INT-RUP Analysis of AE Schemes

Avik Chakraborti, Nilanjan Datta and Mridul Nandi

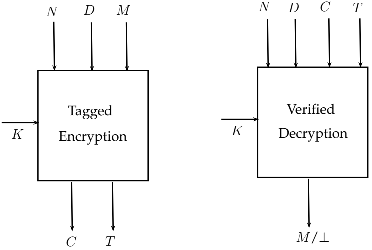
Indian Statistical Institute, Kolkata

Sep 29, DIAC-2015, Singapore

Outline of the talk

1. Introduction.
2. Main Result with Proof Sketch.
3. Future Works.

Authenticated Encryption



Main Goal

- Confidentiality of Plaintext
- Integrity of Plaintext and Associated Data.

Releasing Unverified Plaintext Scenario

Why release unverified plaintext??

- Limited buffer - can't hold entire plaintext.
- Problem: Adversary gets addition information.

RUP Setting (Andreeva et.al.)

- PA: Extractor capable of mimicking the decryption oracle.
- INT-RUP: Integrity Security of AE when adversary is given both encryption and decryption oracle.

Main Result

Result 1.

rate-1 Affine mode Authenticated Encryption mode is INT-RUP insecure.

Significance of the Result

Guideline: To achieve INT-RUP security, one has to compromise efficiency.

Main Result

Result 2.

CPFB (rate $\frac{3}{4}$) is INT-RUP insecure.

Questions

- How much efficiency we have to loose to get INT-RUP security?
- Can we have an INT-RUP secure scheme with rate $\frac{3}{4}$?

Main Result

Result 3.

m-CPFB (rate $\frac{3}{4}$) is INT-RUP insecure.

Significance

- INT-RUP comes with small degrade in efficiency.
- "rate-1" - a borderline criteria for INT-RUP security.

Affine Mode AE

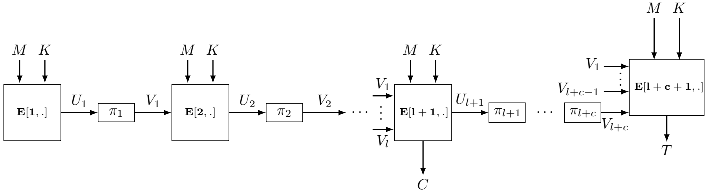


Figure : Structure of Affine Mode AE Schemes

Affine Mode AE

Matrix Representation

$$E.\begin{pmatrix} L \\ M \\ Y^* = \begin{pmatrix} Y \\ Y_{tag} \end{pmatrix} \end{pmatrix} = \begin{pmatrix} X^* = \begin{pmatrix} X \\ X_{tag} \end{pmatrix} \\ Z = \begin{pmatrix} C \\ T \end{pmatrix} \end{pmatrix}$$

Structure of Decryption Matrix

$$\begin{pmatrix} D_{11} & D_{12} & D_{13} & D_{14} \\ D_{21} & D_{22} & D_{23} & D_{24} \\ D_{31} & D_{32} & D_{33} & D_{34} \\ D_{41} & D_{42} & D_{43} & D_{44} \end{pmatrix} \cdot \begin{pmatrix} L \\ C \\ V \\ V_{tag} \end{pmatrix} = \begin{pmatrix} U \\ U_{tag} \\ M \\ T \end{pmatrix}$$

Properties of D-matrix

- Integrity of AE $\Rightarrow$ D_{12} has high rank.
- Privacy of AE $\Rightarrow$ D_{33} has high rank.

INT-RUP Attack

Queries of INT-RUP Adversary

- Encryption Query: $(N, AD, M^0 = (M_1^0, M_2^0, \ldots, M_l^0))$. Let, $C^0 = (C_1^0, C_2^0, \ldots, C_l^0, T^0)$ be the tagged ciphertext.
- Unverified Plaintext Query: $(N, AD, C^1 = (C_1^1, C_2^1, \ldots, C_l^1))$. Let $M^1 = (M_1^1, M_2^1, \ldots, M_l^1)$ be the corresponding plaintext.
- Forged Query: $(N, AD, C^f = (C_1^f, C_2^f, \ldots, C_l^f), T^f)$, which realizes a $\delta = (\delta_1, \ldots, \delta_l)$ sequence.

C^f realizes a $\delta = (\delta_1, \ldots, \delta_l)$-sequence

$\forall i \leq l,\ U_i^f = U_i^{\delta_i}$ and $\forall i > l,\ U_i^f = U_i^0$.

INT-RUP Attack (Construction of Forged Query)

$$\begin{pmatrix} D_{12} & D_{13} \\ D_{32} & D_{33} \end{pmatrix} \cdot \begin{pmatrix} \Delta C^{01} \\ \Delta V^{01} \end{pmatrix} = \begin{pmatrix} \Delta U^{01} \\ \Delta M^{01} \end{pmatrix}$$

Step I: Find ΔV^{01}

$$\Delta V^{01} = D_{33}^{-1}(\Delta M^{01} + D_{32}\Delta C^{01})$$

Note: D_{33} needs to be invertible.

INT-RUP Attack (Construction of Forged Query)

$$\begin{pmatrix} D_{12} & D_{13} \\ D_{32} & D_{33} \end{pmatrix} \cdot \begin{pmatrix} \Delta C^{0f} \\ \Delta V^{0f} \end{pmatrix} = \begin{pmatrix} \Delta U^{0f} \\ \Delta M^{0f} \end{pmatrix}$$

Step II: Find ΔC^{0f} in terms of δ

$$\begin{aligned} \Delta C^{0f} &= D_{12}^{-1}.(\Delta U^{0f} + D_{32}\Delta V^{0f}) \\ &= D_{12}^{-1}(\delta.\Delta U^{01} + D_{32}\delta.\Delta V^{01}) \\ &= D^{*}.\delta \end{aligned}$$

Note: D_{12} needs to be invertible.

INT-RUP Attack (Construction of Forged Query)

$$\begin{pmatrix} D_{22} & D_{23} & D_{24} \\ D_{42} & D_{43} & D_{44} \end{pmatrix} \cdot \begin{pmatrix} \Delta C^{0f} \\ \Delta V^{0f} \\ \Delta V^{0f}_{tag} \end{pmatrix} = \begin{pmatrix} \Delta U^{0f}_{tag} \\ \Delta T^{0f} \end{pmatrix}$$

Step III: Find δ that makes $\Delta U^{0f}_{tag} = 0$

Solve the following set of equations to find a δ:

$$D_{22}\Delta C^{0f} + D_{23}\Delta V^{0f} = 0$$

This equation has at least one solution as long as $l > (c-1).n$

INT-RUP Attack (Construction of Forged Query)

$$\begin{pmatrix} D_{22} & D_{23} & D_{24} \\ D_{42} & D_{43} & D_{44} \end{pmatrix} \cdot \begin{pmatrix} \Delta C^{0f} \\ \Delta V^{0f} \\ \Delta V_{tag}^{0f} \end{pmatrix} = \begin{pmatrix} \Delta U_{tag}^{0f} \\ \Delta T^{0f} \end{pmatrix}$$

Step IV: Find ΔC^{0f} and ΔT^{0f}

Put $\delta = \delta^*$ in the following equations:

$$\begin{aligned} \Delta C^{0f} &= D_{12}^{-1}.D^*.\delta \\ \Delta T^{0f} &= D_{42}\Delta C_{0f} + D_{43}\Delta V_{0f} \end{aligned}$$

Case When rank(D_{12}) or rank(D_{33}) is not full

Properties of Decryption Matrix

rank(D_{12}) and rank(D_{33}) should be high.

Extend the INT-RUP attack

Set l appropriately to a high value with a $(n \times n)$ submatrix which has full rank for both D_{12} as well as D_{33}.

Extensions of the result

- Any "rate-1" block-cipher based AE scheme is not integrity secure against Nonce-repeating adversaries.
- This attack is applicable for IACBC and IAPM (construction with *logl*-many masking keys.
- In general, the attack is applicable to any "rate-1" affine mode AE for which D_{12} and D_{33} are invertible, even if the number of masking keys it use depends on the message length.

Revisit CPFB

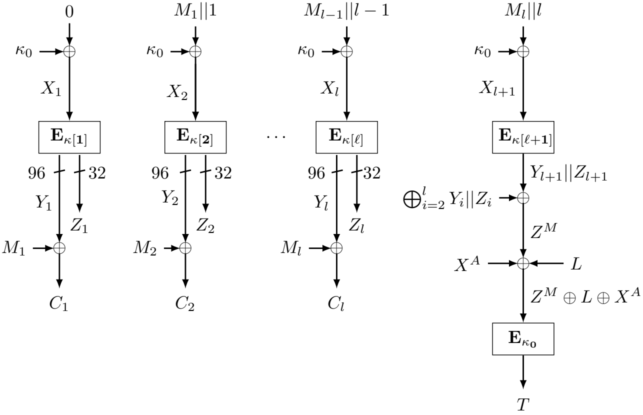


Figure : Encryption and Tag Genration Phase of CPFB. Here $\kappa_i = E_K(N||i||l_N)$, $\kappa[i] = \kappa_j$ where $j = \lceil \frac{i}{2^{32}} \rceil$, $X^A := U_a$ where $U_i = U_{i-1} + E_{\kappa_0}(A_i||i)$ and $L = E_{\kappa_0}(a||l||0)$.

INT-RUP Attack on CPFB

INT-RUP Attack on CPFB

1. Encryption query: (N, A, M^0), $|M^0| = l = 129$. Let C^0 be the ciphertext
2. Unverified Plaintext decryption query: (N, A, C^1) of length l. Let, M^1 be the corresponding plaintext.
3. Compute Y values: $Y_1^0, \cdots, Y_l^0$ and $Y_1^1, \cdots, Y_l^1$ from the two queries (by $M^0 + C^0$ and $M^1 + C^1$).
4. Find the δ-sequence: $\delta = (\delta_1, \ldots, \delta_l)$, with $\delta_1 = 0$ such that,
$$\sum_{i=2}^{l} Y_i^{\delta_i} = \sum_{i=2}^{l} Y_i^0.$$
Expect 2^{32}-many such δ-sequences.

INT-RUP Attack on CPFB

INT-RUP Attack on CPFB

Perform the following for all such δ-sequence:

1. Set $C_1^f = C_1^0$. For all $1 < i < l$, set $C_i^f = C_i^{\delta_i}$ if $\delta_{i-1} = \delta_i$ and $C_i^{\delta_i} + Y_i^0 + Y_i^1$, otherwise.
2. Set $C_l^f = C_l^0$ if $\delta_l = 0$. Else, set $C_l^f = C_l^0 + Y_l^0 + Y_l^1$.
3. Return $(C_1^f, C_2^f, \cdots, C_l^f, T^0)$ as forged Ciphertext.

Building an INT-RUP Secure rate-$\frac{3}{4}$ Construction

Potential Weakness of CPFB

1. Y_i values can be observed. Only Z_i-values are unknown.
2. Z_i has only 32-bit entropy on the Tag.

Requirement of the New Construction

- Ensure 128-bit entropy of Z-values on the tag.
- Ensure at-least 4 different Z-values for 2 messages of same length.

mCPFB: modified CPFB

Introduce ECC Code

Expand $M = (M_1, \ldots, M_l)$ by a Distance 4 Error Correcting Code ECCode:

$$\mathrm{ECCode}(M) = (M_1, \ldots, M_l, M_{l+1}, M_{l+2}, M_{l+3})$$
$$(M_{l+1}, M_{l+2}, M_{l+3}) = V_{\beta}^{(3,l)} \cdot M$$

Produce 128-bit entropy of Z-values during Tag Generation:

Update Z^M as follows:
$Z_M = V_{\alpha}^{(4,l+3)} \cdot (Z_2, Z_3, \cdots, Z_{l+3}, Z_{l+4}) \oplus (0^{32} || (Y_2 \oplus \cdots \oplus Y_{l+3}))$

mCPFB: modified CPFB

Changes in the keys

- κ_0 is used as the masking key only.
- κ_1 is used as block-cipher key for AD processing.
- $\kappa_1, \ldots, \kappa_{-2}$ is used as block-cipher keys for message processing.
- κ_{-1} is used as block-cipher key for tag and producing L-values.

INT-RUP Security of mCPFB

Claim 1

Consider the function f that takes N, I and i as input and outputs O such that $O = E_{\kappa[i]}(I||(i \ mod \ 2^{32}) + \kappa_0)$ where $\kappa[i] = E_K(N||j||I)$, $j = \lceil \frac{i}{2^{32}} \rceil$. f is assumed to have (q, ϵ)-PRF security where ϵ is believed to achieve beyond birthday security.

INT-RUP advantage

f: $(q_e + q_r, \epsilon)$-PRF. Any adversary $\mathcal{A}$ with q_e many encryption query and q_r many unverified plaintext queries, one forgery attempts, has the advantage:

$$Adv^{int\_rup}_{mCPFB}(\mathcal{A}) \leq \frac{5}{2^{128}} + \epsilon$$

Proof Sketch

Argument for Different Cases

- (Case A) $\forall i, N^* \neq N_i$: Through randomness of κ_{-1}.
- (Case B) $\exists$ unique $i \ni N^* = N_i, T^* \neq T_i$: Through randomness of κ_{-1}.
- (Case C) $\exists$ unique $i \ni N^* = N_i,\ T^* = T_i,\ |C_i| = |C^*|$: Through randomness of Z_i's.
- (Case D) $\exists$ unique $i \ni N^* = N_i,\ T^* = T_i,\ |C_i| \neq |C^*|$: Through randomness of κ_{-1}.

Future Works

- INT-RUP analysis for B/C based constructions with $rate < 1$.
- INT-RUP Security Analysis of ELmD, CLOC and SILC.

Thank you