

해밍 웨이트 모델을 이용한 전력 분석공격을 방지할 수 있는 논리회로 및 이를 포함하는 스마트 카드 (한국 등록특허 10-1332376)

Sales Material Kit

기술 소개

- 본 특허는 전력 분석공격을 방지하기 위한 해밍 웨이트 모델을 이용 및 포함한 스마트 카드에 관한 것으로서, 논리회로에 간단한 소자의 설치와 구성으로 보안 기능이 강화된 스마트 카드에 관한 것임

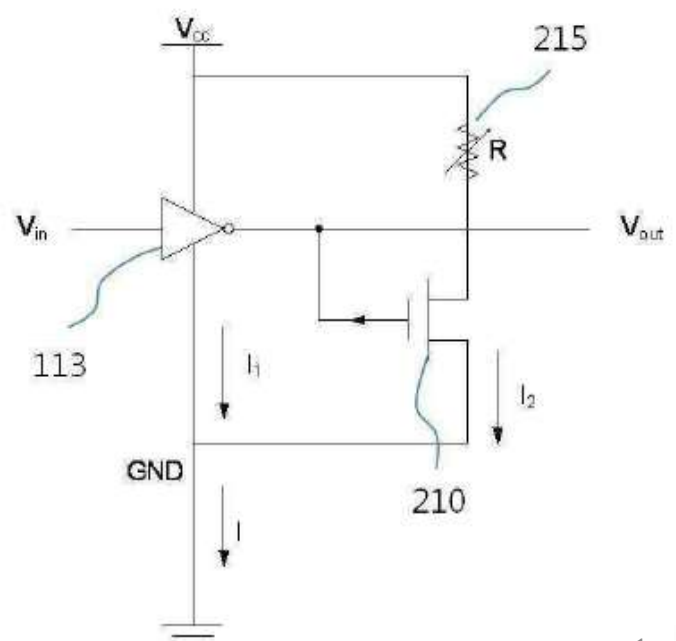
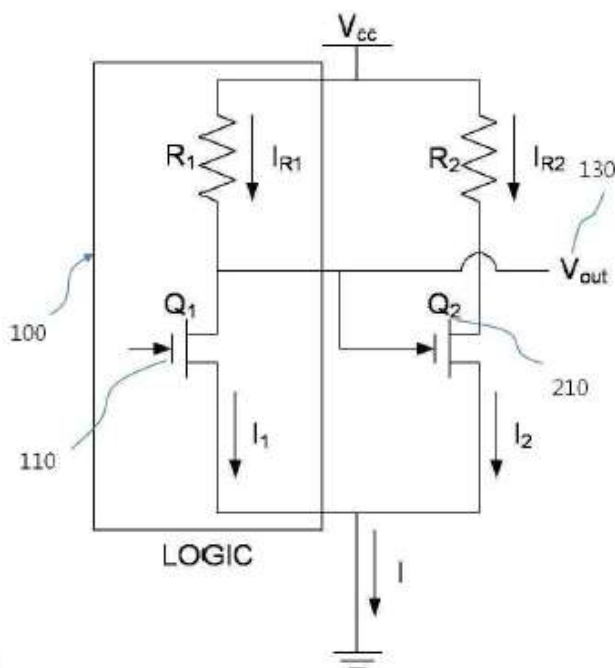
기술 특징



논리 게이트를 포함하는 논리 회로와, 상기 논리 게이트의 출력단에 동일한 특성의 FET 소자가 설치되어, 상기 논리 회로의 전체 전류를 일정하게 유지

암호화 프로세스를 수행하는 논리회로의 출력단에서 전력신호 또는 전류신호를 측정하더라도 일정한 값을 도출시켜 전력 분석공격을 원천적으로 차단할 수 있는 전력 분석공격 방지 논리회로를 제공

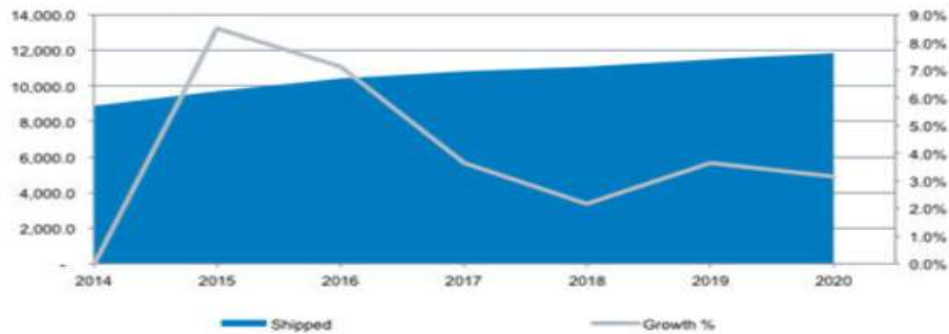
도면



시장 규모 및 전망

- 주요 성장을 주도하는 분야는 은행, 지불, 전자정부, 의료 및 운송업 등에 해당하며 전자 정부, 은행 지불 부분에서 우수한 성장 잠재력을 가지고 있음
- 글로벌 스마트 카드 시장은 2015년 약 88억 개가 출하되었으며, 향후 2020년에는 약 119억 개로 증가할 것으로 전망됨

세계 스마트 카드 출하와 성장 추이



Source: IHS

- 국내 신용카드 발급 현황을 살펴보면 2016년 말 1억 848만 장으로 조사되었으며, 2017년은 1.7%증가한 1억 1,035만 장으로 신용카드 및 체크카드 모두 발급 수가 증가함을 확인할 수 있어 스마트카드 시장 성장은 지속될 것으로 추정됨

국내 카드(누적)발급 매수 추이

(단위 : 만 매, %, %p)

구분	2015년 말	2016년 말(A)	2017년 말(B)	증감(률)(B-A)
신용카드(A)	9,314	9,564	9,946	382 (4.0)
휴먼카드(B)	831	850	800	△50 (5.9)
비중(B/A)	8.9	8.9	8	△0.9 (-)
체크카드	10,527	10,848	11,035	187 (1.7)

Source: 금융감독원

- 신용카드 발급과 모바일 결제시스템의 증가에 따른 모바일 인증 및 보안 중요성의 확대로 인해서 보안성이 강화된 스마트 카드 시장은 지속적으로 증가할 것으로 판단됨

모바일 인증 및 보안 중요성 확대

모바일 결제 시스템 확대에 의한 모바일 인증과 보안 중요성 및 관련 시장이 증가되고 있음

모바일 결제 시스템 증가

현금 대신 신용카드나 스마트 폰을 이용한 모바일 결제 시스템의 공급 확대

신용카드 발급 확대

개인 신용카드 발급의 확대에 스마트 카드 수요 증가

기술 응용분야

후방산업

전자카드

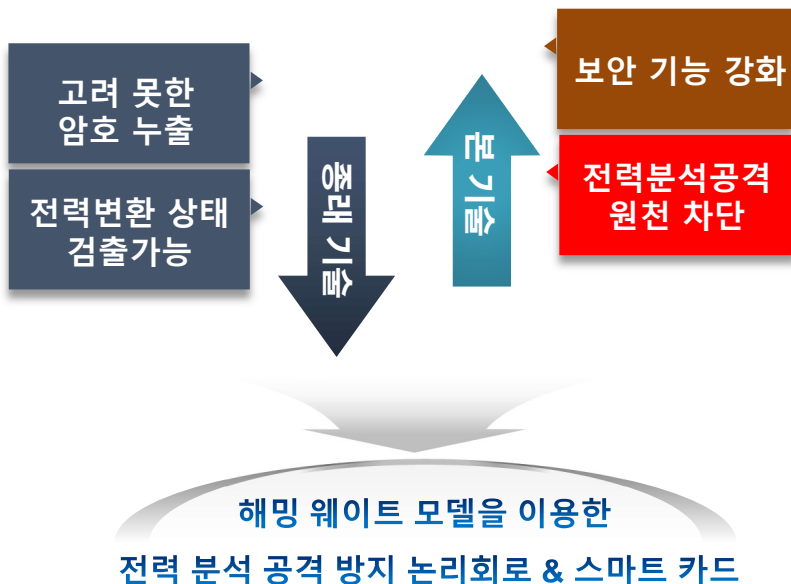
전방산업

- ❖ 전자집적회로 제조업
- ❖ 기타 전자부품 제조업
- ❖ 플라스틱 필름, 시트 및 판 제조업

- ❖ 전자카드
- ❖ 스마트카드

- ❖ 금융 및 보험업
- ❖ 통신업
- ❖ 컴퓨터 프로그래밍, 시스템 통합 및 관리업
- ❖ 정보서비스업
- ❖ 사업지원 서비스업

경쟁기술 대비 특징점



- 논리회로에 간단한 소자의 설치와 구성으로 전력신호를 일정한 값을 도출시켜 전력변환을 외부 파형으로 검출할 수 없도록 하여 전력 분석공격을 원천적으로 차단
- 해밍 웨이트 모델을 이용한 전력 분석공격 방지 논리회로를 포함하는 스마트 카드를 제공함으로써 간단한 구성으로 보안 기능을 강화

기대 효과

- 기존 논리회로 대비 해밍 웨이트 모델을 이용하여 간단한 소자의 설치와 구성으로 전력 분석공격을 원천적으로 차단할 수 있는 논리회로 모델을 제공함으로써 보안 기능을 강화 시킬 수 있음
- 스마트 카드는 현금카드와 신용카드 USIM, IC 카드에 활용 가능하며, 향후 보안성이 요구되는 부분에 있어서 다양하게 적용되어 활용성이 양호할 것으로 전망

협업 방법

- 본 기술의 기술이전
- 본 기술의 상용화/제품화
- 파트너쉽 체결을 통한 동서대학교 해당 연구실과의 Co-Working
- 기술 및 제품 사업화 마케팅 지원
- 특허/상표/디자인 등 신규 IP 창출 및 포트폴리오 컨설팅

연구자 주요 연구분야



- 성명 / 소속 : 이훈재 교수 / 동서대학교 컴퓨터공학부
- 주요 연구분야 : 정보보안(암호시스템 설계/암호해독), 네트워크보안(전자상거래 보안), 정보통신 네트워크/데이터 통신
- 주요 경력
 - 경북대학교 공학박사
 - 국방과학연구소 선임연구원

기술명

해밍 웨이트 모델을 이용한 전력 분석공격을 방지할 수 있는 논리회로 및 이를 포함하는 스마트 카드



Contact Point



성명 ▶ 박동창 / 팀장

소속 ▶ 동서대학교 산학협력단
기술경영센터

전화 ▶ 051-320-2696

E-mail ▶ park123@dongseo.ac.kr

본 기술은 동서대학교 산학협력단이 보유기술로서 동서대학교 우수 기술자산 및 수요자 발굴을 위한 특허 분석 프로그램을 통하여 발굴된 사업화 유망기술입니다. 본 기술에 관심 있으신 기업 및 연구기관 담당자께서는 위 Contact Point로 연락주시기 바랍니다.

