Towards an Improved Bound on CBC Collision Probability and Its Applications

Ashwin Jha, Mridul Nandi

Indian Statistical Institute, Kolkata

India Crypto Meet
16-17 July, 2020

Overview

Towards an improved bound on CBC collision probability and its applications.

Overview

Towards an improved bound on CBC collision probability and its applications.

- What is CBC?

Overview

Towards an improved bound on CBC collision probability and its applications.

- What is CBC?
- Collision probability of CBC.

Overview

Towards an improved bound on CBC collision probability and its applications.

- What is CBC?
- Collision probability of CBC.
- Applications of a “good” bound.

Overview

Towards an improved bound on CBC collision probability and its applications.

- What is CBC?
- Collision probability of CBC.
- Applications of a “good” bound.
- How to get good bounds?
  - Existing techniques and results.
  - Some new insights and results.

Overview

Towards an improved bound on CBC collision probability and its applications.

- What is CBC?
- Collision probability of CBC.
- Applications of a “good” bound.
- How to get good bounds?
  - Existing techniques and results.
  - Some new insights and results. (Work in progress!)

Cipher Block Chaining or CBC

Cipher Block Chaining or CBC

- For a permutation π over $\mathbb{B} := \{0,1\}^n$ and $M \in \mathbb{B}^+$:

Cipher Block Chaining or CBC

- For a permutation π over $\mathbb{B} := \{0,1\}^n$ and $M \in \mathbb{B}^+$:

M_1 M_2 $\cdots\cdots$ M_ℓ

Cipher Block Chaining or CBC

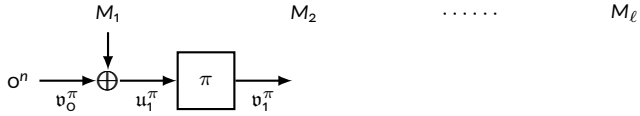
- For a permutation π over $\mathbb{B} := \{0,1\}^n$ and $M \in \mathbb{B}^+$:

M_1 M_2 $\cdots\cdots$ M_ℓ

0^n

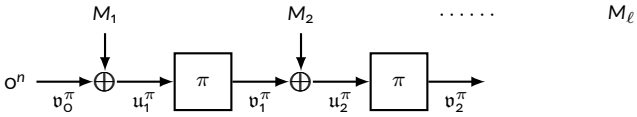
Cipher Block Chaining or CBC

- For a permutation π over $\mathbb{B} := \{0,1\}^n$ and $M \in \mathbb{B}^+$:



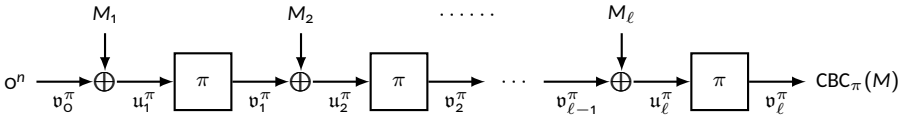
Cipher Block Chaining or CBC

- For a permutation π over $\mathbb{B} := \{0,1\}^n$ and $M \in \mathbb{B}^+$:



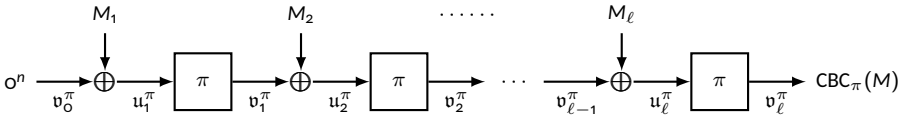
Cipher Block Chaining or CBC

- For a permutation π over $\mathbb{B} := \{0,1\}^n$ and $M \in \mathbb{B}^+$:



Cipher Block Chaining or CBC

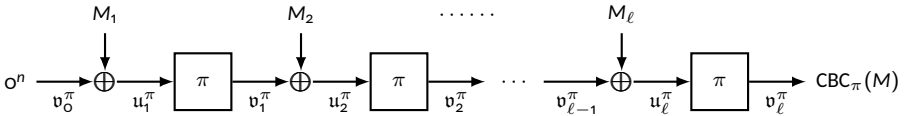
- For a permutation π over $\mathbb{B} := \{0,1\}^n$ and $M \in \mathbb{B}^+$:



- Invented in context of authentication (CBC-MAC [EMST, US Patent '78]).

Cipher Block Chaining or CBC

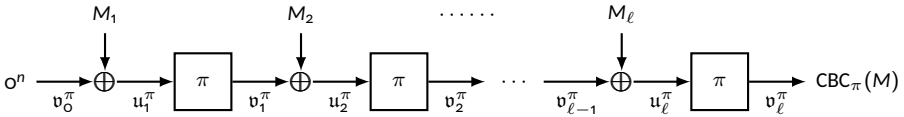
- For a permutation π over $\mathbb{B} := \{0,1\}^n$ and $M \in \mathbb{B}^+$:



- Invented in context of authentication (CBC-MAC [EMST, US Patent '78]).
- Two issues with CBC:

Cipher Block Chaining or CBC

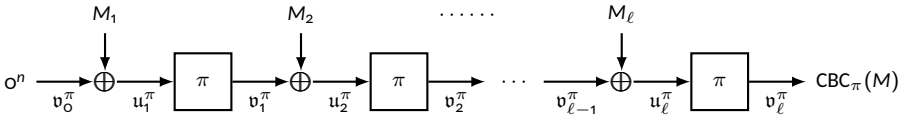
- For a permutation π over $\mathbb{B} := \{0,1\}^n$ and $M \in \mathbb{B}^+$:



- Invented in context of authentication (CBC-MAC [EMST, US Patent '78]).
- Two issues with CBC:
  1. Domain restricted to complete blocks, i.e., $\mathbb{B}^+$.

Cipher Block Chaining or CBC

- For a permutation π over $\mathbb{B} := \{0,1\}^n$ and $M \in \mathbb{B}^+$:



- Invented in context of authentication (CBC-MAC [EMST, US Patent '78]).
- Two issues with CBC:
  1. Domain restricted to complete blocks, i.e., $\mathbb{B}^+$.
  2. Trivial PRF distinguishers exist when messages are chosen arbitrarily from $\mathbb{B}^+$.

CBC Variants

Several variants of CBC-MAC overcome these shortcomings:

CBC Variants

Several variants of CBC-MAC overcome these shortcomings:

- EMAC [BBB$^+$, Project RACE '95]: applies another permutation π_2 over CBC_{π_1}

$$\mathrm{EMAC}(M) := \pi_2(\mathrm{CBC}_{\pi_1}(M)).$$

  This fixes issue 2.

CBC Variants

Several variants of CBC-MAC overcome these shortcomings:

- EMAC [BBB$^+$, Project RACE '95]: applies another permutation π_2 over CBC_{π_1}

$$\mathsf{EMAC}(M) := \pi_2(\mathsf{CBC}_{\pi_1}(M)).$$

  This fixes issue 2.

- For an ℓ-block optionally padded message $\overline{M}^\dagger = (M_1, \ldots, M_\ell)$, we have
  - ECBC [BR, CRYPTO '00]: finalizes with π_2 or π_3 depending upon the last block

$$\mathsf{ECBC}(M) := \pi_b(\mathsf{CBC}_{\pi_1}(\overline{M})).$$

  - FCBC [BR, CRYPTO '00]: $\mathsf{FCBC}(M) := \pi_b(\mathsf{CBC}_{\pi_1}(M_{\ell-1|}) \oplus M_\ell)$.

  This fixes both issue 1 and 2.

† Here $\overline{M}$ denotes the optional 10^* padding of M so that the padded M has bit-length in multiple of n.

PRF Security of CBC Variants

PRF Security and CBC Output Collisions:

PRF Security of CBC Variants

PRF Security and CBC Output Collisions:

- For all $\mathsf{F} \in \{\mathsf{EMAC}, \mathsf{ECBC}, \mathsf{FCBC}\}$:
  - for distinct M, M': $\mathsf{F}(M) = \mathsf{F}(M')$ iff $\mathsf{F}(M\|X) = \mathsf{F}(M'\|X)$.
  - for such a distinguisher making q queries $(M_1, \ldots, M_q)$, we have

$$\mathbf{Adv}^{\mathrm{prf}}_{\mathsf{F}}(\mathscr{A}) \geq \Pr_{\Pi \xleftarrow{\$} \mathrm{Perm}(n)}[\exists i \neq j \in [q] : \mathrm{CBC}_{\Pi}(M_i) = \mathrm{CBC}_{\Pi}(M_j)] - O\left(\frac{q^2}{2^{2n}}\right).$$

PRF Security of CBC Variants

PRF Security and CBC Output Collisions:

- For all $\mathsf{F} \in \{\mathsf{EMAC}, \mathsf{ECBC}, \mathsf{FCBC}\}$:
  - for distinct M, M': $\mathsf{F}(M) = \mathsf{F}(M')$ iff $\mathsf{F}(M\|X) = \mathsf{F}(M'\|X)$.
  - for such a distinguisher making q queries $(M_1, \ldots, M_q)$, we have

$$\mathbf{Adv}^{\mathrm{prf}}_{\mathsf{F}}(\mathscr{A}) \geq \Pr_{\Pi \leftarrow\$ \mathrm{Perm}(n)}[\exists i \neq j \in [q] : \mathrm{CBC}_\Pi(M_i) = \mathrm{CBC}_\Pi(M_j)] - O\left(\frac{q^2}{2^{2n}}\right).$$

- Bellare et al. [BPR, CRYPTO '05] showed that

$$\mathbf{Adv}^{\mathrm{prf}}_{\mathsf{F}}(\mathscr{A}) \leq O\left(\frac{q^2}{2^n}\right) + \Pr_{\Pi \leftarrow\$ \mathrm{Perm}(n)}[\exists i \neq j \in [q] : \mathrm{CBC}_\Pi(M_i) = \mathrm{CBC}_\Pi(M_j)].$$

PRF Security of CBC Variants

PRF Security and CBC Output Collisions:

- For all $\mathsf{F} \in \{\mathsf{EMAC}, \mathsf{ECBC}, \mathsf{FCBC}\}$:
  - for distinct M, M': $\mathsf{F}(M) = \mathsf{F}(M')$ iff $\mathsf{F}(M\|X) = \mathsf{F}(M'\|X)$.
  - for such a distinguisher making q queries $(M_1, \ldots, M_q)$, we have

$$\mathbf{Adv}^{\mathrm{prf}}_{\mathsf{F}}(\mathscr{A}) \geq \Pr_{\Pi \leftarrow\$ \mathrm{Perm}(n)}[\exists i \neq j \in [q] : \mathrm{CBC}_\Pi(M_i) = \mathrm{CBC}_\Pi(M_j)] - O\left(\frac{q^2}{2^{2n}}\right).$$

- Bellare et al. [BPR, CRYPTO '05] showed that

$$\mathbf{Adv}^{\mathrm{prf}}_{\mathsf{F}}(\mathscr{A}) \leq O\left(\frac{q^2}{2^n}\right) + \Pr_{\Pi \leftarrow\$ \mathrm{Perm}(n)}[\exists i \neq j \in [q] : \mathrm{CBC}_\Pi(M_i) = \mathrm{CBC}_\Pi(M_j)].$$

A tight estimation of the probability of CBC output collision gives tight PRF bounds.

CBC Output Collision

CBC Output Collision

- Collision event: for two distinct messages M_1, M_2

$$\texttt{COLL}^{\Pi}(M_1, M_2): \quad \mathsf{CBC}_{\Pi}(M_1) = \mathsf{CBC}_{\Pi}(M_2)$$

CBC Output Collision

- Collision event: for two distinct messages M_1, M_2

$$\texttt{COLL}^{\Pi}(M_1, M_2) : \quad \mathsf{CBC}_{\Pi}(M_1) = \mathsf{CBC}_{\Pi}(M_2)$$

- Collision probability:

$$\mathsf{CP}(M_1, M_2) := \Pr_{\Pi \xleftarrow{\$} \mathsf{Perm}(n)} \left[\texttt{COLL}^{\Pi}(M_1, M_2)\right]$$

CBC Output Collision

- Collision event: for two distinct messages M_1, M_2

$$\mathtt{COLL}^{\Pi}(M_1, M_2) : \quad \mathrm{CBC}_{\Pi}(M_1) = \mathrm{CBC}_{\Pi}(M_2)$$

- Collision probability:

$$\mathrm{CP}(M_1, M_2) := \Pr_{\Pi \xleftarrow{\$} \mathrm{Perm}(n)} \left[\mathtt{COLL}^{\Pi}(M_1, M_2)\right]$$

- Extended over q distinct messages $M^q = (M_1, \ldots, M_q)$
  - $\mathtt{COLL}^{\Pi}(M^q) : \bigcup_{i<j\in[q]} \mathtt{COLL}^{\Pi}(M_i, M_j)$
  - $\mathrm{CP}(M^q) := \Pr_{\Pi \xleftarrow{\$} \mathrm{Perm}(n)} \left[\mathtt{COLL}^{\Pi}(M^q)\right]$

CBC Output Collision

- Restrictions:

CBC Output Collision

- Restrictions:
  - Length: $m_1, \ldots, m_q \leq \ell$ and $\sum_{i=1}^{q} m_i = m \leq \sigma$.

CBC Output Collision

- Restrictions:
  - Length: $m_1, \ldots, m_q \leq \ell$ and $\sum_{i=1}^{q} m_i = m \leq \sigma$.
  - Types of query tuple:
    - type $=$ eq: messages must have equal length;
    - type $=$ pf: no message is a prefix to other messages;
    - type $=$ any: no restrictions except distinctness.

CBC Output Collision

- Restrictions:
  - Length: $m_1, \ldots, m_q \leq \ell$ and $\sum_{i=1}^{q} m_i = m \leq \sigma$.
  - Types of query tuple:
    - type $=$ eq: messages must have equal length;
    - type $=$ pf: no message is a prefix to other messages;
    - type $=$ any: no restrictions except distinctness.
- Maximum collision probabilities: for fixed ℓ, σ and type

$$\mathsf{CP}_{\ell}^{\mathsf{type}} := \max_{\substack{\mathsf{type}(M_1,M_2) \\ m_i \leq \ell}} \mathsf{CP}(M_1, M_2) \qquad \mathsf{CP}_{q,\ell,\sigma}^{\mathsf{type}} := \max_{\substack{\mathsf{type}(M^q) \\ m_i \leq \ell \\ \sum_{i=1}^{q} m_i \leq \sigma}} \mathsf{CP}(M^q)$$

CBC Output Collision

- Restrictions:
  - Length: $m_1, \ldots, m_q \leq \ell$ and $\sum_{i=1}^{q} m_i = m \leq \sigma$.
  - Types of query tuple:
    - type $=$ eq: messages must have equal length;
    - type $=$ pf: no message is a prefix to other messages;
    - type $=$ any: no restrictions except distinctness.
- Maximum collision probabilities: for fixed ℓ, σ and type

$$\mathsf{CP}_{\ell}^{\mathsf{type}} := \max_{\substack{\mathsf{type}(M_1,M_2) \\ m_i \leq \ell}} \mathsf{CP}(M_1, M_2) \qquad \mathsf{CP}_{q,\ell,\sigma}^{\mathsf{type}} := \max_{\substack{\mathsf{type}(M^q) \\ m_i \leq \ell \\ \sum_{i=1}^{q} m_i \leq \sigma}} \mathsf{CP}(M^q)$$

We are interested in $\mathsf{CP}_{\ell}^{\mathsf{type}}$ and $\mathsf{CP}_{q,\ell,\sigma}^{\mathsf{type}}$ for type $\in \{\mathsf{eq}, \mathsf{any}\}$.

CBC Output Collision

Some Known Results:

CBC Output Collision

Some Known Results:

- Dodis et al. [DGHKR, CRYPTO '04] claimed (without proof) that,

$$\mathsf{CP}_{\ell}^{\mathsf{eq}} \leq \frac{1}{2^n} + \frac{\ell(d'(\ell))^2}{2^{2n}} + \frac{\ell^6}{2^{3n}},$$

where $d'(\ell) = \max_{m \leq \ell}$ no. of divisors of m [grows slowly]

CBC Output Collision

Some Known Results:

- Dodis et al. [DGHKR, CRYPTO '04] claimed (without proof) that,

$$\mathsf{CP}_{\ell}^{\mathsf{eq}} \leq \frac{1}{2^n} + \frac{\ell(d'(\ell))^2}{2^{2n}} + \frac{\ell^6}{2^{3n}},$$

  where $d'(\ell) = \max_{m \leq \ell}$ no. of divisors of m [grows slowly]

- Bellare et al. [BPR, CRYPTO '05] proved that:

$$\mathsf{CP}_{\ell}^{\mathsf{any}} \leq \frac{2d'(\ell)}{2^n} + \frac{64\ell^4}{2^{2n}}.$$

CBC Output Collision

Some Known Results:

- Dodis et al. [DGHKR, CRYPTO '04] claimed (without proof) that,

$$\mathsf{CP}^{\mathsf{eq}}_{\ell} \leq \frac{1}{2^n} + \frac{\ell(d'(\ell))^2}{2^{2n}} + \frac{\ell^6}{2^{3n}} \xRightarrow{\text{Union bound}} \mathsf{CP}^{\mathsf{eq}}_{q,\ell,\sigma} \leq \frac{q^2}{2^n} + \frac{q^2\ell(d'(\ell))^2}{2^{2n}} + \frac{q^2\ell^6}{2^{3n}},$$

  where $d'(\ell) = \max_{m \leq \ell}$ no. of divisors of m [grows slowly]

- Bellare et al. [BPR, CRYPTO '05] proved that:

$$\mathsf{CP}^{\mathsf{any}}_{\ell} \leq \frac{2d'(\ell)}{2^n} + \frac{64\ell^4}{2^{2n}} \xRightarrow{\text{Union bound}} \mathsf{CP}^{\mathsf{eq}}_{q,\ell,\sigma} \leq \frac{q^2 d'(\ell)}{2^n} + \frac{32q^2\ell^4}{2^{2n}}.$$

CBC Output Collision

Some Known Results:

- Dodis et al. [DGHKR, CRYPTO '04] claimed (without proof) that,

$$\mathsf{CP}^{\mathsf{eq}}_{\ell} \leq \frac{1}{2^n} + \frac{\ell(d'(\ell))^2}{2^{2n}} + \frac{\ell^6}{2^{3n}} \xrightarrow{\text{Union bound}} \mathsf{CP}^{\mathsf{eq}}_{q,\ell,\sigma} \leq \frac{q^2}{2^n} + \frac{q^2\ell(d'(\ell))^2}{2^{2n}} + \frac{q^2\ell^6}{2^{3n}},$$

  where $d'(\ell) = \max_{m \leq \ell}$ no. of divisors of m [grows slowly]

- Bellare et al. [BPR, CRYPTO '05] proved that:

$$\mathsf{CP}^{\mathsf{any}}_{\ell} \leq \frac{2d'(\ell)}{2^n} + \frac{64\ell^4}{2^{2n}} \xrightarrow{\text{Union bound}} \mathsf{CP}^{\mathsf{eq}}_{q,\ell,\sigma} \leq \frac{q^2 d'(\ell)}{2^n} + \frac{32q^2\ell^4}{2^{2n}}.$$

- Pietrzak [Pietrzak, ICALP '06] proved that:

$$\mathsf{CP}^{\mathsf{any}}_{q,\ell,\sigma} \leq \frac{16q^2}{2^n} + \frac{128q^2\ell^8}{2^{2n}}.$$

CBC Output Collision

Some Known Results:

- Dodis et al. [DGHKR, CRYPTO '04] claimed (without proof) that,

$$\mathsf{CP}^{\mathsf{eq}}_{\ell} \leq \frac{1}{2^n} + \frac{\ell(d'(\ell))^2}{2^{2n}} + \frac{\ell^6}{2^{3n}} \xrightarrow{\text{Union bound}} \mathsf{CP}^{\mathsf{eq}}_{q,\ell,\sigma} \leq \frac{q^2}{2^n} + \frac{q^2\ell(d'(\ell))^2}{2^{2n}} + \frac{q^2\ell^6}{2^{3n}},$$

  where $d'(\ell) = \max_{m \leq \ell}$ no. of divisors of m [grows slowly]

- Bellare et al. [BPR, CRYPTO '05] proved that:

$$\mathsf{CP}^{\mathsf{any}}_{\ell} \leq \frac{2d'(\ell)}{2^n} + \frac{64\ell^4}{2^{2n}} \xrightarrow{\text{Union bound}} \mathsf{CP}^{\mathsf{eq}}_{q,\ell,\sigma} \leq \frac{q^2 d'(\ell)}{2^n} + \frac{32q^2\ell^4}{2^{2n}}.$$

- Pietrzak [Pietrzak, ICALP '06] proved that:

$$\mathsf{CP}^{\mathsf{any}}_{q,\ell,\sigma} \leq \frac{16q^2}{2^n} + \frac{128q^2\ell^8}{2^{2n}}.$$

  Reduces to $\mathsf{CP}^{\mathsf{any}}_{q,\ell,\sigma} = O\left(\frac{q^2}{2^n}\right)$ for $\ell < 2^{n/8}$. (Better than BPR's bound for $\ell < 2^{n/8}$)

CBC Output Collision

Application to PRF bound of $\mathsf{F} \in \{\mathsf{EMAC}, \mathsf{ECBC}, \mathsf{FCBC}\}$:

- Using [DGHKR04]:

$$\mathbf{Adv}^{\mathrm{prf}}_{\mathsf{F}^{\mathrm{eq}}}(\mathscr{A}) = O\left(\frac{q^2}{2^n}\right) \qquad (\text{while } \ell < 2^{n/3})$$

- Using [BPR05]:

$$\mathbf{Adv}^{\mathrm{prf}}_{\mathsf{F}^{\mathrm{any}}}(\mathscr{A}) = O\left(\frac{q^2 d'(\ell)}{2^n}\right) \qquad (\text{while } \ell < 2^{n/4})$$

- Using [Pietrzak06]:

$$\mathbf{Adv}^{\mathrm{prf}}_{\mathsf{F}^{\mathrm{any}}}(\mathscr{A}) = O\left(\frac{q^2}{2^n}\right) \qquad (\text{while } \ell < 2^{n/8})$$

CBC Output Collision

Application to PRF bound of $\mathsf{F} \in \{\mathsf{EMAC}, \mathsf{ECBC}, \mathsf{FCBC}\}$:

- Using [DGHKR04]:

$$\mathbf{Adv}^{\mathrm{prf}}_{\mathsf{F}^{\mathrm{eq}}}(\mathscr{A}) = O\left(\frac{q^2}{2^n}\right) \qquad (\text{while } \ell < 2^{n/3})$$

- Using [BPR05]:

$$\mathbf{Adv}^{\mathrm{prf}}_{\mathsf{F}^{\mathrm{any}}}(\mathscr{A}) = O\left(\frac{q^2 d'(\ell)}{2^n}\right) \qquad (\text{while } \ell < 2^{n/4})$$

- Using [Pietrzak06]:

$$\mathbf{Adv}^{\mathrm{prf}}_{\mathsf{F}^{\mathrm{any}}}(\mathscr{A}) = O\left(\frac{q^2}{2^n}\right) \qquad (\text{while } \ell < 2^{n/8})$$

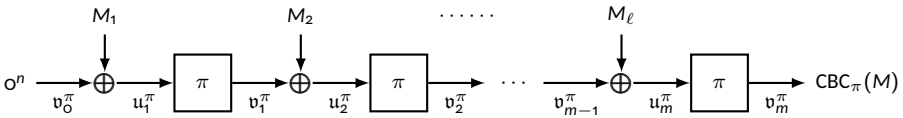
We show that the underlying graph-based analysis has a flaw [JN, JMC '16].

Structure Graphs

Notations and Definitions:

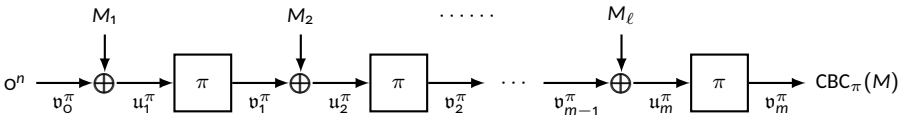
Structure Graphs

Notations and Definitions:



Structure Graphs

Notations and Definitions:



- Intermediate Inputs and Outputs:

$$u^\pi := (u_1^\pi, \ldots, u_m^\pi) \qquad v^\pi := (v_0^\pi, \ldots, v_m^\pi).$$

Structure Graphs

Notations and Definitions:

- Intermediate Inputs and Outputs:

$$\mathfrak{u}^\pi := (\mathfrak{u}_1^\pi, \ldots, \mathfrak{u}_m^\pi) \qquad \mathfrak{v}^\pi := (\mathfrak{v}_\mathsf{o}^\pi, \ldots, \mathfrak{v}_m^\pi).$$

- Fix q distinct messages $M^q = (M_1, \ldots, M_q)$:
  - Intermediate inputs tuple: $\mathfrak{u}^\pi := (\mathfrak{u}^\pi(M_1), \ldots, \mathfrak{u}^\pi(M_q))$.
  - Intermediate outputs tuple: $\mathfrak{v}^\pi := (\mathfrak{v}^\pi(M_1), \ldots, \mathfrak{v}^\pi(M_q))$.
  - Index set: $\mathcal{I} := \{(r, i) : r \in [q], i \in [m_i]\} \cup \{(r, \mathsf{o}) : r \in [q]\}$.

Structure Graphs

Notations and Definitions:

- Intermediate Inputs and Outputs:

$$\mathfrak{u}^\pi := (\mathfrak{u}_1^\pi, \ldots, \mathfrak{u}_m^\pi) \qquad \mathfrak{v}^\pi := (\mathfrak{v}_\mathsf{o}^\pi, \ldots, \mathfrak{v}_m^\pi).$$

- Fix q distinct messages $M^q = (M_1, \ldots, M_q)$:
  - Intermediate inputs tuple: $\mathfrak{u}^\pi := (\mathfrak{u}^\pi(M_1), \ldots, \mathfrak{u}^\pi(M_q))$.
  - Intermediate outputs tuple: $\mathfrak{v}^\pi := (\mathfrak{v}^\pi(M_1), \ldots, \mathfrak{v}^\pi(M_q))$.
  - Index set: $\mathcal{I} := \{(r, i) : r \in [q], i \in [m_i]\} \cup \{(r, \mathsf{o}) : r \in [q]\}$.
  - Dictionary order, $\preceq$ on $\mathcal{I}$: $(r, i) \preceq (r', i')$ iff
    - $r < r'$, or
    - $r = r'$ and $i \leq i'$.

Structure Graphs

Block-vertex Structure Graph, $\mathcal{B}_{\pi}^{M} = (\mathcal{V}, \mathcal{E}, \mathcal{L})$, for a message M and permutation π:

- Vertex and edge labeled digraph.
- Vertex set, $\mathcal{V} := \mathfrak{v}^{\pi}(M)$.
- Edge set, $\mathcal{E} := \{(\mathfrak{v}_{i-1}^{\pi}(M), \mathfrak{v}_{i}^{\pi}(M)) : 1 \leq i \leq m\}$.
- Label function, $\mathcal{L}(\mathfrak{v}_{i-1}^{\pi}(M), \mathfrak{v}_{i}^{\pi}(M)) = M_i$.

Structure Graphs

Block-vertex Structure Graph, $\mathcal{B}_\pi^M = (\mathcal{V}, \mathcal{E}, \mathcal{L})$, for a message M and permutation π:

- Vertex and edge labeled digraph.
- Vertex set, $\mathcal{V} := \mathfrak{v}^\pi(M)$.
- Edge set, $\mathcal{E} := \{(\mathfrak{v}_{i-1}^\pi(M), \mathfrak{v}_i^\pi(M)) : 1 \leq i \leq m\}$.
- Label function, $\mathcal{L}(\mathfrak{v}_{i-1}^\pi(M), \mathfrak{v}_i^\pi(M)) = M_i$.

Example

Let

- $M = (1, 0, 2, 0, 2)$
- $\pi(1) = 2$, $\pi(2) = 3$.

Structure Graphs

Block-vertex Structure Graph, $\mathcal{B}_{\pi}^{M} = (\mathcal{V}, \mathcal{E}, \mathcal{L})$, for a message M and permutation π:

- Vertex and edge labeled digraph.
- Vertex set, $\mathcal{V} := \mathfrak{v}^{\pi}(M)$.
- Edge set, $\mathcal{E} := \{(\mathfrak{v}_{i-1}^{\pi}(M), \mathfrak{v}_{i}^{\pi}(M)) : 1 \leq i \leq m\}$.
- Label function, $\mathcal{L}(\mathfrak{v}_{i-1}^{\pi}(M), \mathfrak{v}_{i}^{\pi}(M)) = M_i$.

Example

Let

- $M = (1, 0, 2, 0, 2)$
- $\pi(1) = 2, \pi(2) = 3$.
- $\mathfrak{v}^{\pi} = (0, 2, 3, 2, 3, 2)$.
- $\mathfrak{u}^{\pi} = (1, 2, 1, 2, 1)$.

Structure Graphs

Block-vertex Structure Graph, $\mathcal{B}_\pi^M = (\mathcal{V}, \mathcal{E}, \mathcal{L})$, for a message M and permutation π:

- Vertex and edge labeled digraph.
- Vertex set, $\mathcal{V} := \mathfrak{v}^\pi(M)$.
- Edge set, $\mathcal{E} := \{(\mathfrak{v}_{i-1}^\pi(M), \mathfrak{v}_i^\pi(M)) : 1 \leq i \leq m\}$.
- Label function, $\mathcal{L}(\mathfrak{v}_{i-1}^\pi(M), \mathfrak{v}_i^\pi(M)) = M_i$.

Example

Let

- $M = (1, 0, 2, 0, 2)$
- $\pi(1) = 2, \pi(2) = 3$.
- $\mathfrak{v}^\pi = (0, 2, 3, 2, 3, 2)$.
- $\mathfrak{u}^\pi = (1, 2, 1, 2, 1)$.

Structure Graphs

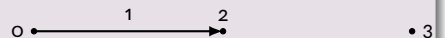
Block-vertex Structure Graph, $\mathcal{B}_\pi^M = (\mathcal{V}, \mathcal{E}, \mathcal{L})$, for a message M and permutation π:

- Vertex and edge labeled digraph.
- Vertex set, $\mathcal{V} := \mathfrak{v}^\pi(M)$.
- Edge set, $\mathcal{E} := \{(\mathfrak{v}_{i-1}^\pi(M), \mathfrak{v}_i^\pi(M)) : 1 \leq i \leq m\}$.
- Label function, $\mathcal{L}(\mathfrak{v}_{i-1}^\pi(M), \mathfrak{v}_i^\pi(M)) = M_i$.

Example

Let

- $M = (1, 0, 2, 0, 2)$
- $\pi(1) = 2, \pi(2) = 3$.
- $\mathfrak{v}^\pi = (0, 2, 3, 2, 3, 2)$.
- $\mathfrak{u}^\pi = (1, 2, 1, 2, 1)$.



Structure Graphs

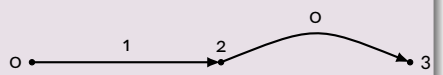
Block-vertex Structure Graph, $\mathcal{B}_\pi^M = (\mathcal{V}, \mathcal{E}, \mathcal{L})$, for a message M and permutation π:

- Vertex and edge labeled digraph.
- Vertex set, $\mathcal{V} := \mathfrak{v}^\pi(M)$.
- Edge set, $\mathcal{E} := \{(\mathfrak{v}_{i-1}^\pi(M), \mathfrak{v}_i^\pi(M)) : 1 \leq i \leq m\}$.
- Label function, $\mathcal{L}(\mathfrak{v}_{i-1}^\pi(M), \mathfrak{v}_i^\pi(M)) = M_i$.

Example

Let

- $M = (1, 0, 2, 0, 2)$
- $\pi(1) = 2, \pi(2) = 3$.
- $\mathfrak{v}^\pi = (0, 2, 3, 2, 3, 2)$.
- $\mathfrak{u}^\pi = (1, 2, 1, 2, 1)$.



Structure Graphs

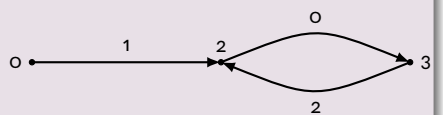
Block-vertex Structure Graph, $\mathcal{B}_\pi^M = (\mathcal{V}, \mathcal{E}, \mathcal{L})$, for a message M and permutation π:

- Vertex and edge labeled digraph.
- Vertex set, $\mathcal{V} := \mathfrak{v}^\pi(M)$.
- Edge set, $\mathcal{E} := \{(\mathfrak{v}_{i-1}^\pi(M), \mathfrak{v}_i^\pi(M)) : 1 \leq i \leq m\}$.
- Label function, $\mathcal{L}(\mathfrak{v}_{i-1}^\pi(M), \mathfrak{v}_i^\pi(M)) = M_i$.

Example

Let

- $M = (1, 0, 2, 0, 2)$
- $\pi(1) = 2, \pi(2) = 3$.
- $\mathfrak{v}^\pi = (0, 2, 3, 2, 3, 2)$.
- $\mathfrak{u}^\pi = (1, 2, 1, 2, 1)$.



Structure Graphs

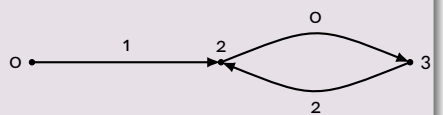
Block-vertex Structure Graph, $\mathcal{B}_{\pi}^{M} = (\mathcal{V}, \mathcal{E}, \mathcal{L})$, for a message M and permutation π:

- Vertex and edge labeled digraph.
- Vertex set, $\mathcal{V} := \mathfrak{v}^{\pi}(M)$.
- Edge set, $\mathcal{E} := \{(\mathfrak{v}_{i-1}^{\pi}(M), \mathfrak{v}_{i}^{\pi}(M)) : 1 \leq i \leq m\}$.
- Label function, $\mathcal{L}(\mathfrak{v}_{i-1}^{\pi}(M), \mathfrak{v}_{i}^{\pi}(M)) = M_i$.
- It is a walk, called the M-walk, starting from 0 following the sequence of labels $M = (M_1, \ldots, M_m)$.

Example

Let

- $M = (1, 0, 2, 0, 2)$
- $\pi(1) = 2, \pi(2) = 3$.
- $\mathfrak{v}^{\pi} = (0, 2, 3, 2, 3, 2)$.
- $\mathfrak{u}^{\pi} = (1, 2, 1, 2, 1)$.



Structure Graphs

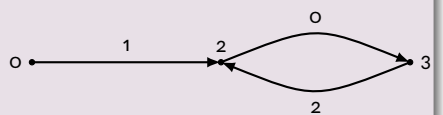
Block-vertex Structure Graph, $\mathcal{B}_\pi^M = (\mathcal{V}, \mathcal{E}, \mathcal{L})$, for a message M and permutation π:

- Vertex and edge labeled digraph.
- Vertex set, $\mathcal{V} := \mathfrak{v}^\pi(M)$.
- Edge set, $\mathcal{E} := \{(\mathfrak{v}_{i-1}^\pi(M), \mathfrak{v}_i^\pi(M)) : 1 \leq i \leq m\}$.
- Label function, $\mathcal{L}(\mathfrak{v}_{i-1}^\pi(M), \mathfrak{v}_i^\pi(M)) = M_i$.
- It is a walk, called the M-walk, starting from o following the sequence of labels $M = (M_1, \ldots, M_m)$.

Example

Let

- $M = (1, 0, 2, 0, 2)$
- $\pi(1) = 2, \pi(2) = 3$.
- $\mathfrak{v}^\pi = (0, 2, 3, 2, 3, 2)$.
- $\mathfrak{u}^\pi = (1, 2, 1, 2, 1)$.



Block-vertex Structure Graph, $\mathcal{B}_\pi^{M^q}$, for M^q and permutation π is simply the union of all M_i-walks.

Structure Graphs

Structure Graph , $\mathcal{S}_{\pi}^{M^q} = (\widetilde{\mathcal{V}}, \widetilde{\mathcal{E}})$, for M^q and a permutation π:

- Let $\alpha : \mathfrak{v}^{\pi}(M^q) \to \mathcal{I}$ such that

$$\alpha(\mathfrak{v}_j^{\pi}(M_i)) = \min\{(i', j') : \mathfrak{v}_j^{\pi}(M_i) = \mathfrak{v}_{j'}^{\pi}(M_{i'})\}.$$

- Let $\alpha(\mathfrak{v}^{\pi}(M^q))$ be the range of α.

Structure Graphs

Structure Graph , $\mathcal{S}_{\pi}^{M^q} = (\widetilde{\mathcal{V}}, \widetilde{\mathcal{E}})$, for M^q and a permutation π:

- Let $\alpha : \mathfrak{v}^{\pi}(M^q) \to \mathcal{I}$ such that

$$\alpha(\mathfrak{v}_j^{\pi}(M_i)) = \min\{(i', j') : \mathfrak{v}_j^{\pi}(M_i) = \mathfrak{v}_{j'}^{\pi}(M_{i'})\}.$$

- Let $\alpha(\mathfrak{v}^{\pi}(M^q))$ be the range of α.
- Then, $\mathcal{S}_{\pi}^{M^q}$ is an isomorphism of $\mathcal{B}_{\pi}^{M^q}$, such that
  - $\widetilde{\mathcal{V}} := \alpha(\mathfrak{v}^{\pi}(M^q))$.
  - $\widetilde{\mathcal{E}} := \{(\alpha(u), \alpha(v), \mathcal{L}(u, v)) : (u, v) \in \mathcal{E}\}$.

Structure Graphs

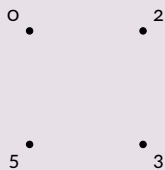
Example

Let $M_1 = (1, 0, 2, 0, 7)$ and $M_2 = (4)$. Let $\pi(1) = 2$, $\pi(2) = 3$, $\pi(4) = 5$. Then, $\mathfrak{v}^{\pi}(M_1) = (0, 2, 3, 2, 3, 5)$ and $\mathfrak{v}^{\pi}(M_2) = (0, 5)$.

Structure Graphs

Example

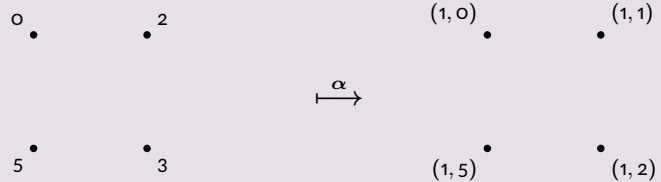
Let $M_1 = (1, 0, 2, 0, 7)$ and $M_2 = (4)$. Let $\pi(1) = 2$, $\pi(2) = 3$, $\pi(4) = 5$. Then,
$\mathfrak{v}^{\pi}(M_1) = (0, 2, 3, 2, 3, 5)$ and $\mathfrak{v}^{\pi}(M_2) = (0, 5)$.



Structure Graphs

Example

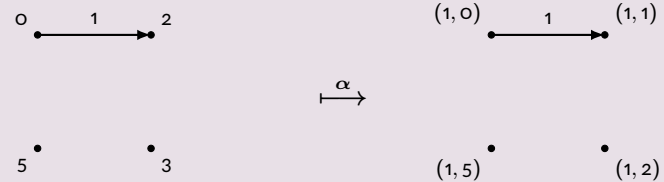
Let $M_1 = (1, 0, 2, 0, 7)$ and $M_2 = (4)$. Let $\pi(1) = 2$, $\pi(2) = 3$, $\pi(4) = 5$. Then, $\mathfrak{v}^\pi(M_1) = (0, 2, 3, 2, 3, 5)$ and $\mathfrak{v}^\pi(M_2) = (0, 5)$.



Structure Graphs

Example

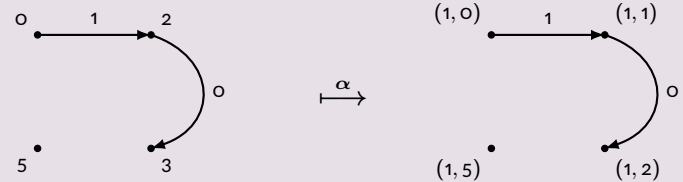
Let $M_1 = (1, 0, 2, 0, 7)$ and $M_2 = (4)$. Let $\pi(1) = 2$, $\pi(2) = 3$, $\pi(4) = 5$. Then, $\mathfrak{v}^\pi(M_1) = (0, 2, 3, 2, 3, 5)$ and $\mathfrak{v}^\pi(M_2) = (0, 5)$.



Structure Graphs

Example

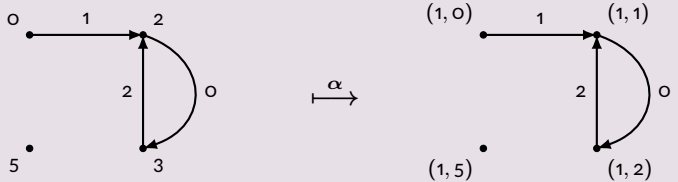
Let $M_1 = (1, 0, 2, 0, 7)$ and $M_2 = (4)$. Let $\pi(1) = 2$, $\pi(2) = 3$, $\pi(4) = 5$. Then, $\mathfrak{v}^\pi(M_1) = (0, 2, 3, 2, 3, 5)$ and $\mathfrak{v}^\pi(M_2) = (0, 5)$.



Structure Graphs

Example

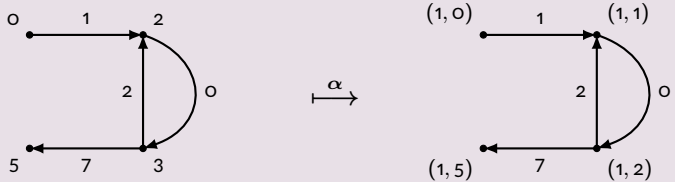
Let $M_1 = (1, 0, 2, 0, 7)$ and $M_2 = (4)$. Let $\pi(1) = 2$, $\pi(2) = 3$, $\pi(4) = 5$. Then, $\mathfrak{v}^\pi(M_1) = (0, 2, 3, 2, 3, 5)$ and $\mathfrak{v}^\pi(M_2) = (0, 5)$.



Structure Graphs

Example

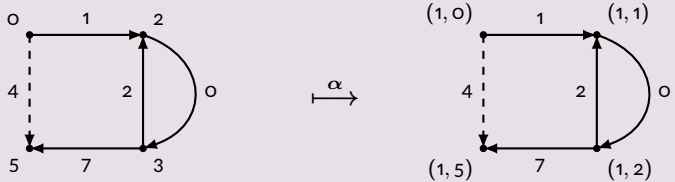
Let $M_1 = (1, 0, 2, 0, 7)$ and $M_2 = (4)$. Let $\pi(1) = 2$, $\pi(2) = 3$, $\pi(4) = 5$. Then, $\mathfrak{v}^\pi(M_1) = (0, 2, 3, 2, 3, 5)$ and $\mathfrak{v}^\pi(M_2) = (0, 5)$.



Structure Graphs

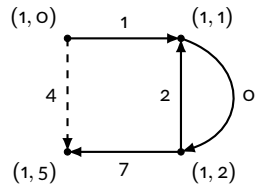
Example

Let $M_1 = (1, 0, 2, 0, 7)$ and $M_2 = (4)$. Let $\pi(1) = 2$, $\pi(2) = 3$, $\pi(4) = 5$. Then, $\mathfrak{v}^\pi(M_1) = (0, 2, 3, 2, 3, 5)$ and $\mathfrak{v}^\pi(M_2) = (0, 5)$.



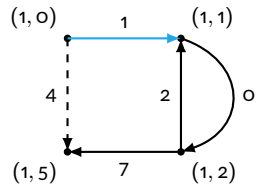
True Collisions and Accidents

- Consider the dictionary order traversal of graph $\mathcal{S}$ for message pair $M_1 = (1, 0, 2, 0, 7)$ and $M_2 = (4)$.



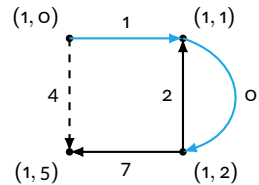
True Collisions and Accidents

- Consider the dictionary order traversal of graph $\mathcal{S}$ for message pair $M_1 = (1, 0, 2, 0, 7)$ and $M_2 = (4)$.



True Collisions and Accidents

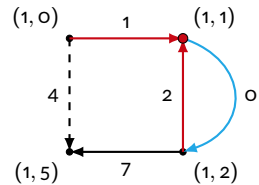
- Consider the dictionary order traversal of graph $\mathcal{S}$ for message pair $M_1 = (1, 0, 2, 0, 7)$ and $M_2 = (4)$.



True Collisions and Accidents

- Consider the dictionary order traversal of graph $\mathcal{S}$ for message pair $M_1 = (1, 0, 2, 0, 7)$ and $M_2 = (4)$.
- True collisions (increases the in-degree of some vertex):

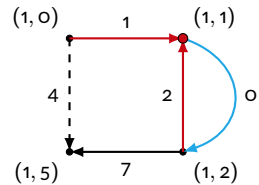
$$((1, 0), (1, 2); (1, 1)).$$



True Collisions and Accidents

- Consider the dictionary order traversal of graph $\mathcal{S}$ for message pair $M_1 = (1, 0, 2, 0, 7)$ and $M_2 = (4)$.
- True collisions (increases the in-degree of some vertex):

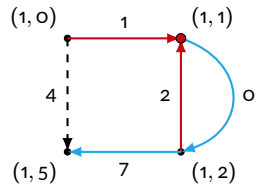
$$((1, 0), (1, 2); (1, 1)).$$



True Collisions and Accidents

- Consider the dictionary order traversal of graph $\mathcal{S}$ for message pair $M_1 = (1, 0, 2, 0, 7)$ and $M_2 = (4)$.
- True collisions (increases the in-degree of some vertex):

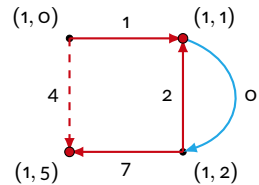
$$((1, 0), (1, 2); (1, 1)).$$



True Collisions and Accidents

- Consider the dictionary order traversal of graph $\mathcal{S}$ for message pair $M_1 = (1, 0, 2, 0, 7)$ and $M_2 = (4)$.
- True collisions (increases the in-degree of some vertex):

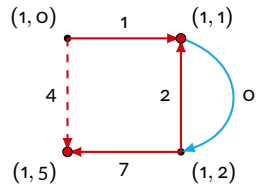
$$((1, 0), (1, 2); (1, 1)) \text{ and } ((1, 0), (1, 2); (1, 5)).$$



True Collisions and Accidents

- Consider the dictionary order traversal of graph $\mathcal{S}$ for message pair $M_1 = (1, 0, 2, 0, 7)$ and $M_2 = (4)$.
- True collisions (increases the in-degree of some vertex):

$$((1, 0), (1, 2); (1, 1)) \text{ and } ((1, 0), (1, 2); (1, 5)).$$



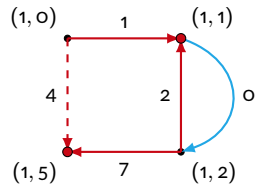
- System of equations L corresponding to true collisions:

$$Y_{1,0} \oplus Y_{1,2} = 1 \oplus 2,$$
$$Y_{1,0} \oplus Y_{1,2} = 4 \oplus 7$$

True Collisions and Accidents

- Consider the dictionary order traversal of graph $\mathcal{S}$ for message pair $M_1 = (1, 0, 2, 0, 7)$ and $M_2 = (4)$.
- True collisions (increases the in-degree of some vertex):

$$((1, 0), (1, 2); (1, 1)) \text{ and } ((1, 0), (1, 2); (1, 5)).$$



- System of equations L corresponding to true collisions:

$$Y_{1,0} \oplus Y_{1,2} = 1 \oplus 2,$$
$$Y_{1,0} \oplus Y_{1,2} = 4 \oplus 7$$

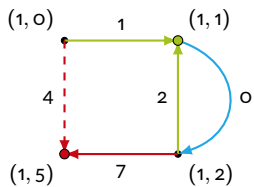
- $\text{rank}(L) = 1$ (second collision is induced by the first one).

True Collisions and Accidents

- Accidents: represents the notion of “surprising” collisions.

True Collisions and Accidents

- Accidents: represents the notion of "surprising" collisions.

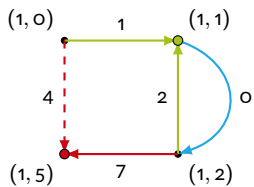


Green edges denote the accident.

True Collisions and Accidents

- Accidents: represents the notion of "surprising" collisions.
- No. of accidents, $\mathrm{Acc}(\mathcal{S})$ is defined as

$$\mathrm{Acc}(\mathcal{S}) := \begin{cases} \mathrm{rank}(L) & \text{if } \mathbf{deg_{in}}(1,0) = 0, \\ \mathrm{rank}(L) + 1 & \text{otherwise.} \end{cases}$$



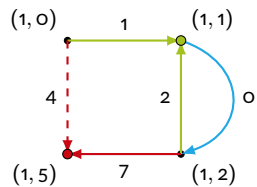
Green edges denote the accident.

True Collisions and Accidents

- Accidents: represents the notion of "surprising" collisions.
- No. of accidents, $\mathrm{Acc}(\mathcal{S})$ is defined as

$$\mathrm{Acc}(\mathcal{S}) := \begin{cases} \mathrm{rank}(L) & \text{if } \mathbf{deg_{in}}(1,0) = 0, \\ \mathrm{rank}(L) + 1 & \text{otherwise.} \end{cases}$$

- Main object of interest: $N_a^{M^q} := \{G : \mathrm{Acc}(G) = a\}$.



Green edges denote the accident.

Results on Structure Graphs

- Lemma 8 in [BPR05]: Let G be a structure graph with a accidents then

$$\Pr_{\Pi}[\mathcal{S}_{\Pi} = G] \leq \frac{1}{2^{na}}.$$

- Lemma 7 in [BPR05]: $N_a^{M^q} \leq \binom{m}{2}^a$.

Results on Structure Graphs

- Lemma 8 in [BPR05]: Let G be a structure graph with a accidents then

$$\Pr_{\Pi}[\mathcal{S}_{\Pi} = G] \leq \frac{1}{2^{na}}.$$

- Lemma 7 in [BPR05]: $N_a^{M^q} \leq \binom{m}{2}^a$.
- Let $N_a(\mathrm{E})$ denote the number of structure graphs with a accidents and satisfying an event E. Then,

$$\Pr_{\Pi}[\mathrm{E}] \leq \sum_{a \geq 0} \frac{N_a(\mathrm{E})}{2^{na}}.$$

Results on Structure Graphs

- Lemma 8 in [BPR05]: Let G be a structure graph with a accidents then

$$\Pr_{\Pi}[\mathcal{S}_{\Pi} = G] \leq \frac{1}{2^{na}}.$$

- Lemma 7 in [BPR05]: $N_a^{M^q} \leq \binom{m}{2}^a$.
- Let $N_a(\mathrm{E})$ denote the number of structure graphs with a accidents and satisfying an event E. Then,

$$\Pr_{\Pi}[\mathrm{E}] \leq \sum_{a \geq 0} \frac{N_a(\mathrm{E})}{2^{na}}.$$

- $N_a = O(m^{2a})$. But, we may have better bound for $N_a(\mathrm{E})$ for small a.

Bounding Collision Probability

- Usual approach for bounding $\Pr[\mathrm{E}]$:

  Let $\mathtt{Bad}$ denote the event $\mathrm{Acc}(\mathcal{S}_\Pi) \geq k$. Then,

$$\Pr[\mathrm{E}] \leq \sum_{0 \leq a < k} \frac{N_a(\mathrm{E})}{2^{na}} + \Pr[\mathtt{Bad}].$$

Bounding Collision Probability

- Usual approach for bounding $\Pr[\mathrm{E}]$:

  Let $\mathtt{Bad}$ denote the event $\mathrm{Acc}(\mathcal{S}_\Pi) \geq k$. Then,

  $$\Pr[\mathrm{E}] \leq \sum_{0 \leq a < k} \frac{N_a(\mathrm{E})}{2^{na}} + \Pr[\mathtt{Bad}].$$

- In [BPR05], $\mathrm{E} = \mathtt{COLL}^\Pi(M_i, M_j)$ and $k = 2$.
  - Further, $N_0^{(M_i, M_j)}(\mathtt{COLL}) = 0$.

Bounding Collision Probability

- Usual approach for bounding $\Pr[\mathtt{E}]$:

  Let $\mathtt{Bad}$ denote the event $\mathsf{Acc}(\mathcal{S}_\Pi) \geq k$. Then,

  $$\Pr[\mathtt{E}] \leq \sum_{0 \leq a < k} \frac{N_a(\mathtt{E})}{2^{na}} + \Pr[\mathtt{Bad}].$$

- In [BPR05], $\mathtt{E} = \mathtt{COLL}^\Pi(M_i, M_j)$ and $k = 2$.
  - Further, $N_0^{(M_i,M_j)}(\mathtt{COLL}) = 0$.
  - This immediately gives (assuming $\ell < 2^{n/2}$)

  $$\mathsf{CP}_\ell^{\mathsf{any}} \leq \frac{N_1^{(M_i,M_j)}(\mathtt{COLL})}{2^n} + O\left(\frac{\ell^4}{2^{2n}}\right).$$

Bounding Collision Probability

- Usual approach for bounding $\Pr[\mathrm{E}]$:

  Let $\mathtt{Bad}$ denote the event $\mathrm{Acc}(\mathcal{S}_\Pi) \geq k$. Then,

  $$\Pr[\mathrm{E}] \leq \sum_{0 \leq a < k} \frac{N_a(\mathrm{E})}{2^{na}} + \Pr[\mathtt{Bad}].$$

- In [BPR05], $\mathrm{E} = \mathtt{COLL}^\Pi(M_i, M_j)$ and $k = 2$.
  - Further, $N_0^{(M_i,M_j)}(\mathtt{COLL}) = 0$.
  - This immediately gives (assuming $\ell < 2^{n/2}$)

  $$\mathrm{CP}_\ell^{\mathrm{any}} \leq \frac{N_1^{(M_i,M_j)}(\mathtt{COLL})}{2^n} + O\left(\frac{\ell^4}{2^{2n}}\right).$$

- BPR showed that $N_1^{(M_i,M_j)}(\mathtt{COLL}) \leq d'(\ell)$.

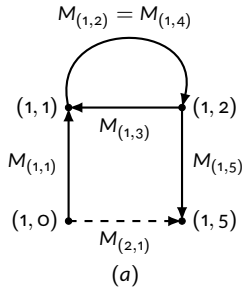
Flaw in [BPR05]

Lemma 10 in [BPR05]: Any structure graph G for a pair of messages with $\mathrm{Acc}(G) = 1$ must have exactly 1 true collision.

Flaw in [BPR05]

Lemma 10 in [BPR05]: Any structure graph G for a pair of messages with $\mathrm{Acc}(G) = 1$ must have exactly 1 true collision.

Counter-examples:



(a) $M_{(1,1)} \oplus M_{(1,3)} \oplus M_{(1,5)} \oplus M_{(2,1)} = 0$ (b) $M_{(1,1)} \oplus M_{(1,2)} \oplus M_{(1,3)} \oplus M_{(2,1)} = 0$.

Impact on CP Bounds in [BPR05] and [Pietrzak06]

- The bound in [BPR05] still holds with a slight change in constant factors.

Impact on CP Bounds in [BPR05] and [Pietrzak06]

- The bound in [BPR05] still holds with a slight change in constant factors.
- The bound in [Pietrzak06] needs revision.

Impact on CP Bounds in [BPR05] and [Pietrzak06]

- The bound in [BPR05] still holds with a slight change in constant factors.
- The bound in [Pietrzak06] needs revision.
    1. A straightforward fix gives $O(\ell q^2/2^n)$ bound.

Impact on CP Bounds in [BPR05] and [Pietrzak06]

- The bound in [BPR05] still holds with a slight change in constant factors.
- The bound in [Pietrzak06] needs revision.
  1. A straightforward fix gives $O(\ell q^2/2^n)$ bound.
  2. A slightly more involved analysis gives $O(q^2 d'(\ell)/2^n)$ while $\ell < 2^{n/8}$.

Impact on CP Bounds in [BPR05] and [Pietrzak06]

- The bound in [BPR05] still holds with a slight change in constant factors.
- The bound in [Pietrzak06] needs revision.
  1. A straightforward fix gives $O(\ell q^2/2^n)$ bound.
  2. A slightly more involved analysis gives $O(q^2 d'(\ell)/2^n)$ while $\ell < 2^{n/8}$.
  3. Both bounds are worse than [BPR05] for all choices of ℓ.

Impact on CP Bounds in [BPR05] and [Pietrzak06]

- The bound in [BPR05] still holds with a slight change in constant factors.
- The bound in [Pietrzak06] needs revision.
  1. A straightforward fix gives $O(\ell q^2/2^n)$ bound.
  2. A slightly more involved analysis gives $O(q^2 d'(\ell)/2^n)$ while $\ell < 2^{n/8}$.
  3. Both bounds are worse than [BPR05] for all choices of ℓ.

A different approach required to get $O(q^2/2^n)$ bound?

A Simple Proof of Tight Bound on $\mathrm{CP}^{\mathrm{any}}_{q,\ell,\sigma}$ [JN16]

- BPR's bound implicitly uses the restriction $\ell \leq 2^{n/4}$.

A Simple Proof of Tight Bound on $\mathrm{CP}^{\mathrm{any}}_{q,\ell,\sigma}$ [JN16]

- BPR's bound implicitly uses the restriction $\ell \leq 2^{n/4}$.
- Modified $\mathtt{Bad}$:

A Simple Proof of Tight Bound on $\mathrm{CP}^{\mathrm{any}}_{q,\ell,\sigma}$ [JN16]

- BPR's bound implicitly uses the restriction $\ell \leq 2^{n/4}$.
- Modified $\mathtt{Bad}$:
  - $\mathrm{Acc}(\mathcal{S}_{\Pi}^{(M_i,M_j)}) \geq 2$ (same as before), and

A Simple Proof of Tight Bound on $\mathrm{CP}^{\mathrm{any}}_{q,\ell,\sigma}$ [JN16]

- BPR's bound implicitly uses the restriction $\ell \leq 2^{n/4}$.
- Modified $\mathtt{Bad}$:
  - $\mathrm{Acc}(\mathcal{S}_{\Pi}^{(M_i,M_j)}) \geq 2$ (same as before), and
  - $\mathrm{Acc}(\mathcal{S}_{\Pi}^{M_i}) \geq 1$ (new addition).

A Simple Proof of Tight Bound on $\mathrm{CP}^{\mathrm{any}}_{q,\ell,\sigma}$ [JN16]

- BPR's bound implicitly uses the restriction $\ell \leq 2^{n/4}$.
- Modified Bad:
  - $\mathrm{Acc}(\mathcal{S}_\Pi^{(M_i,M_j)}) \geq 2$ (same as before), and
  - $\mathrm{Acc}(\mathcal{S}_\Pi^{M_i}) \geq 1$ (new addition).
- So, $\Pr[\mathrm{Bad}] \leq \frac{q\ell^2}{2^n} + \frac{q^2\ell^4}{2^{2n}}$. [using trivial bounds on $N_1^{M_i}$ and $N_2^{(M_i,M_j)}$]

A Simple Proof of Tight Bound on $\mathrm{CP}^{\mathrm{any}}_{q,\ell,\sigma}$ [JN16]

- BPR's bound implicitly uses the restriction $\ell \leq 2^{n/4}$.
- Modified $\mathtt{Bad}$:
  - $\mathrm{Acc}(\mathcal{S}_\Pi^{(M_i,M_j)}) \geq 2$ (same as before), and
  - $\mathrm{Acc}(\mathcal{S}_\Pi^{M_i}) \geq 1$ (new addition).
- So, $\Pr[\mathtt{Bad}] \leq \frac{q\ell^2}{2^n} + \frac{q^2\ell^4}{2^{2n}}$. [using trivial bounds on $N_1^{M_i}$ and $N_2^{(M_i,M_j)}$]
- Further, $N_1^{(M_i,M_j)}(\mathtt{COLL} \wedge \neg\mathtt{Bad}) = 1$ (non-bad graphs are union of paths).

A Simple Proof of Tight Bound on $\mathrm{CP}^{\mathrm{any}}_{q,\ell,\sigma}$ [JN16]

- BPR's bound implicitly uses the restriction $\ell \leq 2^{n/4}$.
- Modified $\mathtt{Bad}$:
  - $\mathrm{Acc}(\mathcal{S}_\Pi^{(M_i,M_j)}) \geq 2$ (same as before), and
  - $\mathrm{Acc}(\mathcal{S}_\Pi^{M_i}) \geq 1$ (new addition).
- So, $\Pr[\mathtt{Bad}] \leq \frac{q\ell^2}{2^n} + \frac{q^2\ell^4}{2^{2n}}$. [using trivial bounds on $N_1^{M_i}$ and $N_2^{(M_i,M_j)}$]
- Further, $N_1^{(M_i,M_j)}(\mathtt{COLL} \wedge \neg\mathtt{Bad}) = 1$ (non-bad graphs are union of paths).
- Finally, we get

$$\mathrm{CP}^{\mathrm{any}}_{q,\ell,\sigma} \leq \frac{q^2}{2^n} + \frac{q\ell^2}{2^n} + \frac{q^2\ell^4}{2^{2n}}.$$

- The bound reduces to $O(q^2/2^n)$ for $\ell < \min\{q^{1/2}, 2^{n/4}\}$.

A Simple Proof of Tight Bound on $\mathrm{CP}^{\mathrm{any}}_{q,\ell,\sigma}$ [JN16]

- BPR's bound implicitly uses the restriction $\ell \leq 2^{n/4}$.
- Modified $\mathtt{Bad}$:
  - $\mathrm{Acc}(\mathcal{S}_\Pi^{(M_i,M_j)}) \geq 2$ (same as before), and
  - $\mathrm{Acc}(\mathcal{S}_\Pi^{M_i}) \geq 1$ (new addition).
- So, $\Pr[\mathtt{Bad}] \leq \frac{q\ell^2}{2^n} + \frac{q^2\ell^4}{2^{2n}}$. [using trivial bounds on $N_1^{M_i}$ and $N_2^{(M_i,M_j)}$]
- Further, $N_1^{(M_i,M_j)}(\mathtt{COLL} \wedge \neg\mathtt{Bad}) = 1$ (non-bad graphs are union of paths).
- Finally, we get

$$\mathrm{CP}^{\mathrm{any}}_{q,\ell,\sigma} \leq \frac{q^2}{2^n} + \frac{q\ell^2}{2^n} + \frac{q^2\ell^4}{2^{2n}}.$$

- The bound reduces to $O(q^2/2^n)$ for $\ell < \min\{q^{1/2}, 2^{n/4}\}$.

Can we do better in terms of ℓ?

Towards an Improved Bound

Towards an Improved Bound

First change: Allow cycles in individual M_i-walks.

Towards an Improved Bound

First change: Allow cycles in individual M_i-walks.

A possible approach:

Towards an Improved Bound

First change: Allow cycles in individual M_i-walks.

A possible approach:

- For a fixed integer $\varphi < q$, let $\texttt{Cyc}_\varphi$ denote the event

$$|\{i \in [q] : M_i\text{-walk contains cycle in } \mathcal{S}_\Pi\}| \geq \varphi.$$

Towards an Improved Bound

First change: Allow cycles in individual M_i-walks.

A possible approach:

- For a fixed integer $\varphi < q$, let $\mathtt{Cyc}_\varphi$ denote the event

$$|\{i \in [q] : M_i\text{-walk contains cycle in } \mathcal{S}_\Pi\}| \geq \varphi.$$

- Then, $N_1^{(M_i,M_j)}(\mathtt{COLL} \wedge \neg \mathtt{Cyc}_\varphi) \leq q\varphi d'(\ell)$. (Better than $q^2 d'(\ell)$ for $\varphi < q$)
- $\Pr\left[\mathtt{Cyc}_\varphi\right] \leq \dfrac{q\ell^2}{\varphi 2^n}$ (using Markov's).

Towards an Improved Bound

First change: Allow cycles in individual M_i-walks.

A possible approach:

- For a fixed integer $\varphi < q$, let $\mathtt{Cyc}_\varphi$ denote the event
$$|\{i \in [q] : M_i\text{-walk contains cycle in } \mathcal{S}_\Pi\}| \geq \varphi.$$
- Then, $N_1^{(M_i,M_j)}(\mathtt{COLL} \wedge \neg \mathtt{Cyc}_\varphi) \leq q\varphi d'(\ell)$. (Better than $q^2 d'(\ell)$ for $\varphi < q$)
- $\Pr\left[\mathtt{Cyc}_\varphi\right] \leq \dfrac{q\ell^2}{\varphi 2^n}$ (using Markov's).

Using $\varphi = \ell/\sqrt{d'(\ell)}$, we get

$$\mathsf{CP}^\Pi(M^q) \leq O\left(\frac{q\ell\sqrt{d'(\ell)}}{2^n}\right) + \sum_{a\geq 2} \frac{N_a(\mathtt{COLL} \wedge \neg \mathtt{Cyc}_\varphi)}{2^{an}}.$$

Towards an Improved Bound

Towards an Improved Bound

Second change: Derive a good estimation for $N_2^{(M_i,M_j)}(\texttt{COLL})$.

Towards an Improved Bound

Second change: Derive a good estimation for $N_2^{(M_i,M_j)}(\texttt{COLL})$.

A possible approach:

Towards an Improved Bound

Second change: Derive a good estimation for $N_2^{(M_i,M_j)}(\texttt{COLL})$.

A possible approach:

- Define $\texttt{Bad}$ as $\mathrm{Acc}(\mathcal{S}_\Pi^{(M_i,M_j)}) \geq 3$.
- So,

$$\mathrm{CP}^{\mathrm{any}}_{q,\ell,\sigma} \leq O\left(\frac{q\ell\sqrt{d'(\ell)}}{2^n}\right) + \binom{q}{2}\frac{N_2^{(M_i,M_j)}(\texttt{COLL})}{2^{2n}} + O\left(\frac{q^2\ell^6}{2^{3n}}\right).$$

Towards an Improved Bound

Second change: Derive a good estimation for $N_2^{(M_i,M_j)}(\texttt{COLL})$.

A possible approach:

- Define $\texttt{Bad}$ as $\mathrm{Acc}(\mathcal{S}_\Pi^{(M_i,M_j)}) \geq 3$.
- So,

$$\mathrm{CP}^{\mathrm{any}}_{q,\ell,\sigma} \leq O\left(\frac{q\ell\sqrt{d'(\ell)}}{2^n}\right) + \binom{q}{2}\frac{N_2^{(M_i,M_j)}(\texttt{COLL})}{2^{2n}} + O\left(\frac{q^2\ell^6}{2^{3n}}\right).$$

- We characterize all structure graphs realizable by two messages (M_i, M_j) with accidents 2 that satisfy $\texttt{COLL}^\Pi(M_i, M_j)$.

Towards an Improved Bound

Second change: Derive a good estimation for $N_2^{(M_i,M_j)}(\texttt{COLL})$.

A possible approach:

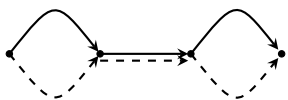
- Define $\texttt{Bad}$ as $\mathrm{Acc}(\mathcal{S}_\Pi^{(M_i,M_j)}) \geq 3$.
- So,

$$\mathrm{CP}^{\mathrm{any}}_{q,\ell,\sigma} \leq O\left(\frac{q\ell\sqrt{d'(\ell)}}{2^n}\right) + \binom{q}{2}\frac{N_2^{(M_i,M_j)}(\texttt{COLL})}{2^{2n}} + O\left(\frac{q^2\ell^6}{2^{3n}}\right).$$

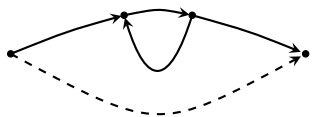
- We characterize all structure graphs realizable by two messages (M_i, M_j) with accidents 2 that satisfy $\texttt{COLL}^\Pi(M_i, M_j)$.
- This characterization also gives an improvement (over [DGHKR04]) for $\mathrm{CP}^{\mathrm{eq}}_\ell$.

Accident 2 Graphs having ℓ^2 choices

(a)



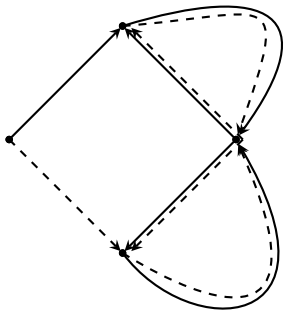
(b)



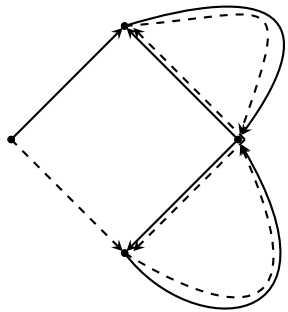
(c)

A closer estimation of probability bound for graphs of types (a) helps in adjusting the ℓ^2 factors arising in (c).

Accident 2 Graphs having less than ℓ^2 choices

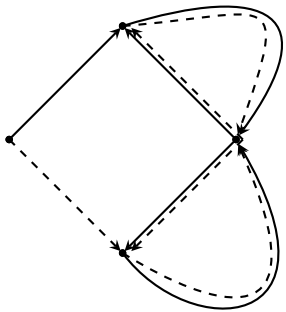


Accident 2 Graphs having less than ℓ^2 choices



- *Claim:* The number of choices of such graph is at most $t(\ell) := \sum_k d(k)d(\ell - k)$.

Accident 2 Graphs having less than ℓ^2 choices



- *Claim:* The number of choices of such graph is at most $t(\ell) := \sum_k d(k)d(\ell - k)$.
- Proof uses tools from theory of free monoids. [potential to obtain sharper bounds]

Improved Bound on $\mathsf{CP}^{\mathsf{any}}_{q,\ell,\sigma}$ and $\mathsf{CP}^{\mathsf{eq}}_{\ell}$

Message type = eq:

- $N_1(\texttt{COLL}) = 1$ (only non-cyclic walks are possible)
- Combining with the bounds for $N_2(\texttt{COLL})$, we have

$$\boxed{\mathsf{CP}^{\mathsf{eq}}_{\ell} \leq \frac{1}{2^n} + O\left(\frac{t(\ell)}{2^{2n}}\right) + O\left(\frac{\ell^6}{2^{3n}}\right).}$$

- Better than [DGHKR04] for sufficiently large ℓ.

Improved Bound on $\mathsf{CP}^{\mathsf{any}}_{q,\ell,\sigma}$ and $\mathsf{CP}^{\mathsf{eq}}_{\ell}$

Message type = eq:

- $N_1(\mathtt{COLL}) = 1$ (only non-cyclic walks are possible)
- Combining with the bounds for $N_2(\mathtt{COLL})$, we have

$$\boxed{\mathsf{CP}^{\mathsf{eq}}_{\ell} \leq \frac{1}{2^n} + O\left(\frac{t(\ell)}{2^{2n}}\right) + O\left(\frac{\ell^6}{2^{3n}}\right).}$$

- Better than [DGHKR04] for sufficiently large ℓ.

Message type = any:

- Recall that $N_1(\mathtt{COLL} \wedge \neg \mathtt{Cyc}_{\ell/\sqrt{d'(\ell)}}) = q\ell\sqrt{d'(\ell)}$.
- Combining with the bounds for $N_2(\mathtt{COLL})$, we have

$$\boxed{\mathsf{CP}^{\mathsf{any}}_{q,\ell,\sigma} \leq O\left(\frac{2q\ell\sqrt{d'(\ell)}}{2^n} + \frac{q^2\ell^2}{2^{2n}} + \frac{q^2\ell^6}{2^{3n}}\right).}$$

- The bound reduces to $O(q^2/2^n)$ for $\ell < 2^{n/3}$. (improves over [JN16])

Conclusion

1. Revisited the collision analysis of CBC function.
2. Improved bounds on collision probability of CBC for eq and any type messages.
3. CP bounds imply improved PRF bounds for EMAC, ECBC and FCBC.

Thank you.