(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2023-0095822
(43) 공개일자 2023년06월29일

(51) 국제특허분류(Int. Cl.)
H04L 9/40 (2022.01) *H04L 9/08* (2006.01)
(52) CPC특허분류
H04L 63/1441 (2013.01)
H04L 9/0858 (2013.01)
(21) 출원번호 10-2022-0175420
(22) 출원일자 2022년12월15일
심사청구일자 2022년12월15일
(30) 우선권주장
1020210184590 2021년12월22일 대한민국(KR)

(71) 출원인
고려대학교 산학협력단
서울특별시 성북구 안암로 145, 고려대학교 (안암동5가)
(72) 발명자
홍석희
서울특별시 노원구 덕릉로71길 30, 206동 2304호 (중계동, 양지대림아파트)
박동준
서울특별시 성북구 종암로5길 90, 102호
김규상
서울특별시 성북구 안암로9가길 85, 404호
(74) 대리인
이대호, 박건홍

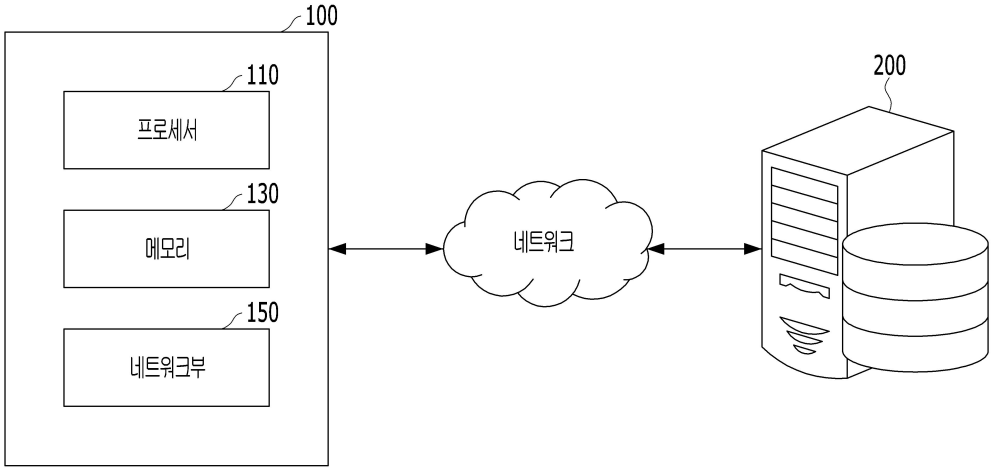
전체 청구항 수 : 총 10 항

(54) 발명의 명칭 **양자 키 교환 시에 전력 부채널 공격을 방지하기 위한 방법 및 장치**

(57) 요 약

본 개시의 몇몇 실시예에 따른 프로세서를 포함하는 컴퓨팅 장치에서 양자 키 교환 시에 전력 부채널 공격을 방지하기 위한 방법으로서, 양자 회로를 이용하여, 0 또는 1을 포함하는 비트를 10 또는 01을 포함하는 변환 비트로 인코딩하는 단계; 상기 변환 비트를 이용한 외부 기기와의 양자 키 교환(Quantum Key Distribution)을 통해 적어도 하나의 변환 비트를 포함하는 제 1 키(key)를 획득하는 단계; 및 10 또는 01을 출력하는 XOR 연산 회로를 이용하여, 상기 적어도 하나의 변환 비트 각각에 대한 적어도 하나의 제 1 연산 결과 비트를 획득하는 단계;를 포함할 수 있다.

대 표 도 - 도1



이 발명을 지원한 국가연구개발사업

과제고유번호	1711134697
과제번호	2021-0-00903-001
부처명	과학기술정보통신부
과제관리(전문)기관명	정보통신기획평가원
연구사업명	정보보호핵심원천기술개발사업
연구과제명	고신뢰 온-디바이스 딥러닝 가속기 설계를 위한 물리채널 기반 취약점 검증 및 대응 기술 개발
기 여 율	1/1
과제수행기관명	고려대학교 산학협력단
연구기간	2021.04.01 ~ 2024.12.31

명 세 서

청구범위

청구항 1

프로세서를 포함하는 컴퓨팅 장치에서 양자 키 교환 시에 전력 부채널 공격을 방지하기 위한 방법으로서,

양자 회로를 이용하여, 0 또는 1을 포함하는 비트를 10 또는 01을 포함하는 변환 비트로 인코딩하는 단계;

상기 변환 비트를 이용한 외부 기기와의 양자 키 교환(Quantum Key Distribution)을 통해 적어도 하나의 변환 비트를 포함하는 제 1 키(key)를 획득하는 단계; 및

10 또는 01을 출력하는 XOR 연산 회로를 이용하여, 상기 적어도 하나의 변환 비트 각각에 대한 적어도 하나의 제 1 연산 결과 비트를 획득하는 단계;

를 포함하는,

방법.

청구항 2

제 1 항에 있어서,

상기 양자 회로를 이용하여, 0 또는 1을 포함하는 비트를 10 또는 01을 포함하는 변환 비트로 인코딩하는 단계는,

상기 양자 회로에 포함된 단일 광자 검출기를 통해 획득되는 광자의 검출 여부에 기초하여 0 또는 1을 포함하는 상기 비트를 10 또는 01을 포함하는 상기 변환 비트로 인코딩하는 단계;

를 포함하는,

방법.

청구항 3

제 1 항에 있어서,

상기 변환 비트를 이용한 상기 외부 기기와의 양자 키 교환(Quantum Key Distribution)을 통해 상기 적어도 하나의 변환 비트를 포함하는 제 1 키(key)를 획득하는 단계는,

상기 변환 비트를 이용하여 상기 외부 기기로부터 사전 결정된 기저(basis)로 부호화 된 난수 변환 비트열을 수신하는 단계;

상기 난수 변환 비트열을 분석하여 역부호화를 위한 제 1 편광 상태 정보를 획득하는 단계;

상기 제 1 편광 상태 정보를 상기 외부 기기와 공유하고, 그리고 상기 외부 기기로부터 상기 제 1 편광 상태 정보와 상기 사전 결정된 기저에 대응되는 제 2 편광 상태 정보를 비교하여 서로 대응되는 적어도 하나의 대응 변환 비트를 획득하는 단계;

상기 외부 기기와 상기 적어도 하나의 대응 변환 비트를 공유하고, 그리고 상기 외부 기기로부터 수신한 양자 비트 오류율(Quantum bit error rate)에 기초하여 상기 적어도 하나의 대응 변환 비트의 선택 여부를 결정하는 단계; 및

상기 적어도 하나의 대응 변환 비트를 선택하기로 결정한 경우, 상기 적어도 하나의 대응 변환 비트를 포함하는 상기 제 1 키(key)를 획득하는 단계;

를 포함하는,

방법.

청구항 4

제 1 항에 있어서,

상기 XOR 연산 회로는,

제 1 변환 비트 및 제 2 변환 비트가 입력되는 경우, 1 또는 0을 포함하는 제 1 출력 변환 비트를 출력하는 제 1 XOR 서브 연산 회로; 및

상기 제 1 출력 변환 비트가 1을 포함하는 경우, 0을 포함하는 제 2 출력 변환 비트를 출력하고, 그리고 상기 제 1 출력 변환 비트가 0을 포함하는 경우, 1을 포함하는 제 3 출력 변환 비트를 출력하는 제 2 XOR 서브 연산 회로;

를 포함하는,

방법.

청구항 5

제 1 항에 있어서,

상기 적어도 하나의 제 1 연산 결과 비트와 상기 외부 기기에서 상기 XOR 연산 회로를 이용하여 상기 제 1 키에 대응되는 제 2 키로부터 획득한 제 2 연산 결과 비트를 비교하여 상기 제 1 키와 상기 제 2 키의 대응 여부를 결정하는 단계;

를 더 포함하는,

방법.

청구항 6

제 5 항에 있어서,

상기 제 1 키와 상기 제 2 키가 대응되지 않는 경우, 오류 정정 부호(error correcting code)를 이용하여 상기 제 1 키를 상기 제 2 키에 대응되는 방향으로 오류를 정정하는 단계;

를 더 포함하는,

방법.

청구항 7

제 1 항에 있어서,

상기 10 또는 01을 출력하는 XOR 연산 회로를 이용하여, 상기 적어도 하나의 변환 비트 각각에 대한 적어도 하나의 제 1 연산 결과 비트를 획득하는 단계는,

상기 XOR 연산 회로를 이용하여, 사전 결정된 연산 순서에 따라 상기 적어도 하나의 변환 비트 각각에 대한 상기 적어도 하나의 제 1 연산 결과 비트를 획득하는 단계; 및

상기 적어도 하나의 제 1 연산 결과 비트를 상기 제 1 키에 포함된 상기 적어도 하나의 변환 비트의 순서에 대응되도록 배치하는 단계;

를 포함하는,

방법.

청구항 8

제 7 항에 있어서,

상기 사전 결정된 연산 순서는,

무작위(random)로 결정된 순서를 포함하는,

방법.

청구항 9

컴퓨터 판독가능 저장 매체에 저장된 컴퓨터 프로그램으로서, 상기 컴퓨터 프로그램은 양자 키 교환 시에 전력 부채널 공격을 방지하기 위한 컴퓨팅 장치의 프로세서로 하여금 이하의 단계들을 수행하기 위한 명령들을 포함하며, 상기 단계들은:

양자 회로를 이용하여, 0 또는 1을 포함하는 비트를 10 또는 01을 포함하는 변환 비트로 인코딩하는 단계;

상기 변환 비트를 이용한 외부 기기와의 양자 키 교환(Quantum Key Distribution)을 통해 적어도 하나의 변환 비트를 포함하는 제 1 키(key)를 획득하는 단계; 및

10 또는 01을 출력하는 XOR 연산 회로를 이용하여, 상기 적어도 하나의 변환 비트 각각에 대한 적어도 하나의 제 1 연산 결과 비트를 획득하는 단계;

를 포함하는,

컴퓨터 판독가능 저장 매체에 저장된 컴퓨터 프로그램.

청구항 10

양자 키 교환 시에 전력 부채널 공격을 방지하기 위한 컴퓨팅 장치에 있어서,

적어도 하나의 코어를 포함하는 프로세서;

상기 프로세서에 의해 실행가능한 컴퓨터 프로그램을 저장하는 메모리; 및

네트워크부;

를 포함하고,

상기 프로세서는,

양자 회로를 이용하여, 0 또는 1을 포함하는 비트를 10 또는 01을 포함하는 변환 비트로 인코딩하고,

상기 변환 비트를 이용한 외부 기기와의 양자 키 교환(Quantum Key Distribution)을 통해 적어도 하나의 변환 비트를 포함하는 제 1 키(key)를 획득하고, 그리고

10 또는 01을 출력하는 XOR 연산 회로를 이용하여, 상기 적어도 하나의 변환 비트 각각에 대한 적어도 하나의 제 1 연산 결과 비트를 획득하는,

컴퓨팅 장치.

발명의 설명

기 술 분 야

[0001] 본 개시는 양자 키 교환 시에 전력 부채널 공격을 방지하기 위한 방법 및 장치에 관한 것으로, 보다 구체적으로 양자 키 교환 시에 발생되는 전력을 처리되는 데이터에 무관하도록 설계하는 기술에 관한 것이다.

배 경 기 술

[0002] 양자 컴퓨터는 양자 얽힘(quantum entanglement), 양자 중첩(quantum superposition) 등의 양자역학과 관련된 현상을 이용하여 데이터를 처리하는 컴퓨터일 수 있다. 양자 얽힘은 둘 이상의 상태가 양자적으로 서로 연결되어 있어, 각각의 상태로 따로 다룰 수 없는 상태를 의미할 수 있다. 양자 중첩은 양자 상태를 측정하기 전에 측정에 의한 여러 결과 상태가 확률적으로 동시에 존재하는 것을 의미할 수 있다.

[0003] 이러한 양자 컴퓨터는 양자 통신을 수행할 수 있다. 양자 통신은 양자상태에 담겨있는 정보를 송신 측에서 수신 측까지 전달하는 과정을 의미할 수 있다. 양자 컴퓨터는 양자 통신 과정에서 양자 키 교환(Quantum Key Distribution)을 통해 보안이 필요한 송수신자 사이에 암호화에 필요한 키(key)를 공유할 수 있다.

[0004] 하지만, 이러한 양자 통신 과정은 전력 부채널 공격(Power Side-Channel Attacks)을 받을 수 있다. 전력 부채널 공격은 전자적 장치가 연산을 수행할 때 장치가 소비하는 전력이 중간 값의 해밍 무게(hamming weights)와 비례한다는 사실을 이용하여 장치 내부에서 처리되는 값을 획득하는 공격일 수 있다. 따라서, 안전한 양자 통신이 이루어지기 위해서 전력 부채널 공격을 방지하기 위한 방법이 필요할 수 있다.

선행기술문헌

특허문헌

[0005] (특허문헌 0001) 대한민국 등록특허 제10-1418962호(2014.07.07. 등록)

발명의 내용

해결하려는 과제

[0006] 본 개시는 전술한 배경기술에 대응하여 안출된 것으로, 양자 키 교환 시에 전력 부채널 공격을 방지하기 위한 방법을 제공하고자 한다.

[0007] 본 개시의 기술적 과제들은 이상에서 언급한 기술적 과제로 제한되지 않으며, 언급되지 않은 또 다른 기술적 과제들은 아래의 기재로부터 당업자에게 명확하게 이해될 수 있을 것이다.

과제의 해결 수단

[0008] 전술한 바와 같은 과제를 해결하기 위한 본 개시의 몇몇 실시예에 따라, 프로세서를 포함하는 컴퓨팅 장치에서 양자 키 교환 시에 전력 부채널 공격을 방지하기 위한 방법으로서, 양자 회로를 이용하여, 0 또는 1을 포함하는 비트를 10 또는 01을 포함하는 변환 비트로 인코딩하는 단계; 상기 변환 비트를 이용한 외부 기기와의 양자 키 교환(Quantum Key Distribution)을 통해 적어도 하나의 변환 비트를 포함하는 제 1 키(key)를 획득하는 단계; 및 10 또는 01을 출력하는 XOR 연산 회로를 이용하여, 상기 적어도 하나의 변환 비트 각각에 대한 적어도 하나의 제 1 연산 결과 비트를 획득하는 단계;를 포함할 수 있다.

[0009] 대안적으로, 상기 양자 회로를 이용하여, 0 또는 1을 포함하는 비트를 10 또는 01을 포함하는 변환 비트로 인코딩하는 단계는, 상기 양자 회로에 포함된 단일 광자 검출기를 통해 획득되는 광자의 검출 여부에 기초하여 0 또는 1을 포함하는 상기 비트를 10 또는 01을 포함하는 상기 변환 비트로 인코딩하는 단계;를 포함할 수 있다.

[0010] 대안적으로, 상기 변환 비트를 이용한 상기 외부 기기와의 양자 키 교환(Quantum Key Distribution)을 통해 상기 적어도 하나의 변환 비트를 포함하는 제 1 키(key)를 획득하는 단계는, 상기 변환 비트를 이용하여 상기 외부 기기로부터 사전 결정된 기저(basis)로 부호화 된 난수 변환 비트열을 수신하는 단계; 상기 난수 변환 비트열을 분석하여 역부호화를 위한 제 1 편광 상태 정보를 획득하는 단계; 상기 제 1 편광 상태 정보를 상기 외부 기기와 공유하고, 그리고 상기 외부 기기로부터 상기 제 1 편광 상태 정보와 상기 사전 결정된 기저에 대응되는 제 2 편광 상태 정보를 비교하여 서로 대응되는 적어도 하나의 대응 변환 비트를 획득하는 단계; 상기 외부 기기와 상기 적어도 하나의 대응 변환 비트를 공유하고, 그리고 상기 외부 기기로부터 수신한 양자 비트 오류율(Quantum bit error rate)에 기초하여 상기 적어도 하나의 대응 변환 비트의 선택 여부를 결정하는 단계; 및 상기 적어도 하나의 대응 변환 비트를 선택하기로 결정한 경우, 상기 적어도 하나의 대응 변환 비트를 포함하는 상기 제 1 키(key)를 획득하는 단계;를 포함할 수 있다.

[0011] 대안적으로, 상기 XOR 연산 회로는 제 1 변환 비트 및 제 2 변환 비트가 입력되는 경우, 1 또는 0을 포함하는 제 1 출력 변환 비트를 출력하는 제 1 XOR 서브 연산 회로; 및 상기 제 1 출력 변환 비트가 1을 포함하는 경우, 0을 포함하는 제 2 출력 변환 비트를 출력하고, 그리고 상기 제 1 출력 변환 비트가 0을 포함하는 경우, 1을 포함하는 제 3 출력 변환 비트를 출력하는 제 2 XOR 서브 연산 회로;를 포함할 수 있다.

[0012] 대안적으로, 상기 적어도 하나의 제 1 연산 결과 비트와 상기 외부 기기에서 상기 XOR 연산 회로를 이용하여 상기 제 1 키에 대응되는 제 2 키로부터 획득한 제 2 연산 결과 비트를 비교하여 상기 제 1 키와 상기 제 2 키의 대응 여부를 결정하는 단계;를 더 포함할 수 있다.

[0013] 대안적으로, 상기 제 1 키와 상기 제 2 키가 대응되지 않는 경우, 오류 정정 부호(error correcting code)를 이용하여 상기 제 1 키를 상기 제 2 키에 대응되는 방향으로 오류를 정정하는 단계;를 더 포함할 수 있다.

[0014] 대안적으로, 상기 10 또는 01을 출력하는 XOR 연산 회로를 이용하여, 상기 적어도 하나의 변환 비트 각각에 대한 적어도 하나의 제 1 연산 결과 비트를 획득하는 단계는, 상기 XOR 연산 회로를 이용하여, 사전 결정된 연산 순서에 따라 상기 적어도 하나의 변환 비트 각각에 대한 상기 적어도 하나의 제 1 연산 결과 비트를 획득하는 단계; 및 상기 적어도 하나의 제 1 연산 결과 비트를 상기 제 1 키에 포함된 상기 적어도 하나의 변환 비트의 순서에 대응되도록 배치하는 단계;를 포함할 수 있다.

[0015] 대안적으로, 상기 사전 결정된 연산 순서는, 무작위(random)로 결정된 순서를 포함할 수 있다.

[0016] 대안적으로, 컴퓨터 판독가능 저장 매체에 저장된 컴퓨터 프로그램으로서, 상기 컴퓨터 프로그램은 양자 키 교환 시에 전력 부채널 공격을 방지하기 위한 컴퓨팅 장치의 프로세서로 하여금 이하의 단계들을 수행하기 위한 명령들을 포함하며, 상기 단계들은: 양자 회로를 이용하여, 0 또는 1을 포함하는 비트를 10 또는 01을 포함하는 변환 비트로 인코딩하는 단계; 상기 변환 비트를 이용한 외부 기기와의 양자 키 교환(Quantum Key Distribution)을 통해 적어도 하나의 변환 비트를 포함하는 제 1 키(key)를 획득하는 단계; 및 10 또는 01을 출력하는 XOR 연산 회로를 이용하여, 상기 적어도 하나의 변환 비트 각각에 대한 적어도 하나의 제 1 연산 결과 비트를 획득하는 단계;를 포함할 수 있다.

[0017] 대안적으로, 양자 키 교환 시에 전력 부채널 공격을 방지하기 위한 컴퓨팅 장치에 있어서, 적어도 하나의 코어를 포함하는 프로세서; 상기 프로세서에 의해 실행가능한 컴퓨터 프로그램을 저장하는 메모리; 및 네트워크부;를 포함하고, 상기 프로세서는, 양자 회로를 이용하여, 0 또는 1을 포함하는 비트를 10 또는 01을 포함하는 변환 비트로 인코딩하고, 상기 변환 비트를 이용한 외부 기기와의 양자 키 교환(Quantum Key Distribution)을 통해 적어도 하나의 변환 비트를 포함하는 제 1 키(key)를 획득하고, 그리고 10 또는 01을 출력하는 XOR 연산 회로를 이용하여, 상기 적어도 하나의 변환 비트 각각에 대한 적어도 하나의 제 1 연산 결과 비트를 획득할 수 있다.

발명의 효과

[0018] 본 개시는 양자 키 교환 시에 전력 부채널 공격을 방지할 수 있다.

[0019] 본 개시에서 얻을 수 있는 효과는 이상에서 언급한 효과로 제한되지 않으며, 언급하지 않은 또 다른 효과들은 아래의 기재로부터 본 개시가 속하는 기술분야에서 통상의 지식을 가진 자에게 명확하게 이해될 수 있을 것이다.

도면의 간단한 설명

[0020] 다양한 양상들이 이제 도면들을 참조로 기재되며, 여기서 유사한 참조 번호들은 총괄적으로 유사한 구성요소들을 지칭하는데 이용된다. 이하의 실시예에서, 설명 목적을 위해, 다수의 특정 세부사항들이 하나 이상의 양상들의 총체적 이해를 제공하기 위해 제시된다. 그러나, 그러한 양상(들)이 이러한 구체적인 세부사항들 없이 실시될 수 있음은 명백할 것이다.

도 1은 본 개시의 몇몇 실시예에 따른 양자 키 교환 시에 전력 부채널 공격을 방지하기 위한 시스템을 나타내는 도면이다.

도 2는 본 개시의 몇몇 실시예에 따른 양자 회로를 설명하기 위한 도면이다.

도 3은 본 개시의 몇몇 실시예에 XOR 연산 회로를 설명하기 위한 도면이다.

도 4는 본 개시의 몇몇 실시예에 따른 컴퓨팅 장치에서 양자 키 교환 시에 전력 부채널 공격을 방지하기 위한

방법을 나타내는 도면이다.

도 5는 본 개시의 실시예들이 구현될 수 있는 예시적인 컴퓨팅 환경에 대한 간략하고 일반적인 개략도를 도시한다.

발명을 실시하기 위한 구체적인 내용

[0021] 다양한 실시예들이 이제 도면을 참조하여 설명된다. 본 명세서에서, 다양한 설명들이 본 개시의 이해를 제공하기 위해서 제시된다. 그러나, 이러한 실시예들은 이러한 구체적인 설명 없이도 실행될 수 있음이 명백하다.

[0022] 본 명세서에서 사용되는 용어 "컴포넌트", "모듈", "시스템" 등은 컴퓨터-관련 엔티티, 하드웨어, 펌웨어, 소프트웨어, 소프트웨어 및 하드웨어의 조합, 또는 소프트웨어의 실행을 지칭한다. 예를 들어, 컴포넌트는 프로세서 상에서 실행되는 처리과정(procedure), 프로세서, 객체, 실행 스레드, 프로그램, 및/또는 컴퓨터일 수 있지만, 이들로 제한되는 것은 아니다. 예를 들어, 컴퓨팅 장치에서 실행되는 애플리케이션 및 컴퓨팅 장치 모두 컴포넌트일 수 있다. 하나 이상의 컴포넌트는 프로세서 및/또는 실행 스레드 내에 상주할 수 있다. 일 컴포넌트는 하나의 컴퓨터 내에 로컬화 될 수 있다. 일 컴포넌트는 2개 이상의 컴퓨터들 사이에 분배될 수 있다. 또한, 이러한 컴포넌트들은 그 내부에 저장된 다양한 데이터 구조들을 갖는 다양한 컴퓨터 판독가능한 매체로부터 실행할 수 있다. 컴포넌트들은 예를 들어 하나 이상의 데이터 패킷들을 갖는 신호(예를 들면, 로컬 시스템, 분산 시스템에서 다른 컴포넌트와 상호작용하는 하나의 컴포넌트로부터의 데이터 및/또는 신호를 통해 다른 시스템과 인터넷과 같은 네트워크를 통해 전송되는 데이터)에 따라 로컬 및/또는 원격 처리들을 통해 통신할 수 있다.

[0023] 더불어, 용어 "또는"은 배타적 "또는"이 아니라 내포적 "또는"을 의미하는 것으로 의도된다. 즉, 달리 특정되지 않거나 문맥상 명확하지 않은 경우에, "X는 A 또는 B를 이용한다"는 자연적인 내포적 치환 중 하나를 의미하는 것으로 의도된다. 즉, X가 A를 이용하거나; X가 B를 이용하거나; 또는 X가 A 및 B 모두를 이용하는 경우, "X는 A 또는 B를 이용한다"가 이들 경우들 어느 것으로도 적용될 수 있다. 또한, 본 명세서에 사용된 "및/또는"이라는 용어는 열거된 관련 아이템들 중 하나 이상의 아이템의 가능한 모든 조합을 지칭하고 포함하는 것으로 이해되어야 한다.

[0024] 또한, "포함한다" 및/또는 "포함하는"이라는 용어는, 해당 특징 및/또는 구성요소가 존재함을 의미하는 것으로 이해되어야 한다. 다만, "포함한다" 및/또는 "포함하는"이라는 용어는, 하나 이상의 다른 특징, 구성요소 및/또는 이들의 그룹의 존재 또는 추가를 배제하지 않는 것으로 이해되어야 한다. 또한, 달리 특정되지 않거나 단수 형태를 지시하는 것으로 문맥상 명확하지 않은 경우에, 본 명세서와 청구범위에서 단수는 일반적으로 "하나 또는 그 이상"을 의미하는 것으로 해석되어야 한다.

[0025] 그리고, "A 또는 B 중 적어도 하나"이라는 용어는, "A만을 포함하는 경우", "B 만을 포함하는 경우", "A와 B의 구성으로 조합된 경우"를 의미하는 것으로 해석되어야 한다.

[0026] 당업자들은 추가적으로 여기서 개시된 실시예들과 관련되어 설명된 다양한 예시적 논리적 블록들, 구성들, 모듈들, 회로들, 수단들, 로직들, 및 알고리즘 단계들이 전자 하드웨어, 컴퓨터 소프트웨어, 또는 양쪽 모두의 조합들로 구현될 수 있음을 인식해야 한다. 하드웨어 및 소프트웨어의 상호교환성을 명백하게 예시하기 위해, 다양한 예시적 컴포넌트들, 블록들, 구성들, 수단들, 로직들, 모듈들, 회로들, 및 단계들은 그들의 기능성 측면에서 일반적으로 위에서 설명되었다. 그러한 기능성이 하드웨어로 또는 소프트웨어로서 구현되는지 여부는 전반적인 시스템에 부과된 특정 어플리케이션(application) 및 설계 제한들에 달려 있다. 숙련된 기술자들은 각각의 특정 어플리케이션들을 위해 다양한 방법들로 설명된 기능성을 구현할 수 있다. 다만, 그러한 구현의 결정들이 본 개시내용의 영역을 벗어나게 하는 것으로 해석되어서는 안된다.

[0027] 제시된 실시예들에 대한 설명은 본 개시의 기술 분야에서 통상의 지식을 가진 자가 본 발명을 이용하거나 또는 실시할 수 있도록 제공된다. 이러한 실시예들에 대한 다양한 변형들은 본 개시의 기술 분야에서 통상의 지식을 가진 자에게 명백할 것이다. 여기에 정의된 일반적인 원리들은 본 개시의 범위를 벗어남이 없이 다른 실시예들에 적용될 수 있다. 그리하여, 본 발명은 여기에 제시된 실시예 들로 한정되는 것이 아니다. 본 발명은 여기에 제시된 원리들 및 신규한 특징들과 일관되는 최광의의 범위에서 해석되어야 할 것이다.

[0028] 본 개시내용에서의 제 1 , 제 2 , 또는 제 3 과 같이 제 N 으로 표현되는 용어들은 적어도 하나의 엔티티들을 구분하기 위해 사용된다. 예를 들어, 제 1 과 제 2 로 표현된 엔티티들은 서로 동일하거나 또는 상이할 수 있다.

[0030] 도 1은 본 개시의 몇몇 실시예에 따른 양자 키 교환(Quantum Key Distribution) 시에 전력 부채널 공격을 방지하기 위한 시스템을 나타내는 도면이다.

[0031] 본 개시에서 전력 부채널 공격은 전자적 장치가 연산을 수행할 때 장치가 소비하는 전력이 중간 값의 해밍 무게(hamming weights)와 비례한다는 사실을 이용하여 장치 내부에서 처리되는 값을 획득하는 공격일 수 있다. 전력 부채널 공격은 연산 시의 전원의 전류 값을 측정하여 단순 분석하는 SPA(Simple power analysis), 전류를 통계적으로 분석하는 DPA(Differential power analysis) 및 여러 DPA의 조합으로 고차원 분석을 하는 HO-DPA(High-order differential power analysis) 등을 포함할 수 있다.

[0032] 본 개시에서 양자 키 교환은 양자 역학의 구성 요소와 관련된 암호화 프로토콜을 구현하는 통신 방법일 수 있다. 양자 키 교환은 송수신자 간에 키(key)를 공유하고, 공유된 키를 이용하여 메시지를 암호화하고 해독할 수 있다.

[0033] 도 1을 참조하면, 시스템은 컴퓨팅 장치(100), 외부 기기(200) 및 네트워크를 포함할 수 있다. 도 1에 도시된 시스템의 구성은 간략화 하여 나타낸 예시일 뿐이다. 본 개시의 일 실시예에서 시스템은 양자 키 교환을 수행하기 위한 다른 구성들이 포함될 수 있고, 개시된 구성들 중 일부만이 시스템을 구성할 수도 있다.

[0034] 본 개시내용에서의 컴퓨팅 장치(100)는 본 개시내용의 실시예들을 구현하기 위한 시스템을 구성하는 임의의 형태의 서버 또는 사용자 단말을 의미할 수 있다. 컴퓨팅 장치(100)는 양자 중첩의 지수적인 정보 표현, 양자 얽힘을 이용한 병렬 연산과 같은 양자역학적인 물리현상을 활용하여 계산을 수행하는 양자 컴퓨팅 장치를 의미할 수 있다.

[0035] 컴퓨팅 장치(100)는 프로세서(110), 메모리(130), 네트워크부(150)를 포함할 수 있다. 프로세서(110)는 하나 이상의 코어로 구성될 수 있으며, 컴퓨팅 장치의 중앙 처리 장치(CPU: central processing unit), 범용 그래픽 처리 장치 (GPGPU: general purpose graphics processing unit), 텐서 처리 장치(TPU: tensor processing unit) 등의 데이터 분석, 양자 처리를 위한 프로세서를 포함할 수 있다. 프로세서(110)는 통상적으로 양자 컴퓨팅 장치(100)의 전반적인 동작을 제어할 수 있다. 예를 들어, 프로세서(110)는 양자 컴퓨팅 장치(100)에 포함된 구성요소들을 통해 입력 또는 출력되는 신호, 데이터 정보 등을 처리할 수 있다. 다른 예를 들어, 프로세서(110)는 메모리(130)에 저장된 컴퓨터 프로그램을 판독하여 본 개시의 일 실시예에 따른 양자 처리를 수행할 수 있다.

[0036] 본 개시의 몇몇 실시예에 따르면, 메모리(130)는 프로세서(110)가 생성하거나 결정한 임의의 형태의 정보 및 네트워크부(150)가 수신한 임의의 형태의 정보를 저장할 수 있다.

[0037] 본 개시의 몇몇 실시예에 따르면, 메모리(130)는 플래시 메모리 타입(flash memory type), 하드디스크 타입(hard disk type), 멀티미디어 카드 마이크로 타입(multimedia card micro type), 카드 타입의 메모리(예를 들어 SD 또는 XD 메모리 등), 램(Random Access Memory, RAM), SRAM(Static Random Access Memory), 롬(ReadOnly Memory, ROM), EEPROM(Electrically Erasable Programmable Read-Only Memory), PROM(Programmable Read-Only Memory), 자기 메모리, 자기 디스크, 광디스크 중 적어도 하나의 타입의 저장매체를 포함할 수 있다. 컴퓨팅 장치(100)는 인터넷(internet) 상에서 상기 메모리(130)의 저장 기능을 수행하는 웹 스토리지(web storage)와 관련되어 동작할 수도 있다. 전술한 메모리에 대한 기재는 예시일 뿐, 본 개시는 이에 제한되지 않는다. 본 개시의 몇몇 실시예에 따른 네트워크부(150)는 임의의 형태의 데이터 및 신호 등을 송수신할 수 있는 임의의 유무선 통신 네트워크를 포함할 수 있다. 본 명세서에서 설명된 기술들은 위에서 언급된 네트워크들뿐만 아니라, 다른 네트워크들에서도 사용될 수 있다.

[0039] 한편, 컴퓨팅 장치(100)의 프로세서(110)는 양자 회로를 이용하여, 0 또는 1을 포함하는 비트를 10 또는 01을 포함하는 변환 비트로 인코딩할 수 있다. 예를 들어, 프로세서(110)는 양자 회로를 이용하여, 비트 0은 변환 비트 10에 대응되고, 비트 1은 변환 비트 01에 대응되도록 인코딩할 수 있다.

[0040] 양자 회로는 양자 정보 시스템에서 사용하는 양자 게이트 회로(quantum gate circuit)일 수 있다. 양자 회로는 단일 광자 검출기(Single Photon Detector) 및/또는 CNOT 게이트를 포함할 수 있다.

[0041] 단일 광자 검출기는 양자 암호 키를 생성하기 위해 사용되는 단일 광자를 검출하는 장치일 수 있다. 예를 들어, 단일 광자 검출기는 애벌란시 광 다이오드(Avalanche Photo-Diode)를 포함할 수 있다.

[0042] CNOT 게이트는 제어(control) 큐비트와 목표(target) 큐비트를 포함할 수 있다. |A〉와 |B〉를 각각 제어 큐비트와 목표 큐비트라고 할 때, CNOT 게이트는 |A〉의 상태를 변경시키지 않고, |A〉의 상태에 따라 |B〉의 상태

를 변경시킬 수 있다. 예를 들어, CNOT 게이트는 |A〉가 |0〉인 경우, |B〉의 상태를 변경시키지 않을 수 있다. 다른 예를 들어, CNOT 게이트는 |A〉가 |1〉인 경우, |B〉의 상태를 NOT 게이트를 수행한 결과로 결정할 수 있다. NOT 게이트는 입력이 1이면 0을 출력하고, 입력이 0이면 1을 출력하는 게이트일 수 있다.

[0043] 프로세서(110)는 양자 회로에 포함된 단일 광자 검출기를 통해 획득되는 광자의 검출 여부에 기초하여 0 또는 1을 포함하는 비트를 10 또는 01을 포함하는 변환 비트로 인코딩할 수 있다. 양자 회로에 관한 구체적인 설명은 도 2를 참조하여 후술한다.

[0045] 프로세서(110)는 변환 비트를 이용한 외부 기기(200)와의 양자 키 교환(Quantum Key Distribution)을 통해 적어도 하나의 변환 비트를 포함하는 제 1 키(key)를 획득할 수 있다.

[0046] 예를 들어, 프로세서(110)는 변환 비트를 이용하여 외부 기기(200)로부터 사전 결정된 기저(basis)로 부호화 된 난수 변환 비트열을 수신할 수 있다.

[0047] 사전 결정된 기저는 컴퓨팅 장치(100)와 외부 기기(200) 간에 사전에 공유된 편광 상태일 수 있다. 예를 들어, 사전 결정된 기저는 수평수직 기저(Rectilinear Basis) 및/또는 대각 기저(Diagonal Basis) 등을 포함할 수 있다.

[0048] 수평수직 기저는 0도 상태, 90도 상태 등을 포함할 수 있다. 수평수직 기저에서의 0도 상태는 변환 비트 10에 대응되고, 90도 상태는 변환 비트 01에 대응될 수 있다.

[0049] 대각 기저는 -45도 상태, 45도 상태 등을 포함할 수 있다. 대각 기저에서의 -45도 상태는 변환 비트 10에 대응되고, 45도 상태는 01에 대응될 수 있다.

[0050] 프로세서(110)는 난수 변환 비트열을 분석하여 역부호화를 위한 제 1 편광 상태 정보를 획득할 수 있다.

[0051] 제 1 편광 상태 정보는 난수 변환 비트열에 포함된 변환 비트들 각각에 대한 편광 상태를 포함할 수 있다. 예를 들어, 제 1 편광 상태 정보는 난수 변환 비트열에 포함된 첫번째 변환 비트의 편광 상태, 두번째 변환 비트의 편광 상태, 세번째 변환 비트의 편광 상태 등을 포함할 수 있다.

[0052] 프로세서(110)는 제 1 편광 상태 정보를 외부 기기(200)와 공유하고, 그리고 외부 기기(200)로부터 제 1 편광 상태 정보와 사전 결정된 기저에 대응되는 제 2 편광 상태 정보를 비교하여 서로 대응되는 적어도 하나의 대응 변환 비트를 획득할 수 있다. 본 개시의 몇몇 실시예에 따르면, 프로세서(110)는 제 1 편광 상태 정보를 외부 기기(200)와 공유하고, 그리고 제 1 편광 상태 정보와 사전 결정된 기저에 대응되는 제 2 편광 상태 정보를 비교하여 서로 대응되는 적어도 하나의 대응 변환 비트를 획득할 수 있다.

[0053] 제 2 편광 상태 정보는 외부 기기(200)에서 부호화 된 난수 변환 비트열을 생성할 때 사용된 사전 결정된 기저에 관한 정보일 수 있다. 따라서, 프로세서(110) 및/또는 외부 기기(200)는 제 1 편광 상태 정보와 제 2 편광 상태 정보를 비교하여 서로 대응되는 적어도 하나의 대응 변환 비트를 획득할 수 있다.

[0054] 프로세서(110)는 외부 기기(200)와 적어도 하나의 대응 변환 비트를 공유하고, 그리고 외부 기기(200)로부터 수신한 양자 비트 오류율(Quantum bit error rate)에 기초하여 적어도 하나의 대응 변환 비트의 선택 여부를 결정할 수 있다. 본 개시의 몇몇 실시예에 따르면, 프로세서(110)는 외부 기기(200)와 적어도 하나의 대응 변환 비트를 공유하고, 그리고 산출된 양자 비트 오류율에 기초하여 적어도 하나의 대응 변환 비트의 선택 여부를 결정할 수 있다.

[0055] 양자 비트 오류율은 키(key)에 포함된 전체 변환 비트에 포함된 오류 변환 비트의 비율일 수 있다. 예를 들어, 양자 비트 오류율은 제 1 키에 포함된 전체 변환 비트에서 적어도 하나의 대응 변환 비트를 제외한 나머지 변환 비트의 비율을 의미할 수 있다. 적어도 하나의 대응 변환 비트를 제외한 나머지 변환 비트는 오류가 발생한 변환 비트로, 제 1 편광 상태 정보와 제 2 편광 상태 정보를 비교한 결과 서로 대응되지 않는 것으로 판단된 변환 비트일 수 있다.

[0056] 따라서, 프로세서(110) 및/또는 외부 기기(200)는 적어도 하나의 대응 변환 비트에 기초하여 양자 비트 오류율을 산출할 수 있다. 프로세서(110) 및/또는 외부 기기(200)는 산출된 양자 비트 오류율에 기초하여 적어도 하나의 대응 변환 비트의 선택 여부를 결정할 수 있다.

[0058] 프로세서(110)는 적어도 하나의 대응 변환 비트를 선택하기로 결정한 경우, 적어도 하나의 대응 변환 비트를 포함하는 제 1 키(key)를 획득할 수 있다. 예를 들어, 프로세서(110)는 양자 비트 오류율이 사전 결정된 임계치(예를 들어, 50% 등) 이상인 경우, 적어도 하나의 대응 변환 비트를 선택하고, 그리고 적어도 하나의 대응 변환 비트를 포함하는 제 1 키(key)를 획득할 수 있다. 프로세서(110)는 획득된 적어도 하나의 대응 변환 비트의 개수가 사전 결정된 기준치(예를 들어, 100개) 미만인 경우, 외부 기기(200)와의 양자 키 교환을 사전 결정된 기준치 이상의 적어도 하나의 대응 변환 비트가 획득될 때까지 반복하여 수행할 수 있다.

[0059] 프로세서(110)는 적어도 하나의 대응 변환 비트를 선택하지 않기로 결정한 경우, 적어도 하나의 대응 변환 비트를 폐기할 수 있다. 예를 들어, 프로세서(110)는 양자 비트 오류율이 사전 결정된 임계치(예를 들어, 50% 등) 미만인 경우, 적어도 하나의 대응 변환 비트를 폐기할 수 있다. 그리고 프로세서(110)는 상술한 외부 기기(200)와의 양자 키 교환을 사전 결정된 기준치 이상의 적어도 하나의 대응 변환 비트가 획득될 때까지 반복하여 수행할 수 있다.

[0061] 프로세서(110)는 10 또는 01을 출력하는 XOR 연산 회로를 이용하여, 적어도 하나의 변환 비트 각각에 대한 적어도 하나의 제 1 연산 결과 비트를 획득할 수 있다.

[0062] XOR 연산 회로는 인코딩된 두 입력(예를 들어, 제 1 변환 비트(A_1A_0) 및 제 2 변환 비트(B_1B_0))에 대한 출력(O_1O_0)에 대하여, “(10,10) → 10, (10,01) → 01, (01,10) → 01, (01,01) → 10”으로 설계된 회로일 수 있다. 즉, XOR 연산 회로는 제 1 변환 비트(A_1A_0)가 10이고, 제 2 변환 비트(B_1B_0)가 10인 경우, 10을 출력할 수 있다. XOR 연산 회로는 제 1 변환 비트(A_1A_0)가 10이고, 제 2 변환 비트(B_1B_0)가 01인 경우, 01을 출력할 수 있다. XOR 연산 회로는 제 1 변환 비트(A_1A_0)가 01이고, 제 2 변환 비트(B_1B_0)가 10인 경우, 01을 출력할 수 있다. XOR 연산 회로는 제 1 변환 비트(A_1A_0)가 01이고, 제 2 변환 비트(B_1B_0)가 01인 경우, 10을 출력할 수 있다.

[0063] XOR 연산 회로는 제 1 변환 비트(A_1A_0) 및 제 2 변환 비트(B_1B_0)가 입력되는 경우, 1 또는 0을 포함하는 제 1 출력 변환 비트를 출력하는 제 1 XOR 서브 연산 회로를 포함할 수 있다.

[0064] 제 1 XOR 서브 연산 회로는 제 1 변환 비트(A_1A_0) 중 제 1 서브 변환 비트(A_1) 및 제 2 변환 비트(B_1B_0) 중 제 2 서브 변환 비트(B_1)를 입력 받아 제 1 출력 변환 비트(O_1)를 출력할 수 있다.

[0065] XOR 연산 회로는 제 1 출력 변환 비트(O_1)가 1을 포함하는 경우, 0을 포함하는 제 2 출력 변환 비트를 출력하고, 그리고 제 1 출력 변환 비트(O_1)가 0을 포함하는 경우, 1을 포함하는 제 3 출력 변환 비트를 출력하는 제 2 XOR 서브 연산 회로를 포함할 수 있다.

[0066] 제 2 XOR 서브 연산 회로는 제 1 변환 비트(A_1A_0) 중 제 3 서브 변환 비트(A_0) 및 제 2 변환 비트(B_1B_0) 중 제 4 서브 변환 비트(B_0)를 입력 받아 제 2 출력 변환 비트(O_0)를 출력할 수 있다. XOR 연산 회로에 관한 구체적인 설명은 도 3을 참조하여 후술한다.

[0067] 본 개시의 몇몇 실시예에 따르면, 프로세서(110)는 XOR 연산 회로를 이용하여, 사전 결정된 연산 순서에 따라 적어도 하나의 변환 비트 각각에 대한 적어도 하나의 제 1 연산 결과 비트를 획득할 수 있다. 사전 결정된 연산 순서는 무작위(random)로 결정된 순서를 포함할 수 있다.

[0068] 종래의 회로는 구현의 편의성을 위해 오름차순 또는 내림차순으로 연산을 하도록 단순하게 구현된다. 이 경우 부채널 공격과 같이 알고리즘 구현상의 취약점을 노리는 공격자에게 유의미한 정보를 노출할 수 있다. 신드롬(syndrome)의 계산에서 첫 번째 XOR 연산이 키의 첫 번째 비트와 관련 있다는 사실을 공격자가 알면 부채널 공격을 통해 알아낸 값이 키의 첫 번째 비트라고 확신할 수 있다. 반면 본 발명의 일 실시예에 따른 프로세서(110)가 무작위로 결정된 순서에 따라 XOR 연산을 수행하는 경우, 공격자는 공격을 통해 알아낸 값이 키의 몇 번째 비트인지 알 수 없으므로 부채널 공격으로 인한 키 노출 위험이 줄어들 수 있다. 신드롬의 계산은 오류 검출 및 오류 정정에 도움을 주는 값을 산출하는 것을 의미할 수 있다.

[0069] 이러한 프로세서(110)가 무작위로 결정된 순서에 따라 XOR 연산을 수행하는 구성은 XOR 연산의 순서를 섞어도 본래 알고리즘이 의도했던 출력이 나오기 때문에 가능할 수 있다. 신드롬의 계산은 걸러진 키(예를 들어, 제 1 키)와 패리티 체크 행렬(Parity Check Matrix)의 이진행렬곱으로 얻을 수 있다. 패리티 체크 행렬은 선형 부호

의 패리티 검사를 나타내는 행렬일 수 있다. 패리티 체크 행렬의 각 행은 패리티 검사를 나타내는 방정식의 계수로 표시될 수 있다. 선형 부호 C의 패리티 검사 행렬을 H라고 하면, 임의의 백터 v가 C의 부호어로 되기 위한 필요 충분 조건은 $vH^T=0$으로 표시될 수 있다. 여기서 T는 전치(轉置, transpose)를 나타낼 수 있다. 이진행렬곱은 XOR 회로로 구현될 수 있다.

[0070] 프로세서(110)는 신드롬을 계산하는 데 있어 각 변환 비트를 독립적으로 처리할 수 있다. 그리고, 프로세서(110)는 적어도 하나의 제 1 연산 결과 비트를 제 1 키에 포함된 적어도 하나의 변환 비트의 순서에 대응되도록 배치할 수 있다. 따라서, 걸러진 키(예를 들어, 제 1 키)의 몇 번째 비트부터 XOR을 수행하는지는 계산결과에 영향을 미치지 않을 수 있다.

[0071] 프로세서(110)는 적어도 하나의 제 1 연산 결과 비트와 외부 기기(200)에서 XOR 연산 회로를 이용하여 제 1 키에 대응되는 제 2 키로부터 획득한 제 2 연산 결과 비트를 비교하여 제 1 키와 상기 제 2 키의 대응 여부를 결정할 수 있다.

[0072] 프로세서(110)는 제 1 키와 상기 제 2 키가 대응되지 않는 경우, 오류 정정 부호(error correcting code)를 이용하여 제 1 키를 상기 제 2 키에 대응되는 방향으로 오류를 정정할 수 있다.

[0073] 오류 정정 부호는 부호를 구성하는 비트 내에 오류가 생겼을 때 그것을 정정할 수 있는 규칙에 따라 구성된 여분의 부호일 수 있다.

[0075] 외부 기기(200)는 서버 또는 다른 컴퓨팅 장치와 상호작용 가능한 임의의 형태의 디바이스를 포함할 수 있다. 외부 기기(200)는 양자 중첩의 지수적인 정보 표현, 양자 얽힘을 이용한 병렬 연산과 같은 양자역학적인 물리현상을 활용하여 계산을 수행하는 양자 컴퓨팅 장치를 의미할 수 있다.

[0077] 네트워크는 컴퓨팅 장치(100) 및 외부 기기(200)가 서로 임의의 형태의 데이터 및 신호를 송수신할 수 있는 임의의 유무선 통신 네트워크를 포함할 수 있다. 예를 들어, 컴퓨팅 장치(100)는 네트워크를 통해 외부 기기(200)와 양자 키 교환을 할 수 있다.

[0079] 도 2는 본 개시의 몇몇 실시예에 따른 양자 회로를 설명하기 위한 도면이다.

[0080] 도 2를 참조하면, 양자 회로(10)는 단일 광자 검출기(11) 및 CNOT 게이트를 포함할 수 있다.

[0081] 양자 회로(10)는 단일 광자 검출기(11)에서 광자를 검출하는 경우, 변환 비트(A_1A_0)의 A_1에 논리신호 0이 지나가고, A_0에 논리신호 1이 지나갈 수 있다. 즉, 프로세서(110)는 양자 회로(10)를 이용하여 비트 1을 변환 비트 01로 인코딩 할 수 있다.

[0082] 양자 회로(10)는 단일 광자 검출기(11)에서 광자를 검출하지 못하는 경우, 변환 비트(A_1A_0)의 A_1에 논리신호 1이 지나가고, A_0에 논리신호 0이 지나갈 수 있다. 즉, 프로세서(110)는 양자 회로(10)를 이용하여 비트 0을 변환 비트 10으로 인코딩 할 수 있다.

[0084] 도 3은 본 개시의 몇몇 실시예에 XOR 연산 회로를 설명하기 위한 도면이다.

[0085] 도 3을 참조하면, XOR 연산 회로(20)는 제 1 서브 연산 회로(21) 및/또는 제 2 서브 연산 회로(22)를 포함할 수 있다.

[0086] 제 1 XOR 서브 연산 회로(21)는 제 1 변환 비트(A_1A_0) 중 제 1 서브 변환 비트(A_1) 및 제 2 변환 비트(B_1B_0) 중 제 2 서브 변환 비트(B_1)를 입력 받아 제 1 출력 변환 비트(O_1)를 출력할 수 있다.

[0087] 제 2 XOR 서브 연산 회로(22)는 제 1 XOR 서브 연산 회로(21)를 변경하여 제 1 출력 변환 비트(O_1)의 반대되는 값을 가지도록 사전 결정된 법칙(예를 들어, 드 모르간의 법칙 등)에 의해 변형된 회로일 수 있다.

[0088] 제 2 XOR 서브 연산 회로(22)는 제 1 변환 비트(A_1A_0) 중 제 3 서브 변환 비트(A_0) 및 제 2 변환 비트(B_1B_0) 중 제 4 서브 변환 비트(B_0)를 입력 받아 제 2 출력 변환 비트 또는 제 3 출력 변환 비트(O_0)를 출력할 수 있다.

[0089] XOR 연산 회로(20)는 제 1 변환 비트(A_1A_0)가 10이고, 제 2 변환 비트(B_1B_0)가 10인 경우, 10을 출력할 수 있다.
XOR 연산 회로(20)는 제 1 변환 비트(A_1A_0)가 10이고, 제 2 변환 비트(B_1B_0)가 01인 경우, 01을 출력할 수 있다.
XOR 연산 회로(20)는 제 1 변환 비트(A_1A_0)가 01이고, 제 2 변환 비트(B_1B_0)가 10인 경우, 01을 출력할 수 있다.
XOR 연산 회로(20)는 제 1 변환 비트(A_1A_0)가 01이고, 제 2 변환 비트(B_1B_0)가 01인 경우, 10을 출력할 수 있다.

[0091] 도 4는 본 개시의 몇몇 실시예에 따른 컴퓨팅 장치에서 양자 키 교환 시에 전력 부채널 공격을 방지하기 위한 방법을 나타내는 도면이다.

[0092] 도 4를 참조하면, 프로세서(110)는 양자 회로를 이용하여, 0 또는 1을 포함하는 비트를 10 또는 01을 포함하는 변환 비트로 인코딩할 수 있다(S110).

[0093] 프로세서(110)는 양자 회로에 포함된 단일 광자 검출기를 통해 획득되는 광자의 검출 여부에 기초하여 0 또는 1을 포함하는 비트를 10 또는 01을 포함하는 변환 비트로 인코딩할 수 있다.

[0095] 프로세서(110)는 변환 비트를 이용한 외부 기기(200)와의 양자 키 교환(Quantum Key Distribution)을 통해 적어도 하나의 변환 비트를 포함하는 제 1 키(key)를 획득할 수 있다(S120).

[0096] 프로세서(110)는 변환 비트를 이용하여 외부 기기(200)로부터 사전 결정된 기저(basis)로 부호화 된 난수 변환 비트열을 수신할 수 있다.

[0097] 프로세서(110)는 난수 변환 비트열을 분석하여 역부호화를 위한 제 1 편광 상태 정보를 획득할 수 있다.

[0098] 프로세서(110)는 제 1 편광 상태 정보를 외부 기기(200)와 공유하고, 그리고 외부 기기(200)로부터 제 1 편광 상태 정보와 사전 결정된 기저에 대응되는 제 2 편광 상태 정보를 비교하여 서로 대응되는 적어도 하나의 대응 변환 비트를 획득할 수 있다.

[0099] 프로세서(110)는 외부 기기(200)와 적어도 하나의 대응 변환 비트를 공유하고, 그리고 외부 기기(200)로부터 수신한 양자 비트 오류율(Quantum bit error rate)에 기초하여 적어도 하나의 대응 변환 비트의 선택 여부를 결정할 수 있다.

[0100] 프로세서(110)는 적어도 하나의 대응 변환 비트를 선택하기로 결정한 경우, 적어도 하나의 대응 변환 비트를 포함하는 제 1 키(key)를 획득할 수 있다.

[0102] 프로세서(110)는 10 또는 01을 출력하는 XOR 연산 회로를 이용하여, 적어도 하나의 변환 비트 각각에 대한 적어도 하나의 제 1 연산 결과 비트를 획득할 수 있다(S130).

[0103] XOR 연산 회로는 제 1 변환 비트 및 제 2 변환 비트가 입력되는 경우, 1 또는 0을 포함하는 제 1 출력 변환 비트를 출력하는 제 1 XOR 서브 연산 회로 및 제 1 출력 변환 비트가 1을 포함하는 경우, 0을 포함하는 제 2 출력 변환 비트를 출력하고, 그리고 제 1 출력 변환 비트가 0을 포함하는 경우, 1을 포함하는 제 3 출력 변환 비트를 출력하는 제 2 XOR 서브 연산 회로를 포함할 수 있다.

[0104] 프로세서(110)는 XOR 연산 회로를 이용하여, 사전 결정된 연산 순서에 따라 상기 적어도 하나의 변환 비트 각각에 대한 상기 적어도 하나의 제 1 연산 결과 비트를 획득할 수 있다. 프로세서(110)는 적어도 하나의 제 1 연산 결과 비트를 제 1 키에 포함된 상기 적어도 하나의 변환 비트의 순서에 대응되도록 배치할 수 있다. 사전 결정된 연산 순서는 무작위(random)로 결정된 순서를 포함할 수 있다.

[0106] 프로세서(110)는 적어도 하나의 제 1 연산 결과 비트와 외부 기기(200)에서 XOR 연산 회로를 이용하여 제 1 키에 대응되는 제 2 키로부터 획득한 제 2 연산 결과 비트를 비교하여 제 1 키와 제 2 키의 대응 여부를 결정할

수 있다.

[0107] 프로세서(110)는 제 1 키와 상기 제 2 키가 대응되지 않는 경우, 오류 정정 부호(error correcting code)를 이용하여 제 1 키를 상기 제 2 키에 대응되는 방향으로 오류를 정정할 수 있다.

[0109] 도 4에 도시되는 단계들은 예시적인 단계들이다. 따라서, 본 개시 내용의 사상 범위를 벗어나지 않는 한도에서 도 4의 단계들 중 일부가 생략되거나 추가적인 단계들이 존재할 수 있다는 점 또한 당업자에게 명백할 것이다. 또한, 도 4에 기재된 구성들(예를 들어, 컴퓨팅 장치(100), 외부 기기(200) 등)에 관한 구체적인 내용은 앞서 도 1 내지 도 3을 통해 설명한 내용으로 대체될 수 있다.

[0110] 도 1 내지 4를 통해 상술한 본 개시의 몇몇 실시예에 따른 컴퓨팅 장치(100)는 양자 회로를 이용하여, 0 또는 1을 포함하는 비트를 10 또는 01을 포함하는 변환 비트로 인코딩함으로써, 양자 키 교환의 모든 단계에서 발생하는 전력을 일정하게 유지시킬 수 있다. 따라서, 컴퓨팅 장치(100)는 부채널 정보를 줄여서 공격복잡도를 높일 수 있다.

[0111] 또한, 컴퓨팅 장치(100)는 전통적인 부채널 공격 대응기법과 달리 난수를 사용하지 않으므로, 난수를 얻기 어려운 IoT 환경, 임베디드 장비에 특히 유용하게 사용되어 전력 부채널 공격을 방지할 수 있다.

[0112] 또한, 컴퓨팅 장치(100)는 무작위로 결정된 순서에 따라 XOR 연산을 수행함으로써, 공격자가 공격을 통해 알아낸 값이 키의 몇 번째 비트인지 알 수 없으므로 부채널 공격으로 인한 키 노출 위험이 줄어들 수 있다.

[0114] 도 5는 본 개시의 실시예들이 구현될 수 있는 예시적인 컴퓨팅 환경에 대한 간략하고 일반적인 개략도이다.

[0115] 본 개시가 일반적으로 컴퓨팅 장치에 의해 구현될 수 있는 것으로 전술되었지만, 당업자라면 본 개시가 하나 이상의 컴퓨터 상에서 실행될 수 있는 컴퓨터 실행가능 명령어 및/또는 기타 프로그램 모듈들과 결합되어 및/또는 하드웨어와 소프트웨어의 조합으로써 구현될 수 있다는 것을 잘 알 것이다.

[0116] 일반적으로, 프로그램 모듈은 특정의 태스크를 수행하거나 특정의 추상 데이터 유형을 구현하는 루틴, 프로그램, 컴포넌트, 데이터 구조, 기타 등등을 포함한다. 또한, 당업자라면 본 개시의 방법이 단일-프로세서 또는 멀티프로세서 컴퓨터 시스템, 미니컴퓨터, 메인프레임 컴퓨터는 물론 퍼스널 컴퓨터, 핸드헬드(handheld) 컴퓨팅 장치, 마이크로프로세서-기반 또는 프로그램가능 가전 제품, 기타 등등(이들 각각은 하나 이상의 연관된 장치와 연결되어 동작할 수 있음)을 비롯한 다른 컴퓨터 시스템 구성으로 실시될 수 있다는 것을 잘 알 것이다.

[0117] 본 개시의 설명된 실시예들은 또한 어떤 태스크들이 통신 네트워크를 통해 연결되어 있는 원격 처리 장치들에 의해 수행되는 분산 컴퓨팅 환경에서 실시될 수 있다. 분산 컴퓨팅 환경에서, 프로그램 모듈은 로컬 및 원격 메모리 저장 장치 둘 다에 위치할 수 있다.

[0118] 컴퓨터는 통상적으로 다양한 컴퓨터 판독가능 매체를 포함한다. 컴퓨터에 의해 액세스 가능한 매체는 그 어떤 것이든지 컴퓨터 판독가능 매체가 될 수 있고, 이러한 컴퓨터 판독가능 매체는 휘발성 및 비휘발성 매체, 일시적(transitory) 및 비일시적(non-transitory) 매체, 이동식 및 비-이동식 매체를 포함한다. 제한이 아닌 예로서, 컴퓨터 판독가능 매체는 컴퓨터 판독가능 저장 매체 및 컴퓨터 판독가능 전송 매체를 포함할 수 있다. 컴퓨터 판독가능 저장 매체는 컴퓨터 판독가능 명령어, 데이터 구조, 프로그램 모듈 또는 기타 데이터와 같은 정보를 저장하는 임의의 방법 또는 기술로 구현되는 휘발성 및 비휘발성 매체, 일시적 및 비-일시적 매체, 이동식 및 비이동식 매체를 포함한다. 컴퓨터 판독가능 저장 매체는 RAM, ROM, EEPROM, 플래시 메모리 또는 기타 메모리 기술, CD-ROM, DVD(digital video disk) 또는 기타 광 디스크 저장 장치, 자기 카세트, 자기 테이프, 자기 디스크 저장 장치 또는 기타 자기 저장 장치, 또는 컴퓨터에 의해 액세스될 수 있고 원하는 정보를 저장하는 데 사용될 수 있는 임의의 기타 매체를 포함하지만, 이에 한정되지 않는다.

[0119] 컴퓨터 판독가능 전송 매체는 통상적으로 반송파(carrier wave) 또는 기타 전송 메커니즘(transport mechanism)과 같은 피변조 데이터 신호(modulated data signal)에 컴퓨터 판독가능 명령어, 데이터 구조, 프로그램 모듈 또는 기타 데이터 등을 구현하고 모든 정보 전달 매체를 포함한다. 피변조 데이터 신호라는 용어는 신호 내에 정보를 인코딩하도록 그 신호의 특성들 중 하나 이상을 설정 또는 변경시킨 신호를 의미한다. 제한이 아닌 예로서, 컴퓨터 판독가능 전송 매체는 유선 네트워크 또는 직접 배선 접속(direct-wired connection)과 같은 유선 매체, 그리고 음향, RF, 적외선, 기타 무선 매체와 같은 무선 매체를 포함한다. 상술된 매체들 중 임의의 것의

조합도 역시 컴퓨터 판독가능 전송 매체의 범위 안에 포함되는 것으로 한다.

[0120] 컴퓨터(1102)를 포함하는 본 개시의 여러가지 측면들을 구현하는 예시적인 환경(1100)이 나타내어져 있으며, 컴퓨터(1102)는 처리 장치(1104), 시스템 메모리(1106) 및 시스템 버스(1108)를 포함한다. 시스템 버스(1108)는 시스템 메모리(1106)(이에 한정되지 않음)를 비롯한 시스템 컴포넌트들을 처리 장치(1104)에 연결시킨다. 처리 장치(1104)는 다양한 상용 프로세서들 중 임의의 프로세서일 수 있다. 듀얼 프로세서 및 기타 멀티프로세서 아키텍처도 역시 처리 장치(1104)로서 이용될 수 있다.

[0121] 시스템 버스(1108)는 메모리 버스, 주변장치 버스, 및 다양한 상용 버스 아키텍처 중 임의의 것을 사용하는 로컬 버스에 추가적으로 상호 연결될 수 있는 몇 가지 유형의 버스 구조 중 임의의 것일 수 있다. 시스템 메모리(1106)는 판독 전용 메모리(ROM)(1110) 및 랜덤 액세스 메모리(RAM)(1112)를 포함한다. 기본 입/출력 시스템(BIOS)은 ROM, EPROM, EEPROM 등의 비휘발성 메모리(1110)에 저장되며, 이 BIOS는 시동 중과 같은 때에 컴퓨터(1102) 내의 구성요소들 간에 정보를 전송하는 일을 돕는 기본적인 루틴을 포함한다. RAM(1112)은 또한 데이터를 캐싱하기 위한 정적 RAM 등의 고속 RAM을 포함할 수 있다.

[0122] 컴퓨터(1102)는 또한 내장형 하드 디스크 드라이브(HDD)(1114)(예를 들어, EIDE, SATA)-이 내장형 하드 디스크 드라이브(1114)는 또한 적당한 섀시(도시 생략) 내에서 외장형 용도로 구성될 수 있음-, 자기 플로피 디스크 드라이브(FDD)(1116)(예를 들어, 이동식 디스켓(1118)으로부터 판독을 하거나 그에 기록을 하기 위한 것임), 및 광 디스크 드라이브(1120)(예를 들어, CD-ROM 디스크(1122)를 판독하거나 DVD 등의 기타 고용량 광 매체로부터 판독을 하거나 그에 기록을 하기 위한 것임)를 포함한다. 하드 디스크 드라이브(1114), 자기 디스크 드라이브(1116) 및 광 디스크 드라이브(1120)는 각각 하드 디스크 드라이브 인터페이스(1124), 자기 디스크 드라이브 인터페이스(1126) 및 광 드라이브 인터페이스(1128)에 의해 시스템 버스(1108)에 연결될 수 있다. 외장형 드라이브 구현을 위한 인터페이스(1124)는 USB(Universal Serial Bus) 및 IEEE 1394 인터페이스 기술 중 적어도 하나 또는 그 둘 다를 포함한다.

[0123] 이들 드라이브 및 그와 연관된 컴퓨터 판독가능 매체는 데이터, 데이터 구조, 컴퓨터 실행가능 명령어, 기타 등등의 비휘발성 저장을 제공한다. 컴퓨터(1102)의 경우, 드라이브 및 매체는 임의의 데이터를 적당한 디지털 형식으로 저장하는 것에 대응한다. 상기에서의 컴퓨터 판독가능 매체에 대한 설명이 HDD, 이동식 자기 디스크, 및 CD 또는 DVD 등의 이동식 광 매체를 언급하고 있지만, 당업자라면 집 드라이브(zip drive), 자기 카세트, 플래쉬 메모리 카드, 카트리지, 기타 등등의 컴퓨터에 의해 판독가능한 다른 유형의 매체도 역시 예시적인 운영 환경에서 사용될 수 있으며 또 임의의 이러한 매체가 본 개시의 방법들을 수행하기 위한 컴퓨터 실행가능 명령어를 포함할 수 있다는 것을 잘 알 것이다.

[0124] 운영 체제(1130), 하나 이상의 애플리케이션 프로그램(1132), 기타 프로그램 모듈(1134) 및 프로그램 데이터(1136)를 비롯한 다수의 프로그램 모듈이 드라이브 및 RAM(1112)에 저장될 수 있다. 운영 체제, 애플리케이션, 모듈 및/또는 데이터의 전부 또는 그 일부분이 또한 RAM(1112)에 캐싱될 수 있다. 본 개시가 여러가지 상업적으로 이용가능한 운영 체제 또는 운영 체제들의 조합에서 구현될 수 있다는 것을 잘 알 것이다.

[0125] 사용자는 하나 이상의 유선/무선 입력 장치, 예를 들어, 키보드(1138) 및 마우스(1140) 등의 포인팅 장치를 통해 컴퓨터(1102)에 명령 및 정보를 입력할 수 있다. 기타 입력 장치(도시 생략)로는 마이크, IR 리모콘, 조이스틱, 게임 패드, 스타일러스 펜, 터치 스크린, 기타 등등이 있을 수 있다. 이들 및 기타 입력 장치가 종종 시스템 버스(1108)에 연결되어 있는 입력 장치 인터페이스(1142)를 통해 처리 장치(1104)에 연결되지만, 병렬 포트, IEEE 1394 직렬 포트, 게임 포트, USB 포트, IR 인터페이스, 기타 등등의 기타 인터페이스에 의해 연결될 수 있다.

[0126] 모니터(1144) 또는 다른 유형의 디스플레이 장치도 역시 비디오 어댑터(1146) 등의 인터페이스를 통해 시스템 버스(1108)에 연결된다. 모니터(1144)에 부가하여, 컴퓨터는 일반적으로 스피커, 프린터, 기타 등등의 기타 주변 출력 장치(도시 생략)를 포함한다.

[0127] 컴퓨터(1102)는 유선 및/또는 무선 통신을 통한 원격 컴퓨터(들)(1148) 등의 하나 이상의 원격 컴퓨터로의 논리적 연결을 사용하여 네트워크화된 환경에서 동작할 수 있다. 원격 컴퓨터(들)(1148)는 워크스테이션, 컴퓨팅 디바이스 컴퓨터, 라우터, 퍼스널 컴퓨터, 휴대용 컴퓨터, 마이크로프로세서-기반 오락 기기, 피어 장치 또는 기타 통상의 네트워크 노드일 수 있으며, 일반적으로 컴퓨터(1102)에 대해 기술된 구성요소들 중 다수 또는 그 전부를 포함하지만, 간략함을 위해, 메모리 저장 장치(1150)만이 도시되어 있다. 도시되어 있는 논리적 연결은 근거리 통신망(LAN)(1152) 및/또는 더 큰 네트워크, 예를 들어, 원거리 통신망(WAN)(1154)에의 유선/무선 연결을

포함한다. 이러한 LAN 및 WAN 네트워킹 환경은 사무실 및 회사에서 일반적인 것이며, 인트라넷 등의 전사적 컴퓨터 네트워크(enterprise-wide computer network)를 용이하게 해주며, 이들 모두는 전세계 컴퓨터 네트워크, 예를 들어, 인터넷에 연결될 수 있다.

[0128] LAN 네트워킹 환경에서 사용될 때, 컴퓨터(1102)는 유선 및/또는 무선 통신 네트워크 인터페이스 또는 어댑터(1156)를 통해 로컬 네트워크(1152)에 연결된다. 어댑터(1156)는 LAN(1152)에의 유선 또는 무선 통신을 용이하게 해줄 수 있으며, 이 LAN(1152)은 또한 무선 어댑터(1156)와 통신하기 위해 그에 설치되어 있는 무선 액세스 포인트를 포함하고 있다. WAN 네트워킹 환경에서 사용될 때, 컴퓨터(1102)는 모뎀(1158)을 포함할 수 있거나, WAN(1154) 상의 통신 컴퓨팅 디바이스에 연결되거나, 또는 인터넷을 통하는 등, WAN(1154)을 통해 통신을 설정하는 기타 수단을 갖는다. 내장형 또는 외장형 및 유선 또는 무선 장치일 수 있는 모뎀(1158)은 직렬 포트 인터페이스(1142)를 통해 시스템 버스(1108)에 연결된다. 네트워크화된 환경에서, 컴퓨터(1102)에 대해 설명된 프로그램 모듈들 또는 그의 일부분이 원격 메모리/저장 장치(1150)에 저장될 수 있다. 도시된 네트워크 연결이 예시적인 것이며 컴퓨터들 사이에 통신 링크를 설정하는 기타 수단이 사용될 수 있다는 것을 잘 알 것이다.

[0129] 컴퓨터(1102)는 무선 통신으로 배치되어 동작하는 임의의 무선 장치 또는 개체, 예를 들어, 프린터, 스캐너, 데스크톱 및/또는 휴대용 컴퓨터, PDA(portable data assistant), 통신 위성, 무선 검출가능 태그와 연관된 임의의 장비 또는 장소, 및 전화와 통신을 하는 동작을 한다. 이것은 적어도 Wi-Fi 및 블루투스 무선 기술을 포함한다. 따라서, 통신은 종래의 네트워크에서와 같이 미리 정의된 구조이거나 단순하게 적어도 2개의 장치 사이의 애드혹 통신(ad hoc communication)일 수 있다.

[0130] Wi-Fi(Wireless Fidelity)는 유선 없이도 인터넷 등으로의 연결을 가능하게 해준다. Wi-Fi는 이러한 장치, 예를 들어, 컴퓨터가 실내에서 및 실외에서, 즉 기지국의 통화권 내의 아무 곳에서나 데이터를 전송 및 수신할 수 있게 해주는 셀 전화와 같은 무선 기술이다. Wi-Fi 네트워크는 안전하고 신뢰성 있으며 고속인 무선 연결을 제공하기 위해 IEEE 802.11(a, b, g, 기타)이라고 하는 무선 기술을 사용한다. 컴퓨터를 서로에, 인터넷에 및 유선 네트워크(IEEE 802.3 또는 이더넷을 사용함)에 연결시키기 위해 Wi-Fi가 사용될 수 있다. Wi-Fi 네트워크는 비인가 2.4 및 5GHz 무선 대역에서, 예를 들어, 11Mbps(802.11a) 또는 54 Mbps(802.11b) 데이터 레이트로 동작하거나, 양 대역(듀얼 대역)을 포함하는 제품에서 동작할 수 있다.

[0131] 본 개시의 기술 분야에서 통상의 지식을 가진 자는 정보 및 신호들이 임의의 다양한 상이한 기술들 및 기법들을 이용하여 표현될 수 있다는 것을 이해할 것이다. 예를 들어, 위의 설명에서 참조될 수 있는 데이터, 지시들, 명령들, 정보, 신호들, 비트들, 심볼들 및 칩들은 전압들, 전류들, 전자기파들, 자기장들 또는 입자들, 광학장들 또는 입자들, 또는 이들의 임의의 결합에 의해 표현될 수 있다.

[0132] 본 개시의 기술 분야에서 통상의 지식을 가진 자는 여기에 개시된 실시예들과 관련하여 설명된 다양한 예시적인 논리 블록들, 모듈들, 프로세서들, 수단들, 회로들 및 알고리즘 단계들이 전자 하드웨어, (편의를 위해, 여기에서 소프트웨어로 지칭되는) 다양한 형태들의 프로그램 또는 설계 코드 또는 이들 모두의 결합에 의해 구현될 수 있다는 것을 이해할 것이다. 하드웨어 및 소프트웨어의 이러한 상호 호환성을 명확하게 설명하기 위해, 다양한 예시적인 컴포넌트들, 블록들, 모듈들, 회로들 및 단계들이 이들의 기능과 관련하여 위에서 일반적으로 설명되었다. 이러한 기능이 하드웨어 또는 소프트웨어로서 구현되는지 여부는 특정한 애플리케이션 및 전체 시스템에 대하여 부과되는 설계 제약들에 따라 좌우된다. 본 개시의 기술 분야에서 통상의 지식을 가진 자는 각각의 특정한 애플리케이션에 대하여 다양한 방식들로 설명된 기능을 구현할 수 있으나, 이러한 구현 결정들은 본 개시의 범위를 벗어나는 것으로 해석되어서는 안 될 것이다.

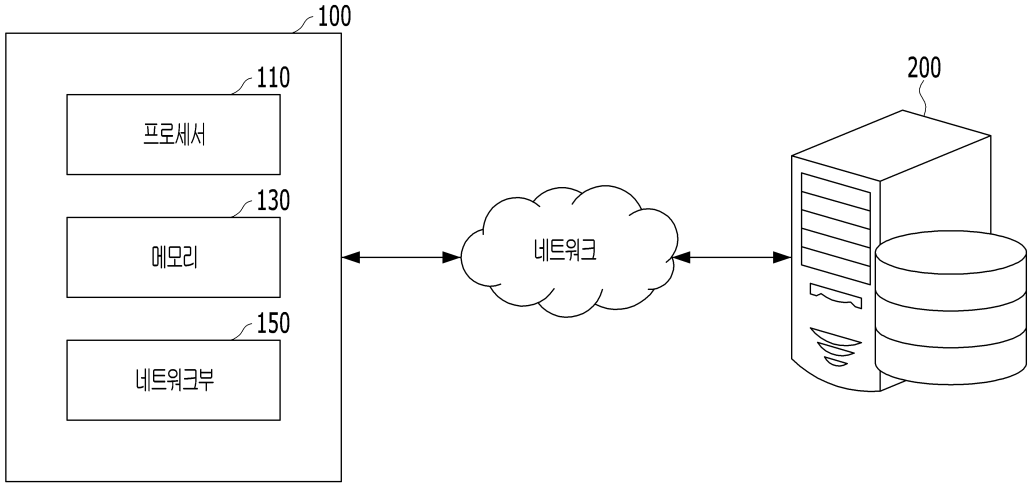
[0133] 여기서 제시된 다양한 실시예들은 방법, 장치, 또는 표준 프로그래밍 및/또는 엔지니어링 기술을 사용한 제조 물품(article)으로 구현될 수 있다. 용어 제조 물품은 임의의 컴퓨터-판독가능 저장장치로부터 액세스 가능한 컴퓨터 프로그램, 캐리어, 또는 매체(media)를 포함한다. 예를 들어, 컴퓨터-판독가능 저장매체는 자기 저장 장치(예를 들면, 하드 디스크, 플로피 디스크, 자기 스트립, 등), 광학 디스크(예를 들면, CD, DVD, 등), 스마트 카드, 및 플래쉬 메모리 장치(예를 들면, EEPROM, 카드, 스틱, 키 드라이브, 등)를 포함하지만, 이들로 제한되는 것은 아니다. 또한, 여기서 제시되는 다양한 저장 매체는 정보를 저장하기 위한 하나 이상의 장치 및/또는 다른 기계-판독가능한 매체를 포함한다.

[0134] 제시된 프로세스들에 있는 단계들의 특정한 순서 또는 계층 구조는 예시적인 접근들의 일례임을 이해하도록 한다. 설계 우선순위들에 기반하여, 본 개시의 범위 내에서 프로세스들에 있는 단계들의 특정한 순서 또는 계층 구조가 재배열될 수 있다는 것을 이해하도록 한다. 첨부된 방법 청구항들은 샘플 순서로 다양한 단계들의 엘리먼트들을 제공하지만 제시된 특정한 순서 또는 계층 구조에 한정되는 것을 의미하지는 않는다.

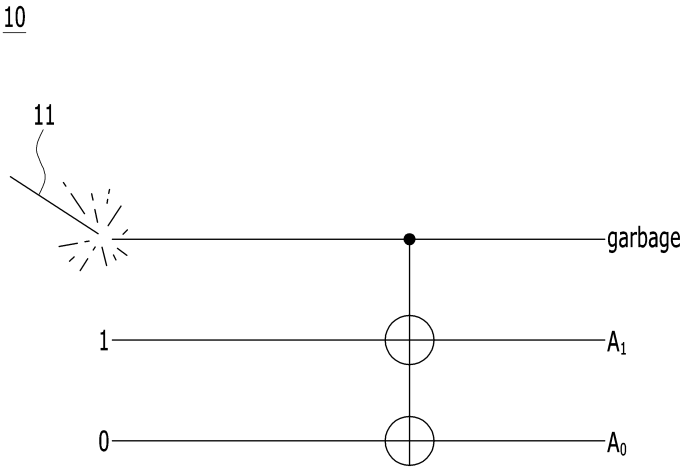
[0135] 제시된 실시예들에 대한 설명은 임의의 본 개시의 기술 분야에서 통상의 지식을 가진 자가 본 개시를 이용하거나 또는 실시할 수 있도록 제공된다. 이러한 실시예들에 대한 다양한 변형들은 본 개시의 기술 분야에서 통상의 지식을 가진 자에게 명백할 것이며, 여기에 정의된 일반적인 원리들은 본 개시의 범위를 벗어남이 없이 다른 실시예들에 적용될 수 있다. 그리하여, 본 개시는 여기에 제시된 실시예들로 한정되는 것이 아니라, 여기에 제시된 원리들 및 신규한 특징들과 일관되는 최광의의 범위에서 해석되어야 할 것이다.

도면

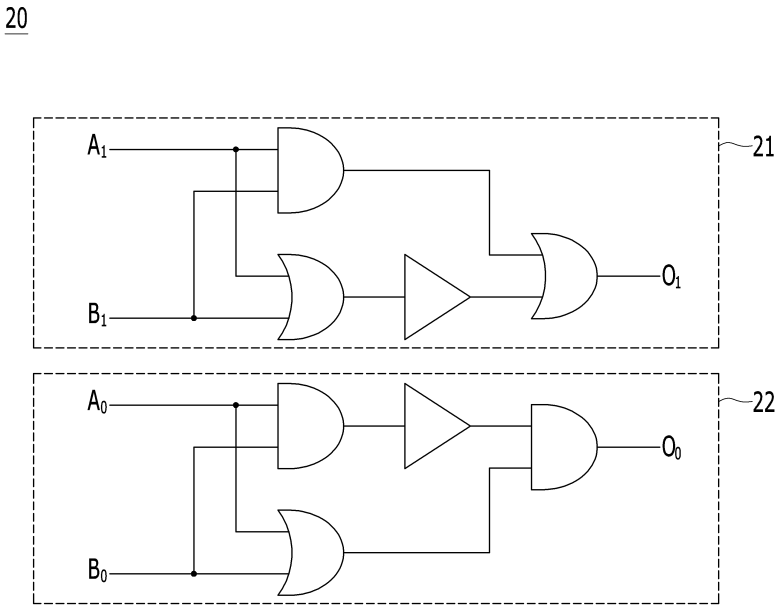
도면1



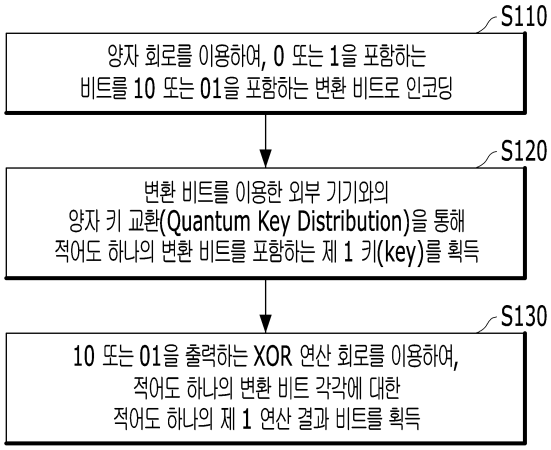
도면2



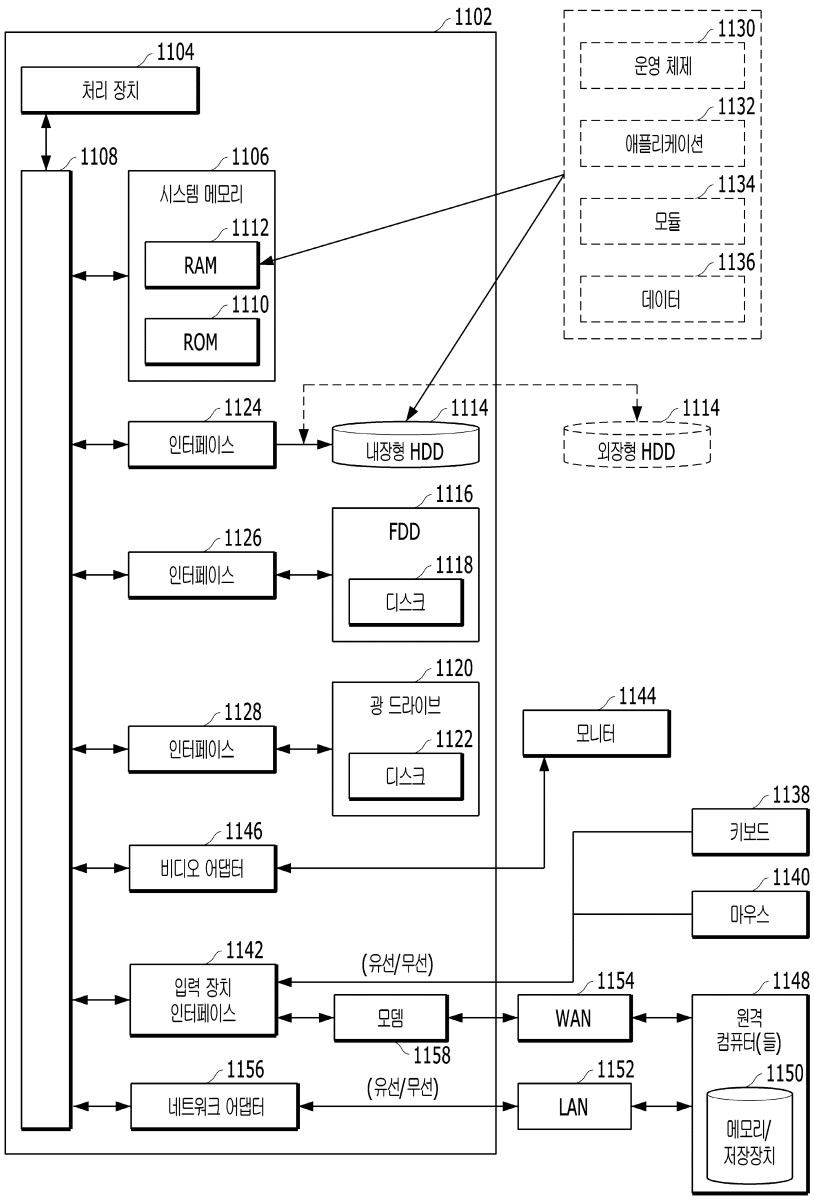
도면3


20
A1
B1
O1
21
A0
B0
O0
22

도면4


S110
양자 회로를 이용하여, 0 또는 1을 포함하는
비트를 10 또는 01을 포함하는 변환 비트로 인코딩
S120
변환 비트를 이용한 외부 기기와의
양자 키 교환(Quantum Key Distribution)을 통해
적어도 하나의 변환 비트를 포함하는 제 1 키(key)를 획득
S130
10 또는 01을 출력하는 XOR 연산 회로를 이용하여,
적어도 하나의 변환 비트 각각에 대한
적어도 하나의 제 1 연산 결과 비트를 획득

도면5


1102
1104
처리 장치
1108
1106
시스템 메모리
1112
RAM
1110
ROM
1130
운영 체제
1132
애플리케이션
1134
모듈
1136
데이터
1124
인터페이스
1114
내장형 HDD
1114
외장형 HDD
1116
FDD
1118
디스크
1126
인터페이스
1120
광 드라이브
1122
디스크
1128
인터페이스
1144
모니터
1138
키보드
1140
마우스
1146
비디오 어댑터
1142
입력 장치 인터페이스
(유선/무선)
모뎀
1158
1154
WAN
1148
원격 컴퓨터(들)
1150
메모리/ 저장장치
1156
네트워크 어댑터
(유선/무선)
1152
LAN