정 보 보 호 학 회 지
제 30 권 제6호, 2020. 12

NIST 암호 표준화 공모전 동향

김 현 준*, 박 재 훈*, 권 혁 동**, 서 화 정***

요 약

NIST에서는 앞으로 다가올 사물인터넷 환경과 양자 컴퓨터 시대를 대비하기 위해 2019년부터 경량암호 표준화 공모전을 그리고 2017년부터 양자내성암호 표준화 공모전을 각각 진행해 오고 있다. 경량암호 표준화 공모전은 경량 블록암호 운영 모드를 통해 저전력 사물인터넷 환경 상에서 높은 가용성을 만족하는 암호 개발을 그리고 양자내성암호 표준화 공모전은 양자컴퓨터 상에서의 양자알고리즘으로부터 안전한 공개키 암호 개발을 각각 목표로 하고 있다. 본 고에서는 차세대 암호의 표준화에 큰 영향을 미치게 될 NIST 경량암호 그리고 양자내성암호 표준화 공모전 동향을 상세히 확인해 보도록 한다.

Ⅰ. 서 론

사물인터넷과 양자컴퓨터 기술의 급격한 발달은 지금까지 구현이 어려웠던 다양한 서비스들을 가능하게 해주고 있다. 하지만 사물인터넷 장비가 가지는 경량성과 양자컴퓨터를 통한 현존 암호에 대한 분석 가능성은 지금까지 폭넓게 활용되어 왔던 현대 암호 기술을 새로운 암호 체계를 통해 가용성과 안전성 확보하는 방향으로 나아가고 있다. 특히 NIST에서는 앞으로 다가올 미래컴퓨팅 시대를 대비하기 위해 2019년부터 경량암호 표준화 공모전을 그리고 2017년부터 양자내성암호 표준화 공모전을 각각 진행해 오고 있다.

경량암호 표준화 공모전은 경량 블록암호 운영 모드를 통해 저전력 사물인터넷 환경 상에서 높은 가용성을 만족하는 암호 개발을 그리고 양자내성암호 표준화 공모전은 양자컴퓨터 상에서의 양자알고리즘으로부터 안전한 공개키 암호 개발을 각각 목표로 하고 있다. 본 고에서는 경량 암호 표준화 공모전과 양자 내성 암호 표준화 공모전의 진행 상황에 대해 상세히 확인해 본다. 이를 통해 앞으로 다가올 미래 암호 표준안을 확인해 보며 앞으로의 보안 위협과 도전을 사전에 대비해 볼 수 있는 계기를 마련할 것으로 사료된다.

본 고의 구성은 다음과 같다. 2장에서 NIST 경량 암호 공모전의 배경과 진행 상황에 대해 확인한다. 3장에서는 NIST 양자 내성 암호 공모전의 배경과 양자 컴퓨터에 대한 간단한 내용 및 양자 내성 암호의 주요 알고리즘과 실제 공모전 진행 상황에 대해서 살펴본다. 마지막으로 4장에서는 본 고의 결론을 내린다.

Ⅱ. NIST 경량 암호 공모전

2.1. NIST 경량 암호 공모전 제안 배경

자동차 시스템, 센서 네트워크, 의료, 분산 제어 시스템, 사물 인터넷, 사이버 물리 시스템 및 스마트 그리드 등과 같은 산업 분야에 IT 기술이 접목되고 있다. 해당 산업군에서의 IT 기술 접목을 위해 RFID 태그, 산업용 컨트롤러, 센서 노드, 그리고 스마트카드와 같은 저전력 컴퓨터가 활발히 활용되고 있다. 하지만 저전력 컴퓨팅 환경에서는 기존 암호화 표준의 경우 연산 복잡도로 인해 활용이 어려운 문제점을 가지고 있다. 따라서 NIST에서는 임베디드 시스템, RFID 장치 및 센서 네트워크와 같이 고도로 자원이 한정된 장치에 중점을 맞춘 경량 암호의 필요성에 대해 인지하고 경량 암호화 알고리즘의 표준화 공모전을 수행 중에 있다.

저전력 사물인터넷 환경에서 사용되는 마이크로 컨트롤러는 크게 8-비트, 16-비트, 그리고 32-비트 기반으로 나누어 볼 수 있다. 저전력 마이크로 컨트롤러에서

이 성과는 2020년도 정부(과학기술정보통신부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임(No. NRF-2020R1F1A1048478).
* 한성대학교 IT융합공학부 (대학원생, khj930704@gmail.com), (대학원생, p9595jh@gmail.com)
** 한성대학교 정보컴퓨터공학과 (대학원생, korlethean@gmail.com)
*** 한성대학교 IT융합공학부 (조교수, hwajeong84@gmail.com)

기존의 암호화 연산을 수행하기 위해서는 많은 연산량이 요구되기에 연산속도가 느리거나 많은 에너지가 소모될 수 있다. 이는 제한된 에너지를 사용하여 동작해야 하는 경우 현실적인 문제로 다가올 수 있다. 가장 적합한 예시로는 수동형 RFID 태그와 같이 제한된 전력을 사용하는 경우이다. 이와 더불어 수동형 RFID 태그는 작은 칩크기도 함께 요구된다. 이러한 제약사항을 만족하며 높은 보안성을 제공하는 것이 경량 암호 공모전이 추구하는 차세대 미래 암호화 알고리즘이라고 할 수 있다[1].

2.2. NIST 경량 암호 공모전 진행 사항

NIST에서는 경량 암호화 공모전 참여 시 고려해야 할 최종 제출 요구 사항 및 평가 기준을 발표하였다. 경량 암호화 공모전의 제출 단계에는 제출물의 품질을 높이기 위해 초기 검토 단계가 포함되어있다. NIST에서는 제출마감일인 2019년 2월 25일까지 표준화를 위해 전세계의 암호 연구자들로부터 57개의 암호 알고리즘을 제출받았다. 이 중에서 56개의 알고리즘이 2019년 4월에 1차 후보로 채택되어 NIST 경량 암호화 공모전의 1차 라운드를 수행하였다. 1차 후보자의 제출물은 공개 검토를 위해 NIST 경량 암호화 공모전 웹 페이지에 온라인으로 게시되었다.

2.3. NIST 경량 암호 공모전 평가 요구 사항

NIST 경량 암호 공모전에서는 블록 암호, 해시 함수, 그리고 메시지 인증 코드에 대한 제안을 목표로 하고 있다. NIST가 제안된 알고리즘을 평가하기 위한 사항은 아래와 같다[1].

2.3.1. 보안강도

제안하는 알고리즘은 최소 112-bit 이상의 보안강도를 만족해야 한다.

2.3.2. 유연성

다양한 플랫폼 상에서 제안하는 암호 알고리즘은 효율적인 구현이 가능해야 한다. 매개 변수를 사용하여 상태 크기 및 키 크기와 같은 속성을 선택하는 조정 가능한 알고리즘은 보다 적은 자원으로 암호화 연산을 구현하는 것이 가능하다.

2.3.3. 낮은 오버헤드

암호화와 복호화에서 동일한 구조를 지니는 경우 완전히 다른 구조를 가지는 것보다 효율적이다. 해시 함수와 블록암호에서 기본 요소를 공유함으로써 구현에 요구되는 자원을 최적화할 수 있다.

2.3.4. 암호문 크기

암호문의 크기를 크게 늘지 않는 경우 저장 및 전송에 보다 효율적이다.

2.3.5. 부채널 및 오류 주입 공격에 대한 내성

암호 구현은 키 또는 평문 정보가 부채널 공격을 통해 유출될 수 있다. 사물인터넷 장비의 경우 공격자가 해당 장비에 물리적으로 접근할 수 있다. 또한 저전력 마이크로 컨트롤러의 특성상 부채널 공격에 대한 내성을 하드웨어 자체적으로 보장하는 것은 어렵다. 따라서 부채널 및 오류 주입 공격으로부터 안전성을 쉽게 확보할 수 있는 암호 알고리즘이 요구된다.

2.3.6. 평문과 암호문 쌍의 수 제한

암호 알고리즘 설계자는 평문과 암호문 쌍의 수에 대한 최대수를 정할 수 있다. 이 제한은 특정한 응용서비스의 경우 적용된다. 예를 들어 동일한 키로 처리될 수 있는 데이터 양을 제한하는 것이다. 하지만 공격자는 단일 키로 암호화되는 데이터의 양이 제한된 경우에도 관련된 여러 개의 독립적인 키로 암호화된 결과물을 사용하여 공격을 수행할 수 있다.

2.4. NIST 경량 암호 공모전 Round 1

NIST에서는 공개된 과정을 통해 제한된 환경에 적합한 암호화 및 해싱 체계를 선택하는 과정을 거쳤다

1) https://csrc.nist.gov/projects/lightweight-cryptography

[2]. 유망한 후보 알고리즘에 집중하기 위해 1차 프로세스 기간을 12개월에서 4개월로 단축하였으며 2차 후보 알고리즘 32개는 2019년 8월 30일에 발표하였다. 공개적인 분석 결과와 암호의 설계 철학이 2차 후보 선정에 큰 영향을 미쳤다. 아래는 후보군에서 제외된 암호 알고리즘이며 제외 사유는 다음과 같다.

2.4.1. 위조 공격

2.4.1.1. Bleep64

Neves는 두 개의 관련 논스 값이 높은 확률로 동일한 출력으로 이어질 수 있는 초기화 단계의 문제점을 확인하였다[2]. Dobraunig와 Rotella는 이전에 획득 한 유효한 암호문 블록의 서명값에 대한 차분 공격을 수행하였다[3].

2.4.1.2. GAGE, InGAGE

Bagheri은 128-bit 태그와 232-bit 상태가 있는 기본 버전의 경우 나머지 104-bit 최종 출력 상태에 대한 추측을 통해 공격이 가능함을 확인하였다[4].

2.4.1.3. HERN, HERON

Mege는 Hern에 대한 위조 공격을 발견하였다[5]. 해당 공격은 서로 다른 관련 데이터 및 메시지 입력 쌍에 대해 충돌하는 태그 값을 확인한다.

2.4.1.4. Liliput-AE

Dunkelman은 nonce-misuse resistance 모드에서 공격이 가능함을 확인하였다[6][3].

2) https://groups.google.com/a/list.nist.gov/forum/?hl=en#!topic/lwc-forum/O-f-ogbUeTU

3) https://csrc.nist.gov/CSRC/media/Projects/Lightweight-Cryptography/documents/round-1/official-comments/Bleep64-official-comment.pdf

4) https://csrc.nist.gov/CSRC/media/Projects/Lightweight-Cryptography/documents/round-1/official-comments/GAGE-and-InGAGE-official-comment.pdf

5) https://csrc.nist.gov/CSRC/media/Projects/Lightweight-Cryptography/documents/round-1/official-comments/HERN-and-HERON-official-comment.pdf

2.4.1.5. Qameleon

Jha은 마지막 블록의 조정 값이 입력 크기에 의존하지 않고 논스에만 의존한다는 사실을 확인하였다[7].

2.4.1.6. Sycon

Mege는 서로 다른 메시지 및 관련 데이터 쌍에 대해 동일한 태그값이 생성됨을 확인하였다[8].

2.4.2. 길이 확장 공격

2.4.2.1. CiliPadi

Bagheri와 Sadeghi는 CiliPadi가 길이 확장 공격에 취약하다는 것을 확인하였다[9].

2.4.2.2. FlexAEAD

Mege는 FlexAEAD가 길이 확장 공격에 취약하다는 것을 확인하였다[10].

2.4.3. 식별공격

2.4.3.1. Limdolen

Rohit은 위조 공격으로 이어지는 Limdolen의 구조적 약점을 확인하였다[11][4].

6) https://csrc.nist.gov/CSRC/media/Projects/Lightweight-Cryptography/documents/round-1/official-comments/Lilliput-AE-official-comment.pdf

7) https://csrc.nist.gov/CSRC/media/Projects/Lightweight-Cryptography/documents/round-1/official-comments/Qameleon-official-comment.pdf

8) https://csrc.nist.gov/CSRC/media/Projects/lightweight-cryptography/documents/round-1/official-comments/SYCON-official-comment.pdf

9) https://csrc.nist.gov/CSRC/media/Projects/Lightweight-Cryptography/documents/round-1/official-comments/CiliPadi-official-comment.pdf

10) https://csrc.nist.gov/CSRC/media/Projects/Lightweight-Cryptography/documents/round-1/official-comments/HERN-and-HERON-official-comment.pdf

11) https://csrc.nist.gov/CSRC/media/Projects/Lightweight-Cryptography/documents/round-1/official-comments/Limdole

2.4.4. 부적합한 특성

2.4.4.1. LAEM

LAEM은 입력으로 비어있는 일반 텍스트를 지원하지 않는다[12]. 또한 크기가 일반 텍스트의 약 두 배에 달하는 암호문을 생성하는 비효율적인 특성을 가지고 있다.

2.4.4.2. SNEIK

Khairallah는 특정 입력 단어와 출력 단어가 모두 동일한 차이를 가지고 있는 특성을 이용하여 효율적인 위조 공격이 가능함을 확인하였다[5].

2.4.4.3. TRIFLE

S-box 고정 포인트, 키에 대한 접근없이 두 라운드에 걸쳐 상태의 1/4을 해독하는 기능 그리고 긴 단일 활성 비트 트레일의 조합을 결합한 공격이 가능하다[13][14].

2.5. NIST 경량 암호 공모전 Round 2

2019년 8월 30일 NIST는 2차 후보군을 발표하였다. NIST는 2차 후보군에 대한 공개적인 평가를 권장하고 있다. 2차 후보군 제출 팀은 2019년 9월 27일까지 업데이트된 사양 및 결과물을 업데이트하도록 하였다. 2차 공모전의 주요 관점은 안전성 분석, 소프트웨어 및 하드웨어 벤치마킹, 그리고 다양성이다. 2차 후보군 제출자는 다양한 플랫폼 상에서 최적화된 구현 결과물을 제출하도록 권고받았다. 두 번째 평가 및 검토는 약 12개월 동안 진행될 예정이며 총 8개의 후보군이 선정될 예정이다. NIST는 2차 선발이 끝난 이후 최종 선발 과정에서 소수의 후보군에 집중할 계획이다. 최종 라운드는 약 1년간 진행될 예정이다.

n-official-comment.pdf

12) https://csrc.nist.gov/CSRC/media/Projects/Lightweight-Cryptography/documents/round-1/official-comments/LAEM-official-comment.pdf

13) https://csrc.nist.gov/CSRC/media/Projects/Lightweight-Cryptography/documents/round-1/official-comments/TRIFLE-official-comment.pdf

14) https://csrc.nist.gov/CSRC/media/Projects/Lightweight-Cryptography/documents/round-1/official-comments/TRIFLE-official-comment.pdf

Ⅲ. NIST 양자 내성 암호 공모전

3.1. NIST 양자 내성 암호 공모전 제안 배경

현대 컴퓨터 시스템 상의 보안은 공개 키 암호화, 디지털 서명 그리고 키 교환에 크게 의존하고 있다. 하지만 1994년 Peter Shor는 양자 컴퓨터가 공개키 암호화 시스템을 무력화시킬 수 있다는 사실을 발표하였다[6,7]. 만약 대규모 양자 컴퓨터 시스템이 개발될 경우 공개키 암호에 의존하고 있는 IT 시스템들은 해킹의 위험이 있다. 따라서 IT 시스템을 안전하게 보호하기 위해 양자 내성 암호 표준화가 요구되고 있다. 전문가들은 향후 20년 이내에 대규모 양자 컴퓨터 시스템이 구축될 것으로 예측하고 있다. 따라서 양자 컴퓨터의 개발 이전에 안전한 양자 내성 암호의 적용이 필요하다. 이러한 양자 내성 암호 개발을 위해 NIST에서는 양자 내성 암호 공모전을 진행해 오고 있다[15]. 특히 해당 양자 내성 암호는 고전 컴퓨터와 양자 컴퓨터 모두에 있어 안전성을 보장해야 한다.

3.2. 양자 컴퓨터의 발달

대규모 양자 컴퓨터 구축에 대한 타당성 연구는 Shor 알고리즘이 발견된 이후 본격화되어 가고 있다. 양자 컴퓨팅 개발 초기에는 양자 상태를 유지하는 것이 어려웠다. 이는 대규모 양자 계산을 수행하기에는 많은 오류가 누적될 수 있는 문제점이 있기 때문이다. 이러한 상황은 1990년대 후반 양자 오류 정정 코드와 임계값 정리의 개발로 인해 바뀌게 되었다[8]. 해당 발견을 기반으로 오류율이 낮아진 하드웨어들이 점진적으로 개발되고 있는 추세이다. 하지만 여전히 대규모 양자 컴퓨터를 개발하려면 많은 시간과 노력이 필요하다.

최근 연구 결과에서는 다항 시간 안에 2,000-bit RSA를 깰 수 있는 양자 컴퓨터가 약 10억의 예산으로 2030년까지 구축될 수 있다고 주장하고 있다. 이는 현재 NIST가 표준화하여 사용하고 있는 공개키 암호화 시스템에 심각한 위협을 끼칠 것으로 예상된다. 기존 공

15) https://csrc.nist.gov/projects/post-quantum-cryptography

격에 대한 보안성을 강화하기 위해 NIST에서는 112-bit 또는 128-bit 보안을 제공하는 암호 알고리즘으로의 전환을 권장하였다. 하지만 이 또한 양자 컴퓨터에 의해 공격될 수 있기 때문에 양자 내성 암호로의 대전환이 필요하다.

NIST에서는 양자 내성 암호 공모전의 제출물들이 공개 키 암호화, 디지털 서명 및 키 교환 알고리즘을 제공하도록 권고하고 있다. 기존의 암호 공모전과 달리 다양한 문제를 기반하고 있는 양자 내성 암호 후보군들이 선정될 가능성 또한 높게 점쳐지고 있다. 여기서 말하는 다양한 양자 내성 암호의 기반 문제는 아래와 같다.

3.3. 기반 문제에 따른 양자 내성 암호 분류

3.3.1. 격자 기반 암호화

격자 기반 암호화는 완전 동형 암호화 및 속성 기반 암호화와 같은 분야에 활용되고 있다. 격자 기반 키 교환 알고리즘은 연산이 효율적이다. 하지만 알려진 암호 분석 기술에 통해 격자 체계의 보안성을 정확하게 추정하는 것은 어렵다.

3.3.2. 코드 기반 암호화

1978년에 McEliece 암호화 시스템이 처음 제안되었으며 현재까지 높은 안전성을 유지하고 있다. 코드 기반 암호화는 연산이 효율적이지만 키 크기가 크다는 단점을 가지고 있다. 키 크기를 줄이기 위해 코드 기반 암호화에 효율적인 구조가 연구되었지만 대부분의 경우 보안 취약점이 발견되었다.

3.3.3. 다변수 다항식 암호화

유한 필드상에서 다변수 다항식 시스템의 해를 찾는 것이 어려다는 것에 기반한 암호화 알고리즘이다. 지난 수십 년 동안 여러 가지 다변수 다항식 알고리즘이 제안되었다. 하지만 많은 경우 취약점이 발견되었다[9].

3.3.4. 해시 기반 서명

해시 기반 서명은 해시 함수를 사용한 디지털 서명 알고리즘이다. 해시 암호의 보안성에 기반을 하고 있으며 해시에 대한 보안성은 많은 연구가 진행되었다는 장점을 가진다. 하지만 제한된 수의 서명만을 생성할 수 있다는 단점을 가지고 있다.

3.3.5. 아이소지니 기반 암호화

타원 곡선 상의 이산 로그 문제는 양자 컴퓨터에서 Shor의 알고리즘을 통해 효율적으로 해결할 수 있다. 하지만 supersingular elliptic curve의 동형성 문제는 현재까지 알려진 양자 공격이 없다. 이와는 반대로 암호의 역사가 짧은 만큼 보안성에 대한 확신을 가질 만큼 충분한 암호 분석이 이루어지지 않았다.

3.4. NIST 양자 내성 암호 공모전 평가 요구 사항

3.4.1. 보안성

AES 및 SHA-3 암호 공모전과 유사하게 양자 내성 암호를 평가할 때도 가장 중요하게 고려하는 요소가 바로 보안성이다. NIST는 양자 내성 암호 알고리즘의 보안 강도를 명확히 판단할 수 있도록 5개의 보안 범주로 나누어 정의하고 있다.

3.4.2. 비용 및 성능

양자 내성 암호 알고리즘을 평가할 때 연산에 소모되는 비용 또한 중요한 기준이다. 연산 비용에는 계산 효율성과 메모리 요구 사항이 포함된다. 계산 효율성은 암호화 알고리즘의 연산 속도이다. NIST는 양자 내성 암호 후보 알고리즘들이 현재 표준화된 공개키 알고리즘과 비슷하거나 향상된 성능을 도달하기를 바라고 있다. 메모리 요구 사항은 소프트웨어 구현을 위한 코드 크기 및 RAM 요구 사항, 그리고 하드웨어 구현의 경우 칩크기를 의미한다. 모든 양자 내성 암호 후보군 제출자들이 Windows 또는 Linux 상에서 도출된 결과를 포함하여 성능 비교가 가능하도록 권장하고 있다.

3.4.3. 알고리즘 및 구현 특성

뛰어난 확장성을 가진 후보 양자 내성 암호 알고리즘

을 선호한다. 여기에는 다양한 플랫폼에서 효율적으로 실행될 수 있는 암호화 알고리즘과 병렬 처리 또는 명령어 집합 확장을 통해 더 높은 성능을 달성할 수 있는 암호 알고리즘 또한 포함된다. 그 다음으로 공개적인 분석이 용이한 단순한 알고리즘이 선호된다. 마지막으로, NIST는 알고리즘 또는 구현을 포함하는 지적 재산, 이해 당사자에 대한 라이선스의 이용 가능성 및 조건을 포함하여 암호 알고리즘 활용에 제한될 수 있는 모든 요소를 고려한다고 발표하였다.

3.5. NIST 양자 내성 암호 공모전 Round 1

2017년 11월 82개의 후보 알고리즘이 NIST에 제출되었다. 이 중에서 69개의 후보가 최소 승인 기준과 제출 요건을 모두 충족했으며 2017년 12월 20일에 1차 후보로 승인되어 NIST 포스트 양자 암호화 표준화 프로세스의 1차 라운드가 시작되었다. 제출물에는 참조 및 최적화된 C코드 구현, 알려진 답변 검사, 그리고 스펙 및 필수 지적 재산 진술이 포함되었다. 1차 평가 기준은 보안, 비용 및 성능, 알고리즘 및 구현 특성으로써 이를 모두 종합하여 평가하였다.

3.6. NIST 양자 내성 암호 공모전 Round 2

NIST는 69개의 1차 후보군 중에서 26개의 2차 후보군을 선택하였다. 26개의 후보 중 공개키 암호가 17개, 서명이 9개로 구성되어 있으며 기반 문제로는 코드 기반, 격자 기반, 다변수 다항식 기반, 아이소지니 기반, 해시 기반 그리고 영지식 증명 기반이 있다. NIST는 2차 후보군을 선정할 때 후보의 보안성, 구현 비용 및 성능, 알고리즘 및 구현 특성을 고려하였다. NIST는 가장 먼저 보안성을 고려하였으며 그 다음으로 성능을 기준으로 2차 후보를 평가하였다. NIST는 제출 문서와 제1차 NIST 양자 내성 암호 표준화 컨퍼런스의 발표에서 제출자가 제공한 연산 성능 그리고 메모리 사용량을 모두 평가에 고려하였다. 이와 함께 제출된 코드를 기반으로 하여 내부 성능 벤치 마크를 수행하였다. 특정 후보군의 경우 제출된 암호 알고리즘의 독창성을 고려하여 선택하였다. NIST는 일반적으로 간단한 알고리즘 혹은 혁신적인 알고리즘에 대해 긍정적으로 평가하였다.

3.7. NIST 양자 내성 암호 공모전 Round 3

2020년 7월 22일, NIST는 7개의 결선 진출 대상과 8개의 대체 후보 알고리즘을 발표했다. 결선 진출 대상의 경우 3차 양자 내성 암호 공모전을 통해 최종 양자 내성 암호 표준으로 결정될 것이다. 이는 본격적인 실용화 단계에 접어들었음을 알리는 시작점이 될 것으로 보인다. 이와는 달리 대체 후보 알고리즘의 일부는 4라운드에서 결선 진출 대상 후보와는 다른 추가적인 단계를 거쳐 표준화가 될 가능성을 가지고 있다. 따라서 NIST에서는 결과적으로 다양한 암호군들을 양자 내성 암호 결과물로 선정할 가능성이 매우 높다.

Ⅳ. 결 론

본 고에서는 급격히 발전하고 있는 사물인터넷 환경과 양자 컴퓨터 시대에 대비하기 위해 진행 중인 NIST 경량 암호 공모전과 양자 내성 암호 공모전에 대해 확인해 보았다. NIST에서는 다양한 평가 기준과 엄정한 심사를 통해 새로운 암호 표준안을 제정하기 위해 노력하고 있으며 전 세계의 연구자들도 해당 공모전에 적극적으로 참여하며 지속적인 연구와 개발 활동을 진행해 오고 있다. 아직 사물인터넷 환경과 양자 컴퓨터 시대가 완전히 도래하지는 않았다. 하지만 빠른 차세대 암호 표준화 제정과 표준화된 암호 알고리즘 신속한 보급은 급격한 시대 변화에도 IT 시스템의 높은 보안성과 가용성을 만족해 줄 것으로 기대되고 있다. 세계적인 추세에 발맞추어 국내에서도 보다 적극적으로 차세대 암호의 발달에 관심을 가지고 대비함으로써 안전한 IT 환경을 만들어 갈 수 있어야 할 것으로 사료된다.

참 고 문 헌

[1] K. A. McKay, L. Bassham, M. S. Turan, and N. Mouha, “Report on Lightweight Cryptography,” *NIST Interagency Report 8114*, Mar. 2017.

[2] M. S. Turan, K. A. McKay, Ç. Çalık, D. Chang, and L. Bassham, “Status Report on the First Round of the NIST Lightweight Cryptography Standardization Process,” *NIST Interagency Report 8268*, Oct. 2019.

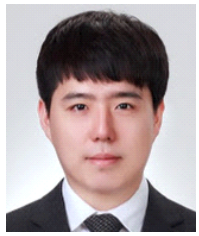
[3] O. Dunkelman, Keller N, Lambooij E, Sasaki Y, “A Practical Forgery Attack on Lilliput-AE,” *Journal of Cryptology*, 33, pp. 910-916, 2020.
[4] R. Rohit, and G. Gong, “Practical Forgery Attacks on Limdolen and HERN,” *IACR Cryptology ePrint Archive*, vol. 2019, pp. 907, 2019.
[5] M. Khairallah, “Forgery Attack on SNEIKEN,” *IACR Cryptology ePrint Archive*, vol. 2019, pp. 408, 2019.
[6] P. W. Shor, “Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer,” *SIAM Journal on Computing*, 26(5), pp. 1484–1509, Oct. 1997.
[7] R. P. Feynman, “Simulating physics with computers,” *International Journal of Theoretical Physics*, 21(6/7), pp. 467-488, June. 1982.
[8] J. Preskill, “Reliable Quantum Computers,” *Proceedings of the Royal Society of London. Series A: Mathematical, Physical and Engineering Sciences*, pp. 385-410, Jan. 1998.
[9] V. Dubois, P. Fouque, A. Shamir and J. Stern, “Practical cryptanalysis of SFLASH,” *Advances in Cryptology. CRYPTO 2007, Lecture Notes in Computer Science*, vol 4622, pp. 1–12, 2007.

〈저자소개〉

김 현 준 (Hyunjun Kim)
학생회원
2019년 2월 : 한성대학교 IT응용시스템공학과 공학 학사
2019년 3월~현재 : 한성대학교 IT융합공학과 석사과정
<관심분야> VR/AR 보안

박 재 훈 (Jaehoon Park)
학생회원
2020년 2월 : 한성대학교 IT응용시스템 공학 학사
202년 3월~현재 : 한성대학교 IT융합공학과 석사과정
<관심분야> 웹 보안, 블록체인

권 혁 동 (Hyeokdong Kwon)
학생회원
2018년 2월 : 한성대학교 정보시스템공학과 공학 학사
2020 2월 : 한성대학교 IT융합공학과 석사
2020년 3월~현재 : 한성대학교 정보컴퓨터공학과 박사과정
<관심분야> 블록체인, 암호구현



서 화 정 (Hwajeong Seo)
종신회원
2010년 2월 : 부산대학교 컴퓨터공학과 학사
2012년 2월 : 부산대학교 컴퓨터공학과 석사
2016년 1월 : 부산대학교 컴퓨터공학과 박사
2016년 1월~2017년 3월 : 싱가포르 과학기술청
2017년 4월~현재 : 한성대학교 IT 융합공학부 조교수
<관심분야> 암호구현