모바일 멀티미디어 데이타를 위한, 의사난수생성기와 순열 기법을 결합한 효율적인 암호화 기법

(An Efficient Encryption Scheme Combining PRNG and Permutation for Mobile Multimedia Data)

한 정 규 † 조 유 근 ††
(JungKyu Han) (YooKun Cho)

요 약 디지털 저작권 관리 기법은 계산비용의 경감을 목적으로 컨텐츠 암호화를 위해 대칭 키 암호화 기법을 채택하였으며 데스크탑 환경에서는 강한 보안성과 적절한 암호화 속도를 가지는 AES를 주로 사용하고 있다. 그러나 낮은 성능의 프로세서와 제한된 전력환경에서 동작하는 모바일 기기에서는 더욱 낮은 계산 비용 실현과 에너지 소모 경감을 요구한다. 이에 본 논문에서는 모바일 기기에서 사용 가능한 효율적인 스트림 암호화 기법을 제안한다. 제안 기법은 의사 난수 생성기를 사용하여 원본 키 스트림을 생성한 다음 이에 동적 생성한 순열을 적용하여 확장 키 스트림을 생성한다. 확장 키 스트림을 평문과 논리합하여 암호문을 생성한다. 순열을 이용하여 키 스트림 생성에 사용되는 의사 난수 생성기의 사용 횟수를 줄였기 때문에 일반 스트림 암호화 기법에 비해 멀티미디어 데이타의 암/복호화 속도가 빠르며 에너지 소모를 줄였다. 특히 제안 기법은 멀티미디어 파일의 임의 접근 시 일반 스트림 암호화 기법에 비해 약 2배의 속도향상을 보인다.

키워드 : 멀티미디어 암호화, 스트림 암호화 기법, 모바일 디지털 저작권 관리, 순열

Abstract In Digital Right Management, symmetric cipher is used for content encryption to reduce encryption cost, AES, advanced encryption standard is usually used to multimedia encryption under desktop environment because of its reasonable security level and computation cost. But mobile handheld device often uses slow speed processor and operates under battery-powered environment. Therefore it requires low computation cost and low energy consumption. This paper proposes new stream cipher scheme which combines pseudo random number generator(PRNG) and dynamically generated permutations. Proposed scheme activates PRNG and generates original key streams. Then it generates extended key streams by applying permutation to original sequence. These extended key streams are XORed with plaintext and generate ciphertext. Proposed scheme reduces the usage of PRNG. Therefore this scheme is fast and consumes less energy in comparison with normal stream cipher. Especially, this scheme shows great speed up (almost 2 times) than normal stream cipher scheme in random access.

Key words : Multimedia encryption, Stream cipher, Mobile Digital Right Management, Permutation

· 이 논문은 2005년 정부(교육 인적 자원부)의 재원으로 한국 학술 진흥 재단의 지원을 받아 수행한 연구임(KRF-2005-042-D00294).

† 정 회 원 : NTT 정보유통플랫폼연구소 연구원
jirnanf91@hotmail.com
†† 정 회 원 : 서울대학교 전기컴퓨터공학부 교수
ykcho@snu.ac.kr

논문접수 : 2007년 1월 22일
심사완료 : 2007년 7월 19일

정보과학회논문지 : 시스템 및 이론 제34권 제11호(2007.12)

1. 서 론

모바일 기기에서 디지털 컨텐츠의 지적 재산권 관리를 위한 모바일 디지털 저작권 관리(Mobile Digital Right Management)가 중요해지고 있으며 OMA[]와 같은 표준화 단체가 모바일 디지털 저작권 관리 표준을 제시하고 있다. 디지털 저작권 관리는 디지털 컨텐츠를 대칭키 기법으로 암호화 하고 컨텐츠에 대한 권리를 명세한 권리 객체를 사용자의 공개키로 암호화하여 전달하는 방식을 사용함으로써 권한을 가진 합법적인 사용자만 컨텐츠를 사용 할 수 있도록 한다.

일반적으로 컨텐츠 암호화에 표준 블록 암호화 기법인 AES가 사용되지만[1] 모바일 휴대 기기는 대부분 낮은 성능의 프로세서를 가지며 전지를 전원으로 동작하기 때문에 암호화 알고리즘의 계산 비용과 에너지 소모를 가능한 한 줄여야 한다[2]. 계산 비용과 에너지 소모를 줄이면서도 디지털 저작권 관리의 사용 제어를 만족하기 위한 방법으로 선택적 암호화(Selective Encryption) 기법이 연구되어 왔다.

멀티미디어 데이타의 일부분만을 암호화하거나 변조시킴으로써 복호화 하지 않고 재생할 경우 데이타의 품질을 시청하기에 적합하지 않도록 만드는 기법이 선택적 암호화 기법이다[3]. 데이타 압축에 사용하는 허프만 표를 여러 개 사용하고 사용한 표를 암호화하는 기법[4], 동영상 압축의 변환 계수(transform coefficient)를 블록 혹은 세그먼트로 나눈 다음 일부 비트를 뒤섞거나 블록순서 변경, 회전을 통해 정상적인 영상이 출력되지 않게 하는 기법[5]등 다양한 기법이 제안되었으며 이들은 모두 적은 비용으로 멀티미디어 데이타 사용제어를 실현할 수 있다. 하지만 이 기법은 데이타의 대부분이 암호화 되지 않은 채 존재하기 때문에 불충분한 보안성이 문제가 되며 암호화가 멀티미디어 파일 압축 방식 고유의 특성을 이용하기 때문에 파일 압축과 암호화를 다른 계층으로 두고 독립적으로 접근하기 어렵다[3-5]. 결과적으로 파일 형식에 따라 서로 다른 암호화 기법을 적용하여야 하므로 선택적 암호화 기법은 범용성을 가지기 어렵다.

RC4와 같은 스트림 암호화 기법은 적절한 방법으로 사용할 경우 블럭 암호화 기법에 비해 빠른 속도와 개선된 에너지 효율을 지니면서도 동등한 수준의 안전성을 제공할 수 있으나[6,7] 데이타의 일부분만 복호화하려해도 그보다 앞의 데이타를 암호화할 때 사용한 임의 시퀀스를 모두 생성해야 하므로 사용자가 시청하려는 부분만 복호화하는 멀티미디어 데이타의 임의 접근 요구[8]를 지원하기 어렵다.

본 논문에서는 의사 난수 생성기와 동적 생성된 순열을 결합한 스트림 암호화 기법을 제안한다. 제안 기법은 의사 난수 생성기를 사용하여 원본 키 스트림을 생성한 후 이에 동적 생성한 순열을 적용하여 데이타 암호화에 필요한 키 스트림을 생성한다. 순열을 이용하여 키 스트림 생성에 사용되는 의사 난수 생성기의 사용 횟수를 줄였기 때문에 일반 스트림 암호화 기법에 비해 멀티미디어 데이타의 암/복호화 응답 속도가 빠르며 에너지 소모를 줄였다. 특히 멀티미디어 데이타의 임의 접근에 있어서는 일반 스트림 암호화 기법에 비해 약 2배의 응답 속도와 에너지 절약을 보인다.

본 논문의 2장에서는 제안 기법을 서술하고 3장과 4장에서는 제안 기법의 보안과 성능 및 비용에 대해 평가한다. 마지막 5장에서 전체 논문을 정리한다.

2. 순열 풀을 사용한 멀티미디어 파일 암호화 기법

2.1 개요

일반적인 스트림 암호화 기법은 의사 난수 생성기(Pseudo Random Number Generator)로 생성한 임의 시퀀스(Random Sequence)를 평문과 논리합하여 암호문을 생성한다. 따라서 평문의 크기가 클수록 스트림 암호화 기법의 전체 비용에서 임의 시퀀스 생성 비용의 비율이 커진다[7]. 멀티미디어 데이타는 매우 큰 크기를 가지므로 임의 시퀀스 생성에 필요한 비용을 감소시킬 수 있다면 전체적인 계산 비용 및 에너지 소모를 줄일 수 있을 것이다. 본 논문에서는 임의 시퀀스의 생성 비용을 줄이기 위해 순열(Permutation)과 의사 난수 생성기를 결합한 암호화 기법을 제안한다.

암호화 할 평문의 길이를 $N \cdot L$이라고 하면 의사 난수 생성기를 사용하여 길이 N의 임의 시퀀스를 L/2개 생성한다. 또한 길이 N인 임의 시퀀스의 원소 위치를 재배열하기 위한 순열을 i개 생성하여 순열 풀(Permutation Pool)을 구성한다. 이 때 i는 $\left(\frac{i}{2}\right) \geq \frac{L}{2}$를 만족한다. 의사 난수 생성기로 생성한 길이 N인 임의 시퀀스 L/2개에 순열 풀에서 추출한 두 개의 순열을 적용하여 길이 N인 임의 시퀀스 L개를 새로 생성한다.

필요로 하는 임의 시퀀스를 절반의 미리 생성해 놓은 임의 시퀀스에 순열을 적용하여 생성하기 때문에(그림 1) 난수 생성기의 사용 횟수를 줄여 일반 스트림 암호화 기법에 비해 적은 비용으로 임의 시퀀스를 생성할 수 있다.

본 논문에서는 이후 의사 난수 생성기(PRNG)로 직접 생성한 임의 시퀀스를 원본 시퀀스(Original Sequence)라 표기하며, 원본 시퀀스에 순열을 적용하여 생성되는 임의 시퀀스를 확장 시퀀스(Extended Sequence)라 표기한다.

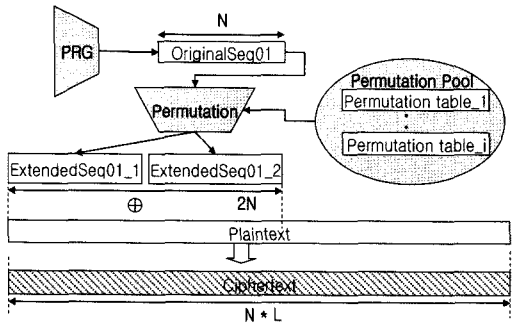


그림 1 제안 기법 개요

2.2 제안기법 구조

본 절에서는 제안 기법의 자세한 구조를 복호화를 예로 들어 설명한다. 멀티미디어 데이타(이하 컨텐츠 객체)는 서버에서 암호화되어 전달되며 권리를 구입한 클라이언트에 해당 컨텐츠의 권리를 명세한 파일(이하 권리 객체)을 전달한다. 권리 객체에는 암호화된 컨텐츠 객체를 복호화 하기 위한 키가 포함되어 있다. 제안 기법으로 암호화 된 데이타를 복호화 하기 위해서는 랜덤 키(PRNG Key)와 순열 키(Permutation Key) 두 개가 필요하다. 랜덤 키는 임의 시퀀스를 생성하기 위해 사용하고 순열 키는 순열을 생성하기 위해 사용된다.

그림 2에 제안 기법의 데이타 복호화 과정을 나타내었다. 제안 기법으로 암호화한 컨텐츠 객체를 복호화하기 위해서는 다음 8단계의 과정을 필요로 한다.

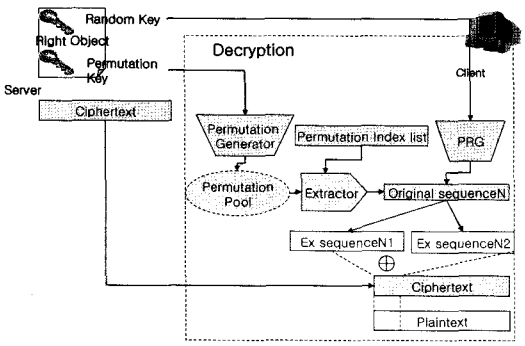


그림 2 제안 기법의 데이타 복호화

Step 1: RK, PK ← CO

권리 객체 CO에서 랜덤 키 RK와 순열 키 PK추출.

Step 2: P_{PK} ← PG(PK)

PK와 순열 생성기 PG를 사용하여 순열 풀 PPK 를 구성. 만약 평문을 복호화 하는데 L개의 확장 시퀀스를 필요로 한다면 순열 풀의 크기 i는 $\left(\frac{i}{2}\right) \geq \frac{L}{2}$를 만족하여야 한다. 이 제약은 보안과 관련된 제약으로 3장 보안성 평가에서 설명한다.

Step 3: On ← PRNG(RK), (1 ≤ n ≤ L/2)

RK를 사용하여 의사 난수 생성기에서 길이 256 바이트의 원본 시퀀스 On (1 ≤ n ≤ L/2)을 하나 생성.

Step 4: P_{n1}, P_{n2} ← P_{PK}(PI)

P_{PK}에서 순열 색인 PI를 이용하여 두 개의 순열 P_{n1}, P_{n2}를 추출. PI에는 추출할 순열의 색인이 추출할 순서대로 명시되어 있으며 PI의 원소, 즉 순열의 색인은 0에서 i-1까지의 범위 값을 가져 모든 순열을 지시할 수 있다. PI는 한번 추출한 순열 쌍을 재사용하지 않도록 구성되어 있다. 제안 기법은 색인과 연관된 순열의 값이 공개되지 않는다. 따라서 PI의 내용이 공개되어도 공격자가 실제 순열 값을 알 수 없다.

Step5: E_{n1}, E_{n2} ← P_{n1}(On), P_{n2}(On)

On에 순열 P_{n1}, P_{n2}를 적용하여 확장 시퀀스 E_{n1}, E_{n2}을 생성.

Step6: PT_{n1}← CT_{n1} XOR E_{n1},
PT_{n2} ← CT_{n2} XOR E_{n2}

E_{n1}, E_{n2}를 해당 암호문 CT_{n1}, CT_{n2}와 각각 논리합 시켜 평문 PT_{n1}, PT_{n2}를 얻는다.

Step7: if n ≠ L/2 → Goto Step 4
else Goto Step 8

전체 평문을 얻을 때까지 Step 4부터 Step 7을 반복한다.

Step 8: End

암호화 과정도 복호화 과정과 동일한 단계를 거친다. 단지 확장 시퀀스와 논리합되는 데이타가 암호문이 아니라 평문인 점이 차이점이다.

제안 기법에 사용되는 순열 생성기로는 8bit 블럭 암호화 알고리즘 혹은 RC4알고리즘을 이용할 수 있으며 의사 난수 생성기로는 스트림 암호화 알고리즘이나 블럭 암호화 알고리즘의 카운터(CTR)모드를 사용할 수 있다. 본 논문에서는 순열 생성에 RC4의 S 박스 스냅샷 값을 이용하였으며 의사 난수 생성기로는 RC4를 사용하였다.

3. 보안성 평가

본 장에서는 제안 기법의 보안성을 평가한다. 1절과 2절에서 암호문 단독 공격, 알려진/선택 평문 공격에 대한 안전성을 논의하며3절에서는 암호화에 필요한 순열의 개수에 대해 논한다.

3.1 암호문 단독 공격(Ciphertext Only Attack)

암호문 단독 공격 모델에서는 공격자에게 암호문만 주어진다. 공격자는 암호문으로부터 의미 있는 정보인 평문을 유추해 내어야 한다. 암호 알고리즘이 암호문 단

독 공격에 대해 안전 하려면 암호화한 암호문이 임의성(Randomness)을 지녀야 함이 알려져 있다[13]. 그림 3은 제안 기법이 임의성을 유지하는지 조사하기 위해 RC4로 암호화한 MP3파일과 제안 기법으로 암호화한 MP3파일을 256바이트 길이로 분할한 시퀀스 5000, 10000개에 대해 AES선별에 사용한 NIST Statistical Test Suite[9]의 임의성 통계 테스트 중 적용 가능한 4개 항목을 적용한 결과이다. 그림 3의 X축은 적용한 테스트의 번호이고 표 1에 그 내용을 명시하였다. Y축은 테스트를 통과한 시퀀스의 비율이다.

테스트 값이 confidence interval 사이에 있으면 해당 의사 난수 생성기로 생성된 시퀀스는 랜덤하다고 볼 수 있다[9,10]. 그림 3의 그래프에서 검은 선이 confidence interval의 하한 값이다. 그림 3의 그래프를 살펴보면 RC4로 암호화한 암호문과 제안 기법으로 암호화한 암호문 모두 임의성을 가진다고 할 수 있다. 제안 기법으로 암호화한 암호문이 임의성을 가진다고 할 수 있으므로 제안 기법은 암호문 단독 공격에 대해 안전하다.

표 1 NIST 임의성 통계 테스트

번호	테스트	테스트 내용
1	빈도	시퀀스 내에 1과 0이 균등하게 분포하는가?
2_1	누적합	0 혹은 1이 시퀀스 초반에 몰려 있는가?
2_2	누적합	0 혹은 1이 시퀀스 후반에 몰려 있는가?
3	런	런(run)의 개수가 적절한가?
4_1 4_2	연속성	8bit 길이의 단어가 균일하게 분포하는가?

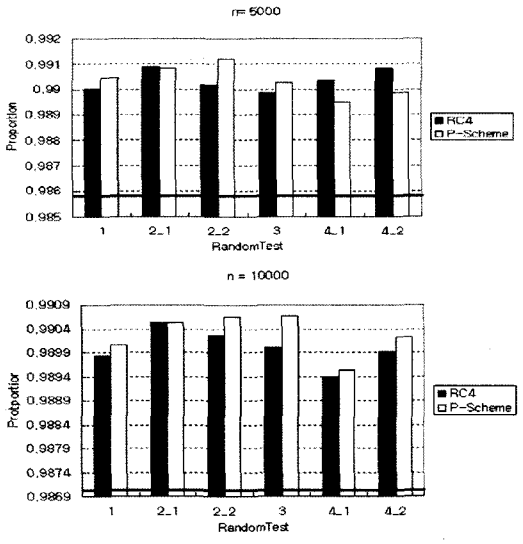


그림 3 RC4와 제안기법을 적용한 암호문의 NIST 통계 테스트 결과

3.2 알려진/선택 평문공격(Known/Chosen Plaintext Attack)

공격자가 여러 개의 주어진 평문과 이에 해당하는 암호문을 사용하여 알려지지 않은 평문을 유추하는 모델이 알려진 평문 공격(known plaintext attack) 모델이다. 공격자의 권한을 더욱 강화하여 공격자가 평문과 이에 해당하는 암호문을 임의로 선택 할 수 있는 권한을 가지는 모델이 선택 평문 공격(Chosen plaintext attack) 모델이다. 어떤 기법이 알려진/선택 평문 공격에 안전하기 위해서는 공격자가 주어진 평문과 암호문 쌍으로부터 새로운 평문 혹은 키를 알아낼 수 없어야 한다[13].

알려진/선택 평문 공격모델에서 공격자는 주어진 평문과 암호문 쌍을 논리 합하여 제안 기법의 확장 시퀀스를 획득 할 수 있다. 공격자가 새로운 확장 시퀀스를 알아 낼 수 있으면 암호문에 논리합을 적용하여 새로운 평문을 알아낼 수 있다. 따라서 제안 기법이 알려진/선택 평문 공격에 안전하려면 공격자가 알고 있는 암호문과 평문 쌍에서

1. 다른 확장 시퀀스를 유추 할 수 없고
2. 랜덤 키, 순열 키를 유추 할 수 없어야 한다.

공격자가 제안 기법의 알려진 확장 시퀀스에서 새로운 확장 시퀀스를 유추할 수 없도록 하기 위해서는 원본 시퀀스 On으로부터 확장 시퀀스를 생성하기 위해 사용한 순열의 집합 S(On)이

$$\forall i \forall j (|S(O_i) \cap S(O_j)| \leq 1), 0 \leq i,j \leq N, i \neq j \quad (1)$$

을 만족해야 한다. 공격자에게는 여러 개의 주어진 평문과 그에 대한 암호문이 있으므로 이를 사용하여 확장 시퀀스를 생성할 수 있다. 그림 4에 공격자가 알고 있는 확장 시퀀스와 알아낼 확장 시퀀스에 대해 나타내었다. 진한 색의 확장 시퀀스가 공격자가 알고 있는 확장 시퀀스. 흰색의 확장 시퀀스가 공격자가 알아내어야 할 확장 시퀀스이다.

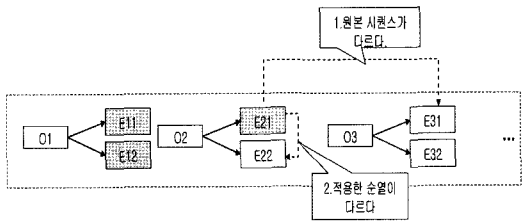


그림 4 공격자가 알고 있는 확장 시퀀스와 알아내어야 할 확장 시퀀스

3.2.1 다른 확장 시퀀스 유추

공격자가 알아내어야 할 확장 시퀀스는 공격자가 이미 알고 있는 확장 시퀀스를 기준으로 하여

1. 같은 원본 시퀀스에 다른 순열을 적용하여 생성된 확장 시퀀스
2. 다른 원본 시퀀스에서 생성된 확장 시퀀스 중 하나로 분류할 수 있다.

그림 4에서 공격자가 알고 있는 확장 시퀀스 E21을 기준으로 할 경우 1은 E22, 2는 E31과 E32에 해당한다.

Case 1: E22를 유추. E22는 O2에 E21과는 다른 순열을 적용하여 생성된 확장 시퀀스이다. 즉 E21과 E22는 O2의 원소의 순서를 다른 방식으로 변경한 것에 지나지 않으므로 E21의 원소 위치를 정확히 변경하면 E22를 구할 수 있다. 하지만 O2, E21은 임의성을 가지며 O2에서 확장 시퀀스를 구하기 위한 순열은 공격자에게 알려지지 않으므로 E22를 구하려면 E21에 가능한 모든 순열을 적용해야 한다. 시퀀스의 원소 개수가 256개이므로 256개의 원소를 재배열하는 순열의 개수는 256!이 되는데 이는 매우 큰 수 이므로 공격자가 E21로부터 E22를 알아내기는 어렵다.

Case 2: E31을 유추. E31은 E21과 원본 시퀀스가 다르므로 비록 확장 시퀀스를 생성하기 위해 적용한 순열이 같다 하더라도 시퀀스의 원소 값이 달라 전혀 다른 값의 확장 시퀀스가 생성된다. 원본 시퀀스는 의사난수 생성기에서 생성된 시퀀스이므로 제안 기법이 알려진/선택 평문 공격에 안전한 의사 난수 생성기를 사용했다면 E31을 유추하기 어렵다.

Case 3: 예외. 그림 5와 같이 공격자가 하나의 원본 시퀀스 O1에서 생성된 확장 시퀀스 E11, E12를 알고 있으며 또한 이와 다른 원본 시퀀스 O2에서 생성된 확장 시퀀스 E21을 알고 있을 경우를 생각해 보자. 공격자는 E11과 E12를 비교하여 E11을 E12로 변환하는 순열 Pa를 알아 낼 수 있다. E11과 E12는 O1으로부터 각각 순열 $P1$과 $P2$를 사용하여 생성되었으므로 순열 Pa는 $P2 \circ P1^{-1}$와 같다. 그런데 같은 순열 $P1$, $P2$를 사용하여 O2로부터 확장 시퀀스 E21과 E22를 생성했다면 E21에서 E22로 변환하는 순열 또한 $P2 \circ P1^{-1}$가 되어 공격자가 이미 알고 있는 순열 Pa와 같다. 공격자는 E21에 순열 Pa를 적용하여 간단히 E22를 알아낼 수 있다.

이를 방지하기 위해서는 하나의 원본 시퀀스에서 확장 시퀀스를 생성하기 위해 사용한 순열 쌍이 재사용되면 안 되며 이를 식 (1)로 공식화 할 수 있다.

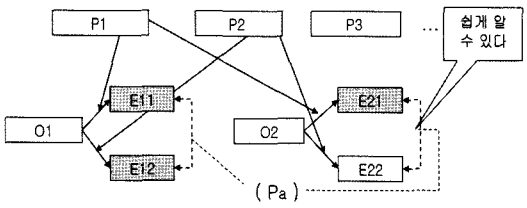


그림 5 알려진/선택 평문 공격에 대한 취약 상황

3.2.1 랜덤 키와 순열 키 유추

알려진/선택 평문 공격으로 제안 기법의 랜덤 키와 순열 키를 알아내기 위해 공격자는 원본 시퀀스와 순열을 알아야 한다. 그러나 알려진/선택 평문 공격 환경에서 제안 기법의 확장 시퀀스는 알 수 있지만 원본 시퀀스와 순열은 알 수 없다. 확장 시퀀스는 임의 시퀀스인 원본 시퀀스에 순열을 적용하여 생성되었기 때문에 공격자가 확장 시퀀스로부터 원본 시퀀스 값을 알아내기 어렵다[14]. 만약 알아내었다 해도 랜덤 키를 알아내기 위해서는 의사 난수 생성기로 사용한 알고리즘의 알려진/선택 평문 공격에 의한 키 추출 복잡도를 따르게 된다. 따라서 알려진/선택 평문 공격에 안전한 의사 난수 생성기를 사용한다면 제안 기법의 랜덤 키를 알려진/선택 평문 공격으로 알아내기 어렵다. 같은 이유로 순열 키를 알아내기도 어렵다.

3.3 순열 풀의 크기

제안 기법에서 식 (1)을 만족하면서 전체 순열 개수 i를 최소화 시키려면 순열 i개중 순열 2개를 선택하여 사용한 다음 한 번 사용한 순열 쌍의 조합은 더 이상 사용하지 않아야 한다. 평문의 암호화에 L개의 확장 시퀀스가 필요하다면 제안 기법은 L개의 확장 시퀀스를 생성하기 위해 L/2개의 순열 쌍을 필요로 한다. 따라서 암호화에 L개의 확장 시퀀스를 필요로 하는 평문을 안전하게 암호화하기 위해서 i는

$$\left(\frac{i}{2}\right) \geq \frac{L}{2} \tag{2}$$

를 만족하여야 한다.

4. 성능 평가

4.1 복호화 시간 및 메모리 사용량

제안 기법의 성능을 측정하기 위해 애플 사의 아이팟 나노(ipod nano)를 사용하여 복호화 속도를 측정하였다. 아이팟 나노의 운영체제로는 리눅스 2.4 커널을 사용하였으며 표 2에 아이팟 나노의 상세한 명세를 나타내었다. 그림 6은 아이팟 나노에서 1, 2, 3, 4, 5 메가 바이트의 MP3파일을 각각 RC4로 암호화 한 파일, 제안 기법으로 암호화 한 파일을 복호화 하였을 경우의 소요 시간을 측정한 것이다. 계산 시간만 측정하였으며 파일

표 2 ipod 나노 명세

항목	명세
OS	Linux 2.4
CPU	ARM7TDMI
RAM	30,380KB
Flash Memory	4GB

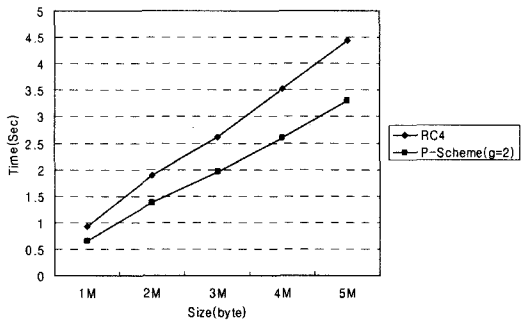


그림 6 ipod nano에서의 복호화 시간

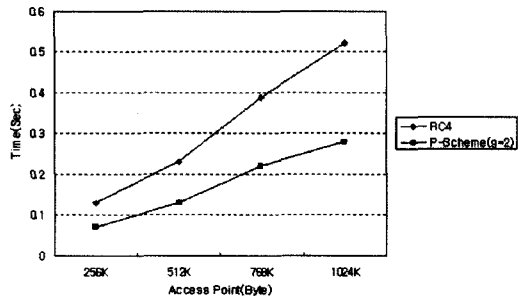


그림 7 블럭 내 데이타의 임의 접근 속도

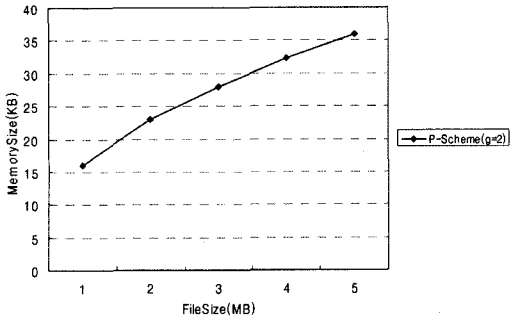
입출력에 소요된 시간은 측정하지 않았다. 그림 6을 보면 제안 기법은 의사 난수 생성기로 RC4를 사용하였을 경우, 일반 RC4를 사용해 복호화하는 것에 비해 약 27%의 속도가 개선되었다.

그림 7에서는 1메가 바이트 크기의 암호화된 블럭 내 데이타의 임의 접근 소요시간을 그래프로 나타내었다. 그래프의 X축은 블럭 내에서 접근해야 할 위치, Y축은 해당 위치에 접근하는데 까지 소요된 시간을 나타내었다.

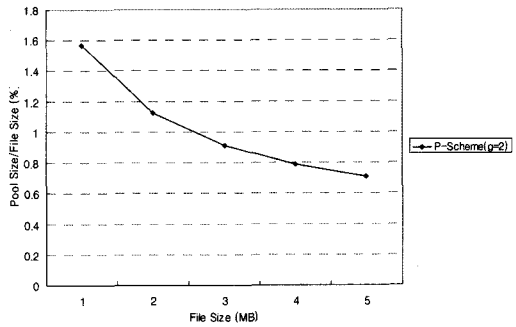
스트림 암호화 기법은 키 스트림 1바이트를 생성할 때마다 내부 상태가 갱신된다. 따라서 암호화 파일의 시작점으로부터 a바이트 위치의 데이타를 복호화 할 경우 (a-1)바이트의 키 스트림을 생성하여 내부 상태를 a바이트 위치의 데이타를 복호화 할 수 있도록 갱신하여야 한다. 하지만 임의 접근의 특성상 접근하는 위치 보다 앞의 데이타는 복호화 하지 않아도 되므로 복호화 할 위치에 접근할 때까지는 키 스트림은 생성하지만 암호 문과의 논리합 연산은 수행하지 않아도 된다. 이 때문에 접근 위치까지 복호화하는데 소요되는 시간보다 접근 위치까지 접근에 소요되는 시간이 작다.

제안 기법은 의사 난수 생성기를 사용한 임의 시퀀스 생성이 RC4의 절반에 지나지 않으므로 임의 접근속도에서는 RC4에 비해 약 50%의 속도 향상을 보인다.

제안 기법은 순열 풀을 암/복호화 동안 유지하여야



(a)



(b)

그림 8 제안 기법 암/복호화 메모리 추가 사용량

한다. 따라서 순열 풀의 크기가 곧 추가 메모리 사용량이 된다. 하나의 확장 시퀀스의 크기는 256바이트이므로 순열 하나의 크기도 또한 256바이트이다. 이 경우 1메가 바이트를 암호화 하기 위해 약 4096개의 확장 시퀀스를 필요로 한다. 순열의 개수 i는 $\left(\frac{i}{2}\right) \geq \frac{L}{2}$을 만족하여야 하므로 1메가 바이트를 암호화 하기 위한 최소한의 순열은 64개가 되어 16킬로 바이트의 메모리 공간이 필요하다. 그림 8의 (a)에 1메가 바이트에서 5메가 바이트까지 복호화에 필요한 최소한의 순열 풀의 크기를 나타내었으며 (b)에 전체 파일 크기에 대한 순열 풀의 크기의 비율을 %로 나타내었다. 일반적인 크기인 5메가 바이트의 MP3파일을 암호화 하는데 제안 기법은 약 36킬로 바이트의 메모리 공간을 필요로 한다. 하지만 일반적인 모바일 휴대 기기의 메모리 용량(아이팟 나노는 약 28메가 바이트)에 비해 그리 큰 크기가 아니므로 무시할 수 있으며 필요한 경우 파일을 좀 더 작은 순열 풀 적용 단위로 분할하여 각 단위마다 순열 풀을 생성하면 복호화할 때 필요로 하는 최소 메모리 크기를 줄일 수 있다.

4.2 에너지 소비

본 절에서는 제안 기법의 에너지 소비를 측정하기 위

해 무트레쟈(Anish Muttreja)의 fsim 시뮬레이터를 사용하였다. Fsim은 명령어 단계(Instruction Level Based) 기반 시뮬레이션과 복합 시뮬레이션(Hybrid)을 제공하는 시뮬레이터이다[11,12].

그림 9에 fsim의 명령어 단계 전력 모델 시뮬레이션을 적용하여 측정한 제안 기법의 에너지 소모를 나타내었다. 시뮬레이션에서 에너지의 단위는 줄(J)이며 에너지 측정에서 파일 입출력은 제외하였다. 시뮬레이션 결과에 따르면 5 메가 바이트의 파일을 복호화 할 경우 RC4는 약 27.68줄의 에너지가 소비되고 제안 기법은 19.25줄의 에너지가 소비된다. 이는 RC4로 암호화 하는 것과 비교해서 제안 기법이 약 30%의 에너지를 절약할 수 있음을 보이고 있다.

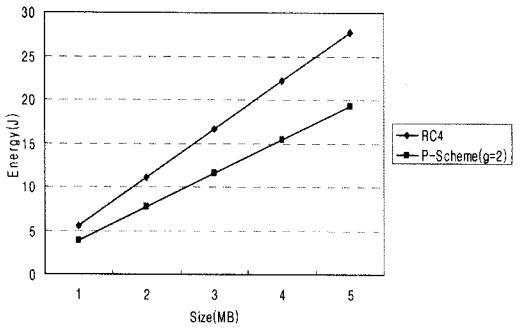


그림 9 fsim을 사용하여 시뮬레이트한 RC4와 제안 기법의 에너지 소모

5. 결 론

본 논문은 기존의 스트림 암호화 기법에 비해 빠른 응답속도와 낮은 에너지 소모율을 가지며 임의 접근에 효율적인 스트림 암호화 기법을 제안하였다. 제안 기법은 평문을 암호화 하는데 필요한 키 스트림의 절반 길이의 원본 시퀀스를 의사 난수 생성기를 사용하여 생성한 다음 동적 생성된 순열을 적용하여 필요 길이의 확장 시퀀스를 생성한다. 제안 기법이 의사 난수 생성기의 사용을 줄임으로써 결과적으로 키 스트림 생성에 드는 비용이 줄어 일반 스트림 암호화 기법보다 빠르고 에너지를 적게 소모함을 보였다. 의사 난수 생성기로 RC4를 사용했을 경우 제안 기법은 일반 RC4에 비해 약 27%의 응답속도 단축과 약 30%의 에너지 소모 감소율을 보인다. 또한 멀티미디어 데이타 임의 접근시 의사 난수 생성기를 사용하여 생성해야 할 키 스트림이 기존 스트림 암호화 기법의 절반에 지나지 않아 임의 접근 속도가 향상되었다. 본 논문은 제안 기법이 순열과 의사 난수 생성기를 결합하여 사용함으로써 암호화 단독 공격 및 알려진/선택 평문 공격에 안전함을 보였다. 제안 기법은 멀티미디어 데이타 압축 독립적인 암호화 알고리즘으로써 특정 멀티미디어 데이타 압축 알고리즘에 의존하지 않는다. 따라서 멀티미디어 파일 종류와 관계없이 적용할 수 있어 선택적 암호화 기법에 비해 활용 범위가 넓으며 표준 모바일 디지털 저작권 관리 구조에 쉽게 포함시킬 수 있다.

다만 현재의 일반적인 모바일 기기의 메모리 용량이나 암호화하는 파일 크기에 비하면 작은 값이기는 하나 안전성을 획득하기 위해 비교적 많은 메모리 공간을 필요(5메가 바이트 암호화에 36킬로 바이트 필요)로 한다. 보안성과 성능을 유지하면서 필요 메모리 요구량을 감소시키는 것이 차후의 연구 과제이다.

참 고 문 헌

[1] http://www.poenmobilealliance.org. Open Mobile Alliance.

[2] D. S. Ravi, A. R. Raghunathan, P. Kocher, and S. Hattangady, "Security in embedded systems: Design challenges," in ACM Trans. On Embedded Computing Systems, 3(3), 2004, pp. 461-491.

[3] B.Macq and J.j.Quisquater, "Cryptology for digital tv broadcasting," in IEEE, Vol.83, No.6, 1995, pp. 944-957.

[4] C. P. Wu and J. Kuo, "Design of integrated multimedia compression and encryption systems," in IEEE Transactions on Multimedia, Vol.7, No.5, 2005.

[5] W. Zeng and S. Lei, "Efficient frequency domain selective scrambling of digital video," in IEEE Transactions on Multimedia, Vol.5, 2003.

[6] R. Wash, "Lecture Notes on Stream Ciphers and RC4," 2001. http://www-personal.si.umich.edu/~rwash/pubs/.

[7] P. Prasithsangaree and P. Krishnamurthy, "Analysis of energy consumption of RC4 and aes algorithms in wireless lans," in OLOBECOM 2003, 2003, pp. 1445-1448.

[8] E.T.Lin, A.M.Eskicioglu, R.L.Lagendijk, and E.J.Delp, "Advances in digital video content protection," in IEEE vol.93 no.1, 2005.

[9] http://csrc.nist.gov/rng, "NIST Random Number Generation and Testing"

[10] J. Soto, "Statistical Testing of Random Number Generators," NIST 2000.

[11] A. Muttreja, A. Raghunathan, S. Ravi, and N. K.Jha, "Automated energy/performance macro-modeling of embedded software," in the 41st Design Automation Conference(DAC04), 2004.

[12] A. Muttreja, A. Raghunathan, S. Ravi, and N. K.Jha, "Hybrid simulation for embedded software energy estimation," in the 42th Design Automation Conference (DAC05), 2005.

[13] W.Stallings, "Cryptography and Network Security: principles and practices," 3rd edition Pearson Education Inc.
[14] D. Xie and C. J. Kuo, "Multimedia data encryption via random rotation in partitioned bit streams," 2005.

한 정 규
2005년 서울대학교 학사. 2007년 서울대학교 석사. 2007년~, NTT 정보유통플랫폼연구소 연구원. 관심분야는 운영체제, 분산 컴퓨팅, 컴퓨터 보안 등

조 유 근
1971년 서울대학교 건축공학 학사. 1978년 미네소타 대학 전산학 박사. 1985년~1992년 미네소타 대학 전산학과 방문교수. 1993년~1995년 서울 대학교 중앙교육연구전산원 원장. 1995년~1996년 한국 정보 과학회 부회장. 1999년~2001년 서울대학교 공과대학 교무담당 부학장. 2001년~2002년 한국정보과학회 회장. 1979년~ , 서울대학교 교수. 2003년~ , 한국 공학 한림원 회원. 관심분야는 운영체제, 알고리즘 설계와 분석. 컴퓨터 보안 등