제 1 교시

국어 영역

[1~6] 다음 글을 읽고 물음에 답하시오.

(가)

중앙은행에서 발행과 통제를 수행하는 기존의 화폐와 달리 암호화폐는 보통 발행과 통제의 주체가 정해져 있지 않다. 이러한 암호화폐의 기본 원리는 '블록체인'에 있다. 블록체인이란 소규모의 데이터들이 블록이라는 단위로 묶여 여러 저장장치에 저장되는 기술을 뜻한다. 블록체인에서 블록이 저장되는 저장장치를 노드라 하며 새로 생성된 블록들은 노드에 전파된다. 블록은 모든 노드가 열람과 검증이 가능하고 모든 노드에게 똑같이 전송되는 특성을 가지기 때문에 특정 노드에 저장된 데이터가 변하더라도 다른 노드에 담긴 데이터는 변하지 않은 상태이므로 위조가 어렵다.

전자서명의 한 종류인 ECDSA는 암호화폐의 저장에 이용되는 기술 중 하나이다. 이 기술에서 노드는 사전에 개인키를 할당받는다. 개인키란 256비트의 정수 범위 내에서 무작위로 지정되는 정수를 말한다. 개인키를 할당받은 노드는 개인키의 값에 특정 함수값을 곱하여 특정 값을 얻게 되는데, 이렇게 구한 특정 값이 공개키에 해당한다. 이 과정에서 특정 함수값은 모든 노드가 공유하는 동일한 식이며 변하지 않는다.

암호화폐의 저장 과정에서 암호화폐의 거래 내역을 만든 노드는 개인키를 이용해 자신의 거래를 서명하고 다른 모든 노드에게 공개키와 서명을 전송한다. 이를 받은 다른 모든 노드는 서명자의 공개키를 활용해 서명을 검증하기 시작한다. 검증 과정에서 수학적으로 오류가 발견되지 않을 경우 해당 거래 내역은 블록에 포함될 수 있는 자격을 가진다. 검증이 완료된 거래 내역은 모든 노드에 전파되기 시작하여 각 노드의 메모리 풀에 보관된다. 이후 블록을 생성하는 노드에 해당하는 채굴자는 메모리 풀에 저장된 거래 내역 중 특정 규칙에 부합하는 거래들을 골라 하나의 블록 후보를 만든다. 이 블록 후보는 채굴자의 작업증명 이후 새로운 블록으로 승인되어 다시 다른 노드에 전파되며, 해당 블록을 수령한 노드는 블록에 수학적 오류가 없는지 재검증을 시작한다. 이상이 없을 경우 각 노드는 수령한 블록을 자신의 블록체인에 추가함으로써 암호화폐의 저장 과정이 종료된다.

그러나 이런 암호화폐에 대한 전망 중 하나로, ㉮ 양자컴퓨터의 개발이 성공할 경우 암호화폐의 보안에 치명적인 결함이 생긴다는 점이 우려되고 있다.

(나)

0 또는 1 중 하나의 상태만 가질 수 있는 비트를 기본 단위로 사용하는 기존의 컴퓨터와 달리, 양자컴퓨터는 0과 1을 동시에 중첩할 수 있는 큐비트를 기본 단위로 사용한다. 이러한 중첩 상태의 큐비트는 관측되면 0 또는 1중 하나의 값을 확률적으로 갖게 된다. 즉, $\alpha|0\rangle + \beta|1\rangle$ 의 방식으로 표현되어 있는 큐비트는 중첩 상태에 해당한다. 이 상태의 큐비트는 어떠한 값도 갖고 있지 않지만 큐비트가 관측되면 중첩상태가 붕괴되어 α와 β의 확률 진폭에 따라 0 또는 1 중 하나의 값을 갖게 되는 것이다. 이러한 큐비트가 여러 개 모인다면 매우 많은 경우의 수를 동시에 고려할 수 있게 되어 복잡한 문제를 기존의 컴퓨터보다 매우 빠르게 해결할 수 있다.

이러한 양자컴퓨터의 알고리즘 중 하나로 Shor 알고리즘이 있다. Shor 알고리즘은 복잡한 수의 소인수 분해나 이산 로그 문제의 해결에 사용되는 알고리즘으로, 양자컴퓨터의 특징을 이용하여 복잡한 문제를 매우 빨리 처리할 수 있다.

그러나 양자컴퓨터의 개발이 성공할 경우 현재 사용되는 암호체계는 중대한 위기를 ⓐ 맞게 된다. 이는 현재의 암호 체계 대부분이 복잡한 수의 소인수분해 혹은 이산 로그 문제를 기반으로 하고 있기 때문이다. 예시로 암호화폐 전자서명의 한 종류인 ECDSA에서는 이산 로그 문제 중 하나인 타원 곡선 함수가 이용되는데, 개인키는 256비트 범위 내의 무작위 정수 d, 타원 곡선 함수 위의 점에 해당하는 값을 G라 하자. d와 G를 곱하여 공개키인 Q를 구하게 되는데, 이 계산과정에서 역으로 d를 구하려면 기존 컴퓨터로는 계산이 매우 느리다. 그러나 Shor 알고리즘의 경우 큐비트의 특징인 중첩과 간섭, 붕괴를 활용하여 $dG=Q$의 식에서 d와 관련된 정보를 매우 빠른 속도로 구할 수 있다. 이때의 간섭이란 확률 진폭을 의도적으로 조작하여 특정 결과의 발생 확률을 수정하는 것을 말한다.

Shor 알고리즘을 통해 d를 역으로 구하는 과정에서 양자컴퓨터는 타원 곡선 함수 문제를 공격 대상의 공개키를 이용해 함수의 주기를 찾는 문제로 변환시킨다. 그다음 임의의 정수인 타원 곡선 함수의 입력값을 큐비트에 중첩시키고 간섭을 통해 주기성과 무관한 정보는 상쇄시켜 주기성과 관련 있는 정보의 측정 확률을 증폭시킨다. 이후 큐비트를 붕괴시켜 함수의 주기에 대한 정보가 담긴 정수를 얻고 해당 값을 계산해 공격 대상의 개인키를 추론한다.

1. (가)와 (나)에 대한 설명으로 가장 적절한 것은?

① (가)는 암호화폐와 기존 화폐의 차이점을 서술하고 있고, (나)는 현대 암호 체계의 장점에 대해 설명하고 있다.

② (가)는 작업증명의 과정에 대해 서술하고 있고, (나)는 Shor 알고리즘에 대해 설명하고 있다.

③ (가)는 기존 화폐의 단점을 나열하고 있고, (나)는 양자컴퓨터의 단점을 나열하고 있다.

④ (가)는 암호화폐의 저장 과정에 대해 서술하고 있고, (나)는 기존 컴퓨터의 장점에 대해 설명하고 있다.

⑤ (가)와 (나)는 모두 특정 값을 구하는 방법에 대해 설명하고 있다.

2. (가)를 읽은 학생이 이해한 내용으로 적절하지 않은 것은?

① 암호화폐의 위조가 어려운 이유는 모든 노드에 동일한 블록이 저장되는 점에 있겠군.
② ECDSA의 한 종류인 전자서명을 통해 암호화폐의 저장이 진행되겠군.
③ 거래내역을 만든 노드는 검증과정에서 검증에 참여하지 않겠군.
④ 노드의 메모리 풀에 저장된 거래내역은 블록에 포함될 수 있는 자격을 갖고 있겠군.
⑤ 검증 과정에서 데이터에 이상이 발견 될 경우 해당 데이터는 블록으로 추가되지 않을 수 있겠군.

3. (나)를 읽고 학생이 추론한 생각중 적절한 것은?

① 큐비트가 관측된다면 이후로는 비트와 동일하게 취급되겠군.
② 중첩상태의 큐비트를 관측하지 않은 상태에서 0 또는 1 중 하나의 값을 확률적으로 가지고 있다는걸 알 수 있겠군.
③ 암호화폐가 현재의 암호체계를 벗어나 새로운 암호체계를 도입하더라도 Shor 알고리즘을 통해 보안이 위협받겠군.
④ 기존 컴퓨터가 d를 역으로 구하는 과정이 느린 이유는 복잡한 수의 소인수분해를 비트를 이용해 진행하기 때문이겠군.
⑤ 큐비트를 붕괴시켜 얻은 결과값은 항상 내가 원하는 정보에 해당하겠군.

4. (가), (나)를 바탕으로 할 때, ㉮의 이유로 가장 적절한 것은?

① 양자컴퓨터의 큐비트를 붕괴시켜 공개키를 직접 구할 수 있기 때문이다.
② 양자컴퓨터를 이용해 함수의 주기성에 대한 정보를 얻음으로써 개인키의 추론을 가능하게 하기 때문이다.
③ 양자컴퓨터가 개발될 경우 모두에게 개인키가 노출되기 때문이다.
④ 오직 양자컴퓨터만 공개키를 얻는 계산식에서 개인키를 역으로 계산하는 시도가 가능하기 때문이다.
⑤ 양자컴퓨터의 개발이 성공할 경우 중첩을 이용해 모든 노드에 저장된 블록체인의 데이터를 동시에 수정할 수 있기 때문이다.

5. (가), (나)를 바탕으로 <보기>를 이해한 내용으로 적절하지 않은 것은? [3점]

<보 기>

노드 A의 공개키를 알고있는 노드 B는 Shor 알고리즘을 통해 A의 개인키를 추론했다. 이후 B는 추론한 A의 개인키를 이용해 암호화폐의 거래에 서명했다. 그리고 다른 노드에게 해당 서명과 A의 공개키를 전송했고, 이를 받은 다른 노드들은 검증 이후 해당 데이터를 자신의 메모리 풀에 저장했다.

① 개인키의 추론 과정에서 노드에 따라 타원 곡선 함수 위의 점이 다르기에 기존의 컴퓨터로는 계산할 수 없어 양자 컴퓨터를 사용했겠군.
② A의 개인키를 사용하여 서명한 데이터가 검증이 완료된 것은, 수학적으로 오류가 없기 때문이겠군.
③ 노드의 메모리 풀에 저장된 해당 데이터는 다시 한번 수학적 오류가 없는지 확인하는 과정을 거친 후 블록체인에 추가되겠군.
④ Shor 알고리즘의 계산 과정에서, 임의의 정수를 중첩시킨후 간섭을 통해 얻어낸 정보는 개인키가 아니겠군.
⑤ Shor 알고리즘의 계산 과정에서, 큐비트를 붕괴시키는 것은 필요한 정보의 측정 확률이 충분히 높아졌기 때문이겠군.

6. ⓐ와 문맥상 의미가 가장 가까운 것은?

① 나는 집에서 손님을 맞았다.
② 할머니께서 오늘 침을 맞고 오셨다.
③ 전염병으로 인해 국가적 위기를 맞게 되었다.
④ 내가 고른 정답이 맞게 되었다.
⑤ 그는 오직 자신의 생각만 맞다고 생각한다.

답: 5 2 1 2 1 3