자 기 소 개 서

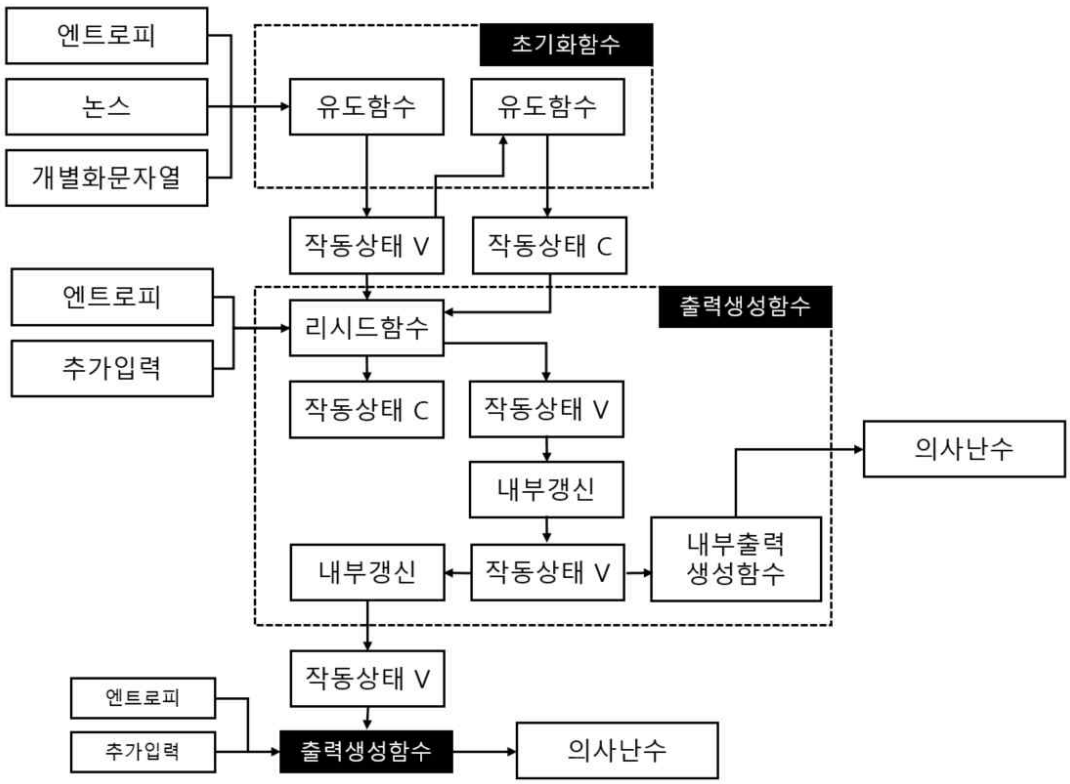
1. 관심 연구 주제 / 지원 동기 / 바라는 점에 대해 기재해 주십시오.

[행적 및 지원 동기]

제가 암호 분야에 발을 담그게 된 것은 그리 오래 되지는 않았습니다. 최초로 보안과 연관된 것을 배우기 시작한 것은, 학부 3학년 네트워크 보안 수업에서입니다. 수업에서는 RSA에 대한 원리를 이해하면서 암호에는 복잡한 수학적 원리가 들어있다는 것을 이해할 수 있었으며, DDoS에 관한 조사 및 발표를 진행하며 단순한 공격으로 매우 큰 피해와 사회적 혼란을 가져올 수 있다는 사실을 알았습니다. 이후 저는 트위터 서드 파티 어플리케이션을 개발하는 프로그래밍 동아리 활동을 하며 암호와 관련된 또 다른 경험을 하게 되었습니다. 유통되는 어플리케이션 중에는 잠금 기능을 지원하는 어플리케이션도 존재합니다. 대부분의 방식은 패턴을 긋는 방식이나 일정 자릿수의 숫자를 입력하는 전통적인 패스워드 방식을 사용합니다. 하지만 저희 팀은 사용자 경험과 어플리케이션의 테마에 걸맞도록 특별한 방식을 하나 만들어보자고 의견을 조율하였습니다. 그 결과 컬러를 조합하는 형식의 잠금 방식을 만들었습니다. 이 방식은 잠금이 열리는 색인 '키 컬러'를 지정합니다. 이후 잠금 화면에서는 기본 9가지 색상 중에서 키 컬러를 완성할 수 있는 색상을 선택하면 잠금이 풀리는 방식이었습니다. 이러한 방식은 어플리케이션의 테마인 팔레트와 매우 잘 맞았으며 사용자에게도 특별한 경험을 선사해줄 수 있어서 좋은 아이디어라 생각하였습니다. 하지만 보안과 암호에 대해서 배운 지금, 제안한 방식은 부적절하다 생각하고 있습니다. 이유는 조합의 가짓수가 오히려 줄어들기 때문입니다. 구체적으로는 숫자를 조합할 경우에는 숫자의 순서가 바뀌면 서로 다른 조합이지만 색상을 조합할 경우 색상의 순서가 바뀌더라도 같은 값을 도출합니다. 가령 1, 2, 3 조합과 1, 3, 2 조합은 서로 다른 조합입니다. 하지만 색상을 조합할 경우, 빨강, 파랑, 초록 순으로 조합한 것과 빨강, 초록, 파랑 순으로 조합한 결과물은 같습니다. 암호에 있어서 조합의 가짓수가 줄어드는 것은 그만큼 안전성에 지장을 초래하기 때문에 부적절한 설계였습니다.

이후 학부 4학년으로 올라간 저는 서화정 교수님의 권유로 졸업에 이어 대학원에 진학하게 되었습니다. 대학원에 진학하면서 본격적으로 보안, 특히 암호에 관해서 배우기 시작했습니다. 처음에 제가 경험한 프로젝트는 국가보안기술연구소 위탁 연구인 해시함수 구현 적합성에 관한 연구였습니다. 당시 해시함수는 처음 듣는 생소한 개념이었고 암호 모듈의 레퍼런스 코드 없이 공개되어 있는 문서만을 통해 직접 구현하였습니다. 사용했던 해시함수는 SHA-3와 LSH였습니다. 이 중에서 LSH(Lightweight Secure Hash)는 국가보안기술연구소에서 개발한 국산 해시함수였습니다. 저는 여기서 한 가지 충격을 받았습니다. 암호 분야를 알지 못했을 때는 암호는 전부 외국 기술이라고 생각했고, 국내에 암호 연구가 활발히 진행되고 있었는 줄 미처 몰랐습니다. 하지만 국내의 각계에서 노력한 분들이 많이 있었으며 국산 암호 기술이 지속적으로 개발되고 있었다는 것을 그때 알았습니다. 구현적합성 연구도 기술의 국산화를 위한 분야였습니다. 현재 사용하는 암호 모듈의 내부에는 해시함수가 적용되는 부분이 있습니다. 이 해시함수를 국산 해시함수인 LSH로 교체하는 것은 단순하나, 해당 값에 대해 신뢰도에 문제가 생깁니다. 이를 극복하기 위해서 서로 다른 연구진이 하나의 모듈에 LSH를 이식하여 같은 값을 가

지는지 확인하는 것이 연구의 골자였습니다. 가장 어려웠던 부분은 DRBG(Deterministic Random Bit Generator)의 구현이었습니다. DRBG는 난수를 생성하는 알고리즘입니다. 컴퓨터의 함수는 입력한 값에 따라 균일한 출력 값을 가지기 때문에 완전한 난수를 생성하기는 어렵습니다. 하지만 DRBG는 그런 조건 하에서도 최대한 난수와 유사하도록 값을 생성하는 알고리즘입니다. 여기서 DRBG는 유도 함수, 내부 출력 생성 함수, 초기화 함수, 리시드 함수, 출력 생성 함수로 구성됩니다. 각각의 함수는 여러 입력을 받지만 가장 중요한 입력 값은 상태 값입니다. 상태 값은 두 종류로, 지속적으로 변하는 값인 V(Variable)와 고정 값인 C(Constant)로 구성됩니다. V는 외부에서 수집한 엔트로피, 고유의 고정 값인 논스 마지막으로 추가 옵션으로 개별화 문자열을 기본으로 사용하며 알고리즘의 동작에 따라 변경됩니다. C는 V에서 초기에 유도된 다음 고정 상태로 남습니다. DRBG는 초기화 이후 리시드 함수를 반복하며 상태 값을 바꾼 다음 최종적으로 출력 함수를 통해 난수 값을 생성하게 됩니다. 대학원에 들어와서 진행한 첫 연구였지만 성공적으로 완수할 수 있었습니다. 이를 통해서 저는 어려운 구현 과제를 해냈다는 성취감을 느낄 수 있었습니다. 또한 단순히 주어진 과제를 진행하는 것뿐만 아니라 DRBG에 대한 개인적인 공부를 해보았습니다. 저는 DRBG를 면밀하게 살펴보던 도중 한 가지 특이한 구조를 발견하였습니다. DRBG는 내부에 반복적으로 진행되는 부분이 여러 군데 존재하는데, 그 중에서 일부 반복 구간은 반복에 사용되는 값이 서로 영향을 주지 않고 독립적임을 발견했습니다. 조금 더 구체적으로는 [그림 1]의 초기화함수에 위치한 유도함수는 내부에서 데이터 갱신을 최대 3회까지 반복하며, 출력생성함수에 위치한 내부출력생성함수의 내부 구조에는 난수 출력 규격에 비례해서 반복을 진행합니다. 어떤 함수가



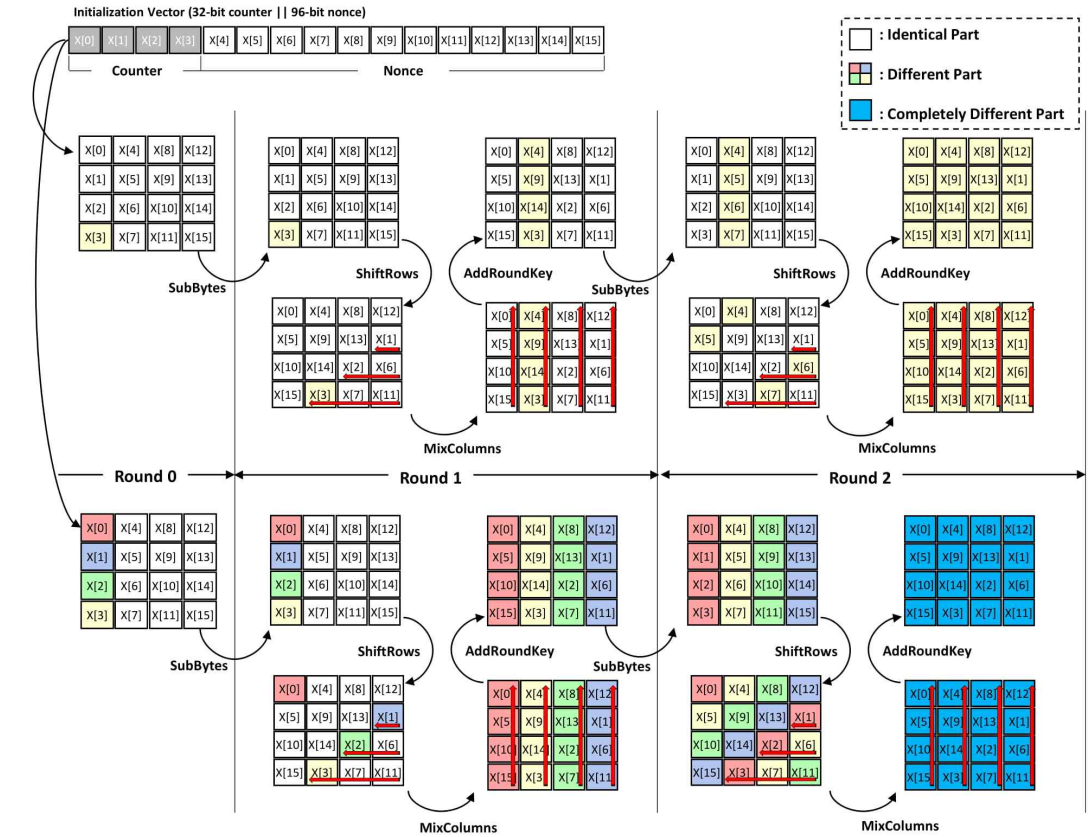
[그림 1] DRBG의 구조

반복되고 있을 때, 반복하며 나오는 값이 입력 값으로 쓰이지 않는다면 반복을 하지 않는 대신에 여러 개의 함수를 동시에 가동하면 반복하는 시간만큼을 줄일 수 있어서 암호 알고리즘을 더욱 빠르게 가동할 수 있습니다. 쉽게 말해서 병렬화를 적용한다는 것입니다. 저는 병렬화에 대한 지식은 없었지만 병렬화를 사용할 수 있게 해주는 다양한 모듈이 있다는 것을 교수님을 통해서 알게 되었습니다. 그 중에서 저는 손쉽게 사용할 수 있는 OpenMP를 사용하였습니다. 하지만 예상과는 달리 처음 OpenMP를 사용하여 병렬화를 적용했을 때는 속도가 향상되지 않았습니다. 그 이유는 스레드를 생성하고 할당 및 해제하는데 들어가는 시간이 함수를 반복하는 시간보다 더 오래 걸렸기 때문입니다. 저는 단순히 병렬화를 적용하는 것으로 속도 개선이 있을 것이라 생각했는데 이 생각이 짧고 안일했습니다. 조금 더 면밀하게 살펴본 결과 반복 구간이 짧은 곳에는 스레드를 관리하는 시간이 더 길기 때문에 해당 구간은 병렬화를 제거하고 긴 반복 구간에만 병렬화를 적용하는 것으로 만족스러운 성능 향상을 이끌 수 있었습니다. 저는 해당 연구 결과를 갈무리하여 학술대회에 제출하였고 LSH를 사용한 DRBG라는 점에서 국가보안기술연구소의 박사님들의 이목을 이끌 수 있었습니다. 저의 첫 최적 구현 경험과 함께 대학원 첫 1년을 마칠 수 있었습니다.

그 다음 제가 접한 분야는 부채널 공격 분야였습니다. 교수님께서 가장 대중적인 기기이며 접근성이 좋은 Chip-Whisperer Lite를 제공해 주셨습니다. 저와 연구실 팀원은 Chip-Whisperer의 소프트웨어를 분석하는 국가보안기술연구소 위탁 연구 과제를 받아서 소스 코드 분석에 나섰습니다. Chip-Whisperer의 소프트웨어는 오픈소스로서 모든 소스 코드가 공개되어 있습니다. 하지만 프로그램의 규모가 방대하고 동작 원리에 대해서 이해하는 사람은 거의 없습니다. 저희는 Chip-Whisperer가 오픈소스라는 장점을 살려 소스 코드 분석에 나섰고, 최종적으로 이 소프트웨어를 개량할 수 있는 방법을 모색하였습니다. 저희가 분석한 Chip-Whisperer은 크게 세 부분으로 나누어집니다. 첫째는 공통적으로 사용되는 부분을 정의한 메인 API, 둘째는 파형 수집을 위한 Capture 소프트웨어, 셋째는 파형 분석을 위한 Analyzer 소프트웨어입니다. 메인 API 부분에는 Chip-Whisperer의 Capture와 Analyzer에서 공통적으로 사용하는 부분에 대한 정의가 이루어져 있습니다. 대체로 UI 정의와 이벤트 리스너, 예외처리에 관한 항목이 있으며 공통적으로 사용하는 메뉴에 관한 호출 및 정의도 이 부분에서 이루어집니다. 따라서 메인 API를 수정하는 것으로 Capture와 Analyzer 소프트웨어 공통으로 사용할 수 있는 부분을 추가하거나 수정을 가할 수 있습니다. 특이한 점으로는 각각의 소프트웨어에서 사용할 모듈 호출도 메인 API에서 이루어지나, 실제로 메인 API에는 정의는 되어있지 않습니다. 이러한 구조가 적용된 이유는 Capture와 Analyzer 두 소프트웨어에서 사용하는 모듈이 다르기 때문에 메인 API에서 호출한다면 필요하지 않은 모듈의 호출 가능성이 존재하기 때문입니다. Capture 소프트웨어는 Chip-Whisperer의 타깃 보드에서 암호 알고리즘을 가동하면 그에 따른 전력 파형을 수집하는 오실로스코프와 관련된 프로그램입니다. 사용자가 일일이 오실로스코프와 타깃 보드, 그리고 컴퓨터와 연결을 하는 것은 손쉽지 않지만 Chip-Whisperer Capture 소프트웨어를 사용하는 것으로 간단하게 연결할 수 있습니다. 이를 위해서 Capture 소프트웨어에는 Chip-Whisperer에서 사용하는 스마트카드, SASEBOW-W 등의 보드와 이를 연결하기 위한 SimpleSerial, Universal Serial 등의 reader를 정의하고 있습니다. 이러한 정의는 사용자가 Chip-Whisperer의 어떤 보드를 연

결하든 Capture 소프트웨어에서 연결한 보드와 동일한 보드를 선택하는 것으로 쉽게 사용할 수 있게 도와줍니다. 만약 사용자가 설정을 어려워한다면 scripts를 통해 기본 설정을 자동적으로 설정할 수 있게 합니다. 초기 사용자를 위해서 기본적으로 사용하는 키와 평문 등의 예시가 있으며 타깃 보드 상에 사용자의 코드를 업로드 할 수 있는 방편도 존재합니다. 수집한 파형은 Capture 소프트웨어에서 처리하며 사용자가 알아볼 수 있게 그래프와 같은 형태로 출력해줍니다. 또한 그래프 외에도 수치 값이 필요하다면 DPAv3와 같은 형태로 텍스트 형태로 값을 획득할 수도 있습니다. Analyzer 소프트웨어는 파형을 분석하기 위해 제공하는 소프트웨어로 Capture와는 다르게 하드웨어 적인 부분은 전혀 정의되어있지 않습니다. 반대로 암호 알고리즘에 대한 정의가 있는데, 가장 대표적인 알고리즘인 DES와 AES가 정의되어 있습니다. 원하는 암호 알고리즘이 없을 확률이 높기에, 사용자는 소스코드를 편집하여 새로운 암호 알고리즘을 포함시킬 수 있습니다. 하지만 일반 사용자가 직접 암호 알고리즘을 소프트웨어에 직접 포함시키는 것은 어렵기 때문에 이를 위해서 암호 알고리즘을 모듈화 할 수 있는 클래스를 제공합니다. 사용자가 모듈 작성 규칙에 따라서 알맞게 작성할 수 있다면 암호 알고리즘을 포함시킬 수 있습니다. 모듈 작성 방법은 복잡하고 어렵기 때문에 저희는 누구나 모듈을 추가시킬 수 있도록 면밀한 분석을 통해 Analyzer 소프트웨어에 암호 알고리즘을 포함하는 방법을 가이드 형태로 정리했습니다. 소프트웨어 분석과는 별개로 이 부채널 장비를 활용하여 암호 알고리즘의 키를 획득하는 방법에 대해서 흥미를 가졌습니다. 놀라웠던 점은 Chip-Whisperer 장비가 수집한 전력 소모 파형을 통해 키 값이 유출된다는 점이었습니다. 이는 단순히 '패스워드를 지키면 안전할 수 있다'라는 생각에서 벗어나서 조금 더 고차원적인 위험을 마주하는 순간이었습니다. 여기서 저희가 사용한 방법은 CPA(Correlation Power Analysis)라는 공격 방법이었습니다. CPA 공격은 예측 파형, 실제 수집 파형의 두 가지 파형을 사용합니다. 여기서 예측 값과 실제 값을 비교하여 값의 일치 여부로 키를 유추하는 것이 CPA 공격의 골자입니다. 저희는 한국전파통신연구원에서 개발한 블록암호 CHAM에 CPA 공격을 시도하였고 성공적으로 키 값을 획득했습니다. 이렇게 부채널과 관련한 지식을 쌓아가던 도중, 우연히도 암호분석 경진 대회가 열렸습니다. 해당 대회에는 부채널 분석과 관련된 문제가 있었기 때문에 저희는 짧은 시간이었지만 얻은 지식을 통해 문제를 풀어보고자 하였습니다. 문제는 알려지지 않은 암호 알고리즘의 키 값을 획득하는 고난이도의 문제였습니다. 어떤 암호를 사용했는지 알 수 없었기 때문에 저희는 공격 지점을 정확히 파악할 수가 없었습니다. 그래서 대안으로 완벽한 키 값을 찾는 대신에 키 값으로 가능한 값을 추려내는 것에 집중했습니다. 저희의 대안은 성공적으로 적중하였고, 키 값이 될 수 있는 범주를 짚어주는 것을 인정받아 장려상을 수상할 수 있었습니다.

이와 더불어 국가암호공모전에 도전하게 되었습니다. 저희 팀에서는 AES에 관한 최적 구현을 시도하였습니다. 기존에 발표된 FACE(Fast AES-CTR mode Encryption)라는 AES 최적 구현 알고리즘을 조금 더 개량하는 것을 목표로 두었습니다. FACE는 AES의 카운터 모드에 관한 최적 구현입니다. 카운터 모드는 암호 알고리즘의 동작 모드 중 하나로, 입력 값은 고정 값인 논스와 카운터 값을 조합하여 이를 키 값과 사용하여 암호화하는 모드입니다. FACE는 첫 블록과 마지막 블록의 차이는 단지 마지막 바이트 하나만 차이나며 나머지는 동일하다는 점에 착안하여 사전 테이블을 사용합니다.

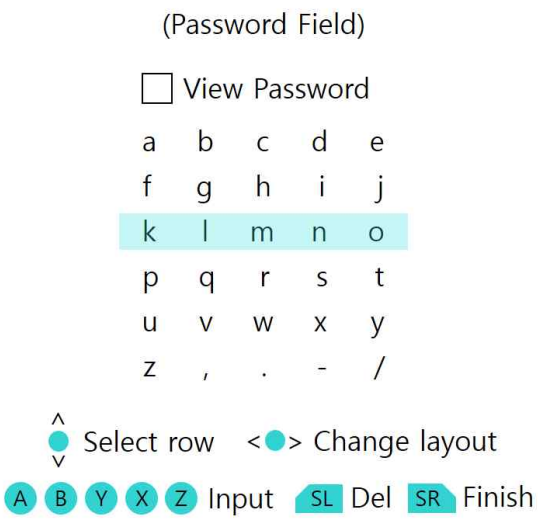


[그림 2] 카운터 1바이트의 전파 과정

이는 암호 알고리즘의 두 라운드 정도를 건너뛸 수 있기 때문에 강력한 최적 구현이 됩니다. 저희는 이를 확장하여 카운터에 의존되는 반복 부분의 전체를 저장하기로 했습니다. 카운터의 전체는 4바이트이며 이는 네 개의 블록으로 저장됩니다. 예시는 [그림 2]에서 카운터의 첫 바이트를 사용합니다. 첫 바이트의 값은 SubBytes 과정 때는 블록 이동이 발생하지 않습니다. SubBytes는 8비트 치환 연산을 할 뿐, 이동과는 관계가 없기 때문입니다. 다음 ShiftRows 과정에서도 이동이 없습니다. 현재 바이트가 위치한 행은 첫 번째 행인데, ShiftRows 과정에서 첫 번째 행은 블록이동이 발생하지 않기 때문입니다. 이후 MixColums 단계에서 블록이 가진 정보가 자신이 위치한 열에 전파됩니다. 다음 라운드에서는 SubBytes 과정은 동일하게 아무 이동이 없고, ShiftRows는 규칙에 따라 이동합니다. 여기까지는 최초 블록이 다른 열에 영향을 주지 못한 것을 알 수 있습니다. 하지만 MixColums 단계를 거치면서 다른 블록에도 모두 최초 블록의 정보가 전파 됩니다. 따라서 두 번째 MixColumns 연산 직전의 값을 사전 연산 테이블로 만들 수 있습니다. 이와 같이 각각의 카운터 바이트 블록은 두 번째 라운드의 MixColums 단계 직전까지 영향을 주지 않고 서로 독립적으로 연산되므로, 두 번째 라운드의 MixColums 단계 직전의 값을 사전 테이블로 저장합니다. 하나의 바이트는 256개의 값을 지닐 수 있기 때문에 블록 하나가 차지하는 테이블의 크기는 1KB가 되며, 카운터 전체가 4바이트 이므로 테이블의 크기는 전체 4KB가 됩니다. 최종적으로 저희의 결과물은 표준적인 AES보다 약 22% 가량의 괄목할만한 성능 향상을 이끌었습니다. 저희는 이 결과물을 국가암호 공모전에 제출하여 장려상을 수상하였고, ICISC'19에도 게재가 되었습니다. 또한 갈로아

카운터 모드(Galois Counter Mode, GCM)를 사용한 형태인 AES-GCM 모드의 추가 최적화를 구현하여 SCI급 논문지에 게재가 확정되었습니다.

키 입력 보안에 관심을 가지고 있었던 저는, 저의 학부생 동아리 경험을 떠올리며 새로운 형태의 보안 키패드를 개발하였습니다. 당시 저는 취미 생활로 닌텐도 스위치로 게임을 즐기곤 했습니다. 닌텐도 스위치는 휴대용, 가정용을 아우르는 하이브리드형 게임기로, 최신형 세대에 걸맞게 인터넷에 접속할 수 있습니다. 인터넷, 특히 닌텐도 쇼핑몰에 접속하기 위해서는 자신의 계정과 패스워드를 통해 로그인이 필요합니다. 저는 여기서 한 가지 의아함을 느꼈습니다. 사용자가 패스워드를 입력하는데 있어서 패스워드의 입력 값은 모두 '*'과 같은 형태로 알 수 없게 가려집니다. 하지만 사용자가 지금 어느 값을 입력하는지 알아야하기 때문에 가상 키보드 창에는 커서가 보입니다. 저는 여기서 '*' 문자가 입력될 때 커서의 위치를 보면 값을 알 수 있다는 것을 깨달았습니다. 그리고 몇 번의 실험 끝에 단순히 화면을 보는 것을 통해 패스워드 입력 전체를 획득할 수 있다는 점을 알았습니다. 닌텐도 스위치는 가정에서 대형 모니터를 통해 즐길 수 있으며, 특히 닌텐도의 기업 철학에 따라 여러 명이서 함께 즐기는 파티형 게임이 많습니다. 패스워드를 입력하는 시점에 다른 사람이 있을 수 있을 확률이 높으며, 화면을 보며 커서를 따라가는 것만으로도 패스워드의 전체가 유출된다는 치명적인 결함이 있는 것을 발견했습니다. 저는 이 문제가 발생한 이유를 생각한 결과, 사용자의 편의성과 닌텐도 스위치라는 환경 때문이라는 결론을 내렸습니다. 첫 번째 이유인 편의성은 사용자가 어떤 값을 입력하기 위해서는 자신이 어떤 값을 입력하는지 알아야 합니다. 이를 위해서 가상 키보드의 커서와 같은 형태를 사용하여 사용자에게 어떤 값을 선택중인지 알려주는 편의성을 제공합니다. 하지만 커서는 다른 사람들도 볼 수 있기 때문에 입력 값이 노출되는 결과를 낳으며, 이는 전체 패스워드의 유출로 이어집니다. 두 번째 이유는 닌텐도 스위치 상의 조작 환경입니다. 닌텐도 스위치는 조이콘이라는 전용 컨트롤러를 사용하는데 이것은 키보드, 마우스와는 다르게 입력이 가능한 버튼의 수가 크게 제한됩니다. 알파벳 소문자 수만 고려한다면 26개이므로, 조이콘 만으로는 모든 입력을 할 수 없습니다. 때문에 가상 키보드 상의 커서를 옮기는 조작과 같은 형태를 취할 수밖에 없는 환경입니다. 저는 이 점에 착안하여 닌텐도 스위치라는 조작 환경을 고려하면서도, 화면 정보는 모두가 공유하지만 현재 입력 값은 사용자만 알 수 있게 한다면 패스워드의 유출을 방지할 수 있을 것으로 생각했습니다.



[그림 3] 행렬 형태 보안 키패드

이를 위해서 [그림 3]과 같은 행렬 형태의 보안 키보드를 제작하였습니다. 키보드에 해당되는 키 값을 행렬 형태로 배치한 다음 [그림 3]과 같이 첫 행의 위치만 음영 형태로 짧게 표시한 다음 해당 표시는 사라지게 합니다. 사용자는 컨트롤러의 상하 이동으로 행을 이동할 수 있고 버튼을 통해 열을 선택하게 됩니다. 이때 선택중인 행과 버튼을 통해 고른 열의 교차지점에 위치한 값을 입력 값으로 사용하게 됩니다. 여기서 두 가지 효과가 발생합니다. 첫째로 현재 선택중인 행은 사용자만 알고 있습니다. 비록 처음에 선택된 행의 위치가 표시되지만 이 표시는 곧 지워지며, 사용자가 행을 이동한다면 그 누구도 현재 선택중인 행을 알 수 없습니다. 둘째는 열을 선택하는 순간이 값이 입력되는 순간인데, 기존 닌텐도 스위치의 가상 키보드는 커서가 노출되기 때문에 값 입력 순간 커서의 위치로 입력 값을 획득할 수 있었습니다. 하지만 제가 구현한 행렬 형태 보안 키패드는 열을 선택할 때 값이 입력되며 사용자가 특정 열을 선택하는 버튼을 입력하는 것으로 값을 지정하기 때문에 화면에는 선택하는 열에 대한 정보가 제공되지 않습니다. 저는 제 구현물을 가지고 불특정 다수에게 실험한 결과 모든 경우에서 패스워드 획득에 실패했습니다. 때문에 구현물이 매우 안전하다는 것을 알 수 있었으며, 이 결과를 통해 졸업논문을 작성하게 되었습니다. 저는 이 경험이 인상적이었습니다. 왜냐하면 저의 구현물은 작고 단순한 시점에서 출발했지만 사회적인 공헌도가 크게 작용할 수 있다고 생각했기 때문입니다. 저의 구현물은 불특정 다수가 바라보는 환경에서는 강력한 보안성을 제공합니다. 시작은 닌텐도 스위치라는 게임기를 대상으로 이루어졌지만, 다수가 지켜보는 환경에서라면 언제든지 사용 가능합니다. 조작에 사용되는 버튼은 통상적인 리모콘의 수준이라면 충분합니다. 그러므로 거리나 행사장 같은 사람이 다수 모이는 환경에서도 관리자 권한 같은 것이 필요하다면 제 구현물이 적용될 수 있습니다. 이렇게 대학원 과정을 거치며 저는 보안이 우리의 일상생활에 매우 밀접하게 관련되어 있다는 것을 느꼈습니다. 심심할 때 플레이하는 게임에도 보안 위협은 상시 존재하고 있었고, 약간의 개선으로도 이를 막을 수 있었으며 암호와 보안을 연구하는 각계의 연구진과 박사님들의 노력으로 우리의 보안을 지킬 수 있었습니다.

학업 외에 연구실 생활에서는 제가 연구실의 최연장자이며 선배이기 때문에 새로 들

어오는 학생들이 연구실에 적응할 수 있도록 도움을 많이 주고자 했습니다. 특히 새로운 학생에게 프로그래밍 언어를 가르쳐주는 역할을 많이 했습니다. 스터디로 C언어와 파이썬을 진행하며 학생을 이끌어주고 고생하는 다른 연구실 학생들을 위해 커피 등의 음료를 자주 사주곤 했습니다. 또한 교내 암호동아리 활동도 진행하며 동아리 내 스터디, 정기적인 동아리 세미나를 진행하고 일반인들을 대상으로 한 암호에 관한 설문조사 등을 진행하였습니다. 이러한 노력으로 2019년도에 한국인터넷진흥원의 우수 암호 동아리 상을 수상하기도 했으며, 2020년도에 또다시 암호 동아리로 선정되어 활발한 활동을 이어가고 있습니다.

석사과정을 졸업하고 박사과정을 접한 지금 저는 부족했던 지식을 채우고자 노력하고 있습니다. 저희 연구실에서는 이전 안규황 학생과 권용빈 학생 두 명의 암호기술 전문인력 양성과정의 수료자가 있습니다. 이 두 명의 연구자의 행적을 보고서 저도 본 연구 과정에 지원하고자 마음을 먹었습니다. 이렇게 생각한 계기는 크게 네 가지로 나누어집니다.

첫째로 다양한 지식의 습득을 통해 연구와 공부의 기반을 다질 수 있는 기회를 획득하는 것 입니다. 저는 석사과정을 마치고 박사과정에 막 진학한 학생입니다. 하지만 석사과정 때 습득한 지식만으로는 제가 하고자 하는 암호 구현, 특히 최적 구현과 관련한 부분을 많이 진행하기란 어려울 것이라 생각했습니다. 연구라는 것은 전문 지식을 계속해서 파고 들어야 하는 분야인데, 이를 위한 기초를 닦는 지점, 초석을 다지는 부분이 저는 부족했으며 아직 어떻게 시작해야 할지 막막한 부분이 있습니다. 저는 이것의 해답을 본 교육 과정에서 찾을 수 있을 것으로 생각했습니다. 특히 연구실에서 본 교육 과정을 열심히 이수한 두 명의 학생의 경험담을 들었으며 매달 마다 이수한 수업과 과제물을 관찰한 결과, 한 단계씩 성장하는 모습을 지켜볼 수 있었습니다. 이것으로 저는 본 교육 과정이 체계적인 교육 과정을 제공한다는 것을 느낄 수 있었기에, 제가 이 교육을 열심히 이수한다면 초석을 다지는 것부터 시작하여 한 걸음씩 나아갈 수 있도록 방향을 제시해주리라 굳게 믿고 있습니다.

둘째로는 이번 양성 과정의 세부 주제인 암호 설계 분석 및 구현 기술에 관한 부분입니다. 저는 국가암호공모전을 통해서 얻은 경험으로 최적 구현을 하고자 공부를 하고 있습니다. 최적 구현에 있어서 가장 중요한 것은 암호 알고리즘의 원리를 세세하게 파악하는 것입니다. 최적 구현은 크게 두 가지 형태로 구현할 수가 있습니다. 하나는 병렬화를 적용하는 것입니다. 암호 알고리즘은 반복되는 구간을 많이 사용합니다. 다수의 라운드를 거칠수록 입력 값의 변화가 더 넓게 전파되기 때문입니다. 하지만 반복이 길어질수록 이에 들어가는 시간적 비용이 매우 크게 증가합니다. 이를 타개하기 위해서 반복을 하는 대신에 반복 구간을 동시에 연산할 수 있도록 병렬 연산을 사용합니다. 병렬 연산에는 직접 구조를 병렬로 구현할 수도 있으나 프로세서에 따라 병렬화를 제공하는 경우가 있습니다. 이때는 병렬화 명령어인 SIMD나 병렬화 모듈을 사용하는 것으로 병렬 구현을 시도할 수 있습니다. 병렬 구현의 단점은 반복 구간에서 사용되는 값들이 반드시 서로 독립적이여야 한다는 것입니다. 이전 반복에서 나온 결과 값이 이후 반복에 입력 값으로 사용된다면 병렬 연산을 진행할 수 없습니다. 또 다른 최적 구현 방법은 사전 연산 테이블입니다. 룩 업 테이블(Look Up Table, LUT)로도 불리는 기법으로, 일부 암호 알고리즘은 평문 값이나 키 값과는 상관없이 특정 구간에는 정형화된 값이 지속적으로

발견되는 경우가 있습니다. 만약 이 값이 정말로 고정 값이라는 것이 확실하게 확인 된다면 해당 값을 미리 계산해둔 다음 메모리에 상주시킵니다. 암호 알고리즘 가동 때 메모리에 저장된 값을 가져오는 것으로 일부 연산 과정을 생략하거나 크게는 라운드를 건너뛸 수 있습니다. LUT는 연산 시간을 매우 큰 폭으로 단축시킬 수 있으나 메모리가 충분해야한다는 단점을 지닙니다. 이러한 최적 구현 기법은 한 가지 공통점을 지니는데 그것은 암호 알고리즘에 대한 상세한 원리 분석이 필요하다는 것입니다. 병렬 연산은 아무데나 사용할 수 없으며 잘못된 위치에 병렬화 적용은 오히려 연산 속도에 역효과를 가져옵니다. 사전 연산 기법은 연산 값이 고정적인 부분을 수학적인 계산을 통해 찾아내야만 합니다. 본 교육 과정에 있어서 암호 설계 분석 및 구현 기술은 암호 알고리즘에 대한 심도 있는 교육을 제공할 것으로 예상됩니다. 특히 암호 설계 분석은 최적 구현에 있어서 매우 중요한 부분임을 이미 인지하고 있습니다. 저는 블록암호 알고리즘이 ARX(Addition Rotation eXclusive-or), SPN(Substitution Permutation Network) 혹은 Feistel 등의 기법을 사용하는 것을 알고 있습니다. 하지만 각각의 기법이 어떤 식으로 안전성을 제공하며 기법 별로 장단점이 어떤지, 어느 환경에 적합한지에 대한 내용은 잘 알지 못합니다. 저는 본 교육 과정의 1주차에 블록암호에 관한 설계 기법과 2주차에 암호 라이브러리 활용 및 알고리즘 최적 구현 기술이 있는 것을 확인하였습니다. 또한 마지막 주차의 양자암호에 관한 내용과 같이 암호 원리에 대한 근본적인 수업이 다수 포진하고 있습니다. 때문에 제가 부족한 부분을 본 교육을 통해서 상당수 채울 수 있다는 점이 가장 큰 매력입니다. 저는 이러한 암호 원리에 대한 이해를 통해 더 뛰어난 최적 구현을 이루고 싶으며, 본 교육을 통해 양질의 지식을 습득할 기회를 얻고자 합니다. 이외에도 2주차에는 최적 구현과 관련된 실습이 있는 것을 확인했습니다. 이러한 과제는 실제로 최적 구현을 연습해보면서 제가 지금까지 해본 최적 구현이 아닌 또 다른 방법을 배울 수도 있을 것입니다. 전체적인 교육 과정이 저에게는 최적 구현 기법을 연구하는데 있어서 큰 기반이 되어줄 것이며 나아가 저의 근간을 아우르는 부분이 되리라 생각합니다.

셋째로 제가 어려워했던 부분에 대해서 도움을 받을 수 있는 기회가 되리라 생각합니다. 저는 부채널 공격에 대해서 처음에는 흥미롭게 생각했습니다. 우리가 정면을 바라보는 때 누군가는 생각지도 못한 부분에서 공격을 하여 암호 알고리즘을 파훼한다는 것이 매우 인상적이었습니다. 하지만 부채널 공격은 제 흥미와 의욕을 뛰어넘는 난이도를 가지고 있었습니다. 저의 연구실과 제 주변 사람들에는 부채널 공격의 전문가가 없었기에 근처에서 쉽사리 도움을 구하기도 어려웠습니다. 이번 교육 과정에서는 부채널과 관련한 교육 과정을 제공하는 것으로 알고 있으며, 기존 연구실 수료생을 보고 교육 과정이 쉽지는 않지만 체계적으로 제공된다는 점을 확인했습니다. 본 교육과정을 통해 제가 노력한다면, 부채널 공격에 대해서 차근차근히 심도 있게 학습할 수 있을 거라 생각했습니다. 제가 할 줄 아는 부분은 오실로스코프를 통해 파형을 읽는 부분입니다. 정밀하지는 않지만 본 교육의 4주차 교육과 같이 파형 수집 실습 등의 교육을 따른다면 충분히 숙달할 수 있는 부분이라 생각합니다. 특별하다고 생각한 부분은 AI 기반 부채널 분석 기술이라는 부분입니다. 제 전공이 기계학습과는 거리가 존재하기 때문에 잘 알지 못하지만, 두 기술이 융합할 수 있다는 점에서 신선함을 느꼈습니다. 2, 5주차의 교육을 통해 신경망을 학습시키고 AI를 사용하여 부채널 분석을 할 수 있다면 부채널 분석에 드는

시간과 노력을 절감시킬 수 있지 않을까 기대됩니다. 특히 전력 파형 분석에는 매우 많은 인력이 소요되는 것을 경험하고 나서, 이를 AI가 대체한다면 공격을 훨씬 효율적이며 더 정확하게 시행할 수 있을 것이라 예상됩니다.

마지막으로 다양한 연구원들과 만나며 다양한 사람들과 교류하는 것입니다. 본 교육은 전문적인 내용을 다루고 있기에 교육 내용에 어려움이 있을지도 모릅니다. 때문에 제가 제일 관심을 가지는 최적 구현과 관련된 부분에서 조금이라도 진전을 얻을 수 있으면 기쁘게 여길 것입니다. 하지만 공부보다 더 중요한 것이 있습니다. 우리나라에는 보안, 암호 분야에서 연구하는 많은 사람들이 있습니다. 이런 연구원들은 각지에 퍼져있으며 이들과 만나서 교류하며 정보를 나누는 것은 쉽지 않습니다. 또한 이렇게 배움을 얻는 신입 연구원들은 후에 우리나라의 보안 분야의 중심에 서있을 것입니다. 따라서 이런 자리에서 여러 연구원들을 만나며 교류하고 서로에 대해서 잘 알게 된다면, 추후에 함께 연구할 때 더 높은 시너지를 발휘할 수 있을 것으로 생각됩니다. 다양한 사람이 모인 자리에서 학술적인 얘기를 하면서 제가 몰랐던 부분을 더 알 수도 있습니다. 반대로 제가 아는 분야에 대해서도, 특히 최적 구현과 관련된 부분에서는 큰 도움을 줄 수 있을 것으로 생각합니다. 학술적인 얘기뿐만 아니라 일상적인 대화를 나누면서도 서로의 커뮤니티를 형성하여 타 연구실과의 교류까지 이어질 수 있으며 이를 통해 연구실 간 협업 등을 이끌어낼 수 있는 기회를 얻고자 합니다.

[관심 연구 주제]

저는 암호 알고리즘 최적 구현을 가장 좋아합니다. 특히 그 중에서도 저에게 가장 익숙한 C언어와 연동이 되는 어셈블리어를 사용한 어셈블리 최적 구현을 중점으로 연구 중에 있습니다. 저의 지도교수님이 최적 구현 전공이라는 점도 저의 관심 분야 형성에 영향을 끼쳤습니다. 최적 구현에 있어서 중요한 것은 단 하나의 명령어를 어떻게 사용할지, 어느 장소에 사용할지를 신중하게 고려해야 하며, 레지스터에 어떤 값을 저장할지, 어느 레지스터를 사용할지 하나씩 생각하며 진행해야 합니다. 저는 어셈블리 최적 구현이 마치 퍼즐 맞추기와 비슷하다는 생각이 듭니다. 퍼즐은 정확한 조각을 정확한 위치에 꽂아 넣어야만 하나의 그림을 완성할 수 있습니다. 퍼즐을 맞출 때 모양만 같다고 해서 아무 자리에 꽂아 넣으면 완벽한 그림이 나오지 않습니다. 어셈블리 최적 구현도 이와 비슷합니다. 아무 명령어를 사용한다면 암호 알고리즘을 구현할 수는 있지만 최적화가 완벽하지 않습니다. 반드시 정확한 명령어를 정확한 위치에 사용해야만 비로소 최적화가 완성됩니다. 명령어를 한땀 한땀 입력하면서 결과물을 획득하게 되면 그 기쁨은 이루 말할 수 없습니다. 최적 구현에 발을 들이게 된 계기는 앞선 장에서 설명 드렸던 국가암호 공모전에 도전한 경험 때문입니다. 공모전에 투고한 주제는 최적 구현이었으며 해당 투고가 수상의 경험도 안겨줬습니다. 이 경험은 제가 최적 구현에 관심을 들이고 이 길을 나아가게 할 원동력이 되었습니다.

최적 구현 기법은 매우 중요합니다. 현재 IoT 기기가 발전함에 따라 기기는 점점 소형화 되었고 초미세 기판 제작이 가능해지며 소형 기기의 성능도 향상되었지만, 그 한계는 엄연히 존재합니다. 암호 알고리즘은 연산의 복잡함을 통해 스스로를 방어하는데, 컴퓨팅 파워가 제한적인 소형기기는 정상적인 암호 알고리즘의 가동이 어렵습니다. 이를 위해 다양한 경량 암호가 제안되었고 소형기기 에서도 암호 알고리즘의 가동이 이루어

졌습니다. 하지만 경량 암호를 가동하는 수준에서 벗어나서 기기가 제공하는 파워를 최대한 이끌 수 있도록 최적 구현을 진행한다면 효율적인 암호 알고리즘의 가동을 이끌 수 있습니다. 저는 8-bit AVR 프로세서를 대상으로 최적 구현을 하는데 우선 집중하고 있습니다. 8-bit AVR 프로세서는 다른 프로세서에 비해 상대적으로 구조가 단순하며 제공하는 명령어의 수도 적기 때문에 손쉽게 시작할 수 있었습니다. 현재는 CHAM과 관련한 최적 구현을 집중적으로 연구하고 있으며 국제 학회인 WISA'20에 주 저자로 논문을 내고자 최선을 다하고 있습니다.

[마무리 지으며]

대학원 석사과정을 마치며 제가 가장 많이 느낀 것은 암호 분야에 있어 많은 사람들이 노력하고 있으며 이것이 잘 보이지는 않지만 우리의 생활에 밀접하게 있다는 것을 알 수 있었습니다. 일반 사용자에게 잘 의식되지 않는 이유는, 보안은 평소에 잘 지켜진다면 의식되지 않지만 무너지게 되는 순간 일반 사용자들에게 크게 다가오기 때문입니다. 즉, 사람들의 불만이 없다면 보안 수준이 뛰어나고 잘 지켜지고 있다는 것이며, 저는 전 세계의 암호학자, 보안 연구가들과 국내 연구원들의 노고에 감사와 경의를 표할 수밖에 없었습니다. 저는 보안 분야에 발을 내딛으면서 이 분야에서 연구하는 분들에게, 국가보안연구소 위탁 과제를 하며 함께한 주왕호 연구원님 그리고 안현진 연구원님과 같은 분께 감사함을 느꼈습니다. 그리고 이제는 제가 한명의 연구자가 되어 보안 분야에서 작더라도 누군가에게, 또는 더 많은 사람들에게 안전한 환경을 제공하는 것을 꿈꾸고 있습니다. 평소 저는 교수님에게 있어서 연구 진행은 서투르지만 다른 사람과 타협하고 공동 연구하는 자세가 뛰어나다는 말씀을 많이 들었습니다. 저는 이것이 본 교육에 있어서 크게 도움되리라 생각합니다. 교육을 잘 따라가지 못할 수는 있습니다. 그 내용이 심도 있고 어렵다는 것을 알고 있습니다. 허나 여러 사람들과 만날 수 있는 자리에 참석하여 의견을 나누고, 서로 같이 연구할 수 있는 시작 지점이 될 수 있을 것입니다. 이것은 교육을 이수하는 것을 뛰어넘어 더 큰 기회를 마련하는 자리가 되며, 저에게는 소중한 경험으로 남을 것입니다. 이러한 사유로 저는 본 교육에 지원하며 교육 이수를 희망하는 바입니다.

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

국내 보안 분야는 어느 나라와 견주어도 상당히 세계적인 수준이라고 생각합니다. 다만, 우리의 수준을 다른 나라에 보여주기가 어렵다는 것입니다. 가장 빠르고 쉬운 수단은 국내 기술의 전 세계 표준화라 생각합니다. 국내 기술이 전 세계적인 표준이 된다면 우리의 기술을 전 세계에 널리 알릴 수 있으며 우리의 기술이 사용되고 있다는 자부심도 가질 수 있습니다. 무엇보다 국내 기술이 표준이 된다면 그 사실 자체만으로 큰 이슈가 됩니다. 가령 국산 블록암호 SEED는 그 성능을 인정받아 OpenSSL에 포함되는 쾌거를 이루었습니다. 반면 최신 암호인 LEA, CHAM과 같은 블록암호나 고성능 경량 해시 함수인 LSH 등은 뛰어난 기술력을 자랑하지만, 세계적인 범주에서는 유명하지 않고

아직은 국내에서만 사용되고 있습니다. 이를 뒤집어서 국내에는 뛰어난 암호 기술이 존재한다는 점에 착안하고 고성능의 국산 암호를 세계적으로 배포할 수만 있다면, 국내에서 보안에 관심을 가지는 인원이 늘어날 것이고 이는 더 뛰어난 인재를 발굴할 가능성이 높아짐을 뜻합니다. 훌륭한 인재가 늘어나면 더욱 좋은 연구 진행이 가능하며 이는 마치 양성 피드백과 같이 지속적으로 긍정적인 영향을 가져올 것입니다. 개인적으로 가장 가능성이 높은 분야는 양자내성암호라 생각합니다. 특히나 2020년 4월에는 국가수리과학연구소에서 다변수(multivariate) 이차식 문제 기반의 공개키 암호 알고리즘을 발표하였습니다. 이 암호 알고리즘은 현 공개키 암호 알고리즘과는 달리 소인수분해 및 이산대수 방정식에 기반하지 않기 때문에 쇼어 알고리즘을 피할 수 있습니다. 발표된 알고리즘의 가장 큰 특징은 저성능 프로세서 환경에서도 가동이 유리하기에 나날이 발전해나가는 사물 인터넷(Internet of Things, IoT) 환경에서 강력한 성능을 자랑할 것으로 예상됩니다. 이처럼 국내 연구소 및 보안 관련 기관이 지속적인 연구를 한다면 국산 암호 알고리즘의 특정 기술은 활용될 가능성의 여지가 남아있지 않을까 합니다.

현재 여러 기관의 노력에도 불구하고 국내의 많은 프로그래밍 꿈나무들은 보안 분야가 어렵다는 인식이 다소 있습니다. 하지만 제가 들어와서 느낀 것은 보안 분야가 우리 생활에 가장 밀접히 붙어있다는 점이었습니다. 가까운 것으로 스마트폰에 지문 인식을 하는 것부터 멀게는 웹 사이트가 비밀번호를 관리하는 것 까지, 이 모든 것들이 제 일상에서 머무는 보안이란 것을 깨닫고 흥미롭게 다가왔습니다. 이렇듯 현대 사회에서 보안은 결코 빠질 수 없는 부분이며 보안을 연구한다는 것은 모든 사람들에게 이로운 훌륭한 분야입니다. 이와 같은 인식을 확산시켜 많은 흥미를 이끄는 것이 최우선 과제이며 이를 위한 수단 중 하나가 우리 기술을 세계 표준으로 등록하는 것이라 생각합니다.

또한 연구진간에 교류할 수 있는 중점이 되는 시설이 필요하다고 생각합니다. 국내에는 뛰어난 연구원들이 많이 있으며 각각이 서로가 속한 연구실, 연구소에서 괄목할만한 성과를 내고 있습니다. 하지만 이들을 묶어줄 수 있는 자리가 부족합니다. 학술대회가 이 역할을 어느 정도 맡고 있으나 지속적인 커뮤니티 제공을 해주기에는 어렵다고 생각합니다. 때문에 모두가 언제든지 서로 모일 수 있는 자리가 필요하다 생각합니다. 이러한 시설은 굳이 오프라인에 존재할 필요는 없습니다. 온라인에서 모두가 모일 수 있는 장소만으로도 충분합니다. 학술적인 대화가 이루어지는 것뿐만 아니라 일상적인 교류까지 이루어진다면 서로가 조금 더 가까워질 수 있습니다. 연구원, 연구실간의 화합이 존재한다면 연구에 있어서도 원활한 소통이 쉬워질 것이며 이러한 환경은 더 좋은 연구 결과를 이끌 수 있지 않을까 합니다. 감사합니다.