Radbound University

Markov Eigenvalues

Joan Daemen and Shahram Rasoozadeh, Radboud University NL and Bochum University DE

BFA, September 10, 2024
Dubrovnik, Croatia

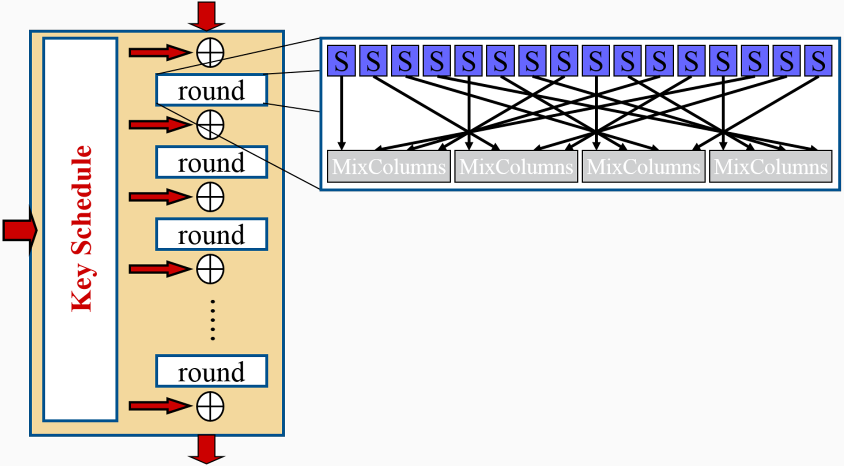
ESCADA

Key-alternating block ciphers

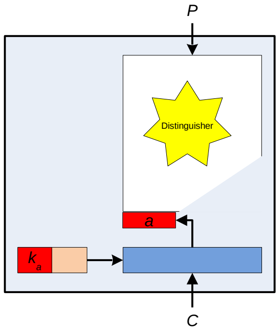
- r-fold iteration of a relatively simple round function R
- alternated with round key additions

Key-alternating block ciphers

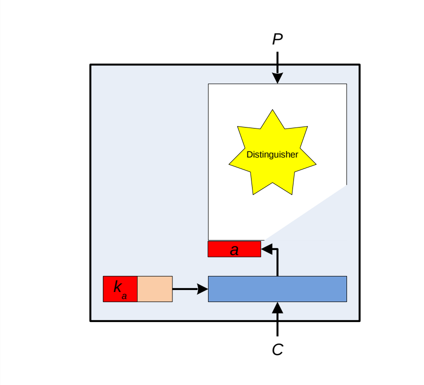
- r-fold iteration of a relatively simple round function R
- alternated with round key additions



Statistical attacks

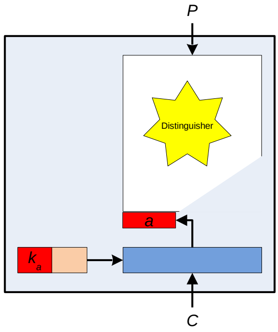


Statistical attacks

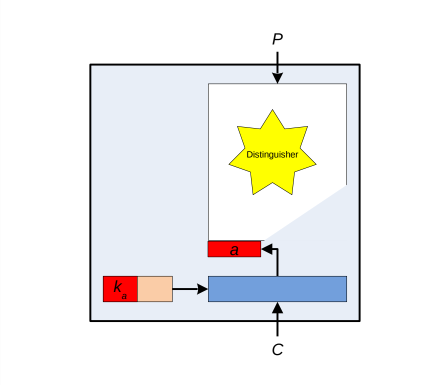


- Example: *Distinguisher*-based key recovery
  - property likely absent in a random permutation
  - to recover part of the last round key

Statistical attacks

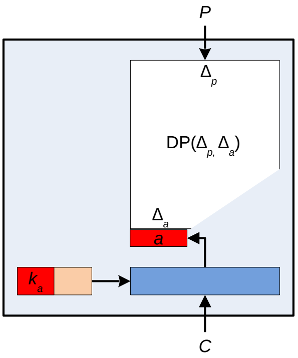


- Example: *Distinguisher*-based key recovery
  - property likely absent in a random permutation
  - to recover part of the last round key
- Attack using Ω over $r-1$ rounds, has two phases:
  - online: get many couples $P_i, C_i = \mathrm{B}_K(P_i)$
  - offline: guess part of last round key k_a and $\forall i$ compute a_i

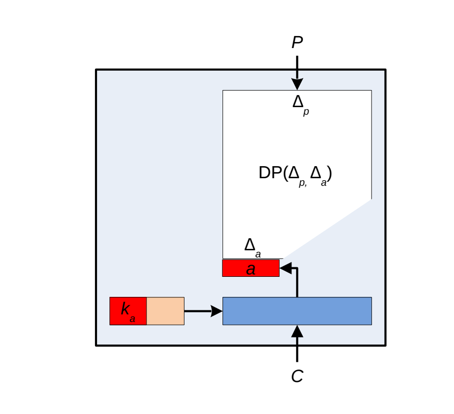


- Example: *Distinguisher*-based key recovery
  - property likely absent in a random permutation
  - to recover part of the last round key
- Attack using Ω over $r-1$ rounds, has two phases:
  - online: get many couples $P_i, C_i = \mathrm{B}_K(P_i)$
  - offline: guess part of last round key k_a and $\forall i$ compute a_i
- This works if
  - guessed k_a gives access to last round input
  - right guess exhibits Ω
  - wrong guess doesn't

Differential cryptanalysis

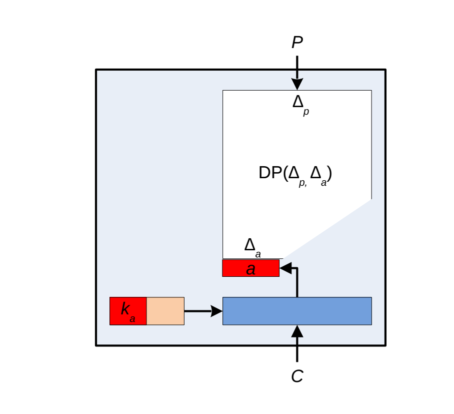


Differential cryptanalysis



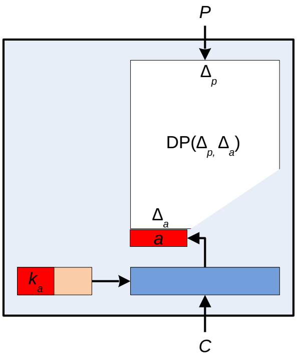
- Statistical attack with following distinguisher:

Differential cryptanalysis



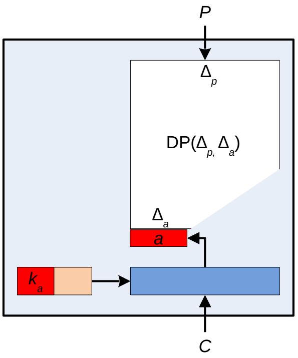
- Statistical attack with following distinguisher:
  - inputs P_i and P_i^* with $P_i \oplus P_i^* = \Delta_p$
  - lead to difference Δ_a at input of last round

Differential cryptanalysis



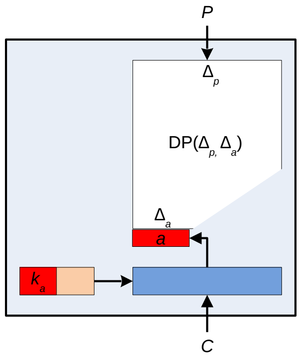
- Statistical attack with following distinguisher:
  - inputs P_i and P_i^* with $P_i \oplus P_i^* = \Delta_p$
  - lead to difference Δ_a at input of last round
  - with some probability $\mathrm{DP}(\Delta_p, \Delta_a) \ggg 2^{-b}$
  - this probability in general depends on the key K

Differential cryptanalysis



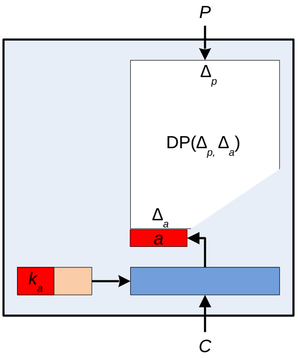
- Statistical attack with following distinguisher:
  - inputs P_i and P_i^* with $P_i \oplus P_i^* = \Delta_p$
  - lead to difference Δ_a at input of last round
  - with some probability $\mathrm{DP}(\Delta_p, \Delta_a) \ggg 2^{-b}$
  - this probability in general depends on the key K
- Requires about $1/\mathrm{DP}(\Delta_p, \Delta_a)$ input/output pairs

Differential cryptanalysis



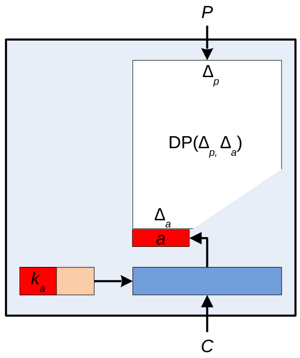
- Statistical attack with following distinguisher:
  - inputs P_i and P_i^* with $P_i \oplus P_i^* = \Delta_p$
  - lead to difference Δ_a at input of last round
  - with some probability $\mathrm{DP}(\Delta_p, \Delta_a) \ggg 2^{-b}$
  - this probability in general depends on the key K
- Requires about $1/\mathrm{DP}(\Delta_p, \Delta_a)$ input/output pairs
- Terminology:
  - (Δ_p, Δ_a) is called a *differential*

Differential cryptanalysis



- Statistical attack with following distinguisher:
  - inputs P_i and P_i^* with $P_i \oplus P_i^* = \Delta_p$
  - lead to difference Δ_a at input of last round
  - with some probability $\mathrm{DP}(\Delta_p, \Delta_a) \ggg 2^{-b}$
  - this probability in general depends on the key K
- Requires about $1/\mathrm{DP}(\Delta_p, \Delta_a)$ input/output pairs
- Terminology:
  - (Δ_p, Δ_a) is called a *differential*
  - $\mathrm{EDP}(\Delta_p, \Delta_a)$ its expected differential probability: $\mathrm{DP}(\Delta_p, \Delta_a)$ averaged over all round key sequences

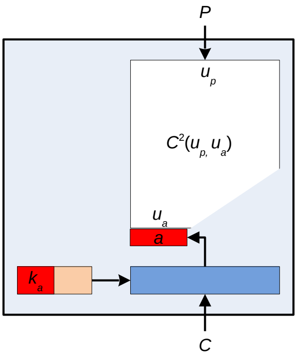
Differential cryptanalysis

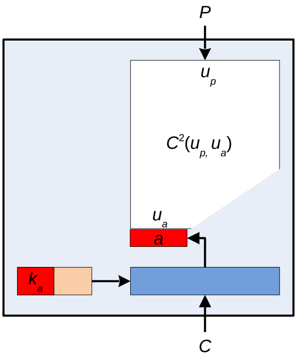


- Statistical attack with following distinguisher:
  - inputs P_i and P_i^* with $P_i \oplus P_i^* = \Delta_p$
  - lead to difference Δ_a at input of last round
  - with some probability $\mathrm{DP}(\Delta_p, \Delta_a) \ggg 2^{-b}$
  - this probability in general depends on the key K
- Requires about $1/\mathrm{DP}(\Delta_p, \Delta_a)$ input/output pairs
- Terminology:
  - (Δ_p, Δ_a) is called a *differential*
  - $\mathrm{EDP}(\Delta_p, \Delta_a)$ its expected differential probability: $\mathrm{DP}(\Delta_p, \Delta_a)$ averaged over all round key sequences

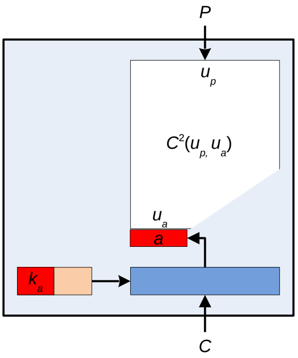
Designers are expected to show their cipher has no differentials with high EDP

Linear cryptanalysis



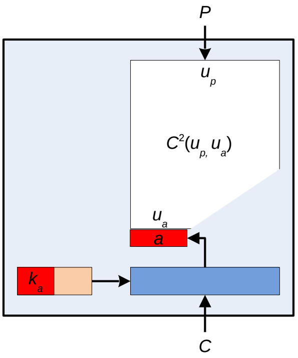


- Statistical attack with following distinguisher:

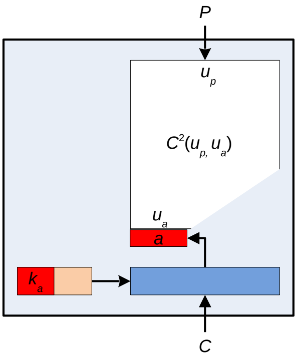


- Statistical attack with following distinguisher:
  - correlation between sum of input bits $u_p^\top P$
  - ... and sum of bits $u_a^\top A$ at input of last round

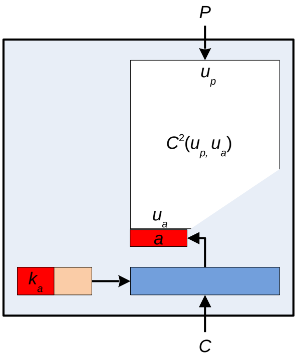
Linear cryptanalysis



- Statistical attack with following distinguisher:
  - correlation between sum of input bits $u_p^\top P$
  - ... and sum of bits $u_a^\top A$ at input of last round
  - with $|\mathrm{C}(u_a, u_p)| \ggg 2^{b/2}$
  - this correlation in general depends on the key K

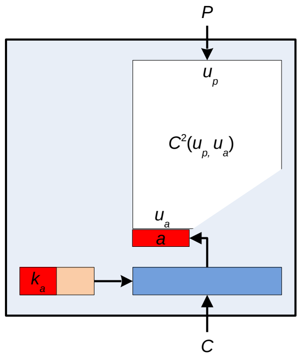


- Statistical attack with following distinguisher:
  - correlation between sum of input bits $u_p^\top P$
  - ...and sum of bits $u_a^\top A$ at input of last round
  - with $|\mathrm{C}(u_a, u_p)| \ggg 2^{b/2}$
  - this correlation in general depends on the key K
- Requires about $1/\mathrm{Corr}^2(u_a, u_p)$ input/output pairs

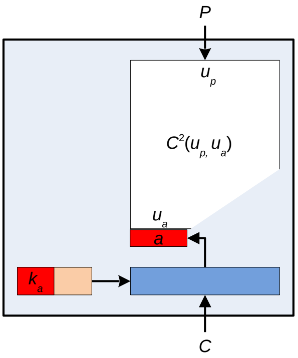


- Statistical attack with following distinguisher:
  - correlation between sum of input bits $u_p^\top P$
  - ...and sum of bits $u_a^\top A$ at input of last round
  - with $|\mathrm{C}(u_a, u_p)| \ggg 2^{b/2}$
  - this correlation in general depends on the key K
- Requires about $1/\mathrm{Corr}^2(u_a, u_p)$ input/output pairs
- Terminology:

Linear cryptanalysis



- Statistical attack with following distinguisher:
  - correlation between sum of input bits $u_p^\top P$
  - ...and sum of bits $u_a^\top A$ at input of last round
  - with $|\mathrm{C}(u_a, u_p)| \ggg 2^{b/2}$
  - this correlation in general depends on the key K
- Requires about $1/\mathrm{Corr}^2(u_a, u_p)$ input/output pairs
- Terminology:
  - (u_a, u_p) is called a *linear approximation*



- Statistical attack with following distinguisher:
  - correlation between sum of input bits $u_p^\top P$
  - ...and sum of bits $u_a^\top A$ at input of last round
  - with $|\mathrm{C}(u_a, u_p)| \ggg 2^{b/2}$
  - this correlation in general depends on the key K
- Requires about $1/\mathrm{Corr}^2(u_a, u_p)$ input/output pairs
- Terminology:
  - (u_a, u_p) is called a *linear approximation*
  - $\mathrm{LP}(u_a, u_p)$ its linear probability (or potential): $\mathrm{C}^2(u_a, u_p)$ averaged over all round key sequences

Designers are expected to show absence of linear approximations with high LP

Express $\mathrm{EDP}(\Delta_p, \Delta_c)$ as a function of DP of S-box differentials

Express $\mathrm{EDP}(\Delta_p, \Delta_c)$ as a function of DP of S-box differentials

- The following was proven in [Lai, Massey & Murphy, 1992]:
  - let D be a $2^b - 1 \times 2^b - 1$ matrix with $\mathrm{DP}(x, y)$ over R in row y and column x

Express $\mathrm{EDP}(\Delta_p, \Delta_c)$ as a function of DP of S-box differentials

- The following was proven in [Lai, Massey & Murphy, 1992]:
  - let D be a $2^b - 1 \times 2^b - 1$ matrix with $\mathrm{DP}(x, y)$ over R in row y and column x
  - then $\mathrm{EDP}(\Delta_p, \Delta_c)$ is the entry in row Δ_c and column Δ_p of D^r

Express $\mathrm{EDP}(\Delta_p, \Delta_c)$ as a function of DP of S-box differentials

- The following was proven in [Lai, Massey & Murphy, 1992]:
  - let D be a $2^b - 1 \times 2^b - 1$ matrix with $\mathrm{DP}(x, y)$ over R in row y and column x
  - then $\mathrm{EDP}(\Delta_p, \Delta_c)$ is the entry in row Δ_c and column Δ_p of D^r
  - For a good round function D^r converges quickly to the uniform matrix with all entries $(2^b - 1)^{-1}$

Express $\mathrm{EDP}(\Delta_p, \Delta_c)$ as a function of DP of S-box differentials

- The following was proven in [Lai, Massey & Murphy, 1992]:
  - let D be a $2^b - 1 \times 2^b - 1$ matrix with $\mathrm{DP}(x, y)$ over R in row y and column x
  - then $\mathrm{EDP}(\Delta_p, \Delta_c)$ is the entry in row Δ_c and column Δ_p of D^r
  - For a good round function D^r converges quickly to the uniform matrix with all entries $(2^b - 1)^{-1}$
- D of a round function R
  - a huge matrix of 2^{2b} probabilities

Express $\mathrm{EDP}(\Delta_p, \Delta_c)$ as a function of DP of S-box differentials

- The following was proven in [Lai, Massey & Murphy, 1992]:
  - let D be a $2^b - 1 \times 2^b - 1$ matrix with $\mathrm{DP}(x, y)$ over R in row y and column x
  - then $\mathrm{EDP}(\Delta_p, \Delta_c)$ is the entry in row Δ_c and column Δ_p of D^r
  - For a good round function D^r converges quickly to the uniform matrix with all entries $(2^b - 1)^{-1}$
- D of a round function R
  - a huge matrix of 2^{2b} probabilities
  - but for the typical round function R its entries are easy to compute

Express $\mathsf{EDP}(\Delta_p, \Delta_c)$ as a function of DP of S-box differentials

- The following was proven in [Lai, Massey & Murphy, 1992]:
  - let D be a $2^b - 1 \times 2^b - 1$ matrix with $\mathsf{DP}(x, y)$ over R in row y and column x
  - then $\mathsf{EDP}(\Delta_p, \Delta_c)$ is the entry in row Δ_c and column Δ_p of D^r
  - For a good round function D^r converges quickly to the uniform matrix with all entries $(2^b - 1)^{-1}$
- D of a round function R
  - a huge matrix of 2^{2b} probabilities
  - but for the typical round function R its entries are easy to compute
  - e.g., if non-linear operation consists of an S-box layer in terms of entries of D of the S-boxes

Express $\mathrm{EDP}(\Delta_p, \Delta_c)$ as a function of DP of S-box differentials

- The following was proven in [Lai, Massey & Murphy, 1992]:
  - let D be a $2^b - 1 \times 2^b - 1$ matrix with $\mathrm{DP}(x, y)$ over R in row y and column x
  - then $\mathrm{EDP}(\Delta_p, \Delta_c)$ is the entry in row Δ_c and column Δ_p of D^r
  - For a good round function D^r converges quickly to the uniform matrix with all entries $(2^b - 1)^{-1}$
- D of a round function R
  - a huge matrix of 2^{2b} probabilities
  - but for the typical round function R its entries are easy to compute
  - e.g., if non-linear operation consists of an S-box layer
    in terms of entries of D of the S-boxes
- D of an S-box: DDT with entries divided by 2^n (and row 0 and col. 0 removed)

Round function resistance against differential cryptanalysis

Round function resistance against differential cryptanalysis

We can do the eigenvalue decomposition: $D = Q\Lambda Q^{-1}$ with

- Λ a diagonal matrix with the (complex) eigenvalues in decreasing order of modulus
- Q an orthogonal matrix with the eigenvectors as its columns

Round function resistance against differential cryptanalysis

We can do the eigenvalue decomposition: $D = Q\Lambda Q^{-1}$ with

- Λ a diagonal matrix with the (complex) eigenvalues in decreasing order of modulus
- Q an orthogonal matrix with the eigenvectors as its columns

$$D^r = Q\Lambda^r Q^{-1}$$

Round function resistance against differential cryptanalysis

We can do the eigenvalue decomposition: $D = Q\Lambda Q^{-1}$ with

- Λ a diagonal matrix with the (complex) eigenvalues in decreasing order of modulus
- Q an orthogonal matrix with the eigenvectors as its columns

$$D^r = Q\Lambda^r Q^{-1}$$

D is a *doubly stochastic matrix*: $\sum_b \mathrm{DP}(a, b) = 1$ and $\sum_a \mathrm{DP}(a, b) = 1$

- The eigenvalues of D are on or within the unit circle
- It has an eigenvalue 1 with eigenvector the uniform vector
- There are $2^b - 2$ other eigenvalues

Round function resistance against differential cryptanalysis

We can do the eigenvalue decomposition: $D = Q\Lambda Q^{-1}$ with

- Λ a diagonal matrix with the (complex) eigenvalues in decreasing order of modulus
- Q an orthogonal matrix with the eigenvectors as its columns

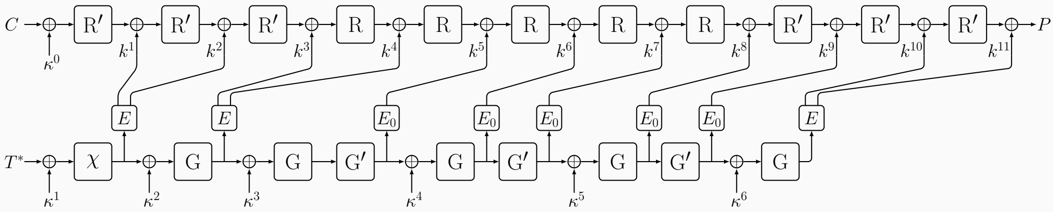
$$D^r = Q\Lambda^r Q^{-1}$$

D is a *doubly stochastic matrix*: $\sum_b \mathrm{DP}(a, b) = 1$ and $\sum_a \mathrm{DP}(a, b) = 1$

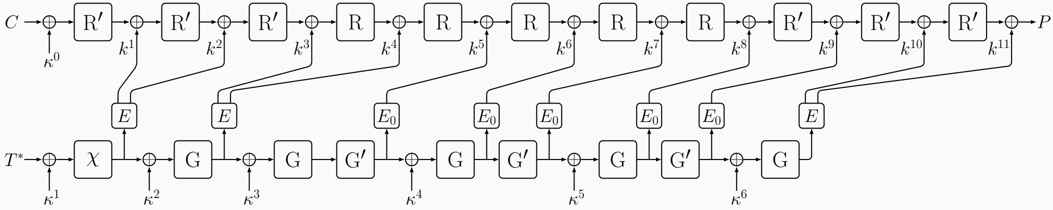
- The eigenvalues of D are on or within the unit circle
- It has an eigenvalue 1 with eigenvector the uniform vector
- There are $2^b - 2$ other eigenvalues

So we wish the $2^b - 2$ other eigenvalues to be as small as possible

BipBip: a small low-latency tweakable block cipher [Belkheyar et al., TCHES 2023]

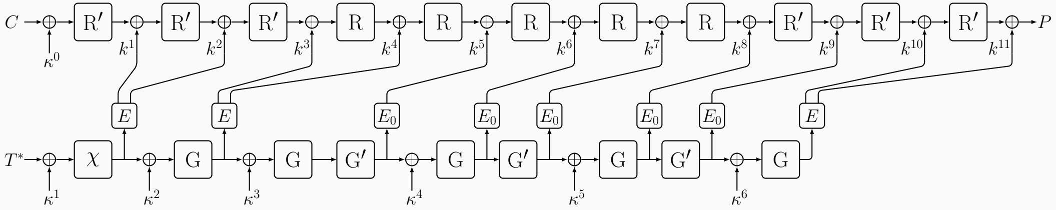


BipBip: a small low-latency tweakable block cipher [Belkheyar et al., TCHES 2023]



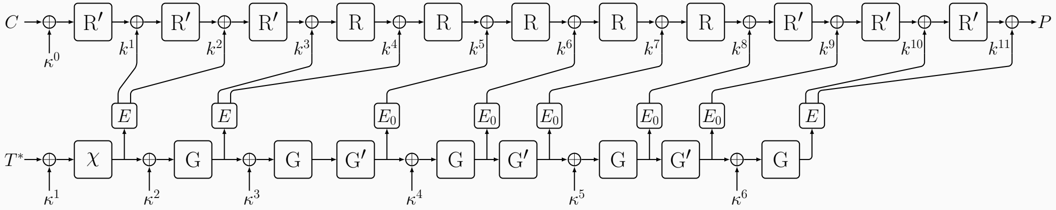
- *Tweakable*: additional input T' giving different permutations for a given key K

BipBip: a small low-latency tweakable block cipher [Belkheyar et al., TCHES 2023]



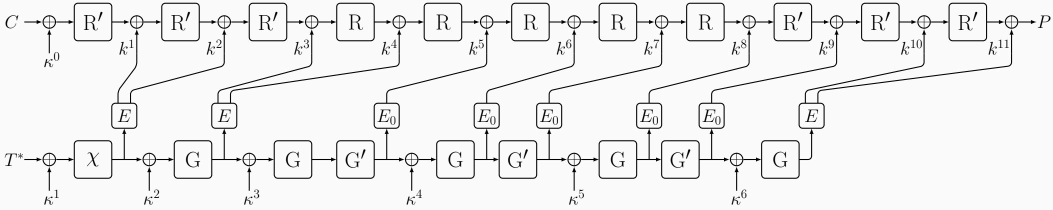
- *Tweakable*: additional input T' giving different permutations for a given key K
- For a fixed tweak it is a key-alternating cipher

BipBip: a small low-latency tweakable block cipher [Belkheyar et al., TCHES 2023]



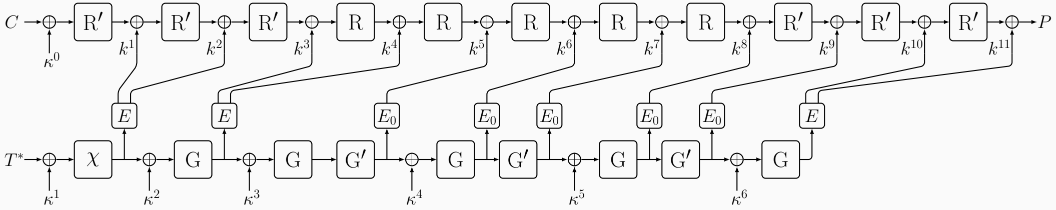
- *Tweakable*: additional input T' giving different permutations for a given key K
- For a fixed tweak it is a key-alternating cipher
- Width $b = 24$ and non-linear layer is a layer of four 6-bit S-boxes

BipBip: a small low-latency tweakable block cipher [Belkheyar et al., TCHES 2023]



- *Tweakable*: additional input T' giving different permutations for a given key K
- For a fixed tweak it is a key-alternating cipher
- Width $b = 24$ and non-linear layer is a layer of four 6-bit S-boxes
- Columns of D^r can be efficiently computed using [Eichlseder et al., Indocrypt 2020]

BipBip: a small low-latency tweakable block cipher [Belkheyar et al., TCHES 2023]



- *Tweakable*: additional input T' giving different permutations for a given key K
- For a fixed tweak it is a key-alternating cipher
- Width $b = 24$ and non-linear layer is a layer of four 6-bit S-boxes
- Columns of D^r can be efficiently computed using [Eichlseder et al., Indocrypt 2020]
- We did that as part of preliminary cryptanalysis

Sampling D^r for BipBip

Sampling D^r for BipBip

- We computed columns of D^r

Sampling D^r for BipBip

- We computed columns of D^r
- About 2^{20} columns: those for input differences with less than 4 active S-boxes

Sampling D^r for BipBip

- We computed columns of D^r
- About 2^{20} columns: those for input differences with less than 4 active S-boxes
- We report here on the variance of these columns:

r	maximum	average
3	$2^{-57.85}$	$2^{-59.46}$
4	$2^{-73.44}$	$2^{-75.22}$
5	$2^{-89.31}$	$2^{-90.99}$
6	$2^{-105.05}$	$2^{-106.74}$

Sampling D^r for BipBip

- We computed columns of D^r
- About 2^{20} columns: those for input differences with less than 4 active S-boxes
- We report here on the variance of these columns:

r	maximum	average
3	$2^{-57.85}$	$2^{-59.46}$
4	$2^{-73.44}$	$2^{-75.22}$
5	$2^{-89.31}$	$2^{-90.99}$
6	$2^{-105.05}$	$2^{-106.74}$

Clearly the variance decreases exponentially for increasing r

Express $\mathsf{LP}(u_c, u_p)$ as a function of LP of S-box approximations

Express $\mathrm{LP}(u_c, u_p)$ as a function of LP of S-box approximations

- The following was demonstrated in the work of Nyberg and [Daemen/Rijmen, 2002]:

Express $\mathrm{LP}(u_c, u_p)$ as a function of LP of S-box approximations

- The following was demonstrated in the work of Nyberg and [Daemen/Rijmen, 2002]:
  - let L be a $2^b - 1 \times 2^b - 1$ matrix with $\mathrm{LP}(x, y)$ over R in row y and column x

Express $\mathrm{LP}(u_c, u_p)$ as a function of LP of S-box approximations

- The following was demonstrated in the work of Nyberg and [Daemen/Rijmen, 2002]:
  - let L be a $2^b - 1 \times 2^b - 1$ matrix with $\mathrm{LP}(x, y)$ over R in row y and column x
  - then $\mathrm{LP}(u_c, u_p)$ is the entry in row u_p and column u_c of L^r

Express $\mathrm{LP}(u_c, u_p)$ as a function of LP of S-box approximations

- The following was demonstrated in the work of Nyberg and [Daemen/Rijmen, 2002]:
  - let L be a $2^b - 1 \times 2^b - 1$ matrix with $\mathrm{LP}(x, y)$ over R in row y and column x
  - then $\mathrm{LP}(u_c, u_p)$ is the entry in row u_p and column u_c of L^r
  - For a good round function L^r converges to the matrix with all entries $(2^b - 1)^{-1}$

Express $\mathrm{LP}(u_c, u_p)$ as a function of LP of S-box approximations

- The following was demonstrated in the work of Nyberg and [Daemen/Rijmen, 2002]:
  - let L be a $2^b - 1 \times 2^b - 1$ matrix with $\mathrm{LP}(x, y)$ over R in row y and column x
  - then $\mathrm{LP}(u_c, u_p)$ is the entry in row u_p and column u_c of L^r
  - For a good round function L^r converges to the matrix with all entries $(2^b - 1)^{-1}$
- L of a round function R
  - a huge matrix of 2^{2b} correlations
  - but for the typical round function R its entries are easy to compute
  - e.g., if non-linear operation consists of an S-box layer in terms of entries of L of the S-boxes
- L of an S-box: correlation matrix with entries squared

Round function resistance against linear cryptanalysis

We can do the eigenvalue decomposition: $L = R\Lambda' R^{-1}$

$$L^r = R\Lambda'^r R^{-1}$$

L is a doubly stochastic matrix as $\sum_y \mathrm{C}^2(x, y) = 1$ and $\sum_x \mathrm{C}^2(x, y) = 1$

- The eigenvalues of L are on or within the unit circle
- It has an eigenvalue 1 with eigenvector the uniform vector
- There are $2^b - 2$ other eigenvalues

So we wish the $2^b - 2$ other eigenvalues to be as small as possible

Sampling L^r for BipBip

- We computed columns of L^r
- About 2^{20} columns: those with output masks with less than 4 active S-boxes
- We report here on the variance of these columns:

Sampling L^r for BipBip

- We computed columns of L^r
- About 2^{20} columns: those with output masks with less than 4 active S-boxes
- We report here on the variance of these columns:

r	maximum	average
3	$2^{-58.54}$	$2^{-59.75}$
4	$2^{-74.38}$	$2^{-75.55}$
5	$2^{-90.20}$	$2^{-91.37}$
6	$2^{-106.09}$	$2^{-107.18}$

Sampling L^r for BipBip

- We computed columns of L^r
- About 2^{20} columns: those with output masks with less than 4 active S-boxes
- We report here on the variance of these columns:

r	maximum	average
3	$2^{-58.54}$	$2^{-59.75}$
4	$2^{-74.38}$	$2^{-75.55}$
5	$2^{-90.20}$	$2^{-91.37}$
6	$2^{-106.09}$	$2^{-107.18}$

so for L^r

r	maximum	average
3	$2^{-57.85}$	$2^{-59.46}$
4	$2^{-73.44}$	$2^{-75.22}$
5	$2^{-89.31}$	$2^{-90.99}$
6	$2^{-105.05}$	$2^{-106.74}$

what we had for D^r

Links between different matrices

Links between different matrices

Transition matrix linearizes mapping

[Vaudenay/Chabaud 1994]

$$T_{\mathsf{R}}[y, x] = \delta(y - \mathsf{R}(x))$$

Links between different matrices

Transition matrix linearizes mapping

[Vaudenay/Chabaud 1994]

$$T_{\mathsf{R}}[y, x] = \delta(y - \mathsf{R}(x))$$

D is self-convolution of T

$$D = 2^{-b} T * T$$

Links between different matrices

Transition matrix linearizes mapping

[Vaudenay/Chabaud 1994]

$$T_{\mathsf{R}}[y, x] = \delta(y - \mathsf{R}(x))$$

D is self-convolution of T

$$D = 2^{-b} T * T$$

Walsh-Hadamard change of basis gives

[Beyne 2023]

$$C = H T^{\top} H^{-1}$$

Links between different matrices

Transition matrix linearizes mapping

[Vaudenay/Chabaud 1994]

$$T_{\mathsf{R}}[y, x] = \delta(y - \mathsf{R}(x))$$

Walsh-Hadamard change of basis gives

[Beyne 2023]

$$C = HT^{\top}H^{-1}$$

D is self-convolution of T

$$D = 2^{-b}T * T$$

L is C with components squared

$$L = C \odot C$$

Links between different matrices

Transition matrix linearizes mapping

[Vaudenay/Chabaud 1994]

$$T_{\mathrm{R}}[y, x] = \delta(y - \mathrm{R}(x))$$

Walsh-Hadamard change of basis gives

[Beyne 2023]

$$C = HT^\top H^{-1}$$

D is self-convolution of T

$$D = 2^{-b} T * T$$

L is C with components squared

$$L = C \odot C$$

(inverse) Walsh-Hadamard converts componentwise product in convolution, so

$$L = HD^\top H^{-1}$$

Iterating rounds

Iterating rounds

- For B: key alternating cipher with rounds R_1 to R_r

$$D_B = D_{\mathrm{R}_r} \cdots D_{\mathrm{R}_2} D_{\mathrm{R}_1} \qquad\qquad L_B = L_{\mathrm{R}_1} L_{\mathrm{R}_2} \cdots L_{\mathrm{R}_r}$$

Iterating rounds

- For B: key alternating cipher with rounds R_1 to R_r

$$D_B = D_{\mathrm{R}_r} \cdots D_{\mathrm{R}_2} D_{\mathrm{R}_1} \qquad\qquad L_B = L_{\mathrm{R}_1} L_{\mathrm{R}_2} \cdots L_{\mathrm{R}_r}$$

- For F: permutation (or fixed-key block cipher) with rounds R_1 to R_r

$$T_F = T_{\mathrm{R}_r} \cdots T_{\mathrm{R}_2} T_{\mathrm{R}_1} \qquad\qquad C_F = C_{\mathrm{R}_1} C_{\mathrm{R}_2} \cdots C_{\mathrm{R}_r}$$

Iterating rounds

- For B: key alternating cipher with rounds R_1 to R_r

$$D_B = D_{\mathrm{R}_r} \cdots D_{\mathrm{R}_2} D_{\mathrm{R}_1} \qquad L_B = L_{\mathrm{R}_1} L_{\mathrm{R}_2} \cdots L_{\mathrm{R}_r}$$

- For F: permutation (or fixed-key block cipher) with rounds R_1 to R_r

$$T_F = T_{\mathrm{R}_r} \cdots T_{\mathrm{R}_2} T_{\mathrm{R}_1} \qquad C_F = C_{\mathrm{R}_1} C_{\mathrm{R}_2} \cdots C_{\mathrm{R}_r}$$

- We also have

$$D_F = 2^{-b} T_F * T_F \qquad L_F = C_F \odot C_F$$

Iterating rounds

- For B: key alternating cipher with rounds R_1 to R_r

$$D_B = D_{\mathsf{R}_r} \cdots D_{\mathsf{R}_2} D_{\mathsf{R}_1} \qquad L_B = L_{\mathsf{R}_1} L_{\mathsf{R}_2} \cdots L_{\mathsf{R}_r}$$

- For F: permutation (or fixed-key block cipher) with rounds R_1 to R_r

$$T_F = T_{\mathsf{R}_r} \cdots T_{\mathsf{R}_2} T_{\mathsf{R}_1} \qquad C_F = C_{\mathsf{R}_1} C_{\mathsf{R}_2} \cdots C_{\mathsf{R}_r}$$

- We also have

$$D_F = 2^{-b} T_F * T_F \qquad L_F = C_F \odot C_F$$

- T and C have the same eigenvalues that were investigated/used by Beyne

Iterating rounds

- For B: key alternating cipher with rounds R_1 to R_r

$$D_B = D_{\mathrm{R}_r} \cdots D_{\mathrm{R}_2} D_{\mathrm{R}_1} \qquad L_B = L_{\mathrm{R}_1} L_{\mathrm{R}_2} \cdots L_{\mathrm{R}_r}$$

- For F: permutation (or fixed-key block cipher) with rounds R_1 to R_r

$$T_F = T_{\mathrm{R}_r} \cdots T_{\mathrm{R}_2} T_{\mathrm{R}_1} \qquad C_F = C_{\mathrm{R}_1} C_{\mathrm{R}_2} \cdots C_{\mathrm{R}_r}$$

- We also have

$$D_F = 2^{-b} T_F * T_F \qquad L_F = C_F \odot C_F$$

- T and C have the same eigenvalues that were investigated/used by Beyne
- D and L have the same eigenvalues and have not been investigated yet (as far as we know)

Interesting research questions

Interesting research questions

- For some concrete ciphers resistance against LC and DC is quite different
  - examples: PRESENT block cipher [Bogdanov et al. CHES 2007] and Gaston permutation [elHirch et al. CRYPTO 2020]
  - how can that be reconciled with similarity of D and L?

Interesting research questions

- For some concrete ciphers resistance against LC and DC is quite different
  - examples: PRESENT block cipher [Bogdanov et al. CHES 2007] and Gaston permutation [elHirch et al. CRYPTO 2020]
  - how can that be reconciled with similarity of D and L?
- Can we use eigenvalues of R to design/choose better linear layers?

Interesting research questions

- For some concrete ciphers resistance against LC and DC is quite different
  - examples: PRESENT block cipher [Bogdanov et al. CHES 2007] and Gaston permutation [elHirch et al. CRYPTO 2020]
  - how can that be reconciled with similarity of D and L?
- Can we use eigenvalues of R to design/choose better linear layers?
- We can classify S-boxes by the value of their eigenvalues or determinant
  - are these meaningful?
  - are these classifications equivalent to an existing ones?

Interesting research questions

- For some concrete ciphers resistance against LC and DC is quite different
  - examples: PRESENT block cipher [Bogdanov et al. CHES 2007] and Gaston permutation [elHirch et al. CRYPTO 2020]
  - how can that be reconciled with similarity of D and L?
- Can we use eigenvalues of R to design/choose better linear layers?
- We can classify S-boxes by the value of their eigenvalues or determinant
  - are these meaningful?
  - are these classifications equivalent to an existing ones?
- Are there ciphers in the wild with a non-trivial eigenvalue on the unit circle?

Interesting research questions

- For some concrete ciphers resistance against LC and DC is quite different
  - examples: PRESENT block cipher [Bogdanov et al. CHES 2007] and Gaston permutation [elHirch et al. CRYPTO 2020]
  - how can that be reconciled with similarity of D and L?
- Can we use eigenvalues of R to design/choose better linear layers?
- We can classify S-boxes by the value of their eigenvalues or determinant
  - are these meaningful?
  - are these classifications equivalent to an existing ones?
- Are there ciphers in the wild with a non-trivial eigenvalue on the unit circle?
- Can we formulate an attack exploiting largest non-trivial eigenvalue and vector?

Interesting research questions

- For some concrete ciphers resistance against LC and DC is quite different
  - examples: PRESENT block cipher [Bogdanov et al. CHES 2007] and Gaston permutation [elHirch et al. CRYPTO 2020]
  - how can that be reconciled with similarity of D and L?
- Can we use eigenvalues of R to design/choose better linear layers?
- We can classify S-boxes by the value of their eigenvalues or determinant
  - are these meaningful?
  - are these classifications equivalent to an existing ones?
- Are there ciphers in the wild with a non-trivial eigenvalue on the unit circle?
- Can we formulate an attack exploiting largest non-trivial eigenvalue and vector?
- What about singular value decomposition of D^r/L^r?

Interesting research questions

- For some concrete ciphers resistance against LC and DC is quite different
  - examples: PRESENT block cipher [Bogdanov et al. CHES 2007] and Gaston permutation [elHirch et al. CRYPTO 2020]
  - how can that be reconciled with similarity of D and L?
- Can we use eigenvalues of R to design/choose better linear layers?
- We can classify S-boxes by the value of their eigenvalues or determinant
  - are these meaningful?
  - are these classifications equivalent to an existing ones?
- Are there ciphers in the wild with a non-trivial eigenvalue on the unit circle?
- Can we formulate an attack exploiting largest non-trivial eigenvalue and vector?
- What about singular value decomposition of D^r/L^r?
- etc. etc.

Illustration: variants of the PRESENT S-box

We computed the eigenvalues for 1000 variants of the Present S-box obtained by applying different linear mappings

Illustration: variants of the PRESENT S-box

We computed the eigenvalues for 1000 variants of the Present S-box obtained by applying different linear mappings

We report on the eigenvalues of *best* one and *worst* one

Illustration: variants of the PRESENT S-box

We computed the eigenvalues for 1000 variants of the Present S-box obtained by applying different linear mappings

We report on the eigenvalues of *best* one and *worst* one

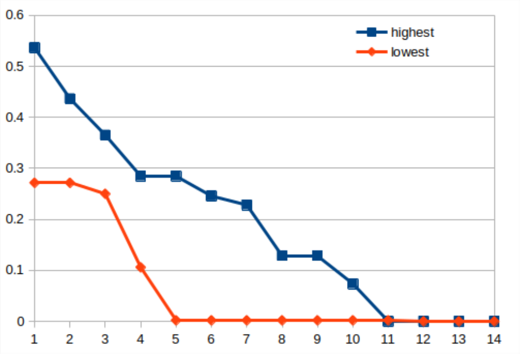
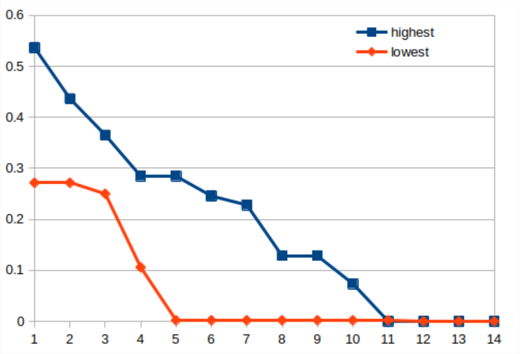


Illustration: variants of the PRESENT S-box

We computed the eigenvalues for 1000 variants of the Present S-box obtained by applying different linear mappings

We report on the eigenvalues of *best* one and *worst* one



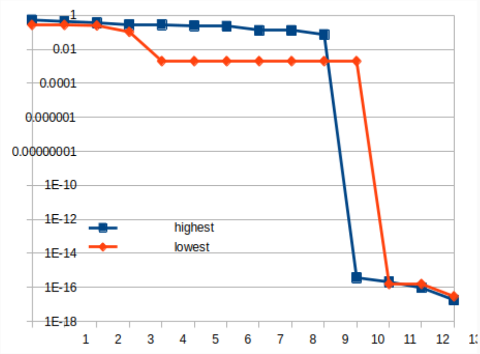
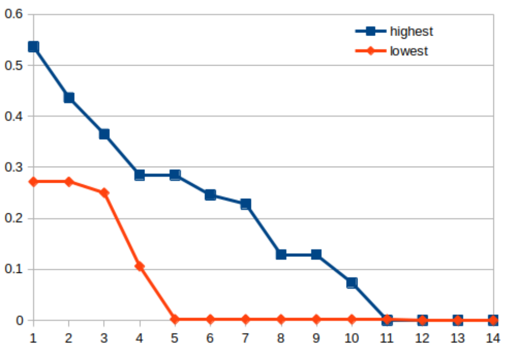
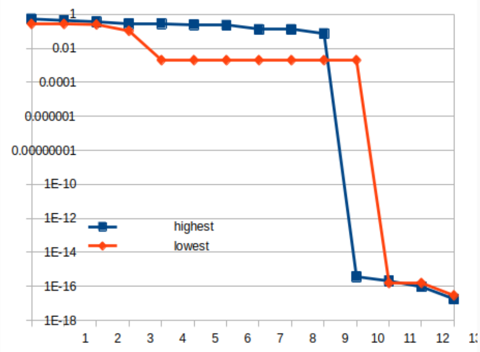


Illustration: variants of the PRESENT S-box

We computed the eigenvalues for 1000 variants of the Present S-box obtained by applying different linear mappings

We report on the eigenvalues of *best* one and *worst* one

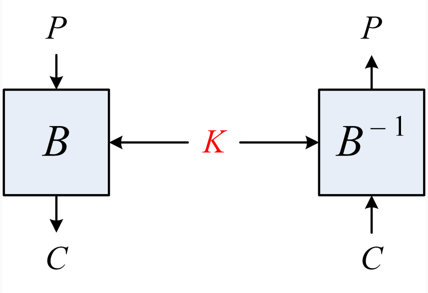




Thanks for your attention!

Supporting slides

Block ciphers



- Permutation B_K operating on $\{0,1\}^b$ with b the block length
- One permutation for each key K

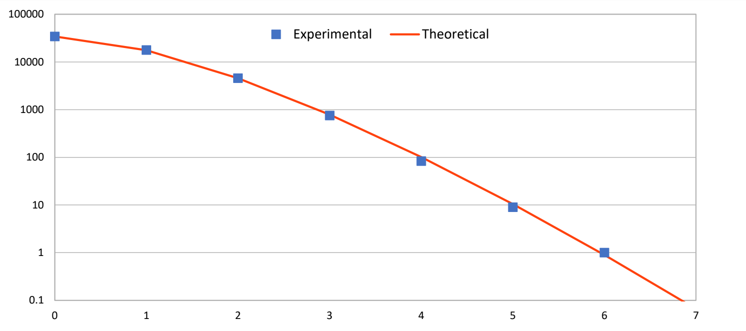
B is called strong pseudorandom permutation (SPRP) secure if …

it is hard to distinguish B_K from a random permutation for an adversary

- …that can query $B_K(P)$ and $B_K^{-1}(C)$ with chosen P or C
- but does not know the secret key K

What EDP means for the fixed-key DP of differentials

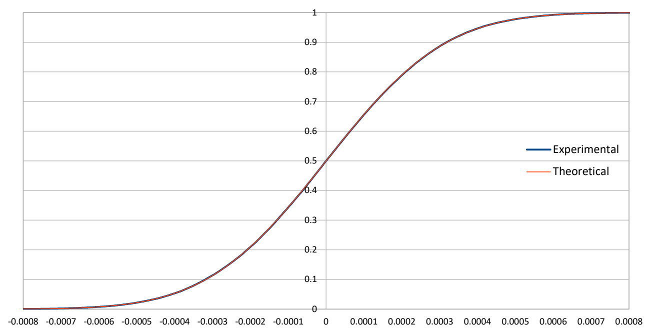
- For fixed-key-and-tweak a differential (a, b) has an integer number of pairs $N(a, b)$
- So $\mathrm{DP}(a, b)$ must be a multiple of $2^{1-b} (= 2^{-23})$
- [Albrecht/Leander SAC '12] conjecture $N(a, b)$ follows Poisson w. $\lambda = 2^{b-1}\,\mathrm{EDP}(a, b)$
- Our experiments confirm this conjecture:



The EDP value can still be *measured* by sampling the differential for many tweaks

What LP means for the fixed-key correlation of linear approximations

- Fixed-key-and-tweak correlation of a linear approximation (u_c, u_p) has a distribution with mean 0 and variance $\mathrm{LP}(u_c, u_p)$
- [Daemen et al. '08] conjecture that for enough rounds this has a normal distribution
- Our experiments confirm this conjecture:



$\mathrm{LP}(u_c, u_p)$ can be *measured* by sampling the linear approximation for many tweaks

Interesting research questions: difference between average and fixed-key values

- For B: 2-round cipher with rounds R, the average DP and LP values are given by

$$D_B = (T * T)^2 \qquad\qquad L_B = (C \odot C)^2$$

- For F: permutation (or fixed-key block cipher) with round R the exact DP and squared values are

$$D_F = (T^2) * (T^2) \qquad\qquad L_F = (C^2) \odot (C^2)$$

- The deviation between average values and fixed-key values are:

$$(T^2) * (T^2) - (T * T)^2 \qquad\qquad (C^2) \odot (C^2) - (C \odot C)^2 \qquad (1)$$

Can (1) be used to investigate key-dependence?