Revisiting the Security of COMET Authenticated Encryption Scheme

Shay Gueron[1,2] Ashwin Jha[3] Mridul Nandi[3]

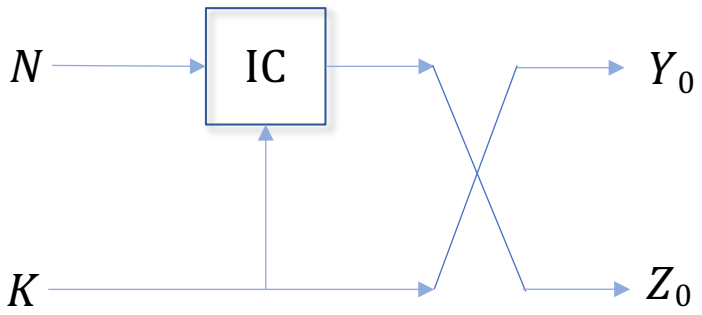
[1]University of Haifa, Israel [2]Amazon Web Services, USA [3]Indian Statistical Institute Kolkata, India

NIST Lightweight Cryptography Workshop 2020

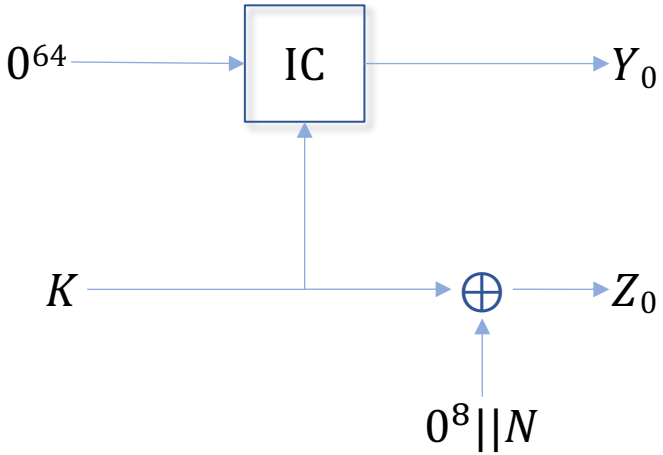
October 19-21, 2020

COMET: a quick overview

Initialization:



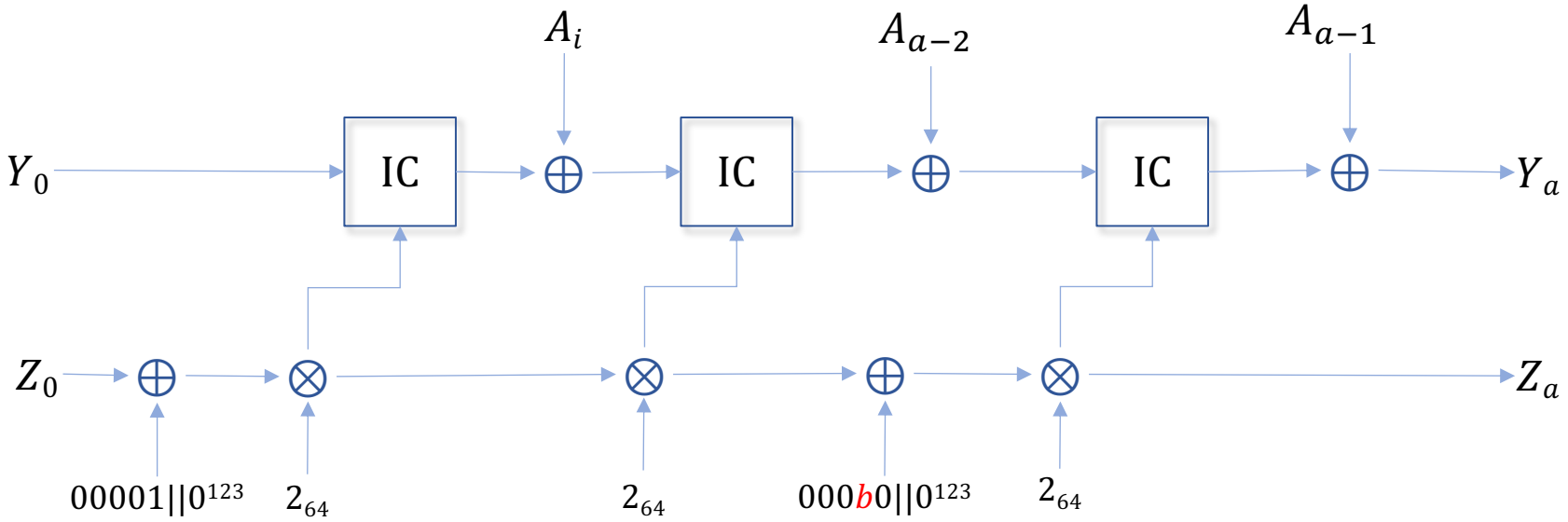
COMET-128



COMET-64

COMET: a quick overview

Associated Data Processing:

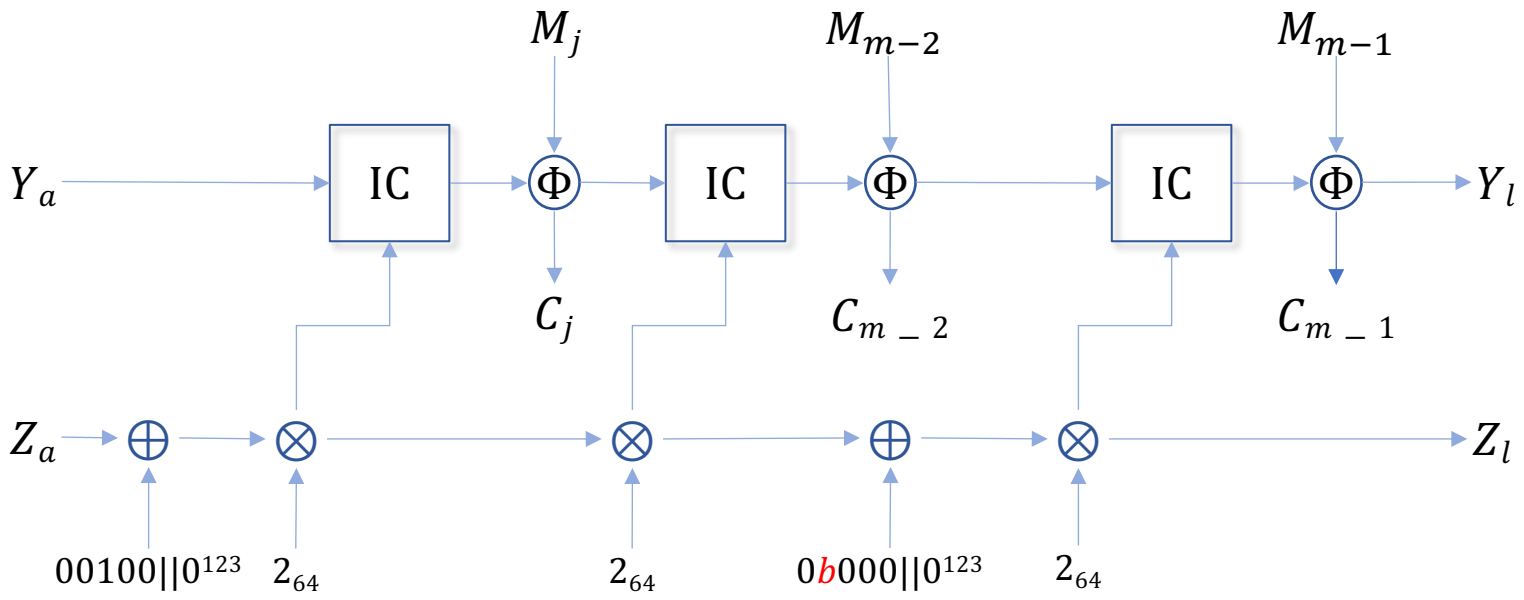


$0 \leq i \leq a-3$

2_{64} is primitive element of $\mathrm{GF}(2^{64})$

COMET: a quick overview

Plaintext Processing:

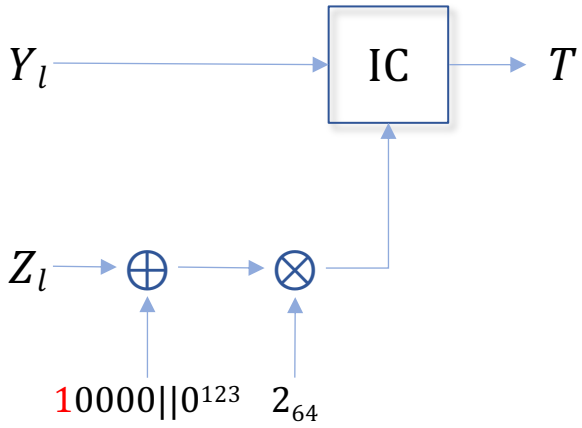


$$0 \leq j \leq m-3$$

$$l = a + m$$

COMET: a quick overview

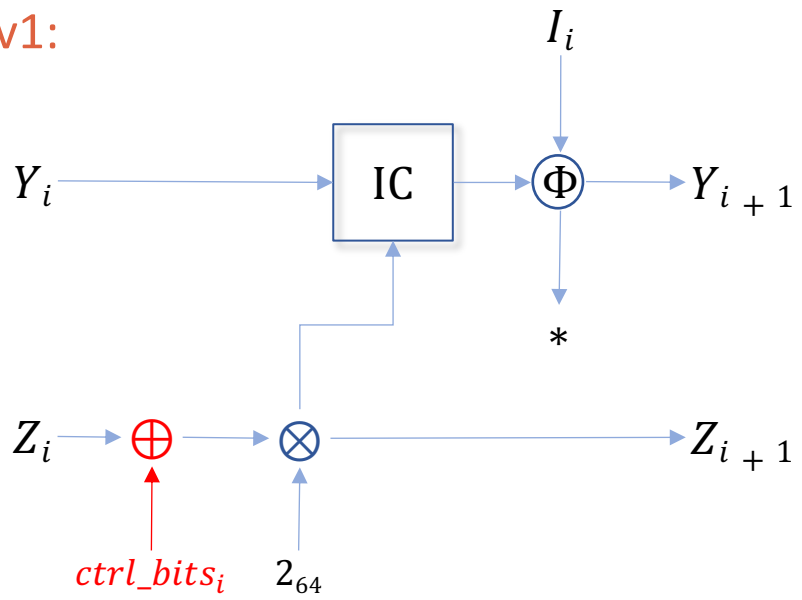
Tag Generation:



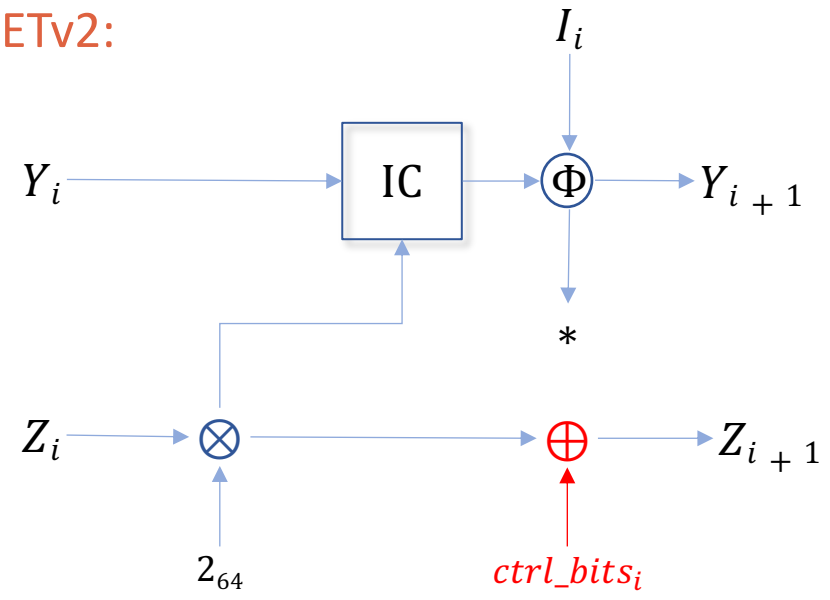
COMETv2: two updates

Change in control bits absorption:

COMETv1:



COMETv2:



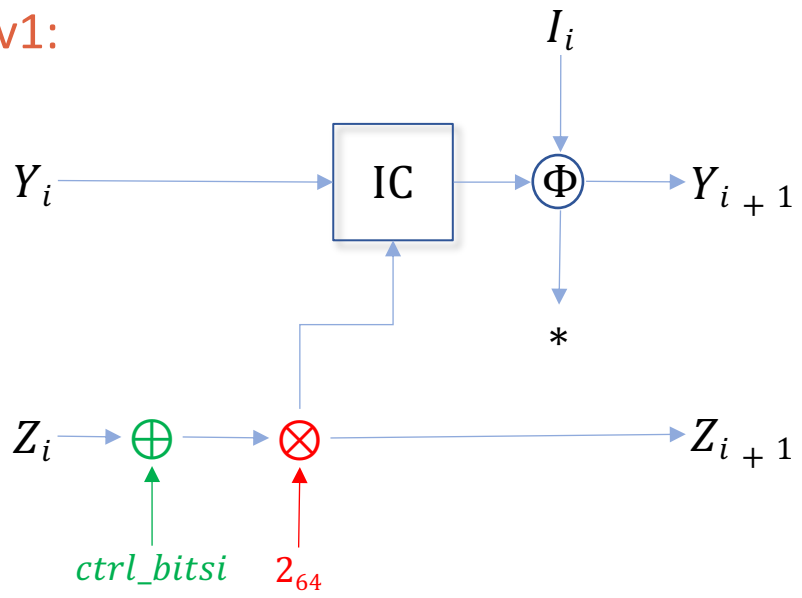
- $ctrl\_bits_i$ depends on the next input block I_i
- Requires n-bit additional memory in hardware.

- Shift the control bits absorption.
- Saves the n-bit additional memory.

COMETv2: two updates

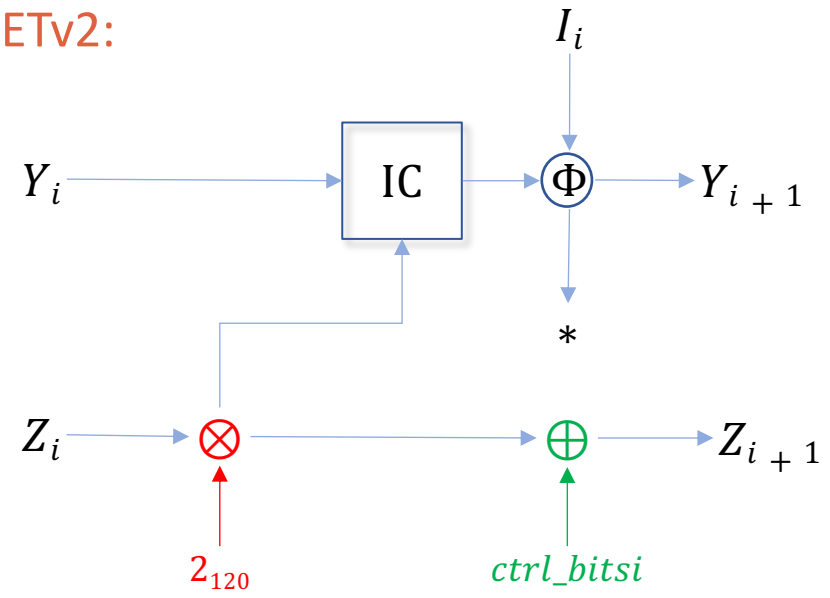
Change in primitive multiplication:

COMETv1:



- Only 64-LSBs of key is updated.
- Leads to key collisions if the 64-LSBs are fixed to 0^{64} .

COMETv2:



$$f(x) = x^{120} + x^9 + x^6 + x^2 + 1$$

- 120-LSBs of key is updated.
- Avoids earlier key-recovery attack strategies.

gCOMET: a generalization of COMET

- Control bit generator (Δ)

$$\Delta(A, M) := (ctrl_0, \ldots, ctrl_{a+m+2}), \qquad \text{where } |ctrl_i| = c.$$

- Feedback matrix (ϕ)

(similar to Beetle feedback)

$$\begin{pmatrix} Y \\ C \end{pmatrix} := \begin{pmatrix} \phi & I_n \\ I_n & I_n \end{pmatrix} . \begin{pmatrix} X \\ M \end{pmatrix}$$

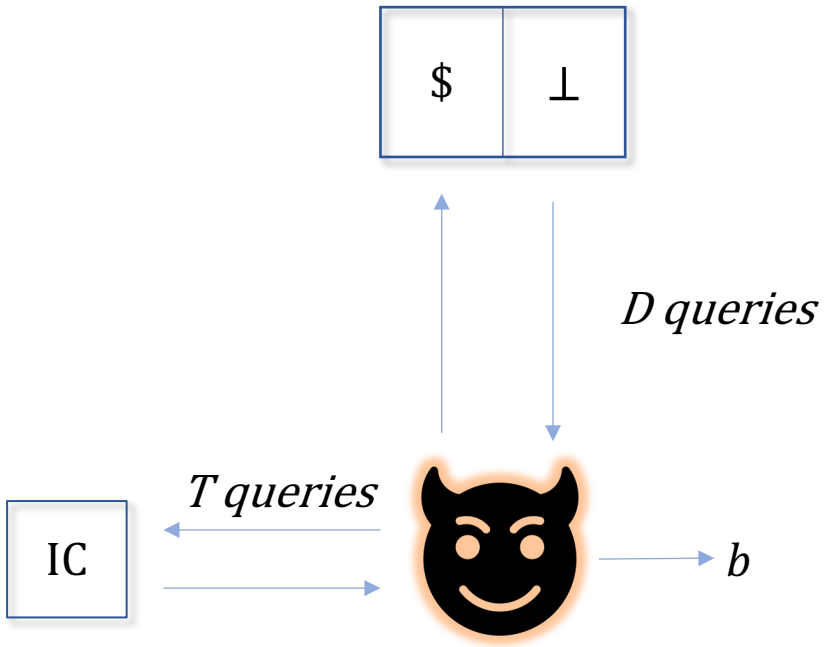
- Key-update matrix (α)

$$K_{i+1} := \begin{pmatrix} I_c & 0_{c \times (\kappa - c)} \\ 0_{(\kappa - c) \times c} & \alpha \end{pmatrix} . K_i$$

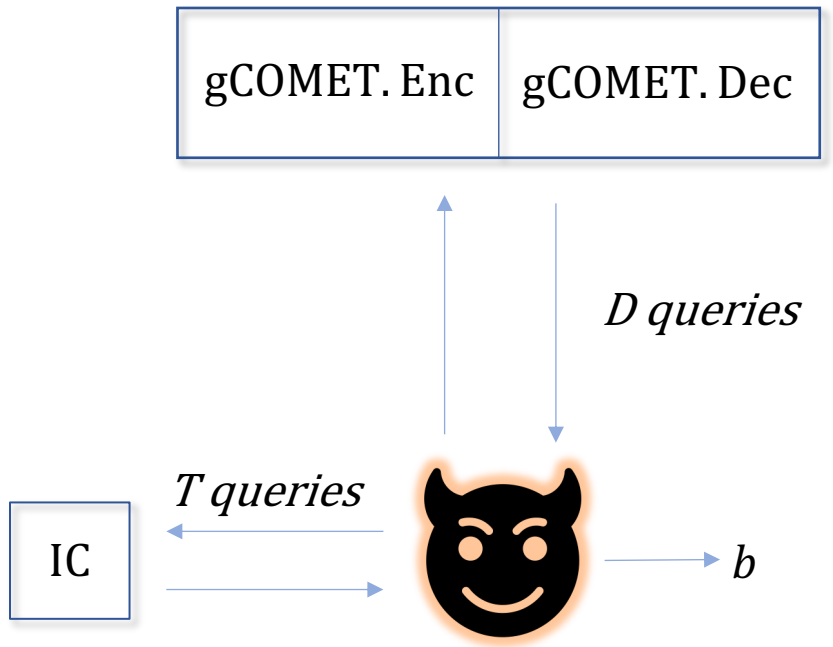
AEAD Security of gCOMET

AEAD Security Notion:

Ideal world (0):



Real world (1):



$$\mathbf{Adv}^{\text{aead}}(😈) := \left|\Pr(b = 1 \text{ in the ideal world}) - \Pr(b = 1 \text{ in the real world})\right|$$

AEAD Security of gCOMET

$$\mathbf{Adv}^{\mathsf{aead}}_{\mathsf{gCOMET}}(\mathcal{A}) \leq \left(\frac{2T}{2^{\kappa}} + \frac{6D}{2^{\mathsf{rank}(\alpha)}} + \frac{4D}{2^{\mathsf{rank}(\alpha)+n}}\right)\mu(D,n) + \frac{4D}{2^{\kappa}}\mu(T,n)$$

$$+ \min\left\{\frac{2D^2}{2^{\kappa}}\mu'(T,n,\mathsf{rank}(\phi)), \frac{2D^2}{2^{\mathsf{rank}(\alpha)}} + \frac{2D}{2^{\kappa}}\mu'(T,n,\mathsf{rank}(\phi))\right\}$$

$$+ \frac{18.77nDT}{2^{\kappa+\frac{\mathsf{rank}(\phi)}{2}}} + \frac{D+T}{2^{\kappa}} + \frac{D}{2^{\mathsf{rank}(\alpha)}} + \frac{4D^2}{2^{\mathsf{rank}(\alpha)+n}} + \frac{4DT}{2^{\kappa+n}} + \frac{2D}{2^{n}}.$$

AEAD Security of gCOMET

Some details:

$$(X_1, \ldots, X_q) \xleftarrow{\$} \{0,1\}^n$$

$$\mu(q,n) := \mathbb{E}\left(\max_a |\{i : X_i = a\}|\right) \qquad \mu'(q,n,\mathsf{rank}(\phi)) := \mathbb{E}\left(\max_a |\{i : \phi(X_i) = a\}|\right)$$

$$\mu(q,n) \leq \begin{cases} 3 & q \leq 2^{n/2} \\ \frac{4n}{\log_2 n} & 2^{n/2} < q \leq 2^n \\ 5n\left\lceil \frac{q}{n2^n} \right\rceil & q > 2^n. \end{cases} \qquad \mu'(q,n,\mathsf{rank}(\phi)) \leq \begin{cases} \frac{4n}{\log_2 n} & q \leq 2^{\mathsf{rank}(\phi)} \\ 5n\left\lceil \frac{q}{n2^{\mathsf{rank}(\phi)}} \right\rceil & q > 2^{\mathsf{rank}(\phi)}. \end{cases}$$

AEAD Security of COMETv1

COMETv1-128:

$$\mathbf{Adv}^{\text{aead}}_{\text{COMET-128}}(\mathcal{A}) \leq \frac{D}{2^{63.75}} + \frac{T}{2^{125.19}} + \frac{DT}{2^{184.24}}$$

Secure while $D \leq 2^{64}$ bytes and $T \leq 2^{120}$.

AEAD Security of COMETv1

COMETv1-64:

$$\mathbf{Adv}^{\text{aead}}_{\text{COMET-64}}(\mathcal{A}) \leq \frac{D}{2^{58.98}} + \frac{T}{2^{121.58}} + \frac{DT}{2^{152.24}} + \frac{D^2T}{2^{193.67}}$$

Secure while $D \leq 2^{40}$ bytes and $T \leq 2^{112}$.

AEAD Security of COMETv2

COMETv2-128:

$$\mathbf{Adv}^{\text{aead}}_{\text{COMETv2-128}}(\mathcal{A}) \leq \frac{D}{2^{119.5}} + \frac{T}{2^{125.19}} + \frac{DT}{2^{184.24}}$$

Secure while $D \leq 2^{64}$ bytes and $T \leq 2^{120}$.

AEAD Security of COMETv2

COMETv2-64:

$$\mathbf{Adv}^{\text{aead}}_{\text{COMETv2-64}}(\mathcal{A}) \leq \frac{D}{2^{66}} + \frac{T}{2^{121.58}} + \frac{DT}{2^{152.24}}$$

Secure while $D \leq 2^{40}$ bytes and $T \leq 2^{112}$.

Some Future Directions

1. Better bounds for COMETv2-64

$$O\left(\frac{nDT}{2^{\kappa+\frac{n}{2}}}\right) \quad \xrightarrow{?} \quad O\left(\frac{DT}{2^{\kappa+\frac{n}{2}}}\right)$$

2. Is perfectly random permutation necessary for Sponge-like AEAD?

COMET is a Sponge-like AEAD with a non-idealized permutation!

3. Key-recovery security can be proved $O(2^{120})$.
   - We have identified bad events corresponding to key-recovery.
   - Need to show it more formally.

This research was partly supported by:

1. NSF-BSF Grant 2018640;
2. NSF Grant CNS 1906360;
3. The Israel Science Foundation (grant No. 3380/19);
4. The BIU Center for Research in Applied Cryptography and Cyber Security, and the Center for Cyber Law and Policy at the University of Haifa, both in conjunction with the Israel National Cyber Bureau in the Prime Minister's Office.

Thank you! Questions?