Eurocrypt'92를 통한 최근 암호학의 연구 동향

김 광조

한국전자통신연구소

Recent Trends of Cryptologic Research from Eurocrypt'92

KwangJo Kim

Electronics and Telecommunications Research Institute

요 약

본고는 1992년 5월 25일부터 5월 28일까지 구 동구권 국가 중 헝거리에서 개최된 Eurocrypt'92에서 88편의 신청 논문 중 발표된 35편의 연구 논문을 중심으로 암호학의 최근 연구 결과와 동향을 요약 정리하고 회의 기간 중에 있었던 "Trapdoor Primes and Moduli"를 주제로 한 패널 토론 내용을 소개하였다.

1 서론

유럽 국가중 한나라에서 매년 4,5월경에 열리는 Eurocrypt'92는 세계가 탈 냉전 시대를 맞이하는 듯 주로 사회 주의국가로만 우리에게 알려진 동유럽[1] 국가 중 헝거리에서 1992년 5월 24일(일) 부터 5월 28일(목)까지 개최되었다. 헝거리는 동유럽 국가 중 3년전부터 가장 먼저 개방정책을 펼쳐 세계적인 학술 대회를 많이 유치한 바가있다. 이로 인해 2년전 세계암호학회 (IACR, International Association for Cryptologic Research) 이사회에서 Eurocrypt'92 개최지 결정에 관한 회의에서 Eurocrypt'93을 개최키로 한 노르웨이와 경합을 벌였으나, 헝거리의 개최를 결정하였다고 한다.

헝거리는 우리나라와 유사한 점이 많다. 우선, 헝거리어는 한글과 같이 우랄 알타이어족에 속하며 헝거리인은 몽고족에게만 있다는 몽고 반점이 있다고 한다. 헝거리 역사상 징기스칸이 유럽까지 진출하였다는 것은 헝거리의 수도인 부다페스트("부다"라는 시와 "페스트"라는 시가 합쳐져 부다페스트가됨)에 있는 옛 성곽의 형상이 유목민의 천막 형태를 하고 있다는 것에서 알 수있었다.

부다페스트로부터 동남쪽으로 약 150Km에 떨어지고, 동유럽 최대의 호수인 Balaton 호수가 바로 옆에 있는 Fured 호텔에서 개최된 본 회의는 총 211명이 참가하였으며, 이중 독일 41명, 미국 30명, 프랑스 27명, 영국 14명, 스웨덴 14명, 헝거리 12명, 일본인 6명, 중국, 싱가폴 등에서 참가하였으며 한국에서는 4명 (ETRI 2명, ADD 2명)이 참석하였다.

본회의에는 발표 신청 논문의 88편 중 35편만이 (채택율 2.5) 프로그램 위원회에서 심사 결과 채택되었다. 본회의의 특징은 앞에서 서술한 바와 같이 동유럽 국가에서 개최되었다는 점과 운영 위원장과 프로그램 위원장을 일반적으로 개최국에서 모두 담당하였다는 전례와 달리 헝거리의 T.Nemetz와 스위스의 R.Rueppel이 각각 담당하였으며, "Trapdoor Primes and Moduli"라는 주제로 패널 토론이 있었다.

[1] 헝거리인은 자기들이 유럽의 중심이라고 자부하고 있어 자기 나라를 중유럽이라고 함.

패널 토론의 개최 목적은 최근 NIST가 제정 중인 DSS (Digital Signature Standard) 의 암호학적 안전성에 관한 공개 토론을 하기 위함이었다.

제2장에서는 본회의에서 발표한 논문을 중심으로 최근 암호학의 주요 연구 결과를 요약하고, 제3장에서는 패널 토론 내용을 정리하고 끝으로 결론을 맺는다.

2 주요 연구 결과

발표된 35편의 논문을 암호학의 주요 분야별 분류하면 표 1과 같으며 발표 논문의 제목과 저자는 부록을 참조바랍니다.

표 1: 발표 논문의 분류

분 류	편수	분 류	편수
비밀공유방법	2	의사랜덤치환발생기	3
해쉬함수	4	복잡도이론과 암호학	6
블럭암호	3	영지식증명	3
스트림암호	3	디지틀서명과 전자현금	3
공개키암호	6	기타	1
계		35	

2.1 비밀 공유 방법(2편)

이태리의 C. Blundo외 3인은 비밀 공유 방법을 위하여 그래프 이론적인 접근 방법를 시도하였다. 즉, 주어진 그래프에서 edge에 있는 사람은 비밀 정보를 계산할 수있고 edge에 없는 사람은 비밀 정보를 얻을 수없도록 하고 비밀 정보에 대한 각 조각(piece)을 분산할 수있는 최적 정보량과 평균 정보량을 제시하였다. Y. Desmedt외 1인은 유한 아벨군(Abelian Group) 상에서 이상적인 homomorphic 비밀 공유 방법에 대한 분류를 하였다. 이상적인 homomorphic 비밀 공유 방법이란 비밀 정보의 조각들의 곱셈이 비밀 정보의 곱셈의 조각과 동일 할때를 의미하며 이상적인 homomorphic 비밀 공유 방법이 존재하지 않는 아벨군이 많이 존재한다는 것을 증명하였다.

2.2 해쉬 함수(4편)

프랑스의 T. Baridaud외 3인은 Crypto'91의 Rump Session에서 C. Schnorr가 발표한 FFT(Fast Fourier Transform)를 이용한 해쉬함수가 충돌을 일으킴 (not collision-free)을 제시하였고 충돌 쌍을 찾는 데는 Schnorr가 제안한 변형된 해쉬함수의 2^{23} 회의 연산으로 가능하다고 하였다. 이것은 실제로 SUN III Workstation에서 수시간, SPARC Workstation에서는 한시간이내에 충돌쌍을 찾을 수있다고 주장하였다. 이결과는 Asiacrypt'91의 Rump Session에서도 유사한 결과가 발표되었다. 곧이어, Schnorr는 위의 공격 방법에 대한 대책으로 FFT-Hash II라고하는 개선된 해쉬함수를 제시하였다. 이 개선된 해쉬함수는 개선전의 해쉬 함수와 동일하게 임의의 크기의 입력 메세지에 대해 128빗트의 해쉬값을 얻으며 FFT와 유한체상의 다항식을 사용하였다. 서로 다른 입력 메세지에 대한 128빗트의 동일한 해쉬값은 최대 2^{-120}의 확율로 발생하여 거의 무시할 정도라고 주장하였다.

X. Lai외 1인은 블럭 암호를 이용하여 해쉬 함수를 구성하는 방법을 제안하였는데 m 빗트의 블럭 암호를 이용하여 $2m$ 빗트의 해쉬값을 얻는 방법이다. 미국의 Anagram Lab.의 사장인 T.A. Berson은 RSA Data Security Inc.의 Rivest가 제안한 해쉬함수인 MD5(Message Digest 5)중 일부분인 2^{32} Modulus 연산을 Differential Cryptanalysis으로 해독하는 방법을 제안하였다.

2.3 블럭 암호(3편)

일본의 M. Matsui외 1인은 일본의 NTT가 1977년 제안한 FEAL (Fast data Encipherment ALgorithm) 암호계에 대한 새로운 KPA(Known Plaintext Attack) 방법을 제안하였다. 이방법으로 FEAL-4는 5개의 알려진 평문, FEAL-6는 100개의 알려진 평문으로 각각 해독되며 FEAL-8은 전수 탐색 방법(Exhaustive Search) 보다 빠른 2^{15}개의 알려진 평문으로 해독될 수 있다고 발표하였다. 이방법으로 7 라운드의 FEAL 즉, FEAL-7을 해독하는 데는 HP9425 Workstation (68040/25MHz) 상의 C 언어와 어셈블리 언어 및 700KByte의 메모리를 사용하여 170 시간이 소요되었다고 발표하였으며, FEAL-8인 경우는 해독에 필요한 계산량을 산정하였다. 독일의 K. Nyberg는 높은 비선형도를 갖는 치환 함수의 구성법에 대하여 제시하였다. 이 방법은 유한체상의 치환 함수가 주어졌을 때 그의 역함수도 동일한 비선형도를 유지하면서 이차 결합을 이용하여 임의의 입력 크기를 갖는 치환 함수를 구성하는 방법이다. 또한, 독일의 R. Wernsdrof는 유한 단순체 (simple group)의 분류를 한 P.J. Cameron의 결과를 이용하여 1 라운드의 DES (Data Encryption Standard)는 대수학적으로 Alternating Group이 된다는 것을 증명하였다. 그러나 16 라운드의 DES는 Alternating Group이 되는 지 여부는 아직 불확실하다.

2.4 스트림 암호(3편)

유고의 J.D. Golic은 스트림 암호에서 사용되는 수열 혼합기(combiner)를 일반화하여 내부 메모리 입력 빗트가 임의인 경우에도 상관 공격 방법 (correlation attack)을 제시하였다. 아울러 그는 잡음이 있는 선형 쉬프트 레지스타에 의한 발생 수열을 Bayesain 적 (product)를 응용한 에러 정정 방법을 정보이론적으로 접근하였다. 이분야에는 발표자 (L. O'Connor)가 불참한 논문으로 "Suffix Tree and Sequence Complexity"가 있었는 데 유한체 상의 원소로 주어진 수열의 선형 복잡도를 산출하는 방법으로 suffix tree라는 데이타 구조를 이용하는 방법을 제시하였다.

2.5 공개키 암호(6편)

독일의 B. Pfitzmann외 4인은 일본의 T. Matsumoto외 2인이 제안한 RSA 공개키 암호의 의뢰 계산 (Server-aided Computation) 프로토콜에 대한 수동 (passive) 및 능동 (active) 공격 방법을 제안하고 Quisquater외 1인이 제안한 의뢰 계산 프로토콜에 대하여도 공격 방법을 제안하였다. S. Vanstone외 2인은 공개키 암호로서 약 100 빗트정도의 키 사이즈를 갖는 타원 곡선을 이용한 암호계를 제안하였다. 이로서 기존의 공개키 암호계 중 가장 키사이즈가 작은 암호계를 구성할 수 있다고 주장하였다. J. Sauerbrey외 1인은 멱승을 효율적으로 계산하는 한가지 방법으로 addition chain을 이용할 때, 중간 값을 계산하는 데 소요되는 연산의 회수와 저장되는 레지스터의 수를 추정하였다. E. Brickell외 4인은 유한체상에 원소 g가 주어지고 멱승을 계산하는 경우, 곱셈의 연산 회수를 줄여 고속 계산이 가능한 addition chain을 이용하는 방법을 제안하였다. g^n $(n < N)$의 계산에 $O(\log N/\log\log N)$의 군 곱셈에 계산 가능이고, 이방법을 병렬화 할때는 $O(\log N/\log\log N)$ 의 프로세서로 $O(\log\log N)$의 군 곱셈으로 연산 가능함을 제시하였다.

M.J. Beller외 2인은 휴대용 통신 시스템에 적합한 DH (Diffie-Hellman) 키분배 방식을 일괄 (batch) 연산하는 방법을 제시하였다. 이방식은 휴대용 통신 방식에서 발생하는 신호의 지연 문제를 해결하기 위하여 Fiat가 제안한 batch RSA 연산 방법을 batch DH 연산 방법으로 확장한 내용이다. K. Iwamura외 2인은 RSA 암호를 가장 고속으로 실현할 수 있는 방법으로 systolic 배열 구조를 이용하여 512 빗트의 modulus 값에 512 빗트의 멱승 계산에 25,000Gate가 필요하며 50 Kb/s의 속도로 처리할 수 있다고 주장하였다.

2.6 의사 랜덤 치환 발생기(3편)

U.M. Mauer는 Luby와 Rackoff가 제안한 의사 랜덤 함수로 부터 의사 랜덤 치환을 구성할 수 있는 방법을 간략화하거나 일반화하는 방법을 제시하였다. 이결과는 암호학에 있어서 확율이론과 복잡도 이론간

의 관계를 분명히 할 수 있다고 주장하였다. J. Patarin은 3 라운드의 DES-like 치환과 한개의 의사 랜덤 함수로서 의사 랜덤 치환기를 발생할 수 있으며 4 라운드의 DES-like 치환과 1개의 의사 랜덤 함수로서 초의사 랜덤 (super pseudorandom) 치환 발생기를 구성할 수 있다고 주장하였다. 위와 유사한 결과로 B. Sadeghiyan외 1인은 한개의 의사 랜덤 함수 발생기로 부터 초의사 랜덤 치환 발생기를 구성하는 방법을 제안하였다.

2.7 복잡도 이론과 암호학(6편)

D. Beaver는 Boer가 Eurocrypt'91에서 발표한 OT (Oblivious Transfer) 프로토콜의 해독 방법을 제시하면서 현재 까지의 OT의 정의에 대한 모순점을 지적하였다. P. Barbaroux는 다항식 안전성에 대하여 표본화 기법을 응용하여 uniform 결과를 얻을 수 있도록 충분 조건을 제시하였다. 이 결과는 Yao가 제안한 next-bit test의 universality를 일반화한 내용이다. D. Beaver외 1인은 다자간 계산 프로토콜을 구성할 때에 동적 방해자 (dynamic adversary) 에 대한 안전성을 증명할 수 있는 프로토콜을 제시하였다. 또한, H. Niederreiter외 1인은 일방향 함수에 대한 부분적인 랜덤성 (local randomness) 를 정의하고 다항식을 이용한 해쉬 함수의 구성 방법에 대하여 논하였다. T. Okamoto외 2인은 유한군 G 상에 이산 대수 문제를 일반화하여 GDL (Generalized Discrete Logarithm) 이라 하면 복잡도 이론 상 G가 $NP \cap co\text{-}NP$ 에 있으면 GDL이 $NP \cap co\text{-}AM$에 있음을 증명하였다. 이를 확장하면, 동일한 가정하에 GDL이 $MA \cap co\text{-}AM$ 에 있음을 증명할 수도 있다고 주장하였다. U.M. Mauer는 임의의 질문에 대하여 yes 또는 no 만을 답하는 oracle의 도움을 받아 n 빗트 정수의 소인수 분해 문제를 풀 수 있는 흥미로운 방법을 제안하였다.

2.8 영지식 증명(3편)

K. Ohta외 2인은 영지식 대화형 증명 (ZKIP, Zero Knowledge Interactive Proof)의 전달성 (diversibility)에 대한 문제점으로 mafia-fruad attack과 multi-verifier attack에 대하여 안전한 divertible-free ZKIP를 제안하였다. I.Damgard는 회로 만족성 (circuit satisfiability)에 대한 비대화형 완전 영지식 증명 시스템을 제안하였다. 이프로토콜은 3-SAT 문제 또는 그래프 일주성 문제 (graph Hamiltonity)에 Karp 축략 (reduction)을 하지 않고 어떠한 NP 문제를 비대화형으로 증명할 수 있는 특징을 갖는다. I. Biehl외 4인은 지금까지 알려진 영지식 증명법에서 영지식 성질을 증명하는 도구를 제안하였다. 이 방법은 2개의 확율적 튜링 기계의 출력 분포상 회로 구분 불능성(circuit indistiguishability)을 어떤 서브루틴상의 구분 불능성으로 환원됨을 이용한 것이다.

2.9 디지틀 서명과 전자 현금(3편)

E.van Heyst외 1인은 서명자가 무한대로 강력한 위조자로 부터 안전한 성질을 갖는 fail-stop 서명 방식을 효율적으로 구성하는 방법을 제안하였다. J.H. Evertse외 1인은 서명 발행처가 서명을 발행하여 여러 사람에게 제공하는 대화형 프로토콜에서 RSA 서명으로 부터 새로운 RSA 서명을 계산하는 방법을 제시하였다. 또한, D. Chaum외 1인은 전자 현금을 전달할 때 각각의 지불시마다 표현하여야하는 빗트 정보가 증가하는 것을 방지하면서 전달할 수 있는 전자 현금 방식을 제안하였다.

2.10 기타

B.Dixon외 1인은 타원 곡선을 이용하여 병렬 처리가 가능한 소인수 분해 방식을 제안하였는 데, Montgomery가 제안한 곱셈 방식을 systolic 구조로 SIMD (Single Instruction Multiple Data) 방식의 병렬 처리가 가능토록 한 실현 방식이다.

3 패널 토론

회의 2일째인 1992년 5월 26일 (화) 오후 4시 부터 6시 까지 2시간에 걸쳐 "Trapdoor Primes and Moduli"라는 주제로 패널 토론이 있었다. 패널참가자는 표 2에 나타내었다. 사회자인 Rueppel은 동전

표 2: 패널 참가자

국 명	소 속	성 명	비 고
스위스	R^3 Security Inc.	R.Rueppel	사회자
미국	Bellcore	A.Lenstra	
미국	NIST	M.Smid	
미국	Sandia Nat'l Lab.	K.McCurley	
미국	U. of Wisconsin	Y.Desmedt	
미국	AT& T	A.Odlyzko	
덴마크	Aarhus U.	P.Landrock	신임 IACR 회장

던지기로 발표 순서를 정하였다 하면서, 암호학 전반에 걸친 배경 설명을 하였다. 현재와 같은 정보화 사회에 있어서 데이타를 전자적인 수단으로 전송하는 데에는 표준국, 제조자, 특허 소유자, 정부, 법률가, 정치가, 암호 해독자, 범죄자 등의 여러 분야의 사람들의 각각 다른 입장에서 정보 보호에 관심이 있다는 점을 처음 설명하고 trapdoor prime은 암호학적으로 약하지만 강한 솟수라고 정의하고 DSS (Digital Signature Standard) 알고리즘에 대하여 소개하였다. DSS의 구체적인 내용은 참고 문헌 [1]에 상세히 소개되어 있으므로 참조바랍니다. 이어, Lenstra는 RSA 암호에 있어서 trapdoor modulus ($n = p \cdot q$) 를 생성할 수 있는 방법을 소개하였다. 예를 들면, p를 랜덤하게 생성하고, 작은 ϵ에 대해 $q = p + S + \epsilon$ 이 되도록 q를 생성하고 n 값을 정하여 공개하였을 때 특정 패턴 S를 알고 있는 사람은 쉽게 n를 소인수 분해가 가능하다. 따라서 이러한 n 값이 trapdoor가 있는 modulus가 된다.

NIST 소속인 Smid는 현재 표준 제정가로서 고소를 당할 지경에 까지 이르렀다고 호소하면서, NIST가 제정중인 DSS에 trapdoor가 있다고 하는 사람보다 없다는 사람보다 훨씬 더많다고 하였다. DES의 경우, 아직 trapdoor는 찾아지지 않았다고 주장하면서 DSS에는 절대 trapdoor가 있을 수 없다고 주장하였다. 그러면, 도대체 trapdoor는 무엇인가에 대하여 그는 trapdoor는 의도적이어야 하며, 취약한 키가 trapdoor이며, 암호 시스템이 안전하다는 것을 어떻게 보장할 것인가에 대해 의문을 제기하였다. 암호 시스템에 가능한 취약점이 가능한 trapdoor가 될 수 있으며, 그것이 결국 trapdoor가 된다고 하였다. DSA (Digital Signature Algorithm)에는 취약한 솟수가 trapdoor가 될 수 있으나 랜덤하게 솟수를 생성하면 문제가 없으며 아직까지 DSA에 구체적인 trapdoor가 있음을 제시한 사람은 아무도 없다고 주장하였다. 앞으로 NIST는 DSS에 대한 계획으로, 공개 수집한 DSS에 대한 코멘트를 평가 및 응답, DSS에 대한 workshop개최, 필요시 DSS의 개정 등을 고려하고 있다고 밝혔다.

McCurley는 trapdoor에 대한 정의로 American Heritage 사전에는 "A hinged or sliding door in a floor, roof or ceiling"로 설명되어 있고 1986년 OECD (Organization for Economic Cooperation and Development) Supplement에는 "A piece of secret information that makes it easy to solve or otherwise very difficult"라고 정의되어 있다고 지적하면서, DES, RSA 등 대부분의 암호 시스템에는 모두 취약한 키가 존재한다고 하였다. 따라서 DSS에도 trapdoor가 존재할 가능성은 절대 배제할 수 없다고 주장하였다.

Desmedt는 trapdoor prime이란 사용자에 의해 선택되고 표준화된 솟수는 아니라고 정의하면서, DSA의 p와 q 값의 크기를 NIST가 축소 조정하였으며 multiplicative attack의 가능성이 있을 것이라고 주장하였다. 그는 현재 512빗트로 고정된 modulus의 값을 최대 1024빗트로 증가시켜야 한다고 결론지었다. Odlyzko는 trapdoor prime이 문제가 아니라 소인수분해 기술의 발전을 우려하였다. 그는 현재 115 자리의 합성수의 소인수분해에 약 400MIPS/year가 소요되며 129 자리의 합성수는 약 6,000MIPS/year

가 소요될 것이라고 하였다. 이는 1977년에 38자리에서 45자리의 합성수의 소인수 분해가 가능하였다는 점을 상기시키면서, 현재 당시와 비교하면 계산 능력은 1,000배 - 10,000 배가 증가됨을 의미하며 그중 소인수분해 알고리즘의 향상도 있었음을 주장하였다.

Landrock은 솟수 발생 방법을 국제적으로 동일하게 하고 그중 취약한 키가 될 수있는 솟수는 사용전에 배제하면 trapdoor에 대한 대책이 될 수 있을 것이라 주장하면서 키발생 방법의 표준화를 강조하였다.

곧이어 사회자는 청중들로 부터 질문을 받았다. 청중중 Diffie의 질문이 있었는 데, Smid(NIST)에 대하여 DSA의 실현 여부와 응용 방법에 관한 질문이었다. Smid는 DSA를 386PC 상에서 구현하였으며 응용에는 전자 우편, 스마트 카드 등에 응용이 가능하다고 하였다. ISO의 표준위원회의 의원인 Rueppel은 현재 DSA는 아직 ISO의 표준화는 되어 있지 않았다고 첨언하였다. 끝으로 Smid는 NIST의 현재 입장을 다음과 같이 발표하였다.

- 누구나 DSA를 실현할 수 있으며 로알티는 없슴.
- 특허 출원되어 있지 않음.
- Shamir 교수외 1인의 코멘트가 접수되어 검토 중.
- 국제적으로는 DSA의 제작시 제작자의 integrity를 유지.

NIST가 DES를 표준화를 1977년에 시행한 지 15년후에야 공개키 암호 시스템의 표준화가 거론되고 있다는 점은 암호학의 응용이 단순한 정보의 비밀 유지 차원에서 주요 정보의 인증 차원까지 실용화 단계에 이르렀슴을 알 수있었다. 또한, 지금까지의 암호학 국제 회의 중 최초로 시행한 패널 토론은 주어진 주제에 대하여 토론자의 논리적인 주장과 사회자의 능숙한 진행으로 성공적이었다고 평가된다.

4 결론

본고에는 최근 암호학의 연구 동향을 패널 토론 내용을 포함하여 Eurocrypt'92를 통하여 조사 분석하였다. 본 회의의 최대 관심사는 1990년 Biham과 Shamir가 발표한 DES 형태의 블럭 암호를 해독하는 Differential Cryptanalysis에 맞추어 지는 듯하다. 그 결과가 1977년 NIST가 표준화한 DES 알고리즘이 갖고 있는 trapdoor라고 까지 주장하는 학자들도 있다.

암호 설계자가 암호 알고리즘을 최선을 다하여 설계하였다 하더라도 해독자의 시각에서 그 알고리즘의 해독에 적합한 최적의 해독 방식을 찾아 내어 공격하는 방법을 공표한다. 이에 설계자는 공표된 특정 공격 방법에 견딜 수있는 알고리즘을 변경 설계한다. 이로서 설계자에게는 더욱 안전한 암호 알고리즘을 설계하는 기회가 주어지고 사용자에게는 신뢰할 수있는 알고리즘을 제공할 수있다. 이를 바탕으로 암호학은 설계자와 해독자 간의 상호 보완적 연구로 지속적으로 발전하는 분야로 생각된다.

참고 문헌

[1] The Digital Signature Standard, Com of ACM, pp.36–54, Vol.35, No.7, 7, 1992.

부 록 : EUROCRYPT'92 PROGRAM

SUNDAY, 24th May, 1992

16:00 - 22:00 Registration
20:00 - 22:30 Informal meeting with snack and wine

MONDAY, 25th May, 1992

07:00 - 08:50 Breakfast
09:00 - 14:00 Registration
12:00 - 13:30 Lunch
13:30 - 14:00 Photography of the participants at the Hotel-entrance

SESSION 1 : SECRET SHARING
— Chair: Tor Helleseth

14:00 - 14:30 **Welcome and opening remarks**
14:30 - 15:00 *Graph decompositions and secret sharing schems*, C.Blundo,A.De Santis D.R.Stinson, U.Vaccaro (University of Salerno,Italy)
15:00 - 15:20 *Classification of ideal homomorphic threshold schemes over finite Abelian groups*, Y.Frankel,Y.Desmedt (University of Wisconsin, Milwaukee, USA)
15:20 - 15:50 Coffee and Tea

SESSION 2 : HASH FUNCTIONS
— Chair: Jacques Stern

15:50 - 16:20 *FFT hashing is not collision-free*, T.Baritaud, H.Gilbert (CNET/PAA), M.Girault (SEPT,France)
16:20 - 16:40 *FFT-Hash II, Efficient Cryptographic Hashing*, C.P.Schnorr (Frankfurt University, Germany)
16:40 - 17:00 *Hash functions based on block ciphers*, X.Lai, J.L.Massey (Institut for Signal and Information Processing,Zurich)
17:00 - 17:20 *Differential cryptanalysis mod* 2^{32} *with application to MD5*, T.A.Berson (Anagram Lab., USA)

18:30 - 19:00 Departure for the welcome dinner
20:00 - 23:00 Welcome dinner at Restaurant Pegazus in Szentbékkáila

TUESDAY, 26th May, 1992

7:00 - 8:50 Breakfast

SESSION 3 : BLOCK CIPHERS
— Chair: Jeniffer Seberry

09:00 - 09:30 *A new method for known plaintext attack of FEAL cipher*,
M.Matsui, A.Yamagishi (Mitsubishi Corp., Kamakura, Japan)
09:30 - 10:00 *On the construction of highly nonlinear permutations*,
K.Nyberg (Finnish Defence Forces, Finland)
10:00 - 10:20 *The one-round functions of the DES generate the alternating group*,
R.Wernsdorf (Germany)
10:20 - 10:50 Lunch

SESSION 4 : STREAM CIPHERS
— Chair: Othmar Staffelbach

10:50 - 11:20 *Correlation via linear sequential circuit approximation of combiners*,
J.D.Golic, (University of Belgrade, Yugoslavia)
11:20 - 11:40 *Convergence of a Bayesian iterative error-correction procedure on a noisy shift register sequences*,
M.J.Mihaljevic, J.D. Golic (University of Belgrade, Yugoslavia)
11:40 - 12:00 *Suffix tree and sequence complexity*
L.O'Connor (University of Waterloo, Canada)
12:15 - 13:50 Lunch

SESSION 5: PUBLIC KEY I.
— Chair: Jovan Golić

14:00 - 14:20 *Attacks on protocols for server-aided RSA computation*,
B.Pfitzmann, M.Waidner (Karlsruhe University, Germany)
14:20 - 14:40 *Public-key cryptosystems with very small key lengths*,
G.Harper, A.Menezes, S.Vanstone (University of Waterloo,Canada)
14:40 - 15:00 *Resource requirements for the application of addition chains in modulo exponentiation*,
J.Sauerbrey, A.Dietel (München University, Germany)
15:00 - 15:30 Coffee or Tea

SESSION 6: FACTORING
— Chair: Rainer A. Rueppel

15:30 - 15:55 *Massively parallel elliptic curve factoring*,
B. Dixon, A.K.Lenstra (Bellcore, NJ, USA)
16:00 - 18:00 **The Eurocrypt'92 Controversial Issue:** *Trapdoor Primes and Moduli*
Panel Discussion.

20:00 - 24:00 **RUMP Session**
Co-ordinater:Laszlo Csirmaz (Math. Inst. of HAS, Budapest,Hungary)
Accepted Paper:*Secure Audio Teleconferencing : A Practical Solution*
R.Heiman (Bellcore, USA)

WEDNESDAY, 27th May, 1992

7:00 - 8:50 Breakfast

SESSION 7 : PUBLIC KEY II
— Chair: Tatsuaki Okamoto

09:00 - 09:30 *Fast exponentiation with precomputation*, E.Brickell, D.M.Gordon, K.S.MaCurley, D.Wilson (Sandia Labs., Albuquerque,USA)
09:30 - 09:50 *Batch Diffie-Hellman key agreement systems and their application to portable communications*, M.J.Beller, Y.Yacobi (Bellcore, NJ, USA)
09:50 - 10:20 *High-speed implementation methods for RSA scheme*, K.Iwamura, T.Matsumoto (Canon Res. Center, Japan) H.Imai (Yokohama National Univ.)
10:20 - 10:50 Coffee

SESSION 8 : PSEUDO-RANDOM PERMUTATION GENERATORS
— Chair: István Vajda

10:50 - 11:15 *A simplified and generalised treatment of Luby-Rackoff pseudorandom generators*, U.M.Mauer (ETH Zürich, Switzerland)
11:15 - 11:40 *How to construct pseudorandom and super pseudorandom permutations from one single pseudorandom function*, J.Patarin (INRIA, France)
11:40 - 11:55 *A construction for super pseudorandom permutations from a single pseudorandom function*, B.Sadeghiyan, J.Pieprzyk (Univ. of New South Wales, Australia)

SESSION 9 : COMPLEXITY THEORY AND CRYPTOGRAPHY I
— Chair: Kevin McCurley

14:00 - 14:30 *How to break a "secure"oblivious transfer protocol*, D.Beaver (Penn State University, USA)
14:30 - 14:50 *Uniform results in polynomial-time security*, P.Barbaroux (University of Paris, France)
14:50 - 15:10 *Cryptographic protocols provably secure against dynamic adversaries*, D.Beaver (Penn State University), S.Haber(Bellcore,USA)
15:10 - 15:40 Coffee or tea

SESSION 10 : ZERO - KNOWLEDGE
— Chair : Yvo Desmedt

15:40 - 16:00 *Secure bit commitment function against diversibility*,
K.Ohta, T.Okamoto, A.Fujioka (NTT,Kanagawa,Japan)
16:00 - 16:20 *Non-interactive circuit based proofs and non-interactive perfect zero-knowledge with preprocessing*, I.Damgard (Aarhus University, Denmark)
16:20 - 16:40 *Tools for proving zero knowledge*,
I.Biehl, J.Buchmann, B.Meyer, C.Thiel, C.Thiel(Saarland Univ., Germany)
16:40 - 17:20 *IACR Business meeting*

20:00 - 23:00 Eurocrypt'92 Banquet

THURSDAY, 28th May, 1992

SESSION 11 : DIGITAL SIGNATURE AND ELECTRONIC CASH
— Chair : Peter Landrock

09:00 - 09:20 *How to make efficient Fail-stop signatures*, E. Van Heyst (CWI, Amsterdam),
T.P.Pederson (Aarhus University, Denmark)
09:20 - 09:40 *Which new RSA signatures can be computed from RSA signatures, obtained in a specific interactive protocol ?*,
J.H.Everste, E. van Heyst (CWI,AMsterdam, The Netherlands)
09:40 - 10:00 *Transfered money grows*, D.Chaum (CWI, The Netherlands),
T.P.Pederson (Aarhus University, Denmark)
10:00 - 10:40 Coffee

SESSION 12 : COMPLEXITY THEORY DIGITAL AND CRYPTOGRAPHY II
— Chair : Joan Feigenbaum

10:40 - 11:00 *Local randomness in candidate one-way functions*, H.Niederreiter (Austrian Acad. of Sci. Austria), C.P.Schnorr (Frankfurt University, Germany)
11:00 - 11:20 *How intractable is the discrete logarithm for a general group*,
T.Okamoto (NTT Labs.), K.Sakurai(Mitsubishi Corp.),
H.Shizuya (Tohuku Univ.)
11:20 - 11:40 *Factoring with an Oracle*,
U.M.Maurer (ETH Zürich,Switzerland)
11:40 - 12:00 **Closing Remarks**
12:00 - 13:40 Lunch