



Clavis XG QKD Portfolio

엔터프라이즈 네트워크를 위한 양자 키 분배
현재와 미래의 사이버 위협으로부터 데이터 기밀성을 보호합니다

디지털 통신의 장기적 보안은 더 이상 기존의 비대칭 키 교환 알고리즘에만 의존할 수 없습니다. 급격히 향상된 컴퓨터 성능, 알려지지 않은 취약점의 위협, 그리고 암호학적으로 위협적인 양자 컴퓨터의 등장 가능성은 암호화된 데이터가 장기간 기밀로 유지될 것이라는 가정을 무너뜨리고 있습니다.

핵심적인 위협은 현재 암호화된 트래픽을 수집하고, 더 강력한 공격 수단이 확보되었을 때 이를 해독하는 능력입니다. 데이터 기밀성을 5년에서 10년 이상 보장해야 하는 정부, 금융 기관, 주요 인프라 운영자에게 이는 사후에 대응할 수 없는 실질적인 위협으로 다가옵니다.

양자 키 분배(QKD)는 수학적 복잡성이 아닌 물리 법칙에 기반한 보안으로 암호 키 교환을 가능하게 하여 이 문제를 해결합니다. 키 정보를 가로채려는 모든 시도는 감지 가능한 교란을 발생시키며, 통신 당사자가 실시간으로 침해 여부를 파악할 수 있습니다.

Clavis XG는 운영 네트워크에서의 원활한 구축을 위해 설계되었습니다. 장거리에 걸쳐 강력하고 높은 키 생성률의 키 분배를 제공하며 엔터프라이즈 및 통신 사업자 환경과 원활하게 통합됩니다. 양자 보안 키 생성을 넘어 양자 내성 암호(PQC)를 결합한 하이브리드 보안 아키텍처로 현재의 사이버 위협과 미래 양자 컴퓨팅 공격 모두에 대응합니다.

주요 시장



통신 및 데이터 센터



금융 서비스



정부 및 국방



주요 인프라



헬스케어



지적재산 소유 기업

주요 응용 분야



데이터 센터 연결



장거리 또는 고처리량 백본 광 네트워크



설계 단계부터 통합된 QKD/PQC 하이브리드



복잡한 네트워크를 통한 키 분배



암호화 키 서비스



엔터프라이즈급 양자 키 분배

Clavis XG QKD Portfolio

모든 데이터 센터에 통합할 수 있는 강력하고 표준화된 설계

Clavis XG는 20년 이상의 양자 기반 제품 개발 및 상업화 경험을 바탕으로 설계된 ID Quantique의 4세대 QKD 시스템입니다.

점대 점, 릴레이, 링 및 스타 네트워크와 같은 모든 종류의 네트워크 토폴로지를 지원합니다. Clavis XG 시스템은 높은 가용성을 제공하여 중단 없이 장기간 안정적인 가동이 가능하도록 설계되었습니다.

시스템 설명

Clavis XG 시스템은 높은 키 생성률이 필요하거나 장거리 네트워크 구성에 사용 가능합니다. 점 대 점, 장거리 릴레이, 링 또는 스타 토폴로지에서도 효율적으로 적용할 수 있습니다. 내장된 키 관리 시스템 (KMS) 소프트웨어를 통해 각 QKD 네트워크 노드에서 QKD와 키 소비자 간의 키 분배를 관리하고 수신자의 위치에 따라 키 소비자 노드에 대해 추가/삭제 또는 전달 기능을 수행합니다.

Clavis XG 시스템은 표준 통신 파장 (C band 또는 O band)에서 동작하며 기존 광섬유 네트워크에 쉽게 구축할 수 있습니다. **Clavis XG 시리즈는 모든 데이터 센터에 간단하고 쉽게 통합될 수 있도록 설계되었습니다.** 19 인치 랙마운트 1U 크기의 컴팩트한 디자인은 상업적으로 완성된 QKD 기술의 최고 수준의 통합을 제공합니다. 키 관리, 모니터링 및 관리자 기능이 내장되어 송신자(Alice)와 수신자(Bob) 간의 양자 채널을 통한 양자 키 생성 및 분배를 수행합니다. 또한, 이중 전원 공급 장치, 핫스왑 배터리 및 팬 모듈과 같은 고가용성 기능을 지원합니다.

표준 광섬유를 통해 양자 암호 키 생성 및 교환을 수행하여 설치 및 유지 관리가 용이하며, 총 소유 비용을 최소화합니다.

ITU 권장 사항에 따라 모든 광채널은 DWDM과 호환됩니다. 전용 광섬유를 통해 양자 채널을 구축하여 노드 간 거리를 최대화할 수 있습니다. 광섬유가 부족할 경우, 단일 코어에서 1310nm(O-band) 대역의 양자 채널을 사용하여 채널 다중화가 가능합니다.

QKD는 RSA 또는 ECC와 같은 기존의 키 분배 기술과 결합하여 이중 보안 키를 생성해 암호화의 견고성을 크게 향상시킬 수 있습니다. 두 원래 키 중 가장 강력한 키로 검증된 양자 보안을 제공합니다. 중요한 것은 기존 시스템의 인증이 이중 보안 키에도 유지되는 것입니다.

Clarion KX 통합 관리 및 모니터링을 통한 Clavis XG 확장성

Enterprise Q-KMS platform

Clarion KX Platform

- 키 릴레이
- 주요 L1~L3 암호화 장비와의 상호운용성
- QKD, ECC 또는 PQC (ML-KEM)을 활용한 하이브리드 키 협약
- 암호화 민첩성
- 고가용성 및 확장성
- 중앙 집중식 관리 및 모니터링*

Clarion KX는 IDQ의 QKD 제품군 및 네트워크 어플라이언스에 내장되어 있으며 연간 라이선스로 제공됩니다.

*물리적 또는 가상 서버 미포함



Clavis XG Product Line

150 km 이하의 모든 광섬유 구축 환경을 위한 엔터프라이즈급 플러그 앤 플레이 BB84 QKD



Solteris Network Appliance

QKD 네트워크를 확장하는 엔터프라이즈급 QKD 구축 역량 및 성능



The Clavis XG QKD System

상호운용성의 중요성

Clavis XG 제품군은 주요 벤더의 암호화 장치와 손쉽게 연결할 수 있는 차세대 상업용 양자 키 분배 (QKD) 시스템입니다. 이중 전원 공급 장치, 핫스왑 배터리 및 팬 모듈, 키 버퍼링, 경고 및 모니터링 기능을 통해 높은 가용성을 제공할 수 있습니다.



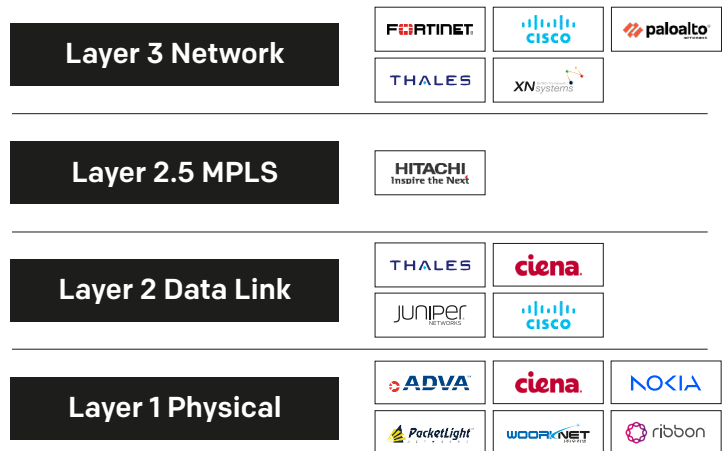
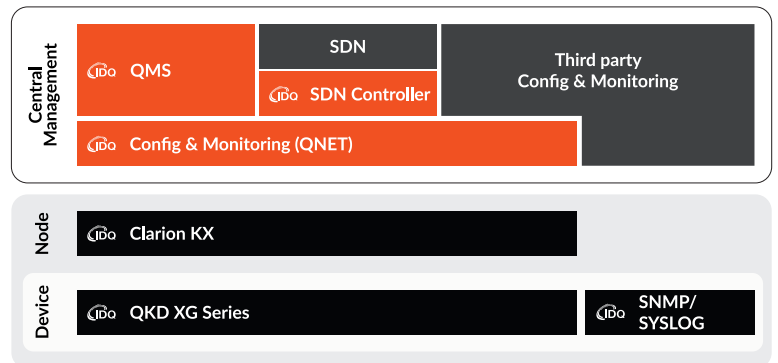
타사 보안 시스템과의 상호 운용성

Clavis XG 제품군은 표준 및 독점 인터페이스를 지원하여 주요 벤더의 암호화 장비들과 손쉽게 접속하고 통신할 수 있습니다. ID Quantique는 QKD 및 기타 보안 시스템의 상호 운용성을 강화하기 위해 ITU 및 ETSI에서 표준화 프로세스에 적극 참여하고 있습니다. 주요 광전송네트워크(OTN) 공급업체는 암호화 장치 (OSI 레이어 1/2/3 및 MPLS)에서 QKD 연동 인터페이스를 제공합니다.

키 관리 및 모니터링

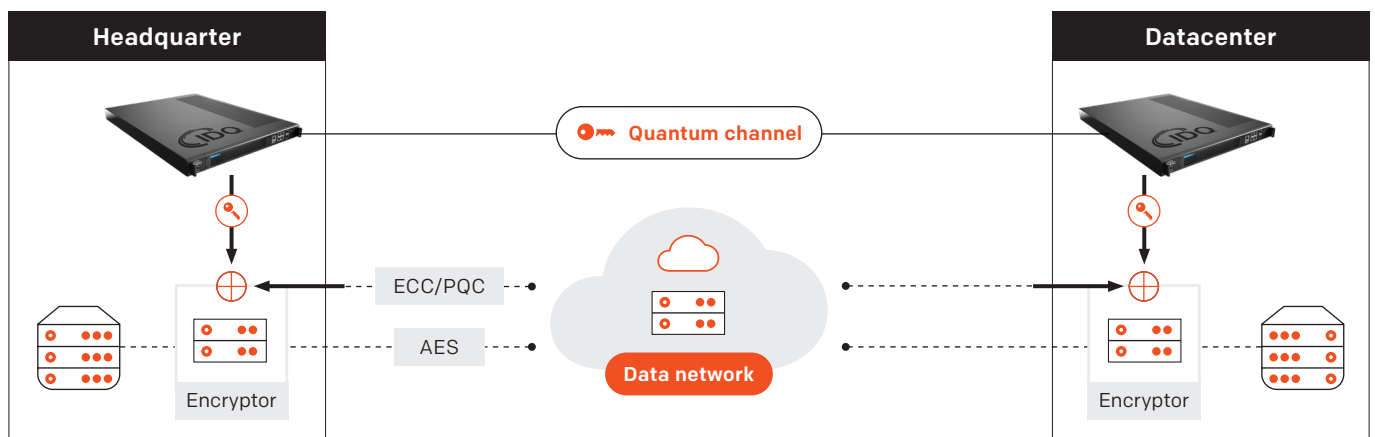
Clavis XG 시스템은 물리적 조작 탐지, 보안 메모리 모듈, 모든 암호 기능 관련하여 무작위성을 제공하는 IDQ의 QRNG 칩을 포함한 강화된 보안 구성 요소들로 이루어져 있습니다. 이를 통해, 키 생성에서 키 전달, 키 저장까지 모든 키 관리 프로세스 전반에 걸쳐 최고 수준의 보안을 보장합니다.

Clavis XG 제품군은 키 관리 소프트웨어 제품군인 Clarion KX와 통합되었으며 IDQ의 QKD 관리 및 모니터링 프레임워크와 연동됩니다. 이 프레임워크는 SDN QKD ETSI 표준뿐만 아니라 IDQ의 양자 관리 시스템 (QNET QMS)로 구성되어 대규모 QKD 배포가 가능하며 기존 인프라에 원활하게 통합될 수 있습니다.



Integration with other suppliers available upon request

"Out-of-band" offering high availability & security



포트폴리오 및 활용 사례

	Clavis XG Short Haul	Clavis XG Backbone	Clavis XG Long Haul	Clavis XG Hub & Spoke	Clavis XG Multiplex
					
Optical layer	Up to 60 km (35 mi)	60 km – 100 km (35 mi – 62 mi)	100 km – 150 km (62 mi – 93 mi)	Up to 90 km (55 mi)	Up to 60 km (37 mi)
	Dedicated fiber for quantum signal				Shared fiber with data
	High data throughput			Medium to high data throughput	
Operation benefits	Easy hardware maintenance (independent Alice/Bob)		Optimized relay node	Optimized footprint, consumption, and cost	Optimized optical fiber usage
Use cases	Access and metro network	Data center interconnection	Extended distance	Star deployment	Access and metro network

Clavis XG 제품군은 광섬유 네트워크를 통해 해킹 불가능한 암호화가 필요한 주요 인프라 운영자 및 정부 기관을 위한 안전한 장거리 **양자 보안 통신**을 지원합니다. 단거리 (60km)부터 장거리 (150km) 전용 광섬유 구축까지 다양한 모델로 최대 데이터 보호를 제공합니다.

기업 및 기관은 이 시스템을 활용하여 현재의 사이버 위협과 미래의 양자 컴퓨팅 공격 모두로부터 **통신, 엔터프라이즈 네트워크, 금융 기관 및 정부 통신**을 보호할 수 있으며, 단순한

점 대 점 연결 (백본, 허브 앤 스포크) 또는 복잡한 **다중 사이트 네트워크** (멀티플렉스)를 위해 최적화된 IDQ 아키텍처를 활용할 수 있습니다.

허브 앤 스포크 및 멀티플렉스 구성은 분산된 사이트 전반에 걸쳐 안전한 키 분배를 가능하게 하면서 하드웨어 유지 관리 요구 사항 및 인프라 복잡성을 최소화하여 확장 가능한 양자 보안 네트워크 인프라를 필요로 하는 엔터프라이즈 및 통신 사업자의 요구를 충족합니다.

주요 장점

- + 대역 외 키 분배 및 즉각적인 침입 탐지
- + 진정한 양자 난수 키 생성
- + 모든 채널을 통일한 하나의 광섬유에 다중화하여 대도시 지역을 단일 코어로 구성
- + 주요 이더넷 및 OTN 암호화 벤더와의 상호 운용성
- + 손쉬운 설치 및 원격 지원
- + 광섬유의 기계적 진동 및 열 변화에 강인 (편광 독립 방식)
- + QNET 소프트웨어를 통한 중앙 집중식 모니터링 솔루션 제공
- + 기존 데이터 통신 채널 무간섭성
- + 소형 폼 팩터: 1U 컴팩트 본체 (송신부 Alice 또는 수신부 Bob)
- + 신뢰할 수 있는 보안 (템퍼 감지, 보안 메모리 모듈, IDQ20MC1 QRNG 칩)



ID QUANTIQUE
www.idquantique.co.kr | sales.kr@idquantique.com



IonQ
www.ionq.com | info@ionq.com