UFLM: A unified framework for Feistel structure and Lai-Massey structure

Zhengyi Dai, Chun Guo and Chao Li

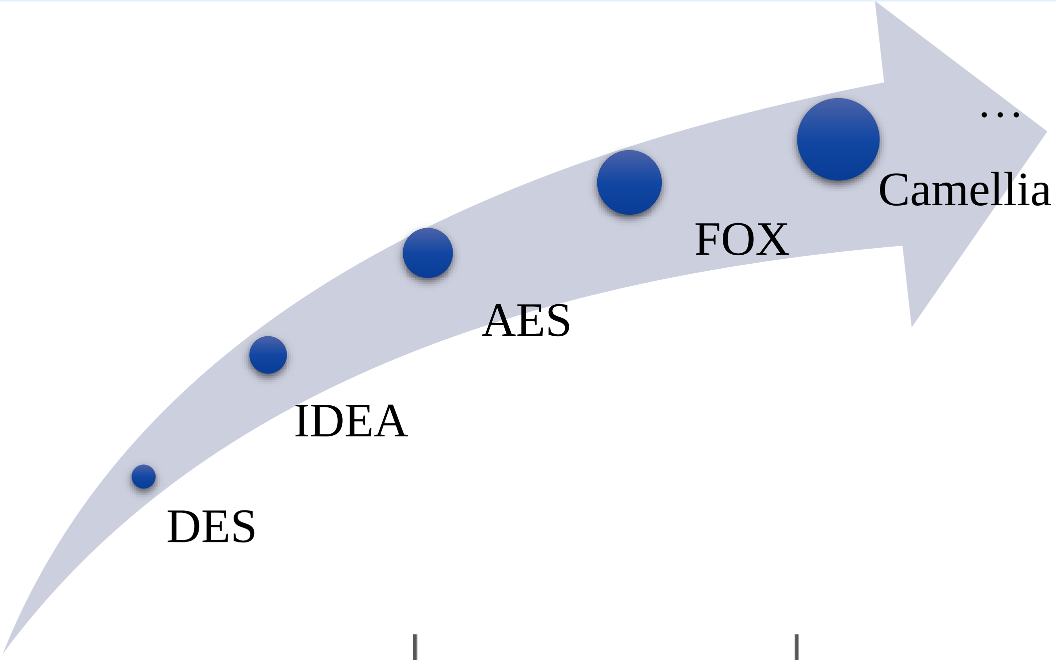
National University of Defense Technology and Shandong University

Dec 19th 2024

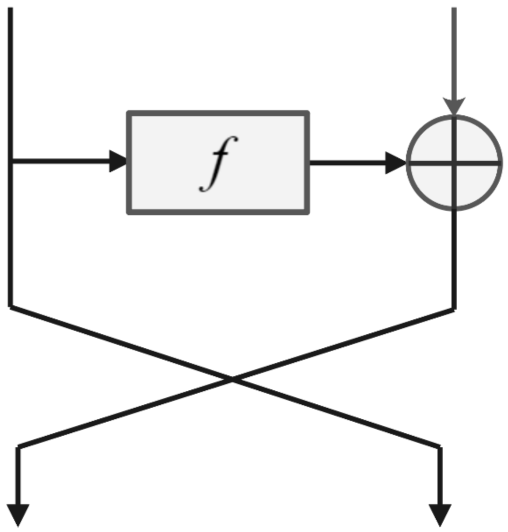
Outline

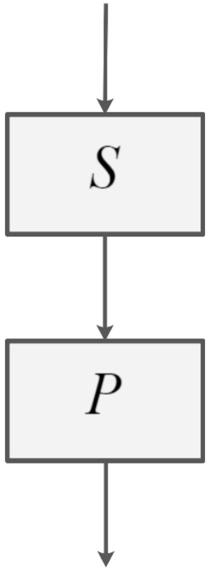
1. Introduction
2. Properties of Lai-Massey structure
3. Design and cryptanalysis of framework UFLM
4. CCA security of UFLM
5. Conclusion and future work

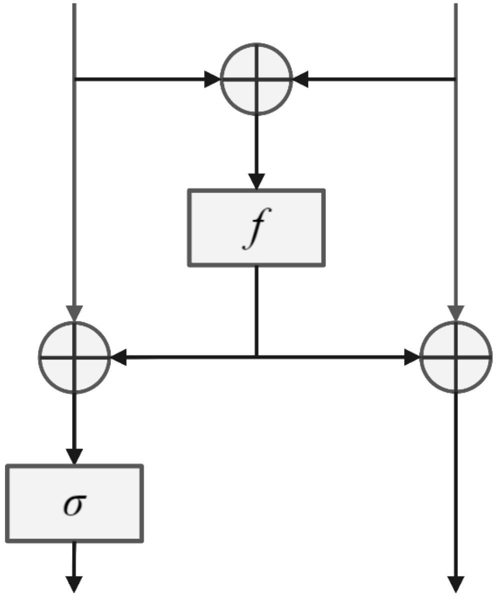
The design of block ciphers



- Confusion: Non-linear components (e.g. S-box)
- Diffusion: Linear components (e.g. MDS matrix)
- Cipher structure: Feistel structure, SP network, Lai-Massey structure, Generalized Feistel structure

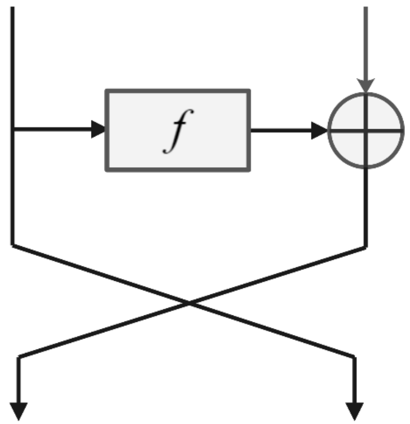


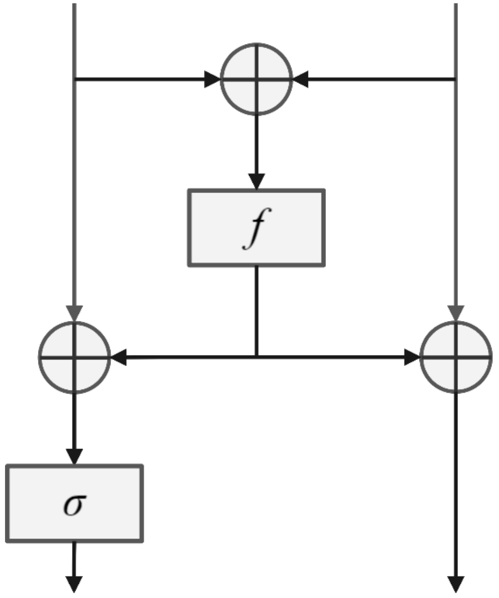




1.2 Comparison between Feistel structure and Lai-Massey structure

Comparison		Feistel structure	Lai-Massey structure
Similarities		Two equal-sized branches.	
		The f-function may not necessarily be invertible.	
		CPA security: 3 rounds CCA security: 4 rounds	
Differences	Design	The input and output of f-function are related to only one branch.	The input and output of f-function are related to two branches.
		Branch permutation	Orthomorphic permutation
	Distinguishers	5-round impossible differentials	FOX block cipher: 4-round impossible differentials

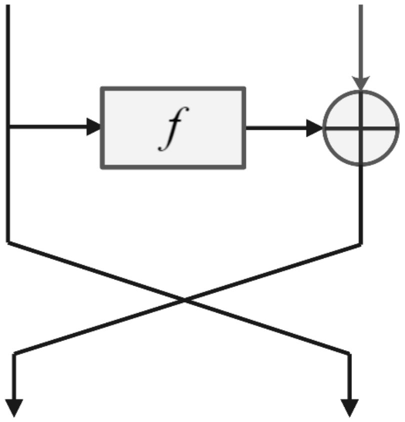




Observation: There is always longer impossible differentials for block ciphers when considering the details of f-functions.

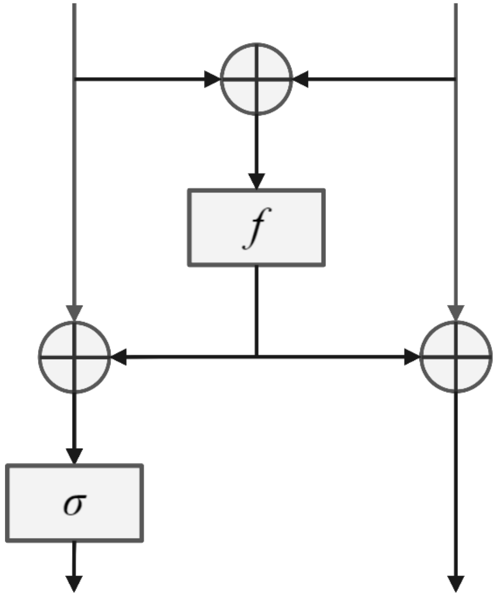
1.3 Several questions

Question 1: The number of rounds of impossible differentials for Lai-Massey structure may be limited to 4 rounds. From the perspective of design, what factors influence the number of rounds of distinguishers?



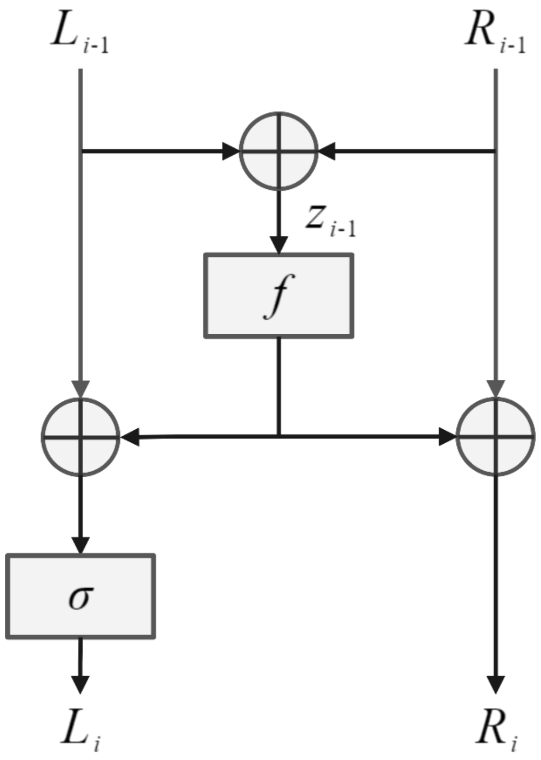
DCC 2011 Quasi-Feistel construction: consistency between Feistel and Lai-Massey constructions regarding CPA and CCA security results;

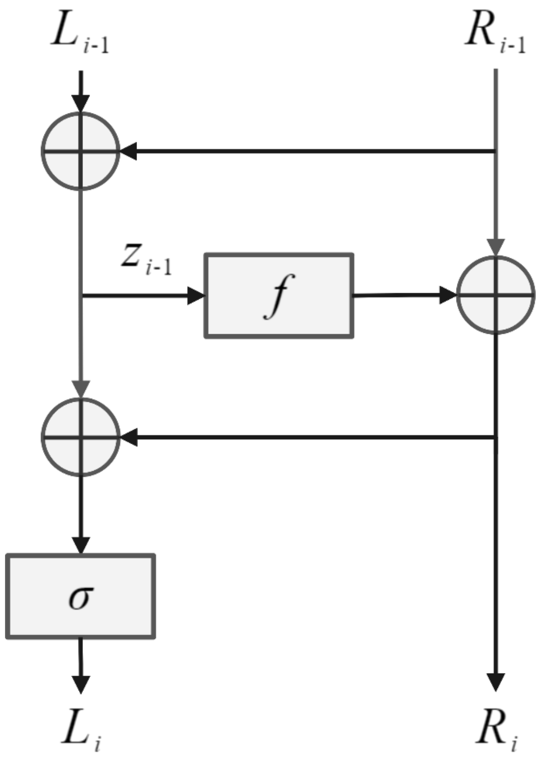
TIT 2023 Unified structure: Feistel-like structures with a single f-function.

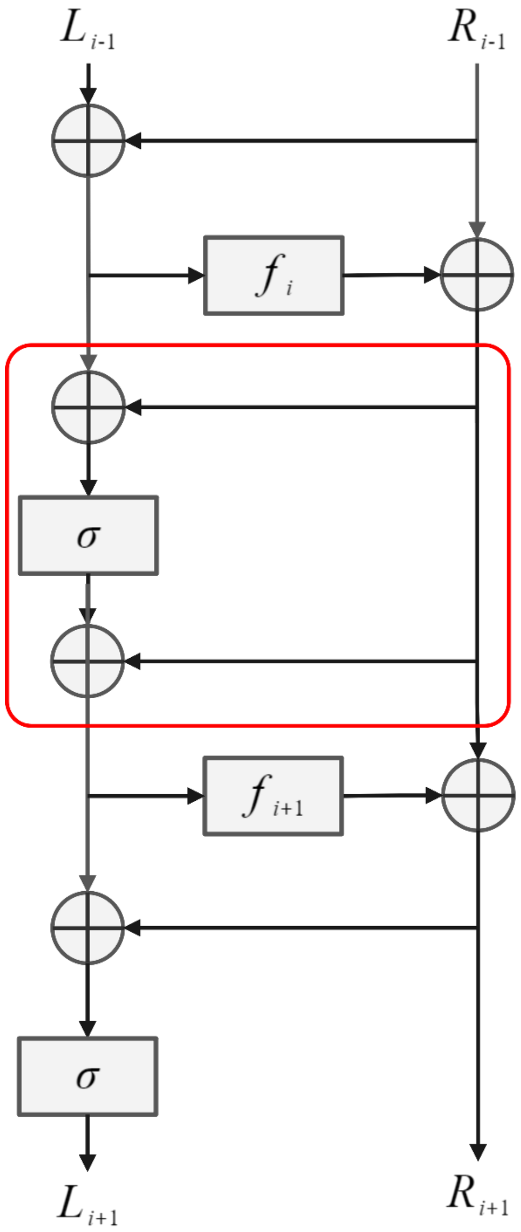


Question 2: Can we reconsider the differences in distinguishers and provable security between Feistel and Lai Massey structures from a unified framework?

2.1 Lai-Massey structure and its another representation

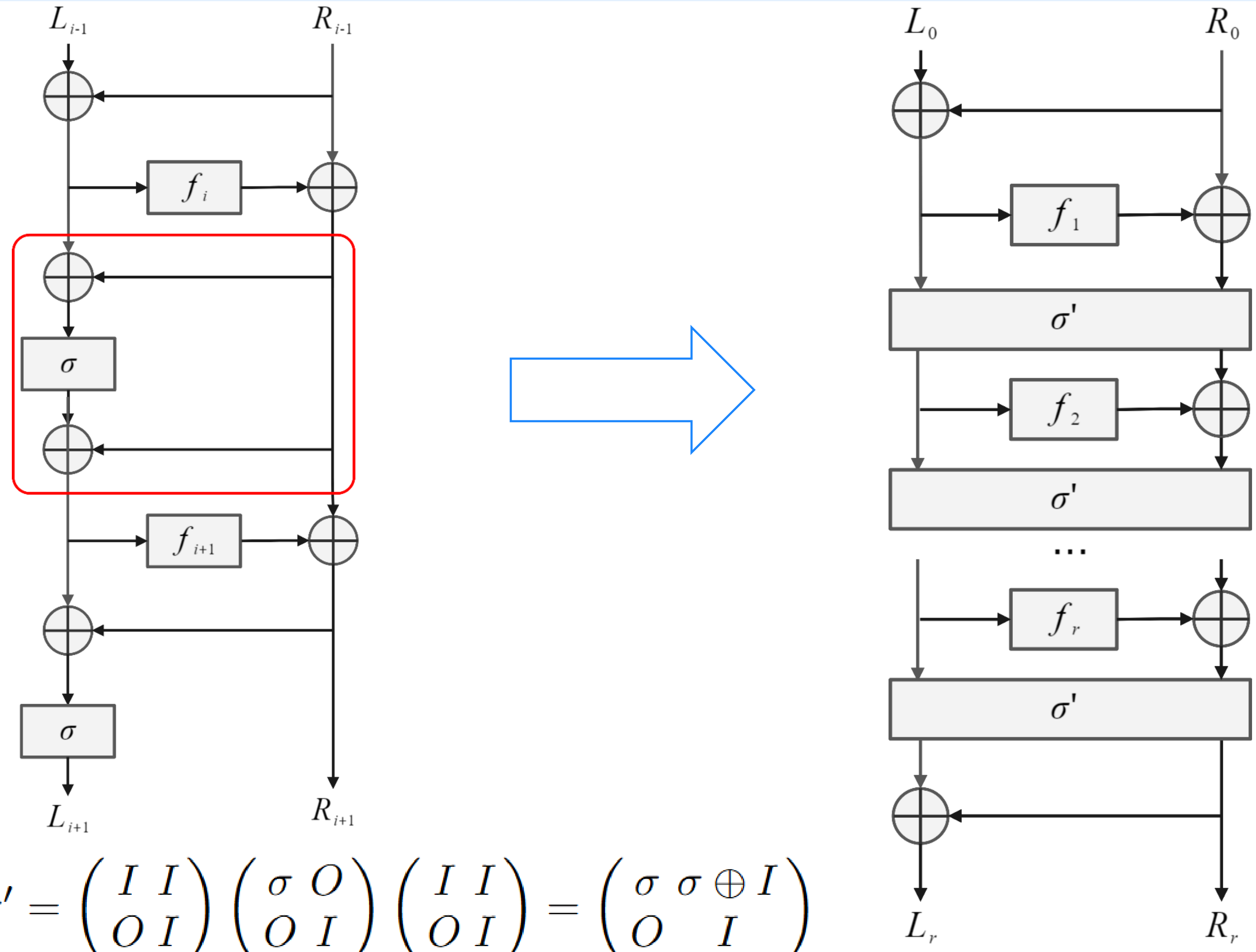






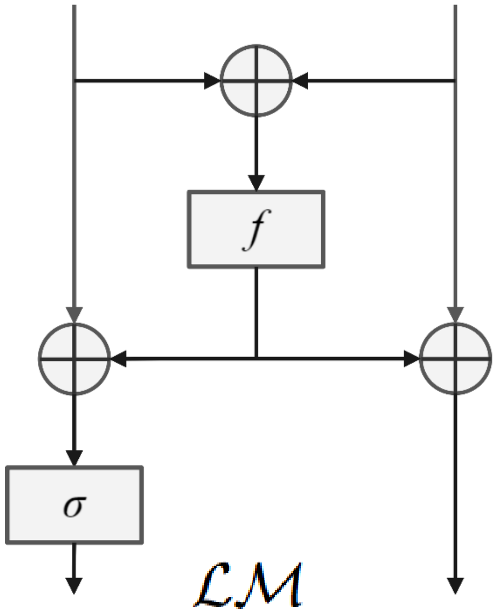
$$
\begin{cases}
z_{i-1} = L_{i-1} \oplus R_{i-1}, \\
L_i = \sigma(L_{i-1} \oplus f(z_{i-1})), \\
R_i = R_{i-1} \oplus f(z_{i-1}).
\end{cases}
$$

2.2 The r-round iteration of Lai-Massey structure

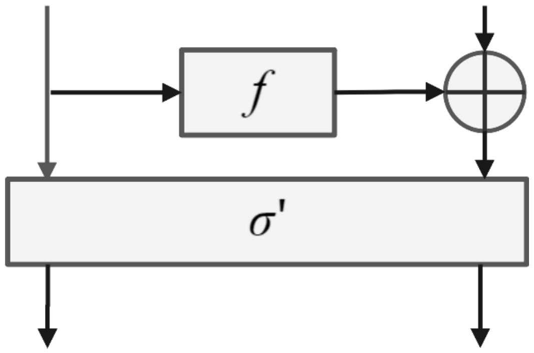


$$\sigma' = \begin{pmatrix} I & I \\ O & I \end{pmatrix} \begin{pmatrix} \sigma & O \\ O & I \end{pmatrix} \begin{pmatrix} I & I \\ O & I \end{pmatrix} = \begin{pmatrix} \sigma & \sigma \oplus I \\ O & I \end{pmatrix}$$

2.3 Lai-Massey structure and its equivalent structure



$\mathcal{LM}$



$\mathcal{ELM}$

$$\mathcal{LM}^{(r)} = \begin{pmatrix} I & I \\ O & I \end{pmatrix} \circ \mathcal{ELM}^{(r)} \circ \begin{pmatrix} I & I \\ O & I \end{pmatrix}$$

The differences between the Lai-Massey and Feistel structures in design and security are attributed to different properties of orthomorphic permutation and branch permutation.

2.4 The properties of orthomorphic permutation

Definition 1: Let (G, +) be a finite abelian group and σ: G $\mapsto$ G be a mapping from G to G. If σ and $x \mapsto \sigma(x) - x$ are both permutations, then σ is called an orthomorphic permutation.

Set G as F_2^n, the group operation as $\oplus$, and the mapping σ as a linear orthomorphic permutation.

Property 1: For a linear orthomorphic permutation σ , we have ord(σ) ≥ 3.

Property 2: The linear mapping $x \mapsto \sigma^2(x) \oplus x$ is a permutation.

The order of branch permutation is 2, while the order of an orthomorphic permutation is at least 3.

2.5 Conjugated equivalence

Definition 2: Suppose M, N are $n \times n$ invertible matrices over F_2, if there exists an $n \times n$ invertible matrix P over F_2 , such that $P^{-1}MP = N$, then matrix M is said to be conjugated equivalent to N, denoted as $M \sim N$.

Property 3: Suppose M, N are $n \times n$ invertible matrices over F_2 , if M is conjugated equivalent to N, then ord(M) = ord(N).

2.6 Examples

Example 1: There are six 2×2 invertible matrices over F_2.

Matrices M_5 and M_6 are orthomorphic permutations.

Other matrices are not orthomorphic permutations.

$$M_1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, M_2 = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, M_3 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix},$$

$$M_4 = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, M_5 = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}, M_6 = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}.$$

$\mathrm{ord}(M_5) = \mathrm{ord}(M_6) = 3,$

$\mathrm{ord}(M_2) = \mathrm{ord}(M_3) = \mathrm{ord}(M_4) = 2,$

$\mathrm{ord}(M_1) = 1.$

Example 2: For a linear orthomorphic permutation σ,

$\mathrm{ord}(\sigma) = \mathrm{ord}(\sigma').$

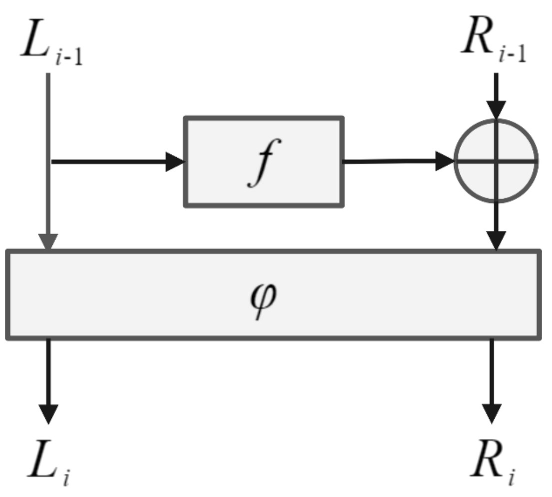
$$\sigma' = \begin{pmatrix} I & I \\ O & I \end{pmatrix} \begin{pmatrix} \sigma & O \\ O & I \end{pmatrix} \begin{pmatrix} I & I \\ O & I \end{pmatrix} = \begin{pmatrix} \sigma & \sigma \oplus I \\ O & I \end{pmatrix}$$

Example 3: As shown in Example 1, there are three equivalence classes:

$$\{M_1\}, \{M_2, M_3, M_4\}, \{M_5, M_6\}.$$

3.1 The framework UFLM

The framework UFLM is a collection of cipher structures, including Feistel and Lai-Massey structures.



$$\begin{pmatrix} L_i \\ R_i \end{pmatrix} := \varphi \begin{pmatrix} L_{i-1} \\ R_{i-1} \oplus f(L_{i-1}) \end{pmatrix}$$

UFLM instance: $\mathcal{U}_\varphi = \{E_{f,\varphi} \mid f: F_2^n \mapsto F_2^n\}$. $E_{f,\varphi}$ is a single-round block cipher employing the instance $\mathcal{U}_\varphi$.

If φ is branch permutation, then the instance is Feistel structure.

If $\varphi = \sigma'$, then the instance is equivalent Lai-Massey structure.

UFLM construction: $\mathcal{UFLM} = \{\mathcal{U}_\varphi \mid \varphi: F_2^{2n} \mapsto F_2^{2n}\}$.

r-round UFLM instance $\mathcal{U}_\varphi^{(r)}$ (construction $\mathcal{UFLM}^{(r)}$): the r-fold composition of $\mathcal{U}_\varphi$ ($\mathcal{UFLM}$)

The f-functions adopted in each round are considered as (secret) random functions.

3.2 Research object

$$A=\left(I\ O\right),B=\left(O\ I\right),\mathcal{A}^{(r)}=\begin{pmatrix}A\\A\varphi\\\vdots\\A\varphi^{r-1}\end{pmatrix},\mathcal{B}^{(r)}=\begin{pmatrix}B\\B\varphi^{\mathrm{T}}\\\vdots\\B(\varphi^{\mathrm{T}})^{r-1}\end{pmatrix}$$

Research object: UFLM instances that satisfy the following conditions:

(1) bijective f-function; (2) $\mathcal{A}^{(2)}$ and $\mathcal{B}^{(2)}$ are full-rank; (3) ord(φ) ≥ 2.

Property 4: If $\mathcal{A}^{(2)}$ is full-rank, then there exists at least one differentially active f-function covering two consecutive rounds for UFLM instances.

Property 5: If $\mathcal{B}^{(2)}$ is full-rank, then there exists at least one linearly active f-function covering two consecutive rounds for UFLM instances.

3.3 5-round impossible differential

Theorem 1: Assume that $\mathcal{A}^{(2)}$ and $\mathcal{B}^{(2)}$ are full-rank. There exists a 5-round impossible differential $\alpha \to \varphi\alpha$ for UFLM instances where α is a non-zero solution for equation $\mathcal{A}^{(1)}x = 0$ and ord(φ) = 2.

Encryption direction:

$$\alpha \to \varphi\alpha \to \alpha \oplus \varphi B^{\mathrm{T}}\beta_1 \to \varphi\alpha \oplus B^{\mathrm{T}}\beta_1 \oplus \varphi B^{\mathrm{T}}\beta_2$$

Decryption direction:

$$\varphi\alpha \oplus B^{\mathrm{T}}\beta_3 \leftarrow \alpha \leftarrow \varphi\alpha$$

$$f_1\colon 0 \to 0$$

$$f_2\colon A\varphi\alpha \to \beta_1$$

$$f_3\colon A\varphi B^{\mathrm{T}}\beta_1 \to \beta_2$$

$$f_4\colon A\varphi\alpha \to \beta_3$$

$$\begin{pmatrix} B^{\mathrm{T}} & \varphi B^{\mathrm{T}} \end{pmatrix} \begin{pmatrix} \beta_1 \oplus \beta_3 \\ \beta_2 \end{pmatrix} = 0 \Longrightarrow \beta_2 = 0 \Longrightarrow \begin{pmatrix} A \\ A\varphi \end{pmatrix} B^{\mathrm{T}}\beta_1 = 0 \Longrightarrow \begin{matrix} B^{\mathrm{T}}\beta_1 = 0 \\ \varphi B^{\mathrm{T}}\beta_1 = 0 \end{matrix} \Longrightarrow \beta_1 = 0$$

$$\Longrightarrow A\varphi\alpha = 0$$

Contradiction!

3.4 Impossible differential cryptanalysis

Theorem 1: Assume that $\mathcal{A}^{(2)}$ and $\mathcal{B}^{(2)}$ are full-rank. There exists a 5-round impossible differential $\alpha \to \varphi\alpha$ for UFLM instances where α is a non-zero solution for equation $\mathcal{A}^{(1)}x = 0$ and ord(φ) = 2.

Corollary 1: Assume that $\mathcal{A}^{(2)}$ and $\mathcal{B}^{(2)}$ are full-rank. There exists a 4-round impossible differential $\alpha \to \varphi\alpha$ for UFLM instances where α is a non-zero solution for equation $\mathcal{A}^{(1)}x = 0$ and ord(φ) = 3.

Corollary 2: Assume that $\mathcal{A}^{(2)}$ and $\mathcal{B}^{(2)}$ are full-rank. There exists a 3-round impossible differential $\alpha \to \varphi^3\alpha$ for UFLM instances where α is a non-zero solution for equation $\mathcal{A}^{(1)}x = 0$ and ord(φ) > 3.

3.5 Zero correlation linear cryptanalysis

Theorem 2: Assume that $\mathcal{A}^{(2)}$ and $\mathcal{B}^{(2)}$ are full-rank. There exists a 5-round zero correlation linear hull $\gamma \rightarrow \varphi^{\mathrm{T}}\gamma$ for UFLM instances where γ is a non-zero solution for equation $\mathcal{B}^{(1)}x = 0$ and ord(φ) = 2.

Corollary 3: Assume that $\mathcal{A}^{(2)}$ and $\mathcal{B}^{(2)}$ are full-rank. There exists a 4-round zero correlation linear hull $\gamma \rightarrow \left(\varphi^{\mathrm{T}}\right)^{2}\gamma$ for UFLM instances where γ is a non-zero solution for equation $\mathcal{B}^{(1)}x = 0$ and ord(φ) = 3.

Corollary 4: Assume that $\mathcal{A}^{(2)}$ and $\mathcal{B}^{(2)}$ are full-rank. There exists a 3-round zero correlation linear hull $\gamma \rightarrow \left(\varphi^{\mathrm{T}}\right)^{k-3}\gamma$ for UFLM instances where γ is a non-zero solution for equation $\mathcal{B}^{(1)}x = 0$ and ord(φ) = k > 3.

3.6 Integral cryptanalysis

[SLR+15]: a nontrivial zero correlation linear hull of a block cipher always implies the existence of an integral distinguisher

Theorem 3: Assume that $\mathcal{A}^{(2)}$ and $\mathcal{B}^{(2)}$ are full-rank. If ord(φ) = 2, then there exists a 5-round integral distinguisher for UFLM instances. If ord(φ) = 3, then there exists a 4-round integral distinguisher for UFLM instances. If ord(φ) > 3, then there exists a 3-round integral distinguisher for UFLM instances.

ord(φ)	Distinguishers	Rounds	Structures
2	Impossible differential	5	Feistel structure
	Zero correlation linear hull	5	
	Integral distinguisher	5	
3	Impossible differential	4	FOX64 structure
	Zero correlation linear hull	4	
	Integral distinguisher	4	
> 3	Impossible differential	3	—
	Zero correlation linear hull	3	
	Integral distinguisher	3	

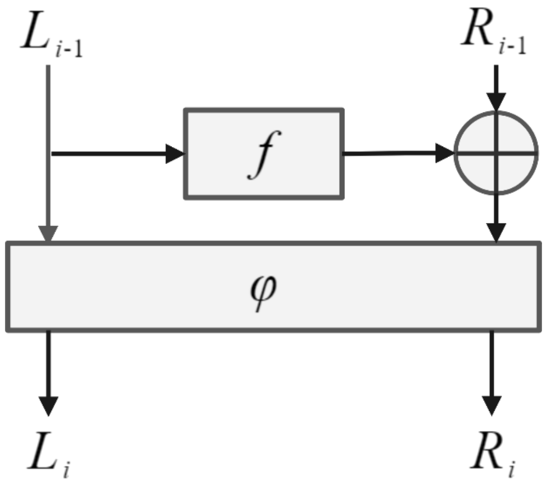
4.1 CCA-security results

The 4-round construction $\mathcal{UFLM}^{(4)}$ is CCA security up to birthday bound.

Case 1: The 4-round construction $\mathcal{UFLM}^{(4)}[f]$ adopts the same f-function in each round:

$$f_1 = f_2 = f_3 = f_4 = f.$$

Case 2: The 4-round construction $\mathcal{UFLM}^{(4)}[f_1, f_2, f_3, f_4]$ adopts independent f-functions in each round.



The last round omits φ.

Definition 3 (Good Linear Transformation): A linear transformation

$$\varphi = \begin{pmatrix} \varphi_{UL} & \varphi_{UR} \\ \varphi_{BL} & \varphi_{BR} \end{pmatrix}$$

over $F_2^{2n\times 2n}$ is said to be good if the three matrices φ_{UR}, φ_{UR}^{-1} and $\varphi_{UR} \oplus \varphi_{UR}^{-1}$ are full-rank.

Example: $\varphi = \begin{pmatrix} \sigma & \sigma \oplus I \\ O & I \end{pmatrix}$

4.2 CCA security for $\mathcal{UFLM}^{(4)}[f]$

Theorem 4: Assume $q \leq 2^n/2$, Then, for the 4-round idealized construction $\mathcal{UFLM}^{(4)}[f]$ defined upon a secret random function f and a good linear transformation φ, it holds:

$$Adv_{\mathcal{UFLM}^{(4)}}^{CCA}(q) \leq \frac{6q^2}{2^n} + \frac{q^2}{2^{2n}}$$

Interaction (q non-redundant forward/inverse queries) between an adversary D and oracles $\mathcal{UFLM}^{(4)}[f]$ or Π:

$$Q = \{\left(\left(L_0^{(1)}, R_0^{(1)}\right), \left(L_4^{(1)}, R_4^{(1)}\right)\right), \cdots, \left(\left(L_0^{(q)}, R_0^{(q)}\right), \left(L_4^{(q)}, R_4^{(q)}\right)\right)\}$$

4.3 Bound the ratio

$\mathcal{UFLM}^{(4)}[f^*] \vdash Q'$: if $\mathcal{UFLM}^{(4)}[f^*](L_0, R_0) = (L_4, R_4)$ for all $\big((L_0, R_0), (L_4, R_4)\big) \in Q'$;

$\Pi^* \vdash Q'$: if $\Pi^*(L_0, R_0) = (L_4, R_4)$ for all $\big((L_0, R_0), (L_4, R_4)\big) \in Q'$.

Fix an attainable Q,

$$\frac{\mu(Q)}{\nu(Q)} = \frac{Pr\big(f \leftarrow (F_2^n \mapsto F_2^n): \mathcal{UFLM}^{(4)}[f] \vdash Q\big)}{Pr(\Pi \leftarrow (F_2^{2n} \mapsto F_2^{2n}): \Pi \vdash Q)}$$

$$Pr(\Pi \leftarrow (F_2^{2n} \mapsto F_2^{2n}): \Pi \vdash Q) = \prod_{i=0}^{q-1} \frac{1}{2^{2n} - i}$$

$$ExtF = \{X \in F_2^n | \big((X, R_0), (L_4, R_4)\big) \in Q \ for\ some\ R_0, L_4, R_4\ or$$

$$\big((L_0, R_0), (X, R_4)\big) \in Q\ for\ some L_0, R_0, R_4\}$$

4.4 Bound the $\mu(Q)$

$$\mu(Q) = Pr\left(f \leftarrow (F_2^n \mapsto F_2^n):\ \mathcal{UFLM}^{(4)}[f] \vdash Q\right) \geq \Pr_f\left(\mathcal{UFLM}^{(4)}[f] \vdash Q \,\middle|\, \neg Bad(f)\right) \times \left(1 - \Pr_f(Bad(f))\right)$$

Given a random function f, let $Bad(f)$ be a predicate that holds if any of the following conditions is met:

1. There exists a record $\left((L_0, R_0), (L_4, R_4)\right) \in Q$ such that $\varphi_{UL} \cdot L_0 \oplus \varphi_{UR} \cdot R_0 \oplus \varphi_{UR} \cdot f(L_0) \in ExtF$ or $(\varphi^{-1})_{UL} \cdot L_4 \oplus (\varphi^{-1})_{UR} \cdot R_4 \oplus (\varphi^{-1})_{UR} \cdot f(L_4) \in ExtF$;
2. There exist distinct records $\left((L_0, R_0), (L_4, R_4)\right)$, $\left((L_0', R_0'), (L_4', R_4')\right) \in Q$, such that $L_0 \neq L_0'$, but
$$\varphi_{UL} \cdot L_0 \oplus \varphi_{UR} \cdot R_0 \oplus \varphi_{UR} \cdot f(L_0) = \varphi_{UL} \cdot L_0' \oplus \varphi_{UR} \cdot R_0' \oplus \varphi_{UR} \cdot f(L_0');$$
3. There exist distinct records $\left((L_0, R_0), (L_4, R_4)\right)$, $\left((L_0', R_0'), (L_4', R_4')\right) \in Q$, such that $L_4 \neq L_4'$, but
$$(\varphi^{-1})_{UL} \cdot L_4 \oplus (\varphi^{-1})_{UR} \cdot R_4 \oplus (\varphi^{-1})_{UR} \cdot f(L_4) = (\varphi^{-1})_{UL} \cdot L_4' \oplus (\varphi^{-1})_{UR} \cdot R_4' \oplus (\varphi^{-1})_{UR} \cdot f(L_4');$$
4. There exist two records $\left((L_0, R_0), (L_4, R_4)\right)$, $\left((L_0', R_0'), (L_4', R_4')\right) \in Q$ (not necessarily distinct) such that: $\varphi_{UL} \cdot L_0 \oplus \varphi_{UR} \cdot R_0 \oplus \varphi_{UR} \cdot f(L_0) = (\varphi^{-1})_{UL} \cdot L_4' \oplus (\varphi^{-1})_{UR} \cdot R_4' \oplus (\varphi^{-1})_{UR} \cdot f(L_4')$.

4.5 Bound the $\mu(Q)$

Lemma 1: When $q \leq 2^n/2$, we have:

$$Pr_f(Bad(f)) \leq \frac{6q^2}{2^n}.$$

If $Bad(f)$ does not hold (the probability of which has a lower bound), then $\mathcal{UFLM}^{(4)}[f] \vdash Q$ is equivalent with 2q distinct equations on the f-function.

$$Pr_f\left(\mathcal{UFLM}^{(4)}[f] \vdash Q \,\middle|\, \neg Bad(f)\right) \geq \frac{1}{(2^n)^{2q}}$$

$$\mu(Q) \geq (1 - \frac{6q^2}{2^n})\frac{1}{(2^n)^{2q}}$$

4.6 Bound the ratio

$$\frac{\mu(Q)}{\nu(Q)} = \frac{Pr\left(f \leftarrow (F_2^n \mapsto F_2^n): \mathcal{UFLM}^{(4)}[f] \vdash Q\right)}{Pr(\Pi \leftarrow (F_2^{2n} \mapsto F_2^{2n}): \Pi \vdash Q)}$$

$$\geq \left(1 - \frac{6q^2}{2^n}\right)\left(\frac{1}{(2^n)^{2q}}\right) / \prod_{i=0}^{q-1} \frac{1}{2^{2n} - i}$$

$$\geq 1 - \frac{6q^2}{2^n} - \frac{q^2}{2^{2n}}$$

⇨ $$Dist\left(\mu(Q), \nu(Q)\right) \leq \frac{6q^2}{2^n} + \frac{q^2}{2^{2n}}$$

⇨ $$Adv_{\mathcal{UFLM}^{(4)}}^{CCA}(q) \leq \frac{6q^2}{2^n} + \frac{q^2}{2^{2n}}$$

4.7 CCA security for $\mathcal{UFLM}^{(4)}[f_1, f_2, f_3, f_4]$

Theorem 5: Assume $q \le 2^n/2$, Then, for the 4-round idealized construction $\mathcal{UFLM}^{(4)}[f_1, f_2, f_3, f_4]$ defined upon four independent secret random functions f_1, f_2, f_3, f_4 and an invertible linear transformation φ, it holds:

$$Adv_{\mathcal{UFLM}^{(4)}}^{CCA}(q) \le \frac{q^2}{2^n} + \frac{q^2}{2^{2n}}$$

Corollary 5: The CCA security of the 4-round Lai-Massey construction is superior to that of the 4-round Feistel construction when utilizing the same f-function in each round.

Corollary 6: If the linear transformation φ of a 4-round UFLM} instance adopts $O - I$ block matrix, then its CCA security is identical to the 4-round Feistel construction.

4.8 CCA security for $\mathcal{UFLM}^{(4)}[p]$ and $\mathcal{UFLM}^{(4)}[p_1, p_2, p_3, p_4]$

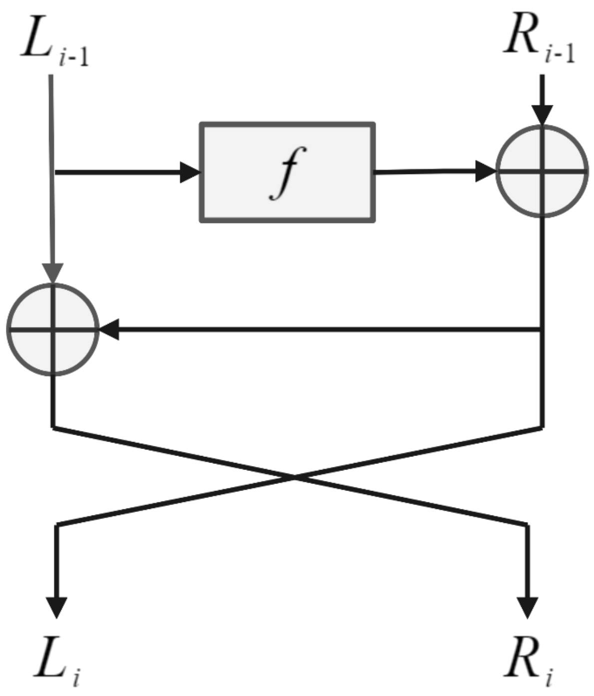
Theorem 6: Assume $q \le 2^n/2$, Then, for the 4-round idealized construction $\mathcal{UFLM}^{(4)}[p]$ defined upon a secret random permutation p and a good linear transformation φ, it holds:

$$Adv_{\mathcal{UFLM}^{(4)}}^{CCA}(q) \le \frac{14q^2}{2^n} + \frac{q^2}{2^{2n}}$$

Theorem 7: Assume $q \le 2^n/2$, Then, for the 4-round idealized construction $\mathcal{UFLM}^{(4)}[p_1, p_2, p_3, p_4]$ defined upon four independent secret random permutations p_1, p_2, p_3, p_4 and an invertible linear transformation φ, it holds:

$$Adv_{\mathcal{UFLM}^{(4)}}^{CCA}(q) \le \frac{3q^2}{2^n} + \frac{q^2}{2^{2n}}$$

4.9 Proposal for a UFLM instance



$$\begin{cases} L_i = R_{i-1} \oplus f(L_{i-1}), \\ R_i = L_{i-1} \oplus R_{i-1} \oplus f(L_{i-1}). \end{cases}$$

Proposition 1: There exists a 4-round impossible differential $(0, \alpha) \rightarrow (\alpha, \alpha)$ where $\alpha \neq 0$.

Proposition 2: There exists a 4-round zero correlation linear hull $(\gamma, 0) \rightarrow (\gamma, \gamma)$ where $\gamma \neq 0$, which leads to a 4-round integral distinguisher.

Proposition 3: The 4-round construction is CCA-secure when utilizing different f-functions in each round.

5.1 Conclusion

- The framework UFLM is proposed for reassessing the security of Feistel and Lai-Massey structures.
- The linear transformation employed in a cipher structure is directly related to its security, which provides guidance for the design and cryptanalysis.
  - The order of branch permutation is 2 and the order of an orthomorphic permutation is at least 3;
  - The number of rounds of distinguishers for UFLM instances with various orders of linear transformations;
  - CCA security of 4-round UFLM construction;
  - Proposal for a UFLM instance.
- Lai-Massey structure does benefit from the orthomorphic permutation in both aspects.

5.2 Future work

- When evaluating the number of rounds of distinguishers, UFLM instances that employ bijective f-functions are considered.
  - The issue of non-invertible f-functions remains a topic for subsequent investigation.

- If f-function is composed of multiple smaller components, such as S-boxes, it is feasible to convert a UFLM instance into an alternative structure with several smaller-scale S-boxes.
  - Security evaluation for structures with multiple branches and multiple f-functions.

Thanks for your attention