

Criptografía cuántica en redes Cenit Segur@ metropolitanas

Madrid, Marzo 2011

(Proyecto subvencionado por el CDTI)



Centro para el Desarrollo
Tecnológico Industrial



Telefonica

Índic

- 01** **e**
Breve resumen del año
Actividades realizadas

- 02**
Nuevos resultados en maquetas
Últimos experimentos
Demostración

- 03**
Publicaciones
Últimos trabajos

- 04**
Futuro
Líneas futuras

01

Breve resumen del año

Actividades realizadas

■ Laboratorio

- Obtención de nuevos resultados en las maquetas y prototipos iniciados durante las anualidades precedentes
- Prueba y modelización de nuevos escenarios
- Integración con IPSEC

■ Fuera del laboratorio

- Elaboración de patentes
- Participación en el grupo de estandarización de ETSI ISG QKD
- Exposición del trabajo en ámbitos internacionales

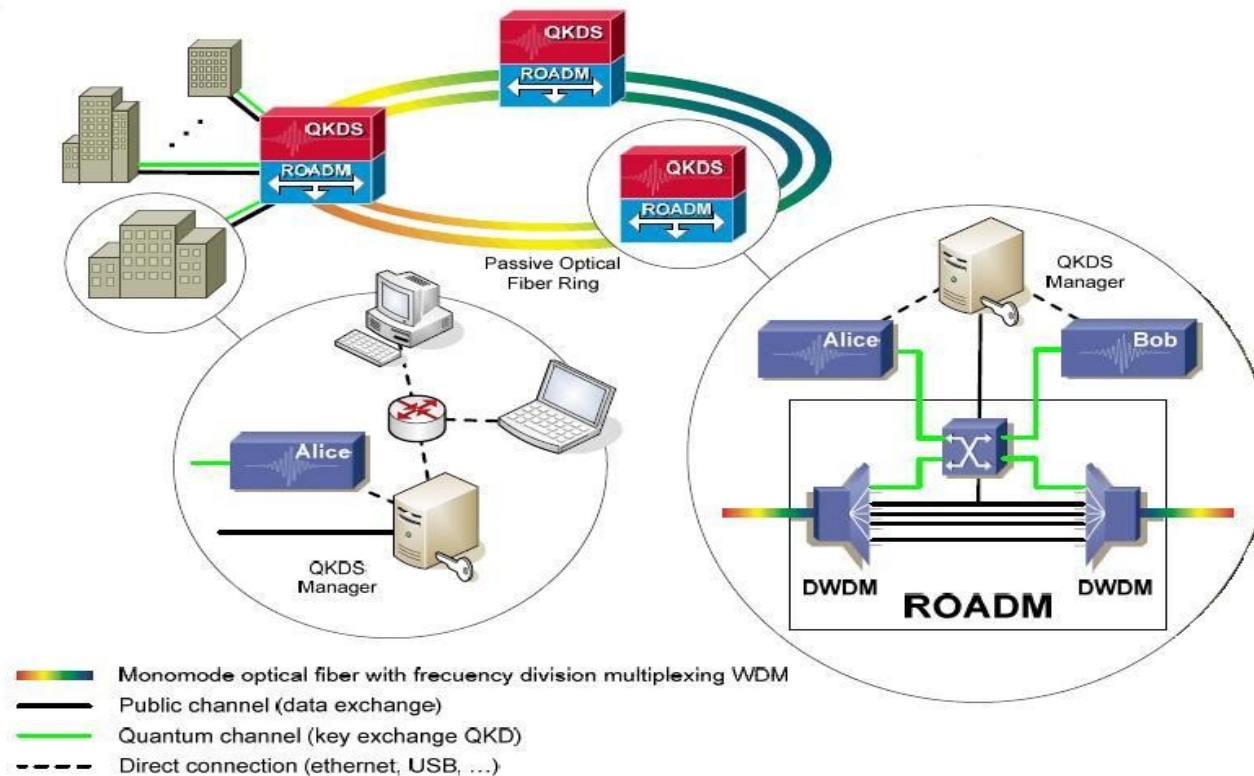
■ Apoyo y seguimiento de otros proyectos (QREP, QUITEMAD, EDISON, SIGREP, RITELQ)

02

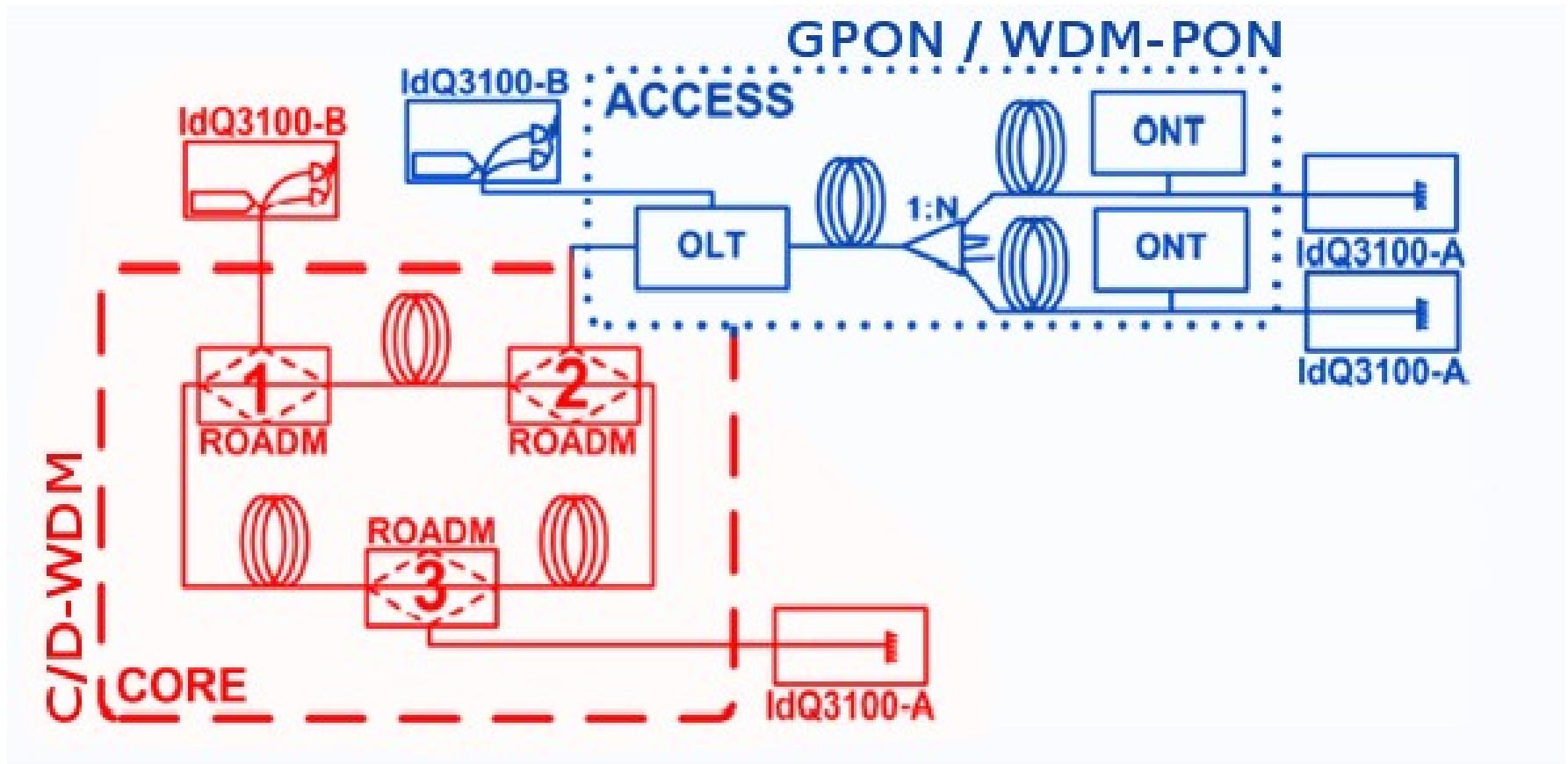
Nuevos resultados en maquetas

Últimos experimentos

- Continuando con la tarea iniciada en las anualidades anteriores, en este caso se han caracterizado, diseñado, definido y medido los resultados para un escenario metropolitano donde canales cuánticos y clásicos coexisten



Últimos experimentos



Demostración



03

Publicaciones

■ Patentes

- *Device for Asynchronous and unreported Allocation of Secret Key Material in spatially distant locations*
 - > J. Dávila, M. Soto, V. Martín
 - > Número de solicitud: P201001362 (registrado 15/10/2010 en OEPM Madrid)
- *Fine optical line monitoring in communication lines through QKD systems*
 - > V. Martín, M. Soto, D. Lancho, J. Martínez
 - > Número de Solicitud: P201032001 (registrado 29/12/2010 en OEPM Madrid)

■ Estándares por el grupo ETSI ISG QKD

- *QKD Use Cases*
 - > TID
- *QKD Application Interface*
 - > TID, UPM
- *QKD Module Security Specification*
 - > UPM

Últimos trabajos

■ Conferencias

- *Integrating QKD in telecommunication networks*
 - › *Quantum Communication Workshop 2010 (Kjeller, Noruega)*
- *Quantum Key Distribution in Optical Switched Networks*
 - › *Quantum Private Telecommunications Workshop 2010 (Aveiro, Portugal)*
- *Deploying QKD in Standard Optical Networks*
 - › *Updating Quantum Cryptography and Communications 2010 (Tokio, Japón)*

NIKKEI SCIENCE ENERO 2011
VERSIÓN JAPONESA DEL SCIENTIFIC
AMERICAN

*Hacia redes prácticas de criptografía
cuántica*

*“...A partir del próximo año, servicios
de redes cuánticas se comenzaran a
ofrecer [...] servicios que está
considerando el gigante español de las
comunicaciones Telefónica, que ya
proporciona sistemas de redes
cuánticas...”*

Razón Social: Telefónica

量子暗号通信 実運用へ
東京ネットワーク始動



04

Futuro

Líneas futuras

- Definición del plan de trabajo 2011-2012 por el grupo ETSI ISG
 - Interfaces de aplicaciones y gestión de claves
 - Integración en redes de telecomunicaciones
 - › Diseño de red cuántica
- Continuación de colaboración con otros proyectos
 - QITEMAD, EDISON, QREP, SIGREP, RITELQ
- Próximos experimentos en el laboratorio con otros grupos de investigación internacionales
 - GAP (Ginebra, Suiza):
 - › Protocolo COW (*Coherent One Way*) en escenarios metropolitanos
 - AIT (Viena, Austria):
 - › Pares entrelazados
- Próximo evento: TQC 2010
 - *Theory of Quantum Computation, Communication and Cryptography*
 - Organizado por QITEMAD, patrocinador Telefónica

Telefónica
