



(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2020-0067414
(43) 공개일자 2020년06월12일

(51) 국제특허분류(Int. Cl.)

H04L 9/06 (2006.01)

(52) CPC특허분류

H04L 9/0656 (2013.01)

H04L 2209/046 (2013.01)

(21) 출원번호 10-2018-0154236

(22) 출원일자 2018년12월04일

심사청구일자 2018년12월04일

(71) 출원인

고려대학교 산학협력단

서울특별시 성북구 안암로 145, 고려대학교 (안암동5가)

(72) 발명자

홍석희

서울특별시 노원구 덕릉로71길 30, 206-2304 (중계동, 양지대림아파트)

김희석

대전광역시 유성구 지족북로 33, 107동 1301호(지족동, 한화꿈에그린 1블럭)

(뒷면에 계속)

(74) 대리인

윤귀상

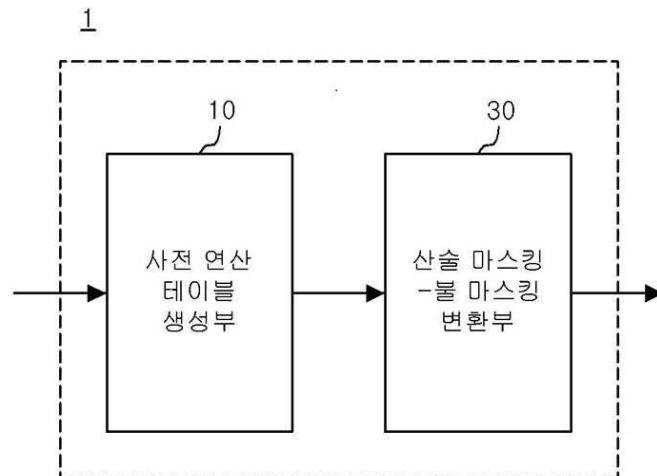
전체 청구항 수 : 총 10 항

(54) 발명의 명칭 산술 마스크-불 마스크 변환 방법, 이를 수행하기 위한 기록매체 및 장치

(57) 요약

산술 마스크-불 마스크 변환 방법, 이를 수행하기 위한 기록매체 및 장치가 개시된다. 산술 마스크-불 마스크 변환 방법은 산술 마스크(Arithmetic Masking) 상태의 데이터에서 최하위 비트(LSB: Least significant bit)를 제외하고 각 비트를 불 마스크(Boolean Masking) 처리하여 G 테이블을 생성하는 단계, 상기 G 테이블 생성 단계에서 발생하는 캐리 비트를 불 마스크 처리하여 C 테이블을 생성하는 단계, 상기 G 테이블을 이용하여 상기 산술 마스크 상태의 데이터 각 비트를 불 마스크 처리하는 단계에서 캐리 비트의 발생 여부를 확인하는 단계 및 상기 C 테이블을 이용하여 상기 산술 마스크 상태의 데이터에서 캐리 비트를 제거한 뒤 상기 G 테이블을 이용하여 상기 산술 마스크 상태의 데이터를 불 마스크 상태로 변환하는 단계를 포함한다.

대표도 - 도1



(72) 발명자

김한빛

서울시 성북구 안암로 145 ((안암동5가, 고려대학교안암캠퍼스)) 자연계캠퍼스 미래융합기술관 301호 암호알고리즘 연구실

조은지

경기도 군포시 산본천로214번길 45(산본동)

이 발명을 지원한 국가연구개발사업

과제고유번호 20170005200022002

부처명 과학기술정보통신부

연구관리전문기관 정보통신기술진흥센터

연구사업명 정보보호핵심원천기술개발(R&D)

연구과제명 (ICT 기초연구실) SCR-Friendly 대칭키 암호 및 응용모드 개발

기 여 율 1/1

주관기관 국민대학교 산학협력단

연구기간 2018.01.01 ~ 2018.12.31

명세서

청구범위

청구항 1

산술 마스크(Arithmetic Masking) 상태의 데이터에서 최하위 비트(LSB: Least significant bit)를 제외하고 각 비트를 불 마스크(Boolean Masking) 처리하여 G 테이블을 생성하는 단계;

상기 G 테이블 생성 단계에서 발생하는 캐리 비트를 불 마스크 처리하여 C 테이블을 생성하는 단계;

상기 G 테이블을 이용하여 상기 산술 마스크 상태의 데이터 각 비트를 불 마스크 처리하는 단계에서 캐리 비트의 발생 여부를 확인하는 단계; 및

상기 C 테이블을 이용하여 상기 산술 마스크 상태의 데이터에서 캐리 비트를 제거한 뒤 상기 G 테이블을 이용하여 상기 산술 마스크 상태의 데이터를 불 마스크 상태로 변환하는 단계를 포함하는 산술 마스크-불 마스크 변환 방법.

청구항 2

제1항에 있어서,

상기 G 테이블 생성 단계에서 발생하는 캐리 비트를 불 마스크 처리하여 C 테이블을 생성하는 단계는,

상기 산술 마스크 상태의 데이터를 불 마스크 상태로 변환하는 경우, 상기 C 테이블을 생성하는 단계에서 캐리 비트와 더해지는 난수(α)를 제거할 수 있도록 상기 산술 마스크 상태의 데이터의 각 비트마다 상기 G 테이블 생성 단계에서 발생하는 캐리 비트를 불 마스크 처리한 값을 더하여 저장하는 단계를 포함하는 산술 마스크-불 마스크 변환 방법.

청구항 3

제1항에 있어서,

산술 마스크 상태의 데이터에서 최하위 비트(LSB: Least significant bit)를 제외하고 각 비트를 불 마스크 처리하여 G 테이블을 생성하는 단계는,

상기 산술 마스크 상태의 데이터 각 비트에 랜덤 값(r)을 더하고 불 마스크 처리하여 상기 G 테이블을 생성하는 단계를 포함하는 산술 마스크-불 마스크 변환 방법.

청구항 4

제3항에 있어서,

상기 G 테이블 생성 단계에서 발생하는 캐리 비트를 불 마스크 처리하여 C 테이블을 생성하는 단계는,

상기 캐리 비트와 난수(α)의 합에 2^k (여기서, k 는 상기 데이터의 비트 자리 수)를 곱한 값으로 연산하여 상기 C 테이블을 생성하는 단계를 포함하는 산술 마스크-불 마스크 변환 방법.

청구항 5

제4항에 있어서,

상기 G 테이블을 이용하여 상기 산술 마스크 상태의 데이터 각 비트를 불 마스크 처리하는 단계에서 캐리 비트의 발생 여부를 확인하는 단계는,

상기 산술 마스크 상태의 데이터 각 비트에 상기 랜덤 값(r) 및 상기 난수(α)를 뺀 값을 초기 값으로 설정하는 단계; 및

하위 비트를 상위 비트로 올릴 수 있도록 상기 초기 값에 마스크 값(R)을 더하여 하위 비트를 상위 비트로 올리는 단계를 포함하는 산술 마스크-불 마스크 변환 방법.

청구항 6

제5항에 있어서,

상기 C 테이블을 이용하여 상기 산술 마스크링 상태의 데이터에서 캐리 비트를 제거한 뒤 상기 G 테이블을 이용하여 상기 산술 마스크링 상태의 데이터를 불 마스크링 상태로 변환하는 단계는,

상기 산술 마스크링 상태의 데이터 각 비트를 불 마스크링 처리하는 단계에서 캐리 비트가 발생한 경우, 상기 초기 값에 마스크링 값(R)을 더한 값에 상기 난수(α) 및 1을 더하여 상기 캐리 비트 및 상기 난수(α)를 제거하는 단계; 및

상기 산술 마스크링 상태의 데이터 각 비트를 불 마스크링 처리하는 단계에서 캐리 비트가 발생하지 않은 경우, 상기 난수(α)를 더하여 상기 캐리 비트 및 상기 난수(α)를 제거하는 단계를 포함하는 산술 마스크링-불 마스크링 변환 방법.

청구항 7

제6항에 있어서,

상기 C 테이블을 이용하여 상기 산술 마스크링 상태의 데이터에서 캐리 비트를 제거한 뒤 상기 G 테이블을 이용하여 상기 산술 마스크링 상태의 데이터를 불 마스크링 상태로 변환하는 단계는,

상기 C 테이블을 이용하여 상기 산술 마스크링 상태의 데이터에서 캐리 비트를 제거하고, XOR 연산을 이용하여 상기 랜덤 값(r)을 반환하는 단계를 포함하는 산술 마스크링-불 마스크링 변환 방법.

청구항 8

제7항에 있어서,

상기 C 테이블을 이용하여 상기 산술 마스크링 상태의 데이터에서 캐리 비트를 제거한 뒤 상기 G 테이블을 이용하여 상기 산술 마스크링 상태의 데이터를 불 마스크링 상태로 변환하는 단계는,

상기 산술 마스크링 상태의 데이터 각 비트를 불 마스크링 상태로 변환하고 데이터의 각 비트 자리에 저장되도록 처리하는 단계를 포함하는 산술 마스크링-불 마스크링 변환 방법.

청구항 9

제1항 내지 제8항 중 어느 하나의 항에 따른 산술 마스크링-불 마스크링 변환 방법을 수행하기 위한, 컴퓨터 프로그램이 기록된 컴퓨터로 판독 가능한 기록 매체.

청구항 10

산술 마스크링(Arithmetic Masking) 상태의 데이터에서 최하위 비트(LSB: Least significant bit)를 제외하고 각 비트를 불 마스크링(Boolean Masking) 처리하여 G 테이블을 생성하고, 상기 G 테이블 생성 단계에서 발생하는 캐리 비트를 불 마스크링 처리하여 C 테이블을 생성하는 사전 연산 테이블 생성부; 및

상기 G 테이블을 이용하여 상기 산술 마스크링 상태의 데이터 각 비트를 불 마스크링 처리하는 단계에서 캐리 비트의 발생 여부를 확인하고, 상기 C 테이블을 이용하여 상기 산술 마스크링 상태의 데이터에서 캐리 비트를 제거한 뒤 상기 G 테이블을 이용하여 상기 산술 마스크링 상태의 데이터를 불 마스크링 상태로 변환하는 산술 마스크링-불 마스크링 변환부를 포함하는 산술 마스크링-불 마스크링 변환 장치.

발명의 설명**기술 분야**

본 발명은 산술 마스크링-불 마스크링 변환 방법, 이를 수행하기 위한 기록매체 및 장치에 관한 것으로, 보다 상세하게는 불 연산자와 산술 연산자를 사용하는 암호 알고리즘에서 산술 마스크링에서 불 마스크링으로 마스크링의 형태를 변환하는 산술 마스크링-불 마스크링 변환 방법, 이를 수행하기 위한 기록매체 및 장치에 관한 것이다.

배경 기술

[0001]

- [0002] 전력 분석 공격은 공격자가 암호 알고리즘이 수행되는 동안 발생하는 전력 신호를 분석하여 비밀 정보를 알아내는 부채널 공격 기법이다.
- [0003] 이러한 부채널 공격의 대응 방안으로 널리 알려진 방법 중 하나는 마스킹 기법이다.
- [0004] 마스킹 기법은 크게 불 마스킹(Boolean Masking) 기법과 산술 마스킹(Arithmetic Masking) 기법의 두 종류로 나뉠 수 있다. 불 마스킹 기법은 XOR 연산을 통한 형태가 대표적이고, 산술 마스킹 기법은 뺄셈 연산을 이용한 형태가 대표적이다.
- [0005] 이러한 두 마스킹 기법은 ARX(addition, Rotation, XOR) 블록 암호 알고리즘에 적용될 수 있다. ARX 블록 암호 알고리즘은 불 마스킹 기법과 산술 마스킹 기법을 반복하여 사용하기 때문에 불 마스킹과 산술 마스킹을 전환하는 단계가 필요하다.
- [0006] 산술 마스킹에서 불 마스킹으로 전환하는 알고리즘은 활발히 연구되고 있다. 산술 마스킹에서 불 마스킹으로 전환하는 알고리즘은 덧셈의 캐리(carry)를 처리하는 방식에 따라 자리 올림수 예측 가산기(carry look-ahead adder)에 기반한 알고리즘과 리플 자리 올림수 가산기(ripple-carry adder)에 기반한 알고리즘으로 나뉠 수 있다.
- [0007] 자리 올림수 예측 가산기에 기반한 알고리즘의 경우, 불 연산만으로 캐리를 처리할 수 있다는 장점이 있으나 메모리를 사용하여 연산 속도를 높이기에는 한계가 있다.
- [0008] 리플 자리 올림수 가산기에 기반한 알고리즘의 경우 메모리를 사용하여 연산 속도를 최적화하기에 용이하나, 저장 공간의 활용과 연산 속도 최적화 사이에 적절한 균형을 유지하여야 한다.

발명의 내용

해결하려는 과제

- [0009] 본 발명의 일측면은 LSB(Least significant bit) 트릭 기술을 적용하여 사전 연산 테이블을 생성하고, 리플 자리 올림수 가산기에 기반한 A2B 알고리즘을 수행하는 산술 마스킹-불 마스킹 변환 방법, 이를 수행하기 위한 기록매체 및 장치를 제공한다.

과제의 해결 수단

- [0010] 본 발명에 따른 산술 마스킹-불 마스킹 변환 방법은 산술 마스킹(Arithmetic Masking) 상태의 데이터에서 최하위 비트(LSB: Least significant bit)를 제외하고 각 비트를 불 마스킹(Boolean Masking) 처리하여 G 테이블을 생성하는 단계, 상기 G 테이블 생성 단계에서 발생하는 캐리 비트를 불 마스킹 처리하여 C 테이블을 생성하는 단계, 상기 G 테이블을 이용하여 상기 산술 마스킹 상태의 데이터 각 비트를 불 마스킹 처리하는 단계에서 캐리 비트의 발생 여부를 확인하는 단계 및 상기 C 테이블을 이용하여 상기 산술 마스킹 상태의 데이터에서 캐리 비트를 제거한 뒤 상기 G 테이블을 이용하여 상기 산술 마스킹 상태의 데이터를 불 마스킹 상태로 변환하는 단계를 포함한다.
- [0011] 한편, 상기 G 테이블 생성 단계에서 발생하는 캐리 비트를 불 마스킹 처리하여 C 테이블을 생성하는 단계는, 상기 산술 마스킹 상태의 데이터를 불 마스킹 상태로 변환하는 경우, 상기 C 테이블을 생성하는 단계에서 캐리 비트와 더해지는 난수(α)를 제거할 수 있도록 상기 산술 마스킹 상태의 데이터의 각 비트마다 상기 G 테이블 생성 단계에서 발생하는 캐리 비트를 불 마스킹 처리한 값을 더하여 저장하는 단계를 포함할 수 있다.
- [0012] 또한, 산술 마스킹 상태의 데이터에서 최하위 비트(LSB: Least significant bit)를 제외하고 각 비트를 불 마스킹 처리하여 G 테이블을 생성하는 단계는, 상기 산술 마스킹 상태의 데이터 각 비트에 랜덤 값(r)을 더하고 불 마스킹 처리하여 상기 G 테이블을 생성하는 단계를 포함할 수 있다.
- [0013] 또한, 상기 G 테이블 생성 단계에서 발생하는 캐리 비트를 불 마스킹 처리하여 C 테이블을 생성하는 단계는, 상기 캐리 비트와 난수(α)의 합에 2^k (여기서, k 는 상기 데이터의 비트 자리 수)를 곱한 값으로 연산하여 상기 C 테이블을 생성하는 단계를 포함할 수 있다.
- [0014] 또한, 상기 G 테이블을 이용하여 상기 산술 마스킹 상태의 데이터 각 비트를 불 마스킹 처리하는 단계에서 캐리 비트의 발생 여부를 확인하는 단계는, 상기 산술 마스킹 상태의 데이터 각 비트에 상기 랜덤 값(r) 및 상기 난수(α)를 뺀 값을 초기 값으로 설정하는 단계 및 하위 비트를 상위 비트로 올릴 수 있도록 상기 초기 값에 마스

킹 값(R)을 더하여 하위 비트를 상위 비트로 올리는 단계를 포함할 수 있다.

[0015] 또한, 상기 C 테이블을 이용하여 상기 산술 마스크 상태의 데이터에서 캐리 비트를 제거한 뒤 상기 G 테이블을 이용하여 상기 산술 마스크 상태의 데이터를 불 마스크 상태로 변환하는 단계는, 상기 산술 마스크 상태의 데이터 각 비트를 불 마스크 처리하는 단계에서 캐리 비트가 발생한 경우, 상기 초기 값에 마스크 값(R)을 더한 값에 상기 난수(α) 및 1을 더하여 상기 캐리 비트 및 상기 난수(α)를 제거하는 단계 및 상기 산술 마스크 상태의 데이터 각 비트를 불 마스크 처리하는 단계에서 캐리 비트가 발생하지 않은 경우, 상기 난수(α)를 더하여 상기 캐리 비트 및 상기 난수(α)를 제거하는 단계를 포함할 수 있다.

[0016] 또한, 상기 C 테이블을 이용하여 상기 산술 마스크 상태의 데이터에서 캐리 비트를 제거한 뒤 상기 G 테이블을 이용하여 상기 산술 마스크 상태의 데이터를 불 마스크 상태로 변환하는 단계는, 상기 C 테이블을 이용하여 상기 산술 마스크 상태의 데이터에서 캐리 비트를 제거하고, XOR 연산을 이용하여 상기 랜덤 값(r)을 반환하는 단계를 포함할 수 있다.

[0017] 또한, 상기 C 테이블을 이용하여 상기 산술 마스크 상태의 데이터에서 캐리 비트를 제거한 뒤 상기 G 테이블을 이용하여 상기 산술 마스크 상태의 데이터를 불 마스크 상태로 변환하는 단계는, 상기 산술 마스크 상태의 데이터 각 비트를 불 마스크 상태로 변환하고 데이터의 각 비트 자리에 저장되도록 처리하는 단계를 포함할 수 있다.

[0018] 또한, 상기 산술 마스크-불 마스크 변환 방법을 수행하기 위한, 컴퓨터 프로그램이 기록된 컴퓨터로 판독 가능한 기록 매체일 수 있다.

[0019] 한편, 본 발명의 산술 마스크-불 마스크 변환 장치는 산술 마스크(Arithmetic Masking) 상태의 데이터에서 최하위 비트(LSB: Least significant bit)를 제외하고 각 비트를 불 마스크(Boolean Masking) 처리하여 G 테이블을 생성하고, 상기 G 테이블 생성 단계에서 발생하는 캐리 비트를 불 마스크 처리하여 C 테이블을 생성하는 사전 연산 테이블 생성부 및 상기 G 테이블을 이용하여 상기 산술 마스크 상태의 데이터 각 비트를 불 마스크 처리하는 단계에서 캐리 비트의 발생 여부를 확인하고, 상기 C 테이블을 이용하여 상기 산술 마스크 상태의 데이터에서 캐리 비트를 제거한 뒤 상기 G 테이블을 이용하여 상기 산술 마스크 상태의 데이터를 불 마스크 상태로 변환하는 산술 마스크-불 마스크 변환부를 포함한다.

발명의 효과

[0020] 본 발명에 따르면 사전 연산 테이블 저장에 필요한 메모리를 적게 사용할 수 있으며 연산 소요시간을 향상시킬 수 있다. 따라서 저메모리 환경에서 부채널 분석 공격에 대응할 수 있다.

도면의 간단한 설명

[0021] 도 1은 본 발명의 일 실시예에 따른 산술 마스크-불 마스크 변환 장치의 블록도이다.

도 2는 본 발명의 일 실시예에 따른 산술 마스크-불 마스크 변환 방법의 순서도이다.

도 3 및 도 4는 도 2에 도시된 산술 마스크-불 마스크 변환 방법을 보여주는 실행 코드의 일 예이다.

발명을 실시하기 위한 구체적인 내용

[0022] 본 발명의 이점 및 특징, 그리고 그것들을 달성하는 방법은 첨부되는 도면과 함께 상세하게 후술되어 있는 실시예들을 참조하면 명확해질 것이다. 그러나 본 발명은 이하에서 개시되는 실시예들에 한정되는 것이 아니라 서로 다른 다양한 형태로 구현될 것이며, 단지 본 실시예들은 본 발명의 개시가 완전하도록 하며, 본 발명이 속하는 기술분야에서 통상의 지식을 가진 자에게 발명의 범주를 완전하게 알려주기 위해 제공되는 것이며, 본 발명은 청구항의 범주에 의해 정의될 뿐이다. 명세서 전체에 걸쳐 동일 참조 부호는 동일 구성 요소를 지칭한다.

[0023] 본 명세서에서 사용된 용어는 실시예들을 설명하기 위한 것이며 본 발명을 제한하고자 하는 것은 아니다. 본 명세서에서, 단수형은 문구에서 특별히 언급하지 않는 한 복수형도 포함한다. 명세서에서 사용되는 "포함한다(comprises)" 및/또는 "포함하는(comprising)"은 언급된 구성요소, 단계 및 동작은 하나 이상의 다른 구성요소, 단계 및 동작의 존재 또는 추가를 배제하지 않는다.

[0025] 도 1은 본 발명의 일 실시예에 따른 산술 마스크-불 마스크 변환 장치의 블록도이다.

- [0026] 도 1을 참조하면, 본 발명의 일 실시예에 따른 산술 마스크-불 마스크 변환 장치(1)는 사전 연산 테이블 생성부(10) 및 산술 마스크-불 마스크 변환부(30)를 포함할 수 있다.
- [0027] 본 발명의 일 실시예에 따른 산술 마스크-불 마스크 변환 장치(1)는 ARX(Addition, Rotation, XOR) 블록 암호 알고리즘에서 마스크 기법을 산술 마스크로부터 불 마스크로 변환하는 산술 마스크-불 마스크 변환(A2B, Authmetic to Boolean Masking Conversion) 알고리즘을 수행할 수 있다.
- [0028] ARX 블록 암호 알고리즘은 산술 마스크(Authmetic Masking)으로 연산되는 덧셈 과정과 불 마스크(Boolean Masking)으로 연산되는 순환 및 XOR 연산이 하나의 라운드에 존재한다.
- [0029] 마스크 기법은 암호 알고리즘이 연산될 때 발생하는 중간 값을 랜덤하게 만들어 공격자에게 필요한 정보의 누출을 막는 대응 기법이다.
- [0030] 산술 마스크는 덧셈, 뺄셈 또는 곱셈의 대수 연산을 이용한 마스크 기법으로, 뺄셈을 이용한 $x' = x - r_x \bmod 2^k$ (x 는 데이터, r_x 는 난수 값)와 같은 형태가 대표적이다.
- [0031] 불 마스크는 배타적 논리합(XOR: Exclusive Or)을 이용한 마스크 기법으로, $x' = x \oplus r_x$ (x 는 데이터, r_x 는 난수 값)와 같은 형태가 대표적이다.
- [0032] 본 발명의 일 실시예에 따른 산술 마스크-불 마스크 변환 장치(1)는 리플 자리 올림수 가산기(ripple-carry adder)를 기반으로 한 산술 마스크-불 마스크 변환 알고리즘을 수행할 수 있다.
- [0033] 리플 자리 올림수 가산기는 하나의 비트를 보고 이 비트에 캐리 비트(올림수)가 발생하는지를 확인하고, 다음 비트에 캐리 비트를 전파하는 일련의 과정을 반복하여 비트를 처리한다. 즉, 리플 자리 올림수 가산기에 기반한 산술 마스크-불 마스크 변환 알고리즘은 상위 비트의 A2B 변환을 위해 하위 비트에서 생성되는 캐리 비트를 필요로 한다. 이러한 리플 자리 올림수 가산기는 메모리를 사용하여 동작 시간을 최적화하기에 용이하다는 장점을 갖는다.
- [0034] 본 발명의 일 실시예에 따른 산술 마스크-불 마스크 변환 장치(1)는 메모리를 사용하는 기기에 탑재되어 기기의 마스크 기법을 지원할 수 있다.
- [0035] 이하, 도 1에 도시된 본 발명의 일 실시예에 따른 산술 마스크-불 마스크 변환 장치(1)의 각 구성에 대하여 구체적으로 설명한다.
- [0036] 사전 연산 테이블 생성부(10)는 산술 마스크-불 마스크 변환에 필요한 참조 테이블(LUT: Look-Up Table)을 생성할 수 있다.
- [0037] 사전 연산 테이블 생성부(10)는 G 테이블 및 C 테이블을 생성할 수 있다.
- [0038] G 테이블은 산술 마스크 상태의 데이터의 각 비트를 불 마스크 처리하여 배열 G에 저장한 테이블이다.
- [0039] 사전 연산 테이블 생성부(10)는 이러한 G 테이블을 생성하는데, LSB(Least Significant bit) 트릭 기술을 적용하여 산술 마스크 상태의 데이터에서 최하위 비트(LSB)를 제외하고, 각 비트를 불 마스크 처리하여 G 테이블을 생성할 수 있다. 여기서, LSB 트릭 기술은 산술 마스크와 불 마스크 간에 최하위 비트의 결과 값이 동일하다는 성질을 이용하여 메모리를 줄이는 기술이다.
- [0040] 데이터의 크기가 $(n \cdot k)$ 비트인 것을 예로 들어 설명하면, 참조 테이블 및 변환 연산의 크기는 k 비트일 수 있다.
- [0041] 사전 연산 테이블 생성부(10)는 산술 마스크 상태의 데이터의 $(k+1)$ 비트에 해당하는 값(A)을 $\{(A + r) \oplus (y \parallel r)\} \in \mathbb{F}_2^{k+1}$ 과 같이 연산하여 불 마스크 처리하고, 배열 G에 저장하여 G 테이블을 생성할 수 있다. 이때, $\mathbb{F}_2$ 에서의 뺄셈 연산은 $(1-1 \equiv 0, 1-0 \equiv 1, 0-1 \equiv 1, 0-0 \equiv 0) \bmod 2$ 이고, XOR 연산은 $(1 \oplus 1 \equiv 0, 1 \oplus 0 \equiv 1, 0 \oplus 1 \equiv 1, 0 \oplus 0 \equiv 0) \bmod 2$ 로 그 결과가 동일하다. 따라서 사전 연산 테이블 생성부(10)는 최하위 비트를 제외하고 k 비트만을 불 마스크 처리하여 G 테이블을 생성하여도 무방하다. 이로 인해 본 발명의 일 실시예에 따른 산술 마스크-불 마스크 변환 장치(1)는 메모리 처리 단위로 8-bit의 char 형을 이용하는 기기에 적용되는 경우, 사용 메모리 양을 크게 줄일 수 있다.

- [0042] C 테이블을 G 테이블 생성 단계에서 발생하는 캐리 비트를 불 마스크 처리하여 배열 C 에 저장한 테이블이다.
- [0043] 사전 연산 테이블 생성부(10)는 산술 마스크 상태의 데이터 각 비트를 불 마스크 처리하는 단계에서 발생하는 캐리 비트(c)를 불 마스크 처리하여 C 테이블을 생성할 수 있다.
- [0044] 사전 연산 테이블 생성부(10)는 캐리 비트(c)를 $C[c \oplus \gamma] = (c + \alpha) \cdot 2^k$ 와 같이 연산하여 C 테이블을 생성할 수 있다. 여기서, α 는 차분 전력 분석으로부터 캐리 비트를 안전하게 만드는 난수이다.
- [0045] 차분 전력 분석은 대표적인 부채널 공격 기법의 하나로 암호 알고리즘이 연산될 때 발생하는 중간 값을 누출하여 비밀 정보를 알아내는 공격 기법이다.
- [0046] 사전 연산 테이블 생성부(10)는 이러한 차분 전력 분석으로부터 캐리 비트를 안전하게 만드는 난수를 더하여 보안성을 강화할 수 있다.
- [0047] 이외에도, 사전 연산 테이블 생성부(10)는 산술 마스크 상태의 데이터의 각 비트 마다 G 테이블 생성 단계에서 발생하는 캐리 비트를 불 마스크 처리한 값을 더하여 저장할 수 있다.
- [0048] 사전 연산 테이블 생성부(10)는 후술하는 산술 마스크-불 마스크 변환부(30)에서 산술 마스크 상태의 데이터를 불 마스크 상태로 변환하는 경우, C 테이블을 생성하는 단계에서 캐리 비트와 더해지는 난수를 제거할 수 있도록 캐리 비트의 연산 값을 k 비트 마다 저장한 Γ 값을 산출하여 저장할 수 있다.
- [0049] 이와 같은 사전 연산 테이블 생성부(10)에서의 사전 연산 테이블 생성 알고리즘에 대한 구체적인 설명은 도 2 이하를 참조하여 후술한다.
- [0050] 산술 마스크-불 마스크 변환부(30)는 G 테이블 및 C 테이블을 이용하여 산술 마스크 상태의 데이터를 불 마스크 상태의 데이터로 변환할 수 있다.
- [0051] 산술 마스크-불 마스크 변환부(30)는 리플 자리 올림수 가산기에 기반하여 산술 마스크 상태의 데이터를 불 마스크 상태의 데이터로 변환할 수 있다.
- [0052] 이때, 산술 마스크-불 마스크 변환부(30)는 G 테이블 및 C 테이블을 이용하여 연산의 시간 복잡도를 줄일 수 있다.
- [0053] 산술 마스크-불 마스크 변환부(30)는 G 테이블을 이용하여 산술 마스크 상태의 데이터 각 비트를 불 마스크 처리하는 단계에서 캐리 비트의 발생 여부를 확인할 수 있다.
- [0054] 산술 마스크-불 마스크 변환부(30)는 C 테이블을 이용하여 산술 마스크 상태의 데이터에서 캐리 비트를 제거한 뒤 불 마스크 처리하여 산술 마스크 상태의 데이터를 불 마스크 상태로 변환할 수 있다.
- [0055] 산술 마스크-불 마스크 변환부(30)에서의 산술 마스크-불 마스크 변환 알고리즘에 대한 구체적인 설명은 도 2 이하를 참조하여 후술한다.
- [0056] 이와 같이, 본 발명의 일 실시예에 따른 산술 마스크-불 마스크 변환 장치(1)는 사전 연산 테이블을 이용하는 리플 자리 올림수 가산기에 기반한 A2B 알고리즘을 수행하는데, LSB 트릭 기술을 적용하여 사전 연산 테이블을 생성함으로써 사전 연산 테이블 저장에 필요한 메모리를 적게 사용할 수 있으며 연산 소요시간을 향상시킬 수 있다. 따라서 본 발명의 일 실시예에 따른 산술 마스크-불 마스크 변환 장치(1)는 저메모리 환경에서 부채널 분석 공격에 대응할 수 있을 것이다.
- [0058] 도 2는 본 발명의 일 실시예에 따른 산술 마스크-불 마스크 변환 방법의 순서도이고, 도 3 및 도 4는 도 2에 도시된 산술 마스크-불 마스크 변환 방법을 보여주는 실행 코드의 일 예이다.
- [0059] 본 발명의 일 실시예에 따른 산술 마스크-불 마스크 변환 방법은 도 1에 도시된 산술 마스크-불 마스크 변환 장치(1)와 실질적으로 동일한 구성에서 실행될 수 있다. 따라서 도 1에 도시된 산술 마스크-불 마스크 변환 장치(1)와 동일한 구성요소는 동일한 도면부호를 부여하고, 반복되는 설명은 생략한다.
- [0060] 도 2를 참조하면, 사전 연산 테이블 생성부(10)는 G 테이블을 생성하고(S100), C 테이블을 생성할 수 있다(S200).
- [0061] 사전 연산 테이블 생성부(10)는 산술 마스크 상태의 데이터에서 최하위 비트(LSB)를 제외하고 각 비트를 불 마

스킹 처리하여 G 테이블을 생성할 수 있으며, G 테이블 생성 단계에서 발생하는 캐리 비트를 불 마스크 처리하여 C 테이블을 생성할 수 있다. 이와 관련하여 구체적인 설명은 도 3을 참조하여 후술한다.

[0062] 산술 마스크-불 마스크 변환부(30)는 G 테이블을 이용하여 캐리 비트의 발생 여부를 확인하고(S300), C 테이블을 이용하여 캐리 비트를 제거한 뒤 G 테이블을 이용하여 산술 마스크-불 마스크 변환을 수행할 수 있다(S400).

[0063] 산술 마스크-불 마스크 변환부(30)는 리플 자리 올림수 가산기에 기반한 A2B 알고리즘을 수행할 수 있으며, 이때, G 테이블 및 C 테이블을 이용할 수 있다. 이와 관련하여 구체적인 설명은 도 4를 참조하여 후술한다.

[0065] 도 3을 참조하면, 사전 연산 테이블 생성부(10)는 $(n \cdot k)$ 비트의 데이터를 A2B 변환시킬 수 있으며, 이때 테이블 및 전환 연산의 크기는 k 비트이다.

[0066] 사전 연산 테이블 생성부(10)는 산술 마스크 상태의 데이터 각 비트에 랜덤 값(r)을 더하고 불 마스크 처리하여 G 테이블을 생성할 수 있다. 즉, 사전 연산 테이블 생성부(10)는 산술 마스크 상태의 데이터의 $(k+1)$ 비트에 해당하는 값(A)을 $\{(A+r) \oplus (y \parallel r)\}$ 과 같이 연산하여 불 마스크 처리하고, 배열 G에 저장하여 G 테이블을 생성할 수 있으며, 이때, 최하위 비트(LSB)는 제외하고 k 비트만을 불 마스크 처리하여 G 테이블을 생성할 수 있다(Step 3).

[0067] 사전 연산 테이블 생성부(10)는 G 테이블 생성 단계에서 발생하는 캐리 비트와 차분 전력 분석으로부터 캐리 비트를 안전하게 만드는 난수(α)의 합에 2^k (여기서, k는 상기 데이터의 비트 자리 수)를 곱한 값으로 연산하여 C 테이블을 생성할 수 있다. 즉, 사전 연산 테이블 생성부(10)는 G 테이블 생성 단계에서 발생하는 캐리 비트(c)를 $C[c \oplus \gamma] = (c + \alpha) \cdot 2^k$ 와 같이 연산하여 C 테이블을 생성할 수 있다(Step 5,6).

[0068] 또한, 사전 연산 테이블 생성부(10)는 캐리 비트의 연산 값을 k 비트 마다 저장한 Γ 값을 산출하여 저장할 수 있다(Step 7).

[0069] 이와 같이 사전 연산 테이블 생성부(10)에 의해 정의되는 랜덤 값(r), G 테이블, C 테이블 및 Γ 값은 A2B 변환 알고리즘에 사용될 수 있다.

[0071] 도 4를 참조하면, 산술 마스크-불 마스크 변환부(30)는 산술 마스크 상태의 데이터 각 비트에 랜덤 값(r) 및 캐리 비트를 안전하게 만드는 난수(α)를 뺀 값($A_i - r - \alpha$)을 초기 값으로 설정할 수 있다. 이때, 산술 마스크-불 마스크 변환부(30)는 캐리 비트의 연산 값을 k 비트 마다 저장한 Γ 값을 이용하여 캐리 비트를 안전하게 만드는 난수(α)를 추가 연산 없이 제거할 수 있다(Step 1).

[0072] 산술 마스크-불 마스크 변환부(30)는 리플 자리 올림수 가산기에 기반하여 하위 비트를 상위 비트로 올릴 수 있다. 산술 마스크-불 마스크 변환부(30)는 초기 값에 마스크 값(R)을 더한 값($A_i - r - \alpha + R_i$)을 변환 대상 데이터 비트로 저장하는 방식으로 하위 비트를 상위 비트로 올릴 수 있다(Step 3). 이러한 리플 자리 올림수 가산기에 기반한 방식은 A2B 알고리즘 속도를 최적화 할 수 있다.

[0073] 산술 마스크-불 마스크 변환부(30)는 G 테이블을 이용하여 변환 대상 데이터 비트를 불 마스크 처리할 수 있으며, 불 마스크 처리하는 단계에서의 캐리 비트 발생 여부를 확인할 수 있다. 산술 마스크-불 마스크 변환부(30)는 G 테이블을 이용하여 변환 대상 데이터 비트를 불 마스크 처리한 B_i 를 $B_i = (A_i + r) \oplus r = A_i \oplus r$ 과 같이 연산하여 저장할 수 있다. 이때, 산술 마스크-불 마스크 변환부(30)는 t를 캐리 비트를 알아내기 위한 인자로 함께 저장할 수 있다(step 4).

[0074] 산술 마스크-불 마스크 변환부(30)는 G 테이블을 이용하여 변환 대상 데이터 비트를 불 마스크 처리한 B_i 를 마스크 값(R_i)으로 불 마스크 처리할 수 있다. 산술 마스크-불 마스크 변환부(30)는 Step 4에서 G 테이블을 이용하여 $B_i = (A_i + r) \oplus r = A_i \oplus r$ 과 같이 연산하여 저장한 B_i 를 $B_i = A_i \oplus r \oplus R_i$ 와 같이 연산하여 저장할 수 있다(Step 5).

[0075] 산술 마스크-불 마스크 변환부(30)는 C 테이블을 이용하여 산술 마스크 상태의 데이터에서 캐리 비트를 제거할

수 있다. 산술 마스크-불 마스크 변환부(30)는 Step 4에서 저장된 t 에 따라 변환 대상 데이터 비트인 초기 값에 마스크 값(R)을 더한 값($A_i - r - \alpha + R_i$)에 캐리 비트를 안전하게 만드는 난수(α)를 더하거나, 캐리 비트를 안전하게 만드는 난수(α) 및 1을 더하여 캐리 비트 및 캐리 비트를 안전하게 만드는 난수(α)를 제거할 수 있다. 이때, t 는 산술 마스크 상태의 데이터 각 비트를 불 마스크 처리하는 단계에서 캐리 비트가 발생하는 경우에는 변환 대상 데이터 비트에 ($\alpha+1$)이 더해지도록 하고, 캐리 비트가 발생하지 않은 경우에는 변환 대상 데이터 비트에 (α)가 더해지도록 할 수 있다(Step 6).

[0076] 산술 마스크-불 마스크 변환부(30)는 Step 6으로부터 캐리 비트 및 난수(α)가 처리된 변환 대상 데이터 비트가 데이터의 각 비트 자리에 저장되도록 처리할 수 있다(Step 7). 산술 마스크-불 마스크 변환부(30)는 이러한 clearing 과정을 통해 부채널 안전성을 보장할 수 있다.

[0077] 산술 마스크-불 마스크 변환부(30)는 최종적으로 Step 5에서 저장한 $B_i = A_i \oplus r \oplus R_i$ 를 최종적으로 반환하는데, 랜덤 값(r)을 XOR 연산을 이용하여 반환할 수 있다. 따라서 산술 마스크-불 마스크 변환부(30)는 결과적으로는 캐리 비트 및 난수(α)가 처리된 변환 대상 데이터 비트를 마스크 값으로 불 마스크 처리한 $A_i \oplus R_i$ 를 최종 반환할 수 있다(Step 9).

[0078] 산술 마스크-불 마스크 변환부(30)는 이와 같은 단계를 거쳐 산술 마스크 상태의 데이터를 마스크 값으로 불 마스크 처리하여 불 마스크 상태로 변환할 수 있다.

[0080] 이와 같은, 본 발명의 산술 마스크-불 마스크 변환 방법은 다양한 컴퓨터 구성요소를 통하여 수행될 수 있는 프로그램 명령어의 형태로 구현되어 컴퓨터 판독 가능한 기록 매체에 기록될 수 있다. 상기 컴퓨터 판독 가능한 기록 매체는 프로그램 명령어, 데이터 파일, 데이터 구조 등을 단독으로 또는 조합하여 포함할 수 있다.

[0081] 상기 컴퓨터 판독 가능한 기록 매체에 기록되는 프로그램 명령어는 본 발명을 위하여 특별히 설계되고 구성된 것들이거나 컴퓨터 소프트웨어 분야의 당업자에게 공지되어 사용 가능한 것일 수도 있다.

[0082] 컴퓨터 판독 가능한 기록 매체의 예에는, 하드 디스크, 플로피 디스크 및 자기 테이프와 같은 자기 매체, CD-ROM, DVD 와 같은 광기록 매체, 플롭티컬 디스크(floptical disk)와 같은 자기-광 매체(magneto-optical media), 및 ROM, RAM, 플래시 메모리 등과 같은 프로그램 명령어를 저장하고 수행하도록 특별히 구성된 하드웨어 장치가 포함된다.

[0083] 프로그램 명령어의 예에는, 컴파일러에 의해 만들어지는 것과 같은 기계어 코드뿐만 아니라 인터프리터 등을 사용해서 컴퓨터에 의해서 실행될 수 있는 고급 언어 코드도 포함된다. 상기 하드웨어 장치는 본 발명에 따른 처리를 수행하기 위해 하나 이상의 소프트웨어 모듈로서 작동하도록 구성될 수 있으며, 그 역도 마찬가지이다.

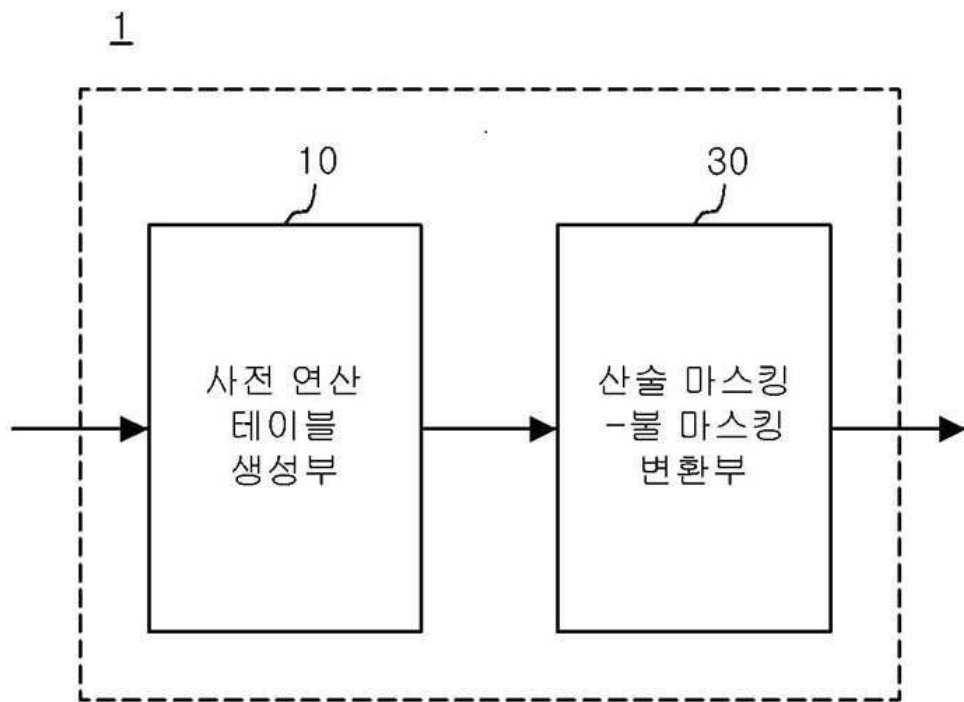
[0084] 이상 첨부된 도면을 참조하여 본 발명의 실시예를 설명하였지만, 본 발명이 속하는 기술분야에서 통상의 지식을 가진 자는 본 발명이 그 기술적 사상이나 필수적인 특징을 변경하지 않고서 다른 구체적인 형태로 실시될 수 있다는 것을 이해할 수 있을 것이다. 그러므로 이상에서 기술한 실시예들은 모든 면에서 예시적인 것이며 한정적이 아닌 것으로 이해해야만 한다.

부호의 설명

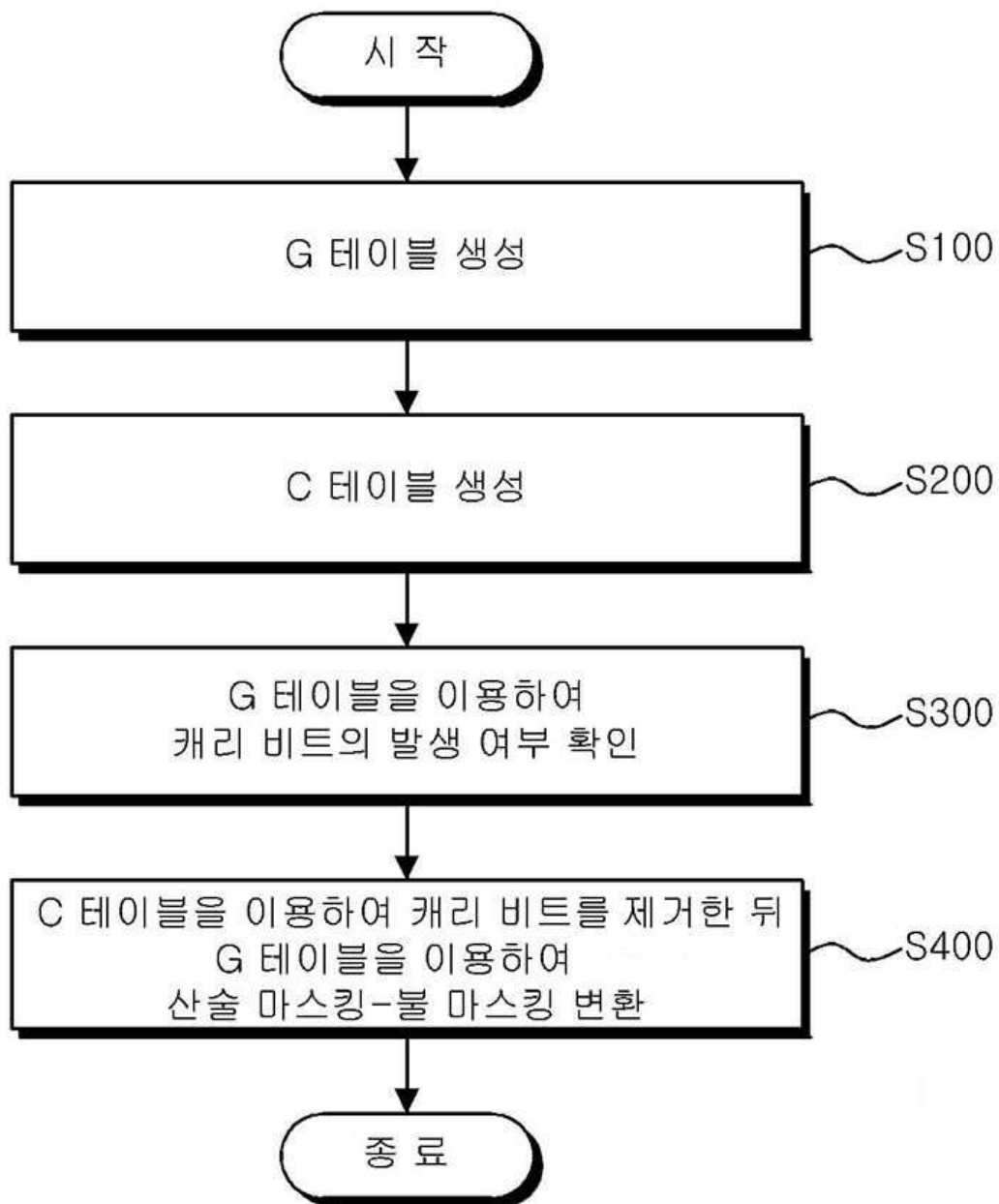
- [0085] 1: 산술 마스크-불 마스크 변환 장치
10: 사전 연산 테이블 생성부
30: 산술 마스크-불 마스크 변환부

도면

도면1



도면2



도면3

Algorithm 8 Table G and C generation

/ G is used of k-bit register */*

/ C and Γ are used of $(k \cdot n)$ -bit register */*

Require: *None*

Ensure: $G[\cdot], C[\cdot], \Gamma, r$

- 1: Generate a random $((k-1) \cdot n)$ -bit random α , a random k -bit r and a random bit γ
 - 2: **for** $A = 0$ to $2^k - 1$ **do**
 - 3: $G[A] \leftarrow \{(A + r) \oplus (\gamma || r)\} \gg 1$
 - 4: **end for**
 - 5: $C[\gamma] \leftarrow \alpha \cdot 2^k$
 - 6: $C[\gamma \oplus 1] \leftarrow (\alpha + 1) \cdot 2^k$
 - 7: $\Gamma \leftarrow \sum_{l=1}^{n-1} (\alpha \cdot 2^{l \cdot k})$
 - 8: **return** $G[\cdot], C[\cdot], \Gamma, r$
-

도면4

Algorithm 9 Conversion of a $(k \cdot n)$ -bit variable

/ Notation: Split A into $A_{n-1} || \dots || A_i || \dots || A_0$ and*

*R into $R_{n-1} || \dots || R_i || \dots || R_0$, such that A_i and R_i have size k */*

/ r and B_i is used of k-bit register */*

/ A is used of $(k \cdot n)$ -bit register */*

Require: $(A, R), G[\cdot], C[\cdot], \Gamma, r$ */* $x = A + R \bmod 2^{k \cdot n}$ */*

/ $G[\cdot], C[\cdot], \Gamma, r$ generated during pre-computation phase */*

Ensure: (x', R) */* $x = x' \oplus R$ */*

- 1: $A \leftarrow A - (r || \dots || r) - \Gamma$
 - 2: **for** $i = 0$ to $n - 1$ **do**
 - 3: $A \leftarrow A + (R_i \cdot 2^{i \cdot k})$
 - 4: $t || B_i \leftarrow G[A_i] || \text{LSB}_{A_i}$
 - 5: $B_i \leftarrow B_i \oplus R_i$
 - 6: $A \leftarrow A + (C[t] \cdot 2^{i \cdot k})$
 - 7: $A \leftarrow A \& (2^{(i+1) \cdot k} - 1)$
 - 8: **end for**
 - 9: **return** $(B_i || \dots || B_0) \oplus (r || \dots || r)$
-