Reliable Shared Secret Extraction through OTFS

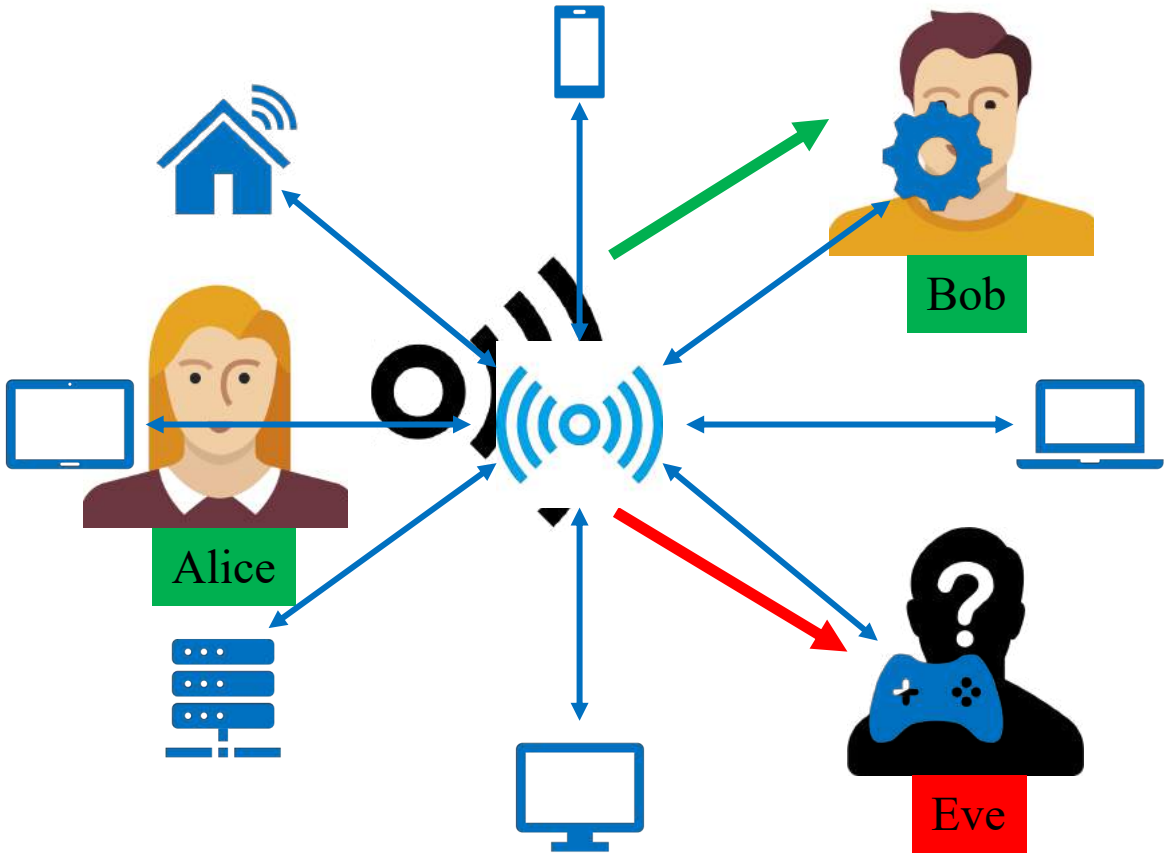
Usama Saeed

Virginia Tech
PhD Advisor: Dr. Lingjia Liu

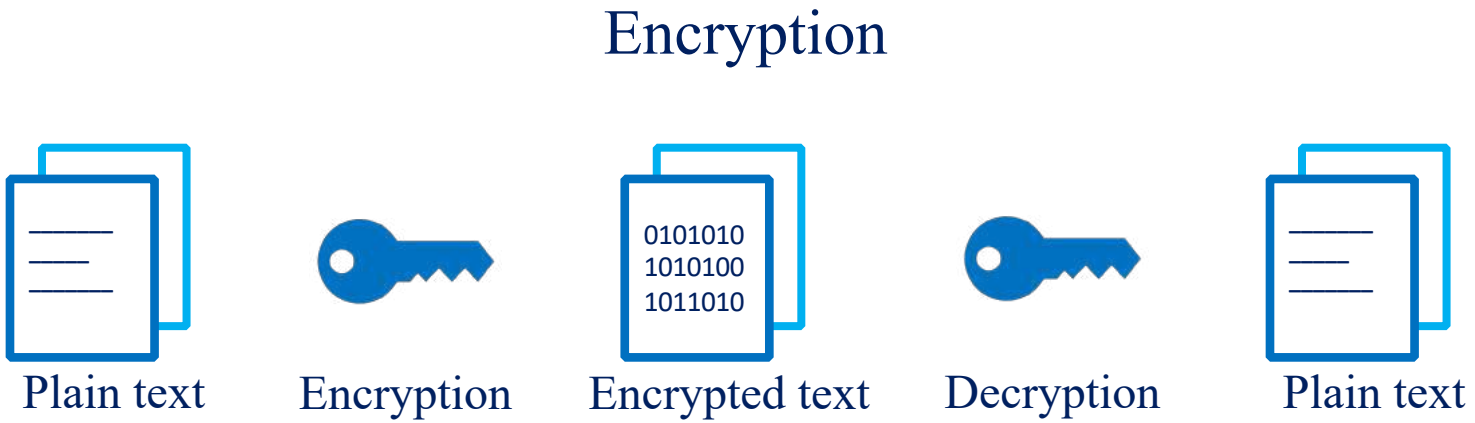
In collaboration with Dr. Kai Zeng (GMU) and Dr. Robert Calderbank (Duke)

Security Risk in Wireless Communication

- Massive number of wireless devices
- Broadcast medium inherently vulnerable
- Security requirement for wireless communications



How to Make Communications Secure?



- Encryption using cryptographic keys
- Keys known to legitimate users, unknown to attackers
- Secret keys are required

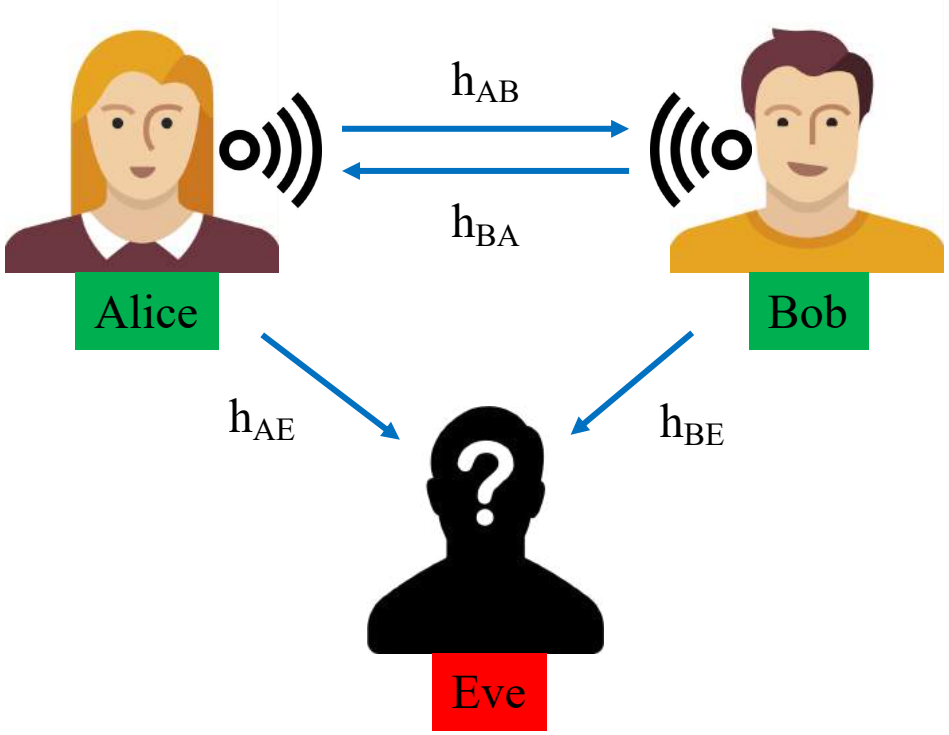
Key Generation – Application Layer Approach

- Key generated by solving computationally intractable problem (Eve cannot solve)
- Example: Diffie-Hellman (D-H) key exchange
- Drawbacks:
  - Significant computational overhead (even for legitimate nodes)
  - Ever-increasing capabilities of attacker – increased key length requirement

- Alternative: Physical layer key generation

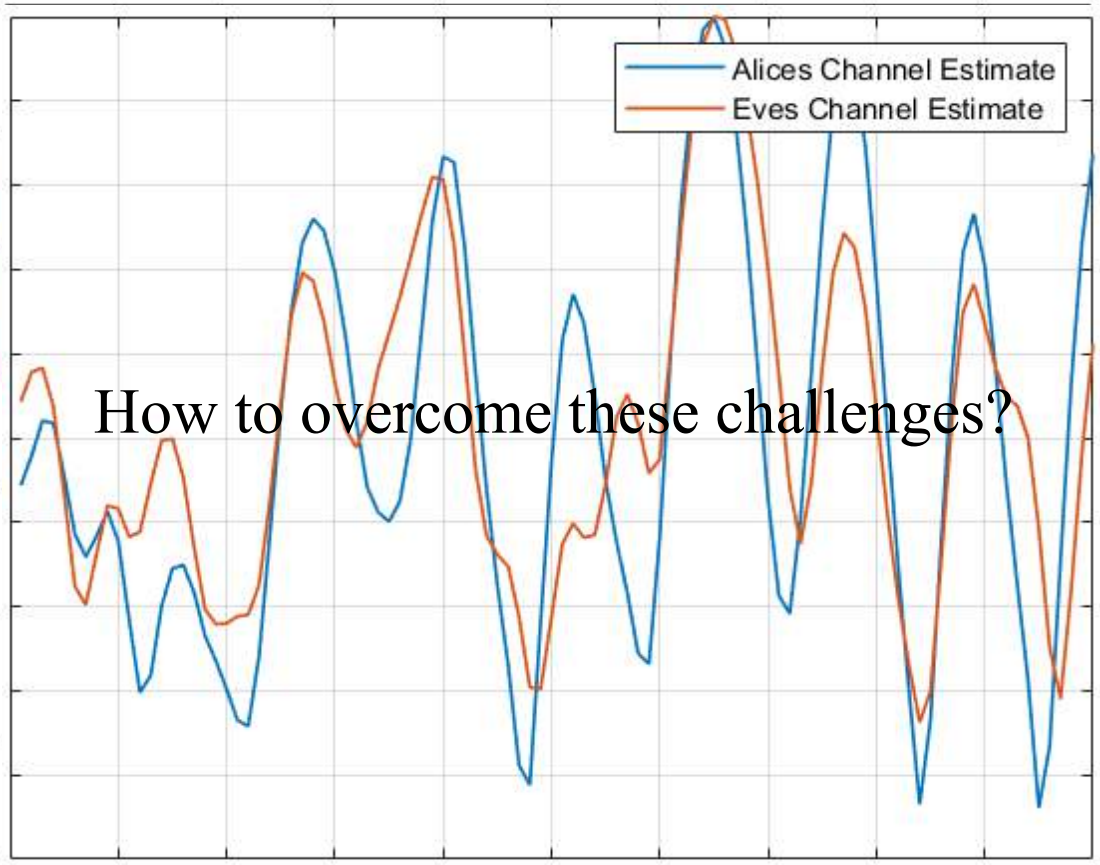
Key Generation – Physical Layer Approach

- Keys (independently) generated using channel measurements if
  - $h_{AB} \approx h_{BA}$
  - $h_{AE} \neq h_{AB}$ and $h_{BE} \neq h_{AB}$
- Benefits:
  - No assumptions on attackers' computational capability
  - Lower computational overhead



Challenge in Physical Layer Key Generation

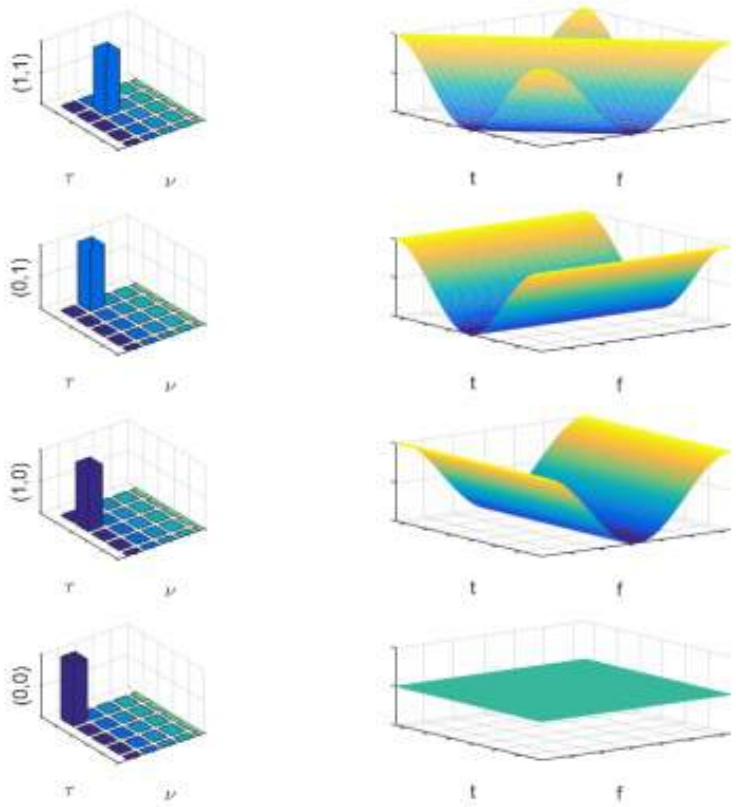
- Challenges:
  - $h_{AB} \not\approx h_{BA}$
  - h_{AE} and h_{BE} have high correlations with h_{AB}
- Causes:
  - Rapidly varying channels
  - Channel estimation accuracy
  - Correlation between Eve's and Alice/Bob's channels



How to overcome these challenges?

OTFS Modulation: An Overview

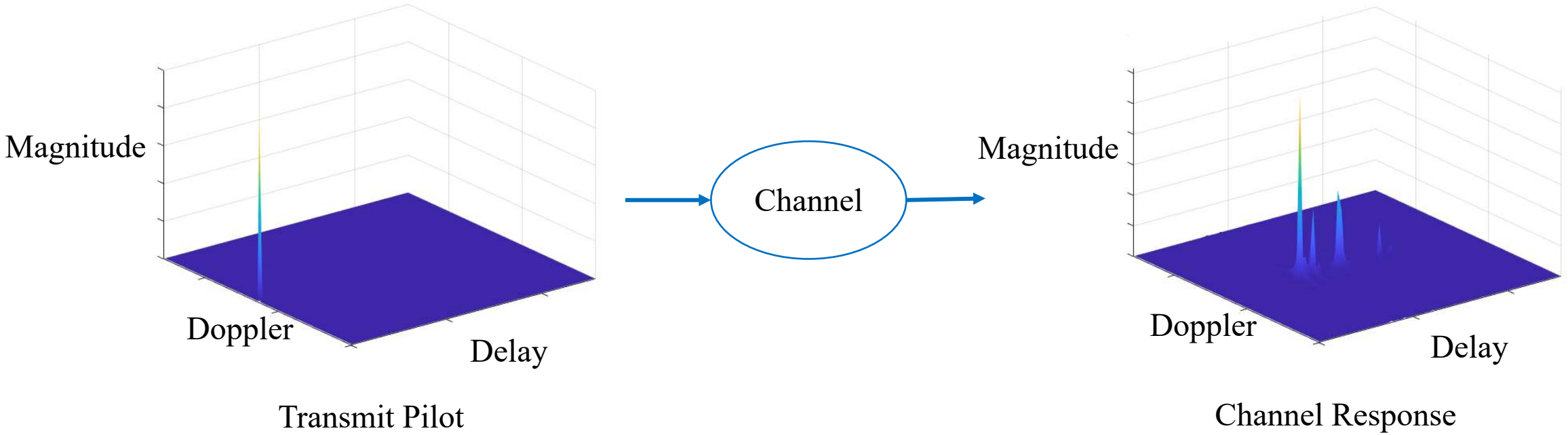
- Orthogonal Time Frequency and Space
- 2D modulation scheme
  - Basis functions span bandwidth and time duration transmission
- Resides in the delay-Doppler coordinate system
  - Mirrors geometry of wireless channel
  - Each path corresponds to a spike



Mapping from delay-Doppler to time-frequency domain [1]

[1] A. Monk, R. Hadani, M Tsatsanis and S Rakib, "OTFS - Orthogonal Time Frequency Space", 2016, arXiv: 1608.02993

OTFS Modulation: Channel Representation



Transmit Pilot

Channel Response

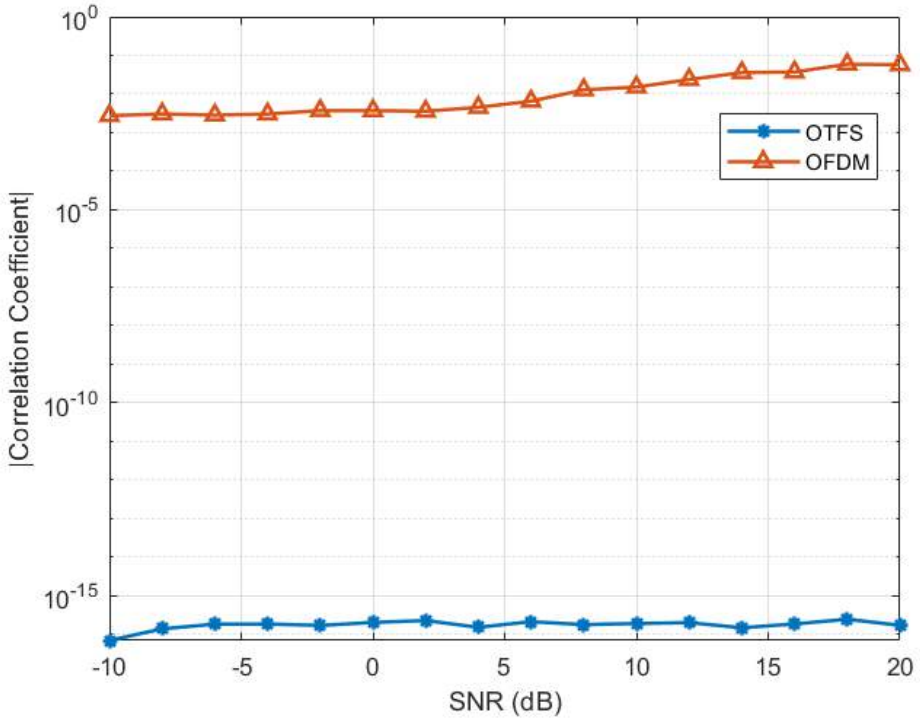
Sparse delay-Doppler domain grid

Spikes represent channel geometry

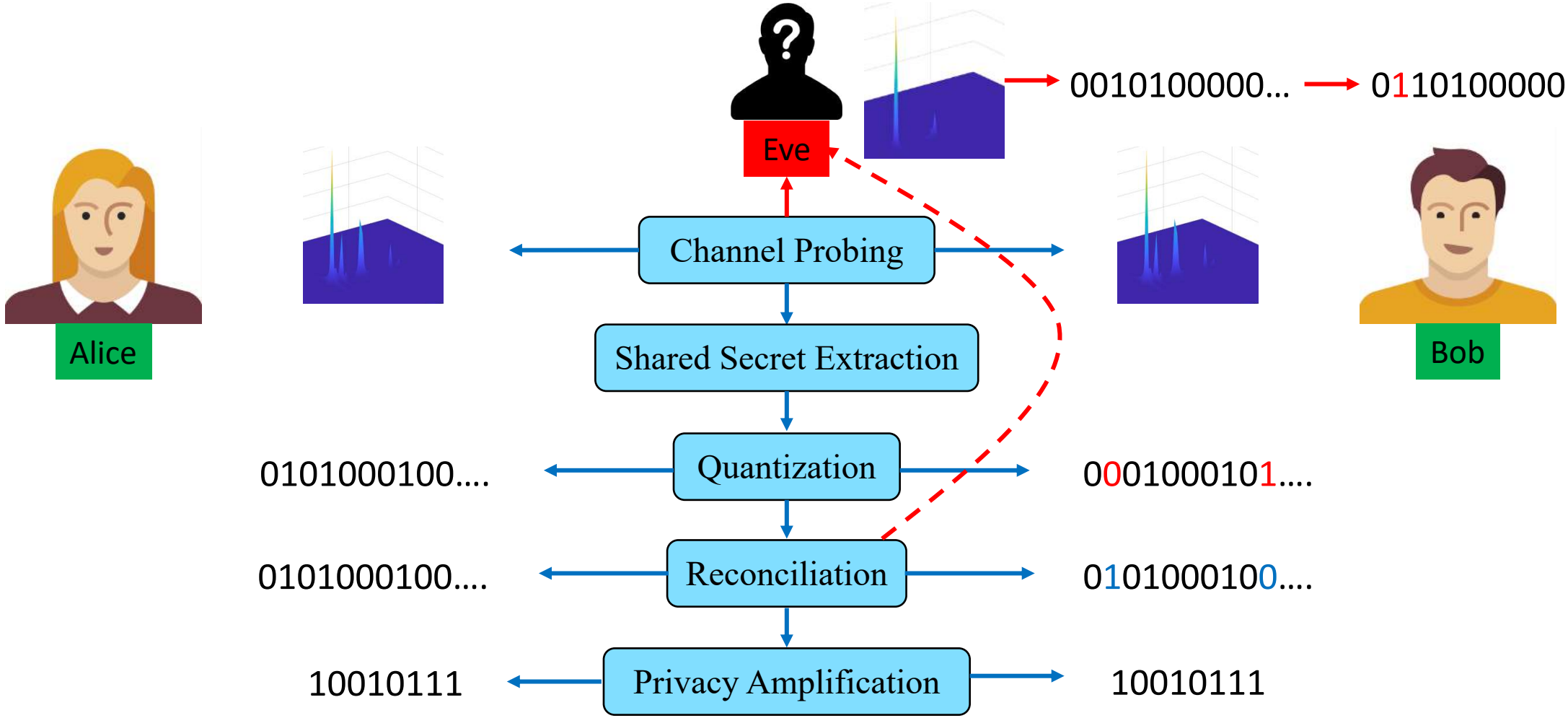
How does that help us?

OTFS Based Key Generation: Motivation

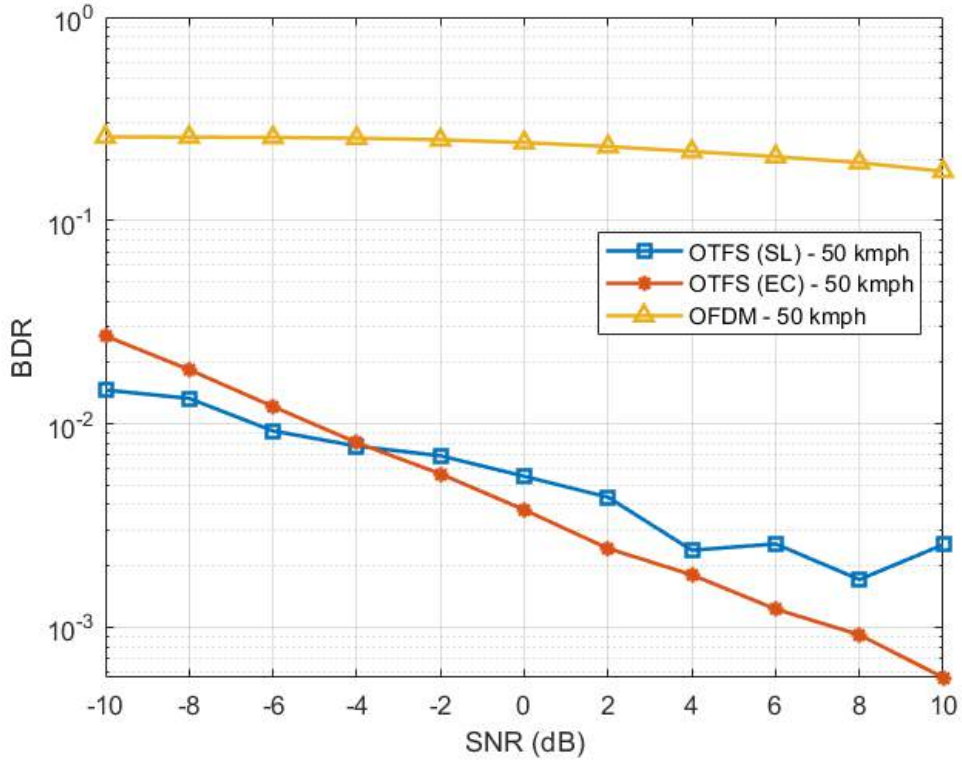
- Existing challenges:
  - Rapidly varying channel
  - Channel estimation accuracy
  - Correlation with Eve's channel
- OTFS solutions:
  - Time-invariant channel representation
  - Localized signal power
  - Channel representation mirrors scatterer geometry



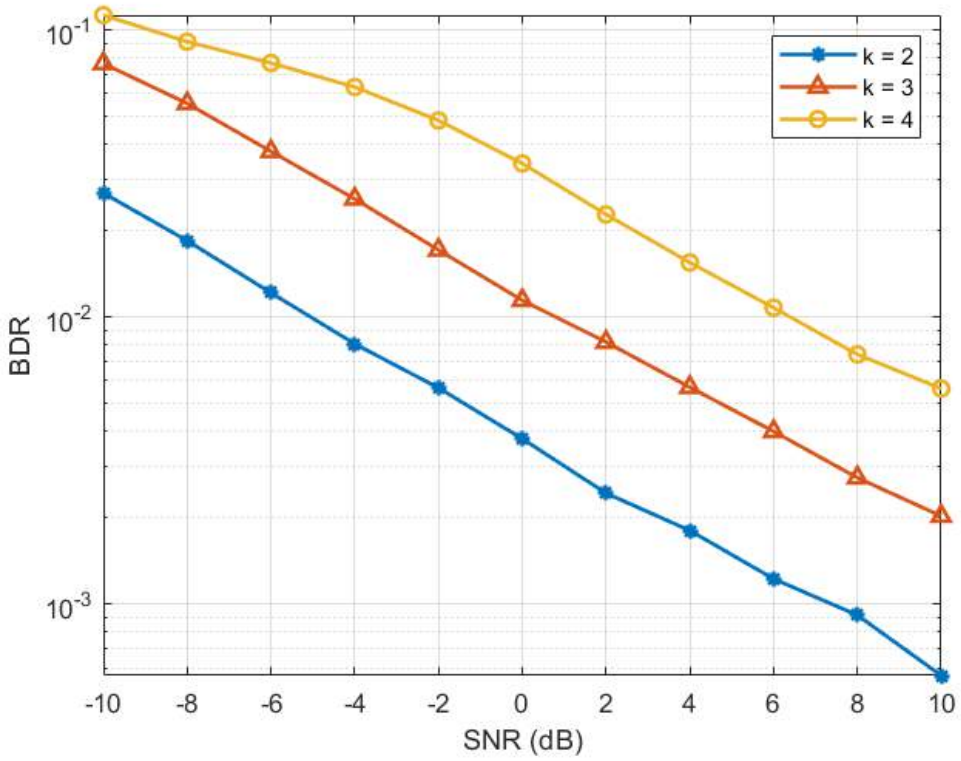
OTFS Based Key Generation: Overview



Results: Bit Disagreement Ratio

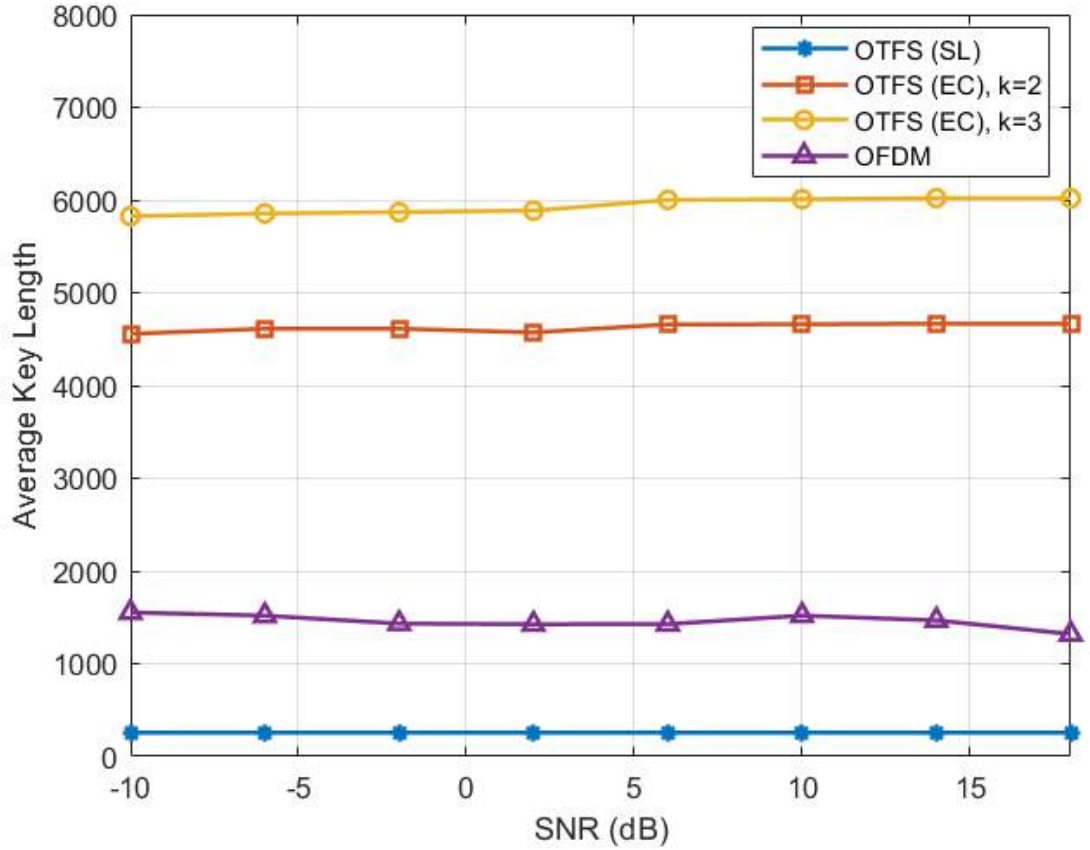


BDR between quantized channel estimates at Alice and Bob



BDR for different quantization levels for OTFS

Results: Key Length



Key length comparison for OTFS methods and OFDM

Thank you!