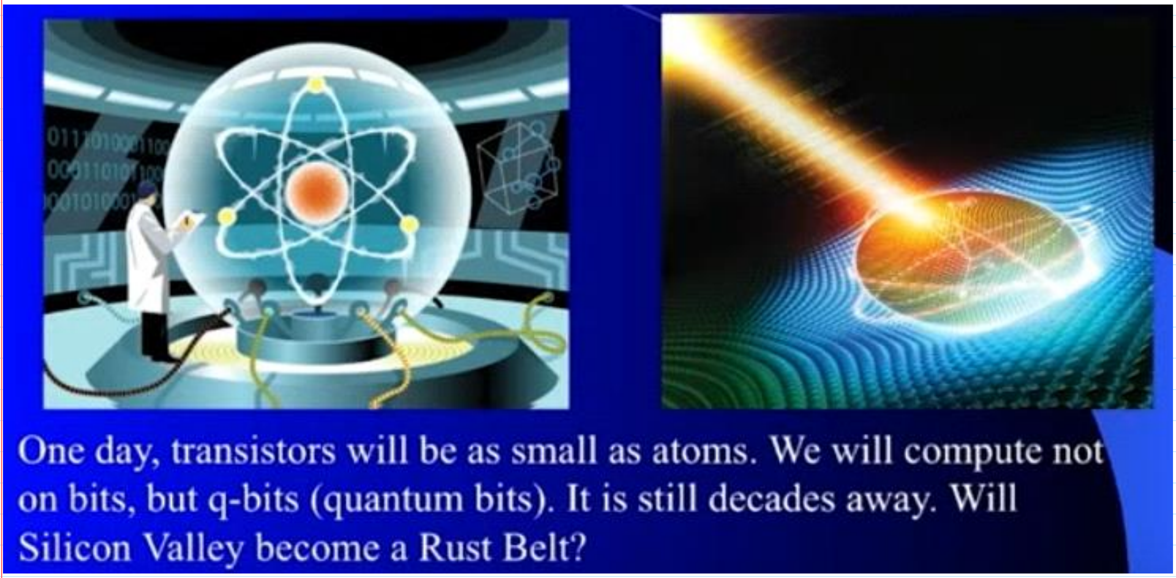
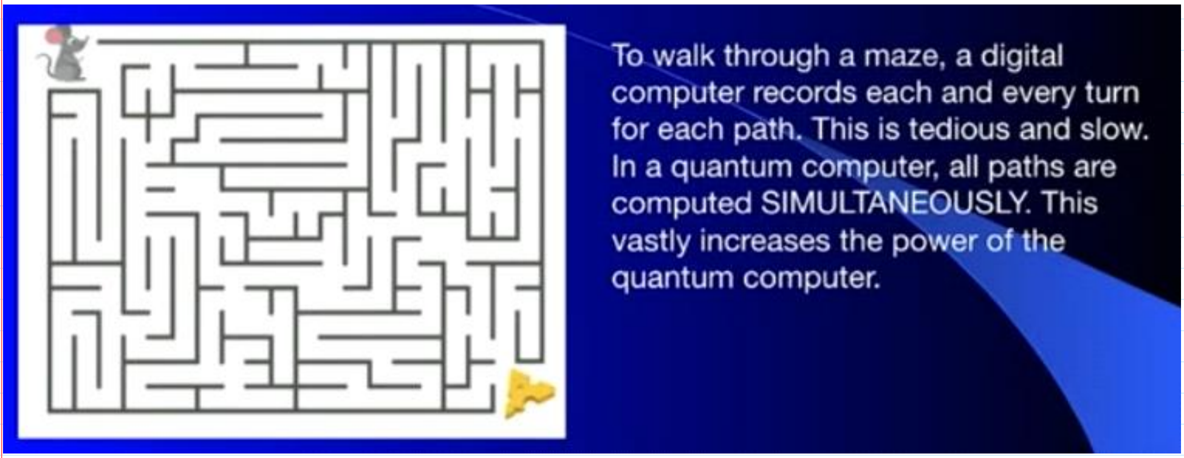
Results of Mid-Term Exam (MTE): Computation with Encrypted Data
https://docs.google.com/spreadsheets/d/1ZVSZMGheC2RCZIpJr8XltwvmKe1I6Zwh/edit?usp=sharing&ouid=111502255533491874828&rtpof=true&sd=true
The final grade will be presented this week.

Post-Quantum Cryptography - 11

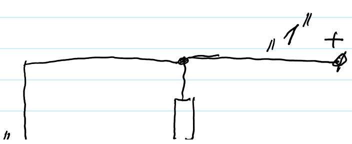
Michio Kaku
https://www.youtube.com/watch?v=_OjRClPzU6Y

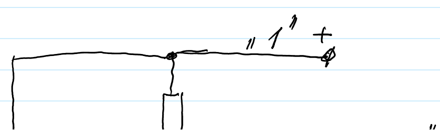


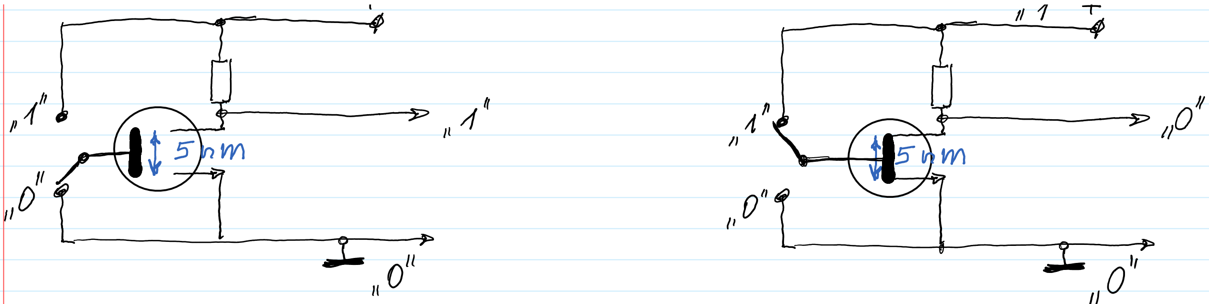


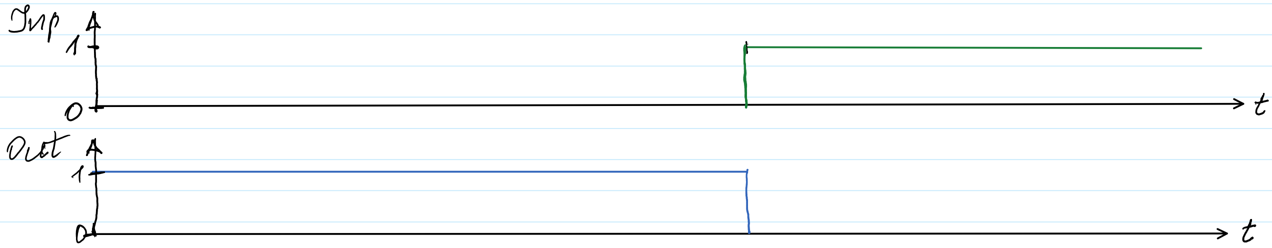
https://fb.watch/vIEogSoMB8/

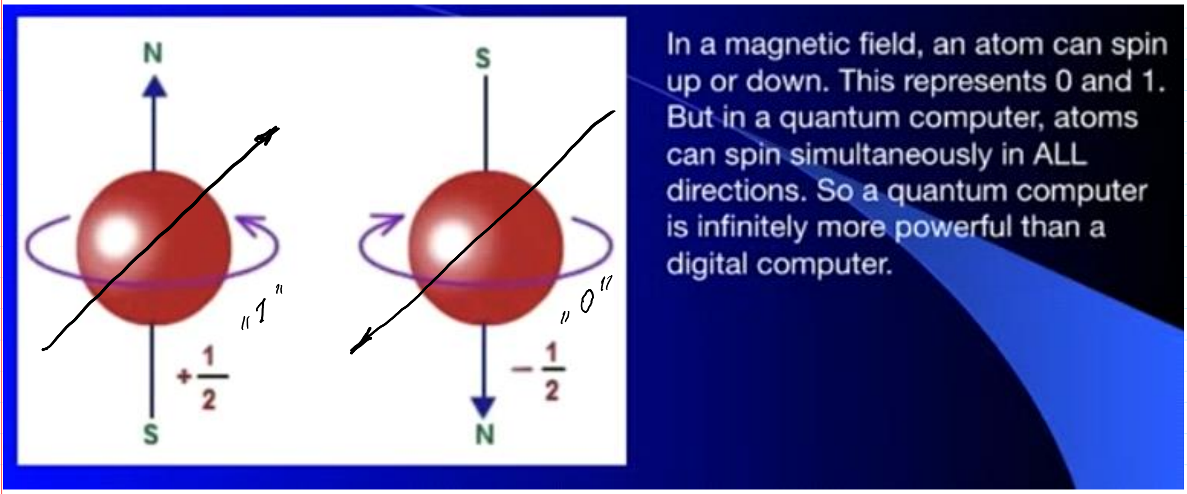
23 min
https://www.youtube.com/watch?v=gfUEUhDbGXA

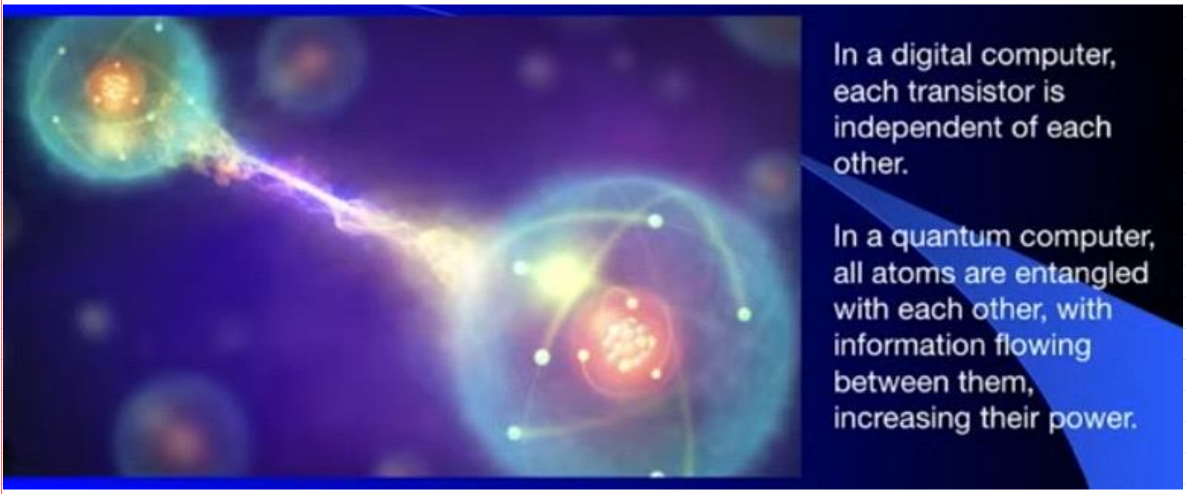


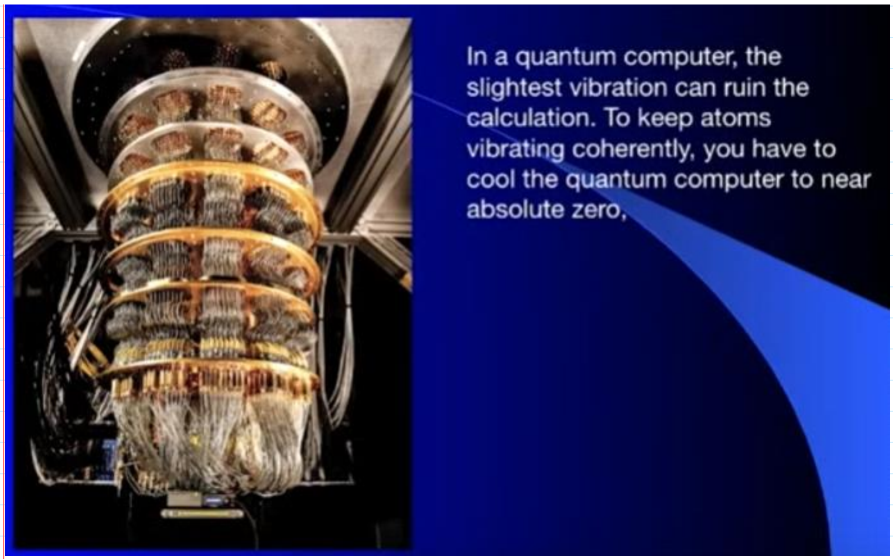


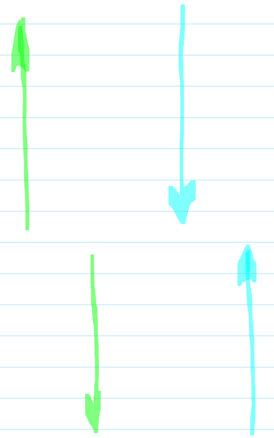

„1"
„0"
5 nm
„1"
„0"
„1"
„0"
5 nm
„0"
„0"


Inp
1
0
t
Out
1
0
t

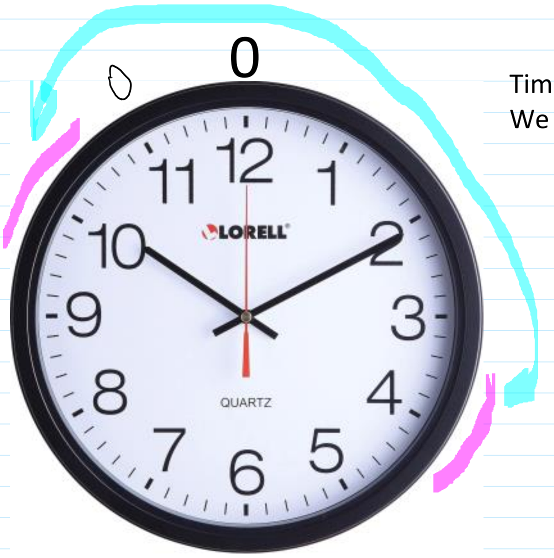

N
S
„1"
„0"
+1/2
−1/2
S
N
In a magnetic field, an atom can spin up or down. This represents 0 and 1. But in a quantum computer, atoms can spin simultaneously in ALL directions. So a quantum computer is infinitely more powerful than a digital computer.


In a digital computer, each transistor is independent of each other.
In a quantum computer, all atoms are entangled with each other, with information flowing between them, increasing their power.





Learning With Errors - LWE paradigm



Time is computed modulo 12.
We will perform computations modulo 11.

11 mod11 = 0.

System of linear equations: **Alex**, **Bill**, **Cecilia** - are programmers.
Has certain reward per hour in CBDC.
In Monday **Alex** worked 1 hour, **Bill** worked 2 hours, **Cecilia** worked 3 hours: their all total salary was 14 Ꞓ.
In Tuesday **Alex** worked 2 hours, **Bill** worked 1 hour, **Cecilia** worked 2 hours: their all total salary was 10 Ꞓ.
In Wednesday **Alex** worked 3 hour, **Bill** worked 2 hours, **Cecilia** worked 2 hours: their all total salary was 13 Ꞓ.

How many **Alex**, **Bill** , **Cecilia** are earning per hour?
The rewards per hour for **Alex**, **Bill** , **Cecilia**
We denote by x y z

Then to find 3 unknown variables x, y, z we have a system 3 of linear equations:

1*x + 2*y + 3*z = 14 (1)
2*x + 1*y + 2*z = 10 (2)
3*x + 2*y + 2*z = 13 (3)

This system of equations can be written matrix form: ***M*w*** = ***s***,
Where ***w'*** = (x, y, z) is vector of unknown salaries x, y, z and ***s*** is a vector of total salaries of every day written in column.
Transposed vector ***s*** we denote by ***s'*** then it can be written in a row: ***s'*** = (14, 10, 13).

This data in Octave is formed in the following way:

```
>> M=[1 2 3; 2 1 2; 3 2 2]
M =
   1   2   3
   2   1   2
   3   2   2
```

$$\begin{pmatrix}1&2&3\\2&1&2\\3&2&2\end{pmatrix} * \overset{w}{\begin{pmatrix}x\\y\\z\end{pmatrix}} = \begin{pmatrix}14\\10\\13\end{pmatrix}$$

```
>> s=[14;10;13]
s =
   14
   10
   13
```

```
>> st=s'
st =
   14   10   13
```

$5*z = 15$

$5^{-1} * 5*z = 5^{-1}*15 \to z = 3$

$m*z = s$

$m^{-1}*m*z = m^{-1}*s$

$1*z = m^{-1}*s$

$z = m^{-1}*s$

$M*w = s$

$\underbrace{M^{-1}*M}*w = M^{-1}*s$

$I*w = M^{-1}*s$

$w = M^{-1}*s$

```
>> w=Mi*s
w =
   1
   2
   3
```

```
>> Mi=inv(M)   % M^-1
Mi =
  -0.4000   0.4000   0.2000
   0.4000  -1.4000   0.8000
   0.2000   0.8000  -0.6000
```

```
>> I=Mi*M
I =
   1.0000   0.0000   0.0000
  -0.0000   1.0000   0.0000
   0.0000        0   1.0000
```

In Thursday   **Alex** worked 3 hour, **Bill** worked 3 hours, **Cecilia** worked 1 hour: they all earned 12 $\mathcal{D}$.

This 4-th condition yields the 4-th equation of the form:

$3*x + 3*y + 1*z = 12 \qquad (4)$

Then we have the following system of 4 equations:

$$\left.\begin{array}{ll}1*x + 2*y + 3*z = 14 & (1)\\ 2*x + 1*y + 2*z = 10 & (2)\\ 3*x + 2*y + 2*z = 13 & (3)\\ 3*x + 3*y + 1*z = 12 & (4)\end{array}\right\}$$

Persalygota

Overdefined linear system of equations

Let's consider the system consisting of (1), (2), (3) equations and their matrix denoting by M123, and the system consisting of (2), (3), (4) equations and their matrix denoting by M234

$$\begin{array}{ll}1*x + 2*y + 3*z = 14 & (1)\\ 2*x + 1*y + 2*z = 10 & (2)\\ 3*x + 2*y + 2*z = 13 & (3)\end{array}$$

$$\begin{array}{ll}2*x + 1*y + 2*z = 10 & (2)\\ 3*x + 2*y + 2*z = 13 & (3)\\ 3*x + 3*y + 1*z = 12 & (4)\end{array}$$

The matrices of these two systems of equations we denote by M123 and M234 respectively.
The salaries vectors of these two systems of equations we denote by s123 and s234 respectively.
The unknown variables x, y, z of these systems we denote by the vectors w123 and w234 respectively.
It is evident that vectors w123 and w234 satisfying both systems are equal, i.e. w123 = w234 = w.

```
>> w=[1;2;3]
w =
   1
   2
   3
```

```
>> M123=[1 2 3; 2 1 2; 3 2 2]
M123 =
  1   2   3
  2   1   2
  3   2   2
```

```
>> s123=[14;10;13]
S123 =
  14
  10
  13
```

```
>> M123i=inv(M123)
M123i =
 -0.4000   0.4000   0.2000
  0.4000  -1.4000   0.8000
  0.2000   0.8000  -0.6000
```

```
>> I=M123i*M123
I =
  1.0000   0.0000   0.0000
 -0.0000   1.0000   0.0000
  0.0000        0   1.0000
```

```
>> w123=M123i*s123
w123 =
  1
  2
  3
```

```
>> M234=[2 1 2; 3 2 2; 3 3 1]
M234 =
```

$$\begin{pmatrix} 2 & 1 & 2 \\ 3 & 2 & 2 \\ 3 & 3 & 1 \end{pmatrix} * \begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} 10 \\ 13 \\ 12 \end{pmatrix}$$

```
>> s234=[10;13;12]
s234 =
  10
  13
  12
```

```
>> M234i=inv(M234)
M234i =
  -4   5  -2
   3  -4   2
   3  -3   1
```

```
>> I=M234i*M234
I =
  1.0000e+00  -8.8818e-16  -8.8818e-16
  6.6613e-16   1.0000e+00   2.2204e-16
  6.6613e-16   2.2204e-16   1.0000e+00
```

```
>> w234=M234i*s234
w234 =
  1
  2
  3
```

Let's change a little the initial system of 4 equations by adding to the right side -1, 1, or 0 at random.

1*x + 2*y + 3*z = 14	(1)	1*x + 2*y + 3*z = 14 - 1	1*x + 2*y + 3*z = 13 = s1e
2*x + 1*y + 2*z = 10	(2)	2*x + 1*y + 2*z = 10 + 0	2*x + 1*y + 2*z = 10 = s2e
3*x + 2*y + 2*z = 13	(3)	3*x + 2*y + 2*z = 13 +1	3*x + 2*y + 2*z = 14 = s3e
3*x + 3*y + 1*z = 12	(4)	3*x + 3*y + 1*z = 12 - 1	3*x + 3*y + 1*z = 11 = s4e

Then we introduce the erroneous vector for the system consisting of (1), (2), (3) equations denoting it by s123, and the erroneous vector for the system consisting of (2), (3), (4) equations denoting it by s234.
The corresponding matrices M123 and M234 are introduced above.

```
>> s123e=[13;10;14]
 s123e =
   13
   10
   14
```

```
>> s234e=[10;14;11]
s234e =
   10
   14
   11
```

Then the solution of the first system of equations can be found by computing the inverse matrix to the matrix M123 we denote by M123i, and

the solution of the second system of equations can be found by computing the inverse matrix to the matrix M234 we denote by M234i

```
>> w123e=M123i*s123e
w123e =
 1.6000
   2.4000
   2.2000
```

```
>> w234e=M234i*s234e
w234e =
  6.0000e+00
 -2.0000e+00
  7.1054e-15
```

1.6000	6.0000e+00
2.4000	-2.0000e+00
2.2000	7.1054e-15

As we see solutions differs.
It is an **inconsistent** system of linear equations.

Till this place

This system of equations can be writthen matrix form: ***Mw*** = ***e***,
Where ***w*** = (x, y, z) is vector of unknown salaries x, y, z and ***e*** is a vector of total earnings written in column.
If transposed vector **e** we denote by **e'** then it can be written in a row: **e'** = (14, 10, 13).
This data in Octave is formed in the following way:

```
>> M=[1 2 3; 2 1 2; 3 2 2]
M =

  1  2  3      x
  2  1  2      y
  3  2  2      z
```

```
>> e=[14;10;13]
e =

  14
  10
  13
```

```
>> et=e'
et =

  14  10  13
```

```
> inv(M)
ans =

 -0.4000   0.4000   0.2000
  0.4000  -1.4000   0.8000
  0.2000   0.8000  -0.6000
```

The solution of this linear system of equations is found by the following Octave commands:

```
>> Me=[M e]
Me =

  1   2   3  14
  2   1   2  10
  3   2   2  13
```

```
>> rref(Me)
ans =

  1  0  0  1
  0  1  0  2
  0  0  1  3
```

```
>> w=ans(:,end)
w =

  1  Đ
  2  Đ
  3  Đ
```

DDDĐ

In Thursday **Alex** worked 3 hour, **Bill** worked 3 hours, **Cecilia** worked 1 hour: they all earned 12 Đ.
This 4-th condition yields the 4-th equation of the form:
3*x + 3*y + 1*z = 13   (4)

Let's take an equations (2), (3), (4) and create the following system of equations:

2*x + 1*y + 2*z = 10   (2)
3*x + 2*y + 2*z = 13   (3)
3*x + 3*y + 1*z = 12   (4)

The unknown variables x, y, z of this system are the same forming the same vector ***w*** = (x, y, z).
The Matrix of created system of equations we denote by $\boldsymbol{M}_{234}$ and corresponding earnings as $\boldsymbol{e}_{234}$.
In Octave representation they have the following form:

```
>> M234=[2 1 2; 3 2 2; 3 3 1]          > e234=[10;13;12]
```

```
>> M234=[2 1 2; 3 2 2; 3 3 1]          > e234=[10;13;12]
M234 =                                 e234 =

  2   1   2        x                     10
  3   2   2        y                     13
  3   3   1        z                     12
```

The solution of this linear system of equations is found in the same way by the following Octave commands:

```
>> M234e234=[M234 e234]          >> rref(M234e234)          >> w=ans(:,end)
M234e234 =                       ans =                      w =

   2   1   2  10                   1  0  0  1                 1
   3   2   2  13                   0  1  0  2                 2
   3   3   1  12                   0  0  1  3                 3
```

In this case it is said that system of equations is **inconsistent**