29. (KR1015901050000*) P 2 M P 네트워크에서 광자수 분리 공격 (P N S) 을 감지할 수 있는 양자 키 분배 방법 및 시스템

국내 서지정보 | 명세서 | 청구범위 | 도면 | 서류

퍼머링크

출원번호: 1020150014467 **출원일:** 29.01.2015

공개번호: 1015901050000* **공개일:** 01.02.2016

공개유형: B1

IPC: H04L 29/06
H04B 10/70
H04L 9/08

출원인: 한국과학기술원

발명자: RHEE, JUNE KOORHEE, JUNE KOO
LIM, KYONG CHUNLIM, KYONG CHUN
KO, HAE SINKO, HAE SIN
이준구
LEE, CHANG HEELEE, CHANG HEE
임경천
SUH, CHAN HOSUH, CHAN HO
고해신
이창희
서창호

대리인: 특허법인충정

우선권 정보

발명의 명칭: **(KO)** P 2 M P 네트워크에서 광자수 분리 공격 (P N S) 을 감지할 수 있는 양자 키 분배 방법 및 시스템
(EN) QUANTUM KEY DISTRIBUTION METHOD AND SYSTEM CAPABLE OF DETECTING PHOTON-NUMBER SPLITTING ATTACKS IN P2MP NETWORK

요약서: **(KO)** 본 발명은 양자 암호 키 분배 방법 및 시스템에 관한 것으로서, 보다 구체적으로는 P2MP(Point to Multi-Point) 네트워크에서 광자수 분리 공격(PNS attack)을 효과적으로 감지하여 도청자의 공격에 대응할 수 있는 양자 키 분배 방법 및 시스템에 관한 것이다. 본 발명은 송신부와 복수의 수신부가 양자 채널로 연결된 P2MP(Point to Multi-Point) 네트워크에서의 양자 키 분배 방법에 있어서, 상기 송신부에서 송출되는 복수의 펄스에 대한 평균 광자수와 상기 복수의 수신부에서의 펄스 수신 정보를 수집하는 정보 수집 단계; 상기 송신부에서의 평균 광자수와 상기 복수의 수신부에서의 펄스 수신 정보 및 수신부의 숫자를 고려하여 상기 양자 채널에서의 광자의 손실률을 산출하는 광자 손실률 산출 단계; 상기 손실률을 고려하여 상기 복수의 수신부에서의 펄스 수신 분포 예측치를 도출하는 펄스 수신 분포 예측치 도출 단계; 상기 복수의 수신부에서의 펄스 수신 정보로부터 상기 복수의 수신부에서의 펄스 수신 분포 측정치를 도출하는 펄스 수신 분포 측정치 도출 단계; 및 상기 펄스 수신 분포 예측치와 상기 펄스 수신 분포 측정치를 비교하여 광자수 분리(Photon Number Splitting) 공격의 여부를 판단하는 공격 여부 판단 단계를 포함하는 것을 특징으로 하는 양자 키 분배 방법을 개시한다.

(EN) The present invention relates to quantum key distribution method and system and, more specifically, to quantum key distribution (QKD) method and system capable of detecting Eves photon-number splitting (PNS) attacks in a point-to-multipoint (P2MP) network, thereby responding against the attacks. The QKD method in a P2MP network in which an Alice and multiple Bobs are connected through a quantum channel comprises: an information collection step of collecting mean photon numbers of multiple pulses transmitted from the Alice and pulse reception information at the multiple Bobs; a photon loss calculation step of calculating a loss rate of photons at the quantum channel with consideration for the mean photon numbers at the Alice, the pulse reception information at the multiple Bobs, and the number of Bobs; a pulse reception distribution expectation deriving step of deriving a pulse reception distribution expectation at the multiple Bobs with consideration for the loss rate; a pulse reception distribution measurement deriving step of deriving a pulse reception distribution measurement at the multiple Bobs from the pulse reception information at the multiple Bobs; and an attack determination step of determining whether there is a PNS attack by comparing the pulse reception distribution expectation and the pulse reception distribution measurement.