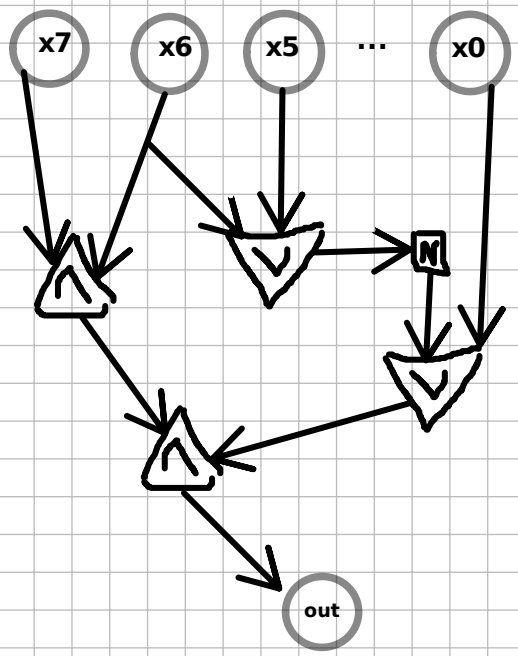
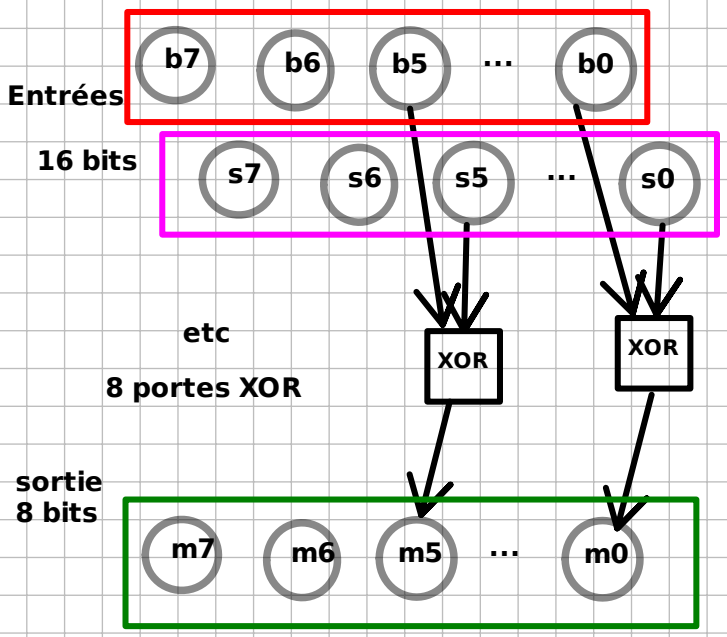
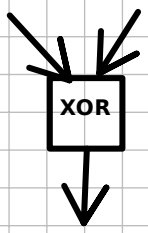

x7
x6
x5
...
x0
N
out

Message en clair que je souhaite crypter (ici le code ascii en binaire d'une lettre)



Bits du message
(8 bits pour une lettre)

Bits de la clé secrète
(aussi long que le message, 8 bits)



voir exo semaine dernière
peut être réalisé par des portes ET, OU et NON.

message chiffré par le protocole de Vernam.

32 bits.

Combien de nombre je peux coder?

2^32

En pratique la mémoire est adressable si j'ai 64 bits, je peux avoir 2^64 adresses.

2^64 = 2^32 * 2^32

Retour sur l'exercice du XOR.

On se deonne des portes concrètes binaires (ET, OU) et des portes unaires (le NON). On souhaite en les branchant fabriquer un circtui qui calcule le XOR (ou exclusif) de 2 entrées.

X	y	x xor y
0	0	0
0	1	1
1	0	1
1	1	0

cahier des charges

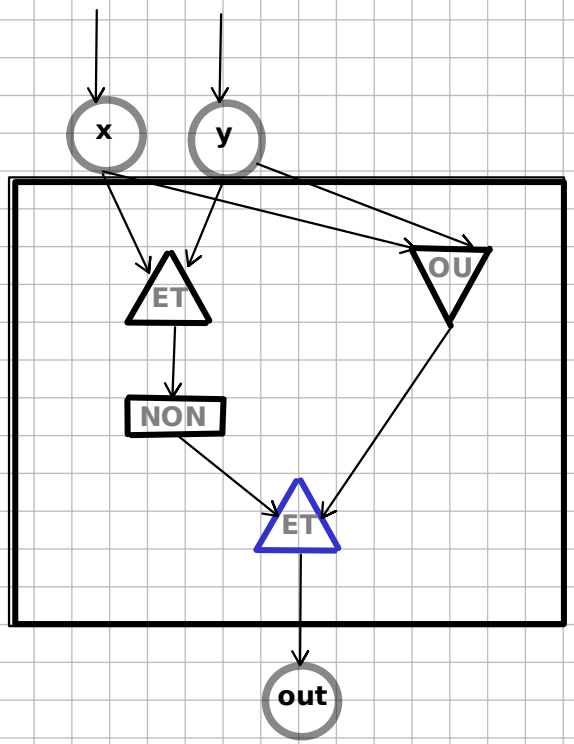
X	y	x et y
0	0	0
0	1	0
1	0	0
1	1	1

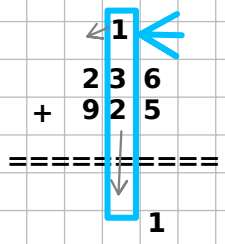
X	y	x OU y
0	0	0
0	1	1
1	0	1
1	1	1

x	Non
0	1
1	0

brouillon

Non(x et y)	ET	x Ou y
1	0	0
1	1	1
1	1	1
0	0	1





On peut voir le calcul colonne par colonne comme une opération qui produit un chiffre
et une retenue
à partir de 3 valeurs 2 chiffres & l'ancienne retenue.

Pourquoi ça marche?

2 3 6 c'est la somme de

2*100 3*10 6*1

Retenue

1*1000 +0*100 + 1*10

0*1000 + 2*100 + 3* 10 + 6 * 1

0*1000 + 9*100 + 2* 10 + 5* 1

==========

6

Retenue 1

11 = 1*10 + 1*1

NB : même principe
si à une autre position

2*100+9*100 =
11*100 =
10*100 +1*100 =
1*1000 + 1*100

Pourquoi faire le calcul de droite à gauche?

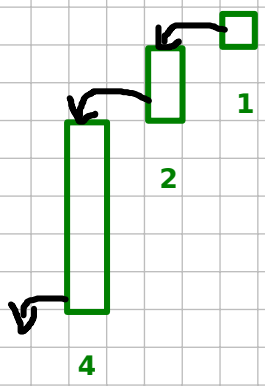
Car en pratique la retenue ne peut pas déborder vers la droite.
Sur un exemple :

xxxxx00
xxxxx00
?????00

8 * 100 + 6 * 100 = ? * 1000+?*100 + 0*10 + 0*1.

(8+6)*100

Retenue = vases successifs qui débordent.

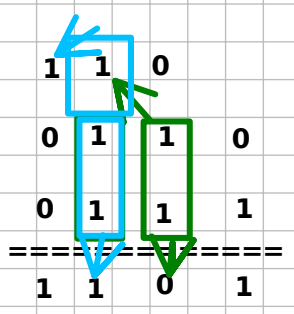


etc

Et en binaire?

Même principe sauf qu'il faut aprendre le calcul binaire pour les retenues

1 + 1 en binaire vaut 2 en décimal qui s'écrit
1 fois 2 plus 0 fois 1
soit 10 en binaire



1+1+1 en binaire vaut 1+(1+1) en binaire
soit 1+(10) en binaire
qui fait 11 en binaire

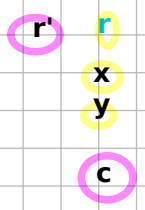
On peut vérifier en décimal que 1+1+1 c'est 3
que 3 s'écrit 2+1 = 1*2 + 1*1 c'est-à-dire 11 en binaire.

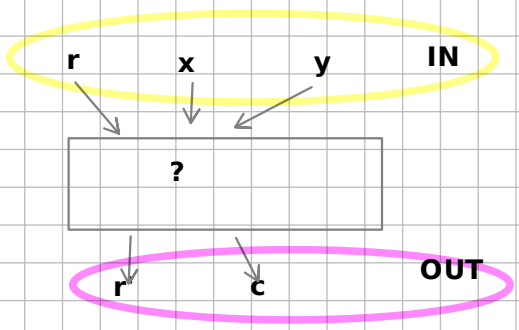
retenue précédente dans la même colonne qui vient du passé

r	x	y	retenue future	chiffre
0	0	0	0	0
0	0	1	0	1
0	1	0	0	1
0	1	1	1	0
1	0	0	0	1
1	0	1	1	0
1	1	0	1	0
1	1	1	1	1

Le calcul de la retenue, peut être vu comme un vote de majorité
2 candidats (0 ou 1)
Je réponds 1 si j'ai 2 ou 3 "votes" pour 1
Je réponds 0 si j'ai 2 ou 3 "votes" pour 0

Shéma de ce qu'on cherche au coeur de notre circuit qui va faire une addition

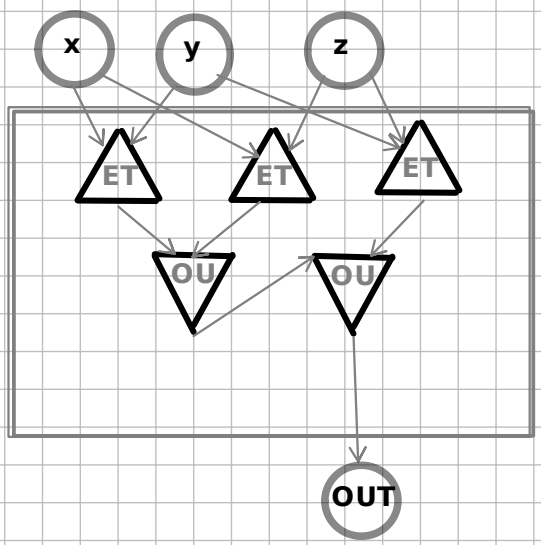


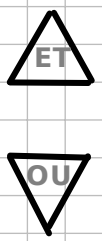


1)

Majorité : (x et y valent 1)
ou (x et z valent 1)
ou (y et z valent 1)

On peut séparer le problème
1) la retenur
2) le chiffre





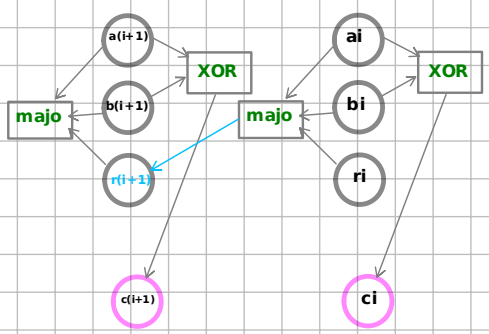
2)

Calcul des chiffres :

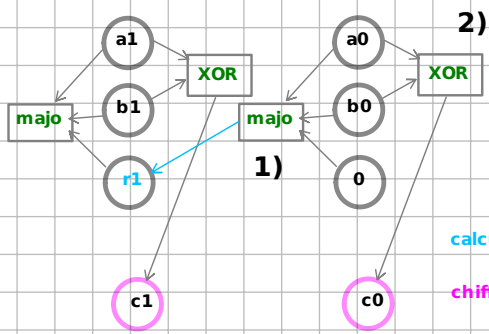
C'est le XOR des 3 bits.

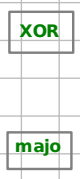
(admis)

Sens du calcul



etc





calcul intermédiaire des retenues

chiffres du résultat

Question : comment faire pour la dernière retenue?

Autre question : peut-on économiser des portes en mélangeant le circuit pour XOR et celui pour maj?