โครงงานเลขที่ วศ.คพ. S054-1/2568

เรื่อง

การใช้สมการสมดุลของแนชกับความมั่นคงความปลอดภัยทางไซเบอร์ในกลศาสตร์ควอนตัม

โดย

นางสาวกนลลัส รัตนภาค รหัส 650610743
นางสาวแก้วตา ลุงต๊ะ รหัส 650610750
นายธีระพันธุ์ พันธุ์วรรธนะสิน รหัส 650610773

โครงงานนี้
เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญาวิศวกรรมศาสตรบัณฑิต
ภาควิชาวิศวกรรมคอมพิวเตอร์
คณะวิศวกรรมศาสตร์ มหาวิทยาลัยเชียงใหม่
ปีการศึกษา 2568

PROJECT No. CPE S054-1/2568

Achieving a Nash-equilibrium in cyberseecurity quantum mechanically

Kanonlas Rattanapak 650610743

Kaewtar Lungta 650610750

Theeraphan Phanwattanasin 650610773

A Project Submitted in Partial Fulfillment of Requirements

for the Degree of Bachelor of Engineering

Department of Computer Engineering

Faculty of Engineering

Chiang Mai University

2025

หัวข้อโครงงาน	: การใช้สมการสมดุลของแนชกับความมั่นคงความปลอดภัยทางไซเบอร์ในกลศาสตร์ควอนตัม	
	: Achieving a Nash-equilibrium in cyberseecurity quantum mechanically	
โดย	: นางสาวกนลลัส รัตนภาค	รหัส 650610743
	นางสาวแก้วตา ลุงต๊ะ	รหัส 650610750
	นายธีระพันธุ์ พันธุ์วรรธนะสิน	รหัส 650610773
ภาควิชา	: วิศวกรรมคอมพิวเตอร์	
อาจารย์ที่ปรึกษา	: รศ.ดร. สรรพวรรธน์ กันตะบุตร	
ปริญญา	: วิศวกรรมศาสตรบัณฑิต	
สาขา	: วิศวกรรมคอมพิวเตอร์	
ปีการศึกษา	: 2568	

ภาควิชาวิศวกรรมคอมพิวเตอร์ คณะวิศวกรรมศาสตร์ มหาวิทยาลัยเชียงใหม่ ได้อนุมัติให้โครงงานนี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญาวิศวกรรมศาสตรบัณฑิต (สาขาวิศวกรรมคอมพิวเตอร์)

..... หัวหน้าภาควิชาวิศวกรรมคอมพิวเตอร์
(รศ.ดร. สันติ พิทักษ์กิจนุกูร)

คณะกรรมการสอบโครงงาน

..... ประธานกรรมการ
(รศ.ดร. สรรพวรรธน์ กันตะบุตร)

..... กรรมการ
(ผศ.ดร. นวดนย์ คุณเลิศกิจ)

..... กรรมการ
(รศ.ดร. สันติ พิทักษ์กิจนุกูร)

..... กรรมการ
(ผศ.ดร. วรานนท์ อนุกูล)

หัวข้อโครงงาน	: การใช้สมการสมดุลของแนชกับความมั่นคงความปลอดภัยทางไซเบอร์ในกลศาสตร์ควอนตัม	
	: Achieving a Nash-equilibrium in cyberseecurity quantum mechanically	
โดย	: นางสาวกนลลัส รัตนภาค	รหัส 650610743
	นางสาวแก้วตา ลุงต๊ะ	รหัส 650610750
	นายธีระพันธุ์ พันธุ์วรรธนะสิน	รหัส 650610773
ภาควิชา	: วิศวกรรมคอมพิวเตอร์	
อาจารย์ที่ปรึกษา	: รศ.ดร. สรรพวรรธน์ กันตะบุตร	
ปริญญา	: วิศวกรรมศาสตรบัณฑิต	
สาขา	: วิศวกรรมคอมพิวเตอร์	
ปีการศึกษา	: 2568	

บทคัดย่อ

โครงงานนี้จัดทำขึ้นเพื่อนำเสนอการประยุกต์ใช้ทฤษฎีเกมและการคำนวณเชิงควอนตัม โดยนำไปแก้ไขปัญหาด้านความมั่นคงปลอดภัยไซเบอร์ ซึ่งมองจากสองมุมมองหลัก อันได้แก่ ฝ่ายป้องกันและฝ่ายโจมตี ภายใต้บริบทของทฤษฎีเกม โดยสมมติให้ผู้เล่นทั้งสองฝ่ายประกอบไปด้วย ผู้ป้องกัน และ ผู้โจมตี

โครงงานนี้ได้พัฒนารูปแบบของระบบความมั่นคงปลอดภัยไซเบอร์แบบหลายชั้น ผ่านรูปแบบโครงสร้างต้นไม้ (tree) จากทฤษฎีกราฟ ซึ่งโหนดแต่ละจุดจะแทนรางวัลหรือข้อมูลที่ผู้โจมตีจะได้รับหลังจากเลือกโหนดนั้น และผู้ป้องกันต้องปกป้องแต่ละโหนดโดยการลดจำนวนรางวัลที่ผู้โจมตีจะได้รับ และเส้นเชื่อม (edge) จะแทนต้นทุนที่ใช้ในการโจมตีเพื่อเข้าถึงรางวัลนั้น ๆ หลังจากนั้นจะทำการศึกษาและวิเคราะห์ปัญหาต่าง ๆ บนแบบจำลองดังกล่าว พร้อมทั้งประยุกต์ใช้แนวคิด ดุลยภาพแนช (Nash Equilibrium) และประมวลผลของผลลัพธ์ด้วยกระบวนการ ควอนตัมแอนนีลลิง (Quantum Annealing) เพื่อหาคำตอบที่เหมาะสมที่สุดสำหรับปัญหาในแบบจำลอง

Project Title	: Achieving a Nash-equilibrium in cyberseecurity quantum mechanically	
Name	: Kanonlas Rattanapak	650610743
	Kaewtar Lungta	650610750
	Theeraphan Phanwattanasin	650610773
Department	: Computer Engineering	
Project Advisor	: Assoc. Prof. Sanpawat Kantabutra, Ph.D.	
Degree	: Bachelor of Engineering	
Program	: Computer Engineering	
Academic Year	: 2025	

ABSTRACT

This project is conducted to present the application of game theory and quantum computation to address cybersecurity issues from two main perspectives: the defender and the attacker, within the framework of game theory. The model assumes two players, namely the defender and the attacker.

The project develops a multi-layered cybersecurity system represented through a tree structure based on graph theory. Each node represents a reward or information that the attacker may obtain upon selecting that node, while the defender's role is to protect each node by reducing the rewards accessible to the attacker. The edges represent the costs incurred by the attacker to reach the corresponding rewards. Subsequently, the project investigates and analyzes problems within this model, applying the concept of Nash Equilibrium and leveraging Quantum Annealing to process the results. This approach aims to determine the optimal solution for the modeled problem.

กิตติกรรมประกาศ

โครงงานนี้สำเร็จลุล่วงได้ด้วยความกรุณาและการสนับสนุนจากหลายฝ่ายทั้งคณาจารย์ และเพื่อนร่วมงาน ผู้จัดทำขอ กราบขอบพระคุณอาจารย์ที่ปรึกษา ซึ่งได้ให้คำแนะนำ ความรู้ และแนวทางในการดำเนินงานอย่างต่อเนื่อง ทำให้ผู้จัดทำสามารถพัฒนาโครงงานได้อย่างมีประสิทธิภาพ นอกจากนี้ยังขอขอบพระคุณคณาจารย์ทุกท่านที่ได้ถ่ายทอดความรู้และทักษะที่จำเป็นในการจัดทำโครงงาน รวมทั้งเพื่อนร่วมชั้นเรียนที่ให้ข้อเสนอแนะและกำลังใจตลอดระยะเวลาการทำงานและสุดท้ายนี้ ขอขอบพระคุณทุกท่านที่มีส่วนเกี่ยวข้องในการทำโครงงานครั้งนี้ไม่ว่าจะทางตรงหรือทางอ้อม

นางสาวกนลลัส รัตนภาค
นางสาวแก้วตา ลุงต๊ะ
นายธีระพันธุ์ พันธุ์วรรธนะสิน
3 ตุลาคม 2568

สารบัญ

สารบัญรูป

สารบัญตาราง

บทที่ 1
บทนำ

1.1 ที่มาของโครงงาน

ระบบคอมพิวเตอร์และเครือข่ายอินเทอร์เน็ตที่ใช้งานโดยทั่วไปก็มีบทบาทสำคัญต่อทุกภาคส่วนของสังคม แต่ในขณะเดียวกัน ความมั่นคงปลอดภัยทางไซเบอร์ (Cybersecurity) ก็กลายเป็นความท้าทายประการหนึ่ง ซึ่งมีความซับซ้อนและยากต่อการจัดการ อันเนื่องจากผู้โจมตีมักจะพัฒนากลยุทธ์ใหม่ ๆ อยู่อย่างเสมอ เพื่อนำมาแทรกแซงระบบซอฟต์แวร์ที่ถูกพัฒนาขึ้นมาใหม่ตามกาลเวลา ทำให้ในขณะเดียวกันนั่นเอง ผู้ป้องกันก็จำเป็นที่จะต้องหาวิธีการที่มีประสิทธิภาพในการรับมือ

โครงงานวิจัยนี้จึงนำเสนอการใช้ **ทฤษฎีเกม (Game Theory)** มาเป็นกรอบแนวคิดในการแก้ปัญหา โดยมองว่าการโจมตีและการป้องกันเป็นเกมที่มีผู้เล่นสองฝ่าย ได้แก่ **ผู้โจมตี (Attacker)** และ **ผู้ป้องกัน (Defender)**

นอกจากนี้ โครงงานยังมีการประยุกต์ใช้ **การคำนวณเชิงควอนตัม (Quantum Computing)** โดยเฉพาะการแก้ปัญหาแบบ **ควอนตัมแอนนีลลิง (Quantum Annealing)** เพื่อนำมาหาคำตอบที่เหมาะสมที่สุดในสถานการณ์ที่ซับซ้อน ซึ่งวิธีการนี้จะสามารถช่วยลดเวลาในการคำนวณและช่วยหาผลลัพธ์ที่มีประสิทธิภาพ กว่าการคำนวณแบบดั้งเดิม

1.2 วัตถุประสงค์ของโครงงาน

1. เพื่อสร้างความเข้าใจในการประยุกต์การใช้ทฤษฎีเกมกับปัญหาด้านความมั่นคงปลอดภัยไซเบอร์ ผ่านการออกแบบให้อยู่ในรูปสมการเชิงควอนตัม
2. เพื่อออกแบบแบบจำลองระบบความมั่นคงปลอดภัยไซเบอร์แบบหลายชั้น โดยใช้โครงสร้างต้นไม้ (Tree) จากทฤษฎีกราฟ
3. เพื่อประยุกต์ใช้แนวคิดดุลยภาพแนช (Nash Equilibrium) ในการวิเคราะห์ผลลัพธ์ของเกมระหว่างผู้โจมตีและผู้ป้องกันผ่านมูลค่าของผลลัพธ์ที่แต่ละฝ่ายได้รับ
4. เพื่อประยุกต์ใช้การคำนวณเชิงควอนตัมแบบ ควอนตัมแอนนีลลิง (Quantum Annealing) ในการแก้ปัญหาบนแบบจำลองโครงสร้างต้นไม้ที่สร้างขึ้น

1.3 ขอบเขตของโครงงาน

1.3.1 ขอบเขตด้านฮาร์ดแวร์

ใช้เพียงคอมพิวเตอร์หรือโน้ตบุ๊กทั่วไปที่สามารถเชื่อมต่ออินเทอร์เน็ตได้ โดยไม่ลงลึกถึงการพัฒนาหรือใช้งานฮาร์ดแวร์ควอนตัมโดยตรงอย่างควอนตัมโพรเซสเซอร์ (Quantum Processor)

1.3.2 ขอบเขตด้านซอฟต์แวร์

เนื่องจากประเทศไทย ไม่มีเครื่องควอนตัมคอมพิวเตอร์ที่สามารถใช้งานเพื่อประมวลผลได้ ดังนั้นจึงจำเป็นที่จะต้องมีการประมวลผลผ่านเครื่องคอมพิวเตอร์แบบคลาสสิคแพลตฟอร์ม Quantum Simulation ที่มีให้

บริการออนไลน์ เช่น D-Wave Leap และใช้ไลบรารีโอเพนซอร์สที่เกี่ยวข้อง เช่น Dimod สำหรับการคำนวณเชิงควอนตัม โดยภาษาโปรแกรมที่ใช้เป็นหลักคือ Python สำหรับการทดลองนี้

1.3.3 ขอบเขตด้านทฤษฎีและการจำลอง

มุ่งเน้นการสร้างแบบจำลองระบบความมั่นคงปลอดภัยไซเบอร์เชิงลำดับชั้นด้วยโครงสร้างต้นไม้ (Tree Structure) โดยโหนด (Node) แทนทรัพยากรหรือรางวัลของระบบ ที่ฝ่ายโจมตีต้องการ โดยอาจจะเป็นข้อมูลหรือทรัพยากรที่สำคัญในบริบทของไซเบอร์ และเส้นเชื่อม (Edge) แทนต้นทุนของการโจมตีเพื่อเข้าถึงรางวัลนั้น ๆ ซึ่งจะนำมาวิเคราะห์ปัญหาผ่านแนวคิด ดุลยภาพแนช (Nash Equilibrium) และ ควอนตัมแอนนีลลิง (Quantum Annealing) โดยจะเน้นไปในบริบทของ ระบบความปลอดภัยเครือข่าย (Network Security) และระบบที่เกี่ยวข้องอื่น ๆ กับความปลอดภัยไซเบอร์

1.4 ประโยชน์ที่ได้รับ

1. ได้ความรู้และความเข้าใจในการประยุกต์ใช้ทฤษฎีเกมกับปัญหาด้านความมั่นคงปลอดภัยไซเบอร์
2. เข้าใจหลักการและศักยภาพของการคำนวณเชิงควอนตัม โดยเฉพาะการแก้ปัญหาเพื่อหากระบวนการหาคำตอบที่ดีที่สุด (Optimization)
3. สามารถนำแบบจำลองที่พัฒนาขึ้นมาใช้เป็นแนวทางในการศึกษาเชิงลึกด้านการป้องกันและการโจมตีภายในระบบความมั่นคงปลอดภัยไซเบอร์
4. เป็นพื้นฐานให้กับงานวิจัยในอนาคตที่เกี่ยวข้องกับการผสมผสานกันระหว่างทฤษฎีเกมและการคำนวณเชิงควอนตัม

1.5 เทคโนโลยีและเครื่องมือที่ใช้

1.5.1 เทคโนโลยีด้านฮาร์ดแวร์

คอมพิวเตอร์หรือโน้ตบุ๊กส่วนตัวที่สามารถเชื่อมต่ออินเทอร์เน็ตได้

1.5.2 เทคโนโลยีด้านซอฟต์แวร์

1. Web Browser สำหรับเข้าใช้งาน Quantum Platform เช่น D-Wave
2. ไลบรารี Python สำหรับ Quantum Simulation เช่น dimod

1.6 แผนการดำเนินงาน

ขั้นตอนการดำเนินงาน	มิ.ย. 2568	ก.ค. 2568	ส.ค. 2568	ก.ย. 2568	ต.ค. 2568	พ.ย. 2568	ธ.ค. 2568	ม.ค. 2569	ก.พ. 2569	มี.ค. 2569
รวบรวมสมาชิกและกำหนดหัวเรื่องโครงงาน										

ขั้นตอนการดำเนินงาน	มิ.ย. 2568	ก.ค. 2568	ส.ค. 2568	ก.ย. 2568	ต.ค. 2568	พ.ย. 2568	ธ.ค. 2568	ม.ค. 2569	ก.พ. 2569	มี.ค. 2569
ศึกษาทฤษฎีและงานวิจัยที่เกี่ยวข้อง										
พัฒนาแบบจำลองขั้นต้นของอัลกอริทึมโดยใช้ปัญหาของทฤษฎีเกมขั้นพื้นฐาน										
รวบรวมข้อมูลและออกแบบแบบจำลองในบริบทปัญหาของไซเบอร์										
นำอัลกอริทึมไปรันบนแพลตฟอร์มจำลองเพื่อทดสอบหาค่าผลลัพธ์										
บันทึกผล วิเคราะห์ผลดีผลเสีย และสรุปผล										
จัดทำรายงาน โปสเตอร์ และสื่อนำเสนอ										

1.7 บทบาทและความรับผิดชอบ

เนื่องจากหัวข้อโครงงานต้องอาศัยศาสตร์แขนงของความรู้ที่หลากหลาย ทั้งในด้านของ ความมั่นคงปลอดภัยทางไซเบอร์, ทฤษฎีเกม และการคำนวณเชิงควอนตัม ทำให้สมาชิกในกลุ่มทุกคนต่างก็มีส่วนร่วมในทุกขั้นตอน โดยจะเน้นการทำงานร่วมกันในแต่ละขั้นตอนของโครงงานพร้อม ๆ กัน ช่วยเหลือกันแบ่งหน้าที่ในการค้นคว้า ออกแบบ และตรวจสอบผลลัพธ์ เพื่อให้โครงงานดำเนินไปอย่างถูกต้องและมีประสิทธิภาพมากที่สุด ซึ่งสามารถแบ่งเป็นหลัก ๆ ได้ดังนี้

1. นางสาวกนลลัส รัตนภาค รับผิดชอบหน้าที่หลักในการรวบรวมงานวิจัยที่เกี่ยวข้อง และสรุปองค์ความรู้ที่จำเป็นต้องใช้ในโครงงาน ทั้งทฤษฎีเกม สมการเชิงควอนตัม รวมไปถึง ออกแบบโครงสร้างแผนภาพต้นไม้ทั้งหมดก่อนนำไปแปลงเป็นสมการทางคณิตศาสตร์
2. นายธีระพันธุ์ พันธุ์วรรธนะสิน ทำหน้าที่ในการแปลงปัญหาในทฤษฎีเกม ทั้งในแบบจำลองตั้งต้นกับปัญหาทางไซเบอร์ซึ่งเป็นแผนภาพต้นไม้ ให้ออกมาอยู่ในรูปแบบของสมการคณิตศาสตร์ที่มีตัวแปรและอัลกอริทึมเพื่อที่จะสามารถแปลงเป็นโค้ด Python ได้
3. นางสาวแก้วตา ลุงต๊ะ รับผิดชอบหน้าที่หลักในการเขียนโค้ด Python ของอัลกอริทึม โดยอาศัยจากสมการคณิตศาสตร์ที่ได้แปลงจากแผนภาพต้นไม้มาแล้ว นำไปเขียนรูปแบบใหม่ในรูปของโค้ด Python โดยอาศัยไลบลารี dimod เพื่อวัดดูประสิทธิภาพและคำตอบของอัลกอริทึมในตอนสุดท้าย

1.8 ผลกระทบด้านสังคม สุขภาพ ความปลอดภัย กฎหมาย และวัฒนธรรม

การประยุกต์ใช้ทฤษฎีเกมเข้ากับความมั่นคงปลอดภัยไซเบอร์ เป็นการส่งเสริมการพัฒนาองค์ความรู้ใหม่ ๆ ที่สามารถต่อยอดไปสู่การป้องกันการโจมตีทางไซเบอร์ในอนาคต ซึ่งนำมาสนับสนุนการพัฒนาเทคนิคการวิเคราะห์ความเสี่ยงที่จะถูกโจมตีเพื่อช่วยเพิ่มความปลอดภัยของระบบเครือข่าย และอีกทั้งยังช่วยให้หน่วยงานหรือองค์กรที่เป็นเจ้าของระบบความปลอดภัยสามารถนำแนวคิดนี้ไปปรับใช้เพื่อป้องกันความเสียหายจากการโจมตี ผ่านการออกแบบเชิงนโยบายและกฎหมายให้รัดกุมมากยิ่งขึ้น

บทที่ 2
ทฤษฎีที่เกี่ยวข้อง

2.1 อัลกอริทึม (Algorithm)

อัลกอริทึม (Algorithm) คือชุดขั้นตอนหรือลำดับคำสั่งที่ใช้แก้ปัญหาหรือดำเนินการในคอมพิวเตอร์หรือระบบต่างๆ โดยมีขั้นตอนที่ชัดเจนและเป็นระบบ เพื่อให้ได้ผลลัพธ์ที่ถูกต้องตามที่ต้องการ อัลกอริทึมคือกระบวนการแก้ปัญหาที่สามารถอธิบายเป็นขั้นตอนอย่างละเอียด เมื่อได้รับข้อมูลนำเข้า จะต้องให้ผลลัพธ์ที่ถูกต้องและมีประสิทธิภาพ อัลกอริทึมที่ดีจะต้องมีความชัดเจนไม่คลุมเครือ ซึ่งการแก้ปัญหาโดยใช้อัลกอริทึมตรงข้ามกับการแก้ปัญหาโดยใช้สามัญสำนึก

2.2 Cybersecurity Model

Cybersecurity Model คือแบบจำลองเพื่อวิเคราะห์และจำลองปฏิสัมพันธ์ระหว่างผู้โจมตี (attacker) และผู้ป้องกัน (defender) ในโลกไซเบอร์ โดยทั่วไปจะมีการใช้เกมสองผู้เล่นที่เป็น zero-sum game ซึ่งผู้โจมตีพยายามหาช่องโหว่เพื่อโจมตี ส่วนผู้ป้องกันพยายามลดความเสียหายและป้องกันระบบ โดยผู้เล่นทั้งสองฝ่ายสามารถเลือกกลยุทธ์หลายระดับ เช่น ระดับไม่โจมตีหรือไม่ป้องกัน, ระดับโจมตี/ป้องกันต่ำ, และระดับโจมตี/ป้องกันสูง

2.3 Graph Theory

ทฤษฎีกราฟ (Graph Theory) คือสาขาหนึ่งของคณิตศาสตร์และวิทยาการคอมพิวเตอร์ที่ศึกษาถึงคุณสมบัติและการใช้งานของกราฟ ซึ่งเป็นโครงสร้างข้อมูลที่ประกอบด้วยจุดยอด (Vertices) และเส้นเชื่อม (Edges) ที่เชื่อมต่อระหว่างจุดยอดเหล่านั้น กราฟเป็นแบบจำลองทางคณิตศาสตร์ที่ใช้แทนความสัมพันธ์หรือโครงสร้างของเครือข่ายต่างๆ

2.3.1 Tree Structure

โครงสร้างต้นไม้ (Tree structure) ในทฤษฎีกราฟ หมายถึงกราฟที่ไม่มีวงจร (acyclic) และเป็นกราฟที่เชื่อมต่อกันทั้งหมด (connected) โดยลักษณะสำคัญของต้นไม้คือ ในกราฟต้นไม้จะมีเส้นเชื่อม (edges) เท่ากับจำนวนจุดเชื่อม (vertices) ลบหนึ่ง

$$|E| = |V| - 1$$

มีเส้นทางเชื่อมโยงเดียวและไม่ซ้ำกันระหว่างจุดเชื่อมใดๆ สองจุด ต้นไม้ไม่มีวงจรใดๆ หากตัดเส้นเชื่อมใดเส้นหนึ่งออก จะทำให้กราฟไม่เชื่อมต่อ (แตกออกเป็นส่วนย่อย)

ต้นไม้ถือเป็นกราฟสองกลุ่ม (bipartite graph) และกราฟแผนที่ (planar graph) จุดที่มีเส้นเชื่อมแค่หนึ่งเส้น เรียกว่าใบไม้ (leaf หรือ terminal vertex) มีจุดศูนย์กลาง (center) หรือจุดสมดุล (centroid) ที่แบ่งต้นไม้ได้อย่างสมดุล

โดยทั่วไป นิยามของต้นไม้คือกราฟที่เชื่อมต่อกันและไม่มีวงจร ซึ่งถือเป็นโครงสร้างพื้นฐานในหลายด้าน เช่น โครงสร้างข้อมูล คอมพิวเตอร์ เครือข่าย และระบบไฟฟ้า เป็นต้น

2.4 Game Theory

Game Theory คือศาสตร์ที่ศึกษาแบบจำลองทางคณิตศาสตร์ของสถานการณ์ที่มีการโต้ตอบเชิงกลยุทธ์ระหว่างผู้เล่นหลายฝ่าย ซึ่งมักใช้วิเคราะห์การตัดสินใจของผู้เล่นที่มีเหตุผลในสถานการณ์แข่งขันหรือร่วมมือกัน โดยตั้งสมมติฐานว่าผู้เล่นแต่ละคนจะพยายามเพิ่มผลประโยชน์ของตนเองจากกลยุทธ์ที่เลือกใช้ โดยในหนึ่งเกม จะประกอบไปด้วย

1. ผู้เล่น (Players) คือผู้มีส่วนร่วมในการตัดสินใจ
2. กลยุทธ์ (Strategies) คือทางเลือกที่ผู้เล่นสามารถเลือกใช้ได้
3. ผลตอบแทน (Payoffs) คือผลลัพธ์หรือรางวัลที่ผู้เล่นได้รับจากการเลือกกลยุทธ์
4. กติกาของเกม (Rules of the game) คือเงื่อนไขที่กำหนดว่าผู้เล่นโต้ตอบกันอย่างไร

2.4.1 เกมเชิงกลยุทธ์ (Strategic Game)

เกมเชิงกลยุทธ์ (Strategic Game) สามารถนิยามได้เป็นพจน์

$$G = (N, S, u)$$

โดยที่

1. $N = \{1, 2, \dots, n\}$ คือเซตของผู้เล่น
2. $S = S_1 \times S_2 \times \cdots \times S_n$ คือเซตของกลยุทธ์
3. $u = (u_1, u_2, \dots, u_n)$ คือฟังก์ชันผลตอบแทนของผู้เล่นแต่ละคน

2.4.2 Nash Equilibrium

Nash Equilibrium คือสภาวะที่ไม่มีผู้เล่นคนใดสามารถได้ผลประโยชน์มากขึ้นโดยการเปลี่ยนกลยุทธ์ของตนเอง หากผู้เล่นคนอื่นยังคงกลยุทธ์เดิมอยู่

2.5 Quantum Mechanics

2.5.1 Superposition

หลักการที่ระบบควอนตัมสามารถอยู่ในหลายสถานะได้พร้อมกัน จนกว่าจะมีการวัดหรือสังเกต

2.5.2 Entanglement

ปรากฏการณ์ที่อนุภาคควอนตัมถูกเชื่อมโยงกัน ทำให้การวัดอนุภาคหนึ่งส่งผลต่ออีกอนุภาคหนึ่งทันที

2.5.3 Tunneling

ปรากฏการณ์ที่อนุภาคสามารถผ่านอุปสรรคพลังงานได้ แม้พลังงานจะต่ำกว่าความสูงของกำแพง

2.5.4 Quantum Computing

เครื่องคอมพิวเตอร์ที่ใช้หลักการควอนตัมในการคำนวณ เช่น Gate-based Quantum Computing และ Quantum Annealing

2.5.5 Quantum Annealing

กระบวนการคำนวณเชิงควอนตัมเพื่อหาค่าที่เหมาะสมที่สุด โดยใช้ Superposition และ Quantum Tunneling

2.5.6 QUBO Formulation

การกำหนดปัญหาให้อยู่ในรูปแบบ Quadratic Unconstrained Binary Optimization ซึ่งเป็นปัญหา NP-hard

2.5.7 Optimization Problems

ปัญหาที่ต้องการหาคำตอบที่ดีที่สุดจากฟังก์ชันวัตถุประสงค์ โดยอาจมีหรือไม่มีข้อจำกัด

2.6 ความรู้ตามหลักสูตรซึ่งถูกนำมาใช้หรือบูรณาการในโครงงาน

2.6.1 Algorithms for Computer Engineers

นำมาใช้ในการพัฒนาอัลกอริทึมในแบบจำลองควอนตัม

2.6.2 Data Structures for Computer Engineers

นำมาใช้ในการออกแบบโครงสร้างแผนภาพต้นไม้ของปัญหา

2.6.3 Discrete Math for Computer Engineers

นำมาใช้ในการพิสูจน์ทางตรรกศาสตร์ ตารางค่าความจริงในสมการ

2.6.4 Advance Algorithm

นำมาใช้เป็นแนวทางการออกแบบ และวิเคราะห์อัลกอริทึมที่ให้ผลลัพธ์ที่เหมาะสมที่สุดสำหรับปัญหาทางไซเบอร์

2.6.5 Quantum Computing

นำมาใช้เป็นกระบวนการหลักในการสร้างอัลกอริทึมในการคำนวณเชิงควอนตัม

2.6.6 Penetration Testing

นำมาใช้ในการจำแนกประเภทของวิธีการโจมตีระบบความปลอดภัย

2.6.7 Defensive Security

นำมาใช้ในการจำแนกประเภทของวิธีการป้องกันระบบความปลอดภัย

2.7 ความรู้นอกหลักสูตรซึ่งถูกนำมาใช้หรือบูรณาการในโครงงาน

2.7.1 Game Theory (ทฤษฎีเกม)

ใช้เป็นทฤษฎีหลักในการประยุกต์กับปัญหาระบบความปลอดภัย

2.7.2 Nash Equilibrium (ดุลยภาพแนช)

ใช้เพื่อวิเคราะห์ผลลัพธ์ที่ดีที่สุดของอัลกอริทึม

2.7.3 Prisoner's Dilemma (ปัญหานักโทษ)

ใช้ในการสร้างตัวต้นแบบก่อนพัฒนาอัลกอริทึมจริง

2.7.4 Layered Security

ใช้อธิบายมาตรการป้องกันระบบความมั่นคงปลอดภัยไซเบอร์

บทที่ 3
โครงสร้างและขั้นตอนการทำงาน

ในบทนี้จะกล่าวถึงหลักการ และการออกแบบระบบ

3.1 การกำหนดแบบจำลองและทฤษฎีที่ใช้

ในการวิจัยครั้งนี้ได้อ้างอิงทฤษฎีดุลยภาพแนช (Nash Equilibrium) และปัญหานักโทษ (Prisoner's Dilemma) เป็นกรอบแนวคิดหลัก โดยกำหนดแบบจำลองเริ่มต้นเป็นเกมที่มีผู้เล่นจำนวนสองคน คือ ผู้เล่น A และ ผู้เล่น B ซึ่งสามารถเปรียบเทียบได้กับระบบที่ประกอบด้วยสองคิวบิต (qubits) แต่ละผู้เล่นมีตัวเลือกสองทางคือ "ยอมรับสารภาพ" และ "ไม่ยอมรับสารภาพ"

3.1.1 ตารางผลตอบแทน (Payoff Matrix)

ผลตอบแทนของผู้เล่นทั้งสองสามารถสรุปเป็นตารางได้ดังนี้ (รูปแบบ: ผลตอบแทนของ A, ผลตอบแทนของ B):

ตารางที่ 3.1: Payoff matrix ของ Prisoner's Dilemma

	B: สารภาพ	**B: ไม่สารภาพ**
A: สารภาพ	$3, 3$	$0, 4$
A: ไม่สารภาพ	$4, 0$	$1, 1$

3.2 การสร้างแบบจำลองเบื้องต้นเพื่อนำมาประยุกต์ใช้

กำหนดให้

$$X \equiv \text{ผู้เล่น A}, \qquad Y \equiv \text{ผู้เล่น B}$$

โดยทั้ง X และ Y มีค่าได้เพียงสองสถานะเท่านั้น คือ

$$0 = \text{ไม่รับสารภาพ}, \qquad 1 = \text{ยอมรับสารภาพ}.$$

3.2.1 เหตุการณ์ที่ 1: ผู้เล่น A พ้นโทษ

$$\begin{aligned} x = 0,\ y = 0 &\longrightarrow f(0,0) = 1, \\ x = 0,\ y = 1 &\longrightarrow f(0,1) = 4, \\ x = 1,\ y = 0 &\longrightarrow f(1,0) = 0, \\ x = 1,\ y = 1 &\longrightarrow f(1,1) = 3. \end{aligned}$$

และฟังก์ชันผลตอบแทนรวมพร้อมบทลงโทษ:

$$g(x,y) = f(x,y) + \alpha(1-x) + \beta y, \quad \alpha = \beta = 1$$

คำนวณค่าต่าง ๆ ได้เป็น

(x,y)	$f(x,y)$	$g(x,y)$
$(0,0)$	1	2
$(0,1)$	4	6
$(1,0)$	0	0
$(1,1)$	3	4

3.2.2 เหตุการณ์ที่ 2: B ติดคุกน้อยที่สุด

$$f(x,y) = 1(1-x)(1-y) + 0(1-x)y + 4x(1-y) + 3xy$$

$$g(x,y) = 1 + \beta + (3+\alpha)x - (1+\beta)y, \quad \alpha = \beta = 1$$

(x,y)	$f(x,y)$	$g(x,y)$
$(0,0)$	1	2
$(0,1)$	0	0
$(1,0)$	4	6
$(1,1)$	3	4

3.2.3 เหตุการณ์ที่ 3: ทั้งคู่ไม่รับสารภาพ

$$f(x,y) = 2(1-x)(1-y) + 4(1-x)y + 4x(1-y) + 6xy$$

$$g(x,y) = (2+\alpha)x - (2+\alpha)y + 2, \quad \alpha = \beta = 1$$

(x,y)	$f(x,y)$	$g(x,y)$
$(0,0)$	2	2
$(0,1)$	4	5
$(1,0)$	4	5
$(1,1)$	6	8

3.2.4 เหตุการณ์ที่ 4: ทั้งคู่ยอมรับสารภาพ

$$g(x,y) = (3x-3)^2 + (3y-3)^2$$

(x,y)	$g(x,y)$
$(0,0)$	18
$(0,1)$	9
$(1,0)$	9
$(1,1)$	0

3.3 การประยุกต์ข้อมูลทางไซเบอร์เพื่อสร้างแบบจำลองการโจมตีและป้องกัน

ในการศึกษานี้ได้ประยุกต์ใช้ข้อมูลเชิงไซเบอร์ (cyber data) เพื่อสร้างแบบจำลอง (model) ที่วิเคราะห์ผลกระทบจากการโจมตี (damage) และผลประโยชน์จากการป้องกัน (benefit) โดยใช้โครงสร้างข้อมูลแบบต้นไม้ (Tree Structure)

- **โหนด (Nodes):** แทนทรัพย์สินหรือสินทรัพย์สารสนเทศ (Asset Value / Payoff Asset Value)
- **เส้นเชื่อม (Edges):** แทนต้นทุนในการป้องกัน (Defense Cost)

ผู้โจมตี (attacker) ต้องเลือกเส้นทาง (path) ผ่านโครงสร้างต้นไม้โดยคำนึงถึงงบประมาณ ขณะที่ผู้ป้องกัน (defender) ต้องจัดกลยุทธ์เพื่อปกป้องโหนดที่สำคัญที่สุด

3.4 วิธีการและแนวทางเชิงอัลกอริทึม

เพื่อให้สามารถหากลยุทธ์การโจมตีและป้องกันที่เหมาะสมได้ มีการใช้แนวคิดทางอัลกอริทึมดังนี้

3.4.1 Depth-First Search (DFS)

ใช้สำรวจเส้นทางจากรากต้นไม้ (root node) ไปยังใบ (leaf node) โดยพิจารณาทุกเส้นทางอย่างละเอียด เพื่อค้นหาความเป็นไปได้ของการโจมตีและการป้องกันในกรณีต่าง ๆ เหมาะสำหรับการตรวจสอบเส้นทางเฉพาะเจาะจงและหา path ที่มี payoff สูงหรือมีต้นทุนต่ำ

3.4.2 Breadth-First Search (BFS)

ใช้สำรวจเชิงกว้าง (layer-by-layer) เพื่อประเมินความเสี่ยงในระดับชั้น (layers) ของต้นไม้ ทำให้สามารถระบุได้ว่าในระดับใดของโครงสร้างมีจุดอ่อนหรือมีโหนดที่มีความสำคัญสูงต่อระบบ เหมาะสำหรับการวิเคราะห์ระดับความลึกและการค้นหาช่องโหว่ที่อยู่ใกล้ราก

3.4.3 Greedy Algorithm

ใช้หลักการเลือกโหนดที่มีค่ารางวัล (payoff / asset value) สูงที่สุดก่อน สร้างกลยุทธ์การป้องกันแบบ “Most Prizes First” ช่วยให้ผู้ป้องกันสามารถจัดสรรทรัพยากรที่มีอยู่อย่างจำกัดได้อย่างมีประสิทธิภาพ โดยอาจผสานกับข้อจำกัดงบประมาณ (budget-aware) เพื่อเลือกชุดโหนดที่ให้ผลตอบแทนสุทธิดีที่สุด

3.5 แนวทางการป้องกัน (Defense Strategy)

ผู้ป้องกันสามารถใช้กลยุทธ์ดังต่อไปนี้:

3.5.1 Most Prizes First

จัดสรรทรัพยากรไปยังโหนดที่มีค่ารางวัล (payoff / asset value) สูงที่สุดก่อน เพื่อให้การป้องกันมีประสิทธิภาพสูงสุด

3.5.2 Budget-Aware Defense

พิจารณาการป้องกันภายใต้งบประมาณที่จำกัด โดยเลือกชุดโหนด (combination) ที่ทำให้ผู้โจมตีไม่สามารถได้ผลตอบแทนเกินระดับที่กำหนด

3.5.3 Hybrid DFS + Greedy

ใช้ DFS สำรวจเส้นทางที่เป็นไปได้ทั้งหมดร่วมกับ Greedy Algorithm เพื่อเลือกป้องกันโหนดที่มี payoff สูงสุด

3.6 การตรวจสอบ พัฒนา และประมวลผล (เนื้อหา 261492)

3.7 การสร้างแผนภาพและการรายงานผล(เนื้อหา 261492)

บทที่ 4
การทดลองและผลลัพธ์

4.1 การประเมินผลและการวิเคราะห์แบบจำลอง (Model Evaluation and Analysis)

4.1.1 การตรวจสอบความถูกต้องของแบบจำลอง (Model Validation)

ตรวจสอบว่าแบบจำลองที่สร้างขึ้นสามารถทำงานได้ตรงตามทฤษฎีหรือหลักการที่นำมาใช้ เช่น *Nash Equilibrium* และ *Prisoner's Dilemma* ทำการแสดงผลการรัน (*simulation results*) ของแต่ละกรณี เช่น *payoff function* และ *tree-based attack-defense model* จากนั้นเปรียบเทียบค่าผลลัพธ์ที่ได้กับค่าที่คาดไว้ (*Expected Values*) เพื่อยืนยันความถูกต้องของแบบจำลอง

4.1.2 การวิเคราะห์ผล (Result Analysis)

วิเคราะห์กรณีต่าง ๆ ของผู้โจมตีและผู้ป้องกัน เพื่อประเมินว่าค่าผลตอบแทน (*Payoff*) และความเสียหาย (*Damage*) เป็นไปตามที่คาดไว้หรือไม่ ใช้ตารางหรือกราฟเพื่อแสดงความแตกต่างของผลลัพธ์ในแต่ละสถานการณ์ (*Scenario*) พร้อมทั้งแสดงให้เห็นว่าแนวทาง *Greedy Algorithm* หรือ *DFS/BFS* มีประสิทธิภาพเพียงใดในการเลือกเส้นทางหรือกลยุทธ์ที่เหมาะสมที่สุด

4.1.3 การเปรียบเทียบกับวิธีอื่น (Comparison)

เปรียบเทียบแบบจำลองที่สร้างขึ้นกับวิธีการหรือโมเดลอื่นที่คล้ายกัน เพื่อระบุข้อดีและข้อจำกัดของแบบจำลองที่พัฒนา เช่น การเปรียบเทียบระหว่าง *Greedy Approach* กับ *Exhaustive Search (DFS แบบเต็ม)* ในด้านเวลาในการคำนวณและความแม่นยำของผลลัพธ์

ข้อจำกัดของโมเดล (Limitations) ระบุข้อจำกัดที่อาจเกิดขึ้น เช่น

- จำนวนโหนดของต้นไม้ (*Tree*) ที่มากเกินไปส่งผลให้เวลาในการคำนวณ (*Computation Time*) สูง
- การประมาณค่า *Payoff* หรือ *Defense Cost* อาจไม่ครอบคลุมทุกสถานการณ์ในโลกจริง

4.1.4 ข้อเสนอแนะในการปรับปรุง (Suggestions for Improvement)

เสนอแนวทางปรับปรุงเพื่อให้แบบจำลองมีความยืดหยุ่นและแม่นยำยิ่งขึ้น เช่น การนำแนวคิดเชิง *Heuristic* หรือ *Machine Learning* มาใช้ในการเลือก *Defense Strategy* การขยายแบบจำลองให้รองรับผู้โจมตีหลายคน หรือการจำลองหลายรอบเพื่อวิเคราะห์ความเสี่ยงเชิงสถิติ

4.1.5 สรุปผลการประเมิน (Evaluation Summary)

สรุปผลการประเมินว่าแบบจำลองสามารถตอบโจทย์วัตถุประสงค์ของงานวิจัยได้หรือไม่ ระบุจุดแข็ง เช่น ความสามารถในการคำนวณ *Payoff Function* และการวิเคราะห์ *Defense Strategy* ได้อย่างชัดเจน รวมถึงระบุจุดอ่อน เช่น เวลาในการคำนวณ (*Computation Time*) ที่สูง หรือสมมติฐานบางประการที่อาจไม่สอดคล้องกับสถานการณ์จริง

บทที่ 5
บทสรุปและข้อเสนอแนะ

5.1 สรุปผล

นศ. ควรสรุปถึงข้อจำกัดของระบบในด้านต่างๆ ที่ระบบมีในเนื้อหาส่วนนี้ด้วย

5.2 ปัญหาที่พบและแนวทางการแก้ไข

ในการทำโครงงานนี้ พบว่าเกิดปัญหาหลักๆ ดังนี้

5.3 ข้อเสนอแนะและแนวทางการพัฒนาต่อ

ข้อเสนอแนะเพื่อพัฒนาโครงงานนี้ต่อไป มีดังนี้

ภาคผนวก

ภาคผนวก ก
The first appendix

ก.1 รายการอ้างอิง (References)

Andrew Lucas. (2014). *Ising formulations of many NP problems.* วิทยานิพนธ์, Department of Physics, Harvard University, Cambridge, MA, USA 02138.

Dax Enshan Koh, Kaavya Kumar, และ **Siong Thye Goh.** (2024). *Quantum Volunteer's Dilemma.* วิทยานิพนธ์, Singapore Management University.

Jedsadakorn Kritsadakul และ **Sanpawat Kantabutra.** (2025). *Hybrid classical quantum computation for cybersecurity strategies in a layered cybersecurity model.* วิทยานิพนธ์, Chiang Mai University.

Kaushik Naskar. (2021). *Quantum version of Prisoners' Dilemma under Interacting Environment.* วิทยานิพนธ์, Department of Physics, Taki Government College.

Kay-Yut Chen และ **Tad Hogg.** (2006). *How Well Do People Play a Quantum Prisoner's Dilemma?* Quantum Information Processing, 5(1), กุมภาพันธ์ 2006.

Vitis Technologies. (n.d.). *What is Layered Security & How Does it Defend Your Network?* สืบค้นเมื่อ 1 กันยายน 2025 จาก https://www.vitistech.com/posts/what□is□layered□security□how□does□it□defend□your□network

ภาคผนวก ข
คู่มือการใช้งานระบบ

Manual goes here.

ประวัติผู้เขียน

Kanonlas Rattanapak (650610743) เป็นนักศึกษาระดับปริญญาตรี ชั้นปีที่ 4 ภาควิชาวิศวกรรมคอมพิวเตอร์ คณะวิศวกรรมศาสตร์ มหาวิทยาลัยเชียงใหม่ มีความสนใจด้าน *Quantum Computing, Game Theory, และ Cybersecurity* โดยเฉพาะการประยุกต์ทฤษฎีเกมควอนตัมกับการวิเคราะห์กลยุทธ์การป้องกันทางไซเบอร์ ปัจจุบันกำลังศึกษาวิจัยในหัวข้อ *Quantum Volunteer's Dilemma* เพื่อพัฒนาแบบจำลองเชิงควอนตัมสำหรับกลยุทธ์การโจมตีและการป้องกันในระบบเครือข่าย.