SCIS'99를 통한 일본의 정보보호기술 연구 동향

김 광조

요 약

1999년 1월 26일부터 1월 29일까지 일본의 고베시에서 태평양을 향한 매립지에 건설한 Portopia에서 개최된 SCIS(Symposium on Cryptography and Information Security)'99에 참석하여 일본의 정보보호 기술의 연구 동향을 분석하여 보고한다. 특히, 내년 SCIS2000은 오끼나와에서 한일 공동 워크샵을 병행하여 계획 중인 바 한국에서도 적극적인 참여가 요망된다.

Ⅰ. 개 요

본 학회는 이미 일본에서 1984년부터 매년 정기적으로 개최된 학술 발표회로 16번째인 금년도는 아래와 같이 개최되었다.

o 일시 : 1999.1.26. - 1.29.
o 장소 : 고베시 Portopia 호텔 국제회의장
o 주최 : 전자정보통신학회 정보 시큐리티 연구 전문위원회
o 협찬 : 일본전자정보통신학회 정보통신 기초 Sub Society
o 논문발표 : 3건의 특별 강연, 166건 논문 발표
o 참가자 : 400여명
o 한국인 참가자 : 김광조, 이병천(ICU), 이선영(동경대), 김일준(YNU), 기타 2명 (성균관대학원생)
o SCIS,2000은 2000년 1월 중 오끼나와에서 한일 공동 워크숍(JW-ISC2000)과 병행하여 추진하는 것으로 확정

Ⅱ. 발표내용

프로그램은 〈표 1〉 과 같이 편성 운영하였으며 발표 내용은 저자가 논문 발표에 참가한 논문에 대하여만 요약하고 기타 논문은 제목과 저자만 나열하였다.

1. 특별 강연(3건)

1)AES 암호에 대하여, Masayuki Kanta (NTT)

1997년 1월 NIST는 DES를 대체할 수 있는 차기 미국정부 표준 암호로서 AES의 제정에 과정에 있다. 후보는 세계에서 공모하여 공개 된 것 중에서 선택하는 방침에 의해 15개의 암호,CAST-256(Entrust,Cananda), Crypton (Future, Korea), DEAL(R. Outerbridge, L.Knudsen, Canada), DFC(CNRS, France), E2(NTT, Japan), Frog(TecApro, Costa Rica), HPC(R. Schroeppel, USA), LOKI97(L. Brown et al, Australia), Magenta(Deutsche Telekom, Germany), Mars(IBM, USA), RC6(RSA Lab., USA),

종신회원,
305-350 대전광역시 유성구 화암동 58-9 한국정보통신대학원 (ICU), 공학부
E-mail : kkj@icu.ac.kr

〈표 1〉 SCIS'99 프로그램 편성

1.26.(화)			
14:00-14:10	Opening Remark		
14:15-15:15	특별강연 I AES 암호에 대하여		
15:30-16:30	특별강연 II SPAM 문제와 인터넷 시큐리티		
16:45-17:45	특별강연 III 법조계에서 본 시큐리티와 프라이버시		
18:15-19:15	Opening Party		
1.27.(수)	Room 1	Room 2	Room 3
9:00-10:20	W1-1 공개키 암호(1)	W1-2 전자투표/전자입찰	W1-3 암호 이론
10:35-12:15	W2-1 암호 해석(1)	W2-2 네트워크보안(I)	W2-3 ID-based 암호
13:40-16:00	W3-1 타원 암호(1)	W3-2 Digital Watermark(1)	W3-3 해쉬함수/디지털서명(1)
16:15-19:15	W4-1 타원 암호(2)	W4-2 Digital Watermark(2)	W4-3 전자 현금
19:30-21:30	Banquet		
1.28.(목)			
9:00-10:20	T1-1 공개키 암호(2)	T1-2 키위탁/분배/복원	T1-3 비밀분산
10:35-12:15	T2-1 난수	T2-2 Digital Watermark(3)	T2-3 디지털 서명
13:30-15:30	T3-1 타원암호(3)	T3-2 네트워크 보안(3)	T3-3 프로토콜
15:45-17:45	T4-1 암호 해석(2)/설계	T4-2 Digital Watermark(4)	T4-3 인증 / 계산법
19:00-22:30	Night Session		
1.29.(금)			
8:30-10:10	F1-1 타원암호(4)	F1-2 구현	F1-3 키 분배/관리(1)
10:30-12:30	F2-1타원암호(5)	F2-2 표준화	F2-3 키 분배/관리(2)

Rijendael(J. Daemen, Belgium), Safer+(Cylink Corporation, USA), Serpent(R. Anderson et al), Twofish (B. Schneier, USA)이다. 각 알고리즘의 내부 주요 구조를 설계 방식에 따라 Feistel 형, 변형 Feistel 형, SPN 형 등으로 구분하고 구현 속도 등을 비교하였다. 2 라운드에서 5개를 선정하도록 되어있는 데 속도 및 지금까지의 해독 상황을 예측하여 선정 후보를 예측하였다.

2) SPAM 문제와 인터넷 시큐리티, Nakamura (Kyoto U.)

최근 급속한 인터넷의 보급과 대중화에 의해 인터넷의 이용에 관하여 여러 가지 문제가 발생하고 있다. 그 중의 하나로 SPAM 문제가 있다. SPAM은 주로 발산자가 이익이 되도록 선전 내용을 담은 전자 우편을 무차별하게 보내는 행위 또는 그 전자 우편 자체를 의미한다. 이렇게 SPAM이 발생하는 데 따라 메일 서버의 처리 시간, 기억 영역, 더욱이 네트워크의 대역이 쓸모 없이 이용되며 수신자는 우편을 읽기 위하여 필요로 하는 시간이나 접속 시간의 영향을 받고 있다. 따라서, 불필요한 SPAM에 대하여 실태와 SPAM의 방지 대책 등을 검토 결과를 소개한다.

3) 법조계로부터 본 시큐리티와 프라이버시 (인터넷 변호사 협회 대표)

불경기에도 불구하고 네트워크 이용자가 증가하고 있다. 이런 증가에 정보 인프라의 확충이 충분하지 못하고 네트워크가 global화에 따른 디지털 사회에서의 프라이버시를 보호하는 방법, 정보 범죄자의 형태 등을 소개하고 프라이버시 보호에 대한 법적 근거의 제정 필요성을 논하고 대책으로는 법적 근거보다는 기술적인 도구가 최선이라는 의견을 제시하였다.

2. 발표 논문

각 논문의 번호는 Session이 개최되는 요일에소 수, 목, 금의 영문 첫 자를 따서 W, T, F로 명명하고 이어서 일련 번호를 부여하였다. 그리고 논문 제목이 영문으로 기술되어 있는 논문은 영문으로 작성되어 있고, 그렇지 아니하면 일본어로 작성되어 있다.

W1-1 공개키 암호(I)
W1-1.1 합성수를 법으로 하는 이산대수문제를 이용한 공개키 암호, Kunikatsu Kobayashi (Yamagata U.)
W1-1.2 Lucas 계열을 이용한 공개키 암호 방식에 관한 고찰, Seiji Kobayashi, Toyokazu Hiramatsu (Hosei U.)
W1-1.3 $p^k q$ 법으로 하는 고속 RSA형 암호, Tsuyoshi Takaki, Shozo Naito, Yoshihiro Kumazawa (NTT)
W1-1.4 곱과 덧셈형 공개키 암호 2, 3 가지 방식, Masao Kasahara, Yasuyuki Murakami (Kyoto Institute of Technology)

W1-2 전자투표 / 전자 입찰
W1-2.1 표의 Shuffle을 이용한 새로운 전자 투표 프로토콜의 제안, Shita, Kobara , Imai (Tokyo U.)
지금까지 전자투표 프로토콜은 준동형 사상을 이용한 방식, Mixnet을 이용한 방식, Blind 서명을 이용한 방식 등 여러 가지가 제안되어 있다. 본 연구에는 ZKIP을 이용하지 않고 준동형 사상을 이용하고 표에 대하여 서명과 투표 내용을 분리하고 표의 shuffle을 이용하는 것에 의해 프라이버시를 유지하고 Universal Verifiability를 실현하는 방식을 제안한다. 본 방식은 프라이버시 보호를 위하여는 센터가 2개이면 충분하다. 그러나 센터의 부정에 대한 대책이 부족함이 지적되었다.

W1-2.2 전자 투표에 있어서 통신과 계산의 무증거성, Kouichi Sakurai (Kyushu U.)
지금까지 제안한 전자 투표 방식을 안전성, Fairness와 무증거성에 성질을 분류하고, 아날로그 투표 방식에서도 악용되는 투표권자가 자신의 투표 결과를 가지고 나가서 이용하는 Araki 공격에 대한 현재 방식들이 안전하지 못함을 지적하였다.

W1-2.3 VCA 모델에 의한 전자 투표 시스템의 제안
Shigeo Tsujii, Hiroshi Yamaguchi, Atsushi Kitazawa, Masaki Nagai, Kaoru Kurosawa(Chuo U.),

지금까지의 전자 투표 프로토콜은 안전한 다자간 프로토콜을 이용한 사례가 많다. 그러나 최근 인터넷의 보급에 따라 몇 가지 실험 시스템이 제안되어 있다. 이런 시스템은 투표자 V와 집계 관리자 A의 2가지 기관 모델이었다. 그러나 실제 시스템은 네트워크 상의 관리자로 ISP와 같은 Collector를 고려하여야 하는 VCA 모델에서 제안한 프로토콜을 ZKIP등을 포함한 실현 및 전자 survey에의 응용 예를 제시한다.

W1-2.4 낙찰 값이외에는 비밀로 하는 전체 검증 가능한 전자 입찰 방식, Kasuo Sako(NEC)
종래의 전자 입찰 방식에 있어서는 대부분이 낙찰치가 최대치 (또는 최소치)임을 나타내기 위하여 모든 입찰치를 공개하였다. 이런 방식은 누구의 입찰치가 비익되어도 참가자의 전략에 관한 정보가 누설되어 다음의 동일한 입찰에 영향을 준다. 본 제안 방식은 낙찰치 이외에는 입찰치는 비익을 하고 낙찰치만을 최대 (또는 최소)인 것을 누구도 검증할 수 있는 single term 전자 입찰 방식을 제안한다. 참가자의 익명성을 보장하는 것이 추후 과제이다.

W1-2.5 공개 게시판을 이용한 비밀 전략이 가능한 전자 입찰 방식, Shingo Miyazaki, Kouichi Sakurai (Kyushu U.)
응찰자의 프라이버시를 보호하고 담합에 의한 응찰 가격의 조작 방지를 위하여 DL 문제, 공개 게시판, 해쉬 함수를 이용하고 Convertible Undeniable Digital Signature 방식을 응용한 방식을 제안하였다.

W1-3 암호이론

W1-3.1 Self-Powering Function and its Application, Mitsuru Tada, Hisao Sakazaki, Eiji Okamoto (JAIST)

W1-3.2 A Construction of Trapdoor No-way Function, Eikoh Chida, Hiroki Shizuya (Tohuku U.)

W1-3.3 Pseudorandom Number Generation on Public Key Cryptosystems with Random Inputs, Takeshi Koshiba (Fujitsu Lab.)

W1-3.4 A Successive Carrier-transmission Model for Narrow-band Subliminal Channels, Kazukuni Kobara, Hideki Imai (Tokyo U.)

W2-1 암호 분석(1)

W2-1.1 Pseudorandomness and Maximum Average of Differential Probability of Block Ciphers with SPN-structures, Makoto Sugita (NTT)
SPN 구조와 E2 구조를 Ruby-Rackoff 방식에 의한 의사 난수성의 안전성 평가 방식을 시도하여 Known Plaintext Attack에 대한 안전성 증명을 시도하였다.

W2-1.2 공통키 암호에 있어서 차분/선형 공격법에 대한 통계적 강도 평가 방법의 검토, Yasuyoshi Kaneko (TAO)
블록 암호에서 사용되는 f 함수의 DC/LC에 대한 안전성을 평가하기 위하여 f 함수를 축소하여 평가하는 방법을 시도하였으나 축소하지 않은 실제의 f 함수와 동일성을 주장하는 데는 한계가 있음을 지적하였다.

W2-1.3 RC5⊕의 고차 차분 특성에 대하여
Atsuhiro Ohtaka, Toshinobu Kaneko (Science U. of Tokyo)
Carry Propagation이 생기지 않도록 RC5의 내부 연산 중 ⊞를 ⊕로 변경한 RC5⊕에 대하여 2차 차분 특성을 이용하여 half-round RC5⊕에 대하여 평문 쌍이 $2^{-25.7}$의 확률로 존재하는 것을 확인하였다.

W2-1.4 SERPENT-FSE 버전 AES 버전의 강도 비교,
Jun Yajima, Takeshi Shimoyama (TAO), Shigeo Tsujii (Chuo U.)
DES의 S-box를 그대로 이용하는 SERPENT-FSE와 새로운 S-box를 이용하는 SERPENT-AES에 대하여 24라운드까지의 DC와 LC 특성을 평가한 결과 SERPENT-FSE는 2^{-116}, $1/2 \pm 2^{-45.8}$, SERPENT-AES는 2^{-232}, $1/2 \pm 2^{-109}$로 AES 판이 FSE보다 강하는 것을 알 수 있었다.

W2-1.5 Byte-oriented 암호의 강도 평가에 관한 고찰, Tokita, Matsui (Mitsubishi)
byte-oriented의 블록 암호의 안전성 평가 방법으로 bytewise DC라고 하는 해독 방법을 도입한다. 입/출력 데이터를 byte 단위로 취급하므로 차분이 있을 때 1, 없을 때 0으로 하여 부호화한 byte characteristic을 정의하고 IT 및 FT가 없는 8단 E2에 대하여 subkey를 찾아내는 데 가능하다는 것을 제시하였다.

W2-2 네트워크 시큐리티 (1)

W2-2.1 멀티미디어 정보 부분 암호화 시스템, Hirokazu Okano (Hiroshima Denki U.), Akira Shoizaki (Osaka Pref. U.), Yasuaki Tanaka, Kazuhisa Yamamoto, Hideki Imai(Tokyo U.)

W2-2.2 시큐리티를 고려한 원격 로그인 시스템의 구축, Ippei Shimura, Wakaha Ogata, Hitoshi Sakagami, Yutaka Takahashi (Himeji U.)

W2-2.3 최대한의 비익이 가능한 전자 메일 시스템의 구축, Masako Wakabayashi, Wakaha Ogata, Hitoshi Sakagami, Yutaka Takahashi(Himeji U.)

W2-2.4 S/MIME 자동 응답 시스템의 실장에 대하여, Yuji Suga, Shigeichiro Yamasaki, Keijiro Araki(Kyushu U.)

W2-2.5 인터넷에 있어서 암호 데이터 회복 시

스템의 시작, Fumihiko Sano, Tatsuya Ishihara 외 6인 (Toshiba)

W2-3 ID-Based 암호

W2-3.1 RSA-ElGamal like Identity-based Cryptosystems, Hatsukazu Tanaka (Kobe U.)

W2-3.2 제4의 키 공유방식 - 확장 ID-NIKS의 제안,
Shigeo Tsujii (Chuo U.), Yasuyuki Murakami, Masao Kasahama (Kyoto Inst. of Tech.)

W2-3.3 확률적인 키공유 가능한 지수형 ID-NIKS, Yasuyuki Murakami, Masao Kasahama (Kyoto Inst. of Tech.)

W2-3.4 ID 정보를 기반으로한 예비 정보 불필요한 확률적 키 공유법의 안전성 평가, Tomoya Ishikawa, Ryuichi Sakai (Osaka Elec. Comm. U.)

W2-3.5 Identity-based Fault-tolerant Key Distribution System, Takeshi Okamoto, Mitsuru Tada, Eiji Okamoto (JAIST)

W3-1 타원곡선(1)

W3-1.1 Construction of Elliptic Cryptosystems Using Supersingular Liftings, Takanori Nakamizo, Kohji Sobataka, Jinhui Chao, Shigeo Tsujii (Chuo U.)

유한체 상에서 초타원 곡선의 canonical lifting을 통하여 CM 타원 곡선을 구성하는 방법을 취급한다. supersingular와 bad reduction에 의한 타원 곡선의 lifting은 2차 확장체 상에서
만 동작하므로 이점이 있고 타원 곡선 암호 시스템에의 응용을 논한다.

W3-1.2 Construction of Elliptic Cryptosystems Using Ordinary Liftings, Mitsuo Hosoya, Kohji Sobataka, Jinhui Chao, Shigeo Tsujii (Chuo U.)

유한 체 상에서 타원 곡선의 Deuring lift 또는 canonical lifting 알고리즘에 대하여 논한다. Kohel의 알고리즘과 합쳐서 유한체 상에 ordinary 타원 곡선의 endormorphism ring의 isomorphism 형태를 결정하게 한다. 이 알고리즘의 복잡도는 타원 곡선의 endormorphism ring의 class number의 다항식 시간임을 제시하고 타원곡선 암호의 효율적인 설계에 이용되는 것을 기대한다.

W3-1.3 A Family of Supersingular Hyperelliptic Curves Suitable for Public-Key Cryptosystems, Kouichi Sakurai (Kyushu U.), Iwan Duursma (U. of Limoges)

odd characterisitc p의 유한체 $GF(p^n)$ 상에서 $y^2=x^p-x+1$방정식에 의해 결정되는 초타원 곡선의 jacobian (class number)으로부터 이산 대수 문제를 조사한다. Koblitz가 DSA을 genus가 1인 초타원 곡선에서 표수 3에서 구현한 것을 임의의 표수 $p\geq 5$에서 유한체 상에서 가능함을 제시한다.

W3-1.4 On Lifting of CM Hyperelliptic Curves, Kazuto Matsuo (Toyo Comm. Equ.), Jinhui Chao, Shigeo Tsujii (Chuo U.)

CM 초타원 곡선의 lifting을 위하여 유한체 상의 초타원 곡선의 Jacobian 다양체의 endomorphism 형태를 계산하는 알고리즘을 제시한다. Kohel이 유한체 상에서 ordinary 타원 곡선의 endomorphism 형태를 계산하는 알고리즘을 확장한 것이다.

W3-1.5 초타원곡선 암호의 효율에 대하여 - $J(F_p)$와 $J(F_{2^n})$의 S/W 구현에 비교, Yasuyuki Sakai(Mitsubishi), Sakurai (Kyushu U.)

초타원 곡선의 Jacobian 군의 이산 대수 문제를 이용한 공개키 암호시스템에서 소수 체 F_p 상의 안전한 Jacobian군을 탐색하여 Alpha 21164A(467HMz)와 Pentium II (300MHz)의 C언어로 S/W 구현을 하였다. 또한, F_{2^n} 상과 F_p 상의 Jacobian 군의 속도 효율을 평가하였다. 타원 곡선군과 비교하여

정의체의 크기가 작아지는 성질을 이용하여 구현 CPU 의 워드 크기를 고려하여 Jacobian 군을 선택하였다. genus g=6의 곡선 F_p (p=29 비트 소수) 상의 Jacobian 군 $J(F_p)$ 의 임의 점의 전수 배 연산에 Pentium II(300MHz)에 있어서도 실용적 속도 176 ms가 소요되었다.

W3-1.6 A Fast Algorithm of Model Lifting for CM Hyperelliptic Curves, Kazuya Kamio, Hiroto Kawashiro, Jinhui Chao, Shigeo Tsujii (Chuo U.)
작은 유한 체 상에서 supersingular abelian variety로 lifting하는 알고리즘을 제시한다.

W3-1.7 어떤 대수 대응을 이용한 Jacobian의 정수배 계산법에 대하여, Takashima
초타원 곡선에 있어서 연산 시간의 감축을 위하여 임의의 초타원 곡선족에서 구체적으로 주어진 대수 대응을 Jacobian의 준동형 사상을 이용하고 새로운 정수배 연산법을 제안한다. 결과 Jacobian의 2배수는 기존에 비해 약 1/2 계산량으로 가능하다.

W3-2 정보은닉법(1)
W3-2.1 정보은닉법에 있어서 평행 이동 / 절취의 내성 향상을 한 가지 방법, Takao Nakamura, Hiroshi Ogawa, Atsuki Tomioka, Youichi Takashima (NTT)
W3-2.2 결탁 공격에 강한 정보 은닉법의 제안, Tadashi Kato, Atsushi Nagasaka(Oki Denki)
W3-2.3 Laplacian 공격법을 고려한 아산 코사인 변환에 의한 정보 은닉법의 한가지 방식
Takahiro Nakazato, Kineo Matsui (National Defence Academy)
W3-2.4 Game-theoretic Analysis of Jamming Attacks on Watermarks in Digital Still Images, Markus Breitbach, Hideki Imai (U. of Tokyo)
W3-2.5 Stirmark 공격에 내성이 있는 화면에 정보 삽입 방법에 관한 방법
Jino Tanimoto, Akira Shiozaki (Osaka Pref. U.)
W3-2.6 Evaluation of a Watermarking Scheme based on Steerable Pyramid, Takuo Mori, Hideki Imai (U. of Tokyo)
W3-2.7 정보은닉법에의 공격에 관한 2,3 가지 고찰,
Takayuki Yamada, Kineo Matsui (National Defence Academy)

W3-3 해쉬함수 / 디지털 서명 (1)
W3-3.1 A New Hash Function using Probability Distribution, Sun-Young Lee, Hideki Imai (U. of Tokyo)
W3-3.2 nMBL-HASH (New Multiblock Algorithm for Hash)
Kouzou Hirata (Laurel Bank Machine)
W3-3.3 On the One-Wayness of the Reduced MD4 Compression Function, Hidenori Kuwakado, Hatsukazu Tanaka (Kobe U.)
W3-3.4 ElGamal 서명을 이용한 검증자 안정 서명과 부인불가 서명
Shunsuka Araki, Satoshi Uehara, Kyoki Imamura(Kyushu Ins. of Tech.)
W3-3.5 A Protocol to Detect Who has leaked a Signed Document, Kensuke Baba (U. of Tokyo), Keiichi Iwamura (Canon Inc.), Yuliang Zheng (Monash U.), Hideki Imai (U. of Tokyo)
W3-3.6 Improvement of Security Using the Combination of Two Authenticated Random Numbers, Yuji Watanabe, Hideki Imai (U. of Tokyo)
W3-3.7 KPS 인프라에 기반을 한 디지털 서명 스킴, Tsuyoshi Nishioka, Hideki Imai (U. of Tokyo)

W4-1 타원암호 (2)
W4-1.1 타원곡선 암호의 연산법에 대하여, Izu Tetsuya (Fujitsu Lab.)
W4-1.2 Fast Computation of Elliptic Curve Cryptosystems, Kenji Takeuchi (Kyoto U.), Kenji Koyama (NTT)
W4-1.3 y 좌표를 필요로 하지 않는 타원 서

명법의 연산법, Kiyoshi Ohgish, Ryuichi Sakai, Masao Kasahara(Kyoto Int. of Tech.)
W4-1.4 Elliptic Curve Algorithm on OEF with Frobenius Map, Tatsutaro Kobayashi, Kazumaro Aoki, Hikaru Morita, Kunio Kobayashi, Fumitaka Hoshino (NTT)
W4-1.5 Optimal Extension Fields에 대한 Frobenius 작용에 대하여,
Taiichi Saito (TAO), Tetsutaro Kobayashi (NTT)
W4-1.6 Fast Scalar Multiplication over Elliptic Curves Using Frobenius Expansions, Yuko Tsuruoka, Kenji Koyama (NTT)

W4-2 정보은닉법 (2)
W4-2.1 MPEG 동화상에 적합한 정보은닉법의 성능에 관한 2,3 가지 고찰, Hideyuki Kakuno, Hiroyuki Inaba, Masao Kasahara (Kyoto Ins. of Tech.)
W4-2..2 MPEG 스트림으로 검출 가능한 동화상 정보 은닉법의 검토, Shigeyuki Sakazawa, Satoshi Hada, Yasuhiro Takishima, Masahiro Wada (KDD)
W4-2.3 압축 동화상에 적합한 정보 은닉법의 방법, Akihiko Kusanagi, Hideki Imai (U. of Tokyo)
W4-2.4 A Digital Watermark Method Using the Wavelet Transform for Video Data, Hisashi Inoue*, Akio Miyazaki+, Takashi Arak+(Kyushu U.), Takashi Katsura* (Matsushita)
W4-2.5 신뢰성을 기반으로 한 동화상 정보 은닉법의 추출 방법, Hiroshi Ogawa, Takao Nakamura, Atsuki Tomioka, Youichi Takashima (NTT)
W4-2.6 정보은닉법을 이용한 고유 정보 삽입에 의한 동화상의 재편집 검출 방식
Kazuki Takeuchi*, Akihisa Kodate(TAO), Yoshiyori Urano*, Hideyoshi Tominaga*(Waseda U.)
W4-2.7 음성에의 정보은닉 변수의 최적화에 대하여
Atsuki Tomioka, Hiroshi Ogawa, Takao Nakamura, Youichi Takashima (NTT)
W4-2.8 패치워크와 이산 코사인 변환을 이용한 정보 은닉법
Hiroyuki Kii, Junji Onishi, Sinji Ozawa(Keio U.)
W4-2.9 패치워크에 의한 정보은닉법의 개량
Arata Sato, Junji Onishi, Shinji Ozawa(Keio U.)

W4-3 전자 화폐
W4-3.1 전자 축구 복권에 관한 고찰,
Takanori Nakanowatari (U. of Electro-Comm.), Hikaru Morita (NTT)
축구 복권의 전자화를 예상하여 인터넷 상에 적합한 방식을 제안한다. 전자 투표 등에 대하여 디지털 서명 등 공개키 암호 알고리즘을 기반으로 여러 가지 방식이 제안되었으나, 전자 축구 복권의 경우 구입이 불특정 다수가 대량으로 구입하리라고 예상되므로 연산량과 통신량이 적어야 한다. 인터넷 상에 공공 게시판을 설치하여 주최자나 판매자에 의한 부정 행위를 방지하고 당선자의 프라이버시를 유지하고 TTP가 불필요한 방식을 구축이 가능하였다. 그리고, 99년 3월부터 http://ntt.ohta.is.uec.ac.jp/에 시범 서비스를 예정하고 있다.

W4-3.2 분할된 티켓의 지불 이력의 관계를 불가능하게 하는 전자 쿠폰 티켓 프로토콜,
Toru Nakanishi, Nobuaki Haruna, Yuji Sugiyama(Okayama U.)
전자 현금 프로토콜에서는 안전성에 추가하여 임의의 2개의 지불 내력에서 한사람의 지불이력을 알 수 있게 하는 관련성 불가능이 필요하다. 이런 성질을 만족하는 것을 전자 쿠폰 티켓 프로토콜이라고 부른다. 이 프로토콜은 은행에서 인출한 1개의 티켓이라고 부르는 전자 현금을 이미 결정된 금액의 서브 티켓이라고 부르는 전자 현금으로 분할하여 이용할 수 있다. 양도성에 대한 부가 기능을 제시하였으나 이는 프라이버시하고는 상반된 조건이 되지 않는 가에 대한 질의가 있었다.

W4-3.3 Study on a New E-cash System Using Two Blind Signatures, Koji Hirohashi, Mitsuru Tada, Eiji Okamoto (JAIST)
SCIS98에서 Miyazaki와 Sakurai이 제안한 전자 현금 프로토콜에서 전자 현금의 위조 방식을 제시하고 Schnorr의 디지털 서명 및 Schoenmaker (ftp://ftp.cwi.nl:/pub/CWIreports/AA/CS-R9522.ps.Z)에서 제시한 Blind Signature
SCIS97에서 Abe등이 제안한 Partially Blind Signature를 이용한 전자 현금 프로토콜을 설계하였으나 표현되는 전자 현금이 금액 정보로만 한정해야 하여야 사용자의 프라이버시가 노출되지 않으므로 주의하여야 한다는 지적이 있었다.

W4-3.4 전자화폐 시스템에 있어서 내부 관리자의 부정에 관한 고찰,
Shingo Miyazaki, Kouichi Sakurai (Kyushu U.)
전자 현금에 있어서 관리자가 정당한 사용자를 동시에 이중 사용하여 공격하는 parallel attack에 대하여는 Ferguson93 방식과 Schoenmaker95의 방식은 방지가 가능하나 저자 등이 제안한 ISEC98-45 방식에는 위험성이 있음을 제시하였다.

W4-3.5 비동기 대화에 의한 전자 화폐의 양도 방법에 관하여,
Hideki Akashika, Hidemi Moribatake (NTT), Yasushi Nakayama (일본은행 금융연구소)
지불자와 수령자간에 On-line 접속이라는 가정 없이 전자 현금을 양도 가능한 프로토콜을 제안하고 전자 현금을 전자 우편으로 첨부하는 방식과 같이 하여 타 이용자에게 보내는 방식을 IC 카드를 이용한 시스템을 구현하고 문제점과 대책을 논하였다. 또한 시스템은 99년4월부터 http://www.icash.gr.jp에서 실험을 준비하고 있다.

W4-3.6 복수의 수령자에 지불이 가능한 전자 현금 시스템, Shinichiro Matsuo, Hidemi Moribatake (NTT)
전자 현금의 사용자가 복수의 수령자를 지정할 경우를 전자 현금 프로토콜을 제안하였다. 특징으로 (1) 지불자는 각 수령자의 수령 금액을 알 필요가 없다. (2) 수령자 간에는 서로 수령액을 알 필요가 없다. (3) 수령자의 수가 증가하여도 지불자가 행하는 프로토콜의 변경이 없다는 특징을 가지고 있다.

W4-3.7 전자 인지 시스템의 설계와 제작, Atsushi Shimbo, Takehisa Kato, Toshiaki Saisho(Toshiba)
관공서 등에서 시행하고 있는 신청 서류에 붙이는 증지를 전자화하는 데 따른 방식으로 Prepaid 형 IC 카드를 매체로 하고 암호 기법을 응용한 전자 인지 시스템의 설계와 제작한 결과를 제시하였다.

W4-3.8 종이 증서의 부분적 전자화와 시큐리티, Tetsuji Kobayashi (Nippon Inst. of Tech.)
전자 우표나 전자 상품권 등과 같은 종이 증서의 인터넷을 통한 판매가 이루어 질 때 2차원 바코드와 디지털 서명 등의 암호와 인증 기술을 응용하는 벙법을 제안하였다.

W4-3.9 전자 상거래의 보급에 있어서 시큐리티 기술의 과제, Hidekazu Tsuji, Toshio Gomi(ECOM)
전자 상거래 시스템에서 시큐리티를 확보하기 위하여 위험성 분석을 위한 여러 가지 위협과 시큐리티 기능간의 관계, 사용의 용이성과 시큐리티 레벨 등에 대하여 분석하였다.

T1-1 공개키 암호(2)
T1-1.1 RSA 암호 상의 법 변환과 그 응용에 관하여, Takeru Miyazaki, Shunsuke Araki, Satoshi Uehara, Kyoki Imamura(Kyushu Inst. of Tech.)
T1-1.2 Itoh-Okamoto-Mambo에 의한 고속 처리 가능한 공개키 암호 방식의 개량,
Takayuki Uchihira, Shunsuke Araki, Satoshi Uehara, Kyoki Imamura (Kyushu Inst. of Tech.)
T1-1.3 내성이 있는 threshold 값을 가진

Cramor-Shoup 암호, Masayuki Abe (NTT)
T1-1.4 EPOC : Efficient Probabilistic Public-Key Encryption, Tatsuaki Okamoto, Shigenori Uchiyama, Eichiro Fujisaki (NTT)

T1-2 소프트웨어 보호
T1-2.1 정보이용 관리와 Anti-tamper 소프트웨어, Shingo Inoue, Ken-ichirou Akai, Jun Kuwahara, Tatsuya Sakamaki, Tsutomu Matsumoto(Yokohama Nat'l U.)
T1-2.2 Software Protection Using Public Key Infrastructure, Byoungcheon Lee, Kwangjo Kim (ICU)
소프트웨어를 UIP(User Independent Part)와 UDP(User Dependent Part)로 구별하고 공개키 암호를 이용하여 불법 복제를 방지하고 안전하게 분배하는 방식을 제안하였다.
T1-2.3 오염 데이터 발신 방식에 의한 화상형 디지털 콘텐트의 지적 재산권 보호,
Akinori Matsumoto, Masakatsu Nishigaki, Masakazu Soga (Shizuoka U.), Akio Takubo(Mitsubishi)
T1-2.4 데이터 오염과 동적 복원에 의한 실용형식 프로토콜의 부정 복사 방지 방법
Tohru Ikuma, Masakazu Soga, Masakatsu Nishigaki(Shizuoka U.), Akio Takubo (Mitsubishi)

T1-3 비밀 분산
T1-3.1 분산 RSA 암호계에 있어서 threshold 방법의 문제점,
Shingo Miyazaki, Kouichi Sakurai (Kyushu U.)
T1-3.2 Timed Release Threshold Cryptosystem, Masayuki Numao (IBM Japan)
T1-3.3 A Threshold Digital Signature Issuing Scheme without Secret Communication, Kunihiko Miyazaki, Kazuo Takaragi, Masahi Takahashi (Hitachi)
T1-3.4 Update of Access Structure in Shamir's (k,n) Threshold Scheme, Yuko Tamura, Mitsuru Tada, Eiji Okamoto (JAIST)

T2-1 난수
T2-1.1 2진 M 수열의 k-error 선형 복잡도에 관하여, Yoshiaki Shiraishi*, Masakatu Morii (U. of Tokushima), Tomohiko Uyematsu*, Kohichi Sakaniwa*(TIT)
T2-1.2 메모리가 있는 비선형 결합기 형 난수 생성기의 상관 특성에 관하여, Keiji Katsura*, Yoshiaki Shiraishi(TIT), Masakatu Morii*, Ryousaku Shimada*(U. of Tokushima)
T2-1.3 1차원 사상에 기반을 한 카오스 의사 난수 계열의 암호학적 안전성에 대하여, Kenji Ohkuma, Kouichi Sakurai (Kyushu U.)
T2-1.4 IP Packet의 도착 시간을 이용한 난수 생성, Yasuhiro Sakaguchi, Eiji Okamoto(JAIST)
T2-1.5 비선형 변환에의 특수한 입력 구조를 갖는 의사 난수 생성기과 그 특성, Takeshi Nagao, Ichi Takumi(Nagiya Inst. of Tech.), Masayasu Hata (Aichi Pref. U.)

T2-2 정보 은닉법 (3)
T2-2.1 직접 확산에 의한 정보 은닉법의 내성 평가, Hirofumi Muratani, Taku Kato, Naoki Endoh (Toshiba)
T2-2.2 논리 필터를 이용한 정보 은닉법의 구현과 평가, Hirokazu Ishizuka (TAO), Yasuyuki Sakai (Mitsubishi), Kouichi Ssakurai(Kyushu U.)

T2-2.3 마스킹 모델을 이용한 정보 은닉법과 그 성능 평가, Jinlin Lu, Akira Nakayama, Satoshi Nakamura, Kiyohiro Shikano (NAIST)
T2-2.4 cookie를 이용한 정보 숨기기 방식과 그 응용, Tsutomu Matsumoto, Hiroshi Itoyama, Tatsuro Ikeda(Yokohama

Nat'l U.), Ichiro Murase(Mitsubishi)
T2-2.5 텍스트 정보 숨기기의 제안과 평가 실험, Hiroshi Nakagawa, Yuusuke Komata, Tsutomu Matsumoto (Yokohama Nat'l U.), Ichiro Murase (Mitsubishi)

T2-3 디지털 서명(3)
T2-3.1 A Generalization of the Simmons' Bounds on Secret-Key Authentication Systems, Hiroki Koga (U. of Tokyo)
T2-3.2 효율이 좋은 Rabin 형 디지털 서명 방식, Kaoru Kurosawa (TIT), Wakaha Ogata (Himeji Inst. of Tech.)
T2-3.3 다차원 Rabin서명과 RSA 암호, Kunikatsu Kobayashi, Minako Sugimoto (Yamagata U.)
T2-3.4 합성수를 법으로 한 이산 대수를 이용한 디지털 서명 방식에 관한 연구, Toshiyuki Koide, Kunikatsu Kobayashi (Yamagata U.)
T2-3.5 TSH-ESIGN : Efficient Digital Signature Scheme Using Trisection Size Hash, Tatsuaki Okamoto, Eiichi Fujisaki, Hikaru Morita (NTT)
T3-1 타원 암호(3)
T3-1.1 A Fast Computation of Multiplication and Division over Certain Finite Fields and Its Application to Elliptic Curves Cryptosystems, Katsutoshi Fukuchi (TIT), Takakazu Satoh (Saitama U.), Kiyomichi Araki (TIT)
GF(2^m)상에서의 곱셈 계산을 효과적으로 수행하기 위하여 Karatsuba 방법을 활용한 결과 O(l^alog l) 시간에 가능하고 타원 곡선형 ElGamal 방식을 설계하였다.

T3-1.2 소프트웨어에 의한 $GF(2^m)$ 상의 타원 곡선의 구현, Tetsuya Chikaraishi, Shigeki Yanagisawa, Kouichi Sugimoto (Toyo Comm. Eq.)
GF(2^m) 상의 cyclotomic polynomial을 이용한 다항식 기저를 이용한 방식을 전용 H/W 승산기를 탑재하지 않는 범용 CPU 상에서 고속 구현을 확인하였다.

T3-1.3 C_{ab}곡선을 이용한 이산 대수 형 암호의 소프트웨어 구현
C_{ab} 곡선의 Jacobian 군에 있어서 가산 알고리즘을 개선하여 S/W 구현에 의하여 실행 속도를 160 비트 Jacobian 군을 갖는 C_{37} 곡선에 대하여 266MHz, Pentium 상에 정수 곱셈이 300ms가 소요되었다.

T3-1.4 초타원 곡선 암호의 고속 실행 하드웨어 형 알고리즘
GF(2^n) 상에 정의된 초 타원 곡선의 Jacobian 다양체의 군 연산을 H/W로 실행하는 효율적인 알고리즘을 제안한다. genus가 3인 $y^2+y=x^7/GF(2^{59})$의 경우 실험한 결과 초타원 곡선 암호도 타원 곡선암호와 동등한 처리가 가능함을 확인하였다.

T3-1.5 IC 카드에 타원곡선의 최적 구현법
기저가 복수인 경우에 기저 배수만을 계산하는 고속 Table lookup 방식을 제안하고 기저 수가 많은 타원 곡선 DSA 서명 및 Okamoto 서명 방식을 IC 카드 상에 처리한 결과 70ms, 120ms가 구현 가능하였다.

T3-1.6 DSP를 이용한 타원곡선 암호의 고속 실현, Kouichi Itoh, Masahiko Takenaka, Naoya Torii, Syouji Temma, Yasushi Kurihara (Fujitsu)
범용 타원 곡선 변수를 전제로 한 소수 체 상의 타원곡선 암호의 고속 처리를 기술한다. DSP를 이용하는 방법으로 (1) Jacobian 좌표를 이용한 계산에서 계산 도중에 이용하는 값을 유효하게 이용하여 IEEE P1363에 제시한 방법보다 13% 고속화 (2) 임의의 점의 스칼라 곱셈에 대하여 NAF(Non-Adjacent Form) Signed Binary 표현 방식과 효율적인 Window method를 병행 이용하여 IEEE P1363 방식보다 10% 고속화 하였고 DSP TMS320C621 (200MHz)에 구현하여 160 비트 소수체 타원 곡선 상에 임의의 스칼

라 곱셈이 3.09ms에 처리 가능함을 확인하였다.

T3-2 네트워크 시큐리티 (2)
T3-2.1 컴퓨터 바이러스의 프랫홈에 관한 고찰, Yasushi Sengoku, Shimmi Hattori(Kanazawa Inst. of Tech.)
T3-2.2 Java 바이러스의 검토, Kei Fujimaki, Akira Nakamura (Int'l Christian U.)
T3-2.3 스마트 오피스의 시큐리티에 대한 요구 분석, Wataru Yamazaki, Wu Wen, Fumio Mizoguchi (Science U. of Tokyo)
T3-2.4 PKI에 있어서 공개키 인증서의 다이나믹스와 온 라인 증명서 검증 프로토콜의 Scaleability. Hiroaki Kikuchi, Kensuke Abe, Shohachiro Nakanishi(Tokai U.)
T3-2.5 k 값 해쉬트리를 이용한 증명서 폐기 트리의 변경 방법의 제안과 평가
Hiroaki Kikuchi, Kensuke Abe, Shohachito Nakanishi (Tokai U.)
T3-2.6 Mobile agent를 이용한 칩입 탐지 및 흔적을 이용한 침입 판정의 검토와 구현, Atsushi Taguchi, Midori Asaka, Shunji Okazawa et al (Information Promotion Agency)
T3-2.7 Java에 의한 안전한 event 처리 API, Yukinobu Mine, We Wen, Fumio Mizoguchi (Science U. of Tokyo)

T3-3 프로토콜

T3-3.1 영 지식과 리버스 엔지니어링, Satoshi Hada (KDD)
T3-3.2 Model checking securty protocols, Wen Wu, Mizoguchi Fumio (Science U. of Tokyo)
T3-3.3 사양 기술 언어를 이용한 시큐리티 프로토콜의 검증, Takamichi Saito, Wu Wen, Fumio Mizoguchi (Science U. of Tokyo)
T3-3.4 Asymmetric Fingerprinting using 'Chameleon', Alexander Vollschwitz, Hideki Imai (U. of Tokyo)
T3-3.5 Analysis of Time-dependent security on Timed-release Cryptographic Protocol, Michiharu Kudo, Anish Mathuria, Takeshi Imamura (IBM Japan)

T4-1 암호 분석(2) / 검토
T4-1.1 선형근사법의 유의성을 높히는 방법, 김일준, Daiki Kato, Tsutomu Matsumoto(YNU)
LC에서 有意性을 높이기 위하여 해독에 필요한 기지 평문 수를 줄이기 위하여 복수의 선형 seive 근사식을 이용한 방법을 제안하고 8단 DES에 대하여 실험 결과를 제시하였다.

T4-1.2 중간변수를 이용한 블록 암호 MISTY의 FO 함수에 관한 공격, Hidema Tanaka, Kazuyuki Hisamatsu, Toshinobu Kaneko (Science U. of Tokyo)
MISTY를 FO 함수를 3단 이상 구성한 경우, 증명 가능성을 제시하였다. 3단 이상의 FO 함수만을 구성한 경우에 대하여 고차 차분 공격을 시도한 결과, 5단으로 구성된 경우 7차 차분을 이용하여 1,508개의 선택 평문과 2^17의 계산량으로 가능함을 확인하였다.

T4-1.3 불능 차분 이용 공격에 대하여, Kazumoaro Aoki (NTT)
1998년 Biham이 Skipjack에 대하여 제안된 불능 차분 이용 공격을 Crypto'98의 Rump Session에 개량판이 발표되었다. 불능 차분 공격에 대하여 안전성의 평가 지표를 제시하고 그 지표와 DC, LC에 안전성이 증명 가능한 암호를 구성하였고 FEAL 및 E2에 적용한 결과 각각 9단, 5단에 가능한 것을 확인하였다.

T4-1.4 Linear Sum 공격, Kazumaro Aoki (NTT)
FSE97에서 Jakobson과 Knudsen에 의한 보간 공격이 제안되었다. 이 공격은 DC와 LC에 안전성이 증명 가능한 PURE 암호에 대하여 효과가 가능하다. 보간 공격은 PURE 와

같이 대수적인 구조를 가진 암호에 대하여 효과가 있으나 일반적인 암호에는 적용이 곤란하다. 이유는 평문과 암호문간에 다항식 관계를 찾는 것이 어렵기 때문이다. 보간 공격을 확장하여 공격 가능한 암호문과 평문의 다항식 조건을 완화하고 바이트 단위로 처리하는 CRYPTON, E2, RIJNDEL에 적용한 결과 6, 3, 6단 까지 공격이 가능하다는 것을 확인하였다.

T4-1.5 공통키 암호 RC5의 해독 알고리즘의 실장에 대하여 (2), Hiroki Mitsuya, Takeshi Shimoyama, Shigeo Tsujii(Chuo U.)
1998년 Biryukov 등이 제안한 RC5의 해독 방법을 개선하여 RC5의 변형 형태에 실험적으로 시도한 결과를 제시하였다.

T4-1.6 개량형 고차차분 공격법에 대한 안전성을 가진 공통키 암호의 설계법, Takeshi Shimoyama (TAO)
고차 차분 공격에서 2회 미분해서 정수가 될 수 있는 공격 가능성에 관한 개념을 제안하고 저차의 경우 부울 다항식으로 표현되는 사례를 제시하였다.

T4-2 정보 은닉법 (2)
T4-2.1 Information Hiding into JPEG Images, Takashi Mano (IBM Japan)
T4-2.2 에러 정정부호를 이용한 알고리즘 공개형 정보 은닉법, Kazuhiko Yamaguchi (U. of Electro-Comm.), Keiichi Iwamura(Canon), Hideki Imai (U. of Tokyo)
T4-2.3 원화상의 색조를 손해보지 않고 제거 가능한 가시 정보 은닉법, Keiji Iwamoto, Eiji Shinbori (Dai Nippon Printing)
T4-2.4 Notes on Privacy Enhanced Protocol for Digital Watermark, Hiroyuki Inaba, Masao Kasahara (Kyoto Inst. of Tech.)
T4-2.5 화상의 2치화 과정에서 정보 삽입 방법의 개량에 대하여, Takeshi Ogihara, Yukio Kaneda (Kobe U.)

T4-3 인증 계산법
T4-3.1 사용자의 고유정보를 3개 이용한 개인식별법 및 키 공유 프로토콜, Hideki Miyata, Yuichi Kaji, Takehiko Tanaka (NAIST)
T4-3.2 새로운 사용자 인증 방법의 개발과 평가, Masashi Sakamaki, Yasushi Sengoku, Shimmi Hattori (Kanazawa Inst. of Tech.)
T4-3.3 동일 패스워드를 가정한 키보드에 의한 개인식별, Kazumasa Omote, Eiji Okamoto(JAIST)
T4-3.4 데이터 압축 알고리즘을 이용한 고속 멱승법의 연산법, Tsuyoshi Sumida, Satoshi Uehara, Kyoki Imamura (Kyushu Inst. of Tech.)
T4-3.5 역원연산법의 비교에 대하여 (1), Junko Nakajima, Mitsutu Matsui (Mitsubishi)
T4-3.6 특수한 법에 의한 몽고메리 축소법의 고속화, Akiko Niwa, Atsushi Shimbo, Shinichi Kawamura(Toshiba)

TN-1 Night Session
TN-1.1 Muraue-Kasahara 형 NIKS에 대한 결탁 공격, Tsuyoshi Nishioka (Advance), Hideki Imai(U. of Tokyo)

TN-1.2 RSA 암호와 동일 Trapdoor를 가진 디지털 서명 방식
합성수를 이용한 DH 형 디지털 서명 방식을 Message가 특수한 경우에 한정된 경우와 난수를 이용한 방식을 제안하고 RSA 암호 방식과 비교하였음.

TN-1.3 Money, Electronic Money, and Quantum Money, Tsutomu Matsumoto (Yokohama National U.)
에너지를 money로 사용하는 방법으로 coin을 teleportation 방식으로 quantum 통신 방식을 이용하는 방식을 제안

F1-1 타원 암호(4)
F1-1.1 확률적 소수 판정을 이용한 타원곡선 암호의 키 생성, Koichiro Akiyama

(Toshiba)
실용화 단계에 들어가고 있는 타원 곡선 암호는 안전한 키 생성 기술이 중요한 과제이다. Realtime 성, 신뢰성, 안전성을 만족하는 키 생성 기술을 목표로 확정적 소수 판정법을 활용한 CM 법을 기반으로 하는 키 생성 방법을 제안한다. 구현한 결과 사용자가 명령 입력 후 불만을 느끼지 못하는 시간 (20초) 내에 생성이 가능하였다.

F1-1.2 안전한 타원곡선 암호 변수 생성법, Tetsuya Izu, Jun Kogure, Masayuki Noro, Kazuhiro Yokoyama (Fujitsu)
타원 곡선 암호를 랜덤하게 선택하기 위하여는 유리점 군의 위수 계산 알고리즘이 필요하다. 큰 표수의 소수체 상의 곡선의 경우는 SEA (Schoof-Elkies-Atkin) 법에 의하여 생성이 가능하나 표수2의 유한체 상에서는 SEA 법이 적용이 되지 않는다. 저자가 표수2의 경우 이미 Lercier 방법과 Couveignes 방법을 구현하고 Asiacrypt98에서 발표한 Intelligent Choice System을 조합 한 결과 표수 2의 경우에도 안전한 타원 곡선의 생성이 가능하였고 구현 결과를 실제 보여주었다.

F1-1.3 Generalizing the Menezes-Okamoto-Vanstone (MOV) Algorithm to Non-Supersingular Elliptic Curves, Junji Shikata*, Yuliang Zheng(Monash U.), Joe Suzuki*(Osaka U.), Hideki Imai (U. of Tokyo)
MOV reduction 알고리즘은 타원 곡선 암호의 안전성 평가에 중요한 기여를 한 바가 있다. 그러나, MOV 알고리즘은 소위 초타원 곡선에서만 적용되어 일반적이지 못하여 본 연구에서는 일반적인 타원 곡선의 경우에서 1998년 J. of Cryptology에 Balasubaramaian과 Koblitz가 발표한 결과를 확장하여 n-torsion point를 구하는 문제로 귀착함을 제시하였다.

F1-1.4 MOV Reduction 및 FR Reduction의 구현과 수치 검증
Naoki Kanayama(Waseda U.), Shigenori Uchiyama(NTT), Taiichi Saitoh (TAO)
타원 곡선 상의 DL 문제를 해결하는 방법으로 MOV 축소와 FR 축소 방법이 있는 데 이 방법의 구현을 시도한 결과를 제시하였는 데 논문 내용이 틀린 것이 많아 저자인 Naoki Kanayama (e-mail : 689m5048@mse.waseda.ac.jp)에 연락하면 보내 준다고 하였다.

F1-2 구현
F1-2.1 소프트웨어에 의한 스트림 암호의 고속 구현, Kouichi Sugimoto (Toyo Com. Equipment.), Kaoru Kurosawa(TIT)
F1-2.2 E2의 소프트웨어 구현, Kazumaro Aoki, Hiroki Ueda(NTT)
F1-2.3 128비트 블록 암호의 하드웨어 구현에 대하여(I), Tetsuya Ichikawa, Tomomi Kasuya, Mitsuru Matsui (Mitsubishi)
F1-2.4 수치 연산 형 공개키 암호 co-processor의 개발, Masanobu Koike, Atsushi Shimbo, Shinichi Kawamura, Masue Shiba (Toshiba)
F1-2.5 $GF(2^m)$연산 및 정수 연산을 처리 가능한 Hybrid Coprocessor의 제안, Masue Shiba, Shinishi Kawamura, Atsushi Shimbo (Toshiba)
F1-2.6 IC 카드에의 ESIGN 구현 방법, Tomomi Sato, Yoichi Sakajiri, Liang Qing(Ricoh), Hidemi Moriobatake, Shinichi Hirata (NTT)

F1-3 키 관리(1)
F1-3.1 카드의 배포에 의한 비밀키 공유를 위한 최적 프로토콜에 대하여, Takaaki Mizuki, Hiroki Shizuya, Takao Nishizeki (Tohuku U.)
F1-3.2 마스크 부가형 그룹키 공유법, Jun Anzai, Natsume Matsuzaki(AMSL), Tsutomu Matsumoto (Yokohama Nat'l U.)
F1-3.3 내 clone 성을 이용한 키 공유 방법, Tsutomu Matsumoto, Takuya Inoue,

Hiromi Kubota, Naoki Tanaka (Yokohama Nat'l U.)
F1-3.4 Key Predistribution System에 있어서 센터의 신뢰성 분산에 관한 개량방법의 검토, Yohei Shibuya*, Goihiro Hanaoka*,Tsuyoshi Nishioka (Advance), Hideki Imai*(U. of Tokyo)

F2-1 타원 암호(5)
F2-1.1 타원곡선의 위수 계산 (SEA에 의한 알고리즘) 의 고찰, Koji Chida (Waseda U.), Taiichi Saito(TAO)
최근 타원 곡선 암호의 필요성으로부터 유한체 상에 정의된 타원 곡선의 유리점의 개수를 계산하는 고속의 알고리즘 구현이 널리 연구되고 있다. SEA 방법에 있어서 특별한 Elkies 소수에 대하여 작은 소수의 exponentiation을 modulo로 하는 유리수 점을 구하는 알고리즘을 제안하고 특별한 Atkin 소수에 대하여 고찰하였다.

F2-1.2 효율적인 소수 위수 타원 곡선의 구성, Yuichi Futa(Matsushita), Atsuko Miyaji(JAIST)
타원 곡선의 위수를 구하는 방법으로 Schoof 알고리즘이 알려져 있다. Schoof 알고리즘을 개량한 SEA 방법이 있다. 실제 발생하는 방법의 가장 dominant step 부분을 고속화 하는 방법을 제안한다.

F2-1.3 Modulus Searching Methods for Secure Elliptic Curve Cryptosystem, Kenji Koyama, Noboru Kunihiro, Yukio Tsuruoka (NTT)
지금까지의 타원 곡선 암호의 선택 방법으로 (a,b,p)를 랜덤하게 생성하는 방법을 주로 하였으나 타원 곡선 $E(a,b,p): y^2 = x^3 + ax + b \pmod{p}$에서 {a≠0, b=0} 또는 {a=0, b≠0}인 경우 주어진 위수 S, a,b로부터 modulo 값 p를 계산하는 방법을 제안한다. 우선 필요한 위수 S를 결정하고 S = #E(a,b,p)를 만족하는 소수 modulo 값 p를 탐색한다. 이 방법으로 $O(\log^5 S)$의 다항식 시간으로 적합한 (S, (a,b), p)를 계산할 수 있었고 기존의 Schoof 알고리즘과 Atkin-Morain 알고리즘에 비하여 고속이다.

F2-1.4 Two Discrete Log Algorithms for Super-Anomalous Elliptic Curves, Noboru Kunihiro, Kenji Koyama (NTT)
소수 체 F_p상의 타원 곡선을 확장하여 환 $Z/nZ(n = \Pi_{i=1}^{k} p_i^{e_i})$ 상의 super-anomalous curve를 정의한다. 이러한 곡선상에서 이산 대수 문제은 n의 소인수 값을 모르고 확정적인 시간에 계산이 가능하고 주의하여야 한다.

F2-2 표준화
F2-2.1 3중 DES에 대한 최근의 표준화 동향에 대하여 Fumikazu Taniguchi(일본은행 금융연구소), Kazuo Ohta, Miyako Ookubo (NTT)
F2-2.2 안전성 증명 가능한 공개키 암호 방식에 대한 동향에 대하여, Masashi Une(일본은행 금융연구소), Tatsuaki Okamoto (NTT)
F2-3 키관리(3)
F2-3.1 결탁공격에 대하여 높은 내성을 가진 KPS의 설계 방법에 대하여, Goichiro Hanaoka*, Tsuyoshi Nishioka(Advance), Yuliang Zheng(Monash U.), Hideki Imai*(U. of Tokyo)
F2-3.2 발신 필터링 환경하의 키 공유 프로토콜에 있어서 폐쇄율 평가, Kanta Matsuura, Hideki Imai (U. of Tokyo)
F2-3.3 Enhancing the Resistance of a Secure Key Agreement Protocol to a Denial-of-Service Attack, Shouichi Hirose(Kyoto U.), Kanta Matsuura (U. of Tokyo)
F2-3.4 프라이버시를 보호하는 키 위탁 방식, Kazumori Takatani, Wakaha Ogata, Hitoshi Sakagami. Yutaka Takahashi (Himeji Inst. of Tech.)
F2-3.5 병렬형 비밀분산에 의한 키 위탁과 암호 데이터의 블라인드 복호, Ikuko

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

Ⅲ. 결언

타원곡선상에서의 각종 암호 시스템의 구현, 변수 선별법, 안전성 평가 등에 관한 연구가 많았으며, watermark 에 관한 연구도 실용화를 위한 연구가 진행된 듯 하였다. 학회 기간 중 미쓰비시가 출품한 PKI 관련 S/W 패키지, (주)Cisco의 Firewall과 VPN 제품은 눈길을 끌었다. 끝으로 2000년 오끼나와에서 개최될 한일간의 마지막으로 개최되는 공동 워크샵 JW-ISC2000에 회원들의 적극적인 참여가 요망된다.

참 고 문 헌

[1] Proc. of the 1999 Symposium on Cryptography and Information Security (SCIS'99), *일본전자정보통신학회정보시큐리티전문연구위원회*, Vol 1, Vol.2, 1999.1.26 ~1.29. Kobe, Japan

김 광 조 (金 光 兆)

1973년 3월~1979년 2월 : 연세대학교 전자공학과 (공학사)
1981년 9월~1983년 8월 : 연세대학교 대학원 전자공학부 (공학석사)
1988년 4월~1991년 3월 : 요꼬하마 국립대 전자정보공학부 (공학박사)
1979년12월~1997년12월 : 한국전자통신연구원 부호1실장
1996년 3월 ~ 1997년 8월 : 충남대학교 컴퓨터과학과 겸임 교수
1998년 1월 ~ 현재 : 한국정보통신대학원 공학부 교수, 본학회 학술(국외) 이사, 세계암호학회 회원, Asiacrypt 조정 위원회 위원,

〈관심분야〉 정보보호와 암호 이론 및 응용