

The Garden-Hose Model

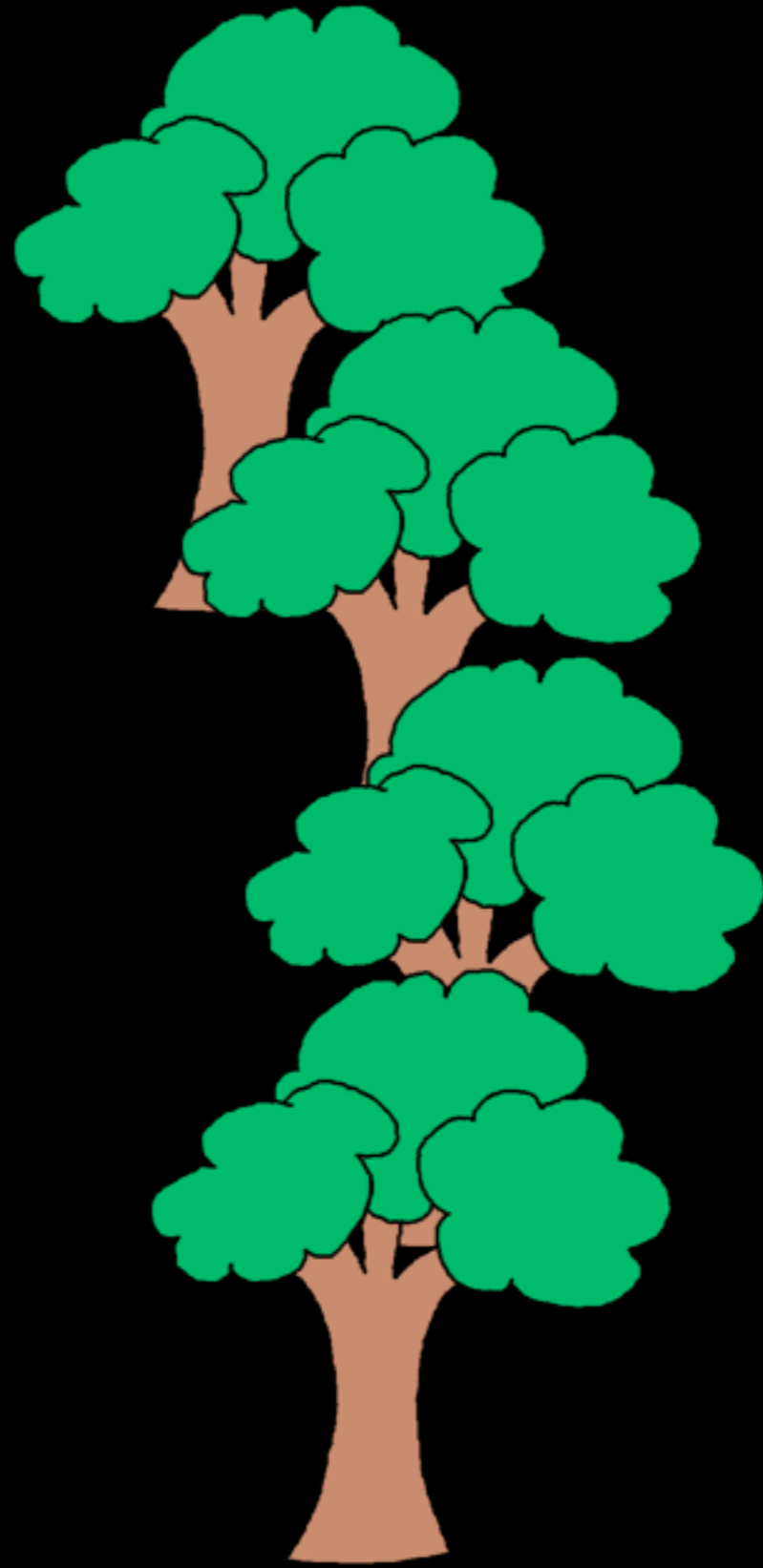
Harry Buhrman, Serge Fehr,
Christian Schaffner, Florian Speelman

The logo for CWI (Centrum voor Wiskunde en Informatica) consists of a red trapezoidal shape pointing to the right, with the letters 'CWI' in white, bold, sans-serif font inside.

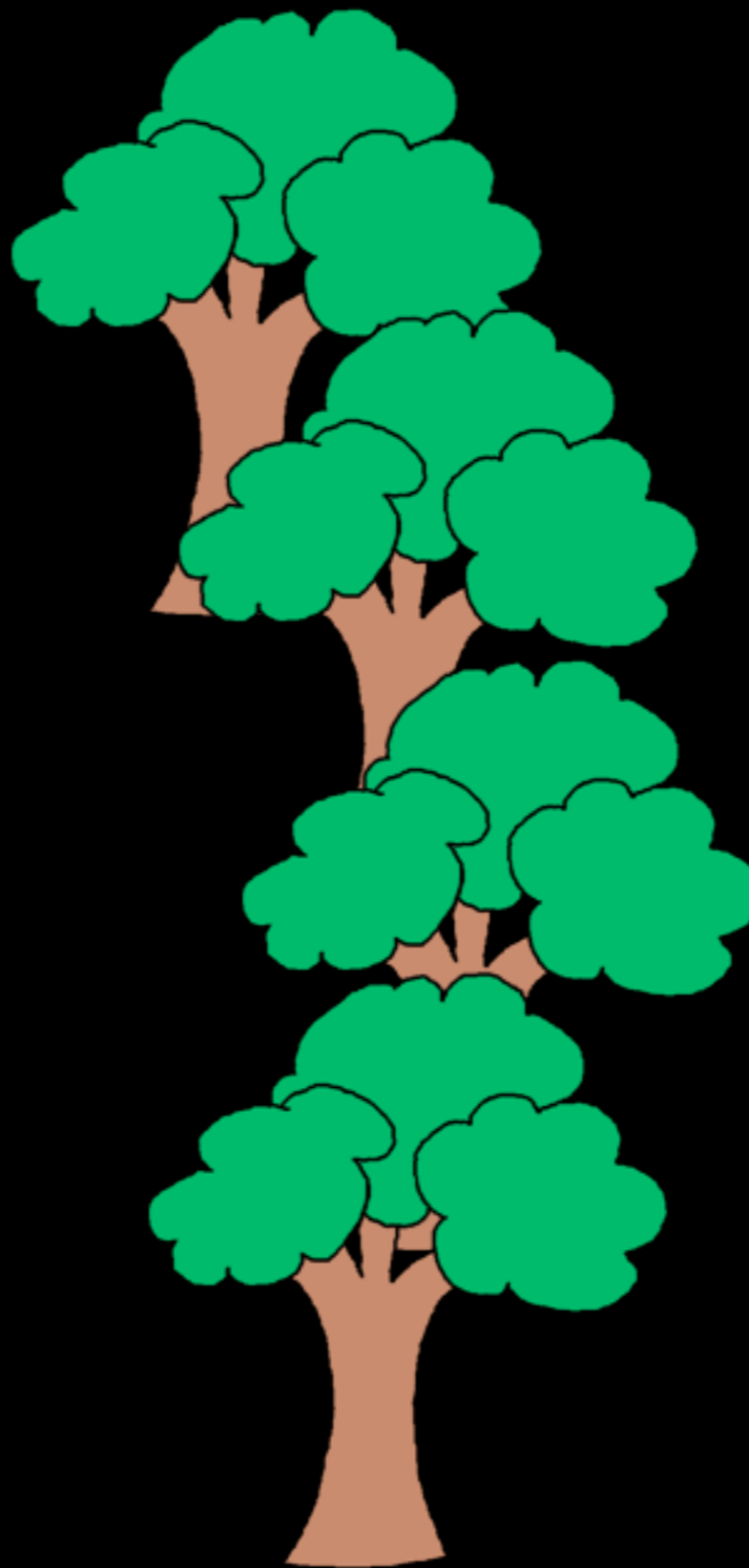
CWI







$$x \in \{0, 1\}^n$$

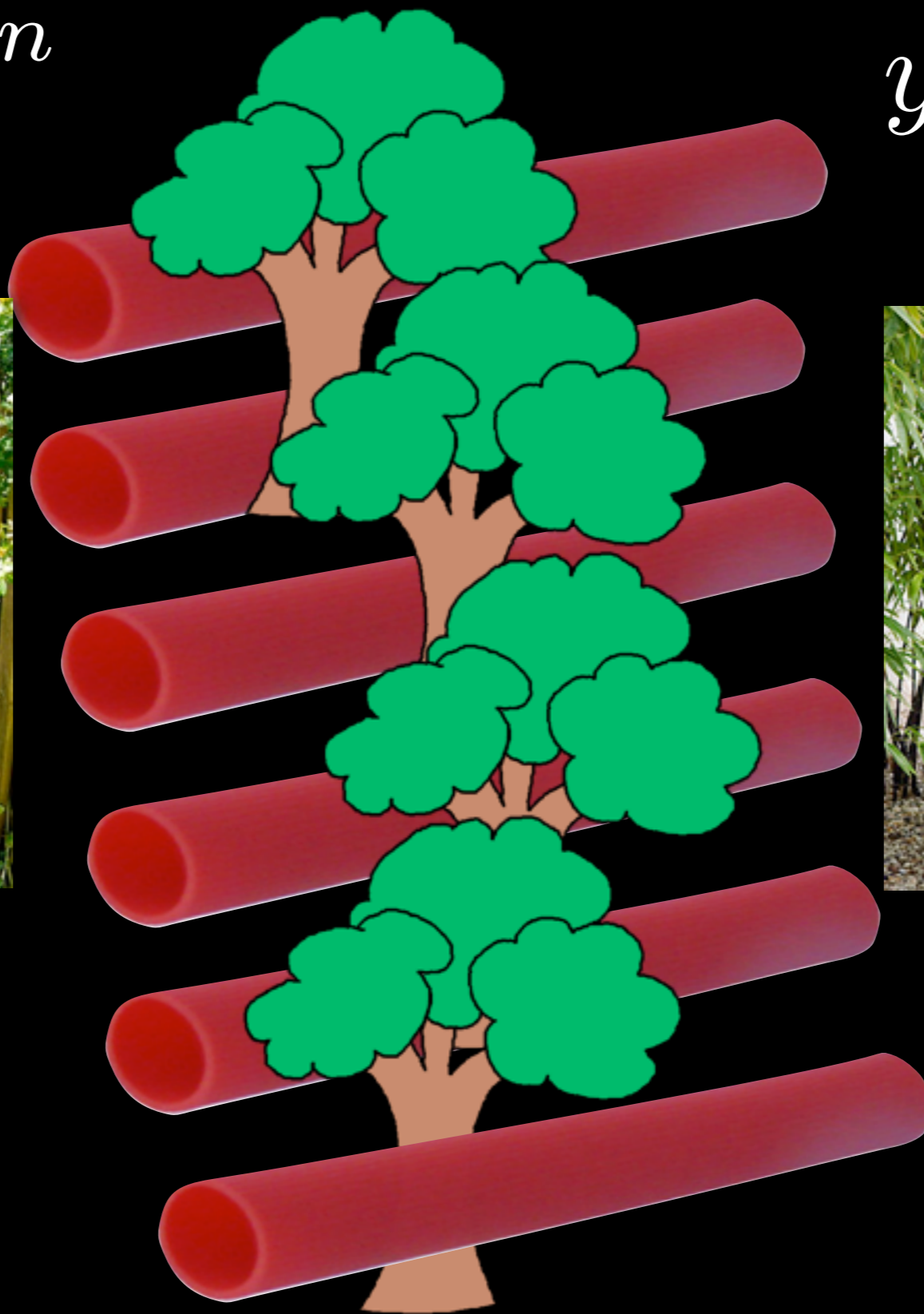


$$y \in \{0, 1\}^n$$



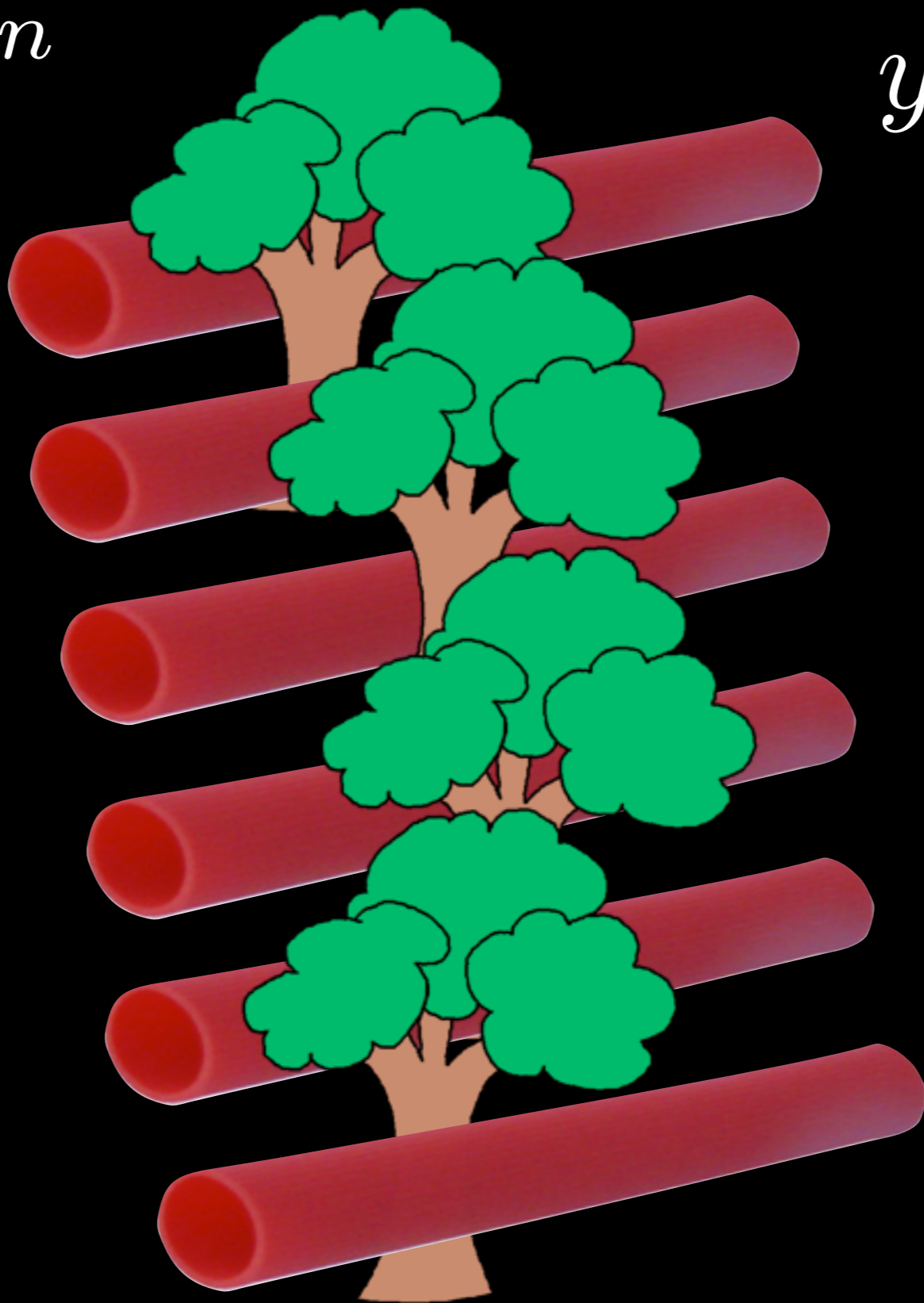
$$x \in \{0, 1\}^n$$

$$y \in \{0, 1\}^n$$



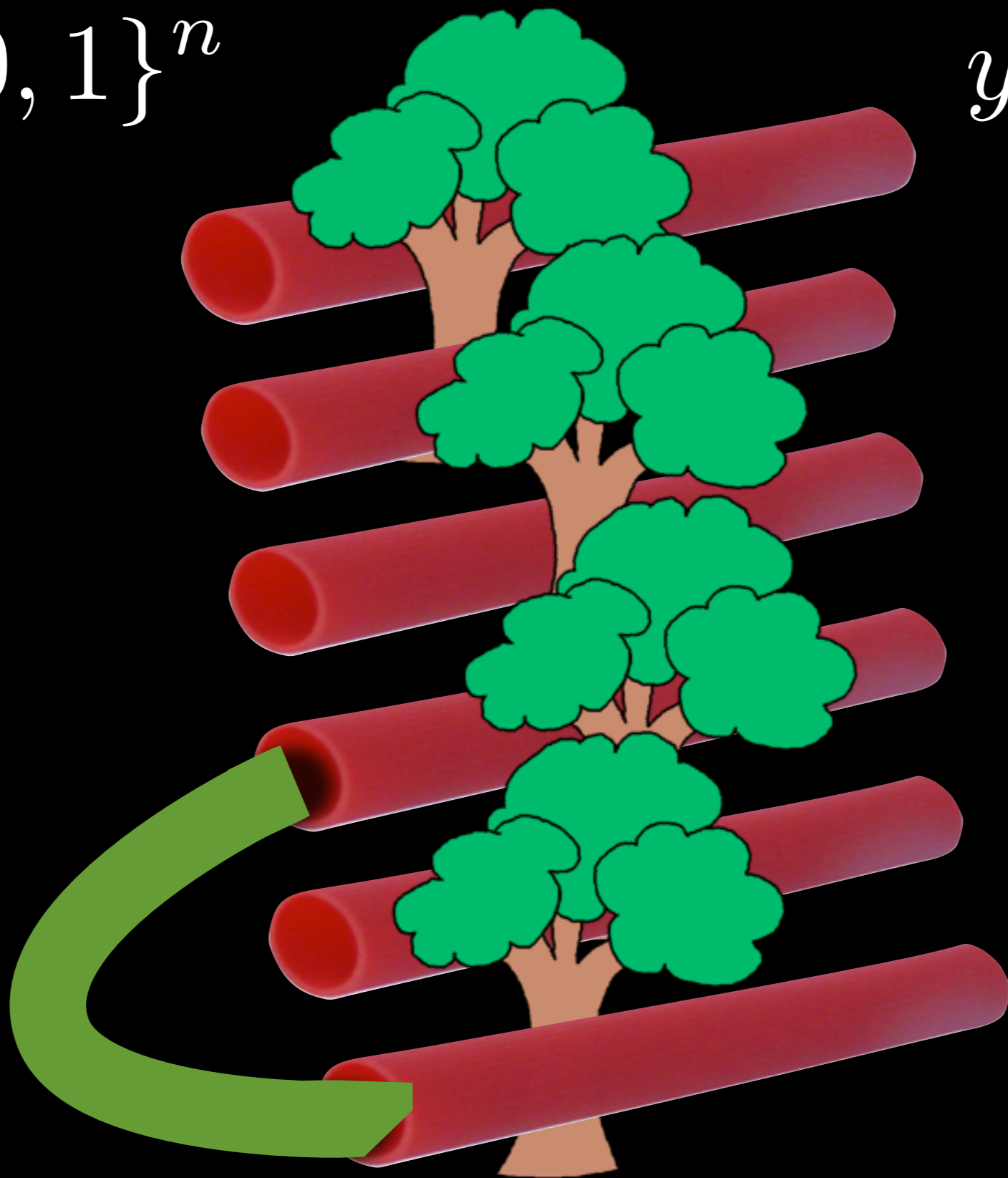
$$x \in \{0, 1\}^n$$

$$y \in \{0, 1\}^n$$



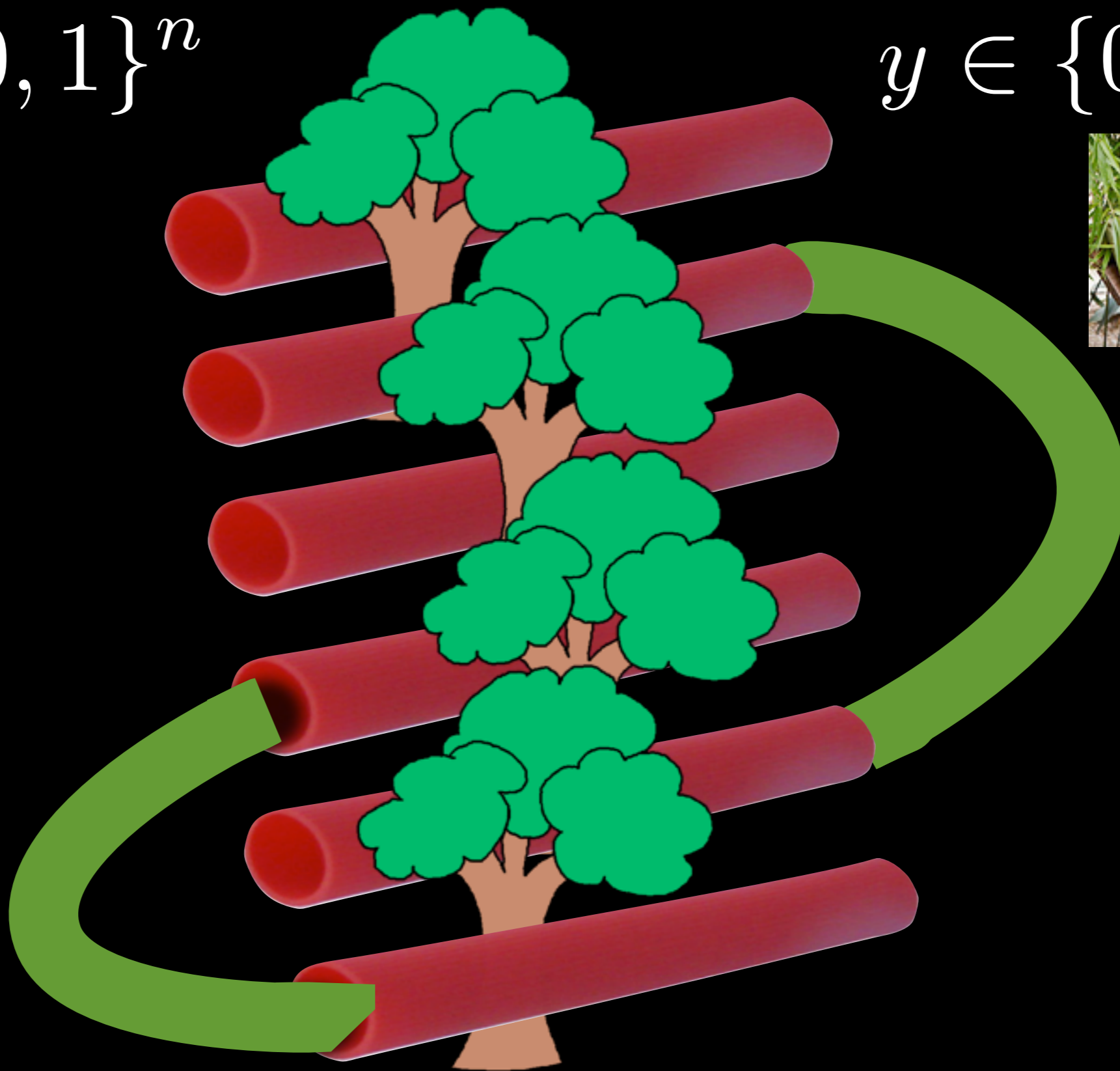
$$x \in \{0, 1\}^n$$

$$y \in \{0, 1\}^n$$



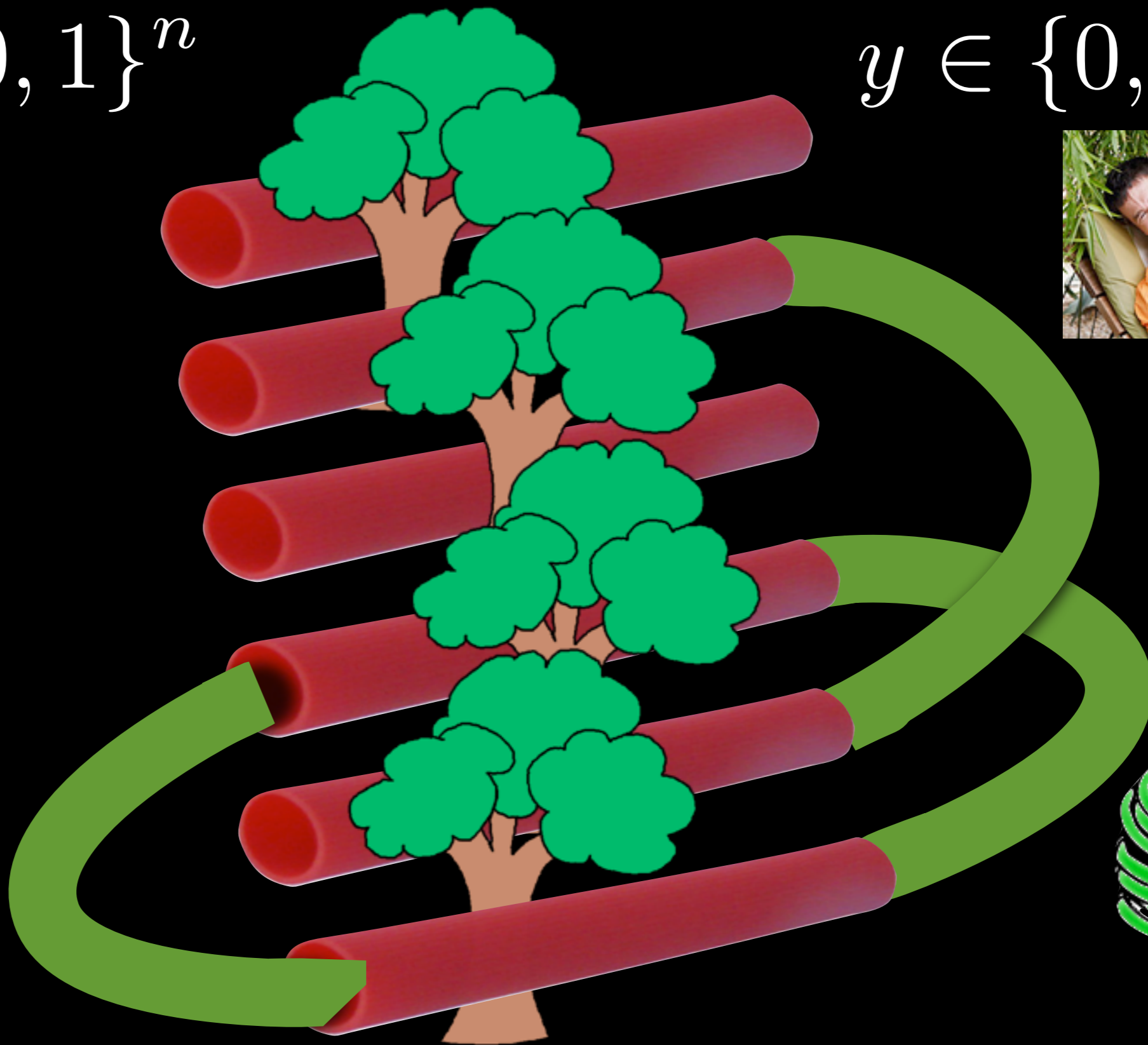
$$x \in \{0, 1\}^n$$

$$y \in \{0, 1\}^n$$



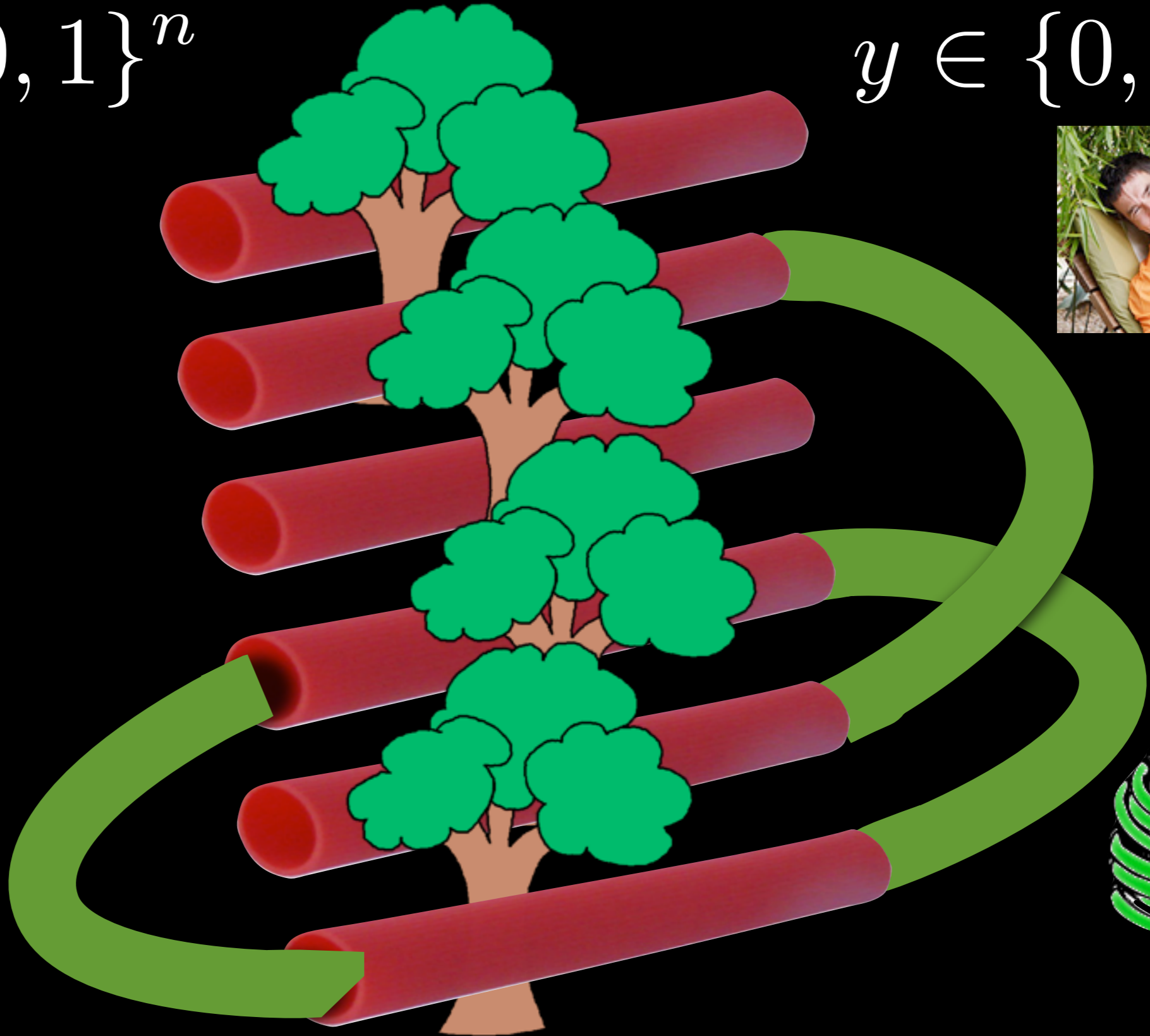
$$x \in \{0, 1\}^n$$

$$y \in \{0, 1\}^n$$



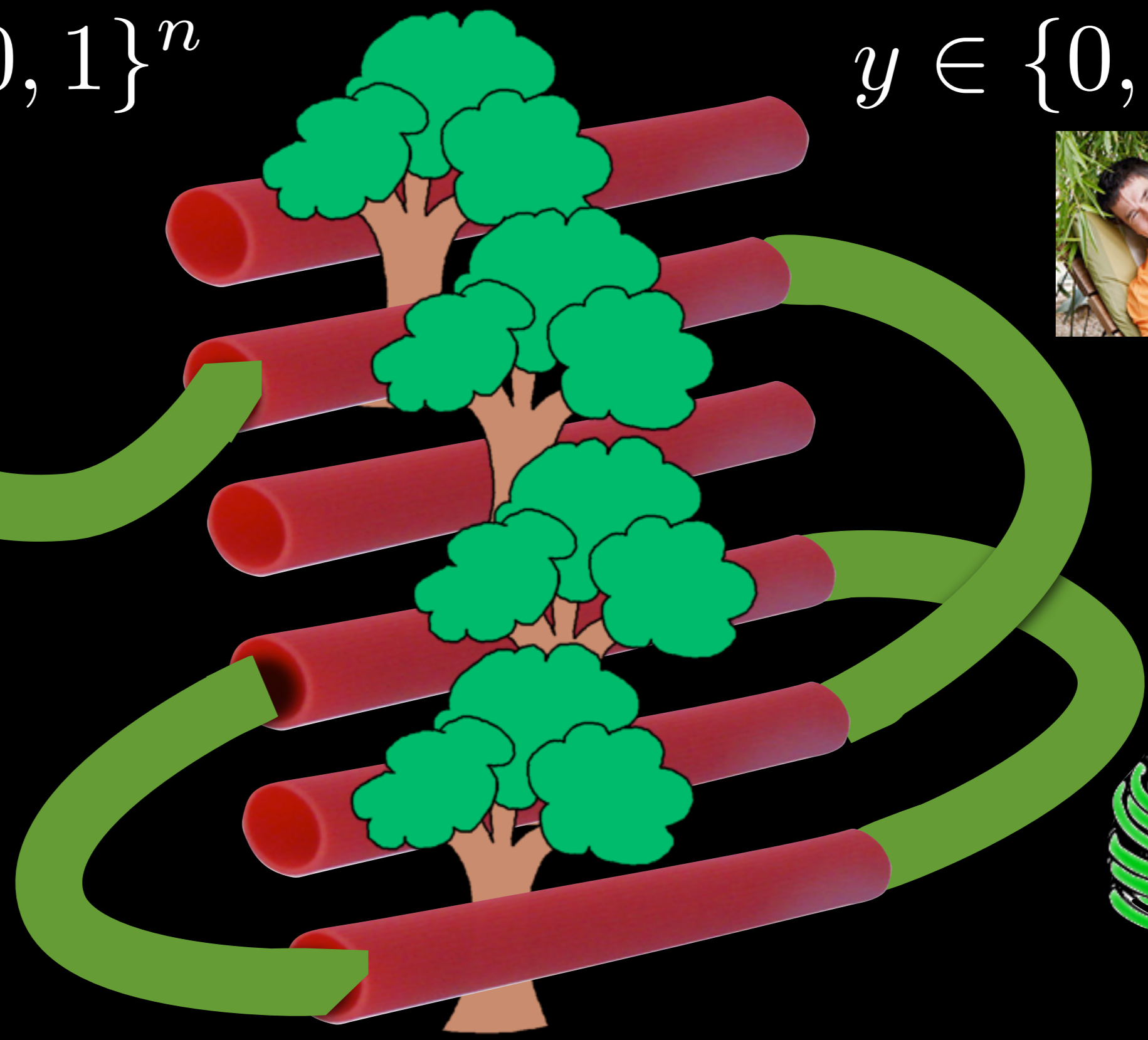
$$x \in \{0, 1\}^n$$

$$y \in \{0, 1\}^n$$



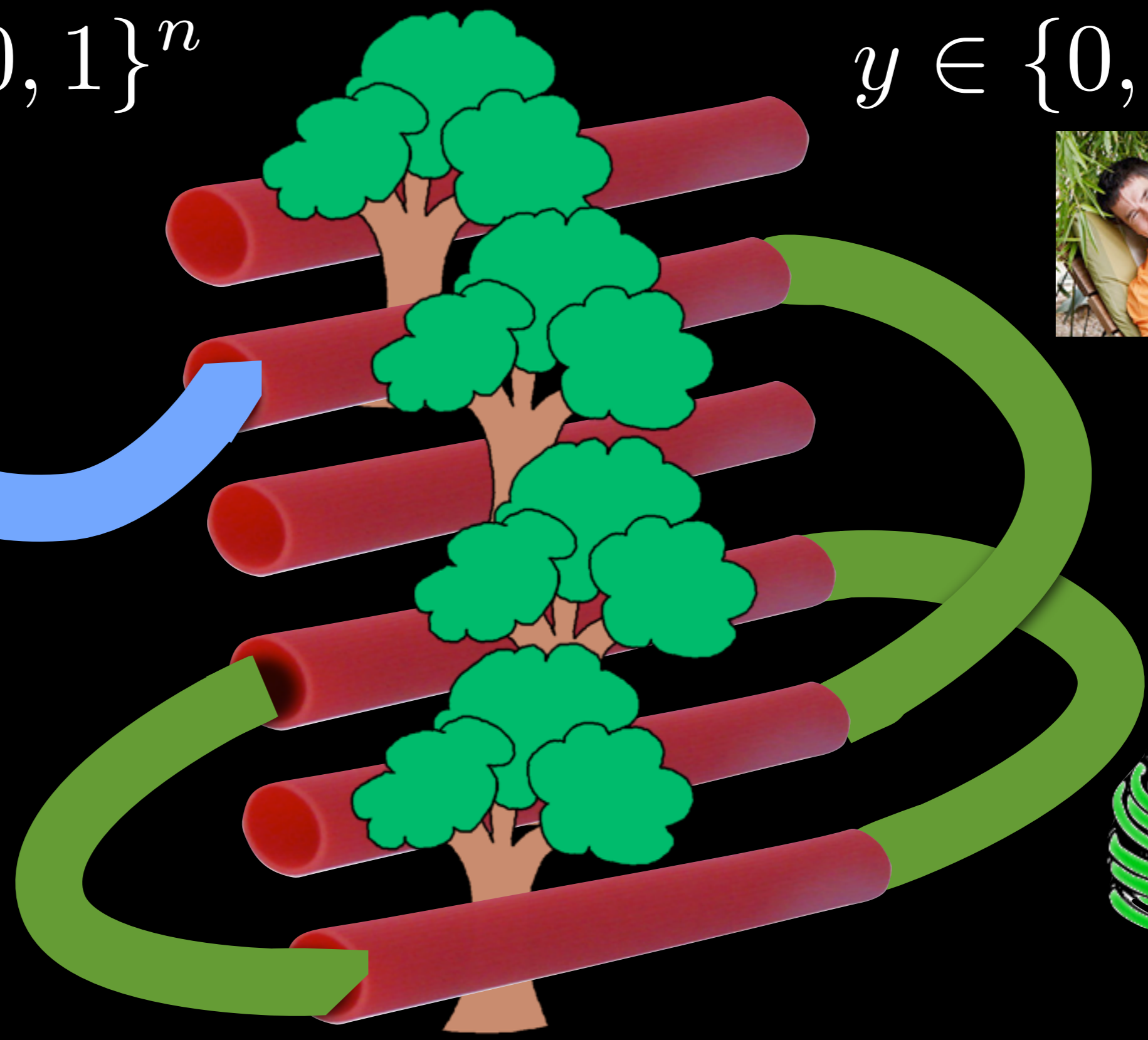
$$x \in \{0, 1\}^n$$

$$y \in \{0, 1\}^n$$



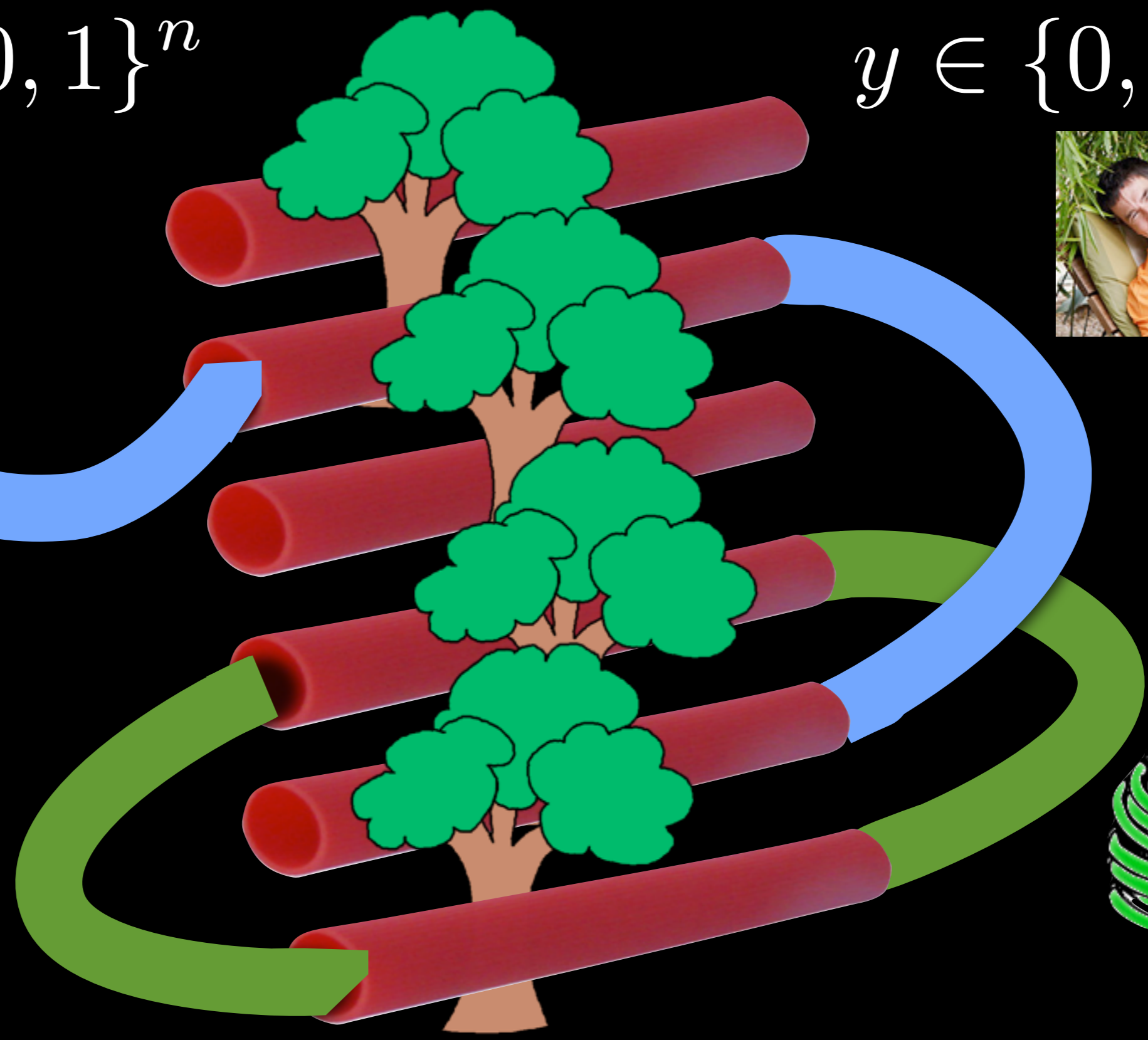
$$x \in \{0, 1\}^n$$

$$y \in \{0, 1\}^n$$



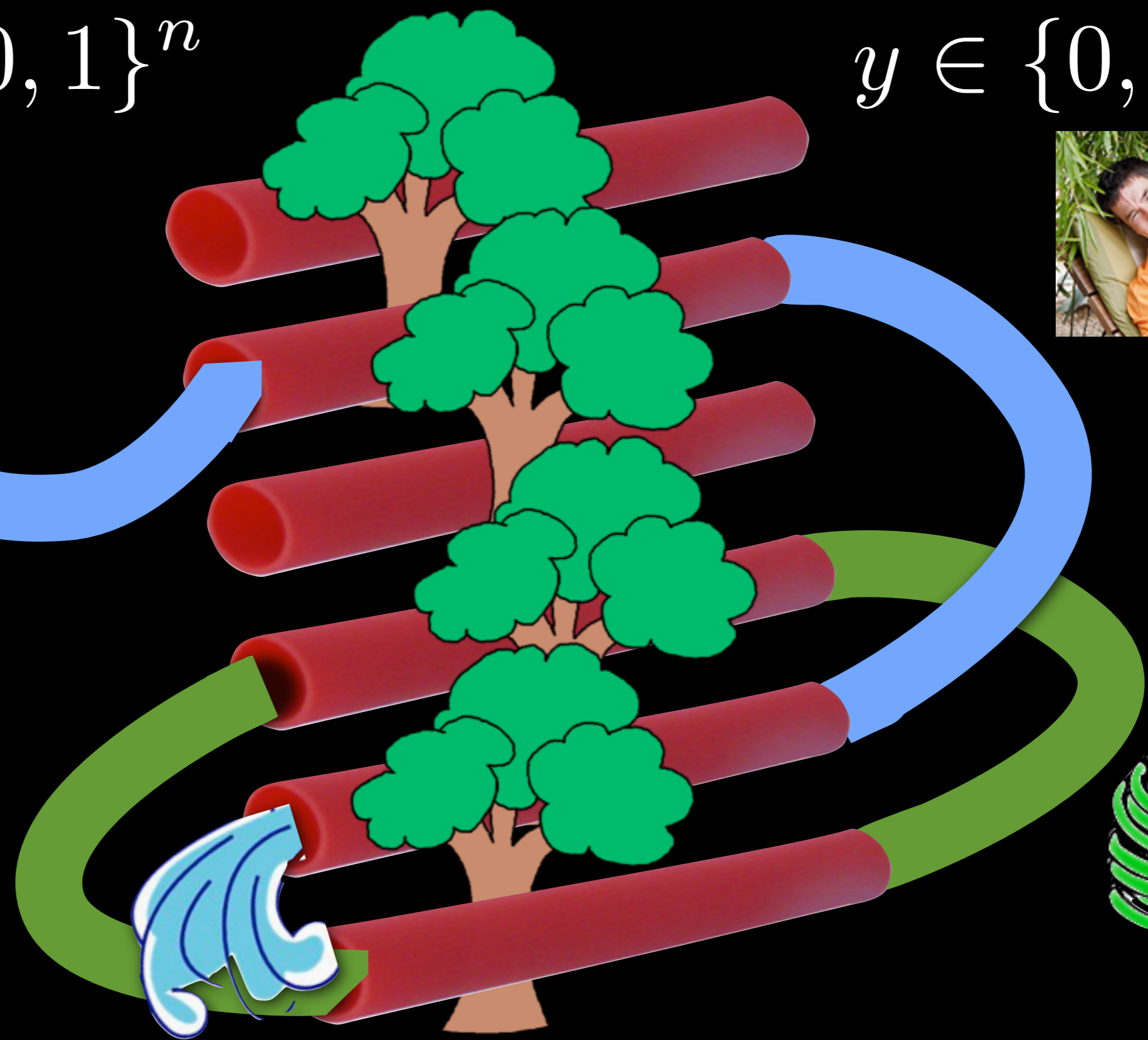
$$x \in \{0, 1\}^n$$

$$y \in \{0, 1\}^n$$



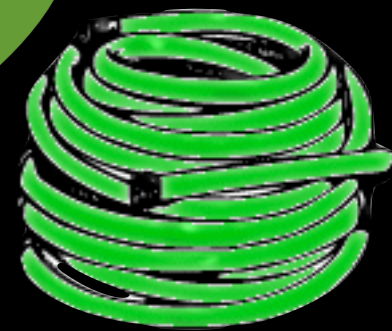
$$x \in \{0, 1\}^n$$

$$y \in \{0, 1\}^n$$

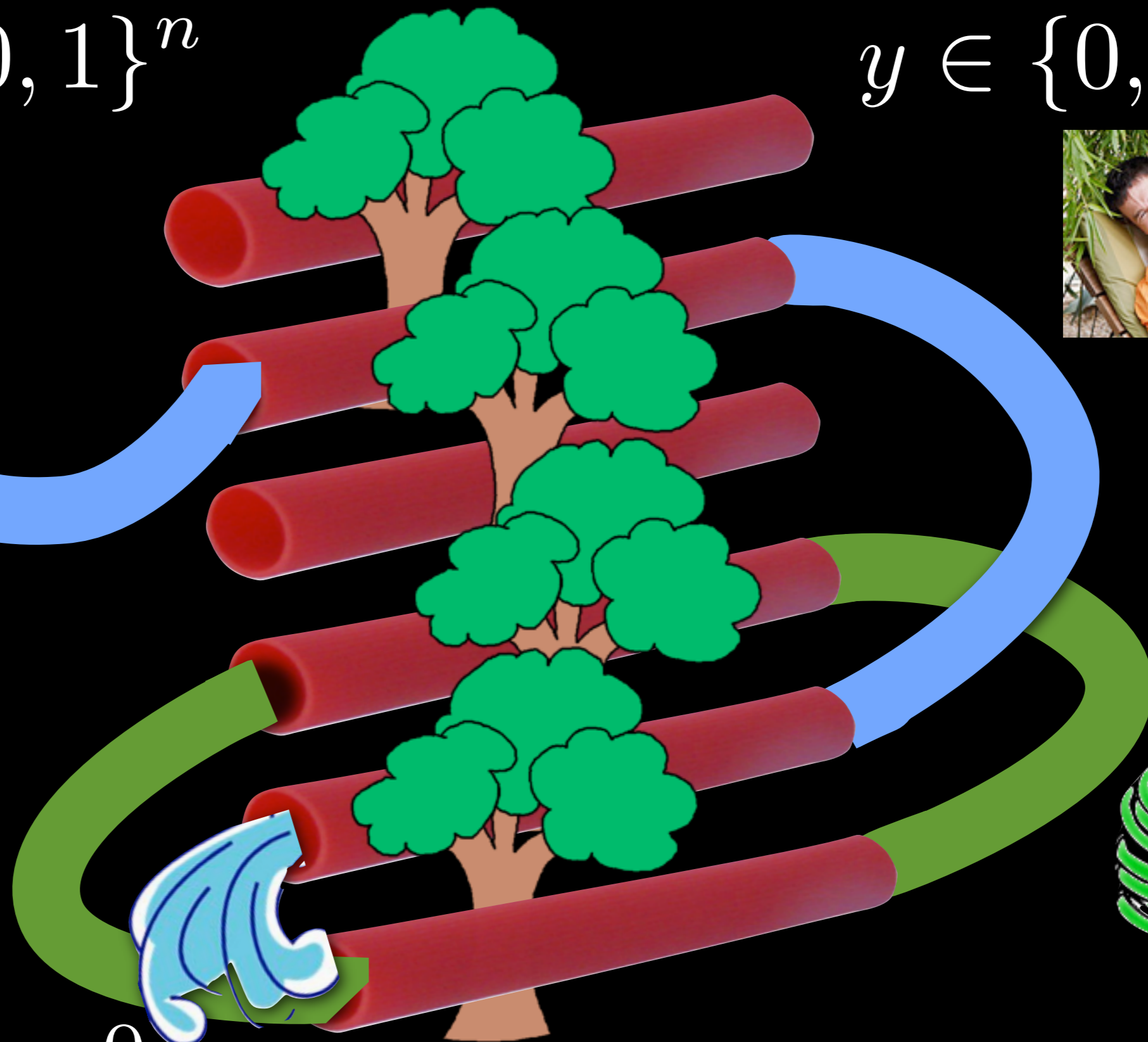


$$x \in \{0, 1\}^n$$

$$y \in \{0, 1\}^n$$



$$f(x, y) = 0$$

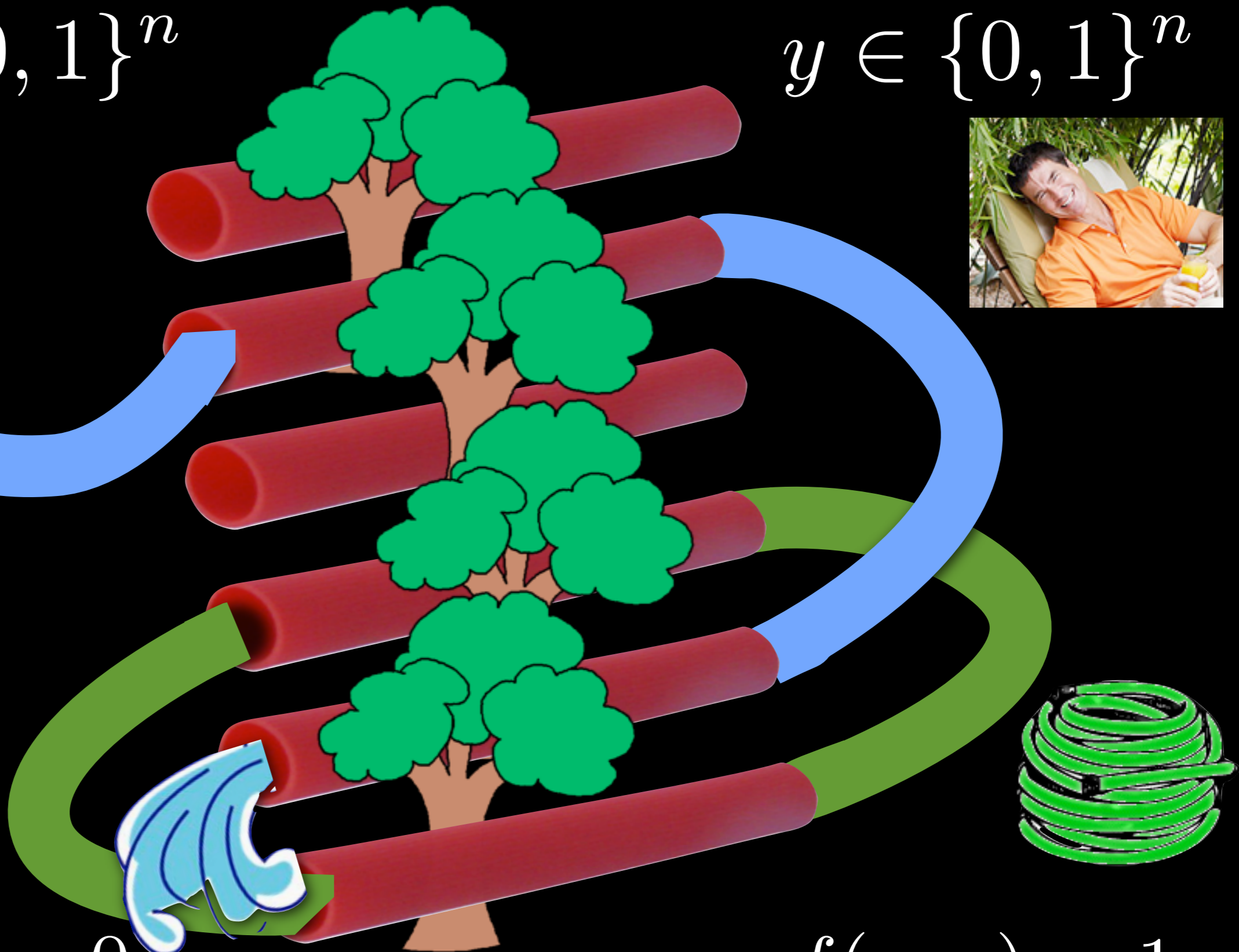


$$x \in \{0, 1\}^n$$

$$y \in \{0, 1\}^n$$



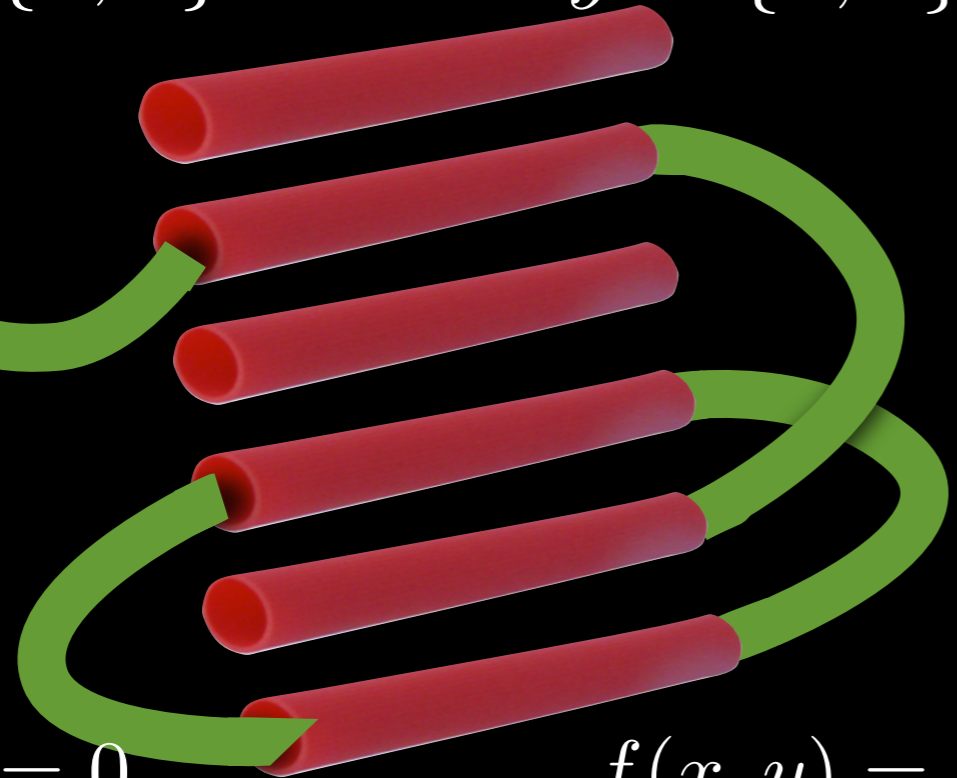
$$f(x, y) = 0$$



$$f(x, y) = 1$$

$$x \in \{0, 1\}^n$$

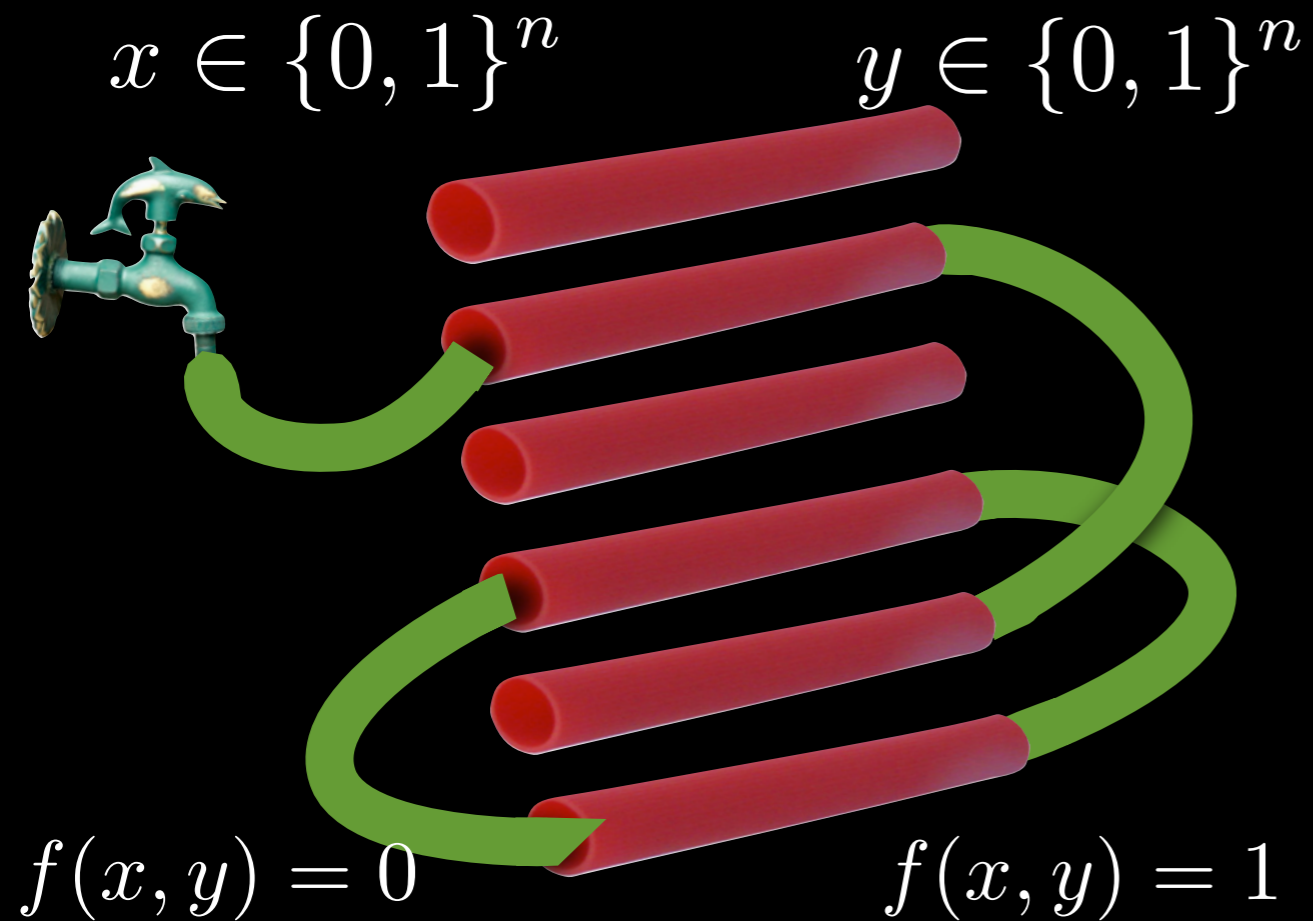
$$y \in \{0, 1\}^n$$



$$f(x, y) = 0$$

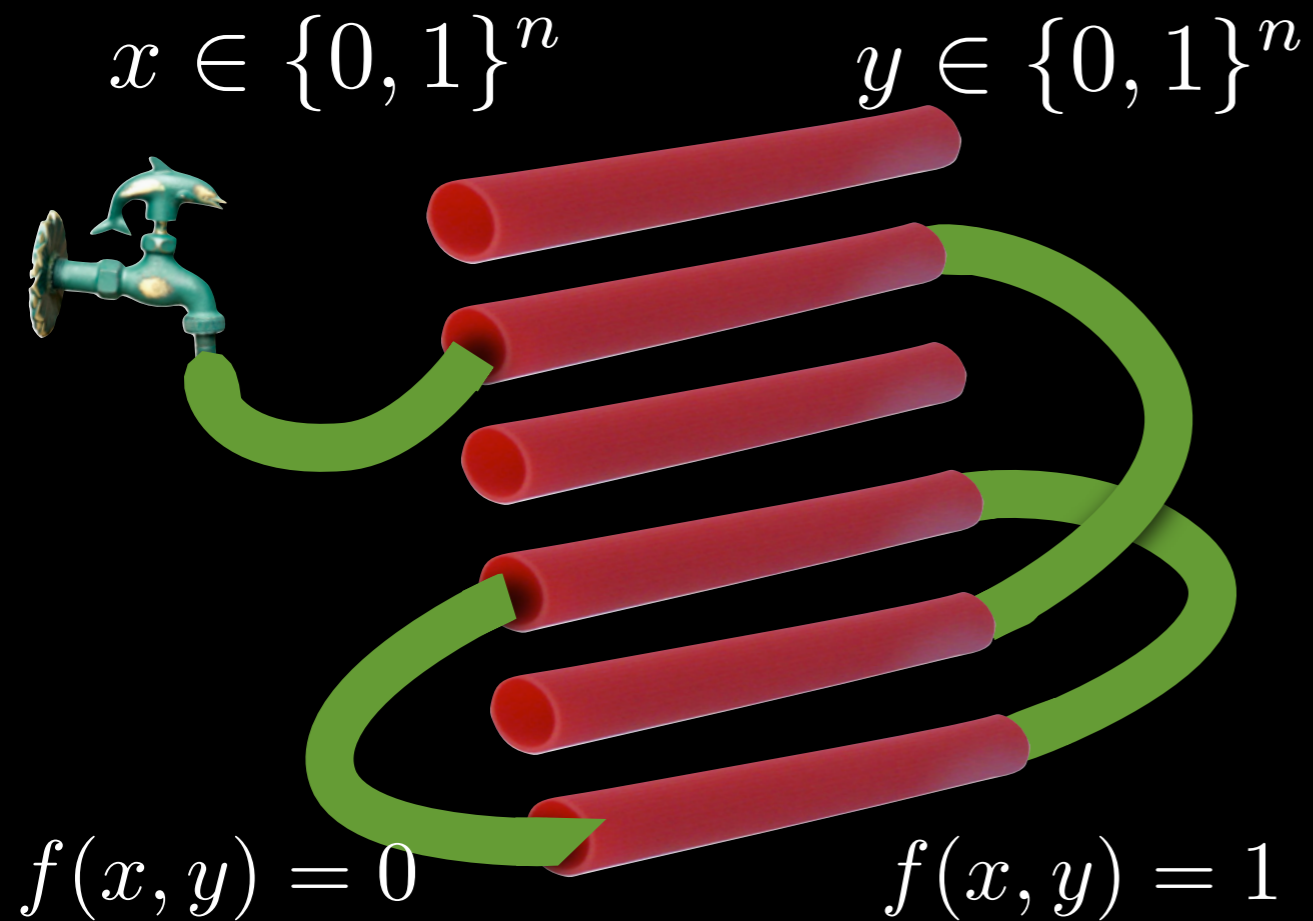
$$f(x, y) = 1$$

Computing a Boolean Function in the Garden-Hose Model



Computing a
Boolean Function in the
Garden-Hose Model

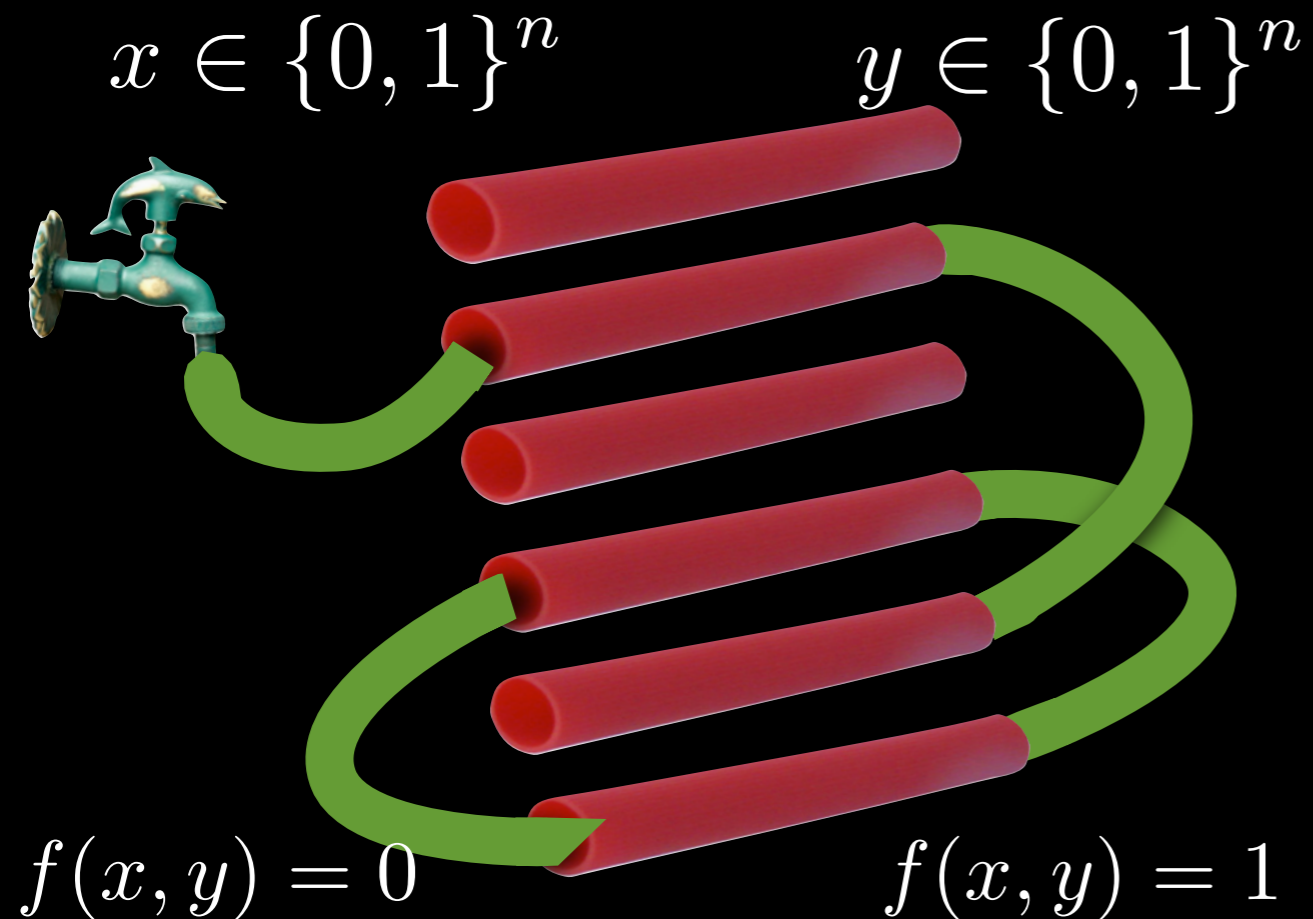
how many pipes are required?



Computing a Boolean Function in the Garden-Hose Model

how many pipes are required?

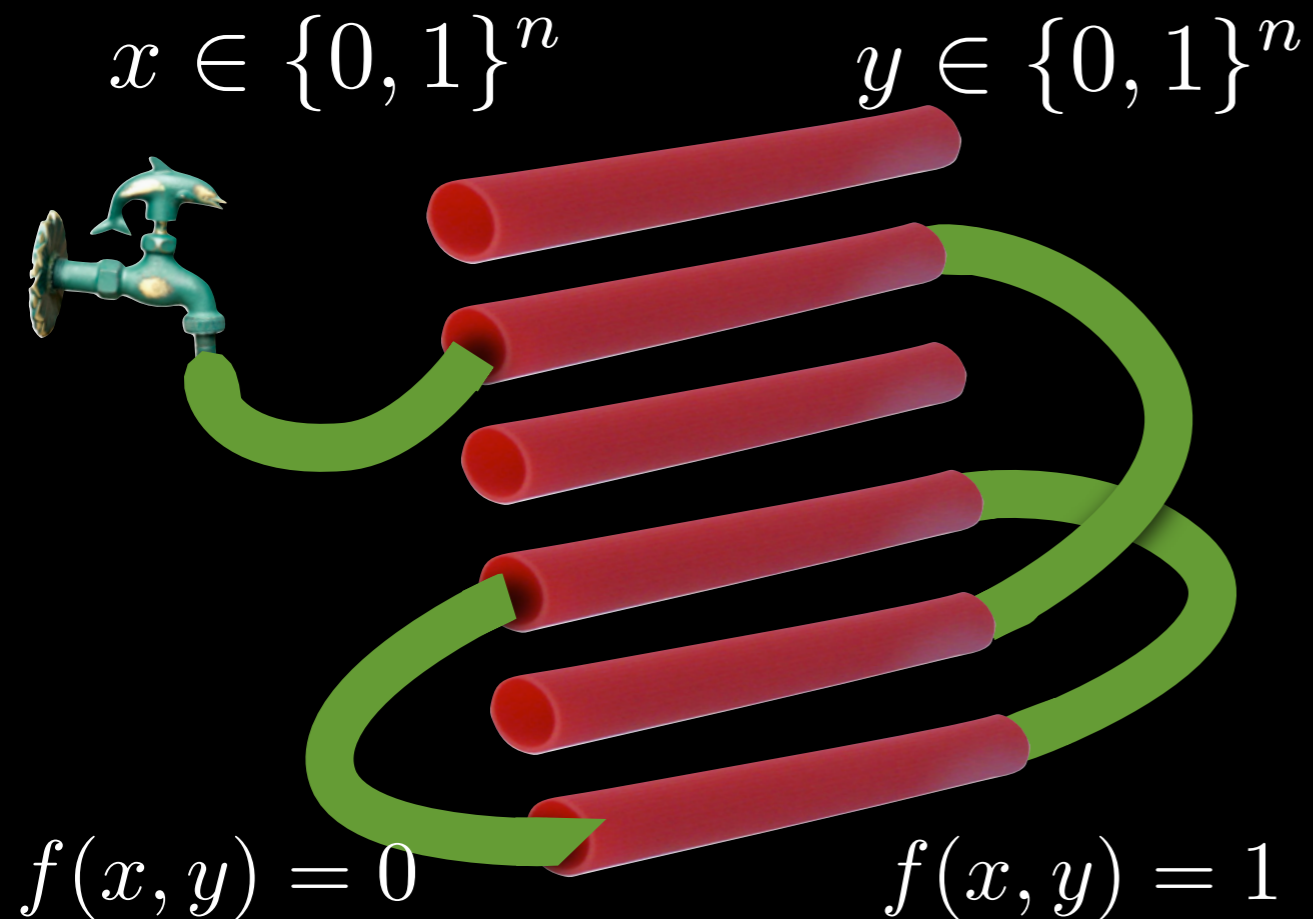
- upper bounds (constructions)



Computing a Boolean Function in the Garden-Hose Model

how many pipes are required?

- upper bounds (constructions)
- lower bounds (counting arguments)



Computing a Boolean Function in the Garden-Hose Model

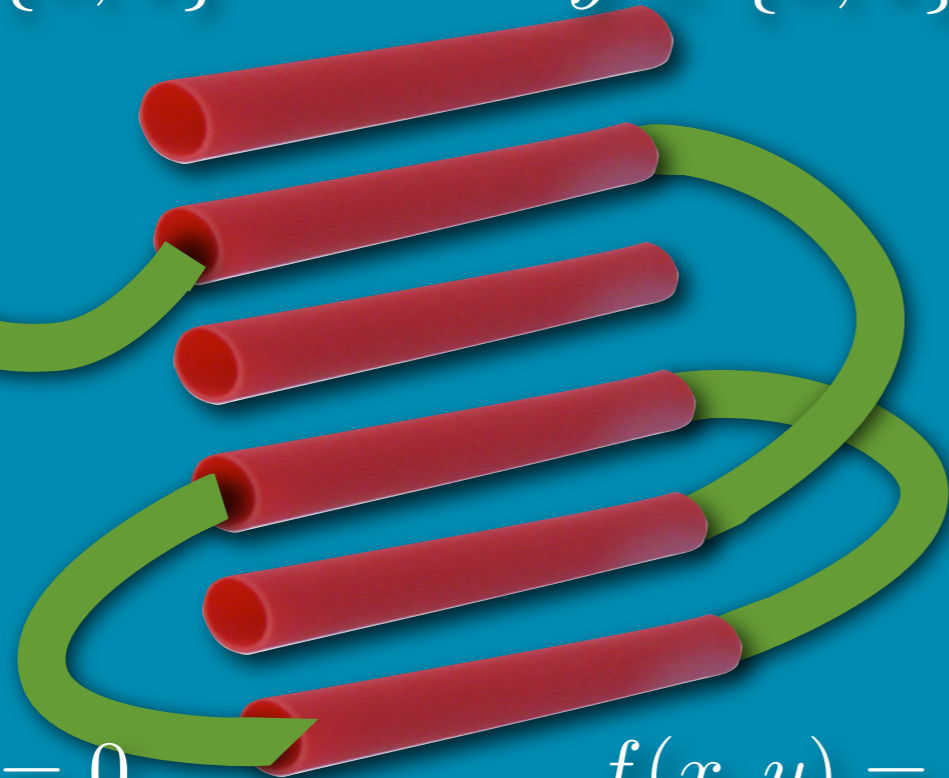
how many pipes are required?

- upper bounds (constructions)
- lower bounds (counting arguments)

good-night puzzle: equality function

$$x \in \{0, 1\}^n$$

$$y \in \{0, 1\}^n$$



$$f(x, y) = 0$$

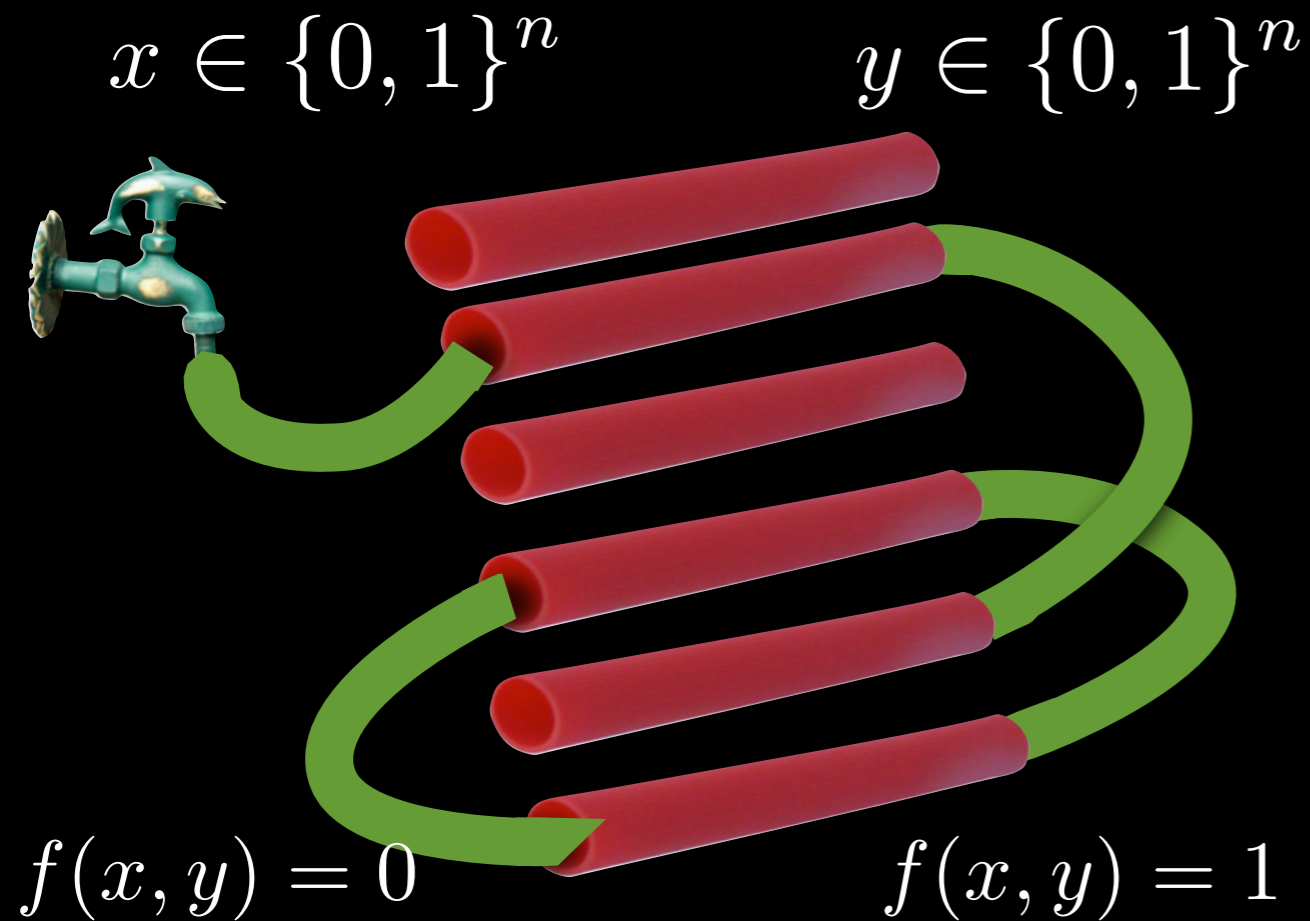
$$f(x, y) = 1$$

Computing a Boolean Function in the Garden-Hose Model

how many pipes are required?



good-night puzzle: equality function

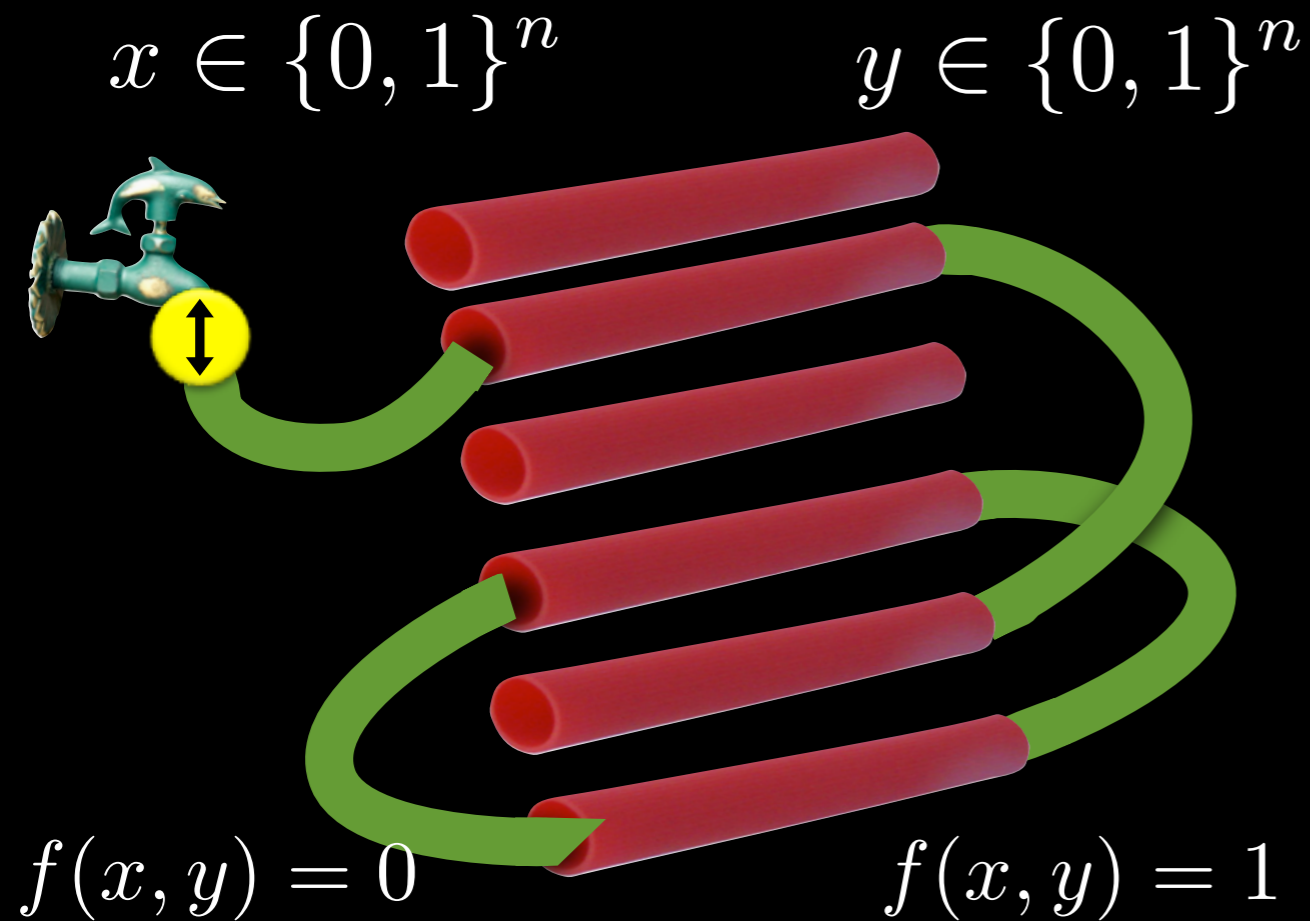


Link to Quantum Crypto

- Garden-Hose strategy

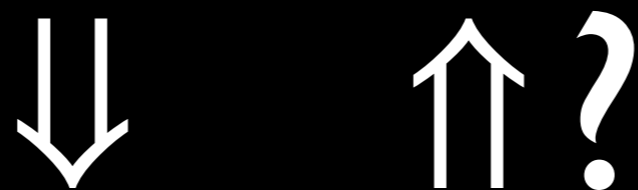


- attack on a simple quantum protocol for position verification

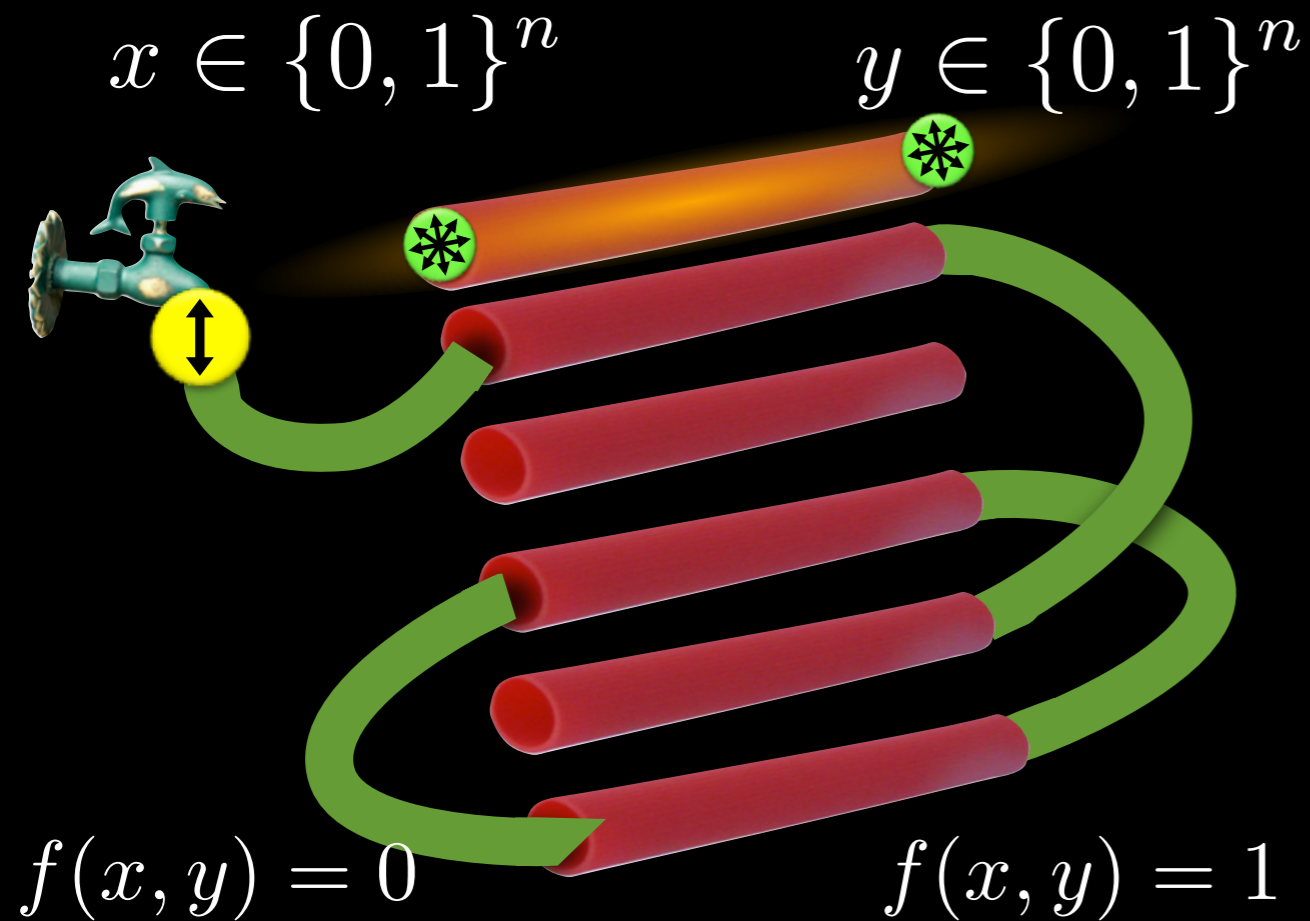


Link to Quantum Crypto

- Garden-Hose strategy



- attack on a simple quantum protocol for position verification

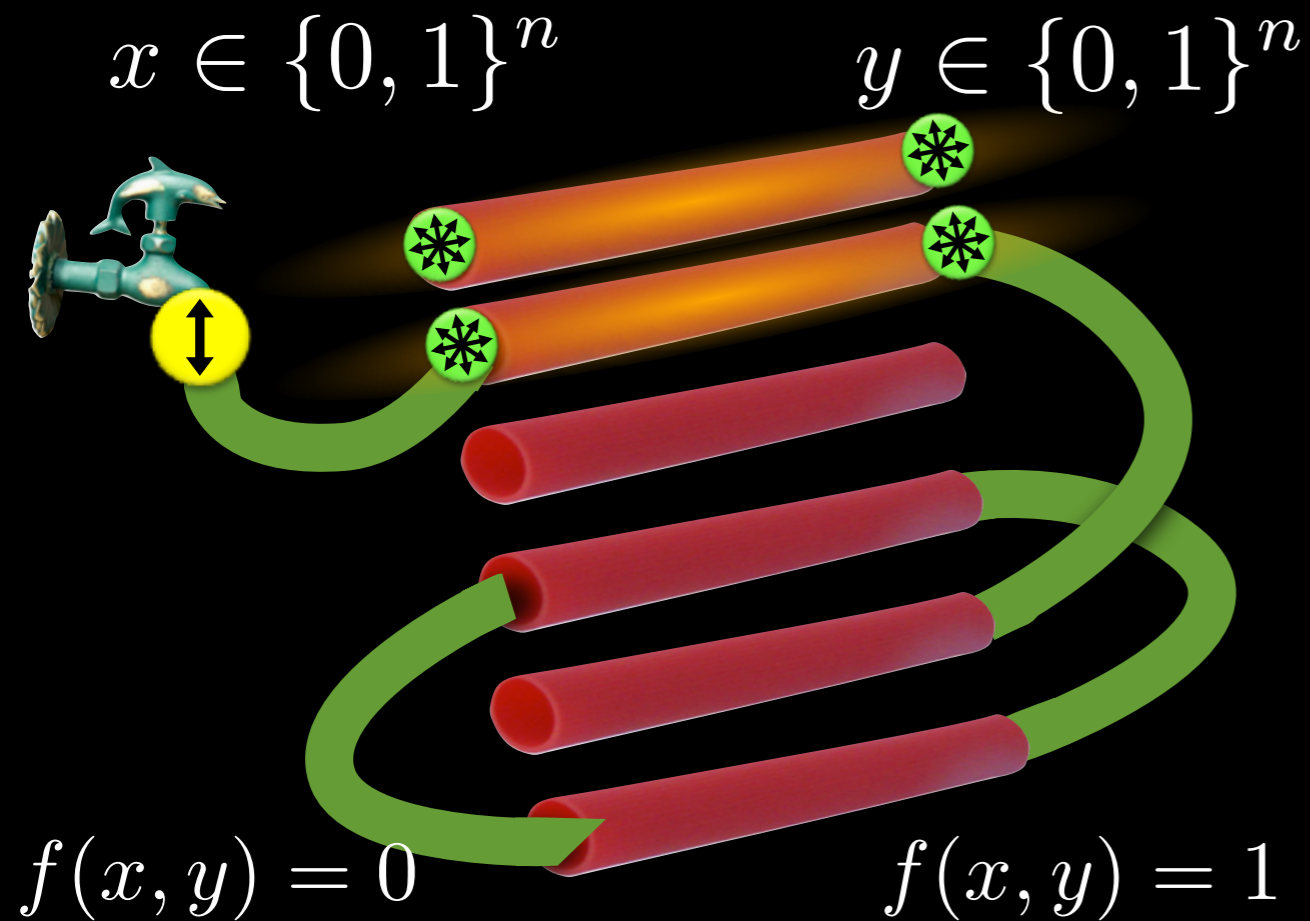


Link to Quantum Crypto

- Garden-Hose strategy



- attack on a simple quantum protocol for position verification

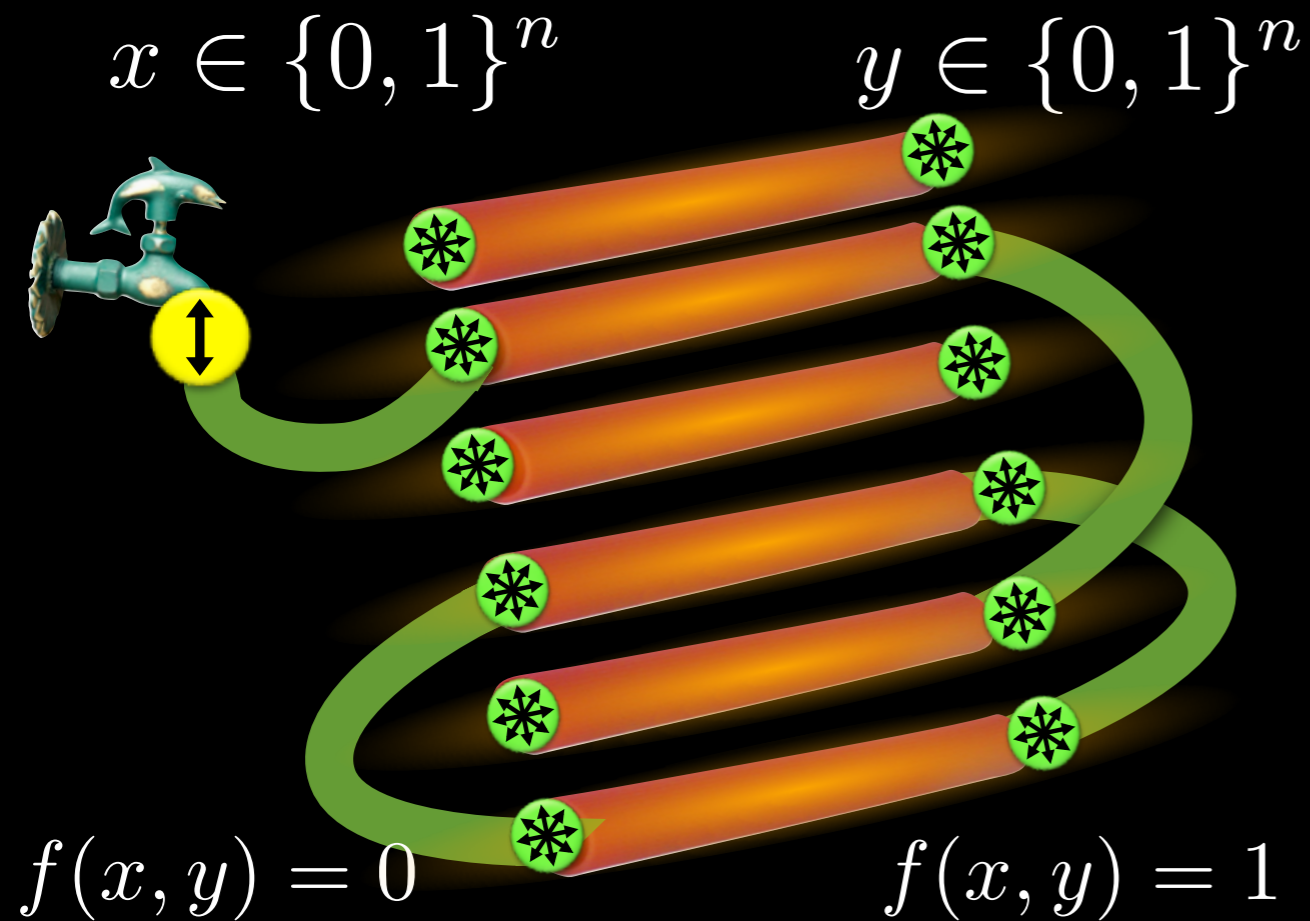


Link to Quantum Crypto

- Garden-Hose strategy



- attack on a simple quantum protocol for position verification

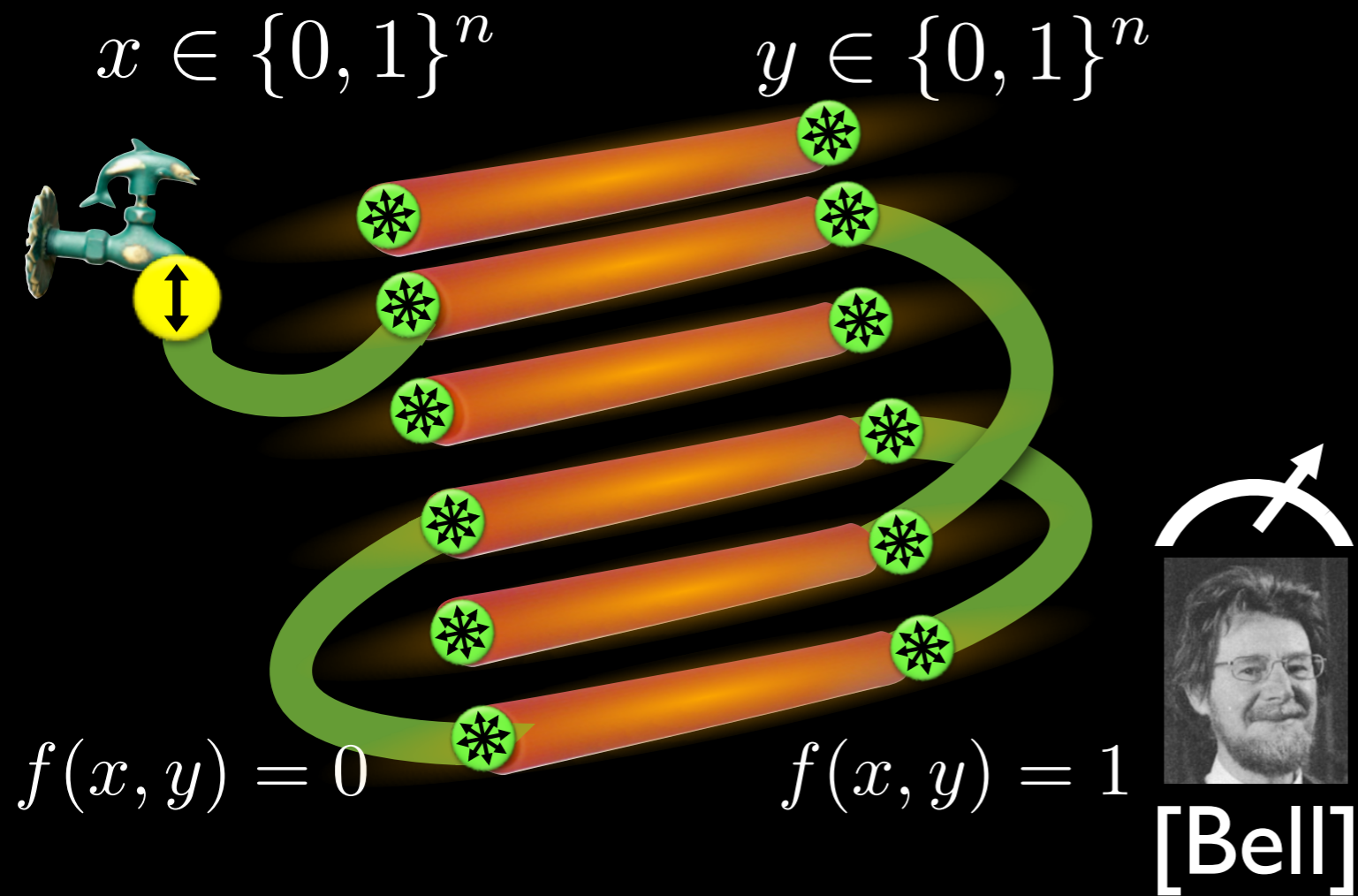


Link to Quantum Crypto

- Garden-Hose strategy



- attack on a simple quantum protocol for position verification

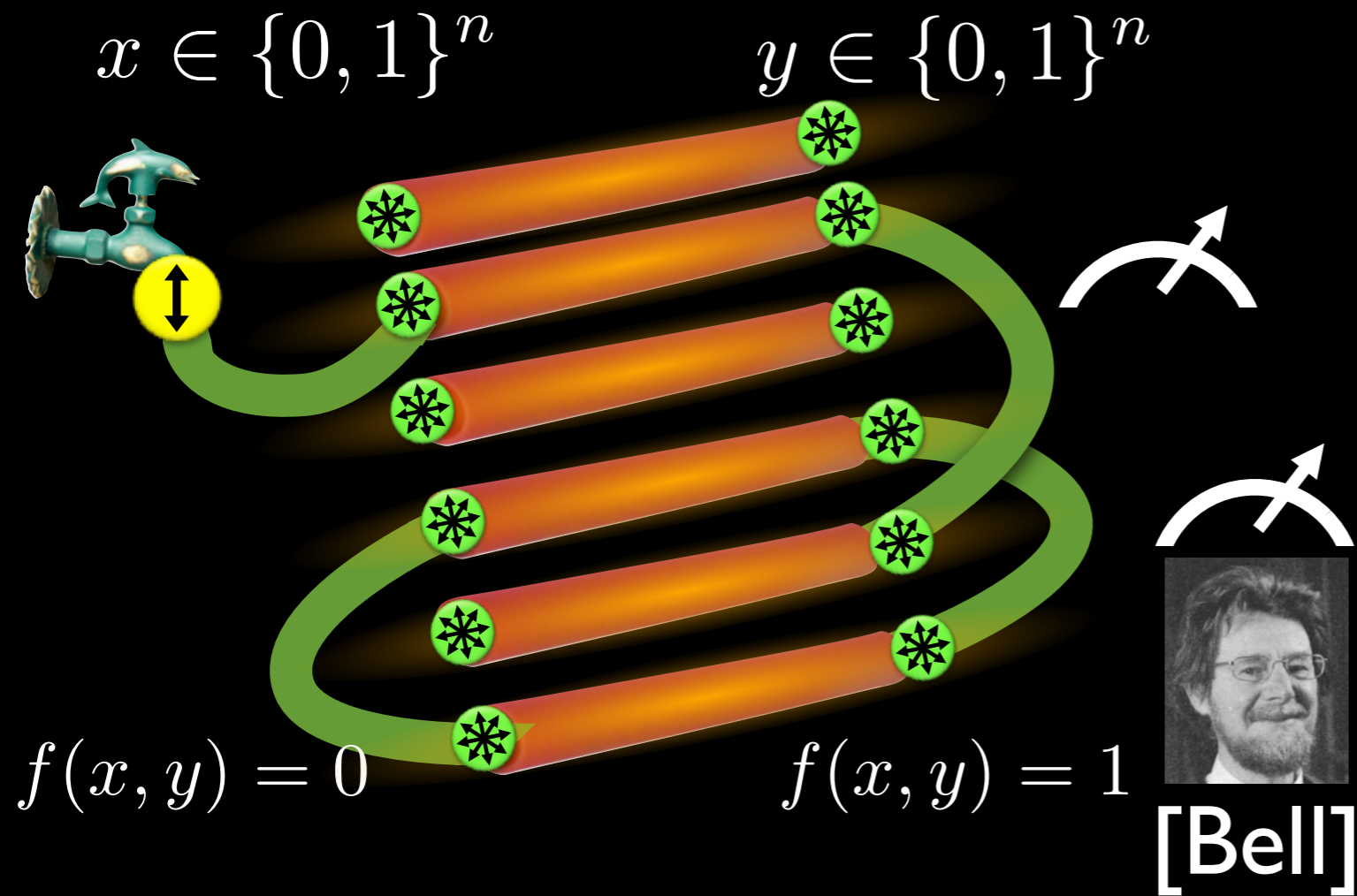


Link to
Quantum
Crypto

- Garden-Hose strategy



- attack on a simple quantum protocol for position verification

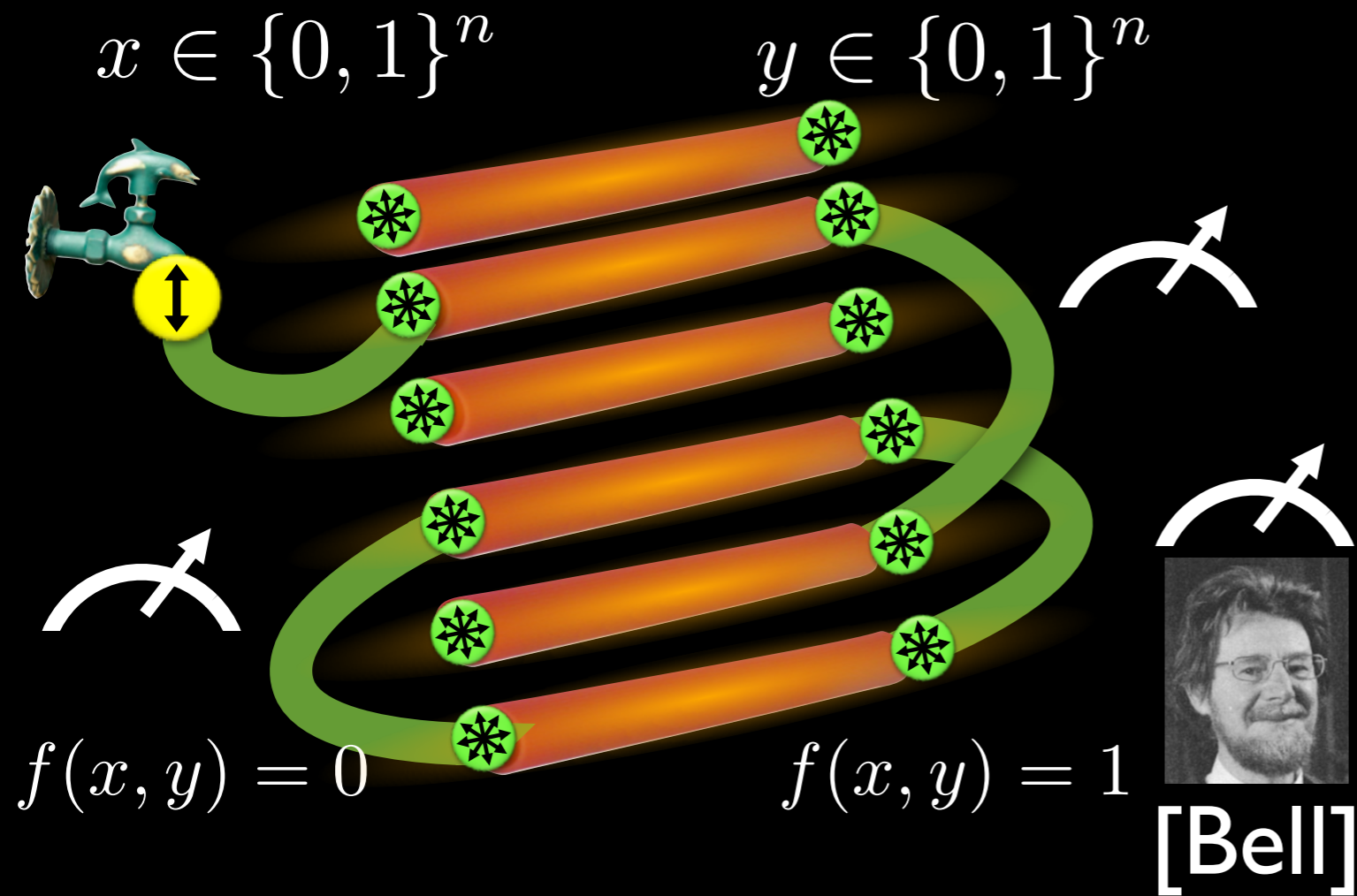


Link to
Quantum
Crypto

- Garden-Hose strategy

\Downarrow $\Uparrow?$

- attack on a simple quantum protocol for position verification

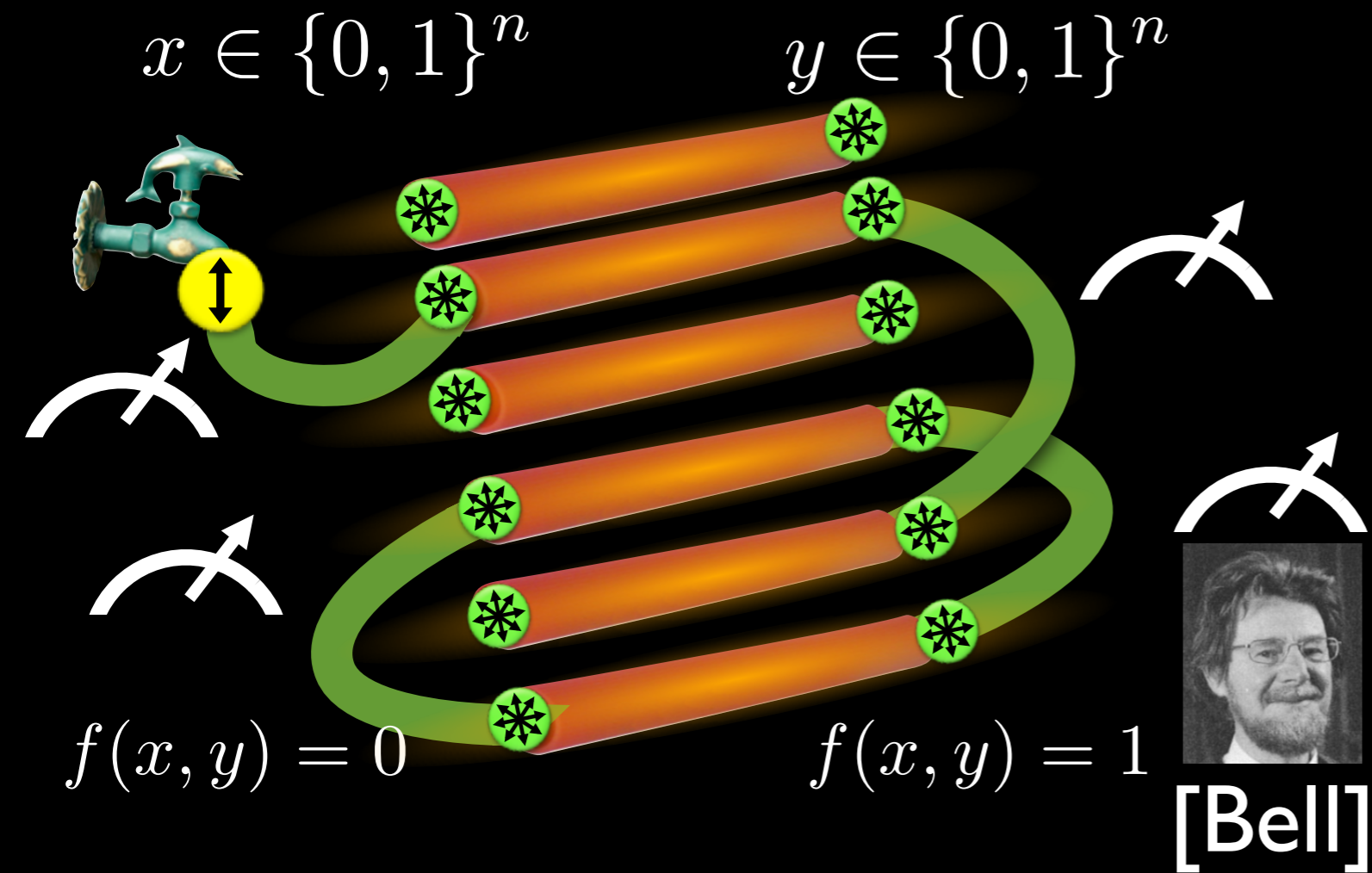


Link to
Quantum
Crypto

- Garden-Hose strategy

↓ ↓ ↑ ↑ ?

- attack on a simple quantum protocol for position verification



Link to
Quantum
Crypto

- Garden-Hose strategy

\Downarrow
 $\Uparrow?$

- attack on a simple quantum protocol for position verification

Qrypt 2011

FIRST ANNUAL CONFERENCE ON QUANTUM CRYPTOGRAPHY
www.qcrypt.net



ETH Zurich
12th-16th September 2011

- results will be presented at QCRYPT 2011
September 12-16 at ETH Zurich
- available on the arxiv soon