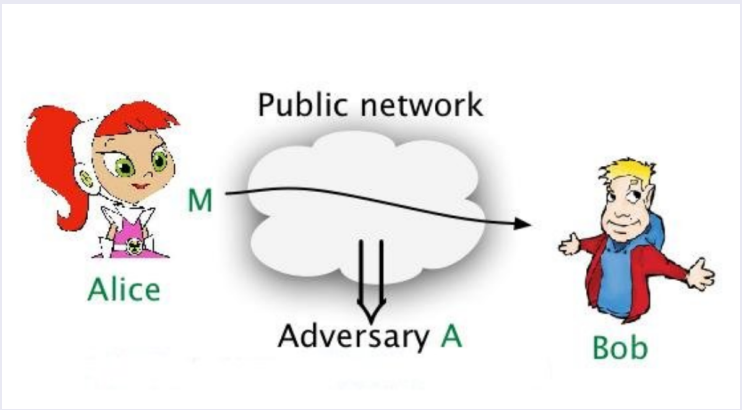
Blockcipher-based Authentcated Encryption: How Small Can We Go?

Avik Chakraborti (Indian Statistical Institute, Kolkata)
Tetsu Iwata (Nagoya University, Japan)
Kazuhiko Minematsu (NEC Corporation, Japan)
Mridul Nandi (Indian Statistical Institute, Kolkata)

September, 2016

Authenticated Encryption (AE)



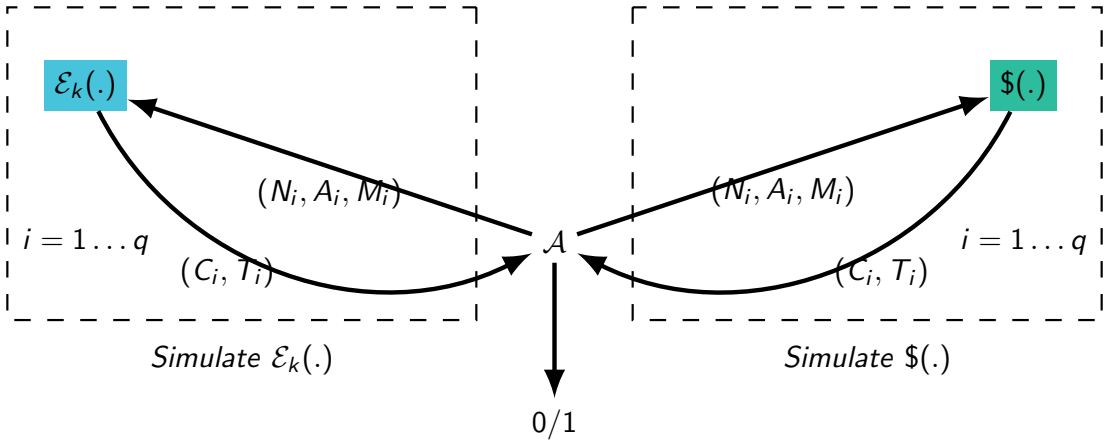
More Formally....

- AE.enc : $\mathcal{M} \times \mathcal{D} \times \mathcal{N} \times \mathcal{K} \rightarrow \mathcal{C}$
- AE.dec : $\mathcal{C} \times \mathcal{D} \times \mathcal{N} \times \mathcal{K} \rightarrow \mathcal{M} \cup \perp$

Goal	Primitive	Security
Privacy	Symmetric Encryption	IND-CPA
Integrity	MAC/Others	INT-CTXT

Table: Security Properties

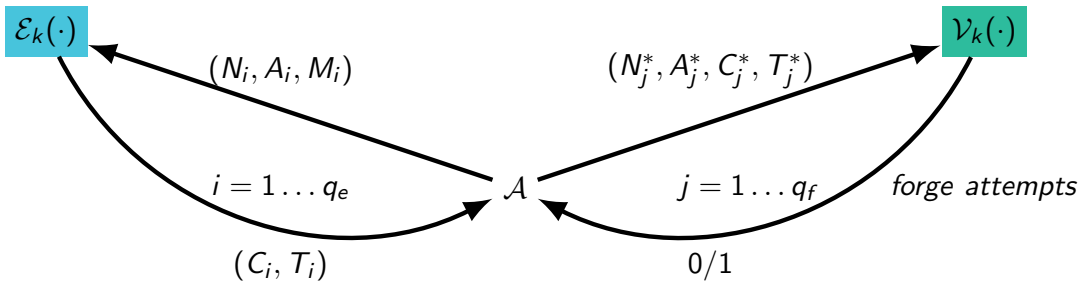
IND-CPA Security for Privacy



$$\Delta_{\mathcal{A}}(\mathcal{O}_1; \mathcal{O}_2) = |\Pr[\mathcal{A}^{\mathcal{O}_1} = 1] - \Pr[\mathcal{A}^{\mathcal{O}_2} = 1]|.$$

- $\mathbf{Adv}^{\mathrm{PRIV}}_{\mathcal{AE}}(\mathcal{A}) := \Delta_{\mathcal{A}}(\mathcal{E}_K; \$)$
- $\mathbf{Adv}^{\mathrm{PRIV}}_{\mathcal{AE}}(q, \sigma, t) = \max_{\mathcal{A}} \mathbf{Adv}^{\mathrm{PRIV}}_{\mathcal{AE}}(\mathcal{A})$
- t: Time, q: #queries , σ: # blocks in all queries

INT-CTXT Security for Integrity



- $\mathcal{A}$ *forges* if $\exists\ (N_j^*, A_j^*, C_j^*, T_j^*) \ni \mathcal{V}_k(N_j^*, A_j^*, C_j^*, T_j^*) = 1$

- $\mathbf{Adv}^{\mathrm{INT}}_{\mathcal{AE}}(\mathcal{A}) := Pr[\mathcal{A}^{\mathcal{E}_k}\ forges]$
- $\mathbf{Adv}^{\mathrm{INT}}_{\mathcal{AE}}((q_e, q_f), (\sigma_e, \sigma_f), t) = \max_{\mathcal{A}} \mathbf{Adv}^{\mathrm{INT}}_{\mathcal{AE}}(\mathcal{A})$

Current State of the Art

Structural Properties

Schemes	CLOC-SILC	AES-JAMBU	iFEED
State	2n + k	1.5n + k	3n + k
Rate	$\frac{1}{2}$	$\frac{1}{2}$	1
Proofs	Yes	Yes (integrity only)	Yes (wrong)

Here n is the blocksize of blockcipher

Main Idea and Motivation Behind the Construction

- Very *small* cipher state
- Provably Security in terms of both *Privacy* and *Integrity*

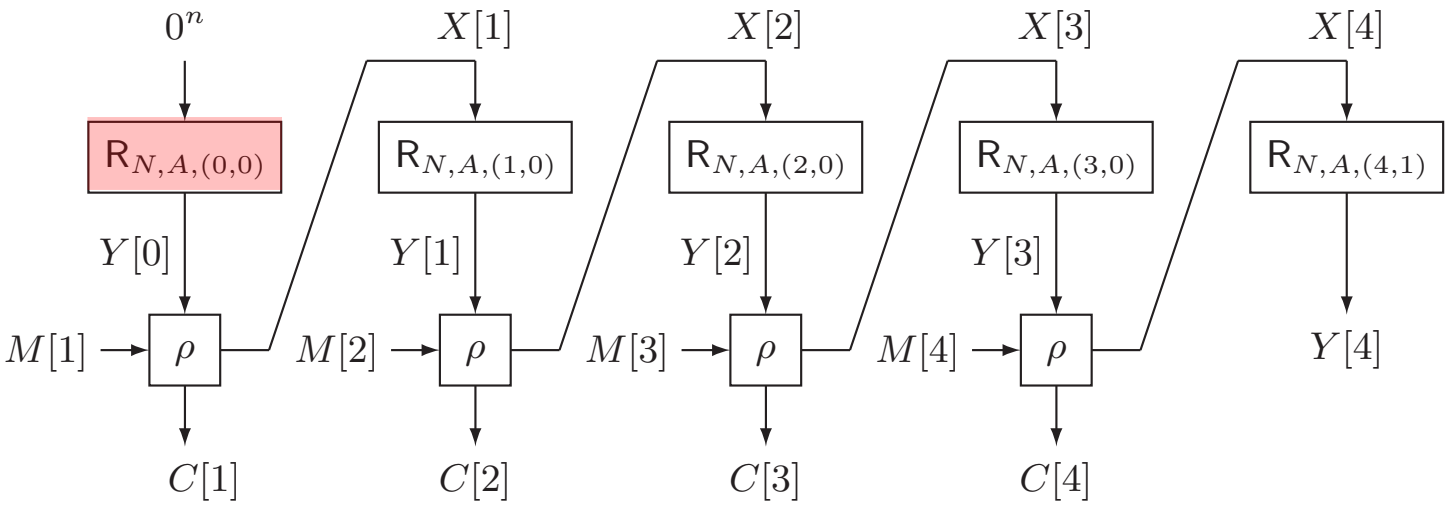
iCOFB Construction

Generic *Combined* Feedback Mode

Instantiated by *COFB* AE scheme

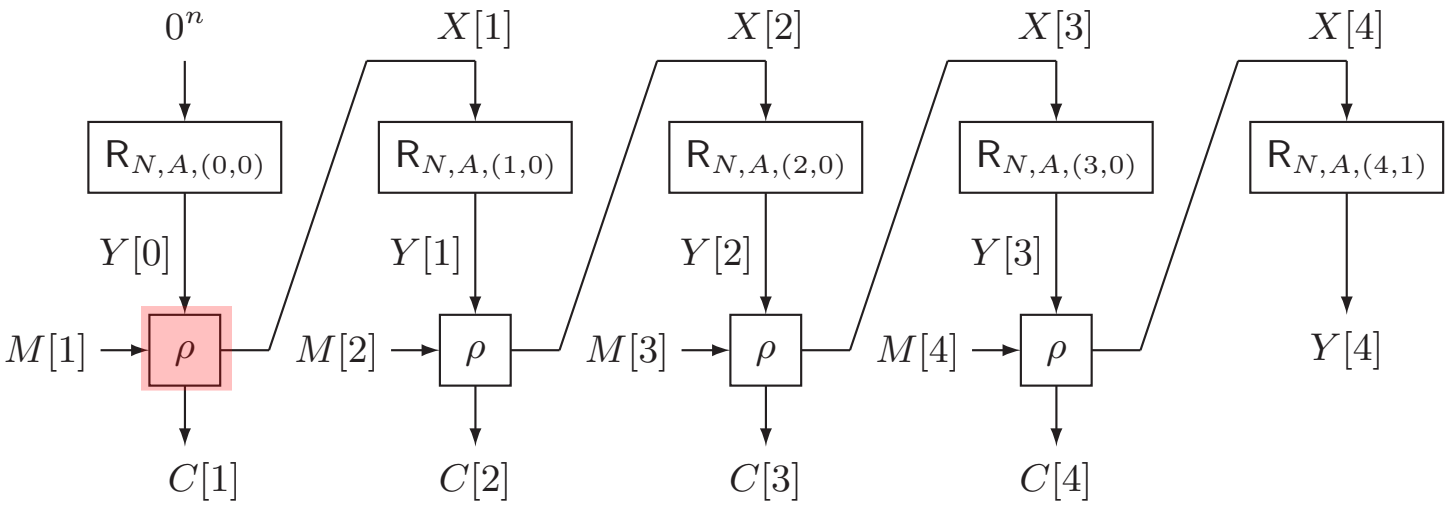
Easy to Understand COFB

iCOFB Construction



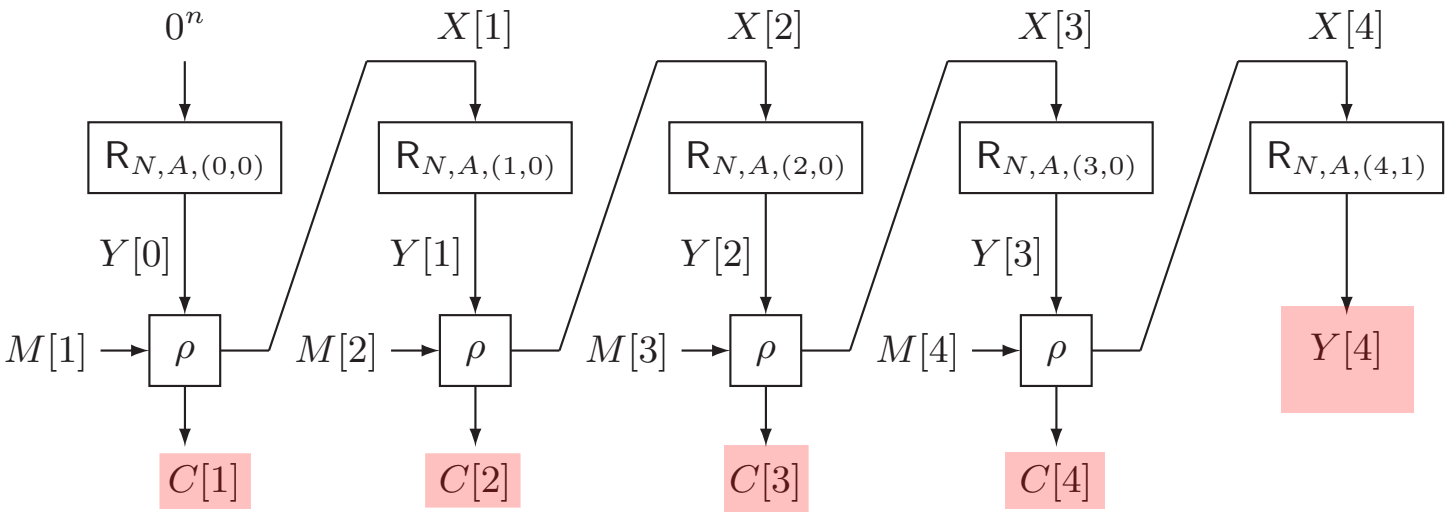
- $\mathsf{R}_{N,A,(a,b)}$: *Tweakable random function*
- $\forall N, A, (a, b)$, $\mathsf{R}_{N,A,(a,b)} : \mathcal{B} \rightarrow \mathcal{B}$

iCOFB Construction



- ρ : *Linear Feedback Function*

iCOFB Construction



- $CT = (C[1], C[2], C[3], C[4]), \quad Tag = Y[4]$

Linear Feedback Function : ρ

- For $\rho : \mathcal{B} \times \mathcal{B} \rightarrow \mathcal{B} \times \mathcal{B}$, $\exists \rho^{'}$
- *Correctness Condition* for encryption,
  - $\forall Y, M \in \mathcal{B}$, $\rho(Y, M) = (X, C) \Rightarrow \rho^{'}(Y, C) = (X, M)$
- ρ ensures given (Y, C): M should be *uniquely* computable
- Example : $\rho = \begin{pmatrix} G & I \\ I & I \end{pmatrix}$, $\rho^{'} = \begin{pmatrix} I + G & I \\ I & I \end{pmatrix}$, G is *invertible*

ρ and ρ'

ρ: During Encryption

- $\begin{pmatrix} X[i] \\ C[i] \end{pmatrix} = \begin{pmatrix} E_{1,1} & E_{1,2} \\ E_{2,1} & E_{2,2} \end{pmatrix} \begin{pmatrix} Y[i-1] \\ M[i] \end{pmatrix}$
- If ρ Satisfies the correctness condition then $E_{2,2}$ must be *inv*

ρ': During Decryption

- $\begin{pmatrix} X[i] \\ M[i] \end{pmatrix} = \begin{pmatrix} D_{1,1} & D_{1,2} \\ D_{2,1} & D_{2,2} \end{pmatrix} \begin{pmatrix} Y[i-1] \\ C[i] \end{pmatrix}$
- $D_{1,1} = E_{1,1} + E_{1,2}.E_{2,2}^{-1}.E_{2,1}$, $D_{1,2} = E_{1,2}$
- $D_{2,1} = E_{2,2}^{-1}.E_{2,1}$, $D_{2,2} = E_{2,2}^{-1}$
- ρ is *Valid* if both $(C1)$ $E_{2,1}$, $(C2)$ $D_{1,2}$ and $(C3)$ $D_{1,1}$ invertible

Privacy and Authencity for iCOFB

- $(C2) \Rightarrow \forall Y, C \neq C',\ D_{1,1}.Y + D_{1,2}.C \neq D_{1,1}.Y + D_{1,2}.C'$
- $(C3) \Rightarrow \rho$ is invertible (for correctness $E_{2,2}^{-1}$ is invertible). Hence,

$$\Pr[Y \xleftarrow{\$} \mathcal{B} : D_{1,1}.Y + D_{1,2}.C = X] = 2^{-n},\ \forall (C, X) \in \mathcal{B}^2$$

Theorem

If ρ is valid then for adversary $\mathcal{A}$ making q encryption queries and q_f forging attempts having at most ℓ_f many blocks, we have

$$\mathbf{Adv}^{\mathrm{priv}}_{iCOFB}(\mathcal{A}) = 0, \quad \mathbf{Adv}^{\mathrm{auth}}_{iCOFB}(\mathcal{A}) \leq \frac{q_f(\ell_f + 1)}{2^n}.$$

Design Rationale and Challenges

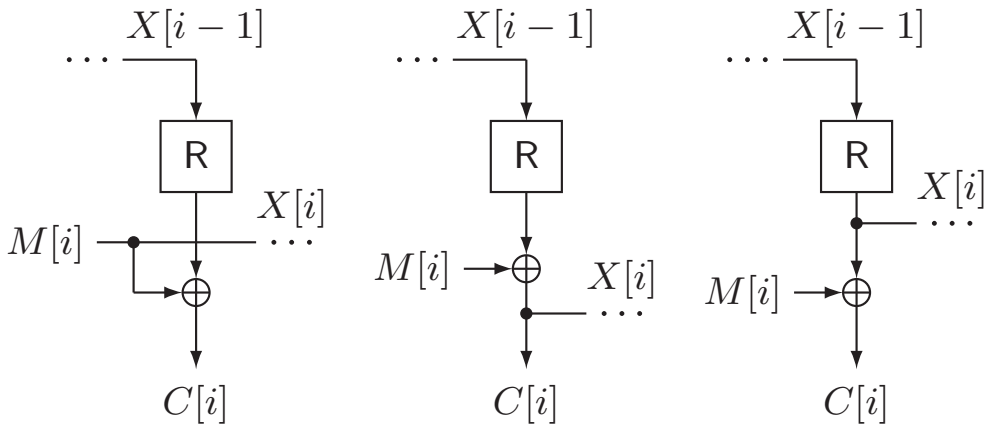
COFB : An instantiation of iCOFB

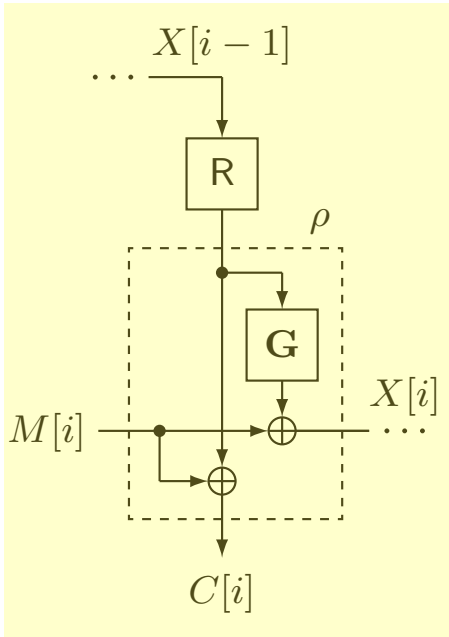
- Instatiation of iCOFB is possible by standard method (like XE mode)
- But results in 2 state memories

- Here, we considered *half* tweak (only Half-bit mask)
- Sufficient for *standard* security bound

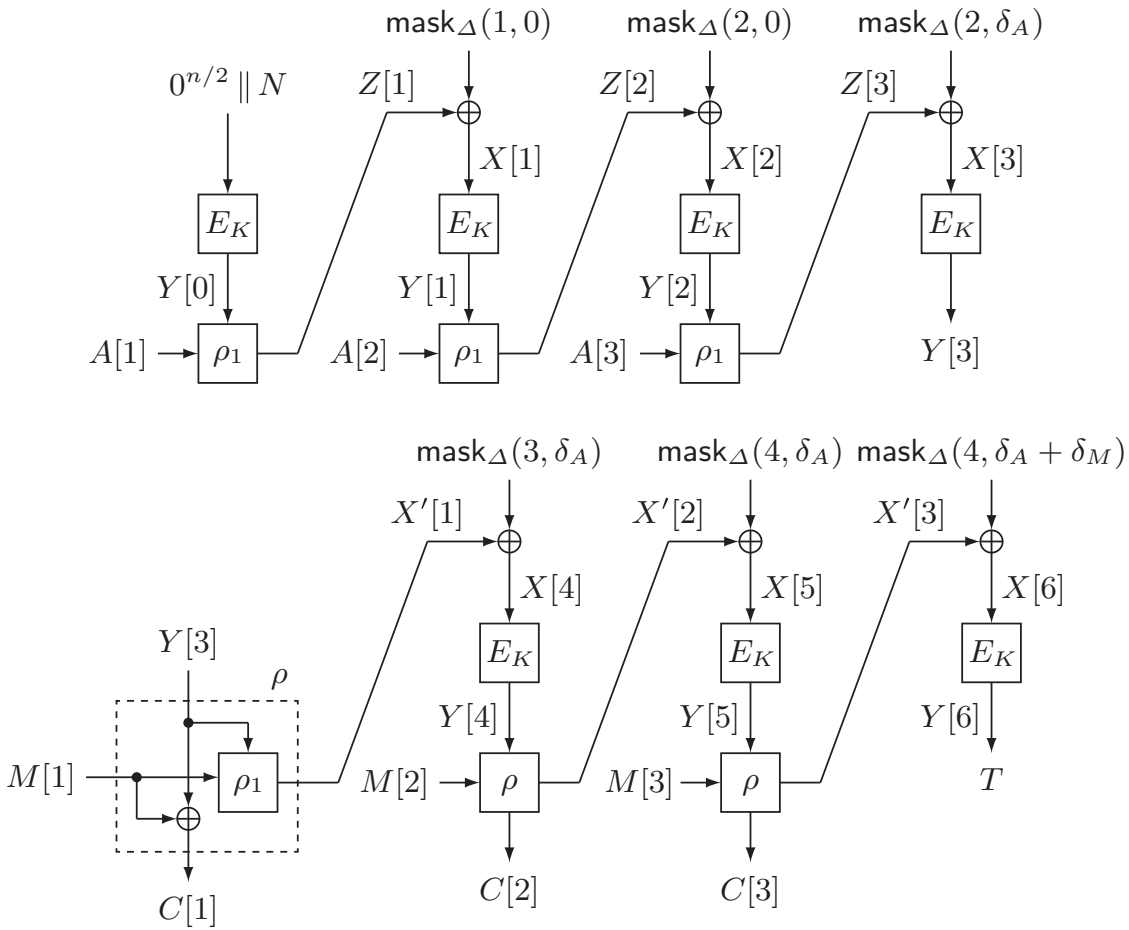
- The proof for COFB is not the same as XE based iCOFB
- Proof based on *specific* design (w/o iCOFBs security bound)

COFB (Combined Feedback) Mode





COFB Authenticated Encryption Scheme



COFB Authenticated Encryption Mode

Underlying Blockcipher

- We use *AES*-128 as the underlying blockcipher
- $n = 128$

mask Function

mask - mask is simple tweak update function

ρ_1 and ρ Functions

ρ_1 and ρ Functions - Simple Linear Feedback Functions.

Last Block has *different* tweak

Tweak Function

- Tweak - *Nonce* dependent 64 -bit secret value.
- Standard Tweak size - 128-bits. Here 64-bit is sufficient
- Computed/ updated by $\text{mask}_\Delta(a, b) = \alpha^a(1+\alpha)^b.\Delta$
- $(a, b) \in [0..L] \times [0..4]$, L be the message length in blocks
- α - primitive element in $\mathbb{F}_{2^{64}}$

Linear Feedback Function

- Two feedback function - ρ_1 and ρ
- $\rho_1(y, M) := G \cdot y \oplus M$ and $\rho(y, M) = (\rho_1(y, M), \quad y \oplus M)$
- $G : (y_1, y_2, y_3, y_4) \rightarrow (y_2, y_3, y_4, y_4 \oplus y_1)$

$$G_{n \times n} = \begin{pmatrix} 0 & I & 0 & 0 \\ 0 & 0 & I & 0 \\ 0 & 0 & 0 & I \\ I & 0 & 0 & I \end{pmatrix}$$

Security Level for COFB

Security Bounds for privacy

- *Birthday* Bound
- 64-bit for *Privacy*

Security Bounds for Authenticity

- *Birthday* Bound
- 64-bit for *Authenticity*

Important Features of COFB

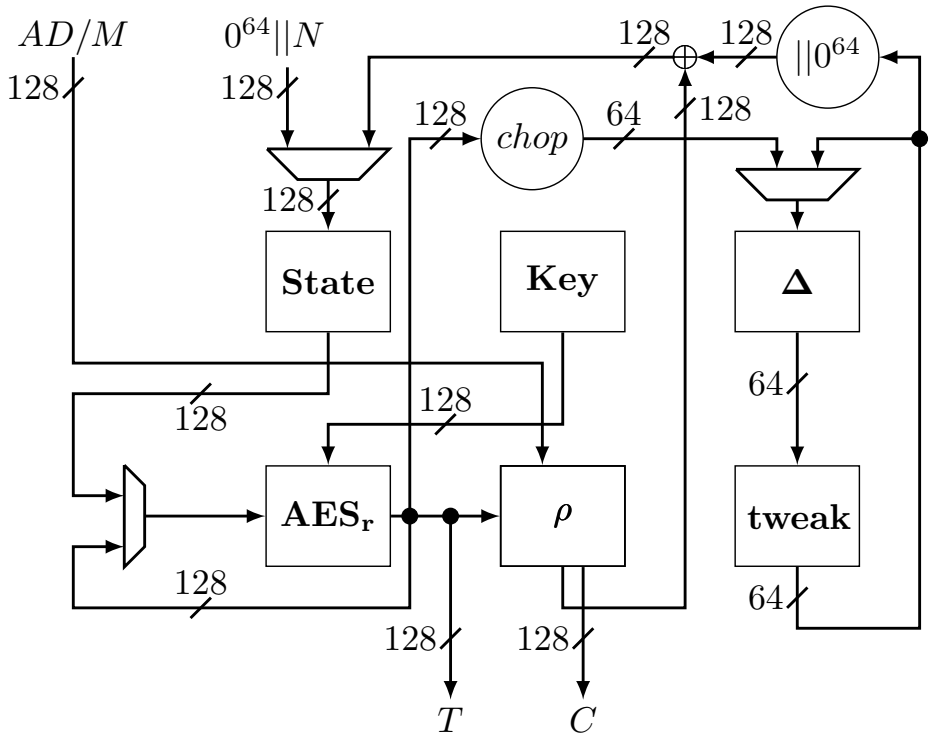
Advantages

- It is a "*Rate* − 1" construction.
- Very low *state size*. Only $1.5n + k$ (n:blockcipher size)
- Very *Flexible* Mode (*Any* Blockcipher)
- It is *inverse*-*free*
- *Simple* yet highly *effective* Linear Feedback
- Very Lightweight and Consumes *Low* Hardware area

Limitations

- *Both* the encryption and decryption are completely *serial*

COFB-Base Architecture



COFB-Base Architecture Properties

- No *pipelined* register
- *Serial* processing of data
- Processes 128-bits per 12 clock cycles
- Uses Very *Low* Storage Registers
- *Minimum* Hardware Area Among All the Known Implementations

COFB FPGA Implementation

Informations

- VHDL
- PLatform - Virtex 6 Under Xilinx 13.4
- Target Device - xc6vlx760

Base Implementation Results

- Area : 722 Slice Reg, 1075 LUTs and 442 Slices
- Frequency : 267.20 MHZ, Throughput : 2.85 Gbps

Benchmarking of COFB

A *fair* comparison is needed

A fair comparison based on *GMU* inteface to be done in future

Conclusion

- COFB : *Blockcipher* based *AE*
- 64-bit privacy and 64-bit authenticity.
- *Low Area* AE and can be used in low resource *embedded device*

Thank you