(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2020년11월02일
(11) 등록번호 10-2172688
(24) 등록일자 2020년10월27일

(51) 국제특허분류(Int. Cl.)
H04L 9/08 (2006.01) *G06N 99/00* (2019.01)
G08B 21/04 (2006.01) *G08C 23/04* (2006.01)
H04L 9/06 (2006.01) *H04L 9/32* (2006.01)
H04N 7/18 (2006.01) *B82Y 10/00* (2017.01)
(52) CPC특허분류
H04L 9/0852 (2013.01)
G06N 10/00 (2019.01)
(21) 출원번호 10-2018-0064279
(22) 출원일자 2018년06월04일
심사청구일자 2018년06월04일
(65) 공개번호 10-2019-0138116
(43) 공개일자 2019년12월12일
(56) 선행기술조사문헌
KR1020140126787 A
KR1020170107047 A
KR1020180037851 A

(73) 특허권자
차보영
대전광역시 유성구

(72) 발명자
채령
대전광역시 유성구

차보영
대전광역시 유성구

전체 청구항 수 : 총 1 항 심사관 : 문형섭

(54) 발명의 명칭 **양자난수 및 의사난수를 결합한 다차원 행렬 해시함수 블럭체인 스마트 블럭 배전반 제어시스템**

(57) 요 약

양자메인보드는 양자난수생성기로 부터 양자난수를 수신하여 대칭암호키를 생성하고, 의사난수생성기로부터 발생한 의사난수로 상기 대칭암호키를 암호화하여 비대칭암호키를 생성함에 있어서,

양자메인보드는 양자난수생성기로 부터 무작위 양자난수를 수신하여 3차원 행렬 함수($\sum KEY_s(x,y,z)$)인 대칭암

(뒷면에 계속)

대 표 도 - 도1

KEY_s : 대칭암호키
KEY_{as} : 비대칭암호키
P : PUF 하드웨어 추출 PIN 데이터
M : MAC Address
(x,y,z) : X,Y,Z 3차 행렬 값
MAX : 두 개의 입력변수 ($\frac{1}{M}\sum KEY_s(x,y,z)$, $\frac{1}{P}\sum KEY_s(x,y,z)$)를 비교하여 좌측의 입력변수가 우측의 입력변수 값보다 크면 1, 작으면 0으로 이진화하는 해시함수

$$KEY_{as} = MAX(\frac{1}{M}\sum KEY_s(x,y,z), \frac{1}{P}\sum KEY_s(x,y,z))$$

호키를 생성하고, 양자메인보드는 의사난수생성기를 통해 MAC Address 데이터(M)를 대칭암호키($\sum KEY_s(x,y,z)$)로 암호화한 데이터 값으로 해시함수($MAX(x,y,z)$)의 X 좌표 값을 생성하고, 양자메인보드는 의사난수생성기를 통해 PUF PIN 데이터(P)를 대칭암호키($\sum KEY_s(x,y,z)$)로 암호화한 데이터 값으로 해시함수($MAX(x,y,z)$)의 Y 좌표 값을 생성하고, 양자메인보드는 의사난수생성기를 통해 TIME 데이터(T)를 대칭암호키($\sum KEY_s(x,y,z)$)로 암호화한 데이터 값으로 해시함수($MAX(x,y,z)$)의 Z 좌표 값을 생성한다.

양자메인보드는 의사난수생성기를 통해 상기 해시함수의 X좌표 값 및 Y좌표 값을 비교하여 X좌표 값이 Y좌표 데이터 값보다 크면 1, 작으면 0으로 이진화하여 TIME 데이터를 포함하여 비대칭암호키를 생성하는 것을 특징으로 한다.

(52) CPC특허분류
G08B 21/0484 (2013.01)
G08C 23/04 (2013.01)
H04L 9/0631 (2013.01)
H04L 9/0643 (2013.01)
H04L 9/0863 (2013.01)
H04L 9/3278 (2013.01)
H04N 7/18 (2013.01)
B82Y 10/00 (2013.01)
H04L 2209/38 (2013.01)

명 세 서

청구범위

청구항 1

삭제

청구항 2

양자난수생성기(QRNG; Quantum Random Number Generator) 및 의사난수생성기(PRNG; Pseudo Random Number Generator)를 포함하는 양자메인보드(Q-MCU), OTP 메모리(OTP M/M)를 포함하여 구성된 스마트 그리드 서버;

제1 내지 제N 스마트 블럭 배전반 집합(N은 2 이상의 자연수)으로 구성되어,

양자난수생성기(QRNG)는 난수소스발생기, 양자검출 다이오드, 양자랜덤펄스 생성기, 양자난수 제어부로 구성되고,

난수소스발생기는 LED(Light-Emitting Diode), LD(Laser Diode), 방사선 동위원소, 노이즈펄스 중 어느 하나 이상으로부터 양자입자를 방출하는 난수소스발생기이며;

양자검출 다이오드는 상기 난수소스발생기로 부터 발생하는 양자입자를 검출하는 양자검출 다이오드이며;

양자랜덤펄스 생성기는 상기 양자검출 다이오드로부터 양자입자 이벤트를 검출하여 양자입자의 검출에 상응하는 랜덤펄스를 발생하는 양자랜덤펄스 생성기이며;

양자난수 제어부는 상기 양자랜덤펄스 생성기를 통해 발생하는 무작위 난수소스로 양자난수를 생성하는 마이크로프로세서로 구성된 양자난수 제어부이며;

양자메인보드(Q-MCU)는 난수발생 프로그램에 의해 의사난수를 생성하는 의사난수생성기(PRNG)를 포함하여 구성되어, 상기 양자난수 제어부로 부터 양자난수를 수신하여 대칭암호키를 생성하고, 양자메인보드(Q-MCU)는 상기 의사난수생성기(PRNG)로부터 발생한 의사난수로 상기 대칭암호키를 암호화하여 비대칭암호키를 생성함에 있어서,

양자메인보드(Q-MCU)는 양자난수생성기로 부터 무작위 양자난수를 수신하여 난수 시드(seed)로 대칭암호키를 생성하며;

양자메인보드(Q-MCU)는 의사난수생성기를 통해 스마트 블럭 배전반 MAC Address 데이터를 대칭암호키로 암호화한 데이터 값으로 해시함수의 X 좌표 값을 생성하며;및

양자메인보드(Q-MCU)는 의사난수생성기를 통해 스마트 블럭 배전반 내부의 PUF PIN 데이터를 대칭암호키로 암호화한 데이터 값으로 해시함수의 Y 좌표 값을 생성하며;및

양자메인보드(Q-MCU)는 의사난수생성기의 이진화 함수인 해시함수로 상기 X좌표 값 및 Y좌표 값을 비교하여 X좌표 값이 Y좌표 데이터 값보다 크면 1, 작으면 0으로 이진화하는 해시함수로 비대칭암호키를 생성하며;

양자메인보드(Q-MCU)는 상기 대칭암호키 및 비대칭암호키를 OTP 메모리(OTP M/M)에 저장 후 비대칭암호키를 스마트 블럭 배전반으로 전송하며;

스마트 블럭 배전반은 스마트 블럭 배전반 ID Address 및 데이터블럭 데이터를 비대칭암호키로 암호화하여 스마트 그리드 서버 내부의 양자메인보드(Q-MCU)로 전송하며;

양자메인보드(Q-MCU)는 상기 비대칭암호키로 암호화한 스마트 블럭 배전반 ID Address 및 데이터블럭 데이터를 수신하여 대칭암호키로 복호화한 후 현재 데이터블럭으로 OTP 메모리(OTP M/M)에 저장하며;및

양자메인보드(Q-MCU)는 이전 데이터블럭 및 현재 데이터블럭을 연속적으로 데이터블럭으로 체인화하고, 체인화된 블럭체인 데이터를 스마트 블럭 배전반 집합으로 전송하여 상호 인증하고, 상호 인증이 완료되면 스마트 그리드 서버는 대칭암호키 및 비대칭암호키를 삭제 후 양자난수생성기 및 의사난수생성기를 통해 대칭암호키와 비대칭암호키를 새로 생성하는 것을 특징으로 하는 양자난수 및 의사난수를 결합한 다차원 행렬 해시함수 블럭체

인 스마트 블럭 배전반 제어시스템.

청구항 3

삭제

청구항 4

삭제

청구항 5

삭제

청구항 6

삭제

청구항 7

삭제

청구항 8

삭제

청구항 9

삭제

청구항 10

삭제

청구항 11

삭제

청구항 12

삭제

청구항 13

삭제

청구항 14

삭제

청구항 15

삭제

청구항 16

삭제

청구항 17

삭제

청구항 18

삭제

청구항 19

삭제

청구항 20

삭제

청구항 21

삭제

청구항 22

삭제

청구항 23

삭제

청구항 24

삭제

청구항 25

삭제

청구항 26

삭제

청구항 27

삭제

청구항 28

삭제

청구항 29

◈청구항 29은(는) 설정등록료 납부시 포기되었습니다.◈

제 2 항에 있어서,

스마트 그리드 서버는 동보방송 서버, 구내방송 서버, CCTV 제어 서버, 고장감시 제어 서버, 원격검침 서버, 디밍제어 서버, 원격제어 서버, 주차관제 서버 중 어느 하나로 대체되며;

스마트 블럭 배전반은 TTS 동보 방송장치, 구내 영상음성 방송장치, 암호화 영상저장 CCTV 감시장치, NB-IoT 고장감시 블랙박스형 CCTV 감시장치, 블럭체인 미터링 태양광 발전장치, 디밍제어 LED 가로등, 태양광 발전판넬, LED 전광판, CCTV 열화상 감시카메라, 영상처리장치, 차량번호 암호화 주차관제장치, 조기화재 감시 CCTV 감시카메라 중 어느 하나로 대체되는 것을 특징으로 하는 양자난수 및 의사난수를 결합한 다차원 행렬 해시함수 블럭체인 스마트 블럭 배전반 제어시스템.

청구항 30

◈청구항 30은(는) 설정등록료 납부시 포기되었습니다.◈

제 2 항에 있어서,

양자메인보드는 양자난수생성기로 부터 양자난수를 수신하여 대칭암호키를 생성하고, 의사난수생성기로부터 발생한 의사난수로 상기 대칭암호키를 암호화하여 비대칭암호키를 생성함에 있어서,

양자메인보드는 양자난수생성기로 부터 무작위 양자난수를 수신하여 3차원 행렬 함수($\sum KEY_s(x,y,z)$)인 대칭암호키를 생성하며;

양자메인보드는 의사난수생성기를 통해 MAC Address 데이터(M)를 대칭암호키($\sum KEY_s(x,y,z)$)로 암호화한 데이터 값으로 해시함수($MAX(x,y,z)$)의 X 좌표 값을 생성하며;및

양자메인보드는 의사난수생성기를 통해 PUF PIN 데이터(P)를 대칭암호키($\sum KEY_s(x,y,z)$)로 암호화한 데이터 값으로 해시함수($MAX(x,y,z)$)의 Y 좌표 값을 생성하며;

양자메인보드는 의사난수생성기를 통해 TIME 데이터(T)를 대칭암호키($\sum KEY_s(x,y,z)$)로 암호화한 데이터 값으로 해시함수($MAX(x,y,z)$)의 Z 좌표 값을 생성하며;

양자메인보드는 의사난수생성기를 통해 상기 해시함수의 X좌표 값 및 Y좌표 값을 비교하여 X좌표 값이 Y좌표 데이터 값보다 크면 1, 작으면 0으로 이진화하여 TIME 데이터를 포함하여 비대칭암호키를 생성하는 것을 특징으로 하는 양자난수 및 의사난수를 결합한 다차원 행렬 해시함수 블럭체인 스마트 블럭 배전반 제어시스템.

발명의 설명

기 술 분 야

[0001] 물리적으로 유니크한 인증 수단의 PUF(Phisycally Unclonable Function) Chip과 양자컴퓨터로 부터의 해킹을 차단하는 양자보안 QRNG(Quantum Random Number Generator) Chip을 이용한 전자기적인 방법에 의한 물리적으로 유니크(unique)한 암호화 기술 및 블럭 체인(Block chain) 검증 수단을 적용한 배전반, 방송장치, CCTV 감시장치, 태양광 발전장치, 가로등, LED 전광판, 주차관제장치 관련이다.

[0003] 특정 물질 감지 기술은 산업계 전반에 걸쳐서 폭넓게 응용되고 있다. 그 중에서 염화수소(HCl) 가스는 다양한 분야에서 사용되며, 노출시 환경오염, 부식성 및 인체에 유독성분으로 대기오염 방지법에 의한 배출기준 및 노동법에 의한 노출기준이 정해져 있다. 또한, 염화수소(HCl) 가스는 유기 화합물 생산 공정에서 반드시 사용되는 물질로서 공정 산출물인 유기 화합물에 소량 포함되며 유기 화합물의 열적 안정성과 밀접한 관련을 가지고 있다. 또한, 일반적으로 전자제품의 전선 및 케이블의 피복에는 폴리에틸렌이나 중간재(역청재)로 이루어져 있다. 이러한 케이블의 외장재는 연소되면서, 염화수소가스(HCl), 일산화가스(CO), 이산화탄소(CO_2) 등의 유독가스가 배출된다.

배 경 기 술

[0005] 안전한 통신을 위해 양자 역학적 특성을 이용한 양자 암호(quantum cryptography) 및 양자 암호 키 분배(QKD: Quantum Key Distribution) 기술로 물리적 입자의 전달이 아닌 큐비트(qubit)를 전송(quantum teleportation)하는 기술로 양자 상태(quantum states)에 정보를 기록해 전송하여 공격자가 도청을 위해 양자 상태를 측정하는 순간 양자 상태 자체가 변화되어 도청이 불가능한 기술관련이다.

[0006] 따라서 수신자는 데이터에 대한 도청 시도를 파악하고 수신된 정보를 폐기할 수 있고, 이에 따라 양자 상태에 기록된 정보는 근본적으로 도청이 불가능하다.

[0007] 하드웨어 보안을 위해 식별키를 생성하는 장치 및 방법에 있어서, 반도체 제조중 공정 편차를 이용하여 PUF(Physically Unclonable Function)를 구현하여 식별키를 생성하는 장치 및 방법을 적용하여 물리적 개체인증을 수행하는 기술을 적용하여 보안성을 강화한다.

[0008] 일반적으로 IP카메라도 소프트웨어적 보안이 가능하지만 소프트웨어적 방법은 하드웨어가 이미 형성된 이후에 부가하는 것이므로 변조될 가능성이 상존하였다.

[0009] 그래서, 데이터 보안의 근본적인 해결을 위해서는 데이터를 처리할 하드웨어의 설계 시작시부터 데이터 보안을

고려한 설계가 되어야 한다.

[0010] 본 발명은 하드웨어로 구현된 물리적 보안으로 메모리 부담이 없고 처리속도가 빠르다.

[0011] IC(Integrated Circuit) 칩의 생산 공정에서 발생하는 하드웨어 핀(PIN) 편차를 이용한 상기 PUF를 통해 PIN(Personal Identification Number)값을 생성한 후 공인인증 플랫폼에서 보관 후 단말기에 설치된 PUF의 PIN 값을 포함하는 인증요청 키가 공인인증 플랫폼에서 수신하여 PIN 값이 일치할 경우 인증절차를 수행한다.

[0012] 상기 PUF가 물리적인 단말기를 하드웨어적으로 인증한다면, 상기 PUF의 PIN 값을 1회성 양자난수 OTP(One Time Password)를 생성한 인증요청 키(암호키/복호키)를 생성하는 것은 양자난수생성기를 통해서 생성하는 것을 특징으로 한다.

[0013] 순수난수생성기는 난수소스발생기, 의사난수생성기를 포함하여 구성되어, 난수소스발생기는 예측 불가한 자연현상을 이용하여 발생한 무작위 난수소스로 암호키를 생성한다.

[0014] 상기 예측불가 자연현상으로는 자연광, LED(Light Emitting Diode), LD(Laser Diode), 방사선, 열잡음, 노이즈 등을 이용해 양자난수(Quantum Random Number, QRN)를 발생한다.

[0015] 상기 암호키를 한 쌍의 암호키로 상호 암호통신을 위한 대칭암호키를 생성한다.

[0016] 상기와 같은 양자난수와 달리 의사난수생성기(pseudorandom number generator, PRNG)를 통해 OTP(One Time Password) 비대칭암호키를 암호화 생성한다.

[0017] 본 발명의 순수난수생성기(True Random Number Generator, TRNG)는 양자난수(Quantum Random Number, QRN) 대칭암호키와 의사난수(pseudorandom number, PRN) 비대칭암호키를 생성하는 것으로, 한 쌍의 대칭암호키를 통해 양방향 통신 및 인증이 가능하다.

[0018] 상기 양자난수 대칭암호키에 의사난수생성기를 통해 다시 암호화한 비대칭암호키를 생성하는 것으로, 대칭암호키를 통해 비대칭암호키를 복호화할 수 있는 것을 특징으로 한다.

[0019] 생활 속 사물들을 유무선 네트워크로 연결해 정보를 공유하는 시스템인 사물인터넷(Internet of Thing)이 보편화 되고 있다.

[0020] 사물인터넷이란, 인간과 사물, 서비스 세 가지 분산된 환경 요소에 대해 인간의 명시적 개입 없이 상호 협력적으로 센싱, 네트워킹, 정보 처리 등 지능적 관계를 형성하는 사물 공간 연결망이다.

[0021] 사물인터넷의 보편화에 따라 보안위협도 높아지고 있으며, 사물인터넷 보안을 위해서는 사물인터넷 기기에서부터 시스템까지 전 구간에 대한 단절 없는 보안이 필요하다.

[0022] 특히 다양한 기능과 프로토콜을 가진 기기들과 통신해야 하기 때문에 개방형 표준기술을 사용해야 하므로 보안위협에 훨씬 노출되고 있다.

[0023] 한편, 소프트웨어 기반의 난수 생성 기술은 리소스를 많이 사용할 뿐 아니라 고도화된 해킹 기술을 이용하면 난수 발생 패턴을 파악할 수 있는 문제점이 있다.

[0024] 따라서, 사물인터넷 기기간의 보안을 위해 자연현상의 무작위성에서 난수를 추출하는 자연 난수 또는 진정 난수가 요청되고 있으며, 이는 특정한 패턴이 없고 예측이 불가능한 장점이 있지만, 크기가 크고 매우 비싸며 추출장치가 필요해 소형화 장치에 적용하기 어려운 문제가 있다.

[0025] 인터넷 보안 프로토콜(IP Security Protocol : IPSec)은 네트워크 통신의 패킷 처리 계층에서의 보안을 위해 개발된 프로토콜로서, 가상 사설망(Virtual Private Network : VPN)을 통하여 송수신되는 데이터를 공중망 사용자들로부터 보호하기 위하여 이용되는 프로토콜이다.

[0026] 로컬 기반의 IPSec VPN 서비스는, 다양한 통신 로컬들이 별도의 VPN 설정 없이, 공중망에 연결된 VPN 로컬에 접속하여 원격지의 사설망에 접속해 VPN 트래픽을 주고 받을 수 있는 가상 사설망 서비스이다.

[0027] 상술한 바와 같은 가상 사설망 서비스를 이용하기 위해 VPN 로컬은, 공중망을 통해 가상사설망게이트웨이(VPN GateWay : VPN G/W)와 IPSec 터널 생성을 위한 인증 단계를 수행하며, IPSec에서는 상기 인증을 위한 키 교환 절차로 IKE 방식을 1단계(Main Mode or Aggressive Mode)와 2단계(Quick Mode)로 나누어 진행한다.

[0028] 상기 IKE의 1단계는 보안성이 없는 공중망에서 암호화된 데이터를 주고받기 위한 ISAKMP(Internet Security Association and Key Management Protocol) 단계로서, VPN 로컬과 가상 사설망 게이트웨이(VPN G/W)가 서로

사전에 공유하여 가지고 있는 사전 공유키(Pre-Shared Key)와, ISAKMP의 암호화 방법 및 해시 함수 등에 대해 서로 협상하는 단계이다.

[0029] 그리고, 2단계는 실제 IPSec 터널(Tunnel)을 통해 주고 받을 데이터의 암호화 방법 및 IPSec 터널을 통해 주고 받을 트래픽의 유형 등을 협상하는 단계이다.

[0030] 이러한 로컬 기반의 IPsec VPN 서비스는 유선 기반과 무선 기반으로 나눌 수 있다.

[0031] 유선 기반은 상술한 VPN 로컬이 유선 네트워크를 통해 가상 사설망 게이트(VPN G/W)에 접속하는 것이고, 무선 기반은 상술한 VPN 로컬이 무선 네트워크를 통해 가상 사설망 게이트웨이(VPN G/W)에 접속하는 것이다.

[0032] 유선 기반의 VPN 서비스에서, VPN 로컬과 가상 사설망 게이트웨이(VPN G/W) 사이에서 IKE 1단계 인증을 위해, VPN 로컬에 고정 IP 주소를 할당하고, VPN 로컬과 가상 사설망 게이트웨이(VPN G/W)에 미리 설정된 사전 공유키(Pre-Shared Key)를 저장한 후, 가상 사설망 게이트웨이(VPN G/W)에서 해당 사전 공유키를 가지고 있는 VPN 로컬의 IP 주소가 상기 고정으로 할당된 IP 주소인지 여부를 확인하는 방식으로 인증을 수행한다.

[0033] 이 경우, 가입자의 VPN 로컬 하위에 위치하는 실제 사용자 로컬은 별도의 인증 절차 없이 VPN 로컬을 통해 원격지의 사설망에 접속할 수 있다.

[0034] 인터넷을 비롯한 유무선 통신의 사용이 급속히 확대됨에 따라 통신네트워크의 보안문제는 국가, 기업, 금융상의 중요기밀 보호 및 개인의 사생활 보호 측면에서 그 중요성이 점점 더 증대되고 있다.

[0035] 1970년대에 개발되어 현재 인터넷 등 통신시스템에 널리 사용되고 있는 비대칭 공개키 암호체계는 해결하기 매우 어려운 수학적인 문제를 공개키로 사용하여 정보를 암호화하고 그 해를 비밀키로 사용하여 해독하는 방식으로서 원리적으로 수학적인 “계산 복잡성”에 기초하고 있다.

[0036] 대표적으로 Rivest, Shamir, Adleman 등 세 사람이 개발한 RSA 공개키 암호체계는 매우 큰 수를 소인수분해하기가 매우 난해하다는 점을 이용한다.

[0037] 즉, 수학적으로 소인수분해 문제는 문제의 크기가 증가함에 따라 계산시간이 지수함수적으로 증가하게 되며 따라서 송신자와 수신자가 충분히 큰 숫자의 소인수분해 문제를 공개키로 사용하면 도청자가 암호문을 해독하기는 현실적으로 불가능 할 것이라는 점을 이용한다.

[0038] 그러나, 이러한 수학적인 계산복잡성에 기초한 암호체계는 보다 정교한 알고리즘의 발전에 따라 그 안전성에 의문이 제기되고 있으며, 또한 1994년 AT&T의 Peter Shor가 양자컴퓨터를 이용한 소인수분해 알고리즘을 개발함으로써 양자컴퓨터가 개발되면 RSA 암호체계는 근본적으로 해독이 가능한 것으로 판명되고 있다.

[0039] 이러한 보안문제를 해결할 대안으로 등장한 양자암호통신(quantum cryptography) 기술은 그 안전성이 수학적인 계산 복잡성이 아닌 자연의 근본 법칙인 양자역학의 원리에 기초하므로 도청 및 감청이 매우 어려워, 최근 크게 주목 받고 있다.

[0040] 즉, 양자암호통신 기술은 “양자 복제불가능성”과 같은 양자물리학의 법칙에 기초해서 송신자와 수신자 사이에 암호 키(일회용 난수표)를 절대적으로 안전하게 실시간으로 분배하는 기술로서 "양자 키 분배 기술(QKD)"로도 알려져 있다.

[0041] 최초의 양자 암호 프로토콜은 1984년 IBM의 C.H. Bennett과 몬트리올 대학의 G. Brassard에 의해 발표되었다.

[0042] 고안자들의 이름을 따서 BB84 프로토콜로 명명된 이 프로토콜은 두 개의 기저(basis)를 이루는 네 개의 양자 상태(예를 들면, 단일광자의 편광상태)를 이용한다.

[0043] 그러나 위의 선행기술에 따르면 양자암호를 송수신하기 위해서는 통신용 영상로컬기와 서버간의 송수신 장치가 필요하며, 통신용 영상로컬기와 서버간의 송수신 장치에 대한 비용 부담이 커지는 한계가 있다.

[0045] 블럭 체인(Block chain)은 공공 거래 장부라고도 부르며 가상 화폐로 거래할 때 발생할 수 있는 해킹을 막는 기술이다 기존 금융 회사의 경우 중앙 집중형 서버에 거래 기록을 보관하는 반면, 블럭체인은 거래에 참여하는 모든 사용자에게 거래 내역을 보내 주며 거래 때마다 이를 대조해 데이터 위조를 막는 방식을 사용한다 블럭체인은 대표적인 온라인 가상 화폐인 비트코인에 적용되어 있다 비트코인은 누구나 열람할 수 있는 장부에 거래내역을 투명하게 기록하며, 비트코인을 사용하는 여러 컴퓨터가 10분에 한 번씩 이 기록을 검증하여 해킹을 막는다.

[0047] LPWAN(Low Power Wide Area Network) 분야에서 NB-IoT와 경쟁하는 로라(LoRA) LPWAN은 10마일(16093Km) 이상의 범위(교외)에서 10년 이상 지속되는 배터리 수명으로 사물 인터넷(IoT)과 M2M(Machine-to-Machine) 무선통신을

구현하고 수백만 개의 무선 센서 노드를 게이트웨이에 연결할 수 있다 민영 LAN, 통신 사업자가 운영하는 공중망을 모두 포함해 기존 인프라와 함께 로라 얼라이언스 인프라와 간편하게 연결할 수 있으며 LPWAN(Low Power Wide Area Network)을 전국적인 규모로 구성할 수 있는 기술이다 LoRA기술은 3G 및 4G 셀룰러 네트워크에 비해 임베디드 애플리케이션이 더 높은 확장 가능성과 비용 효율성을 가질 수 있도록 하고, 보다 넓은 커버 범위와 낮은 전력 소비량 간에 하나만을 선택해야 했던 오랜 딜레마를 해결하는 방법으로 설명되고 있다 LoRA기술을 사용함으로써 두 가지 모두를 극대화하면서 추가적인 리피터 비용을 줄일 수 있으며, 열악한 실외 환경에서도 안정적으로 작동할 수 있으며 광범위한 저속 무선 모니터링 및 제어 설계에 매우 적합하다고 설명되고 있다.

[0048] LTE(Long Term Evolution)는 휴대전화 네트워크의 용량과 속도를 높이기 위해 고안된 무선기술로, LTE-A, 광대역 LTE, LTE-R(Railway), 협대역 LTE, LTE-B(Beyond), LTE-H(Heterogeneous), LTE-U(Unlicensed)로 구분된다.

[0049] 특히, 협대역 LTE는 LTE-MTC(MarrowBand-LTE-Machine)와 더 좁은 NB-LTE-M(NarrowBand-LTE-Machine)로 좁은 대역을 쓰기 때문에 속도는 느리지만 전력 소비량이 적어 LG유플러스와 KT는 NB-LTE-M(NB-IoT)을 상용화 하고 있다.

[0050] MAC Address(media access control address)란, 근거리통신망에서 MAC 주소는 데이터 링크 계층의 MAC 계층에 의해 사용되는 주소로서 네트웍 카드의 48비트 하드웨어 주소를 말하며, 이더넷 주소, 또는 토큰링 주소와 동일하다.

[0051] 네트워크카드 제조사에 의해 부여된 하드웨어 주소는 UAA(universally administered address)로서 모든 네트워크카드가 유일한 값을 가지게 되나 UAA는 관리 목적상 변경이 가능한데, 이러한 MAC 주소를 LAA(locally administered address)라 한다.

[0052] 전기화재 발생전 전선, 버스바 등의 통전 물질을 감싸고 있는 절연피복에서 열에 의해 발생하는 HCl, BHT 가스를 검지하여 화재 발생 전 조기경보가 가능하다.

발명의 내용

해결하려는 과제

[0054] 초소형의 PUF(Phisycally Unclonable Function) Chip과 QRNG(Quantum Random Number Generator) Chip을 이용한 전자기적인 방법에 의한 물리적으로 유니크(unique)한 암호화 기술을 적용한 배전반, 방송장치, CCTV 감시장치, 태양광 발전장치, 가로등, LED 전광판, 주차관제장치를 해결하고자 하는 과제로 한다.

[0055] 화재사고로 발생하는 염화수소가스(HCl)를 감지하고 화재발생 시 전기절연물 등에서 발생하는 염화수소가스(HCl)를 감지하여 전기화재의 발생을 감지하여 가스와 화재의 확산을 방지할 수 있는 HCl 감지 센서가 아닌 적외선 방사 전자기파가 염화수소가스(HCl)를 통과할 때 흡수되는 파장을 검출하는 CCTV 감시카메라를 통해 염화수소가스(HCl) 발생 영상을 제공하는 차별성을 갖는다.

[0056] 즉, 조기화재 발생 이벤트를 발생함에 있어, HCl, BHT 가스 등을 검출하는 센서에 의한 방식이 아닌 적외선 CCTV 감시카메라로 검출하여 시각화한 영상으로 제공하는 차별성을 갖는다.

과제의 해결 수단

[0058] 복제·해킹 불가능한 하드웨어 보안을 위해 식별키를 생성하는 장치 및 방법에 있어서, 반도체 제조중 공정 편차를 이용한 PUF(Physically Unclonable Function)를 구현하여 암호키를 생성한다.

[0059] 제품정보 데이터를 양자난수생성기 QRNG(Quantum Random Number Generator)를 통해 발생한 양자난수로 암호화한 유니크(Unique) 암호화 대칭키를 생성한다.

[0060] 이진화 해시함수에 따라 의사난수생성기 PRNG(Pseudo Random Number Generator)를 통해 1회성 OTP(One Time Password) 비대칭키를 생성한다.

[0061] 특히, 양자난수생성기를 통해 발생한 무작위 양자난수 기반에 MAC Address 데이터, PUF PIN 데이터, 다차원 행렬을 통해 해시함수의 이진화 암호코드를 생성하는 의사난수생성 과정을 주요한 특징으로 한다.

[0062] 각각의 가스는 고유의 흡수 파장대를 보유함에 따라 흡수 파장대를 분석하면 가스의 종류를 파악할 수 있다.

발명의 효과

[0064] 무작위 양자난수를 이용한 원천 보안안키와 물리적으로 유니크한 인증을 수행하는 PUF Chip을 기반으로 하는 다차원 행렬 해시함수를 통한 이진화 과정을 거쳐 비대칭암호키를 생성하여 보안성을 극대화한 상용 서비스를 제공한다.

[0065] CCTV 감시카메라를 통해 HCl, BHT 가스가 발생하는 영상을 제공하여 화재발생 전 조기화재 경보 및 가스 누출을 시각화 영상으로 제공한다.

도면의 간단한 설명

[0067] 도 1은 비대칭암호키 수식 설명도

도 2 ~ 12은 절연물의 열분해 가스크로마토그라피

발명을 실시하기 위한 구체적인 내용

[0068] 본 발명은 다음과 같은 기술을 주요 특징으로 구현된다.

[0069] 1. QRNG를 기반으로 하는 무작위 양자난수 대칭암호키

[0070] 2. PUF Chip에서 PUF PIN 데이터를 추출한 물리적 유니크키

[0071] 3. 기기별 고유의 MAC ADDERS 데이터를 기반으로하는 공개 정보 데이터

[0072] 4. 다차원 행렬 함수를 기반으로 생성하는 데이터블럭 공개암호키 및 비공개암호키

[0073] 5. 해시함수 의사난수생성기를 통해 암호화하는 비대칭암호키

[0074] 6. 비대칭암호키로 연속적인 데이터블럭를 체인화하여 OTP 방식으로 검증하는 블럭체인

[0075] 7. 가스를 검출하는 특수 CCTV 감시카메라를 통해 HCl, BHT 가스가 발생되는 합성영상을 제공한다.

[0077] 일 실시 예를 통해 이하 상세히 설명한다.

[0078] 서버는 순수(자연)난수생성기및 의사(프로그램)난수생성기를 포함하는 양자메인보드, OTP 메모리를 포함하는 서버 및 하나 이상의 단말장치로 구성된다.

[0080] 순수(자연)난수생성기는 난수소스발생기, 양자검출 다이오드, 양자랜덤펄스 생성기, 양자난수 제어부로 구성된다.

[0081] 난수소스발생기는 LED(Light-Emitting Diode), LD(Laser Diode), 방사선 동위원소, 노이즈펄스 중 어느 하나 이상으로부터 난수소스인 양자입자를 방출하는 난수소스발생기이다.

[0082] 양자검출 다이오드는 상기 난수소스발생기로 부터 발생하는 양자입자(난수소스)를 검출하는 양자검출 다이오드이다.

[0083] 양자랜덤펄스 생성기는 상기 양자검출 다이오드로부터 양자입자 검출에 따른 이벤트를 검출하여 양자입자의 검출에 상응하는 펄스(랜덤펄스)를 발생하는 양자랜덤펄스 생성기이다.

[0084] 양자난수 제어부는 상기 양자랜덤펄스 생성기를 통해 발생하는 무작위 난수소스로 양자난수를 생성하는 마이크로프로세서로 구성된 양자난수 제어부이다.

[0086] 양자메인보드는 난수발생 프로그램에 의해 의사난수를 생성하는 의사(프로그램)난수생성기를 포함하여 구성되어, 상기 양자난수 제어부로 부터 양자난수를 수신하여 대칭암호키를 생성한다.

[0087] 또한, 양자메인보드는 상기 의사(프로그램)난수생성기로부터 발생한 의사난수로 상기 대칭암호키를 암호화하여 아래와 같은 비대칭암호키를 생성한다.

[0088] $$KEY_{as} = MAX(\frac{1}{M}\sum KEY_s(x,y), \frac{1}{P}\sum KEY_s(x,y)) = MAX(x,y)$$

[0089] $$KEY_{as} = MAX(\frac{1}{M}\sum KEY_s(x,y,z), \frac{1}{P}\sum KEY_s(x,y,z))$$

[0091] 양자메인보드는 상기 대칭암호키 및 비대칭암호키를 OTP 메모리에 저장 후 비대칭암호키를 단말장치로 전송한다.

[0092] 단말장치은 단말장치 내부의 ID Address 및 데이터블럭 데이터(ID, 블럭체인 데이블럭 등)를 비대칭암호키로 암호화하여 서버 내부의 양자메인보드로 전송한다.

[0093] 양자메인보드는 상기 비대칭암호키로 암호화한 데이터블럭 데이터를 수신하여 대칭암호키로 복호화한 후 현재 데이터블럭으로 OTP 메모리에 저장한다.

[0094] 양자메인보드는 이전 데이터블럭 및 현재 데이터블럭을 연속적으로 데이터블럭으로 체인화하고, 체인화된 블럭체인 데이터를 단말장치 집합(제1 내지 제 N 단말장치) 또는 서버와 단말장치 사이에 상호 인증한다.

[0095] 블럭체인 데이터의 상호 인증(합의)이 완료되면 서버는 대칭암호키 및 비대칭암호키를 삭제 후 순수(자연)난수생성기 및 의사(프로그램)난수생성기를 통해 대칭암호키와 비대칭암호키를 새로 생성하여 블럭체인 주기에 따라 상호 재인증하는 것을 특징으로 한다.

[0097] 일 예로, 상기 서버는 스마트 그리드 서버, 동보방송 서버, 구내방송 서버, CCTV 제어 서버, 고장감시 제어 서버, 원격검침 서버, 디밍제어 서버, 원격제어 서버이다.

[0098] 일 예로, 상기 단말장치는 스마트 블럭 배전반, TTS 동보 방송장치, 구내 영상음성 방송장치, 암호화 영상저장 CCTV 감시장치, NB-IoT 고장감시 블랙박스형 CCTV 감시장치, 블럭체인 미터링 태양광 발전장치, 디밍제어 LED 가로등, 태양광 발전판넬, LED 전광판, CCTV 열화상 감시카메라, 영상처리장치, 차량번호 암호화 주차관제장치, 조기화재 감시 CCTV 감시카메라이다.

[0100] 일 실시 예로,

[0101] 양자난수생성기 및 의사난수생성기를 포함하는 양자메인보드, OTP 메모리를 포함하여 구성된 서버 및 하나 이상의 단말장치으로 구성된다.

[0103] 양자메인보드는 양자난수생성기로 부터 양자난수를 수신하여 대칭암호키를 생성하고, 의사난수생성기로부터 발생한 의사난수로 상기 대칭암호키를 암호화하여 비대칭암호키를 생성함에 있어서, 양자메인보드는 양자난수생성기로 부터 무작위 양자난수를 수신하여 3차원 행렬 함수인 대칭암호키를 생성한다.

[0104] 양자메인보드는 의사난수생성기를 통해 단말장치 MAC Address 데이터를 대칭암호키로 암호화한 데이터 값으로 해시함수의 X 좌표 값을 생성한다.

[0105] 단말장치는 PUF Chip을 포함하여 구성되어, 양자메인보드는 의사난수생성기를 통해 상기 PUF Chip에서 PUF PIN 데이터를 추출한 후 추출된 PUF PIN 데이터를 대칭암호키로 암호화한 데이터 값으로 해시함수의 Y 좌표 값을 생성한다.

[0106] 양자메인보드는 의사난수생성기를 통해 TIME 데이터를 대칭암호키로 암호화한 데이터 값으로 해시함수의 Z 좌표 값을 생성한다.

[0107] Z 값은 블럭체인 인증 주기 및 이전 데이터블럭, 현재 데이터블럭 등을 구별하는 데이터로 사용한다.

[0108] 양자메인보드는 의사난수생성기를 통해 상기 해시함수의 X좌표 값 및 Y좌표 값을 비교하여 X좌표 값이 Y좌표 데이터 값보다 크면 1, 작으면 0으로 이진화하여 TIME 데이터(Z 좌표 값)을 포함하여 비대칭암호키를 생성한다.

[0110] 양자메인보드는 상기 대칭암호키 및 비대칭암호키를 OTP 메모리에 저장 후 비대칭암호키를 단말장치으로 전송한다.

[0111] 단말장치은 단말장치 내부의 ID Address 및 데이터블럭 데이터를 비대칭암호키로 암호화하여 서버 내부의 양자메인보드로 전송한다.

[0112] 양자메인보드는 상기 ID Address 및 데이터블럭 데이터를 수신하여 현재 데이터블럭으로 OTP 메모리에 저장한다.

[0113] 양자메인보드는 이전 데이터블럭 및 현재 데이터블럭을 연속적으로 데이터블럭으로 체인화하고, 체인화된 블럭체인 데이터를 단말장치에 전송하여 상호 인증하는 것을 특징으로 한다.

[0115] 일 실시 예로,

[0116] 적외선센서 어레이부와 영상센서 어레이부로 구성된 촬상부 및 적외선을 방사하는 적외선 투광기 및 마이크로프로세서를 포함하는 주제어부로 구성된다.

[0117] 주제어부는 적외선 투광기부터 방사된 방사적외선이 반사되어 촬상부 내부 감지부의 적외선센서 어레이부를 통해 수신되는 수신적외선 주파수를 비교하여 가스에 의해 흡수된 흡수주파수를 추출하여 가스 종류별로 모니터에 색깔로 표출하기 위한 이미지 데이터를 생성한다.

[0118] 주제어부는 촬상부 내부 영상센서 어레이부로부터 수신되는 영상데이터에 상기 이미지 데이터를 합성한 합성데이터를 생성하여 모니터에 표출한다.

[0120] 스마트 그리드 서버는 양자난수생성기(QRNG; Quantum Random Number Generator) 및 의사난수생성기(PRNG; Pseudo Random Number Generator)를 포함하는 양자메인보드(Q-MCU), OTP 메모리(OTP M/M)를 포함하여 구성된다.

[0121] 제1 내지 제N 스마트 블럭 배전반 집합(N은 2 이상의 자연수)으로 구성된다.(일 예로, 제1 스마트 블럭 배전반, 제2 스마트 블럭 배전반, 제3 스마트 블럭 배전반, 제5 스마트 블럭 배전반, 제5 스마트 블럭 배전반 집합)

[0123] 양자난수생성기(QRNG)는 난수소스발생기, 양자검출 다이오드, 양자랜덤펄스 생성기, 양자난수 제어부로 구성된다.

[0124] 난수소스발생기는 LED(Light-Emitting Diode), LD(Laser Diode), 방사선 동위원소, 노이즈펄스 중 어느 하나 이상으로부터 난수소스인 양자입자를 방출하는 난수소스발생기이다.

[0125] 양자검출 다이오드는 상기 난수소스발생기로 부터 발생하는 양자입자(난수소스)를 검출하는 양자검출 다이오드이다.

[0126] 양자랜덤펄스 생성기는 상기 양자검출 다이오드로부터 양자입자 검출에 따른 이벤트를 검출하여 양자입자의 검출에 상응하는 펄스(랜덤펄스)를 발생하는 양자랜덤펄스 생성기이다.

[0127] 양자난수 제어부는 상기 양자랜덤펄스 생성기를 통해 발생하는 무작위 난수소스로 양자난수를 생성하는 마이크로프로세서로 구성된 양자난수 제어부이다.

[0129] 양자메인보드(Q-MCU)는 난수발생 프로그램에 의해 의사난수를 생성하는 의사난수생성기(PRNG)를 포함하여 구성되어, 상기 양자난수 제어부로 부터 양자난수를 수신하여 대칭암호키를 생성한다.

[0130] 또한, 양자메인보드(Q-MCU)는 상기 의사난수생성기(PRNG)로부터 발생한 의사난수로 상기 대칭암호키를 암호화하여 아래와 같은 비대칭암호키를 생성한다.

[0131] $$KEY_{as} = MAX(\frac{1}{M}\sum KEY_s(x,y,z), \frac{1}{P}\sum KEY_s(x,y,z))$$

[0133] 양자메인보드(Q-MCU)는 상기 대칭암호키 및 비대칭암호키를 OTP 메모리(OTP M/M)에 저장 후 비대칭암호키를 스마트 블럭 배전반으로 전송한다.

[0134] 스마트 블럭 배전반은 스마트 블럭 배전반 ID Address 및 데이터블럭 데이터를 비대칭암호키로 암호화하여 스마트 그리드 서버 내부의 양자메인보드로 전송한다.

[0135] 양자메인보드(Q-MCU)는 상기 비대칭암호키로 암호화한 스마트 블럭 배전반 ID Address 및 합성데이터를 결합한 데이터블럭 데이터를 수신하여 대칭암호키로 복호화한 후 현재 데이터블럭으로 OTP 메모리(OTP M/M)에 저장한다.

[0136] 양자메인보드(Q-MCU)는 이전 데이터블럭 및 현재 데이터블럭을 연속적으로 데이터블럭으로 체인화하고, 체인화된 블럭체인 데이터를 스마트 블럭 배전반 집합(제1 내지 제 N 스마트 블럭 배전반) 또는 스마트 그리드 서버와 스마트 블럭 배전반 사이에 상호 인증한다.

[0137] 블럭체인 데이터의 상호 인증(합의)이 완료되면 스마트 그리드 서버는 대칭암호키 및 비대칭암호키를 삭제 후 양자난수생성기 및 의사난수생성기를 통해 대칭암호키와 비대칭암호키를 새로 생성하여 블럭체인 주기에 따라 상호 재인증하는 것을 특징으로 한다.

[0139] 일 실시 예로,

[0140] 양자난수생성기 및 의사난수생성기를 포함하는 양자메인보드, OTP 메모리를 포함하여 구성된 스마트 그리드 서버 및 하나 이상의 스마트 블럭 배전반 집합으로 구성된다.

[0142] 양자난수생성기는 난수소스발생기, 양자검출 다이오드, 양자랜덤펄스 생성기, 양자난수 제어부로 구성된다.

[0143] 난수소스발생기는 LED, 방사선 동위원소, 노이즈펄스 중 어느 하나 이상으로부터 양자입자를 방출하는 난수소스발생기이다.

[0144] 양자검출 다이오드는 상기 난수소스발생기로 부터 발생하는 양자입자를 검출하는 양자검출 다이오드이다.

[0145] 양자랜덤펄스 생성기는 상기 양자검출 다이오드로부터 양자입자 이벤트를 검출하여 양자입자의 검출에 상응하는 랜덤펄스를 발생하는 양자랜덤펄스 생성기이다.

[0146] 양자난수 제어부는 상기 양자랜덤펄스 생성기를 통해 발생하는 무작위 난수소스로 양자난수를 생성하는 마이크로프로세서로 구성된 양자난수 제어부이다.

[0148] 양자메인보드는 난수발생 프로그램에 의해 의사난수를 생성하는 의사난수생성기를 포함하여 구성되어, 상기 양자난수 제어부로 부터 양자난수를 수신하여 대칭암호키를 생성한다.

[0149] 또한, 상기 의사난수생성기로부터 발생한 의사난수로 상기 대칭암호키를 암호화하여 비대칭암호키를 생성한다.

[0150] 양자메인보드는 상기 대칭암호키 및 비대칭암호키를 OTP 메모리에 저장 후 비대칭암호키를 스마트 블럭 배전반으로 전송한다.

[0151] 스마트 블럭 배전반은 스마트 블럭 배전반 ID Address 및 데이터블럭 데이터를 비대칭암호키로 암호화하여 스마트 그리드 서버 내부의 양자메인보드로 전송한다.

[0152] 양자메인보드는 상기 비대칭암호키로 암호화 스마트 블럭 배전반 ID Address 및 데이터블럭 데이터를 수신하여 비대칭암호키로 복호화한 후 현재 데이터블럭으로 OTP 메모리에 저장한다.

[0153] 또한, 이전 데이터블럭 및 현재 데이터블럭을 연속적으로 데이터블럭으로 체인화하고, 체인화된 블럭체인 데이터를 스마트 블럭 배전반에 전송하여 상호 인증하고, 상호 인증이 완료되면 스마트 그리드 서버는 대칭암호키 및 비대칭암호키를 삭제 후 양자난수생성기 및 의사난수생성기를 통해 대칭암호키와 비대칭암호키를 새로 생성하는 것을 특징으로 한다.

[0155] 일 실시 예로,

[0156] 양자난수생성기 및 의사난수생성기를 포함하는 양자메인보드, OTP 메모리를 포함하여 구성된 스마트 그리드 서버 및 하나 이상의 스마트 블럭 배전반으로 구성된다.

[0158] 양자메인보드는 양자난수생성기로 부터 양자난수를 수신하여 대칭암호키를 생성하고, 의사난수생성기로부터 발생한 의사난수로 상기 대칭암호키를 암호화하여 비대칭암호키를 생성함에 있어서,

[0159] 양자메인보드는 양자난수생성기로 부터 무작위 양자난수를 수신하여 3차원 행렬 함수인 대칭암호키를 생성한다.

[0160] 양자메인보드는 의사난수생성기를 통해 스마트 블럭 배전반 MAC Address 데이터를 대칭암호키로 암호화한 데이터 값으로 해시함수의 X 좌표 값을 생성한다.

[0161] 양자메인보드는 스마트 블럭 배전반은 PUF Chip를 포함하여 구성되어,

[0162] 양자메인보드는 의사난수생성기를 통해 PUF Chip에서 PUF PIN 데이터를 추출한 후 PUF PIN 데이터를 대칭암호키로 암호화한 데이터 값으로 해시함수의 Y 좌표 값을 생성한다.

[0163] 양자메인보드는 의사난수생성기를 통해 TIME 데이터를 대칭암호키로 암호화한 데이터 값으로 해시함수의 Z 좌표 값을 생성한다.

[0164] Z 값은 블럭체인 인증 주기 및 이전 데이터블럭, 현재 데이터블럭 등을 구별하는 데이터로 사용한다.

[0165] 양자메인보드는 의사난수생성기를 통해 상기 해시함수의 X좌표 값 및 Y좌표 값을 비교하여 X좌표 값이 Y좌표 데이터 값보다 크면 1, 작으면 0으로 이진화하여 TIME 데이터(Z 좌표 값)을 포함하여 비대칭암호키를 생성한다.

[0167] 양자메인보드는 상기 대칭암호키 및 비대칭암호키를 OTP 메모리에 저장 후 비대칭암호키를 스마트 블럭 배전반으로 전송한다.

[0168] 스마트 블럭 배전반은 스마트 블럭 배전반 내부의 ID Address 및 데이터블럭 데이터를 비대칭암호키로 암호화하여 스마트 그리드 서버 내부의 양자메인보드로 전송한다.

[0169] 양자메인보드는 상기 배전반 ID Address 및 데이터블럭 데이터를 수신하여 현재 데이터블럭으로 OTP 메모리에

저장한다.

[0170] 양자메인보드는 이전 데이터블럭 및 현재 데이터블럭을 연속적으로 데이터블럭으로 체인화하고, 체인화된 블럭 체인 데이터를 스마트 블럭 배전반에 전송하여 상호 인증하는 것을 특징으로 한다.

[0172] 일 실시 예로,

[0173] 양자난수생성기 및 의사난수생성기를 포함하는 양자메인보드, OTP 메모리를 포함하여 구성된 스마트 그리드 서버 및 하나 이상의 스마트 블럭 배전반으로 구성된다.

[0175] 양자메인보드는 양자난수생성기로 부터 양자난수를 수신하여 대칭암호키를 생성하고, 의사난수생성기를 통해 상기 대칭암호키를 암호화하여 비대칭암호키를 생성함에 있어서,

[0176] 양자메인보드는 양자난수생성기로 부터 무작위 양자난수를 수신하여 대칭암호키를 생성한다.

[0177] 양자메인보드는 의사난수생성기를 통해 스마트 블럭 배전반 MAC Address 데이터를 대칭암호키로 암호화한 데이터 값으로 해시함수의 X 좌표 값을 생성한다.

[0178] 양자메인보드는 의사난수생성기를 통해 스마트 블럭 배전반 내부의 PUF PIN 데이터를 대칭암호키로 암호화한 데이터 값으로 해시함수의 Y 좌표 값을 생성한다.

[0179] 양자메인보드는 의사난수생성기의 이진화 함수인 해시함수로 상기 X좌표 값 및 Y좌표 값을 비교하여 X좌표 값이 Y좌표 데이터 값보다 크면 1, 작으면 0으로 이진화하는 해시함수로 비대칭암호키

[0180] $KEY_{as} = MAX(\frac{1}{M}\sum KEY_x(x,y), \frac{1}{P}\sum KEY_y(x,y)) = MAX(x,y)$ 를 생성한다.

[0182] 양자메인보드는 상기 대칭암호키 및 비대칭암호키를 OTP 메모리에 저장 후 비대칭암호키를 스마트 블럭 배전반으로 전송한다.

[0183] 스마트 블럭 배전반은 스마트 블럭 배전반 내부의 ID Address 및 데이터블럭 데이터를 비대칭암호키로 암호화하여 스마트 그리드 서버 내부의 양자메인보드로 전송한다.

[0184] 양자메인보드는 상기 배전반 ID Address 및 데이터블럭 데이터를 수신하여 현재 데이터블럭으로 OTP 메모리에 저장한다.

[0185] 양자메인보드는 이전 데이터블럭 및 현재 데이터블럭을 연속적으로 데이터블럭으로 체인화하고, 체인화된 블럭 체인 데이터를 스마트 블럭 배전반에 전송하여 상호 인증하는 것을 특징으로 한다.

[0187] 일 실시 예로,

[0188] 양자난수생성기 및 의사난수생성기를 포함하는 양자메인보드, OTP 메모리를 포함하여 구성된 스마트 그리드 서버와 스마트 블럭 배전반으로 구성된다.

[0190] 양자메인보드는 양자난수생성기로 부터 양자난수를 수신하여 대칭암호키를 생성하고, 의사난수생성기를 통해 상기 대칭암호키를 암호화하여 비대칭암호키를 생성함에 있어서,

[0191] 양자메인보드는 양자난수생성기로 부터 무작위 양자난수를 수신하여 대칭암호키를 생성한다.

[0192] 양자메인보드는 의사난수생성기를 통해 스마트 블럭 배전반 MAC Address 데이터를 대칭암호키로 암호화한 데이터 값으로 해시함수의 X 좌표 값을 생성한다.

[0193] 양자메인보드는 의사난수생성기를 통해 스마트 블럭 배전반 내부의 PUF PIN 데이터를 대칭암호키로 암호화한 데이터 값으로 해시함수의 Y 좌표 값을 생성한다.

[0194] 양자메인보드는 의사난수생성기의 이진화 함수인 해시함수로 상기 X좌표 값 및 Y좌표 값을 비교하여 X좌표 값이 Y좌표 데이터 값보다 크면 1, 작으면 0으로 이진화하는 해시함수로 비대칭암호키

[0195] $KEY_{as} = MAX(\frac{1}{M}\sum KEY_x(x,y), \frac{1}{P}\sum KEY_y(x,y)) = MAX(x,y)$ 를 생성한다.

[0196] 스마트 그리드 서버는 상기 상기 비대칭암호키를 스마트 블럭 배전반으로 전송하는 것을 특징으로 한다.

[0198] 일 실시 예로,

[0199] 조기화재 검지 CCTV 감시카메라는 적외선센서 어레이부와 영상센서 어레이부로 구성된 촬상부 및 적외선을 방사하는 적외선 투광기 및 마이크로프로세서를 포함하는 주제어부로 구성된다.

[0200] 주제어부는 적외선 투광기부터 방사된 방사적외선이 반사되어 촬상부 내부 감지부의 적외선센서 어레이부를 통해 수신되는 수신적외선 주파수를 비교하여 가스에 의해 흡수된 흡수주파수를 추출하여 가스 종류별로 모니터에 색깔로 표출하기 위한 이미지 데이터 및 조기화재경보 이벤트 데이터를 생성한다.

[0201] 주제어부는 촬상부 내부 영상센서 어레이부로부터 수신되는 영상데이터에 상기 이미지 데이터를 합성한 합성데이터를 생성하여 모니터에 표출한다.

[0202] 양자난수생성기 및 의사난수생성기를 포함하는 양자메인보드, OTP 메모리를 포함하여 구성된 동보방송 서버 및 하나 이상의 TTS 동보 방송장치 집합으로 구성되어, 양자난수생성기는 난수소스발생기, 양자검출 다이오드, 양자랜덤펄스 생성기, 양자난수 제어부로 구성된다.

[0203] 난수소스발생기는 LED, 방사선 동위원소, 노이즈펄스 중 어느 하나 이상으로부터 양자입자를 방출하는 난수소스발생기이다.

[0204] 양자검출 다이오드는 상기 난수소스발생기로 부터 발생하는 양자입자를 검출하는 양자검출 다이오드이다.

[0205] 양자랜덤펄스 생성기는 상기 양자검출 다이오드로부터 양자입자 이벤트를 검출하여 양자입자의 검출에 상응하는 랜덤펄스를 발생하는 양자랜덤펄스 생성기이다.

[0206] 양자난수 제어부는 상기 양자랜덤펄스 생성기를 통해 발생하는 무작위 난수소스로 양자난수를 생성하는 마이크로프로세서로 구성된 양자난수 제어부이다.

[0207] 양자메인보드는 난수발생 프로그램에 의해 의사난수를 생성하는 의사난수생성기를 포함하여 구성되어, 상기 양자난수 제어부로 부터 양자난수를 수신하여 대칭암호키를 생성 및 양자메인보드는 상기 의사난수생성기로부터 발생한 의사난수로 상기 대칭암호키를 암호화하여 비대칭암호키를 생성한다.

[0208] 양자메인보드는 상기 대칭암호키 및 비대칭암호키를 OTP 메모리에 저장 후 비대칭암호키를 TTS 동보 방송장치로 전송한다.

[0209] TTS 동보 방송장치는 TTS 동보 방송장치 내부의 ID Address 및 합성데이터 및 조기화재경보 이벤트 데이터를 결합한 데이터블럭 데이터를 비대칭암호키로 암호화하여 동보방송 서버 내부의 양자메인보드로 전송한다.

[0210] 양자메인보드는 상기 TTS 동보 방송장치 ID Address 및 데이터블럭 데이터를 수신하여 현재 데이터블럭으로 OTP 메모리에 저장 및 양자메인보드는 이전 데이터블럭 및 현재 데이터블럭을 연속적으로 데이터블럭으로 체인화하고, 체인화된 블럭체인 데이터를 하나 이상의 TTS 동보 방송장치에 전송하여 상호 인증하고, 상호 인증이 완료되고 조기화재경보 이벤트 데이터가 수신될 경우, 비대칭암호키로 암호화된 TTS(Text To Speech) 조기화재경보 방송문안을 방송한다.

[0211] 동보방송 서버는 상기 TTS(Text To Speech) 방송 종료 후 대칭암호키 및 비대칭암호키를 삭제하고, 양자난수생성기 및 의사난수생성기를 통해 대칭암호키와 비대칭암호키를 새로 생성하는 것을 특징으로 한다.

[0213] 일 실시 예로,

[0214] 양자난수생성기 및 의사난수생성기를 포함하는 양자메인보드, OTP 메모리를 포함하여 구성된 동보방송 서버 및 하나 이상의 TTS 동보 방송장치로(또는 집합으로) 구성된다.

[0215] 양자난수생성기는 난수소스발생기, 양자검출 다이오드, 양자랜덤펄스 생성기, 양자난수 제어부로 구성된다.

[0216] 난수소스발생기는 LED, 방사선 동위원소, 노이즈펄스 중 어느 하나 이상으로부터 양자입자를 방출하는 난수소스발생기이다.

[0217] 양자검출 다이오드는 상기 난수소스발생기로 부터 발생하는 양자입자를 검출하는 양자검출 다이오드이다.

[0218] 양자랜덤펄스 생성기는 상기 양자검출 다이오드로부터 양자입자 이벤트를 검출하여 양자입자의 검출에 상응하는 랜덤펄스를 발생하는 양자랜덤펄스 생성기이다.

[0219] 양자난수 제어부는 상기 양자랜덤펄스 생성기를 통해 발생하는 무작위 난수소스로 양자난수를 생성하는 마이크로프로세서로 구성된 양자난수 제어부이다.

[0220] 양자메인보드는 난수발생 프로그램에 의해 의사난수를 생성하는 의사난수생성기를 포함하여 구성되어, 상기 양자난수 제어부로 부터 양자난수를 수신하여 대칭암호키를 생성한다.

[0221] 양자메인보드는 상기 의사난수생성기로부터 발생한 의사난수로 상기 대칭암호키를 암호화하여 비대칭암호키를 생성한다.

[0222] 양자메인보드는 상기 대칭암호키 및 비대칭암호키를 OTP 메모리에 저장 후 비대칭암호키를 TTS 동보 방송장치로 전송한다.

[0223] TTS 동보 방송장치는 내부의 ID Address 및 데이터블럭 데이터를 비대칭암호키로 암호화하여 동보방송 서버 내부의 양자메인보드로 전송한다.

[0224] 양자메인보드는 상기 TTS 동보 방송장치 ID Address 및 데이터블럭 데이터를 수신하여 현재 데이터블럭으로 OTP 메모리에 저장한다.

[0225] 양자메인보드는 이전 데이터블럭 및 현재 데이터블럭을 연속적으로 데이터블럭으로 체인화하고, 체인화된 블럭체인 데이터를 TTS 동보 방송장치에 전송한다.

[0226] 상기 동보방송 서버와 TTS 동보 방송장치 사이에 블럭체인 데이터를 상호 인증 또는 하나 이상의 TTS 동보 방송장치 상호간에 블럭체인 데이터를 상호 인증이 완료되면 비대칭암호키로 암호화된 TTS(Text To Speech) 방송문안을 방송한다.

[0227] 동보방송 서버는 상기 TTS(Text To Speech) 방송 종료 후 대칭암호키 및 비대칭암호키를 삭제하고, 양자난수생성기 및 의사난수생성기를 통해 대칭암호키와 비대칭암호키를 새로 생성하는 것을 특징으로 한다.

[0229] 일 실시 예로,

[0230] 양자난수생성기 및 의사난수생성기를 포함하는 양자메인보드, OTP 메모리를 포함하여 구성된 동보방송 서버 및 하나 이상의 TTS 동보 방송장치로 구성된다.

[0231] 양자메인보드는 양자난수생성기로 부터 양자난수를 수신하여 대칭암호키를 생성하고, 의사난수생성기로부터 발생한 의사난수로 상기 대칭암호키를 암호화하여 비대칭암호키를 생성함에 있어서,

[0232] 양자메인보드는 양자난수생성기로 부터 무작위 양자난수를 수신하여 3차원 행렬 함수인 대칭암호키를 생성한다.

[0233] 양자메인보드는 의사난수생성기를 통해 TTS 동보 방송장치 MAC Address 데이터를 대칭암호키로 암호화한 데이터 값으로 해시함수의 X 좌표 값을 생성한다.

[0234] 양자메인보드는 의사난수생성기를 통해 PUF Chip을 포함하는 TTS 동보 방송장치에서 PUF Chip의 PUF PIN 데이터를 추출 후 대칭암호키로 암호화한 데이터 값으로 해시함수의 Y 좌표 값을 생성한다.

[0235] 양자메인보드는 의사난수생성기를 통해 TIME 데이터를 대칭암호키로 암호화한 데이터 값으로 해시함수의 Z 좌표 값을 생성한다.

[0236] 양자메인보드는 의사난수생성기를 통해 상기 해시함수의 X좌표 값 및 Y좌표 값을 비교하여 X좌표 값이 Y좌표 데이터 값보다 크면 1, 작으면 0으로 이진화하여 TIME 데이터(Z 좌표 값)을 포함하여 비대칭암호키를 생성한다.

[0237] 양자메인보드는 상기 대칭암호키 및 비대칭암호키를 OTP 메모리에 저장 후 비대칭암호키를 TTS 동보 방송장치로 전송한다.

[0238] TTS 동보 방송장치는 TTS 동보 방송장치 내부의 ID Address 및 데이터블럭 데이터를 비대칭암호키로 암호화하여 TTS 동보 방송장치 내부의 양자메인보드로 전송한다.

[0239] 양자메인보드는 상기 ID Address 및 데이터블럭 데이터를 수신하여 현재 데이터블럭으로 OTP 메모리에 저장한다.

[0240] 양자메인보드는 이전 데이터블럭 및 현재 데이터블럭을 연속적으로 데이터블럭으로 체인화하고, 체인화된 블럭체인 데이터를 상기 동보방송 서버와 TTS 동보 방송장치 사이에 블럭체인 데이터를 상호 인증 또는 하나 이상의 TTS 동보 방송장치 상호간에 블럭체인 데이터를 상호 인증하고, 상호 인증이 완료되면 비대칭암호키로 암호화된 TTS(Text To Speech) 방송문안을 방송한다.

[0241] 동보방송 서버는 상기 TTS(Text To Speech) 방송 종료 후 대칭암호키 및 비대칭암호키를 삭제하고, 양자난수생

성기 및 의사난수생성기를 통해 대칭암호키와 비대칭암호키를 새로 생성하는 것을 특징으로 한다.

[0243] 일 실시 예로,

[0244] 양자난수생성기 및 의사난수생성기를 포함하는 양자메인보드, OTP 메모리를 포함하여 구성된 구내방송 서버 및 구내 영상음성 방송장치(또는 하나 이상의 구내 영상음성 방송장치)로 구성된다.

[0245] 양자난수생성기는 난수소스발생기, 양자검출 다이오드, 양자랜덤펄스 생성기, 양자난수 제어부로 구성된다.

[0246] 난수소스발생기는 LED, 방사선 동위원소, 노이즈펄스 중 어느 하나 이상으로부터 양자입자를 방출하는 난수소스 발생기이다.

[0247] 양자검출 다이오드는 상기 난수소스발생기로 부터 발생하는 양자입자를 검출하는 양자검출 다이오드이다.

[0248] 양자랜덤펄스 생성기는 상기 양자검출 다이오드로부터 양자입자 이벤트를 검출하여 양자입자의 검출에 상응하는 랜덤펄스를 발생하는 양자랜덤펄스 생성기이다.

[0249] 양자난수 제어부는 상기 양자랜덤펄스 생성기를 통해 발생하는 무작위 난수소스로 양자난수를 생성하는 마이크로프로세서로 구성된 양자난수 제어부이다.

[0250] 양자메인보드는 난수발생 프로그램에 의해 의사난수를 생성하는 의사난수생성기를 포함하여 구성되어, 상기 양자난수 제어부로 부터 양자난수를 수신하여 대칭암호키를 생성한다.

[0251] 양자메인보드는 상기 의사난수생성기로부터 발생한 의사난수로 상기 대칭암호키를 암호화하여 비대칭암호키를 생성한다.

[0252] 양자메인보드는 상기 대칭암호키 및 비대칭암호키를 OTP 메모리에 저장 후 비대칭암호키를 구내 영상음성 방송장치로 전송한다.

[0253] 구내 영상음성 방송장치는 내부의 ID Address 및 데이터블럭 데이터(ID, 블럭체인 데이터 등)를 비대칭암호키로 암호화하여 구내방송 서버 내부의 양자메인보드로 전송한다.

[0254] 양자메인보드는 상기 ID Address 및 데이터블럭 데이터를 수신하여 현재 데이터블럭으로 OTP 메모리에 저장한다.

[0255] 양자메인보드는 이전 데이터블럭 및 현재 데이터블럭을 연속적으로 데이터블럭으로 체인화하고, 체인화된 블럭체인 데이터를 하나 이상의 구내 영상음성 방송장치에 전송하여 상호 인증한다.

[0256] 양자메인보드는 상기 상호 인증이 완료되면, 비대칭암호키로 워터마크를 생성하여 영상에 워터마크를 삽입한 워터마크 영상 및 음성 데이터를 구내 영상음성 방송장치로 전송한다.

[0257] 구내방송 서버는 상기 워터마크 영상를 모니터에 표출 및 스피커를 통해 음성 데이터를 방송 후 대칭암호키 및 비대칭암호키를 삭제하고, 양자난수생성기 및 의사난수생성기를 통해 대칭암호키와 비대칭암호키를 새로 생성하는 것을 특징으로 한다.

[0259] 일 실시 예로,

[0260] 조기화재 검지 CCTV 감시카메라는 적외선센서 어레이부와 영상센서 어레이부로 구성된 촬상부 및 적외선을 방사하는 적외선 투광기 및 마이크로프로세서를 포함하는 주제어부로 구성된다.

[0261] 주제어부는 적외선 투광기부터 방사된 방사적외선이 반사되어 촬상부 내부 감지부의 적외선센서 어레이부를 통해 수신되는 수신적외선 주파수를 비교하여 가스에 의해 흡수된 흡수주파수를 추출하여 가스 종류별로 모니터에 색깔로 표출하기 위한 이미지 데이터를 생성한다.

[0262] 주제어부는 촬상부 내부 영상센서 어레이부로부터 수신되는 영상데이터에 상기 이미지 데이터를 합성한 합성데이터를 생성하여 모니터에 표출한다.

[0263] 양자난수생성기 및 의사난수생성기를 포함하는 양자메인보드, OTP 메모리를 포함하여 구성된 구내방송 서버와 구내 영상음성 방송장치 집합으로 구성된다.

[0264] 양자난수생성기는 난수소스발생기, 양자검출 다이오드, 양자랜덤펄스 생성기, 양자난수 제어부로 구성된다.

[0265] 양자메인보드는 상기 의사난수생성기로부터 발생한 의사난수로 상기 대칭암호키를 암호화하여 비대칭암호키를

생성한다.

[0266] 양자메인보드는 상기 대칭암호키 및 비대칭암호키를 OTP 메모리에 저장 후 비대칭암호키를 구내 영상음성 방송장치로 전송한다.

[0267] 구내 영상음성 방송장치는 내부의 ID Address 및 합성데이터를 결합한 데이터블럭 데이터를 비대칭암호키로 암호화하여 구내방송 서버 내부의 양자메인보드로 전송한다.

[0268] 양자메인보드는 상기 ID Address 및 데이터블럭 데이터를 수신하여 현재 데이터블럭으로 OTP 메모리에 저장한다.

[0269] 양자메인보드는 이전 데이터블럭 및 현재 데이터블럭을 연속적으로 데이터블럭으로 체인화하고, 체인화된 블럭체인 데이터를 하나 이상의 구내 영상음성 방송장치에 전송하여 상호 인증한다.

[0270] 양자메인보드는 상기 상호 인증이 완료되면, 비대칭암호키로 워터마크를 생성하여 합성데이터 영상에 워터마크를 삽입한 워터마크 영상 및 음성 데이터를 구내 영상음성 방송장치로 전송한다.

[0271] 구내방송 서버는 상기 워터마크 영상를 모니터에 표출 및 스피커를 통해 음성 데이터를 방송 후 대칭암호키 및 비대칭암호키를 삭제하고, 양자난수생성기 및 의사난수생성기를 통해 대칭암호키와 비대칭암호키를 새로 생성하는 것을 특징으로 한다.

[0273] 일 실시 예로,

[0274] 양자난수생성기 및 의사난수생성기를 포함하는 양자메인보드, OTP 메모리를 포함하여 구성된 구내방송 서버와 구내 영상음성 방송장치로 구성된다.

[0275] 양자메인보드는 양자난수생성기로 부터 양자난수를 수신하여 대칭암호키를 생성하고, 의사난수생성기로부터 발생한 의사난수로 상기 대칭암호키를 암호화하여 비대칭암호키를 생성함에 있어서,

[0276] 양자메인보드는 양자난수생성기로 부터 무작위 양자난수를 수신하여 3차원 행렬 함수인 대칭암호키를 생성한다.

[0277] 양자메인보드는 의사난수생성기를 통해 구내 영상음성 방송장치 MAC Address 데이터를 대칭암호키로 암호화한 데이터 값으로 해시함수의 X 좌표 값을 생성한다.

[0278] 양자메인보드는 의사난수생성기를 통해 PUF를 포함하는 구내 영상음성 방송장치 내부의 PUF PIN 데이터를 대칭암호키로 암호화한 데이터 값으로 해시함수의 Y 좌표 값을 생성한다.

[0279] 양자메인보드는 의사난수생성기를 통해 TIME 데이터를 대칭암호키로 암호화한 데이터 값으로 해시함수의 Z 좌표 값을 생성한다.

[0280] 양자메인보드는 의사난수생성기를 통해 상기 해시함수의 X좌표 값 및 Y좌표 값을 비교하여 X좌표 값이 Y좌표 데이터 값보다 크면 1, 작으면 0으로 이진화하여 TIME 데이터(Z 좌표 값)을 포함하여 비대칭암호키를 생성한다.

[0281] 양자메인보드는 상기 대칭암호키 및 비대칭암호키를 OTP 메모리에 저장 후 비대칭암호키를 영상 및 구내방송 방송장치로 전송한다.

[0282] 구내 영상음성 방송장치는 내부의 ID Address 및 데이터블럭 데이터를 비대칭암호키로 암호화하여 구내방송 서버 내부의 양자메인보드로 전송한다.

[0283] 양자메인보드는 상기 ID Address 및 데이터블럭 데이터를 수신하여 현재 데이터블럭으로 OTP 메모리에 저장한다.

[0284] 양자메인보드는 이전 데이터블럭 및 현재 데이터블럭을 연속적으로 데이터블럭으로 체인화하고, 체인화된 블럭체인 데이터를 하나 이상의 구내 영상음성 방송장치에 전송하여 상호 인증한다.

[0285] 양자메인보드는 상기 상호 인증이 완료되면, 비대칭암호키로 워터마크를 생성하여 영상에 워터마크를 삽입한 워터마크 영상 및 음성 데이터를 구내 영상음성 방송장치로 전송한다.

[0286] 구내방송 서버는 상기 워터마크 영상를 모니터에 표출 및 스피커를 통해 음성 데이터를 방송 후 대칭암호키 및 비대칭암호키를 삭제하고, 양자난수생성기 및 의사난수생성기를 통해 대칭암호키와 비대칭암호키를 새로 생성하는 것을 특징으로 한다.

[0288] 일 실시 예로,

[0289] 양자난수생성기 및 의사난수생성기를 포함하는 양자메인보드, OTP 메모리를 포함하여 구성된 CCTV 제어 서버 및 하나 이상의 암호화 영상저장 CCTV 감시장치 집합으로 구성된다.

[0290] 양자난수생성기는 난수소스발생기, 양자검출 다이오드, 양자랜덤펄스 생성기, 양자난수 제어부로 구성된다.

[0291] 난수소스발생기는 LED, 방사선 동위원소, 노이즈펄스 중 어느 하나 이상으로부터 양자입자를 방출하는 난수소스 발생기이다.

[0292] 양자검출 다이오드는 상기 난수소스발생기로 부터 발생하는 양자입자를 검출하는 양자검출 다이오드이다.

[0293] 양자랜덤펄스 생성기는 상기 양자검출 다이오드로부터 양자입자 이벤트를 검출하여 양자입자의 검출에 상응하는 랜덤펄스를 발생하는 양자랜덤펄스 생성기이다.

[0294] 양자난수 제어부는 상기 양자랜덤펄스 생성기를 통해 발생하는 무작위 난수소스로 양자난수를 생성하는 마이크로프로세서로 구성된 양자난수 제어부이다.

[0295] 양자메인보드는 난수발생 프로그램에 의해 의사난수를 생성하는 의사난수생성기를 포함하여 구성되어, 상기 양자난수 제어부로 부터 양자난수를 수신하여 대칭암호키를 생성한다.

[0296] 양자메인보드는 상기 의사난수생성기로부터 발생한 의사난수로 상기 대칭암호키를 암호화하여 비대칭암호키를 생성한다.

[0297] 양자메인보드는 상기 대칭암호키 및 비대칭암호키를 OTP 메모리에 저장 후 비대칭암호키를 암호화 영상저장 CCTV 감시장치로 전송한다.

[0298] 암호화 영상저장 CCTV 감시장치는 내부의 ID Address 및 데이터블럭 데이터를 비대칭암호키로 암호화하여 CCTV 제어 서버 내부의 양자메인보드로 전송한다.

[0299] 양자메인보드는 상기 ID Address 및 데이터블럭 데이터를 수신하여 현재 데이터블럭으로 OTP 메모리에 저장한다.

[0300] 양자메인보드는 이전 데이터블럭 및 현재 데이터블럭을 연속적으로 데이터블럭으로 체인화하고, 체인화된 블럭 체인 데이터를 하나 이상의 암호화 영상저장 CCTV 감시장치에 전송하여 상호 인증한다.

[0301] 양자메인보드는 상기 상호 인증이 완료되면,

[0302] 암호화 영상저장 CCTV 감시장치 내부 촬상부 영상센서 어레이부로부터 수신한 영상데이터에 관리자에 의해 설정된 프라이버시 영역을 블라인드 처리한 프라이버시 촬영영상을 비대칭암호키로 암호화한 데이터를 암호화 영상저장 CCTV 감시장치로 전송한다.

[0303] 프라이버시 촬영영상은 관리자의 지정에 의해 방범용 CCTV 촬영영상 또는 암호화 영상저장 CCTV 감시장치 중 주거지역 등에서 촬영되는 영역을 관리자가 블라인드 처리한 영상이다.

[0304] CCTV 제어 서버는 상기 암호화한 데이터를 메모리에 저장 후 대칭암호키 및 비대칭암호키를 삭제하고, 양자난수생성기 및 의사난수생성기를 통해 대칭암호키와 비대칭암호키를 새로 생성하는 것을 특징으로 한다.

[0306] 일 실시 예로,

[0307] 양자난수생성기 및 의사난수생성기를 포함하는 양자메인보드, OTP 메모리를 포함하여 구성된 CCTV 제어 서버와 암호화 영상저장 CCTV 감시장치로 구성된다.

[0308] 양자메인보드는 양자난수생성기로 부터 양자난수를 수신하여 대칭암호키를 생성하고, 의사난수생성기로부터 발생한 의사난수로 상기 대칭암호키를 암호화하여 비대칭암호키를 생성함에 있어서,

[0309] 양자메인보드는 양자난수생성기로 부터 무작위 양자난수를 수신하여 3차원 행렬 함수인 대칭암호키를 생성한다.

[0310] 양자메인보드는 의사난수생성기를 통해 암호화 영상저장 CCTV 감시장치 MAC Address 데이터를 대칭암호키로 암호화한 데이터 값으로 해시함수의 X 좌표 값을 생성한다.

[0311] 양자메인보드는 의사난수생성기를 통해 PUF Chip을 포함하는 암호화 영상저장 CCTV 감시장치 내부의 PUF PIN 데이터를 대칭암호키로 암호화한 데이터 값으로 해시함수의 Y 좌표 값을 생성한다.

[0312] 양자메인보드는 의사난수생성기를 통해 TIME 데이터를 대칭암호키로 암호화한 데이터 값으로 해시함수의 Z 좌표

값을 생성한다.

[0313] 양자메인보드는 의사난수생성기를 통해 상기 해시함수의 X좌표 값 및 Y좌표 값을 비교하여 X좌표 값이 Y좌표 데이터 값보다 크면 1, 작으면 0으로 이진화하여 TIME 데이터(Z 좌표 값)을 포함하여 비대칭암호키를 생성한다.

[0314] 양자메인보드는 상기 대칭암호키 및 비대칭암호키를 OTP 메모리에 저장 후 비대칭암호키를 암호화 영상저장 CCTV 감시장치로 전송한다.

[0315] 암호화 영상저장 CCTV 감시장치는 내부의 ID Address 및 데이터블럭 데이터를 비대칭암호키로 암호화하여 CCTV 제어 서버 내부의 양자메인보드로 전송한다.

[0316] 양자메인보드는 상기 ID Address 및 데이터블럭 데이터를 수신하여 현재 데이터블럭으로 OTP 메모리에 저장한다.

[0317] 양자메인보드는 이전 데이터블럭 및 현재 데이터블럭을 연속적으로 데이터블럭으로 체인화하고, 체인화된 블럭체인 데이터를 암호화 영상저장 CCTV 감시장치에 전송하여 상호 인증한다.

[0318] 양자메인보드는 상기 상호 인증이 완료되면, CCTV 감시장치에서 촬영된 영상 중 관리자에 의해 설정된 프라이버시 영역을 블라인드 처리한 프라이버시 촬영영상을 비대칭암호키로 암호화한 데이터를 암호화 영상저장 CCTV 감시장치로 전송한다.

[0319] CCTV 제어 서버는 상기 암호화한 데이터를 메모리에 저장 후 대칭암호키 및 비대칭암호키를 삭제하고, 양자난수생성기 및 의사난수생성기를 통해 대칭암호키와 비대칭암호키를 새로 생성하는 것을 특징으로 한다.

[0321] 일 실시 예로,

[0322] NB-IoT 고장감시 블랙박스형 CCTV 감시장치는 적외선센서 어레이부와 영상센서 어레이부로 구성된 촬상부 및 적외선을 방사하는 적외선 투광기 및 마이크로프로세서를 포함하는 주제어부로 구성되어, 주제어부는 적외선 투광기부터 방사된 방사적외선이 반사되어 촬상부 내부 감지부의 적외선센서 어레이부를 통해 수신되는 수신적외선 주파수를 비교하여 가스에 의해 흡수된 흡수주파수를 추출하여 가스 종류별로 모니터에 색깔로 표출하기 위한 이미지 데이터를 생성하며, 주제어부는 촬상부 내부 영상센서 어레이부로부터 수신되는 영상데이터에 상기 이미지 데이터를 합성한 합성데이터를 생성하여 모니터에 표출한다.

[0323] 양자난수생성기 및 의사난수생성기를 포함하는 양자메인보드, OTP 메모리를 포함하여 구성된 고장감시 제어 서버 및 하나 이상의 NB-IoT 고장감시 블랙박스형 CCTV 감시장치 집합으로 구성된다.

[0324] 양자난수생성기는 난수소스발생기, 양자검출 다이오드, 양자랜덤펄스 생성기, 양자난수 제어부로 구성된다.

[0325] 난수소스발생기는 LED, 방사선 동위원소, 노이즈펄스 중 어느 하나 이상으로부터 양자입자를 방출하는 난수소스발생기이다.

[0326] 양자검출 다이오드는 상기 난수소스발생기로 부터 발생하는 양자입자를 검출하는 양자검출 다이오드이다.

[0327] 양자랜덤펄스 생성기는 상기 양자검출 다이오드로부터 양자입자 이벤트를 검출하여 양자입자의 검출에 상응하는 랜덤펄스를 발생하는 양자랜덤펄스 생성기이다.

[0328] 양자난수 제어부는 상기 양자랜덤펄스 생성기를 통해 발생하는 무작위 난수소스로 양자난수를 생성하는 마이크로프로세서로 구성된 양자난수 제어부이다.

[0329] 양자메인보드는 난수발생 프로그램에 의해 의사난수를 생성하는 의사난수생성기를 포함하여 구성되어, 상기 양자난수 제어부로 부터 양자난수를 수신하여 대칭암호키를 생성한다.

[0330] 양자메인보드는 상기 의사난수생성기로부터 발생한 의사난수로 상기 대칭암호키를 암호화하여 비대칭암호키를 생성한다.

[0331] 양자메인보드는 상기 대칭암호키 및 비대칭암호키를 OTP 메모리에 저장 후 비대칭암호키를 NB-IoT 고장감시 블랙박스형 CCTV 감시장치로 전송한다.

[0332] NB-IoT 고장감시 블랙박스형 CCTV 감시장치는 내부의 ID Address 및 데이터블럭 데이터를 비대칭암호키로 암호화하여 고장감시 제어 서버 내부의 양자메인보드로 전송한다.

[0333] 양자메인보드는 상기 ID Address 및 데이터블럭 데이터를 수신하여 현재 데이터블럭으로 갱신하여 OTP 메모리에

저장한다.

[0334] 양자메인보드는 이전 데이터블럭 및 현재 데이터블럭을 연속적으로 데이터블럭으로 체인화하고, 체인화된 블럭체인 데이터를 하나 이상의 NB-IoT 고장감시 블랙박스형 CCTV 감시장치에 전송하여 상호 블럭체인 인증한다.

[0335] 또는 고장감시 제어 서버와 NB-IoT 고장감시 블랙박스형 CCTV 감시장치사이에 상호 인증 중 어느 하나 이상의 방법으로 상호 인증한다.

[0336] 양자메인보드는 상기 상호(체인화된 블럭체인 데이터를 하나 이상의 NB-IoT 고장감시 블랙박스형 CCTV 감시장치에 전송하여 상호 블럭체인 인증 또는 고장감시 제어 서버와 NB-IoT 고장감시 블랙박스형 CCTV 감시장치사이에 상호 인증 중 어느 하나 이상)인증이 완료되면, NB-IoT 고장감시 블랙박스형 CCTV 감시장치의 고장 유/무 상태 데이터(합성데이터)를 비대칭암호키로 암호화한 데이터를 NB-IoT 네트워크망을 통해 고장감시 제어 서버로 전송한다.

[0337] 고장감시 제어 서버는 상기 암호화한 데이터를 메모리에 저장 후 대칭암호키 및 비대칭암호키를 삭제하고, 양자난수생성기 및 의사난수생성기를 통해 대칭암호키와 비대칭암호키를 새로 생성한다.

[0338] 고장감시 제어 서버와 NB-IoT 고장감시 블랙박스형 CCTV 감시장치 사이에 비대칭암호키, ID Address 및 데이터블럭 데이터, 체인화된 블럭체인 데이터, 고장 유/무 상태 데이터를 비대칭암호키로 암호화한 데이터의 무선통신 네트워크망은 NB-IoT 무선 네트워크망인 것을 특징으로 한다.

[0340] 일 실시 예로,

[0341] 양자난수생성기 및 의사난수생성기를 포함하는 양자메인보드, OTP 메모리를 포함하여 구성된 고장감시 제어 서버와 NB-IoT 고장감시 블랙박스형 CCTV 감시장치로 구성된다.

[0342] 양자메인보드는 양자난수생성기로 부터 양자난수를 수신하여 대칭암호키를 생성하고, 의사난수생성기로부터 발생한 의사난수로 상기 대칭암호키를 암호화하여 비대칭암호키를 생성함에 있어서,

[0343] 양자메인보드는 양자난수생성기로 부터 무작위 양자난수를 수신하여 3차원 행렬 함수인 대칭암호키를 생성한다.

[0344] 양자메인보드는 의사난수생성기를 통해 NB-IoT 고장감시 블랙박스형 CCTV 감시장치 MAC Address 데이터를 대칭암호키로 암호화한 데이터 값으로 해시함수의 X 좌표 값을 생성한다.

[0345] 양자메인보드는 의사난수생성기를 통해 PUF Chip을 포함하는 NB-IoT 고장감시 블랙박스형 CCTV 감시장치 내부의 PUF PIN 데이터를 대칭암호키로 암호화한 데이터 값으로 해시함수의 Y 좌표 값을 생성한다.

[0346] 양자메인보드는 의사난수생성기를 통해 TIME 데이터를 대칭암호키로 암호화한 데이터 값으로 해시함수의 Z 좌표 값을 생성한다.

[0347] 양자메인보드는 의사난수생성기를 통해 상기 해시함수의 X좌표 값 및 Y좌표 값을 비교하여 X좌표 값이 Y좌표 데이터 값보다 크면 1, 작으면 0으로 이진화하여 TIME 데이터(Z 좌표 값)을 포함하여 비대칭암호키를 생성한다.

[0348] 양자메인보드는 상기 대칭암호키 및 비대칭암호키를 OTP 메모리에 저장 후 비대칭암호키를 NB-IoT 고장감시 블랙박스형 CCTV 감시장치로 NB-IoT 무선 네트워크망을 통해 전송한다.

[0349] NB-IoT 고장감시 블랙박스형 CCTV 감시장치는 내부의 ID Address 및 데이터블럭 데이터를 비대칭암호키로 암호화하여 고장감시 제어 서버 내부의 양자메인보드로 NB-IoT 무선 네트워크망을 통해 전송한다.

[0350] 양자메인보드는 상기 ID Address 및 데이터블럭 데이터를 수신하여 현재 데이터블럭으로 OTP 메모리에 저장한다.

[0351] 양자메인보드는 이전 데이터블럭 및 현재 데이터블럭을 연속적으로 데이터블럭으로 체인화하고, 체인화된 블럭체인 데이터를 NB-IoT 고장감시 블랙박스형 CCTV 감시장치에 전송하여 상호 인증한다.

[0352] 양자메인보드는 상기 상호 인증이 완료되면, NB-IoT 고장감시 블랙박스형 CCTV 감시장치의 고장 유/무 상태 데이터를 비대칭암호키로 암호화한 데이터를 NB-IoT 네트워크망을 통해 고장감시 제어 서버로 전송한다.

[0353] 고장감시 제어 서버는 상기 암호화한 데이터를 메모리에 저장 후 대칭암호키 및 비대칭암호키를 삭제하고, 양자난수생성기 및 의사난수생성기를 통해 대칭암호키와 비대칭암호키를 새로 생성한다.

[0354] 고장감시 제어 서버와 NB-IoT 고장감시 블랙박스형 CCTV 감시장치 사이에 비대칭암호키, ID Address 및 데이터

블럭 데이터, 체인화된 블럭체인 데이터, 고장 유/무 상태 데이터를 비대칭암호키로 암호화한 데이터의 무선통신 네트워크망은 NB-IoT 무선 네트워크망인 것을 특징으로 한다.

[0356] 일 실시 예로,

[0357] 양자난수생성기 및 의사난수생성기를 포함하는 양자메인보드, OTP 메모리를 포함하여 구성된 원격검침 서버와 하나 이상의 블럭체인 미터링 태양광 발전장치 집합으로 구성된다.

[0358] 양자난수생성기는 난수소스발생기, 양자검출 다이오드, 양자랜덤펄스 생성기, 양자난수 제어부로 구성된다.

[0359] 난수소스발생기는 LED, 방사선 동위원소, 노이즈펄스 중 어느 하나 이상으로부터 양자입자를 방출하는 난수소스발생기이다.

[0360] 양자검출 다이오드는 상기 난수소스발생기로 부터 발생하는 양자입자를 검출하는 양자검출 다이오드이다.

[0361] 양자랜덤펄스 생성기는 상기 양자검출 다이오드로부터 양자입자 이벤트를 검출하여 양자입자의 검출에 상응하는 랜덤펄스를 발생하는 양자랜덤펄스 생성기이다.

[0362] 양자난수 제어부는 상기 양자랜덤펄스 생성기를 통해 발생하는 무작위 난수소스로 양자난수를 생성하는 마이크로프로세서로 구성된 양자난수 제어부이다.

[0364] 양자메인보드는 난수발생 프로그램에 의해 의사난수를 생성하는 의사난수생성기를 포함하여 구성되어, 상기 양자난수 제어부로 부터 양자난수를 수신하여 대칭암호키를 생성한다.

[0365] 양자메인보드는 상기 의사난수생성기로부터 발생한 의사난수로 상기 대칭암호키를 암호화하여 비대칭암호키를 생성한다.

[0366] 양자메인보드는 상기 대칭암호키 및 비대칭암호키를 OTP 메모리에 저장 후 비대칭암호키를 블럭체인 미터링 태양광 발전장치로 전송한다.

[0367] 블럭체인 미터링 태양광 발전장치는 내부의 ID Address 및 원격검침 데이터를 비대칭암호키로 암호화하여 원격검침 서버 내부의 양자메인보드로 전송한다.

[0368] 양자메인보드는 상기 ID Address 및 원격검침 데이터를 수신하여 현재 원격검침 데이터블럭으로 OTP 메모리에 저장한다.

[0369] 양자메인보드는 이전 원격검침 데이터블럭 및 현재 원격검침 데이터블럭을 연속적으로 데이터블럭으로 체인화하고, 체인화된 블럭체인 데이터를 하나 이상의 블럭체인 미터링 태양광 발전장치에 전송하여 상호 인증하며;

[0370] 양자메인보드는 상기 상호 인증이 완료되면, 블럭체인 미터링 태양광 발전장치의 갱신 원격검침 데이터를 비대칭암호키로 암호화한 데이터를 원격검침 서버로 전송하며;

[0371] 원격검침 서버는 상기 암호화한 데이터를 메모리에 저장 후 대칭암호키 및 비대칭암호키를 삭제하고, 양자난수생성기 및 의사난수생성기를 통해 대칭암호키와 비대칭암호키를 새로 생성하는 것을 특징으로 한다.

[0373] 일 실시 예로,

[0374] 양자난수생성기 및 의사난수생성기를 포함하는 양자메인보드, OTP 메모리를 포함하여 구성된 원격검침 서버와 블럭체인 미터링 태양광 발전장치로 구성된다.

[0375] 양자메인보드는 양자난수생성기로 부터 양자난수를 수신하여 대칭암호키를 생성하고, 의사난수생성기로부터 발생한 의사난수로 상기 대칭암호키를 암호화하여 비대칭암호키를 생성함에 있어서,

[0376] 양자메인보드는 양자난수생성기로 부터 무작위 양자난수를 수신하여 3차원 행렬 함수인 대칭암호키를 생성한다.

[0377] 양자메인보드는 의사난수생성기를 통해 블럭체인 미터링 태양광 발전장치 MAC Address 데이터를 대칭암호키로 암호화한 데이터 값으로 해시함수의 X 좌표 값을 생성한다.

[0378] 양자메인보드는 의사난수생성기를 통해 PUF Chip을 포함하는 블럭체인 미터링 태양광 발전장치 내부의 PUF PIN 데이터를 대칭암호키로 암호화한 데이터 값으로 해시함수의 Y 좌표 값을 생성한다.

[0379] 양자메인보드는 의사난수생성기를 통해 TIME 데이터를 대칭암호키로 암호화한 데이터 값으로 해시함수의 Z 좌표 값을 생성한다.

[0380] 양자메인보드는 의사난수생성기를 통해 상기 해시함수의 X좌표 값 및 Y좌표 값을 비교하여 X좌표 값이 Y좌표 데이터 값보다 크면 1, 작으면 0으로 이진화하여 TIME 데이터(Z 좌표 값)을 포함하여 비대칭암호키를 생성한다.

[0381] 양자메인보드는 상기 대칭암호키 및 비대칭암호키를 OTP 메모리에 저장 후 비대칭암호키를 블럭체인 미터링 태양광 발전장치로 전송한다.

[0382] 블럭체인 미터링 태양광 발전장치는 내부의 ID Address 및 원격검침 데이터블럭 데이터를 비대칭암호키로 암호화하여 원격검침 서버 내부의 양자메인보드로 전송한다.

[0383] 양자메인보드는 상기 ID Address 및 데이터블럭 데이터를 수신하여 현재 데이터블럭으로 OTP 메모리에 저장한다.

[0384] 양자메인보드는 이전 데이터블럭 및 현재 데이터블럭을 연속적으로 데이터블럭으로 체인화하고, 체인화된 블럭체인 데이터를 블럭체인 미터링 태양광 발전장치에 전송하여 원격검침 서버와 블럭체인 미터링 태양광 발전장치 상호 인증한다.

[0385] 양자메인보드는 상기 상호 인증이 완료되면, 블럭체인 미터링 태양광 발전장치의 갱신 원격검침 데이터를 비대칭암호키로 암호화한 데이터를 원격검침 서버로 전송원격검침 서버와 블럭체인 미터링 태양광 발전장치

[0386] 원격검침 서버는 상기 암호화한 데이터를 메모리에 저장 후 대칭암호키 및 비대칭암호키를 삭제하고, 양자난수생성기 및 의사난수생성기를 통해 대칭암호키와 비대칭암호키를 새로 생성하는 것을 특징으로 한다.

[0388] 일 실시 예로,

[0389] 양자난수생성기 및 의사난수생성기를 포함하는 양자메인보드, OTP 메모리를 포함하여 구성된 디밍제어 서버와 하나 이상의 디밍제어 LED 가로등 집합으로 구성된다.

[0390] 디밍제어 LED 가로등은 PUF Chip를 포함하는 마이크로프로세서로 구성된 가로등 제어부를 포함한다.

[0391] 상기 가로등 제어부는 디밍제어 서버와 비대칭암호키로 상호 데이터 통신을 통해 디밍제어 서버로 부터 디밍 데이터를 수신하여 가로등을 디밍(절전 점등)제어한다.

[0392] 양자난수생성기는 난수소스발생기, 양자검출 다이오드, 양자랜덤펄스 생성기, 양자난수 제어부로 구성된다.

[0393] 난수소스발생기는 LED, 방사선 동위원소, 노이즈펄스 중 어느 하나 이상으로부터 양자입자를 방출하는 난수소스발생기이다.

[0394] 양자검출 다이오드는 상기 난수소스발생기로 부터 발생하는 양자입자를 검출하는 양자검출 다이오드이다.

[0395] 양자랜덤펄스 생성기는 상기 양자검출 다이오드로부터 양자입자 이벤트를 검출하여 양자입자의 검출에 상응하는 랜덤펄스를 발생하는 양자랜덤펄스 생성기이다.

[0396] 양자난수 제어부는 상기 양자랜덤펄스 생성기를 통해 발생하는 무작위 난수소스로 양자난수를 생성하는 마이크로프로세서로 구성된 양자난수 제어부이다.

[0397] 양자메인보드는 난수발생 프로그램에 의해 의사난수를 생성하는 의사난수생성기를 포함하여 구성되어, 상기 양자난수 제어부로 부터 양자난수를 수신하여 대칭암호키를 생성한다.

[0398] 양자메인보드는 상기 의사난수생성기로부터 발생한 의사난수로 상기 대칭암호키를 암호화하여 비대칭암호키를 생성한다.

[0399] 양자메인보드는 상기 대칭암호키 및 비대칭암호키를 OTP 메모리에 저장 후 비대칭암호키를 디밍제어 LED 가로등으로 전송한다.

[0400] 디밍제어 LED 가로등는 내부의 ID Address 및 PUF Chip으로 부터 추출한 PIN 데이터를 비대칭암호키로 암호화하여 디밍제어 서버 내부의 양자메인보드로 전송한다.

[0401] 양자메인보드는 상기 ID Address 및 PUF Chip으로 부터 추출한 PIN 데이터를 수신하여 현재 PUF Chip으로 부터 추출한 PIN 데이터블럭으로 OTP 메모리에 저장한다.

[0402] 양자메인보드는 이전 PIN 데이터블럭 및 현재 PIN 데이터블럭을 연속적으로 데이터블럭으로 체인화하고, 체인화된 블럭체인 데이터를 하나 이상의 디밍제어 LED 가로등에 전송하여 상호 인증한다.

[0403] 양자메인보드는 상기 상호 인증이 완료되면, 가로등의 디밍제어 데이터를 비대칭암호키로 암호화하여 전송하는 것을 특징으로 한다.

[0405] 일 실시 예로,

[0406] 양자난수생성기 및 의사난수생성기를 포함하는 양자메인보드, OTP 메모리를 포함하여 구성된 디밍제어 서버와 디밍제어 LED 가로등으로 구성된다.

[0407] 디밍제어 LED 가로등은 PUF Chip를 포함하는 마이크로프로세서로 구성된 가로등 제어부를 포함한다.

[0408] 상기 가로등 제어부는 디밍제어 서버와 비대칭암호키로 상호 데이터 통신을 통해 디밍제어 서버로 부터 디밍 데이터를 수신하여 가로등을 디밍(절전 점등)제어한다.

[0409] 양자메인보드는 양자난수생성기로 부터 양자난수를 수신하여 대칭암호키를 생성하고, 의사난수생성기로부터 발생한 의사난수로 상기 대칭암호키를 암호화하여 비대칭암호키를 생성함에 있어서,

[0410] 양자메인보드는 양자난수생성기로 부터 무작위 양자난수를 수신하여 3차원 행렬 함수인 대칭암호키를 생성한다.

[0411] 양자메인보드는 의사난수생성기를 통해 디밍제어 LED 가로등 MAC Address 데이터를 대칭암호키로 암호화한 데이터 값으로 해시함수의 X 좌표 값을 생성한다.

[0412] 양자메인보드는 의사난수생성기를 통해 PUF Chip을 포함하는 디밍제어 LED 가로등 내부의 PUF PIN 데이터를 대칭암호키로 암호화한 데이터 값으로 해시함수의 Y 좌표 값을 생성한다.

[0413] 양자메인보드는 의사난수생성기를 통해 TIME 데이터를 대칭암호키로 암호화한 데이터 값으로 해시함수의 Z 좌표 값을 생성한다.

[0414] 양자메인보드는 의사난수생성기를 통해 상기 해시함수의 X좌표 값 및 Y좌표 값을 비교하여 X좌표 값이 Y좌표 데이터 값보다 크면 1, 작으면 0으로 이진화하여 TIME 데이터(Z 좌표 값)을 포함하여 비대칭암호키를 생성한다.

[0415] 양자메인보드는 상기 대칭암호키 및 비대칭암호키를 OTP 메모리에 저장 후 비대칭암호키를 디밍제어 LED 가로등으로 전송한다.

[0416] 디밍제어 LED 가로등는 내부의 ID Address 및 PUF Chip으로 부터 추출한 PIN 데이터블럭 데이터를 비대칭암호키로 암호화하여 디밍제어 서버 내부의 양자메인보드로 전송한다.

[0417] 양자메인보드는 상기 ID Address 및 PIN 데이터블럭 데이터를 수신하여 현재 PIN 데이터블럭으로 OTP 메모리에 저장한다.

[0418] 양자메인보드는 이전 PIN 데이터블럭 및 현재 PIN 데이터블럭을 연속적으로 데이터블럭으로 체인화하고, 체인화된 블럭체인 데이터를 디밍제어 LED 가로등에 전송하여 상호 인증한다.

[0419] 양자메인보드는 상기 상호 인증이 완료되면, 로등의 디밍제어 데이터를 비대칭암호키로 암호화하여 전송하는 것을 특징으로 한다.

[0421] 일 실시 예로,

[0422] 양자난수생성기 및 의사난수생성기를 포함하는 양자메인보드, OTP 메모리를 포함하여 구성된 원격제어 서버와 하나 이상의 태양광 발전판넬 또는 하나 이상의 LED 전광판 집합과 하나 이상의 CCTV 열화상 감시카메라로 구성된다.

[0423] 양자난수생성기는 난수소스발생기, 양자검출 다이오드, 양자랜덤펄스 생성기, 양자난수 제어부로 구성된다.

[0424] 난수소스발생기는 LED, 방사선 동위원소, 노이즈펄스 중 어느 하나 이상으로부터 양자입자를 방출하는 난수소스발생기이다.

[0425] 양자검출 다이오드는 상기 난수소스발생기로 부터 발생하는 양자입자를 검출하는 양자검출 다이오드이다.

[0426] 양자랜덤펄스 생성기는 상기 양자검출 다이오드로부터 양자입자 이벤트를 검출하여 양자입자의 검출에 상응하는 랜덤펄스를 발생하는 양자랜덤펄스 생성기이다.

[0427] 양자난수 제어부는 상기 양자랜덤펄스 생성기를 통해 발생하는 무작위 난수소스로 양자난수를 생성하는 마이크로프로세서로 구성된 양자난수 제어부이다.

[0428] 양자메인보드는 난수발생 프로그램에 의해 의사난수를 생성하는 의사난수생성기를 포함하여 구성되어, 상기 양자난수 제어부로 부터 양자난수를 수신하여 대칭암호키를 생성한다.

[0429] 양자메인보드는 상기 의사난수생성기로부터 발생한 의사난수로 상기 대칭암호키를 암호화하여 비대칭암호키를 생성한다.

[0430] 양자메인보드는 상기 대칭암호키 및 비대칭암호키를 OTP 메모리에 저장 후 비대칭암호키를 CCTV 열화상 감시카메라로 전송한다.

[0431] CCTV 열화상 감시카메라는 태양광 발전판넬 또는 LED 전광판을 촬영한 열화상 촬영영상 데이터를 비대칭암호키로 암호화하여 원격제어 서버 내부의 양자메인보드로 전송한다.

[0432] 양자메인보드는 대칭암호키로 복호화하여 화재 발생 전 촬영 열화영상에 관리자 입력 값 이상의 온도 상승시 이벤트를 발생하는 것을 특징으로 한다.

[0434] 일 실시 예로,

[0435] 양자난수생성기 및 의사난수생성기를 포함하는 양자메인보드, OTP 메모리를 포함하여 구성된 원격제어 서버와 태양광 발전판넬 또는 LED 전광판과 CCTV 열화상 감시카메라로 구성된다.

[0436] 양자메인보드는 양자난수생성기로 부터 양자난수를 수신하여 대칭암호키를 생성하고, 의사난수생성기로부터 발생한 의사난수로 상기 대칭암호키를 암호화하여 비대칭암호키를 생성함에 있어서,

[0437] 양자메인보드는 양자난수생성기로 부터 무작위 양자난수를 수신하여 3차원 행렬 함수인 대칭암호키를 생성한다.

[0438] 양자메인보드는 의사난수생성기를 통해 CCTV 열화상 감시카메라 MAC Address 데이터를 대칭암호키로 암호화한 데이터 값으로 해시함수의 X 좌표 값을 생성한다.

[0439] 양자메인보드는 의사난수생성기를 통해 PUF Chip을 포함하는 CCTV 열화상 감시카메라 내부의 PUF PIN 데이터를 대칭암호키로 암호화한 데이터 값으로 해시함수의 Y 좌표 값을 생성한다.

[0440] 양자메인보드는 의사난수생성기를 통해 TIME 데이터를 대칭암호키로 암호화한 데이터 값으로 해시함수의 Z 좌표 값을 생성한다.

[0441] 양자메인보드는 의사난수생성기를 통해 상기 해시함수의 X좌표 값 및 Y좌표 값을 비교하여 X좌표 값이 Y좌표 데이터 값보다 크면 1, 작으면 0으로 이진화하여 TIME 데이터(Z 좌표 값)을 포함하여 비대칭암호키를 생성한다.

[0442] 양자메인보드는 상기 대칭암호키 및 비대칭암호키를 OTP 메모리에 저장 후 비대칭암호키를 CCTV 열화상 감시카메라로 전송한다.

[0443] CCTV 열화상 감시카메라는 태양광 발전판넬 또는 LED 전광판을 촬영한 열화상 촬영영상 데이터를 비대칭암호키로 암호화하여 원격제어 서버 내부의 양자메인보드로 전송한다.

[0444] 양자메인보드는 대칭암호키로 복호화하여 화재 발생 전 관리자 입력값 이상 온도상승시 열화영상 이벤트를 발생하는 것을 특징으로 한다.

[0446] 일 실시 예로,

[0447] 투시필터 CCTV 감시카메라는 적외선센서 어레이부와 영상센서 어레이부로 구성된 촬상부 및 마이크로프로세서를 포함하는 주제어부로 구성되어 자동차 차량번호판을 촬영한다.

[0448] 주제어부는 상기 자동차 차량번호판의 흑체방사 적외선을 촬상부 내부 적외선센서 어레이부를 통해 수신하여 안개, 먼지, 물방울(비)의 영향을 받지 않는 투시영상 데이터를 생성한다.

[0449] 주제어부는 촬상부 내부 영상센서 어레이부로부터 수신되는 영상데이터에 상기 투시영상 데이터를 합성한 합성데이터를 생성하여 모니터에 표출한다.

[0450] 양자난수생성기 및 의사난수생성기를 포함하는 양자메인보드, OTP 메모리를 포함하여 구성된 주차관제 서버 및 하나 이상의 주차관제장치 집합으로 구성된다.

[0451] 양자난수생성기는 난수소스발생기, 양자검출 다이오드, 양자랜덤펄스 생성기, 양자난수 제어부로 구성된다.

[0452] 난수소스발생기는 LED, 방사선 동위원소, 노이즈펄스 중 어느 하나 이상으로부터 양자입자를 방출하는 난수소스

발생기이다.

[0453] 양자검출 다이오드는 상기 난수소스발생기로 부터 발생하는 양자입자를 검출하는 양자검출 다이오드이다.

[0454] 양자랜덤펄스 생성기는 상기 양자검출 다이오드로부터 양자입자 이벤트를 검출하여 양자입자의 검출에 상응하는 랜덤펄스를 발생하는 양자랜덤펄스 생성기이다.

[0455] 양자난수 제어부는 상기 양자랜덤펄스 생성기를 통해 발생하는 무작위 난수소스로 양자난수를 생성하는 마이크로프로세서로 구성된 양자난수 제어부이다.

[0456] 양자메인보드는 난수발생 프로그램에 의해 의사난수를 생성하는 의사난수생성기를 포함하여 구성되어, 상기 양자난수 제어부로 부터 양자난수를 수신하여 대칭암호키를 생성한다.

[0457] 양자메인보드는 상기 의사난수생성기로부터 발생한 의사난수로 상기 대칭암호키를 암호화하여 비대칭암호키를 생성한다.

[0458] 양자메인보드는 상기 대칭암호키 및 비대칭암호키를 OTP 메모리에 저장 후 비대칭암호키를 주차관제장치로 전송한다.

[0459] 주차관제장치는 주차관제장치 ID Address 및 합성데이터를 결합한 데이터블럭 데이터를 비대칭암호키로 암호화하여 주차관제 서버 내부의 양자메인보드로 전송한다.

[0460] 양자메인보드는 상기 비대칭암호키로 암호화한 주차관제장치 데이터블럭 데이터를 수신하여 대칭암호키로 복호화한 후 현재 데이터블럭으로 OTP 메모리에 저장한다.

[0461] 양자메인보드는 이전 데이터블럭 및 현재 데이터블럭을 연속적으로 데이터블럭으로 체인화하고, 체인화된 블럭체인 데이터를 하나 이상의 주차관제장치에 전송하여 상호 인증하고, 상호 인증이 완료되고 주차관제 서버가 모니터에 표출된 합성데이터의 자동차 차량번호판이 수배차량일 경우 비대칭암호키로 암호화된 차량번호판을 통합방범센터로 전송하는 것을 특징으로 하는 양자난수 및 의사난수를 결합한 다차원 행렬 해시함수 블록체인 차량번호 암호화 주차관제장치이다.

[0463] 일 실시 예로,

[0464] 양자난수생성기 및 의사난수생성기를 포함하는 양자메인보드, OTP 메모리를 포함하여 구성된 주차관제 서버와 주차관제장치로 구성된다.

[0465] 양자메인보드는 양자난수생성기로 부터 양자난수를 수신하여 대칭암호키를 생성하고, 의사난수생성기로부터 발생한 의사난수로 상기 대칭암호키를 암호화하여 비대칭암호키를 생성함에 있어서, 양자메인보드는 양자난수생성기로 부터 무작위 양자난수를 수신하여 3차원 행렬 함수인 대칭암호키를 생성한다.

[0466] 양자메인보드는 의사난수생성기를 통해 주차관제장치 MAC Address 데이터를 대칭암호키로 암호화한 데이터 값으로 해시함수의 X 좌표 값을 생성한다.

[0467] 양자메인보드는 의사난수생성기를 통해 PUF Chip을 포함하는 주차관제장치 내부의 PUF Chip으로 부터 추출한 PUF PIN 데이터를 대칭암호키로 암호화한 데이터 값으로 해시함수의 Y 좌표 값을 생성한다.

[0468] 양자메인보드는 의사난수생성기를 통해 TIME 데이터를 대칭암호키로 암호화한 데이터 값으로 해시함수의 Z 좌표 값을 생성한다.

[0469] 양자메인보드는 의사난수생성기를 통해 상기 해시함수의 X좌표 값 및 Y좌표 값을 비교하여 X좌표 값이 Y좌표 데이터 값보다 크면 1, 작으면 0으로 이진화하여 TIME 데이터(Z 좌표 값)을 포함하여 비대칭암호키를 생성한다.

[0470] 양자메인보드는 상기 대칭암호키 및 비대칭암호키를 OTP 메모리에 저장 후 비대칭암호키를 주차관제장치로 전송한다.

[0471] 주차관제장치는 주차관제장치 ID Address 및 데이터블럭 데이터를 비대칭암호키로 암호화하여 주차관제 서버 내부의 양자메인보드로 전송한다.

[0472] 양자메인보드는 상기 비대칭암호키로 암호화한 주차관제장치 데이터블럭 데이터를 수신하여 대칭암호키로 복호화한 후 현재 데이터블럭으로 OTP 메모리에 저장한다.

[0473] 양자메인보드는 이전 데이터블럭 및 현재 데이터블럭을 연속적으로 데이터블럭으로 체인화하고, 체인화된 블럭

체인 데이터를 주차관제장치에 전송하여 상호 인증하고, 상호 인증이 완료되면 비대칭암호키, 합성영상을 통합 방범센터로 전송하는 것을 특징으로 하는 양자난수 및 의사난수를 결합한 다차원 행렬 해시함수 블록체인 차량 번호 암호화 주차관제장치이다.

[0475] 일 실시 예로,

[0476] CCTV 열화상 감시카메라 및 투시필터 CCTV 감시카메라는 적외선 필터(일 예로, 가야옵틱스 X-RAY 필터(http://www.kaya-optics.com/))가 삽입된 투시카메라로 대체 되는 것을 특징으로 한다.

[0478] 일 실시 예로,

[0479] 양자컴퓨터는 양자난수생성기로 부터 무작위 양자난수를 수신하여 3차원 행렬 함수($\sum KEY_s(x,y,z)$)인 대칭암호키를 생성한다.

[0480] 양자컴퓨터는 MAC Address 데이터(M)를 대칭암호키($\sum KEY_s(x,y,z)$)로 암호화한 데이터 값으로 해시함수($MAX(x,y,z)$)의 X 좌표 값을 생성 및 PUF PIN 데이터(P)를 대칭암호키($\sum KEY_s(x,y,z)$)로 암호화한 데이터 값으로 해시함수($MAX(x,y,z)$)의 Y 좌표 값을 생성 및 의사난수생성기를 통해 TIME 데이터(T)를 대칭암호키($\sum KEY_s(x,y,z)$)로 암호화한 데이터 값으로 해시함수($MAX(x,y,z)$)의 Z 좌표 값을 생성한다.

[0481] 양자컴퓨터는 상기 해시함수의 X좌표 값 및 Y좌표 값을 비교하여 X좌표 값이 Y좌표 데이터 값보다 크면 1, 작으면 0으로 이진화하여 TIME 데이터를 포함하여 비대칭암호키를 생성하는 것을 특징으로 한다.

[0483] 일 실시 예로,

양자난수생성기(QRNG; Quantum Random Number Generator) 및 의사난수생성기(PRNG; Pseudo Random Number Generator)를 포함하는 양자메인보드(Q-MCU), OTP 메모리(OTP M/M)를 포함하여 구성된 스마트 그리드 서버이다.

제1 내지 제N 스마트 블럭 배전반 집합(N은 2 이상의 자연수)으로 구성된다.

양자난수생성기(QRNG)는 난수소스발생기, 양자검출 다이오드, 양자랜덤펄스 생성기, 양자난수 제어부로 구성된다.

난수소스발생기는 LED(Light-Emitting Diode), LD(Laser Diode), 방사선 동위원소, 노이즈펄스 중 어느 하나 이상으로부터 양자입자를 방출하는 난수소스발생기이다.

양자검출 다이오드는 상기 난수소스발생기로 부터 발생하는 양자입자를 검출하는 양자검출 다이오드이다.

양자랜덤펄스 생성기는 상기 양자검출 다이오드로부터 양자입자 이벤트를 검출하여 양자입자의 검출에 상응하는 랜덤펄스를 발생하는 양자랜덤펄스 생성기이다.

양자난수 제어부는 상기 양자랜덤펄스 생성기를 통해 발생하는 무작위 난수소스로 양자난수를 생성하는 마이크로프로세서로 구성된 양자난수 제어부이다.

양자메인보드(Q-MCU)는 난수발생 프로그램에 의해 의사난수를 생성하는 의사난수생성기(PRNG)를 포함하여 구성되어, 상기 양자난수 제어부로 부터 양자난수를 수신하여 대칭암호키를 생성하고, 양자메인보드(Q-MCU)는 상기 의사난수생성기(PRNG)로부터 발생한 의사난수로 상기 대칭암호키를 암호화하여 비대칭암호키를 생성하함에 있어서,

양자메인보드(Q-MCU)는 양자난수생성기로 부터 무작위 양자난수를 수신하여 난수 시드(seed)로 대칭암호키를 생성한다.

양자메인보드(Q-MCU)는 의사난수생성기를 통해 스마트 블럭 배전반 MAC Address 데이터를 대칭암호키로 암호화한 데이터 값으로 해시함수의 X 좌표 값을 생성 및 양자메인보드(Q-MCU)는 의사난수생성기를 통해 스마트 블럭 배전반 내부의 PUF PIN 데이터를 대칭암호키로 암호화한 데이터 값으로 해시함수의 Y 좌표 값을 생성하며 및 양자메인보드(Q-MCU)는 의사난수생성기의 이진화 함수인 해시함수로 상기 X좌표 값 및 Y좌표 값을 비교하여 X좌표 값이 Y좌표 데이터 값보다 크면 1, 작으면 0으로 이진화하는 해시함수로 비대칭암호키를 생성한다.

양자메인보드(Q-MCU)는 상기 대칭암호키 및 비대칭암호키를 OTP 메모리(OTP M/M)에 저장 후 비대칭암호키를 스마트 블럭 배전반으로 전송한다.

스마트 블럭 배전반은 스마트 블럭 배전반 ID Address 및 데이터블럭 데이터를 비대칭암호키로 암호화하여 스마트 그리드 서버 내부의 양자메인보드로 전송한다.

양자메인보드(Q-MCU)는 상기 비대칭암호키로 암호화한 스마트 블럭 배전반 ID Address 및 데이터블럭 데이터를 수신하여 대칭암호키로 복호화한 후 현재 데이터블럭으로 OTP 메모리(OTP M/M)에 저장 및 양자메인보드(Q-MCU)는 이전 데이터블럭 및 현재 데이터블럭을 연속적으로 데이터블럭으로 체인화하고, 체인화된 블럭체인 데이터를 스마트 블럭 배전반 집합으로 전송하여 상호 인증하고, 상호 인증이 완료되면 스마트 그리드 서버는 대칭암호키 및 비대칭암호키를 삭제 후 양자난수생성기 및 의사난수생성기를 통해 대칭암호키와 비대칭암호키를 새로 생성하는 것을 특징으로 하는 양자난수 및 의사난수를 결합한 다차원 행렬 해시함수 블럭체인 스마트 블럭 배전반 제어시스템이다.

[0484] 삭제

[0485] 삭제

[0486] 삭제

[0487] 삭제

[0488] 삭제

[0489] 삭제

[0490] 삭제

[0491] 삭제

[0492] 삭제

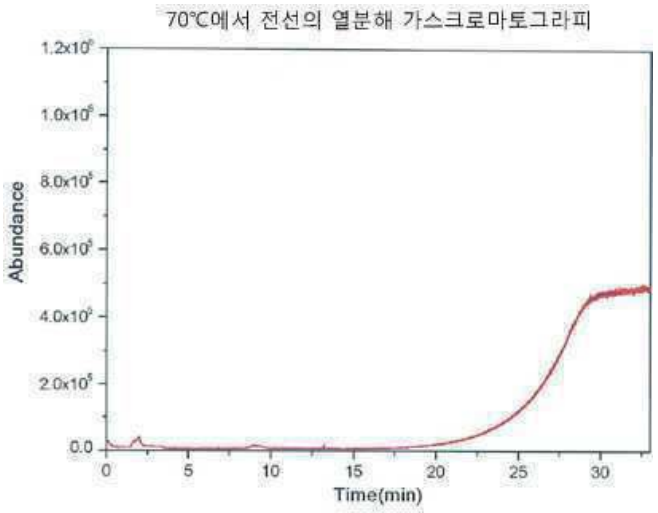
도면

도면1

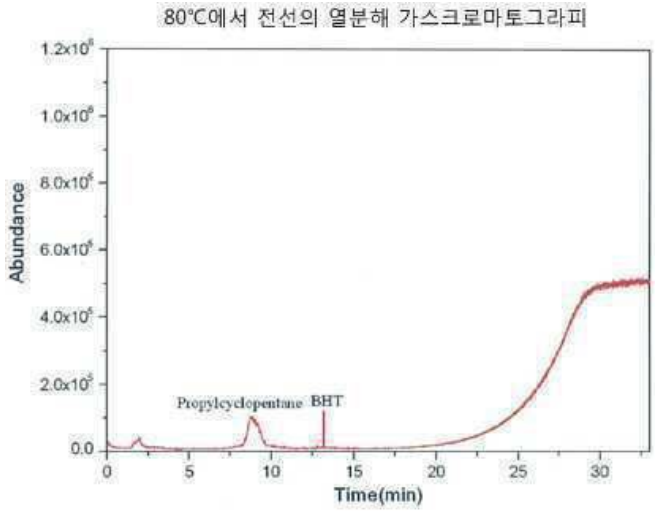
KEY_s : 대칭암호키
KEY_{as} : 비대칭암호키
P : PUF 하드웨어 추출 PIN 데이터
M : MAC Address
(x,y,z) : X,Y,Z 3차 행렬 값
MAX : 두 개의 입력변수 ($\frac{1}{M}\sum KEY_s(x,y,z)$, $\frac{1}{P}\sum KEY_s(x,y,z)$)를 비교하여 좌측의 입력변수가 우축의 입력변수 값보다 크면 1, 작으면 0으로 이진화하는 해시함수

$$KEY_{as} = MAX(\frac{1}{M}\sum KEY_s(x,y,z), \frac{1}{P}\sum KEY_s(x,y,z))$$

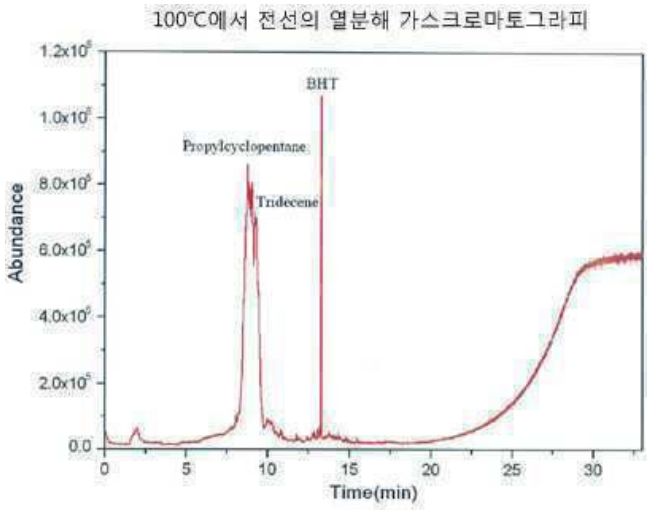
도면2



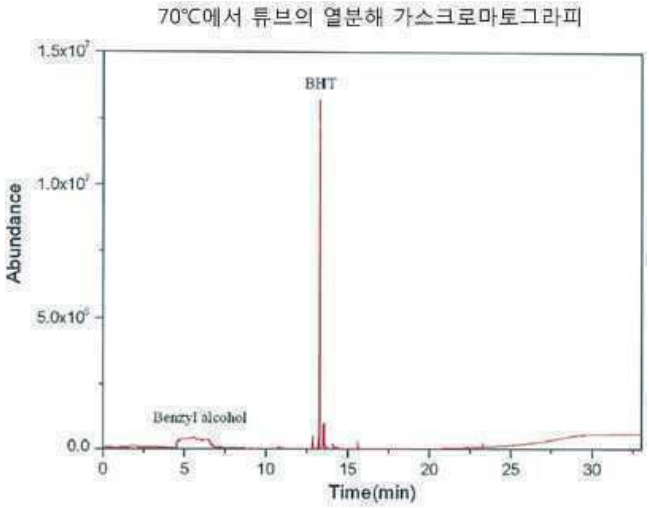
도면3


80℃에서 전선의 열분해 가스크로마토그라피
Abundance
Time(min)
Propylcyclopentane
BHT

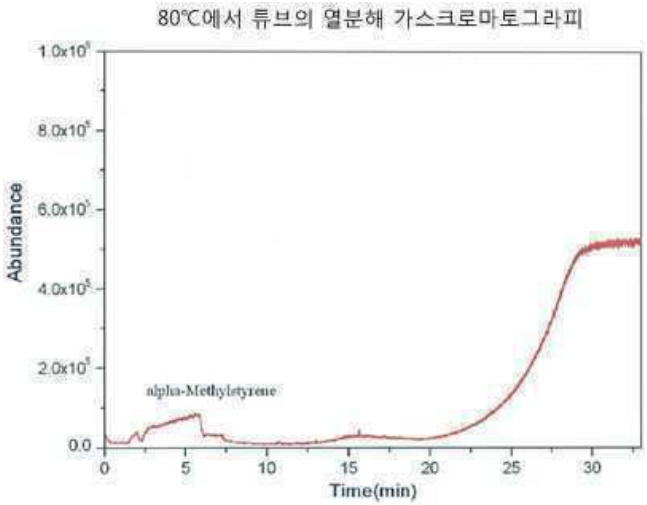
도면4


100℃에서 전선의 열분해 가스크로마토그라피
Abundance
Time(min)
BHT
Propylcyclopentane
Tridecene

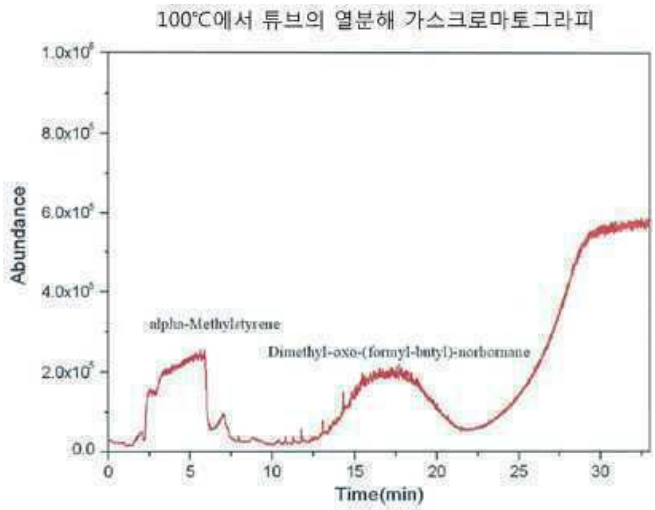
도면5


70℃에서 튜브의 열분해 가스크로마토그라피
Abundance
Time(min)
BHT
Benzyl alcohol

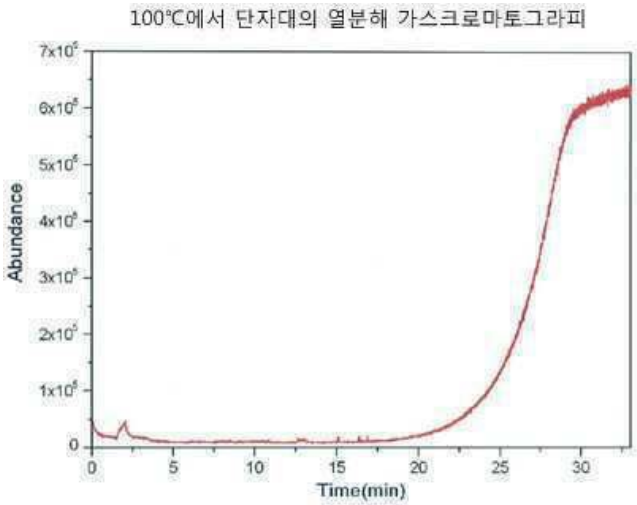
도면6


80℃에서 튜브의 열분해 가스크로마토그라피
Abundance
Time(min)
alpha-Methylstyrene

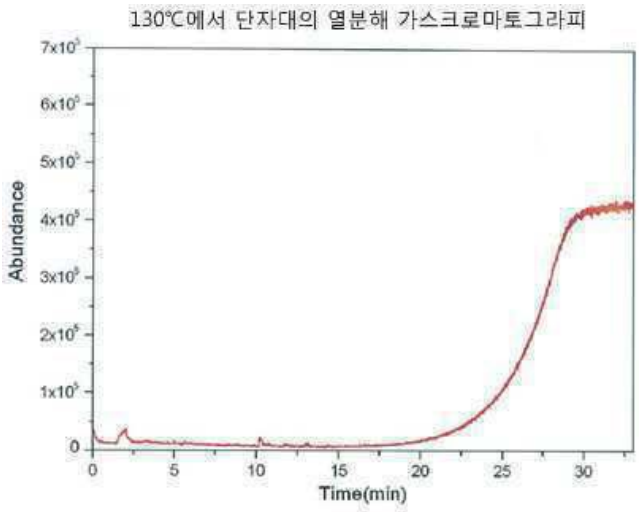
도면7


100℃에서 튜브의 열분해 가스크로마토그라피
Abundance
Time(min)
alpha-Methylstyrene
Dimethyl-oxo-(formyl-butyl)-norbornane

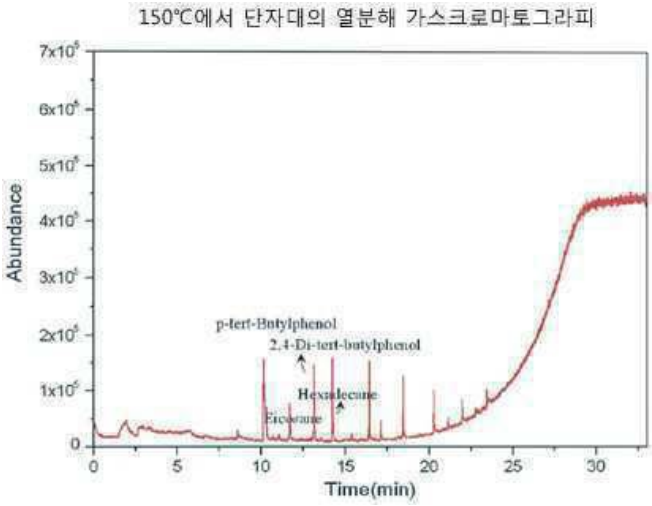
도면8


100℃에서 단자대의 열분해 가스크로마토그라피
Abundance
Time(min)

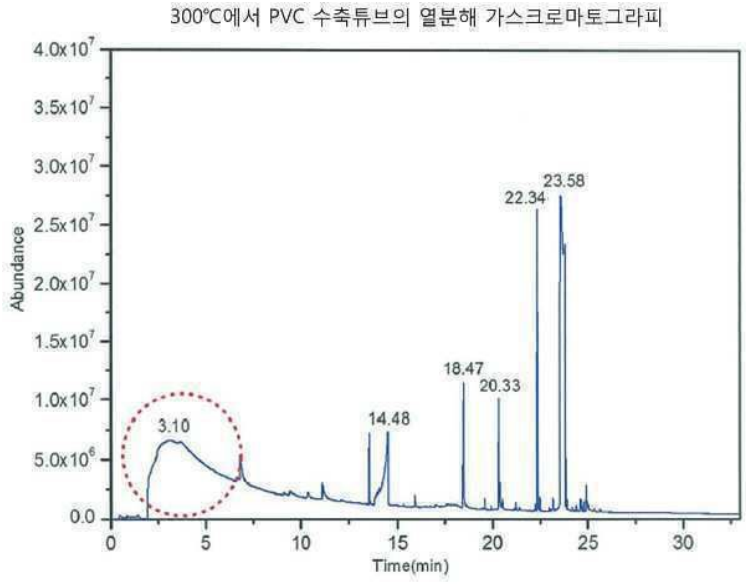
도면9



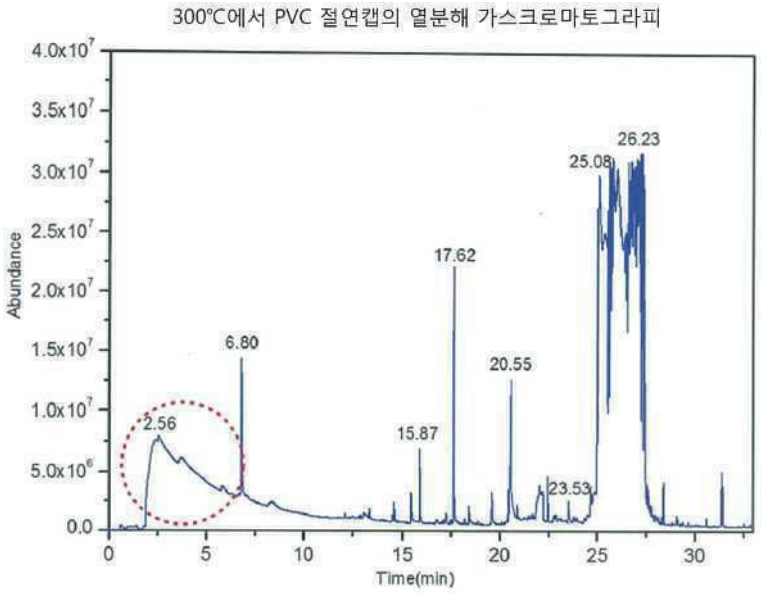
도면10



도면11



도면12


300℃에서 PVC 절연캡의 열분해 가스크로마토그라피
Abundance
Time(min)
2.56
6.80
15.87
17.62
20.55
23.53
25.08
26.23