(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2013-0126825
(43) 공개일자 2013년11월21일

(51) 국제특허분류(Int. Cl.)
G06F 21/60 (2013.01) *G06F 17/30* (2006.01)
(21) 출원번호 10-2012-0045084
(22) 출원일자 2012년04월30일
심사청구일자 2012년04월30일

(71) 출원인
고려대학교 산학협력단
서울 성북구 안암동5가 1
(72) 발명자
정익래
서울특별시 광진구 중곡1동 254-12 호동아파트 203호
김기성
경기도 군포시 산본동 1063 백합아파트 1126동 1503호
김동민
서울특별시 동대문구 청량리동 미주아파트 1동 505호
(74) 대리인
특허법인엠에이피에스

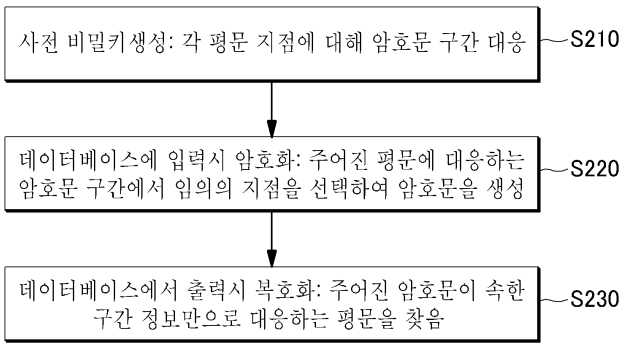
전체 청구항 수 : 총 11 항

(54) 발명의 명칭 **데이터베이스 암호화 시스템 및 방법**

(57) 요 약

본 발명은 순서가 있는 데이터를 암호화하는 방법에 있어서, (a) 전체 평문 후보 구간을 임의의 크기로 확장하여 전체 암호문 후보 구간을 설정하고, 상기 전체 암호문 후보 구간을 임의 크기의, 서로 교집합을 갖지 않는 분할된 암호문 후보 구간들로 분할한 후, 각 평문 후보 데이터를 상기 각 분할된 암호문 후보 구간에 순서대로 대응(mapping)시켜 암호화 키를 생성하는 단계; 및 (b) 상기 암호화 키를 사용하여, 주어진 평문 데이터에 대응하는 분할된 암호문 후보 구간을 찾은 후, 상기 분할된 암호문 후보 구간에 속하는 임의의 암호문 후보 데이터를 암호문 데이터로 산출하여 상기 주어진 평문 데이터를 암호화하는 단계;를 포함하는 데이터 암호화 방법을 제공한다.

대 표 도 - 도2



이 발명을 지원한 국가연구개발사업

과제고유번호	KI002113
부처명	지식경제부
연구사업명	산업융합원천기술개발사업
연구과제명	Car-헬스케어 보안 기술개발
기 여 율	1/1
주관기관	고려대학교 산학협력단
연구기간	2012.03.01 ~ 2013.02.28

특허청구의 범위

청구항 1

데이터베이스 암호화 시스템을 사용하여 순서가 있는 데이터를 암호화하는 방법에 있어서,

(a) 주어진 평문 데이터를 암호화하는 데 사용할 암호화 키를 생성하는 단계; 및

(b) 상기 암호화 키를 사용하여, 주어진 평문 데이터에 대응하는 분할된 암호문 후보 구간을 찾은 후, 상기 분할된 암호문 후보 구간에 속하는 임의의 암호문 후보 데이터를 암호문 데이터로 산출하여 상기 주어진 평문 데이터를 암호화하는 단계;를 포함하되,

상기 (a) 단계는

전체 평문 후보 구간을 임의의 크기로 확장하여 전체 암호문 후보 구간을 설정하는 단계;

상기 전체 암호문 후보 구간을 임의 크기의, 서로 교집합을 갖지 않는 분할된 암호문 후보 구간들로 분할하는 단계; 및

각 평문 후보 데이터를 상기 각 분할된 암호문 후보 구간에 순서대로 대응(mapping)시켜 암호화 키를 생성하는 단계;를 포함하는 데이터 암호화 방법.

청구항 2

제 1 항에 있어서,

(c) 상기 암호화 키를 사용하여, 주어진 암호문 데이터가 속한 분할된 암호문 후보 구간 정보에 대응하는 평문 데이터를 산출하여 상기 주어진 암호문 데이터를 복호화하는 단계;를 더 포함하는 데이터 암호화 방법.

청구항 3

제 1 항에 있어서,

상기 (a) 단계는

기설정된 안전성 수준에 따라 상기 전체 평문 후보 구간의 크기 및 상기 전체 암호문 후보 구간의 크기를 결정하는 것인 데이터 암호화 방법.

청구항 4

제 1 항에 있어서,

상기 (a) 단계는

상기 분할된 암호문 후보 구간의 개수가 상기 각 평문 후보 데이터의 개수와 같은 것인 데이터 암호화 방법.

청구항 5

제 1 항에 있어서,

상기 (b) 단계는

동일한 평문 데이터에 대해 암호화 수행시마다 다른 암호문 데이터가 산출될 수 있는 것인 데이터 암호화 방법.

청구항 6

제 2 항에 있어서,

상기 (c) 단계는

상기 주어진 암호문 데이터의 값에 상관없이 상기 주어진 암호문 데이터가 속한 분할된 암호문 후보 구간 정보만을 사용하여 상기 평문 데이터를 찾아내는 것인 데이터 암호화 방법.

청구항 7

데이터베이스 암호화 시스템에 있어서,

전체 평문 후보 구간을 임의의 크기로 확장하여 전체 암호문 후보 구간을 설정하고, 상기 전체 암호문 후보 구간을 임의 크기의, 서로 교집합을 갖지 않는 분할된 암호문 후보 구간들로 분할한 후, 각 평문 후보 데이터를 상기 각 분할된 암호문 후보 구간에 순서대로 대응(mapping)시켜 암호화 키를 생성하는 키 생성부;

상기 암호화 키를 사용하여, 주어진 평문 데이터에 대응하는 분할된 암호문 후보 구간을 찾은 후, 상기 분할된 암호문 후보 구간에 속하는 임의의 암호문 후보 데이터를 암호문 데이터로 산출하여 상기 주어진 평문 데이터를 암호화하는 암호화부; 및

상기 암호화부에 의해 산출된 암호문 데이터를 저장하는 데이터베이스를 포함하는 데이터베이스 암호화 시스템.

청구항 8

제 7 항에 있어서,

상기 암호화 키를 사용하여, 주어진 암호문 데이터가 속한 분할된 암호문 후보 구간 정보에 대응하는 평문 데이터를 산출하여 상기 주어진 암호문 데이터를 복호화하는 복호화부;를 더 포함하는 데이터베이스 암호화 시스템.

청구항 9

제 7 항에 있어서,

상기 키 생성부는

기설정된 안전성 수준에 따라 상기 전체 평문 후보 구간의 크기 및 상기 전체 암호문 후보 구간의 크기를 결정하며,

상기 분할된 암호문 후보 구간의 개수가 상기 각 평문 후보 데이터의 개수와 같은 것인 데이터베이스 암호화 시스템.

청구항 10

제 7 항에 있어서,

상기 암호화부는

동일한 평문 데이터에 대해 암호화 수행시마다 다른 암호문 데이터가 산출될 수 있는 것인 데이터베이스 암호화 시스템.

청구항 11

제 8 항에 있어서,

상기 복호화부는

상기 주어진 암호문 데이터의 값에 상관없이 상기 주어진 암호문 데이터가 속한 분할된 암호문 후보 구간 정보만을 사용하여 상기 평문 데이터를 찾아내는 것인 데이터베이스 암호화 시스템.

명 세 서

기 술 분 야

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

배 경 기 술

[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 데이터

베이스 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 순서가 있는 데이터를 암호화하는 방법은, (a) 전체 평문 후보 구간을 임의의 크기로 확장하여 전체 암호문 후보 구간을 설정하고, 상기 전체 암호문 후보 구간을 임의 크기의, 서로 교집합을 갖지 않는 분할된 암호문 후보 구간들로 분할한 후, 각 평문 후보 데이터를 상기 각 분할된 암호문 후보 구간에 순서대로 대응(mapping)시켜 암호화 키를 생성하는 단계; 및 (b) 상기 암호화 키를 사용하여, 주어진 평문 데이터에 대응하는 분할된 암호문 후보 구간을 찾은 후, 상기 분할된 암호문 후보 구간에 속하는 임의의 암호문 후보 데이터를 암호문 데이터로 산출하여 상기 주어진 평문 데이터를 암호화하는 단계;를 포함하는 것을 특징으로 한다.

[0011] 상기와 같은 목적을 달성하기 위한 본 발명의 제 2 측면에 따른 데이터베이스 암호화 시스템은, 전체 평문 후보 구간을 임의의 크기로 확장하여 전체 암호문 후보 구간을 설정하고, 상기 전체 암호문 후보 구간을 임의 크기의, 서로 교집합을 갖지 않는 분할된 암호문 후보 구간들로 분할한 후, 각 평문 후보 데이터를 상기 각 분할된 암호문 후보 구간에 순서대로 대응(mapping)시켜 암호화 키를 생성하는 키 생성부; 상기 암호화 키를 사용하여, 주어진 평문 데이터에 대응하는 분할된 암호문 후보 구간을 찾은 후, 상기 분할된 암호문 후보 구간에 속하는 임의의 암호문 후보 데이터를 암호문 데이터로 산출하여 상기 주어진 평문 데이터를 암호화하는 암호화부; 및 상기 암호화부에 의해 산출된 암호문 데이터를 저장하는 데이터베이스를 포함하는 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 데이터의 암호화와 복호화 과정이 매우 단순하므로 효율성이 높다.

[0014] 또한 동일한 평문 데이터가 암호화시마다 다른 암호문으로 암호화되므로 안전성이 높다.

[0015] 또한 사용자가 안전성 수준을 쉽게 제어할 수 있다.

도면의 간단한 설명

[0016] 도 1은 본 발명에 따른 데이터베이스 암호화 시스템의 구조를 도시함.

도 2, 3, 4, 5는 본 발명에 따른 데이터 암호화 방법의 흐름을 도시함.

도 6, 7은 본 발명에 따른 데이터 암호화 방법의 실시예를 도시함.

발명을 실시하기 위한 구체적인 내용

[0017] 아래에서는 첨부한 도면을 참조하여 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 자가 용미만이게 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.

[0018] 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.

[0019] 도 1은 본 발명에 따른 데이터베이스 암호화 시스템(10)을 나타낸 블록도이며, 도 2, 3, 4, 5는 본 발명에 따른 데이터 암호화 방법의 흐름을 도시하고 있다. 이 도면들을 통해 본 발명에 따른 데이터베이스 암호화 시스템(10) 및 방법에 대해 간략하게 살펴보자. 자세한 내용은 이후 본 발명에 따른 데이터 암호화 방법의 실시예를 도시하고 있는 도 6, 7을 통해 살펴보겠다.

[0020] 먼저 도 1을 간략히 살펴보면, 본 발명에 따른 데이터베이스 암호화 시스템(10)은 데이터베이스(100), 데이터베이스(100)에 저장하기 위해 주어진 평문 데이터를 암호화하여 암호문 데이터를 산출하는 암호화부(200), 데이터베이스(100)에서 출력된 암호문 데이터를 복호화하여 평문 데이터를 산출하는 복호화부(300), 및 암호화부(200)와 복호화부(300)에서 사용되는 암호화 키를 생성하는 키 생성부(400)를 포함한다.

[0021] 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.

[0022] 평문 데이터에 대응하는 분할된 암호문 후보 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.

[0023] 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.

[0024] 키 생성부(400)는 전체 평문 후보 구간을 임의의 크기로 확장하여 전체 암호문 후보 구간을 설정하고, 상기 전체 암호문 후보 구간을 임의 크기의, 서로 교집합을 갖지 않는 분할된 암호문 후보 구간들로 분할한 각 분할된 암호문 후보 구간에 각 평문 후보 데이터를 순서대로 대응(mapping)시켜 암호화 키를 생성한다.

[0025] 먼저, 사용할 평문 후보 데이터의 개수, 즉 전체 평문 후보 구간의 크기에 따라 전체 암호문 후보 구간을 정의한다. 전체 암호문 후보 구간을 어느 정도 크게 할 것인지는 사용자에 의해서 결정된다. 전체 암호문 후보 구간의 크기가 커지면 안전성은 높아지고 효율성은 떨어지게 되며, 평문 후보 데이터의 개수에 따른 안전성과 효율성 관계는 이와는 반대로 나타내게 된다.

[0026] 따라서 사용자는 자신에게 맞는 효율성과 안전성 레벨을 정하여 전체 평문 후보 구간의 크기 및/또는 전체 암호문 후보 구간의 크기를 설정할 수 있다. 즉, 키 생성부(400)는 사용자에 의해 기설정된 안전성 수준에 따라 전체 평문 구간의 크기 및/또는 전체 암호문 구간의 크기를 결정할 수 있다.

[0027] 다음, 평문 후보 데이터의 개수만큼 전체 암호문 후보 구간을 임의로 분할한다. 이때 주의할 점은 각 암호문 분할 구간 사이에 교집합이 발생되지 않게 분할해야 복호화시 문제가 발생하지 않는다는 것이다. 또한 구간 분할

시 규칙성이 발생하지 않도록 주의해야 한다.

[0028] 다음, 각 암호문 분할 구간을 순차적으로 각 평문 후보 데이터에 대응시킨다. 이러한 대응 관계가 본 발명에 따른 데이터베이스 암호화 시스템(10)에서 암호화 키 역할을 하게 된다. 따라서 안전하게 저장되어야 한다.

[0029] 암호화부(200)는 주어진 평문 데이터에 대응하는 분할된 암호문 후보 구간에서 임의의 암호문 후보 데이터를 선택하여 암호문 데이터로 산출한다.

[0030] 암호문 데이터를 적절한 후보 중에서 임의로 선택하기 때문에, 동일한 평문 데이터에 대해 암호화 수행시마다 다른 암호문 데이터가 산출될 수 있다. 따라서 본 발명에 따른 데이터베이스 암호화 시스템(10)은 공격자가 원래의 평문 데이터를 추측하는 것을 어렵게 한다. 자세한 내용은 실시예를 통해 후술한다.

[0031] 복호화부(300)는 주어진 암호문 데이터가 속한 분할된 암호문 후보 구간 정보에 대응하는 평문 후보 데이터를 찾아 평문 데이터로 산출한다.

[0032] 주어진 암호문 데이터가 속한 분할된 암호문 후보 구간 정보만을 사용하여 평문 데이터를 찾아내기 때문에, 본 발명에 따른 데이터베이스 암호화 시스템(10)은 연산 부하가 매우 낮아 효율적이다. 자세한 내용은 실시예를 통해 후술한다.

[0033] 또한 도 2를 간략히 살펴보면, 본 발명에 따른 데이터 암호화 방법은 다음과 같은 흐름을 갖는다.

[0034] 데이터베이스(100)에 데이터를 입력하거나 출력하기 전에, 키 생성부(400)에 의해 암호화 키가 생성된다(S210). 이후 데이터베이스(100)에 데이터를 저장할 때는 암호화부(200)에 의해 암호화가 수행되며(S220), 데이터베이스(100)에서 데이터를 읽어올 때는 복호화부(300)에 의해 복호화가 수행된다(S230).

[0035] 도 3, 4, 5는 도 2의 각 단계를 구체적으로 나타낸 흐름도이다.

[0036] 도 3은 본 발명에 따른 데이터 암호화 방법의 암호화 키 생성 단계(S210)를 도시하고 있다.

[0037] 먼저 사용자가 사전에 선택한 안전성 수준에 따라, 전체 평문 후보 구간을 임의의 크기로 확장하여 전체 암호문 후보 구간을 정한다(S310). 전체 암호문 후보 구간을 임의 크기의, 서로 교집합을 갖지 않는 분할된 암호문 후보 구간들로 분할한 후, 각 평문 후보 데이터를 각 분할된 암호문 후보 구간에 순서대로 대응(mapping)시켜 암호화 키를 생성한다(S320).

[0038] 즉, 본 발명에 따른 암호화 방법에서의 암호화 키는 각 평문 후보 데이터와 분할된 암호문 후보 구간의 대응 관계이다.

[0039] 전체 암호문 후보 구간의 크기가 커지면 안전성은 높아지고 효율성은 떨어지게 되며, 전체 암호문 후보 구간의 크기가 작아지면 반대의 결과가 나오게 된다. 따라서 사용자는 자신에게 맞는 효율성과 안전성 수준을 설정하여 전체 암호문 후보 구간의 크기를 제어할 수 있다.

[0040] 도 4는 본 발명에 따른 데이터 암호화 방법의 암호화 단계(S220)를 도시하고 있다.

[0041] 본 발명에 따른 데이터베이스 암호화 시스템(10)의 암호화부(200)는 암호화 키를 사용하여, 주어진 평문 데이터에 대응하는 분할된 암호문 후보 구간을 찾은 후(S410), 이 분할된 암호문 후보 구간에 속하는 임의의 암호문 후보 데이터를 암호문으로 선택한다(S420).

[0042] 즉, 본 발명에 따른 암호화 방법은 동일한 평문 데이터에 대해 암호화 수행시마다 다른 암호문 데이터가 산출될 수 있는 확률론적(probabilistic) 암호화 방법이다. 따라서, 본 발명에 따른 데이터 암호화 방법은 결정론적(deterministic) 암호화 방법 즉, 동일한 평문은 항상 동일한 암호문으로 대응되는 방식보다 안전하다.

[0043] 도 5는 본 발명에 따른 데이터 암호화 방법의 복호화 단계(S230)를 도시하고 있다.

[0044] 본 발명에 따른 데이터베이스 암호화 시스템(10)의 복호화부(300)는 암호화 키를 사용하여, 주어진 암호문 데이터가 속한 분할된 암호문 후보 구간 정보를 찾은 후(S510), 이 분할된 암호문 후보 구간에 대응하는 평문 데이터를 찾아낸다(S520).

[0045] 즉, 주어진 암호문 데이터의 값에 상관없이 암호문 데이터가 속한 분할된 암호문 후보 구간 정보만을 사용하여 대응하는 평문 데이터를 찾아낸다. 따라서, 본 발명에 따른 암호화 방법은 동일한 평문 데이터에 대해 암호화 수행시마다 다른 암호문 데이터가 산출되어 안전성이 높음에도 불구하고 복호화시의 효율성이 높다.

[0046] 도 6, 7은 본 발명에 따른 데이터베이스 암호화 시스템을 활용한 데이터 암호화 방법의 실시예를 도시하고

있다.

[0047] 도 6의 첫번째 도면에는 암호화되기 전의, 두번째 및 세번째 도면에는 암호화된 후의 데이터베이스 테이블의 일 실시예가 도시되어 있다.

[0048] 도시된 실시예에서 테이블(110)은 하나 이상의 암호화 비적용 필드(112) 및/또는 하나 이상의 암호화 적용 필드(114)를 포함한다.

[0049] 예를 들어, 본 실시예의 설계자는 학생의 이름이나 소속은 노출되어도 문제되지 않을 데이터라고 판단하여 암호화 비적용 필드(112)로, 국어 점수나 영어 점수 등 시험 성적은 노출되었을 때 문제가 될 데이터라고 판단하여 암호화 적용 필드(114)로 설정하였을 수 있다.

[0050] 본 발명의 관심 대상은 순서가 있는 데이터가 암호화되어 저장되는 암호화 적용 필드(114)로, 예를 들어 본실시예에서 암호화 적용 필드(114) 중 하나로 도시되어 있는 국어 점수 필드에 저장될 데이터로 선택될 수 있는 값(이를 평문 후보 데이터라고 하자)은 0 이상 100이하의 정수 중에서 하나로 설정되어 있을 수 있다.

[0051] 도시된 바와 같이 이 필드에서 원래의 데이터인 평문 데이터 (55(m1) 및 88(m2)) 대신에 실제로 데이터베이스에 저장되는 것은 암호화 데이터(99(c1) 및 125(c2) 또는 103(c1) 및 124(c2))이다.

[0052] 이렇게, 본 발명에 따른 암호화 방법에 따르면 평문 데이터(m1, m2)가 동일해도 암호화시마다 다른 암호문 데이터(c1, c2)가 산출될 수 있다. 따라서 데이터베이스 공격자가 암호문 데이터(c1, c2)를 획득하더라도 이로부터 원래의 평문 데이터(m1, m2)를 추측하는 것이 어려워지므로 안전성이 향상된다는 장점이 있다.

[0053] 도 7에는 도 6의실시예에서 평문 데이터(m1, m2)와 암호문 데이터(c1, 2)의 대응 관계가 도시되어 있다.

[0054] 좌측의 전체 평문 후보 구간을 나타낸 수직선에 도시되어 있는 바와 같이, 본 실시예에서 평문 후보 데이터는 전술한 바와 같이 [0, 1, 2, ..., 100]이다. 즉, 전체 평문 후보 구간은 0 이상 100이하이다.

[0055] 우측 전체 암호문 후보 구간을 나타낸 수직선을 보면, 본 실시예에서 전체 암호문 후보 구간은 0 이상 200 미만으로 설정되어 있음을 알 수 있다. 즉, 본 실시예에서 암호화 적용 필드(114)에 평문 데이터 대신 선택되어 저장될 수 있는 암호문 후보 데이터는 0 이상 200 미만의 정수이다.

[0056] 이는 사용자가 기설정한 안전성 수준에 따라 암호화 키 생성(S210)의 첫 단계(S310)에서 설정된 전체 암호문 후보 구간의 크기가 200임을 의미한다.

[0057] 암호화 키 생성(S210)의 그 다음 단계(S320)에서 우측의 전체 암호문 후보 구간은 임의의 크기로 서로 겹치지 않게 분할되어 각 평문 후보 데이터에 대응되었다. 도면에서 실선은 이상, 점선은 미만을 의미한다. 예컨대, 평문 후보 데이터 55에 대응되는 분할된 암호문 후보 구간은 85 이상 107 미만이며, 따라서 이 구간에 속하는 암호문 후보 데이터는 [85, 86, ..., 106]이다.

[0058] 이때, 평문 후보 데이터 즉, 선택될 수 있는 평문 데이터의 후보가 101개이므로 분할된 암호문 후보 구간의 개수도 101개이다. 평문 후보 데이터 각각에 대해 분할된 암호문 후보 구간을 순서대로 대응시키기 위함이다.

[0059] 이때 주의할 점은 분할된 암호문 후보 구간들이 서로 겹치지 않아야 한다는 것이다. 또한, 각 구간의 크기에 규칙성이 있으면 안전성이 저하될 수 있다.

[0060] 예를 들어, 평문 후보 데이터 88에 대응하는 분할된 암호문 후보 구간은 120 이상 130 미만으로 이 구간에 속하는 암호문 후보 데이터는[120, 121, ..., 129]의 10개이나, 평문 후보 데이터 100에 대응하는 분할된 암호문 후보 구간은 195 이상 200 미만으로 이 구간에 속하는 암호문 후보 데이터는[195, 196, ..., 199]의 5개이다.

[0061] 정리하자면 도시되어 있는 바와 같이, 각 분할된 암호문 후보 구간은 서로 교집합을 가지고 있지 않으며, 구간의 크기는 임의로 결정되었고, 순서대로 평문 후보 데이터에 대응되고 있다.

[0062] 이렇게 각 평문 후보 데이터와 분할된 암호문 후보 구간의 대응 관계를 정의하여 암호화 키를 생성하고 나면, 데이터베이스에 데이터를 입출력할 때 수행하는 암호화(S220) 또는 복호화(S230) 수행시 정의된 암호화 키를 사용하여 대응 관계를 찾으면 된다.

[0063] 예를 들어, 암호화 적용 필드(114)에 평문 데이터 55(m1)를 저장하려고 한다면, 암호화 키인 대응 관계를 먼저 살펴야 한다. 도면을 보면 55에 대응하는 분할된 암호문 후보 구간은 85 이상 107 미만이다. 따라서 [85, 86, ..., 106] 중 하나가 암호문 데이터로 선택될 수 있다. 본 발명에 따른 암호화 방법은 암호화시마다 이들 중 임의의 하나를 암호문 데이터로 선택하므로, 도 6의 실시예에 도시되어 있는 바와 같이 암호화 적용 필드(114)에

는 암호화시마다 한번은 99(c1)가, 또한번은 103(c1)이 암호화 데이터로 산출되어 저장되었다.

[0064] 암호화 적용 필드(114)에 저장되어 있는 [85, 86, ..., 106] 중 하나(c1)를 출력할 때는 원본인 평문 데이터로 복호화해야 한다. 이때 본 발명에 따른 암호화 방법을 사용하면 단순히 해당 분할된 암호문 후보 구간에 대응되는 평문 후보 데이터를 찾으면 되므로 부하가 매우 낮다. 도시되어 있는 바와 같이, 85 이상 107 미만이라는 분할된 암호문 후보 구간에 대응하는 평문 후보 데이터는 55이므로, 55(m1)가 출력된다.

[0065] 전술한 바와 같이, 본 발명에 따른 암호화 방법은 비결정적이다. 예를 들어, 본 실시예에서 암호화 적용 필드(114)에 저장하도록 선택된 평문 데이터 m1, m2 는 각각 55, 88로 동일하나, 이에 대한 암호문 데이터 c1, c2는 각각 99, 125 또는 각각 103, 124로 암호화 시점마다 다르다. 즉, 평문 데이터가 동일해도 실제 암호화 적용 필드(114)에는 암호화 수행시마다 다른 값이 선택되어 저장된다.

[0066] 암호화 적용 필드(114)가 데이터 중복이 허용되는 필드여서, 55(m1)이 여러 번 저장되더라도, 실제로 저장되는 값은 [85, 86, ..., 106] 중 하나(c1)이므로, 공격자는 암호화 적용 필드(114)를 들여다보더라도 여러 다른 데이터가 사실은 같은 데이터를 나타낸다는 것을 알아내기가 쉽지 않을 것이다.

[0067] 예를 들어, 도시되어 있는 실시예에서 김갑돌 학생의 국어 점수가 55인데, 도시되어 있지 않지만 박순동 학생의 국어 점수도 55이라고 가정해보자. 암호화하지 않고 저장했거나 결정적 암호화 방법을 사용하여 암호화하여 저장했다면 데이터베이스에서 추출한 두 학생의 점수는 같은 값을 가질 것이다. 따라서 적어도 두 학생이 같은 점수를 갖고 있다는 정보는 아무런 연산을 거치지 않고서도 공격자에게 즉시 노출된다. 그러나, 본 발명에 따른 비결정적 암호화 방법을 사용하였을 때는 암호화시마다 다른 값이 선택되어 저장되므로, 공격자는 두 학생이 같은 점수를 받았는지 알 수 없다.

[0068] 이렇게 동일한 평문 데이터에 대해 암호화 수행시마다 다른 암호문 데이터를 산출하기 때문에 본 발명에 따른 확률론적인 순서 유지 암호화 방법은 결정론적 암호화 방법보다 높은 안전성을 제공한다.

[0069] 반면, 복호화시는 별다른 연산 없이 암호화 분할 구간과 평문 후보 데이터 사이의 대응 관계만으로 원래의 평문 데이터를 찾아내므로, 효율성이 높다.

[0070] 예를 들어, 암호화 적용 필드(114)에 저장되어 있는 값이 99(c1)이든 103(c1)이든 85이상 107 미만이라는 분할된 암호문 후보 구간에 속하므로, 이에 대응되는 평문 후보 데이터인 55를 평문 데이터(m1)로 출력하면 된다.

[0071] 한편, 예를 들어, 평문 데이터 55이 변환될 수 있는 암호문 데이터 후보가 [85, 86, ..., 106] 중 하나에서 [85, 86, ..., 200] 중 하나로 그 개수가 늘어난다면 안전성이 좀더 증가할 것이고, 줄어든다면 안전성이 좀더 감소할 것임이 쉽게 이해될 것이다. 이는 각각의 평문 후보 데이터에 대해 마찬가지일 것이므로, 전체 평문 후보 구간에 대해서도 마찬가지일 것임도 쉽게 이해될 것이다.

[0072] 따라서, 전술한 바와 같이, 전체 암호문 후보 구간의 크기를 늘리면 안전성이 높아지고, 전체 암호문 후보 구간의 크기를 줄이면 그 반대가 된다. 반면 전체 암호문 후보 구간의 크기가 늘어날수록 효율성은 낮아지므로, 사용자는 적절한 안전성 수준을 선택하여 전체 암호문 후보 구간의 크기를 제어할 수 있다.

[0073] 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.

[0074] 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

[0075] 10: 데이터베이스 암호화 시스템

100: 데이터베이스

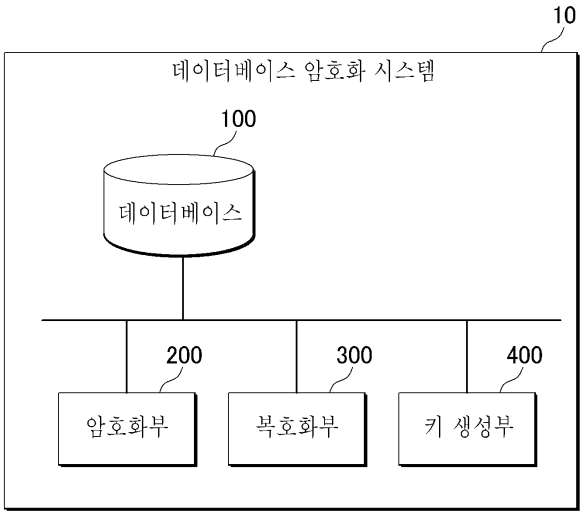
200: 암호화부

300: 복호화부

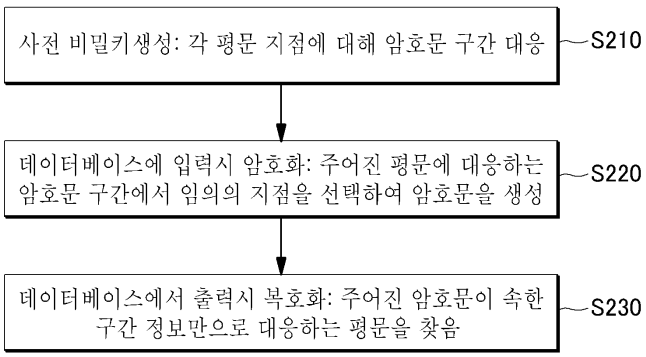
400: 키 생성부

도면

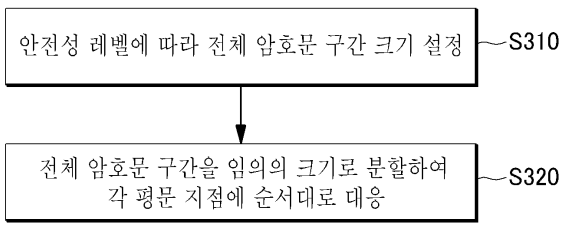
도면1



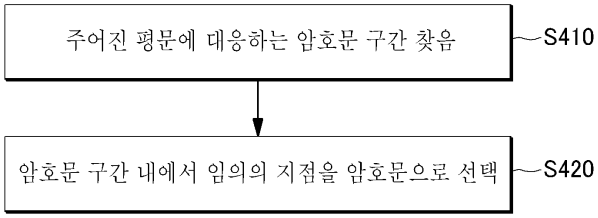
도면2



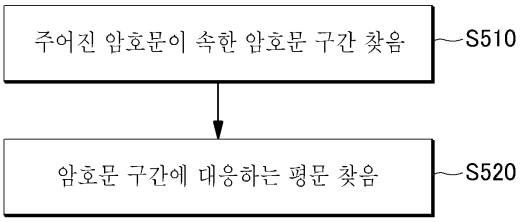
도면3



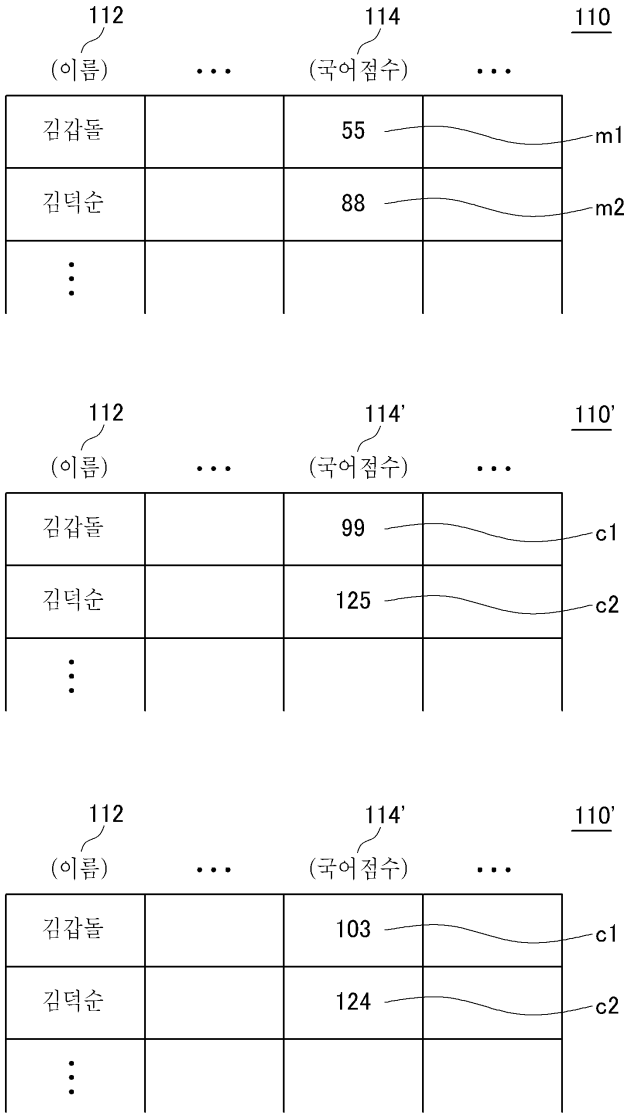
도면4


주어진 평문에 대응하는 암호문 구간 찾음
S410
암호문 구간 내에서 임의의 지점을 암호문으로 선택
S420

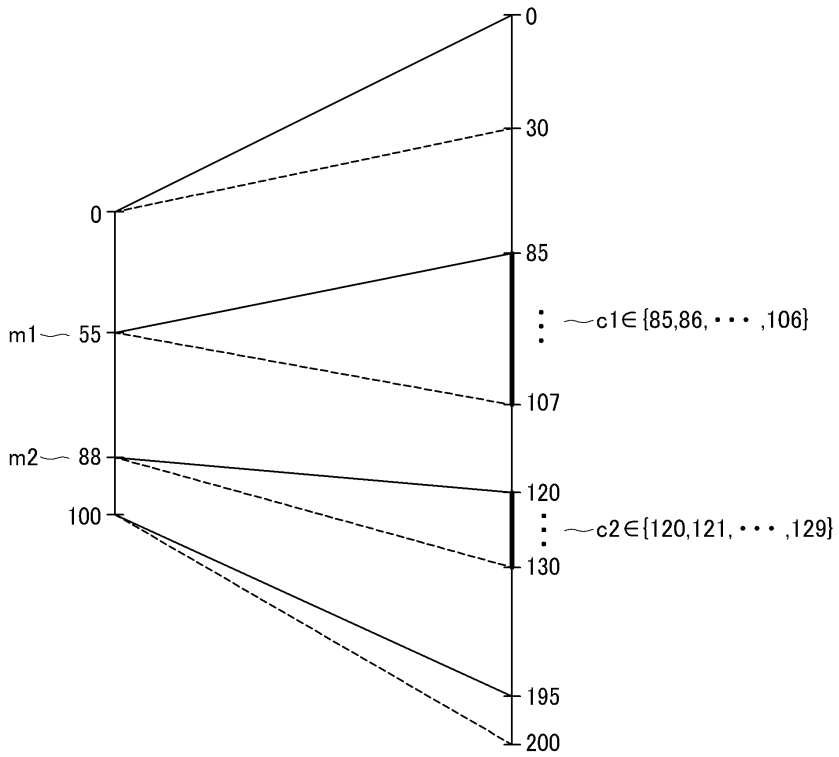
도면5


주어진 암호문이 속한 암호문 구간 찾음
S510
암호문 구간에 대응하는 평문 찾음
S520

도면6


112
114
110
(이름)
(국어점수)
김갑돌
55
m1
김덕순
88
m2
112
114'
110'
(이름)
(국어점수)
김갑돌
99
c1
김덕순
125
c2
112
114'
110'
(이름)
(국어점수)
김갑돌
103
c1
김덕순
124
c2

도면7


0
30
0
85
m1
55
c1∈{85,86,・・・,106}
107
m2
88
120
100
c2∈{120,121,・・・,129}
130
195
200