Enhanced PHY Layer Security through Frequency and Spatial Diversity

Idowu Ajayi

Laboratoire d'Informatique, Signal et Image, Électronique et Télécommunications (LISITE)
Institut Supérieur d'Électronique de Paris (ISEP)

idowu.ajayi@isep.fr

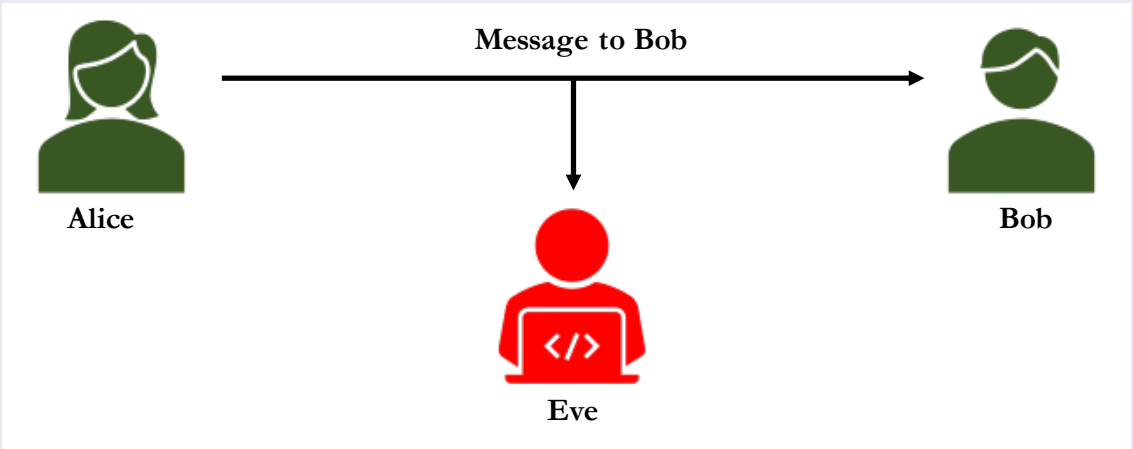
30-11-2022

Outline

Thesis Context

Physical Layer Security (PLS)

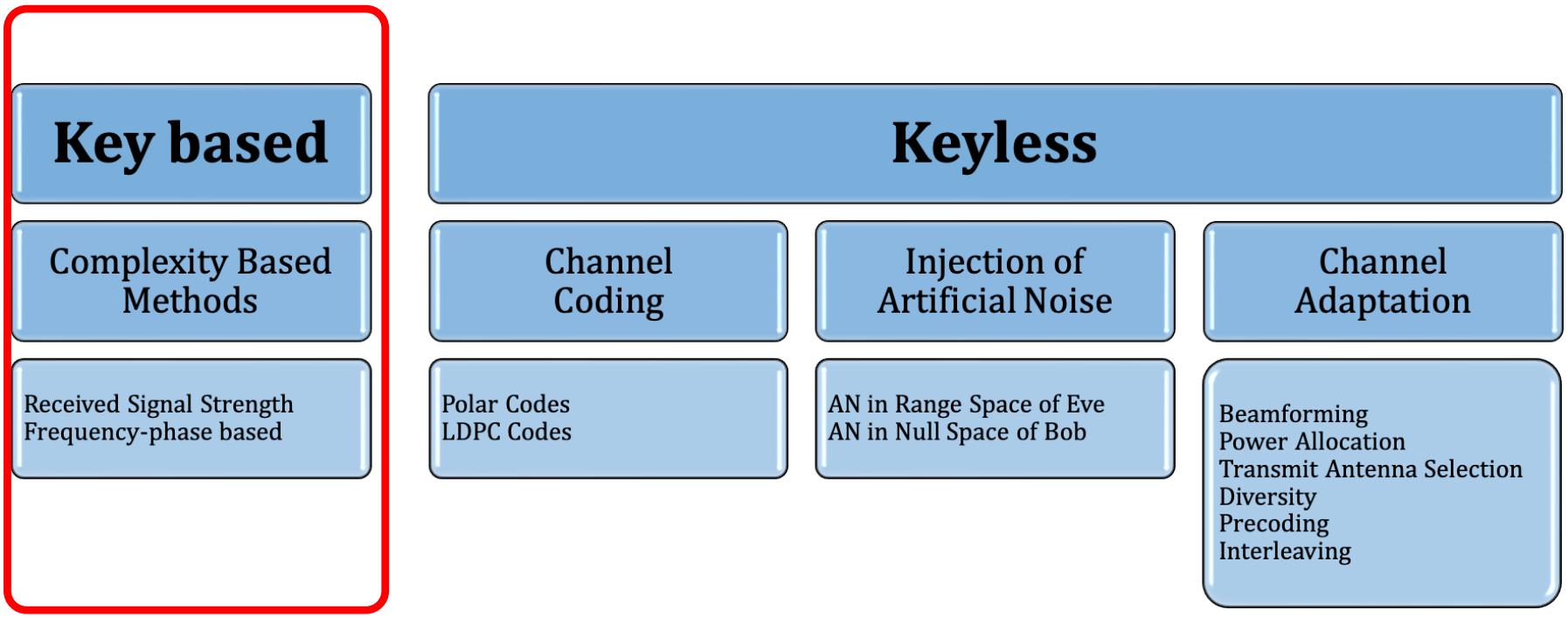
Wiretap Channel Model



PLS Advantages

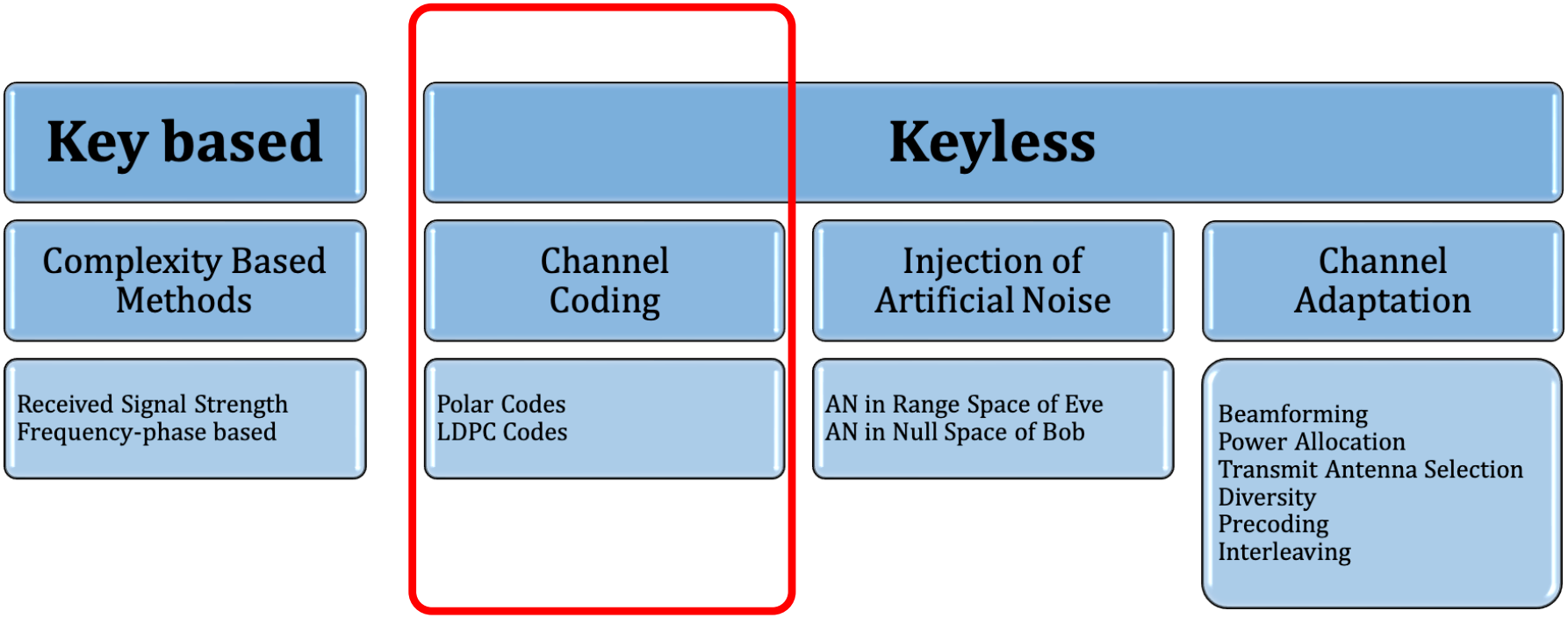
Wireless channel's imperfections, such as noise and fading, become a source of security.
Low computational complexity, low resource requirement and quantum secure.
Eve listens to the legitimate users' communication.
Eve can be passive or active.
Wiretap channel model.

PLS Approaches



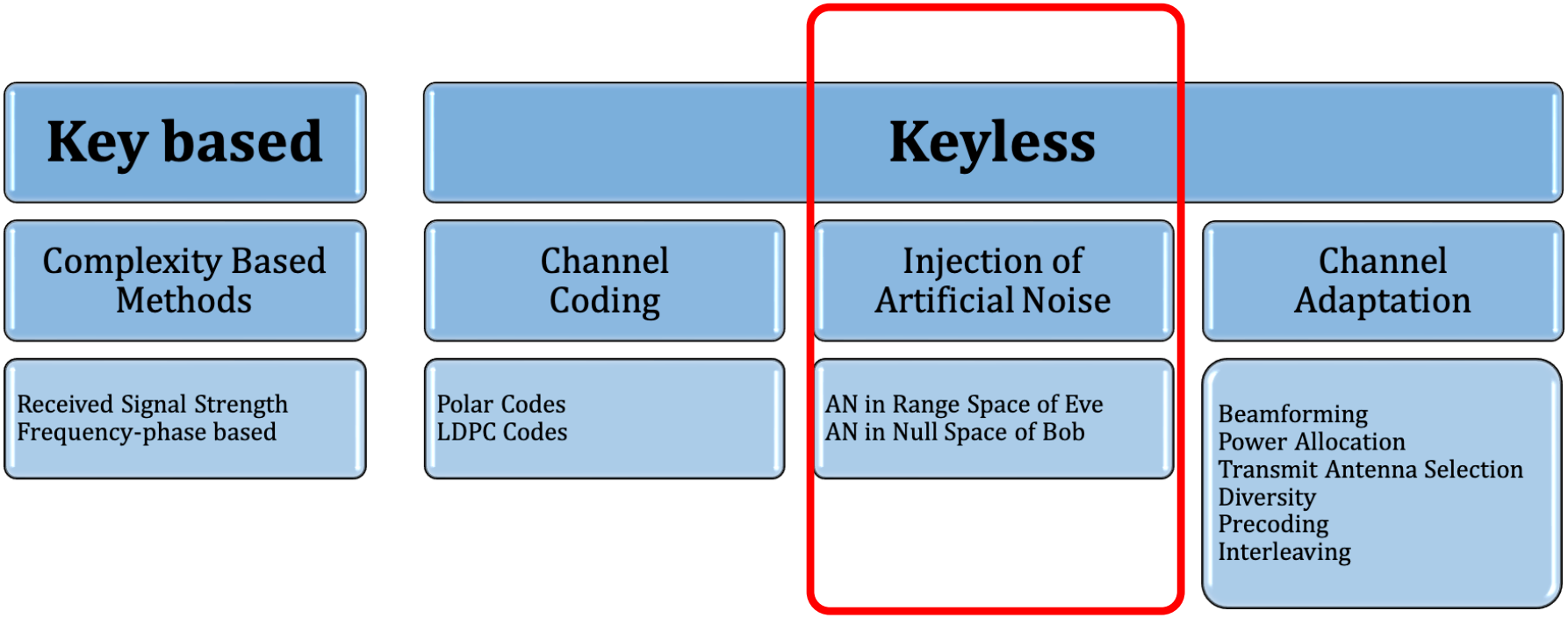
All approaches have been worked on during this thesis

PLS Approaches



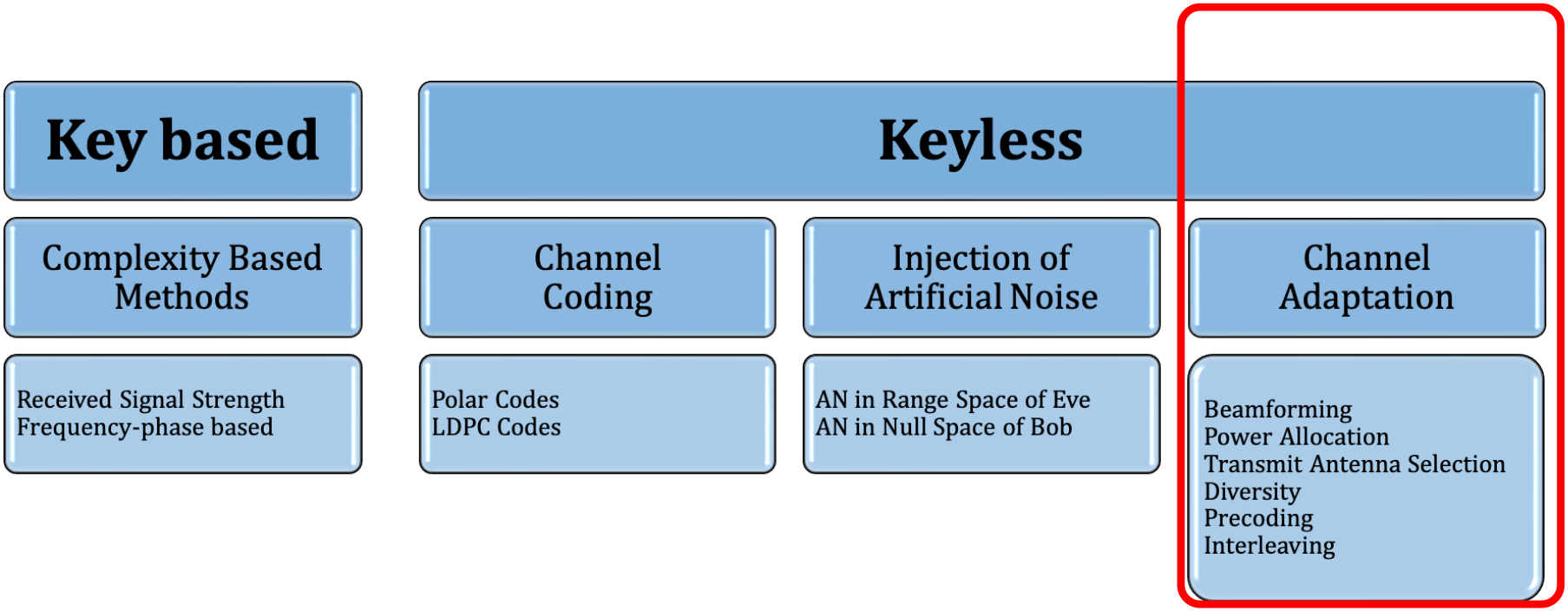
All approaches have been worked on during this thesis

PLS Approaches



All approaches have been worked on during this thesis

PLS Approaches



All approaches have been worked on during this thesis

Technical & Technological Limitations

Technical & Technological Limitations

Assumption of perfect knowledge of radio link at Alice.

Technical & Technological Limitations

Assumption of perfect knowledge of radio link at Alice.

Channel information not available to Eve in time division duplex (TDD).

Technical & Technological Limitations

Assumption of perfect knowledge of radio link at Alice.

Channel information not available to Eve in time division duplex (TDD).

Main channel coding technique is unknown at the eavesdropper.

Technical & Technological Limitations

Assumption of perfect knowledge of radio link at Alice.

Channel information not available to Eve in time division duplex (TDD).

Main channel coding technique is unknown at the eavesdropper.

The main channel is better than the wiretap channel.

Technical & Technological Limitations

Assumption of perfect knowledge of radio link at Alice.

Channel information not available to Eve in time division duplex (TDD).

Main channel coding technique is unknown at the eavesdropper.

The main channel is better than the wiretap channel.

Artificial Injection (AI) for PLS scheme without energy efficiency consideration.

Thesis Motivation

Questions to be answered by our research?

1. How to design a secure transmission strategy in a frequency division duplex (FDD) system?

Questions to be answered by our research?

1. How to design a secure transmission strategy in a frequency division duplex (FDD) system?

2. What is the impact of imperfect channel state information (CSI) at the receiver on the security capability?

Questions to be answered by our research?

1. How to design a secure transmission strategy in a frequency division duplex (FDD) system?

2. What is the impact of imperfect channel state information (CSI) at the receiver on the security capability?

3. How to efficiently estimate the radio link to maximize the security capacity?

Questions to be answered by our research?

1. How to design a secure transmission strategy in a frequency division duplex (FDD) system?

2. What is the impact of imperfect channel state information (CSI) at the receiver on the security capability?

3. How to efficiently estimate the radio link to maximize the security capacity?

4. How can we code to secure and make the legitimate link more reliable while degrading the eavesdropper link?

Questions to be answered by our research?

1. How to design a secure transmission strategy in a frequency division duplex (FDD) system?

2. What is the impact of imperfect channel state information (CSI) at the receiver on the security capability?

3. How to efficiently estimate the radio link to maximize the security capacity?

4. How can we code to secure and make the legitimate link more reliable while degrading the eavesdropper link?

5. How to secure the information without penalizing the PAPR in massive MIMO systems?

Performance Evaluation Metrics

1. Secrecy Capacity

$$SC = [Main\ Channel\ Capacity \quad Wiretap\ Channel\ Capacity]^{+}$$

Performance Evaluation Metrics

1. Secrecy Capacity

$$SC = [Main\ Channel\ Capacity \quad Wiretap\ Channel\ Capacity]^{+}$$

2. Secrecy Energy Efficiency

$$SEE = \frac{Secrecy\ Capacity}{Total\ Power\ Consumption}$$

Performance Evaluation Metrics

1. Secrecy Capacity

$$SC = [Main\ Channel\ Capacity \quad Wiretap\ Channel\ Capacity]^{+}$$

2. Secrecy Energy Efficiency

$$SEE = \frac{Secrecy\ Capacity}{Total\ Power\ Consumption}$$

3. Peak-to-Average Power Ratio

$$PAPR = \frac{Max\ Signal\ Power}{Average\ Signal\ Power}$$

Performance Evaluation Metrics

1. Secrecy Capacity

$$SC = [Main\ Channel\ Capacity \quad Wiretap\ Channel\ Capacity]^{+}$$

2. Secrecy Energy Efficiency

$$SEE = \frac{Secrecy\ Capacity}{Total\ Power\ Consumption}$$

3. Peak-to-Average Power Ratio

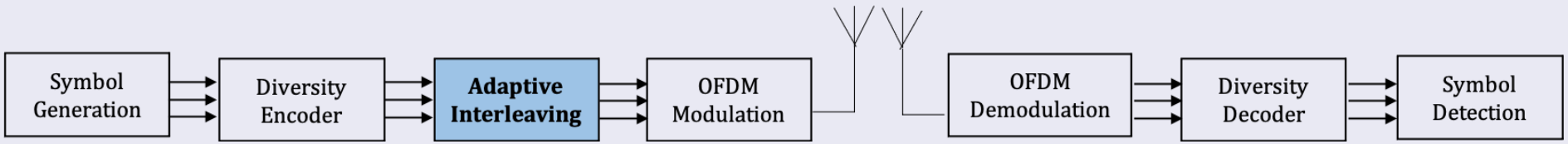
$$PAPR = \frac{Max\ Signal\ Power}{Average\ Signal\ Power}$$

4. Bit Error Rate

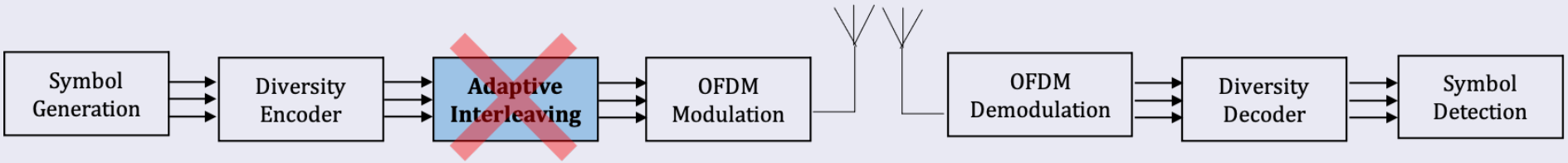
$$BER = \frac{No\ of\ Erroneous\ Bits}{Total\ Number\ of\ Transmitted\ Bits}$$

PLS for an FDD system with imperfect CSI

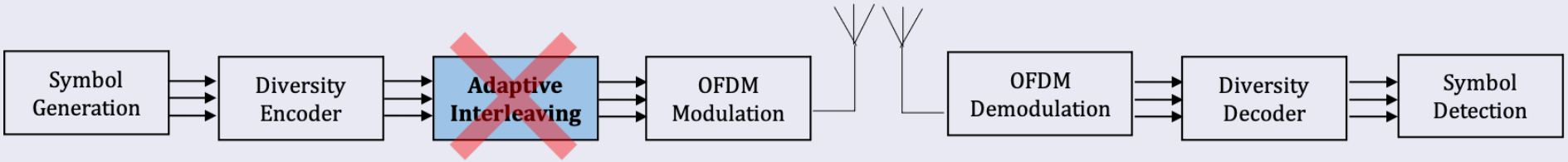
PLS by Interleaving and Diversity

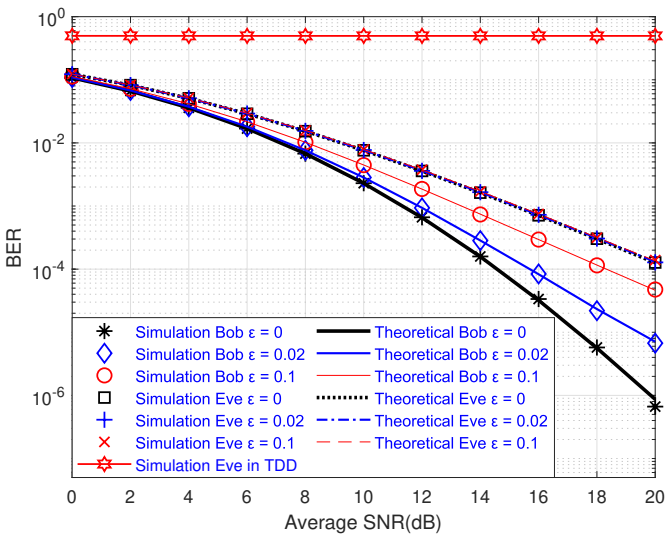


PLS by Interleaving and Diversity



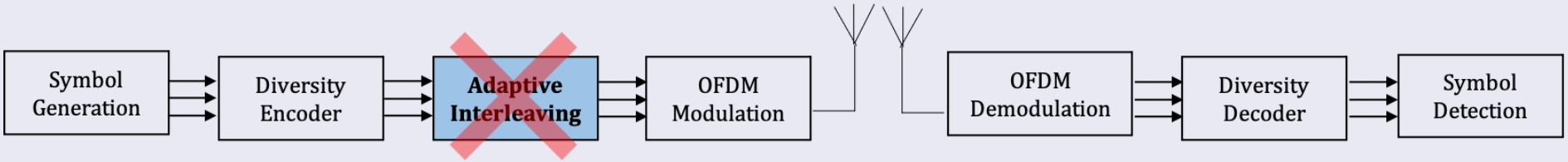
PLS by Interleaving and Diversity

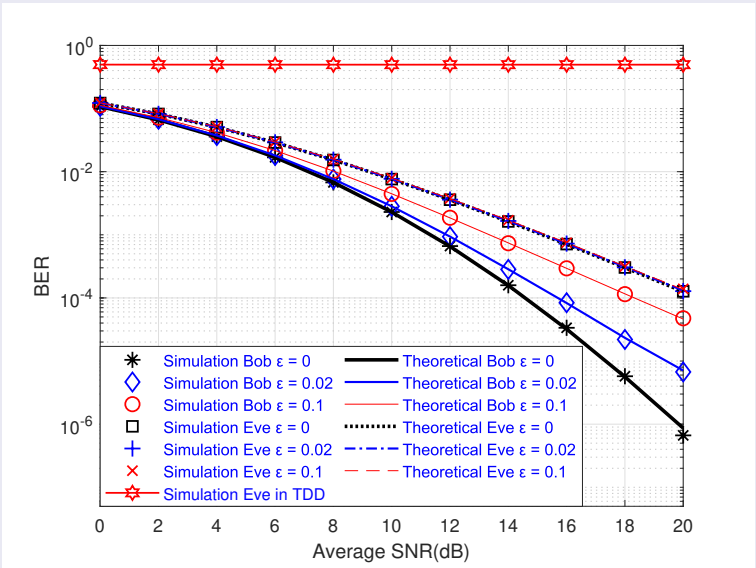




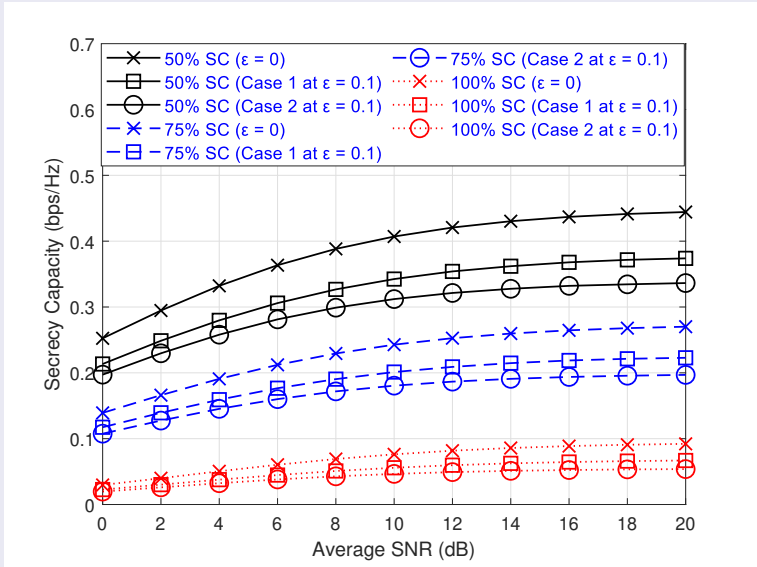
Bob and Eve error rate performances with imperfect CSI at Alice only, = 0, 0.02, 0.1.

PLS by Interleaving and Diversity





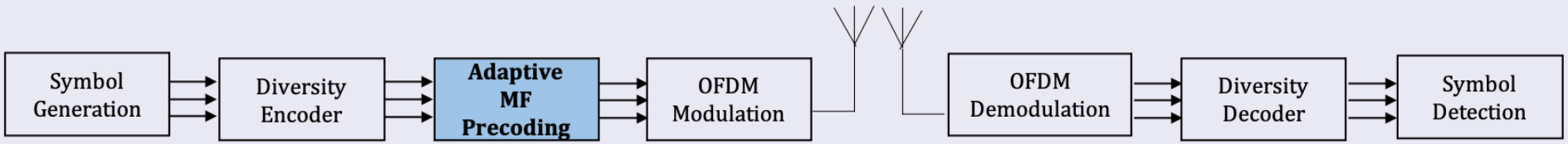
Bob and Eve error rate performances with imperfect CSI at Alice only, = 0, 0.02, 0.1.



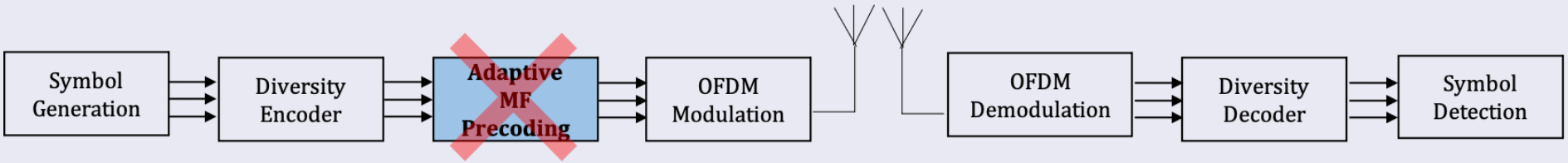
Secrecy capacity performances under perfect and imperfect CSI conditions, = 0, 0.1, subcarrier usage = 50%, 75%, 100%.

PLS with Imperfect Knowledge of CSI

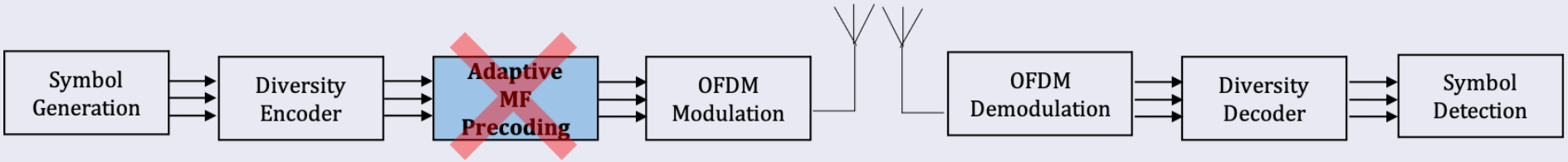
PLS by Precoding and Diversity

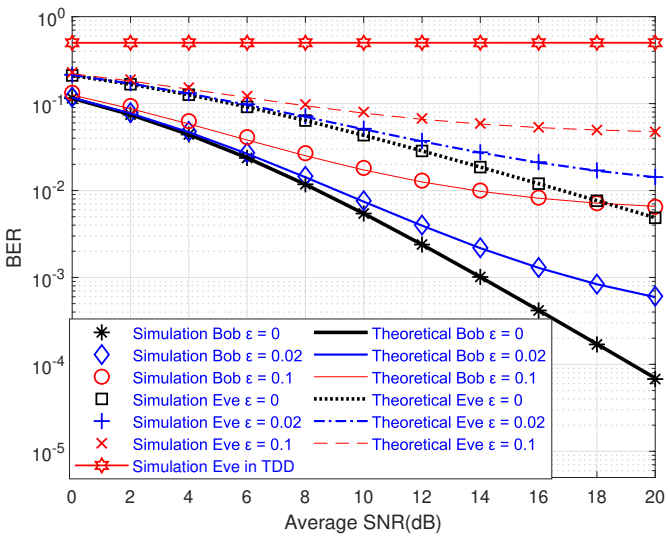


PLS by Precoding and Diversity



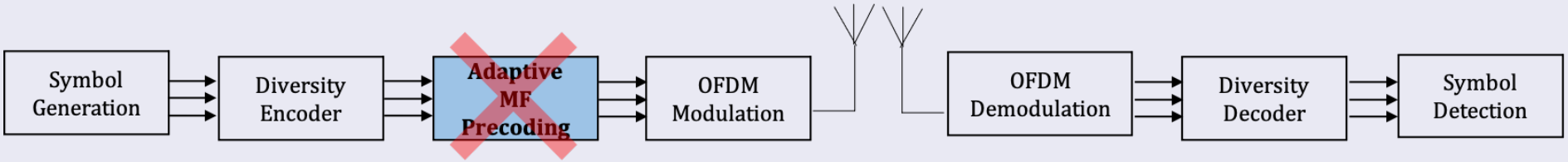
PLS by Precoding and Diversity

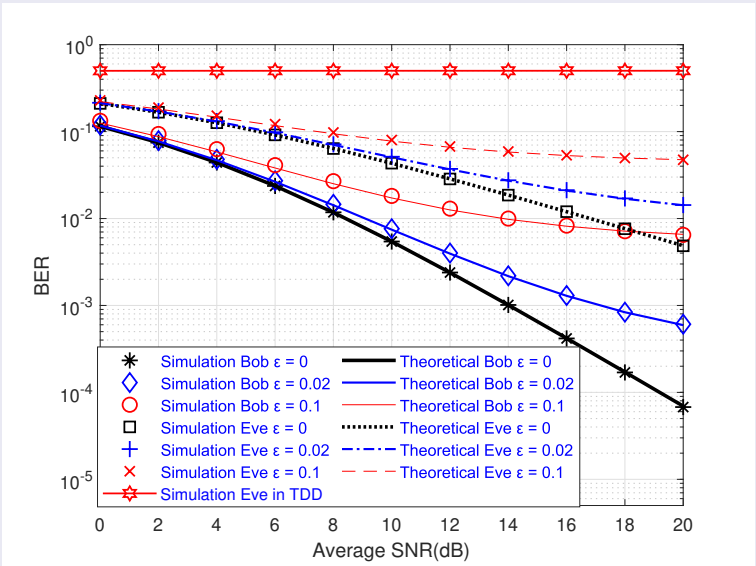




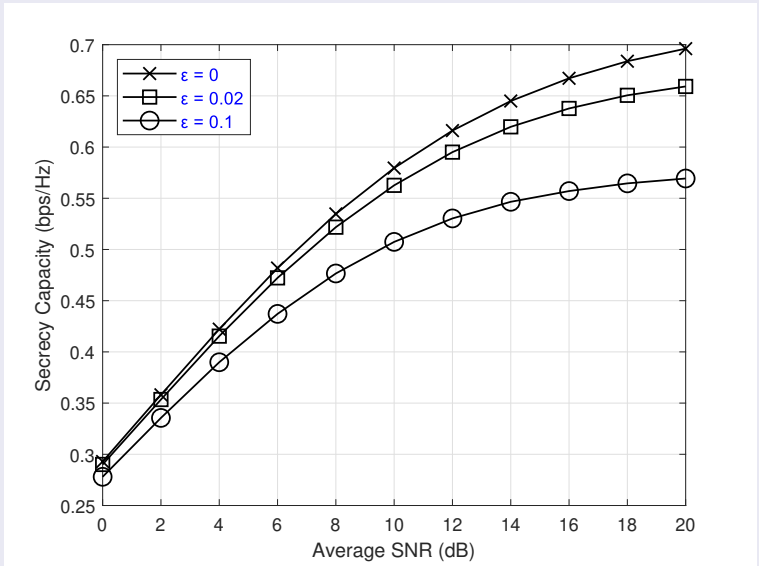
Bob and Eve error rate performances with imperfect CSI at Alice only, $= 0, 0.02, 0.1$.

PLS by Precoding and Diversity



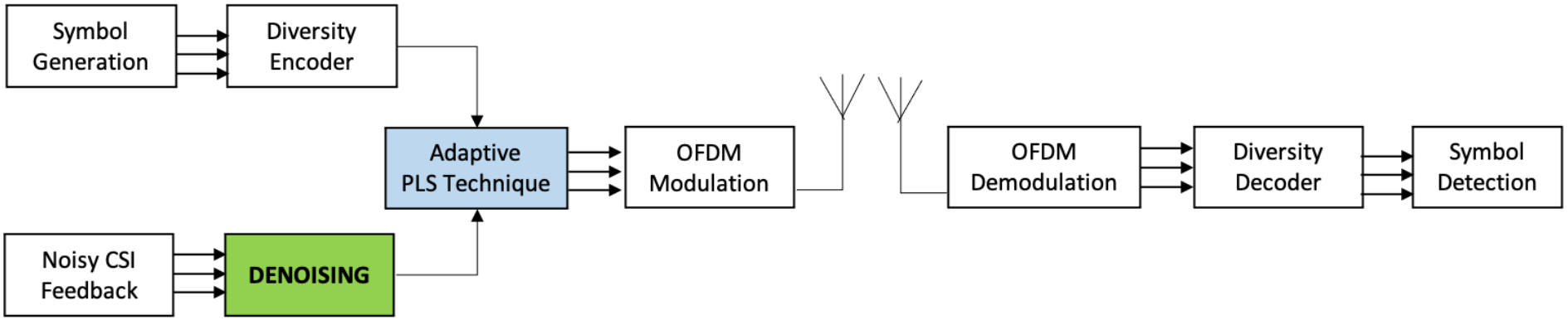


Bob and Eve error rate performances with imperfect CSI at Alice only, = 0, 0.02, 0.1.

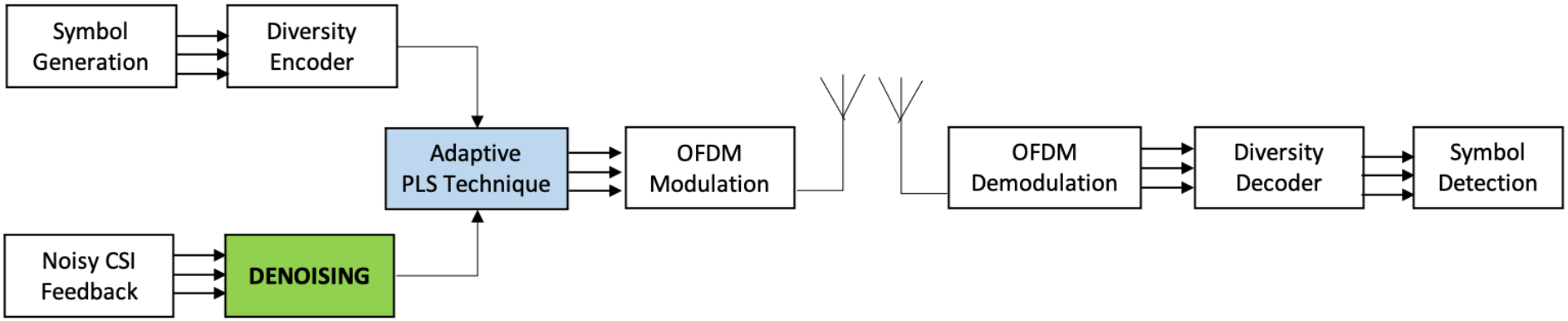


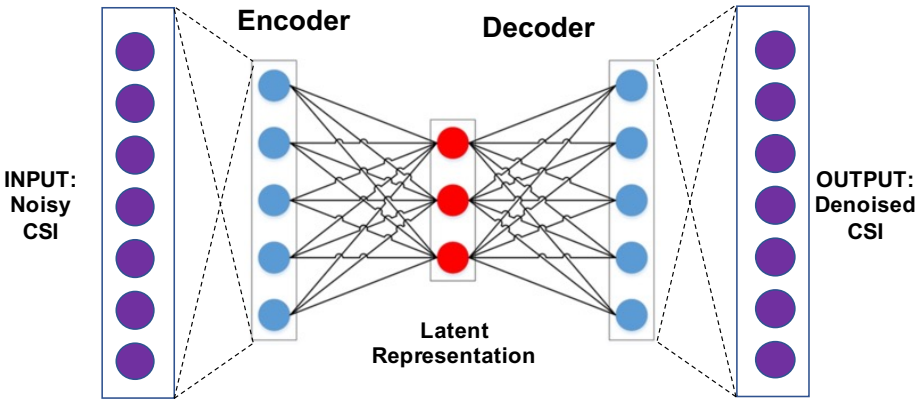
Secrecy capacity performances under perfect and imperfect CSI conditions, = 0, 0.02, 0.1.

Neural Network for Imperfect CSI Denoising



Neural Network for Imperfect CSI Denoising





DenoiseSecNet.

Neural Network for Imperfect CSI Denoising

Hyb-DenoiseSecNet.

Neural Network for Imperfect CSI Denoising

Hyb-DenoiseSecNet.

BER performance of DenoiseSecNet.

PLS with Indexed Partitioned Modulation

Indexed Partitioned Modulation

Indexed partitioned modulation.

Indexed Partitioned Modulation

Indexed partitioned modulation.

Secrecy Rate using 64 QAM..

Energy E cient PLS

Energy E ciency Challenge

Peak-to-average Power Ratio (PAPR).

Power ampli er transfer function.

Power ampli ers (PA) account for up to 70% of transmitter power consumption.
PLS by AN schemes force the PA to operate in the non-linear region.
It results in non-linear in-band distortion and out-of-band radiation.
Input back-o (IBO) can ensure linearity.
At cost of power ine ciency and huge operational expenditure.

System Model

System model of the AN precoded single-carrier massive MIMO downlink transmission with N_t antennas at the BS, N_r single antenna legitimate receivers and $N_{r;e}$ antennas at the eavesdropper where $N_t \quad N_r ; N_{r;e}$.

Algorithm owchart

Result Obtained

CCDFs of the PAPR of the proposed AN-aided scheme compared with signal with random AN and signal without added AN.

Result Obtained

CCDFs of the PAPR of the proposed AN-aided scheme compared with signal with random AN and signal without added AN.

Secrecy capacity performance of the proposed AN-aided scheme compared to the capacity with Random AN injection and no AN injection when = 0.9.

Thesis Publications

Thesis Publications

Journals

I. Ajayi, Y. Medjahdi, R. Zayani, L. Mroueh and F. Z. Kaddour, "PAPR-Aware Artificial Noise for Secure Massive MIMO Downlink," in IEEE Access, vol. 10, pp. 68482-68490, 2022, doi: 10.1109/ACCESS.2022.3186695.

I. Ajayi, Y. Medjahdi, O. Okubadejo, L. Mroueh and F. Z. Kaddour, "Neural Networks for Denoising Imperfect Channel State Information in Physical Layer Security," in final revision to be submitted to IEEE communication letters.

I. Ajayi, L. Mroueh, Y. Medjahdi, and F. Z. Kaddour, "Generalized Indexed Partitioned Modulation for Physical Layer Security in OFDM Communication," in final revision to be submitted to IEEE transaction on communication.

Thesis Publications

Conference

I. Ajayi, Y. Medjahdi, L. Mroueh and F. Kaddour, "**Physical Layer Security by Interleaving and Diversity: Impact of Imperfect Channel State Information**," 2021 8th International Conference on Electrical Engineering, Computer Science and Informatics (EECSI), 2021, pp. 299-304, doi: 10.23919/EECSI53397.2021.9624293.
Best Paper Award Received

I. Ajayi, Y. Medjahdi, F. Kaddour and L. Mroueh, "**Impact of Imperfect Channel State Information on Physical Layer Security by Precoding and Diversity**," 2021 8th International Conference on Electrical Engineering, Computer Science and Informatics (EECSI), 2021, pp. 322-327, doi: 10.23919/EECSI53397.2021.9624230.

I. Ajayi, L. Mroueh, Y. Medjahdi, and F. Z. Kaddour, "Secrecy Energy Efficiency in PAPR-Aware Artificial Noise Scheme for Secure Massive MIMO", submitted to IEEE Wireless Communications and Networking Conference (WCNC 2023).

I. Ajayi, L. Mroueh, Y. Medjahdi, and F. Z. Kaddour, "Indexed Partitioned Modulation for Physical Layer Security in SISO-OFDM Communication", in final revision to be submitted to IEEE Information Theory Workshop 2023.

THANK YOU