The Eagle-1 QKD protocol - Phase encoded BB84 decoy in a practical satellite QKD application

Kevin Günthner, Conrad Rößler, Bastian Hacker, Ivan Derkach, Vladyslav Usenko and Christoph Marquardt

The Eagle-1 QKD Protocol - from science to application Workshop
2024-11-13

Palacký University Olomouc

FAU

MAX PLANCK INSTITUTE FOR THE SCIENCE OF LIGHT

Introduction

- Satellite QKD can provide secure communication over long distances

Introduction

- Satellite QKD can provide secure communication over long distances
- EAGLE-1 project: first European satellite QKD mission with in-orbit demonstration (ESA project with SES as project prime and FAU and MPL as scientific lead among more than 20 consortium partners and close industry collaboration)

Introduction

- Satellite QKD can provide secure communication over long distances
- EAGLE-1 project: first European satellite QKD mission with in-orbit demonstration (ESA project with SES as project prime and FAU and MPL as scientific lead among more than 20 consortium partners and close industry collaboration)

- **QKD Protocol underlying ideas:**
  - Built upon mature and well established QKD security proof
  - Built upon established classical communication technology
  - Possibility to couple QKD signal into fiber on ground connecting it to the quantum receiver that can be placed at different premises

→ BB84 decoy protocol with relative phase encoding in C-Band

Introduction

- Satellite QKD can provide secure communication over long distances
- EAGLE-1 project: first European satellite QKD mission with in-orbit demonstration (ESA project with SES as project prime and FAU and MPL as scientific lead among more than 20 consortium partners and close industry collaboration)

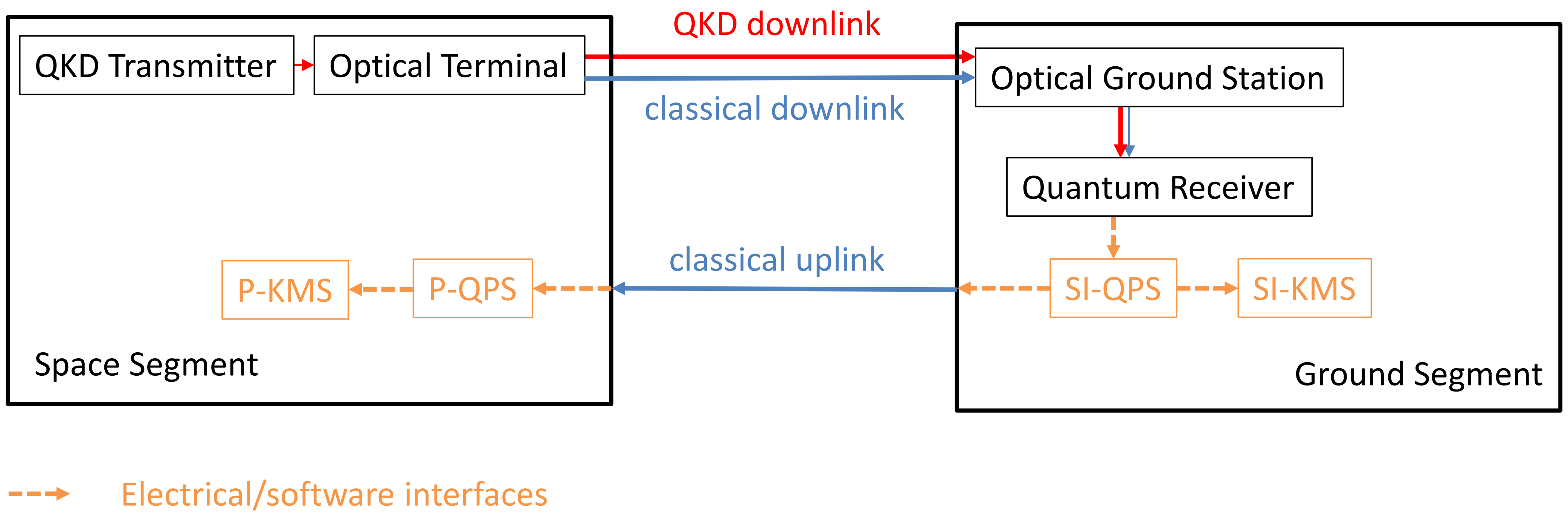
- **QKD Protocol underlying ideas:**
  - Built upon mature and well established QKD security proof
  - Built upon established classical communication technology
  - Possibility to couple QKD signal into fiber on ground connecting it to the quantum receiver that can be placed at different premises

→ BB84 decoy protocol with relative phase encoding in C-Band

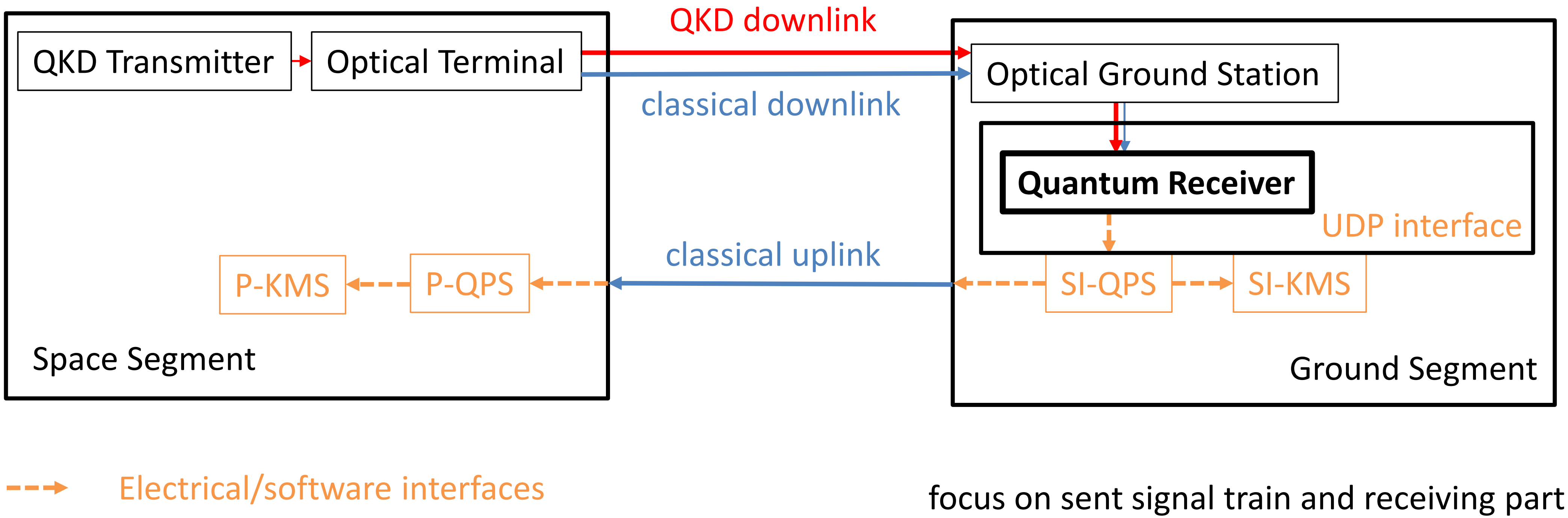
- **Important challenges in satellite QKD:**
  - SWaP (size, weight and power) requirements
  - Doppler effect
  - Clock recovery and time synchronization
  - High losses (up to 60dB)

Eagle-1 Consortium

(simplified) Eagle-1 System Overview



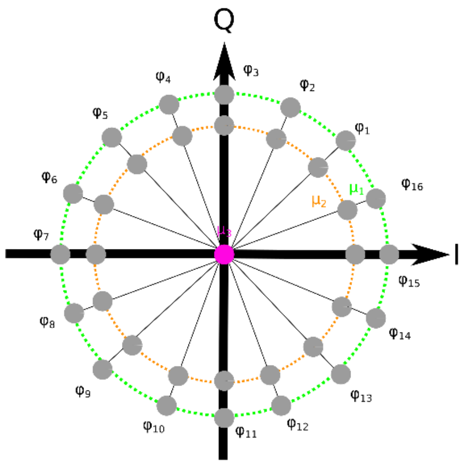
(simplified) Eagle-1 System Overview

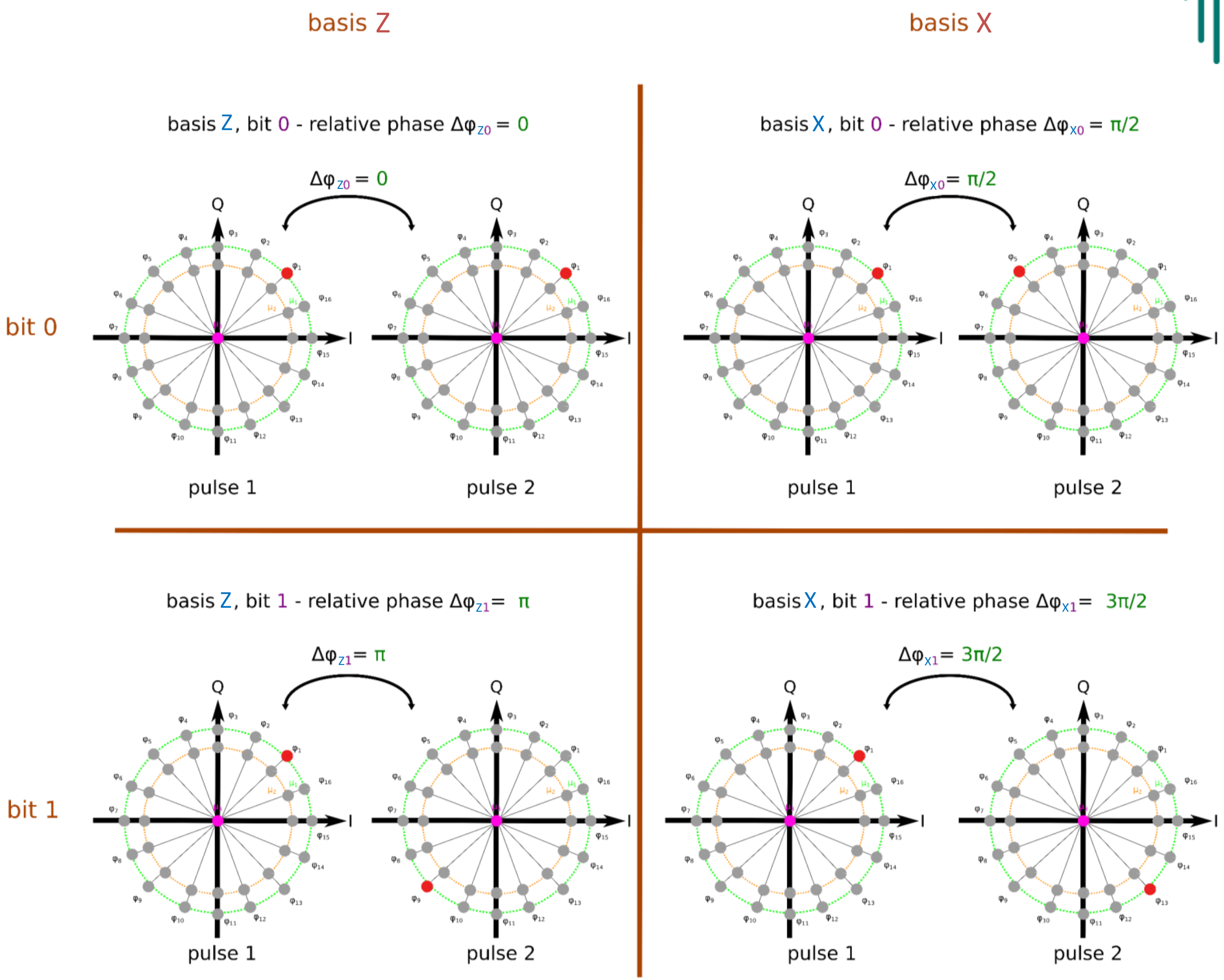


focus on sent signal train and receiving part

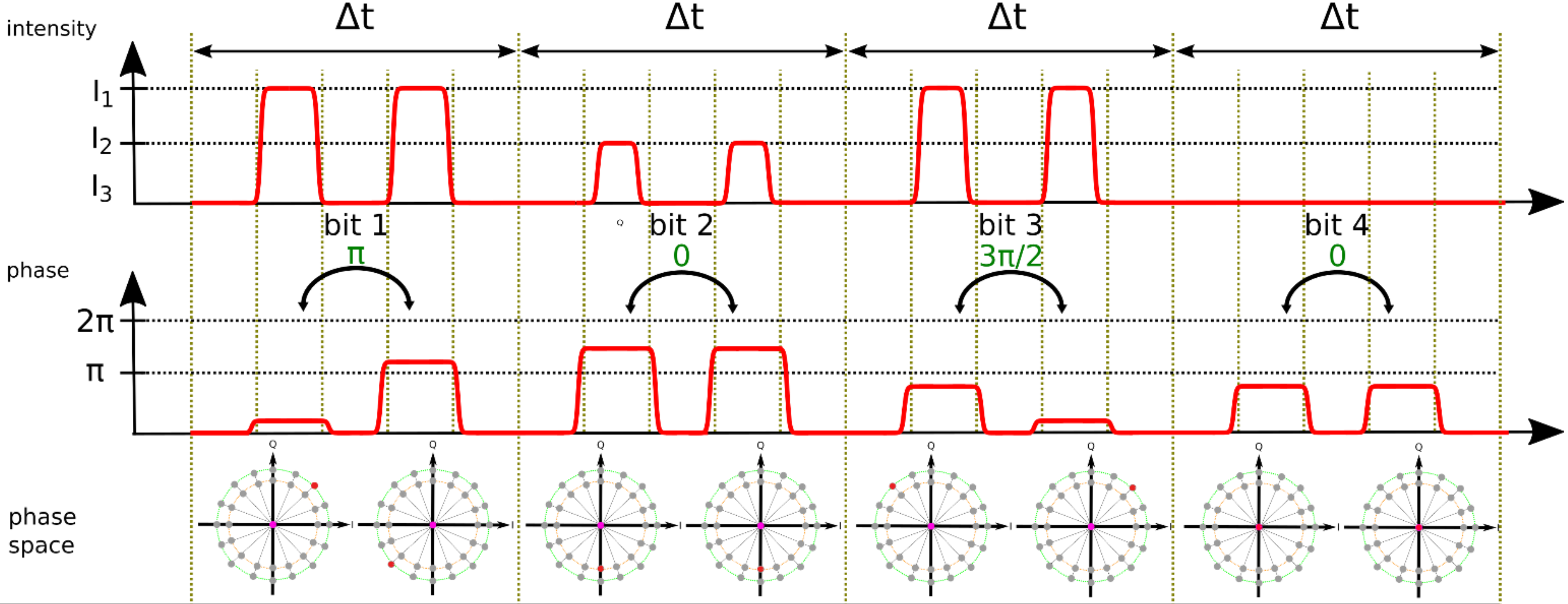
Bit and Base Definition

First pulse: random phase
(1 out of 16 phases)





Encoding Scheme



amplitude	μ_1	μ_2	μ_1	μ_3
phase first pulse (random)	$\varphi_1 = \pi/4$	$\varphi_{11} = 3\pi/2$	$\varphi_5 = 3\pi/4$	$\varphi_5 = 3\pi/4$
basis	Z	Z	X	Z
bit value	1	0	1	0
relative phase	$\Delta\varphi_{Z1} = \pi$	$\Delta\varphi_{Z0} = 0$	$\Delta\varphi_{X1} = 3\pi/2$	$\Delta\varphi_{Z0} = 0$
phase second pulse	$\varphi_1 + \Delta\varphi_{Z1} = 5\pi/4$	$\varphi_{11} + \Delta\varphi_{Z0} = 3\pi/2$	$\varphi_5 + \Delta\varphi_{X1} = \pi/4$	$\varphi_5 + \Delta\varphi_{Z0} = 3\pi/4$

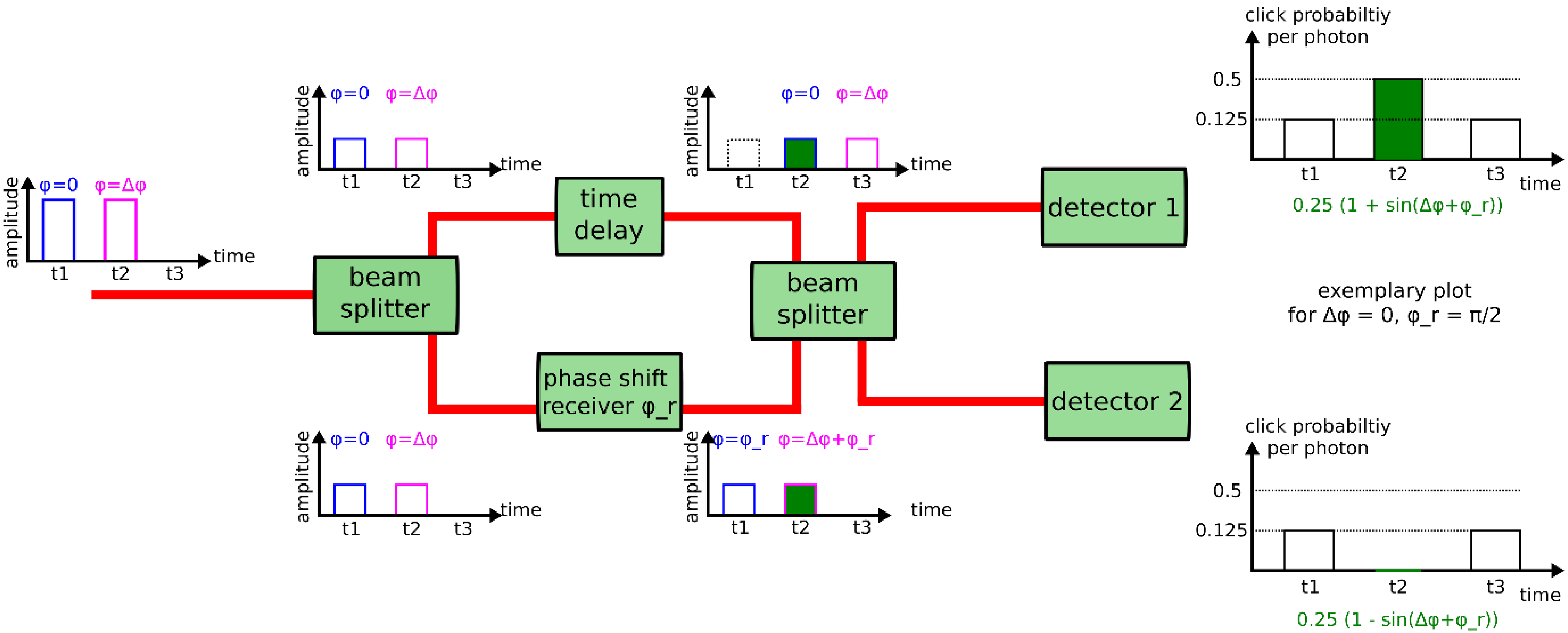
Encoding in **relative phase** of two subsequent pulses forming one quantum state

First pulse: random phase (1 out of 16 phases)

3 different states:

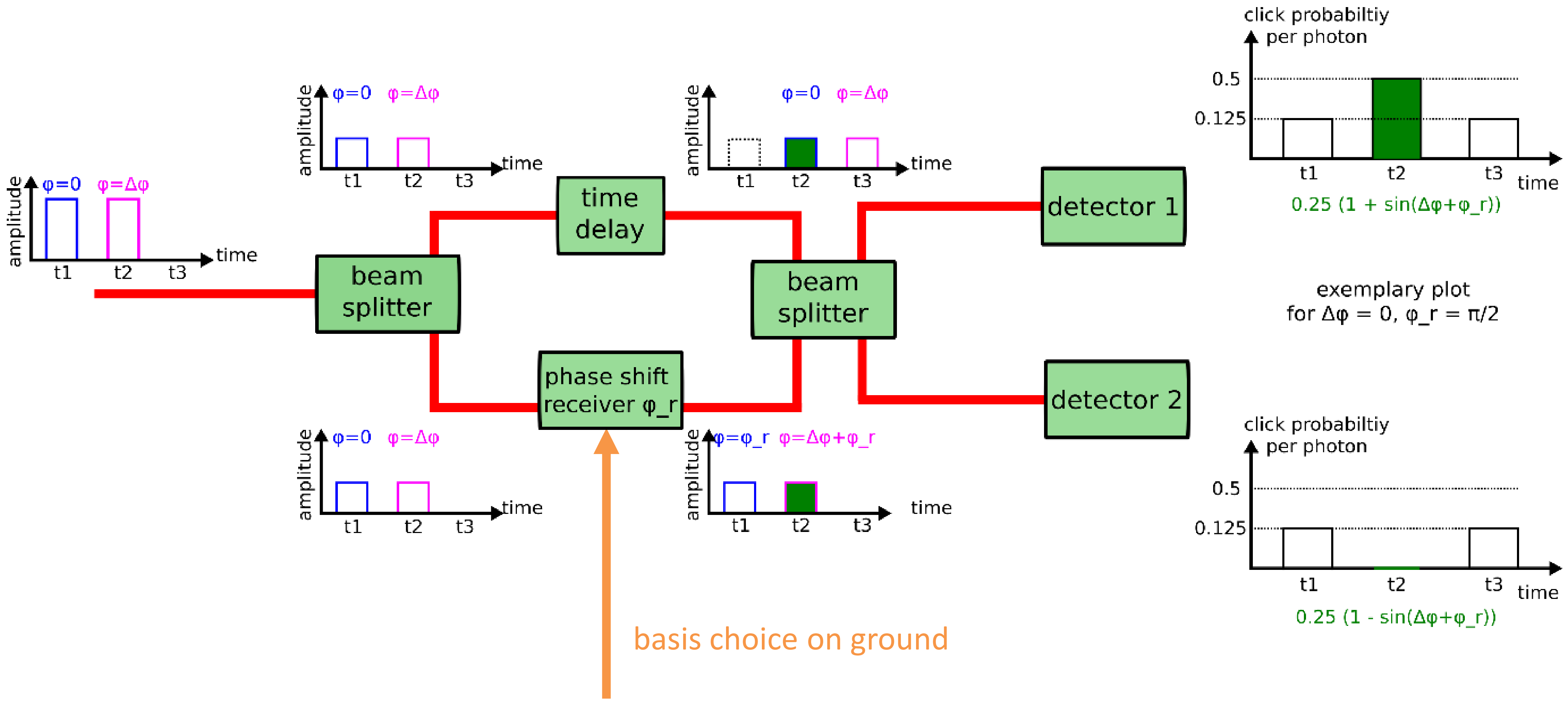
- $p_{signal} = 3/4$, $\mu_1 = 0.63$
- $p_{decoy} = 3/16$, $\mu_2 = 0.14$
- $p_{vacuum} = 1/16$, $\mu_3 = 0.001$

Receiving Scheme



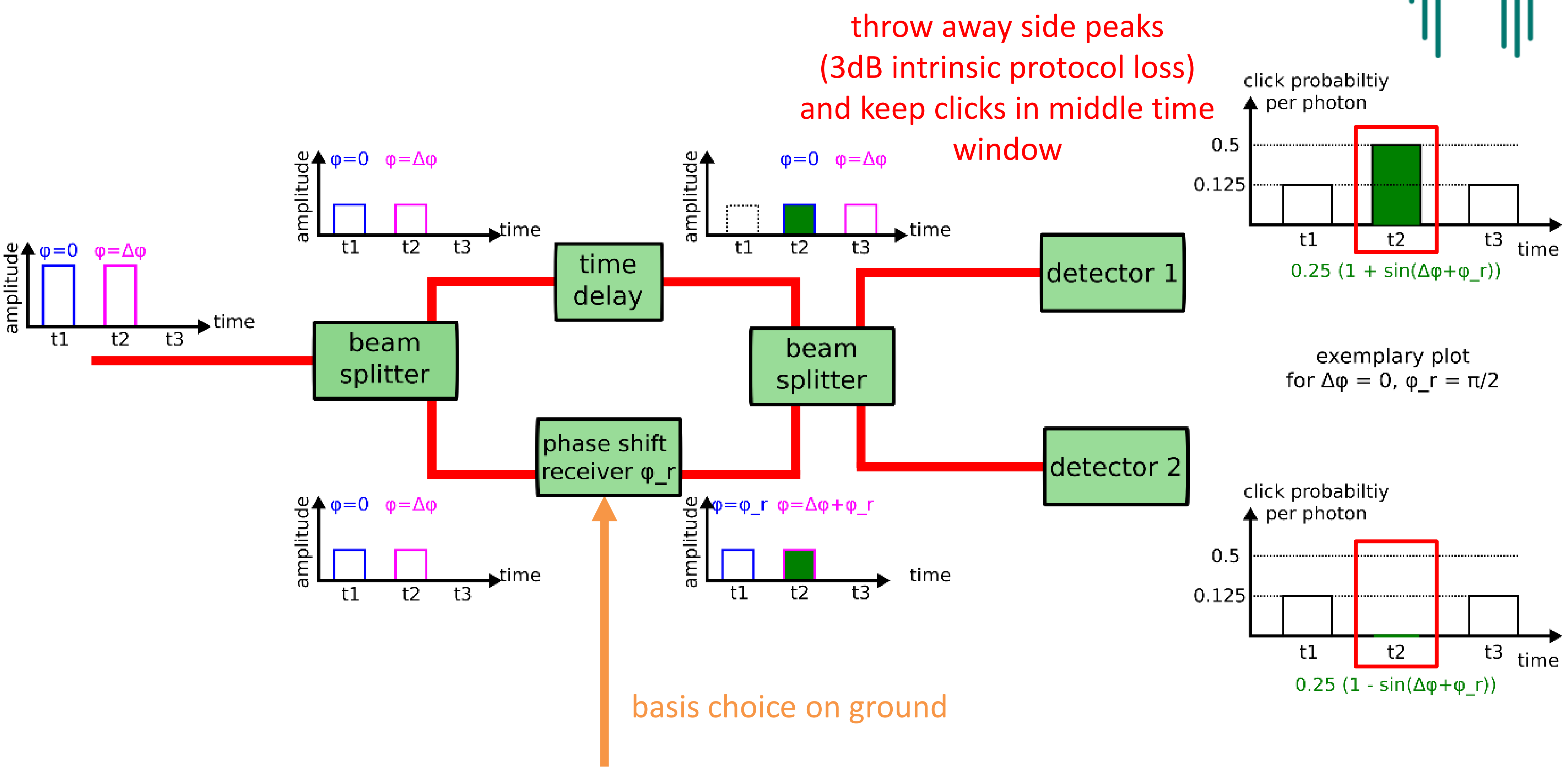
2 interferometers with 2 phase shifts corresponding to the 2 bases

Receiving Scheme



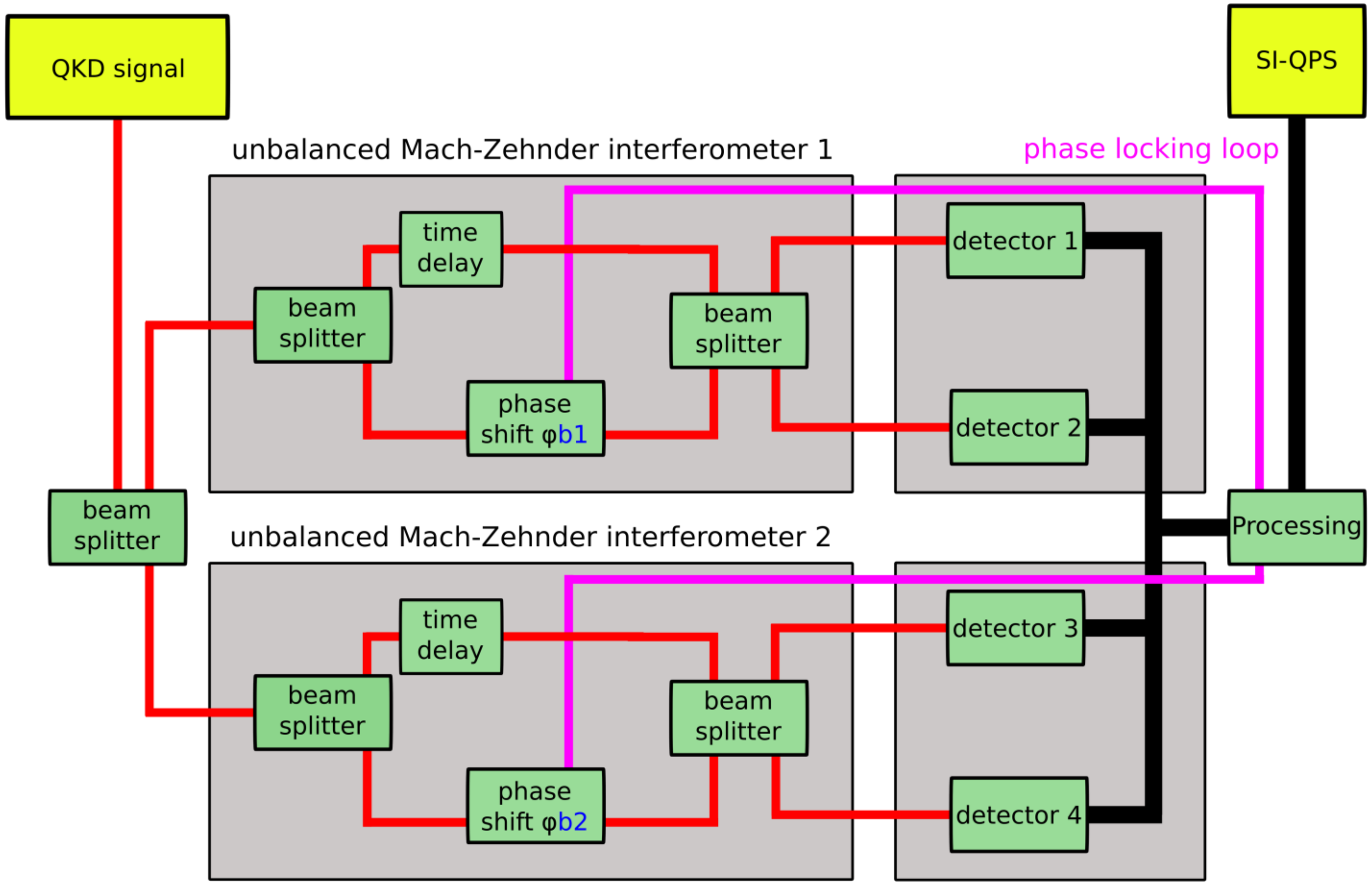
2 interferometers with 2 phase shifts corresponding to the 2 bases

Receiving Scheme

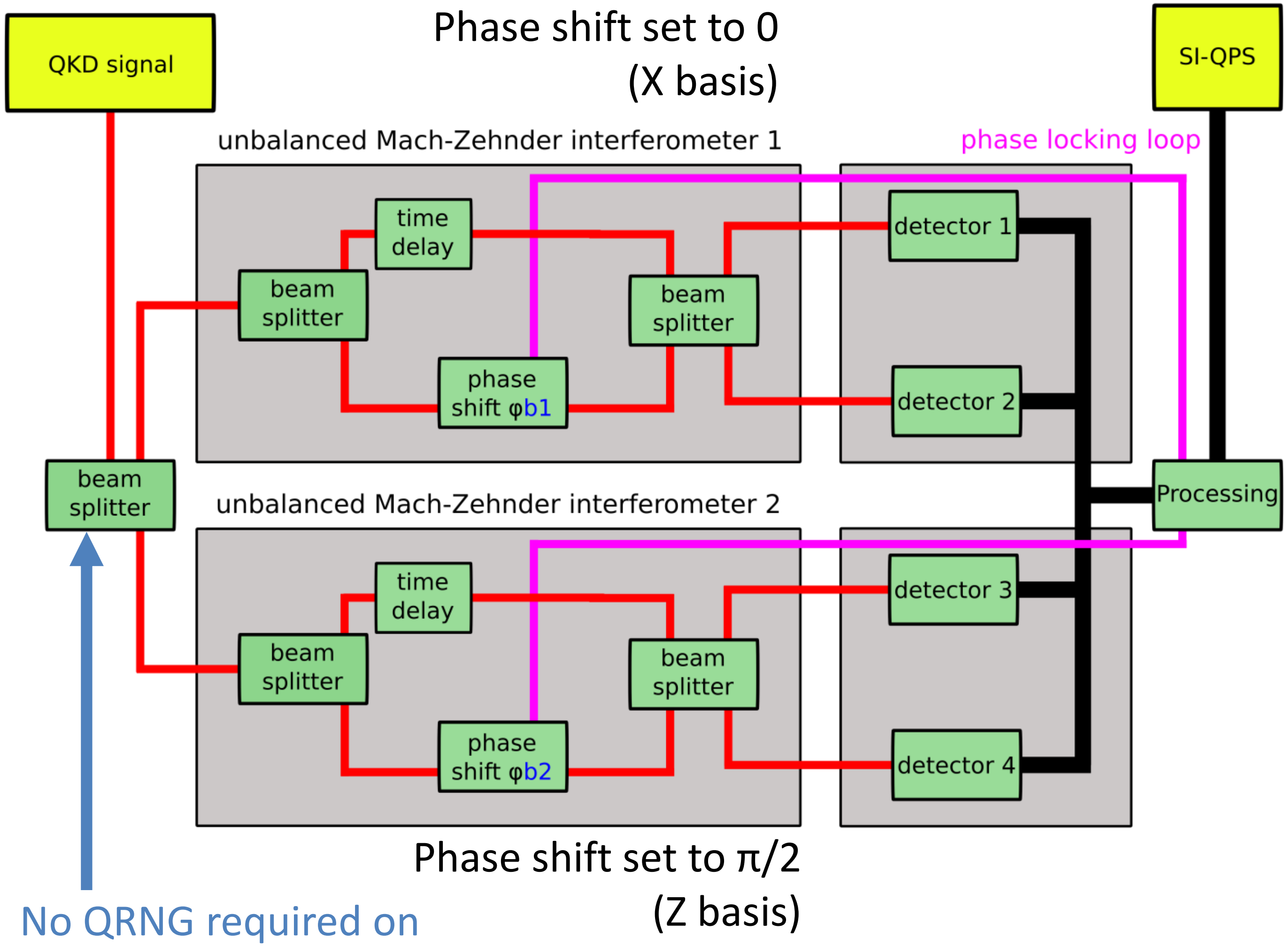


2 interferometers with 2 phase shifts corresponding to the 2 bases

Receiving Scheme

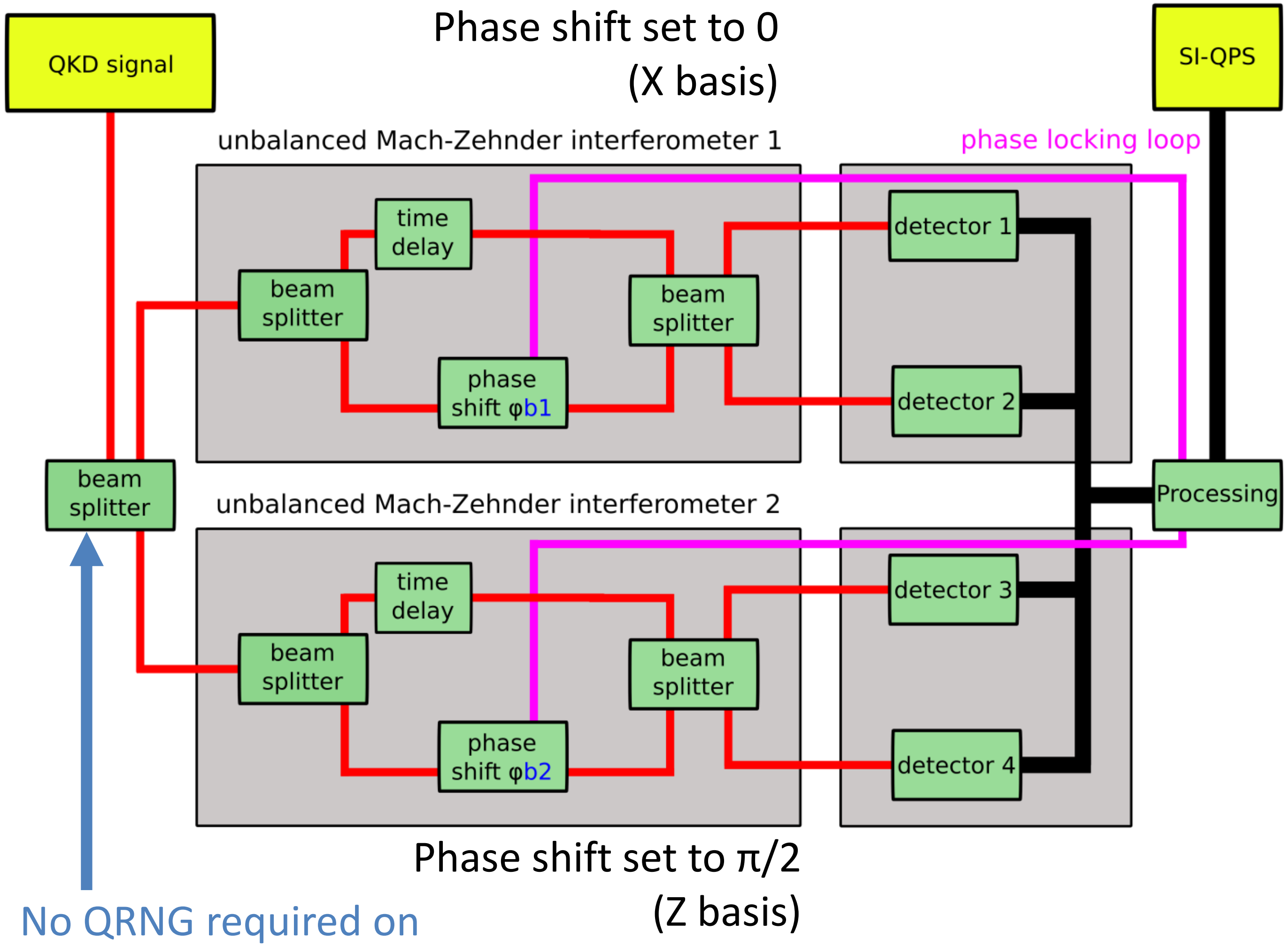


Receiving Scheme

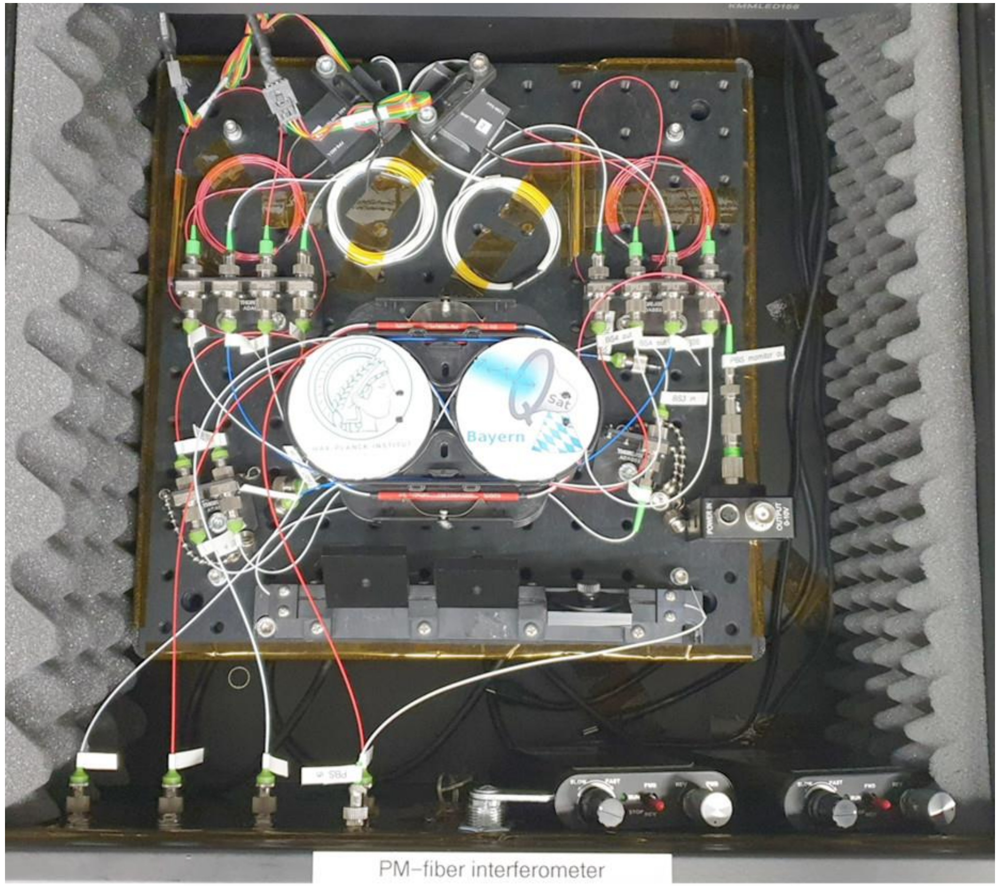


No QRNG required on ground: States sent to interferometer 1 or 2 at random

Receiving Scheme



No QRNG required on ground: States sent to interferometer 1 or 2 at random



Interferometer 1 and 2 integrated setup
[B. Hacker *et al* 2023 *New J. Phys.* **25** 113007]

Truth Table

Basis Sender	Bit Sender	Relative Phase Sender	Basis Receiver	Modulated Phase Receiver	Click Probability detector 1	Click Probability detector 2	Bit Receiver
Z	0	0	Z	π/2	0	1	0
	1	π		π/2	1	0	1
Z	0	0	X	0	1/2	1/2	random
	1	π		0	1/2	1/2	random
X	0	π/2	Z	π/2	1/2	1/2	random
	1	3π/2		π/2	1/2	1/2	random
X	0	π/2	X	0	0	1	0
	1	3π/2		0	1	0	1

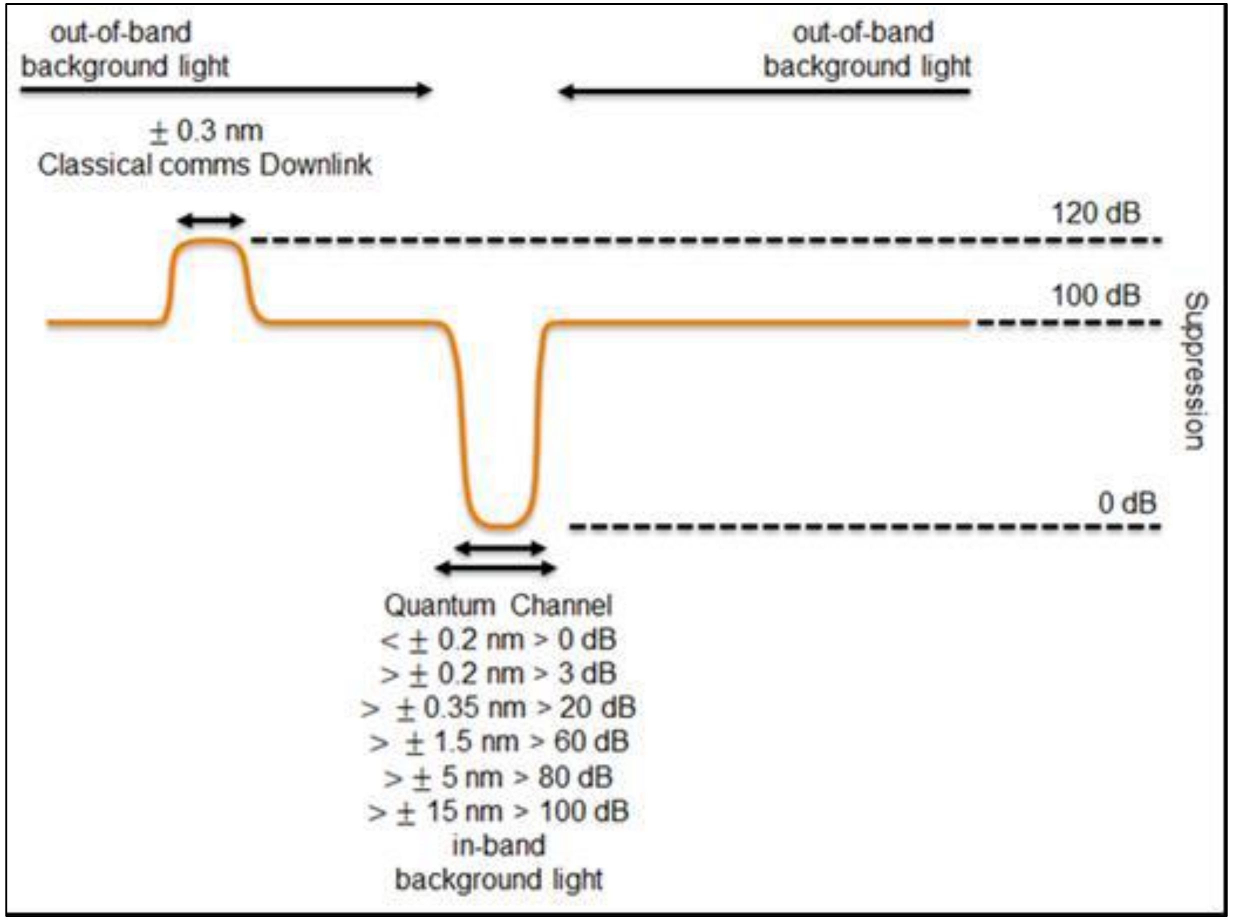
Entrance Filter and background light

Class comm downlink wavelength:

1553.33 nm

Max. background counts at fiber entrance before filter:

- 800 Hz or -129.9 dBm in Quantum channel In-band
- 1000 Hz or -128.9 dBm Quantum channel out-of-band

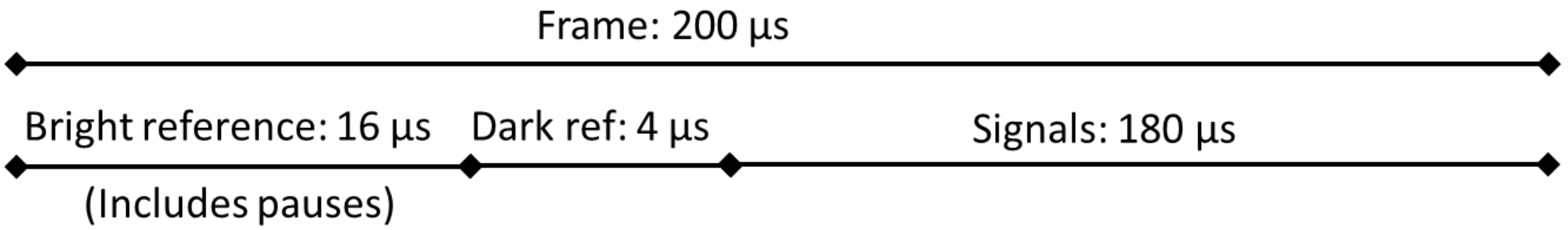


Quantum channel wavelength:

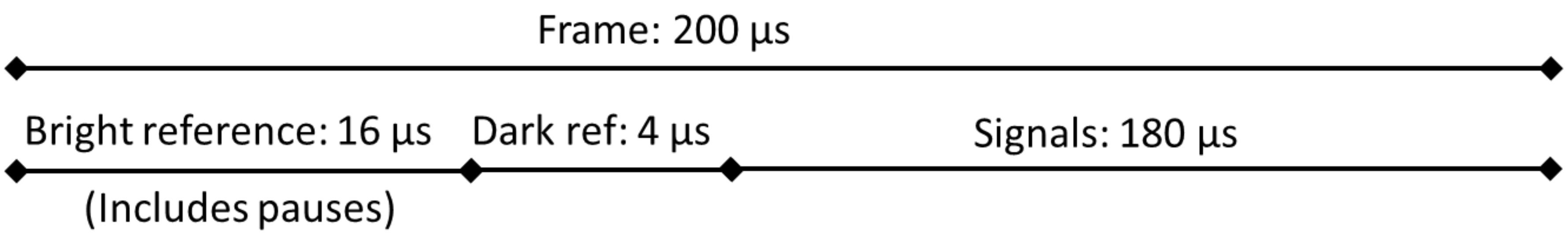
1565.49 nm

[c.f. ICD and DDF Files already released]

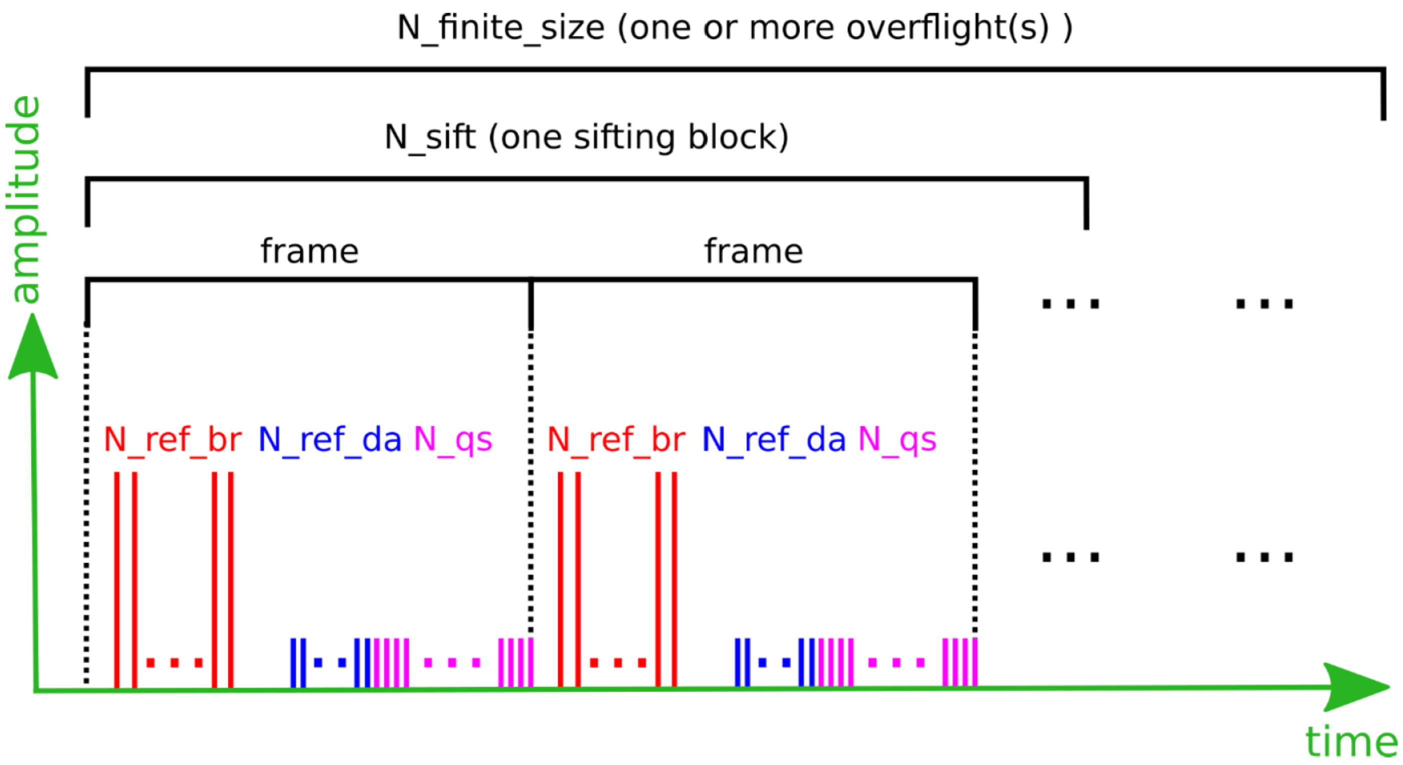
Frame Structure



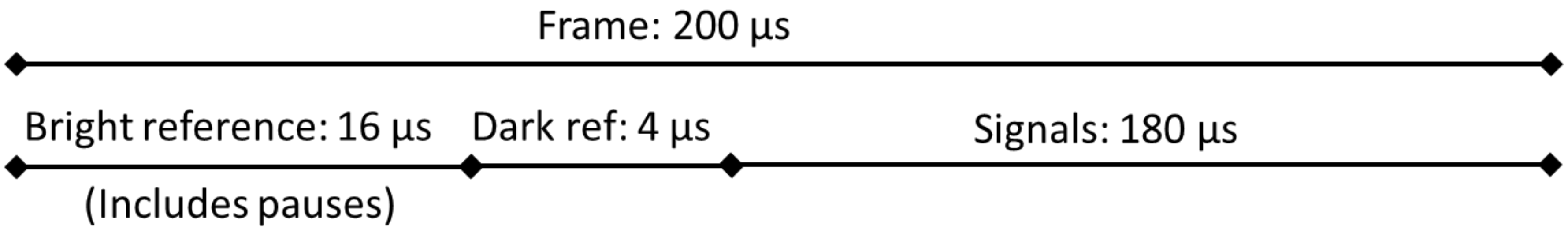
Frame Structure



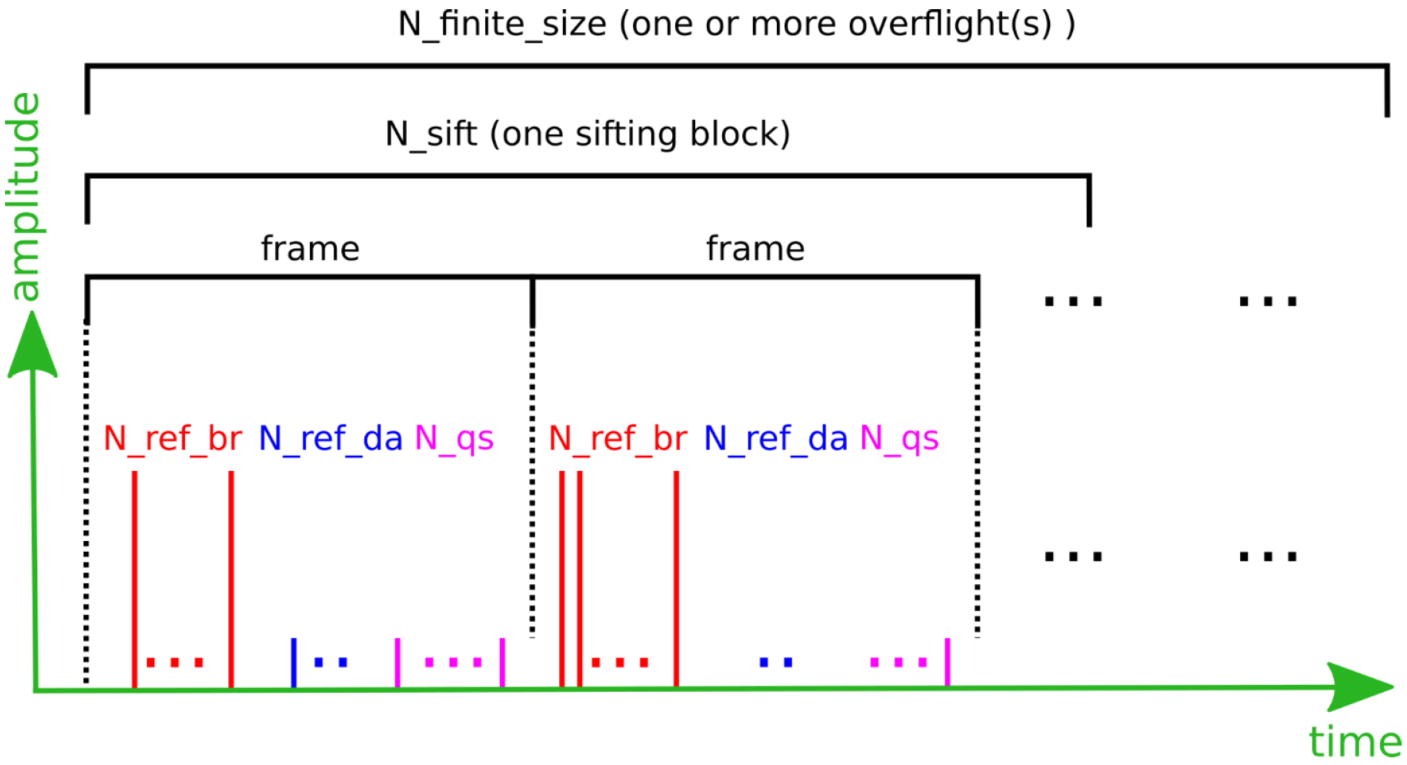
Sent pattern



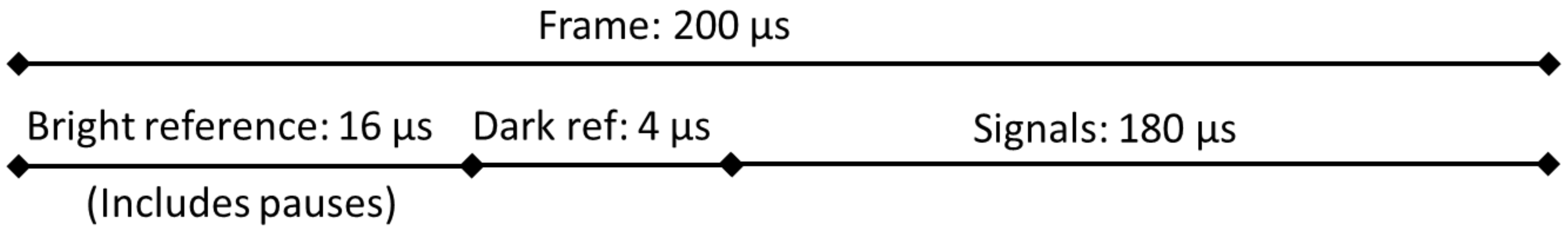
Frame Structure

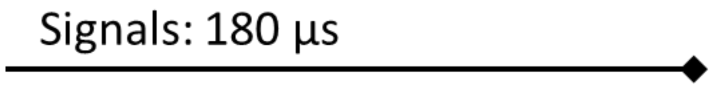


Received pattern



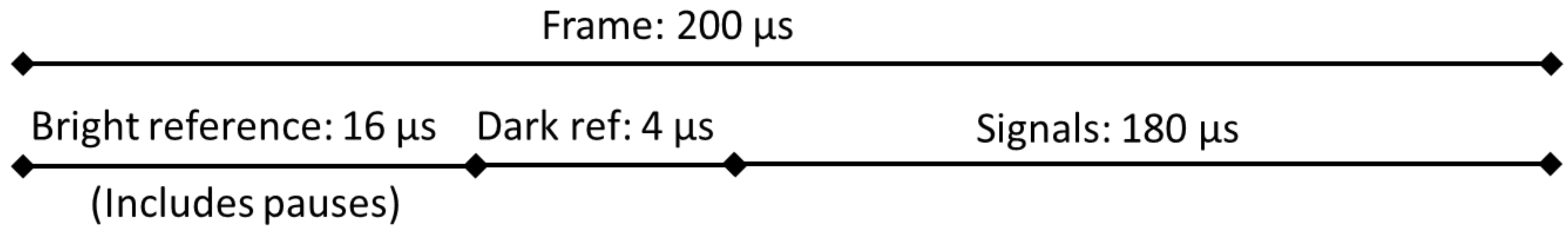
Frame Structure

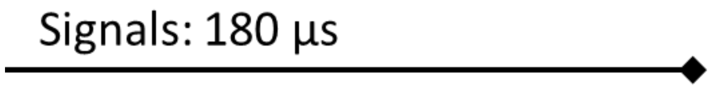




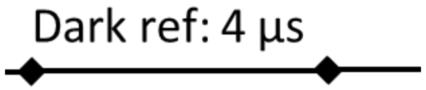
Quantum states
→ used for key creation
(450000 states)

Frame Structure



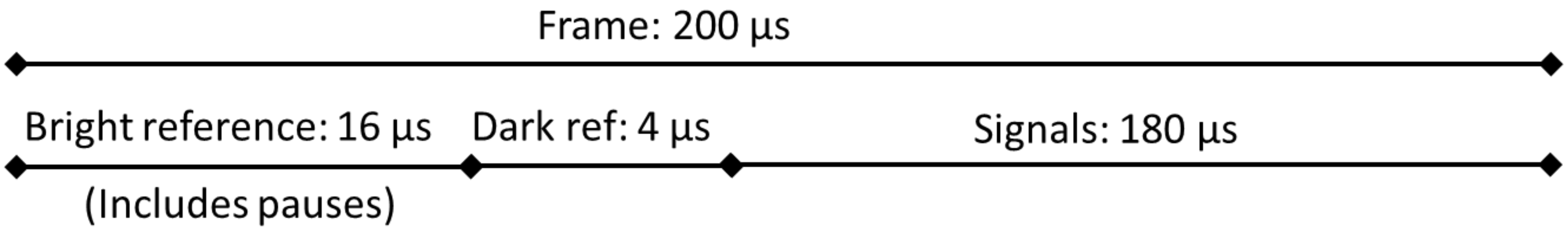


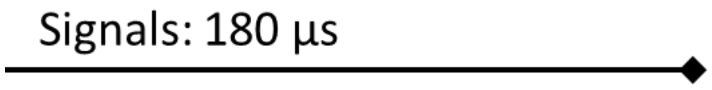
Quantum states
→ used for key creation
(450000 states)



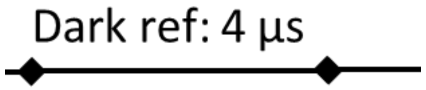
Encoded like quantum states with deterministic states
→ Live reference QBER
(10000 states)

Frame Structure





Quantum states
→ used for key creation
(450000 states)

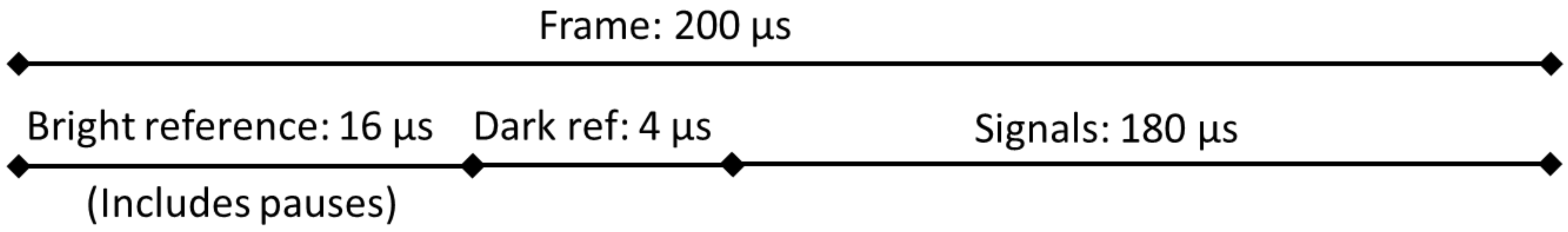


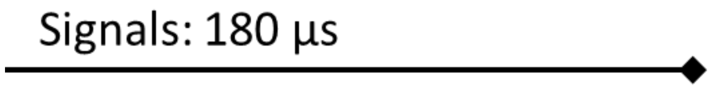
Encoded like quantum states with deterministic states
→ Live reference QBER
(10000 states)

3 different states:

- $p_{signal} = 3/4$, $\mu_1 = 0.63$
- $p_{decoy} = 3/16$, $\mu_2 = 0.14$
- $p_{vacuum} = 1/16$, $\mu_3 = 0.001$

Frame Structure

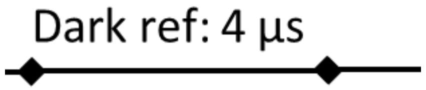




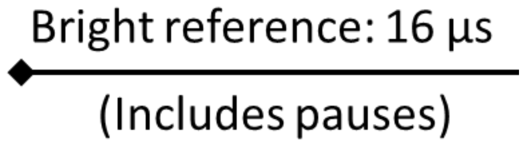
Quantum states
→ used for key creation
(450000 states)

3 different states:

- p_{signal} = 3/4 , μ_1 = 0.63
- p_{decoy} = 3/16 , μ_2 = 0.14
- p_{vacuum} = 1/16 , μ_3 = 0.001



Encoded like quantum states with deterministic states
→ Live reference QBER
(10000 states)



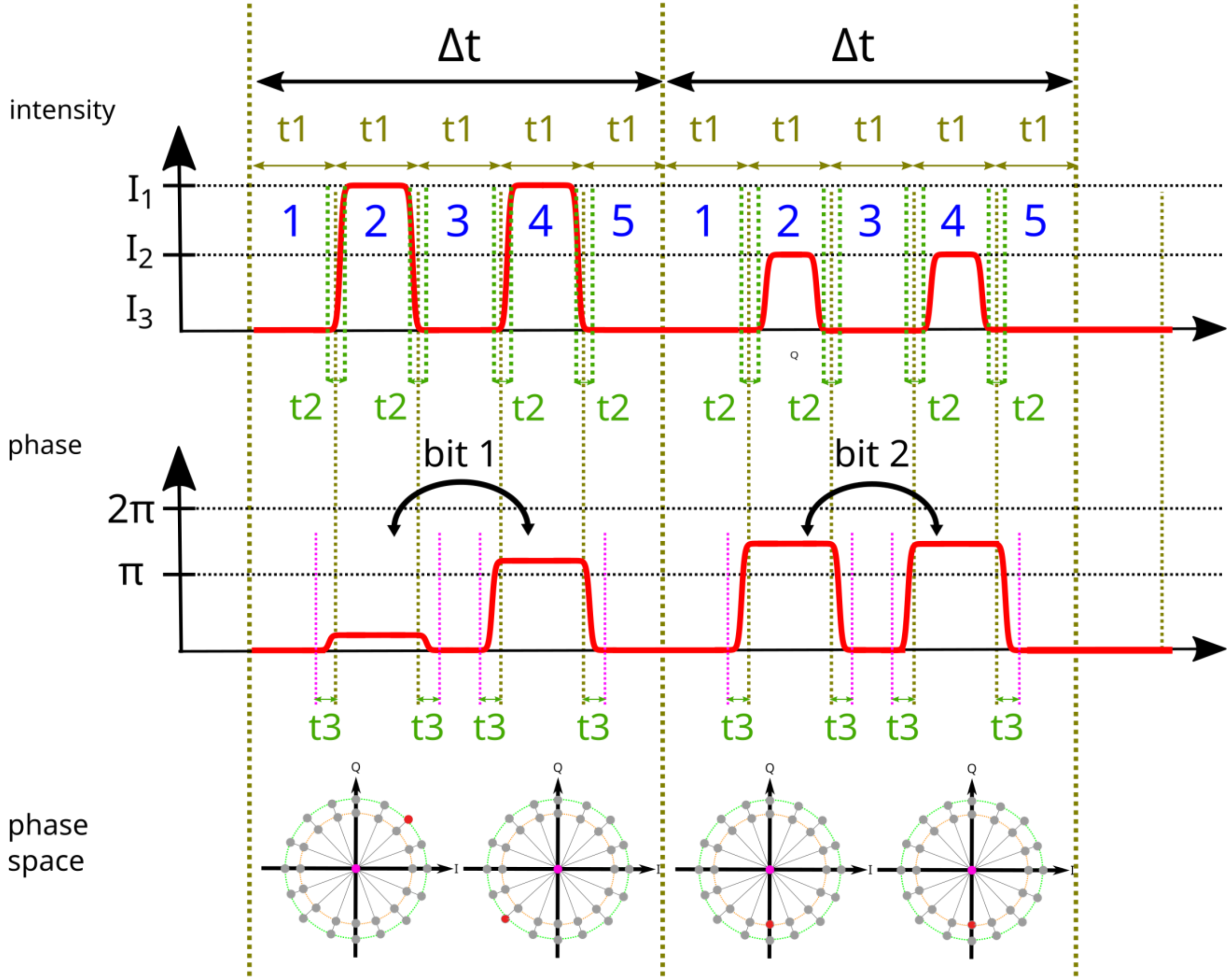
- Clock recovery on ground
- Frame number encoding (time synchronization with satellite)
- Interferometer phase locking
- Balancing of interferometers

Frame Structure

Number	Number of pulse pairs	Duration [μs]
N_ref_br	158 + 2 single pulses	16
N_ref_da	10000	4
N_qs	450000	180

Number	Number of frames	Notes
N_sift	540	Corresponds to a time of 540 x 200μs = 108ms
Number	**Number of detected Qbits on ground per base**	**Notes**
N_finite_size	16.5 x 10^5	Might take more than one overflight to reach this number; configurable in QPS as the key rate is dependent on the choice of this number – values of up to 27.5 x 10^5 can be beneficial depending on the link budget

Quantum States



Time parameter name	Duration [ps]	Notes
Δt	**400**	**Temporal definition of a Qbit**
t1	**80**	**Time duration of a single pulse**
t2	0 <= t2 <= 30	Rise/fall time intensity
t3	0 <= t3 <= 30	Rise/fall time phase

→ Effective symbol rate: **2.25 GS/s**
(considering reference pulse fraction of 0.9)

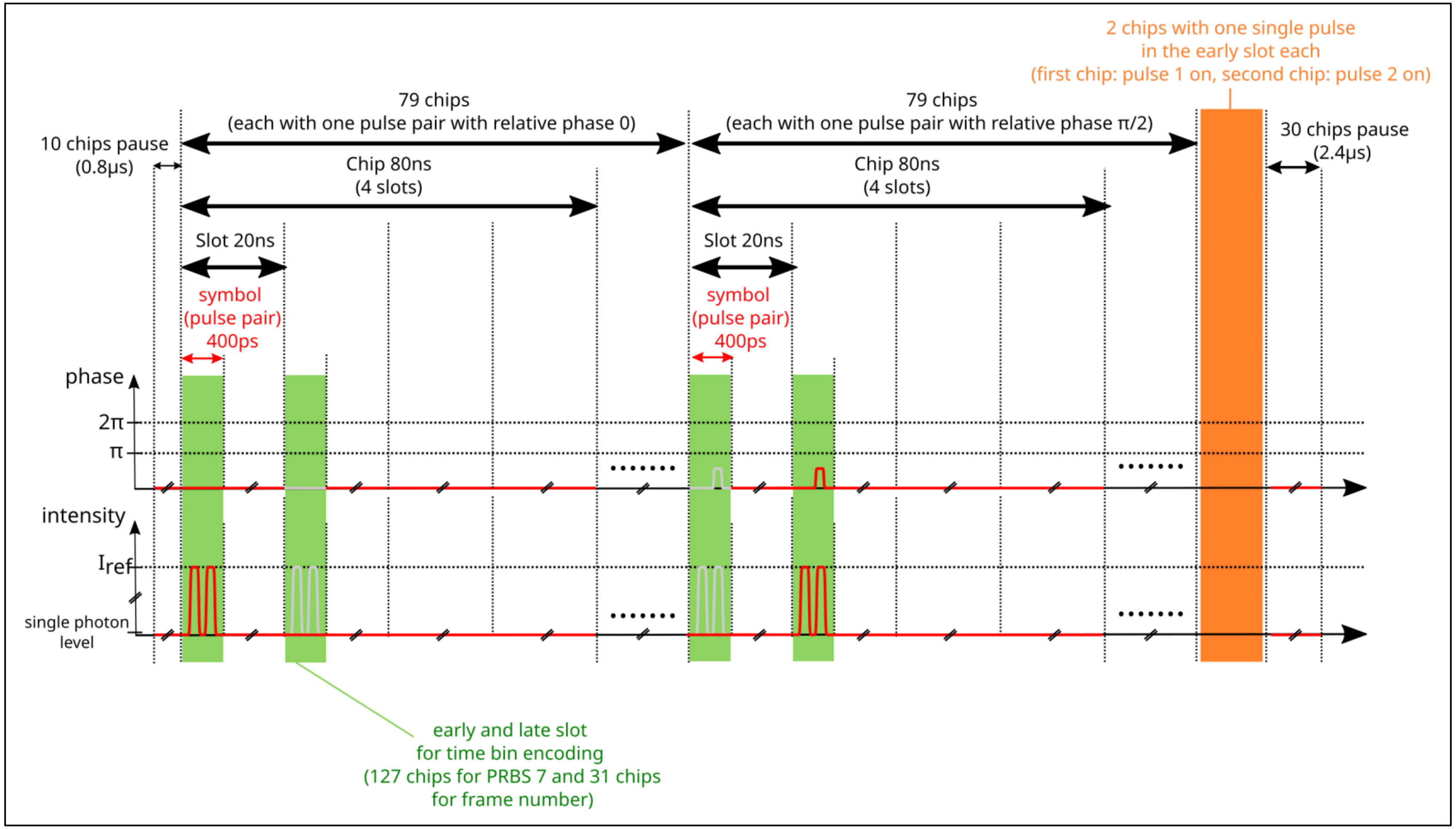
Dark Reference Pulses

- 10000 pulse pairs modulated in a deterministic pattern like quantum states
- **Live reference QBER**
- 10 bits for each symbol (where x means arbitrary):
  - 4 bits for the type:
    - 00xx, 01xx, 10xx for signal (P=3/4)
    - 1100, 1101, 1110 for decoy (P=3/16)
    - 1111 for vacuum (P=1/16)
  - 4 bits for the start phase: $\varphi 0 = xxxx * \pi/8$
  - 2 bits for the relative phase: $\varphi 0 = xx * \pi/2$

  (xxxx created with the PRBS-20 with start value 510795)

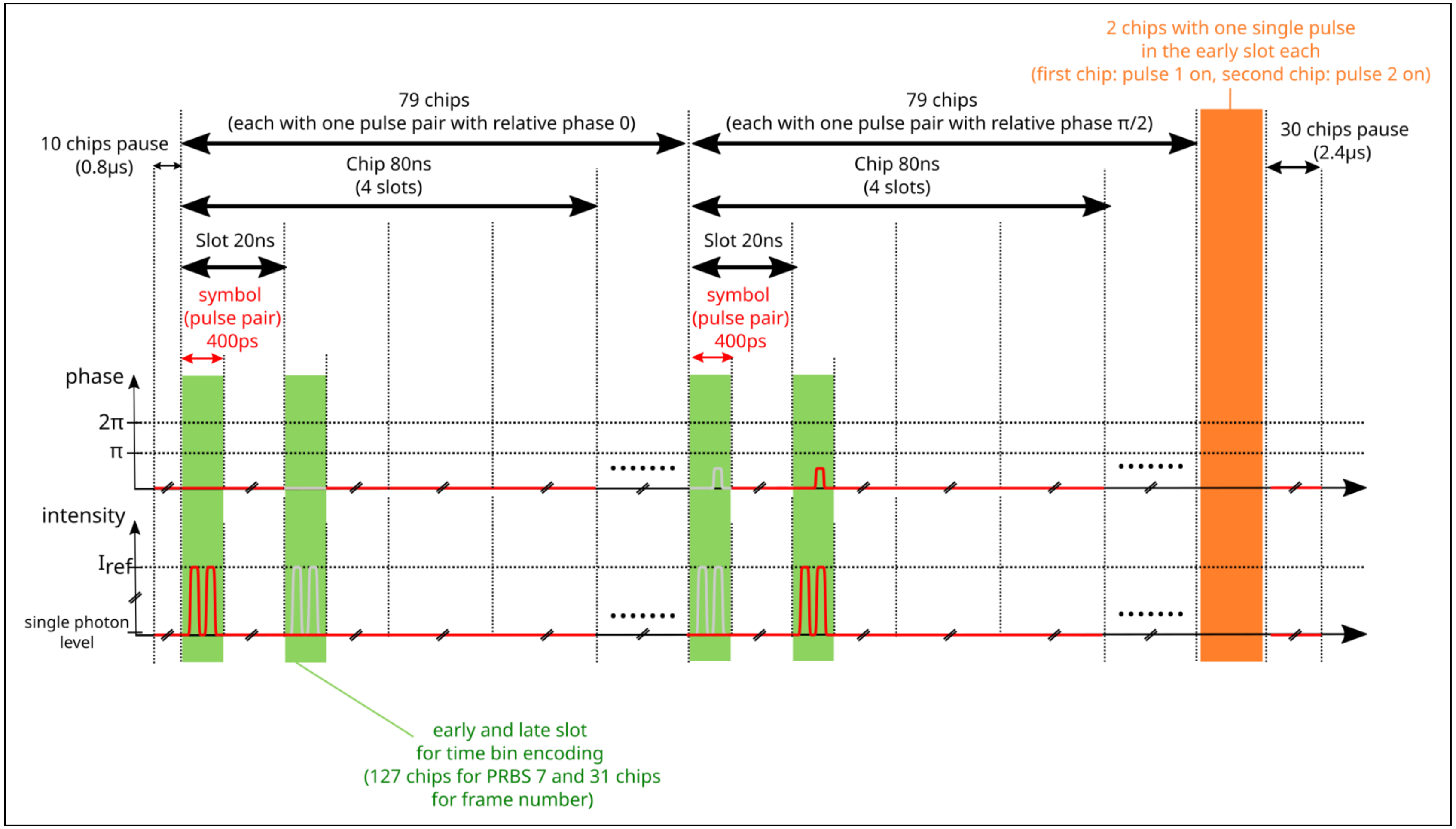
- Not part of key creation, reference only → no security risk

Bright Reference Pulses



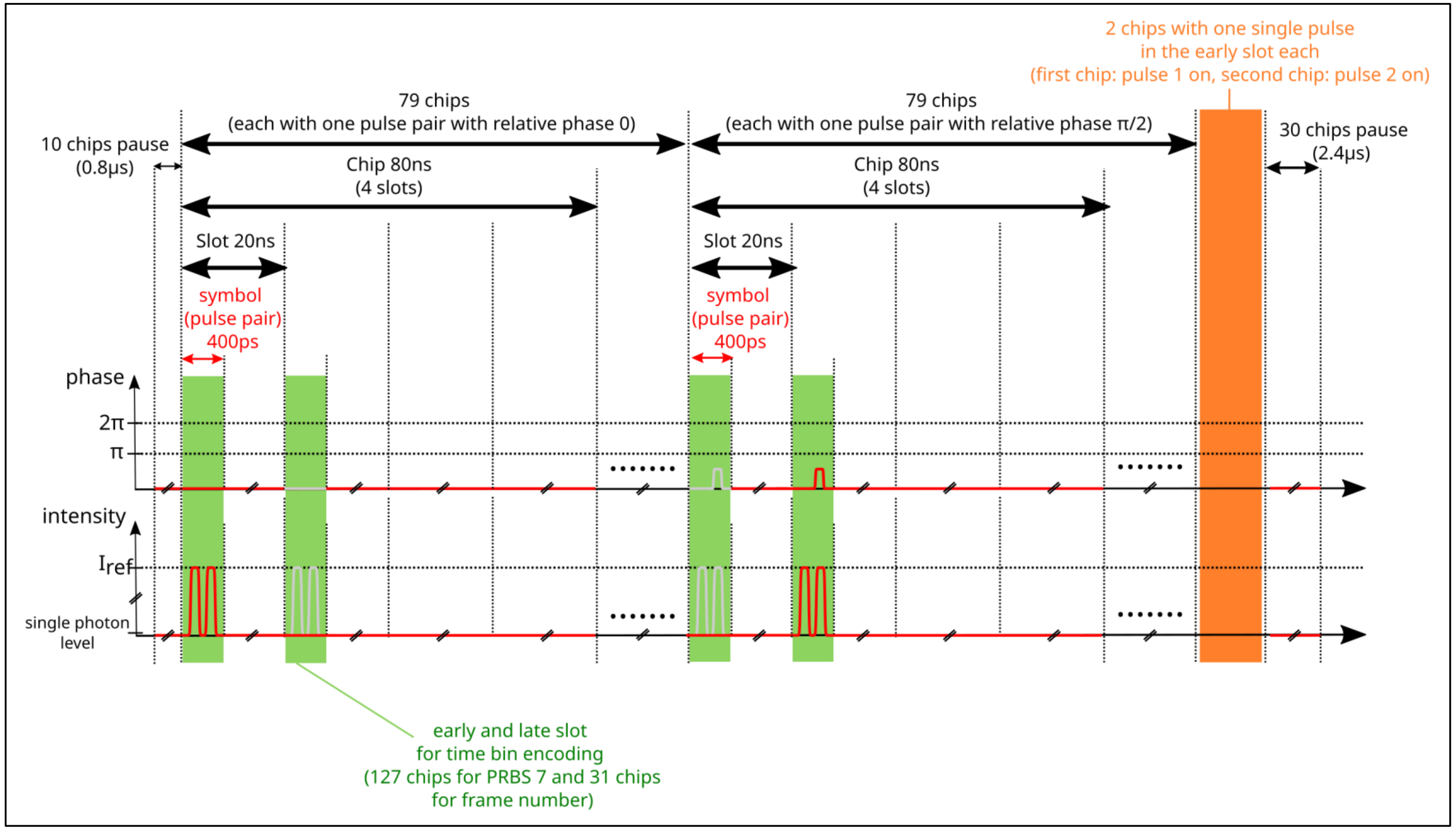
- Much higher intensity than quantum states (about 10000 higher)
- Larger temporal distance between pulse pairs
- 79 pulse pairs with relative phase 0, 79 pulse pairs with relative phase π/2
- Pulse pairs either in early or late slot
- Last two chips: single pulses

Bright Reference Pulses



- Much higher intensity than quantum states (about 10000 higher)
  → high likelihood of photon detection
- Larger temporal distance between pulse pairs
  → overcome dead time of SNSPD detectors (80ns)
- 79 pulse pairs with relative phase 0, 79 pulse pairs with relative phase $\pi/2$
  → phase lock both interferometers within one signal train
- Pulse pairs either in early or late slot
  → frame number encoding
- Last two chips: single pulses
  → balancing of interferometers

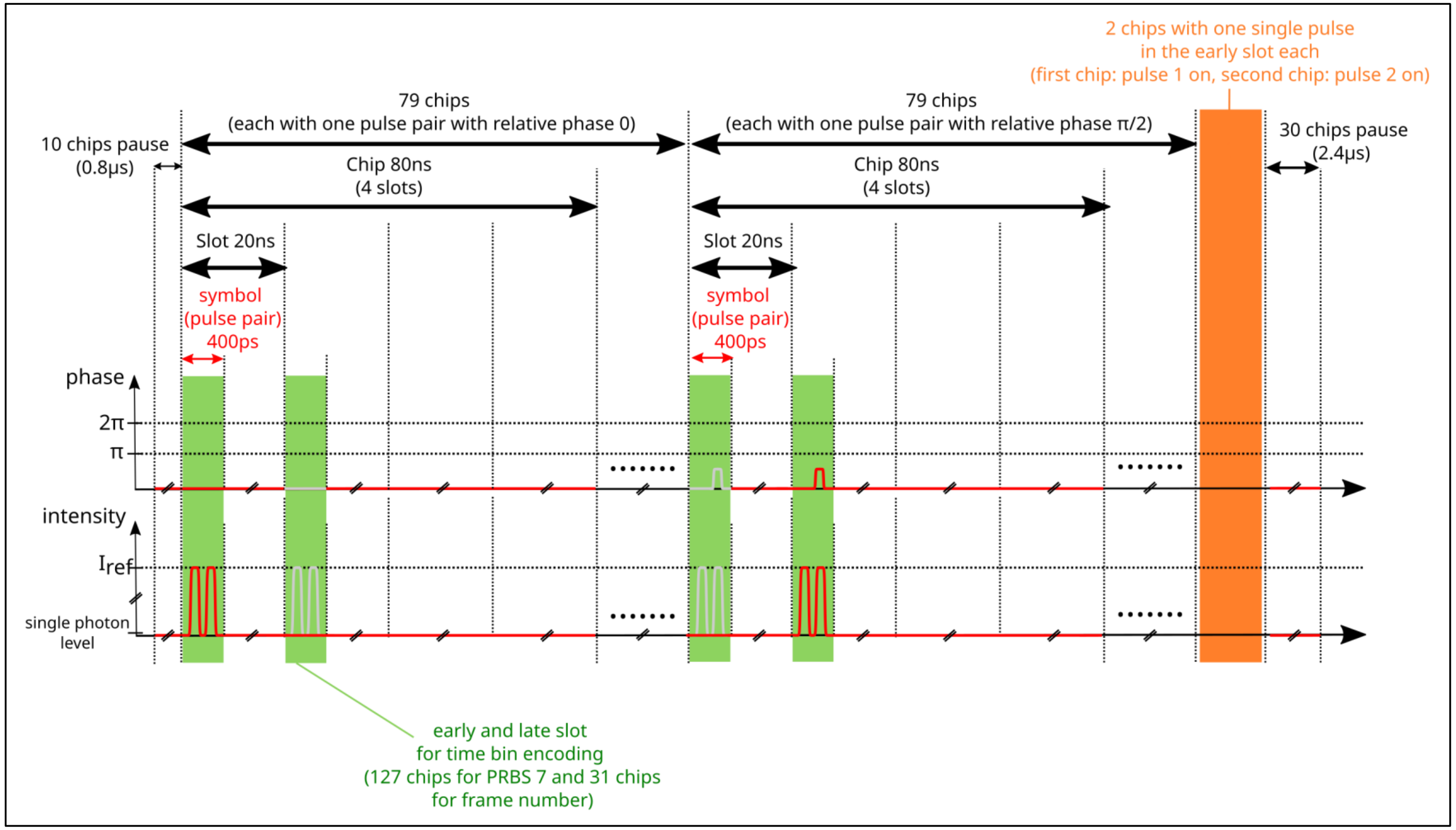
Bright Reference Pulses



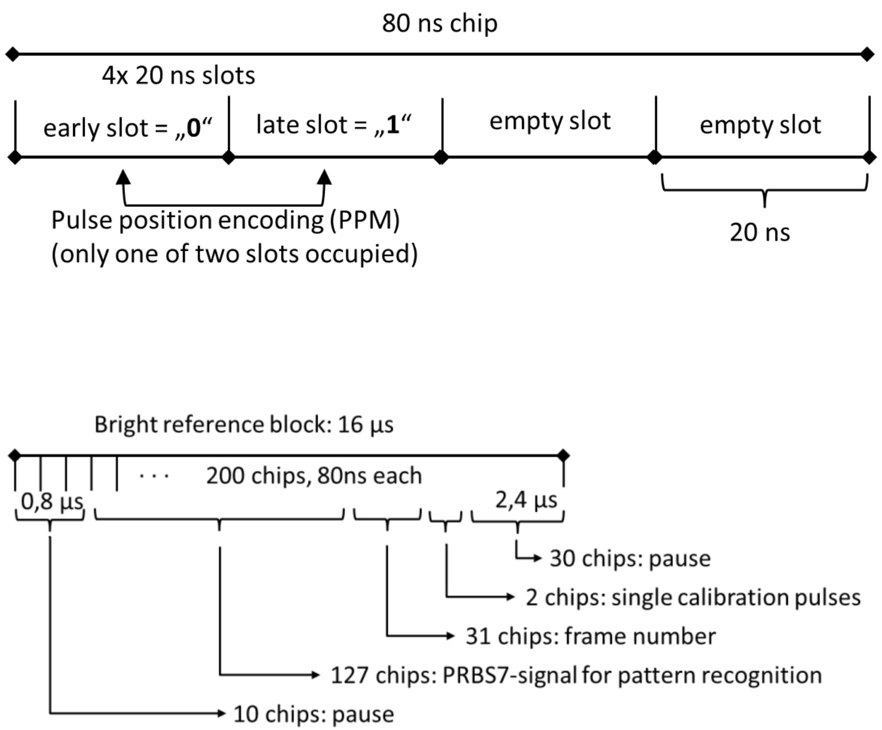
1. Clock recovery on ground

→ see following talk of Conrad Rößler

Bright Reference Pulses

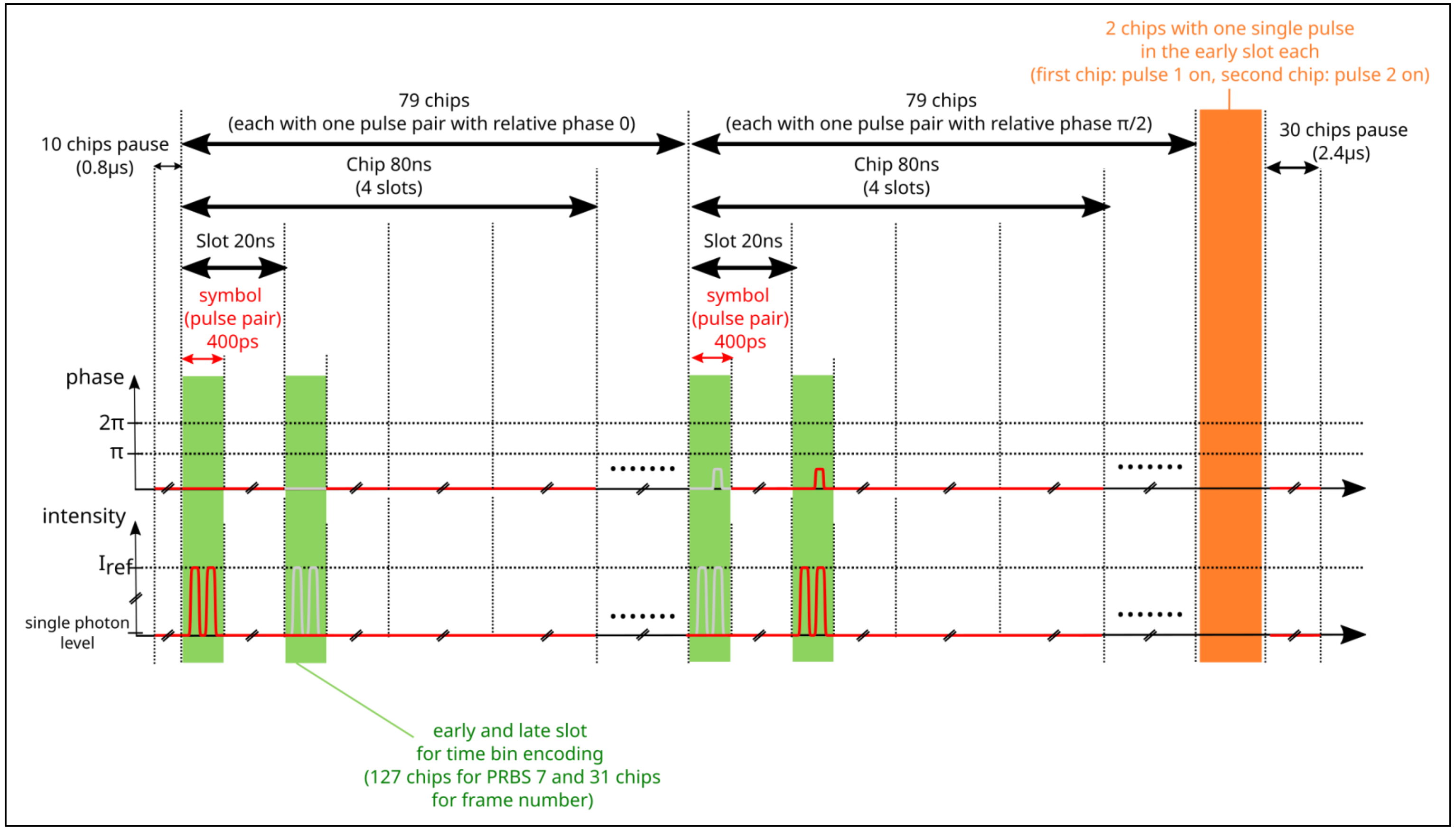


2. Frame Number PPM encoding:

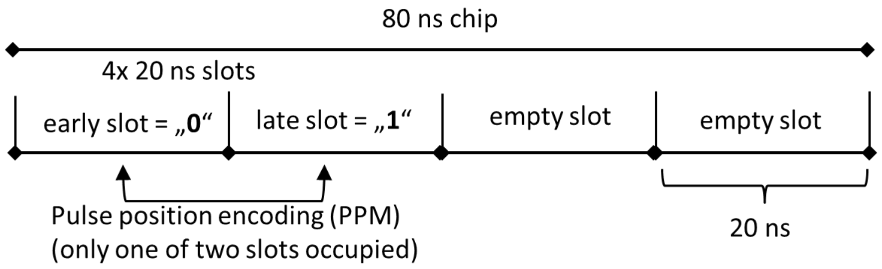


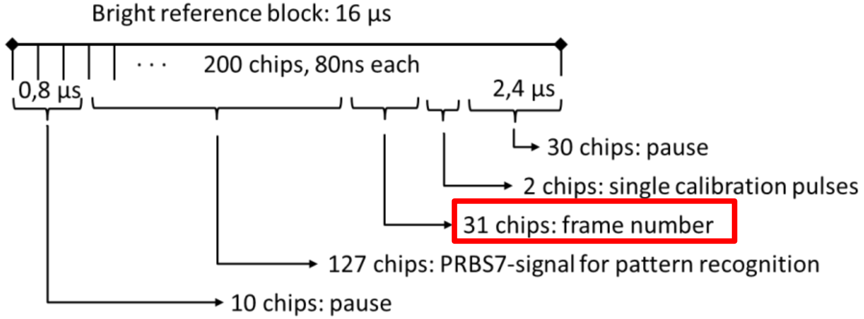
→ Bit synchronization with satellite without absolute time synchronization

Bright Reference Pulses



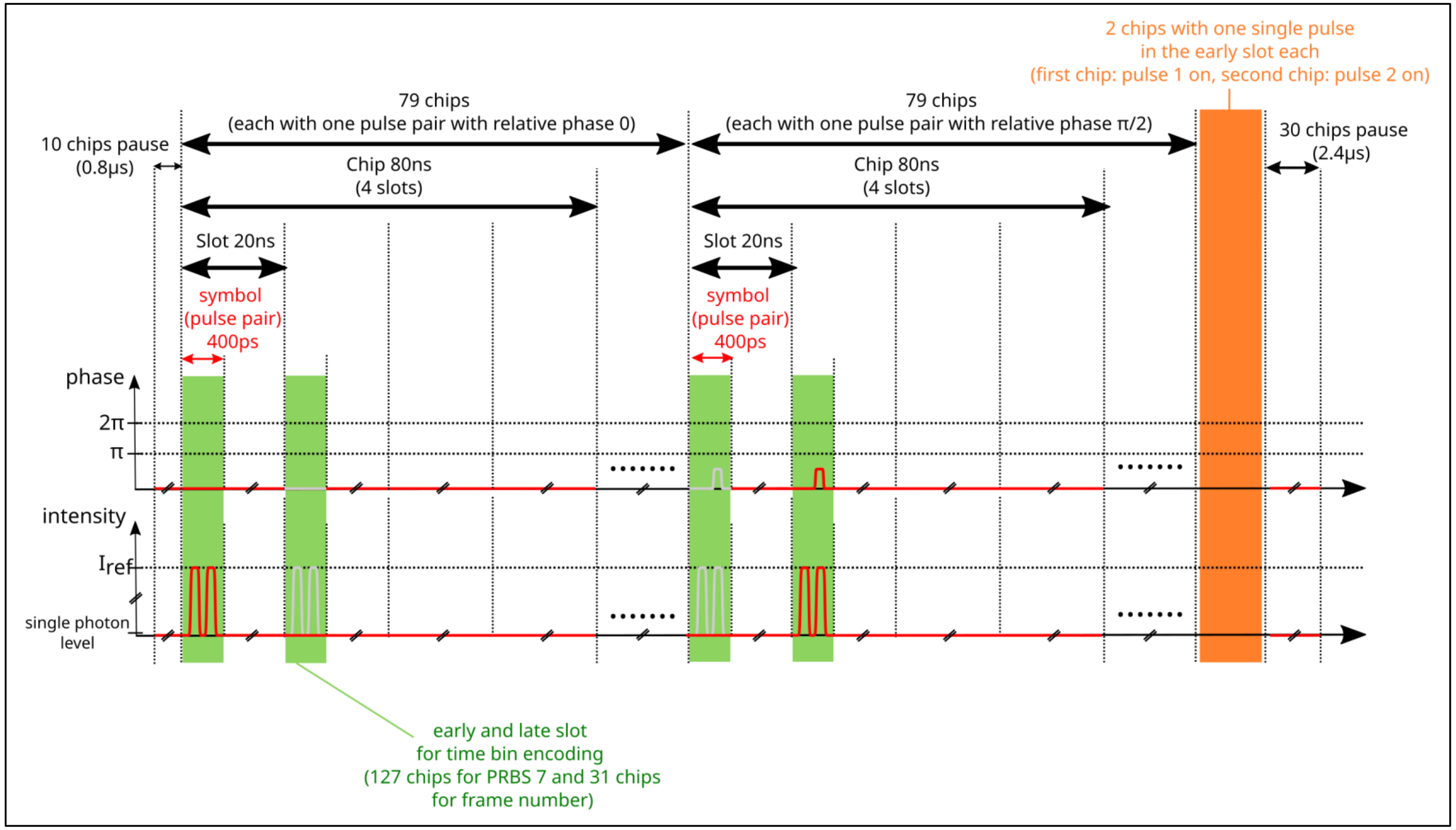
2. Frame Number PPM encoding:





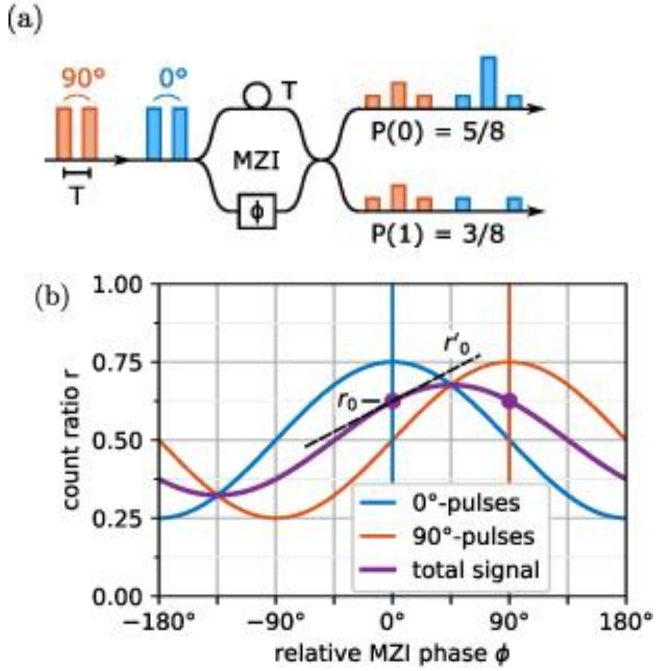
→ Bit synchronization with satellite without absolute time synchronization
(450000 quantum states per frame)

Bright Reference Pulses



[B. Hacker *et al* 2023 *New J. Phys.* **25** 113007]

3. Phase reference for locking :

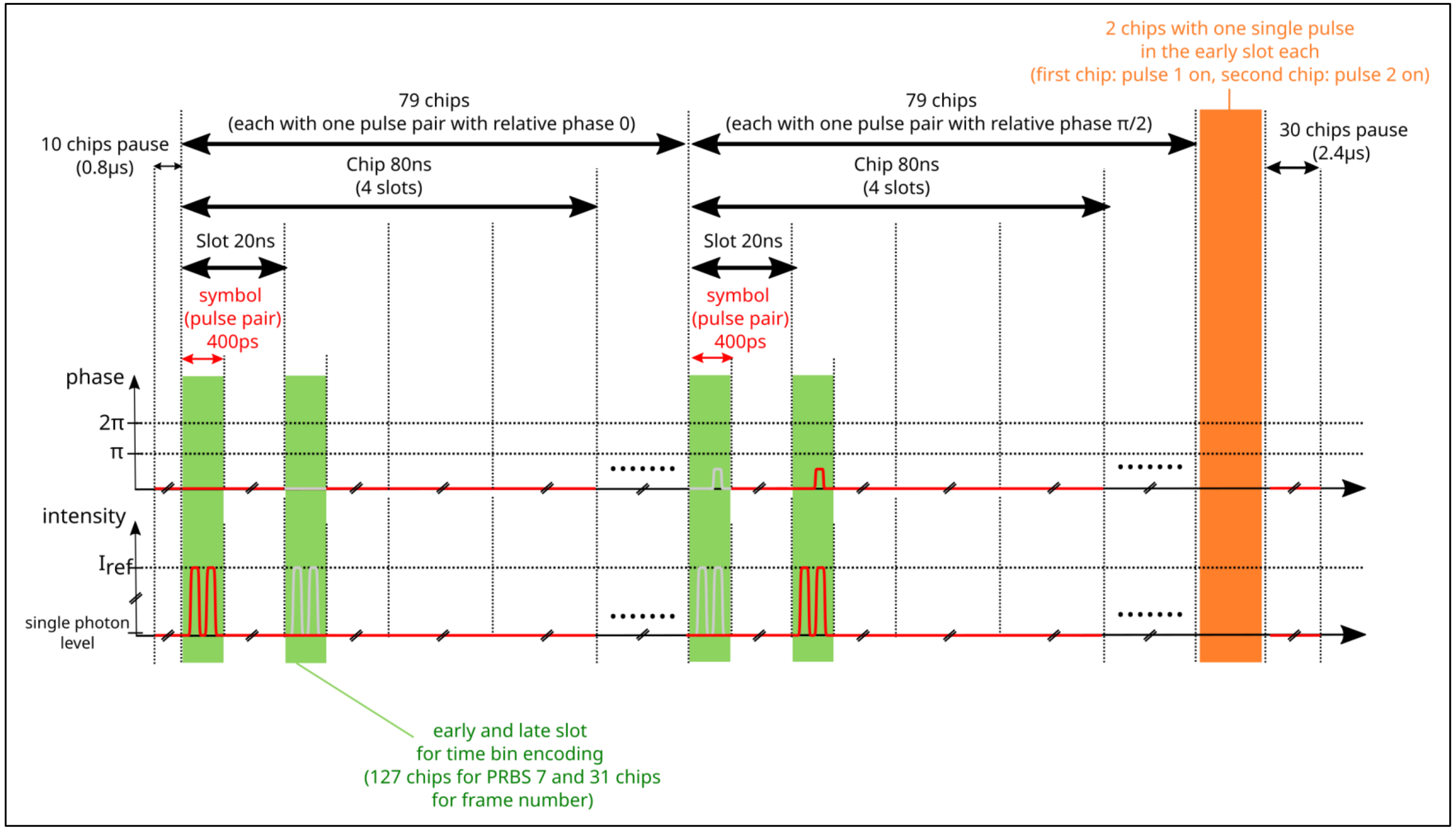


$r_0 = r(\phi_0)$ is the ratio of photons received in the first and second of two channels, respectively, for the desired phase ϕ_0

Locking points:

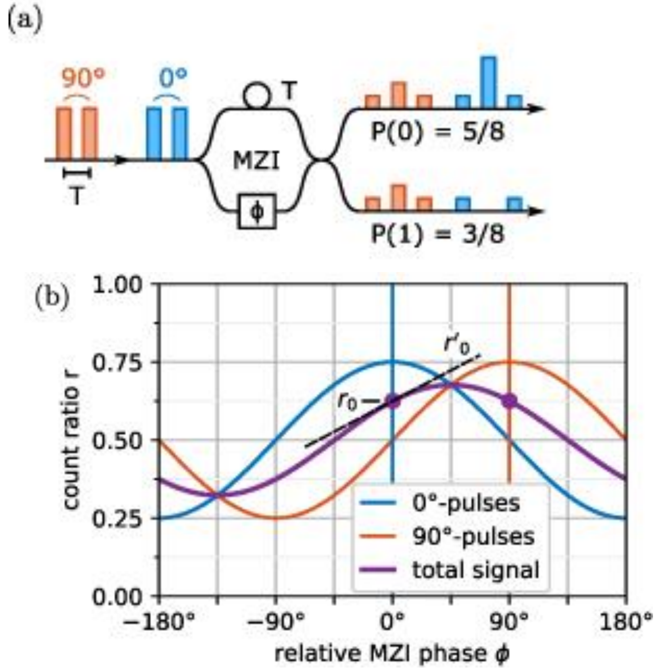
- $r_0 = 5/8$
- $\phi_0 = 0°$ → $r'_0 = +1/8$
- $\phi_0 = 90°$ → $r'_0 = -1/8$

Bright Reference Pulses



[B. Hacker *et al* 2023 *New J. Phys.* **25** 113007]

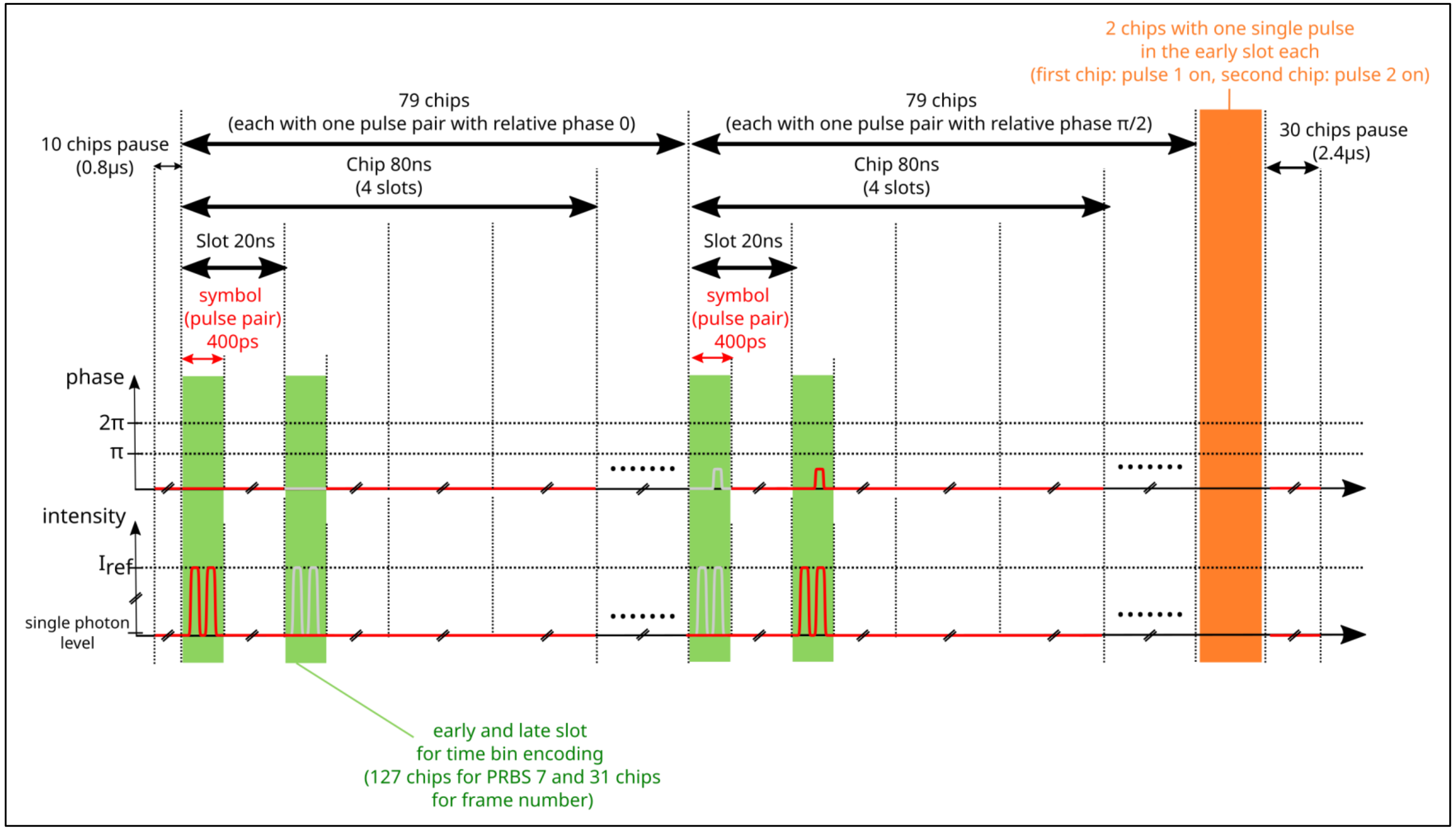
3. Phase reference for locking :



$r_0 = r(\phi_0)$ is the ratio of photons received in the first and second of two channels, respectively, for the desired phase ϕ_0

- Photon in channel 0: $\Delta\phi = \varepsilon_0 = 2\,\varepsilon\,(1-r_0)$
- Photon in channel 1: $\Delta\phi = \varepsilon_1 = -\,2\varepsilon\, r_0$

Bright Reference Pulses



[B. Hacker *et al* 2023 *New J. Phys.* **25** 113007]

3. Phase reference for locking :

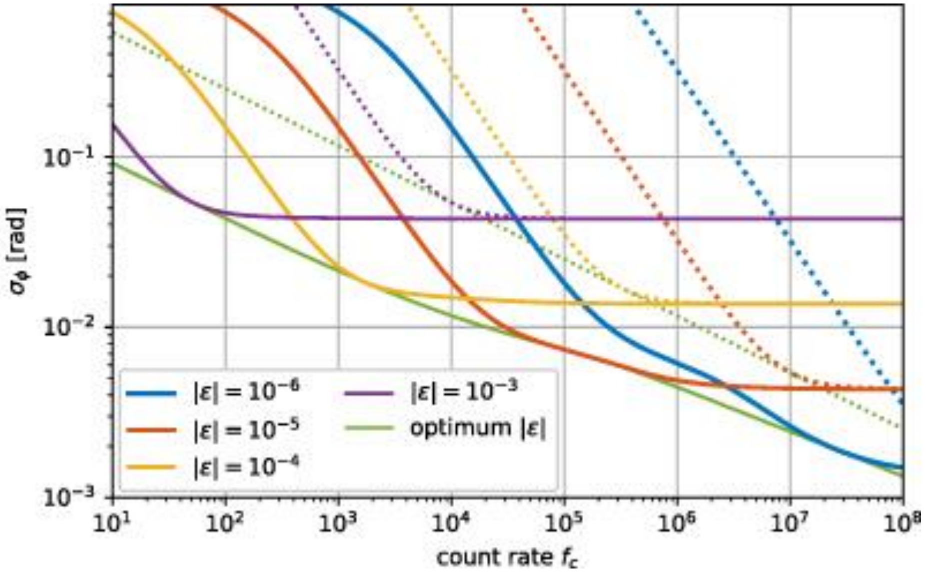
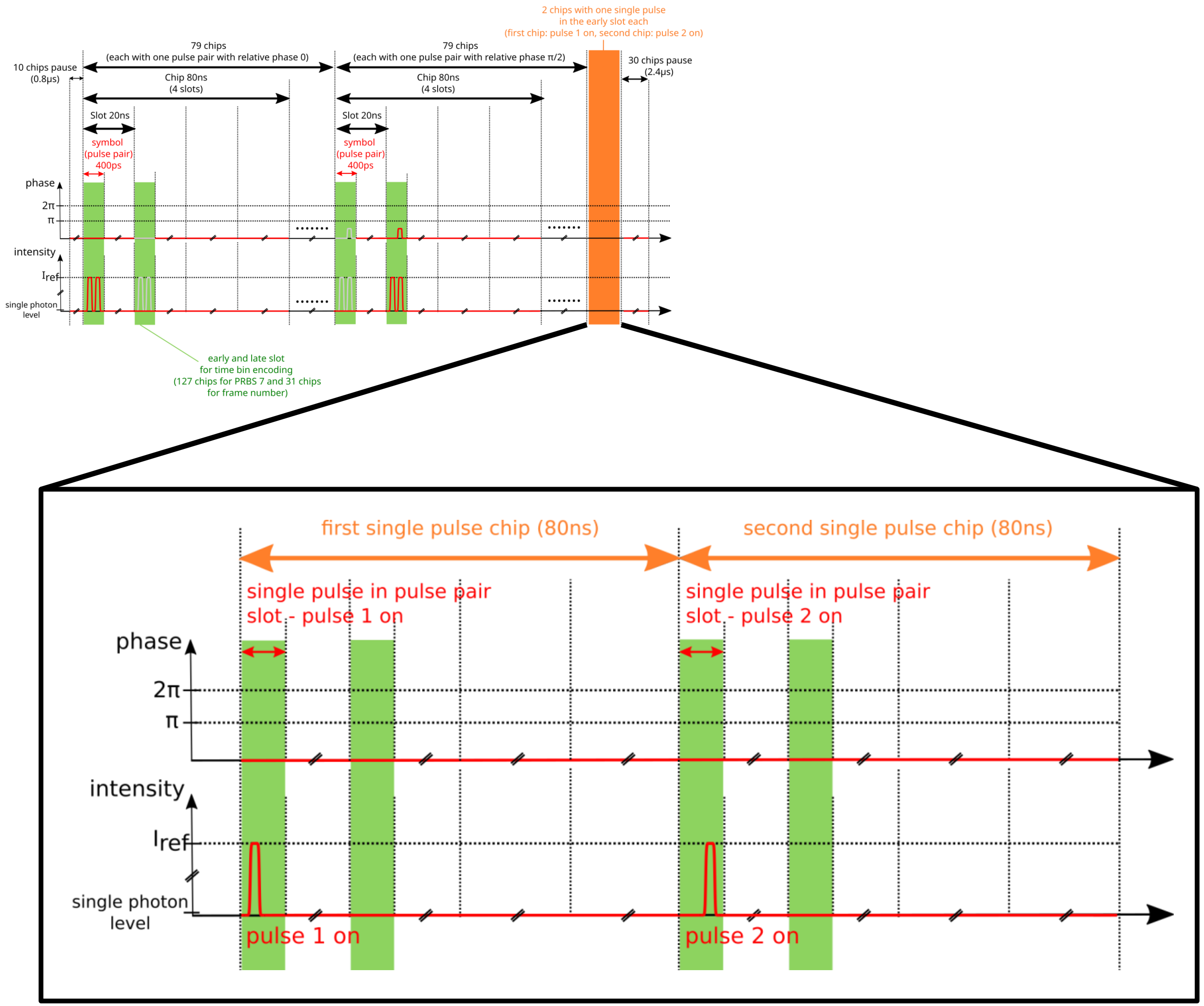
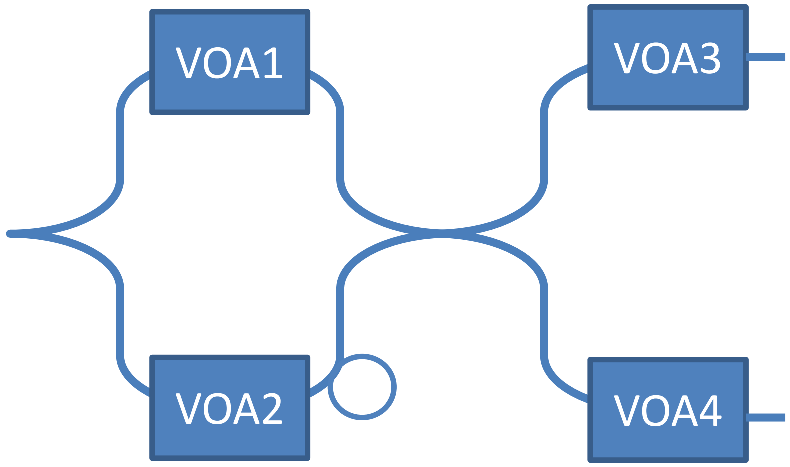


Figure 8. Phase error versus count rate f_c for various fixed values of the locking parameter $|\varepsilon|$. Curves are computed with (14) using the measured free drift spectrum, $r_0 = 5/8$ and $r'_0 = 1/8$. Solid lines are without external phase drift, dotted lines with linear external drift of d = 0.08 rad/s.

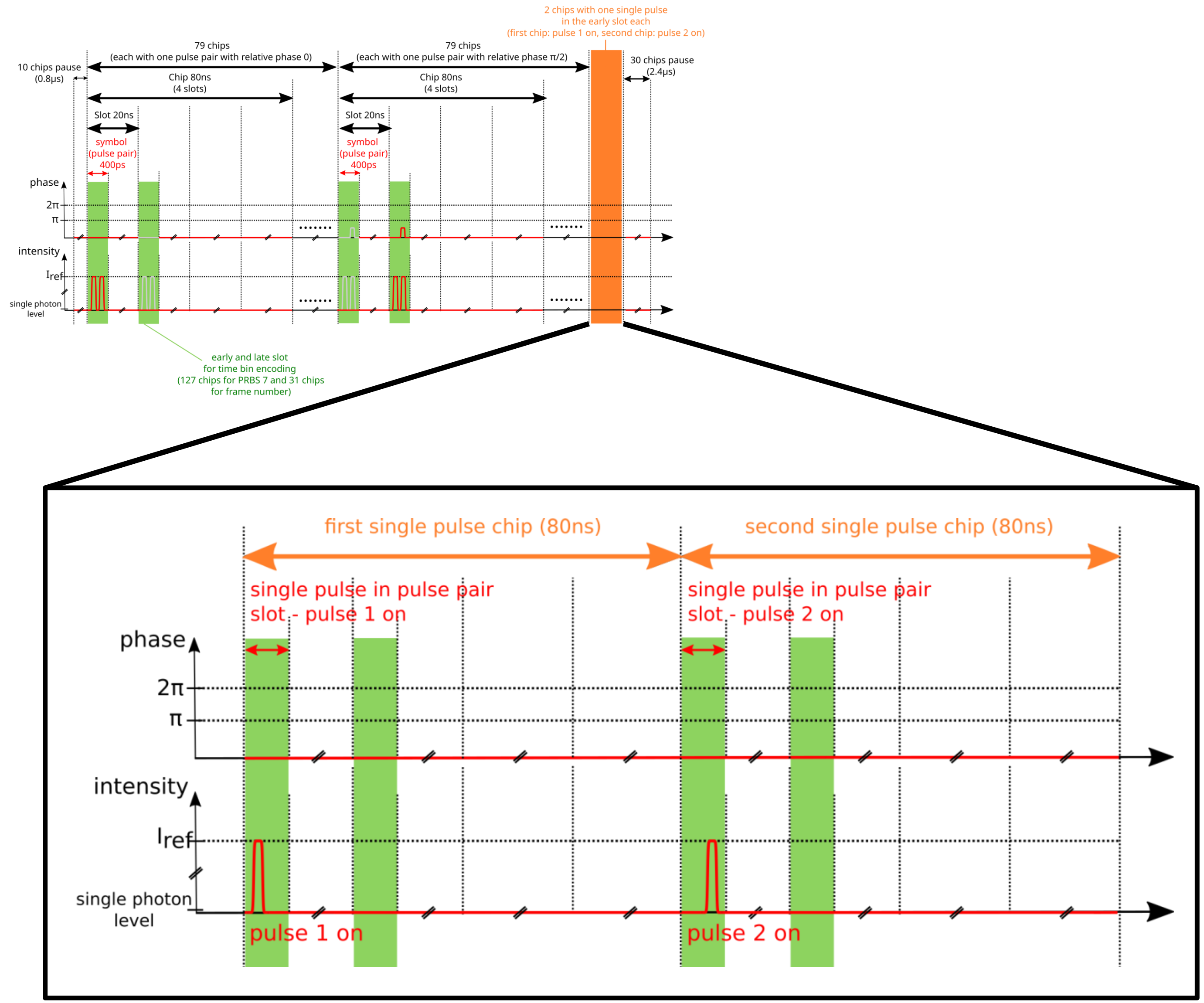
Bright Reference Pulses



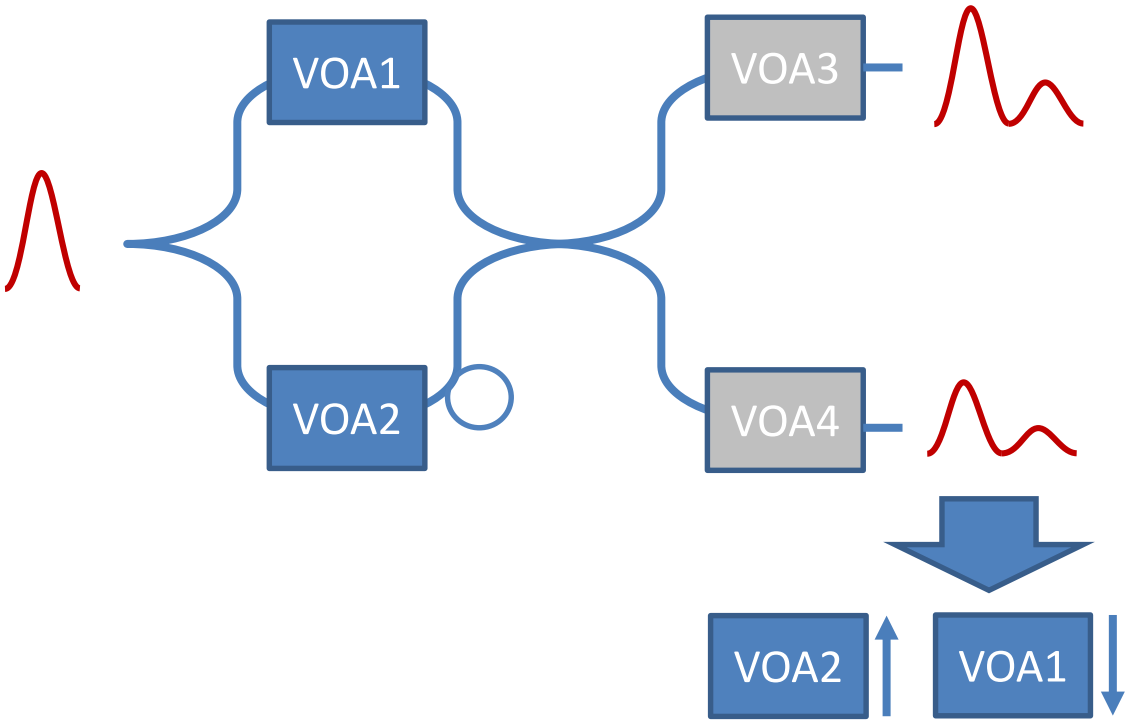
4. Single pulses:



Bright Reference Pulses

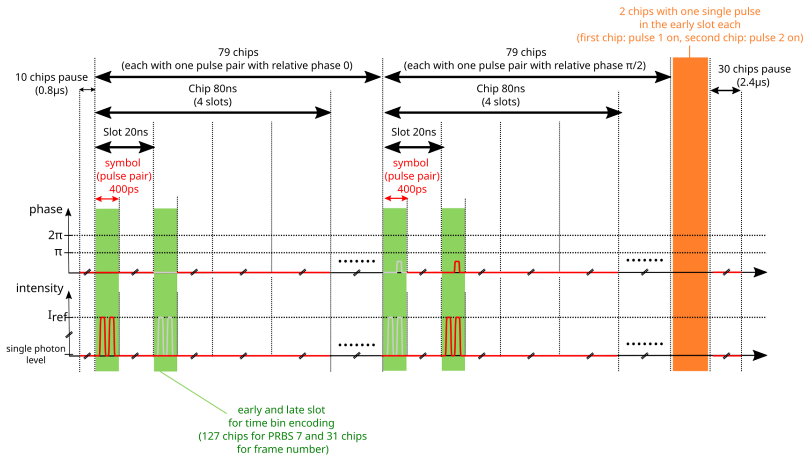


4. Single pulses:

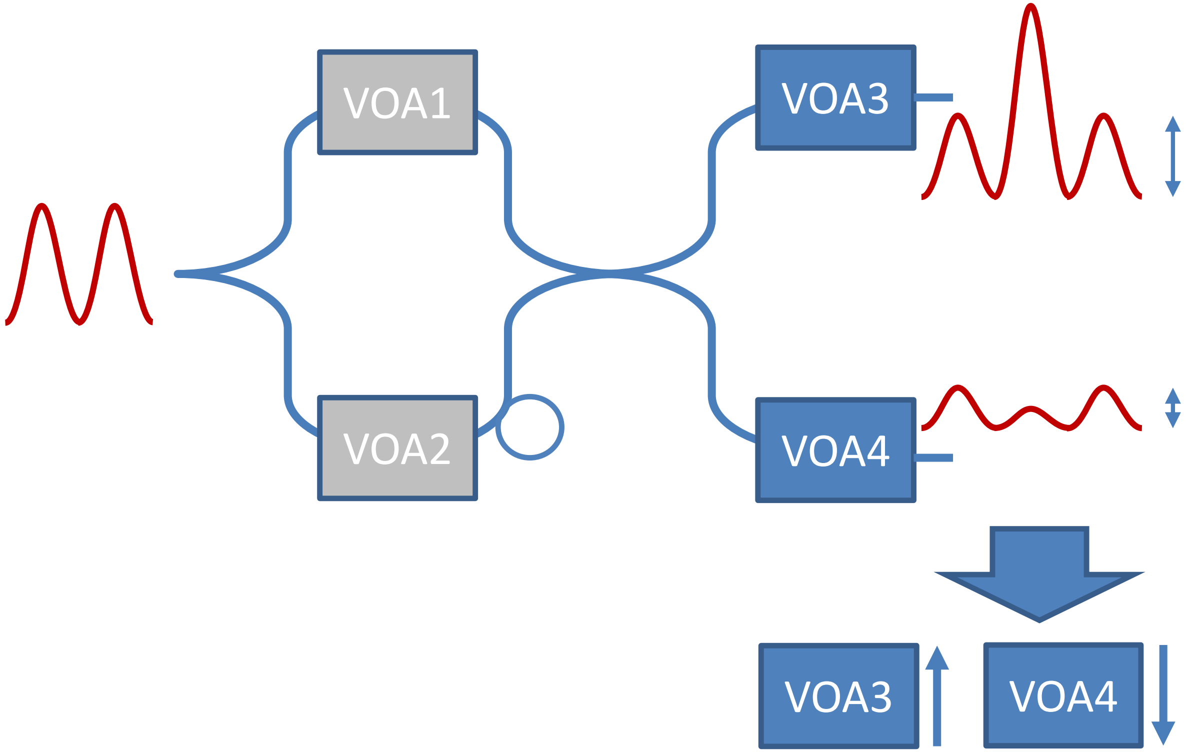


- Check if early/late pulse brighter
- Adjust VOAs in interferometer arms (VOA1/VOA2) until they match

Bright Reference Pulses



5. Side Peaks:



- Check ratio of side peak intensity (mid peak will differ!)
- Adjust VOAs after interferometer arms (VOA3/VOA4) until they match

Security Proof

BB84 Decoy State Protocol with relative phase encoding with two decoy states

- **Finite Size** Technique based on:
  Z. Zhang et al., "Improved key-rate bounds for practical decoy-state quantum-key-distribution systems," *Phys. Rev. A,* **95**, p. 012333, 2017.

- **Finite phase scrambling** method for first pulse in pair incorporated based on:
  Z. Cao et al., "Discrete-phase-randomized coherent state source and its application in quantum key distribution," *New Journal of Physics,* **17,** 5, p. 053014, 2015.

- **Intensity fluctuations** incorporated based on:
  Y. Wang et al., "Tight finite-key analysis of a practical decoy-state quantum key distribution with unstable sources," *Physical Review A,* **94**, 3, p. 032335, 2016.

- **Detector Efficiency Mismatch** incorporated based on:
  Y. Fei et al., "Practical decoy state quantum key distribution with detector efficiency mismatch," *The European Physical Journal D,* **72**, 6, p. 107, 2018.

- **Trojan Horse Attack** incorporated based on:
  M. Lucamarini et al., "Practical Security Bounds Against the Trojan-Horse Attack in Quantum Key Distribution," *Physical Review X,* **5**, p. 031030, 2015.

Security Proof – Key estimation

$$K^L = {M_1}^{x,L} \frac{2\,\eta_{DEM}}{1+\,\eta_{DEM}}\left[1 - H\left(\left[e_1^{zU} + \theta^x + \Lambda\left(e_1^{zU} + \theta^x, \Delta|_{DP,THA}^{x}\right)\right]\frac{1+\eta_{DEM}}{2\,\eta_{DEM}}\right)\right] + {M_1}^{z,L} \frac{2\,\eta_{DEM}}{1+\,\eta_{DEM}}\left[1 - H\left(\left[e_1^{xU} + \theta^z + \Lambda(e_1^{xU} + \theta^z, \Delta|_{DP,THA}^{z})\right]\frac{1+\eta_{DEM}}{2\,\eta_{DEM}}\right)\right] - M_\mu^x\, f\left(E_\mu^x\right) H\left(E_\mu^x\right) - M_\mu^z\, f\left(E_\mu^z\right) H\left(E_\mu^z\right),$$

Security Proof – Key estimation

$$K^L = M_1^{x,L}\frac{2\,\eta_{DEM}}{1+\,\eta_{DEM}}\left[1-H\left(\left[e_1^{zU}+\theta^x+\Lambda\left(e_1^{zU}+\theta^x,\Delta|_{DP,THA}^{x}\right)\right]\frac{1+\eta_{DEM}}{2\,\eta_{DEM}}\right)\right]+$$
$$M_1^{z,L}\frac{2\,\eta_{DEM}}{1+\,\eta_{DEM}}\left[1-H\left(\left[e_1^{xU}+\theta^z+\Lambda(e_1^{xU}+\theta^z,\Delta|_{DP,THA}^{z})\right]\frac{1+\eta_{DEM}}{2\,\eta_{DEM}}\right)\right]-$$
$$M_\mu^x\,f\left(E_\mu^x\right)H\left(E_\mu^x\right)\,-\,M_\mu^z\,f\left(E_\mu^z\right)H\left(E_\mu^z\right),$$

Key from X Basis

Security Proof – Key estimation

Palacký University Olomouc

$$K^{L} = M_1^{x,L} \frac{2\,\eta_{DEM}}{1+\eta_{DEM}} \left[1 - H\left(\left[e_1^{zU} + \theta^{x} + \Lambda\left(e_1^{zU} + \theta^{x}, \Delta|_{DP,THA}^{x}\right)\right] \frac{1+\eta_{DEM}}{2\,\eta_{DEM}}\right)\right] +$$
$$M_1^{z,L} \frac{2\,\eta_{DEM}}{1+\eta_{DEM}} \left[1 - H\left(\left[e_1^{xU} + \theta^{z} + \Lambda\left(e_1^{xU} + \theta^{z}, \Delta|_{DP,THA}^{z}\right)\right] \frac{1+\eta_{DEM}}{2\,\eta_{DEM}}\right)\right] -$$
$$M_\mu^{x} f\left(E_\mu^{x}\right) H\left(E_\mu^{x}\right) - M_\mu^{z} f\left(E_\mu^{z}\right) H\left(E_\mu^{z}\right),$$

Error estimated from Z Basis

Key from X Basis

Security Proof – Key estimation

$$K^L = M_1^{x,L} \frac{2\,\eta_{DEM}}{1+\eta_{DEM}} \left[1 - H\left(\left[e_1^{zU} + \theta^x + \Lambda\left(e_1^{zU} + \theta^x, \Delta|_{DP,THA}^{x}\right)\right] \frac{1+\eta_{DEM}}{2\,\eta_{DEM}}\right)\right] + M_1^{z,L} \frac{2\,\eta_{DEM}}{1+\eta_{DEM}} \left[1 - H\left(\left[e_1^{xU} + \theta^z + \Lambda\left(e_1^{xU} + \theta^z, \Delta|_{DP,THA}^{z}\right)\right] \frac{1+\eta_{DEM}}{2\,\eta_{DEM}}\right)\right] - M_\mu^x f(E_\mu^x) H(E_\mu^x) - M_\mu^z f(E_\mu^z) H(E_\mu^z),$$

Error estimated from Z Basis

Key from X Basis

Key from Z Basis

Error estimated from X Basis

Security Proof – Key estimation

Palacký University Olomouc

Estimated clicks from
Single photon contributions

$$K^L = M_1^{x,L} \frac{2\,\eta_{DEM}}{1+\,\eta_{DEM}}\left[1 - H\left(\left[e_1^{zU} + \theta^x + \Lambda\left(e_1^{zU} + \theta^x, \Delta|_{DP,THA}^{x}\right)\right]\frac{1+\eta_{DEM}}{2\,\eta_{DEM}}\right)\right] +$$
$$M_1^{z,L} \frac{2\,\eta_{DEM}}{1+\,\eta_{DEM}}\left[1 - H\left(\left[e_1^{xU} + \theta^z + \Lambda(e_1^{xU} + \theta^z, \Delta|_{DP,THA}^{z})\right]\frac{1+\eta_{DEM}}{2\,\eta_{DEM}}\right)\right] -$$
$$M_\mu^x\, f\left(E_\mu^x\right) H\left(E_\mu^x\right) - M_\mu^z\, f\left(E_\mu^z\right) H\left(E_\mu^z\right),$$

Error estimated from Z Basis

Key from X Basis

Key from Z Basis

Error estimated from X Basis

Security Proof – Key estimation

Estimated clicks from
Single photon contributions

Finite Size Deviation estimated
via Random Sampling Method

Error estimated
from Z Basis

Key from X Basis

$$K^{L} = M_1^{x,L} \frac{2\,\eta_{DEM}}{1+\,\eta_{DEM}}\left[1 - H\left(\left[e_1^{zU} + \theta^{x} + \Lambda(e_1^{zU} + \theta^{x}, \Delta|_{DP,THA}^{x})\right]\frac{1+\eta_{DEM}}{2\,\eta_{DEM}}\right)\right] +$$
$$M_1^{z,L} \frac{2\,\eta_{DEM}}{1+\,\eta_{DEM}}\left[1 - H\left(\left[e_1^{xU} + \theta^{z} + \Lambda(e_1^{xU} + \theta^{z}, \Delta|_{DP,THA}^{z})\right]\frac{1+\eta_{DEM}}{2\,\eta_{DEM}}\right)\right] -$$
$$M_\mu^{x}\, f(E_\mu^{x})\, H(E_\mu^{x}) - M_\mu^{z}\, f(E_\mu^{z})\, H(E_\mu^{z}),$$

Key from Z Basis

Error estimated
from X Basis

Security Proof – Key estimation

Estimated clicks from Single photon contributions

Finite Size Deviation estimated via Random Sampling Method

Error estimated from Z Basis

Key from X Basis

$$K^L = M_1^{x,L} \frac{2\,\eta_{DEM}}{1+\,\eta_{DEM}} \left[1 - H\left(\left[e_1^{zU} + \theta^x + \Lambda\left(e_1^{zU} + \theta^x, \Delta|_{DP,THA}^{x}\right)\right] \frac{1+\eta_{DEM}}{2\,\eta_{DEM}}\right)\right] +$$
$$M_1^{z,L} \frac{2\,\eta_{DEM}}{1+\,\eta_{DEM}} \left[1 - H\left(\left[e_1^{xU} + \theta^z + \Lambda\left(e_1^{xU} + \theta^z, \Delta|_{DP,THA}^{z}\right)\right] \frac{1+\eta_{DEM}}{2\,\eta_{DEM}}\right)\right] -$$
$$M_\mu^x\, f\left(E_\mu^x\right) H\left(E_\mu^x\right) - M_\mu^z\, f\left(E_\mu^z\right) H\left(E_\mu^z\right),$$

Key from Z Basis

Error estimated from X Basis

DEM = Detector Efficiency Mismatch

Security Proof – Key estimation

Estimated clicks from Single photon contributions

Finite Size Deviation estimated via Random Sampling Method

Error estimated from Z Basis

Key from X Basis

Key from Z Basis

Error estimated from X Basis

$$K^L = M_1^{x,L} \frac{2\,\eta_{DEM}}{1+\eta_{DEM}} \left[1 - H\left(\left[e_1^{zU} + \theta^x + \Lambda\left(e_1^{zU} + \theta^x, \Delta|_{DP,THA}^{x}\right)\right] \frac{1+\eta_{DEM}}{2\,\eta_{DEM}}\right)\right] + M_1^{z,L} \frac{2\,\eta_{DEM}}{1+\eta_{DEM}} \left[1 - H\left(\left[e_1^{xU} + \theta^z + \Lambda\left(e_1^{xU} + \theta^z, \Delta|_{DP,THA}^{z}\right)\right] \frac{1+\eta_{DEM}}{2\,\eta_{DEM}}\right)\right] - M_\mu^x f(E_\mu^x) H(E_\mu^x) - M_\mu^z f(E_\mu^z) H(E_\mu^z),$$

DEM = Detector Efficiency Mismatch

Discrete Phases, Trojan Horse Attack consideration

$$\Lambda(e_{p,1}, \Delta) = 4\,\Delta(1-\Delta)\,(1-2\,e_{p,1}) + 4(1-2\,\Delta)\sqrt{\Delta\,(1-\Delta)\,e_{p,1}\,(1-e_{p,1})}$$

where $\Delta|_{DP,THA} = \frac{1 - F_j e^{-\mu_{out}} \cos \mu_{out}}{2\,Y_1^L}$, $F_j \geq \left| \frac{\sum_{l=0}^{\infty} \frac{\mu^{lN_{DP}+j}}{(lN_{DP}+j)!} 2^{-\frac{lN_{DP}+j}{2}} \left(\cos\frac{lN_{DP}+j}{4}\pi + \sin\frac{lN_{DP}+j}{4}\pi\right)}{\sum_{l=0}^{\infty} \frac{\mu^{lN_{DP}+j}}{(lN_{DP}+j)!}} \right|$

Security Proof – Key estimation

Estimated clicks from Single photon contributions

Finite Size Deviation estimated via Random Sampling Method

Error estimated from Z Basis

Key from X Basis

Key from Z Basis

Error estimated from X Basis

Leak through Error Correction

$$K^L = M_1^{x,L} \frac{2\,\eta_{DEM}}{1+\eta_{DEM}} \left[1 - H\left(\left[e_1^{zU} + \theta^x + \Lambda\left(e_1^{zU} + \theta^x, \Delta|_{DP,THA}^{x}\right)\right] \frac{1+\eta_{DEM}}{2\,\eta_{DEM}}\right)\right] + M_1^{z,L} \frac{2\,\eta_{DEM}}{1+\eta_{DEM}} \left[1 - H\left(\left[e_1^{xU} + \theta^z + \Lambda\left(e_1^{xU} + \theta^z, \Delta|_{DP,THA}^{z}\right)\right] \frac{1+\eta_{DEM}}{2\,\eta_{DEM}}\right)\right] - M_\mu^x f(E_\mu^x) H(E_\mu^x) - M_\mu^z f(E_\mu^z) H(E_\mu^z),$$

DEM = Detector Efficiency Mismatch

Discrete Phases, Trojan Horse Attack consideration

$$\Lambda(e_{p,1}, \Delta) = 4\,\Delta(1-\Delta)\,(1-2\,e_{p,1}) + 4(1-2\,\Delta)\sqrt{\Delta\,(1-\Delta)\,e_{p,1}\,(1-e_{p,1})}$$

where $\Delta|_{DP,THA} = \frac{1 - F_j e^{-\mu_{out}} \cos \mu_{out}}{2\,Y_1^L}$, $F_j \geq \left| \frac{\sum_{l=0}^{\infty} \frac{\mu^{lN_{DP}+j}}{(lN_{DP}+j)!} 2^{-\frac{lN_{DP}+j}{2}} \left(\cos \frac{lN_{DP}+j}{4}\pi + \sin \frac{lN_{DP}+j}{4}\pi\right)}{\sum_{l=0}^{\infty} \frac{\mu^{lN_{DP}+j}}{(lN_{DP}+j)!}} \right|$

Security Proof – Key estimation

Estimated clicks from Single photon contributions

Finite Size Deviation estimated via Random Sampling Method

Error estimated from Z Basis

Key from X Basis

Key from Z Basis

Error estimated from X Basis

Leak through Error Correction

$$K^L = M_1^{x,L} \frac{2\,\eta_{DEM}}{1+\eta_{DEM}}\left[1 - H\left(\left[e_1^{zU} + \theta^x + \Lambda\left(e_1^{zU} + \theta^x, \Delta|_{DP,THA}^x\right)\right]\frac{1+\eta_{DEM}}{2\,\eta_{DEM}}\right)\right] +$$
$$M_1^{z,L} \frac{2\,\eta_{DEM}}{1+\eta_{DEM}}\left[1 - H\left(\left[e_1^{xU} + \theta^z + \Lambda\left(e_1^{xU} + \theta^z, \Delta|_{DP,THA}^z\right)\right]\frac{1+\eta_{DEM}}{2\,\eta_{DEM}}\right)\right] -$$
$$M_\mu^x\, f(E_\mu^x)\, H(E_\mu^x) - M_\mu^z\, f(E_\mu^z)\, H(E_\mu^z),$$

DEM = Detector Efficiency Mismatch

Discrete Phases, Trojan Horse Attack consideration

$$\Lambda(e_{p,1}, \Delta) = 4\,\Delta(1-\Delta)\,(1-2\,e_{p,1}) + 4(1-2\,\Delta)\sqrt{\Delta\,(1-\Delta)\,e_{p,1}\,(1-e_{p,1})}$$

where $\Delta|_{DP,THA} = \dfrac{1 - F_j e^{-\mu_{out}} \cos \mu_{out}}{2\,Y_1^L}$, $F_j \geq \left| \dfrac{\sum_{l=0}^{\infty} \frac{\mu^{lN_{DP}+j}}{(lN_{DP}+j)!} 2^{-\frac{lN_{DP}+j}{2}} \left(\cos\frac{lN_{DP}+j}{4}\pi + \sin\frac{lN_{DP}+j}{4}\pi\right)}{\sum_{l=0}^{\infty} \frac{\mu^{lN_{DP}+j}}{(lN_{DP}+j)!}} \right|$

implemented in QPS

Protocol Parameters

Parameter Name	Value	Notes
Sent states properties		
Bright reference pulses: pulse energy	0.67 fJ	peak power of 4.1875µW at satellite output for pulse pair on time of 160ps if rectangular pulses
Fluctuation of bright reference pulse intensity	±20%	
Bright reference pulse trains repetition rate	5 kHz	c.f. slides before
Symbol rate	2.25 GS/s	considering reference pulses, intermediate off times and the pair-wise encoding
Zero modulation between subsequent pulse pairs in quantum states	160 ps	c.f. slides before
Zero modulation in between the two pulses of a pulse pair	80 ps	c.f. slides before
QKD wavelength	1565.495864 nm	

Protocol Parameters

Parameter Name	Value	Notes
Sample sizes / QPS / error estimation		
Finite size sample size N_finite_size (per basis) – handled by QPS	16.5 x 10^5	• this is the number of Qbits that need to be detected on ground for both bases before the post-processing after sifting continues • is configurable • values of up to 27.5 x 10^5 can be beneficial depending on the link budget
Quantum receiver-QPS UDP interface	Each 108ms send: frame numbers, detected quantum state slots, bits and bases	detailed definition with exact datagram and format to be released
Error correction inefficiency f_EC	1.5	handled by QPS
Security parameter Epsilon	10^{-15}	handled by QPS, configurable

Protocol Parameters

Parameter Name	Value	Notes
Quantum states mean photon numbers/ bases		
Number of decoy states	2	
Mean photon number signal state (referred to as signal states)	0.63	The mean photon number refers to the symbol time slot of 400ps including one pulse pair
Mean photon number decoy state 1 (referred to as decoy states)	0.14	The mean photon number refers to the symbol time slot of 400ps including one pulse pair
Mean photon number decoy state 2 (referred to as vacuum states)	0.001	The mean photon number refers to the symbol time slot of 400ps including one pulse pair
Max. fluctuation of the mean photon numbers	2%	The jitter value δ has to be understood that the mean photon number μ is within an interval $[\mu*(1-\delta); \mu*(1+\delta)]$

Protocol Parameters

Parameter Name	Value	Notes
Probability for choosing the signal state	3/4	
Probability for choosing decoy state 1	3/16	
Probability for choosing decoy state 2	1/16	
Probability for choosing basis 1	0.5	
Probability for choosing basis 2	0.5	

Protocol Parameters

Parameter Name	Value	Notes
Quantum Receiver		
Intrinsic protocol loss	3dB	Is to be applied in software by throwing away the side peaks (c.f. slides before)
Maximum optical loss receiver	7dB	
Temporal filtering window (done in software)	120ps - 40ps	Configurable value that reduces the influence of the background counts on the QBER
Loss due to temporal filter	0.2dB – 4dB	
Visibility interferometers	98% ± 1%	
Detector dead time	80ns	This is especially important for the reference pulses
Entrance filter bandwidth at classical communication wavelength	0.3nm	c.f. slides before

Protocol Parameters

Parameter Name	Value	Notes
System requirements		
Error probability optical system	1.5%	
Timing jitter overall system	50ps	FWHM value
Maximum overall phase jitter	$\pi/50$	
Polarization extinction ratio receiver entrance	-20 dB or better	c.f. ICD already released

Protocol Parameters

Parameter Name	Value	Notes
Background light		
Maximum background counts impinging of entrance fiber receiver	• 800 Hz or -129.9 dBm in Quantum channel In-band • 1000 Hz or -128.9 dBm Quantum channel out-of-band	c.f. slides before
Upper limit receiver detector background counts per detector	75 Hz	This value includes intrinsic dark counts as well as background light contributions

Conclusion

- BB84 decoy protocol with relative phase encoding for EAGLE-1, the first European satellite QKD mission

- Besides the quantum state exchange used for key creation two additional time multiplexed parts:
  dark and bright reference pulses

Live reference QBER

- Clock recovery → see talk of Conrad Rößler
- Frame number encoding for synchronization with satellite (no absolute time synchronization required)
- Phase locking and interferometer balancing on ground

- quantum signal train is self-contained and requires no additional reference signals for QKD operation

- Security proof on rigorous finite-size techniques extended by several security aspects of the practical implementation

[Scientific publication in preparation]

With funding by the European Space Agency and by the European Union

Thank you for your attention!

Questions?

Gefördert durch
Bayerisches Staatsministerium für Wirtschaft, Landesentwicklung und Energie