LINEAR AND DIFFERENTIAL CRYPTANALYSIS: ANOTHER VIEWPOINT

Fedor Malyshev, Andrey Trishin

FUNCTIONAL SCHEME

$$F : V_N \to V_M = GF(2)^M$$

FUNCTIONAL SCHEME

$$F : V_N \to V_M = GF(2)^M$$

$$\begin{array}{ccc} \Psi & & \Psi \\ a & \mapsto & b = F(a) \end{array}$$

FUNCTIONAL SCHEME

$$F : V_N \to V_M = GF(2)^M$$

$$\mathcal{F}: \quad \begin{array}{ccc} \Psi & & \Psi \\ a & \mapsto & b = F(a) \end{array}$$

FUNCTIONAL SCHEME

$$F : V_N \to V_M = GF(2)^M$$

$$\begin{array}{ccc} \Psi & & \Psi \\ a & \mapsto & b = F(a) \end{array}$$

$$\mathcal{F} :$$

$$f_i : V_{n_i} \to V_{m_i}$$

FUNCTIONAL SCHEME

$$F : V_N \to V_M = GF(2)^M$$

$$\begin{array}{ccc} \Psi & & \Psi \\ a & \mapsto & b = F(a) \end{array}$$

$\mathcal{F}$:

$$f_i : V_{n_i} \to V_{m_i}$$

$$\begin{array}{ccc} \Psi & & \Psi \\ x_i & \mapsto & y_i = f(x_i) \end{array}$$

FUNCTIONAL SCHEME

$$F : V_N \to V_M = GF(2)^M$$

$$\begin{array}{ccc} \Psi & & \Psi \\ a & \mapsto & b = F(a) \end{array}$$

$\mathcal{F}$:

$$f_i : V_{n_i} \to V_{m_i},\ i = 1, \ldots, k$$

$$\begin{array}{ccc} \Psi & & \Psi \\ x_i & \mapsto & y_i = f(x_i) \end{array}$$

FUNCTIONAL SCHEME

$$F : V_N \to V_M = GF(2)^M$$

$$\begin{array}{ccc} \Psi & & \Psi \\ a & \mapsto & b = F(a) \end{array}$$

$\mathcal{F}$:

$$f_i : V_{n_i} \to V_{m_i},\ i = 1, \ldots, k$$

$$\begin{array}{ccc} \Psi & & \Psi \\ x_i & \mapsto & y_i = f(x_i) \end{array}$$

$$(x_1, \ldots, x_k, b) = (a, y_1, \ldots, y_k)C$$

PROBABILISTIC LINEAR RELATIONS

$$x_i l'_i \simeq y_i l''_i$$

PROBABILISTIC LINEAR RELATIONS

$$x_i l_i' \simeq y_i l_i'' \,,\;\; l_i' \in V_{n_i}^{*},\;\; l_i'' \in V_{m_i}^{*}$$

PROBABILISTIC LINEAR RELATIONS

$$x_i l_i' \overset{\delta_i}{\simeq} y_i l_i'' , \;\; l_i' \in V_{n_i}^* , \;\; l_i'' \in V_{m_i}^*$$

PROBABILISTIC LINEAR RELATIONS

$$0 \simeq x_i l_i' + y_i l_i'' , \;\; l_i' \in V_{n_i}^* , \;\; l_i'' \in V_{m_i}^*$$

PROBABILISTIC LINEAR RELATIONS

$$0 \simeq \sum_{i=1}^{k} (x_i l'_i + y_i l''_i)$$

PROBABILISTIC LINEAR RELATIONS

$$0 \simeq \sum_{i=1}^{k} (x_i l'_i + y_i l''_i) = aL' + bL''$$

PROBABILISTIC LINEAR RELATIONS

$$0 \simeq \sum_{i=1}^{k} (x_i l_i' + y_i l_i'') = aL' + bL'', \;\; L' \in V_N^*, L'' \in V_M^*$$

PROBABILISTIC LINEAR RELATIONS

$$0 \simeq \sum_{i=1}^{k} (x_i l_i' + y_i l_i'') = aL' + bL'', \;\; L' \in V_N^*, L'' \in V_M^*$$

$$\mathfrak{L} = \left((l_i', l_i''), i = 1, ..., k \right)$$

PROBABILISTIC LINEAR RELATIONS

$$0 \simeq \sum_{i=1}^{k} (x_i l_i' + y_i l_i'') = aL' + bL'', \;\; L' \in V_N^*, L'' \in V_M^*$$

$$\mathfrak{L} = \left((l_i', l_i''), i = 1, ..., k \right)$$

$$\tilde{\delta} = \tilde{\delta}_{\mathfrak{L}} = \delta_1 \cdot ... \cdot \delta_k$$

PROBABILISTIC LINEAR RELATIONS

$$0 \simeq \sum_{i=1}^{k} (x_i l_i' + y_i l_i'') = aL' + bL'', \;\; L' \in V_N^*, L'' \in V_M^*$$

$$\mathfrak{L} = \left((l_i', l_i''), i = 1, ..., k \right)$$

$$\tilde{\delta} = \tilde{\delta}_{\mathfrak{L}} = \delta_1 \cdot ... \cdot \delta_k$$

$$\left| \tilde{\delta}_{\mathfrak{L}} \right| \xrightarrow[\mathfrak{L} \neq 0]{} \max$$

PROBABILISTIC LINEAR RELATIONS

$$0 \simeq \sum_{i=1}^{k} (x_i l_i' + y_i l_i'') = aL' + bL'', \;\; L' \in V_N^*, L'' \in V_M^*$$

$$\mathfrak{L} = \left((l_i', l_i''), i = 1, ..., k \right)$$

$$\delta_{L',L''} \neq \tilde{\delta} = \tilde{\delta}_{\mathfrak{L}} = \delta_1 \cdot ... \cdot \delta_k$$

$$\left| \tilde{\delta}_{\mathfrak{L}} \right| \xrightarrow[\mathfrak{L} \neq 0]{} \max$$

PROBABILISTIC LINEAR RELATIONS

$$0 \simeq \sum_{i=1}^{k} (x_i l_i' + y_i l_i'') = aL' + bL'', \;\; L' \in V_N^*, L'' \in V_M^*$$

$$\mathfrak{L} = \left((l_i', l_i''), i = 1, ..., k \right) \in \mathfrak{M}(L', L'')$$

$$\delta_{L',L''} \neq \tilde{\delta} = \tilde{\delta}_{\mathfrak{L}} = \delta_1 \cdot ... \cdot \delta_k$$

$$\left| \tilde{\delta}_{\mathfrak{L}} \right| \xrightarrow[\mathfrak{L} \neq 0]{} \max$$

PROBABILISTIC DIFFERENTIAL RELATIONS

Malyshev F. M. The duality of differential and linear methods in cryptography // Mat. Vopr. Krypt., 2014, v. 5, № 3, pp. 35-47.

PROBABILISTIC DIFFERENTIAL RELATIONS

Malyshev F. M. The duality of differential and linear methods in cryptography // Mat. Vopr. Krypt., 2014, v. 5, № 3, pp. 35-47.

$$x_i^{(1)} + x_i^{(2)} = d_i' \overset{p_i}{\rightsquigarrow} y_i^{(1)} + y_i^{(2)} = d_i''$$

PROBABILISTIC DIFFERENTIAL RELATIONS

Malyshev F. M. The duality of differential and linear methods in cryptography // Mat. Vopr. Krypt., 2014, v. 5, № 3, pp. 35-47.

$$x_i^{(1)} + x_i^{(2)} = d_i' \overset{p_i}{\rightsquigarrow} y_i^{(1)} + y_i^{(2)} = d_i''$$

$$a^{(1)} + a^{(2)} = D' \overset{p_{D',D''}}{\rightsquigarrow} b^{(1)} + b^{(2)} = D''$$

PROBABILISTIC DIFFERENTIAL RELATIONS

Malyshev F. M. The duality of differential and linear methods in cryptography // Mat. Vopr. Krypt., 2014, v. 5, № 3, pp. 35-47.

$$x_i^{(1)} + x_i^{(2)} = d_i' \overset{p_i}{\rightsquigarrow} y_i^{(1)} + y_i^{(2)} = d_i''$$

$$a^{(1)} + a^{(2)} = D' \overset{p_{D',D''}}{\rightsquigarrow} b^{(1)} + b^{(2)} = D''$$

$$\mathfrak{D} = \left((d_i', d_i''), i = 1, \ldots, k \right)$$

Malyshev F. M. The duality of differential and linear methods in cryptography // Mat. Vopr. Krypt., 2014, v. 5, № 3, pp. 35-47.

$$x_i^{(1)} + x_i^{(2)} = d_i' \overset{p_i}{\rightsquigarrow} y_i^{(1)} + y_i^{(2)} = d_i''$$

$$a^{(1)} + a^{(2)} = D' \overset{p_{D',D''}}{\rightsquigarrow} b^{(1)} + b^{(2)} = D''$$

$$\mathfrak{D} = \left((d_i', d_i''), i = 1, \ldots, k \right)$$

$$\tilde{p} = \tilde{p}_{\mathfrak{D}} = p_1 \cdot \ldots \cdot p_k$$

Malyshev F. M. The duality of differential and linear methods in cryptography // Mat. Vopr. Krypt., 2014, v. 5, № 3, pp. 35-47.

$$x_i^{(1)} + x_i^{(2)} = d_i' \overset{p_i}{\rightsquigarrow} y_i^{(1)} + y_i^{(2)} = d_i''$$

$$a^{(1)} + a^{(2)} = D' \overset{p_{D',D''}}{\rightsquigarrow} b^{(1)} + b^{(2)} = D''$$

$$\mathfrak{D} = \left((d_i', d_i''), i = 1, \ldots, k \right)$$

$$\tilde{p} = \tilde{p}_{\mathfrak{D}} = p_1 \cdot \ldots \cdot p_k$$

$$\boxed{\tilde{p}_{\mathfrak{D}} \xrightarrow[\mathfrak{D} \neq 0]{} \max}$$

Malyshev F. M. The duality of differential and linear methods in cryptography // Mat. Vopr. Krypt., 2014, v. 5, № 3, pp. 35-47.

$$x_i^{(1)} + x_i^{(2)} = d_i' \overset{p_i}{\rightsquigarrow} y_i^{(1)} + y_i^{(2)} = d_i''$$

$$a^{(1)} + a^{(2)} = D' \overset{p_{D',D''}}{\rightsquigarrow} b^{(1)} + b^{(2)} = D''$$

$$\mathfrak{D} = \left((d_i', d_i''), i = 1, \ldots, k \right)$$

$$p_{D',D''} \neq \tilde{p} = \tilde{p}_{\mathfrak{D}} = p_1 \cdot \ldots \cdot p_k$$

$$\tilde{p}_{\mathfrak{D}} \xrightarrow[\mathfrak{D} \neq 0]{} \max$$

Malyshev F. M. The duality of differential and linear methods in cryptography // Mat. Vopr. Krypt., 2014, v. 5, № 3, pp. 35-47.

$$x_i^{(1)} + x_i^{(2)} = d_i' \overset{p_i}{\rightsquigarrow} y_i^{(1)} + y_i^{(2)} = d_i''$$

$$a^{(1)} + a^{(2)} = D' \overset{p_{D',D''}}{\rightsquigarrow} b^{(1)} + b^{(2)} = D''$$

$$\mathfrak{D} = \left((d_i', d_i''), i = 1, \ldots, k\right) \in W(D', D'')$$

$$p_{D',D''} \neq \tilde{p} = \tilde{p}_{\mathfrak{D}} = p_1 \cdot \ldots \cdot p_k$$

$$\tilde{p}_{\mathfrak{D}} \xrightarrow[\mathfrak{D} \neq 0]{} \max$$

Theorem 1. (Malyshev F. M.)

$$\delta_{L',L''} = \sum\nolimits_{\mathfrak{L} \in \mathfrak{M}(L',L'')} \tilde{\delta}_{\mathfrak{L}} .$$

Theorem 1. (Malyshev F. M.)

$$\delta_{L',L''} = \sum\nolimits_{\mathfrak{L} \in \mathfrak{M}(L',L'')} \tilde{\delta}_{\mathfrak{L}}.$$

Theorem 2. (Malyshev F. M.)

$$p_{D',D''} = \sum\nolimits_{\mathfrak{D} \in W(D',D'')} \tilde{p}_{\mathfrak{D}} +$$

$$+ \frac{1}{2^M} \sum\nolimits_{(L',L'') \in V_N^* \times V_M^*} (-1)^{D'L' + D''L''} \sum_{\substack{\mathfrak{L}_1, \mathfrak{L}_2 \in \mathfrak{M}(L',L''): \\ \mathfrak{L}_1 \neq \mathfrak{L}_2}} \tilde{\delta}_{\mathfrak{L}_1} \tilde{\delta}_{\mathfrak{L}_2}.$$

Theorems 1 and 2 are proved based on the separation of the cipher functional scheme into nonlinear part and *linear medium*.

Theorem 1 has been proved in special cases:

Daemen J., Govaerts R., Vandewalle J. Correlation matrices / Advances in Cryptology – FSE'1994. – LNCS, 1995, vol. 1008, pp. 275–285.

Daemen J. Cipher and hash function design strategies based on linear and differential cryptanalysis / Doctorial Dissertation, March 1995, K.U. Leuven.

Daemen J., Rijmen V. The design of Rijndael: AES The Advanced Encryption Standart / Springer, 2002.

Theorem 2 follows from Theorem 1 and the fact taken from

Chabaud F., Vaudenay S. Links between differential and linear cryptanalysis // Advances in Cryptology – EUROCRYPT'1994, LNCS 950, pp. 356-365, 1995;

Daemen J., Govaerts R., Vandewalle J. Correlation matrices // Advances in Cryptology – FSE'1994. – LNCS, 1995, vol. 1008, pp. 275–285

about the link between the linear and differential characteristics of Boolean mappings

Theorem 2 follows from Theorem 1 and the fact taken from

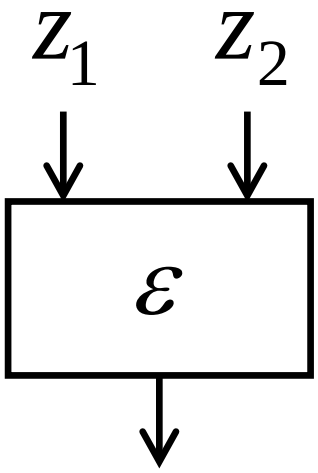
Chabaud F., Vaudenay S. Links between differential and linear cryptanalysis // Advances in Cryptology – EUROCRYPT'1994, LNCS 950, pp. 356-365, 1995;

Daemen J., Govaerts R., Vandewalle J. Correlation matrices // Advances in Cryptology – FSE'1994. – LNCS, 1995, vol. 1008, pp. 275–285

about the link between the linear and differential characteristics of Boolean mappings

Theorem 2 has been proved in a different smart way by Fedchenko V.A.

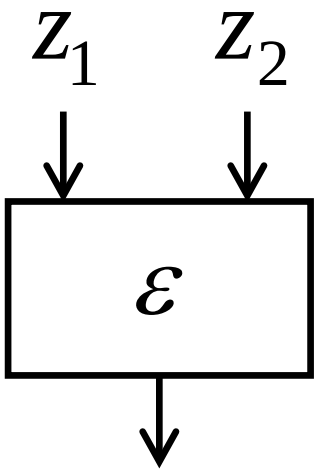
UNIVERSAL FUNCTIONAL SCHEME



$$g_\varepsilon,\ \varepsilon = 0,1$$

$$\overline{z}_1 z_2 \cdot \varepsilon + z_1 \overline{z}_2 \cdot \overline{\varepsilon}$$

UNIVERSAL FUNCTIONAL SCHEME



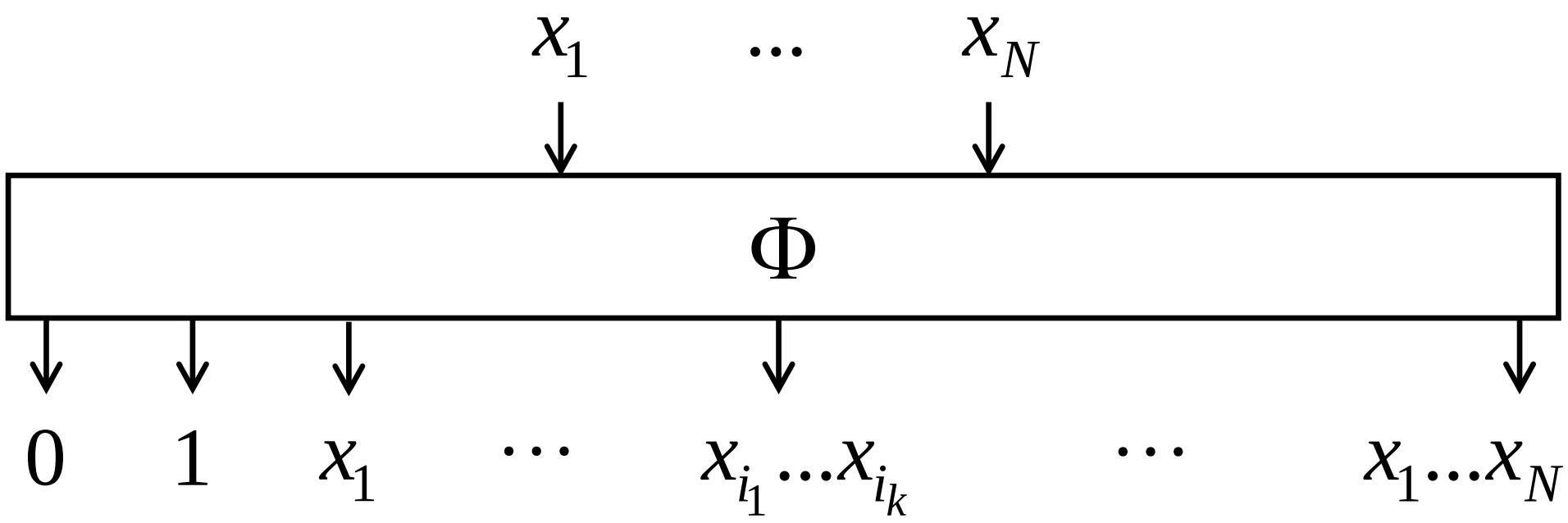
$$g_\varepsilon,\ \varepsilon = 0,1$$

$$\overline{z}_1 z_2 \cdot \varepsilon + z_1 \overline{z}_2 \cdot \overline{\varepsilon}$$

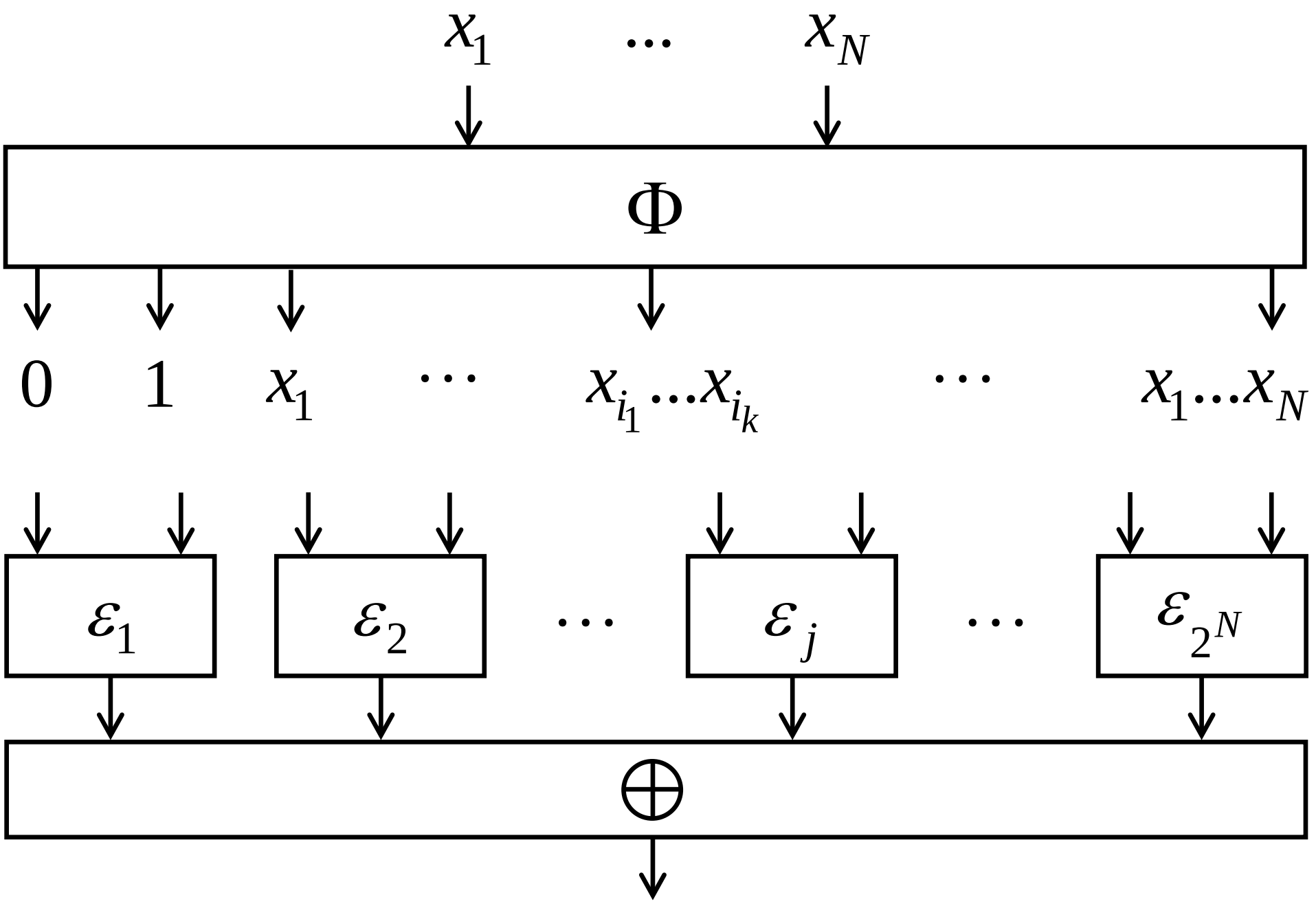
If $l_i'' \neq 0$ then $\left|\delta_{l_i', l_i''}^{g_\varepsilon}\right| = 1/2.$

If $d_i' \neq 0$ then $p_{d_i', d_i''}^{g_\varepsilon} = 1/2.$

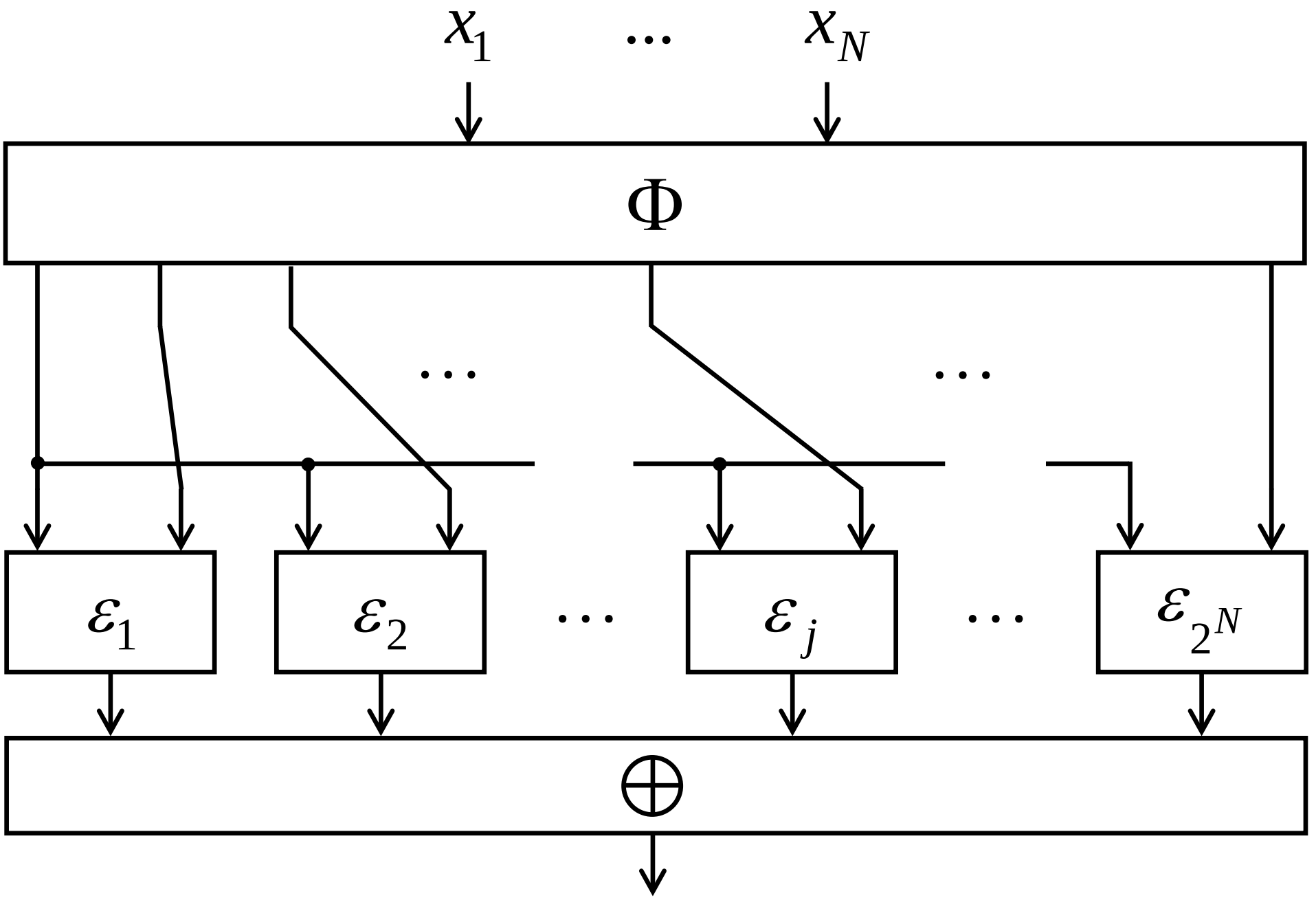
UNIVERSAL FUNCTIONAL SCHEME



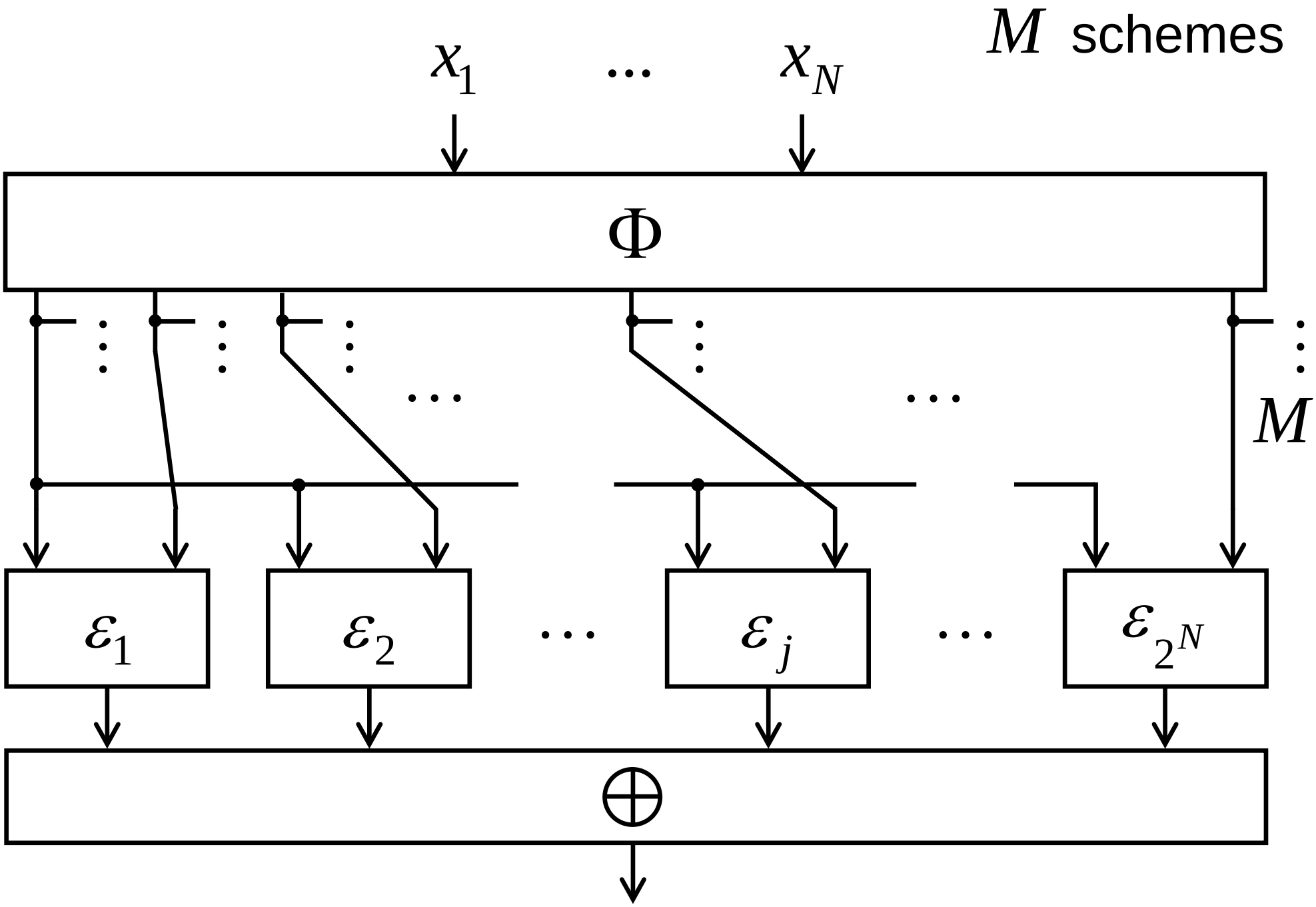
UNIVERSAL FUNCTIONAL SCHEME



UNIVERSAL FUNCTIONAL SCHEME



UNIVERSAL FUNCTIONAL SCHEME



For all $F : V_N \to V_M$ we have

the same linear medium C;

the same $\left|\delta_{l_i', l_i''}^{f_i}\right|$, $p_{d_i', d_i''}^{f_i}$

For all $F : V_N \to V_M$ we have

the same linear medium C;

the same $\left| \delta_{l'_i, l''_i}^{f_i} \right|$, $p_{d'_i, d''_i}^{f_i}$,

so we get

the same $\left| \tilde{\delta}_{\mathfrak{L}} \right|$, $\tilde{p}_{\mathfrak{D}}$.

For all $F : V_N \to V_M$ we have

the same linear medium C;

the same $\left|\delta_{l_i', l_i''}^{f_i}\right|$, $p_{d_i', d_i''}^{f_i}$,

so we get

the same $\left|\tilde{\delta}_{\mathfrak{L}}\right|$, $\tilde{p}_{\mathfrak{D}}$.

We have come to a complete absurdity

Universal functional scheme demonstrates a significant range of possible errors using the current way to estimate the characteristics of probabilistic relations.

Universal functional scheme demonstrates a significant range of possible errors using the current way to estimate the characteristics of probabilistic relations.

Let see more examples.

EXAMPLE (FEDCHENKO V. A.)

XSLP-cipher $F_k : V_{12} \to V_{12}$

$\pi : V_3 \to V_3,\ B \in GL(6,2),\ P \in S_4.$

EXAMPLE (FEDCHENKO V. A.)

XSLP-cipher $F_k : V_{12} \to V_{12}$

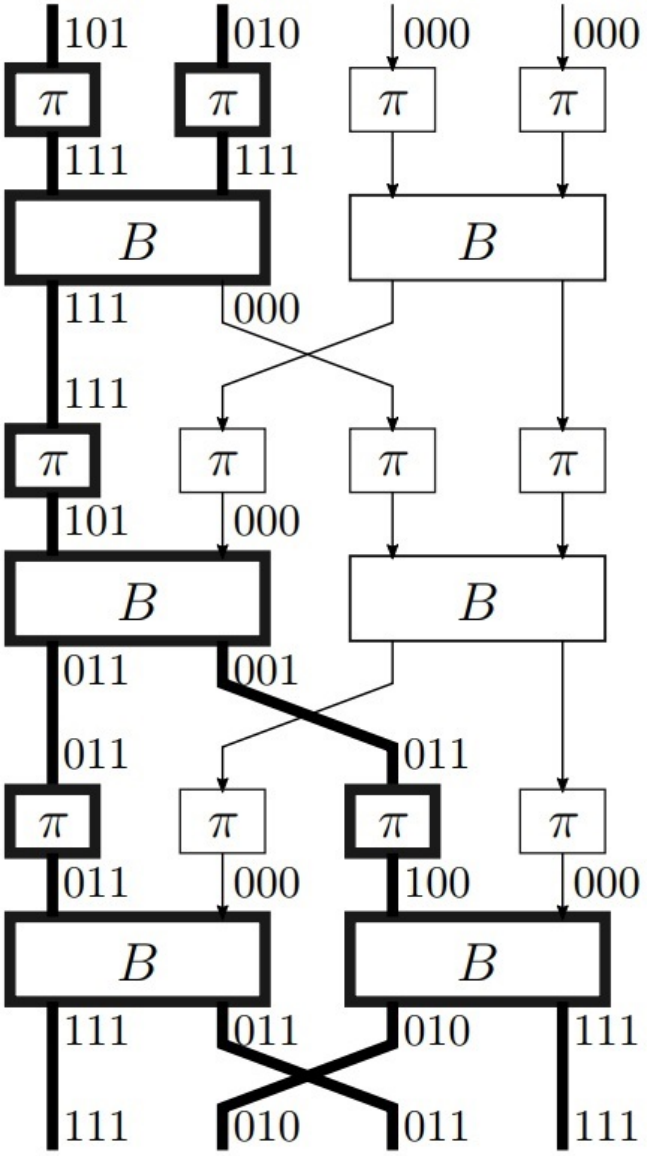
$$\pi : V_3 \to V_3,\ B \in GL(6,2),\ P \in S_4.$$

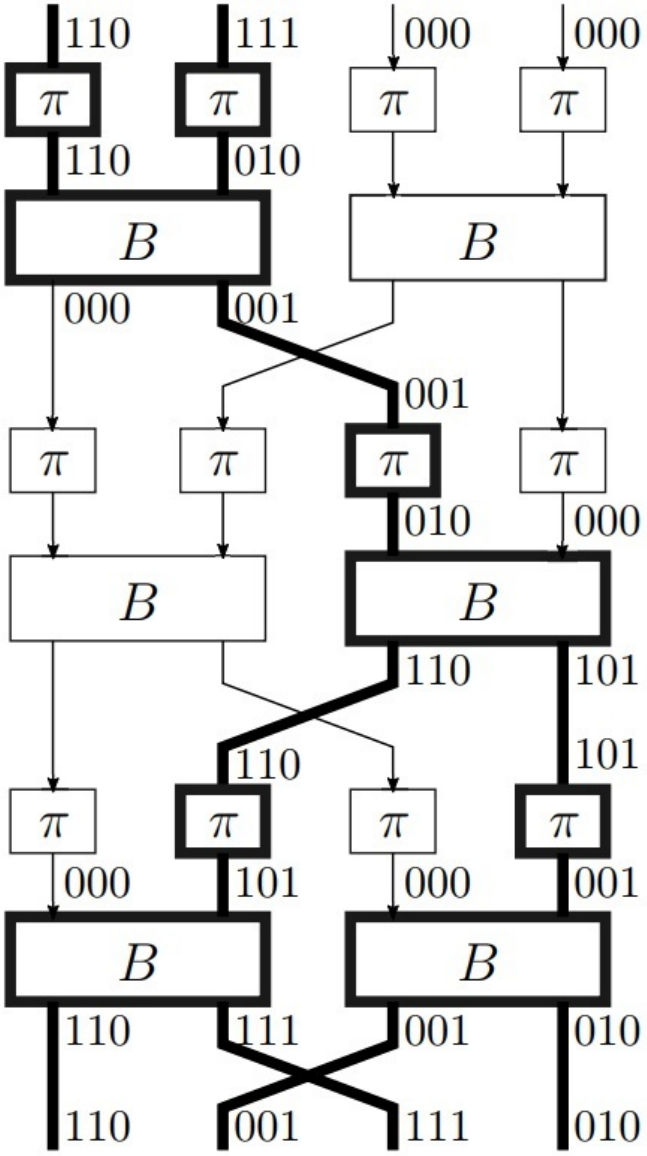
Two systems $\mathfrak{L}_1$, $\mathfrak{L}_2$ have been found such that:

$$\left|\tilde{\delta}_{\mathfrak{L}_1}\right| = \left|\tilde{\delta}_{\mathfrak{L}_2}\right| = 0,03...$$

$$\delta_{L_1', L_1''} = 0,\ \delta_{L_2', L_2''} = -0,2...$$

EXAMPLE (FEDCHENKO V. A.)





EXAMPLE (FEDCHENKO V. A.)

XSLP-cipher $F_k : V_{12} \to V_{12}$

$$\pi : V_3 \to V_3,\ B \in GL(6,2),\ P \in S_4.$$

Two systems $\mathfrak{L}_1$, $\mathfrak{L}_2$ have been found such that:

$$\left|\tilde{\delta}_{\mathfrak{L}_1}\right| = \left|\tilde{\delta}_{\mathfrak{L}_2}\right| = 0,03...$$

$$\delta_{L_1',L_1''} = 0,\ \delta_{L_2',L_2''} = -0,2...$$

Moreover, $\max_{L',L''\neq 0} \left|\delta^F_{L',L''}\right| = 0,75.$

EXAMPLE (FEDCHENKO V. A.)

XSLP-cipher $F_k : V_{12} \to V_{12}$

$$\pi : V_3 \to V_3,\ B \in GL(6,2),\ P \in S_4.$$

Two systems $\mathfrak{L}_1$, $\mathfrak{L}_2$ have been found such that:

$$\left|\tilde{\delta}_{\mathfrak{L}_1}\right| = \left|\tilde{\delta}_{\mathfrak{L}_2}\right| = 0,03...$$

$$\delta_{L_1',L_1''} = 0,\ \delta_{L_2',L_2''} = -0,2...$$

Moreover, $\max_{L',L''\neq 0} \left|\delta^F_{L',L''}\right| = 0,75.$

SO, METHODS DO NOT ALWAYS WORK

1. The methods only work SOMETIMES.

PROBLEM: In what cases the methods work?

DISADVANTAGES OF THE METHODS

1. The methods only work SOMETIMES.

   PROBLEM: In what cases the methods work?

2. We do not obtain the best $\delta_{L',L''}$ and $p_{D',D''}$.

DISADVANTAGES OF THE METHODS

1. The methods only work SOMETIMES.

   PROBLEM: In what cases the methods work?

2. We do not obtain the best $\delta_{L',L''}$ and $p_{D',D''}$.

3. General results about the exactness of approximations

$$\tilde{\delta}_{\mathfrak{L}} \leftrightarrow \delta_{L',L''} \text{ and } \tilde{p}_{\mathfrak{D}} \leftrightarrow p_{D',D''}$$

   are not known.

DISADVANTAGES OF THE METHODS

1. The methods only work SOMETIMES.

   PROBLEM: In what cases the methods work?

2. We do not obtain the best $\delta_{L',L''}$ and $p_{D',D''}$.

3. General results about the exactness of approximations

$$\tilde{\delta}_{\mathfrak{L}} \leftrightarrow \delta_{L',L''} \text{ and } \tilde{p}_{\mathfrak{D}} \leftrightarrow p_{D',D''}$$

   are not known.

IT IS IMPORTANT TO VERIFY THE RESULTS !

METHODOLOGY OF EXPERIMENTS

$$\text{Is } \tilde{\delta}_{\mathfrak{L}} \approx \delta_{L',L''}?$$

Is $\tilde{\delta}_{\Sigma} \approx \delta_{L',L''}$?

if $\tilde{\delta}_{\Sigma}$ is significant

Obtain
an empirical
estimations

δ^*

Is $\tilde{\delta}_{\Sigma} \approx \delta_{L',L''}$?

if $\tilde{\delta}_{\Sigma}$ is significant

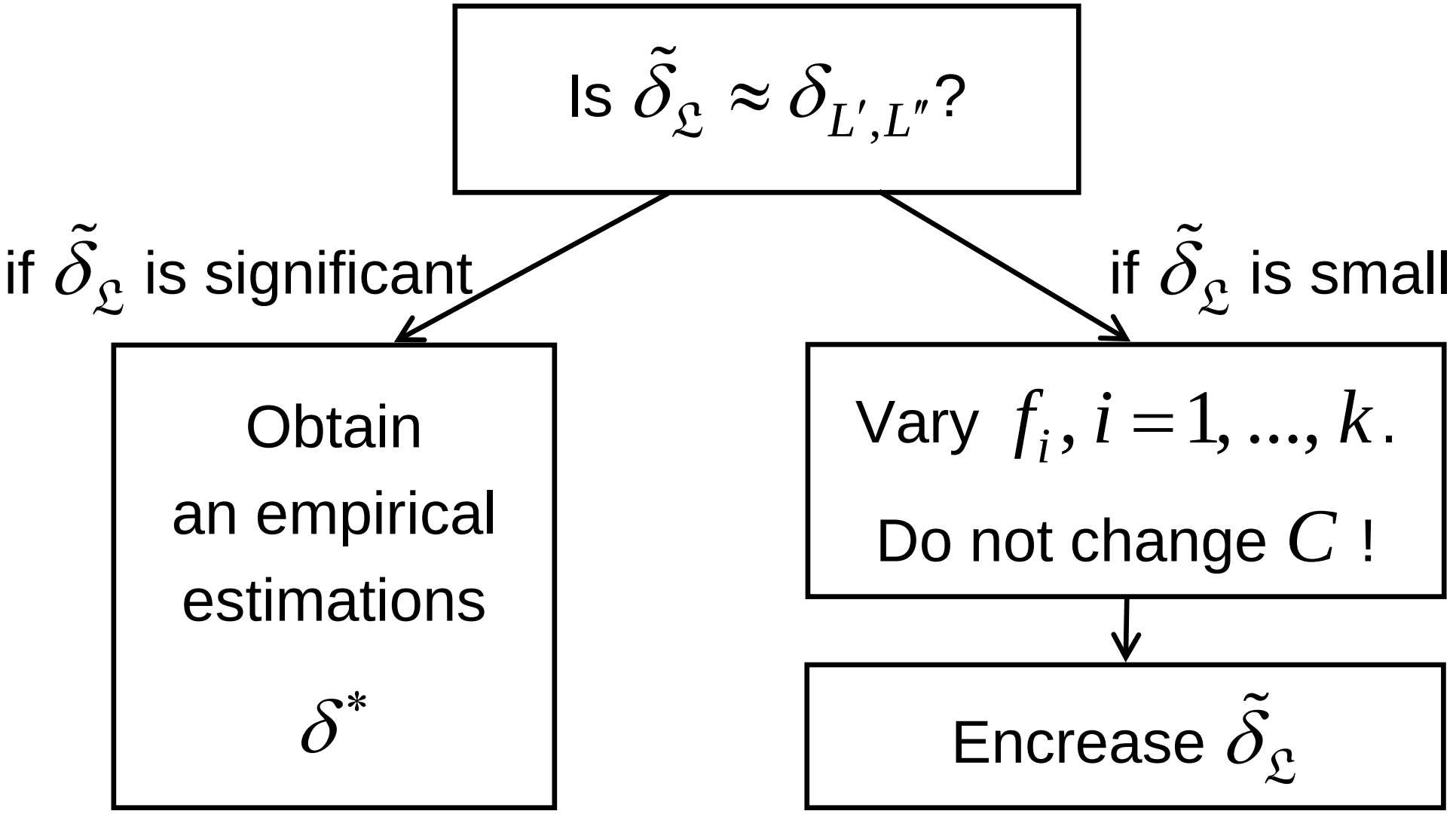
Obtain an empirical estimations δ^*

if $\tilde{\delta}_{\Sigma}$ is small

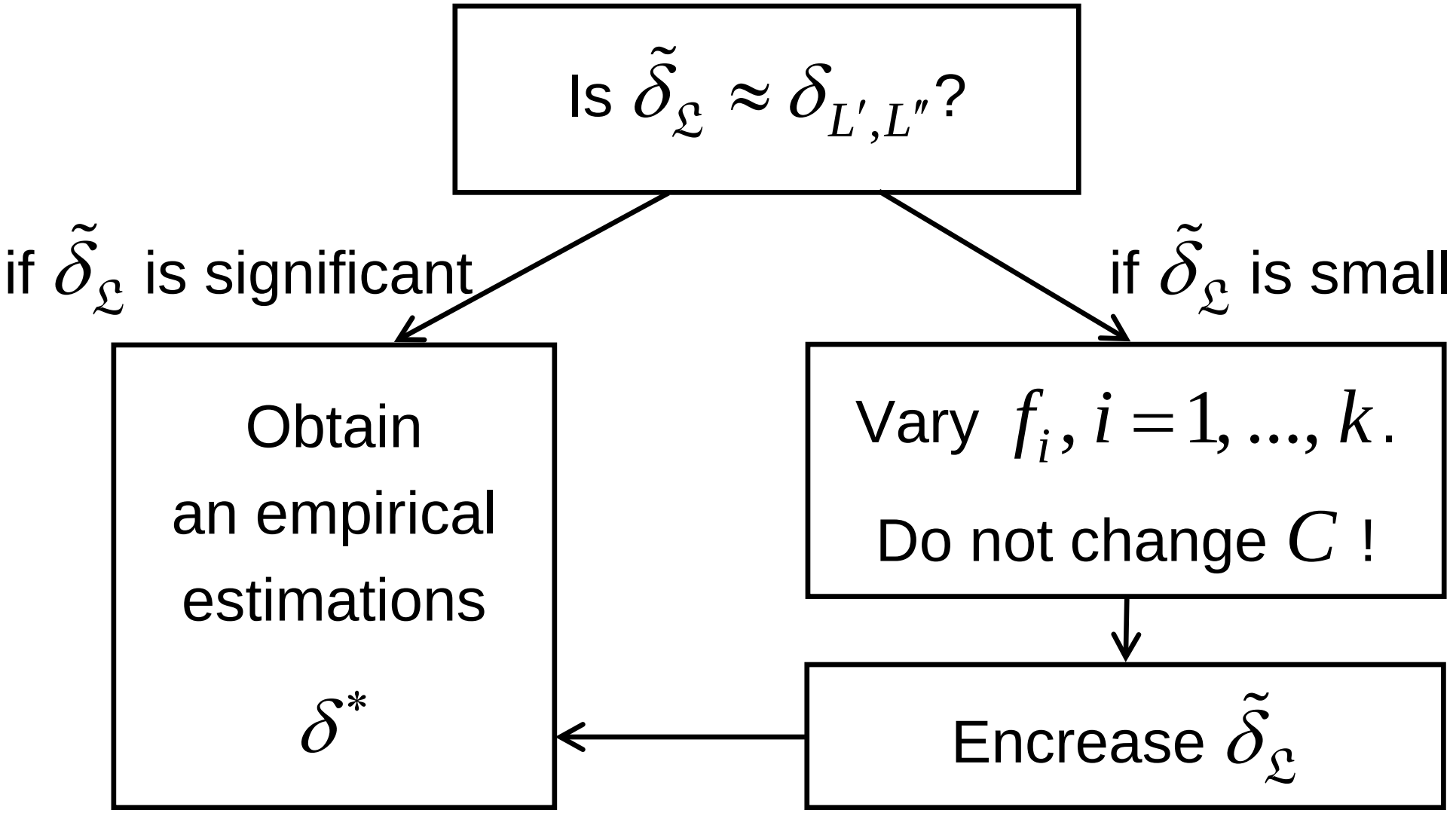
Vary $f_i, i = 1, ..., k$.

Do not change C !

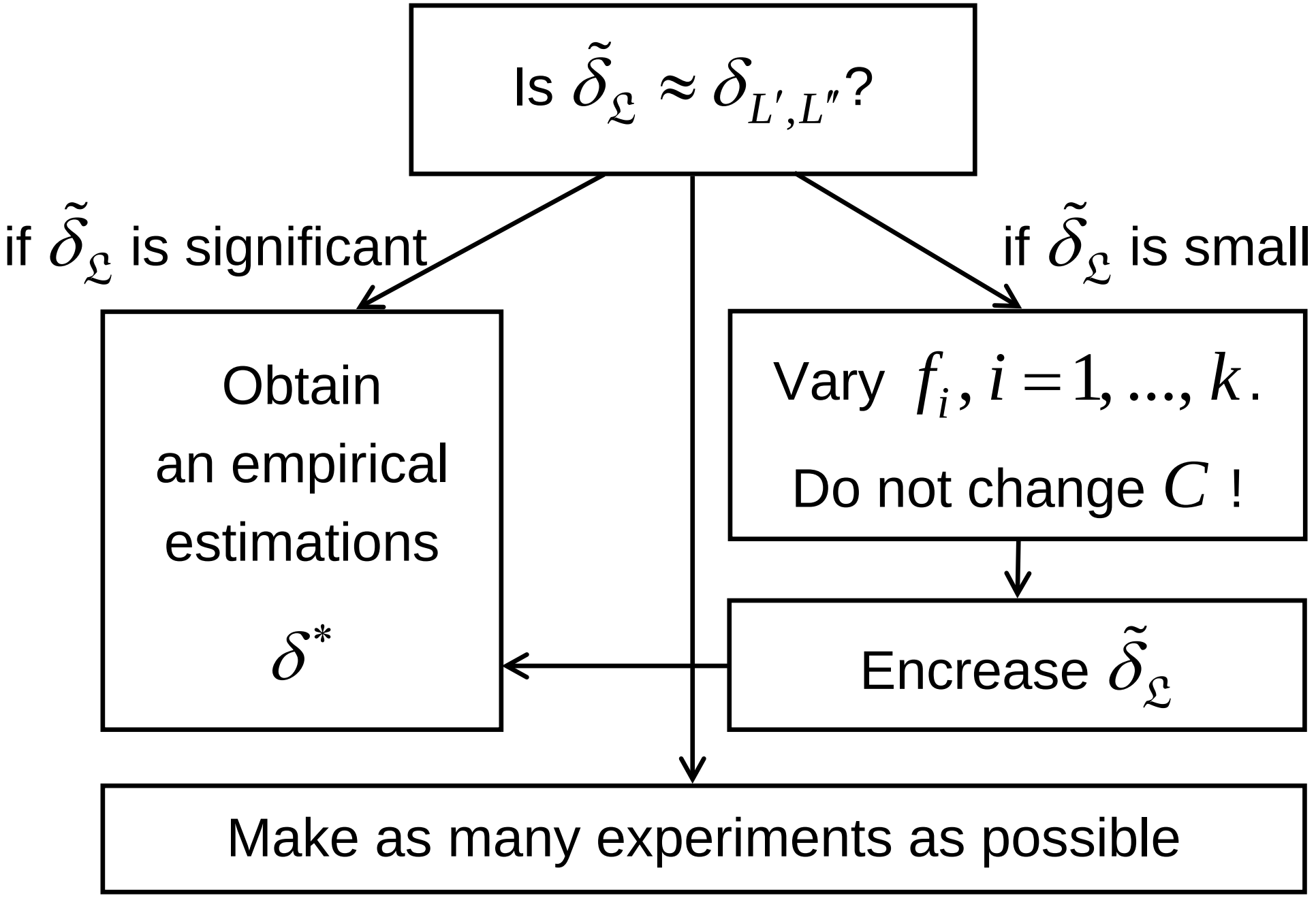
METHODOLOGY OF EXPERIMENTS



METHODOLOGY OF EXPERIMENTS



METHODOLOGY OF EXPERIMENTS



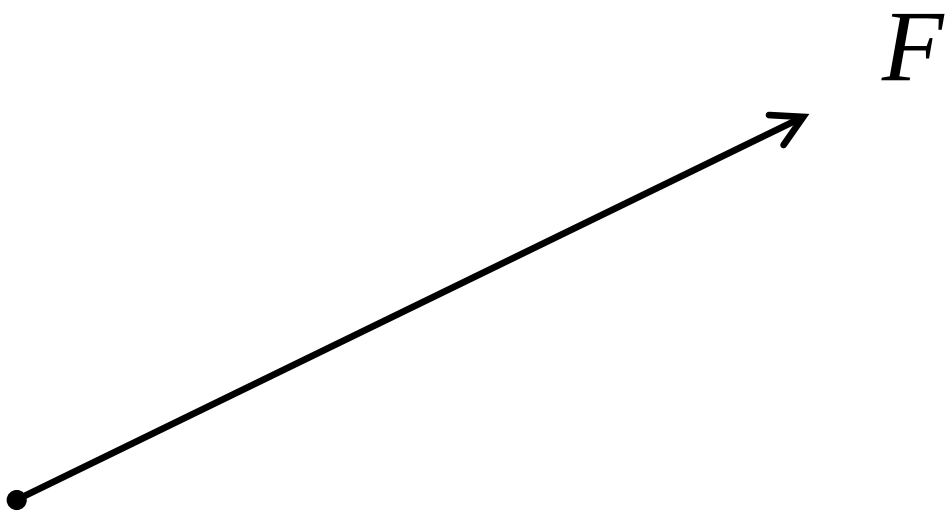
THE MAIN FEATURE OF THE METHODS

The methods only work SOMETIMES.

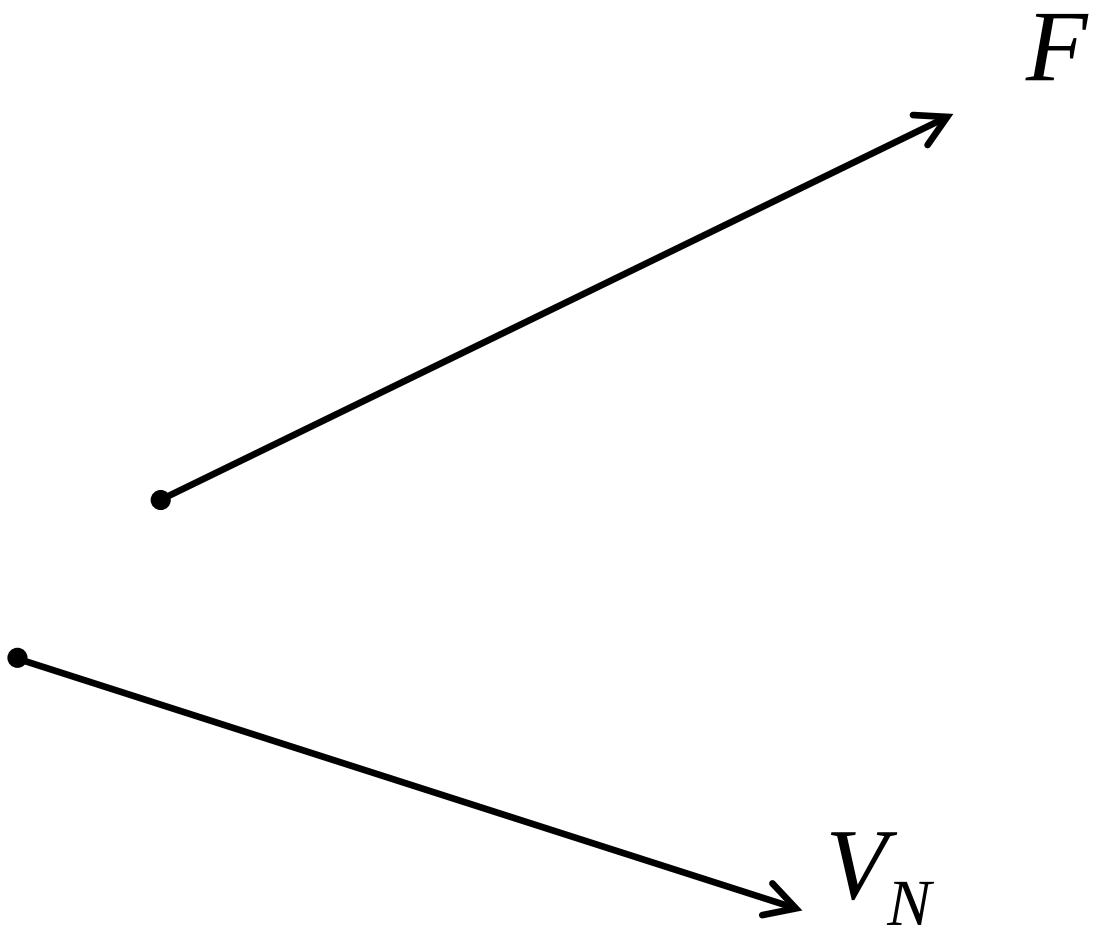
`

How to estimate its effectiveness?

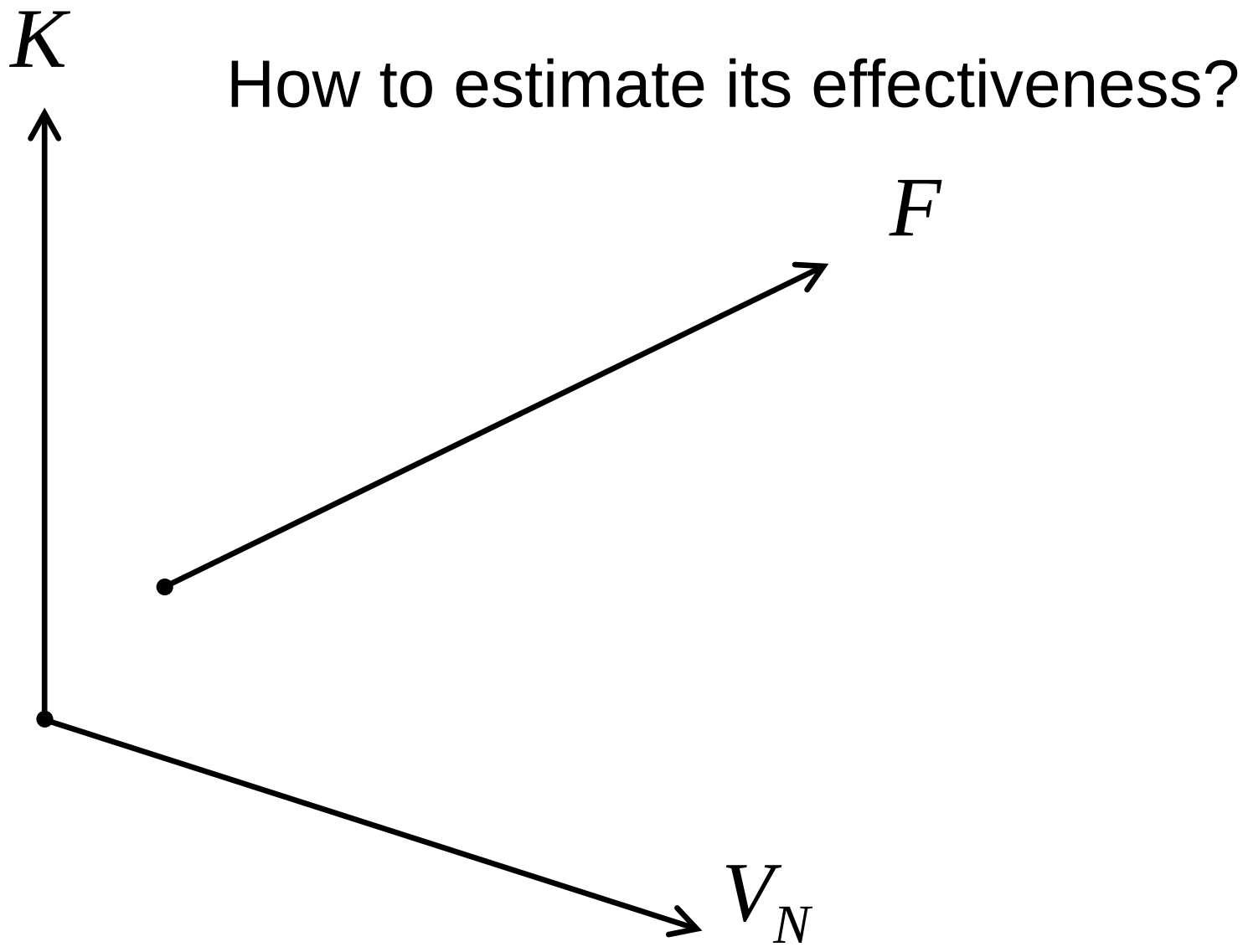
How to estimate its effectiveness?



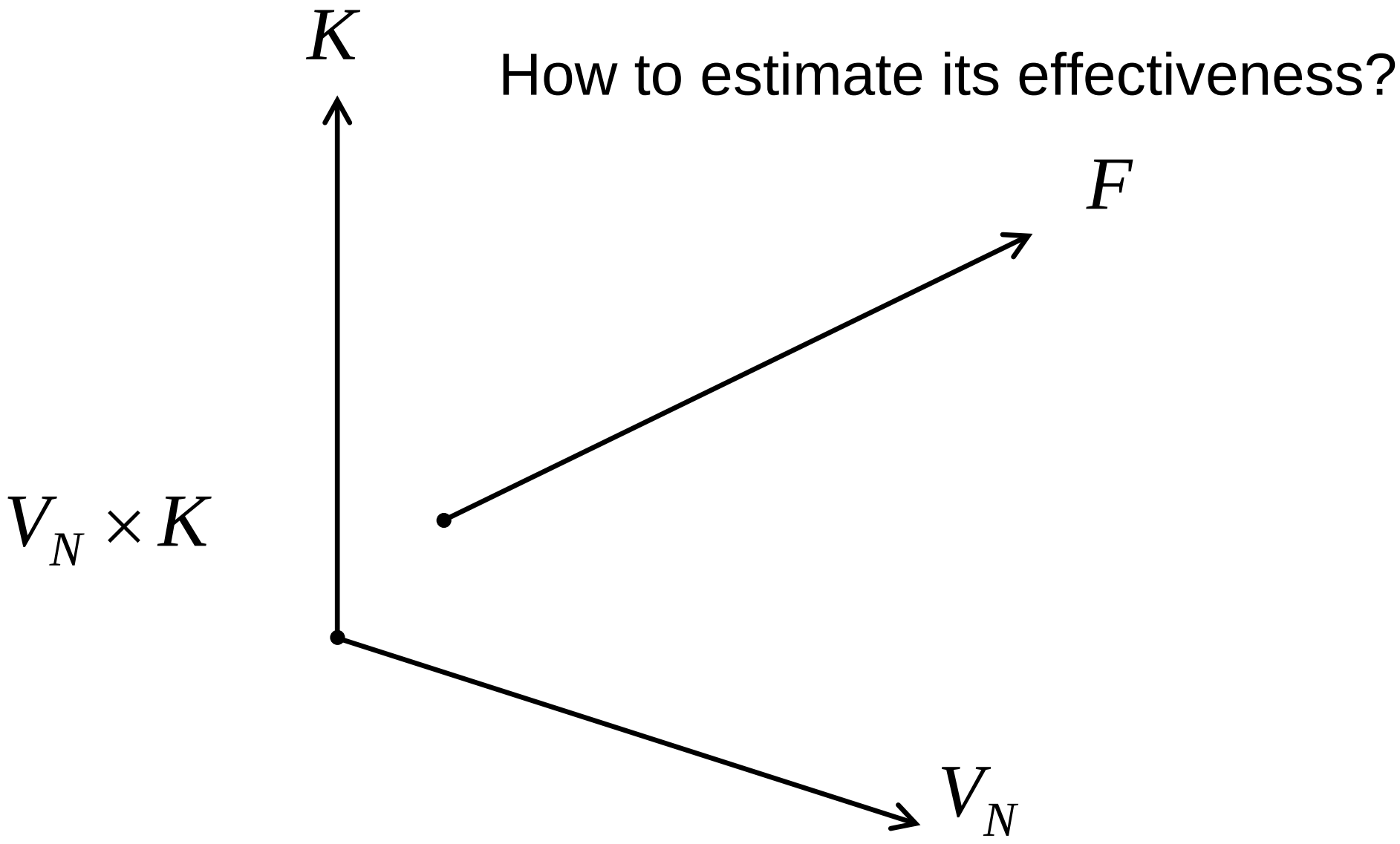
How to estimate its effectiveness?



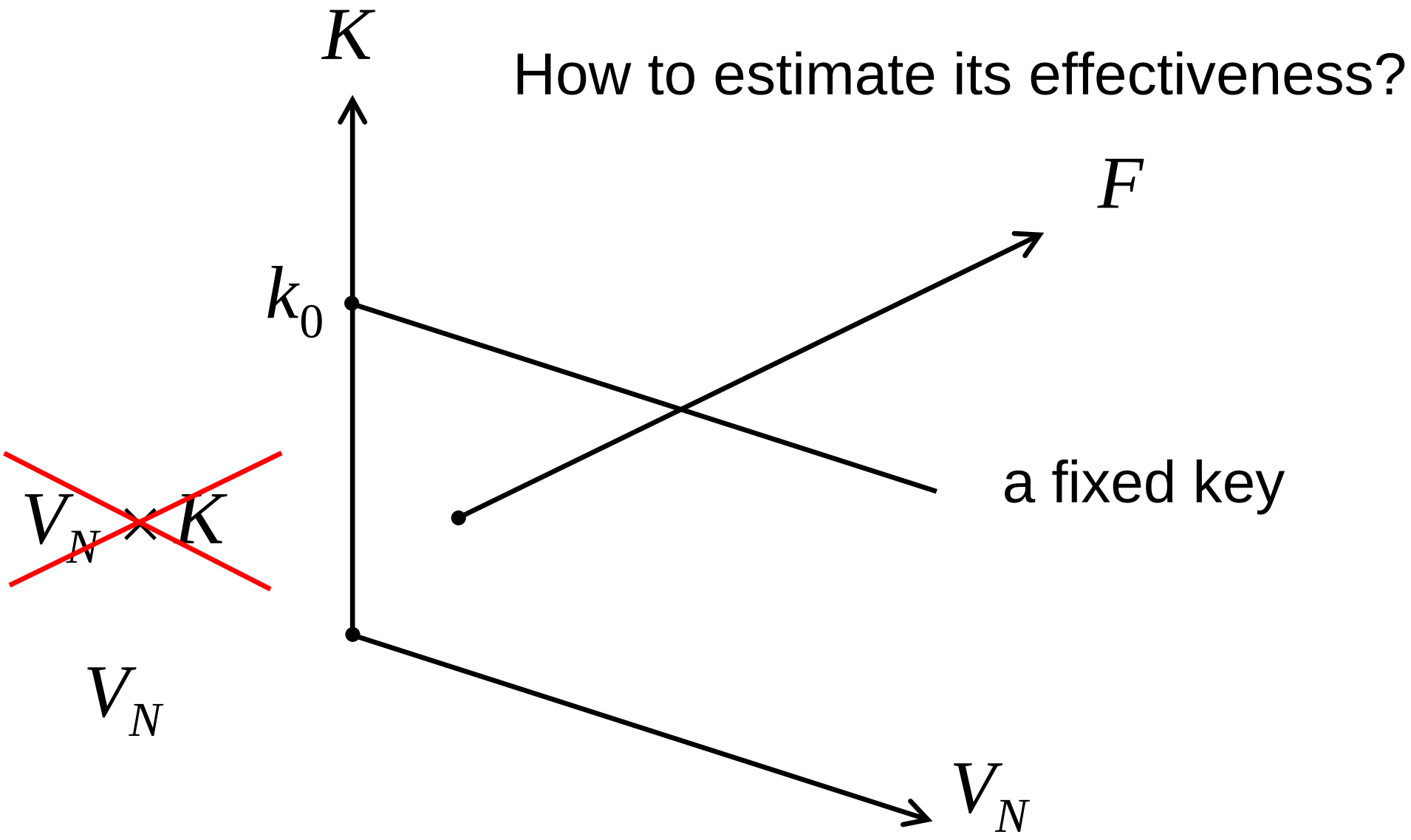
THE MAIN FEATURE OF THE METHODS



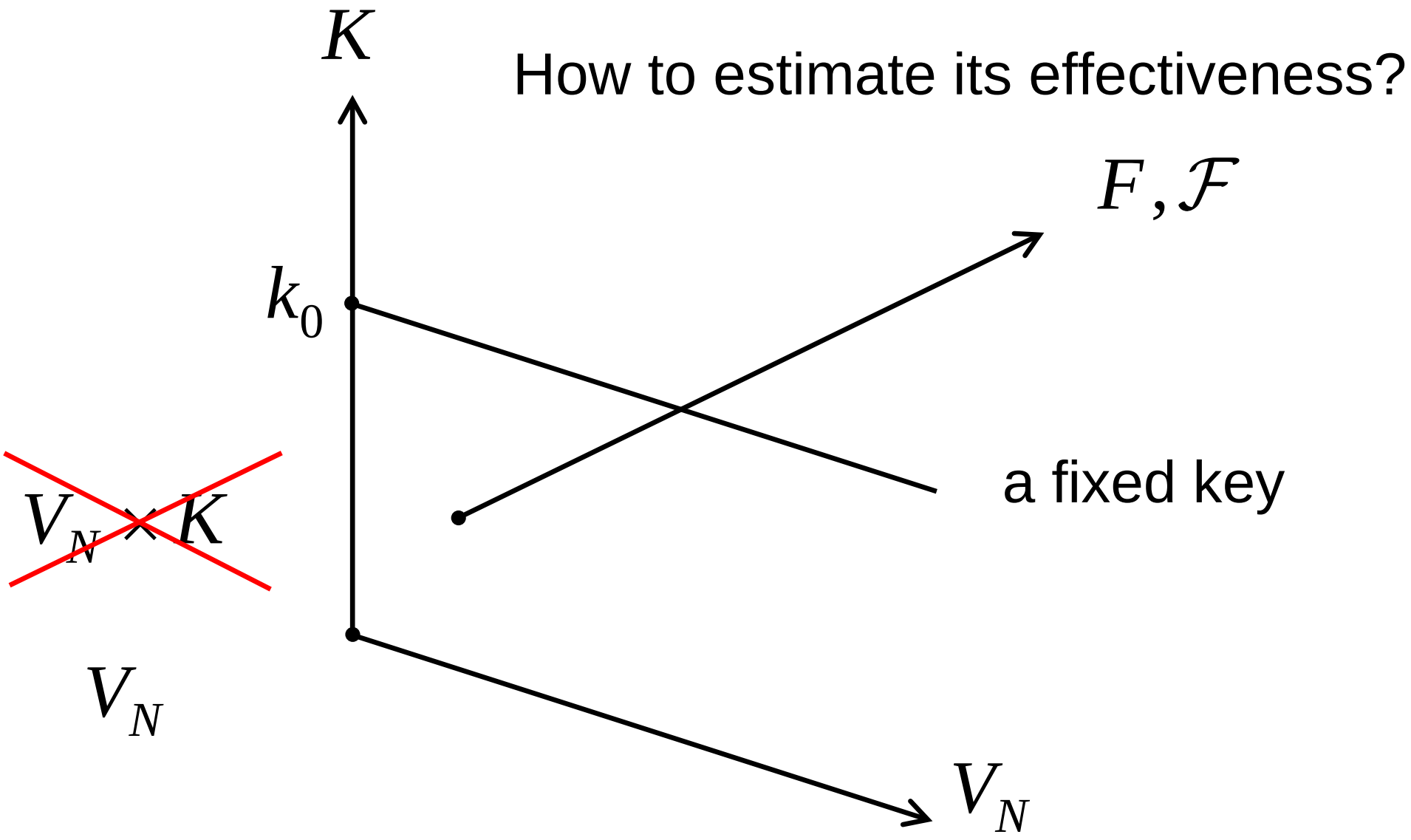
THE MAIN FEATURE OF THE METHODS



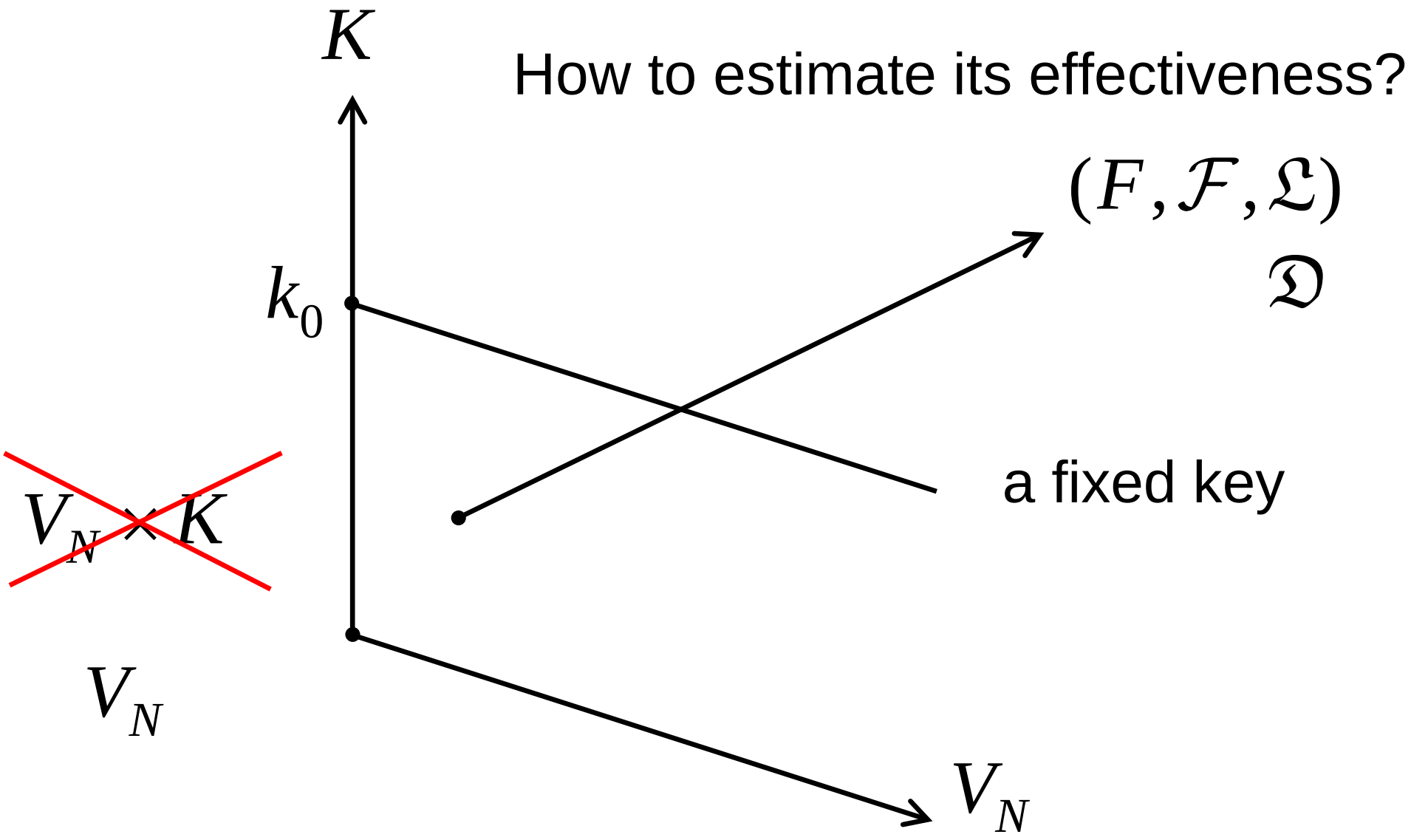
THE MAIN FEATURE OF THE METHODS



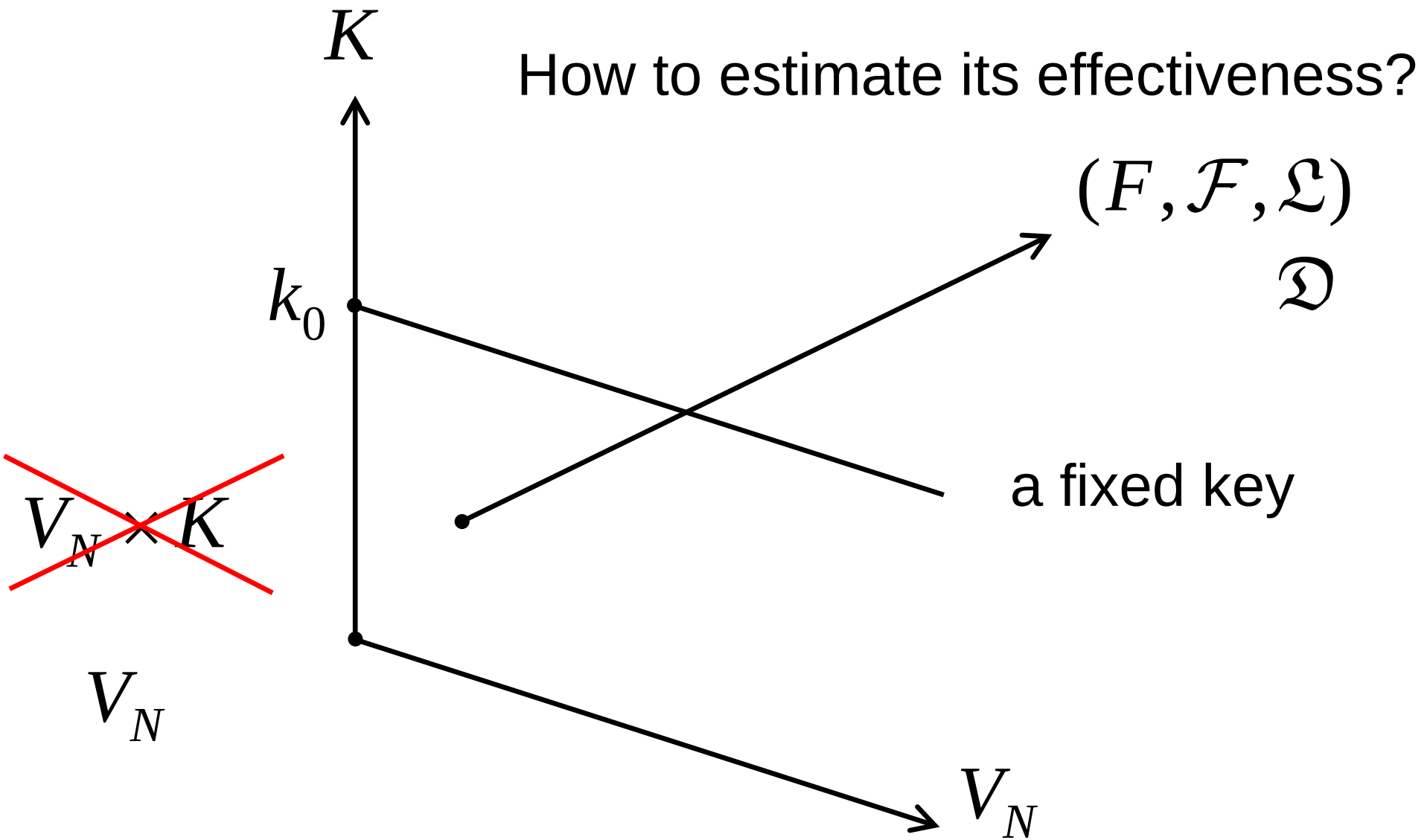
THE MAIN FEATURE OF THE METHODS



THE MAIN FEATURE OF THE METHODS



THE MAIN FEATURE OF THE METHODS



SOMETIMES due to $(F, \mathcal{F}, \mathfrak{L}, k_0)$.
$\mathfrak{D}$

THE DUALITY OF LINEAR AND DIFFERENTIAL CRYPTANALYSIS

$$C\begin{pmatrix} l'_1 \\ \vdots \\ l'_k \\ L'' \end{pmatrix} = \begin{pmatrix} L' \\ l''_1 \\ \vdots \\ l''_k \end{pmatrix}$$

$$(D', d''_1, ..., d''_k)C =$$
$$= (d'_1, ..., d'_k, D'')$$

THE DUALITY OF LINEAR AND DIFFERENTIAL CRYPTANALYSIS

$$C\begin{pmatrix} l'_1 \\ \vdots \\ l'_k \\ L'' \end{pmatrix} = \begin{pmatrix} L' \\ l''_1 \\ \vdots \\ l''_k \end{pmatrix}$$

$$(D', d''_1, ..., d''_k)C = \\ = (d'_1, ..., d'_k, D'')$$

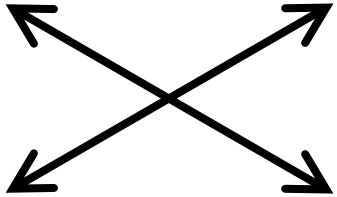
$$(l'^T_1, ..., l'^T_k, L''^T)C^T = \\ = (L'^T, l''^T_1, ..., l''^T_k)$$

$$C^T\begin{pmatrix} D'^T \\ d''^T_1 \\ \vdots \\ d''^T_k \end{pmatrix} = \begin{pmatrix} d'^T_1 \\ \vdots \\ d'^T_k \\ D''^T \end{pmatrix}$$

THE DUALITY OF LINEAR AND DIFFERENTIAL CRYPTANALYSIS

$$C\begin{pmatrix} l'_1 \\ \vdots \\ l'_k \\ L'' \end{pmatrix} = \begin{pmatrix} L' \\ l''_1 \\ \vdots \\ l''_k \end{pmatrix}$$

$$(D', d''_1, ..., d''_k)C = (d'_1, ..., d'_k, D'')$$



$$(l'^T_1, ..., l'^T_k, L''^T)C^T = (L'^T, l''^T_1, ..., l''^T_k)$$

$$C^T\begin{pmatrix} D'^T \\ d''^T_1 \\ \vdots \\ d''^T_k \end{pmatrix} = \begin{pmatrix} d'^T_1 \\ \vdots \\ d'^T_k \\ D''^T \end{pmatrix}$$

E. Biham, A. Shamir, 1990

Biham E., Shamir A. Differential Cryptanalysis of DES-like Cryptosystems (Extended Abstract). – Advances in Cryptology – CRYPTO'90. – LNCS, 1991, vol. 537, p. 2–21.

Biham E., Shamir A. Differential cryptanalysis of DES-like cryptosystems. – Journal of Cryptology, 1991, vol. 4(1), p. 3–72.

Biham E., Shamir A. Differential Cryptanalysis of the Data Encryption Standard. – Berlin, New-York: Springer, 1993.

M. Matsui, 1993

Matsui M. Linear Cryptoanalysis Method for DES Cipher. – Advances in Cryptology – Eurocrypt'1993. – LNCS, 1994, vol. 765, p. 24–27.

Matsui M. The first experimental cryptanalysis of the Data Encryption Standard. – Advances in Cryptology – CRIPTO'1994. – LNCS, 1994, vol. 839, p. 1–11.

Biham E. On Matsui's Linear Cryptanalysis. – Advances in Cryptology – Eurocrypt'1994. – LNCS, 1995, vol. 950, p. 341–355.

LINEAR CRYPTANALYSIS: RUSSIAN WORKS

Malyshev F. M. The duality of differential and linear methods in cryptography // Mat. Vopr. Krypt., 2014, v. 5, № 3, pp. 35-47.

Malyshev F. M., Trifonov D. I., Diffusion properties of XSLP-ciphers // Mat. Vopr. Krypt., 2016, v. 7, № 3, pp. 47-60.

Erokhin A. V., Malyshev F. M., Trishin A. E. Multidimentional linear method and diffusion characteristics of linear medium of ciphering transform // Mat. Vopr. Krypt., 2017, v. 8, № 4, pp. 29-62.

Malyshev F. M., Trishin A. E. Linear and Differential Cryptanalysis: Another Viewpoint / XV Int. Conf. “Algebra, Number Theory and Discrete Geometry: modern problems and applications”, dedicated to the centenary of the birth of the Doctor of Physical and Mathematical Sciences, Professor of the Moscow State University Korobov Nikolai Mikhailovich, Tula, May 28-31, 2018, pp. 42-45.

1. The linear medium of the functional scheme
2. Theorems 1, 2
3. Universal functional scheme
4. Methodology of experiments
5. The degrees of diffusion of the linear medium
6. The dual linear medium (the duality of linear and differential cryptanalysis)

1. The linear medium of the functional scheme
2. Theorems 1, 2
3. Universal functional scheme
4. Methodology of experiments
5. The degrees of diffusion of the linear medium
6. The dual linear medium (the duality of linear and differential cryptanalysis)

QUESTIONS?

QUESTIONS