On Diffusion Layers Of SPN Based Format Preserving Encryption Schemes: Format Preserving Sets Revisited

Rana Barua, Kishan Chand Gupta, Sumit Kumar Pandey and Indranil Ghosh Ray

R.C. Bose Centre for Cryptology and Security, Kolkata, India
Indian Statistical Institute, Kolkata, India
Ashoka University, Sonepat, Haryana, India
City University, London, UK

December 10, 2018

Question

- Let $X = \{0, 1, \cdots, t\}$ (for example, $t = 9$).
- Let $\phi : X \to \mathcal{R}$ be an injective map ($\mathcal{R}$ be a ring).
- Let $\phi(X) = \mathbb{S} \subseteq \mathcal{R}$.

Question

- Given $n \in \mathbb{Z}^+$, $\mathcal{R}$ and $\mathbb{S}$, does there exist any $n \times n$ matrix $M(\mathcal{R})$ such that $Mv \in \mathbb{S}^n$ for all $v \in \mathbb{S}^n$? Or,
- Given $\mathcal{R}$ and $n \times n$ matrix $M(\mathcal{R})$, does there exist any $\mathbb{S}$ such that $Mv \in \mathbb{S}^n$ for all $v \in \mathbb{S}^n$?

Question

- Let $X = \{0, 1, \cdots, t\}$ (for example, $t = 9$).
- Let $\phi : X \to \mathcal{R}$ be an injective map ($\mathcal{R}$ be a ring).
- Let $\phi(X) = \mathbb{S} \subseteq \mathcal{R}$.

Question

- Given $n \in \mathbb{Z}^+$, $\mathcal{R}$ and $\mathbb{S}$, does there exist any $n \times n$ matrix $M(\mathcal{R})$ such that $Mv \in \mathbb{S}^n$ for all $v \in \mathbb{S}^n$? Or,
- Given $\mathcal{R}$ and $n \times n$ matrix $M(\mathcal{R})$, does there exist any $\mathbb{S}$ such that $Mv \in \mathbb{S}^n$ for all $v \in \mathbb{S}^n$?

Definition

If such M exists, we say $\mathbb{S}$ is a format preserving set with respect to matrix M ($\mathbb{S}$ is an FPS wrt M).

Question

Question

- Let $\mathbb{F}_q$ be a finite field. Given $n \in \mathbb{Z}^+$, $\mathbb{F}_q$ and $\mathbb{S}$, does there exist any $n \times n$ matrix $M(\mathbb{F}_q)$ such that $Mv \in \mathbb{S}^n$ for all $v \in \mathbb{S}^n$?

Definition

If such M exists, we say $\mathbb{S}$ is a format preserving set with respect to matrix M ($\mathbb{S}$ is an FPS wrt M).

Kishan Chand Gupta, Sumit Kumar Pandey, and Indranil Ghosh Ray. *Format Preserving Sets: On Diffusion Layers of Format Preserving Encryption Schemes*. In INDOCRYPT, pages 411–428. Springer, 2016.

FPS is not an Invariant Subspace

- Format Preserving Set - It is simply a set. There is no additional algebraic structure on format preserving set.
- Invariant Subspace - It is a vector space over some field.

An invariant subspace W is a subspace of a vector space V that is preserved by a linear transformation $T : V \to V$, i.e. $T(W) \subseteq W$.

FPS is not an Invariant Subspace

There exists a set $\mathbb{S}$ which is a format preserving set with respect to some matrix M but it is not a vector space. Consider $\mathbb{S} = \{\bar{1}, \alpha^3, \alpha^6, \alpha^9, \alpha^{12}\}$ where α is a primitive element of the field $\mathbb{F}_{2^4} = \mathbb{F}_2[x]/\langle x^4 + x + 1\rangle$ and

$$M = \begin{bmatrix} \alpha^3 & \bar{0} & \bar{0} & \bar{0} \\ \bar{0} & \alpha^6 & \bar{0} & \bar{0} \\ \bar{0} & \bar{0} & \alpha^9 & \bar{0} \\ \bar{0} & \bar{0} & \bar{0} & \alpha^{12} \end{bmatrix}$$

In the example above, $\mathbb{S}$ is an FPS but not an invariant subspace.

FPS is not an Invariant Subspace

There exists a set $\mathbb{S}$ which is a format preserving set with respect to some matrix M but it is not a vector space. Consider $\mathbb{S} = \{\bar{1}, \alpha^3, \alpha^6, \alpha^9, \alpha^{12}\}$ where α is a primitive element of the field $\mathbb{F}_{2^4} = \mathbb{F}_2[x]/\langle x^4 + x + 1\rangle$ and

$$M = \begin{bmatrix} \alpha^3 & \bar{0} & \bar{0} & \bar{0} \\ \bar{0} & \alpha^6 & \bar{0} & \bar{0} \\ \bar{0} & \bar{0} & \alpha^9 & \bar{0} \\ \bar{0} & \bar{0} & \bar{0} & \alpha^{12} \end{bmatrix}$$

In the example above, $\mathbb{S}$ is an FPS but not an invariant subspace.

An invariant subspace W over a field $\mathbb{F}$ is a format preserving set with respect to any matrix $M(\mathbb{F})$.

Previous Results

- Let $M = (m_{i,j})$ and $Z = \{m_{i,j} \mid m_{i,j} \neq \bar{0}\}$. Let $\langle Z \rangle$ denotes the smallest subgroup of $\mathbb{F}_q^*$ which contains Z.

Previous Results

- Let $M = (m_{i,j})$ and $Z = \{m_{i,j} \mid m_{i,j} \neq \bar{0}\}$. Let $\langle Z \rangle$ denotes the smallest subgroup of $\mathbb{F}_q^*$ which contains Z.

Theorem

Let $\bar{0} \in \mathbb{S}$. Suppose each row of M contains at most one non-zero entry. Then, $\mathbb{S}$ is an FPS wrt M if and only if there exists a set $H \subseteq \mathbb{F}_q^*$ such that $\mathbb{S} = \bigcup_{s \in H} s\langle Z \rangle \cup \{\bar{0}\}$.

Previous Results

- Let $M = (m_{i,j})$ and $Z = \{m_{i,j} \mid m_{i,j} \neq \bar{0}\}$. Let $\langle Z \rangle$ denotes the smallest subgroup of $\mathbb{F}_q^*$ which contains Z.

Theorem

Let $\bar{0} \in \mathbb{S}$. Suppose each row of M contains at most one non-zero entry. Then, $\mathbb{S}$ is an FPS wrt M if and only if there exists a set $H \subseteq \mathbb{F}_q^*$ such that $\mathbb{S} = \bigcup_{s \in H} s\langle Z \rangle \cup \{\bar{0}\}$.

Theorem

Let $\bar{0} \in \mathbb{S}$. Suppose M has at least one row which contains at least two non-zero entries. Then, $\mathbb{S}$ is an FPS wrt M if and only if $\mathbb{S}$ is a vector space over the field $SF(M)$.

- $SF(M)$ denotes the smallest field containing entries of M.

Remaining Work

- To find out the complete structure of $\mathbb{S}$ with respect to M, when the condition $\bar{0} \in \mathbb{S}$ is relaxed.
- To find out the structure of $\mathbb{S}$ and M, when their entries are from some ring $\mathcal{R}$ instead of the field $\mathbb{F}_q$.

This Paper

- To find out the complete structure of $\mathbb{S}$ with respect to M, when the condition $\bar{0} \in \mathbb{S}$ is relaxed.
  - Gives the complete characterisation of format preserving set over any finite field.
- To find out the structure of $\mathbb{S}$ and M, when their entries are from some ring $\mathcal{R}$ instead of the field $\mathbb{F}_q$.
  - Gives the characterisation of the set over some restrictive rings.
  - Provides format preserving sets of cardinality 10^3 and 26^3 with respect to 4×4 maximum distance separable (MDS) matrices over some specific ring $\mathcal{R}$.

Motivation

Motivation

Donghoon Chang, Mohona Ghosh, Kishan Chand Gupta, Arpan Jati, Abhishek Kumar, Dukjae Moon, Indranil Ghosh Ray, and Somitra Kumar Sanadhya. *SPF: A New Family of Efficient Format-Preserving Encryption Algorithms*, In INSCRYPT, pages 64–83. Springer, 2016.

Motivation

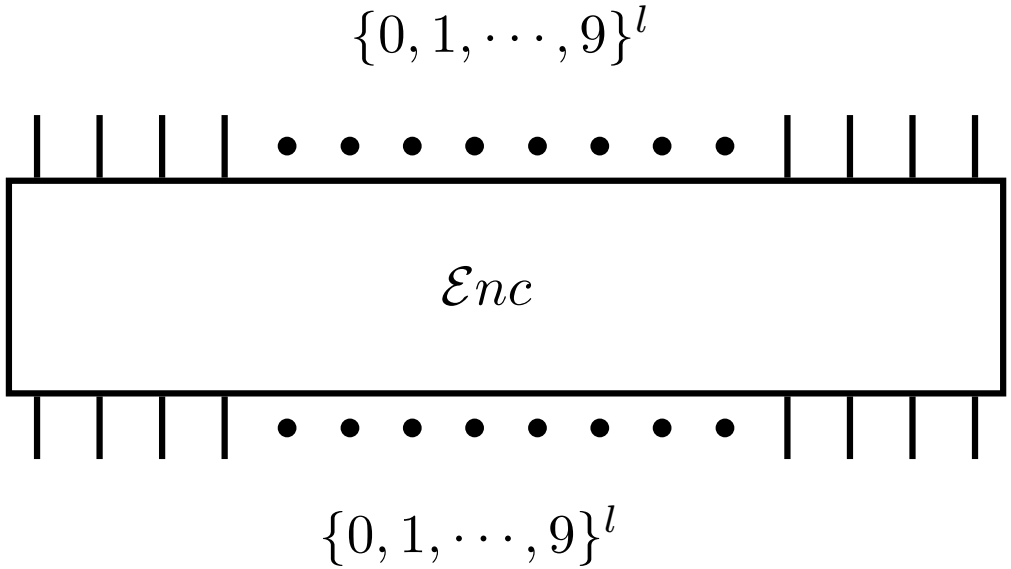

Figure: Format Preserving Encryption

Motivation Contd...

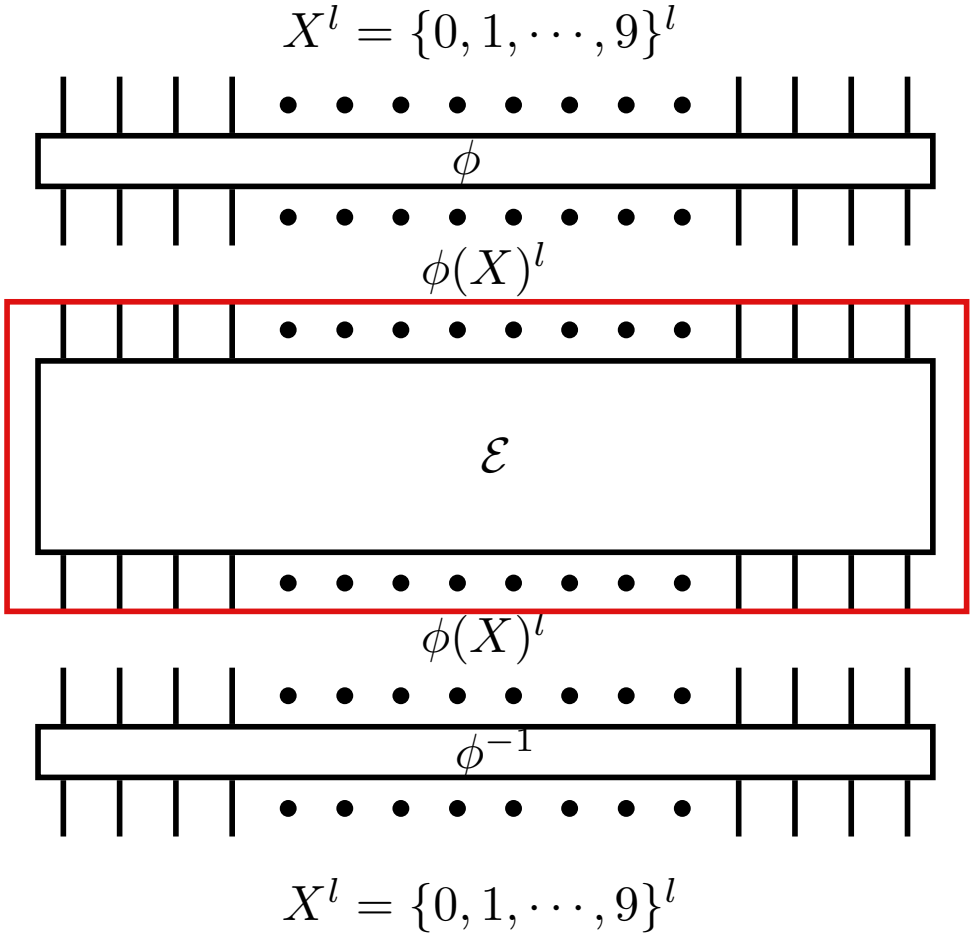

Figure: Format Preserving Encryption

Motivation Contd...

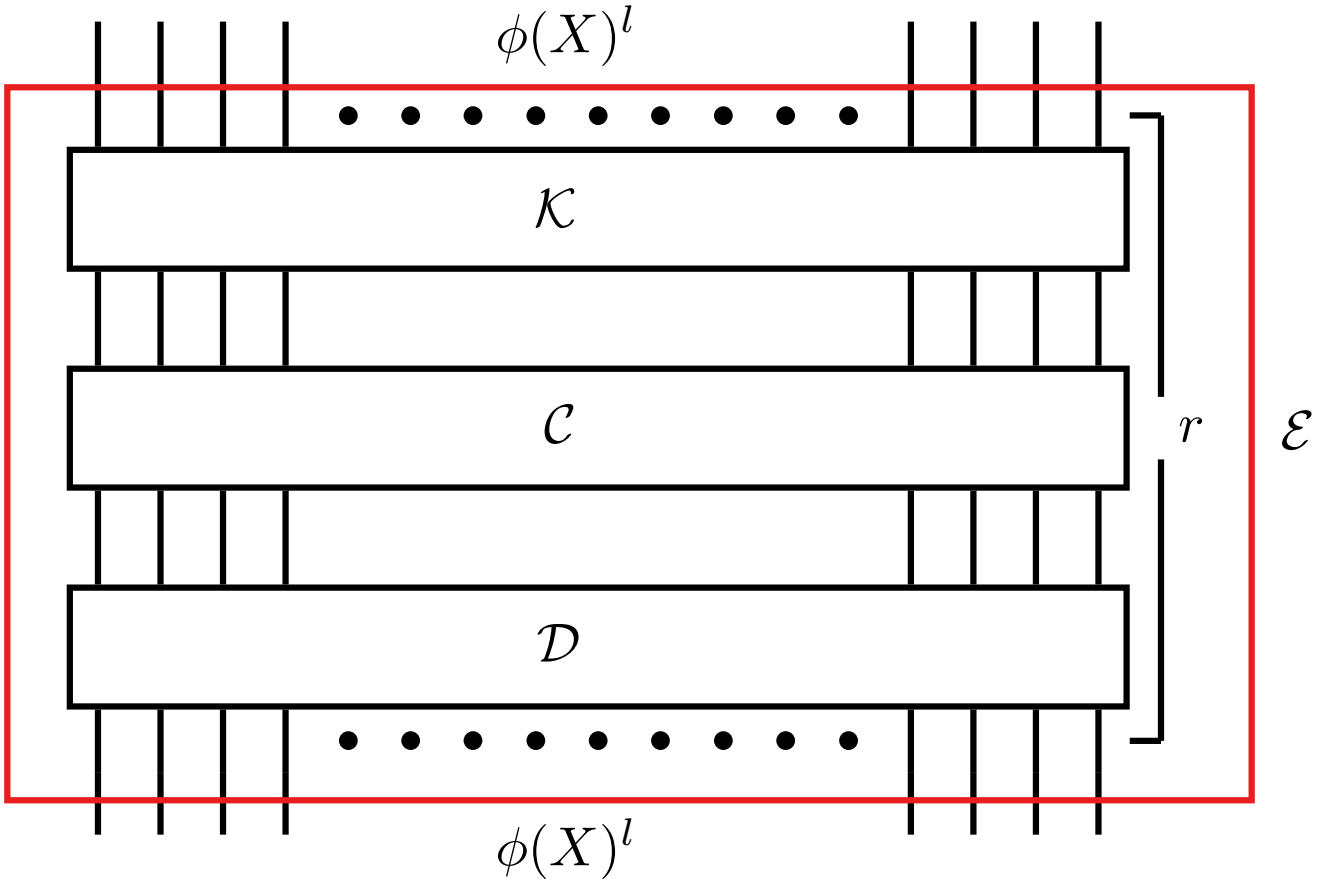

Figure: Format Preserving Encryption (SPN)

Motivation Contd...

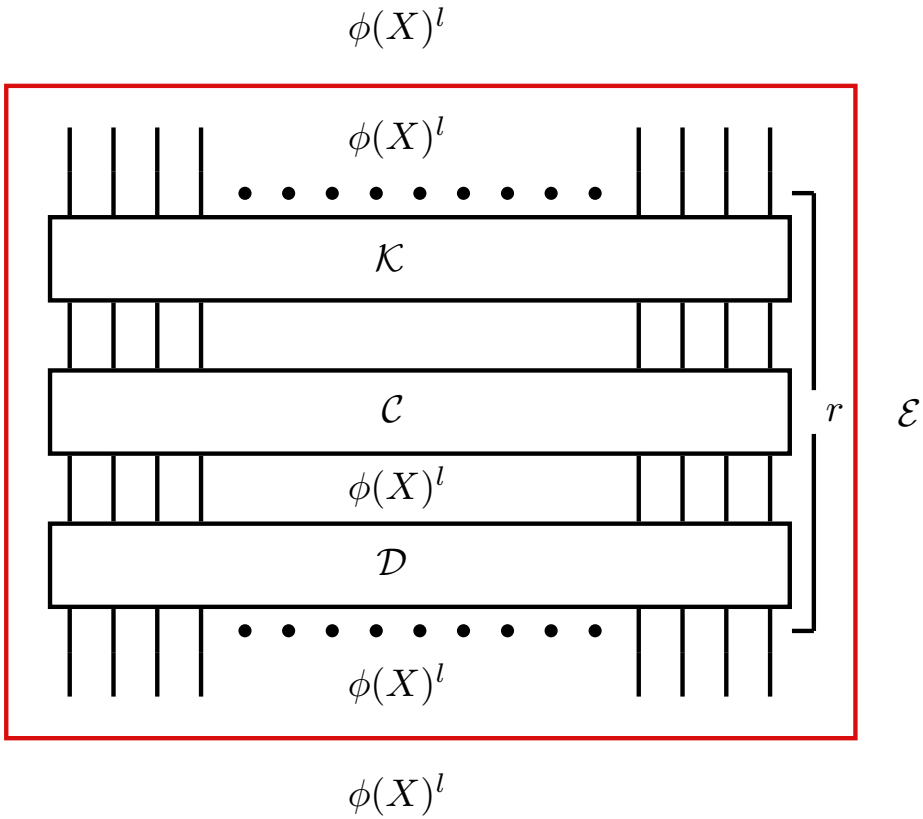

Figure: Format Preserving Encryption (SPN)

Motivation Contd...

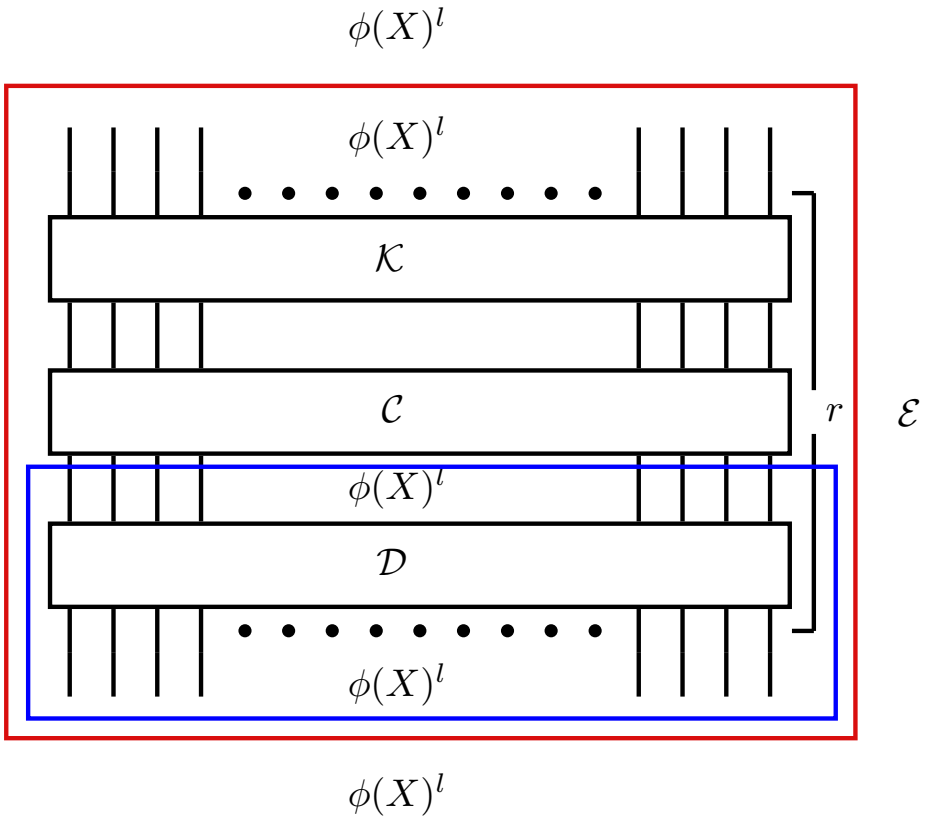

Figure: Format Preserving Encryption (SPN)

Motivation Contd...

Donghoon Chang, Mohona Ghosh, Kishan Chand Gupta, Arpan Jati, Abhishek Kumar, Dukjae Moon, Indranil Ghosh Ray, and Somitra Kumar Sanadhya. *SPF: A New Family of Efficient Format-Preserving Encryption Algorithms*, In INSCRYPT, pages 64–83, Springer, 2016.

$$D = \begin{bmatrix} \bar{1} & \bar{1} & \bar{1} & \bar{0} \\ \bar{0} & \bar{1} & \bar{1} & \bar{1} \\ \bar{1} & \bar{0} & \bar{1} & \bar{1} \\ \bar{1} & \bar{1} & \bar{0} & \bar{1} \end{bmatrix}$$

and $\mathbb{S} = \mathbb{Z}_{10}$. The matrix $D(\mathbb{Z}_{10})$ was used in the diffusion layer.

Motivation Contd...

$$D = \begin{bmatrix} \bar{1} & \bar{1} & \bar{1} & \bar{0} \\ \bar{0} & \bar{1} & \bar{1} & \bar{1} \\ \bar{1} & \bar{0} & \bar{1} & \bar{1} \\ \bar{1} & \bar{1} & \bar{0} & \bar{1} \end{bmatrix}$$

- The entries of D are from $\mathbb{Z}_{10}$, a ring, not a field. Why not entries from a field?
- D is not Maximum Distance Separable (MDS) matrix? Why not MDS matrix in the diffusion layer?

Our Results

Our Results

- Provide the complete characterisation of format preserving set over any finite field.
- Provide the characterisation of the set over some restrictive rings.
- Provide format preserving sets of cardinality 10^3 and 26^3 with respect to 4×4 MDS matrices over some specific ring $\mathcal{R}$.

Our Results

Let $M = (m_{i,j})$ and $Z = \{m_{i,j} \mid m_{i,j} \neq \bar{0}\}$. Recall $\langle Z \rangle$ denotes the smallest subgroup of $\mathbb{F}_q^*$ which contains Z.

Theorem

Let $\mathbb{S} \subseteq \mathbb{F}_q$. Suppose each row of $M(\mathbb{F}_q)$ contains at most one non-zero entry. Then, $\mathbb{S}$ is a format preserving set with respect to M if and only if there exists a set $H \subseteq \mathbb{S}$ such that $\mathbb{S} = \bigcup_{s \in H} s\langle Z \rangle = H\langle Z \rangle$.

Our Results

Let $M = (m_{i,j})$ and $Z = \{m_{i,j} \mid m_{i,j} \neq \bar{0}\}$. Recall $\langle Z \rangle$ denotes the smallest subgroup of $\mathbb{F}_q^*$ which contains Z.

Theorem

Let $\mathbb{S} \subseteq \mathbb{F}_q$. Suppose each row of $M(\mathbb{F}_q)$ contains at most one non-zero entry. Then, $\mathbb{S}$ is a format preserving set with respect to M if and only if there exists a set $H \subseteq \mathbb{S}$ such that $\mathbb{S} = \bigcup_{s \in H} s\langle Z \rangle = H\langle Z \rangle$.

Previous Result

Let $\bar{0} \in \mathbb{S}$. Suppose each row of M contains at most one non-zero entry. Then, $\mathbb{S}$ is an FPS wrt M if and only if there exists a set $H \subseteq \mathbb{F}_q^*$ such that $\mathbb{S} = \bigcup_{s \in H} s\langle Z \rangle \cup \{\bar{0}\}$.

Our Results

Assume $\bar{1} \in \mathbb{S} \subseteq \mathbb{F}_q$. Let $\bar{\mathbb{S}} = \mathbb{S} - \bar{1}$. Then,

Theorem

Let $\bar{0} \neq \mathrm{m}_i \in \mathbb{S}$ for $1 \leq i \leq n$. Suppose the $n \times n$ matrix $M(\mathbb{F}_q)$ has at least one row with at least two non-zero entries. Then $\mathbb{S}$ is a format preserving set with respect to M iff $\bar{\mathbb{S}}$ is a format preserving set with respect to M.

Note that $\bar{0} \in \bar{\mathbb{S}}$.

Over Finite Commutative Rings With Unity

Our Results

Let $Z' = \{m_{i,j} \mid m_{i,j} \neq \bar{0}\}$. Consider $Z = Z' \cup \{\bar{1}\}$ if $\bar{1} \notin Z'$ else $Z = Z'$. Let $\langle Z \rangle_s$ be a submonoid generated by Z of the ring $\mathcal{R}$ under multiplication. We first consider the case when each row of M has exactly one non-zero entry.

Theorem

Let $\mathbb{S} \subseteq \mathcal{R}$. Suppose each row of $M(\mathcal{R})$ contains at most one non-zero entry. Then, $\mathbb{S}$ is a format preserving set with respect to M if and only if there exists a set $H \subseteq \mathbb{S}$ such that $\mathbb{S} = \bigcup_{s \in H} s\langle Z \rangle_s$.

Our Results

Define the following set

$$\mathbb{R} = \{k_1\alpha_1 + k_2\alpha_2 + \cdots + k_r\alpha_r \mid r \geq 0, k_i \geq 1, \alpha_i \in \langle Z \rangle_s\}$$

with the convention that if $r = 0$, the sum over the empty list is $\bar{0}$. It is not hard to check that the set $\mathbb{R}$ is in fact the smallest ring containing entries of Z. Note that Z contains $\bar{1}$ and therefore $\bar{1} \in \mathbb{R}$ too.

Theorem

The following statements are equivalent.

1. $\mathbb{S} \subseteq \mathcal{R}$ *is a format preserving set with respect to* M *and* $\mathbb{S}$ *is closed under* $+$.
2. $\mathbb{S}$ *is a module (unital) over the ring* $\mathbb{R}$.
3. $\mathbb{S}$ *is closed under* $+$ *and for all* $s \in \mathbb{S}$ *and* $\alpha \in \mathbb{R}, s\alpha \in \mathbb{R}$.

Format Preserving Sets with respect to MDS Matrices over Rings

Our Results

Suppose $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}$. Let $(\mathbb{F}_{{p_i}^{\alpha_i}}, +_i, \cdot_i)$ be fields for $1 \leq i \leq r$. For notational convenience, we simply denote $+_i$ and $\cdot_i$ by $+$ and $\cdot$ respectively if it is clear from the context. Then the ring $(\mathcal{R}, +, \cdot)$ is defined as

$$\mathcal{R} = \mathbb{F}_{p_1^{\alpha_1}} \times \mathbb{F}_{p_2^{\alpha_2}} \times \cdots \times \mathbb{F}_{p_r^{\alpha_r}},$$

where

$$(a_1, a_2, \cdots, a_r) + (b_1, b_2, \cdots, b_r) = (a_1 + b_1, a_2 + b_2, \cdots, a_r + b_r)$$

and

$$(a_1, a_2, \cdots, a_r) \cdot (b_1, b_2, \cdots, b_r) = (a_1 \cdot b_1, a_2 \cdot b_2, \cdots, a_r \cdot b_r)$$

It is easy to check that $\mathcal{R}$ is a commutative ring with unity $(\bar{1}, \bar{1}, \cdots, \bar{1})$. The additive identity is $(\bar{0}, \bar{0}, \cdots, \bar{0})$ and the number of elements in $\mathcal{R}$ is n.

Our Results

Construction of $|\mathbb{S}| = 10^3$ wrt a 4×4 MDS matrix $M(\mathcal{R}')$.

- Take $\mathcal{R}' = \mathbb{F}_{2^3} \times \mathbb{F}_{5^3}$.
- Construct 4×4 MDS matrices $M_1(\mathbb{F}_{2^3})$ and $M_2(\mathbb{F}_{5^3})$
- Let $m_{i,j}^{(1)}$ and $m_{i,j}^{(2)}$ for $1 \leq i, j \leq 4$ be the entries of M_1 and M_2.
- Construct $M(\mathcal{R}')$ as follows:

$$\begin{bmatrix} (m_{1,1}^{(1)}, m_{1,1}^{(2)}) & (m_{1,2}^{(1)}, m_{1,2}^{(2)}) & (m_{1,3}^{(1)}, m_{1,3}^{(2)}) & (m_{1,4}^{(1)}, m_{1,4}^{(2)}) \\ (m_{2,1}^{(1)}, m_{2,1}^{(2)}) & (m_{2,2}^{(1)}, m_{2,2}^{(2)}) & (m_{2,3}^{(1)}, m_{2,3}^{(2)}) & (m_{2,4}^{(1)}, m_{2,4}^{(2)}) \\ (m_{3,1}^{(1)}, m_{3,1}^{(2)}) & (m_{3,2}^{(1)}, m_{3,2}^{(2)}) & (m_{3,3}^{(1)}, m_{3,3}^{(2)}) & (m_{3,4}^{(1)}, m_{3,4}^{(2)}) \\ (m_{4,1}^{(1)}, m_{4,1}^{(2)}) & (m_{4,2}^{(1)}, m_{4,2}^{(2)}) & (m_{4,3}^{(1)}, m_{4,3}^{(2)}) & (m_{4,4}^{(1)}, m_{4,4}^{(2)}) \end{bmatrix}$$

- It is easy to check that M will be MDS.
- Take $\mathbb{S} = \mathcal{R}'$.

Our Results

Construction of $|\mathbb{S}| = 26^3$ wrt a 4×4 MDS matrix $M(\mathcal{R}')$.

- Take $\mathcal{R}' = \mathbb{F}_{2^3} \times \mathbb{F}_{13^3}$.
- Construct 4×4 MDS matrices $M_1(\mathbb{F}_{2^3})$ and $M_2(\mathbb{F}_{13^3})$
- Let $m_{i,j}^{(1)}$ and $m_{i,j}^{(2)}$ for $1 \leq i, j \leq 4$ be the entries of M_1 and M_2.
- Construct $M(\mathcal{R}')$ as follows:

$$\begin{bmatrix} (m_{1,1}^{(1)}, m_{1,1}^{(2)}) & (m_{1,2}^{(1)}, m_{1,2}^{(2)}) & (m_{1,3}^{(1)}, m_{1,3}^{(2)}) & (m_{1,4}^{(1)}, m_{1,4}^{(2)}) \\ (m_{2,1}^{(1)}, m_{2,1}^{(2)}) & (m_{2,2}^{(1)}, m_{2,2}^{(2)}) & (m_{2,3}^{(1)}, m_{2,3}^{(2)}) & (m_{2,4}^{(1)}, m_{2,4}^{(2)}) \\ (m_{3,1}^{(1)}, m_{3,1}^{(2)}) & (m_{3,2}^{(1)}, m_{3,2}^{(2)}) & (m_{3,3}^{(1)}, m_{3,3}^{(2)}) & (m_{3,4}^{(1)}, m_{3,4}^{(2)}) \\ (m_{4,1}^{(1)}, m_{4,1}^{(2)}) & (m_{4,2}^{(1)}, m_{4,2}^{(2)}) & (m_{4,3}^{(1)}, m_{4,3}^{(2)}) & (m_{4,4}^{(1)}, m_{4,4}^{(2)}) \end{bmatrix}$$

- It is easy to check that M will be MDS.
- Take $\mathbb{S} = \mathcal{R}'$.

Future Work

- Full characterisation of format preserving sets over rings.

Thank You