Improved Security Analyses for CBC MACs

Mihir Bellare
University of California, San Diego

Krzysztof Pietrzak
ETH Zürich

Phillip Rogaway
University of California, Davis

August 18, 2005

The CBC function

$[n] = \{0,1\}^n$, $\pi : [n] \to [n]$.

The CBC function $\mathrm{CBC}_\pi : [n]^* \to [n]$ is defined as

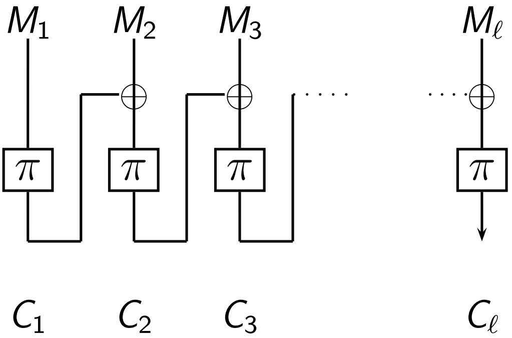
$\mathrm{CBC}_\pi(M_1 \| M_2 \| \dots \| M_\ell) = C_\ell$ where $C_0 = 0^n$, $C_i = \pi(M_i \oplus C_{i-1})$

The CBC function

$[n] = \{0,1\}^n$, $\pi : [n] \to [n]$.

The CBC function $\mathrm{CBC}_\pi : [n]^* \to [n]$ is defined as

$\mathrm{CBC}_\pi(M_1 \| M_2 \| \ldots \| M_\ell) = C_\ell$ where $C_0 = 0^n$, $C_i = \pi(M_i \oplus C_{i-1})$



The Encrypted-CBC (ECBC) function

$\pi_1 : [n] \to [n]$, $\pi_2 : [n] \to [n]$.

The ECBC function $\mathrm{ECBC}_{\pi_1,\pi_2} : [n]^* \to [n]$ is defined as

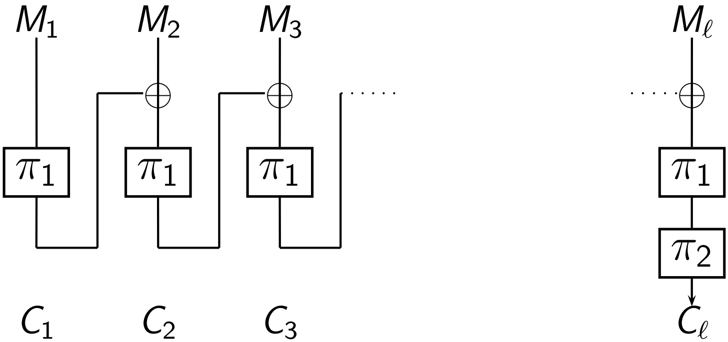
$$\mathrm{ECBC}_{\pi_1,\pi_2}(M) = \pi_2(\mathrm{CBC}_{\pi_1}(M))$$

The Encrypted-CBC (ECBC) function

$\pi_1 : [n] \to [n]$, $\pi_2 : [n] \to [n]$.

The ECBC function $\mathrm{ECBC}_{\pi_1,\pi_2} : [n]^* \to [n]$ is defined as

$$\mathrm{ECBC}_{\pi_1,\pi_2}(M) = \pi_2(\mathrm{CBC}_{\pi_1}(M))$$



Attack Models

$\mathcal{A}[\text{atk}, q, n, \ell]$ all attackers making q queries where each query

Attack Models

$\mathcal{A}[\mathsf{atk}, q, n, \ell]$ all attackers making q queries where each query

$\mathsf{atk} = \mathsf{any}$ has length at most ℓ n-bit blocks.

Attack Models

$\mathcal{A}[\text{atk}, q, n, \ell]$ all attackers making q queries where each query

$\text{atk} = \text{any}$ has length at most ℓ n-bit blocks.

$\text{atk} = \text{eq}$ has length exactly ℓ n-bit blocks.

Attack Models

$\mathcal{A}[\mathsf{atk}, q, n, \ell]$ all attackers making q queries where each query

$\mathsf{atk} = \mathsf{any}$	has length at most ℓ n-bit blocks.
$\mathsf{atk} = \mathsf{eq}$	has length exactly ℓ n-bit blocks.
$\mathsf{atk} = \mathsf{pf}$	has length at most ℓ n-bit blocks and none is the prefix of another.

Attack Models

$\mathcal{A}[\text{atk}, q, n, \ell]$ all attackers making q queries where each query

atk = any	has length at most ℓ n-bit blocks.
atk = eq	has length exactly ℓ n-bit blocks.
atk = pf	has length at most ℓ n-bit blocks and none is the prefix of another.

M is a prefix of M' if $M' = M \| M''$ for some M''.

Attack Models

$\mathcal{A}[\text{atk}, q, n, \ell]$ all attackers making q queries where each query

$\text{atk} = \text{any}$	has length at most ℓ n-bit blocks.
$\text{atk} = \text{eq}$	has length exactly ℓ n-bit blocks.
$\text{atk} = \text{pf}$	has length at most ℓ n-bit blocks and none is the prefix of another.

M is a prefix of M' if $M' = M \| M''$ for some M''.

$$\mathcal{A}[\text{eq}, q, n, \ell] \subseteq \mathcal{A}[\text{pf}, q, n, \ell] \subseteq \mathcal{A}[\text{any}, q, n, \ell]$$

Attack Models

$\mathcal{A}[\text{atk}, q, n, \ell]$ all attackers making q queries where each query

$\text{atk} = \text{any}$	has length at most ℓ n-bit blocks.
$\text{atk} = \text{eq}$	has length exactly ℓ n-bit blocks.
$\text{atk} = \text{pf}$	has length at most ℓ n-bit blocks and none is the prefix of another.

M is a prefix of M' if $M' = M \| M''$ for some M''.

$$\mathcal{A}[\text{eq}, q, n, \ell] \subseteq \mathcal{A}[\text{pf}, q, n, \ell] \subseteq \mathcal{A}[\text{any}, q, n, \ell]$$

$$\mathbf{Adv}_{\mathrm{CBC}}(A) = \Pr[\pi \xleftarrow{\$} \mathit{Perm}(n); A^{\mathrm{CBC}_\pi} \Rightarrow 1] - \Pr[f \xleftarrow{\$} \mathit{Func}(n); A^{f} \Rightarrow 1]$$

$$\boxed{\mathbf{Adv}^{\text{atk}}_{\mathrm{CBC}}(q, n, \ell) = \max_{A \in \mathcal{A}[\text{atk}, q, n, \ell]} \mathbf{Adv}_{\mathrm{CBC}}(A)}$$

Known Results

Known bounds for CBC

Known Results

Known bounds for CBC

BKR94 $\mathbf{Adv}^{\mathrm{eq}}_{\mathrm{CBC}}(q, n, \ell) \le c \cdot \ell^2 q^2 / 2^n$

Known Results

Known bounds for CBC

BKR94 $\mathbf{Adv}^{\mathrm{eq}}_{\mathrm{CBC}}(q, n, \ell) \leq c \cdot \ell^2 q^2 / 2^n$

PR00 $\mathbf{Adv}^{\mathrm{pf}}_{\mathrm{CBC}}(q, n, \ell) \leq c \cdot \ell^2 q^2 / 2^n$

Known Results

Known bounds for CBC

BKR94	$\mathbf{Adv}^{\mathrm{eq}}_{\mathrm{CBC}}(q, n, \ell) \leq c \cdot \ell^2 q^2 / 2^n$
PR00	$\mathbf{Adv}^{\mathrm{pf}}_{\mathrm{CBC}}(q, n, \ell) \leq c \cdot \ell^2 q^2 / 2^n$
folklore	$\mathbf{Adv}^{\mathrm{any}}_{\mathrm{CBC}}(2, n, 2) \approx 1$

Known Results

Known bounds for CBC

BKR94 $\mathbf{Adv}^{\mathrm{eq}}_{\mathrm{CBC}}(q, n, \ell) \leq c \cdot \ell^2 q^2 / 2^n$

PR00 $\mathbf{Adv}^{\mathrm{pf}}_{\mathrm{CBC}}(q, n, \ell) \leq c \cdot \ell^2 q^2 / 2^n$

folklore $\mathbf{Adv}^{\mathrm{any}}_{\mathrm{CBC}}(2, n, 2) \approx 1$

$CBC_\pi(0^n) = \pi(0^n) = Y$

Known Results

Known bounds for CBC

BKR94 $\mathbf{Adv}^{\mathrm{eq}}_{\mathrm{CBC}}(q, n, \ell) \leq c \cdot \ell^2 q^2 / 2^n$

PR00 $\mathbf{Adv}^{\mathrm{pf}}_{\mathrm{CBC}}(q, n, \ell) \leq c \cdot \ell^2 q^2 / 2^n$

folklore $\mathbf{Adv}^{\mathrm{any}}_{\mathrm{CBC}}(2, n, 2) \approx 1$

$CBC_\pi(0^n) = \pi(0^n) = Y$

$CBC_\pi(0^n \| Y) = \pi(\pi(0^n) \oplus Y) = \pi(Y \oplus Y) = \pi(0^n) = Y$

Known Results

Known bounds for CBC

BKR94	$\mathbf{Adv}^{\mathrm{eq}}_{\mathrm{CBC}}(q, n, \ell) \leq c \cdot \ell^2 q^2 / 2^n$
PR00	$\mathbf{Adv}^{\mathrm{pf}}_{\mathrm{CBC}}(q, n, \ell) \leq c \cdot \ell^2 q^2 / 2^n$
folklore	$\mathbf{Adv}^{\mathrm{any}}_{\mathrm{CBC}}(2, n, 2) \approx 1$

Known bounds for ECBC

PR00	$\mathbf{Adv}^{\mathrm{any}}_{\mathrm{ECBC}}(q, n, \ell) \leq c \cdot \ell^2 q^2 / 2^n$

Known Results

Known bounds for CBC

BKR94	$\mathbf{Adv}^{\text{eq}}_{\text{CBC}}(q, n, \ell) \leq c \cdot \ell^2 q^2 / 2^n$
PR00	$\mathbf{Adv}^{\text{pf}}_{\text{CBC}}(q, n, \ell) \leq c \cdot \ell^2 q^2 / 2^n$
folklore	$\mathbf{Adv}^{\text{any}}_{\text{CBC}}(2, n, 2) \approx 1$

Known bounds for ECBC

PR00	$\mathbf{Adv}^{\text{any}}_{\text{ECBC}}(q, n, \ell) \leq c \cdot \ell^2 q^2 / 2^n$
DGHKR04	$\mathbf{Adv}^{\text{eq}}_{\text{ECBC}}(q, n, \ell) \leq c \cdot q^2 / 2^n$ for $\ell \leq 2^{n/2}$.

Known Results

Known bounds for CBC

BKR94	$\mathbf{Adv}^{\mathrm{eq}}_{\mathrm{CBC}}(q, n, \ell) \leq c \cdot \ell^2 q^2 / 2^n$
PR00	$\mathbf{Adv}^{\mathrm{pf}}_{\mathrm{CBC}}(q, n, \ell) \leq c \cdot \ell^2 q^2 / 2^n$ tight for $\ell \in O(1)$
folklore	$\mathbf{Adv}^{\mathrm{any}}_{\mathrm{CBC}}(2, n, 2) \approx 1$

Known bounds for ECBC

PR00	$\mathbf{Adv}^{\mathrm{any}}_{\mathrm{ECBC}}(q, n, \ell) \leq c \cdot \ell^2 q^2 / 2^n$ tight for $\ell \in O(1)$
DGHKR04	$\mathbf{Adv}^{\mathrm{eq}}_{\mathrm{ECBC}}(q, n, \ell) \leq c \cdot q^2 / 2^n$ for $\ell \leq 2^{n/2}$.

$$\mathbf{Adv}^{\mathrm{eq}}_{\mathrm{CBC}}(2^{n/2}, n, \ell) = \Theta(1)$$

$$\mathbf{Adv}^{\mathrm{eq}}_{\mathrm{ECBC}}(2^{n/2}, n, \ell) = \Theta(1)$$

Our Results

Improve prefix free CBC from $\ell^2 \cdot q^2/2^n$ to:

Theorem

$$\mathbf{Adv}^{\mathrm{pf}}_{\mathrm{CBC}}(q, n, \ell) \leq c \cdot \ell \cdot q^2/2^n \qquad \textit{for} \qquad \ell \leq 2^{n/3}$$

Our Results

Improve prefix free CBC from $\ell^2 \cdot q^2/2^n$ to:

Theorem

$$\mathbf{Adv}^{\mathrm{pf}}_{\mathrm{CBC}}(q, n, \ell) \leq c \cdot \ell \cdot q^2/2^n \qquad \textit{for} \qquad \ell \leq 2^{n/3}$$

Improve ECBC from $c \cdot \ell^2 \cdot q^2/2^n$ to:

Theorem

$$\mathbf{Adv}^{\mathrm{any}}_{\mathrm{CBC}}(q, n, \ell) \leq c \cdot \ell^{1/\ln \ln \ell} \cdot q^2/2^n \qquad \textit{for} \qquad \ell \leq 2^{n/4}$$

Permutation vs. Functions

$$\mathrm{CBC} = \{\mathrm{CBC}_\pi; \pi \xleftarrow{\$} Perm(n)\}$$

$$\mathrm{CBC}' = \{\mathrm{CBC}_f; f \xleftarrow{\$} Func(n)\}$$

$$\mathbf{Adv}^{\mathrm{pf}}_{\mathrm{CBC}}(q = 2^{n/4}, n, \ell = 2^{n/4}) \approx \ell \cdot q^2/2^n \leq 2^{-n/4}$$

$$\mathbf{Adv}^{\mathrm{pf}}_{\mathrm{CBC}'}(q = 2^{n/4}, n, \ell = 2^{n/4}) = \Theta(1) \qquad \text{[Berke04]}$$

ECBC and the Carter-Wegman Paradigm

$$\mathrm{ECBC}_{\pi_1,\pi_2}(.) = \pi_2(\mathrm{CBC}_{\pi_1}(.))$$

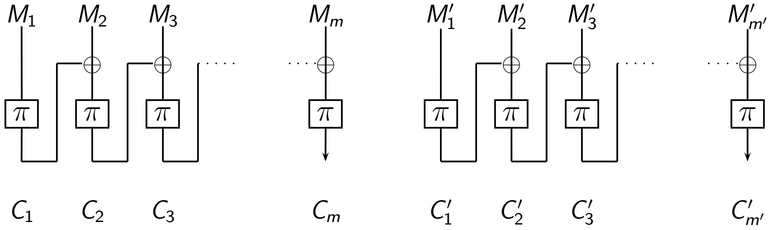
$$\mathbf{CP}_n(M, M') = \Pr[\pi \leftarrow \mathit{Perm}(n); \mathrm{CBC}_\pi(M) = \mathrm{CBC}_\pi(M')]$$

$$\mathbf{CP}^{\mathrm{any}}_{n,\ell} = \max_{M, M', |M| \le \ell n, |M'| \le \ell n} \mathbf{CP}_n(M, M')$$

$$\boxed{\mathbf{Adv}^{\mathrm{any}}_{\mathrm{ECBC}}(q, n, \ell) \le q^2 \cdot \mathbf{CP}^{\mathrm{any}}_{n,\ell}}$$

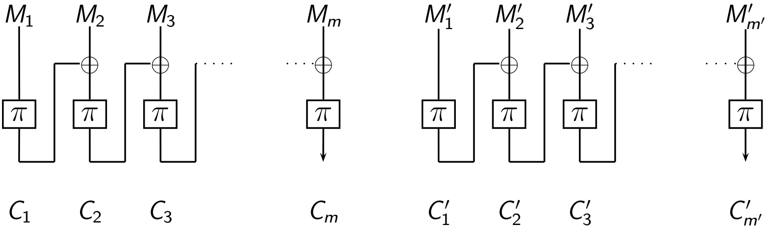
CBC and the Full Collision Probability

$$M = M_1 \| M_2 \| \ldots M_m \text{ and } M' = M'_1 \| M'_2 \| \ldots M'_{m'}$$



CBC and the Full Collision Probability

$$M = M_1 \| M_2 \| \ldots M_m \text{ and } M' = M'_1 \| M'_2 \| \ldots M'_{m'}$$



$$\mathbf{FCP}_n(M, M') = \Pr[\pi \leftarrow Perm(n);\, C'_{m'} \in \{C_1, \ldots, C_m, C'_1, \ldots, C'_{m'-1}\}]$$

$$\mathbf{FCP}^{\mathrm{pf}}_{n,\ell} = \max_{M, M', |M| \leq \ell n, |M'| \leq \ell n} \mathbf{FCP}_n(M, M')$$

$$\boxed{\mathbf{Adv}^{\mathsf{any}}_{\mathsf{ECBC}}(q,n,\ell) \le q^2 \cdot \mathbf{CP}^{\mathsf{any}}_{n,\ell}}$$

$$\boxed{\mathbf{Adv}^{\mathsf{pf}}_{\mathsf{CBC}}(q,n,\ell) \le q^2 \cdot \mathbf{FCP}^{\mathsf{pf}}_{n,\ell} + \frac{4mq^2}{2^n}}$$

$$\boxed{\mathbf{Adv}_{\mathrm{ECBC}}^{\mathrm{any}}(q,n,\ell) \le q^2 \cdot \mathbf{CP}_{n,\ell}^{\mathrm{any}}}$$

Lemma

$$\mathbf{CP}_{n,\ell}^{\mathrm{any}} \le \frac{2d(\ell)}{2^n} + \frac{8\ell^4}{2^{2n}}$$

Where $d(\ell) \le \ell^{1/\ln\ln\ell} = o(\ell)$ is the maximum number of divisors of any $m \le \ell$.

$$\boxed{\mathbf{Adv}_{\mathrm{CBC}}^{\mathrm{pf}}(q,n,\ell) \le q^2 \cdot \mathbf{FCP}_{n,\ell}^{\mathrm{pf}} + \frac{4mq^2}{2^n}}$$

$$\boxed{\mathbf{Adv}^{\mathrm{any}}_{\mathrm{ECBC}}(q,n,\ell) \le q^2 \cdot \mathbf{CP}^{\mathrm{any}}_{n,\ell}}$$

Lemma

$$\mathbf{CP}^{\mathrm{any}}_{n,\ell} \le \frac{2d(\ell)}{2^n} + \frac{8\ell^4}{2^{2n}}$$

Where $d(\ell) \le \ell^{1/\ln\ln\ell} = o(\ell)$ is the maximum number of divisors of any $m \le \ell$.

$$\boxed{\mathbf{Adv}^{\mathrm{pf}}_{\mathrm{CBC}}(q,n,\ell) \le q^2 \cdot \mathbf{FCP}^{\mathrm{pf}}_{n,\ell} + \frac{4mq^2}{2^n}}$$

Lemma

$$\mathbf{FCP}^{\mathrm{pf}}_{n,\ell} \le \frac{8\ell}{2^n} + \frac{8\ell^4}{2^{2n}}$$

The Game-Playing Technique [BR05]

On the s^{th} **query** $F(M_s)$ Game D1

$m_s \leftarrow |M_s|_n, \quad C_s^0 \leftarrow 0^n$
for $i \leftarrow 1$ **to** $m_s - 1$ **do**
  $X_s^i \leftarrow C_s^{i-1} \oplus M_s^i$
  if $X_s^i \in \mathrm{Dom}(\pi)$ **then** $C_s^i \leftarrow \pi(X_s^i)$
    else $\pi(X_s^i) \leftarrow C_s^i \xleftarrow{\$} \overline{\mathrm{Ran}}(\pi)$
$X_s^{m_s} \leftarrow C_s^{m_s-1} \oplus M_s^{m_s}$
$\widehat{C}_s^{m_s} \leftarrow C_s^{m_s} \xleftarrow{\$} \{0,1\}^n$
if $C_s^{m_s} \in \mathrm{Ran}(\pi)$: *bad* $\leftarrow 1$, $C_s^{m_s} \xleftarrow{\$} \overline{\mathrm{Ran}}(\pi)$
if $X_s^{m_s} \in \mathrm{Dom}(\pi)$: *bad* $\leftarrow 1$, $C_s^{m_s} \leftarrow \pi(X_s^{m_s})$
$\pi(X_s^{m_s}) \leftarrow C_s^{m_s}$
if *bad* **then** **return** $C_s^{m_s}$
return $\widehat{C}_s^{m_s}$

D1 implements CBC.

The Game-Playing Technique [BR05]

On the s^{th} **query** $F(M_s)$ — Game D0

$m_s \leftarrow |M_s|_n, \quad C_s^0 \leftarrow 0^n$
for $i \leftarrow 1$ **to** $m_s - 1$ **do**
  $X_s^i \leftarrow C_s^{i-1} \oplus M_s^i$
  if $X_s^i \in \mathrm{Dom}(\pi)$ **then** $C_s^i \leftarrow \pi(X_s^i)$
    else $\pi(X_s^i) \leftarrow C_s^i \xleftarrow{\$} \overline{\mathrm{Ran}}(\pi)$
$X_s^{m_s} \leftarrow C_s^{m_s-1} \oplus M_s^{m_s}$
$\widehat{C}_s^{m_s} \leftarrow C_s^{m_s} \xleftarrow{\$} \{0,1\}^n$
if $C_s^{m_s} \in \mathrm{Ran}(\pi)$: $bad \leftarrow 1$, $C_s^{m_s} \xleftarrow{\$} \overline{\mathrm{Ran}}(\pi)$
if $X_s^{m_s} \in \mathrm{Dom}(\pi)$: $bad \leftarrow 1$, $C_s^{m_s} \leftarrow \pi(X_s^{m_s})$
$\pi(X_s^{m_s}) \leftarrow C_s^{m_s}$
if bad **then** **return** $C_s^{m_s}$
return $\widehat{C}_s^{m_s}$

D1 implements CBC.

D0 implements a random function.

The Game-Playing Technique [BR05]

On the s^{th} **query** $F(M_s)$ Game D0

$m_s \leftarrow |M_s|_n, \quad C_s^0 \leftarrow 0^n$

for $i \leftarrow 1$ **to** $m_s - 1$ **do**

$\quad X_s^i \leftarrow C_s^{i-1} \oplus M_s^i$

$\quad$ **if** $X_s^i \in \mathrm{Dom}(\pi)$ **then** $C_s^i \leftarrow \pi(X_s^i)$

$\quad\quad$ **else** $\pi(X_s^i) \leftarrow C_s^i \xleftarrow{\$} \overline{\mathrm{Ran}}(\pi)$

$X_s^{m_s} \leftarrow C_s^{m_s-1} \oplus M_s^{m_s}$

$\widehat{C}_s^{m_s} \leftarrow C_s^{m_s} \xleftarrow{\$} \{0,1\}^n$

if $C_s^{m_s} \in \mathrm{Ran}(\pi)$: $bad \leftarrow 1$, $C_s^{m_s} \xleftarrow{\$} \overline{\mathrm{Ran}}(\pi)$

if $X_s^{m_s} \in \mathrm{Dom}(\pi)$: $bad \leftarrow 1$, $C_s^{m_s} \leftarrow \pi(X_s^{m_s})$

$\pi(X_s^{m_s}) \leftarrow C_s^{m_s}$

if bad **then** **return** $C_s^{m_s}$

return $\widehat{C}_s^{m_s}$

D1 implements CBC.

D0 implements a random function.

$$\mathbf{Adv}_{\mathrm{CBC}}(A) = \Pr[A^{D0} \Rightarrow 1] - \Pr[A^{D1} \Rightarrow 1]$$

The Game-Playing Technique [BR05]

On the s^{th} **query** $F(M_s)$ Game D0

$m_s \leftarrow |M_s|_n, \quad C_s^0 \leftarrow 0^n$
for $i \leftarrow 1$ **to** $m_s - 1$ **do**
    $X_s^i \leftarrow C_s^{i-1} \oplus M_s^i$
    if $X_s^i \in \mathrm{Dom}(\pi)$ **then** $C_s^i \leftarrow \pi(X_s^i)$
        else $\pi(X_s^i) \leftarrow C_s^i \xleftarrow{\$} \overline{\mathrm{Ran}}(\pi)$
$X_s^{m_s} \leftarrow C_s^{m_s-1} \oplus M_s^{m_s}$
$\widehat{C}_s^{m_s} \leftarrow C_s^{m_s} \xleftarrow{\$} \{0,1\}^n$
if $C_s^{m_s} \in \mathrm{Ran}(\pi)$: $bad \leftarrow 1$, $\boxed{C_s^{m_s} \xleftarrow{\$} \overline{\mathrm{Ran}}(\pi)}$
if $X_s^{m_s} \in \mathrm{Dom}(\pi)$: $bad \leftarrow 1$, $\boxed{C_s^{m_s} \leftarrow \pi(X_s^{m_s})}$
$\pi(X_s^{m_s}) \leftarrow C_s^{m_s}$
if bad **then** $\boxed{\textbf{return } C_s^{m_s}}$
return $\widehat{C}_s^{m_s}$

D1 implements CBC.

D0 implements a random function.

$$\mathbf{Adv}_{\mathrm{CBC}}(A) = \Pr[A^{D0} \Rightarrow 1] - \Pr[A^{D1} \Rightarrow 1] \le \Pr[A^{D0} \text{ sets } bad]$$

The Game-Playing Technique Cnt.

Game D7

$\pi \xleftarrow{\$} \mathrm{Perm}(n)$

$C_1^0 \leftarrow C_2^0 \leftarrow 0^n$

for $i \leftarrow 1$ **to** $\mathtt{m}_1$ **do**

  $X_1^i \leftarrow C_1^{i-1} \oplus \mathtt{M}_1^i,\ C_1^i \leftarrow \pi(X_1^i)$

for $i \leftarrow 1$ **to** $\mathtt{m}_2$ **do**

  $X_2^i \leftarrow C_2^{i-1} \oplus \mathtt{M}_2^i,\ C_2^i \leftarrow \pi(X_2^i)$

$\mathit{bad} \leftarrow X_2^{\mathtt{m}_2} \in \{X_1^1, \ldots, X_1^{\mathtt{m}_1},$
$X_2^1, \ldots, X_2^{\mathtt{m}_2-1}\}$

The Game-Playing Technique Cnt.

Game D7

$\pi \xleftarrow{\$} \mathrm{Perm}(n)$

$C_1^0 \leftarrow C_2^0 \leftarrow 0^n$

for $i \leftarrow 1$ **to** $\mathtt{m}_1$ **do**

  $X_1^i \leftarrow C_1^{i-1} \oplus \mathtt{M}_1^i,\ C_1^i \leftarrow \pi(X_1^i)$

for $i \leftarrow 1$ **to** $\mathtt{m}_2$ **do**

  $X_2^i \leftarrow C_2^{i-1} \oplus \mathtt{M}_2^i,\ C_2^i \leftarrow \pi(X_2^i)$

$\color{red}{bad} \leftarrow X_2^{\mathtt{m}_2} \in \{X_1^1, \ldots, X_1^{\mathtt{m}_1},$

$X_2^1, \ldots, X_2^{\mathtt{m}_2-1}\}$

$$\Pr[A^{D7} \text{ sets } \color{red}{bad}] = \mathbf{FCP}_n(\mathtt{M}_1^1 \| \ldots \| \mathtt{M}_{\mathtt{m}_1}^1, \mathtt{M}_1^2 \| \ldots \| \mathtt{M}_{\mathtt{m}_2}^2)$$

The Game-Playing Technique Cnt.

On the s^{th} **query** $F(M_s)$ — Game D1

$m_s \leftarrow |M_s|_n, \quad C_s^0 \leftarrow 0^n$
for $i \leftarrow 1$ **to** $m_s - 1$ **do**
  $X_s^i \leftarrow C_s^{i-1} \oplus M_s^i$
  if $X_s^i \in \mathrm{Dom}(\pi)$ **then** $C_s^i \leftarrow \pi(X_s^i)$
    else $\pi(X_s^i) \leftarrow C_s^i \xleftarrow{\$} \overline{\mathrm{Ran}}(\pi)$
$X_s^{m_s} \leftarrow C_s^{m_s-1} \oplus M_s^{m_s}$
$\widehat{C}_s^{m_s} \leftarrow C_s^{m_s} \xleftarrow{\$} \{0,1\}^n$
if $C_s^{m_s} \in \mathrm{Ran}(\pi)$: $\textit{bad} \leftarrow 1$, $C_s^{m_s} \xleftarrow{\$} \overline{\mathrm{Ran}}(\pi)$
if $X_s^{m_s} \in \mathrm{Dom}(\pi)$: $\textit{bad} \leftarrow 1$, $C_s^{m_s} \leftarrow \pi(X_s^{m_s})$
$\pi(X_s^{m_s}) \leftarrow C_s^{m_s}$
if *bad* **then return** $C_s^{m_s}$
return $\widehat{C}_s^{m_s}$

. . . .

Game D7

$\pi \xleftarrow{\$} \mathrm{Perm}(n)$
$C_1^0 \leftarrow C_2^0 \leftarrow 0^n$
for $i \leftarrow 1$ **to** $\mathtt{m}_1$ **do**
  $X_1^i \leftarrow C_1^{i-1} \oplus \mathtt{M}_1^i$, $C_1^i \leftarrow \pi(X_1^i)$
for $i \leftarrow 1$ **to** $\mathtt{m}_2$ **do**
  $X_2^i \leftarrow C_2^{i-1} \oplus \mathtt{M}_2^i$, $C_2^i \leftarrow \pi(X_2^i)$
bad $\leftarrow X_2^{\mathtt{m}_2} \in \{X_1^1, \ldots, X_1^{\mathtt{m}_1},$
  $X_2^1, \ldots, X_2^{\mathtt{m}_2 - 1}\}$

$$\Pr[A^{D1} \text{ sets } \textit{bad}] \leq q^2 \cdot \Pr[A^{D7} \text{ sets } \textit{bad}] + \frac{4\ell q^2}{2^n}$$

$$\mathbf{Adv}^{\mathrm{pf}}_{\mathrm{CBC}}(q, n, \ell) \leq q^2 \cdot \mathbf{FCP}^{\mathrm{pf}}_{n,\ell} + \frac{4\ell q^2}{2^n}$$

$$\boxed{\mathbf{Adv}^{\text{any}}_{\text{ECBC}}(q, n, \ell) \leq q^2 \cdot \mathbf{CP}^{\text{any}}_{n,\ell}}$$

Lemma

$$\mathbf{CP}^{\text{any}}_{n,\ell} \leq \frac{2d(\ell)}{2^n} + \frac{8\ell^4}{2^{2n}}$$

Where $d(\ell) \leq \ell^{1/\ln\ln\ell} = o(\ell)$ is the maximum number of divisors of any $m \leq \ell$.

$$\boxed{\mathbf{Adv}^{\text{pf}}_{\text{CBC}}(q, n, \ell) \leq q^2 \cdot \mathbf{FCP}^{\text{pf}}_{n,\ell} + \frac{4mq^2}{2^n}}$$

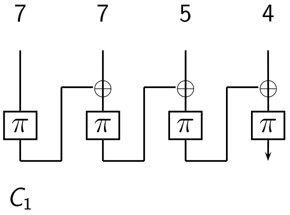
Lemma

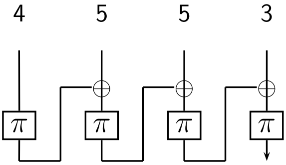
$$\mathbf{FCP}^{\text{pf}}_{n,\ell} \leq \frac{8\ell}{2^n} + \frac{8\ell^4}{2^{2n}}$$

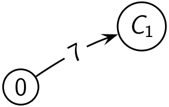
A Graph-Based Representation of CBC [DGHKR04]

0

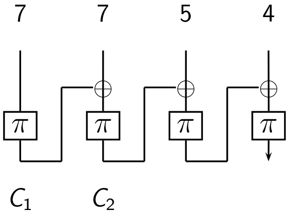
A Graph-Based Representation of CBC [DGHKR04]

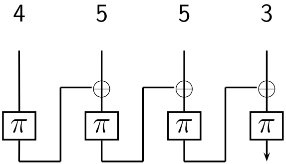


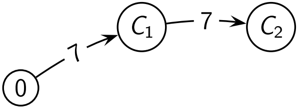




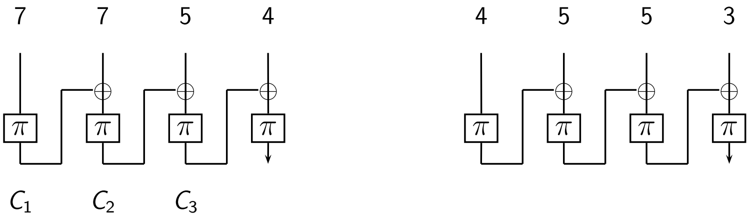
A Graph-Based Representation of CBC [DGHKR04]

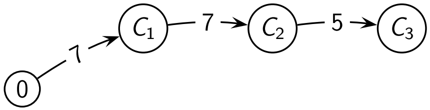




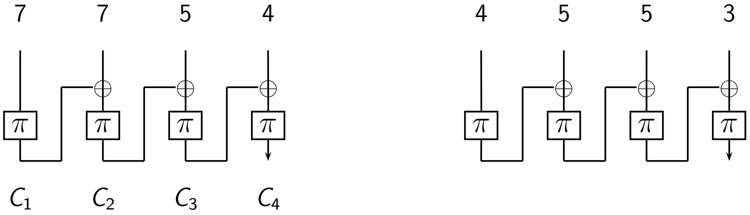


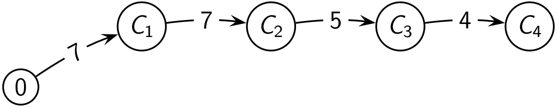
A Graph-Based Representation of CBC [DGHKR04]



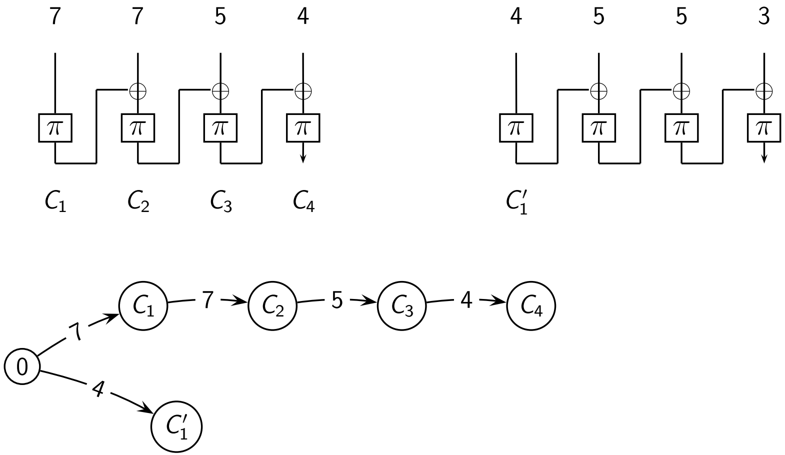


A Graph-Based Representation of CBC [DGHKR04]

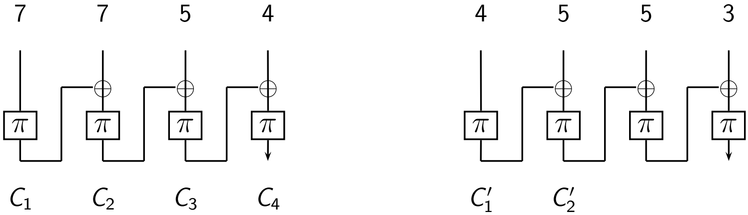




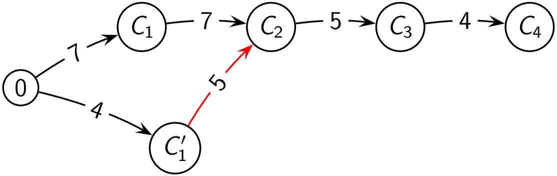
A Graph-Based Representation of CBC [DGHKR04]



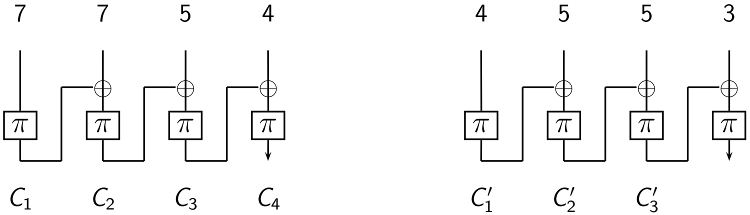
A Graph-Based Representation of CBC [DGHKR04]



Accident: $C'_2 = C_2$

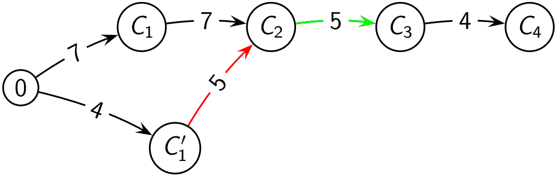


A Graph-Based Representation of CBC [DGHKR04]

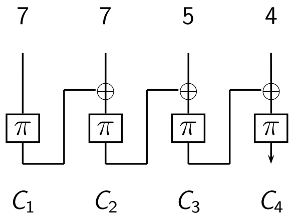


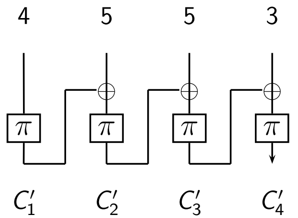
Accident: $C'_2 = C_2$

Induced Collision: $C'_3 = C_3$

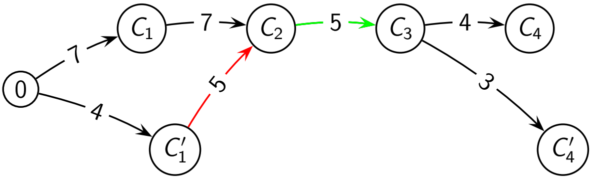


A Graph-Based Representation of CBC [DGHKR04]





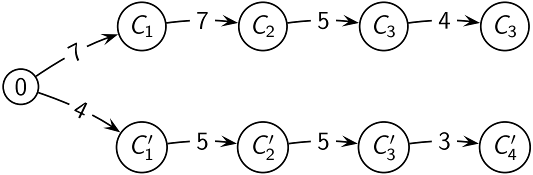
Accident: $C'_2 = C_2$ Induced Collision: $C'_3 = C_3$



Structure Graph G_π, $\mathrm{Acc}(G_\pi) = 1$

Structure Graphs

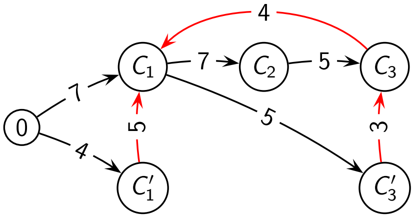
$M = 7\|7\|5\|4 \qquad M' = 4\|5\|5\|3$



$\mathrm{Acc}(H) = 0$

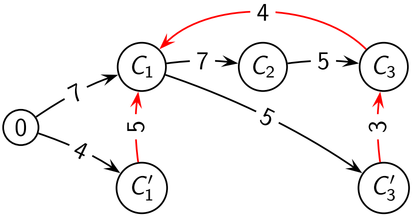
Structure Graphs

$M = 7 \| 7 \| 5 \| 4 \qquad M' = 4 \| 5 \| 5 \| 3 \qquad \mathrm{Acc}(H) = 3$



Structure Graphs

$M = 7 \| 7 \| 5 \| 4$ $\qquad M' = 4 \| 5 \| 5 \| 3$ $\qquad \mathsf{Acc}(H) = 3$



Lemma

$$\Pr[\pi \xleftarrow{\$} \mathrm{Perm}(n);\, G_\pi = H] \leq (2^n - 2\ell)^{-\mathsf{Acc}(H)}$$

$$M = 7\|7\|5\|4 \qquad M' = 4\|5\|5\|3$$

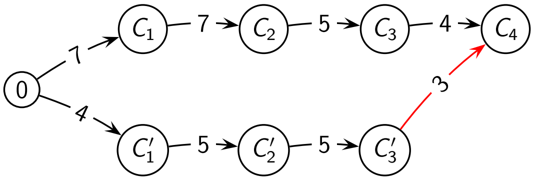
$$\mathbf{CP}_n(M, M') \;=\; \Pr[\pi \xleftarrow{\$} \mathrm{Perm}(n);\, \mathsf{CBC}_\pi(M) = \mathsf{CBC}_\pi(M')]$$

$$M = 7 \| 7 \| 5 \| 4 \qquad M' = 4 \| 5 \| 5 \| 3$$

$$\begin{aligned} \mathbf{CP}_n(M, M') &= \Pr[\pi \xleftarrow{\$} \mathrm{Perm}(n); \mathsf{CBC}_\pi(M) = \mathsf{CBC}_\pi(M')] \\ &= \Pr[\pi \xleftarrow{\$} \mathrm{Perm}(n); G_\pi \text{ satisfies } C_4 = C'_4] \end{aligned}$$

$$M = 7\|7\|5\|4 \qquad M' = 4\|5\|5\|3$$

$$\begin{aligned}\mathbf{CP}_n(M, M') &= \Pr[\pi \xleftarrow{\$} \mathrm{Perm}(n); \mathsf{CBC}_\pi(M) = \mathsf{CBC}_\pi(M')] \\ &= \Pr[\pi \xleftarrow{\$} \mathrm{Perm}(n); G_\pi \text{ satisfies } C_4 = C'_4]\end{aligned}$$



$$M = 7 \| 7 \| 5 \| 4 \qquad M' = 4 \| 5 \| 5 \| 3 \qquad \ell = 4$$

$$\mathbf{CP}_n(M, M') = \Pr[G_\pi \text{ satisfies } C_4 = C'_4]$$

$$\leq \Pr[\mathsf{Acc}(G_\pi) = 1 \text{ and } G_\pi \text{ satisfies } C_4 = C'_4] + \Pr[\mathsf{Acc}(G_\pi) \geq 2]$$

$$\leq \frac{\#G[\text{ with 1 accident where } C_4 = C'_4]}{2^n - 2 \cdot \ell} + \frac{8 \cdot \ell^2}{2^{2n}}$$

Lemma

$$\Pr[\pi \xleftarrow{\$} \mathrm{Perm}(n);\, G_\pi = H] \leq (2^n - 2\ell)^{-\mathsf{Acc}(H)}$$

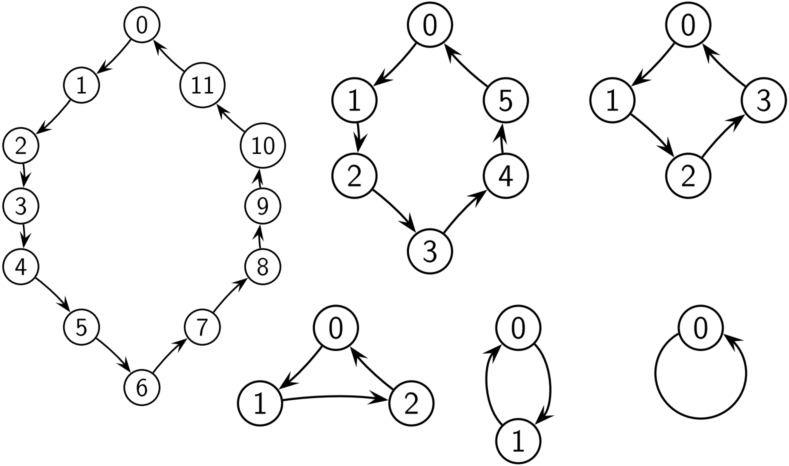
M, M' with $m = |M|, m' = |M'|$, $\ell = \max(m, m')$.

$$\mathbf{CP}_n(M, M') \leq \frac{\boxed{\#G[\text{ with 1 acc. where } C_m = C'_{m'}]}}{2^n - 2 \cdot \ell} + \frac{8 \cdot \ell^2}{2^{2n}}$$

Lemma

$$\#[G \textit{ with 1 acc. where } C_m = C'_{m'}] \leq d(\ell)$$

Where $d(\ell) \leq \ell^{1/\ln\ln\ell} = o(\ell)$ is the maximum number of divisors of any $m \leq \ell$, e.g. $d(15) = 6$ as $12 \leq 15$ has 6 divisors $1, 2, 3, 4, 6, 12$.



Questions?