Understanding RUP Integrity of COLM

Nilanjan Datta, Atul Luykx, Bart Mennink and Mridul Nandi

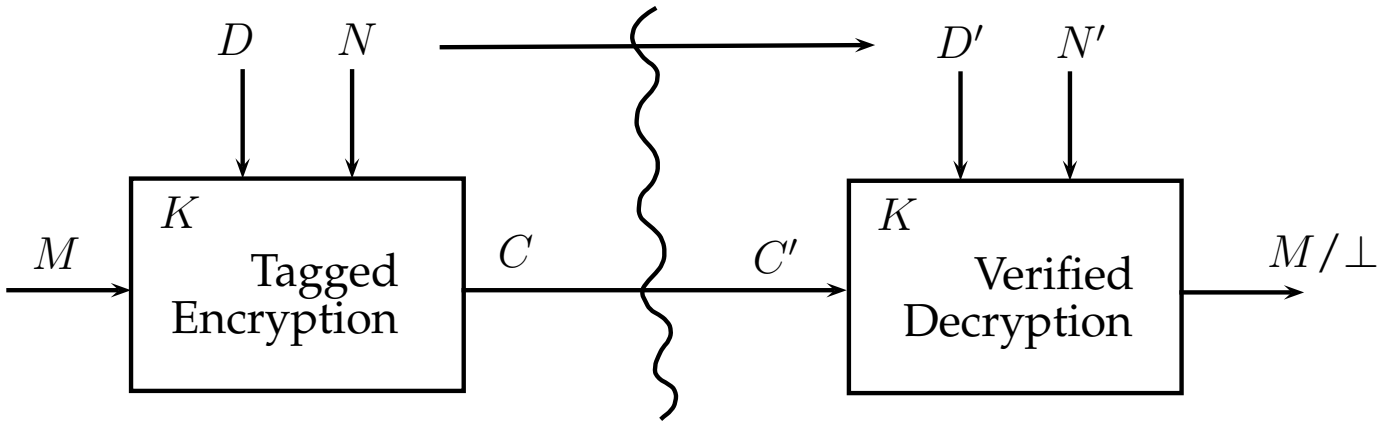
Fast Software Encryption 2018, Bruges, Belgium

05 March, 2018

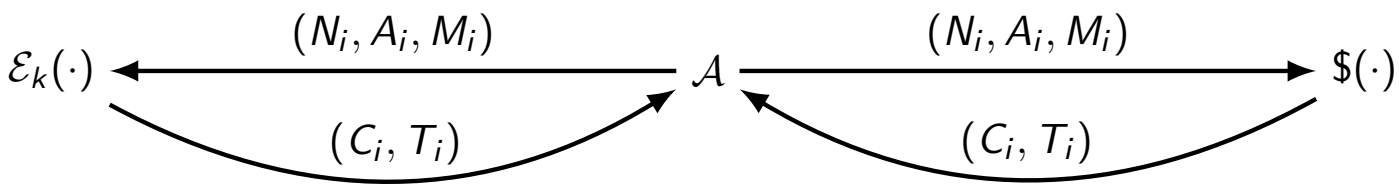
Authenticated Encryption

Definition

1. Tagged Encryption: $\mathcal{M} \times \mathcal{D} \times \mathcal{N} \times \mathcal{K} \rightarrow \mathcal{C}$
2. Verified Decryption: $\mathcal{C} \times \mathcal{D} \times \mathcal{N} \times \mathcal{K} \rightarrow \mathcal{M} \cup \perp$

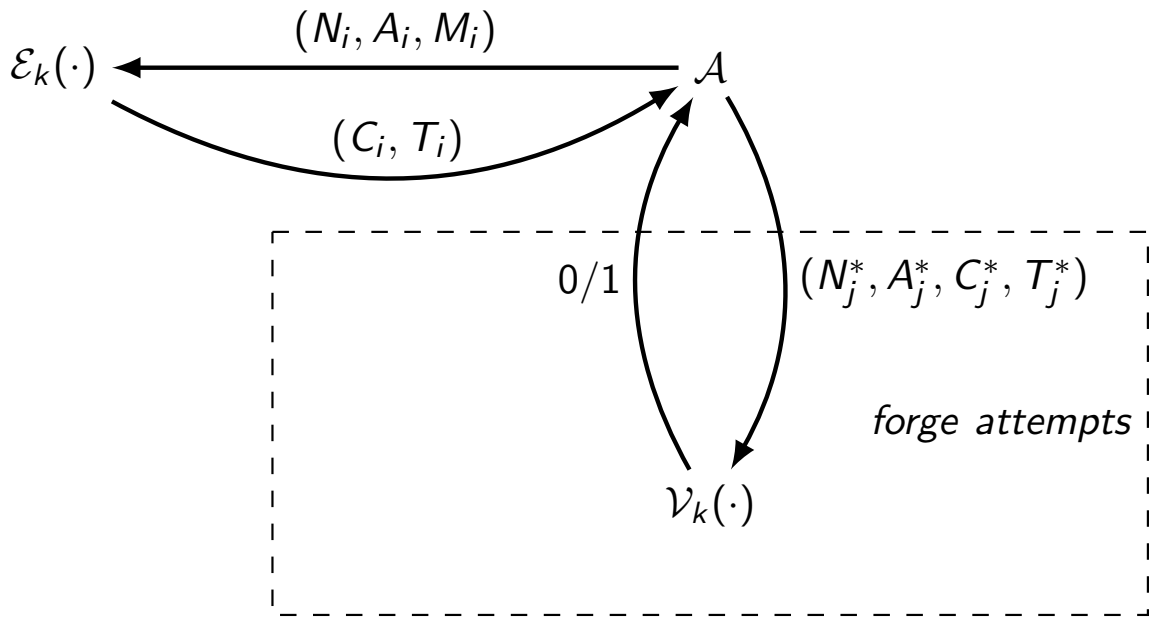


PRF Security for Privacy



- $\mathbf{Adv}^{\mathrm{priv}}_{\mathcal{AE}}(\mathcal{A}) := |\Pr[\mathcal{A}^{\mathcal{E}_k} = 1] - \Pr[\mathcal{A}^{\$} = 1]|$

INT-CTXT Security for Integrity

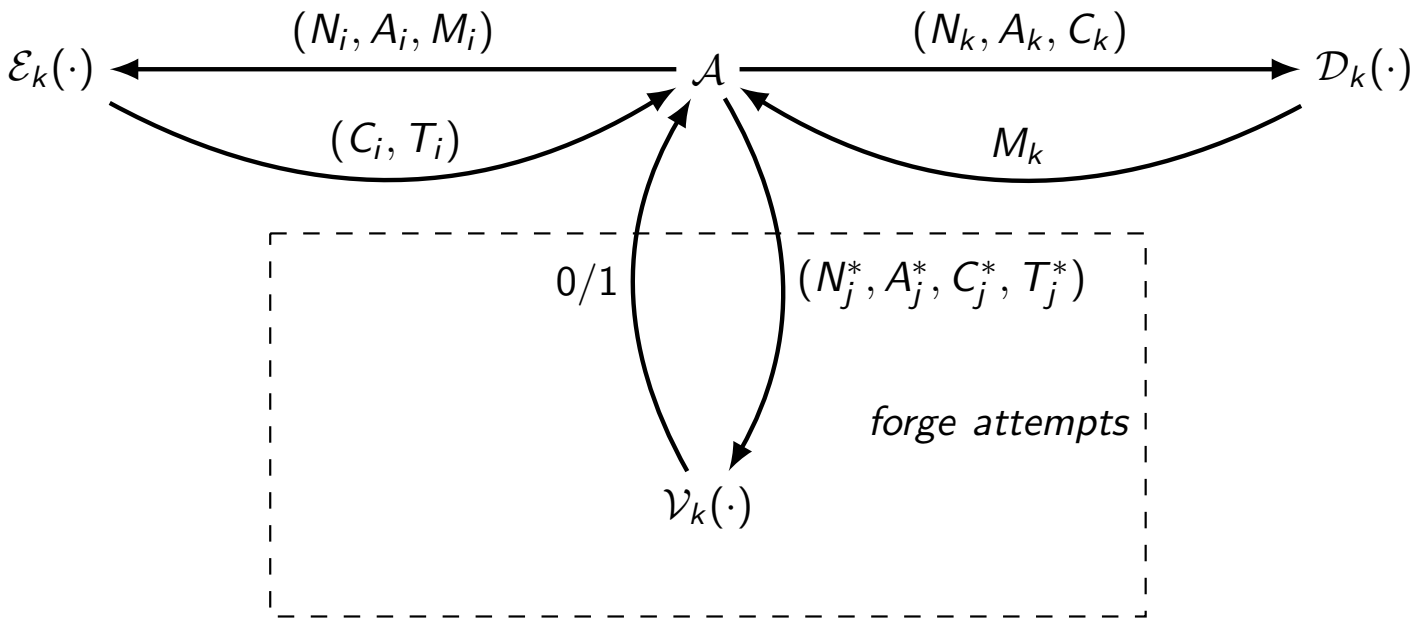


- $\mathbf{Adv}^{\text{int\_ctxt}}_{\mathcal{AE}}(\mathcal{A}) := Pr[\mathcal{A}^{\mathcal{E}_k, \mathcal{V}_k} \text{ forges}]$
- $\mathcal{A}$ forges if $\mathcal{V}_k(N_j^*, A_j^*, C_j^*, T_j^*) = 1$

Issues on AE: Limited Buffer Implementation

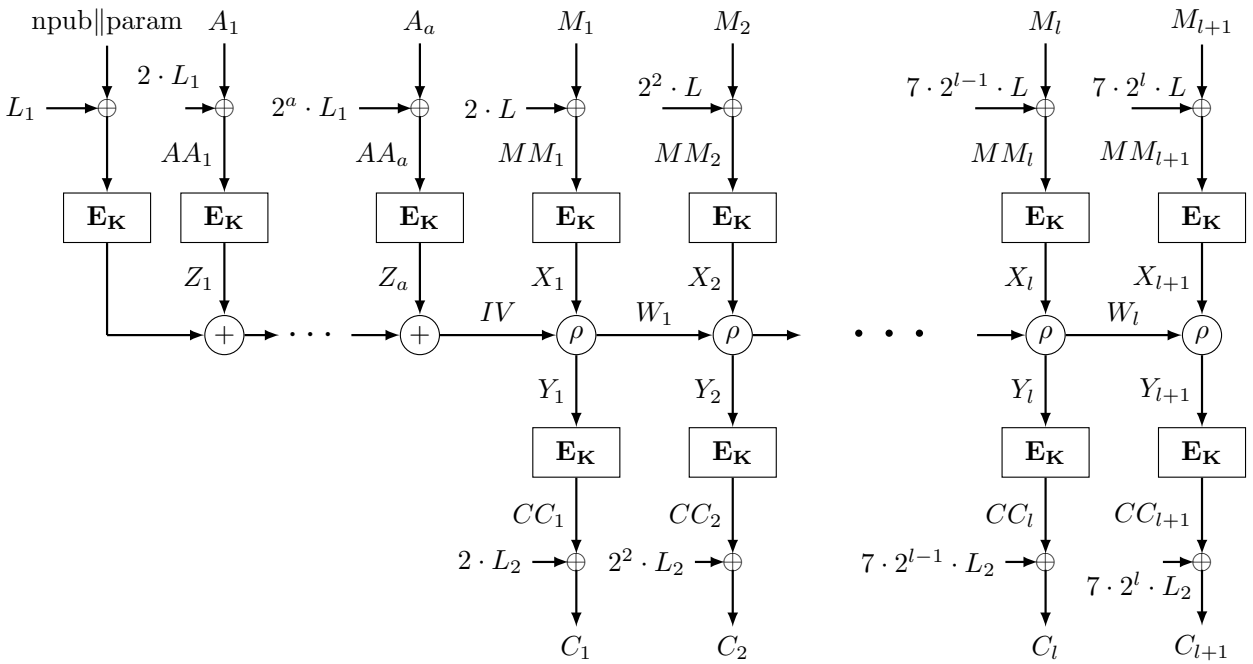
- Small devices may have limited buffer
- Limited buffer $\Longrightarrow$ Release of unverified plaintext
  (If decryption query length is more than buffer size)

INT-RUP Model (Andreeva et al.)

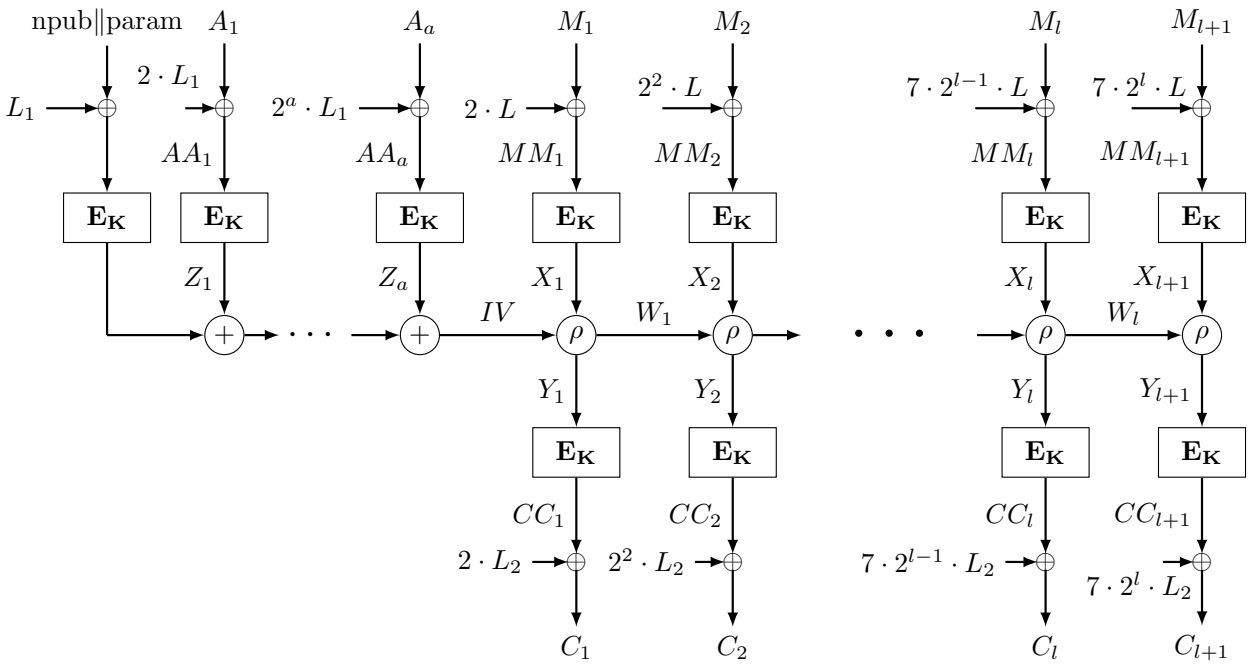


- $\mathbf{Adv}^{\text{int\_rup}}_{\mathcal{AE}}(\mathcal{A}) := Pr[\mathcal{A}^{\mathcal{E}_k, \mathcal{D}_k, \mathcal{V}_k} \text{ forges}]$

COLM Type Structure

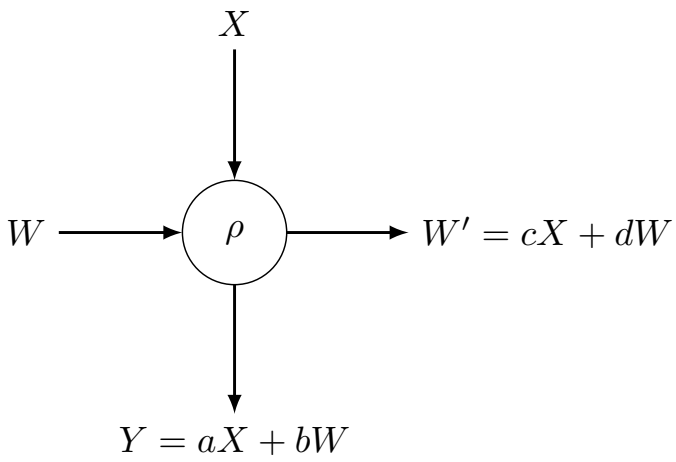


COLM Type Structure

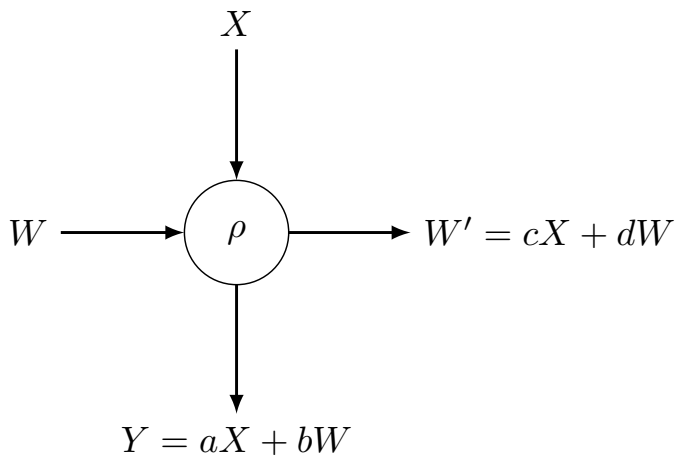


- Enc (Dec) then Mixing then Enc (Dec) type structure
- Linear Mix ρ is used

General ρ Function



General ρ Function



- COPA: $a = b = c = d = 1$.
- ELmD: $a = c = 1$, $b = 3$, $d = 2$.

Revisiting INT-RUP Attack on COPA

Mounting INT-RUP Attack on COPA

First Step: Find Non-trivial State Collision

- Decryption: W_i depends entirely on C_i.

Mounting INT-RUP Attack on COPA

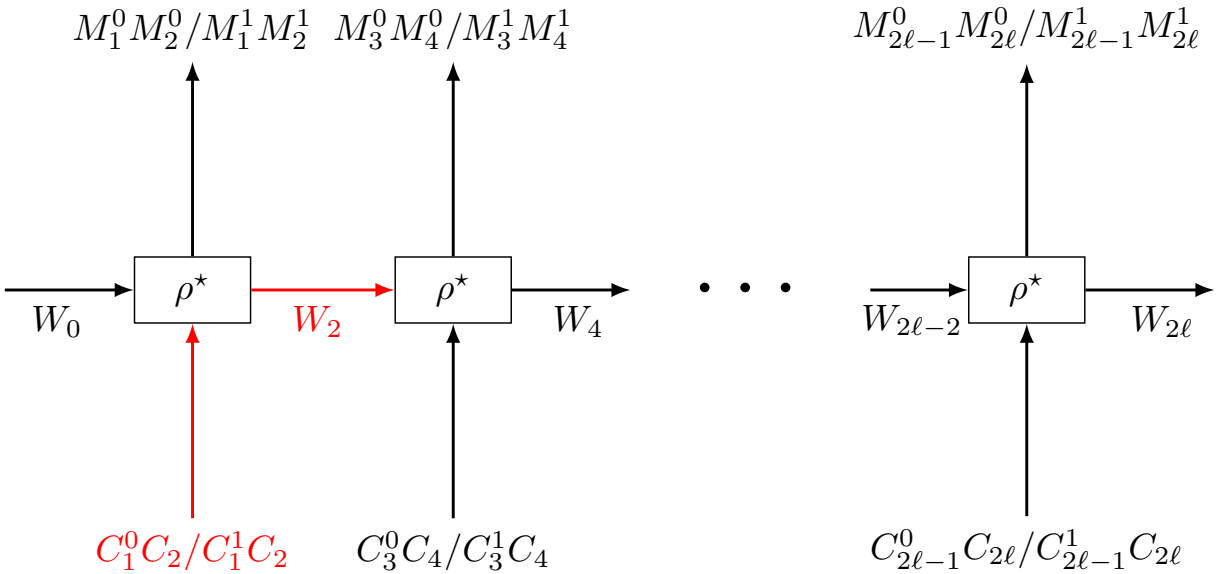
First Step: Find Non-trivial State Collision

- Decryption: W_i depends entirely on C_i.
- (C_1^0, C_2) and (C_1^1, C_2) ensure state collision in W_2.

Mounting INT-RUP Attack on COPA

First Step: Find Non-trivial State Collision

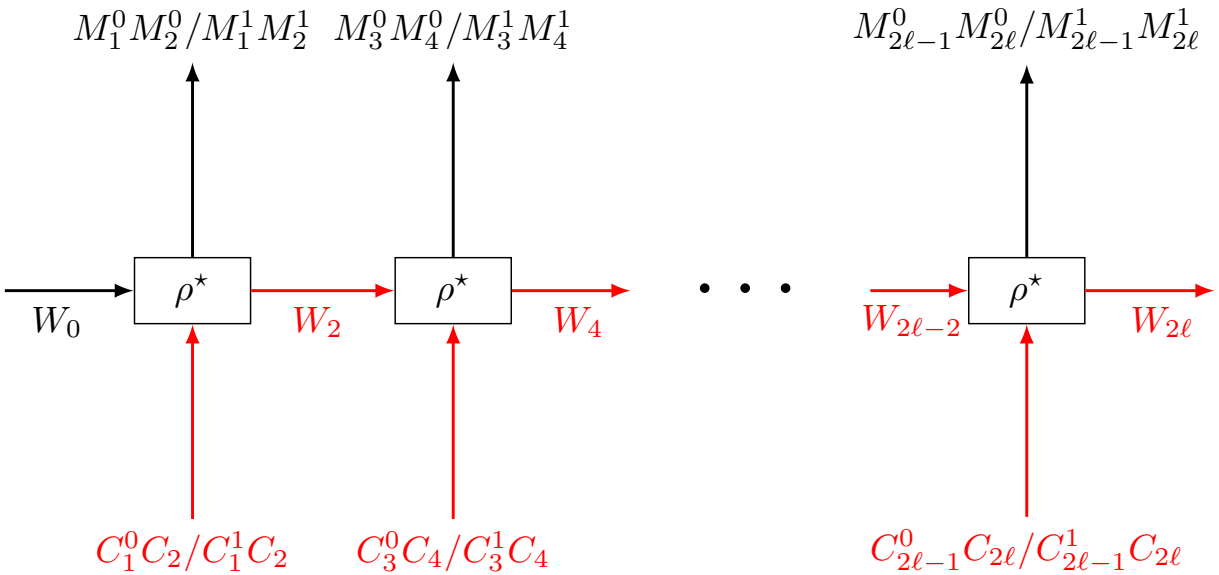
- Decryption: W_i depends entirely on C_i.
- (C_1^0, C_2) and (C_1^1, C_2) ensure state collision in W_2.



Mounting INT-RUP Attack on COPA

Second Step: Strech the State Collision

- (C_3^0, C_4) and (C_3^1, C_4) ensure state collision in $W_4, \cdots$
- $(C_{2\ell-1}^0, C_{2\ell})$ and $(C_{2\ell-1}^1, C_{2\ell})$ ensure state collision in $W_{2\ell}$.



Mounting INT-RUP Attack on COPA

- RUP 1: $(M_1^0 \cdots M_{2\ell}^0) \leftarrow \mathcal{D}(N^*, A^*, C_1^0 C_2 C_3^0 C_4 \cdots C_{2\ell-1}^0 C_{2\ell})$.
- RUP 2: $(M_1^1 \cdots M_{2\ell}^1) \leftarrow \mathcal{D}(N^*, A^*, C_1^1 C_2 C_3^1 C_4 \cdots C_{2\ell-1}^1 C_{2\ell})$.

Mounting INT-RUP Attack on COPA

- RUP 1: $(M_1^0 \cdots M_{2\ell}^0) \leftarrow \mathcal{D}(N^*, A^*, C_1^0 C_2 C_3^0 C_4 \cdots C_{2\ell-1}^0 C_{2\ell})$.
- RUP 2: $(M_1^1 \cdots M_{2\ell}^1) \leftarrow \mathcal{D}(N^*, A^*, C_1^1 C_2 C_3^1 C_4 \cdots C_{2\ell-1}^1 C_{2\ell})$.
- Encryption: $(C_1^0 \cdots C_{2\ell}^0, T) \leftarrow \mathcal{E}(N^*, A^*, M_1^0 \cdots M_{2\ell}^0)$.

Mounting INT-RUP Attack on COPA

- RUP 1: $(M_1^0 \cdots M_{2\ell}^0) \leftarrow \mathcal{D}(N^*, A^*, C_1^0 C_2 C_3^0 C_4 \cdots C_{2\ell-1}^0 C_{2\ell})$.
- RUP 2: $(M_1^1 \cdots M_{2\ell}^1) \leftarrow \mathcal{D}(N^*, A^*, C_1^1 C_2 C_3^1 C_4 \cdots C_{2\ell-1}^1 C_{2\ell})$.
- Encryption: $(C_1^0 \cdots C_{2\ell}^0, T) \leftarrow \mathcal{E}(N^*, A^*, M_1^0 \cdots M_{2\ell}^0)$.

Find $b_1, b_2, \ldots, b_\ell$: (Apply Gaussian Elimination)

$$\oplus_{i=1}^{\ell} M_i^0 = (M_1^{b_1} \oplus M_2^{b_1}) \oplus (M_3^{b_2} \oplus M_4^{b_2}) \oplus \cdots \oplus (M_{2\ell-1}^{b_\ell} \oplus M_{2\ell}^{b_\ell}).$$

Mounting INT-RUP Attack on COPA

- RUP 1: $(M_1^0 \cdots M_{2\ell}^0) \leftarrow \mathcal{D}(N^*, A^*, C_1^0 C_2 C_3^0 C_4 \cdots C_{2\ell-1}^0 C_{2\ell})$.
- RUP 2: $(M_1^1 \cdots M_{2\ell}^1) \leftarrow \mathcal{D}(N^*, A^*, C_1^1 C_2 C_3^1 C_4 \cdots C_{2\ell-1}^1 C_{2\ell})$.
- Encryption: $(C_1^0 \cdots C_{2\ell}^0, T) \leftarrow \mathcal{E}(N^*, A^*, M_1^0 \cdots M_{2\ell}^0)$.

Find $b_1, b_2, \ldots, b_\ell$: (Apply Gaussian Elimination)

$$\oplus_{i=1}^{\ell} M_i^0 = (M_1^{b_1} \oplus M_2^{b_1}) \oplus (M_3^{b_2} \oplus M_4^{b_2}) \oplus \cdots \oplus (M_{2\ell-1}^{b_\ell} \oplus M_{2\ell}^{b_\ell}).$$

- Forge with $(C_1^{b_1} C_2 C_3^{b_2} C_4 \cdots C_{2\ell-1}^{b_\ell} C_{2\ell} T)$.

Nonce Misuse INT-RUP Attack on COLM

Nonce Misuse INT-RUP Attack on COLM

$$C_1 C_2 C_3 \leftarrow \mathcal{E}(N, A, M_1 \star \star)$$

Nonce Misuse INT-RUP Attack on COLM

$$C_1 C_2 C_3 \leftarrow \mathcal{E}(N, A, M_1 \star \star)$$
$$\star M_2' \star \leftarrow \mathcal{D}(N, A, \star C_2 \star)$$

Nonce Misuse INT-RUP Attack on COLM

$$C_1 C_2 C_3 \leftarrow \mathcal{E}(N, A, M_1 \star\star)$$
$$\star M_2' \star \leftarrow \mathcal{D}(N, A, \star C_2 \star)$$
$$\star\star M_3' \leftarrow \mathcal{D}(N, A, \star\star C_3)$$

Nonce Misuse INT-RUP Attack on COLM

$$C_1 C_2 C_3 \leftarrow \mathcal{E}(N, A, M_1 \star \star)$$
$$\star M_2' \star \leftarrow \mathcal{D}(N, A, \star C_2 \star)$$
$$\star \star M_3' \leftarrow \mathcal{D}(N, A, \star \star C_3)$$
$$C_1' C_2' C_3' \leftarrow \mathcal{E}(N, A, \star M_2' M_3')$$

Nonce Misuse INT-RUP Attack on COLM

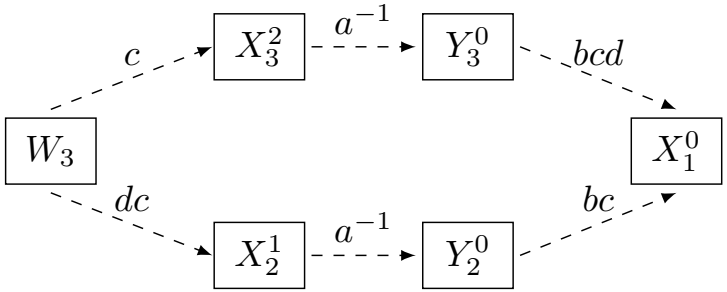
$$C_1 C_2 C_3 \leftarrow \mathcal{E}(N, A, M_1 \star \star)$$
$$\star M_2' \star \leftarrow \mathcal{D}(N, A, \star C_2 \star)$$
$$\star \star M_3' \leftarrow \mathcal{D}(N, A, \star \star C_3)$$
$$C_1' C_2' C_3' \leftarrow \mathcal{E}(N, A, \star M_2' M_3')$$

Main Observation

Last Query's W_3 is independent of M_1.

Nonce Misuse INT-RUP Attack on COLM

$$C_1 C_2 C_3 \leftarrow \mathcal{E}(N, A, M_1 \star \star)$$
$$\star M_2' \star \leftarrow \mathcal{D}(N, A, \star C_2 \star)$$
$$\star \star M_3' \leftarrow \mathcal{D}(N, A, \star \star C_3)$$
$$C_1' C_2' C_3' \leftarrow \mathcal{E}(N, A, \star M_2' M_3')$$



Nonce Misuse INT-RUP Attack on COLM

Main Observation

Last Query's W_3 is independent of M_1.

Nonce Misuse INT-RUP Attack on COLM

Main Observation

Last Query's W_3 is independent of M_1.

Implication

Evaluating this process twice gives different $(M_1^0 M_2^0 M_3^0)$ and $(M_1^1 M_2^1 M_3^1)$ with identical W.

Nonce Misuse INT-RUP Attack on COLM

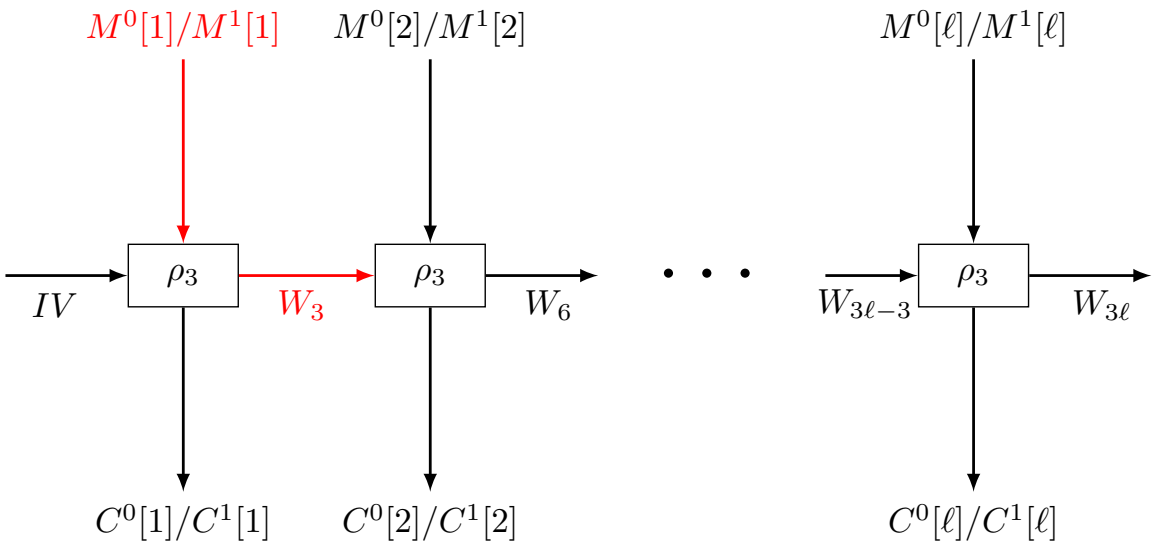
First Step: Find Non-Trivial State Collision

Find $M^0[1] = (M_1^0 M_2^0 M_3^0)$ and $M^1[1] = (M_1^1 M_2^1 M_3^1)$ with identical W_3.

Nonce Misuse INT-RUP Attack on COLM

First Step: Find Non-Trivial State Collision

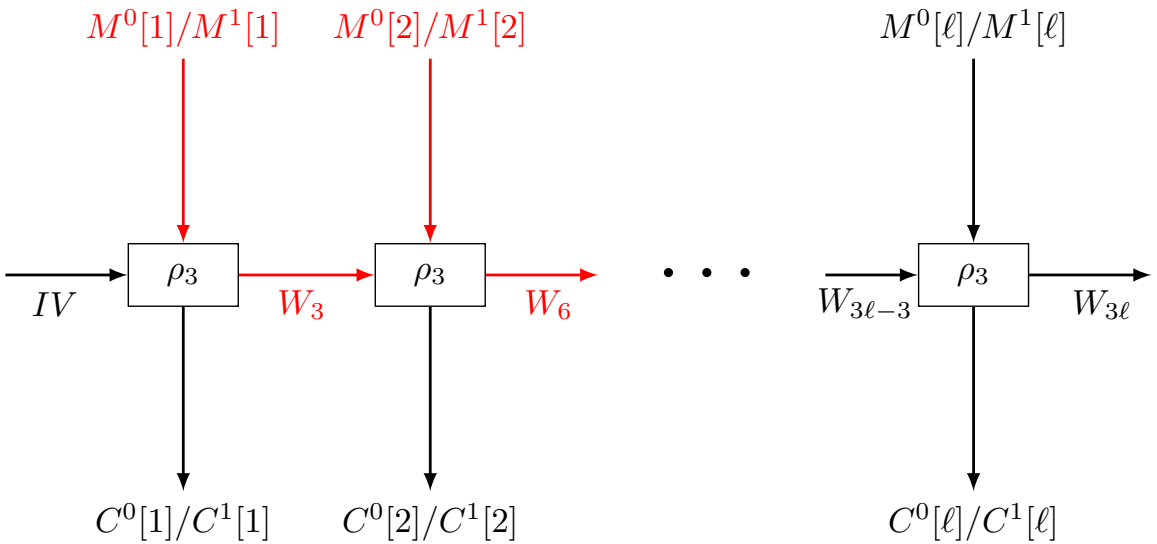
Find $M^0[1] = (M_1^0 M_2^0 M_3^0)$ and $M^1[1] = (M_1^1 M_2^1 M_3^1)$ with identical W_3.



Nonce Misuse INT-RUP Attack on COLM

Second Step: Strech the State Collision

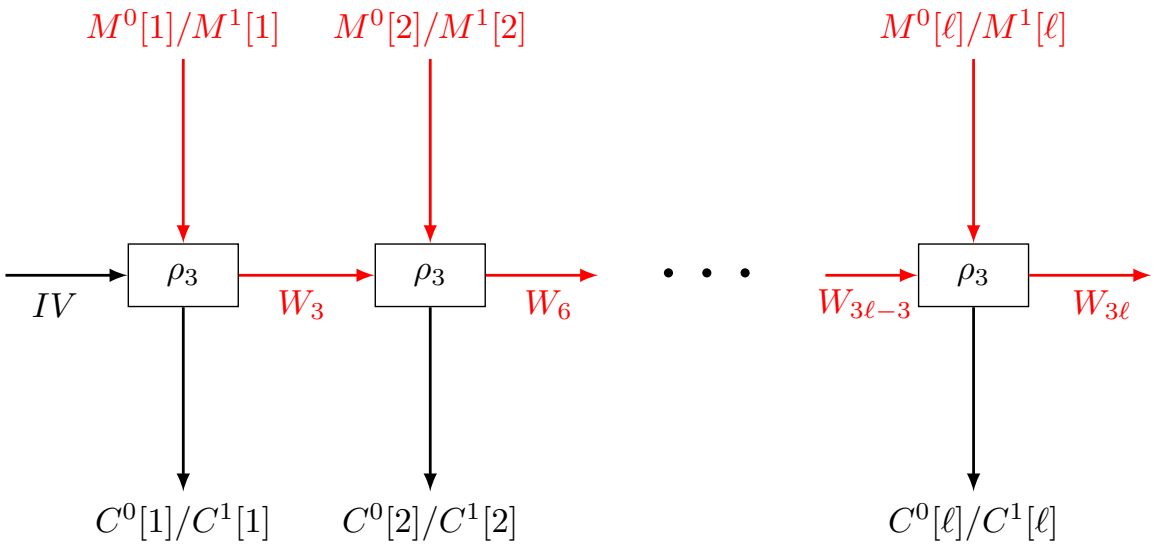
Find $M^0[2] = (M_4^0 M_5^0 M_6^0)$ and $M^1[2] = (M_4^1 M_5^1 M_6^1)$ that ensure state collision in W_6.



Nonce Misuse INT-RUP Attack on COLM

Second Step: Strech the State Collision

Find $M^0[\ell] = (M^0_{3\ell-2} M^0_{3\ell-1} M^0_{3\ell})$ and $M^1[\ell] = (M^1_{3\ell-2} M^1_{3\ell-1} M^1_{3\ell})$ that ensure state collision in $W_{3\ell}$.



Nonce Misuse INT-RUP Attack on COLM

- Encryption 1: $(C^0[1] \cdots C^0[\ell], T) \leftarrow \mathcal{E}(N^*, A^*, M^0[1] \cdots M^0[\ell])$.
- Encryption 2: $(C^1[1] \cdots C^1[\ell], T') \leftarrow \mathcal{E}(N^*, A^*, M^1[1] \cdots M^1[\ell])$.

Find $b_1, b_2, \ldots, b_\ell$: (Apply Gaussian Elimination)

$$\oplus_{i=1}^{3\ell} M_i^0 = (M_1^{b_1} \oplus M_2^{b_1} \oplus M_3^{b_1}) \oplus \cdots \oplus (M_{3\ell-2}^{b_\ell} \oplus M_{3\ell-1}^{b_\ell} \oplus M_{3\ell}^{b_\ell}).$$

Nonce Misuse INT-RUP Attack on COLM

- Encryption 1: $(C^0[1] \cdots C^0[\ell], T) \leftarrow \mathcal{E}(N^*, A^*, M^0[1] \cdots M^0[\ell])$.
- Encryption 2: $(C^1[1] \cdots C^1[\ell], T') \leftarrow \mathcal{E}(N^*, A^*, M^1[1] \cdots M^1[\ell])$.

Find $b_1, b_2, \ldots, b_\ell$: (Apply Gaussian Elimination)

$$\oplus_{i=1}^{3\ell} M_i^0 = (M_1^{b_1} \oplus M_2^{b_1} \oplus M_3^{b_1}) \oplus \cdots \oplus (M_{3\ell-2}^{b_\ell} \oplus M_{3\ell-1}^{b_\ell} \oplus M_{3\ell}^{b_\ell}).$$

- Forge with $(C^{b_1}[1]C^{b_2}[2] \cdots C^{b_\ell}[\ell]T)$.

Nonce Respecting INT-RUP Attack on COLM

Nonce Respecting INT-RUP Attack on COLM

$$M_1 \cdots M_{n+1} \leftarrow \mathcal{D}(N, A, C_1 C_2 \cdots C_{n+1})$$

Nonce Respecting INT-RUP Attack on COLM

$$M_1 \cdots M_{n+1} \leftarrow \mathcal{D}(N, A, C_1 C_2 \cdots C_{n+1})$$
$$M_1^1 \cdots M_{n+1}^1 \leftarrow \mathcal{D}(N, A, C_1^1 C_2 \cdots C_{n+1})$$

Nonce Respecting INT-RUP Attack on COLM

$$M_1 \cdots M_{n+1} \leftarrow \mathcal{D}(N, A, C_1 C_2 \cdots C_{n+1})$$
$$M_1^1 \cdots M_{n+1}^1 \leftarrow \mathcal{D}(N, A, C_1^1 C_2 \cdots C_{n+1})$$

Main Observation

Using primitive polynomial, one can find $M_1^0 \cdots M_{n+1}^0$ whose W_{n+1} matches with $M_1^1 \cdots M_{n+1}^1$.

Nonce Respecting INT-RUP Attack on COLM

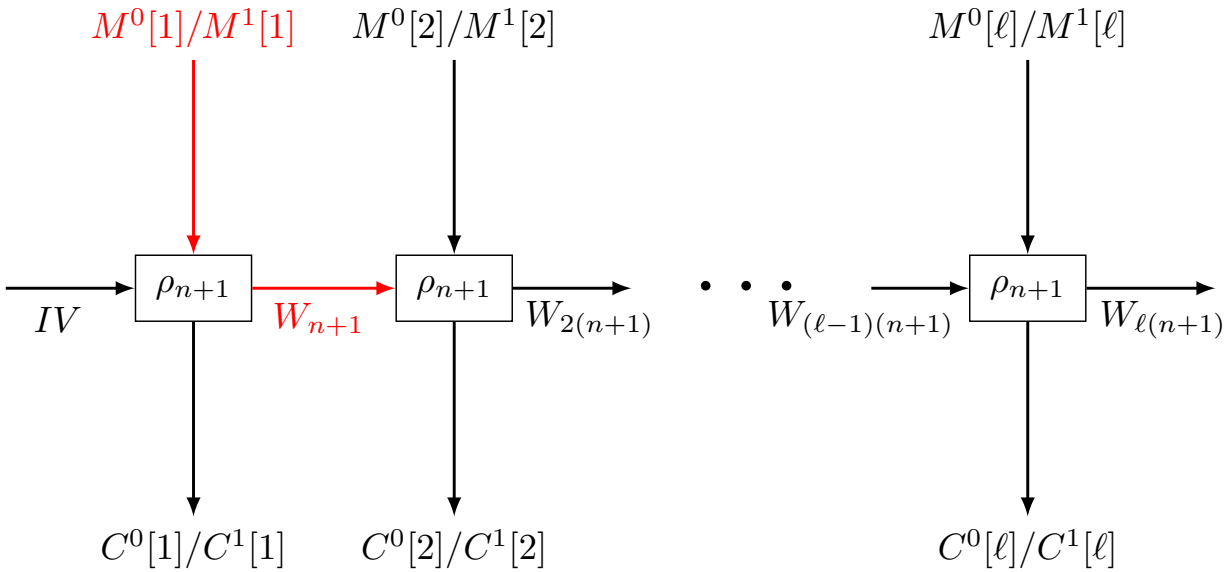
First Step: Find Non-trivial State Collision

Find $M^0[1] = (M^0_1 \cdots M^0_{n+1})$ and $M^1[1] = (M^1_1 \cdots M^1_{n+1})$ with identical W_{n+1}.

Nonce Respecting INT-RUP Attack on COLM

First Step: Find Non-trivial State Collision

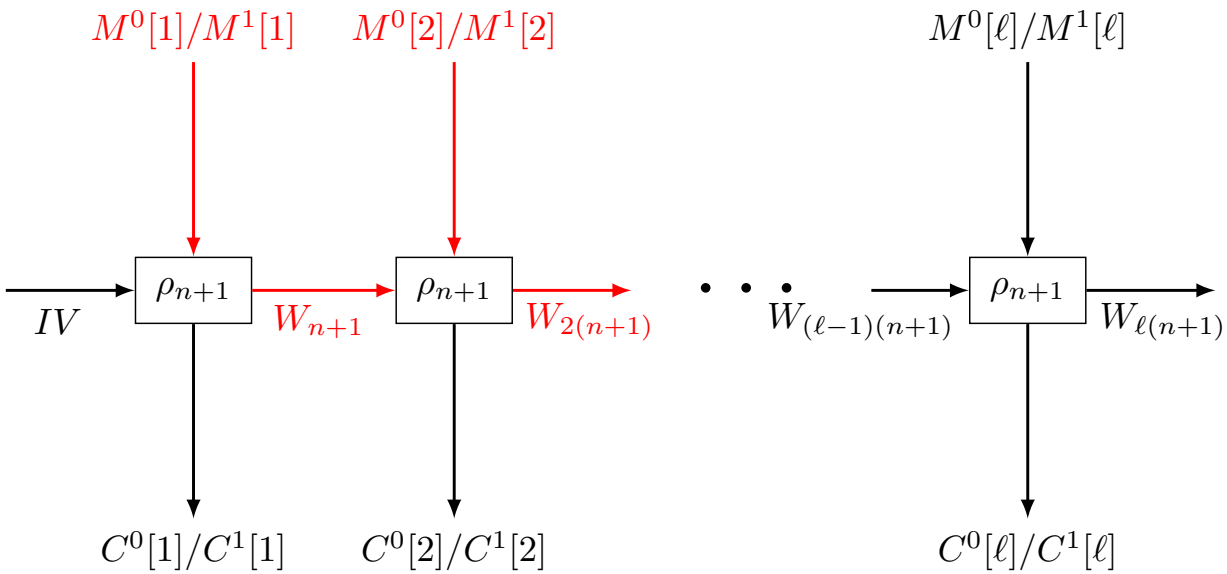
Find $M^0[1] = (M_1^0 \cdots M_{n+1}^0)$ and $M^1[1] = (M_1^1 \cdots M_{n+1}^1)$ with identical W_{n+1}.



Nonce Respecting INT-RUP Attack on COLM

Second Step: Strech the State Collision

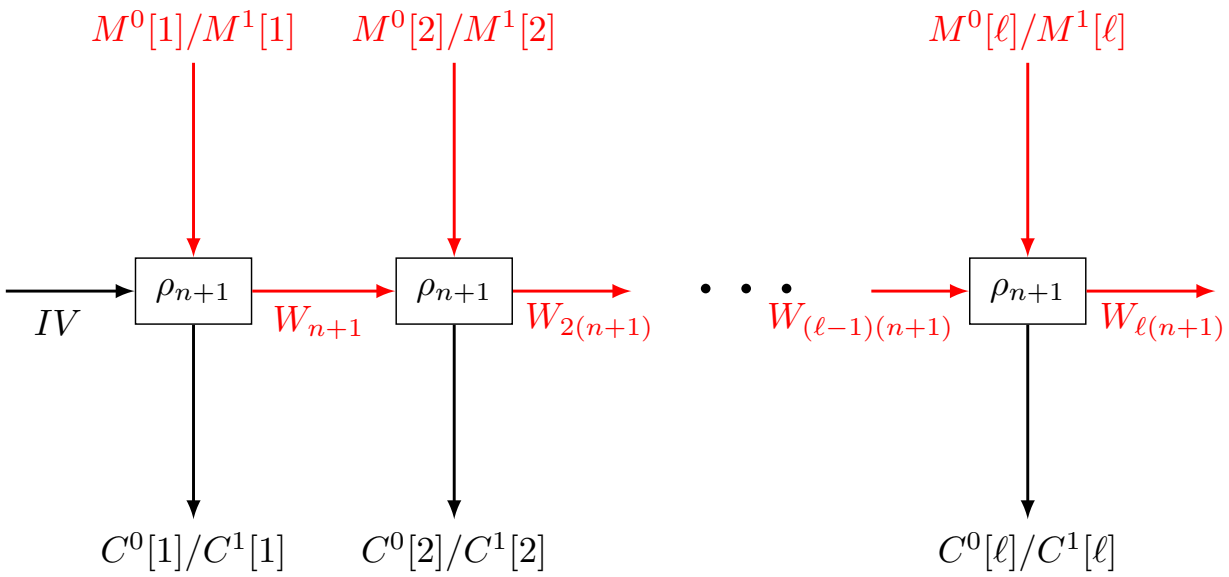
Find $M^0[2] = (M^0_{n+2} \cdots M^0_{2n+2})$ and $M^1[2] = (M^1_{n+1} \cdots M^1_{2n+2})$ that ensure state collision in $W_{2(n+1)}$.



Nonce Respecting INT-RUP Attack on COLM

Second Step: Strech the State Collision

Find $M^0[\ell] = (M^0_{(\ell-1)n+2} \cdots M^0_{\ell(n+1)})$ and $M^1[\ell] = (M^1_{(\ell-1)(n+1)+1} \cdots M^1_{\ell(n+1)})$ that ensure state collision in $W_{\ell(n+1)}$.



Nonce Respecting INT-RUP Attack on COLM

- Encryption: $(C^0[1] \cdots C^0[\ell], T) \leftarrow \mathcal{D}(N^*, A^*, M^0[1] \cdots M^0[\ell])$.

Find $b_1, b_2, \ldots, b_\ell$: (Apply Gaussian Elimination)

$$\oplus_{i=1}^{\ell(n+1)} M_i^0 = (M_1^{b_1} \oplus \cdots \oplus M_{n+1}^{b_1}) \oplus \cdots \oplus (M_{(\ell-1)(n+1)+1}^{b_\ell} \oplus \cdots \oplus M_{\ell(n+1)}^{b_\ell}).$$

- Forge: $(C^{b_1}[1]C^{b_2}[2] \cdots C^{b_\ell}[\ell]T)$.

Conclusion

Security of CAESAR Candidate COLM

- No refusion of security claims of COLM_0 and COLM_{127}.
- Importance of intermediate tags in COLM type structures.

Towards INT-RUP Secure COLM

- Restrict message length to n^2.
- State encryption after each n blocks.

Conclusion

Security of CAESAR Candidate COLM

- No refusion of security claims of COLM_0 and COLM_{127}.
- Importance of intermediate tags in COLM type structures.

Towards INT-RUP Secure COLM

- Restrict message length to n^2.
- State encryption after each n blocks.

Thank You!! Questions??