# 양자정보통신 국내외 연구·기술개발 동향과 관련업체 현황
# (양자컴퓨팅·양자암호통신)

[목 차]

3) Quantum의 활용 가능성

(1) 양자 기술이 적용된 제품 진화 방향

(2) 소재/부품의 성능 고도화 가능성

2.1) 양자점(Quantum Dot)

2.1.1) 정의 및 구조

2.1.2) 발광 원리

2.1.3) Quantum Dot Display

2.1.4) Quantum Dot Display의 4가지 Type

a) QDCF-LCD(Quantum Dot Color Filter LCD)

b) QDEF-LCD(Quantum Dot Enhancement Film LCD)

c) QD-LED(Quantum Dot Light Emitting Diode)

d) QD-OLED(Quantum Dot OLED)

2.1.5) 활용 가능성

(3) 양자정보의 출현

3.1) 고전정보에서 양자정보로 전환

3.1.1) 고전정보소자 극소화

3.1.2) 고전정보소자 극소화의 한계

3.1.3) 고전정보에서 양자정보로 전환

3.2) ICT측면에서의 양자정보 해석

3.2.1) 양자정보의 ICT측면에서 해석 및 상호관계

3.2.2) 양자중첩상태 해석: 메모리 압축 효과

3.2.3) 양자간섭현상 해석: 효율적 병렬계산

3.2.4) 양자얽힘상태 해석: 원거리 상관성

3.2.5) 관측붕괴현상 해석: 일회성 읽기 과정

2) 양자암호통신

(1) 개요

1.1) 개념

1.2) 구성

(2) 기존 암호통신 방식과의 비교

(3) 도입의 필요성

3) 양자컴퓨팅

(1) 3가지 주요 개념

1.1) 중첩

1.2) 얽힘

1.3) No Cloning Theorem

(2) 배경

2.1) 고전컴퓨팅 vs 양자컴퓨팅

2.1.1) 고전컴퓨팅과의 차이점

4.3) 입력크기 기준

(5) 시스템 구조

5.1) 기본 조건

5.2) 방법론

5.2.1) 오류보정방식

5.2.2) 결함허용방식

5.2.3) 일반적인 결함허용 만능컴퓨팅 구현 방식

5.3) 시스템 구조

5.4) 부분별 연구개발 현재 수준

4) 양자 알고리즘

(1) Shor 알고리즘

(2) Grover 알고리즘

## Ⅱ. 국내외 양자정보통신 기술개발 동향 및 연구현황

### 1. 국내외 양자정보통신 기술개발 동향

1) 양자컴퓨터 개발을 위한 국내외 동향

(3) SK telecom

3.1) SKT Quantum Tech. Lab

3.2) 초소형 양자난수생성(QRNG) 칩

3.3) 퀀텀 전송 시스템

(4) KIST 양자정보연구단

4.1) 개요

4.2) 연구 분야

4.3) 세부 연구 내용

4.3.1) 광자-원자 기반 하이브리드 양자컴퓨팅 원천기술

4.3.2) 양자암호통신 기술

a) 1x16 양자키분배 시스템 구현

b) 양자해킹 및 방지책 구현

c) 플러그앤플레이 MDI 양자암호키분배 구현

(5) KRISS 양자측정센터

5.1) 개요

5.2) 주요 연구 분야

5.2.1) 양자 전류

5.2.2) 양자 저항

5.2.3) 저온 고분해능 검출

5.2.4) 나노열물성

5.2.5) 나노역학계

5.2.6) 초전도큐비트

5.2.7) 광큐비트

5.3) 주요 MOU 현황

(6) 스마트 양자통신 연구센터

6.1) 개요

6.2) 목적 및 비전

6.3) 세부 연구 분야

6.3.1) 세부과제별 유기적 연계성

6.3.2) 지상 양자통신 기술개발

6.3.3) 위성 양자통신 기술개발

6.3.4) 양자정보 기술개발

6.3.5) 향상된 후처리 알고리즘 개발 및 구현

6.3.6) UX 디자인 기반의 개인 보안 SW 개발

6.3.7) SW 및 창업 교육

2) 북미

(1) 양자정보통신

1.1) DARPA Quantum Network

2.7) IARPA Quantum

2.7.1) Multi-Qubit Coherent Operation(MQCO)

2.7.2) Quantum Computer Science(QCS)

2.8) NIST Physical Measurement Laboratory(PML)

2.8.1) Quantum Information

a) Faint Photonics Group

2.8.2) Time and Frequency

2.9) Institute for Quantum Computing(IQC)

2.9.1) Quantum Device theory

2.9.2) QEYSSat(Quantum Encryption and Science Satellite)

2.10) Stewart Blusson Quantum Matter Institute(SBQMI)

3) 유럽

(1) European Commission(EC)

1.1) QIPC

1.1.1) Fourth Framework Programme(FP4, 1995-1998)

1.1.2) Fifth Framework Programme(FP5, 1999-2002)

1.1.3) Sixth Framework Programme(FP6, 2003-2006)

1.1.4) Seventh Framework Programme(FP7, 2007-2013)

1.1.5) QIPC 기타 프로젝트 및 연구 동향

1.2) SECOQC

(2) ETSI

2.1) 개요

2.2) QKD에 대한 표준화

(3) Quantum Manifesto

3.1) 배경

3.2) 세부

(4) UK National Quantum Technologies Programme(UKNQT)

4.1) Sensors and Metrology

4.2) Quantum Imaging Centre(QuantiC)

4.3) NQIT(Networked Quantum Information Technologies)

4.4) Quantum Communications Hub(QComm Hub)

(5) ID Quantique

5.1) 주요 비즈니스 분야

(6) Max Planck Institute of Quantum Optics(MPQ)

(7) Vienna Center for Quantum Science and Technology(VCQ)

(8) IQOQI

(9) Institute of Photonic Sciences(ICFO)

(10) QuTech Delft University of Technology

4) 일본

(1) NICT

1.1) Quantu ICT Advanced Development Center

1.2) UQCC

1.2.1) Tokyo QKD Network

a) Tokyo QKD Link 구성

b) 3-layer 아키텍처

(2) Itoh Research Group163

5) 중국

(1) QKD Network

(2) Quantum Experiments at Space Scale(QUESS)

(3) Quantum Random Number Generator(ORNG)

## Ⅲ. 양자암호통신 및 양자컴퓨팅 기술동향

### 1. 양자암호통신 기술동향

1) 기술 개요 및 세계 시장전망

(1) 양자암호통신 시스템 구현을 위한 요소 기술

1.1) 양자 응용 기술

1.2) 시스템 구현을 위한 요소 기술

(2) 기술 트렌드

2.1) Optical-fiber QKD

2.2) Free-space QKD

2.3) 양자 중계 기술

(3) 세계 시장전망 및 경제적 파급효과

3.1) 시장전망

3.2) 산업의 경제적 파급효과

(4) 세계 통신사 간 양자 기술개발 경쟁현황

2) 양자키 분배 프로토콜 및 무선 양자 통신

(1) 양자암호 기술 개요

1.1) 대칭키 암호 시스템 vs 공개키 암호시스템

1.1.1) Rivest Shamir Adelman(RSA)

1.2) 양자 암호 기술의 무조건 안전성

(2) 양자키 분배 프로토콜

2.1) 특징

2.2) 세부 내용

2.2.1) BB84

2.2.2) Ekert

2.2.3) BB92

2.2.4) DPS

2.2.5) SARG04

2.2.6) Decoy

5.1) 양자정보통신 중장기 추진전략

5.1.1) 개요

5.1.2) 추진 계획

5.1.3) 3대 목표

5.1.4) 주요 성과

5.2) 상용화를 위한 향후 연구 방향

5.2.1) 자유공간(무선) 양자암호통신 기술

5.2.2) 중장거리 양자암호통신 전송 기술

a) Trusted Node를 이용한 장거리 전송 방식

b) Quantum Teleportation을 이용한 광자 전용방식

5.3) 최근 관련 이슈

5.3.1) KIST-KT

5.3.2) 드림시큐리티

(2) 기술동향

2.1) 주요 활용 분야

2.2) 연도별 연구 동향

2.3) NIST의 Quantum Algorithm Zoo

2.4) qubit 현황

2.5) 양자컴퓨터 모델

(3) 경쟁 기업 현황 및 영향

3.1) 경쟁 기업 현황

3.2) 양자컴퓨팅의 영향력

2) 포스트양자 암호알고리즘(Post-Quantum Cryptography)

(1) 정의 및 분류

(2) Multivariate-based Cryptography

2.1) 기본 구조

2.2) 연구 동향

2.2.1) Mixed field

a) Hidden Field Equation(HFE)

b) ZHFE

2.2.2) Single Field

a) Unbalanced Oil and Vinegar(UOV)

b) Rainbow

(3) Code-based Cryptography

3.1) 개요

3.2) 분류

3.2.1) McElice 알고리즘

3.2.2) Modern McElice cryptosystem

a) LWE-Frodo

3) 기업·스타트업 및 기관별 연구 동향

(1) Google

1.1) Quantum

1.2) 기술개발 동향

1.2.1) D-Wave Two 활용 연구 동향

1.2.2) 양자 칩 개발 동향

1.2.3) 하이브리드 단열 양자컴퓨팅

1.3) 양자컴퓨터 상용화 계획 및 목적

1.3.1) 상용화 계획

1.3.2) 목적

a) 발견적 양자 알고리즘 구현

b) 양자컴퓨터를 위한 알고리즘 및 응용 프로그램 개발

1.4) IBM vs Google

(2) IBM

2.1) IBM Q

2.1.1) 개요

2.1.2) 로드맵

2.1.3) 외형 및 구조

2.2) Quantum Experience

2.3) Q System(50 qubit Quantum Computer)

2.3.1) 활용 분야

2.3.2) D-Wave vs IBM

(3) Microsoft

3.1) Station Q

(4) 도쿄(東京)대학

4.1) 양자텔레포테이션 관련 기술 개발

(5) 기타 국가 최근 연구 동향 및 이슈

5.1) 캐나다

5.1.1) 2큐비트 설계 발표

5.2) 북한

5.3) 278

5.3.1) 기초과학연구원(IBS)

5.3.2) KAIST

5.4) 양자컴퓨터 실용화에 따른 사이버 보안 업계 위협

# Ⅳ. 양자정보통신 관련업체 동향

## 1. SK텔레콤㈜

### 1) 기업 현황

#### (1) 사업 내용

#### (2) New ICT 전략

##### 2.1) 개요

##### 2.2) 전략 방향

###### 2.2.1) 핵심기술 및 인프라 강화

###### 2.2.2) New ICT 포트포리오 확장

###### 2.2.3) Digital Transformation 파트너

###### 2.2.4) New Biz/ Tech 진출

(3) 매출 현황

2) 양자암호통신 관련 협력 및 연구개발 동향

(1) 주요 협력 현황

(2) 연구개발 동향

2.1) 연구개발 동향

2.1.1) 초소형 양자난수 생성기(QRNG) 개발

2.1.2) 왕복 112Km 구간 양자 전용 중계장치 개발

2.1.3) 퀀텀 전송 체계 연내 개발 및 상용화

2.2) 기타 동향

2.2.1) New T디벨로퍼스

2.2.2) 양자암호통신 국가시험망 개소

2. ㈜우리로

1) 기업 개요 및 현황

(1) 기업 개요

(2) 매출 현황

2) 연구개발 동향

(1) R&D 분야 및 실적현황

1.1) R&D 분야 및 현황

1.2) 연도별 R&D 실적

1.2.1) 2015년

1.2.2) 2016년

1.2.3) 2017년 반기

(2) 주요 제품 포트폴리오

2.1) 수동형 광통신 부문

2.1.1) 수동형 광분배 소자(PLC Splitter Chip)

2.1.2) Rack-Mount type & others

2.1.3) 수동형 광분배기(PLC Splitter Module)

2.2) 능동형 광통신 부문

2.2.1) Photo-Diode Chip

a) 2.5Gbps APD(Avalanche Photo-Diode)

b) Monitor PD

c) Large Area PD

d) 200㎛ APD

e) SPAD(Single Photon Avalanche Diode)

2.2.2) Photo-Diode Module

a) PIN PD (High Sensitive, 2.5G)

b) 10Gbps PIN (Plastic, 10G)

(2) 주요 솔루션 현황

2.1) PKI 인증·암호

2.1.1) Magic PKI (CA/RA)

2.1.2) Magic IoT

2.1.3) Magic PKI Kit

2.1.4) Magic Crypto

2.2) PKI 응용보안

2.2.1) Magic Line V4.0

2.2.2) Magic SSO / EAM

2.2.3) Magic XML

2.2.4) Magic Medicare

2.3) 모바일 보안솔루션

(2) PTN(Packet Transport Network) 장치

(3) MSPP(Multi Service Provisioning Platform)

(4) AGW(Access Gateway System) 장치

(5) WDM(Wavelength Division Multiplexer) 장치

(6) EMS

3) 양자암호통신 관련 현황

# Ⅴ. 부 록

## 1. 영국의 양자 기술 로드맵

### 1) 양자기술 정책 추진현황

3.3) 사업화

3.3.1) 혁신 생태계 육성

3.3.2) 지식재산 보호

3.3.3) 연계 촉진

3.3.4) KTN 및 QT SIG 운영

3.4) 인력

3.5) 제도

3.5.1) 규제 및 표준 개발

3.5.2) RRI

3.6) 국제 협력

3.7) 전략

4) 시장전망