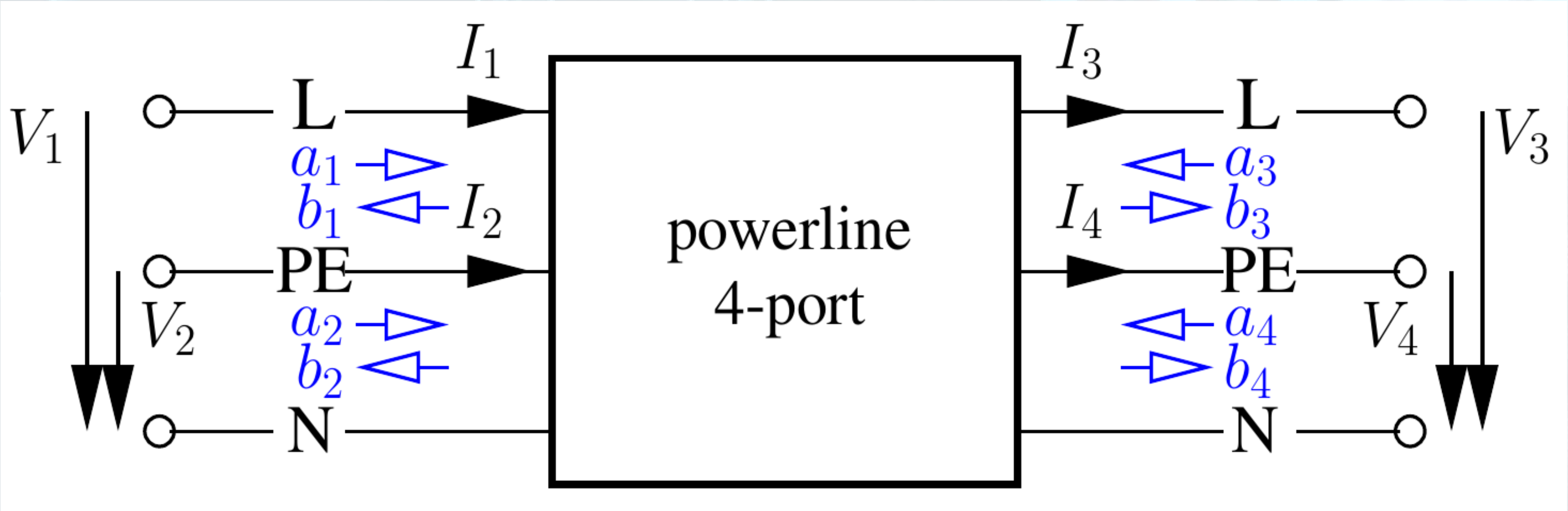
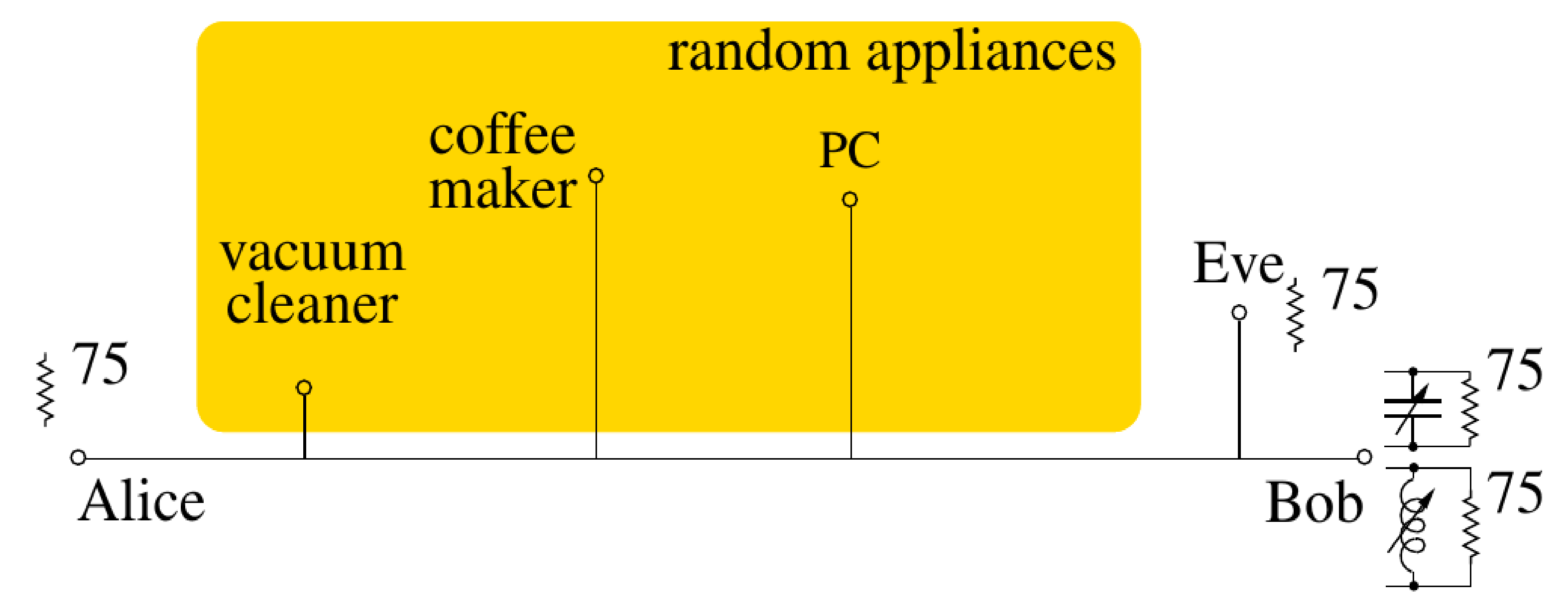
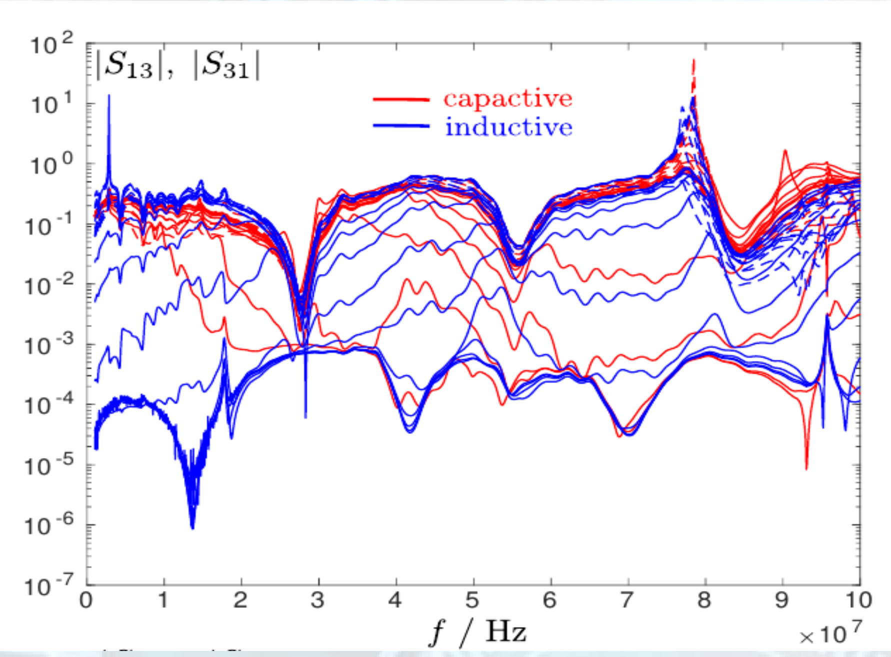
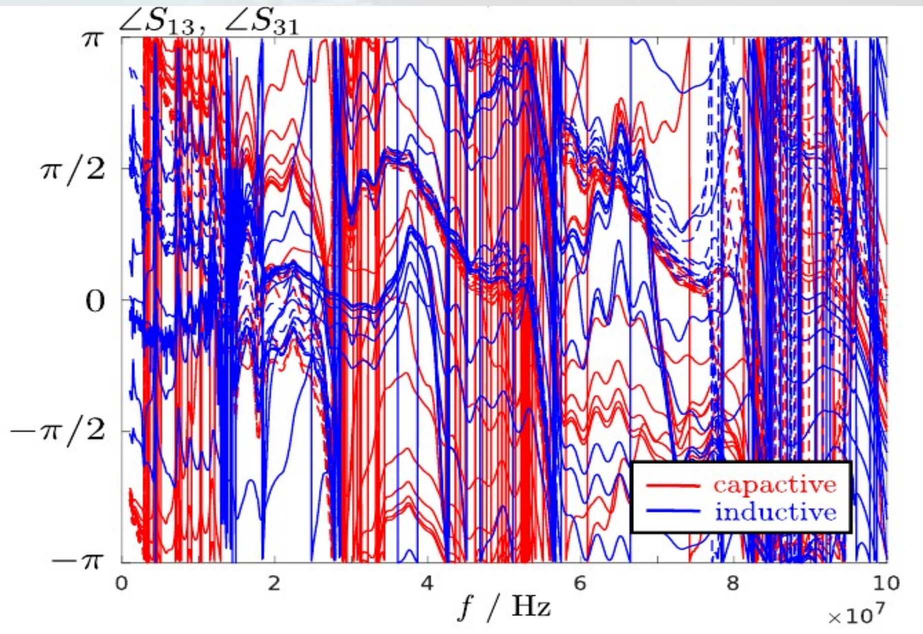
Power-Line Physical-Layer Key Generation Study Based on Low Complexity 3-Wire 4-Port Modeling



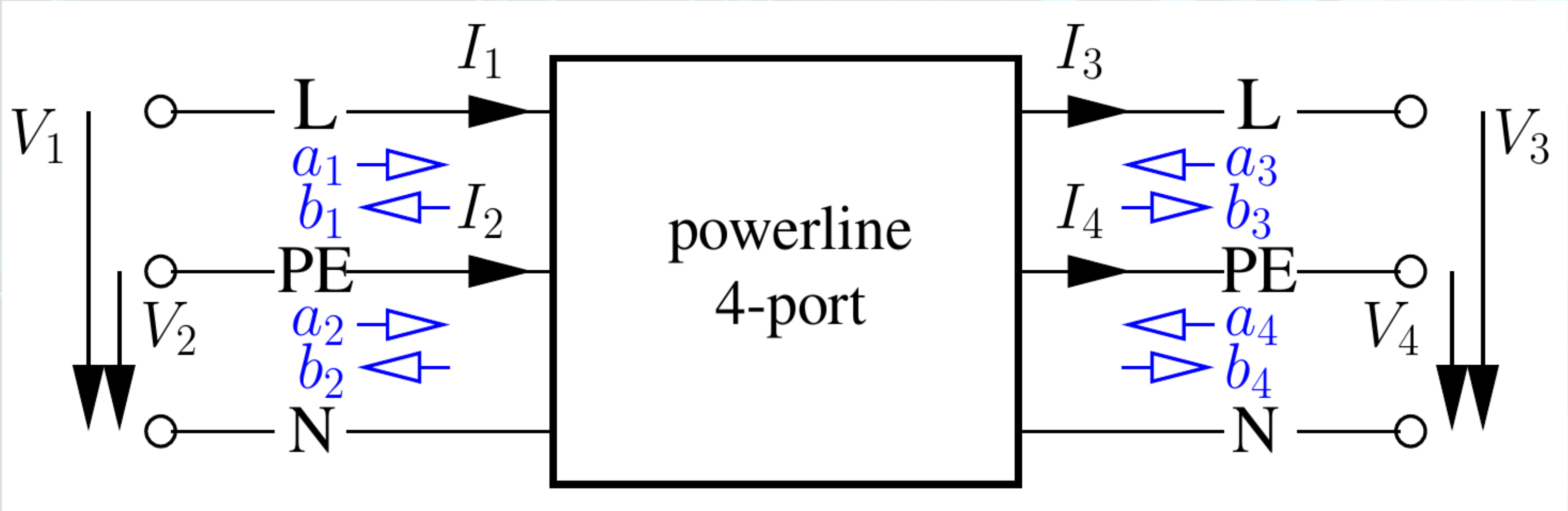


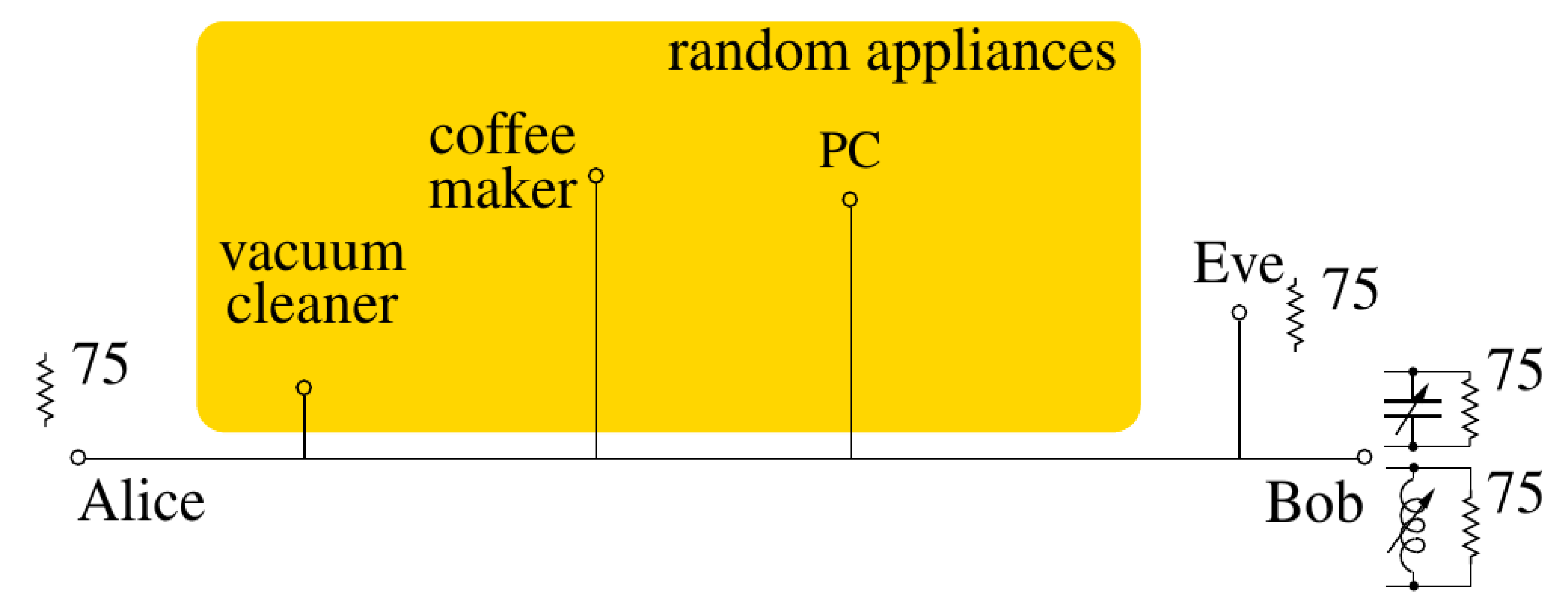




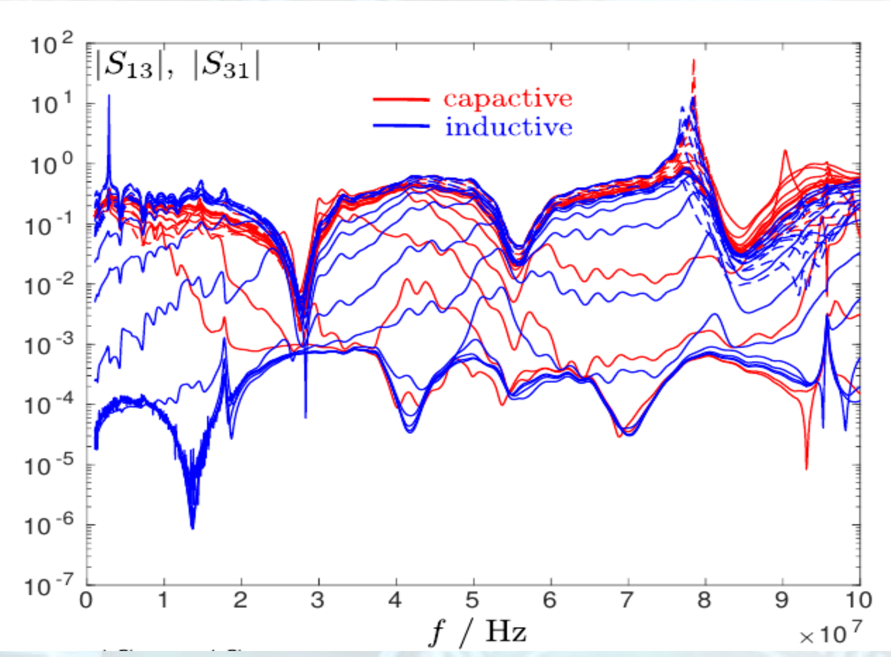
Werner Henkel, Tai Him Yim, Aditya Ojha, Sumit Giri, and Ehsan Olyaei Torshizi
Constructor University Bremen, Germany

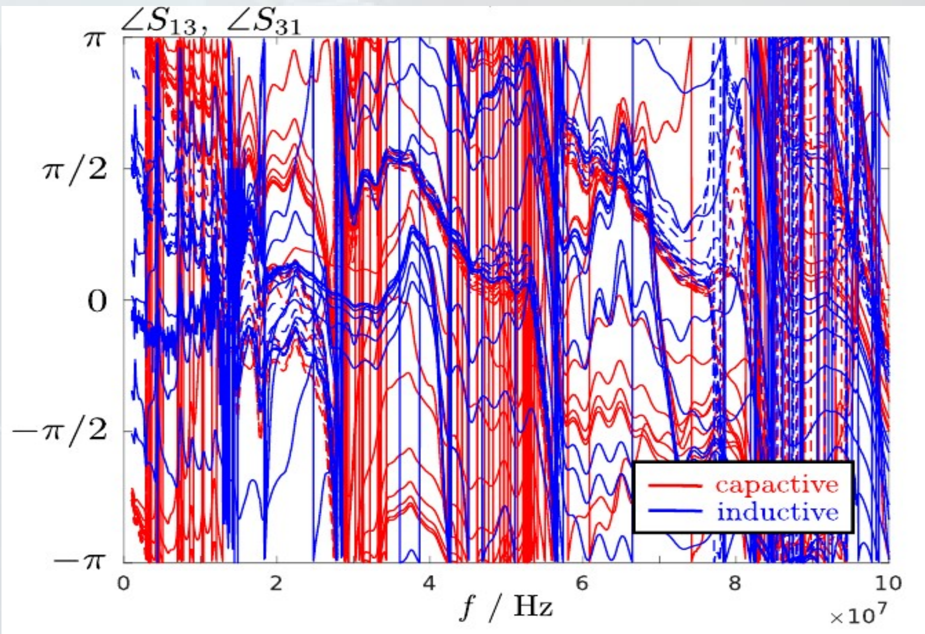
Power-Line Physical-Layer Key Generation Study Based on Low Complexity 3-Wire 4-Port Modeling





- Physical-layer key generation using reciprocity (common randomness)
- Matrix model of a 3-wire transmission line
- 3-wire bridged tap
- Key generation from phase (or amplitude) of the transfer factor / function
- Performance with randomized one-sided centering



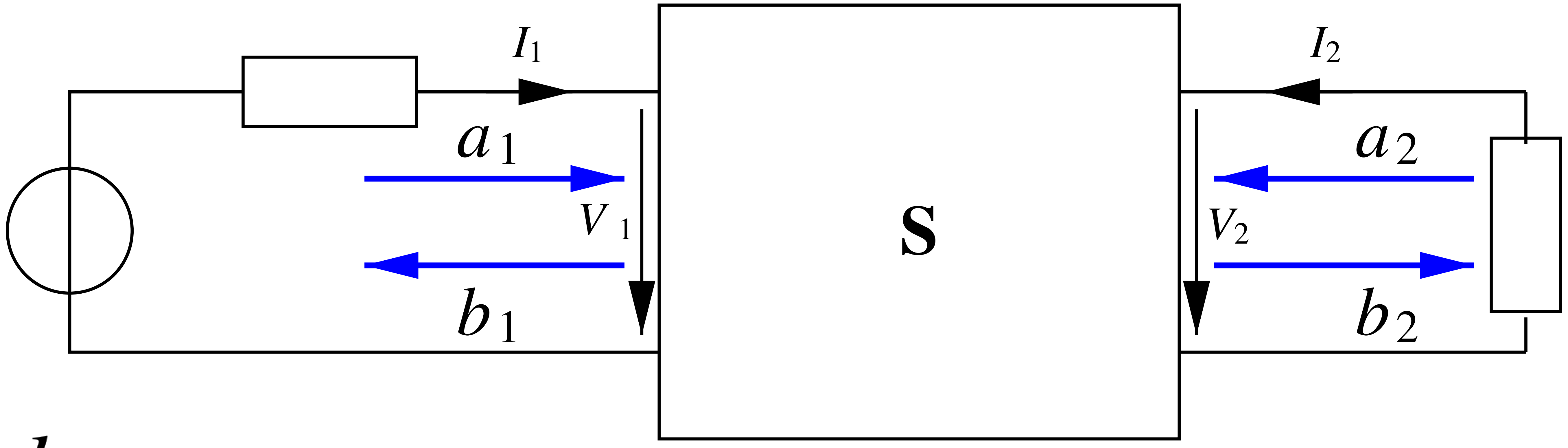


Physical-layer key generation using reciprocity (common randomness)

Reciprocity in two-ports:

$$Z_{12} = Z_{21}, \quad Y_{12} = Y_{21}, \quad \det(\mathbf{A}) = 1 \text{ and } \boxed{S_{12} = S_{21}}, \quad \det(\mathbf{T}) = 1$$

$$\begin{bmatrix} b_1 \\ b_2 \end{bmatrix} = \begin{bmatrix} S_{11} & \boxed{S_{12}} \\ \boxed{S_{21}} & S_{22} \end{bmatrix} \begin{bmatrix} a_1 \\ a_2 \end{bmatrix}$$



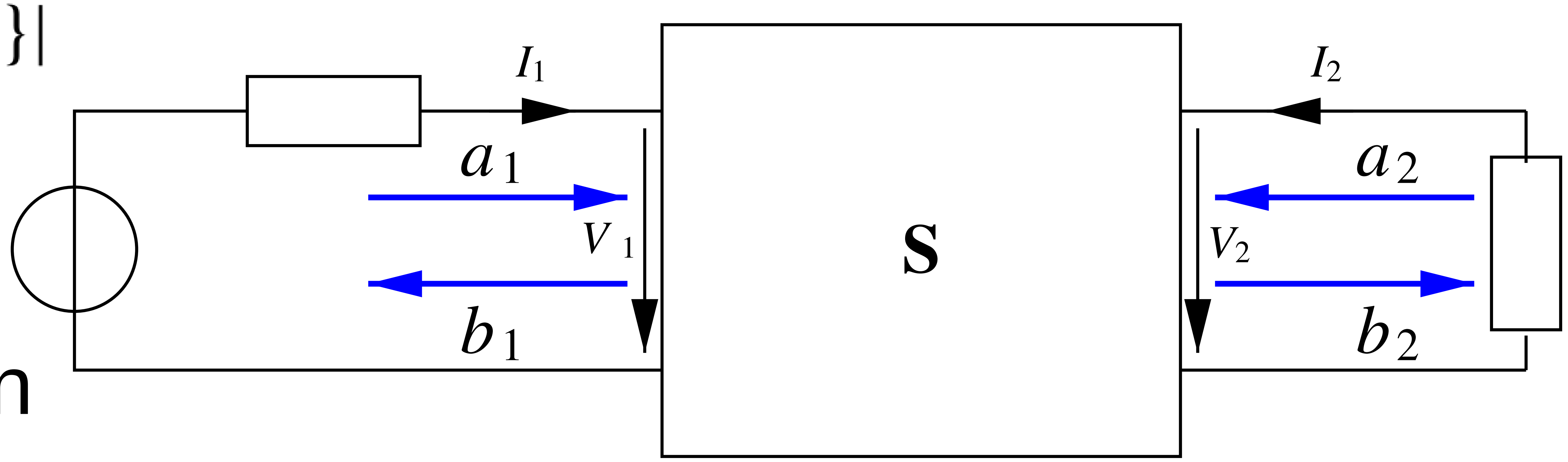
$$S_{11} = \left.\frac{b_1}{a_1}\right|_{a_2=0}, \qquad \boxed{S_{12}} = \left.\frac{b_1}{a_2}\right|_{a_1=0}$$

$$\boxed{S_{21}} = \left.\frac{b_2}{a_1}\right|_{a_2=0}, \qquad S_{22} = \left.\frac{b_2}{a_2}\right|_{a_1=0}$$

Physical-layer key generation using reciprocity (common randomness)

S-parameters vs. transfer function ...

$$a_i = \frac{1}{2}\frac{(V_i + Z_0 I_i)}{\sqrt{|\Re\{Z_0\}|}}, \qquad b_i = \frac{1}{2}\frac{(V_i - Z_0^* I_i)}{\sqrt{|\Re\{Z_0\}|}}$$



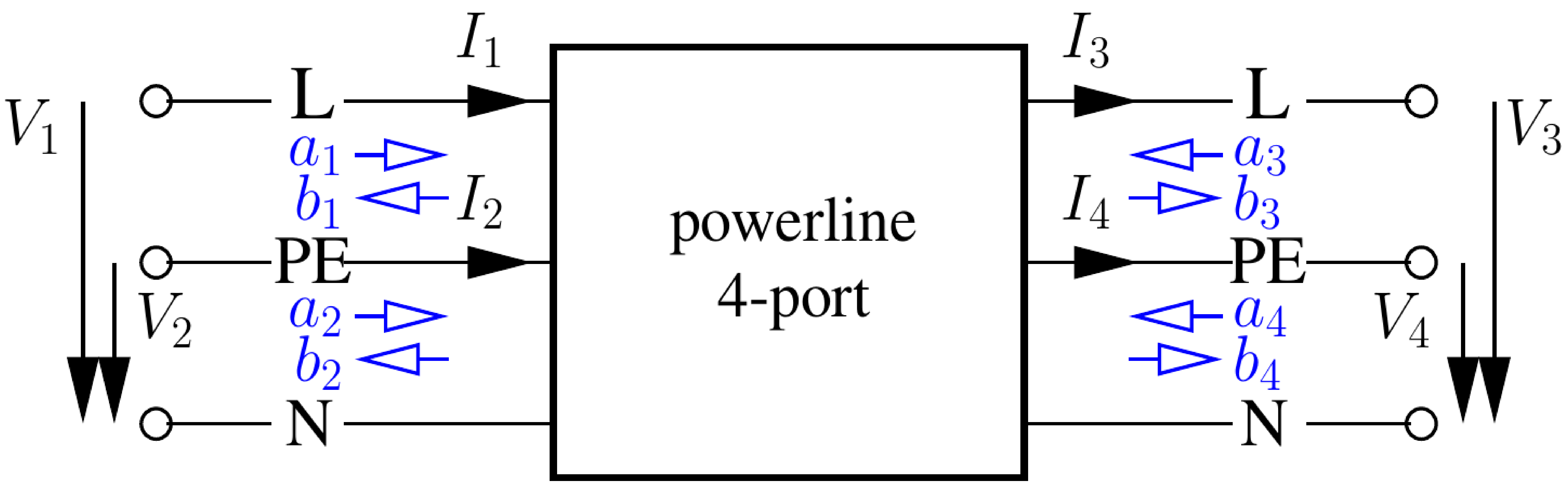
For perfectly matching termination (assuming $Z_0 \in \mathbb{R}$):

$$a_1 = \frac{V_1}{\sqrt{|\Re\{Z_0\}|}} \qquad b_2 = \frac{V_2}{\sqrt{|\Re\{Z_0\}|}}$$

$$\Longrightarrow S_{21} = \frac{b_2}{a_1} = \frac{V_2}{V_1} \text{ and } S_{12} = \frac{b_1}{a_2} = \frac{V_1}{V_2}$$

Transfer factor = transfer function

Matrix model of a 3-wire transmission line



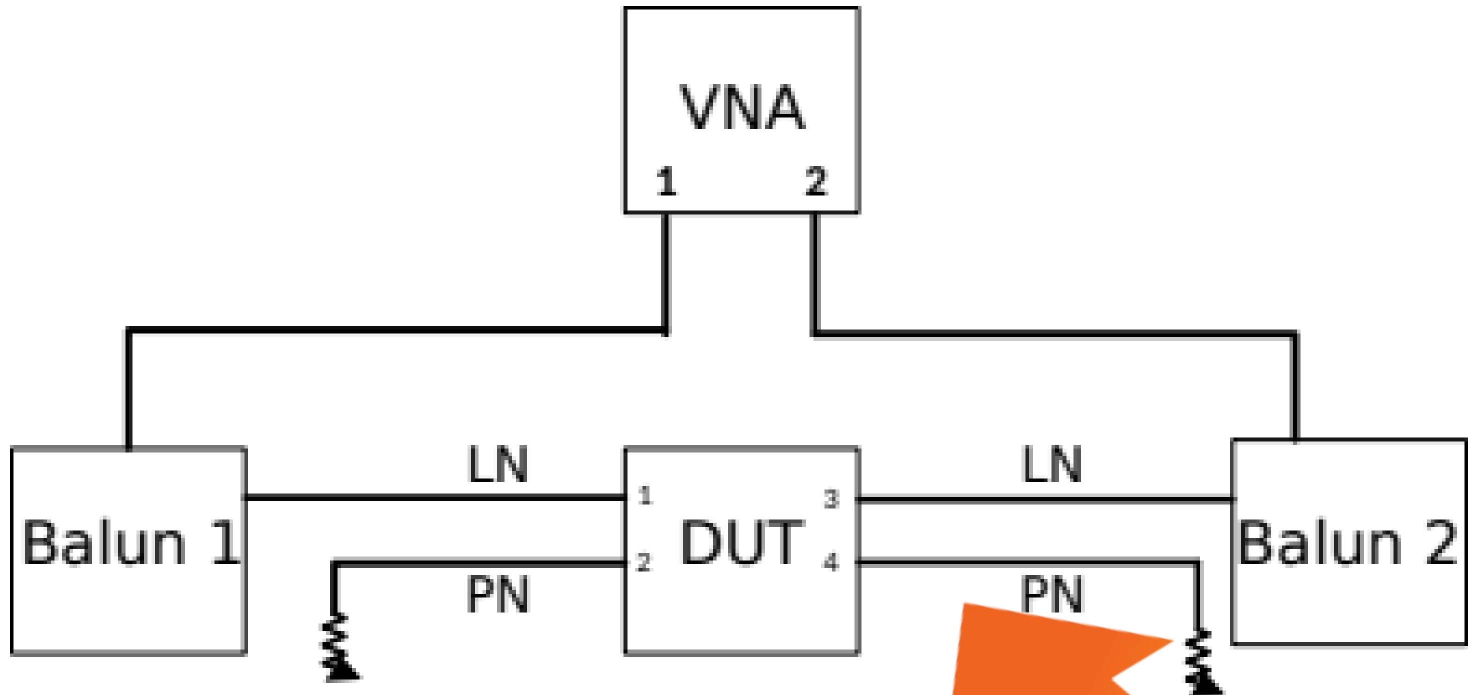
$$\begin{bmatrix} V_1 \\ V_2 \\ I_1 \\ I_2 \end{bmatrix} = \begin{bmatrix} A_1 & A_2 & B_1 & B_2 \\ A_3 & A_4 & B_3 & B_4 \\ C_1 & C_2 & D_1 & D_2 \\ C_3 & C_4 & D_3 & D_4 \end{bmatrix} \begin{bmatrix} V_3 \\ V_4 \\ I_3 \\ I_4 \end{bmatrix} \qquad \begin{bmatrix} b_1 \\ b_2 \\ b_3 \\ b_4 \end{bmatrix} = \begin{bmatrix} S_{11} & S_{12} & S_{13} & S_{14} \\ S_{21} & S_{22} & S_{23} & S_{24} \\ S_{31} & S_{32} & S_{33} & S_{34} \\ S_{41} & S_{42} & S_{43} & S_{44} \end{bmatrix} \begin{bmatrix} a_1 \\ a_2 \\ a_3 \\ a_4 \end{bmatrix}$$

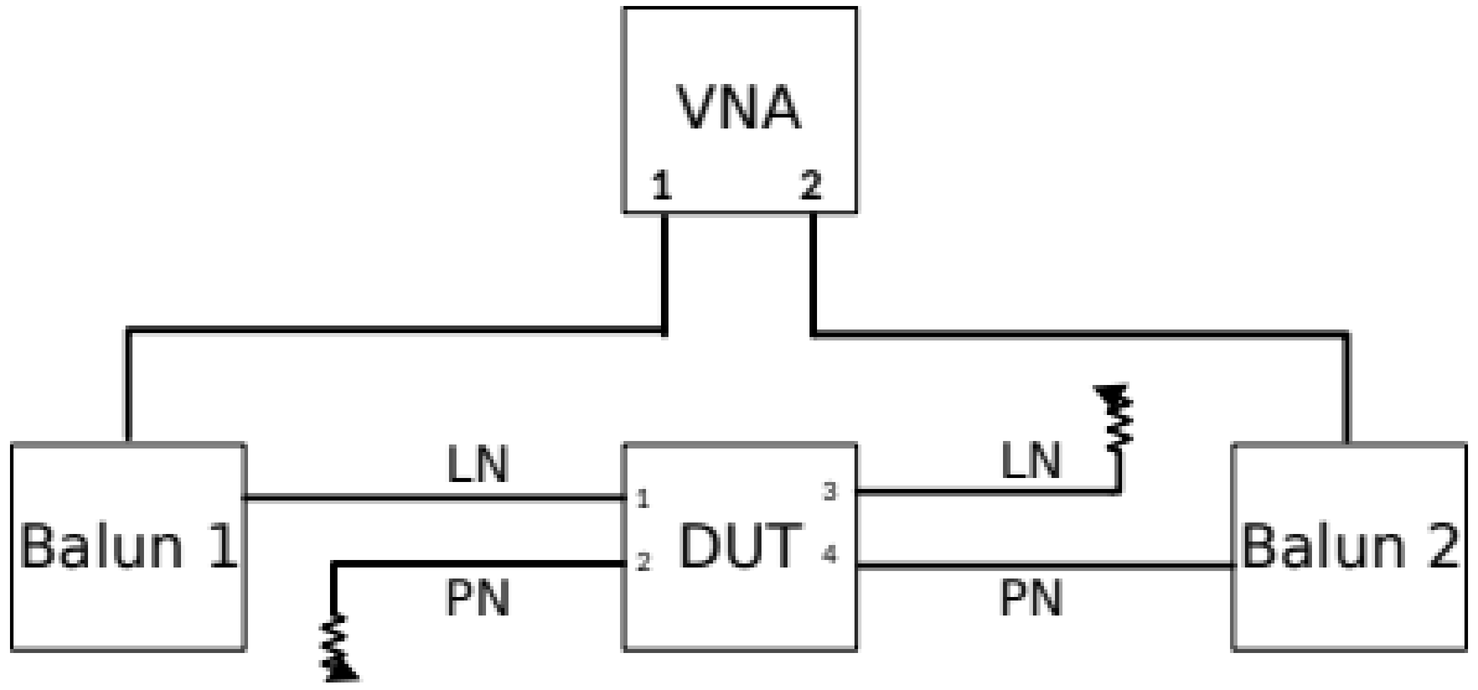
Matrix model of a 3-wire transmission line

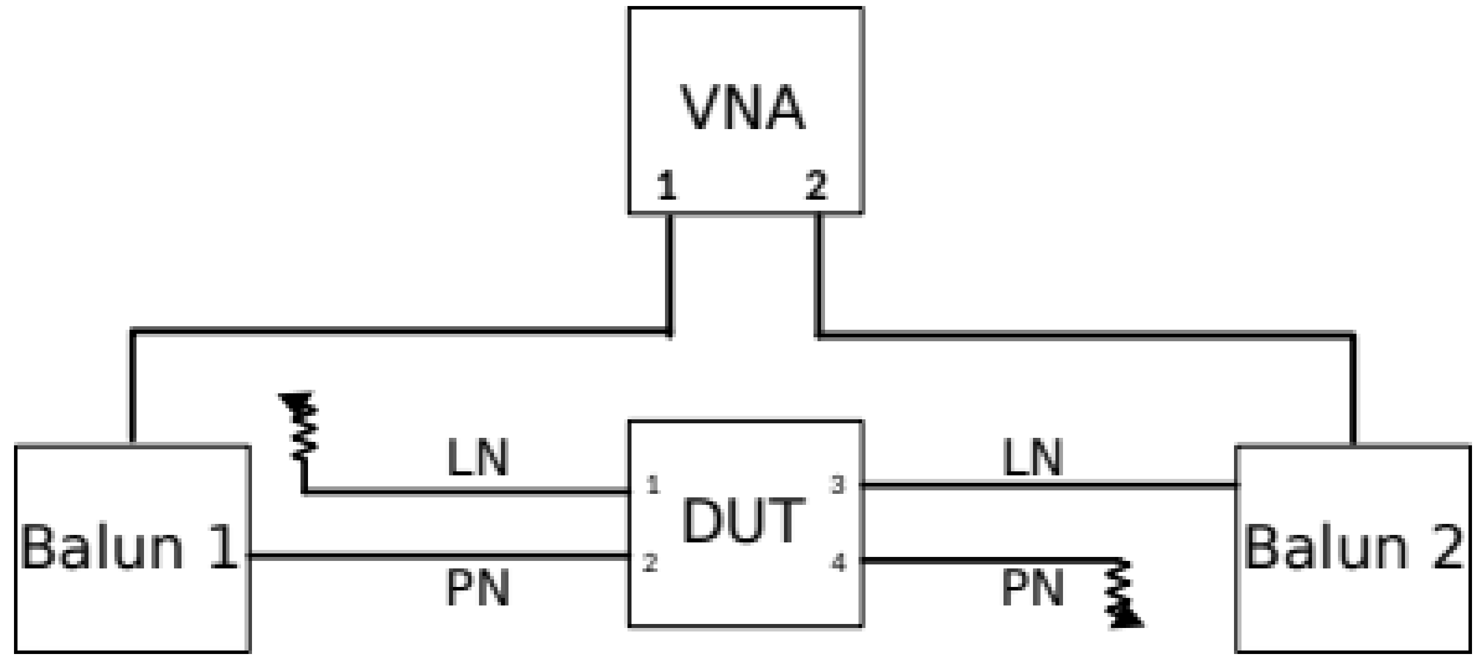
Measurement

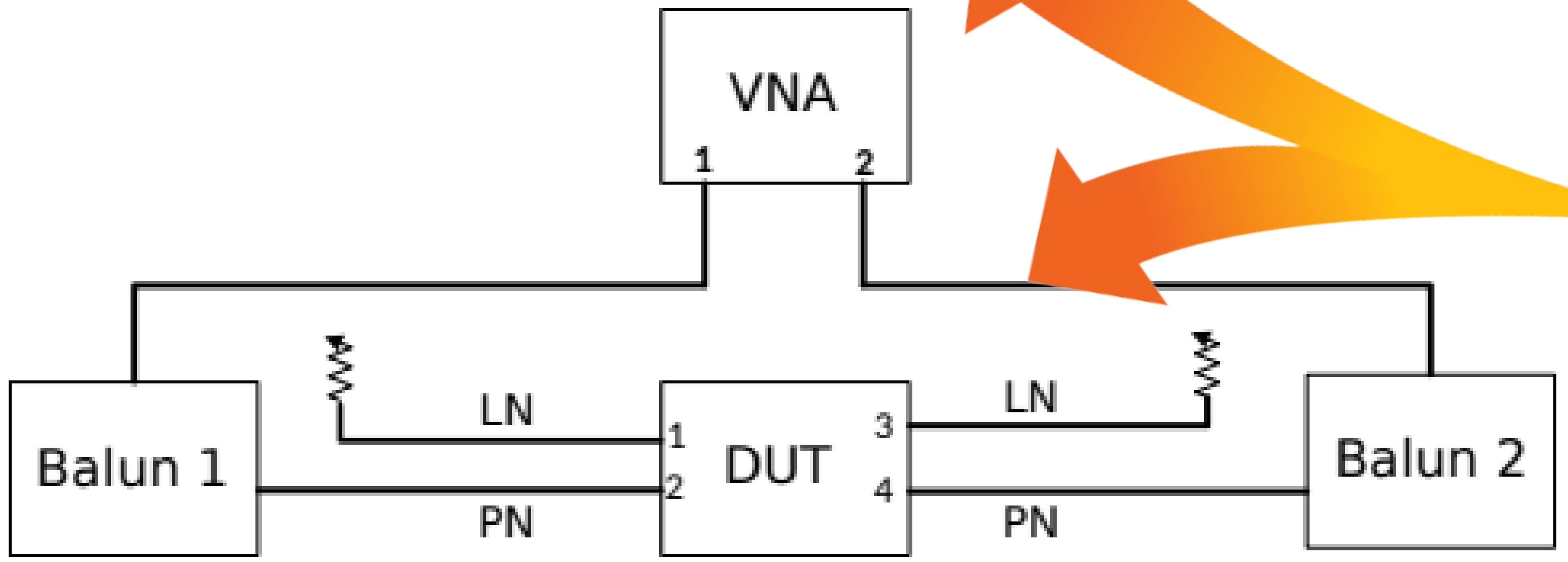
$$\begin{bmatrix} S_{11} & S_{13} \\ S_{31} & S_{33} \end{bmatrix}, \begin{bmatrix} S_{11} & S_{14} \\ S_{41} & S_{44} \end{bmatrix}, \begin{bmatrix} S_{22} & S_{23} \\ S_{32} & S_{33} \end{bmatrix}$$

$$\begin{bmatrix} S_{22} & S_{24} \\ S_{42} & S_{44} \end{bmatrix}, \begin{bmatrix} S_{11} & S_{12} \\ S_{21} & S_{22} \end{bmatrix}, \begin{bmatrix} S_{33} & S_{34} \\ S_{43} & S_{44} \end{bmatrix}$$

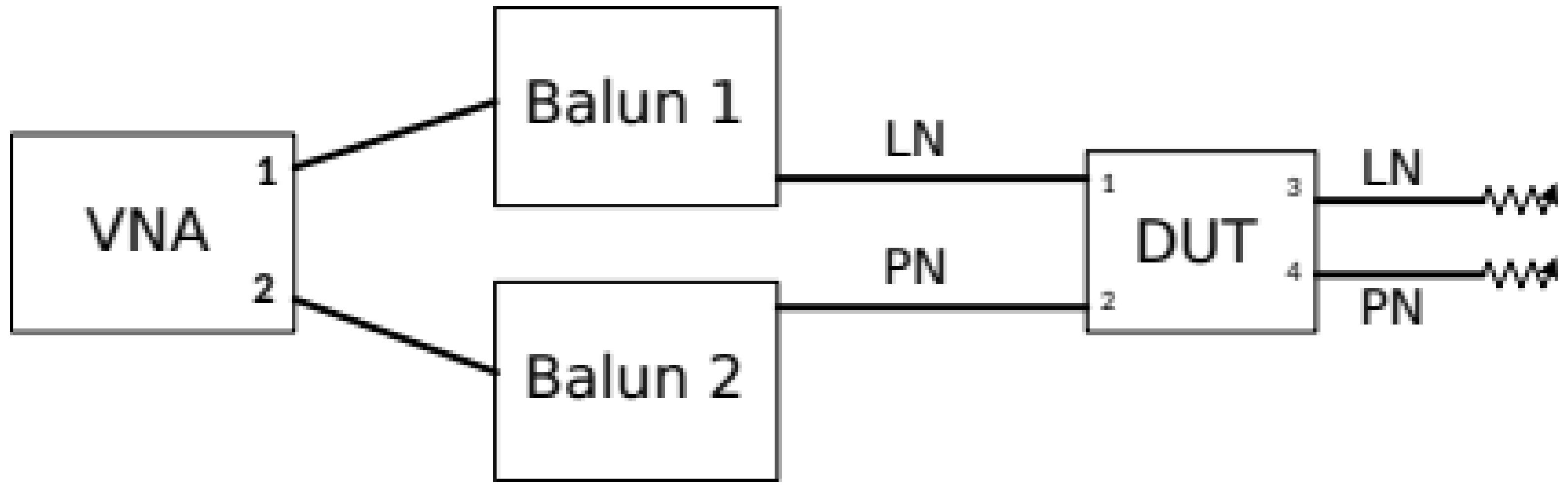


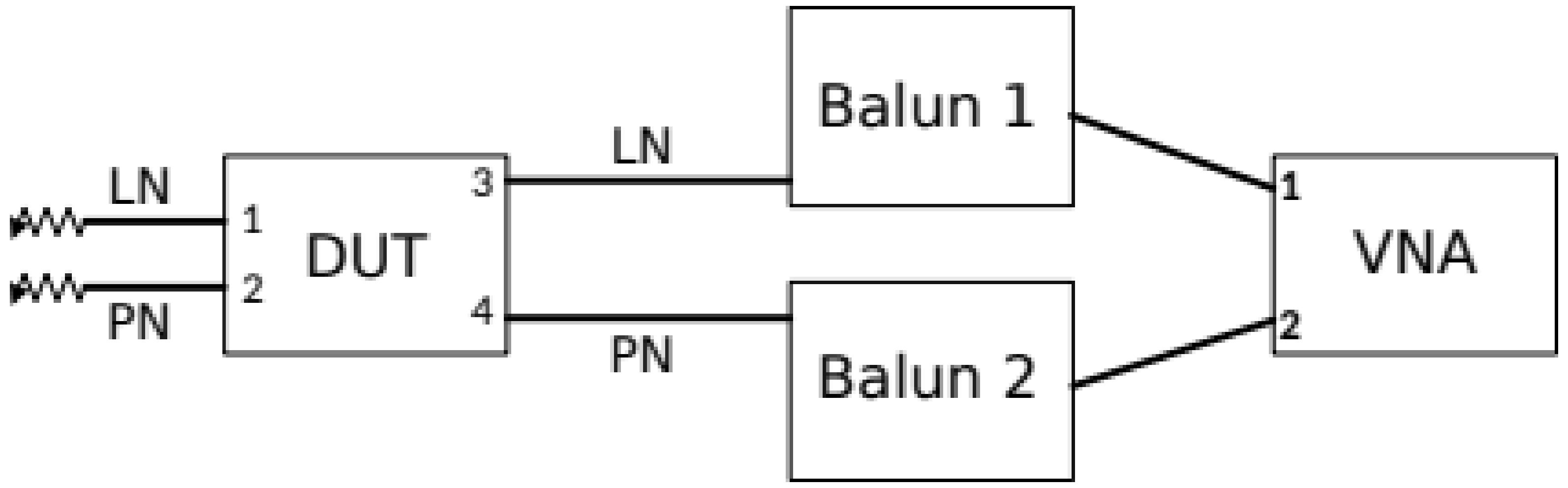






$$\begin{bmatrix} \cosh \gamma l & Z_w \sinh \gamma l \\ \frac{1}{Z_w} \sinh \gamma l & \cosh \gamma l \end{bmatrix}$$

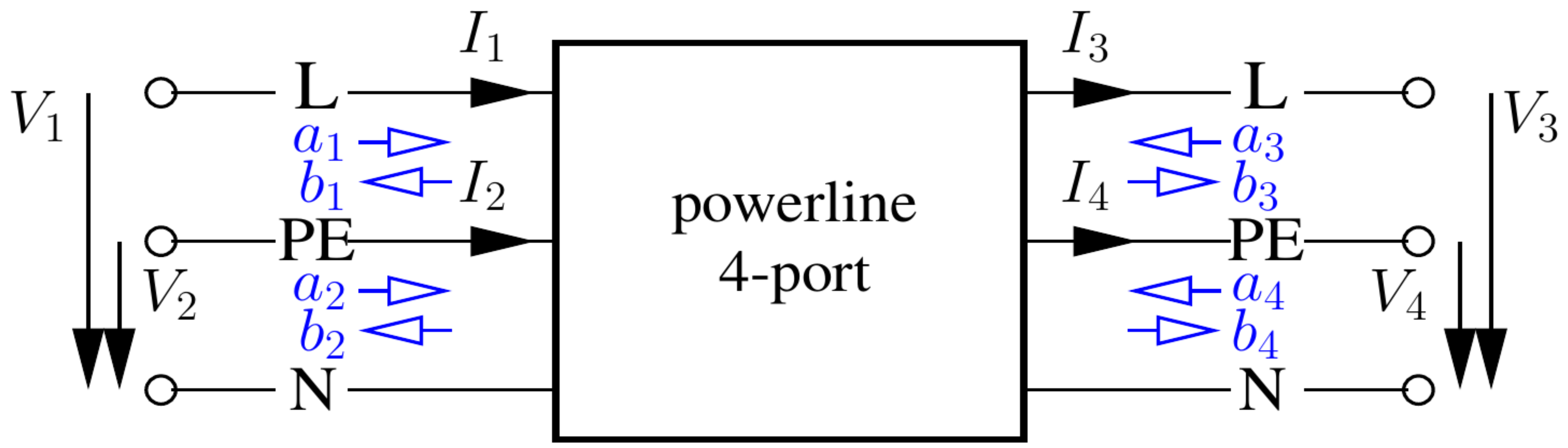




For other measurements and matrix components:

FEXT contribution (Far-End CrossTalk)

Matrix model of a 3-wire transmission line

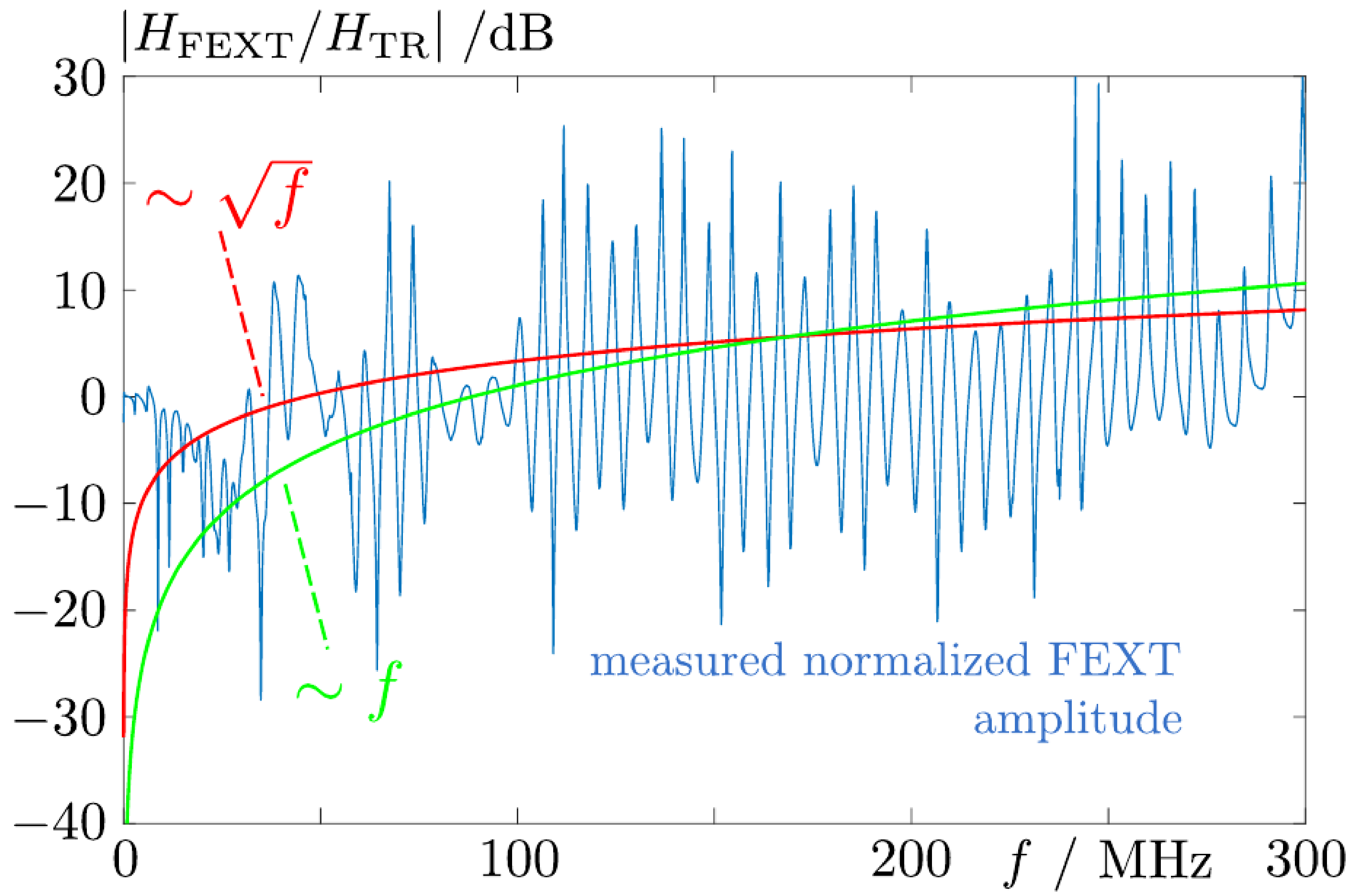


$$\begin{bmatrix} V_1 \\ V_2 \\ I_1 \\ I_2 \end{bmatrix} = \begin{bmatrix} A_1 & A_2 & B_1 & B_2 \\ A_3 & A_4 & B_3 & B_4 \\ C_1 & C_2 & D_1 & D_2 \\ C_3 & C_4 & D_3 & D_4 \end{bmatrix} \begin{bmatrix} V_3 \\ V_4 \\ I_3 \\ I_4 \end{bmatrix}$$

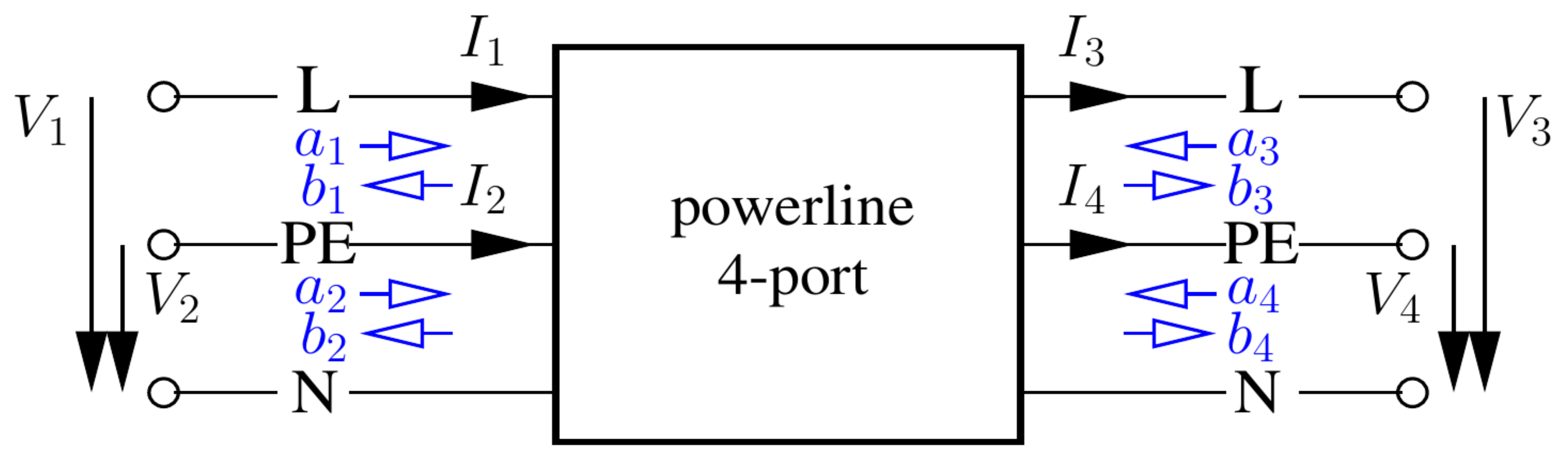
$$\begin{bmatrix} V_1 \\ V_2 \\ I_1 \\ I_2 \end{bmatrix} = \begin{bmatrix} A_1 & A_2 & B_1 & B_2 \\ A_3 & A_4 & B_3 & B_4 \\ C_1 & C_2 & D_1 & D_2 \\ C_3 & C_4 & D_3 & D_4 \end{bmatrix} \begin{bmatrix} V_3 \\ V_4 \\ I_3 \\ I_4 \end{bmatrix}$$

DSL FEXT model: $H_{\mathrm{FEXT}} = H_{\mathrm{TR}} \cdot \sqrt{l/l_0} \cdot \boxed{f} \cdot k$

Modification: $\frac{V_1}{V_4} \approx \frac{V_2}{V_4} \underbrace{\sqrt{l/l_0} \cdot \boxed{\sqrt{f}} \cdot k}_{H_{\mathrm{mod}}}$ and $\frac{I_2}{V_3} \approx \frac{I_1}{V_3} \underbrace{\sqrt{l/l_0} \cdot \boxed{\sqrt{f}} \cdot k}_{H_{\mathrm{mod}}}$



Matrix model of a 3-wire transmission line



$$\begin{bmatrix} V_1 \\ V_2 \\ I_1 \\ I_2 \end{bmatrix} = \begin{bmatrix} A_1 & A_2 & B_1 & B_2 \\ A_3 & A_4 & B_3 & B_4 \\ C_1 & C_2 & D_1 & D_2 \\ C_3 & C_4 & D_3 & D_4 \end{bmatrix} \begin{bmatrix} V_3 \\ V_4 \\ I_3 \\ I_4 \end{bmatrix}$$

$$\begin{aligned} A_1 &= \left.\frac{V_1}{V_3}\right|_{V_4, I_3, I_4 = 0} \\ B_1 &= \left.\frac{V_1}{I_3}\right|_{\dots} \\ C_1 &= \left.\frac{I_1}{V_3}\right|_{\dots} \\ D_1 &= \left.\frac{I_1}{I_3}\right|_{\dots} \end{aligned}$$

$$\begin{aligned} A_3 &= \left.\frac{V_2}{V_3}\right|_{\dots} \approx A_2 \\ B_3 &= \left.\frac{V_2}{I_3}\right|_{\dots} \approx B_2 \\ C_3 &= \left.\frac{I_2}{V_3}\right|_{\dots} \approx C_2 \\ D_3 &= \left.\frac{I_2}{I_3}\right|_{\dots} \approx D_2 \end{aligned}$$

$$\xrightarrow{\text{“abcd2s”}} \mathbf{S}$$

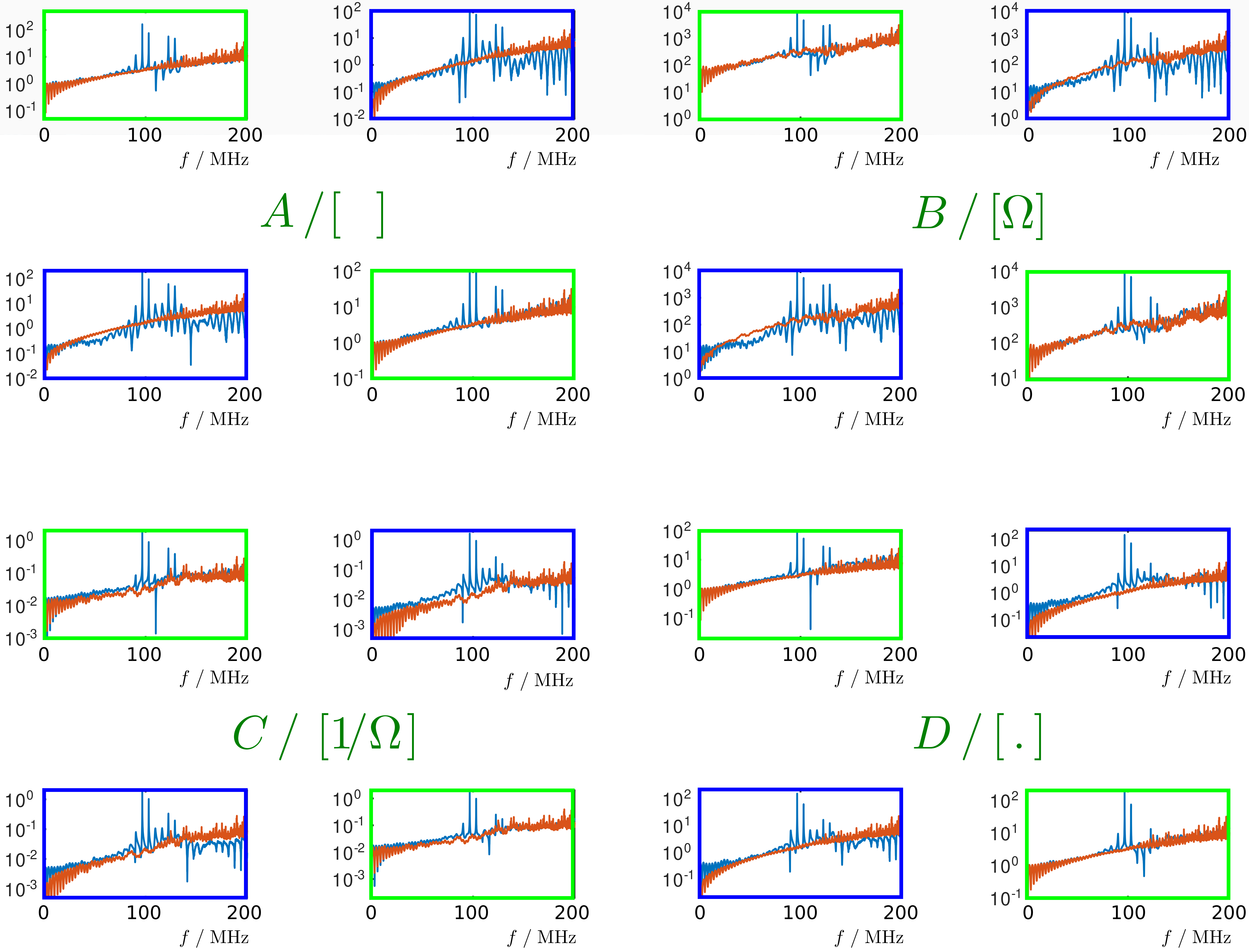
To recover reciprocity…

mirror lower triangle to upper tringle of **S** matrix, thereafter “s2abcd”

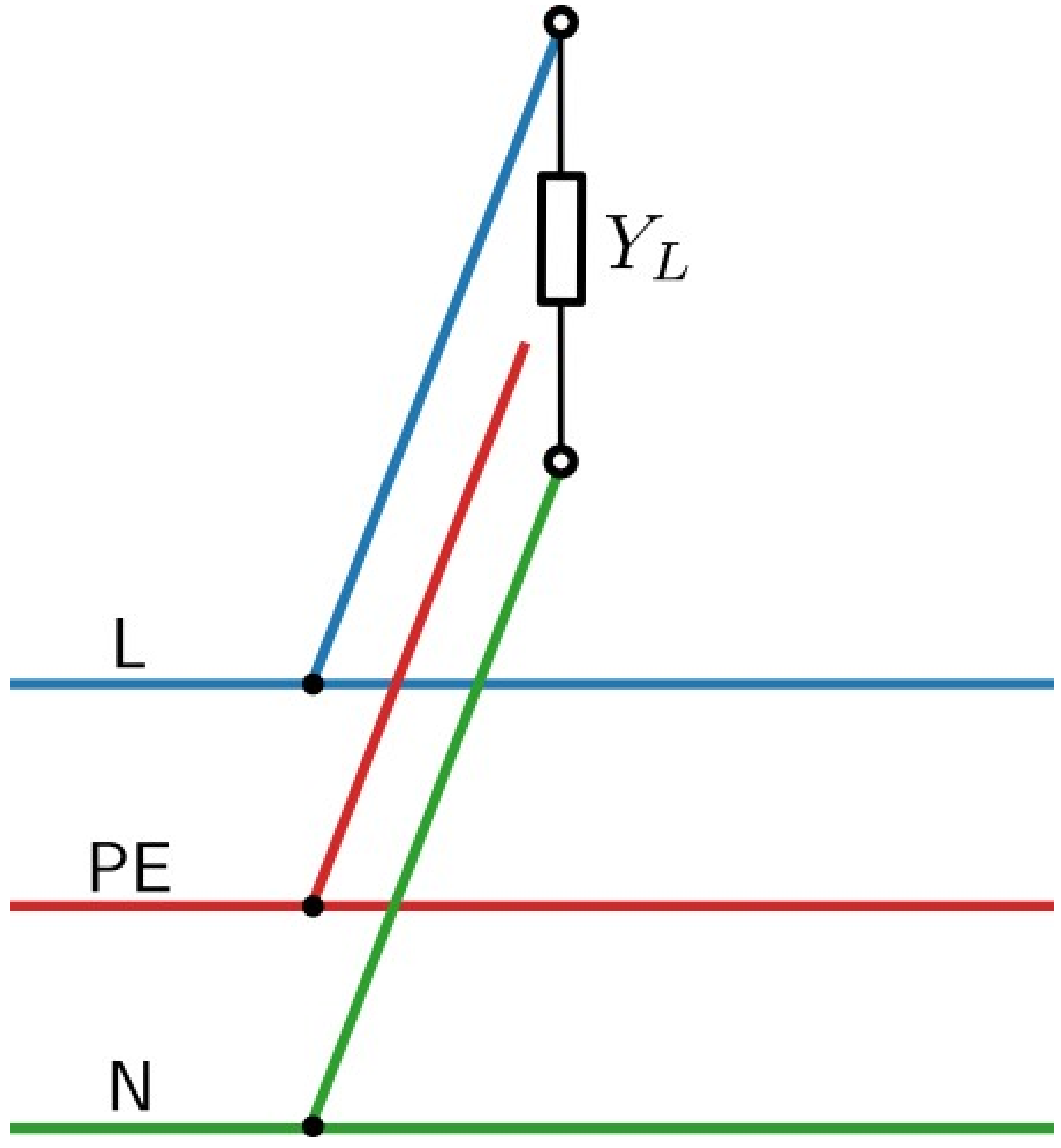
$$\begin{aligned} A_2 &= \left.\frac{V_1}{V_4}\right|_{\dots} \approx H_{\mathrm{mod}} \cdot A_4 \approx H_{\mathrm{mod}} \cdot A_1 \\ B_2 &= \left.\frac{V_1}{I_4}\right|_{\dots} \approx H_{\mathrm{mod}} \cdot B_4 \approx H_{\mathrm{mod}} \cdot B_1 \\ C_2 &= \left.\frac{I_1}{V_4}\right|_{\dots} \approx H_{\mathrm{mod}} \cdot C_4 \approx H_{\mathrm{mod}} \cdot C_1 \\ D_2 &= \left.\frac{I_1}{I_4}\right|_{\dots} \approx H_{\mathrm{mod}} \cdot D_4 \approx H_{\mathrm{mod}} \cdot D_1 \end{aligned}$$

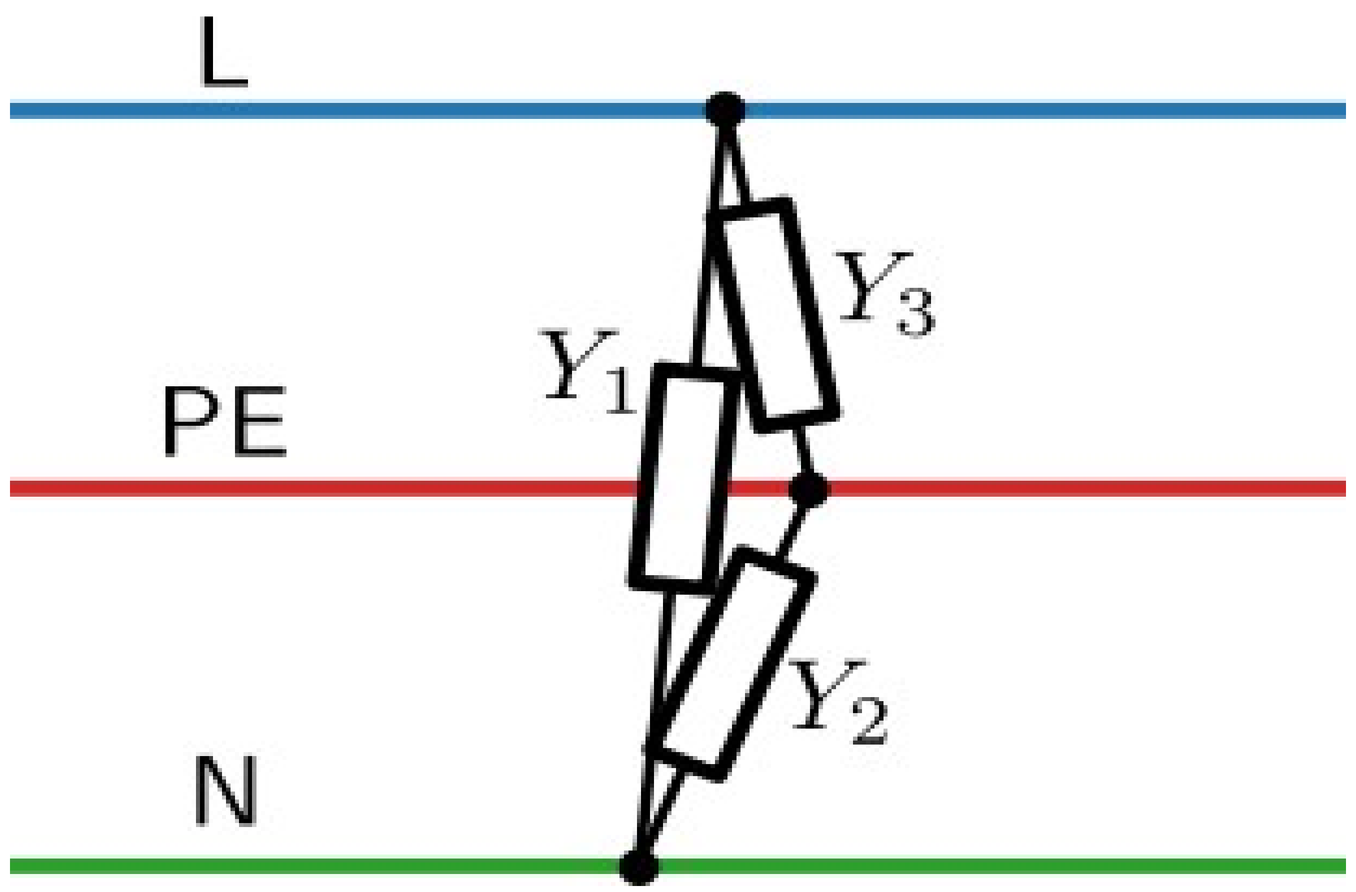
$$\begin{aligned} A_4 &= \left.\frac{V_2}{V_4}\right|_{\dots} \approx A_1 \\ B_4 &= \left.\frac{V_2}{I_4}\right|_{\dots} \approx B_1 \\ C_4 &= \left.\frac{I_2}{V_4}\right|_{\dots} \approx C_1 \\ D_4 &= \left.\frac{I_2}{I_4}\right|_{\dots} \approx D_1 \end{aligned}$$

Matrix model of a 3-wire transmission line



3-wire bridged tap





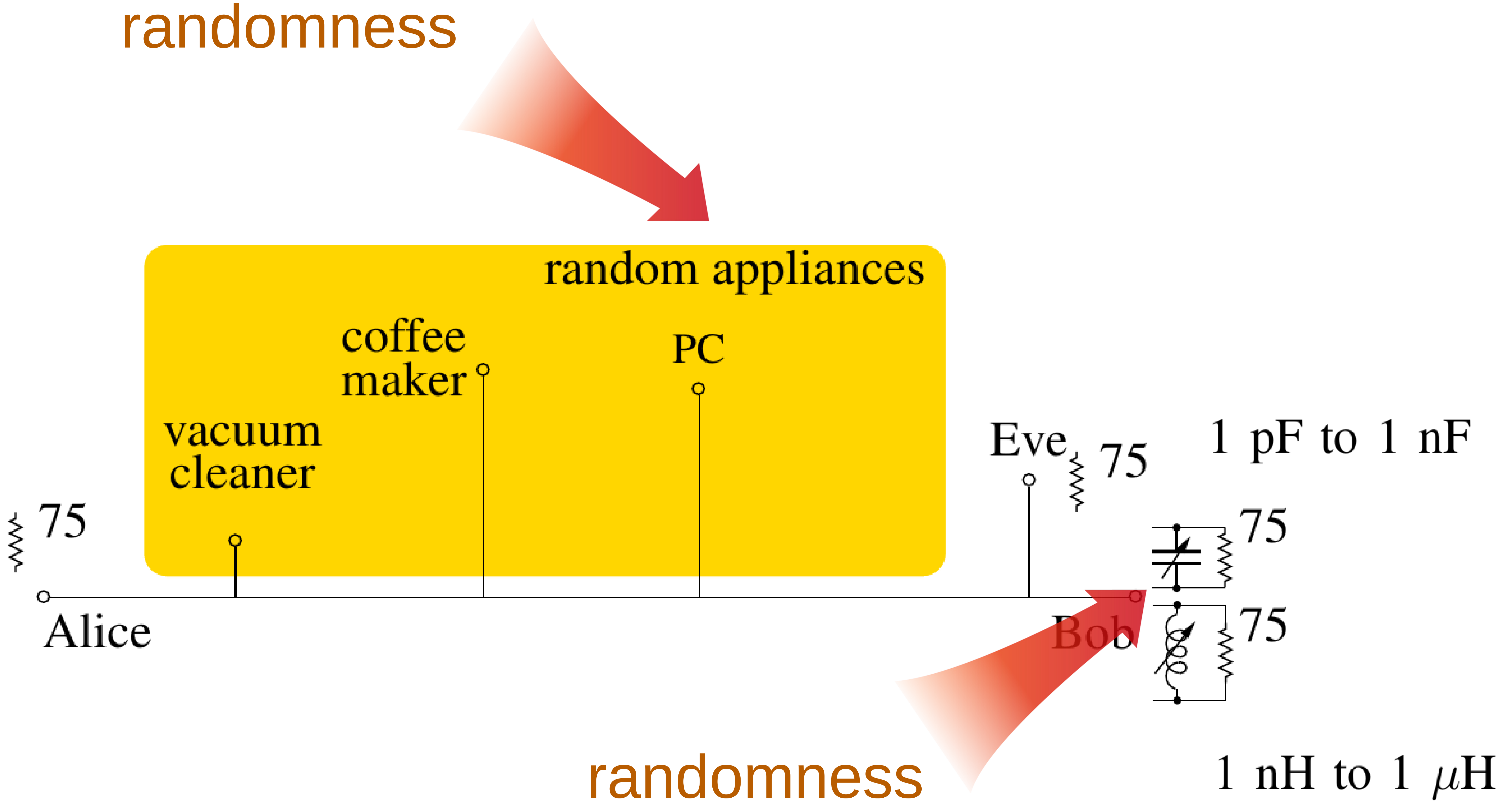
$$V_1 = A_1 V_3 + A_2 V_4 - B_1 Y_L V_3$$
$$I_1 = C_1 V_3 + C_2 V_4 - D_1 Y_L V_3$$
$$V_2 = A_3 V_3 + A_4 V_4 - B_3 Y_L V_3$$
$$I_2 = C_3 V_3 + C_4 V_4 - D_3 Y_L V_3$$

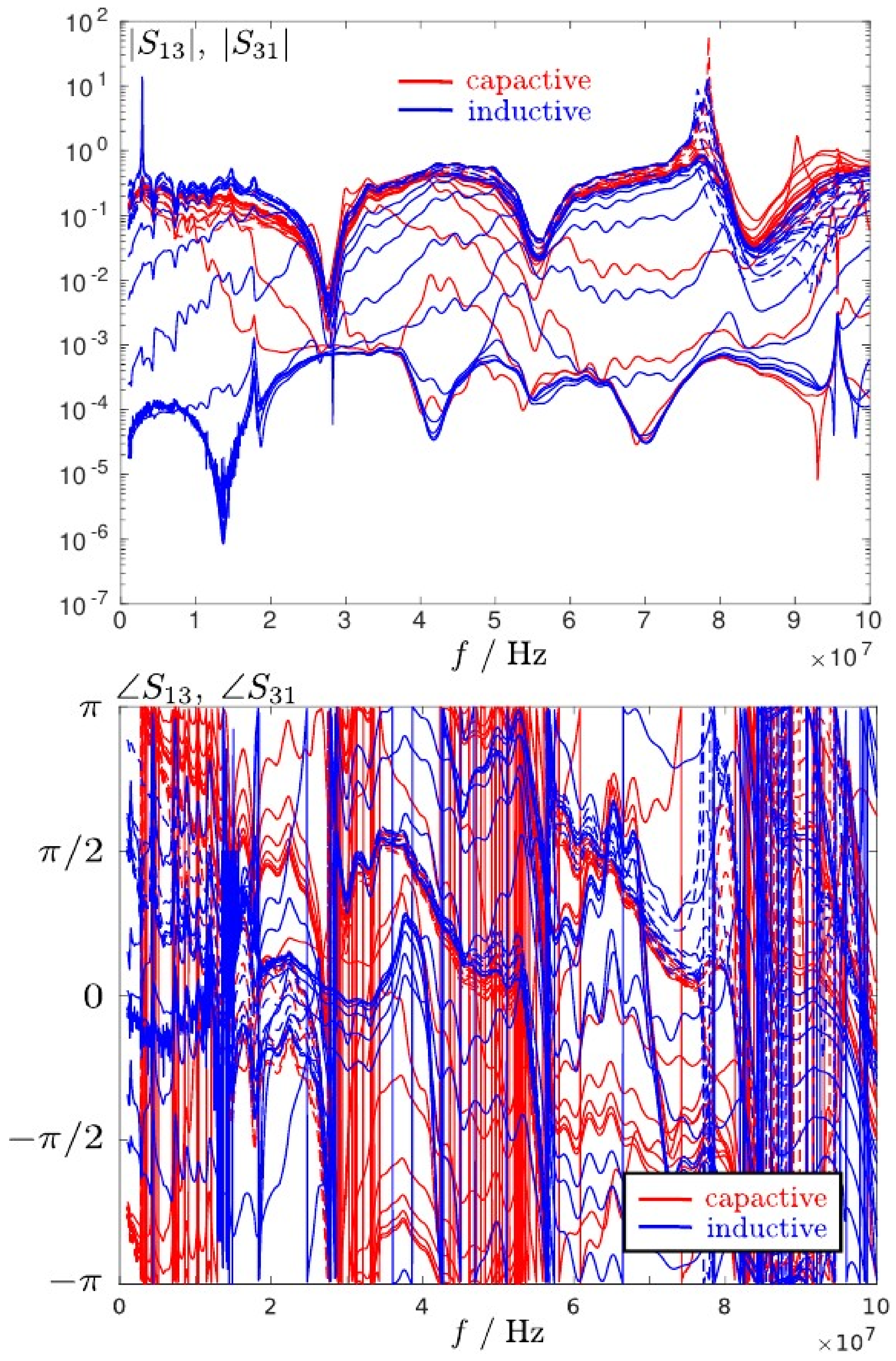
Δ-equivalent
of a bridged tap

$$\begin{bmatrix} V_1 \\ V_2 \\ V_3 \\ V_4 \end{bmatrix} = \frac{1}{Y_1 Y_2 + Y_2 Y_3 + Y_1 Y_3} \cdot \begin{bmatrix} Y_2 + Y_3 & Y_3 & Y_2 + Y_3 & Y_3 \\ Y_3 & Y_1 + Y_3 & Y_3 & Y_1 + Y_3 \\ Y_2 + Y_3 & Y_3 & Y_2 + Y_3 & Y_3 \\ Y_3 & Y_1 + Y_3 & Y_3 & Y_1 + Y_3 \end{bmatrix} \begin{bmatrix} I_1 \\ I_2 \\ I_3 \\ I_4 \end{bmatrix} \xrightarrow{\text{“z2abcd”}}$$

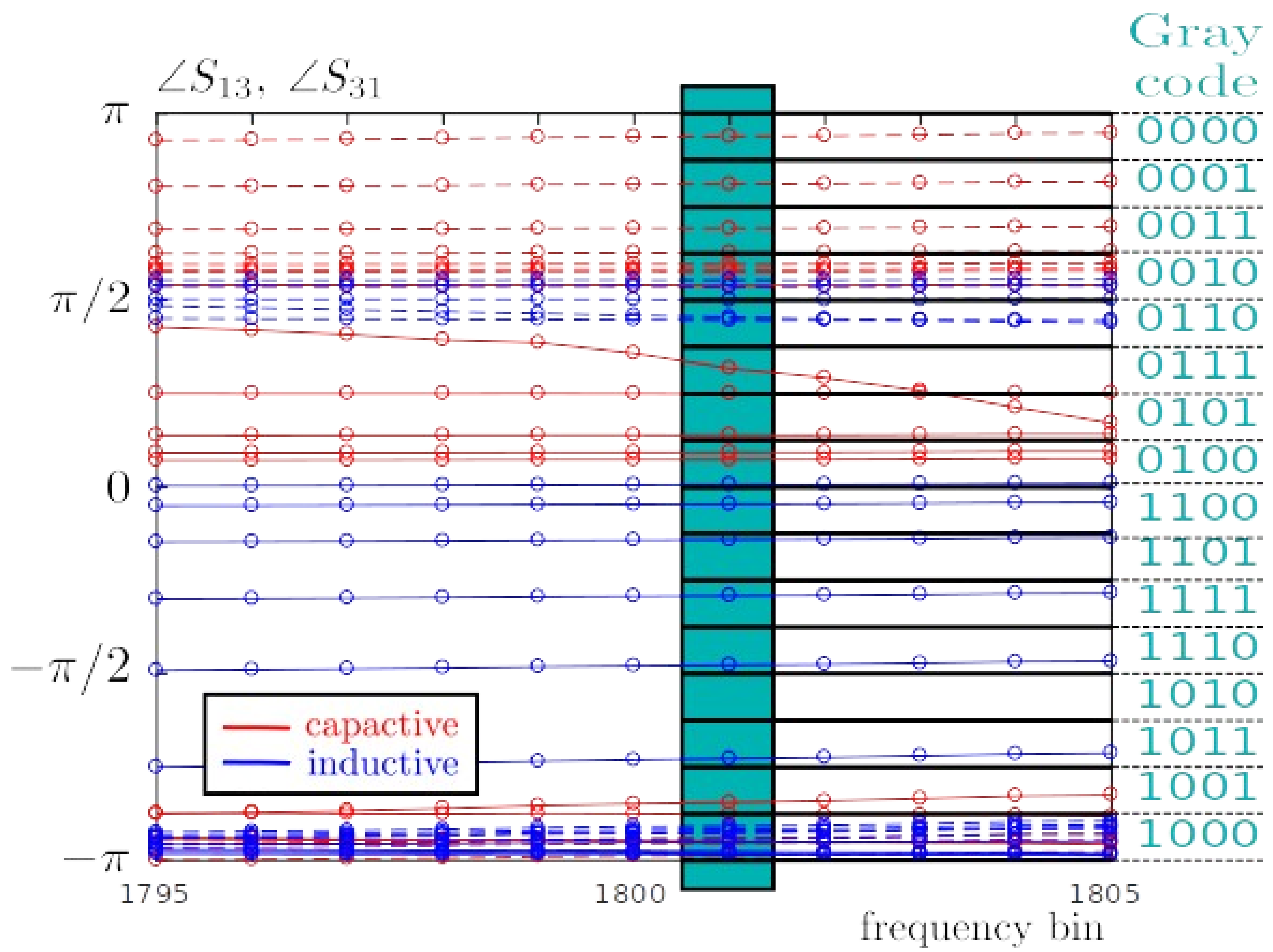
ABCD matrix
of
bridged tap

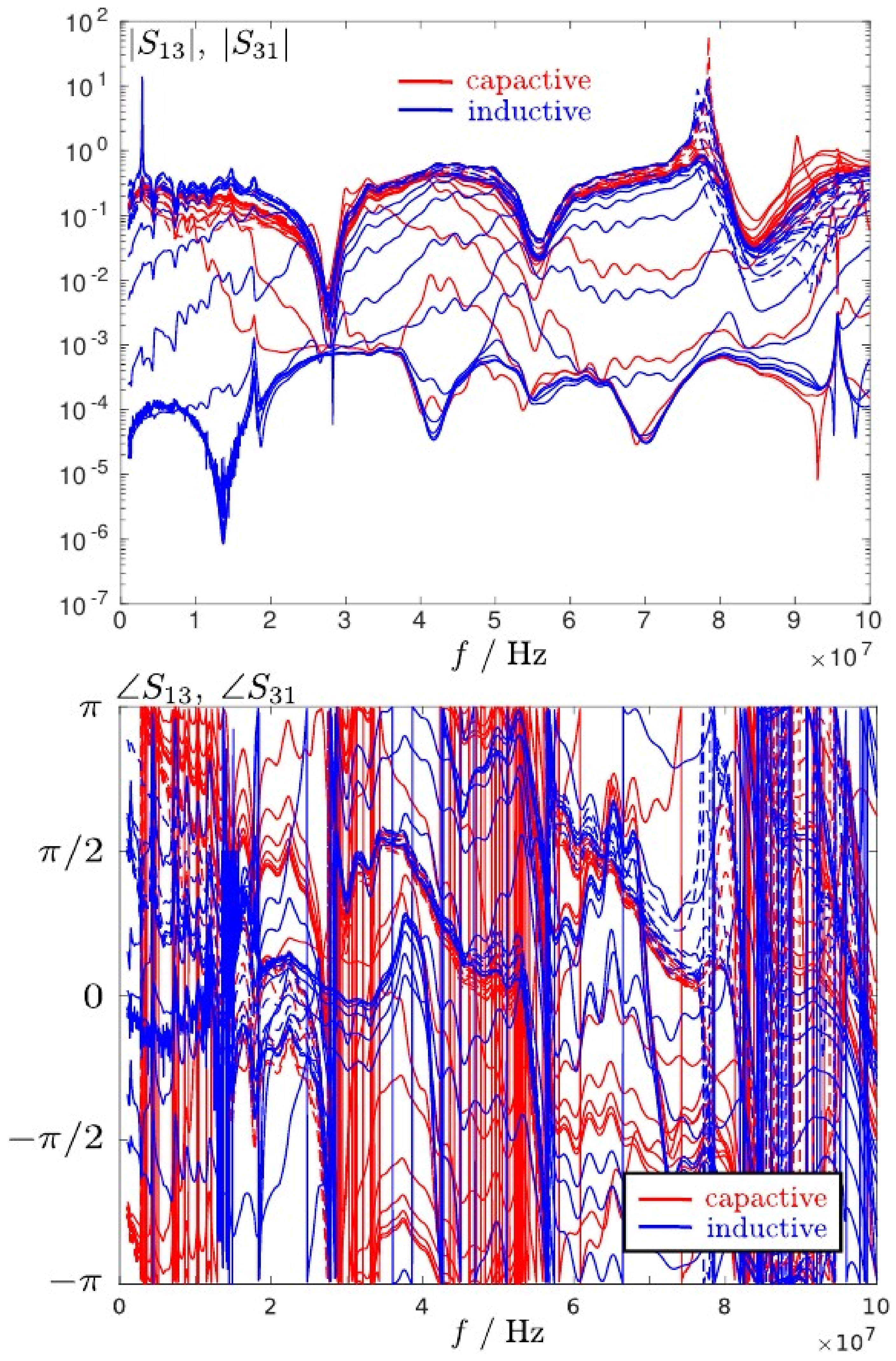
Key generation from phase (or amplitude) of the transfer factor / function





Key generation from phase (or amplitude) of the transfer factor / function





Linear phase quantization

$$\mathrm{Q}(\phi_{\mathrm{A}}) = \mathcal{Q}_{\mathrm{A}}$$

$$\text{if} \quad \bmod\,(\phi_{\mathrm{A}}, 2\pi) \in \left[\frac{2\pi(\mathcal{Q}_{\mathrm{A}}-1)}{2^M}, \frac{2\pi\ \mathcal{Q}_{\mathrm{A}}}{2^M}\right)$$

Performance with randomized one-sided centering

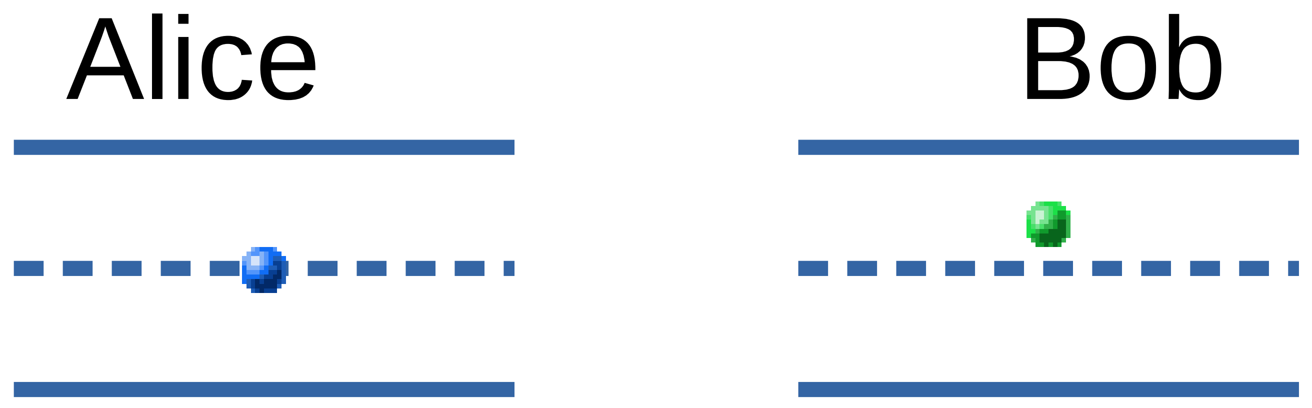
Linear phase quantization

$$\mathrm{Q}(\phi_\mathrm{A}) = \mathcal{Q}_\mathrm{A}$$

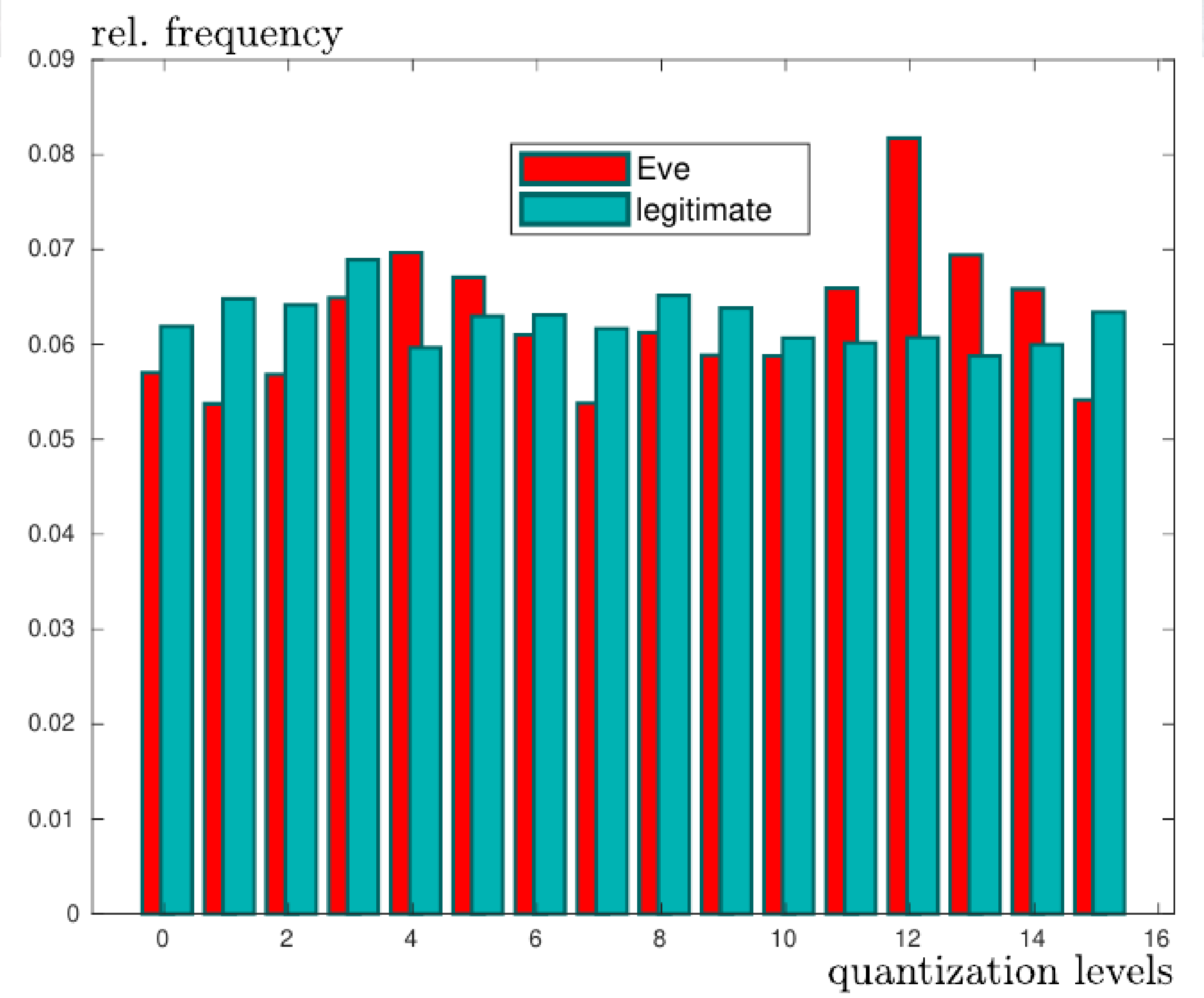
$$\text{if} \quad \bmod\ (\phi_\mathrm{A}, 2\pi) \in \left[\frac{2\pi(\mathcal{Q}_\mathrm{A}-1)}{2^M}\, ,\ \frac{2\pi\ \mathcal{Q}_\mathrm{A}}{2^M}\right)$$

One-side centering as analog key reconciliation

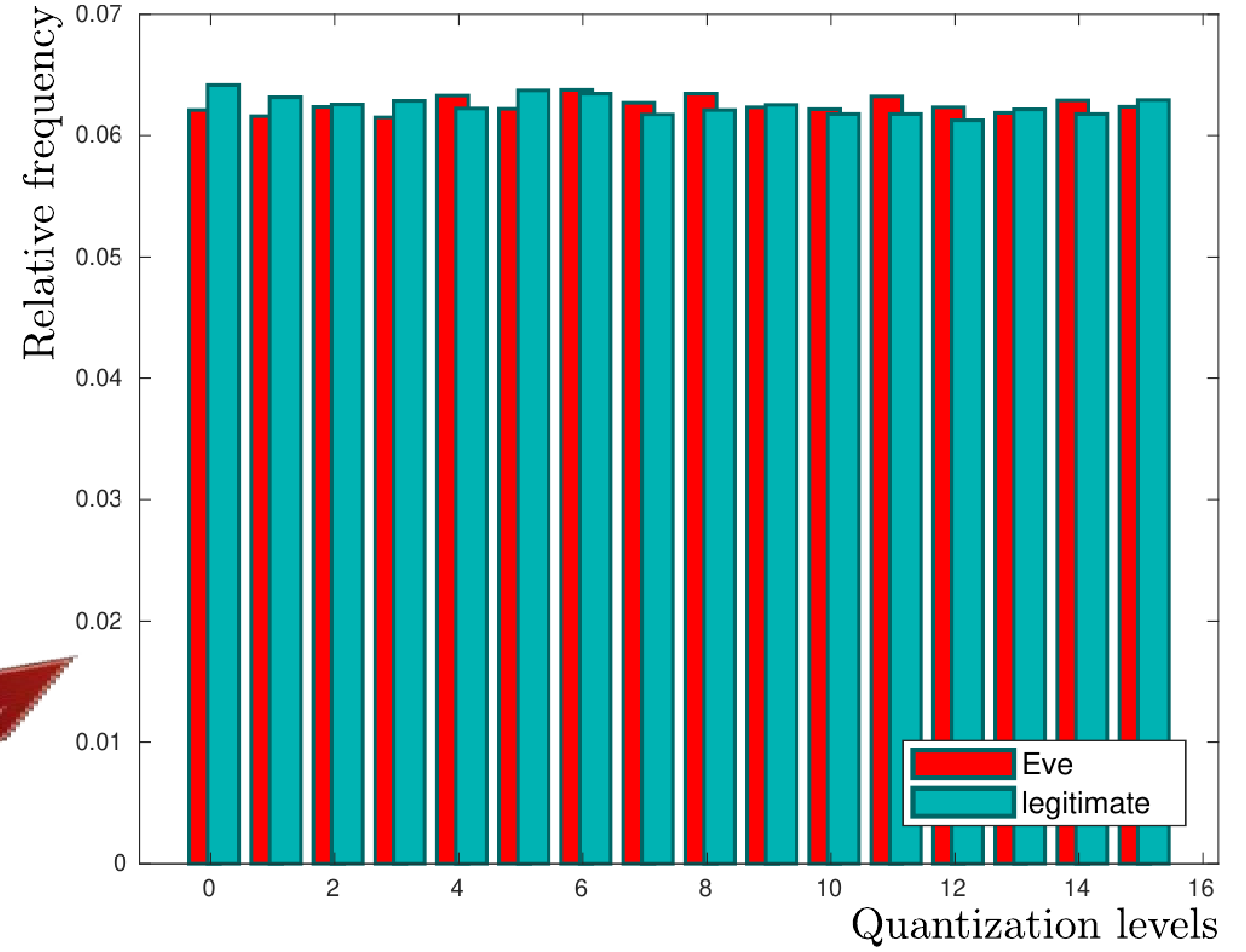
Shift: $S_\mathrm{A} = \phi_\mathrm{A} - \dfrac{\pi(2\mathcal{Q}_\mathrm{A}-1)}{2^M}$



Data update: $\phi_\mathrm{A} := \phi_\mathrm{A} - S_\mathrm{A}\ ,\ \phi_\mathrm{B} := \phi_\mathrm{B} - S_\mathrm{A}$



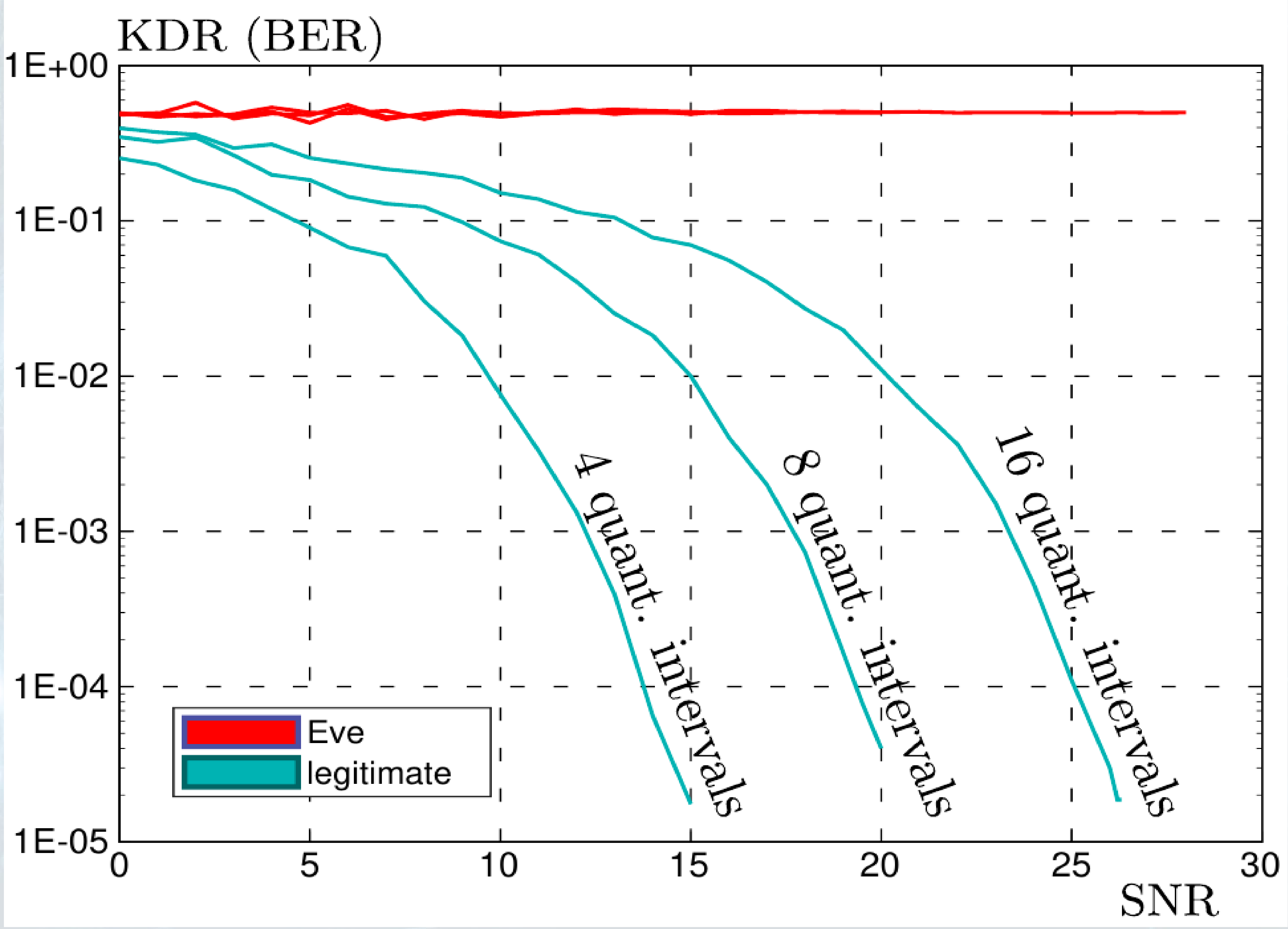
With randomization



To finalize...
some more performance results

Bit-wise Key Disagreement Rate

$$\mathrm{KDR} = \frac{1}{N_T} \sum_{N_T} \frac{1}{M} \sum_{i=1}^{M} |\mathbf{K}_A(i) - \mathbf{K}_B(i)|$$



NIST STATISTICAL TEST RESULTS

Test	p-value
Bits read	400000
Zeros	200520
Ones	199480
Approximate Entropy	0.866468
Frequency (Monobit)	0.100097
Block frequency	0.916856
Cumulative sums (forward)	0.127738
Cumulative sums (reverse)	0.137551
Discrete Fourier Transform	0.051862
Linear complexity	0.086973
Longest Run	0.883510
Overlapping template	0.836970
Rank	0.604315
Runs	0.700469
Serial	0.936740 0.582493
Universal	0.135751

Sequence considered random with 99 % confidence, if the corresponding p-values exceed 0.01

See
ISNCC 25
and more under
http://trsys-wh.de

ISPLC 21