(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2008년04월21일
(11) 등록번호 10-0823736
(24) 등록일자 2008년04월14일

(51) Int. Cl.
G06F 15/00 (2006.01)
(21) 출원번호 10-2006-0094953
(22) 출원일자 2006년09월28일
심사청구일자 2006년09월28일
(65) 공개번호 10-2008-0029200
(43) 공개일자 2008년04월03일
(56) 선행기술조사문헌
JP2002152246 A
(뒷면에 계속)

(73) 특허권자
한국전자통신연구원
대전 유성구 가정동 161번지
(72) 발명자
조상래
대전 서구 월평3동 진달래아파트 103동 1505호
진승헌
대전 서구 월평2동 백합아파트 104-1405
(뒷면에 계속)
(74) 대리인
특허법인 씨엔에스 · 로고스

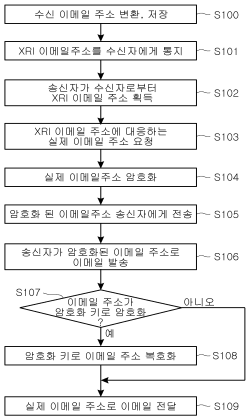
전체 청구항 수 : 총 9 항 심사관 : 이준석

(54) XRI기반의 익명성 보장 방법 및 이를 위한 장치

(57) 요 약

본 발명은 XRI(eXtensible Resource Identifier) 기반의 익명성 보장 방법 및 이를 위한 장치에 관한 것으로서, 이메일 주소가 알려진 사용자가 스팸 메일의 표적이 되는 것을 방지하기 위하여, 이메일 수신자로부터 수신 이메일 주소를 제공받아 XRI 이메일 주소로 변환하여 저장한 다음, 변환된 XRI 이메일 주소를 상기 이메일 수신자에게 통지하고, 이메일 수신자에게서 획득한 상기 변환된 XRI 이메일 주소를 수신처로 하여 이메일을 발송하는 이메일 송신자로부터, 상기 변환된 XRI 이메일 주소에 대응되는 실제 이메일 주소를 요청받는 다음, 상기 이메일 수신자의 변환된 XRI 이메일 주소에 대응되는 실제 수신 이메일 주소를 저장된 암호화키를 이용하여 암호화한 후 이메일 송신자에게 전송하고, 상기 암호화된 수신 이메일 주소로 이메일이 전송되면 상기 암호화된 수신 이메일 주소가 실제 수신 이메일 주소로 복호화 되도록, 상기에서 사용된 암호화키에 관한 정보를 상기 복호화를 행하는 장치에게 제공한다.

대표도 - 도1



(72) 발명자

조영섭

대전 유성구 관평동 672 대덕테크노밸리아파트 604-1702

최대선

대전 서구 월평3동 누리아파트 108-1101

노종혁

대전 유성구 반석동 양지마을아파트 203-1804

김승현

대구 달서구 도원동 1439 가람마을아파트 105동 804호

정교일

대전 유성구 신성동 삼성한울아파트 107-1102

(56) 선행기술조사문헌

JP2005026963 A

JP2005326932 A

KR1020040082155 A

KR1020050063208 A

특허청구의 범위

청구항 1

이메일 수신자로부터 수신 이메일 주소를 제공받아 XRI 이메일 주소로 변환하여 저장한 다음, 변환된 XRI 이메일 주소를 상기 이메일 수신자에게 통지하는 제 1단계;

이메일 수신자에게서 획득한 상기 변환된 XRI 이메일 주소를 수신처로 하여 이메일을 발송하는 이메일 송신자로부터, 상기 변환된 XRI 이메일 주소에 대응되는 실제 이메일 주소를 요청받는 제 2단계;

상기 이메일 수신자의 변환된 XRI 이메일 주소에 대응되는 실제 수신 이메일 주소를 저장된 암호화키를 이용하여 암호화한 후 이메일 송신자에게 전송하는 제 3단계; 및,

상기 암호화된 수신 이메일 주소로 이메일이 전송되면 상기 암호화된 수신 이메일 주소가 실제 수신 이메일 주소로 복호화 되도록, 상기 제 3단계에서 사용된 암호화키에 관한 정보를 상기 복호화를 행하는 장치에게 제공하는 제 4단계를 포함하는 XRI(eXtensible Resource Identifier) 기반의 익명성 보장 방법.

청구항 2

제 1항에 있어서,

상기 암호화키는 일회용 패스워드(암호화키: One Time Password)인 것을 특징으로 하는 XRI 기반의 익명성 보장 방법.

청구항 3

제 1항 또는 제 2항에 있어서,

상기 제 3단계에서 암호화키를 이용하여 이메일 수신자의 XRI 이메일 주소에 대응되는 실제 수신 이메일 주소를 암호화하기 전에, 상기 암호화키를 초기화 셋업하는 단계를 더 포함하는 것을 특징으로 하는 XRI 기반의 익명성 보장 방법.

청구항 4

제 1항 또는 제 2항에 있어서,

제 4단계에서 제공되는 암호화키에 관한 정보는,

상기 수신 이메일 주소를 암호화 하는 과정과 상기 암호화된 수신 이메일 주소를 실제 수신 이메일 주소로 복호화하는 과정간의 동기화를 위한 시간 정보; 및,

상기 암호화에 사용되는 암호화키를 생성할 수 있는 난수 생성기에 사용되는 시드인 것을 특징으로 하는 XRI 기반의 익명성 보장 방법.

청구항 5

수신 이메일 주소를 암호화하는데 사용되는 암호화키를 생성하는 암호화키 생성 모듈;

익명성 보장 서버의 외부에 존재하면서 익명성 보장 서버에 의하여 암호화된 수신 이메일 주소를 복호화하는 장치와 암호화키에 관한 정보를 동기화하고, 관리하며, 생성된 암호화키를 저장하고 관리하는 암호화키 관리 모듈;

상기 수신 이메일 주소를 복호화하는 장치로부터 암호화키 초기화 요청이 있으면, 상기 암호화키 초기화를 위한 작업을 제어하는 암호화키 초기화 요청 제어 모듈;

암호화키를 이용하여 실제 이메일 주소가 익명성을 갖도록 암호화하는 수신 이메일 주소 암호화 모듈; 및,

이전에 암호화된 이메일 주소들을 관리하고 상기 수신 이메일 주소 암호화 모듈에서 암호화된 이메일 주소가 이전에 암호화된 이메일 주소들과 중복되지 않도록 관리하는 암호화된 이메일 주소 관리 모듈을 포함하여 구성되는 익명성 보장 서버.

청구항 6

제 5항에 있어서,

상기 암호화키는 일회용 패스워드(암호화키: One Time Password)인 것을 특징으로 하는 익명성 보장 서버.

청구항 7

제 5항에 있어서,

상기 암호화키 생성 모듈은 암호화키에 해당하는 난수를 생성하는 난수 생성기를 포함하는 것을 특징으로 하는 익명성 보장 서버.

청구항 8

제 5항에 있어서,

상기 암호화키 관리 모듈이 관리하는 암호화키에 관한 정보는 익명성 보장 서버와 익명성 보장 서버의 외부에 존재하면서 익명성 보장 서버에 의하여 암호화된 수신 이메일 주소를 복호화하는 장치의 시간을 동기화 하기 위한 시간 정보; 및,

암호화키를 생성하는데 필요한 시드 정보인 것을 특징으로 하는 익명성 보장 서버.

청구항 9

수신 이메일 주소를 암호화하는 장치와 암호화키를 동기화하기 위하여 상기 이메일 주소를 암호화하는 장치에게 암호화키 초기화를 요청하고, 이에 대한 응답으로 상기 장치로부터 초기화된 암호화키에 관한 정보를 전달받아 처리하는 암호화키 초기화요청 및 응답 처리 모듈;

상기 초기화된 암호화키에 관한 정보에 기초하여 암호화키를 생성하는 암호화키 생성 모듈;

상기 암호화키 생성 모듈에서 생성된 암호화키를 저장하고 관리하는 암호화키 관리 모듈; 및,

이메일이 착신되면 수신 이메일 주소가 상기 암호화키 관리 모듈에 저장되어 있는 암호화키로 암호화되어 있는 이메일을 선별한 다음, 상기 이메일이 수신자에게 전달될 수 있도록 상기 암호화키를 이용하여 상기 암호화된 수신 이메일 주소를 원래 수신 이메일 주소를 복호화하는 이메일 주소 복호화 모듈을 포함하여 구성되는 수신 이메일 주소 복호화기.

명 세 서

발명의 상세한 설명

발명의 목적

발명이 속하는 기술 및 그 분야의 종래기술

<5> 본 발명은 이메일 주소가 알려진 사용자가 스팸 메일의 표적이 되는 것을 방지하기 위하여 XRI 기반의 익명성 보장 방법 및 이를 위한 장치에 관한 것이다.

<6> 인터넷 서비스 환경의 고도화에 따라 데이터를 융합하여 새로운 가치를 제공하는 매쉬업(mash-up) 서비스가 출현하여 증가 추세에 있으며, 현재 이러한 서비스는 일부 포털에서 제공하는 전용 API를 통하여 시범적으로 운영되고 있다. 그러나 해당 도메인에 국한된 조직중심의 식별, 인증, 공유 기술을 기반으로 하고 있어, 도메인을 넘어서는 사용자의 동적인 신뢰관계를 요구하는 매쉬업 서비스에 적용되기에는 한계가 있다. 멀티도메인 환경에서 데이터를 공유하기 위해 다른 도메인의 사용자와 공유대상을 유일하게 식별하는 기술이 요청된다.

<7> 이에 OASIS(Organization for the Advancement of Structured Information Standards)는 기존 인터넷 주소(URL) 시스템의 성능을 향상시켜주는 표준으로 XRI(eXtensible Resource Identifier)를 제안하였다. 이것은 네트워크에 연결된 서버 등 시스템의 URL을 연계시키지 않고도 데이터를 전송하거나 배치, 검색하는 기술을 제공한다.

<8> XRI는 상이한 도메인이나 애플리케이션, 프로토콜을 갖는 웹 서비스간 파일 데이터를 확인해주는 기술이며, 네트워크상에서 시스템의 정확한 출처를 몰라도 데이터를 시스템의 디렉터리로 전송할 수 있도록 해주는 추상화

(abstract) 기술로, 동일한 데이터가 다른 URL(Uniform Resource Location)을 갖는 시스템에 저장돼 있어도 이용자가 별도의 부가적인 작업 없이 데이터를 손쉽게 이용할 수 있다. 즉 이것은 추상화된 식별자들을 위한 표준화된 문법과 협상 프로토콜을 제공한다. XRI는 기존의 URI(Uniform Resource Identifier)와 IRI(Internationalized Resource Identifier)에 문법과 협상 프로토콜을 확장하여 디지털 ID의 관리와 보호 측면을 강화하는 보다 추상적이며 규모의 확장성에 초점을 맞추고 있다.

<9> XRI는 기본적으로 URI 체계 위에 구성된다. 따라서 XRI로 표현되는 식별자는 실제 사용되기 위해서는 연결되는 URI로 변화하는 XRI 변환(resolution) 과정을 거친다. 이러한 XRI의 특성을 이용하여 원천적으로 스팸메일 방지 효과를 볼 수 있다.

<10> 하지만 이메일 송신자가 실제 이메일을 송신하기 위해서는 수신자의 이메일 주소를 가져오는데 이 경우 송신자가 제 3의 객체에게 사용자의 이메일을 유출한다면 사용자에게 스팸으로 돌아오는 문제가 발생한다. 따라서 실제 신뢰할 수 있는 이메일 송신자에게 이메일을 알려 줄 때 익명성을 가지는 이메일 주소를 알려줄 필요가 발생한다.

발명이 이루고자 하는 기술적 과제

<11> 본 발명은 상술한 바와 같은 문제점을 해결하기 위하여, 사용자의 이메일 주소를 SMTP(Simple Mail Transfer Protocol) 서버의 개입 없이 암호 기술을 이용하여 익명으로 제공하므로써, 이메일 주소가 공개되더라도 상기 이메일 사용자에게 무차별적으로 송신되는 스팸메일을 방지할 수 있는 방법 및 장치를 제공하는 것을 목적으로 한다.

발명의 구성 및 작용

<12> 상기한 목적을 실현하기 위한 본 발명의 일 실시예에 따른 XRI(eXtensible Resource Identifier) 기반의 익명성 보장 방법은,

<13> 이메일 수신자로부터 수신 이메일 주소를 제공받아 XRI 이메일 주소로 변환하여 저장한 다음, 변환된 XRI 이메일 주소를 상기 이메일 수신자에게 통지하는 제 1단계;

<14> 이메일 수신자에게서 획득한 상기 변환된 XRI 이메일 주소를 수신처로 하여 이메일을 발송하는 이메일 송신자로부터, 상기 변환된 XRI 이메일 주소에 대응되는 실제 이메일 주소를 요청받는 제 2단계;

<15> 상기 이메일 수신자의 변환된 XRI 이메일 주소에 대응되는 실제 수신 이메일 주소를 저장된 암호화키를 이용하여 암호화한 후 이메일 송신자에게 전송하는 제 3단계; 및,

<16> 상기 암호화된 수신 이메일 주소로 이메일이 전송되면 상기 암호화된 수신 이메일 주소가 실제 수신 이메일 주소로 복호화 되도록, 상기 제 3단계에서 사용된 암호화키에 관한 정보를 상기 복호화를 행하는 장치에게 제공하는 제 4단계를 포함한다.

<17> 본 발명의 또 다른 실시예에 따른 익명성 보장 서버는,

<18> 수신 이메일 주소를 암호화하는데 사용되는 암호화키를 생성하는 암호화키 생성 모듈;

<19> 익명성 보장 서버의 외부에 존재하면서 익명성 보장 서버에 의하여 암호화된 수신 이메일 주소를 복호화하는 장치와 암호화키에 관한 정보를 동기화하고, 관리하며, 생성된 암호화키를 저장하고 관리하는 암호화키 관리 모듈;

<20> 상기 수신 이메일 주소를 복호화하는 장치로부터 암호화키 초기화 요청이 있으면, 상기 암호화키 초기화를 위한 작업을 제어하는 암호화키 초기화 요청 제어 모듈;

<21> 암호화키를 이용하여 실제 이메일 주소가 익명성을 갖도록 암호화하는 수신 이메일 주소 암호화 모듈; 및,

<22> 이전에 암호화된 이메일 주소들을 관리하고 상기 수신 이메일 주소 암호화 모듈에서 암호화된 이메일 주소가 이전에 암호화된 이메일 주소들과 중복되지 않도록 관리하는 암호화된 이메일 주소 관리 모듈을 포함하여 구성된다.

<23> 본 발명의 또 다른 실시예에 따른 수신 이메일 주소 복호화기는,

<24> 수신 이메일 주소를 암호화하는 장치와 암호화키를 동기화하기 위하여 상기 이메일 주소를 암호화하는 장치에게

암호화키 초기화를 요청하고, 이에 대한 응답으로 상기 장치로부터 초기화된 암호화키에 관한 정보를 전달받아 처리하는 암호화키 초기화요청 및 응답 처리 모듈;

<25> 상기 초기화된 암호화키에 관한 정보에 기초하여 암호화키를 생성하는 암호화키 생성 모듈;

<26> 상기 암호화키 생성 모듈에서 생성된 암호화키를 저장하고 관리하는 암호화키 관리 모듈; 및,

<27> 이메일이 착신되면 수신 이메일 주소가 상기 암호화키로 암호화되어 있는 이메일을 선별한 다음, 상기 이메일이 수신자에게 전달될 수 있도록 상기 암호화키를 이용하여 상기 이메일 수신자의 원래 이메일 주소를 복호화하는 이메일 주소 복호화 모듈을 포함하여 구성된다.

<28> 이하 첨부된 도면을 참조하여 본 발명이 속하는 기술분야에서 통상의 지식을 가진 자가 본 발명을 용이하게 실시할 수 있는 바람직한 실시예를 상세히 설명한다. 또한, 도면 전체에 걸쳐 유사한 기능 및 작용을 하는 부분에 대해서는 동일한 도면 부호를 사용한다.

<29> 도 1은 본 발명의 바람직한 일 실시예에 따른 XRI기반의 익명성 보장 방법을 개략적으로 설명하기 위한 순서도이다.

<30> 도 1를 참조하면, 먼저 XRI 기반의 익명성을 보장받고자 하는 이메일 수신자가 자신의 이메일 주소를 XRI 이메일 주소로 변환하고, 이렇게 변환된 XRI 이메일 주소를 별도의 장치에 저장한다(S100). XRI 이메일 주소는 상기 이메일 수신자의 실제 이메일 주소에 기초하여 생성되는데, XRI 표준에 따른 변환 프로토콜에 의하여 상기 이메일 수신자를 식별하기 위한 추상적인 주소이다. 예컨대, 실제 이메일 주소가 alice@abc.com인 경우에는 '=alice+email'이라는 XRI 이메일 주소가 생성된다.

<31> 이렇게 생성된 XRI 이메일 주소는, 이메일 수신자가 이를 자신의 수신 이메일 주소로 사용할 수 있도록 하기 위하여, 이메일 수신자에게 통지된다(S101). 본 발명에 적용될 수 있는 바람직한 실시예에서, 이러한 XRI 이메일 주소 통지는 이메일 수신자의 이메일 서버, 예컨대 SMTP서버로 행하여지고, 이메일 수신자는 이메일 서버로부터 자신의 XRI 이메일 주소를 확인한 다음, 상기 이메일 수신자에게 이메일을 송신할 이메일 송신자에게 자신의 이메일 주소로 상기 XRI 이메일 주소를 사용할 수 있다.

<32> 상기 이메일 수신자에게 이메일을 발송하고자 하는 이메일 송신자는 이메일 수신자로부터 XRI 이메일 주소를 획득한다(S102). 그러나, 상술한 바와 같이 XRI 이메일 주소는 이메일 수신자를 식별하기 위한 추상적인 주소에 불과한 것으로 XRI 이메일 주소만으로는 이메일 수신자에게 이메일을 전송할 수 없으므로, 이메일 수신자에게 이메일을 전송하기 위해서는 이메일 수신자의 XRI 이메일 주소에 기초하여 실제 이메일 주소를 알아야만 한다. 이에 이메일 송신자는 상기 S102단계를 통해 이메일을 보낼 상대방인 이메일 수신자의 XRI 이메일 주소를 알았다면, 이메일 수신자의 실제 이메일 주소를 XRI 이메일 주소로 변환한 장치 또는 서버에 상기 이메일 수신자의 XRI 이메일 주소를 실제 이메일 주소로 전환하여 줄 것을 요청한다(S103).

<33> 다음으로 상기 요청에 대응하여 이메일 수신자의 익명성을 보장하기 위하여 상기 이메일 수신자의 XRI 이메일 주소에 대응하는 실제 이메일 주소에 암호 기술을 적용하여 암호화된 수신 이메일 주소를 생성한 후(S104), 이를 이메일 송신자에게 전달한다(S105). 이때, 본 발명에 적용할 수 있는 바람직한 실시예에서, 이메일 수신자의 이메일 주소를 암호화할 때, 상기 주소가 도용되는 위험을 줄이기 위하여 일회용 패스워드(암호화키: One Time Password)를 사용하는 것이 바람직하다.

<34> 상기 익명 이메일 주소를 전달받은 이메일 송신자는 상기 암호화된 수신 이메일 주소를 착신 주소로 하여 이메일 수신자에게 메일을 발송한다(S106).

<35> 다음으로, 이메일 송신자로부터 이메일이 전달되어 오면, 상기 이메일의 착신 주소가 상기 S104단계에서 사용된 암호화키로 암호화되어 있는지 여부를 확인한다(S107). 상기 확인 결과, 이메일의 착신 주소가 상기 암호화키로 암호화되어 있다면 상기 암호화키를 사용하여 실제 수신 이메일 주소로 복호화한 다음(S108), 상기 복호화된 실제 수신 이메일 주소로 상기 이메일을 전달한다(S109).

<36> 도 2는 상기 S104단계에서 이메일 수신자의 XRI 이메일 주소에 대응하는 실제 이메일 주소에 암호 기술을 적용하여 암호화된 수신 이메일 주소를 생성하는 과정을 개략적으로 설명하기 위한 흐름도이다.

<37> 도 2를 참조하면, 먼저 S200단계~S215단계는 본 발명에 따른 수신 이메일 주소 복호화기(300)이 익명성 보장 서버(200)와 암호화키를 사용하기 위해 초기화 셋업되는 과정을 설명한다. 이러한 초기화 셋업 과정을 통하여 수신 이메일 주소 복호화기(300)은 익명성 보장 서버(200)와 암호화키 생성을 동기화하기 위하여 익명성 보장 서

버(200)로부터 현재시간과 암호화키에 대응되는 난수를 생성하기 위한 시드(Seed)를 제공받는다.

<38> 먼저, 수신 이메일 주소 복호화기(300)은 현재 설정되어 있는 암호화키의 초기화를 익명성 보장 서버(200)에 요청한다(S200). 이는 동일한 패스워드가 지속적으로 사용되는 경우에 발생할 수 있는 예기치 않은 정보 유출에 대비하기 위한 것이다. 이때, 암호화키 초기화 요청의 주기는 미리 설정되는 것이 바람직하고, 당업자의 선택에 의하여 일(day), 주(week)와 같은 기간을 단위로 하여 설정될 수 있다.

<39> 암호화키 초기화 요청을 받은 익명성 보장 서버(200)는, 새로운 암호화키를 생성하기 전에 암호화키를 수신 이메일 주소 복호화기(300)과 동기화하기 위하여 각각의 개체에 시간의 동기화를 할 수 있는 현재시간과 암호화키를 동일하게 생성할 수 있는 난수 생성기에 사용되는 시드(Seed)를 수신 이메일 주소 복호화기(300)에게 제공한다(S205).

<40> 다음으로, 익명성 보장 서버(200)와 수신 이메일 주소 복호화기(300)은 상기 시드에 기초하여 각각 암호화키를 생성한다(S210, S215).

<41> 이메일 송신자(100)가 익명성 보장 서버(200)에게 이메일 수신자의 XRI 이메일 주소를 실제 이메일 주소로 전환하여 줄 것을 요청하면(S220), 익명성 보장 서버(200)는 상기 S210단계에서 생성된 암호화키에 기초하여 상기 XRI 이메일 주소에 대응하는 실제 이메일 주소에 암호 기술을 적용하여 익명 이메일 주소를 생성한다(S225). 예컨대, 이메일 수신자의 이메일 주소가 "username@host.domain"이라면, 이메일 송신자(100)가 익명성 보장 서버(200)로 이메일 수신자(400)의 실제 이메일 주소를 요구하면, 익명성 보장 서버(200)는 미리 생성된 암호화키를 이용하여 "username@host.domain"으로 구성된 부분에서 'username'을 암호화하여 상기 이메일 수신자(400)의 이메일 주소에 대한 암호화된 수신 이메일 주소를 생성한다.

<42> 다음으로, 익명성 보장 서버(200)는 이렇게 생성된 암호화된 수신 이메일 주소를 이메일 송신자(100)로 보낸다. 이메일 송신자(100)는 상기 익명 이메일 주소를 이용하여 이메일 수신자(400)에게 메일을 보내는데, 이때 수신 이메일 주소 복호화기(300)이 먼저 메일을 수신하여 수신된 이메일 주소가 암호화되어 있으면 상기 S215단계에서 익명성 보장 서버(200)와 동기하여 생성한 암호화키를 이용하여 원본 'username'을 복호화하여 이메일 수신자(400)의 실제 수신 이메일 주소를 생성한 다음, 상기 수신 이메일 주소에 기초하여 메시지를 이메일 수신자(400)로 전달한다.

<43> 도 3은 본 발명 또 따른 실시예에 따른 익명성 보장 서버 장치의 개략적인 구성을 나타낸 구조도이다.

<44> 도 3을 참조하면, 본 발명에 따른 익명성 보장 서버(200)는 암호화키 생성 모듈(210), 암호화키 관리 모듈(220), 암호화키 초기화 요청 제어 모듈(230), 수신 이메일주소 암호화 모듈(240) 및 암호화된 이메일 주소 관리 모듈(250)을 포함하여 구성된다.

<45> 상기 암호화키 생성 모듈(210)는 수신 이메일 주소를 암호화하는데 사용되는 암호화키를 생성한다. 이때, 본 발명에 적용할 수 있는 바람직한 실시예에서, 이메일 수신자의 이메일 주소를 암호화할 때, 상기 주소가 도용되는 위험을 줄이기 위하여 일회용 패스워드(암호화키: One Time Password)를 사용하는 것이 바람직하다.

<46> 암호화키 관리 모듈(220)은 상기 암호화키 생성 모듈에서 암호화키를 생성하는데 사용된 시드값을 관리하며, 생성된 암호화키를 저장하고 관리한다. 또한, 상기 암호화키 관리 모듈(220)은, 익명성 보장 서버의 외부에 존재하는 장치로서 익명성 보장 서버에 의하여 암호화된 수신 이메일 주소를 복호화하는 장치와 시간 정보를 동기화한다.

<47> 암호화키 초기화 요청 제어 모듈(230)은 상기 수신 이메일 주소를 복호화하는 장치로부터 암호화키 초기화 요청이 있으면, 상기 암호화키 초기화를 위한 작업을 제어한다.

<48> 수신 이메일 주소 암호화 모듈(240)은 암호화키를 이용하여 실제 이메일 주소가 익명성을 갖도록 암호화한다.

<49> 암호화된 이메일 주소 관리 모듈(250)은 이전에 암호화된 이메일 주소들을 관리하고 상기 수신 이메일 주소 암호화 모듈(240)에서 암호화된 이메일 주소가 이전에 암호화된 이메일 주소들과 중복되지 않도록 관리한다.

<50> 도 4는 본 발명 또 따른 실시예에 따른 수신 이메일 주소 복호화기의 개략적인 구성을 나타낸 구조도이다.

<51> 도 4를 참조하면, 본 발명에 따른 수신 이메일 주소 복호화기(300)은 암호화키 초기화요청 및 응답 처리 모듈(310), 암호화키 관리 모듈(320), 이메일 주소 복호화 모듈(330) 및 암호화키 생성 모듈(340)을 포함하여 구성된다.

<52> 암호화키 초기화요청 및 응답 처리 모듈(310)은 수신 이메일 주소를 암호화하는 장치와 암호화키를 동기화하기 위하여, 상기 수신 이메일 주소를 암호화하는 장치에게 암호화키 초기화를 요청하고, 이에 대한 응답으로 상기 장치로부터 초기화된 암호화키에 관한 정보를 전달받아 처리한다.

<53> 암호화키 생성 모듈(340)는 이메일 송신자로부터 익명 이메일 주소로된 이메일이 수신되면, 이를 복호화하기 위하여 암호화키 초기화 요청 및 응답 처리 모듈(310)이 수신한 시간 및 암호화 시드에 기초하여 암호화키를 생성한다.

<54> 암호화키 관리 모듈(320)은 상기 암호화키 생성 모듈(340)에서 생성된 암호화키를 저장하고 관리한다.

<55> 이메일 주소 복호화 모듈(330)은 이메일이 착신되면 수신 이메일 주소가 상기 암호화키로 암호화되어 있는 이메일을 선별한 다음, 상기 이메일이 수신자에게 전달될 수 있도록 상기 암호화키를 이용하여 상기 이메일 수신자의 원래 이메일 주소를 복호화 하는 작업을 처리한다.

<56> 이상에서 설명한 본 발명은 전술한 실시예 및 첨부된 도면에 의해 한정되는 것이 아니고, 본 발명의 기술적 사상을 벗어나지 않는 범위 내에서 여러가지 치환, 변형 및 변경이 가능하다는 것이 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 당업자에게 있어 명백할 것이다.

발명의 효과

<57> 이상과 같이, 본 발명은 XRI 기반에서 암호화키를 이용하여 주기적으로 변경하므로써 익명성 이메일을 생성하는 방법 및 이를 위한 장치를 제공함으로써, 인터넷에 사용자의 이메일이 유출되더라도 스팸메일에 사용되는 것을 원천적으로 방지하여 사용자의 프라이버시를 보호할 수 있다.

도면의 간단한 설명

<1> 도 1은 본 발명의 바람직한 일 실시예에 따른 XRI기반의 익명성 보장 방법을 개략적으로 설명하기 위한 순서도이다.

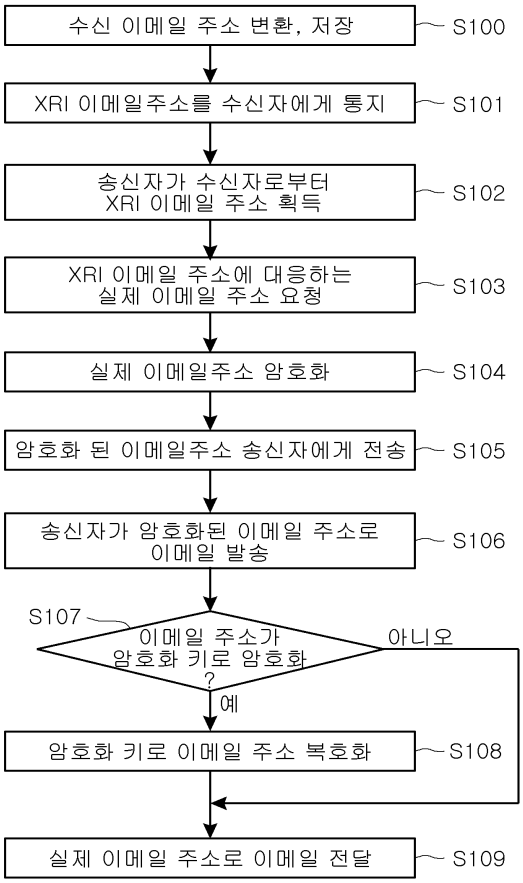
<2> 도 2는 이메일 수신자의 XRI 이메일 주소에 대응하는 실제 이메일 주소에 암호 기술을 적용하여 암호화된 수신 이메일 주소를 생성하는 과정을 개략적으로 설명하기 위한 흐름도이다.

<3> 도 3은 본 발명 또 따른 실시예에 따른 익명성 보장 서버 장치의 개략적인 구성을 나타낸 구조도이다.

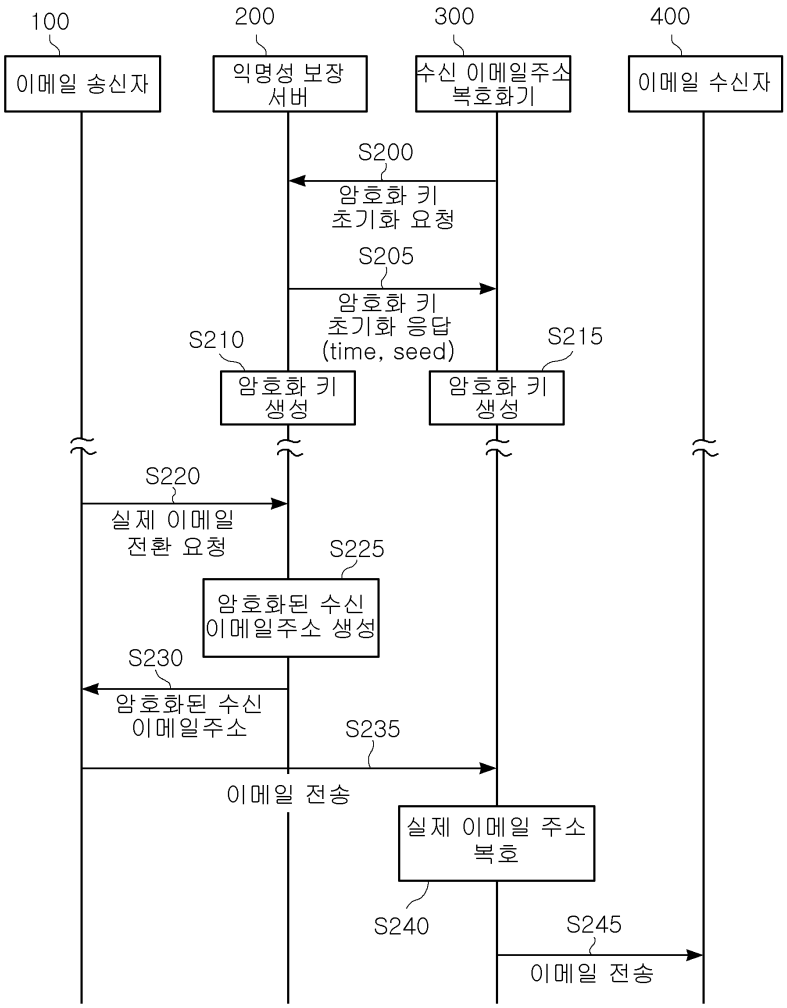
<4> 도 4는 본 발명 또 따른 실시예에 따른 수신 이메일 주소 복호화기의 개략적인 구성을 나타낸 구조도이다.

도면

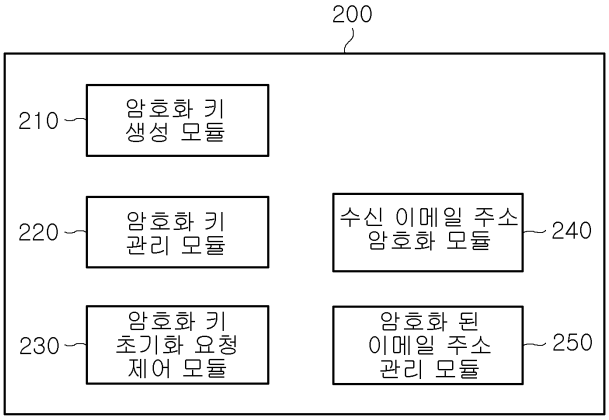
도면1


수신 이메일 주소 변환, 저장
S100
XRI 이메일주소를 수신자에게 통지
S101
송신자가 수신자로부터
XRI 이메일 주소 획득
S102
XRI 이메일 주소에 대응하는
실제 이메일 주소 요청
S103
실제 이메일주소 암호화
S104
암호화 된 이메일주소 송신자에게 전송
S105
송신자가 암호화된 이메일 주소로
이메일 발송
S106
S107
이메일 주소가
암호화 키로 암호화
?
아니오
예
암호화 키로 이메일 주소 복호화
S108
실제 이메일 주소로 이메일 전달
S109

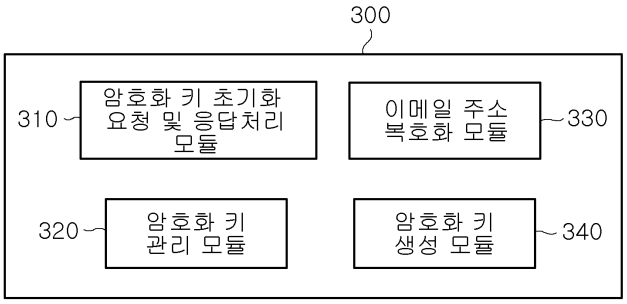
도면2


100
200
300
400
이메일 송신자
익명성 보장 서버
수신 이메일주소 복호화기
이메일 수신자
S200
암호화 키 초기화 요청
S205
암호화 키 초기화 응답 (time, seed)
S210
암호화 키 생성
S215
암호화 키 생성
S220
실제 이메일 전환 요청
S225
암호화된 수신 이메일주소 생성
S230
암호화된 수신 이메일주소
S235
이메일 전송
실제 이메일 주소 복호
S240
S245
이메일 전송

도면3


200
210
암호화 키 생성 모듈
220
암호화 키 관리 모듈
수신 이메일 주소 암호화 모듈
240
230
암호화 키 초기화 요청 제어 모듈
암호화 된 이메일 주소 관리 모듈
250

도면4


300
310
암호화 키 초기화 요청 및 응답처리 모듈
330
이메일 주소 복호화 모듈
320
암호화 키 관리 모듈
340
암호화 키 생성 모듈