

# Currently?: LLM and GNN Security and Applications

## Tools

RAG

In-Context  
Learning

Prompt  
Optimization

Predictive  
Modeling

Question  
Answering

Hardware  
Design  
Automation

## Applications

## Security

Secure Code  
Generation

Adversarial  
Attack and  
Defense

Deepfake  
Detection

Internet  
Security

Channel  
estimation

Spectrum  
Sensing

Physical  
Layer  
Security

## Past: ML for Comminutions