



(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2008년06월30일
(11) 등록번호 10-0842042
(24) 등록일자 2008년06월23일

(51) Int. Cl.

H03M 13/05 (2006.01)

(21) 출원번호 10-2007-0070975

(22) 출원일자 2007년07월16일

심사청구일자 2007년07월16일

(56) 선행기술조사문헌

KR100163717 B1

(뒷면에 계속)

(73) 특허권자

충남대학교산학협력단

대전광역시 유성구 궁동 220번지 충남대학교

(72) 발명자

김형식

대전 유성구 전민동 엑스포아파트 206-1306

정동우

대전 대덕구 법2동 202-8 3층

(74) 대리인

김원준

전체 청구항 수 : 총 4 항

심사관 : 손희수

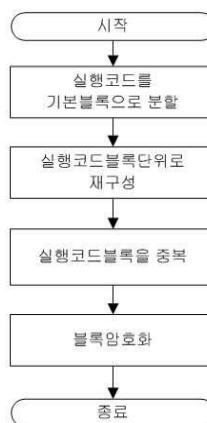
(54) 암호화된 실행코드에 대하여 동적으로 복호화할 수 있게 한코드블록 암호화 방법

(57) 요약

본 발명은 실행코드를 기본블록들로 분할하고 분할한 기본블록들을 일정한 크기의 실행코드블록단위로 재구성하고 이렇게 재구성된 실행코드블록을 중복함으로써, 암호화된 실행코드에 대하여 동적으로 복호화할 수 있게 한 코드블록 암호화 방법에 관한 것이다.

본 발명에 따른 암호화된 실행코드에 대하여 동적으로 복호화할 수 있게 한 코드블록 암호화 방법은 분기 명령어나 점프 명령어 등의 제어이동명령어(control transfer instruction) 위치를 중심으로 실행코드를 기본블록으로 분할하는 과정과 ; 기본블록들을 실행하기에 적합한 일정크기의 블록인 실행코드블록으로 재구성하는 과정과 ; 블록암호화를 하기 전에 선행암호블록이나 키가 두 개 이상 존재하는 문제를 회피하기 위해 실행코드블록을 중복하는 과정과 ; 문제를 회피한 이후 블록암호화를 하는 과정으로 이루어짐을 특징으로 한다.

대표도 - 도1



(56) 선행기술조사문헌
 KR100240372 B1
 KR100628280 B1
 KR1020010102990 A
 KR1020040077754 A
 KR1020060073598 A

이 발명을 지원한 국가연구개발사업

과제고유번호	C1090-0603-0016
부처명	정보통신연구진흥원
연구사업명	대학IT연구센터 육성지원사업
연구과제명	해킹·바이러스 대응기술 연구
주관기관	충남대학교
연구기간	2003년 8월 1일 ~ 2011년 8월 31일

특허청구의 범위

청구항 1

제어이동명령어 위치를 중심으로 실행코드를 기본블록으로 분할하는 과정;

기본블록들을 실행하기에 적합한 일정크기의 블록인 실행코드블록으로 재구성하는 과정;

블록암호화를 하기 전에 선행암호블록이나 키가 두 개 이상 존재하는 문제를 회피하기 위해 제어이동명령어의 목적지에 해당하는 실행코드블록을 중복하는 과정; 및

블록암호화를 하는 과정;을 포함하여 이루어짐을 특징으로 하는 암호화된 실행코드에 대하여 동적으로 복호화할 수 있게 한 코드블록 암호화 방법.

청구항 2

제 1 항에 있어서,

상기 기본블록을 실행코드블록으로 재구성하는 과정에 있어서 기본블록의 크기가 실행코드블록의 크기보다 작을 경우에는 기본블록에 임의 명령어나 분기 명령어 또는 점프 명령어를 추가하여 실행코드블록을 구성함을 특징으로 하는 암호화된 실행코드에 대하여 동적으로 복호화할 수 있게 한 코드블록 암호화 방법.

청구항 3

제 1 항에 있어서,

상기 기본블록을 실행코드블록으로 재구성하는 과정에 있어서 기본블록의 크기가 실행코드블록의 크기보다 클 경우에는 기본블록을 실행코드블록 단위로 분리하고 분리된 실행코드블록 중 기본블록의 크기보다 큰 실행코드블록에는 임의 명령어나 분기 명령어 또는 점프 명령어를 추가하여 실행코드블록을 구성함을 특징으로 하는 암호화된 실행코드에 대하여 동적으로 복호화할 수 있게 한 코드블록 암호화 방법.

청구항 4

제 1 항에 있어서,

상기 실행코드블록을 중복하는 과정은 블록암호화를 하기 전에 선행암호블록이나 키가 두 개 이상 존재하는 문제를 회피하기 위해 제어이동명령어의 목적지에 해당하는 실행코드블록을 중복함을 특징으로 하는 암호화된 실행코드에 대하여 동적으로 복호화할 수 있게 한 코드블록 암호화 방법.

명세서

발명의 상세한 설명

기술 분야

- <1> 본 발명은 실행코드에 대한 암호화 방법에 관한 것으로 상세하게는 분기 명령어나 점프 명령어 등의 제어이동명령어(control transfer instruction) 위치를 중심으로 실행코드를 기본블록들로 분할하고 분할한 기본블록들을 일정한 크기의 실행코드블록단위로 재구성하고 이렇게 재구성된 실행코드블록 중 제어이동명령어의 목적지(target)에 해당하는 실행코드블록을 중복함으로써, 암호화된 실행코드에 대하여 동적으로 복호화할 수 있게 한 코드블록 암호화 방법에 관한 것이다.
- <2> 실행코드를 외부로부터 은닉하기 위해 종래의 블록암호화 방식인 CBC(Cipher Block Chaining)와 키를 연결하는 방법을 이용할 수 있다.
- <3> 이러한 종래의 암호화 방법에 의해 암호화된 블록들은 시스템에서 실행하기 전에 프로그램 전체에 대해서 사전에 모두 복호화하여야 한다. 왜냐하면 실행코드는 데이터와 달리 코드 중간에 제어이동명령어를 포함하고 있어 블록의 실행순서가 일정하지 않기 때문이다.
- <4> 또한 이렇게 전체 블록들을 모두 복호화할 경우 실행코드를 메모리나 디스크에 임시로 저장하는 것이 불가피하므로 복호화된 실행코드가 외부로 노출될 위험이 있다.

- <5> 따라서 실행코드의 안전성을 개선하기 위해서는 블록의 실행순서를 예측할 수 없는 경우에도 실시간으로 실행할 블록별로 복호화할 수 있도록 하는 암호화 방법이 필요하다.
- <6> 도 4a와 도 4b는 종래의 블록암호화 방식을 도시한 블록도이다.
- <7> 도 4a는 종래의 CBC방식의 블록암호화를 도시한 블록도로서, N번째 평문블록N1을 암호화할 때는 N-1번째 암호블록(N-1)2와 N번째 평문블록N1을 배타적 논리합(exclusive or, 이하 "XOR"라 통칭한다.)한 후 암호화한다. 즉, 선행된 암호블록과 현재의 평문블록을 XOR한 후 그 결과를 암호화한다.
- <8> 도 4b는 종래의 키를 연결하는 방식의 블록암호화를 도시한 블록도이다.
- <9> N번째 평문블록N1을 암호화할 때는 N-1번째 평문블록(N-1)1을 이용하여 키를 생성하고, 이 키를 이용하여 N번째 평문블록N1을 암호화한다. 즉, 선행된 평문블록에서 키를 생성하고, 그 키를 이용하여 현재의 평문블록을 암호화하는 방식이다.
- <10> 이와 같은 종래의 블록암호화 방식은 제어이동명령어를 포함하는 실행코드를 암호화할 때 제어이동명령어의 목적지 블록에서 문제가 발생한다. 도 5a와 도 5b는 위와 같은 종래의 방법으로 제어이동명령어를 포함하는 실행코드를 블록암호화할 때 제어이동명령어의 목적지에 해당하는 블록에서 발생하는 문제점의 예를 보이는 도면이다.
- <11> 도 5a는 종래의 CBC방식으로 제어이동명령어를 포함한 실행코드를 블록암호화할 경우, 제어이동명령어의 목적지에 해당하는 블록에서 선행암호블록이 두 개 이상 존재하는 문제점의 예를 도시한 블록도이다. 도시한 바와 같이, 제어이동명령어로 인하여 평문블록21 뿐만 아니라 평문블록51에서도 평문블록31로 제어가 전이되는 경우를 보인다.
- <12> 평문블록31을 암호화하기 위해서 선행암호블록과 평문블록31을 XOR하여야하는데, 평문블록31의 선행암호블록이 암호블록22와 암호블록52 두 개가 존재하므로, 평문블록31을 XOR할 때 선행암호블록이 두 개 이상이 되는 문제가 발생한다.
- <13> 도 5b는 종래의 키를 연결하는 방식으로 제어이동명령어를 포함한 실행코드를 블록암호화 할 경우로서, 제어이동명령어의 목적지에 해당하는 블록에서 키가 두 개 이상 존재하는 문제점의 예를 도시한 블록도이다. 도시한 바와 같이, 제어이동명령어로 인하여 평문블록21 뿐만 아니라 평문블록51에서도 평문블록31로 제어가 전이되는 경우를 보인다.
- <14> 평문블록31을 암호화하기 위해서 선행블록으로부터 키를 생성하여 얻어야 하는데, 평문블록31의 선행블록이 평문블록21과 평문블록51 두 개가 존재하므로, 평문블록31을 암호화할 시점에서 키가 두 개 이상인 문제가 발생한다.

발명의 내용

해결 하고자하는 과제

- <15> 본 발명은 위와 같은 문제점을 해결하기 위해 발명된 것으로, 실행코드를 기본블록들로 분할하고 분할한 기본블록들을 일정한 크기의 실행코드블록단위로 재구성하고 이렇게 재구성된 실행코드블록들 중 제어이동명령어의 목적지에 해당하는 실행코드블록들을 중복하여 실행코드를 암호화할 때 선행암호블록이나 키가 두 개 이상 존재하는 문제를 회피할 수 있게 함으로써 암호화된 실행코드에 대하여 동적으로 복호화할 수 있도록 하는 코드블록 암호화 방법을 제공하는 것을 목적으로 한다.

과제 해결수단

- <16> 상기 목적을 달성하기 위한 본 발명에 따른 암호화된 실행코드에 대하여 동적으로 복호화할 수 있게 한 코드블록 암호화 방법은 제어이동명령어 위치를 중심으로 실행코드를 기본블록으로 분할하는 과정과 ; 기본블록들을 실행하기에 적합한 일정크기의 블록인 실행코드블록으로 재구성하는 과정과 ; 블록암호화를 하기 전에 선행암호블록이나 키가 두 개 이상 존재하는 문제를 회피하기 위해 제어이동명령어의 목적지에 해당하는 실행코드블록을 중복하는 과정과 ; 블록암호화를 하는 과정으로 이루어짐을 특징으로 한다.

효 과

- <17> 본 발명은 실행코드를 기본블록들로 분할하고 분할한 기본블록들을 일정한 크기의 실행코드블록단위로 재구성하고 이렇게 재구성된 실행코드블록들 중 제어이동명령어의 목적지에 해당하는 실행코드블록을 중복하여 암호화함으로써 선행암호블록이나 키가 두 개 이상 존재하는 문제를 회피할 수 있으므로 암호화된 실행코드에 대하여 동적으로 복호화할 수 있도록 한다.
- <18> 이에 따라 실행코드를 실행할 때 코드가 외부로 노출되는 것을 최소화할 수 있다. 즉, 블록복호화모듈을 하드웨어로 구현하고 실행코드를 실행할 시스템과 연동하도록 구현할 경우 전체 실행코드가 아닌 실행 시 필요한 블록들만 복호화가 가능하여 실행코드가 외부로 노출되는 것을 최소화할 수 있는 효과가 있다.
- <19> 또한, 실행코드의 역분석 방지 및 악성코드로 인한 실행코드의 오염 방지에 응용할 수 있는 효과가 있다.

발명의 실시를 위한 구체적인 내용

- <20> 이하에서는 첨부된 도면을 참조하여 기술되는 바람직한 실시예를 통하여 본 발명을 당업자가 용이하게 이해하고 재현할 수 있도록 상세히 기술하기로 한다.
- <21> 도 1은 본 발명에 따른 제어이동명령어를 포함한 실행코드를 암호화하기 위한 방법을 나타낸 순서도이고, 도 2a는 본 발명에 따른 기본블록의 크기가 실행코드블록의 크기보다 작을 때, 기본블록을 일정크기의 블록인 실행코드블록의 크기만큼 명령어를 이용하여 메우는 방법의 예를 보인 블록도이고, 도 2b는 본 발명에 따른 기본블록의 크기가 실행코드블록의 크기보다 클 때, 기본블록을 일정크기의 블록인 실행코드블록의 크기단위로 나누는 방법의 예를 보인 블록도이고, 도 3a는 본 발명에 따른 제어이동명령어를 포함한 실행코드를 CBC방식으로 블록 암호화할 때, 선행암호블록이 두 개 이상 존재하는 문제를 회피하기 위해 제어이동명령어의 목적지에 해당하는 실행코드블록을 중복하는 방법의 예를 보인 블록도이고, 도 3b는 본 발명에 따른 제어이동명령어를 포함한 실행코드를 키를 연결하는 방식으로 블록암호화할 때, 키가 두 개 이상 존재하는 문제를 회피하기 위해 제어이동명령어의 목적지에 해당하는 실행코드블록을 중복하는 방법의 예를 보인 블록도이다.
- <22> 도 1에 도시한 바와 같이 본 발명에 따른 암호화된 실행코드에 대하여 동적으로 복호화할 수 있게 한 코드블록 암호화 방법은 먼저, 제어이동명령어 위치를 중심으로 실행코드를 기본블록으로 분할하는 과정과 ; 기본블록들을 실행하기에 적합한 일정크기의 블록인 실행코드블록으로 재구성하는 과정과 ; 블록암호화를 하기 전에 선행암호블록이나 키가 두 개 이상 존재하는 문제를 회피하기 위해 제어이동명령어의 목적지에 해당하는 실행코드블록을 중복하는 과정과 ; 블록암호화를 하는 과정으로 이루어진다.
- <23> 상기 제어이동명령어는 분기명령어나 점프 명령어 등이 있다.
- <24> 이러한 과정으로 이루어지는 본 발명의 암호화된 실행코드에 대하여 동적으로 복호화할 수 있게 한 코드블록 암호화 방법의 요지는 상기 기본블록들을 실행하기에 적합한 일정크기의 블록인 실행코드블록으로 재구성하는 과정과 블록암호화를 하기 전에 선행암호블록이나 키가 두 개 이상 존재하는 문제를 회피하기 위해 제어이동명령어의 목적지에 해당하는 실행코드블록을 중복하는 과정에 있다.
- <25> 상기 기본블록을 실행코드블록으로 재구성하는 과정은 기본블록의 크기에 따라 달라진다.
- <26> 즉, 상기 기본블록의 크기가 실행코드블록의 크기보다 작을 경우에는 기본블록에 임의 명령어나 분기 명령어 또는 점프 명령어를 추가하여 실행코드블록을 구성하고, 기본블록의 크기가 실행코드블록의 크기보다 큰 경우에는 기본블록을 실행코드블록 단위로 분리하고 분리된 실행코드블록 중 기본블록의 크기보다 큰 실행코드블록에는 임의 명령어나 분기 명령어 또는 점프 명령어를 추가하여 실행코드블록을 구성한다.
- <27> 도 2a에 도시한 바와 같이 기본블록의 크기가 실행코드블록의 크기보다 작을 경우에는 기본블록의 명령어에 분기(Branch)명령어(B)나 점프(Jump) 명령어(J) 또는 임의(Dummy) 명령어(D) 등을 추가하여 기본블록의 크기를 실행코드블록의 크기로 맞춘다.
- <28> 즉, 실행코드블록의 크기와 기본블록의 크기의 차이가 2이면, 하나의 점프(Jump) 명령어(J)와 하나 이상의 임의(Dummy) 명령어(D)를 이용하여 빈 공간을 메운다. 여기서 임의 명령어(D)는 무작위(random)함수를 이용하여 임의의 값으로 생성한다. 대안으로 모든 빈 공간을 무연산(no operation)을 이용하여 메울 수도 있지만, 그럴 경우 암호화시에 암호블록이 보안에 약해지는 문제점을 가지므로 상기한 바와 같은 다양한 종류의 명령어들을 추가하여 메우는 것이 바람직하다.
- <29> 또한, 실행코드블록의 크기와 기본블록의 크기의 차이가 1 이면, 이 빈 공간은 한 개의 무연산(no operation)으로 메울 수 있다.

- <30> 도 2b는 기본블록의 크기가 실행코드블록의 크기보다 클 때로서, 기본블록을 일정크기 즉 크기 4인 실행코드블록의 크기단위로 나누는 방법의 예를 보인 블록도이다.
- <31> 도면의 화살표 왼쪽이 실행코드블록 보다 큰 기본블록이고, 도면의 오른쪽이 실행코드블록으로 나눈 이후의 결과를 나타낸 것이다. 기본블록을 실행코드블록단위로 나누는 방법은 다음과 같다.
- <32> 우선 기본블록의 처음부터 실행코드블록크기만큼 순서대로 나눈다. 이렇게 나눌 경우, 나누는 마지막 부분이 실행코드블록의 크기보다 작게 나뉘지는 경우가 발생하는데, 이때는 도면 2a에서 설명한 블록을 메우는 방법을 이용하여 마지막 부분을 실행코드블록단위로 재구성한다.
- <33> 도 3a 및 3b는 제어이동명령어를 포함한 실행코드를 위에서 설명한 CBC방식이나 키를 연결하는 방식으로 블록암호화 할 때, 선행암호블록이나 키가 두 개 이상 존재하는 문제를 회피하기 위해 제어이동명령어의 목적지에 해당하는 실행코드블록을 중복하는 방법의 예를 보인 블록도이다.
- <34> 도 3a는 본 발명에 따른 분기 명령어를 포함한 실행코드를 CBC방식으로 블록암호화할 때, 선행암호블록이 두 개 이상 존재하는 문제를 회피하기 위해, 제어이동명령어의 목적지에 해당하는 실행코드블록을 중복하는 방법의 예를 보인 블록도이다.
- <35> 평문블록31은 선행암호블록22와 XOR하고, 평문블록3a1은 선행암호블록52와 XOR 하므로 평문블록31에서 발생하던 선행암호블록이 두 개 이상인 문제를 회피하였다.
- <36> 이후 평문블록41은 선행암호블록이 두 개 이상이지만, 평문블록3a1은 평문블록31을 중복한 것이기 때문에 선행암호블록 중 어떤 블록을 선택하든 상관없이 평문블록41과 XOR한 결과는 동일하다.
- <37> 도 3b는 본 발명에 따른 분기 명령어를 포함한 실행코드를 키를 연결하는 방식으로 블록암호화할 때, 키가 두 개 이상 존재하는 문제를 회피하기 위해 제어이동명령어의 목적지에 해당하는 실행코드블록을 중복하는 방법의 예를 보인 블록도이다.
- <38> 도시한 바와 같이, 평문블록31은 암호화를 위해 평문블록21으로부터 키를 얻어오고, 평문블록3a1은 평문블록51로부터 키를 얻어온다. 결과적으로 평문블록31에서 발생하던 키가 두 개 이상 생성되는 문제는 해결되었다.
- <39> 이후 평문블록41은 선행블록이 두 개 이상이지만 평문블록3a1은 평문블록31을 중복한 것이기 때문에, 선행평문블록 중 어떤 블록을 선택하든지 키 생성 결과는 같다.

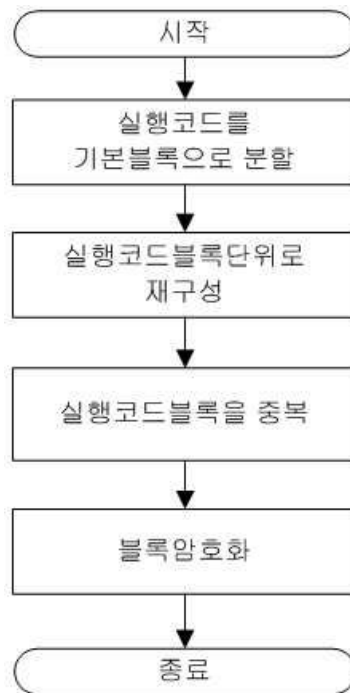
도면의 간단한 설명

- <40> 도 1은 본 발명에 따른 분기 명령어나 점프 명령어 등의 제어이동명령어(control transfer instruction)를 포함한 실행코드를 암호화하기 위한 방법을 나타낸 순서도이고,
- <41> 도 2a는 본 발명에 따른 기본블록의 크기가 실행코드블록의 크기보다 작을 때, 기본블록을 일정크기의 블록인 실행코드블록 크기만큼 명령어를 이용하여 메우는 방법의 예를 보인 블록도이고,
- <42> 도 2b는 본 발명에 따른 기본블록의 크기가 실행코드블록의 크기보다 클 때, 기본블록을 일정크기의 블록인 실행코드블록의 크기단위로 나누는 방법의 예를 보인 블록도이고,
- <43> 도 3a는 본 발명에 따른 제어이동명령어를 포함한 실행코드를 CBC방식으로 블록암호화할 때, 선행암호블록이 두 개 이상 존재하는 문제를 회피하기 위해 제어이동명령어의 목적지에 해당하는 실행코드블록을 중복하는 방법의 예를 보인 블록도이고,
- <44> 도 3b는 본 발명에 따른 제어이동명령어를 포함한 실행코드를 키를 연결하는 방식으로 블록암호화할 때, 키가 두 개 이상 존재하는 문제를 회피하기 위해 제어이동명령어의 목적지에 해당하는 실행코드블록을 중복하는 방법의 예를 보인 블록도이고,
- <45> 도 4a는 종래의 CBC 방식의 블록암호화를 도시한 블록도이고,
- <46> 도 4b는 종래의 키를 연결하는 방식의 블록암호화를 도시한 블록도이고,
- <47> 도 5a는 종래의 CBC 방식으로 제어이동명령어를 포함한 실행코드를 블록암호화할 경우, 제어이동명령어의 목적지에 해당하는 블록에서 선행암호블록이 두 개 이상 존재하는 문제점의 예를 도시한 블록도이고,
- <48> 도 5b는 종래의 키를 연결하는 방식으로 제어이동명령어를 포함한 실행코드를 블록암호화 할 경우, 제어이동명

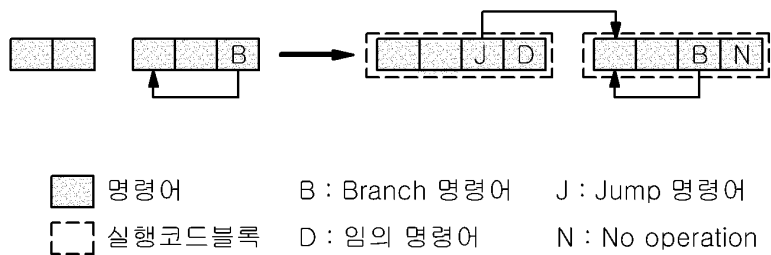
명령어의 목적지에 해당하는 블록에서 키가 두 개 이상 존재하는 문제점의 예를 도시한 블록도이다.

도면

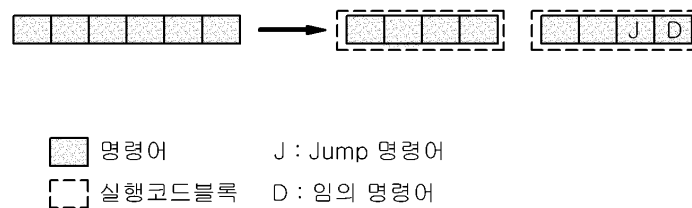
도면1



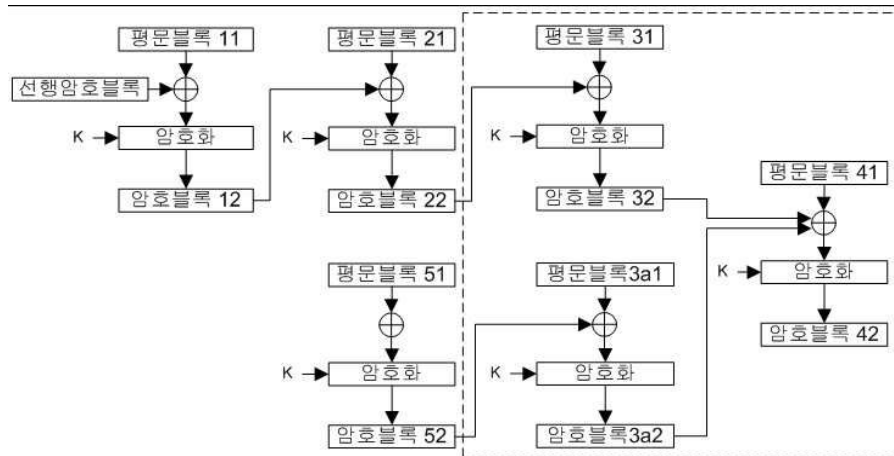
도면2a



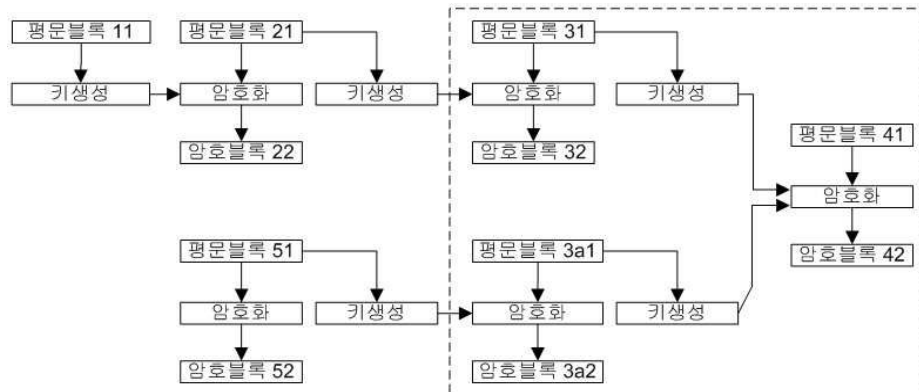
도면2b



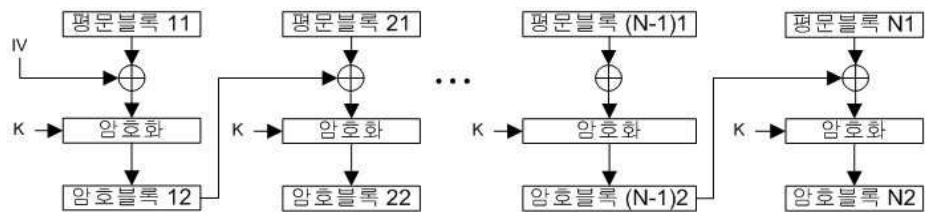
도면3a



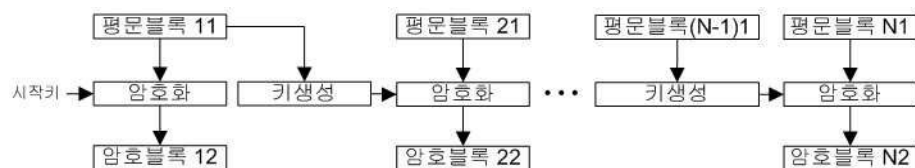
도면3b



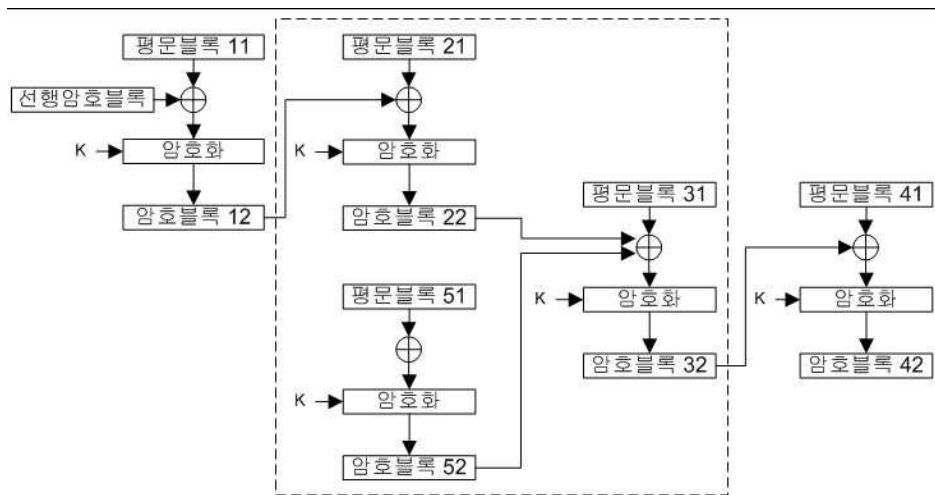
도면4a



도면4b



도면5a



도면5b

