On the Exact Security of Message Authentication using Pseudorandom Functions

Fast Software Encryption '17, Tokyo

Ashwin Jha[1], Avradip Mandal[2], Mridul Nandi[1]

[1]Indian Statistical Institute, Kolkata, India
[2]Fujitsu Laboratories of America, Sunnyvale, USA

Overview

Preliminary

Motivation

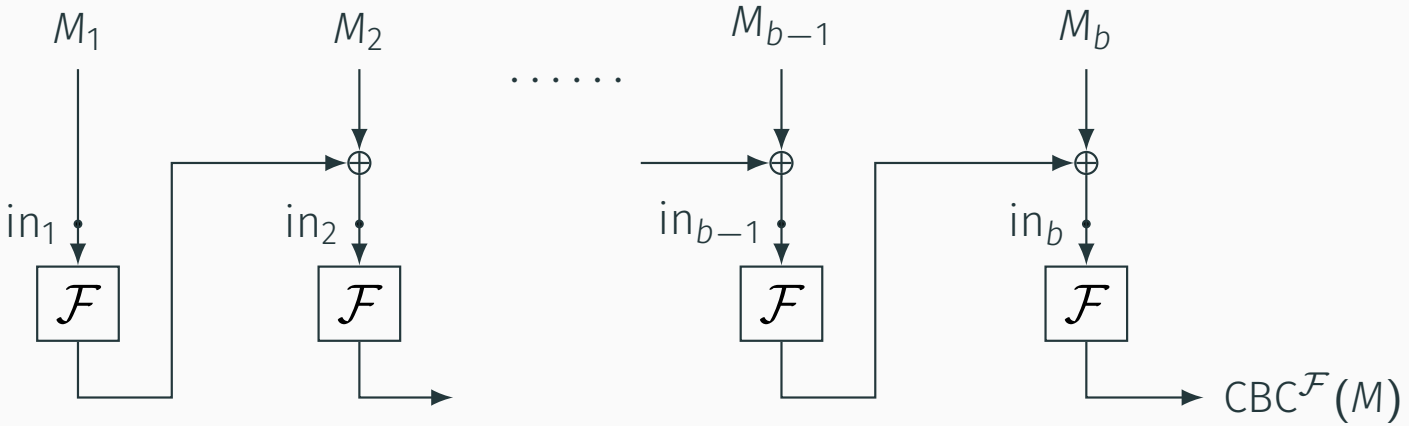
Contributions

Preliminary

Cipher Block Chaining

CBC function

For a length-preserving function $\mathcal{F} : \{0,1\}^n \to \{0,1\}^n$ and input $M := (M_1, M_2, \cdots, M_b) \in \{0,1\}^{nb}$ CBC is defined as,

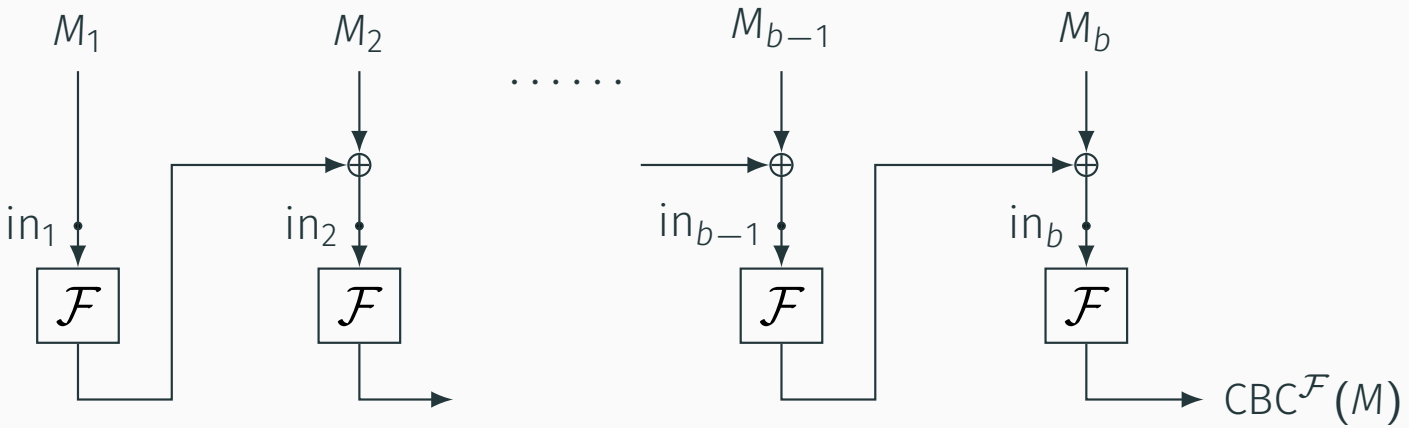


- For all $i \in \{1, \ldots, b\}$, in_i are called internal inputs.

Cipher Block Chaining

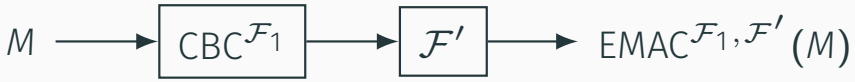
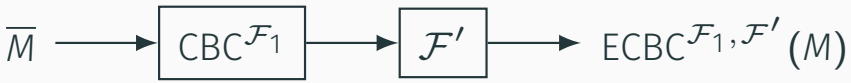
CBC function

For a length-preserving function $\mathcal{F} : \{0,1\}^n \to \{0,1\}^n$ and input $M := (M_1, M_2, \cdots, M_b) \in \{0,1\}^{nb}$ CBC is defined as,

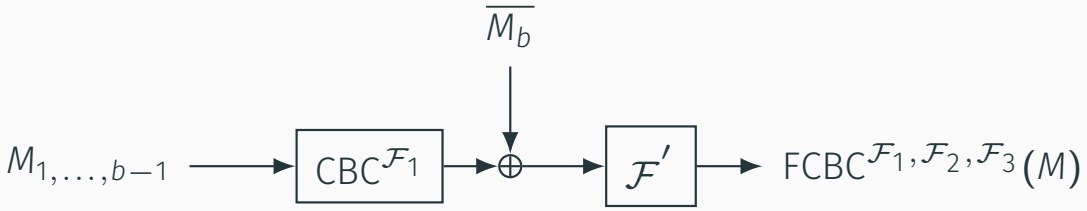
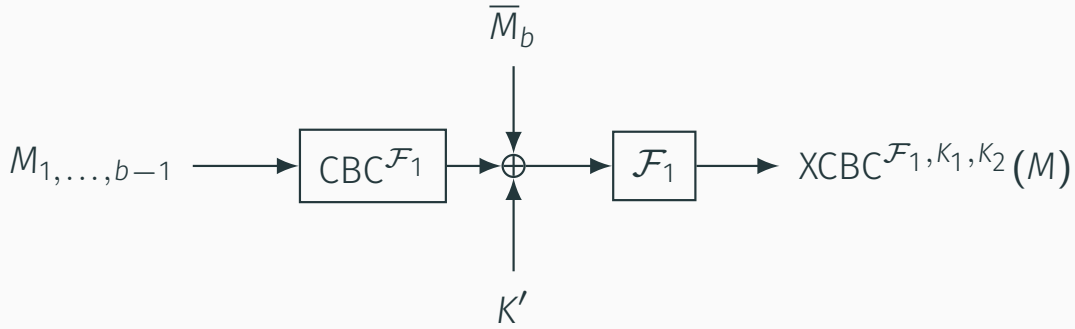
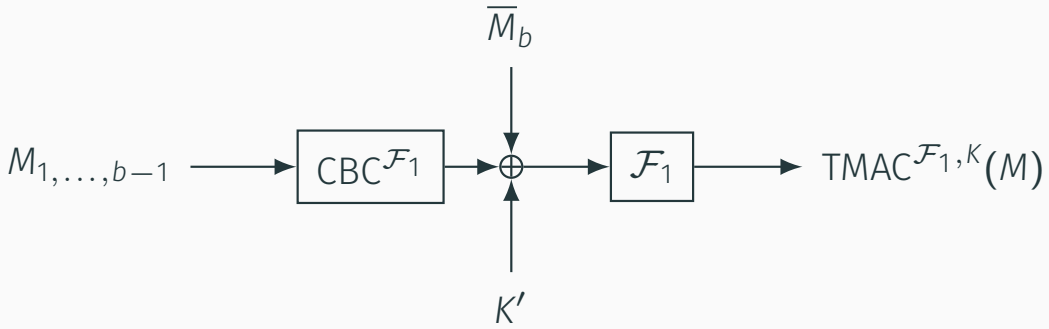


- For all $i \in \{1, \ldots, b\}$, in_i are called internal inputs.
- For prefix-free queries: secure MAC/PRF when $\mathcal{F}$ is a good pseudorandom permutation/function.
- The input space is restricted to $(\{0,1\}^n)^+$.

Some Variants of CBC-MAC

Construction	Multiple of n/Otherwise
	$\mathcal{F}' = \mathcal{F}_2$/not defined
	$\mathcal{F}' = \mathcal{F}_2/\mathcal{F}_3$

Some Variants of CBC-MAC

Construction	Multiple of n/Otherwise
	$\mathcal{F}' = \mathcal{F}_2/\mathcal{F}_3$
	$K' = K_1/K_2$
	$K' = K/u \cdot K$

Motivation

PRP based CBC-MACs

CBC-MACs	Random Permutation	
	Lower Bound	Upper Bound
CBC-MAC (Equal Length)	$\Omega\left(\frac{q^2}{2^n}\right)$	$O\left(\frac{\ell q^2}{2^n}\right)$ [BPR05, JN16]
CBC-MAC (Prefix Free)	$\Omega\left(\frac{q^2}{2^n}\right)$	$O\left(\frac{\ell q^2}{2^n}\right)$ [BPR05]
EMAC, ECBC, FCBC	$\Omega\left(\frac{q^2}{2^n}\right)$	$O\left(\frac{q^2}{2^n}\right)$ [Pie06, JN16]
XCBC, TMAC	$\Omega\left(\frac{q^2}{2^n}\right)$	$O\left(\frac{\sigma^2}{2^n}\right)$ [IK03b], $O\left(\frac{\ell q^2}{2^n}\right)$ [MM07]

PRF based CBC-MACs

Upper Bound

- PRF-PRP switching gives an upper bound of $O\left(\frac{\sigma^2}{2^n}\right)$.
- $O\left(\frac{\sigma^2}{2^n}\right)$ bound is rather loose. Can it be reduced?

PRF based CBC-MACs

Upper Bound

- PRF-PRP switching gives an upper bound of $O\left(\frac{\sigma^2}{2^n}\right)$.
- $O\left(\frac{\sigma^2}{2^n}\right)$ bound is rather loose. Can it be reduced?

Lower Bound

- Berke showed an attack on prefix-free CBC-MAC with $\frac{\ell^2 q^2}{2^n}$ distinguishing advantage.
- Berke's attack doesn't extend to CBC-MAC variants.
- A lower bound of $\frac{q^2}{2^n}$ is trivially achievable. Can we have a better attack?

Contributions

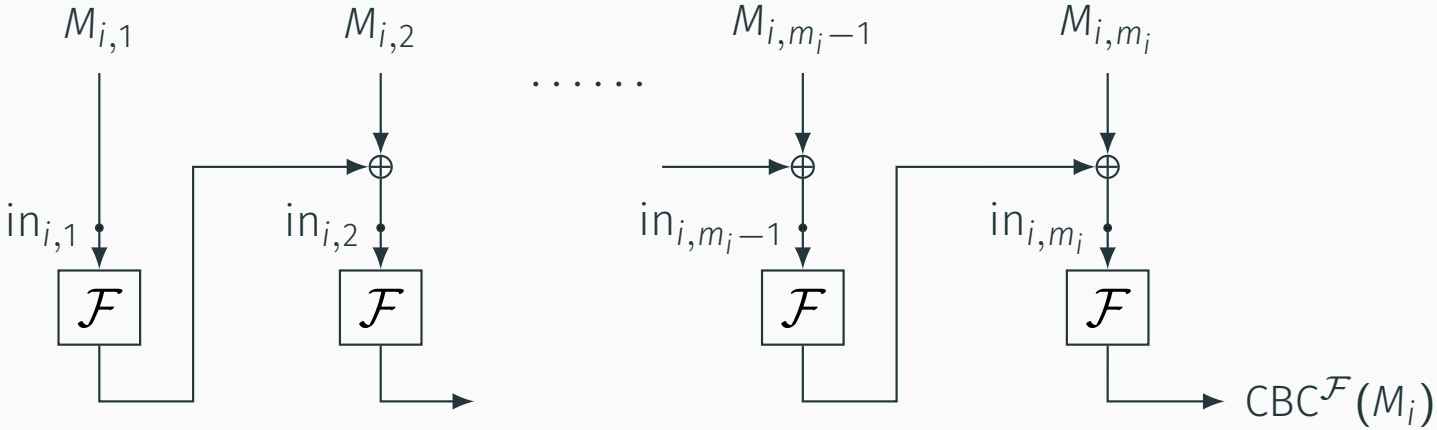
Summary of Our Results

- Tight PRF bounds for PRF based EMAC, ECBC, FCBC, XCBC and TMAC.
- Lower bound applicable to CBC-MAC (equal length), OMAC, and iterated random function.

	Random Function	
	Lower Bound	Upper Bound
CBC-MAC (Equal Length)	$\Omega\left(\frac{q\sigma}{2^n}\right)$	-
EMAC, ECBC	$\Omega\left(\frac{q\sigma}{2^n}\right)$	$O\left(\frac{q\sigma}{2^n}\right)$
FCBC	$\Omega\left(\frac{q\sigma}{2^n}\right)$	$O\left(\frac{q\sigma}{2^n}\right)$
XCBC, TMAC	$\Omega\left(\frac{q\sigma}{2^n}\right)$	$O\left(\frac{q\sigma}{2^n}\right)$

Upper Bound on PRF Security of MAC

For a tuple of $q \geq 2$ distinct messages $\mathcal{M} = (M_1, \ldots, M_q)$,



- $\texttt{INcoll}^{\mathcal{F}}(\mathcal{M})$ denotes the event

$$\exists\, i, j,\ 1 \leq i < j \leq q, \text{ such that } \mathrm{in}_{i,m_i} = \mathrm{in}_{j,m_j}.$$

- $\mathbf{inCP}(\mathcal{M}) = \Pr_{\mathcal{F}}[\texttt{INcoll}^{\mathcal{F}}(\mathcal{M})]$ and $\mathbf{inCP}_{q,\ell,\sigma} = \max_{\mathcal{M}} \mathbf{inCP}(\mathcal{M})$.

Upper Bound on PRF Security of MAC

Lemma

For $q, \ell, \sigma \geq 1$ we have,

1. $\mathbf{Adv}_{\mathrm{EMAC/ECBC}}(q, \ell, \sigma) \leq \mathbf{inCP}_{q,\ell,\sigma} + \dfrac{q(q-1)}{2N}$.
2. $\mathbf{Adv}_{\mathrm{FCBC}}(q, \ell, \sigma) \leq \mathbf{inCP}_{q,\ell,\sigma} + \dfrac{q(q-1)}{2N}$.
3. $\mathbf{Adv}_{\mathrm{XCBC/TMAC}}(q, \ell, \sigma) \leq \mathbf{inCP}_{q,\ell,\sigma} + \dfrac{q\sigma}{N} + \dfrac{q(q-1)}{2N}$.

Form here onwards MAC denotes EMAC, ECBC, FCBC, XCBC and TMAC. N denotes 2^n.

- 1 and 2 follows from the (delta) universal property of CBC-MAC.

Upper Bound on PRF Security of MAC

Lemma

For $q, \ell, \sigma \geq 1$ we have,

1. $\mathbf{Adv}_{\mathrm{EMAC/ECBC}}(q, \ell, \sigma) \leq \mathbf{inCP}_{q,\ell,\sigma} + \dfrac{q(q-1)}{2N}$.
2. $\mathbf{Adv}_{\mathrm{FCBC}}(q, \ell, \sigma) \leq \mathbf{inCP}_{q,\ell,\sigma} + \dfrac{q(q-1)}{2N}$.
3. $\mathbf{Adv}_{\mathrm{XCBC/TMAC}}(q, \ell, \sigma) \leq \mathbf{inCP}_{q,\ell,\sigma} + \dfrac{q\sigma}{N} + \dfrac{q(q-1)}{2N}$.

Form here onwards MAC denotes EMAC, ECBC, FCBC, XCBC and TMAC. N denotes 2^n.

- 1 and 2 follows from the (delta) universal property of CBC-MAC.
- 3 is derived by application of Coefficient H technique.

Upper Bound on CBC Collision Probability

Let $\mathcal{M} = (M_1, \ldots, M_q)$ be a q-tuple of distinct messages such that $M_i \in \{0,1\}^{nm_i}$, $1 \leq m_i \leq \ell$ for all $i \in \{1, \ldots, q\}$, and $\sum_{i=1}^{q} m_i \leq \sigma$.

Theorem: Upper Bound Theorem

For $\ell = O(q)$, $\frac{q^2\ell}{N} \leq 1$ we have,

$$\mathbf{inCP}_{q,\ell,\sigma} = O\left(\frac{q\sigma}{N}\right).$$

Proof Sketch:

- Graph [BPR05] based representation of collision pattern in CBC computation.
- Internal inputs => vertices and transition from in_i to in_{i+1} => directed edge from in_i to in_{i+1}.

Upper Bound on CBC Collision Probability

Proof Sketch:

- $\mathbf{bad}_1$: all graphs where walk corresponding to any message is cyclic. Bounded by $\sum_{i=1}^{q} \frac{m_i^2}{N}$.
- $\mathbf{bad}_2$: all graphs where walks corresponding to any two messages have at least two non-trivial collisions. Bounded $\sum_{1 \le i < j \le q} \frac{(m_i + m_j)^4}{N^2}$.

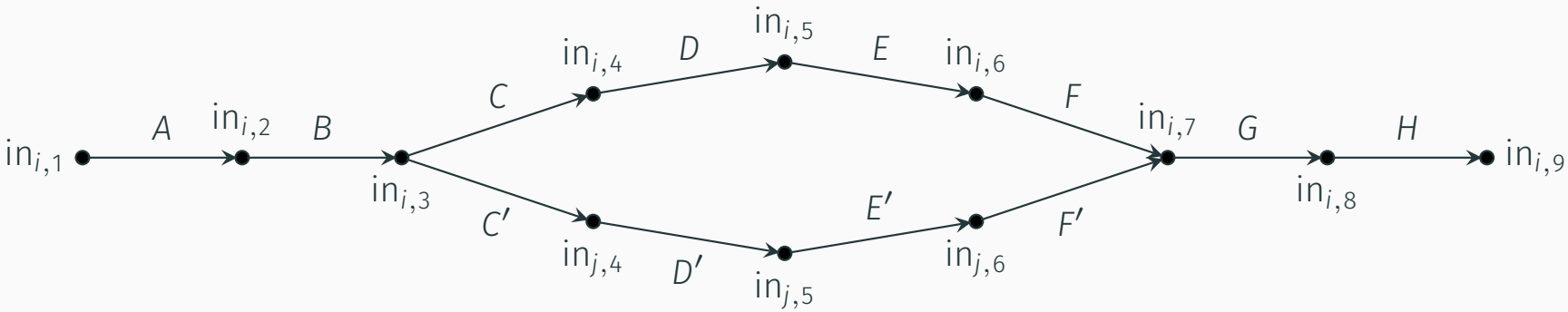
$$M_1 = (A, B, C, D, E, F, G, H) \text{ and } M_2 = (A, B, C', D', E', F', G, H)$$

Upper Bound on CBC Collision Probability

Proof Sketch:

- $\mathbf{bad}_1$: all graphs where walk corresponding to any message is cyclic. Bounded by $\sum_{i=1}^{q} \frac{m_i^2}{N}$.
- $\mathbf{bad}_2$: all graphs where walks corresponding to any two messages have at least two non-trivial collisions. Bounded $\sum_{1 \le i < j \le q} \frac{(m_i + m_j)^4}{N^2}$.

$$M_1 = (A, B, C, D, E, F, G, H) \text{ and } M_2 = (A, B, C', D', E', F', G, H)$$

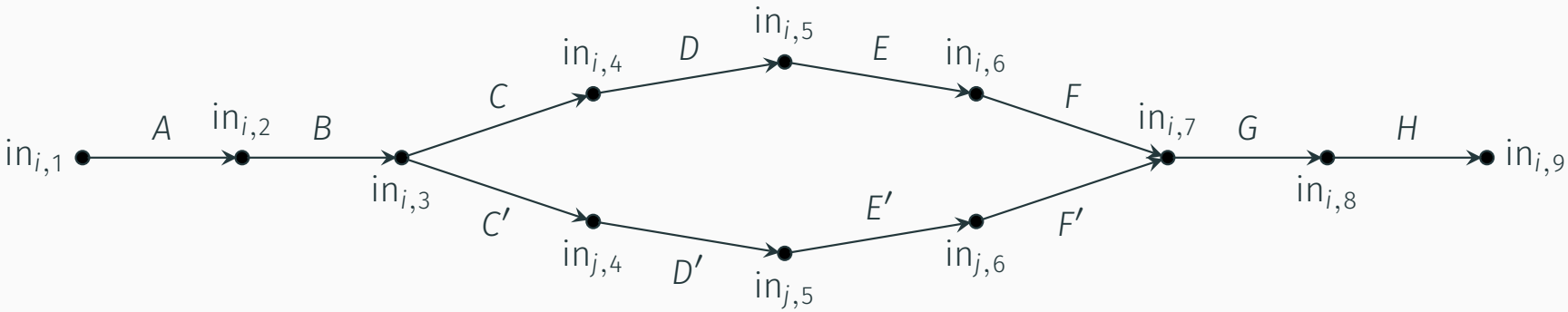


Upper Bound on CBC Collision Probability

Proof Sketch:

- $\mathbf{bad}_1$: all graphs where walk corresponding to any message is cyclic. Bounded by $\sum_{i=1}^{q} \frac{m_i^2}{N}$.
- $\mathbf{bad}_2$: all graphs where walks corresponding to any two messages have at least two non-trivial collisions. Bounded $\sum_{1 \le i < j \le q} \frac{(m_i+m_j)^4}{N^2}$.

$$M_1 = (A, B, C, D, E, F, G, H) \text{ and } M_2 = (A, B, C', D', E', F', G, H)$$



- The probability of collision event over the remaining graphs is bounded by $\sum_{1 \le i < j \le q} \frac{\min\{m_i, m_j\}}{N}$.
- Combining all three we get the result.

Lower Bound on PRF Security of MAC

Collision Distinguisher for MAC

1. Let $M_i = x_i \| 0^{n(\ell-1)}$, $x_i \in \{0,1\}^n$.
2. $\mathcal{A}$ queries M_i and observes the output t_i.
3. If $t_i = t_j$ for some $j < i$ then $\mathcal{A}$ returns 1.

Lemma (PRF–CBC Lower Bound)

$$\mathbf{Adv}_{\mathrm{MAC}}(q,\ell) \geq \mathbf{inCP}(\mathcal{M}) \left(1 - \frac{q(q-1)}{2N}\right).$$

Lower Bound on CBC Collision Probability

Theorem: Lower Bound Theorem

For $\frac{q^2\ell}{N} \leq 1$ and $\ell \leq \frac{N^{\frac{1}{3}}}{4}$ we have, $\mathbf{inCP}(\mathcal{M}) \geq \frac{q^2\ell}{12N}$.

Proof Sketch:

- Using Bonferroni Inequality,

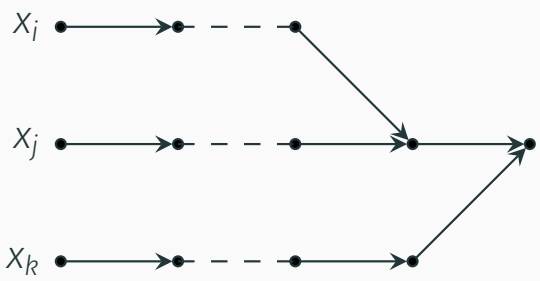
$$\mathbf{inCP}(\mathcal{M}) \geq \sum_{i<j} \overbrace{\Pr_{\mathcal{F}}[\mathtt{INcoll}^{\mathcal{F}}(M_i; M_j)]}^{\mathbf{inCP}_{i,j}}$$

$$- 3 \sum_{i<j<k} \overbrace{\Pr_{\mathcal{F}}[\mathtt{INcoll}^{\mathcal{F}}(M_i; M_j) \cap \mathtt{INcoll}^{\mathcal{F}}(M_j; M_k)]}^{\mathbf{inCP}_{i,j,k}}$$

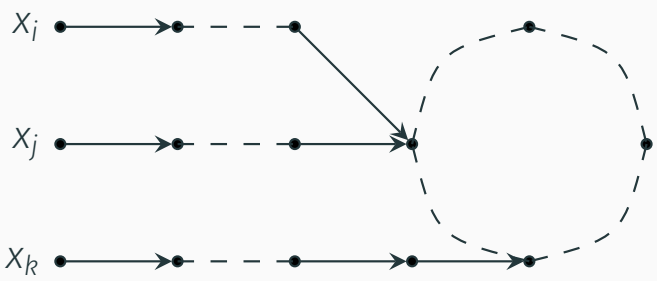
$$- \frac{1}{2} \sum_{\substack{i<j,k<m \\ \{i,j\}\cap\{k,m\}=\emptyset}} \overbrace{\Pr_{\mathcal{F}}[\mathtt{INcoll}^{\mathcal{F}}(M_i; M_j) \cap \mathtt{INcoll}^{\mathcal{F}}(M_k; M_m)]}^{\mathbf{inCP}_{i,j,k,m}}$$

Lower Bound on CBC Collision Probability

Proof Sketch: Bounding $\mathsf{inCP}_{i,j,k}$



Case 1.



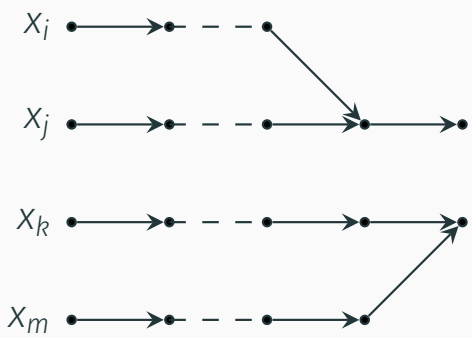
Case 2.

$$\Pr[\textbf{Case 1}] \leq \frac{2\ell^2}{N^2} \qquad \Pr[\textbf{Case 2}] \leq \frac{6\ell^6}{N^3}$$

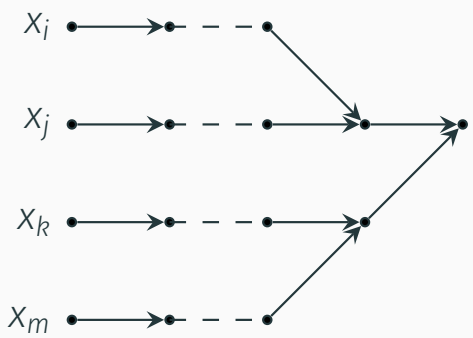
$$\boxed{\mathsf{inCP}_{i,j,k} \leq \frac{2\ell^2}{N^2} + \frac{6\ell^6}{N^3}.}$$

Lower Bound on CBC Collision Probability

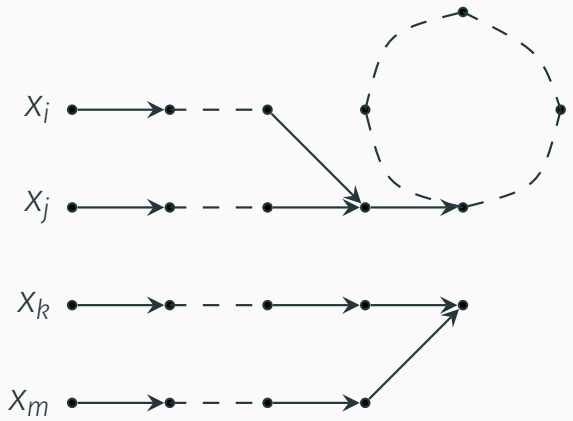
Proof Sketch: Bounding $\text{inCP}_{i,j,k,m}$



Case 1.



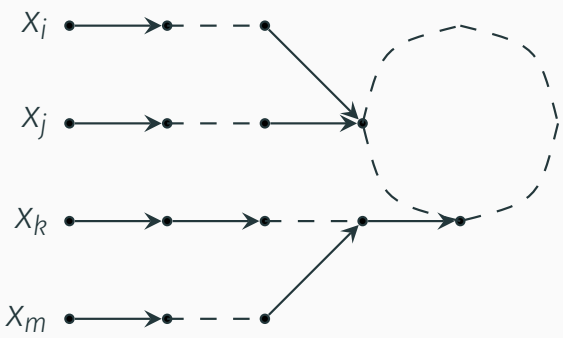
Case 2.



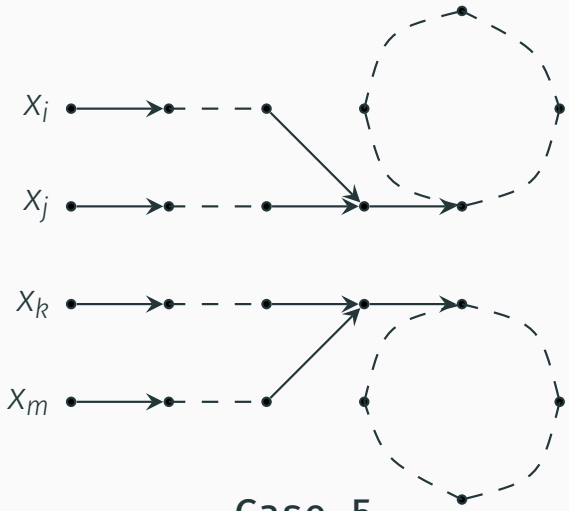
Case 3.

$\Pr[\textbf{Case 4}] \leq \frac{\ell^2}{N^2}$ $\Pr[\textbf{Case 2}] \leq \frac{6\ell^3}{N^3}$ $\Pr[\textbf{Case 3}] \leq \frac{2\ell^5}{N^3}$

Lower Bound on CBC Collision Probability



Case 4.



Case 5.

$$\Pr[\textbf{Case 4}] \leq \tfrac{24\ell^8}{N^4} \qquad \Pr[\textbf{Case 5}] \leq \tfrac{4\ell^8}{N^4}.$$

$$\boxed{\mathsf{inCP}_{i,j,k,m} \leq \frac{\ell^2}{N^2} + \frac{6\ell^3 + 2\ell^5}{N^3} + \frac{28\ell^8}{N^4}.}$$

Lower Bound on CBC Collision Probability

Proof Sketch: Bounding $\mathsf{inCP}_{i,j}$

- $\texttt{cycle}$ denotes the event that at least one of the walks (corresponding to M_i or M_j) has a cycle.

$$\mathsf{inCP}_{i,j|\neg\texttt{cycle}} = \frac{\ell}{N} \qquad \Pr[\texttt{cycle}] \leq \frac{2\ell^2}{N}.$$

$$\boxed{\mathsf{inCP}_{i,j} \geq \frac{\ell}{N}\left(1 - \frac{2\ell^2}{N}\right).}$$

- Combining all the cases we have, for $\frac{q^2\ell}{N} \leq 1$ and $\ell \leq \frac{N^{\frac{1}{3}}}{4}$, $\mathsf{inCP}(\mathcal{M}) \geq \frac{q^2\ell}{12N}$.

Tight PRF Security Bound for MACs

Theorem: PRF Bound

For $\frac{q^2\ell}{N} < 1,\ q \leq \sqrt{N},\ \ell \leq \min\left\{q, \frac{N^{\frac{1}{3}}}{4}\right\}$ we have,

$$\mathsf{Adv}_{\mathsf{MAC}}(q, \ell, \sigma) = \Theta\left(\frac{q\sigma}{N}\right).$$

"For CBC-MACs, PRP is a provably better choice than PRF"

Questions?