KU LEUVEN

Generic Attacks on Lai-Massey Structures

Betül Aşkın Özdemir, Tim Beyne and Vincent Rijmen

Selected Areas in Cryptography 2026

ESAT

COSIC

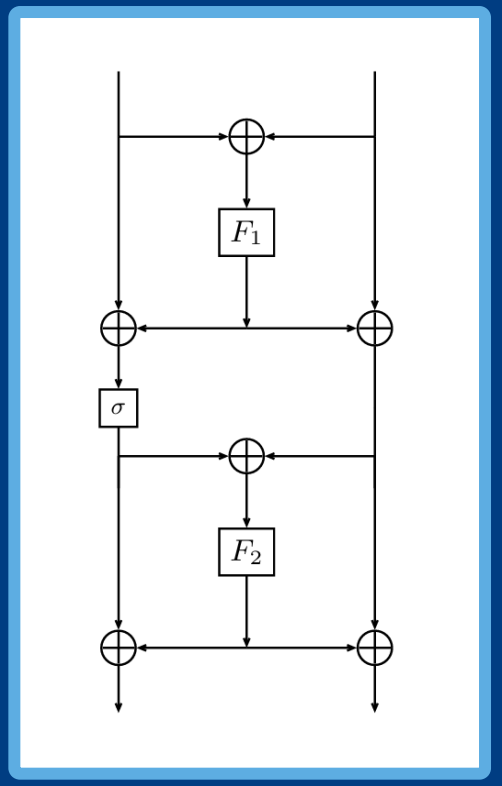
Outline

Part I: Evaluating Cipher Security

Multidimensional linear cryptanalysis

Part II: Our Contributions

Multidimensional linear distinguisher
Message recovery attack
Key recovery attack



Part I

Evaluating Cipher Security

Security testing and cryptanalysis

Linear Cryptanalysis

Multidimensional linear cryptanalysis

Linear Cryptanalysis: Linear Approximations

Finding probabilistic linear relations between plaintext, ciphertext, and key bits

$$\alpha.x \oplus \beta.F(x,k) = 0$$

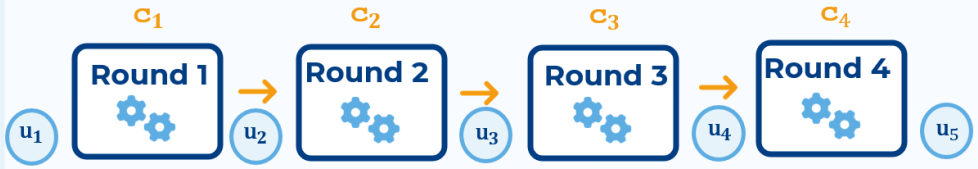
Holds with probability Pr

The Correlation

$$C(\alpha,\beta) = 2.(Pr[\alpha.x \oplus \beta.F(x) = 0] - \tfrac{1}{2})$$

± Correlation Sign

$$(-1)^{u^T k}$$



$$C_{total} = \prod c_i$$

Multiple Linear Cryptanalysis

Using **multiple linear approximations** simultaneously to improve attack efficiency

Why relying on a single linear approximation is insufficient for modern block ciphers?

Data Complexity

Multiple LC

Set of linear approximations:

$$(u_1, v_1), (u_2, v_2), \dots, (u_m, v_m)$$

How does it work?

- **Multiple linear approximations are evaluated together**
- **Each approximation contributes to the correlations**
- **Combined information improves distinguishing capability**

Lower data complexity!

"Linear Cryptanalysis Using Multiple Approximations"

Multidimensional Linear Cryptanalysis

Using multiple linear approximations that form a **vector space**

Why is relying on a single linear approximation insufficient for modern block ciphers?

Data Complexity

The Solution: Multidimensional LC

Vector Space Λ

A set of linear approximations:

$$(u, v) \in \Lambda$$

Multidimensional Analysis Process

- Define **the vector space** Λ of masks
- Calculate **correlations** for each mask and combine them
- Apply the test statistic to obtain a **distinguisher**
- **Possible extensions**: message and/or key recovery

"Multidimensional Linear Cryptanalysis of Reduced Round Serpent"

Multidimensional LC: Distinguisher

Known correlations vs **Unknown correlations**

Known Correlations

- LLR test
- Lower Data Complexity

Data Complexity:

$$q \approx \frac{1}{\mathrm{Cap}(\Lambda)}$$

Optimal
Known signs

Unknown Correlations

- χ^2 test
- Higher Data complexity

Data Complexity:

$$q \approx \frac{\sqrt{|\Lambda|}}{\mathrm{Cap}(\Lambda)}$$

Higher
Unknown signs

$$\mathrm{Cap}(\Lambda) = \Sigma c^2$$

Difference: $\sqrt{|\Lambda|}$ factor

"How Far Can We Go Beyond Linear Cryptanalysis?" and "An Experiment on DES Statistical Cryptanalysis"

Part II

Contributions

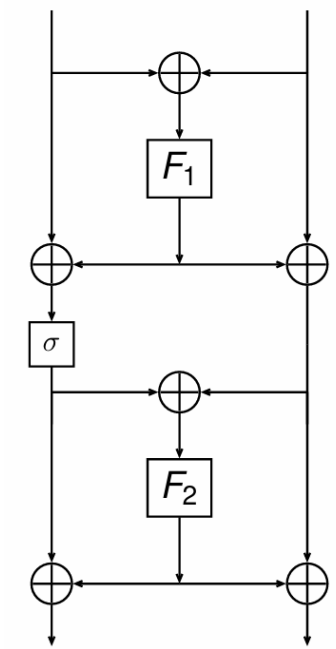
Generic multidimensional linear cryptanalysis of Lai-Massey structures

Roadmap

1. Multidimensional linear distinguisher
2. Message recovery attack
3. Key recovery attack

Lai-Massey Structures: The Concept

Lai-Massey Structures



Round functions

1. Chosen independently and randomly
2. Invertible
3. Key-dependent

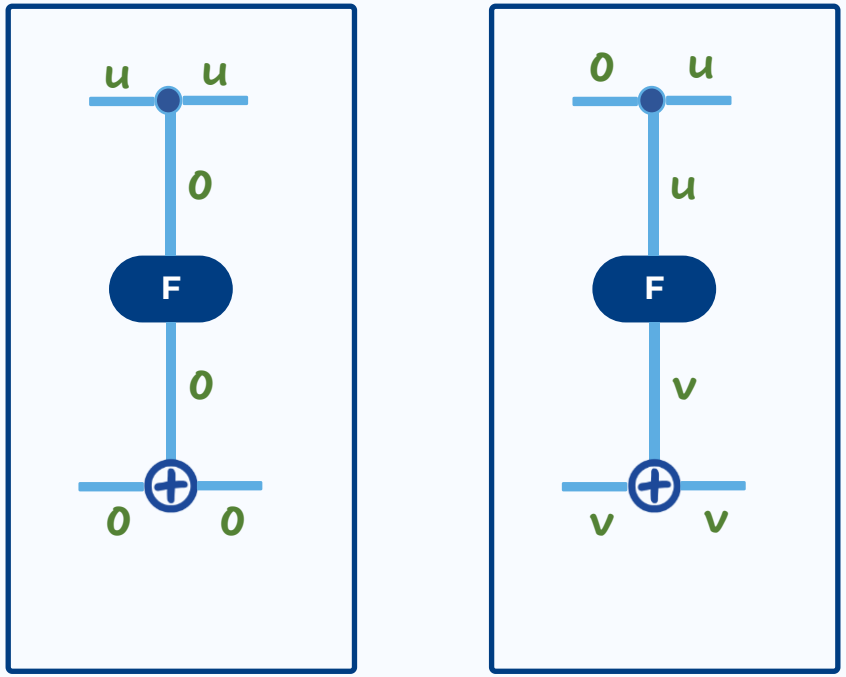
Time to analyze!

Lai-Massey Structures: The Core Idea

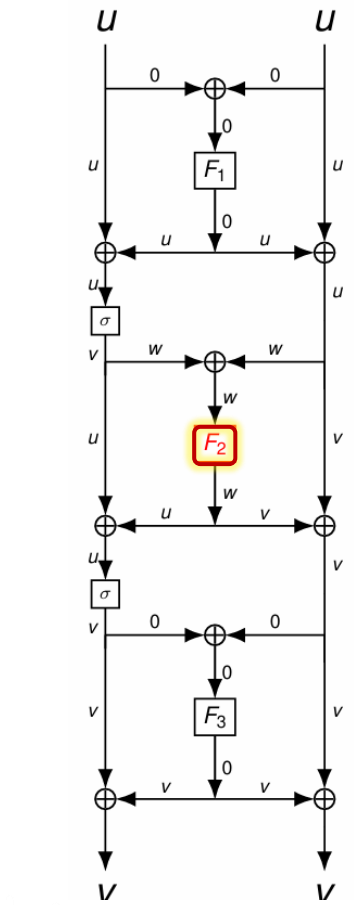
How does the attack work?

1. Invertible round functions
2. Non-zero mask → Non-zero mask
3. Key dependency

RESULT: Stronger statistical tests



Lai-Massey Structures : Distinguisher



What is the data-complexity?

1 **Vector space:** $w = u \oplus v$

$$\Lambda = \{((u,u),(v,v)) \mid w \in F_2^n\}$$

2 **Correlation of the trail:** $c \approx 2^{-n/2}$

$$C = \prod_{1}^{\lfloor r/2 \rfloor} c$$

3 **Capacity of the approximations:**

$$\text{Cap}(\Lambda) \approx 2^n C^2 \approx 2^{n-n\lfloor r/2 \rfloor}$$

χ^2 *test:* $q \approx 2^{n\lfloor r/2 \rfloor - n/2}$

Lai-Massey Structures: Distinguishing Attack

Data complexity for multidimensional distinguishing attacks

Data complexity

		Our results	Prior results*
3-round	KPA	$\approx 2^{n/2}$	$\approx 2^{n}$
4-round	CPA	$\approx 2^{n/2}$	$\approx 2^{n}$
5-round	KPA	$\approx 2^{3n/2}$	$\approx 2^{7n/4}$
6-round	CPA	$\approx 2^{2n}$	–

* “Pseudorandomness Analysis of the (extended) Lai-Massey Scheme” and “Generic Attacks on the Lai–Massey Scheme”

Part II

Contributions

Generic multidimensional linear cryptanalysis of Lai-Massey structures

Roadmap

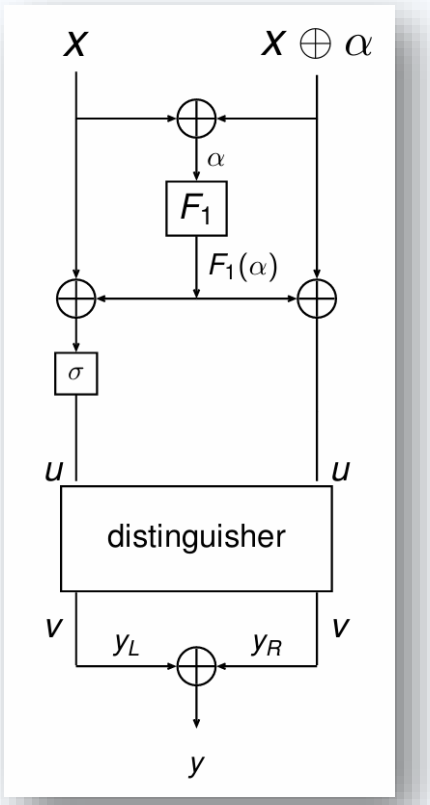
1 Multidimensional linear distinguisher

2 **Message recovery attack**

3 Key recovery attack

Lai-Massey Structures: Extension to Message Recovery

Extending multidimensional linear distinguishers to the message recovery attack



$\alpha_1 \stackrel{?}{=} \alpha_2$

3-round distinguisher

4-round message recovery*

$q \approx 2^{n/2}$

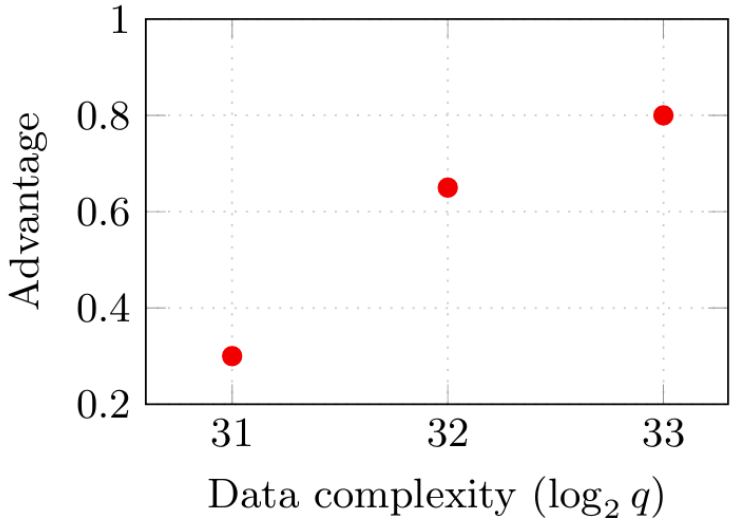
* “Message-recovery attacks on Feistel-based format preserving encryption”

Lai-Massey Structures: Experiment on SPC

Two-sample χ^2 test

$$f_1[E_k(x^i, x^i \oplus \alpha_1)]$$
$$f_2[E_k(x^j, x^j \oplus \alpha_2)]$$

for $i = 0$ *to* $q/2$ **do**
$$s \leftarrow \sum_i \frac{(f_1(z_i) - f_2(z_i))^2}{f_1(z_i) + f_2(z_i)};$$
end



Part II

Contributions

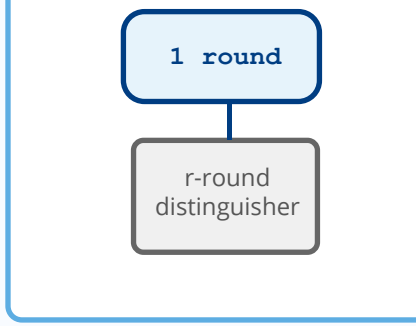
Generic multidimensional linear cryptanalysis of Lai-Massey structures

Roadmap

1. Multidimensional linear distinguisher
2. Message recovery attack
3. **Key recovery attack**

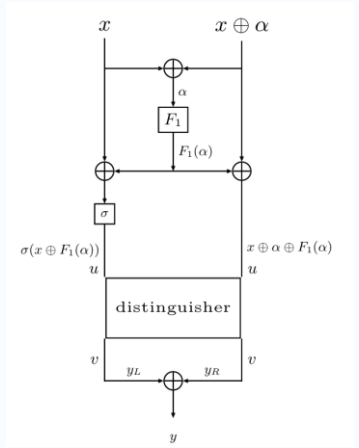
Feistel Structures: Key Recovery

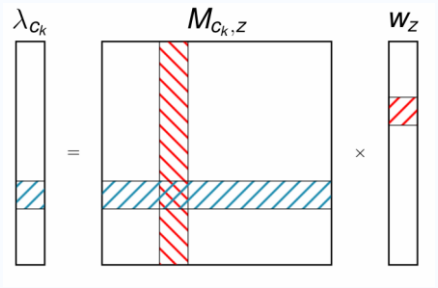
Extending multidimensional linear distinguishers to recover the secret key



Compute statistic

Matrix-vector product using FFT





Round key (n) **Block Size (n)** **Rounds (r)**

FFT Optimization*

$\mathcal{O}(n2^n + q)$

Matrix-vector product

Data complexity

Naive method

$\mathcal{O}(q2^n)$

Matsui's method

$\mathcal{O}(n2^{2n} + q)$

FFT optimization significantly reduces time complexity

* "Improving the Time Complexity of Matsui's Linear Cryptanalysis"

Lai-Massey Structures: Complexity bounds

Distinguishing and key-recovery attack complexity bounds for GFC

$$\mathcal{O}\left(n\,2^{r'n} + q\right)$$

$q \approx 2^{n/2}$

Distinguishing attack rounds

$r = 3$

Key recovery attack rounds

$r + r' = 4, \quad K = 2n \;\; and \;\; T = n2^{n}$

$r + r' = 6, \quad K = 4n \;\; and \;\; T = n2^{3n}$

$q \approx 2^{3n/2}$

Distinguishing attack rounds

$r = 5$

Key recovery attack rounds

$r + r' = 6, \quad K = 2n \;\; and \;\; T = n2^{n}$

$r + r' = 8, \quad K = 4n \;\; and \;\; T = n2^{3n}$

5-round distinguisher can be extended to an 8-round key recovery attack

Conclusion

Generic Multidimensional linear cryptanalysis of Lai-Massey structures:

1 **Multidimensional linear distinguisher**

6-round generic distinguishing attack in the CPA model

2 **Message recovery attack**

Message recovery attack with the same data complexity as the distinguisher

3 **Key recovery attack**

8-round key-recovery attack

References

1. Kaliski, B.S., Robshaw, M.J.B.: Linear Cryptanalysis Using Multiple Approximations. In: Desmedt, Y.G. (ed.) Advances in Cryptology — CRYPTO ’94. pp. 26–39

2. Hermelin, M., Cho, J.Y., Nyberg, K.: Multidimensional Linear Cryptanalysis of Reduced Round Serpent. In: Mu, Y., Susilo, W., Seberry, J. (eds.) Information Security and Privacy. pp. 203–215.

3. Baignères, T., Junod, P., and Vaudenay, S. How Far Can We Go Beyond Linear Cryptanalysis? In Advances in Cryptology-ASIACRYPT 2004 (2004), vol. 3329 pp. 432–450.

4. Vaudenay, S. An Experiment on DES Statistical Cryptanalysis. In Conference on Computer and Communications Security (1996).

5. Luo, Y., Lai, X., Gong, Z.: Pseudorandomness Analysis of the (extended) Lai-Massey Scheme. Inf. Process. Lett. 111, 90–96 (2010).

6. Luo, Y., Lai, X., Zhou, Y.: Generic Attacks on the Lai–Massey Scheme. Designs, Codes and Cryptography 83, 407– 423, 2016.

7. Bellare, M., Hoang, V.T., Tessaro, S.: Message-recovery attacks on Feistel-based format preserving encryption. In: Proceedings of the 2016 ACM SIGSAC. p. 444–455. CCS ’16.

8. Collard, B., Standaert, F.X., Quisquater, J.J.: Improving the Time Complexity of Matsui’s Linear Cryptanalysis. In: Nam, K.H., Rhee, G. (eds.) Information Security and Cryptology- ICISC 2007. pp. 77–88

Multidimensional Linear Distinguishers

Applying Theorem 1 to the vector space $V = \Lambda$ with the random variable $\mathbf{z} = (\mathbf{x}, F(\mathbf{x}))$, where $\mathbf{x}$ is uniformly random over $\mathbb{F}_2^n$ and is a function $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$, yields the following result:

$$\Pr\left((\mathbf{x}, F(\mathbf{x})) = (t_1, t_2) \bmod \Lambda^{\perp}\right) = \frac{1}{|\Lambda|} \sum_{(u,v)\in\Lambda} (-1)^{u^T t_1 + v^T t_2} C^F_{v,u}. \tag{1}$$

where $\Lambda^{\perp} = \left\{(\mathbf{x}, F(\mathbf{x})) \in \mathbb{F}_2^n \times \mathbb{F}_2^n \mid u^T\mathbf{x} + v^T F(\mathbf{x}) = 0 \text{ for all } (u, v) \in \Lambda\right\}$. In other words, the correlations $C^{\mathrm{F}}_{v,u}$ for $(u, v) \in \Lambda$ completely determine the probability distribution of the linear projections of plaintext and ciphertext, which defines a linear map from $\mathbb{F}_2^n \times \mathbb{F}_2^n$ to the quotient space $\mathbb{F}_2^n \times \mathbb{F}_2^n/\Lambda^{\perp}$.

Multidimensional Linear Distinguishers

Let V be a subspace of $\mathbb{F}_2^n$.

1. **Quotient Space.** The *quotient space* $\mathbb{F}_2^n/V$ is defined as

$$\mathbb{F}_2^n/V = \{x + V \mid x \in \mathbb{F}_2^n\},$$

where $x + V = \{x + v \mid v \in V\}$. There is a linear map (projection)

$$\pi_V : \mathbb{F}_2^n \to \mathbb{F}_2^n/V, \quad x \mapsto x + V,$$

and for any $x, y \in \mathbb{F}_2^n$, we have

$$x \equiv y \pmod{V} \iff \pi_V(x) = \pi_V(y) \iff x - y \in V.$$

2. **Orthogonal Complement.** The *orthogonal complement* of V is defined as

$$V^\perp = \{x \in \mathbb{F}_2^n \mid x^\top v = 0, \ \forall v \in V\}.$$

Multidimensional χ^2 Test and Data Complexity

Expected value for the real cipher:

$$\mu_{\text{real}} = \mathbb{E}[\chi^2_{\text{real}}] \approx |\Lambda| - 1 + q \sum_{(u,v)\in\Lambda\setminus\{(0,0)\}} \mathbb{E}\left[(C^F_{v,u})^2\right]$$

Expected value and variance for the ideal cipher:

$$\mu_{\text{ideal}} = |\Lambda| - 1, \qquad \sigma^2_{\text{ideal}} = 2(|\Lambda| - 1)$$

- Successful distinguisher condition:

$$\mu_{\text{real}} - \mu_{\text{ideal}} \gg \sigma_{\text{ideal}}$$

- Substituting yields:

$$q \sum_{(u,v)\in\Lambda\setminus\{(0,0)\}} \mathbb{E}\left[(C^F_{v,u})^2\right] \gg \sqrt{|\Lambda|}$$

- Using the **capacity definition**:

$$q \approx \frac{\sqrt{|\Lambda|}}{\text{Cap}(\Lambda)}$$

By the central limit theorem, the $\boldsymbol{\chi}^2_{\text{ideal}}$ asymptotically approaches the normal distribution $\mathcal{N}(\nu, 2\nu)$ as 2^n and q approach infinity. The false-positive rate is calculated by

$$P_F = \Pr\left[\chi^2_{\text{ideal}} \geq t\right] = \Pr\left[\underbrace{\frac{\chi^2_{\text{ideal}} - \nu}{2\nu}}_{\mathbf{Z} \sim \mathcal{N}(0,1)} \geq \frac{t-\nu}{2\nu}\right] = 1 - \Phi\left[\frac{t-\nu}{2\nu}\right],$$

where $\Phi(x)$ is the cumulative distribution function. Hence, the threshold value t is $t = \nu + \sqrt{2\nu}\,\Phi^{-1}(1 - P_{\text{F}})$. Once t is set for a fixed P_{F}, the success probability can be calculated by how often the χ^2_{real} statistic (the χ^2 statistic based on samples from the real cipher) exceeds t for a given data complexity.

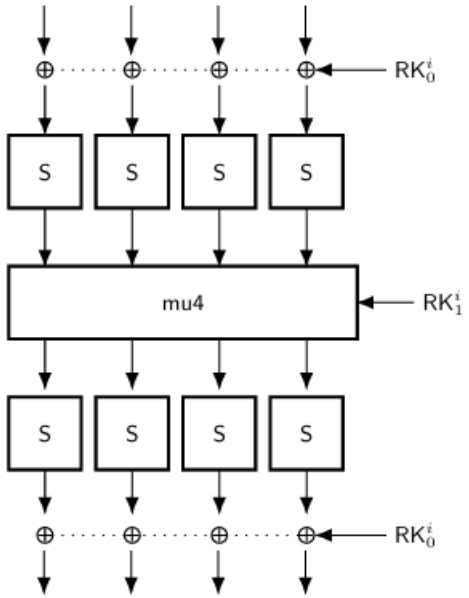


Fig. 2: The round function of FOX64.

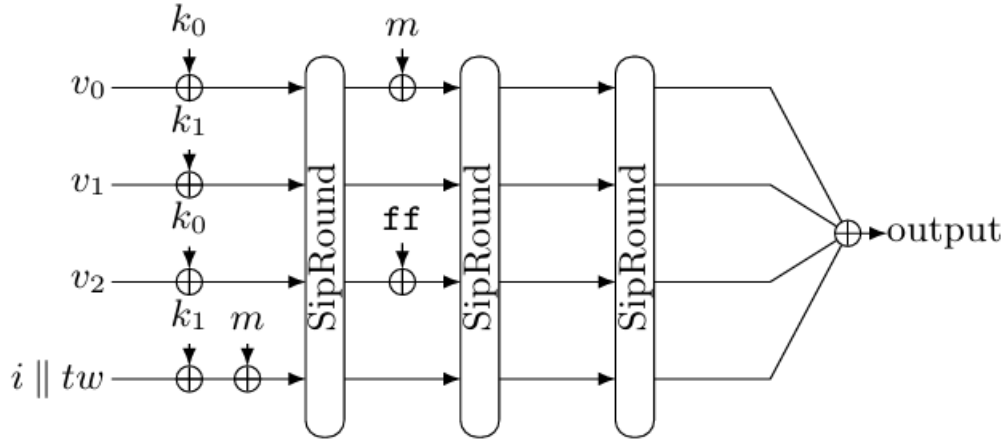
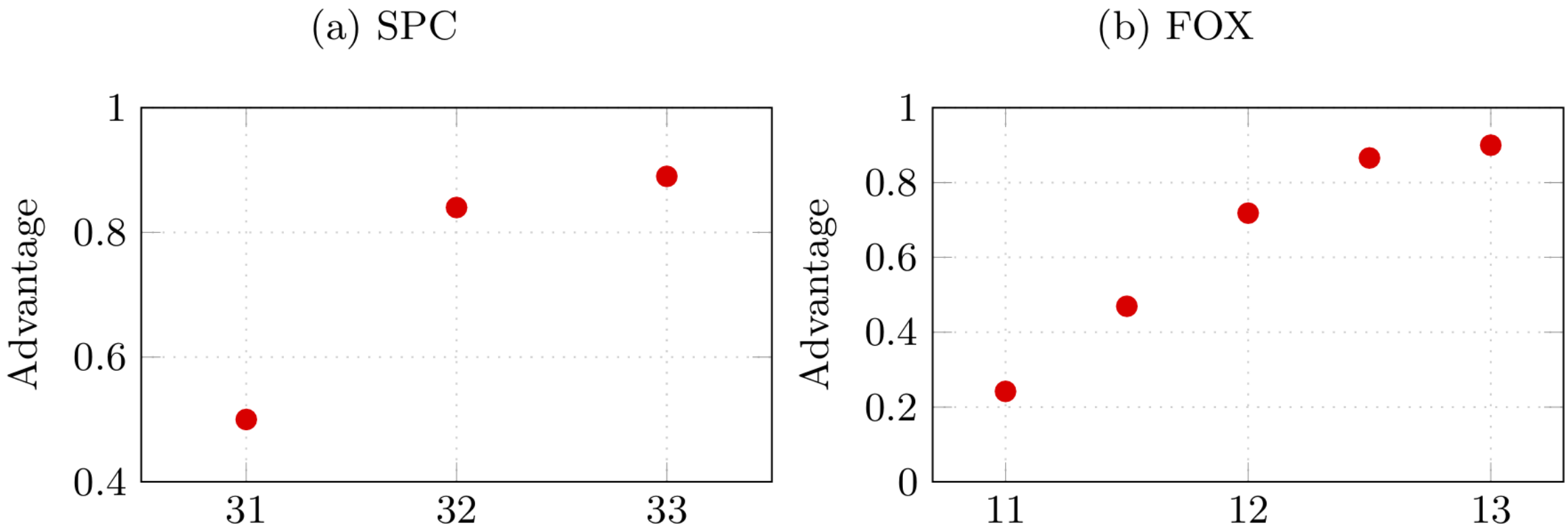
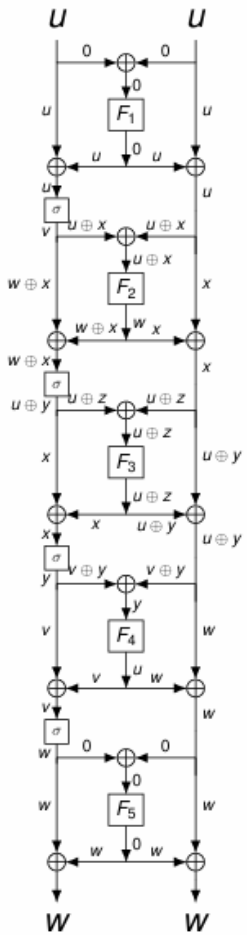


Fig. 3: The round function of SPC.

Fig. 8: Advantage as a function of data-complexity for 3-round χ^2 distinguishers where $P_{\mathrm{F}} = 0.1$.



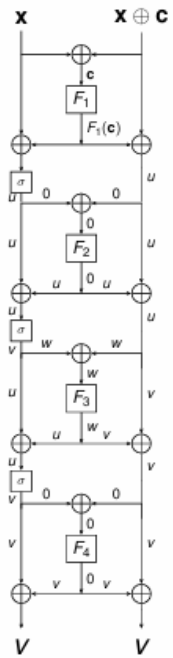
5-round linear trail with 3 active round functions

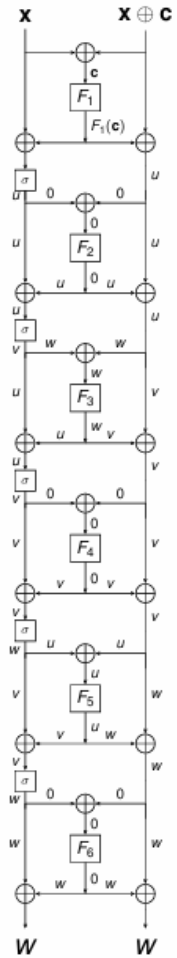


5-Round Lai–Massey Linear Trails

- Case r = 5 needs special attention:
- Direct formula gives $E(c^2(w)) = 2^{-2n}$, usually too small for a distinguisher.
- Additional linear trails exist with identical input/output masks.
- Example trail activates only F_2, F_3, F_4 while F_1 and F_5 stay inactive.
- Permutation consistency: $y = \sigma^{-1}(x)$, $z = \sigma^{-1}(y)$, $x = \sigma^{-1}(z)$ with $x \oplus y = z$.
- 2^n possible x values → extra trails with squared correlation $\approx 2^{-3n}$.
- Total expected squared correlation:
- $E(c^2(w)) \approx 2^{-2n} + 2^n \cdot 2^{-3n} \approx 2 \cdot 2^{-2n}$.
- For $r \leq 4$ multiplicity negligible; for r = 5 correlation doubles.

Generic multidimensional linear distinguisher under CPA model





$$q = \mathcal{O}\left(2^{n\lfloor (r-1)/2 \rfloor - n/2}\right)$$

Generic key recovery attack

$\mathcal{O}(n2^{n(r'-1)\ell}+q+2^{\ell})$

$$T = \begin{cases} \mathcal{O}\left(n2^{n+(r'-1)\ell} + 2^{\ell}\right), & r = 3, \\ \mathcal{O}\left(n2^{n+(r'-1)\ell} + 2^{3n/2} + 2^{\ell}\right), & r = 5, \end{cases}$$

$$\mathcal{O}(n2^{nr'}), \quad \ell = n,$$
$$\mathcal{O}(n2^{2nr'-n} + 2^{2n}), \quad \ell = 2n$$

$r = 3$

$$\mathcal{O}(n2^{nr'} + 2^{3n/2}), \quad \ell = n,$$
$$\mathcal{O}(n2^{2nr'-n} + 2^{2n}), \quad \ell = 2n$$

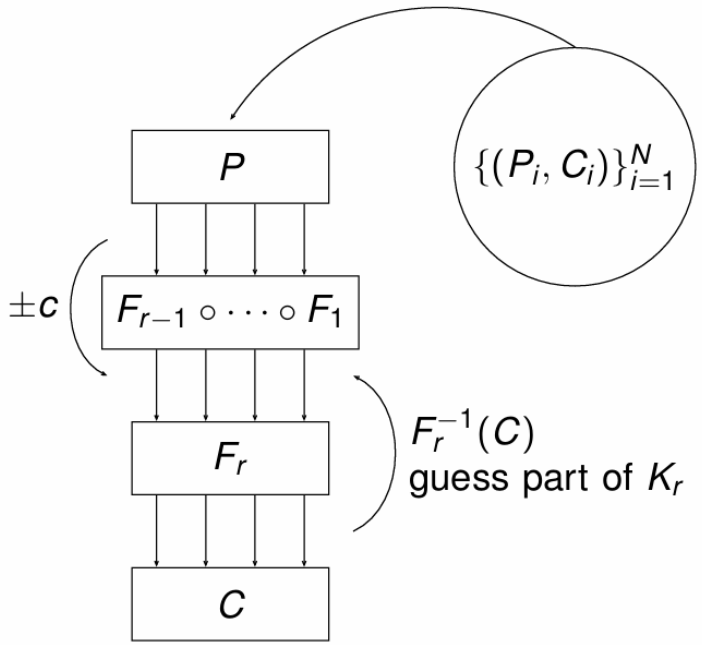
$r = 5$

r	ℓ	K	$r'_{\max}$	T
3 or 5	n	$2n$	1	$n2^n$
		$4n$	3	$n2^{3n}$
	$2n$	$4n$	2	$n2^{3n}$

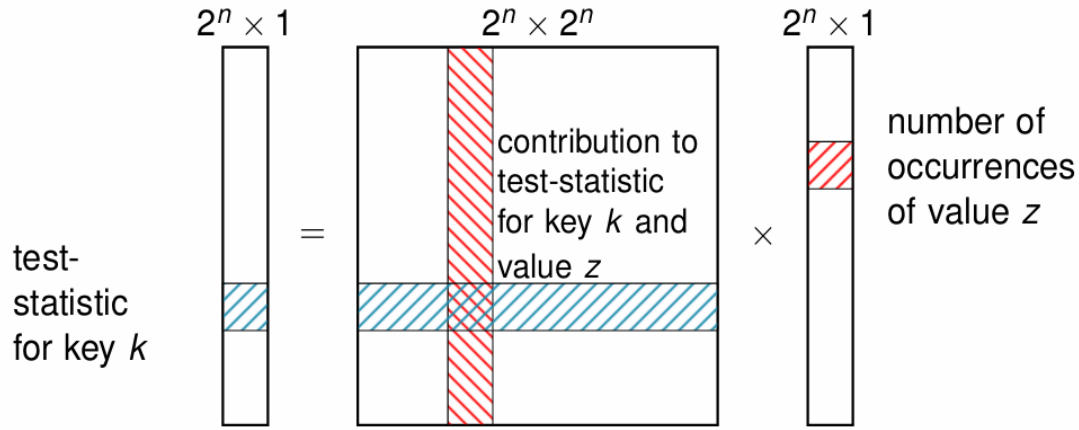
Table 5: Key recovery results of $r + r'$-round FOX64.

$r + r'$	r'	Data	Ref.	Work effort
4	1	$2^{15.8}$	§ 5.1	2^{64}
		2^{9}	[33]	$2^{45.4}$
5	2	$2^{16\,\dagger}$	§ 5.1	2^{101}
		2^{9}	[33]	$2^{109.4}$
6	1	$2^{32\,\dagger}$	§ 5.1	2^{64}
		15	[14]	2^{124}
7	2	$2^{32\,\dagger}$	§ 5.1	2^{101}
		$2^{30.9}$	[14]	2^{124}

† Asymptotic results.



$\mathcal{O}(q2^n)$



Matsui's Method

$\mathcal{O}(q + 2^{2n})$

FFT-based Method

$\mathcal{O}(q + n2^n)$