



(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2013년05월22일
(11) 등록번호 10-1264286
(24) 등록일자 2013년05월08일

(51) 국제특허분류(Int. Cl.)

G06F 21/24 (2006.01) G06F 17/30 (2006.01)

(21) 출원번호 10-2012-0004367

(22) 출원일자 2012년01월13일

심사청구일자 2012년01월13일

(56) 선행기술조사문헌

W02011068996 A1

KR1020090094703 A

KR1020050069955 A

KR1020070110579 A

(73) 특허권자

고려대학교 산학협력단

서울 성북구 안암동5가 1

(72) 발명자

정익래

서울특별시 성동구 성수동1가 709번지 성수2차 대
우아파트 101동 1704호

김동민

서울특별시 동대문구 청량리동 미주아파트 1동
505호

김기성

경기도 군포시 산본동 1063 백합아파트 1126동
1503호

(74) 대리인

특허법인엠에이피에스

전체 청구항 수 : 총 7 항

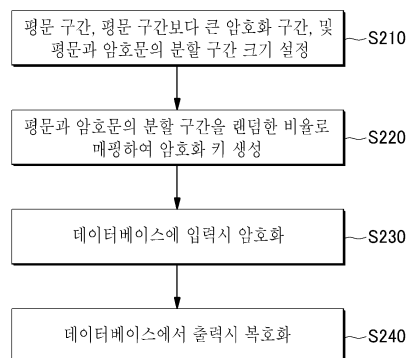
심사관 : 이석형

(54) 발명의 명칭 데이터베이스 암호화 시스템 및 방법

(57) 요약

본 발명은 (a) 평문 구간을 임의의 크기로 확장하여 암호문 구간을 정하고, 상기 평문과 상기 암호문을 동일 크기의 구간들로 분할하는 단계; (b) 상기 각 평문 분할 구간을 순서대로 각각 임의 개의 암호문 분할 구간에 대응(mapping)시켜, 암호화 키를 생성하는 단계; (c) 상기 암호화 키를 사용하여 상기 데이터베이스에 저장할 평문 데이터를 암호화하는 단계; 및 (d) 상기 암호화 키를 사용하여 상기 데이터베이스에서 추출된 암호문 데이터를 상기 암호화 단계의 역변환을 수행하여 복호화하는 단계;를 포함하되, 상기 (a) 단계는 기설정된 안전성 수준에 따라 상기 평문 구간의 크기, 상기 암호문 구간의 크기, 및 상기 분할 구간의 크기를 결정하는 것이며, 상기 (b) 단계에서 상기 암호화 키는 상기 암호문의 분할 지점들 중에서 상기 평문의 분할 구간의 개수보다 하나 적은 수만큼을 임의로 중복되지 않게 선택해서 오름차순으로 정렬한 것이고, 상기 (c) 단계에서 상기 암호화는 상기 평문 데이터가 속하는 평문 분할 구간에 대응되는 암호문 분할 구간 내에서 상기 평문 데이터에 대응되는 값을 찾음으로써 상기 암호문 데이터를 산출하는 것이며, 상기 (d) 단계에서 상기 복호화는 상기 암호문 데이터가 속하는 암호문 분할 구간에 대응되는 평문 분할 구간 내에서 상기 암호문 데이터에 대응되는 값을 찾음으로써 상기 평문 데이터를 산출하는 것인 데이터베이스 암호화 방법을 제공한다.

대표도 - 도2



이 발명을 지원한 국가연구개발사업

과제고유번호	KI002113201103100110013918KI002113201103
부처명	지식경제부
연구사업명	산업원천기술개발사업
연구과제명	Car-헬스케어 보안 기술개발(과제번호:KI002113-2011-03)
주관기관	고려대학교 산학협력단
연구기간	2011.03.01 ~ 2012.02.29

특허청구의 범위

청구항 1

데이터베이스 암호화 방법에 있어서,

- (a) 평문 구간을 임의의 크기로 확장하여 암호문 구간을 정하고, 상기 평문과 상기 암호문을 동일 크기의 구간들로 분할하는 단계;
- (b) 상기 (a) 단계에서 분할된 각 평문 분할 구간을 순서대로 각각 임의 개의 암호문 분할 구간에 대응(mapping)시켜, 암호화 키를 생성하는 단계;
- (c) 상기 암호화 키를 사용하여 상기 데이터베이스에 저장할 평문 데이터를 암호화하는 단계; 및
- (d) 상기 암호화 키를 사용하여 상기 데이터베이스에서 추출된 암호문 데이터를 상기 암호화 단계의 역변환을 수행하여 복호화하는 단계;를 포함하되,

상기 (a) 단계는

기설정된 안전성 수준에 따라 상기 평문 구간의 크기, 상기 암호문 구간의 크기, 및 상기 분할 구간의 크기를 결정하는 것이며,

상기 (b) 단계에서

상기 암호화 키는 상기 암호문의 분할 지점들 중에서 상기 평문의 분할 구간의 개수보다 하나 적은 수 만큼을 임의로 중복되지 않게 선택해서 오름차순으로 정렬한 것이고,

상기 (c) 단계에서

상기 암호화는 상기 평문 데이터가 속하는 평문 분할 구간에 대응되는 암호문 분할 구간 내에서 상기 평문 데이터에 대응되는 값을 찾음으로써 상기 암호문 데이터를 산출하는 것이며,

상기 (d) 단계에서

상기 복호화는 상기 암호문 데이터가 속하는 암호문 분할 구간에 대응되는 평문 분할 구간 내에서 상기 암호문 데이터에 대응되는 값을 찾음으로써 상기 평문 데이터를 산출하는 것인

데이터베이스 암호화 방법.

청구항 2

제 1 항에 있어서,

상기 (c) 단계에서

상기 암호화는 상기 평문 데이터(m)를 상기 암호문 데이터(c)로 변환하는 것이고, 상기 복호화는 상기 암호문 데이터(c)를 상기 평문 데이터(m)로 변환하는 것인바, 상기 평문 데이터(m)가 속하는 평문 분할 구간의 시작값(p_i), 상기 평문 분할 구간에 대응되는 상기 암호문 분할 구간의 시작값(key_i)과 끝값(key_{i+1}), 상기 평문 및 암호문의 분할 구간의 크기(bucketsize)에 기초하여, 각각 하기 수학적식을 사용하여 수행되는 것인 데이터베이스 암호화 방법.

암호화 ($m \rightarrow c$)

$$c = key_i + \frac{(key_{i+1} - key_i)}{bucketsize} \times (m - p_i)$$

복호화 ($c \rightarrow m$)

$$m = p_i + \frac{bucketsize}{key_{i+1} - key_i} \times (c - key_i)$$

청구항 3

제 1 항에 있어서,

상기 암호화 키는 의사 난수(pseudo random number) 생성기를 사용하여 생성되는 것인 데이터베이스 암호화 방법.

청구항 4

제 3 항에 있어서,

상기 (b) 단계는 상기 의사 난수의 시드(seed)만을 저장하며,

상기 (c) 단계와 (d) 단계는 상기 의사 난수 생성기를 사용하여 상기 시드로부터 상기 암호화 키들을 생성하여 사용하는 것인 데이터베이스 암호화 방법.

청구항 5

제 1 항에 있어서,

상기 데이터베이스 암호화 방법은

상기 평균 데이터가 속하는 범위가 상기 평균 구간의 범위를 초과할 경우,

상기 평균 데이터가 속하는 범위를 상기 평균 구간의 크기만큼씩 분할하여 각 평균 구간에 대해 상기 단계들을 수행하는 것인 데이터베이스 암호화 방법.

청구항 6

데이터베이스 암호화 시스템에 있어서,

데이터베이스;

평균 구간을 임의의 크기로 확장하여 암호문 구간을 정하고, 상기 평균과 상기 암호문을 동일 크기의 구간들로 분할한 후, 상기 각 평균 분할 구간을 순서대로 각각 임의의 개의 암호문 분할 구간에 대응(mapping)시켜 암호화 키를 생성하는 키 생성부;

상기 암호화 키를 사용하여 상기 데이터베이스에 저장할 평균 데이터를 암호화하는 암호화부; 및

상기 암호화 키를 사용하여 상기 데이터베이스에서 추출된 암호문 데이터를 상기 암호화 단계의 역변환을 수행하여 복호화하는 복호화부;를 포함하되,

상기 키 생성부는

기설정된 안전성 수준에 따라 상기 평균 구간의 크기, 상기 암호문 구간의 크기, 및 상기 분할 구간의 크기를 결정하는 것이며,

상기 암호화 키는 상기 암호문의 분할 지점들 중에서 상기 평균의 분할 구간의 개수보다 하나 적은 수 만큼을

임의로 중복되지 않게 선택해서 오름차순으로 정렬한 것이고,

상기 암호화부는

상기 평문 데이터가 속하는 평문 분할 구간에 대응되는 암호문 분할 구간 내에서 상기 평문 데이터에 대응되는 값을 찾음으로써 상기 암호문 데이터를 산출하여 상기 평문 데이터를 암호화하는 것이며,

상기 복호화부는

상기 암호문 데이터가 속하는 암호문 분할 구간에 대응되는 평문 분할 구간 내에서 상기 암호문 데이터에 대응되는 값을 찾음으로써 상기 평문 데이터를 산출하여 상기 암호문 데이터를 복호화하는 것인 데이터베이스 암호화 시스템.

청구항 7

제 6 항에 있어서,

상기 암호화는 상기 평문 데이터(m)를 상기 암호문 데이터(c)로 변환하는 것이고, 상기 복호화는 상기 암호문 데이터(c)를 상기 평문 데이터(m)로 변환하는 것인, 상기 평문 데이터(m)가 속하는 평문 분할 구간의 시작값(p_i), 상기 평문 분할 구간에 대응되는 상기 암호문 분할 구간의 시작값(key_i)과 끝값(key_{i+1}), 상기 평문 및 암호문의 분할 구간의 크기(bucketsize)에 기초하여, 각각 하기 수학적식을 사용하여 수행되는 것인 데이터베이스 암호화 시스템.

암호화 ($m \rightarrow c$)

$$c = key_i + \frac{(key_{i+1} - key_i)}{bucketsize} \times (m - p_i)$$

복호화 ($c \rightarrow m$)

$$m = p_i + \frac{bucketsize}{key_{i+1} - key_i} \times (c - key_i)$$

명세서

기술분야

[0001] 본 발명은 데이터베이스 암호화 시스템 및 방법에 관한 것이다.

배경기술

[0002] 데이터베이스 보안의 중요성이 점점 부각되고 있다. 예를 들어 유명 포털 사이트나 게임 서버에서의 사용자 정보 유출 사고와 같은 사건들이 데이터베이스 기밀성 보장이 얼마나 중요한지에 대한 인식을 높였다.

[0003] 데이터베이스에 저장된 데이터의 기밀성을 보장하려면 데이터를 암호화하여 저장해야 하는데, 그럴 경우 데이터베이스 본래의 목적인 데이터 검색의 효율성이 저하된다. 예를 들어, 1부터 10사이의 데이터를 검색하고자 한다면 데이터베이스에 저장된 암호화되어 있는 데이터를 모두 복호화하여 그 중에서 1부터 10사이의 데이터를 검색해야 사용자 질의에 대한 결과를 출력할 수 있다.

[0004] 따라서 데이터를 암호화해 저장하면서도 원래의 순서가 암호화된 데이터에도 반영되도록 하는 순서 유지 암호화 기술이 제안되었다. 순서 유지 암호화 기술을 사용하면 단순히 1에 해당하는 암호화된 데이터와 10에 해당하는 암호화된 데이터 사이의 데이터들만 복호화하여 사용자에게 돌려주면 되기 때문에 효율적이다.

[0005] 그러나 종래에 제안된 순서 유지 암호화 방법들은 저장해야 하는 비밀 정보가 매우 많아 다량의 추가적인 저장

공간이 필요하거나, 데이터의 추가 및 삭제가 자유롭지 못하고, 암호화 및 복호화 과정이 매우 비효율적이라는 등의 문제를 가지고 있어 대용량 데이터베이스에 적용하기에는 부적합한 경우가 많았다.

[0006] 따라서 암호화 및 복호화 연산이 매우 효율적으로 이루어질 뿐만 아니라 높은 안전성을 제공하며, 추가적인 제약 사항이 없어 실제 대용량 데이터베이스에서 사용 가능한 현실적인 순서 유지 암호화 기술이 필요하다.

[0007] 이와 관련하여 한국등록특허 제10-0919824호("데이터 암호화 장치와 이를 이용한 암호화 방법")에는 평문 데이터에 대한 순서 교란 기법과 순서 유지 암호화 기법을 통해 암호화하여 저장하는 구성이 개시되어 있다.

[0008] 또한, 한국등록특허 제10-1045222호("개인 정보를 순서 정보와 내용 정보로 분리하여 암호화하고 합성하는 방법, 장치, 서버 및 기록 매체")는 개인 정보로부터 분리된 순서 정보와 내용 정보를 구분하여 암호화하고 암호화 전과 동일하게 순서 정보를 유지할 수 있도록 각각의 암호화된 정보를 합성하여 저장하는 구성이 개시되어 있다.

발명의 내용

해결하려는 과제

[0009] 본 발명은 전술한 문제를 해결하기 위한 것으로서, 그 목적은 안전성이 높으면서도 효율적인 데이터베이스 암호화 시스템 및 방법을 제공하는 것이다.

과제의 해결 수단

[0010] 상기와 같은 목적을 달성하기 위한 본 발명의 제 1 측면에 따른 데이터베이스 암호화 방법은 (a) 평문 구간을 임의의 크기로 확장하여 암호문 구간을 정하고, 상기 평문과 상기 암호문을 동일 크기의 구간들로 분할하는 단계; (b) 상기 각 평문 분할 구간을 순서대로 각각 임의의 개의 암호문 분할 구간에 대응(mapping)시켜, 암호화 키를 생성하는 단계; (c) 상기 암호화 키를 사용하여 상기 데이터베이스에 저장할 평문 데이터를 암호화하는 단계; 및 (d) 상기 암호화 키를 사용하여 상기 데이터베이스에서 추출된 암호문 데이터를 상기 암호화 단계의 역변환을 수행하여 복호화하는 단계;를 포함하되, 상기 (a) 단계는 기설정된 안전성 수준에 따라 상기 평문 구간의 크기, 상기 암호문 구간의 크기, 및 상기 분할 구간의 크기를 결정하는 것이며, 상기 (b) 단계에서 상기 암호화 키는 상기 암호문의 분할 지점들 중에서 상기 평문의 분할 구간의 개수보다 하나 적은 수 만큼을 임의로 중복되지 않게 선택해서 오름차순으로 정렬한 것이고, 상기 (c) 단계에서 상기 암호화는 상기 평문 데이터가 속하는 평문 분할 구간에 대응되는 암호문 분할 구간 내에서 상기 평문 데이터에 대응되는 값을 찾음으로써 상기 암호문 데이터를 산출하는 것이며, 상기 (d) 단계에서 상기 복호화는 상기 암호문 데이터가 속하는 암호문 분할 구간에 대응되는 평문 분할 구간 내에서 상기 암호문 데이터에 대응되는 값을 찾음으로써 상기 평문 데이터를 산출하는 것을 특징으로 한다.

[0011] 상기와 같은 목적을 달성하기 위한 본 발명의 제 2 측면에 따른 데이터베이스 암호화 시스템은 데이터베이스; 평문 구간을 임의의 크기로 확장하여 암호문 구간을 정하고, 상기 평문과 상기 암호문을 동일 크기의 구간들로 분할한 후, 상기 각 평문 분할 구간을 순서대로 각각 임의의 개의 암호문 분할 구간에 대응(mapping)시켜 암호화 키를 생성하는 키 생성부; 상기 암호화 키를 사용하여 상기 데이터베이스에 저장할 평문 데이터를 암호화하는 암호화부; 및 상기 암호화 키를 사용하여 상기 데이터베이스에서 추출된 암호문 데이터를 상기 암호화 단계의 역변환을 수행하여 복호화하는 복호화부;를 포함하되, 상기 키 생성부는 기설정된 안전성 수준에 따라 상기 평문 구간의 크기, 상기 암호문 구간의 크기, 및 상기 분할 구간의 크기를 결정하는 것이며, 상기 암호화 키는 상기 암호문의 분할 지점들 중에서 상기 평문의 분할 구간의 개수보다 하나 적은 수 만큼을 임의로 중복되지 않게 선택해서 오름차순으로 정렬한 것이고, 상기 암호화부는 상기 평문 데이터가 속하는 평문 분할 구간에 대응되는 암호문 분할 구간 내에서 상기 평문 데이터에 대응되는 값을 찾음으로써 상기 암호문 데이터를 산출하여 상기 평문 데이터를 암호화하는 것이며, 상기 복호화부는 상기 암호문 데이터가 속하는 암호문 분할 구간에 대응되는 평문 분할 구간 내에서 상기 암호문 데이터에 대응되는 값을 찾음으로써 상기 평문 데이터를 산출하여 상기 암호문 데이터를 복호화하는 것을 특징으로 한다.

발명의 효과

[0012] 본 발명은 데이터베이스 암호화 시스템 및 방법에 있어, 추가적인 제약 사항이 없이 암호화된 데이터를 효율적으로 검색할 수 있으며 데이터의 추가 및 삭제가 자유롭다.

[0013] 또한 간단한 연산으로 데이터의 암호화와 복호화가 가능하다.

[0014] 또한 사용자가 안전성 수준을 쉽게 제어할 수 있다.

도면의 간단한 설명

[0015] 도 1은 본 발명에 따른 데이터베이스 암호화 시스템의 구조를 도시함.

도 2는 본 발명에 따른 데이터베이스 암호화 방법의 흐름을 도시함.

도 3은 본 발명에 따른 암호화 및 복호화 수식을 도시함.

도 4, 5, 6, 7은 본 발명에 따른 데이터베이스 암호화 방법의 실시예를 도시함.

발명을 실시하기 위한 구체적인 내용

[0016] 아래에서는 첨부한 도면을 참조하여 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 자가 용이하게 실시할 수 있도록 본 발명의 실시예를 상세히 설명한다. 그러나 본 발명은 여러 가지 상이한 형태로 구현될 수 있으며 여기에서 설명하는 실시예에 한정되지 않는다. 그리고 도면에서 본 발명을 명확하게 설명하기 위해서 설명과 관계없는 부분은 생략하였으며, 명세서 전체를 통하여 유사한 부분에 대해서는 유사한 도면 부호를 붙였다.

[0017] 명세서 전체에서, 어떤 부분이 다른 부분과 "연결"되어 있다고 할 때, 이는 "직접적으로 연결"되어 있는 경우뿐 아니라, 그 중간에 다른 소자를 사이에 두고 "전기적으로 연결"되어 있는 경우도 포함한다. 또한 어떤 부분이 어떤 구성요소를 "포함"한다고 할 때, 이는 특별히 반대되는 기재가 없는 한 다른 구성요소를 제외하는 것이 아니라 다른 구성요소를 더 포함할 수 있는 것을 의미한다.

[0018] 도 1은 본 발명에 따른 데이터베이스 암호화 시스템(10)을 나타낸 블록도이며, 도 2는 본 발명에 따른 데이터베이스 암호화 방법의 흐름을 도시하고 있다.

[0019] 본 발명에 따른 데이터베이스 암호화 시스템(10) 및 방법은 대칭키 기반의 순서 유지 암호화 기술을 사용한다. 즉, 데이터의 암호화와 복호화에 동일한 암호화 키를 사용하며, 평문 데이터의 순서가 암호문 데이터에서도 유지된다.

[0020] 좀더 구체적으로는, 평문 데이터가 속하는 평문 구간과 이에 대응하는 암호문 구간을 설정하고 이 구간 내에서 평문 데이터에 대응되는 암호문 데이터를 찾음으로써 암호화를 수행하고, 암호화의 역변환을 수행하여 즉, 암호문 데이터에 대응되는 평문 데이터를 찾음으로써 복호화를 수행한다.

[0021] 간략히 살펴보면, 본 발명에 따른 데이터베이스 암호화 시스템(10)은 데이터베이스(100), 데이터베이스(100)에 저장할 평문 데이터를 암호화하여 암호문 데이터를 산출하는 암호화부(200), 데이터베이스(100)에 저장된 암호문 데이터를 복호화하여 평문 데이터를 산출하는 복호화부(300), 및 암호화부(200)와 복호화부(300)에서 사용되는 암호화 키를 생성하는 키 생성부(400)를 포함한다.

[0022] 즉, 키 생성부(400)가 사용자가 사전에 선택한 안전성 수준에 따라, 평문 구간, 평문 구간보다 큰 암호화 구간, 및 평문과 암호문의 분할 구간 크기를 설정하고(S210), 평문과 암호문의 분할 구간을 랜덤한 비율로 매핑하여 암호화 키를 생성한다(S220). 그런 다음, 데이터베이스(100)에 데이터를 입력할 때 암호화부(200)가 암호화를 수행하고(S230), 데이터베이스(100)에서 데이터를 출력할 때 복호화부(300)가 복호화를 수행한다(S240).

[0023] 자세한 내용은 본 발명에 따른 데이터베이스 암호화 방법의 실시예를 도시하고 있는 도 4, 5, 6, 7을 통해 살펴 보겠다.

[0024] 도 4에는 암호화되지 않았을 때의 데이터베이스 테이블의 일실시예가 도시되어 있으며, 도 5에는 도 4의 테이블이 암호화된 후의 모습이 도시되어 있다.

[0025] 본 발명에 따른 데이터베이스 암호화 시스템(10) 및 방법은 암호화된 데이터에서도 원래 데이터에서의 순서가 유지되도록 하여 데이터 검색이 효율적으로 이루어지도록 하는 것을 목표로 하므로, 순서가 의미를 갖는 데이터를 대상으로 한다. 순서가 있는 데이터는 간단한 연산으로 양의 정수로 바꿀 수 있을 것이므로, 이후 기술에서 대상 데이터들은 모두 양의 정수라고 가정한다.

[0026] 도시된 실시예에서 테이블(110)은 본 발명에 따른 대칭키 기반의 순서 유지 암호화 기술을 사용하여 암호화 대상 필드(112)와 나머지 필드들(114)을 포함한다. 암호화 대상 필드(112)에 대해 도 4의 평문 데이터 m1, m2,

m3, m4, m5가 도 5의 암호문 데이터 c1, c2, c3, c4, c5로 암호화되었다. 즉, 7, 11, 13, 17, 18이 각각 15, 33, 39, 47, 48로 대응(mapping)되었다.

- [0027] 도 6은 도 4의 평문 데이터들과 도 5의 암호문 데이터들의 대응 관계가 도시되어 있다.
- [0028] 본 발명에 따른 데이터베이스 암호화 시스템(10) 및 방법은 평문 구간을 일정 길이로 분할하고, 각각의 분할 구간을 서로 다른 임의의 비율로 늘려 암호문 구간으로 사용한다. 따라서 전체 암호문 구간은 전체 평문 구간보다 크고, 각 평문 분할 구간에 대응되는 암호문 구간의 크기는 각각 다르지만, 대응 순서는 유지된다.
- [0029] 예를 들어, 본 실시예에서 평문 구간의 크기는 20, 암호문 구간의 크기는 50이다. 즉, [0, 20]의 구간이 [0, 50]의 구간에 대응된다. 분할 구간의 크기는 5이며, 평문의 [0, 5] 구간은 암호문의 [0, 5] 구간에, 평문의 [5, 10] 구간은 암호문의 [5, 30] 구간에, 평문의 [10, 15] 구간은 암호문의 [30, 45] 구간에, 평문의 [15, 20] 구간은 암호문의 [45, 50] 구간에 대응된다.
- [0030] 평문의 [5, 10] 구간에 속하는 평문 데이터 7(m1)은 암호문의 [5, 30] 구간에 속하는 암호문 데이터 15(c1)로, 평문의 [10, 15] 구간에 속하는 평문 데이터 11(m2)은 암호문의 [30, 45] 구간에 속하는 암호문 데이터 33(c2)으로, 평문의 [10, 15] 구간에 속하는 평문 데이터 13(m3)은 암호문의 [30, 45] 구간에 속하는 암호문 데이터 39(c3)로, 평문의 [15, 20] 구간에 속하는 평문 데이터 17(m4)은 암호문의 [45, 50] 구간에 속하는 암호문 데이터 47(c4)로, 평문의 [15, 20] 구간에 속하는 평문 데이터 18(m5)은 암호문의 [45, 50] 구간에 속하는 암호문 데이터 48(c5)로 대응되었다.
- [0031] 평문 구간과 암호문 구간의 대응 관계는 키 생성부(400)가 평문 구간, 평문 구간보다 큰 암호화 구간, 및 평문과 암호문의 분할 구간 크기 등의 안전성 파라미터를 설정하고(S210), 암호화 키를 생성하는 단계(S220)를 수행한 결과이다.
- [0032] 안전성 파라미터는 사용자가 실시 환경에 따라 선택한 안전성 수준에 따라 결정된다. 예를 들어, 높은 안전성 수준을 요구하는 사용자의 경우에는 분할 구간의 개수가 늘어나도록 파라미터를 설정하면 되므로, 분할 구간의 크기가 작아지거나 암호문 구간의 크기가 커질 것이다.
- [0033] 사용자가 대용량의 키 테이블을 저장하고 있지 못할 상황인 경우에는, 분할 구간의 크기를 늘리거나 암호문 구간의 크기를 작게 하여, 분할 구간의 개수를 줄이면, 암호화 키 테이블 크기를 대폭 줄일 수 있다.
- [0034] 또는, 바람직한 실시예에서, 암호화 키 생성에 의사 난수(pseudo random number) 생성기를 사용할 수 있다. 암호화 키 생성 단계(S220)에서는 의사 난수의 시드(Seed) 값만 저장하고, 실제 전체 키 테이블은 암호화 단계(S230) 및 복호화 단계(S240)에서 시드 값으로부터 복구하여 사용하면, 분할 구간 크기를 늘리거나 암호문 구간의 크기를 작게 하지 않고도 대량의 암호화 키를 저장하지 않아도 되므로, 안전성은 높으면서도 저장 공간은 효율적으로 사용할 수 있다.
- [0035] 데이터베이스(100)에 입력되어야 할 평문 데이터가 안전성 파라미터 설정 단계(S210)에서 설정한 평문 구간의 범위를 넘어설 경우, 평문 데이터가 속하는 범위를 평문 구간 크기만큼씩 분할하면 된다. 예를 들어, 본 실시예에서처럼 평문 구간의 크기가 20으로 설정되었을 때, 데이터베이스 테이블(110)에 평문 데이터 35를 저장해야 한다면, 평문 구간을 [0, 20]과 [20, 40]으로 나누어 각각에 대해 암호화 키 생성 단계(S220), 암호화 단계(S230), 및 복호화 단계(S240)를 수행하면 된다. 따라서 본 발명에 따른 데이터베이스 암호화 시스템(10) 및 방법은 평문 데이터의 크기에 대한 제약 없이 암호화 및 복호화를 수행할 수 있다.
- [0036] 키 생성부()는 이런 식으로 사용자가 사전에 선택한 안전성 수준에 따라 안전성 파라미터를 설정하고 나면(S210), 설정된 안전성 파라미터를 이용하여 암호화 키를 생성한다(S220). 본 발명에 따른 데이터베이스 암호화 시스템(10) 및 방법에서 암호화 키는 평문 분할 구간과 대응되는 암호문 분할 구간의 분할 지점을 나타낸다.
- [0037] 도 6에 도시된 바와 같이 본 실시예에서 분할 구간의 크기는 5이고 암호문 구간 크기는 50이므로 암호화 키의 후보는 {5, 10, 15, 20, 25, 30, 35, 40, 45}이다. 암호화 키는 이 분할 지점들 중에서 평문의 분할 구간 개수보다 하나 적은 수 만큼을 임의로 중복되지 않게 선택해서 오름차순으로 정렬한 것이다. 본 실시예에서 평문의 분할 구간은 4개이므로, 암호화 키는 3개가 생성된다.
- [0038] 처음 선택된 값은 30, 그 다음에 선택된 값은 5, 그 다음 선택된 값은 45라고 할 때, 오름차순으로 정렬하면 {5, 30, 45}이므로 암호화 키 k1, k2, k3는 각각 5, 30, 45이다. 이때, 전술한 바와 같이 암호화 키 생성에 의사 난수 생성기를 사용한다면 키 테이블 {5, 30, 45}를 모두 저장하지 않고, 시드인 30만 저장할 수 있다.

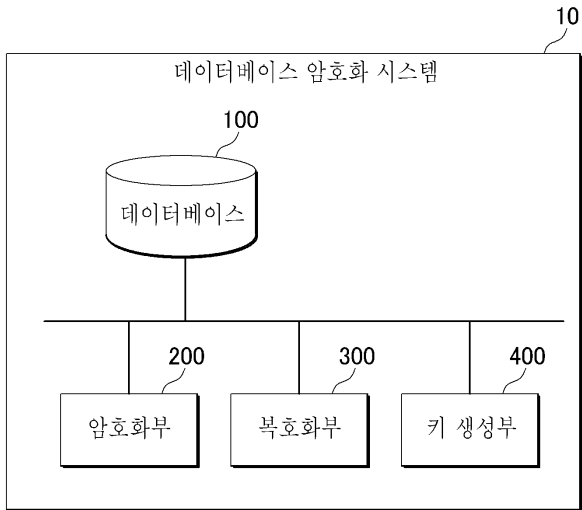
- [0039] 암호화 키에 의해 평문과 암호문의 대응 관계가 정의된 다음에는 데이터베이스(100)에 데이터를 입력할 때는 암호화(S230), 데이터베이스에서 데이터를 검색해 출력할 때는 복호화(S240)를 수행하면 된다.
- [0040] 도 3에 본 발명에 따른 암호화 및 복호화 수식이 도시되어 있다. 격쇠 표시는 반올림하여 정수로 계산한다는 의미이다.
- [0041] 암호화는 평문 데이터 m 을 암호문 데이터 c 에 대응시키는 변환이고, 복호화는 암호화의 역변환이다. 평문 데이터 m 이 평문 구간 $[p_i, p_{i+1}]$ 에 속한다면, 암호문 데이터 c 는 $[p_i, p_{i+1}]$ 에 대응되는 암호문 구간 $[key_i, key_{i+1}]$ 과 분할 구간 크기 $bucketSize$ 를 사용하여 도면의 첫번째 수식을 통해 도출할 수 있다. 복호화는 암호화의 역변환이므로 설명을 생략한다.
- [0042] 도 7은 본 실시예의 암호화 과정에 이 수식을 적용한 모습을 도시하고 있다.
- [0043] 예를 들어, 평문 데이터 7(m_1)은 평문 구간 $[5, 10]$ 에 속하고, 이에 대응되는 암호화 구간은 $[5, 30]$ 이므로, p_i 는 5, $key_i=5$, $key_{i+1}=30$ 이 되어 암호문 데이터 15(c_1)은 도면의 첫번째 수식을 통해 산출된다.
- [0044] 수식에서 보는 바와 같이, 본 발명에 따른 데이터베이스 암호화 시스템(10) 및 방법은 데이터 암호화 및 복호화 과정에서 필연적으로 발생하는 오버헤드를 정수간의 덧셈 3번과 곱셈 2번으로 줄임으로써 암호화 기술을 사용하지 않은 것과 비슷한 수준의 연산 효율성 향상을 이루고 있다.
- [0045] 전술한 본 발명의 설명은 예시를 위한 것이며, 본 발명이 속하는 기술분야의 통상의 지식을 가진 자는 본 발명의 기술적 사상이나 필수적인 특징을 변경하지 않고서 다른 구체적인 형태로 쉽게 변형이 가능하다는 것을 이해할 수 있을 것이다. 그러므로 이상에서 기술한 실시예들은 모든 면에서 예시적인 것이며 한정적이 아닌 것으로 이해해야만 한다. 예를 들어, 단일형으로 설명되어 있는 각 구성 요소는 분산되어 실시될 수도 있으며, 마찬가지로 분산된 것으로 설명되어 있는 구성 요소들도 결합된 형태로 실시될 수 있다.
- [0046] 본 발명의 범위는 상기 상세한 설명보다는 후술하는 특허청구범위에 의하여 나타내어지며, 특허청구범위의 의미 및 범위 그리고 그 균등 개념으로부터 도출되는 모든 변경 또는 변형된 형태가 본 발명의 범위에 포함되는 것으로 해석되어야 한다.

부호의 설명

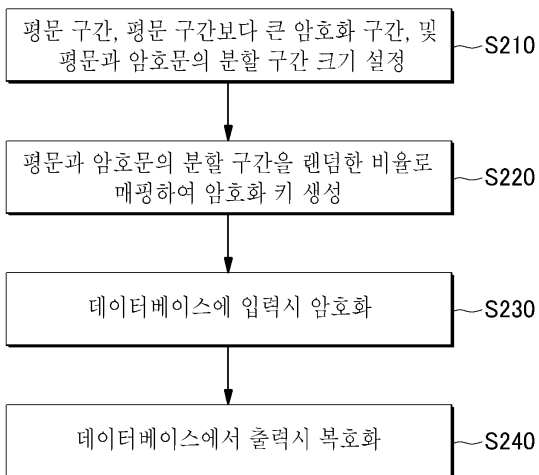
- [0047] 10: 데이터베이스 암호화 시스템
- 100: 데이터베이스
- 200: 암호화부
- 300: 복호화부
- 400: 키 생성부

도면

도면1



도면2



도면3

암호화 ($m \rightarrow c$)

$$c = \text{key}_i + \frac{(\text{key}_{i+1} - \text{key}_i)}{\text{bucketsize}} \times (m - p_i)$$

복호화 ($c \rightarrow m$)

$$m = p_i + \frac{\text{bucketsize}}{\text{key}_{i+1} - \text{key}_i} \times (c - \text{key}_i)$$

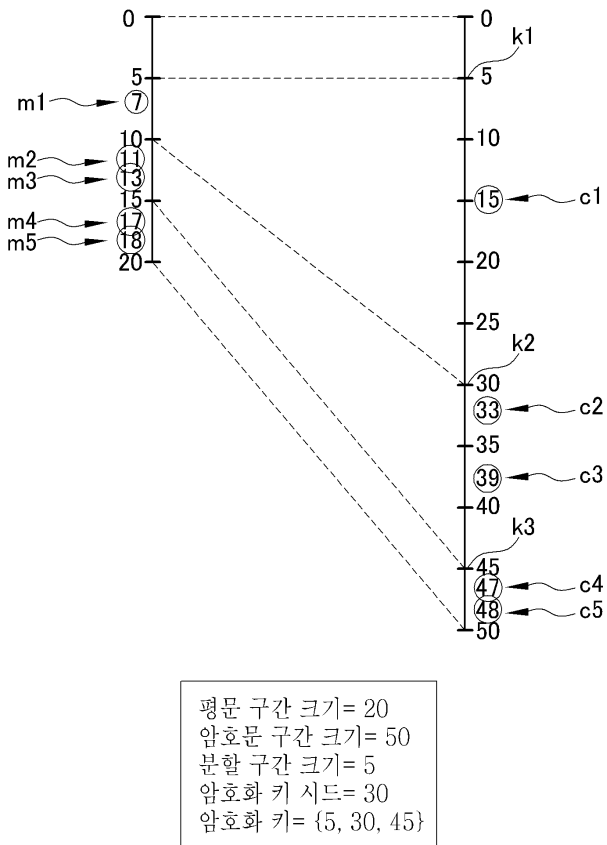
도면4

	112	110	114
m1	7	...	
m2	11	...	
m3	13	...	
m4	17	...	
m5	18	...	
	⋮	⋮	

도면5

	112	110	114
c1	15	...	
c2	33	...	
c3	39	...	
c4	47	...	
c5	48	...	
	⋮	⋮	

도면6



도면7

$$c1 = 5 + \frac{30-5}{5} \times (7-5)$$

$$c2 = 30 + \frac{45-30}{5} \times (11-10)$$

$$c3 = 30 + \frac{45-30}{5} \times (13-10)$$

$$c4 = 45 + \frac{50-45}{5} \times (17-15)$$

$$c5 = 45 + \frac{50-45}{5} \times (18-15)$$