通信情報保護學會誌
第2卷, 第1號, 1992. 3

ASIACRYPT'91에서 본 암호학의 최근 연구 동향

On the Recent Research of Cryptology from ASIACRYPT'91

김 광 조*

요 약

본고는 1991년 11월 11일부터 11월 14일까지 일본의 후지요시다시에 위치한 Highland Resort 호텔에서 아시아권에서는 최초로 개최된 암호학 관련 국제 학술 대회인 ASIACRYPT'91에 참가하여 최근의 암호학 연구 동향을 조사한 내용이다.

1. 서 론

DES(Data Encryption Standard)가 1977년 미국의 연방정부 데이타 보호 표준알고리즘으로 채택된 이래 암호학의 연구는 특정인의 전유물에서 점차 학술적인 연구 분야로 각광을 받기 시작하였다. 이와 더불어 기존의 DES와 같은 재래식 암호 알고리즘에서 문제시 되었던 키분배 문제를 해결 할 수 있는 공개키 암호 방식을 Diffie와 Hellman이 IEEE 논문지에 발표하였다. 그이후 공개키 암호 방식으로 유명한 RSA 알고리즘이 발표되는 등 소인수 분해 문제와 같은 수학적으로 풀기 어렵다고 알려진 문제를 근거로 한 여러가지 암호 방식이 계속 발표되었다.

이에 1981년 8월 미국의 UCSB(Univ. of California, Santa Barbara)에서 암호학에 관심이 있는 몇몇 학자들이 모여 세계 최초로 CRYPTO'81이라는 암호학 관련 국제 학술 대회를 개최하였다. 그러나 공식적인 대회 논문집은 발행하지 못하였다. 이 대회에 자극을 받은 유럽 국가들은 다음해 서독의 Burg Feuerstein에서 EUROCRYPT'82을 개최하였다. 이 모임을 계기로 국제적인 암호학 연구의 전문 학회로서 국제 암호학 학회(IACR, International Association for Cryptologic Research)가 결성되기에 이르렀다. 그 후, IACR이 후원하여 매년 4~5월경에는 유럽 국가 중 한나라에서 EUROCRYPT'nn을, 미국의 UCSB에서 매년 8월경 CRYPTO'nn을 계속 개최하였다.

상대적으로 암호학 연구가 뒤늦게 시작된 호주에서도 1990년 1월 IACR의 후원을 받아 시드니의 NSW(New South Wales) 대학에서 AUSCRYPT'90을 개최하였다. 일련의 세계적인 암호학의 학술 활동은 아시아권에도 영향을 주어 1991년 11월 11일

* 한국전자 통신연구소

부터 11월 14일(3박 4일)까지 일본 후지요시다시내에 위치하고 후지산이 가깝게 보이는 Highland Resort 호텔에서 ASIACRYPT'91를 개최하기에 이르렀다. ASIACRYPT'91은 다른 국제학술 대회와 마찬가지로 IACR의 후원을 받았으며 일본의 전자정보 통신학회(IEICE, Institute of Electronics, Information and Communication Engineers) 산하 정보 시큐리티(ISEC, Information SECurity) 연구회가 중심이 되어 주최하였으며, 아시아권에서 암호학 관련 국제학술 대회가 최초로 개최되었다는 의미에서 우리들의 주목과 관심을 끌고 있다. 이 대회에는 일본, 미국, 호주, 한국(저자는 논문 발표차 참가) 등을 비롯하여 18개 국에서 182명이 참가하였으며, 39편의 심사 논문이 발표되었고 4편의 초청 강연이 있었다. 초청 강연에는 현재 한국정보통신 보호학회의 회장직을 역임하는 한양대학교의 이만영교수가 한국을 대표하여 "Research Activities on Cryptology in Korean"를 발표하였다(부록 A 참조). 표 1과 표 2에는 국가별 참가자수와 심사 논문발표수를 각각 정리 하였다.

표 1. 국가별 참가자 수

	국 명	인 원	비 고
1	일 본	114	62.6%
2	미 국	15	8.2%
3	호 주	9	
4	중 국	6	
5	프 랑 스	6	
6	한 국	5	2.7%
7	대 만	5	
8	노 르 웨 이	5	
9	스 웨 덴	3	
10	루 마 니 아	3	
11	벨 기 에	2	
12	독 일	2	
13	덴 마 크	2	
14	영 국	1	D. Davies
15	스 위 스	1	J. Massey
16	캐 나 다	1	
17	브 라 질	1	
18	남 아 프 리 카	1	
계		182	

표 2. 국가별 심사 논문 발표 수

국 명	편 수	비 고
일 본	11	
호 주	8	
미 국	6.5	
중 국	4	
덴 마 크	2	
벨 기 에	2	
한 국	1	
대 만	1	0.5+0.5
네 덜 란 드	1	대리발표
프 랑 스	1	
영 국	*1 0.5	
이 스 라 엘	0.5	대리발표
캐 나 다	0.5	
총	39	

*1. 국가가 다른 2명이 한 편의 논문을 발표하였을 때 한 국가에 0.5로 계산함.

본고에서는 ASIACRYPT'91에 발표된 39편의 연구 논문을 분류하여 주요 내용을 요약함으로서 암호학의 최근 연구 동향을 고찰하였으며 차기 국제학술 대회 일정을 조사하였고, 끝으로 결론을 맺었다.

2. 주요 연구 결과

전체 12개 session 중 4개의 초청 강연 session을 제외한 8개 session에 걸쳐 발표된 39편의 논문을 표 3과 같이 분류하였다.

분류 항목별 주요 연구결과는 다음과 같다.

표 3. 발표 논문의 종류

분 야	편 수
영지식 증명	10
DES-like 암호계	7
공개키 암호계	5
Hash 함수 및 디지틀 서명	5
비밀공유 및 인증코드	4
Differential Cryptanalysis	3
해독 및 기타	5
계	39

가. 영지식 증명(10편)

본 분야는 2개의 session에 걸쳐 총 10편의 논문이 발표되어 가장 많은 부분을 차지하였다.

L. Harn과 H. Y. Lin은 기존의 Oblivious Transfer (OT) 프로토콜을 비밀 교환을 위하여 검증 가능한 OT 프로토콜(Rabin과 Blum이 제안한 것과 유사한 방법임)을 제안하였다. 이 프로토콜의 특징은 공정성(Fairness), 검증 가능성(Verifiability), 안전성(Security)을 가지고 있고 이산대수 문제에 안전성의 근거로 두고 있다.

T. Saito와 K. Kurosawa는 어떠한 암호학적 가정 없이 지식에 대한 4 move의 완전한 영지식 대화형증명을 제안하였고 T. Itoh와 K. Sakurai는 지식을 갖고 있다는 것을 영지식 대화형 증명으로 증명할 때 일정한 라운드 방식의 복잡도에 대하여 논의하였다. L. Fortnow와 M. Szegedy는 1-bit oracle의 2-oracle Instance-Hiding 방식이 $NP_{poly} \cap$ co-NP_{poly}에 있는 언어에서만 구현될 수 있다는 것을 증명하였는데 본 결과는 Yao의 결과를 확장한 것이다. 이어서 J. Feigenbaum과 R. Ostrovsky는 Instance-Hiding 방식의 실현에 필요한 일방향 치환함수가 가져야 할 성질을 다음과 같이 제시하였다.

- 함수는 One-prover, Instance-Hiding 영지식 증명 시스템을 가진다.
- 함수는 PSPACE에서 계산 가능하고 최대로 입력 길이만큼 누설하는 Instance-Hiding 방식을 갖는다.

Y. Desmedt와 M. Burmester는 smooth number를 기초로 하여 이산대수 문제를 이용하여 적은 통신량을 갖는 intractable 영지식 증명 시스템을 제안하였다. T. Okamoto는 영지식 증명을 oracle-simulation 영지식 증명으로 확장하여 다양한 응용을 논하였다. T. Itoh외 2인은 IP에 존재하는 언어는 divertible 영지식 대화형 증명을 가질 수 있다는 것을 제시하였고 C. Shu외 2인은 한개의 비밀 정보로 identity와 membership을 분리 또는 동시에 증명할 수 있는 영지식 증명시스템을 제안하였다. 또한, M. J. Taussaint는 암호 프로토콜을 확률적 성질에 대하여 형식 검증법을 제시하였다.

나. DES-like 암호계(7편)

저자는 DES-like S-box의 발생 방법으로서 암호학적으로 중요한 의미를 갖는 SAC(Strict Avalanche Criterion) 조건을 만족하는 부울함수를 이용하여 효율적으로 DES-like S-box를 생성하는 방법을 제안하고 생성한 DES-like S-box와 현재 DES에서 사용되는 S-box와 비교한 결과 암호학적으로 우수한 성질을 갖고 있다는 것을 입증하였다.

중국의 Zeng-Duo Dai는 DES의 S-box 중 1개의 row를 구성하는 데 필요한 치환의 데이타베이스의 구성 방법에 대하여 제시하였다. 이는 17,433개의 데이타베이스로부터 총 $17,433 \times 3 \times 2^9$개의 암호학적 필요한 치환을 발생할 수 있다고 발표하였다.

M. Kwan과 J. Piepryzyk는 일반적으로 DES-like 암호계의 Key Schedule상에 나타나는 약점을 효율적으로 찾아 내는 방법을 제시하고 LOKI의 설계시 그 결과를 반영하였다. H. Morita외 2인은 NTT가 발표한 암호 알고리즘인 FEAL에 대하여 Switching-Closure-Test라고 하는 방법을 제안하여 FEAL의 주기적 성질을 검사하였다.

DES-like 치환 함수가 초(Super) 의사 랜덤 성질을 갖기 위한 필요 충분조건을 호주의 B. Sadeghiyan과 J. Piepryzyk가 제시하였는데, 한개의 랜덤

함수으로 4 라운드의 DES-like 치환 함수는 초 의사 랜덤 성질을 가질 수 없으며 Type-1 Feistel 변환에 의한 초 의사 랜덤 성질을 조사하고 이 변환이 k^2 라운드 이상인 경우라야만 초 의사 랜덤 성질을 가질 수 있다고 발표하였다. S.Even과 Y.Mansour는 랜덤하게 선택한 치환 P로 블럭 암호를 구성하는 방법을 제시하였는데, 키는 메세지와 XOR되는 키와 P의 출력을 XOR하는 키로 2 종류가 있으며 암호문은 랜덤하지는 않지만 다음 성질을 갖는다는 것을 증명하였다.

-만일 P를 랜덤하게 선택하면 이 암호는 어떠한 다항식 시간의 공격에 대하여도 안전하다.

-P를 의사 랜덤하게 선택하여도 암호 시스템은 안전하다.

또한, J.Pieprzyk과 B.Sadeghiyan은 Luby와 Rackoff가 제시한 랜덤 생성자(randomizer)를 몇개의 layer로 연결하였을 때 만들어진 랜덤 생성자의 성질을 조사 보고하였다. 주요 결과로는 변형된 Luby와 Rackoff의 랜덤 생성자를 2 layer로 구성하여도 완전 랜덤생성자가 만들어진다고 주장하였다.

다. 공개키 암호계(5편)

J.Brandt외 2인은 RSA 암호 방식 등에서 필요한 100자릿수 이상의 소수 발생법으로 확률적인 방법과 증명가능한 방법에 대하여 논하였다. 확률적인 소수 발생 방법으로 검증 나눗셈 및 2를 기저로 한 Rabin 테스트를 하여 지금까지의 확률적 소수 발생 방법의 신뢰도를 개선하였다. 증명 가능한 소수 발생법으로는 Mauer의 알고리즘을 확장하였으며 이어서 이 방법에 Gordon의 방법을 합쳐서 strong하고 증명가능한 소수 발생법을 제시하였다. 계산력이 약한 entity가 계산력이 상대적으로 강한 네트워크 상의 entity에 비밀을 노출하지 않고 어떤 주어진 계산 결과를 얻는 방법으로 의뢰 계산 프로토콜이 일본의 Matsumoto에 의해 제안된 바 있다. Chi-Sung Laih외 2인은 addition sequence를 이용하여 RSA암호의 디지틀 서명을 보다 빨리 계산하는 의뢰 계산 방법을 제안하였다.

A.Miyaji는 유한체 상에 타원 곡선상 이산대수 문제가 통상의 이산대수 문제로 환원되지 않는 ordinary 타원 곡선을 이용한 암호계에 대한 성질 및 구체적인 예를 제시하였다. A.Joux외 1인은 EUROCRYPT'90에서 Niemi가 발표한 modular knapsack 암호계를 LLL 알고리즘을 이용하여 해독 방법을 제시하였고 Da-xing Li는 NTT의 Okamoto가 제안한 공개키 암호계를 연분수 전개 방식을 이용하여 해독방법을 제시하였다.

라. Hash 함수 및 디지틀 서명(5편)

J.Daemen외 3인은 CRYPTO'89에서 Damgard가 제안한 3가지의 hash 함수 중 2가지는 쉽게 충돌하는 입력 쌍을 찾을수 있으며 나머지 한가지는 공격 가능한 것을 보여주었다. 아울러 충돌이 없는 (collision-free) hash 함수를 설계하는 구체적인 예로 cellhash라고 하는 개념을 새롭게 주장하였다.

B.Sadeghiyan외 2인은 동시에 최대의 hard bits를 갖는 일 방향 치환 함수 m는 세가지 함수의 합성에 의해 만들어진다고 주장하였다. 즉, $m=fogoh$ 으로 f는 임의의 일방향 치환, g는 GF상의 strongly universal$_2$ family of polynomial의 집합에서 랜덤하게 선택한 함수, h는 숨겨진 (hidden) 치환이다. 또한, 이 m는 의사 랜덤수의 발생기와 일방향 hash 함수를 만드는 도구로서 사용된다. W.Ogata와 K.Kurosawa는 "On claw free families"라는 논문에서 claw-free family가 될 충분조건을 제시하였다. Y.Zheng은 Sibling Intractable Function Families (SIFF)라는 새로운 암호 함수를 제안하였는데, 이 함수는 서로 충돌하는 초기값의 집합이 주어졌을 때 초기값와 충돌하는 새로운 값을 구하는 것이 계산상 불가능한 함수의 집합으로 계층적 구조를 갖는 시스템의 악세스 제어, mailbox의 공유 문제, 분산 시스템의 악세스 제어, 다중 메세지 인증에 응용할 수 있다고 주장하였다.

K. Ohta와 T. Okamoto는 Fiat-Shamir 방식을 이용하여 디지틀 다중 서명방식을 제안하였는데, 순차적인 (sequential) 다중 서명방법으로 다음 성질을 증명하였다.

－이미 사용된 다중 서명 방식의 공개정보로 부터 비밀정보를 추출하는 어려움은 단일 서명방식에서 비밀정보를 구하는 어려움과 동일하다.

－부분적인 다중 서명방법을 위조하는 어려움은 Fiat-Shamir 방식을 위조하는 것과 동일하다.

그러나, 본 방식의 문제점으로

－active attack에 대한 안전성

－동시 다중 디지탈 서명의 안전성

－만일 중계소(bridge)가 존재하지 않는다면 단일 서명방식을 여러번 사용하는 것과 동일한 통신량을 갖는 순차적인 다중 서명방식은 존재하는가?

를 제시하였다.

마. 비밀 공유 및 인증 코드(4편)

Hwang-Yu Lin외 1인은 비밀 공유 방식을 일반화하여 새로운 비밀 공유 방식을 제안하였다. 어떠한 정직한 구성원은 다른 전부의 구성원이 결탁하여도 누가 속이는지를 찾아낼 수 있으며, 계산상 안전하다는 것을 제시하였다. 본 방식은 (x, x) homomorphism 성질을 이용하였으며 shadow를 동시에 보여주지 않는다 하더라도 정직하지 않는 구성원으로 부터 비밀을 보호할 수 있는 방식으로 확장하였다. 또한, 그들은 threshold cryptosystem을 일반화하여 서로 신뢰할 수 있는 그룹과 서로 신뢰하지 않는 그룹간에 비밀공유가 가능한 방법도 제안하였다.

R. Safavi-Naini는 Luby와 Rackoff가 제안한 의사 랜덤 치환 발생기를 역함수 발생기로 일반화하고 만일 일반화한 의사 랜덤 함수 발생기가 존재하면 그 역함수도 존재한다는 것을 제시하였다. 이것을 의사 랜덤 인증 코드에 사용하여 t-fold chosen plaintext/ciphertext attack에 대한 안전성을 증명하였고 t차의 strong spoofing에 대하여도 안전하다는 것을 보여주었다. 발표자(Zhe-Xian Wan)가 경제적인 이유로 불참한 연구결과로 인증코드의 구성을 위하여 unitary geometry를 사용하는 방안도 제안되었다.

바. Differential Cryptanalysis(3편)

1990년 호주에서 설계한 64 비트 블럭 암호 알고리즘인 LOKI에 대하여 본 회의에서 덴마크의 L. Knudson가 해독 방법을 제시하여 참가자의 비상한 관심을 모았다.

Knudson에 의한 LOKI의 주요 해독 결과는

－LOKI의 키사이즈는 2^{64}가 아니라 2^{60}이다. 즉, 각 키에 대하여 15개의 등가 키가 존재한다. 이것은 LOKI의 Key Schedule 방식에서 기인한 것이다.

－따라서, 제안한 single-block hash 함수는 충돌을 쉽게 찾을 수 있어 암호학적으로 좋지 않다.

－적어도 원리상 14라운드의 LOKI는 Differential Cryptanalysis가 가능하며 Private Version의 LOKI는 16라운드의 경우라도 Differential Cryptanalysis가 가능하다.

위의 해독 결과에 따라 L. Brown외 3인은 LOKI을 재설계하여 (LOKI91 라고함) 발표하였다. 주요 변경 사항은

－Key Schedule 중 반분된 입력을 매 2라운드 마다 swapping 되도록 변경

－Key Rotation Schedule 중 circularly rotation 함수인 Rot_{13}와 Rot_{12}를 교대로 사용

－1 라운드 전과 마지막 라운드 후에 평문과 라운드 키와의 XOR 부분삭제

－12 bit 입력에 8 bit 출력 함수인 S-box를 다음과 같이 변경

$S(r, c) = (c + ((r \times 17) \oplus ff_{16}) \ \& \ ff_{16})^{31} \bmod g_r$

여기서, r과 c는 4 bit와 8 bit 입력을 의미하며, +, ×는 산술적 덧셈과 곱셈, ⊕는 XOR, 멱승은 $GF(2^8)$ 상에서 연산을 행하며, g_r는 원래의 원시 다항식이다. 위의 수식은 시행 착오적으로 찾아내었다고 한다.

이와 같이 한 결과, LOKI91의 개선점으로

-한 빗트의 보수(complementary) 효과로 실효 키 공간은 2^{63}임

-4 Weak 키와 12 Semi-weak 키가 존재

-10 라운드까지 2 라운드특성 ($f(\dot{x})->0$)를 이용 Pr(122/1048576)이 되고 12 라운드까지 $f(\dot{x})=\dot{x}$인 3 라운드 특성을 이용하면 Pr(16/4096)이 생기나 그 이상의 라운드에서는 Differential Cryptanalysis 적용이 곤란하다고 발표하였다.

또한, NEC의 H. Miyano는 Differential Cryptanalysis를 DES-like 암호계에 적용하기 위하여 각 라운드별 해독에 얼마나 많은 암호문 쌍이 필요한가와 효과적인 counting 방식에 대하여 제안하였다. 아울러, 실제로 8 라운드의 DES를 예를 들어 실험적 결과도 제시하였다.

사. 해독 및 기타(5편)

도시바의 A. Shimbo와 S. Kawamura는 EUROCRYPT'88에서 Koyama와 Ohta가 제안한 성형구조와 완전 그래프상의 회의용 키 분배방식과 Globecom'90에서 발표한 Chikazawa와 Inoue가 제안한 회의용 키 분배방식의 해독 방식을 제안하고 그 개선책을 발표하였다. A. Klapper와 M. Goresky는 부분적으로 주기적인 상관관계가 있는 수열의 통계적 공격 방법을 위하여 기하학적인 수열을 이용한 방안을 제안하였다. Liu Xian과 Xiao Guozhen은 스트림 암호에서 널리 이용되고 있는 클럭 제어 수열의 해독 방법을 제안하였다. J. Meijers와 J. Tilburg는 다수결 방법의 확장과 비밀키 방식의 대수학적 코드를 이용한 암호계에 대하여 논하였고, B. Goldburg와 2인은 암호학의 응용연구로서 이산 코사인 변환을 이용한 아나로그 음성 스크램블러에 관하여 제안하였다.

이상과 같이 ASIACRYPT'91에서 발표된 주요 연구결과를 요약하였다. 지면관계로 상세히는 기술하지 못하였으므로 관심있는 독자는 회의 논문집을 참조바랍니다.

3. 차기 암호학 관련 국제학술대회

전술한 바와 같이 IACR이 후원하여 매년 유럽과 미국에서 차기 EUROCRYPT 및 CRYPTO가 표 4와 같이 개최되며 AUSCRYPT는 90년도에 이어 2년 후인 AUSCRYPT'92의 개최가 확정되어 있다.

표 4. 차기 국제 학술대회 일정

회 의 명	장 소	일 시	논문마감
EUROCRYPT'92	헝거리	1992. 5. 24~5. 28	1992. 1. 15
CRYPTO'92	UCSB, 미국	1992. 8. 16~20	1992. 4. 27
AUSCRYPT'92	Somerset College, 호주	1992. 12. 14~17	
EUROCRYPT'93	노르웨이	1993. 5. 24	
ASIACRYPT'nn	?	?	

4. 결 론

현대 암호학의 연구는 수학, 전자 계산기학, 물리학 등을 전공한 연구자의 이론적 연구와 전자, 전산, 정보 공학 등을 전공한 연구자의 응용적 연구로 분류할 수 있다. 이것은 최근의 첨단 학문 분야의 연구에 유사하게 발생하는 현상으로 암호학의 연구도 복잡 다양한 연구 배경을 갖는 전문 인력이 필요하다고 생각된다.

103편의 신청 논문 중 39편만이 ASIACRYPT'91에 발표된 논문에는 암호학의 이론 연구분야 중 새로운 결과나 향상시킨 논문이 태반이며 암호학의 응용연구에 관한 논문은 다소 적은감이 있다. 그러나, 회의기간 중 NTT를 비롯한 9개의 전기통신 업체가 참가한 암호학을 응용한 제품 전시는 지금까지의 국제학술대회 중 가장 많았다. 이는 일본인

특유의 상술에서 기인하지 않았나 생각된다. 또한, ASIACRYPT'91을 일본에서 최초로 개최함으로해서 그들은 아시권에서 암호학의 중심은 일본이라고 자만하고 있는 듯하다.

우리나라도 학문의 국제화 경향에 적극 대처하는 우리 모두의 노력이 필요하며, 1990년에 태동한 한국정보통신보호학회(KIISC)를 중심으로 관·학·연·산이 공동으로 암호학 연구의 조속한 발전이 요구된다. 또한, 한일간 국제 공동연구의 일환으로 KIISC와 ISEC 연구회의 공동 학술 발표회의 개최 등을 통하여 연구자의 발표 능력 향상과 국제적 연구동향의 조속한 파악이 필요하리라 생각되며, 끝으로 국내에서도 ASIACRYPT가 개최할 수 있는 날을 기대하여 본다.

부록 A. ASIACRYPT'91 프로그램

Monday, November 11, 1991

Session 1: Invited Lecture 1
— Chair: Ronald L. Rivest (Massachusetts Institute of Technology, U.S.A.)

09:00 - 09:50 *The Transition from Mechanisms to Electronic Computers, 1940 to 1950*,
Donald W. Davies (U.K.)

09:50 - 10:10 Coffee Break

Session 2: Differential Cryptanalysis and DES-like Cryptosystems
— Chair: Ronald L. Rivest (Massachusetts Institute of Technology, U.S.A.)

10:10 - 10:35 *Cryptanalysis of LOKI*,
Lars Ramkilde Knudsen (Aarhus Universitet, Denmark)
10:35 - 11:00 *Improving Resistance to Differential Cryptanalysis and the Redesign of LOKI*,
Lawrence Brown, Matthew Kwan, Josef Pieprzyk, and Jennifer Seberry
(University of New South Wales, Australia)
11:00 - 11:25 *A Method to Estimate the Number of Ciphertext Pairs for Differential Cryptanalysis*,
Hiroshi Miyano (NEC Corporation, Japan)
11:25 - 11:50 *Construction of DES-like S-boxes Based on Boolean Functions Satisfying the SAC*,
Kwangjo Kim (Electronics and Telecommunications Research Institute, Korea)
11:50 - 12:15 *The Data Base of Selected Permutations*,
Jun-Hui Yang, Zong-Duo Dai, and Ken-Cheng Zeng (Academia Sinica, P.R.O.C.)

12:15 - 13:30 Lunch

Session 3: Hashing and Signature Schemes
— Chair: Shimon Even (Technion, Israel)

13:30 - 13:55 *A Framework for the Design of One-Way Hash Functions Including Cryptanalysis of Damgård's One-Way Function Based on a Cellular Automaton*,
Joan Daemen, René Govaerts, and Joos Vandewalle
(Katholieke Universiteit Leuven, Belgium)
13:55 - 14:20 *How to Construct a Family of Strong One Way Permutations*,
Babak Sadeghiyan, Yuliang Zheng, and Josef Pieprzyk
(University of New South Wales, Australia)
14:20 - 14:45 *On Claw Free Families*,
Wakaha Ogata and Kaoru Kurosawa (Tokyo Institute of Technology, Japan)
14:45 - 15:10 *Sibiling Intractable Function Families and Their Applications*,
Yuliang Zheng, Thomas Hardjono, and Josef Pieprzyk
(University of New South Wales, Australia)
15:10 - 15:35 *A Digital Multisignature Scheme Based on Fiat-Shamir Scheme*,
Kazuo Ohta and Tatsuaki Okamoto (NTT Corporation, Japan)

15:35 - 15:55 Coffee Break

Session 4: Secret Sharing, Threshold, and Authentication Codes
— Chair: Chin-Chen Chang (National Chung Cheng University, R.O.C.)

15:55 - 16:20 *A Generalized Secret Sharing Scheme with Cheater Detection*,
Hung-Yu Lin and Lein Harn (University of Missouri - Kansas City, U.S.A.)
16:20 - 16:45 *Generalized Threshold Cryptosystems*,
Chi-Sung Laih (National Cheng Kung University, R.O.C.) and
Lein Harn (University of Missouri - Kansas City, U.S.A.)
16:45 - 17:10 *Feistel Type Authentication Codes*,
Reihaneh Safavi-Naini (University of New England, Australia)
17:10 - 17:35 *Application of Unitary Geometry to the Construction of Authentication Codes*,
Zhe-xian Wan (Academia Sinica, P.R.O.C.)

Tuesday, November 12, 1991

Session 5: Invited Lecture 2
— Chair: Sang-Jae Moon (Kyung Pook National University, Korea)

09:00 - 09:50 *Research Activities on Cryptology in Korea*,
Man Y. Rhee (Hanyang University, Korea)

09:50 - 10:10 Coffee Break

Session 6: Block Ciphers — Foundations and Analysis
— Chair: James L. Massey (ETH Zürich, Switzerland)

10:10 - 10:35 *On Necessary and Sufficient Conditions for the Construction of Super Pseudorandom Permutations*,
Babak Sadeghiyan and Josef Pieprzyk (University of New South Wales, Australia)

10:35 - 11:00 *A Construction of a Cipher from a Single Pseudorandom Permutation*,
Shimon Even (Technion, Israel) and Yishay Mansour (Harvard University, U.S.A.)
11:00 - 11:25 *Optimal Perfect Randomizers*,
Josef Pieprzyk and Babak Sadeghiyan (University of New South Wales, Australia)
11:25 - 11:50 *A General Purpose Technique for Locating Key Scheduling Weaknesses in DES-like Cryptosystems*,
Matthew Kwan and Josef Pieprzyk (University of New South Wales, Australia)
11:50 - 12:15 *Results of Switching-Closure-Test on FEAL*,
Hikaru Morita, Kazuo Ohta, and Shoji Miyaguchi (NTT Corporation, Japan)

12:15 - 17:45 Lunch and Excursion (option)
18:00 - 20:00 Banquet

Wednesday, November 13, 1991

Session 7: Invited Lecture 3
— Chair: Ken-Cheng Zeng (Academia Sinica, P.R.O.C.)

09:00 - 09:50 *IC-Cards and Telecommunication Services*,
Jun-ichi Mizusawa (University of Tokyo, Japan)

09:50 - 10:10 Coffee Break

Session 8: Cryptanalysis and New Ciphers
— Chair: Ingemar Ingemarsson (Linköping University, Sweden)

10:10 - 10:35 *Cryptanalysis of Several Conference Key Distribution Schemes*,
Atsushi Shimbo and Shin-ichi Kawamura (Toshiba Corporation, Japan)
10:35 - 11:00 *Revealing Information with Partial Period Correlations*,
Andrew Klapper (University of Manitoba, Canada) and
Mark Goresky (Northeastern University, U.S.A.)
11:00 - 11:25 *Analysis of* $[k_0, k_1]$ *Clock-Controlled Sequences*,
Xian Liu (Xidian University, P.R.O.C.)
11:25 - 11:50 *Extended Majority Voting and Private-Key Algebraic-Code Encryptions*,
Joost Meijers (Eindhoven University of Technology, the Netherlands) and
Johan van Tilburg (PTT Research, the Netherlands)
11:50 - 12:15 *A Secure Analog Speech Scrambler Using the Discrete Cosine Transform*,
B. Goldburg, E. Dawson, and S. Sridharan
(Queensland University of Technology, Australia)

12:15 - 13:30 Lunch

Session 9: Proof Systems and Interactive Protocols 1
— Chair: Yvo G. Desmedt (University of Wisconsin - Milwaukee, U.S.A.)

13:30 - 13:55 *An Oblivious Transfer Protocol and Its Application for the Exchange of Secrets*,
Lein Harn and Hung-Yu Lin (University of Missouri - Kansas City, U.S.A.)

13:55 - 14:20 *4-Move Perfect ZKIP of Knowledge with No Assumption*,
Takeshi Saito and Kaoru Kurosawa (Tokyo Institute of Technology, Japan)
14:20 - 14:45 *On the Complexity of Constant Round ZKIP of Possession of Information*,
Toshiya Itoh (Tokyo Institute of Technology, Japan) and
Kouichi Sakurai (Mitsubishi Electric Corporation, Japan)
14:45 - 15:10 *On the Power of Two-Oracle Instance Hiding Schemes*,
Lance Fortnow and Mario Szegedy (University of Chicago, U.S.A.)
15:10 - 15:35 *A Note on One-Prover, Instance-Hiding Zero-Knowledge Proof Systems*,
Joan Feigenbaum (AT& T Bell Laboratories, U.S.A.) and
Rafail Ostrovsky (Massachusetts Institute of Technology, U.S.A.)

15:35 - 15:55 Coffee Break

Session 10: **Proof Systems and Interactive Protocols 2**
— Chair: **Eiji Okamoto** (NEC Corporation, Japan)

15:55 - 16:20 *An Efficient Zero-Knowledge Scheme for the Discrete Logarithm Based on Smooth Numbers*,
Yvo Desmedt (University of Wisconsin - Milwaukee, U.S.A.) and
Mike Burmester (RHBNC - University of London, U.K.)
16:20 - 16:45 *An Extension of Zero-Knowledge Proofs and Its Applications*,
Tatsuaki Okamoto (NTT Corporation, Japan)
16:45 - 17:10 *Any Language in IP has a Divertible ZKIP*,
Toshiya Itoh (Tokyo Institute of Technology, Japan),
Koichi Sakurai (Mitsubishi Electric Corporation, Japan), and
Hiroki Shizuya (Tohoku University, Japan and Université de Montréal, Canada)
17:10 - 17:35 *A Multi-Purpose Proof System*,
Chaosheng Shu, Tsutomu Matsumoto, and Hideki Imai
(Yokohama National University, Japan)
17:35 - 18:00 *Formal Verification of Probabilistic Properties in Cryptographic Protocols*,
Marie-Jeanne Toussaint (Université de Liège, Belgium)

Rump Session
— Chairs: **Thomas A. Berson** (Anagram Laboratories, U.S.A.) and **Kenji Koyama** (NTT Corporation, Japan)
19:30 - ?

Thursday, November 14, 1991

Session 11: **Invited Lecture 4**
— Chair: **Hideki Imai** (Yokohama National University, Japan)

09:00 - 09:50 *Computational Learning Theory and Cryptography*,
Ronald L. Rivest (Massachusetts Institute of Technology, U.S.A.)

09:50 - 10:10 Coffee Break

Session 12: Public-Key Ciphers — Foundations and Analysis
— Chair: Tsutomu Matsumoto (Yokohama National University, Japan)

10:10 - 10:35 *Speeding Up Prime Number Generation*,
Jørgen Brandt, Ivan Damgård, and Peter Landrock (Aarhus Universitet, Denmark)
10:35 - 11:00 *Two Efficient Server-Aided Secret Computation Protocols Based on the Addition Sequence*,
Chi-Sung Laih, Sung-Ming Yen (National Cheng Kung University, R.O.C.), and Lein Harn (University of Missouri - Kansas City, U.S.A.)
11:00 - 11:25 *On Ordinary Elliptic Curve Cryptosystems*,
Atsuko Miyaji (Matsushita Electric Industrial Corporation, Japan)
11:25 - 11:50 *Cryptanalysis of Another Knapsack Cryptosystem*,
Antoine Joux and Jacques Stern (Ecole Normale Superoeure, France)
11:50 - 12:15 *How to Break Okamoto's Cryptosystems by Continued Fraction Algorithm*,
Da-xing Li (Shandong University, P.R.O.C.)

12:15 Adjourn

□ 著者紹介

金 光 兆(正會員)

本 學會「論文誌」創刊號 參照