



(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2017-0003494
(43) 공개일자 2017년01월09일

(51) 국제특허분류(Int. Cl.)
G06F 21/53 (2013.01) G06F 21/55 (2013.01)
H04M 1/02 (2006.01)
(52) CPC특허분류
G06F 21/53 (2013.01)
G06F 21/55 (2013.01)
(21) 출원번호 10-2016-0175040
(22) 출원일자 2016년12월20일
심사청구일자 없음

(71) 출원인
안나영
서울특별시 동대문구 제기로6길 9-13, 2층 (제기
동)
(72) 발명자
안나영
서울특별시 동대문구 제기로6길 9-13, 2층 (제기
동)

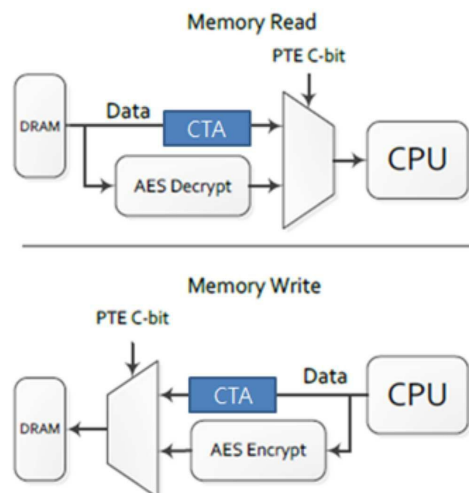
전체 청구항 수 : 총 1 항

(54) 발명의 명칭 부채널 공격에 대한 방어대책을 갖는 모바일 장치

(57) 요약

본 발명의 실시 예에 따른 모바일 장치는, 캐시 라인들; 상기 캐시 라인들 중 어느 하나의 데이터를 전송하는 TEE(trusted execution environment) 데이터 패스; 및 상기 캐시 라인들 중 어느 하나의 데이터를 전송하는 REE(rich execution environment) 데이터 패스를 포함하고, 상기 REE 데이터 패스는 타이밍 공격 방지 회로를 포함할 수 있다.

대표도 - 도7



(52) CPC특허분류

H04M 1/0202 (2013.01)

명세서

청구범위

청구항 1

캐시 라인들;

상기 캐시 라인들 중 어느 하나의 데이터를 전송하는 TEE(trusted execution environment) 데이터 패스; 및

상기 캐시 라인들 중 어느 하나의 데이터를 전송하는 REE(rich execution environment) 데이터 패스를 포함하고,

상기 REE 데이터 패스는 타이밍 공격 방지 회로를 포함하는 모바일 장치.

발명의 설명

기술 분야

[0001] 본 발명은 부채널 공격에 대한 방어대책을 갖는 모바일 장치에 관한 것이다.

배경 기술

[0002] ARM 사에서는 Cortex™-A부터 TrustZone이라고 하는 TEE(Trusted Execution Environment)를 제공하고 있다. TrustZone 기술은 모바일 결제, DRM 그리고 Web OS와 같이 정보 보호가 중요한 어플리케이션이 안전하게 실행될 수 있도록 시스템 및 하드웨어적인 환경을 제공하는 것이 목표이다. 기본적으로 ARM 칩에 TrustZone이 포팅되어 별도의 HW 모듈의 추가 없이 하드웨어 기반의 TEE 환경을 제공할 수 있다. 도 1은 트러스트존을 갖는 모바일 장치를 예시적으로 보여주는 도면이다. 단일 프로세서 상에서 가상화(virtualization)를 통해서 시스템 리소스를 Normal World와 Secure World 두 개의 모드로 분리된다. Monitor Mode는 Secure World에서 동작하는 프로세서로 현재의 Context를 결정하는 역할을 한다. AMBA(Advanced Microcontroller Bus Architecture) 3AXI™ bus라고 하는 하드웨어 로직은 Normal Mode의 컴포넌트가 Secure World의 리소스에 접근하지 못하도록 차단한다. 이를 통해서 DRM이나 결제와 같은 보안과 직결되는 중요한 프로그램의 실행과 일반적인 어플리케이션의 실행을 분리할 수 있다. Secure World의 어플리케이션은 Normal World의 resource에 대한 접근이 가능하지만 Normal World의 어플리케이션은 Secure World의 리소스를 사용할 수 없도록 설계된다.

발명의 내용

해결하려는 과제

[0003] 본 발명의 목적은 부채널 공격으로부터 안전한 모바일 장치를 제공하는 데 있다.

과제의 해결 수단

[0004] 본 발명의 실시 예에 따른 모바일 장치는, 캐시 라인들; 상기 캐시 라인들 중 어느 하나의 데이터를 전송하는 TEE(trusted execution environment) 데이터 패스; 및 상기 캐시 라인들 중 어느 하나의 데이터를 전송하는 REE(rich execution environment) 데이터 패스를 포함하고, 상기 REE 데이터 패스는 타이밍 공격 방지 회로를 포함할 수 있다.

발명의 효과

[0005] 본 발명의 실시 예에 따른 모바일 장치는 제로 캐시 경쟁 혹은 데이터 레이턴시를 일정하게 하는 TEE 및 REE 환경을 구비함으로써, 부채널 공격을 방지하거나 줄일 수 있다.

도면의 간단한 설명

[0006] 도 1은 일반적인 트러스트존(TrustZone)을 구비하는 모바일 장치를 예시적으로 보여주는 도면이다.

도 2는 AMD의 공유 DRAM을 예시적으로 설명하는 도면이다.

도 3은 TruSpy 위협 모델을 예시적으로 보여주는 도면이다.

도 4는 TruSpy 공격의 흐름을 보여주는 도면이다.

도 5는 본 발명의 실시 예에 따른 TEE 및 REE의 분리된 하드웨어 캐시들을 예시적으로 보여주는 도면이다.

도 6은 본 발명의 실시 예에 따른 EE 및 REE 상에서 분리된 캐시 정책을 예시적으로 보여주는 도면이다.

도 7은 본 발명의 실시 예에 따른 REE 데이터 패스에 CTA(타이밍 공격 방지회로)를 보여주는 도면이다.

도 8은 본 발명의 실시 예에 따른 TEE 데이터 패스에서 암호 회로들을 예시적으로 보여주는 도면이다.

발명을 실시하기 위한 구체적인 내용

- [0007] 아래에서는 도면들을 이용하여 본 발명의 기술 분야에서 통상의 지식을 가진 자가 용이하게 실시할 수 있을 정도로 본 발명의 내용을 명확하고 상세하게 기재할 것이다.
- [0008] 도 1은 일반적인 트러스트존(TrustZone)을 구비하는 모바일 장치를 예시적으로 보여주는 도면이다. Software 측면에서 TrustZone을 이용하는 OS 또한 연동이 되어야 TrustZone HW를 이용할 수 있다. 아래의 그림은 ARM사에서 제안하는 소프트웨어 아키텍처의 사용 예이다. 그림에서 볼 수 있는 것처럼, Normal World의 OS외에 별도로 가상화된 Secure World에서 동작하는 OS를 구성한다. Monitor Driver의 역할은 두 가상 프로세서간의 Context를 관리하는 것이다. Monitor Driver는 TrustZone driver의 Secure Monitor Call(SMC) 혹은 각 디바이스의 HW 예외 처리 요청에 의해서 동작한다. 두 모드 간의 Context를 관리하는 Monitor 모드는 안전하게 보호되어야 하기 때문에 Secure World에서 실행되어야 한다.
- [0009] TEE 환경은 기본적으로 3종류의 하드웨어 모델로 구성되고 있다. 1) REE와 TEE 하드웨어를 분리하는 구조, 2) REE와 TEE 하드웨어를 하나의 칩으로 구현하는 구조, 및 3) 하나의 하드웨어를 REE와 TEE가 공유하는 구조이다.
- [0010] 도 2는 AMD의 공유 DRAM을 예시적으로 설명하는 도면이다. AMD의 TrustZone는 하드웨어 공유 구조로 구현되며, REE/TEE에 대한 데이터 접근은 암호비트 C-bit에 의해 결정된다. 특히, REE/TEE는 메인 메모리(main memory), 예를 들어 DRAM을 공유하고 있다. 다른 말로, DRAM은 REE/TEE에 의해 공유된 메모리(shared memory)이다. C-bit의 값에 따라 DRAM의 nonsecure 영역에 접근할지, secure 영역에 접근할 지가 결정된다. 여기서 secure 영역은 암호 알고리즘 (예를 들어, AES)에 의해 암호화된 데이터가 저장되는 영역이다.
- [0011] 최근에 ARM의 Shared Memory에 대한 부채널 공격이 소개되었다. 이 발명에서는 이 부채널 공격의 명칭을 TruSpy로 언급되고 있다.
- [0012] 도 3은 TruSpy 위협 모델을 예시적으로 보여주는 도면이다. TruSpy 공격은 기본적으로 Normal World와 Secure World 사이의 캐시 경쟁(cache contention)의 취약점에 대한 부채널 공격을 수행함으로써, Secure World의 민감한 정보를 탈취하는 것을 목표로 한다. 우선적으로 위협 모델링은 TEE의 특정 어플리케이션과 OS를 장악하고 있고, REE의 OPENSSL을 통하여 유효 정보를 탈취하는 것으로 표현된다. 공격자는 통상적인 Prime 및 Probe 기술을 이용하여 부채널 공격을 감행한다. 이러한 TruSpy 공격의 성공을 위하여 2 가지 조건들이 요구된다.
- [0013] 첫째로, 공격자는 공유된 메모리, 즉 모든 캐시 라인들을 채울 수 있다.
- [0014] 둘째로, 공격자는 캐시 라인의 상태 변화를 감지할 수 있다. 예를 들어, 캐시 라인의 상태 변화는, 굉장히 정밀한 타이머를 통하여 특수한 메모리 어드레스가 레지스터까지 로드되는 데 걸린 시간을 측정함으로써 상태 변화를 감지할 수 있다.
- [0015] 도 4는 TruSpy 공격의 흐름을 보여주는 도면이다. 도 4를 참조하면, TruSpy 공격의 워크 플로우는 다음과 같은 5 단계로 진행된다.
- [0016] 제 1 단계: 캐시 프라이밍(cache priming)을 위해 사용될 메모리를 식별한다. 이 단계는 가상 어드레스를 캐시 셋들에 맵핑함으로써 완성된다.
- [0017] 제 2 단계: 캐시들을 채우는 것이다. Spy 과정은 메모리의 모든 캐시들을 채울 것이다.
- [0018] 제 3 단계: Secure World의 victim process를 실행하는 것이다. Victim process가 실행되면, 공격자에 의해 이전에 점유되었던 캐시 라인들이 DRAM으로부터 쫓겨날 것이다.

- [0019] 제 4 단계: secure world의 victim process가 완료된 후 캐시 구조의 변화를 측정하는 것이다. 제 2 단계에서 이전에 primed 되는 각 캐시 라인에 대하여, 메모리 로드 인스트럭션을 실행하는 시간이 측정된다. 만일 메모리로부터 레지스터로 로드되는 시간이 짧다면, 메모리 캐시 셋은 victim process에 의해 실행된 값이 아니다. 이때, 제 2 단계로 되돌아간다. 반면에 시간이 길다면, 메모리 캐시 셋은 victim process에 의해 실행된 값이다. 이러한 부채널 공격을 통하여, secure world의 민감한 정보를 탈취 및 수집된다.
- [0020] 제 5 단계: 수집된 정보를 분석하여 비밀 정보를 구한다. 여기서 비밀 정보는 보안 도메인이 암호 키들일 수 있다.
- [0021] 본 발명에서 제안하는 TruSpy 부채널 공격에 대한 보안 대책은 크게 두 가지로 정리된다. 하나는 공유 메모리에 대한 캐시 경쟁을 없애거나 완화시키는 것이고, 다른 하나는 캐시 변경을 검출할 수 없도록 타이밍을 조절하는 것이다.
- [0022] **공유 메모리에 대한 제로 경쟁**
- [0023] TruSpy 공격은 기본적인 모델링은, REE와 TEE 사이에서 공유된 캐시 라인에 대한 경쟁에서 비롯된다. 따라서, REE와 TEE의 사이의 캐시 라인 사이의 경쟁을 없애면, TruSpy의 공격 방법을 원천적으로 차단시킬 수 있다.
- [0024] 도 5는 본 발명의 실시 예에 따른 TEE 및 REE의 분리된 하드웨어 캐시들을 예시적으로 보여주는 도면이다. 실시 예에 있어서, 캐시 라인 경쟁을 없애거나 줄이기 위해, 공유 메모리의 캐시 라인들에 대하여, REE 환경의 캐시 라인과 TEE 환경의 캐시 라인은 정책적으로 고정시킬 수 있다. 예를 들어, 제로 경쟁하도록, 고정된 REE용 캐시 라인과 고정된 TEE용 캐시 라인을 갖는 메모리 구조가 하드웨어적으로 설계될 수 있다.
- [0025] 도 6은 본 발명의 실시 예에 따른 EE 및 REE 상에서 분리된 캐시 정책을 예시적으로 보여주는 도면이다.
- [0026] 다른 실시 예에 있어서, 소프트웨어적으로 캐시 정책에 REE 가상 어드레스와 TEE 가상 어드레스를 고정적으로 할당시킬 수 있다. 이 외에 다양한 방법에 의해 캐시 라인들이 제로 경쟁하도록 공유 메모리를 구현하거나 어드레스를 할당할 수 있다.
- [0027] **타이밍 공격 방지**
- [0028] TruSpy는 캐시 라인의 변화를 감지함으로써, 부채널 공격을 수행한다. 특히 캐시 라인 변화는, 메모리에서 레지스터로 로드되는 시간의 변화를 측정함으로써, 캐시 라인 변화를 감지하려 시도한다. 따라서 이러한 타이밍 부채널 공격을 방지하기 위하여, Secure World와 Normal World 사이의 로드 시간에 큰 차이가 없도록 할 수 있다.
- [0029] **REE 데이터 패스 지연**
- [0030] 일반적으로, AMD의 TrustZone 기술은 C-비트를 근거로 하여, REE 환경인지 TEE 환경인 지를 결정한다. TEE 환경의 데이터 패스는 암호 알고리즘 함수를 경유하기 때문에 필연적으로 REE 환경의 데이터 패스보다 지연 시간을 더 갖는다. 공격자는 이러한 지연 시간을 이용하여 타이밍 부채널 공격을 수행한다. 따라서, 이러한 부채널 공격 방지를 위하여 REE 환경이든, TEE 환경이든 데이터 패스의 지연 시간이 유사하게 설정되도록 다음과 같이 구현한다.
- [0031] 도 7은 본 발명의 실시 예에 따른 REE 데이터 패스에 CTA(타이밍 공격 방지회로)를 보여주는 도면이다. 여기서 CTA는 REE 데이터 패스와 TEE 데이터 패스 사이의 지연 시간을 동일하도록 만드는 지연 회로(delay circuit, 예, flip-flop 구성 가능)로 구현될 수 있다.
- [0032] **TEE 병렬 데이터 패스**
- [0033] 한편, REE 환경에서 데이터 패스에 대한 시간 지연이 성능에 영향을 줄 수 있다. 이러한 문제를 해결하기 위해 TEE 데이터 패스가 병렬화될 수 있다. 예를 들어, 병렬 암호 회로 구현함으로써, REE 데이터 패스와 TEE 데이터 패스 사이의 지연 시간 차이를 감추도록 구현할 수 있다.
- [0034] 도 8은 본 발명의 실시 예에 따른 TEE 데이터 패스에서 암호 회로들을 예시적으로 보여주는 도면이다. 도 8을 참조하면, 4개의 암호 회로를 사용하였지만, 병렬 연결된 암호 회로의 개수가 여기에 제한되지 않을 것이다.
- [0035] 본 발명에서는, TrustZone에서 TruSpy 공격을 원천적으로 차단하기 위하여, 캐시 라인의 REE와 TEE 사이의 경쟁을 없애는 메모리 구조 및 캐시 정책을 제안한다. 또한, TruSpy에 의해 타이밍 부채널 공격을 방지하기 위하여, REE의 데이터 패스와 TEE의 데이터 패스에 대한 지연 시간을 유사하게 할 것을 제안한다. 발명에서 제안하는 TruSpy 부채널 공격에 대한 보안 대책은 크게 두 가지로 정리된다. 하나는 공유 메모리에 대한 캐시 경쟁을 없

애거나 완화시키는 것이고, 다른 하나는 캐시 변경을 검출할 수 없도록 타이밍을 조절하는 것이다.

[0036]

한편, 상술 된 본 발명의 내용은 발명을 실시하기 위한 구체적인 실시 예들에 불과하다. 본 발명은 구체적이고 실제로 이용할 수 있는 수단 자체뿐 아니라, 장치 기술로 활용할 수 있는 추상적이고 개념적인 아이디어인 기술적 사상을 포함할 것이다.

부호의 설명

[0037]

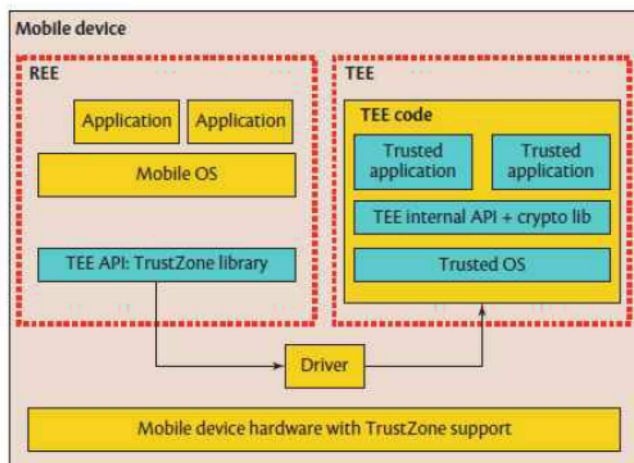
TEE: trusted execution environment

REE: rich execution environment

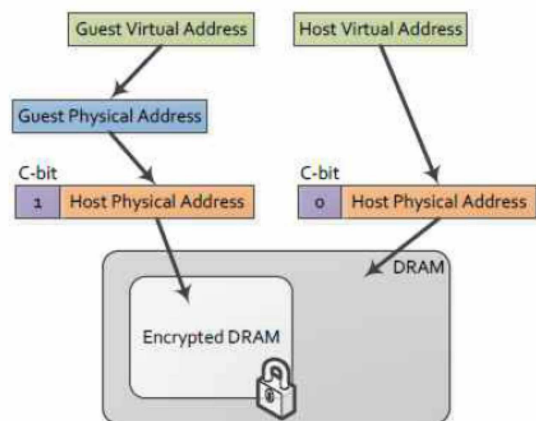
CTA: 타이밍 공격 방지회로

도면

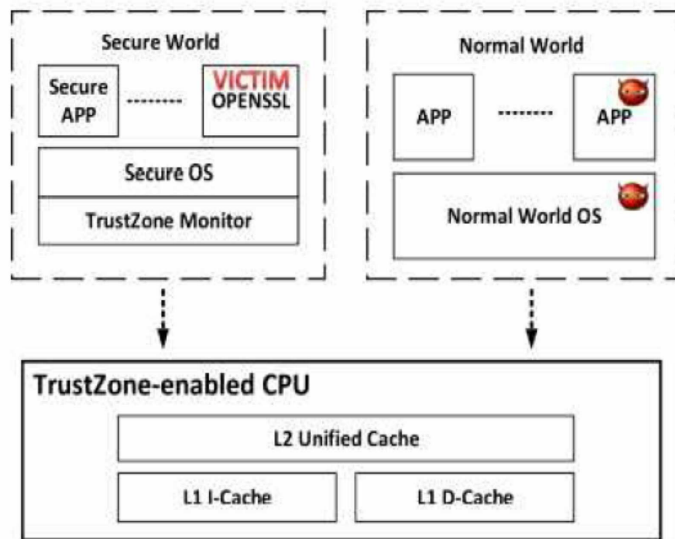
도면1



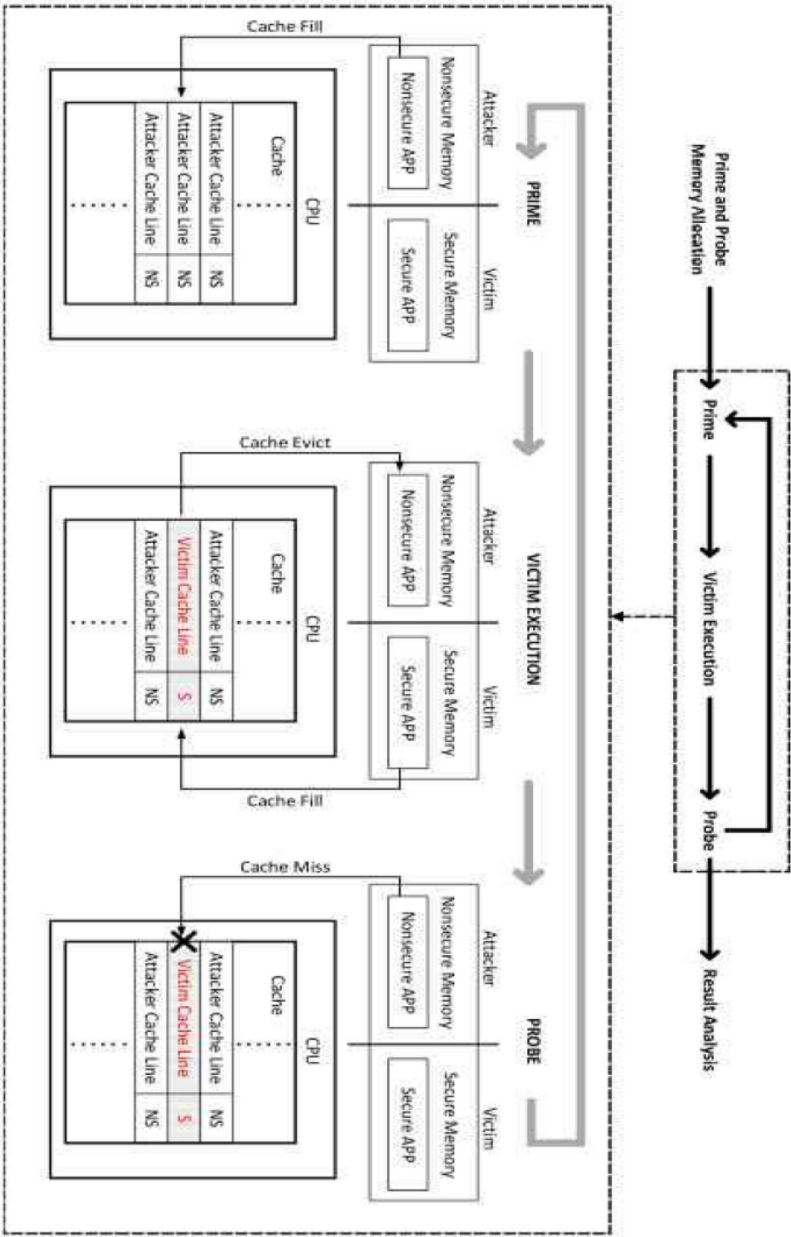
도면2



도면3



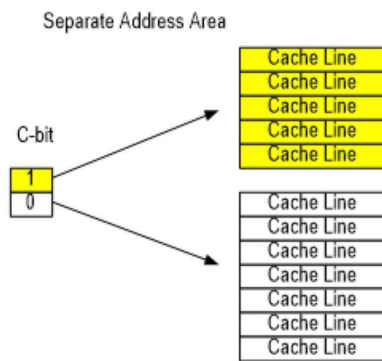
도면4



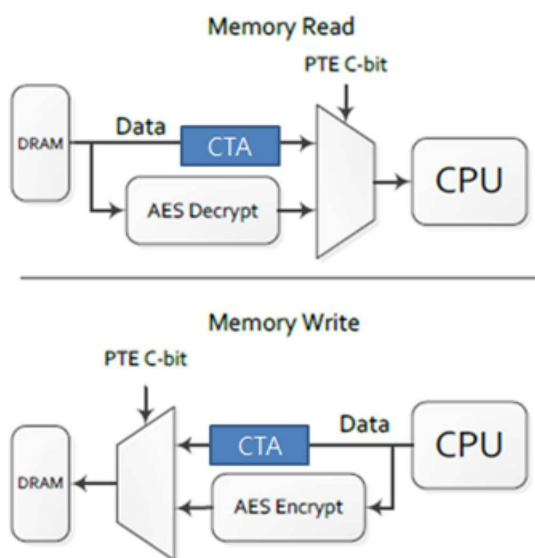
도면5

Cache Line	1	TEE only
Cache Line	1	
Cache Line	1	
Cache Line	1	
Cache Line	1	
Cache Line	0	REE only
Cache Line	0	
Cache Line	0	
Cache Line	0	
Cache Line	0	
Cache Line	0	
Cache Line	0	

도면6



도면7



도면8

