러시아의 표준 암호 알고리즘에 백도어?

이필중 포항공과대학교 명예교수

1. 머리말

2019년 4월 1일부터 5일까지 이스라엘 텔아비브에서 열린 ISO/IEC JTC 1 SC 27(Information security, cybersecurity and privacy protection)의 WG 2(Cryptography and security mechanisms)에 한국대표 8명을 포함하여 18개국 60명의 대표들이 참석하였다.

2. 주요쟁점사항

암호 알고리즘의 표준화는 다른 기술의 표준화에 비해서 무척 까다롭다. 일단 알고리즘이 안전해야 한다는 것이 가장 중요한 점이다. 그러기 위해서 SC 27/WG 2에서는 자체적인 기준을 마련해 놓고 있다. 그러나 이 기준이 명확하지 않고, 보는 관점에 따라 달라질 수 있기 때문에 문제가 없을 때는 괜찮지만, 문제가 생기면 이 기준에 대한 논의가 되풀이되고는 한다.

암호 알고리즘의 표준화가 진행되다가 중단된 예가 몇 번 있었다. 한국의 SEED와 HIGHT도 포함되어 있는 ISO/IEC 18033-3:2010(암호 알고리즘 - 블록암호, 2nd edition, Editor 저자, Co-editor 독일 Hans von Sommerfeld)의 Amd1으로 추가하려던 러시아의 'GOST 28147-89'는 2011년 1st WD 단계에서 중단되었던 적이 있었고, ISO/IEC 29192-2:2012(경량암호 - 블록암호, 1st edition)의 Amd1으로 진행되던 미국의 Simon과 Speck은 2018년 3rd PDAM 단계에서 중단되었던 적이 있었다.

첫 번째 경우는 보안성도 효율성도 문제점이 명확히 드러나서 과제가 중단되었다. 그러나 두 번째 경우는 ISO/IEC 18031:2011(Random bit generation, 2nd edition)에 미국이 포함시켰던 Dual_EC_DRBG에 백도어가 2013년 발견되었던 것이 문제였다. 많은 (특히 유럽의) 나라들이 미국을 믿지 못하겠다고, Simon과 Speck에 어떤 장난을 했을지 알겠냐고 일단 반대하고 보는 분위기였고, 약간의 보안 약점이 보고되자 바로 중단되었다.

한편 러시아는 Kuznyechik(GOST R 34.12:2015)를 ISO/IEC 18033-3:2010에 Amd1으로 추가하는 과제를 진행했고, DAM_by_ITTF까지 나온 상태에서 중국도 SM4를 같은 표준에 Amd2로 추가하는 과제가 비슷한 일정으로 진행되어, ITTF에서 merged(2nd edition, Amd1, Amd2를

모두 합한) ISO/IEC 18033-3(3rd edition)을 낼 준비를 하는 도중, Kuznyechik와 이미 ISO/IEC 10118-3:2016(전용 해쉬함수, 3rd edition)에 표준화된 Streebog(GOST R34.11:2012)에서 동시에 사용되는 S-box에 규칙성이 있다는 보고가 나왔다.

이에 많은 (특히 유럽의) 나라들이 우려를 표시했다. 러시아는 그 전 S-box에 백도어가 없느냐는 구체적인 질문에 없다고 답을 한 적이 있었기에 그 우려는 더욱 심각했다. 이번 회의에서 러시아는 자신들도 규칙성을 몰랐고, 설사 규칙성이 있다고 하더라도 보안에는 문제가 없다고 했다. 그러나 일단 WG2 Study Period 'New results concerning Streebog and Kuznyechik Sbox'를 만들어 연구해 보기로 했다.

3. 맺음말

우리나라도 국가보안기술연구소에서 개발한 LEA(Lightweight Encryption Algorithm)를 ISO/IEC 29192-2:2012에 Amd2(Editor 국민대 김동찬, Co-editors 한양대 송정환, 국가보안기술연구소 노동영)로 진행 중이다. 앞에서 언급된 바와 같이 미국의 Simon과 Speck을 추가하려던 Amd1이 없어진 상태로, DAM까지 통과되고, ISO/IEC 29192-2(1st edition)과 Amd2를 merge하여 ISO/IEC 29192-2(2nd edition)을 내는 fast track을 진행하기로 하여 FDIS 투표를 준비 중이다. LEA는 안전성과 효율성이 충분히 검증되었고, 표준화 준비도 잘되어 왔기 때문에 문제없이 표준으로 채택되리라 판단된다.

그리고 이번 회의의 다른 결론 중 하나는 암호 알고리즘의 선택 기준을 다시 한 번 살펴보자는 것이었다. 우리나라도 여기에 좋은 의견을 내고, 또한 앞으로 추진하고자 하는 알고리즘 표준화에 이들 기준을 잘 참고하면 좋겠다.