Design of AES Based on Dual Cipher and Composite Field

S.Y. Wu, S.C. Lu, and C.S. Laih

Cryptographer’s Track at RSA Conference
Department of Electrical Engineering
National Cheng Kung University
Feb/27/2004
Content

- 1. Introduction
- 2. Motivation and Main Result
- 3. The Dual Cipher (Dual AES)
- 4. How to Construct the Dual AES
- 5. The Dual AES over Composite Field
- 6. Design of the AES from the Dual AES and GF((2^4)^2)
- 7. Implementation of the AES
- 8. Complexity Analysis
- 9. Conclusion
1. Introduction

- AES is a block cipher.
  - ShiftRows, SubBytes, MixColumn and AddRoundKey.
  - AES hardware is implemented with ASIC or FPGA.
- AES is defined over finite field GF(2) and GF(2^8).
  - GF(2): Addition.
  - GF(2^8): Multiplication and inversion.
  - Recently, AES applied over GF((2^4)^2) is discussed.
- Barkan & Biham proposed the concept of the dual ciphers of AES. [AC 2002 p.160-175]
  - Dual ciphers: \{E, E^2, E^4, E^8, E^{16}, E^{32}, E^{64}, E^{128}\}.
2. Motivation and Main Result

- We generalize the dual AES cipher and find a better hardware implementation method with combination of the dual AES ciphers and composite field $GF((2^4)^2)$.
  - Chip area: is reduced by $1/6$.
  - Chip delay: is reduced by $1/4$.
  - (Compared to [CT-RSA2002 p.67-78])
3. The Dual Cipher (1)

- The generalization of the dual AES:

  - Irreducible polynomial \((11B)_x\) with generator \((03)_x\)
  - Generalized Representation
  - Irreducible polynomial \(R(x)\) with generator \(\beta\)
  - AES
  - Transformation will exist between dual AES and AES
  - Dual AES
3. The Dual Cipher (2)

- The **power form** representation in $\text{GF}(2^8)$ with **generator** $\beta = 03$ and the irreducible poly. $p(x) = x^8 + x^4 + x^3 + x + 1$:

$$
\begin{array}{cccc}
00 & 04 & 08 & 0C \\
01 & 05 & 09 & 0D \\
02 & 06 & 0A & 0E \\
03 & 07 & 0B & 0F \\
\end{array}
$$

$\beta$ is chosen as a primitive element in $\text{GF}(2^8)$. 
3. The Dual Cipher (3)  
-- Power Form

- Let generator $\beta = \{03\}_x$, then the elements in the GF($2^8$) field can be presented as power form of $\beta$:
  $$\{00, 01, 02, \ldots, FF\} \rightarrow \{0, 1, \beta, \beta^2, \ldots, \beta^{254}\}$$

- For examples:
  
  - $\{00\}_x$ ($= \{00000000\}_2$) $\rightarrow 0$
  - $\{01\}_x$ ($= \{00000001\}_2$) $\rightarrow \beta^0$
  - $\{03\}_x$ ($= \{00000011\}_2$) $\rightarrow \beta^1$
  - $\{05\}_x$ ($= \{00000101\}_2$) $\rightarrow \beta^2$
  - $\{0F\}_x$ ($= \{00001111\}_2$) $\rightarrow \beta^3$
  
  ......
3. The Dual Cipher (4)  
-- General Representation

- So, we can represent the AES over GF(2^8) as
  \{GF(2^8), \{11B\}_x, \{03\}_x\}
  - Irreducible poly. \(p(x)=x^8+x^4+x^3+x+1\), means \{11B\}_x.
  - Generator: 03.

- We can select another irreducible poly. and the generator to generate the dual AES: \{GF(2^8), \{11D\}_x, \{02\}_x\}
  - Irreducible poly. \(p(x)=x^8+x^4+x^3+x^2+1\), means \{11D\}_x.
  - Generator: 02(hex).
3. The Dual Cipher (5)
-- Relation between the AES and the dual AES

- The AES and the dual AES are isomorphic. $T$ is the transfer function.
4. How to Construct the Dual AES -- Setup Procedures (1)

- 1. Transfer the states of the AES from hex to power form of the generator \( \{03\}_x \) with the poly. \( \{11B\}_x \).
- 2. Select an irreducible poly. and select a new generator.
  - Use the new generator to generate the dual AES with the same power order of the origin AES.
- 3. Build the matrix to map from GF\( (2^8) \) to GF\( (2^4)^2 \):
  - AES:\( \{1,2,4,8,10,20,40,80\}_x \) → power form of generator → dual AES: \( \{\ldots\}_x \) → column of the matrix
4. How to Construct the Dual AES
-- Setup Procedures (2)

- AES: generator \( \{03\}_x \) with poly. \( \{11B\}_x \).
- Dual AES: generator \( \{02\}_x \) with poly. \( \{11D\}_x \).
- Matrix \( T = [ \beta^0, \beta^{25}, \beta^{50}, \beta^{75}, \beta^{100}, \beta^{125}, \beta^{150}, \beta^{175} ] \)

\[
T = \begin{bmatrix}
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\
0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\
0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \\
0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\
0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \\
0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\
\end{bmatrix}
\]

\[
T^{-1} = \begin{bmatrix}
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\
0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\
0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \\
0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\
0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \\
0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\
\end{bmatrix}
\]
5. The Dual AES over Composite Field (1)

\[ PT, MT, T(K), MT(K), GF(2^8), GF((2^4)^2) \]
5. The Dual AES over Composite Field (2)

- AES is defined over $\text{GF}(2^8)$.
  - Inversion is hard to calculate.
- AES defined over $\text{GF}((2^4)^2)$ is practical.
  - Inversion is easy to calculate.
- Dual AES over $\text{GF}((2^4)^2)$ is also practical.
- $M$: Mapping matrix from $\text{GF}(2^8)$ to $\text{GF}((2^4)^2)$.
- $M^{-1}$: Mapping matrix from $\text{GF}((2^4)^2)$ to $\text{GF}(2^8)$. 
5. The Dual AES over Composite Field (3)

- Build the matrix $M$ with the same procedures as stated above.
- Mapping matrix $M$ from $\text{GF}(2^8)$ to $\text{GF}((2^4)^2)$ with
  - $\text{GF}((2^4)^2) : Q(y)=y^4+y+1$
  - $\text{GF}((2^4)^2) : R(z)= z^2+z+\{09\}_x$

$$
M = \begin{bmatrix}
1 & 1 & 0 & 1 & 0 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 \\
0 & 1 & 0 & 1 & 1 & 0 & 0 & 1 \\
0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 \\
0 & 1 & 0 & 1 & 1 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 \\
0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\
\end{bmatrix}
$$

$$
M^{-1} = \begin{bmatrix}
1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 \\
0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 \\
0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 \\
0 & 0 & 1 & 0 & 1 & 1 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\
0 & 1 & 0 & 1 & 0 & 0 & 1 & 1 \\
0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \\
\end{bmatrix}
$$
5. The Dual AES over Composite Field (4)

SubBytes

\[
a_{i,j} \xrightarrow{\text{Inverse}} a_{i,j}^{-1} \xrightarrow{\text{Affine}} b_{i,j}
\]

\[
a_{i,j} * a_{i,j}^{-1} \equiv 1 \mod m(x) \text{ where } m(x) = x^8 + x^4 + x^3 + x + 1
\]

\[
b_{i,j} = C a_{i,j}^{-1}
\]
5. The Dual AES over Composite Field (5)

- The most complicated operation in AES is the calculation of the byte-inversion in GF(2^8).
- Transfer a byte from GF(2^8) to GF((2^4)^2):

\[
a = a_h z + a_l
\]

where \(a \in GF(2^8), a_h, a_l \in GF(2^4)\)

The inverse of \(a\) is:

\[
a^{-1} = (a_h z + a_l)^{-1}
\]

\[
= a_h (Aa_h^2 \oplus a_h a_l \oplus a_l^2)^{-1} z + (a_l \oplus a_h)(Aa_h^2 \oplus a_h a_l \oplus a_l^2)^{-1}
\]
5. The Dual AES over Composite Field (6)

- \( a_h = (a_{h3}, a_{h2}, a_{h1}, a_{h0}) \),
  - \( a_{h0} = (a_4 \oplus a_7) \)
  - \( a_{h1} = (a_1 \oplus a_3) \oplus a_4 \)
  - \( a_{h2} = (a_2 \oplus a_5) \oplus a_6 \)
  - \( a_{h3} = a_5 \)

- \( a_l = (a_{l3}, a_{l2}, a_{l1}, a_{l0}) \),
  - \( a_{l0} = a_0 \oplus (a_1 \oplus a_3) \)
  - \( a_{l1} = (a_1 \oplus a_5) \)
  - \( a_{l2} = (a_1 \oplus a_3) \oplus (a_4 \oplus a_7) \)
  - \( a_{l3} = a_1 \oplus (a_2 \oplus a_5) \)
6. Design of the AES from the Dual AES and GF((2^4)^2) -- Architecture of SubByte (1)

Computing in Dual AES field
GF(2^8) with \( R(x) = \sum_{i=0}^{7} a_i x^i \)

Computing in Composite Field
GF((2^4)^2) with \( f(x) = x^2 + x + a \)
GF(2^4) with \( Q(y) = y^4 + y + 1 \)

Computing in Dual AES field
GF(2^8) with \( R(x) = \sum_{i=0}^{7} a_i x^i \)
6. Design of the AES from the Dual AES and GF((2^4)^2) -- Architecture of SubByte (2)
6. Design of the AES from the Dual AES and GF((2^4)^2)
-- Merging the Other Components
7. Implementation of the AES (1)

-- Architecture of AES

- Architecture of AES:
  - Iterative circuit
    - Components for one round only.
    - Advantage: chip area small.
    - Disadvantage: 10 clocks for each encryption.
  - Pipelining circuit
    - Components for 10 rounds needed.
    - Advantage: 1 clocks for each encryption.
    - Disadvantage: chip area large.
7. Implementation of the AES (2)

--Design Environment

- Language: Verilog-HDL
- Design library: 0.35 µm CMOS
- Logic synthesis: Synopsys
7. Implementation of the AES (3)  
-- Complexity of the SubByte Design

- Compared with other's study: [Wolkerstorfer, CT-RSA’02]
  Our best design: XOR gates counts reduced 17%, critical path of encryption reduced 28%, critical path of decryption reduced 18%.

<table>
<thead>
<tr>
<th></th>
<th>( C_S(#\text{XOR}) )</th>
<th>( C_S(\tau_{\text{XOR}}) )</th>
<th>Max Delay (Encryption)</th>
<th>Max Delay (Decryption)</th>
<th>Sum of XOR gates</th>
</tr>
</thead>
<tbody>
<tr>
<td>Our Design</td>
<td>38</td>
<td>5/6</td>
<td>13</td>
<td>14</td>
<td>102</td>
</tr>
<tr>
<td>Wolkerstorfer et al</td>
<td>59</td>
<td>10/9</td>
<td>18</td>
<td>17</td>
<td>123</td>
</tr>
</tbody>
</table>

(SubBytes only)
7. Implementation of the AES (4)
-- Result of the SubByte Design

- Compare with the design of Look-up table:
  Our best design: ATP (AreaTimeProduct) 3/5 only

<table>
<thead>
<tr>
<th>Design</th>
<th>Area (gates)</th>
<th>Delay (ns)</th>
<th>Max. Freq. (Mbps)</th>
<th>AT (gates×ns)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Design</td>
<td>331.92 (25.05%)</td>
<td>10.37 (236.22%)</td>
<td>96.43 (41.18%)</td>
<td>3442 (59.18%)</td>
</tr>
<tr>
<td>Wolkerstorfer et al's</td>
<td>406 (30.64%)</td>
<td>14.2 (323.46%)</td>
<td>70 (29.89%)</td>
<td>5765 (99.12%)</td>
</tr>
<tr>
<td>Look-up table</td>
<td>1324.86 (100%)</td>
<td>4.39 (100%)</td>
<td>234.19 (100%)</td>
<td>5816 (100%)</td>
</tr>
</tbody>
</table>

Look-up table: inversion design with ROM
8. Complexity Analysis

- **Iterative Circuit**: Chip area increased slightly, the critical path of encryption decreased much.
- **Pipeline Circuit**: Chip area and the critical path of encryption decreased.

<table>
<thead>
<tr>
<th></th>
<th>Design</th>
<th>Wolkerstorfer</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Iterative Circuit</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>C(#XOR)</td>
<td>1168</td>
<td>944</td>
</tr>
<tr>
<td>C(t_XOR)(E)</td>
<td>50</td>
<td>100</td>
</tr>
<tr>
<td>C(t_XOR)(D)</td>
<td>60</td>
<td>90</td>
</tr>
<tr>
<td><strong>Pipelining Circuit</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>C(#XOR)</td>
<td>6496</td>
<td>9440</td>
</tr>
<tr>
<td>C(t_XOR)(E)</td>
<td>5</td>
<td>10</td>
</tr>
<tr>
<td>C(t_XOR)(D)</td>
<td>6</td>
<td>9</td>
</tr>
<tr>
<td><strong>Using Dual AES or not</strong></td>
<td>(11D)_x, (02)_x</td>
<td>No</td>
</tr>
<tr>
<td><strong>Using Improved Architecture</strong></td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>

Design of the AES cipher, except the key expansion.
9. Conclusion

- The dual AES is a new concept in the AES study. It may open new direction for the AES in the basic theory study and new method of implementation.