자 기 소 개 서

1. 관심 연구 주제 / 지원 동기 / 바라는 점에 대해 기재해 주십시오.

저는 학부 3학년에 네트워크 보안 수업을 들으면서 암호기술 분야에 관심을 가지게 되었습니다. 당시 학과 커리큘럼에는 보안 관련된 수업이 없었고, 네트워크 보안 수업에서 공개키, 대칭키, 인증 등의 개념을 처음 접했습니다. 생각보다 가까운 곳에서 많이 사용되고 있다는 점과, 영화에 나오는 고전암호를 암호의 전부라고 생각했던 것과 달리 계속해서 연구가 진행 중이며 수학적 이론을 기반으로 안전하게 잘 설계되어 있다는 점이 신기했고 암호 및 보안 분야에 흥미를 느끼게 되었습니다. 이를 계기로 한성대학교 서화정 교수님 연구실에 학부 연구생으로 들어가게 되었고 연구실의 주 분야였던 암호 알고리즘과 암호 구현에 대해 알게 되었고, 그 외에도 블록체인, 양자 내성 암호, 부채널 분석 등 학부 수업에서는 접하기 어려웠던 다양한 주제들을 대해 폭넓게 접할 수 있는 기회를 얻었습니다. 그러던 중, 교수님의 제안으로 인공지능 기술을 접하게 되었습니다. 당시에는 학부 과정에서 인공지능에 대한 수업이 없었고 처음 접했기 때문에 어렵기도 하고 보안이나 암호에 접목한다는 것이 조금 생소하기도 했지만 흥미를 가지게 되었고, 이후 석사과정 및 박사과정까지 인공지능과 보안 분야를 접목한 연구를 해오고 있습니다.

대학원에 진학한 후에는 가장 먼저, AVR 환경에서 컴파일 된 바이너리 파일을 분류하는 컨볼루션 인공신경망을 설계 및 학습하여 랜섬웨어와 정상적인 펌웨어를 분류하는 연구를 진행하여 WISA'20에서 발표하였습니다. FELICS의 C언어로 구현된 블록암호들을 컴파일 하고 8-bit AVR을 타겟으로 하는 일반 펌웨어들을 수집하여 데이터 셋을 직접 구축하였고, 해당 바이너리 파일들에서 opcode 및 instruction (operand + opcode)를 추출하여 해당 정보들을 이미지로 바꾼 후 컨볼루션 신경망을 통한 분류를 통해 랜섬웨어를 탐지하도록 하였습니다. 이러한 과정에서 데이터셋 구축과 블랙박스 모델인 인공지능의 결과를 해석하는 부분에서 어려움을 겪었습니다. 인공신경망으로 데이터를 성공적으로 분류한다고 하더라도 데이터의 특징을 어느 정도 알아야 실험 결과에 대한 분석이 가능하고 그것을 글로 쓸 수 있다는 것을 느꼈습니다. 실험 결과를 분석하면서 SPN 구조와 ARX 구조 간의 오분류가 거의 없고, 같은 구조의 암호 알고리즘간의 오분류 및 일반 펌웨어와 암호 알고리즘 간의 오분류가 존재함을 발견하였습니다. ARX와 SPN가 주로 사용하는 명령어들을 직접 분석하였을 때, ARX의 경우 산술연산의 비중이 더 컸고, SPN의 경우는 메모리 접근 연산을 위한 명령어가 더 많이 수행되었음을 파악하였습니다. 사용되는 명령어의 패턴과 빈도수가 다르다는 사실을 바탕으로 실험 결과를 해석할 수 있었으며 해당 결과를 SCIE 논문으로 게재할 수 있게 되었습니다.

두 번째로 진행했던 연구는 임베디드 환경에서의 Generative Adversarial Network 기반의 의사난수 생성기입니다. 해당 연구는 기존의 GAN 기반의 의사난수 생성기 연구를 기반으로 시작하게 되었고, 2020년 국가암호공모전에서 장려상을 수상했고, ICISC'20에 게재되었습니다. GAN은 생성자와 판별자를 사용하여 두 모델이 서로 적대적으로 학습하여 성능을 높여가는 생성형 신경망입니다. 이전 연구에서는 여기서의 판별자를 predictor 모델로 변경하여 real data의 입력 없이 생성자의 출력을 부분적으로 자른 후, 해당 데이터의 일부를 학습 데이터로, 일부는 label로 사용하였습니다. 즉, 앞부분의 난수열로 뒷부분의 난수열을 예측할 수 있는지의 여부를 계산하여 점점 더 난수성이 높은 의사난수열을 만 드는 연구입니다. 해당 구조를 기반으로 특정 범위의 숫자 값이 아닌 0과 1의 비트를 생성하는 Deterministic Random Bit Generator (DRBG)를 설계하였습니다.

이전 연구보다 더 긴 비트열에서 더 높은 난수성을 확보할 수 있으면서, 임베디드 상에서 추론이 가능한 DRBG를 만들기 위해 긴 시퀀스에 대한 정보를 학습하고 RNN 레이어를 사용하였고, 해당 시퀀스 데이터들은 각각 n개의 비트 (n개의 feature를 갖는 time series data)로 표현됩니다. 생성된 비트는 각 행이 8개의 특징 값을 갖는 경우 8-bit 단위의 시계열 데이터로 볼 수 있으며, NIST 문서에 작성된 변환 방법을 통해 각 행에 해당하는 비트를 특정 범위의 수로 변환할 수 있습니다. 또한, 임베디드 환경에서 추론이 가능해야하므로 TFLite 모델로 변환한 후 EdgeTPU 상에 배포해야 합니다. 그러나 EdgeTPU에서는 RNN, LSTM 레이어를 지원하지 않아서 RNN 레이어를 predictor 모델에만 사용하여 generator 모델은 TPU 상에서 추론이 가능하도록 하였습니다. 모델이 배포된 후 추론될 때는 이미 학습된 가중치를 통해 추론만을 수행하므로 기존 DRBG와 같이 결정론적인 특징을 갖게 됩니다. 따라서 GAN 모델에 입력되는 noise가 높은 엔트로피를 가질수록 좋을 것이고, 임베디드 상에서는 하드웨어에서 엔트로피를 수집할 수 있으므로 더 안전한 난수생성기로 사용이 가능합니다. 이 연구를 진행하면서 NIST test suite는 성공적으로 통과하였지만, 처음에 NIST test suite의 정확한 동작 과정이나 원리를 잘 알지 못하여서 실험결과 도출에서 어려움을 겪었습니다. 이런 경험을 통해 저는 다시 한 번 인공지능 기술을 통해 어떤 결과를 얻어낸다고 하더라도 이것을 분석하기 위해서는 관련 분야 지식이 충분히 필요하다는 것을 느꼈습니다.

그 다음으로는 인공신경망을 활용한 부채널 분석 또는 인공신경망에 대한 부채널 분석 연구를 수행해보고자 하였습니다. 해당 연구를 진행하기 위해 신경망 연산을 C언어로 변환하여 이를 컴파일 한 뒤, 칩위스퍼러 보드에 업로드하여 실행시키고 그 과정에서 발생하는 전력파형을 수집하여 연산 종류를 분류하거나 비밀 가중치를 찾고자 하였습니다. 그러나 실험환경 구축이나 칩위스퍼러를 사용하는데에 익숙하지 않아서 해당 연구는 아직 진행 중에 있습니다. 이번 기회를 통해 부채널 분석 기술에 대해 배울 수 있다면 이 연구에 큰 도움이 될 것 같아서 꼭 참여하고싶습니다.

최근에는 양자 인공지능(Quantum Neural Networks, QNN)를 통한 암호분석에 관심을 가지게 되었고 이와 관련된 연구를 진행 중입니다. ICCE-Asia 2021에서 Quantum Support Vector Machine을 활용한 고전 암호분석을 주제로 발표하였습니다. 해당 연구는 고전 컴퓨터의 머신러닝 알고리즘인 SVM을 양자 신경망으로 구성한 QSVM을 활용하여 알려진 평문 공격을 수행하는 것입니다. QSVM이 동작하기 위해서는 양자 컴퓨터가 필요하며, 큐비트와 양자게이트를 통해 양자 회로를 구성하여 고전 SVM의 커널 역할을 대신 수행하도록 하는 것입니다. 해당 연구를 진행하기에 앞서, 하고자 하는 작업에 맞게 양자 회로를 구성하고, 신경망을 설계해야하므로 양자 컴퓨터에 대한 공부가 선행되어야 했습니다. 그러나 큐비트나 양자역학적 내용을 이해할 수 있는 수학적 지식이 충분하지 않았습니다. 이러한 배경 지식을 습득하기 위해 꽤 많은 시간을 할애하였고 현재는 하이브리드 양자신경망 및 양자 신경망을 실행시킬 수 있게 되었습니다. 이번 인력양성 과정의 커리큘럼에 양자 컴퓨터를 이용한 공개키 암호 공격이 있는데, 해당 부분에 대해 기본적인 지식부터 실제 공격까지의 과정을 배워서 양자 컴퓨터와 암호분석에 관한 지식을 더욱 확장하고 싶습니다.

마지막으로 최근 KCMVP에 관한 프로젝트에 참여하게 되었습니다. 이번 인력 양성 과정의 교육 내용 중 암호모듈 안전성 검증에 관해 배운다면 이를 실제 프로젝트에 적용할 수 있기 때문에 아주 좋은 기회가 될 것 같습니다.

저는 위와 같은 경험을 통해서, 인공지능을 주 연구 분야로 선택했지만 인공지능 기술을 보안 및 암호 분야에 적용하기 위해서는 그 외의 다른 지식들과 다양한 관점이 뒷받침 되어야 해당 연구도 가능한 것이라고 생각하게 되었습니다. 그래서 저는 다양한 분야의 전문가분들께 교육받을 수 있는 이번 인력 양성과정 참여 기회를 놓치고 싶지 않아 지원하였습니다. 이번 교육 과정에서 암호 기술에 관한 다양한 내용을 습득해서 저의 관심 연구 분야에 적용할 수 있다면 앞으로의 연구에 있어 값진 경험이자 좋은 기반이 될 것이라고 생각합니다. 또한, 암호기술 전문인력 양성과정을 수료했던 선배님들의 후기를 들었을 때, 교육과정뿐만 아니라, 그곳에서 만나게 된 여러 전문가 분들이나 석박사 과정 학생들과 학문적 교류를 할 수 있는 네트워크가 있다고 하셨습니다. 제가 대학원에 입학한 후로 거의 모든 학회 및 행사가 온라인으로 진행되어 다른 연구원 분들을 만나볼 수 있는 기회가 부족했습니다. 그래서 더욱 이번 인력 양성 과정에 참여해서 다른 연구자 분들과 교류하면서 발전하고 싶다는 생각이 들었습니다.

이번 전문인력 양성과정에 참여하게 된다면 바라는 것은 오프라인으로 진행되었으면 하는 점입니다. 앞서 말씀드렸듯이, 이런 소중한 기회를 바탕으로 다른 연구원분들과 교류하며 제가 알지 못했던 부분에 대한 정보를 얻고 반대로 도움을 줄 수 있게 된다면, 교육 내용 이외에도 더 많은 지식과 새로운 시각, 협력하는 방법 등과 같이 연구에 필수적으로 필요한 부분들을 채워나갈 수 있을 것으로 기대하고 있습니다.

2. 국내 암호 관련 대학/연구소/기관/산업계에 암호기술과 관련하여 바라는 점이 있으면 자유롭게 서술해 주십시오.

국내에서도 수많은 연구자분들의 노력으로 암호 관련 기술들이 활발하게 연구되고 있고, 높은 기술력을 가지고 있다고 생각합니다. 암호 관련 워크샵, 세미나, 교육과정 등도 진행되고 있습니다. 또한, 실생활에서 보안은 매우 밀접한 분야이고 어떠한 시스템에서도 필수적으로 들어가는 부분이라고 생각합니다. 그러나 학부 교육과정에서는 암호나 보안관련 수업이 다른 수업에 비해 적은 것 같고, 주변 학생들의 의견을 들어보면 보안 관련 내용을 어렵게 생각하는 경우가 다수입니다. 특히, 암호에 대해서는 거의 알려지지 않은 것 같습니다. 이러한 이유로 대학에서는 학생들이 더 많이 접할 수 있는 교육 기회를 만들어야 한다고 생각합니다. 제가 이번 교육과정을 희망하는 것과 같이 암호 및 보안에 대해 배울 수 있는 기회를 희망하는 학생들이 있을 것입니다.

그리고, 대학이나 연구소 같은 곳에서도 KCMVP 같은 현업에서 실제로 수행되는 프로젝트 같은 것들에 대해 경험할 수 있고 잘 진행될 수 있도록 대학, 연구소, 산업계가 교류하고 협업해야한다고 생각합니다.

마지막으로 산업계에서는 가능하다면 연구에 필요한 자원들을 어느 정도 지원해준다면 좋을 것 같습니다. 예를 들어 대기업에서 GPU 서버를 해당 기업의 교육 과정 참가자들에게 일정 기간 동안 나누어 주는 것과 비슷하게, 더 좋은 연구 환경을 위해 여러 분야에서 협력해야 한다고 생각합니다. 감사합니다.