On the Security of COMET Authenticated Encryption Scheme

NIST Lightweight Workshop '19

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

Motivation

Lightweight Authenticated Encryption Design

- Block cipher based.
- Rate-1.
- Small state size (close to $(n + \kappa)$-bit).
- Simple design (simple operations like XOR, shifts and rotations).

COunter Mode Encryption with authentication Tag

Design Summary

- Rate-1 and Feedback-based authenticated encryption mode.
- Combined feedback function:

  input is a function of current output and next plaintext block.

- Nonce and block counter-based rekeying.
- Parametrized by the block size, $n \in \{64, 128\}$. Tag size $t = n$.
- Two variants:
  - COMET-128: Here $n = 128$, key size $\kappa = 128$, nonce size $r = 128$.
  - COMET-64: Here $n = 64$, key size $\kappa = 128$, nonce size $r = 120$.

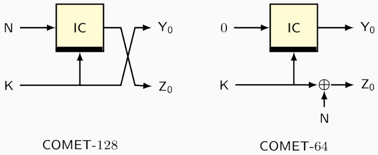
Nonce-based Initial State Derivation

- For COMET-128:

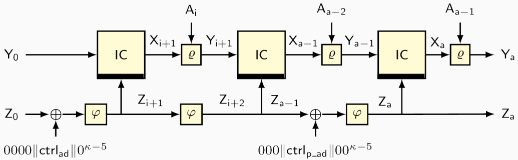
$$(Y_0, Z_0) := (K, IC_K(N))$$

- For COMET-64:

$$(Y_0, Z_0) := (IC_K(0), K \oplus N \| 0^{32})$$



Associated Data Processing



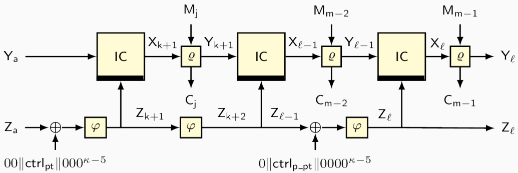
Here,

$$0 \le i \le a - 3$$

$$\mathsf{ctrl}_{\mathsf{ad}} = \begin{cases} 1 & \text{if } |A| > 0, \\ 0 & \text{o.w.} \end{cases}$$

$$\mathsf{ctrl}_{\mathsf{p\_ad}} = \begin{cases} 1 & \text{if } |A_{a-1}| < n, \\ 0 & \text{o.w.} \end{cases}$$

Plaintext Processing



Here,

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

$k = a + j$, and

$\ell = a + m$

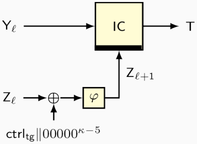
$$\mathsf{ctrl_{pt}} = \begin{cases} 1 & \text{if } |M| > 0, \\ 0 & \text{o.w.} \end{cases}$$

$$\mathsf{ctrl_{p\_pt}} = \begin{cases} 1 & \text{if } |M_{m-1}| < n, \\ 0 & \text{o.w.} \end{cases}$$

Ciphertext processing is symmetrically defined.

COMET : High-level Overview

Tag Generation



Here,

$$\ell = a + m$$

$$\mathsf{ctrl}_{\mathsf{tg}} = \begin{cases} 1 & \text{for tag generation,} \\ 0 & \text{o.w.} \end{cases}$$

Design Features

- Design simplicity: Only requires shift and XOR operations apart from block cipher calls.
- Small state size: Possibility of close to $(n + \kappa)$-bit state size in area optimized implementation.
- Inverse free: No need for block cipher decryption.
- Dynamic key updation: No two blocks share the same key non-trivially.
- Efficiency: Single-pass scheme.

COMET : Recommendations

Submissions to NIST LwC Standardization Project

- COMET-128_AES-128/128 instantiated with AES-128/128. [Primary]
- COMET-128_CHAM-128/128 instantiated with CHAM-128/128.
- COMET-64_Speck-64/128 instantiated with Speck-64/128.
- COMET-64_CHAM-64/128 instantiated with CHAM-64/128.

COMET : Security Claims

Submissions	Confidentiality		Integrity	
	Time	Data (in bytes)	Time	Data (in bytes)
COMET-128_AES-128/128	2^{119}	2^{64}	2^{119}	2^{64}
COMET-128_CHAM-128/128	2^{119}	2^{64}	2^{119}	2^{64}
COMET-64_Speck-64/128	2^{119}	2^{64}	2^{112}	2^{45}
COMET-64_CHAM-64/128	2^{119}	2^{64}	2^{112}	2^{45}

We focus on the security of COMET-128 .

COMET-128 : Security Model

AEAD Security Game

- Indistinguishability game between the ideal system $\mathcal{O}_0$ and real system $\mathcal{O}_1$, where

$$\mathcal{O}_0 := (\$, \perp, \mathsf{IC}^{\pm}) \quad \mathcal{O}_1 := (\text{COMET-128}.\mathsf{E}_\mathsf{K}, \text{COMET-128}.\mathsf{E}_\mathsf{K}, \mathsf{IC}^{\pm}).$$

- Advantage of any adversary $\mathscr{A}$ against COMET-128 is defined as:

$$\mathbf{Adv}^{\text{aead}}_{\text{COMET-128}}(\mathscr{A}) := \left| \Pr\left[\mathscr{A}^{\mathcal{O}_1} = 1\right] - \Pr\left[\mathscr{A}^{\mathcal{O}_0} = 1\right] \right|.$$

- $\mathscr{A}$ is computationally unbounded, but bounded in number of queries to its oracle.
- $\mathscr{A}$ operates under two restrictions:
  - Nonce-respecting: No two encryption query share the same nonce.
  - Non-trivial forger: An encryption query (N, A, M) yields (C, T), a decryption query (N, A, C, T) is not allowed.

COMET-128 : Security Result

Theorem

For $\sigma_e, \sigma_d < 2^{127}$, $q_p < 2^{127}$, and $(q_e, q_d, \sigma_e, \sigma_d, q_p)$-adversary $\mathscr{A}$ we have

$$\mathbf{Adv}^{\mathrm{aead}}_{\mathrm{COMET\text{-}128}}(\mathscr{A}) \leq \frac{4\sigma_c^2}{2^{256}} + \frac{14\sigma_c q_p}{2^{249}} + \frac{3\sigma_c^2}{2^{128}} + \frac{3.01 q_p}{2^{121}} + \frac{4\sigma_c}{2^{128}} + \frac{q_c}{2^{64}} + \frac{6 q_p \sigma_d}{2^{188.5}}$$

- q_e and q_d denote the number of queries to COMET-128.E_K and COMET-128.D_K, respectively.
- σ_e and σ_d denote the sum of input (associated data and message) lengths across all encryption and decryption queries, respectively;

  $q_c = q_e + q_d$ and $\sigma_c = \sigma_e + \sigma_d$.
- q_p denotes the number of direct queries to the block cipher.

Proof tool: Coefficient-H Technique

- Concentrates on the query-response tuple, called the transcript, generated by $\mathscr{A}$'s interaction with the oracle at hand.
- Let Θ_1: transcript random variable corresponding to $\mathcal{O}_1$.
- Let Θ_0: transcript random variable corresponding to $\mathcal{O}_0$.
- Identify a set of bad transcripts, Ω_{bad}.
- Compute $\Pr\left[\Theta_0 \in \Omega_{\mathsf{bad}}\right] \leq \epsilon_{\mathsf{bad}}$.
- Show that $\dfrac{\Pr\left[\Theta_1 = \omega\right]}{\Pr\left[\Theta_0 = \omega\right]} \geq (1 - \epsilon_{\mathsf{ratio}})$ for all $\omega \notin \Omega_{\mathsf{bad}}$.
- Then, $\mathbf{Adv}^{\mathsf{aead}}_{\mathsf{COMET\text{-}128}}(\mathscr{A}) \leq \epsilon_{\mathsf{bad}} + \epsilon_{\mathsf{ratio}}$.

COMET-128 : Security Proof Sketch

Notational Conventions

- Variables in encryption queries are defined as per the figures.
- Variables in decryption queries are defined analogously, topped with a bar.
- Variables in primitive queries are defined analogously, topped with a hat.

Oracle description

- Real oracle: Faithfully responds to encryption, decryption and primitive queries.
- Ideal oracle:

  For the encryption query: samples $X_1, \ldots, X_\ell, T \leftarrow_\$ \{0,1\}^n$, and sets $(Y_j, C_j) = \varrho(X_{a+j+1}, M_j)$ for all $0 \le j \le m$. Sets $Y_j = X_j \oplus A_j$ for $1 \le j \le a$. Returns (C, T).
  For decryption query: Returns $\perp$ symbol.
  For primitive query: Responds faithfully using $IC^{\pm}$.
- After the query phase, both the oracles release all encryption query internal variables and the secret key.

Identifying bad events

- `Kcoll` (key guessing/recovery):

  B1: $\exists i \in [q_e], j \in [m^i]$, such that $\mathsf{Z}_j^i = \mathsf{K}$.
  B2: $\exists i \in [q_d], j \in [\bar{m}^i]$, such that $\bar{\mathsf{Z}}_j^i = \mathsf{K}$.
  B3: $\exists i \in [q_p]$, such that $\widehat{\mathsf{Z}}^i = \mathsf{K}$.
  B4: $\exists i \in [q_e]$, such that $\mathsf{Z}_0^i = *\|0^{n/2}$.
  B5: $\exists i \in [q_d]$, such that $\bar{\mathsf{Z}}_0^i = *\|0^{n/2}$.
  B6: $\exists (i,j) \in [q_e] \times [m^i], (i',j') \in [q_d] \times [\bar{m}^{i'}]$, such that $\mathsf{N}^i \neq \bar{\mathsf{N}}^{i'}$ and $\mathsf{Z}_j^i = \bar{\mathsf{Z}}_{j'}^{i'}$.

- `EEmatch` (encryption-encryption state matching):

  B7: $\exists (i,j) \in [q_e] \times [m^i], (i',j') \in [q_e] \times [m^{i'}]$, such that $(\mathsf{Z}_j^i, \mathsf{Y}_j^i) = (\mathsf{Z}_{j'}^{i'}, \mathsf{Y}_{j'}^{i'})$.
  B7: $\exists (i,j) \in [q_e] \times [m^i], (i',j') \in [q_e] \times [m^{i'}]$, such that $(\mathsf{Z}_j^i, \mathsf{X}_j^i) = (\mathsf{Z}_{j'}^{i'}, \mathsf{X}_{j'}^{i'})$.

Identifying bad events

- `EPmatch` (encryption-primitive state matching):

  B9: $\exists(i,j) \in [q_e] \times [m^i]$ and $i' \in [q_p]$, such that $(\mathsf{Z}^i_j, \mathsf{Y}^i_j) = (\widehat{\mathsf{Z}}^{i'}, \widehat{\mathsf{Y}}^{i'})$.

  B10: $\exists(i,j) \in [q_e] \times [m^i]$ and $i' \in [q_p]$, such that $(\mathsf{Z}^i_j, \mathsf{X}^i_j) = (\widehat{\mathsf{Z}}^{i'}, \widehat{\mathsf{X}}^{i'})$.

- `EPKcoll` (technical requirement: key exhaustion via primitive query):

  B11: $\exists(i,j) \in [q_e] \times [m^i]$ such that $|\{j \in [q_p] : \widehat{\mathsf{Z}}^j = \mathsf{Z}^i\}| \geq 2^{n-1}$.

COMET-128 : Security Proof Sketch

Identifying bad events

- Chain (valid forgery via primitive (and encryption) queries):
  Let domain$(\omega_p) := \{(\hat{Z}_i, \hat{Y}_i)\}_{i \in [q_p]}$ and range$(\omega_p) := \{(\hat{Z}_i, \hat{X}_i)\}_{i \in [q_p]}$.

$$\delta_i := \begin{cases} \max_{\bar{C}^i_{0\ldots k-1} = C^j_{0\ldots k-1}} (\bar{a}^i + k) & \text{if } \bar{A}^i = A^j \wedge (\bar{A}^i, \bar{C}^i) \neq (A^j, C^j) \\ \max_{\bar{A}^i_{0\ldots k-1} = A^j_{0\ldots k-1}} (k) & \text{otherwise.} \end{cases}$$

$$\delta'_i := \begin{cases} \max_{\bar{X}^i_{\delta_i+1}, \ldots, \bar{X}^i_j \in \text{range}(\omega_p)} (j) & \text{if } \bar{X}^i_{\delta_i+1} \in \text{range}(\omega_p) \\ \delta_i & \text{otherwise.} \end{cases}$$

B12: chain using primitive queries
$\exists i \in [q_d]$ such that $\delta_i \geq 0$, $\delta'_i = \bar{\ell}^i$ and $\bar{X}^i_{\bar{\ell}^i+1} = \bar{T}^i$.

B13: partial chain using primitive queries followed by encryption query
$\exists i \in [q_d], (i', j') \in [q_e] \times [m^{i'}]$ such that $0 \leq \delta_i < \delta'_i < \bar{\ell}^i$ and $(\bar{Z}^i_{\delta'_i}, \bar{Y}^{i'}_{\delta'_i}) = (Z^{i'}_{j'}, Y^{i'}_{j'})$.

Bounding $\Pr[\Theta_0 \in \Omega_{\text{bad}}]$

- $\Pr[\texttt{Kcoll}]$: using the fact that $\mathsf{K} \leftarrow_{\$} \{0,1\}^{\kappa}$

$$\Pr[\texttt{B1}] \leq \frac{\sigma_e}{2^{\kappa}}; \;\; \Pr[\texttt{B2}] \leq \frac{\sigma_d}{2^{\kappa}}; \;\; \Pr[\texttt{B3}] \leq \frac{q_p}{2^{\kappa}}.$$

$$\Pr[\texttt{B4}|\neg\texttt{B3}] \leq \frac{q_e}{2^{n/2}}; \;\; \Pr[\texttt{B5}|\neg\texttt{B3}] \leq \frac{q_d}{2^{n/2}}; \;\; \Pr[\texttt{B6}] \leq \frac{\sigma_e\sigma_d}{2^{\kappa}}.$$

- $\Pr[\texttt{EEmatch}|\neg\texttt{Kcoll}]$: using the fact that $\mathsf{K} \leftarrow_{\$} \{0,1\}^{\kappa}$ and $\mathsf{X}^{i}_{j}, \mathsf{X}^{i'}_{j'} \leftarrow_{\$} \{0,1\}^{n}$.

$$\Pr[\texttt{B7}] \leq \frac{\sigma_e^2}{2^{n+\kappa}}; \;\; \Pr[\texttt{B8}] \leq \frac{\sigma_e^2}{2^{n+\kappa}}.$$

COMET-128 : Security Proof Sketch

Bounding $\Pr[\Theta_0 \in \Omega_{\text{bad}}]$

- $\Pr[\texttt{EPmatch} | \neg\texttt{Kcoll}]$:
  - Primitive query occurs before encryption query:

$$\Pr[\texttt{EPmatch} | \neg\texttt{Kcoll}] \leq 2q_p\sigma_e/2^{n+\kappa}.$$

  - Primitive query after encryption query:
    Let, $\text{mcoll}(x) := \left|\{\mathsf{X}_j^i = x : (i,j) \in [q_e] \times [m^i]\}\right|$ and $\texttt{Mcoll}$ denote the event $\max_x \text{mcoll}(x) \geq n$. Then,

$$\begin{aligned}\Pr[\texttt{EPmatch} | \neg\texttt{Kcoll}] &\leq \Pr[\texttt{Mcoll}] + \Pr[\texttt{EPmatch} | \neg(\texttt{Kcoll} \vee \texttt{Mcoll})] \\ &\leq \frac{\sigma_e}{2^{n-1}} + \frac{2nq_p}{2^\kappa}.\end{aligned}$$

- $\Pr[\texttt{EPKcoll}]$: using the fact that the number of keys which are repeated in primitive queries at least 2^{n-1} times is at most $q_p/2^{n-1}$.

$$\Pr[\texttt{EPKcoll}] \leq \frac{2\sigma_e q_p}{2^{n+\kappa}}.$$

COMET-128 : Security Proof Sketch

Bounding $\Pr[\Theta_0 \in \Omega_{\text{bad}}]$

- $\Pr[\texttt{Chain} | \neg(\texttt{Kcoll} \vee \texttt{EEmatch} \vee \texttt{EPmatch})]$:

  Using graph-based analysis (similar to Beetle).
  Let $\mathcal{G}_{\omega_p} = (\mathcal{V}, \mathcal{E})$ be an edge-labeled graph where $\mathcal{V} = \text{domain}(\omega_p)$ and $((\hat{Z}_j, \hat{Y}_i), (\hat{Z}_j, \hat{Y}_j), C^*) \in \mathcal{E}$ if and only if

  $$(\hat{Z}_j, \hat{Y}_j) = (\mathsf{IC}_{\hat{Z}_i}(\hat{Y}_i), \mathsf{IC}_{\hat{Z}_i}(\hat{Y}_i) \oplus C^*)$$

  A walk $\mathcal{W}$ from vertex W_0 to W_k with label $C = (C_1, \ldots, C_k)$, denoted $W_0 \xrightarrow{C} W_k$, is

  $$W_0 \xrightarrow{C_1} W_1 \cdots W_{k-1} \xrightarrow{C_k} W_k.$$

COMET-128 : Security Proof Sketch

Bounding $\Pr[\Theta_0 \in \Omega_{\text{bad}}]$

- $\Pr[\texttt{Chain} | \neg(\texttt{Kcoll} \vee \texttt{EEmatch} \vee \texttt{EPmatch})]$:

  A multi-chain with label $\mathsf{C} = (\mathsf{C}_1, \ldots, \mathsf{C}_k)$, denoted $\mathcal{C}_{\mathsf{C}}$, is a set of labeled walks $\{\mathcal{W}_1, \ldots, \mathcal{W}_s\}$ such that for all $1 \leq i \leq s$,

$$\mathcal{W}_i : (\hat{\mathsf{Z}}^i_0, \hat{\mathsf{Y}}^i_0) \xrightarrow{\mathsf{C}} (\hat{\mathsf{Z}}^i_k, \hat{\mathsf{Y}}^i_k) \ \wedge \ \hat{\mathsf{Y}}^1_0 = \cdots = \hat{\mathsf{Y}}^s_0 \ \wedge \ \hat{\mathsf{X}}^1_{k+1} = \cdots = \hat{\mathsf{X}}^s_{k+1}.$$

$$\begin{array}{ll}
\mathcal{W}_1 : & (\hat{\mathsf{Z}}^1_0, \hat{\mathsf{Y}}^1_0) \xrightarrow{\mathsf{C}_1} (\hat{\mathsf{Z}}^1_1, \hat{\mathsf{Y}}^1_1) \xrightarrow{\mathsf{C}_2} (\hat{\mathsf{Z}}^1_2, \hat{\mathsf{Y}}^1_2) \xrightarrow{\mathsf{C}_3} (\hat{\mathsf{Z}}^1_3, \hat{\mathsf{Y}}^1_3) \xrightarrow{\mathsf{C}_4} (\hat{\mathsf{Z}}^1_3, \hat{\mathsf{Y}}^1_4) \overset{\mathsf{IC}}{\dashrightarrow} \hat{\mathsf{X}}^1_5 \\
\mathcal{W}_2 : & (\hat{\mathsf{Z}}^2_0, \hat{\mathsf{Y}}^2_0) \xrightarrow{\mathsf{C}_1} (\hat{\mathsf{Z}}^2_1, \hat{\mathsf{Y}}^2_1) \xrightarrow{\mathsf{C}_2} (\hat{\mathsf{Z}}^2_2, \hat{\mathsf{Y}}^2_2) \xrightarrow{\mathsf{C}_3} (\hat{\mathsf{Z}}^2_3, \hat{\mathsf{Y}}^2_3) \xrightarrow{\mathsf{C}_4} (\hat{\mathsf{Z}}^2_3, \hat{\mathsf{Y}}^2_4) \overset{\mathsf{IC}}{\dashrightarrow} \hat{\mathsf{X}}^2_5 \\
\vdots & \\
\mathcal{W}_s : & (\hat{\mathsf{Z}}^s_0, \hat{\mathsf{Y}}^s_0) \xrightarrow{\mathsf{C}_1} (\hat{\mathsf{Z}}^s_1, \hat{\mathsf{Y}}^s_1) \xrightarrow{\mathsf{C}_2} (\hat{\mathsf{Z}}^s_2, \hat{\mathsf{Y}}^s_2) \xrightarrow{\mathsf{C}_3} (\hat{\mathsf{Z}}^s_3, \hat{\mathsf{Y}}^s_3) \xrightarrow{\mathsf{C}_4} (\hat{\mathsf{Z}}^s_3, \hat{\mathsf{Y}}^s_4) \overset{\mathsf{IC}}{\dashrightarrow} \hat{\mathsf{X}}^s_5
\end{array}$$

$$\boxed{\Pr[\texttt{B11} | \neg(\texttt{Kcoll} \vee \texttt{EEmatch} \vee \texttt{EPmatch})] \leq \sum_{i \in [q]_d} \Pr\left[\left|\mathcal{C}_{\bar{\mathsf{C}}_{\delta_i \ldots \bar{m}^i}}\right| \geq \lambda_i\right] + \frac{\lambda_i}{2^\kappa}.}$$

COMET-128 : Security Proof Sketch

Bound on $\Pr\left[|\mathcal{C}_{\bar{\mathsf{C}}_{\delta_i\ldots\bar{m}^i}}| \geq \lambda_i\right]$ and λ_i

- Three ways to construct a multi-chain structure:
  - Forward-only: all queries of the form $(\hat{\mathsf{Z}}_i, \hat{\mathsf{Y}}_i)$.

$$\Pr\left[\mathcal{C}_{\mathrm{fwd}} \geq n\left\lceil\frac{q_p}{2^n}\right\rceil\right] \leq \frac{1}{2^n},$$

    (by bounding the multicollisions on $\hat{\mathsf{X}}_j$)
  - Backward-only: all queries of the form $(\hat{\mathsf{Z}}_i, \hat{\mathsf{X}}_i)$.

$$\Pr\left[\mathcal{C}_{\mathrm{bck}} \geq n\left\lceil\frac{q_p}{2^n}\right\rceil\right] \leq \frac{1}{2^n}.$$

    (by bounding the multicollisions on $\hat{\mathsf{Y}}_j$)
  - Both forward and backward type queries:
    reduced to multicollision event at some index $1 \leq i \leq \bar{\ell}^i$ (using Pigeonhole-principle).

$$\Pr\left[\mathcal{C}_{\mathrm{fwd\text{-}bck}} \geq \bar{\ell}^i\,\frac{2\sqrt{n}q_p}{2^{n/2}} + \frac{2q_p}{2^n}\right] \leq \frac{1}{2^n}.$$

- $\Pr\left[|\mathcal{C}_{\bar{\mathsf{C}}_{\delta_i\ldots\bar{m}^i}}| \geq \bar{\ell}^i\,\frac{2\sqrt{n}q_p}{2^{n/2}} + 2n\left\lceil\frac{q_p}{2^n}\right\rceil + \frac{2q_p}{2^n}\right] \leq \frac{3}{2^n}.$

COMET-128 : Security Proof Sketch

- $\Pr\left[\mathtt{B11}|\neg(\mathtt{Kcoll} \vee \mathtt{EEmatch} \vee \mathtt{EPmatch})\right] \leq \frac{2\sqrt{n}\sigma_d q_p}{2^{\kappa+n/2}} + \frac{2nq_d}{2^\kappa}\left\lceil\frac{q_p}{2^n}\right\rceil + \frac{2q_d q_p}{2^{n+\kappa}} + \frac{3q_d}{2^n}$.
- $\Pr\left[\mathtt{B12}|\neg(\mathtt{Kcoll} \vee \mathtt{EEmatch} \vee \mathtt{EPmatch})\right]$ can be bounded in a similar fashion.

$$\Pr\left[\mathtt{B12}|\neg(\mathtt{Kcoll} \vee \mathtt{EEmatch} \vee \mathtt{EPmatch} \vee \mathtt{B11})\right] \leq \frac{2\sqrt{n}\sigma_d q_p}{2^{\kappa+n/2}} + \frac{2nq_d}{2^\kappa}\left\lceil\frac{q_p}{2^n}\right\rceil + \frac{2q_d q_p}{2^{n+\kappa}} + \frac{3q_d}{2^n}.$$

Finally, $\Pr\left[\mathtt{Chain}|\neg(\mathtt{Kcoll} \vee \mathtt{EEmatch} \vee \mathtt{EPmatch})\right] \leq \frac{6\sqrt{n}\sigma_d q_p}{2^{\kappa+n/2}} + \frac{6nq_d}{2^\kappa}\left\lceil\frac{q_p}{2^n}\right\rceil + \frac{4q_d q_p}{2^{n+\kappa}} + \frac{6q_d}{2^n}$.

COMET-128 : Security Proof Sketch

Good transcript analysis

Given any good transcript ω:

$$\frac{\Pr[\Theta_1 = \omega]}{\Pr[\Theta_0 = \omega]} \geq \left(1 - \frac{2\sigma_d(\sigma_e + q_p)}{2^{\kappa+n}} - \frac{2q_d}{2^n}\right).$$

- First term bounds the probability that for some decryption query i an intermediate input $(\hat{Z}^i_j, \hat{Y}^i_j)$ collides with some encryption/primitive input, for $j > \delta_i$.
- The second term bounds the probability that som decryption forgery succeeds given that all intermediate inputs are fresh.

This completes the proof.

Thank you. Questions...

Acknowledgments

This work is supported in part by The Ministry of Science and Technology, Israel, and the Department of Science and Technology, Government of India, DST/INT/ISR/P-20/2017.

Shay Gueron is supported by

The Israel Science Foundation (grant No. 1018/16);
NSF-BSF Grant 2018640;
The BIU Center for Research in Applied Cryptography and Cyber Security, in conjunction with the Israel National Cyber Bureau in the Prime Minister's Office;
The Center for Cyber Law & Policy at the University of Haifa in conjunction with the Israel National Cyber Directorate in the Prime Minister's Office.

The authors would like to thank Mustafa Khairallah for sharing his observations on bad conditions `B4` and `B5`.