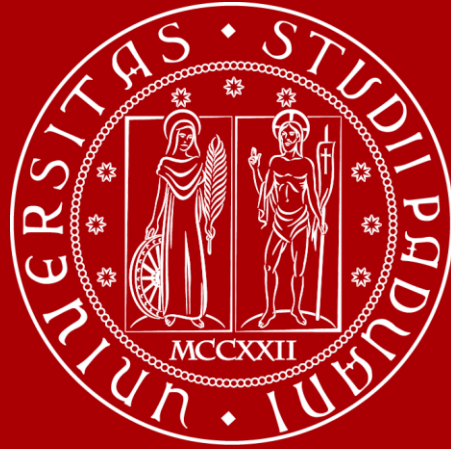




UNIVERSITÀ
DEGLI STUDI
DI PADOVA

Thermal Phase Injection Attack on QKD Fiber Systems

Author: Marco Scarpa

Relatore: Prof. Simone Soderi - Correlatore: Prof. Mauro Conti

University of Padova - Department of Information Engineering (DEI)

Bachelor's Degree – Ingegneria delle Telecomunicazioni, Internet e Multimedia

Academic Year 2025-2026



Motivation and Gap

QKD security is proven by quantum mechanics — the channel cannot be cloned or measured without disturbance

But: the fiber is a classical **physical object**, not a quantum one

Existing physical-layer attacks split into two classes: device-layer confidentiality (Garcia-Escartin 2020, Peng 2025) and channel-transmittance DoS on CV-QKD (Li 2018)

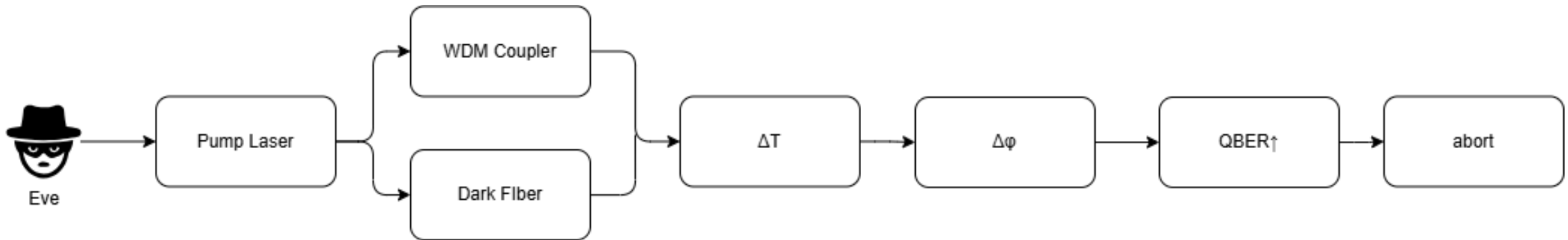
The unoccupied cell: physical-channel $\times$ availability $\times$ phase-sensitive DV protocols

One sentence: “Can an adversary with no quantum technology deny key generation by exploiting the thermo-optic response of the fiber itself?”

Layer	Confidentiality (key-leak)	Availability (DoS)
Network (classical control plane)	-	Dervisevic 2022
Device (source/detector/ modulator)	Garcia 2020, Peng 2025	-
Physical channel (fiber)	Kish 2024	Li 2018, this work



The Attack Concept



Eve injects a CW optical pump → absorbed by silica → raises fiber temperature by ΔT

Thermo-optic effect: $\Delta \phi = (2\pi L \xi / \lambda) \cdot \Delta T$, with $\xi = 1.18 \times 10^{-5} \text{ K}^{-1}$ $\xi \equiv \text{d}n/\text{d}T + n_0 \alpha_{\text{th}}$

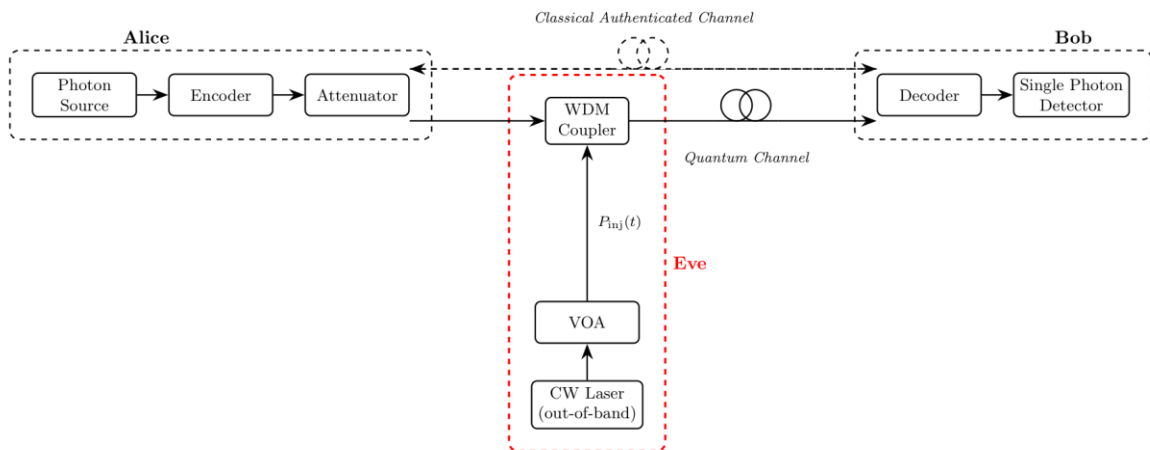
Phase drift pushes QBER above Q_{max} → protocol aborts → key generation denied

No quantum technology required: off-the-shelf CW laser + WDM coupler or dark-fiber access



2 Attack Geometries

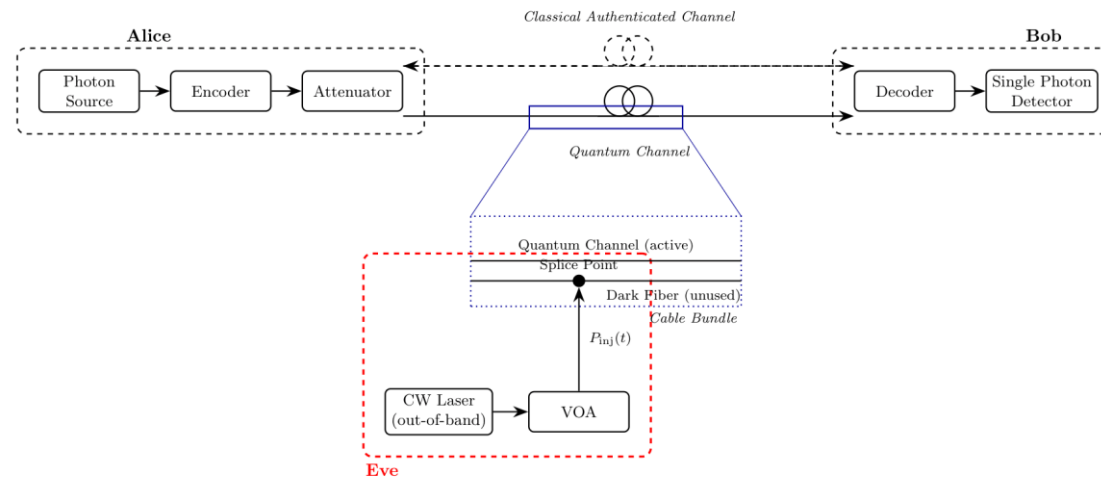
WDM Coupler



Eve splices in-line, pump co-propagates in fiber Q $\rightarrow \eta_{coup} = 1$ (maximum efficiency)

LoS alarm risk

Adjacent Fiber

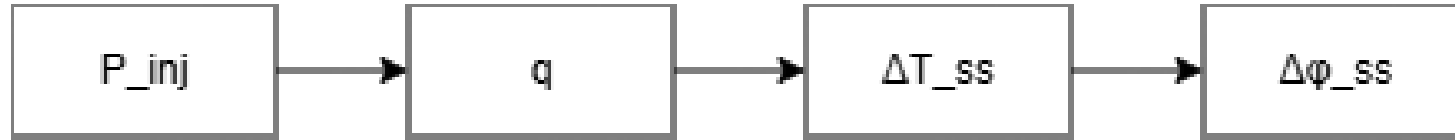


Eve injects into a dark fiber, heat reaches Q by **conduction** $\rightarrow$ no LoS, no optical access to Q, unconstrained λ_E , but $\eta_{coup} \in [0.386, 0.488]$

Threshold penalty: $P_{th}^{(adj)} = P_{th}^{(WDM)} / \eta_{coup} \rightarrow \text{factor } \times 2.05 \text{ to } \times 2.59$



The physical model: chain from P_{inj} to $\Delta\phi$



1. **Beer–Lambert:** $q = \alpha_{abs} \cdot P_{inj}$ [W/m]
2. **Brown–Hoffman:** $\Delta T_{ss} = \alpha_{abs} \cdot P_{inj} \cdot \Gamma / (4\pi k)$,
 $\Gamma \approx 480$
3. **Churchill–Chu convection:** $h \approx 93.3$ W/m²K for
 $D = 125$ μ m
4. **Lumped capacitance** (Incropera 2011): $\tau_{th} = \rho c_p \cdot b / (2h) \approx 0.518$ s, $f_c \approx 0.307$ Hz

$$\Delta\phi(t) = \Delta\phi_{ss} (1 - e^{-t/\tau_{th}})$$

$$\Delta\phi_{ss} = \frac{L \alpha_{abs}(\lambda_E) P_{inj}}{2 \lambda k} \xi \Gamma$$

Single adversarial knob: $\alpha_{abs}(\lambda_E)$.
All other quantities are fixed by the
SMF-28 deployment



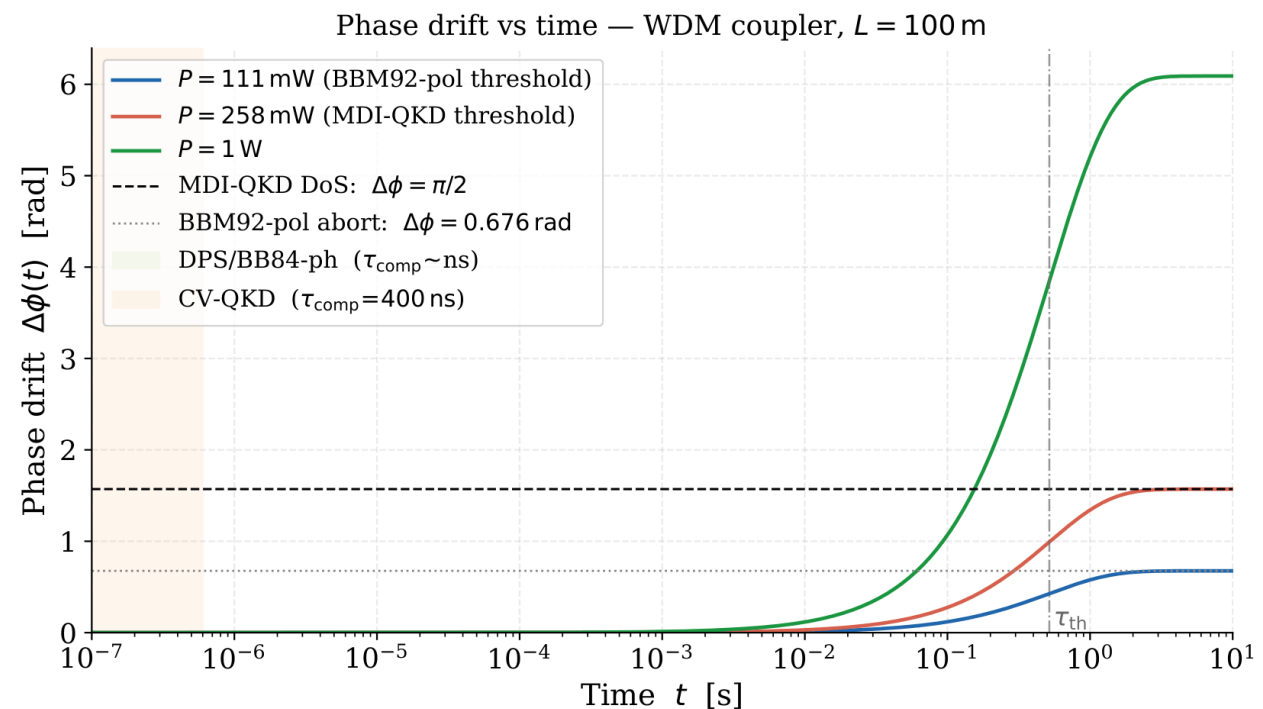
WDM scenario

DoS threshold: $P_{th} = \pi \lambda k / (L \cdot \alpha_{abs} \cdot \xi \cdot \Gamma) \rightarrow$
 $P \cdot L = 25.8 \text{ W} \cdot \text{m}$ (Power needed to reach a $\pi/2$ rotation)

Three representative values: 258 mW at $L = 100 \text{ m}$, 25.8 mW at $L = 1 \text{ km}$, 2.6 mW at $L = 10 \text{ km}$

At $2 \times P_{th}$: $t_{DoS} = \tau_{th} \cdot \ln 2 \approx 0.36 \text{ s}$ — **sub-second attack**

ΔT at threshold: 0.33 mK — thermally covert, below DTS sensitivity by four orders of magnitude



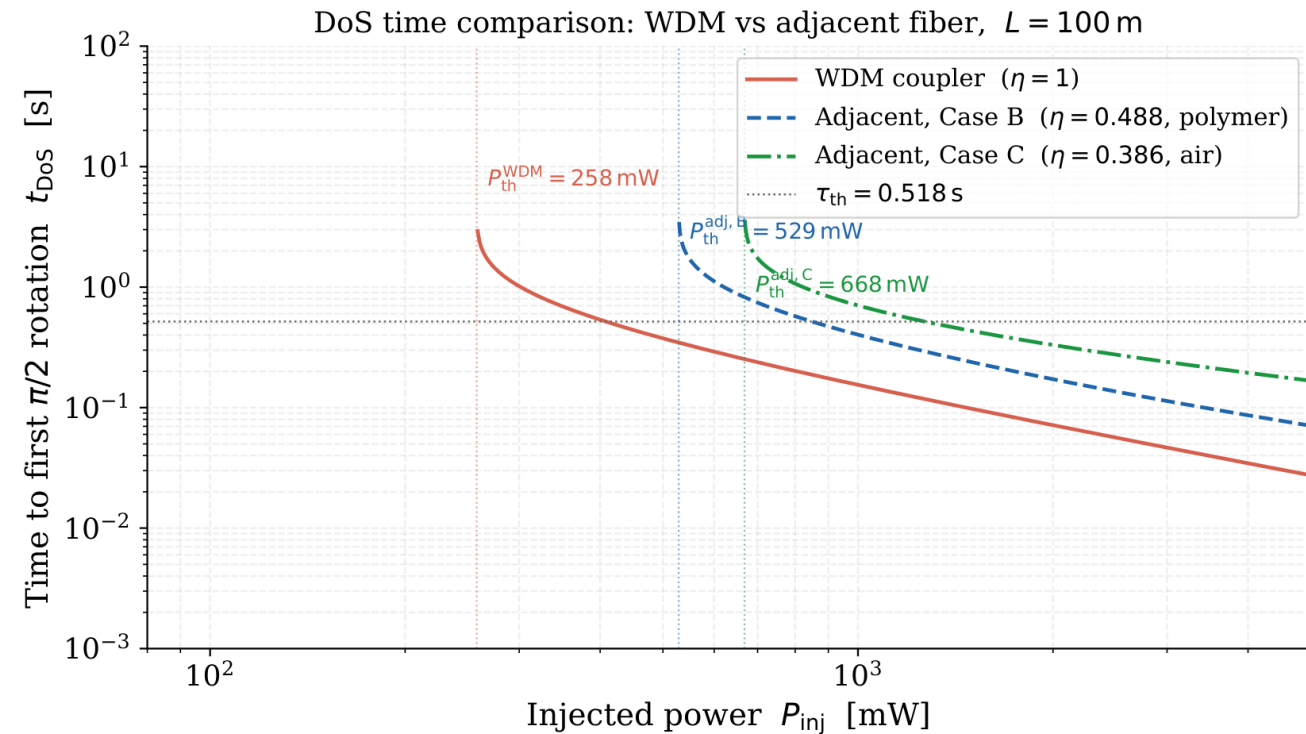


Adjacent scenario

Two-cylinder lumped system $\rightarrow$ matrix ODE $\rightarrow$ eigenvalues $\lambda_1 = -1/\tau_{th}$ (slow, κ -independent), $\lambda_2 = -(1+2\kappa)/\tau_{th}$ (fast)

Coupling efficiency: $\eta_{coup} = \kappa/(1+2\kappa) \rightarrow 1/2$ (universal limit, independent of cable geometry)

Four cable cases A–D: polymer-filled cases deviate $< 4\%$ from $1/2$; air-filled cases deviate $16\text{--}23\%$





Immunity Criterion

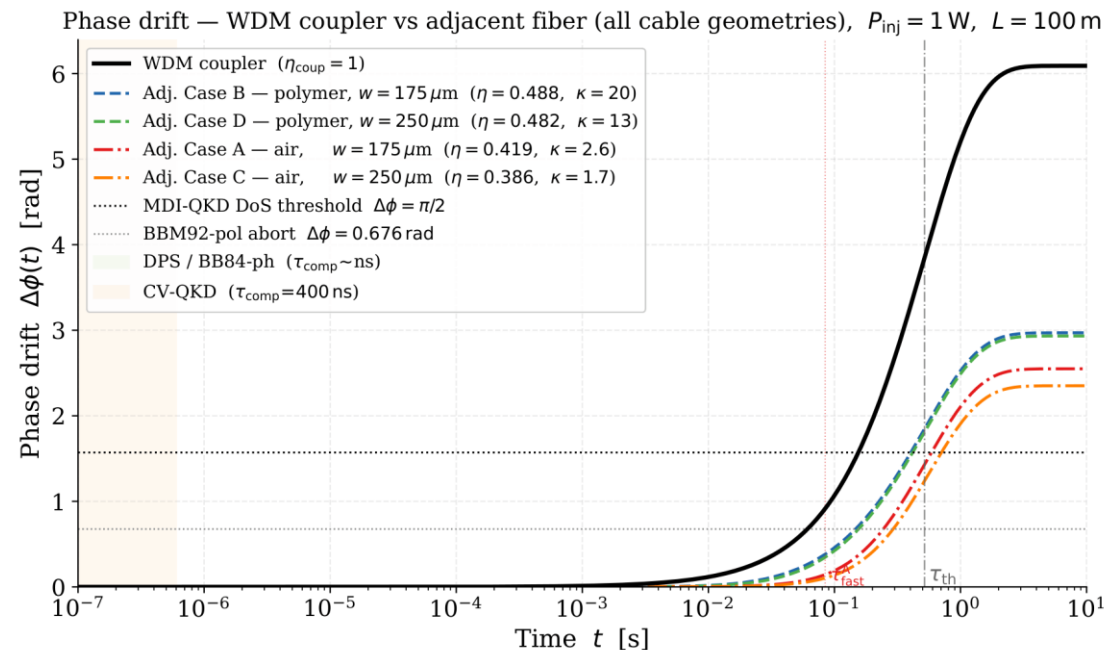
Key dichotomy: **absolute phase** (km-scale separate paths) vs **differential phase** (co-propagating pulses)

Differential operation is a discrete-time differentiator:
 $|H(f)| \approx \tau_{\text{comp}}/\tau_{\text{th}}$ at low f

Immunity criterion: $\tau_{\text{comp}} \ll (\pi/2) \cdot \tau_{\text{th}}/\Delta\phi_{\text{ss}}$

At benchmark (50 W, 100 m, α^*): bound ≈ 2.7 ms — any ns-scale implementation is immune by 6+ orders of magnitude

At 100 ps (DPS-QKD): suppression factor $\approx 2 \times 10^{-10}$





Protocol Classification

Protocol	τ_{comp}	$\delta\phi_{\text{max}}$ or $\Delta\phi_{\text{ss}}$	Verdict
TF-QKD	$\sim\tau_{\text{th}}$	969π	Vulnerable
MDI-QKD	$\sim\tau_{\text{th}}$	97π	Vulnerable
Pol. BBM92	$\sim\tau_{\text{th}}$	97π	Vulnerable
Time-bin BBM92	1 ns	5.9×10^{-7} rad	Immune
DPS-QKD	100 ps	5.9×10^{-8} rad	Immune
COW-QKD	1.6 ns	9.4×10^{-7} rad	Immune †
CV-QKD	400 ns	0.24 mrad	Immune
BB84-ph / SARG04	5 ns	2.9 μ rad	Immune

† COW-QKD has a secondary photon-loss side channel via WDM coupler insertion loss



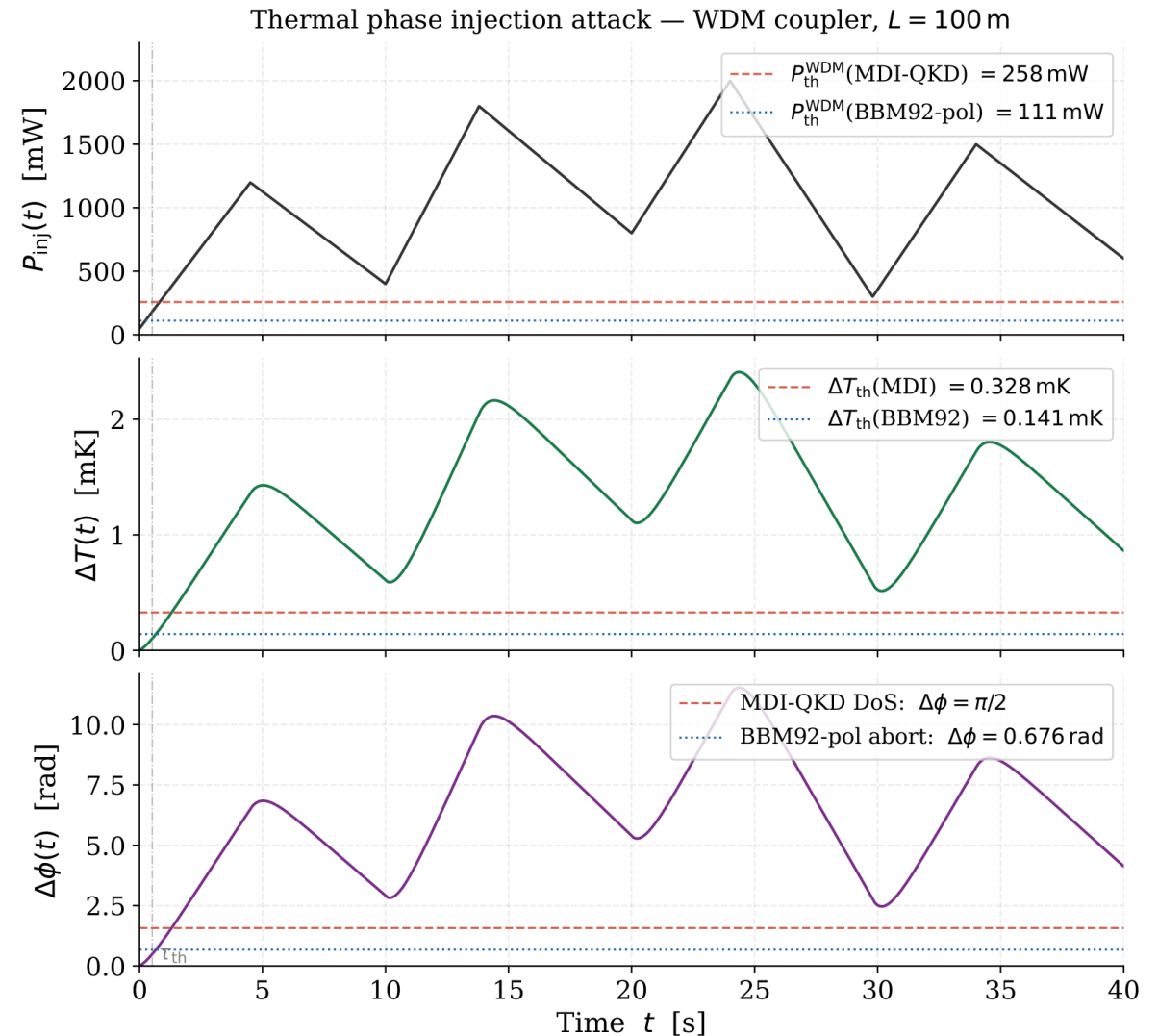
Numerical Validation

Implicit-Euler integration of the lumped-capacitance ODE for an arbitrary $P_{\text{inj}}(t)$ waveform

Verified against the closed-form ramp solution to $<0.01\%$ relative error

Key verification: $\Delta T_{\text{ss}}(258 \text{ mW}) = 0.33 \text{ mK}$,
 $P_{\text{th}}^{\text{WDM}} \cdot L = 25.79 \text{ W} \cdot \text{m} \checkmark$

The attack is operationally indistinguishable from environmental drift

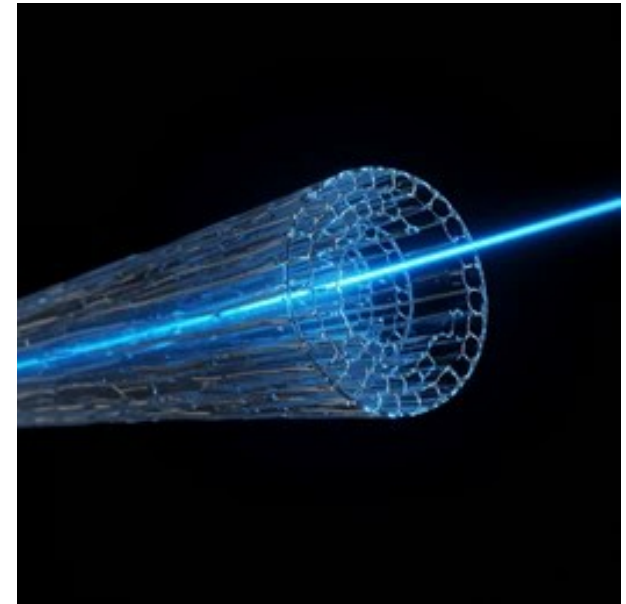




Modelling uncertainty: Brown–Hoffman dn/dT vs Rego 2024 (~22% conservative bias), bare fiber vs coated fiber (~30% understatement), net $\pm 30\%$ on P_{th} — **does not change protocol classification** (margin is orders of magnitude)

Countermeasures:

- Hollow-core fiber: S_ϕ reduced $\sim 20\times$
- Active phase stabilization: loop must track drift rate $\Delta\phi_{ss}/\tau_{th}$, not absolute travel
- Distributed Temperature Sensing (DTS): $\Delta T_{threshold} \approx 33 \mu K$ vs 1 K DTS accuracy $\rightarrow$ only partial detection at substantial overhead above threshold (Bao & Chen 2012)



Cross-layer picture: no prior physical-layer countermeasure stack addresses this attack; thermal isolation is structurally novel



Conclusions

- 1. Physical model:** Master formula $\Delta\varphi_{ss} = L \cdot \alpha_{abs} \cdot P_{inj} \cdot \xi \cdot \Gamma / (2\lambda k)$; $\tau_{th} \approx 0.518$ s; $f_c \approx 0.307$ Hz
- 2. WDM scenario:** 258 mW at $L = 100$ m (MDI-QKD); sub-second t_{DoS} at $2 \times P_{th}$
- 3. Adjacent fiber:** $\eta_{coup} \rightarrow 1/2$ universally; factor $\times 2.05$ – 2.59 above WDM threshold
- 4. Protocol classification:** 3 vulnerable (TF-QKD, MDI-QKD, pol-BBM92); 6 immune; immunity criterion $\tau_{comp} \ll (\pi/2) \cdot \tau_{th} / \Delta\varphi_{ss}$

First physical-channel DoS attack targeting absolute phase in DV QKD, realizable with off-the-shelf hardware



Thank you for your attention.

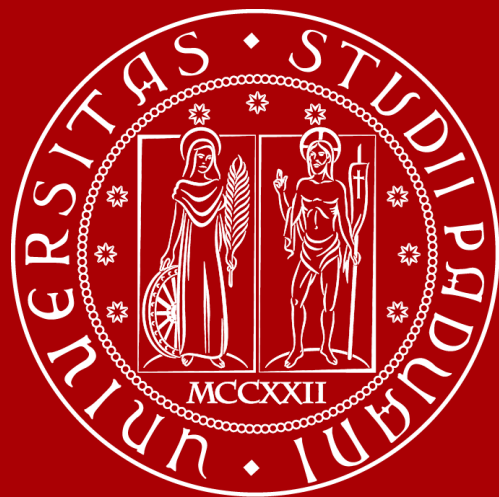
Takeaway: 3 vulnerable, 6 immune protocols

$$\Delta\phi(t) = \Delta\phi_{ss} \left(1 - e^{-t/\tau_{th}}\right)$$

$$\Delta\phi_{ss} = \frac{L \alpha_{abs}(\lambda_E) P_{inj}}{2 \lambda k} \xi \Gamma$$

Protocol	τ_{comp}	$\delta\phi_{max}$ or $\Delta\phi_{ss}$	Verdict
TF-QKD	$\sim\tau_{th}$	969π	Vulnerable
MDI-QKD	$\sim\tau_{th}$	97π	Vulnerable
Pol. BBM92	$\sim\tau_{th}$	97π	Vulnerable
Time-bin BBM92	1 ns	5.9×10^{-7} rad	Immune
DPS-QKD	100 ps	5.9×10^{-8} rad	Immune
COW-QKD	1.6 ns	9.4×10^{-7} rad	Immune †
CV-QKD	400 ns	0.24 mrad	Immune
BB84-ph / SARG04	5 ns	2.9 μ rad	Immune

† COW-QKD has a secondary photon-loss side channel via WDM coupler insertion loss



UNIVERSITÀ
DEGLI STUDI
DI PADOVA