情報保護學會論文誌
第18卷 第5號, 2008. 10

효율적인 Batch 처리를 위한 그룹키 관리 기술

김 대 엽†, 허 미 숙, 주 학 수
삼성전자

Group Key Management Scheme for Batch Operation

DaeYoub Kim†, MiSuk Huh, HakSoo Ju
Samsung Electronics

요 약

인터넷을 이용한 콘텐츠 서비스의 증가는 일반 시청자가 언제, 어디서나 서비스를 즐길 수 있는 유비쿼터스 TV(u-TV)로 발전하고 있다. 그러나 이러한 발전에 비례하여 콘텐츠 불법 복제 및 배포 또한 꾸준히 증가하고 있다. 콘텐츠 서비스의 안전성을 보장하기 위하여 다양한 방법의 기술이 개발/적용되고 있으며, 콘텐츠 암호키의 효과적인 관리에 필요한 기술도 그 중 하나이다. 본 논문에서는 사용자 그룹을 대상으로 암호키를 관리하는 그룹키 관리 기법의 개선된 모델을 제시한다. 제안하는 기법은 묶음처리(Batch)를 통한 암호키 변경 시 전송량을 최소화하도록 설계 되었다.

ABSTRACT

Digital Contents Services based on Internet are developing into an ubiquitous television that allows subscribers to be able to enjoy digital contents anytime and anywhere. However, illegal copies and distributions of digital contents are also increasing proportionally. To guarantee the stability of contents service, many technologies are being developed and installed. The efficient scheme to manage content encryption keys is one of them. In this paper, we propose an improved key management scheme to manage the members of groups. The proposed scheme has a minimized transmission overhead for batch operation to renew content encryption keys.

Keywords : Multicast Security, Hash-Chain

Ⅰ. 서 론

IPTV, DMB와 같은 다양한 디지털 콘텐츠 서비스의 보급이 증가함에 따라 콘텐츠의 불법 복제 및 배포 또한 증가하고 있다. 이와 같은 불법 콘텐츠 이용 방지를 위해 서비스 사업자(Service Provider, SP)는 콘텐츠를 암호화한 후 가입자들에게 공급한다. 이 때 사용되는 암호키를 콘텐츠 암호키(Content Encryption Key, CEK)라 부른다. 기존의 VoD(Video on Demand)와 같은 주문형 서비스는 해당 가입자의 공개키로 CEK를 암호화한 후 암호화된 콘텐츠와 함께 전송해 주는 모델이 일반적으로 사용되었다. 그러나 멀티 캐스트 또는 브로드 캐스트 콘텐츠 서비스는 다수의 가입자들이 동일한 시각에 같은 콘텐츠를 제공 받고, 서비스 모델에 따라 SP가 가입자의 콘텐츠 수신 및 이용 여부를 실시간으로 알 수 없기 때문에 주문형 서비스에서 사용되는 CEK 관리 모델을 방송 서비스에 적용할 경우, 동일한 서비스를 신청한 n명의 사용자를 위하여, n개의 암호화된 CEK를 전송해야 한다. 이러한 모델은 CEK 관리에 필요한 데이터의

접수일 : 2008년 3월 28일; 수정일 : 2008년 5월 22일;
채택일 : 2008년 7월 2일
† 주저자, daeyoub69@paran.com

전송량 증가 및 이에 따른 서비스 지연과 같은 문제를 발생시킬 수 있다. 그러므로 동일한 서비스를 신청한 사용자들을 묶어서 하나의 암호키(이하, 그룹키)를 할당하고, 할당된 그룹키로 CEK를 암호화 하는 방안이 제안되어왔다.

그룹키 관리 모델은 크게 두 가지 모델로 접근되어져 왔다. 첫 번째 모델은 전체 서비스 가입자 수를 예상하고, 이를 지원하기 위해 필요한 모든 그룹키를 미리 생성한 후, 가입자가 새로 가입하면 생성해 놓은 그룹키 중 적당한 집합을 할당하는 모델로, 실제 그룹키 관리는 구성원들의 변동 사항 중 탈퇴(Revoked)만을 고려하는 브로드 캐스트 암호키 관리 기법(Broadcast Encryption Scheme, BES)이다[1-3]. BES는 구성원의 탈퇴를 처리하기 위하여 CEK를 전송할 때 전체 그룹키 중에서 탈퇴한 구성원들에게 할당한 그룹키들을 제외한 나머지 그룹키들 만으로 CEK를 암호화 한다. 그러므로 그룹키 갱신과 같은 복잡한 절차가 필요 없다. 그러나 일반적으로 전송량이 탈퇴한 구성원의 수에 비례하여 증가한다는 단점이 있다. 현재 BES는 DVD와 같은 미디어를 이용한 콘텐츠 서비스에 주로 이용되고 있다[4]. 두 번째 모델은 구성원의 가입과 탈퇴를 고려하여 그룹키를 갱신하는 그룹키 관리 기술(Group Key Management Scheme, GKMS)이다[5-7]. 구성원의 변동이 발생하면 해당 구성원에게 할당한 그룹키를 갱신하여 그룹의 잔류 구성원들에게 전송한다. 그룹키를 갱신하기 때문에 키 관리에 필요한 데이터 전송량을 일정 수준에서 초기화 시킬 수 있다. 그러므로 구성원의 변동이 빈번히 발생하는 서비스 모델에 적합하다.

2005년 Jen-Chiun Lin은 단방향 키 유도 기법(One-way Key Derivation, OKD)을 이용하여 그룹키 갱신에 필요한 데이터 전송량을 줄이는 새로운 GKMS 기법을 제안했다[8]. OKD는 일부 구성원들이 그룹키 갱신/유도 과정에 직접 참여함으로써 갱신된 그룹키 전송량을 줄이는 새로운 방법을 사용했다. 실제 서비스 운영 시, 시스템 운영의 효율성을 확보하기 위하여 일반적으로 가입자 변경 발생 시 마다 그룹키 갱신을 처리하지 않고 정책에 따라 주기적으로 다수의 변경을 묶음 처리(Multiple/Batch Operation)를 한다. 그러므로 묶음처리를 위한 전송량 감소는 서비스 운영을 고려할 때 중요한 요소가 된다. 이와 같은 묶음처리를 수행할 때, OKD는 구성원들이 그룹키 유도에 참여할 수 없는 경우가 증가하여 전송량이 소폭 증가하는 단점이 있다.

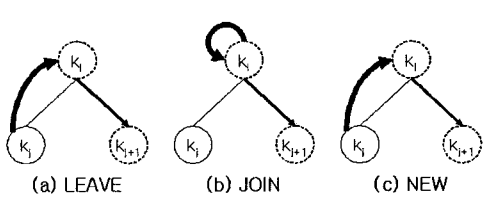
본 논문에서는 이와 같은 단점을 보완하여 묶음 처리 시에도 OKD의 전송량을 최적화 시킬 수 있는 개선된 기법을 제안한다. 본 논문에서 제안하는 기법은 이진트리(Binary Tree)를 사용하기 때문에 Jen-Chiun의 기법 또한 이진트리 기반으로 간략하게 설명하고 전송량을 분석했다.

Ⅱ. 그룹키 관리 기법

2.1 GKM with One-Way Key Derivation(OKD)

Jen-Chiun Lin의 OKD도 일반적인 GKMS처럼 구성원의 가입과 탈퇴를 처리하기 위하여 계층화된 트리 구조의 그룹키를 사용한다. 이 절에서는 앞서 언급한 것처럼 계층화된 이진트리 기반의 OKD를 간략하게 설명한다. 이진트리의 각 내부 노드에는 서로 다른 그룹키가 하나씩 할당되며, i번째 노드 n_i에 할당된 그룹키를 k_i로 표시한다. SP는 가입을 신청한 구성원에게 이진트리의 최하위 노드(Leaf Node) 중에 다른 구성원에게 할당되지 않은 노드를 할당 하고, 할당된 최하위 노드부터 최상위 노드(Root Node)에 이르는 경로(Path) 위의 노드들에 할당된 그룹키들을 해당 구성원에게 제공한다. 단, 최하위 노드의 그룹키는 해당 노드를 할당 받은 구성원과 SP 사이에 별도로 공유된 난수 비밀키 값을 사용한다고 가정한다. 가입(또는 탈퇴)한 구성원의 최하위 노드를 포함하는 경로를 가입경로(또는 탈퇴경로)라 하자. 구성원 변동이 발생하면 가입경로(또는 탈퇴경로) 위에 있는 모든 노드들의 그룹키들이 갱신된다. OKD 기법은 그룹키 갱신을 위해 가입경로(또는 탈퇴경로) 위에 있는 노드들의 상태를 다음과 같이 정의했다 : (a) LEAVE : 해당 노드가 탈퇴경로 위에 있는 경우. (b) JOIN : 해당 노드가 가입경로 위에 있는 경우. 단, 해당 노드는 LEAVE 상태가 아니다. (c) NEW : 해당 노드가 JOIN 상태이고 자식 노드(Child Node)가 새롭게 생성된 경우.

[그림 1]은 앞서 정의한 노드 상태에 따른 OKD의 그



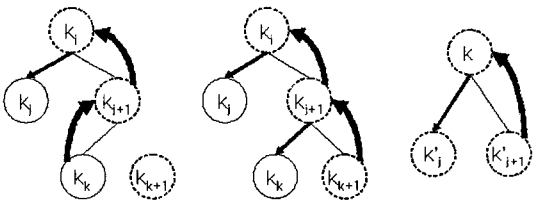
[그림 1] OKD 그룹키 갱신/유도 방법

룹키 갱신/유도 방법을 설명 한다. [그림 1]의 두 자녀 노드들 중에서, 노드 n_{j+1}만 가입경로(또는 탈퇴경로) 위에 있다고 가정하자. f 를 안전한 단방향 함수라 할 때, 노드 n_i의 상태에 따른 갱신된 그룹키 k_i'는 각각 다음과 같다 : (a) $f(k_j \oplus k_i)$, (b) $f(k_i)$, (c) $f(k_j \oplus k_g)$, 단, k_i는 노드 n_i의 갱신 전 그룹키이고, k_g는 새로 가입한 구성원이 모르는 이전 그룹키이다. 노드 n_j의 구성원들은 k_i'를 직접 계산할 수 있기 때문에, k_i'는 노드 n_{j+1}의 갱신된 그룹키 k_{j+1}'로 암호화 되어 전송된다. 이 경우, k_i' 전송을 위해 필요한 데이터 전송량(TO)은 1이 된다. 그러므로 단수 가입/탈퇴(Single Join/Leave) 처리를 위한 전송량은 가입/탈퇴경로 위에 있는 노드의 수와 같다.

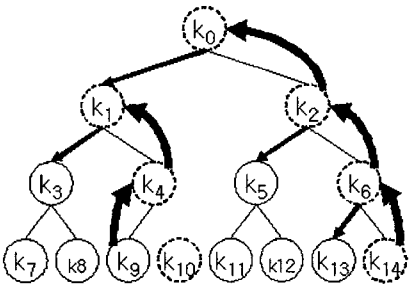
묶음처리 시에는 두 하위 노드의 그룹키가 모두 갱신되는 경우가 발생하게 된다. 예를 들어 노드 n_j와 n_{j+1}이 모두 LEAVE 상태인 경우, k_j와 k_{j+1}이 모두 노출되었기 때문에 갱신된 그룹키 k_i'로 $f(k_j \oplus k_i)$ 와 $f(k_{j+1} \oplus k_i)$을 사용할 수 없다. 이 경우, SP는 k_i'를 생성하여 노드 n_j와 n_{j+1}의 최하위 노드에 대응된 구성원들에게 모두 전송해 주어야 한다. 그러므로 구성원들이 갱신된 그룹키 유도에 참여하여 키 갱신에 필요한 데이터 전송량을 감소시키는 OKD의 장점을 취할 수 없다. 실제로 탈퇴하는 구성원의 수와 가입하는 구성원의 수를 각각 L과 J라 하고, 이진트리의 내부 노드들 중에서 LEAVE, JOIN, NEW 상황에 있는 노드의 수를 각각 S_L, S_J, S_N이라 할 때, 그룹키 갱신을 묶음처리를 통해 수행한다면, 키 갱신을 위해 필요한 전송량은 변경 노드의 개수 ($S_L+S_J+S_N$) 보다 많은 $S_L+S_J+S_N+(max\{L, J\}-1)$이 된다.

2.2 GKM with Hash Chain Key Derivation(HCKD)

이 절에서는 1절에서 설명한 OKD의 묶음 처리 시 발생하는 데이터 전송량 증가 원인을 제거하여 전송량을 최적화시킬 수 있는 개선된 기법을 제안한다. HCKD의 이진트리의 구성과 각각의 노드에 초기 그룹키 할당 방법과 구성원이 저장해야 되는 키의 종류는 1절에서 설명한 OKD의 방법과 동일하다. 제안하는 기법은 단방향 함수 고리(Hach Function Chain)를 사용하여 그룹키를 유도하고, 키 유도의 주체를 OKD와 달리 함으로써 갱신된 그룹키의 전송량을 최소로 유지할 수 있도록 설계되었다. 단방향 함수 고리란 함수 값을 계산하기 위하여 단방향 함수 f를 지정된 수만큼 연속



〔그림 2〕 HCKD 그룹키 유도 방법



〔그림 3〕 HCKD 묶음 처리

적으로 입력 변수 값에 적용시켜서 계산하는 방법을 의미한다. 특히, 갱신 고리 $a \rightarrow b \rightarrow c$의 관계를 $b=f(a)$, $c=f(b)$라고 정의하자.

[그림 2]는 HCKD의 그룹키 유도 방법을 설명한다. (a) 최하위 노드 n_{k+1}의 구성원이 단수 탈퇴한 경우, 탈퇴경로 위에 있는 모든 노드들의 그룹키들이 변경되고, 갱신 고리는 $k_k \rightarrow k_{j+1}' \rightarrow k_i' \rightarrow \cdots \rightarrow k_0'$가 된다. 탈퇴경로의 경우 $k \rightarrow k_r'$이면 $k_r'=f(k \oplus k_r)$와 같이 계산된다. 갱신된 그룹키 $\{k_i', \cdots, k_0'\}$는 각각의 갱신되지 않은 하위 노드의 그룹키로 암호화 되어 전송된다. (b) 최하위 노드 n_{k+1}의 구성원이 새로 단수 가입한 경우, 가입경로 위의 그룹키들이 변경되고, 갱신 고리는 $k_{k+1} \rightarrow k_{j+1}' \rightarrow kk_i' \rightarrow \cdots \rightarrow k_0'$가 된다. 가입경로의 경우, $k \rightarrow k_r'$이면 $k_r'=f(k)$와 같이 계산된다. 갱신된 그룹키 $\{k_{j+1}', k_i', \cdots, k_0'\}$는 각각의 갱신되지 않은 하위 노드의 그룹키로 암호화 되어 전송된다. (c) 묶음 처리 시 노드 n_j의 두 하위 노드의 그룹키가 모두 갱신된 경우, 그룹키 고리는 $k_{j+1}' \rightarrow k_i'$이 된다. 또한, 노드 n_i의 상태는 노드 n_{j+1}의 상태를 따른다. 이 경우, 그룹키는 노드 n_i의 상태에 따라 (a) 또는 (b)에서 제안한 방법을 따라 계산된다. 이렇게 갱신된 k_i'는 갱신된 그룹키 k_j'로 암호화 되어 구성원들에게 전송된다.

[그림 3]은 HCKD의 그룹키 갱신 규칙에 따른 묶음

처리 방법을 설명한다. 최하위 노드 n_{10}와 n_{14}의 구성원들이 탈퇴를 신청하고, 새롭게 가입을 신청한 구성원에게 노드 n_{14}을 다시 할당한다고 가정 하자. 이 같은 경우, 탈퇴경로 처리를 위한 갱신 고리는 $k_9 \rightarrow k_4' \rightarrow k_1'$가 되고, 가입경로 처리를 위한 갱신 고리는 $k_{14} \rightarrow k_6' \rightarrow k_2' \rightarrow k_0'$가 된다. 이렇게 갱신된 그룹키 k_0', k_1', k_2', k_6'는 각각 그룹키 k_1', k_3', k_5', k_{13}'으로 암호화 되어 전송된다.

2.3 HCKD 분석

구성원 수가 2^n명인 경우, 단수 가입 처리를 위한 전송량은 최대 n개이며, 단수 탈퇴 처리의 경우 $n-1$ 개의 메시지 전송이 필요하다. 묶음처리의 경우, 전송량은 $S_L + S_J + S_N$이 된다. [표 1]은 GKMS들의 전송량을 갱신 형태 별로 정리한 것이다. 묶음 처리의 경우, 탈퇴한 구성원에게 할당했던 최하위 노드를 새롭게 가입한 구성원에게 우선 할당하고, 키 유도의 주체는 새롭게 가입한 구성원에게 할당된 최하위 노드가 갖는다. 실제 탈퇴/가입한 구성원들의 최하위 노드들이 균등하게 분포할 때 가장 많은 전송량을 필요로 한다. 이러한 경우, $A = \lfloor \log_2 J \rfloor$ 라 할 때, HCKD의 최대 전송량(TO)은 식(1)이 된다.

$$TO = S_J + S_N + S_L \quad (1)$$
$$= n + \sum_{k=1}^{A} 2^{k-1}(n-k) + (J-2^A)(n-A-1) + (J-L)$$

HCKD의 안전성은 다음과 같다 : HCKD에서 사용하는 단방향 함수 f와 최하위 노드의 그룹키 생성 알고리즘이 충분히 안전하다고 가정하자. [그림 2-(c)]에서 $k_{j+1}' \rightarrow k_i'$와 같은 경우, 탈퇴자가 갱신된 k_i'를 획득하기 위해서는 (i) k_i'를 암호화 할 때 사용하는 k_j'를 확보하거나, (ii) k_i'를 계산할 때 사용한 입력 값 k_{j+1}'를 확보해야 한다. 그러나 (i)의 경우, n_j는 탈퇴경로 위의 노드가 아니므로 탈퇴자는 k_j 뿐만 아니라 n_j의 하위 노드들의 그룹키를 할당 받을 수 없다. 그러므로 탈퇴자는 k_j'를 계산할 수 없다. (ii)의 경우, 갱신 고리를 $k_a \rightarrow \cdots \rightarrow k_{j+1}' \rightarrow k_i'$라 할 때, 해당 노드가 LEAVE 상태이면, 갱신 고리의 초기값은 탈퇴 구성원의 형제 노드의 그룹키 값이다. 그러므로 탈퇴 구성원은 k_a를 할당 받지 못했기 때문에 갱신 고리를 계산할 수 없다. 특히, 그룹키는 $k \rightarrow k_r'$이면 $k_r' = f(k \oplus k_r)$이므로, 동일한 최하위 노드의 탈퇴가 반복되더라도 그룹키는 항상 다르게 갱신된다. 그러므로 과거 탈퇴한 가입자들 역시 새롭게 갱신된 그룹키를 확보할 수 없다. 해당 노드가 JOIN 상태라고 하면, 가입경로 위의 모든 그룹키들은 새로 가입한 구성원에서 유일하게 할당된 난수 키 k_a를 기반으로 모두 갱신되기 때문에, 새로 가입한 구성원이 이전 그룹키 값들을 확보할 수 없을 뿐만 아니라, 탈퇴한 구성원이 새로 가입한 구성원에게 할당된 최하위 노드를 할당 받았었다 하더라도 k_a를 알 수 없기 때문에 갱신된 그룹키들을 계산할 수 없다.

Ⅲ. 결 론

주문형 콘텐츠 서비스로 대표되어 왔던 일대일 방식의 콘텐츠 서비스 방식은 서비스 제공자가 콘텐츠를 주문한 사용자를 직접 인증할 수 있기 때문에 공개키 방식을 이용한 CEK 관리 기술이 주로 사용되어져 왔다. 그러나 그룹 사용자를 대상으로 하는 IPTV, DMB와 같은 다양한 서비스 모델이 속속 보급되고 있기 때문에 기존의 주문형 서비스에서 사용하던 키 관리 기술과는 다른 기술이 요구되고 있다. 이와 같은 요구 사항을 충족시키기 위해 연구되어 온 분야 중 하나가 GKMS다. 특히, 2005년에 발표된 OKD는 일부 구성원들이 직접 갱신된 그룹키를 유도할 수 있도록 함으로써 전송량을 감소시키는 효과를 얻도록 설계 되었다. 그러나 묶음 처

〔표 1〕 전송량 비교

		LKH	OFT	OKD	HCKD
Single	Join	$2n$	$2n$	n	n
	Leave	$2n$	n	$n-1$	$n-1$
Multiple	Join	$2(S_J+S_N)$	$2(S_J+S_N)$	S_J+S_N+J-1	S_J+S_N
	Leave	$2S_N$	S_J+L-1	S_J+L-1	S_L
Batch		$2(S_L+S_J+S_N)+J$	$2(S_J+S_N+S_N+J)+S_L+L-3$	$S_L+S_J+S_N\,(max\{L,J\}-1)$	$S_J+S_N+S_L$

리 시에 어느 구성원도 그룹키를 유도할 수 없는 상태의 노드들이 증가하는 단점을 갖고 있다. 이러한 단점은 전송량 증가의 원인이 된다. 본 논문에서는 그룹키 유도 주체를 OKD와 다르게 설정하고 단방향 함수 고리를 이용함으로써 묶음처리 시에도 그룹의 일부 구성원들이 직접 그룹키를 계속해서 유도할 수 있는 방안을 제안하여 OKD 보다 전송량을 줄일 수 있도록 하였다.

참고문헌

[1] A. Fiat and M. Naor, "Broadcast Encryption", CRYPTO 1993, LNCS 773, pp.480-491. 1993

[2] D. Naor, M. Naor and J. Lotspiech, "Revocation and Tracing Schemes for Stateless Receivers", CRYPTO 2001, LNCS2139, pp. 41-62, 2001.

[3] Nam-Su Jho, Jung Yeon Hwang, Jung Hee Cheon, Myung-Hwan Kim, Dong Hoon Lee, and Eun sun Yoo, "One-Way Chain Based Broadcast Engryption Schemes", EUROCRYPT 2005, LNCS 3494, pp. 559-574, 2005

[4] AACS. Introduction and Common Cryptographic Elements, Revision 0.91, February 17,2006.

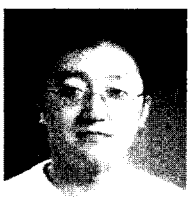
[5] Thomas Hardjono, Lakshminath R. Dondeti, "Ch6. Group Key Management Algorithms", Multicast and Group Security, pp. 129-157, Artech House, 2003.

[6] D.M. Wallner, E.J. Harder, and R.C. Agee, "Key management for multicast issues and architectures", RFC2627, Jun. 1999.

[7] Alan T. Sherman, David A. McGrew, "Key Establishment in Large Dynamic Groups Using One-Way Function Trees", IEEE Trans. on Software Engineering, Vol. 29, No. 5, pp. 444-458, May 2003.

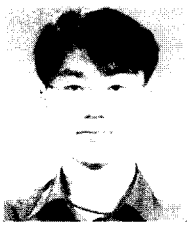
[8] Jen-Chiun Lin, Feipei Lai, and Hung-Chang Lee, "Efficient Group Key Management Protocol with One-Way Key Derivation", Proceedings of the IEEE Conference on Local Computer Networks 30th Anniversary, 2005.

〈著者紹介〉



김 대 엽 (DaeYoub Kim) 종신회원
1996년 8월 : 고려대학교 수학과 석사(대수학 전공)
2000년 2월 : 고려대학교 수학과 박사(대수학 전공)
1997년 8월~2001년 3월 : (주)텔리맨, 위성통신 연구소, CAS팀 선임연구원
2001년 4월~2002년 7월 : 삼성 시큐아이닷컴(주) 정보보호 연구소 PKI실 차장
2002년 9월~현재 : 삼성전자, SAIT, 수석연구원
<관심분야> 네트워크보안, CAS/DRM, PKI, Smart Card, 응용 보안프로토콜

허 미 숙 (MiSuk Huh) 정회원
1990년 2월 : 서울대학교 사범대학 수학교육과 졸업
1992년 2월 : 서울대학교 자연대학 수학과 석사 (정수론 전공)
2001년 2월 : 서울대학교 자연대학 수학과 박사 (정수론 전공)
2001년 12월~현재 : 삼성전자, SAIT, 책임연구원
<관심분야> GKM, 네트워크보안



주 학 수 (Hak-Soo Ju) 정회원
1997년 8월 : 고려대학교 수학과 졸업
1999년 8월 : 고려대학교 수학과 석사(대수학 전공)
2005년 8월 : 고려대학교 수학과 박사(대수학 전공)
2001년 9월~2006년 1월 : 한국정보보호진흥원 연구원
2006년 2월~현재 : 삼성전자, DM연구소, 책임연구원
<관심분야> 암호학, 공개키암호, 응용보안프로토콜, DRM