스트림 암호의 발전 방향

국가보안기술연구소 염용진* · 홍 진 · 지성택

1. 서 론

암호는 과거에는 군사적인 용도 등의 비밀통신을 위하여 주로 사용되었으나 현재는 인터넷 기반의 사회·경제 활동의 안전성, 신뢰성, 프라이버시 보호 등을 위한 핵심 기술로서 메일전송, 사용자 인증, 전자상거래 등에서 널리 사용되고 있다. 점차 암호기술은 특정분야에서 사용하는 특수기술에서 차세대 환경의 기반기술로 변화하고 있으며 중요성이 증대되고 있다.

암호 알고리즘은 크게 나누어 비밀키 암호와 공개키 암호 알고리즘으로 나누어진다. 공개키 암호는 RSA 암호와 같이 암호화와 복호화에 사용되는 키가 다른 암호이며 인터넷 기반의 전자상거래에 주로 사용되고 있다. 비밀키 암호는 대칭키 암호라고도 불리며 주로 고속의 암호화에 사용된다. 비밀키 암호의 가장 대표적인 예는 블록 암호로 미국의 표준인 AES[1], 우리나라의 SEED[2], ARIA[3] 등이 있다. 스트림 암호는 블록 암호와 함께 비밀키 암호의 대표적인 암호화 방식이다. 현재 가장 널리 사용되는 스트림 암호는 RC4로 SSL 등에서 사용된다.

블록 암호의 설계기술은 1990년대 말부터 시작되어 2000년에 종료된 미국의 표준 블록 암호 공모사업을 계기로 비약적으로 발전하였다. 현재는 어느 정도 정형화된 설계가 이루어지고 있으며 고속화와 경량화의 연구도 활발하다. 한편, 스트림 암호의 경우 현재까지 널리 사용되던 구성요소인 선형 궤환 시프트 레지스터(LFSR)가 대수적 공격이라는 새로운 분석법에 의하여 안전성이 크게 위협받고 있으며 블록 암호 기술의 발달로 스트림 암호가 적용되던 많은 환경에서 블록 암호로 대치되는 현상이 나타나기도 한다. 또한, 스트림 암호의 설계기법에 대한 연구도 상당히 산만하게 진행되고 있다. 최근 수년간 매우 많은 스트림 암호가 제안되고 있으나 분석기법의 발전으로 그중 상당수가 안전성에 문제가 있는 것으로 밝혀졌다. 따라서 스트림 암호의 연구에는 해결해야할 과제가 많이 남아있으며 비밀키 암호 분야에서 앞으로 해쉬 함수와 함께 스트림 암호의 연구가 활발히 전개되리라 생각된다.

본 고에서는 스트림 암호의 최신 동향을 살펴보고 향후 스트림 암호의 발전 방향을 전망해 본다.

2. 스트림 암호의 소개

2.1 스트림 암호의 정의

이론적으로 가장 안전한 암호는 Vernam 암호라 불리는 one-time-pad 암호이다. 이 암호는 평문(P)과 같은 길이의 비밀정보인 키(K)를 사용하여 암호문(C)를 생성하는 방식으로 다음과 같이 암호화 및 복호화를 수행한다.

- 암호화: $C = P \oplus K$
- 복호화: $P = C \oplus K$

이 암호 방식은 길이가 긴 평문을 암호화하는 경우 사전에 공유해야 하는 비밀키(K)의 크기가 너무 크다는 문제가 있다. 이러한 문제를 해결하기 위하여 작은 키로부터 충분히 긴 키수열($G(K)$)을 발생시켜 Vernam 암호와 유사한 동작을 하도록 설계한 암호가 스트림 암호이다. 안전한 스트림 암호가 되기 위해서는 그림 1의 키수열 생성기(G)가 작은 키(K)로부터 난수와 구별이 불가능한 우수한 키수열을 출력할 수 있어야 한다. 암복호 원리는 Vernam 암호의 경우와 유사하다. 수식으로 표현하면 아래와 같다.

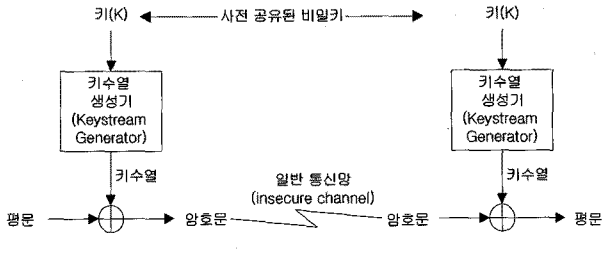

그림 1 스트림 암호 통신 모델

* 정회원

◦ 암호화: $C = P \oplus G(K)$
◦ 복호화: $P = C \oplus G(K)$

2.2 스트림 암호의 구성

스트림 암호를 설계하는데 오랫동안 가장 널리 사용된 구성 요소는 선형 궤환 시프트 레지스터(LFSR, Linear Feedback Shift Register)이다. LFSR은 그림 2와 같이 각 비트를 저장하는 메모리와 그 내용을 업데이트 하기 위한 궤환 다항식으로 구성된다[4].

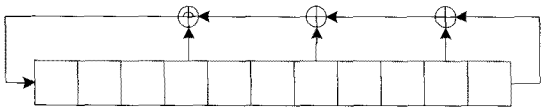

그림 2 선형 궤환 시프트 레지스터(LFSR)의 예

LFSR을 여러 개 결합하는 방법으로 스트림 암호를 구성할 수 있다. 여러 개의 LFSR을 반복적으로 동작시키면서 각 LFSR의 상태(state)비트를 비선형 논리로 결합하여 키수열을 생성하는 방식이 주로 사용된다. 최근까지 LFSR을 기반으로 하는 암호가 스트림 암호의 주류를 이루었으며 상용 알고리즘으로 블루투스[5]에 사용되는 E0, 유럽의 GSM에 쓰이는 A5/1, A5/2 등이 이러한 구조를 택하고 있다.

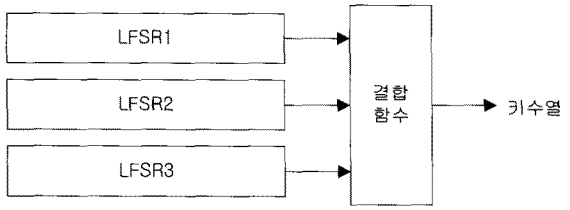

그림 3 LFSR 기반 스트림 암호의 예

이러한 구조는 경량의 하드웨어 구현에 유리하며 비트 단위의 출력이 필요한 경우에 적합하다. 또한 수학적으로 출력 키수열의 주기를 계산하기 쉬운 장점이 있다. 하지만 소프트웨어로 구현하는 경우는 상당한 효율성 저하를 감수해야 한다.

LFSR의 기본 연산 단위를 비트에서 바이트 혹은 워드로 바꾸어 고속 소프트웨어 구현이 가능하도록 하는 시도로 SNOW, Sober 등의 암호가 설계되었다. 이 암호의 안전성에 대한 검증은 아직 충분히 이루어지지 않았으나 최근 워드 단위의 LFSR의 주기를 계산하는 방법 등이 발표되어 향후 새로운 설계 방향을 이룰 것으로 생각된다. 또 다른 변형으로는 LFSR의 궤환 함수를 비선형으로 바꾼 FCSR(Feedback Carry Shift Register)나 NFSR(Nonlinear Feedback Shift Register) 등이 있다.

스트림 암호의 설계에 LFSR 계열만 사용된 것은 아니다. 가장 널리 사용되는 스트림 암호인 RC4의 경우는 블록 암호에서 사용하는 논리를 채택하여 비교적 고속의 소프트웨어 구현이 가능하다.

2.3 상용 스트림 암호

본 소절에서는 현재 널리 사용되고 있는 스트림 암호에 대하여 살펴보도록 한다.

2.3.1 RC4

1987년 RSA사의 Rivest가 설계한 스트림 암호로 비공개 알고리즘이었으나 1994년 역어셈블리 방식으로 그 구조가 인터넷에 공개되었다. 바이트의 치환을 기본 동작으로 하여 내부 상태를 갱신하는 방식으로 동작하며 산업계의 실질적인 표준으로 자리잡고 있다. 많은 암호학자들의 관심을 받았으나 대부분의 키 복구 공격에 대하여 현재까지 안전하다고 여겨지고 있다. 다만, 출력 키수열과 랜덤함수를 구별하는 distinguishing 공격[6,7]이 발표되었고 무선환경인 WEP[8]에 적용되는 경우 재동기 과정에서의 문제가 발견되기도 하였다.

2.3.2 A5/1, A5/2

유럽에서 사용되는 GSM 휴대전화는 A5라는 암호 알고리즘을 사용한다. 이 알고리즘 역시 처음에는 비공개 알고리즘이었으나 RC4와 마찬가지로 결국 밝혀지고 말았다. LFSR 방식을 채택한 암호로 하드웨어에 적합한 경량 암호로 제작되었다. A5/2는 공개된 후 곧바로 해독되었으며, A5/1도 TMTO(Time Memory Trade Off) 공격에 의하여 분석되었다[9]. 이러한 결과로 A5/3가 새로 추가되었는데 A5/3[10]는 블록 암호 KASUMI를 사용한다.

2.3.3 E0

블루투스(Bluetooth) 무선 환경에서 사용되는 스트림 암호인 E0는 합이 128비트인 4개의 LFSR로 이루어져 있으며 64비트 키를 사용한다. 현실적인 적용에서는 아직 안전하지만 많은 분석 결과들이 발표되어 안전성에 위협이 되고 있다.

3. 주요 프로젝트 및 표준화

3.1 NESSIE 프로젝트

NESSIE(New European Schemes for Signature, Integrity, and Encryption) 프로젝트[11]는 2000년부터 3년간 진행된 유럽의 암호 프리미티브 공모 사업이다. 이 프로젝트에서는 스트림 암호 뿐만 아니라 블록 암호, 해쉬함수, 공개키 암호, 서명 등 공개키와 비밀키 암호 전반에 걸친 공모가 있었다. 주요 일정은 표 1과 같다.

이 프로젝트에는 5개의 스트림 암호를 포함한 42개의 암호 알고리즘이 제안되었다. 1차 평가와 2차 평가를 수행한 결과 총 12개의 알고리즘이 선정되었고 공모와는 관계없으나 널리 사용되거나 표준화 중인 5개의 알고리즘을 추가하는 것으로 프로젝트가 종료되었다.

표 1 NESSIE 프로젝트의 주요 일정

2000. 1	NESSIE 프로젝트 1st phase 시작
2000. 3	암호 프리미티브 공모
2000. 9	1차 NESSIE 워크샵 개최
2001. 6	알고리즘 1차 평가 완료 2nd phase 시작
2001. 9	2차 NESSIE 워크샵 개최
2002. 11	3차 NESSIE 워크샵 개최
2003. 2	4차 NESSIE 워크샵 개최
2003. 3	최종 보고서 완료 및 프로젝트 종료

제안된 스트림 암호 5개는 LILI-128, LEVIATHAN, Sober, SNOW, BMGL이다. 1차 평가를 마친 후 LILI-128과 LEVIATHAN이 탈락되고 최종 평가에서 모든 스트림 암호가 탈락되었다. 제안된 모든 암호가 탈락된 것은 스트림 암호 분야 뿐이다. 이러한 이유로 NESSIE 프로젝트의 후속으로 진행되는 ECRYPT 프로젝트에서 스트림 암호의 연구가 중요하게 다루어지게 되었다.

3.2 CRYPTREC 프로젝트

2000년 5월에 시작된 CRYPTREC(Cryptography Research & Evaluation Committe) 프로젝트[12]는 일본의 정보처리진흥사업협회(IPA) 주관으로 전자정부에 사용될 암호 알고리즘의 선정을 위하여 실시되었다. NESSIE 프로젝트와 마찬가지로 공개키 암호 및 비밀키 암호 전반에 걸친 공모가 추진되었다.

표 2 CRYPTREC 프로젝트의 주요 일정

2000. 5.	암호기술평가위원회 설치
2000. 6.	평가기준 공개 및 공모 시작
2001. 4.	CRYPTREC 2000 워크샵 개최
2002. 4.	CRYPTREC 2001 워크샵 개최
2002. 5.	암호 조달 가이드북 작성
2003. 5.	CRYPTREC 2002 워크샵 개최 알고리즘 최종 선정

이 프로젝트에는 총 48건의 응모가 있었으며 9개의 스트림 암호가 제안되었다. 1차 스크리닝 평가와 2차 상세평가를 거쳐 3개의 스트림 암호 MUGI, Multi-S01 및 RC4가 전자정부 추천 암호로 선정되었다. 2003년 5월 CRYPTREC 프로젝트는 종료되었고 현재 암호기술감시위원회에서 지속적으로 선정 알고리즘에 대한 안전성 검토를 하고 있으며 선정된 알고리즘의 안전한 구현을 위한 암호모듈위원회로 나뉘어 진행되고 있다.

3.3 표준화

블록 암호의 경우 미국의 AES, 한국의 SEED 등 각 국가에서 표준암호를 선정하여 사용하고 있다. 하지만 스트림 암호가 표준암호로 채택된 사례는 거의 찾아보기 어렵다. 현재 ISO 국제 표준암호 선정 작업이 진행 중이며 스트림 암호 분야는 MUGI와 SNOW 2.0에 대한 표준화 절차가 진행되고 있다. MUGI는 일본의 CRYPTREC에서 선정된 암호이며 SNOW 2.0은 NESSIE 프로젝트에서 탈락된 SNOW를 개선한 암호이다.

4. 최신 연구 동향

4.1 스트림 암호의 분석 기술

기존에 널리 사용되고 있는 스트림 암호의 안전성에 문제가 발견되고 있으며 스트림 암호의 분석 기술은 최근 큰 진전이 이루어지고 있다.

90년대까지 스트림 암호에 대한 가장 강력한 공격기법은 상관공격(correlation attack)이었다. LFSR기반의 스트림 암호에 대한 상관공격은 고속 상관공격(fast correlation attack)등으로 전개되며 20여 년간 가장 중요한 공격으로 인식되어 왔다[13,14].

2002년 3차 NESSIE 워크샵에서는 Sober에 대한 구별공격(distinguishing attack)[15]이 발표되면서 논란이 있었다[16]. 구별공격은 스트림 암호의 키수열과 난수열을 구분하는 것으로 아직까지 비밀키를 찾을 수 있는 방법으로 발전되지 않았기 때문에 현실적인 위협으로 받아들이기에는 어려운 면이 있다. 하지만 다양한 암호에 대한 구별공격이 계속 발표되고 있으며 구별공격은 NESSIE 프로젝트에서 스트림 암호가 선정되지 못한 근거 중 하나가 되었다. 최근에는 구별공격을 인정하는 것이 대세이며 유럽의 새로운 ECRYPT 프로젝트에서도 구별공격에 대한 안전성 입증을 암호 설계의 조건으로 포함시키고 있다.

대수적 공격[17]은 블록 암호의 분석법으로 연구가 시작되었으나 지금은 스트림 암호의 가장 강력한 공격 중 하나로 인식되고 있다. 입력과 출력의 대수적 관계식을 유도하여 대수방정식을 푸는 방식으로 스트림 암호를 공격하는 것으로 LFSR 기반의 암호가 주로 대수적 공격의 대상이 되었다. LFSR의 결합함수로 사용되는 논리의 대부분에서 대수적 공격에 대한 취약성이 발견되었다. 대수적 공격은 LFSR을 대치하는 새로운 스트림 암

호의 기본 논리의 개발을 가속화하고 있으며, 대안으로 Klimov, Shamir가 제안한 T-함수[18] 등이 거론되고 있다. 또 다른 설계 방향으로는 AES와 같은 블록 암호에 사용된 논리를 차용하여 스트림 암호를 구성하는 방법도 활발히 연구되고 있다. ISO 표준암호로 추진되고 있는 MUGI가 대표적인 예이다.

4.2 유럽의 SASC 학회

유럽에서 NESSIE 프로젝트의 뒤를 이어 추진하고 있는 ECRYPT(European Network of Excellence in Cryptology) 프로젝트[19]는 2004년부터 4년간 5개 분야의 암호기술을 다룬다. 비밀키 암호, 공개키 암호, 프로토콜, 암호 구현, 워터마킹으로 주제를 나누어 각 연구그룹을 운영하면서 진행된다. 그중 가장 먼저 열린 학회는 스트림 암호에 대한 학회인 SASC(the State of the Art of Stream Cipher)이다. NESSIE 프로젝트에서 스트림 암호를 선정하지 못한 부담감 등이 크게 작용했을 것으로 보인다. SASC 학회에서는 여러 개의 새로운 스트림 암호의 제안이 있었고, 설계, 분석 기술에 대한 논문이 다수 발표되었다. 특히 Shamir의 초청강연[20]과 워크샵의 마지막 프로그램으로 열린 패널 토의에서는 스트림 암호의 나아갈 방향을 전망하는 내용이 주로 발표되었다.

Shamir는 초청강연에서 스트림 암호가 당분간 예전과 같은 주목을 받기 어렵다는 주장을 하였다. 미국 표준 블록 암호 AES가 이미 충분한 속도를 제공하며 작은 크기로 구현 가능하기 때문에 산업계에서 AES의 스트림 암호 모드 동작으로 충분하다고 판단하고 있다고 전했다. 따라서 스트림 암호가 필요한 곳은 다음과 같은 2가지 극단뿐이라고 주장하였다.

- Gbps 급 초고속 소프트웨어 환경
- 초경량 하드웨어 환경

첫 번째의 경우 소프트웨어로 구현되는 라우터 등을 예로 생각할 수 있으며 두 번째의 경우는 전력, 면적 등의 환경이 열악한 이동통신이나 RFID 등을 말한다. 이러한 환경을 제외한 곳에서는 스트림 암호의 자리가 블록 암호로 대치되고 있는데 SSL의 RC4가 AES로 대치된다는 점과 유럽의 A5 알고리즘이 블록 암호 KASUMI로 바뀌는 점이 대표적이 사례이다.

Babbage[21]는 산업계를 찾아다니며 스트림 암호의 필요성에 대하여 조사한 결과를 정리하여 발표하였다. 대부분의 산업계에서 스트림 암호는 AES로 대치되는 경향을 보였으며 스트림 암호가 필요하다고 답한 경우는 짧은 재동기 시간과 초기값(IV)의 사용에 대한 중요성을 강조하였다. 주목할만한 새로운 점은 인증과의 결합이었다. 현재 사용된 암호와 MAC의 결합은 너무 느려서 이를 암호와 결합하는 시도가 중요하다고 보고 있다. 현재는 MAC의 속도가 암호화 속도에 비하여 현저하게 느리다는 것이다.

학회의 끝에서는 "The way Forward for Stream Cipher"라는 주제로 패널토의가 있었는데 ECRYPT 프로젝트에서는 스트림 암호의 선정, 표준화를 위한 작업을 준비하고 있다. 그러나 기존의 공모사업과는 달리 경쟁 과정을 통한 선정보다는 평가포럼을 운영하여 공감대를 형성하는 방향으로 진행될 예정이다. 이 패널토의에서 논의된 중요한 것을 정리하면 다음과 같다.

- LFSR기반의 스트림 암호의 회생가능성에 대한 의견교환이 있었으나 의견이 분분하였다. 가장 오랫동안 안전성을 검증해 온 논리이기 때문에 계속되어야 한다는 의견과 이제 대수적 공격으로 폐기해야 한다는 주장이 있었는데 폐기하자는 쪽이 약간 우세하였다.
- 앞으로 스트림 암호가 사용될 분야는 Shamir의 주장처럼 극단적인 두가지 환경이라는 데에 대체로 의견 일치가 있었다. 이제 더 이상의 범용 스트림 암호의 개발은 큰 의미가 없다고 생각된다.
- ISO에서 추진 중인 스트림 암호의 표준화 일정을 ECRYPT 활동을 반영하도록 늦추어야 하는지에 대한 의견교환이 있었다. 현재 표준화 후보로 거론되는 MUGI와 SNOW 2.0은 아직 충분히 성숙되지 못한 알고리즘이라는 의견이 있었으나 표준화는 그대로 진행하는 것이 더 좋다는 쪽으로 정리되었다.

이 토론을 바탕으로 전망한다면 적어도 민간 분야에서는 스트림 암호가 극단의 환경에서만 사용될 것이며 사용 환경의 특성을 최대한 반영하는 쪽으로 연구가 집중될 것으로 판단된다.

4.3 ECRYPT의 새로운 스트림 암호 포럼

앞에서 언급한 바와 같이 ECRYPT 프로젝트에서는 NESSIE 프로젝트에서 선정하지 못한 스트림 암호에 대하여 새로운 포럼를 추진하고 있다. 표준화나 경쟁적인 선정을 목표로 하지는 않고 스트림 암호를 제안받아 공개적인 평가포럼을 운영하는 방식이 될 것이다. 2005년 초에 새로운 암호를 제안 받고 2007년까지 2 단계에 걸친 평가를 추진하며 다음과 같은 4개의 분야로 나누어 진행한다.

- 데스크탑 환경에서 고속 구현이 가능한 암호(32비트, 64비트 프로세서)
- 8비트 환경에서의 우수한 성능의 암호
- 하드웨어 환경에서 고성능의 암호

◦ 특별히 열악한 환경에 사용될 암호

각 분야에 대하여 인증을 결합하는 것을 중요하게 고려하고 있다. 이 포럼의 운영을 통하여 스트림 암호의 개발에 대한 연구가 활성화 될 것으로 기대된다.

5. 결 론

비밀키 암호에서 블록 암호의 연구가 정형화되고 안정화되어 가는데 반하여 스트림 암호의 개발은 혼란을 거듭하고 있는 것으로 보인다. 기존의 상용 스트림 암호가 새로운 분석법으로 공격되고 있으며 새롭게 제안된 암호의 경우도 안전성의 문제로 공모에서 선정 되지 못하는 등 스트림 암호의 연구는 큰 진전을 보지 못하는 것으로 여겨진다.

본 고에서는 스트림 암호를 소개하고 스트림 암호의 최근 연구 동향을 살펴보았다. 특히 2004년 10월에 개최된 SASC라는 스트림 암호 학회에서 전문가들이 토의한 내용을 통하여 스트림 암호 연구를 전망하였고 2005년부터 새롭게 진행될 스트림 암호 포럼에 대하여 알아보았다.

많은 환경에서 스트림 암호가 블록 암호로 대치되는 경향을 보이고 있으나 초고속 소프트웨어 환경이나 초경량 하드웨어 환경에서의 스트림 암호에 연구는 앞으로도 활발히 진행되리라 전망된다. 특히, 유비쿼터스 컴퓨팅 환경과 같은 새로운 초경량 환경에서는 스트림 암호가 중요한 역할을 하리라 기대된다.

참고문헌

[1] AES, "Advanced encryption algorithm (AES) development effort," 1997-2000. http://csrc.nist.gov/encryption/aes/.

[2] SEED, "SEED 블록 암호 알고리즘". http://www.kisa.or.kr/seed/seed_kor.html.

[3] ARIA, "민관겸용 블록 암호 알고리즘 ARIA". http://www.nsri.re.kr/ARIA/.

[4] 강주성 외, "현대암호학", 경문사, 2000.

[5] B. SIG, "Bluetooth specification," Technical Report, http://www.bluetooth.com.

[6] I. Mironov, "(Not So) Random Shuffles of RC4", Advances in Cryptology - CRYPTO 2002.

[7] P. Souradyuti, B. Preneel, "Analysis of Non-fortuitous RC4 key stream generator," Progress in Cryptology - INDOCRYPT 2003.

[8] L. of the IEEE CS, "Wireless LAN medium access control (MAC) and physical layer (PHY) specifications," Technical Report, IEEE Standard 802.11, 1999.

[9] A. Biryukov, A. Shamir, D. Wagner, "Real time cryptanalysis of A5/1 on a PC," Proceedings of Fast Software Encryption - FSE 2000.

[10] G. O. Partners, "Specification of the 3GPP confidentiality and integrity algorithm: Kasumi algorithm specification - 3GPP TS 35.202," Technical Report, http://www.3gpp.org, 2000.

[11] NESSIE Project - New European Schemes for Signature, Integrity, and Encryption. http://cryptonessie.org/.

[12] CRYPTREC Project - Cryptography Research & Evaluation Committe. http://www.ipa.go.jp/security/enc/CRYPTREC.

[13] V. V. Chepyzhov, T. Johansson, and B. Smeets, "A Simple algorithm for fast correlation attacks on stream ciphers," Proceedings of Fast Software Encryption-FSE 2000.

[14] P. Chose, A. Joux, M. Mitton, "Fast correlation attacks:An algorithmic point of view," Advances in Cryptology - EUROCRYPT 2002.

[15] C. Canniere, J. Lano, P. Preneel, J. Vanderwalle, "Distinguishing attacks on Sober-t32," Proceedings of the 3rd NESSIE Workshop, 2002.

[16] P. Hawkes, G. Rose, "On the applicability of distinguishing attacks against stream ciphers," Proceedings of the 3rd NESSIE Workshop, 2002.

[17] N. T. Courtois, W. Meier, "Algebraic attacks on stream ciphers with linear feedback," Advances in Cryptology - EUROCRYPT 2003.

[18] A. Klimov, A. Shamir, "A new class of invertible mappings," Proceedings of CHES 2002.

[19] ECRYPT Project - European Network of Excellence in Cryptology. http://www.ecrypt.

eu.org/
[20] A. Shamir, "Stream ciphers:Dead or Alive," invited lecture at SASC 2004.
[21] S. Babbage, "Stream ciphers: What does the industry want?," Proceedings of SASC 2004.
[22] A. Biryukov, "Block ciphers and stream ciphers: the state of the art," IACR ePrint Archive 2004/094, 2004.

염 용 진

1991 서울대학교 수학과(학사)
1994 서울대학교 수학과(석사)
1999 서울대학교 수학과(박사)
2000~현재 국가보안기술연구소 선임연구원
관심분야 : 암호론, 정보보호
E-mail : yjyeom@etri.re.kr

홍 진

1994 서울대학교 수학과(학사)
1996 서울대학교 수학과(석사)
2000 서울대학교 수학과(박사)
2000~2002 고등과학원 연구원
2002~현재 국가보안기술연구소 선임연구원
관심분야 : 암호론
E-mail : jinhong@etri.re.kr

지 성 택

1985 서강대학교 수학과(학사)
1987 서강대학교 수학과(석사)
1999 고려대학교 수학과(박사)
1989~1999 한국전자통신연구원 정보보호연구본부 선임연구원
2000~현재 국가보안기술연구소 책임연구원
관심분야 : 암호론, 부울함수
E-mail : chee@etri.re.kr