드론 센서를 시드로 활용한 MQ 기반 서명 기법의 변수 생성 방안

조성민*, 홍은기*, 김애영**, 서승현*
*한양대학교 전자공학부
**한양대학교 공학기술연구소
e-mail : smcho3315@hanyang.ac.kr

A Study on the Method of Creating Variables for MQ-based Signature Schemes Using a Drone Sensor as a Seed

Seong-Min Cho*, Eun-Gi Hong*, Ae-Young Kim**, Seung-Hyun Seo*
*Dept of Electronic Engineering, Han-Yang University
**Research Institute of Engineering & Technology, Hanyang University

요 약

IoT 기기 및 드론의 사용자 인증 및 기기 인증을 위해 RSA, ECDSA 등의 여러 전자서명 기법이 기본적으로 사용되고 있다. 그러나 양자 컴퓨터의 개발에 따라 Shor 알고리즘을 이용한 기존 암호 알고리즘의 공격이 가능해지고, 그에 따라 기존 암호 알고리즘의 보안성이 취약해지는 문제가 있다. 따라서 양자 내성 암호를 활용한 보안 체계의 필요성이 대두되고 있는 가운데, 본 논문에서는 양자 내성 암호인 다변수 이차식 기반의 전자서명 기법 중 Rainbow를 드론에 최적화하여 구현하기 위한 방안을 검토 및 분석하고자 한다. 그러나 기존의 Rainbow에서 사용하는 openssl 등의 오픈소스 암호 라이브러리는 PC에 맞춰 설계되었기 때문에 드론에서 난수를 생성할 때 적용이 어려운 점이 있다. 드론에는 각종 센서들이 내장되어 있으며, 센서 데이터들은 난수성을 보장하기에 용이하다. 따라서 드론의 각종 센서들을 시드로 활용하며, XOR 보정기를 통해 난수성을 해치지 않으면서 드론에서 난수를 생성할 수 있는 방안을 제안해 보고자 한다.

1. 서론

최근 무인 항공기(UAV, Unmanned Aerial Vehicle) 시스템인 드론(Drone)이 주목받고 있다. 드론은 현재 취미생활뿐만 아니라 산업의 여러 분야에서도 사용되고 있다. 이러한 드론에도 암호 알고리즘이 사용되고 있는데, 그 중 국제적인 전자 상업 회사인 아마존(Amazon.com)이 선보인 후 화제가 됐던 드론 택배에서는 상품 배달 후 고객을 인증하는 부분에 전자서명을 활용하고 있다[1].

그러나 양자 컴퓨터의 개발과 발전으로 인해 1994년 Peter Shor가 제안한 양자 알고리즘인 Shor 알고리즘을 사용하여 큰 수의 인수분해 문제를 푸는 것이 가능해졌다[2]. 그에 따라 인수분해의 어려움에 기반하는 기존 RSA 등의 암호 알고리즘이 보안에 취약해지면서 새로운 암호 알고리즘의 필요성이 대두되었다. 이에 맞춰 미 국립표준기술연구소(NIST)에서는 2017년 초 양자 내성 암호 알고리즘(PQC, Post Quantum Cryptography) 공개 모집을 진행하였다[2]. NIST 공모는 암호 알고리즘, 전자서명, 키 분배 알고리즘의 세 분야로 나눠 진행됐다. 이에 드론을 비롯한 각종 IoT 기기 또한 양자 컴퓨터 시대에 맞춘 양자 내성 암호 적용의 필요성이 있다. 따라서 본 논문에서는 이 중 다변수 이차식 시스템의 해를 구하는 문제를 활용한 전자서명 기법인 Rainbow를 드론에 적용해 보고자 한다.

Rainbow는 서명 생성 과정에서 랜덤하게 난수를 생성하여 비네가(Vinegar) 변수를 채워 넣어주고 있다. NIST의 PQC 공모전에 제출된 Rainbow의 구현 코드는 openssl 등과 같은 오픈소스 암호 라이브러리를 활용하여 난수를 생성하고 있는데, 이러한 오픈소스 암호 라이브러리는 데스크톱 PC를 위해 만들어진 것들이 많다. 따라서 이러한 오픈소스 암호 라이브러리를 사용하여 드론 및 기타 IoT 기기에서 난수를 생성할 때에는 리소스의 제한 및 엔트로피의 수집이 어려운 문제 등의 이유로 제대로 작동하지

이 논문은 2018년도 정부(과학기술정보통신부)의 재원으로 한국연구재단의 지원을 받아 수행된 기초연구사업임(No. 2018R1A2B6006903)

않는 경우가 많다[3].

따라서 본 논문에서는 드론에서 사용하는 각종 센서로부터 계속해서 변하는 측정값들을 추출하여 시드로 활용하고 XOR 보정기를 통해 난수성을 보장하면서 랜덤하게 비네가 변수를 생성하여 드론에 Rainbow 서명 기법을 적용할 수 있는 방안을 제시해 보고자 한다. 이를 위하여 2장에서는 관련 연구인 다변수 이차식 기반 서명 기법인 Rainbow와 난수 발생기에 대해 간략하게 다루고, 3장에서는 XOR 보정기를 통해 난수성을 보장하며, 드론의 각종 센서로부터 추출한 값을 시드로 활용하여 비네가 변수를 생성하는 방안에 대해 다루도록 한다.

2. 관련 연구

본 장에서는 드론에 적용해 볼 다변수 이차식 기반 서명 기법의 하나인 Rainbow와 난수 발생기에 대해 간략하게 소개한다.

2.1 다변수 이차식 기반 서명 기법

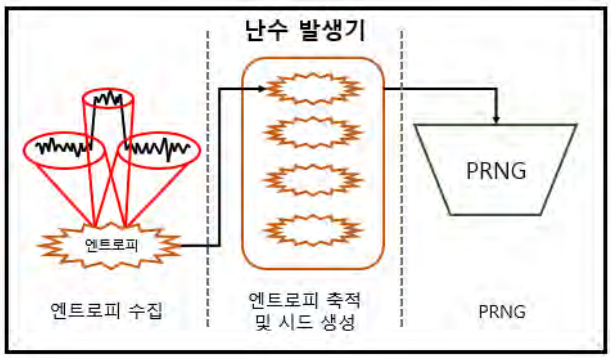
양자 컴퓨터가 개발되면서 그동안 안전하게 사용되던 공개키 암호가 보안에 취약해지고 있다. 이에 NIST에서는 양자 내성 암호 공모전을 진행하였다. 본 논문에서 다룰 양자 내성 암호는 다변수 이차식 기반 전자서명 기법의 하나인 Rainbow이다.

다변수 이차식 기반 서명 기법이란 NP-hard인 다변수 이차식을 푸는 문제에 IP 문제(Isomorphism of Polynomials)와 MinRank 문제를 더한 것을 풀어 그 해를 서명으로 활용하는 전자서명 기법이다.

Rainbow 서명 기법은 2005년 Ding과 Schmidt에 의해 제안되었다. 1997년 Patarin이 발표한 Oil and Vinegar라는 서명 기법의 취약점을 강화한 UOV(Unbalanced Oil and Vinegar)에서 계층을 추가하여 키의 길이와 서명 생성 속도를 개선하였다. 역행렬을 가지는 아핀행렬 S와 T, 중앙행렬 F를 비밀키로 가지며, $P = S \circ F \circ T$를 공개키로 가진다.[4][5]

2.2 난수 발생기

암호 시스템에서 난수 발생기는 매우 중요한 역할을 한다. 암호 시스템에서 난수 발생기의 출력은 대칭키 알고리즘의 비밀키, 공개키 암호 알고리즘의 파라미터, 프로토콜의 논스, 양자키 분배 등에서 중요한 보안 매개변수로 사용된다. 따라서 취약한 난수 발생기의 사용은 암호 시스템의 안전성에 영향을 미치게 된다. 난수 발생기의 구조는 [그림 1]에서 보는 것과 같이 3단계로 구성된다.

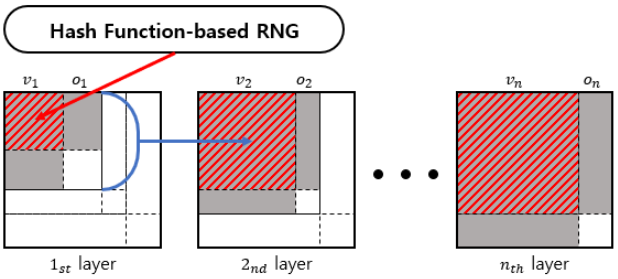


[그림 1] 난수 발생기의 구조

엔트로피 수집 단계는 잡음으로부터 엔트로피를 수집하는 단계이며, 다음 단계에서 엔트로피를 축적하여 그것으로 시드를 생성하게 되고, 의사 난수 생성기(PRNG)를 사용하여 난수를 생성하게 된다.[3]

3. 드론 센서를 활용한 비네가 변수 생성 방안

Rainbow는 키 생성과정과 서명 생성과정에서 난수를 생성하여 사용한다. 키 생성과정에선 아핀행렬을 랜덤하게 채울 때, 그리고 서명 생성과정에선 비네가 변수를 랜덤하게 채울 때 난수를 생성한다. 그러나 스마트폰이나 드론과 같은 기기에서 전자서명을 사용할 경우에 보통 키 생성은 PC에서 생성하여 받아와 사용하는 경우가 많고, 키 생성 과정에서 난수를 생성한 후 아핀행렬의 역행렬 존재 여부를 확인하는 과정이 추가되기 때문에, 본 논문에서는 키 생성은 PC에서 하여 드론에 키가 이식된 상태라고 가정하고, 서명 생성과정에서 비네가 변수를 랜덤하게 채우는 과정만 살펴보도록 한다. [그림 2]는 기존 Rainbow의 비네가 변수 생성 방식이다.

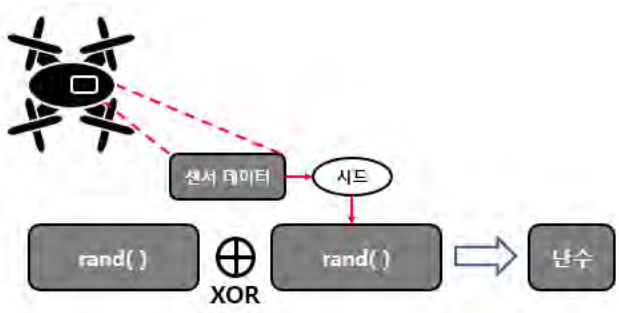


[그림 2] 기존 Rainbow의 비네가 변수 생성 방식

NIST PQC 공모전에 제출된 Rainbow의 구현 코드는 openssl 등의 오픈소스 암호 라이브러리를 사용하여 난수를 생성하고 있다. 이러한 오픈소스 암호 라이브러리를 사용하여 난수를 만들 때는 HAS-160, SHA-224/256/384/512 해시함수에 기반하여 만들며, 엔트로피를 가지는 데이터인 엔트로피 입력은 잡음을 이용하여 생성된다. 잡음의 예로는 시스템 설정 정보 및 네트워크 주소 등의 고정된 시스템 정보, 화면 정보 및 시스템의 시간이나 클럭 등의 가변적 시스템 정보, 키보드 입력 주기 및 마우스 움직임 등의 사용자/외부 주변 장치가 있으며, 고정된 시스템 정보 잡음은 예측이 쉽고, 사용자/외부 주변장치 잡음은 예측이 어렵다는 특징이 있다 [6]. 그러나 이러한 오픈소스 암호 라이브러리는 데스크 톱 PC에 기반하여 만들어졌기 때문에 드론이나 각종 IoT 기기에서 사용이 어려운 경우가 많다 [3].

드론은 정상적인 비행을 위해 자체적으로 각종 센서들을 내장하고 있으며, 프로세서는 센서로부터 데이터를 받아와 처리하여 비행을 하게 된다. 따라서 이러한 센서들로부터 받은 데이터들을 시드로 활용하여 난수를 생성해 비네가 변수를 채울 수 있다. 그러나 이러한 센서값들은 그것의 성질에 따라 각자 고유의 편차를 가지고 있기 때문에, 생성된 난수는 균일한 무작위성을 가지는 분포와 다른 분포를 가지고 있을 수 있다. 따라서 반드시 보정기(corrector)를 사용하여 균일한 무작위성을 가지는 분포를 이루도록 만들어 주어야 한다. 본 논문에서는 이러한 편차들을 없애주고 균일 분포를 만들어 주기 위해서 XOR 보정기를 사용한다. XOR 보정기는 원래의 출력 수열을 쌍으로 묶어 비트별 XOR 연산을 하여 결과를 난수로 사용하는 방식이다.[7]

본 논문에서는 rand와 같은 고정된 시드를 사용하여 난수를 생성하는 함수를 이용하여 1차 난수를 생성한 뒤 드론의 센서로부터 받은 데이터를 시드로 사용하여 생성한 난수와 XOR 연산을 통해 난수성을 강화하는 방안을 사용하고자 한다. [그림 3]은 드론의 센서 데이터를 활용하여 난수를 생성하는 과정을 나타낸다.



[그림 3] 드론의 센서 데이터를 활용한 난수 생성

Algorithm 센서데이터와 XOR 보정기를 활용한 난수 생성기

Input : Sensor Data
Output : Random Number

```
1: for ( i=0; i<v_n; i++ )
2:     RN1 = rand()
3:     srand(SensorData)
4:     RN2 = rand()
5:     RandomNumber = XOR( RN1, RN2 )
6:     vinegar[i] = rand()
```

rand 함수를 이용하여 만든 난수는 난수성이 약하기 때문에 시시각각 변하는 드론의 센서 데이터을 시드로 활용하여 XOR 보정기를 통해 난수를 만들면 난수성을 강화하는 효과를 보게 된다.

4. 결론 및 향후 연구 방향

기존 NIST PQC 공모전에 제출된 Rainbow 서명 기법의 구현 코드는 openssl 등의 오픈소스 라이브러리를 사용하여 난수를 생성한다. 그러나 이는 네트워크 주소 혹은 마우스 움직임 등에서 잡음을 추출하여 난수를 생성하는 등 PC의 데이터를 이용하고 있다. 그에 따라 Rainbow 서명 기법의 구현 코드를 드론에 그대로 적용하기 어려운 점이 있다. 따라서 드론에서 난수를 생성하여 비네가 변수를 채워 넣어줘야 할 필요가 있다. 이에 본 논문에서는 드론의 센서로부터 추출한 값을 시드로 활용하여 난수를 생성하는 방법을 제안하고자 한다. 또한, 그렇게 생성된 난수에 XOR 보정기를 적용하면 난수성 또한 강화될 것으로 예상된다. 향후 연구 계획으로는 드론에서 센서 데이터를 직접 측정하면서 난수성을 테스트해보고, 실제로 생성한 난수로 비네가 변수를 만든 Rainbow 서명 기법을 드론에서 구동한 결과를 확인할 예정이다.

참고문헌

[1] 전자신문, “한국정보인증, ETRI와 ‘드론 택배’ IoT 시뮬레이션 성공”, 2016.01.27.

[2] 박영호 외, “양자컴퓨팅 환경을 고려한 현대암호 안전성 연구”, 한국인터넷진흥원, KISA-WP-2016-0020, 2016

[3] 강하나 외, “센서를 이용한 경량 난수발생기 설계 및 구현”, 한국통신학회논문지 제42권 제2호, pp. 307-315, 2017.2

[4] 박철민 외, “수학적 난제에 기반을 둔 고효율 특수 암호 알고리즘 연구” 국가수리과학연구소, 2015.1

[5] Jintai Ding and Dieter Schmidt,, “Rainbow, a New Multivariate Polynomial Signature Scheme”, ACNS 2005, LNCS 3531, pp. 164-175, Springer, 2005

[6] 한국정보통신기술협회, “결정론적 난수발생기 - 제2부 : 해시함수 기반 난수발생기”, 정보통신단체표준(국문표준)

[7] 강주성, “난수발생기의 현황 및 안전성 분석 기술 동향”, 정보보호학회지 제16권 제4호, pp. 34-46, 2006.8