Centre for Quantum Technologies

NUS National University of Singapore

Entanglement-based Free Space Quantum Cryptography in Daylight

Antía Lamas-Linares, Matthew P. Peloso, Ilja Gerhardt, Caleb Ho and Christian Kurtsiefer

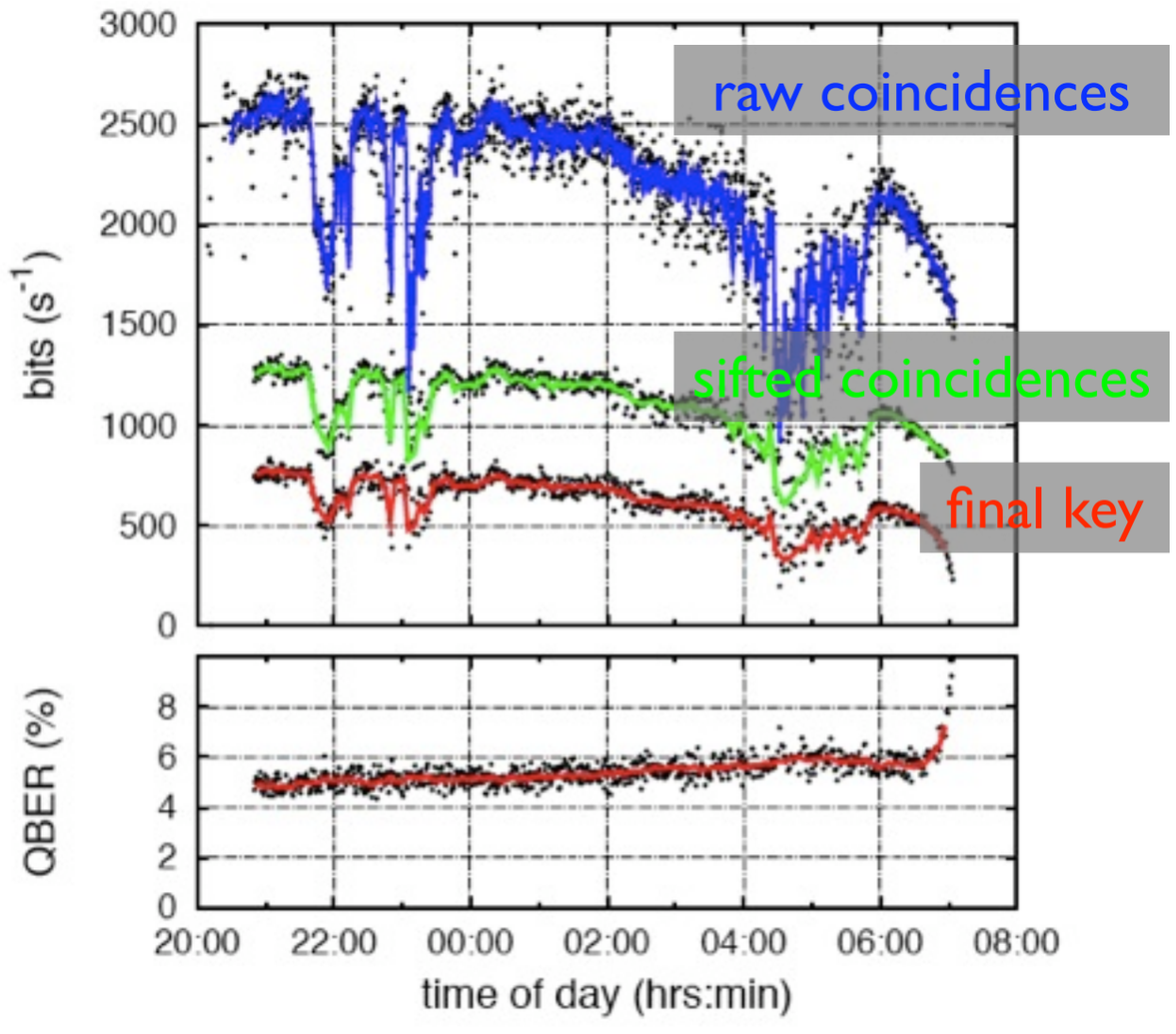
DAMOP 2009, Charlottesville, VA

Why free space? Why entanglement?

- Ad hoc setups (travel: 23C3, BlackHat and DEFCON)
- Does not need preexisting fiber infrastructure
- Satellites

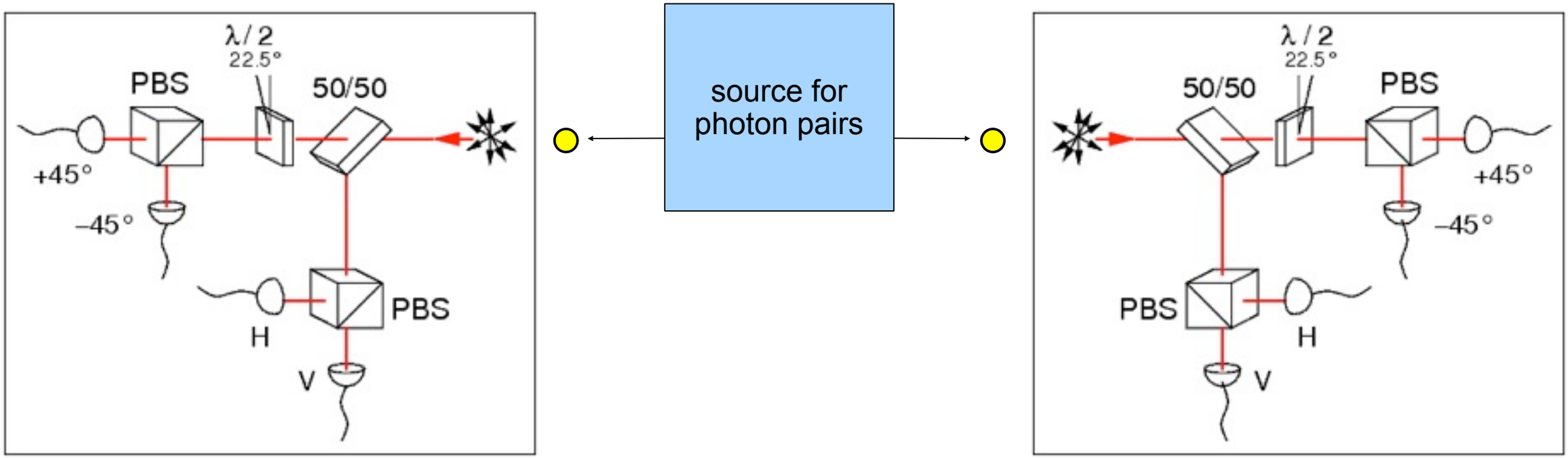
- Does not need a high bandwidth source of random numbers (*)
- Can be used for “device independent” protocols where security does not rely on a trusted measuring box (*)

BBM92 Results

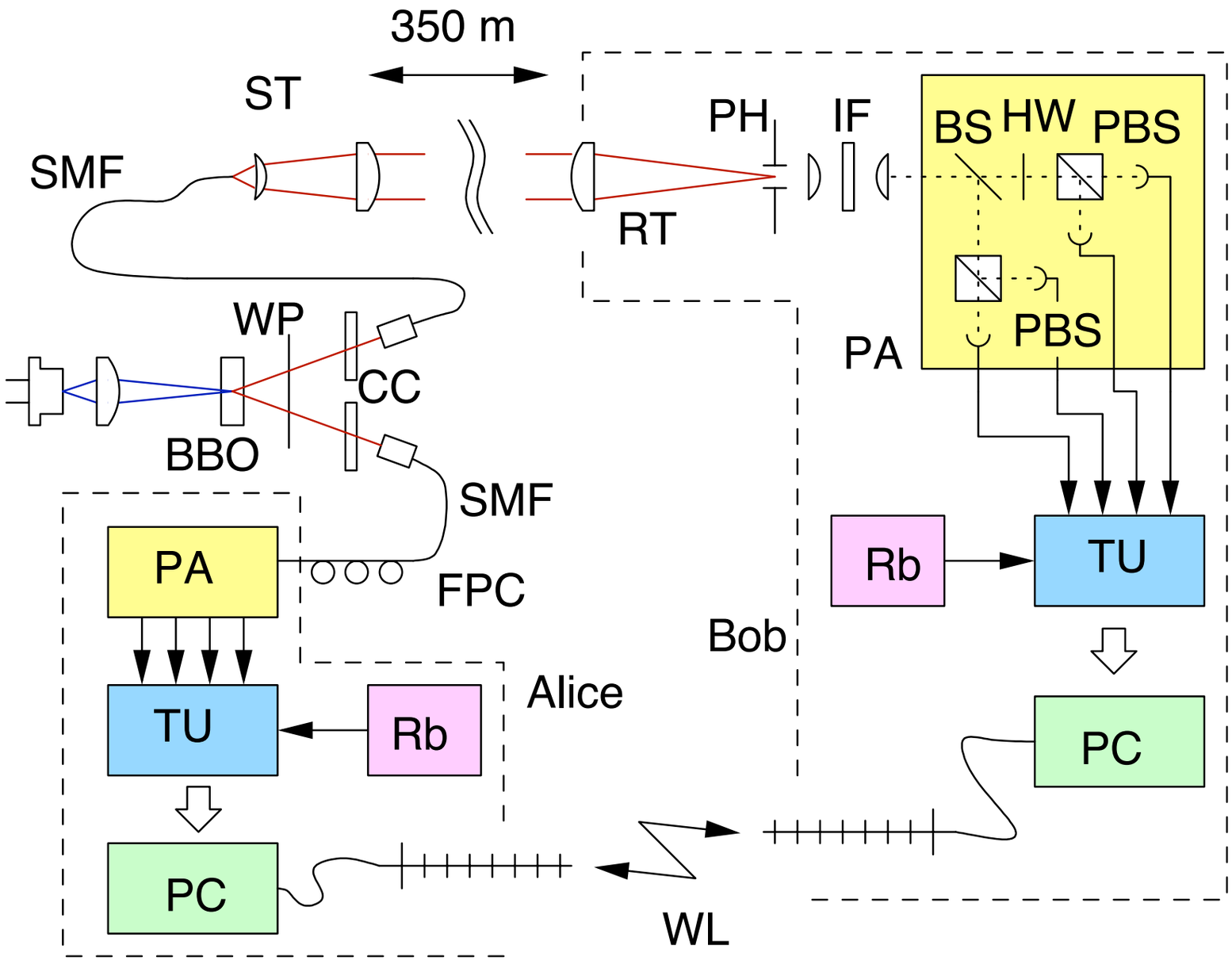


APL 89, 101122 (2006)

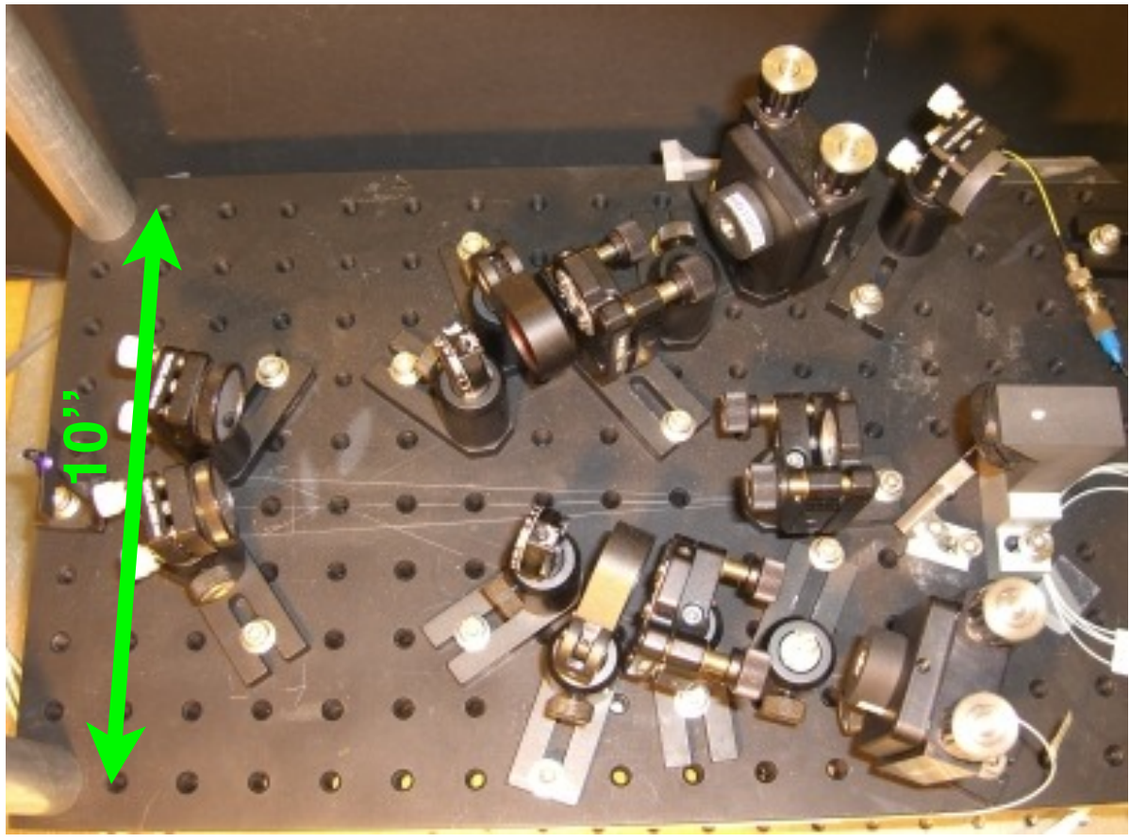
Basic Setup

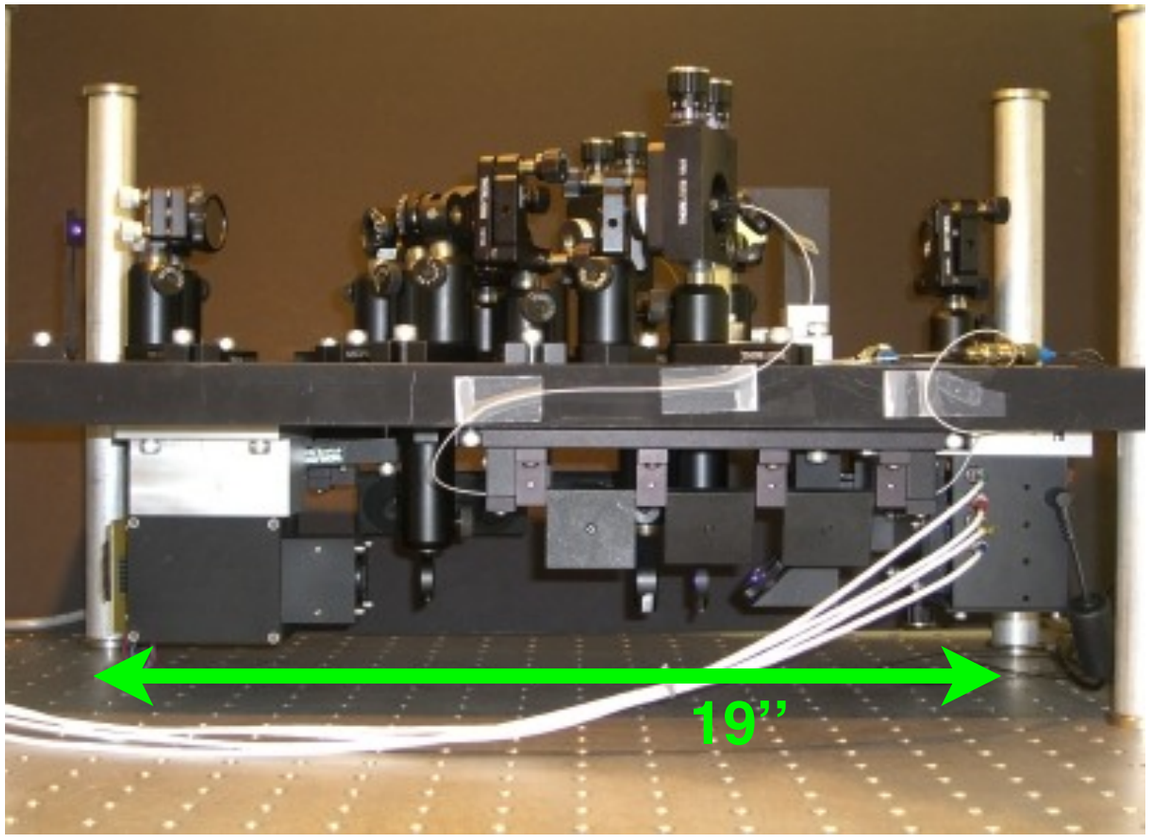

λ / 2
22.5°
PBS
50/50
+45°
–45°
H
PBS
V
source for
photon pairs
λ / 2
22.5°
50/50
PBS
+45°
–45°
PBS
H
V

Basic Setup


350 m
ST
SMF
PH
IF
BS
HW
PBS
RT
WP
CC
PBS
PA
BBO
SMF
PA
FPC
Rb
TU
Alice
Bob
TU
Rb
PC
PC
WL

Entanglement source



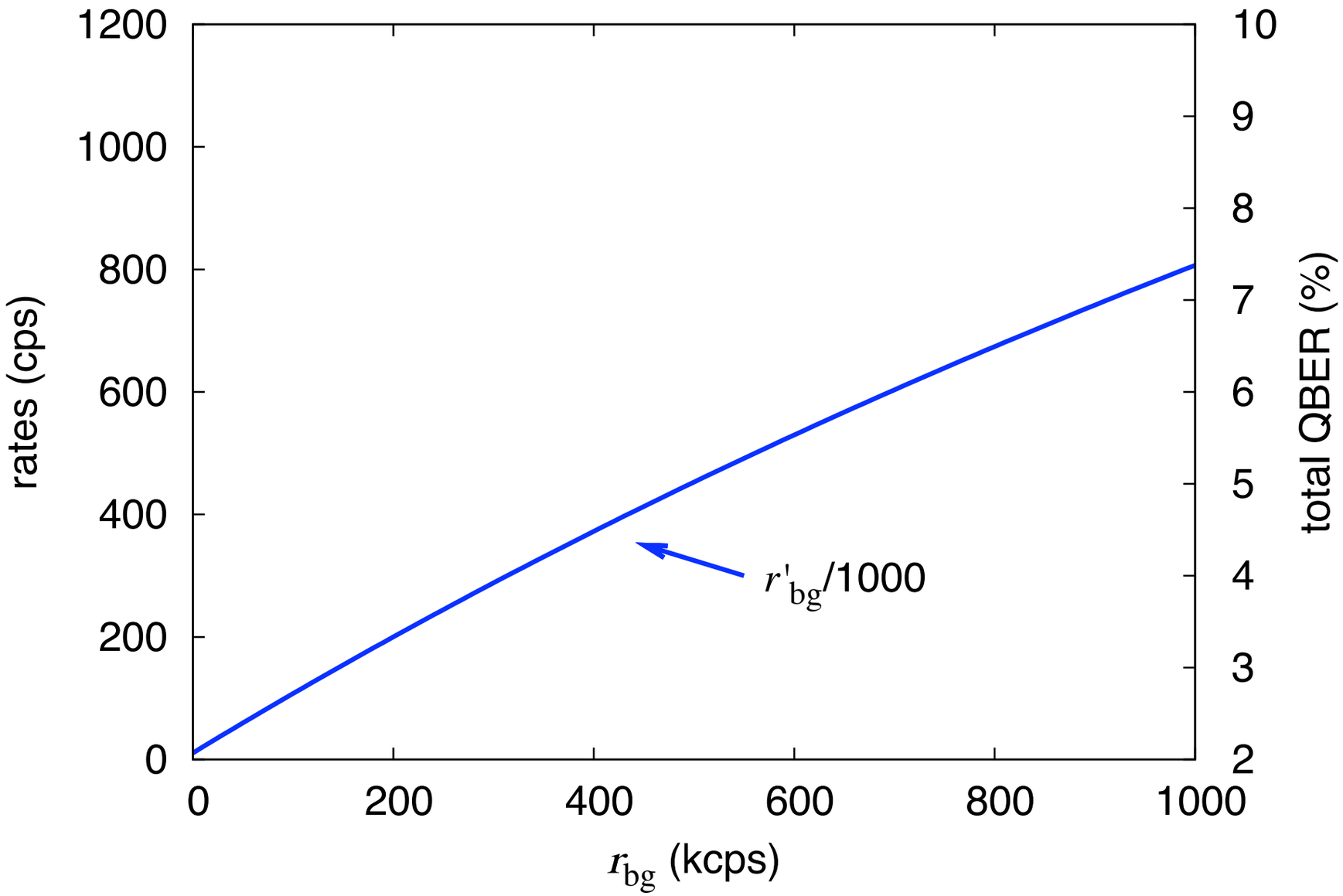


- “classic” type-II crossed ring configuration, 2 mm BBO, 30mW pump@407
- 71k s^{-1} and 78k s^{-1} singles per arm into single mode fibers
- 12k s^{-1} detected pairs from 30 mW pump @ 407nm into single mode fibers
- polarization visibility in H/V and 45° basis: 97% and 92%
- optical bandwidth 8.7 nm FWHM
- small footprint, works in outdoor conditions (30 degrees, 90% humidity)

Now there are better PDC sources for this purpose. PPKTP sources exhibit much higher rates and narrower spectral features. [Fedrizzi et al, Opt. Express 15, 15377 (2007)].

Bright light effects

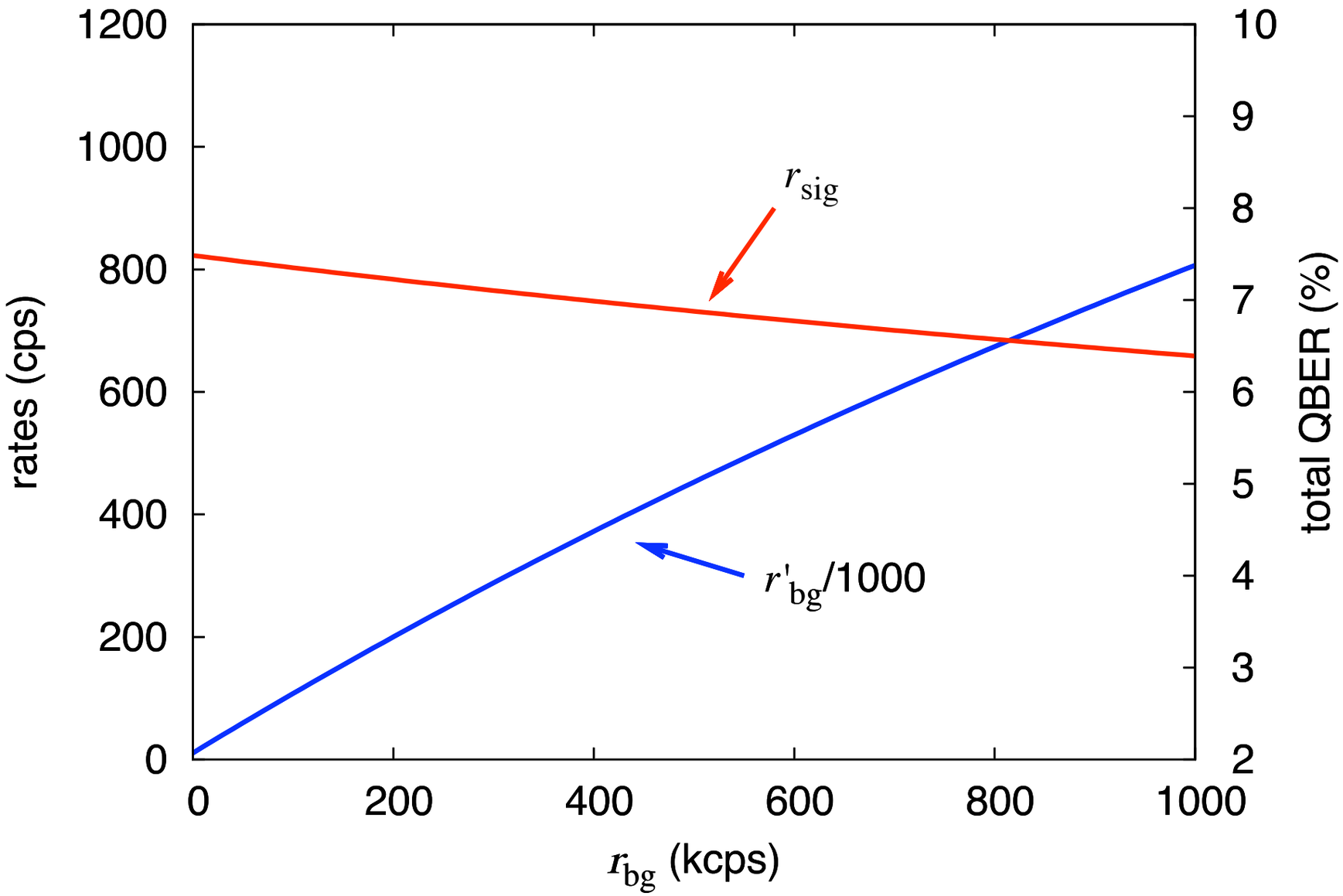
- For all detector types -> saturation
- For actively quenched detectors -> death
- Passively quenched detectors can survive but relatively quickly saturate
- Saturation reduces the probability of detecting the “true” pairs
- Accidental coincidences increase the QBER and can prevent key production



Given the dead time of the detectors (1μs) and a coincidence time window essentially fixed by the jitter (~1ns), our only option is to reduce the background

Bright light effects

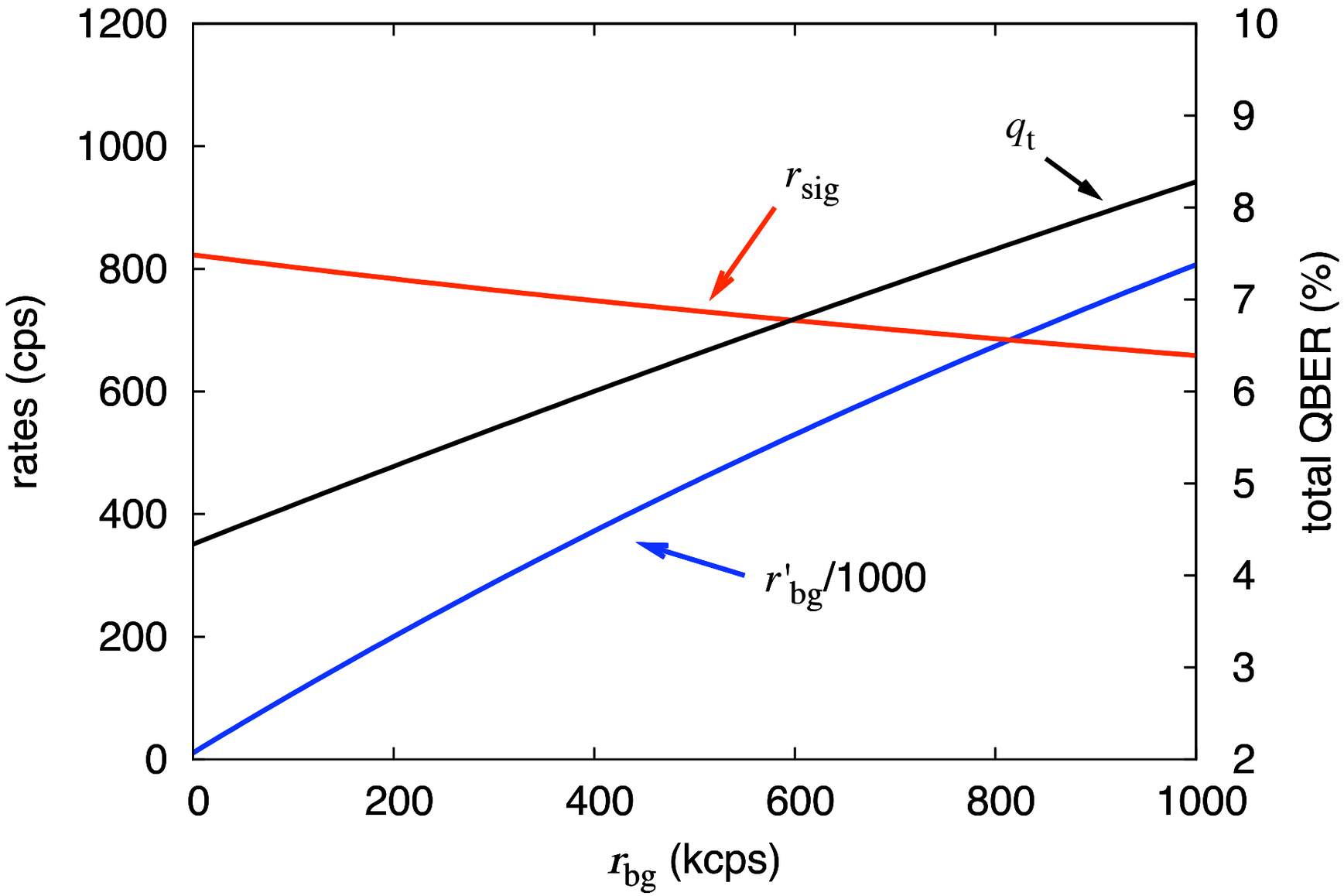
- For all detector types -> saturation
- For actively quenched detectors -> death
- Passively quenched detectors can survive but relatively quickly saturate
- Saturation reduces the probability of detecting the “true” pairs
- Accidental coincidences increase the QBER and can prevent key production



Given the dead time of the detectors (1μs) and a coincidence time window essentially fixed by the jitter (~1ns), our only option is to reduce the background

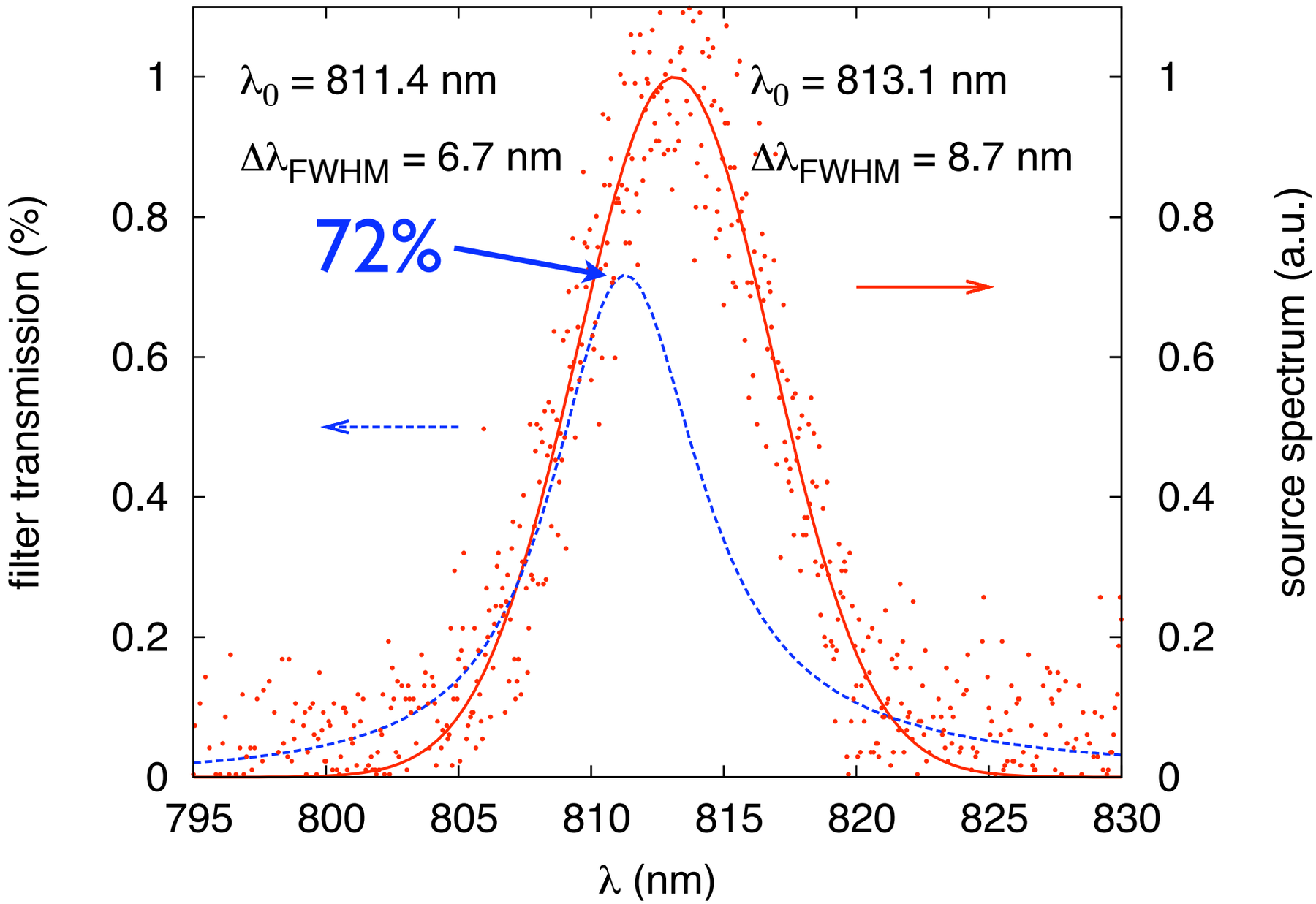
Bright light effects

- For all detector types -> saturation
- For actively quenched detectors -> death
- Passively quenched detectors can survive but relatively quickly saturate
- Saturation reduces the probability of detecting the “true” pairs
- Accidental coincidences increase the QBER and can prevent key production



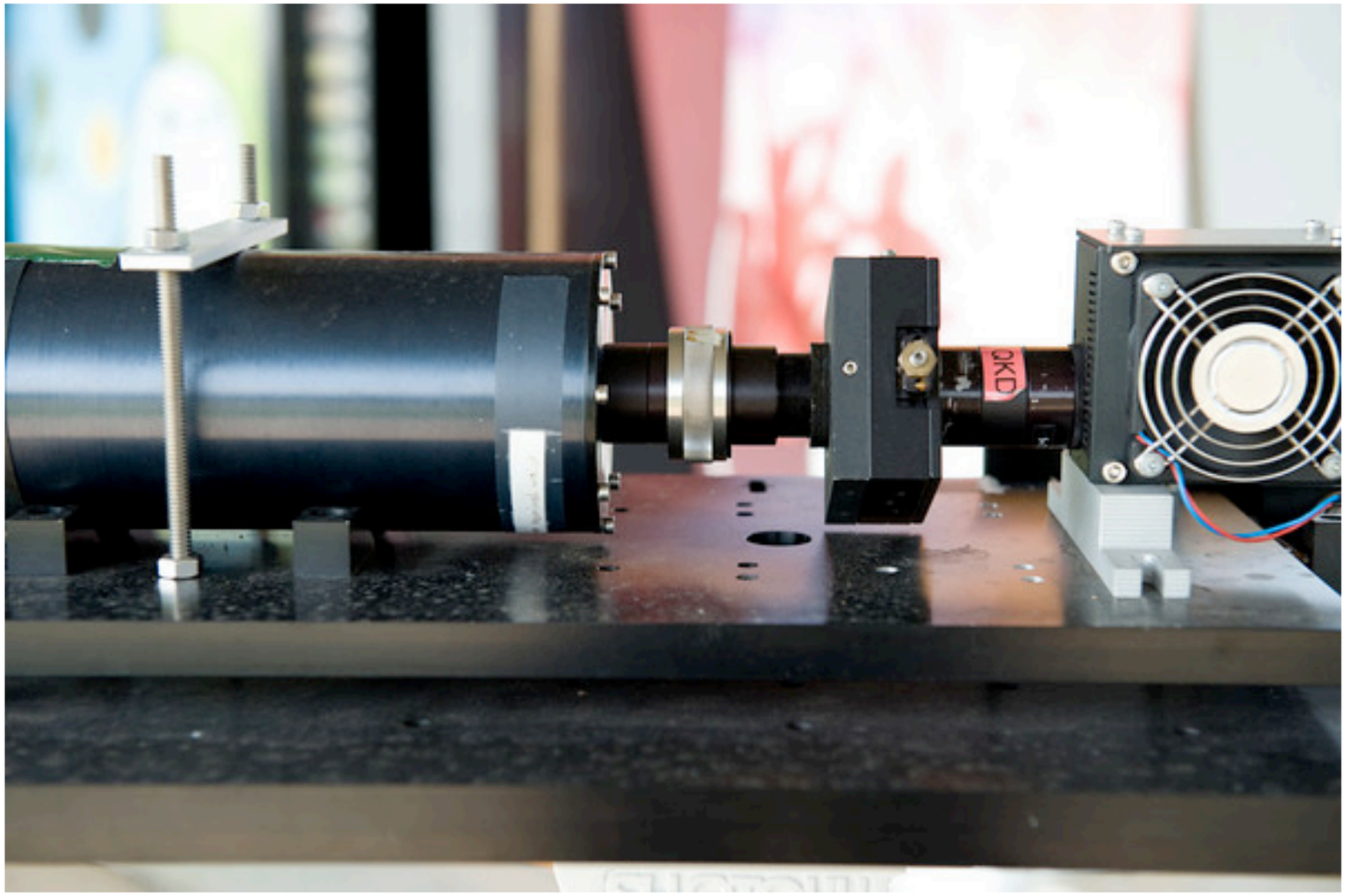
Given the dead time of the detectors (1μs) and a coincidence time window essentially fixed by the jitter (~1ns), our only option is to reduce the background

Spectral filtering: filters matched to PDC source



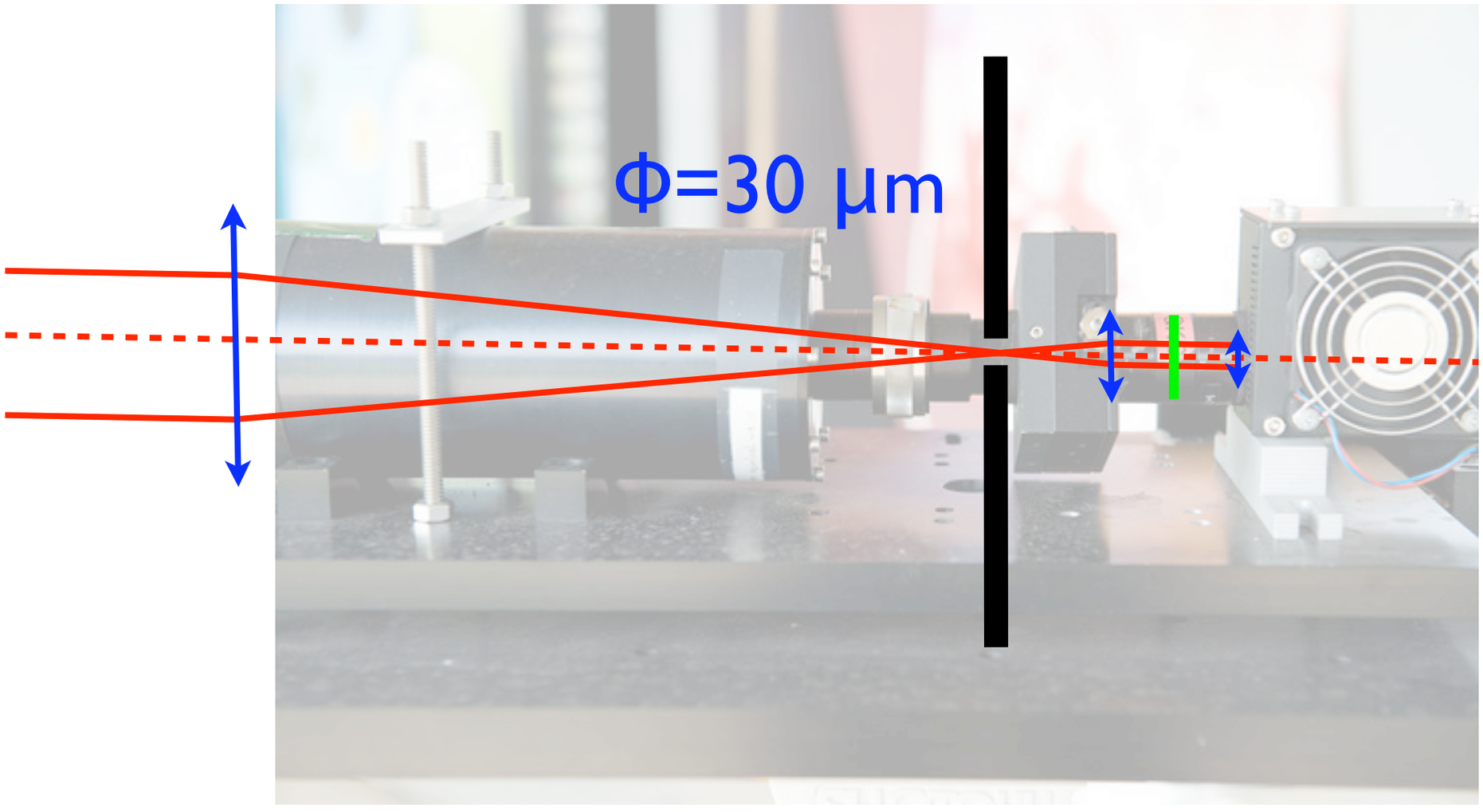
- Background reduced by a factor ~100
- Signal transmission 57%

Spatial filtering: pinhole at focus position + baffles + shading and blackout material



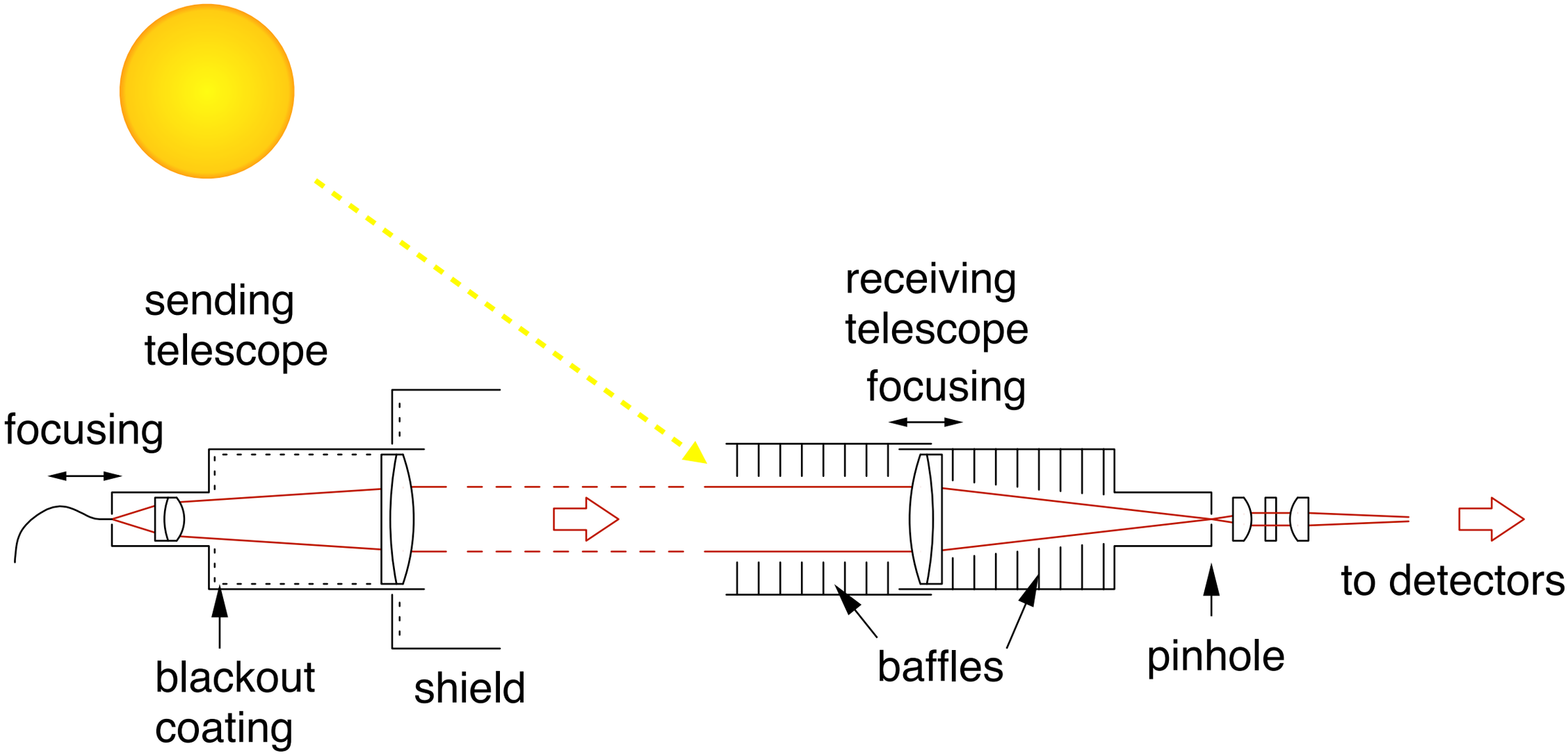
- pinhole+shading ~12 dB reduction in background. Signal unaffected.
- tapered apertures ~3-4 dB reduction in background. Signal unaffected.

Spatial filtering: pinhole at focus position + baffles + shading and blackout material

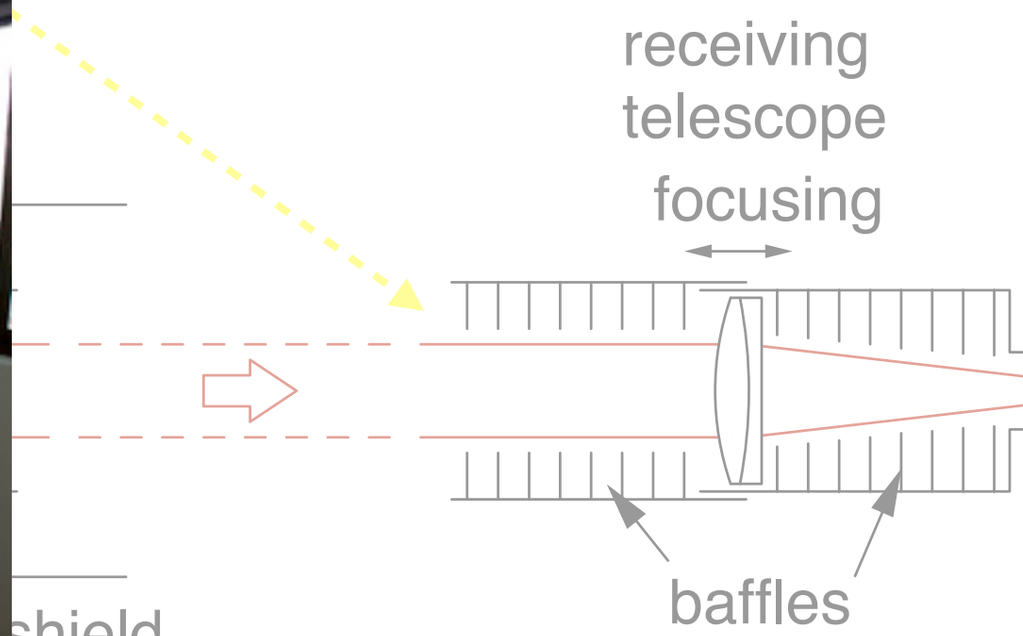


- pinhole+shading ~12 dB reduction in background. Signal unaffected.
- tapered apertures ~3-4 dB reduction in background. Signal unaffected.

Where: Across the sports field at NUS

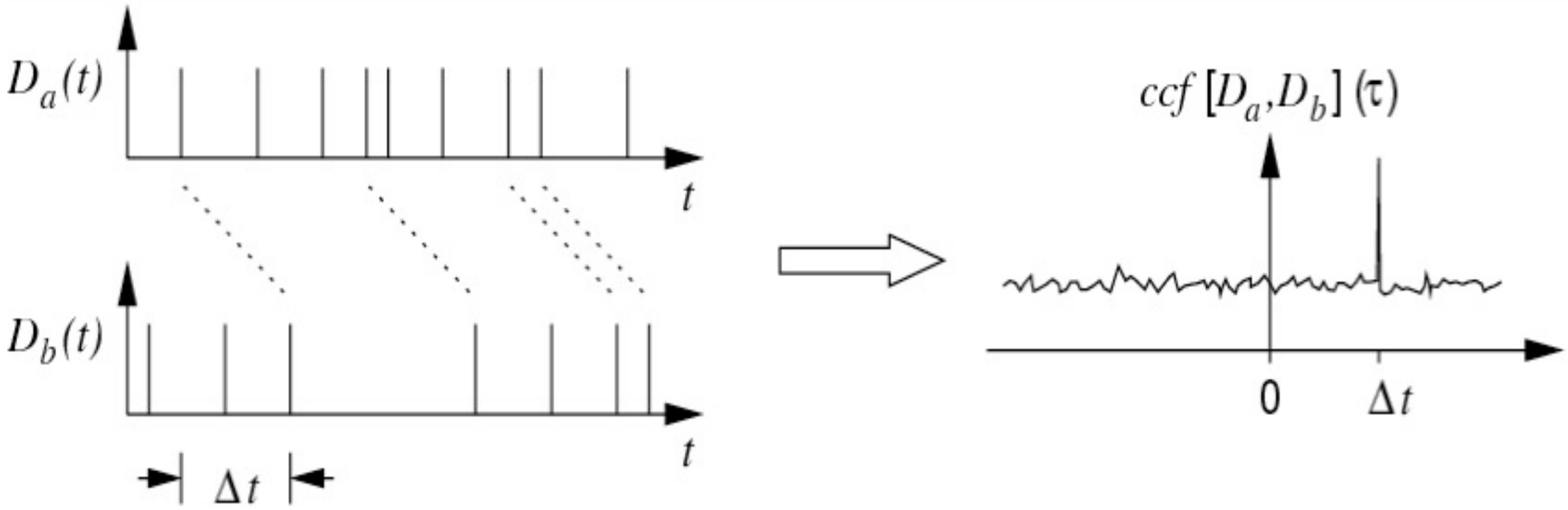


Where: Across the sports field at NUS



A few more things to note are the antennas (classical comms) and the tripods (passive stability)

Synchronization and time filtering

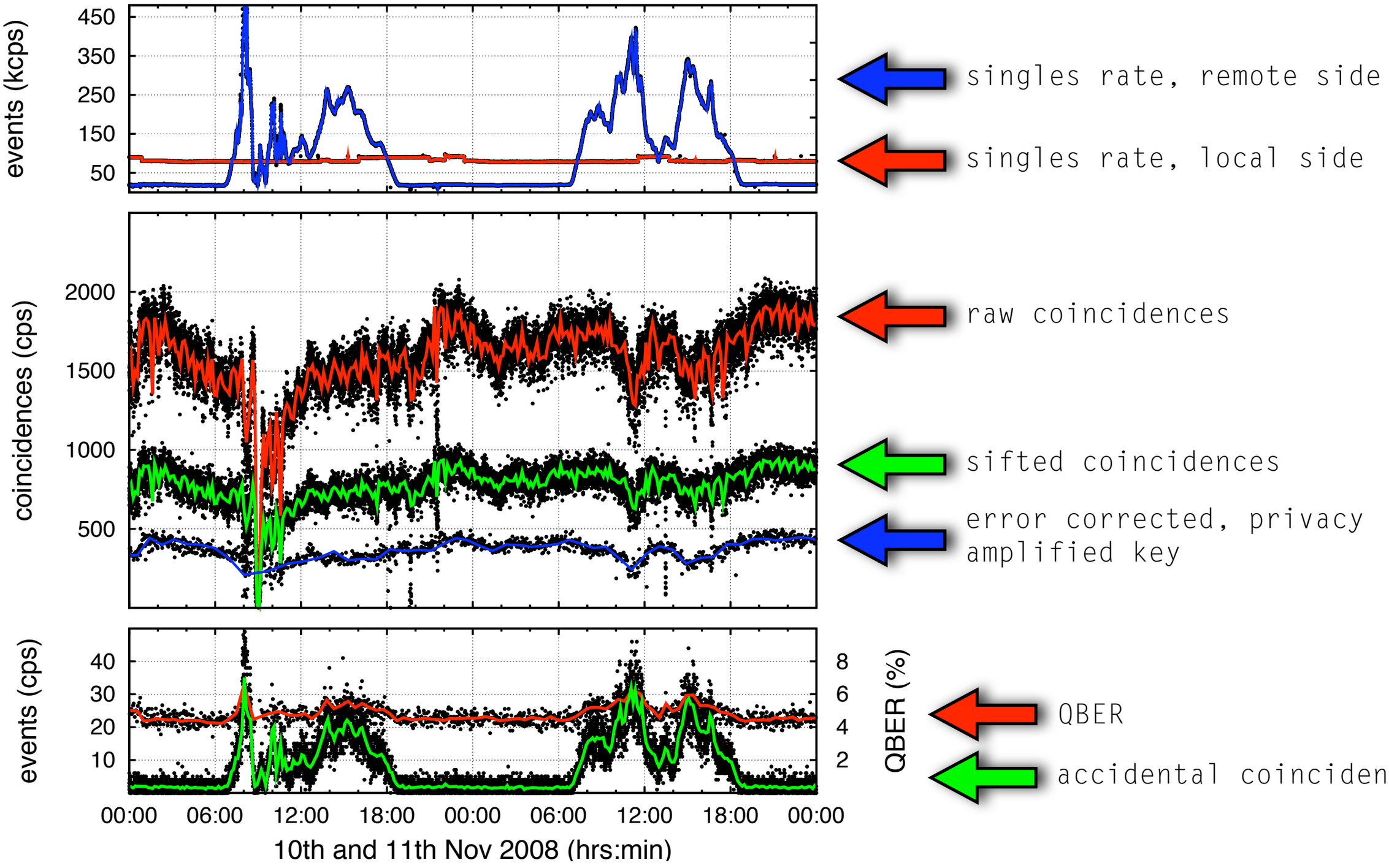


Both sides are synchronized using the intrinsic correlations of the PDC process. An atomic clock is used for ~5 s to get the initial synchronization. Subsequently a feedback loop adjusts the coincidence window to follow the clock drift.

Coincidence time window adjusted to the intrinsic jitter of the detectors. Background diminishes linearly with size of coincidence window.

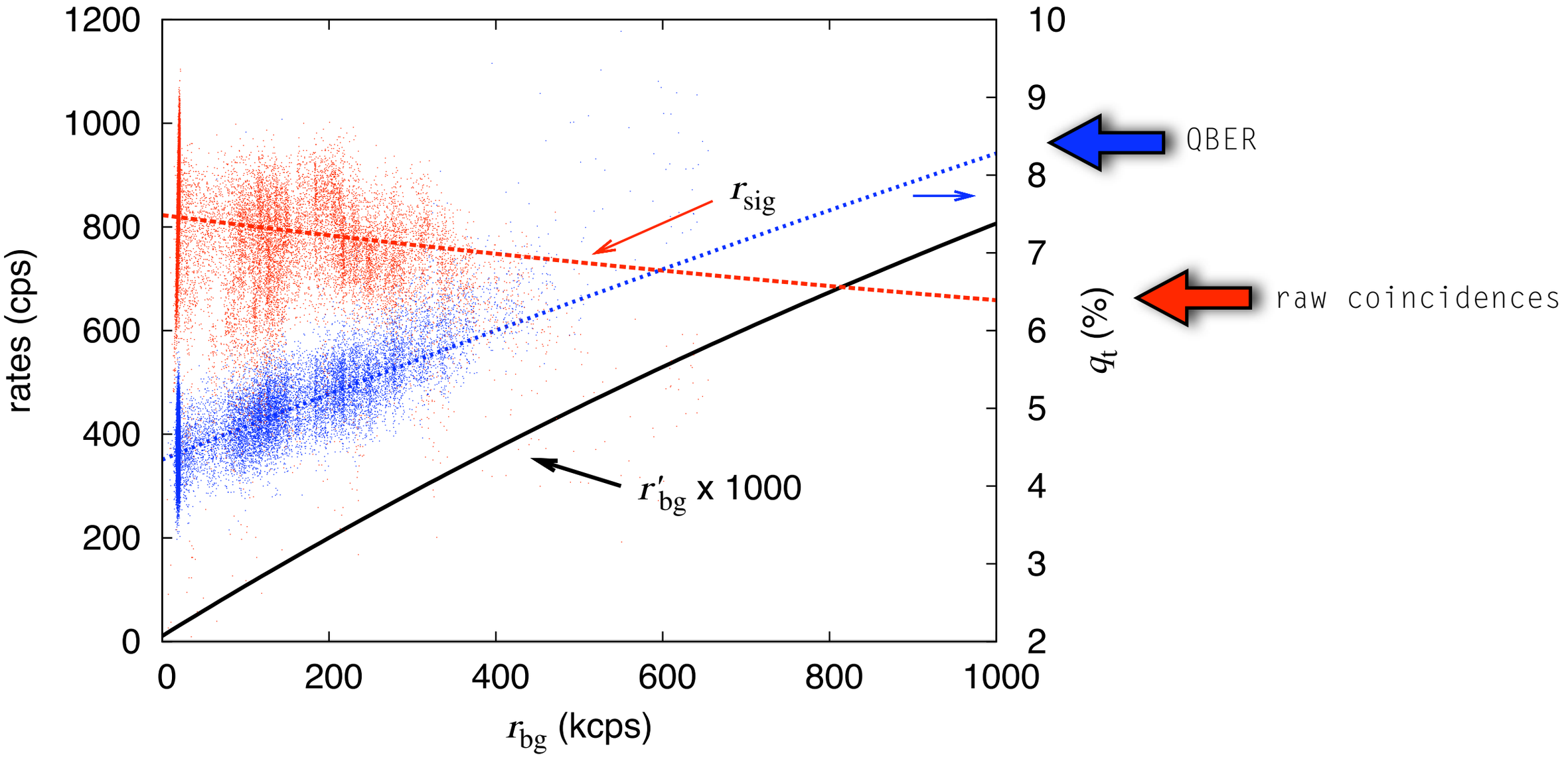
Do we NEED atomic clocks? NO, enough information within the PDC signal. Use better algorithms -> We should be able to use standard “bad” computer clocks [NJP 11, 045011 (2009)]

Daylight crypto 2 day run



[NJP 11, 045007 (2009)]

Effects of detector saturation



Summary

- A combination of spectral, spatial and temporal filtering is sufficient to suppress background from sunlight
- Demonstrated a continuous run of an entanglement based QKD system over several days
- Atomic clocks should be eliminated by taking full advantage of intrinsic timing info in PDC

Centre for Quantum Technologies

Christian Kurtsiefer
Antia Lamas-Linares
Valerio Scarani
Gleb Maslennikov
Ilja Gerhardt
Hou Shun Poh
Matt Peloso
Caleb Ho
Darwin Gosal
Brenda Chng
Tien Tjuen Ng
Syed Abdullah Aljunid
Jianwei Lee

http://qolah.org/

http://quantumlah.org/

NUS National University of Singapore

Thanks!