Introduction to Quantum Computing

Trung T. Pham

Cyberworx & Department of Computer Science

United States Air Force Academy

Colorado, USA

Agenda

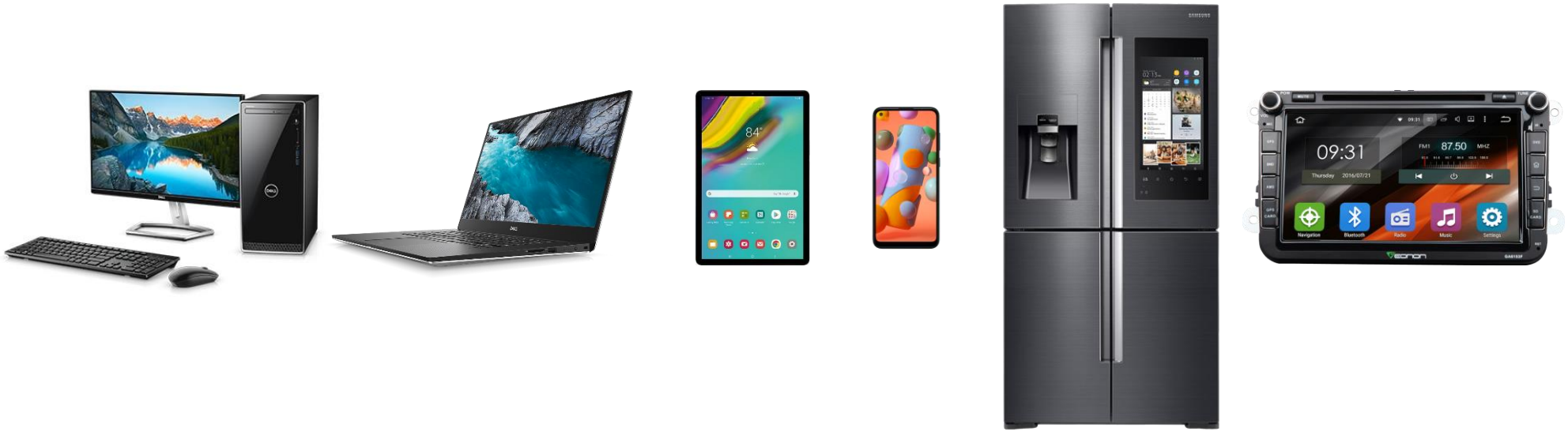
- Introduction
- Traditional Digital Computers
- Concept of Quantum Computers
- Quantum Computing
- Research Topics & Applications
- Conclusion

Introduction

- Digital computers have been popularized through their implementation in various devices that we use in our everyday routines

Introduction

- **Digital computers have been popularized through their implementation in various devices that we use in our everyday routines**



Introduction

- As digital computers gain more computational power, more software applications were developed to help every aspect of our lives
  - the ubiquity of computers in our daily lives makes digital computers even more popular
  - the thirst for more computing power is a good motivation to push the state of the arts further

Introduction

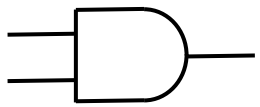
- One direction of pushing the state of the art in computational power is the concept of developing a quantum computer
  - the continuous state inside a quantum computer can simplify computation scheme and improve efficiency
  - faster computation will allow more sophisticated software application beyond imagination

Traditional Digital Computers

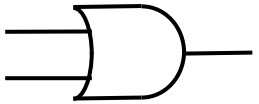
- Traditional digital computers were built based on hardware that can represent and process binary data
  - electronic components rely on using measurable electrical voltage to represent data
  - high voltage of 5V was used to represent a 1 and low voltage of 0V was used to represent a 0
  - electronic hardware was designed to have output of either 5V or 0V

Traditional Digital Computers

- Traditional digital computers were built around the basic digital circuits representing logical AND and logical OR operators



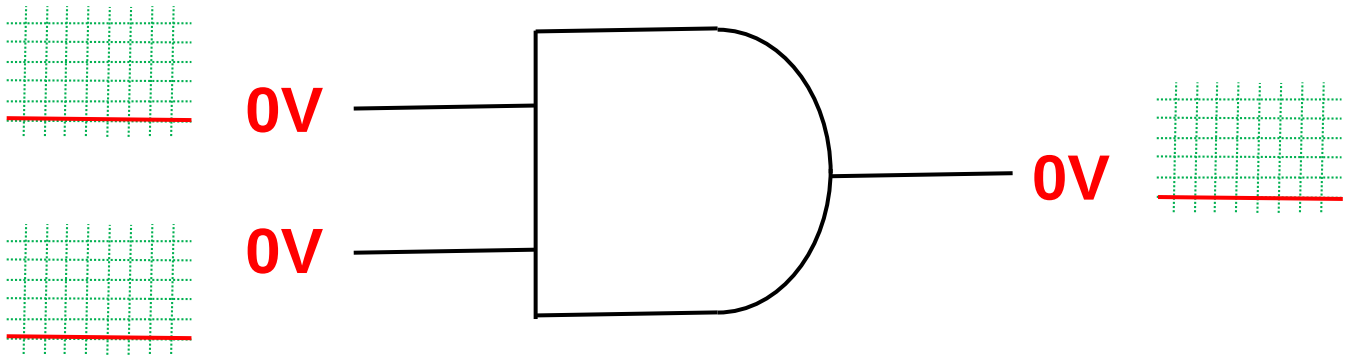
logical AND gate



logical OR gate

IEEE
UNITED STATES AIR FORCE ACADEMY
CYBERWORX

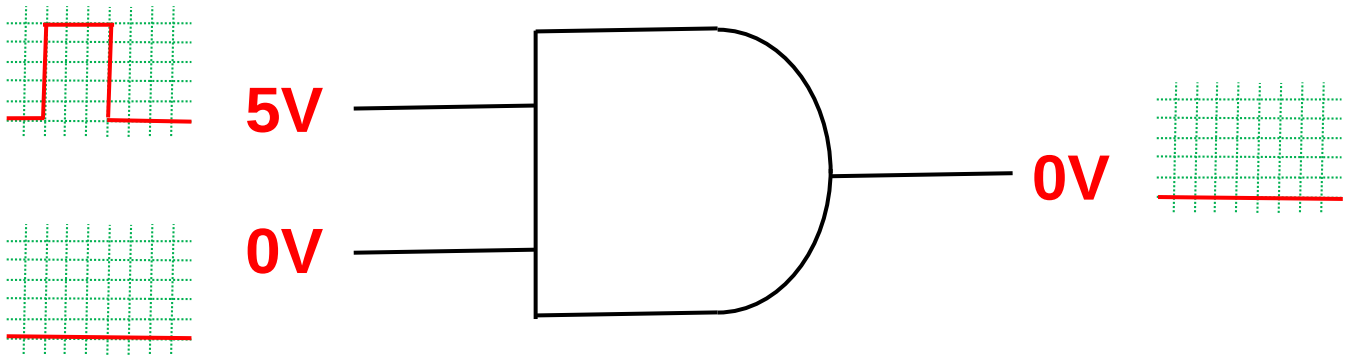
Traditional Digital Computers



logical AND gate

IEEE
UNITED STATES AIR FORCE ACADEMY
AIR FORCE CYBERWORX

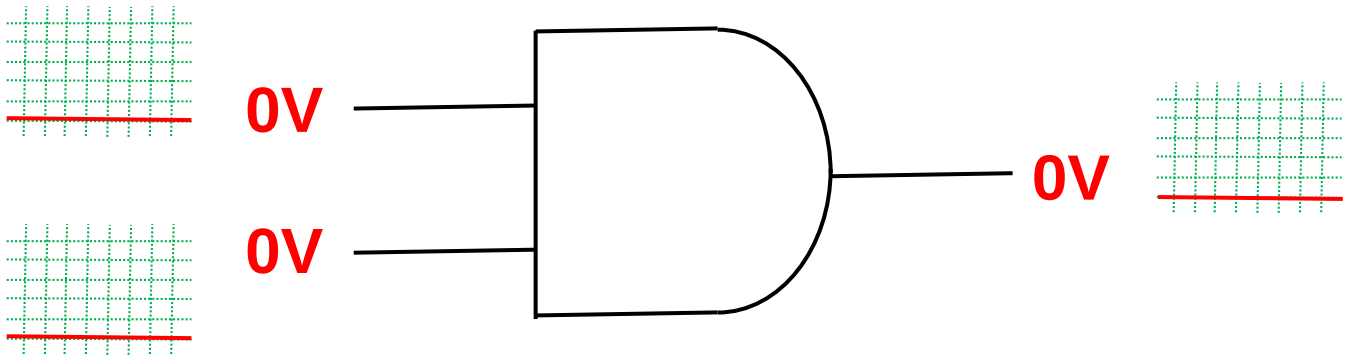
Traditional Digital Computers



logical AND gate

IEEE
UNITED STATES AIR FORCE ACADEMY
CYBERWORX

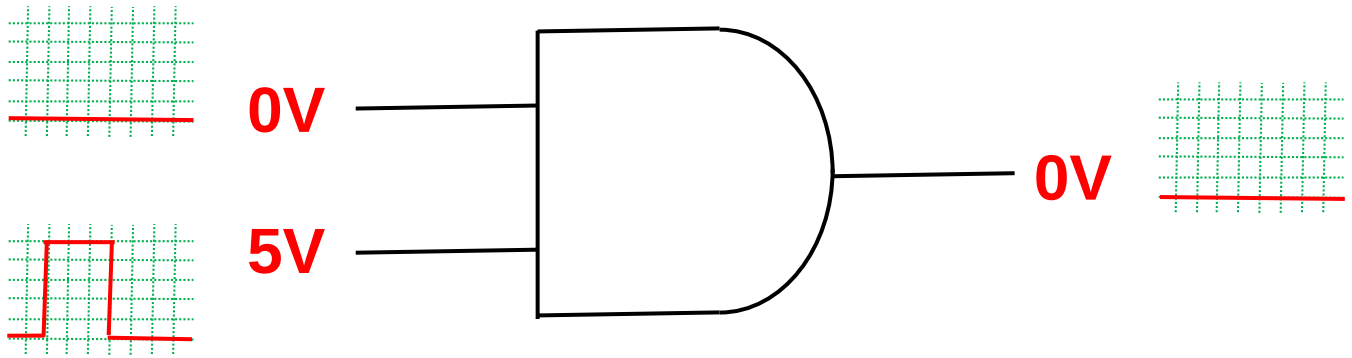
Traditional Digital Computers



logical AND gate

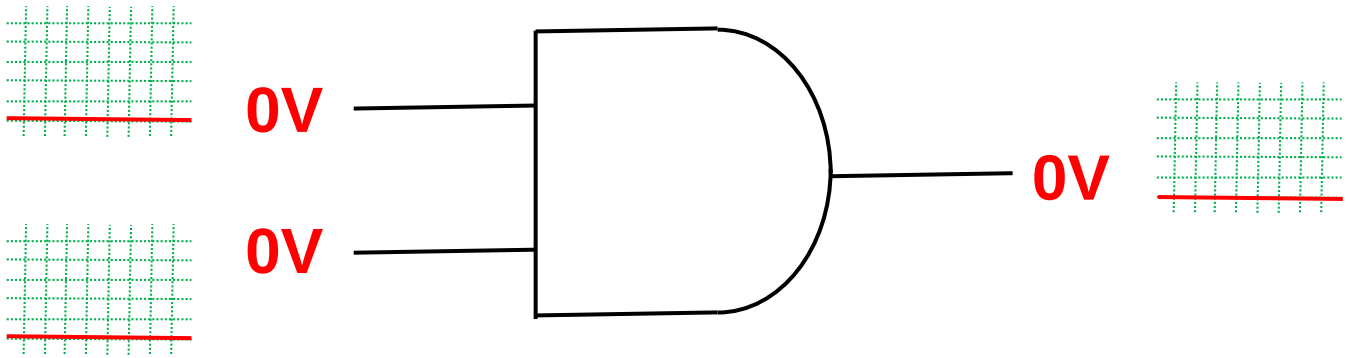
IEEE
UNITED STATES AIR FORCE ACADEMY
AIR FORCE CYBERWORX

Traditional Digital Computers



logical AND gate

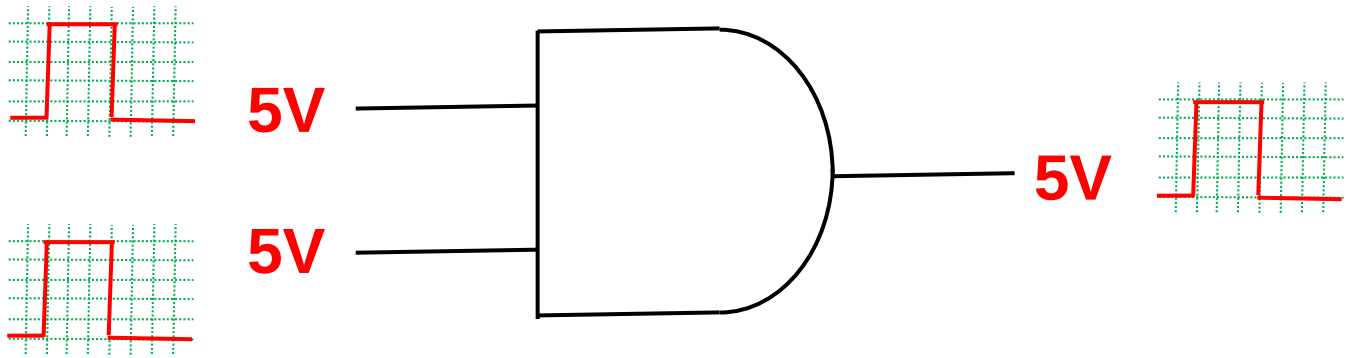
Traditional Digital Computers



logical AND gate

IEEE
UNITED STATES AIR FORCE ACADEMY
AIR FORCE CYBERWORX

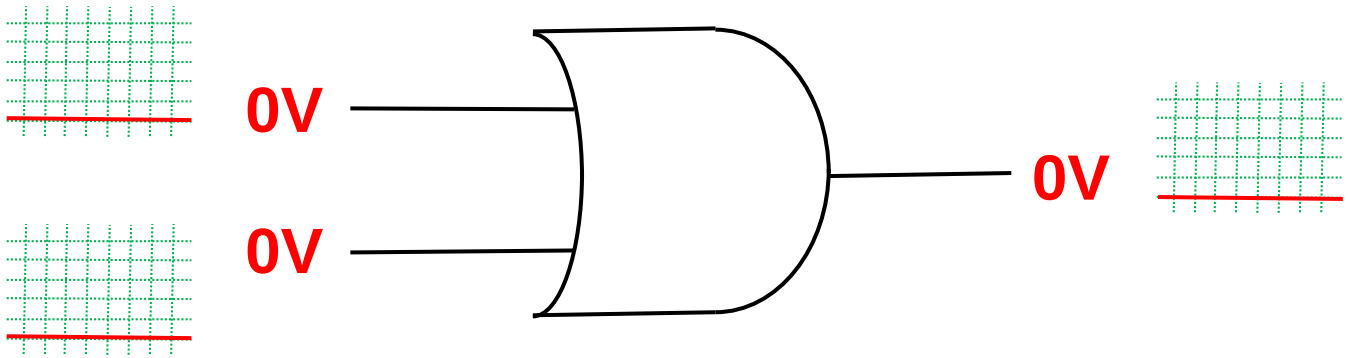
Traditional Digital Computers



logical AND gate

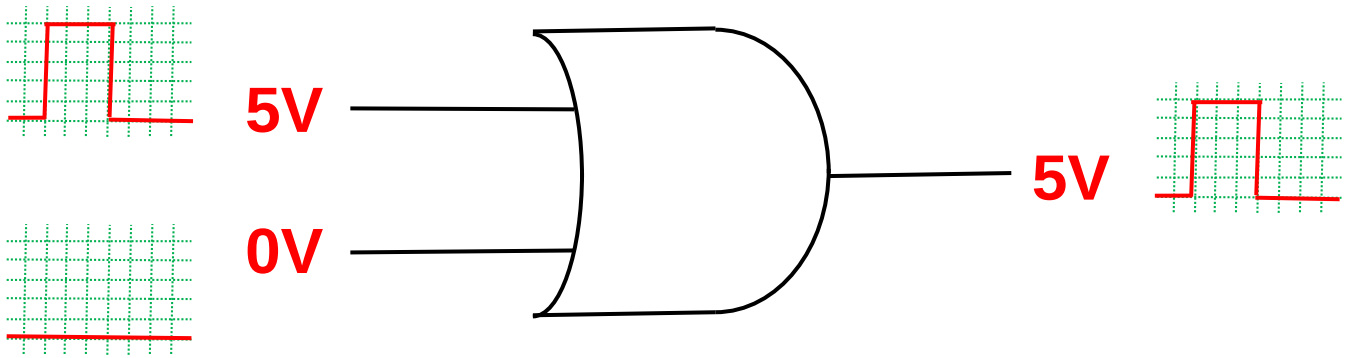
Traditional Digital Computers

Traditional Digital Computers



logical OR gate

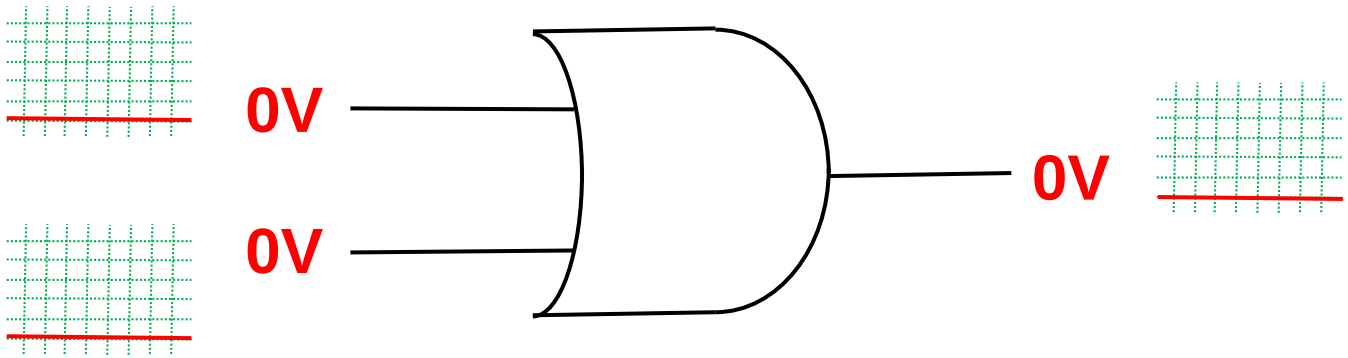
Traditional Digital Computers



logical OR gate

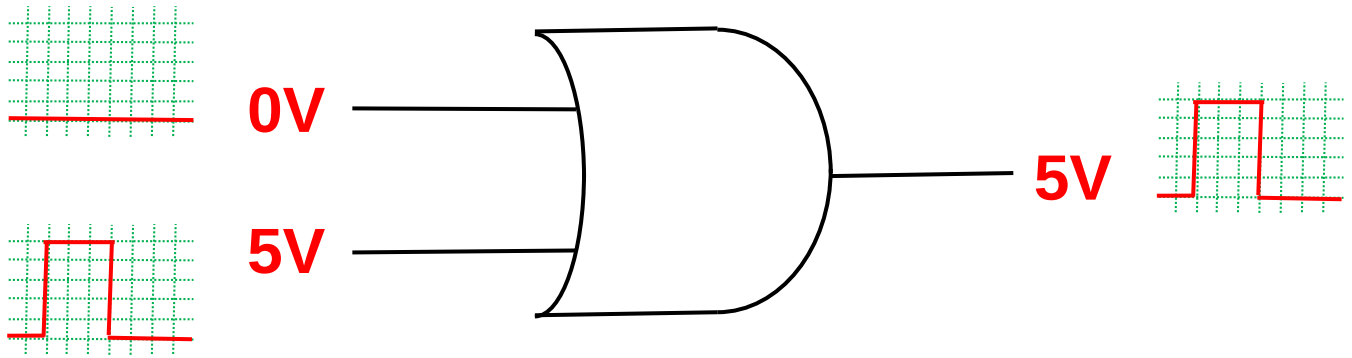
IEEE
UNITED STATES AIR FORCE ACADEMY
CYBERWORX

Traditional Digital Computers



logical OR gate

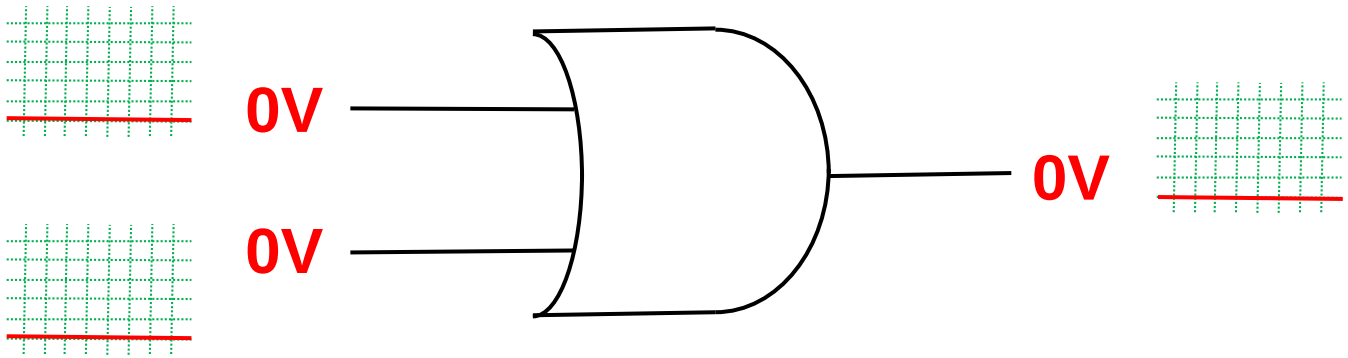
Traditional Digital Computers



logical OR gate

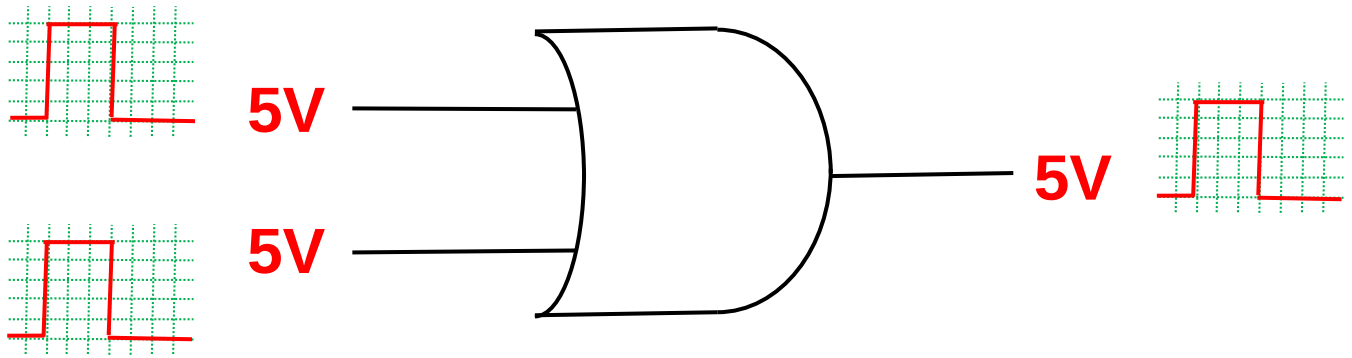
IEEE
UNITED STATES AIR FORCE ACADEMY
AIR FORCE CYBERWORX

Traditional Digital Computers



logical OR gate

Traditional Digital Computers



logical OR gate

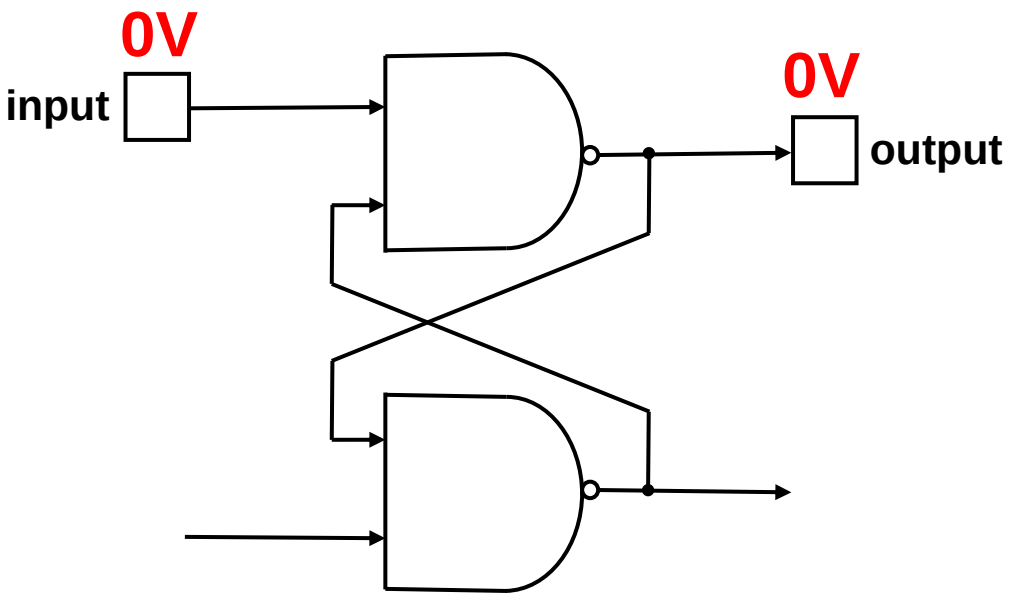
IEEE
UNITED STATES AIR FORCE ACADEMY
AIR FORCE CYBERWORX

Traditional Digital Computers

Traditional Digital Computers

- Logical AND gate and logical OR gates are combined to build:
  - flip-flop: a basic unit of memory
  - adder: basic unit of computation

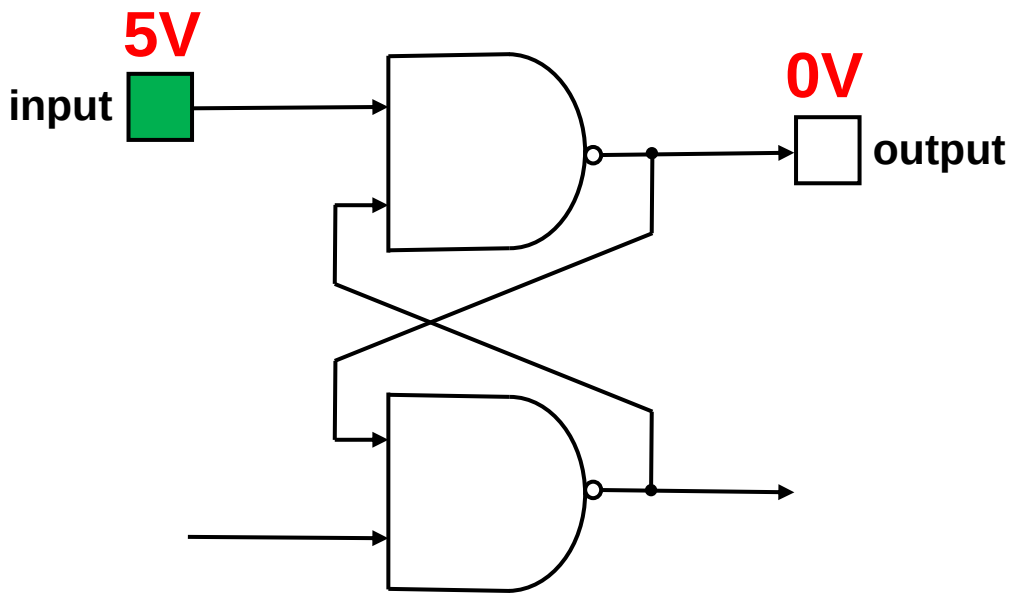
Traditional Digital Computers



flip-flop

IEEE
UNITED STATES AIR FORCE ACADEMY
CYBERWORX

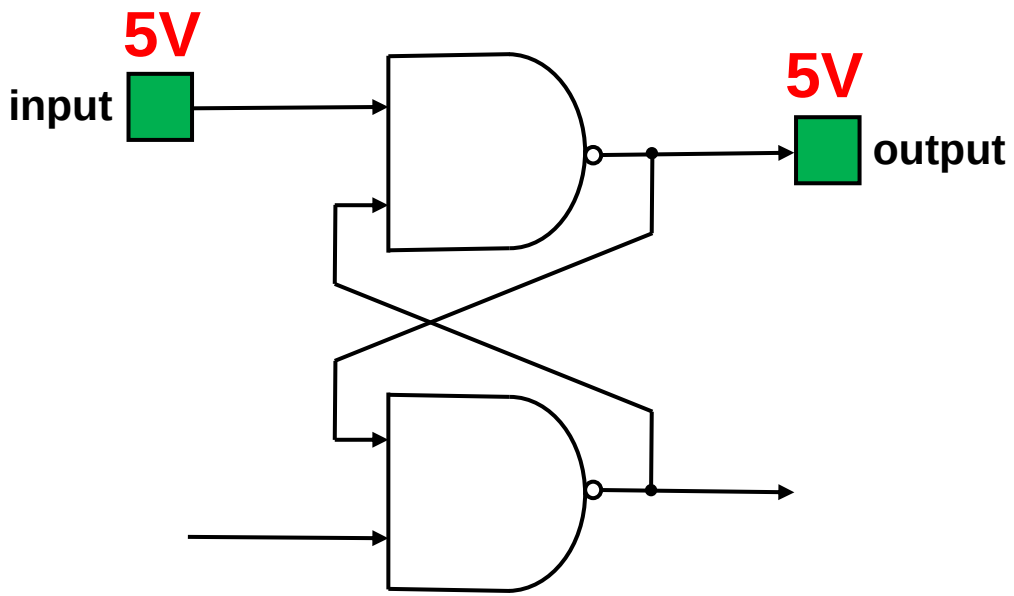
Traditional Digital Computers



flip-flop

IEEE
UNITED STATES AIR FORCE ACADEMY
CYBERWORX

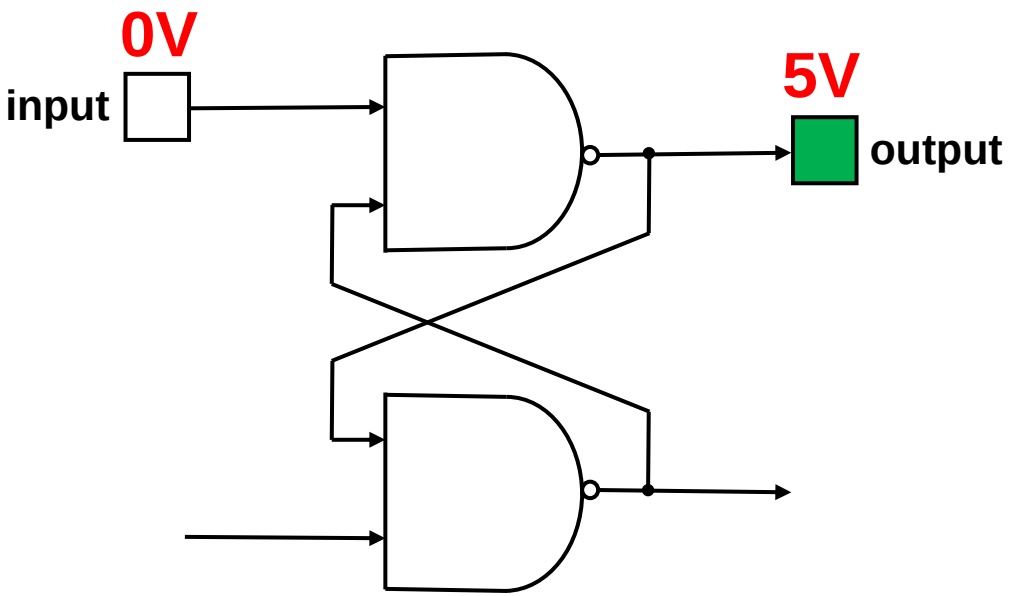
Traditional Digital Computers



flip-flop

IEEE
UNITED STATES AIR FORCE ACADEMY
CYBERWORX

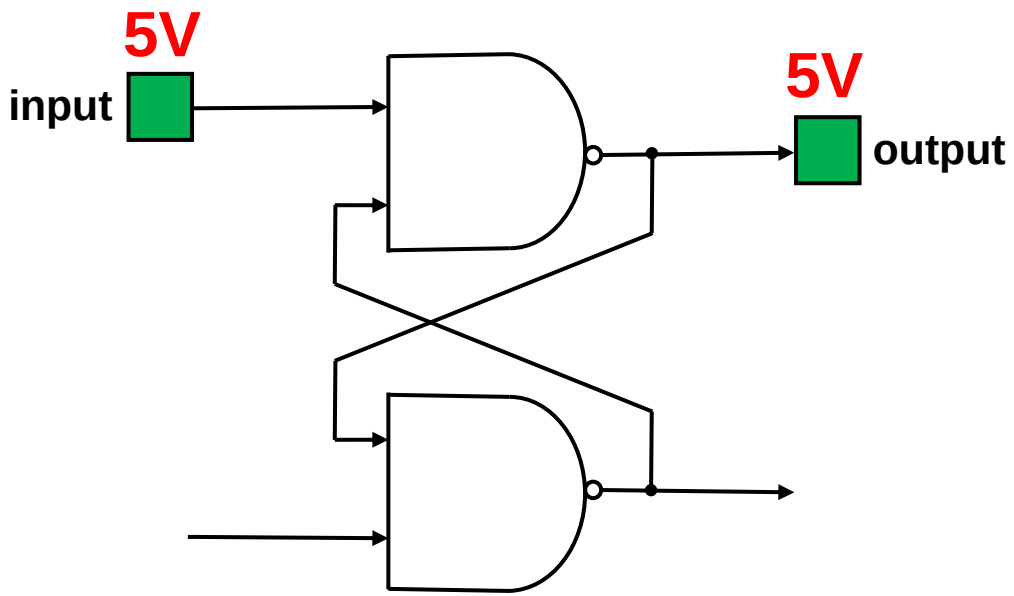
Traditional Digital Computers



flip-flop

IEEE
UNITED STATES AIR FORCE ACADEMY
AIR FORCE CYBERWORX

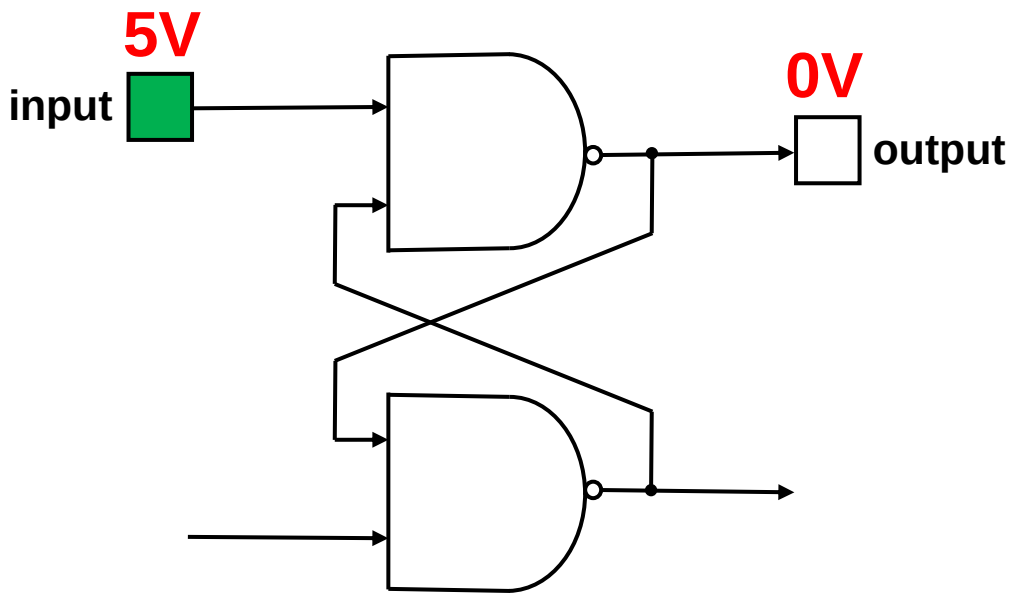
Traditional Digital Computers



flip-flop

IEEE
UNITED STATES AIR FORCE ACADEMY
CYBERWORX

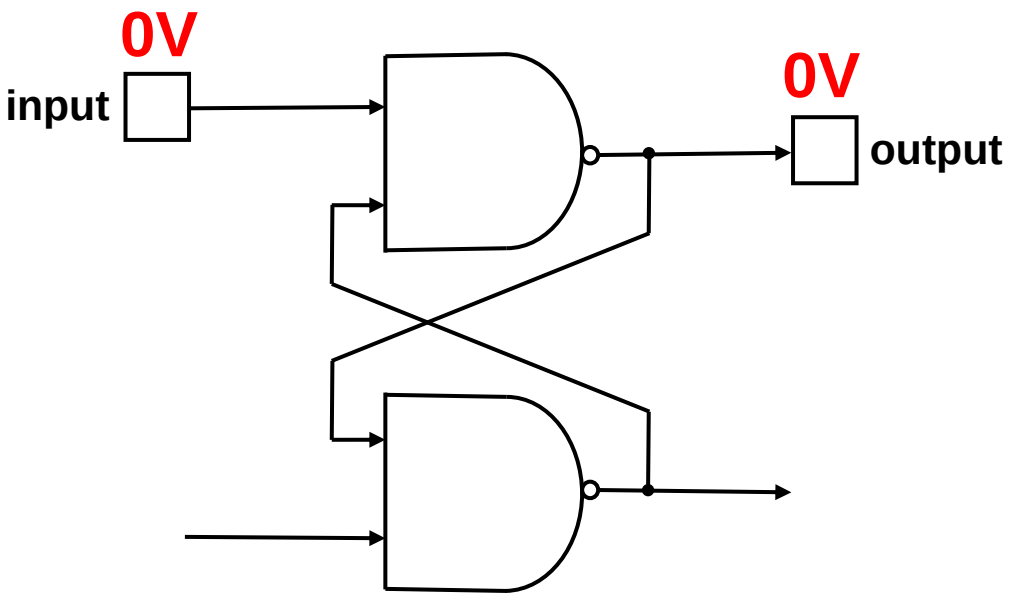
Traditional Digital Computers



flip-flop

IEEE
UNITED STATES AIR FORCE ACADEMY
CYBERWORX

Traditional Digital Computers

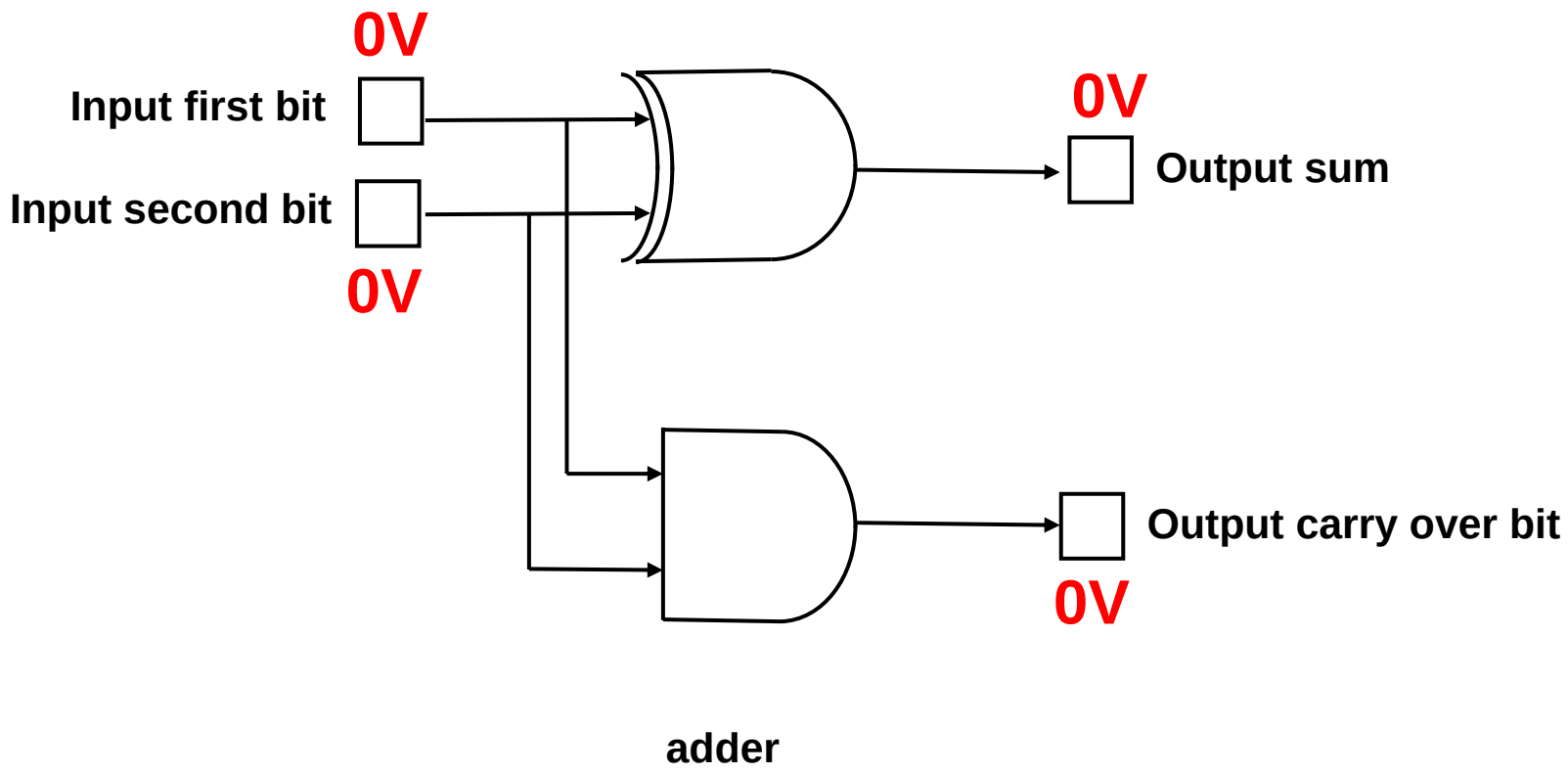


flip-flop

IEEE
UNITED STATES AIR FORCE ACADEMY
CYBERWORX

Traditional Digital Computers

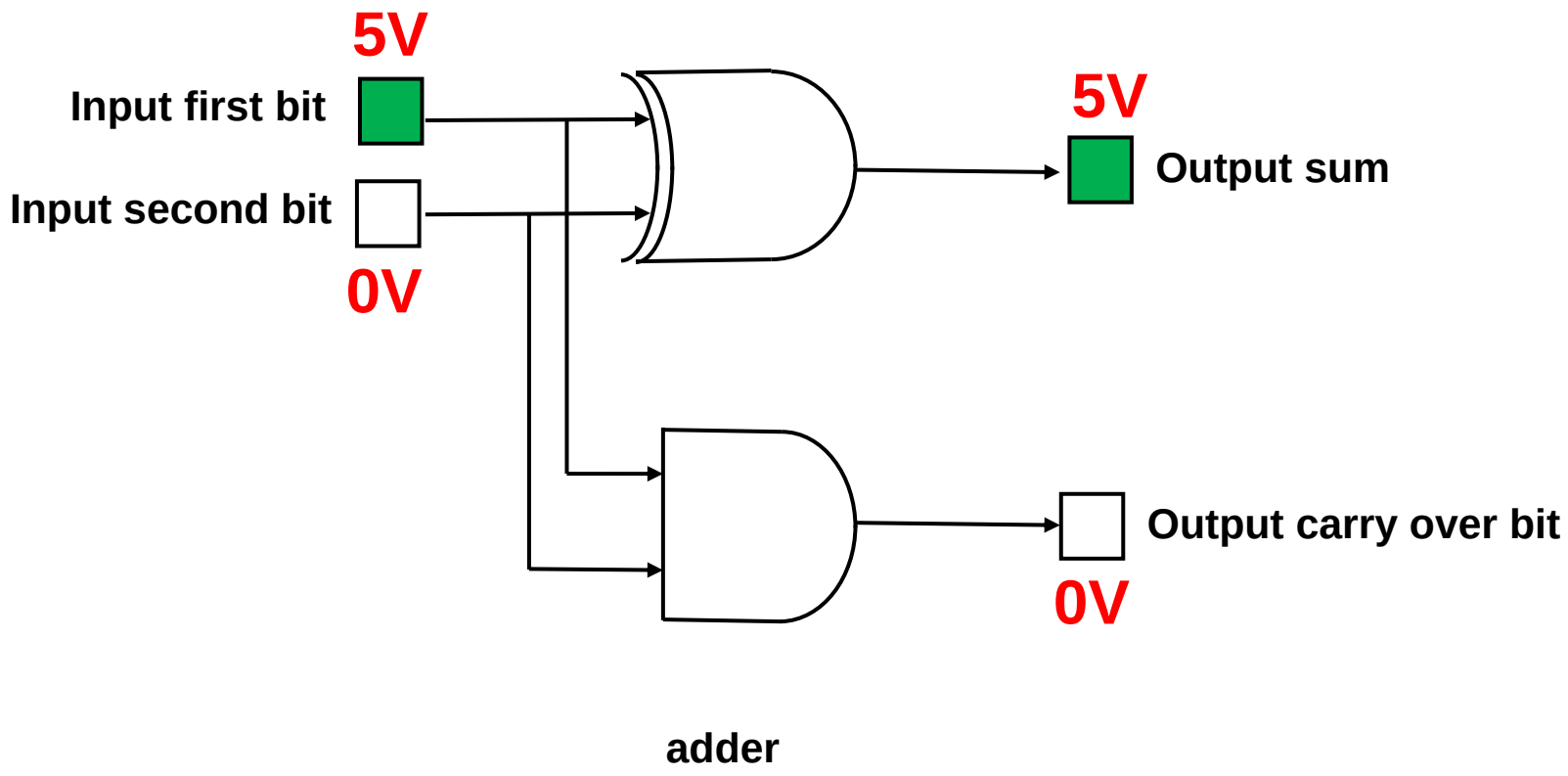
Traditional Digital Computers



adder

IEEE
UNITED STATES AIR FORCE ACADEMY
CYBERWORX

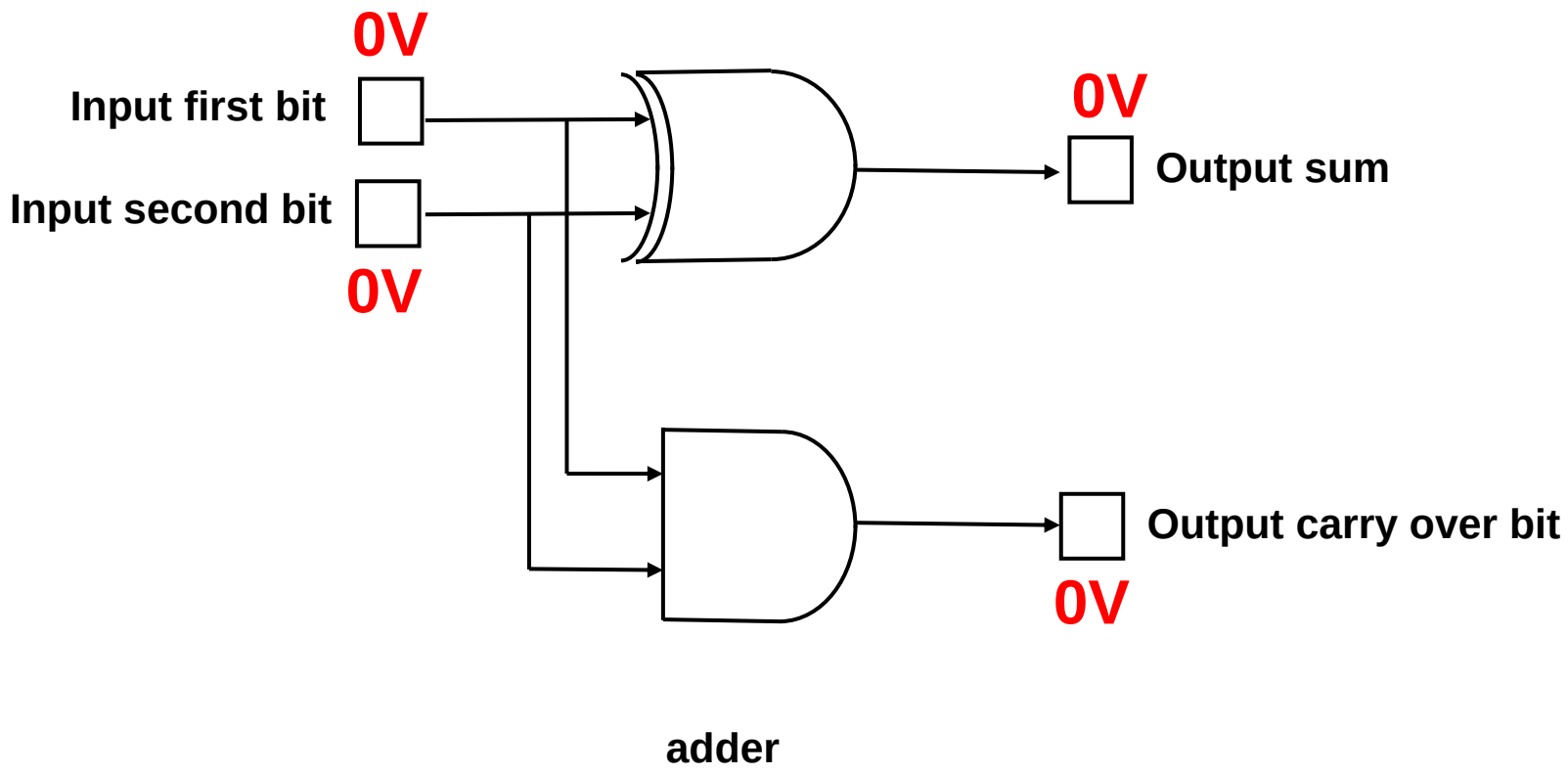
Traditional Digital Computers



adder

IEEE
UNITED STATES AIR FORCE ACADEMY
CYBERWORX

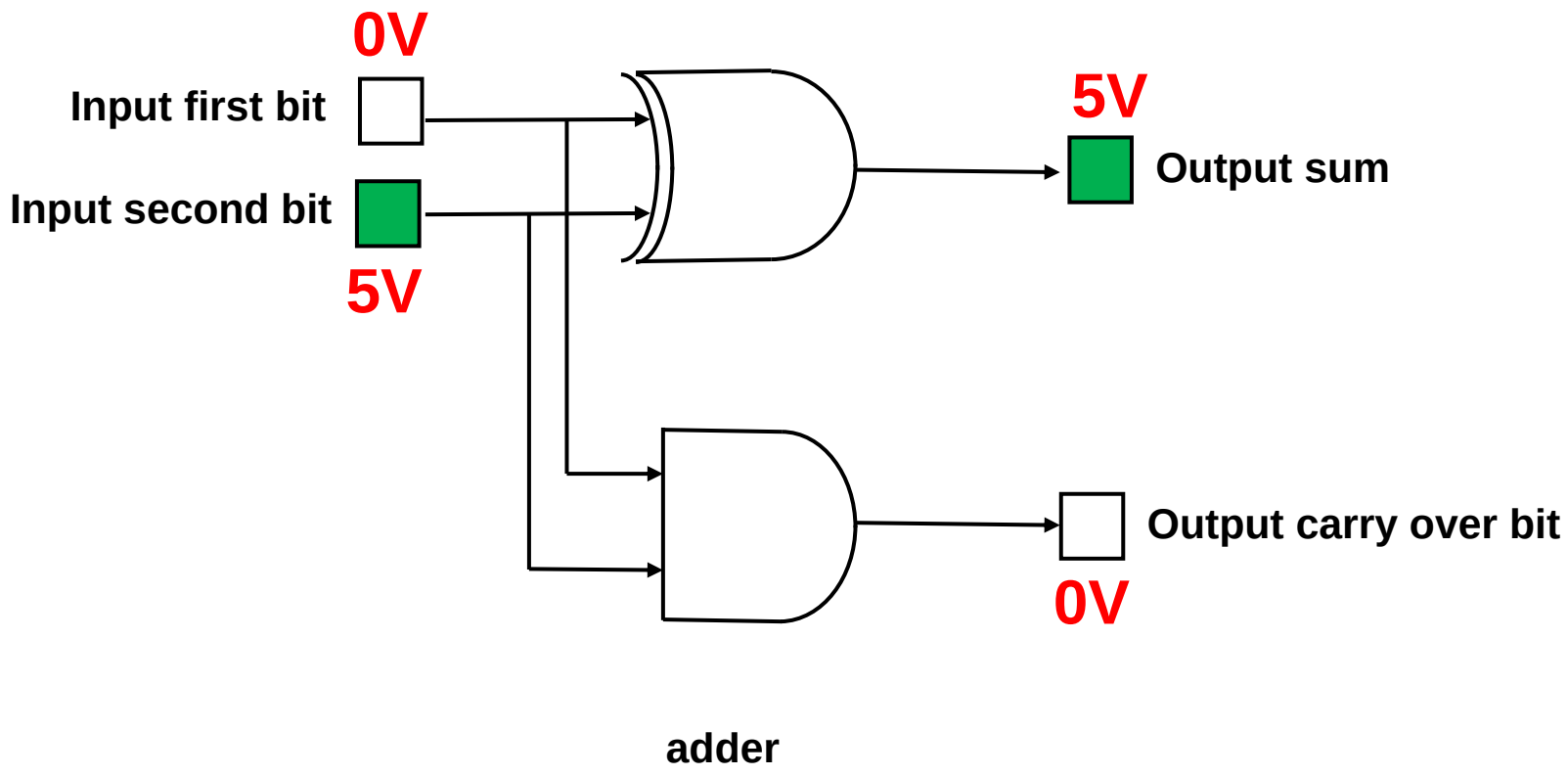
Traditional Digital Computers



adder

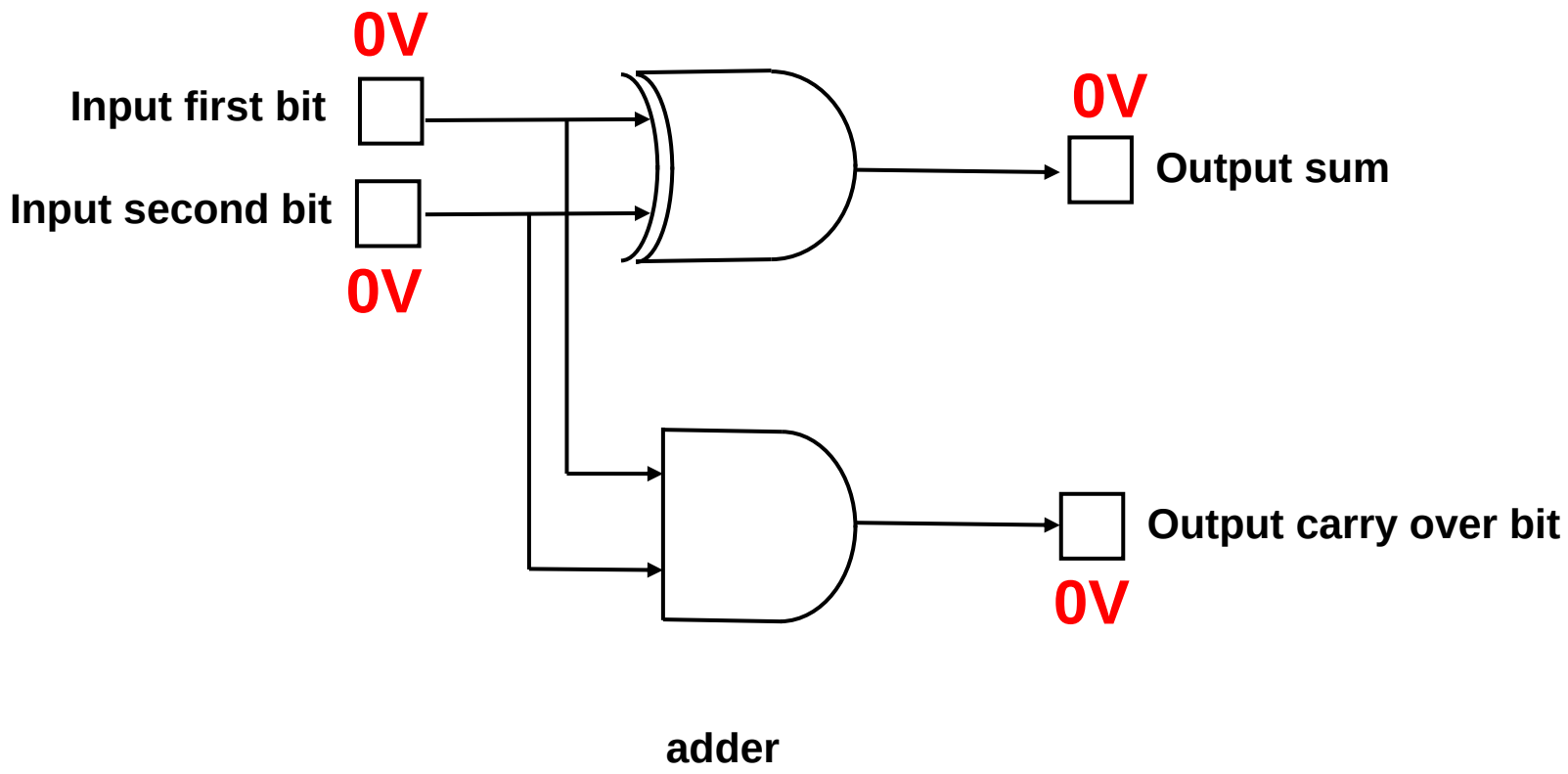
IEEE
UNITED STATES AIR FORCE ACADEMY
CYBERWORX

Traditional Digital Computers



IEEE
UNITED STATES AIR FORCE ACADEMY
CYBERWORX

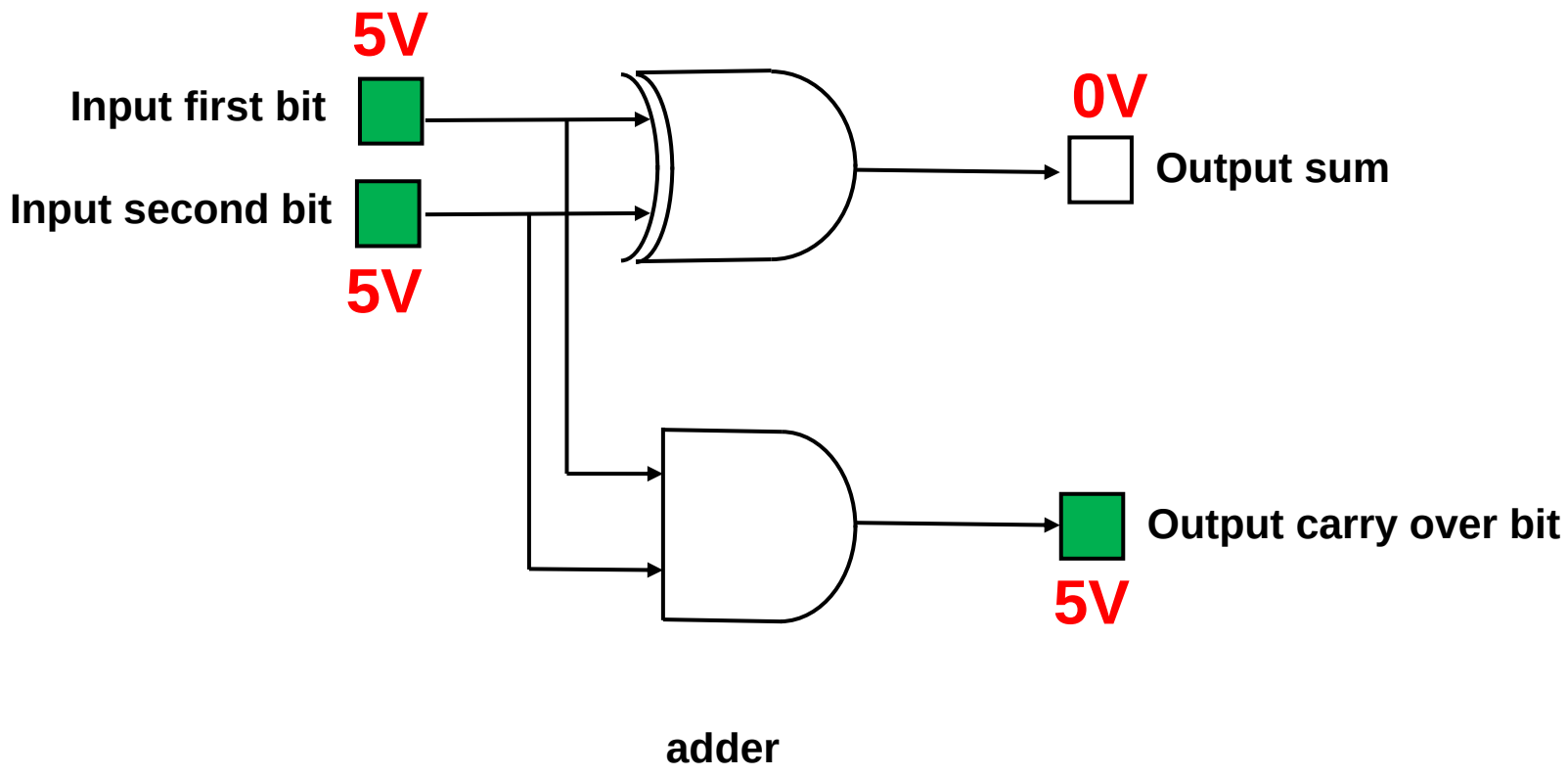
Traditional Digital Computers



adder

IEEE
UNITED STATES AIR FORCE ACADEMY
CYBERWORX

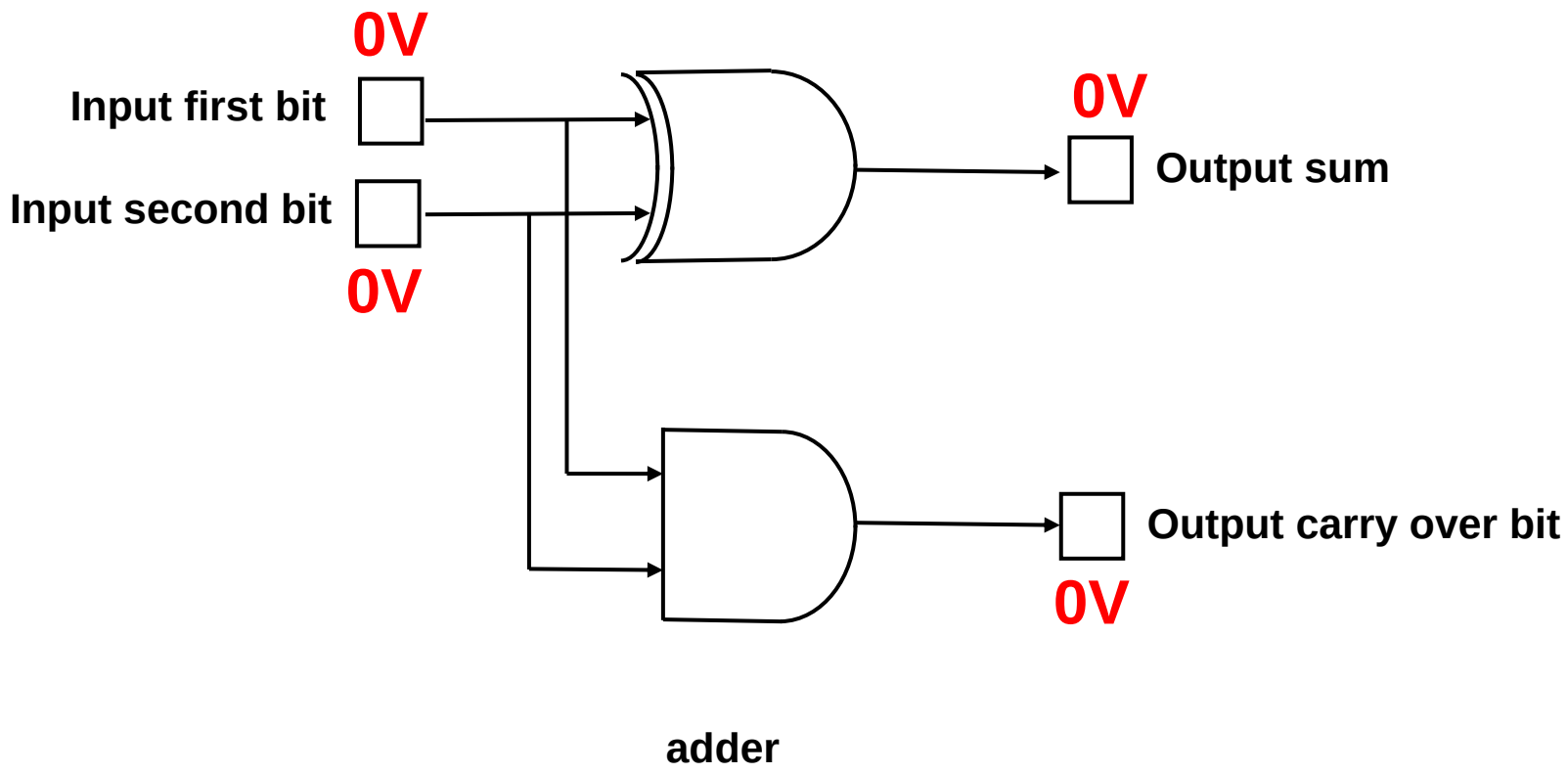
Traditional Digital Computers



adder

IEEE
UNITED STATES AIR FORCE ACADEMY
CYBERWORX

Traditional Digital Computers



adder

IEEE
UNITED STATES AIR FORCE ACADEMY
CYBERWORX

Traditional Digital Computers

Traditional Digital Computers

- Software was developed around a context-free language to instruct a digital computer of what to do
  - variable: an allocated memory area to hold data
  - operator: an instruction of what to do with the data stored in the variables

Traditional Digital Computers

```
main()
{
}
```

Traditional Digital Computers

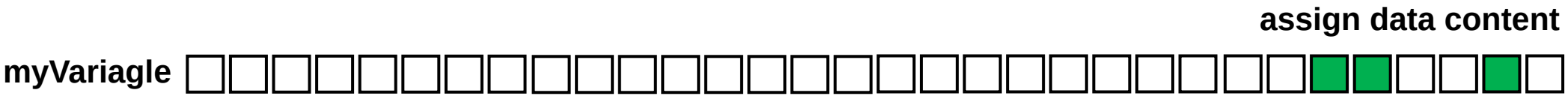
```
main()
{
   int myVariable = 50;
}
```

allocate memory 

IEEE
UNITED STATES AIR FORCE ACADEMY
AIR FORCE CYBERWORX

Traditional Digital Computers

```
main()
{
   int myVariable = 50;
}
```



IEEE
UNITED STATES AIR FORCE ACADEMY
CYBERWORX

Traditional Digital Computers

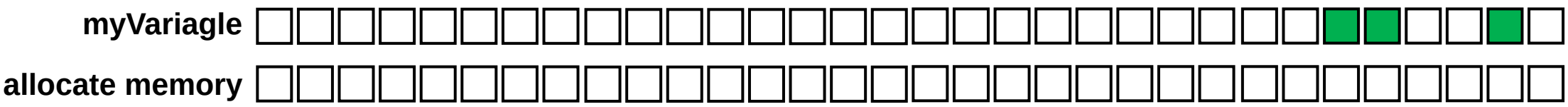
```
main()
{
   int myVariable = 50;
   int myResult = myVariable + 1;
}
```

myVariagle 

IEEE
UNITED STATES AIR FORCE ACADEMY
CYBERWORX

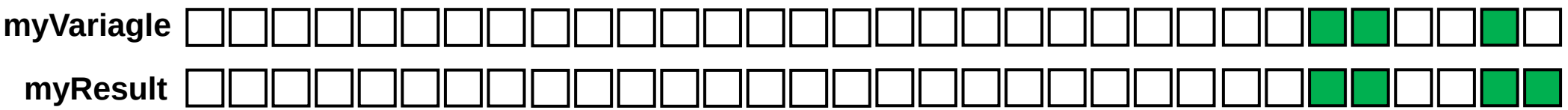
Traditional Digital Computers

```
main()
{
   int myVariable = 50;
   int myResult = myVariable + 1;
}
```



Traditional Digital Computers

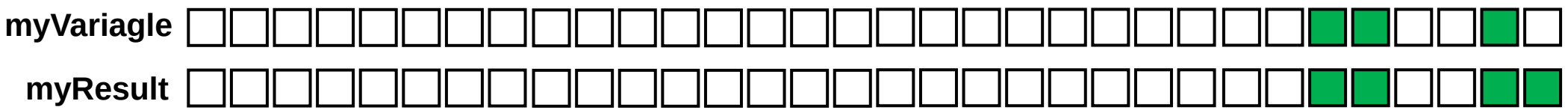
```
main()
{
   int myVariable = 50;
   int myResult = myVariable + 1;
}
```



IEEE
UNITED STATES AIR FORCE ACADEMY
CYBERWORX

Traditional Digital Computers

```
main()
{
   int myVariable = 50;
   int myResult = myVariable + 1;
   printf();
}
```



Traditional Digital Computers

- Traditional digital computers combine both hardware and software together so that
  - users see only an integrated product that can be configured according to the needs
  - the software platform can be updated automatically to improve the performance

Concept of Quantum Computers

Concept of Quantum Computers

- Quantum computers are computers that designed and built based on the hardware that can represent and process data in the quantum state
  - electronic components rely on using measurable electrical voltage to represent data
  - voltage can be varied between an acceptable range to represent data in the quantum state
  - electronic hardware was designed to accept, process, and produce data in the quantum state

Concept of Quantum Computers

- Quantum bit is the smallest unit of data in a quantum computer
  - a quantum bit consists of two parts representing the quantum states of the two binary outcomes
  - voltage can be varied between an acceptable range to represent data in the quantum state
  - electronic hardware was designed to accept, process, and produce data in the quantum state

Concept of Quantum Computers

- A quantum bit is represented by a linear combination of two orthogonal vectors $|0\rangle = [1 \;\; 0]^T$ and $|1\rangle = [0 \;\; 1]^T$

$$b_{quantum} = \alpha\,|0\rangle + \beta\,|1\rangle$$

Where α is the probability of $|0\rangle$ and β is the probability of $|1\rangle$, and

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

Concept of Quantum Computers

- Similar to logic gates in traditional digital computer, there are various gates designed for quantum computers
  - Pauli X gate: an equivalent of the NOT gate reversing the binary data
  - SWAP gate: swapping the two input quantum bits

Concept of Quantum Computers

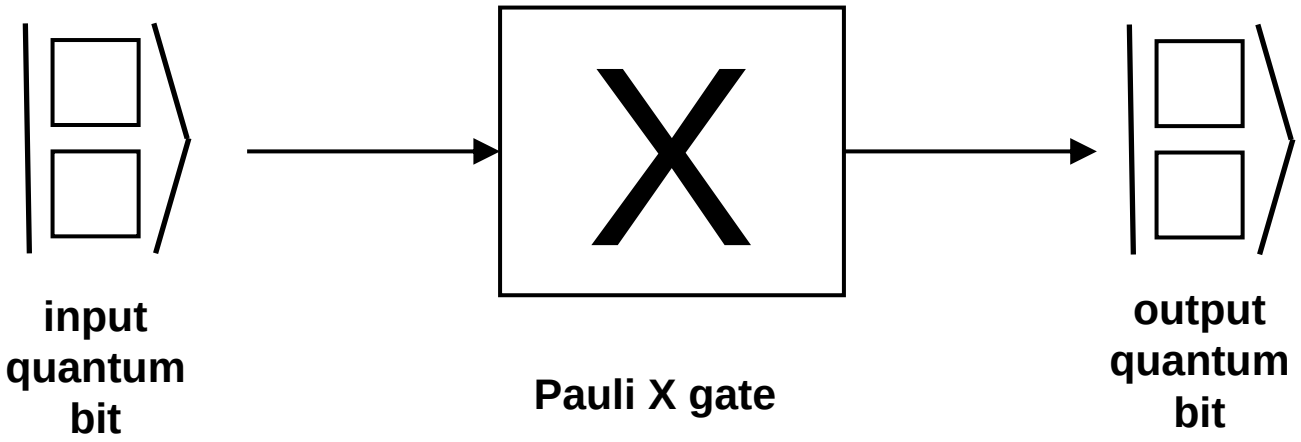
- Similar to logic gates in traditional digital computer, there are various gates designed for quantum computers
  - definitions of more gates can be found at

https://en.wikipedia.org/wiki/Quantum_logic_gate

Concept of Quantum Computers

Concept of Quantum Computers

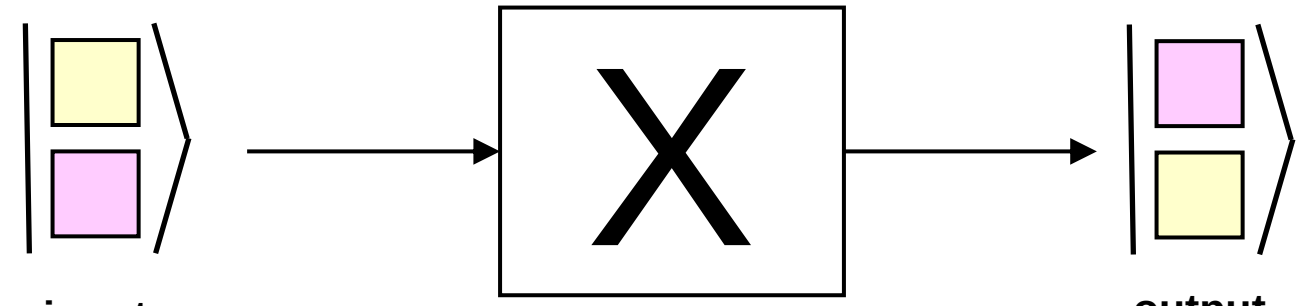
$$\begin{bmatrix} \alpha_{output} \\ \beta_{output} \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} \alpha_{input} \\ \beta_{input} \end{bmatrix}$$



IEEE
UNITED STATES AIR FORCE ACADEMY
CYBERWORX

Concept of Quantum Computers

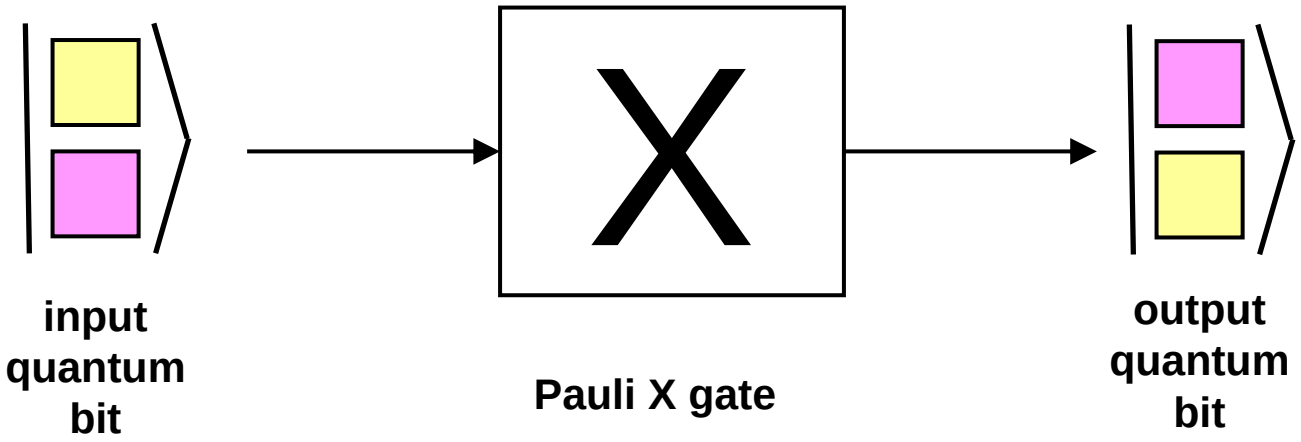
$$\begin{bmatrix} \alpha_{output} \\ \beta_{output} \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} \alpha_{input} \\ \beta_{input} \end{bmatrix}$$



IEEE
UNITED STATES AIR FORCE ACADEMY
CYBERWORX

Concept of Quantum Computers

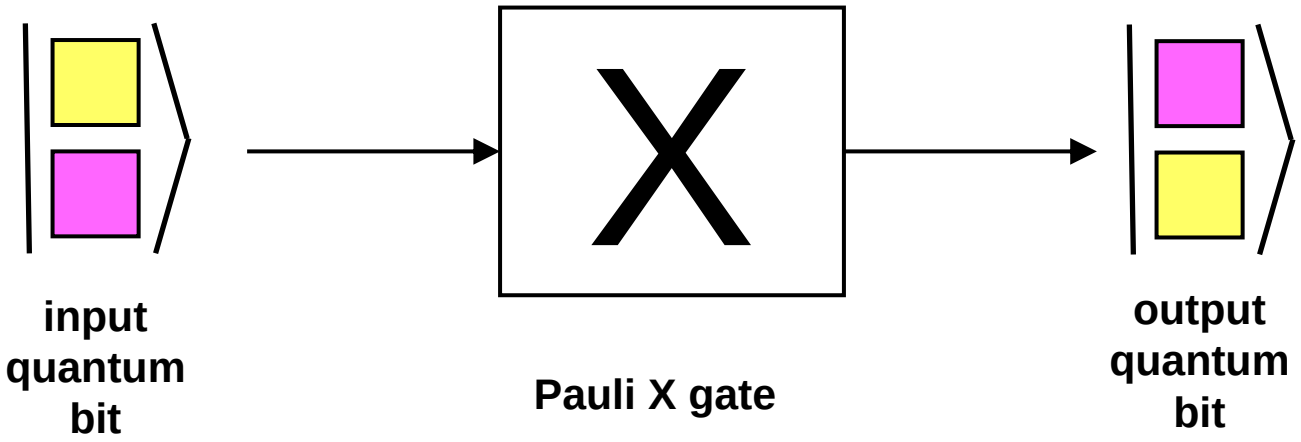
$$\begin{bmatrix} \alpha_{output} \\ \beta_{output} \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} \alpha_{input} \\ \beta_{input} \end{bmatrix}$$



IEEE
UNITED STATES AIR FORCE ACADEMY
CYBERWORX

Concept of Quantum Computers

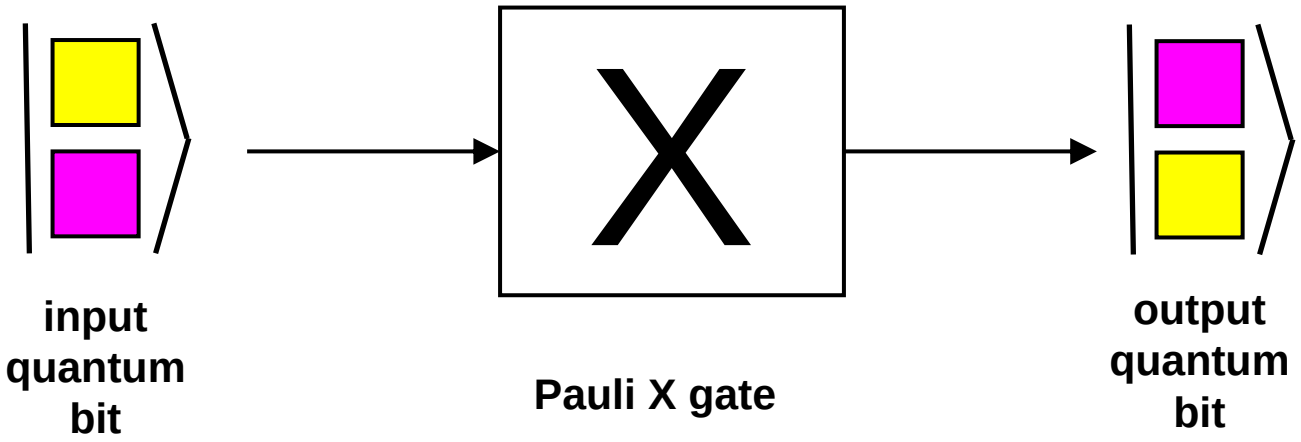
$$\begin{bmatrix} \alpha_{output} \\ \beta_{output} \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} \alpha_{input} \\ \beta_{input} \end{bmatrix}$$



IEEE
UNITED STATES AIR FORCE ACADEMY
CYBERWORX

Concept of Quantum Computers

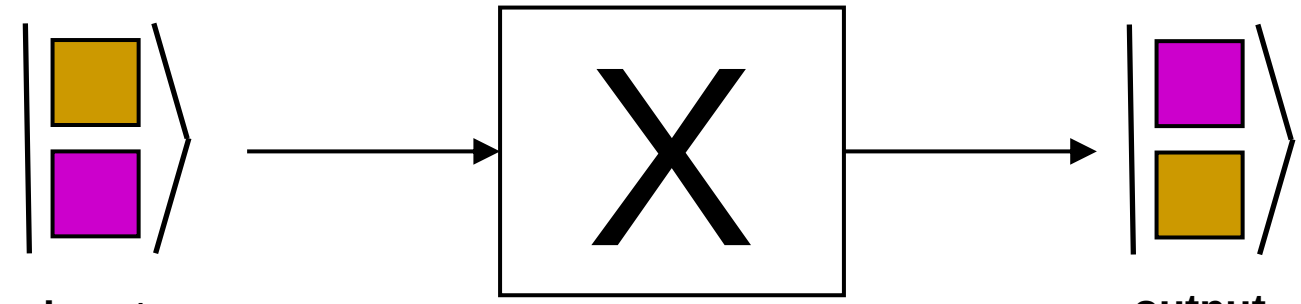
$$\begin{bmatrix} \alpha_{output} \\ \beta_{output} \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} \alpha_{input} \\ \beta_{input} \end{bmatrix}$$



IEEE
UNITED STATES AIR FORCE ACADEMY
CYBERWORX

Concept of Quantum Computers

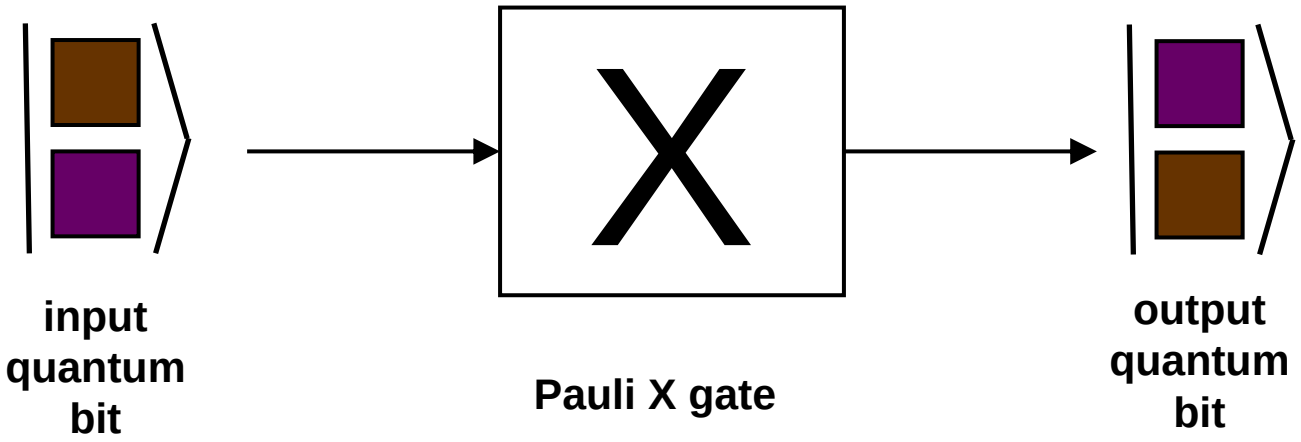
$$\begin{bmatrix} \alpha_{output} \\ \beta_{output} \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} \alpha_{input} \\ \beta_{input} \end{bmatrix}$$



IEEE
UNITED STATES AIR FORCE ACADEMY
CYBERWORX

Concept of Quantum Computers

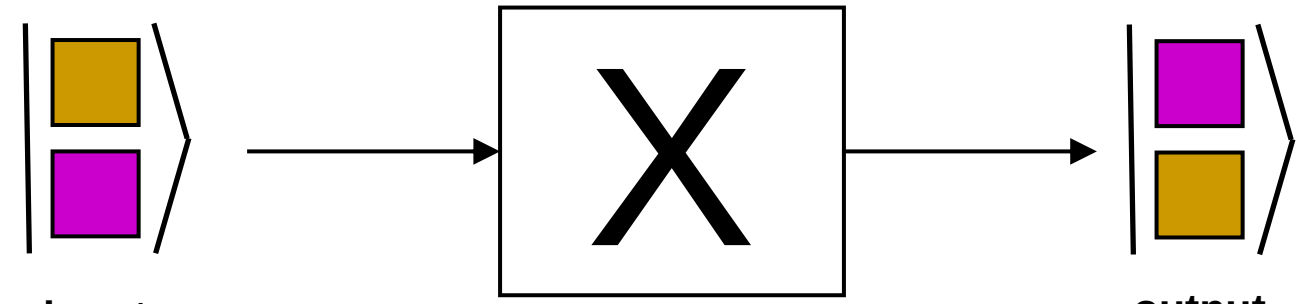
$$\begin{bmatrix} \alpha_{output} \\ \beta_{output} \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} \alpha_{input} \\ \beta_{input} \end{bmatrix}$$



IEEE
UNITED STATES AIR FORCE ACADEMY
CYBERWORX

Concept of Quantum Computers

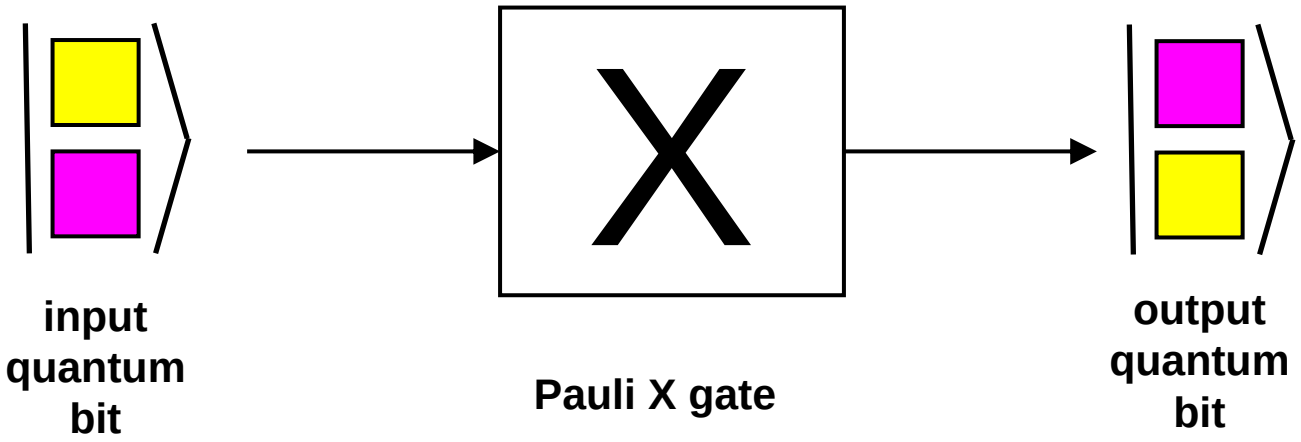
$$\begin{bmatrix} \alpha_{output} \\ \beta_{output} \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} \alpha_{input} \\ \beta_{input} \end{bmatrix}$$



IEEE
UNITED STATES AIR FORCE ACADEMY
CYBERWORX

Concept of Quantum Computers

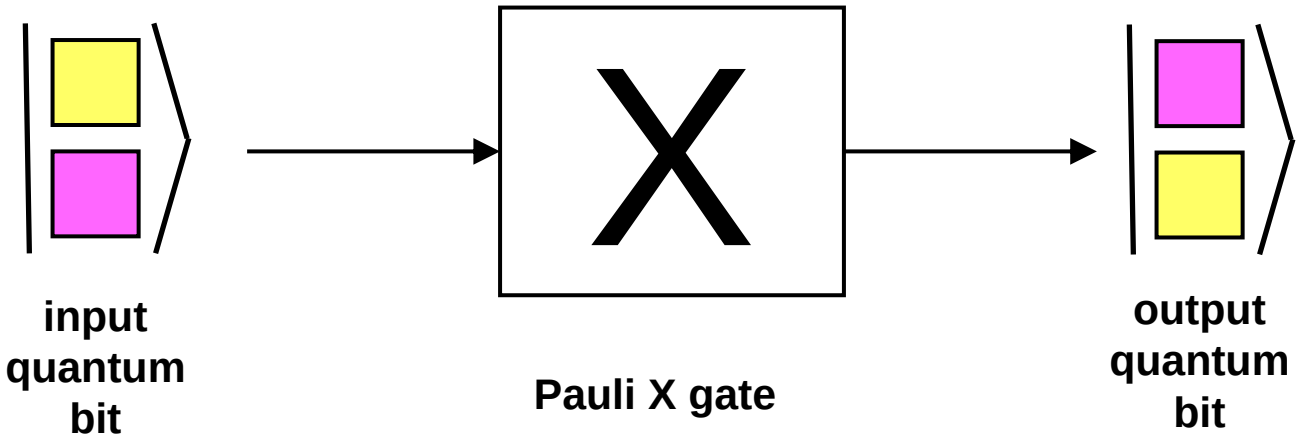
$$\begin{bmatrix} \alpha_{output} \\ \beta_{output} \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} \alpha_{input} \\ \beta_{input} \end{bmatrix}$$



IEEE
UNITED STATES AIR FORCE ACADEMY
CYBERWORX

Concept of Quantum Computers

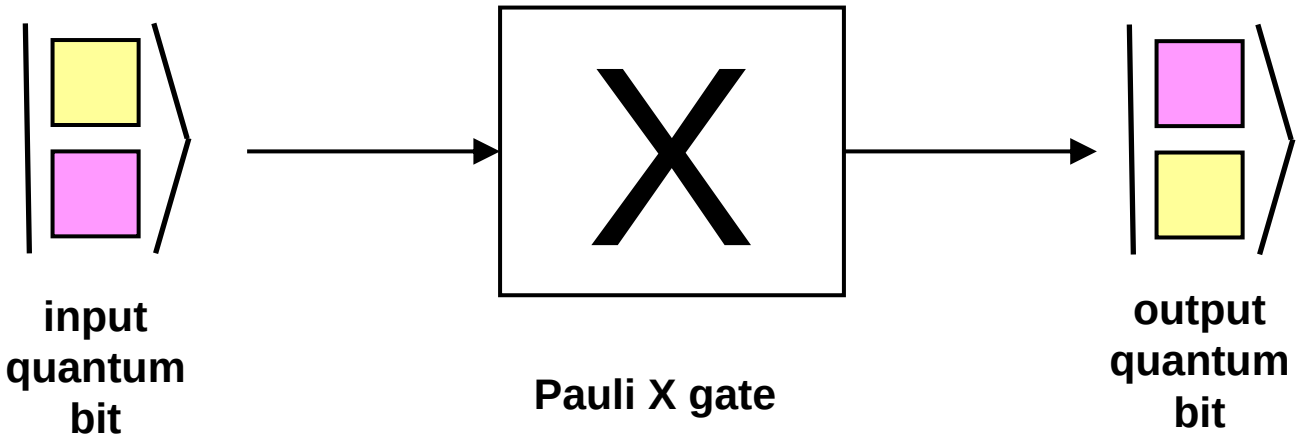
$$\begin{bmatrix} \alpha_{output} \\ \beta_{output} \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} \alpha_{input} \\ \beta_{input} \end{bmatrix}$$



IEEE
UNITED STATES AIR FORCE ACADEMY
CYBERWORX

Concept of Quantum Computers

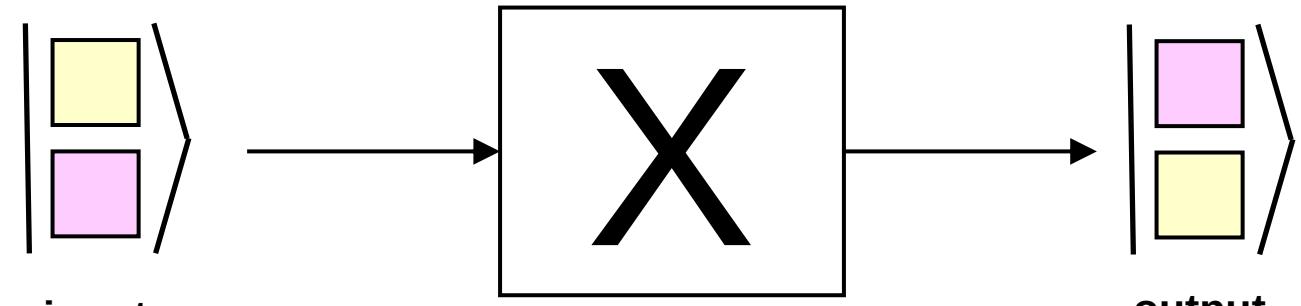
$$\begin{bmatrix} \alpha_{output} \\ \beta_{output} \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} \alpha_{input} \\ \beta_{input} \end{bmatrix}$$



IEEE
UNITED STATES AIR FORCE ACADEMY
CYBERWORX

Concept of Quantum Computers

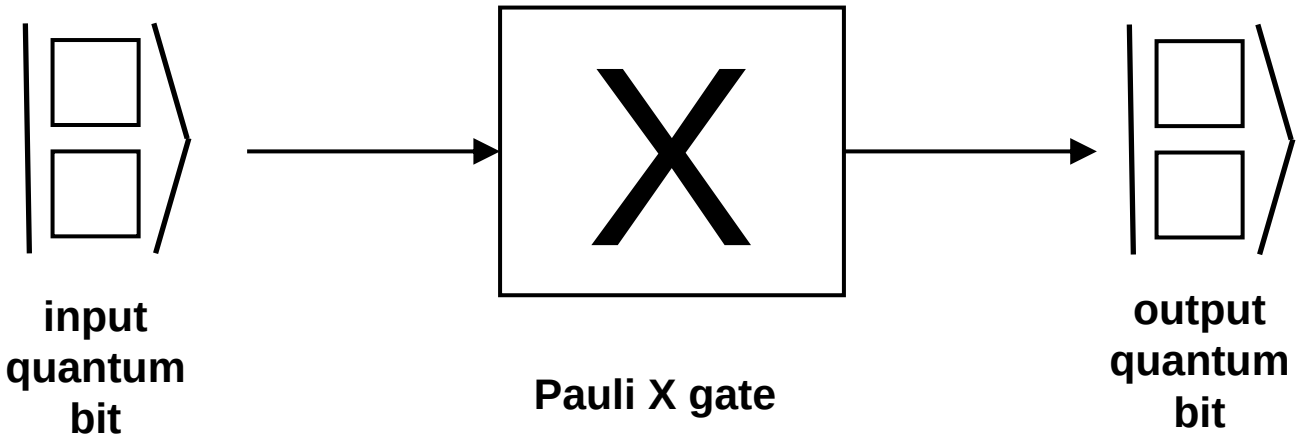
$$\begin{bmatrix} \alpha_{output} \\ \beta_{output} \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} \alpha_{input} \\ \beta_{input} \end{bmatrix}$$



IEEE
UNITED STATES AIR FORCE ACADEMY
CYBERWORX

Concept of Quantum Computers

$$\begin{bmatrix} \alpha_{output} \\ \beta_{output} \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} \alpha_{input} \\ \beta_{input} \end{bmatrix}$$



IEEE
UNITED STATES AIR FORCE ACADEMY
CYBERWORX

Concept of Quantum Computers

Concept of Quantum Computers

$$\begin{bmatrix} \alpha_{input,1} \\ \beta_{input,1} \end{bmatrix}$$

$$\begin{bmatrix} \alpha_{input,2} \\ \beta_{input,2} \end{bmatrix}$$

combining two quantum bits into a vector for mathematical calculation

IEEE
UNITED STATES AIR FORCE ACADEMY
AIR FORCE CYBERWORX

Concept of Quantum Computers

$$\begin{bmatrix} \alpha_{input,1} \\ \beta_{input,1} \end{bmatrix} \begin{bmatrix} \alpha_{input,2} \\ \beta_{input,2} \end{bmatrix} \rightarrow \begin{bmatrix} \alpha_{input,1} \begin{bmatrix} \alpha_{input,2} \\ \beta_{input,2} \end{bmatrix} \\ \beta_{input,1} \begin{bmatrix} \alpha_{input,2} \\ \beta_{input,2} \end{bmatrix} \end{bmatrix}$$

combining two quantum bits into a vector for mathematical calculation

IEEE
UNITED STATES AIR FORCE ACADEMY
CYBERWORX

Concept of Quantum Computers

$$\begin{bmatrix} \alpha_{input,1} \\ \beta_{input,1} \end{bmatrix} \begin{bmatrix} \alpha_{input,2} \\ \beta_{input,2} \end{bmatrix} \rightarrow \begin{bmatrix} \alpha_{input,1} \begin{bmatrix} \alpha_{input,2} \\ \beta_{input,2} \end{bmatrix} \\ \beta_{input,1} \begin{bmatrix} \alpha_{input,2} \\ \beta_{input,2} \end{bmatrix} \end{bmatrix} = \begin{bmatrix} \alpha_{input,1}\alpha_{input,2} \\ \alpha_{input,1}\beta_{input,2} \\ \beta_{input,1}\alpha_{input,2} \\ \beta_{input,1}\beta_{input,2} \end{bmatrix}$$

combining two quantum bits into a vector for mathematical calculation

IEEE
UNITED STATES AIR FORCE ACADEMY
CYBERWORX

Concept of Quantum Computers

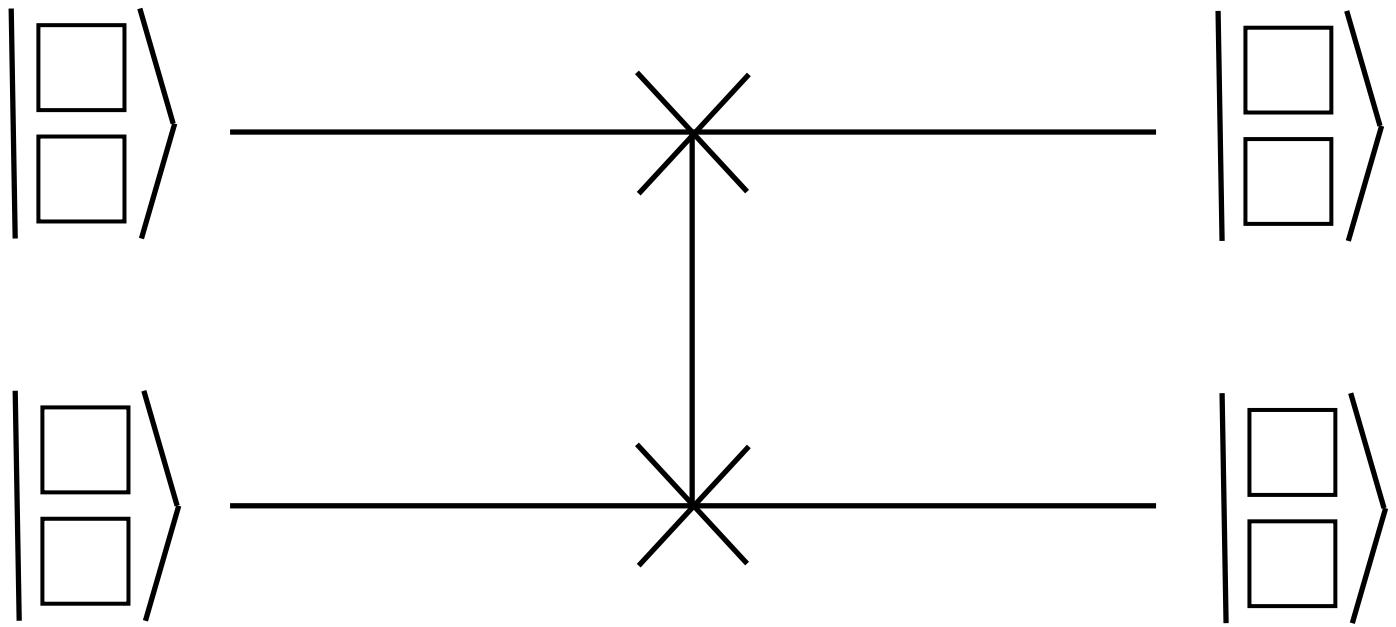
$$\begin{bmatrix} V_{output,00} \\ V_{output,01} \\ V_{output,10} \\ V_{output,11} \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} V_{input,00} \\ V_{input,01} \\ V_{input,10} \\ V_{input,11} \end{bmatrix}$$

mathematical representation of SWAP gate

IEEE
UNITED STATES AIR FORCE ACADEMY
CYBERWORX

Concept of Quantum Computers

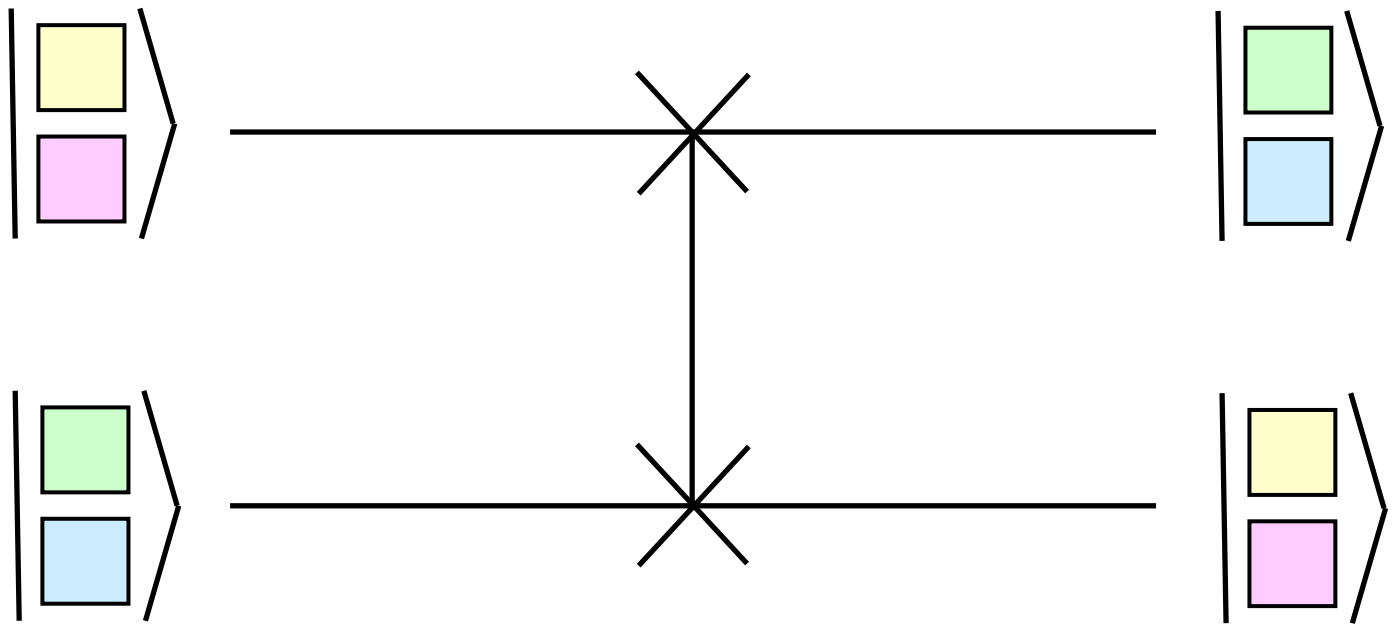
Concept of Quantum Computers



graphical representation of SWAP gate

IEEE
UNITED STATES AIR FORCE ACADEMY
CYBERWORX

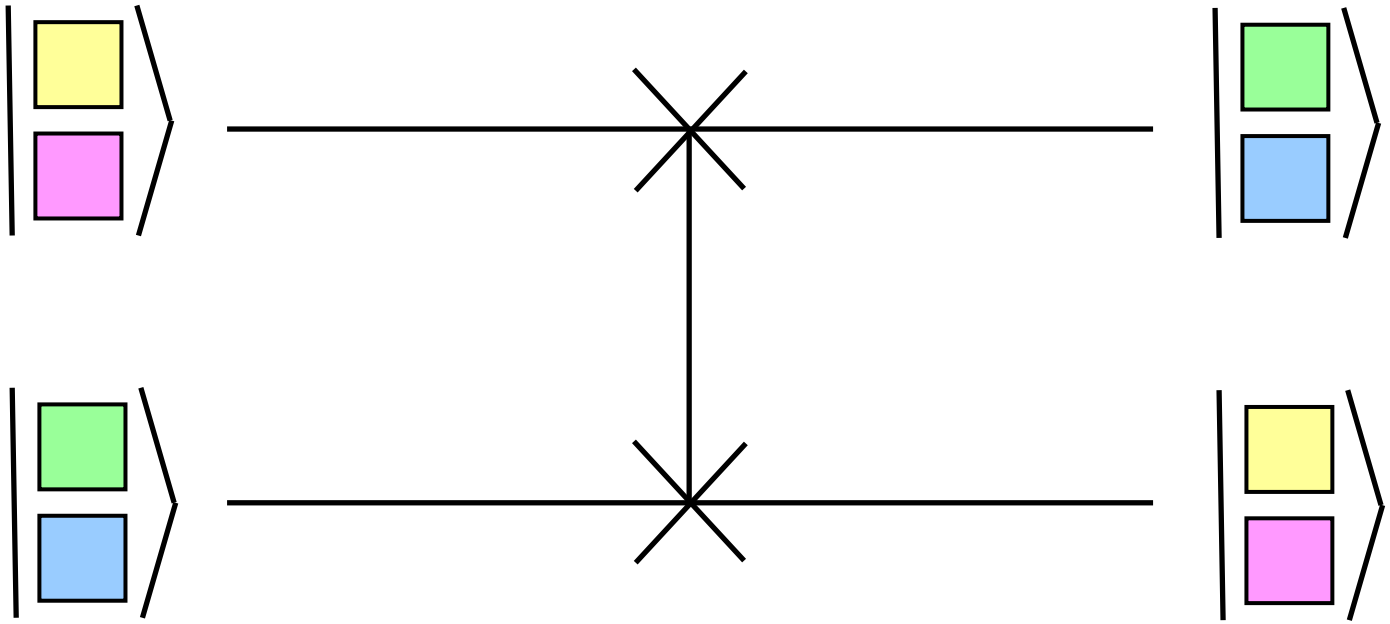
Concept of Quantum Computers



graphical representation of
SWAP gate

IEEE
UNITED STATES AIR FORCE ACADEMY
CYBERWORX

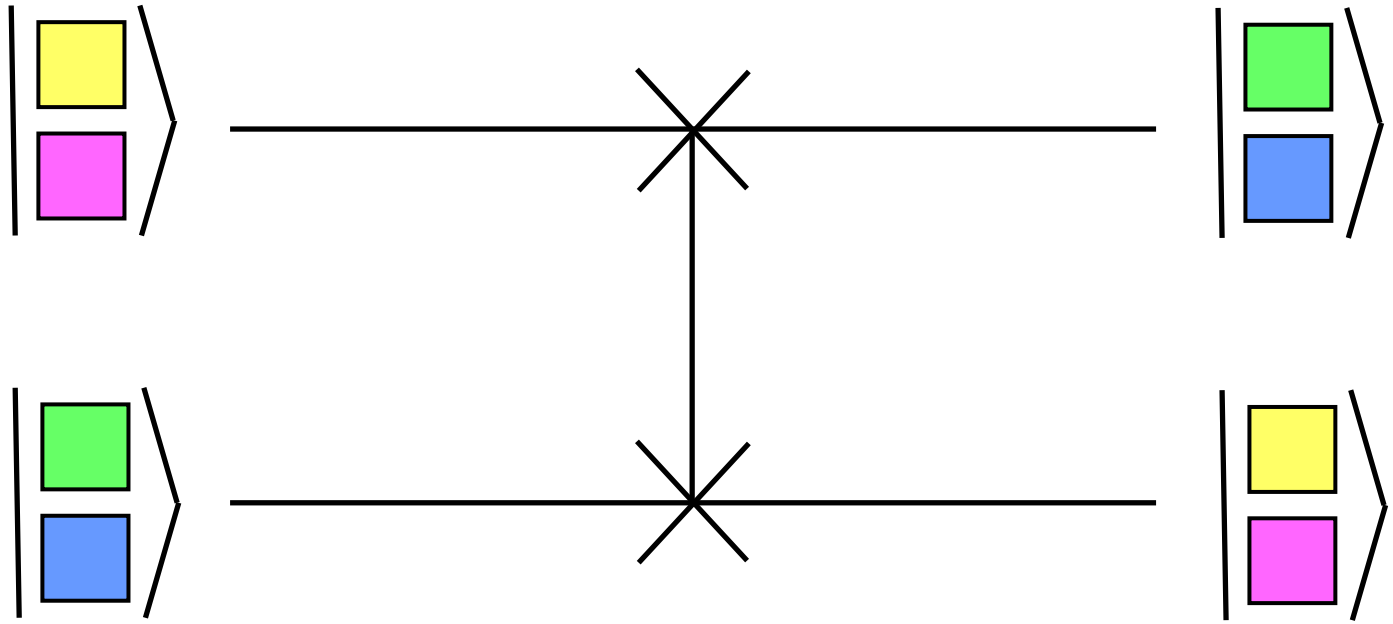
Concept of Quantum Computers



graphical representation of
SWAP gate

IEEE
UNITED STATES AIR FORCE ACADEMY
CYBERWORX

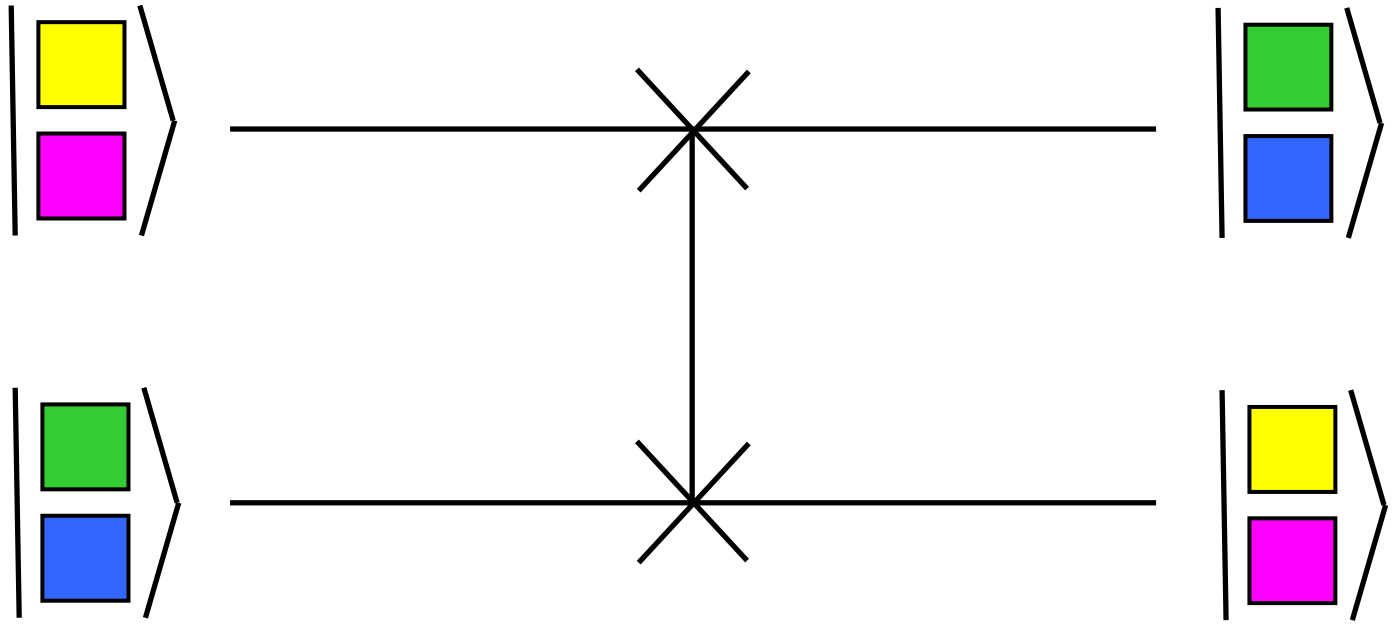
Concept of Quantum Computers



graphical representation of SWAP gate

IEEE
UNITED STATES AIR FORCE ACADEMY
CYBERWORX

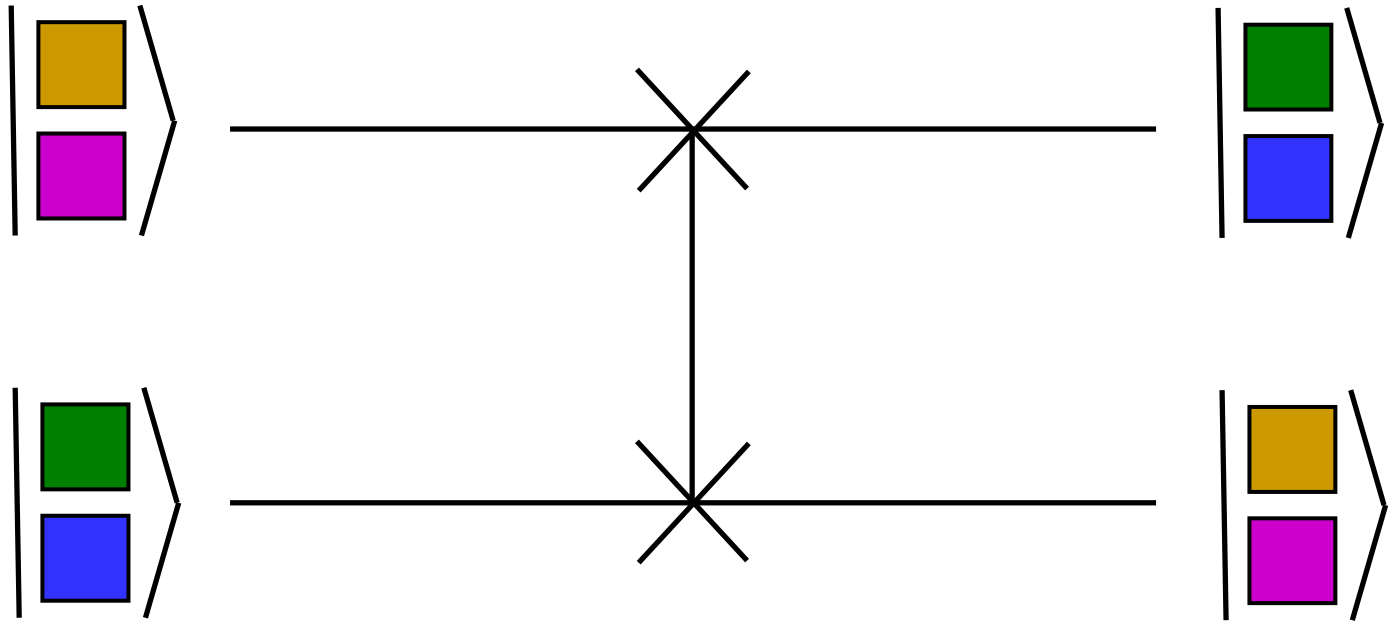
Concept of Quantum Computers



graphical representation of
SWAP gate

IEEE
UNITED STATES AIR FORCE ACADEMY
CYBERWORX

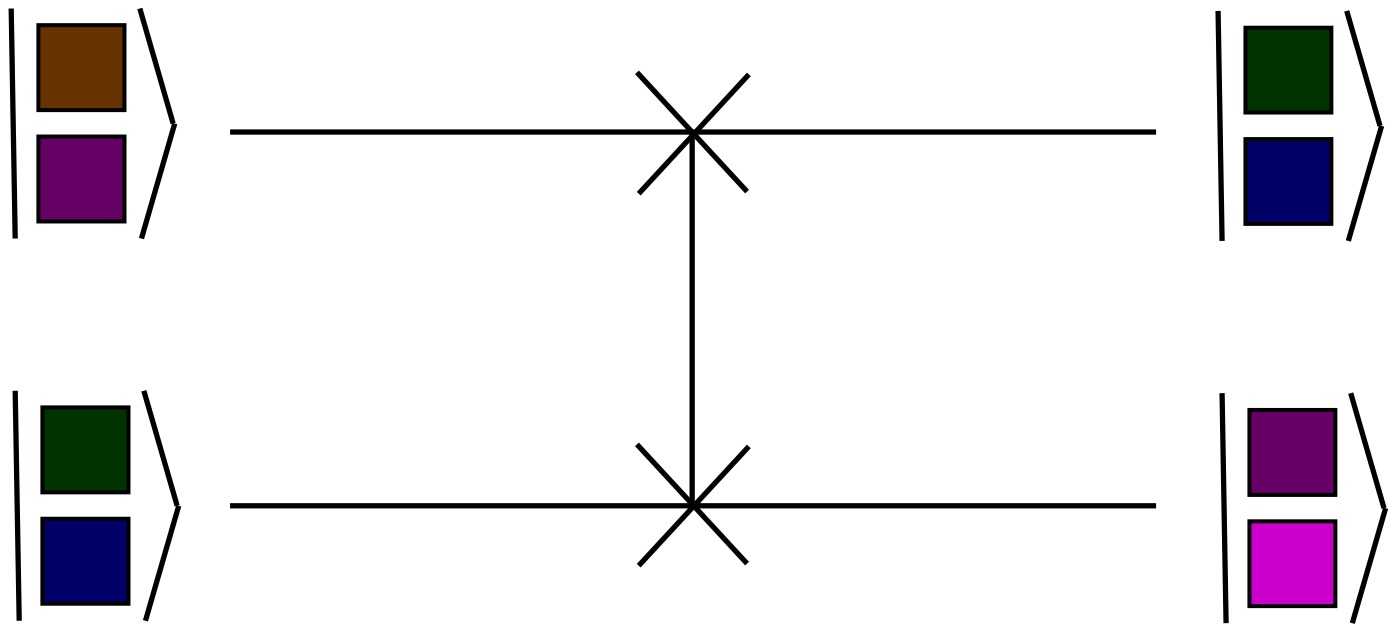
Concept of Quantum Computers



graphical representation of
SWAP gate

IEEE
UNITED STATES AIR FORCE ACADEMY
CYBERWORX

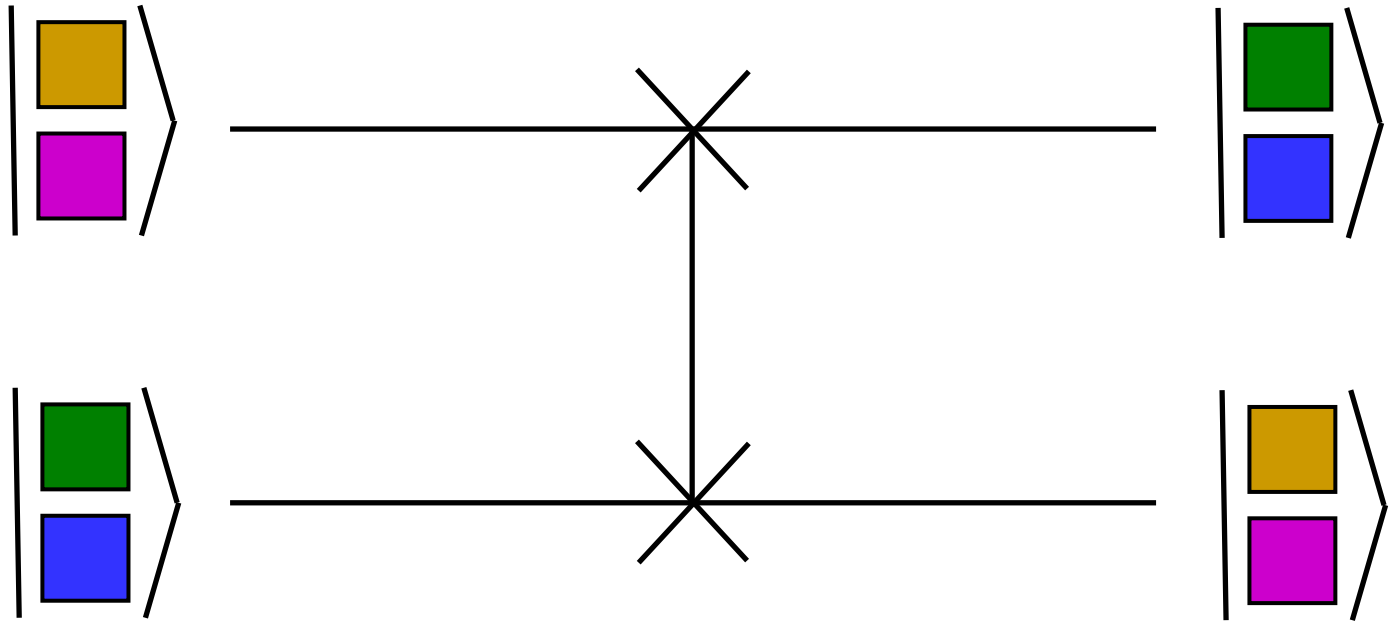
Concept of Quantum Computers



graphical representation of
SWAP gate

IEEE
UNITED STATES AIR FORCE ACADEMY
CYBERWORX

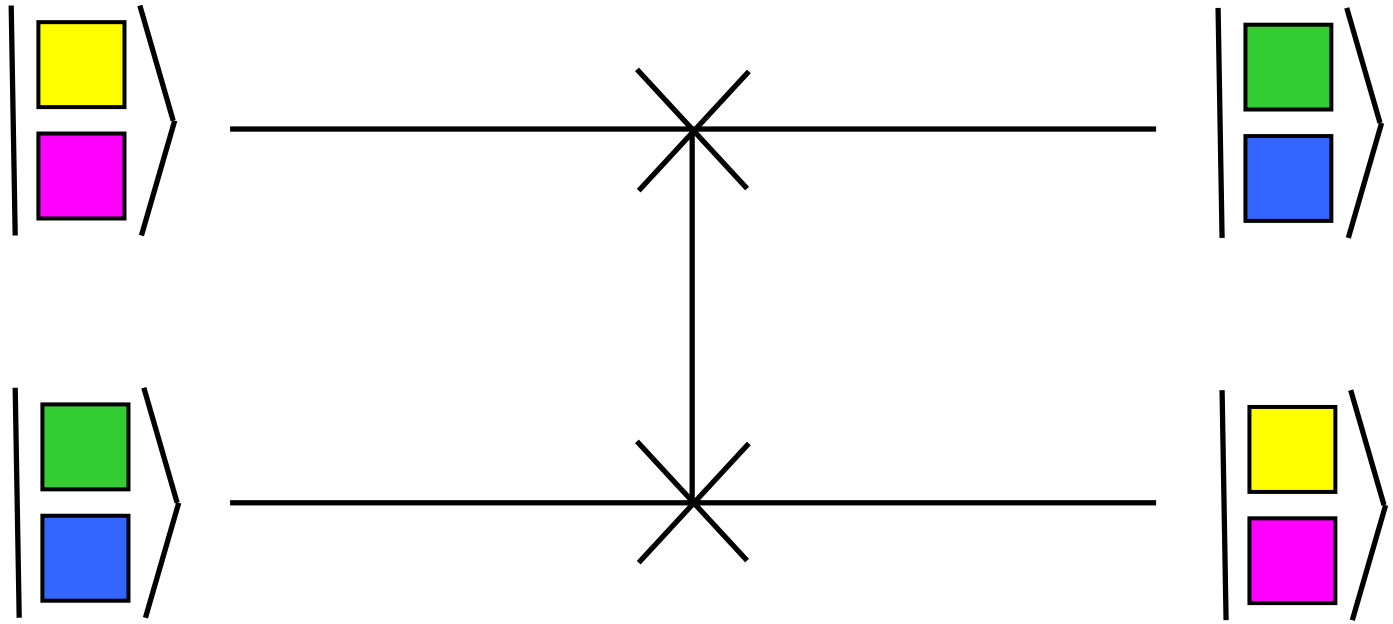
Concept of Quantum Computers



graphical representation of
SWAP gate

IEEE
UNITED STATES AIR FORCE ACADEMY
CYBERWORX

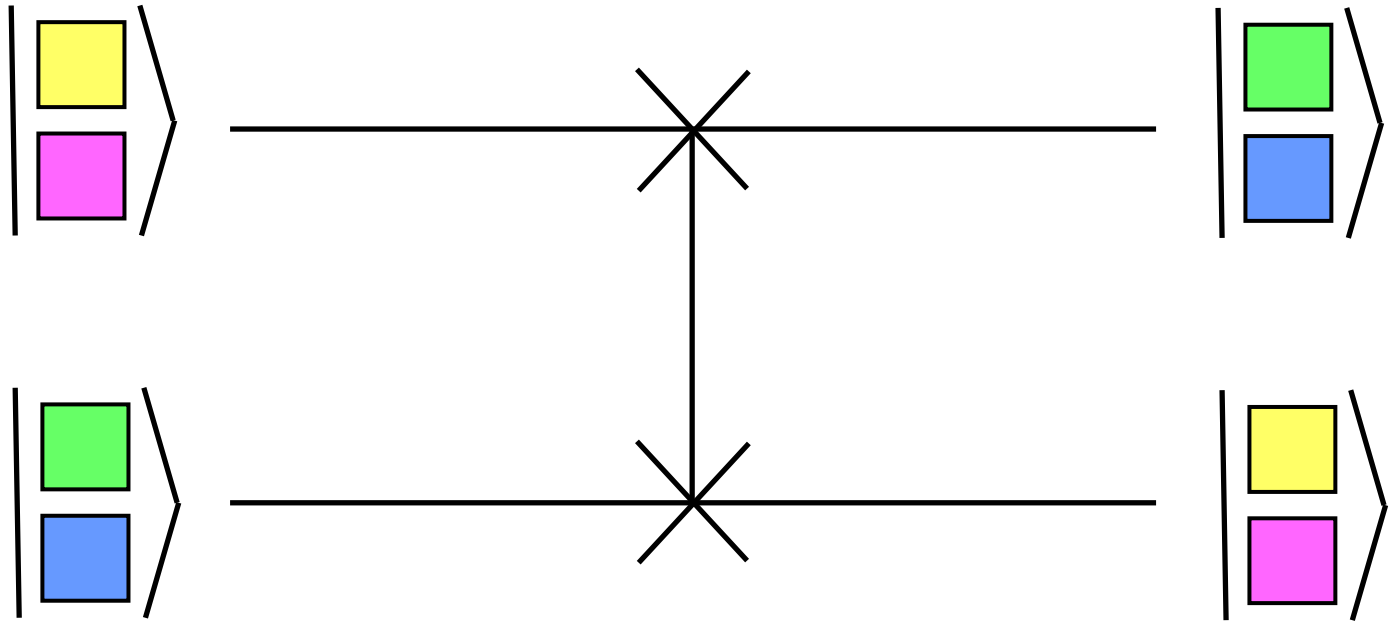
Concept of Quantum Computers



graphical representation of
SWAP gate

IEEE
UNITED STATES AIR FORCE ACADEMY
CYBERWORX

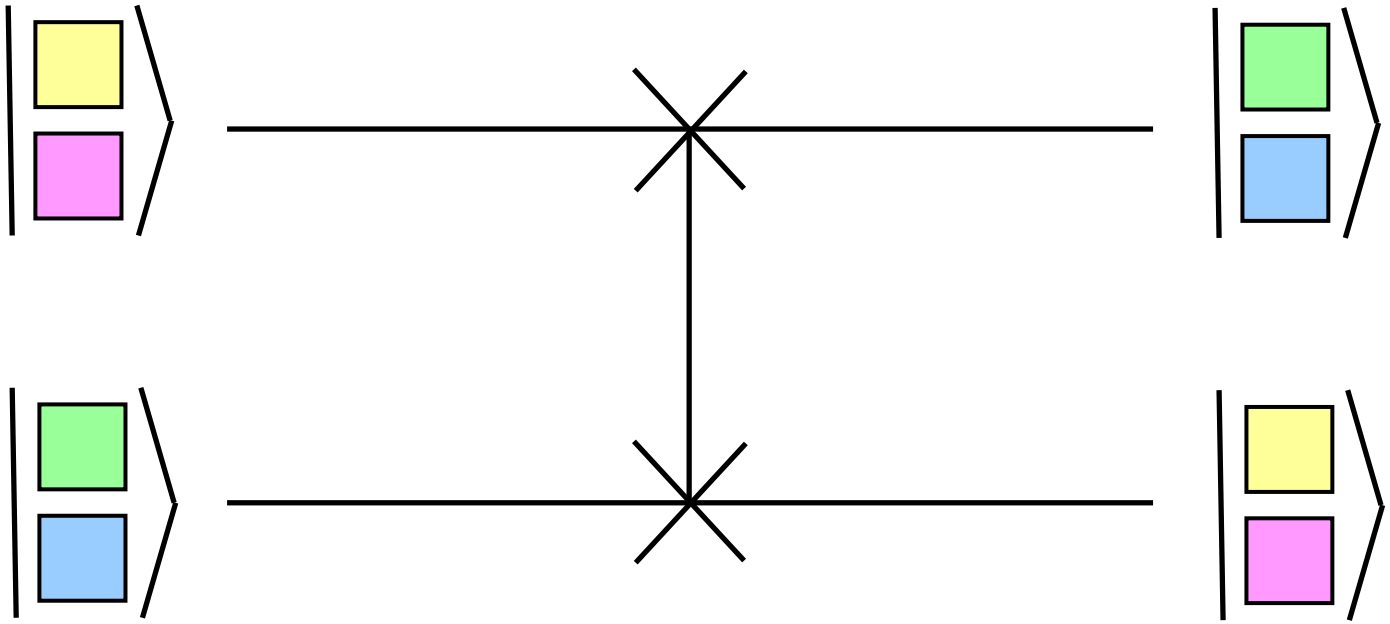
Concept of Quantum Computers



graphical representation of SWAP gate

IEEE
UNITED STATES AIR FORCE ACADEMY
CYBERWORX

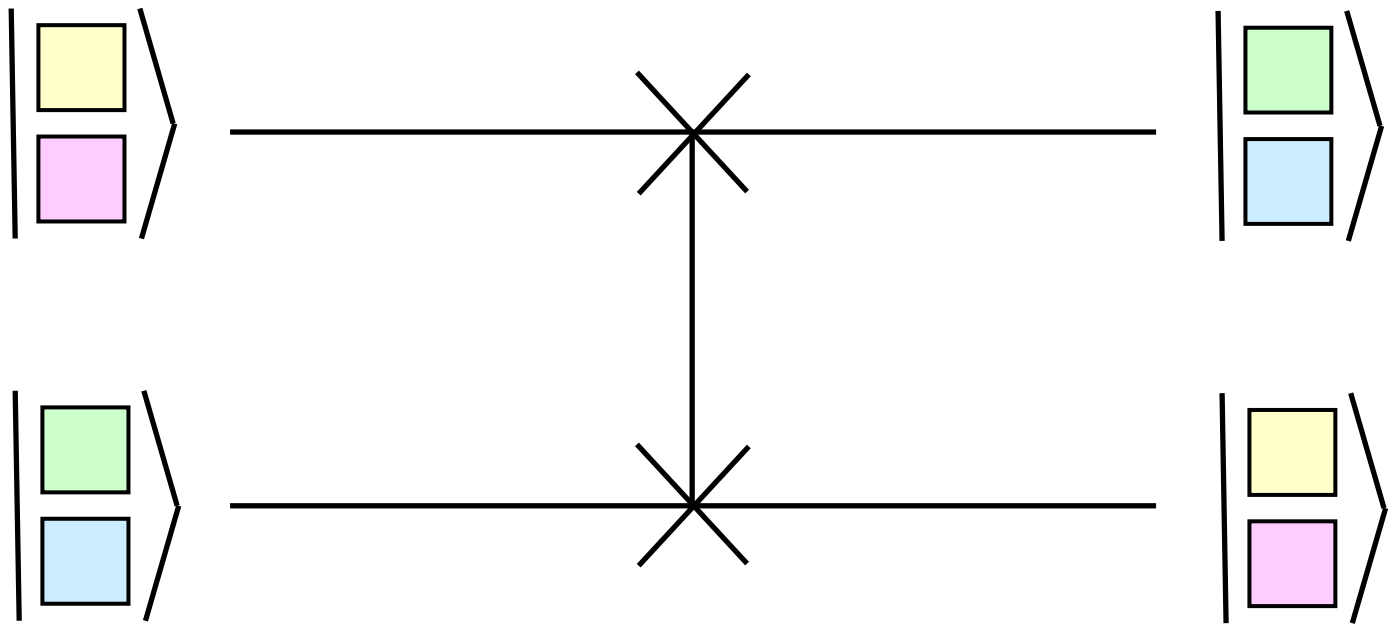
Concept of Quantum Computers



graphical representation of
SWAP gate

IEEE
UNITED STATES AIR FORCE ACADEMY
CYBERWORX

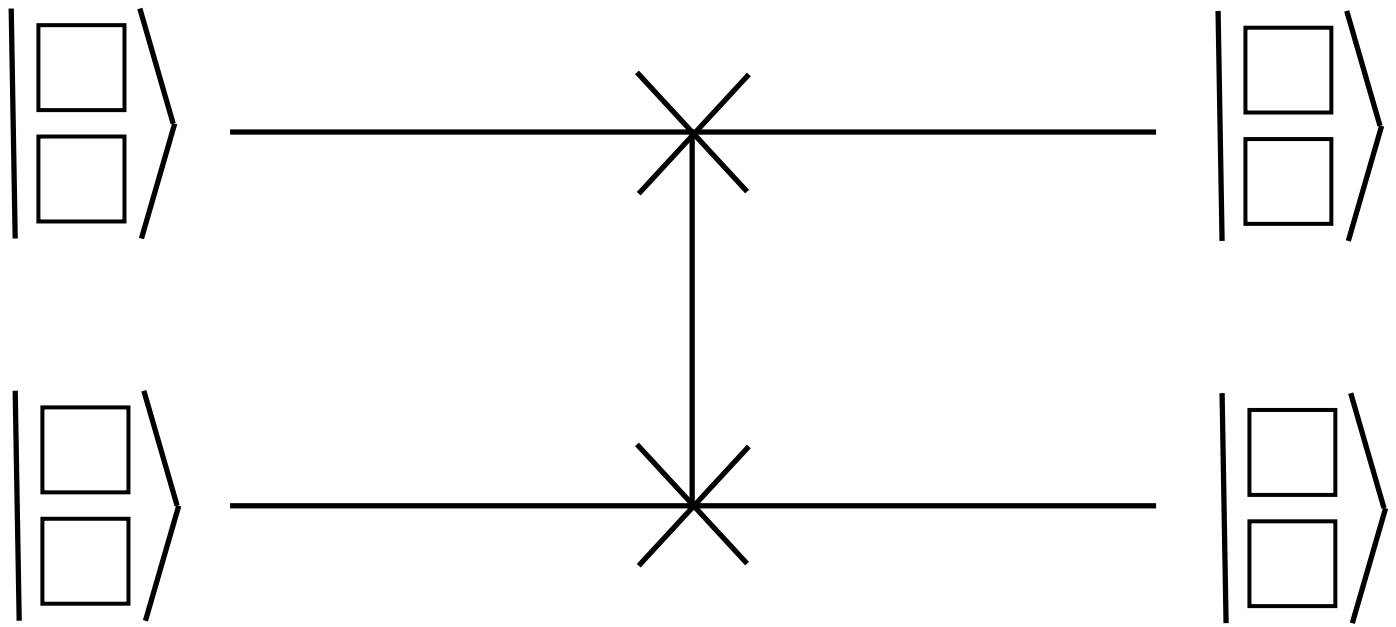
Concept of Quantum Computers



graphical representation of
SWAP gate

IEEE
UNITED STATES AIR FORCE ACADEMY
CYBERWORX

Concept of Quantum Computers



graphical representation of SWAP gate

IEEE
UNITED STATES AIR FORCE ACADEMY
CYBERWORX

Concept of Quantum Computers

Concept of Quantum Computers

- Quantum gates are combined to build more complex quantum calculation units and quantum memory
  - hardware still under development: some working models
  - no standardized design for a general quantum computer

Concept of Quantum Computers

- Recent news about Google Quantum Computer

https://www.livescience.com/google-hits-quantum-supremacy.html

Concept of Quantum Computers

- Google Quantum Computer
  - a basic computing chip using various quantum gates
  - 1.5 trillion times faster than traditional digital computer
  - requires 200 seconds to do equivalent work of 10,000 years by a current super computer

Concept of Quantum Computers

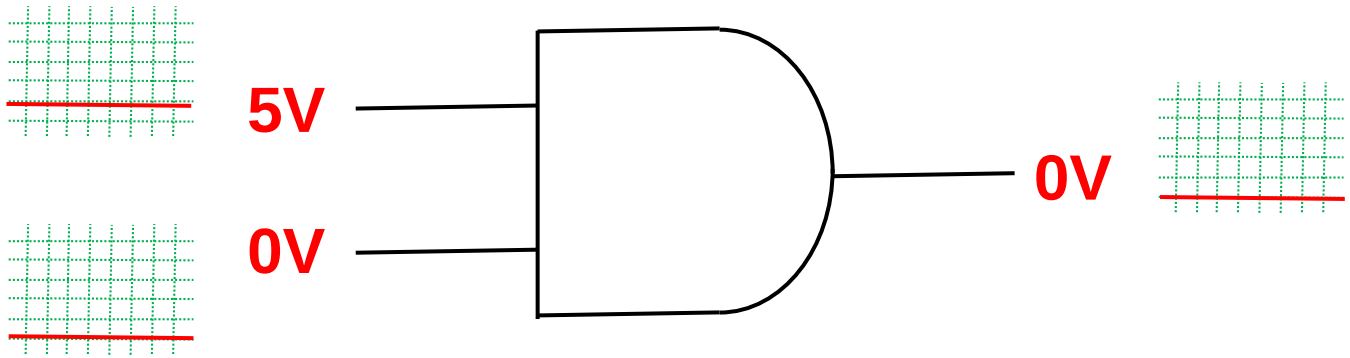
- Since the quantum computing chip is just introduced, quantum software is probably at the very infantry stage similar to that of the Assembly Language when the Z80 chip was introduced in the 80s
  - low level codes to move data in various memory registers and perform basic arithmetic operation
  - proof of concept is shown for comparison with existing computing power

Concept of Quantum Computers

- General observation about a quantum computer
  - a quantum computer is probably fast because it (the hardware) is more spontaneous in its continuous quantum state
  - a quantum computer is probably powerful because more data can be squeezed into a single unit of memory

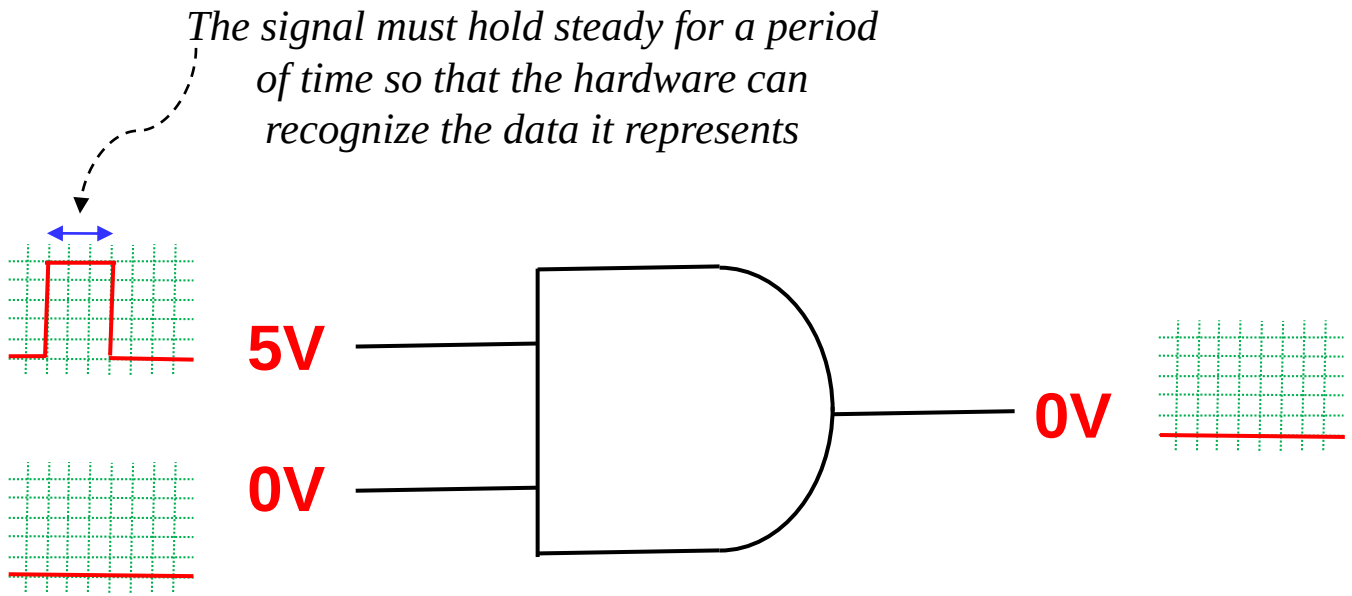
Concept of Quantum Computers

Concept of Quantum Computers



Traditional Hardware
In a Digital Computer

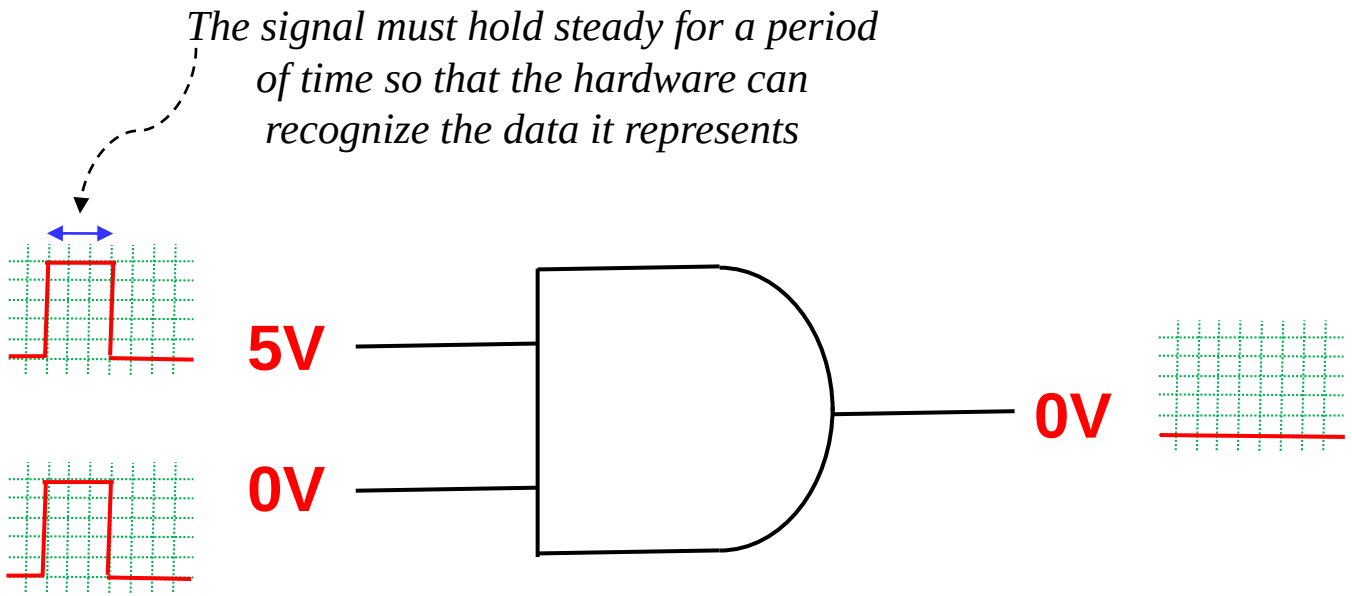
Concept of Quantum Computers



Traditional Hardware
In a Digital Computer

IEEE
UNITED STATES AIR FORCE ACADEMY
CYBERWORX

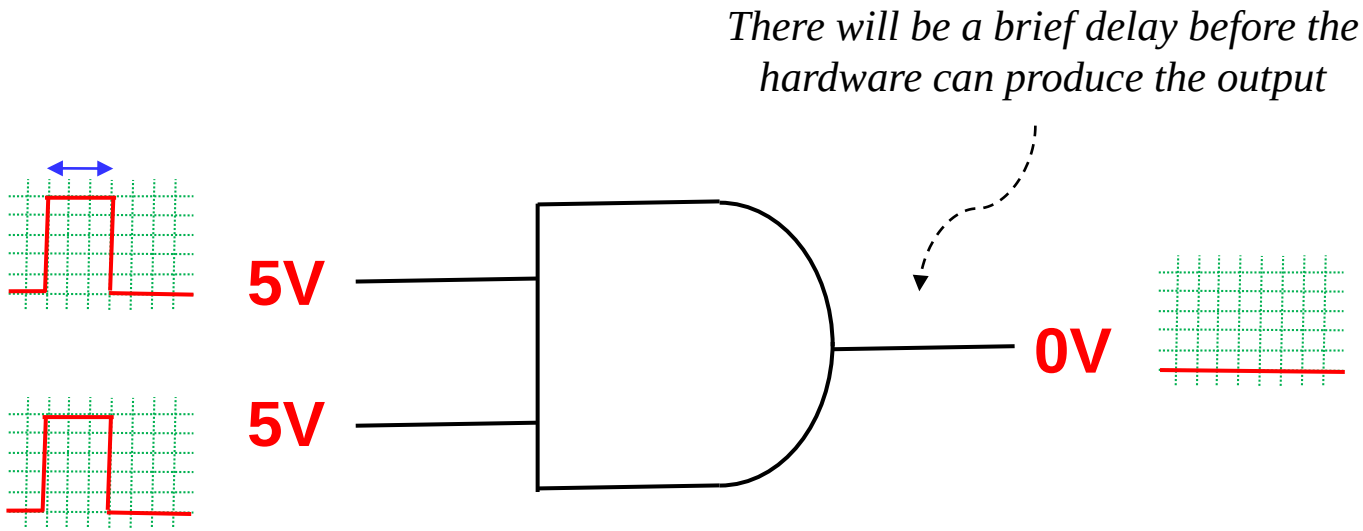
Concept of Quantum Computers



Traditional Hardware
In a Digital Computer

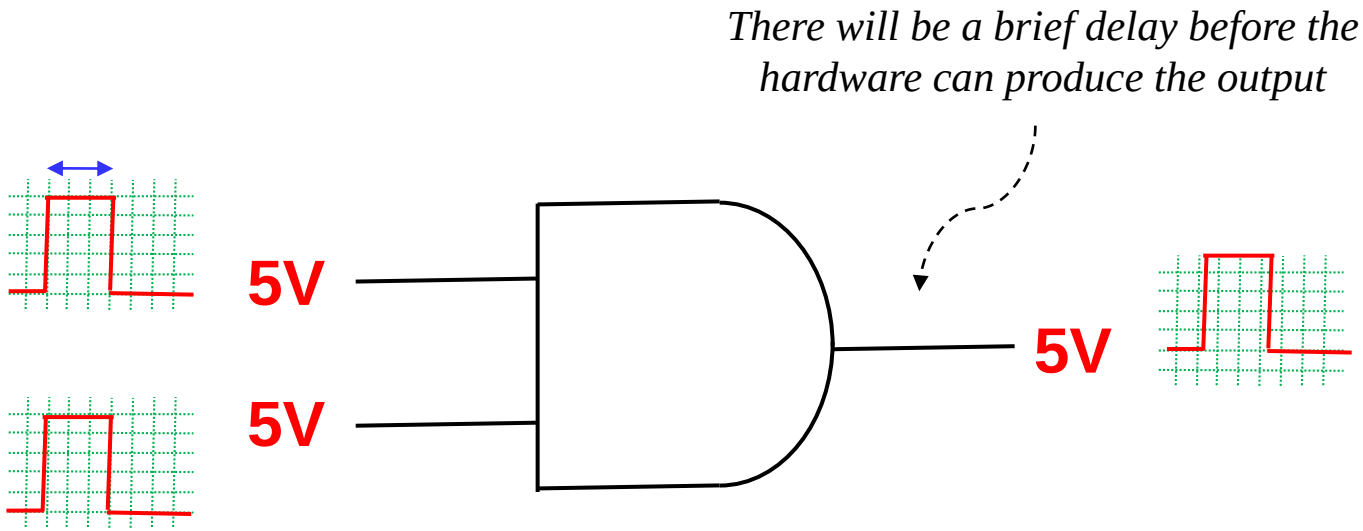
IEEE
UNITED STATES AIR FORCE ACADEMY
CYBERWORX

Concept of Quantum Computers



Traditional Hardware
In a Digital Computer

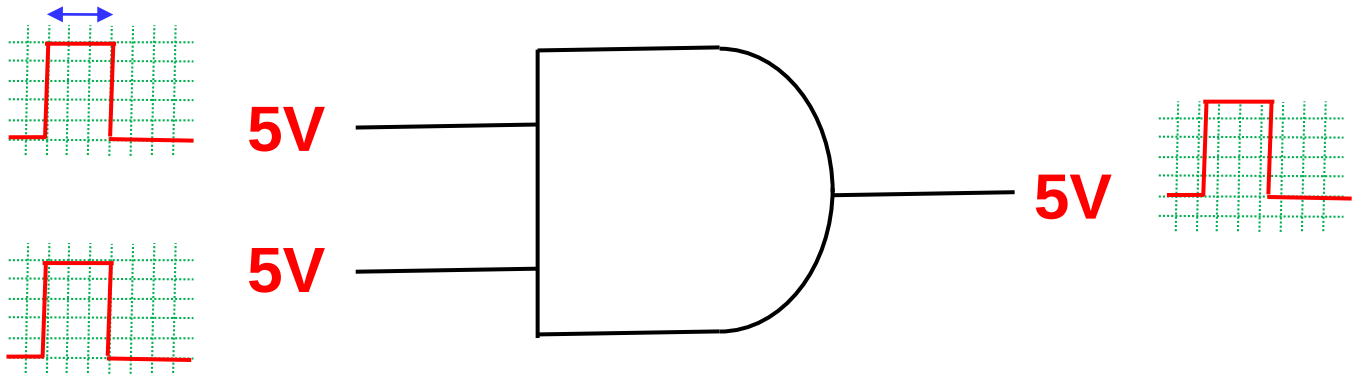
Concept of Quantum Computers



Traditional Hardware
In a Digital Computer

Concept of Quantum Computers

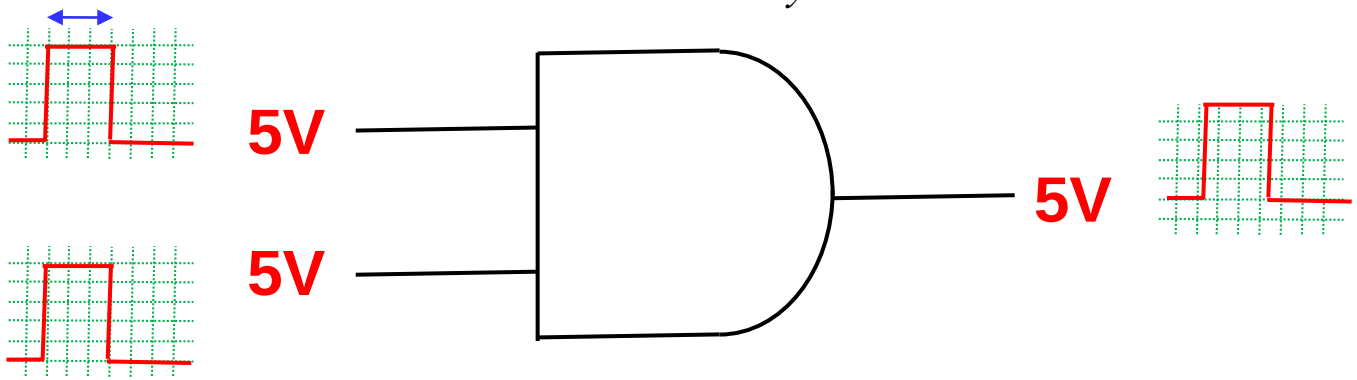
The duration that a signal must hold steady and the delay of its output defines a computational cycle



Traditional Hardware
In a Digital Computer

Concept of Quantum Computers

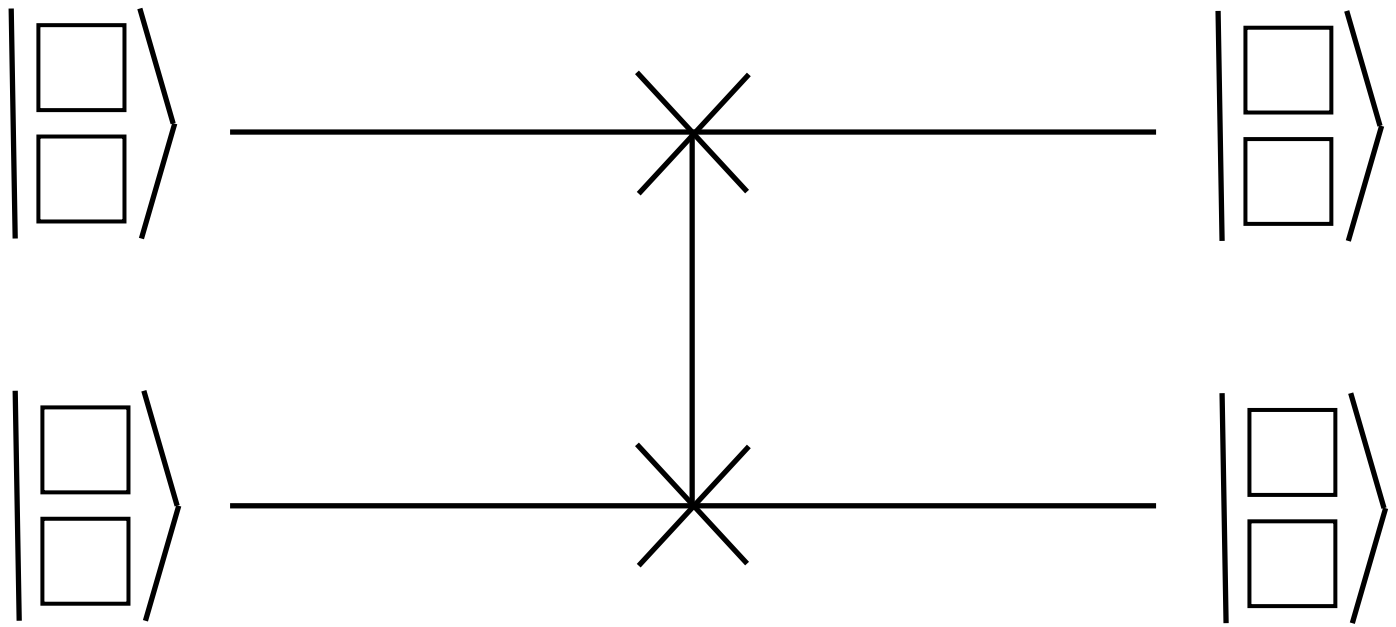
The computational cycle has been improved with time, from the 5Mhz to 10 Mhz in the 8088 chip in 1979 to around 4Ghz in today's CPU



Traditional Hardware In a Digital Computer

Concept of Quantum Computers

Concept of Quantum Computers

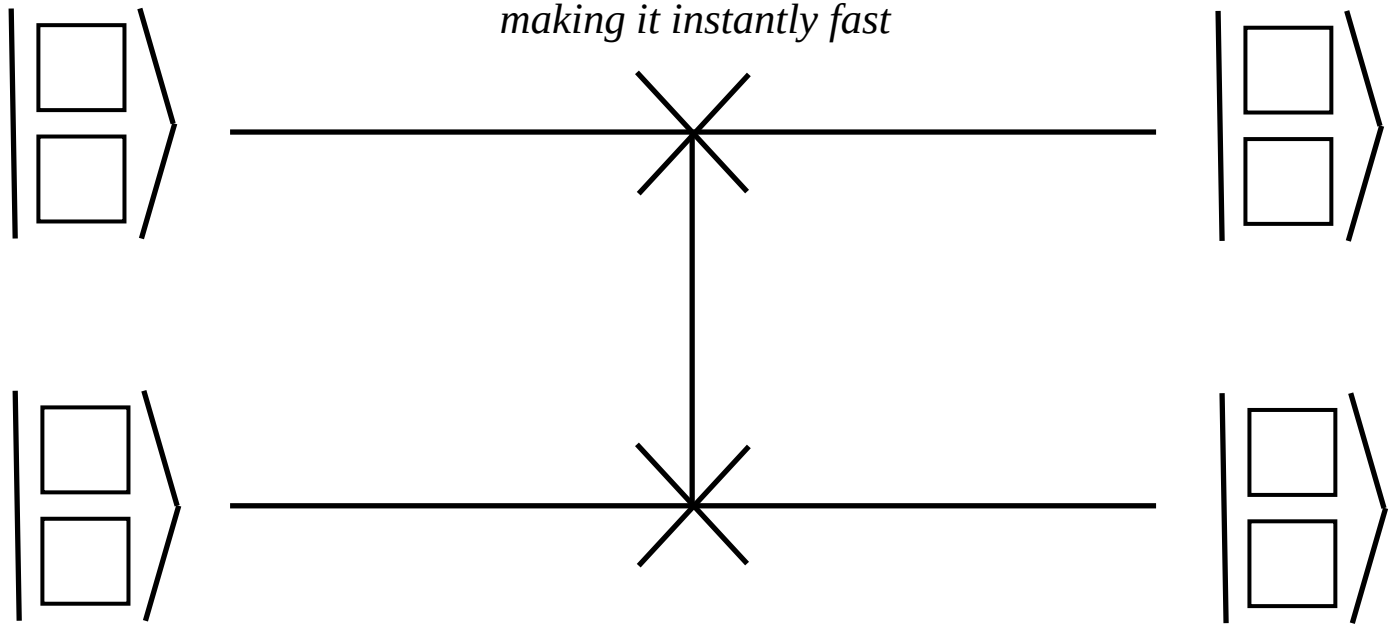


graphical representation of SWAP gate

IEEE
UNITED STATES AIR FORCE ACADEMY
CYBERWORX

Concept of Quantum Computers

It is speculated that the quantum hardware will be spontaneous in managing data, making it instantly fast

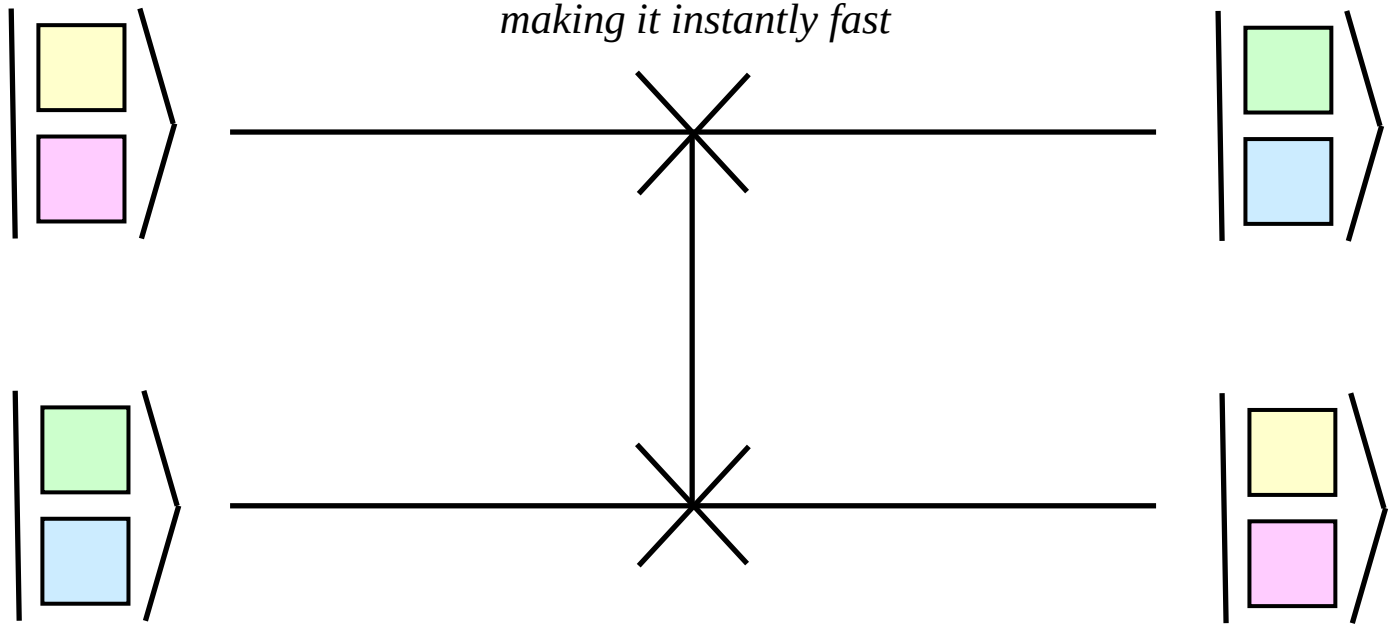


graphical representation of SWAP gate

IEEE
UNITED STATES AIR FORCE ACADEMY
CYBERWORX

Concept of Quantum Computers

It is speculated that the quantum hardware will be spontaneous in managing data, making it instantly fast

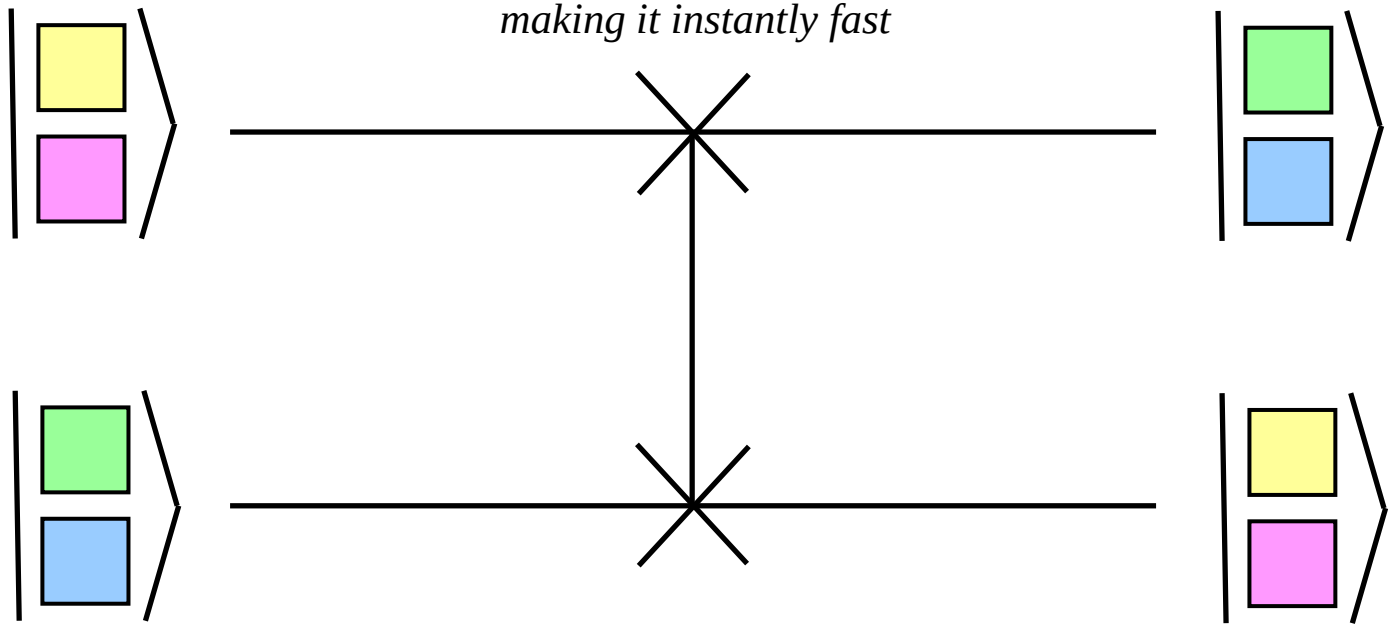


graphical representation of SWAP gate

IEEE
UNITED STATES AIR FORCE ACADEMY
CYBERWORX

Concept of Quantum Computers

It is speculated that the quantum hardware will be spontaneous in managing data, making it instantly fast



graphical representation of SWAP gate

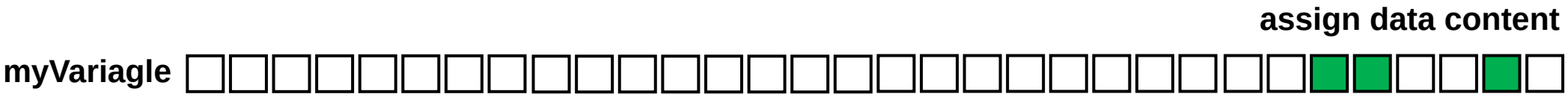
IEEE
UNITED STATES AIR FORCE ACADEMY
CYBERWORX

Concept of Quantum Computers

Traditional Digital Computers

```
main()
{
   int myVariable = 50;
}
```

a number of memory bits must be allocated
to represent a single number
in a traditional digital computer

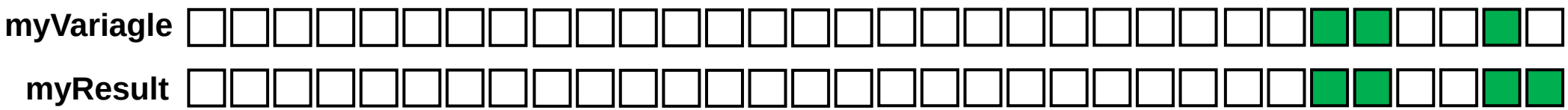


IEEE
UNITED STATES AIR FORCE ACADEMY
CYBERWORX

Traditional Digital Computers

```
main()
{
   int myVariable = 50;
}
```

calculation must be repeated in every memory bit, making it extremely inefficient



IEEE
UNITED STATES AIR FORCE ACADEMY
CYBERWORX

Concept of Quantum Computers

Concept of Quantum Computers

```
main()
{
   int myVariable = 50;
}
```

theoretically, a single quantum bit should be sufficient to represent a number

myVariagle 

Concept of Quantum Computers

```
main()
{
   int myVariable = 50;
}
```

theoretically, a single quantum bit should be sufficient to represent a number

myVariagle 

Concept of Quantum Computers

```
main()
{
   int myVariable = 50;
}
```

calculation in just one bit of data must be more efficient than calculation in many bits of data

myVariagle

myResult

IEEE
UNITED STATES AIR FORCE ACADEMY
CYBERWORX

Concept of Quantum Computers

```
main()
{
   int myVariable = 50;
}
```

theoretically, a single quantum bit should be sufficient to represent a number

myVariagle 

Concept of Quantum Computers

Quantum Computing

- Quantum computing is the process of using quantum computers to perform computationally intensive tasks that a traditional digital computer cannot do within some “reasonable time”
  - as proof concept, quantum computers are designed to do calculation similar to traditional digital computer for comparison
  - in reality, a quantum computer can be designed radically different to do things beyond our imagination

Quantum Computing

- Software designed for quantum computing is probably very basic and application dependent so that
  - brute computational power can be measured and benchmarked
  - the programming language supporting quantum software will evolve with the advance of the quantum hardware

Quantum Computing

Research Topics & Applications

- Since quantum computers demonstrated a tremendous computational power, the push to advancement is justified
  - hardware development
  - software development
  - application development

Research Topics & Applications

- **Hardware Development**
  - **chip designs: CPU, memory, storage, etc.**
  - **integration designs: data bus**
  - **supporting designs: cooling systems, chip interface**

Research Topics & Applications

- Software Development
  - programming language: simplification of the coding process
  - compiler: efficient translation of programming language to basic instructions in a quantum chip
  - simulation: testbed environment for both hardware development and software development

Research Topics & Applications

- Application Development
  - since quantum computing is still in its infantry, application development often focus on problems that require intense computational power
    - encryption & decryption
    - big data

Research Topics & Applications

Research Topics & Applications

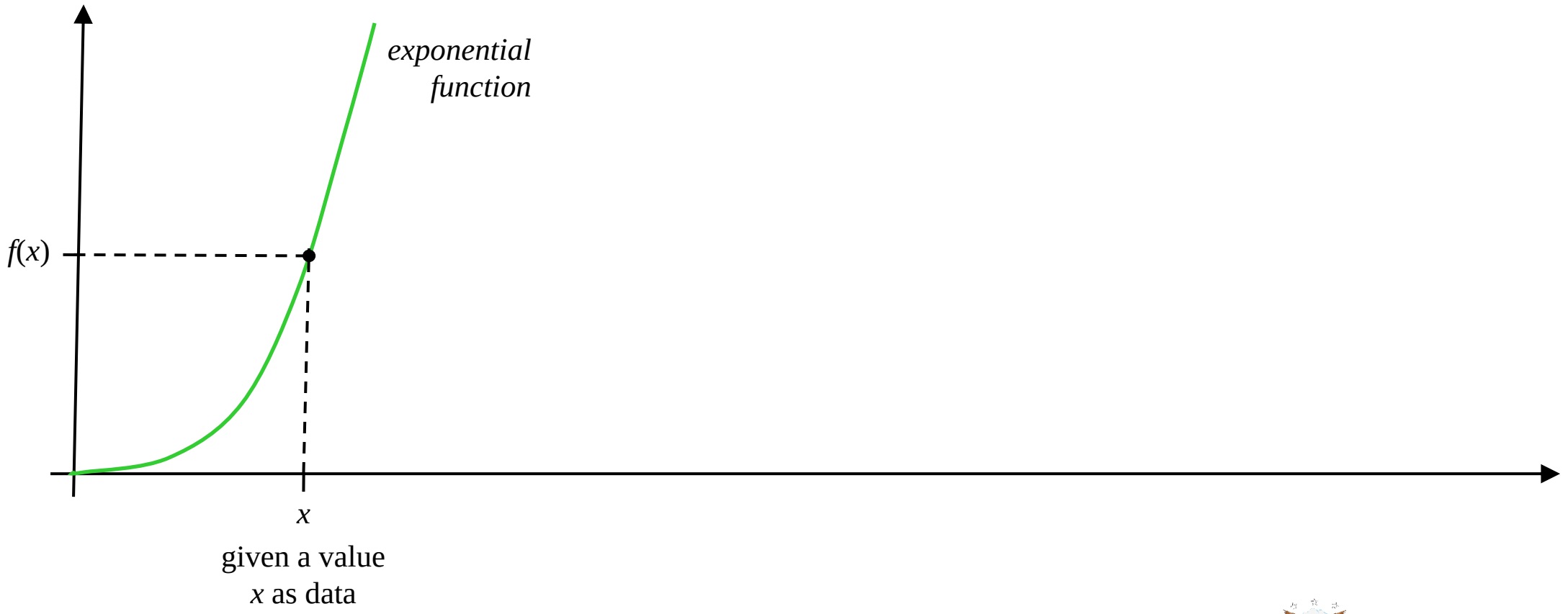
- **Application Development**
  - ***encryption*** **is the process of scrambling data into something that unauthorized users cannot understand**
    - **encryption algorithms depend on mathematical formula that is known to everybody**
    - **the secret of encryption is kept in a key that only an authorized user has to decrypt the data**

Research Topics & Applications

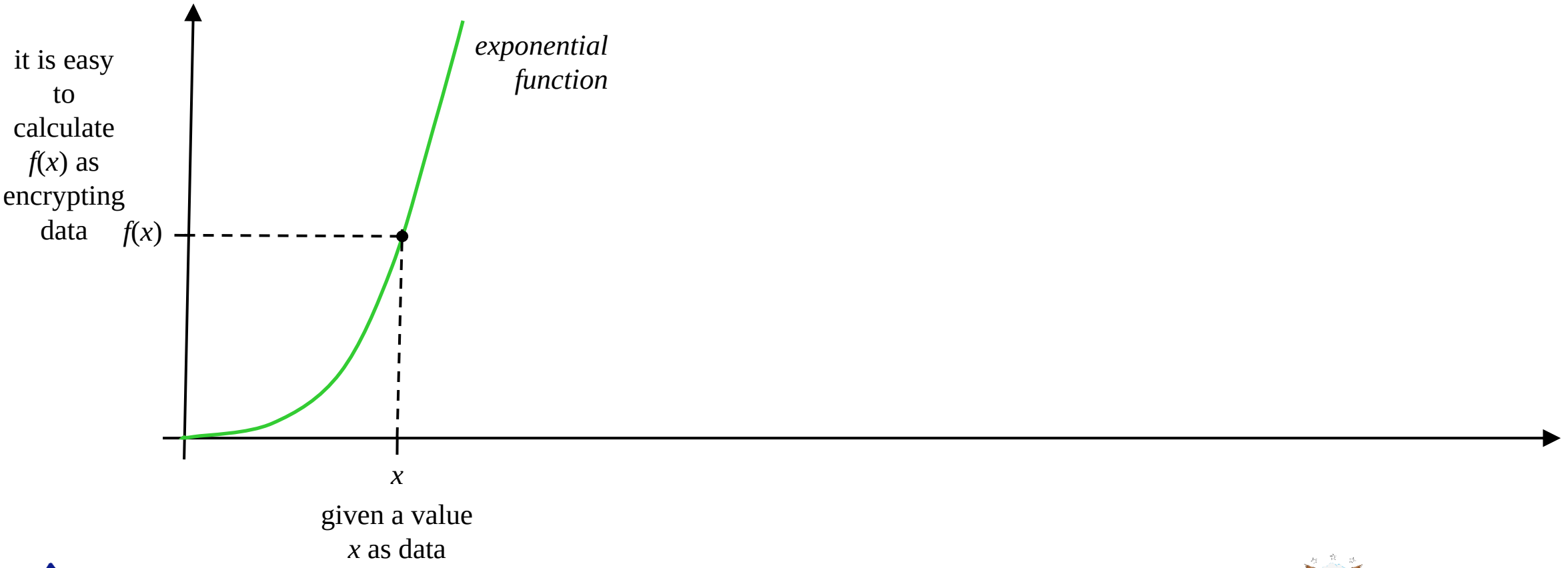
- **Application Development**
  - ***encryption algorithms*** **often develop around the exponential function and the mod function**
    - **the exponential function permits the development of reverse algorithms**
    - **the mod function prevents derivation of an inverse function the original data**

Research Topics & Applications

Research Topics & Applications



Research Topics & Applications

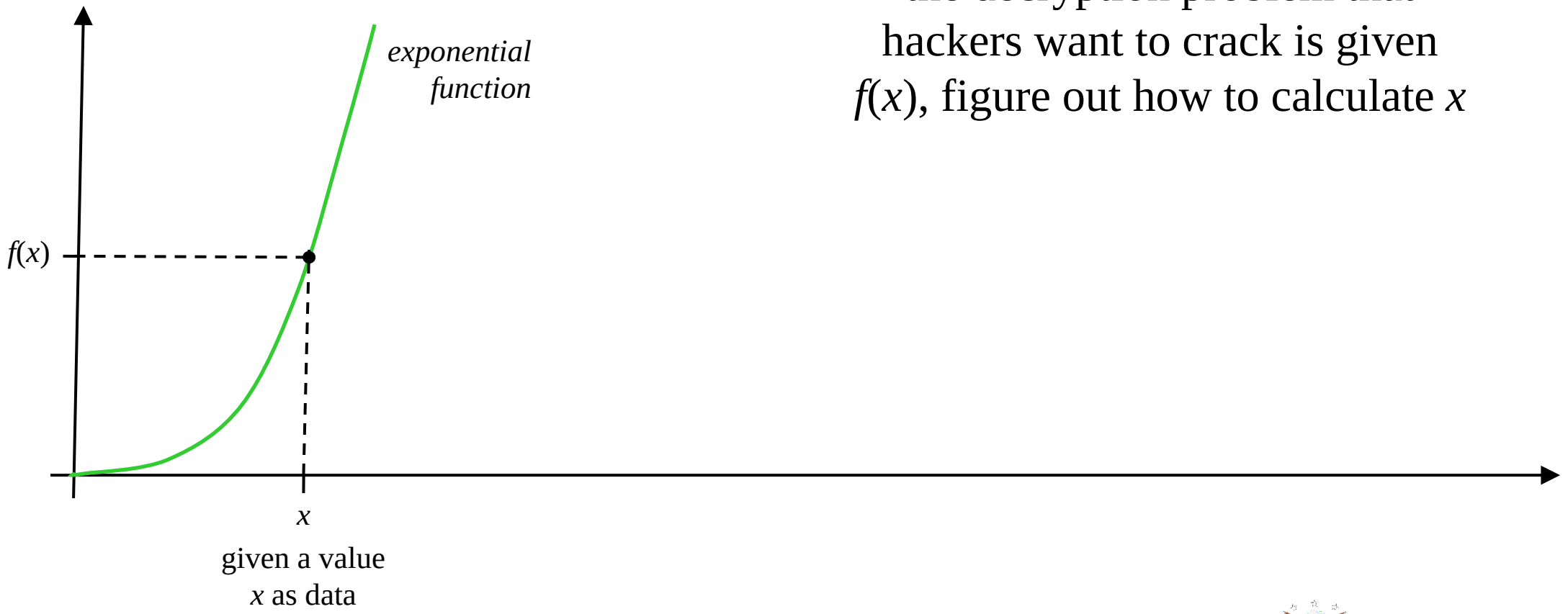


IEEE

UNITED STATES AIR FORCE ACADEMY

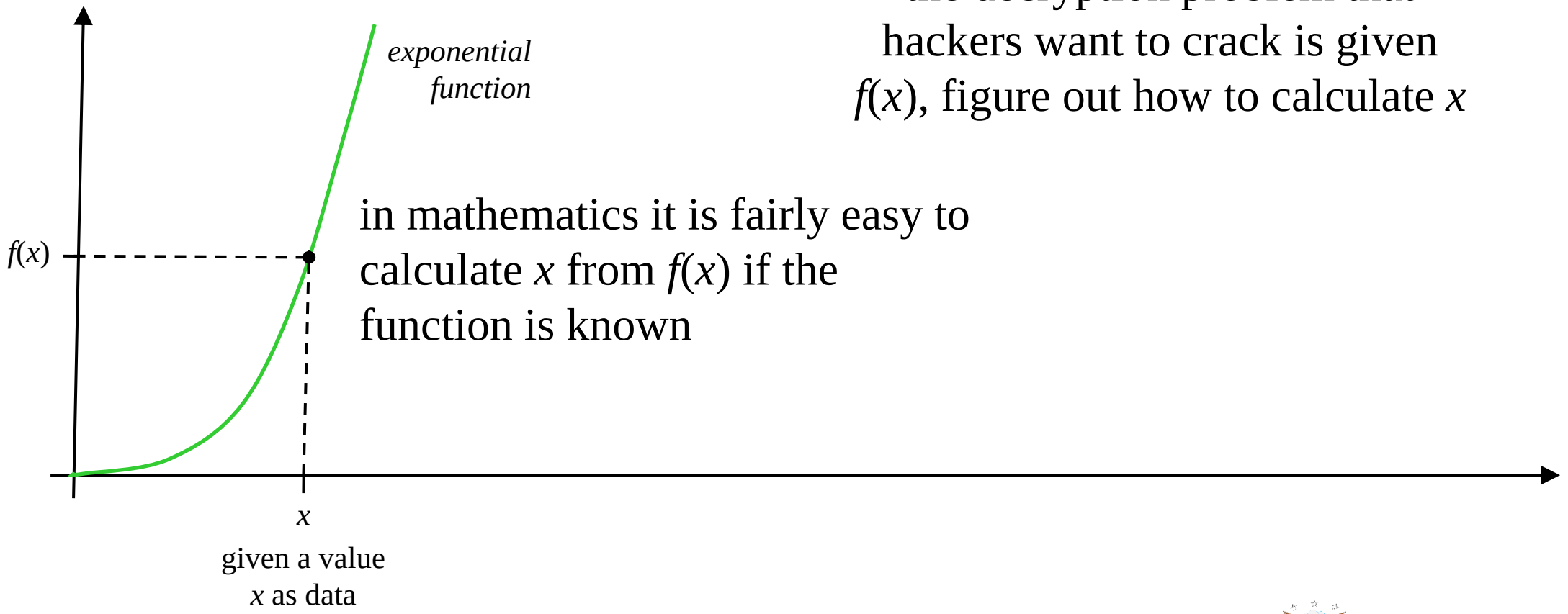
CYBERWORX

Research Topics & Applications



the decryption problem that hackers want to crack is given $f(x)$, figure out how to calculate x

Research Topics & Applications

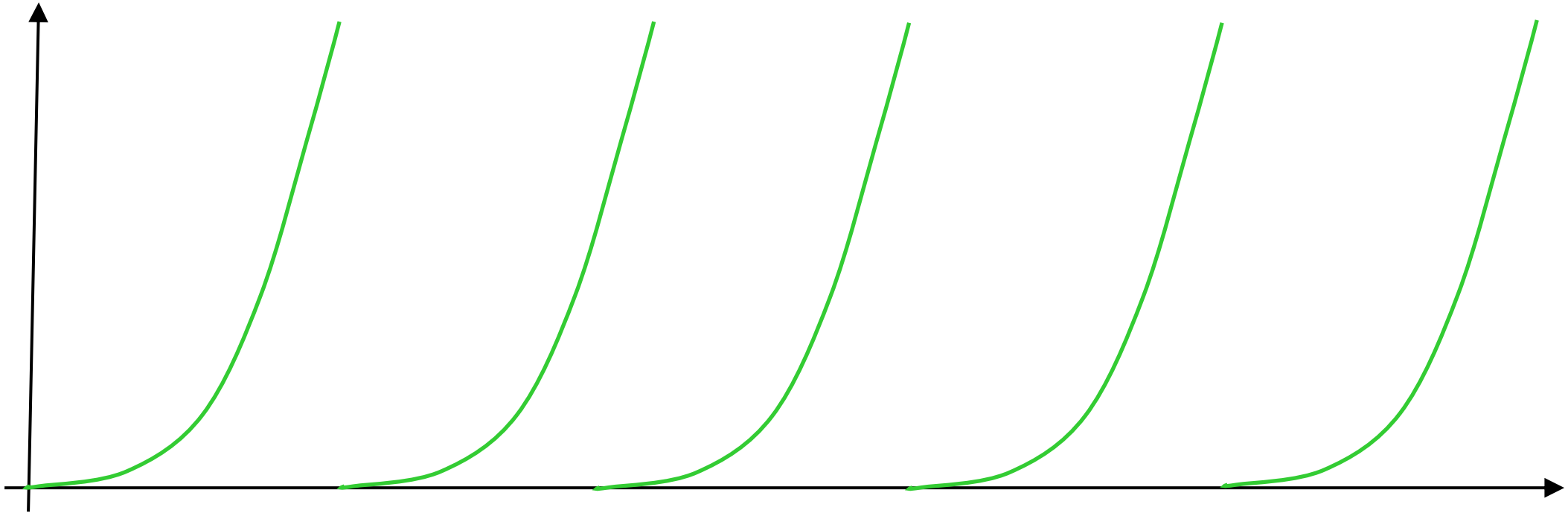


in mathematics it is fairly easy to calculate x from $f(x)$ if the function is known

the decryption problem that hackers want to crack is given $f(x)$, figure out how to calculate x

Research Topics & Applications

mod of an exponential function

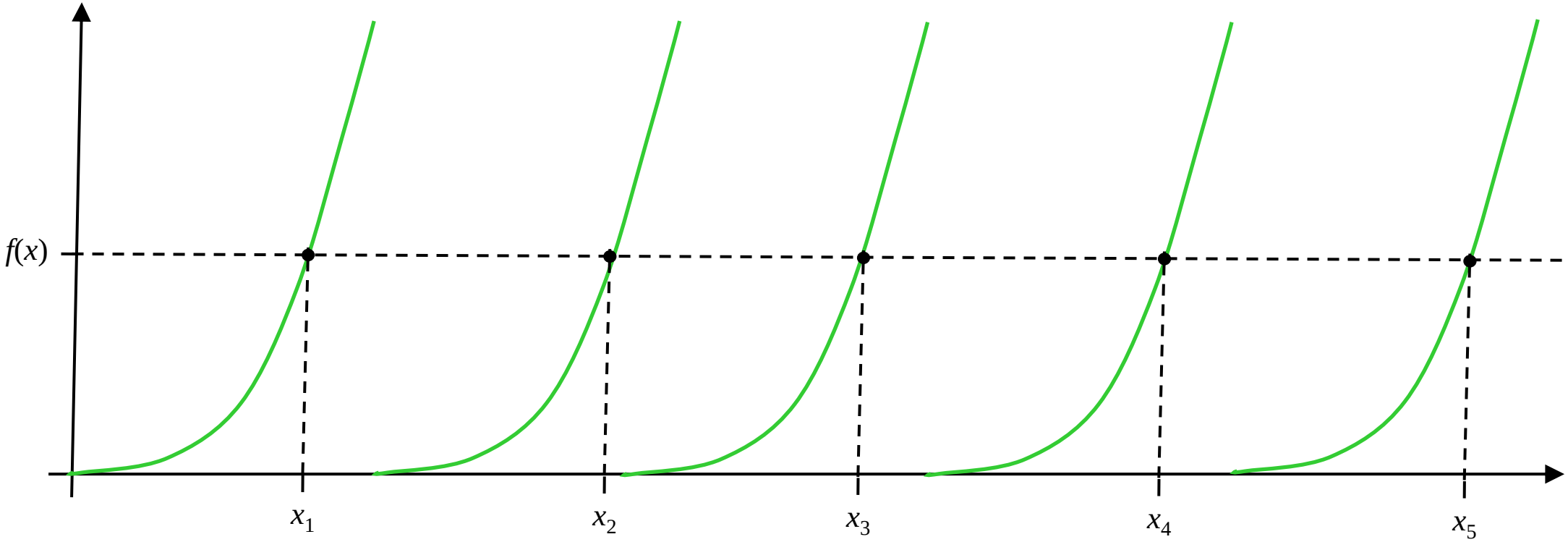


the mod function is used to
prevent reverse engineering

IEEE
UNITED STATES AIR FORCE ACADEMY
CYBERWORX

Research Topics & Applications

mod of an exponential function



for a given value $f(x)$, there are infinitely many possible values x that satisfy the equation, making it impossible to solve for x

IEEE
UNITED STATES AIR FORCE ACADEMY
CYBERWORX

Research Topics & Applications

- Application Development
  - breaking an encryption algorithm requires additional clue
    - the context of the data, e.g., the English language and its vocabulary
    - the construction of the data structure, e.g., how a cypherblock is built based on a sequence of many data points

Research Topics & Applications

- **Application Development**
  - **breaking an encryption algorithm is mathematically possible but requires a lot of computational power to evaluate the correct combination to determine a key**
    - **a strong encryption is how much time it requires to crack the key (in the order of 10^x years, with *x* being very large)**
    - **a quantum computer that can perform a calculation task that requires a traditional digital computer 10^x years to complete, but only in a few hundred seconds will *radically* change the practice of cybersecurity**

Research Topics & Applications

Research Topics & Applications

- Application Development
  - big data is the analytic process of working with a massive amount of data that traditional method of handling them cannot perform
    - big data normally refers to data of all activities on the Internet
    - processing big data often involves data mining algorithm to discover pattern of behavior (both individual behavior and collective behavior)
    - current data mining algorithms are computationally intensive and cannot deliver the results on big data within some “reasonable time”

Research Topics & Applications

IEEE
UNITED STATES AIR FORCE ACADEMY
AIR FORCE CYBERWORX

Research Topics & Applications

IEEE
UNITED STATES AIR FORCE ACADEMY
CYBERWORX

Research Topics & Applications

Google

IEEE

UNITED STATES AIR FORCE ACADEMY

CYBERWORX

Research Topics & Applications

Conclusion

Conclusion

- Quantum computing is a reality that is happening right now

Conclusion

- Quantum computing is a reality that is happening right now
- **While quantum computing is still evolving, it is always possible to do R&D work through simulations without waiting for access of an actual working quantum computer**

Conclusion

- Quantum computing is a reality that is happening right now
- While quantum computing is still evolving, it is always possible to do R&D work through simulations without waiting for access of an actual working quantum computer
- **The future world with quantum computers is both exciting and scary, thus it is important for us to collaborate together to prepare ourselves for it**

THANK YOU