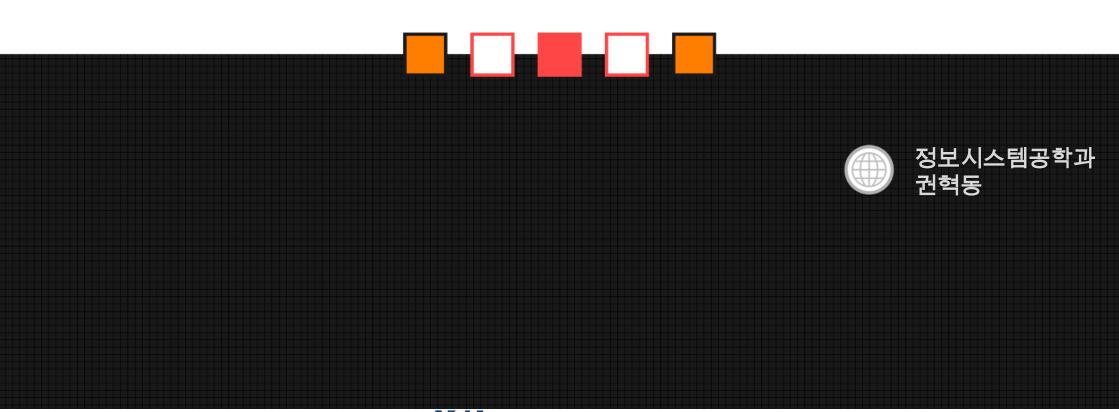
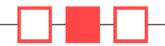
양자통신상의 가용성침해공격

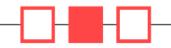
An Availability Invasion Attacks on a Quantum Communications





CONTENTS

- 01 보안의 3요소
- 02 양자
- 03 양자통신
- 04 제안기법
- 05 결론



01 기밀성 | Confidentiality

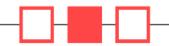
인가되지 않은 제 3자는 정보에 접근할 수 없어야 한다.

02 무결성 | Integrity

전송된 데이터가 원본과 동일하며 수정되지 않았을 보장한다.

03 가용성 | Availability

인가된 사용자는 항상 손쉽게 정보 접근이 가능하다.



01 기밀성 | Confidentiality

Sniffing, Scamming, Traffic analysis

02 무결성 | Integrity

Spoofing, Modification, Fabrication, Masquerading, Replaying, Repudiation

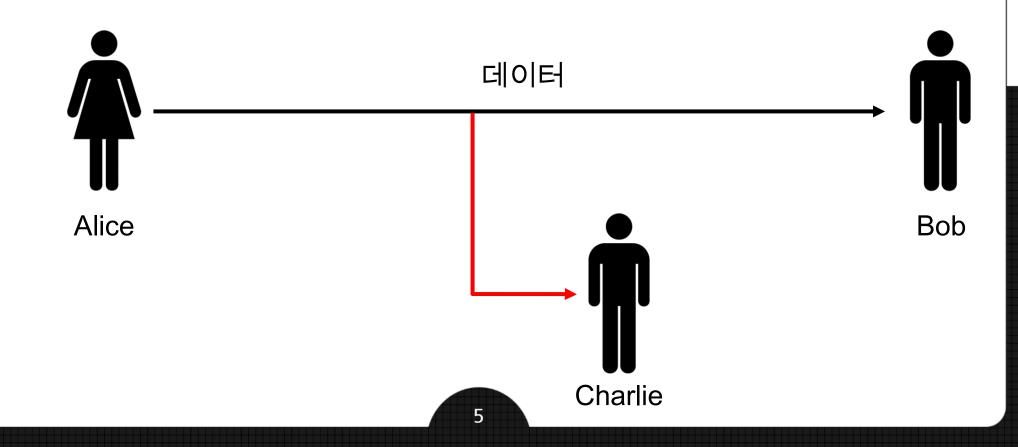
03 가용성 | Availability

Denial of Service, Interruption



스니핑 공격 | Sniffing attacks

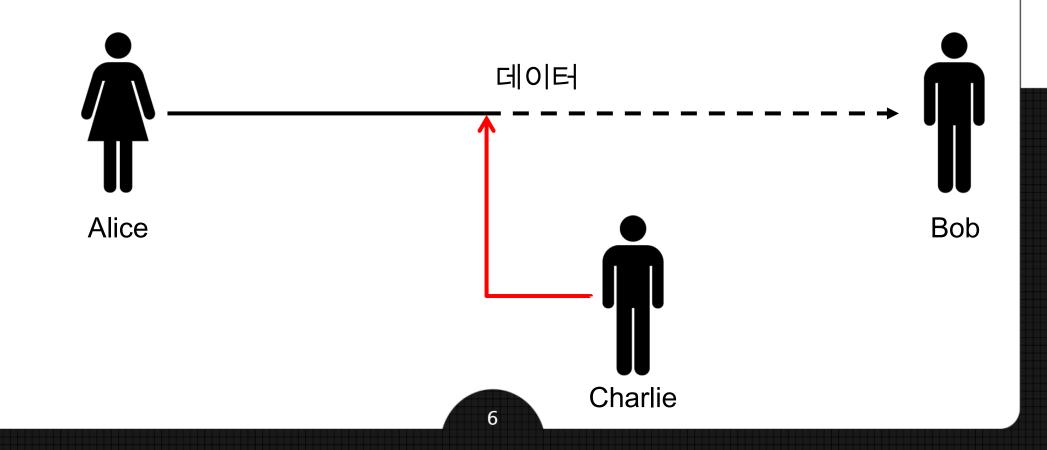
통신의 주체가 아닌 제 3자가 통신 채널을 감청하여 데이터를 관찰하는 공격

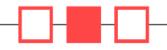




서비스 거부 공격 | Sniffing attacks

통신 자체가 이루어지지 않도록 방해하는 공격





양자 | Quantum

1899년 독일의 물리학자 막스 플랑크가 제시

더 이상 나눌 수 없는 에너지 최소량의 단위

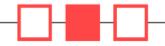
고전역학이 적용되지 않는 일부 특이한 성질 보유



01 양자 중첩 | Superposition

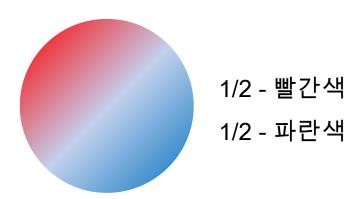
02 양자 얽힘 | Entanglement

03 양자 붕괴 | Collapse



01 양자 중첩 | Superposition

모든 양자는 일정한 확률을 가지고 상태 구성에 기여함 관측되기 전 까지는 가능성에 따라 여러가지 상태로 동시에 존재 가 능





02 양자 얽힘 | Entanglement

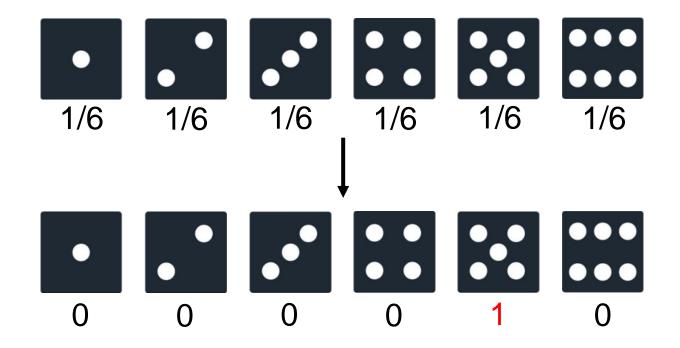
서로 연관이 있는 양자는 한쪽의 상태를 관측하는 순간 다른 쪽의 상태도 결 정됨

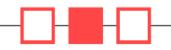
상태가 확정되는 현상은 가 이 가 상된 이 기 즉시 발생



03 양자 붕괴 | Collapse

양자를 관측하는 순간 중첩상태에서 벗어나는 현상 다른 상태가 될 확률은 전부 제거되며 한 가지의 상태가 될 확률만 존재





03 양자통신

01 통신 프로토콜 BB84

1984년 C. H. 베넷, G 브라사드가 제안

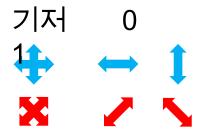
송신자와 수신자간 OTP를 생성하는 프로토콜

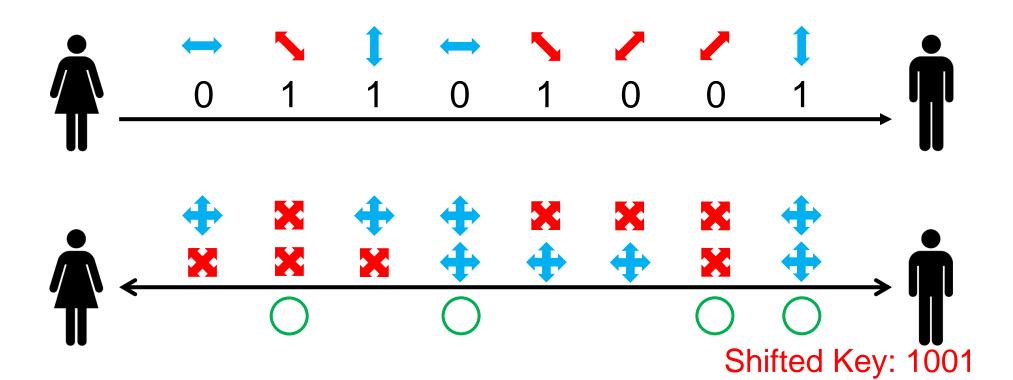
양자 키 분배: Quantum Key Distribution (QKD)

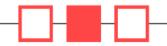


03 양자통신

01 통신 프로토콜 BB84



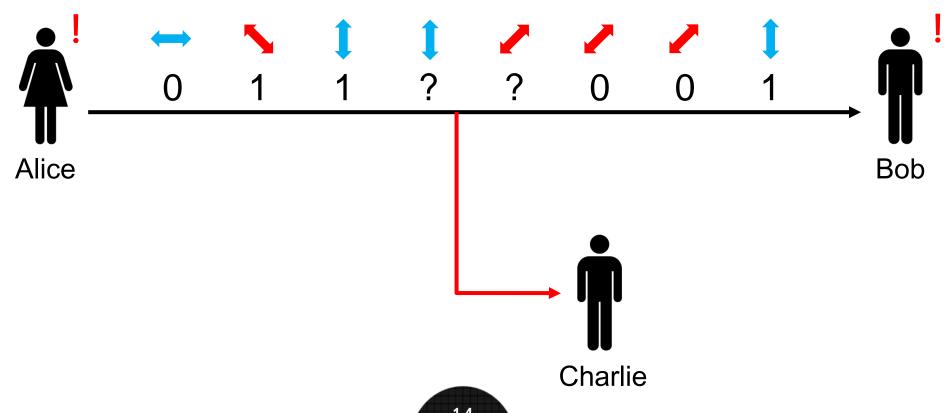


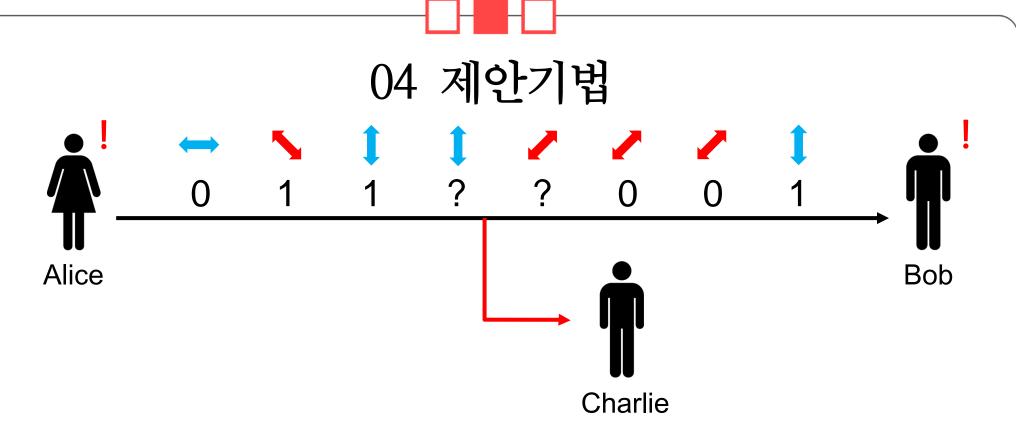


03 양자통신

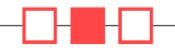
01 통신 프로토콜 BB84

양자 에러 비트율 | Quantum Error Bits Rate (QBER)





지속적인 양자채널 관측을 통해 QBER를 상승 본디 통신을 의도한 사용자들은 QKD의 진행이 불가능 공격자가 관측을 중단하기 전 까지 통신 개시가 어려움



05 결론

01 고전 채널 상에서의 스니핑 공격은 기밀성 침해 공격 공격자가 수동적이며 데이터를 훔쳐보는 선의 공격

02 양자 채널 상에서의 스니핑 공격은 가용성 침해 공격 통신 주체간 정상적인 통신 진행을 방해함

03 통신 채널 자체를 보호할 수 있는 수단이 필요함

원국정보육성숙 회원문자 [Vol. 17. No. 8: 899~408, hor. 2018]

LEIN

LIEILE

양자 통신 환경 상에서의 가용성 침해 공격」

An Availability Invasion Attacks on a Quantum Communications J

#여기도 삭제"/Hyeok-Dong Kwon " Hun-jeong Seol " ,)

"Department" of Information System Engineering, "Hansung University," Seoul "02876," Korea " *Department' of '11" Engineering, 'Hansung' University,' Seoul' 02876," Korea J //이 위도 삭제 // J

B"" 27 J

보안되3요소로 할머니까? 말성,"구절성,"가용상'중'대핫"스니팡"중대은 기밀성'중 대에"대당한다."스니팡"중대은 '동 산대용 "파악은 어렵지만 등 산대상이 아닌 제3자가 중 산대용을 "엿볼"수 있다. "인원적으로 기밀 상"공격은 계획자에 게 되겠다면 방향을 꺼치는 부분이 먹으며 정보가 곧 여자에게 노름되어라도 대가 방호화되어있기 때문에 대회로 곧 격차가 점목 가능 한 정보는 함호화 함 때닷 선 예사 그런다. 양자 등신은 선 기 선호를 내 처하여 공간적인 병 힘을 가할 수 있는 '양자를 활용한 새로운'동산으로 기존의 동산보다'일동한 뭐리'속보를 보여를 것으로 '기대되다.'양자의 외부 에서 결축할 사명되었다는 특성을 이용하면 동안내용이 노근되어도 본래의 내용을 참 할 수 있다. 본 논문 에서는 이 러한 양자의 독성에 집중하여 따켓 스니핑 공격 이 가용성 함께 공격으로 공격의 및 형이 달라지는 것 예쁜 하여 달라본 ch" J

ABSTRACT" J

The confidentiality, integrity and availability are known as the three goals of security among them, packet sniffing attack is a lassified confidentiality invasion attacks. The sniffing attack can funderstand contents of communications. but a third person who is unauthorized can eave sdropping the contents. In general, a confidentiality at tack is less likely to be directly impacted by the victim, and even if the information is esposed to the attacker, it is usually encrypted so that 'the 'attacker' difficult' obtain 'original 'message." The 'quantum' communications' are 'expected lio' show 'faster' than' current communications method by using quantum which has superposition. The quantum collapsed when they are observed, even if the communication contents are exposed, the original can be hidden. In this paper, we concentrate on quantum characteristics, and examine the types of packet softing attack change to a variability invasion at tacks." "J

키워드': '양자' 통신, '패킹' 스니핑' 공격,' 서비스' 거부,' 가용성 J

Key word : "Quama a mananama, Pada sa fling and, Dand of Sarra, Arabbility 🜙

"Borned 29" December 2014," "Accepted 21" January 2015 🚚 Boosed 29 Newsonia 2014 (E#444448) J

*Chrospad & Adler Bra-jong Sca(C-cod/hrajeng@hou gast le Tel:-02-24-03-000) 🌙 Department of TT Lag seeing Banang To see 14, Seed 12274, York ...

Casa Acass (449 j http://doi.org/10.6109/jkilice.2018.17.2.399****

n ISSN 221

இந்த இந்த பட்டும் இது போக்கு இகம் கேக்கில் அந்த கேட்டை சட்டும் போக்கு இணையால் நக்கிய இன்று ஊரும் நுறைபடுக்கு வரச்சிய நிறு விறு வரச்சிய நிறு வரச்சிய நிறிய நிறு வரச்சிய நிறு

한국역 1 등 4약의 는문에 Vol. H. 20. 2, 200 -400, Mar. 2013.

I."서""통J

오늘날 속보가 기름해서 항상되는 한터넷 확정하다 불어"과공"스마트"기기의"발전은"생활에 큰"편리함을" 가져오게"되었다."특히"은라인상의 동신은"우리"생활에" 매우 필접한 관계가 되었으며 자연스레 보안 위험도 따 하고 기계에다 시

이에 따라 '사이버' 보안은 '각종' 보안 위험으로부터 경 보문"보호하기"위해"기필상(confidentiality)," 뮤고션 (integrity), 가용성(availability)의 세 가기를 보안 요소 로 게시(네하게 되었으며 '각각의'의 이는 '다음파'같다. 니

기밀성은 '인가되지'많은 '제'3자가'에이 터를 열람하 거나 "확인함"구" 없다는 "속성이다." 극,"이 미 정보가 함호 화 되었더라도 하가 권이 없는 사용자는 참호화 된 데이 터고 가 확인함 '수 없어야 한다.' 시

무결성은 건송된 케이터가 원본과 동일하다 수정되 지않았음을 보장하는 생일이다. "수정이 뜻하는"범위는" 안순히"레이터의"일부를"변경하는"것뿐만"아니다"추가 적인 케이터의 생생 또는 "삭제까지 포함하는 "것으로 포 관적인 범위이다",

가용성은 '하가'된 '사용자가' 먼지든지 '레이터데' 접근 할 수 "있는 "환경을 "제공하는"것으로 "데이터는 "시시 각각" 변화할 수 있지만 정보의 현장 상태는 지속적으로 가능 하야 함을 의미한다."이러한 보안 '요소예' 따라서 '표 1161 파갈이 여러 보안 위험을 본유한 수 있다. 나

Table "d"Time" of cars of his absolute. I

Affect type -	Attacksome -
Cardidentially invesion at	Briffing + Staroving + Raffic malpois +
Marty in mineral	Specific - Multification - Februation - Responding - Responding - Responding -
Availability investors at	Devis) of Servis.

지금까지 의 동안 환경은 '건기' 신호를 '이용한 '것으로 건기 '신호의'유투에'따라'()과'(의'이긴'강을'사용하여' 등신이 이루어진다. '하지만 '양자' 음리학을 '활용한 '양자'

등산이 새롭게 꾸득받고 있다. 나

[여러달(파우 목1)[여러달(홀수 목1)]목 원호 위치] 』 양자(동신은 빛의)최소(현위인 광자(photon)문)사용 한 것으로 기준의 등신 환경은 '0과' (의 이건 정보만을 건말했지만 말자 등신은 이건 '검보뿐만' 아니라 중천되 상태의 정보를 보면수도 있다. 나

> 양자' 등신의 '가장' 큰 '장점은' 스니핑' 공격(sniffing" attacks)에 강하다는 것이다. 누군가가 개념을 감시하며 정보가 유금되고 있다는 점을 빠르게 확인할 수 있대요. n)."이러한 방어가 가능한 이유는 '양자의'록성에'기인하 는데, '양자는' 전축을 '하는 '순간' 가지고 '있던' 값이' 달라 지며"이 가을 복원한 수 없게"되기"라는이다."이 현상을 양자"붕괴라"부른다. 기

반대로 할아양자 봉회가 발생하게 되면 누신자 속도" 송신자가 보면 원래의 데이터를 확인할 수 없기 때문에" 등산"자체 때" 매교사항이" 생긴다." 이" 원리를 "이용하면" 양자 동산상에서 고현 동산파는 다른 새로운 유행의 가 흥성'꾸격이'가능하다. 니

본 논문 에서는 "이와 같이"고면 '동산상에 서 '피킷 '스니 평'국과이'기밀성'국과으로'본유되지만'양자'동신상대 서는 가용성 공격으로 본류할 수 있음을 확인한 것이다. 구성은 2장에서 관련 '현구' 등장을 '살려보며 3장에서 극 ·계'시나리오라'가능성데'대한'분석을'게 사하고'4장에서' 결론을 짓는다. 나

Ⅱ. '판현 '연구 '동향」

본 장에 서는 항차 등신화 관련 한 연구와 '기관이 '되는" 양자에"대해"알아볼"청이며"양자"등신을"위해"되시된" 프로프론을 확인하는다. 나

2.1 양자 J

양자는 1899년 독일의 음리학자 학스 등광고(Max" Planck)가 '흑세' 부사라 '관련된'은 제품 '현구하던' 보증" 생료은 상수를 발전하였고 끝장고 상수라 병병하였다. 그 '후 '존광크' 상수문' 사용하여 '존광크의 '복사' 법칙을 ' 발전하였고"이"법칙을"실명하기"위해"최초교"양자의 개념을 돼지하였다며. 그

양자는 어이상나 군수 없는 에너지의 회소장의 안 위."복사"에너지에서"처음"발전하여" 에너지"양자"라고" 불렀으며"그것이"빛으로서"공간을"진행할"경우" 광양

05 결론

1241 1244 254 Vol. B. No. 2: 300-400, Mar. 2013-

3자가 동신을 도청하여 내용을 확인하게 된다면 그 순 간양자가 '봉회하여' 수신자축에서는 '송신자가 '천송한' 그림 '6에' 따라 함호 '처음 '생성하는 '첫 이 가능하다 니 정보되는 '다른'정보를 '받게' 되기에 '도청' 사실을 '한식 할 수 있다. 본 내용은 3장에서 '좀 '더 '차세히' 서울하도 **等性味」**



1. Before rolling the dice, each probability is 1/6

2. Rolling the dice

to 0 except 5, and probability of 5 collapses to 1













Pg. 2 The example of Guanium Collapse 🚚

22'양자동산'프로프론 ...

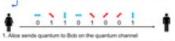
BB84'프로트들은''1984년'할스'H.''버렛파'일'보라사 트가 계안한양자 등산프로트를로서 송산자라 수산자 간 OTP(One Time 'flid)를 성성하는 프로트들이며[n]" 가장"널리"알려진"회초의"많자"기"분배(Quantum"Key Distribution, 'QKD) 이다 'BB84의 '따른' 양차가 본배'원 리는"다음과"같다. 니

기본적으로 '양자' 채널을 '등해' 정보를 '보내기'위해 서는 양자의 역장에 정보를 인코딩해야한다. 표현에 따 라 전쟁은 '괴교' 대작'무 '가지의 '기저(basis)를 '가고'수" 있다."한약"되고기저를"사용한다면"수정점장에는 10."수 괴래장에는" (을" 인코랑하고" 마찬가지로" 대각기저를" 사용한다면 대 과격 장에는 'U.'원래 과경 장에는 'L을'인 크 정한다. 니

Table. 2 The quantum's tale corresponding to the cryp lographic key usite 🌙

Beck ↓	Value 0.	Value 1.
+(Textilines; 10 .	₩.↓	1.1
×[근과 광지기]	/(在外面	がまり

인크링을 등해 '편장에' 따른' 값이 '정의되었으므로'



2. Bob measures quantum



Shifted Key 1001 4. Use bits with the same bases as the shifted key

5. Get secret key from shifted key [=] +

Rg. "S"The BBS+ protocd working fow J

우선 '송산자'축의 '웰킹스가' 임의의 "비트를 생성한" _ 함을 '해당' 비트를 '대장' 신호로 '변정 하기 '위한' 기 처음' 선택하여 '인코딩한다' 단 '선택' 과정은 '양자'는수를 '등 해"무막위로"선택한다"이때"빨리스는"인코딩을"등해" 취득한 양자를 양자되었을 동네 건승하며 자신이 생성 한비트라 '선택한'기저를'기록한다. 니

수전자 축의 밥은 자신이 축정하고 실은 임의의 기 저는 선택하고 수신한 양자는 선택한 기치를 통해 밝 을 '최목한다. '멀리스의' 다 참가지로 '밥은 '축성한' 강파' 선택한기 처음 기록한다.

이후 '빨리스와 '함은'서로 '공개' 웨턴을 '등에' 서로 '현 대한기 저는 '고환하며' 같은 '기 저는 '사용했는 지' 검증을 ' 한다. '점공' 결과 '같은' 기저를 '사용한' 비트에' 대해 서는 값을"저장하고"그"의의"비트예"대해서는"과기한다"이 백 점류한 기 '라운 '시프트' 키(shifted key)라 칭한다. '시 프트'키'경상'파함에는 '누군가가' 채널을 '도청하고' 있 을"가능성이"있기"때문에"빨리스와"밥은"생성된"키의" 일부를 서로 공개하여 오류의 비운을 계산한다는이 를 QBER(Quantum Bir Error Rate)라 항하다 이 비 윤이 임계점을 넘어산비트는 누군가에게 정보가 유근된 첫 으로 간구하고 하기한다. 나

QBER까지 계산하여 최종적으로 남은 비트를 비밀 키(secretkey)로"사용하여"빨리스라"밥"사이의"키"교환 이공료된다.

트 + BB84'프로트들의'도청'억부'확인은'양자'붕피'특성 을"이용한"것이다"공격자가"캐널에서"건송되는"강을" 희목하기"위해"스니핑"공격을"시도하면"건송된"양자는

사람의 TES라다 유는 계수 "

'차'라고'한다.'라고'청의되어있다(a)."다시"말해"원차 '예"따르면"원래부터"꾸더니예"서로"다른"책의'공이'문 가'를 필의"기호"단위하면"양자는"에 너지의"기호"단위 가'되는'것이다. 나

양자는 "고전역학을 "적용하기" 어려운 "임부" 특이한 " 과단적"공이 들어있는 것이 "정해진다." 니 성권을 가지고 있으며 이는 2.11, 2.12, 2.13과 같다. 나

21.1 일자·공합 』

안에서"한가지의 "상태안을" 가진다." 에컨대" 생명치를 " 권축할 경우 "살아있거나"국어있거나"를 공 하나만의 상태를 '가진다.'이는 '임상적인'경험에서' 중분히 '확인 : 할"수"있는"사실이다."아지만"양자역학의"편경에서는" 다르다 '양자역학의 '관점에서는 '상대가' 입정한 '확군을 가지고 '상태'구성대'기억한다는 '것이다.'어떤 생명체 가 있다면 '양자역학의'가 넘어 서는 '살과' 극은의 '가능성 이 모두 가능한 복합적인 상대로 표현된대 비닐 니

이러한 개념을 당자 중청(superposition)이라 한다." 양자는 권축되기 "전"까지는 "가능성에 따라 "억러 "가지" 상태로 동시에 존재 할 수 "있다"이는 무 가지 이상의" 상태가 동시에 적용되어 존합된 모습을 뜻하는 것이 아니다 "먼저문지"여러 상태 중 권축에 따라 특성 상태 문'확실하게'산준환'수"있다는"가능성을'지난'상대로" 이해되어야한다.

21.2 양자 범인 J

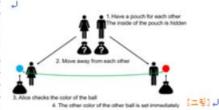
양자 엄청은 양자의 가장 목이한 성권로 고전역학 과 가장 프게 궁물하는 목성이다. 이를 쉽게 서술한다 현 서로 관계있는 '양자는 '아무리' 거리를 두더라도 계 속해서 서로에게 영향을 준다며 그

가장 중요한 점은 변화가 즉시 일어난다는 점이며 특히 "거리에"상편없이"일어난다는"특징이"있다."가령" 무게의 양자가 인상적인 범위를 벗어나 내 우구 공간에 걸처"덜어져"있더라도"하나의"양자문"축청하는"순간" 다른 '양자의'특성이' 거리에 '주변하게'즉시'변화한다. 니

이는"그림"(과 같이"실렁"한"수"있다."널리스라"밥이" 서로 '내부가'보이지'않는 '구머니데'만 '수' 없는 '색희' 공 을 하나씩 넣고 나눠가지며 이때 공은 빨간데 또는 다 단적을 확근적으로 가진 수 있다고 가정한다 이후 시 로" 멀리 "ভ어 긴" 장소로"이 등하여" 빨리스가" 주머니를 " 얼어 '빨간 책' 공인을 '확인했을 '때' 동시에 밥이 '주머니 문 열어본다면 과단적 공을 확인함 수 있다. 고건역학

어있다고"한"구"있다."하지만"양자역학의"관점에서는" 텔리스가 "빨간 약"공을 "확인 "한"순간 "밥의 주머니에는"

실험적으로"양자"엄험을"확인하는"방법은"다음파" 같다."비선형"장학"결정에"레이저를"조사하여"장자를" 무 할래로 본리한 수 있는데, 이 박 한국 장자와 역장을 고전역학의 "관점에 서는 "중인은 "경험"가능한 "정역" - 축정해서 "수정 경장이 '관측된 다면 "그는 간'다른 한국의" 장치는 즉시 '구리편장이'된다 '반대로'한국 장치의 즉 정으로 수지경장이 관측된다면 다른 한국의 장가는 즉 시"구정점장이"된다(이." 리



Rg 1 The example of Quantum Enlargement ...

2.13 양자봉화 J

양차역학에서는 '모든' 상태가 '확률에' 기반하기에'양 자는 '축정하기 '전까지' 확문적으로 '공험된 '상대문' 가지 그 있다가 축정하는 '순간'하나의 상태가 관측된다 '이 처럼 중청상대의 양자는 각각의 상태가 확은적으로 근 계하고 있으나 권촉하는 순간 하나의 상태로 확성적으 로'근 계약계 '회여'다른 '상대로 '활'가능성은 '사라 된다.'' 니

특히 '양자' 붕괴는 '정보 에도' 영향을 '꺼치 며'측정으로' 한하여 정보가 등 파하게 '된다면' 기존 '상대로' 피를 닫다. 없기에 정보가 유실되는 효과를 볼 수 있다.이 ' 니

현실 세계에서도 그림 2의 같이 양자 등의 와비슷한 현상을 확인함 수 있다. 숙면에 구나위를 끌어 기부터 8 자기의 강 중 각각의 눈을 범득한 확률은 모두 18의 확 물을 가진다."이때"구사위를 굴려서"3가"나는 것을 확 인했다면"그"윤강"3가"나를"확률은"1이"되며"다른"눈이" 나는 학문은 모두 10으로 '붕괴한다[6].' 니

이러한 양자 봉화 특성을 환흥하면 양자 동산에서 보안성을 "확보하는데"사용함"수"있다" 동산 중간에 "제"

Thank You