Quantum Shieldz® Cipher™

스마트폰 도청방지 솔루션

Powered by Quantum Shieldz

양자 엔트로피 :
자연현상에 의해 만들어지는 궁극의 무작위성

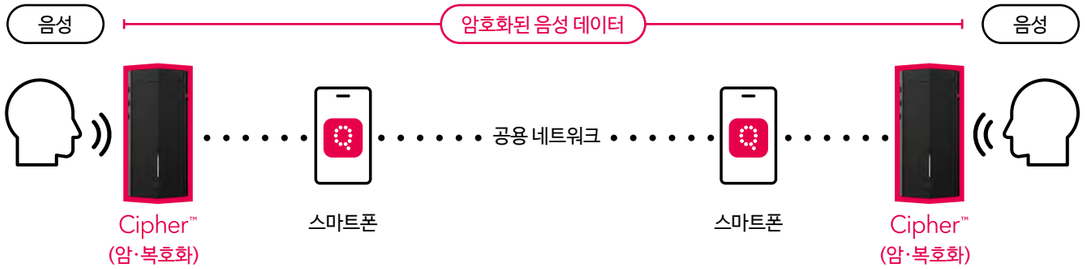
Quantum Shieldz®를 만나보세요.

EYL의 QRNG(Quantum Random Number Generator)과 애플리케이션 제품들은 4차 산업혁명과 차세대 IoT 장치 및 시스템이 요구하는 융합된 보안 문제들을 해결하기 위해 설계되었습니다.

개인 스마트폰을 이용한 비화(祕話)통신 솔루션

Quantum Shieldz® Cipher™는 사용자의 스마트폰과 함께 작동하는 독립형 음성 암호화 장치입니다.
통화하는 사용자의 음성을 양자난수생성기(QRNG, Quantum Random Number Generator)가 생성하는 암호 키로 안전하게 암호화하여 상대방에게 전송함으로써, 스파이웨어를 이용한 도청이나 원하지 않는 녹음을 차단합니다.
Quantum Shieldz® Cipher™는 자신의 스마트폰과 연동되는 간단하면서도 강력한 보안을 갖춘 통신 장치입니다.

Quantum Shieldz® Cipher™를 이용한 음성의 암·복호화



당신의 폰은 안전합니까?

"사생활 몽땅 털려… 스마트폰 도청 비상" - KBS
"당신의 스마트폰이 당신을 도청한다" - 미디어오늘

최근 금융기관을 사칭한 은행 앱은 도청 기능이 몰래 탑재되어 스마트폰 4만 대에 설치되었습니다.
이스라엘의 도청 앱은 프랑스 대통령 등 전 세계 유명 인사 5만 명의 스마트폰에 설치되기도 했습니다.
이와 같이 국방 분야, 국가 간의 정보전쟁, 기업 간의 경쟁, 정치 활동 등의 현장뿐만 아니라 이제 일반인들의 생활에서도 도청이 만연한 상황입니다. 실제로 많은 도청 앱들이 공공연하게 판매, 확산되고 있으며, 본인이 모르는 사이에 도청 앱이 설치될 경우 대화 내용은 실시간으로, 또는 녹음이 되어 어디론가 전송됩니다.
당신의 폰은 더 이상 안전하지 않습니다.

Quantum Shieldz® Cipher™를 통한 안전한 대화

Quantum Shieldz® Cipher™는 사용자의 음성을 강력한 암호 데이터로 변환하여 스마트폰에 전달하며, 아무리 스마트폰을 해킹하여 도청을 시도하더라도 이미 암호화된 데이터는 해독이 불가능합니다. 스마트폰은 전용 앱을 통하여 사용자와 기기를 인증하고 5G 또는 LTE 등의 공용 네트워크를 연결하는 역할만 수행하며, 어떠한 정보도 스마트폰에 저장되지 않습니다.
상대방은 전송받은 암호 데이터를 음성 신호로 복호화 하여 통화를 할 수 있게 됩니다.

스마트폰 제조사, OS 운영 체계, 앱을 신뢰할 수 있을까요?

"미국 CIA, 애플·구글·삼성 운영 체계를 해킹, 도·감청 플랫폼으로 활용"

우리가 사용하는 일반 스마트폰은 안드로이드나 iOS 등의 운영 체계에서 작동합니다. 스마트폰으로 할 수 있는 일이 무궁무진해지면서 사용자들은 수십, 수백 개의 다양한 앱을 다운로드해 사용하고 있지만 그 앱들이 도청에 안전한가에 대하여 잘 아는 사용자는 많지 않습니다. 사용하고 있는 앱은 도청에 안전한지, 안드로이드나 iOS 운영 체계를 제공하는 구글과 애플이 백도어를 만들어 놓지는 않았을지, 핸드폰을 제조하는 삼성, 애플, 화웨이 등은 정말로 믿을 수 있는지 아무도 알 수 없습니다.

현재 국방, 공공 목적으로 비화기가 사용되고 있으나…

"'군 비밀 통화 핸드폰' 최신형으로 교체…2G 폴더폰→5G 스마트폰" -연합뉴스

일반적으로 스마트폰 사용자들은 2년에 한 번씩 새로운 모델로 바꾸고 있고 제조사들은 적어도 6개월에 한 번 이상 새로운 기능을 탑재한 최신 스마트폰을 출시하고 있습니다.
얼마 전까지 국방 및 공공 목적으로 특정 사용자들에게만 지급했던 전용 비화기들은 2G 폴더폰이었습니다.
최근에서야 특정 고위급 500명 만을 대상으로 삼성전자의 갤럭시 S20을 비화기용으로 개조하여 지급하였고 일반인들은 사용할 수 없었습니다.
또한 이 비화기는 스마트폰의 기본적인 기능을 사용하지 못하도록 설정되어 있어 비화 통신 전용으로만 사용해야 하는 단점이 있습니다.
이는 외부에서 접근할 수 없는 높은 보안을 유지하지만, 비밀 통화를 위해 2~3개의 스마트폰을 들고 다녀야 하는 불편함을 유발합니다.

Quantum Shieldz® Cipher™
누구나 사용할 수 있는 음성 암호화 기기입니다.

그래서 Quantum Shieldz® Cipher™ 가 출시되었습니다.
Quantum Shieldz® Cipher™ 는 OS 운영 체계에서 독립된 별도의 기기이며 펌웨어로만 작동하여 스파이웨어, 앱 변조 등으로 인한 위험성은 완전히 차단됩니다. 암호화된 음성 데이터가 스마트폰으로 전달되기 때문에 사용하고 있는 스마트폰의 안전성이 담보되지 않더라도 통화 내용의 도청은 불가능합니다.
이제 Quantum Shieldz® Cipher™ 를 통하여 도청을 걱정하는 일반인들도 비화기를 사용할 수 있습니다.
작은 크기로 소지하기 쉬울 뿐만 아니라 본인의 기존 스마트폰과 함께 여러 기능을 사용하면서도 도청의 걱정을 덜 수 있습니다.

Users

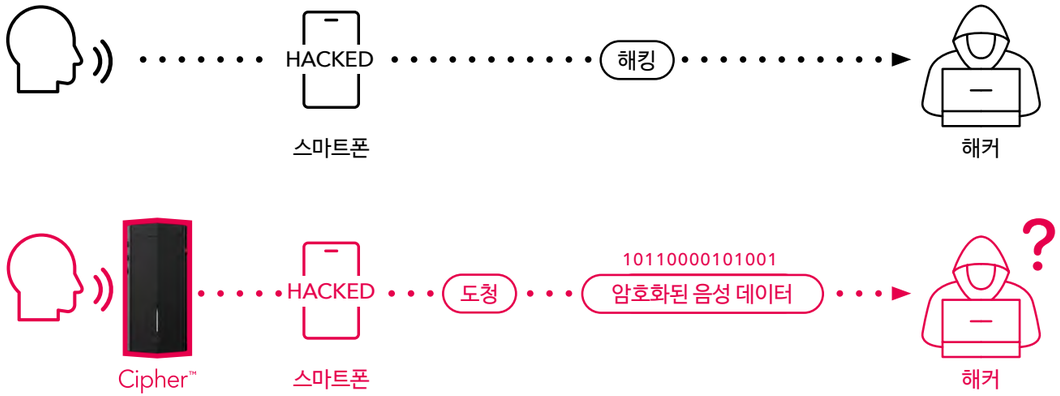
- 주요 정책이 논의되고 결정되는 국가 행정기관,
  수사 및 조사권을 가진 검찰, 경찰 등 사법기관
- 소송 진행 중인 사건의 변호사와 의뢰인, 법무법인
- 산업 스파이의 피해가 예상되는 기업의 CEO 및 주요 임원,
  개발부서, 영업 기획부서 등 비즈니스 분야
- 기밀 정보를 취급하는 정치인, 외교관, 로비스트
- 상대가 있는 선거전을 치르는 대선, 총선, 지자체 선거,
  노조 선거 등의 선거 캠프, 선거관리 위원회
- 입법 활동을 하고 있는 국회의원 및 지방의회 의원
- 각종 감사, 단속을 수행하는 기관
- 기타 개인 사정으로 도청을 우려하는 스마트폰 사용자

Quantum Shieldz® Cipher™
최고 수준의 보안성을 제공합니다.

스파이웨어나 스토커앱을 통하여 스마트폰을 도청하는 것은 어렵지 않습니다. 스마트폰은 사용자에게 많은 편익을 제공하는 반면,
인터넷이 연결된 개방된 구조이기 때문에 해킹 프로그램이나 악성코드에 의해 감염되기도 쉽기 때문입니다.
Quantum Shieldz® Cipher™는 사용자의 음성을 암호화하여 스마트폰에 전달하므로 해커들이 아무리 스마트폰을 해킹하여 도청을 시도
하더라도 암호화된 데이터를 풀어낼 수 없습니다. 암호문을 풀 수 있는 암호 키는 Quantum Shieldz® Cipher™에만 존재하기 때문입니다.

공격자가 암호 키를 예측해서 암호문을 풀 수 있지 않을까요?

암호 키는 예측할 수 없는 난수(亂數)를 이용하여 만듭니다.
하지만 일반적으로 우리가 사용하는 암호 기기는 프로그램으로 만들어진 의사 난수(Pseudo Random Number) 생성기를 사용하고 있기 때문에, 공격자가 난수 생성기 알고리즘을 알아내거나 패턴을 분석하는 방법으로 암호 키를 예측할 수 있습니다.
Quantum Shieldz® Cipher™는 암호 키를 생성하기 위하여 양자난수(Quantum Random Number)생성 칩을 탑재하고 있습니다.
양자난수 생성 기술은 인간이 예측할 수 없는 양자 현상에서 암호 키를 추출하는 방식으로서 대규모 양자암호통신 등 최첨단 통신 기술에 사용되고 있으며 암호 키를 생성하기 위한 현존하는 최고의 보안 기술입니다. 양자난수생성기를 적용하여 만들어진 암호 키를 예측하여 암호문을 푸는 것은 현재뿐만 아니라 미래에도 불가능합니다.



강력한 암호화 솔루션

Quantum Shieldz® Cipher™ 를 사용하는 이상 도청은 불가능합니다.

Quantum Shieldz® Cipher™ 는 스마트폰을 통한 전화 통화와 mVoIP(무선 인터넷망을 통한 음성통화를 이용하는 서비스)에서 발생할 수 있는 모든 취약점이 고려되어 설계되었습니다. 국정원 검증필(KCMVP) 암호모듈이 적용되어 안심하고 사용할 수 있습니다.

사용자 및 기기 인증

비인가 사용자의 접근을 차단하기 위하여 사용자가 서비스를 이용(통화) 할 때마다 사용자와 기기에 대한 인증을 수행합니다. 패턴 모방 방지 기술이 적용된 Quantum OTP 사용자 인증과 검증필 난수발생기를 사용한 양자난수를 이용하여 인증을 수행하며, 128비트 블록 암호 기반 전용 암호화 · 인증 방식이 적용되어 중간자 공격 및 재전송 공격을 방어할 수 있는 멀티-팩터 기반 인증 전 구간 보안 채널을 구현하였습니다.
또한 타원곡선 기반 키 설정 알고리듬(ECDH) 및 Quantum RNG에 의한 일회성 세션키 설정(통화 세션별 독립적 키 설정)과 한국 · 미국 검증기관 권고 타원곡선을 사용하고 있습니다.

사용자 인증정보 재사용 방지

Quantum Shieldz® Cipher™에는 사용자 인증 재사용을 방지하는 메커니즘이 적용되어 있습니다. 단말기에만 인증정보를 저장하며, 네트워크 상에서도 탈취가 불가능하며 이를 위하여 양자난수가 적용됩니다.

중요정보 암호화

외부 공격자가 중요 정보의 내용을 알아채거나 추측하는 것을 방지하기 위하여 사용자, 기기, 통화기록 등을 모두 암호화하여 저장합니다. 이때 필요한 암호 키는 Quantum Shieldz® Cipher™에 별도로 안전하게 보관됩니다.
단말기에서 인코딩된 사용자 음성은 단말기 간 설정된 비밀 키 및 블록 암호 기반 암호화를 통하여 기밀성을 확보하고 출처 인증을 하게 됩니다. 통화가 유지되는 동안 공유 비밀 키 및 키 요소는 오직 단말기 내에서 일시적으로 사용되며 단말기 쌍을 제외한 어떠한 개체에서도 실시간 · 사후 복호화는 불가능하고, 비화 통신 종료 시 세션 정보를 완전히 폐기하게 됩니다.

리코딩 API 차단

악성코드에 감염된 스마트폰의 경우 통화 시 녹음되어 공격자에게 전송될 수 있습니다.
Quantum Shieldz® Cipher™가 작동할 때에는 녹음 API 뿐만 아니라 마이크 및 스피커 기능이 모두 차단되어 이러한 위협에 안전합니다.

KCMVP 검증필 암호모듈 탑재

보안 프로토콜의 모든 암호 기능은 암호모듈 검증 제도(KCMVP: Korea Cryptogrphic Module Validation Program)의 검증필 암호모듈에 의해 제공됩니다.

음성 암호화

모든 음성통화는 암호화됩니다. 암호화를 위하여 SRTP(Secure Real-time Transport Protocol)을 적용하며 키를 가로채지 못하도록 TLS 프로토콜, 상대방과 안전한 키 교환을 위하여 Diffie-Hellman 방식이 사용되며 국정원 검증필 암호인 LEA 암호 알고리즘이 적용되어 있습니다. 암호키 또한 통화 시에 1회 성으로 생성하여 Quantum Shieldz® Cipher™의 암호칩 내에 보관되므로 키 노출이 완벽히 방지됩니다.

아주 간단한 앱 설치로 스마트폰과 연동됩니다

Quantum Shieldz® Cipher™를 스마트폰과 연결하여 사용하기 위한 앱은 안드로이드 및 iOS 앱스토어에서 다운로드할 수 있습니다. 사용자 친화적인 앱 화면 구성을 통해 누구든지 쉽게 사용할 수 있습니다.

전화걸기, 받기

Quantum Shieldz® Cipher™의 전원을 켜면 자동으로 등록된 스마트폰과 블루투스로 연결됩니다. 연결이 안 되어 있을 경우 전화를 걸거나 받을 수 없으며, 앱에서 연결 상태를 알 수 있습니다. 상대방이 수신할 수 있는 상태인지 확인한 후 통화를 요청합니다.

QR Code 사용자 인증 및 등록

앱 [설정]에서 제품 박스에 제공된 QR Code를 통해 단말기와 사용자를 최초로 등록합니다. 복제된 기기가 아닌지, 정당한 사용자인지 검사하는 과정입니다.
Quantum Shieldz® Cipher™와 사용자의 스마트폰은 1:1로 연결되지만, 사용자를 변경해야 할 경우 다른 스마트폰으로 변경 등록이 가능합니다.

전화번호부, 최근 통화 목록

비화 통신을 사용하기 위해 상대방의 전화 번호를 등록하고 상대방이 통화 가능한 상태인지 확인합니다.
상대방의 Quantum Shieldz® Cipher™를 통화 가능한 상태로 요청하기 위해 메시지를 전송할 수 있으며, 최근 통화 목록에서 통화 내역을 볼 수 있고, 편리하게 재발신할 수 있습니다.

기기 및 사용자 추가인증

전화를 걸거나 받을 때, 양자난수를 이용한 패턴 인증을 통한 기기와 사용자 인증에 성공하면 통화를 할 수 있습니다.

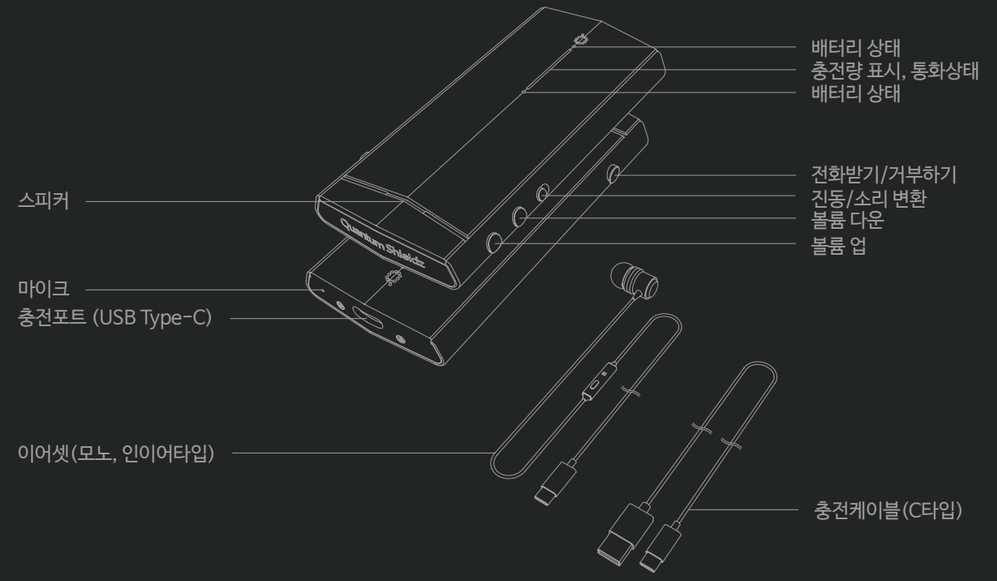
설정

단말기 등록, 사용자 추가인증 여부, 각종 환경 설정을 할 수 있습니다.

획기적인 디자인,
기능과 품격을 함께 생각했습니다

Quantum Shieldz® Cipher™를 사용하면 비화 통신을 위하여 두 개의 스마트폰을 들고 다녀야 하는 불편함이 없어집니다.
한 손에 쏙 들어오는 크기로 셔츠 주머니에 휴대해도 부담이 없습니다.
알루미늄으로 제작된 고급스러운 디자인으로 견고함과 기능성을 함께 고려하여 개발되었습니다.
충전, 전화 송수신, 블루투스 연결, 배터리 잔량을 LED 라이트로 확인할 수 있으며 음량 조절과 진동/소리 모드 변환을 지원합니다.

사이즈 : 44 x 95 x 11 (mm)
무게 : 70g
연결방식 : 블루투스
배터리 : 1,000mA
완충: 2시간
대기: 36시간
연속통화: 4시간



기업 및 단체 전용으로도 사용할 수 있습니다

Quantum Shieldz® Cipher™는 일반인이 요금제 가입을 통하여 사용할 수 있지만 기업 또는 단체 전용으로도 사용할 수 있습니다.
예를 들어 특정 기업 임원 전용으로 서비스를 신청할 경우, 해당 기업 전용 인증 및 통신을 위한 Quantum Shieldz® Cipher™ 서버가 구축되어 단말기를 가진 직원들끼리만 통화를 할 수 있게 됩니다. 이 경우에는 Quantum Shieldz® 단말기를 가진 외부인과의 통화는 차단됩니다.
이것은 기업 내에서 특수한 업무를 수행할 경우 Quantum Shieldz® Cipher™ 단말기를 사안 별로 지급받아 사용될 수 있습니다.
법무법인의 경우 변호사와 의뢰인 간의 소송이 진행될 동안 사용하다가 회수 후 다른 의뢰인이 단말기를 다시 사용하도록 할 수도 있습니다.
또한 기업 및 단체 전용 서비스는 단말기를 분실하거나 부정 사용이 의심될 경우 기업 내 Quantum Shieldz® Cipher™ 관리자는 원격으로 단말기를 사용하지 못하도록 처리하는 등, 기기 등록 및 관리의 편의성을 제공합니다.

제품문의
㈜이와이엘: 서울시 서초구 마방로6길 7-40, 4F (06676)
전화번호: 02-6933-7190, 이메일: contact@eylpartners.com

EYL
EVERYWHERE IN YOUR LIFE