Project guides

I. Cryptogtaphy Project Topics

A. Cipher systems and cryptanalysis

1. **Cryptanalysis and Application of symmetric ciphers**

Focus on cryptanalysis, application scenarios and implementation cryptographic algorithms:

- chaotic-based stream ciphers;
- AES and other light-way block ciphers;

2. **Cryptanalysis and Application of asymmetric ciphers (RSA, ElGamal encryption, ECC)**

Focus on cryptanalysis, application scenarios and implementation cryptographic algorithms:

3. **Identity-based encryption**

Focus on: New encryption algorithms and application scenarios;

4. **Attribute-based encryption (ABE)**

Focus on: New encryption algorithms and application scenarios:

- Ciphertext Policy Attribute-based encryption (CP-ABE);
- Key Policy Attribute-based encryption (CP-ABE);

5. **Homomorphic encryption (HE)**

Focus on: New encryption algorithms and application scenarios:

- Partially homomorphic encryption (PHE);
- Fully homomorphic encryption (FHE);

6. **Functional encryption (FE)**

Focus on: New encryption algorithms and application scenarios:

7. **Thist, fourth Round NIST candidate**

Focus on: Understaning algorithms and application scenarios:

https://csrc.nist.gov/Projects/post-quantum-cryptography/selected-algorithms-2022

https://csrc.nist.gov/Projects/post-quantum-cryptography/round-4-submissions

- CRYSTALS-KYBER
- CRYSTALS-DILITHIUM
- FALCON

- SPHINCS+

8. Other ecryption algorithms

Select your-self and focus on application scenarios;

B. Hash Function and Message authemtication code (MAC)

9. MAC and applications

Focus on: improvement algorithms and application scenarios;

C. Digital signature

10. Signature applications

Focus on algorithms and applications:

- Integrity and authentication
- Digital government (Public administration)
- Digital business

11. Other improvement signature algorithms

Focus on understading algorithms and applications

D. Authentication

12. Authentication and key agreement

Focus on understading schemes and applications

- Client-server communication
- End-to-end communication
- Satellite communication
- IoT communication
- Edge networks
- 5G networks
- Secute API gateway

E. Database securitty

13. Encryption, access control and query in DBMS

Focus on understading schemes and applications

- Untrusted third-party storage;
- Cloud storage

F. Network security

14.Network secure protocols

Focus on understading secure protocols and applications

- Computer network
- IOT network
- Blockchain network

G. Post-quantum security

15.Secure scheme that can resist quantum computer attacks

Focus on understading scheme and applications

II. Guide for select project title and references

1. Project title:

- Determine the them;
- Search webofscience using set of related keywords to determine your topics (may use ChatGPT);
- Study the topic and requirments;
- Determine the research goals;
- Select some the main reference (some good articles) to do research on the topic;
- Determine the application scenario and ways to implementation;

2. References

Select at lease 2 good articles for your project:

- Focus on articles that can easy implementation for a specific application (IEEE,…)
- Don't use theory article,

3. Member

At most 3 students (at most 2 students for ANTN class) for each project with clear division of member works;

4. Submit your project title, References, and members Week 3;

5. Mid-term present (Week 6)

Nội dung:

1**) Tổng quan đề tài**

- Chủ đề;
- Ngữ cảnh vấn đề (tránh viết dài dòng, cần hình vẽ minh họa);
- Các bên liên quan;
- Các yêu câu về bảo mật;
- Tổng quan các giải pháp (các hướng nghiên cứu và các kết quả chính);

2) Đề xuất các hướng nghiên cứu cho project và các kết quả dự kiến

- Lựa chọn các tài liệu tham khảo chính (2 đến 3 bài báo).
- Trình bày sơ lược cách giải quyết (trong các bài báo) cho các yêu cầu về security đặt ra ở mục 1)

3**) Đề xuất ngữ cảnh ứng dụng và triển khai thử nghiệm**

- Lựa chọn ngữ cảnh ứng dụng;
- Đề xuất kịch bản và cách triển khai thử nghiệm bao gồm các vật liệu, dataset, thư viện dùng để triển khai thử nghiệm;
- Triển khai thử nghiệm (demo)

Note: Trong phạm vi đồ án môn học các bạn chỉ cần chọn một vài ý trong mục 2) để demo nhưng cần đảm bảo là giải pháp cụ thể phù hợp với ngữ cảnh.

Note: Có thể chọn để tài theo 2 hướng

1. Hướng thực nghiệm (hands on)

- chọn các vulnarabilities mới (có thể dùng các CVE), nghiên cứu về lỗ hổng, các cách khai thác (exploit), và đề xuất cách phòng thủ, khắc phục;

- Chọn các công cụ phàu hợpđể triển khai cho mootj vấn đề ứng dụng cụ thể;

2. Hướng nghiên cứu academic (minds set)

Các bạn có thể lựa chọn topic mới theo các papers, đọc hiểu, chọn kịch bản để triển khai đánh giá hoặc demo.