KU LEUVEN

Multidimensional Linear Cryptanalysis of Feistel Ciphers

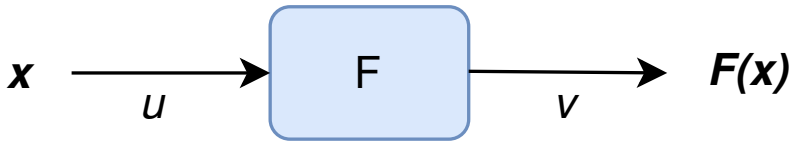
Betül Aşkın Özdemir, Tim Beyne and Vincent Rijmen

ESAT, COSIC

March 25, 2024

Linear cryptanalysis

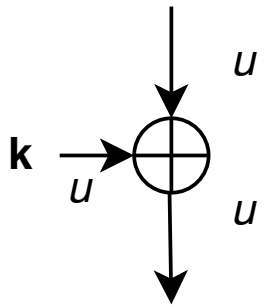
Linear approximation (u, v)



$$C^F_{v,u} = 2 \times (\Pr[u^T x = v^T F(x)] - \tfrac{1}{2})$$

Linear cryptanalysis

Key-alternating ciphers:



$\longrightarrow$ correlation $(-1)^{u^T k}$

Multidimensional linear cryptanalysis

Multidimensional linear cryptanalysis is based on multiple linear approximations whose masks form a vector space Λ

$$\begin{array}{ccc} (u,v) \in \Lambda & & (s,t) \in \mathbb{F}_2^{n\times n}/\Lambda^{\perp} \\ C^F_{v,u} & \begin{array}{c}\longrightarrow\\ \longleftarrow\end{array} & \Pr\left((\mathbf{x}, F(\mathbf{x})) = (s,t) \bmod \Lambda^{\perp}\right) \end{array}$$

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

Multidimensional linear distinguisher

The multidimensional linear property is turned into a distinguisher using statistical tests

- Unknown correlation signs: Chi-squared (χ^2) test
- Known correlation signs: Likelihood-ratio test

$$\mathrm{Cap}(\Lambda) = \sum_{(u,v)\in\Lambda\setminus\{0,0\}} (C^F_{v,u})^2$$

χ^2 test

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

Likelihood-ratio test

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

Multidimensional linear distinguisher

The multidimensional linear property is turned into a distinguisher using statistical tests

- Unknown correlation signs: Chi-squared (χ^2) test
- Known correlation signs: Likelihood-ratio test

$$\mathrm{Cap}(\Lambda) = \sum_{(u,v)\in\Lambda\setminus\{0,0\}} (C^F_{v,u})^2$$

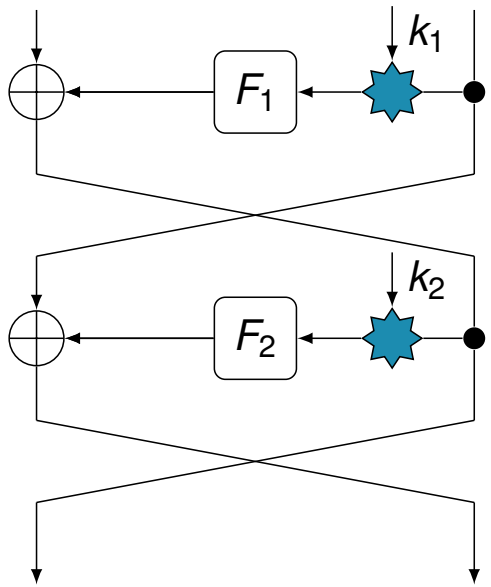
χ^2 test

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

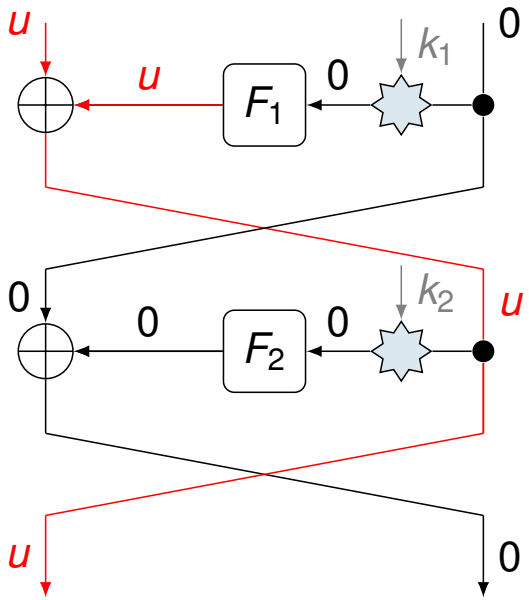
Likelihood-ratio test

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

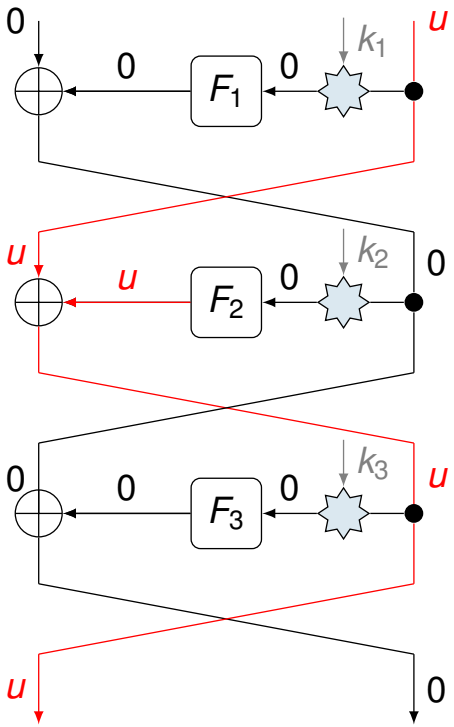
Feistel ciphers



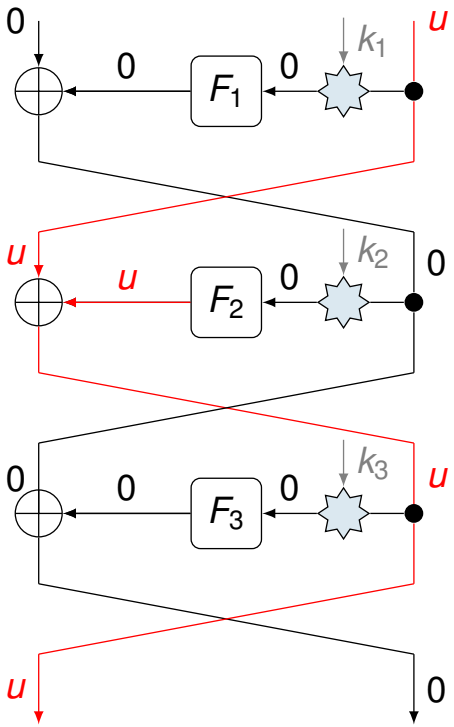
Multidimensional Linear Distinguisher on Feistel Ciphers



Generic multidimensional linear distinguisher on Feistel ciphers



Generic multidimensional linear distinguisher on Feistel ciphers



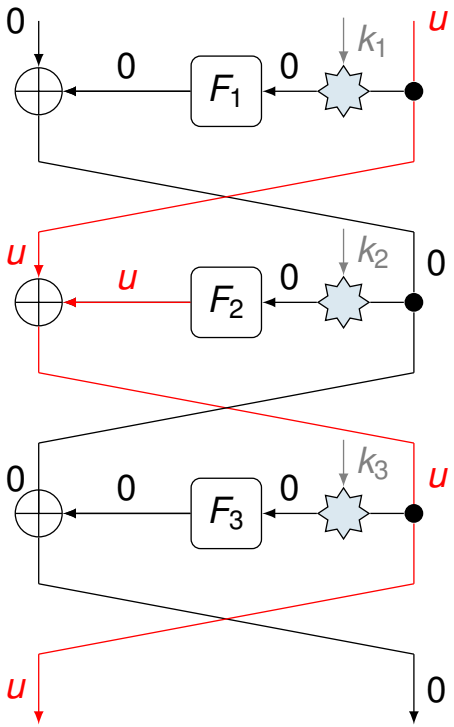
$$\Lambda = \left\{ ((0,u),(u,0)) \mid u \in \mathbb{F}_2^n \right\}$$

$$\mathbf{c}_u = \prod_{i=1}^{\lfloor r/2 \rfloor} \mathbf{c}$$

$$\mathbf{c} \approx 2^{-n/2} \text{ where } F_i : \mathbb{F}_2^n \to \mathbb{F}_2^n$$

$$\mathbf{c}_u^2 \approx 2^{-n\lfloor r/2 \rfloor}$$

Generic multidimensional linear distinguisher on Feistel ciphers



$$\Lambda = \left\{ ((0,u),(u,0)) \mid u \in \mathbb{F}_2^n \right\}$$

$$\mathbf{c}_u = \prod_{i=1}^{\lfloor r/2 \rfloor} \mathbf{c}$$

$$\mathbf{c} \approx 2^{-n/2} \text{ where } F_i : \mathbb{F}_2^n \to \mathbb{F}_2^n$$

$$\mathbf{c}_u^2 \approx 2^{-n\lfloor r/2 \rfloor}$$

$$\sum_{u \in \mathbb{F}_2^n \setminus \{0\}} \mathbf{c}_u^2 = 2^n \mathbf{c}_{u^\star}^2 \approx 2^{n-n\lfloor r/2 \rfloor}$$

$$q \approx 2^{n\lfloor r/2 \rfloor - n}$$

Comparison of generic attacks on r-round Feistel ciphers

Distinguishers in the known-plaintext model

r	Data	Ref.	Work effort
2	$2^{n/2}$	Patarin et al.	$2^{n/2}$
	1	Our work	1
3	$2^{n/2}$	Patarin et al.	$2^{n/2}$
	1	Our work	1
4	2^{n}	Patarin et al.	2^{n}
	2^{n}	Our work	2^{n}
5	$2^{3n/2}$	Patarin et al.	$2^{3n/2}$
	2^{n}	Our work	2^{n}
6	2^{2n}	Patarin et al.	2^{2n}
	2^{2n}	Our work	2^{2n}
7	2^{3n}	Patarin et al.	2^{3n}
	2^{2n}	Our work	2^{2n}

Distinguisher using the likelihood-ratio test

$$\lambda_{\text{real}} = \sum_{i=1}^{q} \log \frac{p_{\text{real}}(z_i)}{p_{\text{ideal}}(z_i)}$$

$$P_{\text{F}} = \Pr\left[\lambda_{\text{ideal}} \geq t\right]$$

$P_{\text{S}} = \Pr[\lambda_{\text{real}} \geq t]$ for a given data complexity

$$Adv = |P_S - P_F|$$

Distinguisher using the likelihood-ratio test

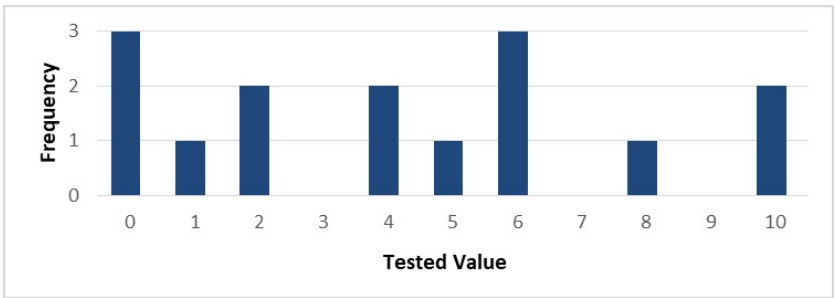
$$\lambda_{\text{real}} = \sum_{i=1}^{q} \log \frac{p_{\text{real}}(z_i)}{p_{\text{ideal}}(z_i)}$$

What happens if $p_{\text{real}}(z_i) = 0$?

Distinguisher using the likelihood-ratio test

$$\lambda_{\text{real}} = \sum_{i=1}^{q} \log \frac{p_{\text{real}}(z_i)}{p_{\text{ideal}}(z_i)}$$

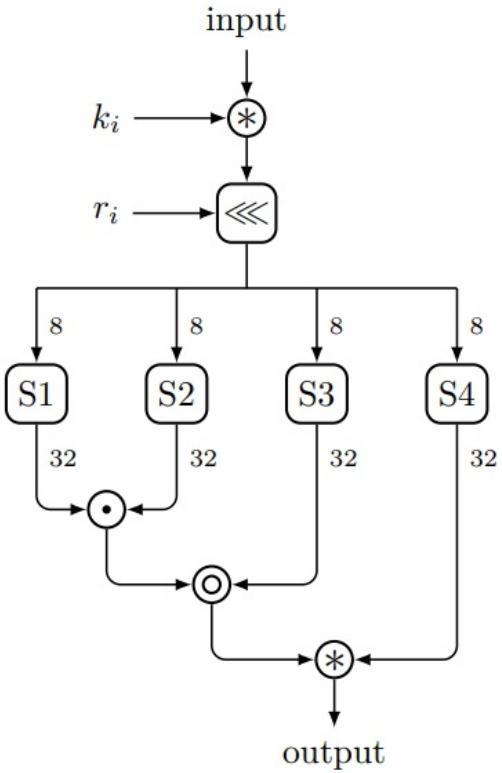
What happens if $p_{\text{real}}(z_i) = 0$?



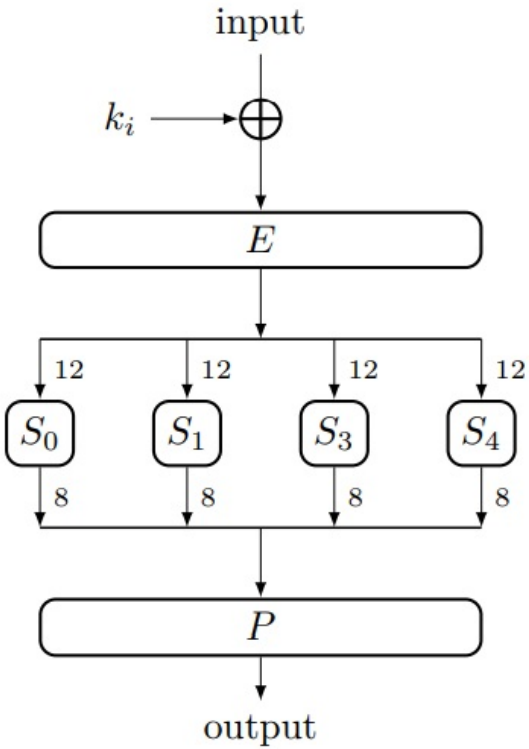
$$\text{Adv} = 1 - \left(1 - \frac{N_{\text{zero}}}{2^{32}}\right)^{q}$$

Round functions of target algorithms

CAST-128



LOKI91

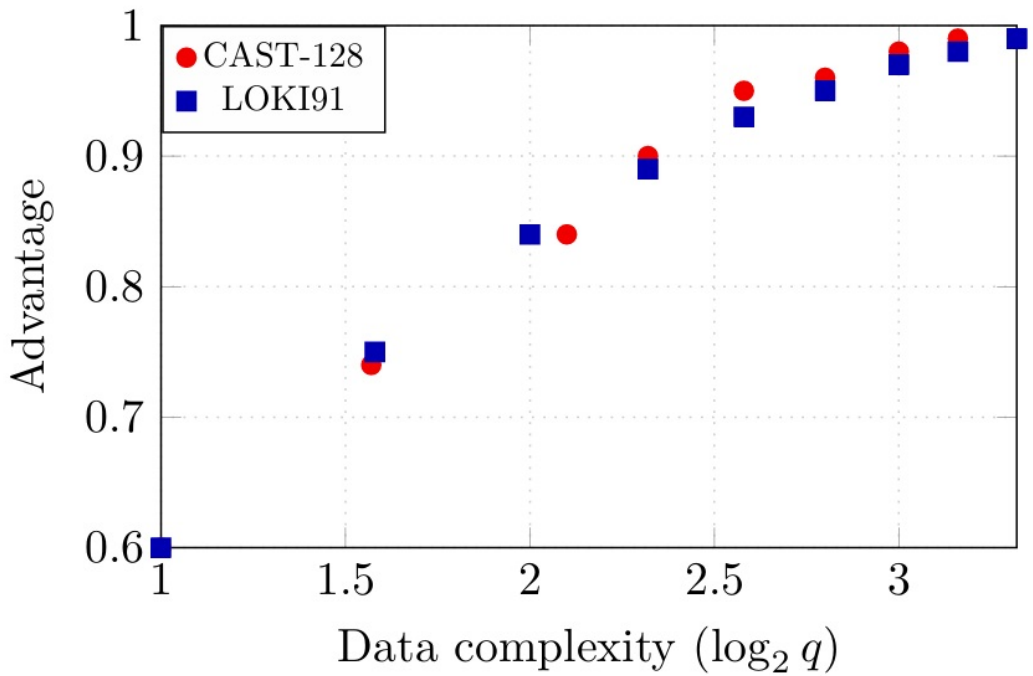


Capacity of reduced-round target algorithms

Cipher	r	Round functions	Capacity
CAST-128	3	F_1	1
		F_2	1
		F_3	1
	5	F_1, F_2	$2^{-31.9}$
		F_1, F_3	$2^{-31.9}$
		F_2, F_3	$2^{-31.9}$
	7	F_1, F_2, F_3	$2^{-63.9}$
LOKI91	3	F	1
	5	F, F	$2^{-21.4}$
	7	F, F, F	$2^{-39.2}$
	9	F, F, F, F	$2^{-56.3}$

$$\mathrm{Cap}(\Lambda) = 2^{n-n\lfloor r/2 \rfloor}$$

Advantage as a function of data-complexity for 3-round LLR distinguishers.

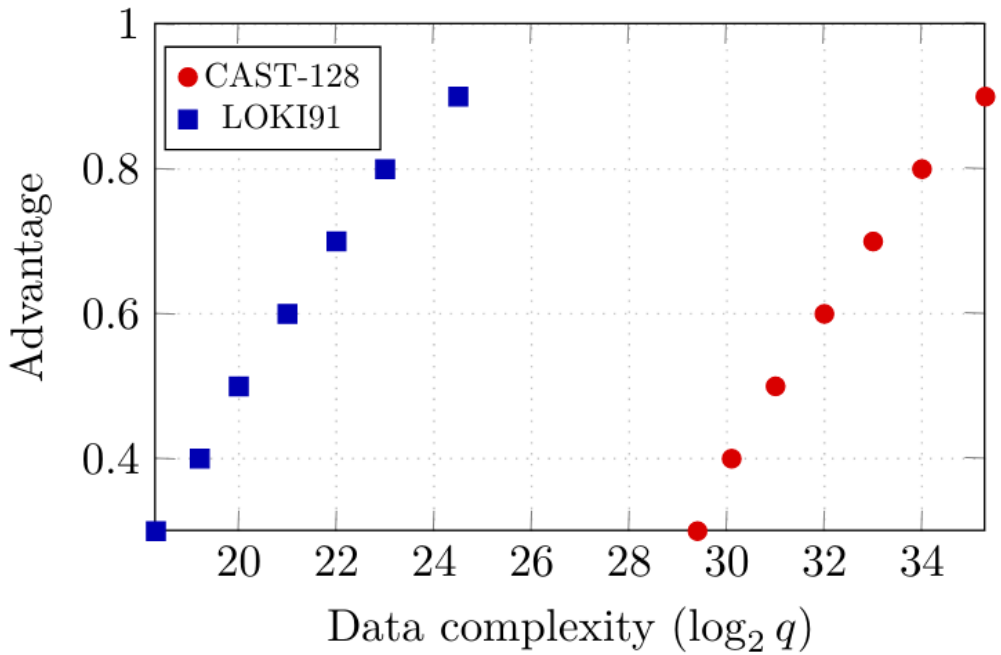


$P_F = 0$

CAST-128	LOKI91
10	14

$P_S \approx 1$ and $P_F = 0$

Advantage as a function of data-complexity for 5-round LLR distinguishers

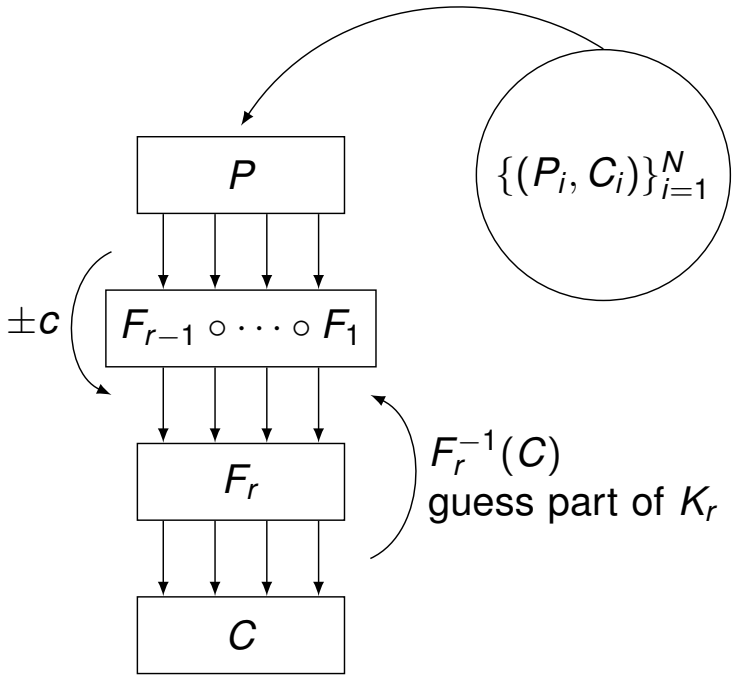


$P_F \approx 0.1$

CAST-128	LOKI91
2^{35}	2^{25}

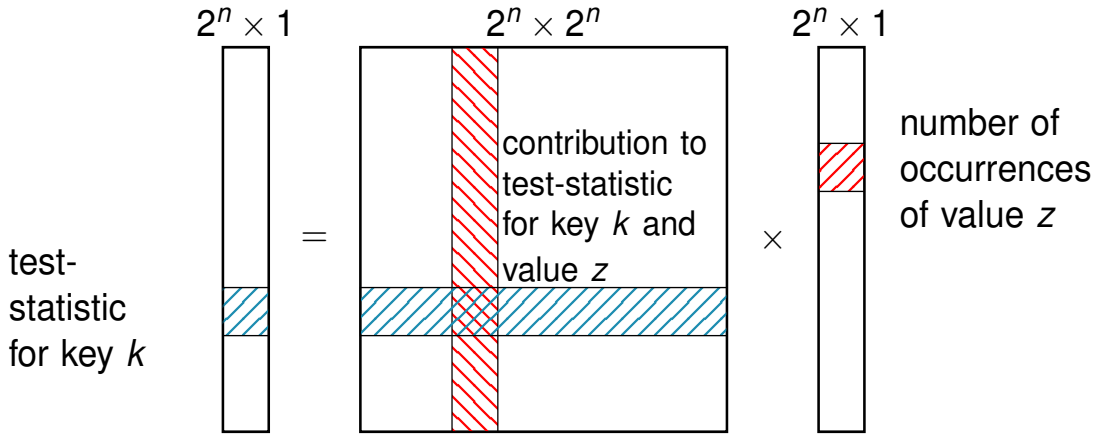
$P_S \approx 1$ and $P_F \approx 0.1$

Key recovery



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

Matsui and FFT-based key recovery



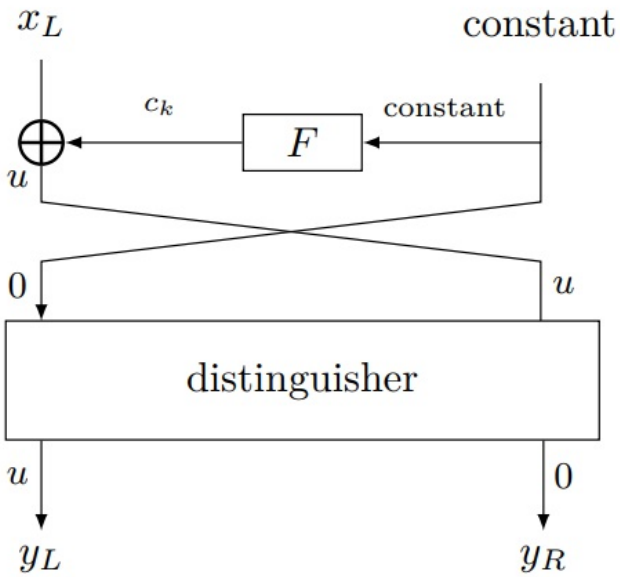
Matsui's Method

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

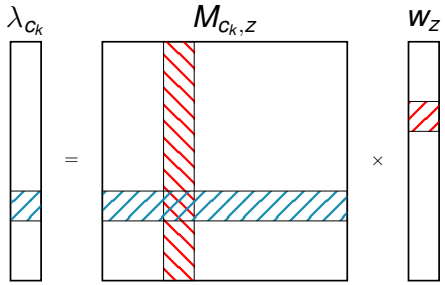
FFT-based Method

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

FFT-based key recovery



$$\lambda_{c_k} = \sum_{z \in \mathbb{F}_2^n} M_{c_k,z}\, w_z$$



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

Generic key recovery attack on an r-round Feistel cipher

k	r	Data	Ref.	Work effort
$2n$	4	1	Isobe et al.	2^n
		1	Our work	2^n
	5	$2^{n/2}$	Isobe et al.	2^n
	6	2^n	Isobe et al.	$2^{3n/2}$
		2^n	Our work	$n2^n$
$4n$	4	1	Isobe et al.	2^n
		1	Our work	2^n
	5	$2^{n/2}$	Isobe et al.	2^n
		1	Our work	2^{2n}
	6	1	Our work	2^{3n}
		2^n	Our work	$n2^n$
	7	2^n	Isobe et al.	$2^{3n/2}$
		2^n	Our work	$n2^{2n}$
	8	1	Isobe et al.	2^{3n}
		2^n	Our work	$n2^{3n}$
	9	$2^{5n/6}$	Isobe et al.	2^{3n}

Key recovery results of CAST-128

r	P_S	Data	Ref.	Work effort
4	1	$2^{33.38}$	Wang et al.	2^{91}
	1	$2^{5.80}$	Our work	2^{37}
5	1	$2^{6.80}$	Our work	2^{74}
6	1	$2^{53.96}$	Wang et al.	2^{91}
	1	$2^{7.39}$	Our work	$2^{118.39}$
	1	2^{35}	Our work	2^{40}
7	1	6	Isobe et al.	2^{114}
	1	2^{35}	Our work	2^{77}
8	1	8	Isobe et al.	2^{118}
	1	2^{35}	Our work	2^{114}

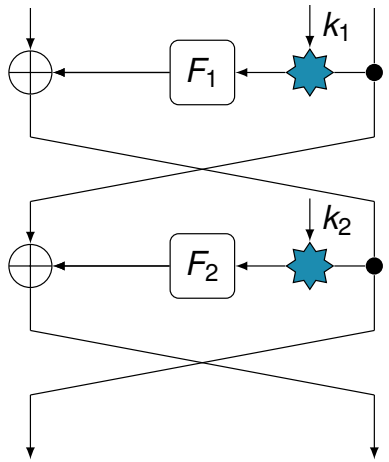
Key recovery results of LOKI91

r	P_S	Data	Ref.	Work effort
	0.90	$2^{21.77}$	Knudsen et al.	2^{49}
	0.86	$2^{20.86}$	Knudsen et al.	2^{44}
	‡	$2^{18.51}$	Sakurai et al.	2^{40}
4	1	$2^{19.60}$	Tokita et al.	2^{51}
	1	$2^{5.55}$	Our work	2^{37}
5	1	$2^{23.20}$	Tokita et al.	2^{51}
	1	$2^{31.70}$	Tokita et al.	2^{51}
6	‡	$2^{27.58}$	Sakurai et al.	2^{40}
	1	$2^{24.2}$	Our work	2^{37}
7	‡	$2^{36.67}$	Sakurai et al.	2^{40}
9	‡	$2^{45.74}$	Sakurai et al.	$2^{45.74}$
10	‡	$2^{54.83}$	Sakurai et al.	$2^{54.83}$

‡ Not explicitly provided.

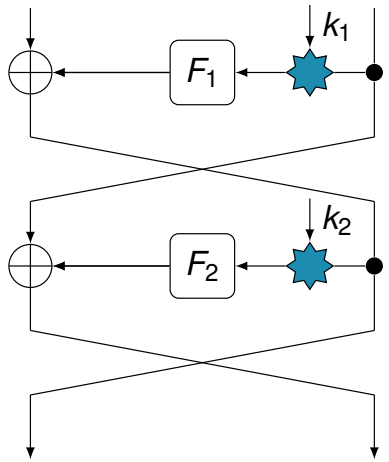
Conclusions

1. Generic distinguishing attack on a class of Feistel cipher
   - Key-independent multidimensional approximations
   - Likelihood-ratio test
2. Key-recovery attacks using a variant of the FFT method
3. Applications: CAST-128 and LOKI91



Conclusions

1. Generic distinguishing attack on a class of Feistel cipher
   - Key-independent multidimensional approximations
   - Likelihood-ratio test
2. Key-recovery attacks using a variant of the FFT method
3. Applications: CAST-128 and LOKI91



Thanks for your attention...