通信情報保護學會誌
第8卷 第1號, 1998. 3

일본의 정보보호기술 최근연구동향 -SCIS'98 참가 결과-

김 광 조*

요 약

본고는 1998년 1월 28일부터 1월 31일까지 일본의 Hamanako Royal 호텔(시즈오가현 야마 나시시 소재)에서 일본의 전자정보통신학회(IEICE) 산하 정보시큐리티 연구회가 14번째로 주관한 SCIS'98(1998 Symposium on Crytography and Information Security)에 참관하여 일본의 정보보호 관련 최신 연구 결과를 요약 보고한다. 특히, 금년에는 암호해석, Digital Watermark, 타원 곡선 암호와 관련된 논문이 많았으며, 발표 논문에 대한 사전 심사가 없음에도 불구하고 논문의 질이 높은 연구 결과도 많았다.

I. 서 론

1998년 1월 28일부터 1월 31일까지 Hamanako Royal 호텔 (시즈오까현 하마마쯔시 소재)에서 일본 전자정보통신학회 산하 정보시큐리티 연구회가 매년 주관하는 SCIS'98 (1998 Symposium on Cryptography and Information Security)에 참가하여 일본의 정보보호 기술의 최근 연구 동향를 소개한다.

본 심포지움은 14번째로 일본 내의 지난 1년간에 연구한 학자들이 모여 최근의 연구 결과를 발표하므로 일본의 최근 연구 동향을 파악하는 데 도움이 될 수 있으며, 365명 참가하여 149건의 논문발표가 있었다. ('96년:75건/224명, '97년:131건/300명)

* 한국정보통신대학원 정보공학부, 종신회원

특히, 회의 기간 중 NTT가 Digital Watermark 시스템, NEC가 전자 추첨 서버, 미쓰비시 전기가 'Time-Memory-Trade-Off 방식 구현, 마쓰시다가 crypto library에 관한 전시회도 있었으며 컴퓨터 시큐리티 연구회가 금년도 새롭게 발족하여 년 4회 연구회과 1회 심포지엄을 계획하고 있다고 하였다. 한국인으로는 유학생을 제외하고 부산 부경 대학의 박 지환 교수와 한국 전력의 이 상기 부장의 논문 발표가 있었다.

II. 프로그램 편성

3박 4일간의 프로그램은 〈표 1〉과 같이 편성되었으며 첫째 날은 Tutorial 성격과 최근 기술 보고에 관한 내용이었으며 이 후, 3개의 병렬 Session으로 진행되었다. 특히, 블록 암호의 암호 해독과 타원 곡선 암호와 국내에서는

아직 활발히 연구되지 않는 Digital Watermark에 관한 논문이 많았으며, 발표 논문의 사전 심사가 없었음에도 불구하고 논문의 질도 상당히 높은 결과도 많이 있었다.

〈표 1〉 SCIS'98 프로그램 편성

1.28.(수)			
14:00-14:10	Opening Remark		
14:10-14:50	특별강연(1) 인터넷에 있어서 시큐리티 문제와 JPCERT/CC		
14:50-15:30	특별강연(2) 인증국의 실용화 실험에 대하여		
15:50-16:50	특별강연(3) 의료정보의 시큐리티 요건의 개요와 다단계인증 시스템		
17:40	Cocktail Party		
1.29.(목)	Room 1	Room 2	Room 3
8:30-10:10	1.1 계산법/정수론 응용	1.2 암호해석(I)	1.3 프로토콜
10:30-12:10	2.1암호방식제안/암호고속화	2.2 암호해석(II)	2.3 ID-based 키분배
13:30-15:30	3.1 전자 현금	3.2 Digital Watermark(I)	3.3 인증서버와 익명통신
15:50-17:30	4.1 타원암호(I)	4.2 암호해석(III)	4.3 접근제어
19:00-21:00	Banquet		
1.30.(금)			
8:30-10:30	5.1 난수생성	5.2 키위탁/분배/복원	5.3 비밀분산
10:50-12:10	6.1 정수론응용	6.2 암호해석(IV)	6.3 암호이론기초
13:30-15:10	7.1 타원암호(II)	7.2 암호해석(V)	7.3 인증방식
15:30-17:30	8.1 공개키암호	8.2 Digital Watermark(II)	8.3프로토콜안전성/영지식증명
20:00-22:00	Night Session		
1.31.(토)			
8:30-10:10	9.1 구현	9.2 소프트웨어보호	9.3 암호시스템/표준화
10:30-12:30	10.1 타원암호(III)	10.2 Digital Watermark(III)	

III. Session 별 발표내용

발표 제목이 국문 또는 영문으로 표기 된 경우는 각각 원고가 일어 또는 영어로 작성되어 있다는 것을 의미한다.

Session 특별강연

(1) 인터넷에 있어서 시큐리티 문제와 JPCERT/CC

(The Internet Security Incidents and JPCERT/CC Activities)

Suguru Yamaguchi (JPCERT/CC,

Chair of Steering Committee)

'96년 10월부터 일본에 있어서 긴급대응 조직으로 발족한 JPCERT/CC의 관련 활동을 소개하는 내용으로 인터넷을 통한 불법적인 접근 시도 기술, 일본의 피해 현황 및 향후 대책에 관하여 발표하였다.

(2) 인증국의 실용화 실험에 대하여

(Initiative for Certification Authority Technology)

Yoshihi Kameshima (ICAT)

인증 실용화 실험 협의회 (ICAT)의 최신 연구 결과로 인증국 관리 Package인 ICAP(ICAT Certification Authority Package)와 proxy 암호 메일 서버인 REPOP (Privacy Enhanced POP) 등에 대하여 발표함. ICAP은 X.509v3를 구현한 공개키 증명서 관리 패키지로 WWW의 GUI와 계층 구조를 가진 복수 ICAP를 가지고 있으며, REPOP은 가입자의 부담을 적게 하고 암호 메일을 보내는 메일 서버로 관리자의 암호키의 일괄 관리와 기존 mailing client의 변경이 필요없는 특징을 가지고 있다. 알고리즘은 타원곡선 암호인 MyEllty와 MISTY를 이용하였고 '98년 2월부터 의료정보 인증국에 대한 실험을 시행할 계획이라고 하였다.

(3) 의료정보의 시큐리티 요건의 개요와 다단계인증 시스템

(Security Requirements for Health Information System and Proposal Delegated Certification System)

Ryuichi Yamamoto (Osaka Medical Univ.)

가용성, 무결성, 인증성을 가져야 하는 의료 정보에 대한 안전성의 요구 사항에 대한 정리하였고, 네트워크를 통한 의료 정보 시스템의 구축에 필요한 의료 정보의 backup 기술, 암호 및 인증 기술에 대하여 기술하였다.

Session 1.1 계산법과 정수론 응용

A) Modular polynomial의 계산 (Computation of Modular Polynomial)

Tetsuya Izu, Masayuki Noro, Kazuhiro Yokoyama (Fujitsu)

타원 곡선 암호에 있어서 위수 계산에서 필요한 모듈러 다항식인 $\Psi_l(X, j)$의 계산을 수식 처리 시스템인 Risa/Asir (ftp://endeavor.fujitsu.co.jp/pub/isis/asir/에 입수가능)를 이용하여 $l = 113$인 경우까지 계산하였다. 실험 결과, Newton 방정식 이용방식이 Borcherd product 이용방식보다 빠른 연산이 가능하였다.

B) 오차를 활용한 역원 연산법 (Inverse Algorithm by Utilizing Acceptable Error Range)

Tetsutaro Kobayashi, Hikaru Morita (NTT)

다정도 정수의 gcd 계산에 있어서 종래의 유크리드 호제법, 2진 gcd 계산법, Lehmer 계산법이 있는 데 Lehmer 법 중 효율을 높이는 방법으로 오차를 이용하는 방법을 제안하고, Sun workstation 상에서 구현결과 256 비트 정수의 gcd 계산에 종래의 2진 gcd 법보다 3.8배 빠르다는 것을 확인하였다.

C) 진동함수를 이용한 소인수분해 알고리즘

(A Factoring Algorithm using Oscillation Functions)

Kunikatsu Kobayashi, Shinnichi Homma, Qian Li (Yamagata U.)

2차 sieve 법과 복수 다항식 2차 sieve 법에는 2차 함수를 이용하여 v-smooth 한 값을 구하여 $k^2 = l^2 \bmod n$ 의 관계가 성립하는 합성수 n의 소인수를 구한다. 4차 이상의 진동함수 (고차 다항식)를 이용하여 소인수 분해 알고리즘을 제안하고 2차 sieve법보다 유효하다는 것을 확인하였다.

D) P-1법에 강한 합성수의 제안

(Note on the Composite Numbers Invulnerable to the P-1 Method)

Yoshizo Sato, Yasuyuki Murakami, Masao Kasahara(Kyoto Inst. of Tech.)

P-1법에 의한 소인수 분해 법에 강한 새로운 소수 발생법으로 평가 지표로 레벨 개념을 도입하여 레벨이 높은 소수의 발생법을 제안하였다.

Session 1.2 암호해석(I)

A) DES의 엄밀한 최적차분특성의 검색

(The Best Differential Characteristics Search of DES Considering Key Dependency)

Takashi Hyodo (U. of Electro-Com), Kazuo Ohta, Kazumaro Aoki(NTT)

DES에서 각 S-box의 입력이 독립이라는 가정 하에 F 함수의 차분확률은 각 S-box의 차분 확률의 곱으로 계산된다. 그러나 F 함수의 차분 확률은 키에도 의존한다. DES의 DC에 대한 안전성을 엄밀히 평가하기 위하여 다음의 3가지를 검토하였다.

(1)F 함수의 엄밀한 차분특성확률을 모든 입력과 출력차분에 대하여 효율적으로 구하는 방법 (2)주어진 확률에 대하여 그 이상의 확률은 모두 구할 수 있는 방법 (3)N 단의 DES에 대하여 차분확률특성을 효율적으로 구하기 위한 탐색 공간의 축소. 시뮬레이션 결과 6라운드 이하인 경우는 Matsui의 결과와 동일하고 7라운드 이상의 경우는 Knudsen의 결과와 동일하다.

B) 최대 비평균 차분확률에 관한 고찰(On Maximum Non-averaged Differential Probability)

Kazumaro Aoki (NTT)

MISTY와 같은 블럭암호에서 안전성의 평가 지표의 하나로서 이용되고 있는 최대평균차분확률에서 평균이라고하는 것은 키에 대한 평균을 의미한다. 최대평균차분확률이 충분히 작다고 하더라고 최대차분확률이 클 가능성이 있다. 키에 의한 최대차분확률이 최대평균확률보다 작아질 수 있는 것을 제시하고 키의 변동에 따른 최대차분확률의 평가를 시도한다. F 함수가 전단사이라고 가정할 때 DES 형태의 암호에서 2단의 경우를 조사한 결과, 종래의 DC,LC에서 이용한 안전성 평가 지표인 최대 평균 차분 확률, 최대평균선형확률에 대한 평가와 동일함을 확인하였다. 3단 이상의 경우는 최대 차분 확률이 최대평균 차분확률의 4.5배나 크다는 것을 확인하였다.

C) FL 함수가 없는 경우의 MISTY1에 대한 고차차분공격에 의한 안전성 평가의 고찰

(On the Strength of MISTY1 without FL Function by the Higher Order Differential Attack)

Kazuyuki Hisamatu, Toshinobu Kaneko (Science U. of Tokyo)

선택평문공격의 한 종류인 고차차분 공격법을 FL함수가 없는 MISTY에 대하여 GF(2) 상의 비선형 함수에 대한 고차차분법을 이용하여 4단의 MISTY에 대하여 36개의 선택평문에 대하여 공격이 가능함을 제시하였다.

D) 고차차분공격에 있어서 SPEED 암호의 취약 키에 관하여

(On the Weak Keys in SPEED Cipher by Higher Order Attack)

Minoru Uemura, Hidema Tanaka, Toshinobu Kaneko (Science U. of Tokyo)

Zheng 등이 '97년에 제안한 SPEED 암호에 대하여 고차 미분치를 이용하는 고차 차분 공격이 가능한 취약키가 존재하는 것을 파악하였다. 14 라운드 SPEED는 16차 차분에 의한 75% 가 취약키를 가지고 있게 되었고 2^{16}개의 선택 평문과 2^{24} 회의 F 함수 연산의 복잡도로 해독이 가능하게 된다. 계산기 시뮬레이션 결과 R10000 200MHz CPU로 약 50분이 소요되었다.

E) CAST 암호의 고차 차분 공격(II)
- 선택차분치를 이용한 고차차분공격 -

(Higher Order Differential Attacks of a CAST Cipher(II) - H.O.D Attacks Using Chosen Higher Order Differentials-)

Shiho Moriai, Takeshi Shimoyama, Toshinobu Kaneko (TAO)

평문의 부울 함수로서 암호문을 표시하는 최대 차수로부터 고차차분의 단수를 결정하였다. 공격자에게는 그 단수의 고차차분에서 임의의 차분치를 이용하는 이점이 있으나, 설계자에게는 고차 차분 공격에 필요한 선택 평문 수나 계산량의 하한치를 구하는 것이 불충분하다. CAST 암호의 경우에 선택고차차분에 대하여 고차차분의 단수가 종래 보다 낮은 것을 제시하였다.

Session 1.3 프로토콜

A) 시간 암호 프로토콜과 그 응용(Timed-release Cryptographic Protocol and its Application)

Michiharu Kudo (Japan IBM)

시간 키 개념을 도입하여 지정된 기간 동안만 암/복호화가 가능한 공개키 관리 프로토콜에 대하여 제안하고 전자 투표, 전자 입찰 등에의 응용 가능성을 제시하였다.

B) 전자 추첨 서버의 구현 (Implementation of Digital Lottery Server)

Kazuo Sako (NEC)

WWW 서버를 통하여 전자 추첨 서버인 digilot의 개발 결과를 발표하였다. 특징으로는 (1)참가자가 선택한 수에 의해 당선자가 결정 (2)주최측이나 참가자가 추첨 결과 조작이 불가능 (3) 참가자의 추첨 결과가 검증 가능 이다.

C) Horster 등의 인증과 동시 암호에 의한 검증자 한정 서명의 해제

(Convertible Limited Verifier Signature based on Horster's authenticated encryption)

Shunsuke Araki, Satoshi Uehara, Kyoki Imamura (Kyushu Inst. of Tech.)

Hoster-Michels-Peterson이 제안한 인증 암호화가 가능한 방식에 Chaum이 제안한 undeniable signature 방식을 추가하여 검증자가 한정되는 서명 방식을 제안하였다.

D) 대인 판매에 있어서 신용카드형 전자결재방식의 고속화에 관한 검토

(A Light Weight Electronic Transaction Protocol for Credit-based Payment)

Goichiro Hanoka*, Kanta Matsura*, Yuliang Zheng(Monash U.), Hideki Imai*(Tokyo U.)

통행료나 주차비 지불 등과 같이 소액을 지불하는 전자 결재의 경우, 신용카드 및 KPS(Key Predistribution System)를 이용하여 고속 및 저렴한 구축 방법을 제안하였다.

E) 효율적인 l-out-of-k 분실 통신 (Efficient l-out-of-k Oblivious Transfer)

Atsushi Fujioka(NTT), Hiroaki Kikuchi (Tokai U.)

준동형성을 만족하는 공개키 암호방식을 이용하여, 효율적인 l-out-of-k 분실 통신의 구성법으로 종래의 Even-Goldreich-Lempel 구성법에서 일반적인 공개키 암호를 가정한 것보다 강한 가정이 필요하나, 송신자의 처리량은 k과 l의 선형 비례하고, 수신자의 처리량은 ElGamal 법과 동일하고 시스템내의 통신량이 최저 20% 삭감된 방법을 제안하였다.

Session 2.1 암호방식 제안 및 암호 고속화

A) 부분 암호화에 의한 암호의 강화 (Strengthen Cipher by Partial Encryption)

Kazuo Matsunage (Nihon Graphic System)

main key 이외에 여러 그룹이 발생한 partial key로 암호화함으로서 평문하나에 대하여 10^{30}이상의 암호문을 얻을 수 있는 방법을 제안하였고 내용은 일본내 특허 출원 중에 있다.

B) A Public Key Cryptosystem based on Minimum Distance Decoding Problem for Binary Linear Code

(선형부호의 최소거리복호 문제를 근거로 한 공개키 암호방식)

Tadashi Wadayama(Okayama Prefectural U.), Koichiro Wakasugi, Masao Kasahara (Kyoto Inst. of Tech.)

최소거리복호 문제를 이용한 공개키 암호 시스템을 제안하였다. 2진 선형 부호,C를 좌표 치환한 부호 C'에 대한 trellis 구조를 비밀키로 하고 C의 generator matrix를 공개키로 이용한 암호 시스템으로 안전성과 효율적인 전송방법 등을 기술하였다.

C) RSA 고속 암호화 방법(A Fast Algorithm of RSA Cryptosystems)

Ryuichi Sakai (Osaka Electro-Comm. U.), Sachie Tsutsui, Masao Kasahara

(Kyoto Inst. of Tech.)

RSA 암호화 연산에 있어서 O(log n) 회의 곱셈과 잉여 계산이 필요하다. 일반적으로 잉여계산이 곱셈보다 시간이 더 소요되므로, 기존의 Satake와 Kasahara가 제안한 특별한 형태로 제약이 있는 모듈러 연산을 어떠한 모듈러에 대하여 계산이 가능한 방법을 제안하였다.

D) 타원암호곡선 고속화의 2, 3 방법 (Fast Algorithm for Elliptic Curve Cryptosystem)

Kiyoshi Ohgishi *, Ryuichi Sakai(Osaka Electro-Comm.), Masao Kasahara * (Kyoto Inst. of Tech.)

타원 ElGamal 암호의 고속화를 위하여 기존의 Satake-Kasahara 법을 개량하여 고속 모듈러 연산이 가능하고 32 비트 CPU에 실험을 수행하였다.

F) 비트 계열에 대응한 Addition-Substraction Chain의 구성에 의한 고속 Modular 멱승에 관하여

(Speeding up Modular Multiplication by Addition-Subtraction Chain based on Bit Series)

Koji Chida (Waseda U.)

기존의 모듈러 연산의 고속화 시 지수에서 "1"의 분포가 0.5의 확률이라는 가정에서 수행하는 데 반하여, "1"이 집중적으로 많은 부분에 대한 고속 모듈러 연산법을 Addition-subtraction chain을 이용하는 방법을 제안하였다.

Session 2.2 암호해석 (II)

A) DES 암호에 있어서 Partitioning 공격에 관한 고찰 (On Partitioning Cryptanalysis of DES)

Takeshi Hamade, Takafumi Yokoyama, Tohru Shimada, Toshinobu Kaneko (Science U. of Tokyo)

Harpes와 Massey가 제안한 선형해독법을 일반화한 partitioning 공격은 입력 패턴과 출력 패턴을 분할하여 각 패턴 쌍의 불균일성을 이용한 선택평문공격이다. 이 공격을 기지평문공격으로 확장을 위해 sieve 형 선형 근사식에 partition의 개념을 도입하고 partition은 1라운드에 적용하고 중간 라운드에는 선형근사식을 접속하는 새로운 partitioning 공격을 제안하였다. 유효성을 확인하기 위하여 이 해독법에 의한 5,9,13 라운드의 DES 공격에 필요한 기지평문수가 삭감된다는 것을 확인하였다.

B) 차분공격법/선형공격법에 대한 안전성 평가 척도의 유효성에 대하여

(Effectiveness of Outline Measures of Strength against Differential and Linear Cryptanalysis)

Yasuyoshi Kaneko (Science U. of Tokyo), Tsutomu Matsumoto (Yokohama Nat'l U.)

DC와 LC에 대한 안전성의 평가 척도로서 차분특성과 선형근사식의 성립 확률의 최대치로 평가하는 데 개념적인 평가를 위하여 여러 가지 Feistel 암호 형태에서 라운드를 증가함에 따른 근사적인 안전성 평가를 시행하여 이론적인 분석의 유효성을 제시하였다.

C) 차분/선형/고차차분/보간 공격에 안전한 S-box의 구성법

(How to Design Secure S-boxes against Differential, Linear, Higher Order

Differential, and Interpolation Attacks)

Shiho Moriai (TAO)

블럭 암호의 안전성 평가시 지금까지 발표된 모든 공격에 대한 충분한 안전성을 보장해야 하는 것이 설계자의 필요조건이다. DC와 LC에 강한 함수로서 Galois Field 상에 power 함수가 알려져 있으나 이런 함수를 이용한 블럭 암호가 고차 차분공격이나 보간 공격에 의하여 해독된 사례가 있다. DC와 LC에 충분한 강도를 가지고 고차 DC나 차분 공격에 강한 함수의 구성법을 제안하였다.

D) 소수의 S-box를 이용한 라운드 함수의 구성에 관하여 (II)

(A round function structure consisting of few S-boxes (Part II))

Masayuki Kanda,Youichi Takashima (NTT HI Lab.),Tsutomu Matsumoto (Yokohama Nat'l U.)

라운드 함수로서 비선형 변환(1), 선형변환, 비선형변환(2)로 구성되는 SPN형의 블럭 암호를 구성하는 데 차분 및 선형 특성의 상한치를 증명가능한 구조를 제안하였다.

E) DES 형태 암호의 안전성에 관한 2,3의 고찰 - 선형근사식의 구성이 곤란한 F 함수의 제안 -

(Notes on Security of DES-like Cryptosystem - A Proposal of Common Key Cryptosystem Invulnerable to Linear Cryptanalysis)

Yosuke Kinoshita, Koichiro Wakasugi, Masao Kasahara (Kyoto Inst. of Tech.)

선형 공격에 강하도록 라운드 함수를 라운드 키에 의하여 결정되어 비선형성을 높힌 구조를 제안하였으나 라운드 키에 의한 swapping은 해독의 위험성이 있음을 지적받았다.

Session 2.3 ID-based 키 분배

A) RSA 암호의 안전성을 기반으로 하는 ID-NIKS

(ID-NIKS based on RSA Cryptosystem)

Yasuyuki Murakami, Atsunori Fujikawa, Masao Kasahara(Kyoto Inst. of Tech.)

RSA 암호를 이용한 안전하고 간단한 ID 정보를 이용한 예비통신이 불필요한 키 공유방식(ID-based Non Interactive Key Sharing Scheme)을 제안하였다.

B) 교신없는 ID-based 키 분배 방식의 안전성에 관하여

(On the Security of a Non-interactive Identity-based Cryptosystem)

Tatsuaki Okamoto, Shigenori Uchiyama (NTT)

저자들이 이미 제안한 타원 곡선 상에 Diffie-Hellman 방식의 예비통신 없는 키 분배 방식이 안전하지 않음을 제시하였다.

C) Identity-based Non-interactive Key Sharing Equivalent to RSA Public-key Cryptosystem

(RSA 공개키 암호와 등가인 ID 정보를 이용한 예비통신이 불필요한 키공유 방법)

Hatsukazu Tanaka (Kobe U.)

새로운 ID-NIKS를 RSA 암호계와 안전성이 동일한 방식을 제안하였다.

D) 서비스에 대응하는 최적화한 KPS (A Study on Optimization of KPS for Certain Services)

Tsuyoshi Nishioka (ADVANCE Co.), Hideki Imai (U. of Tokyo)

KPS 방식 중 실용성이 높은 선형 방식 KPS를 서비스에 따른 이 기능의 일부를 제한하여 안전성, 메모리 및 처리 효율이 향상된 최적 방식을 제안하였다.

Session 3.1 전자 현금

A) 전자 현금의 안전성 평가에 대하여 (An Evaluation of Security of E-money)

Yasushi Nakayama(Bank of Japan), Kazuo Ohta(NTT), Tsutomu Matsumoto (Yokohama Nat'l U.)

여러 가지 제안된 전자 현금 방식들을 위험성과 그 대책에 따른 경비 부담 측면에서 비교 분석하였다.

B) Electronic Cash Scheme for Efficient Deposit (효율적으로 예금이 되는 전자 현금방식)

Masfumi Oka, Toru Nakanishi, Toru Fujiwara (Osaka U.)

예금시 보내는 데이터 양이 현금 사용시 보내지는 데이터 보다 적은 성질을 만족하는 효율적인 전자 현금 방식을 제안하였다.

C) 삽입 서명 방식을 이용한 전자 현금 시스템 (A Method of Embedding Certification in Untraceable Electronic Money)

Shingo Miyazaki, Kouchi Sakurai (Kyushu U.)

Brands의 restrictive blind 서명 방식 [Eurocrypt'95]과 Abe 등의 partial blind 서명 방식[Asiacrypt'96]을 혼합하여 전자 현금 데이터에 여러 가지 정보를 삽입하는 방식과 그 안전성을 기술하였다.

D) 계층형 전자 현금 방식 (Hierarchical Electronic Cash Scheme)

Hidemi Moribatake, Hideki Akashika, Tomohisa Suganuma, Yoshio Takahashi (NTT)

지금까지 제안된 전자 현금 방식에 있어서 실용성 측면에서 문제점을 지적하고 해결책으로 계층적 전자 현금 방식을 제안하였다. 개량점은 (1) ATM을 통한 현금 인출 가능 (2) 지불과 양도 프로토콜을 공유 (3) 대량의 전자 현금을 수령 가능한 점이다.

E) 전자상거래에 적용되는 안전성 해석방법의 제안

(A Study of Security Analysis Method on Electronic Commerce)

Yasuyoshi Tokutsu, Takayoshi Shiraishi (Hiroshima Shudo U.)

전자 상거래에서 정보의 흐름에서 안전성의 분석 방법으로 sequence tree 방법을 이용한 방식을 제안하였다.

F) 고속처리에 적합한 Micro-payment 방식 (Fast Micro-Payment Scheme)

Hideki Akashika, Hidemi Moribatake, Junichi Gohhara (NTT)

해쉬 함수만을 이용하여 소액 결제 방식을 제안하고 타 방식(Payword, Millicent)에 비해 고속이고 익명성 및

분할 지불성을 만족한다고 주장하였다.

Session 3.2 Digital Watermark (I)

A) A Digital Watermark based on the Wavelet Transform and its Robustness on Image Compression and Transformation

(Wavelet 변환에 의한 디지털 워터마크-화상 압축, 변환 처리에 대한 Robust 성에 대하여-)

Hisashi Inoue*, Akio Miyazaki**, Akihoro Yamamoto** (Kyushu U.), Takashi Katsura* (Matsushita)

watermark 정보를 삽입하는 방법으로 wavelet 변환 계수의 zero tree를 이용방법과 화상 신호 중 중요한 주파수 성분인 저주파 성분의 변환 계수에 threshold 값 이용 방법을 제안하였다.

B) Bit Frame 상에 통계적 차이를 이용한 Digital Watermark

(A Watermark Technique using Statistical Difference on Bit Plane)

Jun Furuta(Min. of Finance), Kazukuni Kobara, Hideki Imai(U. of Tokyo)

원화상을 5×5 화소의 블럭 단위로 분할하여 원화상의 특성에서 얻은 상위 비트 프레임위에 문자를 삽입하는 방법을 제안하고 실험 결과 화상의 열화는 거의 없었고 타방식과 비교, 평가 등이 후속 과제이다.

C) Fourier 변환에 의한 화상의 Digital Watermark 방법

(A Watermark Technique for Grayscale Image under Discrete Fourier Transform)

Yoshihide Fukuoka, Kineo Matsui (National Defence Academy)

화상 정보를 Fourier 변환한 주파수 성분을 이용하여 digitial watermark를 삽입하는 방법을 제안하였고 저작권 보호 방식에 응용이 가능함을 기술하였다.

D) DCT를 이용한 Digital Watermark에서 새로운 블럭의 선택법

(A New Method of Selecting Blocks for the Digital Watermark using DCT)

Sun-young Lee, Hideki Imai (U. of Tokyo)

DCT를 이용한 watermark 삽입 시 블럭을 분할하여 효율적인 방법을 제안하였다.

E) The Distribution of DCT Coefficients to Embed Digital Watermark

(Digital Watermark를 삽입한 DCT 계수의 분포)

Takuo Mori, Hideki Imai (U. of Tokyo)

화상 정보의 DCT변환 후 각 계수의 분포를 조사하고 화상의 열화와 공격의 내성을 고찰하였다.

F) 논리 필터를 이용한 새로운 Digital Watermark 방법

(A New Digital Watermark Method using a Logical Filter)

Hirokazu Ishizuka, Yasuyuki Sakai (Mitsubishi), Kouichi Sakurai (Kyushu U.)

새로운 watermark 생성법으로 저주파 성분을 제거하는 logical filter를 이용하는 방법을 제안하였다.

Session 3.3 인증서버와 익명통신

A) Private CA의 구현과 평가

(An Implementation of Private CA and its Evaluation)

Akiko Tsunoda, Akira Nagai, Toshikazu Yamaguchi, Ikuro Oyaizu (NTT)

사용자가 개인이 운영하는 증명서 발행소(Private CA)를 구축에 있어서 Windows NT 상에 필요한 증명서의 발행 및 운영 기능을 구현하고 평가하였다.

B) WIDE 프로젝트에 있어서 CA의 운영 실험과 고찰

(Management and Study of experimental CA in WIDE project)

Mine Sakurai(NEC), Hiroyuki Hattori (Meiji U.)

인터넷 연구 프로젝트를 수행하고 현재 400명이 참가하고 있는 WIDE 프로젝트에서 CA 운영에 관련된 도구 개발과 운영 실험에 대하여 보고하였다.

C) 인증국 3권 분립 모델에 기반으로 한 인증 시스템의 운영

(An Implementation of Authentication System based on the Separation of Three Authority Model)

Yuji Suga, Shigeichiro Yamasaki, Miyuki Murakami, Keijiro Araki (Kyushu U.)

X.509 디지털 증명서를 이용한 인증 방식은 다른 domain에서는 사용이 불가능한 점이 있다. 3권 분립 모델을 제안하여 증명서에 유효한 용도, 권한을 증명서 속에 삽입하는 것이 외에 이용권한을 증명서와 분리함으로서 1장의 증명서로 복수의 서비스를 받도록 3권 분립 모델을 구현하고 운영하였다.

D) A Development of Generic Cryptographic Service Mechanism Open Distributed Network Computing

Sang-gi Lee (KEPC), Yong-rak Choi (Taejon U.)

분산 컴퓨팅 환경에서 암호 서비스를 제공하는 GSS-API, GCS-API에 대한 구현 결과를 보고하였다.

E) Internet 상의 익명통신방식의 평가

(Evaluation of Anonymous Channel in the Internet)

Kenji Seo*, Hiroaki Kikuchi*, Atsushi Fujioka(NTT), Syohachiro Nakanishi* (Tokai U.)

인터넷상에서 송신자의 익명성(예, 전자상거래에서 구매자, web browser의 client)을 확보하기 위하여 public web proxy, anonymizer, onion routing, crowds 등의 익명성의 강도, 수행 속도 등을 비교하였다.

F) 익명 사용자의 연락 방법

(Communication with Anonymous Users)

Tsutomu Matsumoto, Kensuke Shimizu, Katsuya Okamoto, Daisuke Inoue

(Yokohama Nat'l U.)

시청률 조사나 전자 투표의 경우 사용자가 익명으로 참가하는 상황에서 익명의 사용자에게 연락을 취하는 방법과 사용요금 부과 방법에 대하여 고찰하였다.

Session 4.1 타원암호 (I)

A) Efficient Construction of Secure Hyperelliptic Curves with RM family

(RM family를 이용하여 안전한 초타원 곡선의 효율적인 구성법)

Hiroti Kawashiro, Osamu Nakamura, Jinhui Chao, Shigeo Tsujii (U. of Chuo)

초타원 곡선 암호를 구성 시 CM (Fermat Curve)의 genus 2인 초타원 곡선을 찾는 방법을 제안하였다.

B) Design of Elliptic Curves using CM Tests and Lifting

(CM 테스트와 Lifting 에 의한 안전한 타원곡선의 구성법에 관한 고찰)

Kohji Sobataka, Osamu Nakamura, Jinhui Chao, Shigeo Tsujii (U. of Chuo)

CM 타원 곡선은 고속 타원 암호계의 구성에 알려져 있고 CM test algorithm이 제안되어 있다. 이런 CM field algorithm은 급수 전개로 인하여 계산량이 많고 근사 오차에 대응한 필요가 있다. 유한체의 대수적 연산으로 CM test와 lifting에 의해 CM 타원곡선을 구축하는 방법을 제시하였다.

C) 안전한 타원암호 파라메터 설계 (Schoof 알고리즘의 개량)

(Choosing Parameters for Secure Elliptic Curve Cryptosystem (Improvement on Schoof's Algorithm)

Izu, Kogure, Noro, Yokoyama (Fujitsu)

기존의 Schoof 알고리즘에 그 개량과 더불어 isogeny cycle 법, match and sort 법을 효율적으로 조합하여 실용적인 시간에 군의 위수 계산이 가능한 방법을 제안하고 그 결과 240 비트까지 소수체 상의 타원 곡선을 쉽게 구성이 가능하게 되었다.

D) 초타원 곡선 상의 이산 대수 문제에 근거로 한 암호계의 안전성에 관한 고찰

(On Security of Cryptosystems based on Discrete Logarithm Problems over Hyperelliptic Curves)

Kingo Kurotani, Kazuto Matsuo, Junhui Chao, Shigeo Tsujii (Chuo U.)

generic 한 공격을 받지 않아 타원 곡선이 초타원 곡선 상의 이산 대수 문제는 안전성이 보장되어 있다. 그러나 종래의 공격법은 1회의 공격에 대한 안전성만을 평가하였으나 동일한 곡선을 이용한 암호계를 반복하여 운영하는 경우에 안전성을 검토하였다.

E) 부정 방정식에 근거로 한 RSA형 타원 암호의 안전성 해석

(Security Analysis based on Diophantine Equation for RSA-type Elliptic Curve Cryptosystems)

Yukio Tsuruoka, Kenji Koyama (NTT)

타원 곡선 $y^2 = x^3 + b \bmod n$을 이용한 RSA형 타원암호를 동보통신에 이용하는 경우 동보된 암호문으로부터 평문을 구하는 문제는 유리체 상에 타원곡선의 정수점을 구하는 문제 (Mordell의 부정방정식)에 환원되는 것을 제시하였다.

Session 4.2 암호해석(III)

A) 통계적 방법을 이용한 암호강도 평가 지원 시스템

(A Cipher Strength Evaluation System based on Statistical Methods)

Yukiyasu Tsunoo, Ryoji Ohta, Hiroshi Miyauchi, Katsuhiro Nakamura (NEC)

블럭 암호의 강도를 평가하기 위하여 입출력간의 통계적 특성을 3차원 컬러로 표시하는 도구를 개발하고 알고리즘의 비교 검토에 활용할 수 있다고 하였다.

B) 통계적 방법에 의한 안전성이 평가된 암호

(A Secure Cipher Evaluated by Statistical Methods)

Yukiyasu Tsunoo, Hiroyasu Kubo, Hiroshi Miyaguchi, Katsuhiro Nakamura (NEC)

통계적 특성을 만족하는 새로운 블럭 암호로 128비트 키와 64비트 블럭을 갖는 CIPHERCORN을 개발 결과를 제시하였다.

C) 병렬 컴퓨터에 의한 블럭 암호의 해독 실험

(Experimental Results of Cryptanalysis of Block Cipher on Parallel Computer)

Takeshi Shimoyama (TAO)

DES를 LC에 의한 해독시 2단계에서 필요한 30비트 전수 검색 방법을 병렬 컴퓨터로 해독하는 방법을 제안하였다.

D) 선택평문형 선형해독법에 의한 8단 DES의 해독 실험

(An Experiment of Linear Cryptanalysis for 8-round DES using Chosen Plaintexts)

Kenji Ohkuma, Seichi Amada(TAO), Toshinobu Kaneko (Science U. of Tokyo)

저자들이 이미 제안한 선택평문형 선형해독법에 의한 효율성을 확인하기 위하여 8단 DES의 해독 실험을 한 결과 기존의 공격보다 필요 평문이 1/4로 줄 수 있다는 것을 확인하였다.

Session 4.3 접근 제어

A) 사용 조건이 있는 배포 파일의 접근 감시 에이전트

(Access Control Agent of Distributed Files)

Shigeo Kitazawa, Eiji Okamoto (JAIST), Masahiro Mambo (Tohoku U.)

서버 에이전트를 이용하여 저작자에 의한 사용자의 사용권을 제어 및 불법 이용시 통제가 가능한 방법을 제안하였다.

B) 접근 제어를 이용한 저작권 제어

(A Copyright Control Method based on the Access Control)

Hirostugu Kinoshita (Kanagawa U.)

기존의 저작권 보호 방법으로 디지털 서명, concealed image, digital watermark 방법과 달리 접근 제어 방법을 이용하는 방법을 제안하고 coloured Petri net를 불일치성의 검출에 이용하였다.

C) 목적 지향 접근 제어 모델의 고찰

(A Note on Object-Oriented Access

Control Method)

Tomoyuki Tada (ADVANCE Co.), Hiteki Imai (U. of Tokyo)

목적 지향 데이터 베이스의 접근 제어 방식에 대하여 고찰하였다.

D) 공동 관계를 이용한 인가 모델과 그 제어 기구

(The Cooperative Relation based Authorization Model and its Mechanism)

Takeharu Kato, Masakazu Soshi, Mamoru Maekawa (U. of Electro-Comm.)

분산 환경에 있어서 조직간의 공동 작업에 있어서 security 제어 방식에서 인가 모델을 제안하였다.

E) 유연한 조직 운영에 있어서 접근 제어 기구의 고찰

(Consideration on the Access Control System in the Flexible Organization Management)

Takashi Tanaka, Eiji Okamoto(JAIST), Masahiro Mambo(Tohoku U.)

인터넷을 통한 이종 조직간에 연계 작업을 수행할 때, 유연한 작업 환경의 구축과 동시에 통신로를 보호하는 방법을 제안하였다.

Session 5.1 난수생성

A) BBS 생성기와 디지털 카오스생성기의 i.i.d성을 이용한 난수성 검증

(Pseudorandomness Test of BBS Generator and Discrete Chaos Generator based on i.i.d. Property)

Tohru Kohda, Hirokazu Soh(Kyushu U.)

BBS 생성기, 이산 카오스 생성기, 선형 합동식에 의한 난수 발생기의 i.i.d성을 통계적으로 비교하였다

B) Jacobi 계열의 난수성과 암호학적 성질에 관한 고찰

(Consideration on Quality for Random of Jacobi Sequence)

Takanori Niwa, Akihiro Satoh, Ichi Takumi, Masayasu Hata (Nagoya Inst. of Tech.)

이차 잉여류를 이용하는 Legendre 계열을 확장한 Jacobi 계열의 난수성에 대하여 고찰하였다.

C) 안전한 Filter Generator의 구성법

(A Method for Constructing Secure Filter Generators)

Kouichi Sugimoto, Tetsuya Chikaraishi, Tetsuya Morizumi (Toyo Com. Eq. Co.), Takashi Satoh, Kaoru Kurosawa(TIT)

표준형 LFSR의 tapping point 위치를 바꾼 modular LFSR를 이용한 filter generator의 구성법에 대하여 제안하였다.

D) 내 차분 상관 공격을 고려한 비선형 함수에 관한 고찰

(On Non-linear Functions against Differential Correlation Attack)

Tohru Sorimachi, Toshio Tokita, Mitsuru Matsui(Mitsubushi)

상관 공격과 차분 상관 공격에 강한 비선형 combiner의 설계 조건을 제시하고 5차 부울함수를 전수 검사한 결과

700,000개의 양호한 비선형 함수가 존재함을 확인하였다.

E) 자기 조직적 구조를 갖는 비선형 함수의 고찰

(Nonlinear Pseudo-random Sequence Generator with Self-Organizing Structure)

Takeshi Nagao, Ichi Takumi, Masayasu Hata (Nagoya Inst. of Tech.)

암호학적으로 양호한 조건을 갖는 자기 조직적인 비선형 함수로 가변되는 레지스터를 이용하는 제안하였다.

F) Highly Nonlinear t-resilient Functions

Kaoru Kurosawa, Takashi Satoh(TIT)

resiliency와 nonlinearity를 tradeoff의 가능성을 제시하고 높은 resiliency와 nonlinearity를 갖는 부울 함수의 구성법을 제안하였다.

Session 5.2 키 위탁, 키 분배 및 키 복구

A) 키 복원 기능을 갖는 인터넷 상의 Archive Server

(Internet Archiving Server with Key Recovery Function)

Masayuki Numao, Yasutomo Nakayama (Japan IBM)

키 복구 기능에 추가하여 인터넷을 통한 데이터 보존 기능도 가질 수 있는 서버에 대하여 제안하였다.

B) Binding RSA 방식 (The Binding RSA Scheme)

Mototsugu Nishioka, Hisashi Umeki (Hitachi)

key escrow를 위하여 ElGamal 암호에서 데이터의 위조를 검출할 수 있는 binding 기법을 확장하여 RSA 암호에서도 binding이 가능한 방법을 제안하였다.

C) 국제간 통신에 있어서 키 위탁 방법에 관한 고찰

(Notes on International Key Escrow System)

Ikuko Kuroda, Masayuki Kanda(NTT), Shingo Miyazaki, Kouichi Sakurai (Kyushu U.)

Miyazaki-Sakurai[ISEC97-33]가 제안한 국제간 키 위탁 방식에 있어서 법 집행을 무효화를 위하여 송신자가 LEAF 생성을 방지하는 방법과 이 방법이 적용되는 부분 키의 정당성을 보증하는 비밀키 분산법을 제안하였다.

D) A Key Escrow Scheme for Real-time Monitoring

(실시간 감시에 적합한 키 위탁 방법)

Masayuki Abe, Masayuki Kanda (NTT)

(1)수사기관이 실시간 회선 감시가 가능 (2) 감시허가 시간이 지나면 자동적으로 감시가 불가능 (3) 수신자와 수사기관이 동일한 복호 결과를 얻는 것을 보증 (4) 송신자의 부정을 검출 가능한 키 위탁 방식을 제안하였다. 발표 후, NTT가 이러한 시스템을 구축하여 운용하고 있다는 오해의 소지가 없도록 하는 것에 대한 질의가 있었다.

E) A Group Key Renewal Method Suitable for Mobile Telecommunications(I)

(이동 통신에 적합한 그룹 키의 갱신 방법)

Natsume Matsuzaki, Jun Anzai (Advanced Mobile Telecomm. Security Tech.)

성형 네트워크 상에 분실 단말기에 해당하는 사용자를 제외하고, 기타의 모든 사용자에게 공통키를 갱신하는 그룹키 발생 방법을 제안하였다.

F) 그룹키 분배를 동반하고 Compact한 CBT 가입 메시지와 사후 프로세스 메시지

(Compact CBT-Join Message Combined with Group-Key Distribution and Post-Process Messages)

Kanta Matsuura*, Yuliang Zheng (Monash U.), Hideki Imai *(U. of Tokyo)

차세대 인터넷 프로토콜로 IPv6에서 multicast 방식의 키 분배 방식으로 CBT (Core-Based Tree) 메시지의 compact화를 논하고 그룹 내 송수신자 고유키를 운반하는 것이 가능한 방법을 제안하였다.

Session 5.3 비밀분산

A) 비밀 화상의 입체화 방법에 의한 암호화(Visual Cryptography by Stereogram)

Shinichi Matsukawa, Setsuo Arikawa (Kyushu U.)

화상 정보의 입체화를 위하여 기존에는 세로로 중첩하였으나 가로로 중첩하는 방법을 제안하였다.

B) Proposal of a Lattice-Based Visual Secret Sharing Scheme for Color and Gray-Scale Images

(칼러 및 gray-scale 화상에 대하여 lattice를 이용한 시각복호형 비밀 분산법의 제안)

Hiroki Koga, Hirosuke Yamanoto (U. of Tokyo)

J 가지 칼러 화상에 대한 (k,n) VSSS (Visual Secret Sharing Scheme)을 제안하였다.

C) MDS Secret Sharing Schemes Secure against Cheaters

Koji Okada, Kaoru Kurosawa (Tokyo Inst. of Tech.)

비밀 분산법과 에러 정정 부호간의 관계를 규명하였다.

D) 동적 비밀 분산법의 안전성과 효율

(Efficiency and Security of the Dynamic Multi-secret Sharing)

Yuji Watanabe, Hideki Imai (U. of Tokyo)

저자들이 SCIS'97에서 이미 제안한 동적 멀티 비밀 분산방식을 개량하고 효율과 안전성을 논하였다.

E) A Practical and Provably Secure Scheme for Publicly Verifiable Secret Sharing and its Application

(안전성 증명 및 공개적인 검증 가능한 비밀 분산의 효율적 실현법)

Eiichiro Fujisaki, Tatsuaki Okamoto (NTT)

Eurocrypt'96에서 Stadler가 발표한

PVSS(Publicy Verifiable Secret Sharing) 방법에서 안전성 증명 상의 오류를 지적하고 PVSS의 재정의를 하고 효율적인 구성법을 제안하였다.

F) 비밀 분산법에 의한 익명 통신

(Anonymous Communication Using Secret Sharing Schemes)

Hiroaki Kikuchi*, Atsushi Fujioka (NTT),Kenji Seo*, Syohachiro Nakanishi* (Tokai U.)

전체적인 트래픽은 분석이 가능하나 송/수신자 쌍방의 익명성을 보증하는 익명통신로를 제안하였다.

Session 6.1 정수론 응용

A) 결합 구조의 회합수 분포에 대하여

(Meeting Number Distribution of Incidence Structure)

Tsutomu Matsumto, Shuichi Hayashi, Shingo Inoue(Yokohama Nat'l U.)

키 분배 시에 활용이 가능한 2개의 결합 구조에 있어서 행과 행의 중첩이 되는 분포에 논하고 계산 알고리즘을 제안하였다.

B) Stamp-Martin 알고리즘의 일반화와 오류계열의 계산법에 대하여

(On Generalization of the Stamp-Martin Algorithm with Computing the Error Sequence)

Takayasu Kaida, Satoshi Uehara, Kyoki Imamura(Kyushu U.)

주기 계열에 있어서 k-error linear complexity의 고속연산법인 Stamp-Martin 알고리즘을 nonbinary로의 확장을 위해 3^n의 GF(3) 상의 계산법을 제안하였다.

C) 타원곡선 상의 이산 대수 문제에 대하여(I)

(Remarks on Elliptic Curve Discrete Logarithm Problem I)

Taichi Saito, Shigenori Uchiyama (NTT)

MOV reduction에 의한 타원곡선 상의 이산 대수 문제를 해결 시 축소되는 유한체의 크기가 적어져야만 유효하다는 점을 제시하고, Schoof의 상한치 확률을 재평가하였다.

D) A Fast One-Way Hash Function Based on Cellular Automata in GF(q)

(GF(q)상의 선형 Cellular Automata를 이용한 고속 일방향 해쉬 함수)

Miodrag Mihaljevic(Academy of Science and Arts,Yugoslavia), Yuliang Zheng (Monash U.), Hideki Imai (U. of Tokyo)

GF(p) 상에서 선형 cellular automata를 이용한 해쉬함수의 구성법에 대하여 제안하고 구성된 1-way 해쉬함수가 알려진 공격에 안전하다는 것을 제시하였다.

Session 6.2 암호해석 (IV)

A) 암호화 계산의 복잡도에 관한 고찰 (A Study on Complexity of Enciphering)

H. Miyano(TAO)

블럭 암호의 안전성 평가 방법으로 계산 이론적인 관점에서 평가 척도의 연구가 필요하다는 점을 주장하였다.

B) Time-Memory Tradeoff에 위한 암호 강도 평가 능력

(On the Power of Time-Memory Tradeoff Cryptanalysis)

Tsutomu Matsumoto, Takashi Hara, Iljun Kim (Yokohama Nat'l U.)

TMTO를 구현함에 있어 사전 계산표 작성 및 키 검색 단계로 구성된다. 키 검색 시 해쉬 방법을 이용하는 방법을 제안하였다.

C) Time-Memory Tradeoff 해독법에 의한 암호강도평가 장치의 실현성 검토

(The Feasibility Study of a Machine for Time-Memory Trade-Off Cryptanalysis)

Masahiro Iida, Katsumi Takahashi, Hiroyuki Miyata(Mitsubishi), Tsutomu Matsumoto (Yokohama Nat'l U.)

DES의 TMTO 해독 기계를 구현을 검토 한 결과 성공확률 80%, 사전처리 1개월, 해독시간 1시간이라는 목표하에 33MHz 전용 LSI 768개, 기억용량 512GByte로 가능하고 전체 기계의 부피는 Workstation 16대 정도이다고 주장하였다.

Session 6.3 암호 이론 기초

A) A^2- code = Affine Resolvable + BIBD

Satoshi Obana, Kaoru Kurosawa (Tokyo Inst. of Tech.)

ICICS'97에서 이미 발표한 내용과 동일한 것으로 최적 A^2부호는 affine alpha - resolvable design이어야 하고 BIBD를 추가하여도 최적이 된다.

B) On a Fallacious Bound for Authentication Codes

(인증부호에 있어서 하한치의 오류 정정)

Carlo Blundo, Alfred De Santis (U. of Salerno), Kaoru Kurosawa (Tokyo Inst. of Tech.), Wakaha Ogata (Hijime Inst. of Tech.)

De Sorte의 논문(Vol.3, No.3, 1991, pp.173-186, J. of Cryptology)에서 인증부호의 substitution success probability는 오류가 있음을 지적하고 올바른 하한치를 제시하였다.

C) 1 비트의 키 공유에 필요 충분한 카드의 배포 매수에 대하여

(On Dealing Necessary and Sufficient Numbers of Cards to Share a One-bit Key)

Takaaki Mizuki, Hiroki Shizuya, Takao Nishizeki (Tohoku U.)

참가자와 계산적으로 무제한한 능력을 가진 중간 도청자에게 카드를 배표할 때 모든 참가자에게는 정보 이론적 안전한 1 비트 정보를 공유하고자 한다. 이러한 분배 프로토콜의 존재성에 대한 필요 충분 조건을 제시하였다.

D) Self-synchronized Message Randomization Methods for Subliminal Channels

(Subliminal Channel을 위한 자기 동기를 취한 메시지의 랜덤화)

Kazukuni Kobara, Hideki Imai (U. of Tokyo)

subliminal channel을 통하여 비밀 메시지를 송신 시, 난수 계열과 구별 불가능하여야 하며 난수 변환기와 역변환기 간에 자기 동기가 가능한 방법을 제안하였다.

Session 7.1 타원암호 (II)

A) 작은 표수의 유한체 상에 Jacobi 다양체가 almost prime이 되는 초타원곡선

(Jacobian Varieties of Hyperelliptic Curves having Almost Prime Order over Finite Field with Small Characteristic)

Izuru Kitamura (U. of Electro-Comm.)

GF(2^n) (n은 소수) 상에 안전한 암호를 구성할 수 있는 $v^2 + v = f(u)$, $\deg f = 2g + 1$, $3 \leq g \leq 9$의 초타원 곡선을 제안한다.

B) C_{ab} 곡선을 이용한 공개키 암호(2)

(Public Key Cryptosystem with C_{ab} Curve (2))

Seigo Arita (NEC)

타원곡선과 초타원곡선을 포함한 넓은 클래스의 대수 곡선인 C_{ab} 커브의 Jacobian 군에 있어서 가산을 효과적으로 하는 방법을 제안하고 C_{ab}를 이용한 공개키 암호를 제안하였다.

C) Reducing Integer Factoring to Computing the Order of Elliptic Curve over Z_n for Composite n

(Z_n 상에 타원곡선의 위수 계산과 소인수 분해의 등가성)

Noboru Kunihiro, Kenji Koyama (NTT)

합성수 n에 대하여 ring Z_n 상에서 타원곡선의 점을 계산하는 문제가 n을 소인수 분해하는 문제와 계산상 등가임을 증명한다. 즉, 위수 계산이 가능하면 소인수 분해가 쉽게된다.

D) Efficient Elliptic Curve Exponentiation (II)

(효율적인 타원곡선 상의 지수승(II))

Atsuko Miyaji (Matsushita), Takatoshi Ono (Matsushita Information Systems Res. Lab.), Henri Cohen

타원 곡선 상의 연산 기법으로 새로운 좌표계와 혼합된 좌표계를 도입하고 기본 연산이 효과적으로 수행되도록 제안하였다.

E) 타원곡선 상의 서명 처리의 비교

(Comparison of Digital Signature Algorithms over Elliptic Curve)

Kunio Kobayashi, Tetsutaro Kobayashi, Hikaru Morita (NTT)

Okamoto의 디지털 서명 방식을 타원곡선 상에서 가능한 디지털 서명 방식을 제안하고, Pentium-166MHz, Linux 상에서 타원곡선 DSA는 30ms, 새로운 방식은 60ms로 처리됨을 확인하였다.

Session 7.2 암호해석(V)

A) 가변 구조를 갖는 블럭 암호에 있어서

평가 방법에 대하여

(One Method to Evaluate a Block Cipher Including Dynamic Structure)

Masumi Egawa, Ichi Takumi, Masayasu Hata (Nagoya Inst. of Tech.)

기지평문 공격에 대항 수단으로 가변 구조를 갖는 블럭 암호가 제안되어있다. 그러나 키에 의하여 가변되는 구조의 해독 가능성을 지적하였다.

B) SNAKE 암호의 안전성 평가에 대한 고찰

(A Study on the Strength of the Block Cipher SNAKE)

Hidema Tanaka, Kazunori Maekawa, Yasunori Sato, Toshinobu Kaneko (Science U. of Tokyo)

SNAKE 설계자는 4단 이상이면 차수가 30 이상이 되어 고차 차분 공격이 어려우리라고 주장한 반면, 저자들은 차분의 선택에 따라서는 적은 차수의 차분 공격이 가능하다고 주장하였다. 이를 입증하기 위하여 등가의 7단 SNAKE(2)(8,4,64,r)에 대하여 28의 선택 평문으로 8차 차분 공격이 가능함을 보였다.

C) SNAKE 암호의 보간 공격

(Interpolation Attacks of the Block Cipher : SNAKE)

Shiho Moriai, Takeshi Shimoyama (TAO), Toshinobu Kaneko (Science U. of Tokyo)

SNAKE의 S-box로 GF(2^m)상의 x^{-1}를 사용하고 있는 데 이 함수를 유리식으로 표현함으로 하여 보간 공격을 가능함을 제안하였다. 결과 $m = 8$인 경우 11단 이하의 SNAKE(1)과 SNAKE(2), $m = 16$인 경우 13단이하의 SNAKE(1)과 14단 이하의 SNAKE(2)가 해독됨을 보였다.

D) 선택 평문 공격에 의한 skDES의 해독

(An Analysis for skDES by Chosen Plaintext Attack)

Yukiyasu Tsunoo, Hisoyasu Kubo (NEC)

SCIS97에서 제안한 DES에 shift 연산을 추가하고 chain구조를 갖는 skDES 암호에 대하여 중간 키의 갱신 횟수가 일정하도록 한 선택 평문 공격을 제시하였다.

E) 선택 차분을 이용한 안전성 증명 가능한 암호에 대한 고찰

(On an Attack for a Provable Secure Cipher based on Chosen Differential Text)

Yukiyasu Tsunoo, Maki Yamada (NEC)

MISTY에서 차분 루트를 이용하여 FO와 FL 함수의 해독 가능성을 검토하여 FL함수를 포함한 최소단위인 FO함수 2단의 해독을 성공하였다. 그러나 8단 구조를 갖는 MISTY의 해독은 추후 과제이다.

Session 7.3 인증 방식

A) 문자열의 분류 규칙에 근거로 한 인증 방식의 고찰

(Authentication Scheme based on Classification Rules for Strings)

Minoru Chikamune, Ayumi Shinohara

(Kyushu U.)

패스워드는 한번 노출되면 위험한 점이 있는 것을 보완하기 위하여 문자열의 분류규칙을 대화형으로 질의하면서 인증을 시행하는 방법을 제안하였다.

B) 마우스를 이용한 서명에 의한 개인 식별 시스템의 제안

(A User Authentication System Using Signature Written with Mouse)

Fanar Syukri Agus, Eiji Okamoto (JAIST), Masahiro Mambo(Tohoku U.)

마우스로 서명한 정보로 개인 식별 방식을 제안하고 W/S 상에 실험 결과 종래의 87%에서 91%의 검증율이 향상되었다.

C) 곁눈 질에 강한 대화형 개인 식별 방식의 조작성 개선

(Improving the Usability of Interactive Human Identification Schemes)

Tsutomu Matsumoto, Nobuhiko Tsutsumi, Kiyoto Matsui, Akiteru Kamoshida, Hiromi Kubota(Yokohama Nat'l U.)

패스워드 방식에 비해 대화형으로 본인 인식을 하는 개인 식별 방식은 기억량과 조작성이 뒤떨어 진다. 이런 점을 개선한 새로운 방식을 제안하였다.

D) An Authentication Method with the Help of Simple Storage Devices

(간단한 보조기억 장치를 이용한 개인 인증법)

Keiji Amo, Yuichi Kaji, Tadao Kasami (NAIST)

자기 카드등의 저렴한 보조기억장치를 이용하여 간단하고 안전한 개인인증법을 제안하였다. 이 방식은 패스워드를 2개로 나누어 1개는 사용자가 1개는 보조기억장치에 기억시킨다.

보조기억장치의 내용은 암호화되고 사용할 때 랜덤하게 변하고 키 분배는 Diffie-Hellman프로토콜을 개량한 것을 이용한다.

D) 본인 인증의 평가 기준

(Evaluation Criteria of Personal Authentication)

Tomoyuki Suga, Haraku Misawa, Masahiro Azuma (ECOM)

ECOM에서 본인 인증의 평가 기준을 구축한 내용을 보고하였다. 평가 요인으로는 (1)사회적 인지성(2)이용자의 수용성(3)위협의 내성 (4)인식의 정확도 (5)편리성 (5)유지보수성이다.

Session 8.1 공개키 암호

A) Fast RSA-type Cryptosystem using n-adic Expansion

Tsuyoshi Takagi (NTT)

공개키가 n인 경우 n-adic 전개에 의한 2가지 RSA 형 공개키 암호시스템을 제안하였다.

암호문이 평문보다 1블럭이 증가하게되나 복호화가 빠르고 안전성은 기존의 RSA 암호와 동일하다고 주장하였다.

B) Pocklington 법을 이용한 안전한 RSA 키 발생법

(Generating Secure RSA-moduli with Pocklington Algorithm)

Kouichi Itoh, Kazuhiro Yokoyama, Naoya Torii, Masahiko Takenaka (Fujitsu)

(1) 반드시 소수를 생성 (2) p-1 /p+1 공격의 성공확률을 평가하여 안전성을 정량적으로 보증 (3) 반복 공격법에 최고로 강한 키를 발생이라는 장점을 갖는 Pocklington법을 이용한 RSA 비밀키 생성 방법을 제안하였다.

C) Church-Rosser SRS에 근거로 한 공개키 암호계의 키 생성에 관한 고찰

(On the Key Generation Method of the Public-Key Cryptosystem based on Church-Rosser String-Rewriting Systems)

Taizo Shirai, Kiyomichi Araki (TIT)

'95년 Oleshchuk가 제안한 Church-Rosser String Rewriting System을 근간으로 한 공개키 암호에 대한 개념을 설명하고 비밀키와 공개키 생성에 대하여 Knuth-Bendix의 completion 알고리즘이 유효하다는 것을 제시하였다.

D) 비선형 Knapsack 암호의 안전성에 관한 검토

(A Consideration on the Security of a Nonlinear Knapsack Cryptosystem)

Daisuke Nakamura, Yuji Tomuro, Kunikatsu Kobayashi (Yamagata U.)

SCIS'97에서 Hayashi가 제안한 비선형 Knapsack 암호의 안전성을 검토한 결과, LLL 알고리즘에 대하여는 안전하나, Shamir의 알고리즘에 의해 10차까지 해독이 가능한 수치 예를 제시하였다.

E) On the Security of the ElGamal Signature Scheme with Small Parameters

(적은 파라메터를 이용한 ElGamal 서명법의 안전성)

Hidenori Kuwakado, Hatsukazu Tanaka (Kobe U.)

ElGamal 암호를 적용 시 파라메터의 크기가 처리 속도를 좌우한다. modular p 에 대하여 난수의 크기가 $O(p^{1/2})$이하가 되면 주어진 서명문에서 비밀정보를 높은 확률로 구하는 방법을 제안하였다.

F) Bit Security of an Efficient Probabilistic Public-key Encryption

(효율적인 확률 암호의 비트 안전성)

Tatsuaki Okamoto, Shigenori Uchiyama (NTT)

저자가 이미 제안한 $n = p^2q$의 소인수 분해에 어려움을 가지는 공개키 암호에 대하여 p-부분군 문제 ($E(0) = h^r \bmod n$ and $E(1) = gh^t \bmod n$ is indistinguishable where r and t are uniformly and independently selected from Z/nZ) 가 어렵다는 가정하에 semantically secure한 확률적 암호의 안전성을 대하여 제안하였다.

Session 8.2 Digital Watermark(II)

A) 화상이나 음향 데이터를 dummy로 하는 대용량 Steganography 기술

-BCPS-Steganography의 제안

(A Large Capacity Steganography using Image and Acoustic Dummy Data - Proposal of BPCS-Steganography-)

Michiharu Niimi*, Hideki Noda*, Kouichi Nozaki(Nagasaki U.), Eiji Kawaguchi* (Kyushu Inst. of Tech.)

타인에게 비밀정보의 존재 자체를 알리지 않고 전달하는 심층 암호화 기법(Steganography) 기법으로 화상, 음성, 문자 등 임의의 전달 매체에 비밀 정보를 종래에 비하여 대량으로 삽입하는 BPCS(Bit Plane Complexity Segmentation)-steganography 기법을 제안하였다.

B) BCPS-Steganography 기술의 안전성에 관하여 검토

(A Study on the Security with BPCS-Steganography Technique)

Michiharu Niimi, Hideki Miyazaki, Tomohito Ei, Hideki Noda, Eiji Kawaguchi (Kyushu U. of Tech.)

저자들이 이미 제안한 BPCS-steganography의 안전성 즉, 제3자가 삽입된 정보를 의심 하는 정도에 대한 것을 실험적으로 검토하였다.

C) 음악 소프트웨어에 Digital Watemark의 방식

(Watermarking Technique for High Quality Audio Media)

Munetoshi Iwakiri, Kineo Matsui (National Defence Academy)

고품질 음악 정보를 스펙트럼 확산 후 LCT (Linear Cosine Transform) 변환하고 창 함수에 대응하는 신호 성분 중 특정 주파수 성분을 digital watermark 삽입에 이용하는 방법을 제안하였다.

D) 입체감을 이용한 2치 화상의 정보 비익법

(Visual Steganography for Binary Image Appearing with Stereogram)

Maya Yokoi*, Hironori Domen*, Akihisa Kodate**, Yoshiyori Urano**(TAO), Hideyoshi Tominaga*, **(Wasesa U.)

2치 화상 texture를 stereogram의 원리를 이용하여 작성된 texture를 치환함에 의해 부 정보를 삽입하고 삽입한 정보가 1번 보면 잘 보이지는 않지만 삽입 장소를 아는 사람은 해당 부분을 입체화하여 봄으로 하여 읽을 수 있도록 하는 방법을 제안하였다.

E) Peano 주사에 의한 화상의 서명과 Digital Watermark

(Digital Watermark and Signature onto Multi-level Images by Peano Scan)

Takahiro Nakazato, Kineo Matsui (National Defense Academy)

다단조 디지털 화상 정보의 저작권을 명시하기 위하여 Peano 주사를 이용하여 서명과 동시에 서명 정보를 화상내 digital watermark로 삽입하는 방법을 제시하였다.

F) 동화상에 적합한 Digital Watermark에 관한 2,3 고찰

Hiroyuki Inaba, Masao Kasahara (Kyoto Inst. of Tech.)

MPEG 동화상 정보에 digital watermark 삽입 수단으로 ID정보를 활용하는 법을 추가적으로 제안하였다.

Session 8.3 프로토콜 안전성 / 영 지식 증명

A) On Decision Problem for Existence of Forgeable Data in the Infinite Set of Data-An Extended Sufficient Condition for the Decidability-

(답장 위조 불가능성 판정 문제에 대하

여 - 위조조건이 무한개의 경우 충분조건의 확장-)

Maki Yoshida, Toru Fujiwara (Osaka U.)

위조 불가능성을 확인하기 위하여 의미가 없는 행동과 그 인수가 있는 성질을 만족할 때, 의미가 없어지도록 행동을 기술하는 형식화 방법을 제안하였다.

B) Modeling and Security Verification of Real-time Cryptographic Protocols

(시간 개념을 포함한 암호프로토콜의 모델링과 안전성 검증에 대하여)

Takehiko Tanaka, Yuichi Kaji, Hajime Watanabe, Toyoo Takata, Tadao Kasami(NAIST)

암호 프로토콜의 안전성을 검증 방법으로 시간을 이용한 rewriting 방식에 의한 프로토콜의 결함을 검출하는 방법을 제시하였다.

C) A Sufficient Condition under which Security Decision Problem for Cryptographic Protocols is decidable in Polynomial Time

(암호프로토콜의 안전성 판정문제가 다항식 시간에 결정가능하기 위한 충분조건)

Masaya Maeda, Hajime Watanabe, Tadao Kasami (NAIST)

안전성 판정 문제는 암호프로토콜의 항의 집합과 항의 개정 규칙을 형식화하여 안전성을 적대자의 목표를 나타내는 2개 항의 의미론적 단일화 문제로 귀착된다. 이을 이용하여 안전성 판정 문제의 결정 가능성에 대한 충분조건을 제시하고 다항식 시간 내에 안전성을 판정하는 알고리즘을 제시하였다.

D) Contract Signing Protocol and Divisibly Checkable Zero-Knowledge Interactive Proof

(계약 문서 교환 프로토콜과 분할 검정 가능한 영 지식 프로토콜)

Kazuo Ohta, Atsushi Fujioka, Hiroki Ueda

분할 검증 가능한 영 지식 프로토콜을 이용하여 고차 Fiat-Shamir 인증법에 적용하고 Even-Goldreich-Lempel이 제안한 계약문서 교환 프로토콜에의 응용을 제시하였다.

E) A New Definition of Witness Hiding Protocols

(WH 프로토콜의 새로운 정의에 관하여)

Satoshi Hada, Toshiaki Tanaka (KDD)

3라운드로 프로토콜이 종료되는 WH 프로토콜의 새로운 정의를 제시하고 Blum의 영지식 프로토콜의 병렬판이 WH 프로토콜이 되기 위한 필요충분조건을 제시하였다.

F) Zero-Knowledge Proof Systems for NP Based on Self-Definable Claw-Free Functions

(자기 정의 가능한 Claw-free 함수를 근간으로한 NP 언어의 영지식 증명시스템의 구성에 대하여)

Takeshi Koshiba(Fujitsu)

자기 정의 가능성이라는 개념을 Claw-free 함수에 도입하여 이러한 함수족을 이용한 NP언어에 대하여 일정 라운드의 영지식 증명 시스템을 제안하고

Goldreich-Kahan의 영지식 프로토콜의 라운드 수를 줄일 수 있어 4라운드로 증명이 가능하다고 하였다.

Session N. Night Session

1) 이스라엘 방문기(A Visit to Weizmann Institute of Science and Israeli Security Firms)

Takashi Mano(IPA)

민간 기업간의 교류를 목적으로 러시아, 이태리, 이스라엘, 프랑스를 방문한 프로그램 중 이스라엘의 Weizmann 연구소를 비롯한 Security 회사 (Softchip, Fortress, Algorithmic Research, Checkpoint, NDS, Cubital)를 방문한 결과를 보고하였다.

2) 국제회의 보고

A) SAC'97 참가 보고 (A Report on SAC'97)

Takashi Satoh(TIT), Kazumaro Aoki(NTT), Shiho Moriai, Yasuyoshi Kaneko(TAO), Kouichi Itoh(Fujitsu)

'97년 8월 11일부터 12일까지 캐나다의 Carleton 대학에서 개최한 SAC'97 (Workshop on Selected Areas in Cryptography)에 참가하여 Efficiency in Cryptographic System, Symmetric Cipher Design and Implementation, Protocols and Techniques for Web Security라는 주제 관련 워크샵의 내용을 소개하였다. 논문 내용은 http://adonis.ee.queensu.ca:8080/sac/에 전문이 게재되어있다.

B) 국제회의 보고 (ACISP'97, ISW'97, NSPW'97)

Masahiro Mambo (Tohoku U.)

'97년 7월 7일부터 9일까지 호주의 시드니 근교 Windsor에서 개최된 ACISP'97(Australasian Conference on Information Security and Privacy), '97년 9월 17일부터 19일까지 JAIST에서 개최된 ISW'97(Information Security Workshop), '97년 9월23일부터 26일까지 영국의 호수지역, Great Langdale에 개최된 NSPW'97(New Security Paradigm Workshop)에 대하여 참가 결과를 보고하였다.

C) ICICS'97

Tatsuaki Okamoto(NTT)

'97년 중국 북경의 Friendship 호텔에서 '97년 11월 11일부터 14일까지 개최된 ICICS'97 (International Conference on Information and Communications Security)의 참가 결과를 보고하였다.

D) JW-ISC'97

Kanta Matsuura(U. of Tokyo), Kazuo Ohta (NTT)

'97년 10월 26일부터 28일까지 서울 Sofitel Ambassabor 호텔에서 개최된 JW-ISC'97 (1997 Korea-Japan Joint Workshop on Information Security and Cryptology)에 대한 참가 결과를 보고하였다.

Session 9.1 구현

A) 비밀 키 암호 MISTY1의 H/W 구현에 관한 방법

(An Implementation of MISTY1 for H/W Design)

Tetsuya Ichikawa, Junji Katoh, Mitsuru Matsui (Mitsubishi)

MISTY1의 핵심 부분을 H/W로 구현 결과 5,000개 Gate 정도로 가능하고 제어부 및 확장키 부분을 추가하면 8,000개 Gate로 구현이 가능함을 제시하였고 추후 정합회로, 사용 모드의 추가 등이 과제로 남아있다.

B) MISTY의 소프트웨어에 의한 고속실현법에 대하여 (II)

(Fast Software Implementations of MISTY (II))

Junko Nakajima, Mitsuru Matsui (Mitsubishi)

MISTY의 S/W 구현 방법으로 500KB 정도의 사전 계산 테이블을 만들어 실행 명령을 축소하고 Pentium, PentiumPro, Pentium II, PA-RISC등에 구현하였다. 특히, 64비트 CPU인 PA-8200(236MHz) 상에서 어셈블리 언어를 혼용하여 8라운드 MISTY1을 111Mbps 속도를 얻었다고 보고하였다.

C) DSP를 이용한 RSA 암호의 구현

(Fast Implementation of RSA Encryption Algorithm on a Digital Signal Processor)

Masahiko Takenaka, Kouichi Itoh, Naoya Torii, Shouji Temma, Yasushi Kurihara (Fujitsu)

TI사의 최신 DSP 인 TMS320C6x를 이용하여 RSA 알고리즘을 구현한 결과, 중국인의 나머지 정리를 이용하고 1024비트 1회 RSA 서명 시 11.7msec 가 소요되었다고 보고하였다.

D) The Contact-less Smart Card : A Next Standardized Security Device Dedicated to Cryptology

(비접촉 스마트 카드 - 안전한 암호통신을 위한 차세대 표준 디바이스)

Michael W. David (Cubic Co.), Kouichi Sakurai (Kyushu U.)

현재의 접촉식 카드에서 암호 통신을 위하여 점차 지하철 및 버스 카드 등 응용이 확대되리라고 예상되는 비접촉식 스마트카드에 대하여 소개하였다.

E) 범용성을 고려한 고속 암호 라이브러리의 개발과 평가 (2)

(A High-Speed Cryptographic Toolkit on Multi-Platforms (2))

Hidenori Ohta, Takeshi Chikazawa, Mitsuru Matsui (Mitsubishi)

C 또는 BASIC 언어에서 쉽게 이용할 수 있는 암호 알고리즘, 디지털 서명 방식 등의 주요 프리미티브를 라이브러리화한 개발 결과를 보고하였으나 기존의 Crypto API 관련 표준과는 별도로 진행하였다.

Session 9.2 소프트웨어 보호

A) 프로그램에 Digital Watermark를 삽입하는 방법

(A Watermarking Method for Computer Programs)

Akito Monden, Hajime Iida, Ken-ichi Matsumoto, Koji Torii(NAIST), Yuuji Ichisugi (Electro. Lab.)

C, C++, Java 언어로 기술된 실행 파일을 보호하는 방식으로 컴파일 전에 실행되지 않는 부분에 watermark를 삽입하고 컴파일한 후, 실행프로그램 중 watermark 삽입부의 기계어 코드를 변

경함으로 하여 삽입위치 검지가 어렵고 사용자에 의한 제거 및 위조를 방지할 수 있는 방법이다.

B) 서버의 부정행위도 방지하는 부정 복사 방지 시스템

(A Watermarking System which can also Detect Server's Corruption)

Nobuharu Miura, Hajime Watanabe, Tadao Kasami (NAIST)

부정적인 디지털 정보의 복제를 방지하기 위하여 저작자가 직접 watermark를 삽입할 수 있도록 하여야 한다. 그러나 저작자와 서버간에 공동으로 digital watermark를 삽입시 대화형으로 행하여 서버의 부정행위를 방지하도록 하였다.

C) 소프트웨어 보호에 관한 한가지 제안

(A Proposal for Software Protection)

Naoto Hirose, Eiji Okamoto(JAIST), Masahiro Mambo (Tohuku U.)

소프트웨의의 저작권보호 방법으로 개조하기 어려운 저작자의 ID 정보를 삽입하는 방법을 제안하였다.

D) Java로 기술한 프로그램에 관한 Digital Watermarking 방법

(Digital Watermark for Java Programs)

Takashi Kitagawa, Yuichi Kaji, Tadao Kasami (NAIST)

네트워크를 통하여 분배하는 소프트웨어를 Java 언어로 digital watermark를 제작법으로, 배열기구를 이용하여 삽입하고 컴파일한 실행형식의 클래스 파일을 해독하기 어렵게하여 분배하는 방식이다.

E) Postscript 및 PDF 문서에 대한 Digital Watermark의 제안

(Digital Watermark for Postscript and PDF Document)

Ryujiro Shibuya, Yuichi Kaji, Tadao Kasami (NAIST)

화상 정보의 redundancy를 이용하여 digital watermark 정보를 삽입하는 데 반하여 Postscript나 PDF(Portable Document Format)에 추가 정보를 삽입하여 digital watermark를 만들 수 있는 방법을 제안하였다. 현재 PDF 파일에는 MD-5와 RC-4를 접근 제어 용으로 사용하고 있다.

Session 9.3 암호 시스템/ 표준화

A) 2차원 바코드 응용의 시큐리티

(A Security Consideration of Two-Dimensional Bar Code Application)

Tetsuji Kobayashi (Nippon Inst. of Tech.)

1차원 바코드와 달리 수직과 수평 방향으로 정보를 기억하는 2차원 바코드를 응용하는 경우 암호화, 인증,키 관리등에 대한 기본적인 내용을 고찰하였다.

B) 인터넷에 의한 성적 공개

(Opening Student's Records on Internet)

Kazuhisa Takagi(Kochi Nat'l College of Tech.), Kyouhei Murayama (Kansai U.)

대량의 인쇄물에 의하여 배포하는 수능시험 결과 등을 경비 절감을 위하여 인터넷을 통하여 암호화하여 성적 배포 방법을 제안하고, 39명의 학생을 대상으로 타원곡선암호를 Javascript로 구현

실험한 결과를 보고하였다.

C) 매크로 바이러스의 대책과 그 프랫트 홈의 검증

(Anti Macro-Virus and Inspection of the Platforms)

Yasushi Sengoku, Hirofumi Momoi, Shimmi Hattori (Kanazawa Ins. of Tech.)

종래의 바이러스 보다 고속이고 넓게 확산되는 특정 응용 프로그램용 문서 파일에 감염하는 매크로 바이러스에 대한 대책으로 각종 응용 프로그램의 안전성을 검증 및 평가 지표를 제안하였다.

D) WWW 데이터 한정 배달 시스템의 구축(Conditional Access WWW System)

Yasuo Okumura, Shunji Harada (Matsushita Ele. Ind.), Takeshi Saijyo, Takatoshi Ono(Matsushita Inf. Sys.)

네트웨크와 WWW browser사이에 복호 proxy를 설치하여 WWW를 통하여 HTML 문서의 접근 통제 방식을 구현한 결과를 제시하였다.

E) AES (Advanced Encryption Standard)의 표준화와 그 배경

(Standardization of the Advanced Encryption Standard and the Background)

Masashi Une (Bank of Japan)

DES의 안전성이 약화됨에 따라 '97년 1월 미국 정부는 차세대 미국정부 표준 암호로 AES를 공모한다고 발표하였다. 이에 AES의 표준화 배경, 주요 조건, 평가 기준 등에 대하여 기술하였다.

Session 10.1 타원암호 (III)

A) 타원곡선 상의 Fermat Quotient Attack 및 Samaev 알고리즘의 구현과 수치적 검증

(Implementation and numerical consideration of elliptic curve Fermat Quotient Attack and Semaev Algorithm for ECDLP)

Nozomu Takeshita, Takakazu Satoh, Kiyomichi Araki (Tokyo Inst. of Tech.)

GF(p) 상에 위수가 p가 되는 anomalous 타원곡선상의 이산 대수 문제의 복잡도는 지금까지 $O(\sqrt{p})$이었는 데, Sakai등에 의하여 Fermat Quotient Attack 및 Semaev의 대수기하학적 방법으로$O((\log p)^3)$의 복잡도로 해가 구해지는 것을 증명함으로서, 다항식 시간 내에 특수한 타원곡선 암호는 해독이 가능하게 되었다. 이 2가지 방법을 구현한 결과 Pentium-Pro 200MHz상 gcc-2.7.2, 64MB 메모리, 수식처리 시스템 PARI를 사용하여 150 비트인 경우, Fermat Quotient attack 은 41.13초, Semaev에 의한 공격은 17.42초가 소요되었다고 보고하였다.

B) 안전한 타원곡선 암호의 구성과 그 구현

(Construction and Implementation of Secure Hyperelliptic Cryptosystems)

Yasuyuki Sakai, Hirokazu Ishizuka (Mitsubishi), Kouichi Sakurai (Kyushu U.)

초타원곡선의 Jacobi 다양체 상에서 이산대수 문제를 검토하기 위하여 genus g = 3,11이고 곡선 $C : v^2 + v = u^{2g+1}$에서 $J(C ; F_2n)$를 사용하는 초타원 곡선 암호를 제사하였다. 1024 비트의 RSA 암호, 160비트 타원 암호의 안전성과 동등한

$J(C ; F_2^{59})$, $C : v^2 + v = u^7$ $(g = 3)$을 Alpha 21164 (250MHz)에서 C 언어로 구현 결과 118msec가 소요되었다.

C) 타원곡선의 하드웨어 실장

(A Hardware Implementation of Elliptic Curve Cryptosystem)

Shigeki Yanagisawa, Kazuto Matsuo (Toyo Com. Equ. Co.), Jinhui Chao, Shigeo Tsujii(Chuo U.)

$GF(2^m)$상에 동작하는 타원곡선 ElGamal 시스템을 cyclotomic field 상의 다항식 기저를 이용하여 하드웨어를 개발 결과, 316 비트 타원 ElGamal의 경우 200 Kgate로 구현이 가능하였다.

D) 16비트 마이크로프로세서 상의 GF(p) 상의 타원 암호의 구현

(An Implementation of Elliptic Curve Cryptosystem over GF(p) on a 16-bit Microcomputer)

Toshio Hasegawa, Junko Nakajima, Mitsuru Matsui (Mitsubishi)

표수 p인 타원곡선 암호를 16비트 마이크로프로세서인 M16C (10MHz) 상에서 4KByte 메모리로 DSA 서명, SHA-1 처리 루틴을 구현하고, 결과 타원 DSA 서명 작성과 검증이 각각 150msec, 630msec가 소요되었다.

E) IC 카드에 있어서 타원곡선 암호의 고속화 방법

(Fast Elliptic Curve Signature Method on Smart Card)

Seiji Miyazaki, Soichi Furuya, Kazuo Takaragi (Hitachi)

coprocessor가 내장되고 IC카드용으로 사용되는 8비트 CPU(5 MHz), H8/3111 상에서 4.2 KByte code 메모리, 3.2 KByte data 메모리를 사용하여 160비트 타원곡선 DSA를 구현 결과 0.3초 이내에 처리가 가능하도록 하였다.

Session 10.2 Digital Watermark(III)

A) 화질 열화가 적고 결탁 공격에 강한 시각 암호

(A Coding Method for Collusion-secure Watermark and less Decline)

Jun Yoshida, Keichi Iwamura(Canon), Hideki Imai (U. of Tokyo)

화상 정보에 각 사용자 별로 고유 식별이 가능한 fingerprinting 정보가 삽입되어 보호하는 데, 사용자의 결탁에 의하여 화상 정보의 차이를 활용하는 결탁 공격을 방지하기 위하여 화상 열화가 적은 embedding coding 방법을 제안하였다.

B) 모든 결탁 사용자를 특정 가능한 화상 시각 암호법

(A Method of Image Watermarking Which can Detect All Illegal Users in Collusion)

Tetsuya Yamamoto, Hajime Watanabe, Tadao Kasami (NAIST)

사용자 ID 정보를 삽입한 화상 정보 보호 방식에서 사용자가 결탁을 하여 불법 복제물을 배포시 특정화가 되어 방지할 수 있도록 하는 digital watermarking 기법을 제안하였다.

C) Watermark 기술의 응용 : 일반 이용자의 협력을 이용한 해적판 데이터 적발 방법

(An Application System for Watermark Technique : A Protocol for Detecting Illicit Copy Image User's Browsing Operation)

Tatsuya Matsui, Youichi Takashima (NTT)

저작권을 보호하는 방법으로 사용자의 web browsing 기능을 활용하여 불법 복제물의 확인을 가능한 효율적인 프로토콜을 제안하였다.

D) Cell Pattern을 이용한 서명을 삽입하는 방법 확장

(Extension of Embedding Signature Using Cell Patterns)

Hye-Joo Lee, Ji-Hwan Park (Pukyong U.), Shuichi Itoh (U. of Electro-Comm)

기존에 디지털 정보에 서명을 삽입하는 방법으로 hardcopy 시 농암 정보를 발생하도록 하는 불법 복제 방지 방법을 제안하였다. 이 방법을 확장하여 서명을 2개의 화상 정보를 분할하여 삽입하고 2개의 정보를 합치면 서명 정보가 hardcopy 시에 나타날 수 있도록 확장하였다.

E) An Interactive Protocol for Image Fingerprinting

(Digital Fingerprinting을 위한 쌍방향 프로토콜)

Kensuke Baba (U. of Tokyo), Keichi Iwamura (Canon), Yuliang Zheng (Monash U.), Hideki Imai(U. of Tokyo)

판매자만이 디지털 정보에 fingerprinting을 첨가 가능할 때, 제3자가 판매자의 fingerprinting을 변조하여 판매시 선의의 사용자가 불법 복제품을 갖게 되는 피해를 입을 수가 있다. 이러한 문제를 방지할 수 있는 판매 프로토콜을 제안하였다.

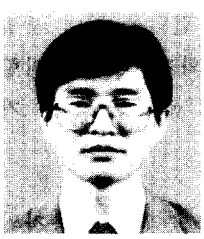
F) 2차 배포에 안전한 시각 암호 시스템

(Secure Digital Watermark Systems for Secondary Distribution)

Keiichi Iwamura(Canon), Kouichi Sakurai(Kyushu U.), Hideki Imai (U. of Tokyo)

서버를 신뢰할 수 없는 경우, 저작권자가 대리점에 배포하고, 대리점에서 사용자로 배포하는 2차 배포 시 부정을 방지하는 digital watermarking 시스템을 제안하였다.

□ 著者紹介



김 광 조(金 光 兆)

1973년 3월 - 1979년 2월 : 연세대학교 전자공학과 (공학사)
1981년 9월 - 1983년 8월 : 연세대학교 대학원 전자공학과 (공학석사)
1988년 4월 - 1991년 3월 : 요꼬하마 국립대 전자정보공학과 (공학박사)
1979년12월 - 1997년12월 : 한국전자통신연구원 부호1실장
1998년 1월 - 현재 : 한국정보통신대학원 정보공학부 부교수

※ 관심연구분야 : 정보보호와 암호학 이론 및 응용, M/W 통신