



FPGAs AND HARDWARE-BASED SECURITY — COMPONENT UP TO SYSTEM LEVEL ASPECTS

Alberto Moreno Herrera

ESCCON, 2023-03-09

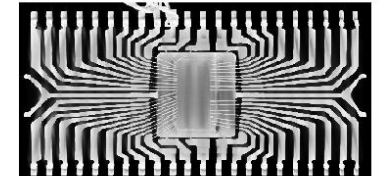
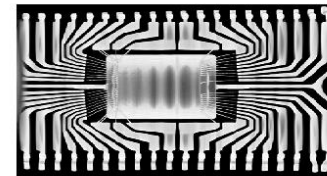
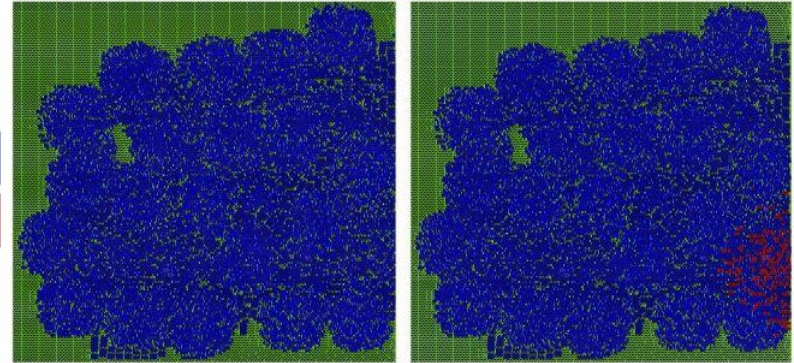
INTRODUCTION

Two old examples

- » Backdoor in ProASIC3
 - » S. Skorobogatov et al. Proceedings of the International Conference on Cryptographic Hardware and Embedded Systems (2012)
- » Trojan Insertion via ECO (Engineering Change Order) – see right
 - » T. Perez et al. IEEE International Symposium on Circuits and Systems (2021)
- » Israel jets bomb a Syrian nuclear site in 2007
 - » S. Adee. IEEE Spectr. 55 (2016)
- » What are security assaults looking for?
 - » Theft of foreign property (for reproduction)
 - » Take-over of foreign property (for own use or blackmailing)
 - » Destruction of foreign property (sabotage)
 - » Gaining access to confidential information (espionage)
 - » Etc.

Target
Circuit

Hardware
Trojan



Ahi, Kiarash et al. SPIE Sensing Technology+ Applications (2015)

INTRODUCTION

The reason for this presentation

- » Operation Skeleton Key – [CyCraft report](#)
 - » At least 7 Taiwanese chip firms from 2018 to 2020
 - » Hackers from mainland China compromised VPNs to gain access
 - » The malware was planted using the penetration testing tool Cobalt Strike
 - » Skeleton keys were injected into domain controllers using the common hacking tools Dumpert and Mimikatz
 - » Main goal was stealing documents about IC chips: software development kits (SDKs), IC designs, source code, etc.



- » NDAA Section 224 (December 2019) required the Secretary of Defense (SECDEF) to establish security standards no later than January 1, 2021. By January 1, 2023, nearly all microelectronics products and wireless network services purchased by the DOD must meet these new security standards.

» Documents:

» Levels of Assurance Definitions and Applications (July 2022)

» 3 Levels of Assurance




» Threat Catalog (December 2022)

» Best practices per LoA for:

» FPGAs: Field Programmable Gate Array

» CIC: Custom Integrated Circuits

» COTS: Commercial Off The Shelf

Level of assurance	Typical criteria
	<p>If the system fails, U.S. Government (USG) capability will be reduced in a meaningful way. If the system is subverted, it can cause harm to U.S. personnel, property, or interests. However:</p> <ul style="list-style-type: none"> • Essential operational capabilities for the DoD will remain available even during a system failure.
	<p>If the system fails, the consequences will be grave. If the system is subverted, it can cause serious harm to U.S. personnel, property, or interests. However:</p> <ul style="list-style-type: none"> • Essential operational capabilities for the DoD may be degraded during a system failure, and • Redundant capabilities can be brought online as part of a continuity of operations plan, and • The failure of the system will not cause cascade effects across many DoD or allied systems.
	<p>If the system fails, the consequences will be extremely grave. If the system is subverted, it can cause exceptionally grave harm to U.S. personnel, property, or interests. A failure or subversion of this system:</p> <ul style="list-style-type: none"> • May represent an existential risk to the USG, and • May cascade across many DoD systems in a way that impacts total operational readiness in an immediate way, and • Will interrupt essential operational capabilities of the DoD.

» NSA [documents on protecting DoD Microelectronic for FPGAs](#) (December 2022):

FOUR REPORTS TO HELP SECURE DEPARTMENT OF DEFENSE MICROELECTRONICS

NSA released the following Cybersecurity Technical Reports today to help programs protect microelectronics during development.

1



Field Programmable Gate Array (FPGA) Overall Assurance Process

Outlines the process used to develop threat categories and mitigations.

2



Field Programmable Gate Array Best Practices — Threat Catalog

Describes the high-level threat categories that relate to FPGA devices at each Level of Assurance.

3



Field Programmable Gate Array Level of Assurance 1 Best Practices

Provides mitigations for each relevant FPGA threat category at Level of Assurance 1.

4



Third-Party IP Review Process for Level of Assurance 1

Details a methodology for performing an engineering review of third-party intellectual property that is included in an FPGA design for Trojan detection.



Visit [NSA.gov/cybersecurity-guidance](https://www.nsa.gov/cybersecurity-guidance) to read all four of the Cybersecurity Technical Reports on protecting microelectronics.

» Design Process

- » Apply robust NIST approved cybersecurity processes to development environments.
- » Perform regular design and code reviews with multiple people involved at each step.
- » Perform robust testing with complete requirements coverage and high code coverage.
- » Use a reproducible build process to generate FPGA bitstreams/configurations.
- » Apply asymmetric authentication algorithms to all configuration files before system start. Manage the private keys using an HSM.

» Design IP and Tools

- » Obtain design software from reputable sources. Validate before installation that its hash is as expected.
- » Select third-party IP carefully, and do not accept encrypted or obfuscated IP blocks. Either notify JFAC about its use or evaluate it for suitability through a security audit.

» Parts Acquisition and Assembly

- » Acquire parts through reputable channels. Validate parts' authenticity either cryptographically or physically.
- » Assemble the system in a controlled way, or validate afterwards that it was assembled correctly. Ensure that the correct configuration and keys are installed.

» Reporting

- » Assist JFAC by providing high-level information about the program's FPGA usage.
- » Contact JFAC if there is suspicion of technical interference by an adversary.

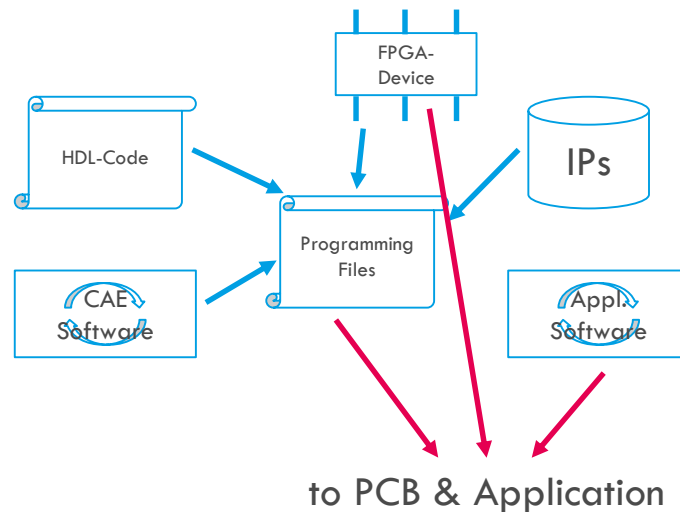
- » The functional FPGA is composed of:
 - » The device itself
 - » The implemented HDL code
 - » additional IP cores (possibly encrypted)
 - » Software running on the device internal processing systems
 - » Software to implement the design
- » The result is the device itself and one or more software files

- » **Design Process**

- » Apply robust NIST approved cybersecurity processes to development environments.
 - » FPGA design development only with dedicated and cleared personnel
 - » Tools and code to be controlled
 - » Perform regular design and code reviews with multiple people involved at each step.
 - » Perform robust testing with complete requirements coverage and high code coverage.
 - » Use a reproducible build process to generate FPGA bitstreams/configurations.
 - » Apply asymmetric authentication algorithms to all configuration files before system start. Manage the private keys using an HSM.

- » **Design IP and Tools**

- » Obtain design software from reputable sources. Validate before installation that its hash is as expected.
 - » Select third-party IP carefully, and do not accept encrypted or obfuscated IP blocks. Either notify JFAC about its use or evaluate it for suitability through a security audit.



- » modify / exchange device → rather unlikely
- » steal programming file
 - for reverse engineering
 - for copy purposes → unlikely for low volume equipment
 - for extracting confidential information, like keys
- » modify programming file → for adding backdoors, virus or functional modification
- » modify application software → similar to programming file actions, but depending on software format possibly easier to detect

Therefore: the Programming File and application software need to be protected against unintended use and modification.

» Storage options:

» One-time programmable FPGAs:

- » Readout of programming file not possible

» Flash-based programmable FPGAs:

- » Programming file is stored on the FPGA and can be protected against readout (Microchip)
- » For reprogramming or refreshing the flash, the programming file needs to be stored either „on-board“ or to be uploaded during flight

» SRAM-based FPGAS:

- » The FPGAs need to be programmed with every power cycle. Therefore the programming file is stored „on-board“ with the option to exchange the programming file for functional updates.
- » Radiation hardening approaches scrub the on-chip SRAMs, perform error correction procedures and, if necessary, reload the configuration from the external memory.

» Updates:

- » Secure exchange of bitstreams
- » Authentication and signature of files
- » Encryption of transfer and signature check
- » Upload only via secure channels and protection upfront for unauthorized uploads

» Bitstream encryption

- » Microchip applies encryption with AES-2 symmetric keys using either unique device factory setting keys or user provided keys (e.g. for Polarfire).
- » Xilinx uses an on-chip AES-GCM 256 bit decryption and authentication logic, using dedicated ports for authentication and without a readout-option for the on-device stored keys. (e.g. Ultrascale+)
- » NanoXplore allows secure programming with SHA-256 BootLoader authentication and bitstream encryption using AES-128
- » Lattice uses ECDSA bitstream authentication, coupled with robust AES-256 encryption

» Disclaimer from Microchip's [RTG4 technical brief](#):

- Microchip values and aggressively protects its intellectual property rights. Attempts to breach the code protection features of Microchip product is strictly prohibited and may violate the Digital Millennium Copyright Act.
- Neither Microchip nor any other semiconductor manufacturer can guarantee the security of its code. Code protection does not mean that we are guaranteeing the product is "unbreakable". Code protection is constantly evolving. Microchip is committed to continuously improving the code protection features of our products.

PARTS ACQUISITION AND ASSEMBLY

Guidelines



- » **Acquire parts through reputable channels. Validate parts' authenticity either cryptographically or physically.**
 - » Increased risk for COTS / NewSpace
 - » IRIS² and LEO PNT follow NewSpace approach
- » **Assemble the system in a controlled way, or validate afterwards that it was assembled correctly. Ensure that the correct configuration and keys are installed.**
 - » Parts handling, storage and manufacturing needs to happen in a controlled environment
 - » Controlled environments are to be equipped with physical access control and other measures pending on level of security
 - » Some countries may insist on local manufacturing



» Cases:

» Satellite to Earth

» Jamming, eavesdropping, hijacking, spoofing, etc.

» Within the satellite

» Satellite to satellite

» Separate user and TMTC data without leaks

» COMSEC – Communications Security

» Physical security

» Cryptographic security

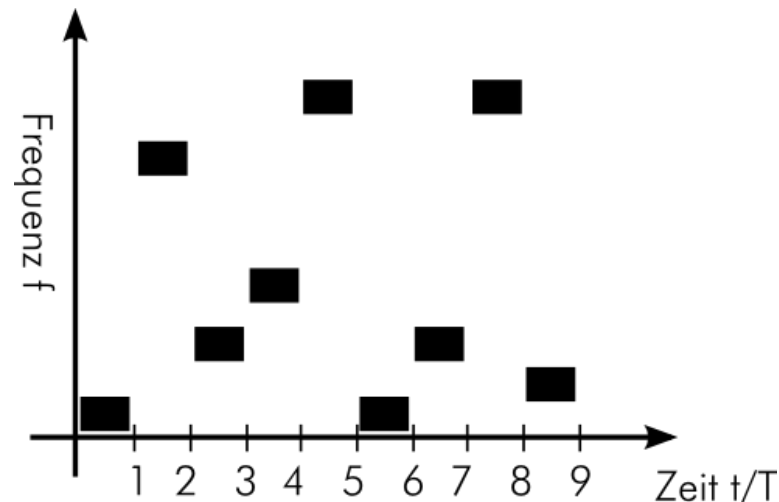
» EMSEC – Emission Security

» TRANSEC – Transmission Security

» Frequency hopping

» Spread spectrum

» TSK - Transmission Security Key



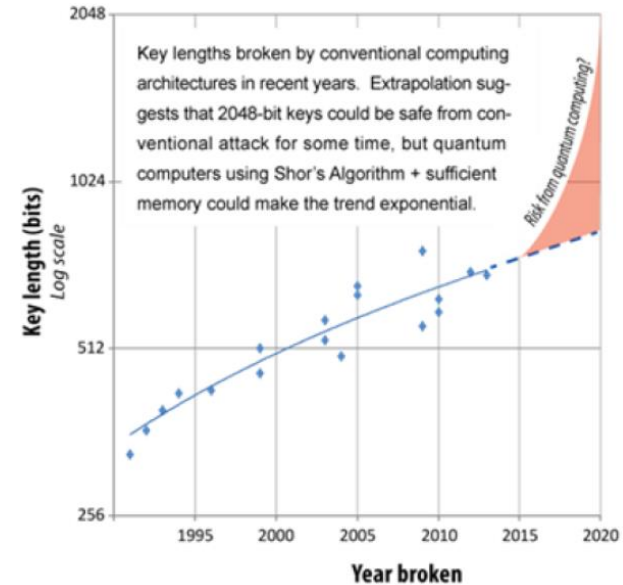
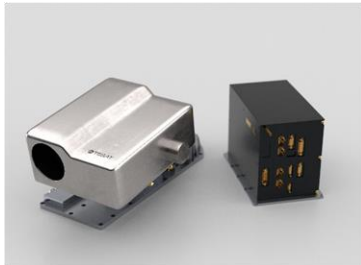
SYSTEM LEVEL

QKD (Quantum Key Distribution)

- » Development of Quantum Computers is progressing
- » **The question is not „IF“ but „WHEN“ QCs become a threat**

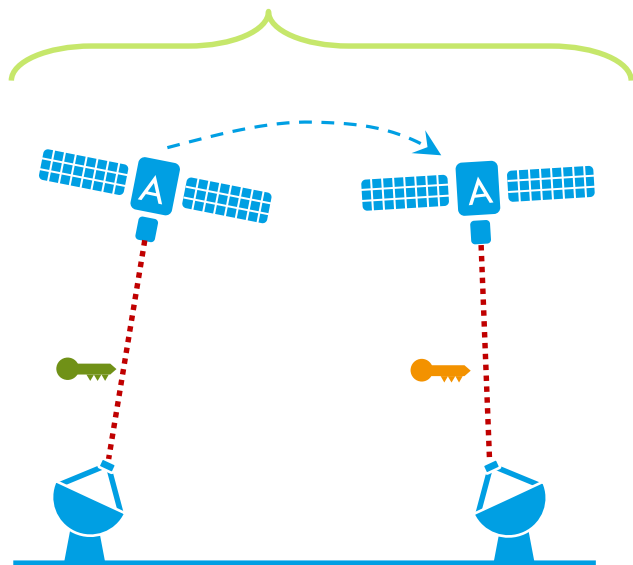
➡ Quantum Key Distribution

- » No cloning theorem (no redundancy)
 - » Able to identify eavesdropping
 - » Limits the range
 - » Secure key-rates are strongly reduced by losses on the quantum channel
 - » Typical attenuation in single-mode optical fibers (@1550nm): 0.2 dB/km
 - » Losses of optical satellite links typically an order of magnitude smaller

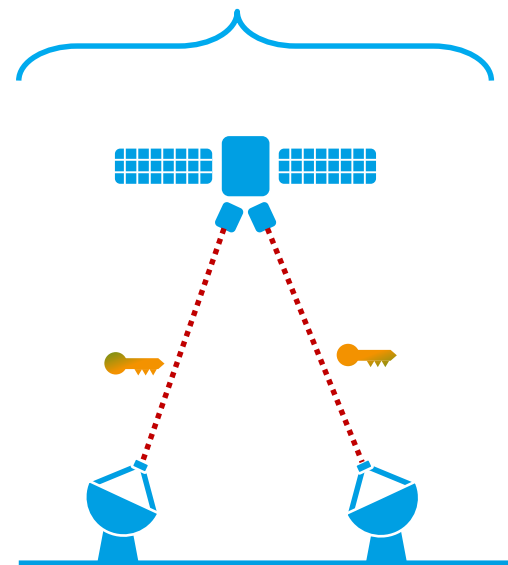


Breaks of the RSA cryptosystem in recent years using conventional computation (ETSI white paper 8, June 2015)

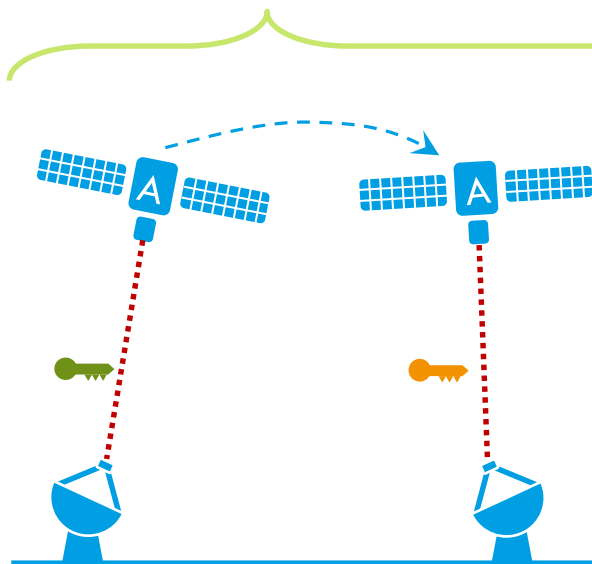
prepare and measure



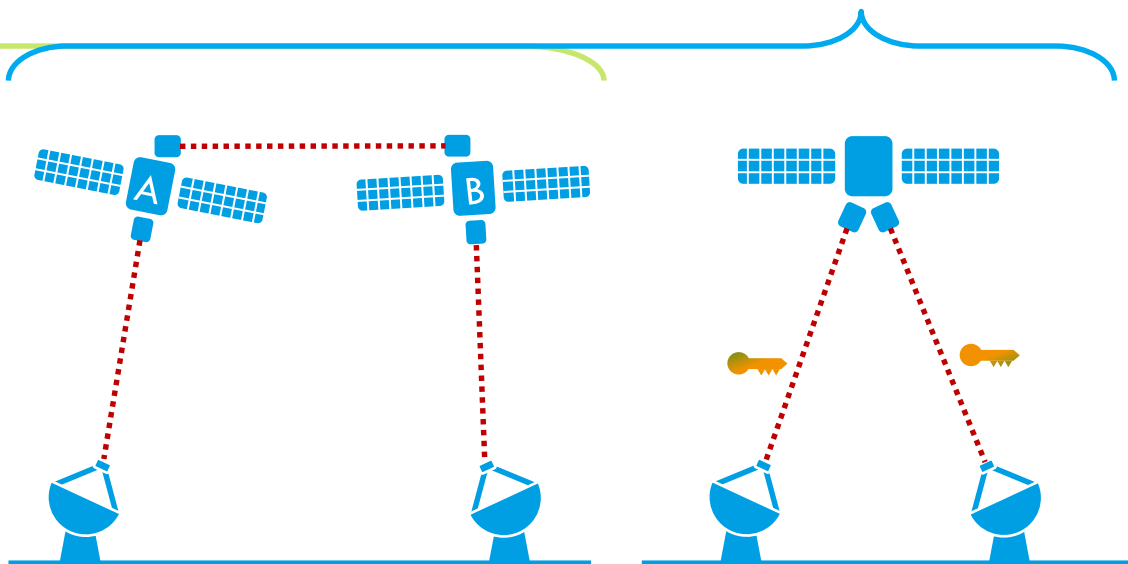
entanglement based



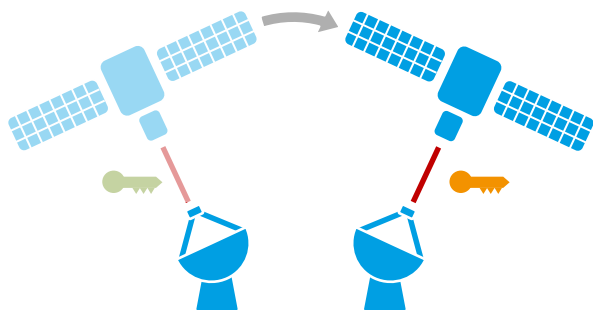
prepare and measure



entanglement based

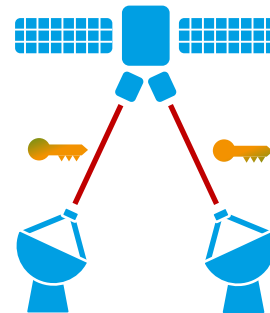


Prepare & measure



- Key rates:
- » ~ kbps (Micius, QUESS)
Liao, S.-K. et al.; Nature 549: 43–47 (2017)
 - » ~ kbps (Socrates)
Carrasco-Casado, A. et al.; Proc. SPIE 10660, QISSC X: 106600B (2018)
 - » ~ 100 kbps range (Tiangong-2)
Y. Li et al.; Optica 9: 933 (2022)

Entanglement-based

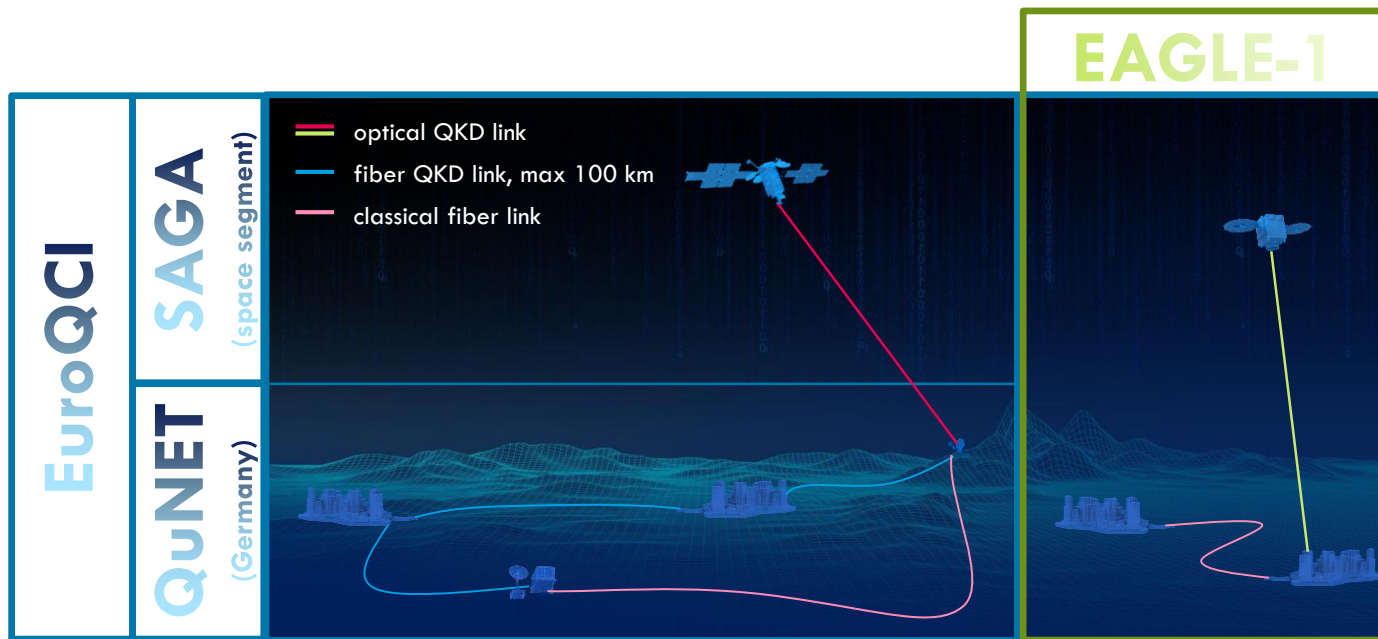


- Key rates:
- » ~ 0.1 bps (Micius 2016, QUESS)
Yin, J. et al.; Nature 582: 501–505 (2020)

In-orbit demonstration of entanglement sources:

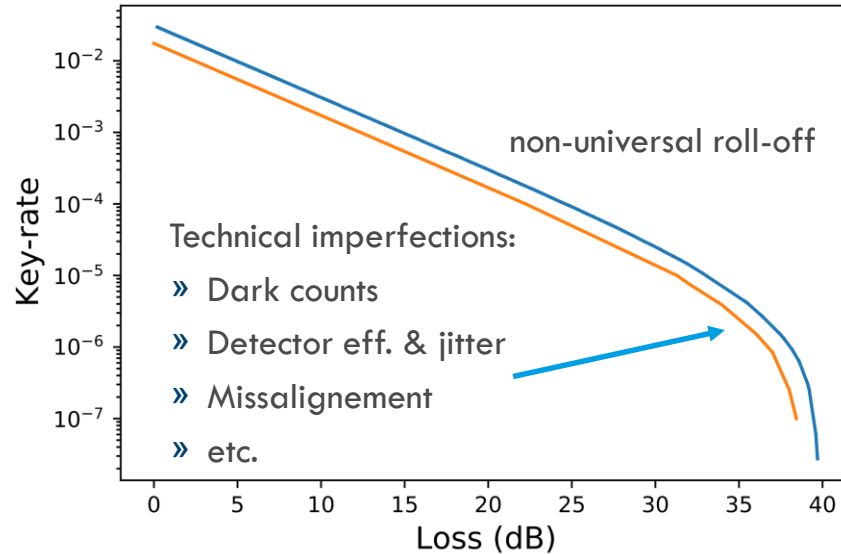
- » Galassia
Tang, Z. et al.; Phys. Rev. App. 5: 054022 (2016)
- » SpooQy-1
Villar, A. et al.; Optica 7: 734 (2020)

Many more scientific missions currently in planning/construction phase



- » EuroQCI (European Quantum Communication Infrastructure): EC initiative, aims to build a secure quantum communication infrastructure spanning the entire EU
 - » SAGA constitutes the space segment with the goal to implement satellite based QKD
 - » national QCI initiatives (Germany QuNET), supposed to implement terrestrial, fibre based QKD
- » EAGLE-1 is contributing mission to SAGA

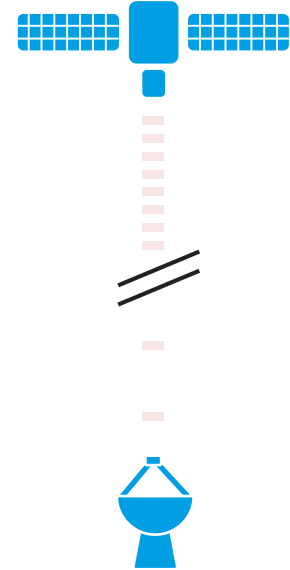
BB84 + Decoy Protocols: Asymptotic secure key-rate



Blue: Attema, T., et al.; Quantum Inf Process 20: 154 (2021)

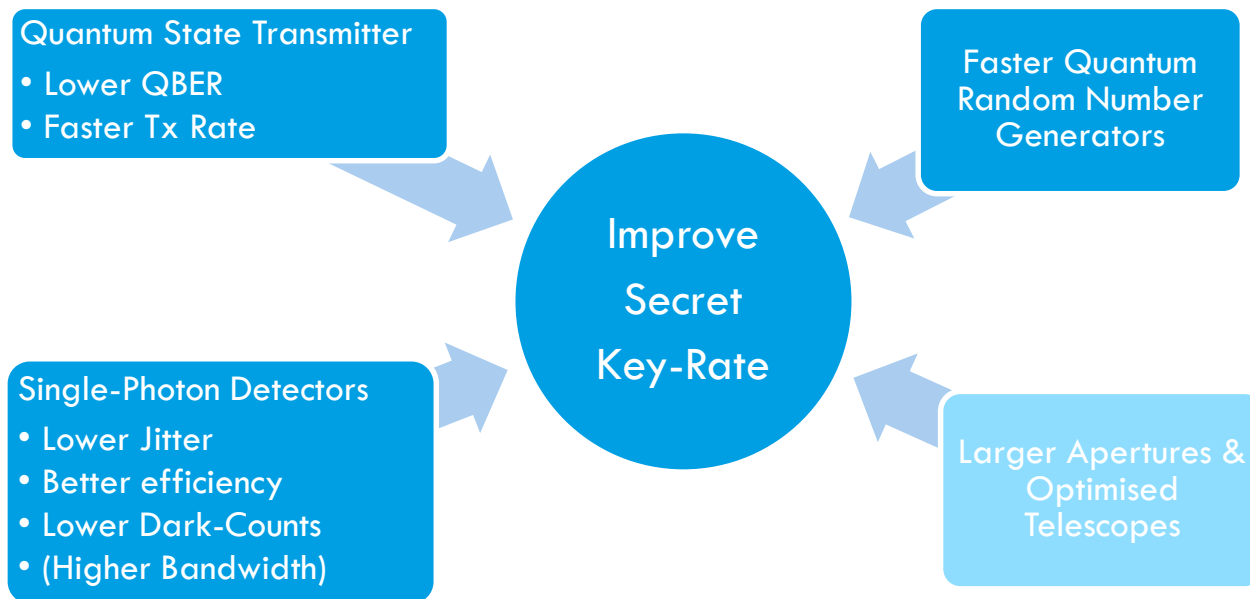
Orange: Lim, C.C.W. et al.; Phys. Rev. A 89: 022307 (2014)

QKD



Emission in the single photon regime
 \rightarrow few photons reach receiver

In principle, only quantitative improvements are required → increase key-rates





THANK YOU FOR YOUR ATTENTION

Acknowledgements:

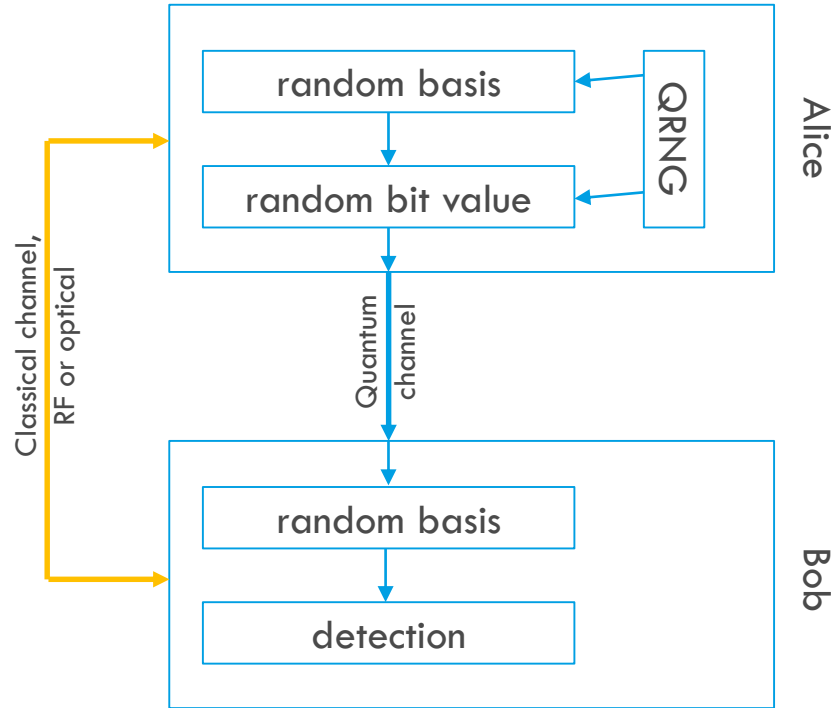
Matthias Düll, Volker Lück, Daniela Staerk, Fabian Reichert, Julian Struck

» Alberto Moreno Herrera
» alberto.moreno-herrera@tesat.de
» +49 151 1849 0562

Tesat-Spacecom GmbH & Co. KG
Gerberstraße 49
71522 Backnang
www.tesat.de

QKD P/M

Example: Polarisation encoding



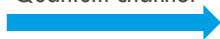
Basis		Bit value
1	2	
horizontal	diagonal	0
vertical	antidiagonal	1



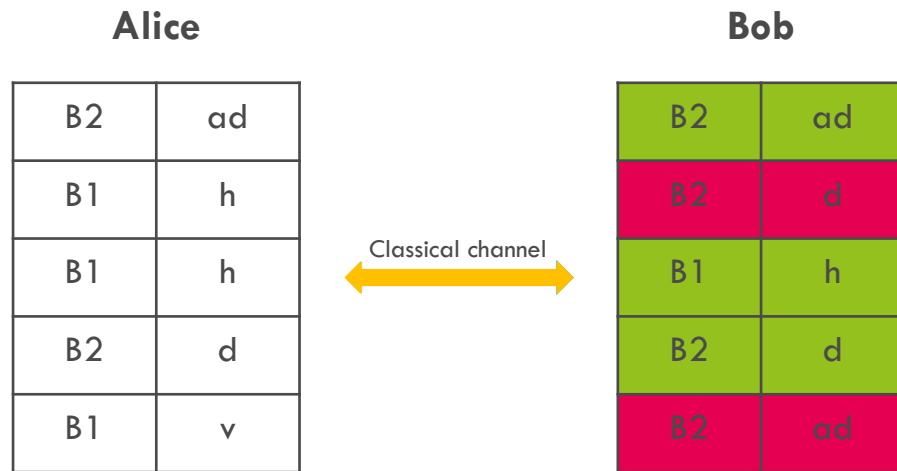
Alice

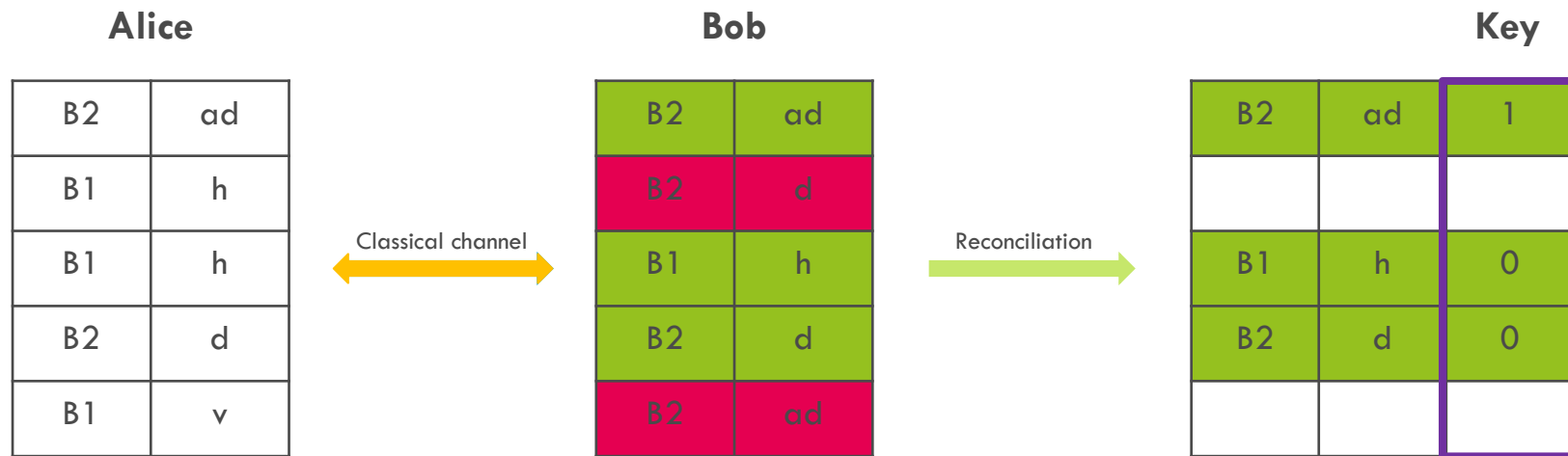
B2	ad
B1	h
B1	h
B2	d
B1	v

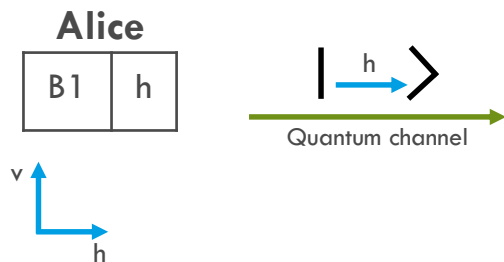
Quantum channel

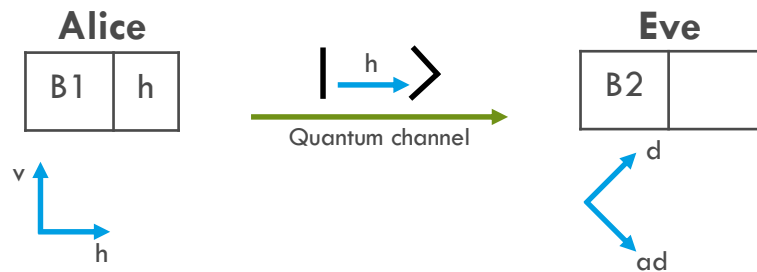
**Bob**

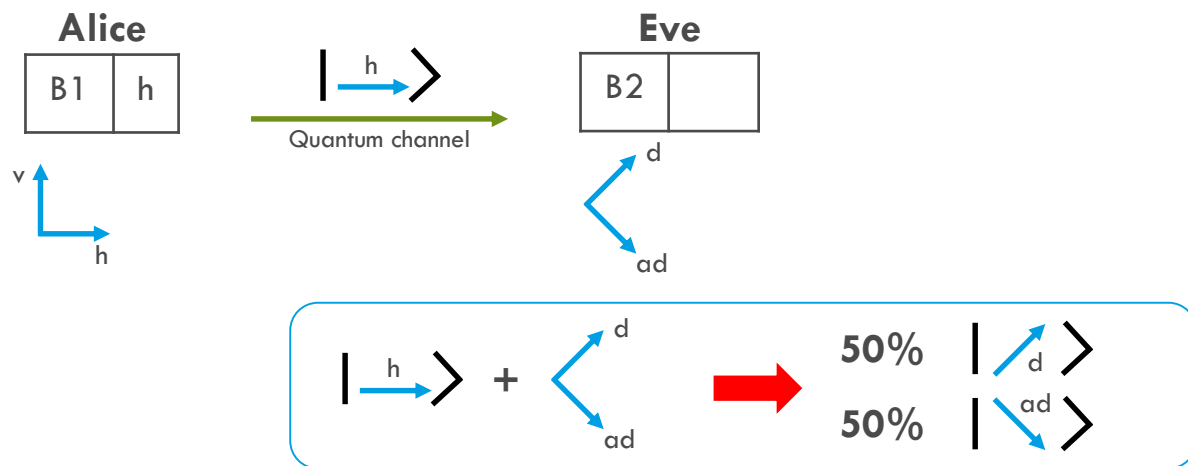
B2	ad
B2	d
B1	h
B2	d
B2	ad

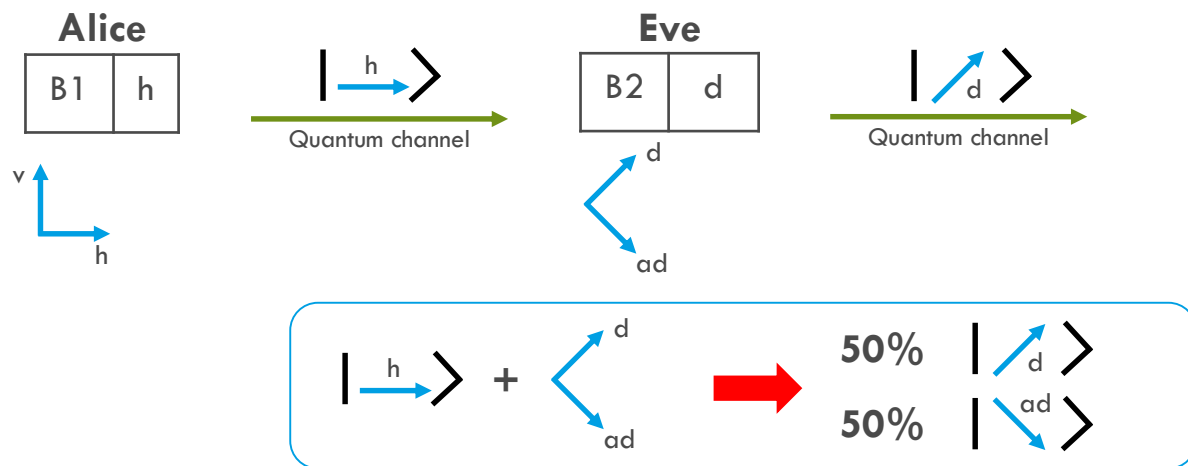


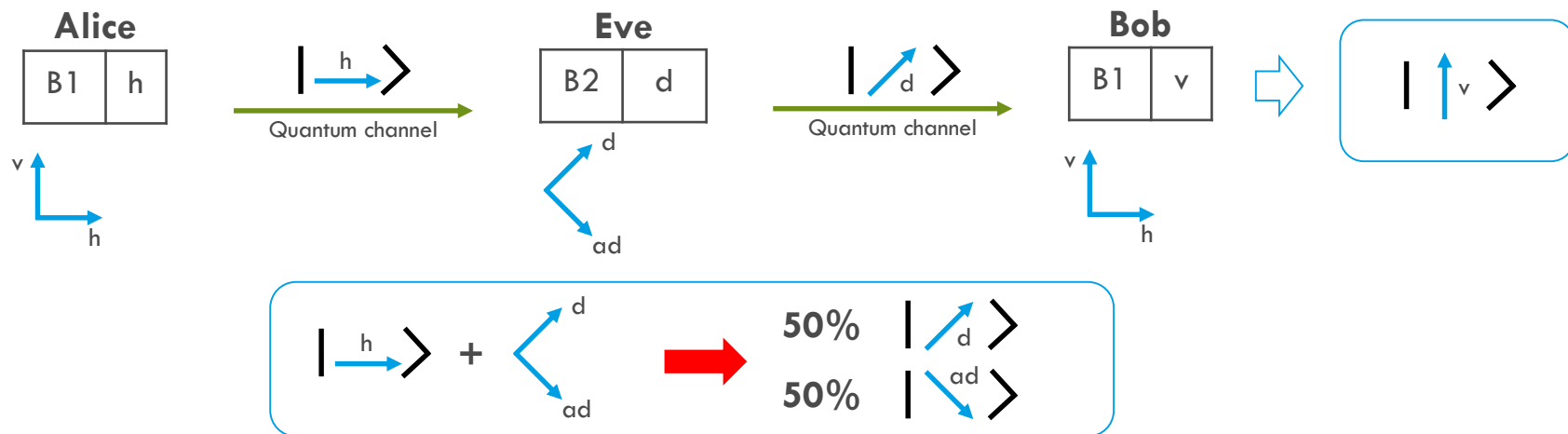


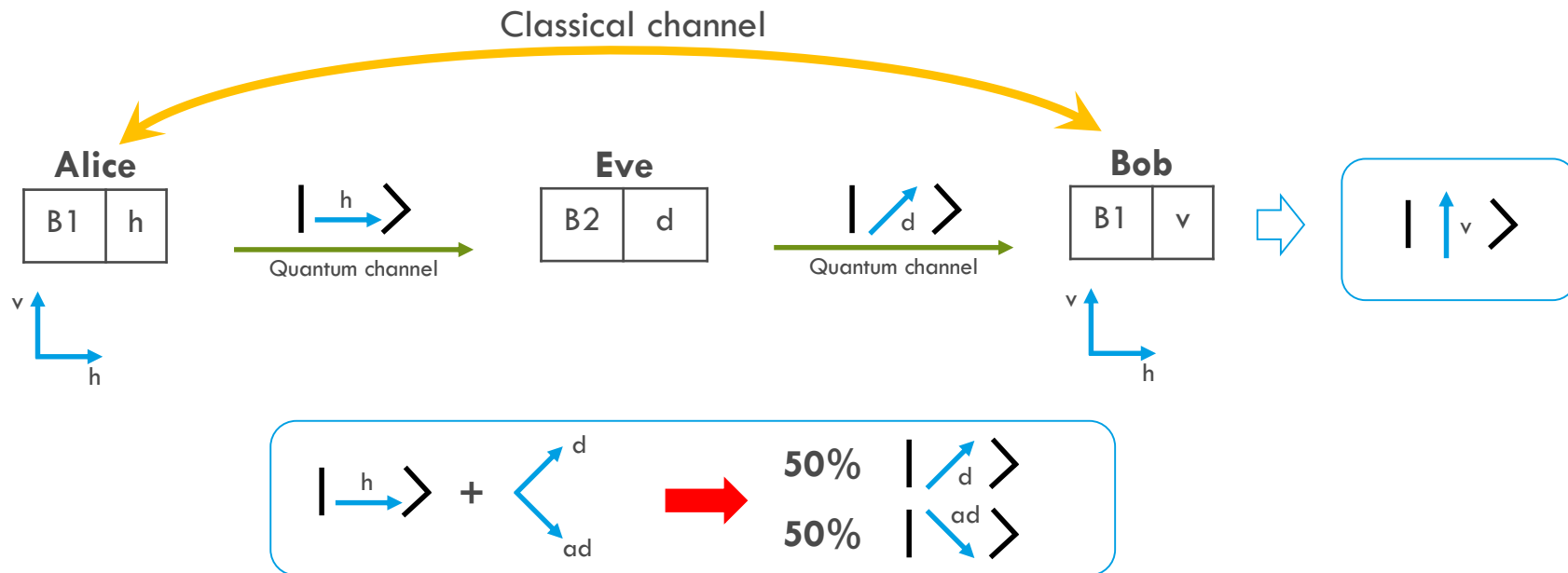






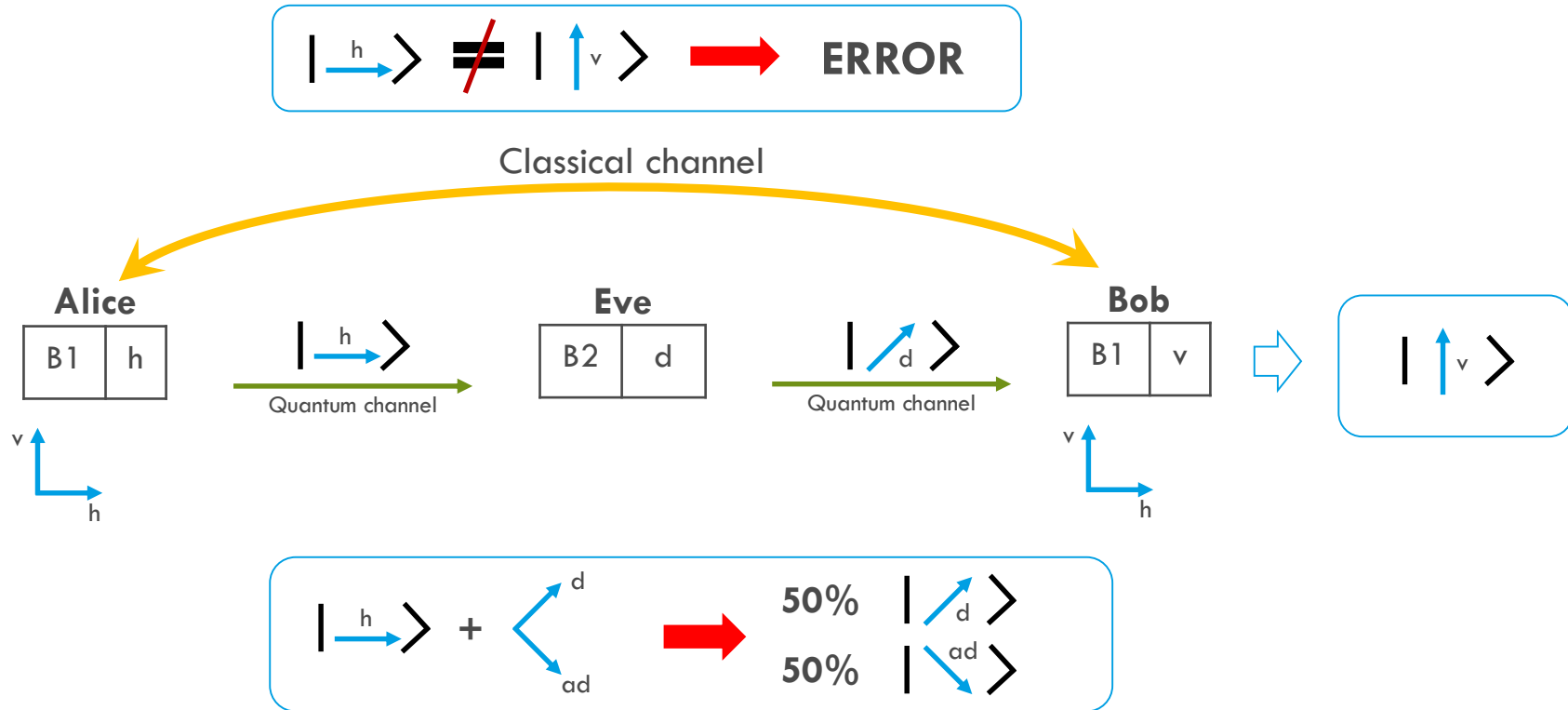






QKD P/M

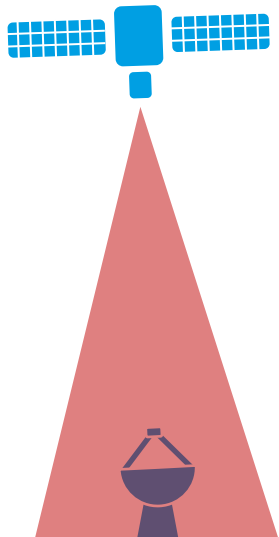
Example: Polarisation encoding





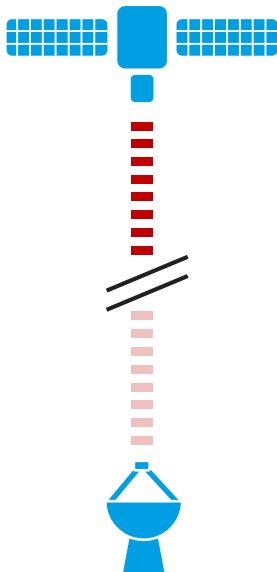
		Eve	
Choice of basis		Correct	Incorrect
Bob {	Correct	100%	50%
	Incorrect	0%	0%

- Man-in-the-middle adds 25% penalty on **Quantum Bit Error Rate**
- Eve's presence will be detected due to QBER exceeding threshold value
→ key material will be discarded



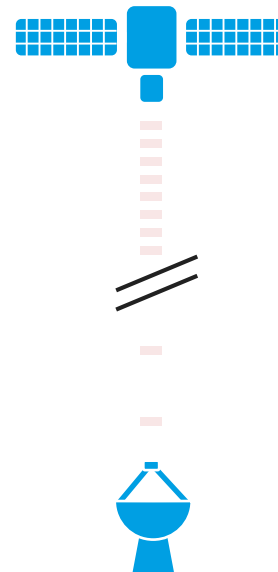
Link losses
(LEO-Ground):
~ 30 to 60 dB
dominated by beam
expansion

Classical laser coms



Losses can be compensated by laser
power → Negligible information loss

QKD



Emission in the single photon regime
→ few photons reach receiver