(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2010-0108493
(43) 공개일자 2010년10월07일

(51) Int. Cl.
H04L 9/30 (2006.01) *H04L 9/14* (2006.01)
(21) 출원번호 10-2009-0026718
(22) 출원일자 2009년03월29일
심사청구일자 2009년03월29일

(71) 출원인
인하대학교 산학협력단
인천 남구 용현동 253 인하대학교
(72) 발명자
양대헌
서울 서초구 서초동 삼풍 ATP 3동 405호
(74) 대리인
특허법인태동

전체 청구항 수 : 총 4 항

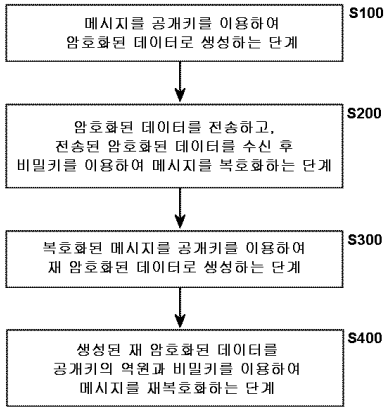
(54) 전송 에러에 강한 공개키 암호화 방법

(57) 요 약

본 발명은 전송 에러에 강한 공개키 암호화 방법에 관한 것으로서, 보다 구체적으로는 (1) 메시지를 공개키를 이용하여 암호화된 데이터로 생성하는 단계; (2) 상기 생성된 암호화된 데이터를 전송하고, 상기 전송된 암호화된 데이터를 수신 후 비밀키를 이용하여 메시지를 복호화하는 단계; (3) 상기 복호화된 메시지를 공개키를 이용하여 재 암호화된 데이터로 생성하는 단계; 및 (4) 상기 생성된 재 암호화된 데이터를 상기 공개키의 역원과 상기 비밀키를 이용하여 메시지를 재 복호화하는 단계를 포함하는 것을 특징으로 한다.

본 발명의 전송 에러에 강한 공개키 암호화 방법에 따르면, 공개키를 이용하여 암호화된 데이터에 전송 도중 에러가 발생하더라도, 상기 암호화된 데이터를 비밀키를 사용하여 복호화하여 메시지를 추출하고, 추출된 메시지를 다시 공개키 및 비밀키를 사용하여 재 암호화 및 재 복호화를 수행함으로써 오류가 없는 메시지를 추출할 수 있는 효과를 제공한다.

대 표 도 - 도1



특허청구의 범위

청구항 1

전송 에러에 강한 공개키 암호화 방법으로서,

(1) 메시지를 공개키를 이용하여 암호화된 데이터로 생성하는 단계;

(2) 상기 생성된 암호화된 데이터를 전송하고, 상기 전송된 암호화된 데이터를 수신 후 비밀키를 이용하여 메시지를 복호화하는 단계;

(3) 상기 복호화된 메시지를 공개키를 이용하여 재 암호화된 데이터로 생성하는 단계; 및

(4) 상기 생성된 재 암호화된 데이터를 상기 공개키의 역원과 상기 비밀키를 이용하여 메시지를 재 복호화하는 단계

를 포함하는 것을 특징으로 하는 전송 에러에 강한 공개키 암호화 방법.

청구항 2

제1항에 있어서,

상기 공개키와 공개키의 역원은 다음 수학식을 이용하여 구하는 것을 특징으로 하는 전송 에러에 강한 공개키 암호화 방법.

<수학식>

$$F_q \otimes f \equiv 1 (mod\ q),$$

$$F_p \otimes f \equiv 1 (mod\ p),$$

$$G_q \otimes g \equiv 1 (mod\ q),$$

$$h \equiv pF_q \otimes g (mod\ q),$$

$$h^{-1} \equiv f \otimes G_q (mod\ q)$$

여기서, 다항식 f는 비밀키를, 다항식 h는 공개키를, h^{-1}은 다항식 h의 역원을, $\otimes$는 컨볼루션 곱을 나타내는 연산자를 각각 나타내며, $g \in L_g$이다. mod q는 다항식 내의 모든 계수가 mod q로 감산되는 것을, mod p는 다항식 내의 모든 계수가 mod p로 감산되는 것을 각각 나타낸다.

청구항 3

제2항에 있어서,

상기 재 암호화된 데이터의 생성은 다음 수학식을 이용하는 것을 특징으로 하는 전송 에러를 강화한 공개키 암호화 방법.

<수학식>

$$e \equiv (m \otimes h + r_0) \bmod q$$

여기서, e는 암호화된 데이터를, m은 메시지를, h는 공개키를, r_0은 임의 다항식을, mod q는 다항식 내의 모든 계수가 mod q로 감산되는 것을 각각 나타낸다.

청구항 4

제2항에 있어서,

상기 재 암호화된 데이터의 재 복호화는 아래 수학식을 이용하는 것을 특징으로 하는 전송 에러에 강한 공개키 암호화 방법.

<수학식>

$h \otimes h^{-1} \equiv 1 \pmod{q}$,

$a \equiv f \otimes e \bmod q$,

$r_0 \equiv F_p \otimes a \bmod p$,

$c \equiv e - r_0 \bmod q$,

$m \equiv c \otimes h^{-1} \bmod q$,

여기서, 다항식 h는 공개키를, h^{-1}은 다항식 h의 역원을, e는 암호화된 데이터를, r_0은 임의 다항식을, mod q는 다항식 내의 모든 계수가 mod q로 감산되는 것을, h^{-1} mod q는 공개키 h의 mod q 상의 역원을 각각 나타낸다.

명 세 서

발명의 상세한 설명

기 술 분 야

[0001] 본 발명은 공개키 암호화 방법에 관한 것으로서, 보다 구체적으로는 전송 에러에 강한 공개키 암호화 방법에 관한 것이다.

배 경 기 술

[0002] 일반적으로, 네트워크를 통하여 데이터를 전송할 때는 전송되는 데이터의 보안을 위하여 암호화를 수행하여 데이터를 전송한다.

[0003] 데이터의 암호화 방법의 하나로서, 공개키를 이용하여 전송될 데이터를 암호화하여 전송하고, 수신자는 자신이 보유하고 있는 개인키를 이용하여 수신받은 공개키로 암호화된 데이터를 복호화하는 공개키 암호화 시스템이 널리 사용되고 있다.

[0004] 공개키 암호화 시스템으로는 NTRU사에서 만든 NTRU라는 공개키 암호화 시스템이 주로 사용된다. NTRU는 몫 링 R이 $R=Z/(X^N-1)$인 환(環, Ring)을 기반으로 하는 공개키 암호화 시스템으로서, NTRU는 3가지 공개 파라미터(N, p, q)를 가진다(여기서, p와 q는 최대공약수가 1인 서로 소의 관계, 및 $p < q$인 관계를 만족한다). 또한, 차수가 N-1이고 원소들이 정수인 4개의 다항식 집합(L_f, L_g, L_ϕ, L_m)을 가진다.

[0005] NTRU 암호화 시스템은 FR의 다항식을 이용하며, 다항식 F의 원소들은 다음 수학식 1과 같다.

수학식 1

[0006] $$F = \sum_{i=0}^{N-1} F_i x^i = [F_0, F_1, \cdots, F_{N-1}]$$

[0007] 두 개의 다항식 A와 B의 컨볼루션 곱 C는 $C=A \otimes B$와 같이 이루어지며, 위 다항식 C의 원소들은 다음 수학식 2와 같다.

수학식 2

[0008] $$C_k = \sum_{i=0}^{N-1} A_i B_{k-1} + \sum_{i=0}^{N-1} A_i B_{N+k-1} = \sum_{i+j \equiv k (mod\ N)} A_i B_j$$

[0009] NTRU의 키 생성 방법

[0010] A와 B가 보안이 보장되어 있지 않은 네트워크 환경에서 서로 비밀 메시지를 주고받고 싶다면, 우선 A가 $f \in L_f$와 $g \in L_g$을 선택한다. 다항식 f는 모듈러 q에 대한 곱셈의 역원인 F_q과 모듈러 p에 대한 곱셈의 역원 F_p를 가진다.

[0011] A는 F_q, F_p를 다음 수학식 3에 의하여 계산한다.

수학식 3

$$F_q \otimes f \equiv 1 (mod\ q)$$

$$F_p \otimes f \equiv 1 (mod\ p)$$

[0012] $$h \equiv F_q \otimes g (mod\ q)$$

[0013] 여기서, A의 공개키는 다항식 h이고, 비밀키는 다항식 f이며, 연산자 $\otimes$는 본 발명의 전체에서 컨볼루션 곱을 의미하는 것으로서 사용된다. 또한, 본 발명의 전체에서 mod q는 다항식 내의 모든 계수가 mod q로 감산되는, 즉 q로 나눈 나머지로 계산됨을 의미하며, mod p는 다항식 내의 모든 계수가 mod p로 감산되는 것을 의미한다.

[0014] NTRU의 암호화 방법

[0015] 송신자 A가 메시지 $m \in L_m$을 B의 공개키 h를 이용해서 암호화하기 위해서 임의 다항식 r을 선택하고 암호문 e를 다음 수학식 4를 이용하여 계산한다.

수학식 4

[0016] $$e \equiv (pr \otimes h + m) \bmod q$$

[0017] NTRU의 복호화 방법

[0018] 수신자 B가 비밀키 f를 이용해서 암호문 e로부터 메시지 m을 복호화하기 위해 $a \equiv f \otimes e \bmod q$를 계산한다. 이때 f의 각 계수들은 -2/q에서 2/q 사이에 있도록 선택한다. 그리고 B는 다음 수학식 5를 이용하여 메시지 m을 복원할 수 있다.

수학식 5

[0019] $$m \equiv F_p^{-1} \otimes a \bmod p$$

[0020] 그러나 이러한 종래의 NTRU의 공개키 암호화 시스템은 통신선로 상에서 비트가 뒤바뀌는 것과 같은 에러가 발생하는 경우(0에서 1로, 1에서 0으로), 메시지 수신자가 에러를 정정하여 메시지를 정확히 복원하는데 어려움이 따르는 문제점이 있었다.

발명의 내용

해결 하고자하는 과제

[0021] 본 발명은 기존에 제안된 NTRU의 공개키 암호화 시스템의 상기와 같은 종래의 문제점들을 해결하기 위해 제안된 것으로서, 암호화를 수행한 데이터의 전송 도중에 에러가 발생하더라도 데이터의 정확한 복호화가 가능하도록 하는 전송 에러에 강한 공개키 암호화 방법을 제공하는 것을 그 목적으로 한다.

과제 해결수단

[0022] 상기한 목적을 달성하기 위한 본 발명의 특징에 따른 전송 에러에 강한 공개키 암호화 방법은,

[0023] (1) 메시지를 공개키를 이용하여 암호화된 데이터로 생성하는 단계;

[0024] (2) 상기 생성된 암호화된 데이터를 전송하고, 상기 전송된 암호화된 데이터를 수신 후 비밀키를 이용하여 메시지를 복호화하는 단계;

[0025] (3) 상기 복호화된 메시지를 공개키를 이용하여 재 암호화된 데이터로 생성하는 단계; 및

[0026] (4) 상기 생성된 재 암호화된 데이터를 상기 공개키의 역원과 상기 비밀키를 이용하여 메시지를 재 복호화하는 단계를 포함하는 것을 특징으로 한다.

[0027] 바람직하게는, 상기 공개키와 공개키의 역원은 아래 수학식을 이용하여 구하는 것을 특징으로 한다.

[0028] <수학식>

$$F_q \otimes f \equiv 1 (mod\ q),$$

$$F_p \otimes f \equiv 1 (mod\ p),$$

$$G_q \otimes g \equiv 1 (mod\ q),$$

$$h \equiv pF_q \otimes g (mod\ q),$$

[0029] $$h^{-1} \equiv f \otimes G_q (mod\ q)$$

[0030] 여기서, 다항식 f는 비밀키를, 다항식 h는 공개키를, h^{-1}는 다항식 h의 역원을, $\otimes$는 컨볼루션 곱을 나타내는 연산자를 각각 나타내며, $g \in L_g$이다. 또한, mod q는 다항식 내의 모든 계수가 mod q로 감산되는 것을, mod p는 다항식 내의 모든 계수가 mod p로 감산되는 것을 각각 나타낸다.

[0031] 더욱 바람직하게는, 상기 재 암호화된 데이터의 생성은 아래 수학식을 이용하는 것을 특징으로 한다.

[0032] <수학식>

[0033] $$e \equiv (m \otimes h + r_0) \bmod q$$

[0034] 여기서, e는 암호화된 데이터를, m은 메시지를, h는 공개키를, $\otimes$는 컨볼루션 곱을 나타내는 연산자를, r_0은 임의 다항식을, mod q는 다항식 내의 모든 계수가 mod q로 감산되는 것을 각각 나타낸다.

[0035] 더욱 바람직하게는, 상기 재 암호화된 데이터의 재 복호화는 아래 수학식을 이용하는 것을 특징으로 한다.

[0036] <수학식>

$$h \otimes h^{-1} \equiv 1 (mod\ q),$$

$$a \equiv f \otimes e \bmod q,$$

$$r_0 \equiv F_p \otimes a \bmod p,$$

$$c \equiv e - r_0 \bmod q,$$

[0037] $$m \equiv c \otimes h^{-1} \bmod q,$$

[0038] 여기서, 다항식 h는 공개키를, h^{-1}는 다항식 h의 역원을, e는 암호화된 데이터를, r_0은 임의 다항식을, mod q는 다항식 내의 모든 계수가 mod q로 감산되는 것을, ⊗는 컨볼루션 곱을 나타내는 연산자를, h^{-1} mod q는 공개키 h의 mod q 상의 역원을 각각 나타낸다.

효 과

[0039] 본 발명의 전송 에러에 강한 공개키 암호화 방법에 따르면, 공개키를 이용하여 암호화된 데이터에 전송 도중 에러가 발생하더라도, 상기 암호화된 데이터를 비밀키를 사용하여 복호화하여 메시지를 추출하고, 추출된 메시지를 다시 공개키 및 비밀키를 사용하여 재 암호화 및 재 복호화를 수행함으로써 오류가 없는 메시지를 추출할 수 있는 효과를 제공한다.

발명의 실시를 위한 구체적인 내용

[0040] 이하에서는 본 발명에 따른 실시예에 대하여 상세하게 설명하기로 한다.

[0041] 도 1은 본 발명의 일실시예에 따른 전송 에러에 강한 공개키 암호화 방법의 흐름을 나타내는 도면이다. 도 1에 도시된 바와 같이, 본 발명의 일실시예에 따른 전송 에러에 강한 공개키 암호화 방법은, 메시지를 공개키를 이용하여 암호화된 데이터로 생성하는 단계(S100), 생성된 암호화된 데이터를 전송하고, 전송된 암호화된 데이터를 수신 후 비밀키를 이용하여 메시지를 복호화하는 단계(S200), 복호화된 메시지를 공개키를 이용하여 재 암호화된 데이터로 생성하는 단계(S300), 및 생성된 재 암호화된 데이터를 공개키의 역원과 비밀키를 이용하여 메시지를 재 복호화하는 단계(S400)를 포함한다.

[0042] 본 발명의 일실시예에 따른 전송 에러에 강한 공개키 암호화 방법의 상세한 구성은 이하에서 보다 상세하게 설명하기로 한다.

[0043] 본 발명의 실시예에 따른 전송 에러에 강한 공개키 암호화 방법은 NTRU라는 공개키 암호화 시스템을 이용한다.

[0044] 본 발명에 따른 전송 에러에 강한 공개키 암호화 방법은 데이터의 수신자가 공개키를 보유하고 있지 않더라도, 아래의 키 생성 방법에 따라 공개키를 생성하여 수신받은 데이터를 재 암호화(Re-encryption)가 가능하도록 할 수 있다. 더욱 자세히 설명하면, 수신자 B는 송신자 A로부터 공개키에 의하여 암호화된 데이터를 전송받은 후, 보유하고 있는 비밀키를 이용하여 전송받은 암호화된 데이터에 대한 복호화를 수행하여 메시지를 획득한다. 또한, 수신자 B는 획득한 메시지에 에러가 발생한 경우 이를 복구하여 정확한 메시지로 복원하기 위하여 아래와 같이 공개키를 생성하여 재 암호화 및 재 복호화를 수행한다.

[0045] 수신자 B의 공개키 생성, 재 암호화 및 재 복호화는 아래를 참조하여 자세히 설명하도록 한다.

[0046] 1. 키 생성

[0047] 종래의 NTRU와는 다르게 다항식 f, g 모두 모듈러 p(mod p)와 모듈러 q(mod q)에 대해서 역 다항식이 존재한다. 수신자 B는 공개키 h와 h^{-1}를 다음 수학식 6을 이용하여 계산한다.

수학식 6

$$F_q \otimes f \equiv 1 (mod\ q),$$

$$F_p \otimes f \equiv 1 (mod\ p),$$

$$G_q \otimes g \equiv 1 (mod\ q),$$

$$h \equiv pF_q \otimes g (mod\ q),$$

[0048] $$h^{-1} \equiv f \otimes G_q (mod\ q)$$

[0049] 여기서, 다항식 h는 공개키이고, h^{-1}는 다항식 h의 역원이며, 다항식 f는 비밀키이다.

[0050] 2. 재 암호화

[0051] 수신자 B가 메시지 $m \in L_m$을 B의 공개키 h를 이용하여 재 암호화하기 위하여 임의 다항식 $r_0 \in L_\phi$을 선택하고 재 암호화된 데이터 e를 다음 수학식 7을 이용하여 계산한다.

수학식 7

[0052] $$e \equiv (m \otimes h + r_0) \bmod q$$

[0053] 여기서, e는 암호화된 데이터를, m은 메시지를, h는 공개키를, r_0은 임의 다항식을, mod q는 다항식 내의 모든 계수가 mod q로 감산되는 것을 각각 나타낸다.

[0054] 3. 재 복호화

[0055] 재 암호화된 데이터는 다음 수학식 8을 이용하여 재 복호화를 수행함으로써 전송받은 메시지를 추출할 수 있다. 수학식 8은 먼저 h의 곱셈에 대한 역원(h^{-1})을 구하고, 비밀키 f를 이용하여 a와 r_0을 구하고, r_0과 h^{-1}을 써서 m을 계산하는 단계를 나타낸다.

수학식 8

$$h \otimes h^{-1} \equiv 1 (mod\ q),$$

$$a \equiv f \otimes e \bmod q,$$

$$r_0 \equiv F_p \otimes a \bmod p,$$

$$c \equiv e - r_0 \bmod q,$$

[0056] $$m \equiv c \otimes h^{-1} \bmod q,$$

[0057] 여기서, 다항식 h는 공개키를, h^{-1}은 다항식 h의 역원을, e는 암호화된 데이터를, r_0은 임의 다항식을, mod q는 다항식 내의 모든 계수가 mod q로 감산되는 것을, h^{-1} mod q는 공개키 h의 mod q 상의 역원을 각각 나타낸다.

[0058] 본 발명에서 제안한 전송 에러에 강한 공개키 암호화 시스템은 암호문에 어떤 한계 값 이하의 비트 에러가 있더라도 정확한 복호화가 가능하다.

[0059] 에러 벡터를 라 하자. 만약 암호문(e′)에 에러 벡터 σ가 추가되었다면 다음 수학식 9를 얻을 수 있다.

수학식 9

[0060] $$e' = (m \otimes h + r_0 + \sigma) \bmod q$$

[0061] 수학식 9와 같이 주어진 암호문에 대하여 복호화 과정을 따르면, 다음 수학식 10을 구할 수 있다.

수학식 10

[0062] $$a' = f \otimes e' \bmod q$$
$$r = f_p^{-1} \otimes a' \bmod p$$

[0063] 복호화를 위한 조건이 성립하면 r은 r_0+와 일치하고, 따라서 다음 수학식 11과 같이 정확한 메시지를 복호화할 수 있게 된다.

수학식 11

[0064] $$c = (e' - r_0 - \sigma) \bmod q$$
$$m = c \otimes h^{-1} \bmod q$$

[0065] 상기 수학식 11에서는 에러 벡터 σ가 더해지는 형태의 에러를 모델링했지만, 실제로 통신선로 상에서의 에러는 비트가 바뀌는(0이 1로, 1이 0으로) 형태의 에러가 발생한다. 하지만 이런 종류의 에러는 에러 벡터의 덧셈으로 모델링이 언제나 가능하므로 본 발명에서 예로서 설명한 에러 벡터를 포함하는 암호문이 더 포괄적인 에러를 포함한다고 할 수 있다.

[0066] 본 발명에서 제안한 전송 에러에 강한 공개키 암호화 방법은 암호문의 일부에 대해서만 에러 정정코드를 사용하더라도 같은 수준의 에러 정정 능력을 가질 수 있게 되므로, 더 효율적임을 알 수 있다. 다음 표 1은 Reed-Solomon 코드, Convolution 코드, Turbo 코드에 각각 적용했을 때, 얻을 수 있는 효율을 나타낸다. 표 1로부터 본 발명에서 제안한 전송 에러에 강한 공개키 암호화 방법의 효율성을 분명하게 확인할 수 있다.

표 1

[0067]

	수정된 NTRU(n,k)를 갖는 Reed Solomon 코드		수정된 NTRU(p,s/t)를 갖는 컨볼루션 코드		수정된 NTRU(s/t)를 갖는 터보 코드	
Parameter	(255,223)	(63,43)	(7,1/2)	(7,1/3)	(1/2)	(1/4)
Redundancy	108비트	351비트	753비트	1506비트	753비트	2259비트
Efficiency	4%	11%	17%	22%	17%	25%

[0068] 본 발명은 통신선로 상에서 에러 정정 코드의 효율을 높일 수 있다는 실질적인 이득을 가질 뿐만 아니라, 암호문에 생긴 에러와 상관없이 복호화를 정확히 할 수 있는 첫 번째 공개키 암호 방법으로서 이론적인 의미도 크다고 할 수 있다.

[0069] 이상 설명한 바와 같이 본 발명은 본 발명이 속한 기술분야에서 통상의 지식을 가진 자에 의하여 다양한 변형이나 응용이 가능하며, 본 발명에 따른 기술적 사상의 범위는 아래의 특허청구범위에 의하여 정해져야 할 것이다.

도면의 간단한 설명

[0070] 도 1은 본 발명의 일실시예에 따른 전송 에러에 강한 공개키 암호화 방법의 흐름을 나타내는 도면.

[0071] <도면 중 주요 부분에 대한 부호의 설명>

[0072] S100: 메시지를 공개키를 이용하여 암호화된 데이터로 생성하는 단계

[0073] S200: 생성된 암호화된 데이터를 전송하고, 전송된 암호화된 데이터를 수신 후 비밀키를 이용하여 메시지를 복호화하는 단계

[0074] S300: 복호화된 메시지를 공개키를 이용하여 재 암호화된 데이터로 생성하는 단계

[0075] S400: 생성된 재 암호화된 데이터를 공개키의 역원과 비밀키를 이용하여 메시지를 재 복호화하는 단계

도면

도면1