(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2018-0041190
(43) 공개일자 2018년04월23일

(51) 국제특허분류(Int. Cl.)
H04L 9/08 (2006.01) *H04L 9/32* (2006.01)
(52) CPC특허분류
H04L 9/0852 (2013.01)
H04L 9/3226 (2013.01)
(21) 출원번호 10-2018-7007490
(22) 출원일자(국제) 2016년08월17일
심사청구일자 없음
(85) 번역문제출일자 2018년03월15일
(86) 국제출원번호 PCT/US2016/047398
(87) 국제공개번호 WO 2017/031228
국제공개일자 2017년02월23일
(30) 우선권주장
201510509537.5 2015년08월18일 중국(CN)

(71) 출원인
알리바바 그룹 홀딩 리미티드
케이만군도, 그랜드 케이만, 피오박스 847, 원 캐피탈 플레이스 4층
(72) 발명자
푸, 잉팡
중국 311121 항저우 위 항 디스트릭트 웨스트 원 이 로드 넘버 969 빌딩 3 5층 알리바바 그룹 리갈 디파트먼트
(74) 대리인
양영준, 백만기

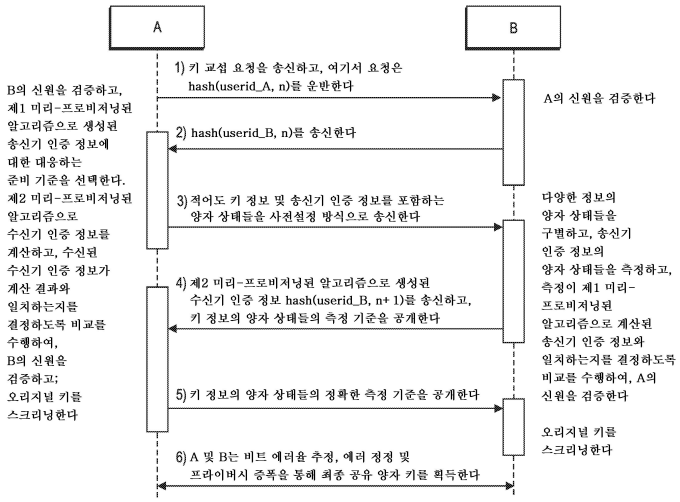
전체 청구항 수 : 총 20 항

(54) 발명의 명칭 **양자 키 분배 프로세스에서 사용되는 인증 방법, 장치 및 시스템**

(57) 요 약

본 출원은 QKD 프로세스에서 사용되는 인증 방법을 개시하고, 인증 시스템 뿐만 아니라 추가의 인증 방법 및 대응하는 장치들을 추가로 개시한다. 이 방법은, 기준 선택 룰에 따라 송신기에 의해, 제1 미리-프로비저닝된 알고리즘으로 생성되고 동적으로 변화하는 송신기 인증 정보에 대한 준비의 기준을 선택하는 단계, 키 정보 및 송신기 인증 정보를 포함하는 양자 상태들을 송신하는 단계, 기준 선택 룰에 따라 송신기 인증 정보의 양자 상태들을 수신기에 의해 측정하는 단계, 및 측정 결과가 제1 미리-프로비저닝된 알고리즘으로 계산된 대응하는 정보와 일치하지 않으면, QKO 프로세스를 종료하는 단계를 포함한다.

대 표 도



명 세 서

청구범위

청구항 1

양자 키 분배(QKD; quantum key distribution) 프로세스에서 사용되는 인증 방법으로서, 상기 프로세스는,

상기 QKD 프로세스에 참여하는 송신기에 의해, 기준 선택 룰(rule)에 따라 송신기 신원 정보를 인증하기 위한 준비 기준을 선택하는 단계;

키 정보 및 상기 송신기 인증 정보를 포함하는 복수의 양자 상태들을 송신하는 단계 - 상기 송신기 인증 정보는 제1 미리-프로비저닝된(pre-provisioned) 알고리즘으로 생성됨 -;

상기 QKD 프로세스에 참여하는 수신기에 의해, 상기 복수의 양자 상태들을 구별하는 단계;

상기 기준 선택 룰에 따라 상기 송신기 인증 정보를 포함하는 상기 복수의 양자 상태들을 측정하는 단계;

상기 송신기에 의해, 제1 미리-프로비저닝된 알고리즘을 사용하여 송신기 인증 정보를 계산하는 단계;

상기 측정된 복수의 양자 상태들과, 상기 제1 미리-프로비저닝된 알고리즘을 사용하여 계산된 상기 송신기 인증 정보를 비교하는 단계;

상기 측정된 복수의 양자 상태들이 상기 제1 미리-프로비저닝된 알고리즘을 사용하여 계산된 상기 송신기 인증 정보와 일치할 때, 상기 송신기가 인증된 것으로 결정하는 단계;

상기 측정된 복수의 양자 상태들이 상기 제1 미리-프로비저닝된 알고리즘을 사용하여 계산된 상기 송신기 인증 정보와 일치하지 않을 때, 상기 송신기가 인증되지 않은 것으로 결정하는 단계; 및

상기 측정된 복수의 양자 상태들이 상기 제1 미리-프로비저닝된 알고리즘을 사용하여 계산된 상기 송신기 인증 정보와 일치하지 않을 때, 상기 QKD 프로세스를 종료하는 단계

를 포함하고,

상기 제1 미리-프로비저닝된 알고리즘으로 생성된 상기 송신기 인증 정보는 상기 수신기를 향해 개시된 상이한 QKD 프로세스들에서 동적으로 변화하는 인증 방법.

청구항 2

제1항에 있어서, 상기 송신기가 인증된 것으로 결정하는 단계는,

상기 수신기에 의해, 제2 미리-프로비저닝된 알고리즘으로 수신기 인증 정보를 생성하는 단계;

상기 수신기 인증 정보를 상기 송신기로 송신하는 단계;

상기 송신기에 의해, 상기 제2 미리-프로비저닝된 알고리즘으로 수신기 인증 정보를 계산하는 단계;

상기 수신기에 의해 생성된 상기 수신기 인증 정보와 상기 송신기에 의해 계산된 수신기 인증 정보를 비교하는 단계;

상기 수신기에 의해 생성된 상기 수신기 인증 정보가 상기 송신기에 의해 계산된 수신기 인증 정보와 일치할 때, 상기 수신기가 인증된 것으로 결정하는 단계;

상기 수신기에 의해 생성된 상기 수신기 인증 정보가 상기 송신기에 의해 계산된 수신기 인증 정보와 일치하지 않을 때, 상기 수신기가 인증되지 않은 것으로 결정하는 단계; 및

상기 수신기에 의해 생성된 상기 수신기 인증 정보가 상기 송신기에 의해 계산된 수신기 인증 정보와 일치하지 않을 때, 상기 QKD 프로세스를 종료하는 단계

를 더 포함하는 인증 방법.

청구항 3

제2항에 있어서, 상기 송신기가 인증된 것으로 결정하는 단계는,

상기 키 정보의 상기 수신된 양자 상태들을 측정하기 위한 측정 기준을 랜덤하게 선택하는 단계;

미리-결정된 채널을 통해 상기 측정 기준을 공개하는 단계;

상기 키 정보의 상기 양자 상태들의 정확한 측정 기준을 결정하는 단계;

오리지널(original) 키를 스크리닝(screening)하는 단계;

상기 미리-결정된 채널을 통해 상기 키 정보의 상기 양자 상태들의 상기 정확한 측정 기준을 공개하는 단계;

상기 수신기에 의해 오리지널 키를 스크리닝하는 단계; 및

상기 송신기 및 상기 수신기에 의해, 비트 에러율 추정, 에러 정정 및 프라이버시(privacy) 증폭 프로세스들을 통해 최종 공유 양자 키를 획득하는 단계

를 더 포함하는 인증 방법.

청구항 4

제2항에 있어서, 상기 제1 미리-프로비저닝된 알고리즘은, 상기 송신기 및 상기 수신기 둘 다에 의해, 사전설정(preset) 정책에 따라 동기적으로 변하는 파라미터 및 송신기 식별 정보에 따라 상기 송신기 인증 정보를 계산함으로써 수행되고, 상기 수신기측의 상기 송신기 식별 정보는 미리-결정된 채널을 통해 상기 송신기에 의해 상기 수신기로 전송되거나 또는 미리-프로비저닝되는 인증 방법.

청구항 5

제4항에 있어서, 준비의 기준을 선택하는 단계는,

상기 송신기 및 상기 수신기 둘 다에 의해, 상기 미리-결정된 채널을 통해 실행되는 상호 작용을 개시하는 요청 동안 상기 사전설정 정책에 따라 상기 동기적으로 변하는 파라미터로 상대방의 피어(peer) 디바이스에 대한 인증 프로세스를 수행하는 단계; 및

어느 디바이스가 상기 인증에 실패하면 상기 QKD 프로세스를 개시하지 않는 단계

를 더 포함하는 인증 방법.

청구항 6

제2항에 있어서, 상기 제2 미리-프로비저닝된 알고리즘은, 상기 송신기 및 상기 수신기 둘 다에 의해, 사전설정 정책에 따라 상기 동기적으로 변하는 파라미터의 변형 및 수신기 식별 정보에 따라 상기 수신기 인증 정보를 계산함으로써 수행되고, 상기 송신기측의 상기 수신기 식별 정보는 미리-결정된 채널을 통해 상기 수신기에 의해 상기 송신기로 전송되거나 또는 미리-프로비저닝되는 인증 방법.

청구항 7

제6항에 있어서, 상기 사전설정 정책에 따라 상기 동기적으로 변하는 파라미터의 상기 변형은, 상기 파라미터 그 자체, 및 사전설정 수학적 변환 방법으로 상기 파라미터를 프로세싱하는 것으로부터 얻어지는 결과 중 적어도 하나를 포함하는 인증 방법.

청구항 8

제4항에 있어서, 상기 송신기 및 상기 수신기 둘 다에 의해 상기 사전설정 정책에 따라 동기적으로 변하는 파라미터는, 상기 송신기 및 상기 수신기가 상기 QKD 프로세스들을 수행하는 횟수를 포함하는 인증 방법.

청구항 9

제4항에 있어서, 상기 인증 정보를 계산하는 단계는 해시 함수(hash function)로 대응하는 인증 정보를 계산하는 단계를 포함하는 인증 방법.

청구항 10

제1항에 있어서, 키 정보 및 상기 송신기 인증 정보를 포함하는 양자 상태들을 송신하는 단계는, 사전설정 정보 포맷으로 각각 상이한 파장들로 제어 정보 및 데이터 정보의 양자 상태들을 송신하는 단계를 포함하며, 상기 데이터 정보는 상기 키 정보 및 상기 송신기 인증 정보를 포함하는 인증 방법.

청구항 11

제10항에 있어서, 상기 사전설정 정보 포맷은, 상기 인증 정보 및 상기 키 정보에 대한 프리픽스(prefix)들로서 제어 정보를 사용하는 것을 포함하는 인증 방법.

청구항 12

제11항에 있어서, 상기 인증 정보의 상기 프리픽스로서 사용되는 상기 제어 정보의 양자 상태들을 전달하는 파장은, 상기 키 정보의 상기 프리픽스로서 사용되는 상기 제어 정보의 양자 상태들을 전달하는 파장과 다른 인증 방법.

청구항 13

제11항에 있어서, 상기 사전설정 정보 포맷은, 상기 인증 정보의 상기 프리픽스로서 사용되는 상기 제어 정보와, 상이한 코드들을 갖는 상기 키 정보의 상기 프리픽스로서 사용되는 상기 제어 정보를 포함하고, 상기 상이한 코드들은 상기 송신기 및 상기 수신기에 의해 사전설정되거나, 또는 미리-결정된 채널을 통한 교섭을 통해 결정되고,

준비를 위한 기준 및 제어 정보의 양자 상태들을 측정하기 위한 기준 중 적어도 하나는 상기 송신기 및 상기 수신기에 의해 사전설정되거나, 또는 미리-결정된 채널을 통한 교섭을 통해 결정되는 인증 방법.

청구항 14

제10항에 있어서, 상기 사전설정 정보 포맷은, 상기 인증 정보 및 상기 키 정보의 프리픽스로서 공통 제어 정보를 사용하는 것을 포함하고, 상기 제어 정보와 상기 키 정보 간의 상기 인증 정보의 길이는 상기 송신기 및 상기 수신기에 의해 사전설정되거나, 또는 미리-결정된 채널을 통한 교섭을 통해 결정되는 인증 방법.

청구항 15

QKD 프로세스에서 사용되는 인증 장치로서,

제1 미리-프로비저닝된 알고리즘으로 송신기 인증 정보를 생성하도록 구성된 송신기 신원 정보 생성 유닛 - 상기 송신기 인증 정보는 수신기를 향해 개시된 상이한 QKD 프로세스들에서 동적으로 변화함 -;

상기 QKD 프로세스에 참여하는 피어 디바이스와 합의된 기준 선택 룰에 따라 상기 송신기 인증 정보에 대한 준비의 기준을 선택하도록 구성된 준비의 기준 선택 유닛; 및

적어도 키 정보와 상기 송신기 인증 정보를 포함하는 양자 상태들을 상기 피어 디바이스에 사전설정 방식으로 송신하도록 구성된 양자 상태들 송신 유닛

을 포함하고,

상기 장치는 QKD 프로세스에 참여하는 양자 통신 송신기 디바이스에 배치되는 인증 장치.

청구항 16

제16항에 있어서, 상기 장치는,

상기 양자 상태들 송신 유닛이 상기 양자 상태들 송신 동작을 완료한 후에 상기 피어 디바이스에 의해 리턴된(returned) 정보를 수신하도록 구성된 수신기 신원 정보 수신 유닛 - 상기 정보는 적어도 수신기 인증 정보를 포함함 -;

제2 미리-프로비저닝된 알고리즘으로 수신기 인증 정보를 계산하도록 구성된 수신기 신원 정보 계산 유닛; 및

수신된 상기 수신기 인증 정보가 상기 계산 결과와 일치할 때 상기 수신기가 인증된 것으로 결정하고, 그렇지 않으면 상기 수신기가 인증되지 않은 것으로 결정하고 상기 QKD 프로세스를 종료하도록 더 구성된 수신기 인증 유닛

을 더 포함하는 인증 장치.

청구항 17

제16항에 있어서,

상기 수신기 인증 유닛이 상기 수신기가 인증된 것으로 결정한 후에, 상기 키 정보의 상기 양자 상태들에 대한 정확한 측정 기준을 결정하고, 상기 오리지널 키를 스크리닝하도록 구성된 오리지널 키 스크리닝 유닛;

미리-결정된 채널을 통해 상기 키 정보의 상기 양자 상태들에 대한 상기 정확한 측정 기준을 공개하도록 구성된 정확한 측정 기준 공개 유닛; 및

비트 에러율 추정, 에러 정정 및 프라이버시 증폭 프로세스들을 통해 최종 공유 양자 키를 획득하도록 구성된 공유 양자 키 생성 유닛

을 더 포함하고,

상기 수신기 신원 정보 수신 유닛에 의해 수신된 상기 정보는, 상기 키 정보의 양자 상태들을 측정하기 위해 상기 피어 디바이스에 의해 사용되는 측정 기준을 더 포함하는 인증 장치.

청구항 18

QKD 프로세스에서 사용되는 인증 장치로서,

상기 QKD 프로세스에 참여하는 피어 디바이스에 의해 전송된 양자 상태들을 수신하고, 상기 피어 디바이스의 것과 동일한 사전설정 방식으로 다양한 정보의 상기 수신된 양자 상태들을 구별하도록 구성된 양자 상태들 수신 및 구별 유닛;

상기 피어 디바이스에 의해 사용된 제1 미리-프로비저닝된 알고리즘으로 송신기 인증 정보를 계산하도록 구성된 송신기 신원 정보 계산 유닛;

상기 피어 디바이스의 것과 동일한 기준 선택 룰에 따라 측정 기준을 선택하고, 송신기 인증 정보의 수신된 복수의 양자 상태들을 측정하도록 구성된 신원 정보 양자 상태들 측정 유닛; 및

수신된 복수의 양자 상태들이 상기 계산된 송신기 인증 정보와 일치하는지를 결정하고, 상기 측정 결과가 일치할 때 송신기가 인증된 것으로 결정하고, 그렇지 않으면 상기 송신기가 인증되지 않은 것으로 결정하고 상기 QKD 프로세스를 종료하도록 구성된 송신기 인증 유닛

을 포함하고,

상기 장치는 QKD 프로세스에 참여하는 양자 통신 수신기 디바이스에 배치되는 인증 장치.

청구항 19

제18항에 있어서, 상기 장치는,

상기 송신기 인증 유닛이 상기 송신기가 인증된 것으로 결정한 후에, 상기 피어 디바이스에 의해 사용되는 제2 미리-프로비저닝된 알고리즘으로 수신기 인증 정보를 생성하도록 구성된 수신기 신원 정보 생성 유닛; 및

상기 피어 디바이스로 상기 수신기 인증 정보를 송신하도록 구성된 수신기 신원 정보 송신 유닛

을 더 포함하는 인증 장치.

청구항 20

제19항의 상기 QKD 프로세스에서 사용되는 인증 장치로서, 상기 장치는,

상기 송신기 인증 유닛이 상기 송신기가 인증된 것으로 결정한 후에, 키 정보의 수신된 양자 상태들을 측정하기 위한 측정 기준을 랜덤하게 선택하고, 미리-결정된 채널을 통해 상기 측정 기준을 공개하도록 구성된 키 정보 양자 상태들 측정 기준 공개 유닛;

상기 미리-결정된 채널을 통해 상기 피어 디바이스에 의해 전송된 상기 키 정보의 상기 양자 상태들의 정확한 측정 기준을 수신하도록 구성된 정확한 측정 기준 수신 유닛; 및

오리지널 키를 스크리닝하고, 비트 에러율 추정, 에러 정정 및 프라이버시 증폭 프로세스들을 통해 최종 공유 양자 키를 획득하도록 구성된 스크리닝 및 공유 양자 키 생성 유닛

을 더 포함하는 인증 장치.

발명의 설명

기 술 분 야

[0001] 본 출원은 2015년 8월 18일에 출원된 푸, 잉팡(Fu, Yingfang)의 중국 특허 출원 제201510509537.5호의 이익을 주장하며, 이는 본원에 참조되어 전체적으로 통합된다.

[0002] 본 출원은 인증의 기술 분야, 특히 양자 키 분배(QKD; quantum key distribution) 프로세스를 위한 인증 방법에 관한 것이다. 본 발명은 또한 QKD 프로세스를 위한 인증 시스템에 관한 것이다.

배 경 기 술

[0003] 인증은 네트워크 보안을 확실하게 하는 중요한 부분이고; 효과적인 인증은 두 통신 당사자의 진위성, 메시지의 무결성 및 소스의 신뢰성을 보장할 수 있으며, 또한 위조, 수정 및 지연과 같은 수단을 통해 불법적인 당사자에 의한 공격으로부터 정보를 보호할 수 있다. 개인 키 암호 기법(cryptography) 메커니즘과 공개 키 암호 기법 메커니즘은 둘 다, 통신에서 신원 정보의 보안, 무결성, 및 부인 봉쇄(non-repudiation)를 확실하게 하고, 신원 스푸핑(spoofing) 공격에 저항하기 위해 암호 기법에 보통 사용된다. 양자 암호 기법은 양자 역학과 암호 기법의 합동 제품이며 향상된 보안 및 도청 탐지 능력을 제공하는 것으로 입증되었다. 양자 암호 기법은 양자 역학의 기본 원리를 채용하며, 공격자의 컴퓨팅 능력과 저장 용량과는 관계가 없다. 그러나, 종래의 QKD 프로토콜은 효과적인 인증 메커니즘을 제공하지 않으므로, QKD 프로세스는 여전히 스푸핑 공격, 중간자(man-in-the-middle) 공격 또는 분산 서비스 거부(DDoS) 공격을 받을 수 있다.

[0004] 상술한 문제점의 관점에서, 종래 기술은 다음의 두 가지 솔루션을 제공한다:

[0005] i. M.Dusek 등은 양자 통신 프로세스에서 모든 미리-결정된 정보를 인증할 필요가 없다는 믿음을 특징으로 하는 하나의 솔루션이다. M.Dusek에 따르면, 양자 상태의 에러율의 정확한 결정에 영향을 주는 미리-결정된 정보만이 인증되어야 하고, 다른 모든 미리-결정된 정보는 인증될 필요가 없다. 결과적으로, M.Dusek은 미리-결정된 메시지 인증 알고리즘과 결합하여 양자 인증 프로토콜을 제안하며, 프로토콜의 본질은 미리-결정된 인증 알고리즘으로 가능한 적은 미리-결정된 메시지를 인증하는 것이다.

[0006] ii. 다른 제안된 솔루션은 인증과 BB84 프로토콜을 결합한다. 이 프로토콜은, 랜덤하게 전송된 양자 비트열의 일부 비트가 특정 인증 비트로서 설정되고, 인증 비트의 특정 위치가 인증 키에 의해 결정되며, 두 통신 당사자 간의 인증이 인증 비트의 비트에 의해 표현되는 광자의 편광 상태 및 측정 기준으로 달성되고, 인증 비트의 양자 상태 정보는 랜덤하게 전송될 수 없으며 특정 룰(rule)에 따라 두 당사자 간에 공유되는 인증 키에 의해 결정되어야 한다는 점에서 오리지널 BB84 프로토콜과 다르다. 송신기 및 수신기는 각 교섭에 의해 획득된 공유 양자 키의 일부를 인증 키로서 설정하여 인증 키의 동적 갱신을 실현한다.

[0007] 상술한 2가지 솔루션은, 둘 다 인증 메커니즘을 채택하기 때문에 QKD 프로세스의 보안을 어느 정도 향상시킬 수 있지만 각각 특정 결함을 갖는다.

[0008] i. M.Dusek 솔루션의 경우, 두 통신 당사자 간에 미리-프로비저닝된(pre-provisioned) 인증 키의 수가 제한되어 있으며, 이 솔루션은 여전히 양자 기술의 이점을 최대한 활용하지 않으면서 미리-결정된 인증 기술을 채택하여, 이 솔루션은 해킹의 위험을 물려 받고 스푸핑 공격, 중간자 공격 및 DDoS 공격에 취약하다.

[0009] ii. 인증이 있는 BB84 프로토콜의 경우, 인증 정보가 키 분배의 보안을 향상시키기 위해 양자 상태의 형태로 전송되더라도, 이 기술적 솔루션은 각 교섭에 의해 획득된 공유 양자 키의 일부를 인증 키로서 선택할 것을 요구하므로, 공유 양자 키의 그 부분은 더 이상 서비스 데이터 암호화에 사용될 수 없고, 양자 키 리소스는 낭비된다.

발명의 내용

해결하려는 과제

과제의 해결 수단

[0010] 본 출원의 실시예들은 QKD 프로세스에서 사용되는 인증 방법을 제공하고, 이는 QKD 프로세스에서 동적 인증을 수행하기 위한 새로운 아이디어를 제공할 뿐만 아니라, 취약성 및 양자 키 리소스 낭비의 문제를 효과적으로 해결할 수 있다. 본 출원의 실시예들은 QKD 프로세스에서 사용되는 다른 2개의 인증 방법들 및 대응하는 장치들, 및 QKD 프로세스에서 사용되는 인증 시스템을 더 제공한다.

[0011] 본 출원은 QKD 프로세스에서 사용되는 인증 방법을 제공하며, 이 방법은 QKD 프로세스에 참여하는 양자 통신 송신기 디바이스 및 양자 통신 수신기 디바이스에서 구현된다. 일 실시예에서, 이 방법은,

[0012] 송신기에 의해, 수신기와 합의된 기준 선택 룰에 따라 송신기 신원 정보를 인증하기 위한 준비의 기준을 선택하고, 적어도 키 정보 및 송신기 인증 정보를 포함하는 양자 상태들을 사전설정(preset) 방식으로 송신하는 단계 - 상기 송신기 인증 정보는 제1 미리-프로비저닝된 알고리즘으로 생성됨 -; 및

[0013] 수신기에 의해, 사전설정 방식으로 다양한 정보의 수신된 양자 상태들을 필터링하고 (또는 구별하고), 기준 선택 룰에 따라 송신기 인증 정보의 수신된 양자 상태들을 측정하고, 측정 결과가 제1 미리-프로비저닝된 알고리즘에 따라 계산된 송신기 인증 정보와 일치하면, 송신기가 인증된 것으로 결정하고; 그렇지 않으면, 송신기가 인증되지 않은 것으로 결정하고 QKD 프로세스를 종료하는 단계를 포함하고,

[0014] 제1 미리-프로비저닝된 알고리즘으로 생성된 송신기 인증 정보는 수신기를 향해 개시된 상이한 QKD 프로세스들에서 동적으로 변화한다.

[0015] 일 실시예에서, 송신기가 인증된 것으로 (수신기에서) 결정한 후에 다음 동작들이 수행된다:

[0016] 수신기에 의해, 제2 미리-프로비저닝된 알고리즘으로 수신기 인증 정보를 생성하고, 수신기 인증 정보를 송신하는 동작; 및

[0017] 송신기에서, 제2 미리-프로비저닝된 알고리즘으로 수신기 인증 정보를 계산하고, 수신된 수신기 인증 정보가 계산 결과와 일치할 때 수신기가 인증된 것으로 결정하고; 그렇지 않으면, 수신기가 인증되지 않은 것으로 결정하고 QKD 프로세스를 종료하는 동작.

[0018] 일 실시예에서, 수신기는 송신기가 인증된 것으로 결정한 후에 다음 동작들을 더 수행한다:

[0019] 키 정보의 수신된 양자 상태들을 측정하기 위한 측정 기준을 랜덤하게 선택하고, 미리-결정된 채널을 통해 측정 기준을 공개하는 동작; 및

[0020] 대응하여, 수신기가 인증된 것으로 결정한 후에, 송신기는 다음 동작들을 수행한다:

[0021] 키 정보의 양자 상태들의 정확한 측정 기준을 결정하고, 오리지널 키를 스크리닝하는 동작; 및

[0022] 미리-결정된 채널을 통해 키 정보의 양자 상태들의 정확한 측정 기준을 공개하는 동작; 및

[0023] 대응하여, 송신기에 의해 키 정보의 양자 상태들의 정확한 측정 기준을 공개하는 단계 후에, 다음 동작들이 수행된다:

[0024] 수신기에 의해 오리지널 키를 스크리닝하는 동작; 및

[0025] 송신기 및 수신기에 의해, 비트 에러율 추정, 에러 정정 및 프라이버시 증폭 프로세스를 통해 최종 공유 양자 키를 획득하는 동작.

[0026] 일 실시예에서, 제1 미리-프로비저닝된 알고리즘은: 송신기 및 수신기 둘 다에 의해 사전설정 정책에 따라 동기적으로 변하는 파라미터 및 송신기 식별 정보에 따라 송신기 인증 정보를 계산하는 단계를 포함하고, 수신기측의 송신기 식별 정보는 미리-결정된 채널을 통해 송신기에 의해 수신기로 전송되거나 또는 미리-프로비저닝된다.

[0027] 일 실시예에서, 수신기와 합의된 기준 선택 룰에 따라 송신기 인증 정보를 위한 준비의 기준을 송신기에 의해 선택하기 전에, 다음 동작이 수행된다:

[0028] 미리-결정된 채널을 통해 실행되는 상호 작용을 개시하는 요청 동안 사전설정 정책에 따라 동기적으로 변하는 파라미터로 상대방의 피어 디바이스에 대한 인증을 송신기 및 수신기 둘 다에 의해 수행하고, 어느 디바이스가 인증에 실패하면 QKD 프로세스를 개시하지 않는 동작.

[0029] 일 실시예에서, 제2 미리-프로비저닝된 알고리즘은: 송신기 및 수신기 둘 다에 의해, 사전설정 정책에 따라 동기적으로 변하는 파라미터의 변형 및 수신기 식별 정보에 따라 수신기 인증 정보를 계산하는 단계를 포함하고, 송신기측의 수신기 식별 정보는 미리-결정된 채널을 통해 수신기에 의해 송신기로 전송되거나 또는 미리-프로비저닝된다.

[0030] 일 실시예에서, 사전설정 정책에 따라 동기적으로 변하는 파라미터의 변형은, 파라미터 그 자체, 또는 사전설정 수학적 변환 방법으로 파라미터를 프로세싱하는 것으로부터 얻어지는 결과를 포함한다.

[0031] 일 실시예에서, 송신기 및 수신기 둘 다의 사전설정 정책에 따라 동기적으로 변하는 파라미터는, 송신기 및 수신기가 QKD 프로세스들을 수행하는 횟수를 포함한다.

[0032] 일 실시예에서, 인증 정보를 계산하는 단계는 해시 함수(hash function)로 대응하는 인증 정보를 계산하는 단계를 포함한다.

[0033] 일 실시예에서, 적어도 키 정보 및 송신기 인증 정보를 포함하는 양자 상태들을 사전설정 방식으로 송신하는 단계는, 사전설정 정보 포맷으로 각각 상이한 파장들로 제어 정보 및 데이터 정보의 양자 상태들을 송신하는 단계를 포함하고, 데이터 정보는 키 정보 및 송신기 인증 정보를 포함한다.

[0034] 일 실시예에서, 사전설정 정보는, 인증 정보 및 키 정보가 각각의 제어 정보를 프리픽스(prefix)로서 사용하도록 포맷팅된다.

[0035] 일 실시예에서, 인증 정보의 프리픽스로서 사용되는 제어 정보의 양자 상태들을 전달하는 파장은 키 정보의 프리픽스로서 사용되는 제어 정보의 양자 상태들을 전달하는 파장과 다르다.

[0036] 일 실시예에서, 사전설정 정보는, 인증 정보의 프리픽스로서 사용되는 제어 정보와 키 정보의 프리픽스로서 사용되는 제어 정보가 각각 상이한 코드들을 사용하도록 포맷팅되고, 상이한 코드들은 송신기 및 수신기에 의해 사전설정되거나 미리-결정된 채널을 통한 교섭을 통해 결정되고; 제어 정보의 양자 상태들을 준비 또는 측정하기 위한 기준은 송신기 및 수신기에 의해 사전설정되거나 또는 미리-결정된 채널을 통한 교섭을 통해 결정된다.

[0037] 일 실시예에서, 사전설정 정보는, 인증 정보 및 키 정보가 프리픽스로서 공통 제어 정보를 사용하도록 포맷팅되고, 제어 정보와 키 정보 간의 인증 정보의 길이는 송신기 및 수신기에 의해 사전설정되거나, 또는 미리-결정된 채널을 통한 교섭을 통해 결정된다.

[0038] 또한, 본 출원은 QKD 프로세스에서 사용되는 인증 방법을 더 제공하며, 이 방법은 QKD 프로세스에 참여하는 양자 통신 송신기 디바이스에서 구현되며, 이 방법은,

[0039] 제1 미리-프로비저닝된 알고리즘으로 송신기 인증 정보를 생성하는 단계;

[0040] QKD 프로세스에 참여하는 피어 디바이스와 합의된 기준 선택 룰에 따라 송신기 인증 정보에 대한 준비의 기준을 선택하는 단계; 및

[0041] 적어도 키 정보 및 송신기 인증 정보를 포함하는 양자 상태들을 사전설정 방식으로 피어 디바이스에 송신하는 단계를 포함하고, 여기서

[0042] 제1 미리-프로비저닝된 알고리즘으로 생성된 송신기 인증 정보는 피어 디바이스를 향해 개시된 상이한 QKD 프로세스들에서 동적으로 변화한다.

[0043] 일 실시예에서, 적어도 키 정보 및 송신기 인증 정보를 포함하는 양자 상태들을 사전설정 방식으로 QKD 프로세스에 참여하는 피어 디바이스에 송신한 후, 다음 동작들이 수행된다:

[0044] 피어 디바이스에 의해 리턴된(returned) 정보를 수신하는 동작 - 상기 정보는 적어도 수신기 인증 정보를 포함함 -;

[0045] 제2 미리-프로비저닝된 알고리즘으로 수신기 인증 정보를 계산하는 동작; 및

[0046] 수신된 수신기 인증 정보가 계산 결과와 일치하는지를 결정하고, 일치한다면 수신기가 인증된 것으로 결정하고; 그렇지 않으면, 수신기가 인증되지 않은 것으로 결정하고 QKD 프로세스를 종료하는 동작.

[0047] 일 실시예에서, 피어 디바이스에 의해 리턴된 정보는 수신기 인증 정보를 포함할 뿐만 아니라, 키 정보의 양자 상태들을 측정하는데 사용되는 측정 기준을 포함하고;

[0048] 대응하여, 수신기가 인증된 것으로 결정한 후에, 다음 동작들이 수행된다:

[0049] 키 정보의 양자 상태들의 정확한 측정 기준을 결정하고, 오리지널 키를 스크리닝하는 동작;

[0050] 미리-결정된 채널을 통해 키 정보의 양자 상태들의 정확한 측정 기준을 공개하는 동작; 및

[0051] 비트 에러율 추정, 에러 정정 및 프라이버시 증폭 프로세스들을 통해 최종 공유 양자 키를 획득하는 동작.

[0052] 일 실시예에서, 제1 미리-프로비저닝된 알고리즘은, 사전설정 정책에 따라 피어 디바이스의 동기적으로 변하는 파라미터 및 호스트 디바이스의 식별 정보에 따라 송신기 인증 정보를 계산하는 것을 포함한다.

[0053] 일 실시예에서, 제2 미리-프로비저닝된 알고리즘은, 사전설정 정책에 따라 피어 디바이스의 동기적으로 변하는 파라미터의 변형 및 피어 디바이스의 식별 정보에 따라 수신기 인증 정보를 계산하는 것을 포함한다.

[0054] 일 실시예에서, 사전설정 정책에 따라 피어 디바이스의 동기적으로 변하는 파라미터는, QKD 프로세스가 피어 디바이스에서 수행되는 횟수를 포함한다.

[0055] 일 실시예에서, 인증 정보를 계산하는 단계는 해시 함수로 대응하는 인증 정보를 계산하는 단계를 포함한다.

[0056] 일 실시예에서, 사전설정 방식으로 적어도 키 정보 및 송신기 인증 정보를 포함하는 양자 상태들을 송신하는 단계는, 사전설정 정보 포맷으로 각각 상이한 파장들로 제어 정보 및 데이터 정보의 양자 상태들을 송신하는 단계를 포함하고, 데이터 정보는 키 정보 및 송신기 인증 정보를 포함한다.

[0057] 일 실시예에서, 사전설정 정보는 인증 정보 및 키 정보가 각각의 제어 정보를 프리픽스로서 사용하도록 포맷팅된다.

[0058] 일 실시예에서, 사전설정 정보는, 인증 정보 및 키 정보가 프리픽스로서 공통 제어 정보를 사용하도록 포맷팅되고, 제어 정보와 키 정보 간의 인증 정보의 길이는 사전설정되거나, 또는 미리-결정된 채널을 통한 피어 디바이스와의 교섭을 통해 결정된다.

[0059] 대응하여, 본 출원은 QKD 프로세스에서 사용되는 인증 장치를 더 제공하며, 이 장치는 QKD 프로세스에 참여하는 양자 통신 송신기 디바이스에 배치되고, 이 장치는,

[0060] 제1 미리-프로비저닝된 알고리즘으로 송신기 인증 정보를 생성하도록 구성된 송신기 신원 정보 생성 유닛 - 상기 송신기 인증 정보는 수신기에서 개시된 상이한 QKD 프로세스들에서 동적으로 변화함 -;

[0061] QKD 프로세스에 참여하는 피어 디바이스와 합의된 기준 선택 룰에 따라 송신기 인증 정보에 대한 준비의 기준을 선택하도록 구성된 준비의 기준 선택 유닛; 및

[0062] 적어도 키 정보와 송신기 인증 정보를 포함하는 양자 상태들을 피어 디바이스에 사전설정 방식으로 송신하도록 구성된 양자 상태들 송신 유닛을 포함한다.

[0063] 일 실시예에서, 이 장치는,

[0064] 양자 상태들 송신 유닛이 양자 상태들 송신 동작을 완료한 후에 피어 디바이스에 의해 리턴된 정보를 수신하도록 구성된 수신기 신원 정보 수신 유닛 - 상기 정보는 적어도 수신기 인증 정보를 포함함 -;

[0065] 제2 미리-프로비저닝된 알고리즘으로 수신기 인증 정보를 계산하도록 구성된 수신기 신원 정보 계산 유닛; 및

[0066] 수신된 상기 수신기 인증 정보가 계산 결과와 일치하는지를 결정하고, 일치한다면 수신기가 인증된 것으로 결정하고; 그렇지 않으면, 수신기가 인증되지 않은 것으로 결정하고 QKD 프로세스를 종료하도록 구성된 수신기 인증 유닛을 더 포함한다.

[0067] 일 실시예에서, 수신기 신원 정보 수신 유닛에 의해 수신된 정보는 수신기 인증 정보를 포함할 뿐만 아니라, 키 정보의 양자 상태들을 측정하기 위해 피어 디바이스에 의해 사용되는 측정 기준을 포함한다. 이들 실시예에 따르면, 이 장치는,

[0068] 수신기 인증 유닛이 수신기가 인증된 것으로 결정한 후에, 키 정보의 양자 상태들에 대한 정확한 측정 기준을 결정하고, 오리지널 키를 스크리닝하도록 구성된 오리지널 키 스크리닝 유닛;

[0069] 미리-결정된 채널을 통해 키 정보의 양자 상태들에 대한 정확한 측정 기준을 공개하도록 구성된 정확한 측정 기준 공개 유닛; 및

[0070] 비트 에러율 추정, 에러 정정 및 프라이버시 증폭 프로세스들을 통해 최종 공유 양자 키를 획득하도록 구성된 공유 양자 키 생성 유닛을 포함한다.

[0071] 일 실시예에서, 송신기 신원 정보 생성 유닛에 의해 사용되는 제1 미리-프로비저닝된 알고리즘은, 사전설정 정책에 따라 피어 디바이스의 동기적으로 변하는 파라미터 및 호스트 디바이스의 식별 정보에 따라 송신기 인증 정보를 계산하는 것을 포함한다.

[0072] 일 실시예에서, 수신기 신원 정보 계산 유닛에 의해 사용되는 제2 미리-프로비저닝된 알고리즘은, 사전설정 정책에 따라 피어 디바이스의 동기적으로 변하는 파라미터의 변형 및 피어 디바이스의 식별 정보에 따라 수신기 인증 정보를 계산하는 것을 포함한다.

[0073] 일 실시예에서, 송신기 신원 정보 생성 유닛 및 수신기 신원 정보 계산 유닛에 의해 사전설정 정책에 따라 계산을 위해 사용되는 동기적으로 변하는 파라미터는, QKD 프로세스가 피어 디바이스에서 수행되는 횟수를 포함한다.

[0074] 일 실시예에서, 송신기 신원 정보 생성 유닛 또는 수신기 신원 정보 계산 유닛은 해시 함수로 대응하는 인증 정보를 계산하도록 구체적으로 구성된다.

[0075] 일 실시예에서, 양자 상태들 송신 유닛은, 사전설정 정보 포맷으로 각각 상이한 파장들로 제어 정보 및 데이터 정보의 양자 상태들을 송신하도록 구체적으로 구성되고, 데이터 정보는 키 정보 및 송신기 인증 정보를 포함한다.

[0076] 일 실시예에서, 양자 상태들 송신 유닛에 의해 사용되는 사전설정 정보 포맷은 인증 정보 및 키 정보가 각각의 제어 정보를 프리픽스로서 사용하도록 한다.

[0077] 일 실시예에서, 양자 상태들 송신 유닛에 의해 사용되는 사전설정 정보 포맷은, 인증 정보 및 키 정보가 프리픽스로서 공통 제어 정보를 사용하도록 하고, 제어 정보와 키 정보 간의 인증 정보의 길이는 사전설정되거나, 또는 미리-결정된 채널을 통한 피어 디바이스와의 교섭을 통해 결정된다.

[0078] 또한, 본 출원은 QKD 프로세스에서 사용되는 인증 방법을 더 제공하며, 이 방법은 QKD 프로세스에 참여하는 양자 통신 수신기 디바이스에 구현되며, 이 방법은,

[0079] QKD 프로세스에 참여하는 피어 디바이스에 의해 전송된 양자 상태들을 수신하고, 피어 디바이스의 것과 동일한 사전설정 방식으로 다양한 정보의 수신된 양자 상태들을 구별하는 단계;

[0080] 피어 디바이스의 것과 동일한 제1 미리-프로비저닝된 알고리즘으로 송신기 인증 정보를 계산하는 단계;

[0081] 피어 디바이스의 것과 동일한 기준 선택 룰에 따라 측정 기준을 선택하고, 송신기 인증 정보의 수신된 양자 상태들을 측정하는 단계; 및

[0082] 측정 결과가 계산된 송신기 인증 정보와 일치하는지를 결정하고, 일치한다면 송신기가 인증된 것으로 결정하고; 그렇지 않으면, 송신기가 인증되지 않은 것으로 결정하고 QKD 프로세스를 종료하는 단계를 포함한다.

[0083] 일 실시예에서, 송신기가 인증된 것으로 결정한 후에 다음 동작들이 수행될 수 있다:

[0084] 피어 디바이스의 것과 동일한 제2 미리-프로비저닝된 알고리즘으로 수신기 인증 정보를 생성하는 동작; 및

[0085] 피어 디바이스에 수신기 인증 정보를 송신하는 동작.

[0086] 일 실시예에서, 송신기가 인증된 것으로 결정한 후에 다음 동작들이 수행될 수 있다:

[0087] 키 정보의 수신된 양자 상태들을 측정하기 위한 측정 기준을 랜덤하게 선택하고, 미리-결정된 채널을 통해 측정 기준을 공개하는 동작;

[0088] 미리-결정된 채널을 통해 피어 디바이스에 의해 전송된 키 정보의 양자 상태들의 정확한 측정 기준을 수신하는 동작; 및

[0089] 오리지널 키를 스크리닝하고, 비트 에러율 추정, 에러 정정 및 프라이버시 증폭 프로세스들을 통해 최종 공유 양자 키를 획득하는 동작.

[0090] 대응하여, 본 출원은 QKD 프로세스에서 사용되는 인증 장치를 더 제공하며, 이 장치는 QKD 프로세스에 참여하는 양자 통신 수신기 디바이스에 배치되며, 이 장치는,

[0091] QKD 프로세스에 참여하는 피어 디바이스에 의해 전송된 양자 상태들을 수신하고, 피어 디바이스의 것과 동일한 사전설정 방식으로 다양한 정보의 수신된 양자 상태들을 필터링 또는 구별하도록 구성된 양자 상태들 수신 및 구별 유닛;

[0092] 피어 디바이스의 것과 동일한 제1 미리-프로비저닝된 알고리즘으로 송신기 인증 정보를 계산하도록 구성된 송신기 신원 정보 계산 유닛;

[0093] 피어 디바이스의 것과 동일한 기준 선택 룰에 따라 측정 기준을 선택하고, 송신기 인증 정보의 수신된 양자 상태들을 측정하도록 구성된 신원 정보 양자 상태들 측정 유닛; 및

[0094] 측정 결과가 계산된 송신기 인증 정보와 일치하는지를 결정하고, 일치한다면 송신기가 인증된 것으로 결정하고, 그렇지 않으면 송신기가 인증되지 않은 것으로 결정하고 QKD 프로세스를 종료하도록 구성된 송신기 인증 유닛을 포함한다.

[0095] 일 실시예에서, 이 장치는,

[0096] 송신기 인증 유닛이 송신기가 인증된 것으로 결정한 후에, 피어 디바이스의 것과 동일한 제2 미리-프로비저닝된 알고리즘으로 수신기 인증 정보를 생성하도록 구성된 수신기 신원 정보 생성 유닛; 및

[0097] 피어 디바이스로 수신기 인증 정보를 송신하도록 구성된 수신기 신원 정보 송신 유닛을 더 포함한다.

[0098] 일 실시예에서, 이 장치는,

[0099] 송신기 인증 유닛이 송신기가 인증된 것으로 결정한 후에, 키 정보의 수신된 양자 상태들을 측정하기 위한 측정 기준을 랜덤하게 선택하고, 미리-결정된 채널을 통해 측정 기준을 공개하도록 구성된 키 정보 양자 상태들 측정 기준 공개 유닛;

[0100] 미리-결정된 채널을 통해 피어 디바이스에 의해 전송된 키 정보의 양자 상태들의 정확한 측정 기준을 수신하도록 구성된 정확한 측정 기준 수신 유닛; 및

[0101] 오리지널 키를 스크리닝하고, 비트 에러율 추정, 에러 정정 및 프라이버시 증폭 프로세스들을 통해 최종 공유 양자 키를 획득하도록 구성된 스크리닝 및 공유 양자 키 생성 유닛을 더 포함한다.

[0102] 또한, 본 출원은, 상술한 부분들 중 임의의 것에 따른 양자 통신 송신기 디바이스에 배치되는 인증 장치를 포함하는, QKD 프로세스에서 사용되는 인증 시스템을 더 제공하며, 이 인증 장치는 상술한 부분들 중 임의의 것에 따른 양자 통신 수신기 디바이스에 배치된다.

발명의 효과

[0103] 종래 기술과 비교하여, 본 출원은 다음의 이점들을 갖는다:

[0104] 본 출원에 제공된 QKD 프로세스에서 사용되는 인증 방법에 따르면, 송신기는, 수신기와 합의된 기준 선택 룰에 따라, 제1 미리-프로비저닝된 알고리즘으로 생성된 송신기 인증 정보의 준비의 기준을 선택하고, 적어도 키 정보 및 송신기 인증 정보를 포함하는 양자 상태들을 사전설정 방식으로 송신하고; 수신기는, 다양한 정보의 수신된 양자 상태들을 사전설정 방식으로 구별하고(필터링하고), 기준 선택 룰에 따라 송신기 인증 정보의 수신된 양자 상태들을 측정하고, 측정 결과가 제1 미리-프로비저닝된 알고리즘으로 계산된 송신기 인증 정보와 일치하면 송신기가 인증된 것으로 결정하고; 그렇지 않으면 송신기가 인증되지 않은 것으로 결정하고 QKD 프로세스를 종료한다. 위의 기술적 솔루션에서, 송신기에 의해 양자 상태들의 형태로 전송되고 제1 미리-프로비저닝된 알고리즘으로 생성되는 송신기 인증 정보는, 수신기를 향해 개시된 상이한 QKD 프로세스들에서 동적으로 변화하고, 수신기는, QKD 프로세스에서 요청자의 동적 인증을 달성할 수 있도록, 동일한 미리-프로비저닝된 알고리즘으로 수신된 인증 정보를 검증하여, 수신기에 대한 스푸핑 공격, 중간자 공격 및 분산 서비스 거부(DDoS) 공격에 대해 효과적인 방어가 제공될 수 있으며, QKD 프로세스의 보안이 향상되고; 또한, 인증 정보가 알고리즘으로 동적으로 생성되므로 양자 키 리소스의 낭비를 피할 수 있다.

도면의 간단한 설명

[0105] 도 1은 본 출원에 제공된 바와 같은 QKD 프로세스에서 사용되는 인증 방법의 실시예의 흐름도이다.

도 2는 본 출원의 실시예에 제공된 바와 같은 인증 정보 및 키 정보를 포함하는 양자 상태들을 송신하는 송신기를 나타내는 프로세스 흐름도이다.

도 3은 본 출원의 실시예에 제공된 바와 같은 제1 정보 포맷의 개략도이다.

도 4는 본 출원의 실시예에 제공된 바와 같은 제2 정보 포맷의 개략도이다.

도 5는 본 출원의 실시예에 제공된 바와 같은 제3 정보 포맷의 개략도이다.

도 6은 본 출원의 실시예에 제공된 바와 같은 인증 동작을 수행하는 수신기를 나타내는 프로세스 흐름도이다.

도 7은 본 출원에 제공된 바와 같은 QKD 프로세스에서 사용되는 다른 인증 방법의 실시예의 흐름도이다.

도 8은 본 출원에 제공된 바와 같은 QKD 프로세스에서 사용되는 인증 장치의 실시예의 개략도이다.

도 9는 본 출원에서 제공된 바와 같은 QKD 프로세스에서 사용되는 제3 인증 방법의 실시예의 흐름도이다.

도 10은 본 출원에서 제공된 바와 같은 QKD 프로세스에서 사용되는 인증 장치의 실시예의 개략도이다.

도 11은 본 출원에서 제공된 바와 같은 QKD 프로세스에서 사용되는 인증 시스템의 실시예의 개략도이다.

도 12는 본 출원의 실시예에서 제공된 바와 같은 인증 시스템의 상호적 프로세싱 흐름을 도시하는 개략도이다.

발명을 실시하기 위한 구체적인 내용

[0106] 많은 특정 세부 사항들이 본 출원의 완전한 이해를 돕기 위해 아래의 설명에서 상세하게 설명된다. 그러나, 본 출원은 본 명세서에 설명된 것과 다른 다른 방식으로 구현될 수 있으며, 통상의 기술자는 본 출원의 사상을 벗어나지 않고 유사한 확장을 할 수 있다. 본 출원은 아래에 공개된 특정 실시예들에 한정되지 않는다는 것을 이해해야 한다.

[0107] 본 출원은, 다음의 실시예들에서 각각 상세하게 설명되는, QKD 프로세스에서 사용되는, 인증 방법, 및 추가의 다른 2개의 인증 방법 및 대응하는 장치, 및 인증 시스템을 제공한다.

[0108] 도 1은 본 출원에 따르는 QKD 프로세스에서 사용되는 인증 방법의 실시예의 흐름도를 도시한다. 이 방법은 QKD 프로세스에 참여하는 양자 통신 송신기 디바이스 및 양자 통신 수신기 디바이스에서 구현된다. 본 실시예의 구체적인 단계들을 상세히 설명하기 전에, 본 실시예에 관련된 양자 통신 송신기 디바이스 및 양자 통신 수신기 디바이스가 간략하게 설명된다.

[0109] 이 실시예에서, QKD 프로세스에 참여하는 양자 통신 디바이스의 신원은 분배 프로세스에서 동적으로 인증된다. 특히, 제1 디바이스는 준비의 기준을 선택하고 양자 상태들을 피어 디바이스로 송신한다. 이 디바이스(QKD 프로세스의 개시자 또는 요청자라고도 함)는 양자 통신 송신기 디바이스, 또는 이 기술적 솔루션 내에서 짧게 송신기로 정의된다. 수신된 양자 상태들을 측정하기 위한 측정 기준을 선택하는 제2 디바이스는 양자 통신 수신기 디바이스, 또는 이 기술적 솔루션 내에서 짧게 수신기로 정의된다.

[0110] 하나 이상의 실시예에 따르면, QKD 프로세스는 다음의 단계들: 송신기에 의해 양자 상태들을 송신하고, 수신기에 의해 양자 상태들을 측정하고, 송신기 및 수신기에 의해 측정 기준을 비교하고, 오리지널 키를 스크리닝하고, 비트 에러율을 추정하고, 에러를 정정하고, 프라이버시를 증폭하는 단계를 포함한다. 이 기술적 솔루션에 따라 위의 프로세스에서 동적 인증이 달성된다. 구체적으로, 송신기가 키 정보 및 인증 정보를 포함하는 양자 상태들을 송신한 후에, 수신기는 인증 정보의 양자 상태들을 측정함으로써 송신기의 신원을 검증하여, 스푸핑 공격, 중간자 공격 또는 DDoS 공격을 피하도록 한다. 상술한 단-방향 인증 이외에, 송신기는 "피싱(phishing) 공격"을 피하기 위해 수신기에 의해 제공되는 인증 정보에 따라 수신기의 신원을 검증할 수 있고, 이에 따라 더 안전한 양-방향 인증을 달성할 수 있다.

[0111] 아래의 예들은 이 양-방향 인증을 설명하는데 초점을 맞출 것이다. 이 기술적 솔루션의 하나 이상의 구현에서, 수신기에 의한 송신기에 대한 단-방향 인증이 단독으로 수행될 수 있으며, 이는 또한 보안을 향상시키고 낭비되는 양자 키 리소스를 피하는 유익한 효과를 달성할 수 있음을 알아야 한다.

[0112] 또한, 이 기술적 솔루션의 하나 이상의 구현에서, 키 정보의 양자 상태들을 측정하고 측정 기준을 비교하는 것과 같은 후속 단계는 인증이 완료된 후에 진행될 수 있다. 상호 인증은 또한 다양한 단계들에서 달성될 수 있

고 인터리빙(interleave)될 수 있다. 두 번째 구현은 상호 작용 프로세스를 단순화하고 실행 효율성을 향상시킬 수 있다. 이와 같이, 아래의 실시예들은 이들 구현을 사용하여 설명된다. 이 실시예는 아래에서 상세하게 설명된다.

[0113] QKD 프로세스에서 사용되는 인증 방법은 다음의 단계들을 포함한다:

[0114] 단계 101: 송신기는 수신기와 합의된 기준 선택 룰에 따라 송신기 인증 정보의 준비 기준을 선택하고, 키 정보와 송신기 인증 정보를 포함하는 양자 상태들을 사전설정 방식으로 송신하고, 여기서 송신기 인증 정보는 제1 미리-프로비저닝된 알고리즘으로 생성되고, 수신기를 향해 개시된 상이한 QKD 프로세스들에서 동적으로 변화한다.

[0115] 비-합법적인 양자 통신 디바이스들 간의 QKD 프로세스를 개시하는 것을 피하기 위해, 송신기 및 수신기의 양자 통신 디바이스는, 송신기가 QKD 프로세스를 개시하기 전에 (클래식 채널과 같은) 미리-결정된 채널을 통해 피어 디바이스의 신원을 확인해야 한다. 하나 이상의 실시예에 따르면, 임의의 후속 QKD 프로세스는 두 디바이스가 모두 인증될 때만 개시될 수 있다.

[0116] 이 기술적 솔루션에서, 송신기는 제1 미리-프로비저닝된 알고리즘으로 송신기 인증 정보를 생성하고, 송신기 인증 정보는 상이한 QKD 프로세스들에 대해 동적으로 변화한다. 이 기능을 달성하기 위해, 이 실시예에서, 송신기 및 수신기는 각각 사전설정 정책에 따라 동기적으로 변하는 파라미터 n(관련 설명은 후속 단계 101-1에서의 관련 텍스트로부터 찾을 수 있음)을 유지할 수 있고, 송신기 및 수신기는 상술한 미리-결정된 채널-기반 인증 프로세스를 달성하기 위해 파라미터 n을 사용할 수 있다.

[0117] 예를 들어, QKD 프로세스의 요청자, 즉, 본 출원의 송신기는 먼저 양자 키 교섭 요청을 송신할 수 있고, 이 요청은, 파라미터 n 및 송신기의 식별 정보 userid_A(식별 정보의 설명은 후속 단계 101-1에서의 관련 텍스트로부터 찾을 수 있음)에 기초하여 계산된 해시값 hash(userid_A, n)를 포함한다. QKD 프로세스에 참여하는 피어 디바이스, 즉, 본 출원의 수신기는 다음으로, 상술한 요청 정보를 수신한 후 국부적으로 사전설정된 userid_A와 국부적으로 유지된 파라미터 n의 해시값을 계산하고, 계산된 값이 수신된 값과 일치하는 경우 해시값 hash(userid_B, n)를 포함하는 응답 정보를 송신기에 리턴하고; 그렇지 않으면 QKD 프로세스를 종료한다. 마찬가지로, 송신기는 또한 동일한 방식으로 수신기의 신원을 검증할 수 있고, 수신기가 인증되면, QKD 프로세스가 개시될 수 있고; 그렇지 않으면 QKD 프로세스가 개시되지 않는다.

[0118] 상술된 구현에서, 송신기 및 수신기 모두를 상대방의 식별 정보로 미리-프로비저닝하기 위한 방식이 채택된다. 다른 구현들에서, 송신기 및 수신기는 상대방의 식별 정보로 미리-프로비저닝되지 않고; 대신에, QKD 프로세스의 요청 상호 작용에서 식별 정보를 전달하는 방식이 채택된다. 예를 들어, 송신기에 의해 전송된 정보는 hash(userid_A, n) 및 userid_A를 포함하고, 수신기에 의해 리턴된 정보는 hash(userid_B, n) 및 userid_B를 포함하고, 송신기 및 수신기는 또한 상대방의 식별 정보를 이런 방식으로 획득할 수 있다.

[0119] 송신기 및 수신기가 모두 상기 프로세스에서 인증되면, 후속 QKD 프로세스가 개시되고, 송신기는 적어도 인증 정보 및 키 정보를 포함하는 양자 상태들을 수신기에 송신한다. 이 프로세스는 단계 101-1 내지 101-3을 포함하며, 도 2를 참조하여 아래에서 더 설명된다.

[0120] 단계 101-1: 제1 미리-프로비저닝된 알고리즘으로 송신기 인증 정보를 생성한다.

[0121] 이 기술적 솔루션에서, 송신기 및 수신기는, 송신기 인증 정보를 계산하기 위해 동일한 알고리즘, 즉, 본 출원의 제1 미리-프로비저닝된 알고리즘으로 미리-프로비저닝되고, 이 알고리즘으로 생성된 송신기 인증 정보는 수신기를 향해 개시된 상이한 QKD 프로세스들에 대해 동적으로 변화한다. 다시 말해, 수신기에 의해 수신된 각 요청자의 인증 정보는 수신기에 대해 동적으로 변화하고, 수신기는 제1 미리-프로비저닝된 알고리즘에 따라 요청자에 대한 인증을 수행할 수 있으며, 공격자가 동적으로-변화하는 인증 정보를 모방하기 어렵게 되고, 따라서 수신기는 스푸핑 공격, 중간자 공격 또는 DDoS 공격에 대해 효과적으로 방어할 수 있다.

[0122] 하나 이상의 구현에서, 요구되는 제1 미리-프로비저닝된 알고리즘은, 동적-변동 요구가 충족되는 한 요구들에 따라 설계될 수 있다. 본 실시예에서는 다음의 제1 미리-프로비저닝된 알고리즘이, 송신기 및 수신기에 의해 사전설정 정책에 따라 동기적으로 변하는 파라미터 n 및 송신기 식별 정보 userid_A에 따라 송신기 인증 정보를 계산하기 위해 사용된다.

[0123] 송신기 식별 정보 userid_A는 일반적으로 송신기를 다른 양자 통신 디바이스와 구별할 수 있는 식별 정보를 지칭한다. 예를 들어, 송신기 식별 정보 userid_A는 공장 출하시의 디바이스 식별자 또는 송신기의 고정 IP 주소

일 수 있다(동일한 식별 방식이 다음의 텍스트에 포함된 수신기 식별 정보 userid_B에도 채택될 수 있다).

[0124] 파라미터 n은 송신기 및 수신기에 의해 동일한 사전설정 정책에 따라 동기적으로 변하는 수치, 즉, 송신기 및 수신기에 의해 추론될 수 있는 변수일 수 있다. 예를 들어, 송신기 및 수신기는 동일한 초기 수치로 미리-프로비저닝된 다음, 사전설정 기간에 따라 각각 유지된 수치를 동기적으로 변경하거나, 또는 QKD 프로세스가 개시되기 전에 동기식 변경이 매번 트리거될 수 있다. 동기식 변경은 덧셈, 뺄셈, 곱셈 또는 나눗셈 또는 사전설정 함수와 같은 기본 연산에 의해 구현될 수 있다. n이 양 당사자 간에 교섭을 요구하지 않는 송신기 및 수신기에서 국부적으로 설정되고, n이 동적으로 변하는 값이므로, n이 누설되거나 추측될 확률이 낮고, 이에 따라 인증 정보의 보안을 보장한다.

[0125] 이 실시예에서, 송신기 인증 정보 Y는 다음의 제1 미리-프로비저닝된 알고리즘:Y=f(userid_A,n)에 따라 계산될 수 있고, 여기서 송신기 및 수신기는 동일한 함수 f, 예를 들어, 해쉬 함수를 사용한다. 송신기는 로컬 함수 인터페이스를 호출함으로써 자신의 식별 정보 userid_A를 획득할 수 있고, 수신기 측의 userid_A의 정보는 미리-결정된 채널을 통해 송신기에 의해 수신기로 전송되거나 또는 미리-프로비저닝될 수 있다. 예를 들어, 정보는, QKD 프로세스가 개시되기 전에, 교섭 요청 단계에서 전송된다(송신기 측의 userid_B의 정보는 또한 동일한 방식으로 획득될 수 있다).

[0126] userid_A는 송신기 및 수신기에 의해 알려지고, 송신기 및 수신기의 파라미터 n은 또한 상술한 제1 미리-프로비저닝된 알고리즘에서 추론될 수 있음을 알 수 있다. 따라서, 특정 QKD 프로세스에서 제1 미리-프로비저닝된 알고리즘으로 계산된 송신기 인증 정보는 송신기 및 수신기에 대해 명확하고, 송신기는 양자 상태들의 정보를 포함하고, 수신기는 그 정보로 송신기의 신원을 검증할 수 있다. 식별 정보의 고유성 및 n 값의 동적 변화로 인해 수신기는 스푸핑 공격, 중간자 공격 또는 DDoS 공격에 대해 효과적으로 방어할 수 있다.

[0127] 위에서 제공된 제1 미리-프로비저닝된 알고리즘에 기초하여, 이 실시예는 송신기 및 수신기가 QKD 프로세스를 수행하는 횟수가 파라미터 n의 값으로서 사용될 수 있는 예시적인 구현을 더 제공한다. 예를 들어, 송신기 및 수신기는 파라미터 n의 초기값을 0으로 설정하고, 송신기 및 수신기가 QKD 프로세스를 처음으로 개시할 때 양 측은 각각 n의 값을 1로 유지되게 설정하고, QKD 프로세스를 두 번째 개시할 때 n의 값을 2로 설정하는 등의 설정을 행하여, 송신기와 수신기 모두에 대한 n의 값의 동기식 변경을 실현한다. 하나 이상의 구현에서, n의 값이 사전설정 상한까지 누적될 때, 송신기 및 수신기는 n을 0으로 동기적으로 클리어(clear)하여 누적을 재시작할 수 있다.

[0128] 상술한 구현에서, 상이한 QKD 요청자들, 즉, 본 출원의 송신기들의 식별 정보는 동일한 수신기에 대해 명확하게 상이하므로, QKD 프로세스에서 각 요청자에 의해 제공되는 송신기 인증 정보는 상이하다. 동일한 QKD 요청자에 대해, QKD 프로세스가 수행되는 횟수에 따라 n의 값이 변화하므로, 상이한 QKD 프로세스들에서 동일한 요청자에 의해 제공되는 송신기 인증 정보도 상이하다. 이 경우 수신기는 요청자의 신원 정보를 보다 안전하게 검증할 수 있고, 따라서 스푸핑 공격, 중간자 공격 또는 DDoS 공격을 보다 효과적으로 방지할 수 있다.

[0129] 하나 이상의 구현에서, 이 실시예에서 제공되는 식별 정보 및 파라미터 n에 기초한 제1 미리-프로비저닝된 알고리즘에 더하여, 다른 형태의 제1 미리-프로비저닝된 알고리즘이 또한 사용될 수 있다. 예를 들어, 본 출원의 이러한 기술적 솔루션은, 송신기와 수신기 간에 동일한 난수를 미리-프로비저닝하고, 상이한 송신기 및 수신기에 대해 상이한 난수를 미리-프로비저닝하고, 난수를 사용하여 식별 정보를 대체함으로써 구현될 수도 있다.

[0130] 단계 101-2: 수신기와 합의된 기준 선택 룰에 따라 송신기 인증 정보의 준비 기준을 선택한다.

[0131] 송신기 및 수신기가 동일한 제1 미리-프로비저닝된 알고리즘으로 송신기 인증 정보를 계산하기 때문에, 송신기는 양자 상태들의 정보를 송신하고, 수신기는 동일한 정보로 송신기의 신원을 검증하고, 송신기 및 수신기는, 송신기 및 수신기가 계산에 의해 송신기 인증 정보를 얻은 후에, 합의된 기준 선택 룰에 따라 측정 기준 또는 준비의 대응하는 기준을 선택할 수 있다.

[0132] 합의된 기준 선택 룰은 송신기 및 수신기에 의해 사전설정되거나, 또는 QKD 프로세스가 개시되기 전에 미리-결정된 채널을 통해 교섭되고 결정될 수 있다. 예를 들어, 송신기는 수평 편광 및 수직 편광의 준비 기준을 사용하고, 수신기는 측정을 위해 선형 편광 측정 기준을 사용하거나; 또는 송신기는 좌측 편광 및 우측 편광의 준비 기준을 사용하고, 수신기는 측정을 위해 원형 편광 측정 기준을 사용한다. 구체적으로 예를 들어, 비트 0의 경우, 송신기는 수평 편광의 준비 기준을 사용하고, 수신기는 선형 편광 측정 기준을 사용하며, 비트 1의 경우, 송신기는 좌측 편광의 준비 기준을 사용하고, 수신기는 원형 편광 측정 기준을 사용한다.

[0133] 송신기는, 단계 101-1에서 생성된 송신기 인증 정보에 대응하는 비트열에 대한 대응하는 준비 기준을 합의된 기

준 선택 룰에 따라 선택한다.

[0134] 단계 101-3: 적어도 키 정보 및 송신기 인증 정보를 포함하는 양자 상태들을 (사전설정 방식으로) 송신한다.

[0135] 사전설정 방식은 송신기 및 수신기에 의해 미리 결정될 수 있으며, 송신기는 사전설정 방식에 따라 양자 상태들을 송신하고, 수신기는 동일한 방식에 따라 다양한 정보의 양자 상태들을 구별한다. 예를 들어, 송신기는, 상이한 파장들로 랜덤하게 생성된 키 정보 및 송신기 인증 정보의 양자 상태들을 송신할 수 있고, 수신기는 그에 따라 상이한 파장들로 양자 상태들을 구별한다.

[0136] 바람직하게, 추가적인 보안 보증을 제공하고 공격자가 타겟으로 하는 모니터링을 행하는 것을 방지하기 위해, 송신기 인증 정보 및 키 정보의 양자 상태들(포괄적으로 데이터 정보의 양자 상태들이라고도 함)은 동일한 파장을 사용하여 전송될 수 있고, 제어 정보는, 수신기에 의한 양자 상태들의 구별을 용이하게 하기 위해 송신기 인증 정보 및 키 정보의 프리픽스로서 도입될 수 있다. 이 고려에 기초하여, 이 실시예에서, 송신기는 사전설정 정보 포맷으로 상이한 파장들을 사용하여 제어 정보 및 데이터 정보(키 정보 및 송신기 인증 정보를 포함함)의 양자 상태들을 송신하고, 수신기는 파장 특성 및 정보 포맷에 따라 다양한 정보의 수신된 양자 상태들을 구별한다. 상이한 파장들은 송신기 및 수신기에 의해 사전설정되거나, QKD 프로세스가 개시되기 전에 미리-결정된 채널을 통해 교섭되고 결정될 수 있다.

[0137] 정보 포맷은 수신기가 양자 상태들을 정확하게 구별할 수 있는 한 많은 방식으로 정의될 수 있다. 몇 가지 구체적인 예가 아래에 주어진다.

[0138] 예 1: 도 3에 도시된 정보 포맷의 개략도를 참조하면, 송신기 인증 정보 및 키 정보는 각각의 제어 정보(즉, 요컨대 각각 인증 제어 정보 및 키 제어 정보)를 프리픽스로서 가지며, 2가지 타입의 제어 정보의 양자 상태들을 전달하는 파장이 상이하다. 데이터 정보(송신기 인증 정보 및 키 정보를 포함함)의 양자 상태들을 전달하는 파장은 λ_1이고, 인증 제어 정보의 양자 상태들을 전달하는 파장은 λ_2이고, 키 제어 정보의 양자 상태들을 전달하는 파장은 λ_3이고, λ_1, λ_2 및 λ_3은 서로 상이하다. λ_2 및 λ_3은 송신기 및 수신기에 의해 사전설정되거나, 양자 키 교섭 프로세스가 개시되기 전에 교섭되고 결정될 수 있다. 이러한 방식으로, 송신기는 2가지 타입의 제어 정보의 양자 상태들을 랜덤하게 선택할 수 있고, 수신기는 파장에 따라 키 제어 정보와 인증 제어 정보를 바로 구별할 수 있다.

[0139] 예 2: 도 4에 도시된 정보 포맷의 개략도를 참조하면, 송신기 인증 정보 및 키 정보는 각각의 제어 정보를 프리픽스로서 가지며, 2가지 타입의 제어 정보는 상이한 코드를 갖는다. 데이터 정보(송신기 인증 정보 및 키 정보를 포함함)의 양자 상태들을 전달하는 파장은 λ_1이고, 인증 제어 정보의 양자 상태들을 전달하는 파장 및 키 제어 정보의 양자 상태들을 전달하는 파장은 모두 λ_2(λ_1과 상이함)이지만, 2가지 타입의 제어 정보는 상이한 코드를 갖는다. 예를 들어, 00000은 인증 제어 정보의 코드이고, 11111은 키 제어 정보의 코드이다. 상이한 코드들은 송신기 및 수신기에 의해 사전설정되거나, 또는 QKD 프로세스가 개시되기 전에 미리-결정된 채널을 통해 교섭되고 결정되며; 2가지 타입의 제어 정보의 양자 상태들을 준비 또는 측정하기 위한 기준은 송신기 및 수신기에 의해 사전설정되거나, 또는 QKD 프로세스가 개시되기 전에 미리-결정된 채널을 통해 교섭되고 결정될 수 있다.

[0140] 예 3: 도 5에 도시된 정보 포맷의 개략도를 참조하면, 송신기 인증 정보 및 키 정보는 공통 제어 정보를 프리픽스로서 사용한다. 데이터 정보(송신기 인증 정보 및 키 정보를 포함함)의 양자 상태들을 전달하는 파장은 λ_1이고, 송신기 인증 정보와 키 정보는 동일한 제어 정보 프리픽스를 공유하며, 제어 정보의 양자 상태들을 전달하는 파장은, λ_1과 상이한 λ_2이다. 이러한 방식으로, 수신기는 파장에 따라 데이터 정보와 제어 정보를 구별할 수 있기 때문에, 송신기는 제어 정보의 양자 상태들을 랜덤하게 선택할 수 있지만, 제어 정보와 키 정보 간에 위치하는 송신기 인증 정보의 길이는, 수신기가 데이터 정보의 송신기 인증 정보와 키 정보를 정확하게 구별할 수 있게 하기 위해서, 송신기 및 수신기에 의해 합의되어야 한다. 하나 이상의 구현에서, 송신기 인증 정보의 길이는 송신기 및 수신기에 의해 사전설정되거나, 또는 QKD 프로세스가 개시되기 전에 미리-결정된 채널을 통해 교섭되고 결정될 수 있다.

[0141] 상술한 예들 및 대응하는 도면들은 정보 포맷의 단지 일부를 제공하고, 하나 이상의 구현에서, 각 정보 포맷은 여러번 반복되고 연결될 수 있음을 알아야 한다. 예를 들어, 예 3에 제공된 정보 포맷은 다음과 같이 확장될 수 있다(예시적인 것으로서, 이에 한정되지 않음): 제어 정보|송신기 인증 정보|키 정보|제어 정보|송신기 인증 정보|키 정보.

[0142] 이 실시예에서 제공되는 상술한 구현에서, 송신기는, 수신기와 합의된 파장 특성 및 정보 포맷에 따라, 제어 정보, 송신기 인증 정보 및 키 정보의 양자 상태들을 송신한다. 이해를 용이하게 하기 위해, 예 3의 정보 포맷을 예로서 사용하여 아래에서 설명한다.

[0143] 예를 들어, 송신기는 시점(time point) t_1, t_2 ... t_n에서 길이 n을 갖는 2진 비트열의 양자 상태들을 송신하고, 2진 비트열은 아래에 도시된다:

[0144] $$x_1, x_2 \dots x_i, x_{i+1} \dots x_{i+m+1} \dots x_n$$

[0145] 2진 비트열은 3개의 부분을 포함하고: 제1 부분은 제어 정보 비트열이고, 제2 부분은 인증 정보 비트열이고, 제3 부분은 키 정보 비트열이다. 제어 정보 비트열은 랜덤하게 선택된 2진 비트열이고 i의 길이를 가지며; 인증 정보 비트열은 단계 101-1에서 제1 미리-프로비저닝된 알고리즘으로 생성된 송신기 인증 정보 비트열이고, 그 길이 m은 미리-결정된 채널을 통해 송신기 및 수신기에 의해 교섭되고 결정될 수 있으며; 키 정보 비트열은 랜덤하게 생성된 2진 비트열이고 n-m-i의 길이를 갖는다.

[0146] 송신기는 시점 t_1, t_2 ... t_n에서 2진 비트열의 코딩된 양자 상태들 $\left(\left|\varphi_{j_1}^{x_1}\right\rangle, \left|\varphi_{j_2}^{x_2}\right\rangle \dots \left|\varphi_{j_i}^{x_i}\right\rangle, \left|\varphi_{j_{i+1}}^{x_{i+1}}\right\rangle \dots \left|\varphi_{j_{i+m}}^{x_{i+m}}\right\rangle \left|\varphi_{j_{i+m+1}}^{x_{i+m+1}}\right\rangle \dots \left|\varphi_{j_n}^{x_n}\right\rangle\right)$을 수신기에 송신하고, 여기에서 $j_1, j_2, \dots j_i, j_{i+1} \dots j_{i+m}, j_{i+m+1}, \dots j_n$는 송신기에 의해 사용되는 준비 시퀀스의 기준이고, $j_1, j_2, \dots j_i$는 제어 정보 비트열에 대응하는 준비의 랜덤 양자 상태들 기준이고 파장 λ_2을 가지며, $j_{i+1} \dots j_{i+m}$는, 송신기와 수신기에 의해 합의된 기준 선택 룰에 따라 선택된 인증 정보 비트열의 준비의 양자 상태들 기준이고, $j_{i+m+1}, \dots j_n$는 키 정보 비트열에 대응하는 준비의 랜덤 양자 상태들 기준이며, 인증 정보 비트열 및 키 정보 비트열의 준비 기준들의 파장은 모두 λ_1이며, 이는 λ_2와는 다르다.

[0147] 따라서, 수신기는 파장에 따라 데이터 정보와 제어 정보를 구별하고, 길이 m에 따라 데이터 정보 내의 키 정보와 송신기 인증 정보를 구별하고, 측정 기준 시퀀스 $k_{i+1} \dots k_{i+m}, k_{i+m+1} \dots k_n$을 사용하여 데이터 정보의 수신된 양자 상태들을 측정할 수 있으며, 여기서, $k_{i+1} \dots k_{i+m}$는 송신기 인증 정보의 양자 상태들에 대한 측정 기준이고, 이 측정 기준은 송신기와 합의된 기준 선택 룰에 따라 선택되고, $k_{i+m+1} \dots k_n$ 키 정보의 양자 상태들에 대응하는 랜덤 양자 상태들 측정 기준이다.

[0148] 이 지점에서, 송신기는 단계 101-1 내지 101-3을 통해 양자 상태들 송신 동작을 완료한다. 이 프로세스에서, 송신기는 제1 미리-프로비저닝된 알고리즘으로 송신기 인증 정보를 생성하고, 송신기 인증 정보는 고정되어 있지 않고 수신기를 향해 개시된 상이한 QKD 프로세스들에서 동적으로 변화하여, 수신기가 다양한 가능한 스푸핑 공격, 중간자 공격 또는 DDoS 공격에 대해 방어하도록 하는 보장을 제공한다.

[0149] 단계 102: 수신기는 다양한 정보의 수신된 양자 상태들을 구별하기 위해 사전설정 방식을 사용하고, 수신기는 기준 선택 룰에 따라 송신기 인증 정보의 수신된 양자 상태들을 측정하고, 측정 결과가 제1 미리-프로비저닝된 알고리즘으로 계산된 송신기 인증 정보와 일치하면, 제2 미리-프로비저닝된 알고리즘으로 생성된 수신기 인증 정보를 송신하고; 그렇지 않으면 송신기가 인증되지 않은 것으로 결정하고 QKD 프로세스를 종료한다.

[0150] 이 기술적 솔루션의 하나 이상의 구현에서, 수신기는 송신기 인증 정보의 수신된 양자 상태들을 측정함으로써 송신기의 신원을 검증하고, 송신기가 인증되지 않으면 QKD 프로세스를 종료하고; 그렇지 않으면, 수신기는 키 정보의 양자 상태들을 측정하는 후속 동작 등을 수행할 수 있다.

[0151] 바람직하게, 상기 단-방향 인증에 기초하여, 수신기는 자신의 신원 정보를 검증을 위해 송신기에 더 제공할 수 있고, 송신기는 이 방식에 따라서 "피싱 공격" 및 다른 가능한 공격들을 피할 수 있어, 보다 안전한 양-방향 인증을 달성할 수 있다. 구현의 특정 프로세스는 단계들 102-1 내지 102-5를 포함하고, 도 6을 참조하여 아래에서 더 설명된다.

[0152] 단계 102-1: 다양한 정보의 수신된 양자 상태들을 사전설정 방식으로 구별한다.

[0153] 이 단계에서, 수신기는, 양자 채널로부터 수신된 다양한 정보의 양자 상태들에 대해, 송신기와 합의된 사전설정 방식으로 송신기 인증 정보 및 키 정보와 같은 정보의 양자 상태들을 구별한다. 하나 이상의 구현에서, 상이한

프로세싱 방식이 상이한 사전설정 방식에 따라 채택될 수 있다. 송신기가 상이한 파장들로 제어 정보 및 데이터 정보의 양자 상태들을 송신하는 단계 101-3에서 제공되는 구현을 예로 들면, 제어 정보 및 데이터 정보의 양자 상태들은 상이한 파장에 따라 먼저 구별될 수 있고, 인증 정보 및 키 정보의 양자 상태들은 사전설정 정보 포맷에 따라 더 구별될 수 있다.

[0154] 예를 들어, 송신기 및 수신기가 단계 101-3의 예 1에 명시된 바와 같은 파장 특성 및 정보 포맷에 합의하는 경우, 이 단계에서, 수신기가 파장 λ_2를 갖는 양자 상태들을 수신하면, 양자 상태들은 인증 제어 정보의 양자 상태들이며, 순차적으로 수신된 파장 λ_1을 갖는 양자 상태들이 송신기 인증 정보의 양자 상태들이며, 측정 기준은 측정을 위해 양 측에 의해 합의된 기준 선택 룰에 따라 선택되어야 한다는 것을 알 수 있다. 대신에, λ_3의 파장을 갖는 양자 상태들이 수신되면, 순차적으로 수신된 파장 λ_1을 갖는 양자 상태들이 키 정보의 양자 상태들이며, 랜덤하게 선택된 측정 기준이 측정을 위해 사용될 수 있음을 알 수 있다.

[0155] 다른 예로서, 송신기 및 수신기가 단계 101-3의 예 2에 명시된 바와 같은 파장 특성 및 정보 포맷에 합의하는 경우(예를 들어, 수신기가 파장 λ_2를 갖는 양자 상태들을 수신하는 경우), 양자 상태들은 제어 정보의 양자 상태들이며, 송신기와 합의된(사전설정되거나 또는 교섭되고 결정된) 측정 기준이 측정에 사용됨을 알 수 있다. 측정 결과는, 수신된 제어 정보:인증 제어 정보 또는 키 제어 정보의 타입을 획득하도록, 합의된 코딩된 값과 비교되고, 파장 λ_1을 갖는 양자 상태들이 순차적으로 수신되면, 그 타입에 대응하는 측정 기준이 측정에 사용될 수 있다.

[0156] 단계 101의 예 3에 명시된 바와 같은 파장 특성 및 정보 포맷, 및 송신기에 의해 사용될 수 있는 다른 파장 특성 및 정보 포맷에 대해서, 수신기는 또한 유사한 방식으로 다양한 정보의 양자 상태들을 구별하거나 필터링할 수 있고, 이는 여기에서 다시 설명하지 않을 것이다.

[0157] 단계 102-2: 제1 미리-프로비저닝된 알고리즘으로 송신기 인증 정보를 계산한다.

[0158] 이 실시예에 따르면, 송신기 및 수신기는 송신기 인증 정보를 계산하기 위한 동일한 알고리즘, 즉, 본 출원의 제1 미리-프로비저닝된 알고리즘으로 사전설정된다. 알고리즘의 상세에 대해서는 단계 101-1의 설명을 참조할 수 있으며, 이는 여기에서 다시 설명하지 않을 것이다.

[0159] 수신기가 동일한 알고리즘으로 미리-프로비저닝되기 때문에, 송신기에 의해 제공되어야 하는 인증 정보가 예상될 수 있고, 이 단계에서, 수신기는 송신기 인증 정보를 제1 미리-프로비저닝된 알고리즘으로 계산하여, 송신기에 의해 제공된 인증 정보의 예상값으로서 서빙(serve)한다.

[0160] 단계 102-3: 기준 선택 룰에 따라 측정 기준을 선택하고, 송신기 인증 정보의 수신된 양자 상태들을 측정한다.

[0161] 이 실시예에 따르면, 송신기 및 수신기는 기준 선택 룰에 합의한다. 기준 선택 룰의 설명에 대해서는 단계 101-2의 설명을 참조할 수 있으며, 이는 여기에서 다시 설명하지 않을 것이다.

[0162] 기준 선택 룰에서 수신기에 대해 고정된 측정 기준(예를 들어, 선형 편광 측정 기준)이 설정되면, 송신기 인증 정보의 수신된 양자 상태들은 고정된 측정 기준을 사용하여 측정된다. 기준 선택 룰에서 상이한 비트 값들에 대해 상이한 측정 기준들이 설정되면, 이 단계에서, 단계 102-2에서 계산된 송신기 인증 정보의 각 비트의 값에 따라 대응하는 측정 기준이 선택되고, 송신기 인증 정보의 수신된 양자 상태들의 대응하는 비트가 측정된다.

[0163] 단계 102-4: 측정 결과가 계산된 송신기 인증 정보와 일치하는지를 결정하고, 일치한다면 단계 102-5를 수행하고; 그렇지 않으면 QKD 프로세스를 종료한다.

[0164] 대응하는 측정 결과, 즉, 양자 상태들로 전달된 송신기 인증 정보는 단계 102-3의 측정을 통해 얻어진다. 이 단계에서, 측정된 송신기 인증 정보는 단계 102-2에서 계산된 송신기 인증 정보와 비교되어, 송신기에 대한 인증을 완료한다.

[0165] 이 실시예에서, 송신기는 제1 미리-프로비저닝된 알고리즘 Y=f(userid_A, n)로 송신기 인증 정보를 생성한다. 수신기는 또한 동일한 알고리즘을 사용하여 정보의 예상값을 계산하고, 측정된 송신기 인증 정보를 예상값과 비교한다. 측정된 송신기 인증 정보가 예상값과 일치하면, 이는, 송신기가 자신의 인증 정보를 생성할 때 정확한 식별 정보 userid_A, 변수 n, 및 함수 *f*를 사용하고, 합법적인 신원을 갖는 양자 통신 디바이스만이 상술한 정보를 획득할 수 있음을 나타낸다. 따라서, 송신기가 인증된 것으로 결정될 수 있고, 이에 따라 후속 단계 102-5가 이어서 수행될 수 있다. 대조적으로, 송신기가 인증되지 않은 것으로 결정되면, QKD 프로세스는 종료된다.

[0166] 양자 채널 전송 프로세스에서, 약간의 광자들이 검출되지 않거나, 또는 측정 결과가 감쇠 및 잡음 간섭과 같은 팩터들로 인해 예상과 완전히 일치하지 않을 수 있다. 이 경우, 송신기가 인증에 실패한 것으로 간주되고 QKD 프로세스가 종료되면, 양자 키의 분배량의 무의미한 감소를 초래할 수 있다. 스푸핑 공격, 중간자 공격 또는 DDoS 공격에 대한 방어에 있어서의 요구 뿐만 아니라 이러한 고려에 기초하여, 임계값을 설정하는 방식이 채택될 수 있다. 즉, 수신기에 의해 측정된 송신기 인증 정보와 예상값 간의 차이가 사전설정 임계값보다 작으면, 예를 들어, 예상값과 일치하지 않는 측정된 송신기 인증 정보의 비트 수가 사전설정 상한값보다 작으면, 수신기는 송신기가 인증된 것으로 간주할 수 있다.

[0167] 단계 102-5: 키 정보의 수신된 양자 상태들을 측정하기 위한 측정 기준을 랜덤하게 선택하고, 측정 기준을 공개하고, 제2 미리-프로비저닝된 알고리즘으로 생성된 수신기 인증 정보를 송신한다.

[0168] 이 단계에 도달하면, 송신기는 수신기에 의해 인증되고, 이에 따라 QKD 프로세스는 계속될 수 있고, 수신기는, 키 정보의 수신된 양자 상태들을 측정하기 위한 측정 기준을 랜덤하게 선택하고, QKD 프로토콜에 따라 미리-결정된 채널을 통해 측정 기준을 공개할 수 있다. 이 실시예에서, 공개된 측정 기준은 수신기에 의해 유지되는 변수 n으로 암호화된 다음 송신될 수 있고, 송신기는 또한 송신기에 의해 유지되는 변수 n을 사용하여, 측정 기준을 수신한 후에 이를 해독할 수 있다.

[0169] 추가적인 보안 보증을 제공하고 양-방향 인증을 달성하기 위해, 송신기 및 수신기는 수신기 인증 정보를 계산하기 위한 동일한 알고리즘, 즉 본 출원에서의 제2 미리-프로비저닝된 알고리즘으로 미리-프로비저닝될 수 있다. 이들 실시예에 따르면, 수신기는 이 알고리즘으로 자신의 인증 정보를 생성하고 이를 송신기에 제공하며, 송신기는 동일한 알고리즘으로 수신기의 신원을 검증한다.

[0170] 하나 이상의 구현에서, 요구되는 제2 미리-프로비저닝된 알고리즘은 요구들을 충족시키도록 설계될 수 있다. 이 실시예에서, 동적 수신기 인증 정보를 생성하기 위해, 다음의 제2 미리-프로비저닝된 알고리즘이 제1 미리-프로비저닝된 알고리즘에 기초하여 적용되고: 수신기 인증 정보는, 송신기 및 수신기에 의해 사전설정 정책에 따라 동기적으로 변하는 파라미터 n의 변형 및 수신기 식별 정보 userid_B에 따라서 계산된다. 파라미터 n에 대한 설명은 단계 101-1의 관련 텍스트를 참조할 수 있다. 사전설정 정책에 따라 동기적으로 변하는 파라미터 n의 변형은 다음을 포함할 수 있다: 파라미터 n 자체; 또는 사전설정 수학적 변환 방법, 예를 들어, n+1을 사용하여 파라미터를 프로세싱함으로써 얻어진 결과. 파라미터 n의 변형을 생성하기 위한 룰은 송신기 및 수신기에 의해 합의될 수 있다.

[0171] 제2 미리-프로비저닝된 알고리즘의 특정 예는 아래에서 주어진다: 수신기 인증 정보 Y=hash(userid_B, n+1), 즉, 수신기 식별 정보와 파라미터 n의 변형의 정보를 결합함으로써 형성된 문자열의 해시값이 계산되고, 해시값은 수신기 인증 정보로서 사용된다.

[0172] 상기 설명으로부터, 제2 미리-프로비저닝된 알고리즘으로 계산된 수신기 인증 정보는 또한 동적으로 변화한다는 것을 알 수 있다. 이 실시예의 송신기에 대해서, 상이한 수신기는 상이한 식별 정보를 가지므로, 상이한 수신기 인증 정보를 제공한다. 동일한 수신기에 대해서, n의 값이 동적으로 변화하기 때문에, 수신기에 의해 제공된 수신기 인증 정보도 동적으로 변화한다. 또한, 송신기 및 수신기가 QKD 프로세스를 수행하는 횟수가 파라미터 n으로 사용되면, 상이한 QKD 프로세스에서 동일한 수신기에 의해 제공되는 수신기 인증 정보도 상이하다. 공격자가 동적 특성을 모방하기가 어렵고, 따라서 송신기가 수신기의 신원을 검증함으로써 피싱과 같은 공격을 피할 수 있는 강력한 보장을 제공한다.

[0173] 단계 103: 송신기는 제2 미리-프로비저닝된 알고리즘에 의해 수신기 인증 정보를 계산하고, 수신된 수신기 인증 정보가 계산 결과와 일치하면, 수신기가 인증된 것으로 결정한다. 수신된 수신기 인증 정보가 일치하지 않으면, 수신기는 인증되지 않은 것으로 결정되고 QKD 프로세스는 종료된다.

[0174] 수신기 인증 정보를 수신한 후에, 송신기는 제2 미리-프로비저닝된 알고리즘으로 수신기 인증 정보를 계산하고, 수신된 수신기 인증 정보와 계산된 정보를 비교하여, 수신기에서의 인증을 완료한다.

[0175] 단계 102-5에서 주어진 특정 예를 사용하여, 송신기는 제2 미리-프로비저닝된 알고리즘, 즉, Y=hash(userid_B, n+1)로 수신기 인증 정보를 계산하고, 여기서 userid_B는 미리-결정된 채널을 통해 수신기에 의해 송신기로 미리 전송되거나 또는 미리-프로비저닝될 수 있다. 수신된 수신기 인증 정보가 계산 결과와 일치하면, 이는, 수신기가 자신의 인증 정보를 생성할 때 정확한 식별 정보 userid_B, 변수 n, 및 해시 함수를 사용함을 나타낸다. 송신기가 양 측에 의해 합의된 변형 생성 룰을 또한 알고 있고, 합법적인 신원을 갖는 양자 통신 디바이스만이 상술한 정보를 획득할 수 있다면, 수신기가 인증된 것으로 결정할 수 있고; 그렇지 않으면, 수신기가 인증되지

않은 것으로 결정하고 QKD 프로세스가 종료된다.

[0176] 송신기가 수신기가 인증된 것으로 결정하면, 송신기는, QKD 프로토콜에 따라, 수신기에 의해 공개된 측정 기준을 송신기에 의해 사용되는 준비 기준과 비교하여 정확한 측정 기준을 선택하고, 정확한 측정 기준에 따라 오리지널 키를 스크리닝하고, 정확한 측정 기준을 미리-결정된 채널을 통해 수신기에 공개할 수 있다.

[0177] 순차적으로, 수신기는 송신기에 의해 공개된 정확한 측정 기준에 따라 오리지널 키를 스크리닝하고, 송신기 및 수신기는 비트 에러율 추정, 에러 정정 및 프라이버시 증폭 프로세스를 통해 최종 공유 양자 키를 또한 획득하고, QKD 프로세스는 종료된다. 이 실시예에서, 비트 에러율 추정, 에러 정정 및 프라이버시 증폭 단계에서, 미리-결정된 채널을 통해 송신기 및 수신기에 의해 교섭되는 정보는 대응하는 암호화 또는 복호화 동작을 수행하기 위한 파라미터 n의 변형(예를 들어, n+1)일 수 있다.

[0178] 이 지점에서, 상술한 단계 101 내지 단계 103으로부터, 이 실시예에서 설명된 이 기술적 솔루션은 기존의 QKD 프로토콜을 향상시키고 QKD 프로세스에서 동적 인증을 수행하기 위한 새로운 아이디어를 제공한다는 것을 알 수 있다. 송신기가, 양자 채널을 통해, 제1 미리-프로비저닝된 알고리즘으로 생성되고 수신기를 향해 개시된 상이한 QKD 프로세스들에서 동적으로 변화하는 인증 정보를 송신하기 때문에, 수신기도 동일한 미리-프로비저닝된 알고리즘을 사용하여 수신된 인증 정보를 검증하고, 동적 인증이 QKD 프로세스의 QKD 요청자에서 실현되며, 수신기에 대한 스푸핑 공격, 중간자 공격 및 DDoS 공격에 대해서 효과적으로 방어할 수 있다. 또한, 단-방향 인증에 기초하여, 송신기 및 수신기는 제2 미리-프로비저닝된 알고리즘을 사용하여 송신기에 의해 수신기에 대한 동적 인증을 실현하고, 이에 따라 송신기에 대한 피싱 공격의 잠재적인 위험을 효과적으로 방지한다.

[0179] 또한, 이 솔루션에서는, 송신기 인증 정보가 양자 상태들의 형태로 전송되므로 보안이 더욱 향상될 수 있고, 인증 정보가 알고리즘으로 동적으로 생성되므로, 양자 키 리소스의 낭비를 피할 수 있다.

[0180] 또한, 본 출원은 QKD 프로세스에서 사용되는 다른 인증 방법을 더 제공한다. 이 방법은 QKD 프로세스에 참여하는 양자 통신 송신기 디바이스에서 구현된다. 도 7은 본 출원의 QKD 프로세스에서 사용되는 다른 인증 방법의 실시예의 흐름도를 도시한다. 본 실시예에서 상술한 실시예와 동일한 단계는 다시 설명되지 않으며, 아래의 설명은 그 차이에 초점을 둔다. 이 방법은 다음 단계들을 포함한다:

[0181] 단계 701: 제1 미리-프로비저닝된 알고리즘으로 송신기 인증 정보를 생성하고, 여기서 제1 미리-프로비저닝된 알고리즘으로 생성된 송신기 인증 정보는 수신기에 대해 개시된 상이한 QKD 프로세스들에서 동적으로 변화하고, 수신기 디바이스는 QKD 프로세스에 참여하는 피어 디바이스를 지칭한다.

[0182] 제1 미리-프로비저닝된 알고리즘은: 사전설정 정책에 따라 피어 디바이스와 동기적으로 변하는 파라미터 및 호스트 디바이스의 식별 정보에 따라 송신기 인증 정보를 계산하는 단계를 포함한다. 송신기 인증 정보의 계산은 해시 함수를 채용할 수 있다.

[0183] 단계 702: 송신기 인증 정보의 준비 기준은 피어 디바이스와 합의된 기준 선택 룰에 따라 선택된다.

[0184] 단계 703: 적어도 키 정보 및 송신기 인증 정보를 포함하는 양자 상태들이 사전설정 방식으로 피어 디바이스에 송신된다.

[0185] 예를 들어, 제어 정보 및 데이터 정보의 양자 상태들은 사전설정 정보 포맷으로 상이한 파장들로 전송될 수 있고, 여기서 데이터 정보는 키 정보 및 송신기 인증 정보를 포함한다.

[0186] 사전설정 정보는, 인증 정보 및 키 정보가 프리픽스로서 각각의 제어 정보를 갖도록 포맷되거나; 또는 인증 정보 및 키 정보는 공통 제어 정보를 프리픽스로서 사용하고, 제어 정보와 키 정보 간의 인증 정보의 길이는 사전설정되거나 또는 미리-결정된 채널을 통해 피어 디바이스와 교섭되고 결정된다.

[0187] 이 단계에서 양자 상태들 송신 동작이 완료된 후에, 피어 디바이스에 의해 리턴된 정보가 수신될 수 있으며, 이 정보는 적어도 수신기 인증 정보를 포함한다. 또한, 수신기 인증 정보는 제2 미리-프로비저닝된 알고리즘으로 계산될 수 있고; 수신된 수신기 인증 정보가 계산 결과와 일치하는지 여부가 결정된다. 수신된 수신기 인증 정보가 계산 결과와 일치하면, 수신기는 인증된 것으로 결정되고; 그렇지 않으면, 수신기가 인증되지 않은 것으로 결정되고 QKD 프로세스가 종료된다.

[0188] 제2 미리-프로비저닝된 알고리즘은, 사전설정 정책에 따라 피어 디바이스와 동기적으로 변하는 파라미터의 변형 및 피어 디바이스의 식별 정보에 따라 수신기 인증 정보를 계산하는 단계를 포함한다. 사전설정 정책에 따라 피어 디바이스와 동기적으로 변하는 파라미터는, QKD 프로세스가 피어 디바이스에서 수행되는 횟수로 구성된다.

수신기 인증 정보의 계산은 해시 함수를 채용할 수 있다.

[0189] 피어 디바이스에 의해 리턴된 정보는 수신기 인증 정보 뿐만 아니라 키 정보의 양자 상태들을 측정하기 위한 측정 기준을 포함할 수 있다. 수신기가 인증된 것으로 결정된 후, 다음의 동작들이 수행될 수 있다: 키 정보의 양자 상태들의 정확한 측정 기준을 결정하고, 오리지널 키를 스크리닝하고, 키 정보의 양자 상태들의 정확한 측정 기준을 미리-결정된 채널을 통해 공개하고, 비트 에러율 추정, 에러 정정 및 프라이버시 증폭 프로세스를 통해 최종 공유 양자 키를 획득하여, QKD 프로세스를 완료하는 동작.

[0190] QKD 프로세스에서 사용되는 다른 인증 방법이 상술한 실시예에서 제공된다. 따라서, 본 출원은 QKD 프로세스에서 사용되는 인증 장치를 더 제공한다. 이 장치는 QKD 프로세스에 참여하는 양자 통신 송신기 디바이스에 배치된다. 도 8은 본 출원의 QKD 프로세스에서 사용되는 인증 장치의 실시예의 개략도를 도시한다. 장치 실시예는 기본적으로 방법 실시예와 유사하므로 간략하게 설명된다. 관련 부분에 대한 방법 실시예의 설명을 참조할 수 있다. 아래에서 설명되는 장치 실시예는 단지 예시적인 것이다.

[0191] 본 실시예에서 QKD 프로세스에서 사용되는 인증 장치는:

[0192] 제1 미리-프로비저닝된 알고리즘으로 송신기 인증 정보를 생성하도록 구성된 송신기 신원 정보 생성 유닛(801) - 상기 송신기 인증 정보는 수신기에 대해 개시된 상이한 QKD 프로세스들에서 동적으로 변화함 -; QKD 프로세스에 참여하는 피어 디바이스와 합의된 기준 선택 룰에 따라 송신기 인증 정보의 준비의 기준을 선택하도록 구성된 준비의 기준 선택 유닛(802); 및 적어도 키 정보와 송신기 인증 정보를 포함하는 양자 상태들을 피어 디바이스에 사전설정 방식으로 송신하도록 구성된 양자 상태들 송신 유닛(803)을 포함한다.

[0193] 일 실시예에서, 이 장치는,

[0194] 양자 상태들 송신 유닛이 양자 상태들 송신 동작을 완료한 후에 피어 디바이스에 의해 리턴된 정보를 수신하도록 구성된 수신기 신원 정보 수신 유닛 - 상기 정보는 적어도 수신기 인증 정보를 포함함 -;

[0195] 제2 미리-프로비저닝된 알고리즘으로 수신기 인증 정보를 계산하도록 구성된 수신기 신원 정보 계산 유닛; 및

[0196] 수신된 수신기 인증 정보가 계산 결과와 일치하는지를 결정하고, 일치한다면 수신기가 인증된 것으로 결정하고, 그렇지 않으면 수신기가 인증되지 않은 것으로 결정하고 QKD 프로세스를 종료하도록 구성된 수신기 인증 유닛을 더 포함한다.

[0197] 일 실시예에서, 수신기 신원 정보 수신 유닛에 의해 수신된 정보는, 수신기 인증 정보를 포함할 뿐만 아니라, 키 정보의 양자 상태들을 측정하기 위해 피어 디바이스에 의해 사용되는 측정 기준을 포함한다. 이들 실시예에서, 이 장치는,

[0198] 수신기 인증 유닛이 수신기가 인증된 것으로 결정한 후에, 키 정보의 양자 상태들의 정확한 측정 기준을 결정하고, 오리지널 키를 스크리닝하도록 구성된 오리지널 키 스크리닝 유닛;

[0199] 미리-결정된 채널을 통해 키 정보의 양자 상태들의 정확한 측정 기준을 공개하도록 구성된 정확한 측정 기준 공개 유닛; 및

[0200] 비트 에러율 추정, 에러 정정 및 프라이버시 증폭 프로세스들을 통해 최종 공유 양자 키를 획득하도록 구성된 공유 양자 키 생성 유닛을 포함할 수 있다.

[0201] 일 실시예에서, 송신기 신원 정보 생성 유닛에 의해 사용되는 제1 미리-프로비저닝된 알고리즘은, 사전설정 정책에 따라 피어 디바이스와 동기적으로 변하는 파라미터 및 호스트 디바이스의 식별 정보에 따라 송신기 인증 정보를 계산하는 단계를 포함한다.

[0202] 일 실시예에서, 수신기 신원 정보 계산 유닛에 의해 사용되는 제2 미리-프로비저닝된 알고리즘은, 사전설정 정책에 따라 피어 디바이스와 동기적으로 변하는 파라미터의 변형 및 피어 디바이스의 식별 정보에 따라 수신기 인증 정보를 계산하는 단계를 포함한다.

[0203] 일 실시예에서, 사전설정 정책에 따라 송신기 신원 정보 생성 유닛 및 수신기 신원 정보 계산 유닛 내의 계산에 사용되는 동기적으로 변하는 파라미터는, 피어 디바이스에서 QKD 프로세스가 수행되는 횟수를 포함한다.

[0204] 일 실시예에서, 송신기 신원 정보 생성 유닛 또는 수신기 신원 정보 계산 유닛은 해시 함수로 대응하는 인증 정보를 계산하도록 구체적으로 구성된다.

[0205] 일 실시예에서, 양자 상태들 송신 유닛은, 사전설정 정보 포맷으로 상이한 파장을 각각 사용함으로써 제어 정보

및 데이터 정보의 양자 상태들을 전송하도록 구체적으로 구성되고, 데이터 정보는 키 정보 및 송신기 인증 정보를 포함한다.

[0206] 일 실시예에서, 양자 상태들 송신 유닛에 의해 사용되는 사전설정 정보 포맷은 프리픽스로서 각각의 제어 정보를 사용하는 인증 정보 및 키 정보를 포함한다.

[0207] 일 실시예에서, 양자 상태들 송신 유닛에 의해 사용되는 사전설정 정보 포맷은 공통 제어 정보를 프리픽스로서 사용하는 인증 정보 및 키 정보를 포함하고, 제어 정보와 키 정보 간의 인증 정보의 길이는 사전설정되거나 또는 미리-결정된 채널을 통해 피어 디바이스와 교섭되고 결정된다.

[0208] 또한, 본 출원은 QKD 프로세스에서 사용되는 제3 인증 방법을 더 제공한다. 이 방법은 QKD 프로세스에 참여하는 양자 통신 수신기 디바이스에서 구현된다. 도 9는 본 출원의 QKD 프로세스에서 사용되는 제3 인증 방법의 실시예의 흐름도를 도시한다. 본 실시예에서 상술한 실시예와 동일한 단계는 다시 설명되지 않으며, 아래의 설명은 그 차이에 초점을 둔다. 이 방법은 다음 단계들을 포함한다:

[0209] 단계 901: QKD 프로세스에 참여하는 피어 디바이스에 의해 전송된 양자 상태들을 수신하고, 피어 디바이스의 것과 동일한 사전설정 방식으로 다양한 정보의 수신된 양자 상태들을 구별한다.

[0210] 단계 902: 피어 디바이스 것과 동일한 제1 미리-프로비저닝된 알고리즘으로 송신기 인증 정보를 계산한다.

[0211] 단계 903: 피어 디바이스의 것과 동일한 기준 선택 룰에 따라 측정 기준을 선택하고, 송신기 인증 정보의 수신된 양자 상태들을 측정한다.

[0212] 단계 904: 측정 결과가 계산된 송신기 인증 정보와 일치하는지를 결정하고, 일치한다면 송신기가 인증된 것으로 결정하고; 그렇지 않으면 송신기가 인증되지 않은 것으로 결정하고 QKD 프로세스를 종료한다.

[0213] 하나 이상의 실시예에서, 송신기가 인증된 것으로 결정한 후, 다음의 동작들이 수행될 수 있다: 피어 디바이스의 것과 동일한 제2 미리-프로비저닝된 알고리즘으로 수신기 인증 정보를 생성하고, 수신기 인증 정보를 피어 디바이스에 송신하는 동작.

[0214] 하나 이상의 다른 실시예에서, 송신기가 인증된 것으로 결정한 후, 다음의 동작들이 수행될 수 있다: 키 정보의 수신된 양자 상태들을 측정하기 위한 측정 기준을 랜덤하게 선택하고, 미리-결정된 채널을 통해 측정 기준을 공개하고; 미리-결정된 채널을 통해 피어 디바이스에 의해 전송된 키 정보의 양자 상태들의 정확한 측정 기준을 수신하고; 오리지널 키를 스크리닝하고, 비트 에러율 추정, 에러 정정 및 프라이버시 증폭 프로세스를 통해 최종 공유 양자 키를 획득하는 동작.

[0215] QKD 프로세스에서 사용되는 제3 인증 방법이 상술한 실시예에서 제공된다. 따라서, 본 출원은 QKD 프로세스에서 사용되는 인증 장치를 더 제공한다. 이 장치는 QKD 프로세스에 참여하는 양자 통신 수신기 디바이스에 배치된다. 도 10을 참조하면, 도 10은 본 출원의 QKD 프로세스에서 사용되는 인증 장치의 실시예의 개략도이다. 장치 실시예는 기본적으로 방법 실시예와 유사하므로 간략하게 설명된다. 관련 부분에 대한 방법 실시예의 설명을 참조할 수 있다. 아래에서 설명되는 장치 실시예는 단지 예시적인 것이다.

[0216] 본 실시예의 QKD 프로세스에서 사용되는 인증 장치는: QKD 프로세스에 참여하는 피어 디바이스에 의해 전송된 양자 상태들을 수신하고, 피어 디바이스의 것과 동일한 사전설정 방식으로 다양한 정보의 수신된 양자 상태들을 구별하도록 구성된 양자 상태들 수신 및 구별 유닛(1001); 피어 디바이스의 것과 동일한 제1 미리-프로비저닝된 알고리즘으로 송신기 인증 정보를 계산하도록 구성된 송신기 신원 정보 계산 유닛(1002); 피어 디바이스의 것과 동일한 기준 선택 룰에 따라 측정 기준을 선택하고, 송신기 인증 정보의 수신된 양자 상태들을 측정하도록 구성된 신원 정보 양자 상태들 측정 유닛(1003); 및 측정 결과가 계산된 송신기 인증 정보와 일치하는지를 결정하고, 일치한다면 송신기가 인증된 것으로 결정하고, 그렇지 않으면 송신기가 인증되지 않은 것으로 결정하고 QKD 프로세스를 종료하도록 구성된 송신기 인증 유닛(1004)을 포함한다.

[0217] 일 실시예에서, 이 장치는:

[0218] 송신기 인증 유닛이 송신기가 인증된 것으로 결정한 후에, 피어 디바이스의 것과 동일한 제2 미리-프로비저닝된 알고리즘으로 수신기 인증 정보를 생성하도록 구성된 수신기 신원 정보 생성 유닛; 및

[0219] 피어 디바이스로 수신기 인증 정보를 송신하도록 구성된 수신기 신원 정보 송신 유닛을 더 포함한다.

[0220] 일 실시예에서, 이 장치는:

[0221] 송신기 인증 유닛이 송신기가 인증된 것으로 결정한 후에, 키 정보의 수신된 양자 상태들을 측정하기 위한 측정 기준을 랜덤하게 선택하고, 미리-결정된 채널을 통해 측정 기준을 공개하도록 구성된 키 정보 양자 상태들 측정 기준 공개 유닛;

[0222] 미리-결정된 채널을 통해 피어 디바이스에 의해 전송된 키 정보의 양자 상태들의 정확한 측정 기준을 수신하도록 구성된 정확한 측정 기준 수신 유닛; 및

[0223] 오리지널 키를 스크리닝하고, 비트 에러율 추정, 에러 정정 및 프라이버시 증폭 프로세스들을 통해 최종 공유 양자 키를 획득하도록 구성된 스크리닝 및 공유 양자 키 생성 유닛을 더 포함한다.

[0224] 또한, 본 출원의 실시예는 QKD 프로세스에서 사용되는 인증 시스템을 더 제공한다. 도 11에 도시된 바와 같이, 이 시스템은 양자 통신 송신기 디바이스에 배치된 인증 장치(1101) 및 양자 통신 수신기 디바이스에 배치된 인증 장치(1102)를 포함한다.

[0225] 양자 통신 송신기 디바이스 및 양자 통신 수신기 디바이스에 각각 배치된 인증 장치는, 본 출원에서 제공되는 인증 방법을 사용하여 QKD 프로세스에서 피어 디바이스에 대한 동적 인증을 실현한다. QKD 프로세스에서 사용되는 인증 시스템의 상호적 프로세싱 흐름이 도 12를 참조하여 아래에서 간략하게 설명된다. 양자 통신 송신기 디바이스에 배치된 인증 장치를 짧게 A라고 하고, 양자 통신 수신기 디바이스에 배치된 인증 장치를 짧게 B라고 하며, 송신기 및 수신기는 모두 제1 미리-프로비저닝된 알고리즘 및 제2 미리-프로비저닝된 알고리즘 뿐만 아니라 식별 정보 userid_A 및 userid_B로 사전설정되고, 송신기 및 수신기는 각각 사전설정 정책에 따라 동기적으로 변하는 파라미터 n을 유지한다.

[0226] 1) A는 B에게 키 교섭 요청을 송신하고, 여기서 요청은 hash(userid_A, n)를 전달한다.

[0227] 2) B는 A의 신원의 유효성을 검증하고 hash(userid_B, n)를 A에 송신한다.

[0228] 3) A는 B의 신원의 유효성을 검증하고; 제1 미리-프로비저닝된 알고리즘 f(userid_A, n)로 생성된 송신기 인증 정보에 대한 대응하는 준비의 기준을, B와 합의된 기준 선택 룰에 따라 선택하고, 적어도 키 정보 및 송신기 인증 정보를 포함하는 양자 상태들을 사전설정 방식으로 송신한다.

[0229] 4) B는 다양한 정보의 수신된 양자 상태들을 사전설정 방식으로 구별하고, 기준 선택 룰에 따라 송신기 인증 정보의 수신된 양자 상태들을 측정한다. 또한, 측정 결과가 제1 미리-프로비저닝된 알고리즘 f(userid_A, n)로 계산된 송신기 인증 정보와 일치하면, B는 또한 제2 미리-프로비저닝된 알고리즘으로 생성된 수신기 인증 정보 hash(userid_B, n+1)를 송신하고, 키 정보의 수신된 양자 상태들을 측정하기 위한 측정 기준을 랜덤하게 선택한 다음, 측정 기준을 공개한다. 그렇지 않으면, 송신기가 인증되지 않고 QKD 프로세스가 종료된다.

[0230] 5) A는 제2 미리-프로비저닝된 알고리즘으로 수신기 인증 정보를 계산하고, 수신된 수신기 인증 정보가 계산 결과와 일치하면, 오리지널 키를 스크리닝하고, 미리-결정된 채널을 통해 키 정보의 양자 상태들의 정확한 측정 기준을 공개하고; 그렇지 않으면, 수신기가 인증되지 않고 QKD 프로세스를 종료한다.

[0231] 6) B는 오리지널 키를 스크리닝하고; A 및 B는 비트 에러율 추정, 에러 정정 및 프라이버시 증폭 프로세스를 통해 최종 공유 양자 키를 획득한다.

[0232] 시스템의 가능한 상호 작용 프로세스가 위에서 보여지고, 다른 방식의 상호 작용이 다른 구현에서 채택될 수 있다는 것을 알아야 한다. 관련 설명은 위에서 제공된 방법 실시예들에서 이루어지며, 여기에서 반복되지 않을 것이다.

[0233] 본 출원은 하나 이상의 실시예에 따라 위에서 공개되었지만, 이에 한정되는 것은 아니다. 본 출원의 사상 및 범위를 벗어나지 않으면서 통상의 기술자에 의해 가능한 변경들 및 수정들이 이루어질 수 있다. 따라서, 본 출원의 범위는 본 출원의 청구 범위에 의해 규정될 것이다.

[0234] 통상적인 구성에서, 컴퓨팅 디바이스는 하나 이상의 프로세서(CPU), 입-출력 인터페이스, 네트워크 인터페이스 및 메모리를 포함한다.

[0235] 메모리는 컴퓨터-판독가능 매체 내의 휘발성 메모리, 랜덤 액세스 메모리 (RAM; random access memory) 및/또는 판독-전용 메모리(ROM; read-only memory) 또는 플래시 RAM과 같은 비-휘발성 메모리를 포함할 수 있다. 메모리는 컴퓨터-판독가능 매체의 일 예이다.

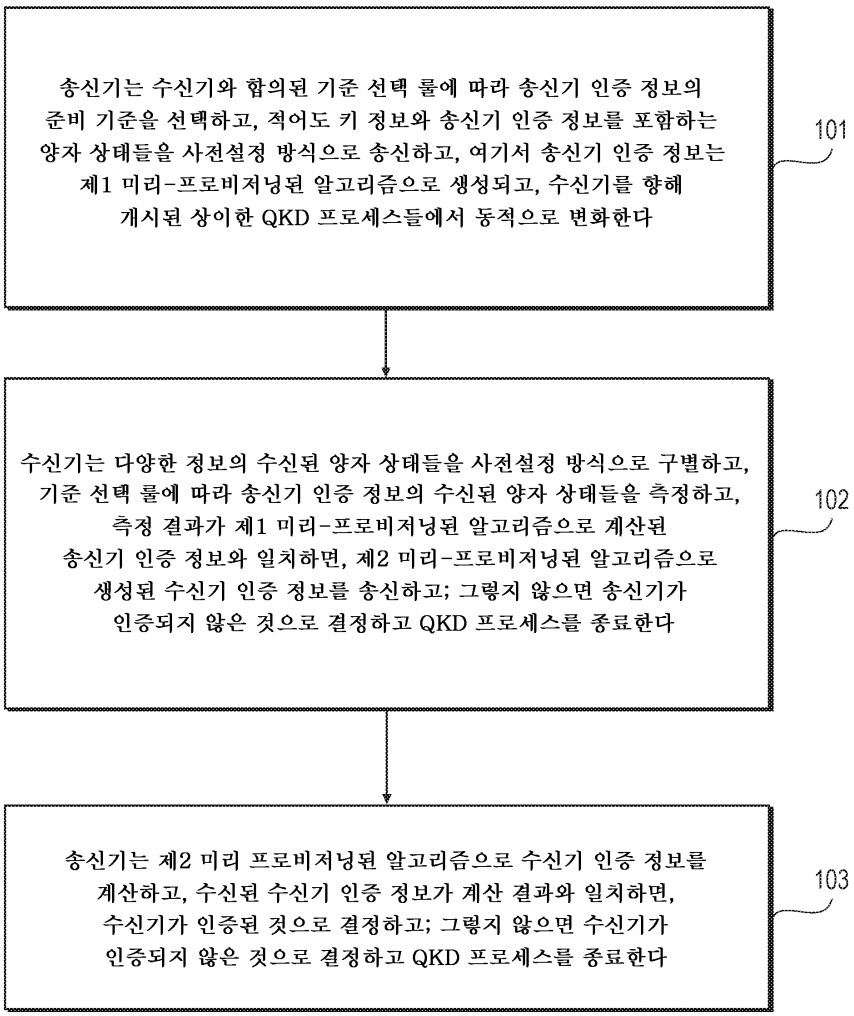
[0236] 컴퓨터-판독가능 매체는, 임의의 방법 또는 기술에 의해 정보 저장을 구현할 수 있는 비-휘발성 매체, 휘발성

매체, 이동 매체 또는 고정 매체를 포함한다. 정보는 컴퓨터-판독가능 명령, 데이터 구조, 프로그램 모듈 또는 기타 데이터일 수 있다. 컴퓨터 저장 매체는 예로서, 상 변화 랜덤 액세스 메모리(PRAM), 정적 랜덤 액세스 메모리(SRAM), 동적 랜덤 액세스 메모리(DRAM), 다른 유형의 랜덤 액세스 메모리(RAM), 판독-전용 메모리(ROM), 전기적으로 소거가능한 프로그램가능 판독-전용 메모리(EEPROM), 플래시 메모리 또는 다른 메모리 기술들, 컴팩트 디스크-판독 전용 메모리(CD-ROM), 디지털 다기능 디스크(DVD) 또는 다른 광 메모리들, 카트리지 자기 테이프, 자기 테이프 또는 자기 디스크 메모리 또는 다른 자기 저장 디바이스, 또는 컴퓨팅 디바이스에 의해 액세스될 수 있는 정보를 저장하도록 구성될 수 있는 임의의 다른 비-송신 매체를 포함하지만, 이에 한정되는 것은 아니다. 본 명세서에 정의된 바와 같이, 컴퓨터-판독가능 매체는 일시적 매체, 예를 들어 변조된 데이터 신호 및 캐리어를 포함하지 않는다.

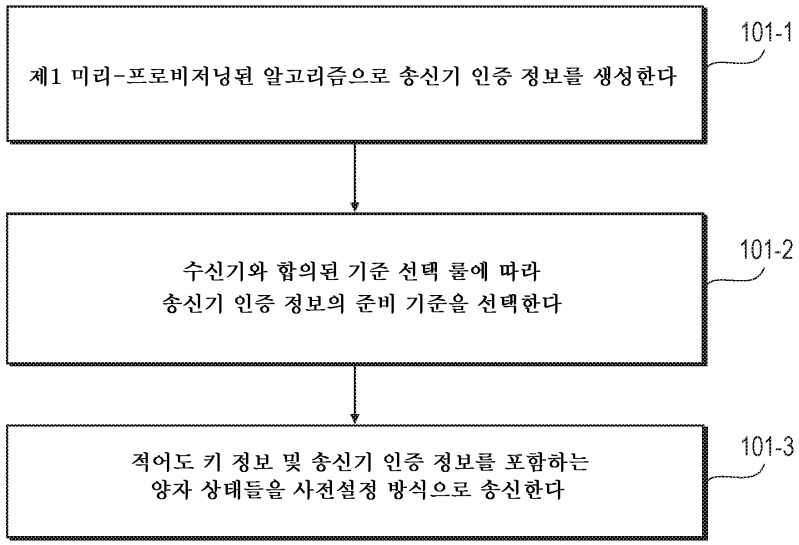
[0237] 통상의 기술자는, 본 출원의 실시예가 방법, 시스템 또는 컴퓨터 프로그램 프로덕트로서 제공될 수 있음을 이해해야 한다. 따라서, 본 출원은 완전한 하드웨어 실시예, 완전한 소프트웨어 실시예, 또는 소프트웨어와 하드웨어를 결합한 실시예의 형태일 수 있다. 또한, 본 출원은 하나 이상의 컴퓨터 저장 매체(자기 디스크 메모리, CD-ROM, 광 메모리 등을 포함하지만 이에 한정되지는 않음) 상에 구현되는 컴퓨터 프로그램 프로덕트의 형태일 수 있으며, 이는 컴퓨터 프로그램 코드를 포함한다.

도면

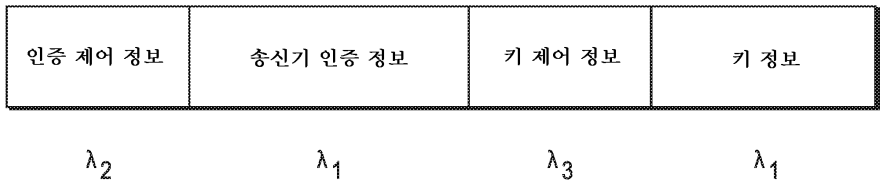
도면1



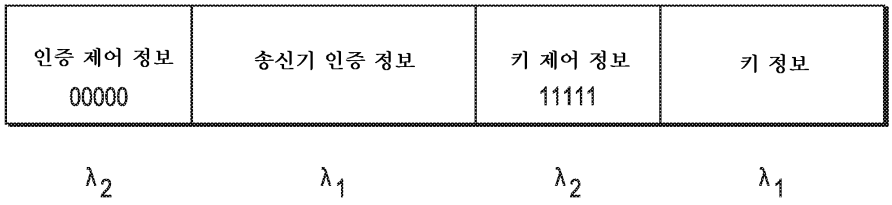
도면2



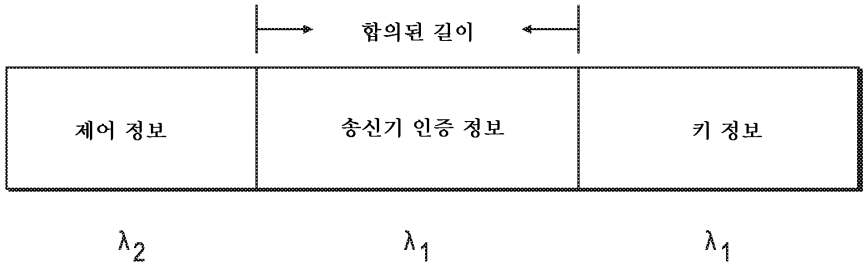
도면3



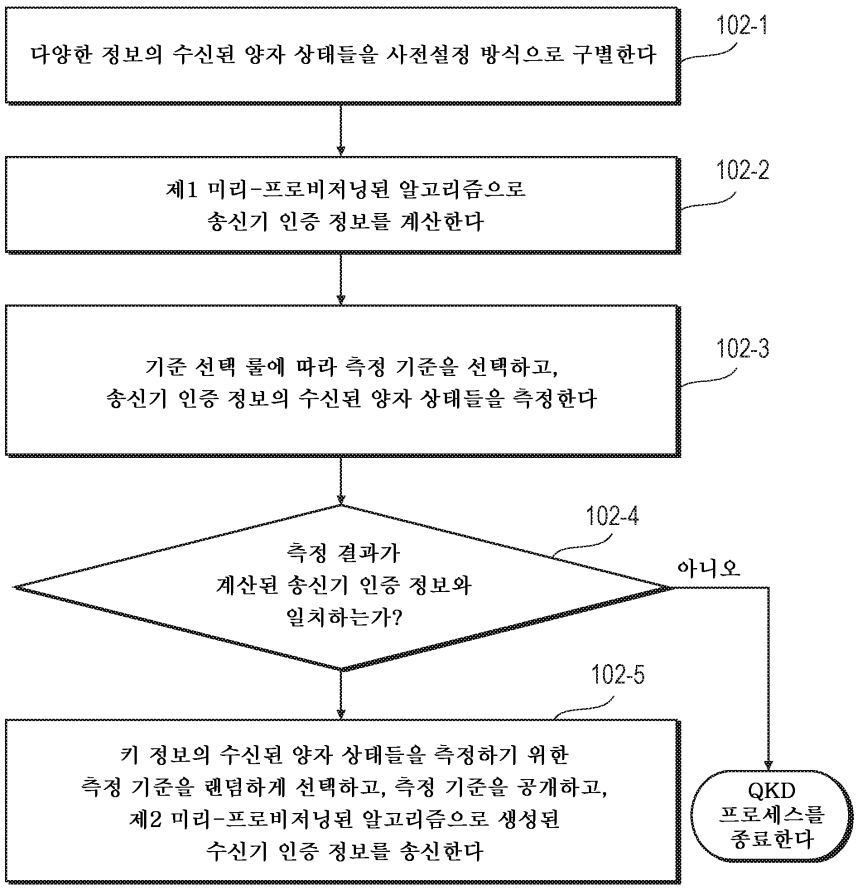
도면4



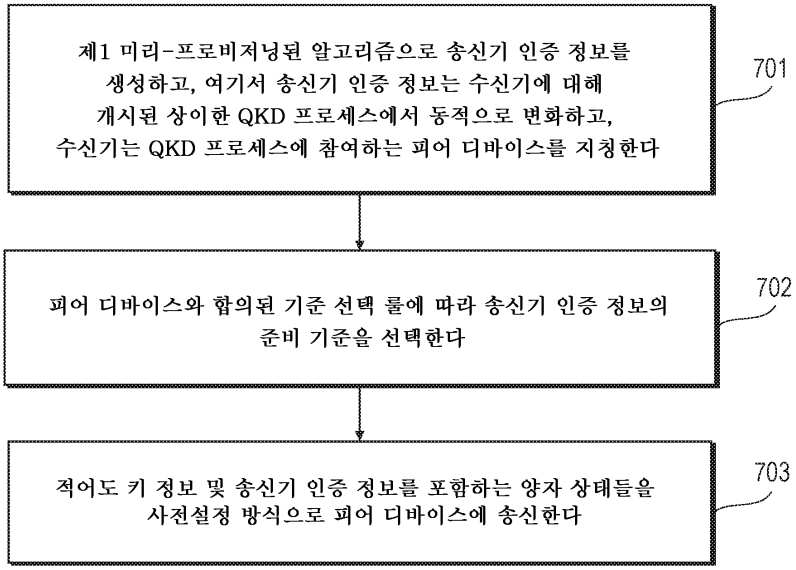
도면5



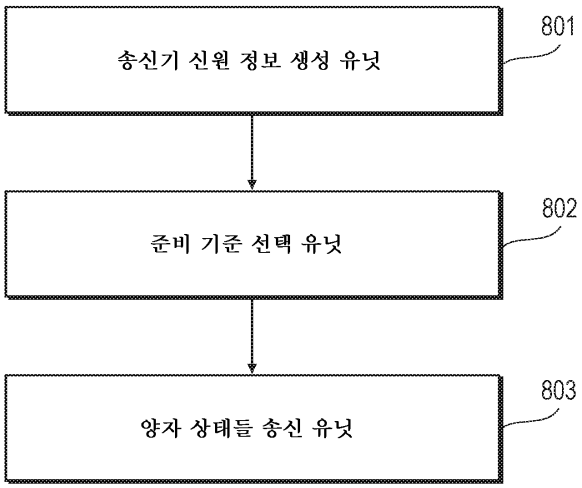
도면6


다양한 정보의 수신된 양자 상태들을 사전설정 방식으로 구별한다
102-1
제1 미리-프로비저닝된 알고리즘으로
송신기 인증 정보를 계산한다
102-2
기준 선택 룰에 따라 측정 기준을 선택하고,
송신기 인증 정보의 수신된 양자 상태들을 측정한다
102-3
측정 결과가
계산된 송신기 인증 정보와
일치하는가?
102-4
아니오
키 정보의 수신된 양자 상태들을 측정하기 위한
측정 기준을 랜덤하게 선택하고, 측정 기준을 공개하고,
제2 미리-프로비저닝된 알고리즘으로 생성된
수신기 인증 정보를 송신한다
102-5
QKD
프로세스를
종료한다

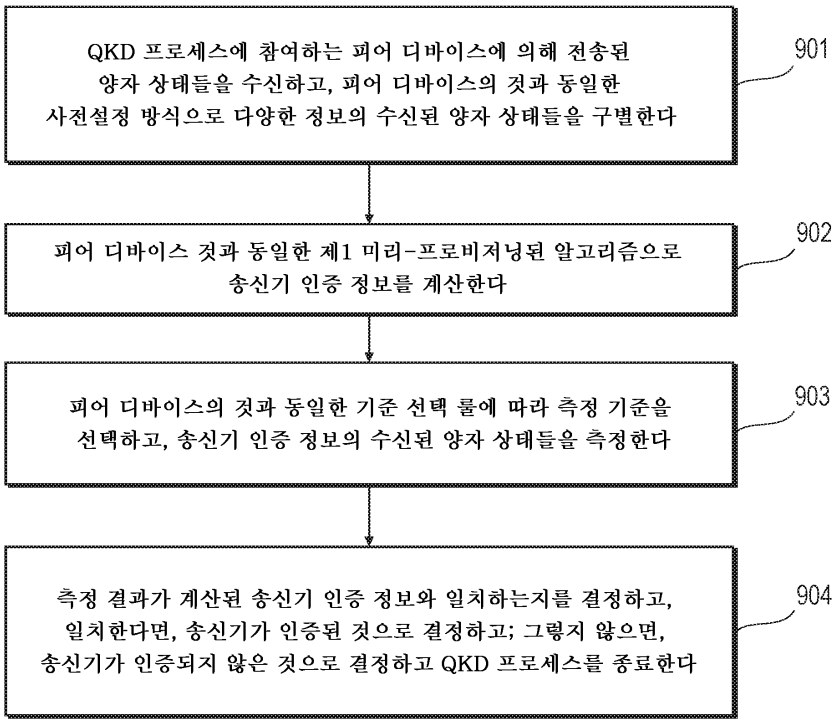
도면7


제1 미리-프로비저닝된 알고리즘으로 송신기 인증 정보를
생성하고, 여기서 송신기 인증 정보는 수신기에 대해
개시된 상이한 QKD 프로세스에서 동적으로 변화하고,
수신기는 QKD 프로세스에 참여하는 피어 디바이스를 지칭한다
701
피어 디바이스와 합의된 기준 선택 룰에 따라 송신기 인증 정보의
준비 기준을 선택한다
702
적어도 키 정보 및 송신기 인증 정보를 포함하는 양자 상태들을
사전설정 방식으로 피어 디바이스에 송신한다
703

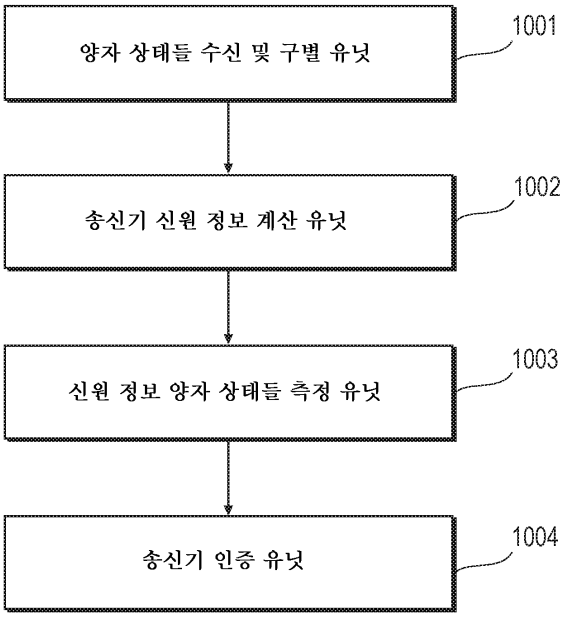
도면8


송신기 신원 정보 생성 유닛
801
준비 기준 선택 유닛
802
양자 상태들 송신 유닛
803

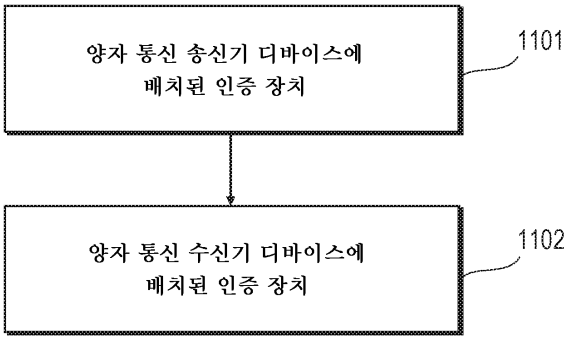
도면9


QKD 프로세스에 참여하는 피어 디바이스에 의해 전송된 양자 상태들을 수신하고, 피어 디바이스의 것과 동일한 사전설정 방식으로 다양한 정보의 수신된 양자 상태들을 구별한다
901
피어 디바이스 것과 동일한 제1 미리-프로비저닝된 알고리즘으로 송신기 인증 정보를 계산한다
902
피어 디바이스의 것과 동일한 기준 선택 룰에 따라 측정 기준을 선택하고, 송신기 인증 정보의 수신된 양자 상태들을 측정한다
903
측정 결과가 계산된 송신기 인증 정보와 일치하는지를 결정하고, 일치한다면, 송신기가 인증된 것으로 결정하고; 그렇지 않으면, 송신기가 인증되지 않은 것으로 결정하고 QKD 프로세스를 종료한다
904

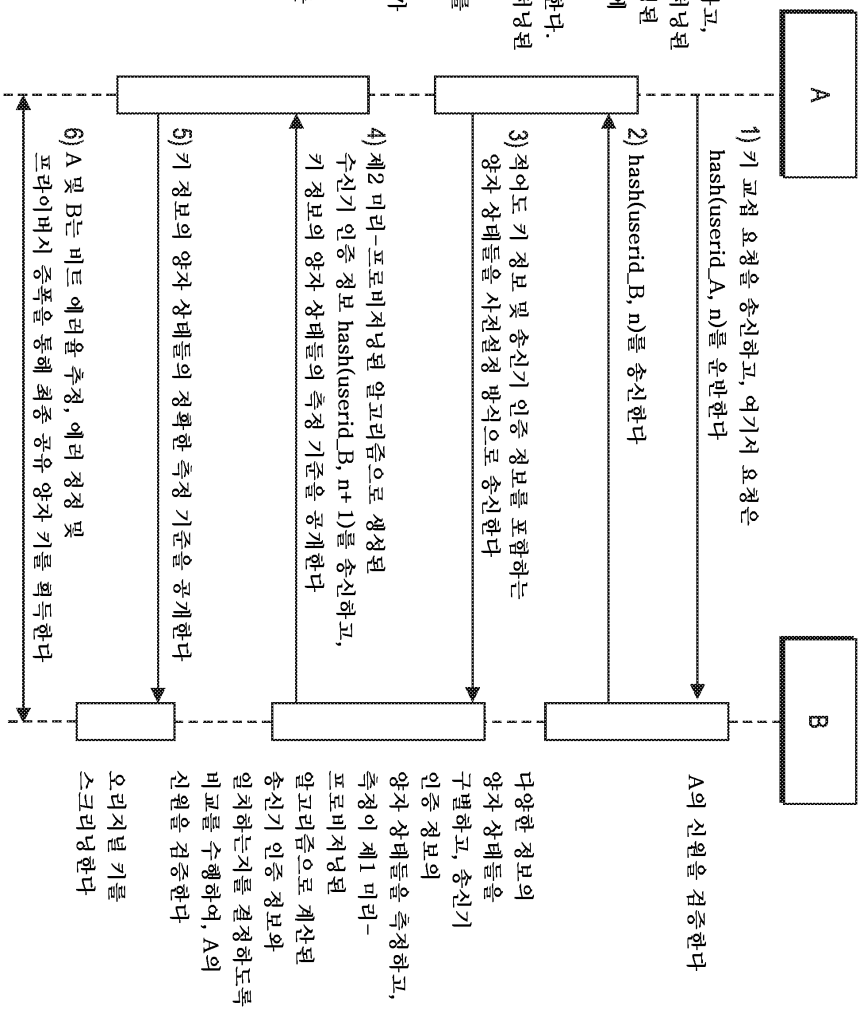
도면10


양자 상태들 수신 및 구별 유닛
1001
송신기 신원 정보 계산 유닛
1002
신원 정보 양자 상태들 측정 유닛
1003
송신기 인증 유닛
1004

도면11


양자 통신 송신기 디바이스에
배치된 인증 장치
1101
양자 통신 수신기 디바이스에
배치된 인증 장치
1102

도면12


A
B
1) 키 교섭 요청을 송신하고, 여기서 요청은 hash(userid_A, n)를 운반한다
2) hash(userid_B, n)를 송신한다
3) 적어도 키 정보 및 송신기 인증 정보를 포함하는 양자 상태들을 사전설정 방식으로 송신한다
4) 제2 미리-프로비저닝된 알고리즘으로 생성된 수신기 인증 정보 hash(userid_B, n+ 1)를 송신하고, 키 정보의 양자 상태들의 측정 기준을 공개한다
5) 키 정보의 양자 상태들의 정확한 측정 기준을 공개한다
6) A 및 B는 비트 에러율 추정, 에러 정정 및 프라이버시 증폭을 통해 최종 공유 양자 키를 획득한다
B의 신원을 검증하고, 제1 미리-프로비저닝된 알고리즘으로 생성된 송신기 인증 정보에 대한 대응하는 준비 기준을 선택한다. 제2 미리-프로비저닝된 알고리즘으로 수신기 인증 정보를 계산하고, 수신된 수신기 인증 정보가 계산 결과와 일치하는지를 결정하도록 비교를 수행하여, B의 신원을 검증하고; 오리지널 키를 스크러닝한다
A의 신원을 검증한다
다양한 정보의 양자 상태들을 구별하고, 송신기 인증 정보의 양자 상태들을 측정하고, 측정이 제1 미리-프로비저닝된 알고리즘으로 계산된 송신기 인증 정보와 일치하는지를 결정하도록 비교를 수행하여, A의 신원을 검증한다
오리지널 키를 스크러닝한다