[정보보호] 블록암호알고리즘 국제표준화 현황

ISO/IEC JTC1/SC27 WG2 (Cryptography and Security Mechanisms) 소개

ISO와 IEC가 공동으로 만들어 1987년부터 운영하고 있는 JTC1(Joint Technical Committee 1)은 IT(Information Technology)을 다루고 있고, 같은 시기에 SC20 (Sub-Committee 20 - Data cryptographic techniques)을 만들었으나, 1989년 6월 JTC1 총회에서 보다 넓은 범위의 보안 표준화를 위하여 SC27 (IT security techniques)로 확대 개편을 결정하여 1990년 4월부터 3개의 WG(Working Group)으로 시작하였다가 2006년 5월부터 2개를 더해 현재 5개의 WG를 운영하고 있다. 그 중 ISO/IEC JTC1/SC27 WG2(이하 WG2)는 Cryptography and Security Mechanisms라는 제목으로 원래의 SC20과 거의 같은 목적을 갖고 있다.

ISO/IEC 9979 (Procedures for the registration of cryptographic algorithms)

원래 암호알고리즘은 표준화의 대상에서 제외되었었다. 그래서 WG2에서는 표준화의 대안으로 단지 등록만 하기로 해서 등록 절차에 대한 표준을 1999년 4월 ISO/IEC 9979 (Procedures for the registration of cryptographic algorithms)로 만들었다. 그래서 한동안 영국의 BSI(British Standards Institution)에서 맡아 등록해 오다가, 형편없이 나쁜 암호알고리즘도 등록되는 등, 별로 효과도 없고, 또한 국제적으로 암호알고리즘이 표준화될 필요에 공감하여 ISO/IEC 18033 (Encryption algorithms)을 표준화한 이후에 ISO/IEC 9979는 2005년 6월 철회되었다

ISO/IEC 18033 (Encryption algorithms)

ISO/IEC 18033는 1999년 10월 미국 회의에서 GB의 제안으로 NWI(New Work Item) Proposal을 내서 통과된 과제로 Part 1: General (1sted 2005년 08월, 2nded 2015년 08월), Part 2: Asymmetric ciphers (1sted 2006년 05월, AMD1(Amendment 1) 작업 중), Part 3: Block ciphers (아래에 상세 설명), Part 4: Stream ciphers (1sted 2005년 07월, 2nded 2011년 12월)의 4개의 part로 시작되었다가, 2011년 04월 시작된 Part 5: Identity-based ciphers (1sted 2015년 12월)과 2014년 4월 시작된 Part 6: Homomorphic encryption(아직 WD(working draft)상태)를 추가하였다.

ISO/IEC 18033-3 (Encryption algorithms - Block ciphers) - 1st edition

ISO/IEC 18033-3 (Encryption algorithms - Block ciphers)는 가장 많은 관심을 받은 과제였다. 특히 미국에서 1976년 DES (Data Encryption Standard)를 선택했을 때와 달리 1997년에 시작하여 2000년까지 진행된 AES (Advanced Encryption Standard) 선택 과정은 전 세계를 대상으로 했고, 보다 open된 분위기였기 때문에, WG2에서도 많은 NB(National Body, NB의 이름은 ISO 3166-1-alpha-2 code로 표시)들이 관심을 보이며 자국의 암호알고리즘을 국제표준화 하려고 노력했다. 2000년 3월 CA는 CAST-128을, JP는 CIPHERUNICORN-A, MARS, MISTY1, Hierocrypt, MULTI-S01, Camellia를, KR은 SEED를, NO는 AES를, US는 MARS, RC6, Rijndael(=AES), Serpent, Twofish를 포함시키기를 원하는 NB Contributions 문서 N2530를 냈다. 그 이후 상당히 오랜 기간의 논의를 거쳐 64-bit block cipher로는 TDEA(Triple Data Encryption Algorithm, 일명 3DES), MISTY1, CAST-128이, 128-bit block cipher로는 Rijndael(=AES), Camellia, SEED가 선택되어 2005년 07월에 1sted이 출판되었다. 1998년에 개발된 KR의 SEED를 ISO/IEC 18033-3에 포함시킨 데에는 KISA의 전문가들과 특히 당시 한국 WG2 위원장을 맡고 있던 경동대의 장청룡 교수가 많은 노력을 했다. 그 후 SEED의 표현에 오류가 발견되어, 본인이 Editor가 되어 COR2(Corrigendum 2) 를 2007년 09월에 출판했다.

ISO/IEC 18033-3 (Encryption algorithms - Block ciphers) - 2nd edition

한편 2003년에 국내에서 개발된 ARIA는 AES에 비해 사소한 장점만을 가지고 있었기 때문에, ISO/IEC 18033-3에 포함될 timing을 놓쳤다. 그러나 2005년에 개발된 HIGHT를 국제표준화 시키고 싶었는데, 2006년 5월 JTC1의 요청으로 Low Power Encryption이라는 제목으로 WG2_SP(Study Period)를 시작했다가 2007년 10월 Lightweight cryptography 로 제목을 바꾸고 2009년 5월에서야 NWI Proposal을 내서 통과된 ISO/IEC 20192가 방향을 잡지 못하고 시간을 끄는 동안, 2008년 8월 FR이 PRESENT를 포함시키기 위해 제출한 자료에 HIGHT가 3000 GE(Gate Equivalent)라는 작은 space로 구현했을 때, AES에 비해 약 500배의 Throughput을 보인다는 장점을 부각시켰다. 그래서 KR은 2008년 10월 ISO/IEC 18033-3의 periodic pre-

review에 3건의 COR도 있으니, HIGHT를 포함시켜 revision을 내자고 주장했고, 통과되어 본인 editor가 되어 단 1번씩의, WD, CD (Committee Draft), FCD (Final CD), FDIS(Final Draft International Standard)를 거쳐 2010년 12월에 2nded이 출판되었다. 한편 2009년 5월 RU가 “GOST R 34.11-2012”를 ISO/IEC 18033-3의 AMD1으로 넣자고 주장하여 일단 그렇게 하기로 결정되었다가 NB들의 심한 반대에 1STWD까지만 내 놓고 NB Letter Ballot을 거쳐 AMD를 중지하고 추후 다시 논의하자고 결정되었다.

Russia의 Kuznyechik 추가 요청

그런데 ISO/IEC 18033-3의 2nded에 대한 2016년 초의 systematic review에 RU는 2013년에 발표되어 2015년에 RU의 국내 표준 “GOST R 34.12-2015”이 된 KUZNYECHIK를 ISO/IEC 18033-3에 AMD하자고 주장했다. 회의 도중 미리 배포되지는 않은 TP를 보여주며 128-bit block, 256-bit key (key schedule 32 round Feistel), 8-bit S-box same as GOST R 34.11-2012, XSL-cipher, MDS linear mapping by LFSR, 9.5 rounds, security margin > 30%, ~336 MB/s (9.8 cpb) on Intel (R) Core (TM) i5-6500 CPU A@ 3.2 GHz 의 implementation result가 있다고 했고, Known Cryptanalyses로는 IEICE Trans에 발표된 5 round에 대한 Meet in the Middle Attack과 CTCrypt 2015에 Fault analysis에 대한 논문과, 같은 곳에 발표된 간접적으로 관련된 논문, 도합 3개만을 보였다. CTCryptology(Current Trends in Cryptology)라는 annual conference는 2012년에 시작한, paper는 영어로 쓰고, official language는 영어와 러시아어인, 준 국제 conference이다. 2014년까지는 PC chair는 물론 PC members도 전원 RU인이었고, 2015년에는 13명 중 외국인 PC member를 2명, 2016년에는 19명 중 4명으로 조금은 더 국제화를 해 나가는 듯. (http://tc26.ru/CTCrypt/2015/) 워낙 미리 얻을 수 없었던 정보였기에 좌중에서 나온 질문은 특별한 것은 없었고, WG2_SP "Inclusion of the block cipher Kuznyechik in ISO/IEC 18033-3"를 establish하고, Call for Contribution을 내는 것을 결정하고 회의를 마쳤다.

결론 – 한국의 LEA 추가의 반면교사로

본인의 견해로는 Kuznyechik라는 Cipher 자체에 대한 정보도 충분하지 않고, 분석 논문도

충분하지 않고, WG2에서는 RU의 국내표준을 국제표준화 하는 데에 별로 호의적이지 않았던 전례가 있던 바, Kuznyechik이 ISO/IEC 18033-3에 추가될 가능성은 별로 없다고 생각된다. 한국에서 LEA를 ISO/IEC 29192-2(Lightweight cryptography - Block Cipher)에 추가시키고 싶어하는데 Kuznyechik의 경우를 좋은 반면교사로 삼을 수 있을 것 같다.

이필중 (포항공대 전자과 교수, pjl@postech.ac.kr)