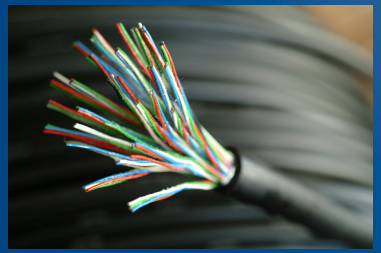
JACOBS UNIVERSITY

Wireline Physical-Layer Key Generation

Werner Henkel, Oana Graur,
and Uwe Pagel

WSPLC workshop, Prague, 2017



Perfect secrecy and the wiretap channel

Shannon‘s perfect secrecy:

$$H(M|C) = H(M) \text{ or equivalently } I(M;C) = 0$$

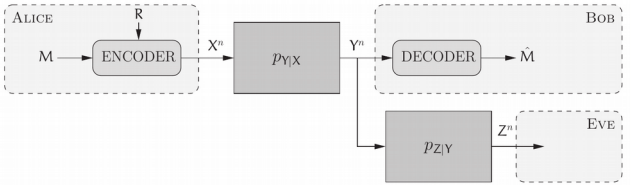
Strong and weak secrecy:

$$\lim_{N\to\infty} I(\mathbf{M};\mathbf{C}) = 0 \text{ and } \lim_{N\to\infty} \frac{1}{N} I(\mathbf{M};\mathbf{C}) = 0$$

Secrecy capacity for Wyner‘s wiretap channel:

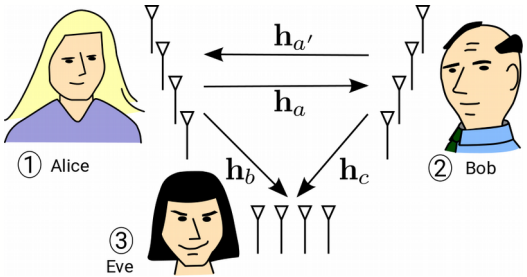
$$C_s = \max_{P_x} [I(X;Y) - I(X;Z)]$$

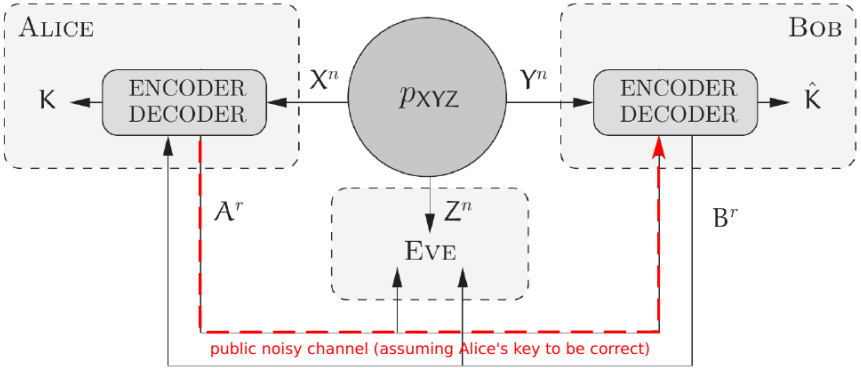
M. Bloch and J. Barros, Physical-Layer Security: From Information Theory to Security Engineering. Cambridge University Press, 2011.



JACOBS UNIVERSITY

Physical layer key generation





M. Bloch and J. Barros, Physical-Layer Security: From Information Theory to Security Engineering. Cambridge University Press, 2011.

Secret key capacity

$$I(X;Y) - \min\{I(X;Z), I(Y;Z)\} \leq C_s \leq \min\{I(X;Y), I(X;Y|Z)\}$$

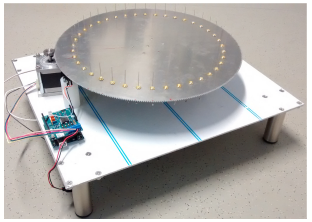
Typical scenario:

Wireless TDD (time-division duplexing) providing common randomness through channel reciprocity (apart from hardware deficiencies and uncorrelated noise asking for key reconcilation schemes)

Physical layer key generation

Other options?

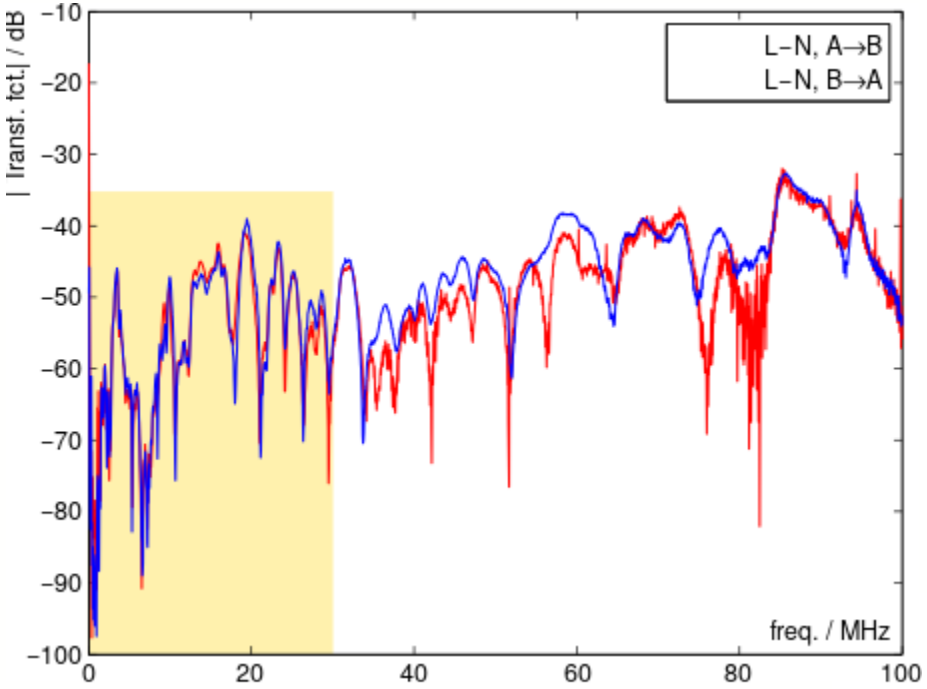
How about Wireless FDD (frequency division duplexing)
– possibly solution through DoA estimates



How about Power Lines
and Twisted Pairs ?

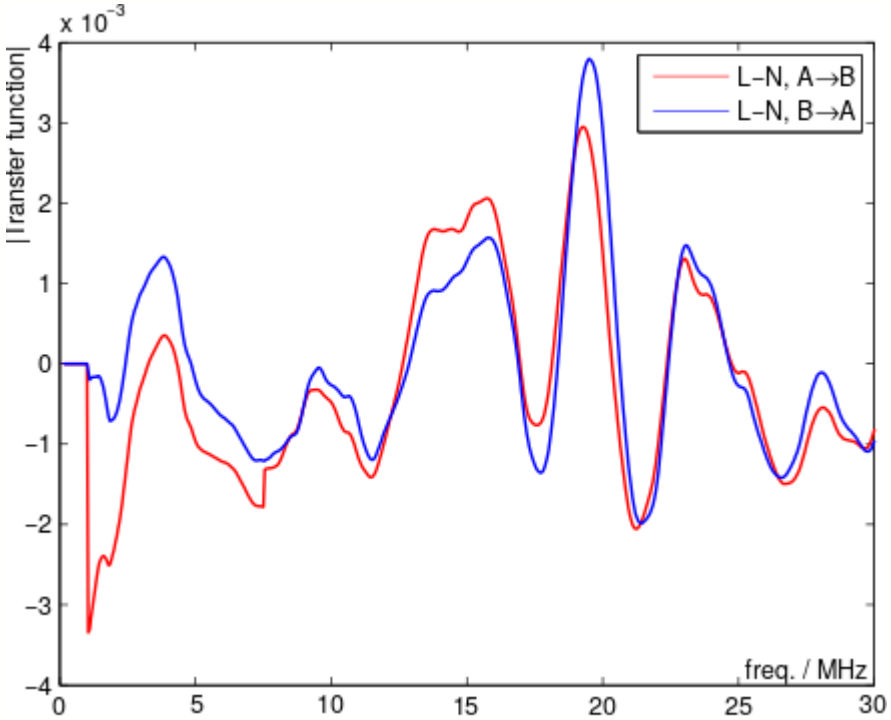
Transfer function between
power outlets ?

Usable range with decent
reciprocity property
seems to be up to ~30 MHz



Physical layer key generation with a power line transfer function

The 30 MHz range after calibration, smoothing, and leveling

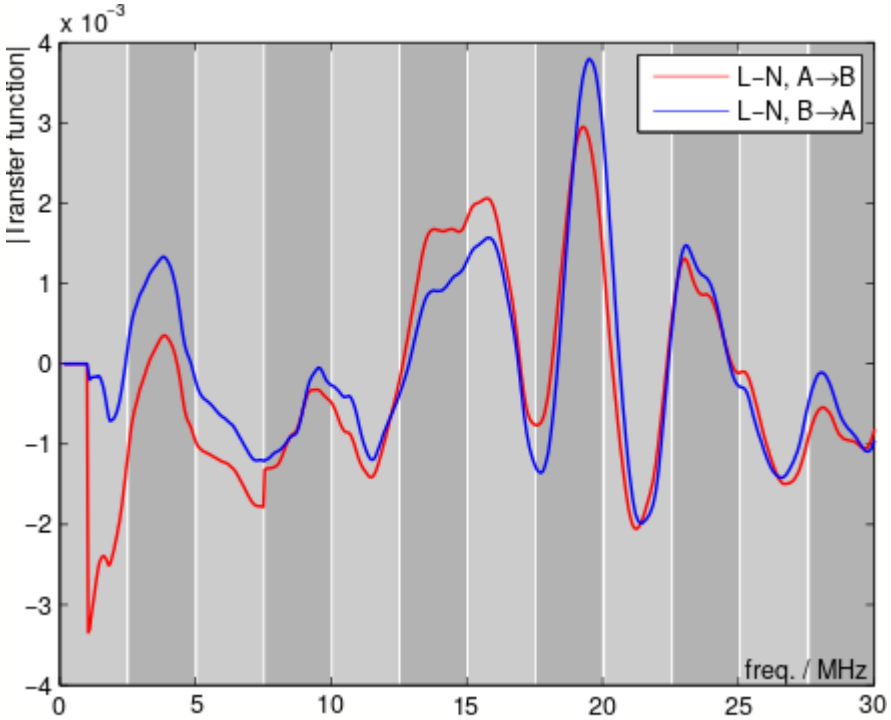


JACOBS UNIVERSITY

Physical layer key generation with a power line transfer function

The 30 MHz range after calibration, smoothing, and leveling

Quantization of the frequency range to localize local maxima

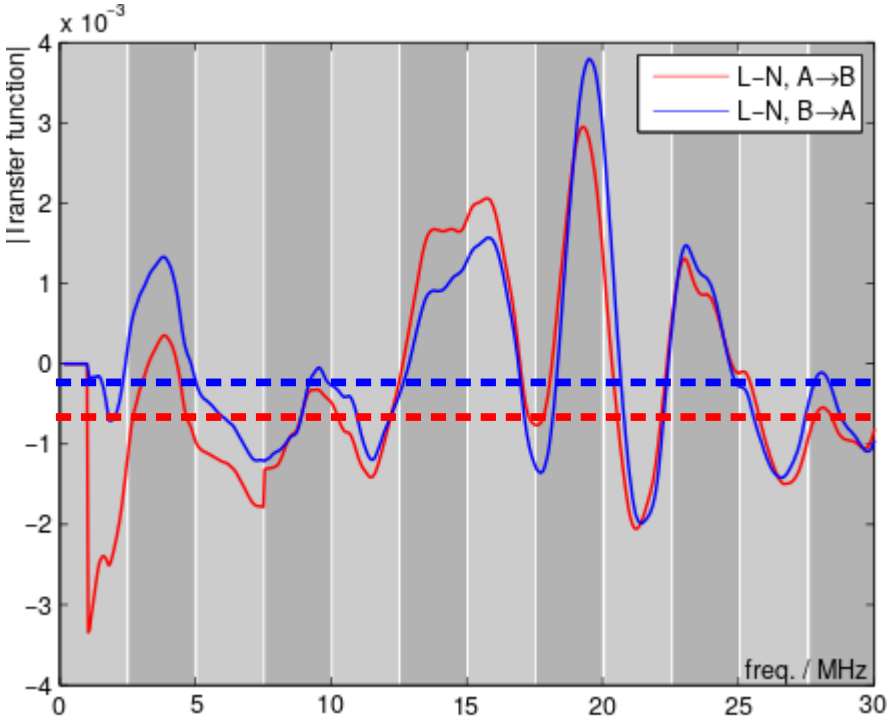


JACOBS UNIVERSITY

Physical layer key generation with a power line transfer function

The 30 MHz range after calibration, smoothing, and leveling

Introduce thresholds ensuring an identical number of local maxima



JACOBS UNIVERSITY

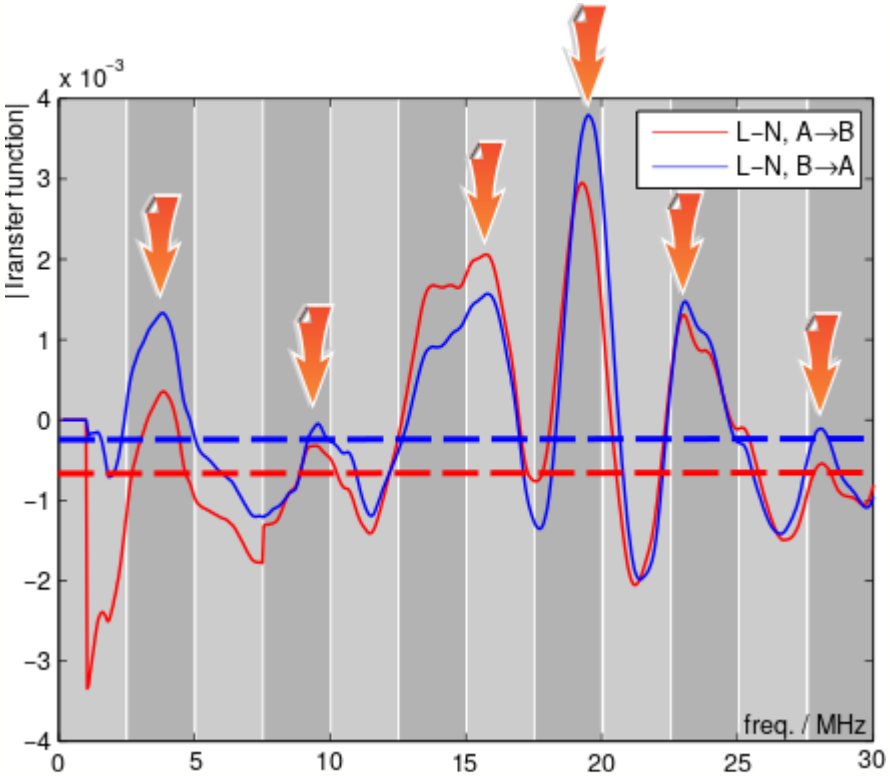
Physical layer key generation with a power line transfer function

The 30 MHz range after calibration, smoothing, and leveling

Mark the maxima and use a translation table of maxima locations to key patterns

List length in the example

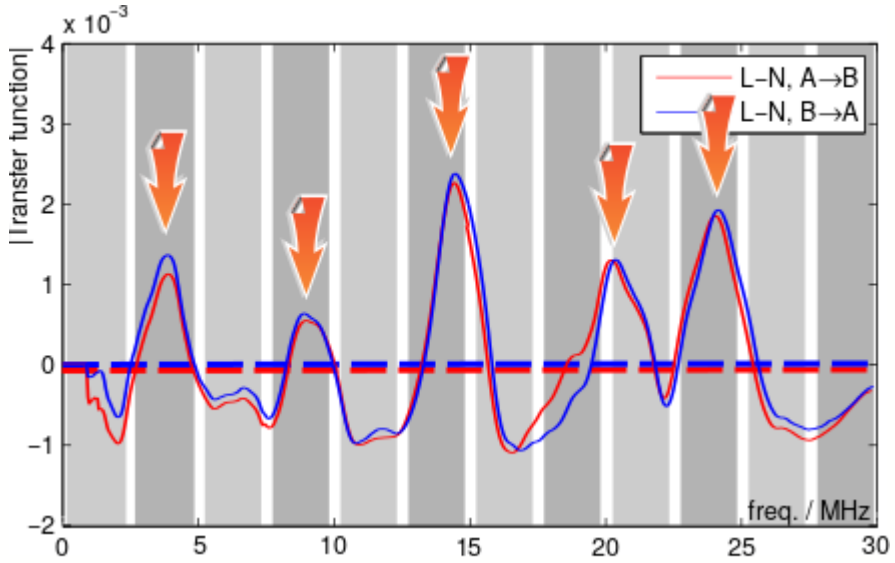
$$\binom{n}{e} = \binom{12}{6}$$



JACOBS UNIVERSITY

Physical layer key generation with a power line transfer function

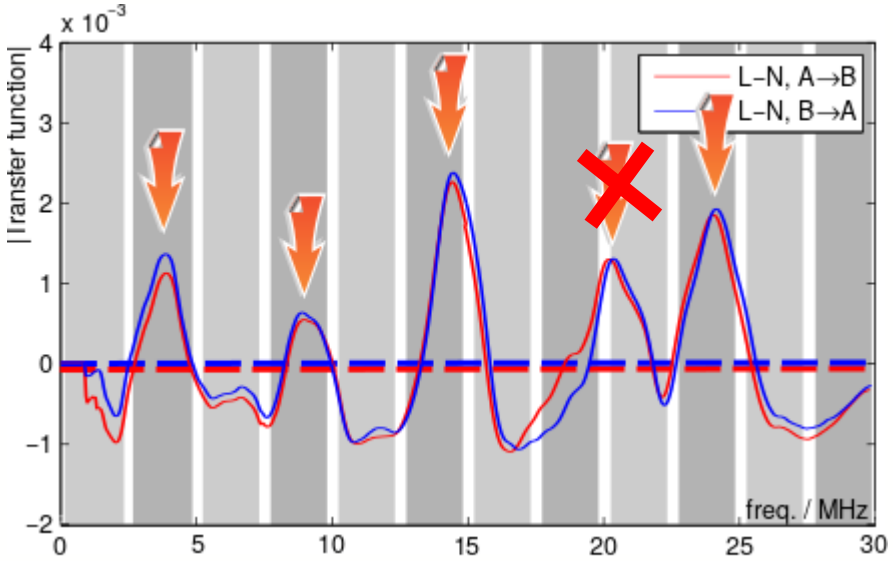
Key reconciliation with guard bands



JACOBS UNIVERSITY

Physical layer key generation with a power line transfer function

Key reconciliation with guard bands



If local maxima end up in a guard band, irrespective of at Alice‘s or Bob‘s side, that maximum will not be considered for key generation.

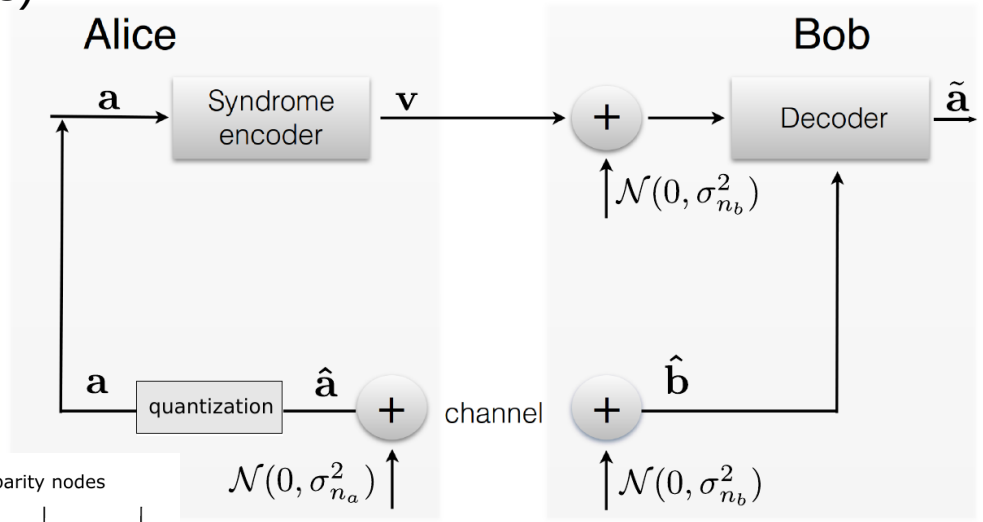
JACOBS UNIVERSITY

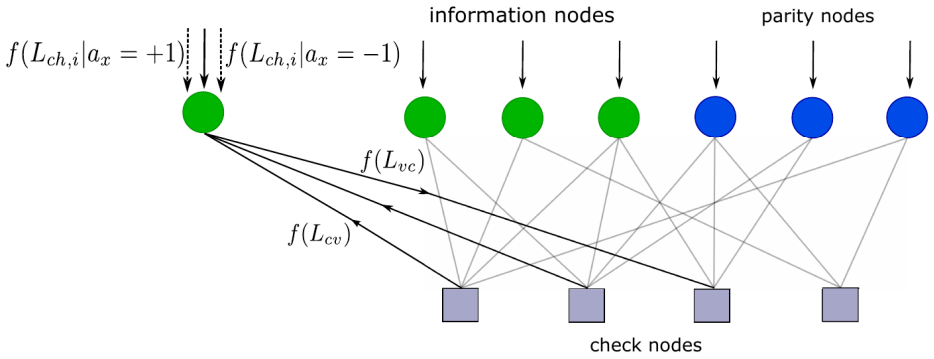
Physical layer key generation with a power line transfer function

Key reconciliation with Slepian-Wolf coding
(to be combined with guard intervals)

Slepian-Wolf bound:

$$M_p \geq H(\mathbf{a}|\hat{\mathbf{b}})$$



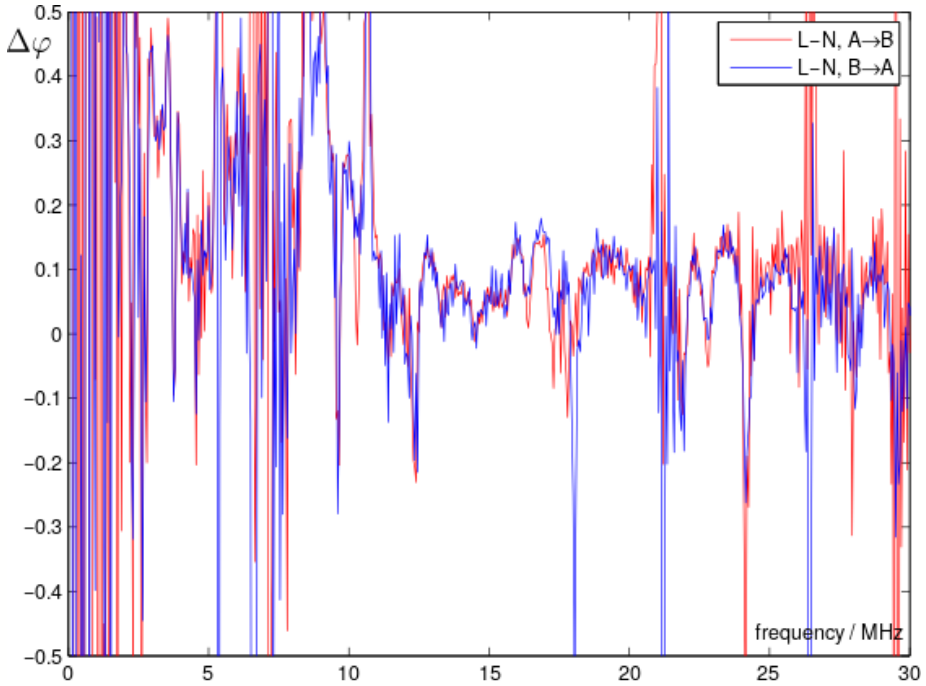


JACOBS UNIVERSITY

Physical layer key generation with a power line transfer function

How about phase properties – are they reciprocal, too?

We show the phase differences between neighboring frequency samples, i.e., similar to the group-delay.



Some reciprocity, but less usable for key generation purposes.

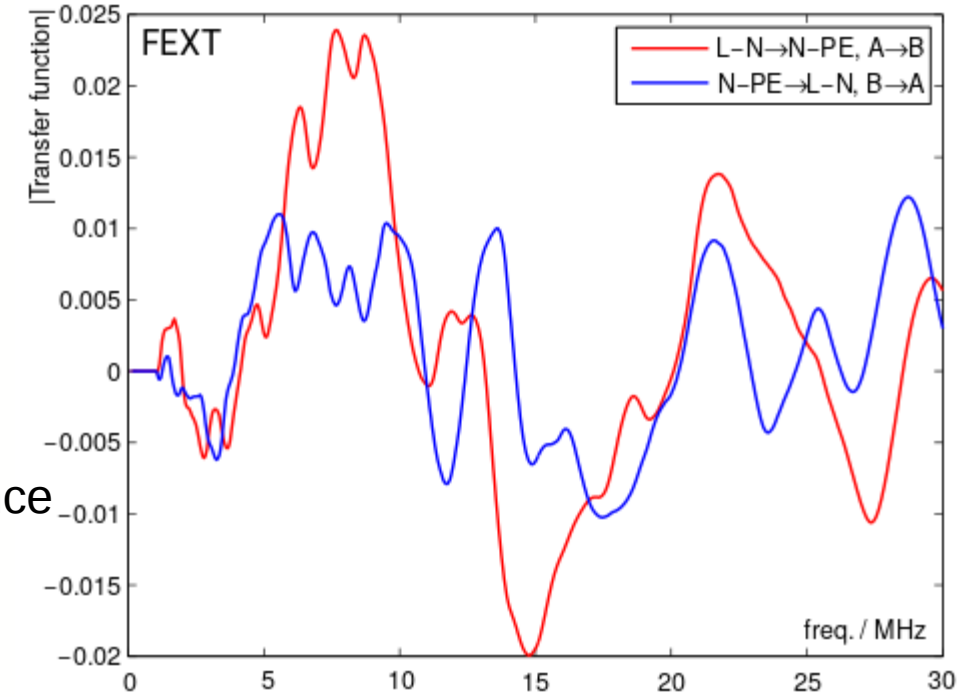
JACOBS UNIVERSITY

Physical layer key generation with a power line transfer function

How about FEXT functions – are they reciprocal?

Mostly not!

Reason: effect of bridge taps to other appliances, switches, sockets, ... obviously stronger influence on FEXT than on the transfer function.



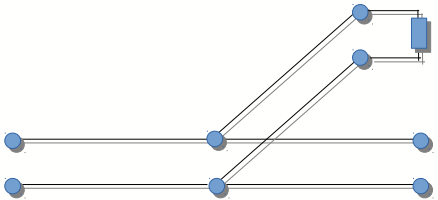
Physical layer key generation with a power line transfer function

Reciprocal … but need

common randomness!

How to make a more or less deterministic powerline connection random?

- Switched appliances change terminations, but only occasionally.
- One might add bridge taps (with random terminations) artificially.

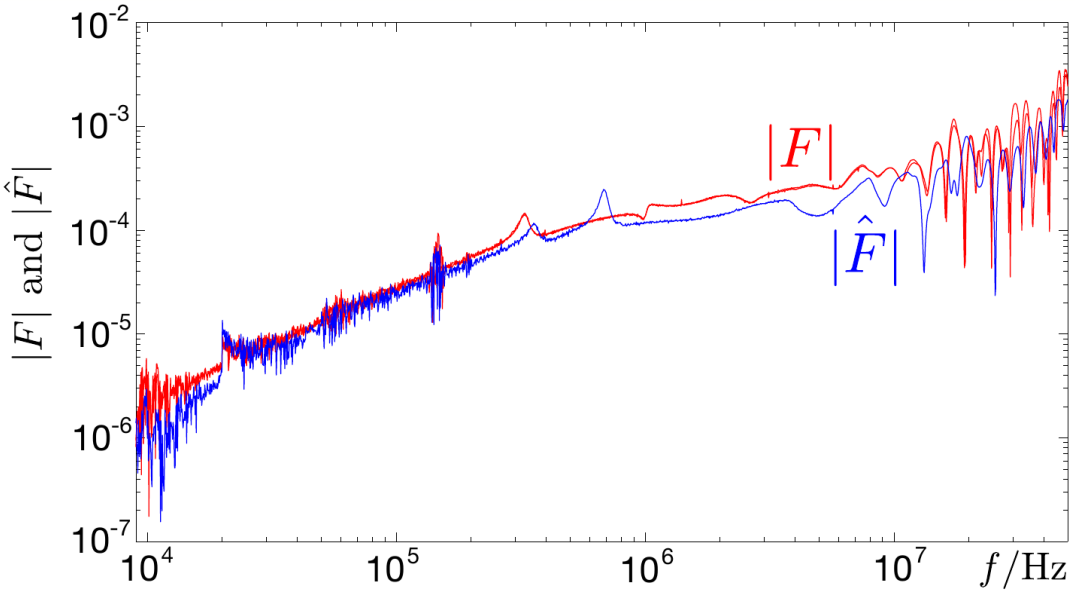


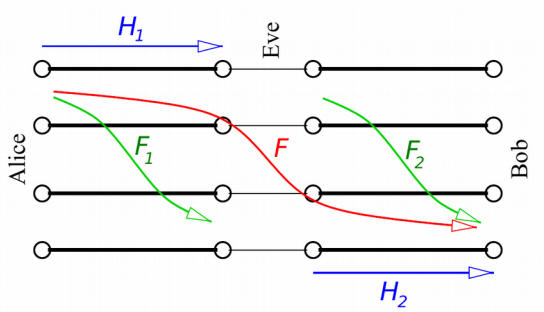
JACOBS UNIVERSITY

Physical layer key generation for a single loop, e.g., Ethernet

Using the FEXT function with its known randomness across frequency

$$F \approx \hat{F} = F_1 \cdot H_2 + H_1 \cdot F_2$$

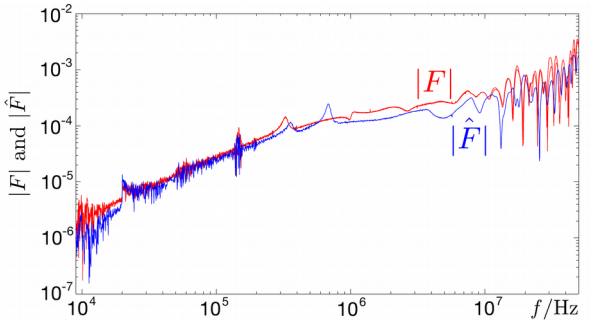




Randomization of FEXT by random coupling to other pairs or to the shield.

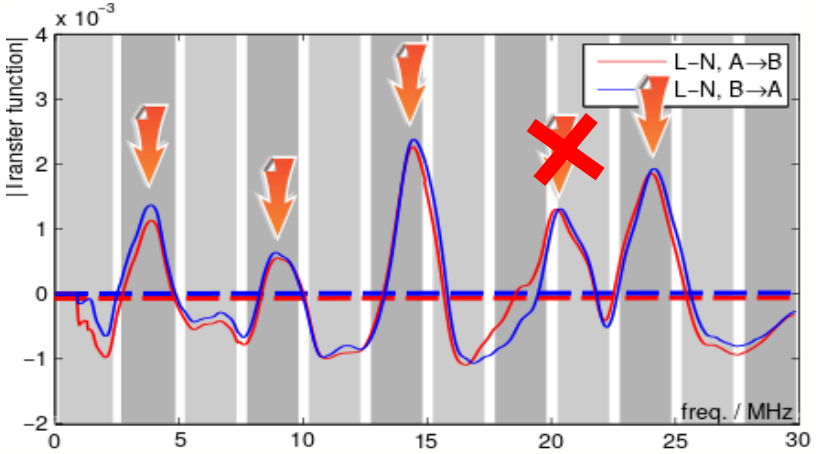
JACOBS UNIVERSITY

To summarize...



Reciprocity is given also in power line and Ethernet connections, be it in the transfer or FEXT functions, respectively.

Powerline modems determine the transfer function, anyhow, hence, key information is readily available.



JACOBS UNIVERSITY