On the Lightweight Design Choices for Diffusion Layer of Block Ciphers

SUMANTA SARKAR

TCS Innovation Labs

December 11, 2017
- Internet of things (IoT): Network of smart devices.
- Examples: cyberphysical systems: health monitoring, environmental monitoring, supply chain
  Smart cities: citizens, traffic systems, social system, waste management, etc all connected for better usage of resources.
- Connected car: core to driverless cars. (California clears the way for testing of fully driverless cars)
Jeep Cherokee Hacked in July 2015. Sitting 10 miles away hackers took the control from the driver.
Jeep Cherokee Hacked in July 2015. Sitting 10 miles away hackers took the control from the driver.

picture source: amazon.in
Threats!

- Jeep Cherokee Hacked in July 2015. Sitting 10 miles away hackers took the control from the driver.

- Alexa accidentally ordered dollhouse for many houses (January 2017).
- Phillips Hue smart bulbs were shown to be hackable.

Picture source: amazon.in
Why Lightweight Cryptography?

- IoT network is comprised of RFID/Sensors.
- AES or RSA: popular choices of encryption in practice.
Why Lightweight Cryptography?

- IoT network is comprised of RFID/Sensors.
- AES or RSA: popular choices of encryption in practice.
- For secure communication in IoT, we cannot employ AES, we need “lightweight” encryption/decryption algorithm.
Why Lightweight Cryptography?

IoT network is comprised of RFID/Sensors.

AES or RSA: popular choices of encryption in practice.

For secure communication in IoT, we cannot employ AES, we need “lightweight” encryption/decryption algorithm.

NIST is in the process of lightweight standardisation.
Lightweight cryptography mostly based on symmetric key.

- Lightweight stream ciphers: eSTREAM finalists Grain v1, MICKEY 2.0, and Trivium, etc.

- Lightweight block ciphers: CLEFIA, PRESENT: Standardized by ISO/IEC 29192, etc.
• Lightweight cryptosystem: How to measure the “weight”?
• (Silicon) Area, Performance and power consumption
Lightweight cryptosystem: How to measure the “weight”?

(Silicon) Area, Performance and power consumption

Area measured by number of Gate Equivalent (GE)
Block cipher LED 64 bit \( \Rightarrow \) GE \( = 966 \) (\( .18\mu m \)).

Performance: Throughput.

Consult Cryptolux/Lightweight Cryptography for the list of lightweight ciphers.
A block cipher has two building blocks:

- Confusion layer makes the relation between key and ciphertext as complex as possible.
- Diffusion spreads the plaintext statistics throughout the ciphertext.
A block cipher has two building blocks: Confusion & Diffusion.

- Confusion layer makes the relation between key and ciphertext as complex as possible.
- Diffusion spreads the plaintext statistics throughout the ciphertext.
Metric for Diffusion Layer

- $F : \mathbb{F}_q^n \rightarrow \mathbb{F}_q^n$: Differential Branch Number of $F$:
  \[
  \min\{\text{wt}(x + y) + \text{wt}(F(x) + F(y))\}.
  \]
- Differential Branch Number of $F \leq n + 1$
- Diffusion layer: multiplication of a vector with a matrix (over $GF(2^n)$).
- **Maximum Distance Separable (MDS)** matrix is chosen for Diffusion: Highest diffusion power $n+1$.
- **MDS matrix**: square matrix whose every submatrix is nonsingular.
Diffusion layer: multiplication of a vector with a matrix (over $GF(2^n)$).

**Maximum Distance Separable (MDS)** matrix is chosen for Diffusion: Highest diffusion power $n+1$.

*MDS matrix*: square matrix whose every submatrix is nonsingular.

In practice, product of two field elements is implemented simply by some XORs.

[Khoo et al. CHES 2014] looked at the number of XORs required to multiply a fixed field element by an arbitrary field element and termed it as

**XOR Count**
\( \beta \in \mathbb{GF}(2^n) \) is implemented by the corresponding vector \((\beta_0, \ldots, \beta_{n-1}) \in \mathbb{GF}(2)^n\) by choosing some basis of \(\mathbb{GF}(2^n)\).
• \( \beta \in \text{GF}(2^n) \) is implemented by the corresponding vector \((\beta_0, \ldots, \beta_{n-1}) \in \text{GF}(2)^n\) by choosing some basis of \(\text{GF}(2^n)\).

• Consider \(\text{GF}(2^3)\) under \((X^3 + X + 1)\) and a basis \(\{1, \alpha, \alpha^2\}\).

• How many XORs required to multiply \(\alpha^4\) with a general field element?
\( \beta \in \text{GF}(2^n) \) is implemented by the corresponding vector 
\((\beta_0, \ldots, \beta_{n-1}) \in \text{GF}(2)^n\) by choosing some basis of \(\text{GF}(2^n)\).

Consider \(\text{GF}(2^3)\) under \((X^3 + X + 1)\) and a basis \(\{1, \alpha, \alpha^2\}\).

How many XORs required to multiply \(\alpha^4\) with a general field element?

\(\alpha^4 = \alpha + \alpha^2 \rightarrow (0, 1, 1)\)

Take a general element \(b_0 + b_1 \alpha + b_2 \alpha^2 \in \text{GF}(2^3) \rightarrow (b_0, b_1, b_2)\).
• $\beta \in \mathbf{GF}(2^n)$ is implemented by the corresponding vector $(\beta_0, \ldots, \beta_{n-1}) \in \mathbf{GF}(2)^n$ by choosing some basis of $\mathbf{GF}(2^n)$.

• Consider $\mathbf{GF}(2^3)$ under $(X^3 + X + 1)$ and a basis $\{1, \alpha, \alpha^2\}$.

• How many XORs required to multiply $\alpha^4$ with a general field element?

• $\alpha^4 = \alpha + \alpha^2 \rightarrow (0, 1, 1)$

• Take a general element $b_0 + b_1 \alpha + b_2 \alpha^2 \in \mathbf{GF}(2^3) \rightarrow (b_0, b_1, b_2)$. Implement

  $(b_0, b_1, b_2)(0, 1, 1)$
• $\beta \in \mathbb{GF}(2^n)$ is implemented by the corresponding vector 
  $(\beta_0, \ldots, \beta_{n-1}) \in \mathbb{GF}(2)^n$ by choosing some basis of $\mathbb{GF}(2^n)$.

• Consider $\mathbb{GF}(2^3)$ under $(X^3 + X + 1)$ and a basis $\{1, \alpha, \alpha^2\}$.

• How many XORs required to multiply $\alpha^4$ with a general field element?

• $\alpha^4 = \alpha + \alpha^2 \rightarrow (0, 1, 1)$

• Take a general element $b_0 + b_1\alpha + b_2\alpha^2 \in \mathbb{GF}(2^3) \rightarrow (b_0, b_1, b_2)$.
  Implement

  $$(b_0, b_1, b_2)(0, 1, 1)$$

  $$(b_0 + b_1\alpha + b_2\alpha^2)\alpha^4 = (b_1 + b_2) + (b_0 + b_1)\alpha + (b_0 + b_1 + b_2)\alpha^2.$$ 

• In vector form this product is of the form $(b_1 \oplus b_2, b_0 \oplus b_1, b_0 \oplus b_1 \oplus b_2)$
\( \beta \in \mathbb{GF}(2^n) \) is implemented by the corresponding vector 
\((\beta_0, \ldots, \beta_{n-1}) \in \mathbb{GF}(2)^n \) by choosing some basis of \( \mathbb{GF}(2^n) \).

Consider \( \mathbb{GF}(2^3) \) under \( (X^3 + X + 1) \) and a basis \( \{1, \alpha, \alpha^2\} \).

How many XORs required to multiply \( \alpha^4 \) with a general field element?

\( \alpha^4 = \alpha + \alpha^2 \rightarrow (0, 1, 1) \)

Take a general element \( b_0 + b_1 \alpha + b_2 \alpha^2 \in \mathbb{GF}(2^3) \rightarrow (b_0, b_1, b_2) \).
Implement

\[(b_0, b_1, b_2)(0, 1, 1)\]

\[(b_0 + b_1 \alpha + b_2 \alpha^2)\alpha^4 = (b_1 + b_2) + (b_0 + b_1)\alpha + (b_0 + b_1 + b_2)\alpha^2.\]

In vector form this product is of the form \( (b_1 \oplus b_2, b_0 \oplus b_1, b_0 \oplus b_1 \oplus b_2) \)

\(XOR(\alpha^4) = 4.\)
XOR count of a matrix

- Challenge in lightweight block ciphers: Construct diffusion matrices with low XOR counts.
- Others (Kranz et al 17, JPS17]) considered re-usage of terms to decrease the number of XORs. But this costs delay and/or additional memory.
\( \alpha \) is a root of irreducible polynomial \( X^n + q(X) + 1 \), if there are \( t \) nonzero terms, then \( XOR(\alpha) = 1 \).

For example, \( \alpha \) is a root of \( X^4 + X + 1 \) that defines \( GF(2^4) \), then \( XOR(\alpha) = 1 \). But if we change the irreducible polynomial to \( X^4 + X^3 + X^2 + X + 1 \) then none of the elements of \( GF(2^4) \) has XOR count 1.
XOR count distribution also varies when a different basis of GF($2^n$) is considered, even if the underlying irreducible polynomial remains fixed.
XOR count distribution also varies when a different basis of GF\((2^n)\) is considered, even if the underlying irreducible polynomial remains fixed.

<table>
<thead>
<tr>
<th>Elements</th>
<th>0</th>
<th>1</th>
<th>(\alpha)</th>
<th>(\alpha^2)</th>
<th>(\alpha^3)</th>
<th>(\alpha^4)</th>
<th>(\alpha^5)</th>
<th>(\alpha^6)</th>
<th>Sum</th>
</tr>
</thead>
<tbody>
<tr>
<td>Basis ({1, \alpha, \alpha^2})</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>2</td>
<td>4</td>
<td>4</td>
<td>3</td>
<td>1</td>
<td>15</td>
</tr>
<tr>
<td>Basis ({\alpha^3, \alpha^6, \alpha^5})</td>
<td>0</td>
<td>0</td>
<td>3</td>
<td>3</td>
<td>2</td>
<td>3</td>
<td>2</td>
<td>2</td>
<td>15</td>
</tr>
</tbody>
</table>

XOR count distribution of GF\((2^3)\) under \(X^3 + X + 1\)
A matrix is called circulant if every row is a cyclic shift of other rows.

\[
T = \begin{bmatrix}
a_0 & a_1 & a_2 & a_3 \\
a_3 & a_0 & a_1 & a_2 \\
a_2 & a_3 & a_0 & a_1 \\
a_1 & a_2 & a_3 & a_0 \\
\end{bmatrix}.
\]
A matrix is called Toeplitz if every descending diagonal from left to right is constant.

A typical $4 \times 4$ Toeplitz matrix looks like

$$T = \begin{bmatrix}
a_0 & a_1 & a_2 & a_3 \\
a_{-1} & a_0 & a_1 & a_2 \\
a_{-2} & a_{-1} & a_0 & a_1 \\
a_{-3} & a_{-2} & a_{-1} & a_0
\end{bmatrix}.$$

A matrix $M$ is called involutory if $M \ast M = \text{Identity matrix}$. 
Let $T_1(x)$ be the following $4 \times 4$ Toeplitz matrix defined over $\mathbb{F}_{2^m}$:

$$T_1(x) = \begin{bmatrix}
    x & 1 & 1 & x^{-2} \\
    1 & x & 1 & 1 \\
    x^{-2} & 1 & x & 1 \\
    x^{-2} & x^{-2} & 1 & x
\end{bmatrix}.$$

If $x \in \mathbb{F}_{2^m}^*$ is such that the degree of its minimal polynomial over $\mathbb{F}_2$ is $\geq 5$, then $T_1(x)$ is MDS.
The Matrix $T_2$

Let $T_2(x)$ be the following $4 \times 4$ Toeplitz matrix defined over $\mathbb{F}_{2^m}$:

$$
T_2(x) = \begin{bmatrix}
1 & 1 & x & x^{-1} \\
x^{-2} & 1 & 1 & x \\
1 & x^{-2} & 1 & 1 \\
x^{-1} & 1 & x^{-2} & 1
\end{bmatrix}.
$$ (1)

If $x \in \mathbb{F}_{2^m}^*$ is such that

- the degree of the minimal polynomial of $x$ is $\geq 4$, and
- $x$ is not a root of the polynomial $X^6 + X^5 + X^4 + X + 1$,

then $T_2(x)$ is MDS.
For $GF(2^8)$, the family $T_2(x)$ of MDS matrixes contains matrix with XOR count $30$.

For $GF(2^8)$, the family $T_2(x)$ of MDS matrixes contains matrix with XOR count $27$. Earlier best known matrix was $32$.

For $GF(2^4)$, the family $T_2(x)$ of MDS matrixes contains matrix with XOR count $10$. Earlier best known matrix was $12$. 
For GF($2^8$), the lowest XOR count of a $4 \times 4$ MDS matrix is 27.

For GF($2^4$), the lowest XOR count of a $4 \times 4$ MDS matrix is 10.
Let $T$ be an $n \times n$ Toeplitz matrix defined over $GF(2^m)$. Then $T$ cannot be both MDS and involutory.
Suppose $N_1(x)$ is a $4 \times 4$ matrix over $\mathbb{F}_{2^m}$ such that

$$N_1(x) = \begin{bmatrix}
1 & x & 1 & x^2 + 1 \\
x & 1 & x^2 + 1 & 1 \\
x^{-2} & 1 + x^{-2} & 1 & x \\
1 + x^{-2} & x^{-2} & x & 1
\end{bmatrix}.$$  \hspace{1cm} (2)

Then $N_1(x)$ is an involutory matrix for all nonzero $x \in \mathbb{F}_{2^m}$, and if the degree of the minimal polynomial of $x$ over $\mathbb{F}_2$ is $\geq 4$, then $N_1(x)$ is also MDS.
Suppose $N_1(x)$ is a $4 \times 4$ matrix over $\mathbb{F}_{2^m}$ such that

$$N_1(x) = \begin{bmatrix}
1 & x & 1 & x^2 + 1 \\
x & 1 & x^2 + 1 & 1 \\
x^{-2} & 1 + x^{-2} & 1 & x \\
1 + x^{-2} & x^{-2} & x & 1
\end{bmatrix}.$$  \hspace{2cm} (2)

Then $N_1(x)$ is an involutory matrix for all nonzero $x \in \mathbb{F}_{2^m}$, and if the degree of the minimal polynomial of $x$ over $\mathbb{F}_2$ is $\geq 4$, then $N_1(x)$ is also MDS.

- For $GF(2^8)$, the minimum XOR count obtained in $N_1$ class is 64, this is matching with the known lowest bound (obtained through search).
Suppose $N_2(x)$ is a $4 \times 4$ matrix over $\mathbb{F}_{2^m}$ such that

$$N_2(x) = \begin{bmatrix}
1 & x^2 + 1 & x & 1 \\
x^2 + 1 & 1 & 1 & x \\
x^3 + x & x^2 + 1 & 1 & x^2 + 1 \\
x^2 + 1 & x^3 + x & x^2 + 1 & 1
\end{bmatrix}.$$  \hspace{1cm} (3)

Then $N_2(x)$ is an involutory matrix for all $x \in GF(2^m)$, and if the degree of the minimal polynomial of $x$ over $\mathbb{F}_2$ is $\geq 4$, then $N_2(x)$ is also MDS.

- For $GF(2^4)$, the minimum XOR count obtained for $N_2$ is 16.
- The best known was 24.
Toeplitz matrices have repeating submatrices [SS17].

\[
\begin{bmatrix}
a_0 & a_1 & a_2 & a_3 \\
a_{-1} & a_0 & a_1 & a_2 \\
a_{-2} & a_{-1} & a_0 & a_1 \\
a_3 & a_{-2} & a_{-1} & a_0
\end{bmatrix}
\]

The number of distinct $d \times d$ Toeplitz submatrices are

\[
\delta_{d,n} = \begin{cases} 
2n - 1 & \text{if } d = 1 \\
(n - d + \tau_{d,n} + 1) \cdot \left\lfloor \frac{n - 1}{d - 1} \right\rfloor & \text{if } d = 2, \ldots, n 
\end{cases}
\]

where $\tau_{d,n}$ is given by $n - 1 = \left\lfloor \frac{n - 1}{d - 1} \right\rfloor (d - 1) + \tau_{d,n}$. 
**Comparison of Number of Submatrices**

<table>
<thead>
<tr>
<th>Dimension</th>
<th># submatrix in general</th>
<th># of submatrices of Toeplitz matrix</th>
<th># of Toeplitz submatrices of Toeplitz Matrix</th>
</tr>
</thead>
<tbody>
<tr>
<td>4 × 4</td>
<td>69</td>
<td>50</td>
<td>20</td>
</tr>
<tr>
<td>5 × 5</td>
<td>251</td>
<td>182</td>
<td>35</td>
</tr>
<tr>
<td>6 × 6</td>
<td>923</td>
<td>672</td>
<td>55</td>
</tr>
<tr>
<td>7 × 7</td>
<td>3431</td>
<td>2508</td>
<td>81</td>
</tr>
<tr>
<td>8 × 8</td>
<td>12869</td>
<td>9438</td>
<td>113</td>
</tr>
</tbody>
</table>
An Open Question

- Prob [an $n \times n$ matrix over $\mathbb{F}_q$ is nonsingular] $= \prod_{i=1}^{n} \left(1 - \frac{1}{q^i}\right)$.
- Prob [an $n \times n$ TOEPLITZ matrix over $\mathbb{F}_q$ is nonsingular] $= 1 - 1/q$.
- What is the probability that a Toeplitz matrix is MDS?
The lowest XOR count $GF(2^8)$ is 232.
The lowest XOR count for $GF(2^4)$ is 170.
A serial matrix of order $n \times n$ over $\mathbb{F}_{2^m}$ is a matrix of the form

$$S = \begin{bmatrix}
0 & 1 & \ldots & 0 \\
0 & 0 & \ldots & 0 \\
\vdots & \vdots & \ddots & \vdots \\
0 & 0 & \ldots & 1 \\
a_0 & a_1 & \ldots & a_{n-1}
\end{bmatrix}$$

A Recursive MDS matrix is a MDS matrix of the form $M = S^i$ for some $i \geq 1$. Least $S^n = \text{MDS}$.

$$\begin{bmatrix}
0 & 1 & 0 \\
0 & 0 & 1 \\
c_0 & c_1 & c_2
\end{bmatrix} \begin{bmatrix}
x \\
y \\
z
\end{bmatrix} = [y, z, c_0x + c_1y + c_2z]$$

Serial matrix is not MDS
Repeat until we get MDS.
Serial Matrix iterated further

- LED:
  \[ S = \begin{bmatrix}
  0 & 1 & 0 & 0 \\
  0 & 0 & 1 & 0 \\
  0 & 0 & 0 & 1 \\
  \alpha^2 & 1 & 1 & \alpha
  \end{bmatrix} \]

  \[ S^4 = \text{MDS}, \quad \text{XOR}(S) = 16. \]

- Last row \((1, 1, 1, 1)\) or \((a, 1, 1, 1)\) or \((1, a, 1, 1)\) or \((1, 1, 1, a)\) then \(S^i \neq \text{MDS}\) for \(i \leq 8\)

- But for the last row of \((1, 1, a, 1)\), then it is possible to have \(S^8 = \text{MDS}\).

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

- \(S\) is the lightest possible serial matrix with \(\text{XOR}(S) = 13\) and \(S^8\) MDS, \(\alpha\) is root of the irreducible polynomial \(X^4 + X + 1\)
Nonlinear diffusion layer

- Nonlinear function cannot achieve the highest branch number $n + 1$.
- Binary function $\mathbb{F}_2^n \to \mathbb{F}_2^n$
  - differential branch number of
  $$F = \min\{HW(x \oplus y) + HW(F(x) \oplus F(y))\}$$
  - highest branch number $< n + 1$.
- Differential branch number of PRESENT S-box $= 3$.
- Highest diff branch number of $4 \times 4$ S-boxes $= 3$.
- If it $4$ then it is affine. [eprint 2017/990]
Bounds : Differential Branch Number of Nonlinear Permutations

- Linear permutations : Griesmer Bound (1960)

\[ N \geq \sum_{i=0}^{K-1} \left\lceil \frac{d}{2^i} \right\rceil. \]

- Our bound : \([2n/3]\). [eprint 2017/990]

<table>
<thead>
<tr>
<th>( n )</th>
<th>Griesmer Bound</th>
<th>Our Bound</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td>4</td>
<td>4</td>
</tr>
<tr>
<td>5</td>
<td>4</td>
<td>4</td>
</tr>
<tr>
<td>6</td>
<td>4</td>
<td>4</td>
</tr>
<tr>
<td>7</td>
<td>5</td>
<td>5</td>
</tr>
<tr>
<td>8</td>
<td>6</td>
<td>6</td>
</tr>
<tr>
<td>9</td>
<td>6</td>
<td>6</td>
</tr>
<tr>
<td>10</td>
<td>7</td>
<td>7</td>
</tr>
<tr>
<td>11</td>
<td>8</td>
<td>8</td>
</tr>
<tr>
<td>12</td>
<td>8</td>
<td>8</td>
</tr>
<tr>
<td>13</td>
<td>8</td>
<td>9</td>
</tr>
</tbody>
</table>
THANK YOU