자 기 소 개 서

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

[지원동기]

전문가 분께 암호교육을 받을 수 있다는 이런 기회를 놓이고 싶지 않기에 국가 암호 기술 전문 인력 양성 과정에 지원하였습니다. 이번 교육과정에서는 AI와 실용 암호기술이라는 주제로 교육이 진행되는 것을 보았습니다. 작년 국가 암호 기술 전문 인력 양성 과정의 교육과정에서 AI를 사용한 부채널 분석 주제에 대하여 꼭 듣고 싶었지만 아쉽게도 선전되지 못해 아쉬웠던 경험이 있습니다. 이번에도 동일한 AI를 사용한 부채널 분석 교육을 들을 수 있다는 점과 함께 실용적인 암호모듈 계발과 사용을 위한 암호모듈의 안전성 및 검증, 최근 나날이 발전해가는 IoT에 대한 보안에 실용적인 교육을 들을 수 있는 IoT 무선 취약점 및 암호, 암호와 범죄와 관련하여 밀접한 디지털 포렌식과 암호라는 다양한 주제의 교육을 앞서 연구하시는 전문가 분들의 교육을 꼭 듣고 싶습니다.

최근 이러한 교육들을 듣는 것이 얼마나 값진 경험인지 알게 되었습니다. 기본적인 지식들이 다양하게 적용되는 것이 중요하다는 것을 작년 3회 부채널 문제풀이를 참가였을 때 느꼈습니다. 부채널 분석 문제는 AES로 암호화된 한글 문서를 주어진 7과 8라운드의 소비 전력 파형과 10라운드의 라운드키의 7바이트가 주어지고 해당 한글파일을 복호화하고 내부의 문제를 푸는 것입니다. 처음 생각해낸 방법으로 공격을 위해서는 AES의 연산 중에 4byte 연산인 Mixcoum 연산을 거처야 했고 너무 많은 전수조사 횟수가 필요했습니다. 작년 대회 문제에 많은 시간을 들여 풀어보았지만 끝내 풀지 못했다는 점과 막막한 상황이 겹쳐 해당 문제가 너무 어렵게 느껴졌습니다. 그러나 답이 있는 문제는 시간을 투자하면 뭐든지 풀 수 있다는 믿음으로 가능할 것 같은 방법을 여러 번 시도하였습니다. 여러 시도 가운데에 AES에 대해서 다시 공부해보자 했고 결과적으로 AES의 Mixcoum 연산이 선형 연산이라는 점을 사용하면 사전 조사 횟수를 줄일 수 있다는 것을 알게 되어 해당 문제를 풀 수 있었습니다. 끝까지 해보겠다는 마음과 다시 한번 공부해보는 식으로 해결할 수 있었습니다. 그 다음 한글파일속의 문제는 ECDSA에서 같은 난수 k를 사용하면 개인키를 알아낼 수 있는 점을 사용하여 개인키를 알아내는 것 이었고 검색을 통해 풀 수 있었습니다. 어떻게 보면 이미 잘 알려진 문제이지만 처음 봤을 때는 이러한 정보를 알 수 없어서 매우 어렵게 느껴졌습니다. 이렇게 문제를 풀다보면 처음에는 어려웠지만 알고 보면 쉬운 문제들이 있습니다. 이유는 얕고 고정적인 생각 때문이라고 생각됩니다. 전문 인력 양성 과정의 암호 기술 교육을 받을 수 있다면 암호에 대한 다양하고 유연한 지식을 바탕으로 앞으로의 제게 큰 기반이 될 것이라 생각합니다.

그리고 이전 지원에 합격하여 참여했던 선배들에게 이 교육과정이 매우 큰 도움이 되었다고 들었습니다. 다양한 연구 분야로 연구한 사람들과 교류 할 수 있는 공간이 되었다고 장점을 이야기해 주었습니다. 저는 여러 공모전 경험을 통해 협력의 상승효과를 낸다는 것을 크게 느꼈습니다. 공모전에서 누군가의 아이디어는 다른 사람의 의견을 통해서 좀 더 강화되고 세세한 부분까지 바라볼 수 있었으며, 각자 충실한 역할 수행과 이견을 조율을 통해서 완성할 수 있었습니다. 국가 암호 기술 전문 인력 양성 과정의 교육과정에서 다른 연구자분들과 함께 교류할 수 있는 점에서 토론하며 배워가는 경험을 쌓고 싶습니다.

[관심 연구 주제]

저는 부 채널 분석, 암호구현, 블록체인 연구에 관심이 있습니다. 먼저 이러한 연구 주제와 관심을 두게 된 이유에 대해 설명해 드리고 싶습니다. 처음 연구라 비스름하게 표현 할 수 있는 졸업 작품에서 저는 'VR 상의 키보드 입력장치'라는 주제로 대학 졸업 작품 프로젝트를 진행했습니다. VR 상에서는 기존 PC의 키보드와 같은 타이핑 장치가 없고 음성입력 같은 장치는 보안 측면에서 민감한 정보를 입력할 때는 부적합하기 때문에 이러한 장치가 필요하며 새로운 키보드 인터페이스를 제안한 아이디어의 졸업 작품이었습니다. 결과로 VR에서 사용하는 장갑형의 손 모션 인식 장치와 사용할 수 있는 키보드 인터페이스를 만들었습니다. 처음에는 VR과 관련된 아이디어를 생각해 보았지만 생각지 못하게 보안과 관련된 연구를 하게 되었습니다. 이후에 지금 지도교수님이신 서화정 교수님께서 국가암호 공모전을 소개해 주시며 참가를 권유해 주셨습니다. 이때 졸업 작품에서 사용했던 아이디어를 기반으로 'VR 상에서의 안전한 PIN 입력'이란 주제로 논문을 제출하였고 장려상을 받을 수 있었습니다. 그리고 같은 공모전에서 동시에 참여할 수 있었던 2분야에서 '스마트 컨트랙트를 활용한 아동 급식 시스템'으로 제출하여 총 2개의 장려상을 받을 수 있었습니다. 대부분 잘 알지 못하는 지식에 기반하고 처음 써보는 툴과 언어들을 사용해야 하는 것이 힘들었지만 하나씩 해결해나가는 성취감과 완성할 수 있었던 것에 대한 보람을 느낄 수 있었습니다. 이때 프로젝트들을 통해서 복잡한 수학이며 접근하기 어렵다고 생각하고 있었던 암호에 대한 인식을 바꿀 수 있었습니다. 저는 크게 관련이 없다고 생각했던 VR과의 연관성, 암호 기반 화폐를 접하게 되면서 암호란 우리가 사용하는 시스템 대부분에서 적용되는 밀접한 관계이며 새로운 기술들과 함께 사용되는 다양한 기법과 용도가 있다는 것임을 알게 되었습니다. 그렇게 암호에 관해서 공부해보고 싶다는 마음과 함께 대학원 진학하였습니다.

대학원에 진학을 결정하고 겨울방학 다른 대학 연구실에서 연구를 도와주면서 교류하는 기회가 있었고 부 채널 분석에 대하여 알게 되었습니다. 그때 처음 부 채널 분석에 대하여 알게 되었습니다. 전자장치에서 암호 알고리즘이 작동될 때 의도치 않게 발생하는 누수 정보를 통해서 수학적으로 안전성이 증명된 암호도 공격이 가능하다는 새로운 사실에 놀랐습니다. 그러나 처음 알게 된 만큼 도움이 되지 않았다는 생각이 들었고 관련 지식은 백지 상태지만 부채널 분석에 대하여 연구해보겠다는 목표를 세우게 되었습니다. 대학원에 입학 후 소속한 연구실이 생긴 지 2년째여서 부 채널 분석에 대하여 알려줄 사람이 없었습니다. 다행히도 연구실에 chipwhisperer라는 부 채널 분석 장비가 있어 해당 장비를 사용하는 방법을 공부하면서 부채널 분석을 위한 코드를 작성 할 수 있었습니다. 이후에 상용 부채널 도구의 오픈SW 소스코드 분석 연구과제 참여를 통해서 소프트웨어의 소스 코드를 분석하는 경험을 할 수 있었습니다. 해당 프로젝트는 해당 소프트웨어 분석을 통해서 전반적인 구조를 분석하여 개선이 필요한 점을 찾거나 필요에 따라 변경하거나 추가하여 자산화하기 위한 분석 과제였습니다. 해당 프로그램은 전력 수집을 위한 장치와 연결되어 소스코드 업로드, 수집환경, 입력 전송, 출력확인 등의 역할을 하는 캡처와 수집된 파형을 분석하는 어널라이저로 구성되고 소스코드는 사용자가 편리하게 기능을 추가 할 수 있도록 최대한 캡슐화 되어있었습니다. 따라서 함수와 모듈의 수가 많아 단순히 함수 호출을 확인하는 것만으로는 분석이 어려웠습니다. 그래서 동작의 흐름을 이해하기 위해선 부채널 분

석 과정에 대한 이해가 있어야 했으며 이를 위해 부채널에 대한 지식을 공부하였고 각각 모듈과 함수의 역할과 연결되는 지점을 파악하여 소스 코드의 기능을 변경하거나 추가 할 수 있었습니다. 이후에도 과제를 통해 익힌 툴을 여러 방면으로 사용할 수 있었습니다. 2~3회 부 채널 분석 경진 대회에 참가하여 의미 있는 상을 수상할 수 있었습니다. 또한 부채널 분석에 영향을 미칠 수 있는 AVR 어셈블리 코딩을 배우고 암호 모듈을 안전하게 구현할 수 있는 마스킹 기법을 공부하고 익힌 프로그램 툴을 사용하여 '초경량 블록 암호 CHAM에 대한 CPA 공격과 대응기법 제안'이란 논문 게재 하였습니다. 국산암호 CHAM에 구현과 공격을 해보았고 마스킹 기법을 적용한 후 안전성을 확인 할 수 있었습니다. 그리고 암호 모듈의 파형을 수집하고 해당 파형을 기반으로 작업증명 방식을 제안하는 논문을 작성하여 게재 할 수 있었습니다. 비트코인과 같은 PoW 방식의 합의 알고리즘을 사용하는 블록체인은 현재 값비싼 ASIC 채굴기를 사용해야 되어 일반사용자의 채굴 참여는 불가능에 가까워 졌습니다. 이러한 점을 고려하여 암호모듈을 동작할 때 발생하는 전력파형을 작업증명에 추가하여 저사양의 마이크로 컨트롤러 기반의 합의 알고리즘을 제안한 'ASIC-Resistant Proof of Work based on Power Analysis of Low-end Microcontrollers'란 SCIE논문을 게재 할 수 있었습니다. 잘 알고 시작하지 않았지만 작은 성과부터 하나씩 이루어가며 더 높은 결과를 낼 수 있었습니다. 국가 암호 기술 전문 인력 양성 과정에 선정된다면 교육받은 내용을 원동력으로 최선을 다하고 싶습니다.

앞으로의 연구는 NIST에서 공모전 진행중인 PQC와 경량암호에 대한 구현과 부 채널 분석에 관심을 갖고 있습니다. NIST 양자 내성 암호 공모전은 암호 학계에서 큰 관심을 받고 있으며 내년 NIST에서는 2022년에 초기 표준을 작성할 예정으로 이후에 많은 사용이 예상됩니다. 실제 사용에는 실용적인 구현과 부 채널적인 분석이 필요합니다. 그렇기에 IoT 환경을 위한 최적화된 실용적인 구현에 대하여 연구 중으로 먼저 결선에 진출한 NTRU의 곱셈을 최적화하여 ARMv8에 구현을 진행 중입니다.

[바라는 점]

이전 참여했던 선배들에게 교육해주시는 전문가 분들께서 큰 지원과 열정을 다해주신다고 들었습니다. 이러한 기회의 과정이 있다는 것에 대하여 감사드립니다. 이러한 과정에 참여하게 된다면 다양한 전문가 분들에게 교육받을 수 있어 기쁠 것 같습니다. 그러나 접해보지 않은 분야가 교육과정에 포함되어 있어 기대되지만 잘 따라가지 못할까봐 다소 걱정됩니다. 잘 모르는 분야에 대해서도 흥미롭게 학습할 수 있도록 지도해주셨으면 합니다.

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

4차 산업시대에 여러 분야에서 새로운 기술 혁신이 나타나며 여러 분야가 융합되는 만큼 어느 한 곳에서 해결하기에는 힘든 문제입니다. 때문에 여러 대학, 연구소, 기관, 산업계가 정보를 공유하고 협력해야 된다고 생각합니다. 초등학교 코딩수업을 할 정도로 ICT가 실생활에 매우 밀접한 시대가 됬으며 많은 새로운 기술들의 등장과 실생활에서의 보안 취약점은 함께 증가할 것 입니다. 보안의 필요 늘어날 것이므로 빠른 변화에 적응을 위해서는 교육 확대가 더 필요할 것이라 생각됩니다. 이번 국가 암호 기술 전문 인력 양성 과정과 같은 교육의 증대를 통해서 많은 관심과 기회를 준다면 국내 암호 기술의 발전이 이루어 질것이라고 생각합니다.

그리고 이전에 KCMVP 암호모듈 검증에 대해 강연을 들은 적이 있습니다. KCMVP 행정기관 등 국가·공공기관의 중요 정보를 보호하기 위해 도입하는 국산 알고리즘을 탑재한 암호모듈의 안전성과 구현 적합성을 검증하는 제도입니다. 이 KCMVP를 한번에 통과한 곳이 엄청 드물다는 이야기를 들었습니다. 물론 꼼꼼하게 검증하기 때문에 힘든 것 일 수 도 있지만 보안 요구사항을 지키면서 구현하는 것이 현업에 종사하는 전문가 또한 어려운 일이라는 생각이 들었습니다. 이러한 점에서 암호기술에 관한 협력이 필수적이라는 생각 됩니다. 이러한 문제를 방지하기 위해 NIST의 보안성 자동평가 프로토콜 같은 한국의 환경에 맞는 국산 프로토콜을 통해 편의성을 주어야한다고 생각합니다. 여러 대학, 연구소, 기관, 산업계가 정보를 공유하고 협력해야 된다고 생각합니다.