


# THÔNG TIN CHUNG CỦA BÁO CÁO

- Link YouTube video của báo cáo (tối đa 5 phút):  
<https://youtu.be/A6guSqlapTA>
- Link slides (dạng .pdf đặt trên Github):  
<https://github.com/haova/CS2205.APR2023>
- *Mỗi thành viên của nhóm điền thông tin vào một dòng theo mẫu bên dưới*
- *Sau đó điền vào Đề cương nghiên cứu (tối đa 5 trang), rồi chọn Turn in*

<ul style="list-style-type: none"><li>• Họ và Tên: Vũ Anh Hào</li><li>• MSSV: 220202014</li></ul> 	<ul style="list-style-type: none"><li>• Lớp: CS2205.APR2023</li><li>• Tự đánh giá (điểm tổng kết môn): 8/10</li><li>• Số buổi vắng: 2</li><li>• Số câu hỏi QT cá nhân: 2</li><li>• Số câu hỏi QT của cả nhóm: 0</li><li>• Link Github: <a href="https://github.com/haova/CS2205.APR2023">https://github.com/haova/CS2205.APR2023</a></li><li>• Mô tả công việc và đóng góp của cá nhân cho kết quả của nhóm:<ul style="list-style-type: none"><li>○ Lên ý tưởng đề tài</li><li>○ Viết nội dung đề cương, báo cáo</li><li>○ Thiết kế poster</li><li>○ Làm video YouTube</li></ul></li></ul>
--	--

# ĐỀ CƯƠNG NGHIÊN CỨU

## TÊN ĐỀ TÀI (IN HOA)

XÁC THỰC DỰA TRÊN CHỨNG MINH KHÔNG CÓ KIẾN THỨC THỂ HỆ TIẾP THEO CHO MẠNG CẢM BIẾN KHÔNG DÂY SỬ DỤNG GIẢI PHÁP DỰA TRÊN LƯỚI

## TÊN ĐỀ TÀI TIẾNG ANH (IN HOA)

NEXT-GENERATION ZERO-KNOWLEDGE PROOF-BASED AUTHENTICATION FOR WIRELESS SENSOR NETWORKS USING LATTICE-BASED SOLUTIONS

## TÓM TẮT *(Tối đa 400 từ)*

Trong một xã hội ngày càng phổ biến Internet vạn vật nói chung và mạng cảm biến không dây nói riêng, việc gia tăng các nguy cơ mất an toàn thông tin là điều không thể tránh khỏi [1]. Trong đó, các thông tin nhạy cảm được lưu trữ ở cảm biến dễ dàng bị đánh cắp hoặc giả mạo [2]. Vì vậy, xác thực là một quá trình cần thiết để đảm bảo tính hợp lệ của các nút cảm biến cũng như an toàn cho dữ liệu. Tuy nhiên, các thiết bị cảm biến có những đặc thù riêng: khả năng tính toán và lưu trữ thấp, kết nối không dây, môi trường triển khai không an toàn, số lượng triển khai lớn. Do đó, chúng cần những kỹ thuật xác thực vừa gọn nhẹ lại vừa đảm bảo an toàn [3].

Đề tài này sẽ đề xuất một mô hình bảo mật hiệu quả hơn trong quá trình xác thực giữa các nút cảm biến và trạm của mạng cảm biến không dây. Trong đó kỹ thuật được sử dụng là Chứng minh không có kiến thức (Zero-knowledge Proof). Từ đó, có thể đảm bảo hệ thống an toàn dưới mối đe dọa của ba loại tấn công phổ biến của mạng cảm biến không dây: Clone Attack, Man in the Middle Attack và Replay Attack [4]. Hơn nữa, dưới áp lực của thời đại, đề tài ứng dụng giải pháp lưới (lattice-based) để đảm bảo an toàn cho hệ thống xác thực trước những mối đe dọa của tấn công lượng tử [5]. Đây chính là những điểm mới mà đề tài mong muốn đạt được.

## **GIỚI THIỆU** (Tối đa 1 trang A4)

Trong hệ thống mạng cảm biến không dây (Wireless Sensor Network - WSN), các nút cảm biến rất dễ bị tấn công. Khả năng tính toán và lưu trữ hạn chế khiến chúng trở thành mục tiêu tấn công. Kết nối không dây dễ bị giả mạo. Môi trường triển khai các nút cảm biến không an toàn [2]. Do đó, quá trình xác thực đóng vai trò quan trọng trong việc định danh và phát hiện những tấn công giả mạo vào hệ thống [4].

Zero-knowledge Proof (ZKP) có thể giải quyết được nhiều vấn đề bảo mật của WSN [6]. Bằng cách sử dụng các mô hình toán học, ZKP cho phép chứng minh tính đúng đắn của một thông tin mà không cần phải tiết lộ nội dung của thông tin đó [7]. Trong trường hợp của WSN, ZKP có thể được sử dụng để xác thực tính toàn vẹn và nguồn gốc của dữ liệu thu thập từ các nút cảm biến, đảm bảo rằng dữ liệu không bị giả mạo trong quá trình truyền tải. Đối với các nút cảm biến, chúng có thể chứng minh rằng mình có thông tin chính xác mà không cần tiết lộ dữ liệu thực tế, từ đó bảo vệ được tính toàn vẹn của dữ liệu. Đối với trạm, có thể xác minh được các nút hợp lệ và có quyền truy cập hệ thống, ngăn chặn các nút cảm giả mạo hoặc không được ủy quyền.

Các giải pháp dựa trên lưới (lattice-based) có thể ngăn chặn các cuộc tấn công lượng tử [5]. Trước thuật toán Shor - thuật toán lượng tử mạnh mẽ có thể phân tích một số nguyên bất kỳ thành thừa số nguyên tố - lattice-based không bị ảnh hưởng. Trước những thuật toán lượng tử khác, như giải thuật giải thuật Grover - thuật toán lượng tử tìm kiếm nhanh - mật mã lattice-based cũng được chứng minh là có khả năng chống lại. Hơn nữa, mật mã dựa trên lưới không chỉ chống lại máy tính lượng tử mà còn đảm bảo các máy tính thông thường an toàn. Điều này có ý nghĩa quan trọng trong quá trình chuyển từ hệ thống truyền thống sang hệ thống chống máy tính lượng tử.

ZKP dựa trên lattice-based được xem là state-of-the-art trong việc chống lại các tấn công từ máy tính thông thường và máy tính lượng tử. Với tiềm năng phát triển trong tương lai, và nhu cầu cần một hệ thống với quá trình xác thực ổn định, ZKP dựa trên lattice-based trở thành một lựa chọn an toàn và bền vững trong IoT và WSN.

## MỤC TIÊU

*(Viết trong vòng 3 mục tiêu, lưu ý về tính khả thi và có thể đánh giá được)*

- Đề xuất mô hình bảo mật cho hệ thống Mạng cảm biến không dây với trung tâm là việc xác thực Zero-knowledge Proof dựa trên Lattice giữa các nút cảm biến và trạm.
- Đánh giá tính hiệu quả của hệ thống trong việc ngăn chặn các cuộc tấn công thường thấy trong hệ thống Mạng cảm biến không dây là: Clone Attack, Man in the Middle Attack và Reply Attack.
- Đánh giá tính hiệu quả của hệ thống trong việc ngăn chặn các cuộc tấn công lượng tử: Shor, Grover.

## NỘI DUNG VÀ PHƯƠNG PHÁP

*(Viết nội dung và phương pháp thực hiện để đạt được các mục tiêu đã nêu)*

### **Mô hình bảo mật cho hệ thống Mạng cảm biến không dây.**

- Nghiên cứu, tìm hiểu các bài báo khoa học liên quan đến lĩnh vực Internet vạn vật và Mạng cảm biến không dây để đảm bảo hệ thống được xây dựng là state-of-the-art.
- Thiết kế một mạng cảm biến không dây thu thập thông tin thời tiết bao gồm các nút cảm biến, trạm (base station) và máy chủ trung tâm để lưu trữ dữ liệu.
- Giả lập hệ thống WSN đã được thiết kế trên máy ảo để kiểm tra tính khả thi của mô hình được thiết kế.
- Xây dựng một hệ thống WSN trên thiết bị thật, trong đó các nút cảm biến sử dụng mạch điều khiển Arduino được kết nối với các cảm biến thời tiết như nhiệt độ, độ ẩm, lượng mưa,... Giao tiếp với trạm thông qua bộ truyền LoRA. Trạm là một bộ máy tính mini Raspberry PI, có chức năng xác thực các nút cảm biến kết nối trực tiếp tới trạm.
- Các nút cảm biến cần mang thông tin định danh (id), fingerprint của chính nó và một số thông tin về các nút lân cận nhằm phục vụ cho việc chứng minh.

- Đảm bảo hệ thống WSN hoạt động bình thường.

### **Đánh giá hiệu quả trong việc ngăn chặn các cuộc tấn công thường thấy**

Xây dựng và thử nghiệm một số kịch bản tấn công vào hệ thống WSN để kiểm chứng hệ thống trong thực tế.

- Clone Attack - tạo một nút cảm biến giả mạo với dữ liệu bên trong được sao chép từ một nút cảm biến trong mạng thật bất kì. Sau đó kích hoạt nút để nó giao tiếp với mạng. Bởi vì việc sao chép một nút sẽ khiến cho một số “kiến thức” về môi trường và các nút xung quanh xuất hiện sai lầm, dẫn đến verifier ở phía trạm có thể dễ dàng từ chối xác thực và xác định được vị trí xảy ra lỗi.
- Man-In-The-Middle Attack - tạo một thiết bị lắng nghe tín hiệu LoRa từ các nút cảm biến phát ra và từ trạm phát ra. Bởi vì sử dụng ZKP, nên không có thông tin nhạy cảm nào của quá trình xác thực được truyền ra bên ngoài, nên thiết bị lắng nghe không thể thu thập được dữ liệu thật.
- Replay Attack - cố gắng lặp lại các thông tin kết nối của tín hiệu LoRa đến trạm và ngược lại. Bởi vì các kết nối xác thực luôn khác nhau nên dễ dàng bị trạm phát hiện và từ chối dựa trên kỹ thuật ZKP.

Sau khi thử nghiệm các cuộc tấn công, đưa ra kết luận ban đầu về tính an toàn của hệ thống.

Sử dụng các logic toán và mô hình toán để chứng minh tính an toàn của hệ thống và đưa ra kết luận đầy đủ.

### **Đánh giá hiệu quả trong việc ngăn chặn các cuộc tấn công lượng tử**

Sử dụng các phương trình toán để phân tích, chứng minh tính đúng đắn của hệ thống khi đối mặt với các cuộc tấn công lượng tử.

### **KẾT QUẢ MONG ĐỢI**

*(Viết kết quả phù hợp với mục tiêu đặt ra, trên cơ sở nội dung nghiên cứu ở trên)*

- Xây dựng được hệ thống Mạng cảm biến không dây thật với trung tâm là xác thực Zero-knowledge Proof dựa trên Lattice giữa các nút cảm biến và trạm.
- Hệ thống ngăn chặn và phát hiện các cuộc tấn công thường thấy trong hệ thống Mạng cảm biến không dây: Clone Attack, Man in the Middle Attack và Reply Attack.
- Hệ thống hiệu quả trong việc ngăn chặn các cuộc tấn công lượng tử: Shor, Grover.

### **TÀI LIỆU THAM KHẢO** (*Định dạng DBLP*)

- [1] Arbia Riahi, Enrico Natalizio, Yacine Challal, Zied Chtourou:  
A roadmap for security challenges in the Internet of Things. Digit. Commun. Networks 4(2): 118-137 (2018)
- [2] Fangmin Sun, Zhan Zhao, Zhen Fang, Lidong Du, Zhihong Xu, Diliang Chen:  
A Review of Attacks and Security Protocols for Wireless Sensor Networks. J. Networks 9(5): 1103-1113 (2014)
- [3] Poornima M. Chanal, Mahabaleshwar S. Kakkasageri:  
Security and Privacy in IoT: A Survey. Wirel. Pers. Commun. 115(2): 1667-1693 (2020)
- [4] Siba K. Udgate, Alefiah Mubeen, Samrat L. Sabat:  
Wireless Sensor Network Security Model Using Zero Knowledge Protocol. ICC 2011: 1-5
- [5] Vadim Lyubashevsky, Ngoc Khanh Nguyen, Maxime Plançon:  
Lattice-Based Zero-Knowledge Proofs and Applications: Shorter, Simpler, and More General. CRYPTO (2) 2022: 71-101
- [6] Francisco Martín-Fernández, Pino Caballero-Gil, Cándido Caballero-Gil:  
Authentication Based on Non-Interactive Zero-Knowledge Proofs for the Internet of Things. Sensors 16(1): 75 (2016)
- [7] Feng Li, Bruce M. McMillin:  
A Survey on Zero-Knowledge Proofs. Adv. Comput. 94: 25-69 (2014)

