

# Quantum spooks

---

# Cryptography

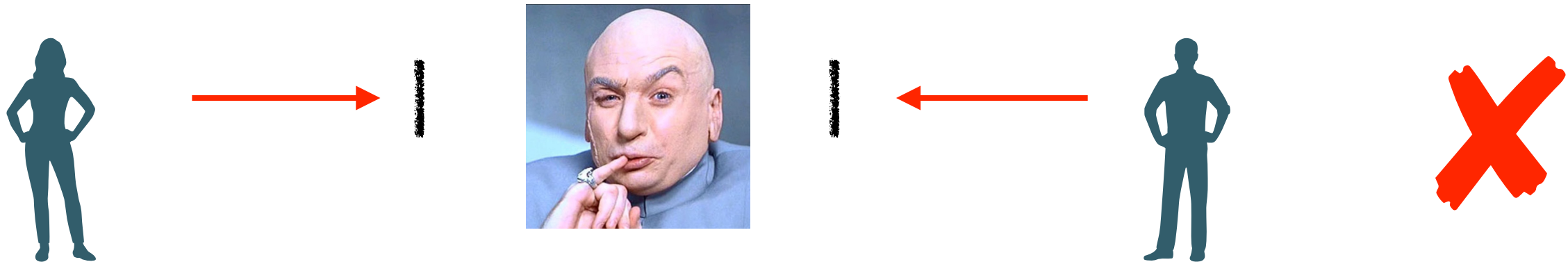
---

- “Lets have lunch at one”
- Simple encryption
  - “ohwv kdyh oxfk dw rqh”
- Cryptography:
  - encrypt message ➡ send ➡ decrypt message

# What is cryptography ***not*** useful for?

---

Messages blocked

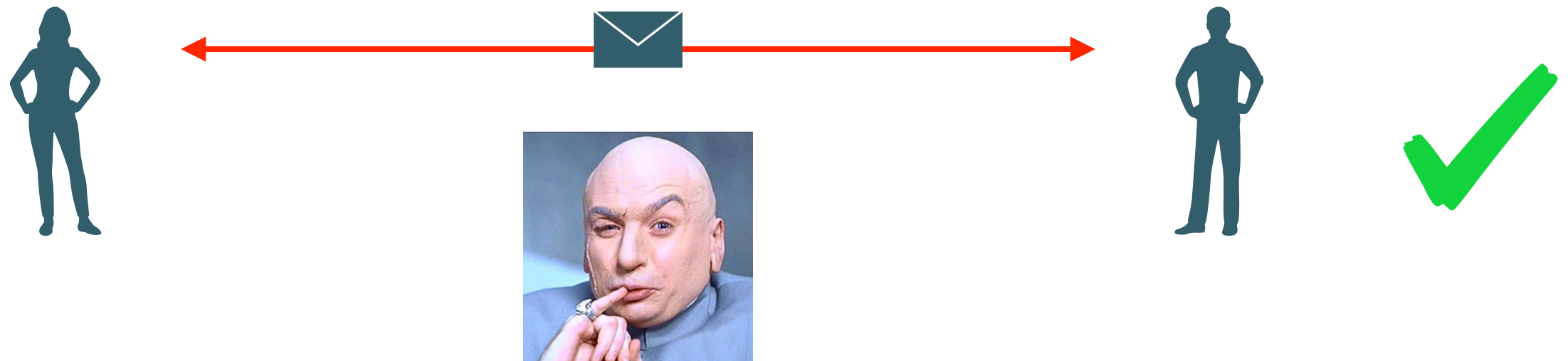


Messages never intercepted



# What is cryptography useful for?

---



- Sending a message that even if intercepted (copied) cannot be understood (read)

# Cryptography

---

- ***Huge*** industry, everything from iMessage to Amazon purchases to banking
- Almost every online communication is now encrypted

encrypt message ➡ send ➡ decrypt message

# Cryptography classes

---

A) Encrypted by some cypher or key

- Always breakable given enough computation
- (quantum computers will be very good at some common cyphers)



B) Encrypted by a random number as long as the message  
(one time pad)

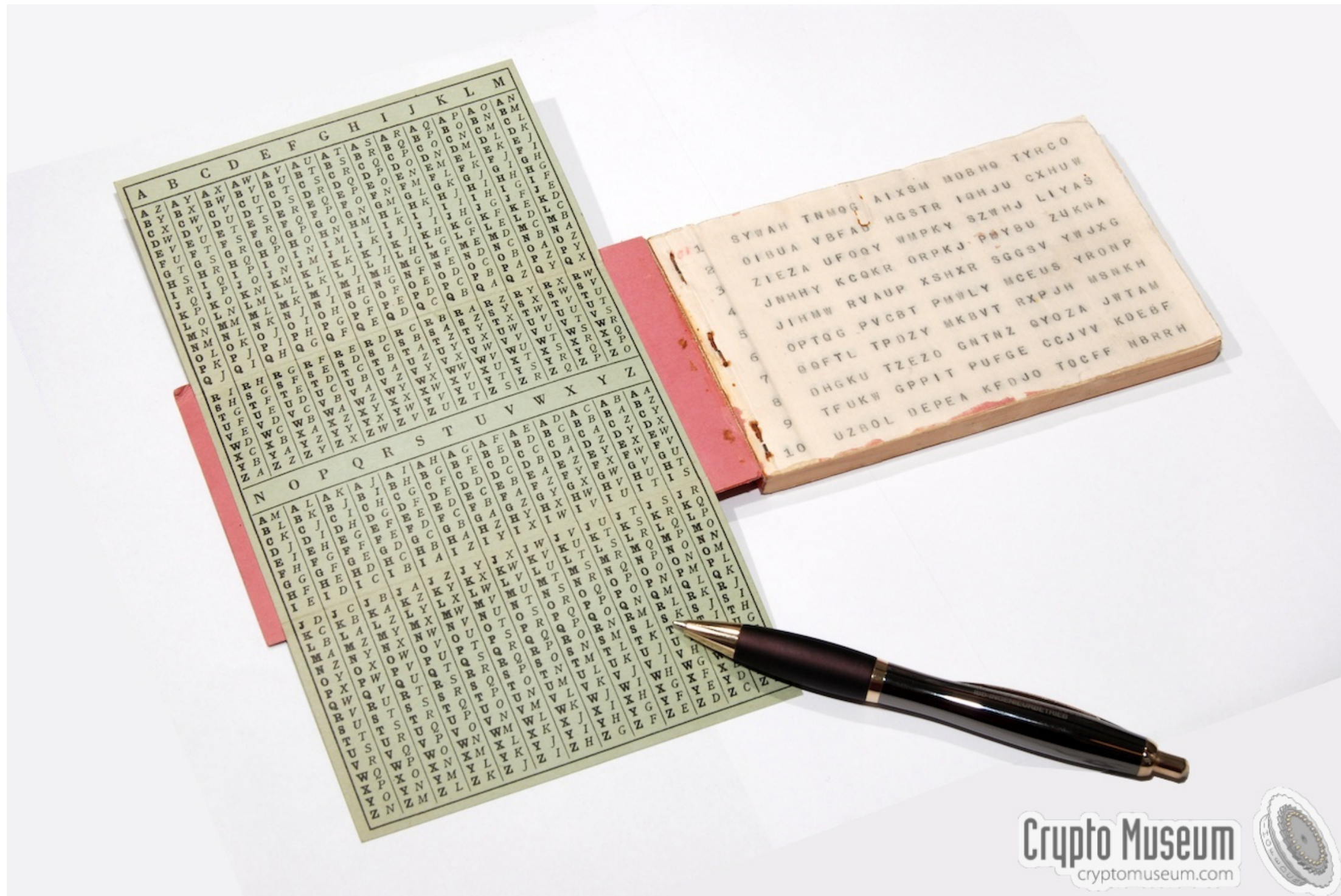
- Unbreakable\*

# One time pad

---

- “Lets have lunch at one”
- Random number (key) as long as the message
  - 152009215330282426582
- mjvs qcwjcouppebevftwg
- Unbreakable unless VBM has a copy of the key

# One time pad





# One time pad

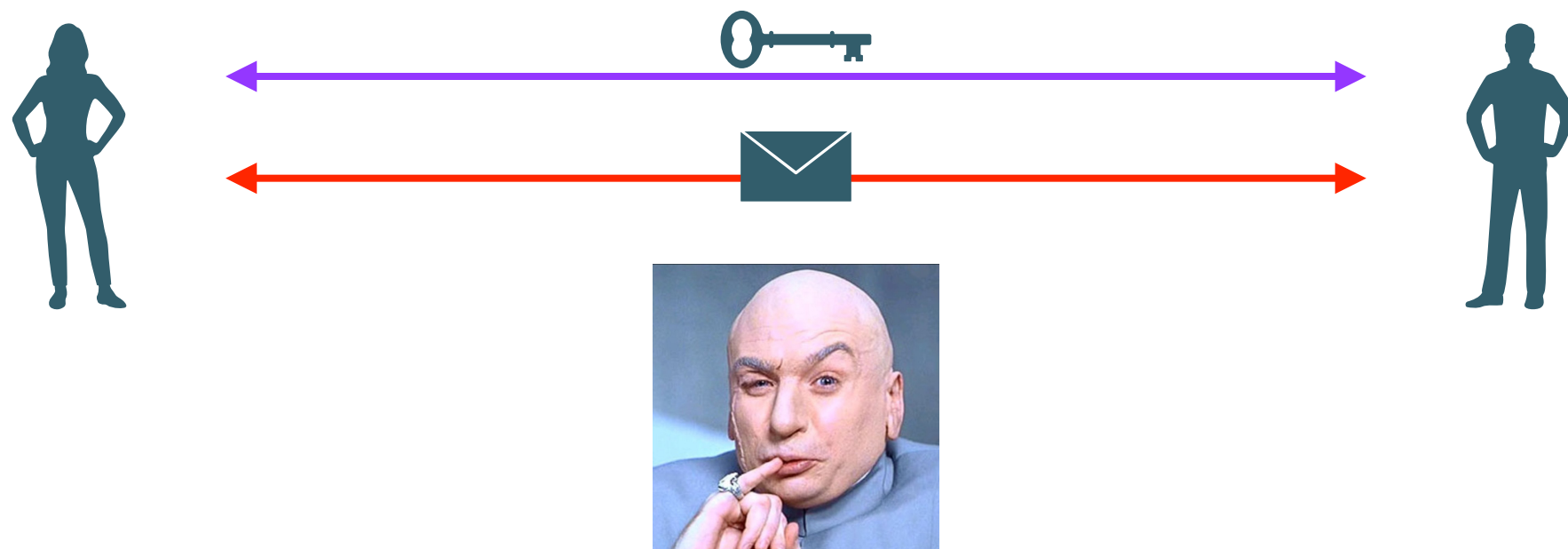
---



- Breakable only if the key is intercepted and copied

# Modern cryptography

---

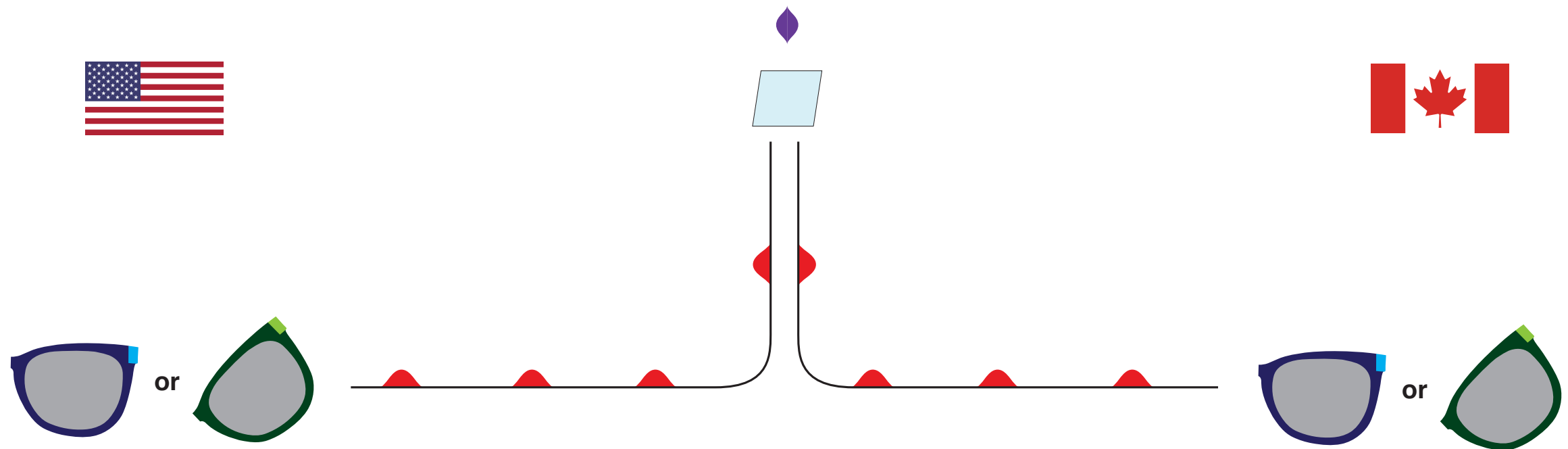


- Use one time pad for messages (long random key, unbreakable)
- Protect key from being copied

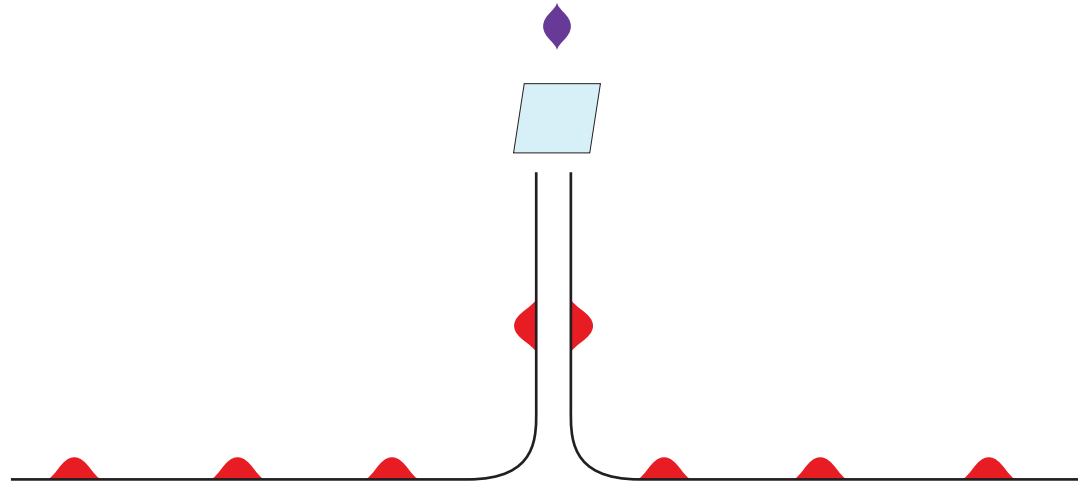
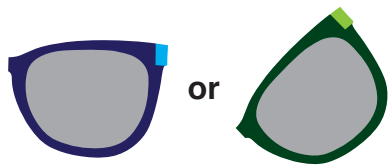
Quantum cryptography

# Twinned photons

---



- It is possible to split one photon into two ‘twins’
- Twin photons have the same polarization



		→														
	0	1	0	0	1	1	0	0	0	0	1	0	1	1	0	0
		→														
	0	1	0	0	1	1	0	0	0	0	1	0	1	1	0	0





Same random  
(deterministic)

		→														
	0	0	0	1	0	0	1	0	1	1	0	1	0	0	1	1
		→														
	1	0	0	1	1	0	0	1	0	1	1	1	0	0	0	1





Different  
random

# Terms of entanglement

- Twin knows what happens *instantly*
- So weird
- Fundamental feature of how our world works

		→														
	0	1	0	0	1	1	0	0	0	0	1	0	1	1	0	0
		→														
	0	1	0	0	1	1	0	0	0	0	1	0	1	1	0	0





Same random  
(deterministic)

		→														
	0	0	0	1	0	0	1	0	1	1	0	1	0	0	1	1
		→														
	1	0	0	1	1	0	0	1	0	1	1	1	0	0	0	1

Different  
random

# Looks like a key

---

		→														
	0	1	0	0	1	1	0	0	0	0	1	0	1	1	0	0
		→														
	0	1	0	0	1	1	0	0	0	0	1	0	1	1	0	0

Same random  
(deterministic)

- But VBM could intercept the key


# Protecting against the VBM

																
	1	0	0	0	0	1	1	1	0	1	0	0	0	1	0	1
																
	0	1	0	0	0	1	1	1	1	1	0	1	0	1	0	0

- Send twinned photons
- Randomly choose set (blue vs. green frames)
- Later publicly say which frame you used for each photon (but not what you saw)
  - Only keep photons where you happened to pick glasses from the same set



# Protecting against the VBM

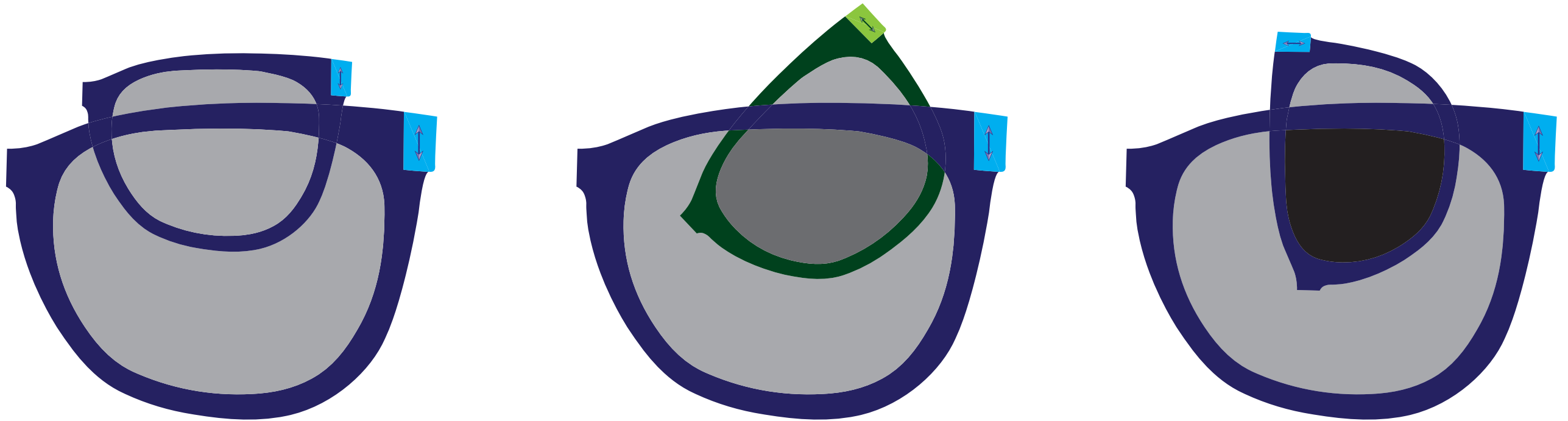
																
	1	0	0	0	0	1	1	1	0	1	0	0	0	1	0	1
																
	0	1	0	0	0	1	1	1	1	1	0	1	0	1	0	0

- Lastly, share a small part of the key
- If VBM cut fiber, he had to guess which set you would use.
  - VBM guesses wrong 1/2 the time, when he does friends see different answers 1/2 the time (becomes random)
- Can tell if the key was intercepted



# Sunglasses

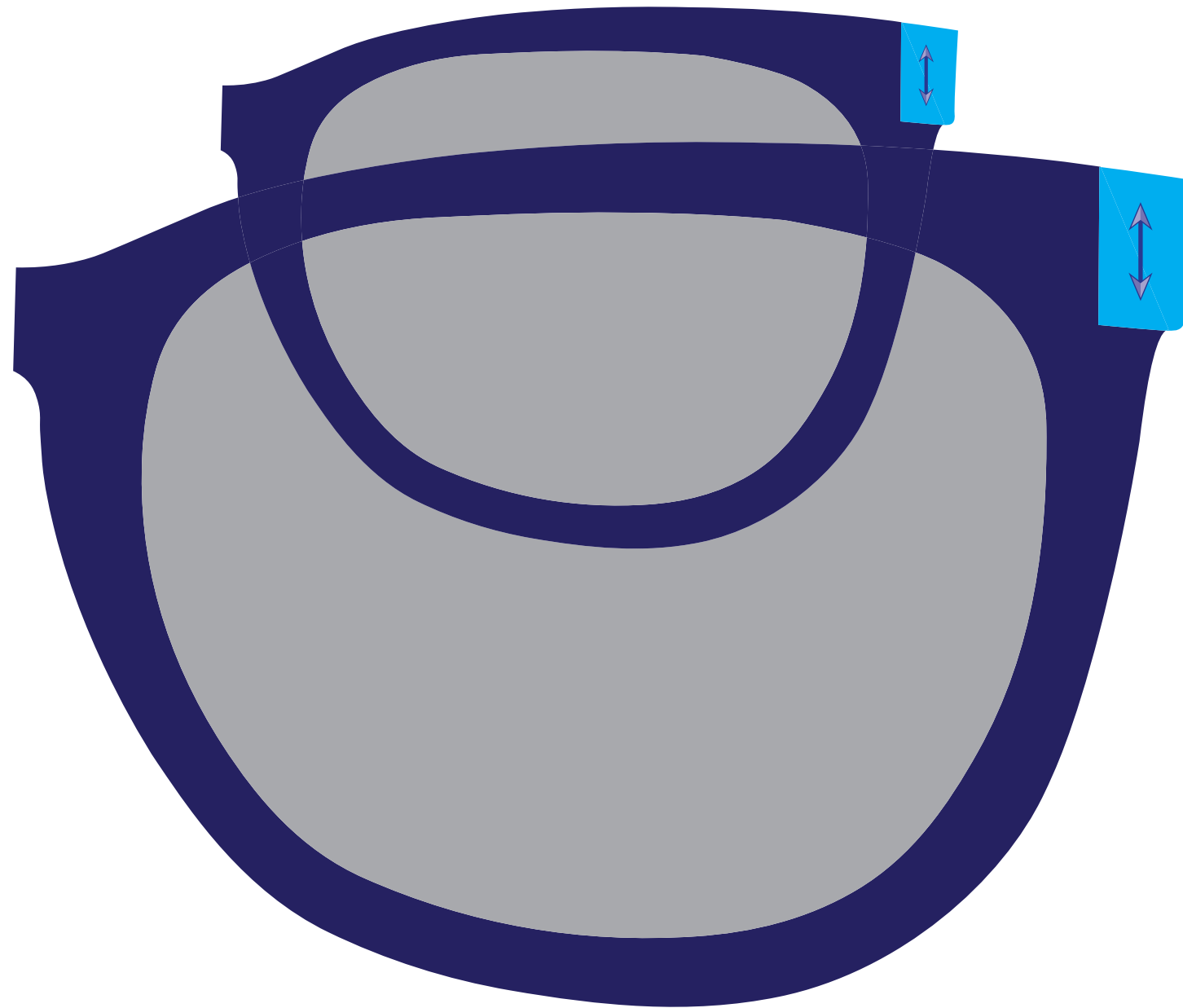
---



# Two glasses

---

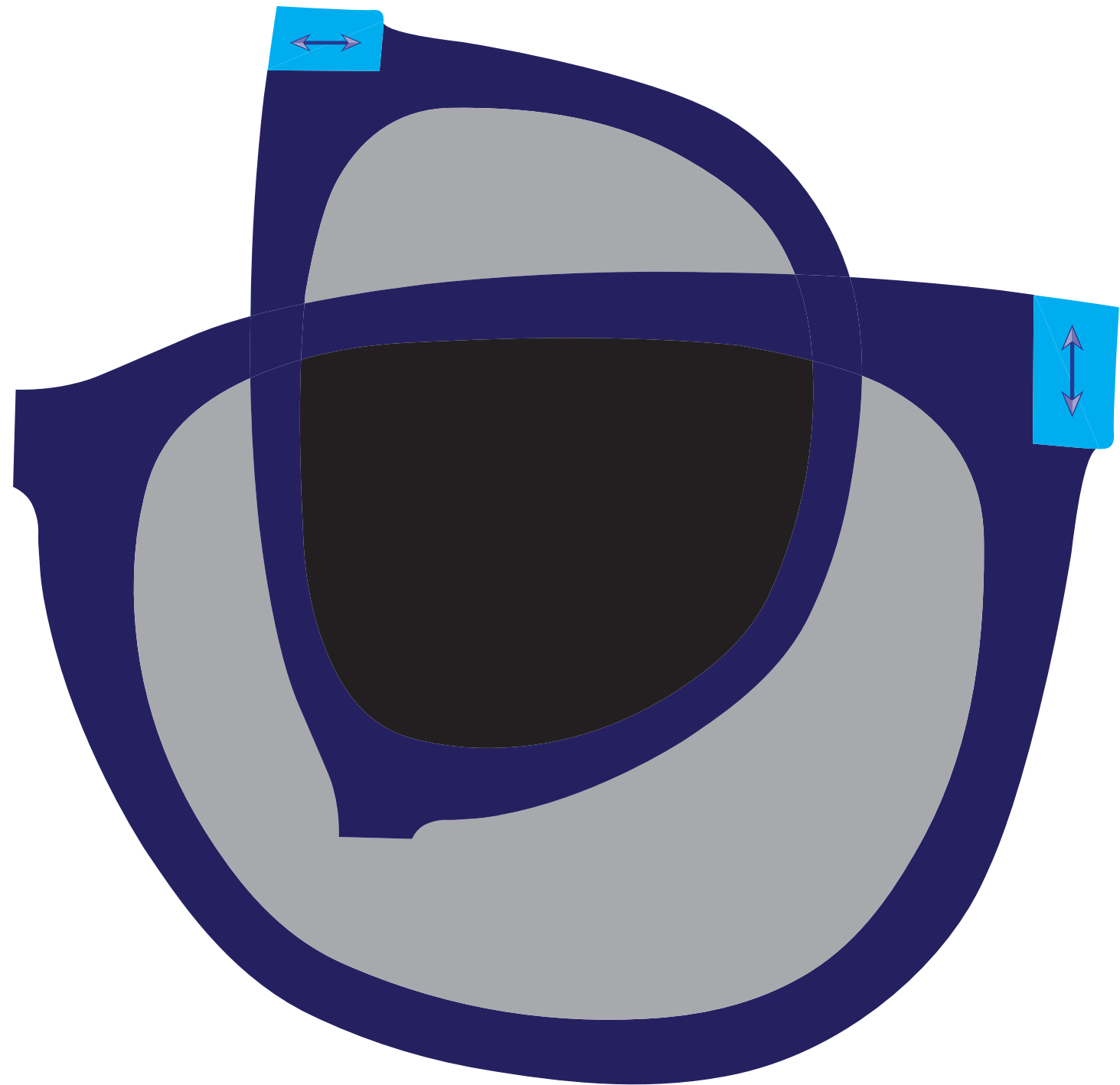
- Half of the unpolarized light (background) makes it through the rearmost glasses. Only vertically polarized light makes it through.
- Since forward glasses only let vertical polarization through, all the light that got through the first pair make it through the second.



# Two glasses

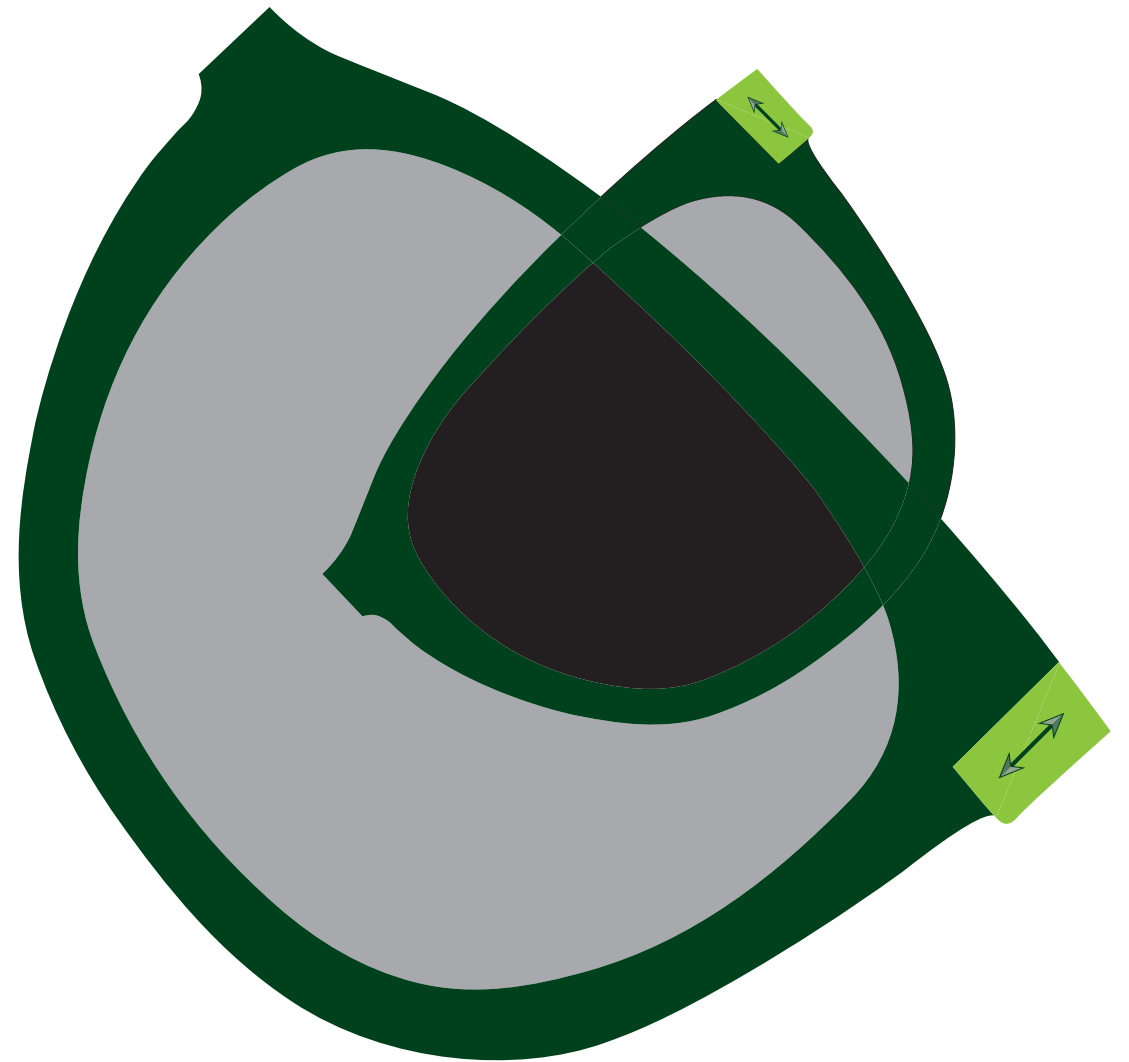
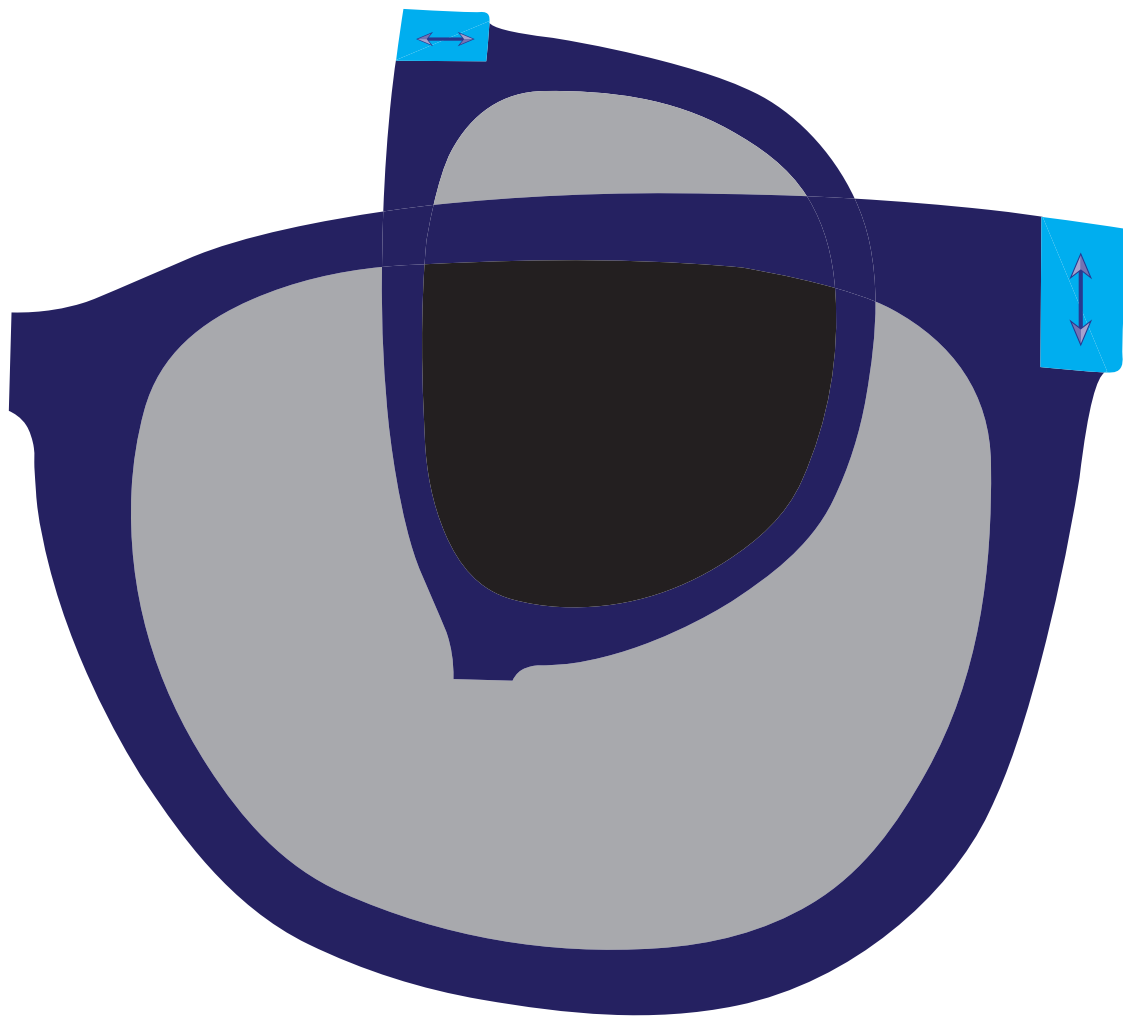
---

- Half of the unpolarized light (background) makes it through the rearmost glasses. Only horizontally polarized light makes it through.
- Since forward glasses only let vertical polarization through, all the light that got through the first pair is blocked by the second pair.



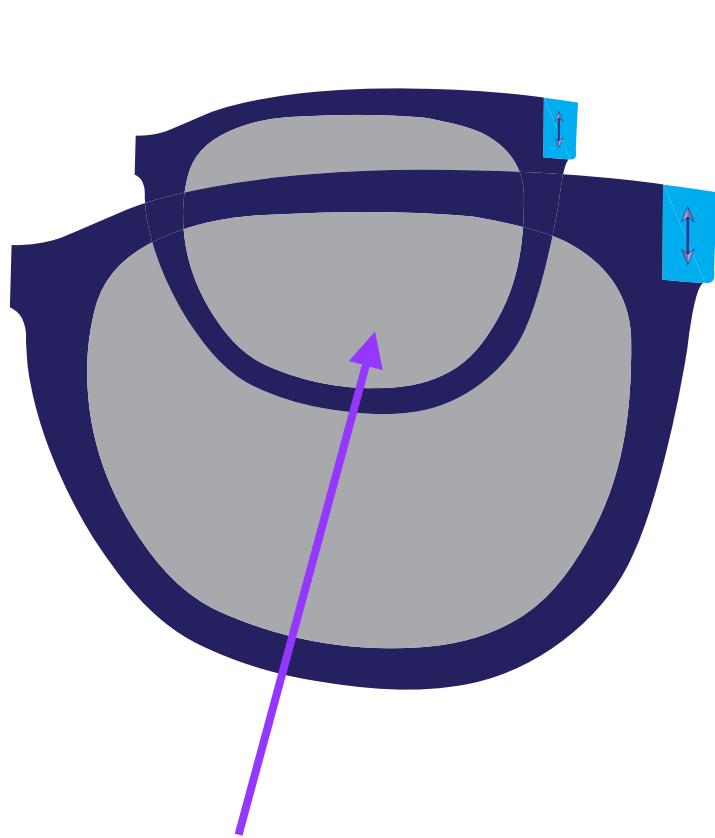
# Only relative orientation matters

---

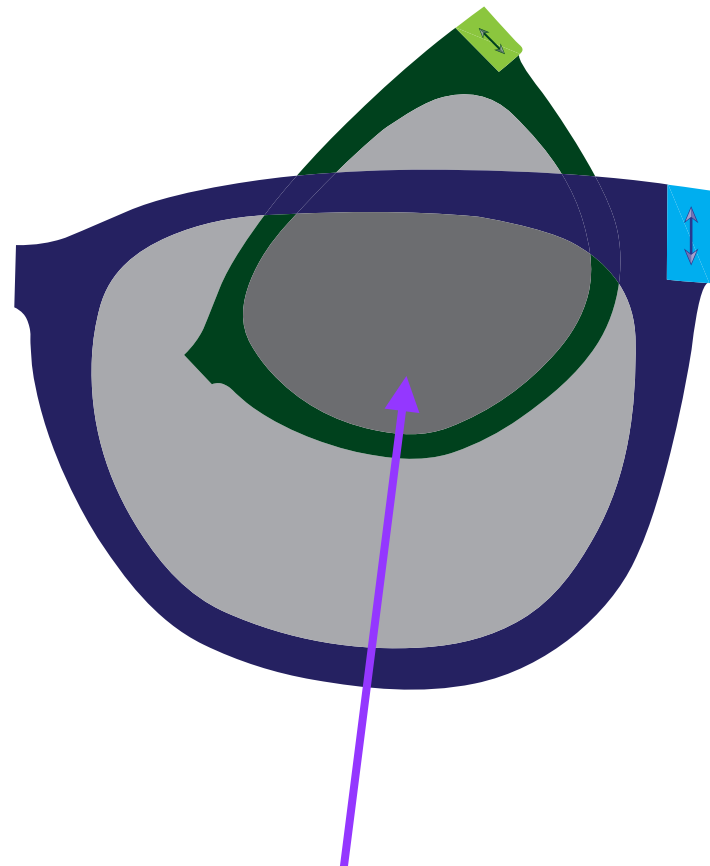


# Mixing sets

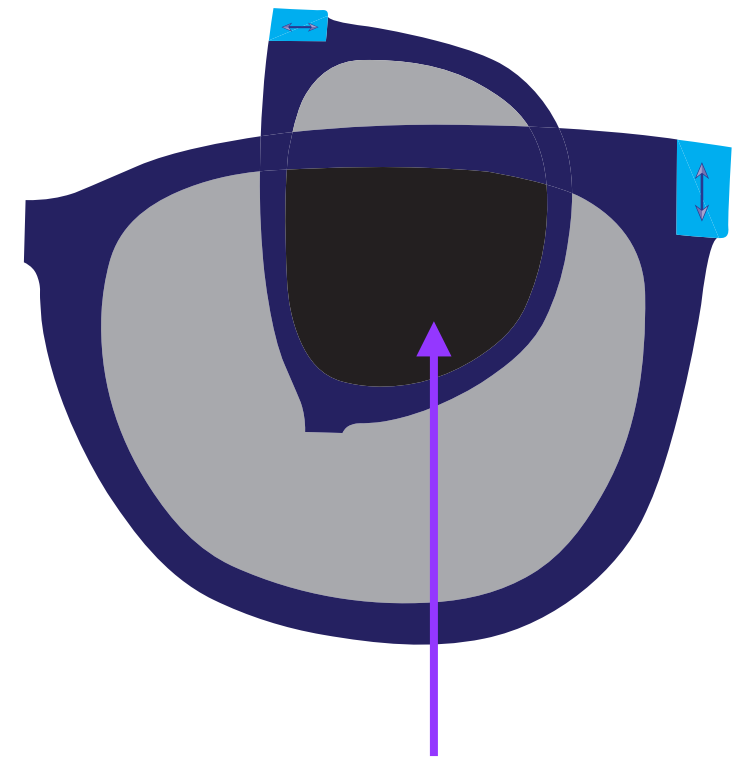
---



$$1/2 * \text{all} = 1/2$$



$$1/2 * 1/2 = 1/4$$

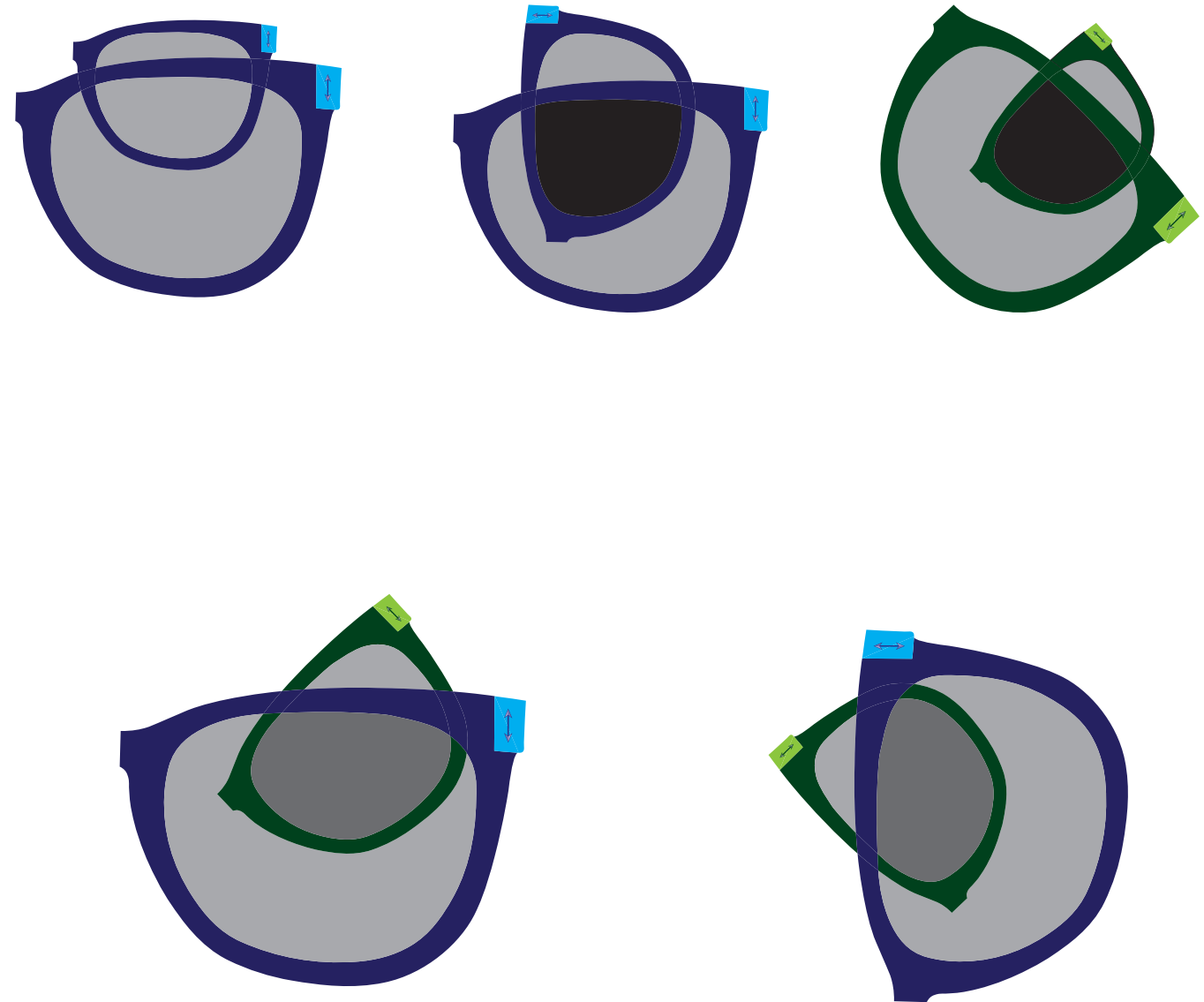


$$1/2 * \text{none} = 0$$

# Mixing sets

---

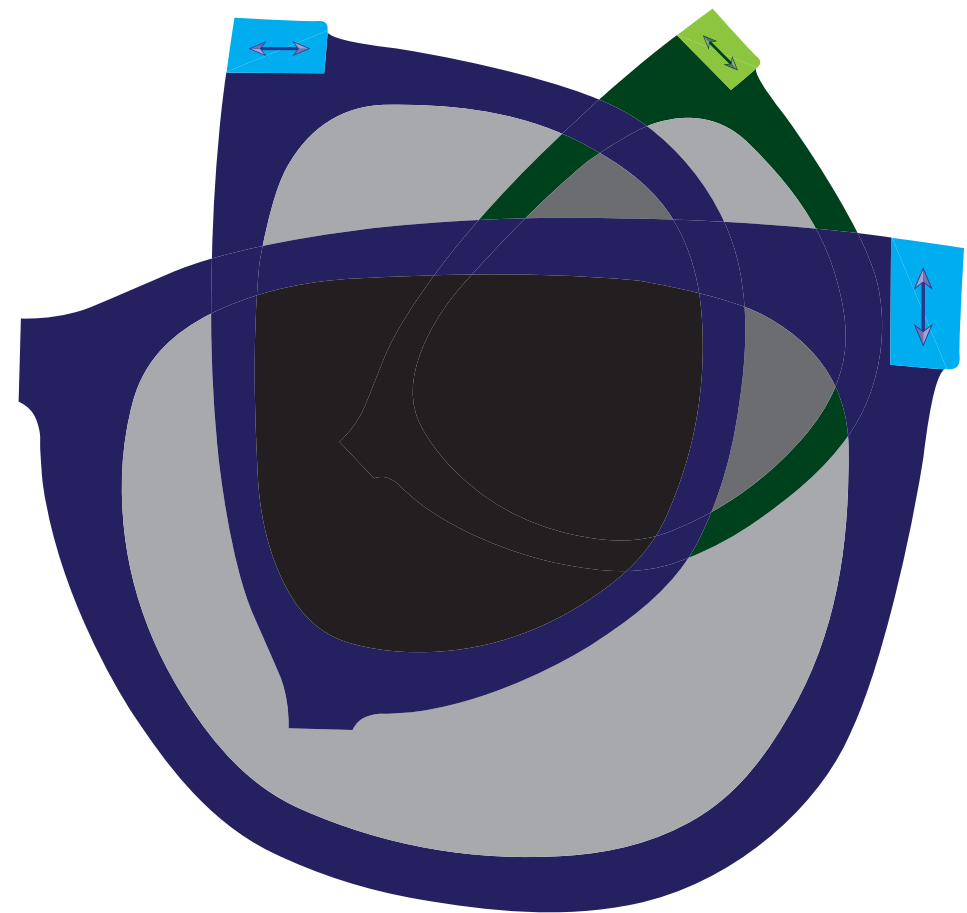
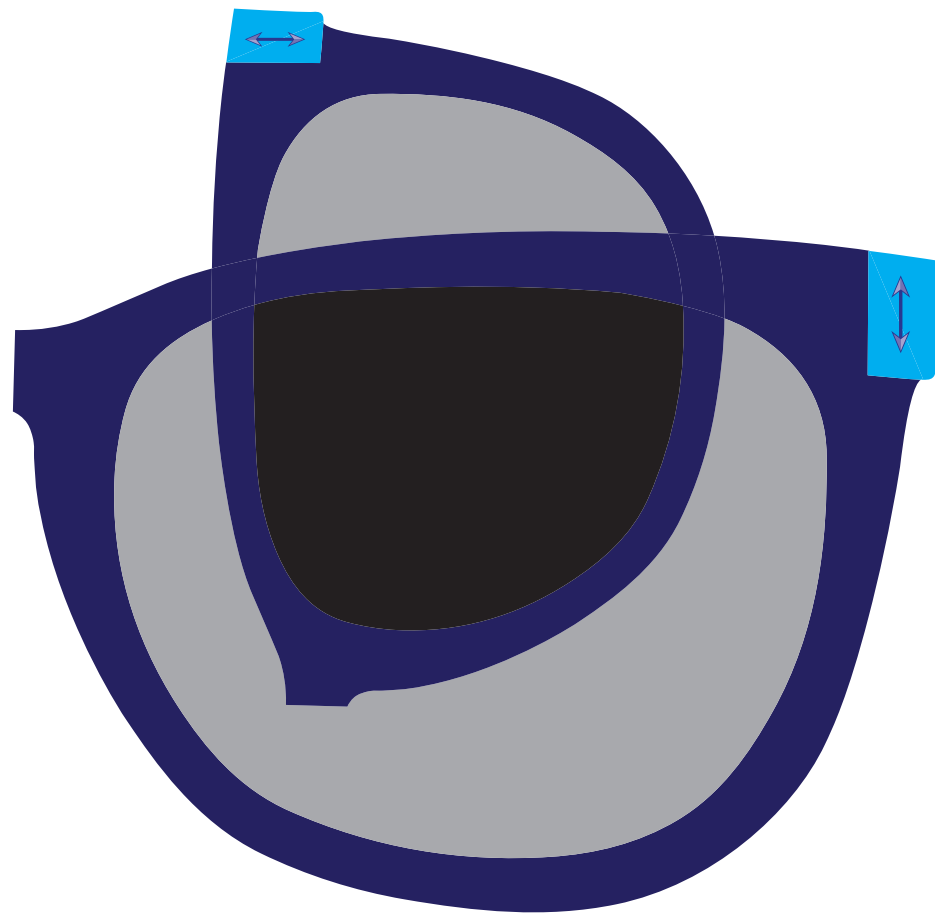
- Two glasses of the same 'set' (frame color) gives either all of light through the first or none.
- Two glasses from different sets always gives  $1/2$  of light through the first pair.





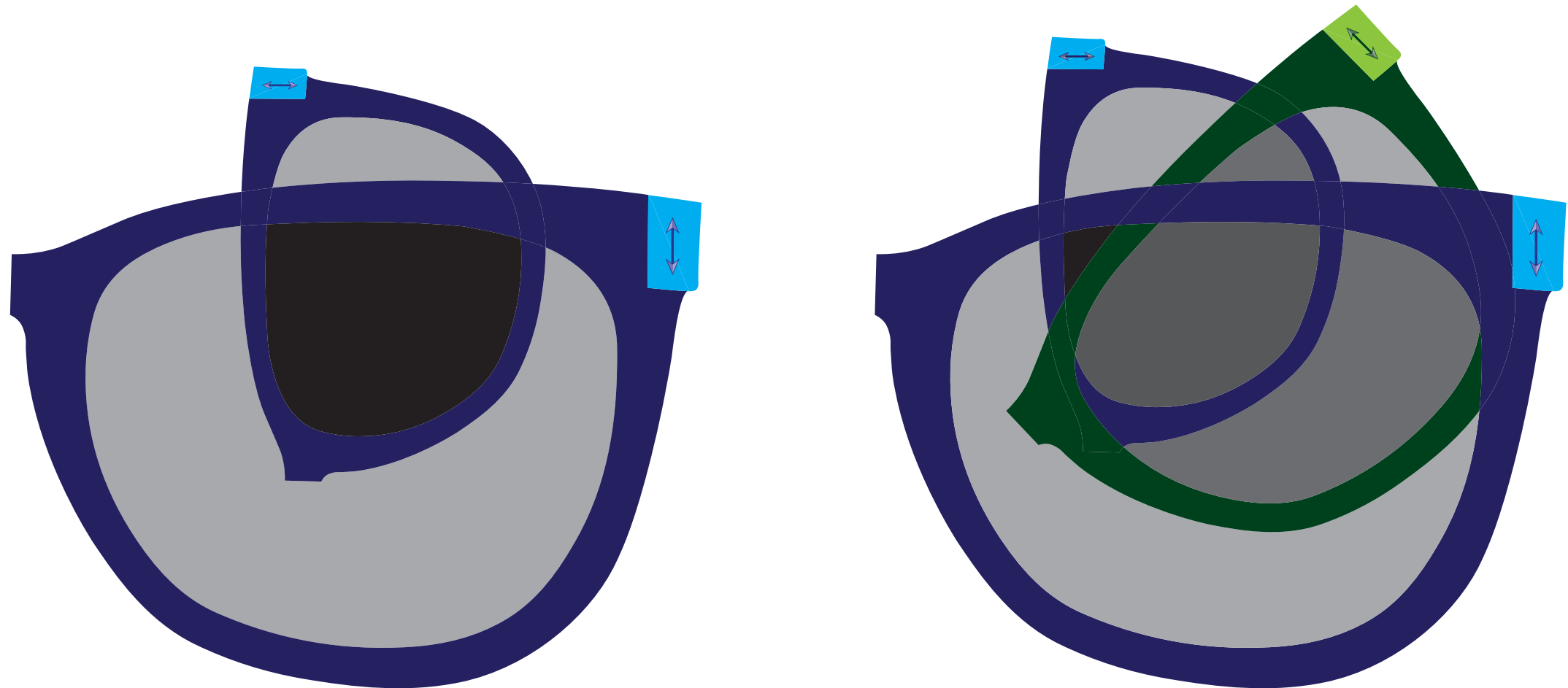
# Adding a third pair of glasses

---



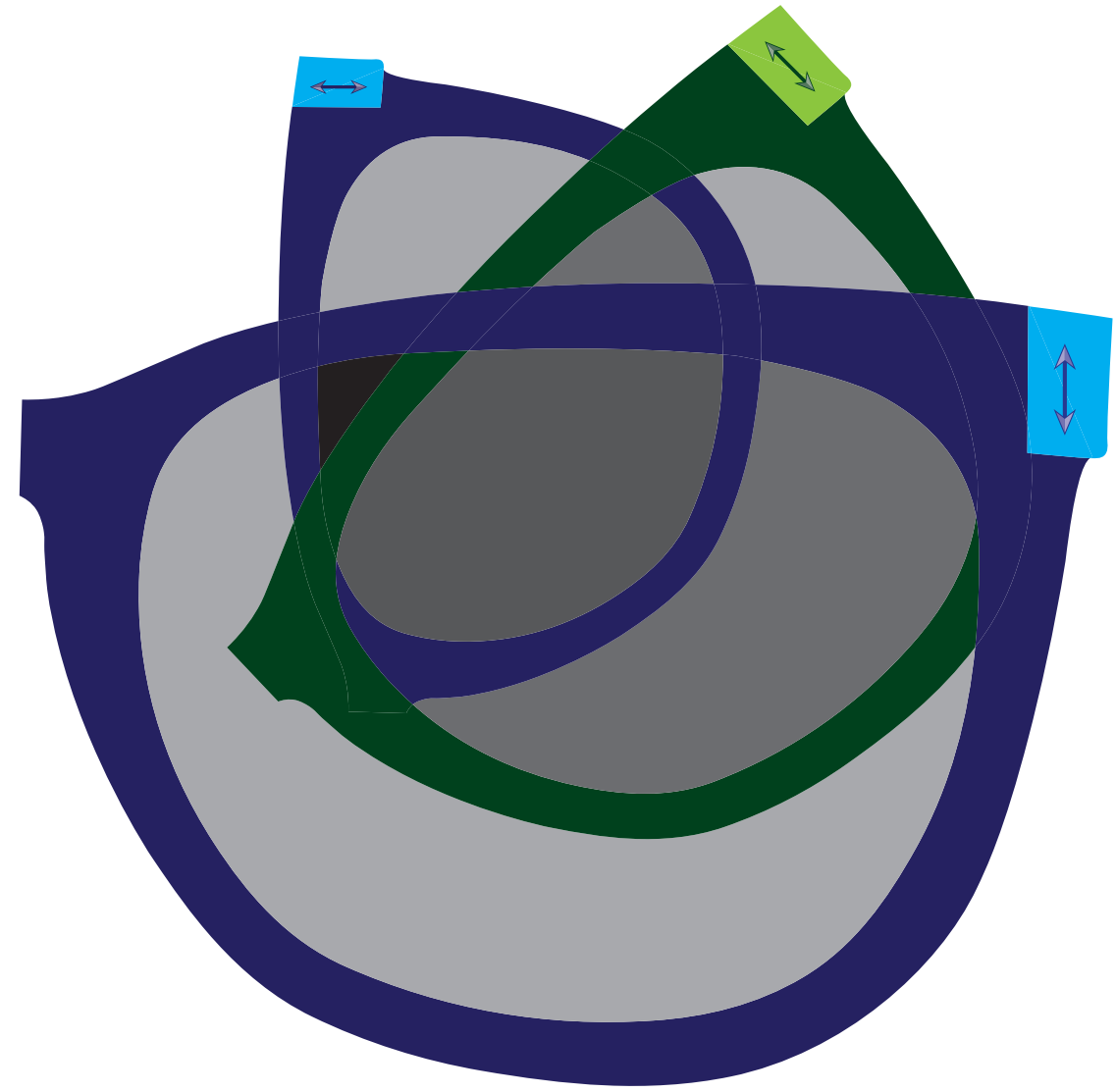
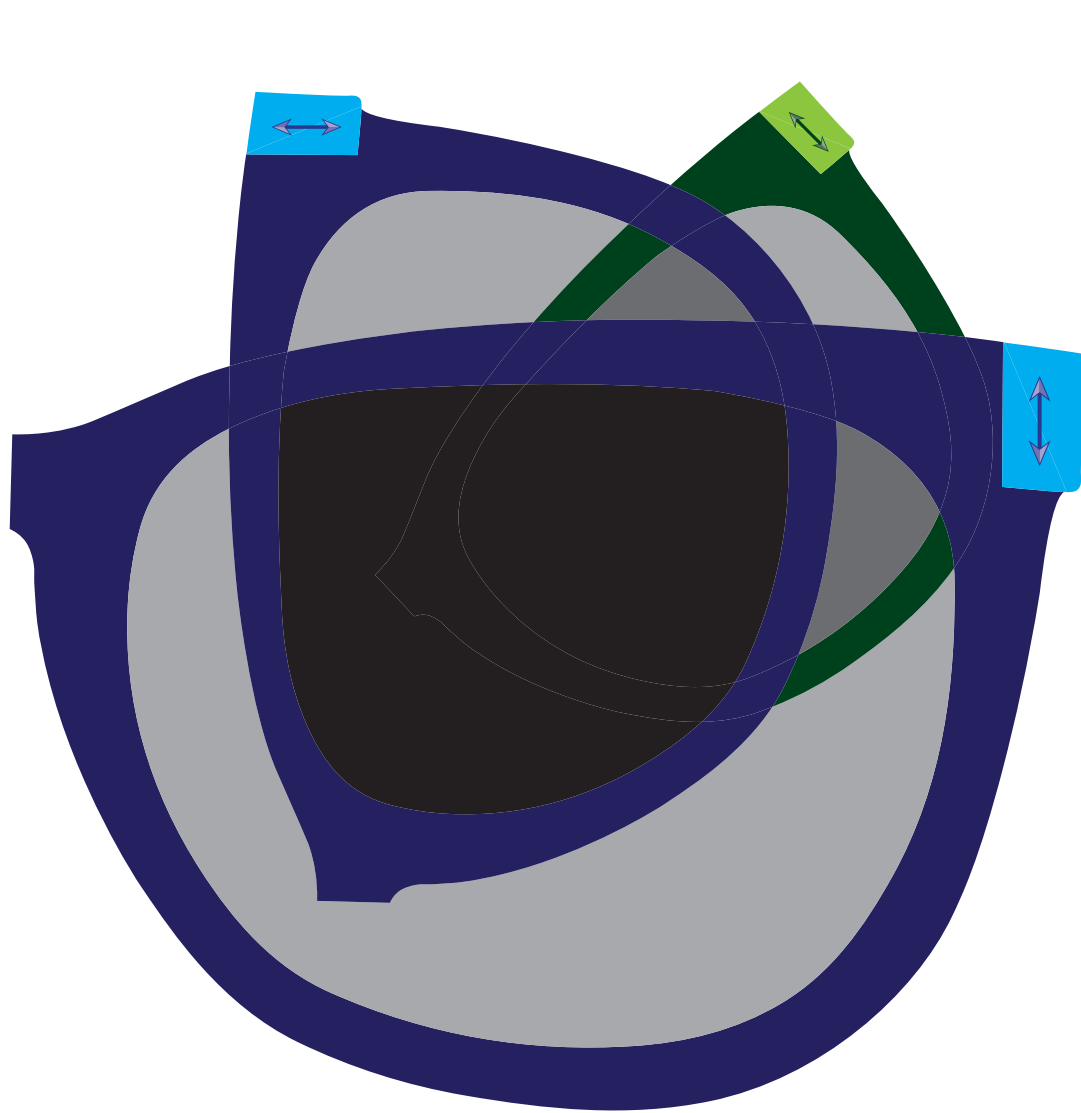
# Adding a third pair of glasses

---



# Order matters!

---



# Wearing sunglasses at night

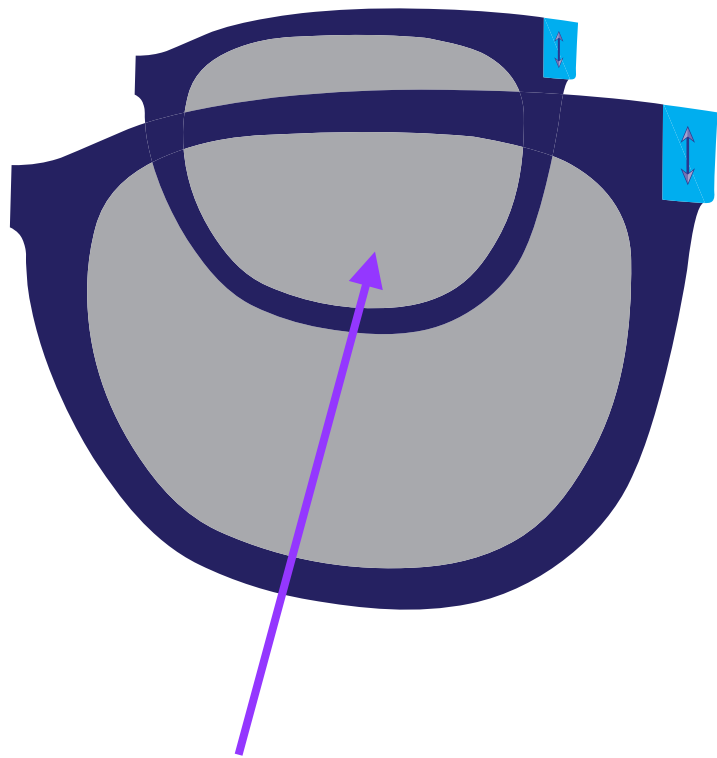
---



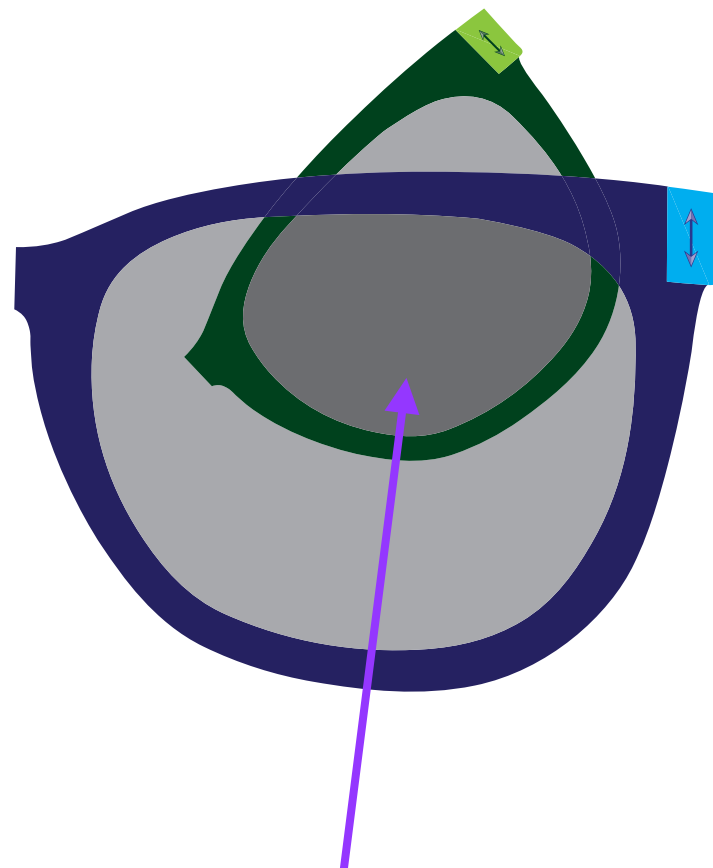
**Diane Knutson,  
International Dark-Sky  
Association**

# Fraction of photons making it through

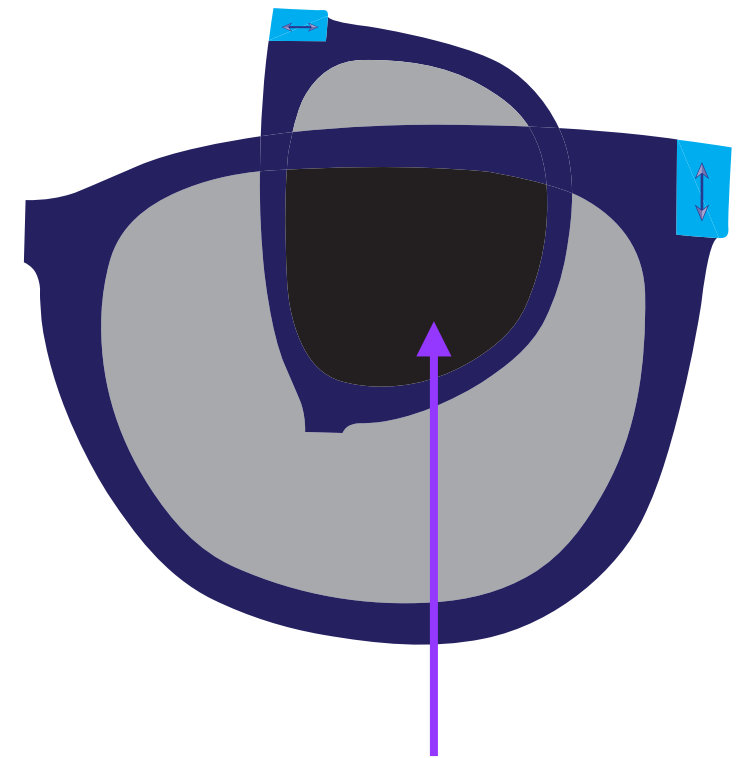
---



$$1/2 * \text{all} = 1/2$$



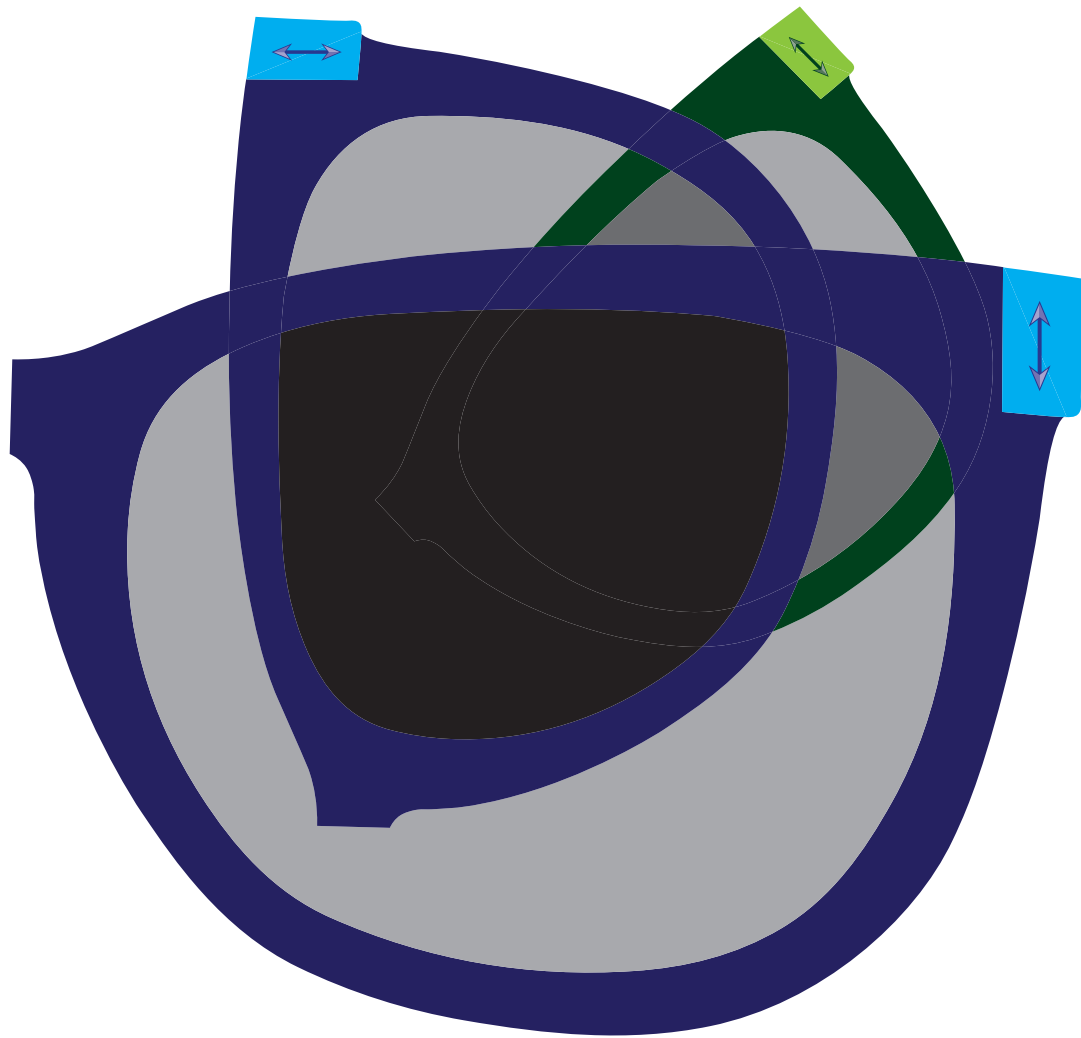
$$1/2 * 1/2 = 1/4$$



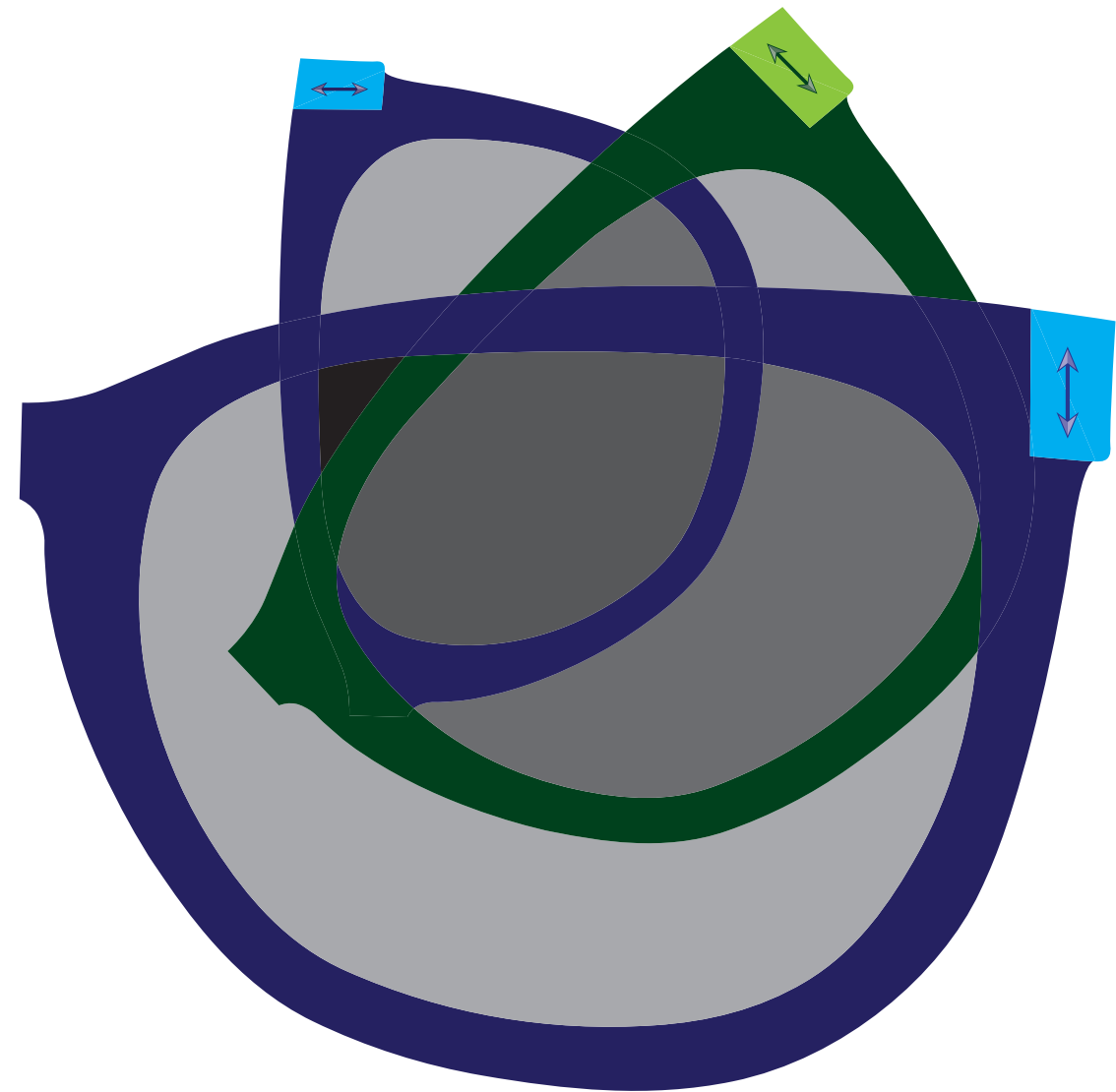
$$1/2 * \text{none} = 0$$

# Fraction of photons making it through

---



$$1/2 * 1/2 * \text{none} = 0$$

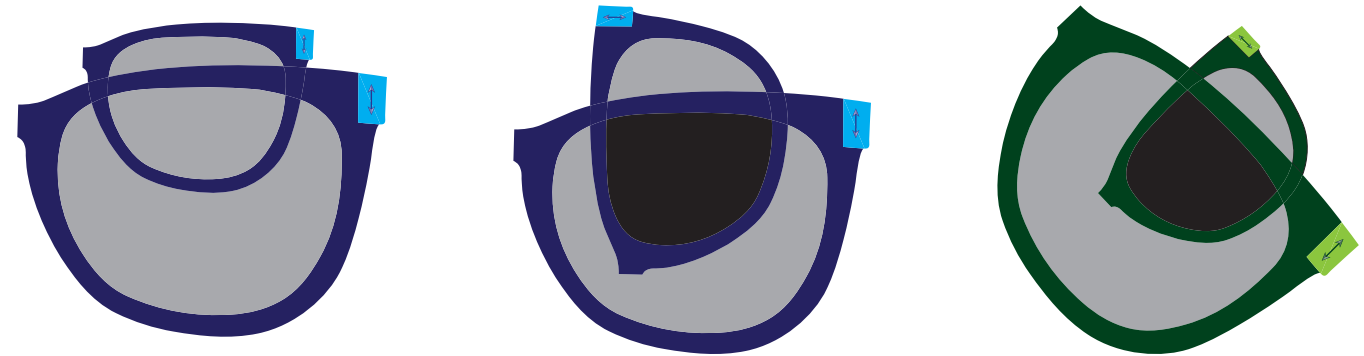


$$1/2 * 1/2 * 1/2 = 1/8$$

# Deterministic or Random

---

- If two glasses from the same set (frame color), whether a photon makes it through the next pair is deterministic (all or none)



- If two glasses from different sets, probability of photon making it through the second pair is *random* (always 50-50)



# Deterministic and random

---

- We've made two sets of glasses (green or blue frame color) that are internally deterministic but mutually random.
- A **deep** feature of quantum mechanics