情 報 保 護 學 會 誌
第 11 券 第 3 號, 2001. 6

ISO/IEC JTC1/SC27(정보기술보안) WG2 22차 오슬로 회의 참가보고

이 필 중*, 장 청 룡**, 임 영 숙***, 강 경 희***

요 약

SC27의 WG2는 정보기술보안 그 자체에 대한 표준을 만드는 Working Group이다. SC27 소개는 한국통신정보보호학회지 제3권 제2호 (1993년 6월)를 참고하기 바라며, 본 고에서 소개하는 오슬로회의(2001. 4) 이전에 개최된 21차 동경회의(2000. 10)는 동 학회지 제11권 1호(2001년 2월)을 참고하면 본 고를 이해함에 있어 많은 도움이 될 것으로 사료된다. 본 고에서는 지난 2001. 4. 23(월)~27(금) 노르웨이 오슬로에서 개최된 22차 회의에 다녀와서 보안기술 표준화에 관한 최신 정보를 이 분야의 관심이 있는 전문가들에게 전파하고자 각 과제별로 진행사항과 회의결과 및 회의 중 특기할 사항들을 정리하였다.

Ⅰ. 서 론

이번 SC27/WG2 Oslo 회의에는 한국인이 본 고의 기고자 4명이 하였고, 한국에서 열렸던 95년 11월 회의를 제외한 과거 어느 회의보다 한국인이 많이 참석한 회의였다.

회의는 WG2 Convener 인 M. DeSoete(벨기에)가 4월 12일 개정된 문서번호 N2816 (=WG2/N464r3) "Revised meeting agenda for 22nd meeting of SC27/WG2, April 2001 Oslo(Norway)"에 따라 진행했고, 회의의 결의사항들은 4월 27일에 작성된 WG2/N467draft "Draft Resolutions of the 22nd meeting of SC27/WG2, April 2001"에 정리되었다.

본문에서 자주 쓰일 약어에 대한 풀이를 Ⅱ절에서 하고, Ⅲ절에 과제별로 진행사항을 정리하였다. 과제번호가 간혹 누락된 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 n으로 정리되어 있는 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
CfC	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
SoV	Summary of Voting
WD	Working Draft

* 포항공과대학교 전자전기공학과(pjl@postech.ac.kr)
** 경동대학교 정보통신공학부(crjang@kyungdong.ac.kr)
*** 한국통신 멀티미디어연구소(ylim@hanmir.com, puppycat@hanmir.com)

Ⅲ. 과제별 진행사항

본 절에서는 다음과 같은 순서로 각 과제별 논의 및 진행 결과를 정리하였다.

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

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

Mo64 지난 회의에서 Forward만 수정한 채로 재심 통과된 IS 8372(1987-1st ed., 2nd confirmation in 1997, 3rd confirmation in 2002)가 2004년 재심 예정이므로 본 회의에서는 논의되지 않았음.

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

MoN 〈2799r2 50 SoC on N2711 01-04-18〉
〈2711 36 1st WD 10116 00-12-19〉

지난 회의 재심 결과 수정하기로 한 IS 10116 (1991-1st ed., 1997-2nd ed.)의 1st WD에 대해 한국 등 9개국이 의견이 정리된 N2799r2를 중심으로 O. Jung(독일)의 주재로 수요일 오후 내내 검토하였음. 새로 추가하기로 한 Counter mode와 Statistical Self-Synchronization 부분에서 역시 고칠 것이 많았음. 특히 논의가 되었던 점들은 어떻게 parameter들을 택할 것인가에 대한 guide를 넣는 문제와, numerical example들을 보다 유용한 AES와 3DES로 바꾸는 문제였음. 한국이 낸 의견들은 다 받아들여졌으나, 워낙 고쳐야 할 부분이 많았던 관계로 다시 한번 WD 단계를 거치기로 하였음. 만족할 만한 진척이 있으면 서울회의 후에 1st CD를 내기로. Editor는 N2711을 update하여 WD N2985를 만들어 SC27 secretariat에게 01-05-31까지 보내고 [R1a] 각 NB는 이를 Study & Comment하기로 함. [R6a]

03.01 Entity authentication Part 1 : General model

EA1 지난 회의에서 reconfirm된 IS 9798-1 (1991-1st ed., 1997-2nd ed., 1st confirmation in 2002)는 2004년 재심 예정이므로 본 회의에서는 논의되지 않았음.

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

EA2 IS 9798-2 (1994-1st ed., 1999-2nd ed.)는 2002년 재심 예정이므로 본 회의에서는 논의되지 않았음.

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

EA3 〈2788 52 SoC on N2759 01-04-09〉
〈2759 2 CfC on periodical rev. for 9798-3 & 10118-3 00-12-20〉

정기 review 중인 IS 9798-3 (1993-1st ed., 1998-2nd ed.)에 독일만이 의견을 내었으나 9798-2와 9798-3이 review된 후 9798-1도 review하자는 것이었으므로 무시하고 특별한 논의는 없이 reconfirm하기로 함.

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

EA4 IS 9798-4 (1995-1st ed., 2000-2nd ed.)는 2003년 재심 예정이므로 본 회의에서는 논의되지 않았음.

03.05 Entity authentication Part 5 : Mechanisms using zero knowledge techniques

EA5 IS 9798-5 (1999-1st ed.)는 2002년 재심 예정이므로 본 회의에서는 논의되지 않았음.

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

Mac1 IS 9797-1 (1989-1st ed., 1994-2nd ed., 2000-3rd ed.)는 2003년 재심 예정이므로 본 회의에서는 논의되지 않았음.

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

Mac2 〈2807 5 SoV on N2651 01-03-21 〉
〈2651 17 FDIS 9797-2 00-09-14〉

1998-11에 1st CD가 되었던 것이 작년 9월

FDIS문서로 voting을 하였으나 미국만이 Disapprove 했고, 영국이 Approve with comments 였음. 그런데 Editor인 B. Preneel이 N2807을 미리 받지 못한 상태로 목요일 오전 열렸회의에서 미국의 comments는 쉽게 해결할 수 있는 것으로 확인되었고, 영국의 의견도 쉬운 것들이었으나, revision 중에 있는 10118-3에서 다루는 새로운 HF를 포함시킬 것인가에 대한 결론은 내지 못했음. Redundancy에 대한 중복 정의 중 한 개는 빼기로 했음.

06.01 Non-repudiation Part 1 : General

NR1 〈2531 50 SoC on review of 8372, 10116, 9798-1, 13888-1~3 (N2489) 00-04-03〉

Review 중인 IS 13888-1 (1997-1st ed.)에 N2531로 의견을 모였었고, 지난 회의에서 토의 결과 재심을 받은 결과가 그냥 confirmation하는 것으로 재심추천을 하기로 하였으나, 독일의 comment가 있어서 다시 목요일 오전에 잠시 논의되었음. Public and Private Key, 10181의 정의, Annex A should be changed because it is an informative annex, 새 정의를 위해서 표준을 수정할 필요가 있는지? 등이 거론되었음. 독일이 Editor를 provide한다면 가능성이 있다. 독일에서 새로운 WD를 만들어서 돌리기로, Secretariat은 NB에게 Call for Editor를 보내기로 함. [R12]

06.02 Non-repudiation Part 2 : Mechanisms using symmetric techniques

NR2 IS 13888-2 (1998-1st ed., 1st confirmation in 2000)는 2004년 재심 예정이므로 본 회의에서는 논의되지 않았음.

06.03 Non-repudiation Part 3 : Mechanisms using asymmetric techniques

NR3 IS 13888-3 (1997-1st ed., 1st confirmation in 2000)는 2004년 재심 예정이므로 본 회의에서는 논의되지 않았음.

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〉

이 표준은 삭제된 상태라 이번 회의에서는 논의되지 않았음.

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

DSM2 〈2784 11 SoV on CD 9796-2 (N2703) 01-04-04〉

〈2703 28 CD 9796-2 00-10-19〉

수정 중인 IS 9796-2(1997-1st ed.)의 1st CD에 독일, 일본, 미국이 Disapprove, 프랑스, 폴란드, 영국이 Approve with Comments, 이태리, 남아공, 스위스가 기권, 그리고 한국을 비롯한 14개의 NB가 Approve하였음. 이 결과를 Editor인 Mitchell(영국)의 주도로 월요일 오후와 화요일 오전에 걸쳐 회의를 했음. 독일이 반대한 이유는 한 scheme의 안전에 대한 note를 넣어야 한다는 것이었으나 잘못 생각한 것이었고, 다른 하나의 새로운 scheme을 넣자는 것이었으나 부가형이므로 이 표준에 맞지 않는다는 이유로 기각되었음. 또 제목을 "Methods relying on the difficulty of Factorization"으로 바꾸자는 것이었으나 지난 회의에 많은 시간을 들여 결정하였고, 또 이미 시기적으로도 너무 늦었다는 이유로 기각되었음. 일본이 반대한 이유는 10절의 security proof를 설명한 것에 "it is believed …", "it is likely that …"과 같은 표현이 나오는 것은 문제가 있으니 보다 정확한 표현으로 써야 하며, 본문보다는 차라리 informative annex로 돌려야 한다는 것이었고 받아들여졌음. 미국이 반대한 주요 이유는 몇 개의 scheme에는 Hash-function identifier가 option으로 사용되도록 하여야 하고 또 그래야 하는 이유도 설명해야 한다는 것이었는데 Editor를 미국에 도와주는 조건으로 받아들여졌음. 그 이외의 의견들은 다 받아들여졌음. Editor는 N2703을 update하여 FCD N2893를 SC27 secretariat에게 01-05-31까지 보내고 [R1b] 투표절차를 거치기로 함. [R8a]

07.03 Digital signature schemes giving message recovery Part 4 : Discrete logarithm based

mechanisms

DSM3 IS 9796-3 (2000-1st ed.)는 2003년 재심 예정이므로 본 회의에서는 논의되지 않았음

08.01 Digital signature with appendix - Part 1: General

DSA1 IS 14888-1 (1998-1st ed., 2000-corrected)는 2003년 재심 예정이므로 본 회의에서는 논의되지 않았음

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

DSA2 IS 14888-2 (2000-1st ed.)는 2003년 재심 예정이므로 본 회의에서는 논의되지 않았음

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

DSA3 〈2787r 3 SoV on N2705 01-04-18〉
〈2705 4 Draft Technical Corrigendum to 14888-3 00-12-20〉

IS 14888-3(1998-1st ed., 2000-corrected)에 대한 Corrigendum에 대한 투표의 결과는 헝가리, 남아공, 스위스 만이 기권하고 19개국이 찬성하였고, 한국은 numerical example을 확인해 봤다는 comment를 붙여서 찬성하였음. Editor인 A. Fujioka(일본)는 N2705을 update하여 N2899를 만들어서 SC27 secretariat에게 01-05-31까지 보내고 [R1c], secretariat은 이를 ITFF에 보내기로 함. [R10]

09.01 Hash-functions Part 1: General

HF1 IS 10118-1 (1994-1st ed., 2000-2nd ed.)는 2003년 재심 예정이므로 본 회의에서는 논의되지 않았음.

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

HF2 IS 10118-2 (1994-1st ed.)의 2nd edition인 〈2551 DIS 10118-2〉

이 00-12-15에 출판되었고, 2004년 재심 예정이므로 본 회의에서는 논의되지 않았음.

09.03 Hash-functions Part 3 : Dedicated hash-functions

HF3 〈2885 20 Belgian contribution : Whirlpool HF 01-04-24〉
〈2788 52 SoC on per. review of 9798-3 & 10118-3 01-04-09〉

재심 중인 IS 10118-3 (1998-1st ed.)에 대해 Acting Editor인 C. Mitchell[R3a]이 주제하여 목요일 오전에 한시간 가량 회의를 하였음. Call for Contribution 문서인 N2759에 대해 스웨덴과 미국 만이 응답을 하였고, 지난 회의에서도 거론되었던 미국 NIST의 SHA-256, SHA-384, SHA-512도 넣자는 제안이 있었음. 그리고 사소한 2가지 수정을 요구하였음. 그리고 현지에서 추가된 문서로 벨기에서 Whirlpool이라 부르는 새 HF를 포함시키자는 제안이 있었는데 이것은 Rijndael과 같은 원리로 HW구현 시 효율적으로 S box를 바꾼 512 bit의 hash-code를 내는 것으로 NESSIE에 제출된 것이라 함. Whirlpool도 SHA'도 아직 나온지도 얼마 되지 않았고 NIST와 NESSIE의 review process도 끝나지 않은 것이라 당분간 관망하기로 함. 그리고 새 editor로 중국계 영국 대표인 L. Chen이 결정되었음 [R14]. Revision하기를 recommend하는 문서인 N2926를 SC27 Plenary에 보고하기로 함. [R15] Editor는 IS 10118-3을 update하여 N2897을 만들어 SC27 secretariat에게 01-05-31까지 보내고 [R1d] 각 NB는 이를 Study & Comment하기로 함. [R6b]

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

HF4 IS 10118-4 : (1999-1st ed.)는 2002년 재심 예정이므로 본 회의에서는 논의되지 않았음.

18.02 Key management Part 2 : Mechanisms using symmetric cryptographic techniques

KM2 IS 11770-2 (1996-1st ed., 1st reconfirmation in 1999)는 2002년 재심 예정이므로 본 회의에서는 논의되지 않았음.

18.03 Key management Part 3 : Mechanisms

using asymmetric techniques

KM3 IS 11770-3 (1999-1st ed.)는 2002년 재심 예정이므로 본 회의에서는 논의되지 않았음.

23 Data processing Check character systems

CCS 〈2763r 9 SoV on N2569 01-02-28〉
〈2569 15 FCD of IS 7064 00-09-14〉

IS 7064의 재심 수정판의 FCD인 N2569에 대한 Voting 결과는 독일만이 Disapprove했고, 덴마크, 일본, 폴란드, 영국이 Approve with comments를 했음. 회의에 참가하지 않아 구체적인 회의 내용을 모르겠음. Editor인 B. Preneel은 N2569을 update하여 FDIS N2902를 만들어 SC27 secretariat에게 01-05-31까지 보내고 [R1e] 투표절차를 거치기로 함. [R9]

26.01 Cryptographic techniques based on elliptic curves Part 1 : General

EC1 〈2713 FDIS 15946-1 00-11-01〉
FDIS 투표 중이라 본 회의에서는 논의되지 않았음.

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

EC2 〈2555 ?? FDIS 01-04-??〉

회의에 참석하지도 않은 Editor R. Horne(영국)이 준비하기로 했던 FDIS N2555만을 회의 직전에 SC27 비서에게 전달했다는 이야기만 있었고 런던 회의에서 주어졌던 문서번호를 붙여 투표하기로 함.

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

EC3 〈2708 ?? FDIS 15946-3, Key establishment 00-11-01〉

FDIS 투표 중이라 본 회의에서는 논의되지 않았음.

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

EC4 〈2803 7 Numerical Examples of ECMR & ECAO 01-04-09〉
〈2785r 24 SoV on 2710 01-04-17〉
〈2710 29 1st CD 15946-4 00-10-18〉

1st CD에 대한 Voting 결과는 카나다, 프랑스, 독일, 한국이 Disapprove였고, 3 NB가 기권, 일본, 폴란드, 스웨덴, 영국, 미국이 Approve with Comments, 그리고 11 NB가 Approve였음. 반대한 나라들의 기본적인 이유는 notation등의 inconsistency이었고, 아직 FCD로 갈 만큼 mature하지 못하다는 것이었음. 프랑스의 주장은 EC는 워낙 짧으니까 서명 속에 메시지의 일부를 포함시킬 것이 얼마나 있겠느냐는 것인데 그것도 사용될 수가 있다는 반론에 밀렸음. 독일의 주장 중의 가장 문제가 된 것은 현재의 4개 scheme(EC-NR, EC-MR, EC-AO, EC-PV)들이 모두 EC-DSA에만 근거했지 EC-GDSA에 근거한 것은 없으며 특히 EC- GDSA의 형태의 key를 갖고 있으면 쓸 수가 없으므로 현재의 CD는 complete한 표준이 되지 못하므로 N2785r에 첨부한 대로 EC-GDSA에 기반한 EC-GNR, EC-GMR, EC-GAO, EC-GPV를 추가하자는 것이었음. 독일의 EC1 Editor를 비롯한 몇 명의 대표는 또 EC-KCDSA에 기반한 것도 들어가야 하지 않느냐는 의견도 주장했음. 물론 반대의 의견도 있었기에 열띤 공방은 했으나 한국의 의견을 물었을 때 이미 18:00가 넘어가는 중이었으므로 하루 저녁 생각할 시간이 필요하니 다음날 계속하자고 했음. 본인은 새벽에 많은 고민 끝에 EC-KCDSA에 기반한 것을 3가지 변형을 만들어 가지고 갔고, 많은 토론 끝에 추가를 결정했으나 Editor가 독일과 한국의 도움으로 새로운 CD를 만들기로 결론을 보았음. Editor는 N2710을 update하여 N2904를 만들어 SC27 secretariat에게 01-05-31까지 보내고 [R1f] 각 NB는 이를 Study & Comment하기로 함. [R6c]

27.01 Time Stamping Services - Part 1 : Framework

TSS1 〈 2715 Text of 1st CD 18014-1 〉
〈 286r1 SoC on 1st CD 18014-1 01.4.24〉

Time stamping Service part1 (WD 18014-1)을 final CD로의 승격에 대한 안건과 각 문서와 관

련된 특허 인용의 문제가 다음과 같이 논의되었음:

- Final CD ballot에 각국 찬성. (R8b)
- 특허 관련된 정보를 annex 로 만들기로 함(informative annex).
- time stamp renewal, reissue에 대하여 논의 · renewal은 기존의 time stamp token에 TS서버의 전자서명만 첨가. Reissue는 새로 time stamp token 구성하여 재 발행하는 것으로 정리되고 이 둘사이의 차이점을 표준문서에 반영하기로 함.
- ASN.1 표기 오류 수정 및 전체적인 ASN.1 표기를 자세히 기술 하기로 함.
- definition을 보강하기로 함. tss의 전체 part에서 사용되는 용어를 다 열거하기로 함 (definition세부 내용까지).
- annex 들의 변경, bibliography는 annex 로 하지 않고 별도로 두기로 함.(Bibliography)
- ASN.1 표기를 IETF와 맞추기로 함.
- 전반적으로 editorial comments 수용.

27.02 Time Stamping Services - Part 2 : Mechanisms producing independent tokens

TSS2 〈2804 SoC on 2nd WD 18014-2 01.04.09〉
〈2717 2nd WD 18014-2 01.01.26〉
〈2854 UK expert comments on WD 18014-2 01.4.23〉

IETF에서 논의되는 TIME STAMPING SERVICE와의 consistency, 즉 상호 연동에 대한 해결 방안 제시에 관한 사항도 논의됨. IETF time stamp draft를 준용하는 client의 요구를 받아줄 수 있도록 Conformance 확보를 위해 ISO 측 전문가들이 기술 검토할 것을 요구함. 문서를 전체적으로 명확히 하고 읽는 사람의 이해도를 높이는 쪽으로 다음과 같이 보완 서술하기로 함:

- 용어 정의를 추가하기로 함. 각 part에서 사용되는 용어들은 part1으로도 반영하자는 요청이 있었고 part1 editor 가 수용함.
- 대칭키를 사용하는 메카니즘과 전자서명을 사용하는 메카니즘의 절 제목을 좀더 엄밀하게 정의하기로 함.
- 전자서명을 사용하여 time stamp 토큰을 생성하는 scheme 에서 PKI 기술을 사용할 때의 장단점을 기술하기로 함.
- validation, verification 의 주체를 각각 time stamp requester와 time stamp verifier 로 명확히 구분함. 이를 표준문서에 반영하기로 함.
- Part 2는 1st CD (SC27 N2912)로 지정됨(R7a).

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

TSS3 〈2805r1 SoC on 2nd WD 18014-3 01.04.18〉
〈2719 text of WD 18014-3 〉
〈2855 UK Expert contribution on WD 18014-3 01.04.23〉
〈2891 Additional Extonian NB comments on 2nd WD 18014-3 (S27 N2719) part 3 01.4.25〉

Part3에 대한 에스토니아 COMMENTS (linking, aggregation) 내용을 보면 기존 구조체와 프로토콜에 많은 변형을 줄 요소들을 내포하고 있고 그 중요도가 인지되어 해당 문서의 부록으로 첨부하도록 하고 세부 내용을 차기 서울회의에서 재 논의하기로 함. 또한 에스토니아 안이 part1에 미치는 영향을 검토하고 part1으로 comment를 내기로 함. part2와 3 회의에서 part1의 scheme이 part2와 3 의 데이터 구조 및 프로토콜을 수용할 수 있도록 변경되어야 한다는 논의가 있었고 이를 확인하기 위해 각 part들의 editor 들이 함께 part1을 검토하기로 함. time stamp request transaction에 대한 전반적인 시나리오를 기술하고 각 경우에 프로토콜 및 메시지 구조체에 대한 기술적인 부분을 차기 서울회의에서 다시 논의하기로 함. 전체적으로 part3가 너무 general하게 서술되어 있어서 모호함이 많은 것을 인정하고 part3를 전체적으로 자세히 기술하기로 하고 데이터 구조체에 대한 그림도 싣기로 하였으며 다음 사항을 보완하기로 함:

- 용어를 추가로 정의하여 서술하기로 함.
- 상세한 ASN.1 표기를 문서에 기술하기로 함.

part3와 관련된 특허를 소지한 회사에 특허에 대한 ISO 절차 준수 여부를 묻는 편지를 보내서

resonable 한 범위내에서 특허 사용에 대한 허용 여부를 check 하기로 함. 특허 사용에 대한 문제가 있을 경우 표준에서 삭제하기로 함.

Editor는 에스토니아 comment를 포함하여 N2914를 만들어 SC27 secretariat에게 01-05-31까지 보내고 [R1i] 각 NB는 이를 Study & Comment하기로 함. [R6d]

31 Random bit generation

RNG 〈2802 German & Swedish comments on WD 18031 (N2559) 01-04-19〉
〈2727 17 3rd WD 18031 01-04-19〉
〈2559 20 2nd WD 18031 00-10-04〉

Editor인 Chawrun(카나다)가 주관하여 1st WD이었던 N2559에 대한 독일과 스웨덴의 comment 문서인 N2802와 새로 준비한 2nd WD N2727을 가지고 수요일 오전에 잠간 회의를 하였음. 아직도 채워지지 않은 많은 부분들이 있고, 또 randomness testing을 넣을 것인가에 대한 토의도 있었으나 결론을 내지 못하고 일단 그냥 문서를 update하기로 함. Editor는 N2727을 update하여 N2906를 만들어 SC27 secretariat에게 01-05-31까지 보내고 [R1j] 각 NB는 이를 Study & Comment하기로 함. [R6e]

32 Prime number generation

PNG 〈2465 Bellgium contribution on efficient PRG with provable security ??〉
〈2743 8 WD 18032 01-04-18〉

새로 지명된 T. Tederson 회의 직전에 만든 N2743은 WD라기 보다는 WD의 초안에 해당되는 것이었고, WD2 N465문서도 검토를 할 시간이 없었기에 특별한 토의가 없었음. Editor는 N2743을 update하여 N2908를 만들어 SC27 secretariat에게 01-05-31까지 보내고 [R1k] 각 NB는 이를 Study & Comment하기로 함. [R6f]

33.01 Encryption algorithms Part 1 : General

Enc1 〈2723 14 Text of 1st WD 18033-1 01.02.10〉
〈2806 9 SoC on WD 18033-1 01.04.19〉

SC27 N2730(Report of the Tokyo meeting on NP 18033-1)에 준거하여 작성한 SC27 N2723을 SC27 N2806에서 제안된 각 회원국의 의견을 논의하였다. 주요 토의 사항으로는

- 본 표준의 목적 및 적용 범위를 기밀성(confidentiality)에 한정하는 암호 알고리즘의 표준화로 하고 무결성 및 인증에 관한 것은 별도의 표준화로 처리 하기는 것으로 함.
- 7절(본 표준에서의 알고리즘 선정 기준)에 대하여 한국에서는 본 표준의 범위가 기밀성을 위한 알고리즘들을 표준화하는 것이며 암호 알고리즘의 선정에 대한 표현을 이 절에 수용함은 바람직하지 않음을 주장.
- 일본 측에서 SC27 N2848을 후보 암호알고리즘의 선정 절차를 Part 1의 7절을 보다 상세히 규정하는 것을 제안함.
- Editor 인 Christ Michel의 중재로 7절을 본 표준의 부기(Annex, Informative)로 처리하기로 하고 세부 내용은 일본국의 일부 내용을 수용하기로 함.
- 제 7절에서 7.1의 4인 maturity 절을 2가지로 나누어 처리하기로 함
  + 사용의 광의성, 분석의 공개성, 고찰성
  + recognized organization으로부터의 endorsement.

33.02 Encryption algorithms Part 2 : Asymmetric ciphers

Enc2 〈2765 55 Editor's contributions on public key 01.02.13〉
〈2812 14 US NB contributions on N2712(on OAEP) 01.04.09〉
〈2858 7 Additional expert contributions on 18033-2(on CRYPTREC) 01.04.24〉

이번 Oslo 회의 기고(editor 기고(N2765) 포함)에 대한 전문가들의 의견을 2001년 5월까지 제안하도록 회원국에 요청하기로 함. 이번 Oslo 회의 기고와 5월까지의 기고들을 포함한 모든 기고들을 고려하여 N2765에 기술된 분석을 재 작성하여 확장시키도록 editor에게 요구하기로 함. 또한 금년 Crypto 2001(2001년 8월 21일) 기간내에 전문가 회의를 개최할 수 있도록 editor에게 요구하고 만일 가능할 경우, SC27/WG2 사무국을 통하여 회의

개최를 소집하도록 요구함. WD18033-1에 있는 알고리즘 선정 기준에 의하여 제안된 알고리즘들의 비교 평가 분석 데이터를 이용하여 본 표준에 수용할 알고리즘의 결정이 용이하도록 많은 자료들을 각 회원국 및 그의 전문가들로부터 제안이 되도록 요구함.

33.03 Encryption algorithms Part 3 : Block ciphers

Enc3 〈2725 29 Text for ISO/IEC WD 18033-3 01.04.10〉
〈2742 1 Report of Oct.-2000 meeting 00.10. 19〉
〈2820r1 6 Japan-Korea contribution 01.04.17〉
〈2852 4 Comparison of MISTY1 and KASUMY 01.04.19〉
〈2859 3 CRYPTREC results 01.04.24〉
〈WG2 Oslo1 15 Presentation of Camellia 01.04.24〉

현 작업 문서(N2725, TDEA와 AES만 포함)에 대한 주요 토의 사항으로는,

- 미국은 AES에 대하여 2001. 5. 29일 까지 의견수렴 기간에 있으며 최종 표준은 금년 10월에나 가능 함.
- TDEA의 안전성(예, 평문의 길이 등)을 부기(informative)로 포함시키기로 하고 이의 해당 내용을 미국측에서 제공하기로 함.
- 부기에 DES를 추가하기로 함.
- TDEA 키 선택의 2가지 선택사항을 본문에 수용하고 그와 동치의 single-DES에 관한 선택사항은 삭제하기로 함(그러나 이를 주석으로 처리).

나. 그 밖의 제안 알고리즘에 대한 주요 논의로서,

- 일본측의 기고문은 :
  - 64-비트와 128-비트로 분류하여 MISTY1을 현재 수용된 Triple-DES에 추가로 처리하자는 제안이었으며,
  - 그밖에 MISTY1과 KASUMI와의 차이, Camellia와 Hierocrypt에 대한 추가 기고문이 제안됨.
  - 지금까지는 일본국의 특정 후보로 제안하는 것은 없으며, 지난 동경회의에서 Cryptrec의 결과를 보고하기로 되어 있었으나 아직 그 결과를 얻을 수 없어 금년 9월에 평가 결과가 나오므로 10월 서울 회의에 제안이 가능할 것임.
- NESSIE도 9월 2차 평가 결과가 나오면 이를 제안할 것임.

한편, 논의 결과 한국측은 Zodiac을 후보 알고리즘에서 철회(N2820r)하기로 하고, 미국에서는 Rijndael이 AES로 선정되어 이것만을 남기고 나머지는 철회하기로 함. 다만, AES finalist 후보로 제안된 것 중에서 다른 회원국으로부터 제안된 것은 그대로 두기로 함. 또한, 일본국이 알고리즘 선정의 편의를 위하여 평가 기준에 의하여 비교표를 작성하여 서울회의에 제안하기로 하고 이에 SEED도 포함하여 처리하기 함. (그러나, Oslo 회의 보고(N2919 : Oslo 회의 보고)에는 이의 표현을 "현재의 알고리즘(TDEA, AES 이외 알고리즘의 추가에 대한 고려에 앞서 더 많은 정보가 필요하므로 본 표준에 특정 알고리즘을 포함시키기 위한 이유에 대한 비교 정보를 제공하도록 모든 회원국(특히, 알고리즘 제안 NB)에게 요구하기로 함" 으로 처리하기로 함.

33.04 Encryption algorithms Part 4 : Stream ciphers

Enc4 〈2882 17 Japanese expert contribution to 18033-4
MULTI-S01 with PANAMA 01.04.24〉
〈2884 3 Editor's contribution to project 1.27.33.04(NP 18033-4)? Part 4 01.04.24〉

차기 서울회의 까지 관련 기고문의 제출을 각원국에 또 다시 요구하기로 함. 다음의 알고리즘(및 모드)에 대하여 1차 WD에 다음 사항을 포함하도록 함;

- 키 스트림의 생성을 위한 블록 사이퍼의 모드
  + 동기 스트림 사이퍼의 예로서 블록 사이퍼의 OFB 모드
  + 자기동기 스트림 사이퍼의 예로서 블록 사이퍼의 1-비트 사이퍼 피드백(CFB) 모드
  + 블록 사이퍼에 의한 여타 유용한 모드(N2711의 WD18066에 있는 통계적 모드와 카운터 모드 포함)
- 스트림 사이퍼의 모드
  + 2진 합 모드(전형적인 XOR-연산)

+ 여타 유용한 모드(N2882 MULT-S01의 모드 포함)
+ 키-스트림 생성을 위한 전용 알고리즘(N2882의 PANAMA 포함).

S.P. Hash function identifier for digital signature schemes

〈2752r 6 SoC on N 2748 01-01-19〉
〈2748 2 CfC on WG2 study period on Hash-function identification for digital signature schemes 00-11-06〉

Hash function identifier가 잘 되어 있지 않으면 보안에 문제가 될 수 있음을 벨기에와 미국의 제안을 검토하여 인식하여 이러한 해쉬함수 식별자를 서명과정에 이용할 때 문제가 없는 경우와 잠재적 공격 가능성을 방지할 수 있는 경우가 있음을 확인하였다. 따라서, 해쉬함수 식별자의 사용은 허용하되 하나이상의 식별자를 허용하는 본 복원형 디지털 서명의 표준에서는 필요치 않으며 이러한 식별자의 사용에 대한 적합 여부는 비용대 효익 문제로 하여 사용자가 결정토록 함을 9796-2에 여기에 대한 언급을 하고 study period를 끝내기로 함. Editor인 D. Johnson은 Final Report를 N2883으로 내어 돌리기로. [R2]

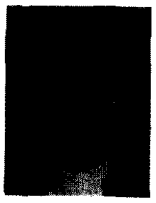
Ⅳ. 소감 및 결론

차기 WG2회의는 2001.10.16(화) 10:00 ~ 10.19(금) 16:00에 대한민국 서울 ASEM 회의장에서 개최키로 [R5b] 하였다. Logistical Information for Seoul Meeting 문서가 Oslo-03으로 배포되었는데 Hotel 정보가 누락되어 물어보는 사람들이 많았다. 그리고 가격이 저렴한 호텔이 있느냐는 질문도 많았으며 여러 종류의 Hotel을 알아봐서 Hotel 정보도 보내야 할 것으로 생각된다.

특히, 한국에서 제안한 SEED 암호 알고리즘과 관련하여서 관련 자료의 공개는 KISA를 통하여 하고, 일본측에서의 관련자료의 분석을 위하여 우선 지난 동경회의 기고 자료를 분석자료로 활용하도록 할 것이다. 일본국의 분석 비교 자료는 안전성과 실용성(특히, 구현(S/W, H/W, 속도별 환경별로))에 중점을 둘 것으로 예상되어 국내에서도 이에 준하는 활동(일본국과의 긴밀한 협력을 갖지만 이들도 평가자를 선정하여 그로부터 평가 결과를 받기까지는 상당한 시일이 소요될 것으로 예상하며(5~6개월), 평가결과의 초안은 이의 검토가 어느 정도의 결과를 얻을 때가 되어야 가능한 것으로 예상되어 이에 대응한 국내의 활동이 필요함)이 요구되며, 관계 전문가들의 많은 주의와 관심이 요구된다.

〈著者紹介〉

이 필 중 (Pil Joong Lee)
1974년 2월 : 서울대학교 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~1985년 8월: 미국 Jet Propulsion Lab. Senior Engineer (M.T.S.)
1985년 8월~1990년 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.



장 청 룡 (Chung-ryong Jang) 종신회원
1980년 2월 : 성균관대학교 전자공학과 졸업
1986년 8월 : 연세대학교 대학원 전자공학과 석사
1994년 2월 : 성균관대학교 대학원 정보공학과 박사
1979년 12월~1983년 12월 : 한국전자통신기술연구소(현, ETRI), 연구원
1984년 1월~1997년 1월 : 한국통신 연구개발본부 선임연구원
1997년 3월~현재: 경동대학교 정보보통신공학부 조교수
관심분야 : 보안제품 시험, 통신망 보호, 블록암호,

임 영 숙 (Young Sook Lim)
1987년 2월 : 연세대학교 전산과학과
1989년 2월 : 한국과학기술원 전산과 석사
1989년 3월~1998년 7월 : 한국통신 통신망연구소
1998년 7월~현재 : 한국통신 멀티미디어연구소

관심분야 : PKI 기반의 정보보안 및 응용서비스,
차세대 통신망의 정보보안

강 경 희 (Kang Kyung Hee)
1991년 2월 : 한국외국어대학교 경영정보학과
1993년 2월 : 한국외국어대학교 경영정보학과 석사
1993년 3월~현재 : 한국통신 멀티미디어 연구소 전임연구원 재직
관심분야 : PKI기반의 응용서비스 개발