(19)대한민국특허청(KR)
(12) 공개특허공보(A)

(51) 。Int. Cl.[7]
G06F 7/52

(11) 공개번호 10-2005-0072537
(43) 공개일자 2005년07월12일

(21) 출원번호 10-2004-0000879
(22) 출원일자 2004년01월07일

(71) 출원인 삼성전자주식회사
경기도 수원시 영통구 매탄동 416

(72) 발명자 백유진
경기도성남시분당구정자동(한솔마을)503-1901

(74) 대리인 이영필
이해영

심사청구 : 있음

(54) 암호화 장치, 암호화 방법 및 그 기록매체

요약

암호화 장치, 암호화 방법 및 그 기록매체가 개시된다. 상기 암호화 장치는 제1난수와 데이터를 수신하고 제1마스크된 데이터를 출력하는 제1마스킹 회로; 제2난수와 상기 제1마스킹 회로로부터 출력된 상기 제1마스크된 데이터를 수신하고, 제2마스크된 데이터를 출력하는 제2마스킹 회로를 구비한다. 상기 제2마스킹 회로는 상기 제1마스크된 데이터와 상기 제2난수를 논리곱하는 논리곱 회로, 상기 논리곱 회로의 출력신호를 수신하고 수신된 출력신호를 소정의 방향으로 소정의 비트만큼씩 쉬프트시키는 쉬프트 회로, 및 상기 제1마스크된 데이터와 상기 쉬프트 회로의 출력신호를 수신하고 상기 제1마스크된 데이터로부터 상기 쉬프트 회로의 출력신호를 산술 뺄셈하고 제2마스크된 데이터를 출력하는 감산기를 구비한다. 상기 제1마스크된 데이터는 부울 마스크된 데이터이고 상기 제2마스크된 데이터는 산술 마스크된 데이터이다.

대표도

도 2

색인어

몽고메리 알고리즘, 역원

명세서

도면의 간단한 설명

본 발명의 상세한 설명에서 인용되는 도면을 보다 충분히 이해하기 위하여 각 도면의 상세한 설명이 제공된다.

도 1은 본 발명의 실시예에 따른 암호화 장치의 블락도를 나타낸다.

도 2는 도 1에 도시된 제2마스킹 블락이 부울 마스크된 데이터를 산술 마스크된 데이터로 변환하는 블락인 경우, 상기 제2마스킹 블락의 제1회로도를 나타낸다.

제 3은 도 1에 도시된 제 2마스킹 블락이 부울 마스크된 데이터를 산술 마스크된 데이터로 변환하는 블락인 경우, 상기 제2마스킹 블락의 제2회로도를 나타낸다.

도 4는 도 1에 도시된 제2마스킹 블락이 산술 마스크된 데이터를 부울 마스크된 데이터로 변환하는 블락인 경우, 상기 제2마스킹 블락의 회로도를 나타낸다.

발명의 상세한 설명

발명의 목적

발명이 속하는 기술 및 그 분야의 종래기술

본 발명은 암호화 장치에 관한 것으로, 보다 상세하게는 차분전력해석 (Differential Power Analysis; 이하 'DPA'라 한다.)공격에 강한 암호화 장치, 암호화 방법 및 상기 암호화 방법을 실행시키기 위한 프로그램을 기록한 컴퓨터로 읽을 수 있는 기록매체에 관한 것이다.

암호(cryptography)는 원래 국가의 비밀을 보안할 목적으로 군사·외교분야에서 사용되었고, 금융기관들은 전자자금이동(Electronic Funds Transfer)을 위하여 암호를 사용했다.

따라서 암호는 경제·금융분야에서 널리 사용된 이래, 동일성의 인증 (Authentication), 암호화 키에 대한 관리(Key Management), 디지털 서명(Digital Signature), 및 신원확인(Identity Verification) 등 광범위하게 사용되고 있다.

암호해독은 해독키의 관리소홀, 비밀번호의 예측가능성, 또는 통신망에서 키보드 입력에 대한 모니터링 등으로도 가능하다. 여기서 암호해독은 암호해독행위자가 암호문(Ciphertext)만을 가지고 평문(Plaintext)에 대한 해독을 감행하는 방법(소위, 무작정공격; Bruteforce Attack)이 아니라 평문의 암호화에 사용된 알고리즘의 종류, 사용된 운영체제 등 시스템에 대한 모든 정보를 알고있는 상태에서 암호화에 사용된 키만 모르는 경우에 그 키를 찾아내어 암호문을 평문으로 해독하려는 행위를 지칭한다.

암호를 해독하는 기술로는 단순 암호문 공격(Ciphertext Only Attack), 이미 알고 있는 평문공격(Known Plaintext Attack), 선택 평문공격(Chosen Plaintext Attack), 최적 선택 평문 공격(Adaptively Chosen Plaintext Attack), 시간 공격 (timing attack) 및 DPA(또는 '전력분석'이라고도 한다.)공격 등이 있다.

시간 공격은 암호 알고리즘의 연산 수행시간 정보를 이용하여 특정한 비트의 값이 0인지 또는 1인지를 판단하고, 이에 따라 암호를 해독하는 방법을 말한다. 그리고 차분전력해석 공격은 입력 비트값에 따라 암호 알고리즘이 사용하는 전력량을 분석하고, 이에 따라 비밀키의 비트값을 알아냄으로서 암호를 해독하는 방법을 말한다.

따라서 정보의 누설을 방지하기 위한 방법으로 데이터를 난수화하는 마스킹 방법이 사용되고 있다. 상기 마스킹 방법으로 부울 연산(Boolean operation)을 이용한 마스킹 방법, 산술 연산과 상기 부울 연산을 함께 사용하는 마스킹 방법이 있다.

발명이 이루고자 하는 기술적 과제

따라서 본 발명이 이루고자 하는 기술적인 과제는 차분전력해석 공격에 강한 암호화 장치, 암호화 방법 및 상기 암호화 방법을 실행시키기 위한 프로그램을 기록한 컴퓨터로 읽을 수 있는 기록매체를 제공하는 것이다.

발명의 구성 및 작용

상기 기술적 과제를 달성하기 위한 암호화 장치는 난수와 제1마스크된 데이터를 논리곱하는 논리곱 회로; 상기 논리곱 회로의 출력신호를 수신하고, 수신된 신호를 오른쪽과 왼쪽중에서 어느 하나의 방향으로 m(여기서, m은 자연수)비트만큼씩 쉬프트시키는 쉬프트 회로; 및 상기 제1마스크된 데이터와 상기 쉬프트 회로의 출력신호를 수신하고, 상기 제1마스크된 데이터로부터 상기 쉬프트 회로의 출력신호를 산술 뺄셈하고, 그 결과로서 제2마스크된 데이터를 출력하는 감산기를 구비한다.

상기 기술적 과제를 달성하기 위한 암호화 장치는 난수와 제1마스크된 데이터를 논리곱하는 논리곱 회로; 상기 논리곱 회로의 출력신호와 상기 난수를 수신하고, 이들을 배타 논리합하는 배타 논리합 회로; 상기 배타 논리합 회로의 출력신호를 수신하고, 수신된 신호를 오른쪽과 왼쪽중에서 어느 하나의 방향으로 m(여기서, m은 자연수)비트만큼씩 쉬프트시키는 쉬프트 회로; 및 상기 제1마스크된 데이터와 상기 쉬프트 회로의 출력신호를 수신하고, 상기 제1마스크된 데이터와 상기 쉬프트 회로의 출력신호를 산술덧셈하고, 그 결과로서 제2마스크된 데이터를 출력하는 가산기를 구비한다.

상기 기술적 과제를 달성하기 위한 암호화 방법은 n비트의 데이터와 n비트의 제1난수를 수신하고, n비트의 산술 마스크된 데이터 $a_n,a_{n-1}...,a_2,a_1$을 출력하는 단계; 및 n비트의 제2난수 $r_n,r_{n-1},...,r_2,r_1$과 상기 산술 마스크된 데이터 $a_n,a_{n-1},...,a_2,a_1$을 수신하고, n비트의 부울 마스크된 데이터 $y_n,y_{n-1},...,y_2,y_1$을 출력하는 단계를 구비하며, 상기 부울 마스크된 데이터 $y_n,y_{n-1},..,y_2,y_1$ 을 출력하는 단계는,

상기 a_1을 y_1로서 출력하는 단계; 상기 y_1과 r_1을 논리곱하고 그 결과를 저장장치에 저장하고, 상기 a_2와 상기 저장장치에 저장된 데이터를 배타 논리합하고 그 결과를 y_2로서 출력하고, a_2와 상기 저장장치에 저장된 데이터를 논리곱하고 그 결과로서 올림수로서 발생하는 단계; 상기 y_{k-1}과 상기 r_{k-1}을 논리곱하고 그 결과를 상기 저장장치에 저장하고, a_k와 상기 저장장치에 저장된 데이터와 상기 올림수를 각각 배타 논리합하고 그 결과로서 y_k를 출력하고, (a_k와 상기 저장장치에 저장된 데이터를 논리곱한 결과)와 (a_k와 상기 올림수를 논리곱한 결과)를 논리합하고 그 논리합의 결과와 (상기 저장장치에 저장된 데이터와 상기 올림수를 논리곱한 결과)를 논리합하고 그 결과를 상기 올림수로서 발생하는 단계; 및 상기 y_{n-1}과

상기 r_{n-1}을 논리곱하고 그 결과를 상기 저장장치에 저장하고, a_n과 상기 저장장치에 저장된 데이터와 상기 올림수 각각을 배타 논리합하고 그 결과를 y_n으로서 출력하는 단계를 구비하고, 소정의 변수 k는 3부터 (n-1)까지 1씩 증가되는 것을 특징으로 한다.

상기 방법의 각 단계를 실행시키기 위한 프로그램은 컴퓨터로 읽을 수 있는 기록매체에 저장된다.

본 발명과 본 발명의 동작상의 이점 및 본 발명의 실시에 의하여 달성되는 목적을 충분히 이해하기 위해서는 본 발명의 바람직한 실시예를 예시하는 첨부 도면 및 첨부 도면에 기재된 내용을 참조하여야만 한다.

이하, 첨부한 도면을 참조하여 본 발명의 바람직한 실시예를 설명함으로써, 본 발명을 상세히 설명한다. 각 도면에 제시된 동일한 참조부호는 동일한 부재를 나타낸다.

현재까지 제안된 부울 마스킹을 산술 마스킹으로 변환하는 알고리즘은 3가지가 있다. 여기서, n비트 이진 수열 $x \in \{0,1\}^n$에 대하여 x의 부울 마스킹(boolean masking)이란 $x = x' \oplus r$을 만족시키는 순서쌍 $(x',r) \in \{0,1\}^n \times \{0,1\}^n$을 의미한다. 여기서 $\oplus$은 배타 논리합을 의미한다. 즉, 부울 마스킹이란 원래의 데이터에 소정의 난수를 배타 논리합하여 상기 원래의 데이터를 은닉하는 방법이다.

그리고, n비트 이진 수열 $x \in \{0,1\}^n$에 대하여 x의 산술 마스킹(arithmetic masking)이란 $x = x' \bmod r$을 만족시키는 순서쌍 $(x',r) \in \{0,1\}^n \times \{0,1\}^n$을 의미한다. 여기서 mod는 2^n에 대한 모듈러 덧셈(addition modulo 2^n) 또는 2^n 에 대한 모듈러 뺄셈(subtraction modular 2^n)을 의미한다. 즉, 산술 마스킹이란 원래의 데이터에 소정의 난수를 산술덧셈(modular addition)이나 산술뺄셈(modular subtraction)을 통하여 상기 원래의 데이터를 은닉하는 방법이다.

먼저, FSE(Fast Software Encryption Workshop) 2000에서 T.S. Messerges가 제안한 방법은 먼저 부울 마스킹(또는 산술 마스킹)된 데이터를 원래의 데이터나 논리적으로 반전된 데이터(logical complement data)로 랜덤(random)하게 변환시킨 후, 다시 산술 마스킹(또는 부울 마스킹)된 데이터로 변환하는 방법이다. 그러나 이 방법은 DPA 공격에 대한 완전한 대응책(countermeasure)을 제공하지 못함이 증명되었다.

그리고 L. Goubin이 CHESS(Workshop on Cryptographic Hardware and Embedded System) 2001에서 제안한 방법은 5개의 n(n은 자연수)비트 배타 논리합 연산과 2개의 n비트 산술뺄셈연산을 이용하여 부울 마스킹을 산술 마스킹으로 변환한다. 또한, 상기 방법은 (2n+ 4)개의 n비트 배타 논리합 연산, (2n+ 1)개의 n비트 논리곱 연산, 그리고 n개의 n비트 논리 왼쪽 쉬프트 연산을 사용하여 산술 마스킹을 부울 마스킹으로 변환할 수 있다. 그러나 상기 방법은 너무 많은 오버헤드(overhead)때문에 실용적이지 못하다.

마지막으로 CHESS 2003에서 J.S. Coron 등이 제안한 방법은 L. Goubin이 제안한 방법 중에서 산술 마스킹을 부울 마스킹으로 변환하는 알고리즘의 오버헤드를 줄이기 위하여 미리 계산된 표를 사용한다. 따라서 상기 마지막 방법은 상기 표를 저장하기 위한 메모리 장치를 사용하므로 상기 메모리 장치의 오버헤드가 있다.

도 1은 본 발명의 실시예에 따른 암호화 장치의 블락도를 나타낸다. 도 1을 참조하면, 암호화 장치(100)는 제1마스킹 블락(110) 및 제2마스킹 블락(200)을 구비한다.

제1마스킹 블락(110)이 부울 마스킹 블락인 경우, 제2마스킹 블락(200)은 산술 마스킹 블락이다. 즉, 제1마스킹 블락(110)은 데이터(X)와 난수(R1)를 수신하고, 난수(R1)를 사용하여 상기 데이터(X)를 부울 마스크된 데이터(X')로 변환하고, 부울 마스크된 데이터(X')를 출력한다. 그리고 제2마스킹 블락(200)은 부울 마스크된 데이터(X')와 난수(R2)를 수신하고, 난수(R2)를 사용하여 부울 마스크된 데이터 (X')를 산술 마스크된 데이터(OUT)로 변환하고, 산술 마스크된 데이터(OUT)를 출력한다. 여기서 난수(R1)와 난수(R2)는 서로 동일한 수 인 것이 바람직하다.

그러나, 제1마스킹 블락(110)이 산술 마스킹 블락인 경우, 제2마스킹 블락 (200)은 부울 마스킹 블락이다. 즉, 제1마스킹 블락(110)은 데이터(X)와 난수(R1)를 수신하고, 난수(R1)를 사용하여 상기 데이터(X)를 산술 마스크된 데이터(X')로 변환하고, 산술 마스크된 데이터(X')를 출력한다. 그리고 제2마스킹 블락(200)은 산술 마스크된 데이터(X')와 난수(R2)를 수신하고, 난수(R2)를 사용하여 산술 마스크된 데이터(X')를 부울 마스크된 데이터(OUT)로 변환하고, 부울 마스크된 데이터(OUT)를 출력한다. 여기서 난수(R1)와 난수(R2)는 서로 동일한 수 인 것이 바람직하다.

도 2는 도 1에 도시된 제2마스킹 블락이 부울 마스크된 데이터를 산술 마스크된 데이터로 변환하는 블락인 경우, 상기 제2마스킹 블락의 제1회로도를 나타낸다.

도 1 및 도 2를 참조하여 제2마스킹 블락(200)을 설명하면 다음과 같다. 우선, 본 발명의 실시예에 따른 부울 마스킹이 적용된 데이터(이하 '부울 마스크된 데이터'라 한다.)를 산술 마스킹이 적용된 데이터(이하 '산술 마스크된 데이터'라 한다.)로 변환하는 제1알고리즘은 다음과 같다.

Input : $X'(= X \oplus R1), R2$

Output: $OUT = X - R2$

1. $temp = X' \wedge R2$

2. $temp = (temp \ll 1)$

3. Return (X' - temp)

여기서 "∧"는 논리곱 연산을 나타내고, "≪"는 1비트씩 왼쪽으로 논리적으로 쉬프트(logical shift left by 1 bit)시키는 것을 의미하고, "⊕"는 배타 논리합을 의미하고, "-"는 산술 뺄셈 연산을 의미한다. 그리고 "temp"는 일시적으로 데이터를 저장하는 의미를 나타내고, 래치 또는 레지스터 등을 포함하는 데이터 저장회로로 구현될 수 있다.

도 2는 본 발명에 따른 부울 마스크된 데이터를 산술 마스크된 데이터로 변환하는 알고리즘을 H/W로 구현한 것이다. 즉, 제2마스킹 블락(200)은 논리곱 회로(210), 쉬프트 회로(220) 및 감산기(230)를 구비한다.

논리곱 회로(210)는 부울 마스크된 데이터(X')와 난수(R2)를 수신하고, 이들을 비트단위(bitwise)로 논리곱하고, 그 결과를 쉬프트 회로(220)로 출력한다. 부울 마스크된 데이터(X')와 난수(R2)는 각각 n비트로 구성된다.

쉬프트 회로(220)는 논리곱 회로(210)로부터 출력된 n비트 데이터를 수신하고, 이를 m(m은 자연수, 예컨대 m은 1)비트씩 왼쪽과 오른쪽 중에서 어느 한쪽으로 쉬프트시킨다. 예컨대 쉬프트 회로(220)는 1비트씩 왼쪽으로 쉬프트시킬 수 있다.

감산기(230)는 부울 마스크된 데이터(X')와 쉬프트 회로(220)의 출력신호를 수신하고, 부울 마스크된 데이터(X')로부터 쉬프트 회로(220)의 출력신호를 산술뺄셈하고, 그 결과로서 발생된 산술 마스크된 데이터(OUT)를 출력한다. 따라서 본 발명에 따른 암호화 장치는 DPA 공격에 대하여 완전한 대응책을 제공한다.

제 3은 도1에 도시된 제2마스킹 블락이 부울 마스크된 데이터를 산술 마스크된 데이터로 변환하는 블락인 경우, 상기 제2마스킹 블락의 제2회로도를 나타낸다.

도 1 및 도 3을 참조하여 제2마스킹 블락(200)을 설명하면 다음과 같다. 본 발명의 실시예에 따른 부울 마스크된 데이터를 산술 마스크된 데이터로 변환하는 제2알고리즘은 다음과 같다.

Input : X'(= X $\oplus$ R1), R2

Output: OUT= X + R2

1. temp = (X' ∧ R2) $\oplus$ R2

2. temp = (temp ≪ 1)

3. Return (X' + temp)

여기서, "+ "는 산술 덧셈 연산을 의미한다.

도 3은 본 발명에 따른 부울 마스크된 데이터를 산술 마스크된 데이터로 변환하는 알고리즘을 H/W로 구현한 것이다. 즉, 제2마스킹 블락(200)은 논리곱 회로 (240), 배타 논리합 회로(250), 쉬프트 회로(260) 및 가산기(270)를 구비한다.

논리곱 회로(240)는 부울 마스크된 데이터(X')와 난수(R2)를 수신하고, 이들을 비트단위로 논리곱하고, 그 결과를 배타 논리합 회로(250)로 출력한다. 부울 마스크된 데이터(X')와 난수(R2)는 각각 n비트로 구성된다.

배타 논리합 회로(250)는 논리곱 회로(240)의 출력신호와 난수(R2)를 수신하고, 이들을 비트단위로 배타 논리합하고, 그 결과를 쉬프트 회로(260)로 출력한다.

쉬프트 회로(260)는 배타 논리합 회로(250)로부터 출력된 n비트 데이터를 수신하고, 이를 m(m은 자연수, 예컨대 m은 1)비트씩 왼쪽과 오른쪽 중에서 어느 한쪽으로 쉬프트시킨다. 예컨대 쉬프트 회로(260)는 1비트씩 왼쪽으로 쉬프트시킬 수 있다.

가산기(270)는 부울 마스크된 데이터(X')와 쉬프트 회로(260)의 출력신호를 수신하고, 부울 마스크된 데이터(X')와 쉬프트 회로(260)의 출력신호를 산술덧셈하고, 그 결과로서 발생된 산술 마스크된 데이터(OUT)를 출력한다. 따라서 본 발명에 따른 암호화 장치는 DPA 공격에 대하여 완전한 대응책을 제공한다.

도 4는 도 1에 도시된 제2마스킹 블락이 산술 마스크된 데이터를 부울 마스크된 데이터로 변환하는 블락인 경우, 상기 제2마스킹 블락의 회로도를 나타낸다.

본 발명의 실시예에 따른 산술 마스크된 데이터를 부울 마스크된 데이터로 변환하는 알고리즘은 다음과 같다.

Input: X'(= X - R2) = a_n,...,a_1, R2 = r_n,...,r_1

Output: OUT = X $\oplus$ R2 = y_n,...,y_1

1. $y_1=a_1$;

2. temp = $y_1 \wedge r_1$

$y_2= a_2 \oplus temp$

carry = $a_2 \wedge temp$

3. For k=3 to (n-1) by 1

temp = $y_{k-1} \wedge r_{k-1}$;

$y_k = a_k \oplus temp \oplus carry$;

carry = $(a_k \wedge temp) \vee (a_k \wedge carry) \vee (temp \wedge carry)$;

4. temp = $y_{n-1} \wedge r_{n-1}$;

$y_n = a_n \oplus temp \oplus carry$;

5. Return $(y_n,...y_1)$

여기서 "∨"는 논리합 연산을 나타내고, carry는 올림수를 나타낸다. 따라서 산술 마스크된 데이터를 부울 마스크된 데이터로 변환하는 알고리즘은 (2n-3)개의 1비트 배타 논리합회로, (4n-9)개의 1비트 논리곱회로, 및 2(n-3)개의 1비트 논리합회로를 사용하여 구현될 수 있다.

도 4는 본 발명에 따른 산술 마스크된 데이터를 부울 마스크된 데이터로 변환하는 알고리즘을 H/W로 구현한 것이다. 즉, 제2마스킹 블락(200)은 다수개의 AND 게이트들(201, 203, 205, 215, 221, 225, 및 227), 다수개의 OR게이트들(207, 209) 및 다수개의 배타 논리합 게이트들(XOR; 211, 213, 217, 219)을 구비한다. 도 4는 설명의 편의를 위하여 n은 4인 경우의 회로도를 나타낸다.

AND 게이트(201)는 산술 마스크된 데이터(X'<4:1>)의 LSB(X'<1>)와 난수 (R2<4:1>)의 LSB(R2<1>)를 논리곱하고, AND 게이트(203)는 산술 마스크된 데이터 (X'<4:1>)의 두 번째 비트(X'<2>)와 AND 게이트(201)의 출력신호를 논리곱하고, AND 게이트(205)는 산술 마스크된 데이터(X'<4:1>)의 세 번째 비트(X'<3>)와 AND 게이트(203)의 출력신호를 논리곱한다.

OR게이트(207)는 AND 게이트(205)의 출력신호와 AND 게이트(225)의 출력신호를 논리합하고, OR게이트(209)는 OR게이트(207)의 출력신호와 AND 게이트(227)의 출력신호를 논리합하고, XOR게이트(211)는 OR게이트(209)의 출력신호와 XOR게이트 (223)의 출력신호를 배타 논리합한다.

XOR 게이트(213)는 AND게이트(201)의 출력신호와 산술 마스크된 데이터 (X'<4:1>)의 두 번째 비트(X'<2>)를 배타 논리합하고, AND게이트(215)는 난수 (R2<4:1>)의 두 번째 비트(R2<2>)와 XOR 게이트(213)의 출력신호를 논리곱한다.

XOR 게이트(217)는 AND게이트(215)의 출력신호와 산술 마스크된 데이터 (X'<4:1>)의 세 번째 비트(X'<3>)를 배타 논리합하고, XOR 게이트(219)는 AND게이트(203)의 출력신호와 XOR 게이트(217)의 출력신호를 배타 논리합한다.

AND게이트(221)는 난수(R2<4:1>)의 세 번째 비트(R2<3>)와 XOR 게이트(219)의 출력신호를 논리곱하고, XOR 게이트(223)는 AND 게이트(221)의 출력신호와 산술 마스크된 데이터(X'<4:1>)의 MSB(X'<4>)를 배타 논리합한다. AND 게이트(225)는 산술 마스크된 데이터(X'<4:1>)의 세 번째 비트(X'<3>)와 AND게이트(215)의 출력신호를 논리곱하고, AND 게이트(227)는 AND 게이트(215)의 출력신호와 AND 게이트(203)의 출력신호를 논리곱한다.

따라서 제2마스킹 블락(200)의 출력신호(X $\oplus$ R=OUT<4:1>)의 LSB(OUT<1>)는 산술 마스크된 데이터(X'<4:1>)의 LSB(X'<1>)와 같고, 제2마스킹 블락(200)의 출력신호(OUT<4:1>)의 두 번째 비트(OUT<2>)는 XOR 게이트(213)의 출력신호이고, 제2마스킹 블락(200)의 출력신호(OUT<4:1>)의 세 번째 비트(OUT<3>)는 XOR 게이트(219)의 출력신호이고, 제2마스킹 블락(200)의 출력신호(OUT<4:1>)의 MSB(OUT<4>)는 XOR 게이트(211)의 출력신호이다.

따라서 본 발명에 따른 제2마스킹 블락(200)은 L. Goubin이 CHESS 2001에서 제안한 방법보다 오버헤드를 상당히 줄일 수 있다. 또한, 본 발명에 따른 제2마스킹 블락(200)은 미리 계산된 표를 사용하지 않으므로, 제2마스킹 블락(200)은 CHESS 2003에서 J.S. Coron 등이 제안한 방법에 비하여 메모리 오버헤드가 없다.

그리고 본 발명에 따른 암호화 장치는 스마트 카드와 같은 저소비전력 기기에서 사용될 수 있다. 또한, 본 발명에 따른 암호화 방법, 장치 및 그 기록매체는 부울 연산과 산술연산을 동시에 사용하는 알고리즘(또는 상기 알고리즘이 구현된 하드웨어)에 대하여 DPA 공격에 완전한 대응책이 된다.

본 발명은 도면에 도시된 일 실시 예를 참고로 설명되었으나 이는 예시적인 것에 불과하며, 본 기술 분야의 통상의 지식을 가진 자라면 이로부터 다양한 변형 및 균등한 타 실시예가 가능하다는 점을 이해할 것이다. 따라서, 본 발명의 진정한 기술적 보호 범위는 첨부된 등록청구범위의 기술적 사상에 의해 정해져야 할 것이다.

발명의 효과

상술한 바와 같이 본 발명에 따른 암호화 장치는 알고리즘의 오버헤드를 감소시키는 효과가 있다. 또한, 상기 암호화장치는 미리 계산된 표를 사용하지 않으므로 메모리 오버헤드를 감소시키는 효과가 있다.

(57) 청구의 범위

청구항 1.

암호화 장치에 있어서,

난수와 제1마스크된 데이터를 논리곱하는 논리곱 회로;

상기 논리곱 회로의 출력신호를 수신하고, 수신된 신호를 오른쪽과 왼쪽중에서 어느 하나의 방향으로 m(여기서, m은 자연수)비트만큼씩 쉬프트시키는 쉬프트 회로; 및

상기 제1마스크된 데이터와 상기 쉬프트 회로의 출력신호를 수신하고, 상기 제1마스크된 데이터로부터 상기 쉬프트 회로의 출력신호를 산술 뺄셈하고, 그 결과로서 제2마스크된 데이터를 출력하는 감산기를 구비하는 것을 특징으로 하는 암호화 장치.

청구항 2.

암호화 장치에 있어서,

난수와 제1마스크된 데이터를 논리곱하는 논리곱 회로;

상기 논리곱 회로의 출력신호와 상기 난수를 수신하고, 이들을 배타 논리합하는 배타 논리합 회로;

상기 배타 논리합 회로의 출력신호를 수신하고, 수신된 신호를 오른쪽과 왼쪽중에서 어느 하나의 방향으로 m(여기서, m은 자연수)비트만큼씩 쉬프트시키는 쉬프트 회로; 및

상기 제1마스크된 데이터와 상기 쉬프트 회로의 출력신호를 수신하고, 상기 제1마스크된 데이터와 상기 쉬프트 회로의 출력신호를 산술덧셈하고, 그 결과로서 제2마스크된 데이터를 출력하는 가산기를 구비하는 것을 특징으로 하는 암호화 장치.

청구항 3.

암호화 장치에 있어서,

제1난수와 데이터를 수신하고 부울 마스크된 데이터를 출력하는 제1마스킹 회로;

제2난수와 상기 제1마스킹 회로로부터 출력된 상기 부울 마스크된 데이터를 수신하고, 산술 마스크된 데이터를 출력하는 제2마스킹 회로를 구비하며,

상기 제2마스킹 회로는,

상기 제2난수와 상기 부울 마스크된 데이터를 논리곱하는 논리곱 회로;

상기 논리곱 회로의 출력신호를 수신하고, 수신된 신호를 오른쪽과 왼쪽중에서 어느 하나의 방향으로 m(여기서, m은 자연수)비트만큼씩 쉬프트시키는 쉬프트 회로; 및

상기 부울 마스크된 데이터와 상기 쉬프트 회로의 출력신호를 수신하고, 상기 부울 마스크된 데이터로부터 상기 쉬프트 회로의 출력신호를 산술 뺄셈하고, 그 결과로서 상기 산술 마스크된 데이터를 출력하는 감산기를 구비하는 것을 특징으로 하는 암호화 장치.

청구항 4.

암호화 장치에 있어서,

제1난수와 데이터를 수신하고 부울 마스크된 데이터를 출력하는 제1마스킹 회로;

제2난수와 상기 제1마스킹 회로로부터 출력된 상기 부울 마스크된 데이터를 수신하고, 산술 마스크된 데이터를 출력하는 제2마스킹 회로를 구비하며,

상기 제2마스킹 회로는,

제2난수와 상기 부울 마스크된 데이터를 논리곱하는 논리곱 회로;

상기 논리곱 회로의 출력신호와 상기 제2난수를 수신하고, 이들을 배타 논리합하는 배타 논리합 회로;

상기 배타 논리합 회로의 출력신호를 수신하고, 수신된 신호를 오른쪽과 왼쪽중에서 어느 하나의 방향으로 m(여기서, m은 자연수)비트만큼씩 쉬프트시키는 쉬프트 회로; 및

상기 부울 마스크된 데이터와 상기 쉬프트 회로의 출력신호를 수신하고, 이들을 산술덧셈하고, 그 결과로서 상기 산술 마스크된 데이터를 출력하는 가산기를 구비하는 것을 특징으로 하는 암호화 장치.

청구항 5.

제1항 또는 제3항에 있어서, 상기 쉬프트 회로는 상기 논리곱 회로의 출력신호를 1비트씩 왼쪽방향으로 쉬프트시키는 것을 특징으로 하는 암호화 장치.

청구항 6.

제3항 또는 제4항에 있어서, 상기 제1난수와 상기 제2난수는 서로 동일한 수인 것을 특징으로 하는 암호화 장치.

청구항 7.

암호화 방법에 있어서,

난수와 제1마스크된 데이터를 논리곱하는 (a)단계;

상기 (a)단계의 결과를 수신하고, 수신된 결과를 오른쪽과 왼쪽 중에서 어느 하나의 방향으로 m(여기서, m은 자연수)비트만큼씩 쉬프트시키는 (b)단계; 및

상기 제1마스크된 데이터와 상기 (b)단계의 결과를 수신하고, 상기 제1마스크된 데이터로부터 상기 (b)단계의 결과를 산술 뺄셈하고, 그 결과로서 제2마스크된 데이터를 출력하는 (c)단계를 구비하는 것을 특징으로 하는 암호화 방법.

청구항 8.

암호화 방법에 있어서,

난수와 제1마스크된 데이터를 논리곱하는 (a)단계;

상기 (a)단계의 결과와 상기 난수를 수신하고, 이들을 배타 논리합하는 (b)단계;

상기 (b)단계의 결과를 수신하고, 수신된 신호를 오른쪽과 왼쪽중에서 어느 하나의 방향으로 m(여기서, m은 자연수)비트만큼씩 쉬프트시키는 (c)단계; 및

상기 제1마스크된 데이터와 상기 (c)단계의 결과를 수신하고, 이들을 산술덧셈하고, 그 결과로서 제2마스크된 데이터를 출력하는 (d)단계를 구비하는 것을 특징으로 하는 암호화 방법.

청구항 9.

난수와 제1마스크된 데이터를 논리곱하는 (a)단계;

상기 (a)단계의 결과를 수신하고, 수신된 결과를 오른쪽과 왼쪽 중에서 어느 하나의 방향으로 m(여기서, m은 자연수)비트만큼씩 쉬프트시키는 (b)단계; 및

상기 제1마스크된 데이터와 상기 (b)단계의 결과를 수신하고, 상기 제1마스크된 데이터로부터 상기 (b)단계의 결과를 산술 뺄셈하고, 그 결과로서 제2마스크된 데이터를 출력하는 (c)단계를 실행시키기 위한 프로그램을 기록한 컴퓨터로 읽을 수 있는 기록매체.

청구항 10.

난수와 제1마스크된 데이터를 논리곱하는 (a)단계;

상기 (a)단계의 결과와 상기 난수를 수신하고, 이들을 배타 논리합하는 (b)단계;

상기 (b)단계의 결과를 수신하고, 수신된 신호를 오른쪽과 왼쪽중에서 어느 하나의 방향으로 m(여기서, m은 자연수)비트만큼씩 쉬프트시키는 (c)단계; 및

상기 제1마스크된 데이터와 상기 (c)단계의 결과를 수신하고, 이들을 산술덧셈하고, 그 결과로서 제2마스크된 데이터를 출력하는 (d)단계를 실행시키기 위한 프로그램을 기록한 컴퓨터로 읽을 수 있는 기록매체.

청구항 11.

암호화 방법에 있어서,

제1난수와 데이터를 수신하고 부울 마스크된 데이터를 출력하는 단계;

제2난수와 상기 부울 마스크된 데이터를 수신하고 산술 마스크된 데이터를 출력하는 단계를 구비하며,

상기 산술 마스크된 데이터를 출력하는 단계는,

상기 제22난수와 상기 부울 마스크된 데이터를 논리곱하는 (a)단계;

상기 (a)단계의 결과를 수신하고, 수신된 결과를 오른쪽과 왼쪽 중에서 어느 하나의 방향으로 m(여기서, m은 자연수)비트만큼씩 쉬프트시키는 (b)단계; 및

상기 부울 마스크된 데이터와 상기 (b)단계의 결과를 수신하고, 상기 부울 마스크된 데이터로부터 상기 (b)단계의 결과를 산술 뺄셈하고, 그 결과로서 상기 산술 마스크된 데이터를 출력하는 (c)단계를 구비하는 것을 특징으로 하는 암호화 방법.

청구항 12.

암호화 방법에 있어서,

제1난수와 데이터를 수신하고 부울 마스크된 데이터를 출력하는 단계;

제2난수와 상기 부울 마스크된 데이터를 수신하고 산술 마스크된 데이터를 출력하는 단계를 구비하며,

상기 산술 마스크된 데이터를 출력하는 단계는,

상기 제2난수와 상기 부울 마스크된 데이터를 논리곱하는 (a)단계;

상기 (a)단계의 결과와 상기 난수를 수신하고, 이들을 배타 논리합하는 (b)단계;

상기 (b)단계의 결과를 수신하고, 수신된 신호를 오른쪽과 왼쪽중에서 어느 하나의 방향으로 m(여기서, m은 자연수)비트 만큼씩 쉬프트시키는 (c)단계; 및

상기 부울 마스크된 데이터와 상기 (c)단계의 결과를 수신하고, 이들을 산술덧셈하고, 그 결과로서 상기 산술 마스크된 데이터를 출력하는 (d)단계를 구비하는 것을 특징으로 하는 암호화 방법.

청구항 13.

암호화 방법에 있어서,

n비트의 데이터와 n비트의 제1난수를 수신하고, n비트의 산술 마스크된 데이터 $a_n,a_{n-1}...,a_2,a_1$을 출력하는 단계; 및

n비트의 제2난수 $r_n,r_{n-1},...,r_2,r_1$과 상기 산술 마스크된 데이터 $a_n,a_{n-1}...,a_2,a_1$을 수신하고, n비트의 부울 마스크된 데이터 $y_n,y_{n-1},..,y_2,y_1$을 출력하는 단계를 구비하며,

상기 부울 마스크된 데이터 $y_n,y_{n-1},..,y_2,y_1$을 출력하는 단계는,

상기 a_1을 y_1로서 출력하는 단계;

상기 y_1과 r_1을 논리곱하고 그 결과를 저장장치에 저장하고, 상기 a_2와 상기 저장장치에 저장된 데이터를 배타 논리합하고 그 결과를 y_2로서 출력하고, a_2와 상기 저장장치에 저장된 데이터를 논리곱하고 그 결과로서 올림수로서 발생하는 단계;

상기 y_{k-1}과 상기 r_{k-1}을 논리곱하고 그 결과를 상기 저장장치에 저장하고, a_k와 상기 저장장치에 저장된 데이터와 상기 올림수를 각각 배타 논리합하고 그 결과로서 y_k를 출력하고, (a_k와 상기 저장장치에 저장된 데이터를 논리곱한 결과)와 (a_k와 상기 올림수를 논리곱한 결과)를 논리합하고 그 논리합의 결과와 (상기 저장장치에 저장된 데이터와 상기 올림수를 논리곱한 결과)를 논리합하고 그 결과를 상기 올림수로서 발생하는 단계; 및

상기 y_{n-1}과 상기 r_{n-1}을 논리곱하고 그 결과를 상기 저장장치에 저장하고, a_n과 상기 저장장치에 저장된 데이터와 상기 올림수 각각을 배타 논리합하고 그 결과를 y_n으로서 출력하는 단계를 구비하고,

소정의 변수 k는 3부터 (n-1)까지 1씩 증가되는 것을 특징으로 하는 암호화 방법.

청구항 14.

n비트의 난수 $r_n,r_{n-1},...,r_2,r_1$과 산술 마스크된 데이터 $a_n,a_{n-1}...,a_2,a_1$을 수신하고 n비트의 부울 마스크된 데이터 $y_n,y_{n-1},..,y_2,y_1$을 출력하는 방법에 있어서, 상기 방법은,

상기 a_1을 y_1로서 출력하는 단계;

상기 y_1과 r_1을 논리곱하고 그 결과를 저장장치에 저장하고, 상기 a_2와 상기 저장장치에 저장된 데이터를 배타 논리합하고 그 결과를 y_2로서 출력하고, a_2와 상기 저장장치에 저장된 데이터를 논리곱하고 그 결과로서 올림수로서 발생하는 단계;

상기 y_{k-1}과 상기 r_{k-1}을 논리곱하고 그 결과를 상기 저장장치에 저장하고, a_k와 상기 저장장치에 저장된 데이터와 상기 올림수를 각각 배타 논리합하고 그 결과로서 y_k를 출력하고, (a_k와 상기 저장장치에 저장된 데이터를 논리곱한 결과)와 (a_k와 상기 올림수를 논리곱한 결과)를 논리합하고 그 논리합의 결과와 (상기 저장장치에 저장된 데이터와 상기 올림수를 논리곱한 결과)를 논리합하고 그 결과를 상기 올림수로서 발생하는 단계; 및

상기 y_{n-1}과 상기 r_{n-1}을 논리곱하고 그 결과를 상기 저장장치에 저장하고, a_n과 상기 저장장치에 저장된 데이터와 상기 올림수 각각을 배타 논리합하고 그 결과를 y_n으로서 출력하는 단계를 구비하고,

소정의 변수 k를 3부터 (n-1)까지 1씩 증가시키는 것을 특징으로 하는 암호화 방법.

청구항 15.

n비트의 데이터와 n비트의 제1난수를 수신하고, n비트의 산술 마스크된 데이터 $a_n,a_{n-1}...,a_2,a_1$을 출력하는 단계; 및

n비트의 제2난수 $r_n,r_{n-1},...,r_2,r_1$과 상기 산술 마스크된 데이터 $a_n,a_{n-1}...,a_2,a_1$을 수신하고, n비트의 부울 마스크된 데이터 $y_n,y_{n-1},..,y_2,y_1$을 출력하는 단계를 구비하며,

상기 부울 마스크된 데이터 $y_n,y_{n-1},..,y_2,y_1$을 출력하는 단계는,

상기 a_1을 y_1로서 출력하는 단계;

상기 y_1과 r_1을 논리곱하고 그 결과를 저장장치에 저장하고, 상기 a_2와 상기 저장장치에 저장된 데이터를 배타 논리합하고 그 결과를 y_2로서 출력하고, a_2와 상기 저장장치에 저장된 데이터를 논리곱하고 그 결과로서 올림수로서 발생하는 단계;

상기 y_{k-1}과 상기 r_{k-1}을 논리곱하고 그 결과를 상기 저장장치에 저장하고, a_k와 상기 저장장치에 저장된 데이터와 상기 올림수를 각각 배타 논리합하고 그 결과로서 y_k를 출력하고, (a_k와 상기 저장장치에 저장된 데이터를 논리곱한 결과)와 (a_k와 상기 올림수를 논리곱한 결과)를 논리합하고 그 논리합의 결과와 (상기 저장장치에 저장된 데이터와 상기 올림수를 논리곱한 결과)를 논리합하고 그 결과를 상기 올림수로서 발생하는 단계; 및

상기 y_{n-1}과 상기 r_{n-1}을 논리곱하고 그 결과를 상기 저장장치에 저장하고, a_n과 상기 저장장치에 저장된 데이터와 상기 올림수 각각을 배타 논리합하고 그 결과를 y_n으로서 출력하는 단계를 구비하고,

소정의 변수 k는 3부터 (n-1)까지 1씩 증가되는 것을 단계를 실행시키기 위한 프로그램을 기록한 컴퓨터로 읽을 수 있는 기록매체.

청구항 16.

n비트의 난수 $r_n,r_{n-1},...,r_2,r_1$과 산술 마스크된 데이터 $a_n,a_{n-1}...,a_2,a_1$을 수신하고 n비트의 부울 마스크된 데이터 $y_n,y_{n-1},..,y_2,y_1$을 출력하는 방법에 있어서, 상기 방법은,

상기 a_1을 y_1로서 출력하는 단계;

상기 y_1과 r_1을 논리곱하고 그 결과를 저장장치에 저장하고, 상기 a_2와 상기 저장장치에 저장된 데이터를 배타 논리합하고 그 결과를 y_2로서 출력하고, a_2와 상기 저장장치에 저장된 데이터를 논리곱하고 그 결과로서 올림수로서 발생하는 단계;

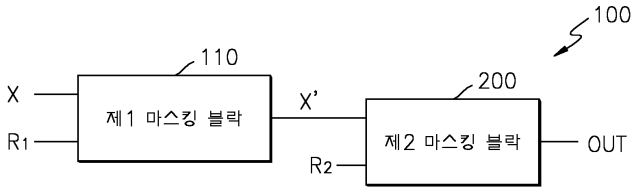
상기 y_{k-1}과 상기 r_{k-1}을 논리곱하고 그 결과를 상기 저장장치에 저장하고, a_k와 상기 저장장치에 저장된 데이터와 상기 올림수를 각각 배타 논리합하고 그 결과로서 y_k를 출력하고, (a_k와 상기 저장장치에 저장된 데이터를 논리곱한 결과)와 (a_k와 상기 올림수를 논리곱한 결과)를 논리합하고 그 논리합의 결과와 (상기 저장장치에 저장된 데이터와 상기 올림수를 논리곱한 결과)를 논리합하고 그 결과를 상기 올림수로서 발생하는 단계; 및

상기 y_{n-1}과 상기 r_{n-1}을 논리곱하고 그 결과를 상기 저장장치에 저장하고, a_n과 상기 저장장치에 저장된 데이터와 상기 올림수 각각은 배타 논리합하고 그 결과를 y_n으로서 출력하는 단계를 구비하고,

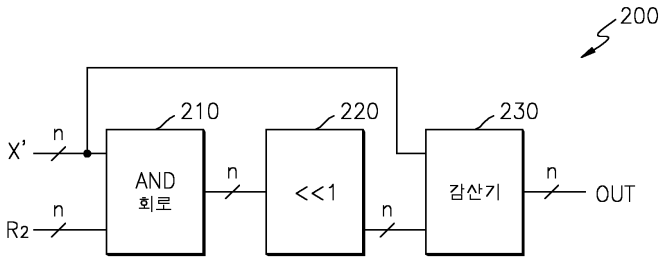
소정의 변수 k는 3부터 (n-1)까지 1씩 증가되는 것을 단계를 실행시키기 위한 프로그램을 기록한 컴퓨터로 읽을 수 있는 기록매체.

도면

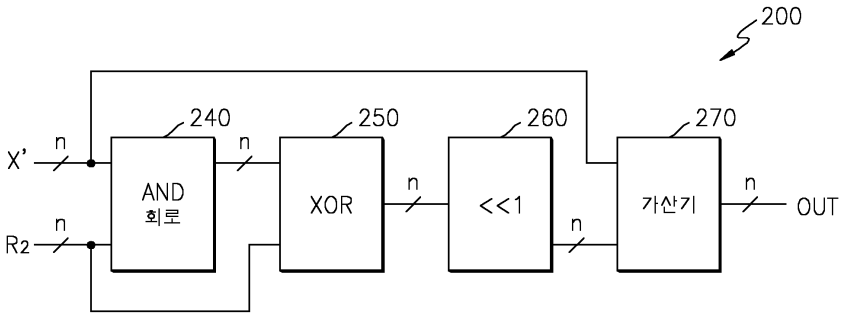
도면1


100
110
X
R1
제1 마스킹 블락
X'
200
R2
제2 마스킹 블락
OUT

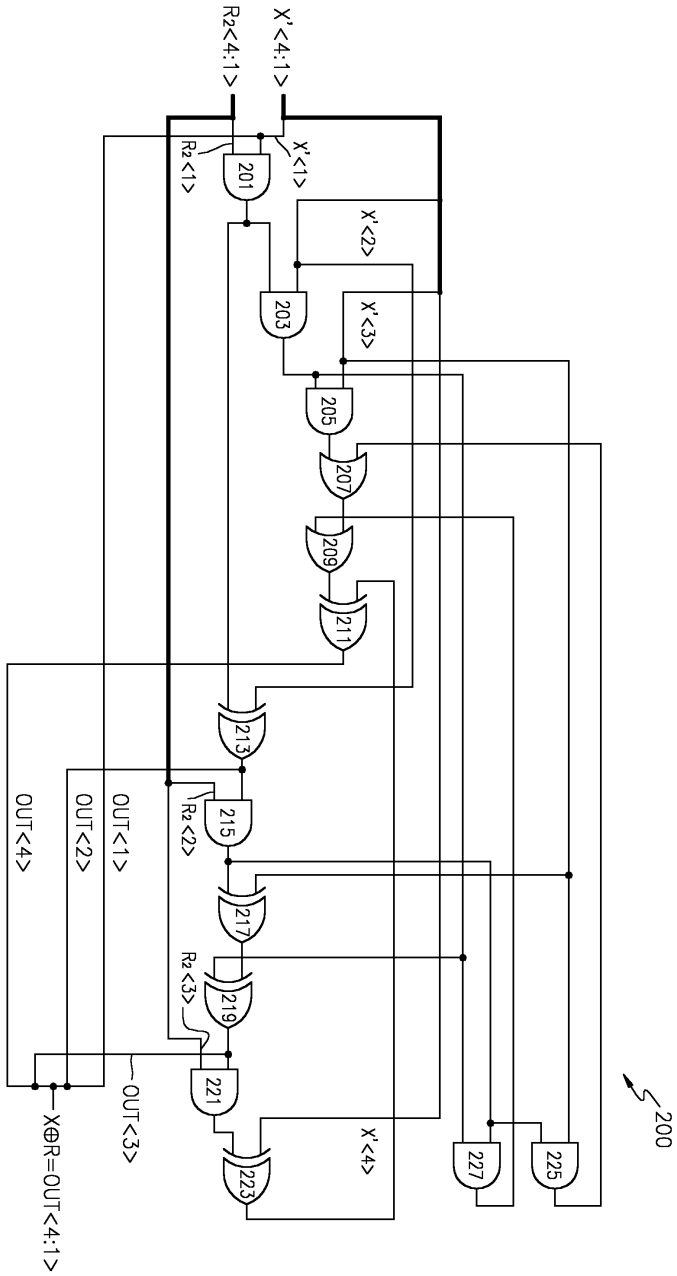
도면2


200
210
220
230
X'
n
AND
회로
<<1
감산기
OUT
R2

도면3


200
240
250
260
270
X'
n
AND
회로
XOR
<<1
가산기
OUT
R2

도면4


R2<4:1>
X'<4:1>
R2 <1>
X'<1>
201
X'<2>
203
X'<3>
205
207
209
211
213
R2 <2>
215
217
R2 <3>
219
221
223
X'<4>
227
225
200
OUT<4>
OUT<2>
OUT<1>
OUT<3>
X⊕R=OUT<4:1>