

청구범위

- [청구항 1] 비밀키를 설정하고, 상기 비밀키 및 에러를 이용하여 공개키를 생성하는 단계; 및
메시지에 상기 공개키를 적용한 후, 라운딩 처리를 수행하여, 상기 메시지를 암호화하는 단계;를 포함하며,
상기 비밀키는 -1, 0, 1 중에서 랜덤하게 조합되고,
상기 에러의 크기는, 0보다 크고 1보다 작게 설정된 에러 파라미터에 의해 결정되는, 암호화 방법.
- [청구항 2] 제1항에 있어서,
상기 공개키를 생성하는 단계는,
랜덤하게 결정된 값들로 구성된 제1 랜덤 행렬(A)을 산출하는 단계;
각 성분이 -1, 0, 1 중 하나의 값을 갖는 열 벡터를 행렬 형태로 랜덤하게 조합하여 상기 비밀키(s)를 산출하는 단계;
이산 가우시안 분포 또는 상기 이산 가우시안 분포와 통계적 거리가 가까운 분포로부터 상기 에러(E)를 추출하는 단계;
상기 제1 랜덤 행렬 및 상기 비밀키와, 상기 에러를 모듈러 연산하여 제2 랜덤 행렬(B)을 산출하는 단계;
상기 제1 랜덤 행렬 및 상기 제2 랜덤 행렬을 포함하는 상기 공개키를 산출하는 단계;를 포함하는, 암호화 방법.
- [청구항 3] 제2항에 있어서,
상기 메시지를 암호화하는 단계는,
각 성분이 -1, 0, 1의 값을 갖는 랜덤 벡터를 설정하는 단계;
상기 제1 랜덤 행렬 및 상기 랜덤 벡터를 연산한 제1 값, 상기 제2 랜덤 행렬 및 상기 랜덤 벡터를 연산한 결과값에 상기 메시지를 인코딩한 값을 추가한 제2 값을 각각 산출하는 단계;
상기 제1 및 제2 값 각각에 대해서 기 설정된 개수의 하위 비트를 제거하기 위한 라운딩 처리를 수행하여, 상기 메시지에 대응되는 암호문을 산출하는 단계;를 포함하는, 암호화 방법.
- [청구항 4] 제1항에 있어서,
상기 공개키를 생성하는 단계는,
기 설정된 계수를 가지는 다항식의 집합인 링(Ring)을 설정하는 단계;
상기 링으로부터 상기 비밀키를 산출하는 단계;
상기 링으로부터 제1 랜덤 다항식을 산출하는 단계;
이산 가우시안 분포 또는 상기 이산 가우시안 분포와 통계적 거리가 가까운 분포로부터 상기 에러를 추출하는 단계;
상기 제1 랜덤 다항식 및 상기 비밀키에 상기 에러를 모듈러 연산하여 제2 랜덤 다항식을 산출하는 단계;

상기 제1 랜덤 다항식 및 상기 제2 랜덤 다항식을 포함하는 상기 공개키를 설정하는 단계;를 포함하는, 암호화 방법.

[청구항 5] 제4항에 있어서,
상기 메시지를 암호화하는 단계는,
각 계수가 -1, 0, 1 중 하나의 값을 갖는 다항식을 랜덤하게 추출하는 단계;
상기 제1 랜덤 다항식 및 상기 다항식을 연산한 제1 값, 상기 제2 랜덤 다항식 및 상기 다항식을 연산한 결과값에 상기 메시지를 인코딩한 값을 추가한 제2 값을 각각 산출하는 단계;
상기 제1 및 제2 값 각각에 대해서 기 설정된 개수의 하위 비트를 제거하기 위한 라운딩 처리를 수행하여, 상기 메시지에 대응되는 암호문 다항식을 산출하는 단계;를 포함하는, 암호화 방법.

[청구항 6] 제1항 내지 제5항 중 어느 한 항에 있어서,
상기 공개키로 암호화된 다른 메시지가 수신되면, 수신된 다른 메시지를 상기 비밀키로 복호화하는 단계;를 더 포함하는 암호화 방법.

[청구항 7] 메모리; 및
비밀키를 설정하고, 상기 비밀키 및 에러를 이용하여 공개키를 생성하며, 상기 비밀키 및 상기 공개키를 상기 메모리에 저장하는 프로세서;를 포함하며,
상기 프로세서는,
암호화할 메시지에 대하여 상기 공개키를 적용한 후 라운딩 처리를 수행하여 상기 메시지를 암호화하며,
상기 비밀키는 -1, 0, 1 중에서 랜덤하게 조합되고,
상기 에러의 크기는, 0보다 크고 1보다 작게 설정된 에러 파라미터에 의해 결정되는, 연산 장치.

[청구항 8] 제7항에 있어서,
상기 프로세서는,
랜덤하게 결정된 벡터들로 구성된 제1 랜덤 행렬(A)을 산출하고, 이산 가우시안 분포 또는 상기 이산 가우시안 분포와 통계적 거리가 가까운 분포로부터 상기 에러를 산출하며, 상기 제1 랜덤 행렬 및 상기 비밀키와, 상기 에러를 모듈러 연산하여 제2 랜덤 행렬(B)을 산출하여, 상기 제1 랜덤 행렬 및 상기 제2 랜덤 행렬을 포함하는 상기 공개키를 설정하는, 연산 장치.

[청구항 9] 제8항에 있어서,
상기 프로세서는,
각 성분이 -1, 0, 1의 값을 갖는 랜덤 벡터를 설정하고, 상기 제1 랜덤 행렬 및 상기 랜덤 벡터를 연산한 제1 값, 상기 제2 랜덤 행렬 및 상기 랜덤 벡터를 연산한 결과값에 상기 메시지를 인코딩한 값을 추가한 제2 값을 각각 산출하며, 상기 제1 및 제2 값 각각에 대해서 기 설정된 개수의 하위

비트를 제거하기 위한 라운딩 처리를 수행하여, 상기 메시지에 대응되는 암호문을 산출하는, 연산 장치.

- [청구항 10] 제9항에 있어서,
상기 프로세서는,
기 설정된 계수를 가지는 다항식의 집합인 링(Ring)을 설정하고, 상기 링으로부터 상기 비밀키 및 제1 랜덤 다항식을 각각 산출하고, 이산 가우시안 분포 또는 상기 이산 가우시안 분포와 통계적 거리가 가까운 분포로부터 상기 에러를 산출하며, 상기 제1 랜덤 다항식 및 상기 비밀키에 상기 에러를 모듈러 연산하여 제2 랜덤 다항식을 산출하여, 상기 제1 랜덤 다항식 및 상기 제2 랜덤 다항식을 포함하는 상기 공개키를 설정하는, 연산 장치.
- [청구항 11] 제10항에 있어서,
상기 프로세서는,
각 계수가 -1, 0, 1 중 하나의 값을 갖는 다항식을 랜덤하게 추출하고, 상기 제1 랜덤 다항식 및 상기 다항식을 연산한 제1 값, 상기 제2 랜덤 다항식 및 상기 다항식을 연산한 결과값에 상기 메시지를 인코딩한 값을 추가한 제2 값을 각각 산출하며, 상기 제1 및 제2 값 각각에 대해서 기 설정된 개수의 하위 비트를 제거하기 위한 라운딩 처리를 수행하여, 상기 메시지에 대응되는 암호문 다항식을 산출하는, 연산 장치.
- [청구항 12] 제7항 내지 제11항 중 어느 한 항에 있어서,
상기 메모리에 저장된 상기 공개키를 브로드캐스팅하기 위한 통신부;를 더 포함하며,
상기 프로세서는,
상기 브로드캐스팅된 공개키에 의해 암호화된 다른 메시지가 상기 통신부를 통해 수신되면, 수신된 상기 다른 메시지를 상기 비밀키를 이용하여 복호화하는 연산 장치.
- [청구항 13] 프로그램 코드가 저장된 기록 매체에 있어서,
상기 프로그램 코드는,
랜덤하게 결정된 값들로 구성된 제1 랜덤 행렬(A)을 산출하는 단계;
각 성분이 -1, 0, 1 중 하나의 값을 갖는 열 벡터를 행렬 형태로 랜덤하게 조합하여 비밀키(s)를 산출하는 단계;
이산 가우시안 분포 또는 상기 이산 가우시안 분포와 통계적 거리가 가까운 분포로부터 상기 에러를 산출하는 단계;
상기 제1 랜덤 행렬 및 상기 비밀키와, 상기 에러를 모듈러 연산하여 제2 랜덤 행렬(B)을 산출하는 단계; 및,
상기 제1 랜덤 행렬 및 상기 제2 랜덤 행렬을 포함하는 공개키를 설정하는 단계;를 순차적으로 수행하는, 기록 매체.
- [청구항 14] 제13항에 있어서,

상기 프로그램 코드는,
각 성분이 -1, 0, 1의 값을 갖는 랜덤 벡터를 설정하는 단계;
상기 제1 랜덤 행렬 및 상기 랜덤 벡터를 연산한 제1 값, 상기 제2 랜덤
행렬 및 상기 랜덤 벡터를 연산한 결과값에 메시지를 인코딩한 값을
추가한 제2 값을 각각 산출하는 단계; 및
상기 제1 및 제2 값 각각에 대해서 기 설정된 개수의 하위 비트를
제거하기 위한 라운딩 처리를 수행하여, 상기 메시지에 대응되는
암호문을 산출하는 단계;를 더 수행하는, 기록매체.