

청구범위

- [청구항 1] 전자 장치에 있어서,
적어도 하나의 인스트럭션(instruction)을 저장하고, 복수의 변수 정보를 암호화된 상태를 저장하는 동형 암호문을 복수개 저장하는 메모리; 및
상기 적어도 하나의 인스트럭션을 실행하는 프로세서;를 포함하고,
상기 프로세서는,
상기 적어도 하나의 인스트럭션을 실행함으로써, 상기 복수의 동형 암호문에 대한 연산 명령이 수신되면 상기 동형 암호문 각각에 대해서 서로 다른 변수 정보 구분하여 갖는 빈 마스크를 이용하여 변수 조합에 대응되는 개수 정보를 생성하는 전자 장치.
- [청구항 2] 제1항에 있어서,
상기 동형 암호문은 복수의 슬롯을 포함하며,
상기 복수의 슬롯 각각에 하나의 변수 정보를 갖는 전자 장치.
- [청구항 3] 제1항에 있어서,
상기 빈 마스크는,
복수의 슬롯을 포함하며,
상기 복수의 슬롯 각각은 하나의 변수 값의 존재 여부에 대한 정보를 포함하며,
상기 프로세서는,
동형 암호문 각각에 대해서 상기 동형 암호문에 포함된 변수 정보별 복수의 빈 마스크를 생성하고, 생성된 복수의 빈 마스크 중 상기 변수 조합에 대응되는 빈 마스크를 선별하고, 상기 선별된 빈 마스크 간의 곱을 이용하여 상기 변수 조합을 갖는 개수 정보를 생성하는 전자 장치.
- [청구항 4] 제1항에 있어서,
상기 빈 마스크는,
복수의 슬롯을 포함하며,
상기 복수의 슬롯 각각은 하나의 변수 값의 존재 여부에 대한 정보를 포함하는 복수의 서브 슬롯을 포함하고,
상기 프로세서는,
동형 암호문 각각에 대해서 하나의 빈 마스크를 생성하고, 상기 복수의 빈 마스크 중 상기 변수 조합에 대응되는 상기 빈 마스크 내의 서브 슬롯을 이용하여 상기 변수 조합을 갖는 개수 정보를 생성하는 전자 장치.
- [청구항 5] 제4항에 있어서,
상기 복수의 서브 슬롯은, 기설정된 비트 간격을 갖고 하나의 슬롯 내에 배치되는 전자 장치.
- [청구항 6] 제1항에 있어서,
상기 프로세서는,

동일한 특징에 대한 복수의 정보를 포함하는 제1 동형 암호문 및 제2 동형 암호문을 하나의 동형 암호문으로 결합하는 전자 장치.

[청구항 7]

제6항에 있어서,
상기 프로세서는,
상기 제1 동형 암호문과 상기 제2 동형 암호문 내의 공통된 정보에 대한 제1 동형 암호문 내의 제1 위치 정보와 상기 제2 동형 암호문 내의 제2 위치 정보를 이용하여, 상기 제1 동형 암호문과 제2 동형 암호문을 하나로 결합하는 전자 장치.

[청구항 8]

제7항에 있어서,
상기 프로세서는,
제1 및 제2 동형 암호문 내에 포함된 복수의 정보 각각에 대해서 기설정된 공통된 키로 일방향 암호화 방식으로 암호화된 데이터와 상기 암호화된 데이터에 대한 동형 암호문 내의 위치 정보가 입력되면, 상기 제1 동형 암호문에 대한 암호화된 데이터와 상기 제2 동형 암호문에 대한 암호화된 데이터를 비교하여, 두 동형 암호문 간에 공통된 정보를 갖는 상기 제1 위치 정보와 상기 제2 위치 정보를 확인하는 전자 장치.

[청구항 9]

동형 암호문에 대한 암호문 처리 방법에 있어서,
복수의 변수 정보를 암호화된 상태를 저장하는 동형 암호문을 복수개 저장하고, 상기 복수의 동형 암호문에 대한 연산 명령을 수신하는 단계;
상기 복수의 동형 암호문 각각에 대해서 서로 다른 변수 정보 구분하여 갖는 빈 마스크를 생성하는 단계;
상기 빈 마스크를 이용하여 변수 조합에 대응되는 개수 정보를 생성하는 단계; 및
상기 생성된 개수 정보를 출력하는 단계;를 포함하는 암호문 처리 방법.

[청구항 10]

제9항에 있어서,
상기 동형 암호문은 복수의 슬롯을 포함하며,
상기 복수의 슬롯 각각에 하나의 변수 정보를 갖는 암호문 처리 방법.

[청구항 11]

제9항에 있어서,
상기 빈 마스크는,
복수의 슬롯을 포함하며,
상기 복수의 슬롯 각각은 하나의 변수 값의 존재 여부에 대한 정보를 포함하며,
상기 빈 마스크를 생성하는 단계는,
동형 암호문 각각에 대해서 상기 동형 암호문에 포함된 변수 정보별 복수의 빈 마스크를 생성하고,
상기 개수 정보를 생성하는 단계는,
생성된 복수의 빈 마스크 중 상기 변수 조합에 대응되는 빈 마스크를 선별하고, 상기 선별된 빈 마스크 간의 곱을 이용하여 상기 변수 조합을

- 찾는 개수 정보를 생성하는 암호문 처리 방법.
- [청구항 12] 제9항에 있어서,
상기 빈 마스크는,
복수의 슬롯을 포함하며,
상기 복수의 슬롯 각각은 하나의 변수 값의 존재 여부에 대한 정보를 포함하는 복수의 서브 슬롯을 포함하고,
상기 빈 마스크를 생성하는 단계는,
동형 암호문 각각에 대해서 하나의 빈 마스크를 생성하고,
상기 개수 정보를 생성하는 단계는,
상기 복수의 빈 마스크 중 상기 변수 조합에 대응되는 상기 빈 마스크 내의 서브 슬롯을 이용하여 상기 변수 조합을 갖는 개수 정보를 생성하는 암호문 처리 방법.
- [청구항 13] 제12항에 있어서,
상기 복수의 서브 슬롯은, 기설정된 비트 간격을 갖고 하나의 슬롯 내에 배치되는 암호문 처리 방법.
- [청구항 14] 제9항에 있어서,
동일한 특징에 대한 복수의 정보를 포함하는 제1 동형 암호문 및 제2 동형 암호문을 하나의 동형 암호문으로 결합하는 단계;를 더 포함하는 암호문 처리 방법.
- [청구항 15] 제14항에 있어서,
상기 결합하는 단계는,
상기 제1 동형 암호문과 상기 제2 동형 암호문 내의 공통된 정보에 대한 제1 동형 암호문 내의 제1 위치 정보와 상기 제2 동형 암호문 내의 제2 위치 정보를 이용하여, 상기 제1 동형 암호문과 제2 동형 암호문을 하나로 결합하는 암호문 처리 방법.
- [청구항 16] 제15항에 있어서,
상기 결합하는 단계는,
제1 및 제2 동형 암호문 내에 포함된 복수의 정보 각각에 대해서 기설정된 공통된 키로 일방향 암호화 방식으로 암호화된 데이터와 상기 암호화된 데이터에 대한 동형 암호문 내의 위치 정보가 입력되면, 상기 제1 동형 암호문에 대한 암호화된 데이터와 상기 제2 동형 암호문에 대한 암호화된 데이터를 비교하여, 두 동형 암호문 간에 공통된 정보를 갖는 상기 제1 위치 정보와 상기 제2 위치 정보를 확인하는 암호문 처리 방법.
- [청구항 17] 암호문 처리 방법을 실행하기 위한 프로그램을 포함하는 컴퓨터 판독가능 기록매체에 있어서,
상기 암호문 처리 방법은,
복수의 변수 정보를 암호화된 상태를 저장하는 동형 암호문을 복수개 저장하고, 상기 복수의 동형 암호문에 대한 연산 명령을 수신하는 단계;

상기 복수의 동형 암호문 각각에 대해서 서로 다른 변수 정보 구분하여
갖는 빈 마스크를 생성하는 단계;
상기 빈 마스크를 이용하여 변수 조합에 대응되는 개수 정보를 생성하는
단계; 및
상기 생성된 개수 정보를 출력하는 단계;를 포함하는 컴퓨터 판독가능
기록매체.