# PKC'99 논문 발표 동향

ETRI 통신정보보호기술 워크샵 발표 자료,'99.5.28(금)

한국정보통신대학원대학교
ICU(Information and Communications Univ.)
공학부
School of Engineering

김 광조
e-mail : kkj@icu.ac.kr
Tel: (042)866-6118, Fax:(042)866-6154

1. 회의개요

가. 회의명 : 2nd International Workshop on Practice and Theory in Public Key Cryptography (PKC99)

나. 일시 : '99.3.1. ~ 3.3

다. 장소 : Kamakura Prince Hotel, 일본

라. Session 구성

- 3개 초청 강연
- 12개국 61편 논문 신청 중 25편 발표 (채택률: 2.44:1)
- Lecture Notes in Computer Science, Vol. 1560, Springer Verlag, p.326 으로 출간

마. 참가자 : 총 126여명 중 한국 6명 (이 만영박사, 김 광조교수, 신 상옥(부경대), 이 창휘박사(SAIT), 유학생 2명)

사. 특이 사항 : 회의 장소는 바로 태평양이 보이는 해변 가에서 경관이 좋고 조용한 분위기였으며, 동경 근처로 이동에도 크게 불편하지 아니하였음. 또한, 회의 후, 이 만영박사님이 동경대에서 특별 강의가 있었음.

2. 회의 내용

Day 1 (Monday, 1 March 1999), Venue: Hall No. 6 & 7

08.00 - Registration

09.50 - 10.00 Opening address (Hideki Imai)
프로그램 편성 및 일반적인 안내, 감사

10.00 - 11.00 Invited talk 1 (Chair : Kwangjo Kim)

*New Work on Watermarking, Traitor Tracing, and Related Issues,* Amos Fiat (Algorithmic Research, Israel)

Fiat-Shamir Identification 및 서명 방식을 제안한 Fiat 박사가 Watermarking, Traitor tracing 등에 관한 일반적인 기술과 현황을 제시하였다.

11.00 - 11.30 Coffee break

11.30 - 12.30 Session 1 -- Supporting techniques

(Chair : Markus Jakobsson)
*Preserving Privacy in Distributed Delegation with Fast Certificates*, Pekka Nikander (Ericsson, Finland), Yki Kortesniemi and Jonna Partanen (Helsinki Uni of Tech, Finland)
인증서를 이용한 사용자의 프라이버시를 유지하는 방법을 제시하였다.

*Hash Functions and the MAC Using All-or-Nothing Property,* Sang Uk Shin and Kyung Hyune Rhee (PuKyong Nat Uni, Korea), Jae Woo Yoon (ETRI, Korea)
Rivest가 최근 All-or-nothing 암호를 제안한 개념을 해쉬 함수를 설계하는 데 도입하여 결과를 제시하였다.

12.30 - 14.00 Lunch break

14.00 - 15.00 Invited talk 2 (Chair : Kanta Matsuura)
*Business Needs for Cryptographic Technology in Financial Industry in Japan*, Naoyuki Iwashita (Bank of Japan)
일본 금융에서 필요로 하는 암호 기술의 필요성과 미국, 유럽과의 비교하고 현황을 제시하였다.

15.00 - 15.30 Coffee break
15.30 - 18.00 Session 2 - Applications (I) (Chair : Yve Desmedt)
*Toward Fair International Key Escrow - An Attempt by Distributed Trusted Third Agencies with Threshold Cryptography -,* Shingo Miyazaki (Kyushu Univ, Japan), Ikuko Kuroda (NTT, Japan) and Kouichi Sakurai (Kyushu Univ, Japan)

Esrow 정책이 다른 2개의 국가간에 TTP를 설정하는 방식을 Threshold cryptography를 이용한 결과를 제시하였다.

*Auto-Recoverable Cryptosystems with Faster Initialization and the Escrow Hierarchy*, Adam Young (Columbia Uni, USA), Moti Yung (CertCo, USA)
자동 복구 가능한 암호 시스템으로 RSA 와 일반화한 ElGamal 공개키 암호 방식을 이용하여 기존의 방식보다 빠르고 Escrow hierarchy를 구성할 수 있는 개념을 새롭게 제안하였다.

*Shared Generation of Random Number with Timestamp : How to Cope with the Leakage of the CA's Secret*,
Yuji Watanabe and Hideki Imai (Uni of Tokyo, Japan)
신뢰하여야 하는 CA의 비밀키가 누설되는 것을 방지하기 위하여 난수와 Timestamp 정보를 이용하여 CA의 비밀을 보장하는 방법을 제안하였다.

*A New Type of "Magic Ink" Signatures -- Towards Transcript-Irrelevant Anonymity Revocation,*
Feng Bao and Robert H. Deng (Kent Ridge Digital Labs, Singapore)
매직 잉크 서명이란 범죄자의 활동을 있을 경우 기관에 의하여 서명에 감사 추적과 익명성 취소를 가능하게 하는 내용은닉 서명이다
기존의 공평한 은닉 서명 방식에서 서명 수신자를 추적하기 위하여는 해당되는 서명의 인스턴스를 기록한 데이터 베이스를 탐색할 필요가 있다. 달리말하면, 익명성 취소를 위하여는 신뢰자는 서명 과정에서 서명자에 의하여 생성한 어떤 정보를 알아야 한다. 이것은 어떤 경우에 익명성 취소 과정에서 적절하지 못하다. 이 논문에서는 새로운 형태의 매직 잉크 서명을 제안

한다. 새로운 서명의 특징은 익명성 취소는 transcript에 무관하다. 즉, 신뢰자는 서명에 내재된 정보만으로 수신자의 익명성을 취소할 수가 있다. 따라서, 서명자는 누구에게서 추적당하였다는 사실을 모르고 신뢰자는 서명자의 익명성을 취소할 수가 있다.

*Message Recovery Fair Blind Signature*
Hyung-Woo Lee and Tai-Yun Kim (Korea Uni)
(발표 미 참가)
메시지와 서명자간에 익명성이 보장되는 blind signature는 범죄자들에 의한 악용의 소지가 있다. 의심스러운 메시지에 대하여는 심판관이 추적하여 검증할 수 있는 메커니즘이 필요하다. 메시지 복원이 가능한 modified fair blind 서명 기법을 제안한다. Horster 가 제안한 meta-ElGamal 방식을 해석하여 메시지 복원형 blind signature를 우선 고려한다. 또한, Oblivious Transfer 프로토콜을 이용하여 심판관이 공정성을 검증할 수 있는 새로운 fair blind signature를 제안한다. 제안한 방법은 blind multi-signature에 이용되고 다양한 전자 지불 시스템에 이용된다.

19.00-21.00Reception (Venue: Hall No. 3&5)
No official event, food only and free environments

Day 2 (Tuesday, 2 March 1999), Venue: Hall No. 6 & 7
09.00 - 10.00 Invited talk 3 (Chair : Moti Yung)
*On the Provable Security of Practical Public-Key Cryptosystems,* Tatsuaki Okamoto (NTT Labs, Japan)
Indistinguishability, Non-malleability, Chosen Ciphertext Attack1, Chosen Ciphertext Attack2 등 공개키 암호의 안전성 평가 척도를 정의한 후 OAEP, EPOC 등의 최근 안전성이

증명되는 PKC 연구 동향을 제시하였다.

10.00 - 10.30 Coffee break
10.30 - 12.30 Session 3 -- Theory (Chair : Amos Fiat)
*Anonymous Fingerprinting Based on Committed Oblivious Transfer,* Josep Domingo-Ferrer (Uni Rovira i Virgili, Spain)
전자 상거래 시스템에 있어서 전자 정보의 불법적인 재 분배를 방지하는 문제가 중요하다. 전자 거래에 있어서 구입자의 익명성과 호환되는 소유권 보호 기술로 익명 지문 방식(anonymous fingerprinting)이 있다. 이 방식은 안전한 다자간 계산이나 일반적인 영지식 증명에 의존하므로 실제 구현에 제약점이 있다. 모든 계산이 효과적으로 가능한 Committed Oblivious Transfer 기법을 이용한 효율적인 익명 지문 방식을 제안하였다.

*Decision Oracles are Equivalent to Matching Oracles,*
Helena Handschuh (Gemplus and ENST, France)
Yiannis Tsiounis (GTE Labs, USA), and Moti Yung (CertCo, USA)
Decision DH 문제를 Matching DH 문제로 동등 변환을 할 수 있는 특성을 논하고, universal malleability의 개념을 도입하였다.

*A Relationship between One-Wayness and Correlation Intractability,*
Satoshi Hada and Toshiaki Tanaka (KDD, Japan)
랜덤 oracle의 불 예측성을 정의하기 위하여 Correlation intractable function ensemble이 도입되었다. 만일 R이 랜덤 oracle이면 입 출력 쌍 (x, R(x))가 어떤 성질을 가지도록 하는 x를 찾는 것이 불가능하다고 가정한다. 본 연구에서는 "일

방향 함수가 존재하면 correlation intractable function ensemble이 존재한다“는 것이 ”BPP와 같은 trivial 언어에 대한 3 라운드 보조 입력 Arthur-Merlin 영지식 증명이 존재한다“ 것을 증명하는 어려운 문제임을 밝힌다.

*On the Security of Random Sources*
Jean-Sebastien Coron (ENS and Gemplus, France)
난수 발생기가 많은 곳에서 응용되고 있고 통계적 검정은 난수원에서의 약점을 찾는 데 이용된다. Maurer의 universal test는 통계적 결함을 찾는 데 유용하다. 이 검정은 난수 생성원의 엔트로피 (즉, 난수원의 출력에 의해 키 입력이 되는 블록 암호의 실효 키 크기) 와 점근적으로 관계되어 있다. 본 논문에서는 Maurer의 검증 방법의 변형으로  검정 함수가 이론적으로 발생원의 엔트로피와 동일하여 결함을 보다 효율적으로 찾는 방법을 제안하였다.

12.30 - 14.00  Lunch break

14.00 - 16.00  Session 4 -- Attacks (Chair : Tatsuaki Okamoto)
*On the Security of RSA Screening*
Jean-Sebastien Coron (ENS and Gemplus, France), David Naccache (Gemplus, France)
복수의 디지털 서명문을 개별적으로 하는 것보다는 동시에 처리하는 과정을 batching이라고 하는 데, 이 과정은 개별적으로 하는 방식과 등가이어야 한다. Eurocrypt'98에서 Bellare가 RSA bach 검증 방법으로 screening 방식을 제안하였는 데 본 논문은 이방법의 공격 방식을 제시하고 위장 서명을 하는 방법을 제안하였다.

*Unknown Key-Share Attacks on the Station-to-Station*

*(STS) Protocol*, Simon Blake-Wilson (Certicom, Canada), Alfred Menezes (Uni of Waterloo, Canada)
키 확인을 위하여 MAC 알고리즘을 사용하고 Station-to-station 키 일치 프로토콜인 STS-MAC에 대한 unknown key-share 공격에 대하여 제시하고 DSA, Rabin, ElGamal, ECDSA 방식에서 비 공격이 견딜 수 있는 방법을 제시하였다.

*The Effectiveness of Lattice Attacks against Low-Exponent RSA,* Christophe Coupe (ENS de Lyon, France), Phong Nguyen and Jacques Stern (ENS Paris, France)
Coppersmith가 Eurocrypt'96에서 Lattice Reduction을 이용한 단변수 모듈러 다항식의 해를 구하는 방법을 제시한 것은 RSA암호에서 지수가 적은 경우(예, e=3)에 대단히 주의하여야 하며 해독의 위험성이 있다. 이 논문은 Coppersmith의 결과를 실험적으로 제시하고, 실질적인 개선점을 제시하였다.

*Evaluating Differential Fault Analysis of Unknown Cryptosystems,* Pascal Paillier (Gemplus and ENST, France)
Biham과 Shamir가 1997년도에 제안한 DFA (Differential Fault Analysis) 공격에 내성을 갖는 암호 시스템의 설계 방법을 제안하였다.

16.00 - 16.30 Coffee break

16.30 - 18.00 Session 5 -- Fast computation (Chair : Man Young Rhee)
*A New Aspect of Dual Basis for Efficient Field*

*Arithmetic,* Chang-Hyi Lee (SAIT, Korea) and Jong-In Lim (Korea Uni)
GF(2^m) 상의 곱셈과 역수 계산에 필요한 연산을 위하여 표현 방법을 소개한다. 이 방법은 S/W와 H/W 구현이 용이하나 본논문에서는 S/W 구현에 관하여만 취급한다. GF(2^m)에서 체 곱셈은 m+1회의 vector rotation과 vector XOR 연산에 가능하고 제곱은 비트 단위의 치환에 의하여 가능하다.

*Low-Cost Double-Size Modular Exponentiation or How to Stretch Your Cryptoprocessor,* Pascal Paillier (Gemplus and ENST, France)
모듈러 멱승을 효과적으로 시행하는 방법 중 거의 최적인 방법을 제안하였다.

*How to Enhance the Security of Public-Key Encryption at Minimum Cost,* Eiichiro Fujisaki and Tatsuaki Okamoto (NTT, Japan)
passive adversary에 대응하여 Semantically Secure 공개키 암호 시스템을 랜덤 oracle 모델에서 adaptive chosen-ciphertext attack (active adversary)에 강한 non-malleable (or semantically secure) 공개키 암호 시스템을 변환하는 방법을 제안한다. 이 변환 방법은 1회의 해쉬 함수 연산을 필요로 하기 때문에 변환된 방식은 해쉬함수를 SHA-1과 MD5 등으로 대체하면 원래의 방식과 거의 동등 수준으로 효율적이다. 안전성 증명 방식을 제시하고 거의 최적임을 제시하고 ElGamal, Blum-Goldwasser, Okamoto-Uchiyama 공개 키 암호 시스템에 적용한 사례를 제시한다.

19.00-21.00 Banquet (Venue: Hall No. 3&5)

Day 3 (Wednesday, 3 March 1999), Venue: Hall No. 6 & 7
09.00 - 10.00 Invited talk 4 (Chair : Takashi Mano)
*A Research Agenda for Public Key Cryptography for the Next Century,*
Yvo Desmedt (University of Wisconsin-Milwaukee, USA)
미래의 공개키 암호 시스템으로 현재 여러 가지 대안이 검토되고 있는 방식에 대하여 논하였다.

10.00 - 10.30 Coffee break

10.30 - 12.30 Session 6 -- Applications (II) (Chair : Miodrag Mihaljevic)
*Mini-Cash: A Minimalistic Approach to E-Commerce*
Markus Jakobsson (Bell Labs, USA)
양도 가능한 익명성 구좌라는 개념을 새롭게 도입하여 시스템에 강한 공격에 대하여는 보호하고 저장 요구도를 경감하고 계산 시간을 최소화하는 방법을 제공한다. 제안 방식은 지불자와 상점의 저장 경비를 이론적으로 가장 최소화할 수 있고, 공격자가 화폐 발행 기관의 비밀키를 입수하는 bank robbery attack에 대하여 보호할 수 있다. 또한, 스마트 카드로서 실질적으로 구현함으로 해서, 사용자의 viral attack을 방지한다. 카드 소유자의 개안 정보를 연결하지 않는 선불 카드 개념을 새롭게 제시한다.

*A Secure Pay-per-View Scheme for Web-Based Video Service,* Jianying Zhou (Kent Ridge Digital Labs, Singapore), Kwok-Yan Lam (Nat Uni of Singapore)
컴퓨터 통신망의 발전에 따는 Web 상에 비디오 서비스가 가능한 시점을 대비하여 안전한 PPV (Pay-per-View) 시스템을 구축하기 위하여 공정한 부인방지 프로토콜를 이용한 서비스를 제안하였다. 제안 방식은 가입자 측면에서 저장 소요와 계산

요구도가 최소이며 물리적인 위치에 관계없이 스마트 카드로서 비디오를 시청할 수 있다.

*Removing Interoperability Barriers between the X.509 and EDIFACT Public Key Infrastructures: The DEDICA Project,* Montse Rubia, Juan Carlos Cruellas and Manel Medina (Polytech Uni of Catalonia, Spain)
X.509의 PKI와 EDIFACT OKI 간의 호환성을 가질 수 있는 방법으로 DEDICA (Directory based EDI Certificate Access and management) project에서 처리 정보를 최소화하고 2개의 PKI를 변환하는 gateway를 설계하여 제시하였다.

*Encrypted Message Authentication by Firewalls,*
Chandana Gamage, Jussipekka Leiwo and Yuliang Zheng (Monash Uni, Australia)
응용 계층에서 firewall을 설치 운용 시, 메시지 인증성을 암호화된 메시지를 복호화하여 검증하기가 어렵다는 현실적인 문제를 해결하기 위하여 signcryption 기법을 이용하여 메시지의 내용을 노출시키지 않고, 서명 검증을 수월하게 하는 방법을 제안한다.

12.30 - 14.00 Lunch break
14.00 - 15.30 Session 7 -- New techniques (Chair : Yuliang Zheng)
*How to Copyright a Function?*
David Naccache (Gemplus, France), Adi Shamir (Weizmann Inst of Sci, Israel) and Julien P. Stern (UCL, Belgium, and Uni de Paris-Sud, France)
복수의 암호 함수가 있을 시 하나의 함수를 일정한 복잡도로 특정화하는 방법을 제안하였다.

*On Quorum Controlled Asymmetric Proxy Re-encryption*
Markus Jakobsson (Bell Labs, USA)
단체를 조정 가능한 비 대칭 대리 재 암호화 방법 (Quorum controlled aymmetric proxy re-enecryption)을 제안한다. 이 방법은 유로 TV나 전자 우편과 같은 응용에서 키 분배에 유용하다. 대리 서버에 정직한 부 정직한 단체가 없다면 ElGamal 암호를 근간으로 한 이 방식은 정보를 누설하지 않는다는 것을 증명한다. 별도의 응용으로는 공개적으로 검증 가능한 translation certificate를 제공하는 방법이다. 입력과 출력의 암호화는 각각 동일한 평문에 해당하고 평문에 대한 정보를 검증자나 증명자의 부분에 대하여 어떠한 정보도 부설하지 않는다. certificate의 크기는 작고 증명 서버의 수에 무관하다. 세부 방식으로 Proactive 서명 방식, 부인 불가 서명 방식, Schnorr 서명, 정보이론적 비밀 공유 방법을 이용하였다.

*A Trapdoor Permutation Equivalent to Factoring*
Pascal Paillier (Gemplus and ENST, France)
Eurocrypt'98에서 mod p^2q 상에서 Okamoto 등이 제안한 새로운 공개키 암호 시스템이 제안하였는 데 선택평문공격이 소인수분해 문제와 동등함을 제시한 바가 있다. 그러나 제안 방식이 치환이 아니므로 디지털 서명에는 사용할 수가 없다. 본 연구에는 치환이 될 수 있는 변형 공개키 암호 시스템을 제안하였다.
15.30 Adjourn

3. 차기 회의 (PKC2000)
- 장소 : 멜보른, 호주
- 일정 : 2000.1.18. ~ 1.20.
- 논문 Deadline : '99.8.27.

* PKC2001 will be held in Korea(?)