



Masking



https://www.youtube.com/watch?v=ddDQ8Q_OzFw&t=2s

Table of Contents

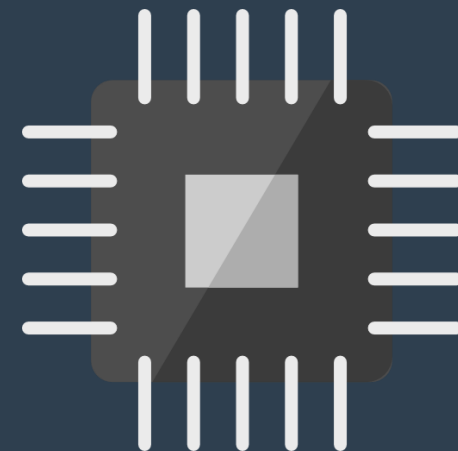
- ▶ 01 부채널분석(전력)
- ▶ 02 마스킹 기법
- ▶ 03 고차 마스킹 연구
- ▶ 04 마스킹 변환 연구
- ▶ 05 축소 마스킹 연구

Masking

PART 1

부채널분석
(전력)

부채널 분석이란?

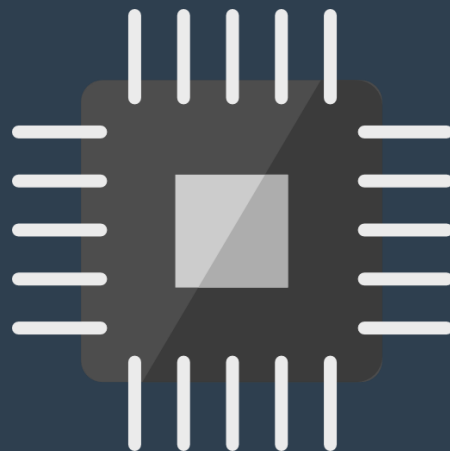


암호 장치에서 발생하는 물리 신호 분석!

SOUND



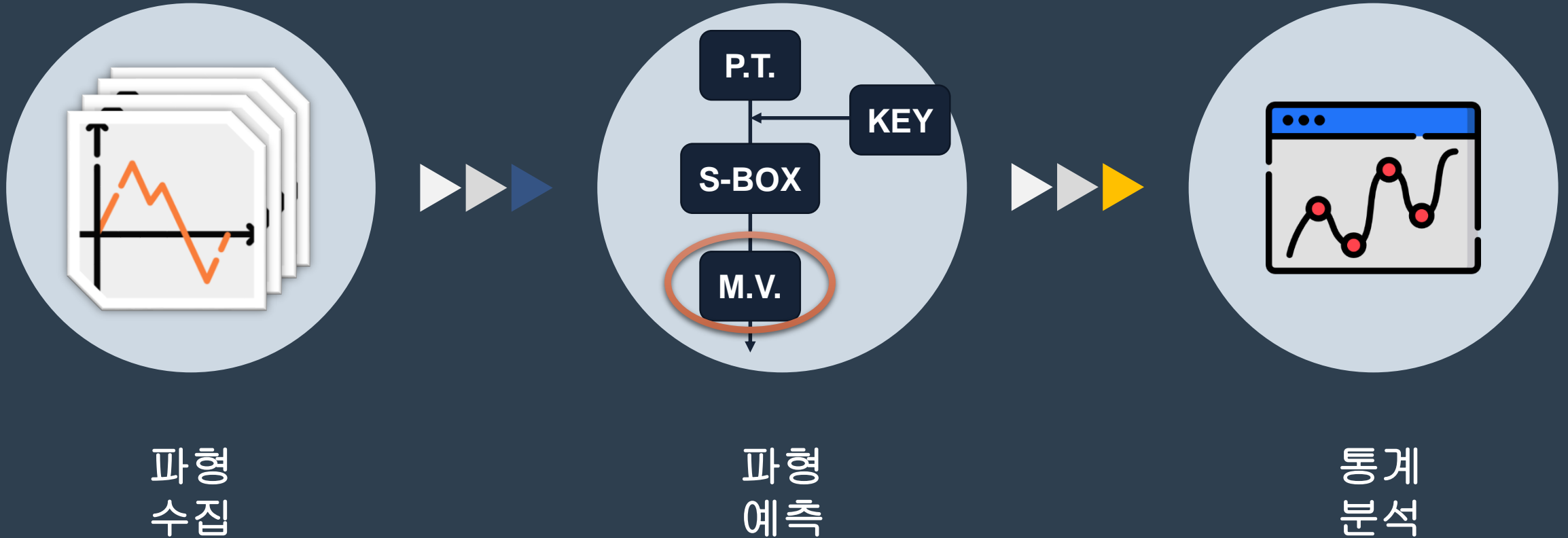
POWER
Consumption



TIME
Elapsed



전력 분석(통계적 전력 분석) ⚡

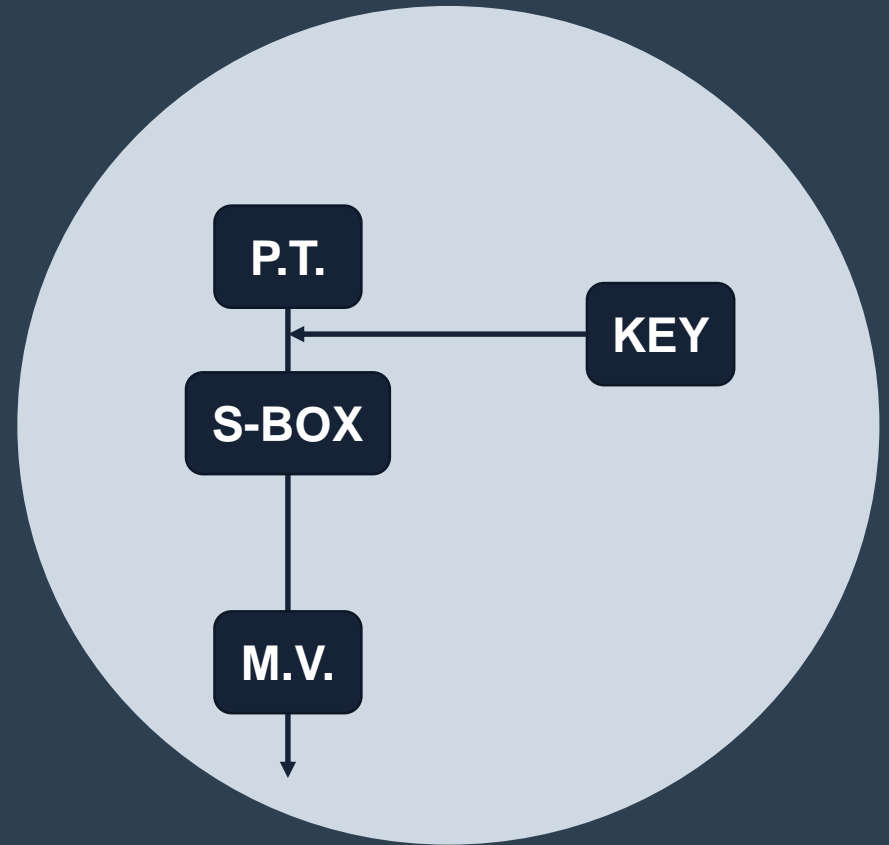


Masking

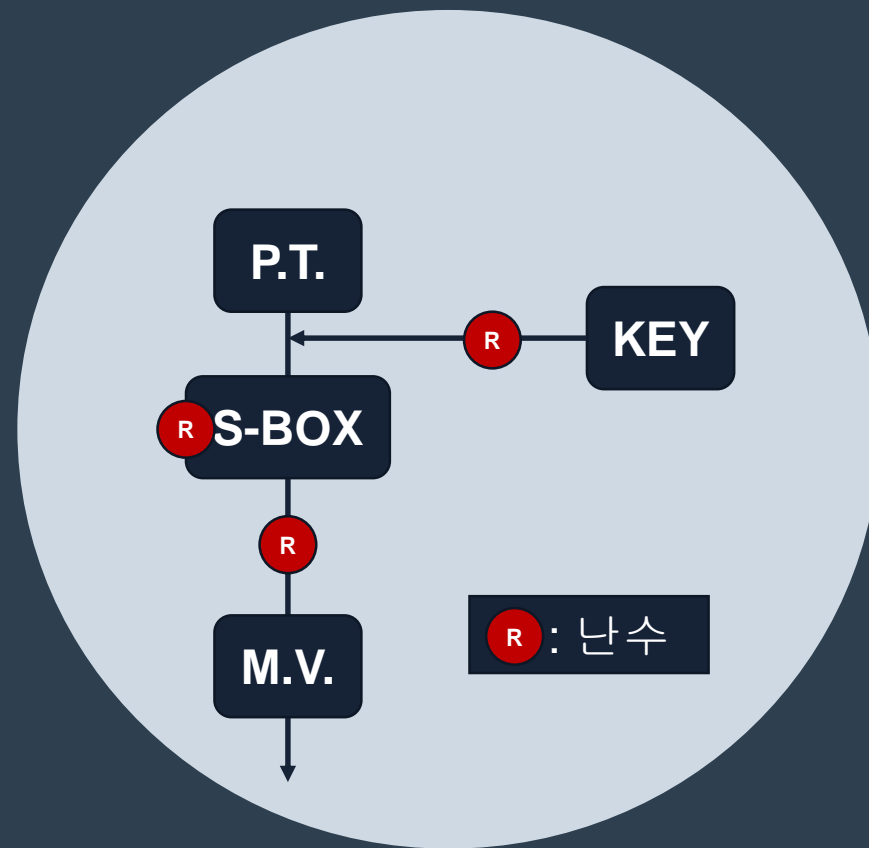
PART 2

마스킹 기법

마스킹 기법이란?



중간값에 난수를
더해 예측 방지!



Masking

PART 3

고차 마스킹

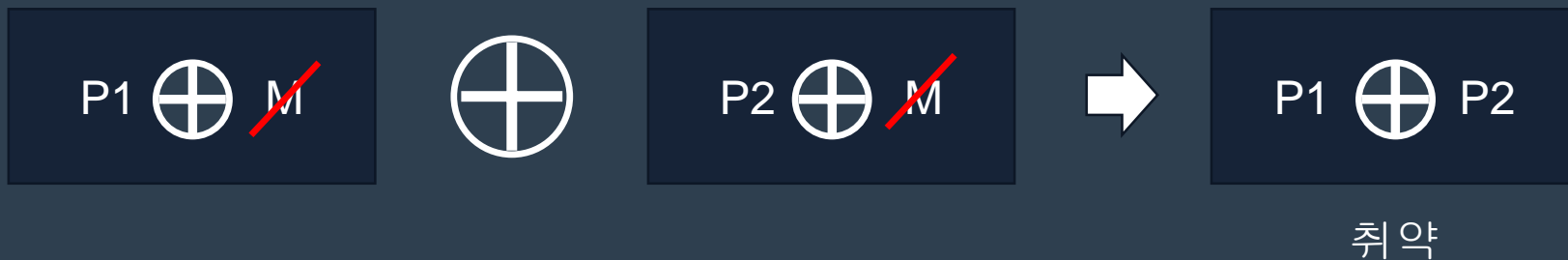
마 스 킹 파 휘 법

마스킹 기본

$$: P \oplus M$$



따라서, 다음의
취약점이 존재 -> 고차 전력 분석



대응 기법으로, 여러 난수를
적용하는 고차 마스킹이 연구됨



안전

하지만 상관관계를 완전히
지우는 것은 불가능

고차마스킹 고려사항

속도

공간

난수

저전력 환경을 고려한 관점으로 연구가 진행 중

최근에는 AES에 대한마스킹으로

고차마스킹 확장 가능성, 빠른 속도, 적은 공간, 안전한 난수를 발생하는 기법 발표

Masking

PART 4

마스킹 변환

마 스 킹 변 환 이 란 ?

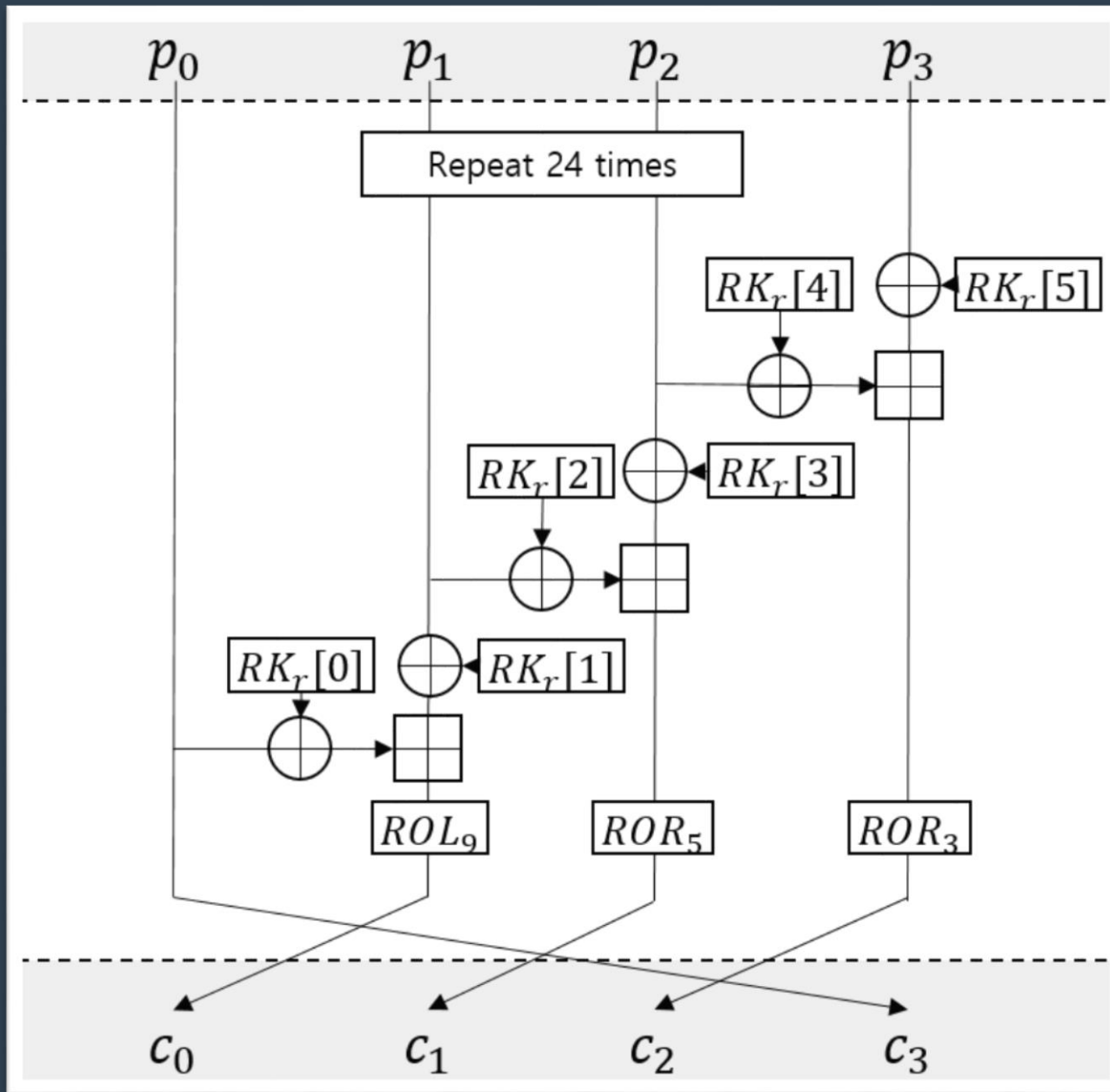
저 전력 에 적 합 한 A R X 구 조

A d i t i o n - - - - - - - - - - → 산 술

R o t a t i o n , **X** O R - - - - - - - - - - → 불

산술(Arithmetic) 마스크	불(Boolean) 마스크
$X + r, X - r \pmod{N}$	$X \oplus R$

상 이 한 마스크 방식을 가 짐



불 마스크 된 p

~~산술 연산 $F(p)$~~

불 \rightarrow 산술 변환
($p \rightarrow p'$)

산술 연산 $F(p')$

$$X + r \leftrightarrow X \oplus r$$

마 스 킹 변 환 !

→ A t o B

← B t o A

마스킹 변환 고려 사항

속도

공간

난수

저전력 환경을 고려한 관점으로 연구가 진행 중

최근에는 LEA에 적용할 마스킹 변환 기법으로

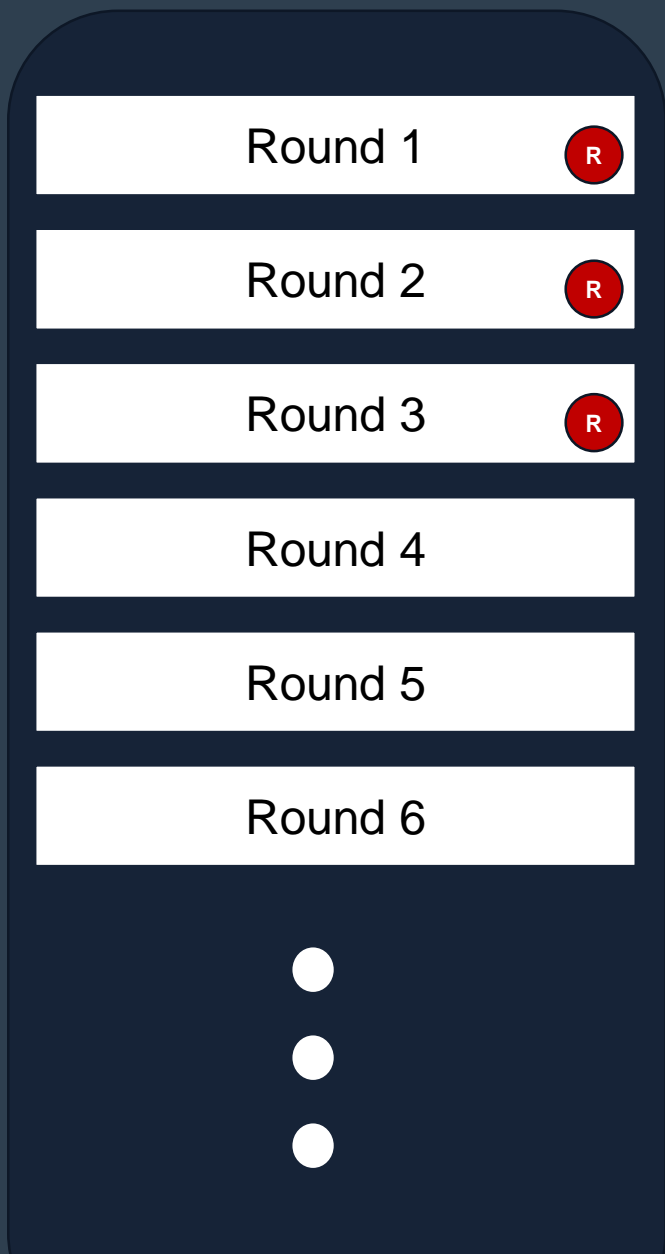
적은 메모리를 요구하면서도 빠른 연산량을 가지는 기법이 발표됨

Masking

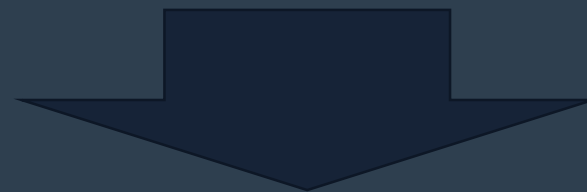
PART 5

축소 마스킹

축 소 마 스 킹 이 란 ?



일부 라운드에만
마스킹을 하는 기법



마스킹 비용 최소화

첫, 마지막 라운드에 마스크
(평문으로부터, 암호문으로부터의
중간값 예측을 차단)

축 소 마 스 킹 공 격

마 스 킹 되 지 않 은 라 운 드 의 입 력 의
해 밍 웨 이 트 획 득
(해 밍 웨 이 트 필 터 링)

→ 통 계 전 력 분 석

축소마스킹 고려사항



속도



공간



난수

최근에는 **SIMON** 알고리즘을 대상으로
10라운드까지의 축소마스킹에 대한 취약점이 존재함이 발표되었다.

결론

마스킹기법은 상당한 비용이 존재하며 다양한 기법을 가진다.

따라서 부채널분석의 타겟이 될 저전력 장치들에 효율적인 적용을 고려해야 한다.

의도에 따라 적절한 차수로 마스킹을 해야 할 것이다.

시간과 공간, 난수를 고려하여 기존의 마스킹기법의 효율성을 높이는 것이 필요하다.

T h a n k Y o u !