



(19)대한민국특허청(KR)
(12) 공개특허공보(A)

(51) 。 Int. Cl.

H04L 9/30 (2006.01)

H04L 9/08 (2006.01)

H04L 9/32 (2006.01)

(11) 공개번호 10-2007-0064121

(43) 공개일자 2007년06월20일

(21) 출원번호 10-2005-0124708

(22) 출원일자 2005년12월16일

심사청구일자 2005년12월16일

(71) 출원인 고려대학교 산학협력단
서울 성북구 안암동5가1 고려대학교 내

(72) 발명자 임종인
서울 종로구 내수동 95 삼성파크팰리스 101-901
김창한
서울 서초구 반포동 20-9 주공아파트 328-402호
박영호
서울 광진구 광장동 576 현대9차아파트 902동 1203호
장남수
서울 마포구 성산2동 200-84
김태현
서울 강서구 화곡2동 846-19
임대성
경기 안산시 상록구 이동 530-14 301호
지성연
경기 수원시 영통구 매탄2동 111-97
김성경
서울 성북구 안암동5가 11-5번지 리베르타 302호
윤택영
경기 성남시 중원구 성남동 3020번지

(74) 대리인 현중철

전체 청구항 수 : 총 15 항

(54) 효율적으로 이중 복호화 기능을 제공하면서 사용자의 프라이버시를 보호할 수 있는 공개키 암호화 방법

(57) 요약

본 발명은 이중 복호화 기능을 효율적으로 제공하면서 사용자의 프라이버시를 보호할 수 있는 공개키 암호화 방법에 관한 것으로서, 본 발명의 공개키 암호화 방법은, 복호화 주체에 따른 선택적 복호 권한 부여를 위한 암호화에 필요한 공개키 및 비밀키를 포함하는 키 파라미터를 생성하는 단계, 복호 권한 부여 여부에 따라 생성된 서로 다른 키 파라미터를 기초로 주어진 평문 m에 대한 암호화를 수행하는 단계, 암호화가 수행된 평문 m을 소정 통신 채널을 전송하는 단계, 암호화가 수행

된 평문 m 을 수신 받으면 암호화가 수행된 평문 m 에 대한 복호화 모드의 수행 여부를 판별하는 단계, 및 암호화가 수행된 평문 m 에 대한 복호화 모드가 수행되면 복호화 주체에 따른 복호 권한 부여에 따라 설정된 알고리즘을 통해 평문 m 을 복호화를 수행하는 단계를 포함한다. 이에 따라, 복호화를 위해 필요한 비밀키에 대한 접근 권한을 사용자와 시스템 관리자에 대해 차별적으로 부여함으로써, 사용자의 비밀키를 완전히 노출하지 않으면서 시스템 관리자에 대한 사용자의 프라이버시를 보호받을 수 있다.

대표도

도 1

특허청구의 범위

청구항 1.

이중 복호화 기능을 효율적으로 제공하면서 사용자의 프라이버시를 보호할 수 있는 공개키 암호화 방법에 있어서,

복호화 주체에 따른 선택적 복호 권한 부여를 위한 암호화에 필요한 공개키 및 비밀키를 포함하는 키 파라미터를 생성하는 단계;

상기 생성된 키 파라미터를 기초로 주어진 평문 m 에 대한 암호화를 수행하는 단계;

상기 암호화가 수행된 평문 m 을 소정 통신 채널로 전송하는 단계;

상기 암호화가 수행된 평문 m 을 수신 받으면, 상기 암호화가 수행된 평문 m 에 대한 복호화 모드의 수행 여부를 판별하는 단계; 및

상기 암호화가 수행된 평문 m 에 대한 복호화 모드가 수행되면, 상기 복호화 주체에 따라 설정된 알고리즘을 통해 상기 평문 m 을 복호화를 수행하는 단계를 포함하는 것을 특징으로 하는 공개키 암호화 방법.

청구항 2.

제 1항에 있어서,

상기 키 파라미터를 생성하는 단계는,

k 비트의 두 소수 p, q 를 생성하는 단계;

상기 생성한 k 비트를 갖는 두 수 p, q 에 대해, 수학식 $n=p^2q$ 을 만족하는 값(n)을 산출하는 단계;

수학식 $ord(g^{p-1} \bmod(p^2))=p$ 를 만족하는 임의의 수 $g(g \in Z_n)$ 를 생성하는 단계;

임의의 $k-1$ 비트의 수 a 를 생성하는 단계; 및

함수 $h=g^a \bmod(n)$ 를 계산하는 단계를 포함하는 것을 특징으로 하는 공개키 암호화 방법.

청구항 3.

제 2항에 있어서,

상기 키 파라미터를 생성하는 단계를 통해 공개키가 (n, g, h, k) 이고 대응되는 비밀키가 a 인 키 파라미터를 획득하는 것을 특징으로 하는 공개키 암호화 방법.

청구항 4.

제 3항에 있어서,

상기 p, q 는 시스템 관리자에게 주어지는 마스터키 정보인 것을 특징으로 하는 공개키 암호화 방법.

청구항 5.

제 4항에 있어서,

상기 암호화 수행 단계는,

선택된 평문 $m(m \in Z_n)$ 을 입력 받는 단계;

상기 $k-1$ 비트의 난수 r 을 생성하는 단계;

수학식 $A = g^r \bmod(n)$, 및 수학식 $B = h^r m \bmod(n)$ 를 통해 각각 A 값 및 B 값을 산출하는 단계; 및

상기 산출한 A 값 및 B 값을 수학식 $C = (A, B)$ 에 대입함으로써 평문 m 에 대한 암호화를 완료하는 단계를 포함하는 것을 특징으로 하는 공개키 암호화 방법.

청구항 6.

제 5항에 있어서,

상기 복호화 수행 단계는,

상기 복호화 모드가 수행되면, 복호 주체가 암호화를 수행한 상기 사용자인지 상기 시스템 관리자인지를 판별하는 단계;

상기 복호 주체가 사용자이면, 암호화시 사용한 비밀키 a 를 획득하는 단계; 및

상기 비밀키 a 를 수학식 $m = B/A^a \bmod(n)$ 에 대입하여 상기 평문 m 을 복호화하는 단계를 포함하는 것을 특징으로 하는 공개키 암호화 방법.

청구항 7.

제 6항에 있어서,

상기 복호 주체가 시스템 관리자이면, 수학식 $h_p = h^{p-1} \bmod(p^2)$ 및 $g_p = g^{p-1} \bmod(p^2)$ 를 통해 각각 h_p 및 g_p 값을 획득하는 단계;

상기 획득한 값 h_p 및 g_p 를 수학식 $a = L(h_p)/L(g_p) \bmod(p)$ 에 대입하여 비밀키 a 를 복원하는 단계; 및

상기 복원된 비밀키 a 를 수학적식 $m=B/A^a \bmod(n)$ 에 대입하여 상기 평문 m 을 복호화하는 단계를 포함하는 것을 특징으로 하는 공개키 암호화 방법.

청구항 8.

제 1항에 있어서,

상기 키 파라미터를 생성하는 단계는,

k 비트의 두 소수 p, q 를 생성하는 단계;

상기 생성한 k 비트를 갖는 두 수 p, q 에 대해, 수학적식 $n=p^2q$ 을 만족하는 값(n)을 산출하는 단계;

수학적식 $ord(g^{p-1} \bmod(p^2))=p$ 를 만족하는 임의의 수 $g(g \in Z_n)$ 를 생성하는 단계;

시스템 관리자에 대한 복호 허용 여부를 결정하는 단계;

상기 시스템 관리자에 대한 복호가 허용된 경우, 임의의 $k-1$ 비트의 수 a 를 생성하고 함수 $h=g^a \bmod(n)$ 를 계산하는 단계; 및

상기 시스템 관리자에 대한 복호가 허용되지 않은 경우, 임의의 $t(t > k)$ 비트의 수 a 를 생성하고 $h=g^a \bmod(n)$ 을 계산하는 단계를 포함하는 것을 특징으로 하는 공개키 암호화 방법.

청구항 9.

제 8항에 있어서,

상기 시스템 관리자에 대한 복호가 허용된 경우 생성되는 상기 키 파라미터는, 공개키가 (n, g, h, k) 이고 대응되는 비밀키가 a 인 것을 특징으로 하는 공개키 암호화 방법.

청구항 10.

제 8항에 있어서,

상기 시스템 관리자에 대한 복호가 허용되지 않은 경우 생성되는 상기 키 파라미터는, 공개키가 (n, g, h, t) 이고 대응되는 비밀키가 a 인 것을 특징으로 하는 공개키 암호화 방법.

청구항 11.

제 8항에 있어서,

상기 p, q 는 시스템 관리자에게 주어지는 마스터키 정보인 것을 특징으로 하는 공개키 암호화 방법.

청구항 12.

제 8항에 있어서,

상기 암호화 수행 단계는,

선택된 평문 $m(m \in \mathbb{Z}_n)$ 을 입력 받는 단계;

상기 시스템 관리자에 대한 복호 허용 여부를 판별하는 단계;

상기 시스템 관리자에 대한 복호가 허용된 경우 상기 $k-1$ 비트의 난수 r 을 생성하고, 복호가 허용되지 않은 경우 상기 t 비트의 난수 r 을 생성하는 단계;

수학식 $A = g^r \bmod(n)$, 및 수학식 $B = h^r m \bmod(n)$ 를 통해 각각 A 값 및 B 값을 산출하는 단계; 및

상기 산출한 A 값 및 B 값을 수학식 $C=(A,B)$ 에 대입함으로써 평문 m 에 대한 암호화를 완료하는 단계를 포함하는 것을 특징으로 하는 공개키 암호화 방법.

청구항 13.

제 12항에 있어서,

상기 복호화 수행 단계는,

상기 복호화 모드가 수행되면, 복호 주체가 암호화를 수행한 상기 사용자인지 상기 시스템 관리자인지를 판별하는 단계;

상기 복호 주체가 사용자이면, 암호화시 사용한 비밀키 a 를 획득하는 단계; 및

상기 비밀키 a 를 수학식 $m = B/A^a \bmod(n)$ 에 대입하여 상기 평문 m 을 복호화하는 단계를 포함하는 것을 특징으로 하는 공개키 암호화 방법.

청구항 14.

제 13항에 있어서,

상기 복호 주체가 시스템 관리자이면, 상기 시스템 관리자에 대한 복호 허용 여부를 판별하는 단계; 및

상기 시스템 관리자에 대한 복호가 허용되지 않은 것으로 판단되면, 상기 복호화 모드를 종료하는 단계를 포함하는 것을 특징으로 하는 공개키 암호화 방법.

청구항 15.

제 14항에 있어서,

상기 시스템 관리자에 대한 복호가 허용된 것으로 판단되면, 수학식 $h_p = h^{p-1} \bmod(p^2)$ 및 $g_p = g^{p-1} \bmod(p^2)$ 를 통해 각각 h_p 및 g_p 값을 획득하는 단계;

상기 획득한 값 h_p 및 g_p 를 수학식 $a = L(h_p)/L(g_p) \bmod(p)$ 에 대입하여 비밀키 a 를 복원하는 단계; 및

상기 복원된 비밀키 a 를 수학적식 $m = B/A^a \bmod(n)$ 에 대입하여 상기 평문 m 을 복호화하는 단계를 포함하는 것을 특징으로 하는 공개키 암호화 방법.

명세서

발명의 상세한 설명

발명의 목적

발명이 속하는 기술 및 그 분야의 종래기술

본 발명은 공개키 암호화 방법에 관한 것으로서, 보다 상세하게는, 이중 복호화 기능을 효율적으로 제공하면서 사용자의 프라이버시를 보호할 수 있는 기법을 제공하는 안전한 공개키 암호화 방법에 관한 것이다.

공개키 암호시스템은 암호를 통해서 안전한 통신 서비스를 제공하기 위한 도구로 많은 관심을 받아왔고 많은 연구가 진행되었다. 그러므로 안전한 통신 서비스를 제공하기 위한 도구로써 유용하게 사용될 수 있는 새로운 암호를 구성하는 것은 이론적인 관점에서뿐만 아니라 현실적인 관점에도 매우 중요하다.

그런데 종래의 암호화 방법에 대한 기술을 살펴보면, 일반적인 공개키 암호의 기능인 암호·복호화 기능을 효율적으로 제공하거나 새로운 난제를 기반으로 설계하는 것이 주를 이루고 있다. 이는 환, 유한 비가환군, 소수체, 타원곡선 그리고 브레이드 그룹에서 정의된 수학적 어려운 문제인 디피-헬만 가정(Diffie-Hellman assumption), 이산대수의 어려움 그리고 인수분해의 어려움 등을 기반으로 설계되어 있다. 또한 선택평문공격(Adaptive Chosen Plaintext Attack)에 안전하도록 구성하는 방법에 대한 개발도 제안되고 있다.

일반적으로, 암호화 방법은 정보통신망에서 다양한 정보가 네트워크를 통해서 교류될 때 안전한 통신을 제공하기 위한 도구로 사용되는데, 다양한 정보보호 서비스를 제공하기 위해서는 다양한 기능이 제공되는 암호화 방법의 개발이 중요하다. 기존의 암호화 방법에 대한 기술들에서는 이와 같은 다양한 기능에 대한 고려는 많이 이루어지지 않고 있다.

2003년도 브레슨(Bresson), 카탈라노(Catalano) 그리고 포앙쉐발(Pointcheval)은 이중 복호화 기법이라는 특성이 제공되는 암호화 기법을 제안하였다. 이러한 이중 복호화 기법은 다양한 프로토콜을 설계함에 있어 유용하게 사용될 수 있는 특성을 갖는다.

그런데 종래의 이중 복호화 특성을 제공하는 암호화 방법은 효율적인 암호·복호화 서비스를 제공하지 못한다. 그리고 이러한 암호화 시스템을 사용하는 사용자는 시스템의 관리자에 대한 프라이버시를 보장받지 못한다. 실제로, 시스템 관리자가 가지는 인수분해 정보를 통해서 개별 사용자의 암호문을 복원할 수 있고, 이러한 이유로 인해, 종래의 암호화 방법은 사용자의 시스템 관리자에 대한 프라이버시 침해의 우려가 있다.

발명이 이루고자 하는 기술적 과제

상기와 같은 문제점을 해결하기 위한 본 발명의 목적은, 사용자의 프라이버시를 보호할 수 있는 공개키 암호화 방법을 제공하는 데 있다.

본 발명의 다른 목적은, 이중 복호화 기능을 효율적으로 제공하면서 사용자의 프라이버시를 보호할 수 있는 공개키 암호화 방법을 제공하는 데 있다.

발명의 구성

상기와 같은 목적은 본 발명의 실시예에 따라, 이중 복호화 기능을 효율적으로 제공하면서 사용자의 프라이버시를 보호할 수 있는 공개키 암호화 방법에 있어서, 복호화 주체에 따른 선택적 복호 권한 부여를 위한 암호화에 필요한 공개키 및 비밀키를 포함하는 키 파라미터를 생성하는 단계; 상기 생성된 키 파라미터를 기초로 주어진 평문 m 에 대한 암호화를 수행하는 단계; 상기 암호화가 수행된 평문 m 을 소정 통신 채널로 전송하는 단계; 상기 암호화가 수행된 평문 m 을 수신 받으면, 상

기 암호화가 수행된 평문 m 에 대한 복호화 모드의 수행 여부를 판별하는 단계; 및 상기 암호화가 수행된 평문 m 에 대한 복호화 모드가 수행되면, 상기 복호화 주체에 따라 설정된 알고리즘을 통해 상기 평문 m 을 복호화를 수행하는 단계를 포함하는 공개키 암호화 방법에 의해 달성된다.

바람직하게는, 상기 키 파라미터를 생성하는 단계는, k 비트의 두 소수 p, q 를 생성하는 단계; 상기 생성한 k 비트를 갖는 두 수 p, q 에 대해, 수학적식 $n=p^2q$ 을 만족하는 값(n)을 산출하는 단계; 수학적식 $ord(g^{p-1} \bmod(p^2))=p$ 를 만족하는 임의의 수 $g(g \in Z_n)$ 를 생성하는 단계; 임의의 $k-1$ 비트의 수 a 를 생성하는 단계; 및 함수 $h=g^a \bmod(n)$ 를 계산하는 단계를 포함한다.

상기 키 파라미터를 생성하는 단계를 통해 공개키가 (n, g, h, k) 이고 대응되는 비밀키가 a 인 키 파라미터가 획득된다.

상기 p, q 는 시스템 관리자에게 주어지는 마스터키 정보이다.

바람직하게는, 상기 암호화 수행 단계는, 선택된 평문 $m(m \in Z_n)$ 을 입력 받는 단계; 상기 $k-1$ 비트의 난수 r 을 생성하는 단계; 수학적식 $A=g^r \bmod(n)$, 및 수학적식 $B=h^r m \bmod(n)$ 를 통해 각각 A 값 및 B 값을 산출하는 단계; 및 상기 산출한 A 값 및 B 값을 수학적식 $C=(A, B)$ 에 대입함으로써 평문 m 에 대한 암호화를 완료하는 단계를 포함한다.

바람직하게는, 상기 복호화 수행 단계는, 상기 복호화 모드가 수행되면, 복호 주체가 암호화를 수행한 상기 사용자인지 상기 시스템 관리자인지를 판별하는 단계; 상기 복호 주체가 사용자이면, 암호화시 사용한 비밀키 a 를 획득하는 단계; 및 상기 비밀키 a 를 수학적식 $m=B/A^a \bmod(n)$ 에 대입하여 상기 평문 m 을 복호화하는 단계를 포함한다.

한편, 본 실시예의 공개키 암호화 방법의 복호화 단계에서는, 상기 복호 주체가 시스템 관리자이면, 수학적식 $h_p=h^{p-1} \bmod(p^2)$ 및 $g_p=g^{p-1} \bmod(p^2)$ 를 통해 각각 h_p 및 g_p 값을 획득하는 단계; 상기 획득한 값 h_p 및 g_p 를 수학적식 $a=L(h_p)/L(g_p) \bmod(p)$ 에 대입하여 비밀키 a 를 복원하는 단계; 및 상기 복원된 비밀키 a 를 수학적식 $m=B/A^a \bmod(n)$ 에 대입하여 상기 평문 m 을 복호화하는 단계를 포함한다.

바람직하게는, 상기 키 파라미터를 생성하는 단계는, 본 발명의 제2 실시예에 따라, k 비트의 두 소수 p, q 를 생성하는 단계; 상기 생성한 k 비트를 갖는 두 수 p, q 에 대해, 수학적식 $n=p^2q$ 을 만족하는 값(n)을 산출하는 단계; 수학적식 $ord(g^{p-1} \bmod(p^2))=p$ 를 만족하는 임의의 수 $g(g \in Z_n)$ 를 생성하는 단계; 시스템 관리자에 대한 복호 허용 여부를 결정하는 단계; 상기 시스템 관리자에 대한 복호가 허용된 경우, 임의의 $k-1$ 비트의 수 a 를 생성하고 함수 $h=g^a \bmod(n)$ 를 계산하는 단계; 및 상기 시스템 관리자에 대한 복호가 허용되지 않은 경우, 임의의 $t(t > k)$ 비트의 수 a 를 생성하고 $h=g^a \bmod(n)$ 을 계산하는 단계를 포함한다.

상기 시스템 관리자에 대한 복호가 허용된 경우 생성되는 상기 키 파라미터는, 공개키가 (n, g, h, k) 이고 대응되는 비밀키가 a 이다. 또한 상기 시스템 관리자에 대한 복호가 허용되지 않은 경우 생성되는 상기 키 파라미터는, 공개키가 (n, g, h, t) 이고 대응되는 비밀키가 a 이다.

상기 p, q 는 시스템 관리자에게 주어지는 마스터키 정보이다.

바람직하게는, 상기 암호화 수행 단계는, 본 발명의 제2 실시예에 따라, 선택된 평문 $m(m \in Z_n)$ 을 입력 받는 단계; 상기 시스템 관리자에 대한 복호 허용 여부를 판별하는 단계; 상기 시스템 관리자에 대한 복호가 허용된 경우 상기 $k-1$ 비트의 난수 r 을 생성하고, 복호가 허용되지 않은 경우 상기 t 비트의 난수 r 을 생성하는 단계; 수학적식 $A=g^r \bmod(n)$, 및 수학적식 $B=h^r m \bmod(n)$ 를 통해 각각 A 값 및 B 값을 산출하는 단계; 및 상기 산출한 A 값 및 B 값을 수학적식 $C=(A, B)$ 에 대입함으로써 평문 m 에 대한 암호화를 완료하는 단계를 포함한다.

바람직하게는, 상기 복호화 수행 단계는, 본 발명의 제2 실시예에 따라, 상기 복호화 모드가 수행되면, 복호 주체가 암호화를 수행한 상기 사용자인지 상기 시스템 관리자인지를 판별하는 단계; 상기 복호 주체가 사용자이면, 암호화시 사용한 비밀키 a 를 획득하는 단계; 및 상기 비밀키 a 를 수학적식 $m=B/A^a \bmod(n)$ 에 대입하여 상기 평문 m 을 복호화하는 단계를 포함한다.

바람직하게는, 본 발명의 공개키 암호화 방법의 복호화 단계에서는, 상기 복호 주체가 시스템 관리자이면, 상기 시스템 관리자에 대한 복호 허용 여부를 판별하는 단계; 및 상기 시스템 관리자에 대한 복호가 허용되지 않은 것으로 판단되면, 상기 복호화 모드를 종료하는 단계를 포함한다.

본 발명의 실시예에 따른 복호화 단계에서는, 상기 시스템 관리자에 대한 복호가 허용된 것으로 판단되면, 수학적식 $h_p=h^{p-1} \bmod(p^2)$ 및 $g_p=g^{p-1} \bmod(p^2)$ 를 통해 각각 h_p 및 g_p 값을 획득하는 단계; 상기 획득한 값 h_p 및 g_p 를 수학적식 $a=L(h_p)/L(g_p) \bmod(p)$ 에 대입하여 비밀키 a 를 복원하는 단계; 및 상기 복원된 비밀키 a 를 수학적식 $m=B/A^a \bmod(n)$ 에 대입하여 상기 평문 m 을 복호화하는 단계를 포함한다.

본 발명에 따르면, 본 발명의 이중 복호화 기능이 제공되는 암호화 방법에서는 복호화를 위해 필요한 비밀키 a 에 대한 접근 권한을 사용자와 시스템 관리자에 대해 차별적으로 부여함으로써, 사용자의 비밀키 a 를 완전히 노출하지 않으면서 시스템 관리자에 대한 개인 사용자의 프라이버시를 보호받을 수 있다. 또한, 일반적인 공개키 암호시스템에서 제공하는 이중 복호화 기능을 효율적으로 제공하고, 기존의 이중 복호화 기능이 제공되는 암호화 방법에서 시스템 관리자에 대해서 사용자의 프라이버시가 보호받지 못하는 것을 개선하여 사용자의 프라이버시를 보장하는 이중 복호화 기능을 제공할 수 있다.

이하, 본 발명의 바람직한 실시예들을 첨부한 도면을 참조하여 상세히 설명한다. 본 발명의 요지를 불필요하게 흐릴 수 있는 공지 기능 및 구성에 대한 상세한 설명은 생략한다.

본 발명이 제공하는 이중 복호화 기능을 효율적으로 제공하면서 사용자의 프라이버시를 보호할 수 있는 공개키 암호화 방법은 다음과 같이 상세히 설명될 것이다.

도 1은 본 발명의 바람직한 실시예에 따른 이중 복호화 기능을 제공하면서 사용자의 프라이버시를 보호할 수 있는 공개키 암호화 방법을 도시한 흐름도이다.

먼저, 사용자는 암호화에 필요한 공개키 및 비밀키를 포함하는 키 파라미터를 통신 기기의 암호화 장치를 통해 생성한다(S100).

이에 따라, 사용자는 생성된 키 파라미터를 기초로 주어진 평문 $m \in Z_n^1$ 에 대한 암호화를 암호화 장치를 통해 수행한다(S300). 이렇게 암호화가 수행된 평문 m 은 소정 통신 채널을 시스템 관리자에게 전송될 수 있다.

복호화 모드가 수행되면(S500), 통신 기기의 복호화 장치는 복호 주체에 따라 설정된 알고리즘을 기초로 평문 m 을 복호화 처리한다(S700).

도 2는 본 발명의 제1 실시예에 따라 도 1의 키 파라미터 생성 단계(S100)를 보다 상세하게 나타낸 흐름도이다.

먼저, 사용자는 암호화 장치를 통해 k 비트의 두 소수 p, q 를 선택 생성한다(S110). 이후 사용자는 생성한 k 비트를 갖는 두 수 p, q 에 대해, 수학적식 $n=p^2q$ 을 만족하도록 설정한다(S120). 또한 사용자는 수학적식 $\text{ord}(g^{p-1} \bmod(p^2))=p$ 를 만족하는 임의의 수 g 를 생성한다(S130). 여기서 g 는 $g \in Z_n$ 를 만족하는 값이다.

이후, 사용자는 임의의 $k-1$ 비트의 수 a 를 선택한다(S140). 그리고 사용자는 암호화 장치를 통해 함수 $h=g^a \bmod(n)$ 를 계산한다(S150).

이에 따라, 공개키는 (n, g, h, k) 이고 대응되는 비밀키는 a 인 키 파라미터를 얻을 수 있다(S160). 두 인수 p, q 는 관리자에게 주어지는 마스터키에 해당하는 정보이고, 관리자만이 알고 있는 값이다.

도 3은 본 발명의 제1 실시예에 따라 도 1의 암호화 수행 단계(300)를 보다 상세하게 나타낸 흐름도이다.

선택된 키 파라미터를 사용해서 수행되는 암호화 단계는 다음과 같다. 먼저, 사용자에게 의해 선택된 평문 $m \in Z_n^*$ 이 입력되면(S310), 암호화 장치는 사용자에게 의해 입력된 $k-1$ 비트의 난수 r 을 선택 생성한다(S320).

이후, 암호화 장치는 아래 수학식 1을 통해 A, B 각각의 값을 산출한다(S330, S340).

$$A = g^r \bmod(n),$$

$$B = h^r m \bmod(n)$$

이에 따라, 암호화 장치는 A, B를 조합하여 아래 수학식 2와 같은 암호문 C를 계산한다(S350).

$$C = (A, B)$$

이에 따라 암호화 장치를 통한 암호화가 완료된다(S360).

도 4는 본 발명의 제1 실시예에 따라 도 1의 복호화 단계(S700)를 보다 상세하게 나타낸 흐름도이다.

복호화 모드가 수행되면(S710), 복호화 장치는 복호자가 암호화를 수행한 일반 사용자인지를 판별한다(S720).

복호자가 일반 사용자인지, 복호화 장치는 암호화시 사용한 비밀키 a를 획득한다(S732). 이에 따라, 복호화 장치는 복호화시 암호화시 이용된 엘가말(ElGamal) 암호 기법과 동일한 기법을 적용하여 복호화를 수행한다(S734).

이에 따라, 복호화 장치는 아래 수학식 3을 통해 평문 m 을 복호화한다.

$$m = B/A^a \bmod(n)$$

이에 따라, 평문 m 에 대한 복호화가 완료된다(S738).

한편, S720 단계에서, 복호자가 일반 사용자가 아닌 것으로 판단되면, 복호화 장치는 복호자가 시스템 관리자인지를 판별한다(S752). 복호자가 시스템 관리자이면, 복호화 장치는 두 소수 p, q 를 사용해서 복호화를 수행한다.

즉, 복호화 장치는 아래 수학식 4를 통해 h_p 및 g_p 값을 획득한다(S754, S756).

$$h_p = h^{p-1} \bmod(p^2)$$

$$g_p = g^{p-1} \bmod(p^2)$$

이에 따라 획득한 값 h_p 및 g_p 를 아래 수학식 5에 대입하여 비밀키 a를 복원한다(S758).

$$a = L(h_p)/L(g_p) \bmod(p)$$

이에 따라, 시스템 관리자는 복호화 장치를 통해 복원된 비밀키 a를 사용해서 수학식 3과 동일한 아래 수학식 6을 통해 평문 m 을 복호화 할 수 있다(S762).

$$m = B/A^a \bmod(n)$$

이러한 과정을 통해 평문 m 에 대한 복호화가 완료된다(S764).

따라서, 본 발명에 따른 사용자의 프라이버시를 보호할 있는 이중 복호화 기능이 제공되는 암호화 방법에서는 복호화를 위해 필요한 비밀키 a 에 대한 접근 권한을 사용자와 시스템 관리자에 대해 차별적으로 부여함으로써, 사용자의 비밀키 a 를 완전히 노출하지 않으면서 시스템 관리자에 대한 사용자의 프라이버시를 보호받을 수 있다.

표 1을 이중 복호화 기법을 적용함에 있어서 종래와 본 발명의 처리 성능의 효율성을 비교한 정보이다.

[표 1]

암호화 기법	종래의 이중 복호화	본 발명의 이중 복호화
평문의 길이	1000 비트	1600 비트
암호문의 길이	4000 비트	3200 비트
암호화의 계산복잡도	$2ME(2000, 1000)$	$2ME(1600, 533)$
복호화 1의 계산복잡도	$ME(2000, 1000)$	$ME(1600, 533)$
복호화 2의 계산복잡도	$2ME(2000, 1000)$	$ME(1066, 533)+ME(1600, 533)$

본 발명에 따른 이중 복호화 기능이 제공되는 암호화 방법은, 종래의 이중 복호화 기능을 제공하는 암호화 방법에 비해서 상기와 같은 효율성의 우위가 있음을 알 수 있다.

즉, M 와 e 는 각각 모듈로(mod) M 과 지수값 e 의 비트사이즈라 할 때, 모듈로 M 과 지수값 e 에 대해서 모듈로 지수승 연산을 수행하는 연산량을 $ME(M, e)$ 라고 하자.

참고로, $ME(a, b)$ 와 $ME(\alpha a, \beta b)$ 의 연산량의 비율은 $1:\alpha^2\beta$ 이다. 예를 들어, $ME(a, b)$ 는 $ME(2a, 3b)$ 보다 $2^2 \cdot 3 = 12$ 배 정도 효율적으로 연산을 수행한다.

페랄타(Peralta)는 p^2q 형태의 정수와 RSA(Rivest, Shamir, Adleman) 정수가 각각 1600비트와 1000비트에서 동일한 안전성을 가진다는 것을 밝혔다. 그러므로 동일한 안전성에서 두 정수를 모듈러(modular)로 설계된 공개키 암호의 효율성을 비교하기 위해서는 p^2q 형태의 1600 비트 정수와 1000 비트의 RSA 정수를 비교해야 한다.

상기 표 1에서와 같이 본 발명이 제공하는 이중 복호화가 적용되는 공개키 암호 방법은 종래의 방법에 비해 매우 효율적임을 알 수 있다. 즉, 종래에 제안된 암호화 기법은 1000 비트의 평문을 전송하기 위해서 4000 비트의 암호문을 생성해야 한다. 그러나 본 발명의 공개키 암호 방법에서는 1600 비트의 평문에 대해서 3200 비트의 암호문만을 생성하면 된다. 이와 같이, 종래에 비해 본 발명의 이중 복호화가 적용된 암호화 방법은 평문과 암호문의 비율이 현저히 낮은 것을 확인할 수 있다.

또한 계산량의 측면에서 보면 본 발명에서 제안하는 이중 복호화 기능이 적용되는 공개키 암호화 기법은 기존의 것보다 3 배정도 빠른 암호화 연산과 복호화 연산을 제공함을 알 수 있다. 특히, 시스템 관리자는 기존의 것보다 4배 효율적으로 복호화 연산을 수행할 수 있다.

이하, 사용자의 프라이버시를 보호할 수 있는 공개키 암호화 기법의 다른 예에 대해 설명한다.

도 5는 본 발명의 제2 실시예에 따라 도 1의 키 파라미터 생성 단계(S100)를 보다 상세하게 나타낸 흐름도이다.

먼저, 사용자는 암호화 장치를 통해 k 비트의 두 소수 p, q 를 선택 생성한다(S210). 이후 사용자는 생성한 k 비트를 갖는 두 수 p, q 에 대해, 수학적식 $n=p^2q$ 을 만족하도록 설정한다(S220). 또한 사용자는 수학적식 $ord(g^{p-1} \bmod(p^2))=p$ 를 만족하는 임의의 수 g 를 생성한다(S230). 여기서 g 는 $g \in \mathbb{Z}_n$ 를 만족하는 값이다.

이때, 암호화 장치는 사용자에게 의해 입력되는 시스템 관리자에게 복호화 할 수 있는 능력의 허용 여부를 판별한다(S240).

사용자가 관리자에게 복호화 할 수 있는 능력을 허용하는 경우에는 아래와 같은 과정을 통해 공개키를 생성한다. 즉, 사용자는 임의의 $k-1$ 비트의 수 a 를 선택한다(S252). 그리고 사용자는 암호화 장치를 통해 함수 $h=g^a \bmod(n)$ 를 계산한다(S254).

이에 따라, 공개키는 (n, g, h, k) 이고 대응되는 비밀키는 a 인 키 파라미터를 얻을 수 있다(S256). 두 인수 p, q 는 관리자에게 주어지는 마스터키에 해당하는 정보이고, 관리자만이 알고 있는 값이다.

한편, S240 단계에서 시스템 관리자의 복호화 능력을 허용하지 않는 경우, 사용자는 암호화 장치를 통해 임의의 t 비트의 a 를 선택 생성한다(S262). 여기서 t 는 $t > k$ 를 만족하는 값이다.

그리고 사용자는 암호화 장치를 통해 함수 $h=g^a \bmod(n)$ 를 계산한다(S264). 이에 따라, 공개키는 (n, g, h, t) 이고 대응되는 비밀키는 a 인 키 파라미터를 얻을 수 있다(S266).

도 6은 본 발명의 제2 실시예에 따라 도 1의 암호화 수행 단계(300)를 보다 상세하게 나타낸 흐름도이다.

도 5에서 생성된 키 파라미터를 사용해서 수행되는 암호화 단계는 다음과 같다. 먼저, 사용자에 의해 선택된 평문 $m \in \mathbb{Z}_n$ 이 입력되면(S410), 암호화 장치는 사용자에 의해 입력된 명령에 따라 시스템 관리자에 대한 복호화 허용 여부를 판별한다(S420).

시스템 관리자에 대한 복호화가 허용되도록 설정된 경우, 암호화 장치는 사용자에 의해 입력된 $k-1$ 비트의 난수 r 을 선택 생성한다(S430).

이후, 암호화 장치는 아래 수학적 식 7을 통해 A, B 각각의 값을 산출한다(S450, S460).

$$A=g^r \bmod(n),$$

$$B=h^r m \bmod(n)$$

이에 따라, 암호화 장치는 A, B를 조합하여 아래 수학적 식 8과 같은 암호문 C를 계산한다(S470).

$$C=(A, B)$$

이에 따라 암호화 장치를 통한 암호화가 완료된다(S480).

한편, S420 단계에서 시스템 관리자에 대한 복호화가 허용되지 않도록 설정된 경우, 암호화 장치는 사용자에 의해 입력된 t 비트의 난수 r 을 선택 생성한다(S440). 이후 암호화 과정은 S450 단계 내지 S480 단계를 동일하게 수행한다.

도 7은 본 발명의 제2 실시예에 따라 도 1의 복호화 단계(S700)를 보다 상세하게 나타낸 흐름도이다.

복호화 모드가 수행되면(S810), 복호화 장치는 복호자가 암호화를 수행한 일반 사용자인지 아니면 시스템 관리자인지를 판별한다(S820).

복호자가 일반 사용자이면, 복호화 장치는 암호화시 사용한 비밀키 a 를 획득한다(S832). 이에 따라, 복호화 장치는 복호화시 암호화시 이용된 엘가말(ElGamal) 암호 기법과 동일한 기법을 적용하여 수학적 식 3과 동일하게 아래 수학적 식 9를 통해 평문 m 을 복호화한다(S834).

$$m=B/A^a \bmod(n)$$

이에 따라, 평문 m 에 대한 복호화가 완료된다(S836).

한편, S820 단계에서, 복호자가 일반 사용자가 아닌 시스템 관리자인 것으로 판단되면, 복호화 장치는 시스템 관리자에 대해 설정된 복호 허용 여부를 판별한다(S840). 복호자인 시스템 관리자에 대한 복호 허용이 불허된 것으로 판단되면, 시스템 관리자는 복호화 장치를 통한 비밀키 a 에 대한 산출을 불가능하다(S842). 이에 따라, 복호화 장치는 평문 m 에 대한 복호화가 불가능하게 된다(S844).

한편, S840 단계에서 복호자인 시스템 관리자에 대한 복호가 허용된 것으로 판단되면, 복호화 장치는 두 소수 p, q 를 사용해서 아래와 같이 복호화를 수행한다.

즉, 복호화 장치는 수학적 4와 동일한 아래 수학적 10을 통해 h_p 및 g_p 값을 획득한다(S852, S854).

$$h_p = h^{p-1} \bmod(p^2)$$

$$g_p = g^{p-1} \bmod(p^2)$$

이에 따라 획득한 값 h_p 및 g_p 를 수학적 5와 동일한 아래 수학적 11에 대입하여 비밀키 a 를 복원한다(S856).

$$a = L(h_p)/L(g_p) \bmod(p)$$

이에 따라, 시스템 관리자는 복호화 장치를 통해 복원된 비밀키 a 를 사용해서 수학적 6과 동일한 아래 수학적 12를 통해 평문 m 을 복호화 할 수 있다(S858).

$$m = B/A^a \bmod(n)$$

이러한 과정을 통해 평문 m 에 대한 복호화가 완료된다(S859).

이와 같이, 사용자의 복호화 동의가 없으면, 시스템 관리자는 비밀 지수 a 를 계산할 수 없다. 시스템 관리자가 계산할 수 있는 값은 비밀지수 a 에 대해서 $a' = a \bmod(p)$ 만 알 수 있다.

그러나 충분히 큰 k 와 t 가 선택되면 a' 에서 a 를 알아내는 것은 어렵다. 이 문제의 어려움은 암호가 정의된 군의 부분군에서의 디피-헬만 가정에 의해 안전성을 보장받는다.

따라서, 공개키의 소유자인 사용자가 시스템 관리자의 복호화 능력을 제한하더라도, 사용자의 선택에 의해 시스템 관리자에게 복호화 능력을 선택적으로 제공할 수 있다. 또한 사용자가 시스템 관리자의 복호화 능력을 허용하려면, 암호화시 t 비트가 아닌 $k-1$ 비트의 난수 r 을 선택한다. 이때 시스템 관리자는 공개키의 소유자인 사용자의 비밀키 a 를 통해 평문 m 을 복호화하는 방법과 같이, h_p 및 g_p 를 획득하여 이를 통해 비밀키 a 를 산출함으로써 암호문에서 평문을 복원할 수 있다.

이상에서는 본 발명에서 특정의 바람직한 실시예에 대하여 도시하고 또한 설명하였다. 그러나, 본 발명은 상술한 실시예에 한정되지 아니하며, 특허 청구의 범위에서 첨부하는 본 발명의 요지를 벗어남이 없이 당해 발명이 속하는 기술 분야에서 통상의 지식을 가진 자라면 누구든지 다양한 변형 및 균등한 타 실시가 가능할 것이다. 따라서 본 발명의 진정한 기술적 보호범위는 첨부한 특허 청구범위에 의해서만 정해져야 할 것이다.

발명의 효과

상술한 바와 같이, 본 발명의 이중 복호화 기능이 제공되는 암호화 방법에서는 복호화를 위해 필요한 비밀키 a 에 대한 접근 권한을 사용자와 시스템 관리자에 대해 차별적으로 부여함으로써, 사용자의 비밀키 a 를 완전히 노출하지 않으면서 시스템 관리자에 대한 사용자의 프라이버시를 보호받을 수 있다.

또한, 전술한 일반적인 공개키 암호시스템에서 제공하는 이중 복호화 기능을 기존에 제안된 것보다 처리성능 면에서 보다 효율적으로 제공할 수 있다.

뿐만 아니라, 본 발명의 공개키 암호화 방법은 암호화 기법을 구성하기 위해 사용하는 모듈러(mod)를 새롭게 구성함으로써, 기존에 제안된 이중 복호화 기능을 4배 빠른 효율적인 암호화 기법을 제공할 수 있다. 또한 시스템 관리자의 능력으로 획득할 수 있는 비밀정보를 제한함으로써, 사용자의 비밀정보를 완전히 노출하지 않고 이를 통해서 시스템 관리자에 대해서도 사용자의 프라이버시를 보호 받을 수 있다.

도면의 간단한 설명

도 1은 본 발명의 바람직한 실시예에 따른 이중 복호화 기능을 효율적으로 제공하면서 사용자의 프라이버시를 보호할 수 있는 공개키 암호화 방법을 도시한 흐름도,

도 2는 본 발명의 제1 실시예에 따라 도 1의 키 파라미터 생성 단계를 보다 상세하게 나타낸 흐름도,

도 3은 본 발명의 제1 실시예에 따라 도 1의 암호화 수행 단계를 보다 상세하게 나타낸 흐름도,

도 4는 본 발명의 제1 실시예에 따라 도 1의 복호화 단계를 보다 상세하게 나타낸 흐름도,

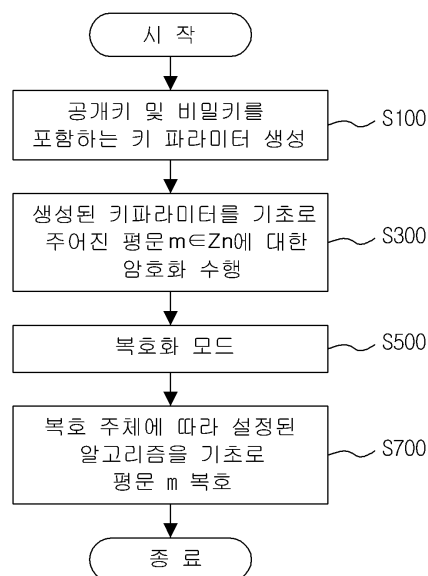
도 5는 본 발명의 제2 실시예에 따라 도 1의 키 파라미터 생성 단계를 보다 상세하게 나타낸 흐름도,

도 6은 본 발명의 제2 실시예에 따라 도 1의 암호화 수행 단계를 보다 상세하게 나타낸 흐름도, 그리고

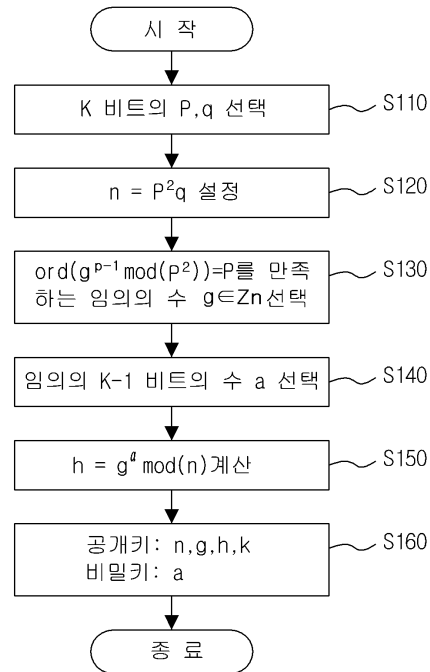
도 7은 본 발명의 제2 실시예에 따라 도 1의 복호화 단계를 보다 상세하게 나타낸 흐름도이다.

도면

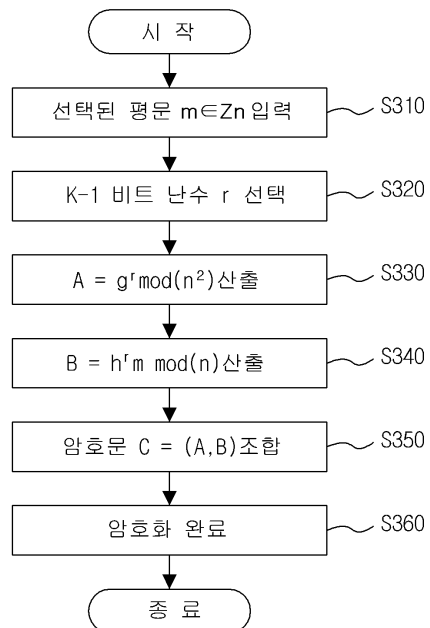
도면1



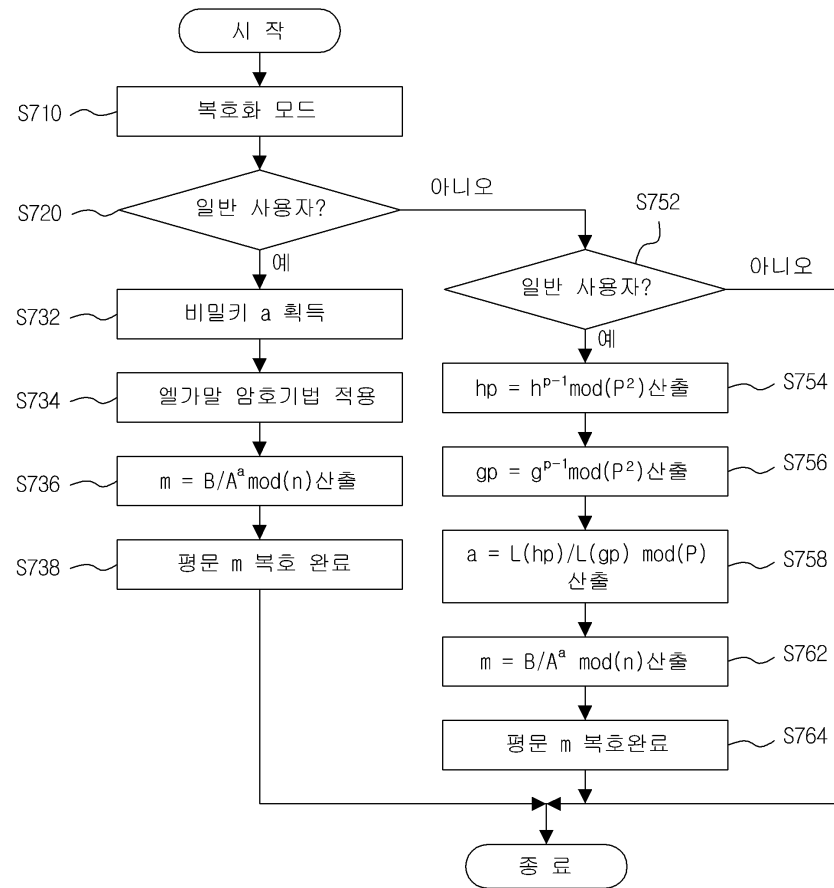
도면2



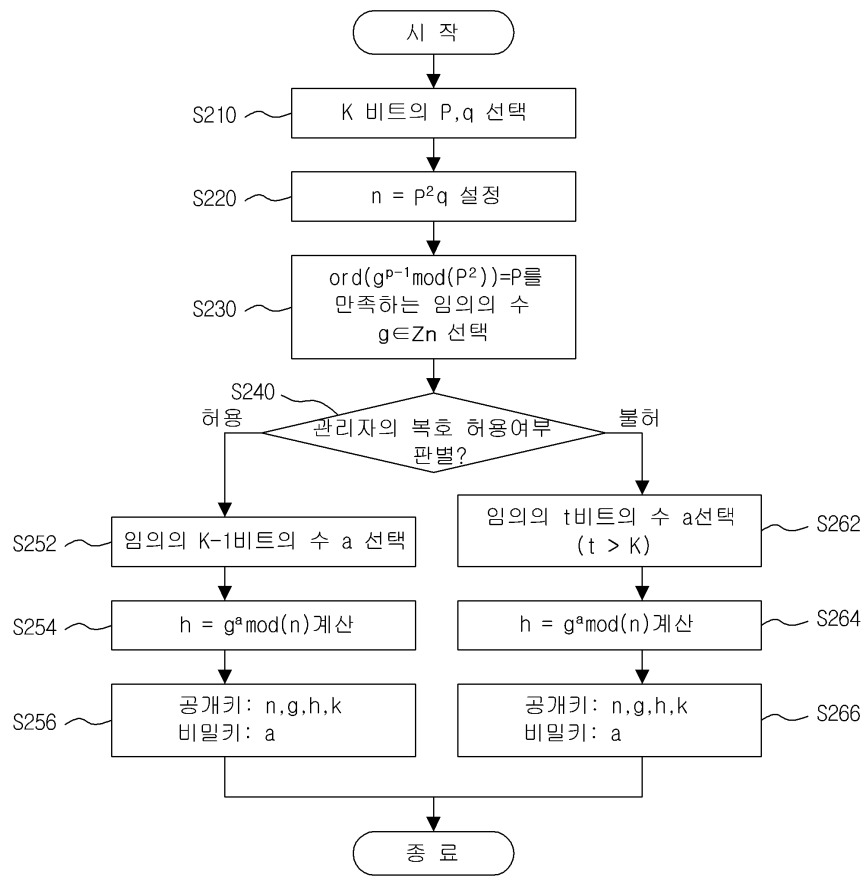
도면3



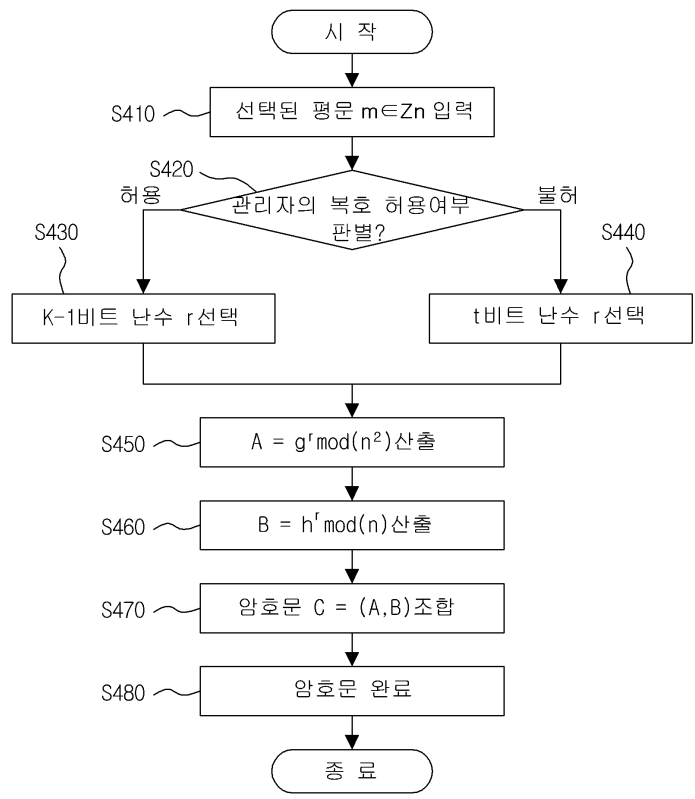
도면4



도면5



도면6



도면7

