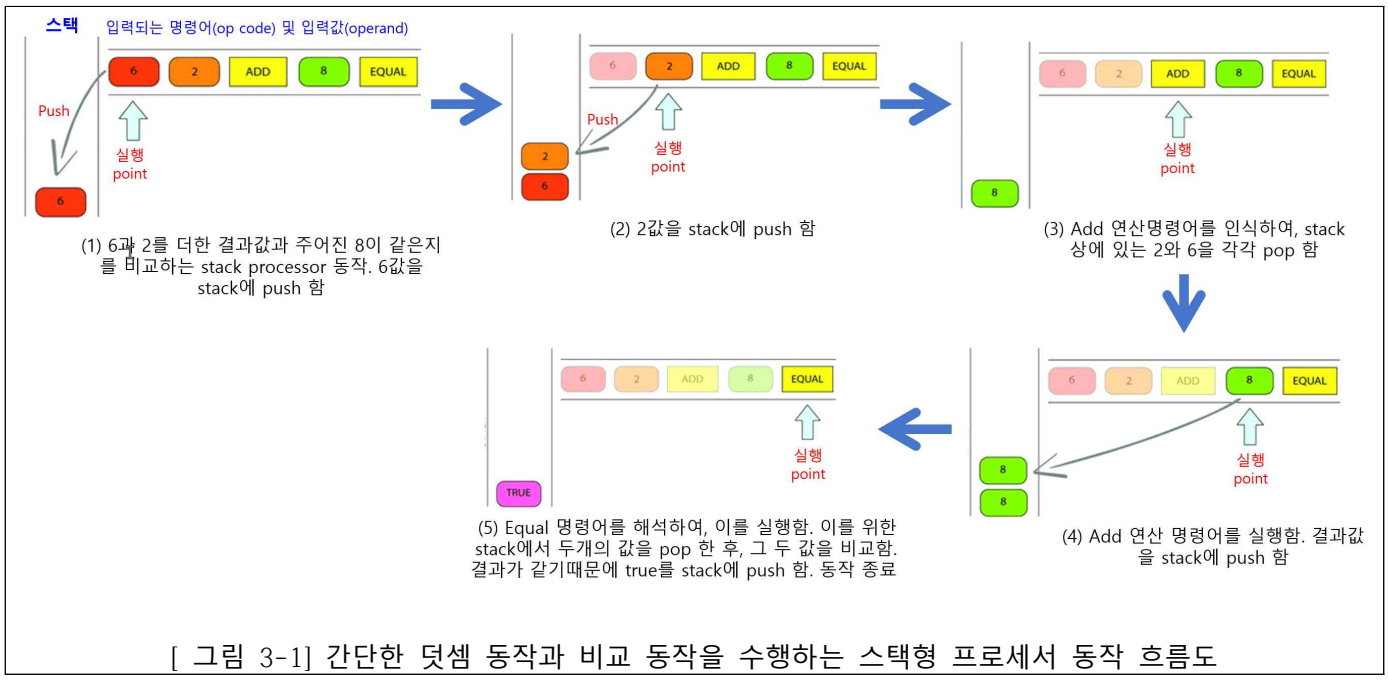
# 2021 암호분석경진대회

## 3번 문제 : 암호 응용

스택 프로세서(Stack Processor)는 다음 [그림 3-1]과 같은 스택의 푸시와 팝 동작만을 사용하여 실행 제어를 수행한다. 이러한 스택 프로세서의 동작 제어 모델과 공개키 암호의 서명/검증 기술을 결합하면, 특정 메시지에 대한 소유권을 특정인에게 지정할 수 있으며, 향후, 해당 특정인은 그 메시지에 대해 자신의 소유권을 검증함을 서 주장할 수 있게 된다. 최근 이슈화되고 있는 비트코인과 같은 많은 암호화폐/블록체인에서는 이러한 개념을 사용하여 메시지에 대한 소유권 관리를 하고 있으며, 이를 토대로 블록체인의 Smart Contract으로 발전시키고 있다.

문제 3-1 ) 다음 동작을 수행하는 간단한 스택 프로세서를 구현하라.

- 스택을 기반으로 두 정수를 더하는 간단한 덧셈 연산과 주어진 결과 값과 연산 결과값을 비교하는 스택 프로세서를 SW로 구현하라. ( 아래 그림 3-1 참고, C/C++, Python, Java 등 범용 프로그래밍 언어 사용 )




[ 그림 3-1] 간단한 덧셈 동작과 비교 동작을 수행하는 스택형 프로세서 동작 흐름도

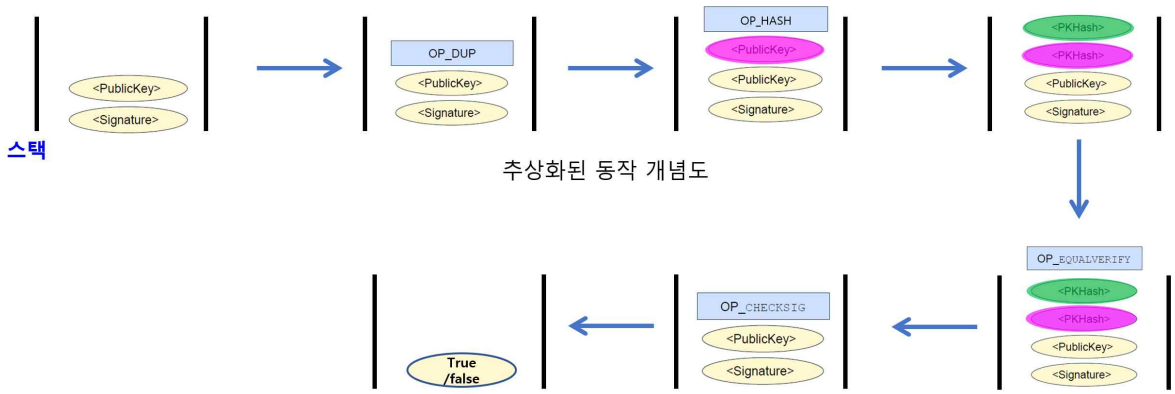
문제 3-2) ECC P256r1과 LSH 해쉬 함수를 사용하는 ECDSA 서명 생성 및 검증 프로토콜을 구현하고 정상 동작함을 보여라.

문제 3-3) 문제 3-1)에서 구현한 스택 프로세서를 확장하고 ECDSA 보안 프로토콜을 사용하여, [그림 3-2]의 동작을 수행하는 스택 프로세서를 구현하라. 확장된 스택 프로세서는 메시지 트랜잭션에 대한 소유권 지정 및 소유권을 확인할 수 있게 된다.

**확장된 스택형 프로세서에서 수행할 명령어:**

<수신자가 만든 서명값> , <수신자의 공개키 값> , 복사명령어, 해쉬명령어, <수신자의 공개키 값에 대한 해쉬값 > , 동일한지를 검증하는 명령어, 서명값을 검증하는 명령어

예: <Signature> <Publickey> OP_DUP OP_HASH <PKHash> OP_EqualVerify OP_CheckSig




추상화된 동작 개념도

[ 그림 3-2] 메시지 트랜잭션의 소유권을 지정하고 확인할 수 있는 확장된 스택 프로세서

▣ 참고 사항

1) 스택형 프로세서(스택형 머신) FILO(First In Last Out) 메모리 버퍼인 스택 동작인 푸시(Push)와 팝(Pop) 동작만을 사용하여, 실행 제어가 되는 머신으로 성능은 낮지만 경량 프로세서를 구현할 수 있다.

2) 비트코인 등에서는 공개키 암호 시스템을 사용하여 어떤 트랜잭션의 소유권을 제어할 수 있다. 예를 들면, 특정인 A의 공개키의 해시값을 사용하여 특정 트랜잭션에 대한 소유권을 지정(Locking mechanism, 잠금 메커니즘이라고 함)할 수 있으며, 향후, 해당 특정인 A는 자신의 공개키 값에 대한 해시값을 생성하여 이를 비교하고 또한, 특정인 A는 자신의 개인키 값을 사용하여 서명 검증을 수행함으로서 추가로 트랜잭션에 자신의 소유권을 검증할 수 있다.

비트코인에서 정의된 ScriptPubKey는 특정 트랜잭션 메시지에대한 Locking 메커니즘이 되며, ScriptSig라는 것은 Unlocking 메커니즘이 된다.

- 비트코인의 P2PKH의 Locking Script와 Unlocking Script 참고
- 비트코인의 Script Language 참고: https://en.bitcoin.it/wiki/Script

3) 본 문제를 푸는데 있어서 필요로 하는 공개키 암호로는 반드시 타원곡선 암호를 사용해야 하며, 이때 ECC P256r1 (Koblitz curve가 아닌 Ordinary curve)를 사용해야 한다. 또한, ECDSA 프로토콜에서 필요로 하는 해쉬함수로는 반드시 국산암호인 LSH 256을 사용하라.

- ECDSA 프로토콜 : https://en.wikipedia.org/wiki/Elliptic_Curve_Digital_Signature_Algorithm
- ECC P256r1 curve (NIST P-256 curve): https://en.wikipedia.org/wiki/SECG
- LSH 국산해쉬함수 : https://seed.kisa.or.kr/kisa/algorithm/EgovLSHInfo.do

4) 문제 3-3)을 푸는데 있어서 비트코인의 Script 언어 모델을 참고할 수 있다. 또한, 문제 3-3)의 구체적인 메시지 형태 등은 설계가 필요하다.