FMCP 2024 presentation proposal

Title: AI-assisted Formal Method Verifications on Cryptographic Designs and Implementations

Abstract: This presentation explores the integration of artificial intelligence (AI) with formal methods to verify cryptographic designs and implementations. We will discuss how AI can enhance the efficiency and accuracy of formal verification processes, which are crucial for ensuring the security and correctness of cryptographic systems. The talk will cover recent advancements, case studies, and future research directions in this emerging field.

Introduction: Cryptographic systems are foundational to the security of digital communications, transactions, and data storage. Ensuring their correctness and security through formal verification is critical but often complex and time-consuming. AI-assisted formal methods offer a promising solution by automating and enhancing the verification process, thereby improving both efficiency and reliability. This presentation aims to provide an in-depth look at how AI is transforming formal verification in cryptography.

Objectives:

- To explain the importance of formal verification in cryptographic design and implementation.
- To demonstrate how AI techniques can be integrated with formal methods to improve verification processes.
- To present case studies showcasing successful AI-assisted formal verifications.
- To discuss the challenges and future directions in this research area.

Methodology/Approach: Our approach involves a comprehensive review of current AI techniques and their applications in formal method verifications. We will analyse case studies where AI has been successfully implemented to verify cryptographic systems. Additionally, we will present insights from recent research and experiments conducted in this field. The presentation will utilize a combination of slides, visual aids, and interactive discussions to engage the audience.

Content Outline:

1. **Introduction to Formal Methods in Cryptography**
   - Definition and significance
   - Traditional challenges in formal verifications
2. **AI Techniques in Formal Verification**
   - Overview of relevant AI techniques (e.g., machine learning, neural networks)
   - How AI can be applied to formal methods
3. **Case Studies of Formal Verification Tools for cryptography**
   - Example 1: Formal Verifiers with non or limited AI assistance

    - Example 2: AI-assisted formal verifiers
    - Lessons learned and best practices.
4. **Challenges and Considerations**
    - Limitations of current AI techniques
    - Training data development.
5. **Future Directions**
    - Emerging trends in AI and formal methods
    - Potential research areas and innovations

Conclusion and Implications: AI-assisted formal verification represents a significant advancement in ensuring the security and correctness of cryptographic systems. By automating complex verification processes, AI not only enhances efficiency but also reduces the likelihood of human error. This presentation will provide attendees with a comprehensive understanding of this innovative approach, its current applications, and future potential.

Bio: Dr. Long Ngo holds a Ph.D. in cryptographic security and formal verification. As an engineer at TeronLabs, he specializes in evaluating the security design and implementation of IT systems. Long leads research and development projects focused on AI-assisted security verification and vulnerability exploration tools, leveraging his expertise to advance cybersecurity solutions.