GEFÖRDERT VOM Bundesministerium für Bildung und Forschung

PHYve-G: Evaluating Channel Reciprocity and Secret Key Generation in 5G Networks

Ghazal Bagheri, Stefan Köpsell

Dresden University of Technology (TUD)

Julian Dreyer, Ralf Tönjes

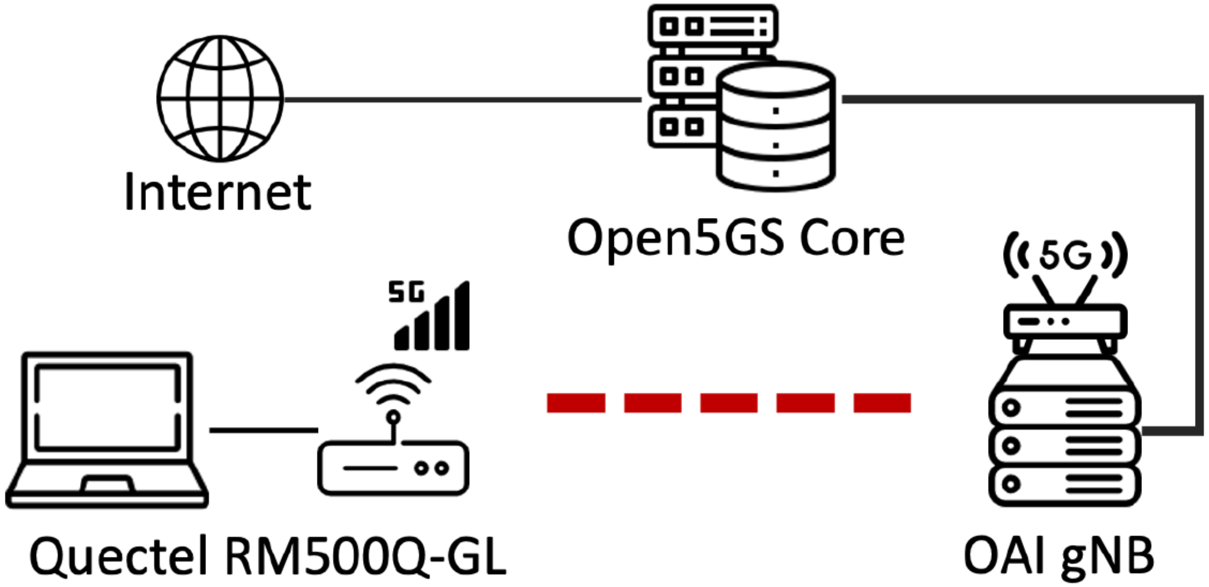
Hochschule Osnabrück (University of Applied Sciences)

28. VDE-ITG-Fachtagung Mobilkommunikation

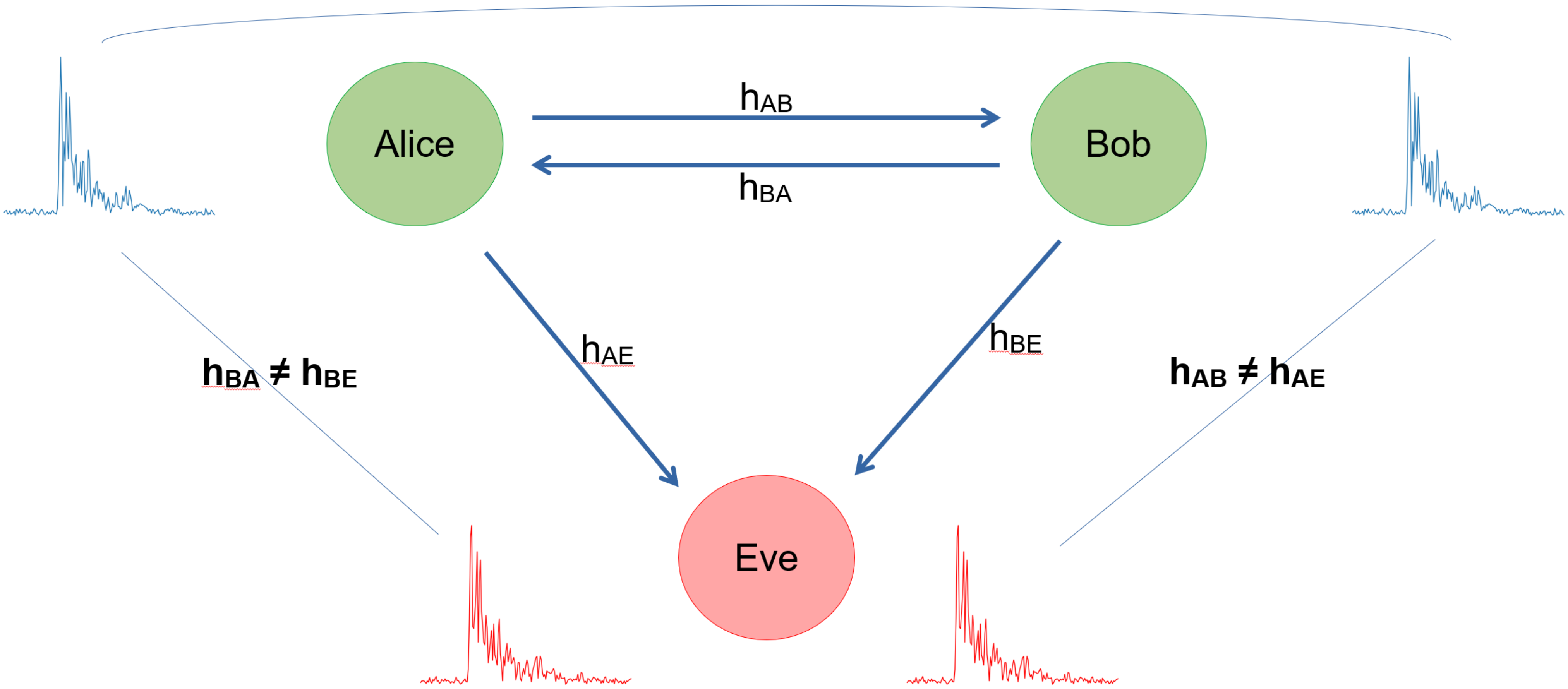
Hochschule Osnabrück //16.05.2024

The goal of the study:

Establishment of Secure Wireless Communication via Channel Reciprocity-based Key Generation.

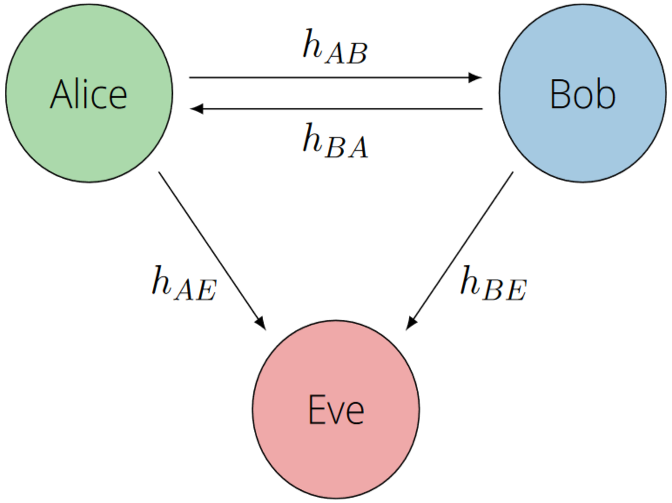


The General Overview of the Channel Reciprocity

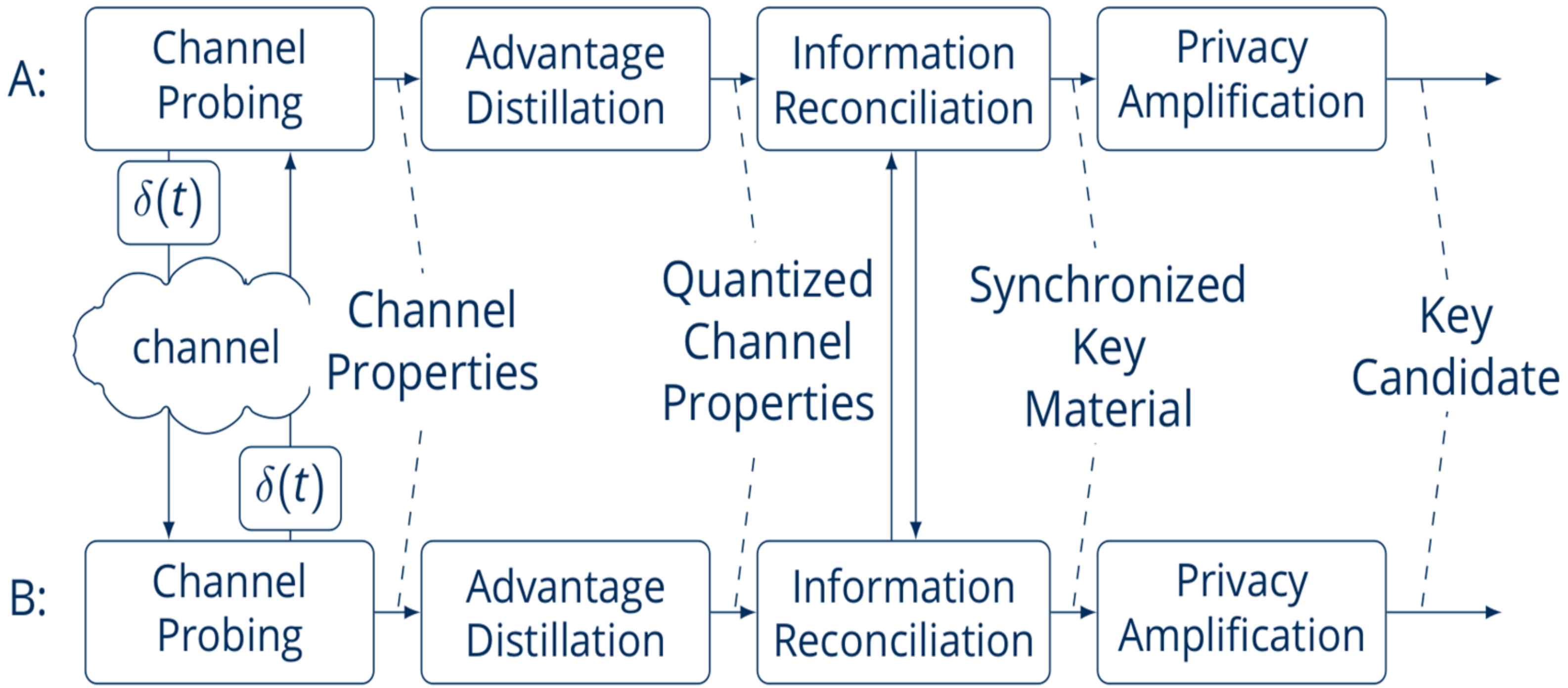


h_{AB}: Channel states transmitted from Alice to Bob
h_{BA}: Channel states transmitted from Bob to Alice
h_{AE}: Channel states transmitted from Alice to Eve
h_{BE}: Channel states transmitted from Bob to Eve

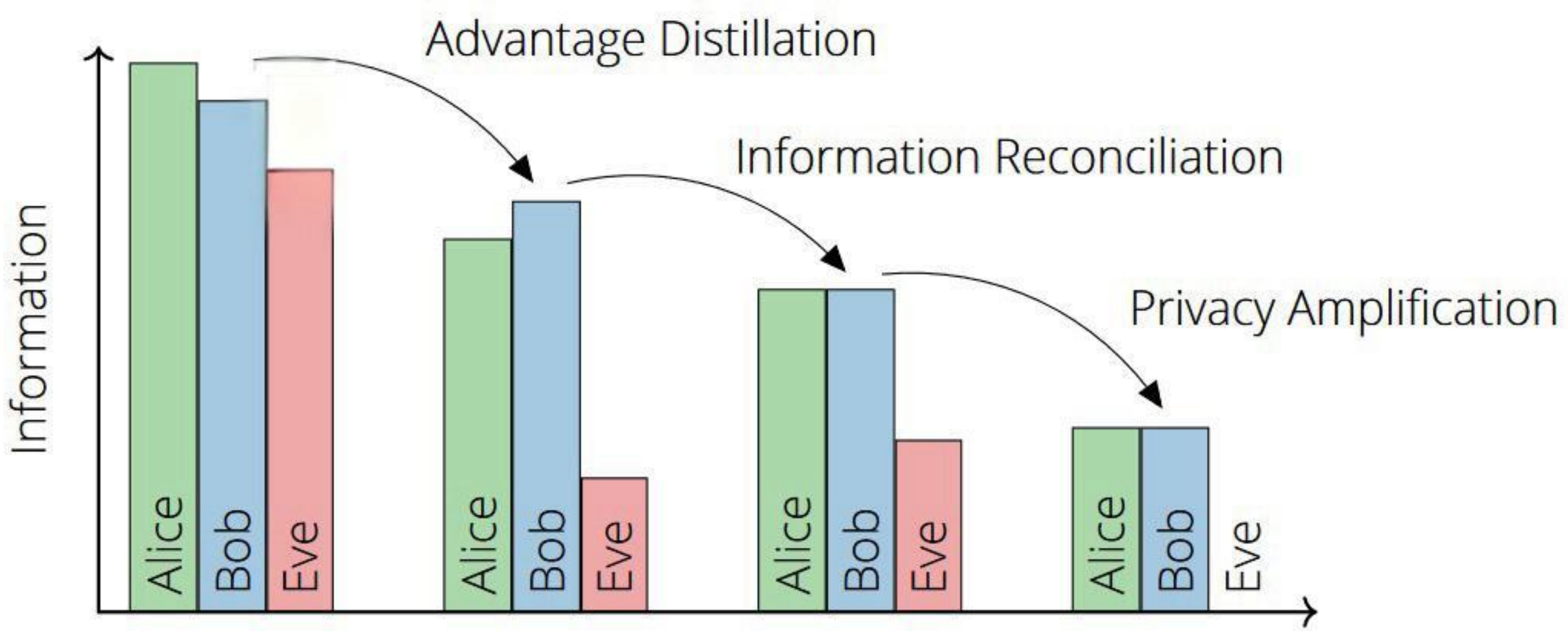
Channel Reciprocity-based Key Generation Steps



General Setup of the CRKS Scheme



Qualitative Representation of Sequential Key Derivation Participants



5G Channel State Information (CSI) evaluation setup

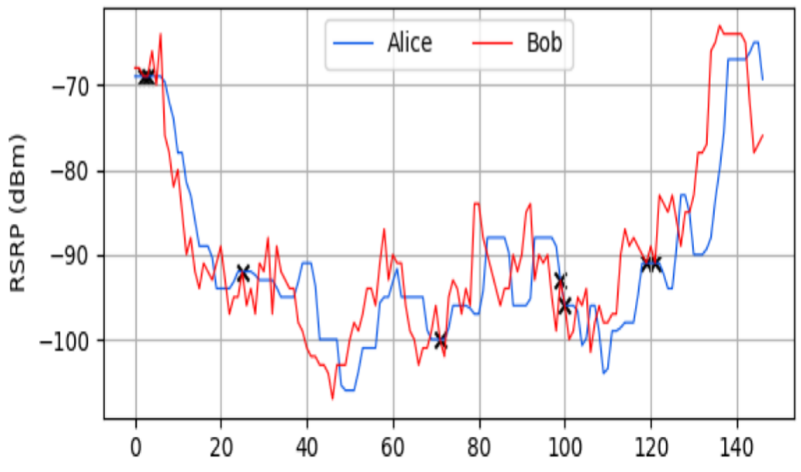
- ❑ **gNB and Radio Unit (RU)**
- ❑ **User Equipment (UE)**

Parameter Extraction and Analysis:

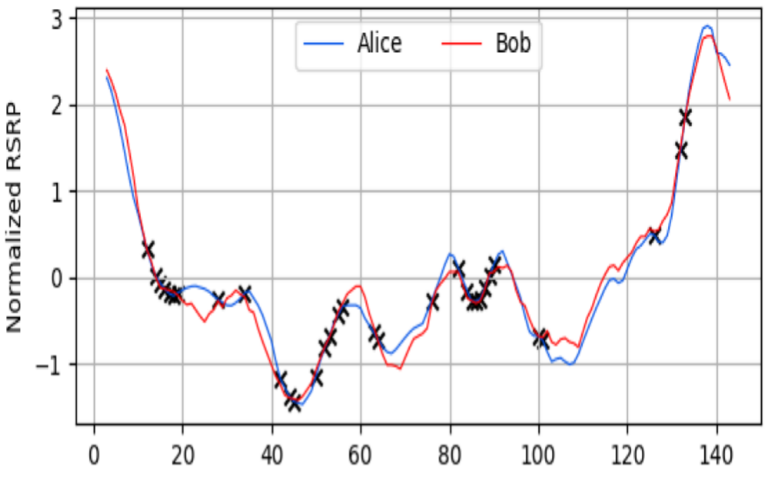
- ➢ **UE utilizes Reference Signal Received Power (RSRP) for general channel reciprocity assessment.**
- ➢ **Analyze RSRP values, and apply statistical normalization for CSI profile enhancement.**
- ➢ **Employ Discrete cosine transform (DCT) to assess signal similarity in the frequency domain.**

5G CHANNEL RECIPROCITY EVALUATION

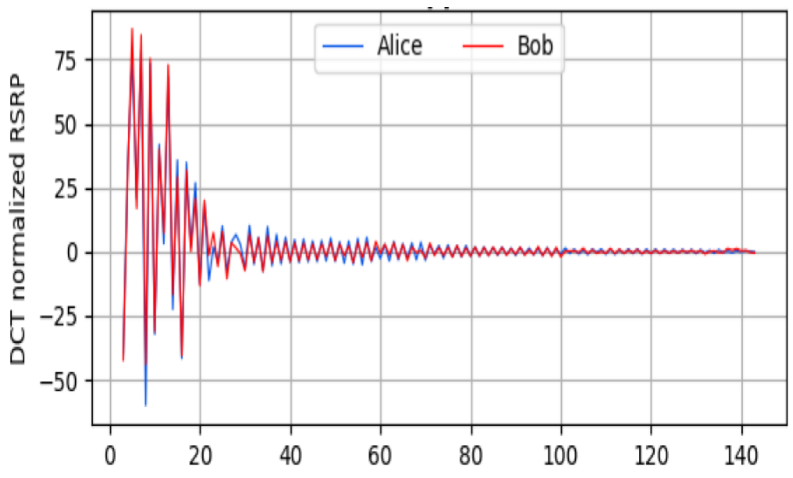
First lab test with one UE (Alice) communicating with Bob gNB



Reference Signal Received Power (RSRP) in dBm



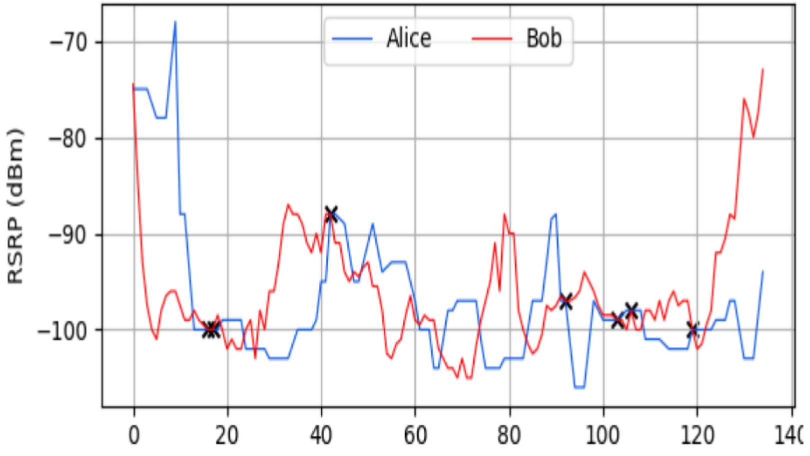
Normalized RSRP to remove the effect of the dominant component



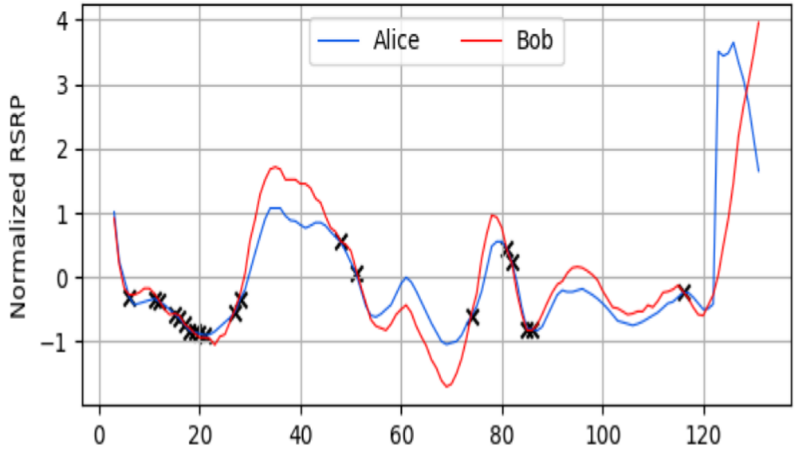
Discrete Cosine Transform (DCT) of the normalized RSRP

5G CHANNEL RECIPROCITY EVALUATION

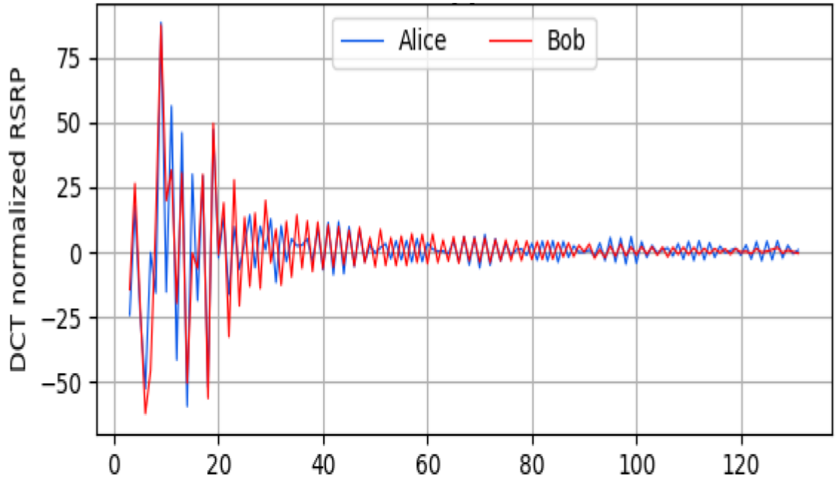
Second lab test with one UE (Alice) communicating with Bob gNB



Reference Signal Received Power (RSRP) in dBm



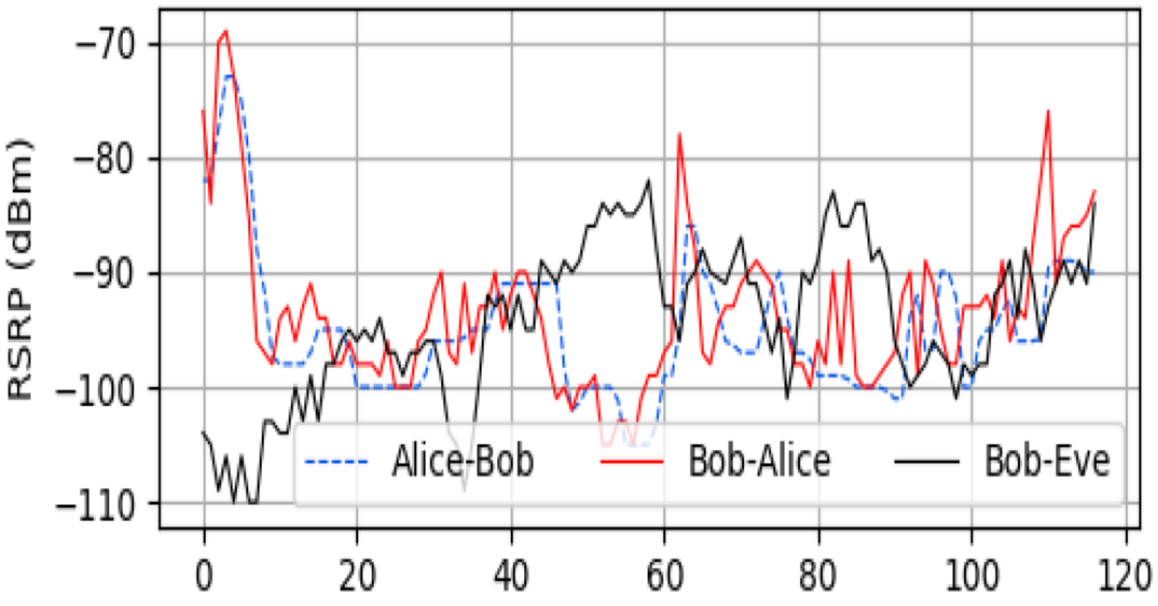
Normalized RSRP to remove the effect of the dominant component



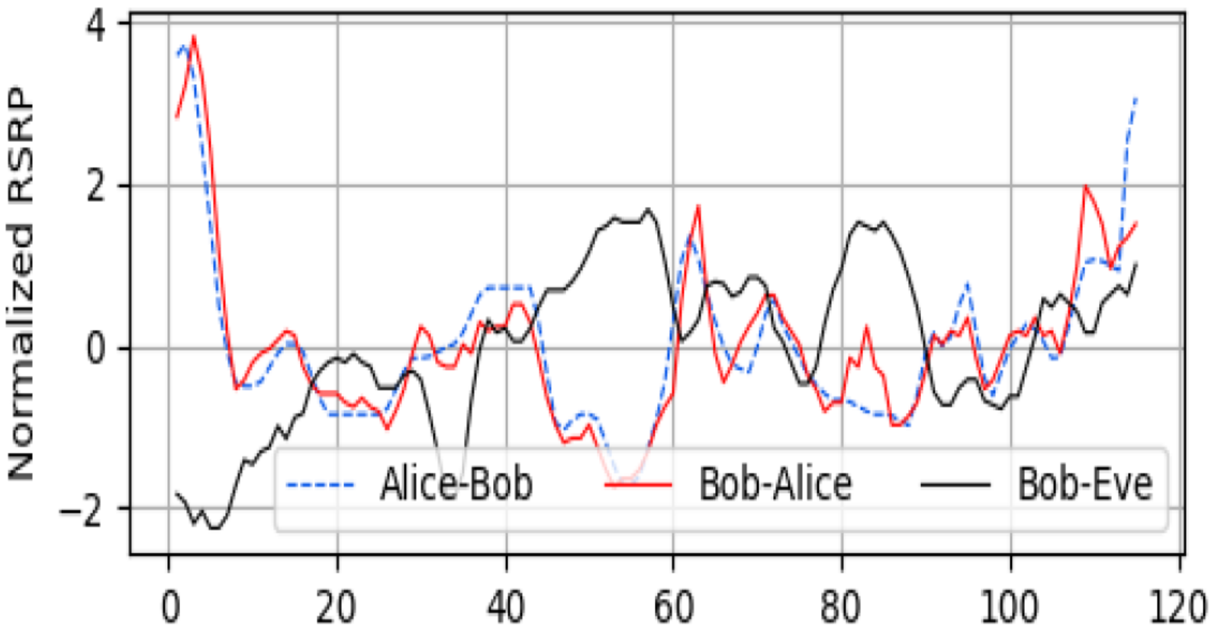
Discrete Cosine Transform (DCT) of the normalized RSRP

5G CHANNEL RECIPROCITY EVALUATION

Evaluation with one attacker UE (Eve) and a normal UE (Alice)



Reference Signal Received Power (RSRP) in dBm



Normalized RSRP to remove the effect of the dominant component

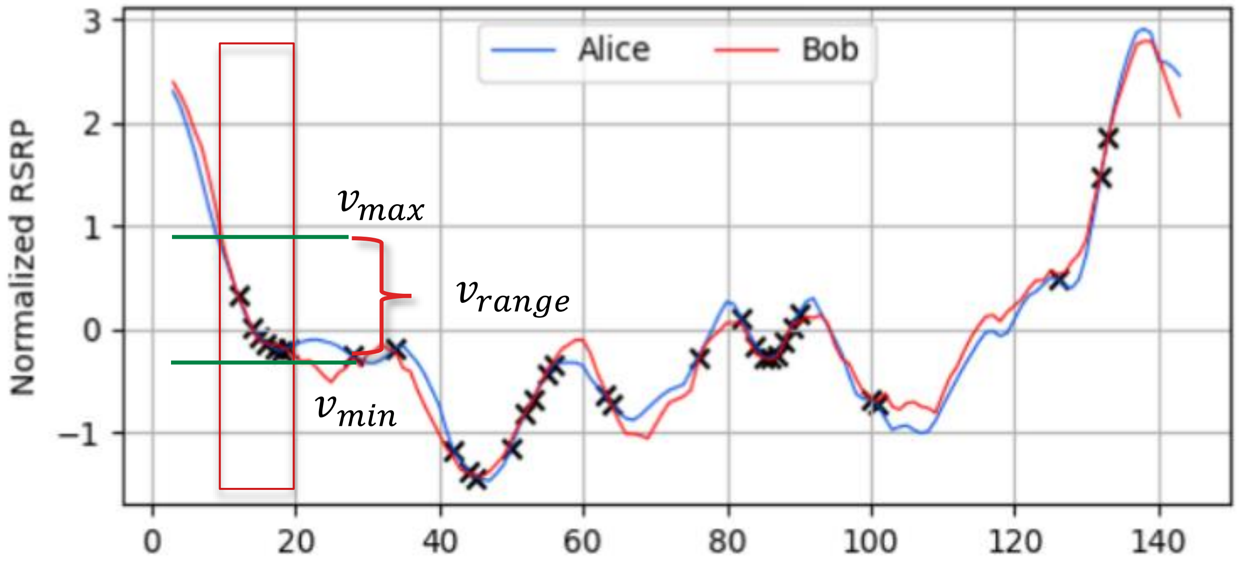
Channel Reciprocity-based Key Generation- Advantage Distillation

Algorithm 1 Multi-bit Quantization

Input: Sequence s, sequence length L, window size B, number of quantization bits bit_{num}

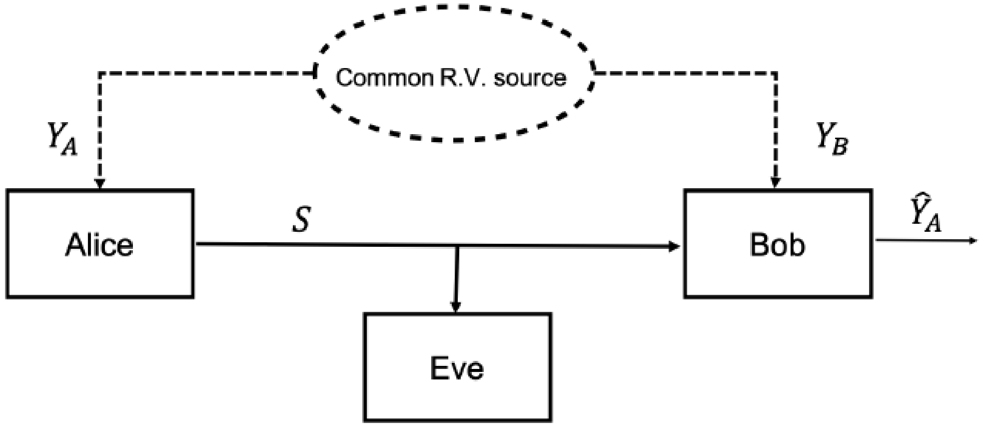
Output: Quantized sequence q

for $i = 0$ to L **do**
    $q \leftarrow 0$
    $v_{max} \leftarrow$ max in range $(s[i], s[i+B])$
    $v_{min} \leftarrow$ min in range $(s[i], s[i+B])$
    $v_{range} \leftarrow v_{max} - v_{min}$
    if $s[i] = v_{max}$ **then**
        $q \mathrel{+}= \text{Gray}(2^{bit_{num}} - 1)$
    else if $s[i] = v_{min}$ **then**
        $q \mathrel{+}= \text{Gray}(0)$
    else
        $m \leftarrow \left\lfloor \frac{s[i] - v_{min}}{v_{range}} \times 2^{bit_{num}} \right\rfloor$
        $q \mathrel{+}= \text{Gray}(m)$
    end if
end for
return q

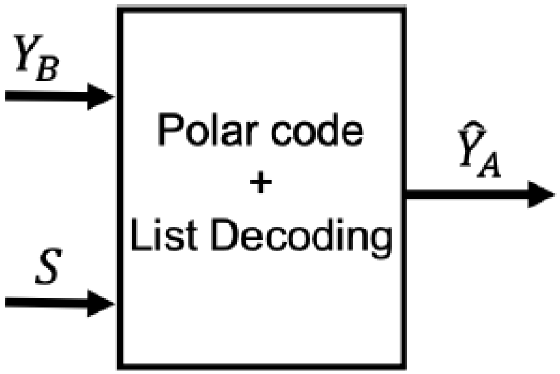


An example of normalized reference signal received power (RSRP)

Channel Reciprocity-based Key Generation- Information Reconciliation



The system model for the reconciliation step



Decoder structure for polar codes with list decoding

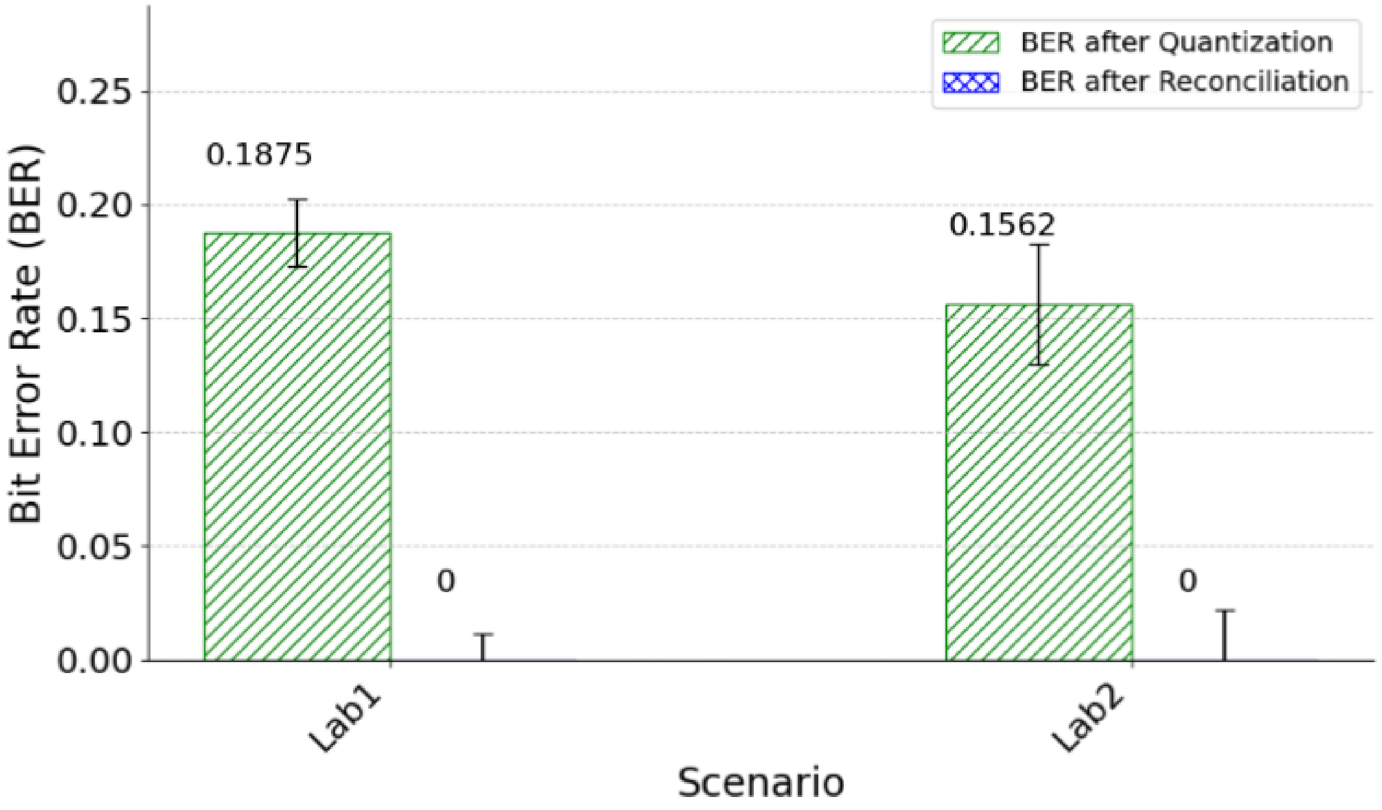
Channel Reciprocity-based Key Generation-Result

Lab 1:

- **Bit Error Rate After Quantization: 0.18**
- **Bit Error Rate After Reconciliation: 0**

Lab 2:

- **Bit Error Rate After Quantization : 0.15**
- **Bit Error Rate After Reconciliation: 0**



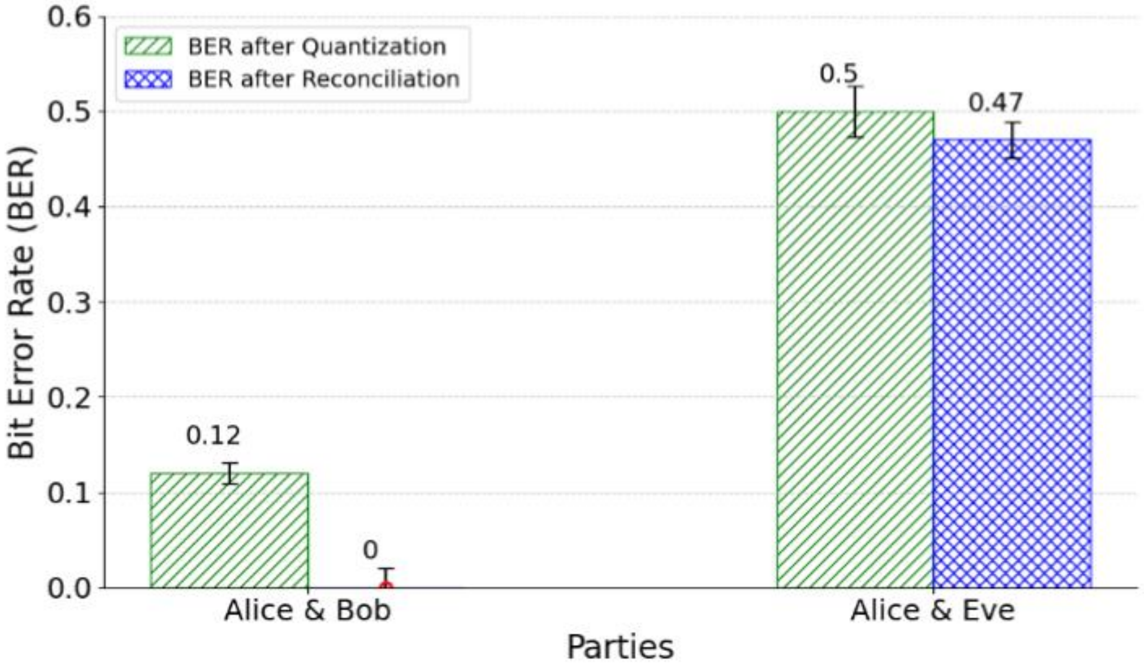
BER after quantization and reconciliation for the first and second lab tests when UE (Alice) communicates with gNB (Bob)

Channel Reciprocity-based Key Generation-Result

Lab 3: At the Presence of an Attacker

- Bit Error Rate (Alice&Bob) After Quantization: 0.12
- Bit Error Rate (Alice&Bob) After Reconciliation: 0

- Bit Error Rate (Alice&Eve) After Quantization : 0.5
- Bit Error Rate (Alice&Eve) After Reconciliation: 0.47



BER after quantization and reconciliation for the scenario in the presence of an attacker

Channel Reciprocity-based Key Generation

Summary and Conclusion:

- ❑ This study demonstrates the derivation of symmetric shared secrets between UEs and gNBs.
- ❑ Channel reciprocity enables the generation of secure keys for 5G communication.

For Further improvement:

- ❑ Applying different quantization methods to enhance the key’s quality.
- ❑ Enhancing key security by applying a privacy amplification step.

Thank you

For your attention

References

[1] C. Zenger. “Physical-Layer Security for the Internet of Things”. PhD thesis. Ruhr Universität Bonn, 2017.