通信情報保護學會誌
第5卷 第2號, 1995. 6

Asiacrypt'94를 통한 최신 암호학의 연구 동향

(Recent Trends of Cryptologic Research from Asiacrypt'94)

김 광 조*

요 약

본고는 1994년 11월 25일 부터 12월 1일 까지 호주의 Wollongong 대학에서 세계 암호학 학회의 협찬으로 아시아 국가를 중심으로 개최되는 Asiacrypt'94에 참가하여 발표 논문을 중심으로 암호학의 최근 연구 동향과 결과를 요약 정리하고 한국에서 개최하기로 확정된 Asiacrypt'96에 대비한 참조 사항을 기술하였다.

1. 서 론

1981년 이후 암호학 관련 국제 회의는 이미 미국이나 유럽 지역을 중심으로 Crypto나 Eurocrypt가 매년 정례적으로 개최되어 지금까지 최근 연구 결과의 발표 및 토론장을 제공해오고 있다. 그리하여 전세계적으로는 94년말 현재 약 700여명의 회원을 가진 세계 암호학 학회(IACR, International Association for Cryptologic Research)가 결성되어 운영되고 있다.

아시아 지역을 개최 지역으로 한 Asiacrypt는 1991년에 일본이 최초로 개최하였으며 그후, 차기 개최국이 결정되지 않고 있다가 이미 1990년과 1992년에 Auscrypt를 개최한 바 있는 호주가 3년만에 2번째 Asiacrypt를 개최하기에 이르렀다.

본고에는 저자가 Asiacrypt'94에 참가하여 회의 진행 사항 및 최신 연구 결과, 초청 강연 내용 등을 요약 보고하고자 하며 Asiacrypt'96을 한국에서 개최하기로 확정 된 바 차후 국내 개최에 필요한 참조 사항을 기술하고자 한다.

본고의 구성으로는 제2장에는 본인의 여행 일정을 간단히 소개하고 제3장에는 회의 개요를 비롯하여 초청 강연 및 발표 논문의 내용 등을 요약하며 마지막에는 맺는 말을 기술한다.

* 종신회원, 한국전자통신연구소 실장

2. 여행 일정

1994년 11월 25일 오후 8시 대한항공 KE671편으로 서울을 출발하여 시드니 국제 공항에 도착하니 현지 시간으로11월 26일 오전 8시(한국과 시차가 1시간과 Summer time 1시간 포함 2시간 시차 있음)가 되었다. 동행한 일행이 미리 연락하여 공항에는 한국 사람이 반갑게 반겨 주었으며 예약된 호텔까지 자동차로 안내하여 주었다. 미리 1주일전 호주 현지에 출장온 ETRI의 지성택 선임 연구원을 호텔에서 만나 같이 행동하기 시작하였다. 11월27일 시드니에서 Asiacrypt'94의 개최지인 Wollongong 대학으로 가기 위해 기차로

1시간 40분 소요하여 Wollongong역으로 이동하였다. 이동 중 중간에 Waterfall이라는 기차역에서 버스로 갈아 타는 예기치 않는 일도 있었다. 이것은 주중에는 정기 기차를 운행시키고 주말에는 구간별 선로 보수 작업을 위하여 기차 운행을 중단한다는 사실을 나중에야 알았다. 숙소는 역에서 택시로 약 10분 거리에 위치한 Weerona college이었으며 Wollongong 대학은 Weerona college에서 걸어서 25분 정도 소요되는 곳에 위치하였다. 호주는 우리나라와 달리 좌측 통행이므로 직접 차를 운전할 경우에는 사전에 충분히 지도를 숙지할 필요가 있다. 11월 27일 오후 5시 30분경, 등록을 마치고 오후 6시 부터 Reception이 시작되었다. Reception에는 간단한 다과와 함께 세계 여러 유명 암호학자들과 면담할 수 있는 좋은 계기가 되었다. 11월 28일 9시부터 12월 1일 12시까지 총 30편의 논문이 발표되어 이를 경청하였고, 특히 11월 28일에는 한국에서 유일하게 발표 논문으로 채택된 "Semi-bent function"이란 제목의 논문이 발표되었다. 12월 1일 Wollongong 대학의 Zheng 박사와 요꼬하마 국립 대학의 Matsumoto 교수와 함께 차기 Asiacrypt'96에 관한 의견을 교환한 후, Wollongong을 출발하여 시드니에 도착하였다.

3. 회의 내용 및 주요 연구 결과

3.1 개 요

114명이 참석한 이번 회의는 매년 개최되는 Crypto나 Eurocrypt에 비해 다소 참석자 수가 적었다고 할 수 있다. 프로그램 중 3건의 초청 강연이 있었으며, 논문은 총 94편이 제출되어 이중 30편의 논문이 선정, 발표되었다. 먼저 각 국가별 논문 제출수와 채택된 논문수는 〈표 1〉과 같다. 중국은 채택된 논문 발표자가 회의에 참가하지 않았다.

국가별 참가자 수는 〈표 2〉와 같으며 한국이 주최국 호주를 제외하고 미국, 일본 다음으로 6명(ETRI 2명 외 4명)이 참석하였다. 회의장은 대학의 강의실로 의자 만이 나열된 교실이었으며 기간 중의 날씨는 섭씨 15 ~ 25도로 더운 편이었고 때때로 저녁에 1회씩 비가 내렸다. 또한, 기간 중 숙소와 회의장간의 교통편이 별도로 없어 시내 버스나 도보로 회의장에 참석하여야 하였고 휴식 시간에 다과의 부족 등 참석자가 다소 불편하였으며 정규 프로그램 이외에 별도의 현장 견학 프로그램은 없었다. 부록에는 프로그램의 전체 구성과 각종 위원회의 구성을 첨부하였다.

〈표 1〉 국가별 제출 및 채택 논문 수

국 가	제출 논문 수	채택 논문 수	비 고	국 가	제출 논문 수	채택 논문 수	비 고
호주	17	6		뉴질랜드	2	2	
일본	14	8		캐나다	1	0	
대만	13	0		덴마크	1	0	
미국	9	3		핀란드	1	0	
한국	7	1		남아프리카	1	0	
중국	7	1	미발표	스페인	1	1	
독일	6	1		스위스	1	0	
프랑스	5	2		영국	1	0	
이스라엘	3	2		유고	1	1	
사우디	3	1		계	94	30	

〈표 2〉 국가별 참가자 수

국 가	참가자 수	국 가	참가자 수	국 가	참가자 수
호주	55	중국	3	사우디	1
미국	8	싱가폴	3	영국	1
일본	8	체코	3	스페인	1
한국	6	러시아	2	덴마크	1
독일	5	이스라엘	2	유고	1
프랑스	4	핀란드	2	뉴질랜드	1
노르웨이	4	벨기에	2	스웨덴	1
계	114				

3.2 초청강연(3건)

독일의 Beth (U. of Karlsruhe)는 자신이 소장으로 근무하고 있는 EISS(European Institute of System Security)에서 연구하고 있는 Cryptographic primitives, 일방향 함수, DSA(Digital Signature Algorithm)의 현황, 자신이 제안한 영지식 증명 방법, 의료 정보 보호를 위한 스마트 카드의 응용등을 소개하고 Kerbores 프로토콜의 문제점을 지적하고 자신의 연구소의 최신 연구 결과인 SELANE에 관하여 발표하였다. 미국의 Meadow(Naval Research Lab.)는 최근의 연구 과제로서 대두되고 있는 암호 프로토콜의 형식 검정 기법으로 상태 기계를 이용한 방법, Modal 논리를 이용한 방법, 대수학적 방법 등의 기존의 방법들을 조사하여 소개하고 앞으로 하여야 할 분야를 제기하였다. 일본의 Imai(동경대)는 대역 확산 통신 방식에서 비익성, 불추적성, 인증성, 내 재밍성(Anti-jamming)의 개념을 소개하고 암호학적 기법을 이용하여 이러한 성질을 만족시키는 방법의 현황을 조사 분석하고 CDMA (Code Division Multiple Access) 시스템의 암호학적 문제점을 지적하고 이에 대한 대비를 강조하였다.

3.3 Session 별 주요 발표 내용

3.3.1 비밀 공유법(4편)

미국의 Desmedt(U. of Wisconsin-Milwaukee)외 2인은 두 그래프사이에 isomorphism 성질을 이용하여 perfect zero-knowledge threshold proof의 설계 방법을 제안하였고 그 결과를 일반적인 접근 제어 구조 설계로 확장하였다. 일본 Okada외 1인(동경공업대)는 비밀 공유 방법으로 각 참가자 P_i에 대하여 비밀 S의 부분 정보 V_i를 $|V_i| < |S_i|$인 불완전 비밀 공유방법에서 $|V_i|$의 하한을 구했으며, 특정한 접근 구조에 적합한 최적 $|V_i|$의 크기를 결정하였다. 호주의 Jackson외 2인(U. of Adelaide)은 다중 비밀 공유 방법으로 참가자가 복수의 비밀에 관한 복수의 부분 정보를 갖는 구조를 분석하여 일반적인 구성 방법과 이상적인 구성 방법이 Matriod에 대응된다는 결과를 제시하였다. 일본의 Kurosawa외 1인(동경공업대)은 비밀 공유법를 정보 이론적 해석에서 탈피하여 조합론적 해석 방법을 제안하여 비밀 정보의 분포 상태에 무관한 경우에도 적용되는 결과를 제시하였다.

3.3.2 스트림 암호(3편)

유고의 Mihaljevic(Ins. of Applied Mathematics and Electronics)는 이진 수열의 새로운 척도로서 통계적 가설 검정의 개념을 응용한 2개의 수열간의 Levenshtein distance를 도입하고 이에 근거한 새로운 해독 방법을 제안하였다. 이를 이용하면 MacLaren-Marsaglia shuffler와 1990년 Golic이 제안한 시각에 따라 메모리가 가변되는 논리가 해독됨을 보였다. 스페인의 Amparo외 1인(CSIC)는 비선형 여과 함수에 의해서 생성된 이진 수열의 선형복잡도를 계산하는 방법으로 Rueppel이 제안한 Root Presence Test를 확장하여 일반적인 하한을 제시하였다. 호주의 Golic(QUT)는 임의의 M 비트 메모리를 가지는 이진 수열 생성자는 많아야 M 개의 변수를 갖는 non-autonomous 선형 궤환 쉬프트 레지스터로 선형적으로 모델화될 수 있음을 보였다.

3.3.3 암호 함수(3편)

스트림 암호, 블럭 암호 그리고 해쉬 함수 등에 사용되는 암호 함수는 대부분 부울 함수로서 세계적으로 지속적인 연구가 되고 있다. 먼저 한국의 지성택외 2인(ETRI)은 짝수의 벡타 공간에서 bent 함수와 유사한 성질을 갖고, 더우기 bent 함수가 갖는 암호학적 취약점을 제거한 semi-bent 함수를 제안하였다. 또한, 부울 함수를 이용하여 치환(Permutation)을 생성할 때, 부울 함수 쌍사이에 필수적으로 요구되는 성질로 SUC (Strict Uncorrelated Criterion)을 정의하고 이를 만족하는 부울 함수쌍을 생성하는 방법을 제안하였다. 호주의 Seberry외 2인(U. of Wollongong)은 Propagation Criterion(PC)을 만족하지 않는 점의 개수와 벡터 공간의 차원, 비선형치 그리고 선형 구조와의 관계를 규명하였다. 또한, PC를 만족하지 않는 점의 개수가 3이나 6인 경우는 존재하지 않음을 증명하였다. 중국의 Xiao외 1인(Xidian U.)는 불참으로 논문 발표는 생략되었으나 논문 내용은 부울 함수의 입력과 출력 사이에 최대 상관값을 조사한 내용으로 그들이 정의한 최대 상관값이 진정한 의미로 상관 측도(Correlation measure)임을 주장하였다.

3.3.4 프로토콜(4편)

미국의 Yacobi(Bellcore)는 off-line상에서 추적 불가능한 새로운 전자 현금 방식을 제안하였다. Crypto'93에서 Brands 등이 개발한 현재까지 가장 효율적인 방식에 비하여 계좌의 인출 문제를 제외한 모든 면에서 이 방식은 효과적이다고 주장하였다. 핀란드의 Niemi외 1인(U. of Vaasa)은 지금까지 제안된 전자 선거 방식에서 고려되지 않았던 "buying of votes"를 해결하는 방식을 제안하였다. 이 방식은 복잡도 측면에서는 크게 문제되지 않으나 현실적으로 실현되기 까지에는 문제가 있음을 저자 자신들도 인정하였다. 영국의 Boyd외 1인(U. of Manchester)은 기존의 키 분배 프로토콜로 TMN(Tatabayashi Matsuzaki Newman)의 방식과 Diffie-Hellman 키 분배 방식 등의 문제점을 개선하는 새로운 프로토콜을 논리 언어를 이용하여 제안하였다. 이탈리아의 Santis 외 2인(U. of Salerno)은 shared string model에서 계산량적 영지식 증명 방법을 정형화하였다.

3.3.5 인증과 디지털 서명(4편)

호주의 Safavi-Naini 외 1인(U. of Wollongong)은 인증 부호의 구성법으로 조합론에서 취급하는 t-design과 orthogonal array를 이용한 개념을 도입하고 Delsarte의 선형 계획법을 이용하여 인증 부호의 부호화 규칙 수를 밝혔다. 독일의 Horster외 2인(U. of Technonlogy)은 Meta-ElGamal signature 방식에 이용하여 Meta-Message recovery 방식을 일반화하였

고, Meta-blind signature 방식을 제안하였다. 사우디아라비아의 Alabbadi 외 1인(KACST)은 McEliece의 디지털 서명 방식과 유사하게 선형 에라 정정 블럭 부호를 사용한 trapdoor를 갖는 디지털 서명 방식을 제안하였으나 이미 전날 개최된 Rump Session에서 해독되었다. 프랑스의 Beguin(Ecole Normale Supérieure)외 1인은 insecure server를 이용하여 암호 프로토콜을 구성하는 방안을 제시하였다.

3.3.6 암호 해독(3편)

미국의 Atkin(MIT)외 3인은 129자리 합성수를 전세계적으로 운용되고 있는 Internet를 통해 1,600개의 컴퓨터와 600명의 도움을 받아 소인수 분해에 성공한 상세 경과를 제시하였다. 그들이 사용한 S/W를 가지고 RSA 512비트 키를 해독하는데는 수백만불과 몇 주만에 해독이 가능하다고 주장하였다. 이스라엘의 Biham(Technion)은 블럭 암호를 다중으로 사용하는 경우 각 운영 모드에 대해 분석한 결과를 제시하였다. 대부분의 복합 3중 모드 운영 방식은 단일 운영 모드(ECB)로 복수 사용하는 방식보다 안전성이 취약하다고 주장하였다. 일본의 Tokita외 2인(Mitsubishi)은 현재 널리 알려진 DES를 비롯한 호주의 Seberry외 2인이 제안한 LOKI89 및 LOKI91과 저자가 Asiacrypt'91에서 제안한 s^2DES 블럭 암호시스템의 DC(Differential Cryptanalysis)와 LC(Linear Cryptanalysis)에 대한 강도를 조사 분석하였다. DC와 LC에 대한 강도 탐색 알고리즘을 제안하고 그 결과 DC에 대한 강도 순위는 s^2DES 〈 DES 〈 LOKI89 〈 LOKI91이나 LC에 대한 강도는 DES 〈 s^2DES 〈 LOKI91 〈 LOKI89임을 제시하였다.

3.3.7 해쉬 함수(2편)

프랑스의 Patarin은 Damgard에 의해서 제안된 해쉬 함수가 LLL 알고리즘을 이용하여 해독 가능하기 때문에 이를 방지하기 위해서 두 함수를 혼합 사용하여 공격에 안전하도록하는 방식을 제안하였다. 호주의 Charnes외 1인은 Tillich외 1인이 Crypto'94에서 제안한 SL_2 해쉬 함수를 해독하였다. SL_2는 속도가 빠르고 입력의 작은 변화도 검출된다는 장점을 가지고 있으나 대수학의 군론을 이용하여 출력값이 충돌하는 서로 다른 작은 길이의 이진 수열을 찾아내었다.

3.3.8 키 분배 방식(2편)

일본의 Kurosawa(동경공업대)외 2인은 부정한 b명의 사용자에 대비하고 t명의 비빌 공유 방식을 갖는 b-secure 하고 t-group의 키 분배 방식을 제안하였다. 일본의 Matsumoto(요꼬하마 국립대)는 그래프 이론에서 널리 활용되는 incidence 구조를 유한 투영 공간 상으로 변환하여 키 공유 방식을 제안하였다.

3.3.9 공개 키 암호(2편)

뉴질랜드의 Smith외 1인은 모듈러 멱승 대신에 최근 새로운 공개키 방식의 구성 함수로 각광받는 Lucas 함수를 이용하여 디지털 서명 방식에 활용하는 방안을 제안하였다. 일본의 Abe외 1인(NTT)은 소형 무선 전화기나 스마트 카드와 같이 제한된 H/W 자원에 적합한 모듈러 곱셈 알고리즘과 LSI 구조를 제안하고 제작한 LSI 칩은 17MHz 동작 주파수에 512비트 모듈러 곱셈을 0.1초 이내에 처리할 수 있다고 하였다. 일본의 Kurosawa(동경 공업대)외 1인은 지수가 작은 값을 사용한 RSA 암호시스템이 쉽게 해독이 되듯이 타원곡선을 이용한 RSA형 암호 시스템에서도 지수가 작으면 해독될 수 있음을 주장하였다. 또한, Koyama외 3인이 Crypto'91에서 제안한 방식은 $e = 5$, $n \geq 2^{1024}$, 수신자의 수가 428일 때 해독되며, Demytko가 Eurocrypt'93에서

제안한 방식은 $e = 2$, $n \geq 2^{175}$, 수신자의 수가 11일 때, 해독됨을 제시하였다.

3.3.10 블럭 암호 알고리즘(2편)

호주의 O'Connor외 1인(QUT)은 Markov chain을 이용한 DES-like 암호의 안전성 분석 방법으로 DC에 중요한 Differential의 확률을 정형화하고 DES의 경우 균일 분포를 가짐을 증명하였다. 마찬가지로 LC의 경우에도 대부분의 라운드 함수에 대하여 균일한 분포를 가짐을 보였다. 즉, 독립된 라운드 키를 사용할 경우 대부분의 product 암호는 충분한 라운드수만 보장하면 DC와 LC에 강할 수 있음을 보였다. 이스라엘의 Biham외 1인(Technion)에 의해 기존의 DES H/W를 그대로 이용하면서 DC와 LC 및 Improved Davies 공격에 강한 DES를 구성하는 방법을 제시하였다. 그들의 방법은 현재 시판되고 있는 DES 칩이 S-box를 사용자가 선택할 수 있는 구조로 되어있다는 데서 착안하여 key-dependent invariant S-box transformation이란 개념을 사용하였으며, 기존 DES의 S-box를 변형하여 키의 크기를 증가시킨 S-box를 제안하였다. 특히, 본인외 2인이 1993년에 제안한 s^3DES S-box를 이용하면 DC와 LC에 현재의 DES보다 안전성이 강화되고 Improved Davies 공격은 성립하지 않음을 보였다.

3.4 Rump Session

회의 2일째인 11월 29일 오후 6시 30분 부터 10시까지 Wollongong 대학의 Naini 교수의 사회로 다음과 같은 제목의 논문이 발표 시간 5분, 질의 2분 형식으로 각각 발표되었다.

1. On Sharing Secrets with Time, J.Seberry, A.P.Street
2. Unicity Distances, Trapdoors and Pseudorandomness, B.Colbert, L.Brown
3. Q-Deformed Quntaum Cryptography and a New Eavesdropping Strategy, J. Hruby
4. Blind Multi-signature Scheme Based on the Discrete Logarithm Problem, P.Horster, M.Michles, H.Peterson
5. Some Cryptographic Properties of Exponential Permutations and Boolean functions, X.Chang, Z.Dai, G.Gong
6. Testing for Independence between Subsets of Plaintext and Ciphertext Blocks, H.Gustafson, E.Dawson, J.Golic
7. DESV-1, G.Carter et. al.
8. The New Draft ISO Standard for Hash Functions Based on Modular Arithmetic, B.Preneel
9. Factoring: the DNA Solution, D.Beaver
10. Can you actually sign with error-correcting codes?, J.Stern
11. How to use the LUC Digital Signature Scheme as an Encryption scheme, N.Demytko
12. Cryptography-the Business Requirements, M.Ames
13. STRANDOM-A Cryptographically Strong Pseudorandom Number Generator Based on HAVAL, Y.Zheng

4. 맺는 말

- 90년과 92년에 개최된 Auscrypt는 Asiacrypt로 통합되어 향후 개최되지 않음.
- Asiacrypt'96을 한국에서 개최함을 저자가 회의 기간(11월29일 10시)중 공포함.
- Asiacrypt'98은 중국 과학원의 Dai 교수가 중국에서 개최 의지가 있음을 밝혔으며 일본의 Imai 교수로 부터는 대만이 Asiacrypt'98 개최 의지도 있음을 통보 받았음.
- 11월 29일 12시 15분 이후에는 오세아니아 주의 암호 학술 학회(ASIS: Australasian Society for Information Security)의 발기대회가 열려 근본적으로 참석자가 학회 결성에 대하여 찬동하였음.
- Asiacrypt'94의 특징으로는 General Chairman이 Wollongong 대학의 J. Seberry 교수가 여성인 점에 영향을 받아서인지 여성 암호학자(Naini 교수, Meadow 박사, Dai 박사 등)의 역할이 증대된 점과 참가자 수가 역대 IACR 후원 학술회의에 비해 비교적 적었다는 점.
- 또하나의 특징은 회의 Pre-Proceeding에 호주에서 개최한 2회의 Auscrypt를 포함하여 Asiacrypt'94를 4회째라고 명기된 점과 프로그램 위원회에 한국학자가 1명도 없었다는 점은 차기 개최국에 대한 배려가 전혀 없었음.
- Asiacrypt'96의 한국 개최를 국내외에 공표된 이상, 국내의 암호 기술 발전의 획기적인 전기를 마련함과 동시에 성공적인 회의 개최를 위하여 전회원의 적극적인 협력, 양질의 논문 발굴 및 발표, 국내외 홍보 활동 등이 요망되며 국내 정보 보호 기술 수준이 아시아 국가에서 확고한 위상을 확보하여야 할만 아니라 나아가 세계화를 위한 노력을 경주하여야 함.

부록 A Asiacrypt'94의 프로그램

November 28

8:00 - 9.00 Registration
9:00 - 9.15 Welcome, J. Seberry, J. Pieprzyk
9:15 - 10:15 Invited Speaker - T. Beth, European Institute for System Security, Multifeature Security through Homomorphic Encryption

10:15 - 10:45 Coffee Break

10:45 - 12:25 Secret Sharing
- M. Burmester, Y. Desmedt, and G. Di Crescenzo, Linear non-abelian sharing systems and their application to threshold cryptography
- K. Okada and K. Kurosawa, Lower bound on the size of shares of nonperfect secret sharing scheme
- W-A Jackson, K.M. Martin and C.M. O'Keefe, On sharing many secrets
- K. Kurosawa and K. Okada, Combinatorial interpretation of secret sharing schemes

12:05 - 2:00 Lunch

2:00 - 3:15 Stream Ciphers
- M.J. Mihaljevic, A correlation attack on the binary sequence generators with time-varying output function
- A. Fuster-Sabater and P. Caballero-Gil,

On the linear complexity of nonlinearly filtered PN-sequences
- J.D. Golic, Intrinsic statistical weakness of keystream generators

3:15 - 3:45 Coffee Break

3:45 - 5:00 Cryptographic Functions
- S. Chee, S. Lee, and K. Kim, Semi-bent functions
- J. Seberry, X-M. Zhang, and Y. Zheng, Structures of cryptographic functions with strong avalanche characteristics
- G-Z. Xiao and M-X. Zhang, Maximum correlation analysis of nonlinear combining functions

November 29

9:00 - 10:00 Invited speaker - Catherine Meadows, Naval Research Laboratory, USA, Formal Verification of Cryptographic Protocols: A Survey

10:00 - 10:30 Coffee Break

10:30 - 12:10 Protocols
- Y. Yacobi, Efficient electronic money
- V. Niemi and A. Renvall, How to prevent buying of votes in computer elections
- C. Boyd and W. Mao, Design and analysis of key exchange protocols via secure channel identification
- A. De Santis, T. Okamoto, and G. Persiano, Zero-knowledge proofs of computational power in the shared string model

Free Afternoon

6:30 - 10:00 Rump Session

November 30

9:00 - 10:00 Invited speaker - Hideki Imai, The University of Tokyo, Information security aspect of spread spectrum

10:00 - 10:30 Coffee Break

10:30 - 12:10 Authentication and Digital Signature
- R. Safavi-Naini and L. Tombak, Combinatorial structure of A-codes with r-fold security
- P. Horster, H. Petersen, and M. Michels, Meta message recovery and Meta blind signature schemes based on the discrete logarithm problem and their applications
- M.M. Alabbadi and S.B. Wicker, A digital signature scheme based on linear error-correcting block codes
- P. Beguin and J-J. Quisquater, Secure acceleration of DSS signatures using insecure server

12:10 - 2:00 Lunch Break

2:00 - 3:15 Cryptanalysis
- D. Atkins, M. Graff, A.K. Lenstra, and P.C. Leyland, The magic words are squeamish ossifrage
- E. Biham, Cryptanalysis of multiple modes of operation
- T. Tokita, T. Sorimachi, and M. Matsui, Linear cryptanalysis of LOKI and s2DES

3:15 - 3:45 Coffee Break

3:45 - 4:35 Hash Functions
- Jacques Patarin, Collisions and inversions for Damgard's whole hash function
- C. Charnes and J. Pieprzyk, Attacking the SL2 hashing scheme

4:35 - 5:25 Key Distribution
- K. Kurosawa, K. Okada, and K. Sakano, Security of the center in key distribution scheme
- T. Matsumoto, Incidence Structures for Key Sharing

December 1

9:00 - 10:15 Public Key Cryptography
- P. Smith and C. Skinner, A public-key cryptosystem and a digital signature system based on the Lucas function
- M. Abe and H. Morita, Higher radix nonrestoring modular multiplication algorithm and public-key LSI architecture
- K. Kurosawa, K. Okada, and S. Tsujii, Low exponent attack against elliptic curve RSA

10:15 -10:45 Coffee Break

10:45 - 11:35 Block Cipher Algorithms
- L. O'Connor and J.D. Golic, A Unified Markov Approach to Differential and Linear Cryptanalysis
- E. Biham and A. Biryukov, How to strengthen DES using existing hardware

부록 B 각종 위원회 구성

General Chair:
Jennifer Seberry
Department of Computer Science
U. of Wollongong
NSW 2522, Australia
Phone: +61 42 214327
Fax: +61 42 214329
e-mail: jennie@cs.uow.edu.au

Organizing Committee
Margot Hall (U. of Wollongong, Australia)
Mark Arnold (U. of Wollongong, Australia)
Ghulam Chaudhry (U. of Wollongong, Australia)
Ahmad Dastjerdi (U. of Wollongong, Australia)
Nitin Devikar (U. of Wollongong, Australia)
Mansour Esmaili (U. of Wollongong, Astralia)
Bill Forsyth (U. of Wollongong, Australia)
Hossein Ghodosi (U. of Wollongong, Australia)
Shahram Lang (U. of Wollongong, Australia)
Justin Lister (U. of Wollongong, Australia)
Anish Mathuria (U. of Wollongong, Australia)
Viswanathan Narain (U. of Wollongong, Australia)
Colin Spargo (U. of Wollongong, Australia)

Program Chair:
Josef Pieprzyk
Department of Computer Science
U. of Wollongong
NSW 2522, Australia
Phone: +61 42 213872
Fax: +61 42 214329
e-mail: josef@cs.uow.edu.au

Program Committee:
D. Beaver (Pennsylvania State Univ., USA),
E. Biham (Technion, Israel),
C. Chang (Chung Cheng Univ., Taiwan),
Z. Dai (Academia Sinica, PROC),
Y. Desmedt (U.of Wisconsin, USA),
T. Itoh (Tokyo Institute of Technology, Japan),
T. Matsumoto (Yokohama National Univ., Japan),
A. Odlyzko (AT&T Bell Laboratories, USA),
T. Okamoto (NTT, Japan),
B. Preneel (Katholieke Universiteit Leuven, Belgium),
R. Rueppel (R3, Switzerland),
R. Safavi-Naini (U. of Wollongong, Australia),
Y. Zheng (U. of Wollongong, Australia).

□ 著者紹介

김 광 조(종신회원)

1973년 ~ 1980년 연세대학교 전자공학과(학사)
1981년 ~ 1983년 연세대학교 대학원 전자공학과(석사)
1988년 ~ 1991년 요꼬하마 국립대학 대학원 전자정보공학과(박사)
현 한국전자통신연구소 실장,
본 학회 암호이론연구회 및 ISO/IEC JTC1 JSC-27 의장,
KIISC, IEICE, IEEE, IACR 각 회원

※ 주관심 분야 : 암호학 및 응용 분야, M/W 통신