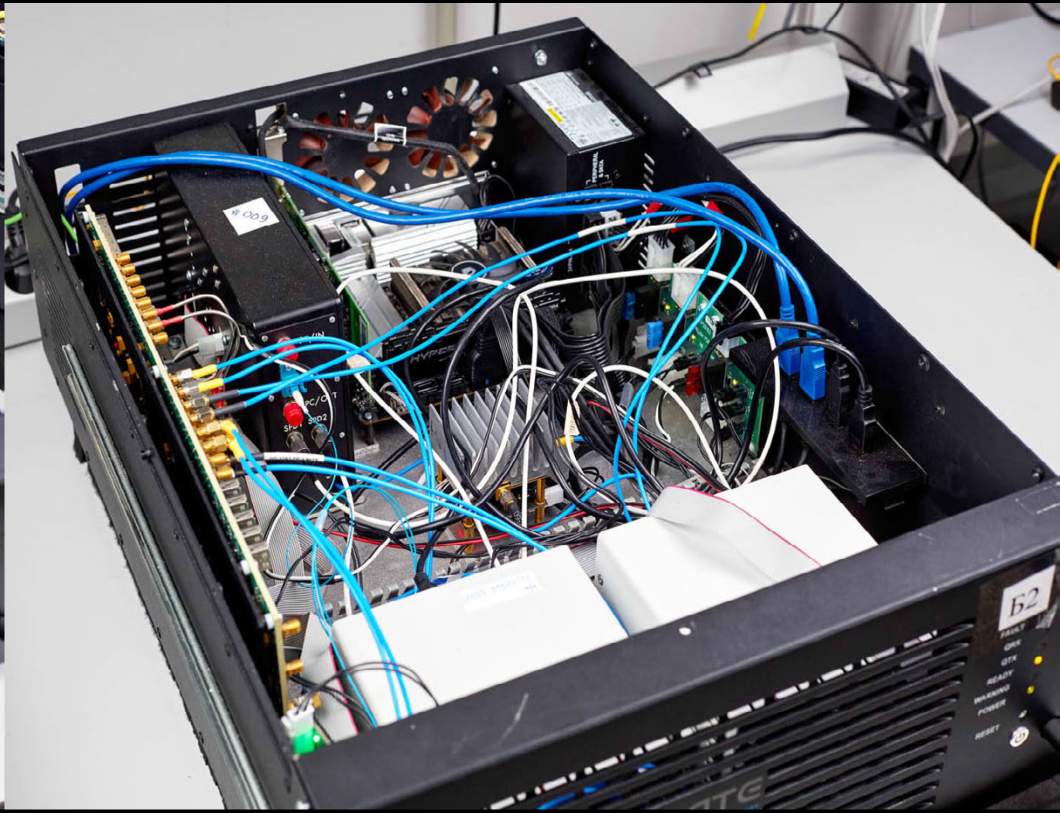
Talk at ITU workshop “Insights on QKD & QKDN certification: Recent developments and challenges”, Singapore, 17 May 2024

Certification of a quantum key distribution system against implementation loopholes

Vadim Makarov

RQC MISIS VQ

vad1.com/lab



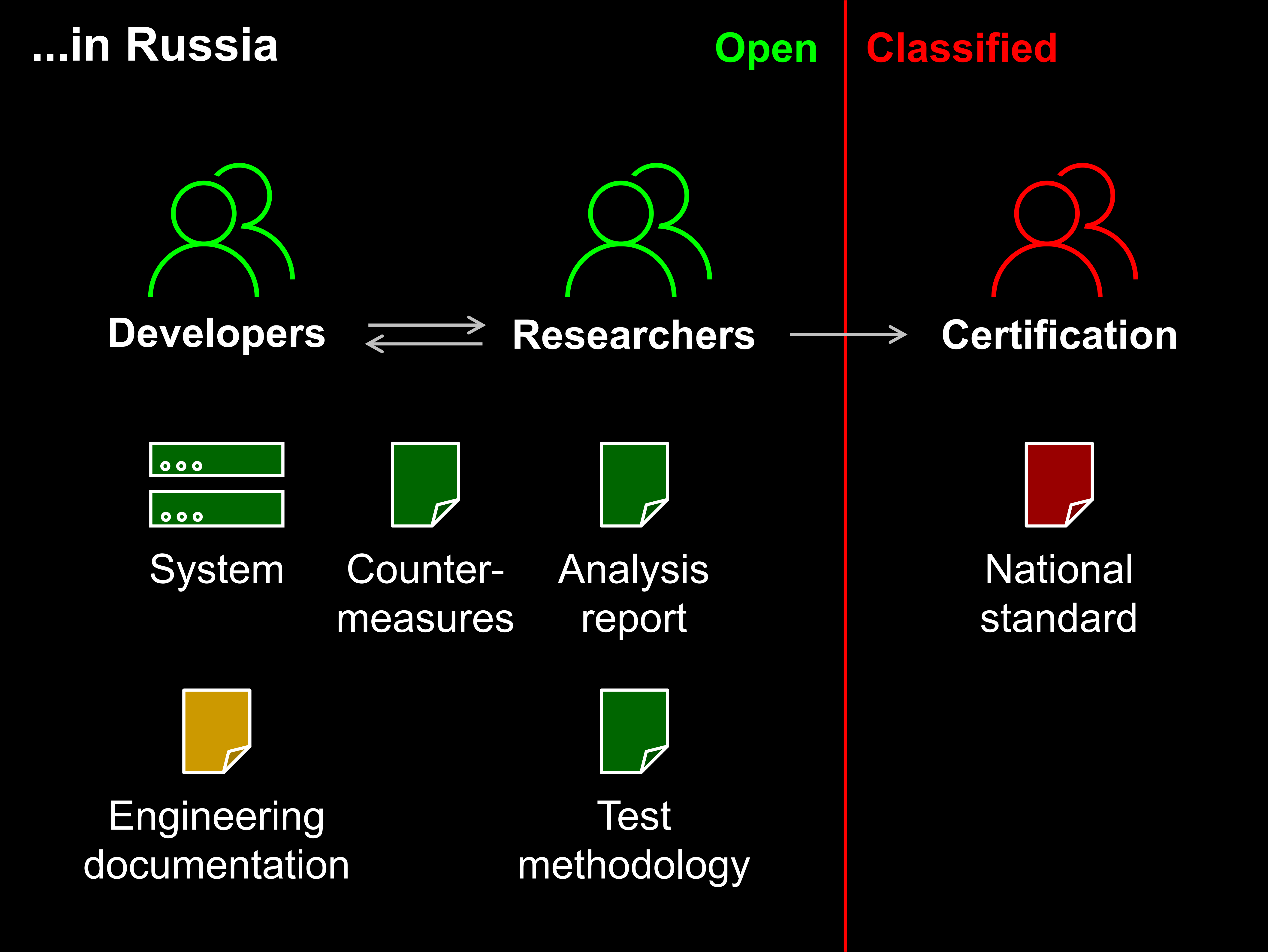
QRATE 312.5 MHz

Certification of a quantum key distribution system against implementation loopholes

Vadim Makarov,[1,2,3,*] Alexey Abrikosov,[1,3] Poompong Chaiwongkhot,[4,5,6,7] Aleksey K. Fedorov,[1,8]
Anqi Huang,[9] Evgeny Kiktenko,[1,3,10] Mikhail Petrov,[2,1,11,3] Anastasiya Ponosova,[1,3]
Daria Ruzhitskaya,[1,3] Andrey Tayduganov,[3,8] Daniil Trefilov,[2,1,11,3,12,13] and Konstantin Zaitsev[2,1,11,3,12]

[1] *Russian Quantum Center, Skolkovo, Moscow 121205, Russia*
[2] *Vigo Quantum Communication Center, University of Vigo, Vigo E-36310, Spain*
[3] *NTI Center for Quantum Communications, National University of Science and Technology MISiS, Moscow 119049, Russia*
[4] *Department of Physics, Faculty of Science, Mahidol University, Bangkok, 10400 Thailand*
[5] *Institute for Quantum Computing, University of Waterloo, Waterloo, ON, N2L 3G1 Canada*
[6] *Department of Physics and Astronomy, University of Waterloo, Waterloo, ON, N2L 3G1 Canada*
[7] *Quantum technology foundation (Thailand), Bangkok, 10110 Thailand*
[8] *QRate, Skolkovo, Moscow 143026, Russia*
[9] *Institute for Quantum Information & State Key Laboratory of High Performance Computing, College of Computer Science and Technology, National University of Defense Technology, Changsha 410073, People's Republic of China*
[10] *Steklov Mathematical Institute, Russian Academy of Sciences, Moscow 119991, Russia*
[11] *atlanTTic Research Center, University of Vigo, Vigo E-36310, Spain*
[12] *School of Telecommunication Engineering, Department of Signal Theory and Communications, University of Vigo, Vigo E-36310, Spain*
[13] *National Research University Higher School of Economics, Moscow 101000, Russia*

arXiv:2310.20107



...in Russia
Open
Classified
Developers
Researchers
Certification
System
Counter-
measures
Analysis
report
National
standard
Engineering
documentation
Test
methodology

Risk evaluation

Loophole		+	Exploitable with		+	Leaks	
likely	1		today's	1		major	1
or unlikely	0		or future	0		or minor	0
to exist?			technology?			fraction of key?	

= risk
- 3 High
- 2 Medium
- 1 Low
- 0 Low

or Solved

V. Makarov *et al.*, arXiv:2310.20107

We don’t have a unified security proof

Perfect system: key rate R

System with vulnerability A: key rate $R - R_A$

System with vulnerability B: key rate $R - R_B$

System with vulnerability C: key rate $R - R_C$

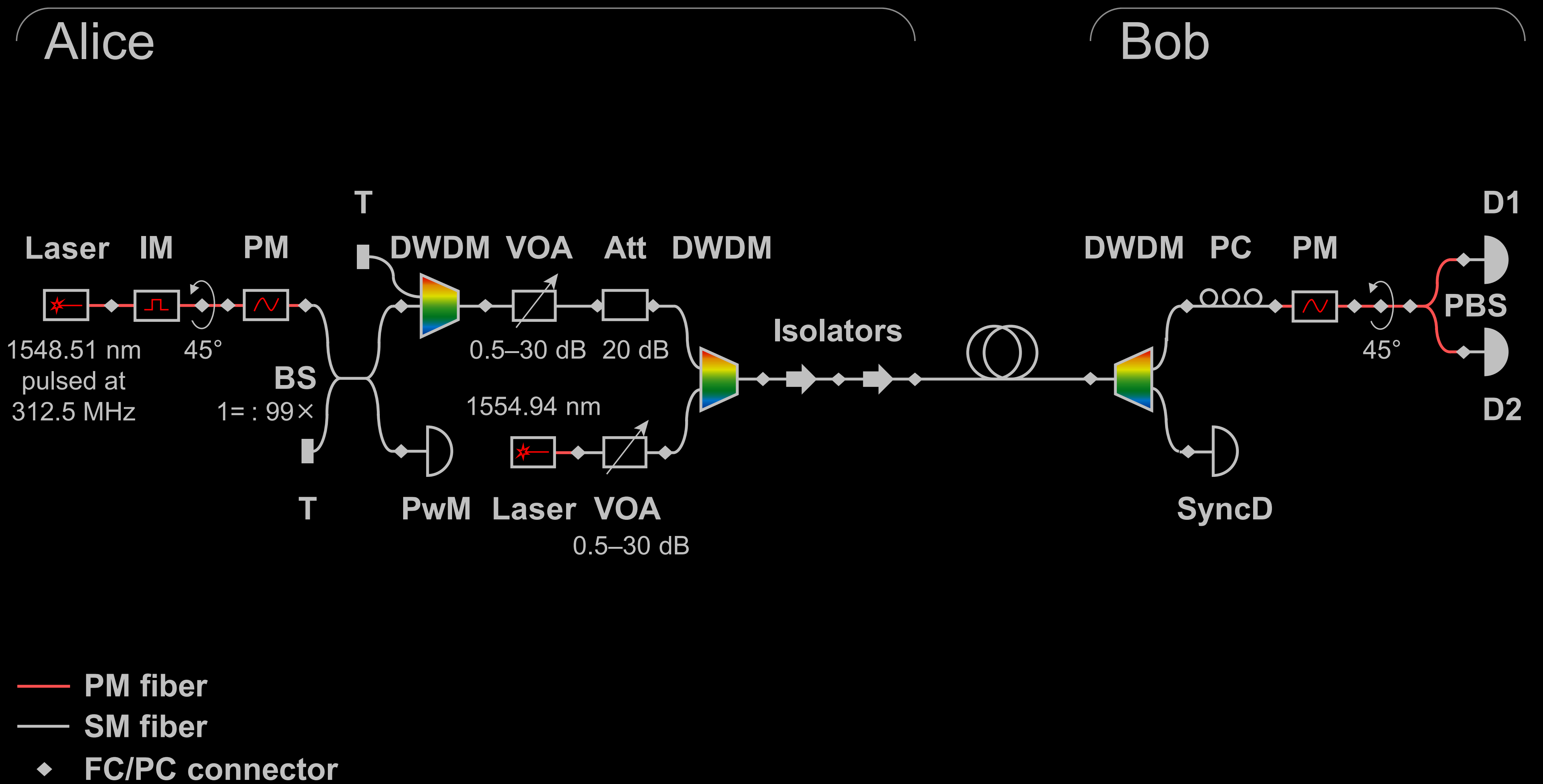
System with vulnerabilities A, B, and C:

key rate $R - R_A - R_B - R_C$ ✗ 

$R_A, R_B, R_C \overset{\rightarrow}{\sim} 0 \Rightarrow$ key rate R ?

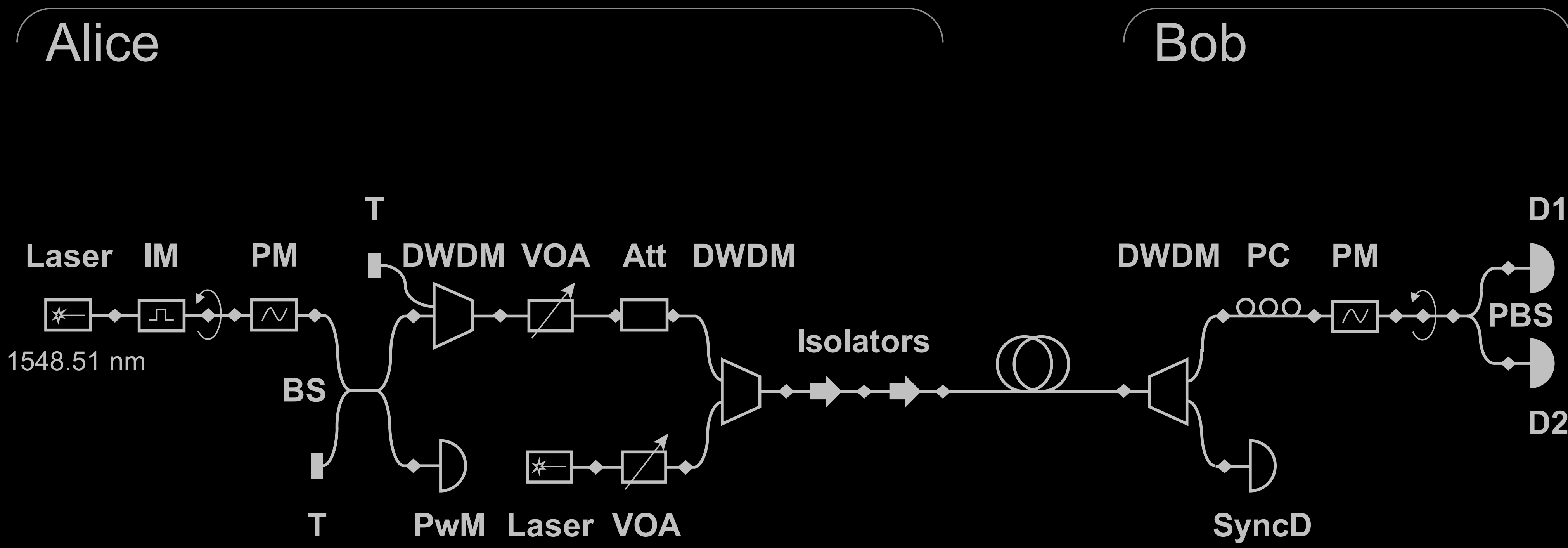
V. Makarov *et al.*, arXiv:2310.20107

QKD system



V. Makarov *et al.*, arXiv:2310.20107

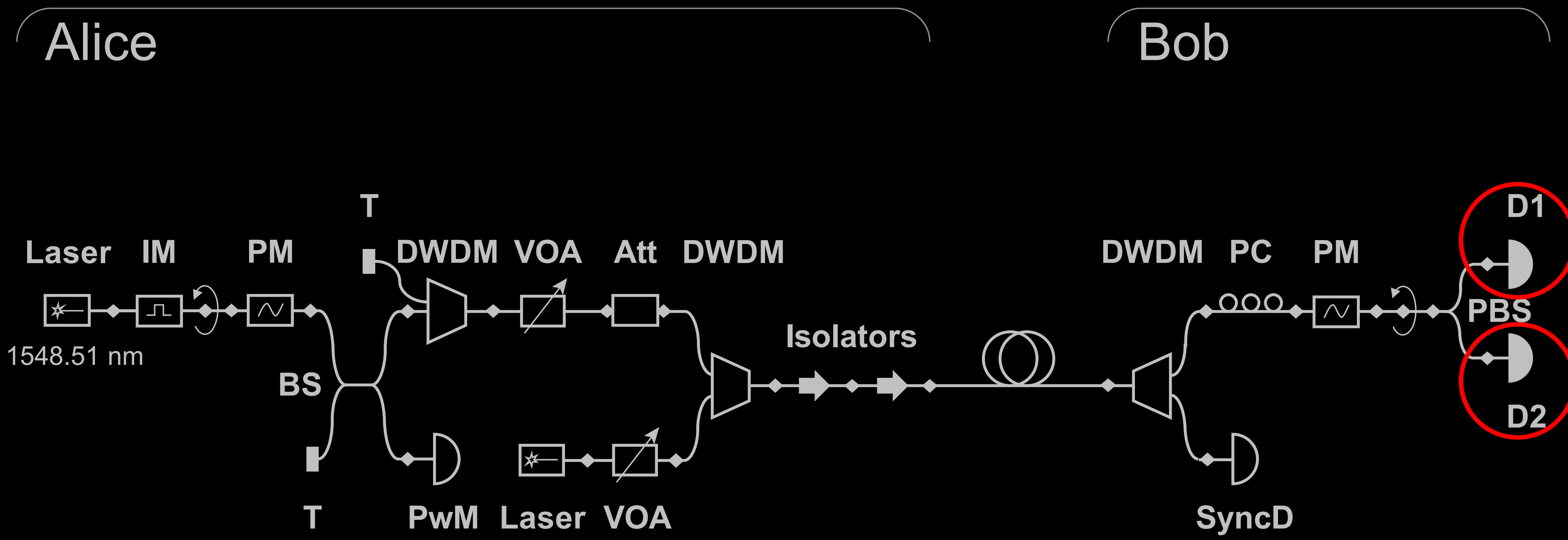
1. Choice of QKD protocol



BB84 decoy-state ✓

Solved

2. Superlinear detector control



Countermeasure: photocurrent monitor

1st iteration failed to pulsed blinding

P. Acheva *et al.*, EPJ Quantum Technol. 10, 22 (2023)

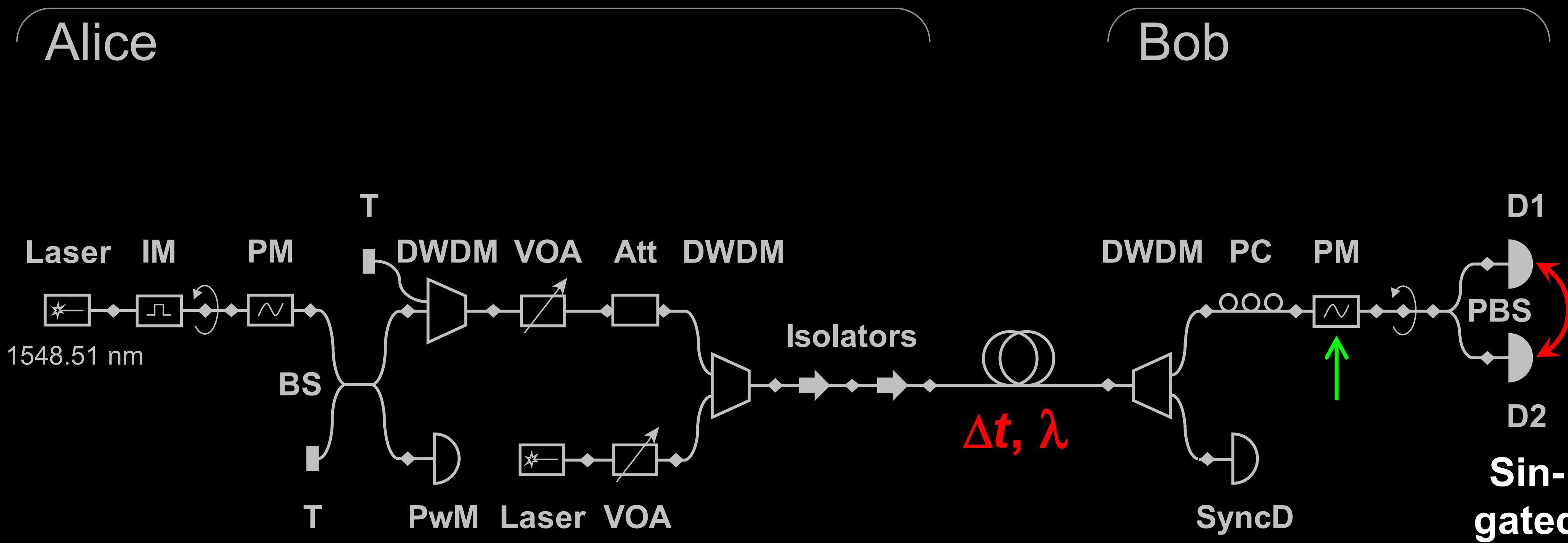
High-frequency version implemented, to be tested

Superlinearity characterised

K. Zaitsev *et al.*, unpublished

H (1,1,1)

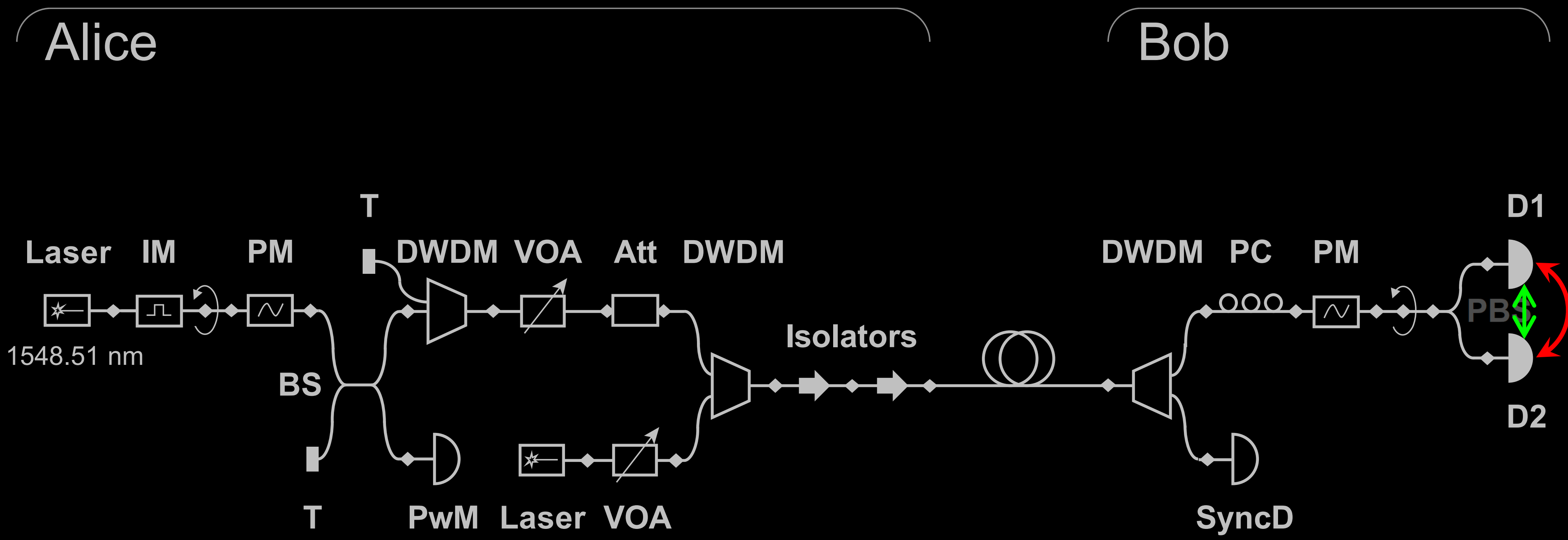
3. Detector efficiency mismatch



Countermeasure: four-state Bob

Counter-attack: Trojan-horse on Bob, need a security proof

4. Detector deadtime



Countermeasure: simultaneous deadtime in hardware

C. Wiechers *et al.*, New J. Phys. **13**, 013043 (2011)

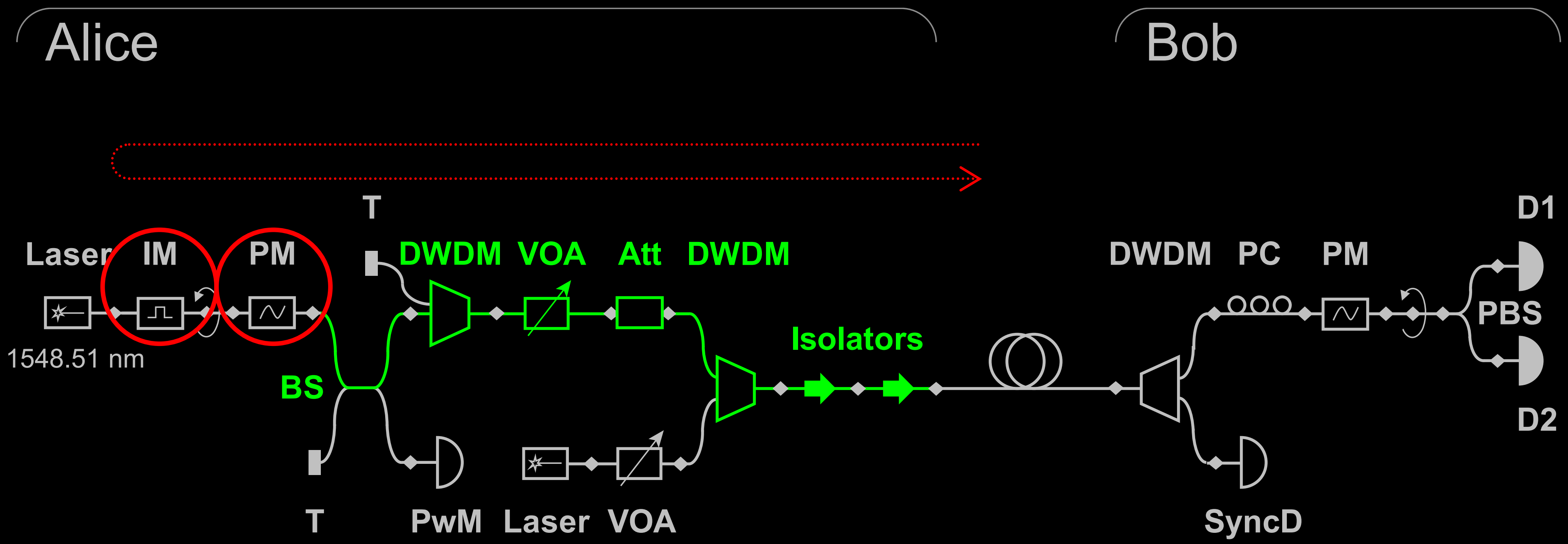
Mismatch remained

V. Makarov *et al.*, arXiv:2310.20107

Countermeasure: simultaneous deadtime in post-processing

H (1,1,1)

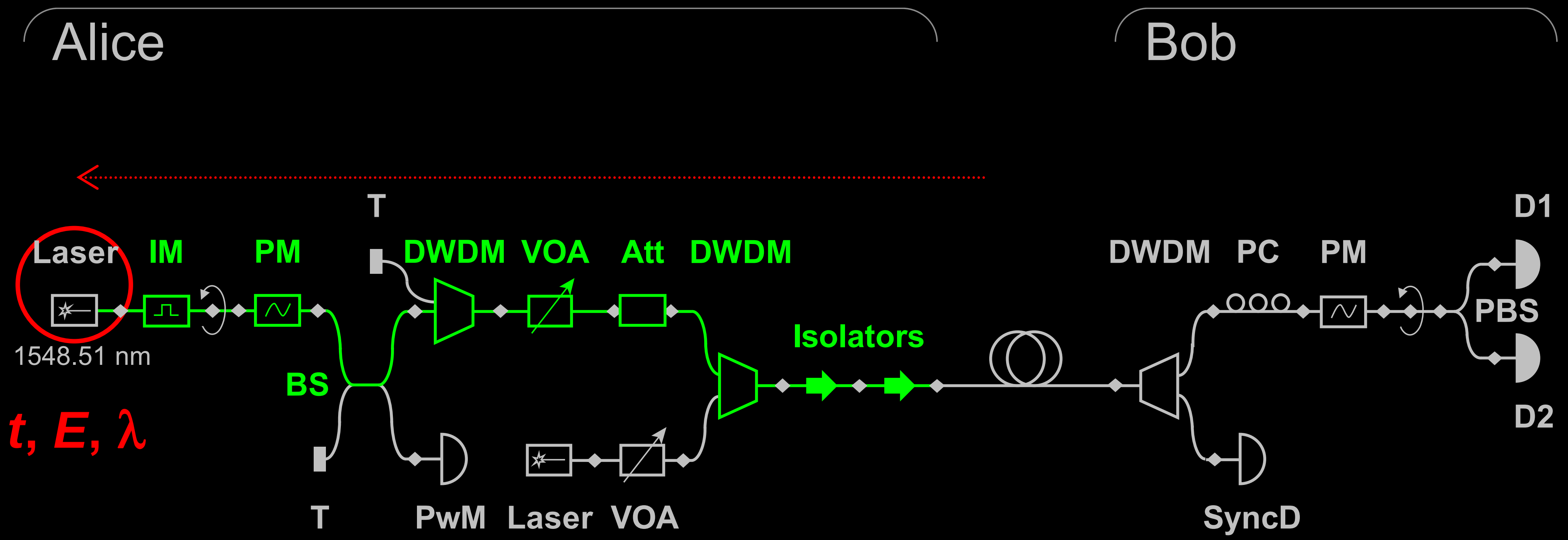
5. Trojan-horse



Countermeasure: enough isolation in a wide spectral range

H. Tan, M. Petrov *et al.*, unpublished

6. Laser seeding

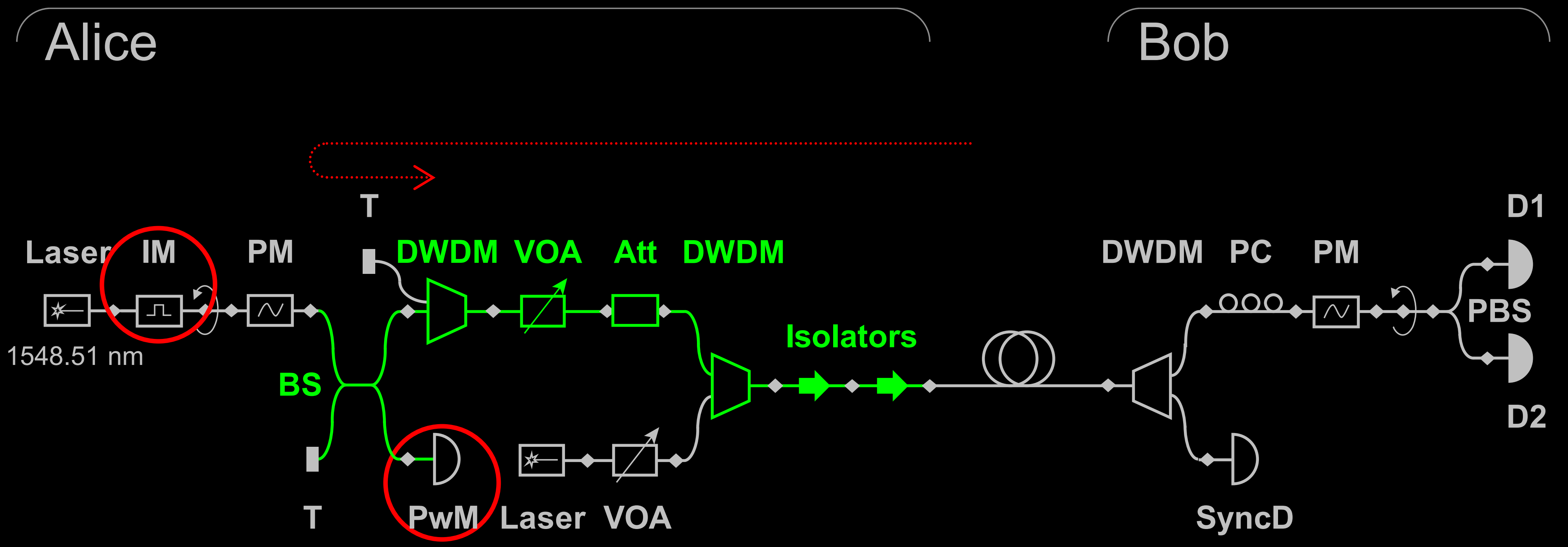


Enough isolation based on specs

V. Lovic *et al.*, Phys. Rev. Appl. **20**, 044005 (2023).

Solved

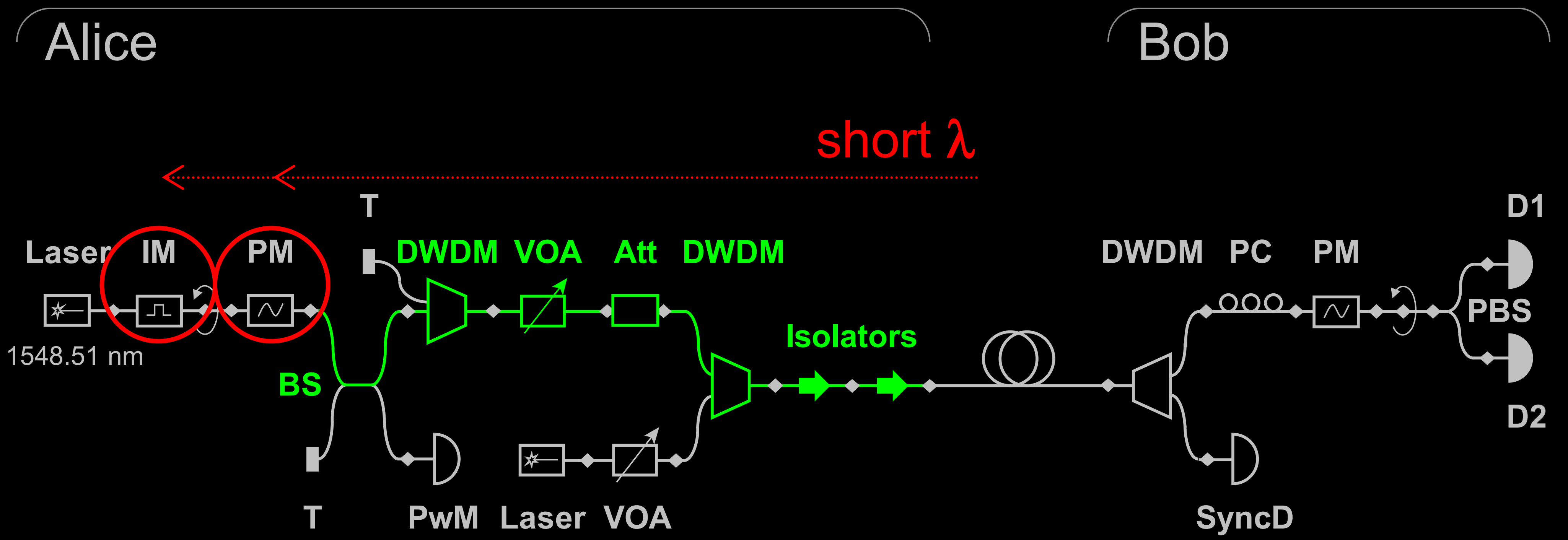
7. Light injection into Alice's power meter



Countermeasure: enough isolation in a wide spectral range

H. Tan, M. Petrov *et al.*, unpublished

8. Induced photorefraction

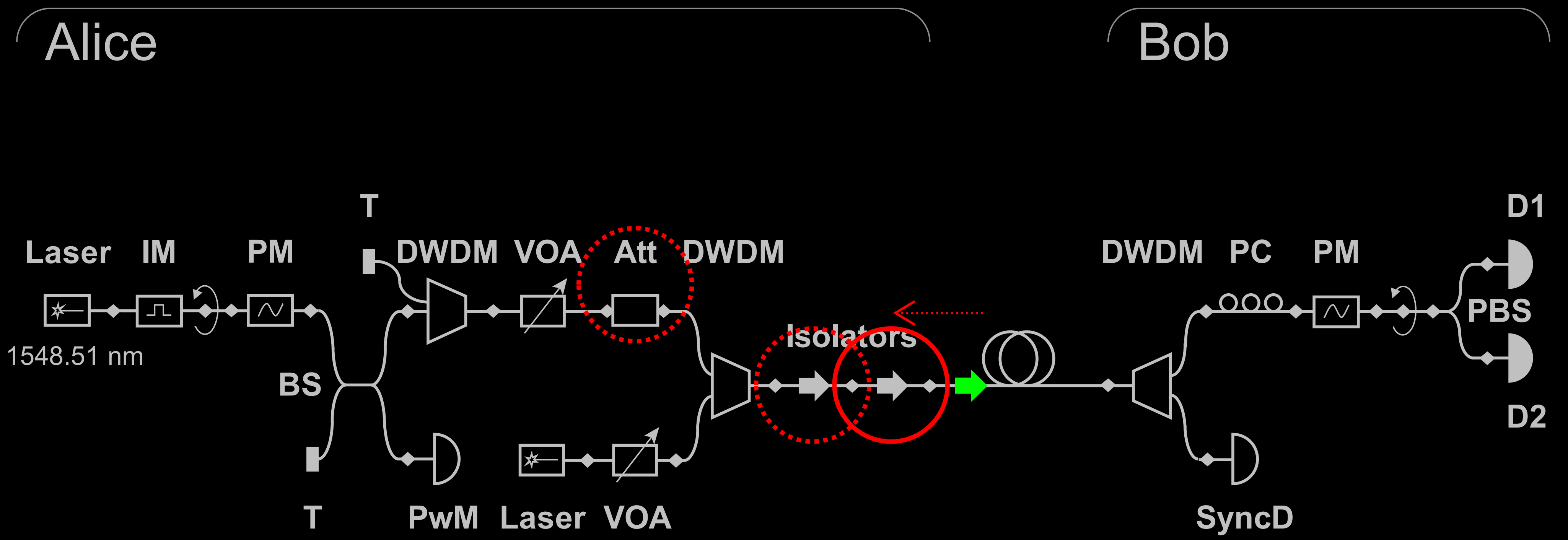


Countermeasure: enough isolation in a wide spectral range

H. Tan, M. Petrov *et al.*, unpublished

Test the modulators

9. Laser damage

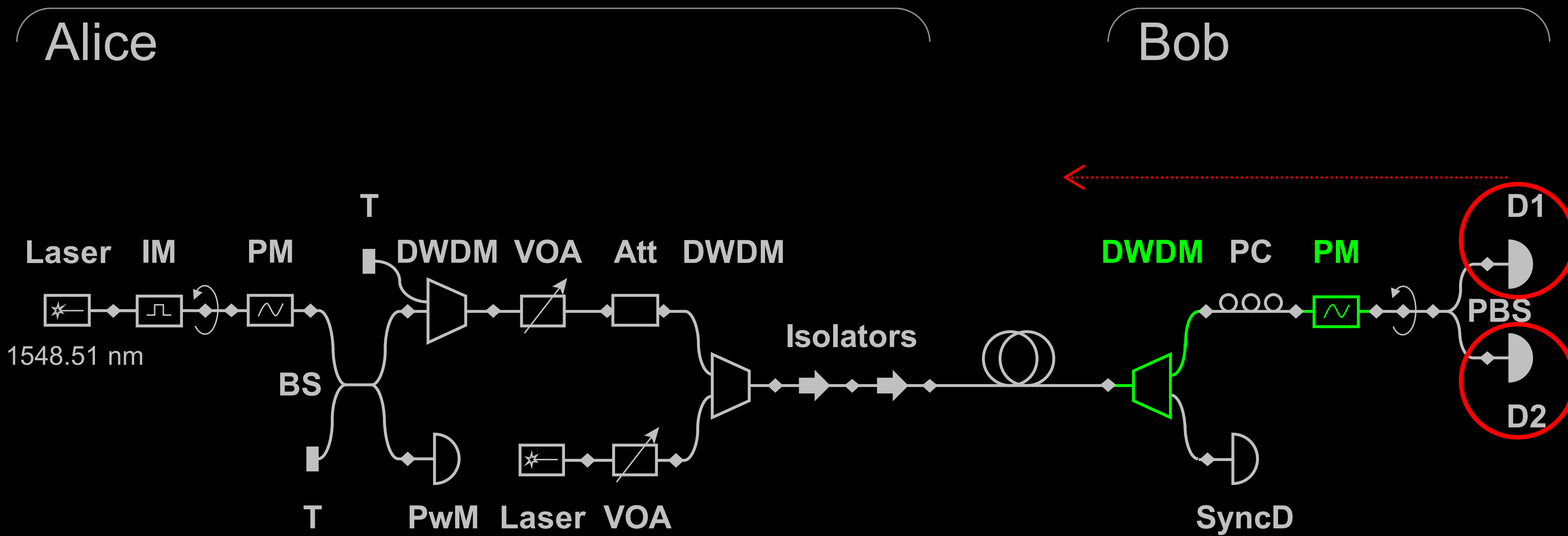


Countermeasure: power-limiting device, a sacrificial isolator, tested

A. Ponosova *et al.*, PRX Quantum **3**, 040307 (2022)

M (1,0,1) (0,1,1)

10. APD backflash



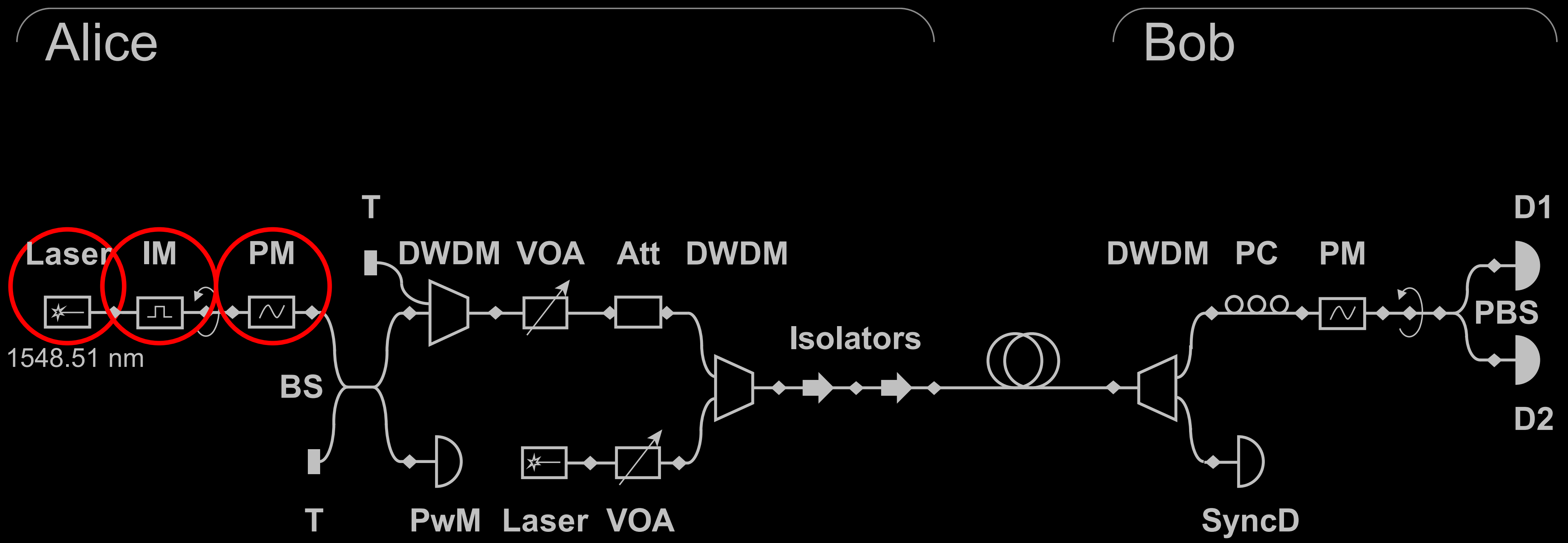
Characterise the backflash

A. Shilko *et al.*, unpublished

Countermeasure: enough filtering in a wide spectral range

H. Tan, M. Petrov *et al.*, unpublished

11. Intersymbol interference



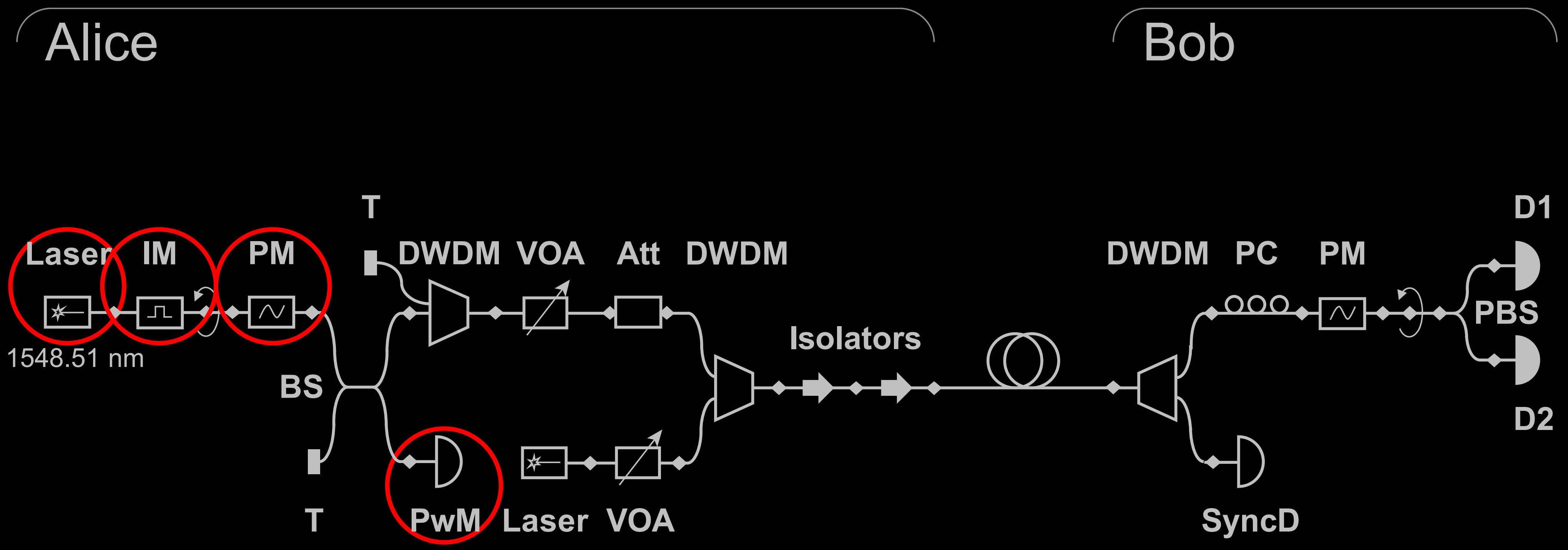
Correlations are present,

to be characterised and incorporated into a security proof

D. Trefilov *et al.*, unpublished

L (1,0,0)

12. Imperfect state preparation

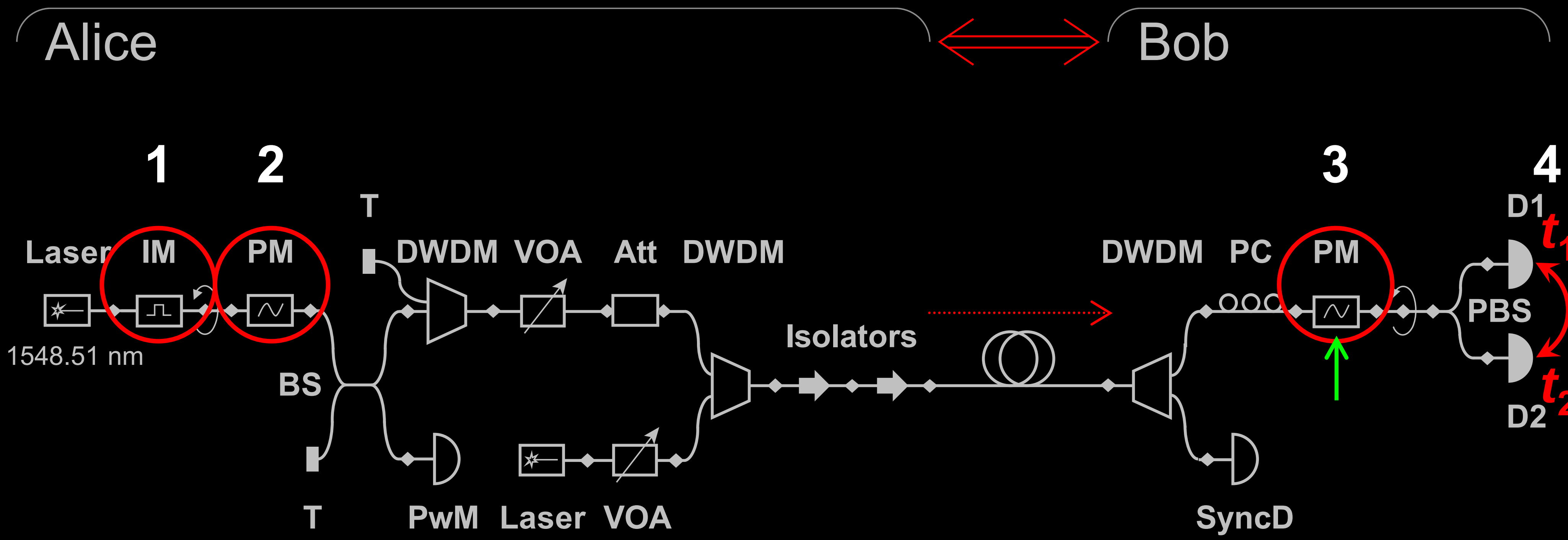


To be characterised and incorporated into a security proof

D. Trefilov *et al.*, unpublished

L (1,0,0)

13. Calibrations via channel Alice–Bob

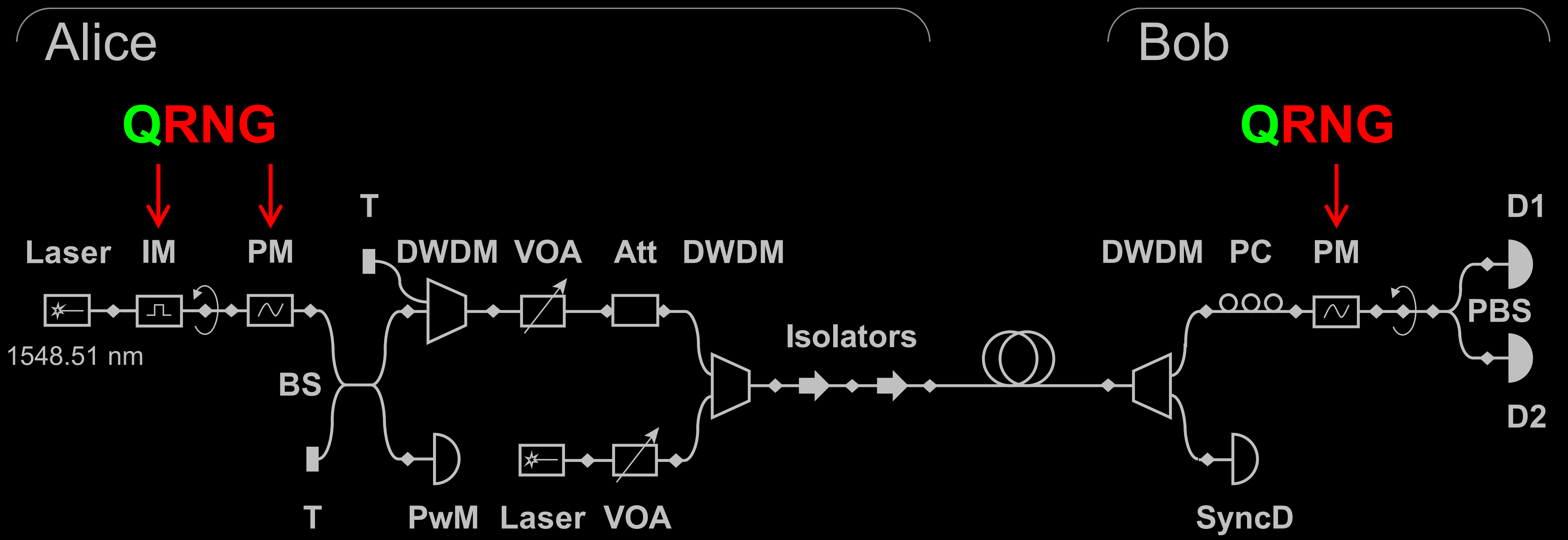


1: Now calibrated with PwM only

2: Now pre-calibrated at factory

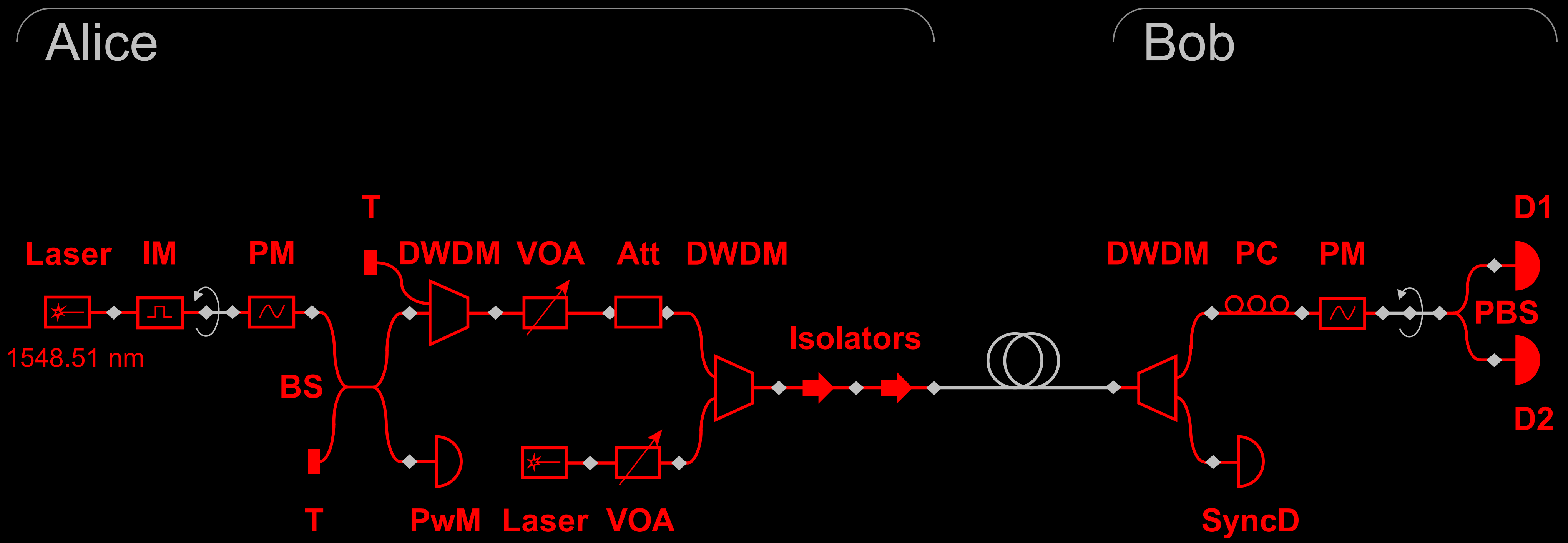
3, 4: Countermeasure: four-state Bob

14. Quantum random number generator



L (1,0,0)

15. Compromised supply chain

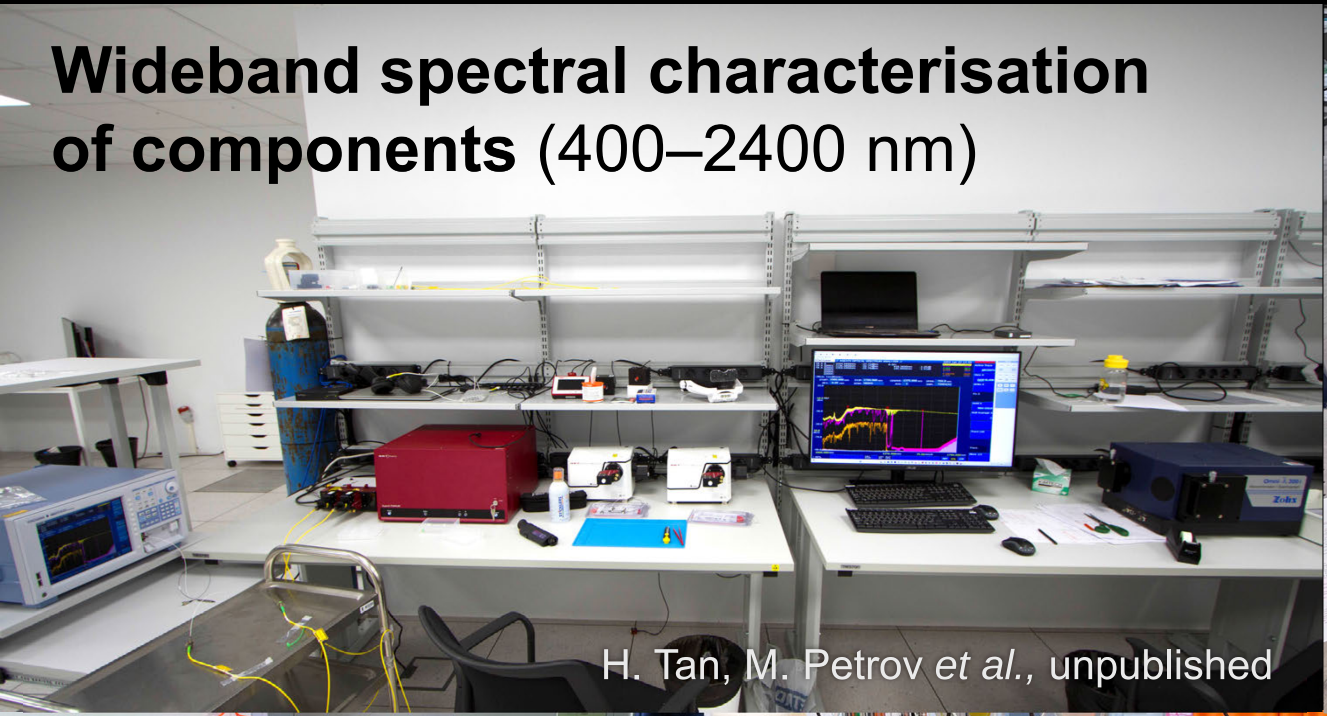


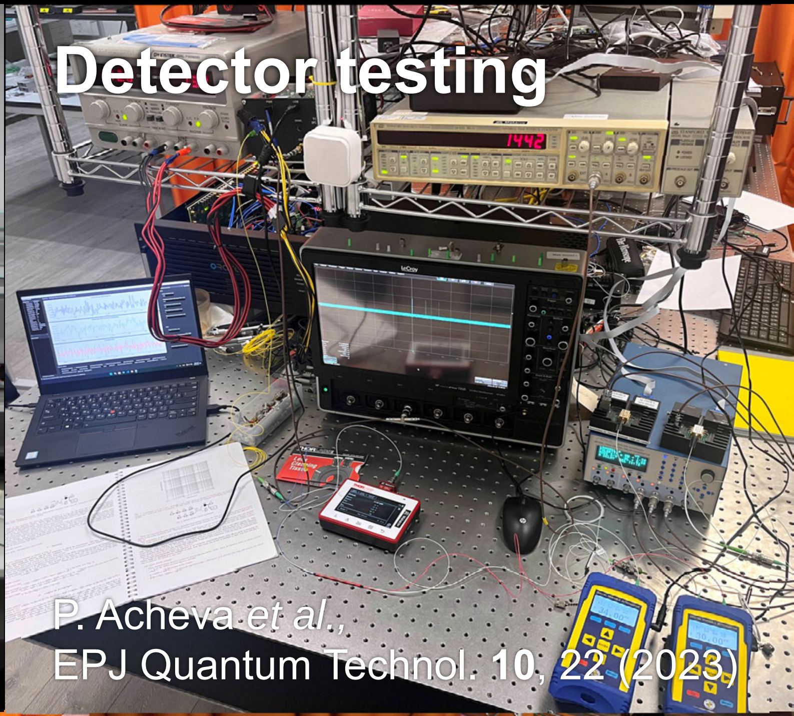
Ask national security agency for advice

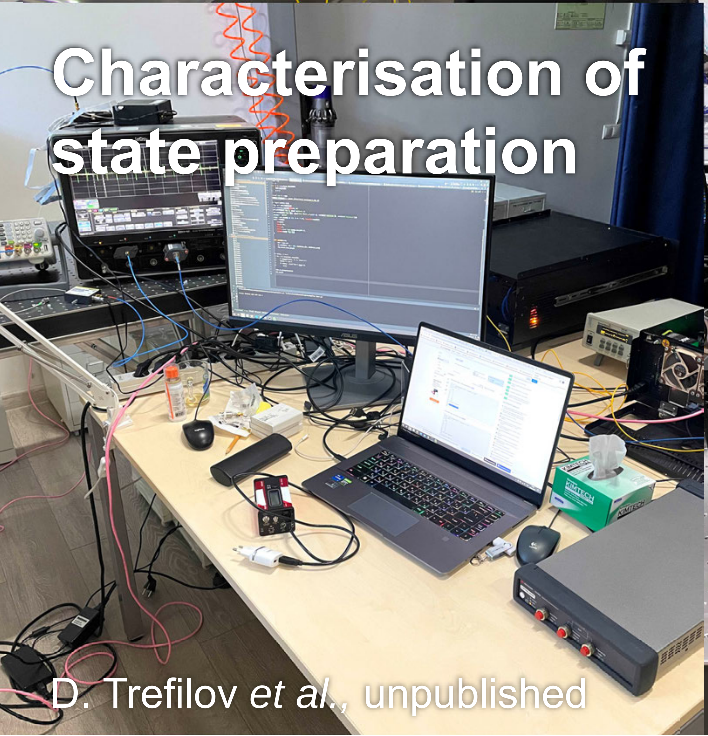
Potential issue	Risk evaluation	Countermeasure implemented	Recommended for certification
1. Choice of QKD protocol	Solved		
2. Superlinear detector control	H	●	●
3. Detector efficiency mismatch	H	●	
4. Detector deadtime	H	●	●
5. Trojan-horse	L		●
6. Laser seeding	Solved		●
7. Light injection into PwM	L		●
8. Induced photorefraction	M		●
9. Laser damage	M	●	●
10. APD backflash	M		●
11. Intersymbol interference	L		●
12. Imperfect state preparation	L		●
13. Calibrations via channel	H	●	
14. Quantum RNG	L		
15. Compromised supply chain	M		

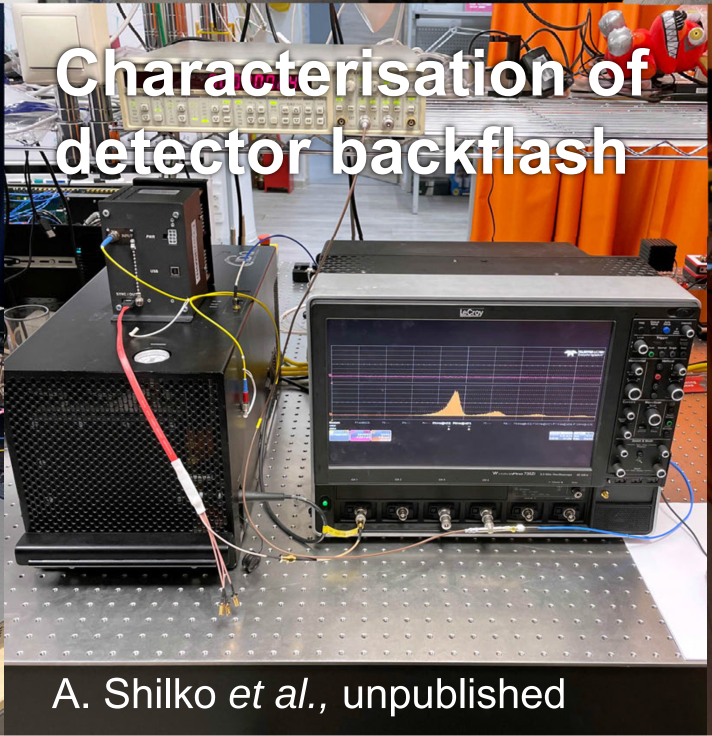
V. Makarov *et al.*, arXiv:2310.20107

Certification lab

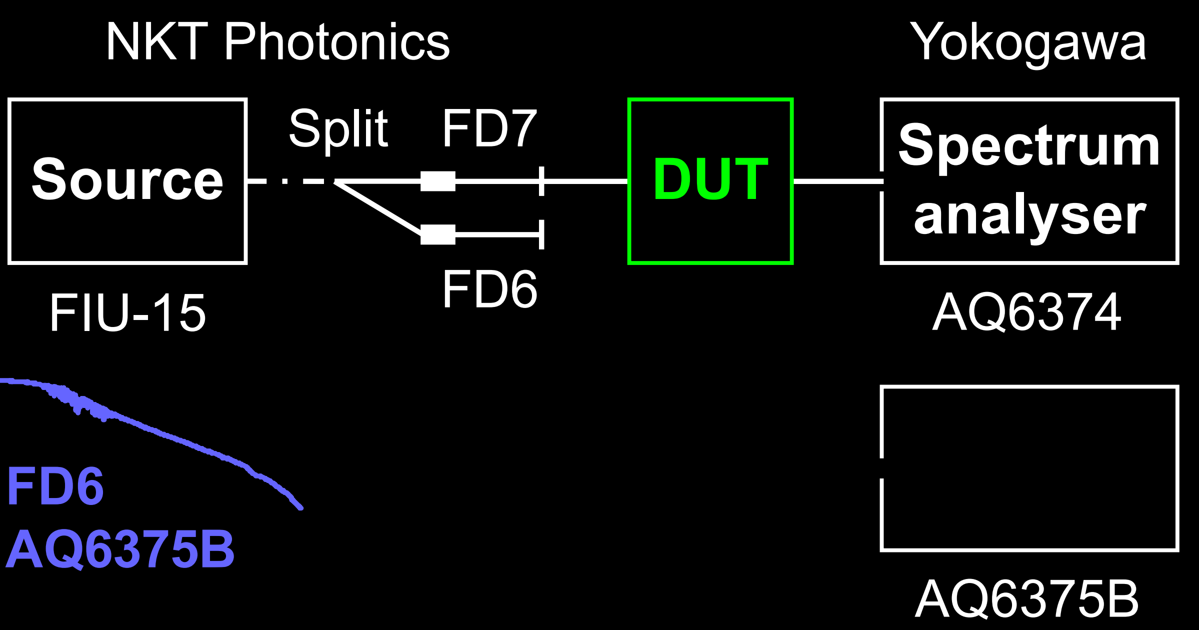


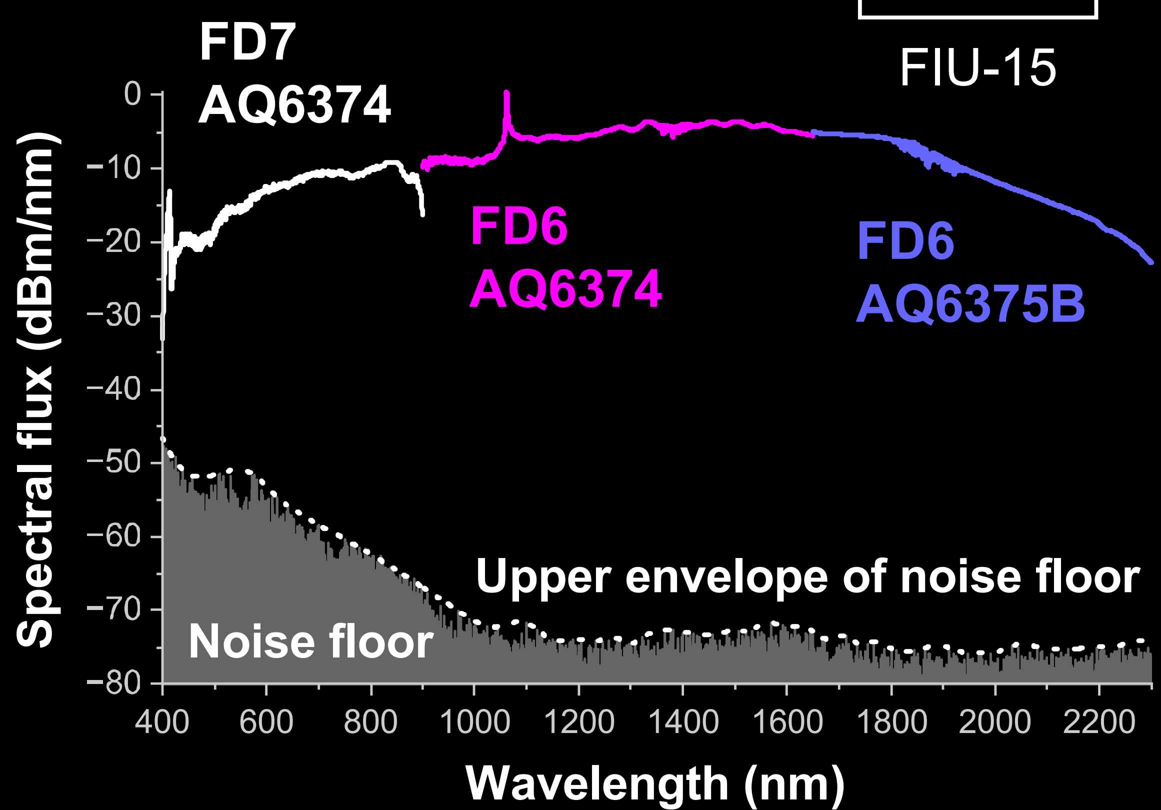






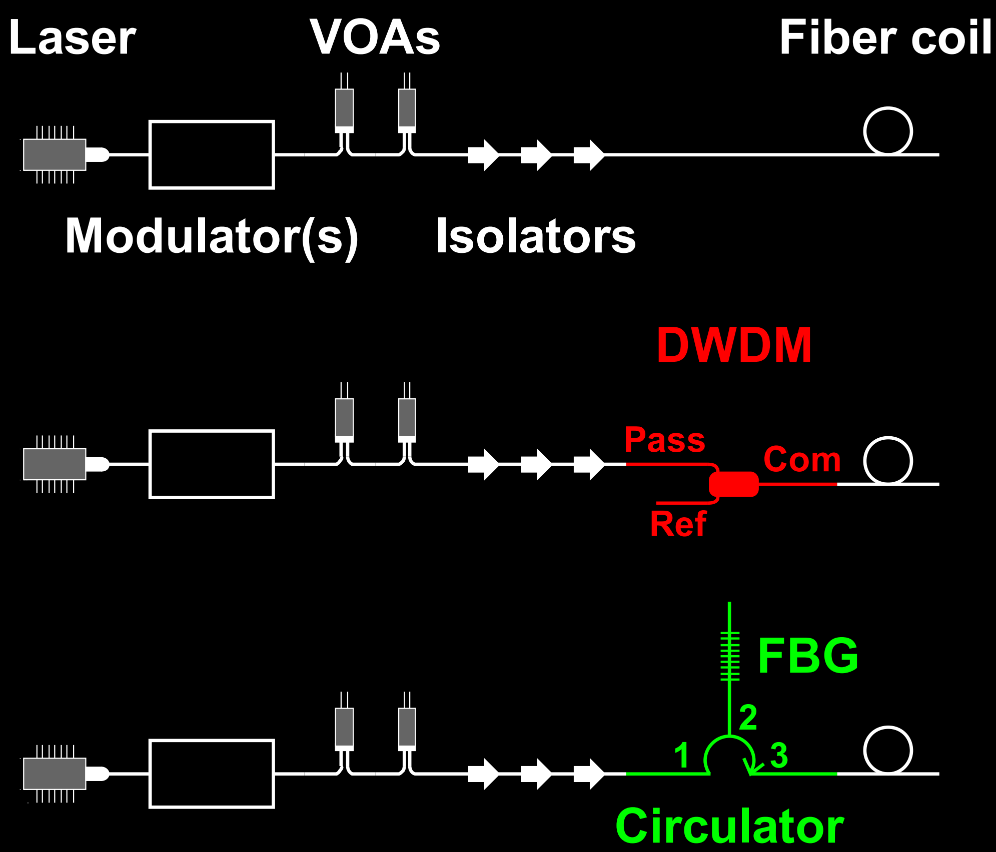
Wideband spectral characterisation

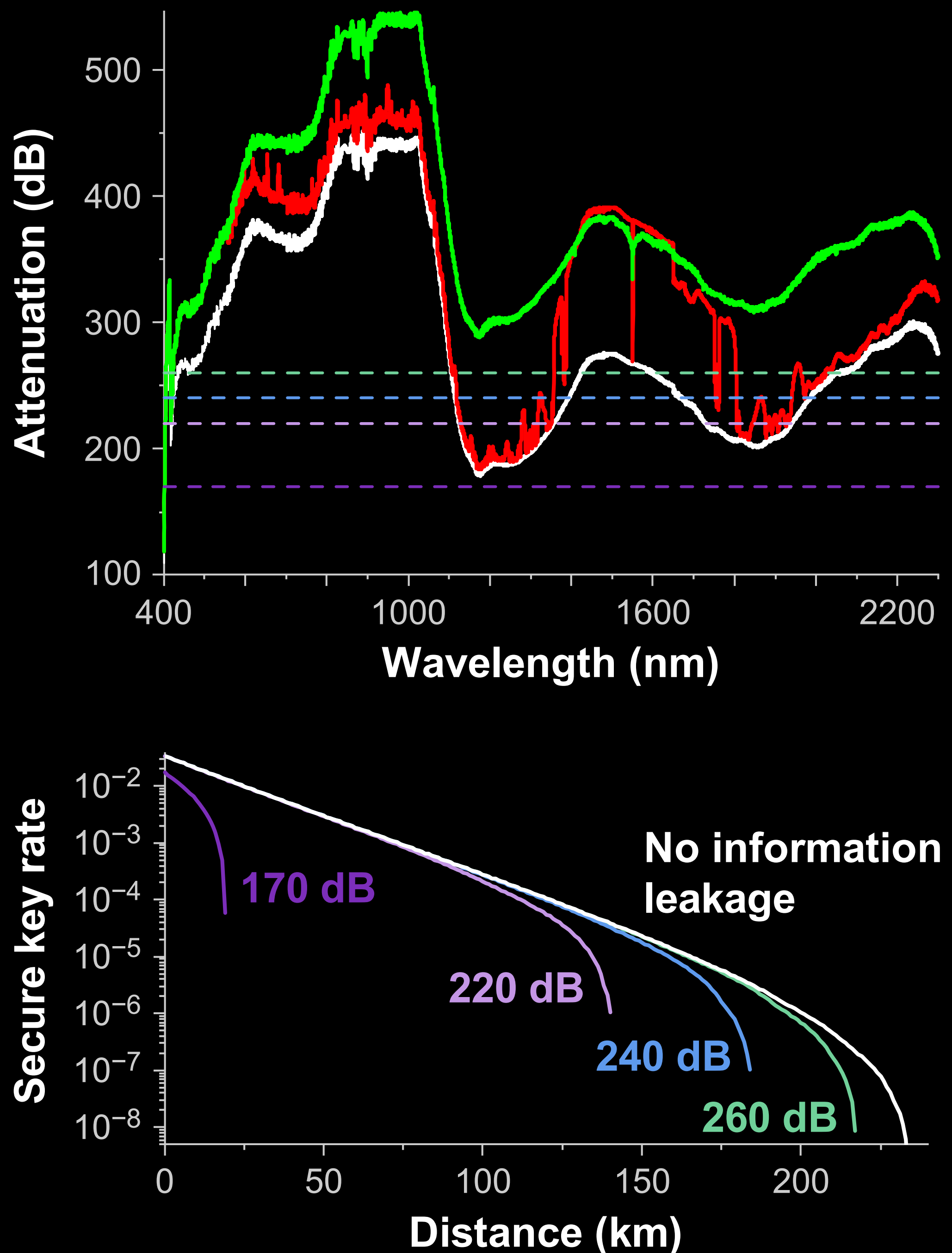




H. Tan, M. Petrov *et al.*, unpublished

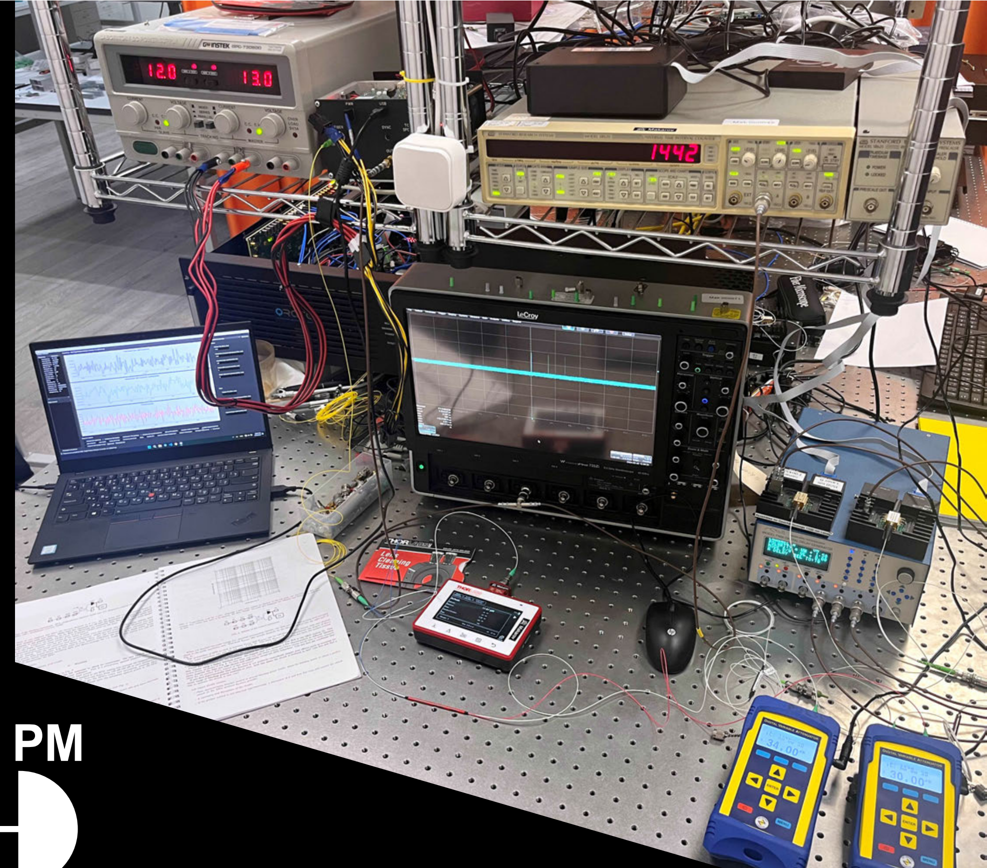
Security against Trojan-horse attack

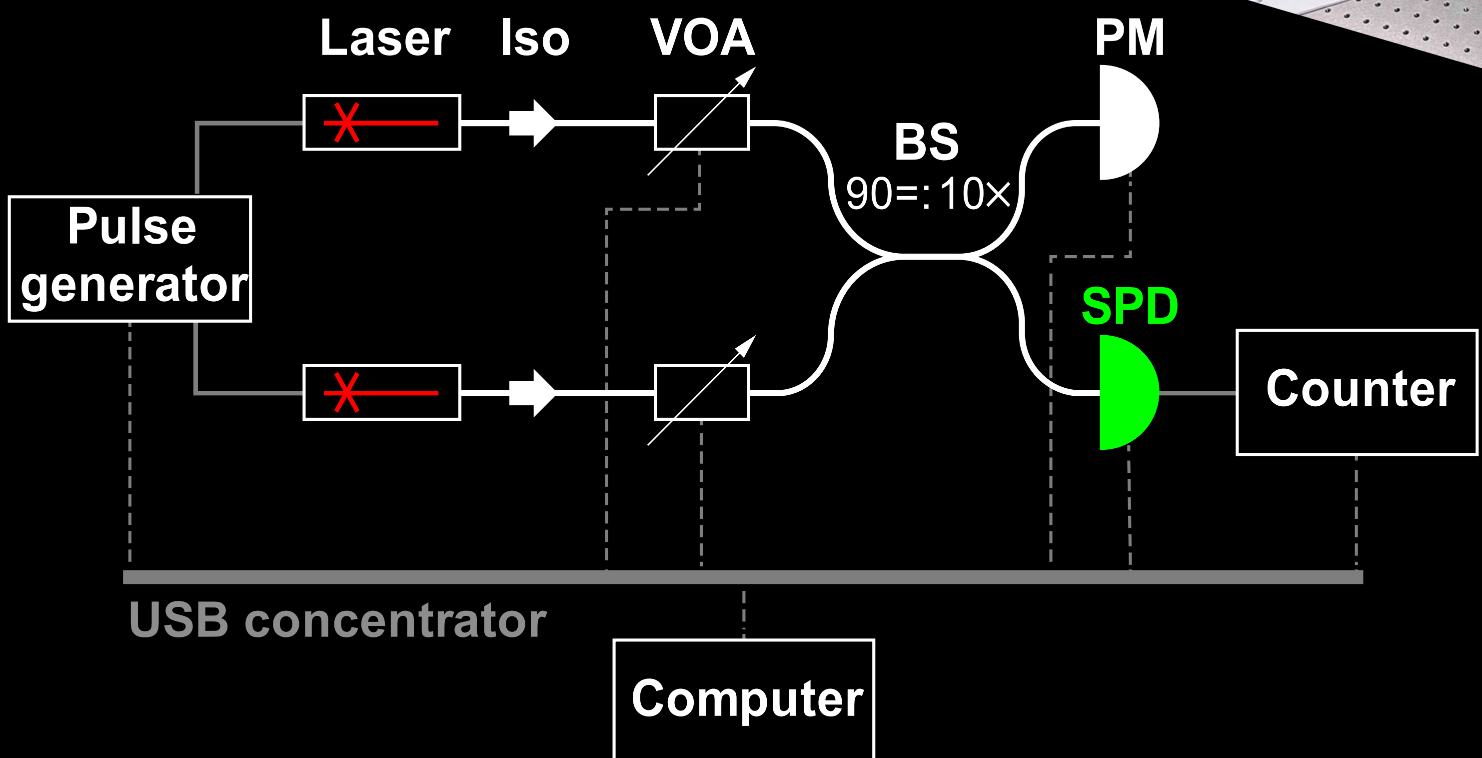




H. Tan, M. Petrov *et al.*, unpublished

Detector testbench





P. Acheva *et al.*, EPJ Quantum Technol. **10**, 22 (2023)

Automatic report

REPORT ON AUTOMATED TESTING OF SINGLE PHOTON DETECTOR FOR BRIGHT-LIGHT CONTROL

Test complited on: 19.09.2022 12:15

TEST SETTINGS

Power range: 2.3E-11 W - 1.25E-5 W
Laser pulses energy range: 10E-18 J - 10E-12 J
Pulse frequency: 10 kHz

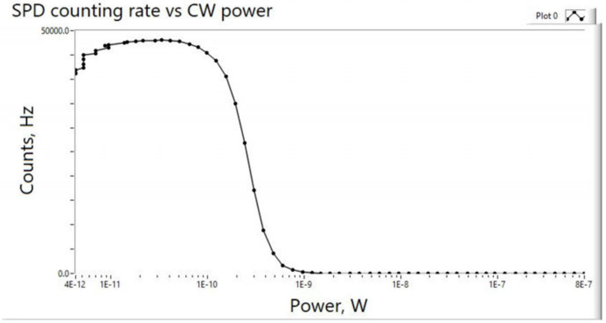
PARAMETERS ADDED BY OPERATOR

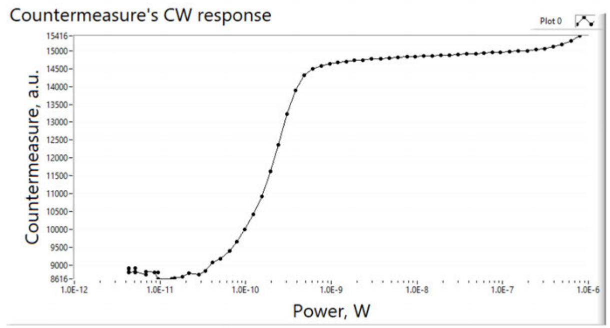
SPD: 3-054
CW - blinding step: 1.000000 dB
CW - control step: 1.000000 dB
PL - control step: 1.000000 dB

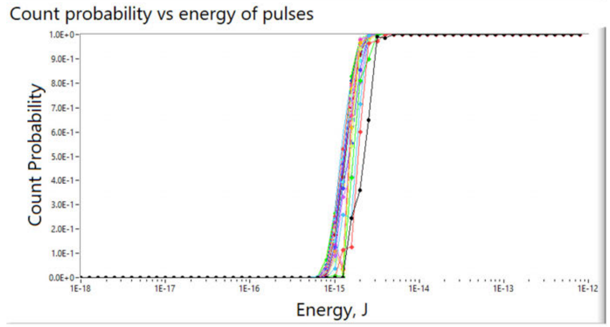
RESULTS

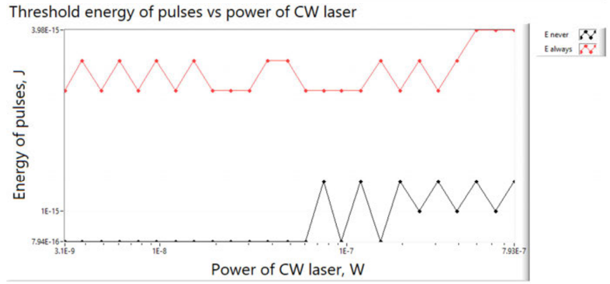
Is SPD blind? TRUE;
Blinding attenuation of CW laser: 24.000000 dB
Blinding power: 2.9615E-9 W
Succesfull pulse attack: TRUE
Power of CW laser, when Ealways/Enever is less or equal to 3 dB: 7.5626E-8 W
Enever, when Ealways/Enever is less or equal to 3 dB: 1.2589E-15 J
Ealways, when Ealways/Enever is less or equal to 3 dB: 2.5119E-15 J

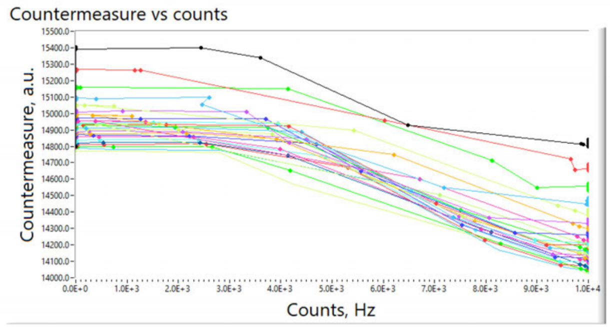
RAW DATA PLOTS











DESCRIPTION OF AUTOMATED SOFTWARE

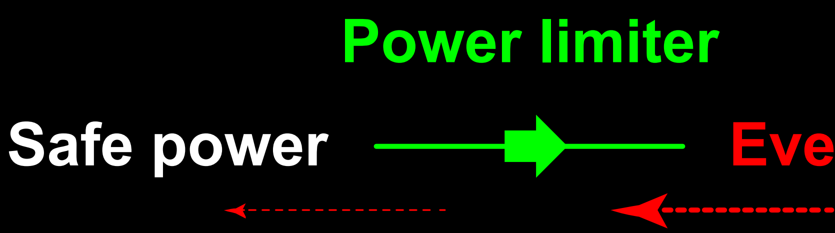
The device under test is tested for vulnerability against an attack by bright light. First, blinding with constant radiation is carried out, then control using combined, constant and pulsed radiation. In this report you can see the result - whether it was possible to carry out successful blinding and successful control. Successful blinding refers to a situation when constant radiation is applied to the detector, and the output of the device under test is 0 Hz. Successful control - when the control pulses are applied, the detector captures them all (count probability is 100 percent).

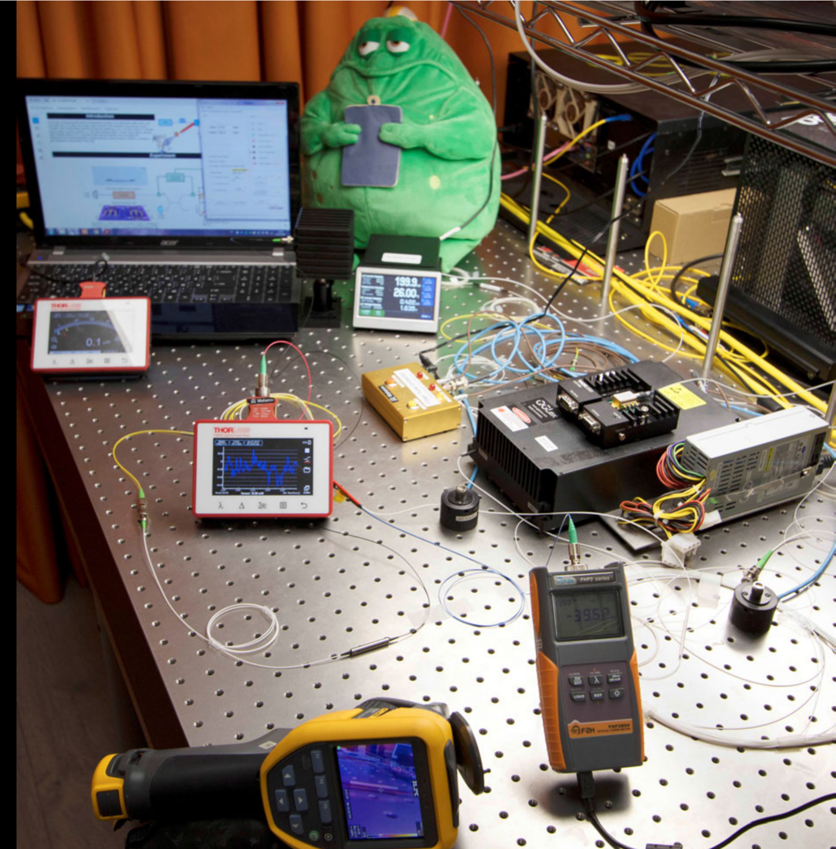
At the first stage, only constant laser radiation is applied to the detector. The power of constant laser gradually increases (the step is set by user, CW - blinding step). At the second stage, constant radiation is supplied along with pulsed radiation. At first, the power of the constant laser is set equal to the blinding power (from the first stage), and the pulse energy gradually increases (the step is also set, PL - control step). Then the power of the constant laser (CW - control step) increases, and the pulse energy changes again from the minimum to the maximum possible. The second stage ends when both constant and pulsed laser radiation reaches a maximum.

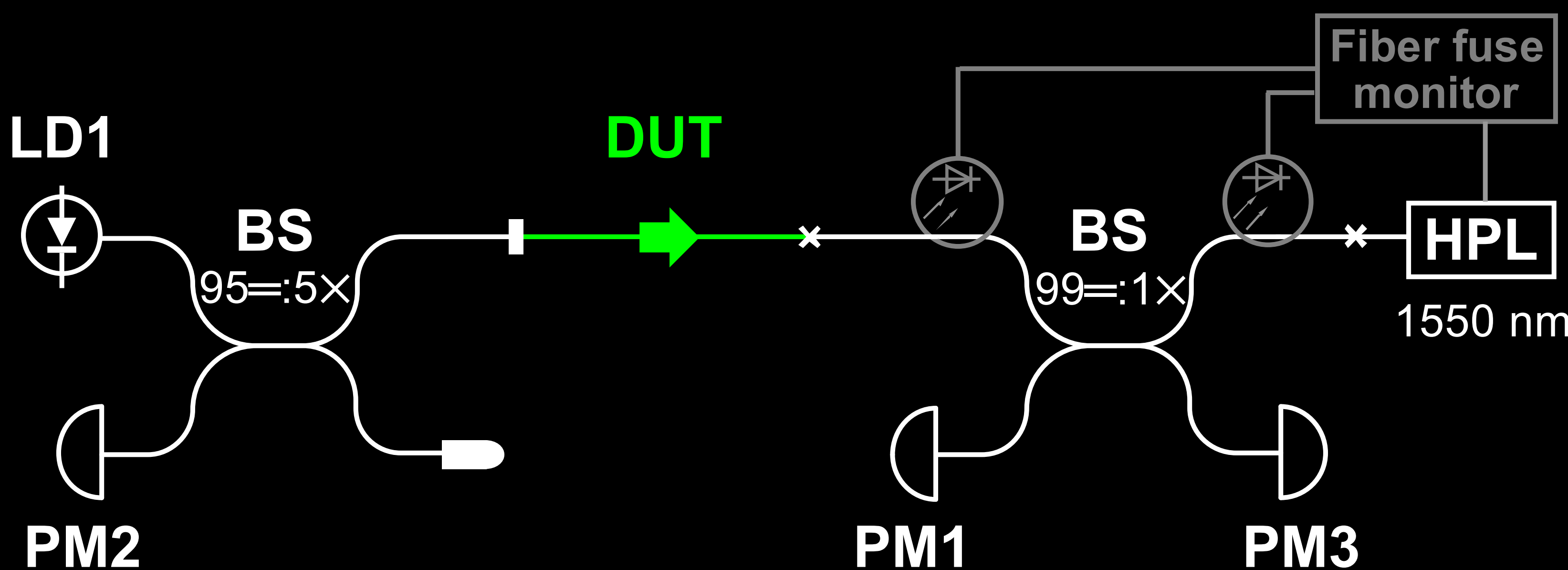
Automated testbench was developed by Quantum hacking lab.

P. Acheva *et al.*, EPJ Quantum Technol. **10**, 22 (2023)

Protection against laser damage

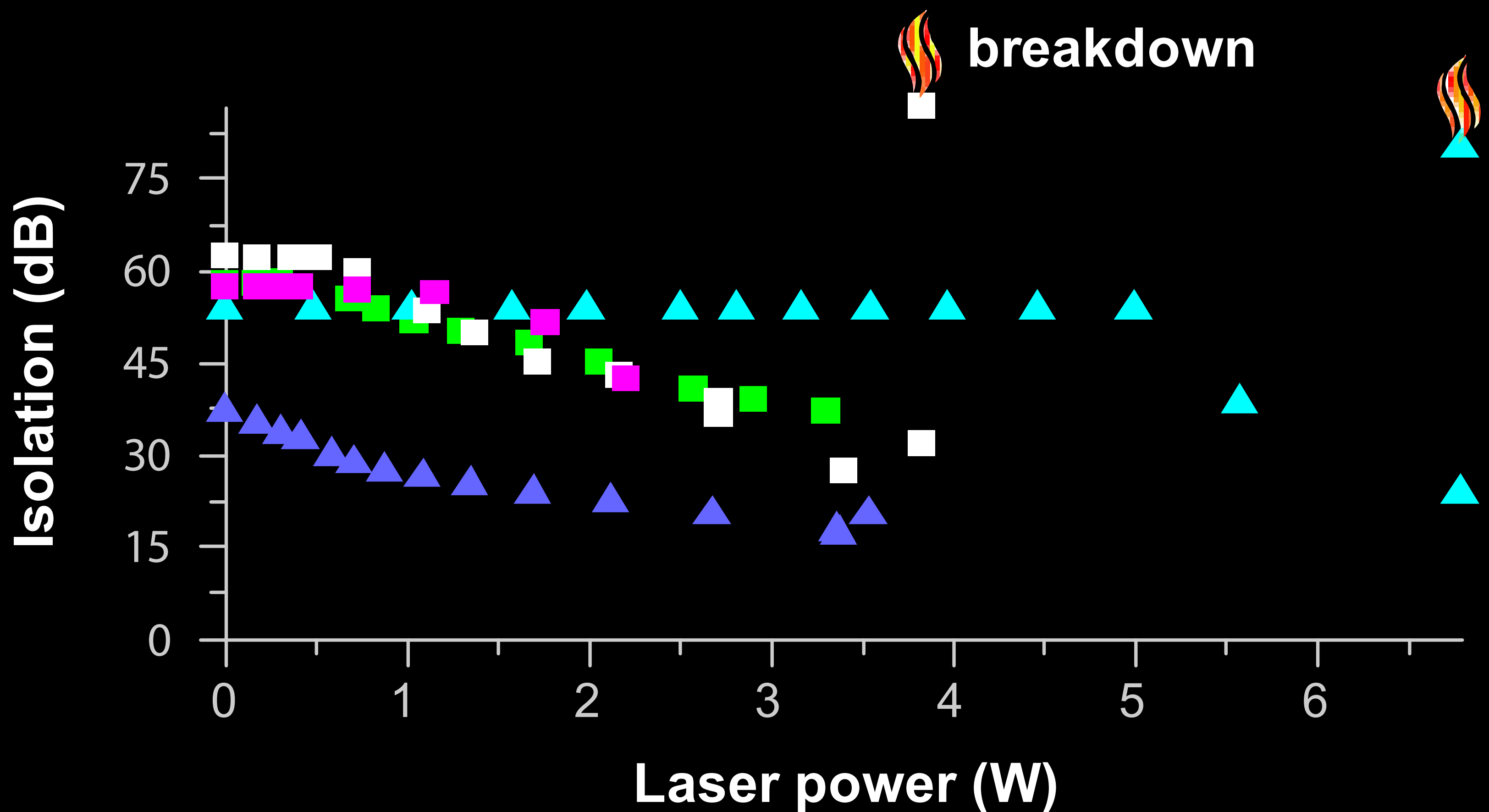






A. Ponosova *et al.*, PRX Quantum **3**, 040307 (2022)

Isolator as power limiter



A. Ponosova *et al.*,
PRX Quantum **3**, 040307 (2022)

Postdoc and PhD positions available

VQCC
VIGO QUANTUM
COMMUNICATION CENTER