자 기 소 개 서

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

- 암호기술 분야의 관심 연구 주제, 연구 계획

저의 암호기술 분야의 관심 연구 주제와 계획은 계속해서 변화하고 있습니다. 대학교 학부시절 1학년부터 4학년까지 저의 대학생으로서의 공부 결과를 평가받는 졸업작품회에서 저는 머신러닝을 이용해 문헌유사도를 평가하여 자신과 비슷한 글을 찾아주는 웹서비스를 제안하고 구현하였습니다. 구체적으로는 주제에 맞추어 떠오르는 단어들을 계층 구조가 되도록 계속 작성해나가는 '마인드맵'이라는 형태에 적용하였는데요. 이 때 암호기술 이라는 것의 필요성을 처음으로 깨닫게 되었습니다. 저는 이 어플리케이션을 웹으로 작성하였는데 사용자마다 로그인 과정이 들어가게 되었습니다. 이유는 사용자 맞춤 서비스를 제공하기 위해서였습니다. 사용자가 작성한 글들을 바탕으로 비슷한 글들을 작성한 사람들끼리 군집화를 한 뒤 함께 군집화 된 사람들의 마인드맵을 바탕으로 사용자에게 내용을 추천해주는 서비스였기 때문입니다. 이러한 사용자 맞춤 서비스를 제공하기 위해서는 이 사용자가 적합한 사용자인지 판단해주는 인증과정이 필요했습니다. 제가 선택한 방법은 그냥 인터넷에서 자주 사용되는 아이디/비밀번호를 이용하는 방식이었습니다. 물론, 보안에 대한 아무런 장치도 하지 않고 코딩을 하여 서비스를 만들게 되었습니다. 그리고 기계학습을 위해 많은 데이터가 필요했던 저는 주변 사람들에게 가입을 권유하고 상술한 문헌의 한 형태인 마인드맵의 작성을 부탁했습니다. 그런데 하루는 저와는 다르게 네트워크 쪽에서 회사를 다니고 있는 친구가 아이디, 비밀번호를 대충 작성하면서 제게 이렇게 보안을 전혀 고려하지 않고 작성된 사이트는 매우 취약하다는 사실을 알려주었습니다. 간단하게 패킷을 조사하는 프로그램인 와이어샤크를 통해 검사한 결과 비밀번호와 아이디가 그대로 노출된다는 것을 처음으로 알게 되었습니다. 부끄러운 기분이 들었습니다. 지금까지의 발표회에서 제 서비스가 잘 쓰일 것이다 강력하게 주장해왔는데 이렇게 쉽게 고객들의 정보가 새어나갈 수 있다는 사실이 굉장히 크게 느껴졌습니다. 물론 마인드맵을 작성해준 주변 사람들의 아이디, 비밀번호도 패킷을 통해 그대로 노출되고 있었으며 그 중에는 다른 사이트에서 이용하는 아이디와 비밀번호를 동일하게 사용하는 사람도 있었기 때문에 아주 큰 문제가 될 수 있었다는 것을 깨닫게 되었습니다. 이렇게 인증 수단으로서의 비밀번호가 노출된다는 것을 알고 또 하나의 문제점을 자각하였는데요. 바로 두 번째, 사용자가 작성하는 문헌들이 그대로 노출되어 개인의 프라이버시가 보장되지 못한다는 점 이었습니다. 문헌을 작성하는 사람들은 자신의 관심사에 따라 많은 글들을 작성할 수 있을 것입니다. 그리고 이러한 많은 글들의 경향성을 통해 한 사람의 경향성을 알 수 있을 것이고 이 경향성에 준하여 비슷한 경향성을 띄는 사람들을 모아 그 사람들의 글들을 보여준다면 지식의 공유와 아이디어의 창출에 큰 도움이 될 것입니다. 이러한 서비스를 위해 문헌들이 처리되는 과정에서 사용자가 작성한 모든 문서들은 머신러닝을 위해 서버에 보내지게 됩니다. 여기서 사용자가 작성한 모든 문서들이 노출되게 됩니다. 물론, 저의 마인드맵은 상용화가 되지 않은 프로그램이기에 문제가 되지 않지만 만약 정말 좋은 아이디어를 문서로 정리해 놓은 사용자가 있었다면 또는 평소에 자신에 관한 모든 것들을 문서화하는 사용자가 있었다면 프라이버시에 많은 침해가 있었을 겁니다. 지금은 서버에서 문서가 처리되는 것 자체도 문제가 된다고 생각

하지만, 당시에는 암호화를 하지 않는다면 모든 데이터가 패킷에 그대로 노출된다는 점이 크게 느껴졌습니다. 이후 저는 제가 서비스를 제공하기 위해서는 단지 좋은 기술을 제공할 뿐만 아니라 보안을 통한 신뢰를 제공하기 위해 보안에 대해서 관심을 갖게 되었습니다. 하지만 결국 머신러닝, 패턴인식을 통해 작성된 마인드맵 어플리케이션은 PHP에서 기본으로 제공하는 최소한의 암호화만을 적용한 뒤 기술적인 부분만을 중점으로 발표하게 됩니다.

졸업작품회 이후 사이버 보안에 관심을 갖게 된 저는 한성대학교 서화정 교수님의 연구실에 지원하게 되었습니다. 연구실 입실 전 방학 기간에 저는 교수님이 학부연구생과 대학원생을 대상으로 주기적으로 연구한 내용을 발표하는 세미나에 참여하게 됩니다. 당시 제가 관심을 갖고 공부하던 연구 주제는 안전한 PIN 입력, 블록체인이었습니다. 안전한 PIN 입력이라는 주제는 비밀번호와 관련된 졸업작품 경험이 영향을 미쳐 관심을 갖게 되었고 블록체인이라는 주제는 무결성을 보장하면서도 복사된 여러 데이터베이스를 유지할 수 있다는 점이 매력적으로 다가와 연구하였습니다. 왜냐하면 과거 폴더 체계에서 데이터가 이 곳 저 곳 분산되어 저장되면 한 곳의 데이터가 갱신되었을 시 다른 곳의 데이터들이 갱신되지 않아 무결성에 대한 문제가 생깁니다. 그렇기 때문에 데이터베이스를 한 곳에 두고 관리함으로써 이를 막는 것이었는데 반대로 이 데이터베이스를 모두가 갖게 함으로써 무결성을 막는다는 점이 흥미로웠습니다. 이 두 주제에 대해서 각각 공부했던 부분이 있습니다. 첫 번째는 안전한 PIN 입력 방식입니다. 당시 비밀번호에 관심이 많던 저는 연구실 선배님들과 함께 PIN입력에 대하여 공부하게 되었습니다. 처음에는 실생활에서 쉽게 접할 수 있는 분야를 맡게 되어서 좋다 생각하였는데요. 공부할수록 이런 간단한(그 당시에는 간단하다고 생각하였습니다.) PIN 입력조차 정말 심도있게 연구하여 서비스를 제공하는 것을 알게 되어 제가 좀 더 암호에 대하여 진중하게 생각하게 되었던 기억이 납니다. 당시에 저희가 제안했던 아이디어는 기존의 고정된 넘버패드에 어깨너머 공격이 가능하다는 것에 대한 대응책이었습니다. 기존의 고정된 패드의 경우 손 동작을 멀리서 지켜본 뒤 넘버패드에 남아있는 지문 정보와 조합하여 공격이 쉽게 가능하기 때문입니다. 이에 대한 다른 대응책을 보면 모든 수를 무작위로 섞는 기법이 있었지만 적법한 사용자도 PIN을 푸는 시간이 꽤 걸린다는 단점이 있었습니다. 따라서 저희는 기존 넘버패드 디스플레이에 적정한 여백을 주고 넘버패드의 위치가 그 여백을 포함한 디스플레이에 랜덤하게 표시되도록 하였습니다. 그 결과 멀리서 지켜보더라도 정확한 위치를 알기 어렵고 또 지문이 고정된 위치에만 남아있는 것을 막을 수 있다는 것을 제안하였었습니다. 아이디어는 교수님으로부터 얻게 되었고 저는 이 아이디어를 프로그래밍해보는 것이 전부였지만 저로서는 보안에 대해서 더욱 깊이 있게 생각할 수 있게 된 연구였습니다. 두 번째는 스마트 컨트랙트입니다. 스마트 컨트랙트는 블록체인 2세대라 칭하기도 합니다. 기능을 설명하자면 블록체인 네트워크 상에서 컨트랙트에 정의된 조건을 만족하면 컨트랙트의 정해진 코드가 실행되는 기능을 말합니다. 이를 통해 가장 보편성있게 생각해 볼 수 있는 생각은 제 3자가 해주던 중개자의 역할을 대신할 수 있다는 점입니다. 기존의 계약에서는 거래와 같은 활동을 할 때 부인방지 등 안전한 거래를 제 3자를 통해 보장하였습니다. 대표적으로 공인중개사가 있습니다. 하지만 이상적인 스마트 컨트랙트 환경에서는 이러한 제 3자의 필요성을 컨트랙트가 대체하게 됩니다. 컨트랙트 실행 조건을 만족시키면 컨트랙트는 자동으로 계약 내용을 실행할 수 있습

니다. 저는 이 기능을 통해 안전한 영상 검증 모델을 제안하고 이를 이더리움을 통해 구현하였습니다. CCTV를 활용한 서비스들이 공공기관을 중심으로 증가하고 있는 현 상황에서 촬영된 영상을 기반으로 서비스를 제공할 때, 영상의 무결성은 반드시 보장되어야 할 것입니다. 그렇지 않으면 악의적인 해킹이나 촬영기기의 오작동 등으로 인해 소중한 인적, 물적 자원이 낭비될 수 있기 때문입니다. 저는 하나의 CCTV가 다른 주변의 CCTV들과 서로의 촬영 결과물을 검증하는 시스템을 제안하였습니다. 이 때 용량에 대하여 제한이 있는 블록체인의 특징을 고려하여 영상 자체를 저장하는 것이 아닌 영상을 분석한 결과만을 비교하여 저장하는 방식을 택하였습니다. 컨트랙트는 CCTV로부터 받은 내용이 주변의 다른 CCTV로부터 받은 내용과 동일한지를 검사하여 무결성을 보장하게 됩니다. 두 분야에 대한 연구결과를 국가암호공모전에 제출했는데, PIN의 경우 떨어졌지만 블록체인과 관련한 아이디어의 경우 좋게 봐주셔서 특별상을 받게 되었습니다. 저의 첫 수상 경험이었고 너무나 값진 경험이었습니다. 이 경험을 통해 암호에 대해 더욱 흥미가 샘솟았고 그에 따라 더 많은 관심을 쏟게 되었습니다. 국가암호공모전에 제출했던 주제에 대하여 수상 이후에도 계속하여 보완하여 논문을 작성하게 되었고 이번에 게재가로 판정이 나서 정말 기뻤습니다. 방학 동안 이 두 가지 활동을 하였고 저는 연구실에 들어가게 되었습니다. 암호에 대한 공부를 계속 더해나갔습니다. 제가 잘 몰랐던 암호의 기본부터 시작해서 정말 암호가 우리 생활에 이렇게나 많이 쓰이는 구나 싶었던 응용까지 깊이 있진 않지만 전반적인 내용을 대학원 수업, 연구를 통해 공부하게 되었고요. 그러는 과정에 부채널 분석이라는 암호기술의 한 분야를 알게 되었습니다! 부채널 분석에서도 통계적으로 키를 찾아내는 방식이 상당히 흥미로웠는데 제가 이런 흥미를 느낀 이유는 “암호화만 하면 내 정보는 노출되지 않는다.”라고 생각했는데 이러한 암호화 과정이 또 다른 정보 형태로 그대로 노출되고 있었다는 점과 이러한 정보들을 통계적 처리 하는 과정에서 머신러닝을 공부했던 경험이 작용했던 것 같습니다. 더 자세히 말하자면 당시까지 제가 DES에 이어 AES를 공부하고 구현해보면서 현재 널리 사용되는 이 표준화 암호 알고리즘은 절대 안전하다고 생각하고 있었습니다. 그러면서 어떻게 이렇게 장기간 안전한 암호를 만들 수 있었을까 하면서 대단하다고도 생각하고 있었습니다. 그런데 하루는 서화정 교수님이 암호 세미나에 저를 데려가셨는데 그 때 공유되는 캐시 메모리의 시간 차를 이용한 부채널 분석을 듣게 되었습니다. 이 때가 저와 부채널 분석과의 첫 만남이었습니다. 이후 국민대 한동국 교수님의 전력 분석에 대한 발표도 듣게 되어서 관심이 생기던 때에 지도 교수님이 부채널 분석 도구인 Chip-Whisperer_lite를 사주셨습니다. 초반에는 이러한 기계를 다루어 본 경험이 없어 고생하였으나 나중에는 감이 잡혀서 예제 코드를 통해 AES 공격에 성공하게 됩니다. AES 공격은 예제에 있기 때문에 실험을 해보는 것은 어렵지 않았습니다.(사실 그 당시에는 어려웠습니다.) 하지만 개념적인 공부를 마치고 실습으로 확인하는 과정이 의미가 있었습니다. 부채널 분석이란 암호를 기계에서 구동할 때 발생하는 물리 정보들을 이용하여 암호를 분석하는 기법입니다. 이용할 수 있는 물리 정보로는 시간, 소리, 전자기파, 전력 등이 있는데요. 연산의 종류에 따라 물리 정보의 속성이 다르기 때문에 이를 통해 분석을 할 수 있는 것입니다. 가령, 아무런 연산을 하지 않을 때의 전력 소모량과 곱하기 연산을 할 때의 전력 소모량은 다를 것입니다. 만약 이러한 연산들의 여러 번 반복하여 발생할 경우 어떠한 패턴을 띌 수 있습니다. 이러한 차이를 이용하여 암호화에서 사용하는 비밀정보(주

로 키가 됩니다.)를 분석해내는 방법이 부채널 분석입니다. 위에서 언급한 Chip-Whisperer_lite는 전력 분석 도구입니다. 오실로스코프 역할을 하는 파형 수집장치가 있고 암호를 구동하는 타겟 장치가 있습니다. 타겟 장치의 암호를 구동 시키고 이 때 발생하는 전력 파형을 수집하여 데이터의 형태로 저장해주는 역할을 합니다. 이러한 전력 파형을 이용하여 여러 분석을 시도해 볼 수 있는데요. 대표적으로 파형 모양을 분석하는 방법과 여러 파형을 수집하여 통계적으로 분석하는 방법이 있습니다. 상관관계를 이용한 통계적인 분석 방법인 CPA(Correlation Power Analysis)가 제가 집중하여 공부했던 내용입니다. 예측한 전력소모량과 실제 전력 소모량과의 상관관계를 측정하여 키를 찾아내는 방식인데요. 비밀정보(비트)가 변화함에 따라 함께 변화하는 연산 중간 값과 실제 파형과의 피어슨 상관관계를 구하여 가장 높은 상관관계를 갖는 비밀정보(비트)를 찾는 것입니다. 여기서 연산 중간 값이란 암호 알고리즘이 수행 시 발생하는 데이터 플로우에서의 어느 한 지점을 말합니다. 그리고 피어슨 상관관계란 상관관계를 표현하는 식 중의 하나로 비례에 관계에 있는 양의 상관관계를 띌 경우 1, 음의 상관관계의 경우 -1, 아무런 관계를 띄지 않을 경우 0에 수렴하는 식입니다. 이 CPA 공격을 통해 AES의 모든 키를 확인할 수 있었습니다. 하지만 이 때까지는 이론적 공부를 확인하는 정도였던 터라 커다란 울림은 없었습니다. 제가 정말 부채널 분석에 대해서 뭔가를 느낀 시점은 더욱 최근인데요. 다른 암호 알고리즘은 부채널 분석으로 분석할 때입니다. 암호 알고리즘에 대한 파형, 파형에 해당하는 평문, 키 이 세가지 정보를 가지고 CPA 알고리즘을 코딩하여 키를 찾아냈을 때, 저는 뭔가 연구할 수 있는 베이스가 생겼구나라는 느낌이 들어 감동했던 것 같습니다. 현재는 이러한 전력 분석 방법의 대응기법을 공부하고 있습니다. 이 전에는 마스킹 기법에 대하여 이론적으로만 공부를 했으나 현재에는 실제 키가 찾아지는지 여부를 실험해 볼 수 있게 되었기 때문에 더 피부에 와닿는 연구를 하고 있습니다. 이렇듯 저는 현재 부채널 분석 세부적으로는 전력분석에 관심을 갖고 있으며 앞으로 가능하다면 더욱 다양한 암호 알고리즘을 공부하여 부채널 분석에 적용해 보고 싶고 이러한 암호 알고리즘이 적용되는 환경(IoT, TEE)에 따라 발생할 수 있는 부채널 분석 취약점등을 살펴보고 싶습니다. 암호 알고리즘을 제안할 시 지금까지는 선형분석, 차분분석 등이 당연하게 여겨졌었습니다. 하지만 부채널 분석의 등장으로 이제는 시간 공격에 대비한 연산 시간의 상수화, 전력 공격에 대비한 마스킹, 셔플링 등의 여러한 기법들이 함께 고려되어야 할 것입니다. 따라서 부담이 커질 것입니다. 하지만 이와 동시에 새로운 환경, 예를 들어 IoT의 경우 제한된 자원만을 이용하기에 가능한 부담을 줄여야 합니다. 따라서 암호를 다각도에서 분석하여 기존의 분석법에도 안전하고 현재의 부채널 분석에도 안전하며 미래에 다가올 양자 알고리즘에도 안전할 암호를 위해서는 여러 방면에서의 분석이 필요할 것입니다. 저는 부채널 분석을 공부하면서 암호를 바라보는 시선이 하나 더 생겼다고 생각합니다. 이렇듯 암호를 여러 시선으로 보게 된다면 더 많은 것이 보일 것 같습니다. 이번 기회가 그 기회일 것이라고 확신하고있으며 꼭 잡아서 제가 더 많은 시선을 갖고 암호를 연구할 수 있었으면 좋겠습니다. 제기 그런 기회를 주신다면 부족하겠지만 최선을 다해 수업을 따라갈 것이며 최대한 습득하여 앞으로의 암호 연구에 활용할 것을 약속드립니다.

- 암호기술 전문인력 양성과정 지원 동기

제가 “암호기술 전문인력 양성과정”에 대해서 알게 된 것은 서화정 교수님과 연구실

선배인 안규황 연구원을 통해서인데 지원하게 된 동기에는 세 가지가 있습니다.

첫 번째, 안규황 연구원이 저번 학기 양성과정에 참가하였는데 정말 다양한 측면으로 도움이 된다고 강력 추천하였고, 서화정 교수님께서 이러한 좋은 기회에 대해 지원하는 것을 장려하셨기 때문입니다. 저는 석사과정 2년차를 진행 중입니다. 어찌 보면 자리가 잡혀야 할 상황이라고 여겨질 수 있는 시기 이지만 저는 제가 아직 너무나도 부족하다고 생각합니다. 그리고 이런 저를 잘 알고 계신 두 분이고 동시에 제가 믿고 따르는 두 분이기 때문에 강력한 지원 동기가 되었습니다. 특히 안규황 연구원이 지난 학기 양성과정에서 배웠던 내용들 중 부채널 분석, 암호 분석(차분 공격, 선형 공격)에 관련된 내용을 설명해주었습니다. 각각이 의미있다고 느껴졌고 그런 좋은 교육을 적절한 시점에 받게 되어 부럽기도 했었는데요. 부채널 분석의 경우 분석 도구과 함께 실제 공격 과정을 소개 해 주셨다고 합니다. 저는 그런 기회가 없어서 이론과 실습 과정 모두 진행에 어려움이 있었는데 전문가에게 지도를 받을 수 있었다는 점이 장점인 것 같다고 생각했습니다. 또한 암호 분석에서도 가장 기본이 되는 차분 공격과 선형 공격에 대해서도 저는 어려움을 느끼는데 이를 전문가한테 배울 기회가 사실 없기도 한 만큼 부러웠던 것 같습니다. 저도 이번 기회에 전문가에게 이러한 평소 궁금했던 주제들을 상세하게 공부할 수 있었으면 더할 나위가 없을 것 같습니다.

두 번째, 이번 양성의 주제인 인공지능을 활용한 암호분석과 해당하는 세부 과정들(기계학습, 패턴인식, 부채널 분석, 암호분석)이 제가 공부했던 분야이고 앞으로 가진 연구계획에 도움이 되는 내용이기 때문입니다. 저는 학부시절 머신러닝과 패턴인식을 공부하여 졸업작품을 제출하였습니다. 구체적으로 제가 머신러닝과 관련하여 한 작업을 말씀드리겠습니다. 먼저, 존재하는 모든 문서들의 단어를 문자열로부터 분리 해 냅니다. 실제 문서에서는 의미를 나타내는 부분과 문법에 의해서 필요한 부분을 분리해 내어 의미 부분만을 분리해야 하지만 제가 적용한 마인드맵의 특성 상 단어 위주로 되어있기 때문에 난이도는 상대적으로 더 쉬웠습니다. 의미만으로 분리된 단어들을 배열로 만듭니다. 예를 들어, 제가 제공하는 시스템이 총 5단어라고 가정한다면(실제로는 훨씬 더 많게 됩니다.) (단어1, 단어2, 단어3, 단어4, 단어5)라는 배열을 만들게 됩니다. 이는 데이터베이스의 '컬럼명' 역할을 합니다. 그리고 문서 A가 만약 단어1, 단어3을 각각 1개, 2개씩 표현한다면 문서 A에 해당하는 배열은 (1, 0, 2, 0, 0)이 됩니다. 즉 모든 문서는 이렇듯 문서가 포함하는 단어를 카운팅한 배열을 갖게 됩니다. 제 경우에는 마인드맵에서 좀 더 포괄적인 역할을 하는 상위 계층에 속한 단어의 경우 가중치를 주어 입력하였습니다. 이유는 포괄적인 단어가 그 마인드맵의 정체성을 더 잘 표현한다고 판단했기 때문입니다. 이렇게 만들어진 배열들을 벡터로 생각하여 거리를 재게 됩니다. 기계학습에서 두 벡터의 거리를 다양한데요, 여러 방식을 적용한 결과를 검토해보니 유클리드 거리 방식이 가장 마음에 드는 결과를 주어 유클리드 거리 방식을 택하게 되었습니다.(주관적인 결정이었습니다.) 이를 통해 모든 문헌간의 유사도를 조사하고 높은 유사도를 가진 사람들을 모았습니다.(이를 군집화 또는 클러스터링이라고 합니다.) 군집화에도 줄 수 있는 여러 기법이 있는데 제가 택한 방법은 계층적 클러스터링 방법입니다. 그 이유는 제가 원하는 만큼의 강도까지 클러스터링을 할 수 있었기 때문입니다.(매우 낮은 계층도 개별의 군집으로 볼지, 묶는지에 관련한 문제) 이렇게 한 결과로 문헌간의 유사도를 체크할 수 있었고 그에 따라 사람들을 군집화하여 비슷한 성향의 문헌작성 스타일을 가진 사람을 추천

할 수 있었고 유사한 단어들을 추천해주는 서비스 제안할 수 있었습니다. 과정에서의 난항이라고 하면 양질의 많은 데이터를 구하기가 어려웠다는 점입니다. 같이 진행하던 친구의 인맥을 총 동원하여 데이터를 만들었던 기억이 남습니다. 다음으로 부채널 분석의 성능을 이끌어 낼 때 머신러닝은 큰 도움이 된다고 합니다. 이 부분에 대해서는 제가 아직 깊게 공부하지 않아 자세히는 모릅니다. 하지만 알고 있는 부분은 이렇습니다. 전력 분석을 위해 많은 파형들을 수집하게 됩니다. 이러한 파형을 해석하여 우리가 타겟으로 하는 지점을 찾고 또 그러한 파형의 시작점을 맞추는 등의 과정을 전처리 과정이라고 합니다. 이러한 전처리 과정을 사람이 다 해도 되겠지만 AI를 이용하면 꽤 괜찮은 결과가 나온다고 합니다. 저는 머신러닝까지는 얕게나마 이용해 본 경험이 있지만 딥러닝의 경우에는 아직 개요만을 알고 있는 수준입니다. 하지만 이번 양성에 참여할 수 있다면 이러한 호기심을 해결할 수 있을 것이고 이는 암호 알고리즘의 분석법에 대해 한 발 다가서는 기회가 될 것이라고 생각합니다. 제가 머신러닝을 공부했을 때 느꼈던 점은 결과에 대한 해석이 어렵다는 것이었습니다. 반대로 말하면 기계가 바라보는 암호 알고리즘의 시선을 제가 이해하기는 어렵다는 것을 의미할 것입니다. 하지만, 어렵다고 생각했던 해석도 최근의 기계학습 논문에서 보면 수학을 기반으로 다 해석을 하는 것을 확인할 수 있었습니다. 따라서 저는 인공지능을 통해 암호 분석을 하는 것이 암호를 보는 새로운 시선을 준다는 생각이 듭니다. 따라서 이 부분이 제게 큰 의미를 줄 것 같기에 꼭 공부해보고 싶습니다. 또한, 저의 앞으로의 목표는 다양한 환경에 올라간 암호 알고리즘의 분석을 통해 취약점을 찾는 것입니다. 현재의 암호들은 모두 기본적인 암호 분석들을 고려하여 나오지만 이러한 암호 알고리즘이 다양한 환경에 접목될 때 예기치 못한 또는 피하지 못할 취약점이 생길 것입니다. 그렇기 때문에 이러한 취약점들을 많이 분석하여 효율적으로 대응할 수 있어야 할 것입니다. 이러한 제 목적을 위해서는 암호 분석에 대한 연구가 필요한데 이번 양성 프로그램이 어쩌면 지금 이 시기 제게 꼭 필요한 프로그램이 아닐까 생각합니다. 여기까지 저의 머신러닝, 패턴인식을 해보았다는 점과 앞으로 제 암호 연구에 인공지능, 암호 분석에 대한 경험이 엄청난 도움이 될 것이라는 점이 제가 이 양성 프로그램을 신청하게 된 큰 동기라고 말씀드리고 싶습니다. 다음으로 제가 Python 언어에 대한 깊은 소양은 없지만 암호 DES 알고리즘을 Python으로 코딩해 본 경험이 있습니다. 또한, 전력 분석에서의 CPA 알고리즘 또한 코딩해 본 경험이 있습니다. 그리고 C, Java, C++, Javascript, Solidity 등에 대한 얕고 깊은 언어 경험이 있기 때문에 Python의 활용에 대한 자신감이 있습니다. 또한, Python언어는 머신러닝, 전력 분석과 같은 많은 데이터를 다루는 작업에 있어 특화된 라이브러리와 인터페이스를 제공하기 때문에 현재 계속해서 공부하고 있습니다. 또한 저는 대학원생 1학기에 한성대학교 구동영 교수님의 기초 암호학 개론을 들었습니다. 이를 통해 모듈러 연산에서부터 시작하여 ECC까지의 개론적인 내용들을 어느 정도 숙지하고 있으며 올해 2월 한국암호포럼과 한국정보보호학회에서 주최하는 정보보호 전문가를 위한 암호 교육(2.18~2.22)을 수료하였습니다. 또한 저의 지도교수님이신 한성대학교 서화정 교수님이 주최하시는 세미나에 매주 참여하여 암호와 관련된 공부, 연구 내용을 학부생과 또 다른 대학원생들과 공유하고 있습니다. 물론 많이 부족하지만 제가 양성과정을 따라갈 수 있는 이 정도의 바탕에 최대의 노력을 함께 한다면 이번 과정에서 많은 것을 배워갈 수 있다고 확신합니다. 선형대수에 대한 내용으로는 학부시절 개론 수업을 수강하여 벡터의 기본부터 행렬

을 다루는 연산들까지 공부하였었습니다.. 저는 이렇게 양성과정을 따라갈 수 있는 최소한의 지식과 최대한의 동기를 가지고 있습니다. 이에, 노력과 함께 이번 과정을 잘 흡수하며 따라갈 수 있다고 생각합니다. 따라갈 수 없다면 더욱 노력하여 따라가겠습니다.

세 번째, 커뮤니티입니다. 제가 짧게나마 연구생활을 하면서 느끼는 점은 많은 교류가 중요하다는 점입니다. 저는 암호와 관련해서 이야기 나눌 사람이 많지 않다고 생각합니다. 학부생이나 대학원생들이 전부입니다. 즉 주변에 암호에 대해서 이야기할 사람이 매우 제한적이기 때문에 많은 아이디어를 획득할 기회가 적습니다. 반면에 항상 좋은 생각이나 호기심이 가는 흥미로운 내용들은 다른 사람들과 이야기할 때 나왔던 것 같습니다. 그런 이유로 다양한 사람들과 교류를 할 수 있다면 제 연구생활에 더 큰 도움이 될 것 같습니다. 이번 기회에 알게 될 같은 분야를 가진 다양한 생각을 가진 사람들(모든 연구자들)과 교류하여 눈을 트이고 싶습니다.

- 암호기술 전문인력 양성과정에 참여하게 되었을 때 바라는 점 등

저는 이전 양성과정에 참여했던 선배를 통해 제가 열심히 노력한다면 그 어떤 다른 활동보다도 많은 것을 배워갈 수 있다는 사실을 압니다. 그럼에도 더욱 바라는 점이 있다면 수업을 허투루 보내지 않도록 잘 따라가도록 해 주시면 감사드리겠습니다. 양성과정이 한 달을 주기로 이루어지는 것으로 압니다. 한 달을 알차게 보내도록 적절한 과제를 내주셨으면 합니다. 또한 다음 수업에 대한 예습이 가능하도록 수업 자료를 미리 주시거나 내용에 대한 귀띔을 부탁드립니다. 가능하다면 간단한 질문 등을 받아 주시면 좋겠습니다. 현재 저의 마음가짐은 어떻게든 많은 것을 배워서 앞으로의 저의 암호 연구에 도움이 되도록 하는 바람입니다. 그렇기 때문에 어떠한 정보라도 주신다면 참고하여 습득하려고 노력하겠습니다.

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

국산화, 국문화

LEA나 HIGHT, SEED와 같은 국산 암호들을 보면 우리나라에는 그래도 다른 나라에는 없는 우리만의 기술이 있구나 하는 뿌듯함을 느낍니다. 그렇지만 부채널 분석과 같은 비교적 최신의 분야를 공부하다 보면(또는 다른 최신의 암호적인 요소를 공부하다 보면) 국문으로 되어있는 글이 존재하지 않고 장비 또한 마찬가지로 외국산입니다. 게다가 영어로 된 용어의 경우 연구자들마다 해석도 다르게 되어 의사소통의 어려움이 있습니다. 만약에 이렇게 화제가 되는 최신 기술에 대하여 기준이 되는 국문이 있으면 좋겠습니다. 그렇게 되면 저와 같은 초보 연구자들이 최신 주제에 대해 가지는 부담을 덜을 수 있을 것 같습니다.

홍보

부끄럽지만 제 경우에는 어플리케이션 서비스를 제공하려는 목적이 있었음에도 보안적인 부분을 전혀 모르고 있었습니다. 사정은 제 주변에도 마찬가지입니다. 제가 암호를 공부한다고 하면 잘 모르시거나 비주류 분야로서 이해하고 계십니다. 하지만 제가 생각하기에 암호학은 최신 기술에 이용되며 현재도 매우 범용적으로 사용되고 있는데 그렇

게들 생각하시는 것이 아쉽습니다. 아마 다른 연구자 분들도 저와 같은 생각을 많이 하시겠지만 학문에 대한 인식이 비주류가 아닌 일상생활에도 항상 쓰이고 있는 대중적인 분야로서 여겨졌으면 좋겠습니다. 구체적으로는 암호의 기초부터 차근차근 공부를 하여 학문을 이해하는 것은 나중 문제이더라도 먼저 암호기술이 우리 생활에 얼마나 밀접하게 존재하는지를 많은 사람들이 알았으면 좋겠습니다. 포털 사이트의 로그인, 지문 인식, 신용카드의 사용 등에도 암호가 적용되어 우리에게 안전함을 준다는 것을 인지한다면 흥미가 생길 사람이 분명 있을 것입니다.(저처럼 말입니다.) 또 다른 방법으로는 랜섬웨어, 비트코인과 같은 큰 이슈가 되었던 기술들에도 암호가 적용됨을 알리면 홍보가 될 것 같습니다. 영화와 같은 곳에서 소개되는 것도 큰 역할을 하는 것 같습니다. 예를 들어, '미션 임파서블'의 시리즈를 거듭할 때마다 나오는 최신 인증 기법들은 보는 것만으로 신기하고 흥미롭습니다. 따라서 이런 멋진 영화에 후원을 하는 것도 좋을 것 같습니다. 암호라는 분야는 어떻게 보면 철통의 보안을 유지하는 것에만 쓰일 것 같지만 인증을 통해 적절한 서비스를 제공한다거나, 블록체인처럼 부인방지의 역할을 톡톡히 해낸다거나 하는 다른 다양한 역할도 수행합니다. 이러한 부분에 대해서도 사람들이 많이 알았으면 좋겠습니다. 현재 암호에 대하여 자세한 지식이 없는 사람은 현재 사용하고 있는 암호 기술에 대해서 아이디어를 전혀 낼 수 없습니다. 그렇지만 핵심적인 특징들이라도 인지하고 있다면 참신한 아이디어를 내는 것이 가능할 것입니다. 예를 들어 블록체인의 경우 자원의 어떻게 관리되는지 네트워크가 어떤 방법으로 유지될 수 있는지 등 구현 측면에서의 문제들은 고려하지 않더라도 분산 원장이라는 특징을 이해하고 그에 따라 투명성을 제공하는 어떠한 서비스를 제안하는 것은 가능할 것입니다. 물론, 현실적으로 불가능한 서비스일 수 있을지 모릅니다. 하지만 과거에 보행 패턴을 인식하여 개인을 인식하는 것을 불가능하다고 생각했을지 모르지만 현재 가능하게 된 것처럼, 과거 인공지능을 이론적으로만 생각했지만 컴퓨터 성능의 발전으로 실현이 된 것처럼 암호 학문의 발전에는 큰 도움이 될 것이라고 생각합니다.

교육의 기회

프로그래밍을 가르치는 학원은 넘쳐나는 반면 암호학원은 들어본 적이 없습니다. 제가 이토록 양성과정에 참여하고 싶은 이유도 이러한 양질의 수업을 들을 기회가 흔치 않기 때문입니다. 앞으로도 이번과 같은 체계적인 교육의 기회가 많았으면 좋겠습니다. 흥미를 갖고 입문하는 사람들에게 가이드가 되었으면 합니다.

커뮤니티

코딩을 하는 사람들은 스택오버플로우라는 곳에 가서 자신의 정보를 공유합니다. 암호를 하는 사람도 이렇게 자신의 생각을 공유하여 새로운 아이디어가 창출되도록 하면 좋을 것 같습니다. 코딩도 창의력이 필요하지만 암호기술도 창의력이 필요하기 때문입니다. 제가 아이디어를 얻을 때는 혼자서 번뜩 떠오를 때도 있지만 주로 많은 사람들과 대화를 통해서 얻게 되는 경우가 훨씬 더 많습니다. 같은 분야를 공부하더라도 사람마다 생각하는 점이 다를 수밖에 없었고 이러한 차이가 새로운 관점을 주었기 때문입니다. 따라서 자신의 정보를 공유할 커뮤니티가 있다면 좋을 것 같습니다.

기관에서는 이런 부분들을 장려하여 최첨단 기술을 우리나라가 선도하도록 했으면 좋겠습니다. 저도 열심히 노력하여 가까운 미래에 한국의 암호기술의 발전에 조금의 보탬이 되도록 하겠습니다.

저는 암호기술 분야에 숙련된 지식을 가지고 있는 사람은 아닙니다. 하지만 암호기술에 애정을 가지고 있습니다. 그렇기에 많은 홍보를 통해 널리 알려졌으면 좋겠고 국내의 기술로 만들어진 암호 기술이 더욱 늘어나길 바랍니다. 또한, 많은 사람들의 연구에 도움이 될 수 있게 영어로 된 전문 영어에 대한 통일된 해석, 국문으로 된 매뉴얼의 제작, 국내산 암호 기기들이 많기를 희망합니다. 또한 많은 교육의 기회와 활성화된 커뮤니티를 통한 원활한 의사소통이 되었으면 좋겠습니다. 바라는 점만을 작성하게 되어 민망합니다. 열심히하는 모습으로 보답하겠습니다. 읽어주셔서 감사합니다.