# Design of Lightweight Linear Diffusion Layers from Near-MDS Matrices

Chaoyun Li[1] Qingju Wang[1,2]

[1]imec and COSIC, KU Leuven

[2]DTU Compute, Technical University of Denmark

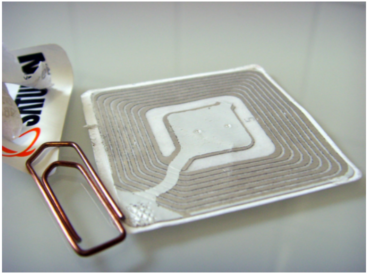
March 6, 2017

# Outlines

# Lightweight cryptography

- Meet the security requirements of ubiquitous computing
  - *Internet of Things (IoT)*

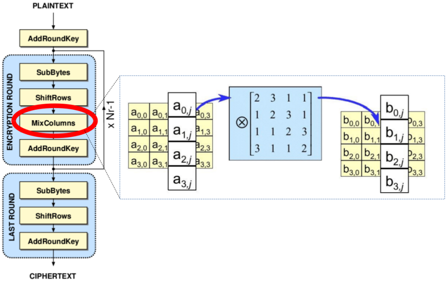
- Explore the tradeoffs between implementation cost and security



# Linear diffusion layers

- Confusion and Diffusion (Shannon 1949)
  - SPN structure: Nonlinear layer and *linear diffusion layer*
- Diffusion matrices
  - Spread internal dependency
  - Provide resistance against differential/linear attacks (Daemen and Rijmen 2002)

  $\hookrightarrow$ The focus of attention in lightweight cryptography



# MDS matrices

### Direct construction

MDS matrix in MixColumns of AES (Daemen and Rijmen 2002)

$$\mathrm{circ}(2,3,1,1) = \begin{pmatrix} 2 & 3 & 1 & 1 \\ 1 & 2 & 3 & 1 \\ 1 & 1 & 2 & 3 \\ 3 & 1 & 1 & 2 \end{pmatrix}.$$

### Efficiency

1. Direct constructions are costly in hardware

# MDS matrices

### Direct construction

MDS matrix in MixColumns of AES (Daemen and Rijmen 2002)

$$\mathrm{circ}(2,3,1,1) = \begin{pmatrix} 2 & 3 & 1 & 1 \\ 1 & 2 & 3 & 1 \\ 1 & 1 & 2 & 3 \\ 3 & 1 & 1 & 2 \end{pmatrix}.$$

### Recursive construction

Recursive MDS in PHOTON and LED (Guo *et al.* 2011)

$$A^4 = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 2 & 1 & 4 \end{pmatrix}^4 = \begin{pmatrix} 1 & 2 & 1 & 4 \\ 4 & 9 & 6 & 17 \\ 17 & 38 & 24 & 66 \\ 66 & 149 & 100 & 11 \end{pmatrix}$$

### Efficiency

1. Direct constructions are costly in hardware
2. Recursive constructions are lighweight but need additional clock cycles

# Near-MDS matrices

## Near-MDS matrices

An $n \times n$ matrix $M$ is *near-MDS* if $\mathcal{B}_d(M) = \mathcal{B}_l(M) = n$

- Suboptimal diffusion but require less area than MDS
- Better tradeoff of security and efficiency
  - *FOAM* framework (Khoo *et al.* 2014)

# Near-MDS matrices

### Near-MDS matrices

An $n \times n$ matrix $M$ is *near-MDS* if $\mathcal{B}_d(M) = \mathcal{B}_l(M) = n$

- Suboptimal diffusion but require less area than MDS
- Better tradeoff of security and efficiency
  - *FOAM* framework (Khoo *et al.* 2014)

### Our goal

1. Construct lightweight near-MDS matrices over finite fields
2. Investigate near-MDS matrices with minimal implementation cost

# Outlines

# Previous work

## The $4 \times 4$ near-MDS matrix

$$\mathrm{circ}(0,1,1,1) = \begin{pmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \end{pmatrix}$$

+ Implementation cost can be only 50% of MDS matrix in AES
+ With lowest XOR count among all near-MDS matrices of order 4
+ **Involutory**

⋆ Used in PRINCE, FIDES, PRIDE, Midori, MANTIS

## Nonexistence result for $n > 4$ (Choy and Khoo 2008)

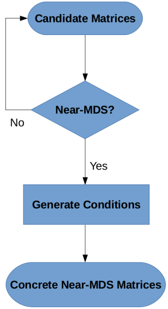
$\{0,1\}$-matrix of order $n$ cannot be near-MDS

# Search strategy

- Generic matrices
- Special form
- Maximize occurrences of $0, 1$ and minimize the number of distinct entries

# Main approach

1. Consider generic circulant/Hadamard matrices with entries 0 and $x^i$, first search matrices consisting of $0, 1, x, x^{-1}, x^2$
2. Check near-MDS property and generate conditions for the matrix to be near-MDS
3. Substitute $x$ with the lightest $\alpha \in \mathbb{F}_{2^m}$ satisfying all the conditions



# Lightweight near-MDS circulant matrices

## Generic near-MDS circulant matrices of order $5 \leq n \leq 9$

- Near-MDS property holds for almost all finite fields
- Occurrences of $0, 1$ maximized
- Only four distinct entries $0, 1, x, x^{-1}$

## Example

$$\begin{pmatrix} 0 & \alpha & 1 & 1 & 1 & \alpha \\ \alpha & 0 & \alpha & 1 & 1 & 1 \\ 1 & \alpha & 0 & \alpha & 1 & 1 \\ 1 & 1 & \alpha & 0 & \alpha & 1 \\ 1 & 1 & 1 & \alpha & 0 & \alpha \\ \alpha & 1 & 1 & 1 & \alpha & 0 \end{pmatrix}$$

is near-MDS over $\mathbb{F}_{2^m}$ if $\alpha$ is not a root of the following polynomials

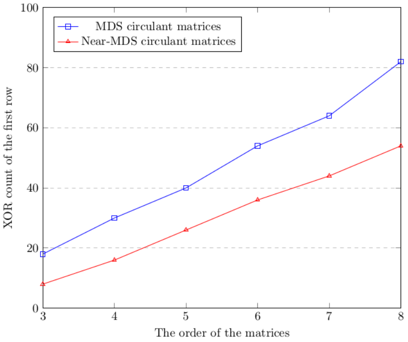
$$x,\ x+1,\ x^2+x+1\,.$$

# Comparison with MDS matrices

**XOR count of $\alpha$**

Number of XOR operations required to implement $\alpha \cdot \beta$ with arbitrary $\beta$

XOR counts of best known lightweight MDS and near-MDS circulant matrices over $\mathbb{F}_{2^8}$



# Involutory near-MDS matrices

### Hadamard matrices

- Easy to be involutory
- Efficient implementation

### Involutory near-MDS Hadamard matrices of order 8

- 2688 matrices with five distinct entries $0, 1, x, x^{-1}, x^2$
- Two different equivalence classes

$$\mathrm{had}(0, x^2, x^{-1}, x^2, x^{-1}, x, x, 1)$$
$$\mathrm{had}(0, x^2, x^{-1}, x^{-1}, x^2, x, x, 1)$$

# Outlines

# Near-MDS matrices with minimal implementation cost

- Focus on the total XOR count of the near-MDS matrices
- Comparison with all near-MDS matrices of the same order
- For $2 \leq n \leq 4$, binary circulant matrices achieve lowest XOR count

# Near-MDS circulant matrices of order $7, 8$

### Theorem

If $\alpha$ is the lightest element in $\mathbb{F}_{2^m} \setminus \{0, 1\}$ and satisfies the near-MDS conditions, then the following near-MDS circulant matrices have lowest XOR counts. **For any $4 \leq m \leq 2048$, the matrices always have instantiations with lowest XOR count over $\mathbb{F}_{2^m}$.**

| $n$ | Coefficients of the first row | Conditions |
|---|---|---|
| 7 | $(0, \alpha, 1, \alpha^{-1}, 1, 1, 1)$ | $x, x+1, x^2+x+1, x^3+x+1$<br>$x^3+x^2+1, x^4+x^3+x^2+x+1$ |
| 8 | $(0, \alpha, 1, \alpha, \alpha^{-1}, 1, 1, 1)$ | $x, x+1, x^2+x+1, x^3+x+1$<br>$x^3+x^2+1, x^4+x^3+x^2+x+1$<br>$x^5+x^4+x^3+x^2+1$ |

# Proof sketch

1. Determine the maximum occurrences of 0 and 1 for all near-MDS matrices
2. Show circulant matrices attain the maximum occurrences of 0 and 1 simultaneously
3. The remaining entries ($\alpha$ and $\alpha^{-1}$) all have the smallest XOR count

# Proof sketch

1. Determine the maximum occurrences of 0 and 1 for all near-MDS matrices
2. Show circulant matrices attain the maximum occurrences of 0 and 1 simultaneously
3. The remaining entries ($\alpha$ and $\alpha^{-1}$) all have the smallest XOR count
4. For $4 \leq m \leq 2048$, there always exists $\alpha$ which is the lightest element in $\mathbb{F}_{2^m} \setminus \{0, 1\}$ and satisfies the near-MDS conditions (Beierle *et al.* CRYPTO 2016)

## Proof sketch

1. Determine the maximum occurrences of 0 and 1 for all near-MDS matrices
2. Show circulant matrices attain the maximum occurrences of 0 and 1 simultaneously
3. The remaining entries ($\alpha$ and $\alpha^{-1}$) all have the smallest XOR count
4. For $4 \leq m \leq 2048$, there always exists $\alpha$ which is the lightest element in $\mathbb{F}_{2^m} \setminus \{0, 1\}$ and satisfies the near-MDS conditions (Beierle *et al.* CRYPTO 2016)

**For $m > 2048$**

The existence of lightest $\alpha$ satisfying the near-MDS conditions?

# Results for $n = 5, 6$

### Theorem

For any $m \geq 3$, if $\alpha$ and $\beta$ are lightest elements in $\mathbb{F}_{2^m} \setminus \{0, 1\}$ and $\beta^2 + \beta + 1 \neq 0$, the following two matrices have the lowest XOR count. **For any $4 \leq m \leq 2048$, the matrices always have instantiations with lowest XOR count over $\mathbb{F}_{2^m}$.**

$$\begin{pmatrix} 0 & \alpha & 1 & 1 & 1 \\ 1 & 0 & \alpha & 1 & 1 \\ 1 & 1 & 0 & \alpha & 1 \\ \alpha & 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 1 & 0 \end{pmatrix} \text{and} \begin{pmatrix} 0 & \beta & \beta & 1 & 1 & 1 \\ 1 & 0 & 1 & \beta & 1 & 1 \\ 1 & 1 & 0 & 1 & \beta & 1 \\ 1 & 1 & \beta & 0 & 1 & \beta \\ 1 & \beta & 1 & 1 & 0 & \beta \\ \beta & 1 & 1 & 1 & 1 & 0 \end{pmatrix}$$

# Results for $n = 5, 6$

### Theorem

For any $m \geq 3$, if $\alpha$ and $\beta$ are lightest elements in $\mathbb{F}_{2^m} \setminus \{0,1\}$ and $\beta^2 + \beta + 1 \neq 0$, the following two matrices have the lowest XOR count. **For any $4 \leq m \leq 2048$, the matrices always have instantiations with lowest XOR count over $\mathbb{F}_{2^m}$.**

$$\begin{pmatrix} 0 & \alpha & 1 & 1 & 1 \\ 1 & 0 & \alpha & 1 & 1 \\ 1 & 1 & 0 & \alpha & 1 \\ \alpha & 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 1 & 0 \end{pmatrix} \text{and} \begin{pmatrix} 0 & \beta & \beta & 1 & 1 & 1 \\ 1 & 0 & 1 & \beta & 1 & 1 \\ 1 & 1 & 0 & 1 & \beta & 1 \\ 1 & 1 & \beta & 0 & 1 & \beta \\ 1 & \beta & 1 & 1 & 0 & \beta \\ \beta & 1 & 1 & 1 & 1 & 0 \end{pmatrix}$$

- Circulant matrices cannot achieve the minimal values
- They can be very close to

# Outlines

# Primary security analysis

- Lower bounds on the number of differential and linear active S-boxes for SPN structures using near-MDS matrices

| *n* | # Rounds | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 |
| 4 | 0 | 4 | 7 | 16 | 17 | 20 | 23 | 32 | 33 | 36 | 39 | 48 | 49 | 52 | 55 | 64 |
| 5 | 0 | 5 | 9 | 25 | 26 | 30 | 34 | 50 | 51 | 55 | 59 | 75 | 76 | 80 | 84 | 102 |
| 6 | 0 | 6 | 11 | 36 | 37 | 42 | 47 | 72 | 73 | 78 | 83 | 108 | 109 | 114 | 119 | 144 |
| 7 | 0 | 7 | 13 | 49 | 50 | 56 | 62 | 98 | 99 | 105 | 111 | 147 | 148 | 154 | 160 | 196 |
| 8 | 0 | 8 | 15 | 64 | 65 | 72 | 79 | 128 | 129 | 136 | 143 | 192 | 193 | 200 | 207 | 256 |

# Primary security analysis

- Lower bounds on the number of differential and linear active S-boxes for SPN structures using near-MDS matrices

| $n$ | # Rounds | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 |
| 4 | 0 | 4 | 7 | 16 | 17 | 20 | 23 | 32 | 33 | 36 | 39 | 48 | 49 | 52 | 55 | 64 |
| 5 | 0 | 5 | 9 | 25 | 26 | 30 | 34 | 50 | 51 | 55 | 59 | 75 | 76 | 80 | 84 | 102 |
| 6 | 0 | 6 | 11 | 36 | 37 | 42 | 47 | 72 | 73 | 78 | 83 | 108 | 109 | 114 | 119 | 144 |
| 7 | 0 | 7 | 13 | 49 | 50 | 56 | 62 | 98 | 99 | 105 | 111 | 147 | 148 | 154 | 160 | 196 |
| 8 | 0 | 8 | 15 | 64 | 65 | 72 | 79 | 128 | 129 | 136 | 143 | 192 | 193 | 200 | 207 | 256 |

- Linear layers based on near-MDS matrices can provide sufficient security with well-chosen nonlinear layers

# Outlines

# Conclusion

## Proposed lightweight matrices

- Near-MDS circulant matrices of order $n \leq 9$
- Involutory near-MDS matrices of order 8

## Matrices over $\mathbb{F}_{2^m}$ with lowest XOR counts for $4 \leq m \leq 2048$

- $n = 7, 8$, circulant matrices achieve the lowest XOR count
- $n = 5, 6$, the XOR counts of circulant matrices are very close to the minimum values

## Future work

- Design of involutory near-MDS matrices of order not a power of 2
- Further security analysis of the primitives based on near-MDS matrices

Thank you:)

**Any questions?**