Revisiting Randomness Extraction and Key Derivation Using the CBC and Cascade Modes

Niranjan Balachandran
IIT Bombay

Ashwin Jha
CISPA → RUB

Mridul Nandi
ISI Kolkata

Soumit Pal
ISI Kolkata

FSE 2024

CASA
Cyber Security in the Age of Large-Scale Adversaries

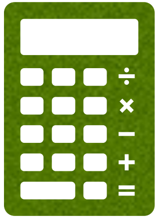
Ruhr Universität Bochum RUB

Gefördert durch DFG Deutsche Forschungsgemeinschaft

HGI Horst Görtz Institut

RANDOMNESS EXTRACTOR

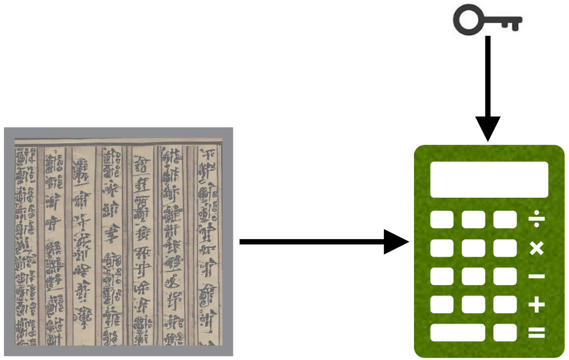
RANDOMNESS EXTRACTOR



$$h : \{0,1\}^k \times \{0,1\}^{n\ell} \rightarrow \{0,1\}^n$$

RANDOMNESS EXTRACTOR

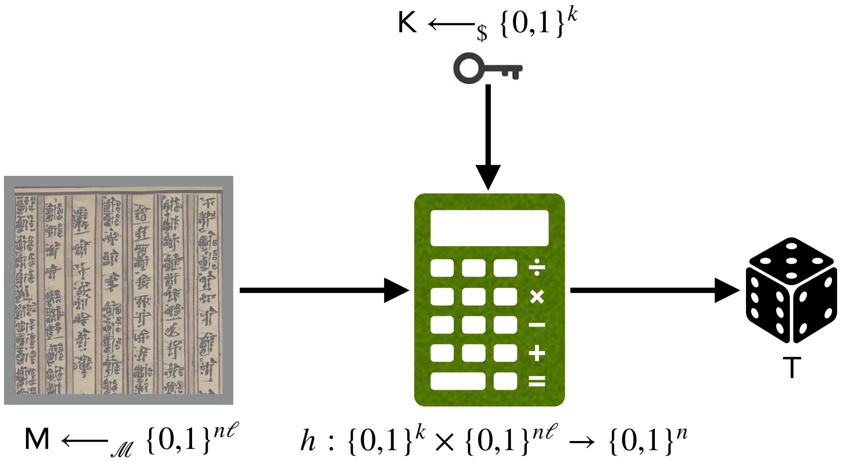
$\mathsf{K} \xleftarrow{}_{\$} \{0,1\}^k$



$\mathsf{M} \xleftarrow{}_{\mathscr{M}} \{0,1\}^{n\ell}$

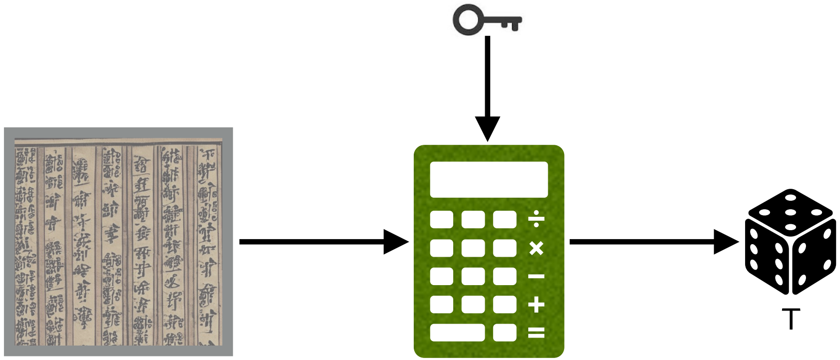
$h : \{0,1\}^k \times \{0,1\}^{n\ell} \to \{0,1\}^n$

RANDOMNESS EXTRACTOR



RANDOMNESS EXTRACTOR

$\mathsf{K} \xleftarrow{}_{\$} \{0,1\}^k$



$\mathsf{M} \xleftarrow{}_{\mathscr{M}} \{0,1\}^{n\ell}$ $\quad h : \{0,1\}^k \times \{0,1\}^{n\ell} \to \{0,1\}^n$

$$(\mathsf{K}, \mathsf{T}) \approx_{\mathrm{neg}(n)} (\mathsf{K}, \mathsf{U}_n)$$

$\mathsf{U}_n \xleftarrow{}_{\$} \{0,1\}^n$

UNIVERSAL HASHING TO EXTRACTOR

CASA
CYBER SECURITY IN THE AGE OF LARGE-SCALE ADVERSARIES

UNIVERSAL HASHING TO EXTRACTOR

CASA
Cyber Security in the Age of Large-Scale Adversaries

Leftover Hash Lemma+ [DGHKR, CRYPTO 2004]

Suppose $h : \{0,1\}^k \times \{0,1\}^{n\ell} \to \{0,1\}^n$ satisfies the property

$$\Pr\left(h_{\mathsf{K}}(\mathsf{M}) = h_{\mathsf{K}}(\mathsf{M}') \mid \mathsf{M} \neq \mathsf{M}'\right) \leq \frac{1}{2^n} + \epsilon_h,$$

where $\mathsf{K} \xleftarrow{}_{\$} \{0,1\}^k$ and $\mathsf{M}, \mathsf{M}' \xleftarrow{}_{\mathscr{M}} \{0,1\}^{n\ell}$. Then,

$$(\mathsf{K}, h_{\mathsf{K}}(\mathsf{M})) \approx_{O\left(\sqrt{2^{n-H_\infty(\mathscr{M})} + 2^n \epsilon_h}\right)} (\mathsf{K}, \mathsf{U}_n)$$

where $\mathsf{M} \xleftarrow{}_{\mathscr{M}} \{0,1\}^{n\ell}$.

UNIVERSAL HASHING TO EXTRACTOR

Leftover Hash Lemma+ [DGHKR, CRYPTO 2004]

Suppose $h : \{0,1\}^k \times \{0,1\}^{n\ell} \to \{0,1\}^n$ satisfies the property

$$\Pr\left(h_{\mathsf{K}}(\mathsf{M}) = h_{\mathsf{K}}(\mathsf{M}') \mid \mathsf{M} \neq \mathsf{M}'\right) \leq \frac{1}{2^n} + \epsilon_h,$$

where $\mathsf{K} \xleftarrow{}_{\$} \{0,1\}^k$ and $\mathsf{M}, \mathsf{M}' \xleftarrow{}_{\mathscr{M}} \{0,1\}^{n\ell}$. Then,

$$(\mathsf{K}, h_{\mathsf{K}}(\mathsf{M})) \approx_{O\left(\sqrt{2^{n-H_\infty(\mathscr{M})} + 2^n\epsilon_h}\right)} (\mathsf{K}, \mathsf{U}_n)$$

where $\mathsf{M} \xleftarrow{}_{\mathscr{M}} \{0,1\}^{n\ell}$.

ϵ_h must be in $o\left(2^{-n}\right)$

CBC AND Cascade FUNCTIONS

CBC AND Cascade FUNCTIONS

CYBER SECURITY IN THE AGE OF LARGE-SCALE ADVERSARIES

CIPHER BLOCK CHAINING

$$\mathtt{CBC} : \{0,1\}^k \times \{0,1\}^{n\ell} \to \{0,1\}^n$$

CBC AND Cascade FUNCTIONS

CIPHER BLOCK CHAINING

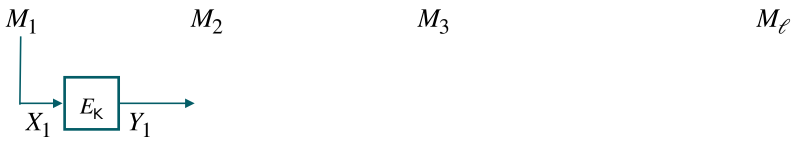
$$\mathtt{CBC} : \{0,1\}^k \times \{0,1\}^{n\ell} \to \{0,1\}^n$$

M_1 M_2 M_3 M_ℓ

CBC AND Cascade FUNCTIONS

CIPHER BLOCK CHAINING

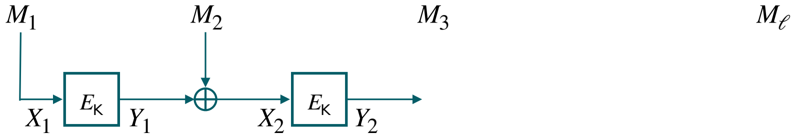
$$\texttt{CBC} : \{0,1\}^k \times \{0,1\}^{n\ell} \to \{0,1\}^n$$



CBC AND Cascade FUNCTIONS

CIPHER BLOCK CHAINING

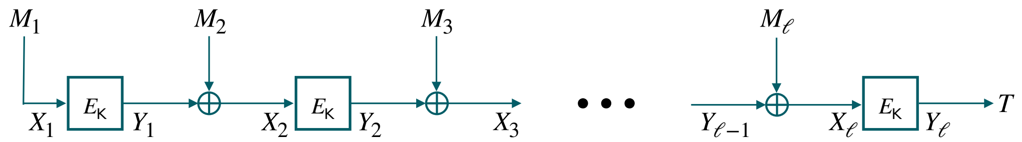
$$\mathsf{CBC} : \{0,1\}^k \times \{0,1\}^{n\ell} \to \{0,1\}^n$$



CBC AND Cascade FUNCTIONS

CIPHER BLOCK CHAINING

$$\mathtt{CBC} : \{0,1\}^k \times \{0,1\}^{n\ell} \rightarrow \{0,1\}^n$$

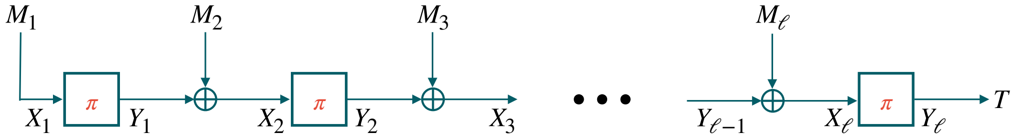


CBC AND Cascade FUNCTIONS

CYBER SECURITY IN THE AGE OF LARGE-SCALE ADVERSARIES

CIPHER BLOCK CHAINING

$$\mathrm{CBC}_{\pi} : \{0,1\}^{n\ell} \rightarrow \{0,1\}^{n}$$



$\pi \longleftarrow_{\$} \mathsf{Perm}(n)$

$\mathtt{CBC}$ AND $\mathtt{Cascade}$ FUNCTIONS

CASA
CYBER SECURITY IN THE AGE OF LARGE-SCALE ADVERSARIES

$\mathtt{Cascade}$

$$\mathtt{Cas}_f : \{0,1\}^n \times \{0,1\}^{n\ell} \to \{0,1\}^n$$

$f \longleftarrow_{\$} \mathsf{Func}(2n, n)$

CBC AND Cascade FUNCTIONS

Cascade

$$\texttt{Cas}_f : \{0,1\}^n \times \{0,1\}^{n\ell} \to \{0,1\}^n$$

M_1 M_2 M_3 M_ℓ

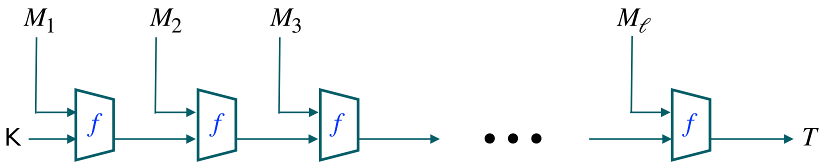
$f \longleftarrow_\$ \mathsf{Func}(2n, n)$

CBC AND Cascade FUNCTIONS

CASA
Cyber Security in the Age of Large-Scale Adversaries

Cascade

$$\mathtt{Cas}_f : \{0,1\}^n \times \{0,1\}^{n\ell} \rightarrow \{0,1\}^n$$



$f \longleftarrow_{\$} \mathsf{Func}(2n, n)$

COLLISION BIAS OF $\texttt{CBC}$ AND $\texttt{Cascade}$

Lemma 3 [DGHKR, CRYPTO 2004]

For $\pi \xleftarrow{}_{\$}$ Perm(n), $\ell \le 2^{n/4}$, and distinct $M, M' \in \{0,1\}^{n\ell}$, we have

$$\Pr\left(\texttt{CBC}_\pi(M) = \texttt{CBC}_\pi(M')\right) \le \frac{1}{2^n} + O\left(\frac{\ell^2}{2^{2n}}\right)$$

Lemma 4 [DGHKR, CRYPTO 2004]

For $f \xleftarrow{}_{\$}$ Func$(2n, n)$, $\ell \le 2^{n/4}$, $H_\infty(\mathscr{X}) > \log_2(\ell)$, we have

$$\Pr\left(\texttt{Cas}_f(K, \mathsf{M}) = \texttt{Cas}_f(K, \mathsf{M}')\right) \le \frac{\ell}{2^{n+H_\infty(\mathscr{X})}} + O\left(\frac{\ell^2}{2^{2n}}\right),$$

where $\mathsf{M}, \mathsf{M}' \xleftarrow{}_{\mathscr{X}} \{0,1\}^{n\ell}$ and K is some arbitrary constant.

COLLISION BIAS OF $\texttt{CBC}$ AND $\texttt{Cascade}$

Lemma 3 [DGHKR, CRYPTO 2004]

For $\pi \xleftarrow{}_{\$} \mathsf{Perm}(n)$, $\ell \leq 2^{n/4}$, and distinct $M, M' \in \{0,1\}^{n\ell}$, we have

$$\Pr\left(\texttt{CBC}_\pi(M) = \texttt{CBC}_\pi(M')\right) \leq \frac{1}{2^n} + O\left(\frac{\ell^2}{2^{2n}}\right)$$

Lemma 4 [DGHKR, CRYPTO 2004]

For $f \xleftarrow{}_{\$} \mathsf{Func}(2n, n)$, $\ell \leq 2^{n/4}$, $H_\infty(\mathscr{X}) > \log_2(\ell)$, we h

$$\Pr\left(\texttt{Cas}_f(K, \mathsf{M}) = \texttt{Cas}_f(K, \mathsf{M}')\right) \leq \frac{\ell}{2^{n+H_\infty(\mathscr{X})}} + O\left(\frac{\ell^2}{2^{2n}}\right)$$

where $\mathsf{M}, \mathsf{M}' \xleftarrow{}_{\mathscr{X}} \{0,1\}^{n\ell}$ and K is some arbitrary constant.

No proof available in the paper!

OUR CONTRIBUTIONS

- A proof of Lemma 3 and 4 in [DGHKR].
- Some new insights in the graph-based analysis of $\mathtt{CBC}$ and $\mathtt{Cascade}$.

$\mathtt{CBC}$ COLLISION PROBABILITY

CYBER SECURITY IN THE AGE OF LARGE-SCALE ADVERSARIES

The Problem

For any $M, M' \in \{0,1\}^{n+}$ let

$$\text{Coll}(M, M') : \quad \mathtt{CBC}_\pi(M) = \mathtt{CBC}_\pi(M').$$

Then, for $\ell \leq 2^{n/4}$ and any $M \neq M' \in \{0,1\}^{n\ell}$, we want to show

$$\Pr\left(\text{Coll}(M, M')\right) \leq \frac{1}{2^n} + O\left(\frac{\ell^2}{2^{2n}}\right)$$

CBC COLLISION PROBABILITY

Lemma 5 [BPR, CRYPTO 2005]

For $\pi \longleftarrow_{\$} \mathsf{Perm}(n)$, $\ell \leq 2^{n/4}$, and $M \neq M' \in \{0,1\}^{n(\leq \ell)}$

$$\Pr\left(\mathsf{Coll}(M, M')\right) \leq \frac{\ell^{o(1)}}{2^n} + O\left(\frac{\ell^4}{2^{2n}}\right)$$

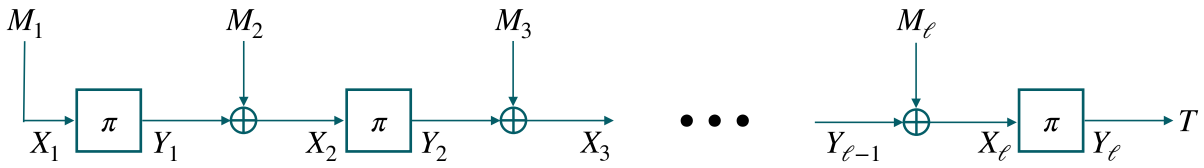
Lemma 8.1 [JN, J. Math. Cryptol. 2016]

For $\pi \longleftarrow_{\$} \mathsf{Perm}(n)$, $\ell \leq 2^{n/4}$, and $M^1 \neq \cdots \neq M^q \in \{0,1\}^{n(\leq \ell)}$

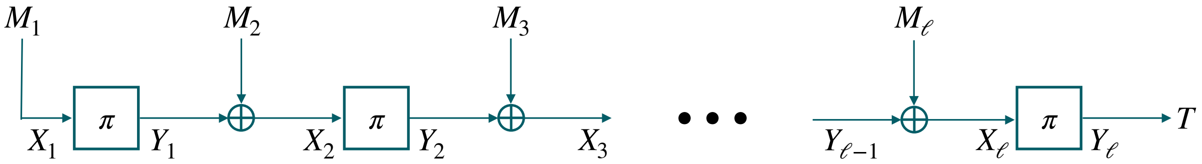
$$\Pr\left(\exists i \neq j : \mathsf{Coll}(M^i, M^j)\right) \leq \frac{q^2}{2^{n+1}} + \frac{q\ell^2}{2^n} + O\left(\frac{q^2\ell^4}{2^{2n}}\right)$$

STRUCTURE GRAPH

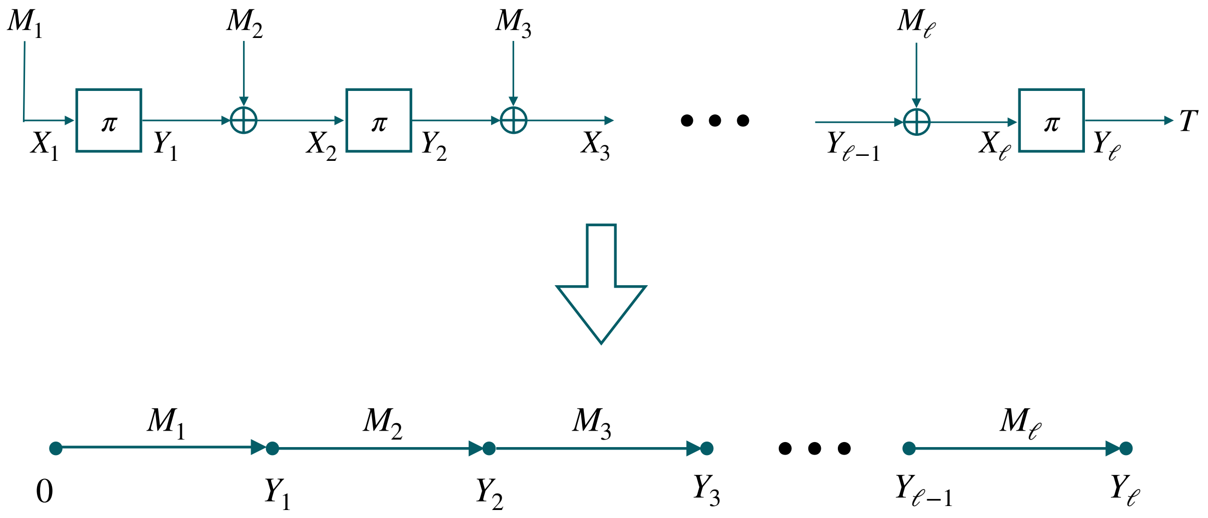
STRUCTURE GRAPH



STRUCTURE GRAPH

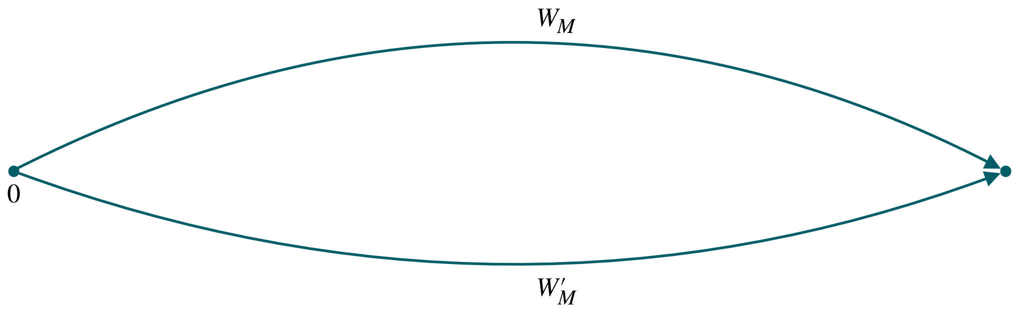


STRUCTURE GRAPH



CASA
CYBER SECURITY IN THE AGE OF LARGE-SCALE ADVERSARIES

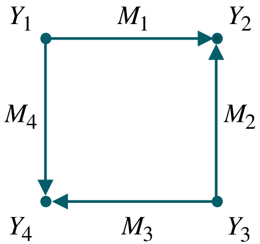
COLLISIONS ON THE STRUCTURE GRAPH



$$\text{Coll}(M, M') : \quad \big(\text{Endpoint}(W_M) = \text{Endpoint}(W_{M'})\big)$$

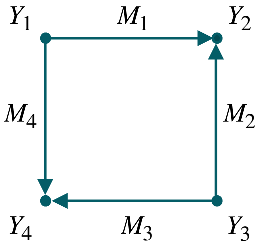
ACCIDENTS AND INDUCED COLLISIONS

ACCIDENTS AND INDUCED COLLISIONS

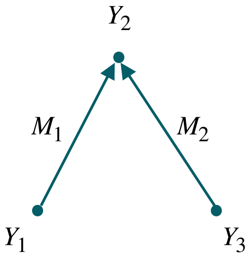


$$M_1 \oplus M_2 \oplus M_3 \oplus M_4 = 0$$

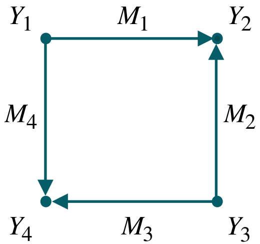
ACCIDENTS AND INDUCED COLLISIONS



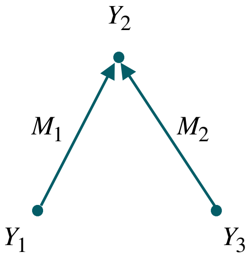
$$M_1 \oplus M_2 \oplus M_3 \oplus M_4 = 0$$



ACCIDENTS AND INDUCED COLLISIONS



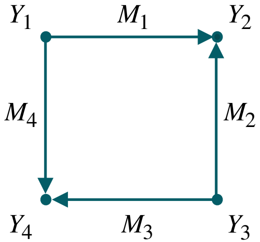
$$M_1 \oplus M_2 \oplus M_3 \oplus M_4 = 0$$



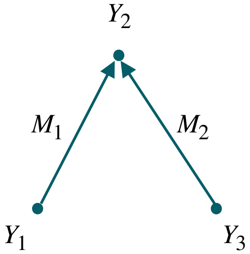
$$\pi(Y_1 \oplus M_1) = \pi(Y_3 \oplus M_2)$$
$$\iff Y_1 \oplus Y_3 = M_1 \oplus M_2$$
$$\iff Y_1 \oplus Y_3 = M_3 \oplus M_4$$
$$\iff \pi(Y_1 \oplus M_4) = \pi(Y_3 \oplus M_3)$$

CYBER SECURITY IN THE AGE OF LARGE-SCALE ADVERSARIES

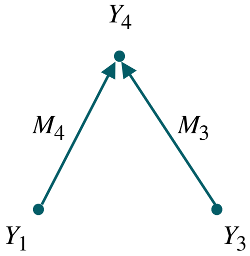
ACCIDENTS AND INDUCED COLLISIONS



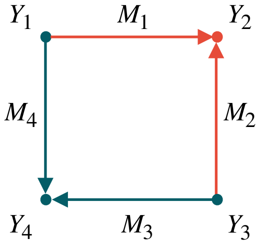
$$M_1 \oplus M_2 \oplus M_3 \oplus M_4 = 0$$



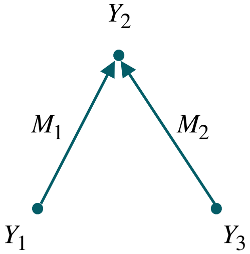
$$\pi(Y_1 \oplus M_1) = \pi(Y_3 \oplus M_2)$$
$$\Longleftrightarrow Y_1 \oplus Y_3 = M_1 \oplus M_2$$
$$\Longleftrightarrow Y_1 \oplus Y_3 = M_3 \oplus M_4$$
$$\Longleftrightarrow \pi(Y_1 \oplus M_4) = \pi(Y_3 \oplus M_3)$$



ACCIDENTS AND INDUCED COLLISIONS

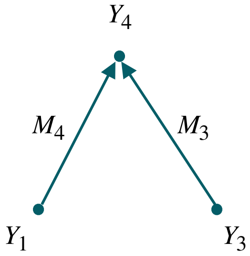


$$M_1 \oplus M_2 \oplus M_3 \oplus M_4 = 0$$



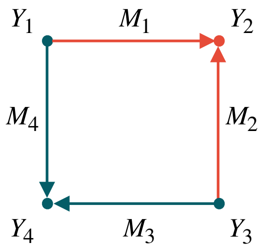
Accident

$$\pi(Y_1 \oplus M_1) = \pi(Y_3 \oplus M_2)$$
$$\Longleftrightarrow Y_1 \oplus Y_3 = M_1 \oplus M_2$$
$$\Longleftrightarrow Y_1 \oplus Y_3 = M_3 \oplus M_4$$
$$\Longleftrightarrow \pi(Y_1 \oplus M_4) = \pi(Y_3 \oplus M_3)$$

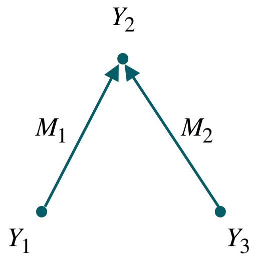


Induced collision

ACCIDENTS AND INDUCED COLLISIONS

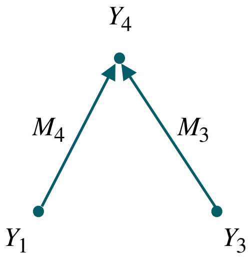


$$M_1 \oplus M_2 \oplus M_3 \oplus M_4 = 0$$



Accident

$$\begin{aligned} & \pi(Y_1 \oplus M_1) = \pi(Y_3 \oplus M_2) \\ \iff & Y_1 \oplus Y_3 = M_1 \oplus M_2 \\ \iff & Y_1 \oplus Y_3 = M_3 \oplus M_4 \\ \iff & \pi(Y_1 \oplus M_4) = \pi(Y_3 \oplus M_3) \end{aligned}$$



Induced collision

Lemma 7 [BPR, CRYPTO 2005]

Any graph is uniquely determined by its set of accidents and the messages M and M'.

ACCIDENTS AND INDUCED COLLISIONS

CASA
Cyber Security in the Age of Large-Scale Adversaries

The Tool

For any $a \geq 1$

$$\Pr\left(\mathsf{Coll}(M, M')\right) \leq \sum_{i=1}^{a} \frac{|\mathcal{G}_i(\mathsf{Coll}(M, M'))|}{2^{ni}} + O\left(\frac{\ell^{2(a+1)}}{2^{n(a+1)}}\right)$$

where $\mathcal{G}_i(\mathsf{Coll}(M, M'))$ is the set of all graphs with exactly i accidents and that satisfy $\mathsf{Coll}(M, M')$.

ACCIDENTS AND INDUCED COLLISIONS

CASA
Cyber Security in the Age of Large-Scale Adversaries

The Tool

For any $a = 2$

$$\Pr\left(\mathsf{Coll}(M, M')\right) \leq \sum_{i=1}^{2} \frac{|\mathcal{G}_i(\mathsf{Coll}(M, M'))|}{2^{ni}} + O\left(\frac{\ell^6}{2^{3n}}\right)$$

where $\mathcal{G}_i(\mathsf{Coll}(M, M'))$ is the set of all graphs with exactly i accidents and that satisfy $\mathsf{Coll}(M, M')$.

ACCIDENTS AND INDUCED COLLISIONS

CASA
CYBER SECURITY IN THE AGE OF LARGE-SCALE ADVERSARIES

The Tool

For any $a = 2$

$$\Pr\left(\mathsf{Coll}(M, M')\right) \leq \sum_{i=1}^{2} \frac{|\mathcal{G}_i(\mathsf{Coll}(M, M'))|}{2^{ni}} + O\left(\frac{\ell^6}{2^{3n}}\right)$$

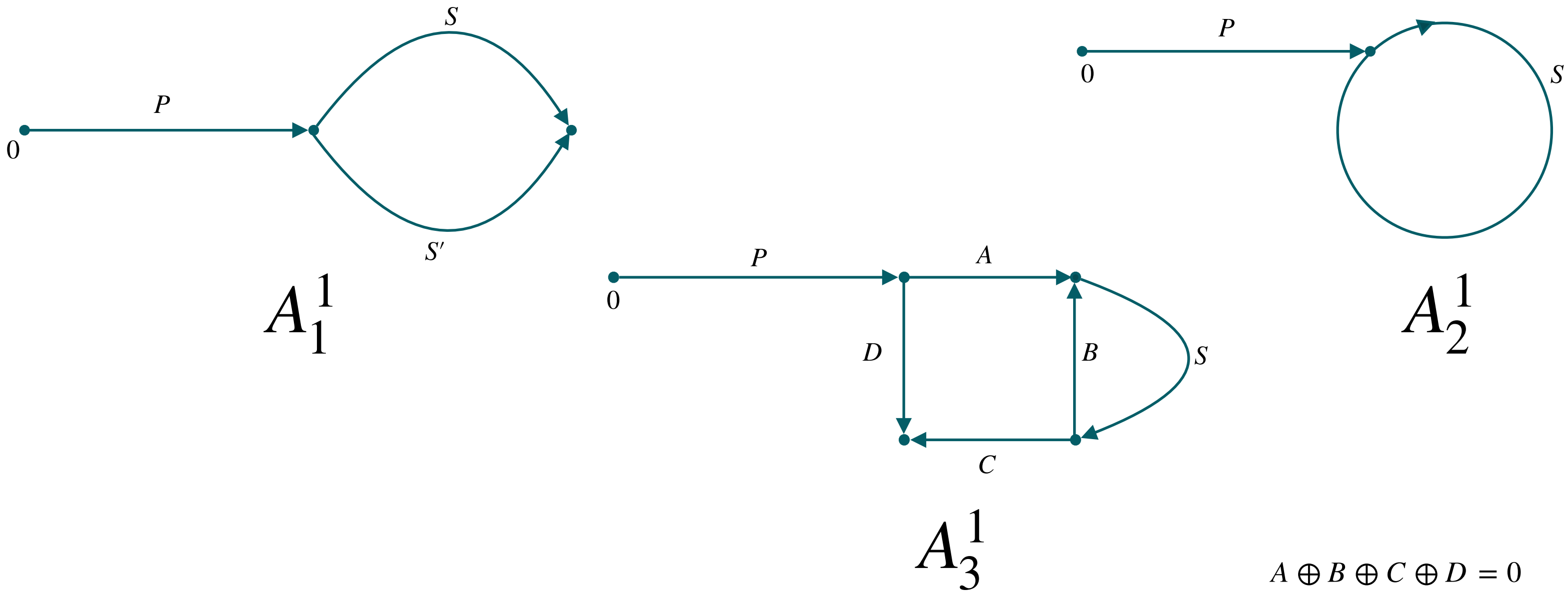
where $\mathcal{G}_i(\mathsf{Coll}(M, M'))$ is the set of all graphs with exactly i accidents and that satisfy $\mathsf{Coll}(M, M')$.

$|\mathcal{G}_1(\mathsf{Coll}(M, M'))| \leq 1$ $\qquad$ $|\mathcal{G}_2(\mathsf{Coll}(M, M'))| = O(\ell^2)$

CHARACTERISING ACCIDENT ≤ 2 GRAPHS

CHARACTERISING ACCIDENT ≤ 2 GRAPHS

Accident 1 Graphs, Lemma 7.2 [JN, J. Math. Cryptol. 2016]



CHARACTERISING ACCIDENT ≤ 2 GRAPHS

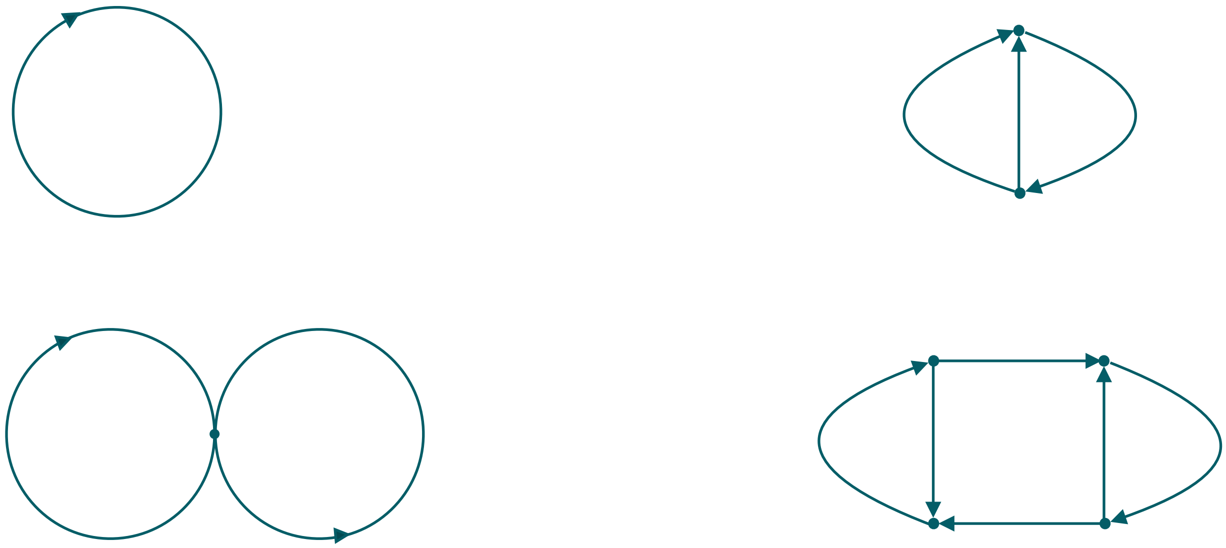
CASA
CYBER SECURITY IN THE AGE OF LARGE-SCALE ADVERSARIES

Core

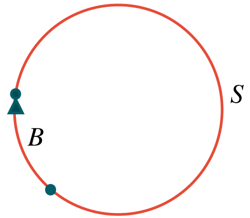
Maximal strongly connected components of a structure graph.

CHARACTERISING ACCIDENT ≤ 2 GRAPHS

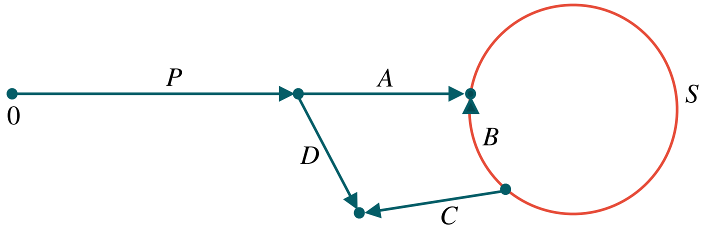
Core



CHARACTERISING ACCIDENT ≤ 2 GRAPHS



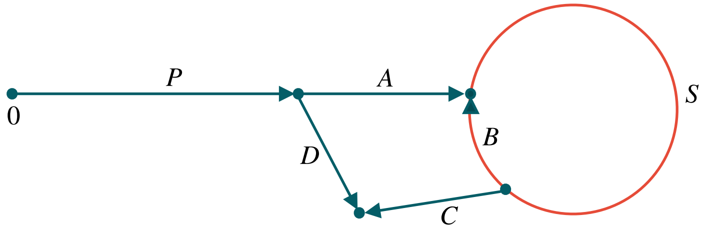
CHARACTERISING ACCIDENT ≤ 2 GRAPHS

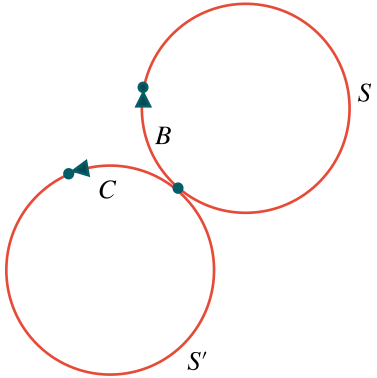


$$A_3^1$$

#accidents = 1,
#collisions = 2

CHARACTERISING ACCIDENT ≤ 2 GRAPHS

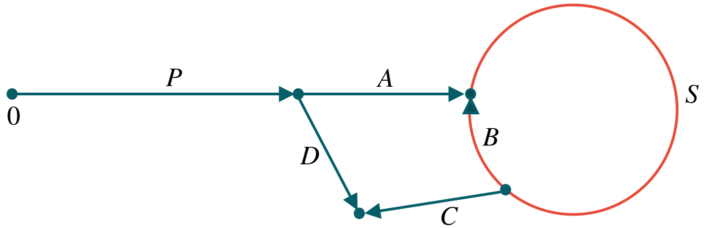




A_3^1

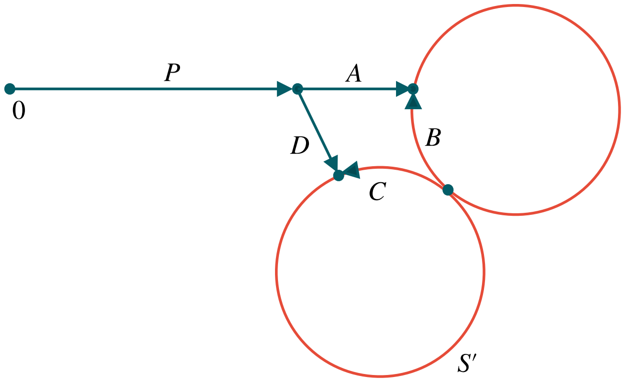
#accidents = 1,
#collisions = 2

CHARACTERISING ACCIDENT ≤ 2 GRAPHS



A_3^1

#accidents = 1,
#collisions = 2



#accidents = 2,
#collisions = 3

FINAL REMARKS

CASA
CYBER SECURITY IN THE AGE OF LARGE-SCALE ADVERSARIES

- A total of 18 non-isomorphic types of accident-2 graphs possible.

- In the paper:

$$|\mathcal{G}_1(\mathsf{Coll}(M, M'))| = 1$$

$$|\mathcal{G}_2(\mathsf{Coll}(M, M'))| = O(\ell^2)$$

- A similar analysis for the $\mathtt{Cascade}$ construction.

FINAL REMARKS

CASA
Cyber Security in the Age of Large-Scale Adversaries

- A total of 18 non-isomorphic types of accident-2 graphs possible.
- In the paper:

$$|\mathcal{G}_1(\mathsf{Coll}(M, M'))| = 1$$

$$|\mathcal{G}_2(\mathsf{Coll}(M, M'))| = O(\ell^2)$$

  - A similar analysis for the $\mathtt{Cascade}$ construction.

Thank you for your attention!