(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2019-0010251
(43) 공개일자 2019년01월30일

(51) 국제특허분류(Int. Cl.)
H04L 9/08 (2006.01) *H04L 9/06* (2006.01)
(52) CPC특허분류
H04L 9/0869 (2013.01)
H04L 9/0631 (2013.01)
(21) 출원번호 10-2017-0092786
(22) 출원일자 2017년07월21일
심사청구일자 2017년07월21일

(71) 출원인
건국대학교 산학협력단
서울특별시 광진구 능동로 120, 건국대학교내 (화양동)
(72) 발명자
김기천
서울특별시 서초구 방배로 270, 다동 504호 (방배본동, 신삼호아파트)
유요셉
서울특별시 노원구 공릉로 320, 401동 304호 (하계동, 하계동청구빌라)
(74) 대리인
특허법인 무한

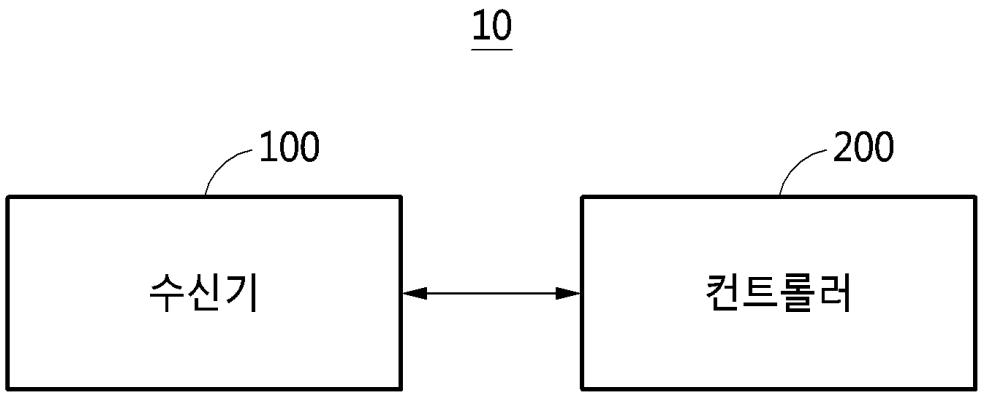
전체 청구항 수 : 총 15 항

(54) 발명의 명칭 **클라우드 스토리지 전송단계에서의 보안성 강화를 위한 LPES 방법 및 장치**

(57) 요 약

일 실시예에 따른 암호화 방법 및 장치가 개시된다. 일 실시예에 따른 암호화 방법은, 전송하기 위한 객체의 일부를 암호화하는 단계와, 난수(random number) 규칙을 이용하여 상기 일부가 암호화된 객체를 셔플링(shuffling)함으로써 암호화된 데이터를 생성하는 단계를 포함한다.

대 표 도 - 도1



이 발명을 지원한 국가연구개발사업

과제고유번호 2016A0150017

부처명 미래창조과학부

연구관리전문기관 정보통신기술진흥센터

연구사업명 방통융합서비스 사업화 기반구축사업

연구과제명 (2차) 글로벌딜리버리 클라우드 플랫폼의 대규모 OTT서비스 적용을 위한 방송-통신 사업자 공동의 시범 사업

기 여 율 1/1

주관기관 주식회사 솔박스

연구기간 2016.08.01 ~ 2017.07.31

명 세 서

청구범위

청구항 1

전송하기 위한 객체의 일부를 암호화하는 단계; 및

난수(random number) 규칙을 이용하여 상기 일부가 암호화된 객체를 셔플링(shuffling)함으로써 암호화된 데이터를 생성하는 단계

를 포함하는 암호화 방법.

청구항 2

제1항에 있어서,

상기 암호화하는 단계는,

상기 객체의 일부를 경량 AES(Advanced Encryption Standard) 알고리즘을 통해 암호화하는 단계

를 포함하는 암호화 방법.

청구항 3

제1항에 있어서,

상기 생성하는 단계는,

상기 일부가 암호화된 객체를 복수의 블록으로 분할하는 단계;

상기 난수 규칙을 생성하는 단계; 및

상기 복수의 블록을 상기 난수 규칙에 따라 셔플링하는 단계; 및

셔플링된 복수의 블록을 병합하는 단계

를 포함하는 암호화 방법.

청구항 4

제1항에 있어서,

상기 난수 규칙을 암호화하여 상기 암호화된 데이터를 복호화하는 장치로 전송하는 단계

를 더 포함하는 암호화 방법.

청구항 5

암호화된 데이터 및 암호화된 난수 규칙을 수신하는 단계; 및

상기 암호화된 난수 규칙에 기초하여 상기 암호화된 데이터의 순서를 복원함으로써 데이터를 복원하는 단계

를 포함하는 암호화 방법.

청구항 6

제5항에 있어서,

상기 복원하는 단계는,

상기 암호화된 난수 규칙을 복호화하여 난수 규칙을 생성하는 단계;

상기 난수 규칙을 이용하여 상기 암호화된 데이터의 순서를 복원하는 단계; 및

순서가 복원된 암호화된 데이터를 복호화하는 단계

를 포함하는 암호화 방법.

청구항 7

제6항에 있어서,

상기 복호화하는 단계는,

상기 순서가 복원된 암호화된 데이터를 경량 AES(Advanced Encryption Standard) 알고리즘을 통해 복호화하는 단계

를 포함하는 암호화 방법.

청구항 8

전송하기 위한 객체를 수신하는 수신기; 및

상기 전송하기 위한 객체의 일부를 암호화하고, 난수(random number) 규칙을 이용하여 상기 일부가 암호화된 객체를 셔플링(shuffling)함으로써 암호화된 데이터를 생성하는 컨트롤러

를 포함하는 암호화 장치.

청구항 9

제8항에 있어서,

상기 컨트롤러는,

상기 전송하기 위한 객체의 일부를 암호화하는 부분 암호화기; 및

상기 난수(random number) 규칙을 이용하여 상기 일부가 암호화된 객체를 셔플링(shuffling)함으로써 상기 암호화된 데이터를 생성하는 암호화 데이터 생성기

를 포함하는 암호화 장치.

청구항 10

제8항에 있어서,

상기 컨트롤러는,

상기 객체의 일부를 경량 AES(Advanced Encryption Standard) 알고리즘을 통해 암호화하는

암호화 장치.

청구항 11

제9항에 있어서,

상기 암호화 데이터 생성기는,

상기 일부가 암호화된 객체를 복수의 블록으로 분할하고, 상기 난수 규칙을 생성하고, 상기 복수의 블록을 상기 난수 규칙에 따라 셔플링하고, 셔플링된 복수의 블록을 병합하는

암호화 장치.

청구항 12

제9항에 있어서,

상기 컨트롤러는,

상기 난수 규칙을 암호화하여 상기 암호화된 데이터를 복호화하는 장치로 전송하는 난수 규칙 공유기

를 더 포함하는 암호화 장치.

청구항 13

암호화된 데이터 및 암호화된 난수 규칙을 수신하는 수신기; 및

상기 암호화된 난수 규칙에 기초하여 상기 암호화된 데이터의 순서를 복원함으로써 데이터를 복원하는 컨트롤러

를 포함하는 암호화 장치.

청구항 14

제13항에 있어서,

상기 컨트롤러는,

상기 암호화된 난수 규칙을 복호화하여 난수 규칙을 생성하는 난수 규칙 복호화기;

상기 난수 규칙을 이용하여 상기 암호화된 데이터의 순서를 복원하는 순서 복원기; 및

순서가 복원된 암호화된 데이터를 복호화하는 데이터 복호화기

를 포함하는 암호화 장치.

청구항 15

제13항에 있어서,

상기 컨트롤러는,

상기 순서가 복원된 암호화된 데이터를 경량 AES(Advanced Encryption Standard) 알고리즘을 통해 복호화하는

암호화 장치

발명의 설명

기 술 분 야

[0001] 아래 실시예들은 클라우드 스토리지 전송 단계에서의 보안성 강화를 위한 LPES(Lightweight Partial Encryption

and Shuffling) 방법 및 장치에 관한 것이다.

배 경 기 술

[0002] 최근 컨텐츠 제공 업체와 사용자들로부터 생성되는 미디어 데이터 용량이 늘어나고 있다. 이에 따라, 사용자들은 자신이 보유한 단말 외에 추가적인 저장공간이 필요하게 되었다. 또한, 단말의 교체 시 이동하는 데이터가 증가하며 이를 제공해주는 서비스에 대한 요구가 늘어나고 있다.

[0003] 이에 추가 저장소 및 백업 장치로써 클라우드 스토리지 서비스의 사용률이 늘어나는 추세이다. 클라우드 서비스에 대한 수요가 증가하고 이와 함께 보안 이슈가 대두됨에 따라 서비스 제공자들은 다양한 보안 기술들을 클라우드 시스템에 적용하기 시작했다.

[0004] 가장 기본적인 보안 위협 중 하나인 데이터 스니핑(data sniffing)에 대응하기 위해 주요 클라우드 스토리지 제공 업체들은 데이터 전송 시 암호화 통신을 제공한다. 그러나 암호화를 통한 대용량 데이터 전송은 양측 단말에 부하를 발생시켜 처리 및 전송 속도의 저하를 야기할 수 있다.

[0005] 따라서, 단말의 부하를 감소시키고, 전송속도 저하를 야기하지 않는 암호화 방법이 필요하다.

발명의 내용

해결하려는 과제

[0006] 실시예들은 클라우드 스토리지 전송 단계에서 단말의 부하를 감소시키면서 전송 속도를 저하시키지 않는 암호화 기술을 제공할 수 있다.

과제의 해결 수단

[0007] 일 실시예에 따른 암호화 방법은, 전송하기 위한 객체의 일부를 암호화하는 단계와, 난수(random number) 규칙을 이용하여 상기 일부가 암호화된 객체를 셔플링(shuffling)함으로써 암호화된 데이터를 생성하는 단계를 포함한다.

[0008] 상기 암호화하는 단계는, 상기 객체의 일부를 경량 AES(Advanced Encryption Standard) 알고리즘을 통해 암호화하는 단계를 포함할 수 있다.

[0009] 상기 생성하는 단계는, 상기 일부가 암호화된 객체를 복수의 블록으로 분할하는 단계와, 상기 난수 규칙을 생성하는 단계와, 상기 복수의 블록을 상기 난수 규칙에 따라 셔플링하는 단계와, 셔플링된 복수의 블록을 병합하는 단계를 포함할 수 있다.

[0010] 상기 암호화 방법은, 상기 난수 규칙을 암호화하여 상기 암호화된 데이터를 복호화하는 장치로 전송하는 단계를 더 포함할 수 있다.

[0011] 일 실시예에 따른 암호화 방법은, 암호화된 데이터 및 암호화된 난수 규칙을 수신하는 단계와, 상기 암호화된 난수 규칙에 기초하여 상기 암호화된 데이터의 순서를 복원함으로써 데이터를 복원하는 단계를 포함한다.

[0012] 상기 복원하는 단계는, 상기 암호화된 난수 규칙을 복호화하여 난수 규칙을 생성하는 단계와, 상기 난수 규칙을 이용하여 상기 암호화된 데이터의 순서를 복원하는 단계와, 순서가 복원된 암호화된 데이터를 복호화하는 단계를 포함할 수 있다.

[0013] 상기 복호화하는 단계는, 상기 순서가 복원된 암호화된 데이터를 경량 AES(Advanced Encryption Standard) 알고리즘을 통해 복호화하는 단계를 포함할 수 있다.

[0014] 일 실시예에 따른 암호화 장치는, 전송하기 위한 객체를 수신하는 수신기와, 상기 전송하기 위한 객체의 일부를 암호화하고, 난수(random number) 규칙을 이용하여 상기 일부가 암호화된 객체를 셔플링(shuffling)함으로써 암호화된 데이터를 생성하는 컨트롤러를 포함한다.

[0015] 상기 컨트롤러는, 상기 전송하기 위한 객체의 일부를 암호화하는 부분 암호화기와, 상기 난수(random number) 규칙을 이용하여 상기 일부가 암호화된 객체를 셔플링(shuffling)함으로써 상기 암호화된 데이터를 생성하는 암호화 데이터 생성기를 포함할 수 있다.

[0016] 상기 컨트롤러는, 상기 객체의 일부를 경량 AES(Advanced Encryption Standard) 알고리즘을 통해 암호화할 수

있다.

[0017] 상기 암호화 데이터 생성기는, 상기 일부가 암호화된 객체를 복수의 블록으로 분할하고, 상기 난수 규칙을 생성하고, 상기 복수의 블록을 상기 난수 규칙에 따라 셔플링하고, 셔플링된 복수의 블록을 병합할 수 있다.

[0018] 상기 컨트롤러는, 상기 난수 규칙을 암호화하여 상기 암호화된 데이터를 복호화하는 장치로 전송하는 난수 규칙 공유기를 더 포함할 수 있다.

[0019] 일 실시예에 따른 암호화 장치는, 암호화된 데이터 및 암호화된 난수 규칙을 수신하는 수신기와, 상기 암호화된 난수 규칙에 기초하여 상기 암호화된 데이터의 순서를 복원함으로써 데이터를 복원하는 컨트롤러를 포함한다.

[0020] 상기 컨트롤러는, 상기 암호화된 난수 규칙을 복호화하여 난수 규칙을 생성하는 난수 규칙 복호화기와, 상기 난수 규칙을 이용하여 상기 암호화된 데이터의 순서를 복원하는 순서 복원기와, 순서가 복원된 암호화된 데이터를 복호화하는 데이터 복호화기를 포함할 수 있다.

[0021] 상기 컨트롤러는, 상기 순서가 복원된 암호화된 데이터를 경량 AES(Advanced Encryption Standard) 알고리즘을 통해 복호화할 수 있다.

도면의 간단한 설명

[0022] 도 1은 일 실시예에 따른 암호화 장치의 개략적인 블록도를 나타낸다.

도 2는 도 1에 도시된 컨트롤러의 개략적인 블록도를 나타낸다.

도 3은 도 2에 도시된 컨트롤러의 동작의 예시를 나타낸다.

도 4는 도 2에 도시된 암호화 데이터 생성기 및 순서 복원기의 동작의 예시를 나타낸다.

도 5는 도 1에 도시된 컨트롤러가 암호화하는 동작의 순서도를 나타낸다.

도 6은 도 1에 도시된 암호화 장치가 복호화하는 동작의 순서도를 나타낸다.

발명을 실시하기 위한 구체적인 내용

[0023] 본 명세서에 개시되어 있는 본 발명의 개념에 따른 실시예들에 대해서 특정한 구조적 또는 기능적 설명들은 단지 본 발명의 개념에 따른 실시예들을 설명하기 위한 목적으로 예시된 것으로서, 본 발명의 개념에 따른 실시예들은 다양한 형태로 실시될 수 있으며 본 명세서에 설명된 실시예들에 한정되지 않는다.

[0024] 본 발명의 개념에 따른 실시예들은 다양한 변경들을 가할 수 있고 여러 가지 형태들을 가질 수 있으므로 실시예들을 도면에 예시하고 본 명세서에 상세하게 설명하고자 한다. 그러나, 이는 본 발명의 개념에 따른 실시예들을 특정한 개시형태들에 대해 한정하려는 것이 아니며, 본 발명의 사상 및 기술 범위에 포함되는 변경, 균등물, 또는 대체물을 포함한다.

[0025] 제1 또는 제2 등의 용어를 다양한 구성요소들을 설명하는데 사용될 수 있지만, 상기 구성요소들은 상기 용어들에 의해 한정되어서는 안 된다. 상기 용어들은 하나의 구성요소를 다른 구성요소로부터 구별하는 목적으로만, 예를 들어 본 발명의 개념에 따른 권리 범위로부터 이탈되지 않은 채, 제1 구성요소는 제2 구성요소로 명명될 수 있고, 유사하게 제2 구성요소는 제1 구성요소로도 명명될 수 있다.

[0026] 어떤 구성요소가 다른 구성요소에 “연결되어” 있다거나 “접속되어” 있다고 언급된 때에는, 그 다른 구성요소에 직접적으로 연결되어 있거나 또는 접속되어 있을 수도 있지만, 중간에 다른 구성요소가 존재할 수도 있다고 이해되어야 할 것이다. 반면에, 어떤 구성요소가 다른 구성요소에 “직접 연결되어” 있다거나 “직접 접속되어” 있다고 언급된 때에는, 중간에 다른 구성요소가 존재하지 않는 것으로 이해되어야 할 것이다. 구성요소들 간의 관계를 설명하는 표현들, 예를 들어 “~사이에”와 “바로~사이에” 또는 “~에 직접 이웃하는” 등도 마찬가지로 해석되어야 한다.

[0027] 본 명세서에서 사용한 용어는 단지 특정한 실시예들을 설명하기 위해 사용된 것으로, 본 발명을 한정하려는 의도가 아니다. 단수의 표현은 문맥상 명백하게 다르게 뜻하지 않는 한, 복수의 표현을 포함한다. 본 명세서에서, “포함하다” 또는 “가지다” 등의 용어는 설시된 특징, 숫자, 단계, 동작, 구성요소, 부분품 또는 이들을 조합한 것이 존재함으로 지정하려는 것이지, 하나 또는 그 이상의 다른 특징들이나 숫자, 단계, 동작, 구성요소, 부분품 또는 이들을 조합한 것들의 존재 또는 부가 가능성을 미리 배제하지 않는 것으로 이해되어야

한다.

[0028] 다르게 정의되지 않는 한, 기술적이거나 과학적인 용어를 포함해서 여기서 사용되는 모든 용어들은 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 자에 의해 일반적으로 이해되는 것과 동일한 의미를 가진다. 일반적으로 사용되는 사전에 정의되어 있는 것과 같은 용어들은 관련 기술의 문맥상 가지는 의미와 일치하는 의미를 갖는 것으로 해석되어야 하며, 본 명세서에서 명백하게 정의하지 않는 한, 이상적이거나 과도하게 형식적인 의미로 해석되지 않는다.

[0030] 이하, 실시예들을 첨부된 도면을 참조하여 상세하게 설명한다. 그러나, 특허출원의 범위가 이러한 실시예들에 의해 제한되거나 한정되는 것은 아니다. 각 도면에 제시된 동일한 참조 부호는 동일한 부재를 나타낸다.

[0032] 도 1은 일 실시예에 따른 암호화 장치의 개략적인 블록도를 나타낸다.

[0033] 도 1을 참조하면, 암호화 장치(10)는 객체를 수신하고, 수신한 객체를 암호화한다. 암호화 장치(10)는 LPES(Lightweight Partial Encryption and Shuffling) 방법을 이용하여 암호화된 데이터를 생성할 수 있다.

[0034] 암호화 장치(10)가 암호화하는 객체는 사용자와 클라우드 스토리지 서버 간에 주고받는 데이터를 포함할 수 있다. 예를 들어, 객체는 이미지, 텍스트, 동영상, 음악과 같은 전자적 정보를 포함할 수 있다. 전자적 정보는 전송되는 대용량 파일의 형태일 수 있다.

[0035] 암호화 장치(10)는 마더보드(motherboard)와 같은 인쇄 회로 기판(printed circuit board(PCB)), 집적 회로(intergrated circuit(IC)), 또는 SoC(system on chip)로 구현될 수 있다. 예를 들어, 인공 신경망 학습 장치(10)는 애플리케이션 프로세서(application processor)로 구현될 수 있다.

[0036] 암호화 장치(10)는 PC(personal computer), 데이터 서버, 또는 휴대용 장치 내에 구현될 수 있다.

[0037] 휴대용 장치는 랩탑(laptop) 컴퓨터, 이동 전화기, 스마트 폰(smart phone), 태블릿(tablet) PC, 모바일 인터넷 디바이스(mobile internet device(MID)), PDA(personal digital assistant), EDA(enterprise digital assistant), 디지털 스틸 카메라(digital still camera), 디지털 비디오 카메라(digital video camera), PMP(portable multimedia player), PND(personal navigation device 또는 portable navigation device), 휴대용 게임 콘솔(handheld game console), e-북(e-book), 또는 스마트 디바이스(smart device)로 구현될 수 있다. 스마트 디바이스는 스마트 와치(smart watch), 스마트 밴드(smart band), 또는 스마트 링(smart ring)으로 구현될 수 있다.

[0038] 암호화 장치(10)는 대용량 파일에 대하여 경량 AES 알고리즘을 적용한 부분 암호화 및 셔플링(shuffling)을 수행할 수 있다.

[0039] 암호화 장치(10)는 데이터에 대한 암호화 시 발생하는 계산 비용과 자원 소모를 해결하기 위한 방법으로 데이터의 특정 부분만을 선택하여 암호화하는 선택적 암호화를 수행할 수 있다.

[0040] 기존의 선택적 암호화는 파일 포멧에 대한 이해가 필요하고, 파일 포멧 별로 개별적인 암호화를 적용해야 한다는 단점이 있을 수 있다. 그러나, 암호화 장치(10)는 파일 포멧에 관계없이 블록 단위로 부분 암호화를 수행할 수 있다.

[0041] 암호화 장치(10)는 부분 암호화를 적용함으로써 전체 암호 연산의 양을 줄일 수 있다. 부분 암호화를 적용한 후 셔플링을 적용함으로써 추가로 소요되는 연산 비용은 크지 않기 때문에, 암호화 장치(10)는 전체 데이터를 암호화하는 것에 비하여 연산 속도를 향상시킬 수 있다.

[0042] 암호화 장치(10)가 수행하는 암호화 방법은 전체 데이터에 대해 암호화를 적용하는 것에 비해 암호화의 강도는 떨어질 수 있지만, 셔플링을 통해 원본에 대한 순서를 유추하기 어렵게 하여 암호 키와 셔플 규칙을 모르는 사용자가 데이터를 획득하기 어렵게 할 수 있다.

[0043] 암호화 장치(10)는 수신기(100) 및 컨트롤러(200)를 포함할 수 있다.

[0044] 수신기(100)는 전송하기 위한 객체를 수신할 수 있다. 수신기(100)는 암호화된 데이터 및 암호화된 난수(random number) 규칙을 수신할 수 있다.

[0045] 컨트롤러(100)는 전송하기 위한 객체의 일부를 암호화하고, 난수 규칙을 이용하여 상기 일부가 암호화된 객체를 셔플링함으로써 암호화된 데이터를 생성할 수 있다. 또한, 컨트롤러(100)는 암호화된 난수 규칙에 기초하여 암호화된 데이터의 순서를 복원함으로써 데이터를 복원할 수 있다.

[0047] 도 2는 도 1에 도시된 컨트롤러의 개략적인 블록도를 나타내고, 도 3은 도 2에 도시된 컨트롤러의 동작의 예시를 나타낸다.

[0048] 도 2 및 도 3을 참조하면, 컨트롤러(200)는 부분 암호화기(210), 암호화 데이터 생성기(220), 난수 규칙 공유기(230), 난수 규칙 복호화기(240), 순서 복원기(250) 및 데이터 복호화기(260)을 포함할 수 있다.

[0049] 부분 암호화기(210)는 전송하기 위한 객체의 일부를 암호화할 수 있다. 또한, 부분 암호화기(210)는 객체를 분할하여 분할된 객체의 일부만을 암호화할 수도 있다.

[0050] 예를 들어, 도 3과 같이 객체가 파일인 경우에 부분 암호화기(210)는 객체를 복수의 파트로 분할할 수 있다. 이 때, 분할의 단위는 128 bit 일 수 있다.

[0051] 부분 암호화기(210)는 객체의 일부를 경량 AES(Advanced Encryption Standard) 알고리즘을 통해 암호화할 수 있다. 예를 들어, 부분 암호화기(210)는 el-AES를 사용하여 객체를 암호화함으로써, 암호화 속도를 향상시킬 수 있다.

[0052] eL-AES 알고리즘은 AES-256 알고리즘을 변형한 것으로 2 개의 애드 라운드 키(AddRoundKey)를 사용하도록 내부 함수의 구조를 변한 것일 수 있다.

[0053] eL-AES 알고리즘은 라운드 당 256 bit의 키를 사용하여 키 스케쥴(key schedule)의 반복 횟수를 늘릴 수 있다. eL-AES 알고리즘은 라운드의 수를 7회로 축소하여도 AES-256과 키 스케쥴의 반복 횟수가 같아서 릴레이티드 키(related-key) 공격에 대하여 동일한 보안성을 가질 수 있다.

[0054] eL-AES 알고리즘은 AES-256에 비해서 낮은 시간 복잡도를 가진다는 측면에서 보안성이 낮을 수 있으나, 10 라운드를 거치는 AES-128과 비교하면 256bit의 키 사용을 통해 보다 높은 시간 복잡도를 가질 수 있어 키 획득에 대한 보안성이 높을 수 있다. 또한, eL-AES 알고리즘은 AES-129보다 적은 라운드를 돌면서 보다 높은 키 획득 시간 복잡도를 가지므로, 처리 속도를 향상시킬 수 있는 동시에 암호화된 부분에 대한 유추를 더욱 어렵게 할 수 있다.

[0055] 부분 암호화기(210)는 암호화 알고리즘에 따라 적절한 분할 단위로 분할하여 객체의 일부만을 암호화할 수 있다.

[0056] 예를 들어, 부분 암호화기(210)가 eL-AES 알고리즘을 사용할 경우에, eL-AES 알고리즘은 256 bit의 키(key)를 사용하므로, 256 bit의 배수 단위로 분할 단위를 정할 수 있다. 부분 암호화기(210)는 분할 단위의 1/4 크기만큼 블록의 시작과 끝부분을 eL-AES로 암호화시킬 수 있다.

[0057] 도 3의 예시와 같이 분할 단위를 128bit로 정하여 분할한 경우에, 부분 암호화기(210)는 복수의 파트 각각의 시작 부분의 32bit 및 끝 부분의 32bit를 암호화할 수 있다.

[0058] 분할 단위가 크면 암호화되지 않는 부분이 늘어나는 문제가 있고, 분할 단위가 너무 작으면 암호화 연산이 지나치게 많아지는 문제가 발생할 수 있다.

[0059] 암호화 데이터 생성기(220)는 난수 규칙을 이용하여 상기 일부가 암호화된 객체를 셔플링함으로써 암호화된 데이터를 생성할 수 있다.

[0060] 암호화 데이터 생성기(220)는 일부가 암호화된 객체를 복수의 블록으로 분할하고, 난수 규칙을 생성할 수 있다. 암호화 데이터 생성기(220)는 복수의 블록을 난수 규칙에 따라 셔플링하고, 셔플링된 복수의 블록을 병합할 수 있다.

[0061] 암호화 데이터 생성기(220)는 부분 암호화기(210)가 분할한 분할 단위를 단위 블록으로 사용하여 분할을 수행할 수 있다. 암호화 데이터 생성기(220)가 복수의 블록을 셔플링하는 동작은 도 4를 참조하여 자세하게 설명할 것이다.

[0062] 도 3의 예시와 같이 암호화 데이터 생성기(220)는 각각의 파트로 분할된 후도 3의 일부가 암호화된 블록을 셔플

링함으로써, Part A*, Part B* 등의 새로운 순서를 가진 복수의 블록들을 생성할 수 있다. 암호화 데이터 생성기(220)는 새로운 순서를 가진 복수의 블록들을 병합하여 암호화된 파일(File*)를 생성할 수 있다.

[0063] 난수 규칙 공유기(230)는 난수 규칙을 암호화하여 암호화된 데이터를 복호화하는 장치로 전송할 수 있다. 난수 규칙 공유기(230)는 암호화된 데이터를 수신할 장치에 암호화된 데이터를 전송하기 전에 사전 공유할 수 있다.

[0064] 예를 들어, 난수 규칙 공유기(230)는 AES-256와 같은 알고리즘을 사용하여 난수 규칙을 암호화할 수 있다. 난수 규칙 공유기(230)가 전송하는 암호화된 난수 규칙은 셔플링의 비밀키 역할을 할 수 있다.

[0065] 난수 규칙 복호화기(240)는 암호화된 난수 규칙을 복호화하여 난수 규칙을 생성할 수 있다. 난수 규칙 복호화기(240)가 생성한 난수 규칙은 암호화 데이터 생성기(220)가 암호화 데이터를 생성하는데 사용한 난수 규칙과 동일할 수 있다.

[0066] 예를 들어, 난수 규칙 복호화기(240)는 AES-256 알고리즘을 사용하여 난수 규칙을 복호화할 수 있다. 난수 규칙 복호화기(240)는 생성한 난수 규칙을 순서 복원기(250)로 출력할 수 있다.

[0067] 순서 복원기(250)는 난수 규칙을 이용하여 상기 암호화된 데이터의 순서를 복원할 수 있다. 순서 복원기(250)는 난수 규칙을 이용하여 셔플링에 의해 암호화된 데이터의 순서를 원래의 순서로 복원할 수 있다. 원래의 순서로 복원된 암호화된 데이터는 부분 암호화기(210)가 일부를 암호화한 객체와 동일할 수 있다.

[0068] 데이터 복호화기(260)는 순서가 복원된 암호화된 데이터를 복호화할 수 있다. 데이터 복호화기(260)는 부분 암호화기(210)가 객체의 일부를 암호화하기 위해 사용한 알고리즘과 동일한 알고리즘을 사용하여 순서를 복원한 암호화된 데이터를 복호화할 수 있다.

[0069] 데이터 복호화기(260)는 순서가 복원된 암호화된 데이터를 경량 AES(Advanced Encryption Standard) 알고리즘을 통해 복호화할 수 있다. 예를 들어, 데이터 복호화기(260)는 eL-AES 알고리즘을 사용하여 순서가 복원된 암호화된 데이터를 복호화할 수 있다.

[0071] 도 4는 도 2에 도시된 암호화 데이터 생성기 및 순서 복원기의 동작의 예시를 나타낸다.

[0072] 도 4를 참조하면, 암호화 데이터 생성기(220)는 클라우드 스토리지 시스템에 전송하는 데이터의 보안 강도를 더욱 높이기 위하여 셔플링 기법을 사용할 수 있다.

[0073] 암호화 데이터 생성기(220)는 부분 암호화기(210)에서 부분 암호화를 위하여 사용한 분할 단위 또는 그 배수를 단위로 셔플링을 수행할 수 있다. 암호화 데이터 생성기(220)가 지나치게 큰 배수를 사용할 경우 연속적인 블록이 늘어남에 따라 셔플링의 효과가 감소할 수 있다.

[0074] 암호화 데이터 생성기(220)는 사전 공유된 셔플 규칙에 따라 셔플링을 수행할 수 있다. 셔플 규칙은 난수 규칙을 포함할 수 있다.

[0075] 예를 들어, 부분 암호화기(210)는 하나의 객체를 7개의 블록으로 분할하고, 각각의 블록의 시작 부분과 끝부분의 일부를 암호화하여 암호화 데이터 생성기(220)로 출력할 수 있다. 도 4의 로우 데이터(raw data)는 암호화되지 않은 부분을 의미할 수 있다. 암호화 데이터 생성기(220)는 부분 암호화기(210)가 분할한 분할 단위를 블록으로 사용하여 분할을 수행할 수 있다.

[0076] 암호화 데이터 생성기(220)는 난수 규칙을 사용하여 셔플링을 수행할 수 있다. 암호화 데이터 생성기(220)는 암호화된 데이터를 전송하는 순간 랜덤하게 규칙을 생성할 수 있다. 예를 들어, 암호화 데이터 생성기(220)는 일정 범위 내의 연속된 숫자로 난수 규칙을 생성할 수 있다.

[0077] 예를 들어, 암호화 데이터 생성기(220)는 생성한 난수 규칙에 따라 도 4에 나타난 화살표방향으로 복수의 블록을 셔플링할 수 있다. 셔플링의 경우의 수는 n개의 블록에 대하여 n!을 가질 수 있다. 이 때, 단일 셔플링 단위의 용량은 (n!×128) byte를 가질 수 있다.

[0078] 예를 들어, n이 12일 경우, 셔플링의 경우의 수는 약 57 GB 이고, 총 데이터(용량 N)는 $(57\times1024^3)\times(N/1536)=39916800\times N$ byte일 수 있고, 모든 경우에 수에 따라 데이터를 생성하는 것은 공격자에게 매우 부담스러울 수 있다.

[0079] 12개의 블록을 분할하여 셔플링 하는 경우, 전체 경우의 수에 대한 조합으로 생성되는 용량은 원본 데이터에 비

하여 약 4000만 배 증가할 수 있다. 공격자가 암호화된 데이터를 복원하기 위해서는 약 4억 8천(12!) 개의 경우의 수에 해당하는 조합을 풀어야 하며, 원래 데이터의 조합을 알아내더라도 원본 객체를 복원하기 위해서 부분 암호화기(210)가 사용한 암호화 알고리즘의 시간 복잡도를 해결해야 할 수 있다.

[0080] 순서 복원기(250)는 셔플 규칙의 역순에 따라 셔플링 되어있는 암호화된 데이터를 복원할 수 있다. 도 4의 셔플 규칙은 난수 규칙 복호화기(240)가 생성한 난수 규칙을 포함할 수 있다. 예를 들어, 난수 규칙 복원기(250)는 도 4의 화살표와 같이 난수 규칙에 따라 암호화된 데이터의 순서를 원래의 순서로 복원할 수 있다.

[0082] 도 5는 도 1에 도시된 컨트롤러가 암호화하는 동작의 순서도를 나타낸다.

[0083] 도 5를 참조하면, 부분 암호화기(210)는 전송하기 위한 객체의 일부를 암호화할 수 있다(S510). 부분 암호화기(210)는 객체를 분할하여 분할된 객체의 일부만을 암호화할 수 있고, 객체의 일부를 암호화한 후 분할할 수도 있다. 부분 암호화기(210)는 암호화 알고리즘의 종류에 따라 상이한 분할 단위를 사용하여 객체를 분할할 수 있다.

[0084] 암호화 데이터 생성기(220)는 난수 규칙을 이용하여 일부가 암호화된 객체를 셔플링함으로써 암호화된 데이터를 생성할 수 있다(S530). 암호화 데이터 생성기(220)는 일부가 암호화된 객체를 복수의 블록으로 분할한 후 셔플링할 수 있다. 암호화 데이터 생성기(220)는 부분 암호화기(210)가 사용한 분할 단위와 동일한 분할 단위로 복수의 블록을 생성할 수 있다. 암호화 데이터 생성기(220)는 중복되지 않고, 연속된 난수를 사용하여 셔플링을 수행할 수 있다.

[0085] 난수 규칙 공유기(230)는 난수 규칙을 암호화하여 수신기로 전송할 수 있다(S550). 수신기는 암호화된 데이터를 복호화하기 위한 장치의 수신기를 의미할 수 있다. 난수 규칙 공유기(230)는 암호화된 데이터를 생성하기 전에 클라우드 및 복호화를 수행할 장치와 난수 규칙을 공유할 수 있다.

[0087] 도 6은 도 1에 도시된 암호화 장치가 복호화하는 동작의 순서도를 나타낸다.

[0088] 도 6을 참조하면, 수신기(100)는 암호화된 데이터 및 암호화된 난수 규칙을 수신할 수 있다(S610). 수신기(100)는 복호화를 수행할 장치 또는 클라우드 스토리지 상에 포함될 수 있다. 암호화된 데이터는 암호화 장치(10)가 클라우드 스토리지를 통하여 전송한 데이터를 의미할 수 있다.

[0089] 컨트롤러(200)는 암호화된 난수 규칙에 기초하여 암호화된 데이터의 순서를 복원함으로써 데이터를 복원할 수 있다(S630).

[0090] 난수 규칙 복호화기(240)는 암호화된 난수 규칙을 복호화할 수 있다. 난수 규칙 복호화기(240)가 복호화에 사용하는 알고리즘은 난수 규칙 공유기(230)가 난수 규칙을 암호화하는데 사용한 알고리즘과 동일한 알고리즘일 수 있다.

[0091] 순서 복원기(250)는 복호화한 난수 규칙을 이용하여 암호화된 데이터의 순서를 복원할 수 있다. 순서 복원기(250)는 암호화 데이터 생성기(220)가 셔플링의 역순으로 암호화된 데이터의 순서를 복원할 수 있다. 순서가 복원된 암호화된 데이터는 부분 암호화기(210)에서 일부를 암호화한 객체와 동일할 수 있다.

[0092] 데이터 복호화기(260)는 순서가 복원된 암호화된 데이터를 복호화할 수 있다. 즉, 데이터 복호화기(260)는 암호화된 객체의 일부를 복호화하여 원래의 객체를 획득할 수 있다.

[0094] 이상에서 설명된 장치는 하드웨어 구성요소, 소프트웨어 구성요소, 및/또는 하드웨어 구성요소 및 소프트웨어 구성요소의 조합으로 구현될 수 있다. 예를 들어, 실시예들에서 설명된 장치 및 구성요소는, 예를 들어, 프로세서, 컨트롤러, ALU(arithmetic logic unit), 디지털 신호 프로세서(digital signal processor), 마이크로컴퓨터, FPGA(field programmable gate array), PLU(programmable logic unit), 마이크로프로세서, 또는 명령(instruction)을 실행하고 응답할 수 있는 다른 어떠한 장치와 같이, 하나 이상의 범용 컴퓨터 또는 특수 목적 컴퓨터를 이용하여 구현될 수 있다. 처리 장치는 운영 체제(OS) 및 상기 운영 체제 상에서 수행되는 하나 이상의 소프트웨어 애플리케이션을 수행할 수 있다. 또한, 처리 장치는 소프트웨어의 실행에 응답하여, 데이터를 접근, 저장, 조작, 처리 및 생성할 수도 있다. 이해의 편의를 위하여, 처리 장치는 하나가 사용되는 것으로 설

명된 경우도 있지만, 해당 기술분야에서 통상의 지식을 가진 자는, 처리 장치가 복수 개의 처리 요소(processing element) 및/또는 복수 유형의 처리 요소를 포함할 수 있음을 알 수 있다. 예를 들어, 처리 장치는 복수 개의 프로세서 또는 하나의 프로세서 및 하나의 컨트롤러를 포함할 수 있다. 또한, 병렬 프로세서(parallel processor)와 같은, 다른 처리 구성(processing configuration)도 가능하다.

[0095] 소프트웨어는 컴퓨터 프로그램(computer program), 코드(code), 명령(instruction), 또는 이들 중 하나 이상의 조합을 포함할 수 있으며, 원하는 대로 동작하도록 처리 장치를 구성하거나 독립적으로 또는 결합적으로(collectively) 처리 장치를 명령할 수 있다. 소프트웨어 및/또는 데이터는, 처리 장치에 의하여 해석되거나 처리 장치에 명령 또는 데이터를 제공하기 위하여, 어떤 유형의 기계, 구성요소(component), 물리적 장치, 가상 장치(virtual equipment), 컴퓨터 저장 매체 또는 장치, 또는 전송되는 신호 파(signal wave)에 영구적으로, 또는 일시적으로 구체화(embody)될 수 있다. 소프트웨어는 네트워크로 연결된 컴퓨터 시스템 상에 분산되어서, 분산된 방법으로 저장되거나 실행될 수도 있다. 소프트웨어 및 데이터는 하나 이상의 컴퓨터 판독 가능 기록 매체에 저장될 수 있다.

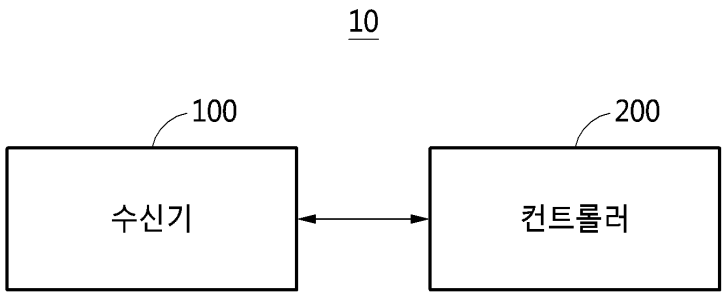
[0096] 실시예에 따른 방법은 다양한 컴퓨터 수단을 통하여 수행될 수 있는 프로그램 명령 형태로 구현되어 컴퓨터 판독 가능 매체에 기록될 수 있다. 상기 컴퓨터 판독 가능 매체는 프로그램 명령, 데이터 파일, 데이터 구조 등을 단독으로 또는 조합하여 포함할 수 있다. 상기 매체에 기록되는 프로그램 명령은 실시예를 위하여 특별히 설계되고 구성된 것들이거나 컴퓨터 소프트웨어 당업자에게 공지되어 사용 가능한 것일 수도 있다. 컴퓨터 판독 가능 기록 매체의 예에는 하드 디스크, 플로피 디스크 및 자기 테이프와 같은 자기 매체(magnetic media), CD-ROM, DVD와 같은 광기록 매체(optical media), 플롭티컬 디스크(floptical disk)와 같은 자기-광 매체(magneto-optical media), 및 롬(ROM), 램(RAM), 플래시 메모리 등과 같은 프로그램 명령을 저장하고 수행하도록 특별히 구성된 하드웨어 장치가 포함된다. 프로그램 명령의 예에는 컴파일러에 의해 만들어지는 것과 같은 기계어 코드뿐만 아니라 인터프리터 등을 사용해서 컴퓨터에 의해서 실행될 수 있는 고급 언어 코드를 포함한다. 상기된 하드웨어 장치는 실시예의 동작을 수행하기 위해 하나 이상의 소프트웨어 모듈로서 작동하도록 구성될 수 있으며, 그 역도 마찬가지이다.

[0097] 이상과 같이 실시예들이 비록 한정된 실시예와 도면에 의해 설명되었으나, 해당 기술분야에서 통상의 지식을 가진 자라면 상기의 기재로부터 다양한 수정 및 변형이 가능하다. 예를 들어, 설명된 기술들이 설명된 방법과 다른 순서로 수행되거나, 및/또는 설명된 시스템, 구조, 장치, 회로 등의 구성요소들이 설명된 방법과 다른 형태로 결합 또는 조합되거나, 다른 구성요소 또는 균등물에 의하여 대치되거나 치환되더라도 적절한 결과가 달성될 수 있다.

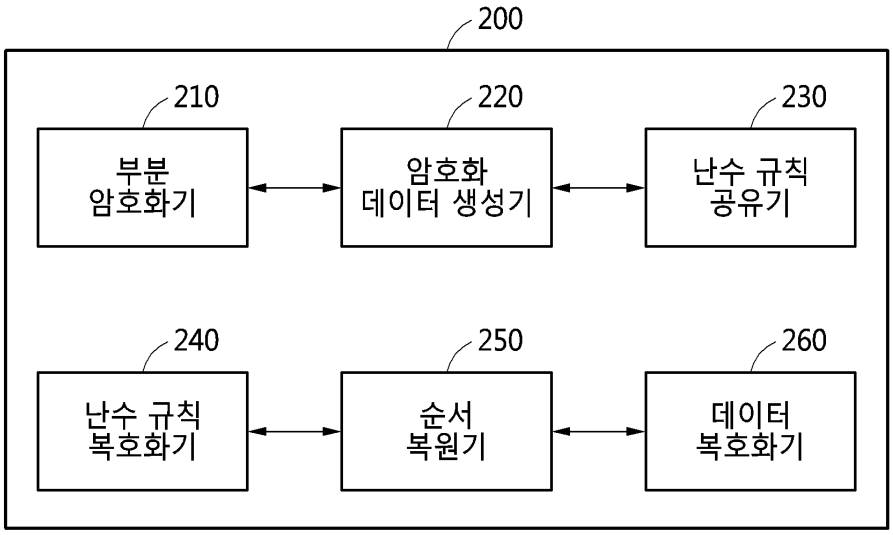
[0098] 그러므로, 다른 구현들, 다른 실시예들 및 특허청구범위와 균등한 것들도 후술하는 특허청구범위의 범위에 속한다.

도면

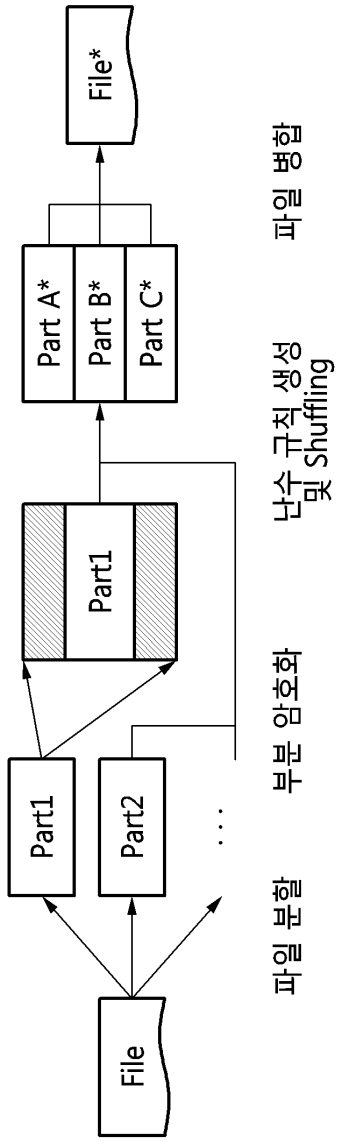
도면1



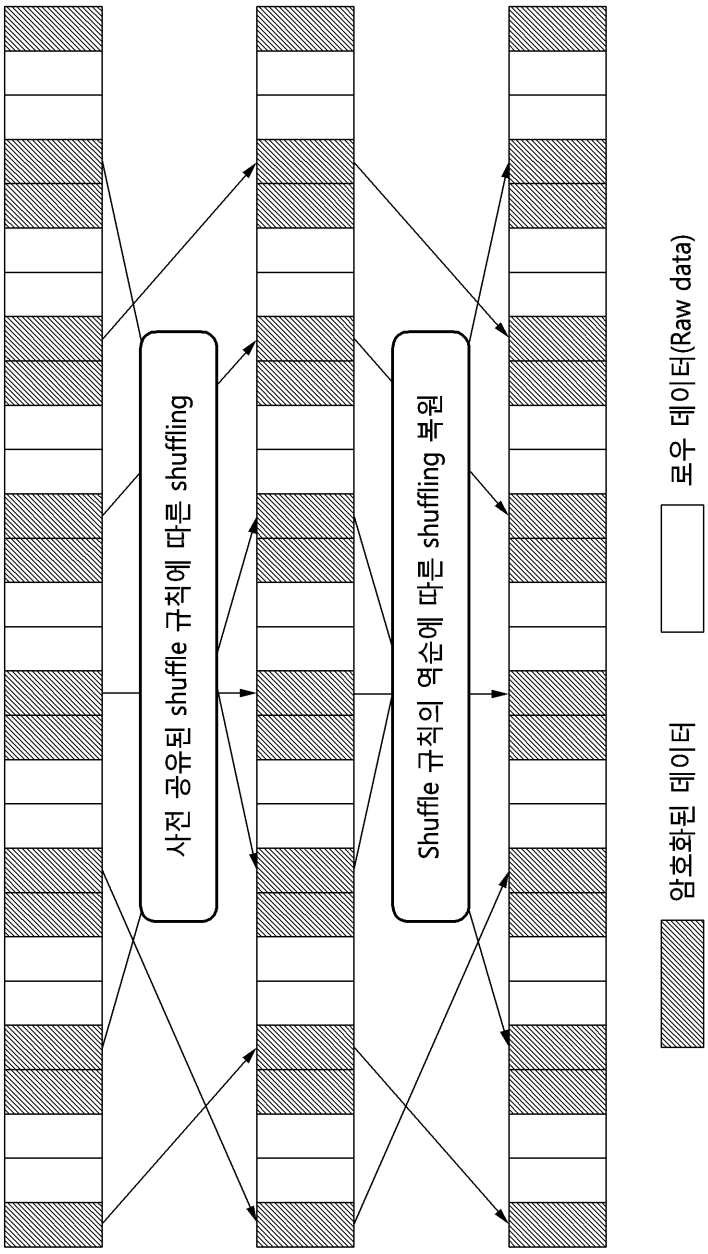
도면2


200
210
부분
암호화기
220
암호화
데이터 생성기
230
난수 규칙
공유기
240
난수 규칙
복호화기
250
순서
복원기
260
데이터
복호화기

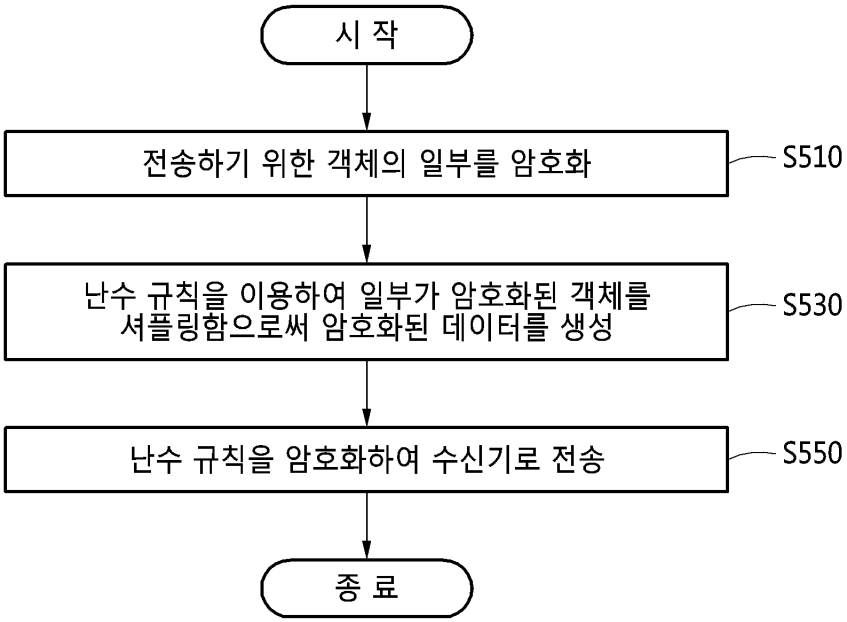
도면3


File
Part1
Part2
...
Part1
Part A*
Part B*
Part C*
File*
파일 분할
부분 암호화
난수 규칙 생성
및 Shuffling
파일 병합

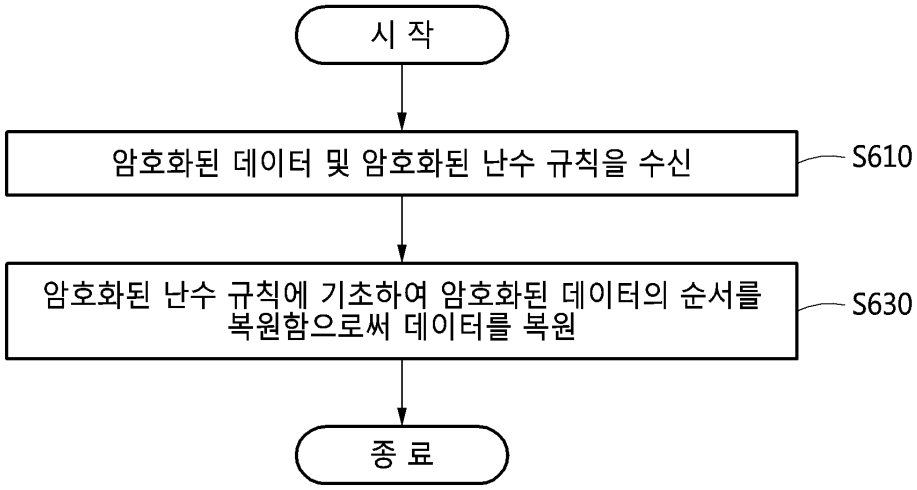
도면4


사전 공유된 shuffle 규칙에 따른 shuffling
Shuffle 규칙의 역순에 따른 shuffling 복원
암호화된 데이터
로우 데이터(Raw data)

도면5


시 작
전송하기 위한 객체의 일부를 암호화
S510
난수 규칙을 이용하여 일부가 암호화된 객체를 셔플링함으로써 암호화된 데이터를 생성
S530
난수 규칙을 암호화하여 수신기로 전송
S550
종 료

도면6


시 작
암호화된 데이터 및 암호화된 난수 규칙을 수신
S610
암호화된 난수 규칙에 기초하여 암호화된 데이터의 순서를 복원함으로써 데이터를 복원
S630
종 료