(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2019년11월04일
(11) 등록번호 10-2022333
(24) 등록일자 2019년09월10일

(51) 국제특허분류(Int. Cl.)
H04L 9/08 (2006.01) *H04L 9/12* (2006.01)
H04L 9/30 (2006.01)
(52) CPC특허분류
H04L 9/0825 (2013.01)
H04L 9/12 (2013.01)
(21) 출원번호 10-2018-0045856
(22) 출원일자 2018년04월20일
심사청구일자 2018년04월20일
(56) 선행기술조사문헌
용승림 et al., "정수계획법에 기반한 공개키 암호 알고리즘의 설계", 정보과학회논문지: 시스템 및 이론 27.9 (2000.09.)*
Roohallah Rastaghi, "Cryptanalysis of a new knapsack type public-key cryptosystem" (2012.)*
*는 심사관에 의하여 인용된 문헌

(73) 특허권자
금오공과대학교 산학협력단
경상북도 구미시 대학로 61 (양호동)
(72) 발명자
유원석
경상북도 구미시 산호대로 423
신승혁
경상북도 구미시 도봉로 67 도량뜨란채5단지아파트
(74) 대리인
특허법인 피씨알

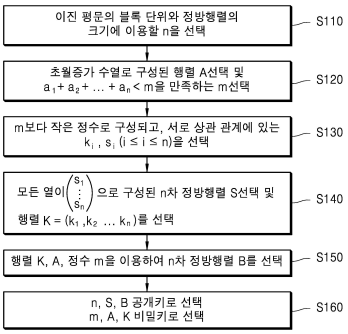
전체 청구항 수 : 총 10 항 심사관 : 박보미

(54) 발명의 명칭 **공개키 암호 알고리즘을 이용한 암호화/복호화 방법 및 장치**

(57) 요 약

본 발명은 공개키 암호알고리즘을 이용한 암호화/복호화 방법 및 장치에 대한 것으로, 이진평문의 블록 단위와 정방행렬의 크기에 이용할 정수 n을 선택하고, 행렬 A=(a_1, a_2, ..., an)을 선택하고, $a_1 + a_2 + \ldots + an < m$을 만족하는 정수 m을 선택하고, 상기 m보다 작은 정수로 구성되는 수열, ki, si (1≤i≤n)을 선택하고, 모든 열이 $\begin{pmatrix} s_1 \\ s_2 \\ \cdot \\ \cdot \\ \cdot \\ s_n \end{pmatrix}$으로 구성된 n차 정방행렬 S를 선택하고, 상기 수열 ki (1≤i≤n)로 구성된 행렬 K=(k_1, k_2, ..., kn)을 선택하고, 상기 행렬 A, K 및 상기 정수 m을 이용하여 n차 정방행렬 B를 선택하고, 상기 정수 n 및 상기 행렬 B, S를 공개키로 선택하고, 상기 정수 m 및 상기 행렬 A, K를 비밀키로 선택하되, 상기 행렬 A의 구성요소 a1, a2, an은 초월증가수열로 구성되는 것을 특징으로 한다.

대 표 도



(52) CPC특허분류
H04L 9/302 (2013.01)

명 세 서

청구범위

청구항 1

이진평문의 블록 단위와 정방행렬의 크기에 이용할 정수 n을 선택하는 단계;

행렬 A=(a1, a2, ... an)을 선택하고, $a_1 + a_2 + \ldots + an < m$을 만족하는 정수 m을 선택하는 단계;

상기 m보다 작은 정수로 구성되는 수열, ki, si (1≤i≤n)을 선택하는 단계;

모든 열이 $\begin{pmatrix} s_1 \\ s_2 \\ \cdot \\ \cdot \\ s_n \end{pmatrix}$으로 구성된 n차 정방행렬 S를 선택하고, 상기 수열 ki (1≤i≤n)로 구성된 행렬 K=(k_1, k_2, ..., kn)을 선택하는 단계;

상기 행렬 A, K 및 상기 정수 m을 이용하여 n차 정방행렬 B를 선택하는 단계; 및

상기 정수 n 및 상기 정방행렬 B, S를 공개키로 선택하고, 상기 정수 m 및 상기 행렬 A, K를 비밀키로 선택하는 단계를 포함하되,

상기 행렬 A의 구성요소 a_1, a_2, an은 초월증가수열로 구성되고,

상기 수열, ki, si (1≤i≤n)은 다음과 같은 수학식 1을 만족하여 선택되는 것을 특징으로 하는, 공개키 암호알고리즘을 이용한 암호화/복호화 방법.

[수학식 1]

$k_1s_1 + k_2s_2 + \ldots + knsn \equiv 0 \pmod m$

청구항 2

삭제

청구항 3

제1항에 있어서,

상기 정수 n은 1024 이상의 정수로 선택되는 것을 특징으로 하는, 공개키 암호알고리즘을 이용한 암호화/복호화 방법.

청구항 4

제1항에 있어서,

상기 n차 정방행렬 B은 수학식 2를 만족하여 선택되는 것을 특징으로 하는, 공개키 암호알고리즘을 이용한 암호화/복호화 방법.

[수학식 2]

$KB \equiv (a_1, a_2, \ldots, an) \pmod m$

청구항 5

제1항에 있어서,

상기 공개키를 이용하여 이진평문 M=(m_1, m_2, ..., mn)을 암호화하는 단계를 더 포함하되,

상기 암호화하는 단계는,

n차 정방행렬인 행렬 P를 선택하는 단계; 및

상기 공개키에 포함된 상기 정방행렬 S, B, 및 상기 정수 m 및 상기 행렬 P를 이용하여 상기 이진평문을 암호화하는 단계를 포함하는 것을 특징으로 하는, 공개키 암호알고리즘을 이용한 암호화/복호화 방법.

청구항 6

제5항에 있어서,

상기 행렬 P의 구성요소 $p_{ij}(1 \leq i,j \leq n)$는 상기 정수 m보다 작은 정수로 구성되고,

상기 이진평문을 암호화하는 단계는,

아래와 같은 수학식 3을 이용하여 암호화하는 것을 특징으로 하는, 공개키 암호알고리즘을 이용한 암호화/복호화 방법.

[수학식 3]

$$(SP+B)M^{T} \equiv C^{T} \pmod{m}$$

여기서, M은 이진평문을 나타내고, C^{T}는 암호문을 나타낸다.

청구항 7

제1항에 있어서,

상기 비밀키를 이용하여 암호문 C^{T}을 복호화하는 단계를 더 포함하되,

상기 복호화하는 단계는,

상기 암호문에 비밀키를 이용하여 복호중간값을 획득하는 단계; 및

상기 복호중간값을 이진평문으로 복호화하는 단계를 포함하는 것을 특징으로 하는, 공개키 암호알고리즘을 이용한 암호화/복호화 방법.

청구항 8

제7항에 있어서,

상기 복호중간값 $\alpha \equiv a_1m_1 + a_2m_2 + \ldots + anmn \pmod{m}$이고,

상기 복호중간값을 획득하는 단계는,

아래와 같은 수학식 4를 이용하여 암호화하는 것을 특징으로 하는, 공개키 암호알고리즘을 이용한 암호화/복호화 방법.

[수학식 4]

$$KC^{T} \equiv \alpha \pmod{m}$$

여기서, C^{T}는 암호문을 나타내고, α는 복호중간값을 나타낸다.

청구항 9

제8항에 있어서,

상기 복호중간값을 이진평문으로 복호화하는 단계는,

초월증가수열의 특징을 이용하여 복호화하는 것을 특징으로 하는, 공개키 암호알고리즘을 이용한 암호화/복호화 방법.

청구항 10

통신부;

프로그램을 저장하는 메모리; 및

이진평문의 블록 단위와 정방행렬의 크기에 이용할 정수 n을 선택하고,

행렬 A=(a_1, a_2, ..., an)을 선택하고, $a_1 + a_2 + \ldots + an < m$을 만족하는 정수 m을 선택하고,

상기 m보다 작은 정수로 구성되는 수열, ki, si (1≤i≤n)을 선택하고,

모든 열이 $\begin{pmatrix} s_1 \\ s_2 \\ \cdot \\ \cdot \\ \cdot \\ s_n \end{pmatrix}$으로 구성된 n차 정방행렬 S를 선택하고, 상기 수열 ki (1≤i≤n)로 구성된 행렬 K=(k1, k2, ... kn)을 선택하고,

상기 행렬 A, K 및 상기 정수 m을 이용하여 n차 정방행렬 B를 선택하고,

상기 정수 n 및 상기 정방행렬 B, S를 공개키로 선택하고, 상기 정수 m 및 상기 행렬 A, K를 비밀키로 선택하도록 제어하는 프로세서를 포함하되,

상기 행렬 A의 구성요소 a_1, a_2, an은 초월증가수열로 구성되고,

상기 수열, ki, si (1≤i≤n)은 다음과 같은 수학식 1을 만족하여 선택되는 것을 특징으로 하는, 공개키 암호알고리즘을 이용한 암호화/복호화 장치.

[수학식 1]

$k_1s_1 + k_2s_2 + \ldots + knsn \equiv 0 \pmod{m}$

청구항 11

제1항, 제3항 내지 제9항 중 어느 하나의 청구항의 공개키 암호알고리즘을 이용한 암호화/복호화 방법을 구현하기 위한 프로그램이 기록된 컴퓨터로 판독 가능한 비일시적 기록 매체.

발명의 설명

기 술 분 야

[0001] 본 발명은 공개키 암호알고리즘을 이용한 암호화/복호화 방법 및 장치에 관한 것으로, 보다 상세하게는 암호화 및 복호화를 위한 공개키 및 비밀키를 생성하기 위한 방법을 구현함으로써 암호화/복호화 처리의 보안성 확보를 도모할 수 있는 암호화 방법 및 장치에 관한 것이다.

배 경 기 술

[0002] 최근 정보통신 분야의 급속한 성장과 함께 통신망을 이용한 정보의 전달이 일반화되고 있는 현실이다. 그러나, 이와 같이 통신망을 이용하여 정보를 전달하고자 할 경우, 전화망의 '도청' 또는 인터넷상의 '해킹'등으로 인해 그 정보의 보안 유지가 사실상 어렵다는 단점이 있다. 따라서, 이러한 '도청'이나 '해킹'으로부터 정보를 안전하게 보호하기 위해, 정보를 전달하는 측에서 정보에 대한 암호화를 수행하고, 그 정보를 수신하는 측에서 해당 정보를 해독하는 과정을 거침으로써, 해당 정보의 유출을 방지하고자 하는 기술이 발달하고 있다. 이러한 기술을 일반적으로 암호 알고리즘이라고 한다.

[0003] 서버/클라이언트 구조에서 임의의 클라이언트가 서버로부터 원하는 서비스를 제공받기 위해 자신의 신상정보 등과 같이 보안이 요구되는 정보를 서버측으로 전송하고자 하는 경우, 그 정보를 암호화하기 위한 암호화 알고리즘이 요구된다. 즉, 임의의 클라이언트가 전송할 정보를 생성하여 그 정보를 암호화한 후 암호화된 정보를 전송하면, 정보를 수신한 측은 그 암호화된 정보를 복호화함으로써 해당 내용을 해독한다. 이러한 암호 알고리즘은 해당 정보를 암호화하고 복호화하는 키의 종류에 따라 암호화 및 복호화 시 동일키를 사용하는 '비밀키 암호 알고리즘'과, 암호화 및 복호화 시 서로 다른 키를 사용하는 '공개키 암호 알고리즘'으로 구분된다.

[0004] 본 발명은 이들 중 '공개키 암호 알고리즘'에 관한 것으로서, '공개키 암호 알고리즘'은 암호화 및 복호화 시

서로 다른 키를 사용한다는 특징으로 인해 비대칭키 암호 알고리즘이라고도 칭한다. 이러한 '공개키 암호 알고리즘'은 키 생성 알고리즘을 통해 두 개의 키를 생성하여 그중 하나를 전화번호부에 전화번호를 공개하듯이 공개하고, 나머지 하나를 개인키로 자신이 보관하여 사용한다.

[0005] 예를 들어, 'A'가 'B'로 문서를 송신하고자 할 경우, 'A'는 공개된 'B'의 공개키를 이용하여 해당 문서를 암호화하고, 'B'는 수신된 암호문을 자신의 개인키로 풀게되는 것이다. 따라서, '공개키 암호 알고리즘'의 사용자는 상호 정보를 교환하고자 하는 사람들의 수가 증가하더라도, 그 사람들의 수와 관계없이 자신의 개인키만을 관리하면 된다.

[0006] '공개키 암호 알고리즘'의 대표적인 예로 RSA(Rivest-Shamir-Adleman) 알고리즘이 있다. RSA 알고리즘에서는 3개의 개인키와 2개의 공개키를 사용하게 되며, 이러한 개인키 및 공개키는 소정의 키 생성 알 고리즘에 의해 생성된다.

[0007] 일반적으로 RSA 알고리즘에서 개인키 및 공개키를 선정하는 과정은 다음과 같다. 우선, 두 개의 큰 소수(p,q)를 선택하여, 그 소수들(p,q)을 2개의 개인키로 사용하고, 그 두수의 곱(p*q)을 공개키(n)로 선정한다. 그리고, 그 공개키(n)를 오일러(Euler) 공식에 적용한 후, 그 결과값(ϕ(n))과 서로 소인 임의의 정수(e)를 선정하여 또 하나의 공개키(e)로 선정한다. 마지막으로, 유클리드_알고리즘(Euclidean Algorithm)에 의해 수학식 1 을 만족하는 수(d)를 계산하여, 상기 두 개의 소수(p,q)와 함께 개인키로 선정한다.

[0008] [수학식 1]

[0009] $$e \cdot d \equiv 1 \pmod{\phi(n)}$$

[0010] 하지만, 이러한 공개키 암호 알고리즘은 '공개키 암호 알고리즘'의 특성으로 인해, 공개키 암호 알고리즘 사용자의 개인키가 제3자에게 유출될 경우, 그 제3자는 해당 사용자에게 전송되는 모든 정보를 해독할 수 있게된다는 단점이 있다.

[0011] 예를들어, 회원들에게 금융 거래 서비스 또는 전자 상거래 관련 서비스 등을 제공하기 위해, 공개키 암호 알고리즘을 채택하고 있는 서버의 경우, 그 개인키가 제3자에게 유출될 경우 해당 서버 및 회원(클라이언트)들 모두에게 치명적이다.

[0012] 이러한 장비의 사용이 증가할수록 암호화 방법에 대한 중요성과 필요성은 점점 늘어날 수밖에 없음을 이미 충분히 경험하였으며, 따라서 보안성의 확보가 도모할 수 있는 방안이 필요하다.

발명의 내용

해결하려는 과제

[0013] 따라서, 본 발명에서는 이와 같은 문제점을 해결하기 위해, 공개키 암호 알고리즘을 이용하는 사용자들간 정보 전달 요청이 발생할 경우, 그 요청에 따른 공개키 및 암호키를 생성하여 정보를 전달하고자 하는 당사자들이 공유할 수 있도록 하는 공개키 암호알고리즘을 이용한 암호화/복호화 방법을 제공하는 것을 목적으로 한다.

[0014] 발명에서 이루고자 하는 기술적 목적들은 이상에서 언급한 사항들로 제한되지 않으며, 언급하지 않은 또 다른 기술적 과제들은 이하 설명할 본 발명의 실시예들로부터 본 발명이 속하는 기술분야에서 통상의 지식을 가진 자에 의해 고려될 수 있다.

과제의 해결 수단

[0015] 상기 기술적 과제를 해결하기 위한 공개키 암호알고리즘을 이용한 암호화/복호화 방법 및 장치는, 이진평문의 블록 단위와 정방행렬의 크기에 이용할 정수 n을 선택하고, 행렬 A=(a_1, a_2, ... an)을 선택하고, $a_1 + a_2 + \ldots + an < m$을 만족하는 정수 m을 선택하고, 상기 m보다 작은 정수로 구성되는 수열, ki, si ($1 \le i \le n$)을 선택하고, 모든 열이 $\begin{pmatrix} s_1 \\ s_2 \\ \cdot \\ \cdot \\ \cdot \\ s_n \end{pmatrix}$으로 구성된 n차 정방행렬 S를 선택하고, 상기 수열 ki ($1 \le i \le n$)로 구성된 행렬 K=(k_1, k_2, ... kn)을 선택하고, 상기 행렬 A, K 및 상기 정수 m을 이용하여 n차 정방행렬 B를 선택하고, 상기 정수 n 및 상기 행렬 B, S를 공개키로 선택하고, 상기 정수 m 및 상기 행렬 A, K를 비밀키로 선택하되, 상기 행렬 A의

구성요소 a_1, a_2, an은 초월증가수열로 구성되는 것을 특징으로 한다.

[0016] 또한, 상기 수열, ki, si (1≤i≤n)은 다음과 같은 수학식 1을 만족하여 선택되는 것을 특징으로 한다.

[0017] [수학식 1]

[0018] $k1s1 + k2s2 + ... + knsn \equiv 0 \pmod m$

[0019] 또한, 상기 정수 n은 1024 이상의 정수로 선택되는 것을 특징으로 한다.

[0020] 또한, 상기 n차 정방행렬 B은 수학식 2를 만족하여 선택되는 것을 특징으로 한다.

[0021] [수학식 2]

[0022] $KB \equiv (a_1, a_2, ..., an) \pmod m$

[0023] 또한, 상기 공개키를 이용하여 이진평문 $M=(m_1, m_2, ..., mn)$을, 상기 암호화는, n차 정방행렬인 행렬 P를 선택하고, 상기 공개키에 포함된 상기 행렬 S, B, 및 상기 정수 m 및 상기 행렬 P를 이용하여 상기 이진평문을 암호화하는 것을 특징으로 한다.

[0024] 또한, 상기 행렬 P의 구성요소 $p_{ij}(1\leq i,j\leq n)$는 상기 정수 m보다 작은 정수로 구성되고, 상기 이진평문 암호화는, 아래와 같은 수학식 3을 이용하여 암호화하는 것을 특징으로 한다.

[0025] [수학식 3]

[0026] $(SP+B)M^T \equiv C^T \pmod m$

[0027] 여기서, M은 이진평문을 나타내고, C^T는 암호문을 나타낸다.

[0028] 또한, 상기 비밀키를 이용하여 암호문 C^T을 복호화하되, 상기 복호화는 상기 암호문에 비밀키를 이용하여 복호중간값을 획득하고, 상기 복호중간값을 이진평문으로 복호화하는 것을 특징으로 한다.

[0029] 또한, 상기 복호중간값 $\alpha \equiv a_1m_1 + a_2m_2 + ... + anmn \pmod m$이고, 상기 복호중간값을 획득하는 아래와 같은 수학식 4를 이용하여 암호화하는 것을 특징으로 한다.

[0030] [수학식 4]

[0031] $KC^T \equiv \alpha \pmod m$

[0032] 여기서, C^T는 암호문을 나타내고, α는 복호중간값을 나타낸다.

[0033] 또한, 상기 복호중간값을 이진평문으로 복호화는, 초월증가수열의 특징을 이용하여 복호화하는 것을 특징으로 한다.

발명의 효과

[0034] 본 발명의 실시예들에 따르면 다음과 같은 효과를 기대할 수 있다.

[0035] n차 정방행렬을 이용하여 암호화에 사용되는 비밀키, 공개키를 생성하고 암호화 시점에 임의의 n차 정방행렬 P를 생성하고, 사용함으로써 일회성 암호통신 형태의 암호문을 생성하게 되어 비밀키의 유추가 어려운 효과가 있다.

[0036] 또한, n차 정방행렬의 n을 1024으로 구성할 경우 초월증가수열로 구성된 개인키를 유추하기 어려운 효과가 있다.

[0037] 본 발명의 실시예들에서 얻을 수 있는 효과는 이상에서 언급한 효과들로 제한되지 않으며, 언급하지 않은 또 다른 효과들은 이하의 본 발명의 실시 예들에 대한 기재로부터 본 발명이 속하는 기술분야에서 통상의 지식을 가진 자에게 명확하게 도출되고 이해될 수 있다. 즉, 본 발명을 실시함에 따른 의도하지 않은 효과들 역시 본 발명의 실시예들로부터 당해 기술분야의 통상의 지식을 가진 자에 의해 도출될 수 있다.

도면의 간단한 설명

[0038] 이하에 첨부되는 도면들은 본 발명에 관한 이해를 돕기 위한 것으로, 상세한 설명과 함께 본 발명에 대한 실시예들을 제공한다. 다만, 본 발명의 기술적 특징이 특정 도면에 한정되는 것은 아니며, 각 도면에서 개시하는 특징들은 서로 조합되어 새로운 실시 예로 구성될 수 있다. 각 도면에서의 참조 번호(reference numerals)들은 구조적 구성요소(structural elements)를 의미한다.

도 1은 본 발명이 적용되는 일 실시예로서, 공개키 및 비밀키를 선택(결정)하는 방법에 대한 것이다.

도 2는 본 발명이 적용되는 일 실시예로서, 공개키를 이용하여 이진평문을 암호화하는 방법을 나타낸다.

도 3은 본 발명이 적용되는 일 실시예로서, 비밀키를 이용하여 암호문을 복호화하는 방법을 나타낸다.

발명을 실시하기 위한 구체적인 내용

[0039] 본 발명에서 사용되는 용어는 본 발명에서의 기능을 고려하면서 가능한 현재 널리 사용되는 일반적인 용어들을 선택하였으나, 이는 당 분야에 종사하는 기술자의 의도 또는 판례, 새로운 기술의 출현 등에 따라 달라질 수 있다. 또한, 특정한 경우는 출원인이 임의로 선정한 용어도 있으며, 이 경우 해당되는 발명의 설명 부분에서 상세히 그 의미를 기재할 것이다. 따라서 본 발명에서 사용되는 용어는 단순한 용어의 명칭이 아닌, 그 용어가 가지는 의미와 본 발명의 전반에 걸친 내용을 토대로 정의되어야 한다.

[0040] 이하의 실시 예들은 본 발명의 구성요소들과 특징들을 소정 형태로 결합한 것들이다. 각 구성요소 또는 특징은 별도의 명시적 언급이 없는 한 선택적인 것으로 고려될 수 있다. 각 구성요소 또는 특징은 다른 구성요소나 특징과 결합되지 않은 형태로 실시될 수 있으며, 일부 구성요소들 및/또는 특징들을 결합하여 본 발명의 실시 예를 구성할 수도 있다. 또한, 본 발명의 실시예들에서 설명되는 동작들의 순서는 변경될 수 있다. 어느 실시 예의 일부 구성이나 특징은 다른 실시예에포함될 수 있고, 또는 다른 실시 예의 대응하는 구성 또는 특징과 교체될 수 있다.

[0041] 도면에 대한 설명에서, 본 발명의 요지를 흐릴 수 있는 절차 또는 단계 등은 기술하지 않았으며, 당업자의 수준에서 이해할 수 있을 정도의 절차 또는 단계는 또한 기술하지 아니하였다.

[0042] 명세서 전체에서, 어떤 부분이 어떤 구성요소를 "포함(comprising 또는 including)"한다고 할 때, 이는 특별히 반대되는 기재가 없는 한 다른 구성요소를 제외하는 것이 아니라 다른 구성요소를 더 포함할 수 있는 것을 의미한다. 또한, 명세서에 기재된 "...부", "...기", "모듈(module)" 등의 용어는 적어도 하나의 기능이나 동작을 처리하는 단위를 의미하며, 이는 하드웨어나 소프트웨어 또는 하드웨어 및 소프트웨어의 결합으로 구현될 수 있다. 또한, "일(a 또는 an)", "하나(one)", "그(the)" 및 유사 관련어는 본 발명을 기술하는 문맥에 있어서(특히, 이하의 청구항의 문맥에서) 본 명세서에 달리 지시되거나 문맥에 의해 분명하게 반박되지 않는 한, 단수 및 복수 모두를 포함하는 의미로 사용될 수 있다

[0043] 이하, 본 발명에 따른 바람직한 실시 형태를 첨부된 도면을 참조하여 상세하게 설명한다. 첨부된 도면과 함께 이하에 개시될 상세한 설명은 본 발명의 예시적인 실시 형태를 설명하고자 하는 것이며, 본 발명이 실시될 수 있는 유일한 실시형태를 나타내고자 하는 것이 아니다.

[0044] 또한, 본 발명의 실시예들에서 사용되는 특정 용어들은 본 발명의 이해를 돕기 위해서 제공된 것이며, 이러한 특정 용어의 사용은 본 발명의 기술적 사상을 벗어나지 않는 범위에서 다른 형태로 변경될 수 있다.

[0045] 본 발명을 실시하기 위한 구체적인 내용의 설명에 앞서 이해의 편의를 위해 본 발명이 해결하려는 과제의 해결방안의 개요를 우선 제시한다.

[0046] 공개키 암호화 방식에는 모듈로 승산 연산(modulo multiplication operation)이 반드시 포함된다. 공개키 암호화 방식은 공개키와 비밀키에 대해 모듈로 멱승(modulo exponentiation)을 취하여 암호화 및 복호화가 이루어지며, 모듈로 멱승은 모듈로 승산을 기본 연산으로 하여 이루어지기 때문이다. 모듈로 승산 연산은 연속된 덧셈 연산으로부터 수행될 수 있으며, 연산 시에 캐리(carry)의 지연을 고려하지 않아도 되는 장점이 있는 몽고메리 승산 연산(Montgomery multiplication operation)을 주로 사용한다. 몽고메리 승산은 모듈로 승산을 가장 효율적으로 수행하는 알고리즘으로 알려져 있다.

[0047] 암호화 모듈(복호화 모듈도 병행됨)의 구현을 위한 기존의 방식은 모두 하드웨어적인 처리(하드웨어적인 구현 효율화) 또는 소프트웨어적인 처리(소프트웨어 최적화) 중 어느 한 처리 측면에서만의 구현 내지 개선을 염두하

고 있었으며, 각 처리에 관해서는 이미 다수의 기법들이 제안되거나 실시되고 있다.

[0048] 위에서 언급한 바와 같이 스마트카드의 암호화/복호화 모듈은 공개키 암호화 방식에 의해 이루어짐이 압도적이며, 이 암호화 방식에는 모듈로 승산 연산이 반드시 수반된다. 한편 공개키 암호화와 관련된 제반 연산에 있어서 모듈로 승산 연산이 가장 많은 연산량을 차지하기 때문에 공개키 암호화/복호화 방식의 소요 시간(암호화/복호화 속도)은 모듈로 승산 연산에 소요되는 시간에 의해 좌우된다.

[0049] 본 발명은 암호화/복호화 방법을 하드웨어적인 처리와 소프트웨어적인 처리를 동시에 이용하여 실현할 수 있으며, 성능(속도) 향상과 직접 관련된 측면에서는 하드웨어적인 처리로, 보안성 확보를 위한 측면에서 는 소프트웨어적인 처리로 분리하여 암호화/복호화 모듈을 구현할 수 있다. 아울러 이러한 분리 구현은 어느 한 측 면에서의 변경이 발생하여도 나머지 측면에는 전혀 영향을 주지 않도록 구현될 수 있다.

[0050] 이를 위해 본 발명은 공개키 암호화 방식으로 암호화/복호화 모듈이 구현되는 방법 및 장치에 있어서 소프트웨어적인 처리가 요구되며 아울러 소프트웨어적인 처리만으로도 성능(속도)에 지장이 없고 하드웨어적인 처리와는 무관한 키 값의 업데이트(저장) 및 암호화/복호화 알고리즘은 소프트웨어적인 처리로 구현하고, 성능(속도)과 직접 관련되 고 소프트웨어적인 처리와는 무관한 모듈로 승산 연산은 하드웨어적인 처리로 구현하여 두 처리 간 핸드셰이킹 (handshaking)을 통해 스마트카드에 있어서의 암호화/복호화 모듈을 구현될 수 있다.

[0051] 암호화/복호화 알고리즘의 구현 및 설정, 키 값의 업데이트(저장)와 입력값(예를 들어 사용자 ID 등 고유 정보)의 입력을 위한 외부 인터페이스의 구현은 위에서 언급한 바와 같이 소프트웨어적인 처리에 의해 이루어진다. 외부 인터페이스는 소정의 소프트웨어 모듈로 구현되며 일종의 에뮬레이터를 통해 CPU 와 통신한다. 외부 인터페이스를 통해 업데이트된 키 값 또는 입력값도 CPU의 내부 메모리에 또는 CPU를 통해 외부 메모리에 업로드될 수 있다.

[0052] 암호화/복호화를 위한 알고리즘으로는 공개키 암호화 방식을 이용할 수 있으며, 공개키 암호화 방식의 여러 방식 중에 RSA(Rivest, Shamir, Adleman) 암호화 방식을 이용할 수 있다. 암호화/복호화 알고리즘의 소프트웨어적인 처리에 의 한 구현은 효율성을 위해 컴퓨터 프로그래밍 언어의 일종인 어셈블리어(assembly language)에 의하여 구현될 수 있다.

[0053] 한편 암호화/복호화 알고리즘의 소프트웨어적인 처리에 의한 구현의 효율성은 알고리즘의 프로그래밍 기법을 통해서도 이룰 수 있는 바, 본 발명은 소위 loop unrolling 기법을 통해 암호화/복호화 알고리즘의 프로그래밍될 수 있다. 암호화/복호화 알고리즘의 경우 암호화/복호화에 수반되는 소정의 연산을 행함에 있어 통상 루프 알고리즘을 수반하는데(C 언어에서는 for문으로 표현됨), 루프 알고리즘은 암호화/복호화에 수반되는 연산의 소요 시간을 증가시켜 암호화/복호화 속도를 저하시키는 주된 원인으로 지목되어 왔으며 특히 소프트웨어적인 처리에만 의한 암호화/복호화 모듈의 구현에 있어서는 더욱 그러했다.

[0054] 이러한 루프 알고리즘의 문제를 완화하기 위한 프로그래밍 기법이 loop unrolling 기법이며, 이는 반복 처리가 요구되는 연산에 루프 처리가 아닌 순차적 처리(sequential process)를 통해 연산을 수행하는 기법이다. 이 기법은 순차적 처리에 근간을 두므로 프로그램 코드의 크기 상승을 가져오는 단점은 있으나, 처리 속도 향상의 측면에서 루프 처리에 비해 커다란 이점을 가져 빠른 처리 속도가 요구되는 응용에 흔히 사용하는 프로그래밍 기법이다.

[0055] 공개키 암호화 방식에는 모듈로 승산 연산이 반드시 포함됨을 위에서 언급했는데, 모듈로 승산의 연산량은 공개키 암호화 방식에 의한 암호화/복호화에 소요되는 연산량의 90% 이상을 차지하며, 연산량 자체가 너무 많아 이를 소 프트웨어적인 처리를 통해 구현하는 것은 성능(속도) 향상 측면에서는 아무런 실효성이 없으므로, 본 발명에서는 공개키 암호화 방식(RSA 방식)에 의한 암호화/복호화 알고리즘 중 모듈로 승산 연산 부분을 하드웨어적인 처리를 통해 구현할 수 있다. 하드웨어적인 처리란 일단 구현이 이루어지고 나면 변경이 되지 아니함(또는 변경이 불가능함)을 의미하며, 아울러 소프트웨어적인 처리 측면에서의 변경이 발생하더라도 그 영향을 받지 않는다. 즉, 소프트 웨어적인 처리 측면에서의 변경이 발생하더라도 하드웨어적인 처리로 구현된 모듈로 승산 연산을 위한 입력값은 변하지 아니하므로 영향을 받지 아니한다는 의미이다.

[0056] 이하에서는 본 발명의 일 실시예에 따른 공개키 및 비밀키 생성방법에 대해서 설명하도록 한다.

[0057] 도 1은 본 발명이 적용되는 일 실시예로서, 공개키 및 비밀키를 선택(결정)하는 방법에 대한 것이다.

[0058] 이진평문의 블록 단위와 정방행렬의 크기에 이용되는 n을 선택할 수 있다(S110).

[0059] n은 정수로서, 1024보다 큰 양의 정수로 선택될 수 있다.

[0060] 초월증가수열로 이루어진 행렬 A와 a1 + a2 + ... + an < m을 만족하는 m을 선택할 수 있다(S120).

[0061] 여기서, 초월증가수열은 n번째항(an)이 a_1부터 a_{n-1}까지의 합보다 큰 수열을 나타낸다. 예를들어, 초월증가수열 4번째 항인 a_4은 $a_1 + a_2 + a_3$인 값보다 큰 값으로 선택될 수 있다.

[0062] 행렬 A는 1부터 n번째 항까지의 초월증가수열로 구성된 행렬로서, A=(a_1, a_2, ..., an)으로 구성될 수 있다.

[0063] m은 1부터 n번째 항까지의 합보다 큰 정수를 나타낸다.

[0064] m보다 작은 정수로 구성되고, 서로 상관 관계에 있는 ki, si를 선택할 수 있다(S130).

[0065] ki, si(1≤i≤n) ∈ Zm으로 선택되고, 여기서, Zm은 m보다 작은 임의의 정수를 나타내는 것으로서, ki, si(1≤i≤n)의 각 요소는 m보다 작은 임의의 정수 또는 양의 정수로 구성될 수 있다.

[0066] 또한, ki와 si는 서로 상관 관계를 가지고 선택될 수 있다. 예를 들어, ki와 si의 상관관계는 아래와 같은 수학식 2처럼 나타낼 수 있다.

[0067] [수학식 2]

[0068] $k_1s_1 + k_2s_2 + \ldots + knsm \equiv 0 \pmod m$

[0069] ki와 si를 이용하여 행렬 K와 행렬 S가 선택될 수 있다(S140).

[0070] 행렬 K는 상기 선택된 요소 ki에 기초하여, K=(k1, k2, ..., kn)으로 구성될 수 있다.

[0071] 행렬 S는 상기 선택된 요소 si에 기초하여, 모든 열이 $\begin{pmatrix} s_1 \\ s_2 \\ \cdot \\ \cdot \\ \cdot \\ s_n \end{pmatrix}$으로 구성된 n차 정방행렬로 구성될 수 있다.

[0072] 행렬 A, K, 정수 m을 이용하여 n차 정방행렬 B를 선택할 수 있다(S150).

[0073] 행렬 B는 n차 정방행렬로서, 행렬 A, K, 정수 m을 아래와 같은 수학식 3을 만족하는 행렬로 구성될 수 있다.

[0074] [수학식 3]

[0075] $KB \equiv A \pmod m \equiv (a_1, a_2, \ldots, an) \pmod m$

[0076] n, S, B를 공개키로 선택하고, m, A, K를 비밀키로 선택할 수 있다(S160).

[0077] 여기서, 공개키는 이진평문을 암호화하는데 이용되는 요소들을 나타낸다. 공개키는 이진평문을 암호화하려는 장치에 전송될 수 있다.

[0078] 비밀키는 암호화된 이진평문을 복호화하는데 이용되는 요소들을 나타낸다. 암호키는 암호화된 복호화하려는 장치에 전송될 수 있다.

[0079] 이하에서는 공개키를 이용하는 암호화 과정에 대해서 설명하도록 한다.

[0080] 도 2는 본 발명이 적용되는 일 실시예로서, 공개키를 이용하여 이진평문을 암호화하는 방법을 나타낸다.

[0081] n차 정방행렬 P를 선택할 수 있다(S210).

[0082] P=(p_{ij})(p_{ij}∈Zm, 1≤i,j≤n)를 임의로 선택할 수 있다. Zm은 m보다 작은 정수를 나타낸다. 그리고, p_{ij}는 정수로서, m보다 작은 정수로 선택될 수 있다.

[0083] 이진평문 M을 행렬 P 및 공개키를 이용하여 암호화할 수 있다(S220).

[0084] 이진평문 M은 M=(m1, m2, 쪋, mn), mi∈{0, 1}으로 구성될 수 있다.

[0085] 그리고, 이진평문 M은 아래와 같은 수학식 4에 의하여 암호화될 수 있다.

[0086] [수학식 4]

[0087] $(SP+B)M^T \equiv C^T \pmod m$

[0088] 상기 수학식에서 S, B, m은 공개키를 나타낸다.

[0089] 그리고, M은 이진평문을 나타낸다.

[0090] mod는 모듈레이션 연산을 나타낸다.

[0091] C^T는 암호문을 나타낸다.

[0092] 이하에서는 비밀키를 이용하는 암호화 과정에 대해서 설명하도록 한다.

[0093] 도 3은 본 발명이 적용되는 일 실시예로서, 비밀키를 이용하여 암호문을 복호화하는 방법을 나타낸다.

[0094] 암호문에 비밀키를 이용하여 복호중간값을 획득할 수 있다(S310).

[0095] 복호중간값은 비밀키를 곱하여 암호문을 복호화하는 과정에서 생성되는 값을 나타낸다. 복호중간값은 암호문 C^T의 왼쪽에 비밀키 행렬 K를 곱하여 획득할 수 있다. 복호중간값은 아래와 같은 수학식 5을 이용하여 획득될 수 있다.

[0096] [수학식 5]

[0097] $KC^T \equiv \alpha \pmod m$

[0098] 여기서, $\alpha \equiv a_1m_1 + a_2m_2 + \ldots + anmn \pmod m$를 나타낸다.

[0099] $\alpha \equiv a_1m_1 + a_2m_2 + \ldots\ldots + anmn \pmod m$임은 아래와 같이 증명할 수 있다.

[0100] $\alpha \equiv KC^T \equiv K\{(SP+B)M^T\} \equiv (KS)PM^T + (KB)M^T \equiv 0 + (KB)M^T$

[0101] $\equiv (KB)M^T \equiv (a_1\ a_2\ \ldots\ a_n)\begin{pmatrix} m_1 \\ m_2 \\ \cdot \\ \cdot \\ m_n \end{pmatrix} \equiv a_1m_1 + a_2m_2 + \ldots + anmn \pmod m$

[0102] 복호중간값을 초월증가수열의 성질을 이용하여 이진평문으로 복호화할 수 있다(S320).

[0103] 복호중간값 α는 $a_1m_1 + a_2m_2 + \ldots + anmn \pmod m$으로 구성되고, 여기서, a_1, a_2, ..., an은 초월증가수열로서, n번째 항이 1번째 항부터 n-1번째 항까지의 합보다 크기 때문에, 연산을 통해 이진 평문 m_1, m_2, ..., mn을 획득할 수 있다. 따라서, 복호중간값을 초월증가수열의 성질을 통해 이진평문으로 복호화할 수 있다.

[0104] 이하에서는 공개키 암호알고리즘을 이용한 암호화/복호화 방법이 적용된 장치의 구성에 대해서 설명하도록 한다.

[0105] 암호화/복호화 장치는 적어도 통신부, 메모리, 프로세서를 포함할 수 있다.

[0106] 통신부는 이진평문, 암호문, 공개키, 비밀키 등을 전송하기 위해 다른 기기들과 통신 신호를 송신 및 수신하도록 구성될 수 있다. 여기서, 통신부는 송신부와 수신부로 구성될 수 있다.

[0107] 프로세서는 각각 동작을 지시(예를 들어, 제어, 조정, 관리 등)한다. 각각의 프로세서들은 프로그램 코드들 및 데이터를 저장하는 메모리들과 연결될 수 있다. 메모리는 프로세서에 연결되어 오퍼레이팅 시스템, 어플리케이션, 및 일반 파일(general files)들을 저장한다.

[0108] 본 발명의 프로세서는 상기 설명한 공개키 암호알고리즘을 이용한 암호화/복호화 방법으로, 도 1, 도 2 내지 도 3에서 언급한 각 단계들을 구현할 수 있다.

[0109] 본 발명의 프로세서는 컨트롤러(controller), 마이크로 컨트롤러(microcontroller), 마이크로 프로세서(microprocessor), 마이크로 컴퓨터(microcomputer) 등으로도 호칭될 수 있다. 한편, 프로세서(820, 860, 900)는 하드웨어(hardware) 또는 펌웨어(firmware), 소프트웨어, 또는 이들의 결합에 의해 구현될 수 있다.

[0110] 하드웨어를 이용하여 본 발명의 실시 예를 구현하는 경우에는, 본 발명을 수 행하도록 구성된 ASICs(application specific integrated circuits) 또는 DSPs(digital signal processors), DSPDs(digital signal processing devices), PLDs(programmable logic devices), FPGAs(field programmable gate arrays) 등이 프로세서(820, 870)에 구비될 수 있다.

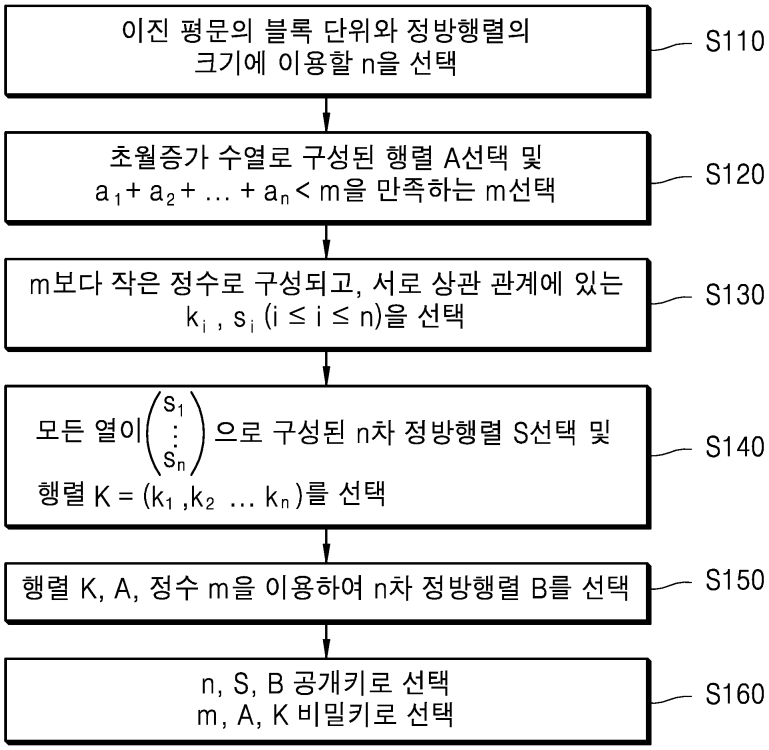
[0111] 한편, 상술된 실시예들은 컴퓨터에 의하여 실행 가능한 명령어 및 데이터를 저장하는 컴퓨터로 읽을 수 있는 기록매체의 형태로 구현될 수 있다. 상기 명령어 및 데이터 중 적어도 하나는 프로그램 코드의 형태로 저장될 수 있으며, 프로세서에 의해 실행되었을 때, 소정의 프로그램 모듈을 생성하여 소정의 동작을 수행할 수 있다.

[0112] 컴퓨터로 읽을 수 있는 기록매체란, 예를 들어 하드디스크 등과 같은 마그네틱 저장매체, CD 및 DVD 등과 같은 광학적 판독매체 등을 의미할 수 있으며, 네트워크를 통해 접근 가능한 서버에 포함되는 메모리를 의미할 수도 있다. 예를 들어, 컴퓨터로 읽을 수 있는 기록매체는 전자 장치 또는 서버의 메모리가 될 수도 있다. 또한, 전자 장치 또는 서버와 네트워크를 통하여 연결된 단말, 서버 등에 포함되는 메모리가 될 수도 있다.

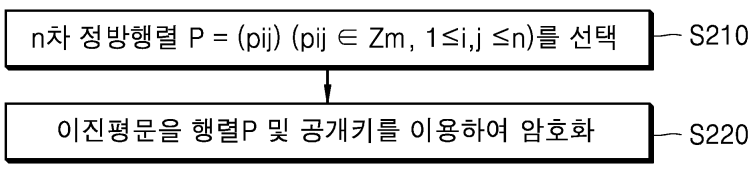
[0113] 이상과 첨부된 도면을 참조하여 실시예를 설명하였지만, 일 실시예가 속하는 기술분야에서 통상의 지식을 가진 자는 일 실시예가 그 기술적 사상이나 필수적인 특징을 변경하지 않고서 다른 구체적인 형태로 실시될 수 있다는 것을 이해할 수 있을 것이다. 그러므로 이상에서 기술한 실시예들은 모든 면에서 예시적인 것이며 한정적이 아닌 것으로 이해해야만 한다.

도면

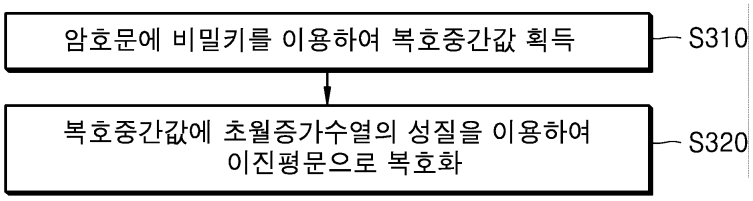
도면1



도면2



도면3



【심사관 직권보정사항】

【직권보정 1】

【보정항목】 청구범위

【보정세부항목】 청구항 5

【변경전】

상기 행렬 S, B, 및

【변경후】

상기 정방행렬 S, B, 및

【직권보정 2】

【보정항목】 청구범위

【보정세부항목】 청구항 1,10

【변경전】

상기 행렬 B, S를 공개키로 선택하고,

【변경후】

상기 정방행렬 B, S를 공개키로 선택하고,