The Garden-Hose Game and Application to Position-Based Quantum Cryptography

Harry Buhrman, Serge Fehr,
Christian Schaffner, Florian Speelman

12 September 2011

CWI
Centrum Wiskunde & Informatica

Universiteit van Amsterdam

Position-based cryptography

- In cryptography, the parties use credentials such as digital keys or biometric features
- Position-based cryptography aims to use geographical position as a new credential

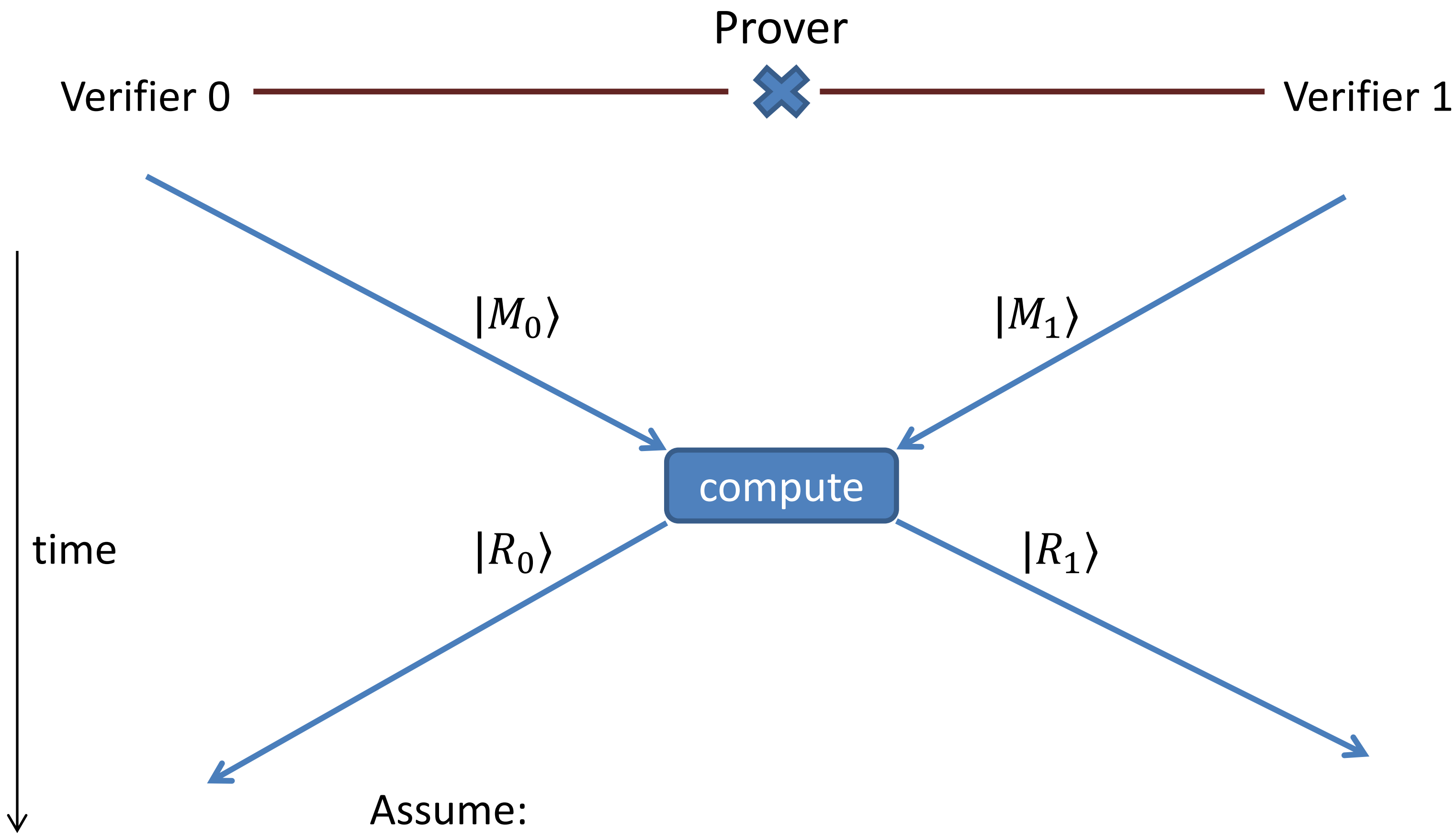
Position verification

The most basic task:

A prover has to convince multiple verifiers that he/she is at a certain location.

(For simplicity, let's only consider 1 dimension)

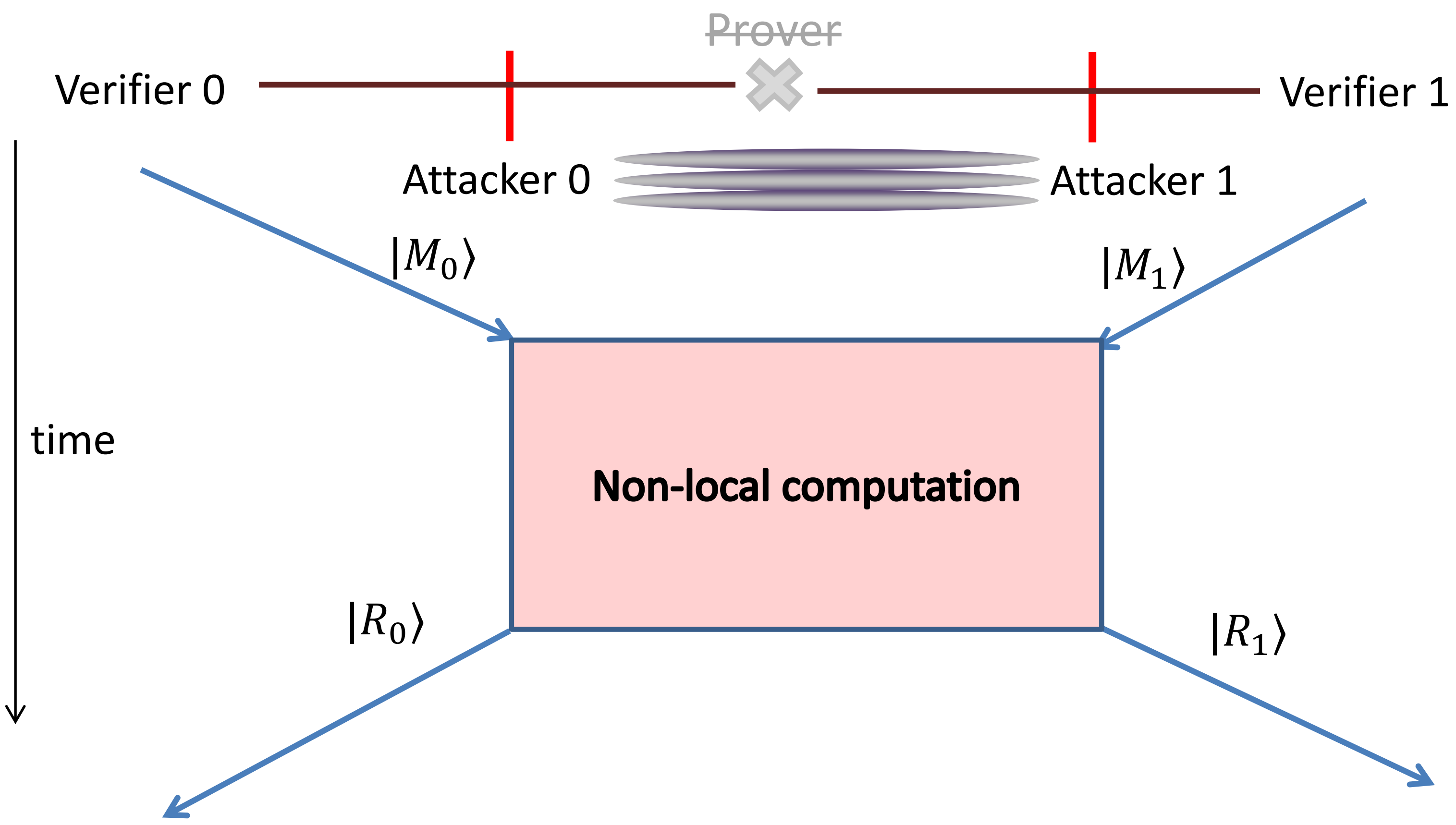
Quantum position verification in one dimension



Assume:
Communication at by the speed of light
Instantaneous computation
Verifiers can coordinate actions

The view of the attackers

Multiple colluding adversaries



General quantum attacks

- *Buhrman*, *Chandran*, *Fehr*, *Gelles*, *Goyal*, *Ostrovsky* and *Schaffner* show a general quantum attack, using a shared state of doubly exponential many qubits.

- Currently, any scheme can be attacked using pre-shared entanglement of exponential size.
(*Beigi* and *König*)

- On the positive side:
With no entanglement, security can be proven.

The next step

- Position-based quantum crypto might still be possible
- Are there schemes that are efficient for the honest parties, but require a lot of resources to attack?
- Zoom in on one set of schemes

Our Work

- For a specific class of schemes we obtain a trade-off:

  Increased classical communication for the honest players → bigger quantum state for the attackers

- The security of these schemes can be linked to classical complexity theory

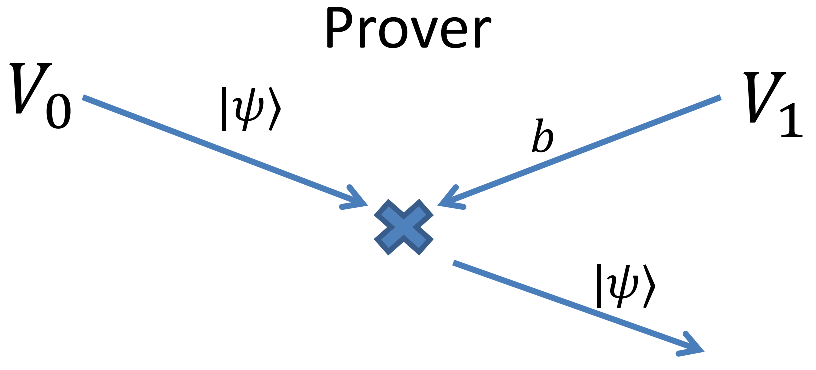
- A new model of communication complexity: the garden-hose model

Example scheme

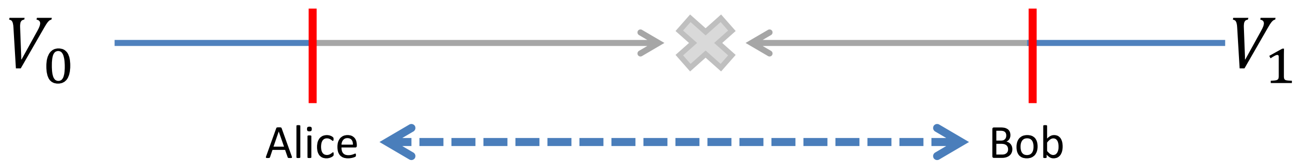
Verifier 0 sends qubit $|\psi\rangle$ to the Prover

Verifier 1 sends bit $b \in \{0,1\}$ to the Prover

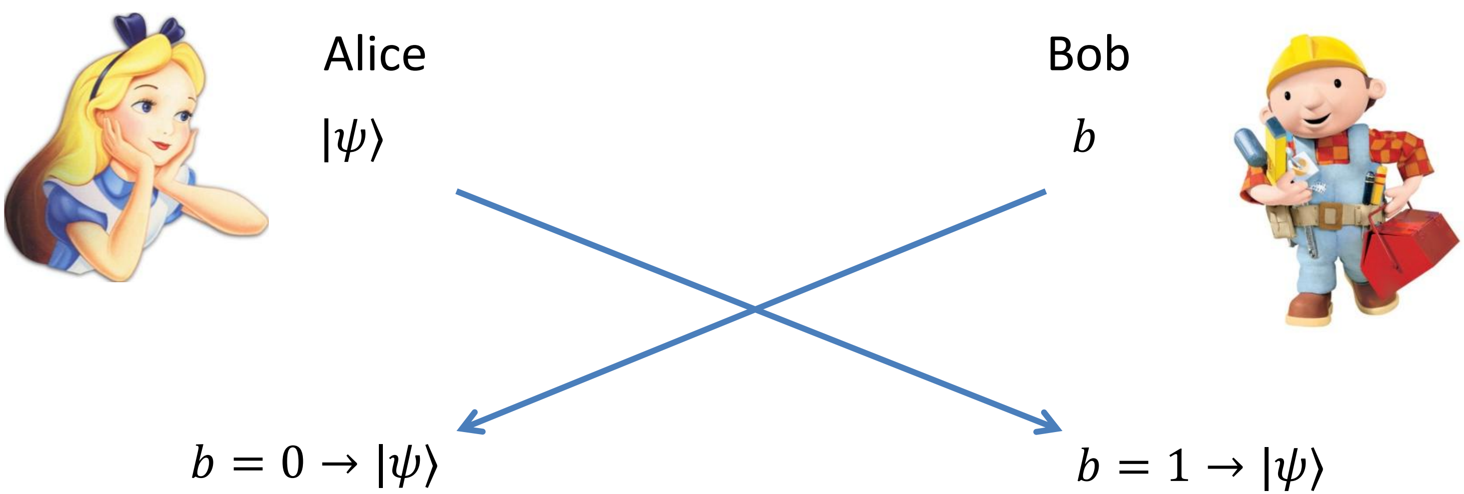
The Prover sends $|\psi\rangle$ to Verifier 0 or 1 depending on b



Attacking the example scheme



Alice starts with $|\psi\rangle$, Bob starts with b.
One round of simultaneous communication
Now Alice must have $|\psi\rangle$ if $b = 0$.
Otherwise, Bob must have $|\psi\rangle$.



Attacking the example scheme

- The task of Alice and Bob is impossible if they share no entanglement
- But if they do...

Alice

$|\psi\rangle$

Bob

b

$b = 0 \rightarrow |\psi\rangle$

$b = 1 \rightarrow |\psi\rangle$

Attacking the example scheme

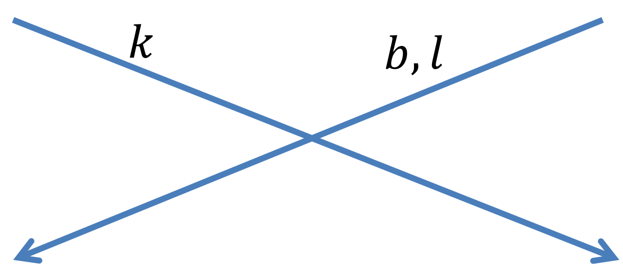
$b = 0$

Alice

$|\psi\rangle$

Bob

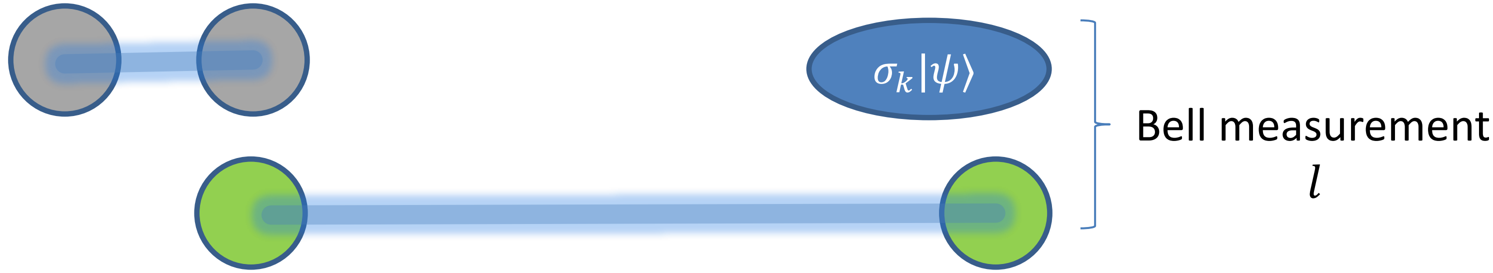
b



$|\psi\rangle$

Attacking the example scheme

$$b = 0$$

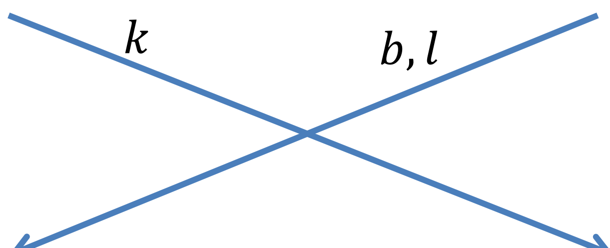


Alice

$|\psi\rangle$

Bob

b



$|\psi\rangle$

Attacking the example scheme

$b = 0$

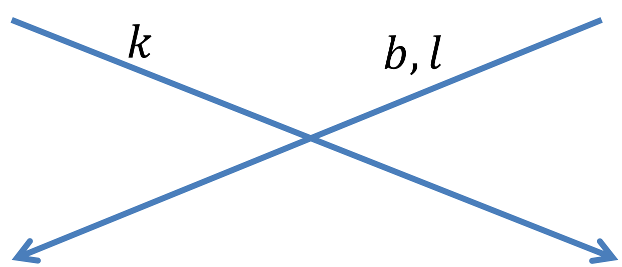
Alice only knows that she has the qubit after receiving Bob's message

Alice

$|\psi\rangle$

Bob

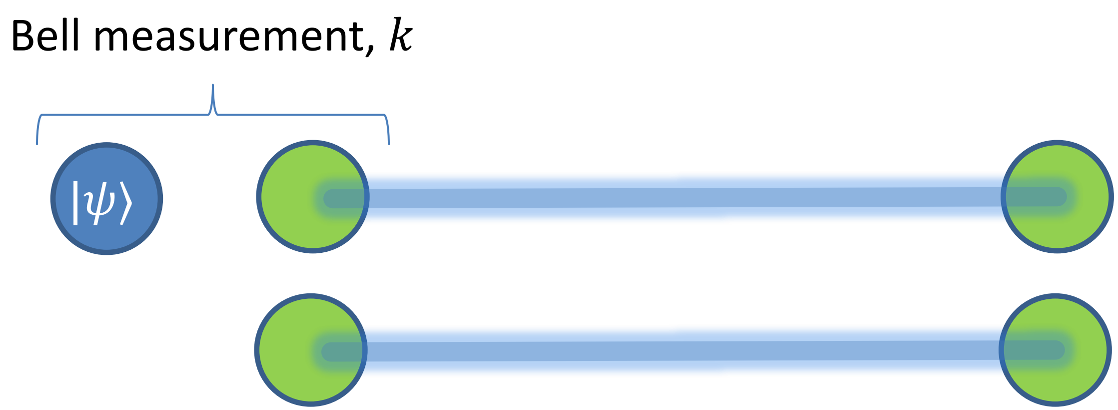
b



$|\psi\rangle$

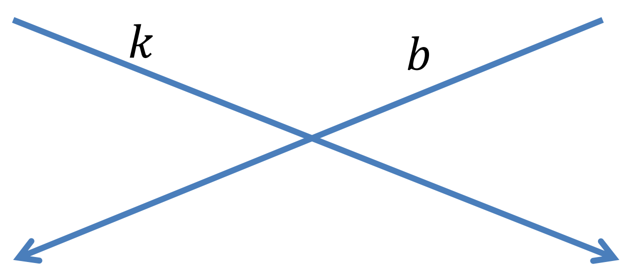
Attacking the example scheme

$b = 1$



Alice

$|\psi\rangle$

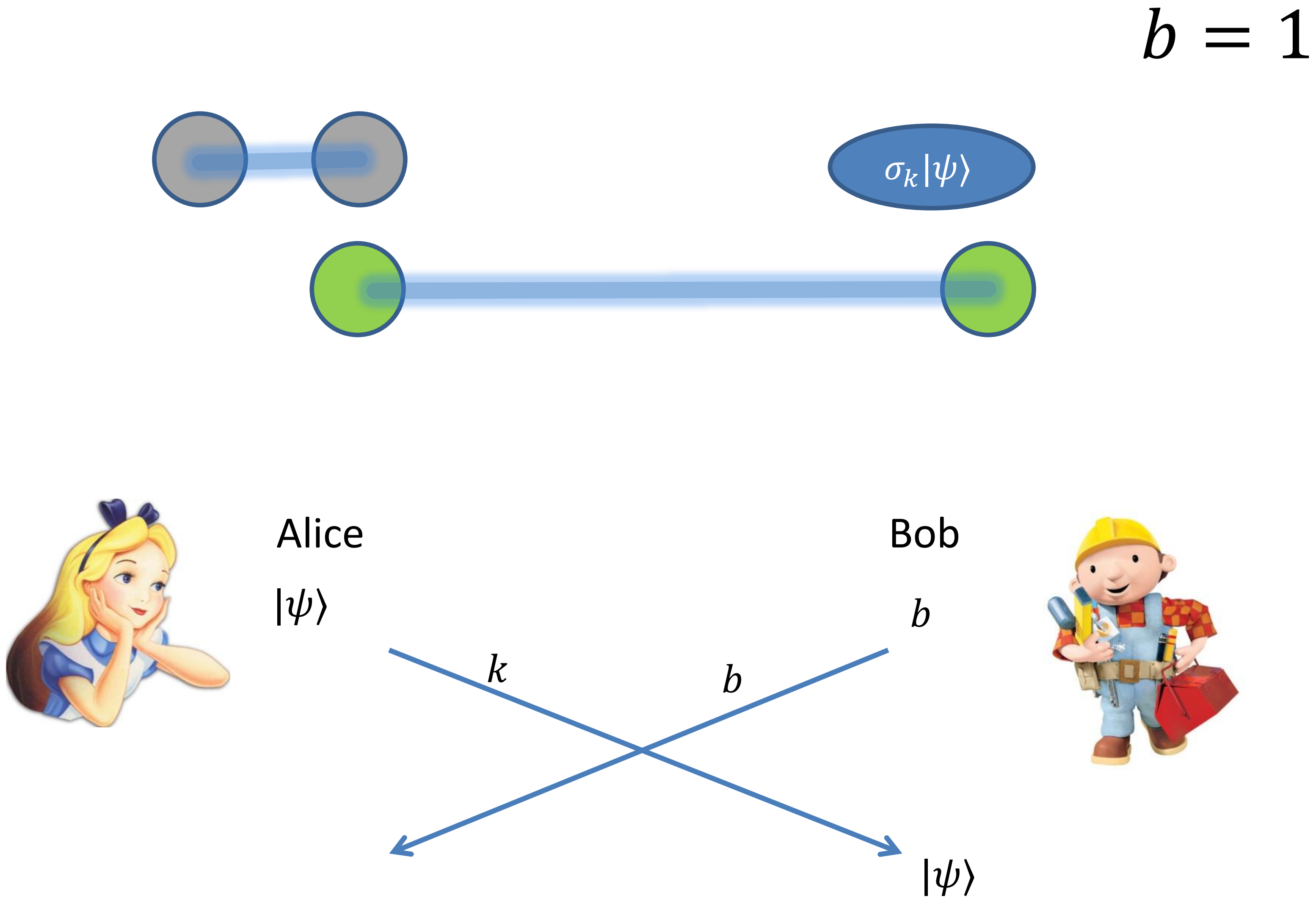


Bob

b

$|\psi\rangle$

Attacking the example scheme



The class of schemes

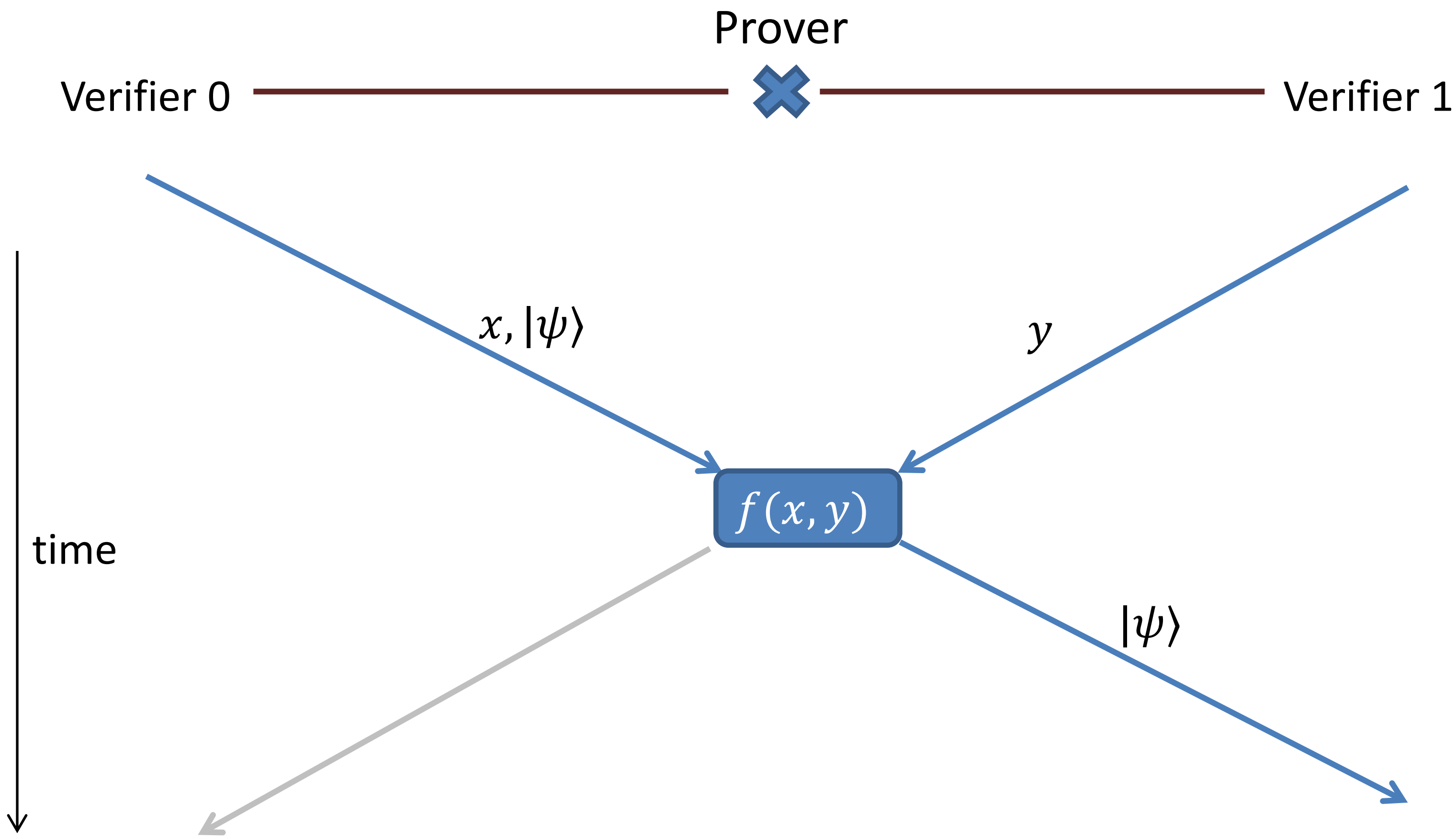
Instead of one bit, we use a function:

- V_0 sends $|\psi\rangle$ and n-bit string x to Prover
- V_1 sends n-bit string y to Prover

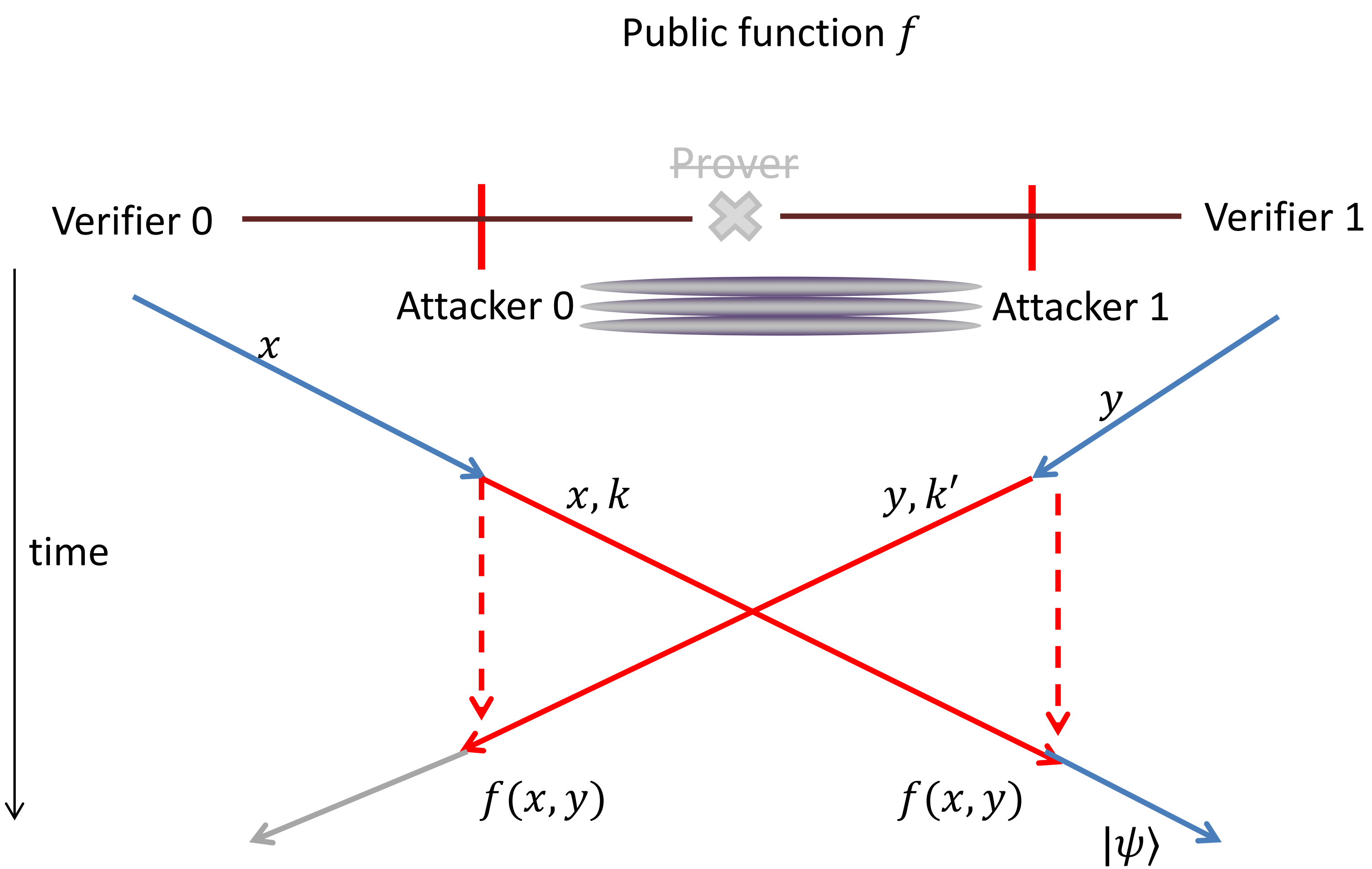
- Prover computes function $f(x,y)$ and sends $|\psi\rangle$ to V_0 or V_1 depending on outcome

Adrian Kent, William Munro, and Timothy Spiller
Quantum tagging: Authenticating location via quantum
Information and relativistic signaling constraints.
Physical Review A, 84(1), July 2011.

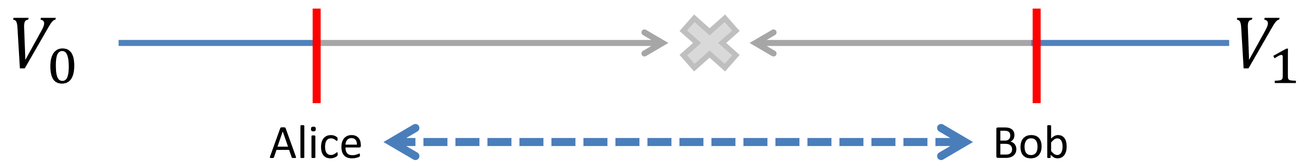
The class of schemes



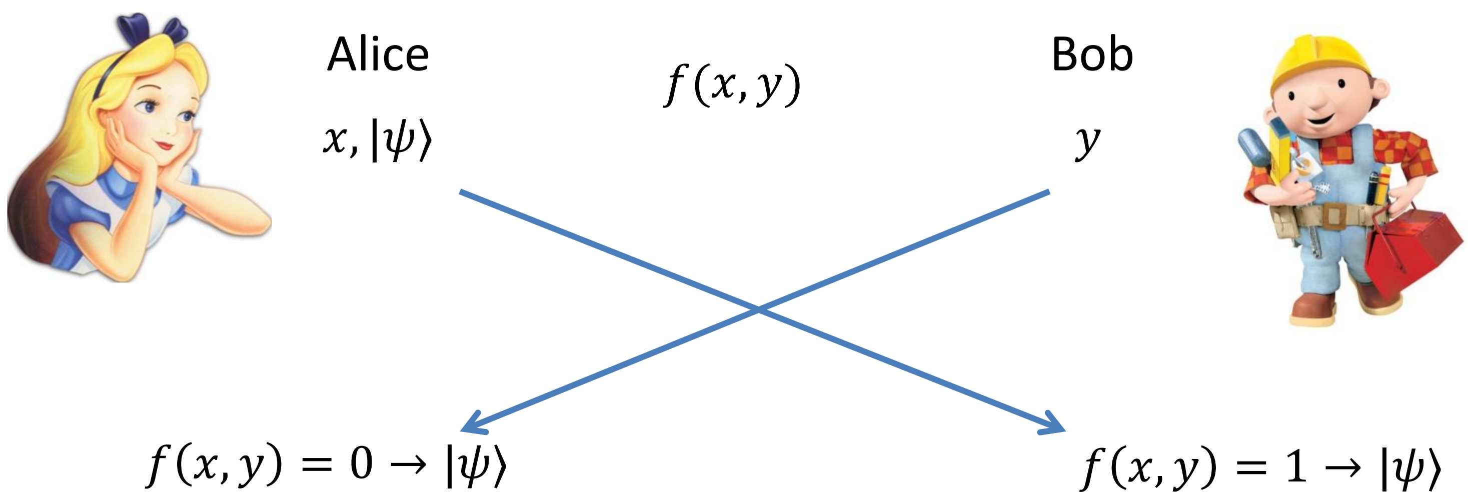
Attacking the schemes



The attack as a game

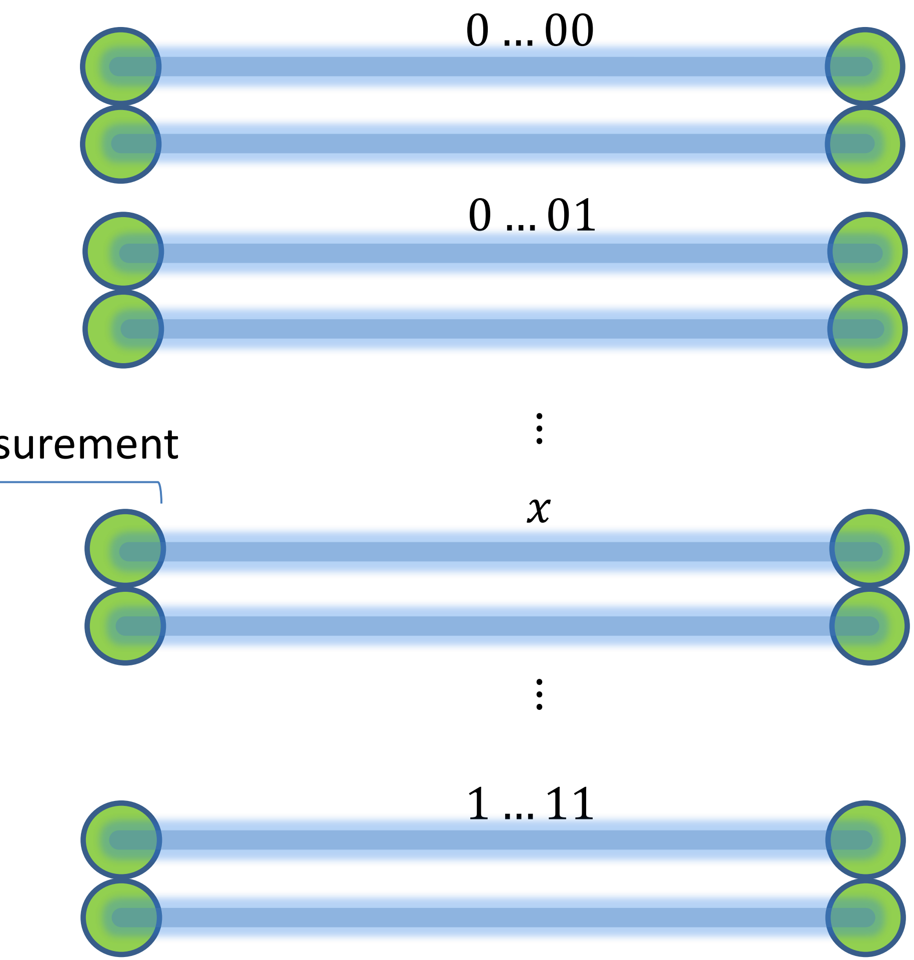


Alice starts with $x, |\psi\rangle$
Bob starts with y.
One round of simultaneous communication
Alice must have $|\psi\rangle$ if $f(x, y) = 0$.
Otherwise, Bob must have $|\psi\rangle$.



Breaking the schemes

Using $2 \cdot 2^n$ EPR pairs



Teleport if $f(0 \dots 00, y) = 0$

Teleport if $f(0 \dots 01, y) = 0$

$\vdots$

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

$\vdots$

Teleport if $f(1 \dots 11, y) = 0$

Attacks

- Exponentially many qubits, not feasible
- Breaking might be much easier for some functions $f(x, y)$

- We would like a function $f(x, y)$ that is easily computable for the Prover, but gives a scheme that is hard to break

The Garden-Hose Model

Alice and Bob share s pipes between them.

$f(x, y)$

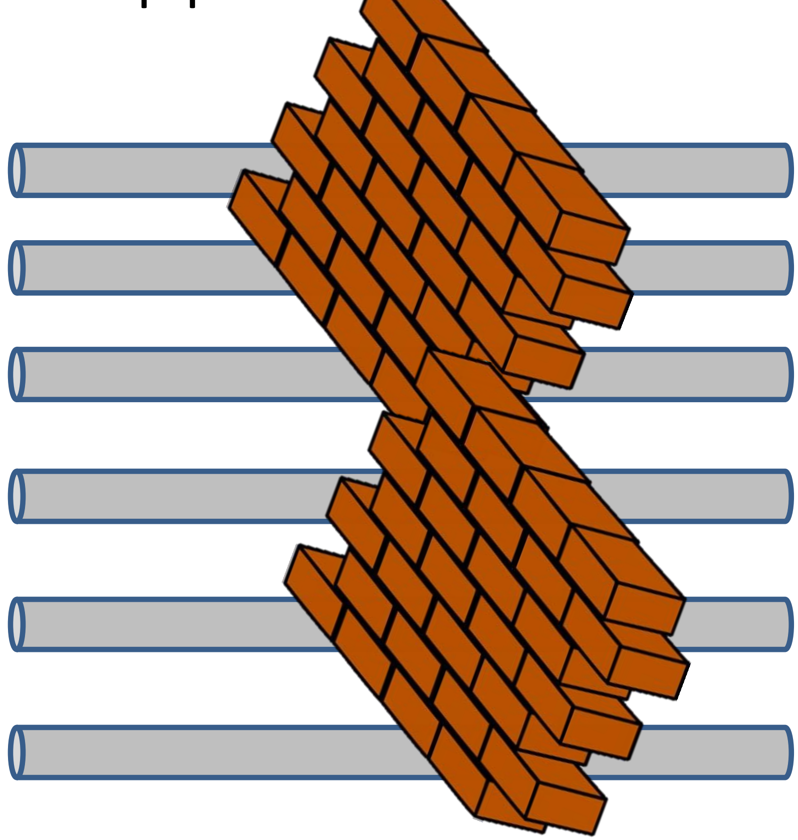
$y \in \{0,1\}^n$

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

The Garden-Hose Model

Alice and Bob share s pipes between them.

$f(x, y)$



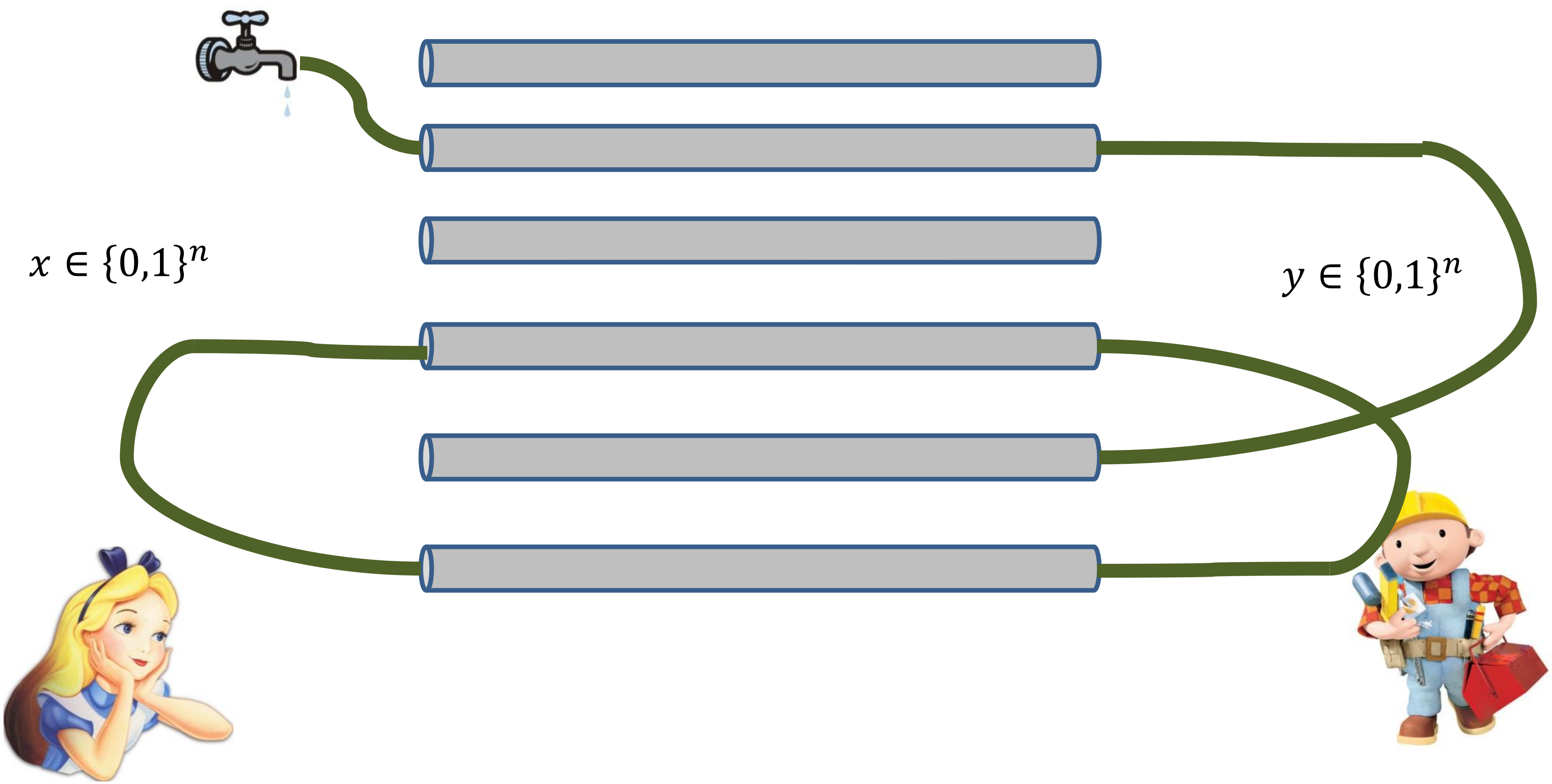
$y \in \{0,1\}^n$

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

The Garden-Hose Model

They connect the pipes with pieces of hose.
Alice also has a water tap she connects.

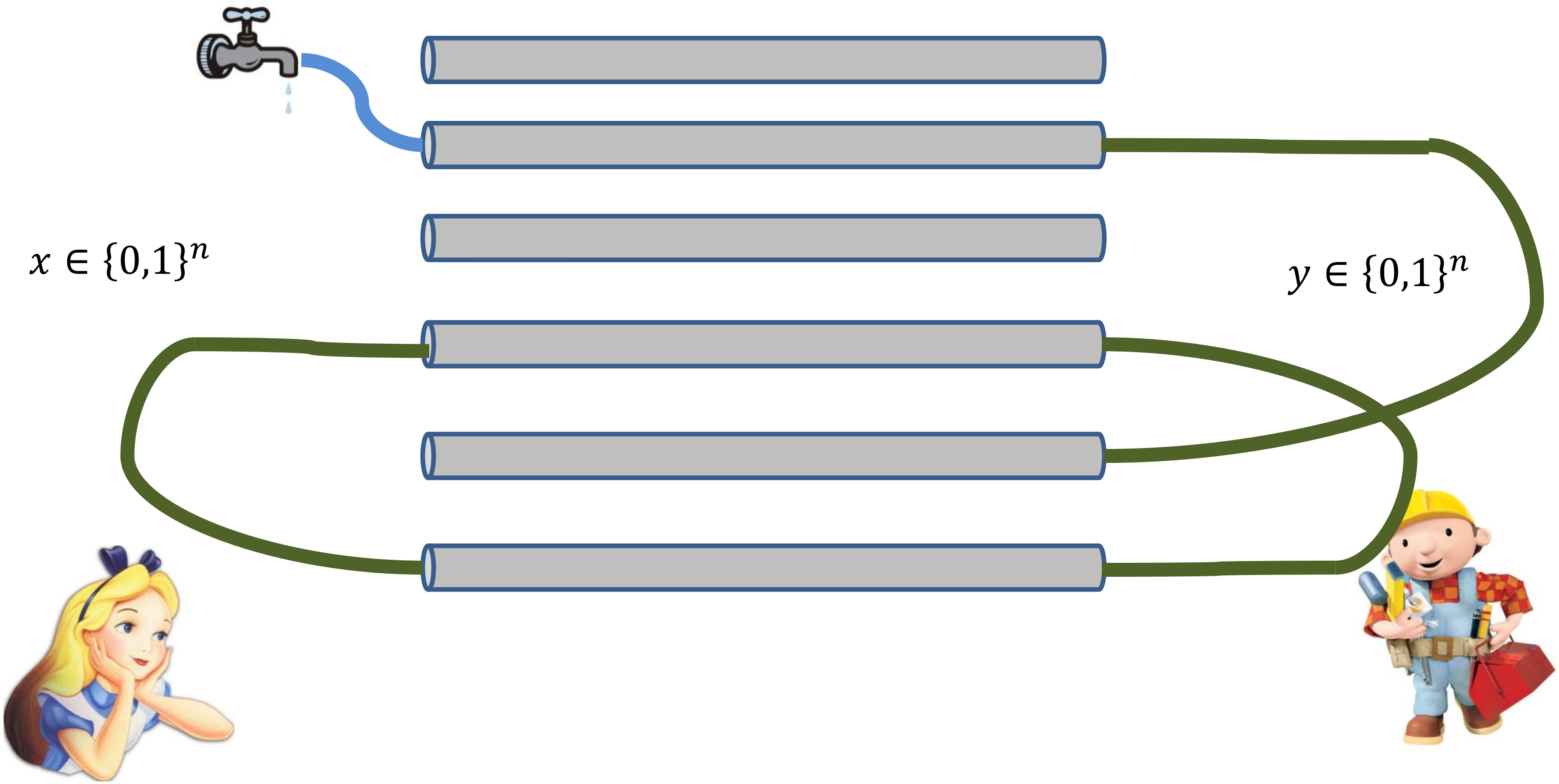
$f(x, y)$



The Garden-Hose Model

They connect the pipes with pieces of hose.
Alice also has a water tap she connects.

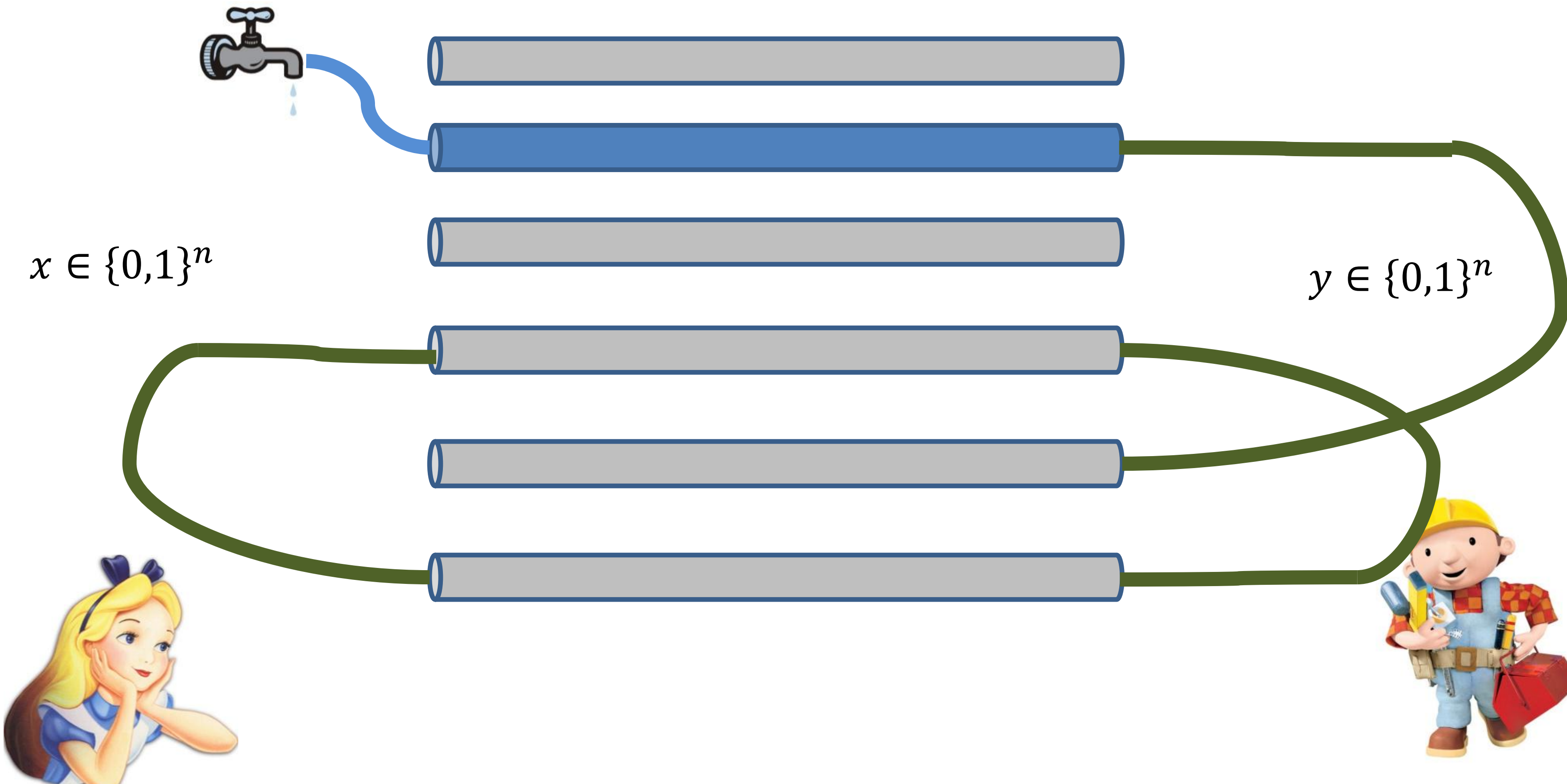
$f(x, y)$



The Garden-Hose Model

They connect the pipes with pieces of hose.
Alice also has a water tap she connects.

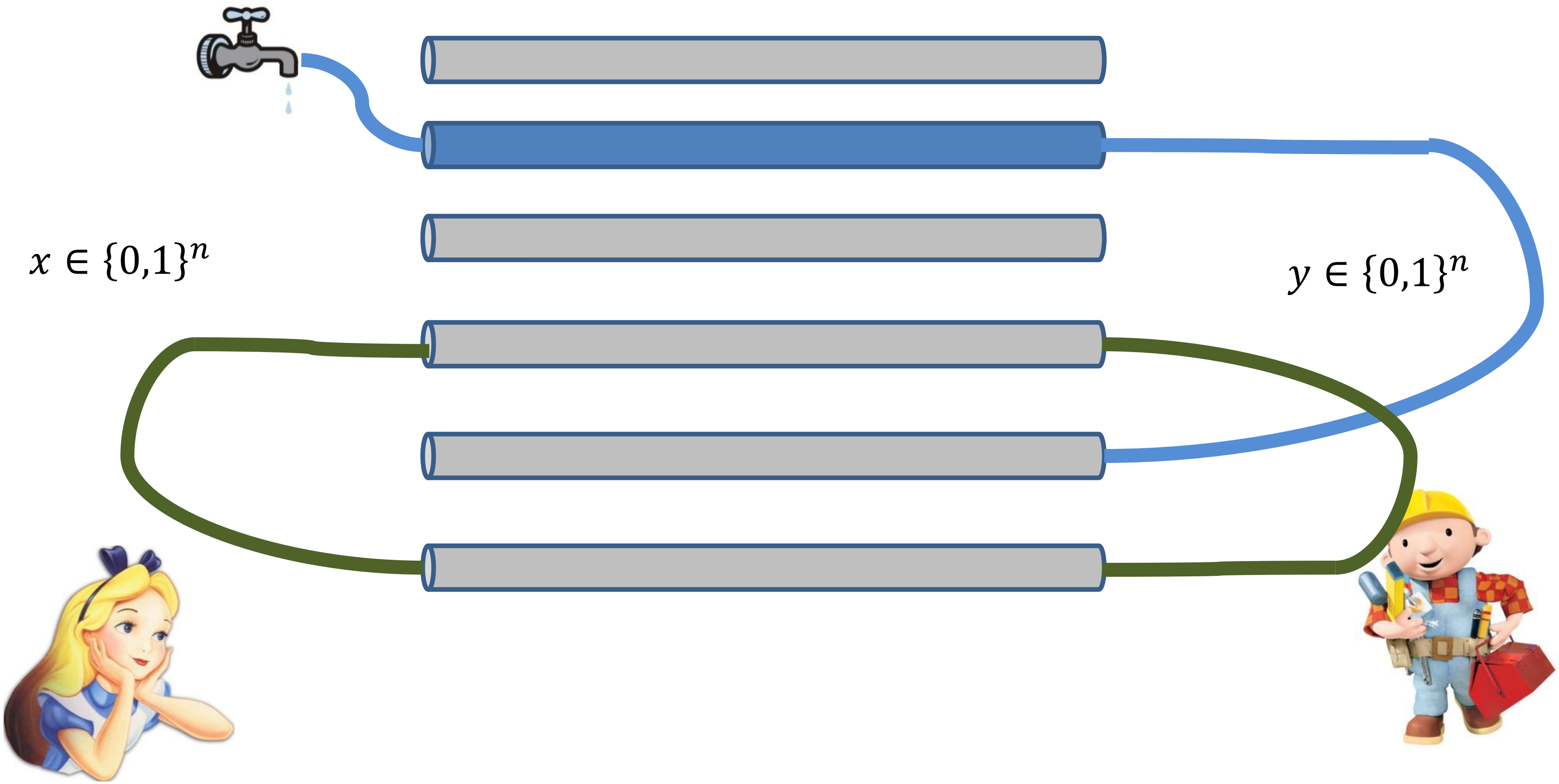
$f(x, y)$



The Garden-Hose Model

They connect the pipes with pieces of hose.
Alice also has a water tap she connects.

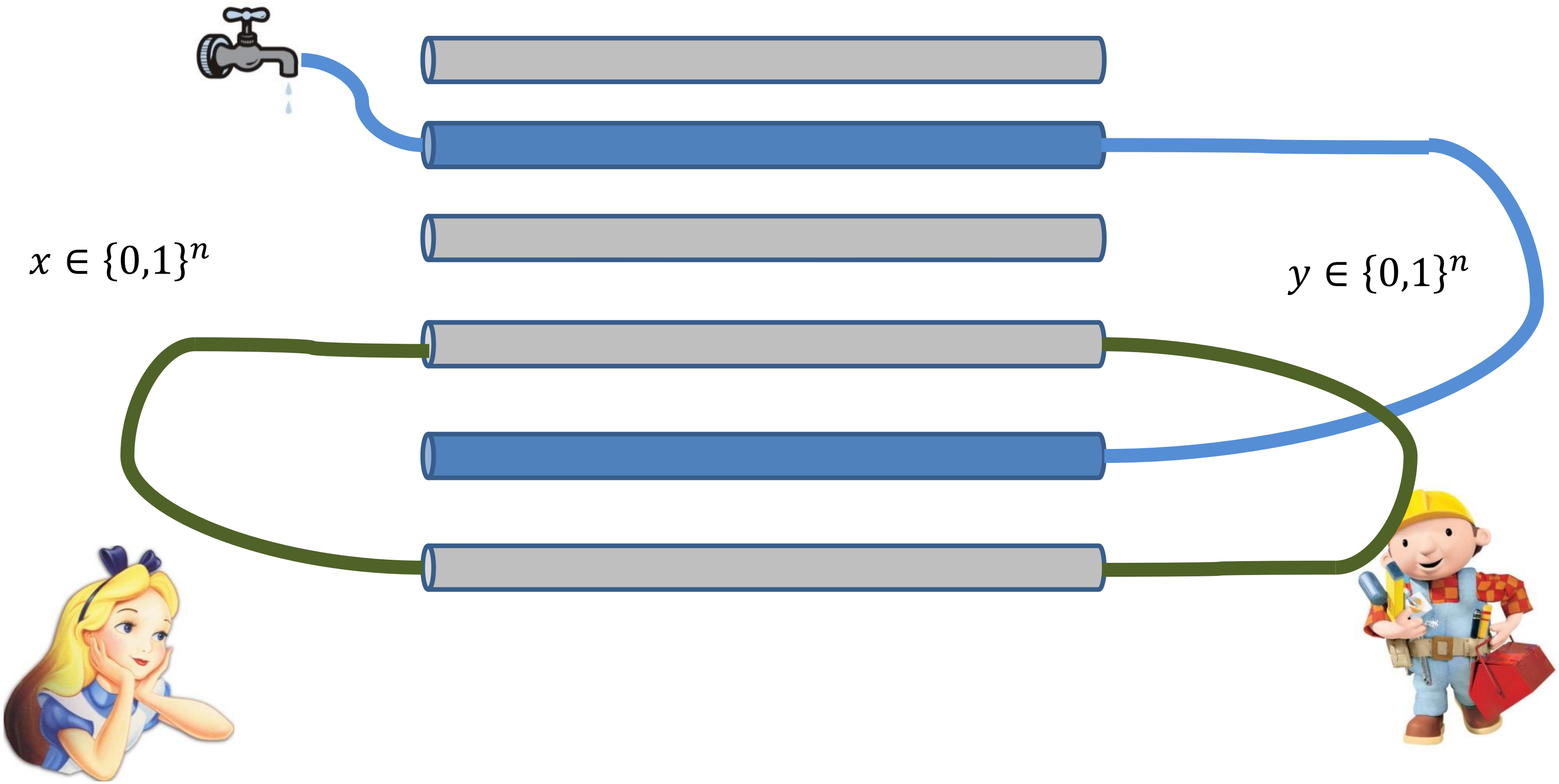
$f(x,y)$



The Garden-Hose Model

They connect the pipes with pieces of hose.
Alice also has a water tap she connects.

$f(x,y)$

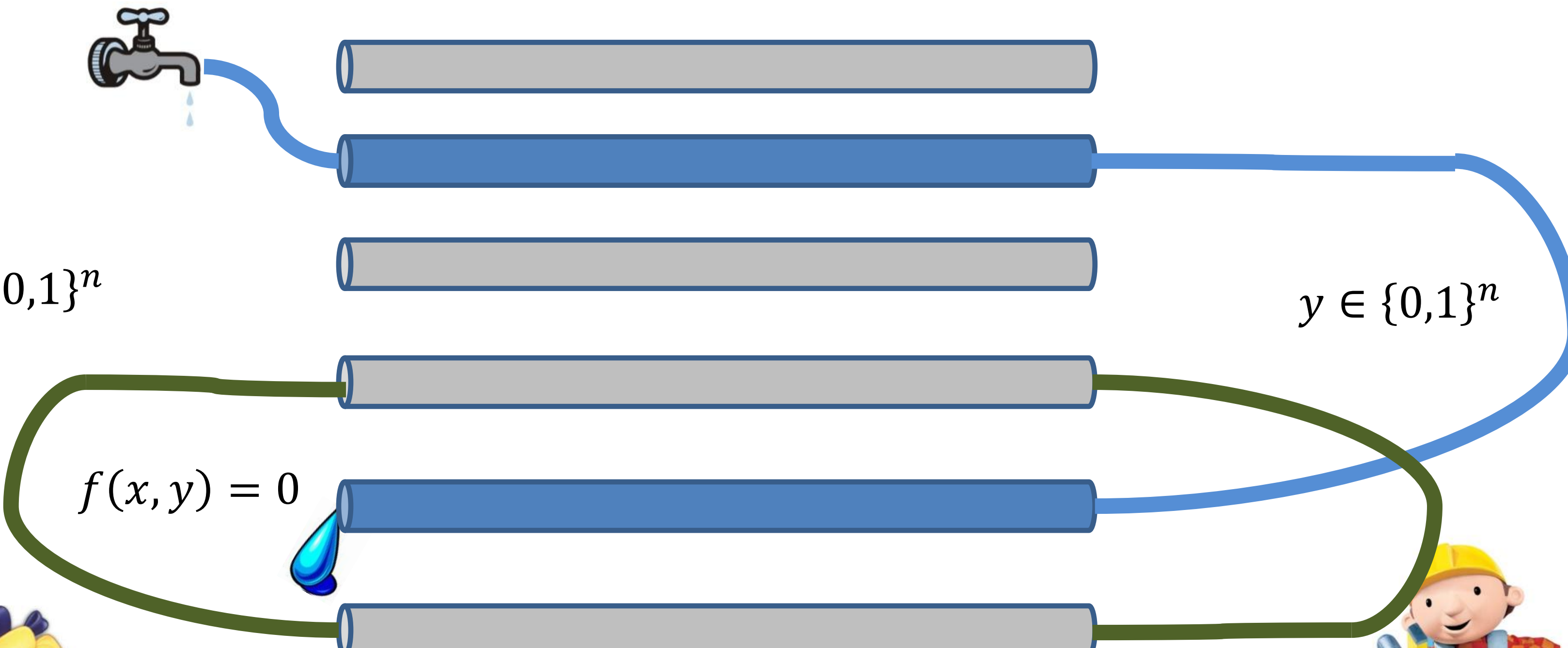


The Garden-Hose Model

They connect the pipes with pieces of hose.
Alice also has a water tap she connects.

$f(x,y)$

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

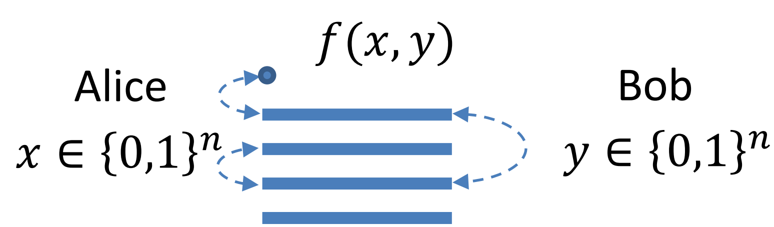


The Garden-Hose Model

A strategy in the garden-hose model for a function f gives an attack on that scheme.
(Number of pipes → number of EPR pairs.)

The garden-hose complexity upper bounds the entanglement needed to break corresponding scheme

The garden-hose model captures a class of perfect attacks.



Barrington's Theorem:

Logarithmic depth circuits can be computed by a ***width-5 permutation branching program*** of polynomial length.

Instructions: (i, π, τ) with $\pi, \tau \in S_5$

Evaluate to π if $x_i = 1$, evaluate to τ if $x_i = 0$

The branching program is a list of these instructions:

$(i_1, \pi_1, \tau_1)(i_2, \pi_2, \tau_2)(i_3, \pi_3, \tau_3) = e$ if circuit outputs 0

Otherwise a 5-cycle

Applying Barrington's theorem

If $f(x, y)$ has a log-depth circuit, the garden-hose complexity of f is bounded by a polynomial.

Proof sketch:

Barrington's theorem gives a polynomially long list of instructions.

Assume these instructions alternate between depending on x and y.

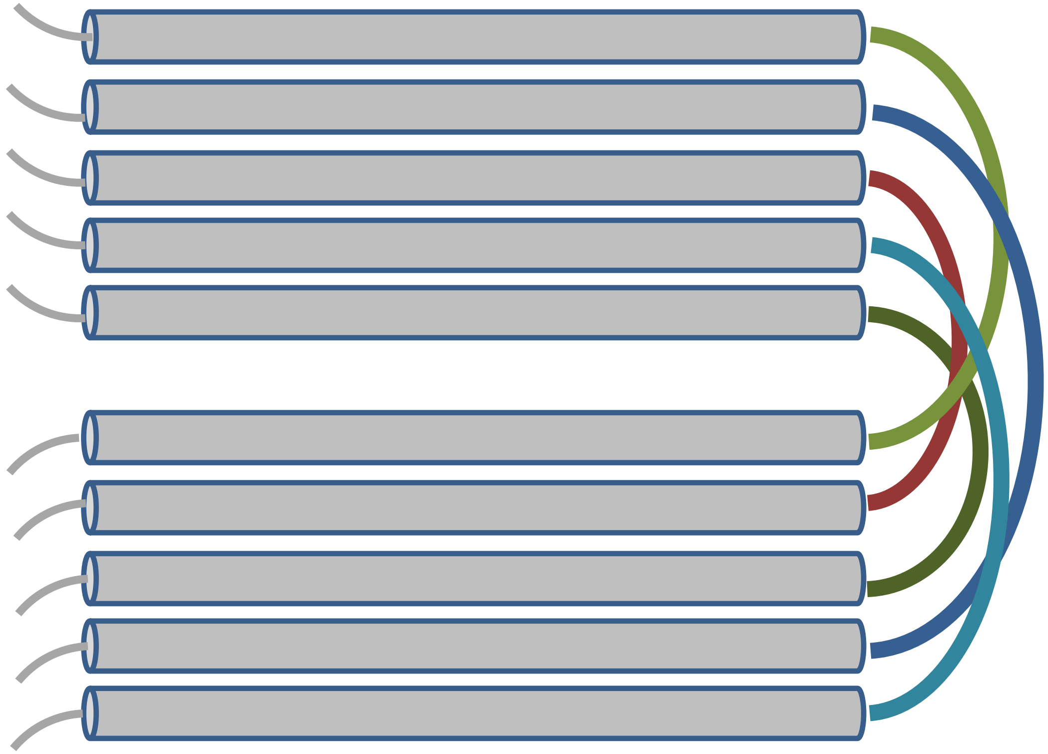
Permutation branching program outputs:

The identity permutation when $f(x, y) = 0$

and a 5-cycle when $f(x, y) = 1$

Applying Barrington's theorem

For every even instruction k in the permutation branching program



According to π_k,
with π_k the output of
the current instruction

Using π_{k+1}

To the pipe corresponding to $\pi_1(1)$,
with π_1 the output of the first instruction

Logarithmic space computations

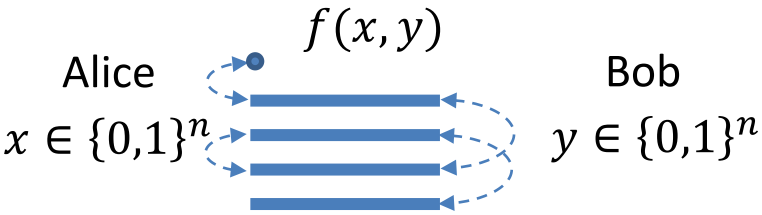
If $f(x, y)$ can be computed in logarithmic space,

then the garden-hose complexity of f is polynomial.

Corollary: If $L = P$ then every efficiently computable function's scheme can be broken using a polynomial amount of EPR pairs

Other results

- Garden-hose lower bounds:
  - Linear lower bound for many functions
  - There exist functions that need an exponential number of pipes
- Quantum lower bounds
  - For specific functions: logarithmic number of qubits
  - There exist functions that need a linear number of qubits



Summary

- Position-based quantum cryptography might still be possible when the pre-shared state is bounded

- A new model of communication complexity: the garden-hose model

- In the considered schemes:
  more classical computation for the Prover →
  Adversaries need a bigger quantum state

- The security of these schemes can be linked to classical complexity theory

Further work

- Extend the results to a randomized setting
- Parallel repetition theorems
- Closing the gap between upper and lower bounds
- Find a function in P that needs exponential entanglement (assuming $P \neq L$)

Thank you!