On the Lightweight Design Choices for Diffusion Layer of Block Ciphers

SUMANTA SARKAR

TCS Innovation Labs

December 11, 2017

Internet of Things / Connected Cars

- 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)

Threats!

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

Threats!

- 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.

picture source: amazon.in

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

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: Examples

- 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 Cryptography: Metric

- Lightweight cryptosystem: How to measure the “weight”?
- (Silicon) Area , Performance and power consumption

Lightweight Cryptography: Metric

- 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 => GE = 966 (.18μm).
- Performance: Throughput.
- Consult Cryptolux/Lightweight_Cryptography for the list of lightweight ciphers.

Block Ciphers: Design Principles

- A block cipher has two building blocks:

Block Ciphers: Design Principles

- 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

- $F : \mathbb{F}_q^n \longrightarrow \mathbb{F}_q^n$: Differential Branch Number of F : $\min\{wt(x+y) + wt(F(x) + F(y))\}$.
- Differential Branch Number of $F \leq n+1$

Implementation Cost Diffusion Layer

- 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.

Implementation Cost Diffusion Layer

- 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

XOR count

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

XOR count

- $\beta \in \mathrm{GF}(2^n)$ is implemented by the corresponding vector $(\beta_0, \ldots, \beta_{n-1}) \in \mathrm{GF}(2)^n$ by choosing some basis of $\mathrm{GF}(2^n)$.
- Consider $\mathrm{GF}(2^3)$ under $(X^3 + X + 1)$ and a basis $\{1, \alpha, \alpha^2\}$.
- How many XORs required to multiply α^4 with a general field element?

XOR count

- $\beta \in \mathrm{GF}(2^n)$ is implemented by the corresponding vector $(\beta_0, \ldots, \beta_{n-1}) \in \mathrm{GF}(2)^n$ by choosing some basis of $\mathrm{GF}(2^n)$.
- Consider $\mathrm{GF}(2^3)$ under $(X^3 + X + 1)$ and a basis $\{1, \alpha, \alpha^2\}$.
- How many XORs required to multiply α^4 with a general field element?
- $\alpha^4 = \alpha + \alpha^2 \rightarrow (0, 1, 1)$
- Take a general element $b_0 + b_1\alpha + b_2\alpha^2 \in \mathrm{GF}(2^3) \rightarrow (b_0, b_1, b_2)$.

XOR count

- $\beta \in GF(2^n)$ is implemented by the corresponding vector $(\beta_0, \ldots, \beta_{n-1}) \in GF(2)^n$ by choosing some basis of $GF(2^n)$.
- Consider $GF(2^3)$ under $(X^3 + X + 1)$ and a basis $\{1, \alpha, \alpha^2\}$.
- How many XORs required to multiply α^4 with a general field element?
- $\alpha^4 = \alpha + \alpha^2 \rightarrow (0, 1, 1)$
- Take a general element $b_0 + b_1\alpha + b_2\alpha^2 \in GF(2^3) \rightarrow (b_0, b_1, b_2)$. Implement

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

XOR count

- $\beta \in \mathrm{GF}(2^n)$ is implemented by the corresponding vector $(\beta_0, \ldots, \beta_{n-1}) \in \mathrm{GF}(2)^n$ by choosing some basis of $\mathrm{GF}(2^n)$.
- Consider $\mathrm{GF}(2^3)$ under $(X^3 + X + 1)$ and a basis $\{1, \alpha, \alpha^2\}$.
- How many XORs required to multiply α^4 with a general field element?
- $\alpha^4 = \alpha + \alpha^2 \rightarrow (0, 1, 1)$
- Take a general element $b_0 + b_1\alpha + b_2\alpha^2 \in \mathrm{GF}(2^3) \rightarrow (b_0, b_1, b_2)$. 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 count

- $\beta \in \mathrm{GF}(2^n)$ is implemented by the corresponding vector $(\beta_0, \ldots, \beta_{n-1}) \in \mathrm{GF}(2)^n$ by choosing some basis of $\mathrm{GF}(2^n)$.
- Consider $\mathrm{GF}(2^3)$ under $(X^3 + X + 1)$ and a basis $\{1, \alpha, \alpha^2\}$.
- How many XORs required to multiply α^4 with a general field element?
- $\alpha^4 = \alpha + \alpha^2 \longrightarrow (0, 1, 1)$
- Take a general element $b_0 + b_1\alpha + b_2\alpha^2 \in \mathrm{GF}(2^3) \longrightarrow (b_0, b_1, b_2)$. 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.

XOR Count of some Specific Elements

- α is a root of irreducible polynomial $X^n + q(X) + 1$, if there are t nonzero terms, then $XOR(\alpha)1$.
- For example, α is a root of $X^4 + X + 1$ that defines $\mathrm{GF}(2^4)$, 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 $\mathrm{GF}(2^4)$ has XOR count 1.

XOR count distribution [SS16])

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 [SS16])

XOR count distribution also varies when a different basis of $GF(2^n)$ is considered, even if the underlying irreducible polynomial remains fixed.

Elements	0	1	α	α^2	α^3	α^4	α^5	α^6	Sum
Basis $\{1, \alpha, \alpha^2\}$	0	0	1	2	4	4	3	1	15
Basis $\{\alpha^3, \alpha^6, \alpha^5\}$	0	0	3	3	2	3	2	2	15

XOR count distribution of $GF(2^3)$ under $X^3 + X + 1$

Circulant Matrix

Definition

A matrix is called circulant if every row is a cyclic shift of other rows.

$$T = \begin{bmatrix} a_0 & a_1 & a_2 & a_3 \\ a_3 & a_0 & a_1 & a_2 \\ a_2 & a_3 & a_0 & a_1 \\ a_1 & a_2 & a_3 & a_0 \end{bmatrix}.$$

Toeplitz Matrices

Definition

A matrix is called Toeplitz if every descending diagonal from left to right is constant.

A typical 4×4 Toeplitz matrix looks like

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

Definition

A matrix M is called involutory if $M * M =$ Identity matrix.

Constructing 4×4 Toeplitz MDS Matrices over $\mathbb{F}_{2^m}$ [SS16]

Let $\mathrm{T}_1(x)$ be the following 4×4 Toeplitz matrix defined over $\mathbb{F}_{2^m}$:

$$\mathrm{T}_1(x) = \begin{bmatrix} x & 1 & 1 & x^{-2} \\ 1 & x & 1 & 1 \\ x^{-2} & 1 & x & 1 \\ x^{-2} & x^{-2} & 1 & x \end{bmatrix}.$$

If $x \in \mathbb{F}_{2^m}^*$ is such that the degree of its minimal polynomial over $\mathbb{F}_2$ is ≥ 5, then $\mathrm{T}_1(x)$ is MDS.

The Matrix T_2

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

$$\mathrm{T}_2(x) = \begin{bmatrix} 1 & 1 & x & x^{-1} \\ x^{-2} & 1 & 1 & x \\ 1 & x^{-2} & 1 & 1 \\ x^{-1} & 1 & x^{-2} & 1 \end{bmatrix}. \tag{1}$$

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

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

then $\mathrm{T}_2(x)$ is MDS.

XOR count of T_2

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.

Search Results

Search result:

For $GF(2^8)$, the lowest XOR count of a 4×4 MDS matrix is 27.

For $GF(2^4)$, the lowest XOR count of a 4×4 MDS matrix is 10.

Involutory MDS Matrices

Let T be an $n \times n$ Toeplitz matrix defined over $GF(2^m)$. Then T cannot be both MDS and involutory.

Involutory MDS Matrix

Suppose $N_1(x)$ is a 4×4 matrix over $\mathbb{F}_{2^m}$ such that

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

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 ≥ 4, then $N_1(x)$ is also MDS.

Suppose $N_1(x)$ is a 4×4 matrix over $\mathbb{F}_{2^m}$ such that

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

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 ≥ 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).

Involutory MDS Matrix

Suppose $N_2(x)$ is a 4×4 matrix over $\mathbb{F}_{2^m}$ such that

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

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 ≥ 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 MDS Matrices

- 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

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

where $\tau_{d,n}$ is given by $n-1 = \lfloor \frac{n-1}{d-1} \rfloor (d-1) + \tau_{d,n}$.

Comparison of Number of Submatrices

Dimension	# submatrix in general	# of submatrices of # of Toeplitz matrix	# of Toeplitz submatrices # of Toeplitz Matrix
4×4	69	50	20
5×5	251	182	35
6×6	923	672	55
7×7	3431	2508	81
8×8	12869	9438	113

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?

8×8 Toeplitz MDS Matrices with lowest XOR counts [SS17]

- The lowest XOR count $GF(2^8)$ is 232.
- The lowest XOR count for $GF(2^4)$ is 170.

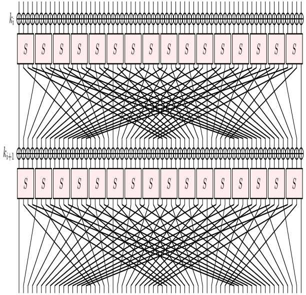
Recursive MDS Layer

- A serial matrix of order $n \times n$ over $\mathbb{F}_{2^m}$ is a matrix of the form
$$S = \begin{bmatrix} 0 & 1 & \dots & 0 \\ 0 & 0 & \dots & 0 \\ \vdots & \vdots & \dots & \vdots \\ 0 & 0 & \dots & 1 \\ a_0 & a_1 & \dots & a_{n-1} \end{bmatrix}$$
- A Recursive MDS matrix is a MDS matrix of the form $M = S^i$ for some $i \geq 1$.. Least $S^n =$ 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:
$$S = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ \alpha^2 & 1 & 1 & \alpha \end{bmatrix}$$
$S^4 =$ MDS. $XOR(S) = 16$.
- Last row $(1,1,1,1)$ or $(a,1,1,1)$ or $(1,a,1,1)$ or $(1,1,1,a)$ then $S^i \neq$ MDS for $i \leq 8$
- But for the last row of $(1,1,a,1)$, then it is possible to have $S^8 =$ 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 $XOR(S) = 13$ and S^8 MDS, α 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 $\mathbb{F}_2^n \longrightarrow \mathbb{F}_2^n$
  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 4×4 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)

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

- Our bound :$\lceil 2n/3 \rceil$. [eprint 2017/990]

n	Griesmer Bound	Our Bound
4	4	4
5	4	4
6	4	4
7	5	5
8	6	6
9	6	6
10	7	7
11	8	8
12	8	8
13	8	9

THANK YOU