Algebraic Insights into the Secret Feistel Network

Léo Perrin[1,2] Aleksei Udovenko[1,2]

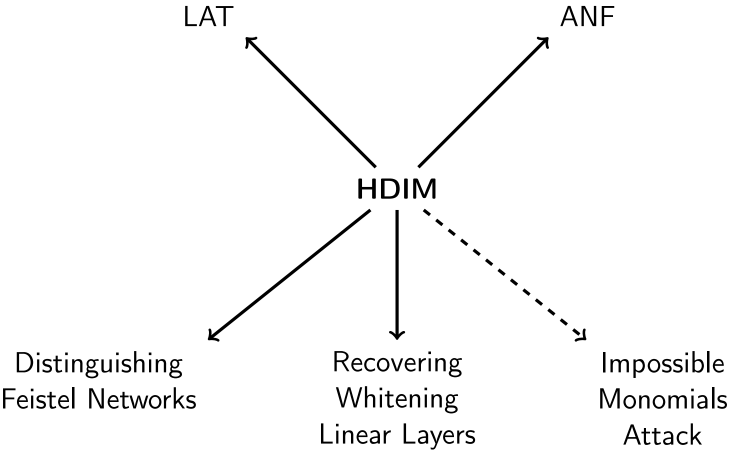
[1]University of Luxembourg,
[2]SnT

March 22, 2016

UNIVERSITÉ DU LUXEMBOURG

securityandtrust.lu

Outline


LAT
ANF
HDIM
Distinguishing Feistel Networks
Recovering Whitening Linear Layers
Impossible Monomials Attack

Plan

Linear Approximation Table (LAT)

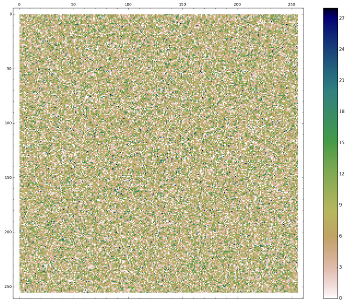
Definition (LAT, Fourier Transform, Walsh Spectrum)

The *Linear Approximation Table* of $f : \{0,1\}^n \rightarrow \{0,1\}^m$ is a $2^n \times 2^m$ matrix $\mathcal{L}$ where

$$\begin{aligned}\mathcal{L}[a,b] &= \#\{x \in \mathbb{F}_2^n, a \cdot x = b \cdot f(x)\} - 2^{n-1} \\ &= -\frac{1}{2} \sum_{x \in \mathbb{F}_2^n} (-1)^{a \cdot x \oplus b \cdot f(x)}.\end{aligned}$$

Jackson Pollock Representation of LAT

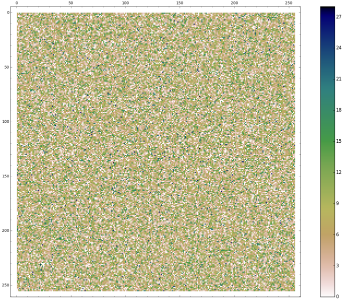
[Biryukov, Perrin CRYPTO2015]: graphical representation of LAT to reverse-engineer S-Boxes.



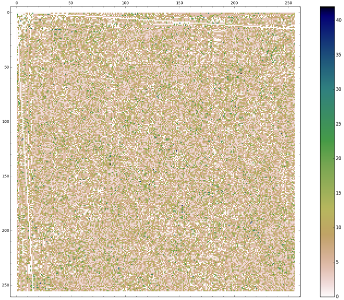
S-Box F of Skipjack

Jackson Pollock Representation of LAT

[Biryukov, Perrin CRYPTO2015]: graphical representation of LAT to reverse-engineer S-Boxes.



S-Box F of Skipjack



4-round Feistel Network with bijective functions

LAT modulo 4

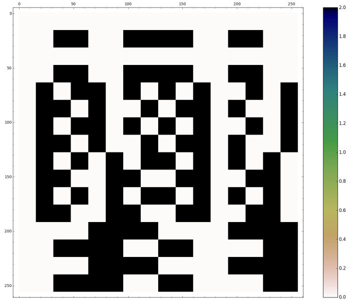
Idea

- Look at LAT modulo 4!
- Why? LAT modulo 2^k is related to algebraic degree.

LAT modulo 4

Idea

- Look at LAT modulo 4!
- Why? LAT modulo 2^k is related to algebraic degree.

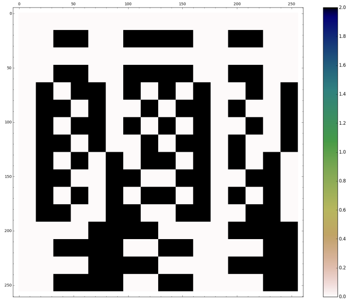


4-round Feistel Network
with bijective functions

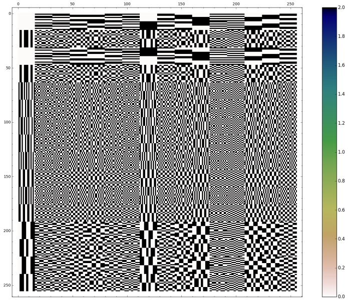
LAT modulo 4

Idea

- Look at LAT modulo 4!
- Why? LAT modulo 2^k is related to algebraic degree.



4-round Feistel Network
with bijective functions

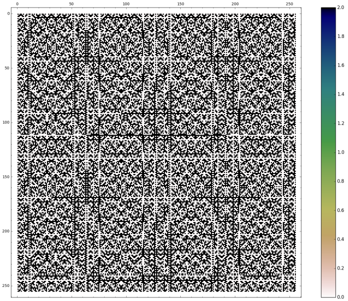


5-round Feistel Network
with bijective functions

LAT modulo 4

Idea

- Look at LAT modulo 4!
- Why? LAT modulo 2^k is related to algebraic degree.

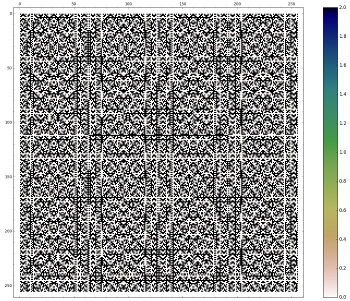


6-round Feistel Network
with bijective functions

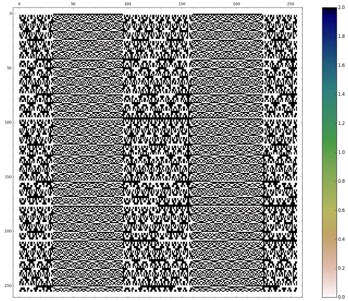
LAT modulo 4

Idea

- Look at LAT modulo 4!
- Why? LAT modulo 2^k is related to algebraic degree.



6-round Feistel Network with bijective functions



Random permutation

Bilinear Form

- LAT modulo 4 has highly linear patterns even for random permutations.

Bilinear Form

- LAT modulo 4 has highly linear patterns even for random permutations.
- Explanation? It is a bilinear form!

Bilinear Form

- LAT modulo 4 has highly linear patterns even for random permutations.
- Explanation? It is a bilinear form!
- The following is true:

$$\frac{\mathcal{L}[a,b]}{2} \equiv \bigoplus_{x\in\mathbb{F}_2^n} \left(b\cdot F(x)\right)\left(a\cdot x\right) \pmod 2. \tag{1}$$

Bilinear Form

- LAT modulo 4 has highly linear patterns even for random permutations.
- Explanation? It is a bilinear form!
- The following is true:

$$\frac{\mathcal{L}[a,b]}{2} \equiv \bigoplus_{x \in \mathbb{F}_2^n} \big(b \cdot F(x)\big)\big(a \cdot x\big) \pmod 2. \tag{1}$$

- $\Rightarrow$ express $\mathcal{L}[a,b]/2$ as a vector-matrix-vector product:

$$\frac{\mathcal{L}[a,b]}{2} \equiv b^T \times \hat{H}(F) \times a \pmod 2, \tag{2}$$

where $\hat{H}(F)$ is an $n \times n$ matrix over $\mathbb{F}_2$, such that

$$\hat{H}(F)[i,j] = \bigoplus_{x \in \mathbb{F}_2^n} \big(e_i \cdot F(x)\big)\big(e_j \cdot x\big). \tag{3}$$

Another meaning of LAT modulo 4

Algebraic Normal Form (ANF)

Recall that any Boolean function f mapping n bits to 1 can be represented in a unique way as:

$$f(x) = \bigoplus_{u \in \mathbb{F}_2^n} a_u x^u = \bigoplus_{u \in \mathbb{F}_2^n} a_u \prod_{i \in [0, n-1]} x_i^{u_i}.$$

Another meaning of LAT modulo 4

Algebraic Normal Form (ANF)

Recall that any Boolean function f mapping n bits to 1 can be represented in a unique way as:

$$f(x) = \bigoplus_{u \in \mathbb{F}_2^n} a_u x^u = \bigoplus_{u \in \mathbb{F}_2^n} a_u \prod_{i \in [0, n-1]} x_i^{u_i} .$$

Lemma (Another meaning of LAT modulo 4)

$\hat{H}(F)[i, j] = 1$ *if and only if the ANF of* i*th bit of* F *contains the monomial* $\prod_{k \neq j} x_k$ *(which has degree* $n - 1$*).*

High-Degree Indicator Matrix

Definition (High-Degree Indicator Matrix)

We will call $\hat{H}(F)$ High-Degree Indicator Matrix (**HDIM**).

High-Degree Indicator Matrix

Definition (High-Degree Indicator Matrix)

We will call $\hat{H}(F)$ High-Degree Indicator Matrix (**HDIM**).

Computing the **HDIM**

- Each row or column of $\hat{H}(F)$ is a $\oplus$-sum of F over a particular cube of dimension $n-1$.

High-Degree Indicator Matrix

Definition (High-Degree Indicator Matrix)

We will call $\hat{H}(F)$ High-Degree Indicator Matrix (**HDIM**).

Computing the **HDIM**

- Each row or column of $\hat{H}(F)$ is a $\oplus$-sum of F over a particular cube of dimension $n-1$.
- For one row/column we need 2^{n-1} data and 2^{n-1} time.

High-Degree Indicator Matrix

Definition (High-Degree Indicator Matrix)

We will call $\hat{H}(F)$ High-Degree Indicator Matrix (**HDIM**).

Computing the **HDIM**

- Each row or column of $\hat{H}(F)$ is a $\oplus$-sum of F over a particular cube of dimension $n-1$.
- For one row/column we need 2^{n-1} data and 2^{n-1} time.
- For whole $\hat{H}(F)$ we need full codebook and $n2^{n-1}$ time.

High-Degree Indicator Matrix

Definition (High-Degree Indicator Matrix)

We will call $\hat{H}(F)$ High-Degree Indicator Matrix (**HDIM**).

Computing the **HDIM**

- Each row or column of $\hat{H}(F)$ is a $\bigoplus$-sum of F over a particular cube of dimension $n - 1$.
- For one row/column we need 2^{n-1} data and 2^{n-1} time.
- For whole $\hat{H}(F)$ we need full codebook and $n2^{n-1}$ time.
- Neglible memory complexity - n bits to store the sum.

Properties of HDIM

Theorem (Linear transformations and HDIM)

Let μ, η be linear n-bit mappings, F be an n-bit permutation and let $G = \eta \circ F \circ \mu$. Then it holds that

$$\hat{H}(G) = \eta \times \hat{H}(F) \times (\mu^t)^{-1}.$$

Properties of HDIM

Theorem (Linear transformations and HDIM)

Let μ, η be linear n-bit mappings, F be an n-bit permutation and let $G = \eta \circ F \circ \mu$. Then it holds that

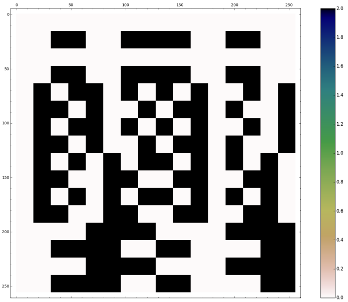
$$\hat{H}(G) = \eta \times \hat{H}(F) \times (\mu^t)^{-1}.$$

- Linear transformations applied to a permutation modify its HDIM in a linear way.
- We will use this Theorem to recover whitening linear layers.

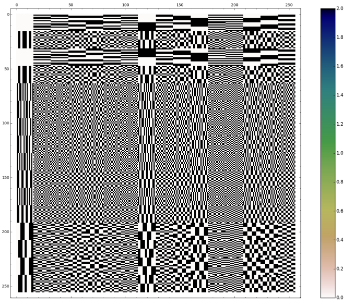
Plan

LAT modulo 4 patterns

- Recall the LAT modulo 4 patterns that we have spotted:



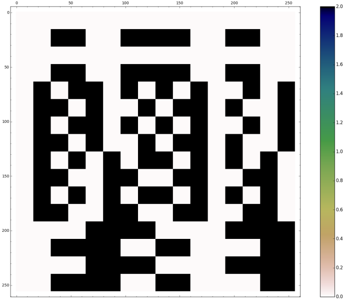
4-round Feistel Network
with bijective functions



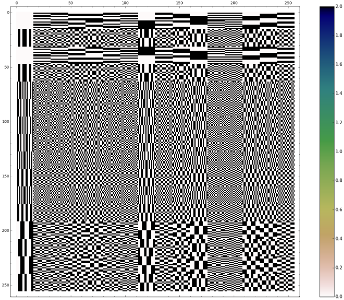
5-round Feistel Network
with bijective functions

LAT modulo 4 patterns

- Recall the LAT modulo 4 patterns that we have spotted:
- Can be nicely rephrased in terms of **HDIM**.



4-round Feistel Network with bijective functions



5-round Feistel Network with bijective functions

HDIM Patterns in Feistel Networks

Theorem

Let F^r be r-round Feistel Network with bijective functions. Then

$$\hat{H}(\mathsf{F}^4) = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & ? & ? & ? \\ 0 & 0 & 0 & ? & ? & ? \\ 0 & 0 & 0 & ? & ? & ? \end{bmatrix} \qquad \hat{H}(\mathsf{F}^5) = \begin{bmatrix} 0 & 0 & 0 & ? & ? & ? \\ 0 & 0 & 0 & ? & ? & ? \\ 0 & 0 & 0 & ? & ? & ? \\ ? & ? & ? & ? & ? & ? \\ ? & ? & ? & ? & ? & ? \\ ? & ? & ? & ? & ? & ? \end{bmatrix}$$

Example is given for $n = 3$ (6-bit Feistel Network).

Generalization by Number of Rounds

Theorem

- *Let* F_d^r *be a Feistel Network with* r **rounds** *and* **degree** d *of round functions.*

Generalization by Number of Rounds

Theorem

- *Let* F_d^r *be a Feistel Network with* r **rounds** *and* **degree** d *of round functions.*
- *Let* $\theta(d,r) = d^{\lfloor r/2 \rfloor - 1} + d^{\lceil r/2 \rceil - 1}$ *be a parameter.*

Generalization by Number of Rounds

Theorem

- *Let* F_d^r *be a Feistel Network with* r **rounds** *and* **degree** d *of round functions.*
- *Let* $\theta(d, r) = d^{\lfloor r/2 \rfloor - 1} + d^{\lceil r/2 \rceil - 1}$ *be a parameter.*
- *Assume that the round functions are permutations. Then*
  - $\hat{H}(\mathsf{F}_d^r) = \begin{bmatrix} \mathbf{0} & \mathbf{0} \\ \mathbf{0} & ? \end{bmatrix}$, *when* $\theta(d, r) < 2n$.
  - $\hat{H}(\mathsf{F}_d^r) = \begin{bmatrix} \mathbf{0} & ? \\ ? & ? \end{bmatrix}$, *when* $\theta(d, r-1) < 2n$.

Generalization by Number of Rounds

Theorem

- *Let* F_d^r *be a Feistel Network with* r **rounds** *and* **degree** d *of round functions.*
- *Let* $\theta(d, r) = d^{\lfloor r/2 \rfloor - 1} + d^{\lceil r/2 \rceil - 1}$ *be a parameter.*
- *Assume that the round functions are permutations. Then*
    - $\hat{H}(\mathsf{F}_d^r) = \begin{bmatrix} \mathbf{0} & \mathbf{0} \\ \mathbf{0} & ? \end{bmatrix}$, *when* $\theta(d, r) < 2n$.
    - $\hat{H}(\mathsf{F}_d^r) = \begin{bmatrix} \mathbf{0} & ? \\ ? & ? \end{bmatrix}$, *when* $\theta(d, r-1) < 2n$.
- *For non-bijective round functions, the results hold for one round less.*

Generalization by Number of Rounds

Theorem

- *Let* F_d^r *be a Feistel Network with* r **rounds** *and* **degree** d *of round functions.*
- *Let* $\theta(d, r) = d^{\lfloor r/2 \rfloor - 1} + d^{\lceil r/2 \rceil - 1}$ *be a parameter.*
- *Assume that the round functions are permutations. Then*
  - $\hat{H}(\mathsf{F}_d^r) = \begin{bmatrix} \mathbf{0} & \mathbf{0} \\ \mathbf{0} & ? \end{bmatrix}$, *when* $\theta(d, r) < 2n$.
  - $\hat{H}(\mathsf{F}_d^r) = \begin{bmatrix} \mathbf{0} & ? \\ ? & ? \end{bmatrix}$, *when* $\theta(d, r-1) < 2n$.
- *For non-bijective round functions, the results hold for one round less.*

Distinguisher for Feistel Networks: one HDIM row or column is enough.

Generalization by Number of Rounds

Theorem

- *Let* F_d^r *be a Feistel Network with* r **rounds** *and* **degree** d *of round functions.*
- *Let* $\theta(d, r) = d^{\lfloor r/2 \rfloor - 1} + d^{\lceil r/2 \rceil - 1}$ *be a parameter.*
- *Assume that the round functions are permutations. Then*
  - $\hat{H}(\mathsf{F}_d^r) = \begin{bmatrix} \mathbf{0} & \mathbf{0} \\ \mathbf{0} & ? \end{bmatrix}$, *when* $\theta(d, r) < 2n$.
  - $\hat{H}(\mathsf{F}_d^r) = \begin{bmatrix} \mathbf{0} & ? \\ ? & ? \end{bmatrix}$, *when* $\theta(d, r-1) < 2n$.
- *For non-bijective round functions, the results hold for one round less.*

Distinguisher for Feistel Networks: one HDIM row or column is enough. Weak compared to known distinguishers for up to 5 rounds, but can attack more rounds when the degree is low.

Proof Idea

- Recall the equation for HDIM:

$$\hat{H}(F)[i,j] = \bigoplus_{x \in \mathbb{F}_2^{2n}} \left(e_i \cdot F(x)\right)\left(e_j \cdot x\right)$$

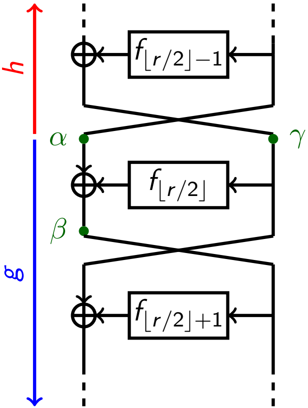
Proof Idea

- Recall the equation for HDIM:

$$\hat{H}(F)[i,j] = \bigoplus_{x \in \mathbb{F}_2^{2n}} (e_i \cdot F(x))(e_j \cdot x)$$

- Change sum variables:

$$= \bigoplus_{\alpha || \gamma \in \mathbb{F}_2^{2n}} (e_i \cdot g(\alpha,\gamma))(e_j \cdot h(\alpha,\gamma)).$$



Proof Idea

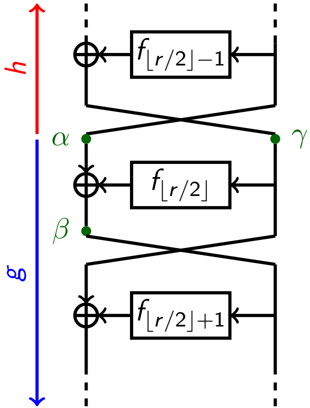
- Recall the equation for HDIM:

$$\hat{H}(F)[i,j] = \bigoplus_{x\in\mathbb{F}_2^{2n}} (e_i \cdot F(x))(e_j \cdot x)$$

- Change sum variables:

$$= \bigoplus_{\alpha||\gamma\in\mathbb{F}_2^{2n}} (e_i \cdot g(\alpha,\gamma))(e_j \cdot h(\alpha,\gamma)).$$

- Calculate the degrees of h and g straightforwardly and sum them.



Proof Idea

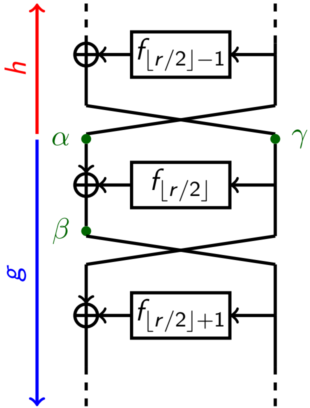
- Recall the equation for HDIM:

$$\hat{H}(F)[i,j] = \bigoplus_{x \in \mathbb{F}_2^{2n}} (e_i \cdot F(x))\,(e_j \cdot x)$$

- Change sum variables:

$$= \bigoplus_{\alpha || \gamma \in \mathbb{F}_2^{2n}} (e_i \cdot g(\alpha, \gamma))\,(e_j \cdot h(\alpha, \gamma)).$$

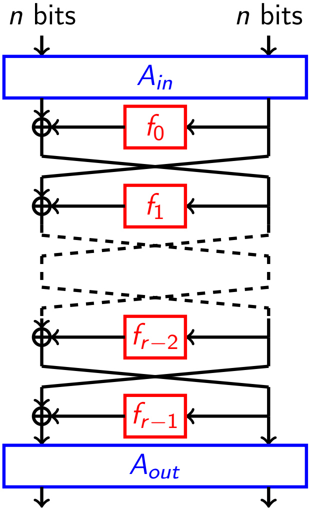
- Calculate the degrees of h and g straightforwardly and sum them.
- For bijective round functions, we can get one round more by summing over α and β.



Feistel Network with Whitening Linear Layers

The AF^{r}A structure:

- Feistel Network with r rounds and n-bit branches.
- f_i: secret and independent random functions.
- whitened with secret affine layers A_{in}, A_{out}.



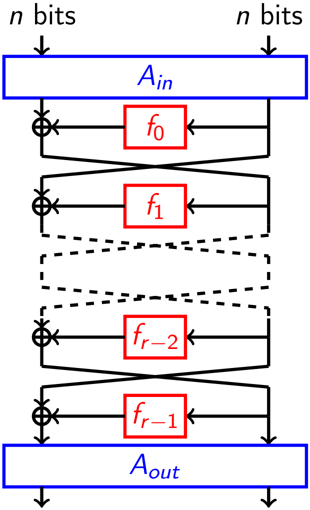
Feistel Network with Whitening Linear Layers

The AF^rA structure:

- Feistel Network with r rounds and n-bit branches.
- f_i: secret and independent random functions.
- whitened with secret affine layers A_{in}, A_{out}.

Cryptanalysis goals:

- distinguish from random permutation;
- recover the secret components.



Attacking AF^{r}A

- Let F be a Feistel Network with r rounds, such that $\hat{H}(F) = \begin{bmatrix} \mathbf{0} & \mathbf{0} \\ \mathbf{0} & ? \end{bmatrix}$ (e.g. 4 rounds with bijective functions).
- Let $G = \eta \circ F \circ \mu$. That is, G is AF^{r}A.

Attacking AF^{r}A

- Let F be a Feistel Network with r rounds, such that $\hat{H}(F) = \begin{bmatrix} \mathbf{0} & \mathbf{0} \\ \mathbf{0} & ? \end{bmatrix}$ (e.g. 4 rounds with bijective functions).
- Let $G = \eta \circ F \circ \mu$. That is, G is AF^{r}A.
- Then by properties of HDIM we have:

$$\eta^{-1} \times \hat{H}(G) \times \mu^t = \begin{bmatrix} \mathbf{0} & \mathbf{0} \\ \mathbf{0} & ? \end{bmatrix}.$$

Attacking AF^{r}A

- Let F be a Feistel Network with r rounds, such that $\hat{H}(F) = \begin{bmatrix} \mathbf{0} & \mathbf{0} \\ \mathbf{0} & ? \end{bmatrix}$ (e.g. 4 rounds with bijective functions).
- Let $G = \eta \circ F \circ \mu$. That is, G is AF^{r}A.
- Then by properties of HDIM we have:

$$\eta^{-1} \times \hat{H}(G) \times \mu^t = \begin{bmatrix} \mathbf{0} & \mathbf{0} \\ \mathbf{0} & ? \end{bmatrix}.$$

- Parts of η and μ merge into the Feistel structure, so we have less unknowns and we can solve the system.

Attacking AF^{r}A

- Let F be a Feistel Network with r rounds, such that $\hat{H}(F) = \begin{bmatrix} \mathbf{0} & \mathbf{0} \\ \mathbf{0} & ? \end{bmatrix}$ (e.g. 4 rounds with bijective functions).
- Let $G = \eta \circ F \circ \mu$. That is, G is AF^{r}A.
- Then by properties of HDIM we have:

$$\eta^{-1} \times \hat{H}(G) \times \mu^t \;=\; \begin{bmatrix} \mathbf{0} & \mathbf{0} \\ \mathbf{0} & ? \end{bmatrix}.$$

- Parts of η and μ merge into the Feistel structure, so we have less unknowns and we can solve the system.
- Distinguisher for AF^{r}A and Partial recovery of linear layers.
- Complexity is dominated by computing HDIM - $n2^{2n-1}$.

Attacking one round more

- In some special cases we can attack one more round. Then we will need only that $\hat{H}(F) = \begin{bmatrix} \mathbf{0} & ? \\ ? & ? \end{bmatrix}$ (for example, 5 rounds with bijective functions).

Attacking one round more

- In some special cases we can attack one more round. Then we will need only that $\hat{H}(F) = \begin{bmatrix} \mathbf{0} & ? \\ ? & ? \end{bmatrix}$ (for example, 5 rounds with bijective functions).
- One of such cases is when the linear layers are *inverses* of each other ($\mathrm{A}^{-1}\mathrm{F}^{\mathrm{r}}\mathrm{A}$).

Attacking one round more

- In some special cases we can attack one more round. Then we will need only that $\hat{H}(F) = \begin{bmatrix} \mathbf{0} & ? \\ ? & ? \end{bmatrix}$ (for example, 5 rounds with bijective functions).
- One of such cases is when the linear layers are *inverses* of each other ($\mathsf{A}^{-1}\mathsf{F}^{\mathsf{r}}\mathsf{A}$).
- Another possible case is one-sided whitening: $\mathsf{F}^{\mathsf{r}}\mathsf{A}$.

Attacking one round more

- In some special cases we can attack one more round. Then we will need only that $\hat{H}(F) = \begin{bmatrix} \mathbf{0} & ? \\ ? & ? \end{bmatrix}$ (for example, 5 rounds with bijective functions).
- One of such cases is when the linear layers are *inverses* of each other ($\mathsf{A}^{-1}\mathsf{F}^{\mathsf{r}}\mathsf{A}$).
- Another possible case is one-sided whitening: $\mathsf{F}^{\mathsf{r}}\mathsf{A}$.
- Partial recovery of linear layers for $\mathsf{A}^{-1}\mathsf{F}^{\mathsf{r}}\mathsf{A}$ or $\mathsf{F}^{\mathsf{r}}\mathsf{A}$.
- Complexity is dominated by computing HDIM - $n2^{2n-1}$.

Plan

Generalizing to other ANF Monomials

- Previously, we exploited predictable absence of particular terms of degree $n-1$ in the ANFs of some output bits (entries $\hat{H}(F)_{i,j} = 0$).

Generalizing to other ANF Monomials

- Previously, we exploited predictable absence of particular terms of degree $n-1$ in the ANFs of some output bits (entries $\hat{H}(F)_{i,j}=0$).
- This is an *extreme* case, we tried to cover more rounds, but we recovered only surrounding linear layers.

Generalizing to other ANF Monomials

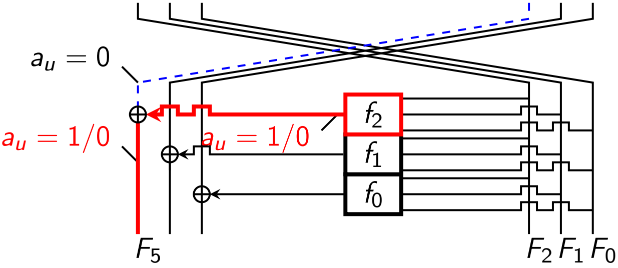
- Previously, we exploited predictable absence of particular terms of degree $n-1$ in the ANFs of some output bits (entries $\hat{H}(F)_{i,j} = 0$).
- This is an *extreme* case, we tried to cover more rounds, but we recovered only surrounding linear layers.
- Consider the case when $\hat{H}(F) = \begin{bmatrix} \mathbf{0} & \mathbf{0} \\ \mathbf{0} & ? \end{bmatrix}$. There are $3n^2$ impossible terms of degree $n-1$. But there are more impossible terms of lower degree.

Generalizing to other ANF Monomials

- Previously, we exploited predictable absence of particular terms of degree $n-1$ in the ANFs of some output bits (entries $\hat{H}(F)_{i,j} = 0$).
- This is an *extreme* case, we tried to cover more rounds, but we recovered only surrounding linear layers.
- Consider the case when $\hat{H}(F) = \begin{bmatrix} \mathbf{0} & \mathbf{0} \\ \mathbf{0} & ? \end{bmatrix}$. There are $3n^2$ impossible terms of degree $n-1$. But there are more impossible terms of lower degree.
- The predictable absence of such terms may be used to recover a secret round function.

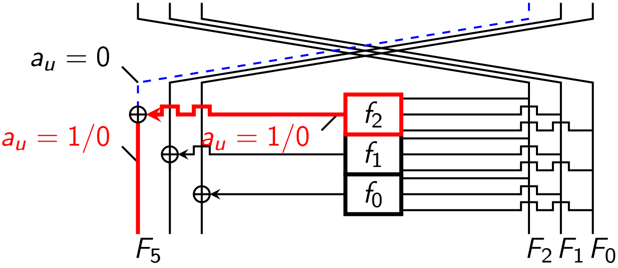
Recovery attack on 5-round Feistel Network (1/2)

- Consider a 5-round Feistel Network F with bijective round functions. Let f be the last round function.



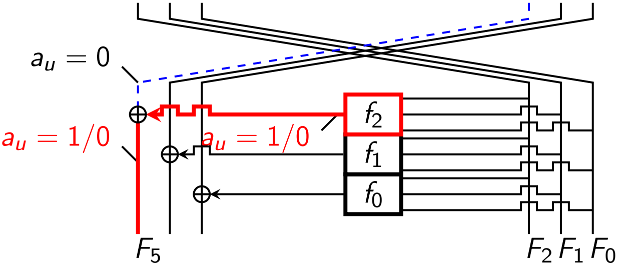
Recovery attack on 5-round Feistel Network (1/2)

- Consider a 5-round Feistel Network F with bijective round functions. Let f be the last round function.
- We can prove that there are more than 2^n monomials which can't occur in the ANFs on right branch of the 4-round FN.



Recovery attack on 5-round Feistel Network (1/2)

- Consider a 5-round Feistel Network F with bijective round functions. Let f be the last round function.
- We can prove that there are more than 2^n monomials which can't occur in the ANFs on right branch of the 4-round FN.
- This gives us information about the last round function f.



Recovery attack on 5-round Feistel Network (2/2)

- We obtain a linear system with 2^n unknowns (ANF coefficients of f_i) and more than 2^n equations.

Recovery attack on 5-round Feistel Network (2/2)

- We obtain a linear system with 2^n unknowns (ANF coefficients of f_i) and more than 2^n equations.
- By solving the system we recover the secret round function f (up to a XOR constant).

Recovery attack on 5-round Feistel Network (2/2)

- We obtain a linear system with 2^n unknowns (ANF coefficients of f_i) and more than 2^n equations.
- By solving the system we recover the secret round function f (up to a XOR constant).
- Complexity is dominated by generating the system and is $O(2^{3n})$.

Generalization by number of rounds

- If the degrees of round functions are low, we can attack more rounds.

Generalization by number of rounds

- If the degrees of round functions are low, we can attack more rounds.

Theorem (Impossible Monomials in Feistel Networks)

Let F be a $2n$-bit Feistel Network with r rounds and round functions of degree at most d. If $d^{r-2} < n$, then there are at least 2^n impossible monomials in the ANFs of right bits of F.

Generalization by number of rounds

- If the degrees of round functions are low, we can attack more rounds.

Theorem (Impossible Monomials in Feistel Networks)

Let F be a $2n$-bit Feistel Network with r rounds and round functions of degree at most d. If $d^{r-2} < n$, then there are at least 2^n impossible monomials in the ANFs of right bits of F.

- Recovery attack when $d^{r-3} < n$. Note that the bound is not tight, the previously described attack on 5 rounds does not satisfy this condition.

Generalization by number of rounds

- If the degrees of round functions are low, we can attack more rounds.

Theorem (Impossible Monomials in Feistel Networks)

Let F be a $2n$-bit Feistel Network with r rounds and round functions of degree at most d. If $d^{r-2} < n$, then there are at least 2^n impossible monomials in the ANFs of right bits of F.

- Recovery attack when $d^{r-3} < n$. Note that the bound is not tight, the previously described attack on 5 rounds does not satisfy this condition.
- Moreover, with low degrees there are less unknowns and we need less impossible monomials.

Plan

Relation with Division Property

- *Division Property* is a tool for integral attacks introduced recently by Todo.

Relation with Division Property

- *Division Property* is a tool for integral attacks introduced recently by Todo.
- *Division Property* allows to find cubes of dimension $2n-1$ (or less) over which a given Feistel Network sums to zero.

Relation with Division Property

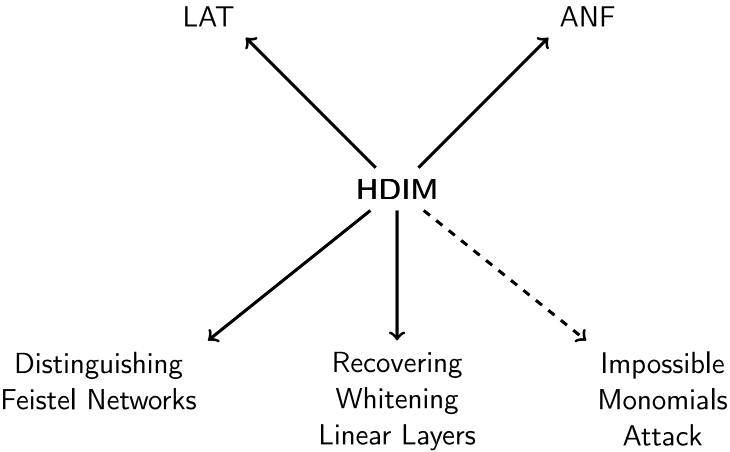
- *Division Property* is a tool for integral attacks introduced recently by Todo.
- *Division Property* allows to find cubes of dimension $2n - 1$ (or less) over which a given Feistel Network sums to zero.
- Such cubes correspond to the absent ANF coefficients of degree $2n - 1$ (or less) which correspond to zero items in HDIM.

Relation with Division Property

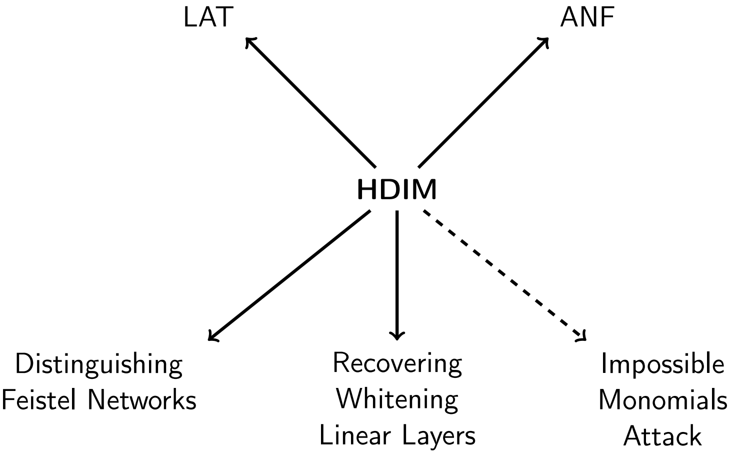
- *Division Property* is a tool for integral attacks introduced recently by Todo.
- *Division Property* allows to find cubes of dimension $2n - 1$ (or less) over which a given Feistel Network sums to zero.
- Such cubes correspond to the absent ANF coefficients of degree $2n - 1$ (or less) which correspond to zero items in HDIM.
- The results for concrete Feistel Networks obtained by Todo are very similar to ours.

Plan

Conclusions



Conclusions



Thank you!