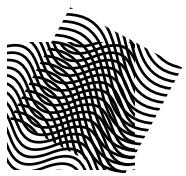
Block cipher invariants
as eigenvectors of correlation matrices

Tim Beyne

COSIC / ESAT, KULeuven

December 3, 2018



COSIC

Joan Daemen

Correlation Matrices

Joan Daemen, René Govaerts, and Joos Vandewalle

Katholieke Universiteit Leuven
ESAT-COSIC
K. Mercierlaan 94, B-3001 Heverlee, Belgium

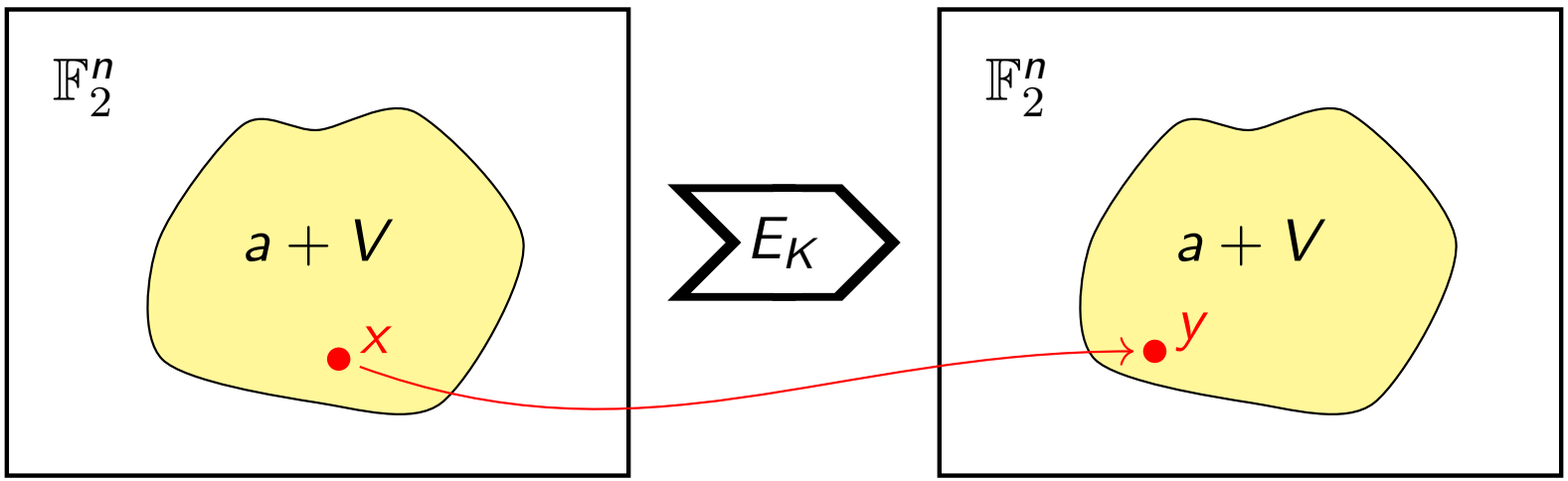
joan.daemen@esat.kuleuven.ac.be

Abstract. In this paper we introduce the *correlation matrix* of a Boolean mapping, a useful concept in demonstrating and proving properties of Boolean functions and mappings. It is argued that correlation matrices are the "natural" representation for the proper understanding and description of the mechanisms of linear cryptanalysis [4]. It is also shown that the difference propagation probabilities and the table consisting of the squared elements of the correlation matrix are linked by a scaled Walsh-Hadamard transform.

Key Words: Boolean Mappings, Linear Cryptanalysis, Correlation Matrices.

Invariant subspaces and nonlinear invariants

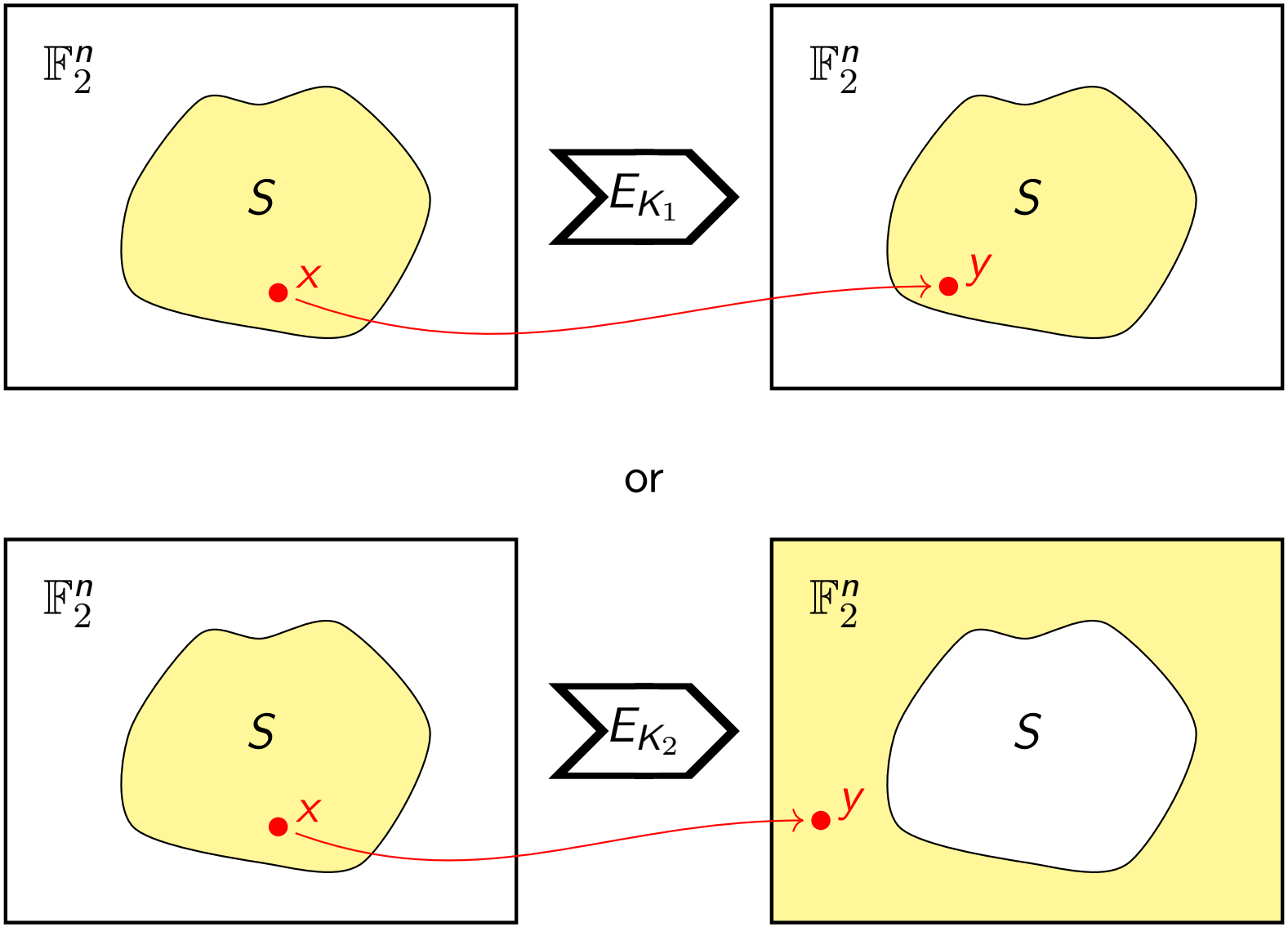
[Leander et al., 2011]



K is a *weak key*

Invariant subspaces and nonlinear invariants

[Todo et al., 2016]



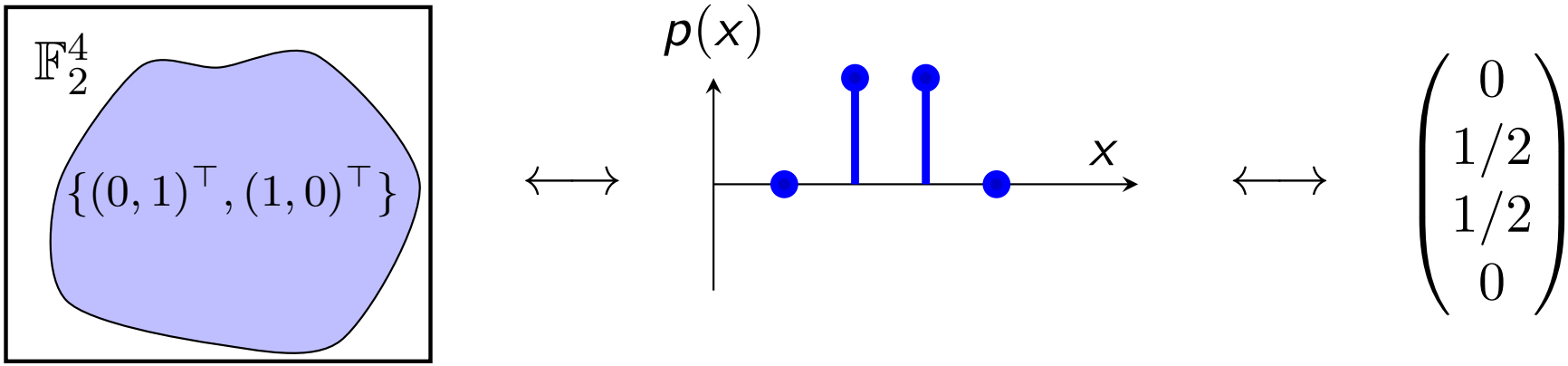
Three problems

1. Improve understanding (theory)

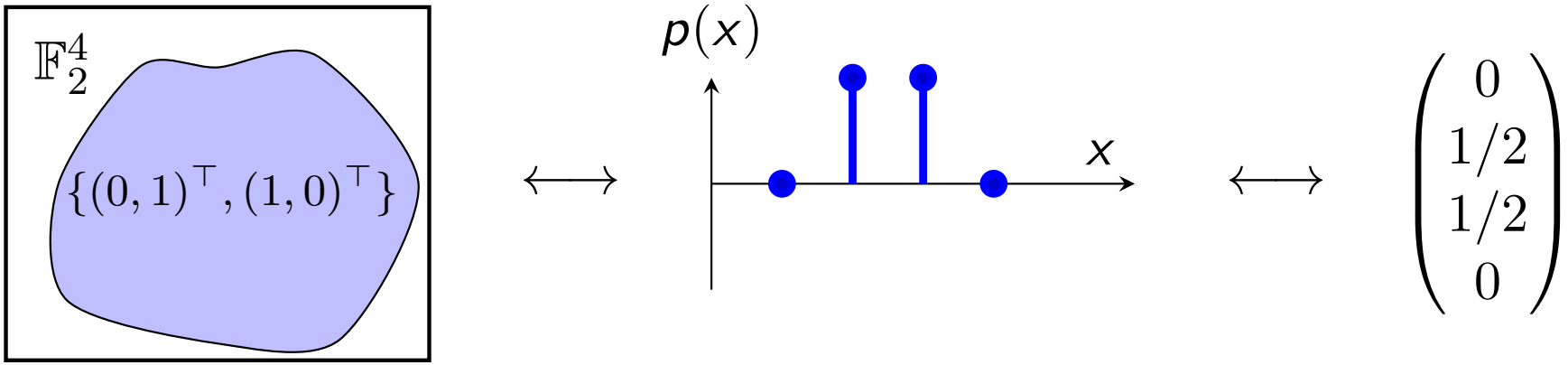
2. Invariants which are not invariant under the round function

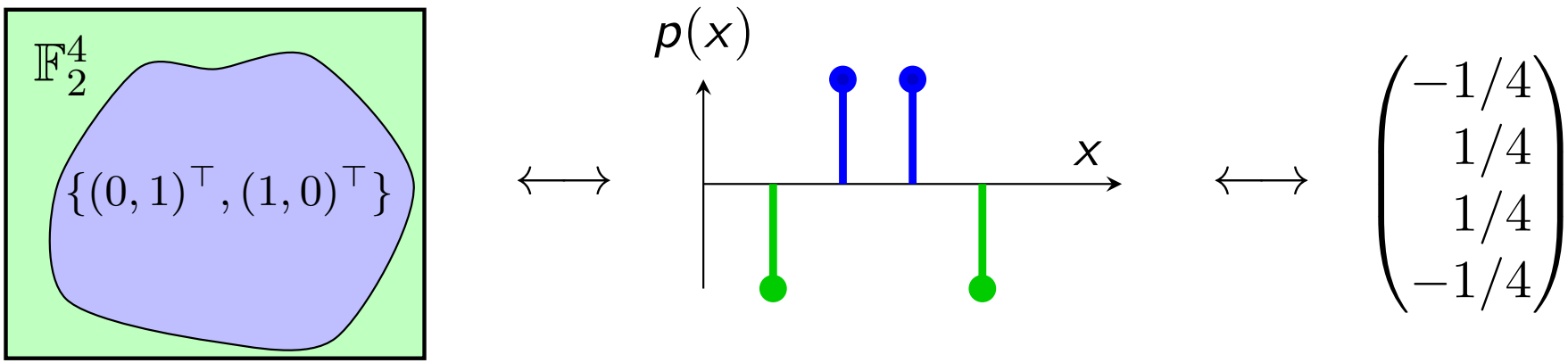
3. Attacks based on invariants that work for all round constants
   cf. [Beierle et al., 2017]

Representing the state

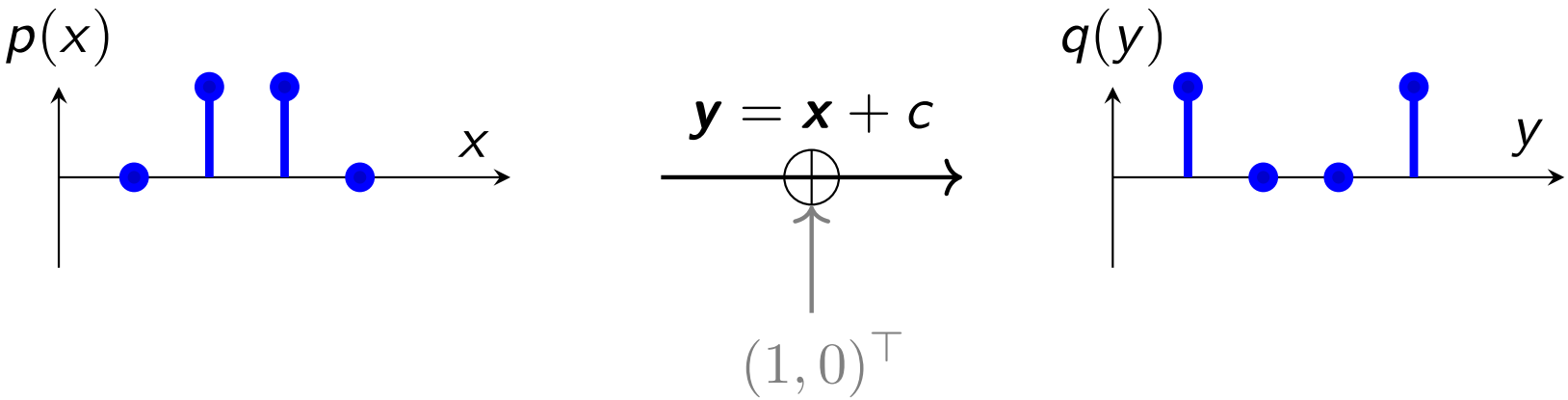


Representing the state

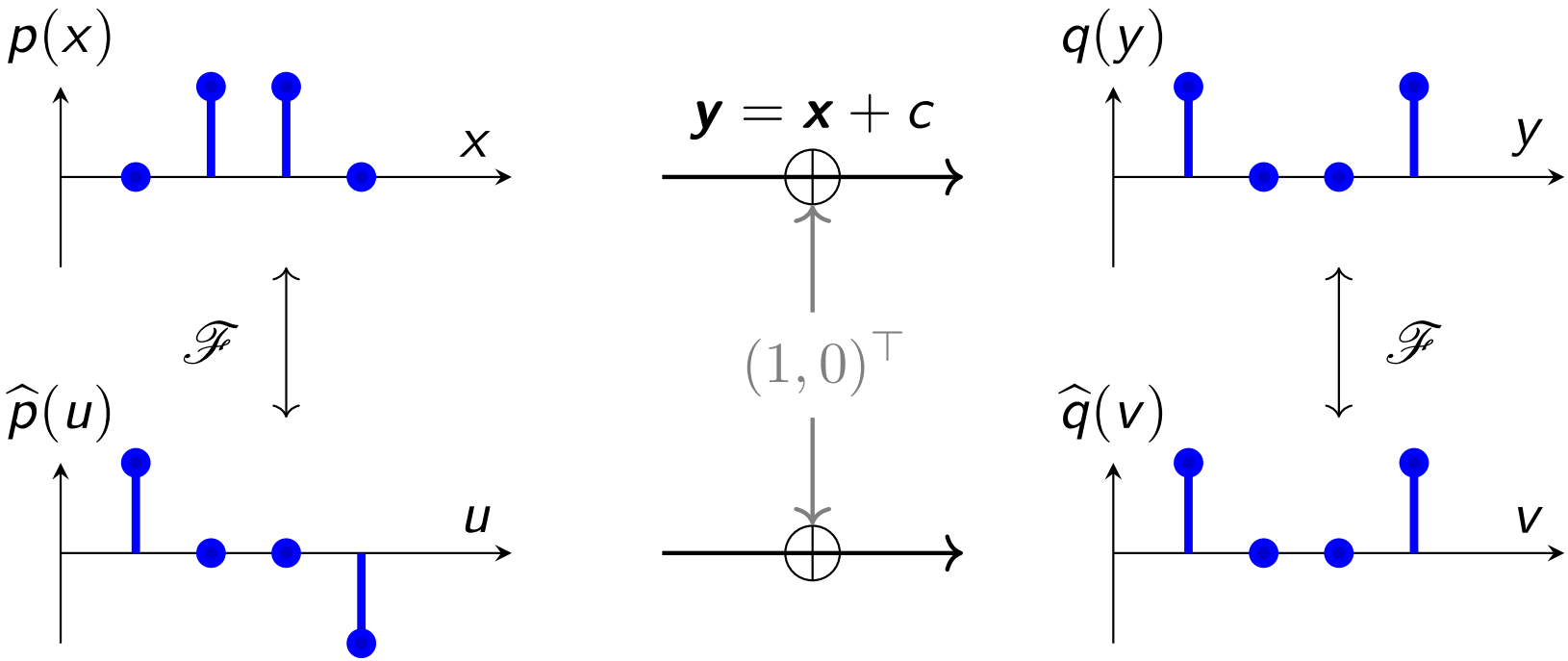




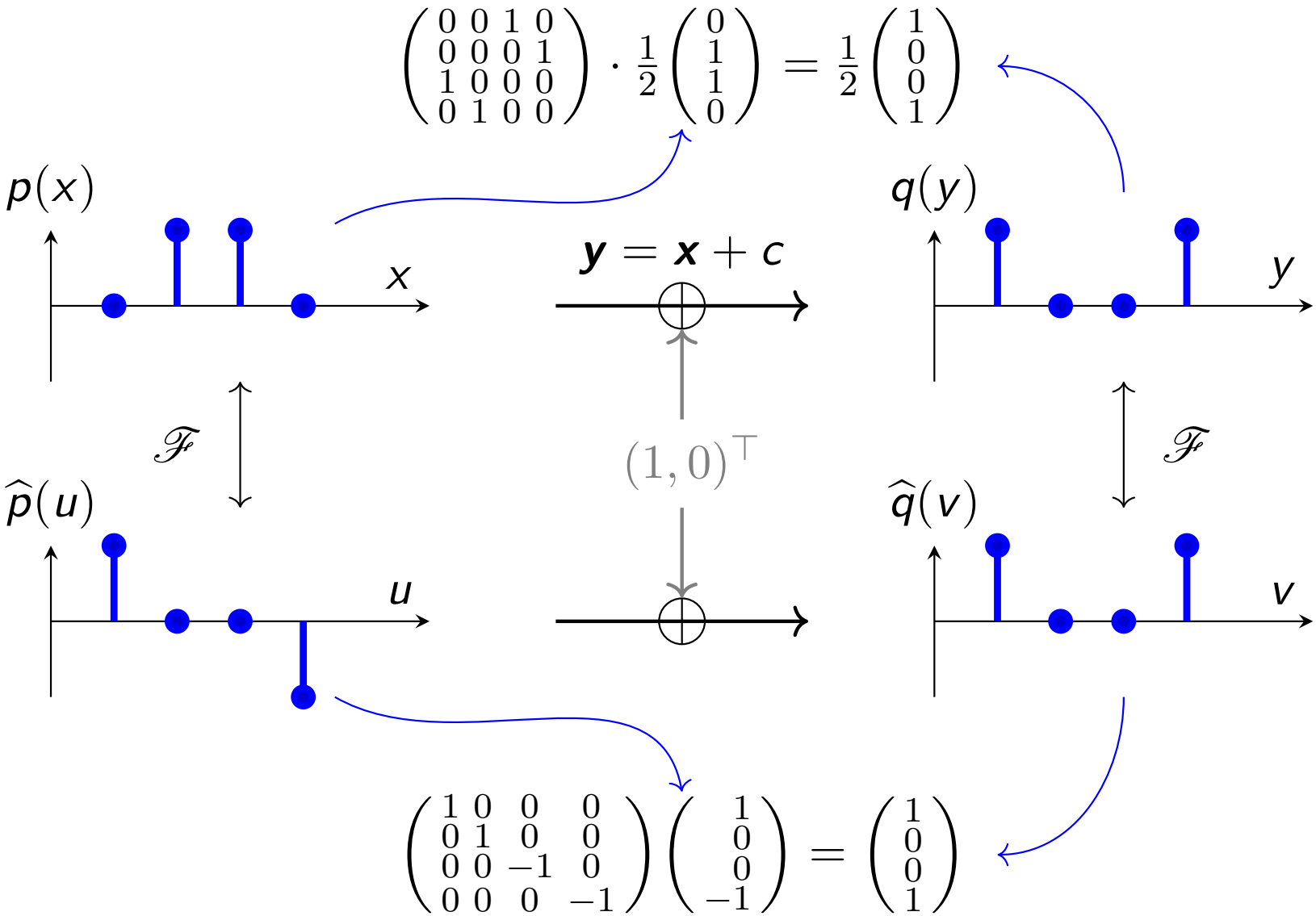
Operations on the state



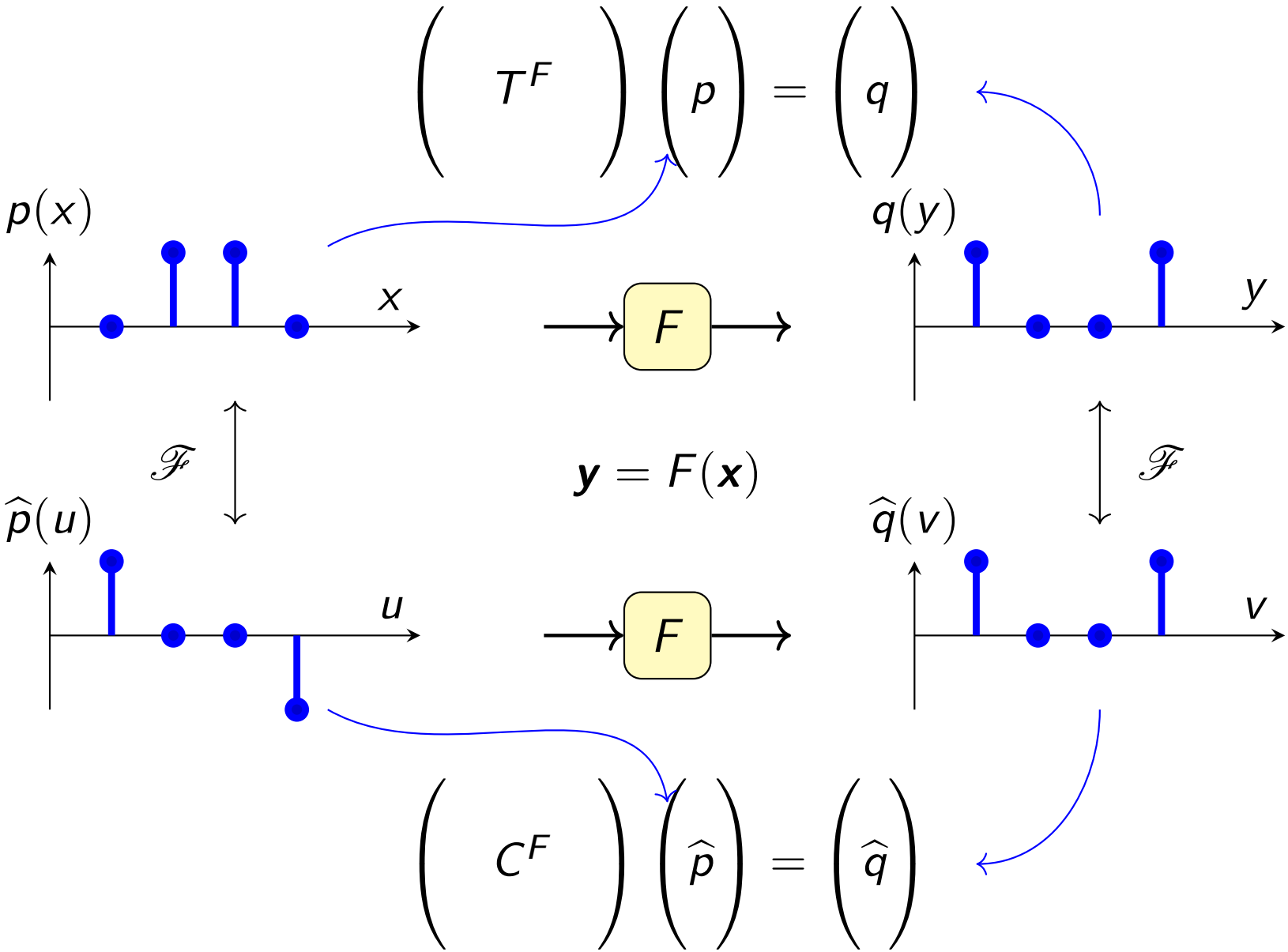
Operations on the state



Operations on the state

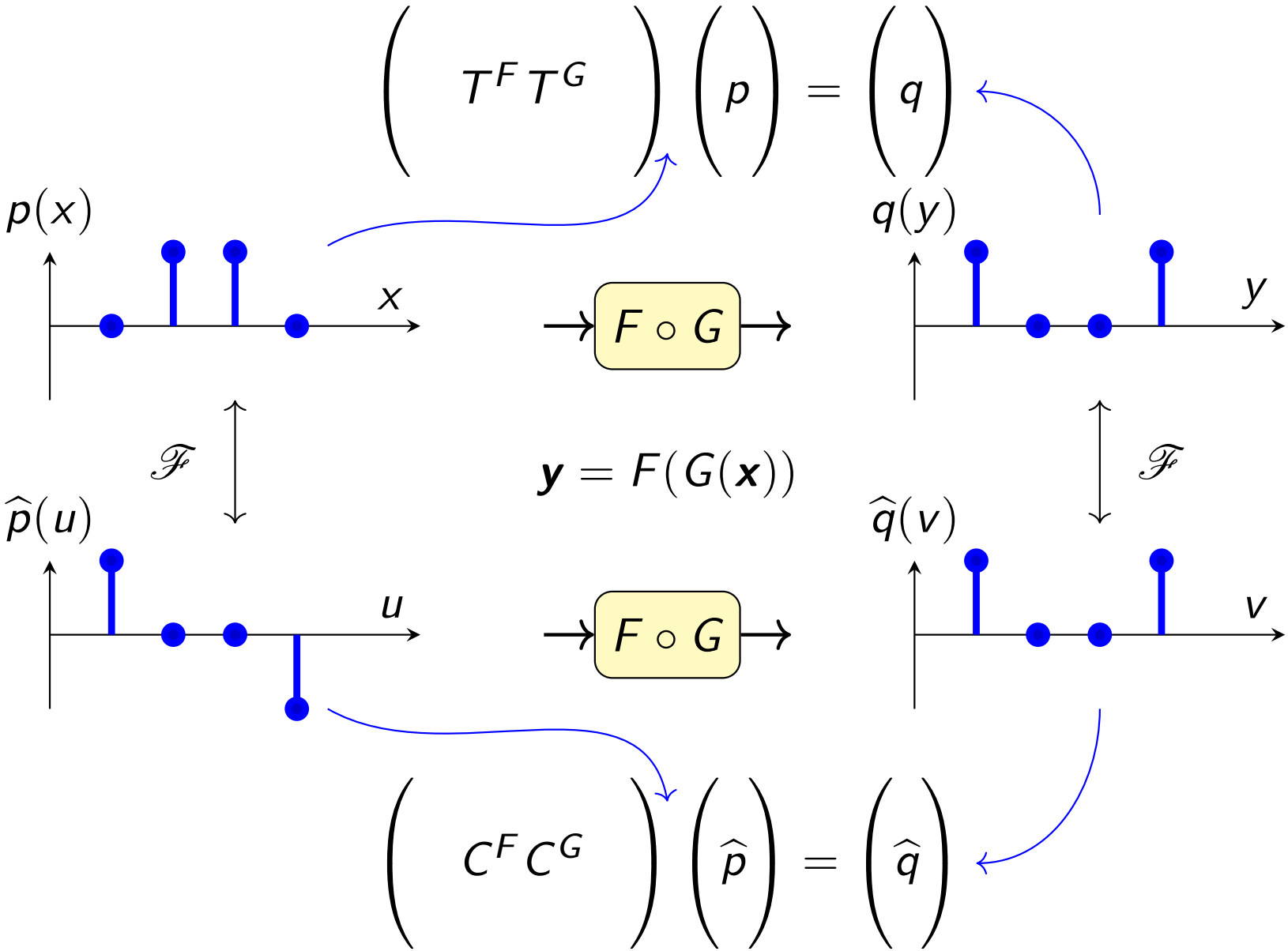


Operations on the state



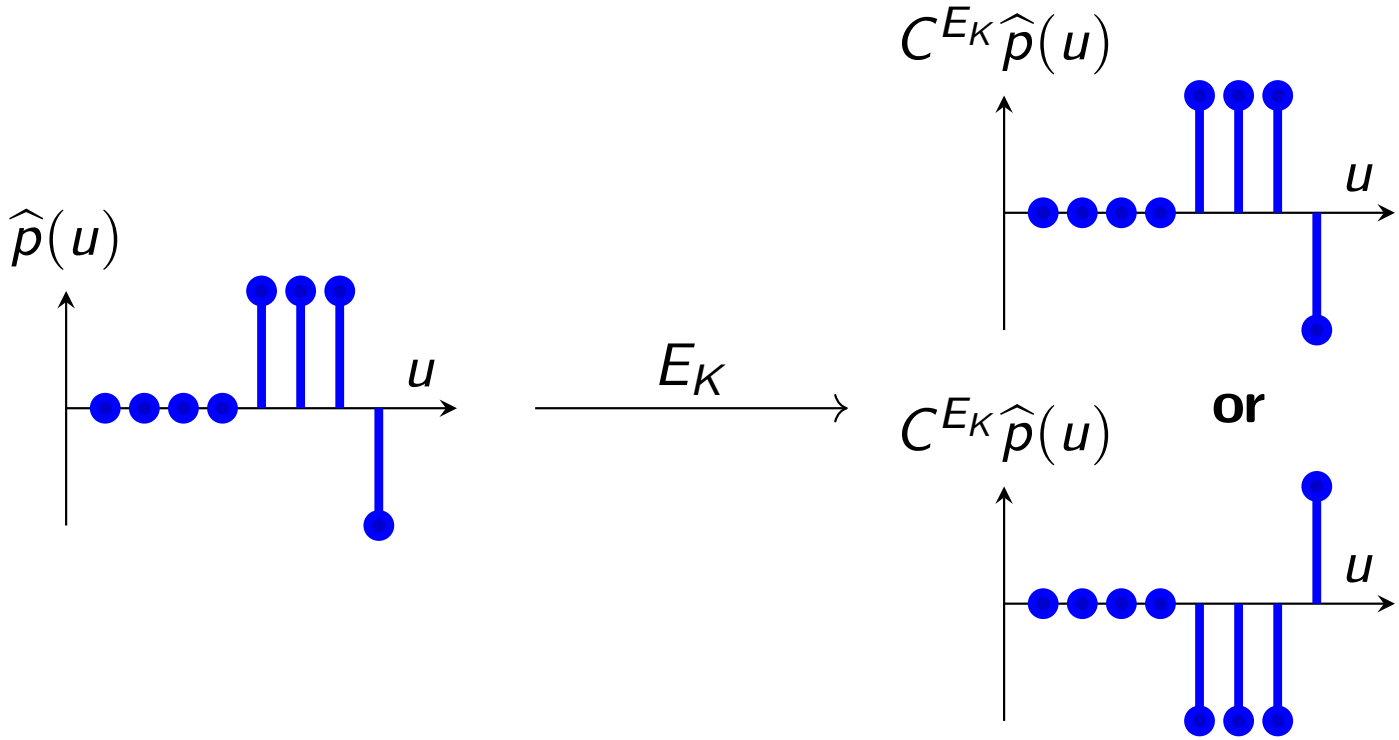
Correlation matrix

Operations on the state

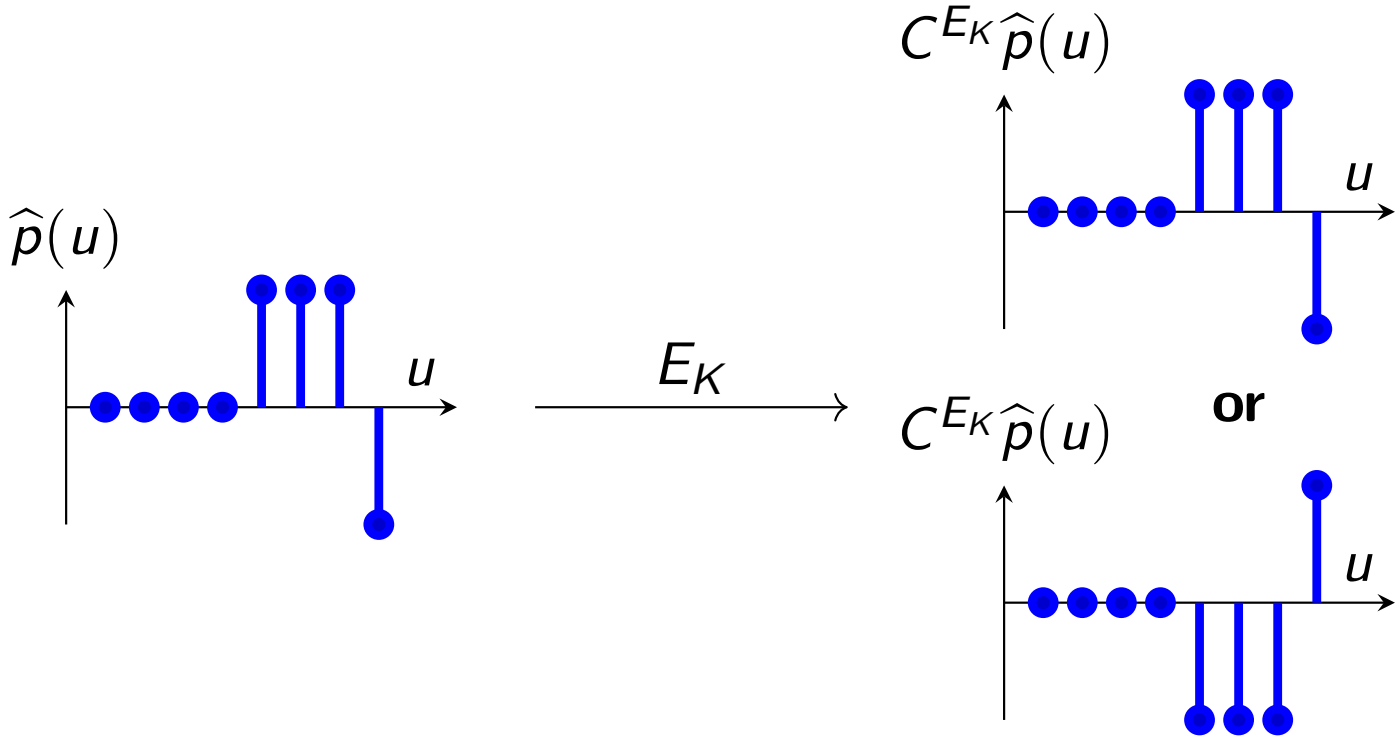


Correlation matrix

Eigenvectors of correlation matrices



Eigenvectors of correlation matrices



$$\left(\quad C^{E_K} \quad \right) \left(\widehat{p} \right) = \lambda \left(\widehat{p} \right)$$

The invariants of a block cipher E_K are the eigenvectors of C^{E_K}.

Rank one states in Midori-64

Midori-64 state

$\in \mathbb{R}^{2^{64}} \cong (\mathbb{R}^{2^4})^{\otimes 16}$

x_1	x_5	x_9	x_{13}
x_2	x_6	x_{10}	x_{14}
x_3	x_7	x_{11}	x_{15}
x_4	x_8	x_{12}	x_{16}

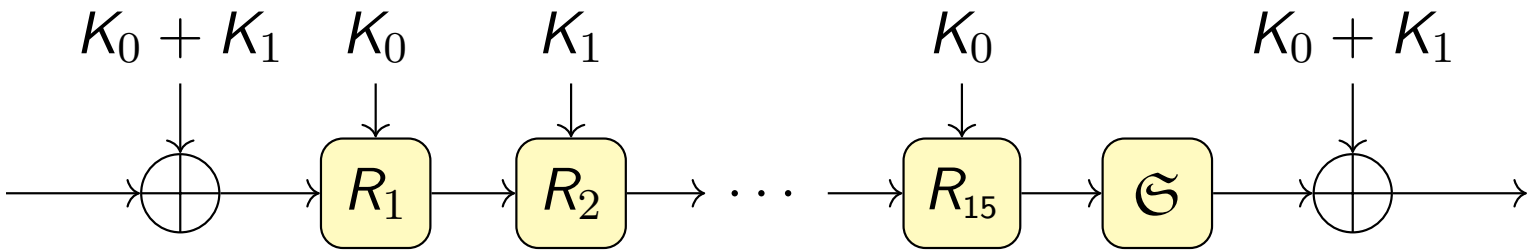
Independence:

$$p(x_1, x_2, \ldots, x_{16}) = \prod_{i=1}^{16} p_i(x_i)$$

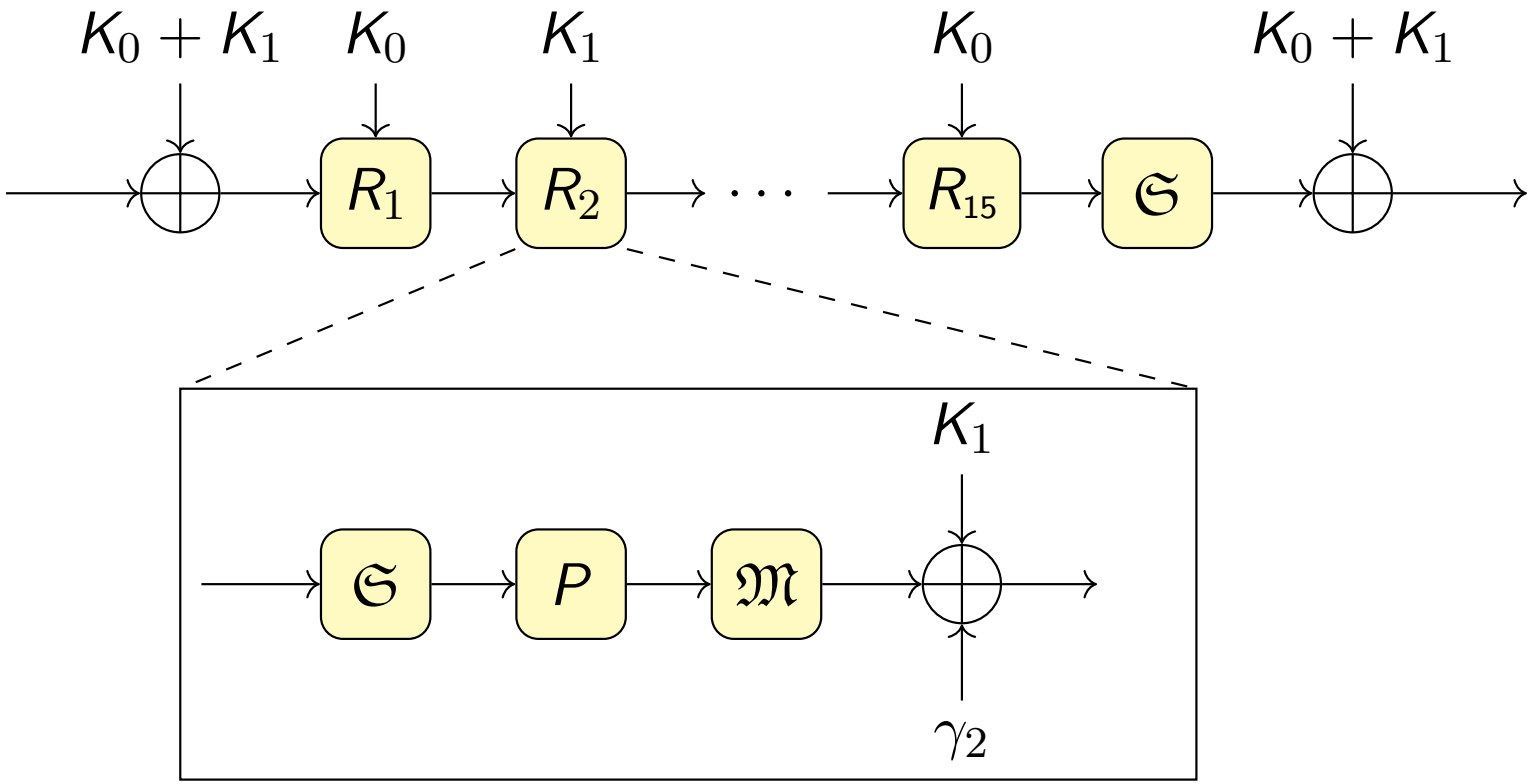
Equivalently:

$$p = \bigotimes_{i=1}^{16} p_i \quad \text{or} \quad \widehat{p} = \bigotimes_{i=1}^{16} \widehat{p}_i$$

Overview of Midori-64



Overview of Midori-64

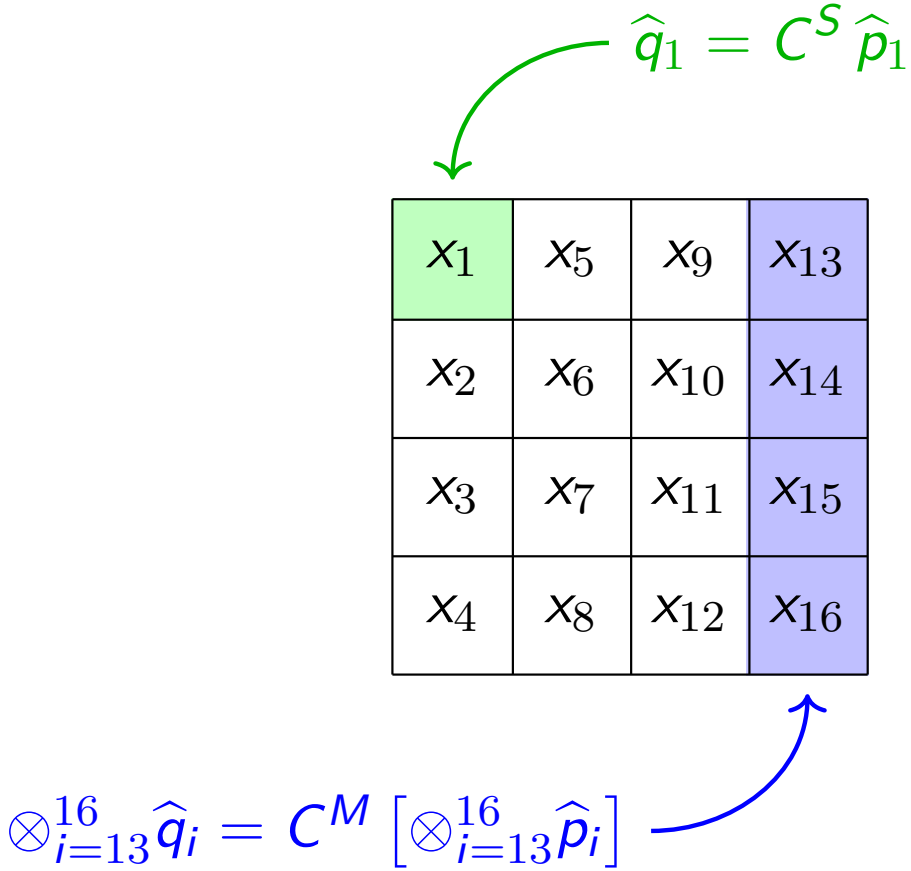


Key addition

Correlation matrix for addition of $K = (k_1, k_2, \ldots, k_n) \in \mathbb{F}_2^n$:

$$\begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & (-1)^{k_1} & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & (-1)^{\sum_{i=1}^{n} k_i} \end{pmatrix} = \bigotimes_{i=1}^{n} \begin{pmatrix} 1 & 0 \\ 0 & (-1)^{k_i} \end{pmatrix}$$

Boxed mappings



$$C^{\mathfrak{S}} = \left(C^S\right)^{\otimes 16}$$

$$C^{\mathfrak{M}} = \left(C^M\right)^{\otimes 4}$$

Three problems

1. Improve understanding (theory)
   eigenvectors of correlation matrices

2. Invariants which are not invariant under the round function

3. Attacks based on invariants that work for all round constants

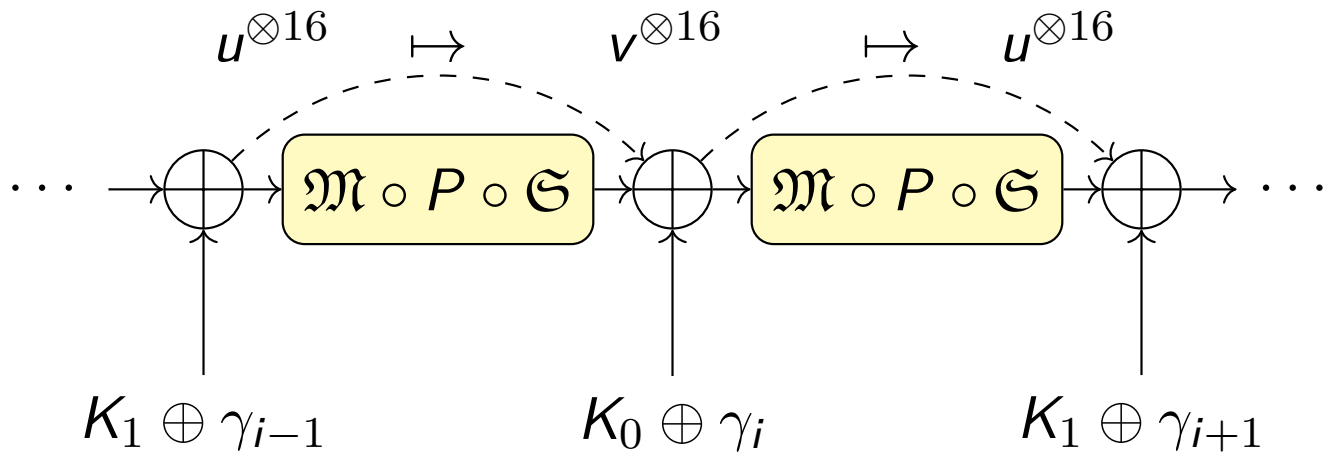
Invariants in the intersection of eigenspaces

- We want to solve
$$C^{E_K} v = \lambda v$$
- To simplify things, let's assume $v = w^{\otimes 16}$
- Require invariance under $\mathfrak{S}$, $\mathfrak{M}$ and key addition:

$$(C^S)^{\otimes 16} w^{\otimes 16} = \lambda_1 w^{\otimes 16}$$
$$(C^M)^{\otimes 4} w^{\otimes 16} = \lambda_2 w^{\otimes 16}$$
$$C^{K_i+\gamma_i} w^{\otimes 16} = \lambda_3 w^{\otimes 16}$$

$\rightarrow$ Invariants from [Guo et al., 2016, Todo et al., 2016].

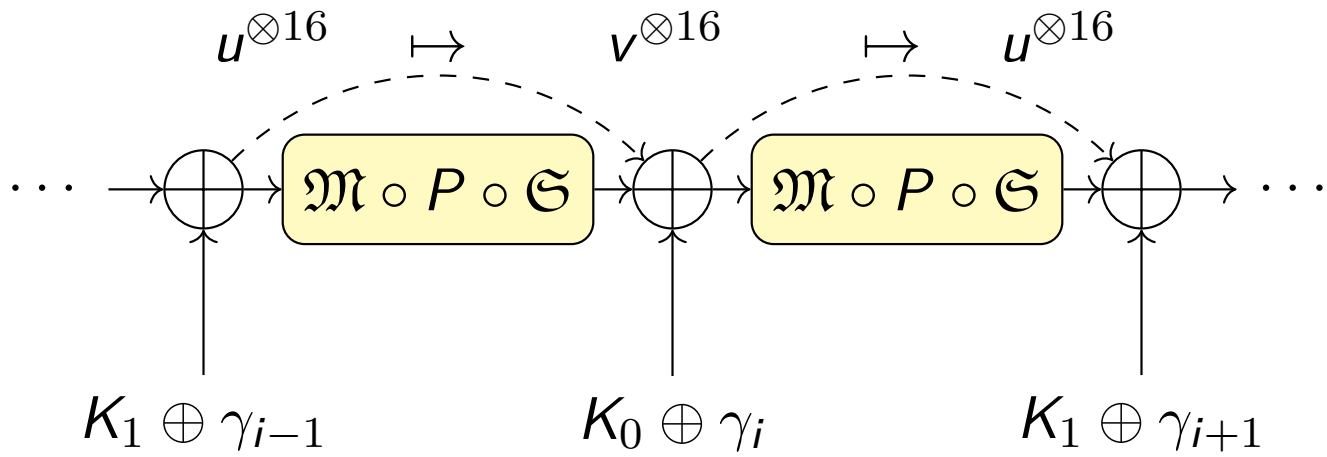
Somewhat more general invariants



$$C^S u = v$$

$$C^M u^{\otimes 4} = u^{\otimes 4},\ C^M v^{\otimes 4} = v^{\otimes 4}$$

Somewhat more general invariants



$$C^S u = v$$

$$C^M u^{\otimes 4} = u^{\otimes 4},\ C^M v^{\otimes 4} = v^{\otimes 4}$$

Most important solution: (Perfect linear approximation)

$$u = (0,0,0,0,0,1,0,0,0,0,0,0,0,0,0,0)^\top$$
$$v = (0,0,0,0,0,0,0,0,0,0,-1,-1,0,0,1,-1)^\top/2$$

Midori-64 round constants

Midori-64
0001 0101 1011 0011
0111 1000 1100 0000
1010 0100 0011 0101
0110 0010 0001 0011
0001 0000 0100 1111
1101 0001 0111 0000
0000 0010 0110 0110
0000 1011 1100 1100
1001 0100 1000 0001
0100 0000 1011 1000
...
$\rightarrow 2^{64}$ weak keys

Midori-64 round constants

Midori-64	"Almost" Midori-64
0001 0101 1011 0011	0008 0808 8088 0088
0111 1000 1100 0000	0888 8000 8800 0000
1010 0100 0011 0101	8080 0800 0088 0808
0110 0010 0001 0011	0880 0080 0008 0088
0001 0000 0100 1111	0008 0000 0800 8888
1101 0001 0111 0000	8808 0008 0888 0000
0000 0010 0110 0110	0000 0080 0880 0880
0000 1011 1100 1100	0000 8088 8800 8800
1001 0100 1000 0001	8008 0800 8000 0008
0100 0000 1011 1000	0800 0000 8088 8000
...	...
$\rightarrow 2^{64}$ weak keys	$\rightarrow 2^{96.02}$ weak keys

Midori-64 round constants

Midori-64	"Almost" Midori-64
0001 0101 1011 0011	082a 2888 028a 0a80
0111 1000 1100 0000	01cc 510f 2b77 349a
1010 0100 0011 0101	0280 880a a22a 8a2a
0110 0010 0001 0011	a374 8d6a dd67 62eb
0001 0000 0100 1111	0a80 822a 80a2 0a82
1101 0001 0111 0000	6182 5031 b4ed 0c0d
0000 0010 0110 0110	8028 a888 0aa2 a202
0000 1011 1100 1100	410d 5161 db17 8b17
1001 0100 1000 0001	0aa0 a088 0088 2a22
0100 0000 1011 1000	0a64 c6cf ee81 14a4
...	...
$\rightarrow 2^{64}$ weak keys	$\rightarrow 2^{96}$ weak keys

Three problems

1. Improve understanding (theory)
   eigenvectors of correlation matrices

2. Invariants which are not invariant under the round function
   real-world example: modified Midori-64

3. Attacks based on invariants that work for all round constants

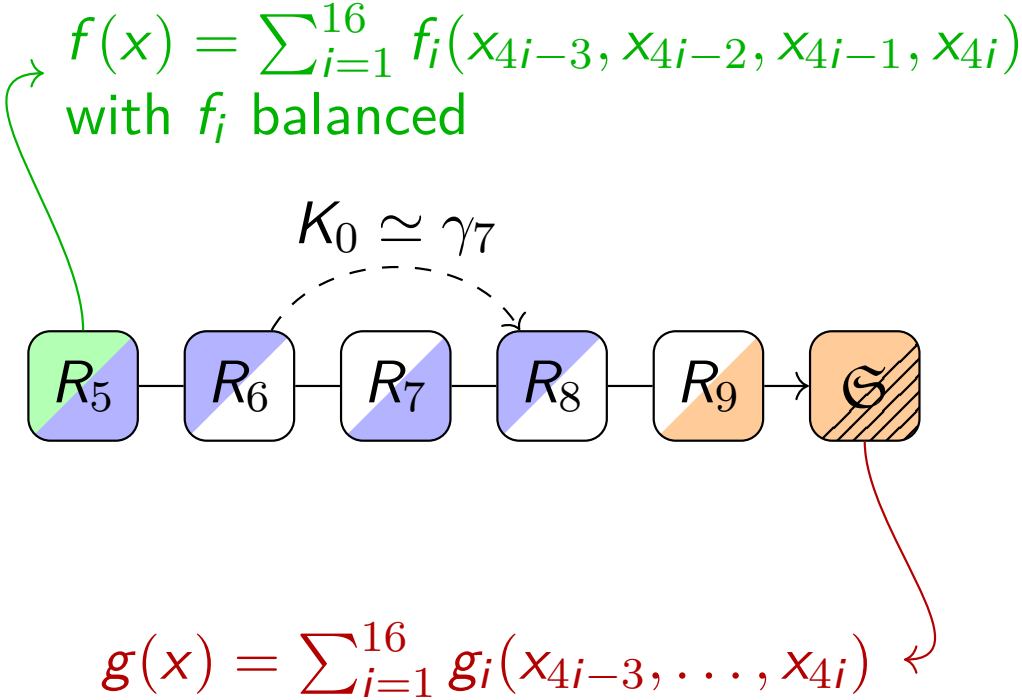
Attacks on Midori-64 and MANTIS

- Independent of the round constants
- 10 rounds of Midori-64
  - 2^{96} (out of 2^{128}) weak keys
  - $\sim 1.25 \cdot 2^{21}$ chosen plaintexts
- MANTIS-4
  - 2^{32} (out of 2^{64}) *weak tweaks*
  - ~ 640 chosen plaintexts

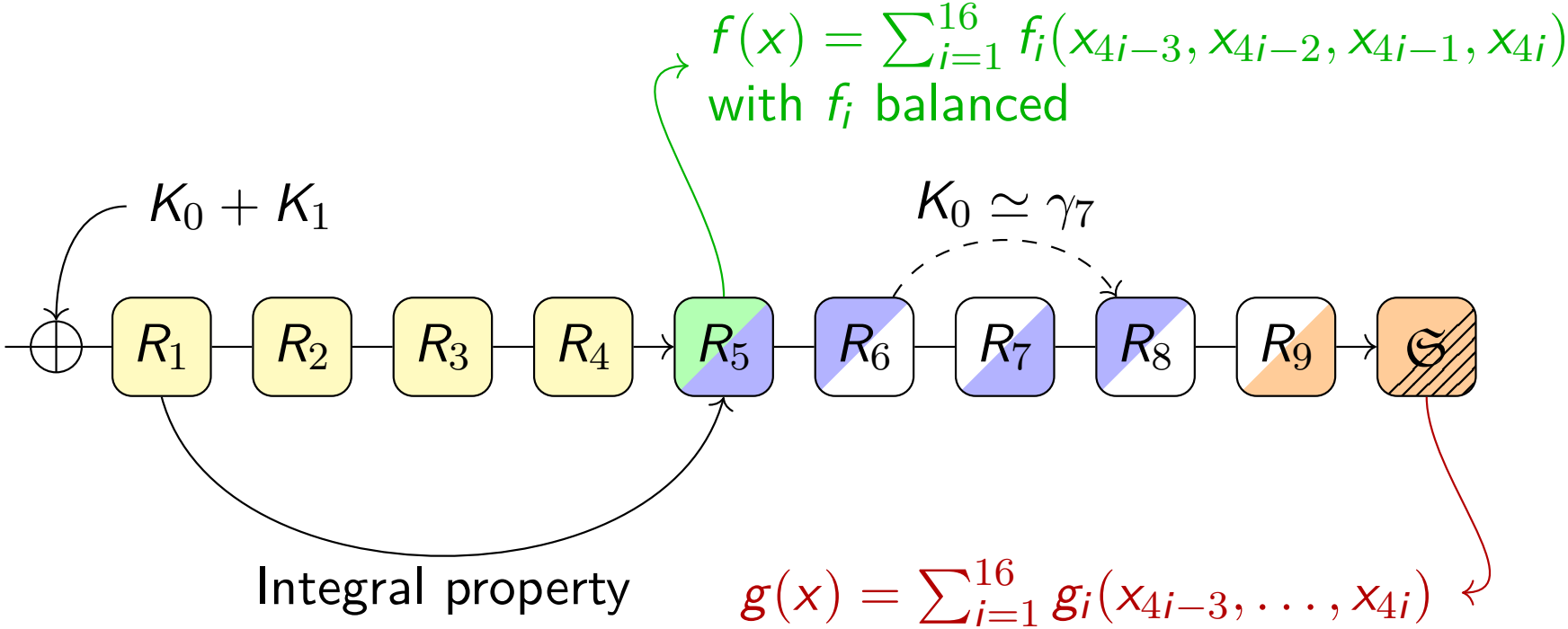
Attacks on Midori-64 and MANTIS

- Independent of the round constants
- 10 rounds of Midori-64
  - 2^{96} (out of 2^{128}) weak keys
  - $\sim 1.25 \cdot 2^{21}$ chosen plaintexts
- MANTIS-4
  - 2^{32} (out of 2^{64}) *weak tweaks*
  - ~ 640 chosen plaintexts
- Both attacks: 2^{56} block cipher calls, but
  - $40 + 32$ bits of the key almost for free
  - Guess the remaining 56 bits (no optimizations)

Attack on 10 rounds of Midori-64



Attack on 10 rounds of Midori-64



$\mathcal{I}_1$

A_1	C	C	C
C	A_2	C	C
C	C	A_3	C
C	C	C	A_4

$\longrightarrow$

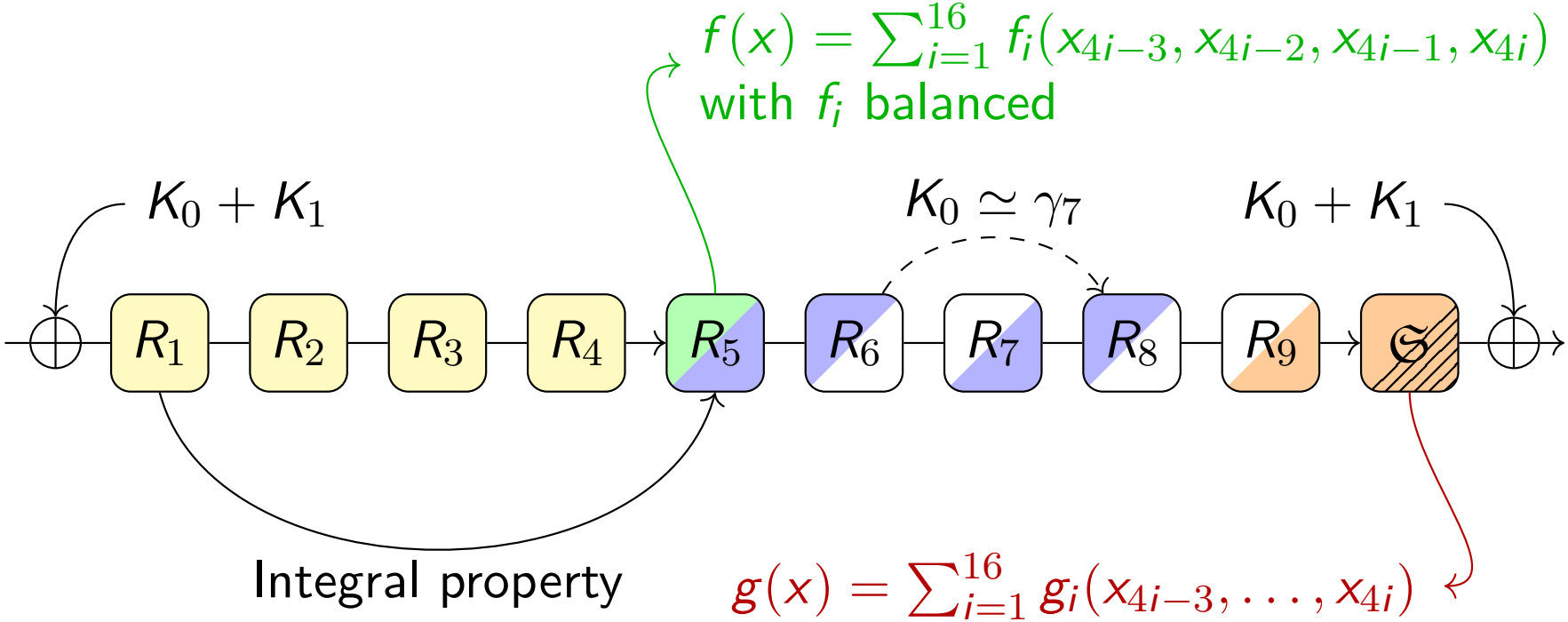
$\mathcal{I}_2$

A	A	A	A
A	A	A	A
A	A	A	A
A	A	A	A

$$\sum_{x \in \mathcal{I}_2} f(x) = 0$$

$$\Rightarrow \sum_{x \in E_K(\mathcal{I}_1)} g(x) = 0$$

Attack on 10 rounds of Midori-64



$\mathcal{I}_1$

A_1	C	C	C
C	A_2	C	C
C	C	A_3	C
C	C	C	A_4

$\longrightarrow$

$\mathcal{I}_2$

A	A	A	A
A	A	A	A
A	A	A	A
A	A	A	A

$$\sum_{x \in \mathcal{I}_2} f(x) = 0$$

$$\Rightarrow \sum_{x \in E_K(\mathcal{I}_1)} g(x + K_0 + K_1) = 0$$

Conclusions

1. Improve understanding (theory)
   eigenvectors of correlation matrices
2. Invariants which are not invariant under the round function
   real-world example: modified Midori-64
3. Attacks based on invariants that work for all round constants
   attacks on 10 rounds of Midori-64 and on MANTIS-4

More to explore:

- "statistical variant" (part of my master's thesis)
- complex eigenvalues / partitioning
- improving the attacks

`https://homes.esat.kuleuven.be/~tbeyne/`
tim.beyne@student.kuleuven.be