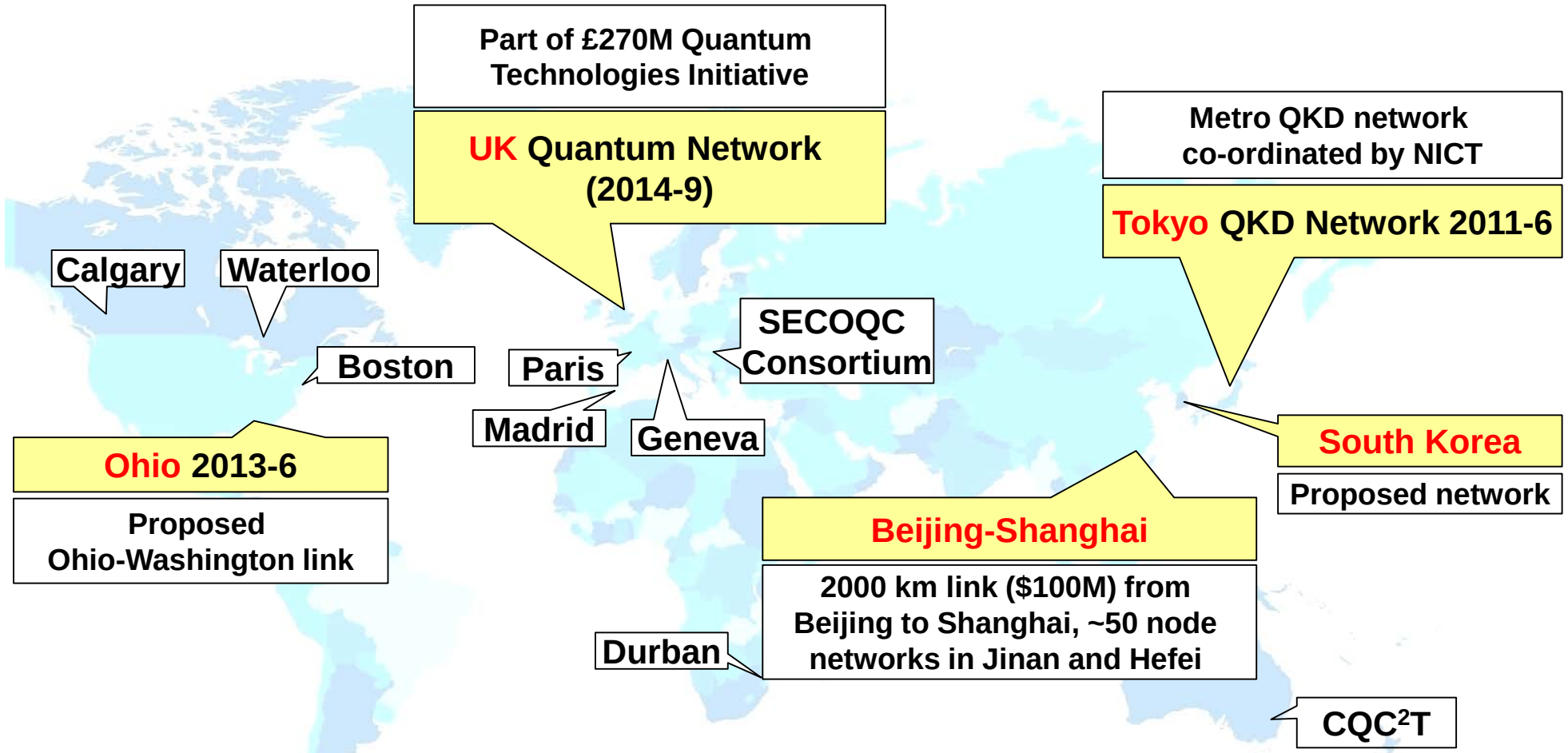
INDUSTRIAL STANDARDS FOR QUANTUM COMMUNICATIONS

Andrew Shields (Toshiba Research Europe Ltd)

Industry Specification Group in Quantum Key Distribution

Global Deployments of Quantum Key Distribution



- Pilot deployments are taking place
  - it is meaningful to define requirements and industrial standards now

Industrial Standards

Industrial Standards are essential for …

- Interoperability of systems from different manufacturers
- Integration into conventional telecom networks
- Stimulate application development on common interfaces
- Stimulate a component supply chain for Quantum Technologies
- Security assurance
  - Ensure that QKD is implemented securely

ETSI Industry Specification Group in QKD

- ISG-QKD established in 2008
- Published Group Standardisation Documents on QKD Use Cases, Application Interfaces, Security Proofs, QKD Module specification, Ontology, Components and Internal Interfaces
- Membership comprises large industry, telecom operators, SMEs, NMIs, government labs, universities
- New members are welcome

Current Work Items of ETSI ISG

- Deployment parameters
  - User requirements for implementing QKD
  - Defining a common language between supplier and user
- Quantum component specification
  - Parameters and test procedures for quantum components
  - Impact on system security
- Implementation security
  - Ensure that implementations are secure and robust against attack

Implementation Security

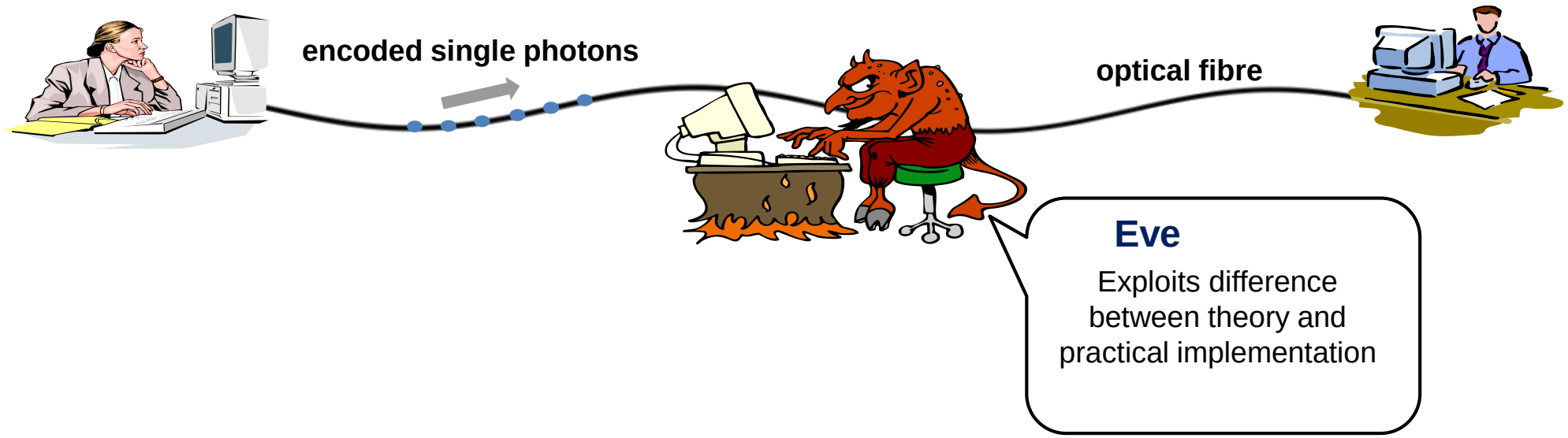
Objective: Investigate and close security loopholes of real QKD systems

Motivation

- Small deviations between ideal and real system could be exploited by Eve.
- Passive or active attacks may provide Eve information while she remains unnoticed.

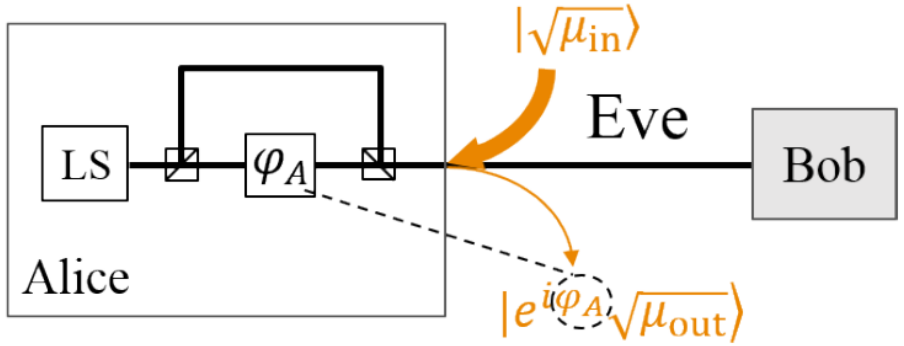
Approach

- Catalogue known attacks
- Introduce appropriate countermeasures
- Modify the QKD protocol if necessary



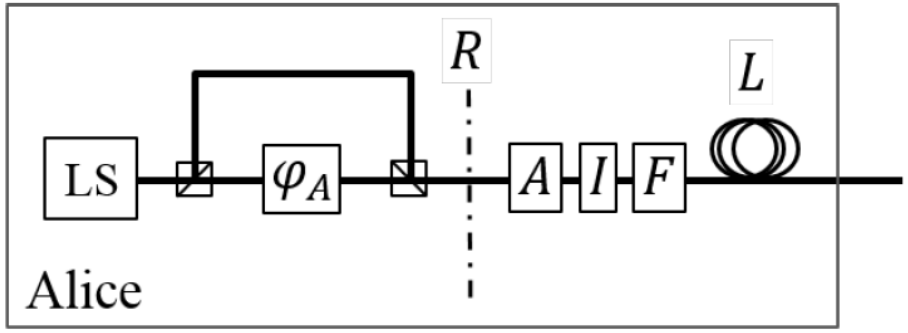
Example: Trojan Horse Attack

Trojan Horse Attack

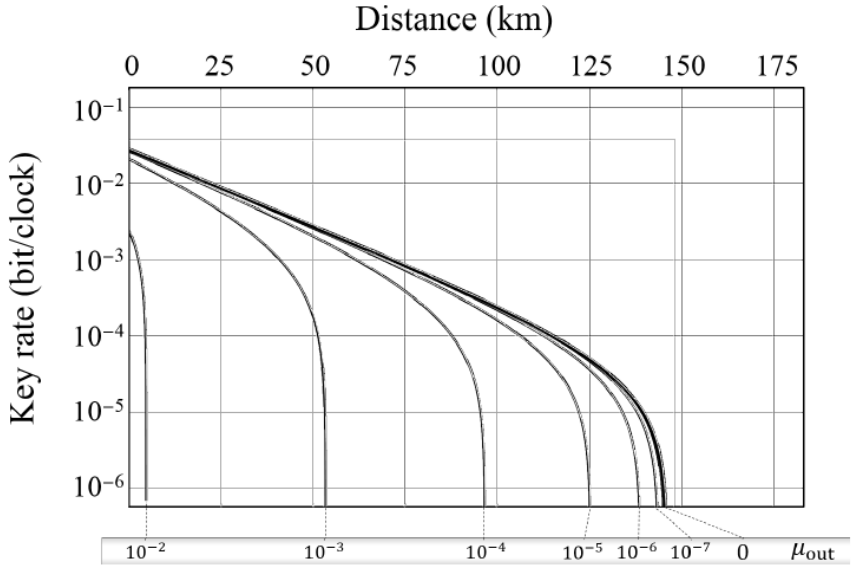


- Eve injects bright light into Alice and measures weak backreflections
- Eve might determine info about Alice's settings without causing disturbance!!

Shutting out the Trojan Horse with Passive Components



- Eve's max intensity limited by fibre fuse effect (< 10W)
- Reduce back-reflection using attenuators (A), optical isolators (I) and bandpass filters (F)
- For μ_{out}<10^{-6}, typically need isolation ~170 dB



- Remove remaining info using privacy amplification
- For μ_{out}<10^{-6}, key rate hardly affected

Lucamarini et al, Phys Rev X 5, 031030 (2015)

Summary

- Several large **QKD network deployments** underway worldwide
- Standards are essential … for **future interoperability**
- To assure customers that technology **implemented securely**
- And to **stimulate markets for components, systems and applications**

Thank you!

Contact: andrew.shields@crl.toshiba.co.uk