Hacia comunicaciones seguras de tipo cuántico

Guillermo Morales-Luna
Departamento de Computación
Centro de Investigación y Estudios Avanzados del IPN, Cinvestav-IPN
gmorales@cs.cinvestav.mx

26 de julio de 2015

Resumen

Presentamos una breve reseña de las implementaciones en la última década de comunicaciones seguras de tipo cuántico, en particular de los procesos de distribución cuántica de claves. A grandes rasgos, recontamos los prototipos de Peev, Zeilinger *et al.*, de Jouguet *et al.*, de Lucamarini *et al.*, de Scarani *et al.*, de Walenta *et al.*, los realizado en la R. P. de China y el más reciente de Vallone *et al.*

1 Introducción

La computación cuántica es un riesgo para la criptografía actual. Desde la década de los 90 fueron presentados algoritmos de cómputo cuántico capaces de resolver el *Problema de Factorización*, el cual es la base matemática de RSA, y el *Problema del Logaritmo Discreto*, el cual es la base matemática de El-Gamal y de la criptografía de curvas elípticas. Presenta pues un riesgo para la criptografía de clave pública usual hoy en día en todos los sistemas de comunicación segura: militares, diplomáticos, comerciales, bancarios, notariales, etc. Así que la aparición de computadoras cuánticas podría ocasionar una gran crisis social y económica.

Ha habido grandes avances en la implementación de la criptografía cuántica, en especial, en los métodos para la *distribución cuántica de claves* (QKD: *quantum key distribution*).

Idealmente, una red QKD de tipo bancaria con comunicaciones a otros tipos de servicios se bosqueja en la Figura 1.

Diseños previstos para redes nacionales de tipo cuántico en los EUA y en China se muestran en la Figura 2.

Presentaremos varios prototipos desarrollados para la distribución de claves. Los principales problemas a resolver en las implementaciones son lo limitado de las distancias entre participantes, la tasa baja de distribución de claves, pues decrece exponencialmente con la distancia, y la limitante actual de que actúen punto-a-punto.

2 SECOQC

En 2009 se reportó [1] el sistema de distribución de claves (SECOQC: *SEcure COmmunication based on Quantum Cryptography*) desarrollado principalmente en Viena, Austria.

SECOQC se diseñó como una red abocada a la QKD, considerando comunicaciones punto-a-punto entre usuarios y repetidores confiables que preservan la seguridad en las transmisiones. Es pues una gráfica cuyos nodos son los participantes, haciendo también las veces de repetidores, plenamente confiables, y cuyas aristas son canales cuánticos punto-a-punto. En cada uno de éstos, se realiza también tareas de autenticación.

La red de comunicaciones se montó en diferentes dependencias de Siemens, en Viena:

SIE: Siemensstraße, BRT: Breitenfurterstraße, GUD: Gudrunstraße,
ERD: Erdberger Lände, FRM: Siemens Forum STP: St Pölten

El diagrama técnico de conexión se muestra en la Figura 4. Se implementó los protocolos BB84 y SARG [8].

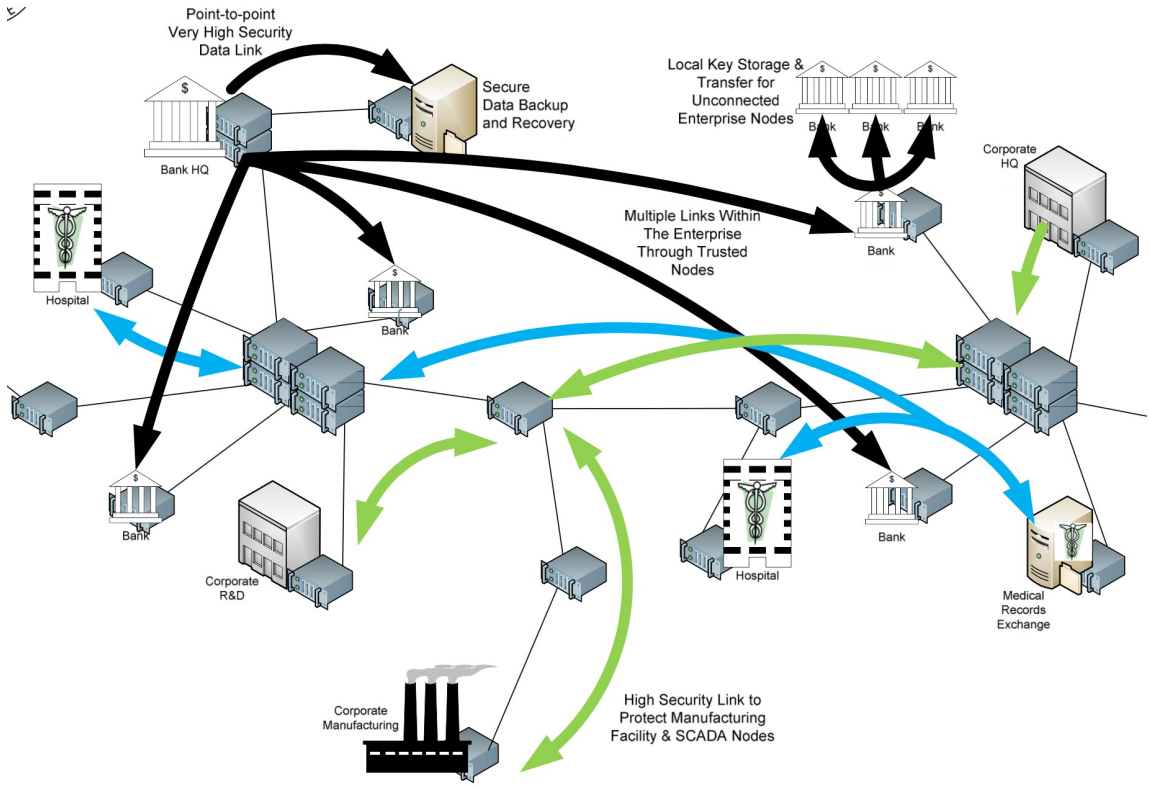


Figure 1: Diagrama de una red ideal para la QKD, la imagen proviene de [3].

En esta red también se implementó protocolos basados en entrelazamiento, en particular BBM92 [2], utilizando fotones entrelazados, con bases distintas realizadas por polarización. Naturalmente, ha de atenderse problemas de estabilización, de alineación, de polarización y de sincronización. La conectividad entre dos nodos se muestra en la Figura 5, las conexiones rojas son ópticas, en tanto que las negras son electrónicas.

En esta red se hicieron pruebas también de un sistema de *variables continuas* (CVQKD: *continuous-variable*) para protocolos de QKD de *estados coherentes con reconciliación revertida* (*coherent-state reverse-reconciliated*.

3 CVQKD a distancias de decenas de kms

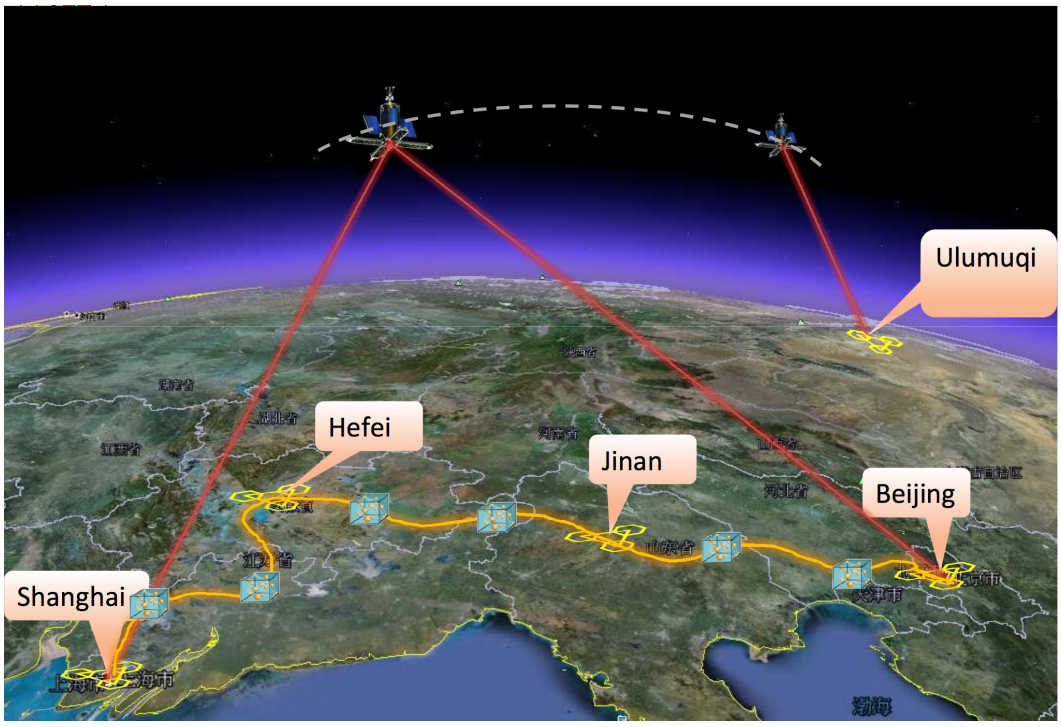
En [5] se reporta el prototipo desarrollado en Francia en 2012. Se implementó el protocolo GG02 de tipo CVQKD presentado en [4]. Está basado en estados coherentes con modulación gaussiana, haciendo mediciones de cuadratura utilizando sistemas de detección de homodinas, así como esquemas de reconciliación revertida. Un diagrama de la conexión entre dos partes se ve en la Figura 6.

El propósito principal de esta red consistió en evitar el uso de repetidores, pues la suposición de que éstos siempre serán confiables es inadmisible en un ambiente de seguridad extrema.

4 QKD en laboratorios Toshiba

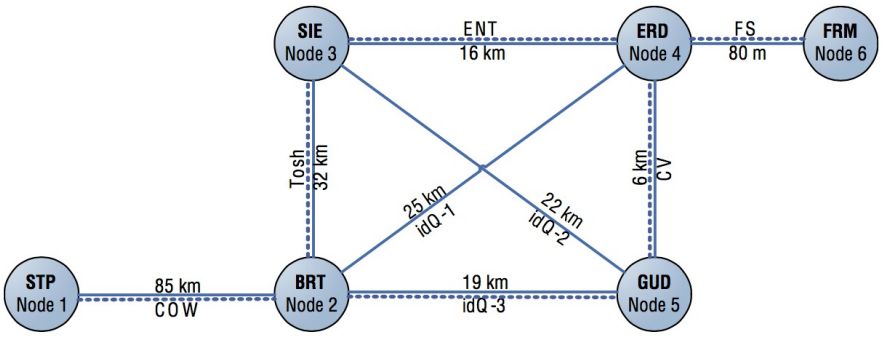
En [7] se reporta el prototipo desarrollado en los laboratorios Toshiba, en 2013. Los fotones simples, sencillamente, no existen o, al menos, no pueden ser detectados individualmente. En la práctica, se utiliza fuentes de lśeres en estados de coherencia débil, los cuales conllevan un flujo de fotones, por lo cual, al utilizrseles como portadores de información, pueden introducir ruido. Así pues, es necesario utilizar láseres muy débiles. Surgen así los QKD de *estados de señuelo* (*decoy-states QKD*), con los que flujos de fotones se comportan

Red en los EUA



Red en China

Figure 2: Ambas imágenes provienen de [3].



(a)

(b)

Figure 3: (a) Gráfica de conexión y (b) localización geográfica del sistema de comunicaciones de la red de QKD (ambas imágenes provienen de [1]).

como fotones individuales.

Se implementa BB84 en un QKD con sincronía al nivel de GHz, lo que les permite una red con separación entre participantes de hasta 50 km. Los autores presentan con detalle una variante, llamada T12, de BB84. Reportan una precisión en el establecimiento de claves de probabilidad $1 - 10^{-10}$.

5 QKD en China

En [13] se reporta el prototipo desarrollado en Shangai, China, en 2012. Se transmite qubits a una distancia de 97 kms, punto-a-punto, en un canal al aire libre y entrelazamiento de varios fotones, utilizando esquemas de codificación superdensa. Mediante láseres y sus polarizaciones se realiza el entrelazamiento.

En [12] se presenta un segundo desarrollo por el mismo equipo que permite la transmisión de qubits entre satélites, el *Chinese Quantum Science Satellite* y el *CHAllenging Minisatellite Payload* (CHAMP) alemán y estaciones terrenas (separados alrededor de 400 kms), con lo que es posible establecer una QKD segura de manera incondicional.

6 QKD en Suiza

En [6] se reporta un prototipo desarrollado en Ginebra, Suiza, en 2014, el cual implementa el protocolo de *coherencia unidireccional* (COW-QKD: *coherent one-way QKD*) [9].

Los desarrollos arriba descritos utilizan, en sus conexiones, detectores superconductores de fotonones

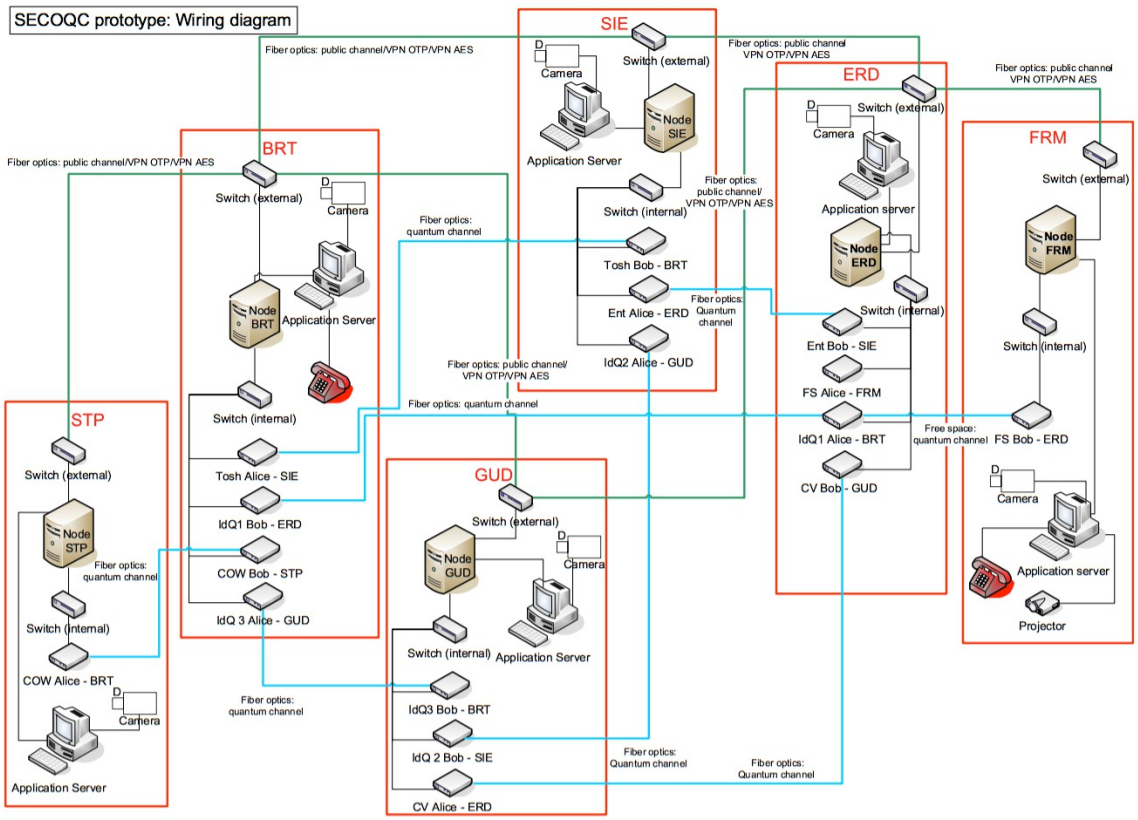


Figure 4: Diagrama técnico de conexión de la red. Las líneas azules son canales cuánticos, las verdes son canales clásicos y las negras son canales internos en cada nodo.

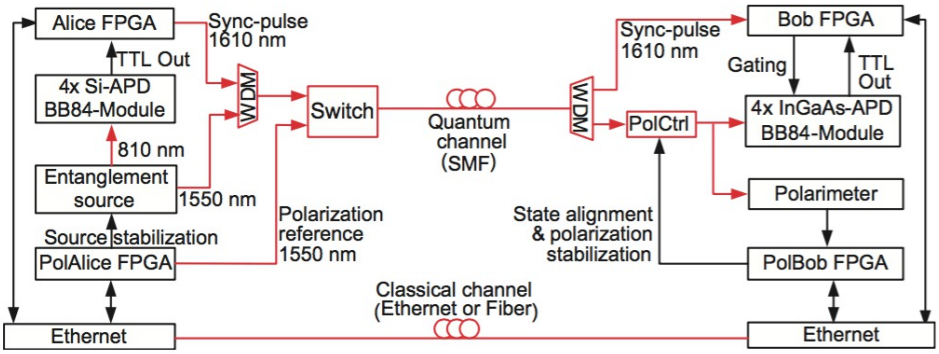


Figure 5: Conectividad entre dos nodos adyacentes.

simples en nano-alambres (SNSPD: *superconducting nanowire single-photon detectors*), aquí se utilizó pulsos débiles de láser coherente (WCP: *weak coherent laser pulses*) y detectores basados en diodos en avalancha con retroalimentación negativa de arseniuro de indio y galio y de fosfuro de indio (materiales semiconductores de indio, galio, arsénico y fósforo) (InGaAs/InP NFAD: *negative feedback avalanche diodes*), con lo que la red presentada permite separaciones de hasta 307 kms entre cualesquiera dos de sus participantes. Una descripción completa de los detectores utilizados aparece en [11].

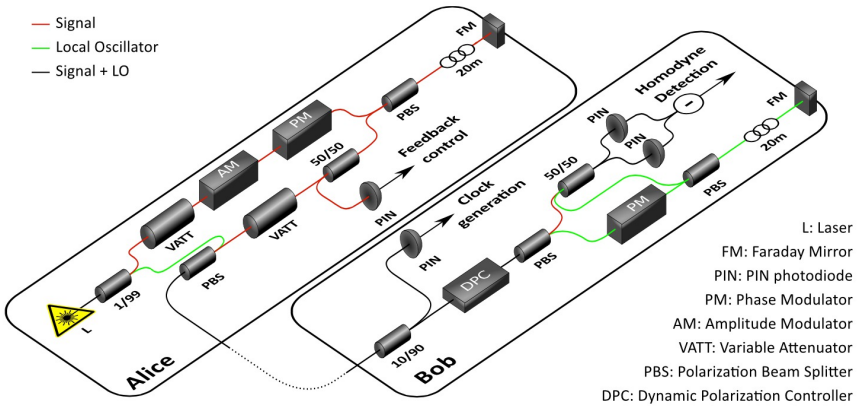


Figure 6: Conectividad entre dos nodos adyacentes en el esquema CVQKD (la imagen proviene de [5]).

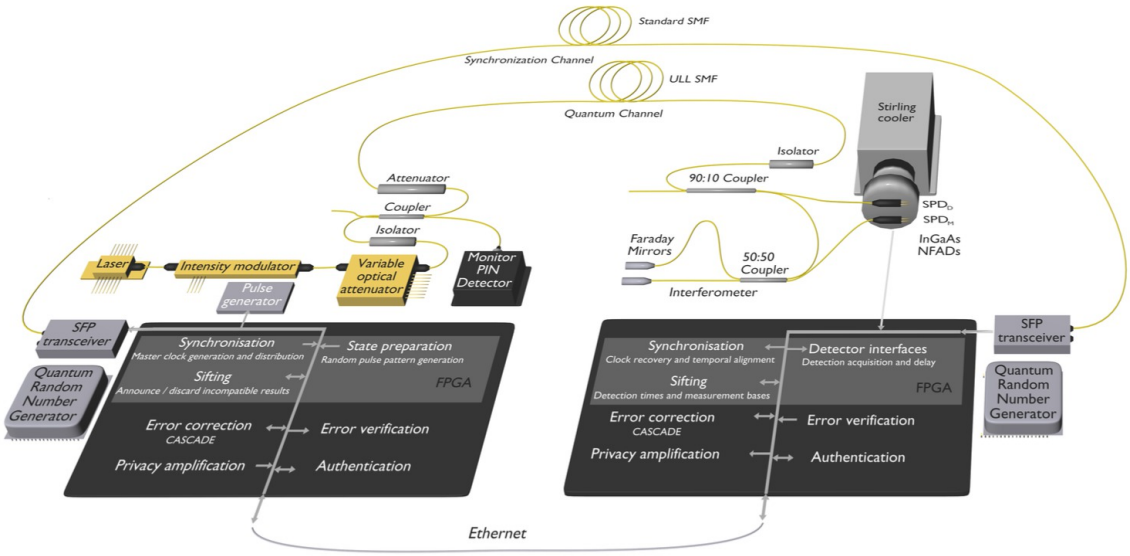


Figure 7: Conectividad entre dos nodos adyacentes en el esquema en Ginebra (la imagen proviene de [6]).

La conexión entre dos participantes se bosqueja en la Figura 7.

En [6] los autores presentan un análisis probabilista sobre la seguridad, la corrección y la confiabilidad de la red construída.

7 QKD satelital

Los protocolos anteriores utilizan canales cuánticos hechos de fibra de vidrio para el transporte de fotones o láseres, de donde resultan las limitaciones en las distancias entre los participantes. También las comunicaciones de tipo cuántico al aire libre están limitadas por la introducción de ruido proveniente de muy diversos orígenes.

En [10] se presenta un experimento de una primera comunicación cuántica entre una estación terrena, el observatorio de Matera en Italia, y un satélite orbitando la Tierra.

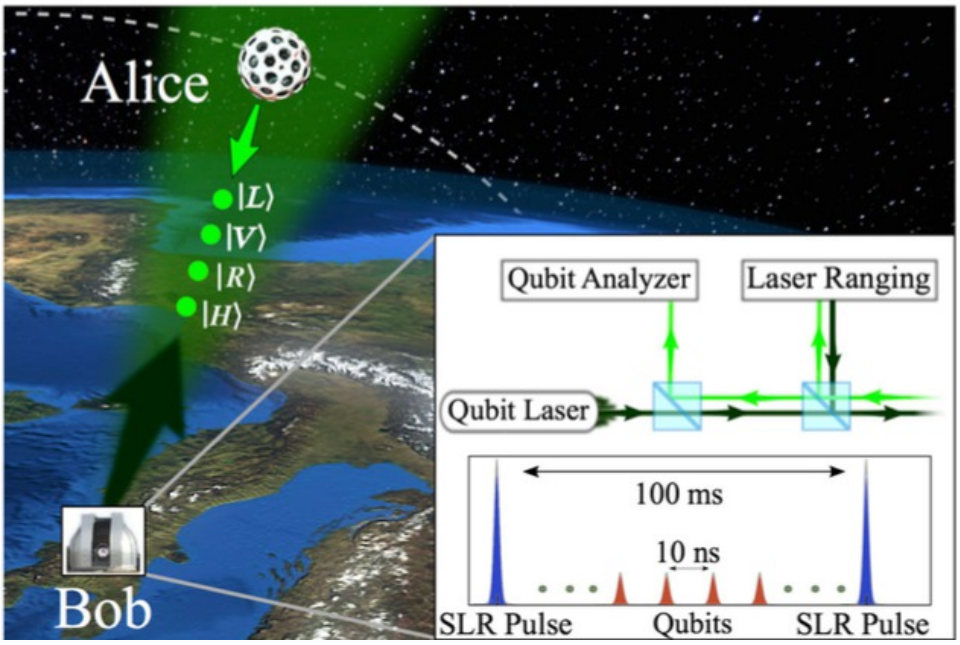


Figure 8: Conectividad entre la estación terrestre y el satétlite (la imagen proviene de [10]).

Se implementa un protocolo de QKD basado en polarizaciones que no utiliza entrelazamiento alguno. Mediante pulsos de fotones generados por láseres, que realizan tanto la base canónica como la base de Hadamard en el espacio de los qubits, el satétilte refleja los fotones sin afectar la polarización cuando ésta está en una do los estados básicos, pero hay un quinto estado de polarización que no se preserva. Esto permite la implementación plena de QKD. La sincronización de señales es, por supuesto, un elemento esencial en esta implementación.

Se envía pulsos, a manera de qubits, con una tasa de repetición de 100 MHz y son reflejados por el satélite. La sincronización se realiza mediante pulsos en frecuencias de radio de resonancia magnética (MRI: *magnetic resonance imaging radio frequency*) utilizando el algoritmo de Shinnar-Le Roux (SLR). Véase la Figura 8.

Una meta actual de ese mismo grupo de trabajo, es la de realizar procesos de entrelazamiento. Se está abriendo así una gran posibilidad para telecomunicaciones cuánticas seguras en un plazo corto.

Referencias

[1] A. J. Shields A. W. Sharpe L. Salvail S. Robyr G. Ribordy E. Querasser A. Poppe J. B. Page S. Nauerth L. Monat O. Maurhardt M. Suda C. Tamas T. Themel H. Zbinden Z. L. Yuan I. Wimberger H. Weinfurter H. Weier N. Walenta F. Vannel R. Tualle-Brouri P. Trinkler A. Treiber Y. Thoma R. T. Thew T. Matyus A. Marhold M. Fuerst S. Fossier S. Fasel J. F. Dynes M. Dianati E. Diamanti T. Debuisschert W. Boxleitner J. Bouda C. Barreiro R. Alléaume C. Pacher J. D. Gautier O. Gay N. Gisin N. Lütkenhaus T. Lorünser J. Lodewyck R. Lieger M. Legré T. Laenger G. Humer H. Hübel M. Hentschel Y. Hasani A. Happe P. Grangier M. Peev A. Zeilinger, D. Stucki. The SECOQC quantum key distribution network in Vienna. 11:075001, 2009.

[2] Charles H. Bennett, Gilles Brassard, and N. David Mermin. Quantum cryptography without Bell's theorem. *Phys. Rev. Lett.*, 68:557–559, Feb 1992.

[3] Nicolas Gisin. Quantum information processing, 2015. `http://docbox.etsi.org/Workshop/2014/201410_CRYPTO/S01_Setting_the_Scene/S01_Gisin.pdf`.

[4] Frédéric Grosshans and Philippe Grangier. Continuous variable quantum cryptography using coherent states. *Phys. Rev. Lett.*, 88:057902, Jan 2002.

[5] Paul Jouguet, Sébastien Kunz-Jacques, Anthony Leverrier, Philippe Grangier, and Eleni Diamanti. Experimental demonstration of continuous-variable quantum key distribution over 80 km of standard telecom fiber. In *CLEO: 2013*, page QTu2C.4. Optical Society of America, 2013.

[6] Boris Korzh, Charles Ci Wen Lim, Raphael Houlmann, Nicolas Gisin, Ming Jun Li, Daniel Nolan, Bruno Sanguinetti, Rob Thew, and Hugo Zbinden. Provably secure and practical quantum key distribution over 307?km of optical fibre. *Nature Photonics*, 9:163?168, February 2015.

[7] M. Lucamarini, K. A. Patel, J. F. Dynes, B. Fröhlich, A. W. Sharpe, A. R. Dixon, Z. L. Yuan, R. V. Penty, and A. J. Shields. Efficient decoy-state quantum key distribution with quantified security. *Opt. Express*, 21(21):24550–24565, Oct 2013.

[8] Valerio Scarani, Antonio Acín, Grégoire Ribordy, and Nicolas Gisin. Quantum cryptography protocols robust against photon number splitting attacks for weak laser pulse implementations. *Phys. Rev. Lett.*, 92:057901, Feb 2004.

[9] D. Stucki, N. Brunner, N. Gisin, V. Scarani, and H. Zbinden. Fast and simple one-way quantum key distribution. *Applied Physics Letters*, 87(19):194108, 2005.

[10] Giuseppe Vallone, Davide Bacco, Daniele Dequal, Simone Gaiarin, Vincenza Luceri, Giuseppe Bianco, and Paolo Villoresi. Experimental satellite quantum communications. *Phys. Rev. Lett.*, 115:040502, Jul 2015.

[11] Nino Walenta, Tommaso Lunghi, Olivier Guinnard, Raphael Houlmann, Hugo Zbinden, and Nicolas Gisin. Sine gating detector with simple filtering for low-noise infra-red single photon detection at room temperature. *Journal of Applied Physics*, 112(6):063106, 2012.

[12] Juan Yin, Yuan Cao, Shu-Bin Liu, Ge-Sheng Pan, Jin-Hong Wang, Tao Yang, Zhong-Ping Zhang, Fu-Min Yang, Yu-Ao Chen, Cheng-Zhi Peng, and Jian-Wei Pan. Experimental quasi-single-photon transmission from satellite to Earth. *Opt. Express*, 21(17):20032–20040, Aug 2013.

[13] Juan Yin, Ji-Gang Ren, He Lu, Yuan Cao, Hai-Lin Yong, Yu-Ping Wu, Chang Liu, Sheng-Kai Liao, Fei Zhou, Yan Jiang, Xin-Dong Cai, Ping Xu, Ge-Sheng Pan, Jian-Jun Jia, Yong-Mei Huang, Hao Yin, Jian-Yu Wang, Yu-Ao Chen, Cheng-Zhi Peng, and Jian-Wei Pan. Quantum teleportation and entanglement distribution over 100-kilometre free-space channels. *Nature*, 488(7410):185–188, 08 2012.