Quantum Information and Computation

Eric Moorhouse

Department of Mathematics
University of Wyoming

Aspects of Quantum Information Theory

- quantum computation
- quantum cryptography
- quantum (error-correcting) codes
- quantum teleportation

Cryptosystem

- protecting information from unauthorized access or alteration
- authentication (certifying authorship of messages)

Cryptology

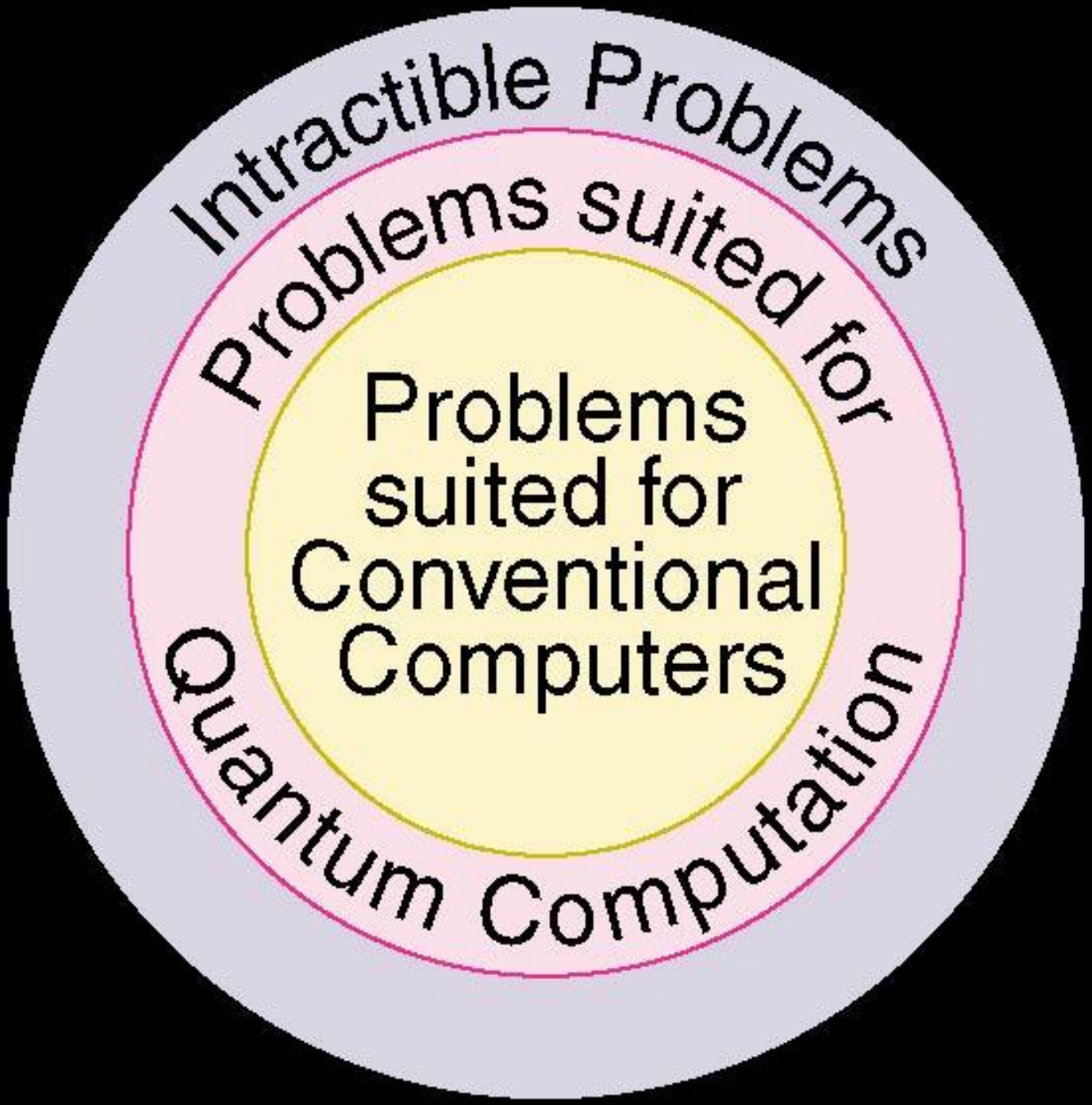
Cryptography
(making/using cryptosystems)

Cryptanalysis
(attempting to break cryptosystems)

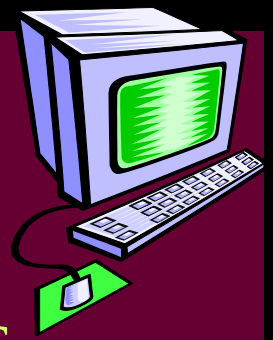
vs.

Coding Theory (Error-Correcting Codes)

- protecting information from alteration due to environment

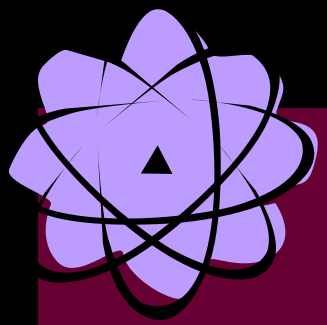

Intractible Problems
Problems suited for
Quantum Computation
Problems
suited for
Conventional
Computers

nanocomputers



- Miniaturization of conventional computers using conventional algorithms
- Increase in computation speed by a few orders of magnitude only

vs.



quantum computers

- Entirely new breed of (hypothetical) computers using massively parallel algorithms
- Increase in computation speed by indefinitely many orders of magnitude

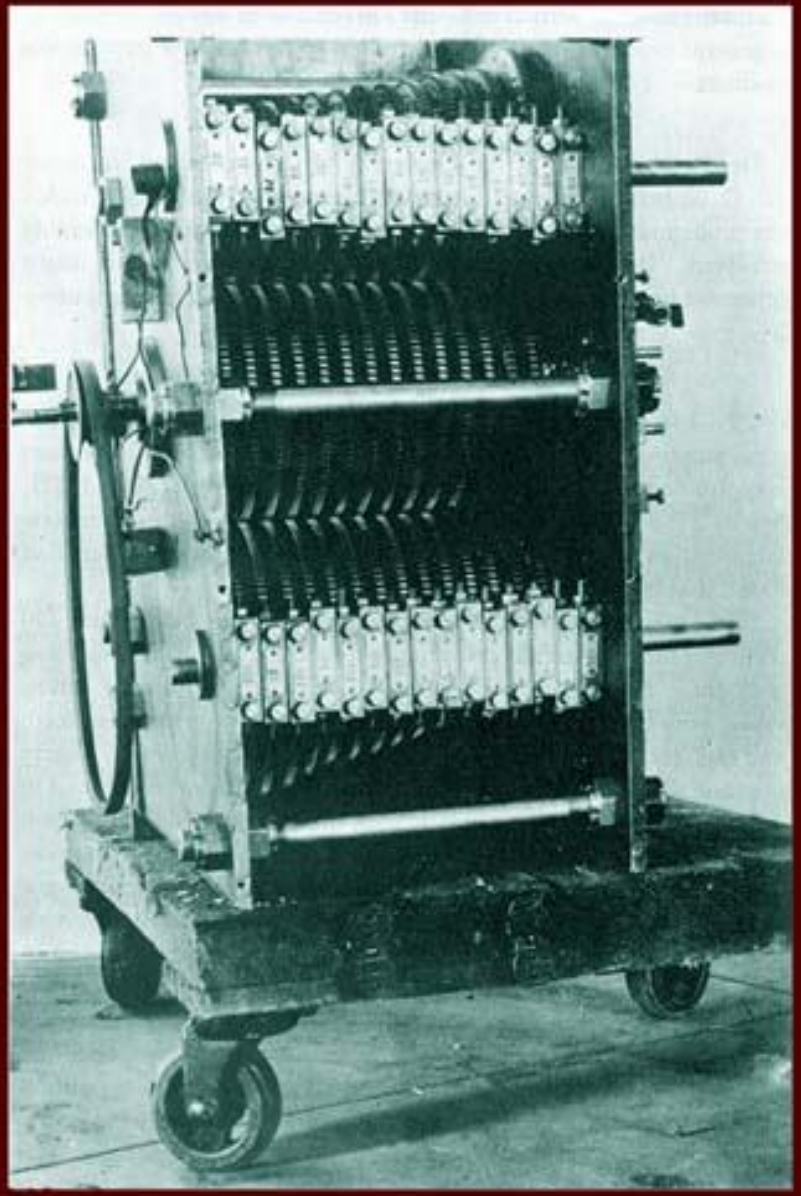
Peter Shor

Why the recent interest in quantum computers?

Conventional computers are able to factor integers of at most 120 digits.

$$1751799061916670 73$$
$$= 88917251 \times 1970145323$$

Shor (mid-1990's) showed much larger integers can be factored using a (hypothetical) quantum computer.



Dr. Lehmer's Factoring Machine (1930's)

15372286720933014 19

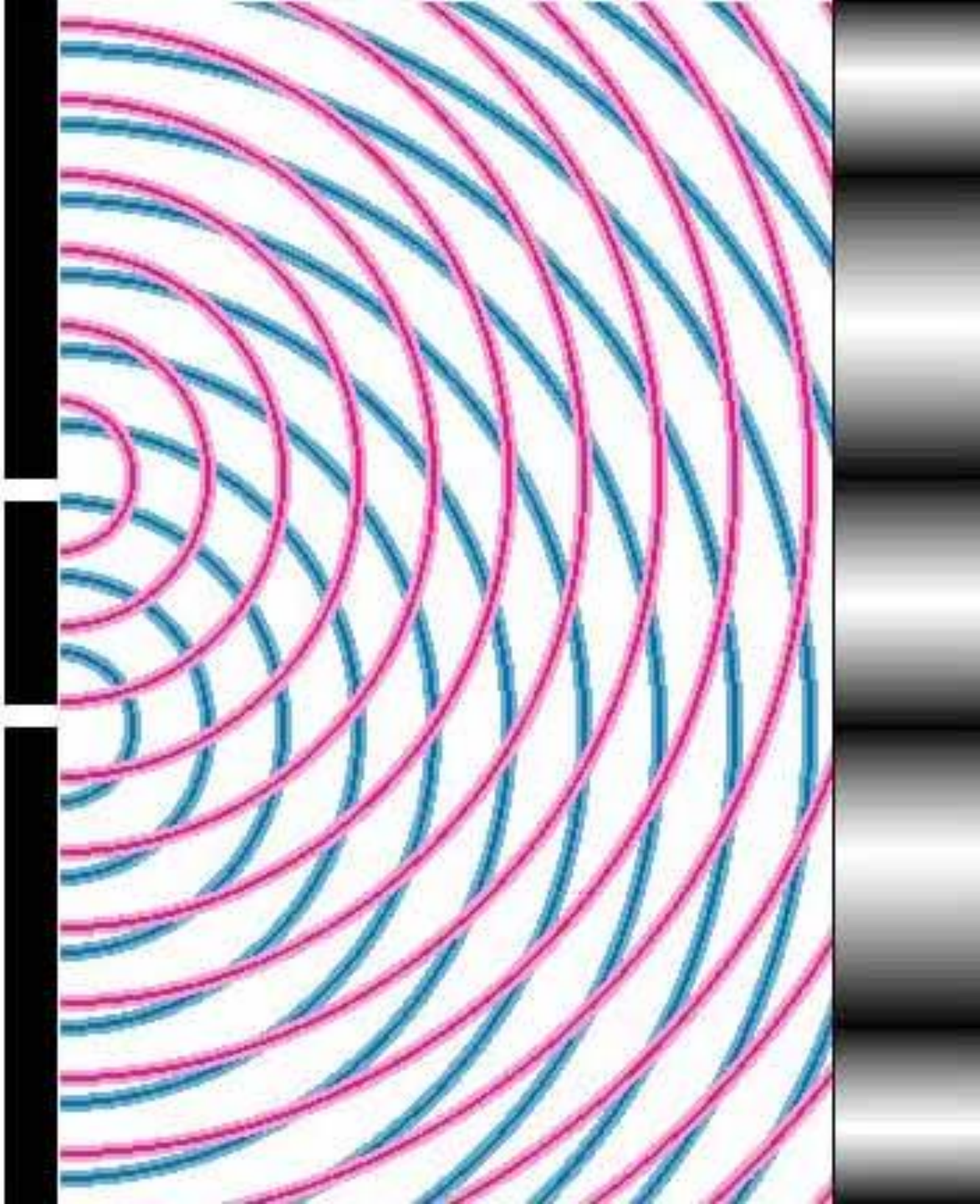
= 529510939 x 2903110321

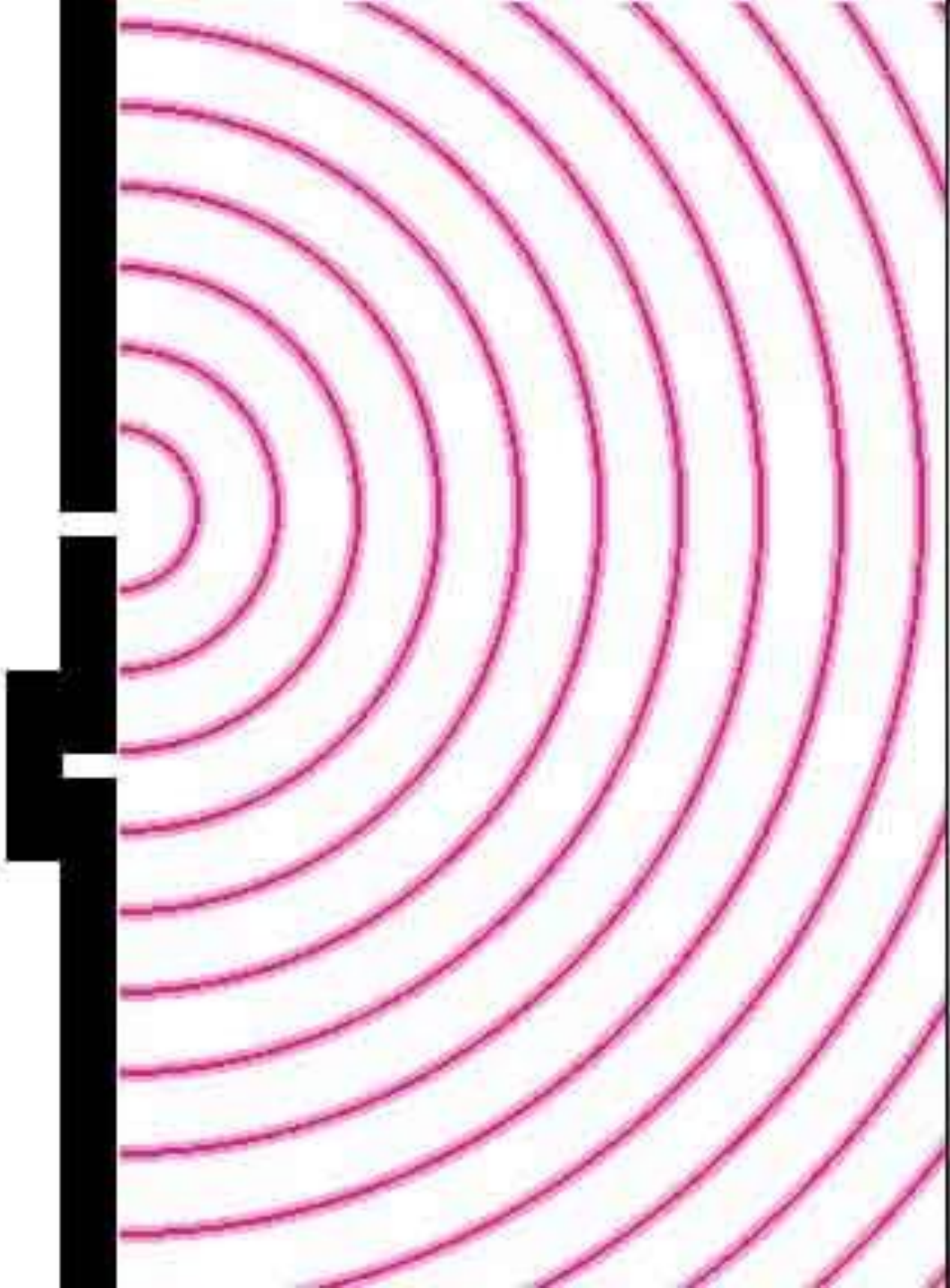
RSA Public Key Cryptography

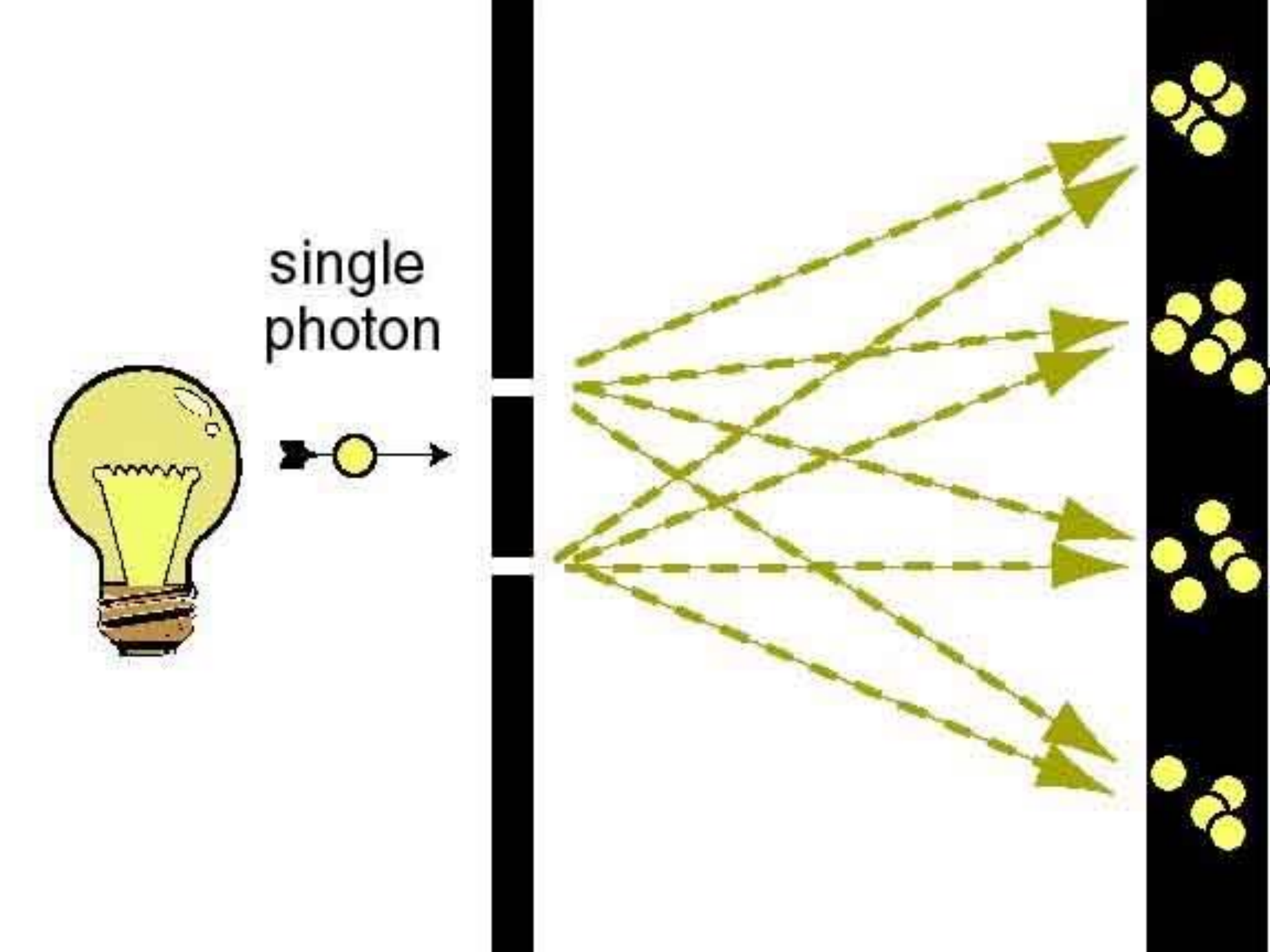
Encryption uses $n = pq$ *(public key)* where p and q are *large* primes.

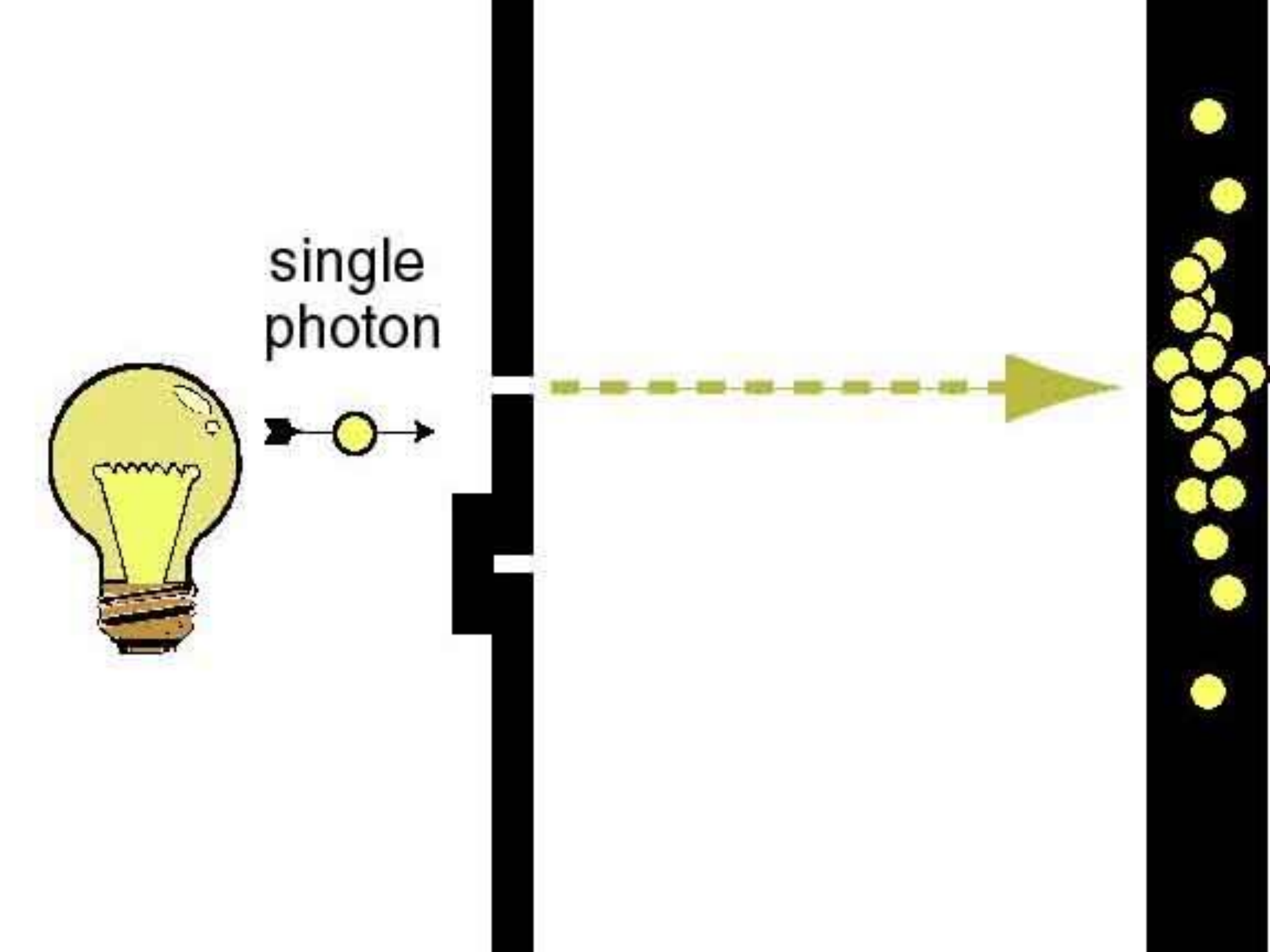
Decryption requires knowledge of p and q *(private key)*.

A Crash Course in Quantum Mechanics



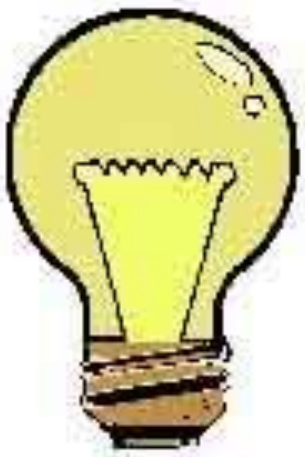


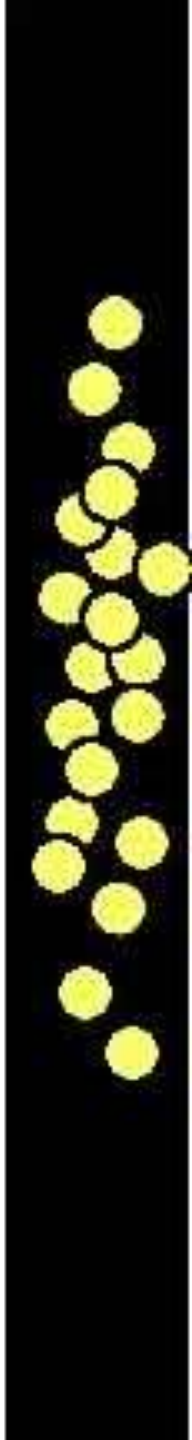

single
photon

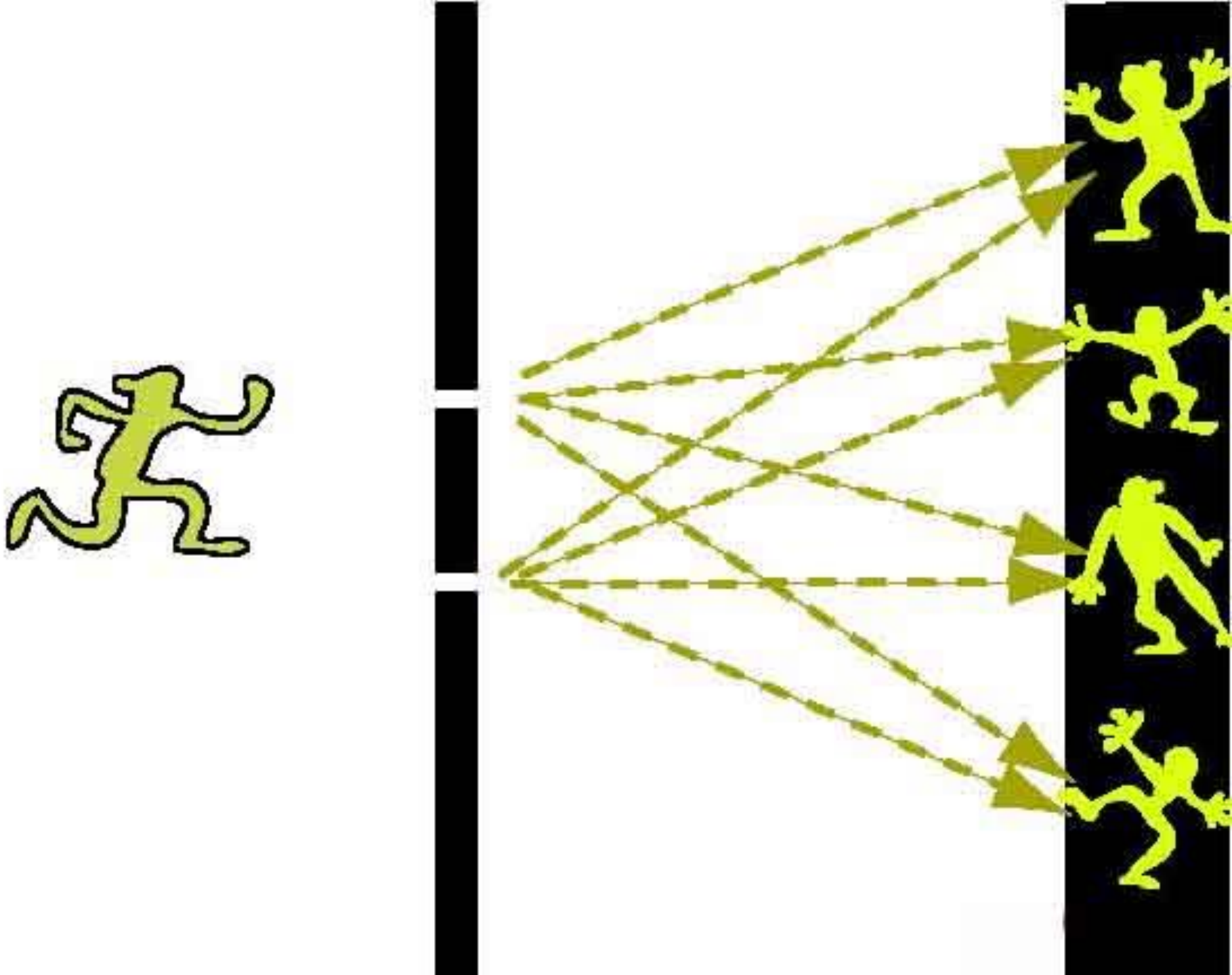

single
photon

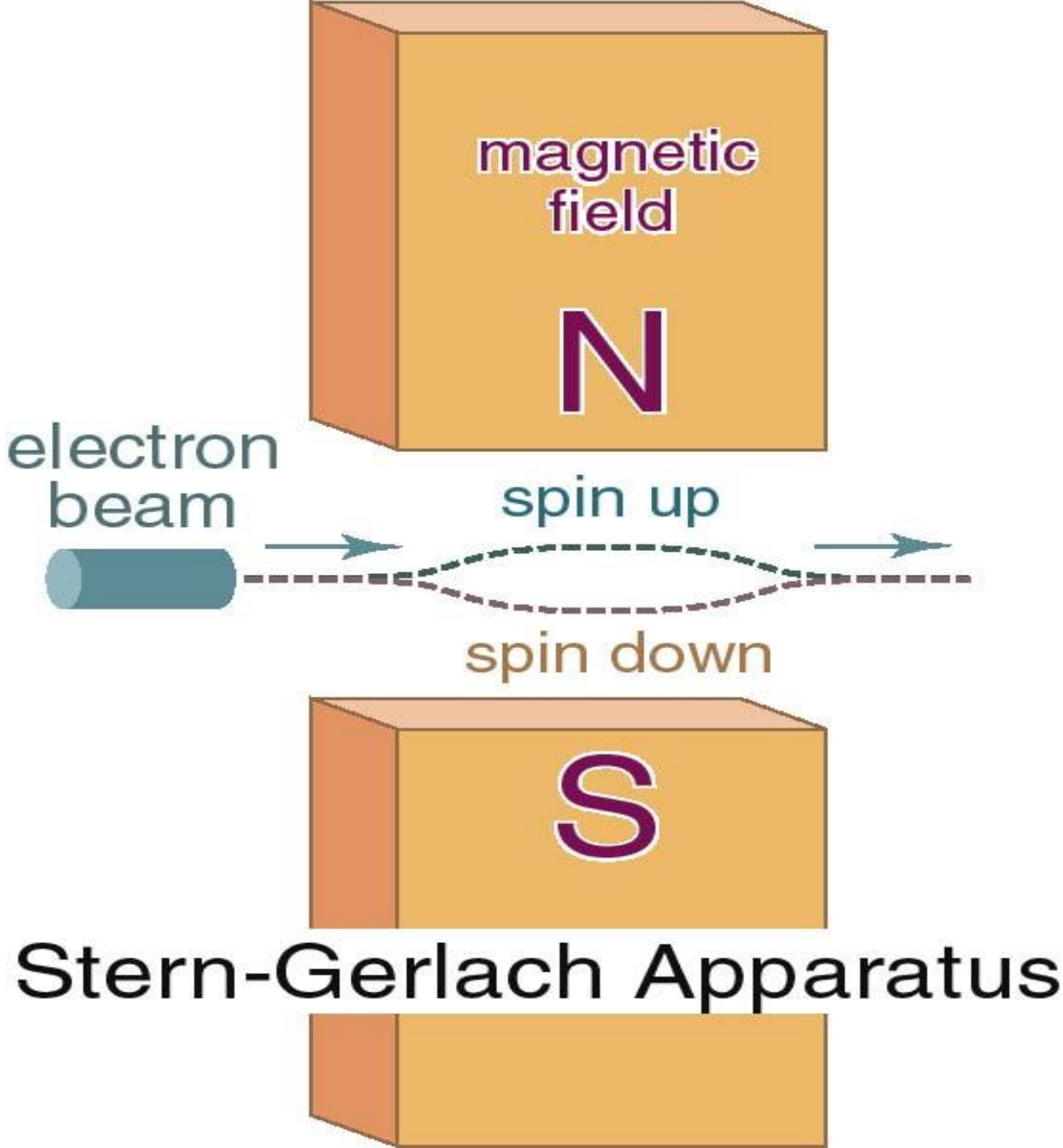
Prediction of
Classical Mechanics
(incorrect)

single
photon

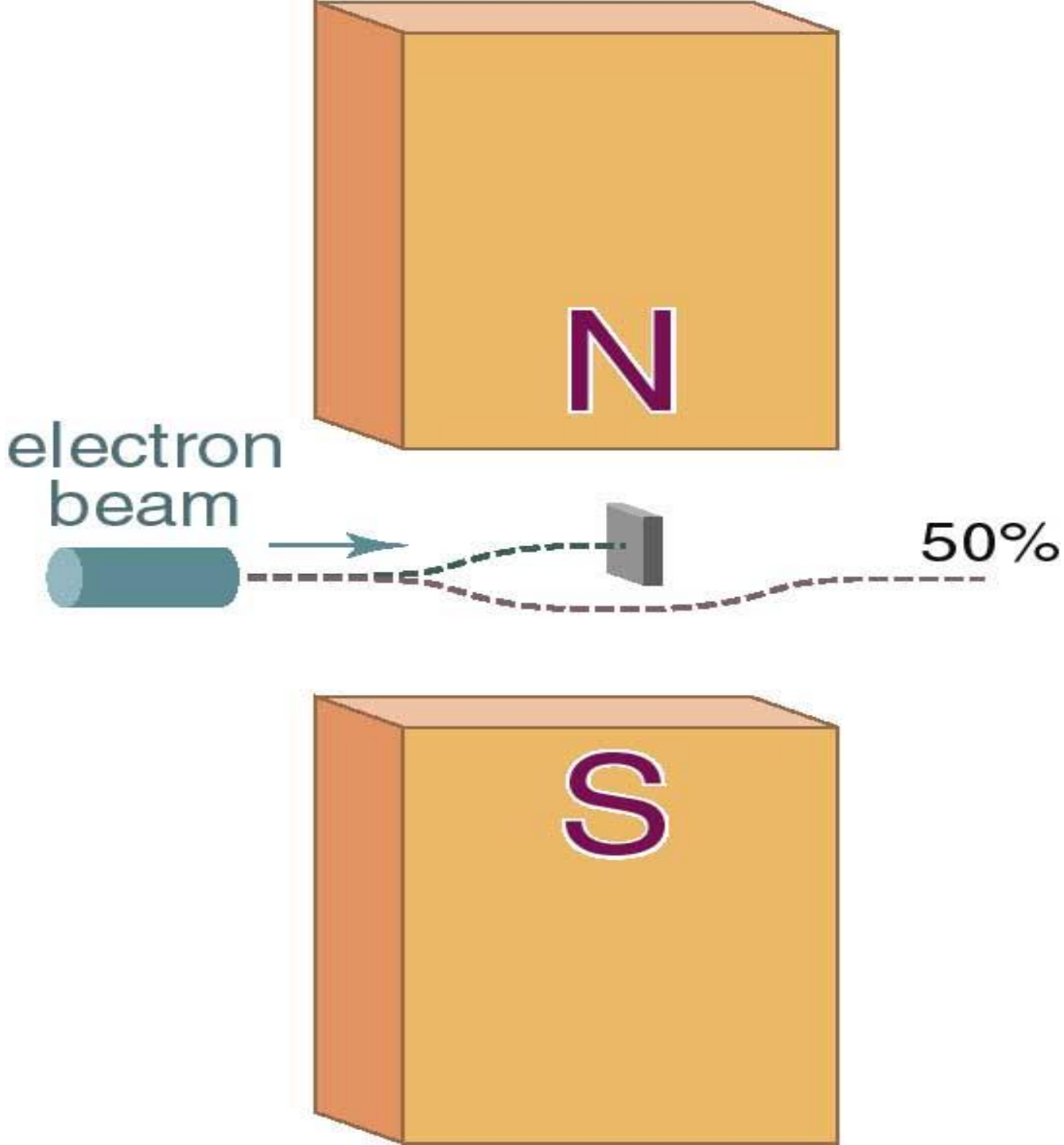


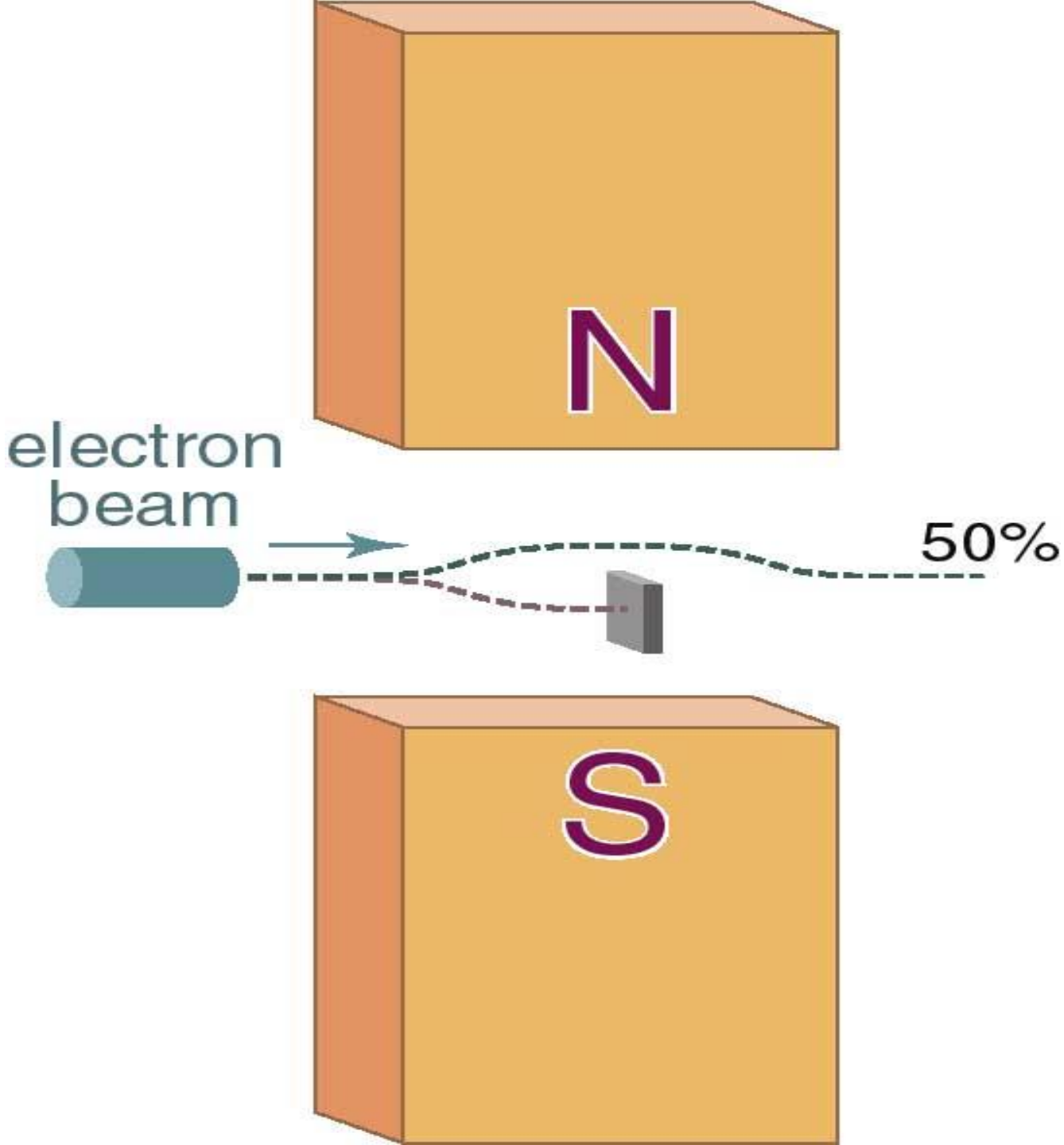


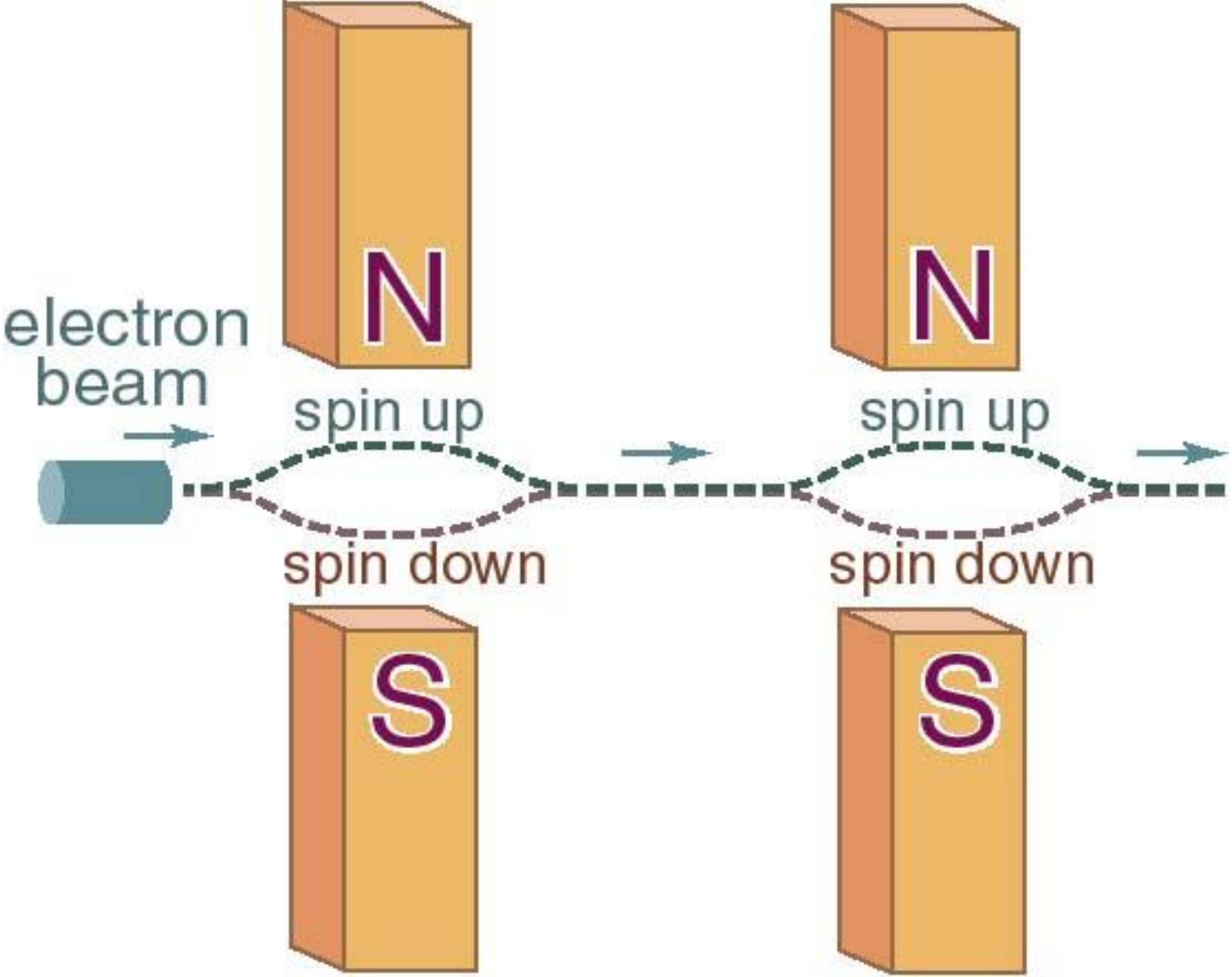


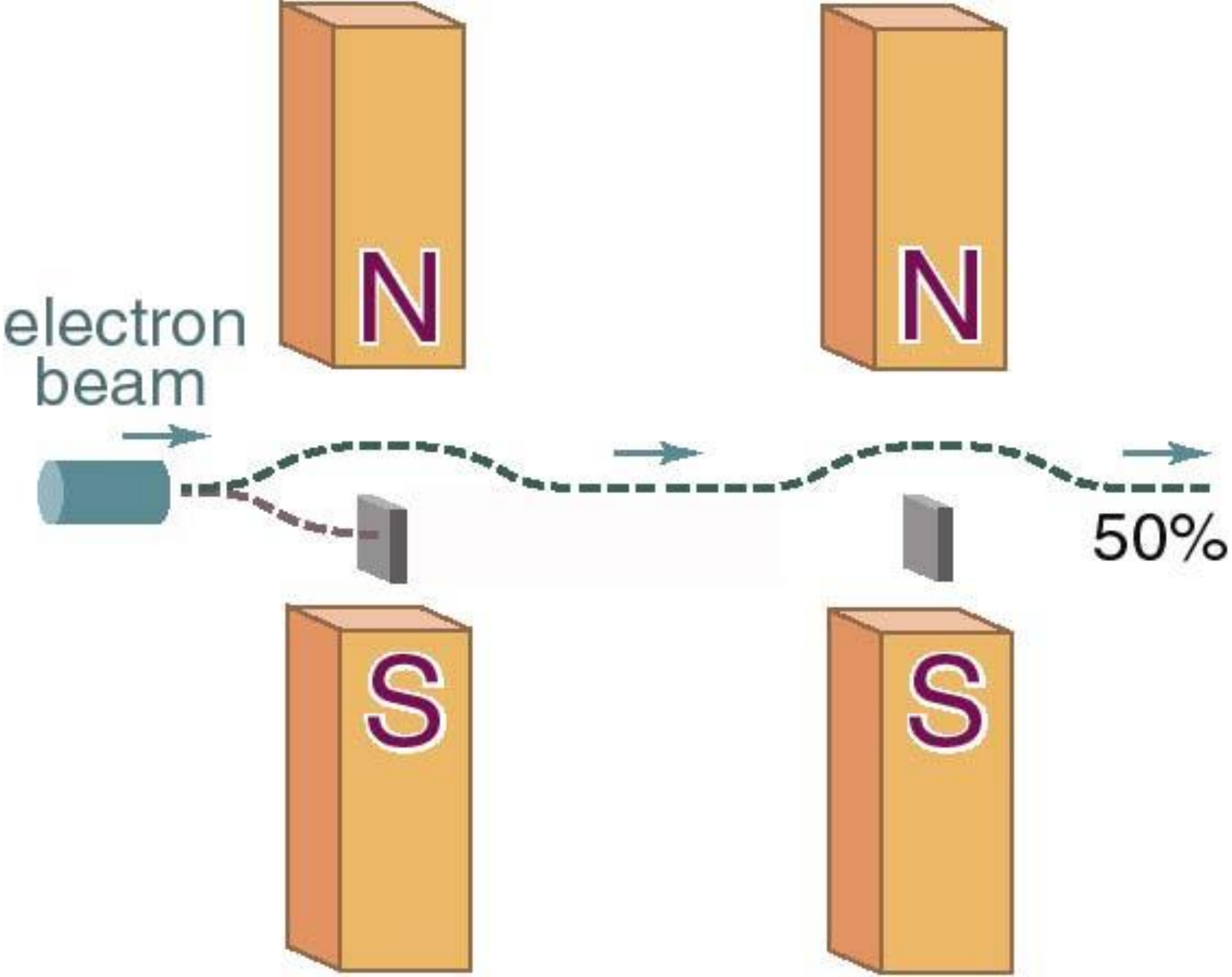


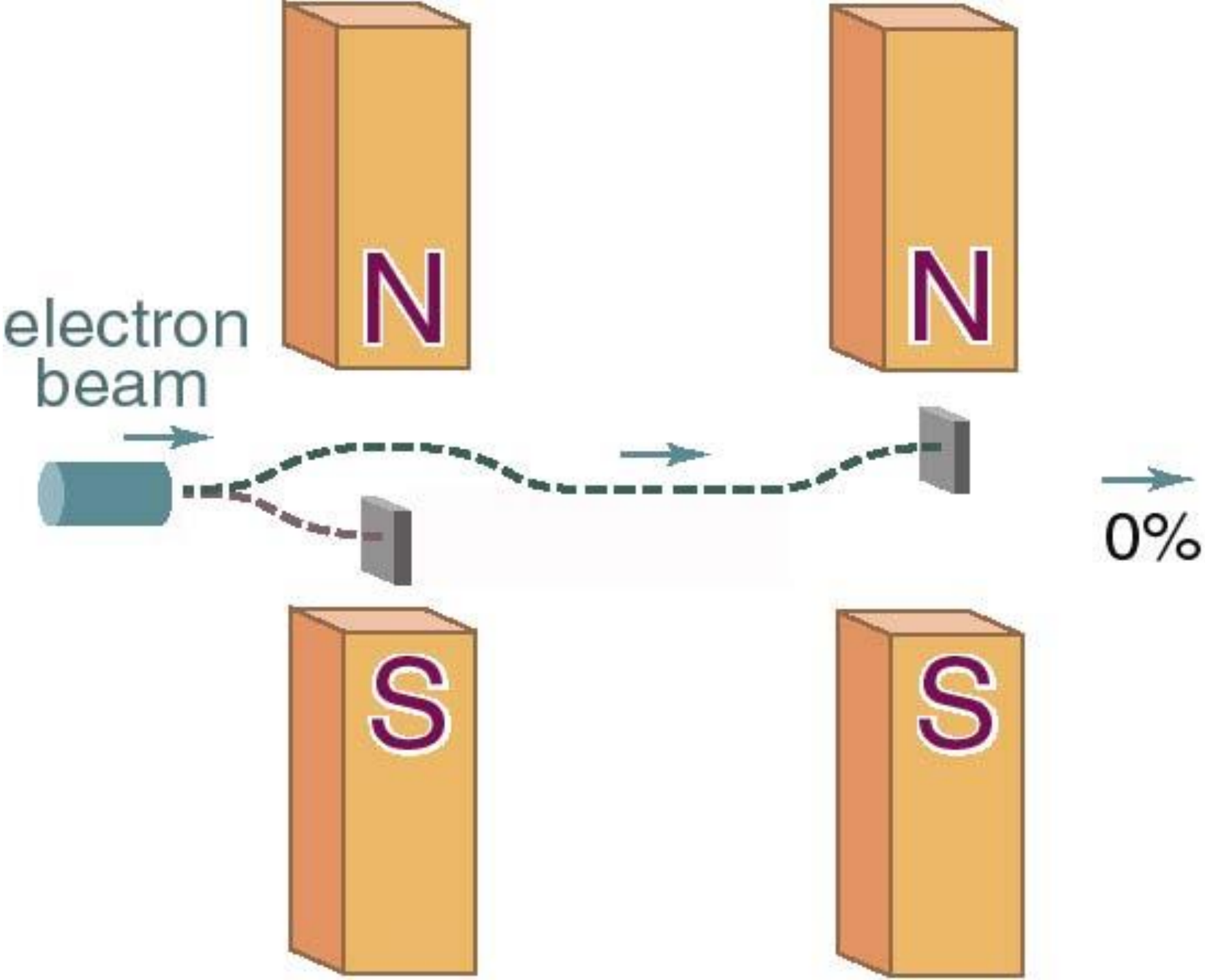
Stern-Gerlach Apparatus

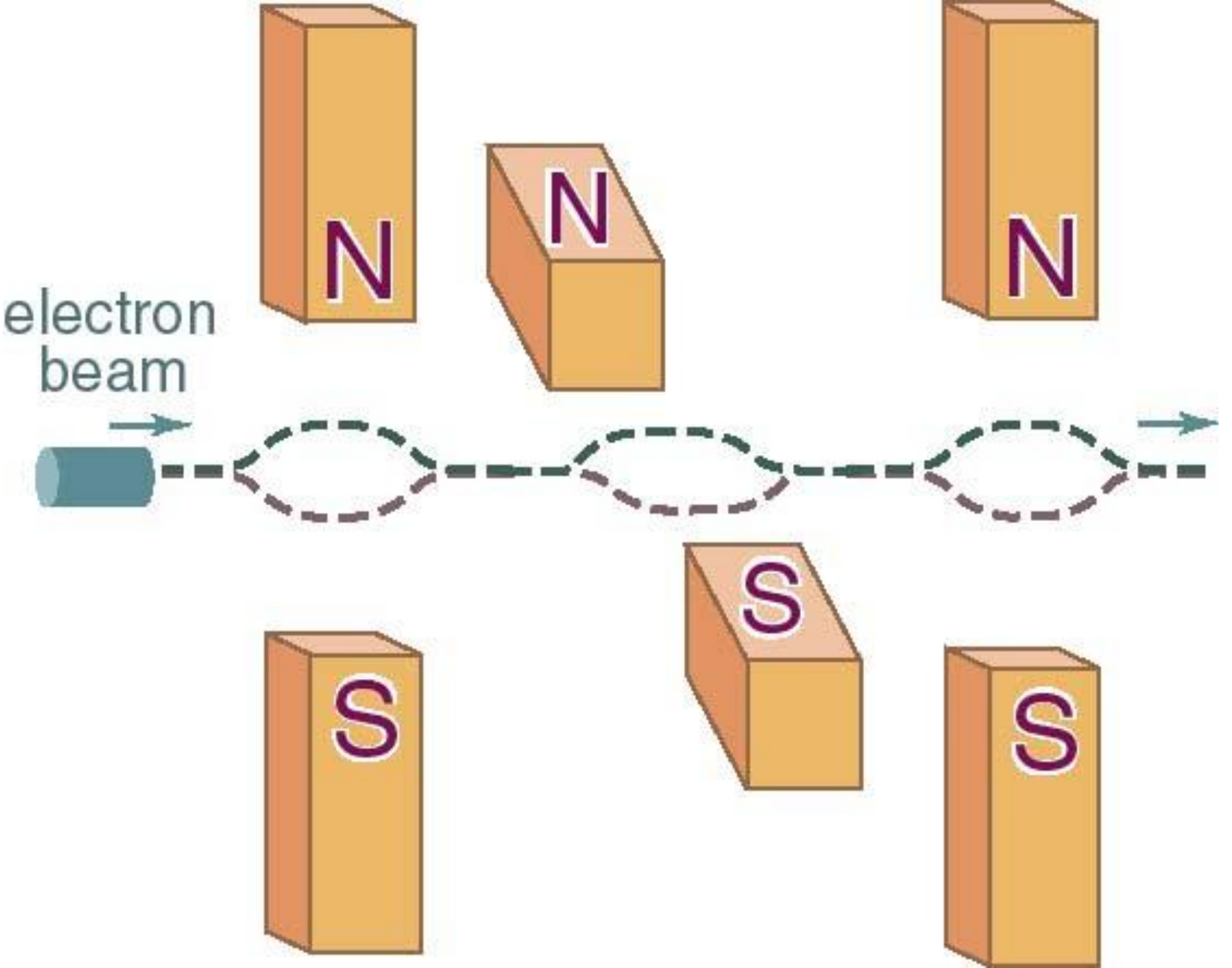

N
electron
beam
50%
S

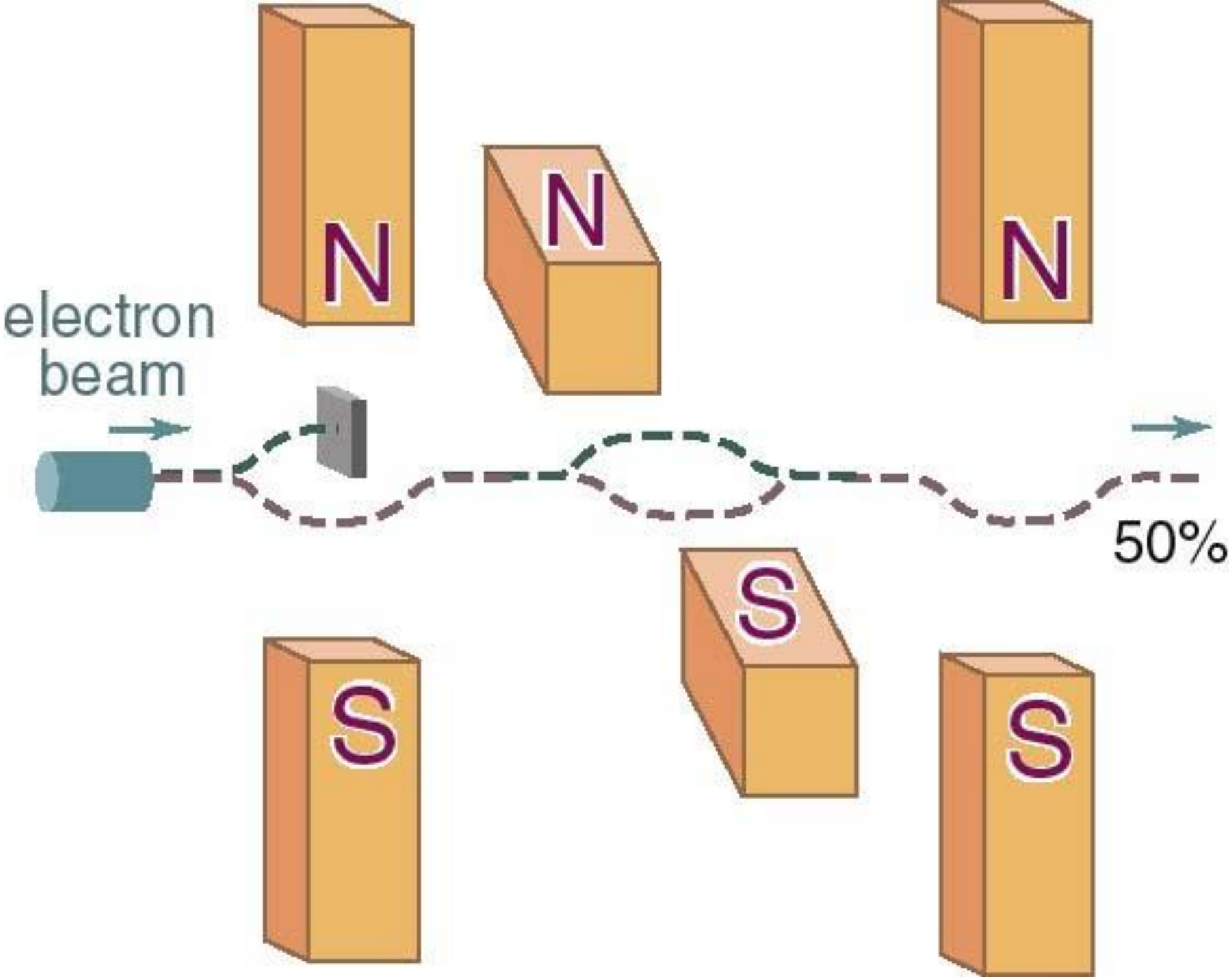

N
electron
beam
50%
S

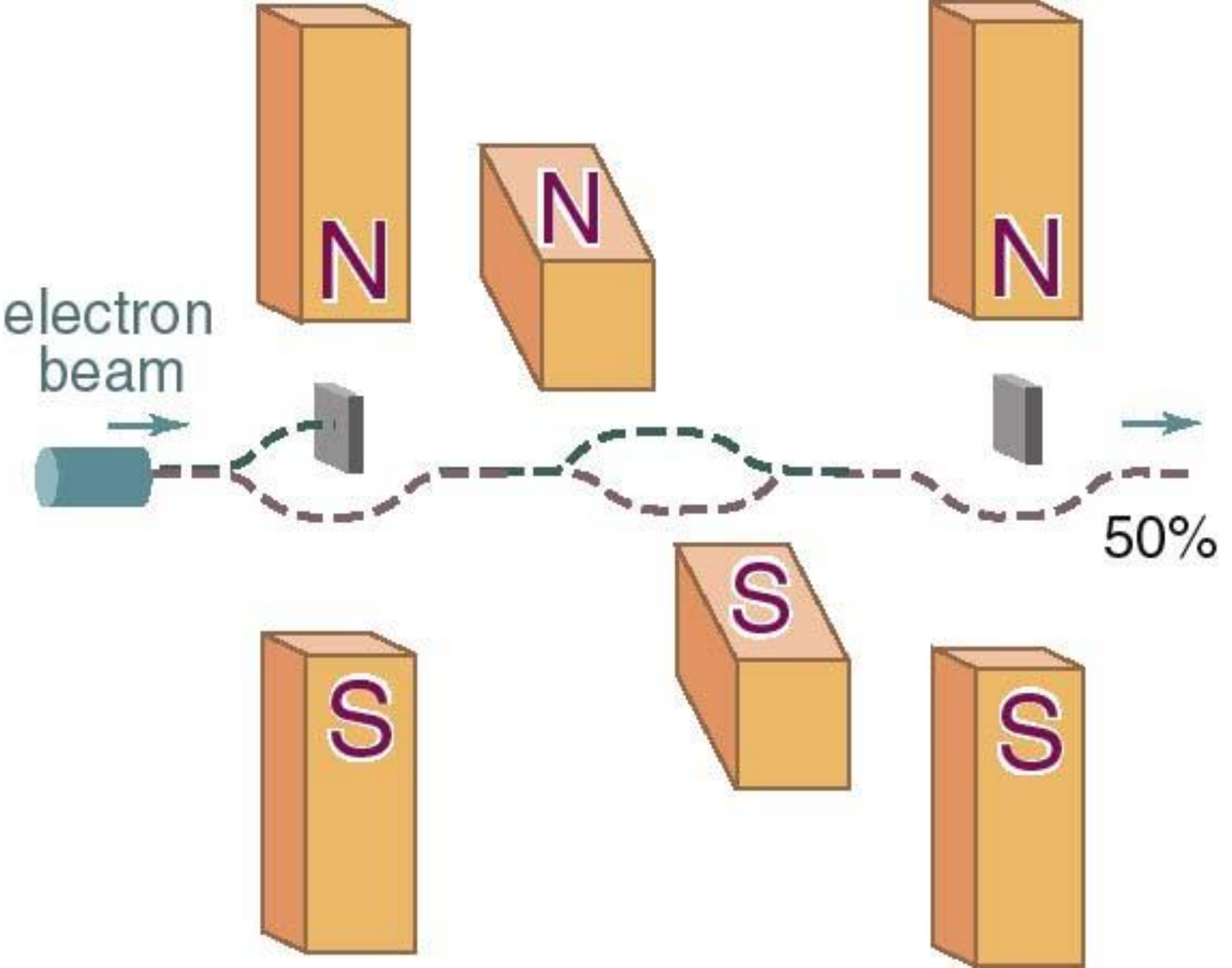

N
N
electron
beam
spin up
spin up
spin down
spin down
S
S

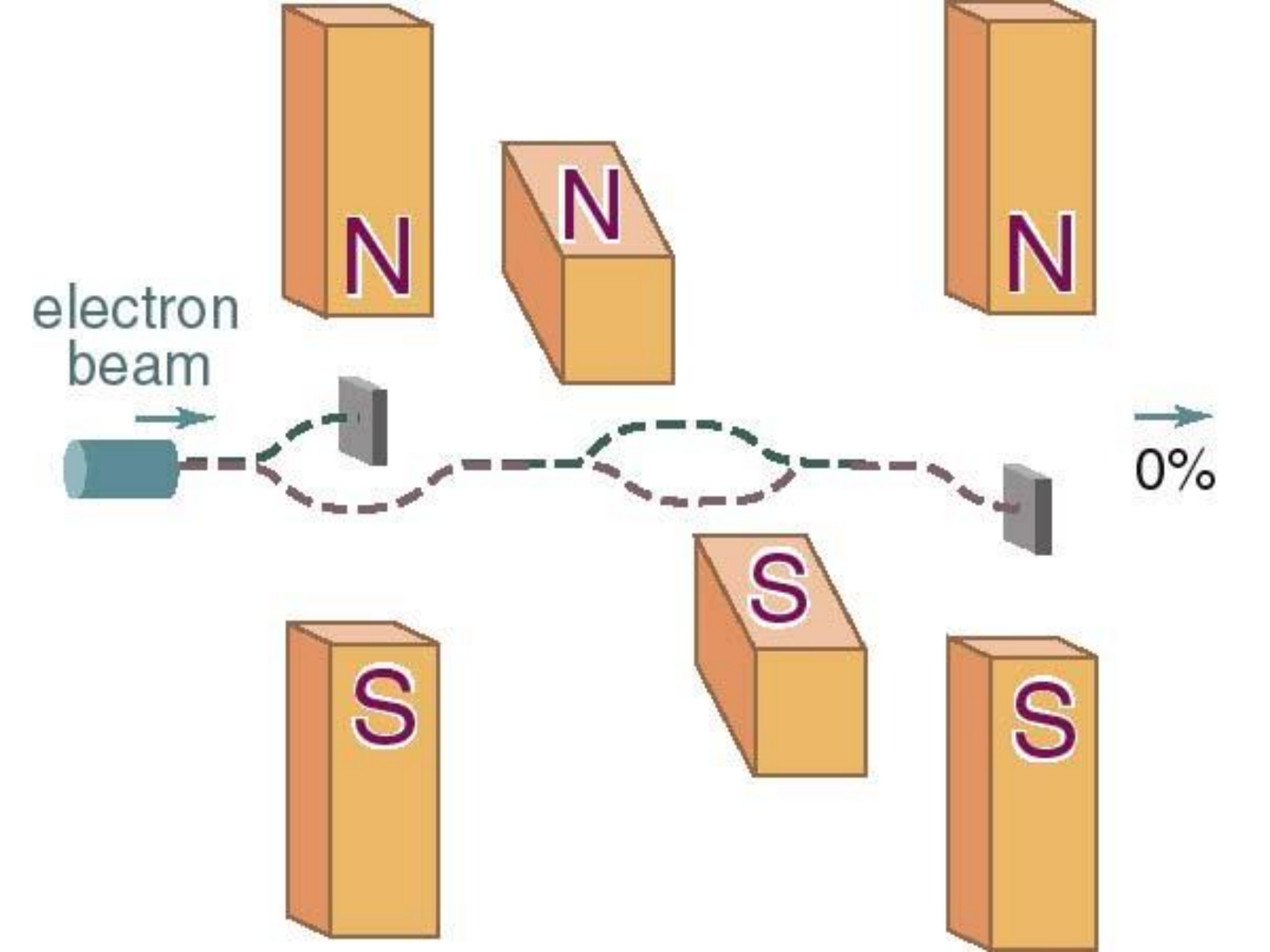

N
N
electron
beam
50%
S
S

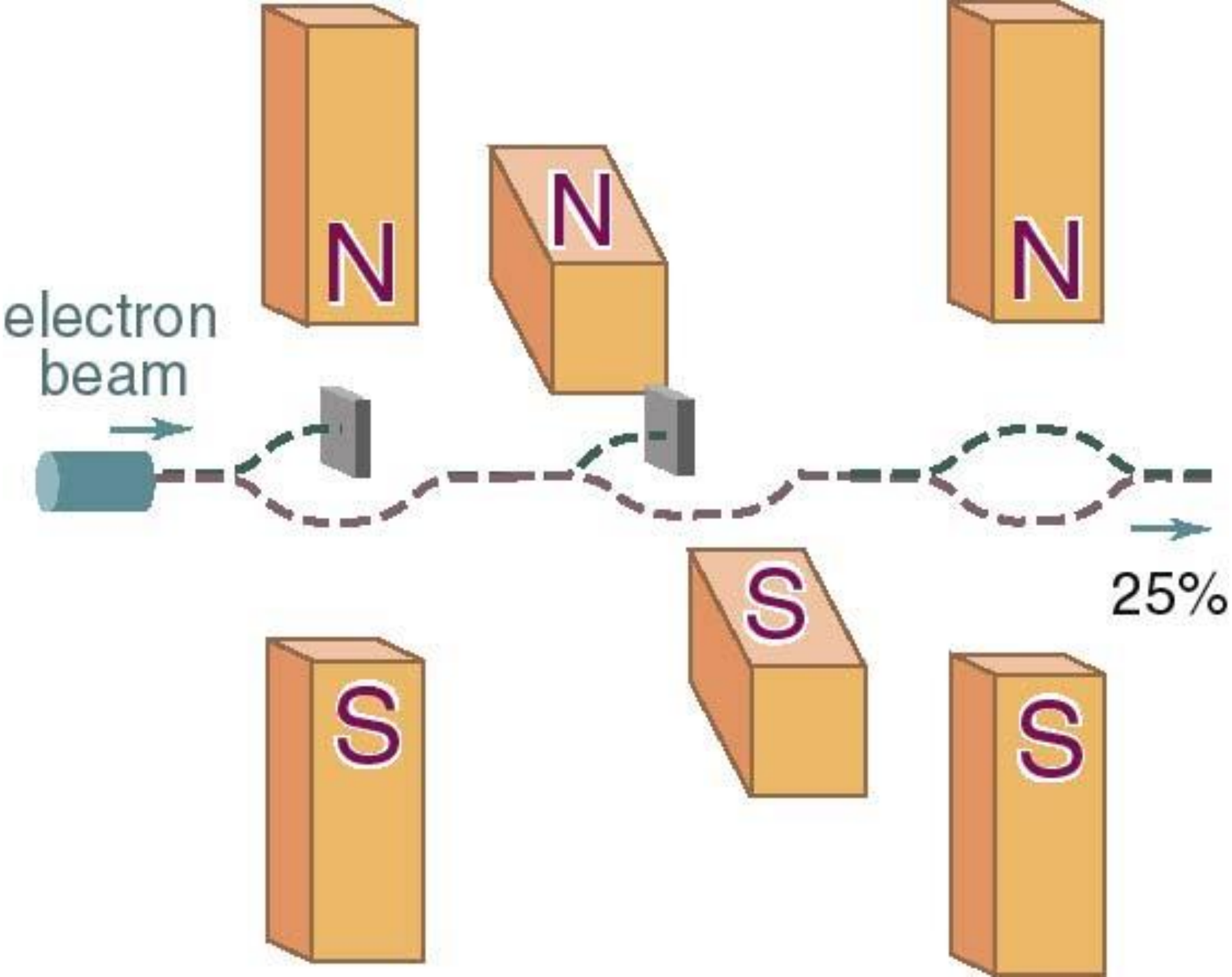

N
N
electron
beam
0%
S
S

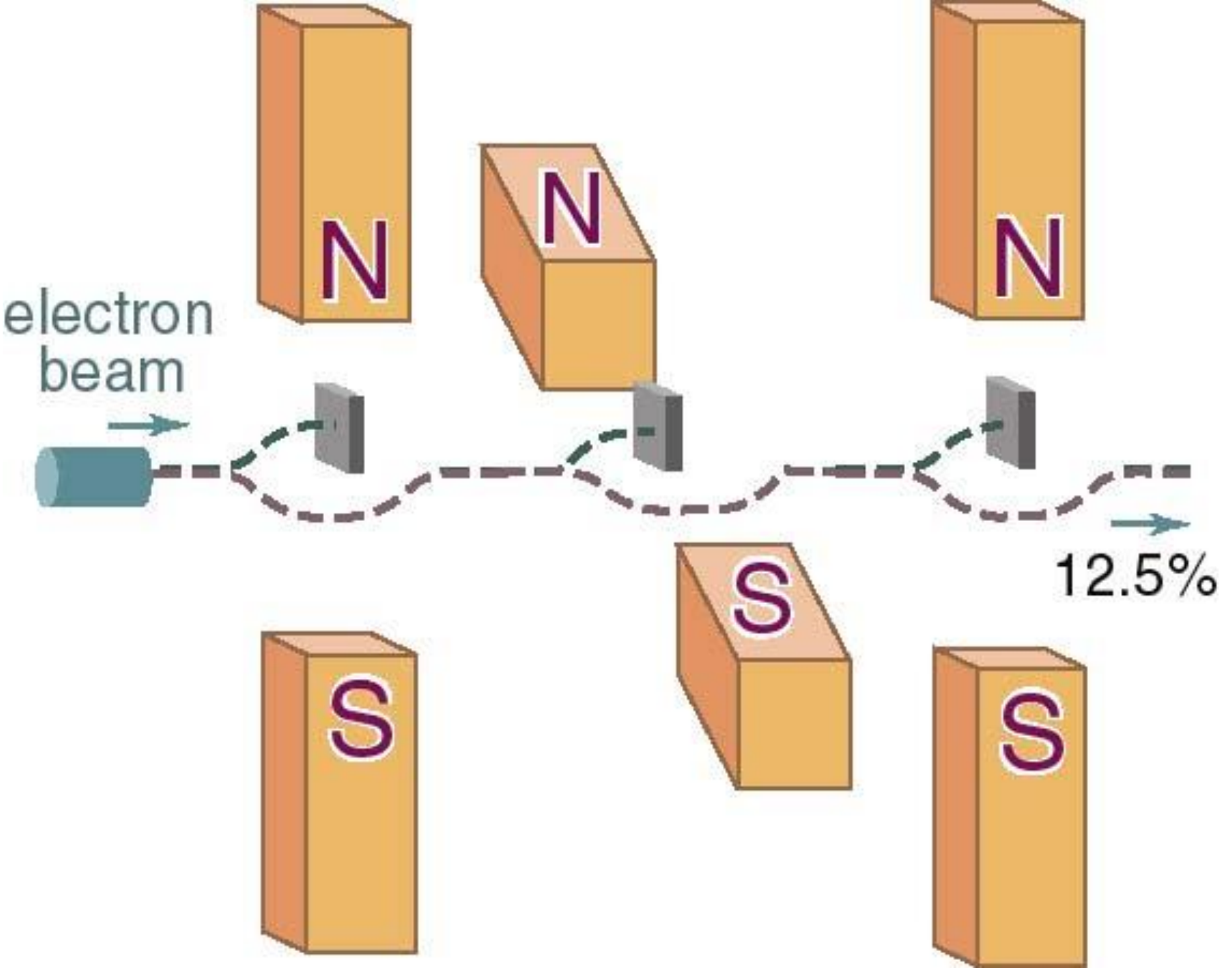

N
N
N
electron
beam
S
S
S

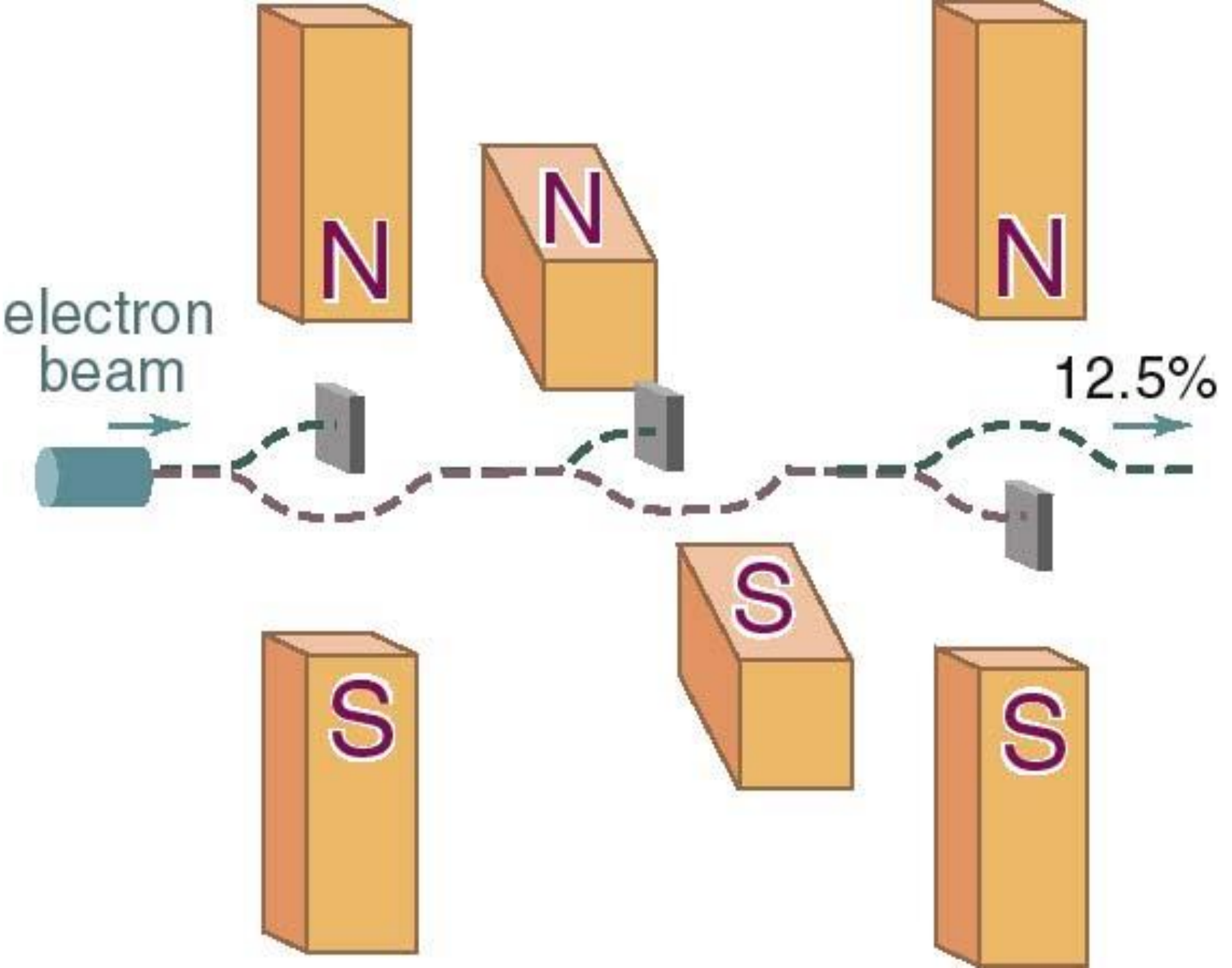

N
N
N
electron
beam
50%
S
S
S


N
N
N
electron
beam
50%
S
S
S


N
N
N
electron
beam
0%
S
S
S

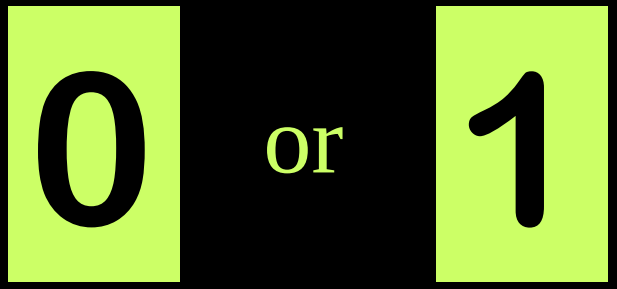

N
N
N
electron
beam
S
S
S
25%


N
N
N
electron
beam
12.5%
S
S
S


N
N
N
electron
beam
12.5%
S
S
S

Conventional Information

Unit: bit



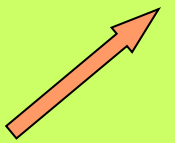
Conventional Information

Unit: bit

0 or **1**

Quantum Information

Unit: qubit



$\alpha, \beta \in \mathbb{C}, \quad |\alpha|^2 + |\beta|^2 = 1$

i.e. $(a,b,c,d) \in \mathbb{R}^4$,

$a^2+b^2+c^2+d^2 = 1$

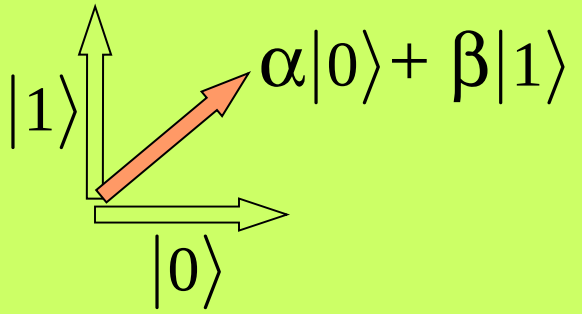
Conventional Information

Unit: bit

0 or **1**

Quantum Information

Unit: qubit



$\alpha, \beta \in \mathbb{C}, \quad |\alpha|^2 + |\beta|^2 = 1$

The State of an Electron

State $= |\psi\rangle = \alpha|0\rangle + \beta|1\rangle$

where $\alpha, \beta \in \mathbb{C}$ (complex numbers) such that

$$|\alpha|^2 + |\beta|^2 = 1$$

$|\alpha|^2 =$ probability that the electron, if measured, will be found to have spin *up*

$|\beta|^2 =$ probability that the electron, if measured, will be found to have spin *down*

The State of a Pair of Electrons

$$|\psi\rangle = \alpha_{00}|00\rangle + \alpha_{01}|01\rangle + \alpha_{10}|10\rangle + \alpha_{11}|11\rangle$$

where $\alpha_{00}, \alpha_{01}, \alpha_{10}, \alpha_{11} \in \mathbb{C}$ such that

$$|\alpha_{00}|^2 + |\alpha_{01}|^2 + |\alpha_{10}|^2 + |\alpha_{11}|^2 = 1$$

$|\alpha_{00}|^2$ = probability that both electrons, if measured, will be found to have spin *up*

$|\alpha_{01}|^2$ = probability that if measured, the first electron will be found to have spin *up*, and the second electron spin *down*

etc.

The State of a System of n Electrons

$$|\psi\rangle = \sum_{i_1,i_2,\ldots,i_n} \alpha_{i_1,i_2,\ldots,i_n} |i_1, i_2, \ldots, i_n\rangle$$

where $$\sum_{i_1,i_2,\ldots,i_n} |\alpha_{i_1,i_2,\ldots,i_n}|^2 = 1$$

$|\alpha_{i_1,i_2,\ldots,i_n}|^2 =$ probability that if the entire system of electrons is measured, the k-th electron will have spin *up* or *down* according as $i_k = 0$ or 1

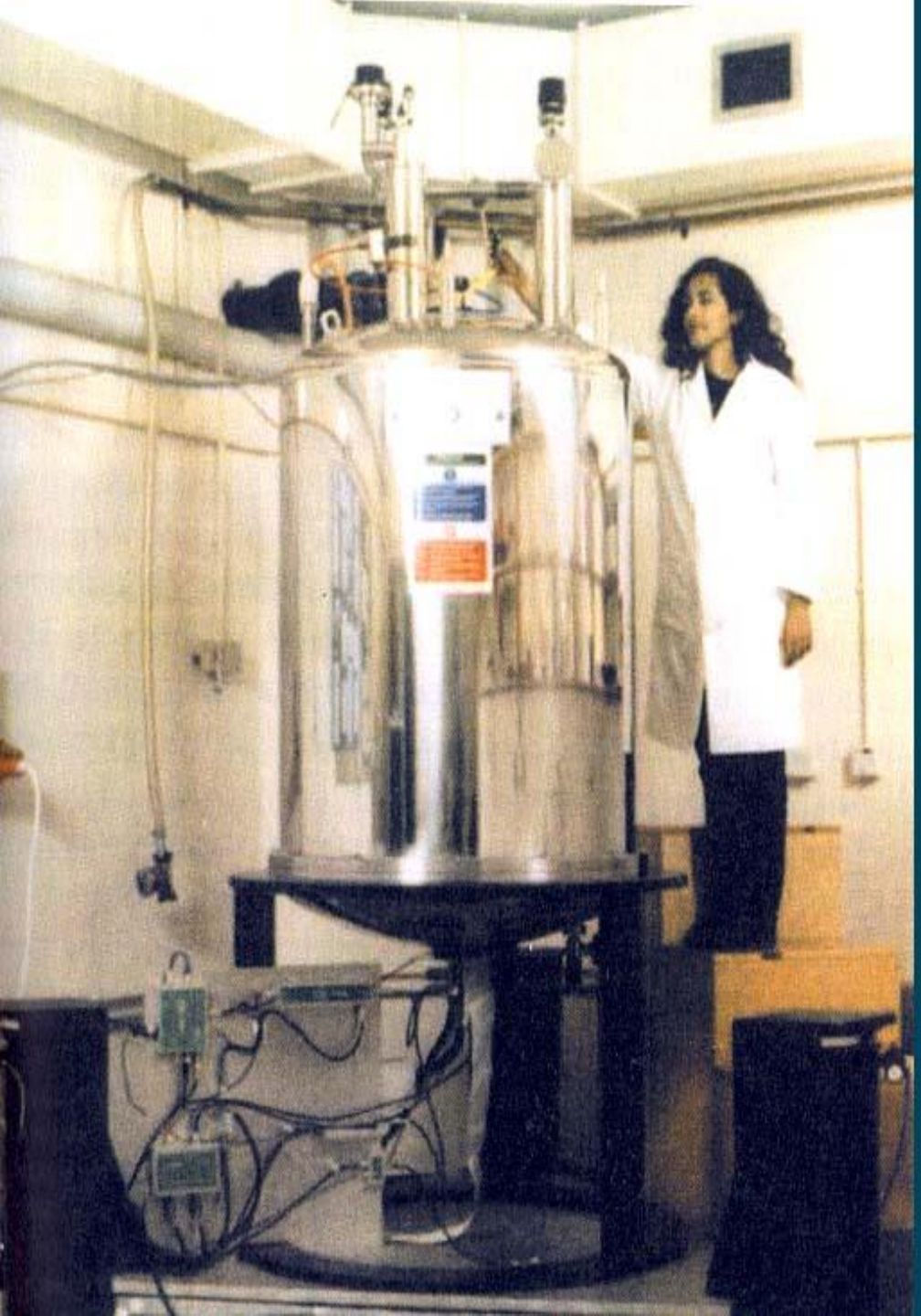
The vector space of all possible states is $\mathbb{C}^{2^n}$

What gives a quantum computer its exceptional power?

1. superposition principle
2. exponential number of base states
3. quantum entanglement

Useful computation requires hundreds of thousands of qubits (electrons).

We have only recently managed to realize a quantum computer with 7 qubits (electrons) using NMR techniques.

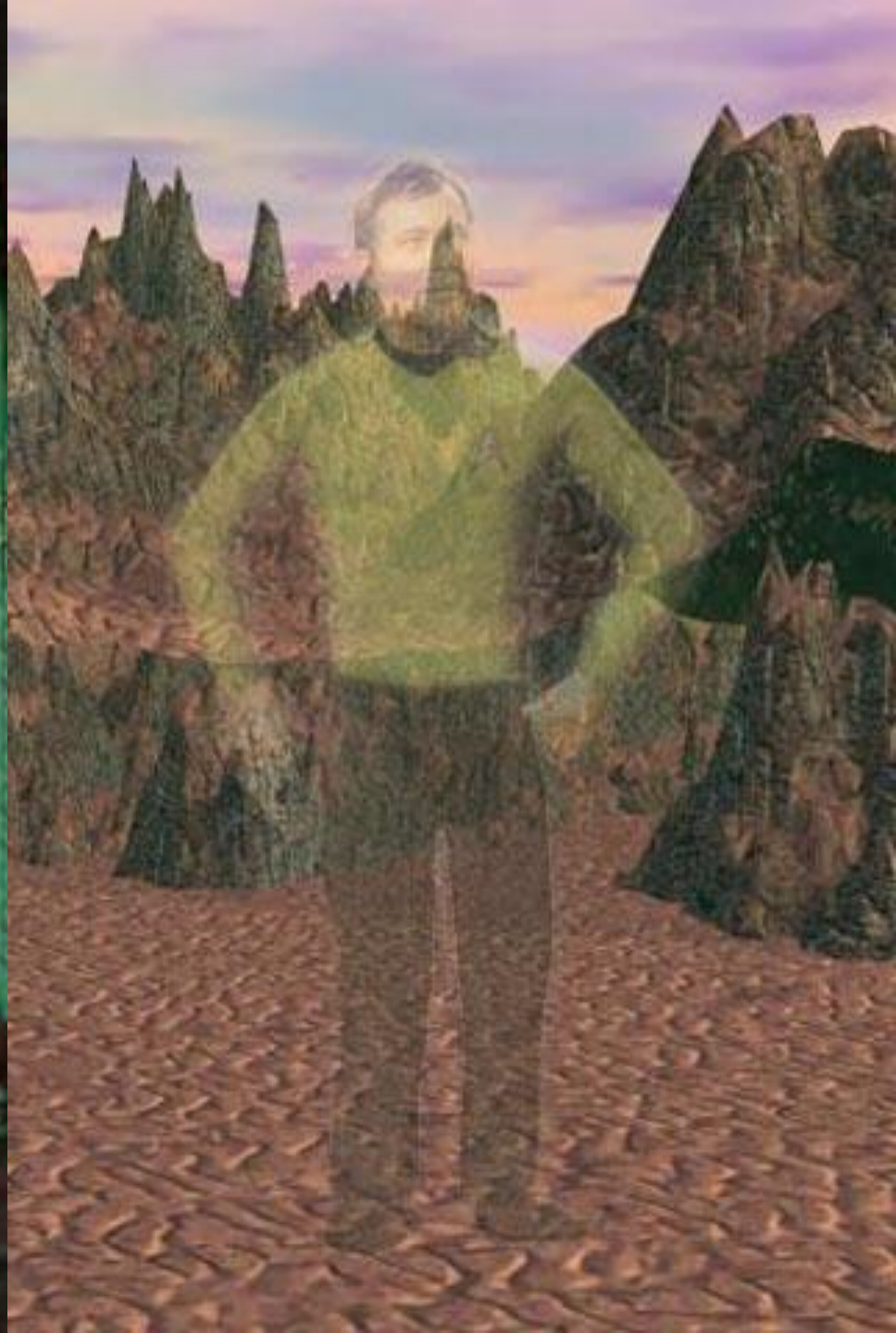


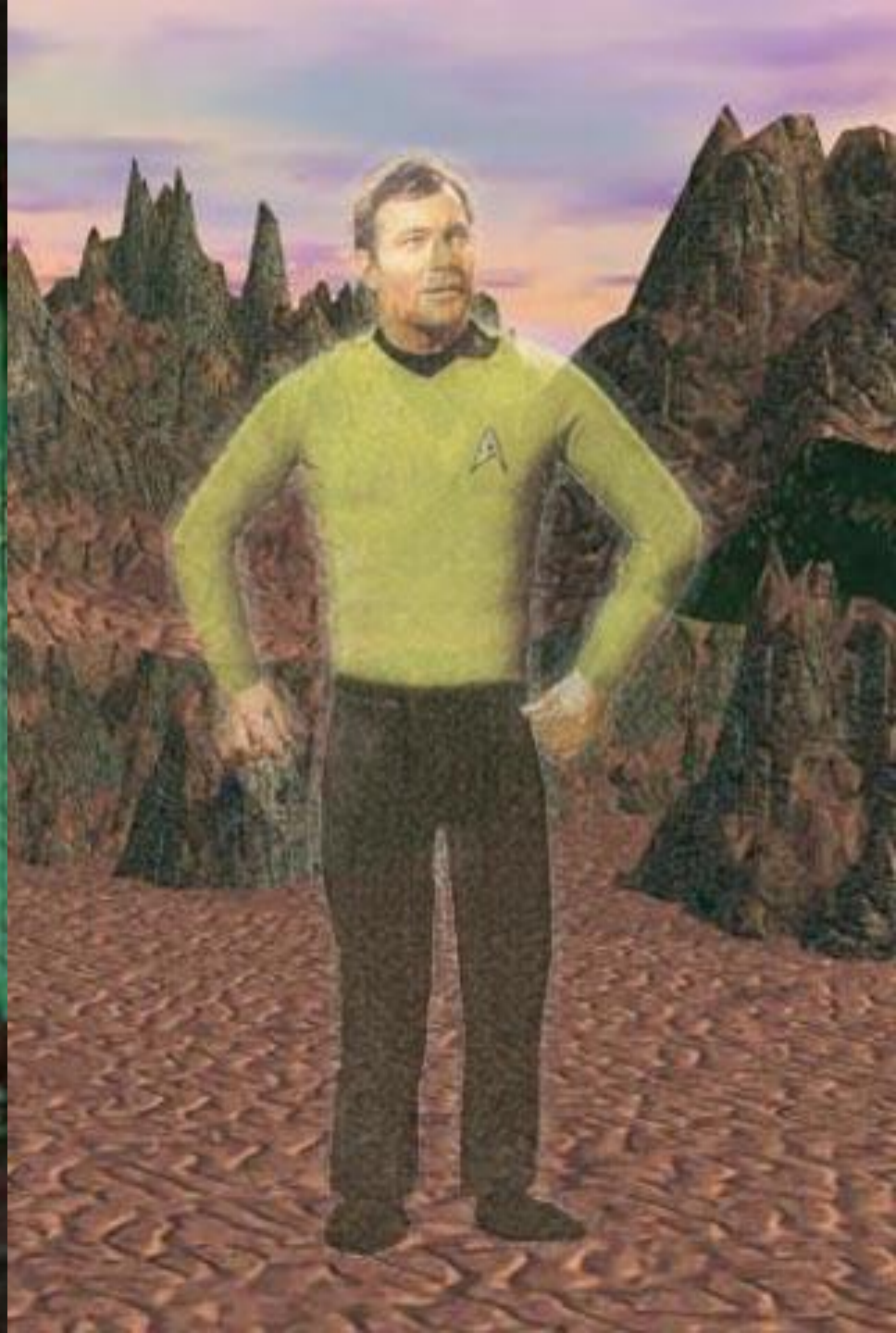
NMR apparatus used in quantum computation

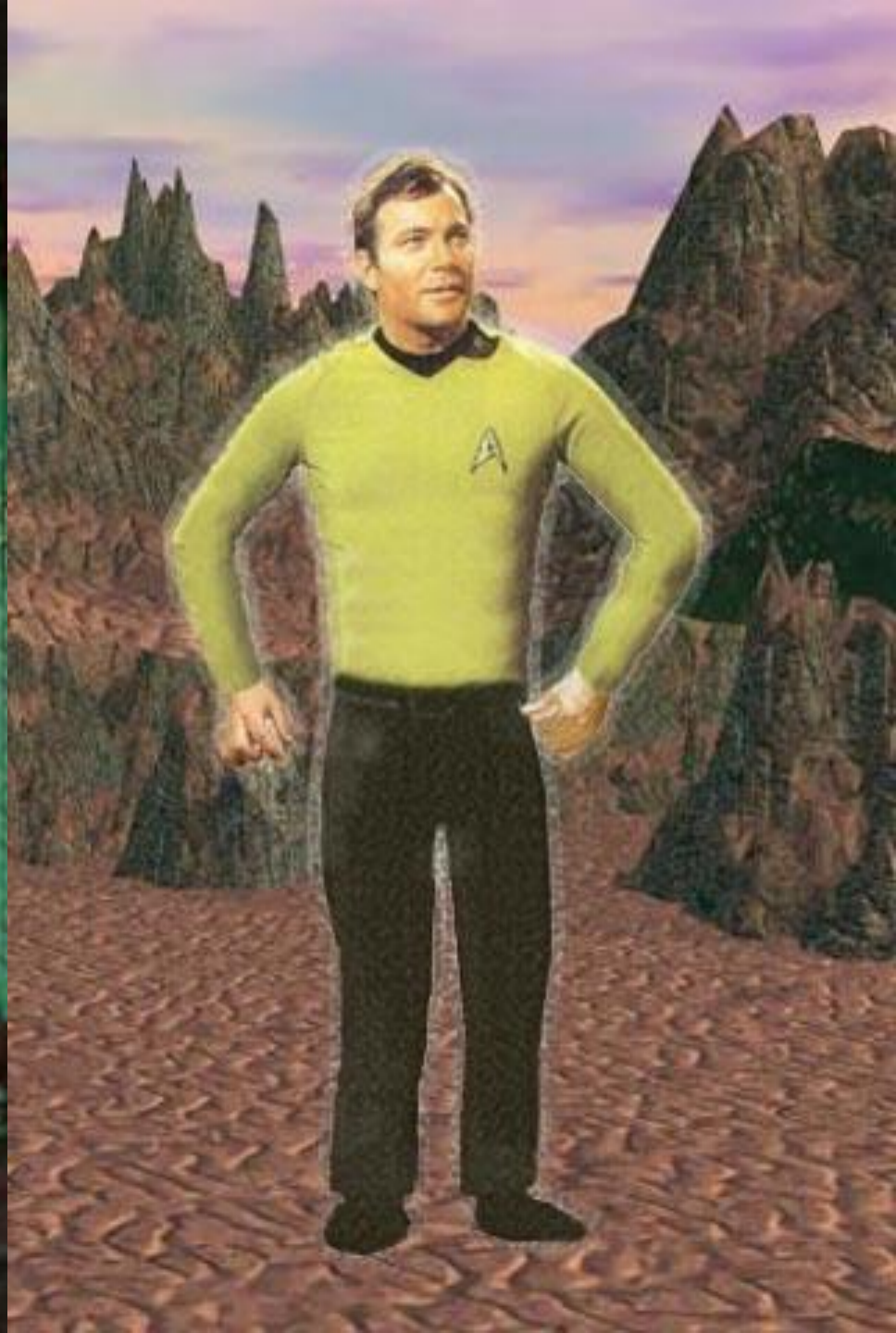
University of Oxford

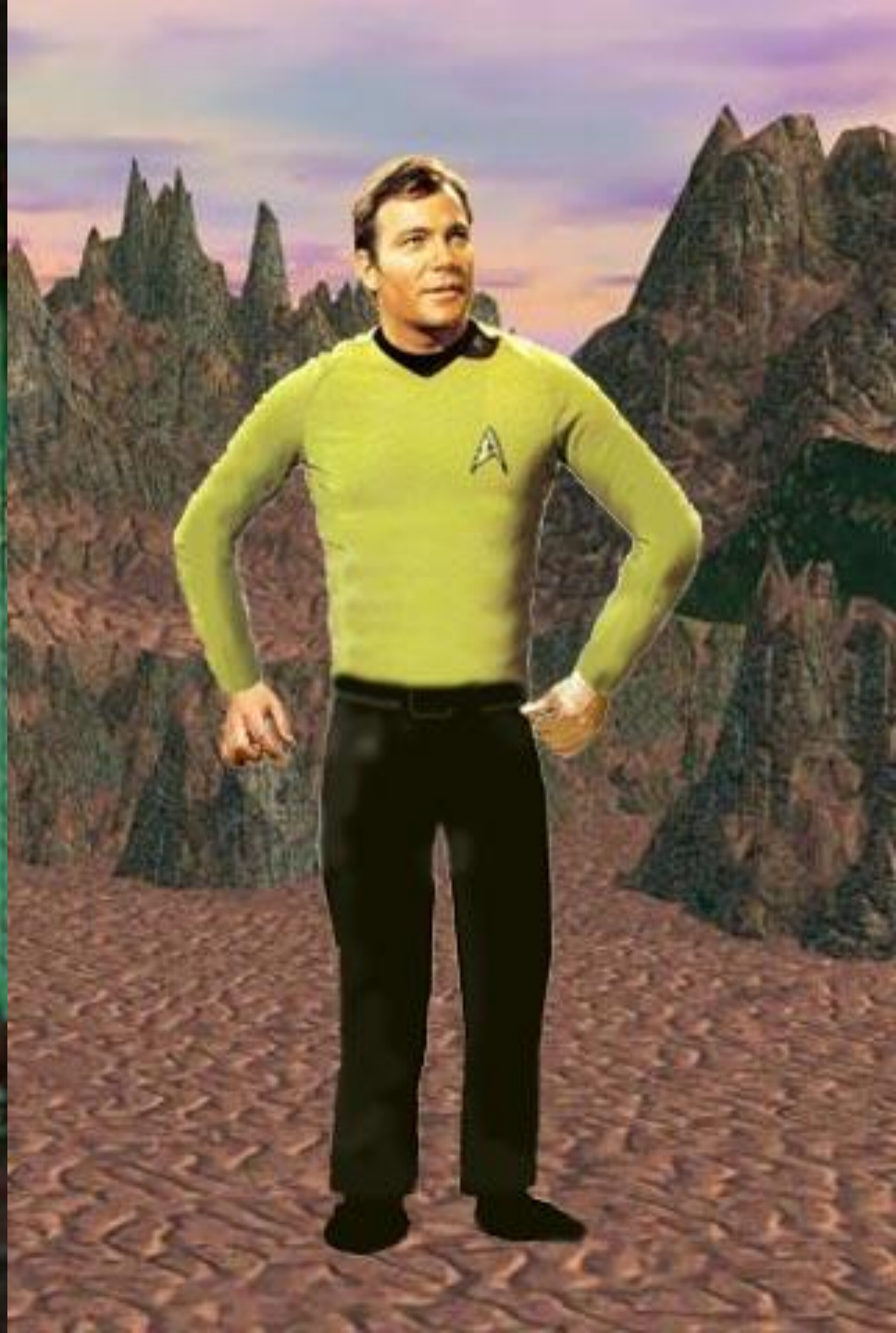
1997

Quantum Teleportation









Properties of Teleportation

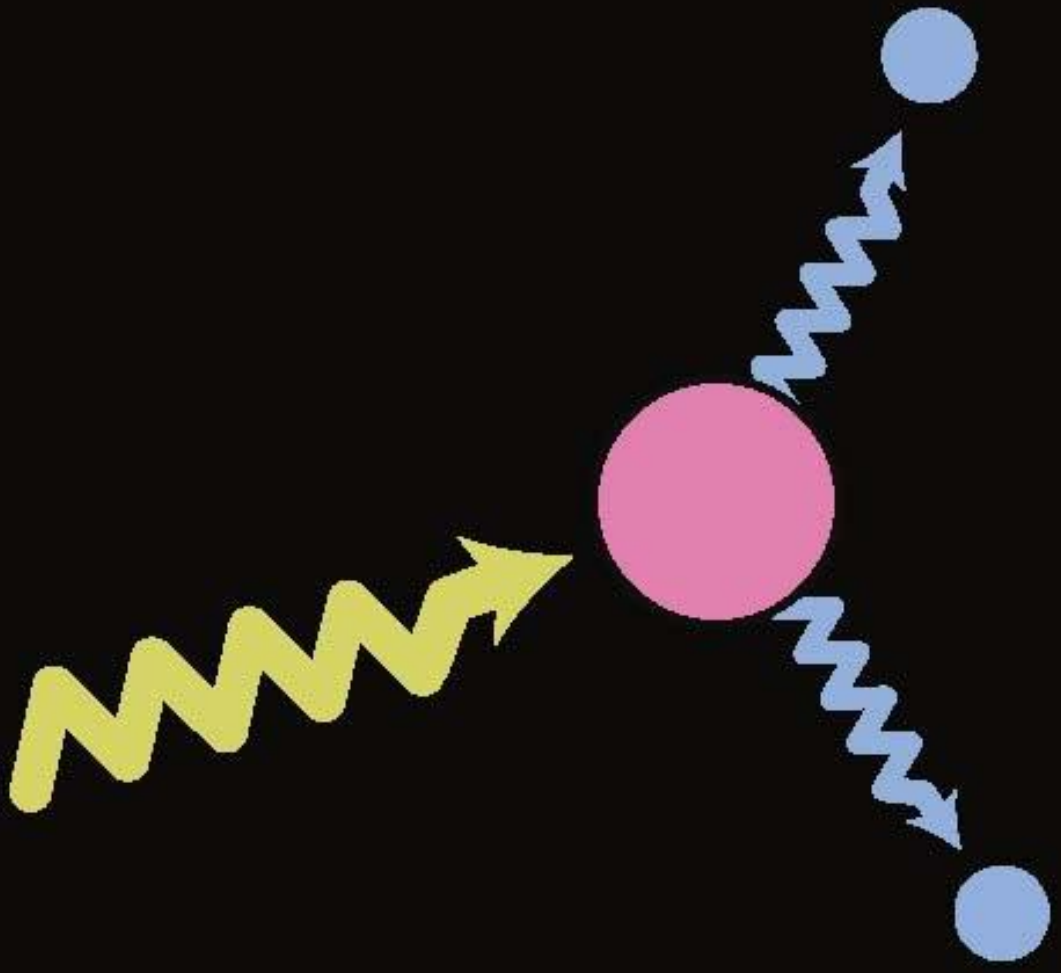
1. Kirk's molecules are not physically transported.

   Rather, new molecules are assembled at the destination according to transmitted instructions.

2. The new copy of Kirk is indistinguishable from the original.

3. The original Kirk is expended in the process.

EPR Pairs of Particles



Einstein, Podolsky & Rosen (1935)

An EPR Pair of Electrions

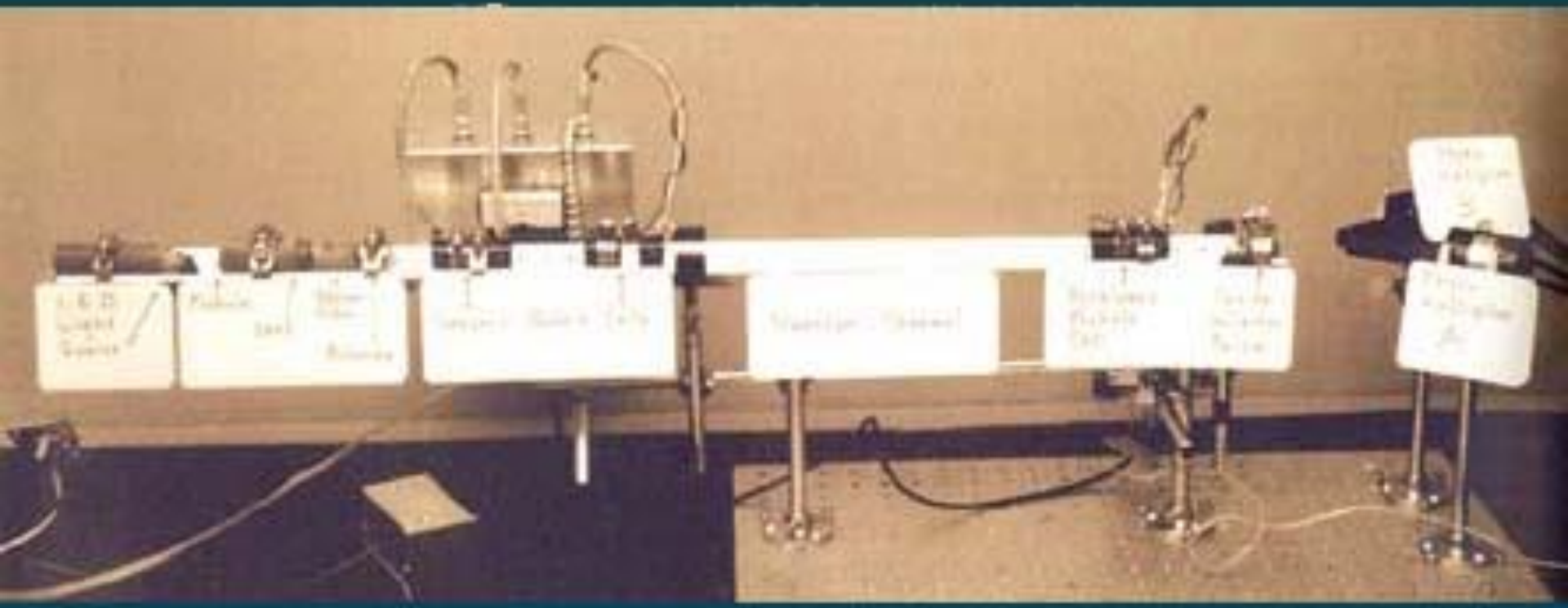
$$\text{State} = |\psi\rangle = \frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle$$

The two electrons are *entangled:* even if they are light years apart, both electrons, if measured, will be found to have the same spin.

Shared EPR pairs of electrons are a resource for teleporting quantum information.

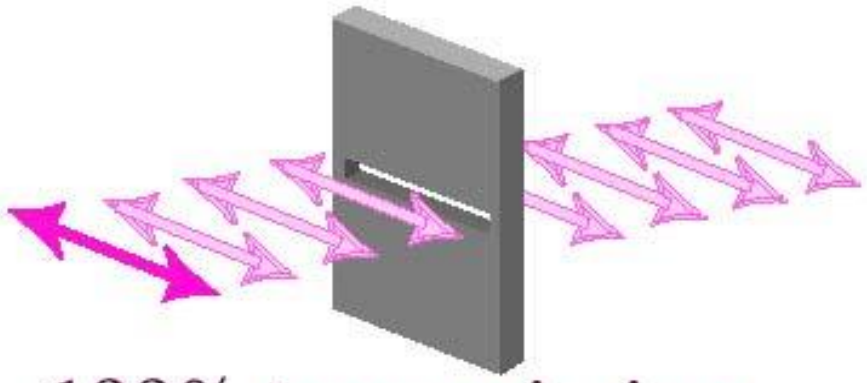
Quantum Cryptography

Apparatus of the First Quantum Cryptographic Experiment

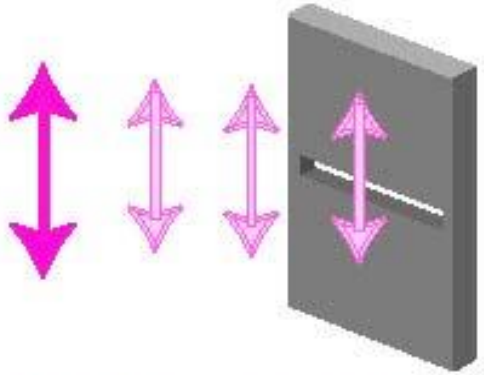


C. Bennett, G. Brassard, J. Smolin (1989)

Polarized Light passing through Polarized Filter

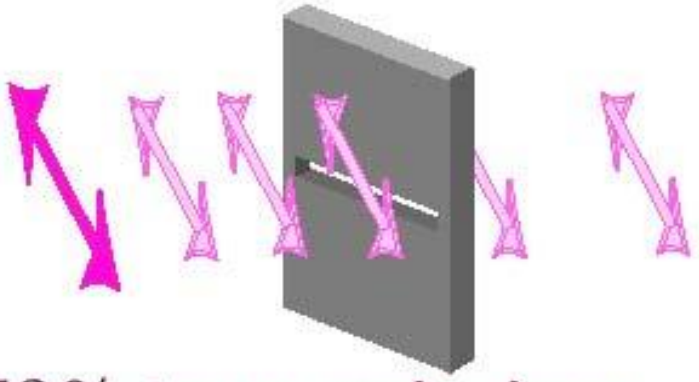


100% transmission



0% transmission

50% transmission



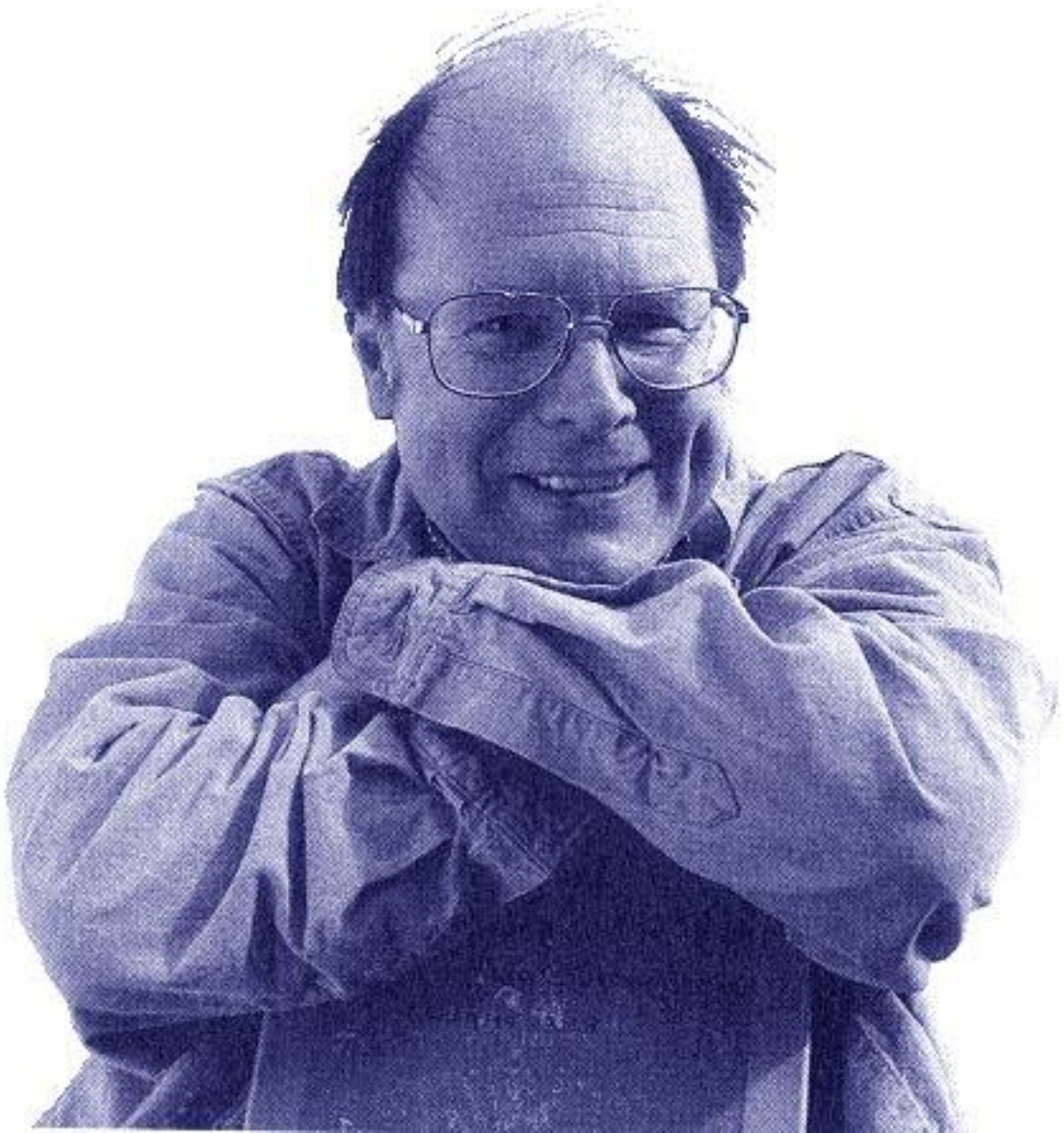
50% transmission

Quantum Money

Stephen Wiesner's Quantum Money (late 1960's)

20 trapped polarized photons

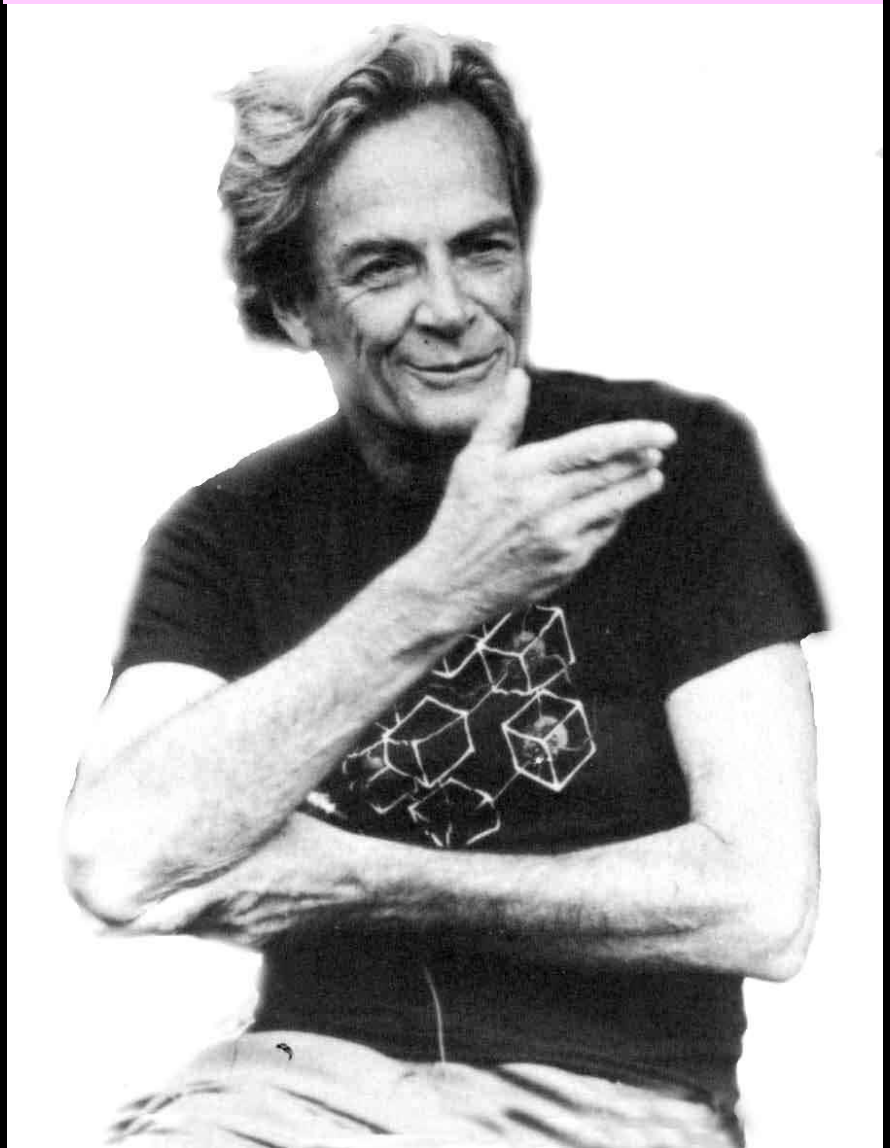
Charles Bennett



David Deutsch

Richard Feynman

1918–88



Initially, concerns were raised that the effects of decoherence would present an insurmountable obstacle to useful quantum computation.

Palma, Suominen and Ekert, *Quantum computers and dissipation*, 1996.

Unruh, *Maintaining coherence in quantum computers*, 1995.

Initially, concerns were raised that the effects of decoherence would present an insurmountable obstacle to useful quantum computation.

Palma, Suominen and Ekert, *Quantum computers and dissipation*, 1996.
Unruh, *Maintaining coherence in quantum computers*, 1995.

Later studies showed how quantum codes could protect quantum computation from the effects of decoherence.

Calderbank and Shor, *Good quantum error-correcting codes exist*, 1996.

References

Lo, Popescu and Spiller, *Introduction to Quantum Computation and Information*, 1998.

Shor, *Quantum computing*, 1998.
http://www.research.att.com/~shor/papers/ICM.pdf

RSA
Public Key
Cryptography

Alice privately chooses two large primes $p \neq q$ and two large integers d, e such that $de \bmod (p-1)(q-1)$ is 1.

She publishes the pair (n, e) as her public key, where $n = pq$.

Bob encrypts the message m $(1 < m < n)$ as $m' = m^e \bmod n$, which he sends to Alice.

To decrypt the message m', Alice computes $(m')^d \bmod n$, which equals the original message m.

Security of the System

Alice's private key d cannot be determined without a knowledge of the factorisation of n. Without this information, it is presumably infeasible to recover the original message m given the encrypted message m'.

Example

Alice chooses

$p = 99103,\ q = 80177$

$d = 5144067831,\ e = 2968833449$

so

$$(p-1)(q-1) = 7945601952$$

and

$$de \bmod 7945601952 \text{ is } 1.$$

(e is determined from d by Euclid's Algorithm.)

She publishes

$n = pq = 7945781231$ and $e = 2968833449$.

Encryption

Using blank=00, A=01, B=02, . . . , Z=26
we translate

Bob's message:	S E N D	M O N E Y
Translation:	19 05 14 04 00	13 15 14 05 25

Encryption

Original message

Encrypted message

$$1905140400^{e} \bmod n = 6151146242$$

$$1315140525^{e} \bmod n = 7738879657$$

Decryption

$$6151146242^{d} \bmod n = 1905140400$$

$$7738879657^{d} \bmod n = 1315140525$$

Encrypted message

Decrypted message

Quantum Teleportation

An EPR Pair of Electrions

$$\text{State} = |\psi\rangle = \frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle$$

The two electrons are *entangled:* even if they are light years apart, both electrons, if measured, will be found to have the same spin.

Shared EPR pairs of electrons are a resource for teleporting quantum information.

Bell Basis

The state of any pair of electrons is expressible as

$$\alpha_{00}|00\rangle + \alpha_{01}|01\rangle + \alpha_{10}|10\rangle + \alpha_{11}|11\rangle$$

where $\sum |\alpha_{jk}|^2 = 1$, *or* as

$$\beta_1|B_1\rangle + \beta_2|B_2\rangle + \beta_3|B_3\rangle + \beta_4|B_4\rangle$$

in terms of the basis

$$|B_1\rangle = \tfrac{1}{\sqrt{2}}\big(|00\rangle + |11\rangle\big), \qquad |B_2\rangle = \tfrac{1}{\sqrt{2}}\big(|00\rangle - |11\rangle\big),$$

$$|B_3\rangle = \tfrac{1}{\sqrt{2}}\big(|01\rangle + |10\rangle\big), \qquad |B_4\rangle = \tfrac{1}{\sqrt{2}}\big(|01\rangle - |10\rangle\big)$$

Quantum Teleportation

Two distant parties (Alice and Bob) share an EPR pair of electrons (2 and 3). Alice wants to teleport electron 1 (in unknown state $\alpha|0\rangle + \beta|1\rangle$) to Bob.

The complete state of the three electrons is

$$\big(\alpha|0\rangle + \beta|1\rangle\big) \otimes \tfrac{1}{\sqrt{2}}\big(|00\rangle + |11\rangle\big)$$

$$= \tfrac{1}{\sqrt{2}}\big(\alpha|000\rangle + \alpha|011\rangle + \beta|100\rangle + \beta|111\rangle\big)$$

$$= \tfrac{1}{2}|B_1\rangle \otimes \big(\alpha|0\rangle + \beta|1\rangle\big)$$

$$+ \tfrac{1}{2}|B_2\rangle \otimes \big(\alpha|0\rangle - \beta|1\rangle\big)$$

$$+ \tfrac{1}{2}|B_3\rangle \otimes \big(\beta|0\rangle + \alpha|1\rangle\big)$$

$$+ \tfrac{1}{2}|B_4\rangle \otimes \big(-\beta|0\rangle + \alpha|1\rangle\big)$$

Alice measures her pair of electrons (1 and 2) relative to the Bell basis, observing the pair to be in one of the four states B_1, B_2, B_3 or B_4.

She calls Bob and tells her which of the four states was observed (two bits of classical information only).

Bob applies one of the four unitary operators

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \quad \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$$

respectively to his electron (electron 3) to put it into the unknown state $\alpha|0\rangle + \beta|1\rangle$.