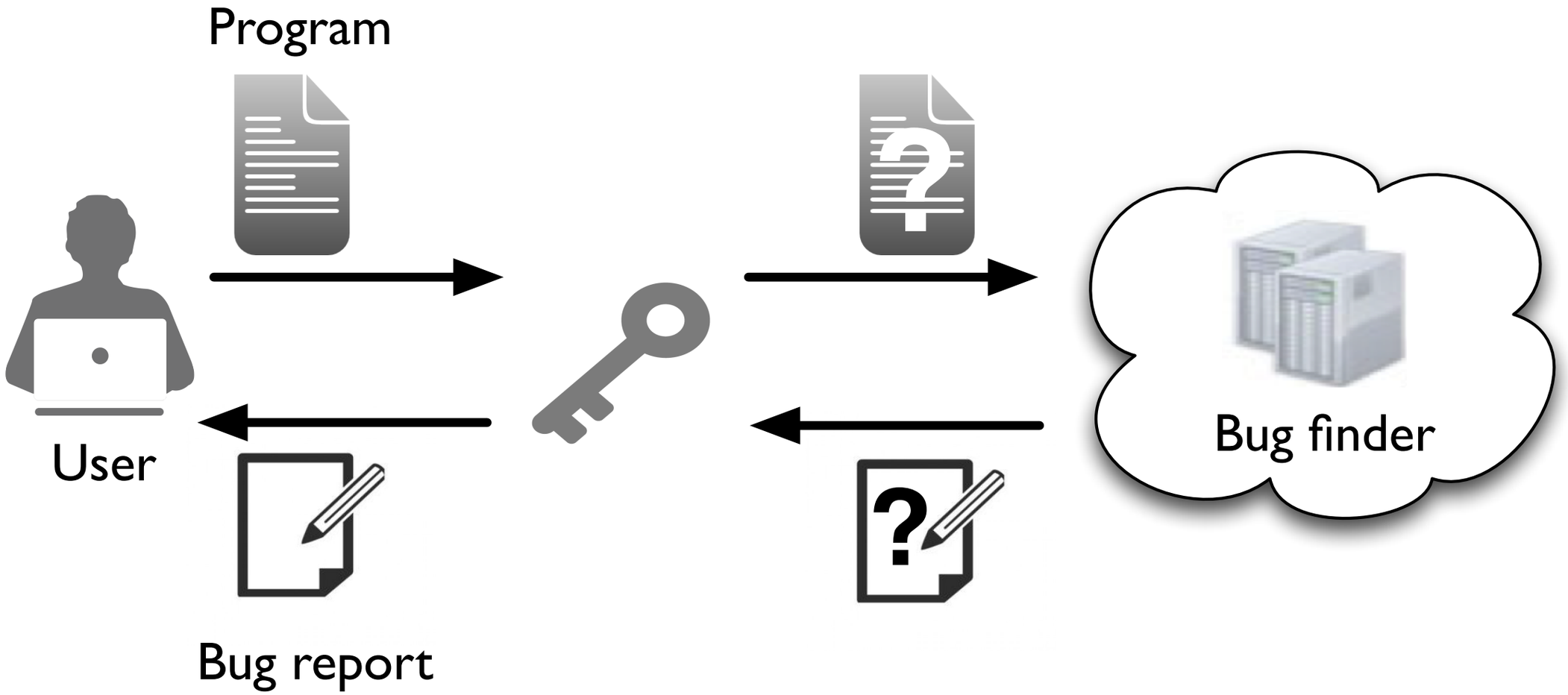
비밀 프로그램 정적분석

[1]이우석, [2]홍현숙, [2]천정희, [1]이광근

[1]서울대학교 컴퓨터공학부 프로그래밍 연구실

[2]서울대학교 수리과학부 암호학적 난제 연구단

비밀 분석



응용

- 견고한 앱스토어 리뷰 시스템
  - 예 : 애플 앱스토어, 삼성앱스
- 온라인 분석 서비스
  - SW 클리닉 서비스

가능하게 하는 열쇠 : 동형암호

- 암호문에 연산한 것이 평문연산 결과 보존

$$\underline{op}(\mathcal{E}(m)) \equiv \mathcal{E}(op(m))$$

- 임의의 연산이 위 성질 만족시 완전동형암호

가능하게 하는 열쇠 : 동형암호

- 완전동형암호의 간단한 예:

$$\mathcal{E}(m) = m + pq + 2\epsilon$$

$$\mathcal{D}(c) = (c \; mod \; p) \; mod \; 2$$

- 다음 성질 만족 (이진 덧셈(XOR), 곱셈(AND)보존)

$$\mathcal{E}(m_1) + \mathcal{E}(m_2) \equiv \mathcal{E}(m_1 + m_2)$$

$$\mathcal{E}(m_1) \times \mathcal{E}(m_2) \equiv \mathcal{E}(m_1 \times m_2)$$

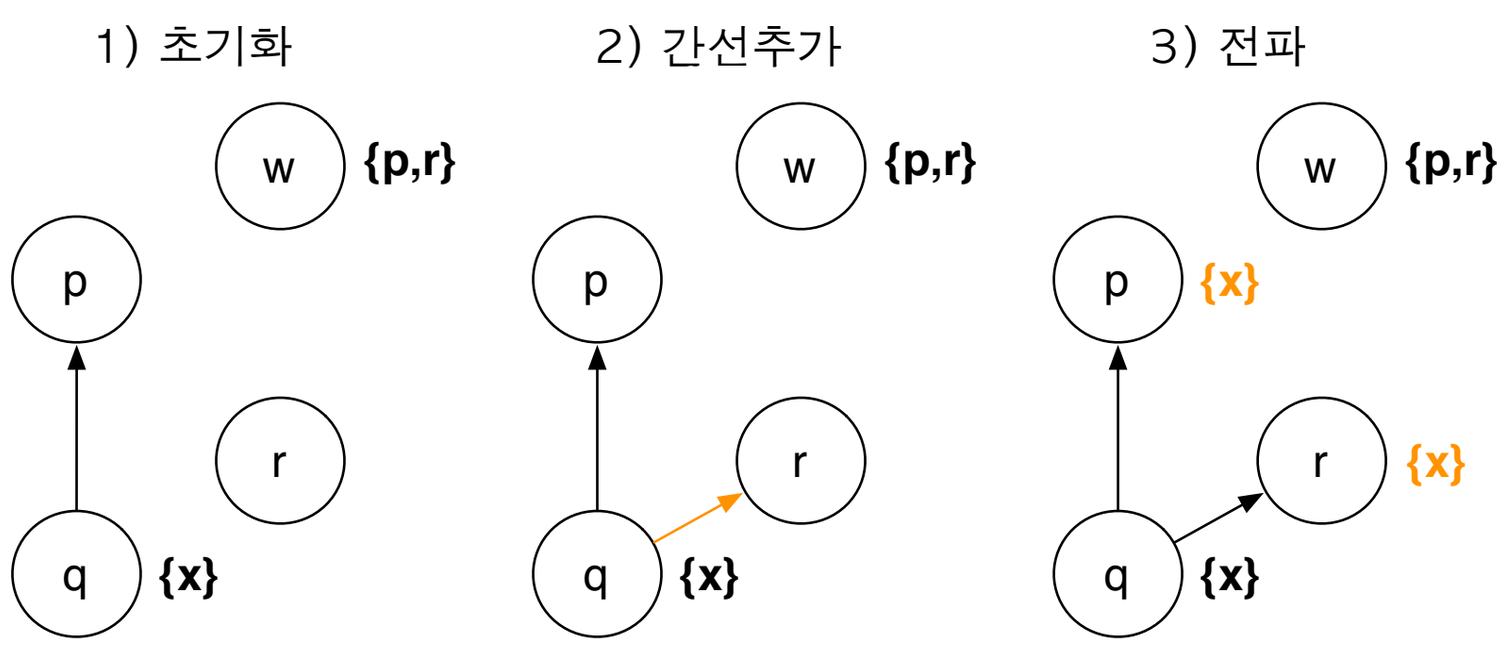
첫 걸음 : 비밀 포인터 분석

- 어떤 포인터 참조가 실행 중 어느 변수/저장장소를 가릴킬 수 있는지 분석
- 거의 모든 분석의 기본
- 간단한 연산(합집합, 부분집합)만 필요
- 다른 간단한 집합 제약분석들도 비슷
  - 클로저 분석, 타입 분석 등

그래프를 이용한 포인터분석

```
int x
int *p, *q, *r
int **w

q = &x
p = q
w = &p
w = &r
*w = q
```



비밀분석화

- 분석에 필요한 모든 것 암호화:
  - 그래프, 각 변수가 가리키는 주소
  - 프로그램 명령어들 암호화
- 가장 빠른 최신 동형암호[†]로 구현할 예정
- 쓸 수 있을 수준의 성능이 예상됨
- 자세한 것은 포스터에서.

† Jung Hee Cheon and Damien Stehl. *Fully homomorphic encryption over the integers revisited.*
In EUROCRYPT 2015 - 34th Annual International Conference on the Theory and Applications of Cryptographic Techniques. To appear.