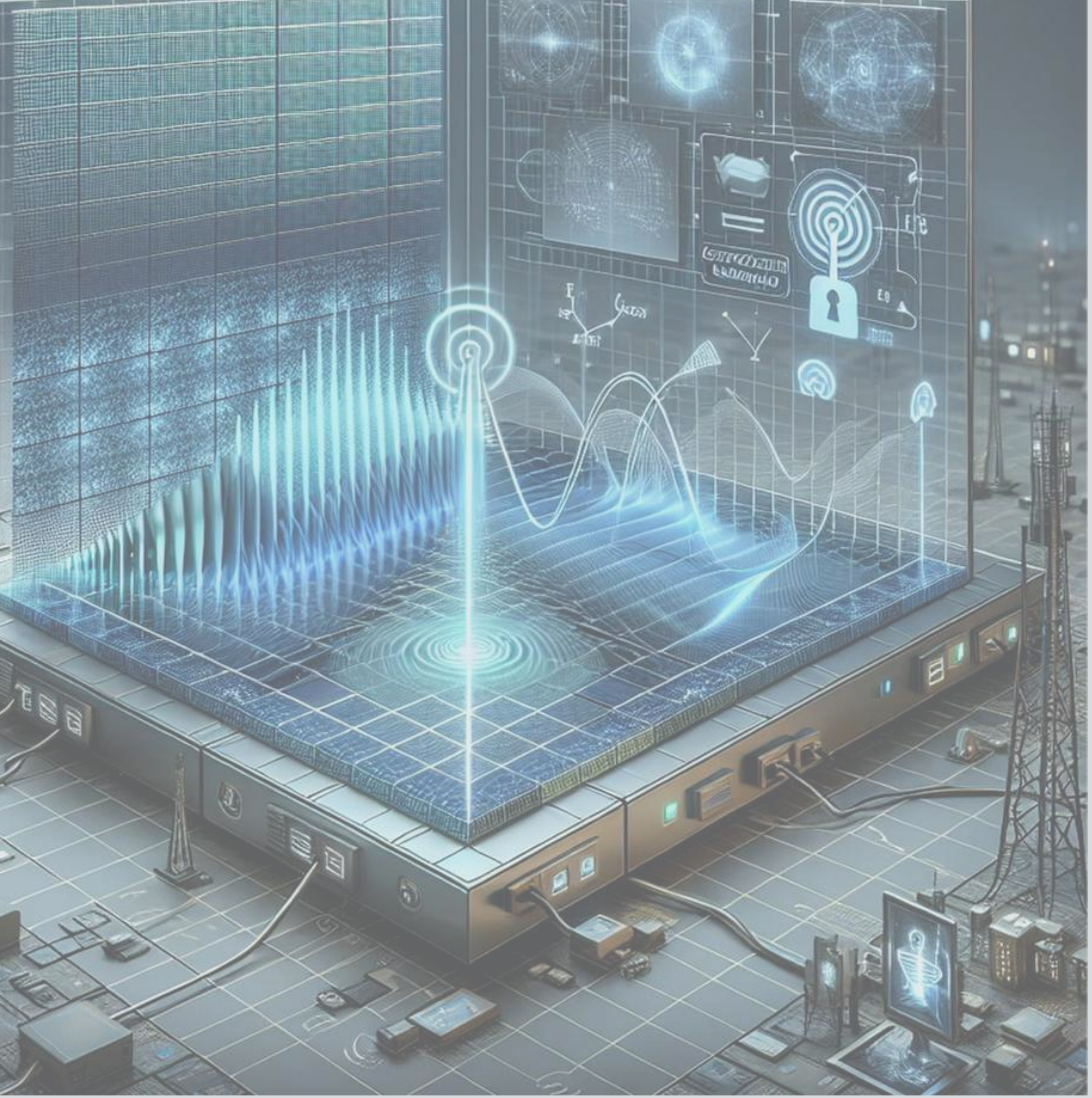



Deutsches Forschungszentrum für Künstliche Intelligenz
*German Research Center for Artificial Intelligence*

Rheinland-Pfälzische Technische Universität Kaiserslautern Landau


# Enhancing Physical Layer Key Generation Leveraging Reconfigurable Intelligent Surfaces


**29. VDE / ITG Fachtagung Mobilkommunikation**
Hochschule Osnabrück
20th May 2025



**Wenqing Dai**, Sachinkumar B. Mallikarjun, Yorman Munoz, Christoph Lipps and Hans Dieter Schotten

# Content

- Motivation
- Overview on PLKG
- Overview on RIS
- System Considerations
- Simulation Results and Insights
- Conclusion and Outlook

# Motivation

| Traditional Cryptography | Physical Layer Key Generation (PLKG) |
| --- | --- |
| Key Distribution | Reciprocity-based |
| High Overhead | Lightweight |
| Quantum-Vulnerable | Quantum-Resistant |

Table 1: Comparison between PLKG and traditional cryptography

High dynamics, multi-path interference and security risks in wireless communications. Traditional encryption methods rely on software layers and are vulnerable to quantum computing and key lifecycle limitations.

# Overview on PLKG

- A promising technology to extract symmetric keys from wireless fading channel.
- PLKG is based on short-term channel reciprocity, spatial channel uniqueness and intrinsic channel randomness, which require no public key infrastructure (PKI).

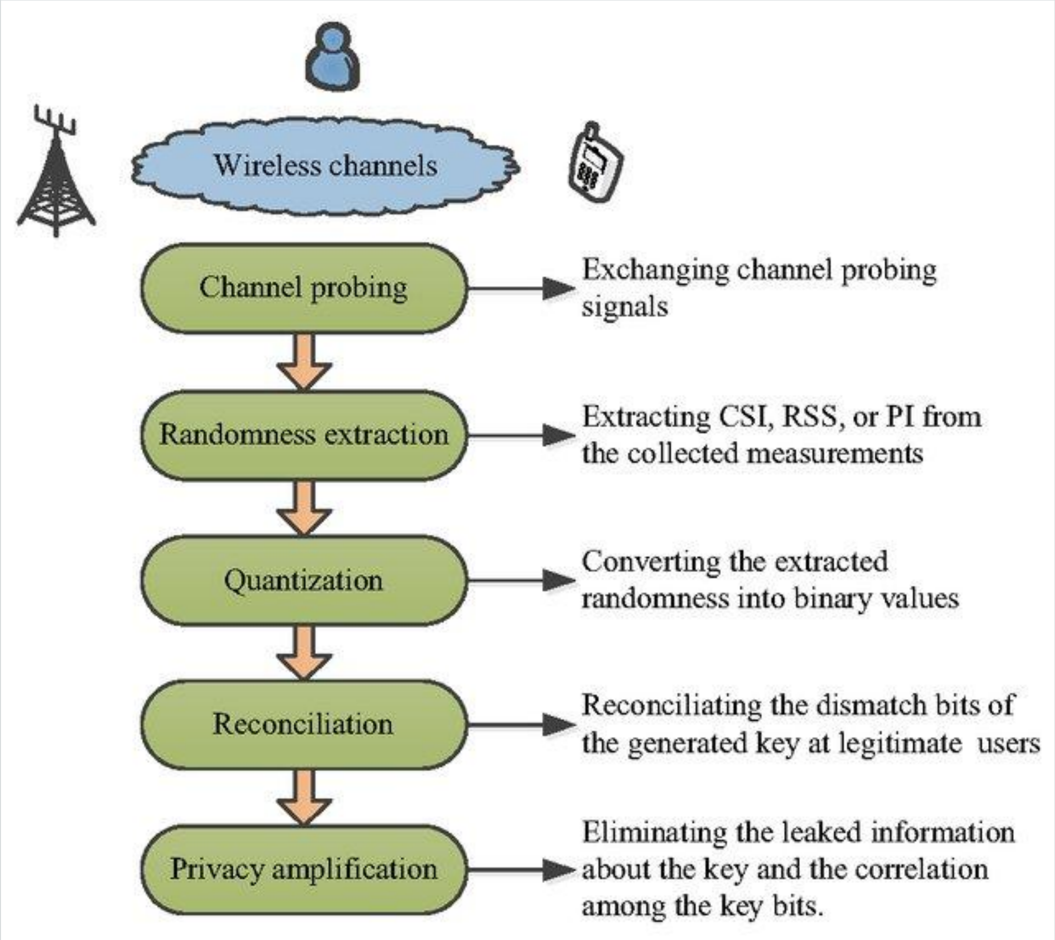



Figure 1: Typical process of the physical layer key generation

Wang, Dong & Bai, Bo & Lei, Kai & Zhao, Wenbo & Yang, Yanping & Han, Zhu. (2019). Enhancing Information Security via Physical Layer Approaches in Heterogeneous IoT With Multiple Access Mobile Edge Computing in Smart City. IEEE Access. PP. 1-1. 10.1109/ACCESS.2019.2913438.

# Challenges in static or block fading scenarios

- Lack of sufficient channel variations in static environments, leading to lower entropy.
- Easily leads to increased key predictability and increased risk of leakage.

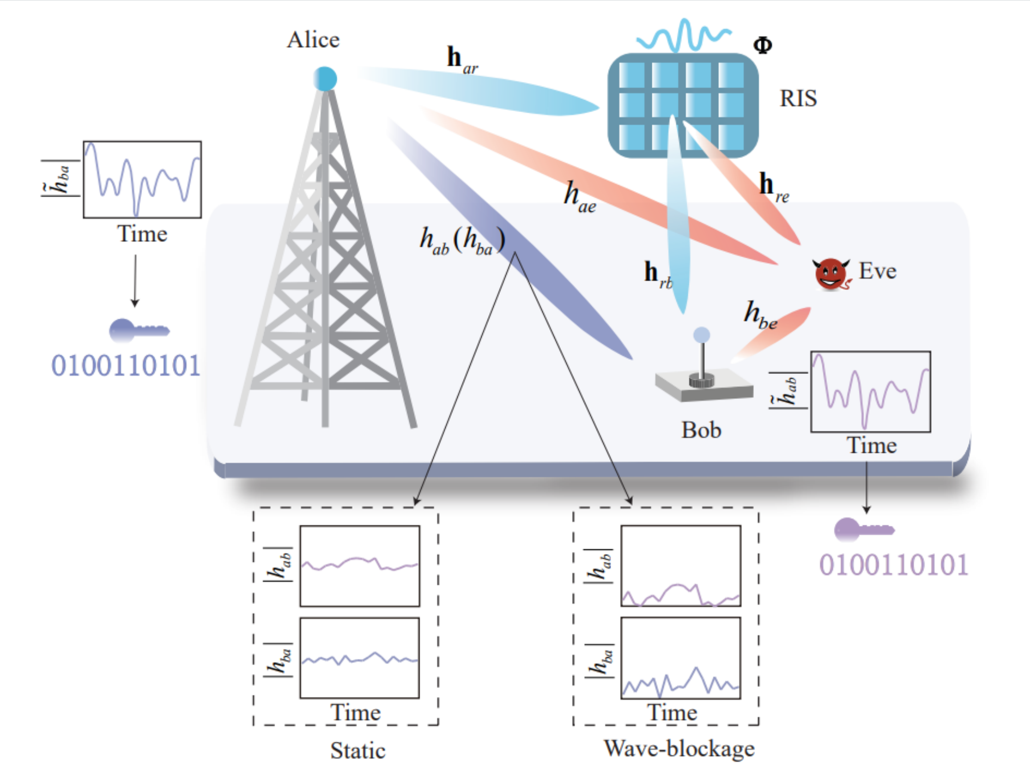



Figure 2: Eavesdropping risks in static enviroment

G. Li et al., "Reconfigurable Intelligent Surface for Physical Layer Key Generation: Constructive or Destructive?," in IEEE Wireless Communications, vol. 29, no. 4, pp. 146-153, August 2022, doi: 10.1109/MWC.007.2100545.

# Overview on RIS

- RIS can be programmed to control the phase and direction of signal reflections.
- It can be used to enhance channel entropy, introduce artificial randomness, and improve the security of key generation.

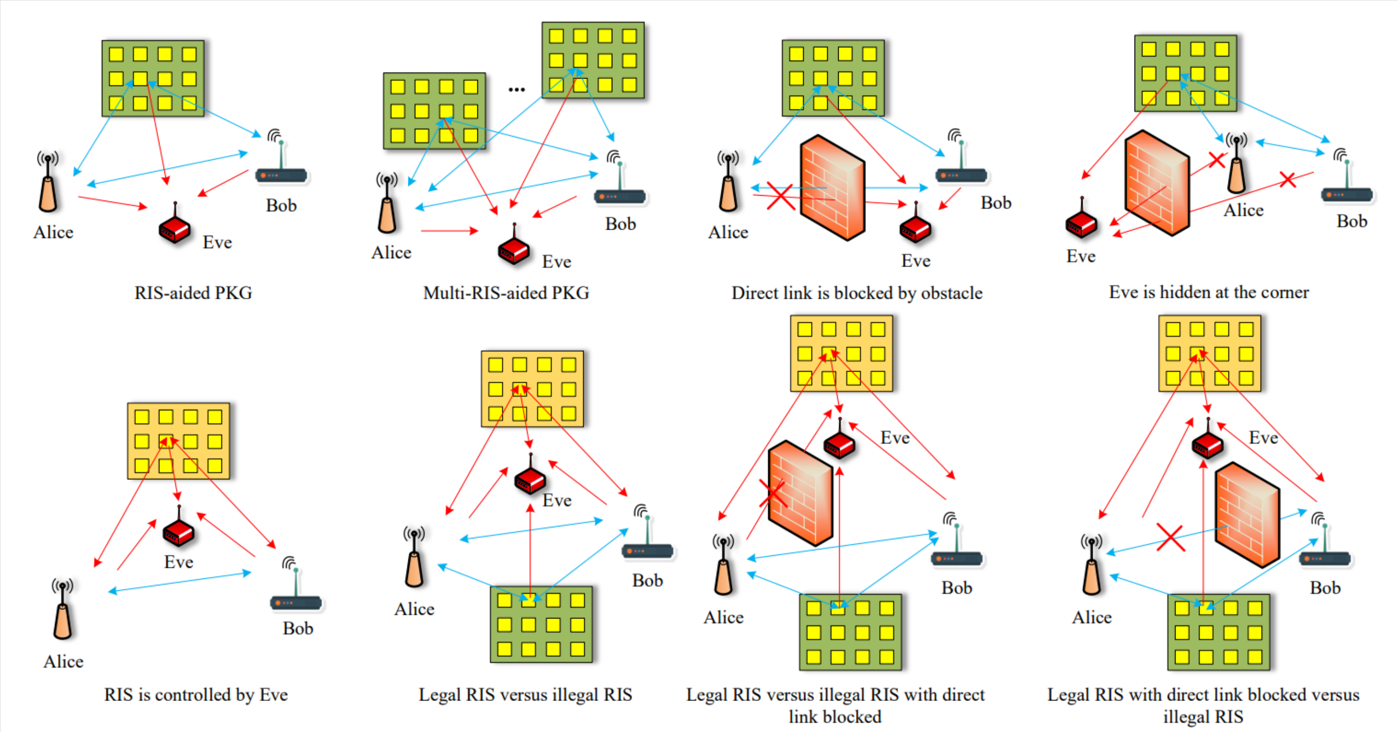



Figure 3: The potential application scenarios for RIS-aided PLKG

N. Gao, Y. Han, N. Li, S. Jin and M. Matthaiou, "When Physical Layer Key Generation Meets RIS: Opportunities, Challenges, and Road Ahead," in IEEE Wireless Communications, vol. 31, no. 3, pp. 355-361, June 2024, doi: 10.1109/MWC.013.2200538.



dfki ai Intelligent Networks RPTU

# System Model Considerations

- System operates @3.5 GHz with a 100 MHz bandwidth and OFDM modulation. The system supports 1,000 sampling iterations.
- The RIS is configured with different phase control strategies: random phase, On-Off switching and optimized phase alignment.
- Key generation is performed by extracting the CSI, applying 4-bit quantization, and computing three key performance indicators: the KGR, BMR, and entropy.

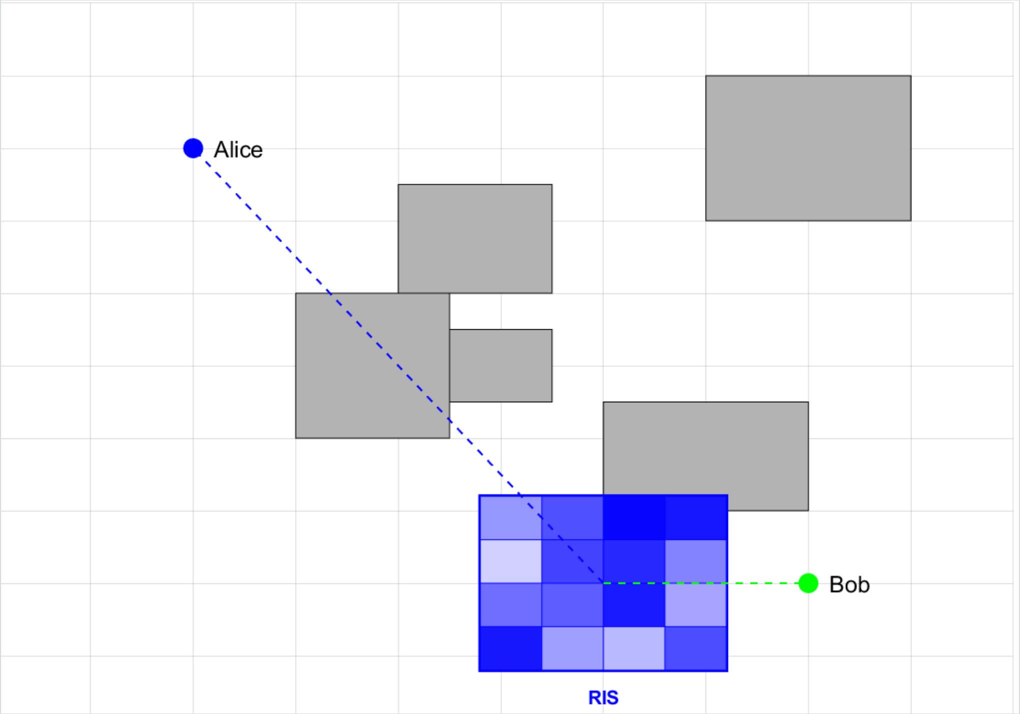



Figure 4: Simulation system layout with Alice, Bob and obstacles

# Security Metrics

- Entropy: randomness of the channel for key extraction.
- Bit Mismatch Rate (BMR): synchronization error between users.
- Key Generation Rate (KGR): how many bits per trial.
- Evaluated under different SNR (0dB- 40dB) and RIS modes.

# Simulation Results and Insights

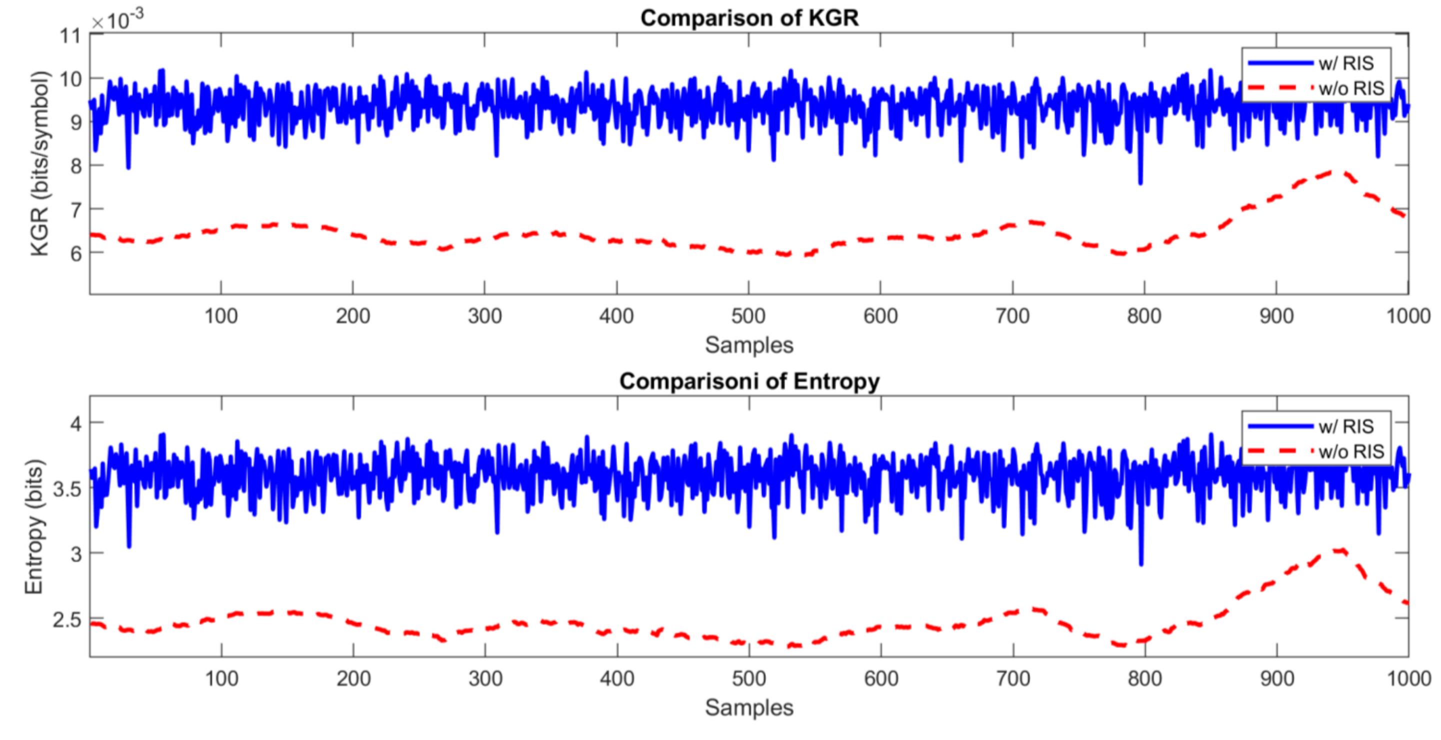
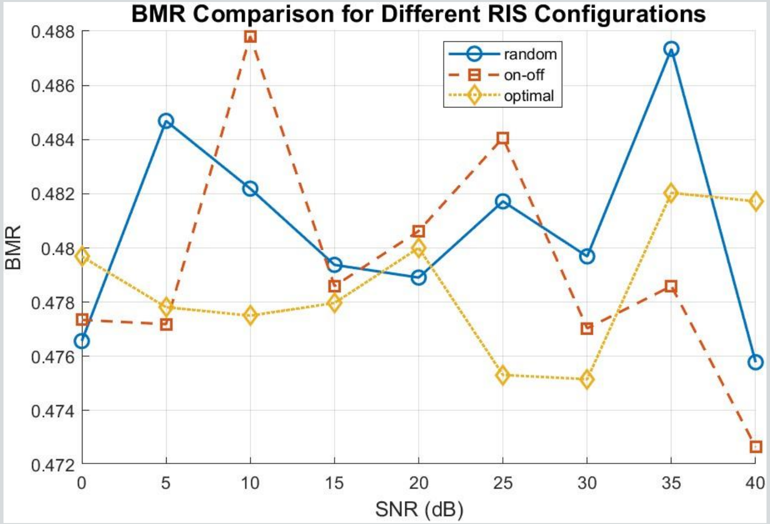
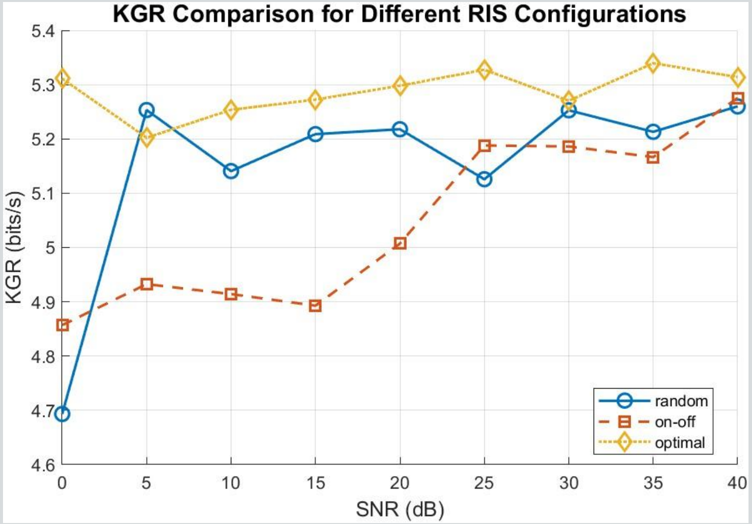



Figure 5: Performance comparison between baseline (without RIS's enhancement) and RIS-aided PLKG

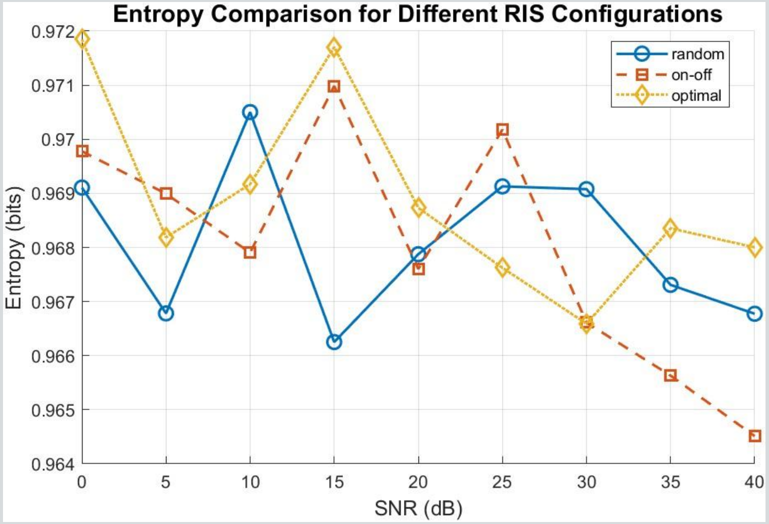
# Simulation Results and Insights




(a) Random Phase




(b) On-Off Switching




(c) Optimized Phase Alignment

Figure 6: Performance evaluation between 3 RIS configurations with varying SNR

# Simulation Results and Insights

- Performance varies with configurations and SNR.
- Optimized RIS significantly improves KGR in poor environments.
- High entropy alone is not enough — needs low BMR.
- Random RIS helps, but optimized design gives best trade-off.

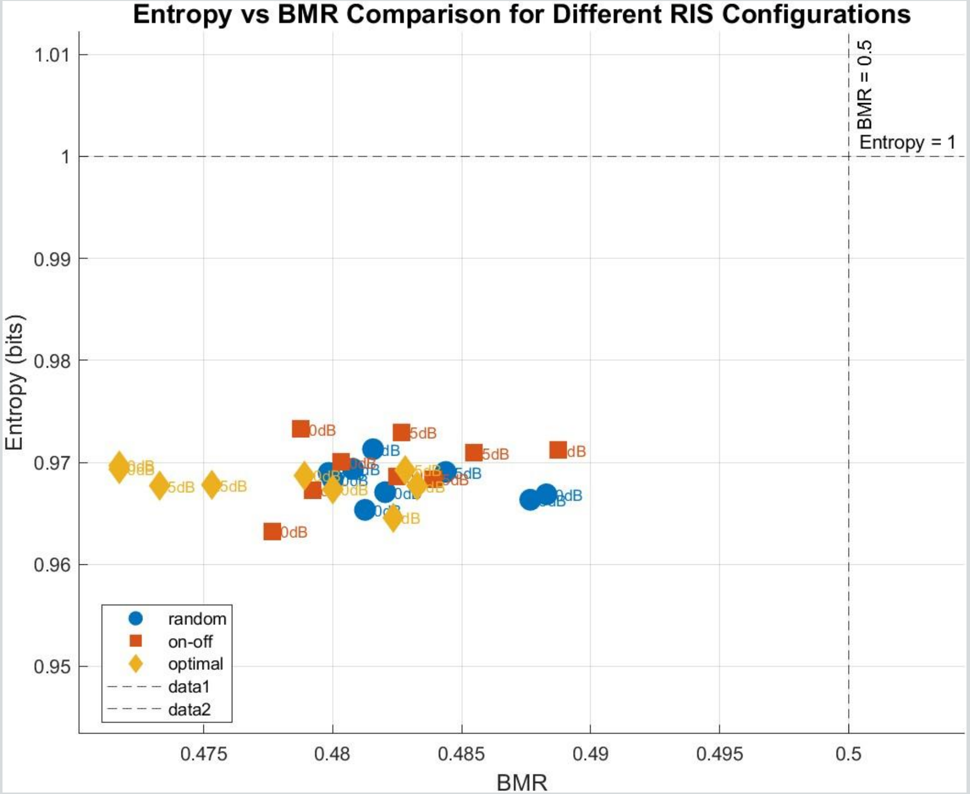


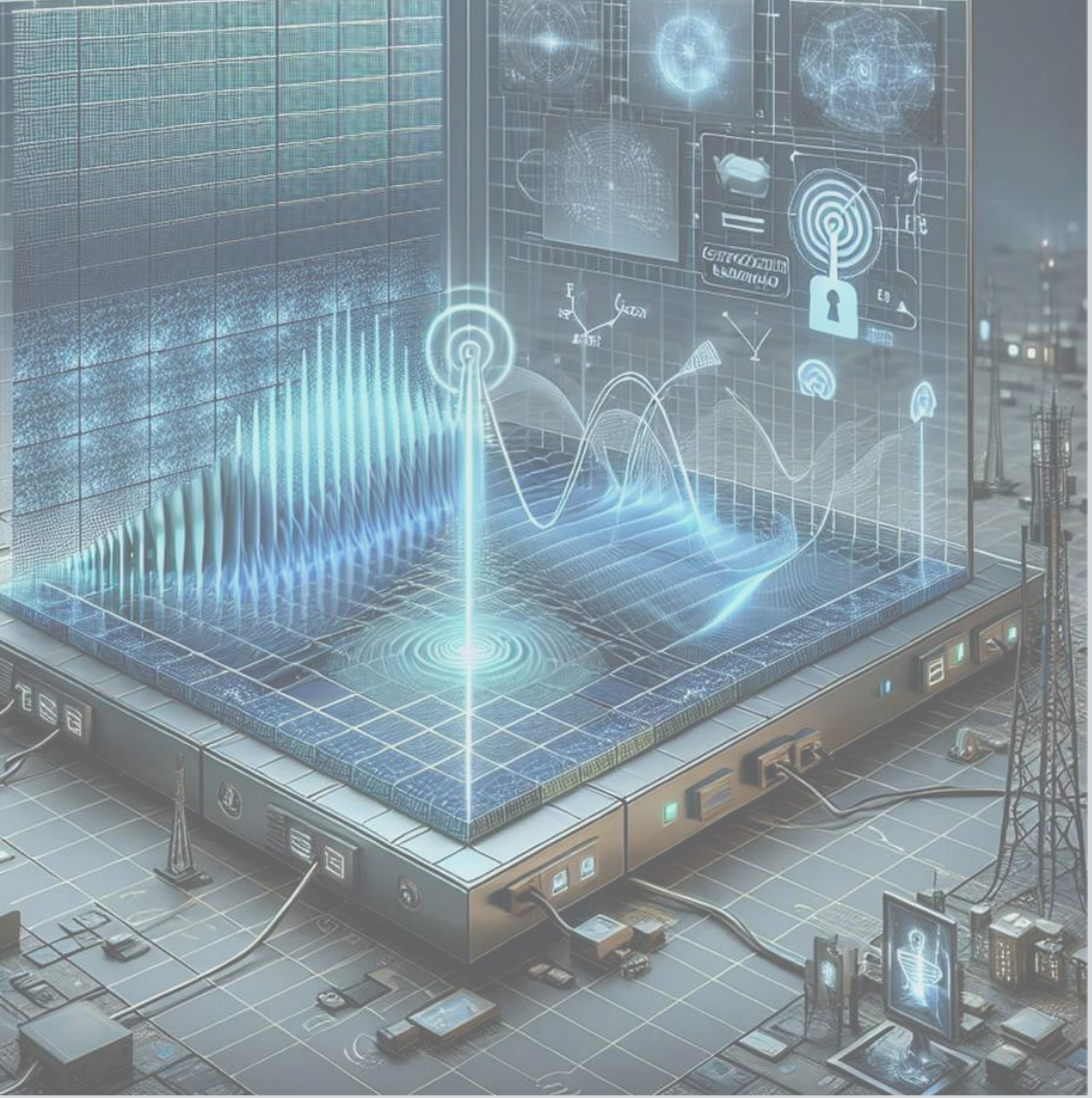

Figure 7: Comparison of 3 configurations regarding entropy vs. BMR

# Conclusion and Outlook

- A study on physical layer key generation enhanced by RIS.
- RIS can enhance overall system entropy and key generation.
- Performance comparison between different RIS configurations
- Trade-off between entropy and reliability (BMR) is critical.

Future work:

- Adaptive learning-based optimization.
- Non-symmetric quantization for improved entropy.
- Dynamic RIS reconfiguration in mobile or obstructed scenarios.




Deutsches Forschungszentrum für Künstliche Intelligenz
*German Research Center for Artificial Intelligence*

Rheinland-Pfälzische Technische Universität Kaiserslautern Landau


# Enhancing Physical Layer Key Generation Leveraging Reconfigurable Intelligent Surfaces


**Wenqing.Dai@dfki.de**