Lightweight Diffusion Layer: Importance of Toeplitz Matrices

SUMANTA SARKAR Habeeb Syed

TCS Innovation Labs

March 6, 2017

Outline

Outline

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 hash function: PHOTON, SPONGENT, etc.

Lightweight Cryptography: Metric

- Lightweight cryptosystem: How to measure the “weight”?
- Measure (Silicon) Area.
- Area measured by number of Gate Equivalent (GE)

Block Ciphers

- A block cipher has two building blocks:
  Confusion & Diffusion
- Diffusion spreads the plaintext statistics throughout the ciphertext.

Lightweight Block Ciphers: Metric

- 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.

Lightweight Block Ciphers: Metric

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

Lightweight Block Ciphers: Metric

- 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.
  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

Lightweight Block Ciphers: Metric

- 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.
  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 is strongly related to GE.

Our Contribution in a Nutshell

We construct 4×4 MDS and involutory MDS matrices with low XOR counts.

Outline

XOR count

- 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

- 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

- 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

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

XOR count

- 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 count

- 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 $(b_1 \oplus b_2, b_0 \oplus b_1, b_0 \oplus b_1 \oplus b_2)$
- $XOR(\alpha^4) = 4$.

XOR count distribution

- XOR count distribution The set of XOR counts of all the elements of $\mathrm{GF}(2^n)$ is the XOR count distribution of $\mathrm{GF}(2^n)$.

XOR count distribution

- XOR count distribution The set of XOR counts of all the elements of $GF(2^n)$ is the XOR count distribution of $GF(2^n)$.

XOR count distribution of $GF(2^n)$ varies when different irreducible polynomial is considered or a different basis of $GF(2^n)$ is considered.

$GF(2^4)$ under $X^4 + X + 1$ basis $\{1, \alpha, \alpha^2\}$ then $XOR(\alpha) = 1$. But for irreducible polynomial to $X^4 + X^3 + X^2 + X + 1$, then none of the elements of $GF(2^4)$ has XOR count 1.

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 $X^3 + X + 1$

Outline

XOR count of full matrix

- M is $n \times n$ matrix over GF(2^m)

$$\text{XOR count of M} = \sum_{i=0}^{n-1} \left(\sum_{j=0}^{n-1} \gamma_{ij} + (\ell_i - 1) \cdot m \right) = C(M) + \sum_{i=0}^{n-1} (\ell_i - 1) \cdot m\,.$$

γ_i = XOR count of the i-th entry,
ℓ = number of nonzero entries,
The term $C(M)$ is the sum of XOR counts of all the entries of M.

XOR count of full matrix

- M is $n \times n$ matrix over GF(2^m)

$$\text{XOR count of M} = \sum_{i=0}^{n-1}\left(\sum_{j=0}^{n-1}\gamma_{ij} + (\ell_i - 1)\cdot m\right) = C(M) + \sum_{i=0}^{n-1}(\ell_i - 1)\cdot m\,.$$

γ_i = XOR count of the i-th entry,
ℓ = number of nonzero entries,
The term $C(M)$ is the sum of XOR counts of all the entries of M.

- For MDS matrix M XOR count is

$$C(M) + n(n-1)m$$

XOR Count of Some Field Elements

We present following properties of XOR counts of field elements.

XOR count under polynomial basis

Suppose $\mathbb{F}_{2^m}$ is defined by $q(X) = X^m + p(X) + 1$ which is an irreducible polynomial of degree m over $\mathbb{F}_2$, where $p(X)$ has t nonzero coefficients. Then XOR count of $\alpha \in \mathbb{F}_2[X]/(q(x))$ is t, where $q(\alpha) = 0$.

Further $XOR(\alpha) = XOR(\alpha^{-1})$.

If α is a primitive element of $\mathrm{GF}(2^4)$ and root of the irreducible polynomial $X^4 + X^3 + X^2 + X + 1$.
Then $XOR(\alpha) = 3$

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

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

More concisely as:

$$\mathrm{T} = [m_{i,j}] \quad \text{where} \quad m_{i,j} = a_{j-i}.$$

- Recall that a matrix is "Circulant" if each of its row is left circulant shift of its previous row.
- Circulant Matrices are specific kinds of Toeplitz Matrices.

Our results on Toeplitz MDS Matrices

Result: Theorem 1

Let T be an $n \times n$ Toeplitz matrix defined over $\mathbb{F}_{2^m}$. Then T cannot be both MDS and involutory.

Result: Theorem 2

Let T be an $n \times n$ Toeplitz matrix defined over $\mathbb{F}_{2^m}$. Then T cannot be both MDS and orthogonal when $n = 2^r$.

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

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.

Proof idea that T_1 is MDS.

Find the determinants of all the submatrices, then check the degrees of their irreducible factors. Max degree is 4.

The Matrix T_2

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

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

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.

Proof idea that T_2 is MDS.

Check the irreducible factors of the determinants of all the submatrices, Max degree is 3 and only one factor $X^6 + X^5 + X^4 + X + 1$.

XOR count of T_2

Consider $\mathbb{F}_{2^8}$ generated by the primitive element α which is a root of $X^8 + X^6 + X^5 + X^2 + 1$, then the matrix $\mathrm{T}_2(\alpha)$ as given in (2) is MDS and has XOR count $30 + 4 \cdot 3 \cdot 8$.

Consider $\mathbb{F}_{2^8}$ generated by the primitive element α which is a root of $X^8 + X^7 + X^6 + X + 1$, then the MDS matrix $\mathrm{T}_2(\alpha)$ as given in (2) has XOR count $27 + 4 \cdot 3 \cdot 8$.
Earlier best known matrix was $32 + 4 \cdot 3 \cdot 8$.

Consider $\mathbb{F}_{2^4}$ generated by the primitive element α which is a root of $X^4 + X^3 + 1$, then the matrix $\mathrm{T}_2(\alpha)$ as given in (2) has XOR count $10 + 4 \cdot 3 \cdot 4$.
Earlier best known matrix was $12 + 4 \cdot 3 \cdot 4$.

Searching for 4×4 MDS Matrices with Minimal XOR Count

Search result:

For $GF(2^8)$, the lowest XOR count of a 4×4 MDS matrix is $27 + 4 \cdot 3 \cdot 8$.

For $GF(2^4)$, the lowest XOR count of a 4×4 MDS matrix is $10 + 4 \cdot 3 \cdot 4$.

The search Technique

- We apply a kind of "divide and conquer" method.
- Divide 4×4 matrix A in two 2×4 submatrices.

$$A = \left[\begin{array}{c} A_u \\ \hline A_\ell \end{array} \right]$$

The search Technique

- We apply a kind of "divide and conquer" method.
- Divide 4×4 matrix A in two 2×4 submatrices.

$$A = \left[\begin{array}{c} A_u \\ \hline A_\ell \end{array} \right]$$

- If A is MDS then every submatrix of both A_u and A_ℓ are nonsingular!
- Search only for A_u such that all its submatrices are nonsingular.
- This will serve for A_ℓ also.
- Combine every options of A_u and A_ℓ check if A is MDS.
- Search space: suppose A takes elements from S, search space is $|S|^{2\times 4}$.

The search Technique (Contd..)

- $C(A) =$ Sum of the XOR counts of all the elements of A.
- Suppose the least known $C(A)$ for any 4×4 MDS matrix A is $\mathtt{C}$.
- First find A such that $C(A) < \mathtt{C}$.
- Update $\mathtt{C} = C(A)$.

Search: 4×4 MDS matrix over $\mathbb{F}_{2^8}$ with the minimum XOR count

- Consider the primitive polynomial $X^8 + X^7 + X^6 + X + 1$ of $\mathbb{F}_{2^8}$.
- Goal: Find A such that $C(A) \leq 26$.

Search: 4×4 MDS matrix over $\mathbb{F}_{2^8}$ with the minimum XOR count

- Consider the primitive polynomial $X^8 + X^7 + X^6 + X + 1$ of $\mathbb{F}_{2^8}$.
- Goal: Find A such that $C(A) \leq 26$.
- Form all 2×4 matrices from the set $S = \{1, \alpha, \alpha^{-1}, \alpha^2, \alpha^{-2}\}$ and find the one with minimum XOR count such that
  all its submatrices are nonsingular

Search: 4×4 MDS matrix over $\mathbb{F}_{2^8}$ with the minimum XOR count

- Consider the primitive polynomial $X^8 + X^7 + X^6 + X + 1$ of $\mathbb{F}_{2^8}$.
- Goal: Find A such that $C(A) \leq 26$.
- Form all 2×4 matrices from the set $S = \{1, \alpha, \alpha^{-1}, \alpha^2, \alpha^{-2}\}$ and find the one with minimum XOR count such that
  all its submatrices are nonsingular
- The minimum XOR count of 2×4 matrices over S is 11.
- Further we verify that this is indeed minimum XOR count of all 2×4 submatrices over $\mathbb{F}_{2^8}$.

Search: 4×4 MDS matrix over $\mathbb{F}_{2^8}$ with the minimum XOR count

- Consider the primitive polynomial $X^8 + X^7 + X^6 + X + 1$ of $\mathbb{F}_{2^8}$.
- Goal: Find A such that $C(A) \leq 26$.
- Form all 2×4 matrices from the set $S = \{1, \alpha, \alpha^{-1}, \alpha^2, \alpha^{-2}\}$ and find the one with minimum XOR count such that all its submatrices are nonsingular
- The minimum XOR count of 2×4 matrices over S is 11.
- Further we verify that this is indeed minimum XOR count of all 2×4 submatrices over $\mathbb{F}_{2^8}$.
- So in $A = \left[\begin{array}{c} A_u \\ \hline A_\ell \end{array} \right]$, the maximum XOR count of A_u and A_ℓ can be $26 - 11 = 15$.

Search: 4×4 MDS matrix over $\mathbb{F}_{2^8}$ with the minimum XOR count

- Consider the primitive polynomial $X^8 + X^7 + X^6 + X + 1$ of $\mathbb{F}_{2^8}$.
- Goal: Find A such that $C(A) \leq 26$.
- Form all 2×4 matrices from the set $S = \{1, \alpha, \alpha^{-1}, \alpha^2, \alpha^{-2}\}$ and find the one with minimum XOR count such that all its submatrices are nonsingular
- The minimum XOR count of 2×4 matrices over S is 11.
- Further we verify that this is indeed minimum XOR count of all 2×4 submatrices over $\mathbb{F}_{2^8}$.
- So in $A = \left[\begin{array}{c} A_u \\ \hline A_\ell \end{array} \right]$, the maximum XOR count of A_u and A_ℓ can be $26 - 11 = 15$.
- Now we need to search for 2×4 matrices over $\mathbb{F}_{2^8}$ such that their XOR count is bounded by 15.
- For this we just need to check 2×4 matrices over $S = \{\beta \in \mathbb{F}_{2^8}^* : XOR(\beta) \leq 12\}$.

Search: 4×4 MDS matrix over $\mathbb{F}_{2^8}$ with the minimum XOR count (Contd.)

- Number of 2×4 submatrices obtained is 3360 (these are the options for A_u and A_ℓ).
- Combine pairs and check if $A = \left[\begin{array}{c} A_u \\ \hline A_\ell \end{array}\right]$, is MDS or not.
- Need to check $3360^2 \approx 2^{24}$ pairs.
- We do not find any MDS matrix with XOR count ≤ 26.

Search: 4×4 MDS matrix over $\mathbb{F}_{2^8}$ with the minimum XOR count (Conclusion)

- For all irreducible polynomial there were no 4×4 MDS matrix with XOR count ≤ 26.

Search: 4×4 MDS matrix over $\mathbb{F}_{2^8}$ with the minimum XOR count (Conclusion)

- For all irreducible polynomial there were no 4×4 MDS matrix with XOR count ≤ 26.

For $GF(2^8)$, the lowest XOR count of a 4×4 MDS matrix is $27 + 4 \cdot 3 \cdot 8$.

Search: 4×4 MDS matrix over $\mathbb{F}_{2^8}$ with the minimum XOR count (Conclusion)

- For all irreducible polynomial there were no 4×4 MDS matrix with XOR count ≤ 26.

For $GF(2^8)$, the lowest XOR count of a 4×4 MDS matrix is $27 + 4 \cdot 3 \cdot 8$.

Similarly we search for $GF(2^4)$ and obtain that

For $GF(2^4)$, the lowest XOR count of a 4×4 MDS matrix is $10 + 4 \cdot 3 \cdot 4$.

Involutory MDS Matrix

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

$$N_1(x) = \begin{bmatrix} 1 & x & 1 & x^2+1 \\ x & 1 & x^2+1 & 1 \\ x^{-2} & 1+x^{-2} & 1 & x \\ 1+x^{-2} & x^{-2} & x & 1 \end{bmatrix}. \qquad (3)$$

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 $\mathbb{F}_{2^8}$, the minimum XOR count obtained for N_1 is $64 + 4 \cdot 3 \cdot 8$ over all irreducible polynomials of degree 8 over $\mathbb{F}_2$. Note that this is the known lower bound for XoR count of 4×4 MDS involutory matrices over $\mathbb{F}_{2^8}$ [Sim et al. FSE 2015].

Involutory MDS Matrix

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

$$N_2(x) = \begin{bmatrix} 1 & x^2+1 & x & 1 \\ x^2+1 & 1 & 1 & x \\ x^3+x & x^2+1 & 1 & x^2+1 \\ x^2+1 & x^3+x & x^2+1 & 1 \end{bmatrix}. \qquad (4)$$

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

- For $\mathbb{F}_{2^4}$, the minimum XOR count obtained for N_1 is $16 + 4 \cdot 3 \cdot 4$.
- The best known was $24 + 4 \cdot 3 \cdot 4$ [Sim et al. FSE 2015].

Examples of Involutory MDS Matrices

The matrix

$$\begin{bmatrix} 1 & \alpha & 1 & \alpha^{211} \\ \alpha & 1 & \alpha^{211} & 1 \\ \alpha^{-2} & \alpha^{209} & 1 & \alpha \\ \alpha^{209} & \alpha^{-2} & \alpha & 1 \end{bmatrix}$$

is involutory and MDS over $\mathbb{F}_{2^8}$, where α is a root of the irreducible polynomial $X^8 + X^6 + X^5 + X^2 + 1$. XOR count of this matrix is $64 + 4 \cdot 3 \cdot 8$.

The matrix

$$\begin{bmatrix} 1 & \alpha & \alpha^2 & 1 \\ \alpha & 1 & 1 & \alpha^2 \\ \alpha^3 & \alpha & 1 & \alpha \\ \alpha & \alpha^3 & \alpha & 1 \end{bmatrix}$$

is involutory and MDS over $\mathbb{F}_{2^4}$, where α is a root of the irreducible polynomial $X^4 + X + 1$ with XOR count $16 + 4 \cdot 3 \cdot 4$.

Conclusions

- Searching for lightweight MDS matrices is an important problem and we have settled this for 4×4 MDS matrix.
- We have shown the importance of Toeplitz matrices in the context of MDS property for 4×4 matrices.
- What about the 8×8 MDS matrices?
- Any theoretical construction in this regard will be welcome.

THANK YOU