

알고리즘의 방어기술 적용방법

I. 기술소개

◆ 종래기술의 문제점

- 종래에는 전력분석공격에 취약한 알고리즘(즉, PingPong-128 알고리즘) 사용시 전력분석공격에 대해 방어기술을 적용하지 못하여 안전성을 제공하지 못하는 단점이 있음

◆ 기술의 특징

- PingPong-128 알고리즘에 전력분석공격에 대한 방어기술 적용방법
 - 스크램블러와 디스크램블러를 활용하여 랜덤화 방법을 적용함에 따라, 회로가 단순하면서 도 차등 전력 분석(DPA)에 대한 방어를 제공함
 - 랜덤화 방법은 키 랜덤화 방법과 평문 랜덤화 방법으로 구분되고, 키 랜덤화 방법은 키 값과, 평문상태로 전송될 초기벡터 값에 스크램블러를 적용함
 - 평문 랜덤화 방법은 평문 값에 스크램블러를 적용함

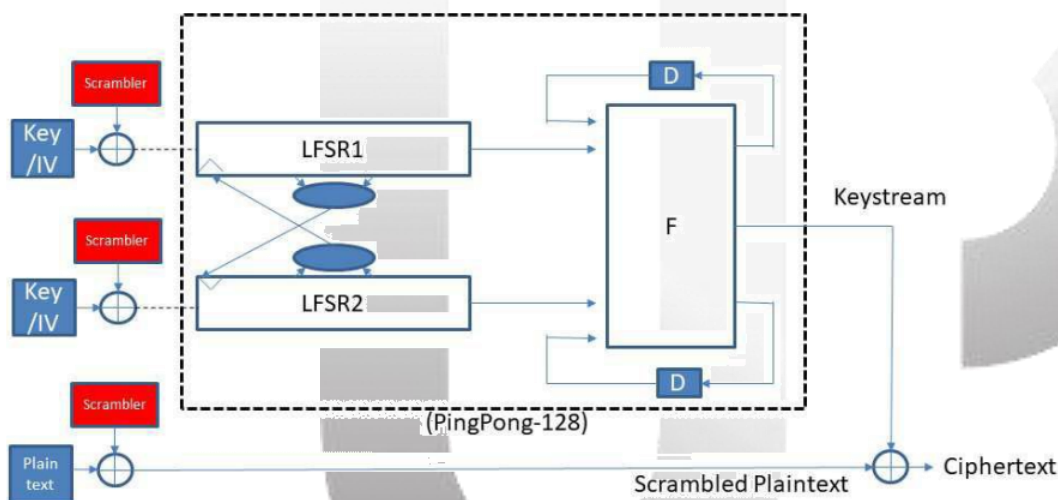


그림1: 알고리즘의 방어기술 적용방법에 대한 개념도

기대 효과

- 전력분석공격에 취약한 알고리즘(즉, PingPong-128 알고리즘)에 전력분석공격에 대한 방어기술을 적용하여 전력분석공격에 대한 안전성을 제공하는 현저한 효과가 있음

◆ 알고리즘의 방어기술 적용방법

• 전력분석공격에 대한 안정성 제공

전력분석공격에 취약한 알고리즘(즉, PingPong-128 알고리즘)에만 방어기술을 적용하는 것으로, 송·수신 암호에는 방어기술을 적용하지 않아 암호 알고리즘의 성능이 저하되지 않으며, 전력분석공격에 대한 안전성을 제공함

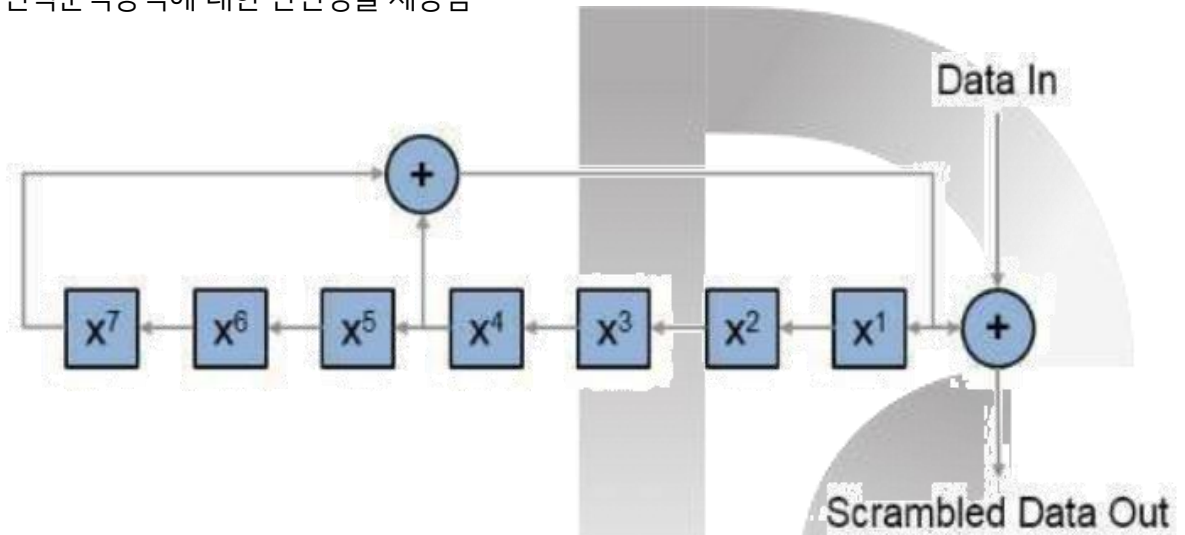


그림2: 알고리즘의 방어기술 적용방법에 대한 스크램블 작동 개념도

• 회로가 단순하면서도 차등 전력 분석에 대한 방어가 가능

전력분석공격에 취약한 알고리즘에 적용할 수 있는 방어기술로써, 스크램블러와 디스크램블러를 활용하여 랜덤화 방법을 적용함에 따라, 회로가 단순하면서도 차등 전력 분석(DPA)에 대한 방어 수행이 가능함

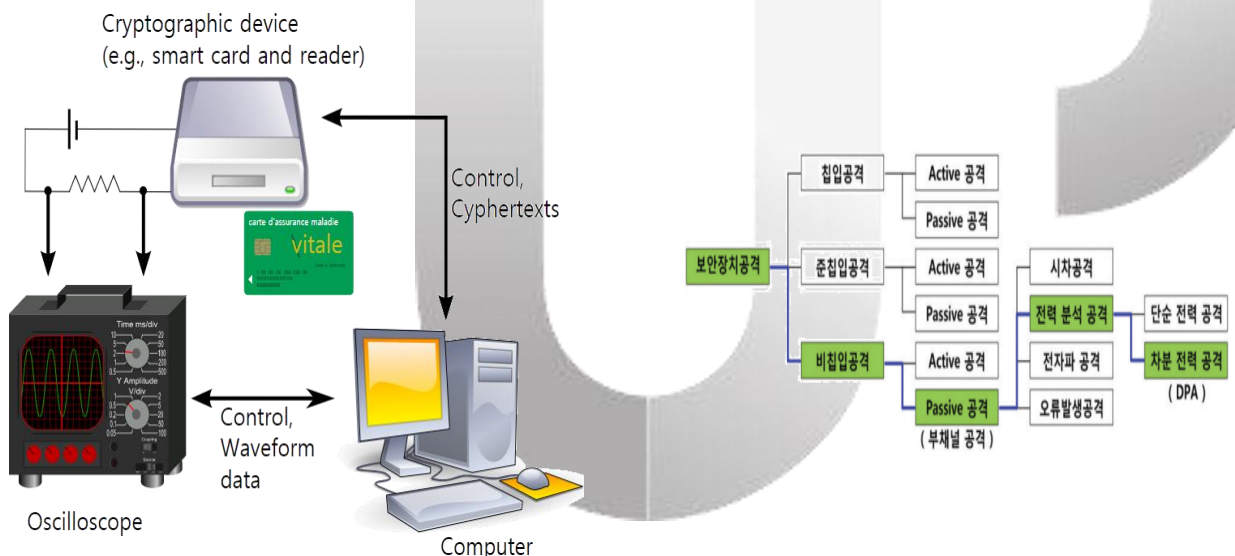


그림3: 전력 분석 공격에 대한 다이어그램
출처: 위키백과, '전력 분석'

그림4: 차등 전력 분석 공격에 대한 개념
출처: IDEC 뉴스레터, 2012.09

II. 상업화

◆ 적용

- 전력분석공격에 대한 방어기술 적용기술

◆ 시장성(해외)

- 본 기술과 밀접한 관련이 있는 사이버보안 글로벌 시장은 2016년 814억 달러에서 연평균 성장률 8.1%로 성장하여 2021년에는 1,200억 달러 규모를 형성할 것으로 전망됨

(단위 : 백만 달러, %)

구분	'16	'17	'18	'19	'20	'21	CAGR
세계시장	81,439	88,093	95,283	102,923	111,143	120,146	8.1

표1: 사이버보안 분야 글로벌 시장 전망

출처: 중소기업기술로드맵-정보보안, 2019.12

- 지역별로는, 북미 지역은 2016년 332억 달러에서 연평균 성장률 7.1%로 성장하여 2021년에는 466억 달러 규모를 형성할 것으로 전망됨
- 아태 지역은 2016년 164억 달러에서 연평균 성장률 9.5%로 성장하여 2021년에는 260억 달러 규모를 형성할 것으로 전망됨
- 분야별로는, 정보보안(사이버 보안) 지출이 가장 큰 분야는 컨설팅 및 IT 아웃소싱 분야이며, 2020년 말까지 보안 테스트, IT아웃소싱, 데이터 손실 방지(DLP) 분야의 지출이 가장 높은 성장세를 보일 것으로 전망됨

(단위 : 백만 달러, %)

구분	'15	'16	'17	'18	'19	'20	'21	CAGR
북미	30,926	33,227 (7.4)	35,413 (6.6)	37,732 (6.5)	40,346 (6.9)	43,346 (7.4)	46,554 (7.4)	7.1
유럽	18,103	19,382 (7.1)	20,702 (6.8)	22,201 (7.2)	23,569 (6.2)	25,007 (6.1)	26,637 (6.5)	6.6
아태지역	15,086	16,451 (9.0)	18,059 (9.8)	19,914 (10.3)	21,717 (9.1)	23,785 (9.5)	26,037 (9.5)	9.5
중동·아프리카	6,788	7,411 (9.2)	8,193 (10.6)	8,957 (9.3)	10,086 (12.6)	11,114 (10.2)	12,119 (9.0)	10.1
남미	4,526	4,968 (9.8)	5,726 (15.3)	6,479 (13.2)	7,205 (11.2)	7,891 (9.5)	8,639 (9.5)	11.4
전체	75,429	81,439 (8.0)	88,093 (8.2)	95,283 (8.2)	102,923 (8.0)	111,143 (8.0)	119,986 (8.0)	8.0

표2: 사이버보안 분야 지역별 시장 전망

출처: 중소기업기술로드맵-정보보안, 2019.12

◆ 시장성(국내)

- 본 기술과 밀접한 관련이 있는 정보보호산업 국내 시장은 2016년 8조 9,502억 원에서 연평균 성장률 7.7%로 성장하여 2021년에는 12조 9,566억 원 규모를 형성할 것으로 전망됨
- 특히, 정보보안(사이버 보안) 시장은 2016년 2조 4,318억원에서 연평균 성장률 10.4%로 성장하여 2021년에는 3조 9,836억원 규모를 형성할 것으로 전망됨

(단위 : 백만 원, %)

구분	'16	'17	'18	'19	'20	'21	CAGR
정보보안	2,431,868	2,756,121	3,125,784	3,473,237	3,764,969	3,983,673	10.4
물리보안	6,518,300	7,435,542	8,026,512	8,478,577	8,785,381	8,972,894	6.6
합계	8,950,168	10,191,663	11,152,296	11,951,814	12,550,350	12,956,567	7.7

표3: 사이버보안 분야 국내 시장 전망
출처: 중소기업기술로드맵-정보보안, 2019.12

- 분야별로는, 정보보안 지출이 가장 큰 분야는 네트워크 분야이며, 다음으로 콘텐츠/정보유출 방지 보안 분야, 시스템(단말) 보안 분야, 보안관리 분야 및 암호/인증 분야 순으로 시장 규모가 크게 형성될 것으로 전망됨

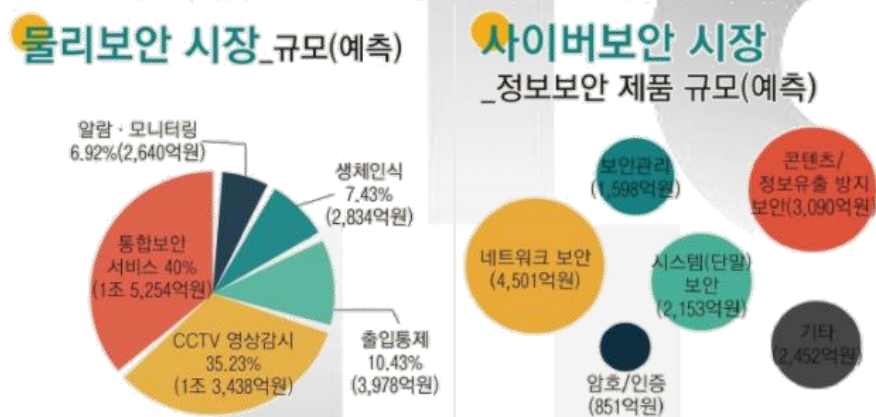


그림5: AI 헬스케어의 시장 규모 및 전망
출처: 과학기술정보통신부 홈페이지, 2019.07

◆ 연구개발 현황

- 실제 기업 니즈를 반영한 연구 개발 결과이며, 본 연구실은 사이버 보안과 관련하여 지속적으로 특허 출원을 진행함

◆ 상업화 단계 현황

- 본 연구는 현재 시제품 제작 완료 후 성능 테스트 중에 있음

◆ Contact Point

- 담당자 : 기술경영센터
- Tel : 010-4312-3972 • E-mail : sem903@dongseo.ac.kr
- 주소 : 부산시 사상구 주례로 47 동서대학교 산학협력단 기술경영센터