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
1 Introduction

2 Idealized Combined Feedback Construction : iCOFB

3 Specification for COFB

4 Hardware Implementation Results of COFB

5 Conclusion
Authenticated Encryption (AE)

More Formally....

- \(\text{AE.\text{enc}} : M \times D \times N \times K \rightarrow C\)
- \(\text{AE.\text{dec}} : C \times D \times N \times K \rightarrow M \cup \perp\)

Table: Security Properties

<table>
<thead>
<tr>
<th>Goal</th>
<th>Primitive</th>
<th>Security</th>
</tr>
</thead>
<tbody>
<tr>
<td>Privacy</td>
<td>Symmetric Encryption</td>
<td>IND-CPA</td>
</tr>
<tr>
<td>Integrity</td>
<td>MAC/Others</td>
<td>INT-CTXT</td>
</tr>
</tbody>
</table>
IND-CPA Security for Privacy

\[
\Delta_A(O_1; O_2) = | \Pr[A^{O_1} = 1] - \Pr[A^{O_2} = 1] |
\]

- \( \text{Adv}^{\text{PRIV}}_{A\mathcal{E}} (A) := \Delta_A(\mathcal{E}_K; $) 
- \( \text{Adv}^{\text{PRIV}}_{A\mathcal{E}} (q, \sigma, t) = \max_A \text{Adv}^{\text{PRIV}}_{A\mathcal{E}} (A) \)
- \( t: \text{Time}, \ q: \# \text{queries}, \ \sigma: \# \text{blocks in all queries} \)
INT-CTXT Security for Integrity

- $A$ **forges** if $\exists (N_j^*, A_j^*, C_j^*, T_j^*)$ $\ni V_k(N_j^*, A_j^*, C_j^*, T_j^*) = 1$

- $\text{Adv}_{\mathcal{AE}}^{\text{INT}}(A) := Pr[A^E_k \text{ forges}]$
- $\text{Adv}_{\mathcal{AE}}^{\text{INT}}((q_e, q_f), (\sigma_e, \sigma_f), t) = \max_A \text{Adv}_{\mathcal{AE}}^{\text{INT}}(A)$
1. Introduction

2. Idealized Combined Feedback Construction: iCOFB
   - Motivation
   - Idealized Combined-Feedback Authenticated Encryption: iCOFB
   - Security of iCOFB

3. Specification for COFB

4. Hardware Implementation Results of COFB

5. Conclusion
### Structural Properties

<table>
<thead>
<tr>
<th>Schemes</th>
<th>CLOC-SILC</th>
<th>AES-JAMBU</th>
<th>iFEED</th>
</tr>
</thead>
<tbody>
<tr>
<td>State</td>
<td>$2n + k$</td>
<td>$1.5n + k$</td>
<td>$3n + k$</td>
</tr>
<tr>
<td>Rate</td>
<td>$\frac{1}{2}$</td>
<td>$\frac{1}{2}$</td>
<td>1</td>
</tr>
<tr>
<td>Proofs</td>
<td>Yes</td>
<td>Yes (integrity only)</td>
<td>Yes (wrong)</td>
</tr>
</tbody>
</table>

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
1 Introduction

2 Idealized Combined Feedback Construction: iCOFB
   - Motivation
   - Idealized Combined-Feedback Authenticated Encryption: iCOFB
   - Security of iCOFB

3 Specification for COFB

4 Hardware Implementation Results of COFB

5 Conclusion
iCOFB Construction

Generic *Combined* Feedback Mode

Instantiated by *COFB* AE scheme

*Easy* to Understand COFB
iCOFB Construction

- $R_{N,A,(a,b)}$: *Tweakable random function*
- $\forall N, A, (a, b), R_{N,A,(a,b)} : \mathcal{B} \rightarrow \mathcal{B}$
**iCOFB Construction**

\[
\begin{align*}
0^n & \rightarrow R_{N,A,(0,0)} \\
Y[0] & \rightarrow R_{N,A,(1,0)} \\
M[1] & \rightarrow \rho \\
C[1] & \\
X[1] & \rightarrow R_{N,A,(2,0)} \\
Y[1] & \rightarrow R_{N,A,(3,0)} \\
M[2] & \rightarrow \rho \\
C[2] & \\
X[2] & \rightarrow R_{N,A,(4,1)} \\
Y[2] & \rightarrow R_{N,A,(0,0)} \\
M[3] & \rightarrow \rho \\
C[3] & \\
X[3] & \rightarrow R_{N,A,(1,0)} \\
Y[3] & \rightarrow R_{N,A,(2,0)} \\
M[4] & \rightarrow \rho \\
C[4] & \\
X[4] & \\
Y[4] & 
\end{align*}
\]

- \( \rho \): Linear Feedback Function
iCOFB Construction

\[ CT = (C[1], C[2], C[3], C[4]), \quad Tag = Y[4] \]
Linear Feedback Function: $\rho$

- For $\rho : \mathcal{B} \times \mathcal{B} \rightarrow \mathcal{B} \times \mathcal{B}$, $\exists \rho'$

- **Correctness Condition** for encryption,
  - $\forall Y, M \in \mathcal{B}, \rho(Y, M) = (X, C) \Rightarrow \rho'(Y, C) = (X, M)$

- $\rho$ 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
**Introduction**

**Idealized Combined Feedback Construction : iCOFB**

**Specification for COFB**

**Hardware Implementation Results of COFB**

**Conclusion**

---

**Motivation**

**Idealized Combined-Feedback Authenticated Encryption : iCOFB**

**Security of iCOFB**

---

### $\rho$ and $\rho'$

#### $\rho$: During Encryption

$$(X[i]) = \begin{pmatrix} E_{1,1} & E_{1,2} \\ E_{2,1} & E_{2,2} \end{pmatrix} \begin{pmatrix} Y[i - 1] \\ M[i] \end{pmatrix}$$

- If $\rho$ Satisfies the correctness condition then $E_{2,2}$ must be $\text{inv}$

#### $\rho'$: During Decryption

$$(X[i]) = \begin{pmatrix} D_{1,1} & D_{1,2} \\ D_{2,1} & D_{2,2} \end{pmatrix} \begin{pmatrix} Y[i - 1] \\ C[i] \end{pmatrix}$$

- $D_{1,1} = E_{1,1} + E_{1,2} \cdot E_{2,2}^{-1} \cdot E_{2,1}$, $D_{1,2} = E_{1,2}$
- $D_{2,1} = E_{2,2}^{-1} \cdot E_{2,1}$, $D_{2,2} = E_{2,2}^{-1}$
- $\rho$ is $\text{Valid}$ if both $(C1)$ $E_{2,1}$, $(C2)$ $D_{1,2}$ and $(C3)$ $D_{1,1}$ invertible
1 Introduction

2 Idealized Combined Feedback Construction: iCOFB
   - Motivation
   - Idealized Combined-Feedback Authenticated Encryption: iCOFB
   - Security of iCOFB

3 Specification for COFB

4 Hardware Implementation Results of COFB

5 Conclusion
Privacy and Authenticity 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,

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

**Theorem**

If \(\rho\) is valid then for adversary \(A\) making \(q\) encryption queries and \(q_f\) forging attempts having at most \(\ell_f\) many blocks, we have

\[
\text{Adv}^\text{priv}_{iCOFB}(A) = 0, \quad \text{Adv}^\text{auth}_{iCOFB}(A) \leq \frac{q_f(\ell_f + 1)}{2^n}.
\]
1. Introduction

2. Idealized Combined Feedback Construction: iCOFB

3. Specification for COFB
   - Underlying Mathematical Components for COFB
   - Security Bounds
   - Properties

4. Hardware Implementation Results of COFB

5. Conclusion
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

\[ \begin{align*}
X[i] & \quad \text{R} \\
M[i] & \quad X[i - 1] \\
C[i] & \\
\end{align*} \]

\[ \begin{align*}
X[i] & \quad \text{R} \\
M[i] & \quad X[i - 1] \\
C[i] & \\
\end{align*} \]

\[ \begin{align*}
X[i] & \quad \text{R} \\
M[i] & \quad X[i - 1] \\
C[i] & \\
\end{align*} \]
COFB Authenticated Encryption Scheme

\[
\begin{align*}
&0^{n/2} \parallel N \\
&Y[0] \\
&A[1] \rightarrow \rho_1 \\
&E_K \\
&Y[1] \\
&A[2] \rightarrow \rho_1 \\
&E_K \\
&Z[1] \\
&X[1] \\
&mask_\Delta(1, 0) \\
&Y[2] \\
&A[3] \rightarrow \rho_1 \\
&E_K \\
&Z[2] \\
&X[2] \\
&mask_\Delta(2, 0) \\
&Y[3] \\
&A[4] \rightarrow \rho_1 \\
&E_K \\
&Z[3] \\
&X[3] \\
&mask_\Delta(2, A) \\
&Y[4] \\
&M[1] \rightarrow \rho_1 \\
&E_K \\
&Y[5] \\
&M[2] \rightarrow \rho \\
&E_K \\
&C[2] \\
&mask_\Delta(3, A) \\
&Y[6] \\
&M[3] \rightarrow \rho \\
&E_K \\
&T \\
&mask_\Delta(4, A + M) \\
\end{align*}
\]
**Underlying Blockcipher**

- We use *AES-128* as the underlying blockcipher
- \( n = 128 \)

**mask Function**

- mask - mask is simple tweak update function

**\( \rho_1 \) and \( \rho \) Functions**

- \( \rho_1 \) and \( \rho \) 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 $\text{mask}_\Delta (a, b) = \alpha^a (1 + \alpha)^b \cdot \Delta$

- $(a, b) \in [0..L] \times [0..4]$, $L$ be the message length in blocks.

- $\alpha$ - primitive element in $\mathbb{F}_{2^{64}}$.
Linear Feedback Function

- Two feedback functions: $\rho_1$ and $\rho$

- $\rho_1(y, M) := G \cdot y \oplus M$ and $\rho(y, M) = (\rho_1(y, M), y \oplus M)$

- $G : (y_1, y_2, y_3, y_4) \rightarrow (y_2, y_3, y_4, y_4 \oplus y_1)$

$$G_{n \times n} = \begin{pmatrix}
0 & 1 & 0 & 0 \\
0 & 0 & 1 & 0 \\
0 & 0 & 0 & 1 \\
1 & 0 & 0 & 1
\end{pmatrix}$$
Introduction

Idealized Combined Feedback Construction: iCOFB

Specification for COFB

Underlying Mathematical Components for COFB

Security Bounds

Properties

Hardware Implementation Results of COFB

Conclusion
Security Level for COFB

Security Bounds for privacy

- Birthday Bound
- 64-bit for Privacy

Security Bounds for Authenticity

- Birthday Bound
- 64-bit for Authenticity
1. Introduction

2. Idealized Combined Feedback Construction: iCOFB

3. Specification for COFB
   - Underlying Mathematical Components for COFB
   - Security Bounds
   - Properties

4. Hardware Implementation Results of COFB

5. Conclusion
## 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*
1 Introduction

2 Idealized Combined Feedback Construction : iCOFB

3 Specification for COFB

4 Hardware Implementation Results of COFB

5 Conclusion
COFB-Base Architecture

[Diagram showing the COFB-Base Architecture with labels for AD/M, State, Key, AES_r, chop, ρ, tweak, Δ, T, C, and notation for 0^64||N, 128, 64, and other values as indicated in the diagram.]
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* interface to be done in future
1. Introduction

2. Idealized Combined Feedback Construction: iCOFB

3. Specification for COFB

4. Hardware Implementation Results of COFB

5. 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