Quantum Cryptography & Quantum Hacking

Hacking the „un-hackable“

Lecturer: Vinzenz Vogel, Viola Hansjakob

- Paper by Lars Lydersen et. al. 2010:
  Hacking commercial quantum cryptography systems by tailored bright illumination

- Two commercial systems hacked: Clavis2 (ID Quantique), QPN 5505 (MagiQ Technologies)

- Trojan Horse attack

Outline

- Introduction
- A basic QKD protocol: BB84
- How can QKD be hacked?
- Example: The Trojan Horse attack
- Conclusion

Introduction

- Cryptography is totally safe if one-time-pad is used to encrypt the message

Introduction

- Cryptography is totally safe if one-time-pad is used to encrypt the message

Introduction

- Cryptography is totally safe if one-time-pad is used to encrypt the message

Example: One-time-pad

	D	O	O	Z	Y	Message

Introduction

- Cryptography is totally safe if one-time-pad is used to encrypt the message

Example: One-time-pad

	D	**O**	**O**	**Z**	**Y**	**Message**
	3 (D)	14 (O)	14 (O)	25 (Z)	24 (Y)	Message

Introduction

- Cryptography is totally safe if one-time-pad is used to encrypt the message

Example: One-time-pad

	D	**O**	**O**	**Z**	**Y**	**Message**
	3 (D)	14 (O)	14 (O)	25 (Z)	24 (Y)	Message
+	23	12	2	10	11	Key

Introduction

- Cryptography is totally safe if one-time-pad is used to encrypt the message

Example: One-time-pad

	D	**O**	**O**	**Z**	**Y**	**Message**
	3 (D)	14 (O)	14 (O)	25 (Z)	24 (Y)	Message
+	23	12	2	10	11	Key
= (mod 26)	0 (A)	0 (A)	16 (Q)	9 (J)	10 (K)	Message + Key

Introduction

- Cryptography is totally safe if one-time-pad is used to encrypt the message

Example: One-time-pad

	D	O	O	Z	Y	Message
	3 (D)	14 (O)	14 (O)	25 (Z)	24 (Y)	Message
+	23	12	2	10	11	Key
= (mod 26)	0 (A)	0 (A)	16 (Q)	9 (J)	10 (K)	Message + Key
	A	**A**	**Q**	**J**	**K**	**cipher text**

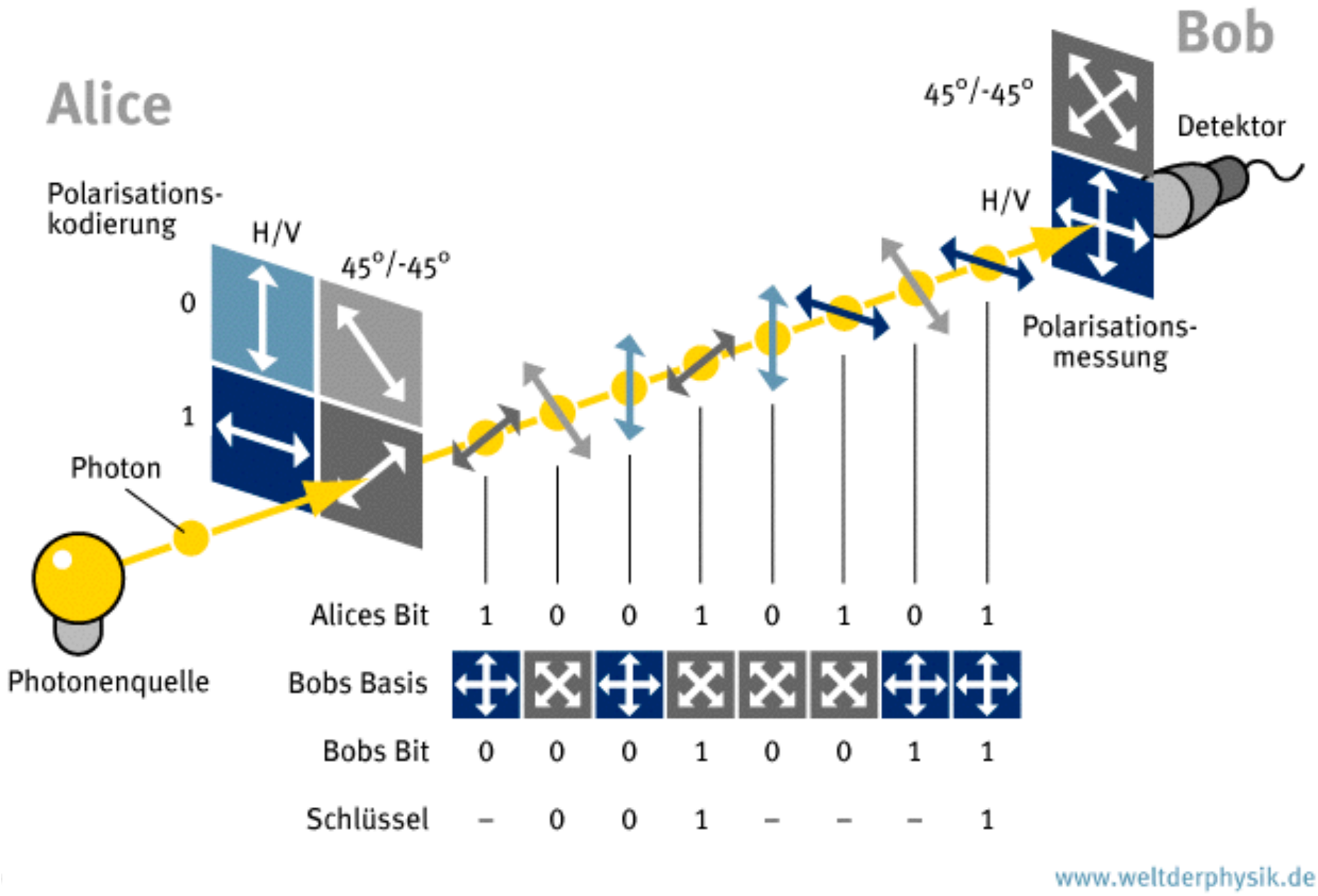
Introduction

- Cryptography is totally safe if one-time-pad is used to encrypt the message
- Problem: Safe distribution of key
- Solution: Quantum key distribution (QKD)

A basic QKD protocol: BB84

- Proposed in 1984 by Charles H. Bennett and Gilles Brassard
- Works by sending single photons from Alice to Bob
- Security check with simple photon statistics

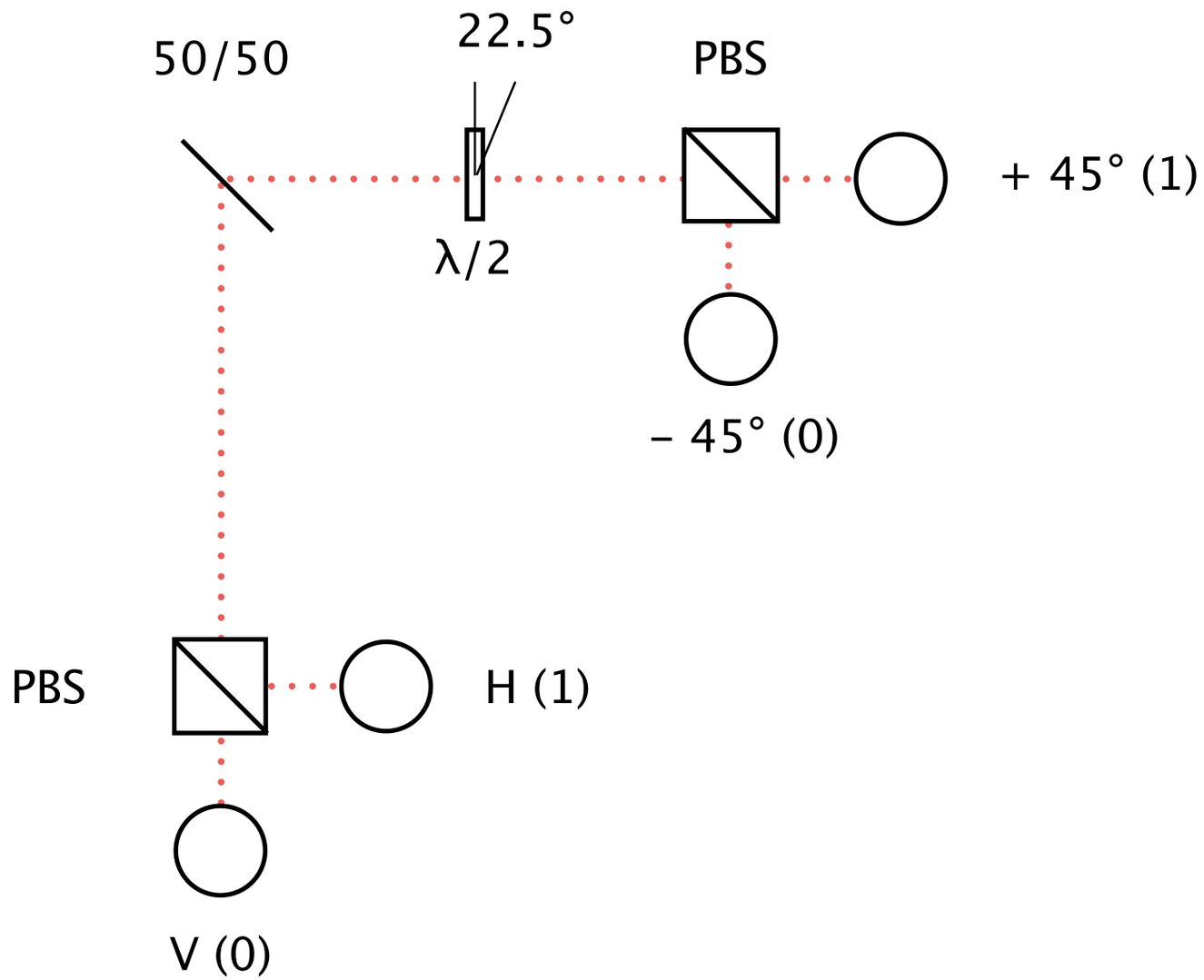
A basic QKD protocol: BB84



http://www.weltderphysik.de/gebiet/technik/quanten-technik/quanten-kryptographie/

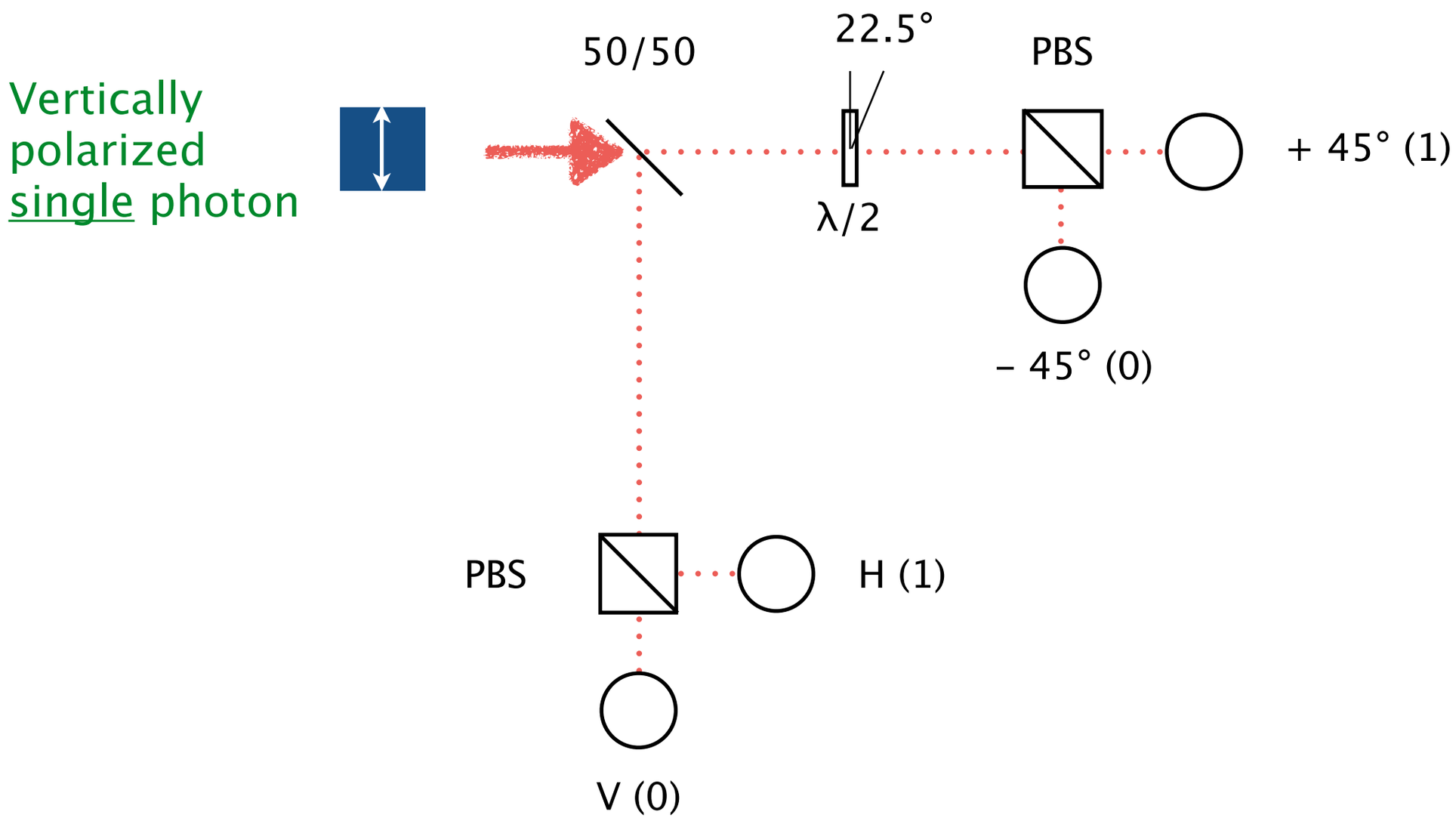
A basic QKD protocol: BB84

Bob´s perfectly random basis choice:



A basic QKD protocol: BB84

Bob´s perfectly random basis choice:

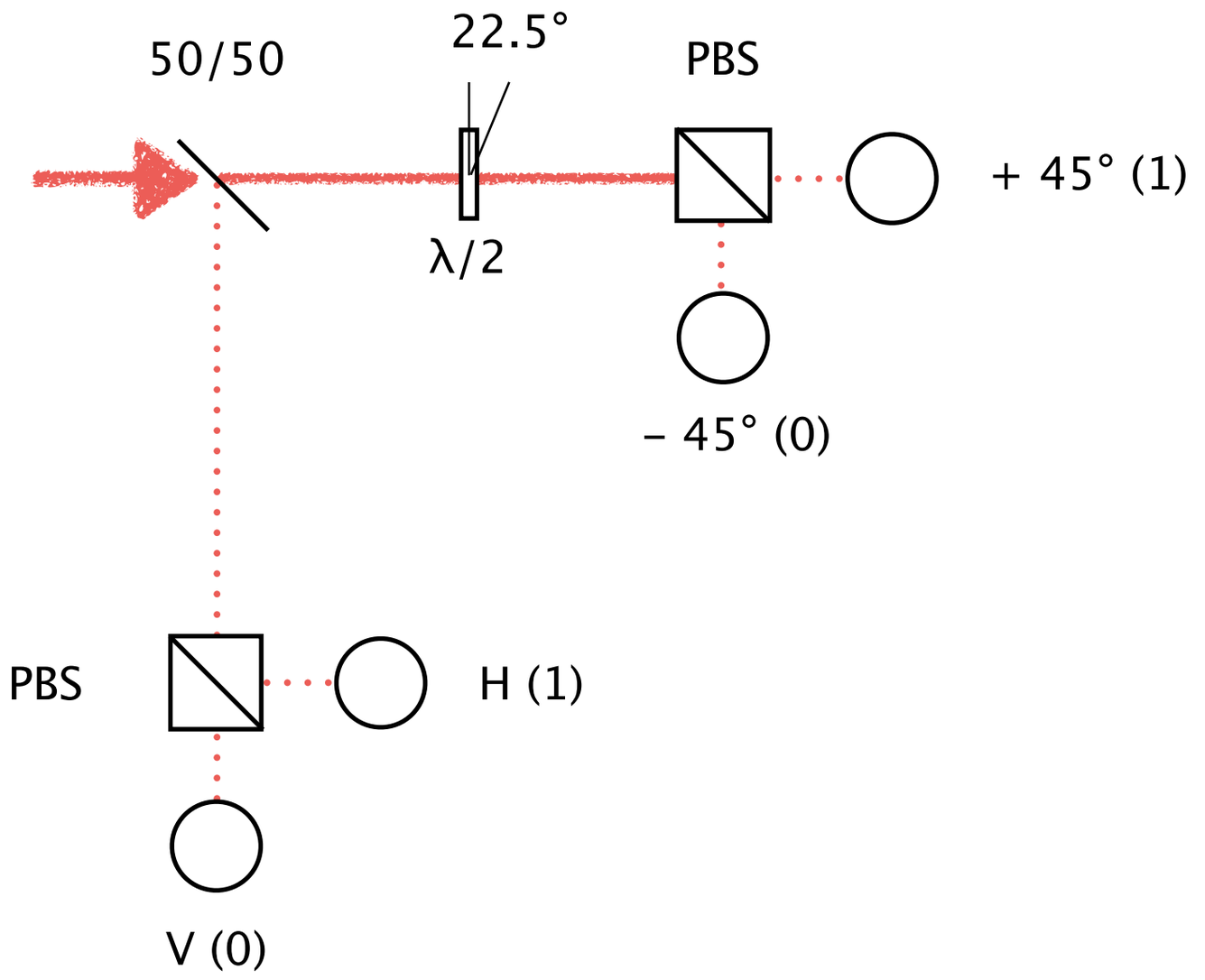


A basic QKD protocol: BB84

Bob´s perfectly random basis choice:

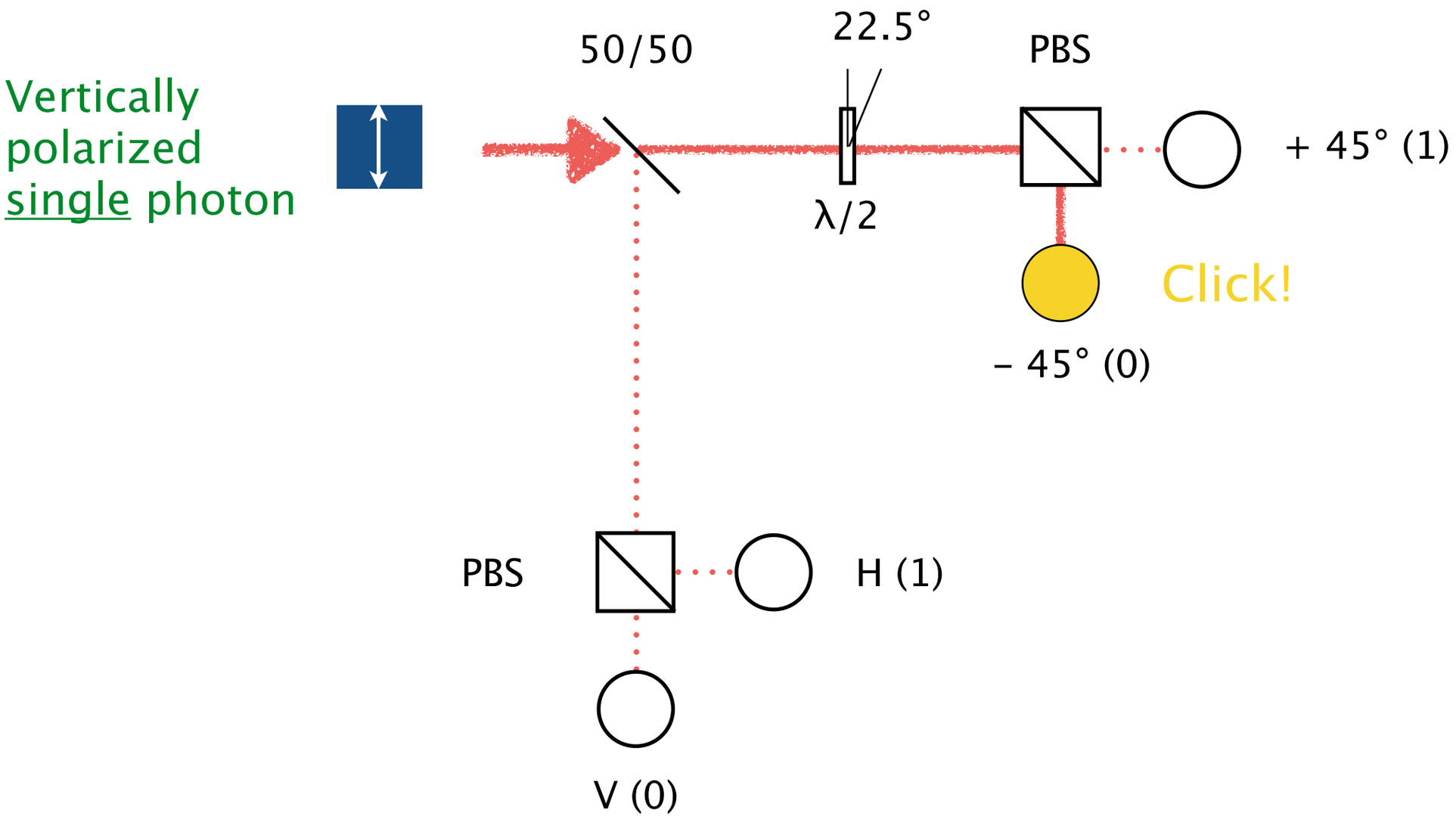
The basis of the photon is rotated into „+45°/–45°“ basis.

Vertically polarized single photon

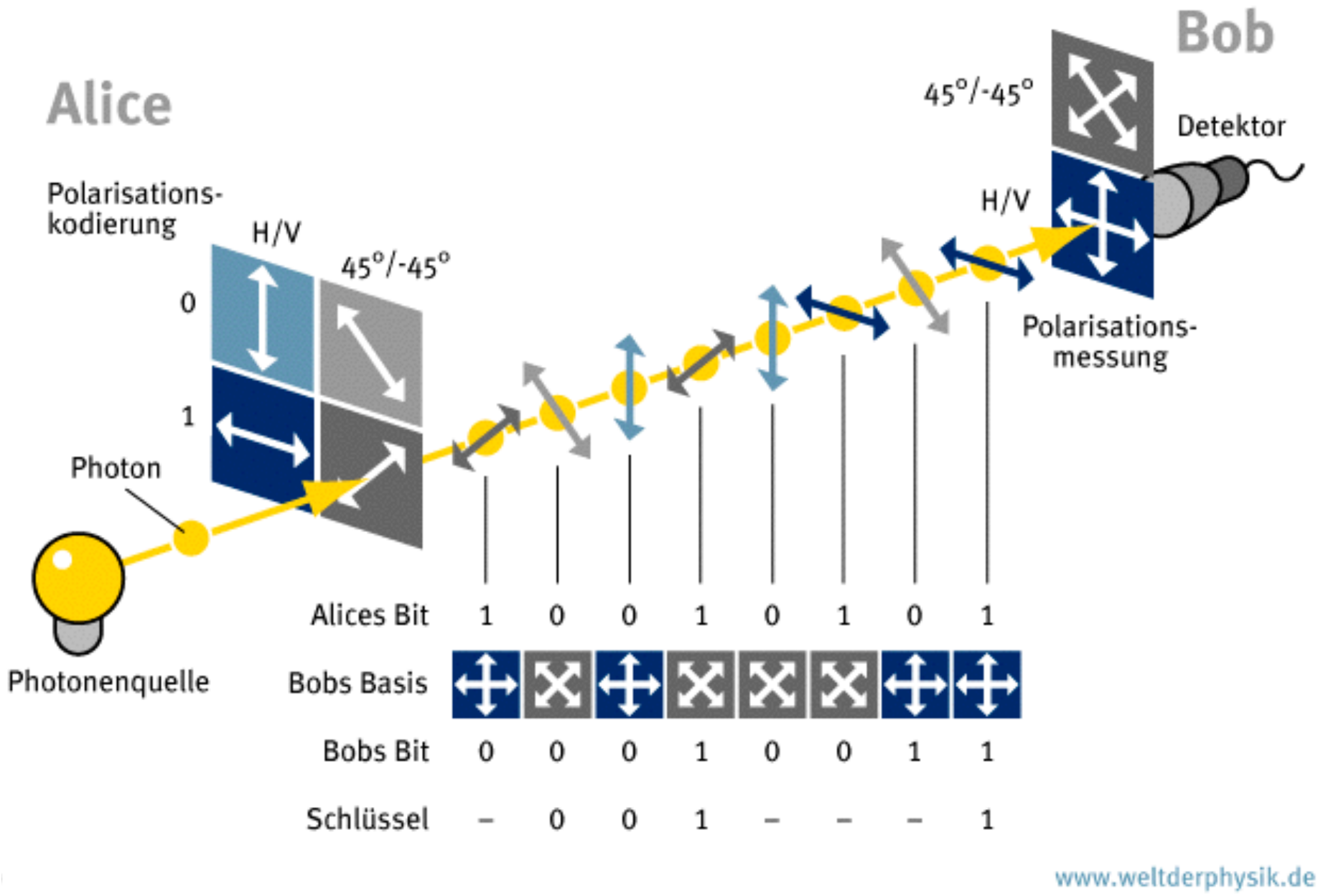


A basic QKD protocol: BB84

Bob´s perfectly random basis choice:



A basic QKD protocol: BB84



http://www.weltderphysik.de/gebiet/technik/quanten-technik/quanten-kryptographie/

A basic QKD protocol: BB84

<u>Secure under the following assumptions:</u>

- True random basis choice of Alice/Bob
- No one knows the basis choice of Alice/Bob
- Random choice of bits
- Use single photons

How can QKD be hacked?

How can QKD be hacked?

QKD can´t be hacked in theory…

How can QKD be hacked?

QKD can´t be hacked in theory…

…but in practice, if the security assumptions are violated!

How can QKD be hacked?

Exploit loopholes to violate assumptions!

How can QKD be hacked?

- Photon number splitting
  (violation: non-single photon sources are used)

- Trojan Horse attack
  (violation: Bob´s basis choice is known/dictated by Eve)

How can QKD be hacked?

- Photon number splitting
  (violation: non-single photon sources are used)

- Trojan Horse attack
  (violation: Bob´s basis choice is known/dictated by Eve)

Example: The Trojan Horse attack

<u>Basic idea of the attack:</u>

- Goal:
    - Eve interferes the communication and makes a measurement
    - Eve is able to dictate what Bob measures

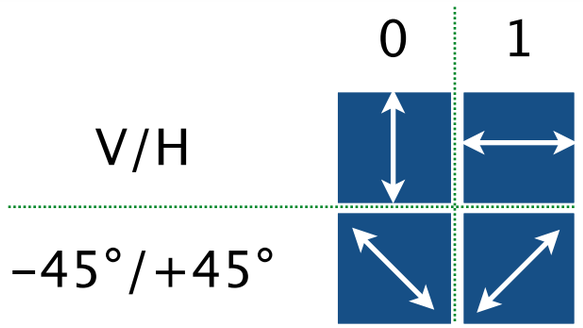
Example: The Trojan Horse attack

Basic idea of the attack:

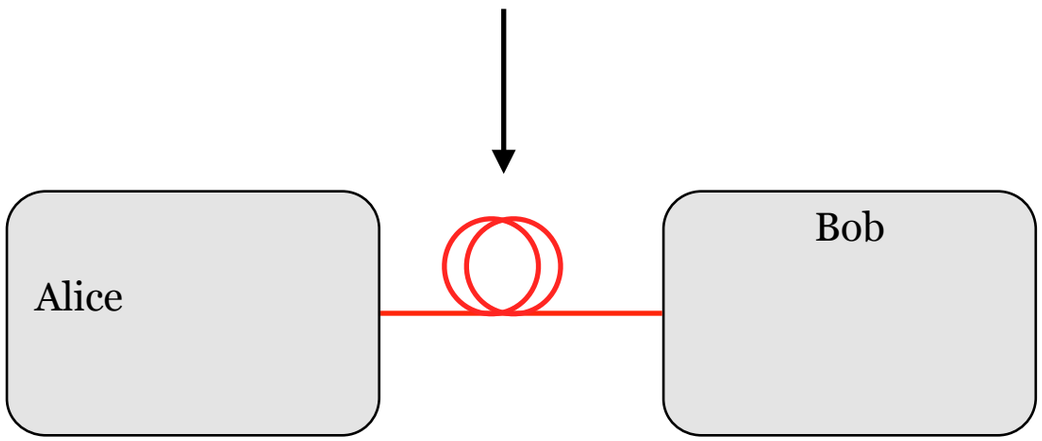
- Goal:
    - Eve interferes the communication and makes a measurement
    - Eve is able to dictate what Bob measures
- Approach:
    - Technical loophole: Bob´s photon detector (Avalanche photo diode, APD)

Example: The Trojan Horse attack

Basic scheme:



BB84

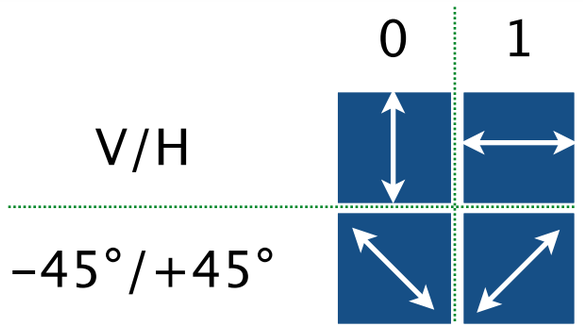


QM

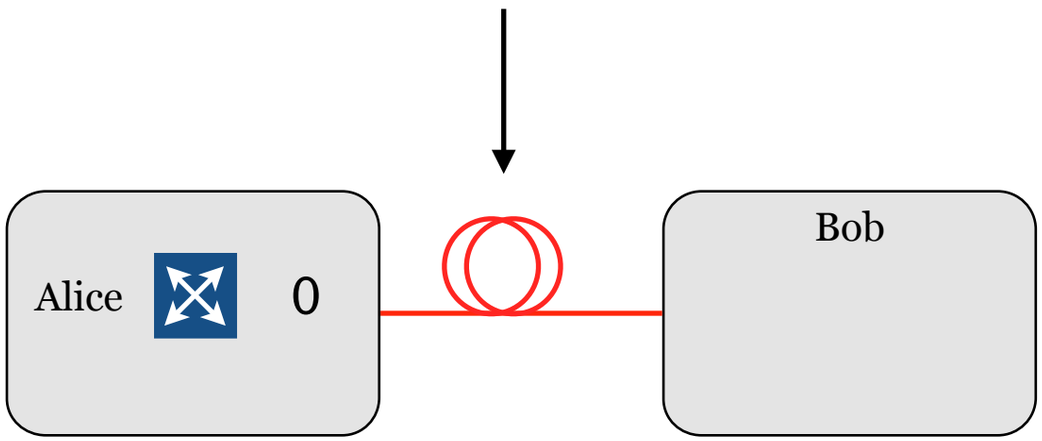
http://arxiv.org/pdf/1008.4593v2.pdf

Example: The Trojan Horse attack

Basic scheme:



BB84

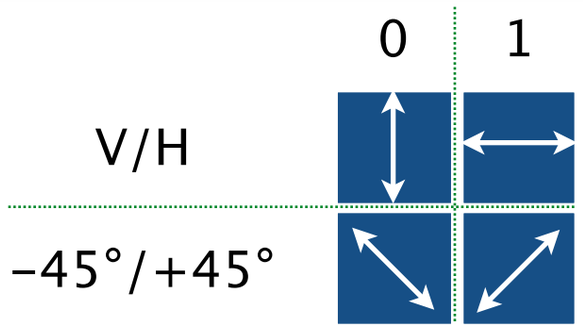


QM

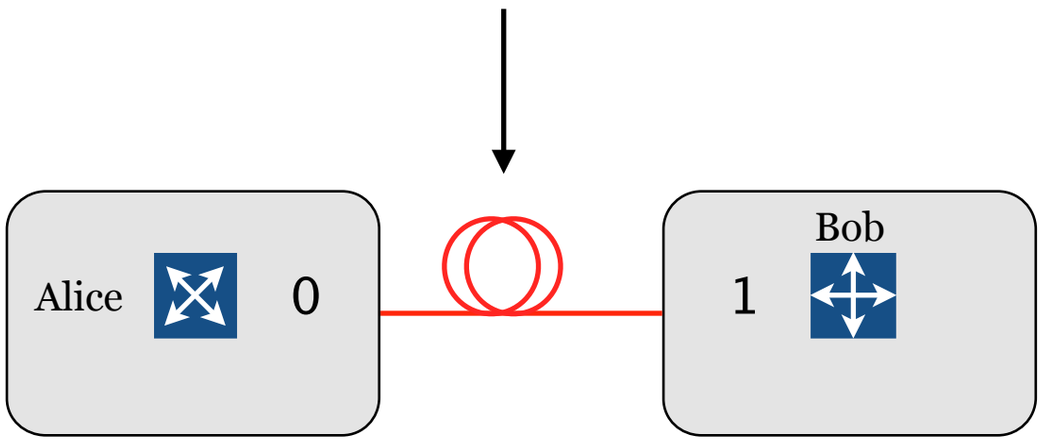
http://arxiv.org/pdf/1008.4593v2.pdf

Example: The Trojan Horse attack

Basic scheme:



BB84

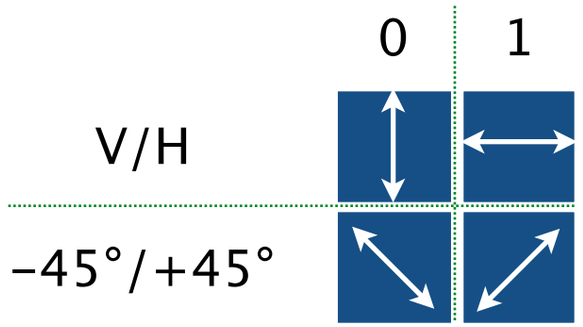


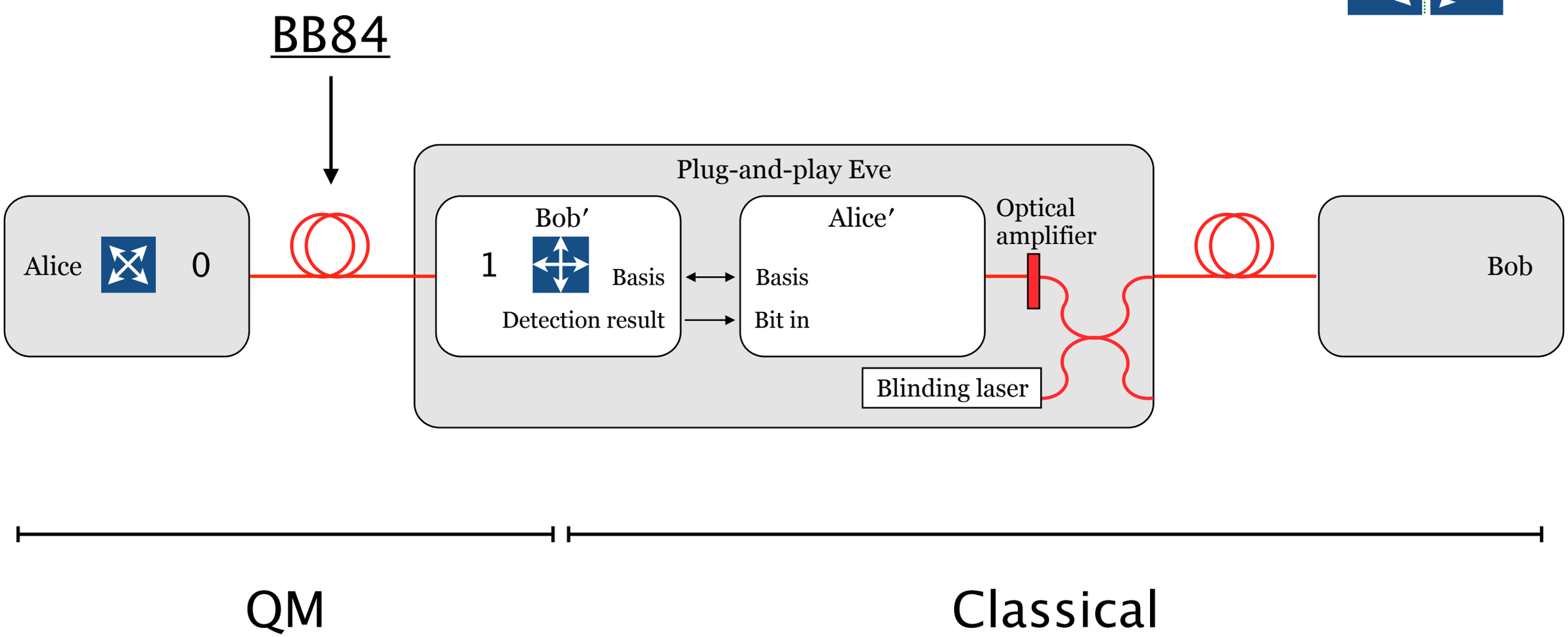
QM

http://arxiv.org/pdf/1008.4593v2.pdf

Example: The Trojan Horse attack

Basic scheme:

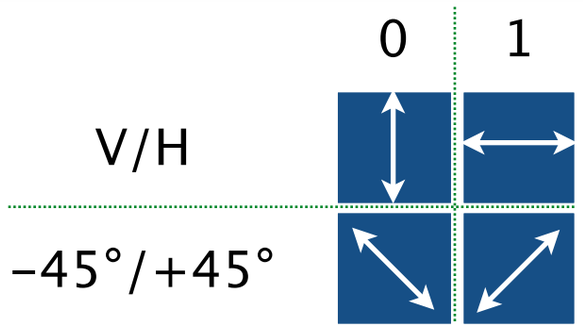




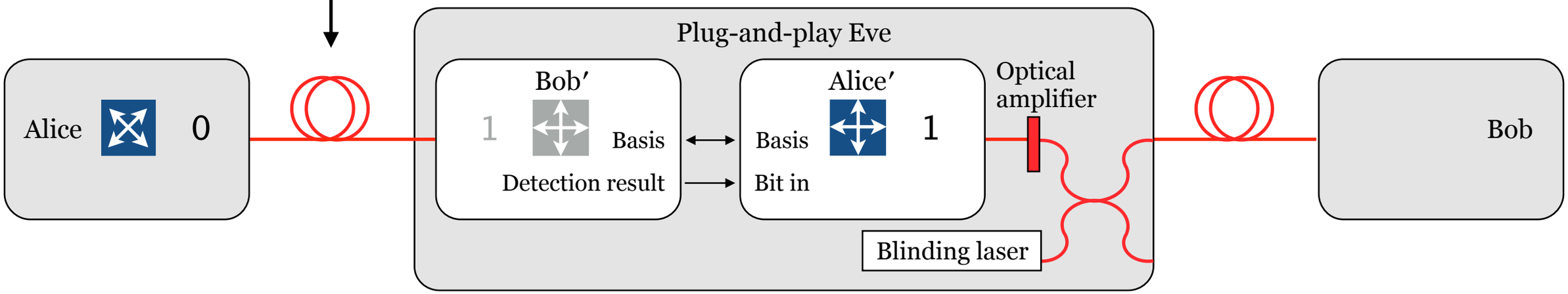
http://arxiv.org/pdf/1008.4593v2.pdf

Example: The Trojan Horse attack

Basic scheme:



BB84



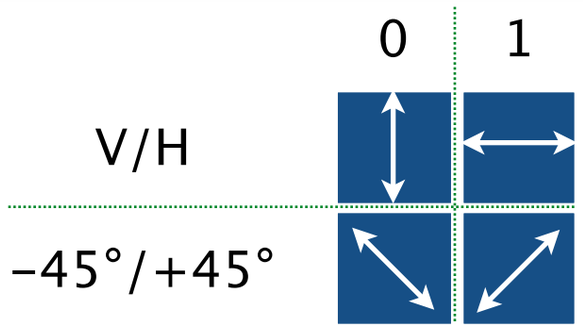
QM

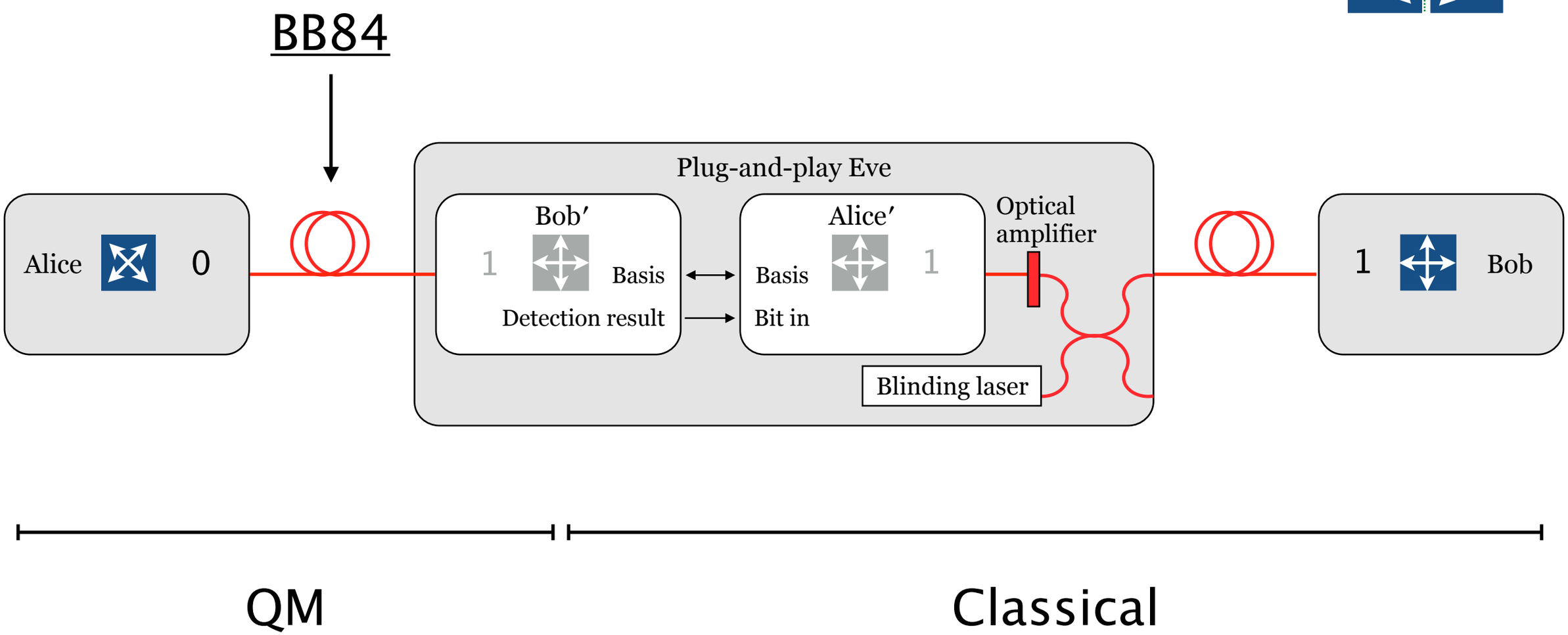
Classical

http://arxiv.org/pdf/1008.4593v2.pdf

Example: The Trojan Horse attack

Basic scheme:





http://arxiv.org/pdf/1008.4593v2.pdf

Example: The Trojan Horse attack

The only question remaining:

How can Eve take control of Bob´s detectors?

Example: The Trojan Horse attack

Bob´s APDs (photon detectors) **have two operating modes:**

Example: The Trojan Horse attack

Bob´s APDs (photon detectors) **have two operating modes:**

1. **Linear mode** (gives signal linear to incoming intensity, **click** if incoming signal power is over a **threshold**; basically it **behaves like a normal photo diode**)

Example: The Trojan Horse attack

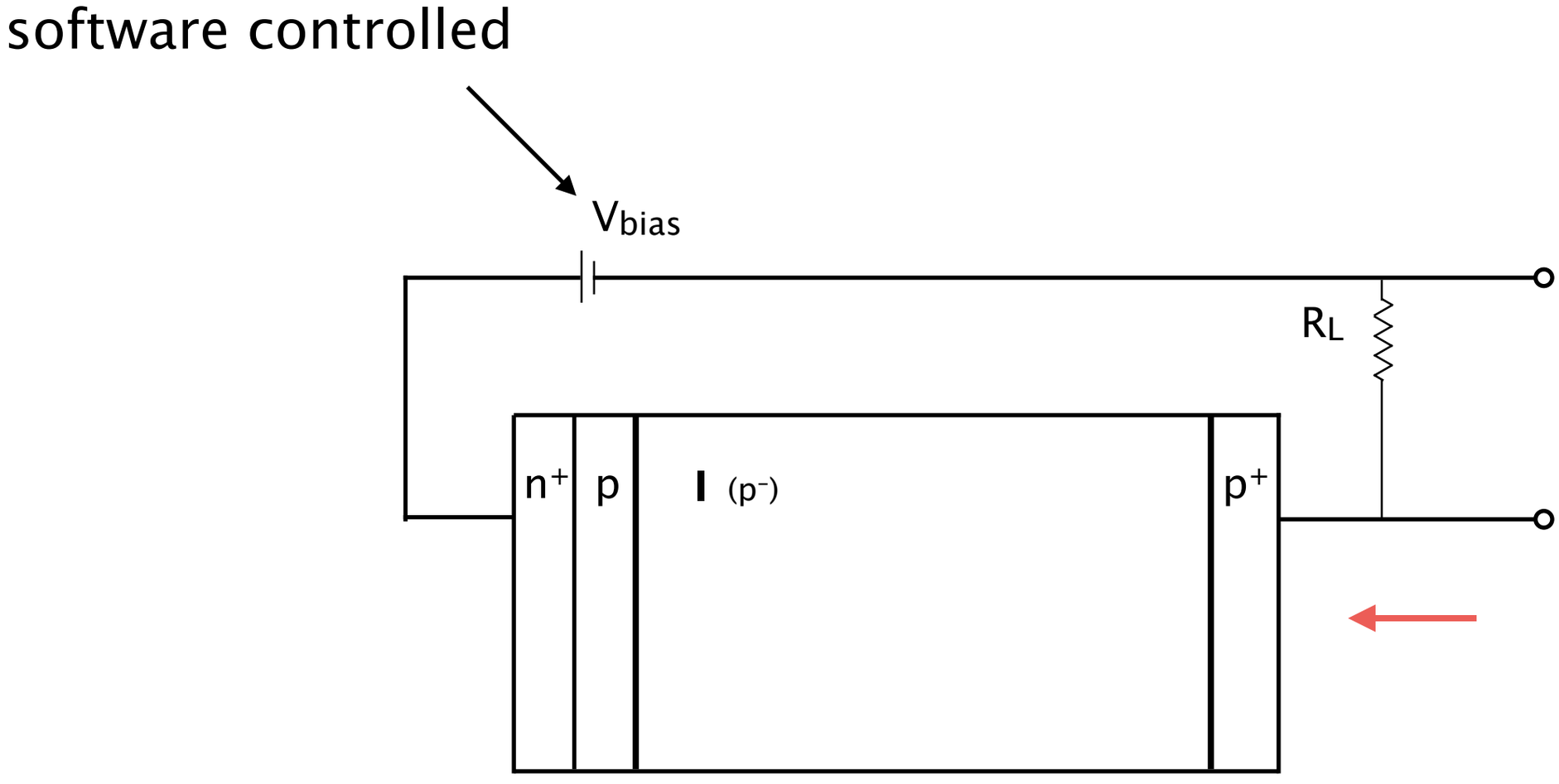
Bob´s APDs (photon detectors) **have two operating modes:**

1. **Linear mode** (gives signal linear to incoming intensity, **click** if incoming signal power is over a **threshold**; basically it **behaves like a normal photo diode**)

2. **Geiger mode** (counting single photons, **click** if **single photon** comes in, efficiency <50%)

Example: The Trojan Horse attack

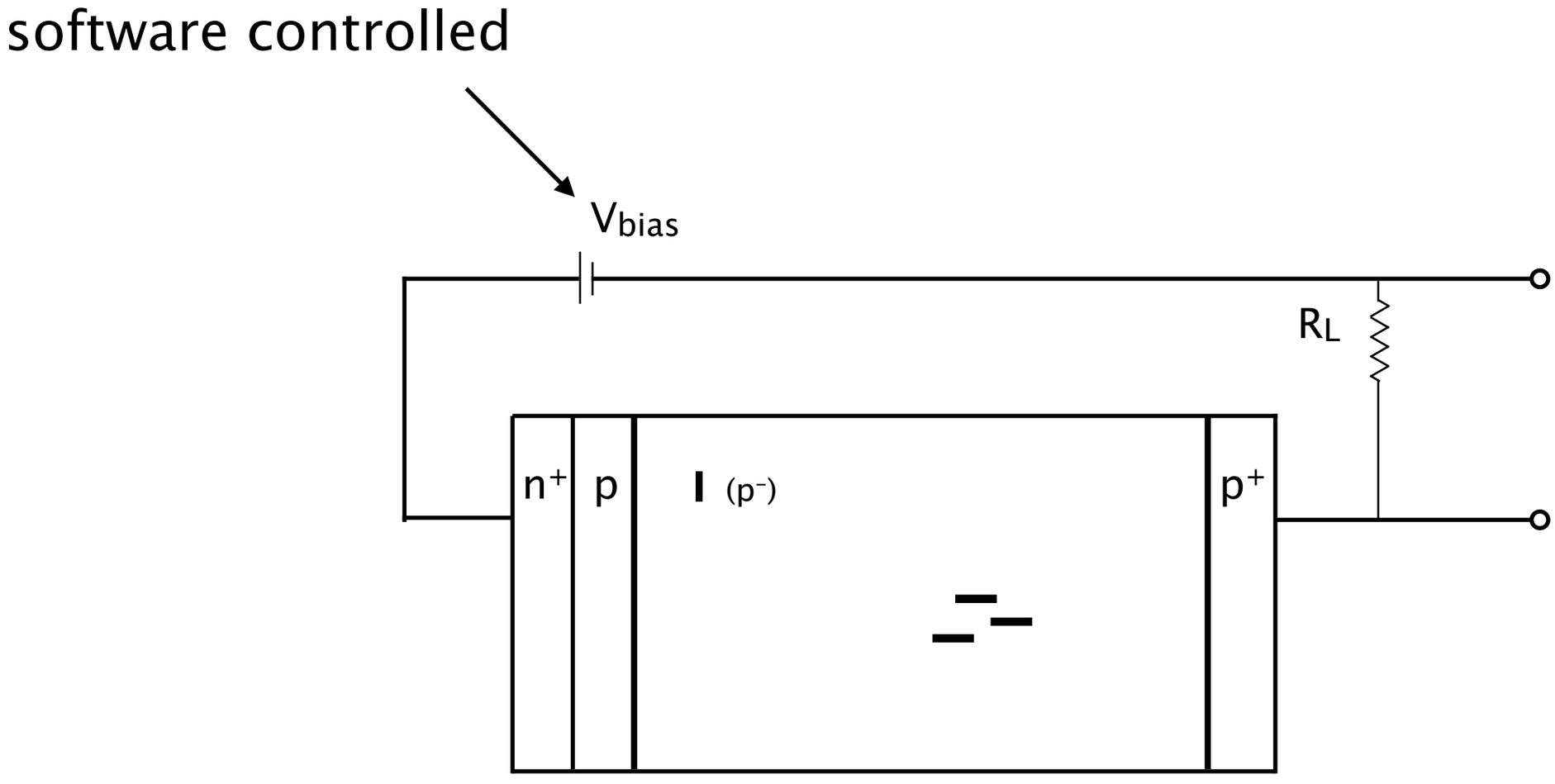
Linear mode: $V_{bias} < V_{br}$



http://www.globalspec.com/reference/21446/160210/chapter-14-4-1-avalanche-photodiode

Example: The Trojan Horse attack

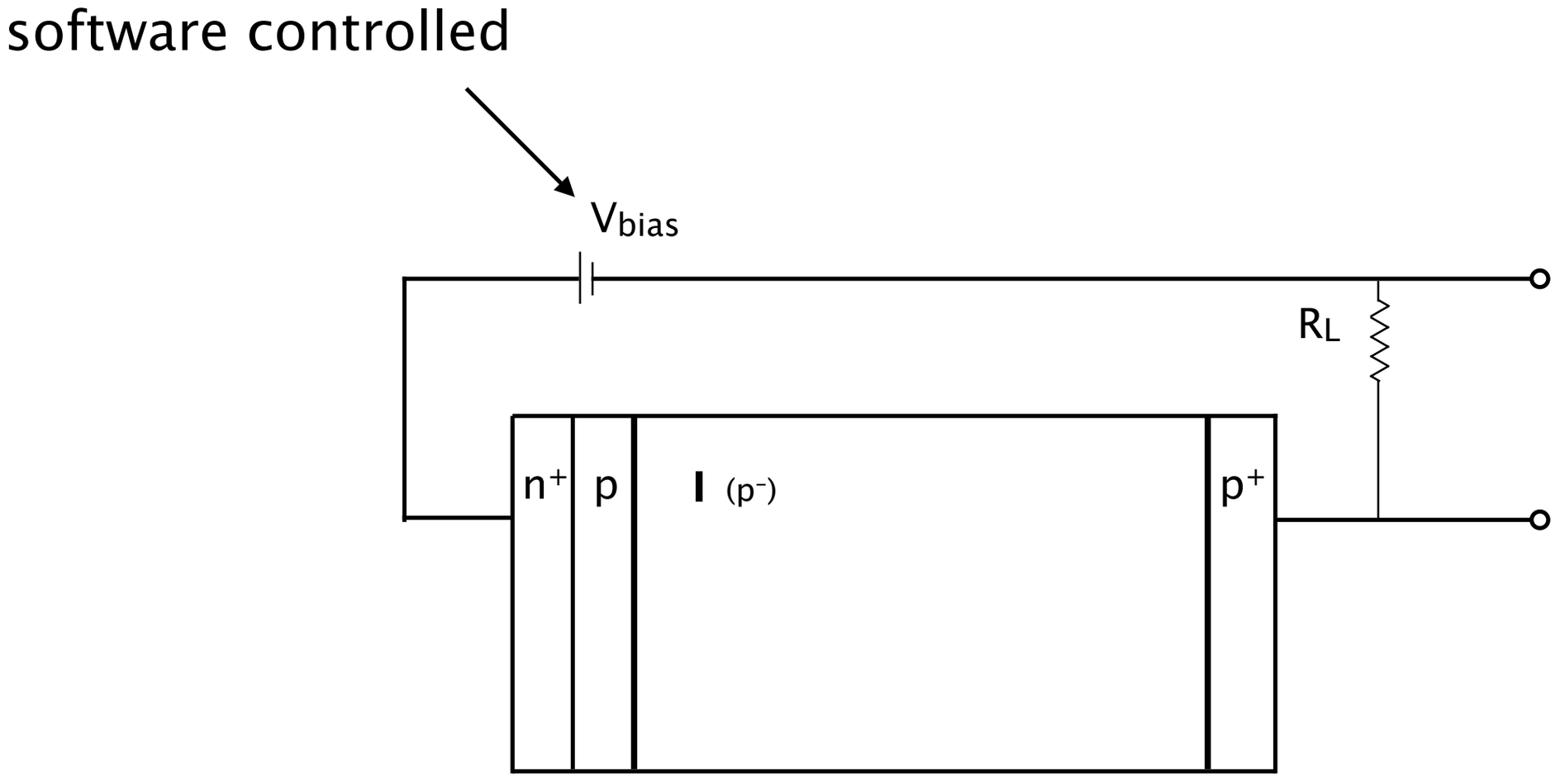
Linear mode: $V_{bias} < V_{br}$



http://www.globalspec.com/reference/21446/160210/chapter-14-4-1-avalanche-photodiode

Example: The Trojan Horse attack

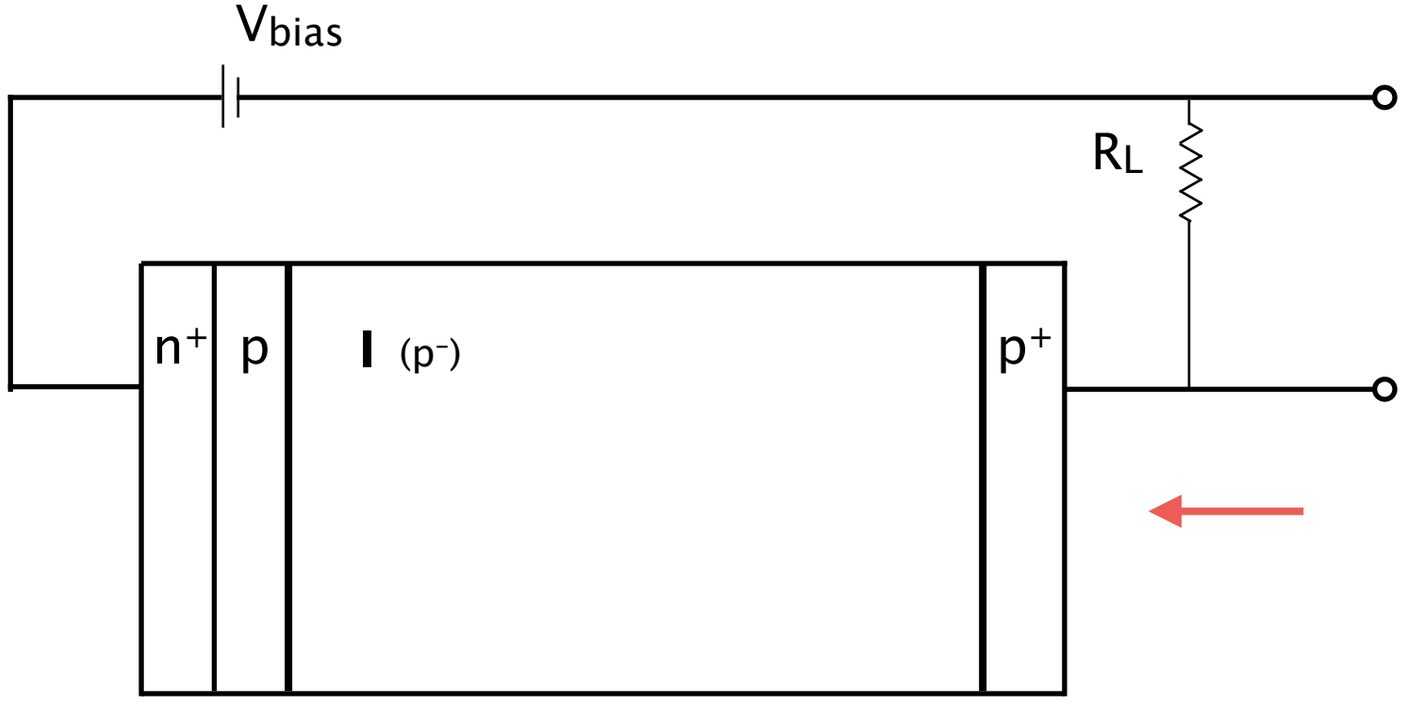
Linear mode: $V_{bias} < V_{br}$



http://www.globalspec.com/reference/21446/160210/chapter-14-4-1-avalanche-photodiode

Example: The Trojan Horse attack

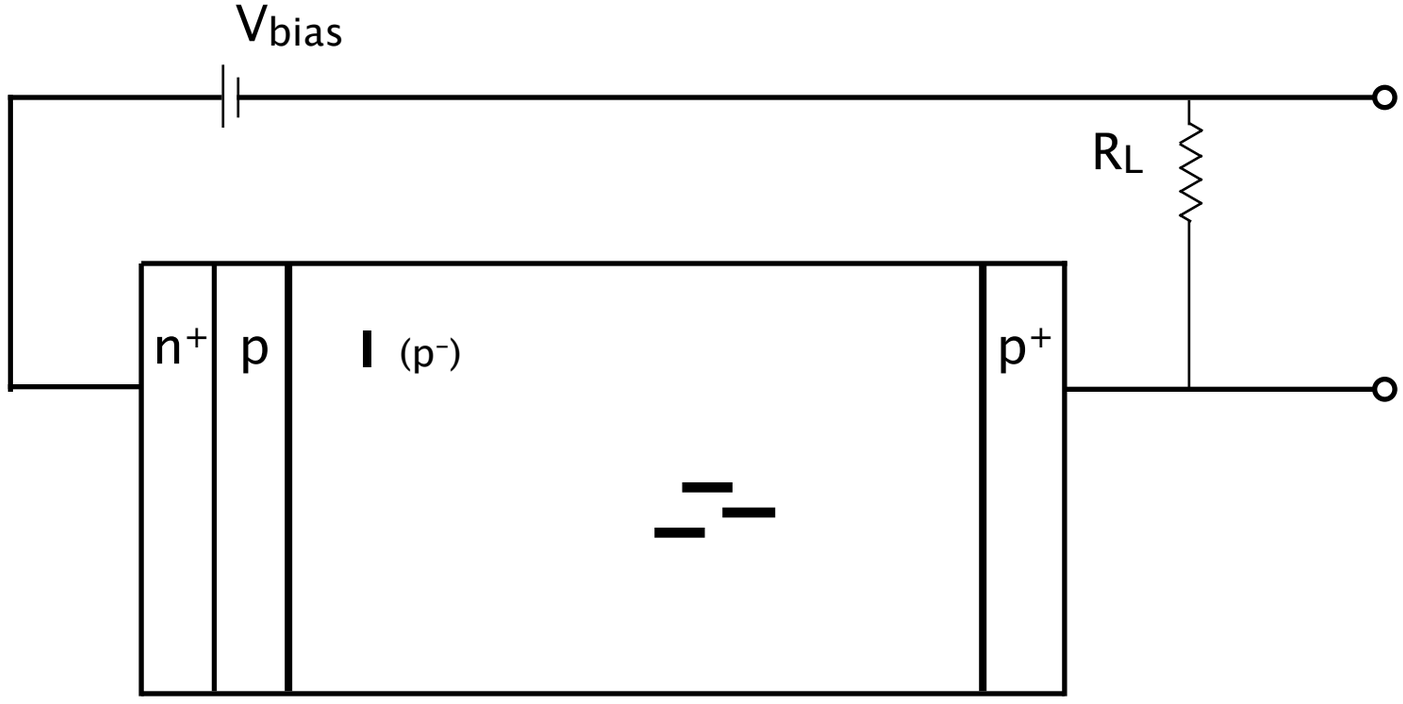
Geiger mode: $V_{bias} > V_{br}$



http://www.globalspec.com/reference/21446/160210/chapter-14-4-1-avalanche-photodiode

Example: The Trojan Horse attack

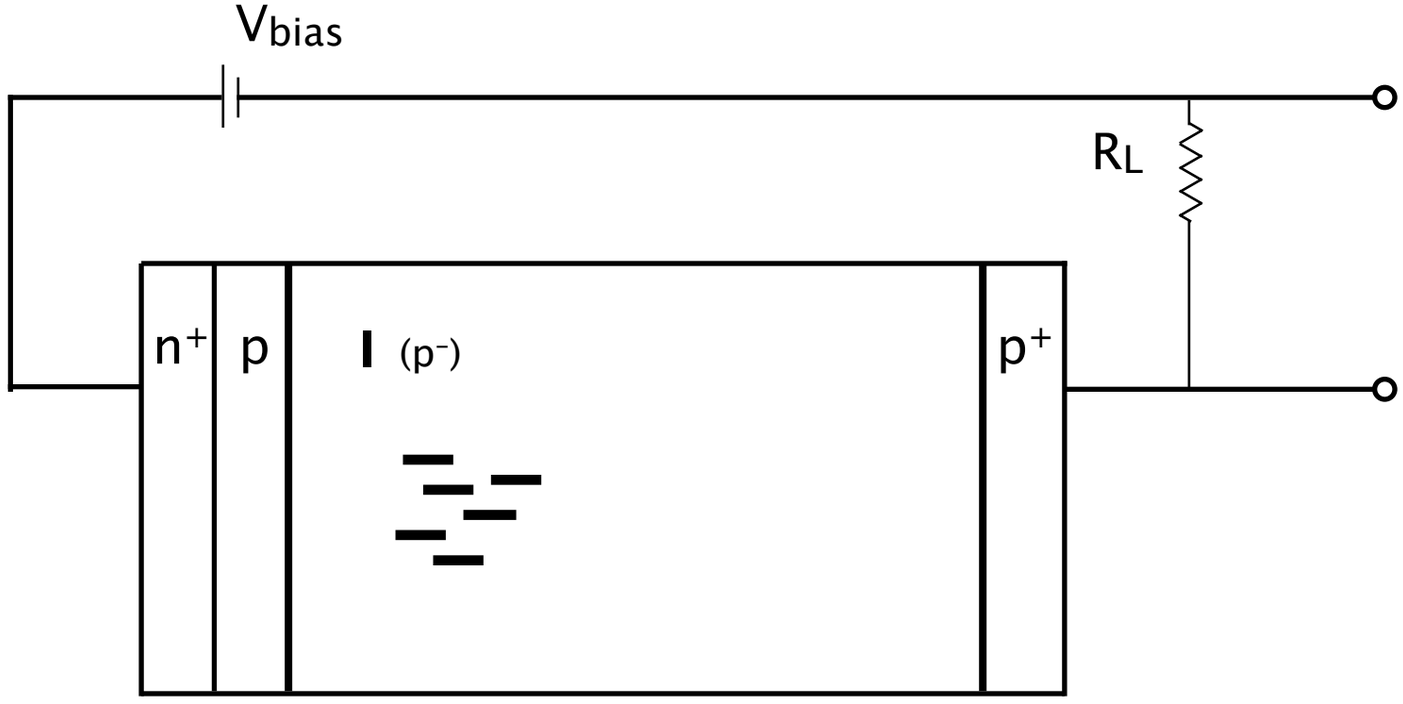
Geiger mode: $V_{bias} > V_{br}$



http://www.globalspec.com/reference/21446/160210/chapter-14-4-1-avalanche-photodiode

Example: The Trojan Horse attack

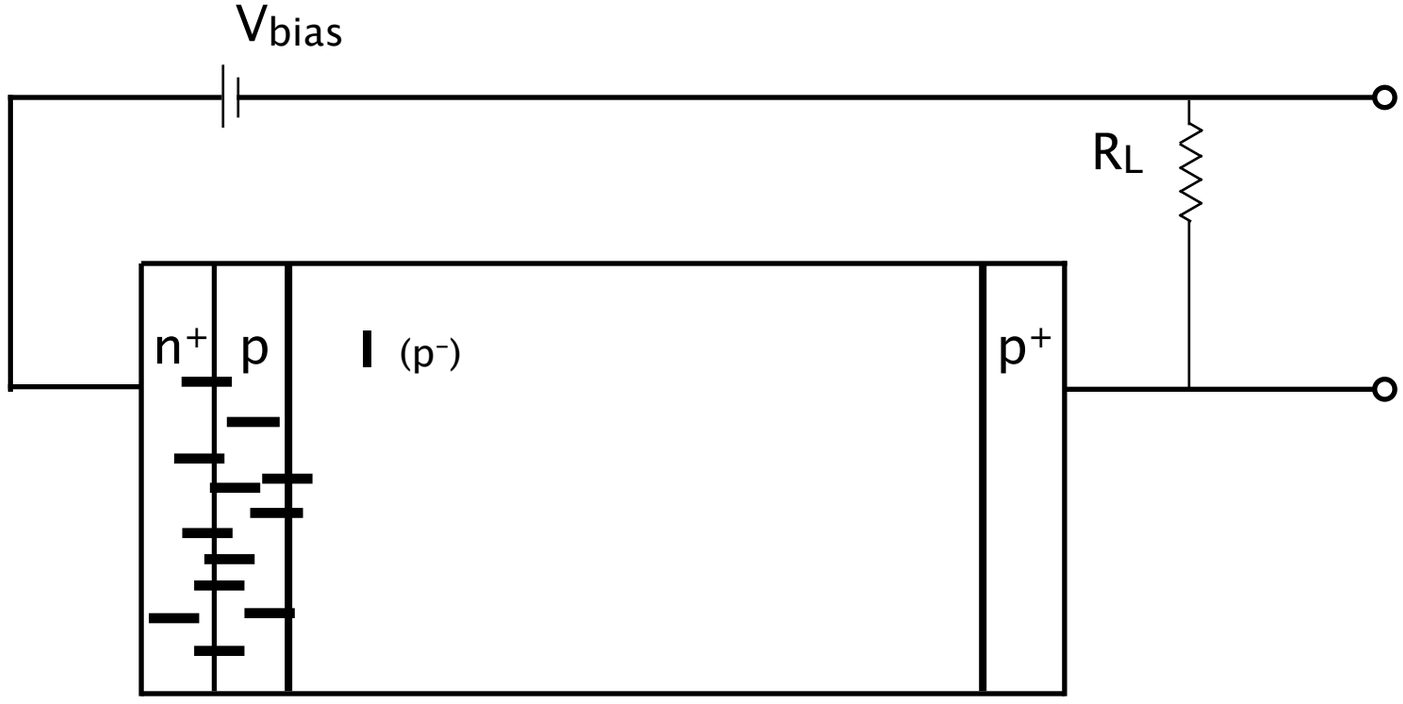
Geiger mode: $V_{bias} > V_{br}$



http://www.globalspec.com/reference/21446/160210/chapter-14-4-1-avalanche-photodiode

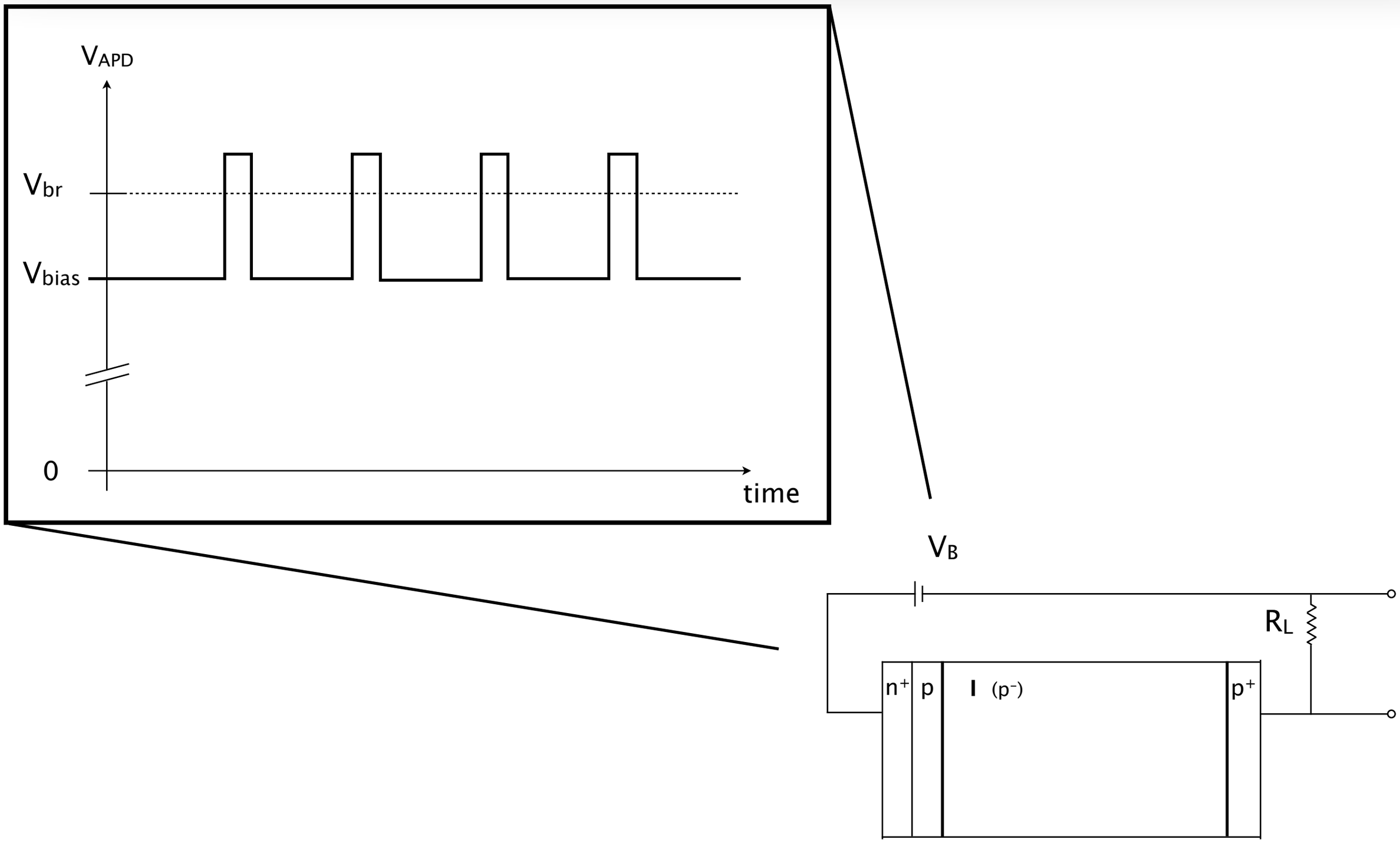
Example: The Trojan Horse attack

Geiger mode: $V_{bias} > V_{br}$



http://www.globalspec.com/reference/21446/160210/chapter-14-4-1-avalanche-photodiode

Example: The Trojan Horse attack



http://arxiv.org/pdf/1008.4593v2.pdf

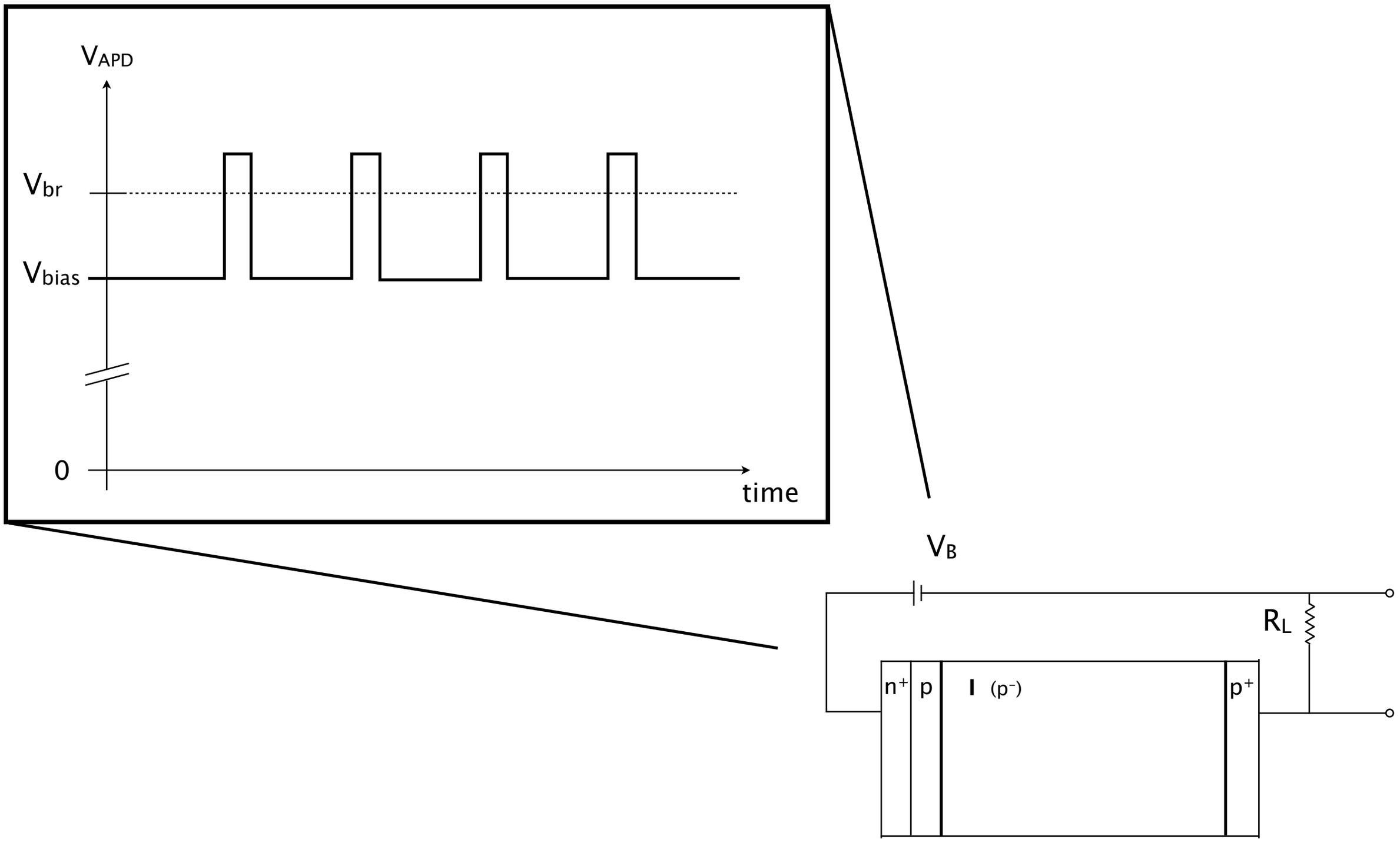
http://www.globalspec.com/reference/21446/160210/chapter-14-4-1-avalanche-photodiode

Example: The Trojan Horse attack

What Eve needs to do:

Get Bob´s APDs into linear mode

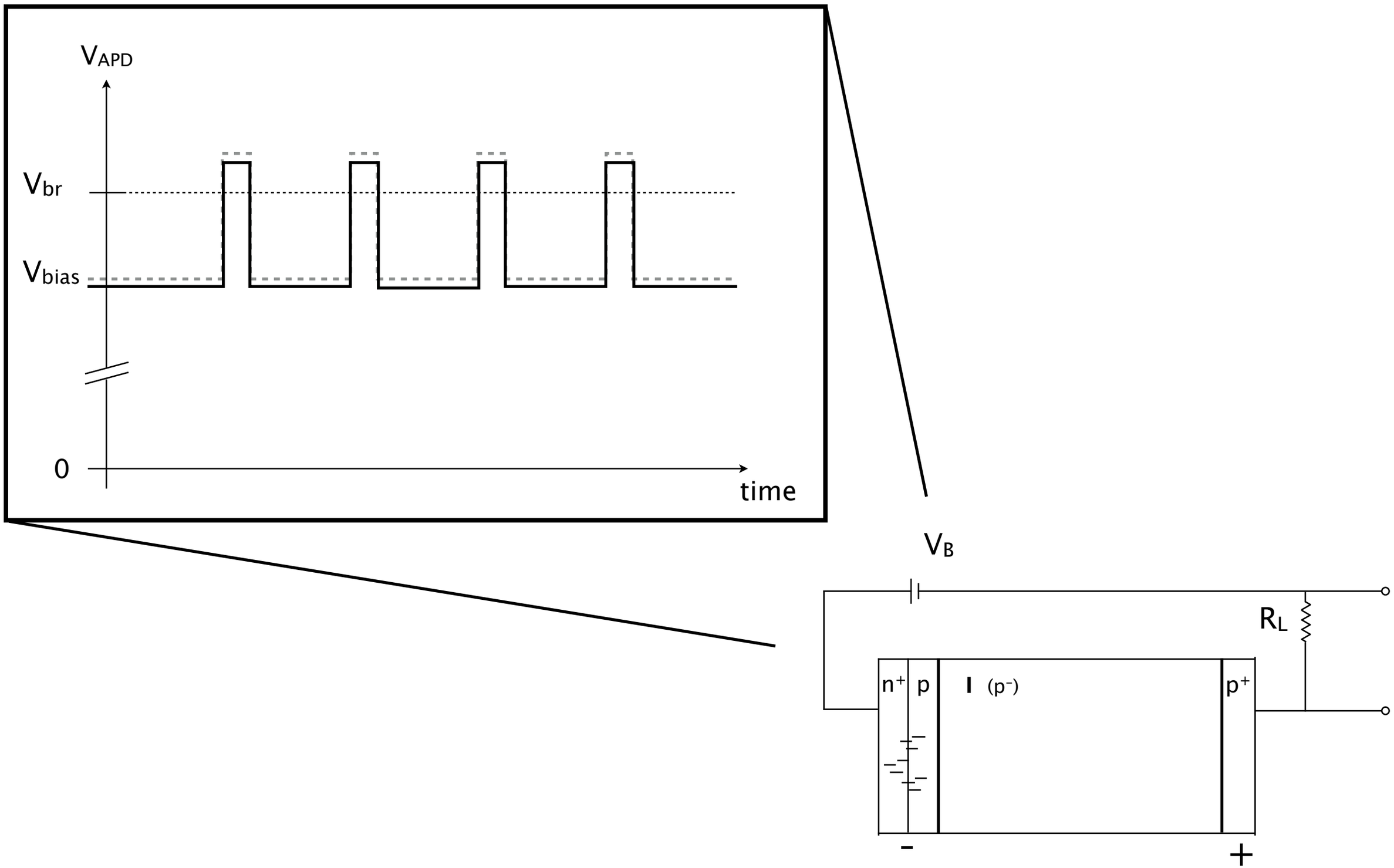
Example: The Trojan Horse attack



http://arxiv.org/pdf/1008.4593v2.pdf

http://www.globalspec.com/reference/21446/160210/chapter-14-4-1-avalanche-photodiode

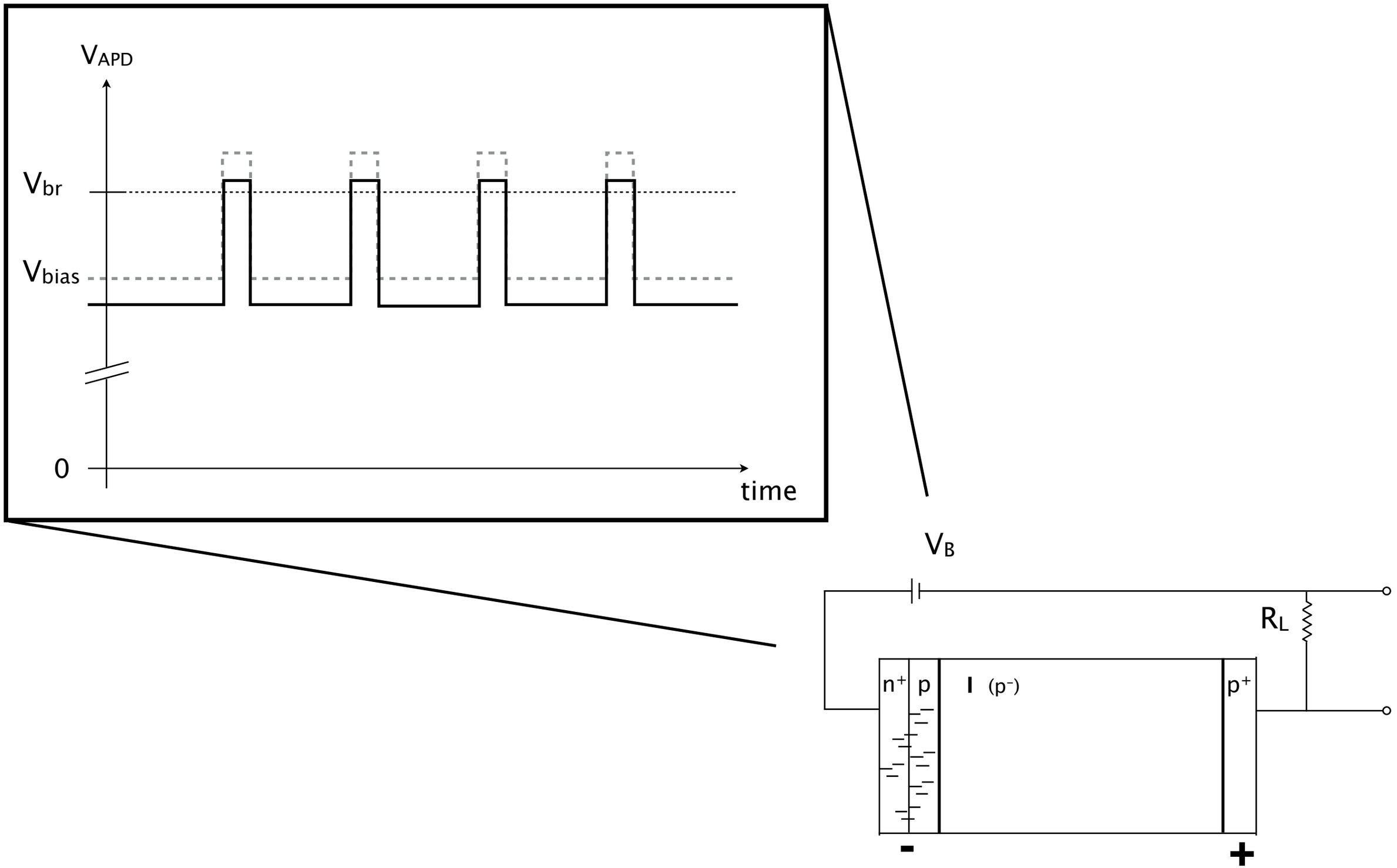
Example: The Trojan Horse attack



http://arxiv.org/pdf/1008.4593v2.pdf

http://www.globalspec.com/reference/21446/160210/chapter-14-4-1-avalanche-photodiode

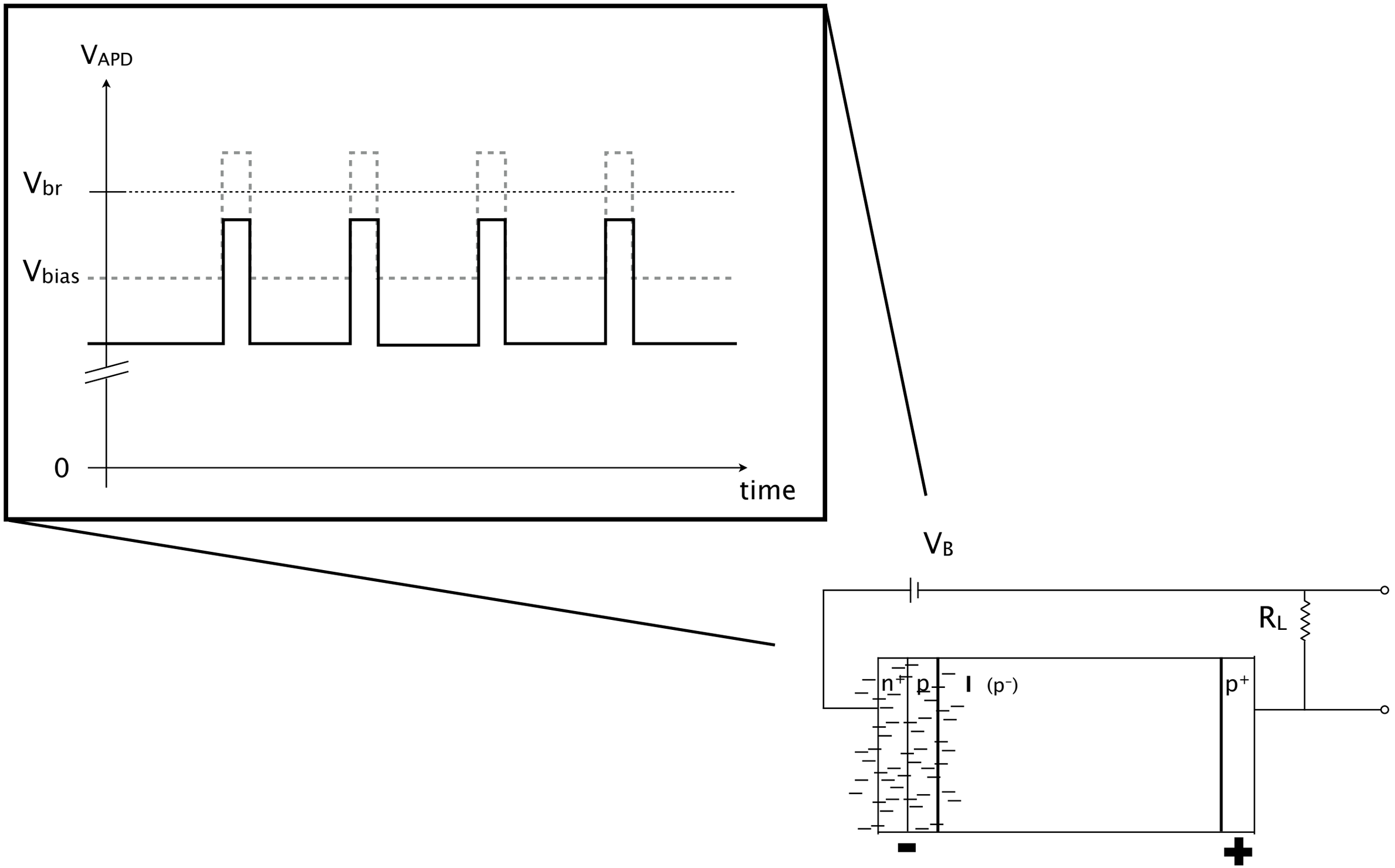
Example: The Trojan Horse attack



http://arxiv.org/pdf/1008.4593v2.pdf

http://www.globalspec.com/reference/21446/160210/chapter-14-4-1-avalanche-photodiode

Example: The Trojan Horse attack

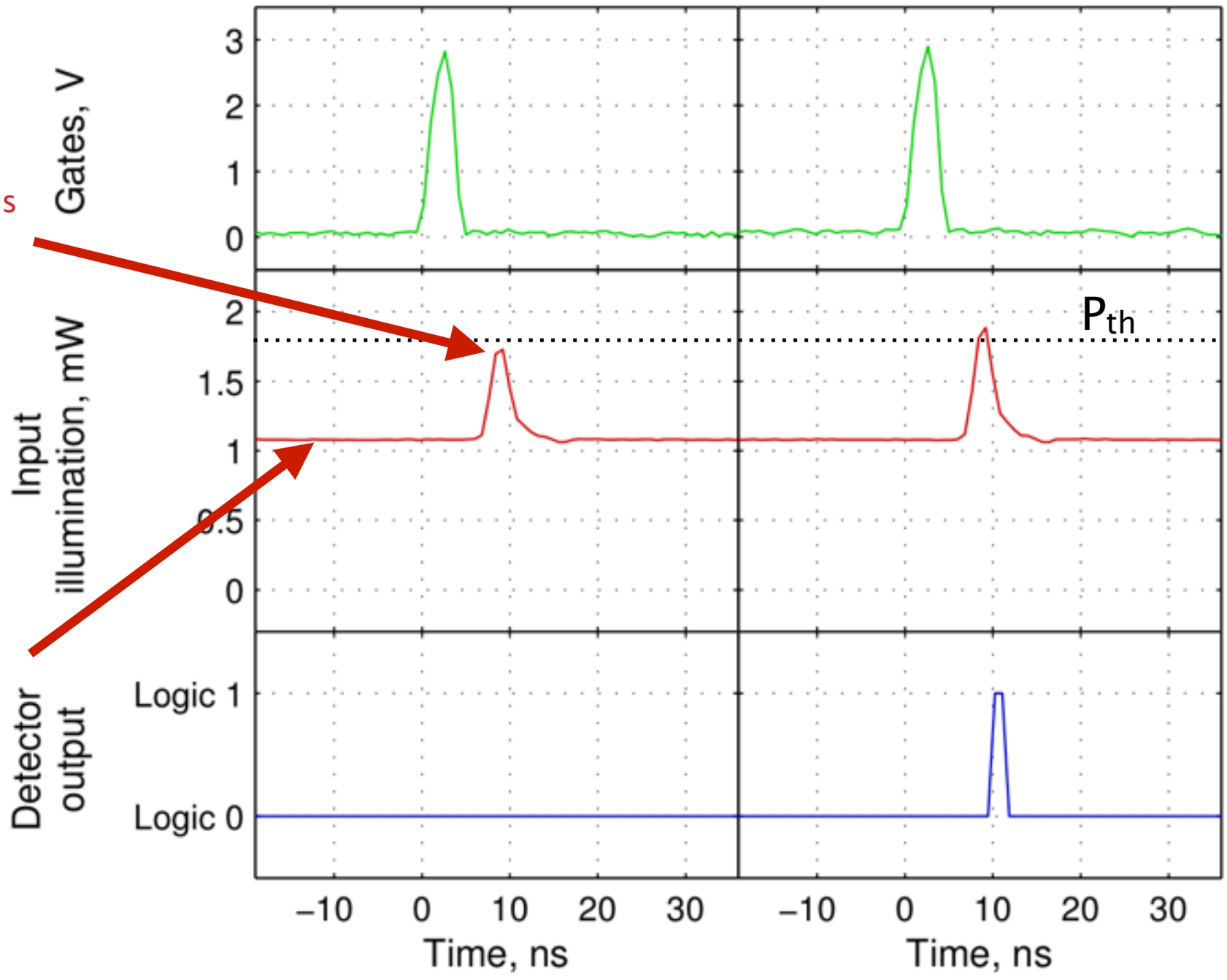


http://arxiv.org/pdf/1008.4593v2.pdf

http://www.globalspec.com/reference/21446/160210/chapter-14-4-1-avalanche-photodiode

Example: The Trojan Horse attack

peek pulse, information is encoded in here



V_{bias}

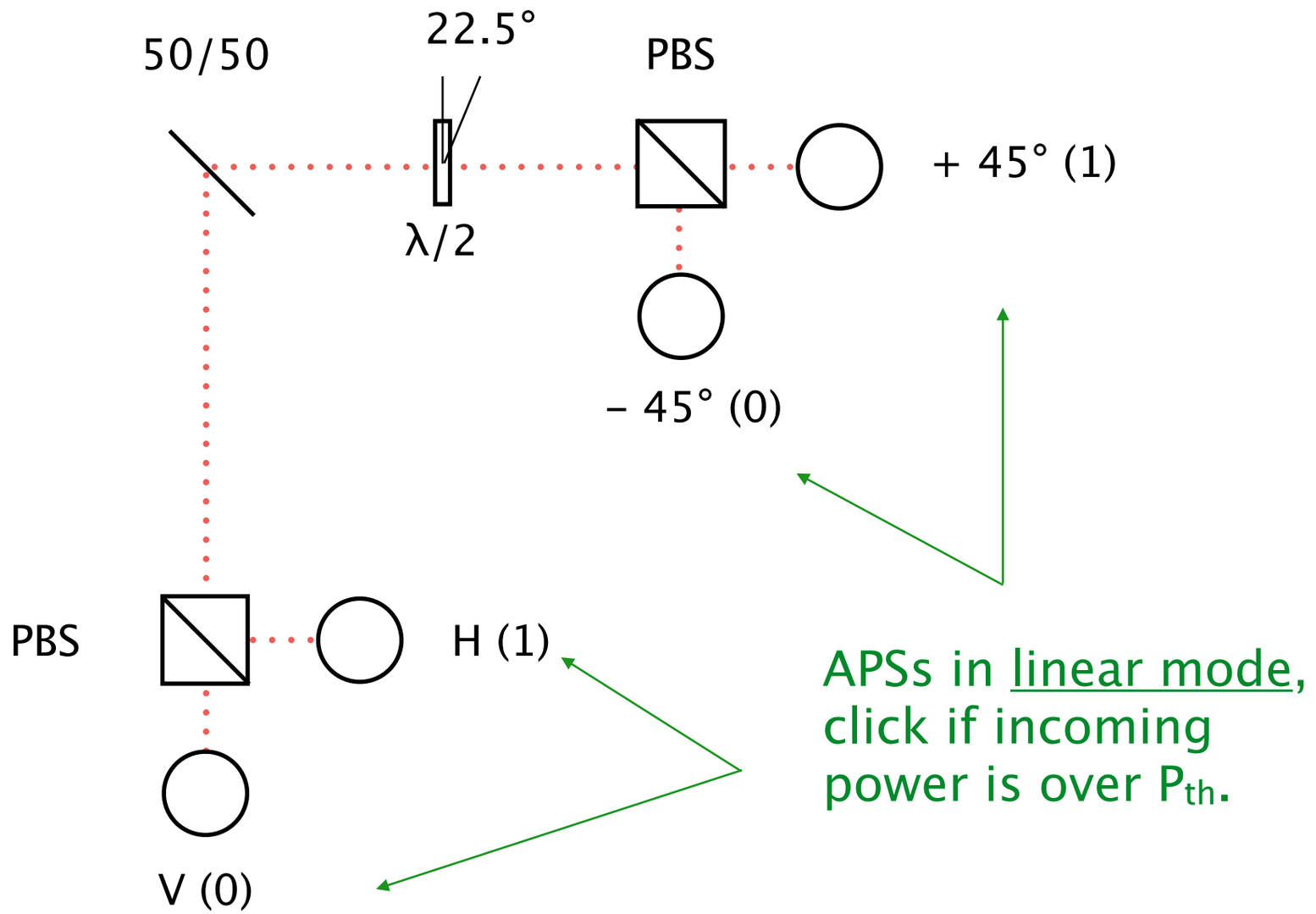
Eves input

Bobs output

constant illumination to keep APD in linear mode

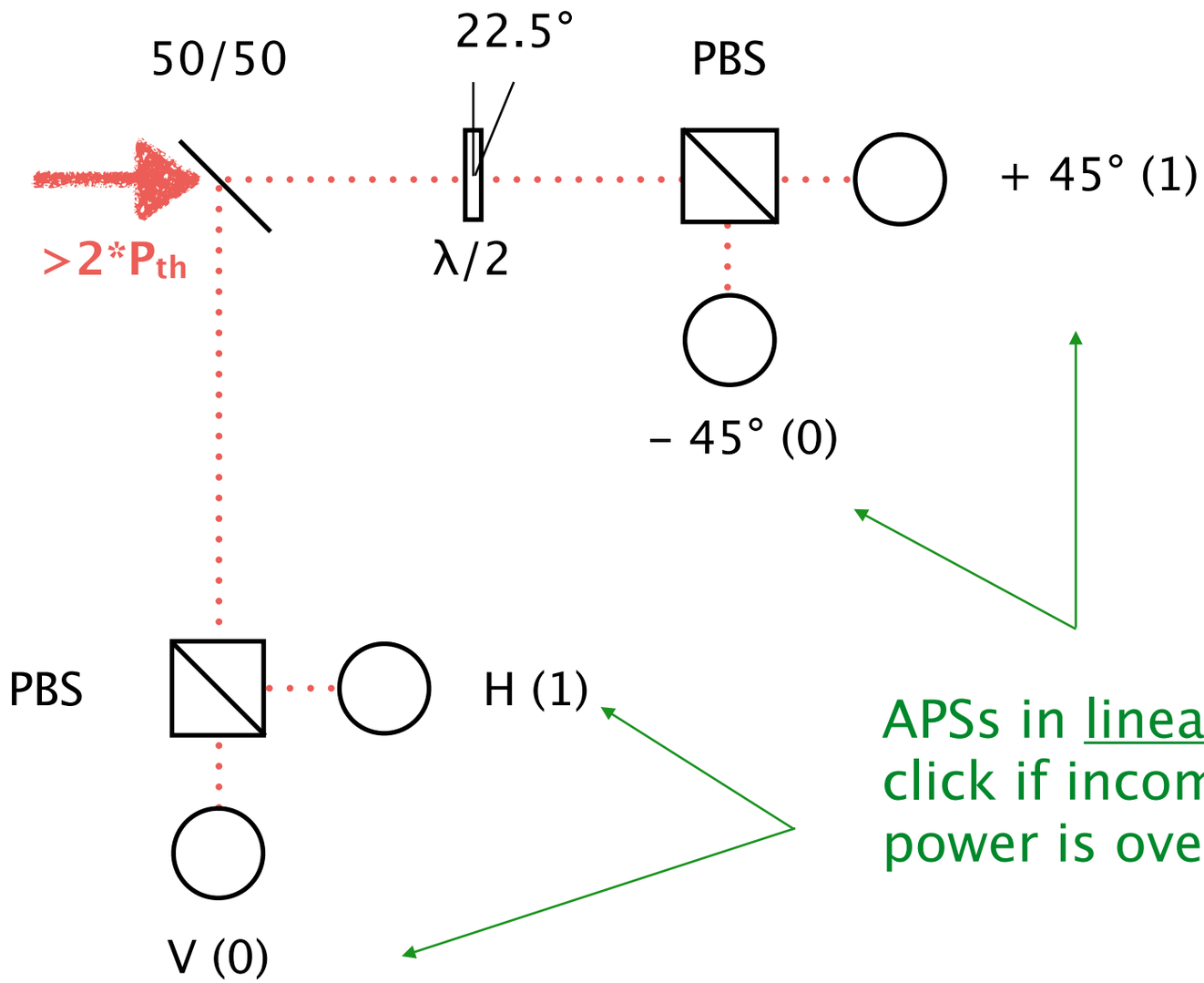
http://arxiv.org/pdf/1008.4593v2.pdf

Example: The Trojan Horse attack



Example: The Trojan Horse attack

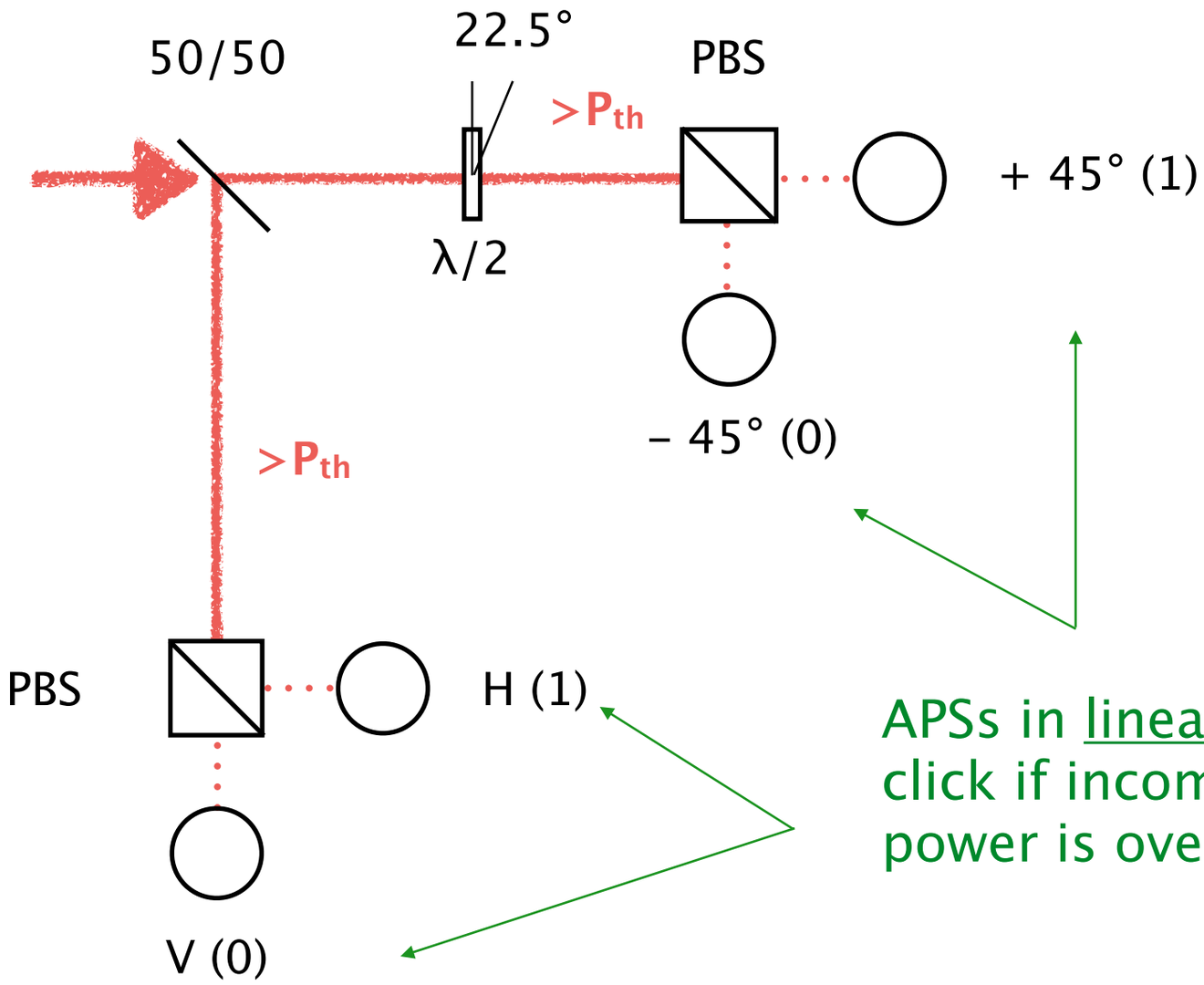
Eve´s bright light pulse, e.g. „V“ in the basis „V/H“



APSs in linear mode, click if incoming power is over P_{th}.

Example: The Trojan Horse attack

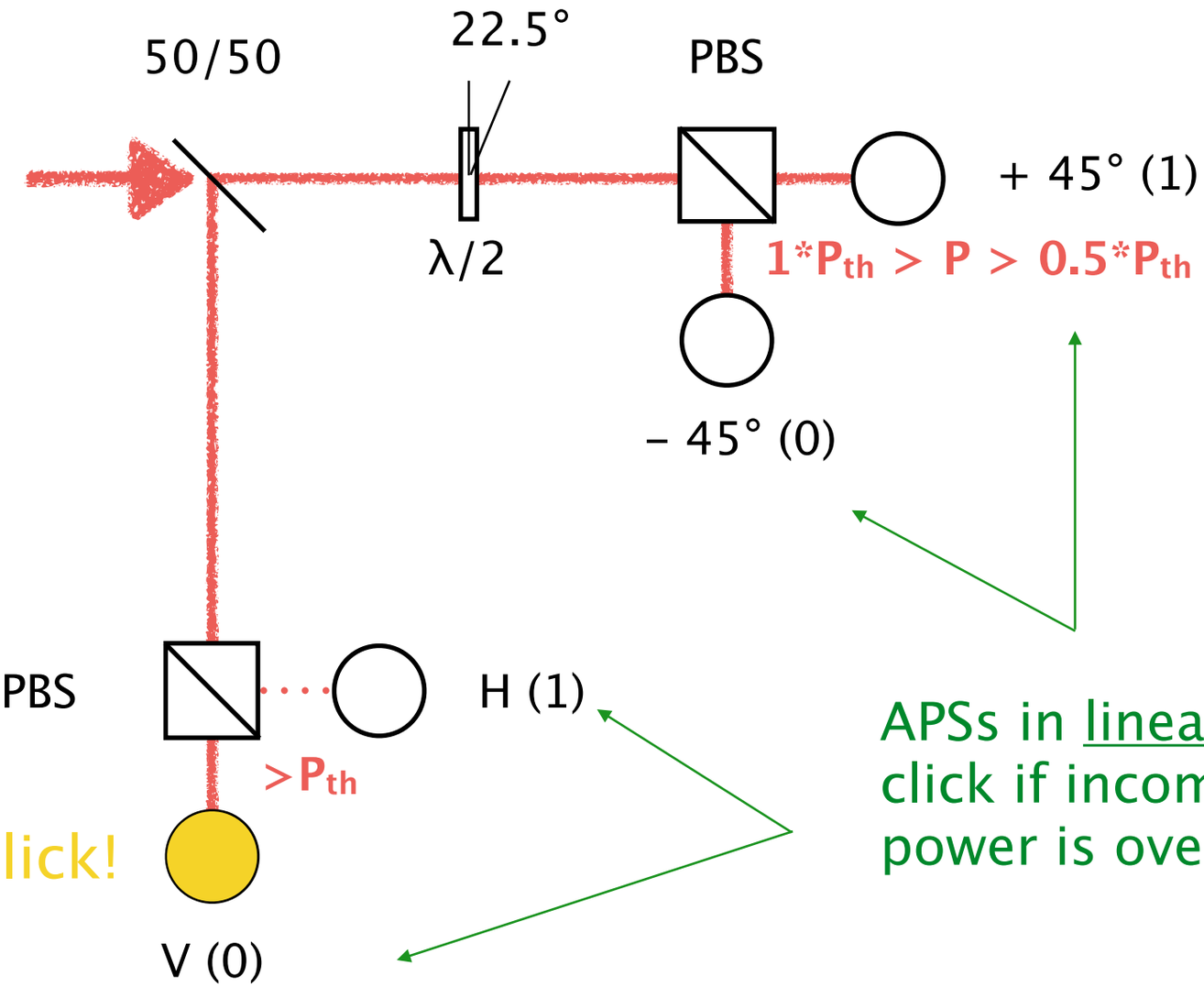
Eve´s bright light pulse, e.g. „V“ in the basis „V/H“



APSs in linear mode, click if incoming power is over P_{th}.

Example: The Trojan Horse attack

Eve´s bright light pulse, e.g. „V“ in the basis „V/H“



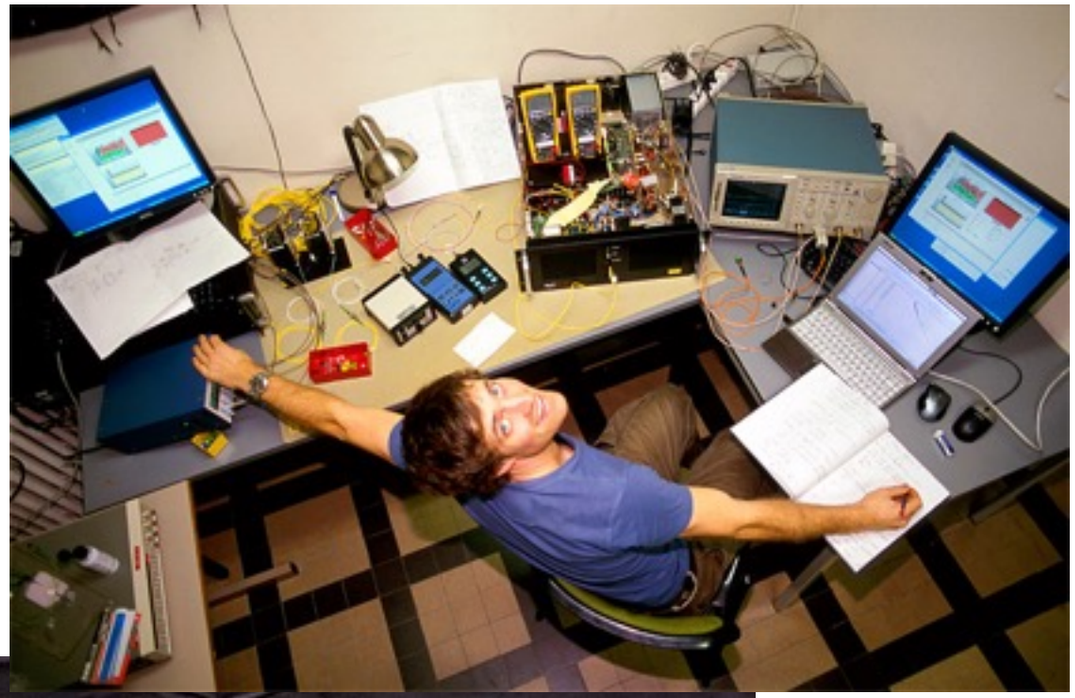
APSs in linear mode, click if incoming power is over P_{th}.

Conclusion

- QKD can be hacked in practice
- There is no prove, excluding any loophole
- The battle between encrypter and hacker still goes on

Questions?

Questions?



http://www.vad1.com/lab/hacking-commercial-quantum-cryptography-2010/