Mixing Layers in Symmetric Crypto

Ko Stoffelen
Part I

Shorter Linear Straight-Line Programs for MDS Matrices

Part II

Column Parity Mixers
MDS Matrices in Symmetric Crypto

- **Maximum Distance Separable**
MDS Matrices in Symmetric Crypto

- Maximum Distance Separable
- Common linear layer with optimal \textit{branch number}
MDS Matrices in Symmetric Crypto

- **Maximum Distance Separable**
- Common linear layer with optimal *branch number*
- A lot of effort on finding efficient MDS matrices over $(\mathbb{F}_2^k)^{n\times n}$
MDS Matrices in Symmetric Crypto

- Maximum Distance Separable
- Common linear layer with optimal branch number
- A lot of effort on finding efficient MDS matrices over $\left(\mathbb{F}_2^k\right)^{n \times n}$
- Compared by ‘XOR count’: multiplication of single element
MDS Matrices in Symmetric Crypto

- **Maximum Distance Separable**
- Common linear layer with optimal *branch number*
- A lot of effort on finding efficient MDS matrices over $(\mathbb{F}_2^k)^{n \times n}$
- Compared by ‘XOR count’: multiplication of single element
- But when viewed as binary matrix:
MDS Matrices in Symmetric Crypto

• **Maximum Distance Separable**
• Common linear layer with optimal *branch number*
• A lot of effort on finding efficient MDS matrices over \((\mathbb{F}_2^k)^{n \times n}\)
• Compared by ‘XOR count’: multiplication of single element
• But when viewed as binary matrix:
  – Problem becomes shortest-linear straight-line program
MDS Matrices in Symmetric Crypto

• Maximum Distance Separable
• Common linear layer with optimal branch number
• A lot of effort on finding efficient MDS matrices over $(\mathbb{F}_2^k)^{n \times n}$
• Compared by ‘XOR count’: multiplication of single element
• But when viewed as binary matrix:
  – Problem becomes shortest-linear straight-line program
  – Global optimization saves more XORs
MDS Matrices in Symmetric Crypto

- **Maximum Distance Separable**
- Common linear layer with optimal *branch number*
- A lot of effort on finding efficient MDS matrices over \((\mathbb{F}_2^k)^{n \times n}\)
- Compared by ‘XOR count’: multiplication of single element
- But when viewed as binary matrix:
  - Problem becomes shortest-linear straight-line program
  - Global optimization saves more XORs
  - Old algorithms improve many results (e.g., AES MixColumns)
MDS Matrices in Symmetric Crypto

- **Maximum Distance Separable**
- Common linear layer with optimal *branch number*
- A lot of effort on finding efficient MDS matrices over \((\mathbb{F}_2^k)^{n \times n}\)
- Compared by ‘XOR count’: multiplication of single element
- But when viewed as binary matrix:
  - Problem becomes shortest-linear straight-line program
  - Global optimization saves more XORs
  - Old algorithms improve many results (e.g., AES MixColumns)
  - We find new MDS matrices with lowest number of XORs
Column Parity Mixers

- Keccak-$f$ has very strong bounds on differential trails due to $\theta$
Column Parity Mixers

- Keccak-$f$ has very strong bounds on differential trails due to $\theta$
- Properties of $\theta$-like mixing layers not well understood
Column Parity Mixers

- Keccak-f has very strong bounds on differential trails due to $\theta$
- Properties of $\theta$-like mixing layers not well understood
- CPM: generalization of $\theta$
Column Parity Mixers

- Keccak-\( f \) has very strong bounds on differential trails due to \( \theta \)
- Properties of \( \theta \)-like mixing layers not well understood
- CPM: generalization of \( \theta \)
  - Interesting algebraic properties
Column Parity Mixers

- Keccak-$f$ has very strong bounds on differential trails due to $\theta$
- Properties of $\theta$-like mixing layers not well understood
- CPM: generalization of $\theta$
  - Interesting algebraic properties
  - Good diffusion properties
**Column Parity Mixers**

- Keccak-$f$ has very strong bounds on differential trails due to $\theta$
- Properties of $\theta$-like mixing layers not well understood
- CPM: generalization of $\theta$
  - Interesting algebraic properties
  - Good *diffusion* properties
  - Also suitable for strongly aligned ciphers
Column Parity Mixers

- Keccak-$f$ has very strong bounds on differential trails due to $\theta$
- Properties of $\theta$-like mixing layers not well understood
- CPM: generalization of $\theta$
  - Interesting algebraic properties
  - Good diffusion properties
  - Also suitable for strongly aligned ciphers
  - Competitive with MDS matrices
Column Parity Mixers

For an $m \times n$ matrix $A$ over $\mathbb{F}_2^k$:

$$\theta(A) = A + f(A)$$

$$\begin{pmatrix}
a_{0,0} & a_{0,1} & a_{0,2} & a_{0,3} \\
a_{1,0} & a_{1,1} & a_{1,2} & a_{1,3} \\
a_{2,0} & a_{2,1} & a_{2,2} & a_{2,3}
\end{pmatrix}$$
Column Parity Mixers

For an $m \times n$ matrix $A$ over $\mathbb{F}_2^k$:

$$\theta(A) = A + 1_m^T A$$

\[
\begin{pmatrix}
1 & 1 & 1
\end{pmatrix}
\begin{pmatrix}
a_{0,0} & a_{0,1} & a_{0,2} & a_{0,3} \\
a_{1,0} & a_{1,1} & a_{1,2} & a_{1,3} \\
a_{2,0} & a_{2,1} & a_{2,2} & a_{2,3}
\end{pmatrix}
\]

$1 \times n$ column parity
Column Parity Mixers

For an \( m \times n \) matrix \( A \) over \( \mathbb{F}_2^k \):

\[
\theta(A) = A + 1^T_mAZ
\]

\[
\begin{pmatrix}
a_{0,0} & a_{0,1} & a_{0,2} & a_{0,3} \\
a_{1,0} & a_{1,1} & a_{1,2} & a_{1,3} \\
a_{2,0} & a_{2,1} & a_{2,2} & a_{2,3}
\end{pmatrix}
\begin{pmatrix}
z_{0,0} & z_{0,1} & z_{0,2} & z_{0,3} \\
z_{1,0} & z_{1,1} & z_{1,2} & z_{1,3} \\
z_{2,0} & z_{2,1} & z_{2,2} & z_{2,3} \\
z_{3,0} & z_{3,1} & z_{3,2} & z_{3,3}
\end{pmatrix}
\]

1\times n \text{ column parity}

\text{n\times n \text{ parity-folding matrix}}

1\times n \text{ \( \theta \)-effect}
Column Parity Mixers

For an $m \times n$ matrix $A$ over $\mathbb{F}_2^k$:

$$\theta(A) = A + 1_m 1^T_m A Z$$

\[
\begin{pmatrix}
1 \\
1 \\
1
\end{pmatrix}
\begin{pmatrix}
1 & 1 & 1
\end{pmatrix}
\begin{pmatrix}
a_{0,0} & a_{0,1} & a_{0,2} & a_{0,3} \\
a_{1,0} & a_{1,1} & a_{1,2} & a_{1,3} \\
a_{2,0} & a_{2,1} & a_{2,2} & a_{2,3}
\end{pmatrix}
\begin{pmatrix}
z_{0,0} & z_{0,1} & z_{0,2} & z_{0,3} \\
z_{1,0} & z_{1,1} & z_{1,2} & z_{1,3} \\
z_{2,0} & z_{2,1} & z_{2,2} & z_{2,3} \\
z_{3,0} & z_{3,1} & z_{3,2} & z_{3,3}
\end{pmatrix}
\]

$1 \times n$ column parity

$n \times n$ parity-folding matrix

$1 \times n$ $\theta$-effect

$m \times n$ expanded $\theta$-effect
Column Parity Mixers

For an $m \times n$ matrix $A$ over $\mathbb{F}_2^k$:

$$\theta(A) = A + 1^m_m A Z$$

\[
\begin{pmatrix}
1 \\
1 \\
1
\end{pmatrix}
\begin{pmatrix}
1 & 1 & 1
\end{pmatrix}
\begin{pmatrix}
a_{0,0} & a_{0,1} & a_{0,2} & a_{0,3} \\
a_{1,0} & a_{1,1} & a_{1,2} & a_{1,3} \\
a_{2,0} & a_{2,1} & a_{2,2} & a_{2,3}
\end{pmatrix}
\begin{pmatrix}
z_{0,0} & z_{0,1} & z_{0,2} & z_{0,3} \\
z_{1,0} & z_{1,1} & z_{1,2} & z_{1,3} \\
z_{2,0} & z_{2,1} & z_{2,2} & z_{2,3} \\
z_{3,0} & z_{3,1} & z_{3,2} & z_{3,3}
\end{pmatrix}
\]
Column Parity Mixers

For an $m \times n$ matrix $A$ over $\mathbb{F}_2^k$:

$$\theta(A) = A + 1_m^T A Z$$

\[
\begin{pmatrix}
1 \\
1 \\
1
\end{pmatrix}
\begin{pmatrix} 1 & 1 & 1 \\
\end{pmatrix}
\begin{pmatrix} a_{0,0} & a_{0,1} & a_{0,2} & a_{0,3} \\
a_{1,0} & a_{1,1} & a_{1,2} & a_{1,3} \\
a_{2,0} & a_{2,1} & a_{2,2} & a_{2,3}
\end{pmatrix}
\begin{pmatrix}
z_{0,0} & z_{0,1} & z_{0,2} & z_{0,3} \\
z_{1,0} & z_{1,1} & z_{1,2} & z_{1,3} \\
z_{2,0} & z_{2,1} & z_{2,2} & z_{2,3} \\
z_{3,0} & z_{3,1} & z_{3,2} & z_{3,3}
\end{pmatrix}
\]

$1 \times n$ column parity

$n \times n$ parity-folding matrix

$1 \times n$ $\theta$-effect

$m \times n$ expanded $\theta$-effect

$\theta$ fully defined by $m$, $n$ and $Z$