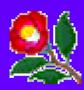
Smartcard Security to DPA attack

& Common Criteria (CC)



HoonJae Lee

E-mail: hjlee@dongseo.ac.kr

Homepg: http://kowon.dongseo.ac.kr/~hjlee

Lab.Hm: http://crypto.dongseo.ac.kr

Hot Issues(2003.6.17) (2003.3.25)

종합·해설

반응 '극과 극'

정보보호

생체인식·스마트카드 응용제품

CC 평가대상 포함 가능성

정통부, '연구위' 구성

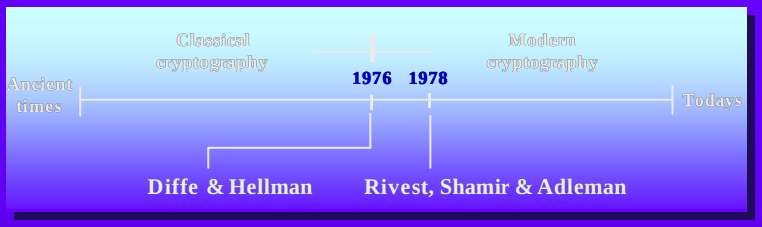
상반기에 제품 선정

PKI 솔루션도 거론

Outline

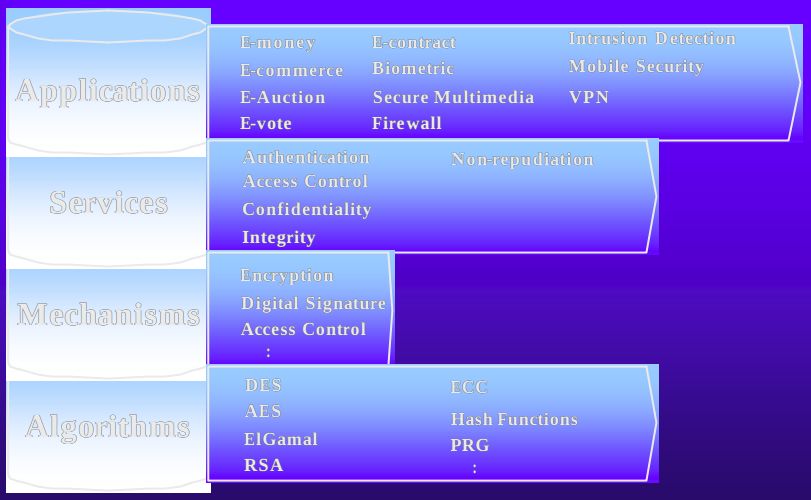
- What's Smartcard?
- DPA attacks to Smartcard
- Experimental Results
  - DES
  - RSA
  - ECC
- Common Criteria
- Conclusion

History of Cryptology



- Symmetric-key cryptography
  - use the same key in both encryption and decryption
  - Examples: DES('77), IDEA('90), SEED('97,Korea), AES('02)
- Asymmetric-key cryptography
  - use different keys in encryption and decryption
  - Examples: D-H key distribution('76), RSA('78), and ECC('80L)
- Big Projects
  - AES('02, USA), NESSIE('03, EU), CRYPTREC('03, Japan)

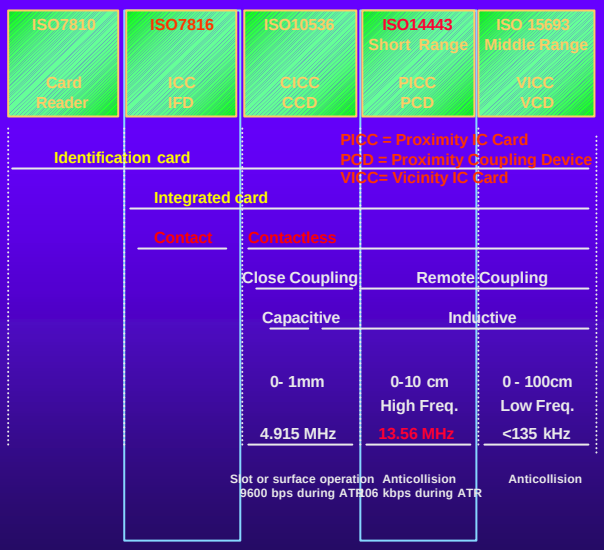
Security Service and Mechanism



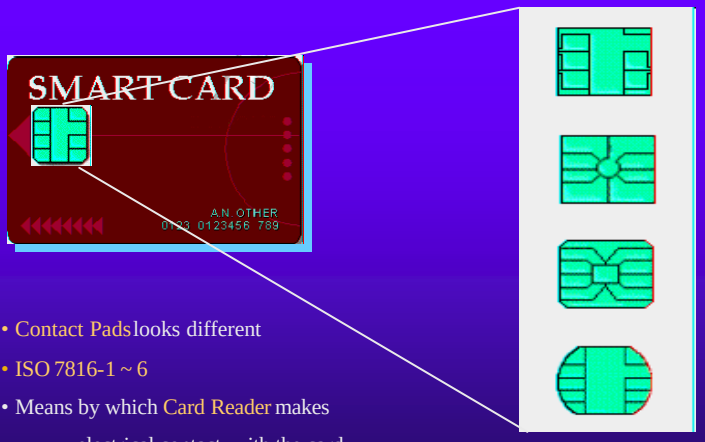
❑ Smart Card Security

- ❍ 스마트카드 산업 (전자상거래, 신분인증 분야) - 비약적인 발전
  - ▪ 공무원카드, 전자화폐, 교통카드, 의료카드, 전자주민카드 등에 적용
  - ▪ 한국전자통신연구원 제시 IT분야 30/40대 전략품목
- ❍ 스마트카드 수요 : 2003년까지 PKI 인증 서명용으로
  - ▪ (국내) 수요 1,000만개의 카드 소지 유도 : 정보통신부
  - ▪ (국제) 수요 50억개 (70억불)의 생산이 예측
- ❍ 스마트카드 공격 기술 : 미국 크립토리서치 사 Kocher에 의하여 제안
  - ▪ 부채널공격 유형: Timing Attack/Fault-Ins. Attack/**Power Analysis Attack**
  - ▪ 전력분석공격 유형: SPA/**DPA**/IPA/HO-DPA
  - ▪ RSA공격 유형 : SEMD/**MESD**/ZEMD
- ❍ DPA 기술/실험/방어대책 수립 필요
  - ▪ (국내) 스마트카드 공격 대응 기반기술 축적
- ❍ 국내 스마트카드 DPA 공격에 대한 안전성 평가기준 개발 필요
  - ▪ 국제 공통평가기준 수용(2002년 8월 5일 정보통신부 공시)
  - ▪ DPA 방어 대응 기술 수용 → 안전성 평가기준서 개발시 필수적

Smart Card - Standards

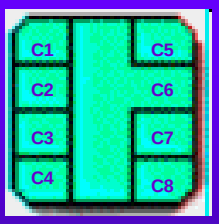


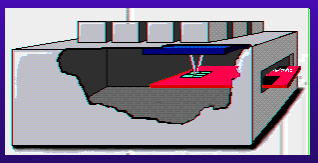
Smart Card - Contact Pad



- Contact Pads looks different
- ISO 7816-1 ~ 6
- Means by which Card Reader makes electrical contact with the card

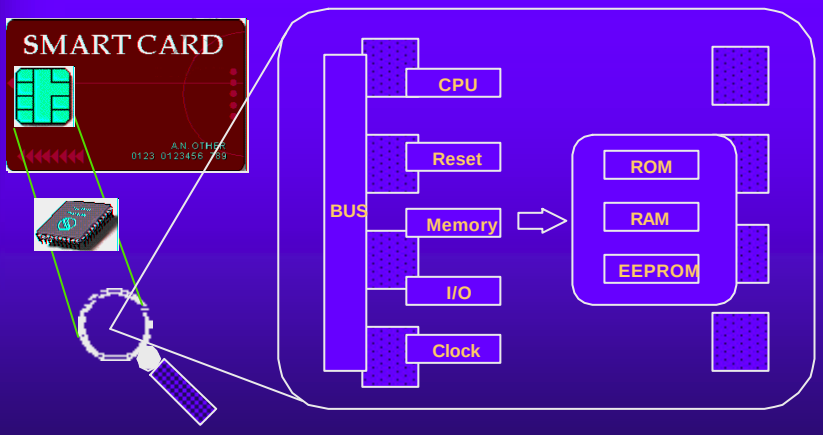
❑ Smart Card - Contact Pad





- **C1** : power supply input (Vcc)
- **C2** : RST for reset signal to card
- **C3** : CLK (clock)
- **C4** : not defined
- **C5** : GND (ground)
- **C6** : Vpp
- **C7** : communication
- **C8** : not defined

❑ Smart Card – Internal Structure



Smart Card - CPU and OS

- Smartcard CPU
  - INTEL 8051, Motorolla 6805 8-bit processor
  - 32-bit processor based on RISC architecture
- Smartcard Chip Category
  - Dumb Cards, Wired Logic Cards
  - Smartcards
- Smartcard Operating System
  - OS → COS, Mult-OS
  - commands to open, read, write, erase files
  - access control to files through key or PIN
  - message certification, and communication

Smart Card - Memory

- Volatile Memory
  - DRAM
  - Scratchpad, RAM Stack (Working Area)
  - 128 ~ 512 Bytes

- Nonvolatile Memory
  - ROM
    - Smartcard Operating System, Card Mask
    - 2 ~ 16K Bytes
  - EEPROM, Flash Memory
    - User/Application Area (UAM)
    - 1 ~ 16 K Bytes

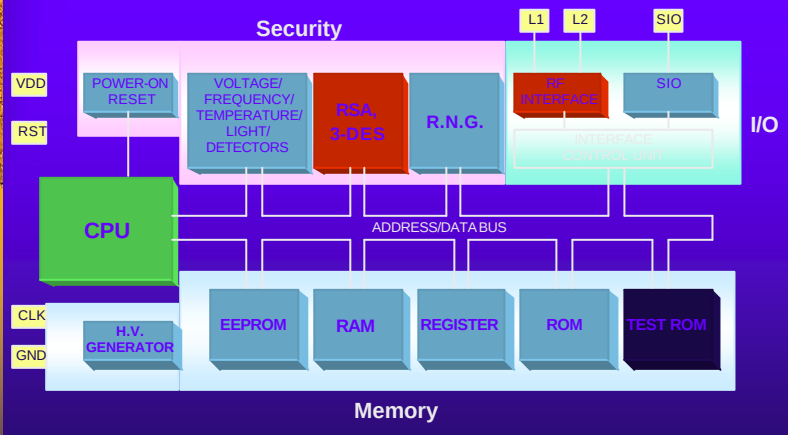
❑ SmartCard - Chip Manufacturer

❖ Samsung

Memory	■ EEPROM,FLASH, ROM, SRAM ■ Reliable Process and Design for Small Size ■ Endurance and Data Retention
RF and I/O	■ ISO14443 and ISO7816 ■ Modulation: 10% or 100% ASK ■ Bit-Coding: PWM, BPSK, NRZ, Modified Miller
Security	■ Crypto Processor (RSA, 3-DES) ■ Various Detector against Attacks ■ Random Number Generator for Authentication
CPU	■ 8-Bit CPU (SAM87RC) ■ 16-Bit/32-Bit CPU (CalmRISC) ■ 32-Bit CPU (ARM7TDMI,SC100)

❑ SmartCard - Chip Manufacturer

❖ Samsung



SmartCard - Chip Manufacturer

- International

Chip	Maker	Core	RAM (bytes)	ROM (Kbytes)	NVM (Kbytes)	Surface (mm)
SC01	Motorolla	68HC05	36	1.6	*1*	3.5 x 5.5
SC24	Motorolla	68HC05	128	3	1	4.14 x 3.44
SC28	Motorolla	68HC05	240	12.8	8	27
ST1821	Thompson	8048	44	2	*1*	3.4 x 5.36
ST16301	Thompson	68HC05	160	3	1	3.66 x 4.93
ST16F48	Thompson	68HC05	512	16	8	4.8 x 4.9
44C10	Siemens	80C51	128	4	1	13
44C40	Siemens	80C51	256	8	4	18.39
44C80	Siemens	80C51	256	16	4	24.49

SmartCard - Chip w/ Coprocessor

- International

- Public-Key Cryptosystem
- 8-bit Processor and Coprocessor for modular exponentiation
- ISO 7816-1, chip size of 25mm^2, some EEPROM area occupied

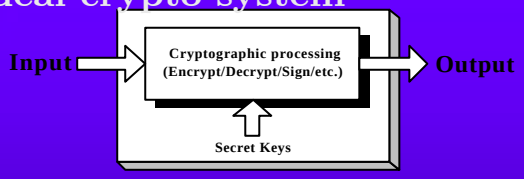
Name	Maker	Core	Core	ACP	RAM	EE	ROM
ST16CF54	Thompson	68HC05	secret	secret	352	16	16
ST16KL74	Thompson	68HC05	secret	secret	608	20	20
SLE44C200	Siemens	80C51	24.5	5.7	256	9	9
SLE44CR80S	Siemens	80C51	<25		256	8	17
P83C852	Philips	80C51	22.3	2.5	256	2	6
P83C858	Philips	80C51			640	8	20
MC68HC05	Motorolla	68HC05	27	5	512	4	13.3
CY512i	Cylink	80C31	73		768	8	8

SmartCard - Other Circuits

- RST and ATR
  - RESET signal, card initialization
  - Answer to RESET signal, (card type and appliation type)
- Synchronization Circuit
  - Timing signal from internal clock or external clock
  - synchronize card's internal operations and communications
  - 5 ~ 14 MHz
- Communication Circuit
  - I/O Port in contact C7
  - Synchronous or Asynchronous Mode
  - Internal Amplifier

Side Channel Attack

Ideal crypto system

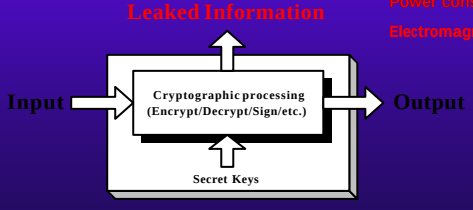


Real crypto system

Timing

Power consumption(RSA, ECC ..)

Electromagnetic radiation ....



History of Power Attacks

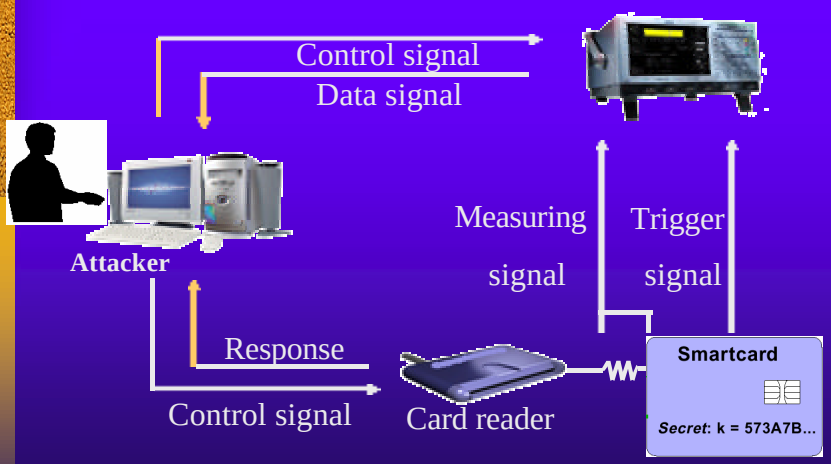
1999 — Differential Power Analysis in CRYPTO ' 99
Paul C. Kocher, et al

2000 — Power Analysis Attacks of Modular Exponentiation in CHES' 99
T. S. Messerges, et al
Resistance against DPA for ECC in CHES'99
J. S. Coron

2001 — Randomized Addition-Subtraction Chains against PA in CHES' 01
E. Oswald et al

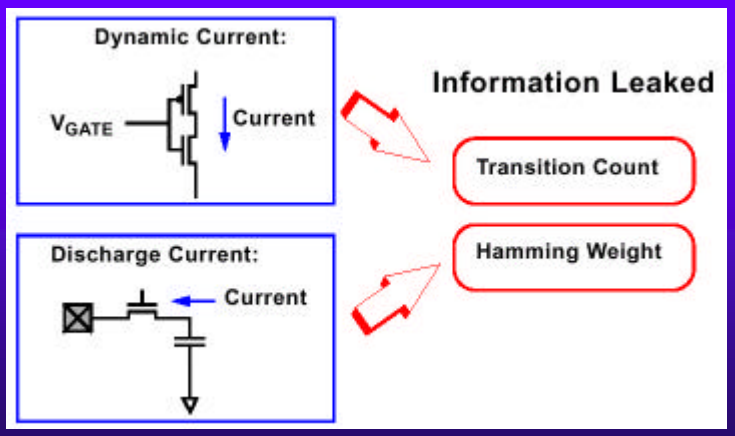
2002 — DPA Countermeasure by improving the window method in CHES'02
K. Itoh et al

Equipments for Attacks



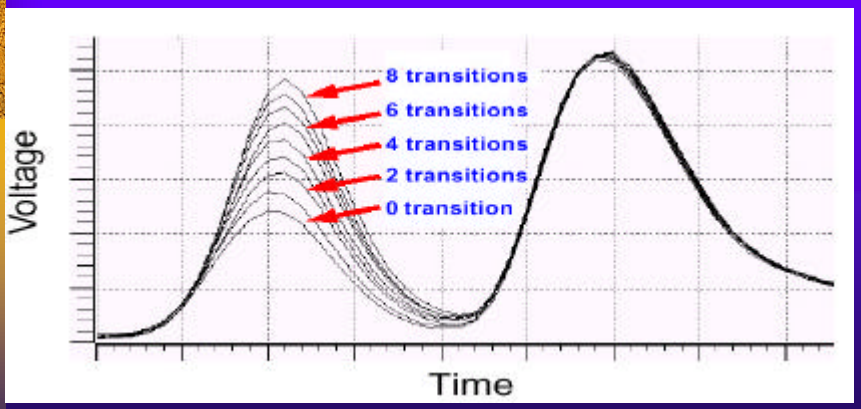
❑ Power Analysis Attack

- Information from Power Consumption

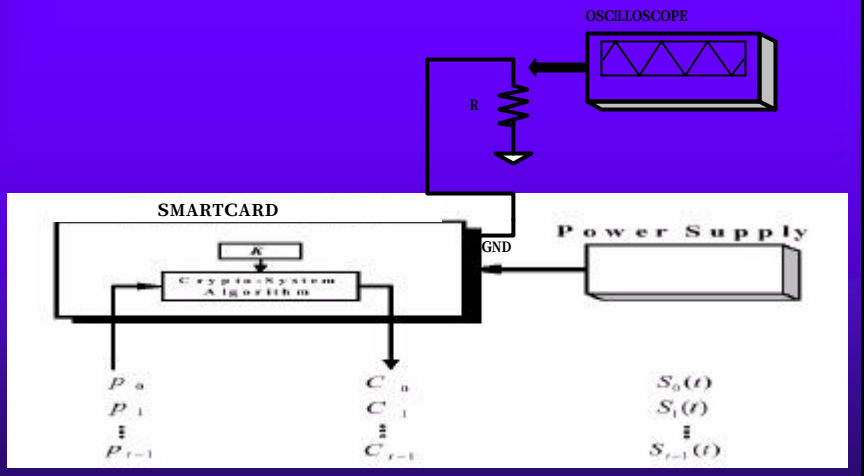


Power Analysis Attacks

- Number of Bit Transitions vs. Power Consumption [Messerges,1999]
  - **LDA instruction** → 6.5mV difference in ith and (i+1)th transition
  - **Ex) LDA A,#00h → LDA A,#FFh (8-bit transitions): 52 mV**



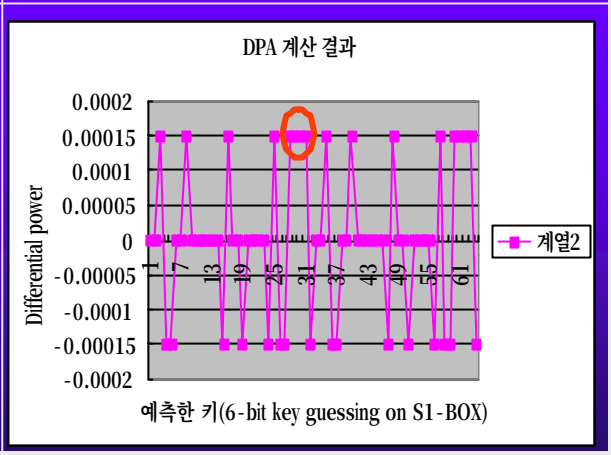
❑ Power Analysis Attack: DES



❑ Power Analysis Attack: DES

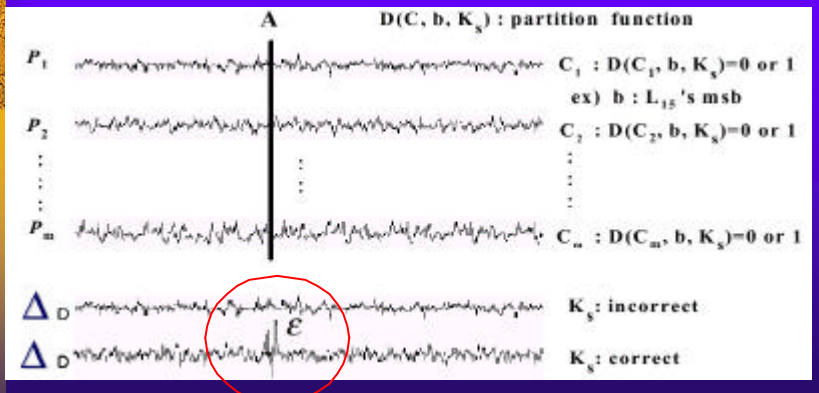
항 목	실험 내용
○ 전력 파형 측정 - 수집된 그룹 1 전력 샘플데이터(DES의 S1-box 시작 위치에서의 1,000 샘플포인트, 카드 리더기 활용) - 그룹 1 전력 샘플 : 100개 - 그룹 2 전력 샘플 : 100개 - 그룹 3 전력 샘플 : 100개	a) 1st sample power data b) 2nd sample power data c) 3rd sample power data d) 100th sample power data

❑ Power Analysis Attack: DES

항 목	실험 내용
○ 전력 파형 측정 - s1-box에 대한 결과(correct key=011100B=28D 가정, group 1) ➔ 유사 키 군을 추정함 ➔ 정확한 키의 추정은 1000개 이상의 정밀한 전력 데이터 수집이 요구됨	

❑ Power Analysis Attack: DES

○ DES-DPA : Correct key estimated → peak
Incorrect key → noise



❑ Power Analysis Attack: RSA

RSA-MESD 공격 방법

1. 데이터 수집 단계
   평문과 암호문에 대한 소모전력파형을 수집한다.
   수집하는 과정을 K번 반복한다.
2. 데이터 분석 단계
   키의 일부를 추측한다.
   두 스마트카드의 소모전력 파형을 각각 분류한다.
   분류한 전력데이터를 평균하여 차분 전력파형을 구한다.

$$D[r] = \frac{1}{K}\sum_{j=0}^{K-1} S_j[r] - \frac{1}{K}\sum_{j=0}^{K-1} T_j[r]$$

S_j : 공격대상 스마트카드의 소모전력 파형
T_j : 비밀키 변경이 가능한 비교용 스마트카드의 소모전력 파형

피크의 유·무로 추측키를 검증한다.

❑ Power Analysis Attack: RSA

MESD 공격 가정

- 동일 구조 스마트카드 2개 보유
  공격 대상 스마트카드
  비밀키 변경이 가능한 비교용 스마트카드.
- 스마트카드의 암호 알고리듬의 종류와 비밀키 연산의 동작 시점을 알고 있다.
  LR method를 사용하는 암호 알고리듬
- 비밀키의 비트 길이 k를 알고 있다.
  최상위 비트부터 최하위 비트까지의 비트 수.

❑ Power Analysis Attack: RSA

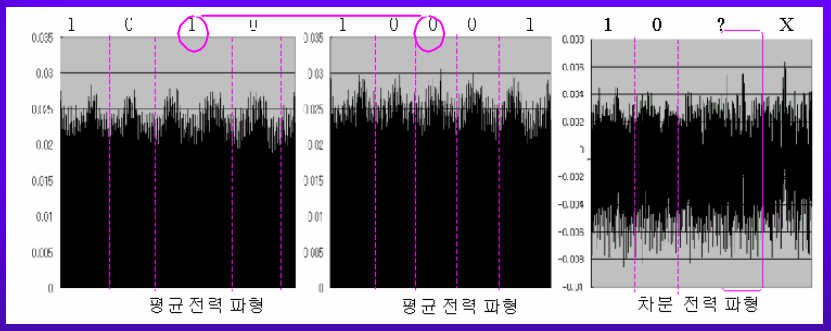
- 이진 멱승 알고리즘
  - 데이터 수집
    - ✓ 200회 이상의 소모전력 파형을 수집
  - 데이터 분석

Input : m , $d=(d_{k-1}, \ldots, d_0)_2$, n
Output : $A = m^d \bmod n$

A ← 1
For i from k-1 downto 0
  $A \leftarrow A^2 \bmod n$ ← Squaring
  if $(d_i = 1)$ then $A \leftarrow A \cdot m \bmod n$ ← Multiplication
endfor

❑ Power Analysis Attack: RSA

- RSA-MESD ➔ 세 번째 비트 차분 전력분석공격시



(a) guessing (b) original (c) result

- 비밀키 *d* 의 추측한 비트 위치(Miss guessing) ➔ Peak
- 차분 전력 파형에서 피크가 생성되면 정확한 비트가 아님

❑ Power Analysis Attack: ECC

Preliminaries

- Binary scalar multiplication(ECC)

  - $Q=O$

    for $i=n$ -1 to 0 by--1 do {

    $Q=2Q$: Doubling

    if (k_i==1) then $Q=Q+P$ } : Addition

    Return Q

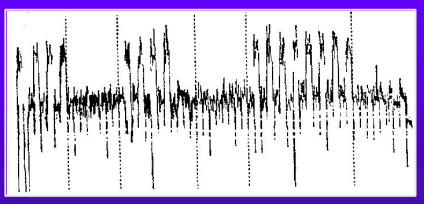
  - # of doubling : n, average # of addition: $n/2$

❑ Power Analysis Attack: ECC

Our Power Attack – I

- SPA(Simple Power Attack)

```
Q=O
for i=n -1 to 0 by -1 do {
  Q=2Q
  if (k_i==1) then Q=Q + P
}
Return Q
```



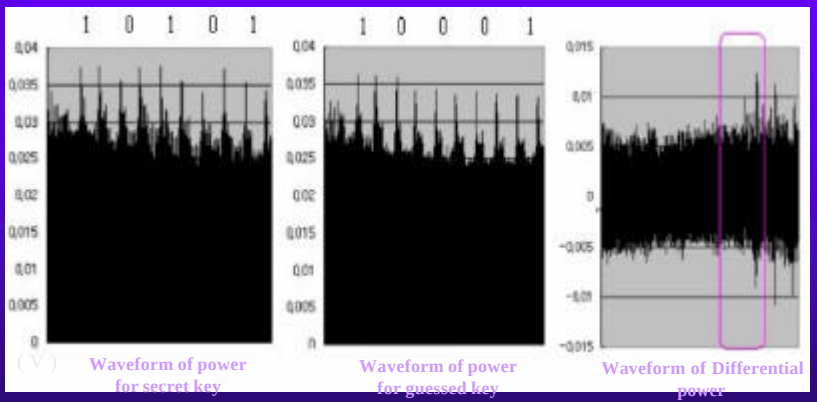
A D A D A D

LR binary scalar multiplication

❑ Power Analysis Attack: ECC

Our Power Attack - II

❍ DPA(Differential Power Attack)



Countermeasure

❍ To prevent SPA for ECC

- Independency of secret information and computational procedures

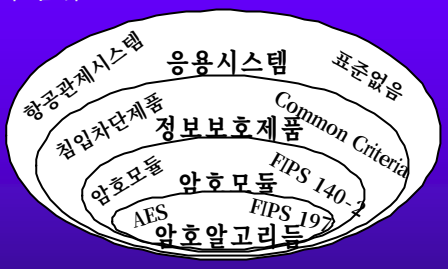
❍ To Prevent DPA for ECC($Q = kP$)

- **Randomize (blind) the secret key k, k' =k+r#E(K)**
- **Blind the Point P, P' = P+R**
- **Use Randomized projective coordinates**
- Randomize the computational trace

안전성 평가 기준 분석

1. 안전성평가기준 적용범위(1)

- 암호기술평가 범위



✓정보보호 응용시스템의 안전성 평가 범위

- 암호 알고리듬 < 암호모듈 < 정보보호제품 < 응용시스템
- 스마트 카드 Ì 정보보호 제품(Firewall, IDS, VPN, PKI-CA 등)

안전성 평가 기준 분석

1. 안전성평가기준 적용범위(2)

- CC, PP & ST의 관계

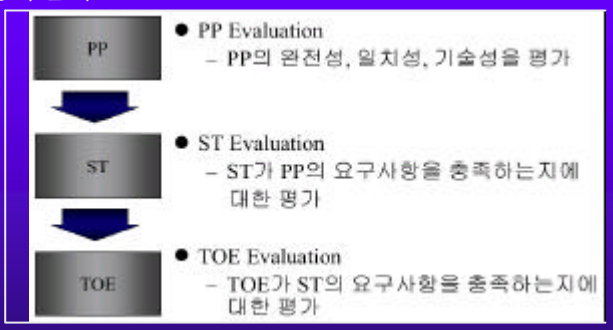
CC		PP		ST
✍ 국제표준 ✍ 보안제품에 중립적 ✍ 보안기술의 전체관점에서의 안전성평가 기준	작성시 참조 →	✍ 개발업체 또는 시용자 그룹에서 작성 ✍ CC를 특정 제품에 맞게 해석하여 작성	작성시 참조 →	✍ 개발업체 또는 사용자 그룹에서 작성 ✍ 안전성 평가 신청 시 제출

✓ CC(Common Criterian): 정보보호제품 전반에 대한 평가 기준서
✓ PP(Protection Profile) 보호프로파일
✓ ST(Security Target) 보안목표명세서
} 개별제품단위 (신청업체)

안전성 평가 기준 분석

1. 안전성평가기준 적용범위(3)

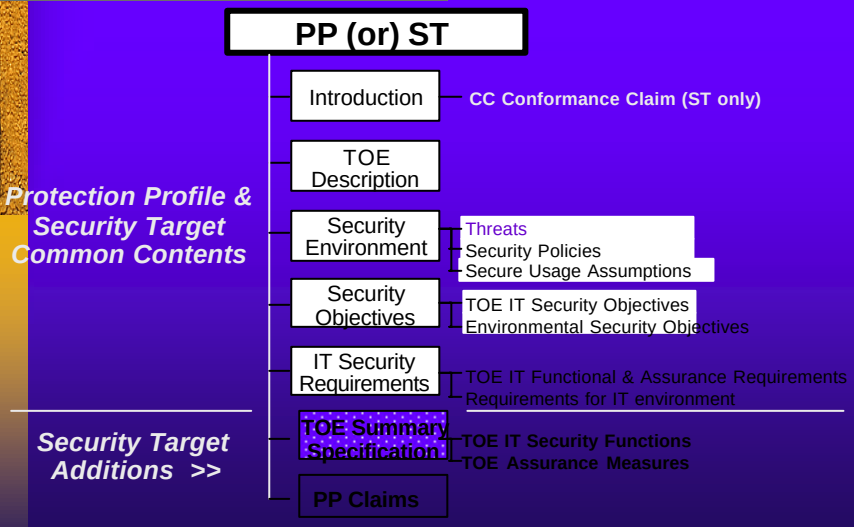
- CC의 평가단계



✓ 평가방법에 대한 자세한 사항은 CEM에서 기술

안전성 평가 기준 분석

1. 안전성평가기준 적용범위(4)



안전성 평가 기준 분석

2. DPA관련 안전성평가기준 분석결과(1)

- 암호 알고리듬에서 DPA관련 평가 분석
  - ✓미국
    - FIPS 197 AES(Rijndael) Specification
    - **Implementation attack (Specification) 기준**
      - ✓**Timing Attack, Power Analysis(SPA, DPA) 사례**
  - ✓ 유럽
    - NESSIE Project
    - 유럽연합의 원천기술 공모사업
    - 보안성 평가의 세부 요구사항
      - ✓ **Timing Attack, Power Analysis(SPA, DPA)**
  - ✓ 일본
    - CRYPTREC Project
    - 암호 알고리듬 7개 분야의 후보에 대한 평가 진행 중
    - 안전성 평가 라운드(TA, SPA, DPA 분석 중)

안전성 평가 기준 분석

2. DPA관련 안전성평가기준 분석결과(2)

- 암호모듈에서 DPA관련 평가 분석
  - ✓ 미국
    - FIPS140-2 (CMVP)
    - 보안성 요구조건 : 13개 부분
    - 전력분석, 시차공격, 오류주입, TEMPEST 등 항목 언급됨

      (13. Mitigation of other attacks)

      ➡ 구체적 평가방안 없음 (FIPS140-1에 없던 사항이 추가됨)

안전성 평가 기준 분석

2. DPA관련 안전성평가기준 분석결과(3)

- SCSUG-SCPP에서 DPA 공격 관련 위협

명칭	의미	설명
T.P_Probe (3.3.1.1 TOE에 대한 물리적 공격관련 위협)	Physical Probing of the IC (IC의 물리적 검사)	공격자가 설계정보와 동작 내용을 밝혀내기 위해 TOE에 대한 물리적 검사를 수행할 수 있다. IC failure analysis, IC reverse engineering 등의 기술을 이용
T.I_Leak (3.3.1.6 정보감시위협 들)	Information Leakage (정보누출)	공격자가 TOE의 정상적인 사용으로부터 누출된 TSF 데이터를 이용할 수 있다. 전력분석(power analysis)는 정보누출의 한 예가 될 수 있다.

안전성 평가 기준 분석

2. DPA관련 안전성평가기준 분석결과(4)

- SCSUG-SCPP에서 TOE 보안목적

명칭	의미	설명
O.I_Leak (4.1 TOE 보안목적)	Information Leakage (정보누출)	TOE는 전원, 접지, 클럭, 리셋 또는 I/O 선을 통하여 유용한 정보가 누출되지 않도록 TOE로부터 정보의 누출을 통제 및 제한하는 수단을 제공해야 한다. TOE는 전력소비와 같은 요소분석이 오퍼레이션 처리 정보누출과 안전한 정보에 손상을 입히지 않도록 설계되고 프로그램 되어야 한다.
O.Phys_Prot (4.1 TOE 보안목적)	Physical Protection (물리적 보호)	TOE는 물리적 공격에 저항 할 수 있어야 하고 또는 물리적 공격으로부터 유도된 정보를 이해하는데 어려움이 가해지도록 할 수 있어야 한다.

안전성 평가 기준 분석

2. DPA관련 안전성평가기준 분석결과(5)

- EUROSMART-CPP에서 DPA 공격 관련 위협

명칭	의미
T.Leak-inherent	Inherent Information Leakage (고유의 정보 누출)
T.Phys-Probing	Physical Probing (물리적 탐침)
T.Malfunction	Malfunction due to Environmental Stress (환경적 스트레스에 의한 장애)
T.Phys-Manipulation	Physical Manipulation (물리적 조작)
T.Leak-Forced	Forced Information Leakage (강제 정보 누출)

안전성 평가 기준 분석

2. DPA관련 안전성평가기준 분석결과(6)

- EUROSMART-CPP에서 TOE 보안목적

명칭	설명
O.TAMPER_ES	보안적 메커니즘은 기능적 요소, 생명주기나 암호키에 대한 보안 속성이나 비밀 등의 비인가적인 변경을 막아야 한다.
O.SIDE	임베디드 시스템(ES)는 TOE의 하드웨어 부분에서 전자적인 신호의 해석으로부터 안전하게 구현되어야 한다.
O.MOD_MEMORY	TOE는 비인가된 변형이나 손상으로부터 메모리의 중요한 정보가 안전해야 한다.

안전성 평가 기준 분석

2. DPA관련 안전성평가기준 분석결과(7)

- EUROSMART-CPP에서 TOE 보안기능요구사항

명칭	설명
FPR_UNO.1.1	TSF는 〔할당: 보호된 사용자나 주체〕에 의해 [할당: 사용자나 주체]가 〔할당: Objects〕에서 〔할당: 동작〕 동작을 관찰하지 못해야 한다. - Not Applicable
FPT_FLS.1.1	TSF는 다음의 사건[할당: TSF에서의 실패의 형태]에서 안전한 상태를 유지해야 한다. - Not management activity
FPT_PHP.3.1	TSF는 TSP가 위반하지 않도록 하기 위해 자동 대응함으로써 할당: TSF 장치/요소 목록〕에 대해 〔할당: 물리적인 대응하는 시나리오〕가 저항해야 한다. - Not Applicable

안전성 평가 기준 분석

2. DPA관련 안전성평가기준 분석결과(8)

- EUROSMART-CPP에서 TOE 보증요구사항

명칭	설명
AVA_VLA.4 - 매우 높은 내성(highly resistant)	TOE가 적의적인 환경에 놓일 수 있으므로 매우 높은 내성을 가져야 한다. 독립적인 취약성 공격이 매우 자세한 기술 정보를 바탕으로 하기 때문이다.

- ✓ EUROSMART-CPP(9806/9911) = EAL 4+ 평가등급 적용
- ✓ EUROSMART-CPP(0001) = EAL 5+ 평가등급 적용
  (독일, 전자서명법 요구)
- ✓ SCSUG-PP(v3.0) = EAL 4+ 평가등급 적용

안전성 평가 기준 제안

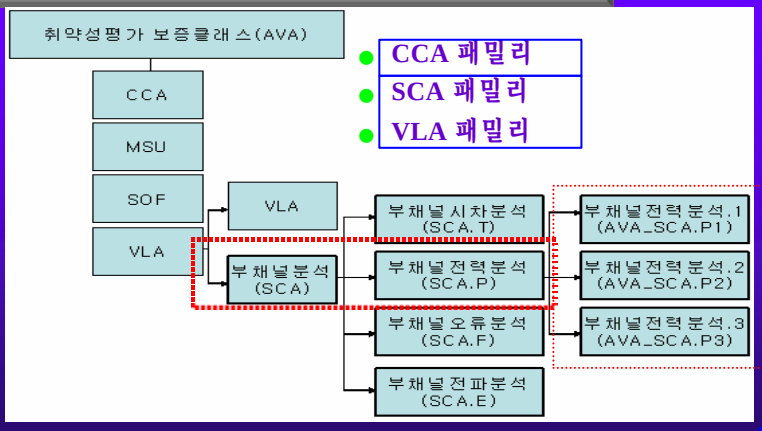
1. 제안 기준 고려 사항

- Covert Channel & Side Channel 정의
  (1) Covert Channel(비밀채널) : 개발자 고의적(의도적)/데이터 채널
  (2) Side Channel(부채널): Timing, Power, Fault-Insertion, EM등에 의한 비의도적/Non-Data 채널

- Side Channel Analysis 보증 패밀리 추가제안 근거
  (1) 일부 정보보호 제품 평가 시 부채널이 비밀채널보다 위협적
  ⇨ 부채널분석에 대한 취약성 평가 보증이 필요
  (2) CC V2.1 ⇨ CC V3.0 개정 추진 중(2003년도)
  - Power Analysis Attack ➔ 부채널 전력분석 보증 컴포넌트(SCA.P)
  - Timing Attack ➔ 부채널 시차분석 보증 컴포넌트(SCA.T)
  - Fault Attack ➔ 부채널 오류분석 보증 컴포넌트(SCA.F)
  - Electromagnetic Attack ➔ 부채널 전파분석 보증 컴포넌트(SCA.E)

안전성 평가 기준 제안

2. DPA관련 부채널분석 패밀리(AVA_SCA) 제안



안전성 평가 기준 제안

3. 수정 제안된 평가보증등급

보증클래스	보증패밀리	평가보증등급에 따른 보증 컴포넌트						
		EAL1	EAL2	EAL3	EAL4	EAL5	EAL6	EAL7
형상관리	ACM_AUT				1	1	2	2
	ACM_CAP	1	2	3	4	4	5	5
	ACM_SCP			1	2	3	3	3
배포 및 운영	ADO_DEL		1	1	2	2	2	3
	ADO_IGS	1	1	1	1	1	1	1
개발	ADV_FSP	1	1	1	2	3	3	4
	ADV_HLD		1	2	2	3	4	5
	ADV_IMP				1	2	3	3
	ADV_INT					1	2	3
	ADV_LLD				1	1	2	2
	ADV_RCR	1	1	1	1	2	2	3
	ADV_SPM				1	3	3	3
설명서	AGD_ADM	1	1	1	1	1	1	1
	AGD_USR	1	1	1	1	1	1	1
생명주기지원	ALC_DVS			1	1	1	2	2
	ALC_FLR							
	ALC_LCD				1	2	2	3
	ALC_TAT				1	2	3	3
시험	ATE_COV		1	2	2	2	3	3
	ATE_DPT			1	1	2	2	3
	ATE_FUN		1	1	1	1	2	2
	ATE_IND	1	2	2	2	2	2	3
취약성 평가	AVA_CCA					1	2	2
	AVA_MSU			1	2	2	3	3
	AVA_SOF		1	1	1	1	1	1
	AVA_VLA		1	1	2	3	4	4
	AVA_SCA.P [4]		***1***	***1***	***2***	***2***	***2***	***2***

안전성 평가 기준 제안

4. 제안된 보안 목적과 관련된 보증요구사항

보증요구사항		관련된 보안목적
컴포넌트	컴포넌트 이름	
ADV_IMP.1	Subset of the implementation of the TSF	O.Phy_Prot
AVA_VLA.3	Moderately resistant	O.Env_Strs, O.Phys_prot
AVA_SCA.P2	체계적인 부채널전력공격 분석 (Systematic side-channel power analysis)	O.Flt_Ins, O.I_Leak

안전성 평가 기준 제안

5. 제안된 부채널전력분석 관련 보증 컴포넌트

보증 클래스	보증 패밀리	보증컴포넌트	목적	응용시 주의사항	PA[21]
취약성 평가	AVA_SCA.P	AVA_SCA.P1 (Power Analysis Attack)	전력분석관련 부채널에 대한 비정형화된 조사를 통하여 식별가능한 전력분석관련 부채널을 식별함.	-	- Basic SPA - Basic DPA
		AVA_SCA.P2 (Systematic PAA)	전력분석관련 부채널에 대한 체계적인 조사를 통하여 식별 가능한 전력분석관련 부채널을 식별함.	전력분석관련 부채널을 체계적으로 분석하는 것은 개발자가 전력분석관련 부채널을 임시적인 방식으로 식별하는 것이 아니라 구조적이고 반복 가능한 방법으로 식별할 것을 요구함	- Advanced SPA - Advanced DPA
		AVA_SCA.P3(Exhaustive PAA)	전력분석관련 부채널에 대한 철저한 조사를 통하여 식별 가능한 전력분석관련 부채널을 식별함.	철저한 방식의 전력분석관련 부채널분석은 부채널식별에 사용된 계획이 부채널조사를 위해 가능한 모든 방법이 이용되었음을 보증하기에 충분하다는 추가적인 증거를 제공하도록 요구함	- Exhaustive SPA/DPA

안전성 평가 기준 제안

6. 평가 기준 고려 사항

- 3개 보증 등급화 비교
  - P1 등급 - PAA(AVA_SCA.P1): 비정형화된 기본 DPA 공격
  - P2 등급 - Systematic PAA: 정형화된 공격, 설계회로도&소스코드 제공
    - ✓ 인적구성 - 유사시스템의 사용/분석 경험이 풍부한 전문가로 구성,
    - ✓ 문서측면 - 규격화된 명시적인 시험절차서 제공,
    - ✓ 장비측면 - 성능이 우수한 다양한 측정장비를 갖추며,
    - ✓ 데이터측면 - 유사장비 시험데이터 등 충분한 데이터 제공
  - P3 등급 - Exhaustive PAA: Exhaustive Key-search attack 등가
- 추후: 평가기준 상세화 – 시험절차서 요구
  - 알고리듬/실험횟수
  - 공격 방법

결 론

결론 및 향후 연구

- 스마트카드 부채널 공격 실험: DES, RSA-MESD, ECC-DPA
- DPA 공격에 대한 안전성 평가 항목 분석 및 제안
  - 암호 알고리즘/암호모듈/정보보호제품 모두 적용(부채널공격)
  - 암호 알고리즘: AES/NESSIE/CRYPTREC 과제 평가내용 분석
  - 암호 모듈: CMVP(FIPS 140-1,2) 항목 분석
  - 스마트카드 보호프로파일: SCSUG-SCPP/EUROSMART-PP 분석
- 부채널 공격에 대한 안전성 평가기준 제안 (AVA_SCA.P1 ~.P3)
- 향후 연구방향
  - 스마트카드 DPA관련 시험평가절차/기준서 연구
    (DPA 기술검사기준서 등)