First Light Imaging Group

Quantum Key Distribution in space

September 2023

Isaure de Kernier
isaure.dekernier@first-light.fr

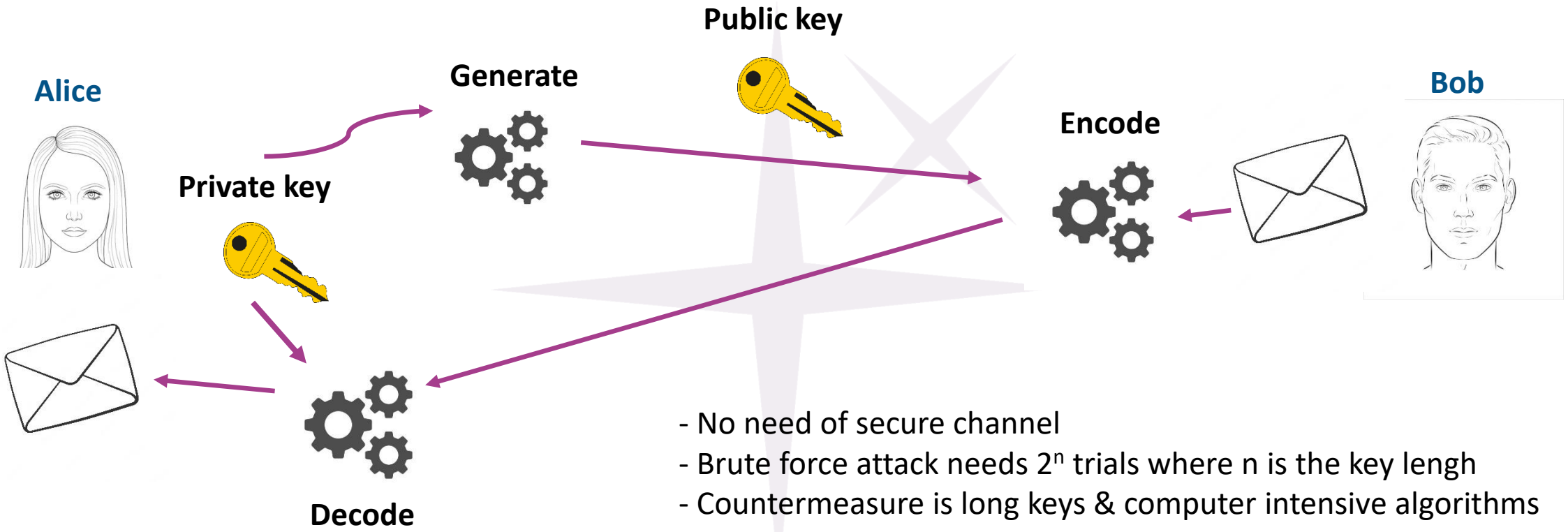
Jean-Luc Gach
jeanluc.gach@first-light.fr

First Light Imaging

- Fast low noise cameras in the UV/visible/SWIR
- Ultra performance cameras (photon counting)
- Custom / OEM

Cryptography at a glance

Assymetric crypto (ex: RSA)

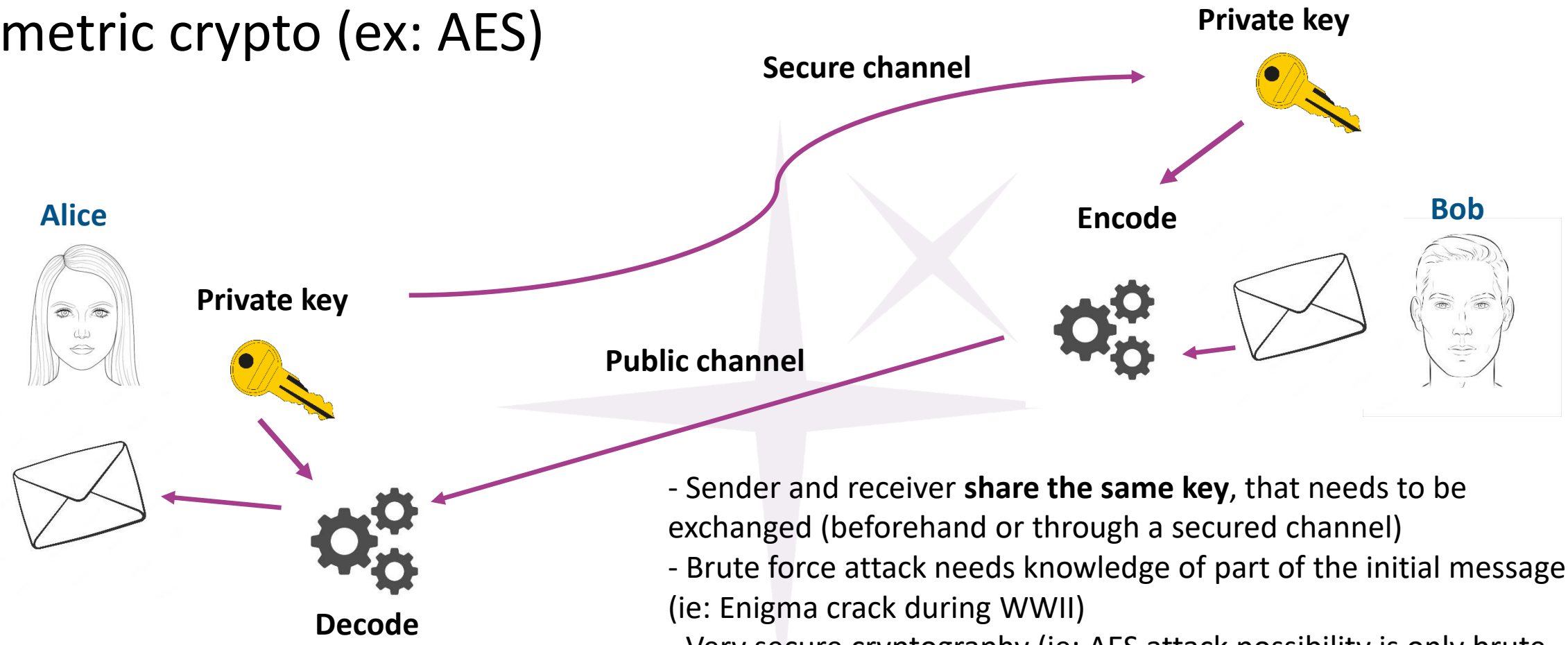


- No need of secure channel
- Brute force attack needs 2^n trials where n is the key lengh
- Countermeasure is long keys & computer intensive algorithms

➢ **Inefficient with quantum computers**

Cryptography at a glance

Symetric crypto (ex: AES)

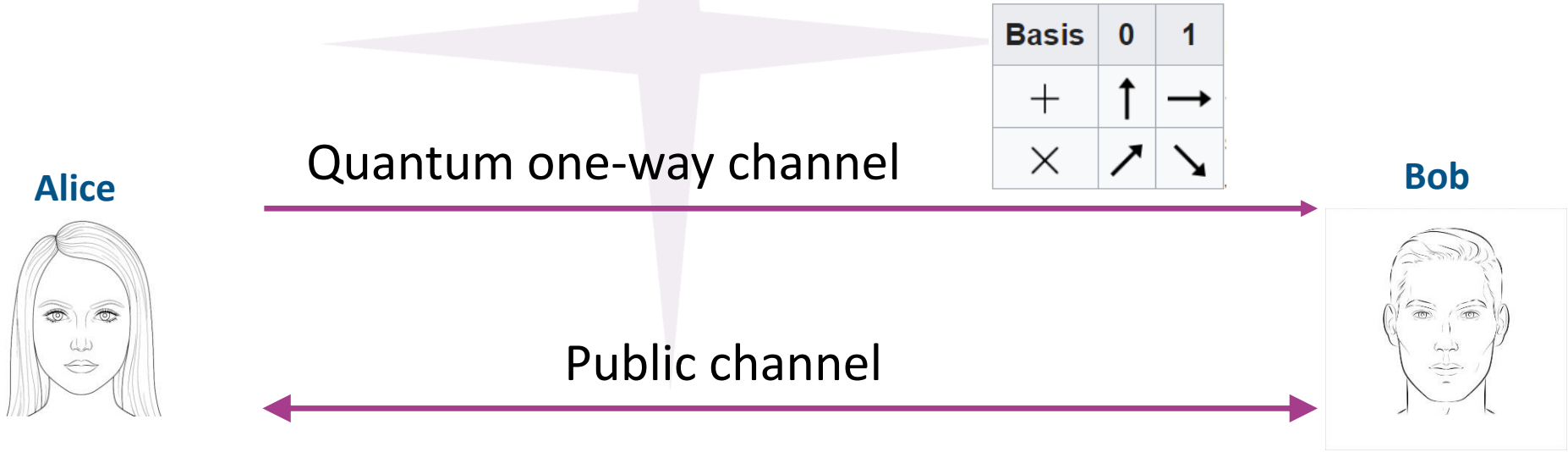


- Sender and receiver **share the same key**, that needs to be exchanged (beforehand or through a secured channel)
- Brute force attack needs knowledge of part of the initial message (ie: Enigma crack during WWII)
- Very secure cryptography (ie: AES attack possibility is only brute force)

➢ **Weakness is the key exchange**

Quantum key distribution

- Quantum = single photon transmission on one channel.
- Any attack needs to intercept and re-emit the photon. Quantum properties permits to detect any attack
- Example : BB84 protocol
  - Use of polarization to encode data on 2 bases
  - **Existing COTS components**



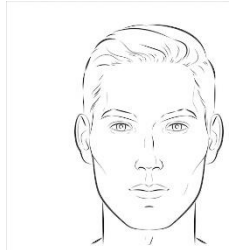
Quantum key distribution (BB84)

Alice

Alice's random bit	0	1	1	0	1	0	0	1
Alice's random sending basis	+	+	×	+	×	×	×	+
Photon polarization Alice sends	↑	→	↘	↑	↘	↗	↗	→
Bob's random measuring basis	+	×	×	×	+	×	+	+
Photon polarization Bob measures	↑	↗	↘	↗	→	↗	→	→
Shared secret key	0		1			0		1

1 Encode data with random basis & send on quantum channel

Bob



3 Exchange basis sequence Via unsecured channel

2 Measure polarization with Bob's random basis

4 Select bits of matched basis = final encryption key

If the measuring basis is wrong, the measured result is random (quantum indeterminacy)

QKD attack

Alice

1 Encode data with random basis & send on quantum channel

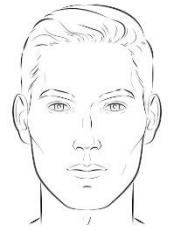
Alice's random bit	0	1	1	0	1	0	0	1
Alice's random sending basis	+	+	×	+	×	×	×	+
Photon polarization Alice sends	↑	→	↘	↑	↘	↗	↗	→
Eve's random measuring basis	+	×	+	+	×	+	×	+
Polarization Eve measures and sends	↑	↗	→	↑	↘	→	↗	→
Bob's random measuring basis	+	×	×	×	+	×	+	+
Photon polarization Bob measures	↑	↗	↗	↘	→	↗	↑	→
Shared secret key	0		0			0		1
Errors in key	✓		✗			✓		✓

2 **Eve**

Eve intercepts the quantum channel, measure and retransmits it but she does not know yet the transmission basis

3 Measure retransmitted signal polarization with Bob's random basis

Bob



4 Exchange basis sequence Via unsecured channel

5 Select bits of matched basis = final encryption key

6 Compare part of the key and detect errors, then discard the revealed part of the key

QKD attack detection

- Eve has 50% chance to choose the right base, and if not, Bob has 50% chance to make an error during the photon polarization measurement. The total error probability per intercepted bit is then 25%

- The probability to detect an attack depends then on the number of bits used to secure the link, it is :

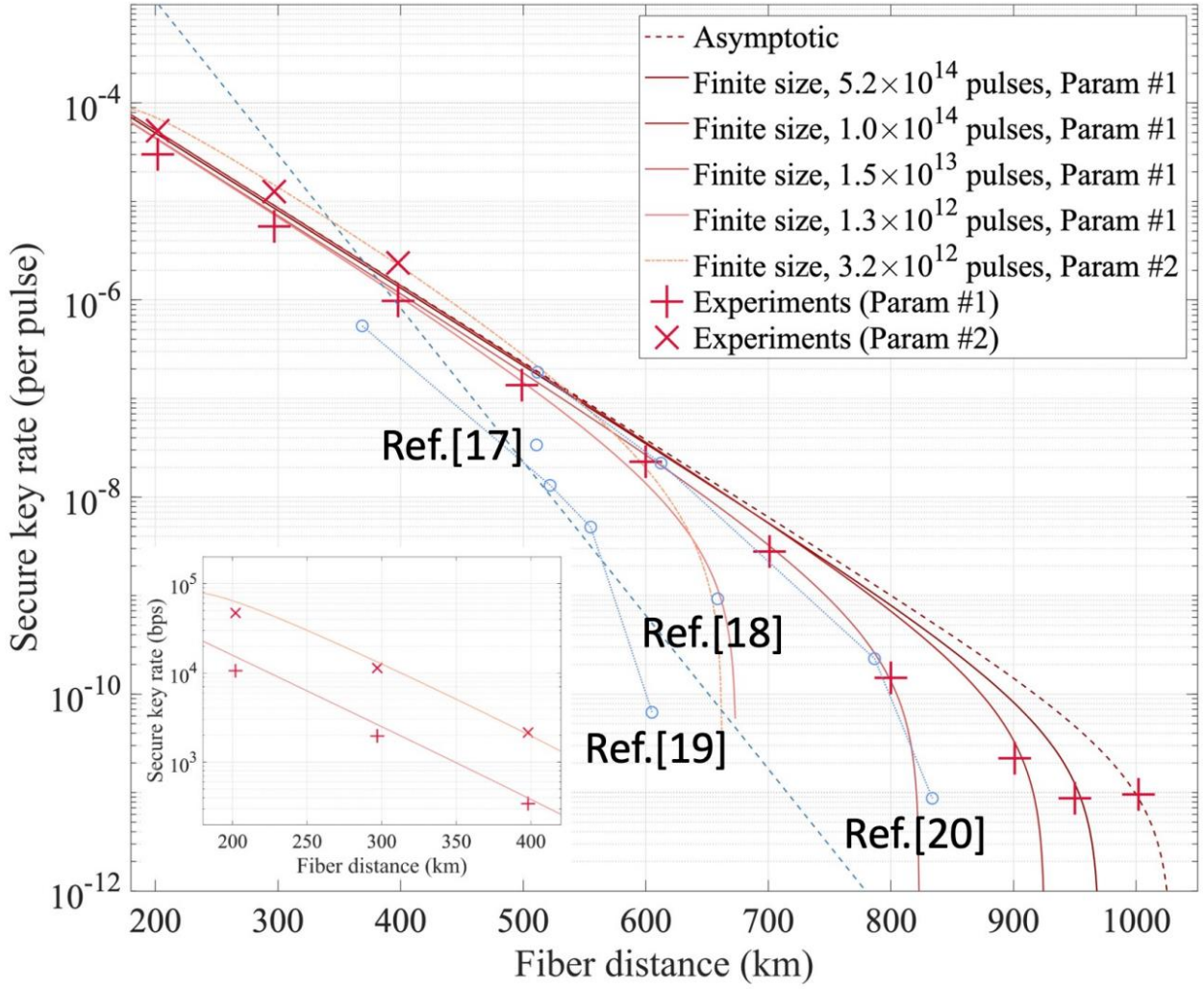
$$P_d = 1 - \left(\frac{3}{4}\right)^n$$

- With n=72 this gives 1 ppb to fail in detecting an attack

QKD limits

- QKD uses weak photon sources. With the poissonian probability, most of the emitted pulses contains no photons. Efficiency is low.
- Channel attenuation lowers the efficiency
- Std repeaters are inefficient and is a weakness
- Quantum amplifiers/repeaters not yet exist

➢ **QKD over long distances is very challenging**



QKD over fiber from Yang Liu et al. (Phys. Rev. Lett. **130**, 210801 – Published 25 May 2023)

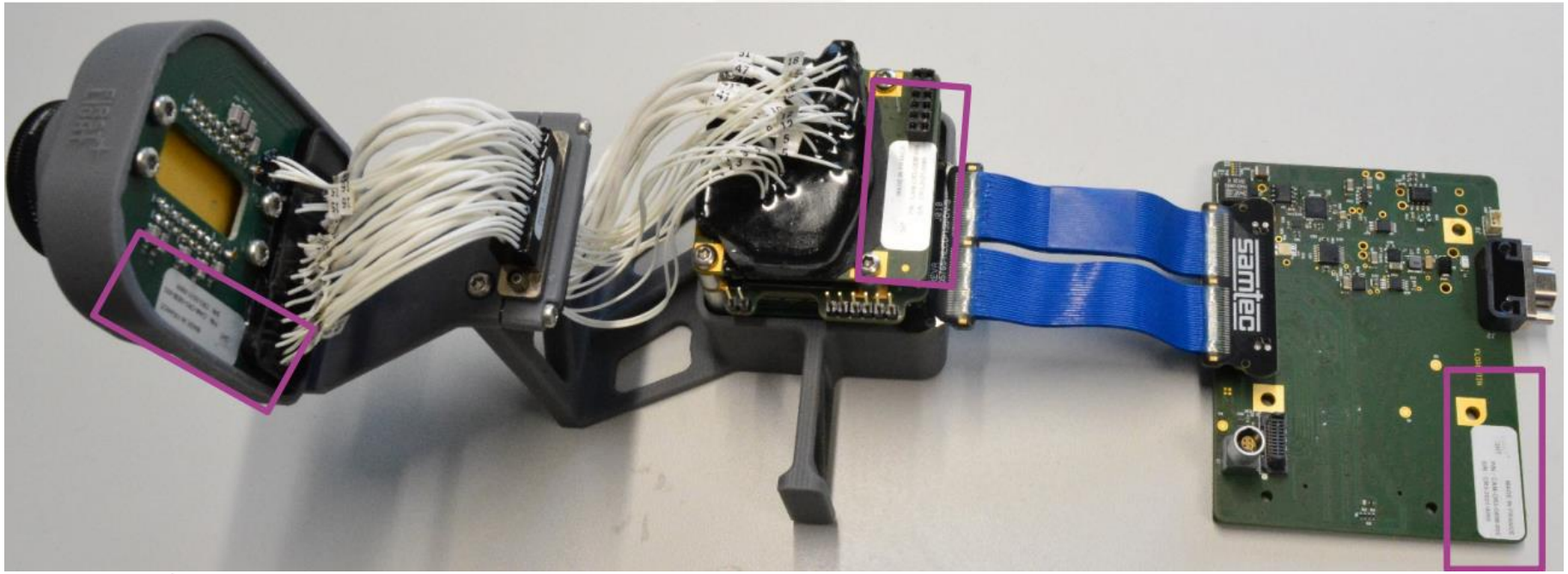
QKD over FSO in space

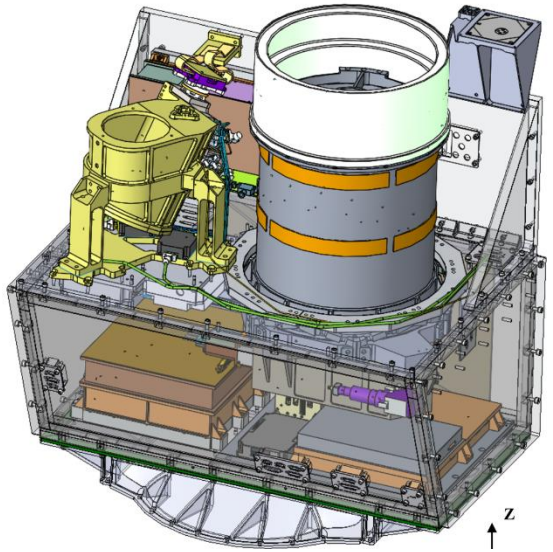
- Transmission of the key to a satellite (LEO or GEO)
- Transmission loss is lower
- High security
- All the FSO tools can be used (steering cameras, adaptive optics)

QKD over FSO in space

C-RED 3 camera for QEYSSAT (Quantum EncrYption and Science Satellite (QEYSSat) mission (Honeywell – CSA)

See: QEYSSAT: a mission proposal for a quantum receiver in space, T. Jennewein et al, SPIE 89970A (2014)

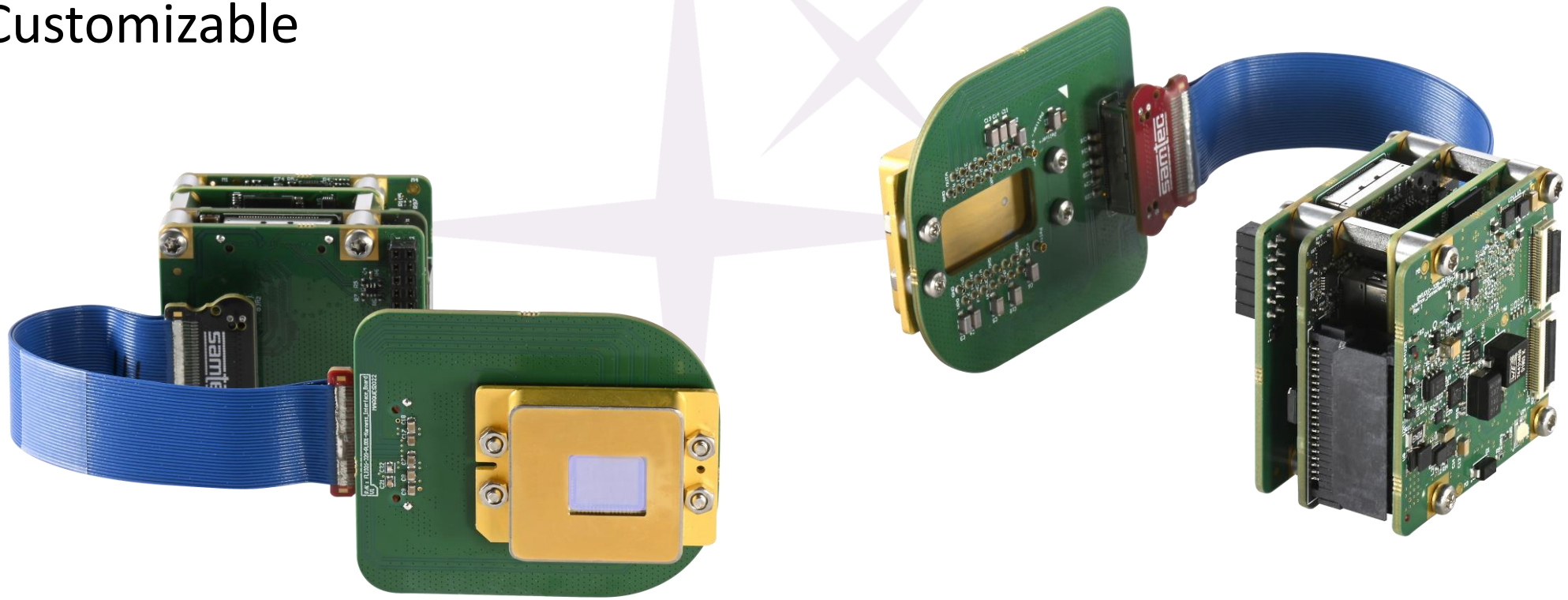




3 flight models delivered in 2022

What First Light brings : New Space SWIR camera

- C-RED New Space
  - New Space designed
  - Customizable



What First Light brings : Fast low noise SWIR cameras

- Ground segment use :
  - Beam steering cameras/pointing
  - Adaptive optics for FSO

SPIE.

C-RED 3: A SWIR camera for FSO applications
Gach et al. SPIE 11272-14 (2020)

C-RED 2 Lite (stabilized)

C-RED 3 (uncooled)

600 FPS FF/ 1980 FPS 256x256 / 4780 FPS 128x128 - <30^{e}- RON

Thank You !

www.first-light-imaging.com


FIRST
LIGHT
ADVANCED IMAGERY