通信情報保護學會誌
第 11 券 第 1 號, 2001. 2

ISO/IEC JTC1/SC27(정보보안기술)WG2 21th Meeting 참가보고

이 필 중*

요 약

SC27의 WG2 는 보안기술 그 자체에 대한 표준을 만드는 Working Group 이다. SC27 소개는 한국통신정보보호학회지 제 3 권 제 2 호 (1993년 6 월) 29~34 쪽을 보기를 바란다. 2000. 10. 17(화)~20(금) 일본 동경 미나토구 시바코겐 기계진흥회관에서 개최된 21차 회의에 다녀와서 그 얻은 정보를 나누고자 과제별로 진행사항과 회의결과 및 회의 중 특기할 사항들을 정리하였다.

Ⅰ. 서 론

본인은 1992년 10월 미국 Geitersburg 에서 열린 SC27 회의부터 거의 빠짐없이 WG2 회의에 참석해 오고 있다. 국제표준화회의에 참여하는 목적은 한국의 입장을 국제표준에 반영시켜 국익에 도움을 주고자 하는 것이 주된 목적이고, 다른 부수적인 목적은 최신의 기술동향을 파악하는 것이다.

이번 회의에 참가한 한국인 참석자는 WG2에 본인 이외에 (존칭생략) 장청룡(경동대), 박경환(KISA), 강경희(KT), 보안관리/정책 쪽을 담당하는 WG1 에는 이경석(산업연구원), 김정덕(중앙대), 차재현(기술표준원), 보안평가 분야를 담당하는 WG3에는 이완석(KISA), 김석우(순신대) 이었고, 한국에서 열렸던 95년 11월 회의를 제외한 과거 어느 회의보다 한국인이 많이 참석한 회의였다.

회의는 WG2 Convener 인 M. DeSoete(벨기에)가 불참하고 위임받은 M. Ward(벨기에)가 10월 2일 개정된 문서번호 N2672r "Meeting Agenda for 21th SC27/ WG2 meeting in Tokyo"(8쪽)에 따라 진행했고, 회의의 결의사항들은 10월 20일에 작성된 N2720 "Resolutions of 21th meeting of SC27/ WG2, Oct. 2000"에 정리되었다.

본문에서 자주 쓰일 약어에 대한 풀이를 Ⅱ절에서 하고, Ⅲ절에 과제별로 진행사항을 정리하였다. 과제번호가 사이사이 빠진 것은 다른 WG의 과제이거나 없어진 과제일 경우도 있고, 과제 18의 세부과제가 18.02부터 시작하는 것은 18.01은 WG1이 담당하고 있기 때문이다. [Rn]이라고 쓴 것은 N2720의 Resolution 번호 n에 나와있는 내용이라는 표시이다. 마지막으로 Ⅳ절에 소감을 중심으로 결론을 내었다.

Ⅱ. 약어 풀이

과제(project) 이름에 대한 약어는 과제별 진행사항의 (과제)번호 밑에 나와있고, 다른 약어는 아래에 풀이한다.

CD	Committee Draft
CfG	Call for (National Body) Comments
DIS	Draft International Standard
DoC	Disposition of(National Body) Comments
FCD	Final Committee Draft
FDIS	Final Draft International Standard
IS	International Standard
NB	National Body
NWI	New Work Item
SoC	Summary of (National Body) Comments

* 포항공과대학교 전자전기공학과 (pjl@postech.ac.kr)

SoV Summary of Voting
WD Working Draft

Ⅲ. 과제별 진행사항

번호 과제명/
약어 〈관련문서번호 쪽수 제목 날짜〉
논의사항 및 보고.

01 Modes of operation for a 64-bit block cipher algorithm

Mo64

〈2732 2 Recommendations on review of 8732, 9798-1, 13888-1~3 00.10.20〉

〈2728 2 Recommendations on review of 8732, 10116 00.10.20〉

〈2531 50 SoC on review of 8372, 10116, 9798-1, 13888-1~3(N2489) ??〉

IS 8372(1987, 2nd confirm 1997)가 재심을 받았는데, 중국과 독일이 confirmation 하기를, 미국이 revision을 카나다가 withdrawal을 원했음. 토의결과 IS 8372을 IS 10116에 합치기로 하고 SC27 비서가 그 가능성을 invest 하기로 [R4]. N2728 과 N2732로 재심추천을 하기로 [R16a].

02 Modes of operation for an n-bit block cipher algorithm

MoN

〈2728 2 Recommendations on review of 8732, 10116 00.10.20〉

〈2531 50 SoC on review of 8372, 10116, 9798-1, 13888-1~3 (N2489) ??〉

IS 10116(1997-2nd ed)가 재심을 받았는데, 중국과 카나다가 confirmation하기를, 독일과 미국이 revision을 원했음. 토의 결과 IS 10116을 수정하되 기존의 modes이외에 독일이 제안한 Statistical self-synchronization mode도 포함시키는 것을 주로 해서 N2728로 재심추천을 하기로 [R16b]. O. Jung(독일)을 Editor로 지명하고 [R19a], Editor는 IS 10116을 11월 30일까지 update하여 [R1b] 만든 새 문서 N2711에 대한 NB의 comments를 01.02.28까지 받기로 [R8a]. 다음 WG모임에서 충분한 지지가 있으면 N2711의 수정 version을 1st CD로 progress시키기로 [R13d].

03.01 Entity authentication Part 1 : General model

EA1

〈2732 2 Recommendations on review of 8732, 9798-1, 13888-1~3 00.10.20〉

〈2531 50 SoC on review of 8372, 10116, 9798-1, 13888-1~3 (N2489) ??〉

IS 9798-1(1997-2nd ed) 가 재심을 받은 결과가 N2531에 있었음. 독일, 미국, 중국, 카나다가 confirmation하기 원했고 revision이나 withdrawal을 원한 나라는 없었음. 따라서 N2732로 그냥 confirmation하는 것으로 재심추천을 하기로 [R16c].

03.02 Entity authentication Part 2 : Mechanisms using symmetric encipherment algorithm.

EA2 IS 9798-2(1999-2nd ed) : 2002 재심예정. 이번 회의에서 논의 안됨.

03.03 Entity authentication Part 3 : Mechanisms using digital signature techniques.

EA3 IS 9798-3(1998-2nd ed) : 내년 정기 review가 되었으므로 각 NB는 2001.02.28이전에 contribution하도록 CfC을 보내기로. [R18a]

03.04 Entity authentication Part 4 : Mechanisms using a cryptographic check function

EA4 IS 9798-4(2000-2nd ed.) : 2003 재심예정. 이번 회의에서 논의 안됨.

03.05 Entity authentication Part 5 : Mechanisms using zero knowledge techniques

EA5 IS 9798-5(1999) : 2002 재심예정. 이번 회의에서 논의 안됨.

04.01 Message authentication codes Part 1 : Mechanisms using a block cipher

Mac1 IS 9797-1(2000-3rd ed) : 2003 재심예정. 이번 회의에서 논의 안됨.

04.02 Message authentication codes Part 2 : Mechanisms using a hash-function

Mac2 〈2651 17 FCD 9797-2 00.09.14〉
이번 회의에서 논의 안됨. N2651이 FDIS로 준비되었고 ballot하기로 〔R12a〕

06.01 Non-repudiation Part 1 : General

NR1

〈2732 2 Recommendations on review of 8732, 9798-1, 13888-1~3 00.10.20〉

〈2531 50 SoC on review of 8372, 10116, 9798-1, 13888-1~3 (N2489) ??〉

IS 13888-1(1997)가 재심을 받은 결과가 N2531에 있었음. Withdrawal을 원한 NB는 없었고, 중국과 미국, 카나다가 confirmation을, 독일이 revision을 원했으나 독일의 의견은 minor editorial change 뿐이었음. 따라서 N2732로 그냥 confirmation하는 것으로 재심추천을 하기로 〔R16d〕.

06.02 Non-repudiation Part 2 : Mechanisms using symmetric techniques

NR2

〈2732 2 Recommendations on review of 8732, 9798-1, 13888-1~3 00.10.20〉

〈2531 50 SoC on review of 8372, 10116, 9798-1, 13888-1~3 (N2489) ??〉

IS 13888-2(1997)가 재심을 받은 결과가 N2531에 있었음. Withdrawal을 원한 NB는 없었고, 중국, 미국, 카나다, 독일이 confirmation을 원했음. 따라서 N2732로 그냥 confirmation하는 것으로 재심추천을 하기로 〔R16e〕.

06.03 Non-repudiation Part 3 : Mechanisms using asymmetric techniques

NR3

〈2732 2 Recommendations on review of 8732, 9798-1, 13888-1~3 00.10.20〉

〈2531 50 SoC on review of 8372, 10116, 9798-1, 13888-1~3 (N2489) ??〉

IS 13888-3(1997)가 재심을 받은 결과가 N2531에 있었음. Withdrawal을 원한 NB는 없었고, 중국, 미국, 카나다, 독일이 confirmation을 원했으므로 그냥 reconfirmation하기로, N2732로 재심추천을 하기로 〔R16f〕.

07.01 Digital signature schemes giving message recovery Part 1 : Mechanisms using redundancy

DSM1

〈2636 2 Withdrawal of ISO/IEC 9796(1991) 00.07.27〉

Crypto'99에 제출된 가짜서명을 만드는 공격을 시작으로 여러 건의 공격이 있어서 이 표준은 삭제하도록 한 권고에 대해 approval이 N2636으로 났고 이번 회의에서는 논의되지 않았음.

07.02 Digital signature schemes giving message recovery Part 2 : Integer factorization based methods

DSM2 〈2703 28 CD 9796-2, Integer factorization based mechanisms 00.10.19〉

〈2702 7 DoC on 1st WD 9796-2 (2633) 00.10.19〉

〈2702s 3 Agenda of meeting for 9796-2 (2669) 00.10.17〉

〈2702t 2 US C on IS 9796-2 (Kaliski) 00.10.19〉

〈2669a 13 SoC on WD 9796-2 (N2633) 00.10.13〉

〈2633 29 Text for 1st WD 9796-2 (revision) 00.07.16〉

재심 중인 IS 9796-2를 Editor Mitchell(영국)의 주도로 화요일 오후와 수요일 오전에 걸쳐 회의를 했음. WD인 N2633에 대한 의견을 벨기에, 프랑스, 독일, 한국, 폴란드, Ukraine, 미국이 내었음. 의견 하나 하나에 대한 논의가 있었고, 한국의 의견을 포함 대부분이 받아들여져 N2702로 DoC를 내었음. 중요한 변화는 Title을 보다 적절하게 위와 같이 바꾸도록 〔R10〕 결정하였음. Editor는 N2633을 11월 30일까지 update하도록 하라는 resolution 〔R1a〕이 나왔으나 현장에서 벌써 N2703이 나왔고, 이것을 1st CD로서 Ballot할 것〔R11a〕을 결정. 그리고 다음 WG모임에서 충분한 지지가 있으면 N2703의 수정 version을 FCD로 progress시키기로 〔R14a〕.

07.03 Digital signature schemes giving

message recovery Part 4 : Discrete logarithm based mechanisms

DSM3 IS 9796-4 : 2003 재심예정. 이번 회의에서 논의 안됨

08.01 Digital signature with appendix -Part 1: General

DSA1 IS 14888-1 : 2003 재심예정. 이번 회의에서 논의 안됨.

08.02 Digital signature with appendix -Part 2: Identity-based mechanisms

DSA2 IS 14888-2 : 2003 재심예정. 이번 회의에서 논의 안됨

08.03 Digital signature with appendix -Part 3: Certificate-based mechanisms

DSA3 〈2659 3 Japanese comments on IS 14888-3 ??〉

현재의 표준문서에 급히 고쳐야 할 사소한 technical mistake 가 보고되어 수요일 오전에 간단히 논의하였음. A. Fujioka(일본)를 acting editor로 [R5a] 하여 N2705로 Draft Technical Corrigendum을 만들어 ballot 하기로 [R17]

09.01 Hash-functions Part 1: General

HF1 IS 10118-1: 2003 재심예정. 이번 회의에서 논의 안됨

09.02 Hash-functions Part2 : Hash-functions using an n-bit block cipher algorithm

HF2 IS 10118-2 출판을 기다리는 중. 이번 회의에서는 논의 안됨

09.03 Hash-functions Part 3 : Dedicated hash-functions

HF3 IS 10118-3 : 2001년 정기 review가 되었으므로 각 NB는 2001.02.28이전에 contribution 하도록 CfC을 보내기로 [R18a]. SHA-256, SHA-512등도 거론됨.

09.04 Hash-functions Part 4 : Hash-functions using modular arithmetic

HF4 IS 10118-4 : 2002 재심예정. 이번 회의에서는 논의 안됨.

18.02 Key management Part 2 : Mechanisms using symmetric cryptographic techniques

KM2 IS 11770-2 : 2002 재심예정. 이번 회의에서는 논의 안됨.

18.03 Key management Part 3 : Mechanisms using asymmetric techniques

KM3 IS 11770-3 : 2002 재심예정. 이번 회의에서는 논의 안됨.

23 Data processing Check character systems

CCS 〈2569 15 FCD of ISO/IEC 7064 ballot due 01.01.28〉

FCD ballot을 기다리는 중. 이번 회의에서는 논의 안됨.

26.01 Cryptographic techniques based on elliptic curves Part 1 : General

EC1 〈2657 2 US Comments on FCD 15946-1〉

〈2553 34 FDIS 15946-1 00.05.18〉

화요일 오전 Editor Weissmann(독일)의 주재로 회의를 하였음. FDIS ballot 문서에 미국만이 정식으로 comment를 내었고 이 editorial comments가 간단히 논의되었음. 한국도 미리 보내지는 못했지만 그 자리에서 준비해 갔던 comments를 즉시 주었고 다 받아들여졌음. 단 한가지 technical 한 결정은 GF(2^m)의 경우 m을 prime인 경우로 한정하기로. Editor는 N2553을 11월 30일까지 update하여 [R1c] N2713을 만들고 FDIS로 ballot하기로 [R12a].

26.02 Cryptographic techniques based on elliptic curves Part 2 : Digital Signatures

EC2 〈2443 37 FCD 00.04.04〉

회의에 참석하지도 않은 Editor R. Horne(영국)이 준비하기로 했던 FDIS N2555를 patent문제가 해결되지 않았다는 이유로 만들지 않아서 회의가 진행될 수 없었음. Editor는 N2443을 11월 30일까지 update하도록 [R1d] 결의하였고, 다음

WG모임에서 충분한 지지가 있으면 N2443의 수정 version인 N2555를 FDIS로 progress시키기로 [R15].

26.03 Cryptographic techniques based on elliptic curves Part 3 : Key establishment

EC3 〈2660a 10 SoV on FCD 15946-3, Key establishment 00.10.13〉

〈2557 34 FCD 15946-3 Key establishment ballot due 00.10.06〉

〈2556 4 DoC on 2nd CD 15946-3, 00.05.18〉

화요일 오후 Acting Editor Weissmann(독일)의 주재로 FCD ballot 문서 N2557에 한국을 비롯한 7개의 NB가 Approve with comments, 11개의 NB가 Approve, 3개의 NB가 Abstain한 N2660a을 가지고 회의를 하였음. 대부분 editorial comments였고 한국의 것도 그랬는데 3개중 2개는 comment의 내용을 이해하지 못해서 reject가 되었음. D. Johnson(미국)을 Editor로 지명하기로 [R19b] 하였고, 새 Editor는 N2557을 11월 30일까지 update [R1e] 하여 N2708을 만들어 FDIS로 ballot하기로 [R12b].

26.04 Cryptographic techniques based on elliptic curves Part4 : Digital Signatures with Message Recovery

EC4

〈 2710 29 1st CD 15946-4 00.10.18〉

〈2709 4 DoC on 1st CD 15946-4 00.10.18〉

〈2664 12 SoC on 1st WD 15946-4 00.10.06〉

〈2592 28 1st WD15946-4, DS & Revision 00.09.20〉

화요일 오후인 EC3에 이어서 미숙한 Editor A Miyaki(일본)을 대신해서 EC1 Editor 인 Weissman 의 주재로 1st WD N2592에 한국을 비롯한 8개의 NB 가 comments 한 N2664를 가지고 회의를 하였음. 대부분 comments 받아들여졌으나 한국의 것 중에는 표준 전체에 대한 이해가 없이한 comment 도 있어서 그 자리에 있던 한국대표가 무색해지는 내용도 있었음. Editor 는 N2592를 11월 30일 까지 update [R1f]하여 N2710을 만들어 1st CD로 ballot 하기로 [R111b]. SC27 비서는 CfC를 NB에게 보내 2001.02.08까지 input을 요청키로.[R9c]. 다음 WG 모임에서 충분한 지지가 있으면 N2710의 수정 version을 FCD로 progress 시키기로 [R14c]

27.01 Time Stamping Services Part 1 : Framework

TSS1

〈2715 12 Text of 1st CD 18014-1 00.10.19〉

〈2714 3 DoC on WD 18014-1 (2595) 00.10.19〉

〈2661b 16 SoC on 1st WD 18014-1 00.10.17〉

〈2595 11 WD 18014-1 00.05.30〉

수요일 오전 Editor R. Müller(독일)의 주재로 WD N2595에 한국을 비롯한 6개의 NB가 comments 한 N2661r2를 가지고 회의를 하였음. Comments 중 reject 된 것보다는 accept된 것이 많았음. 한국의 안은 PKI에서나 그 밖의 많은 보안서비스에서 local clock이 정확하지 않으면 사용자가 만드는 timestamp가 받아들여지지 않을 수도 있고, 또 정확하게 만든 timestamp도 local에서 받아들여지지 않을 수도 있으므로, local clock을 정확히 setting하는 trusted timing service를 포함시키자는 것이었음. 많은 사람들이 그러한 서비스의 필요성은 인정했지만 TSS라는 scope에는 맞지 않는다고 reject하였음. 이 서비스는 NWI으로도 필요하다는 의견도 있었지만 IETF등 다른 표준에서 어떻게 진행되고 있는지도 모르고, 구체적인 NWI proposal이 나온 다음 다시 논의하자는 것으로 하고 resolution에도 포함시키지 않고 이야기를 끝냈음. Editor는 N2595을 11월 30일까지 update [R1g] 하여 N2715을 만들어 1st CD로 ballot하기로 [R11e]. 다음 WG모임에서 충분한 지지가 있으면 N2715의 수정 version을 FCD로 progress 시키기로 [R14b].

27.02 Time Stamping Services Part 2 : Mechanisms producing independent tokens (N2357)

TSS2 〈2662 11 SoC on 1st WD 18014-2 00.10.06〉

〈2596 7 WD 18014-2 00.05.31〉

수요일 오후까지 Editor인 J. Manas(스페인)가 도착하지 않아 R. Muller(독일)를 acting

editor로 [R5b] 하여 WD N2596에 미국을 비롯한 4개의 NB가 comments 한 N2662를 가지고 회의를 하였으나 다른 회의를 참여하느냐고 불참하였음. Editor는 N2596을 11월 30일까지 update [R1h]하여 새 WD N2717을 만들고 이에 대한 NB의 comments를 01.02.28까지 받기로.[R8g] 다음 WG모임에서 충분한 지지가 있으면 N2717의 수정 version을 1st CD로 progress시키기로 [R13b].

27.03 Time Stamping Services Part 3 : Mechanisms producing linked tokens (N2357)

TSS2 〈2663 7 SoC on 1st WD 18014-3 00.10.06〉

〈2597 11 WD 18014-3 00.05.31〉

수요일 오후 Editor인 W. Doonan(미국)의 주재로 WD N2597에 프랑스를 비롯한 4개의 NB가 comments 한 N2663를 가지고 회의를 하였으나 다른 회의를 참여하느냐고 불참하였음. Editor는 N2597을 11월 30일까지 update [R1i]하여 새 WD N2719을 만들고 이에 대한 NB의 comments를 01.02.28까지 받기로.[R8h] 다음 WG 모임에서 충분한 지지가 있으면 N2719의 수정 version을 1st CD로 progress시키기로 [R13c].

31 Random number generation

RNG 〈2658 2 German comments on 1st WD 18031 00.??.??〉

〈2559 20 2nd WD 18031 00.10.04〉

Editor인 Chawrun(카나다)가 주관하여 1st WD이었던 N2458에 대한 독일의 comment와 새로 나와서 충분히 검토될 기회가 없었던 2nd WD N2559를 가지고 목요일 오후에 회의를 하였으나 참석하지 못했음. 제목도 Random bit generation으로 변경하는 것을 고려 중. Editor는 N2559을 11월 30일까지 update [R1j]하여 3rd WD N2727을 만들고 그것에 대한 NB의 comments를 01.02.28까지 받기로[R8f]. 또한 SC27 비서는 CfC를 NB에게 보내 2001.02.28까지 input을 요청키로. [R9c]. 다음 WG모임에서 충분한 지지가 있으면 N2727의 수정 version을 1st CD로 progress시키기로 [R13a].

32 Prime number generation

PNG 〈2671 27 Swedish contribution An efficient PRG with provable security ??〉

Editor도 정해지지 않았고, 따라서 1st WD N2561도 만들어지지 않은 상태에서 스웨덴이 제안한 N2671을 참고로 RNG의 Editor인 Chawrun의 주관으로 목요일 오후에 회의를 하였으나 참석하지 못했음. T. Tederson을 Editor로 지명하기로 [R19c] 하였고, 새 Editor는 01.01.30까지 새로운 WD N2646을 만들어 SC27비서에게 보내기 [R6e] 이 WD에 대한 NB의 comments를 01.02.28까지 받기로 [R8i].

33.01 Encryption algorithms Part 1 : General

Enc1 〈2656 802 NB contributions on NP 18033 in response to N256300.10.10〉

〈2730 1 Report of meeting on NP 18033-1 00.10.19〉

N2563에 응답해서 NB들이 응모한 algorithms가 있는 N2656r2는 무려 802쪽이나 되는 것이었음. 그러나 구체적으로 이 part에 관한 것은 없었음. Editor로 지명된 [R19d] C. Mitchell(영국)이 주도하여 수요일 오후에 회의를 진행하였고, 현장에서 Mitchell이 작성한 Preliminary outline (문서 번호 없음)을 돌려 간단히 의논하였고, 합의된 주요 사항은 meeting report N2730에 정리되어 있음. Editor는 01.01.30까지 1st WD N2723를 만들어 SC27비서에게 보내고 [R6a] 이것에 대한 NB의 comments를 01.02.28까지 받기로 [R8b].

33.02 Encryption algorithms Part 2 : Asymmetric ciphers

Enc2 〈2656 802 NB contributions on NP 18033 in response to N2563 00.10.10〉

N2656r2에 Enc2에 관한 것은 일본의 PSEC, EPOC(NTT), HIME-1 & -2 (HITACHI), 미국의 ECIES, RSA-OAEP, 독일의 ACE, 스웨덴의 RSA-OAEP이었음. Editor로 지명된 [R19e] V. Shoup(독일)의 주관으로 수요일 오후에 회의를 했음. 제안 알고리즘의 기본적 안전성의 이론 근거 (Random Oracle, Complementary Diffie-Hellman, ElGamal, PDH, Elliptic Curve, 소

인수분해 등)에 의한 분류에 의한 모델링을하고 제안 알고리즘들 중 유사한 것은 그룹별로 통일시키기로 하여 정리하되 우선 (1) RSA-OAEP와 (2) EC-ElGamal의 변형인 ACE 및 PSEC(가능하면 ECIES도)를 통합한 하나의 일반형을 다음 WD에 포함시키고 다른 것들은 차차 고려하기로. 제안 알고리즘의 선정은 제3의 객관화될 수 있는 기관 또는 전문가들에 평가(NESSIE, Cryptrec, 등)한 결과를 우선적으로 고려하기로. 또 다른 고려 사항은 특장점(키 설정), 메시지 길이(고정, 임의), 적용 분야, 실용성, 효율성, 보급 등을 포함하기로. Editor는 1st WD N2724를 만들어 01.01.30까지 SC27 비서에게 보내고 [R6b], 이것에 대한 NB의 comments는 01.02.28까지 받기로 [R8c].

33.03 Encryption algorithms Part 3 : Block ciphers

Enc3 〈2656 802 NB contributions on NP 18033 in response to N2563 00.10.10〉

N2656r2에 Enc3에 관한 것은 일본의 CHIPERUNICORN-A, MISTY1, Hierocrypt-3 / -L1, Camellia, MARS, 한국의 SEED, ZODIAC, XENON, 캐나다의 CAST5, 스웨덴의 RC6, 스위스의 IDEA, 미국의 MARS, RC6, Rijndael, Serpent, Twofish 등이었음. Acting editor를 하기로 했던 J. Foti(미국)이 참석하지 않아 Enc1의 Editor가 Acting editor가 되어 회의를 진행하였음. Enc2와 같이 제안 알고리즘의 선정은 제 3의 객관화될 수 있는 기관 또는 전문가들에 평가(AES, NESSIE, Cryptrec, 등)한 결과를 우선적으로 고려하기로. 우선 다음 WD는 AES에서 선정된 Rijndeal과 현장에서 추천된 3DES (FIPS 46) 만을 넣어서 만들고 다른 알고리즘들의 포함은 추후 고려하기로. 참고로 Cryptrec은 일본 정부 관련 기간에서 사용될 암호의 표준으로 00.06.13~07.14에 응모를 받아 2001.03까지 평가 완료 예정으로 평가 대상은 현재 일본이 SC27에 제안된 후보를 포함하여 RC6, Rijndeal 등이 추가로 평가될 예정임. NESSIE 는 유럽의 여러 학자들이 유럽표준으로 사용할 목적으로 암호 뿐 아니라 여러 보안 기술을 응모 받는 중이고 앞으로도 평가까지 시간이 걸릴 것임. Acting Editor가 한국의 제안은 SEED 하나 뿐으로 생각했던 것을 포함 한국의 제안은 다른 NB 대표들의 관심을 전혀 끌지 못했고 거론되지도 않았음. 여기에 대해 아래의 소감 항목에 좀 더 쓸 것임. X. Lai(스위스)를 새 Editor로 지명하기로 [R19f] 하였고, 새 Editor는 01.01.30까지 1st WD N2725를 만들어 SC27비서에게 보내고 [R6c] 이에 대한 NB의 comments를 01.02.28까지 받기로 [R8d].

33.04 Encryption algorithms Part 3 : Stream ciphers

Enc3 〈2656 802 NB contributions on NP 18033 in response to N2563 00.10.10〉

Editor로 지명된 [R19a] K. Sakurai(일본)이 주도하여 수요일 오후와 목요일 오전에 걸쳐서 회의를 진행. 일본에서 제안한 MULTI-S01 밖에는 아무 것도 제안된 것이 없었음. 그러나 이 MULTI-S01는 자체가 stream cipher라기보다 PANAMA (FSE98발표)라는 stream cipher를 암호화와 더불어 integrity를 동시에 주는 stream cipher의 mode of operation이었음. 논의 끝에 이 문서를 Pseudo Random Sequence Generation (IS 10116을 인용하여 block cipher부터 PSSG를 만드는 방법과 해쉬함수를 이용해 만드는 방법, 그리고 PANAMA나 SEAL 등의 dedicated PSSG를 포함)과 Usage of PRSG(C=P+K, MULTI-S01, f8 Keystream generator for 3GPP 등 포함)로 2개의 section으로 나누기로 하고 Editor는 01.01.30까지 1st WD N2726를 만들어 SC27비서에게 보내고 [R6d] NB는 이에 대한 comments를 01.02.28까지 보내기로 [R8e]. 한편 SC27 비서는 모자라는 부분에 대한 CfC를 NB에게 보내 2001.02.28까지 input을 요청키로.[R9c]. 만일 충분한 input이 없다면 이 project는 cancel될 가능성도 있음.

S.P. Hash function identifier for digital signature schemes

Hash function identifier가 잘 되어 있지 않으면 보안에 문제가 됨. 9796-2나 14888-2의 경우에도 그렇고, 있다가 없어진 9796-3 역시 이것이 가장 먼저 공격의 대상이었음. 따라서 acting editor로는 D. Johnson(미국)을 지정 [R3]하여 study period를 갖기로. 비서가 NB들에게 Call for Contribution을 내고, 각 NB는 2000.11.30이전에 제출하기로 [R2].

Ⅳ. 소감 및 결론

다음 WG회의는 04.23(월) 14:30~27(금)에 Oslo (Norway)에서 개최키로 [R7]하였고, 그 다음 SC27 Plenary와 동시에 열리는 가을 WG회의는 내년 10월 혹은 11월에 한국 서울에서 개최하기로 되어있다. 다른 NB들은 다들 비용이 많이 드는 회의를 가능한 하지 않으려 하고 있는 것이 실정이다. 일본도 10년만에 SC27 Plenary+WG 회의를 개최하였고, 미국도 7년만에 SC27 Plenary+WG 회의를 개최하였을 뿐 어느 나라도 우리처럼 6년만에 Plenary+WG 회의를 개최하는 나라는 없다. 영국이나 Norway는 짧은 기간에 두 번의 회의를 유치하였지만 그것은 WG 회의만 한 것이다. 우리나라의 경우는 기술적인 기여에 비해서 회의개최 등의 서비스에 너무 연연하는 것이 아닌가 하는 것이 소감이다. 이번에 회의는 이미 결정된 것이니 어쩔 수 없다 하더라도 다음부터는 실익이 없다면 비용이 드는 회의 개최를 다른 나라에 비해서 더 자주 하는 것은 삼가 했으면 한다.

비록 이번 회의에서는 아무 결론 없이 끝나기는 했지만 Trusted Time Service의 개념을 표준화하자는 idea가 우리 나라에서 나온 것은 고무적인 일이라고 생각한다. 앞으로 NWI으로 가지고 가는 데에 많은 수고를 더 해야 할 것이다.

매번 이야기 하지만 WG 회의에 참가할 사람과 의논 없이 comment/ballot을 해서는 안된다고 생각한다. 참석하고 있으면 그 NB를 대표하고 있는 사람이 되는 것이고, 그 NB의 의견을 대변해야 할 의무가 생긴다. 그런 경우 참석자가 이해하지 못하거나 동의할 수 없는 의견이 문서로서 올라가 있는 경우 무척 당황하게 되는 것이다.

〈著者紹介〉

이 필 중 (Pil Joong Lee)
1974년 2월 : 전자공학과
1977년 2월 : 서울대학교 전자공학과 석사
1982년 6월 : 미국 U.C.L.A. System Science, Engineer
1985년 6월 : 미국 U.C.L.A. Electrical Eng., Ph.D.
1980년 6월~85년 8월 : 미국 Jet Propulsion Lab. Senior Engineer (M.T.S.)
1985년 8월~90년 2월 : 미국 Bellcore, M.T.S.
1990년 2월~현재 : 포항공대 전자전기공학과 교수
2000년 9월~현재 : 포항공대 정보통신대학원 원장 겸 정보통신연구소 소장
관심분야 : 암호학을 중심으로 한 정보보안, Error correction coding을 중심으로 한 통신.