightarrow 1\right]$, $\quad \Pr\left[A^{E_0'(\cdot)} \Rightarrow 1\right] = \Pr\left[C^{f(\cdot)} \Rightarrow 1\right]$

Die Sicherheit von CBC (Forts.)

- $\Pr\left[\boldsymbol{A}^{E_0(\cdot)} \Rightarrow 1\right] = \Pr\left[\boldsymbol{C}^{E_K(\cdot)} \Rightarrow 1\right]$
- $\Pr\left[\boldsymbol{A}^{E'_0(\cdot)} \Rightarrow 1\right] = \Pr\left[\boldsymbol{C}^{f(\cdot)} \Rightarrow 1\right]$
- Also
$$\Pr\left[\boldsymbol{A}^{E_0(\cdot)} \Rightarrow 1\right] - \Pr\left[\boldsymbol{A}^{E'_0(\cdot)} \Rightarrow 1\right] \;=\; \mathrm{Adv}^{\mathsf{PRF}}_{E_K,\boldsymbol{C}}$$
- Eigentlich interessiert uns $\Pr\left[\boldsymbol{A}^{E'_0(\cdot)} \Rightarrow 1\right] - \Pr\left[\boldsymbol{A}^{E_0(\cdot)} \Rightarrow 1\right]$ ...
- Wir haben
$$\Pr\left[\boldsymbol{A}^{E'_0(\cdot)} \Rightarrow 1\right] - \Pr\left[\boldsymbol{A}^{E_0(\cdot)} \Rightarrow 1\right] \;=\; \mathrm{Adv}^{\mathsf{PRF}}_{E_K,\boldsymbol{C}'}$$
mit $\boldsymbol{C}'$ als „umgedrehtem“ $\boldsymbol{C}$ (Ausgabe 0 statt 1 und umgekehrt)!
- Laut *PRF/PRP Switching Lemma:*
Wenn $\boldsymbol{A}$ höchstens q Blöcke verschlüsseln lässt ($\rightarrow$ hier höchstens q Orakelanfragen für $\boldsymbol{C}$), gilt
$$\mathrm{Adv}^{\mathsf{PRF}}_{E_K,\boldsymbol{C}'} \;\leq\; \mathrm{Adv}^{\mathsf{PRP}}_{E_K,\boldsymbol{C}'} + \frac{q^2}{2^{\ell+1}}$$
- Also:
$$\Pr\left[\boldsymbol{A}^{E'_0(\cdot)} \Rightarrow 1\right] - \Pr\left[\boldsymbol{A}^{E_0(\cdot)} \Rightarrow 1\right] \;\leq\; \mathrm{Adv}^{\mathsf{PRP}}_{E_K,\boldsymbol{C}'} + \frac{q^2}{2^{\ell+1}}$$

Die Sicherheit von CBC (Forts.)

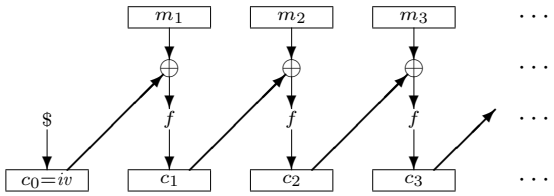
$$\Pr\left[\boldsymbol{A}^{E_1(\cdot)} \Rightarrow 1\right] - \Pr\left[\boldsymbol{A}^{E'_1(\cdot)} \Rightarrow 1\right] \textit{!}$$

$$\Pr\left[\boldsymbol{A}^{E'_1(\cdot)} \Rightarrow 1\right] - \Pr\left[\boldsymbol{A}^{E'_0(\cdot)} \Rightarrow 1\right] \textit{???}$$

$$\Pr\left[\boldsymbol{A}^{E'_0(\cdot)} \Rightarrow 1\right] - \Pr\left[\boldsymbol{A}^{E_0(\cdot)} \Rightarrow 1\right] \textit{!}$$

Die Sicherheit von CBC (Forts.)

- $\Pr\left[\boldsymbol{A}^{E'_1(\cdot)} \Rightarrow 1\right] - \Pr\left[\boldsymbol{A}^{E'_0(\cdot)} \Rightarrow 1\right]$?
- Das ist der *Vorteil* von $\boldsymbol{A}$ gegen „idealisierte CBC-Verschlüsselung“, nämlich CBC auf Basis von $f \in_{\$} \mathrm{Func}(\{0,1\}^{\ell})$



- (... bei der man übrigens oft nicht eindeutig entschlüsseln könnte, denn f muss nicht umkehrbar sein! Das ist hier aber egal.)
- Wir verwenden wieder ein stochastisches Argument!
  Unter welchem Ereignis C können die Fälle “real” und “random” überhaupt verschiedene Verteilungen ergeben? ...

Die Sicherheit von CBC (Forts.)

- Verschlüsselungsalgorithmus $\mathcal{E}_K(m)$ lief mit E_K so ab:
  - zerlege $m = m_1 \parallel m_2 \parallel \ldots \parallel m_n$ (mit $|m_i| = \ell$ für jedes i)
  - setze $c_0 \xleftarrow{\$} \{0,1\}^{\ell}$
  - setze $c_i \leftarrow E_K(c_{i-1} \oplus m_i)$ für $i = 1, \ldots, n$
  - gib $c_0 \parallel c_1 \parallel c_2 \parallel \ldots \parallel c_n$ aus
- ... also mit f so:
  - zerlege $m = m_1 \parallel m_2 \parallel \ldots \parallel m_n$ (mit $|m_i| = \ell$ für jedes i)
  - setze $c_0 \xleftarrow{\$} \{0,1\}^{\ell}$
  - setze $c_i \leftarrow f(c_{i-1} \oplus m_i)$ für $i = 1, \ldots, n$
  - gib $c_0 \parallel c_1 \parallel c_2 \parallel \ldots \parallel c_n$ aus

Die Sicherheit von CBC (Forts.)

- Variante von $\mathcal{E}_K(m)$ mit f:
  - zerlege $m = m_1 \parallel m_2 \parallel \ldots \parallel m_n$ (mit $|m_i| = \ell$ für jedes i)
  - setze $c_0 \xleftarrow{\$} \{0,1\}^\ell$
  - setze $c_i \leftarrow f(c_{i-1} \oplus m_i)$ für $i = 1, \ldots, n$
  - gib $c_0 \parallel c_1 \parallel c_2 \parallel \ldots \parallel c_n$ aus
- *Kombinierte Form* für $E'_1(\cdot)$ (*"real" mit f* wie vorhin) und $E'_0(\cdot)$ (*"random"*-Variante dazu):
  - zerlege $m = m_1 \parallel m_2 \parallel \ldots \parallel m_n$ (mit $|m_i| = \ell$ für jedes i)
  - setze $m_{0,i} \xleftarrow{\$} \{0,1\}^\ell$ für $i = 1, \ldots, n$
  - setze $c_0 \xleftarrow{\$} \{0,1\}^\ell$, $c'_0 \leftarrow c_0$
  - setze $c_i \leftarrow f(c_{i-1} \oplus m_i)$ für $i = 1, \ldots, n$
  - setze $c'_i \leftarrow f(c'_{i-1} \oplus m_{0,i})$ für $i = 1, \ldots, n$
  - für $E'_1(\cdot)$: gib $c_0 \parallel c_1 \parallel c_2 \parallel \ldots \parallel c_n$ aus
  - für $E'_0(\cdot)$: gib $c_0 \parallel c'_1 \parallel c'_2 \parallel \ldots \parallel c'_n$ aus
- *Gleiche Verteilung der Ausgabe,* solange es keine Kollision gibt unter *allen* $c_{i-1} \oplus m_i$ und $c'_{i-1} \oplus m_{0,i}$ aus *allen* Verschlüsselungsvorgängen!

Die Sicherheit von CBC (Forts.)

- Gleiche Verteilung der Ausgabe, solange es keine Kollision gibt unter *allen* $c_{i-1} \oplus m_i$ und $c'_{i-1} \oplus m_{0,i}$ aus *allen* Verschlüsselungsvorgängen
- Wenn $\boldsymbol{A}$ höchstens q Blöcke verschlüsseln lässt (insgesamt bei vielen Anfragen ans Verschlüsselungsorakel), sind das $2q$ ℓ-Bit-Werte!
- Für das Ereignis C einer solchen Kollision gilt

$$\Pr[C] \;\leq\; \frac{1}{2^\ell} + \frac{2}{2^\ell} + \frac{3}{2^\ell} + \cdots + \frac{2q-1}{2^\ell} \;\leq\; \frac{q^2}{2^{\ell-1}}$$

- Wir können folgern

$$\Pr\left[\boldsymbol{A}^{E'_1(\cdot)} \Rightarrow 1\right] - \Pr\left[\boldsymbol{A}^{E'_0(\cdot)} \Rightarrow 1\right] \;\leq\; \Pr[C] \;\leq\; \frac{q^2}{2^{\ell-1}}$$

Die Sicherheit von CBC (Forts.)

$$\Pr\left[\boldsymbol{A}^{E_1(\cdot)} \Rightarrow 1\right] - \Pr\left[\boldsymbol{A}^{E_1'(\cdot)} \Rightarrow 1\right] \mathit{!}$$

$$\Pr\left[\boldsymbol{A}^{E_1'(\cdot)} \Rightarrow 1\right] - \Pr\left[\boldsymbol{A}^{E_0'(\cdot)} \Rightarrow 1\right] \mathit{!}$$

$$\Pr\left[\boldsymbol{A}^{E_0'(\cdot)} \Rightarrow 1\right] - \Pr\left[\boldsymbol{A}^{E_0(\cdot)} \Rightarrow 1\right] \mathit{!}$$

Die Sicherheit von CBC (Forts.)

- Es bleibt nur noch, alles zusammenzusetzen:
  Bei *maximal q Blocks in Anfragen von $\boldsymbol{A}$* gilt

$$\begin{aligned}
\mathrm{Adv}^{\text{RoR-CPA}}_{(\mathcal{K},\mathcal{E},\mathcal{D}),\boldsymbol{A}} &= \Pr\left[\boldsymbol{A}^{E_1(\cdot)} \Rightarrow 1\right] - \Pr\left[\boldsymbol{A}^{E_0(\cdot)} \Rightarrow 1\right] \\
&= \Pr\left[\boldsymbol{A}^{E_1(\cdot)} \Rightarrow 1\right] - \Pr\left[\boldsymbol{A}^{E_1'(\cdot)} \Rightarrow 1\right] \\
&\quad + \Pr\left[\boldsymbol{A}^{E_1'(\cdot)} \Rightarrow 1\right] - \Pr\left[\boldsymbol{A}^{E_0'(\cdot)} \Rightarrow 1\right] \\
&\quad + \Pr\left[\boldsymbol{A}^{E_0'(\cdot)} \Rightarrow 1\right] - \Pr\left[\boldsymbol{A}^{E_0(\cdot)} \Rightarrow 1\right] \\
&\leq \left(\mathrm{Adv}^{\text{PRP}}_{E_K,\boldsymbol{B}} + \frac{q^2}{2^{\ell+1}}\right) + \frac{q^2}{2^{\ell-1}} + \left(\mathrm{Adv}^{\text{PRP}}_{E_K,\boldsymbol{C}'} + \frac{q^2}{2^{\ell+1}}\right) \\
&\leq \mathrm{Adv}^{\text{PRP}}_{E_K,\boldsymbol{B}} + \mathrm{Adv}^{\text{PRP}}_{E_K,\boldsymbol{C}'} + \frac{3 \cdot q^2}{2^{\ell}}
\end{aligned}$$

  ($\boldsymbol{B}$, $\boldsymbol{C}'$ beide direkt von $\boldsymbol{A}$ abgeleitet)

- Dieses *Sicherheitsresultat für CBC* sagt uns: CBC ist RoR-CPA-sicher –
  es sei denn, schon die Blockchiffre ist unsicher oder q ist „zu groß“