Authenticated – Encryption in Hardware

Milind M. Parelkar
Cryptographic Security Services

Confidentiality

Non-Repudiation

Authentication

Integrity
Confidentiality

Alice --X-- Charlie -- > Bob

Message Integrity

Alice            --X-- Charlie    -- > Bob
Authentication

Alice

Bob

Charlie
What is Authenticated – Encryption?

- Integration of Authentication and Encryption into a single algorithm

- Possible Advantages –
  - Reduction in Implementation Area → Cost
  - Reduced Power Consumption
  - Single Key for both services
  - Improved Efficiency (Better Throughput/Area Ratio)
Encryption Options

- Confidentiality – Only Modes of Operation of Block Ciphers
  - Electronic Code Book (ECB)
  - Cipher Block Chaining (CBC)
  - Counter (CTR)
  - Cipher Feed Back (CFB)
  - Output Feed Back (OFB)

- Stream Ciphers
Confidentiality-Only Modes of Operation

ECB

CBC
Authentication Options

- Message Authentication Codes (MACs)
  - Block Cipher Based
  - Hash Function Based
  - Stream Cipher Based
  - Dedicated
Block Cipher Based MACs

Cipher Block Chaining – Message Authentication Code (CBC-MAC)
Hash Functions and MACs

Hash Function

MAC
Authenticated – Encryption Options

- **Traditional**
  - Separate Encryption and Authentication Algorithm
  - Also known as Generic Composition Schemes
  - Example: In IPSec
    - Encryption: AES-CBC
    - Authentication: HMAC SHA-1
  - **Drawback:** Separate keys required for encryption and authentication

- **Modern**
  - Authenticated-Encryption Mode of Operation
  - Example: In IEEE 802.11i
    - Counter with CBC-MAC (CCM)
  - Other Modes of Operations:
    - Offset Code Book (OCB)
    - Encrypt then Authenticate then X(trans)late (EAX)
    - Integrity Aware Parallelizable Mode (IAPM)
    - Galois/Counter Mode (GCM)
Authenticated – Encryption Modes

- Single Pass Schemes
  - ✗ AE Schemes
  - ✓ Encrypt and Authenticate in One Pass
  - ✓ Fast – about $n$ block cipher calls for $n$ data blocks
  - ✗ Patented

- Two Pass Schemes
  - ✓ AEAD Schemes
  - ✗ Separate Pass for Encryption and Authentication
  - ✗ ~2x slower than single-pass schemes in software
  - ✓ Free for use

- e.g. OCB, IAPM
- e.g. CCM, EAX
Target Applications for New Modes

- FPGA Bitstream Security
- Secure Communication in Wireless Networks
FPGA Bitstream Security

Remote Re-configurable FPGA

- Configuration Controller
- Configurable Logic Blocks (CLBs)
- I/O Blocks (IOBs)

Module 1
Module 2
Module 3

Unsecured Network

✓ Stealing the Bitstream
✓ Fabricating Malicious Bitstream
Encrypting the FPGA Bitstream

Xilinx Virtex II Pro – 3DES
Xilinx Virtex 4 – AES-256

Cannot easily steal the Bitstream IP
✓ Can still Fabricate Malicious Bitstream

Remotely Re-configurable FPGA

Decryption Engine

Configuration Controller
Encrypting and Authenticating the FPGA Bitstream

- CRC-32 - Detecting Transmission Errors
  - No Provably Secure Authentication Engine

- Cannot easily steal the Bitstream
- Cannot configure an FPGA with Fabricated Malicious Bitstream

Decryption Engine
Authentication Checking Engine

Configuration Controller
Application Requirements

- Maximum FPGA Configuration Throughput – 152 Mbps (SelectMAP Interface)
- Cryptographic Unit should have a small footprint

Smallest Area Implementation supporting ~150 Mbps
Authenticated – Encryption in Wireless Networks

- Current and Projected Throughput
  - 802.11b – 11 Mbps
  - 802.11g – 54 Mbps
  - 802.11n – 100 + Mbps (Projected)

Smallest Area Implementation supporting ~150-200 Mbps
Scope of Research (1)

- Implemented 3 authenticated – encryption modes of operation:
  - OCB
  - CCM
  - EAX

  Modes of Operation based on 3 underlying block ciphers designed by Pawel Chodowiec, from the same research group
  - AES (Rijndael)
  - Twofish
  - Serpent

- Implemented 2 generic composition schemes:
  - AES+HMAC SHA-1
  - AES+HMAC SHA-512
Scope of Research (2)

- Target Technology:
  - Xilinx Virtex 4 FPGA
    - Part No.: xc4vlx60 ff 1148 -11
  - 90 nm and 130 nm ASICs
    - Based on TSMC library
Top-Level View

AES, Twofish or Serpent

OCB, CCM, EAX or any combination
Assumptions, Limitations etc. (1)

- **Wrapper Related**
  - Pre-processing assumed to be done externally
    - Length Calculation etc.
  - Padding of partially filled blocks assumed to be done externally
  - Single Block Cipher instantiation for Modes of Operation
Assumptions, Limitations etc. (2)

- Block Cipher Related
  - Limited use of Block Cipher Pipeline
    - Only 1 block allowed in the pipeline at a time
    - Emulates basic iterative architecture
    - Pipelined to meet a certain clock frequency
  - Both encryption and decryption functionality
FPGA Design Flow

Design Entry → Functional Simulation

FPGA Synthesis

Netlist without accurate Routing Delays → Post Synthesis Simulation

FPGA Implementation

Netlist with Timing Information

Timing Simulation

Timing Analysis

Active HDL

Synplify Pro

Xilinx ISE

Static Timing Analyzer
ASIC Design Flow

1. Design Entry
2. Define design environment
3. Set design constraints
4. Compile design
5. Analyze Area and Timing Reports
6. Save design database
Traditional Authentication Schemes
HMAC

Derive $K_0$ from $K$

$K_0 \oplus \text{ipad}$

$K_0 \oplus \text{ipad}$

$H((K_0 \oplus \text{ipad}) \| \text{text})$

$K_0 \oplus \text{opad}$

$K_0 \oplus \text{opad}$

$H((K_0 \oplus \text{ipad}) \| \text{text})$

$H((K_0 \oplus \text{opad}) \| H((K_0 \oplus \text{ipad}) \| \text{text}))$

Select leftmost $t$ bytes of $H((K_0 \oplus \text{opad}) \| H((K_0 \oplus \text{ipad}) \| \text{text}))$

Message

Hash Function

Hash Function

MAC
Hash Function – SHA-1

Input Message

\( f_1, K, W[0...19] \)
20 steps

\( f_2, K, W[20...39] \)
20 steps

\( f_3, K, W[40...59] \)
20 steps

\( f_4, K, W[60...79] \)
20 steps

\( CV_{Q+1} \)
OCB
Mode of Operation
OCB Encryption and Tag Generation

For $m$ Message Blocks, $m+3$ block cipher calls
$\approx m$, if $m$ is large
OCB Decryption and Tag Verification

Encryption and Decryption Functions of the Block Cipher are Required
OCB Datapath
CCM
Mode of Operation
CCM Mode of Operation

- **Discard**: No Decryption Function Required
- **Ciphertext**
- **No Decryption Function Required**
# CCM – AEAD Scheme

<table>
<thead>
<tr>
<th>Block Type</th>
<th>Notation</th>
<th>Encrypt</th>
<th>Authenticate</th>
</tr>
</thead>
<tbody>
<tr>
<td>Initialization Block</td>
<td>B[0]</td>
<td>✗</td>
<td>✓</td>
</tr>
<tr>
<td>Associated Data (AD)</td>
<td>B[i]</td>
<td>✗</td>
<td>✓</td>
</tr>
<tr>
<td>Payload</td>
<td>P[i]</td>
<td>✓</td>
<td>✓</td>
</tr>
</tbody>
</table>

![Diagram showing the structure of CCM blocks](image.png)
CCM Datapath
EAX
Mode of Operation
EAX Encryption and Tag Generation

Encrypt

then

Authenticate
OMAC: One-Keyed MAC

Completely Filled Last Block

Partially Filled Last Block
EAX Decryption and Tag Verification

Verify then Decrypt

Authentication failed
Discard ciphertext

Authentication successful
Decrypt ciphertext using CTR mode with N as IV
EAX Datapath
Analysis of Results
Criteria for Comparison of Results

- Implementation Area
  - CLB Slices for FPGAs
  - Cell Area in Sq. Microns for ASICs
- Throughput
- Throughput/Area Ratio
Throughput for Modes of Operation

Factors affecting Throughput

- Size of the Message \((L)\) blocks
- Wrapper Related
  - Block Cipher Calls \((n_{\text{cipher\_calls}})\)
  - Clock Period \((t_p)\)
- Block Cipher Core Related
  - Number of Rounds \((n_{\text{rounds}})\)
  - Number of Pipeline Stages \((n_{\text{pipeline\_stages}})\)
  - Number of Blocks allowed in the pipeline \((n_{\text{allowed\_blocks}})\)

\[
\text{Throughput} = \frac{128 \times L}{n_{\text{cipher\_calls}} \times n_{\text{rounds}} \times n_{\text{pipeline\_stages}} \times t_p} \times n_{\text{allowed\_blocks}}
\]
Throughput for Modes of Operation

- Wrapper Related Parameters

<table>
<thead>
<tr>
<th></th>
<th>OCB</th>
<th>CCM</th>
<th>EAX</th>
</tr>
</thead>
<tbody>
<tr>
<td>( n_{\text{cipher calls}} )</td>
<td>L+3</td>
<td>2L+2+A</td>
<td>2L+H+3</td>
</tr>
<tr>
<td>( n_{\text{cipher calls for large messages}} )</td>
<td>L</td>
<td>2L</td>
<td>2L</td>
</tr>
</tbody>
</table>

L: Number of Blocks of Message
A, H: Number of Blocks of Associated Data
Throughput for Modes of Operation

- Block Cipher Related Parameters

<table>
<thead>
<tr>
<th></th>
<th>AES – 128</th>
<th>AES – 192</th>
<th>AES – 256</th>
<th>Twofish</th>
<th>Serpent</th>
</tr>
</thead>
<tbody>
<tr>
<td>n_rounds</td>
<td>11</td>
<td>13</td>
<td>15</td>
<td>16</td>
<td>16</td>
</tr>
<tr>
<td>n_pipeline_stages</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>8</td>
<td>2</td>
</tr>
</tbody>
</table>

Number of blocks allowed to be present in the pipeline at any time \( (n\_{\text{allowed\_blocks}}) = 1 \)
FPGA Throughput Comparison

Throughput (Mbps)

Required Throughput

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Throughput (Mbps)</th>
</tr>
</thead>
<tbody>
<tr>
<td>ECB</td>
<td>708</td>
</tr>
<tr>
<td>OCB</td>
<td>601</td>
</tr>
<tr>
<td>AES</td>
<td>255</td>
</tr>
<tr>
<td>AES + HMAC SHA-1</td>
<td>542</td>
</tr>
<tr>
<td>AES + HMAC SHA-512</td>
<td>708</td>
</tr>
</tbody>
</table>
FPGA Resource Utilization

<table>
<thead>
<tr>
<th>Mode</th>
<th>CLB Slices</th>
</tr>
</thead>
<tbody>
<tr>
<td>ECB</td>
<td>1188</td>
</tr>
<tr>
<td>OCB</td>
<td>2964</td>
</tr>
<tr>
<td>AES</td>
<td>2993</td>
</tr>
<tr>
<td>AES + HMAC SHA-1</td>
<td>3076</td>
</tr>
<tr>
<td>AES + HMAC SHA-512</td>
<td>4246</td>
</tr>
</tbody>
</table>

Legend:
- ECB
- OCB
- CCM
- EAX
- AES + HMAC SHA-1
- AES + HMAC SHA-512
FPGA Throughput/Area Ratio

Throughput/Area (Mbps/CLB Slice)

- ECB: 0.60
- OCB: 0.20
- AES: 0.09
- CCM: 0.10
- EAX: 0.18
- AES + HMAC SHA-1: 0.17
- AES + HMAC SHA-512: 0.18
### FPGA Throughput Comparison

The throughput can be calculated using the formula:

$$\text{Throughput} = \frac{128 \times L}{n_{\text{cipher\_calls}} \times n_{\text{rounds}} \times n_{\text{pipeline\_stages}} \times t_p}$$

<table>
<thead>
<tr>
<th>Cipher Mode</th>
<th>AES-128</th>
<th>AES-192</th>
<th>AES-256</th>
<th>Twofish</th>
<th>Serpent</th>
</tr>
</thead>
<tbody>
<tr>
<td>ECB</td>
<td>708</td>
<td>601</td>
<td>599</td>
<td>508</td>
<td>519</td>
</tr>
<tr>
<td>OCB</td>
<td>255</td>
<td>287</td>
<td>215</td>
<td>243</td>
<td>186</td>
</tr>
<tr>
<td>CCM</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>EAX</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Required Throughput**

- ECB: 8 Mbps
- OCB: 16 Mbps
- CCM: 8 Mbps
- EAX: 16 Mbps

The throughput values for each cipher mode and key size are shown in the chart.
ASIC Throughput Comparison (90 nm)

Throughput (Mbps)

- ECB: 1097 Mbps
- OCB: 854 Mbps
- CCM: 434 Mbps
- EAX: 421 Mbps
- AES + HMAC SHA-1: 842 Mbps
- AES + HMAC SHA-512: 1097 Mbps

Required Throughput

Throughput (Mbps) Scale:
- 0
- 200
- 400
- 600
- 800
- 1000
- 1200
ASIC Throughput Comparison (130 nm)

Throughput (Mbps)

- ECB: 765 Mbps
- OCB: 717 Mbps
- CCM: 338 Mbps
- EAX: 350 Mbps
- AES + HMAC SHA-1: 765 Mbps
- AES + HMAC SHA-512: 765 Mbps

Required Throughput
ASIC Resource Utilization (90 nm)

<table>
<thead>
<tr>
<th>Method</th>
<th>Total Cell Area (Sq. Microns)</th>
</tr>
</thead>
<tbody>
<tr>
<td>ECB</td>
<td>41,250</td>
</tr>
<tr>
<td>OCB</td>
<td>63,585</td>
</tr>
<tr>
<td>AES</td>
<td>56,541</td>
</tr>
<tr>
<td>CCM</td>
<td>62,889</td>
</tr>
<tr>
<td>EAX</td>
<td>114,676</td>
</tr>
<tr>
<td>AES + HMAC SHA-1</td>
<td>182,514</td>
</tr>
<tr>
<td>AES + HMAC SHA-512</td>
<td></td>
</tr>
</tbody>
</table>
ASIC Resource Utilization (130 nm)

<table>
<thead>
<tr>
<th>Algorithm</th>
<th>Total Cell Area (Sq. Microns)</th>
</tr>
</thead>
<tbody>
<tr>
<td>ECB</td>
<td>79,293</td>
</tr>
<tr>
<td>OCB</td>
<td>114,232</td>
</tr>
<tr>
<td>CCM</td>
<td>111,386</td>
</tr>
<tr>
<td>EAX</td>
<td>112,968</td>
</tr>
<tr>
<td>AES + HMAC SHA-1</td>
<td>228,924</td>
</tr>
<tr>
<td>AES + HMAC SHA-512</td>
<td>377,065</td>
</tr>
</tbody>
</table>
Possible Improvements

- Improvement in Throughput
- Reduction of Implementation Area
Throughput Improvement

\[
\text{Throughput} = \frac{128 \times L}{n_{\text{cipher \_ calls}} \times n_{\text{rounds}} \times n_{\text{pipeline \_ stages}} \times t_p} \times n_{\text{allowed \_ blocks}}
\]

- **Under-Utilized Pipeline**
  - \((n_{\text{allowed \_ blocks}} / n_{\text{pipeline \_ stages}}) < 1\)
  - Throughput reduces by a factor of under-utilization

- **Under-utilization Factor:**
  - AES, Serpent = 1/2
  - Twofish = 1/8
Optimal Number of Pipeline Stages

- OCB
  - $m$ blocks can be processed in parallel
  - $m$ stage pipeline can be fully utilized

Ref: P. Chodowiec, "Comparison of Hardware Performance of AES Candidates using Reconfigurable Hardware", Master’s Thesis, George Mason University, 2002
Optimal Number of Pipeline Stages

- CCM, EAX
  - Interleaved CTR, CBC
  - Max. 2 blocks processed in parallel
  - More than 2 stage pipeline would be under-utilized
Projected Throughput Increase

Projected Throughput Increase for $n_{\text{allowed\_blocks}} = n_{\text{pipeline\_stages}}$

- **OCB**
- **CCM, EAX**

**Factor of Increase in Throughput**

**Number of Pipeline Stages**
Reduction in Circuit Area

- Sacrificing Performance
- Resource Sharing
- Using Specially Designed Properties of Modes of Operations
  - CCM, EAX
    - Only encryption function of block cipher is required
- Preprocessing (e.g. CCM Implementation)
  - Padding
  - Length Calculation
Conclusion
Conclusion

- FPGA Bitstream Security
  - Decryption – Verification Engine on FPGA Fabric → ASIC Synthesis Results
  - All schemes support more than 150 Mbps
  - CCM has smallest area
  - CCM is standardized

AES-CCM
Conclusion

- Secure Communication in Wireless Networks
  - Both FPGAs and ASICs
    - All modes meet throughput requirements
    - CCM has smallest area
    - Projected Throughput Increase for CCM \(~2x~\)
    - Part of IEEE 802.11i standard for wireless networks

AES-CCM
Conclusion

- Secure Communication in High Speed Networks
  - FPGA Based Platforms
    - AES-OCB or AES + HMAC SHA-512
  - Almost no scope for throughput improvement with HMAC
  - AES-OCB
    - More than 2 Gbps with 4 stage pipeline

AES-OCB
Conclusion

- Secure Communication in High Speed Networks
  - ASIC Platforms
    - AES-OCB
  - Highest Throughput/Area Ratio

- Potential Problem
  - Patent Restrictions
    - CCM is the next best

AES-OCB       AES-CCM