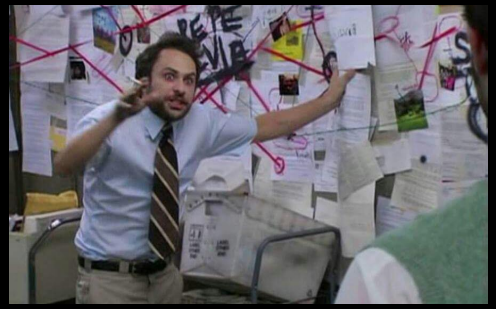
Chercheuse en sécurité informatique

Comment la société
me voit

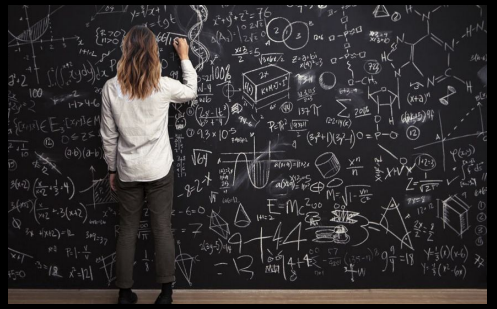


Comment on me voit quand
j'explique mes idées

Comment l'Etat me voit

Comment je me sens quand
j'attaque un chiffrement

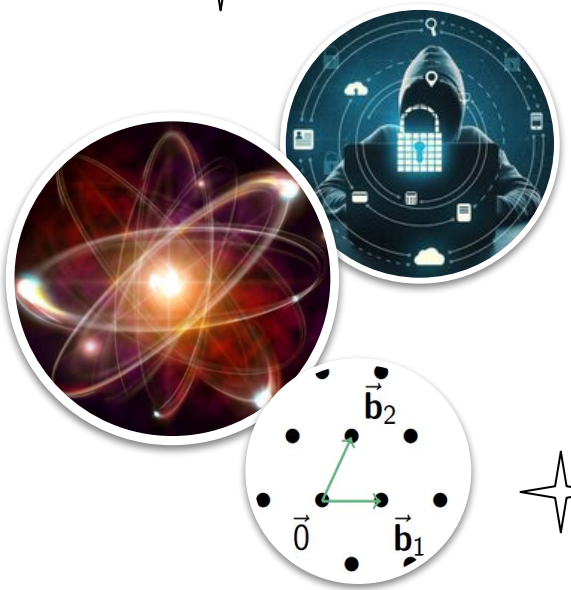
Comment mon copain me voit
quand je suis en télétravail



Ce que je fais vraiment

Cryptanalyse quantique des lattices

Dr. Johanna Loyer



52 av. J.C.

Chiffre de César

PREPAREZ LE PIEGE
SUR LA COLLINE
D'ALESIA

QSFQBSFA MF QJFHF
TVS MB DPMMJOF
E'BMFTJB

Chiffrer
A → B
B → C
C → D
...
Y → Z
Z → A

Déchiffrer
A → Z
B → A
C → B
...
Y → W
Z → Y

Chiffre de César

Chiffrer
A → B
B → C
C → D
…
Y → Z
Z → A

PVQT, QBT TJ
TFDVSJTF RVF DB !

Déchiffrer
A → Z
B → A
C → B
…
Y → W
Z → Y

Chiffre de César

Chiffrer
A → B
B → C
C → D
...
Y → Z
Z → A

OUPS, PAS SI SECURISE QUE CA !

PVQT, QBT TJ TFDVSJTF RVF DB !

Déchiffrer
A → Z
B → A
C → B
...
Y → W
Z → Y

Enigma

1939

- 83 - ADJ JNA -

LMHNX WEKLM UERDS EVHLC
JSQQK VLDES ANEVT YEDGI
ZQDOD RMDKG SXGSQ SHDQP
VIEAP IENLI CLZCL LAGWC
BJZD

Enigma

1939

- 83 - ADJ JNA -

LMHNX WEKLM UERDS EVHLC
JSQQK VLDES ANEVT YEDGI
ZQDOD RMDKG SXGSQ SHDQP
VIEAP IENLI CLZCL LAGWC
BJZD

Cryptanalyse

Enigma

1939

- 83 - ADJ JNA -

LMHNX WEKLM UERDS EVHLC
JSQQK VLDES ANEVT YEDGI
ZQDOD RMDKG SXGSQ SHDQP
VIEAP IENLI CLZCL **HEIL**
HITLER

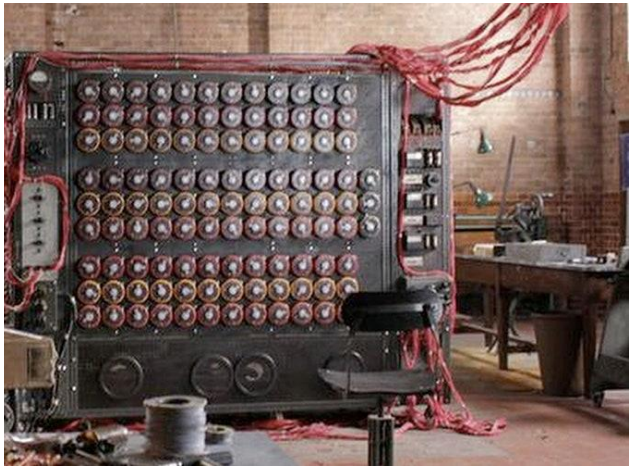
Cryptanalyse

Enigma

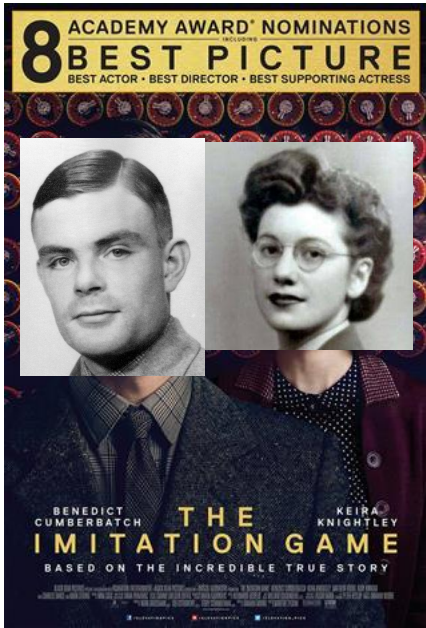
1939

- 83 - ADJ JNA -

LMHNX WEKLM UERDS EVHLC
JSQQK VLDES ANEVT YEDGI
ZQDOD RMDKG SXGSQ SHDQP
VIEAP IENLI CLZCL **HEIL**
HITLER



Cryptanalyse

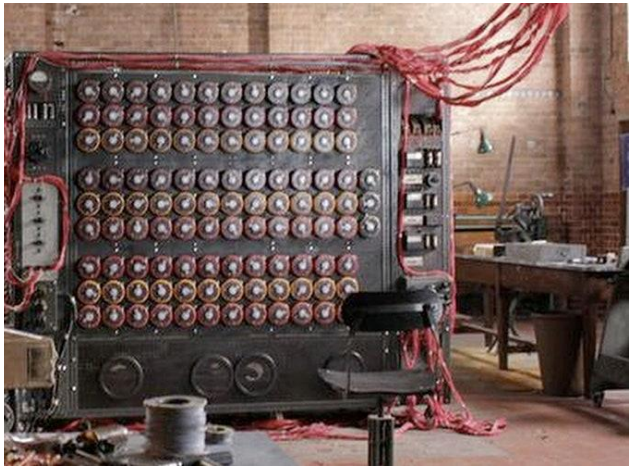


Enigma

1939

- 83 - ADJ JNA -

LMHNX WEKLM UERDS EVHLC
JSQQK VLDES ANEVT YEDGI
ZQDOD RMDKG SXGSQ SHDQP
VIEAP IENLI CLZCL **HEIL**
HITLER



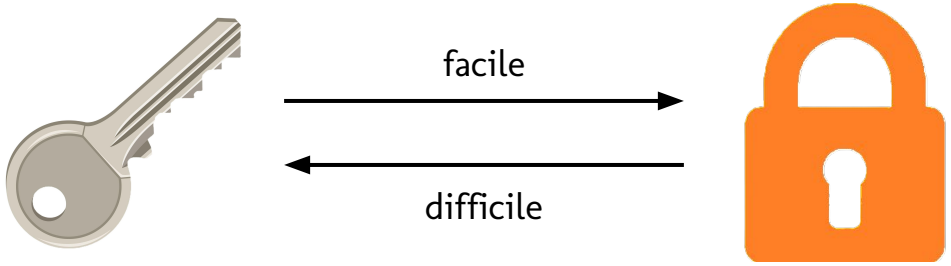
Cryptanalyse

Années 1970

Années 1970

Pourquoi la sécurité informatique est-elle importante ?

Chiffrement asymétrique



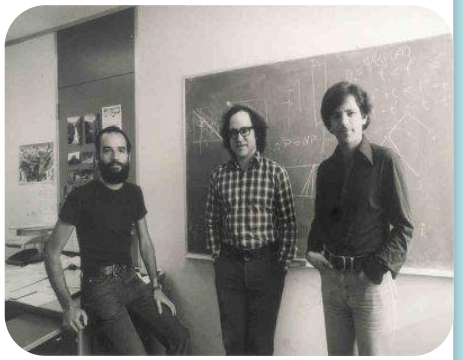
Chiffrement asymétrique

Nombres premiers
P et Q

facile

difficile

P x Q



Rivest, Shamir & Adleman

P x Q =

74878699273822876703064100565258237666411689559192594203231204582142538055207300529107695893101544302285678867823222531639866636710659744105915162579167843270306555246801155878556576226941551105463408603339191780725522801191200608171918541903015033793585331447145527846567719938866348562414058098801174410295089751917375133263563865933238557538941723730338075606925266631282392347185904432064577557685220581069833747643821937065461995187624955073855467031904244121946465203504873765791374992250323841791944925639154313605530971632068666907223368419736311550104287833712374108664439422637803390559200661604067300560819104161704706205200664074137162928870311324415793998060900514238053152075799254400484063330872200400824694161458762313699244427168410010234953322369230131008875207144178060016690500990949035506940693521719866602606841848144161385641366094783418163579176641469113458683986636271624156226808640075322348660856868239917652135854264247202737344360664539192915544469799363161283822017014838671695003776896400160348133286390895951889005438424738056352165480745114676326959230635700000124926420279435942759877089278064723846752483221531798870290858806573151284453558386481970879327217338061580998730755633028370075723805063

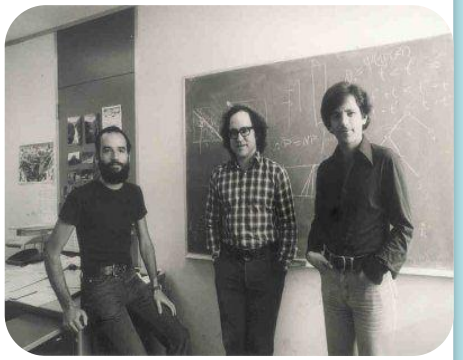
Chiffrement asymétrique

Nombres premiers
P et Q

facile

difficile

P x Q



Rivest, Shamir & Adleman

Chiffrement asymétrique

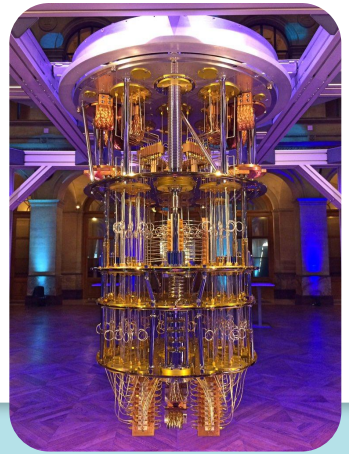
Nombres premiers
P et Q

facile

difficile

facile avec un
ordinateur quantique !

P x Q



Ordi classique : 0 ou 1

Ordi quantique : 0 et 1
en même temps

Physique quantique

Particule quantique dans plusieurs états en même temps

Chat de Schrödinger

Physique quantique

Particule quantique dans plusieurs états en même temps

Chat de Schrödinger

« Personne ne comprend vraiment la physique quantique. »

— Richard Feynman

Qui veut construire un ordinateur quantique ?

SORBONNE UNIVERSITÉ

Inria

HARVARD UNIVERSITY

YALE

UNIVERSITY OF CAMBRIDGE

UNIVERSITY OF OXFORD

NATIONAL SECURITY AGENCY
UNITED STATES OF AMERICA

Google

IBM

Alibaba Group

Microsoft

D-Wave
The Quantum Computing Company™

rigetti

PASQAL

QUANDELA

ALICE & BOB

Edward Snowden

Petit résumé jusqu'ici

Chiffrement

Chiffre de César

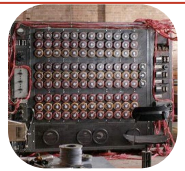
Enigma

R.S.A. (P x Q)

???

Facile à la main !

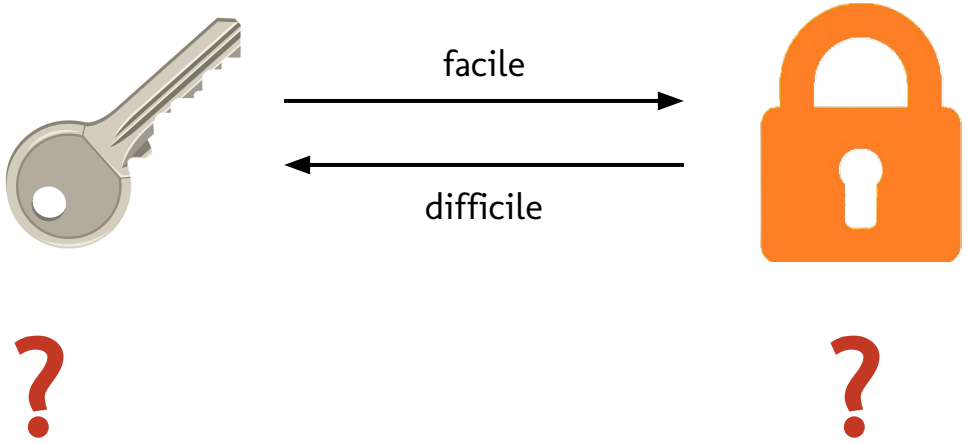
Ordinateurs



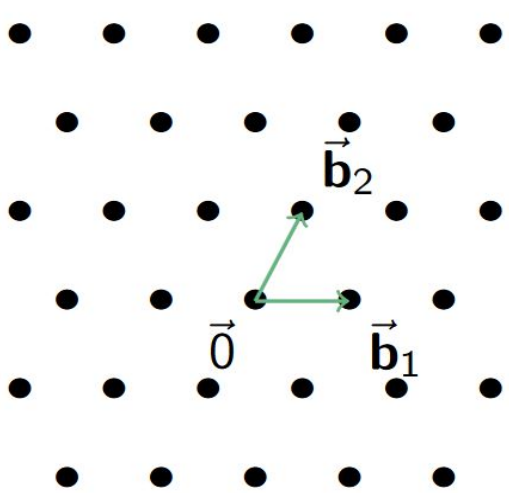
Ordinateur quantique

Cryptanalyse

Chiffrement “post-quantique”

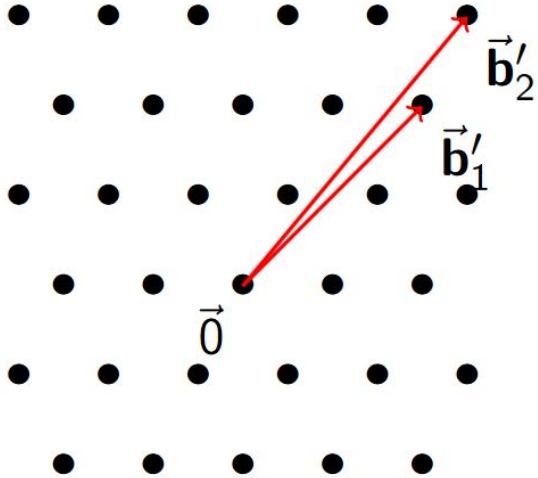


Chiffrement “post-quantique”



facile

difficile (?)

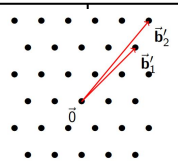


Chiffrement

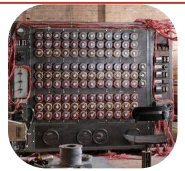
Enigma

R.S.A.
(P x Q)

Lattices



Ordinateurs



Ordinateur quantique

???

Cryptanalyse

Les lattices sont-ils aussi sécurisés qu’on le croit ?

Plan

1

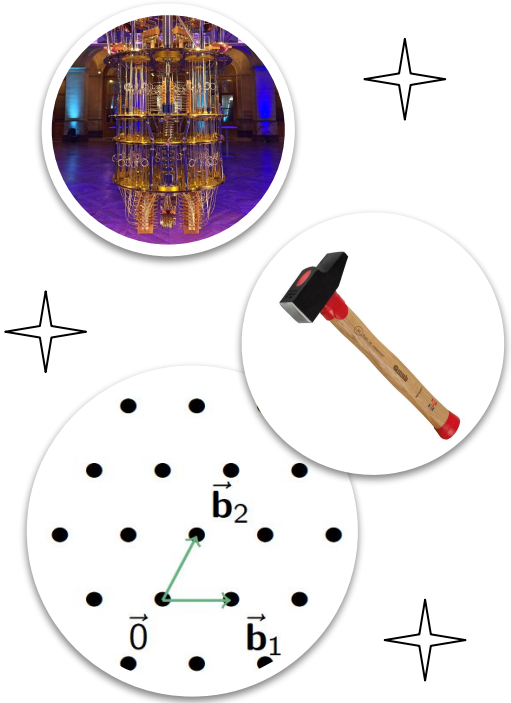
Attaque sur les lattices

2

Amélioration de l’attaque

3

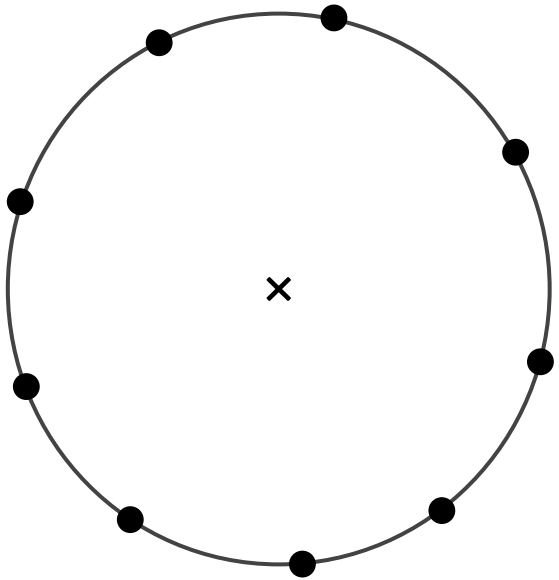
Mon attaque



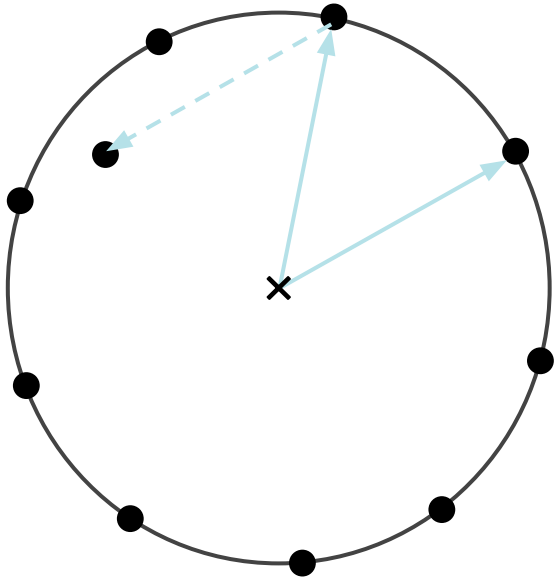
Attaque sur les lattices

En combien de temps peut-on retrouver un petit vecteur ?

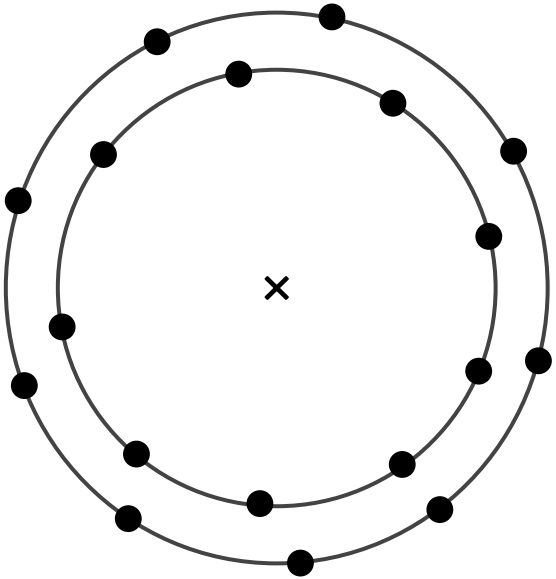
Méthode du crible



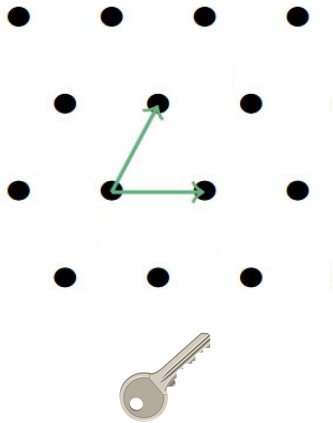
Méthode du crible

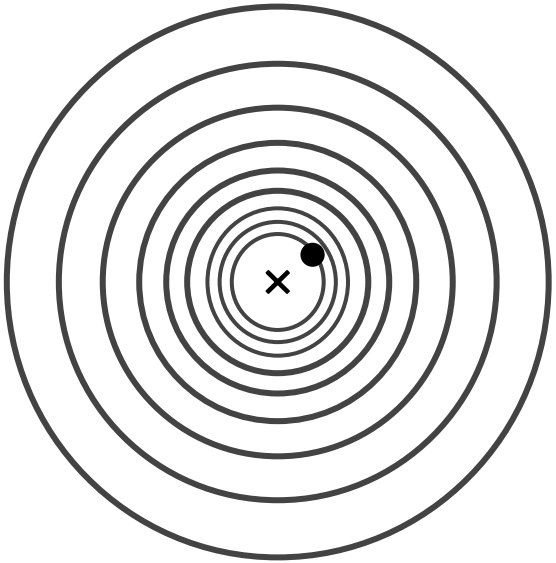


Méthode du crible



Méthode du crible





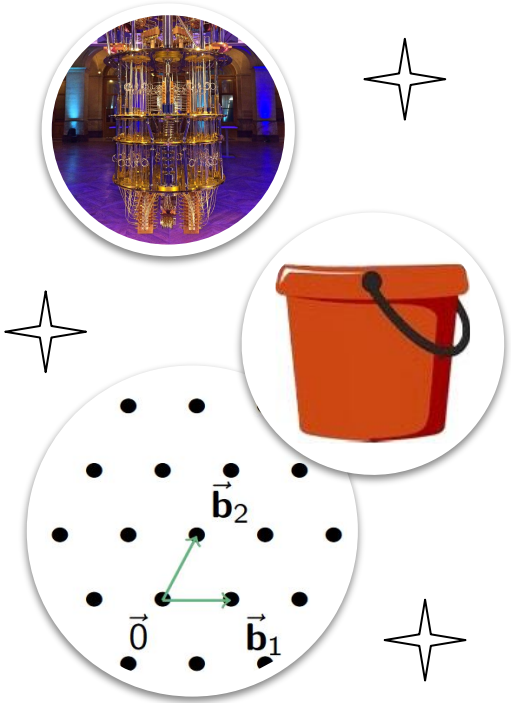
Temps de l'attaque :

$10^{0.125d}$ opérations

Meilleure attaque > 10^{39} :
"Sécurisé"

En dimension d=308 :

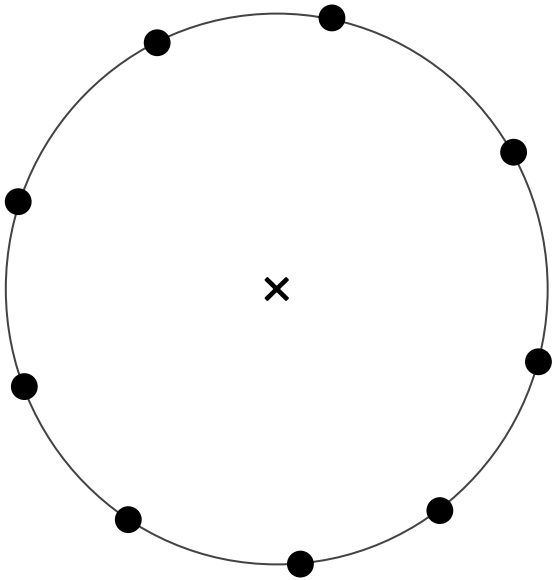
$10^{0.125d} = 10^{39}$



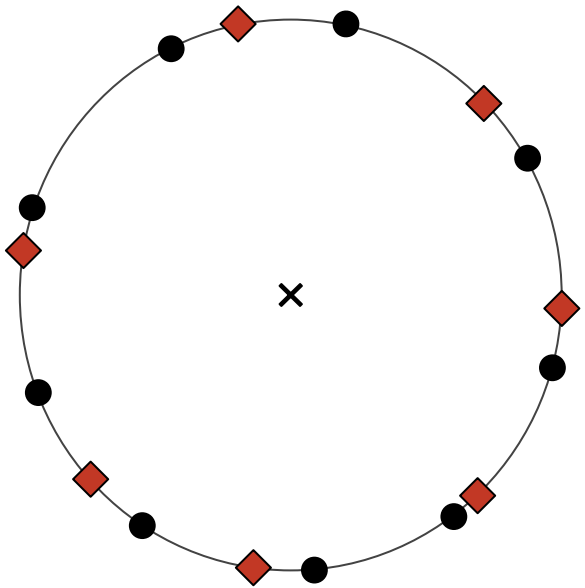
Amélioration de l'attaque

Comment trouver les points proches plus rapidement ?

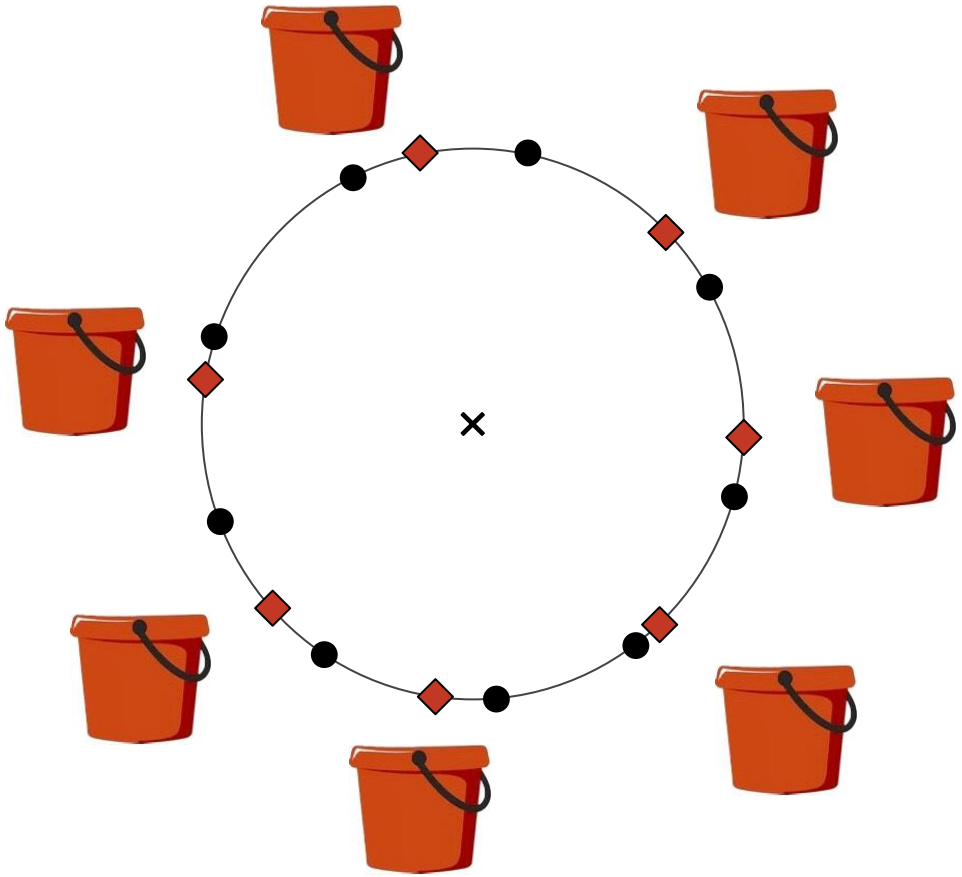
Filtrage



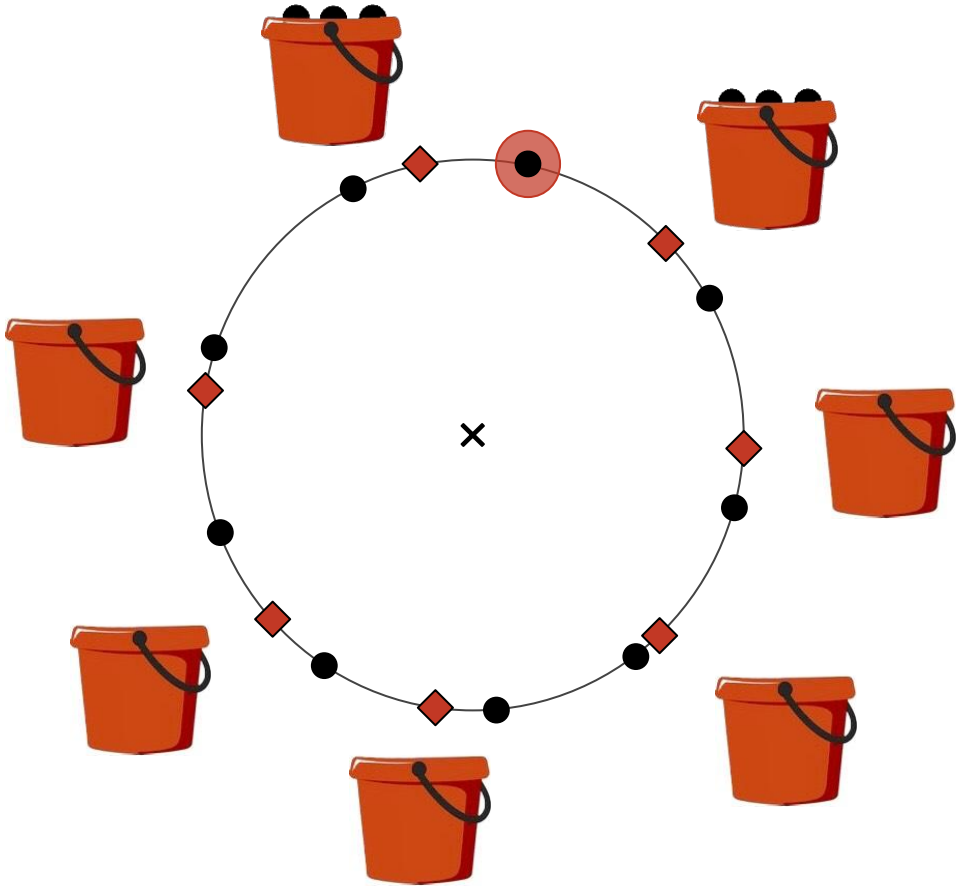
Filtrage



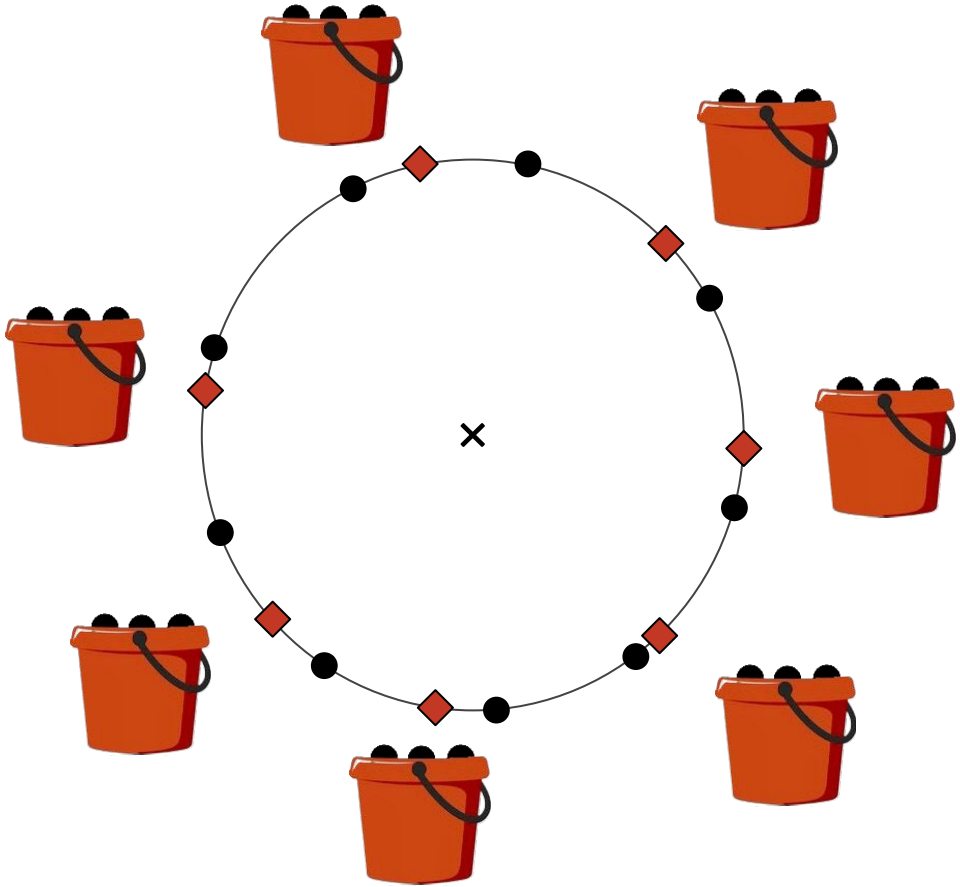
Filtrage



Filtrage



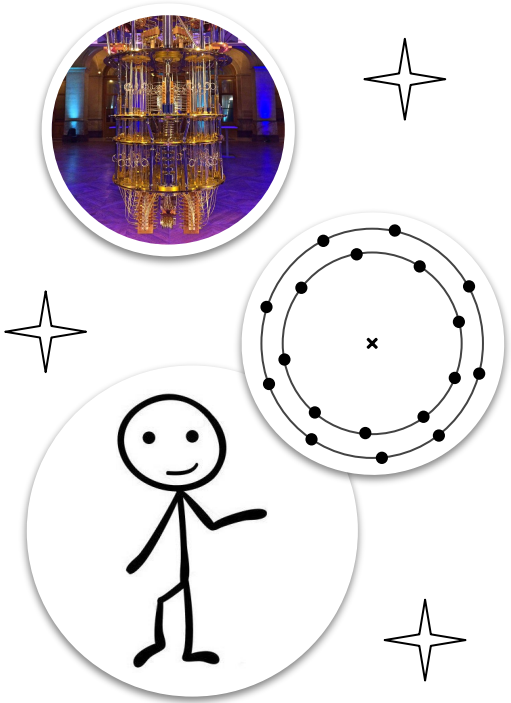
Filtrage



Méthode du crible avec filtrage

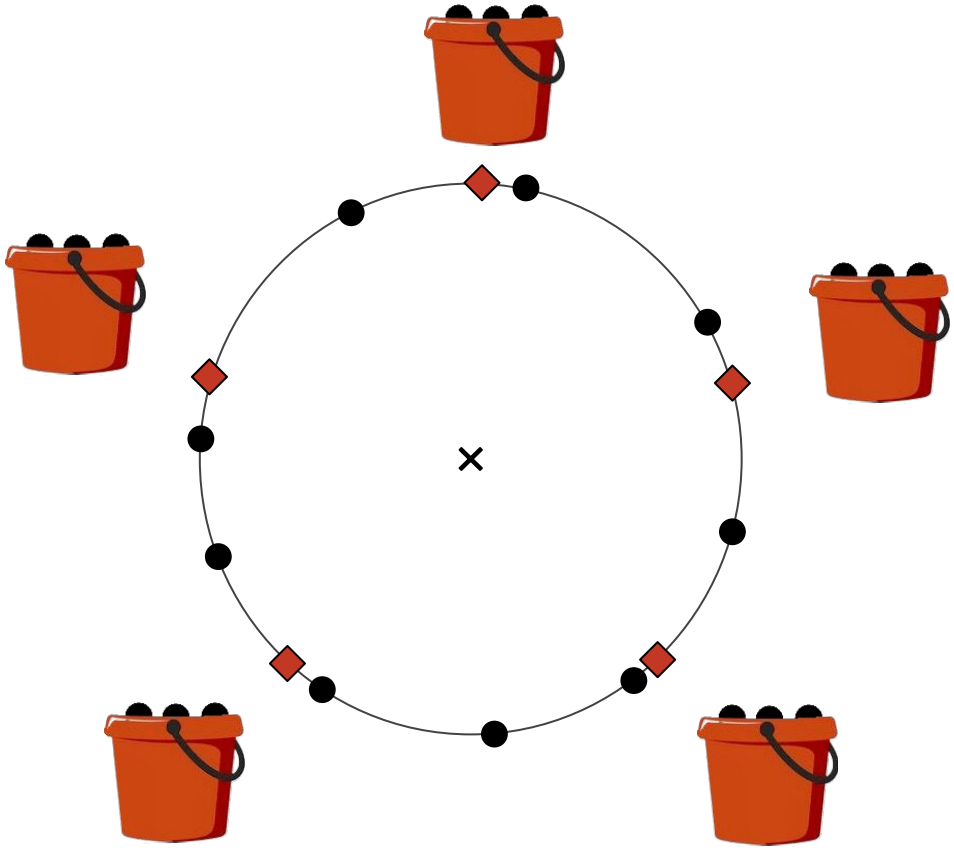
d = 500	Classique	Quantique
Sans filtrage	10^{62}	10^{47}
Avec filtrage 	10^{44}	10^{40}

Nombre d'opérations des attaques
$> 10^{39}$ "Sécurisé"



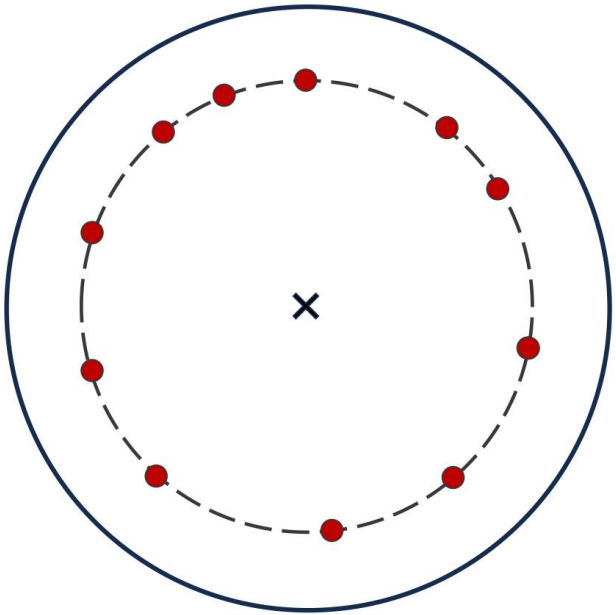
Mon attaque

(avec Sticky en guest star)

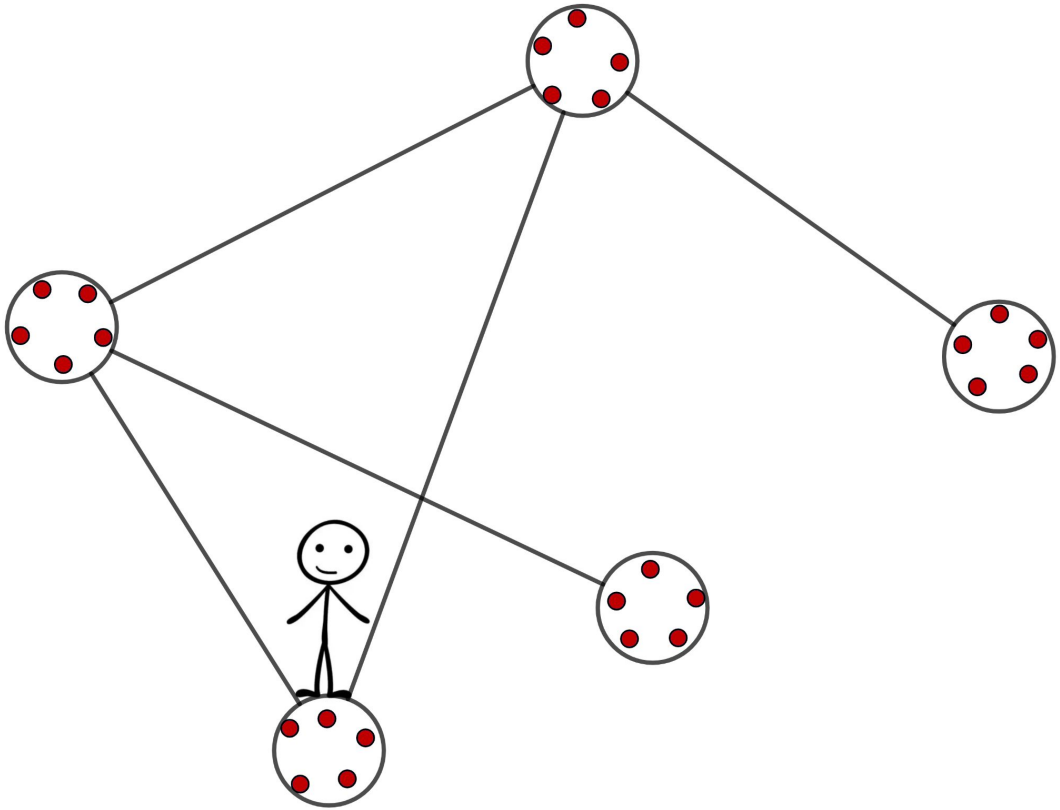


Objectif : Trouver 2 points proches dans 

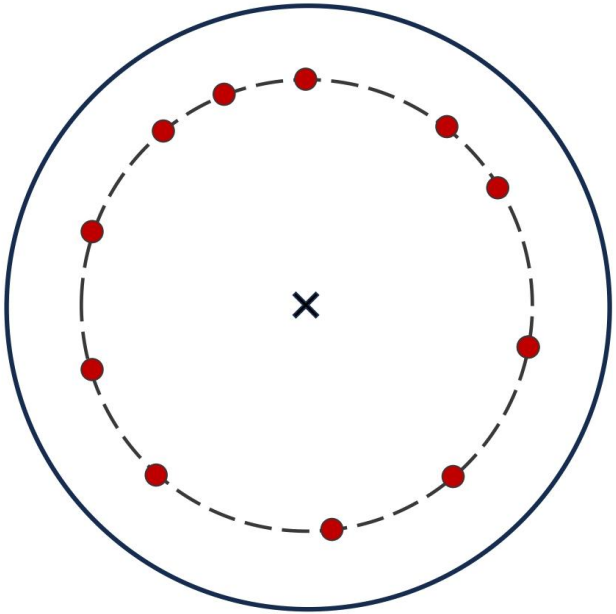
Objectif : Trouver 2 points proches dans 



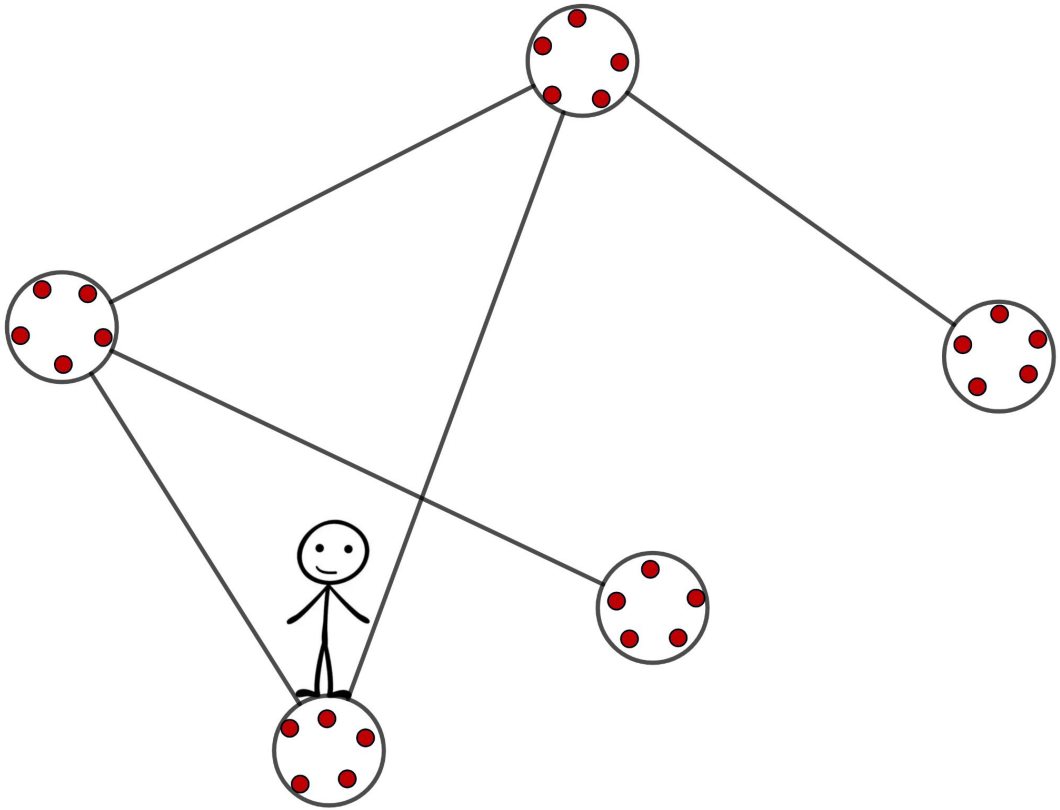
Objectif : Trouver 2 points proches dans 

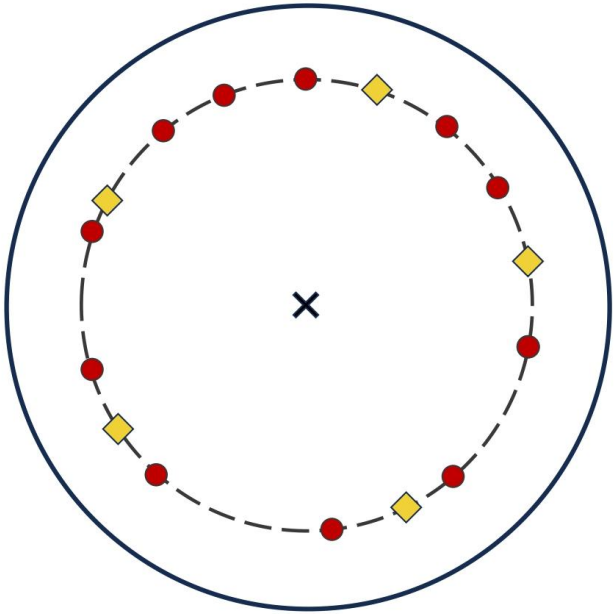


Zoom sur l'ensemble de points où se trouve Sticky

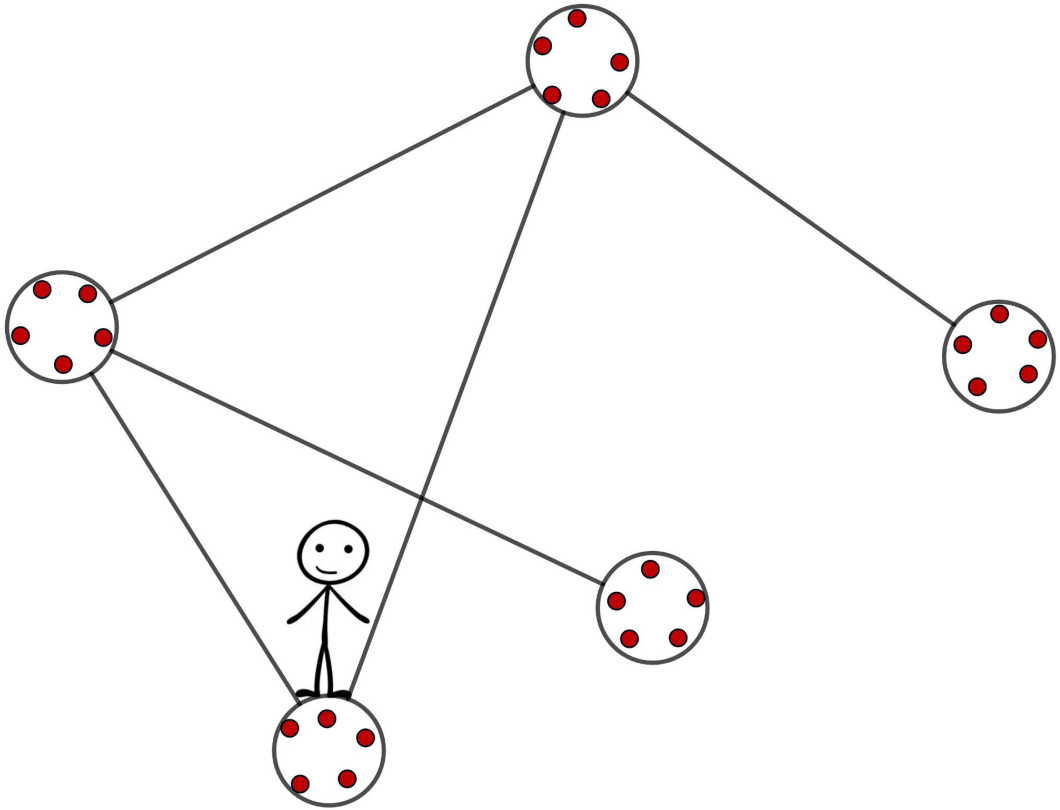


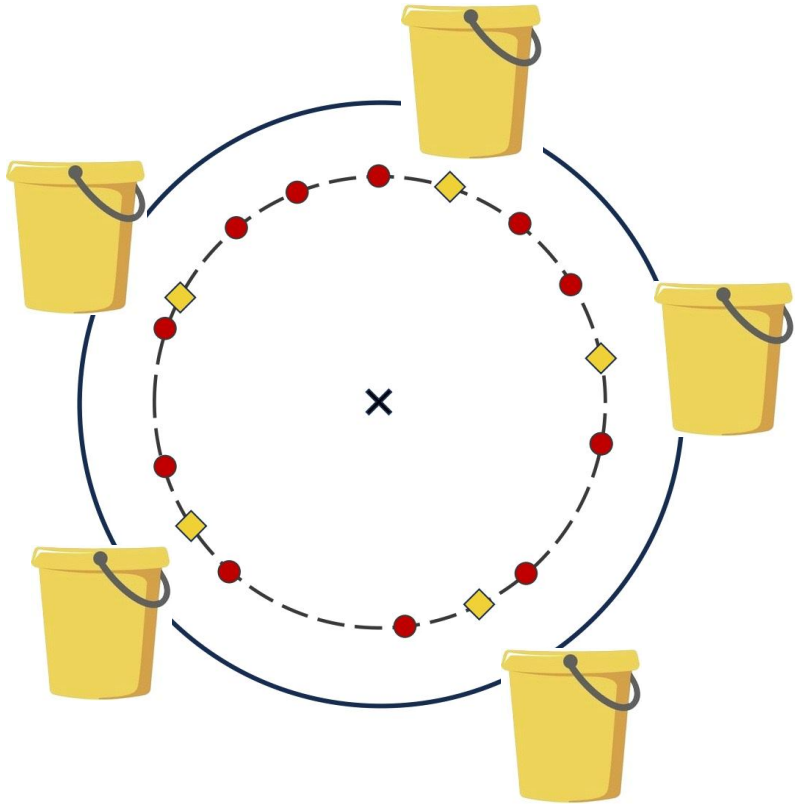
Objectif : Trouver 2 points proches dans 



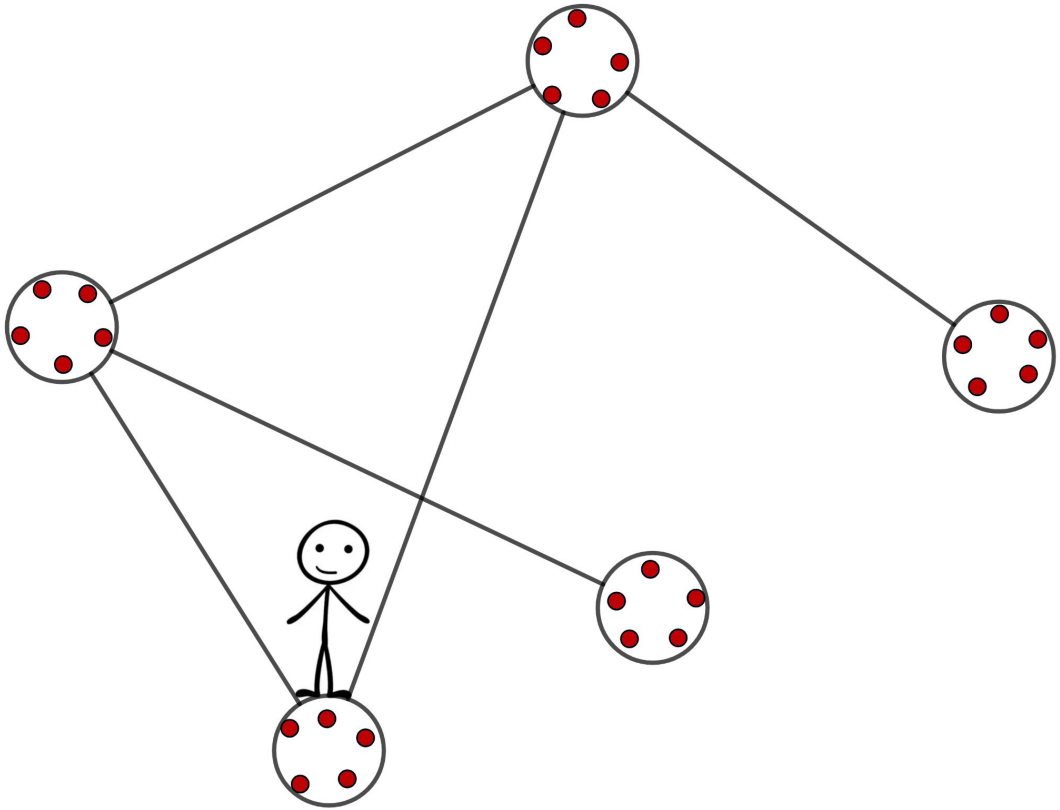


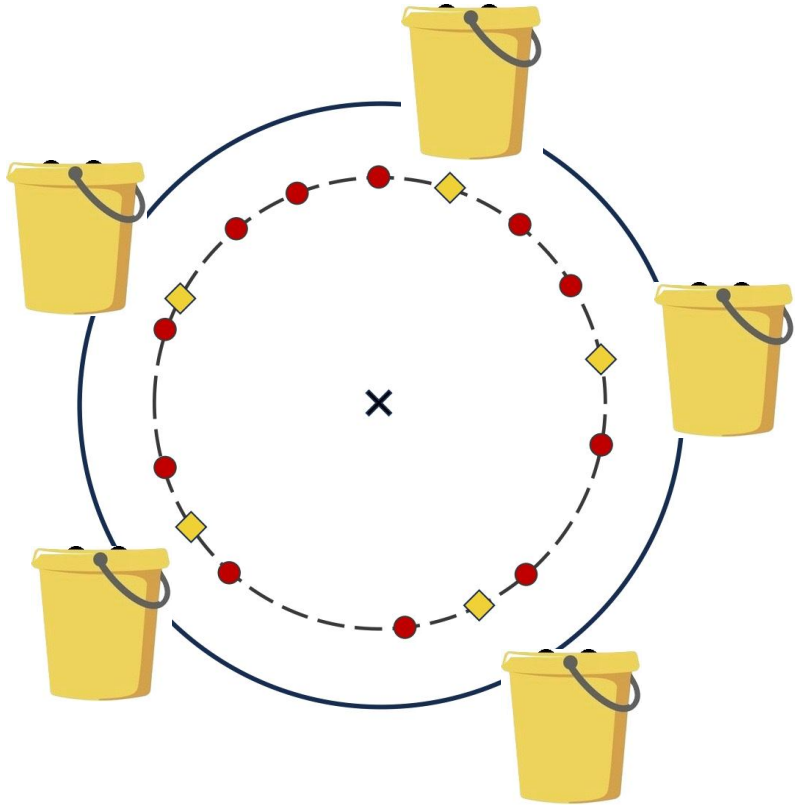
Objectif : Trouver 2 points proches dans 



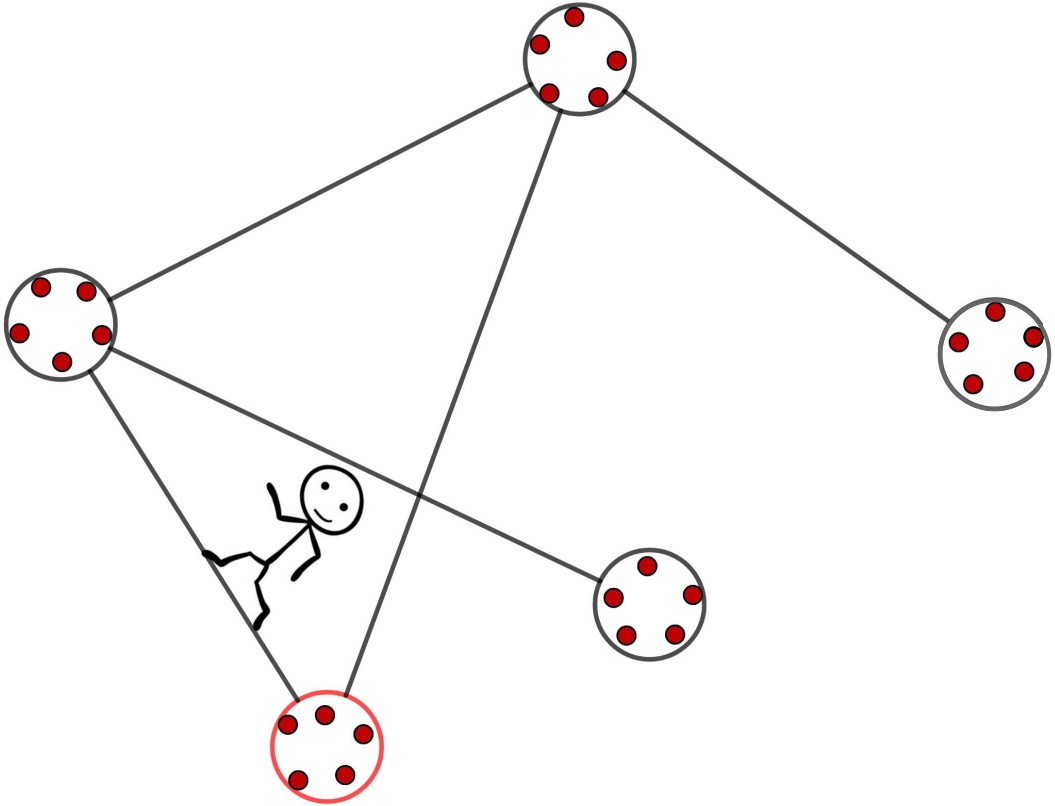


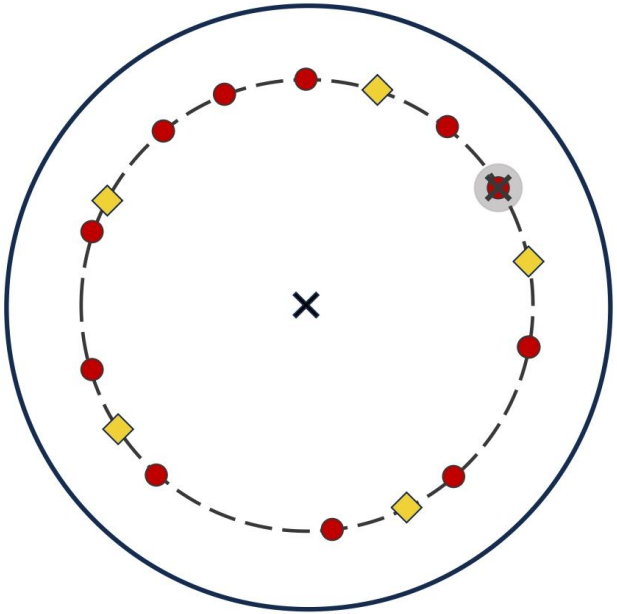
Objectif : Trouver 2 points proches dans 



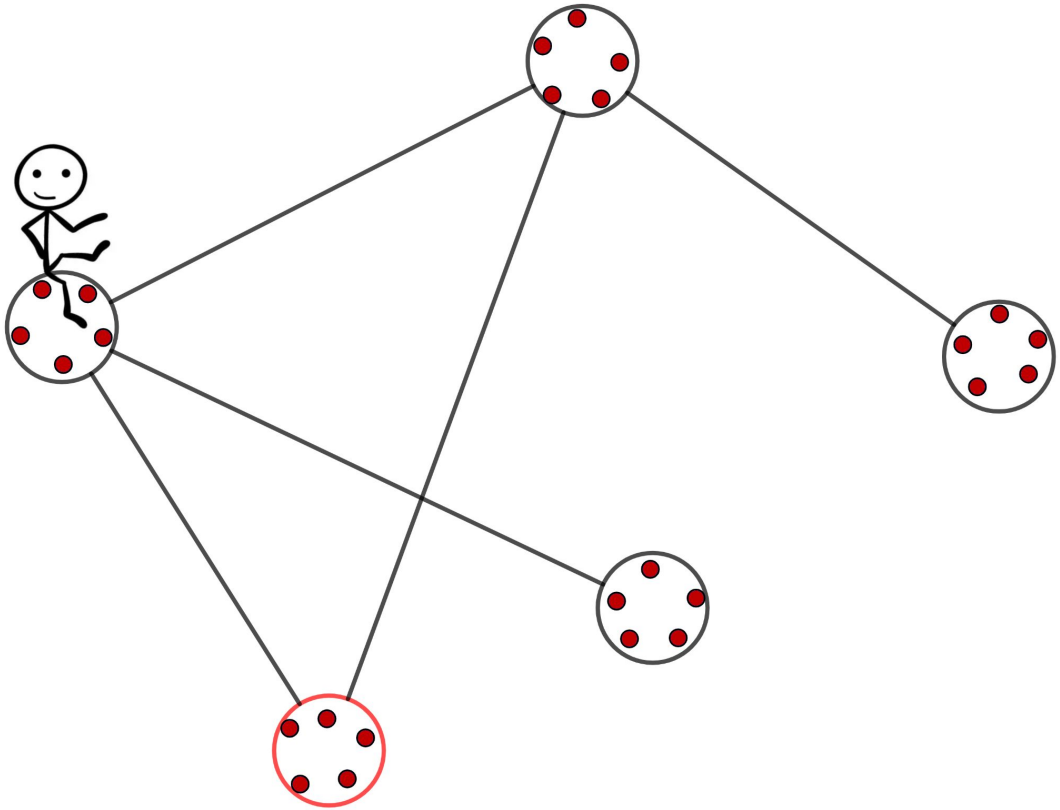


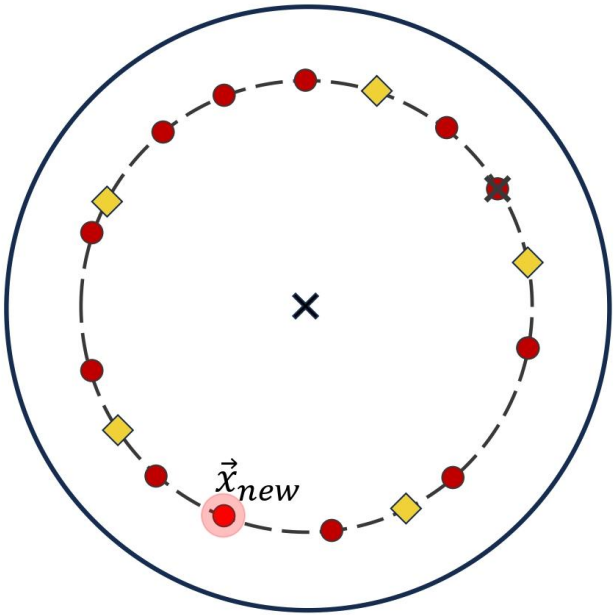
Objectif : Trouver 2 points proches dans 



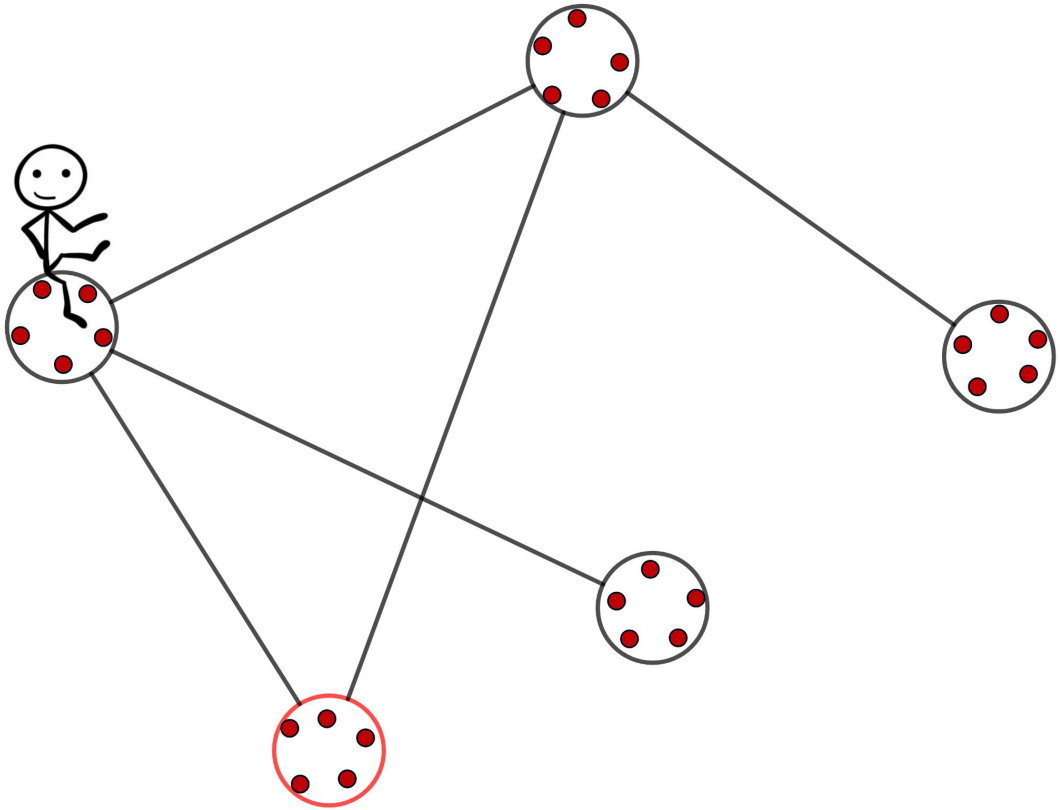


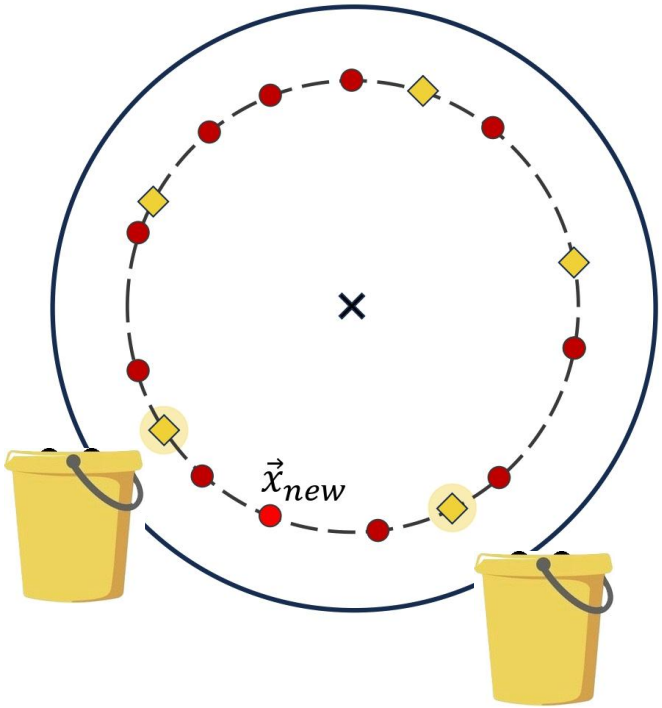
Objectif : Trouver 2 points proches dans



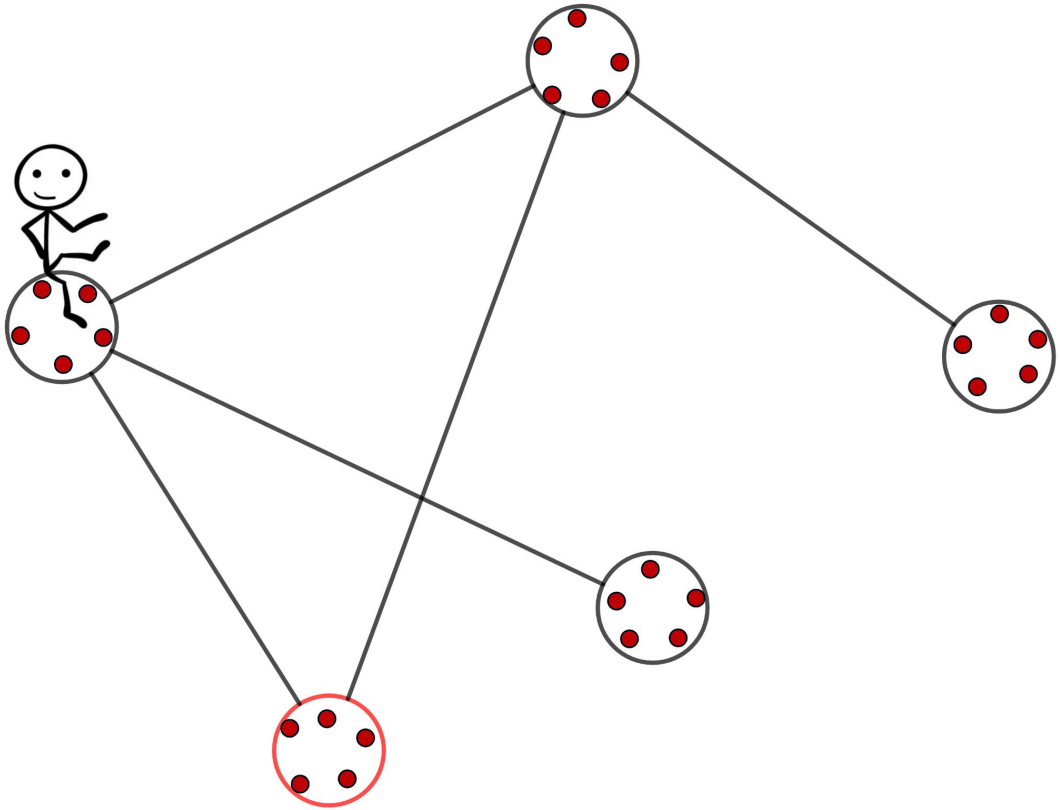


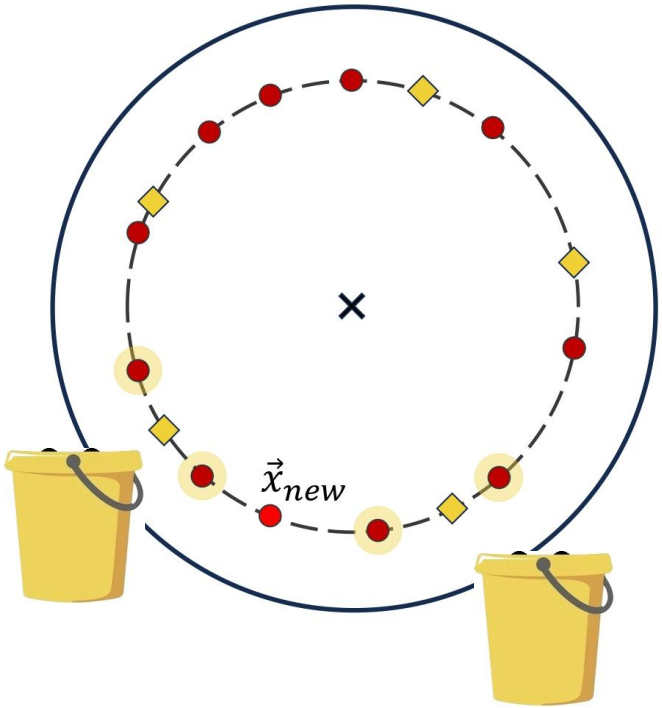
Objectif : Trouver 2 points proches dans 



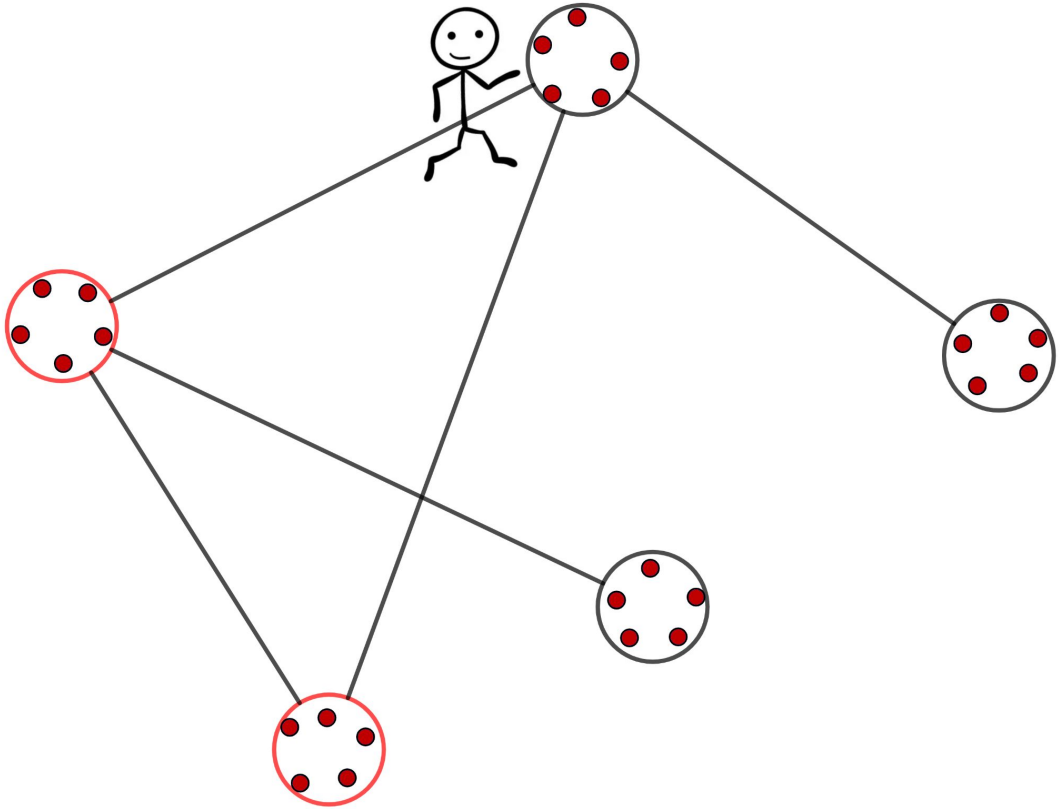


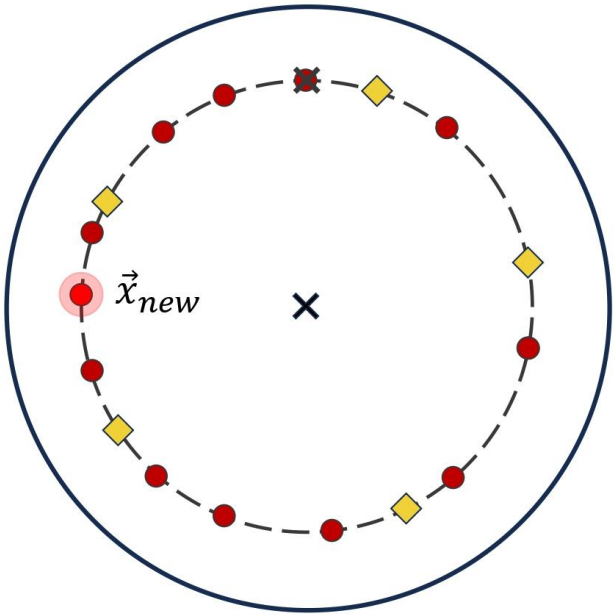
Objectif : Trouver 2 points proches dans 



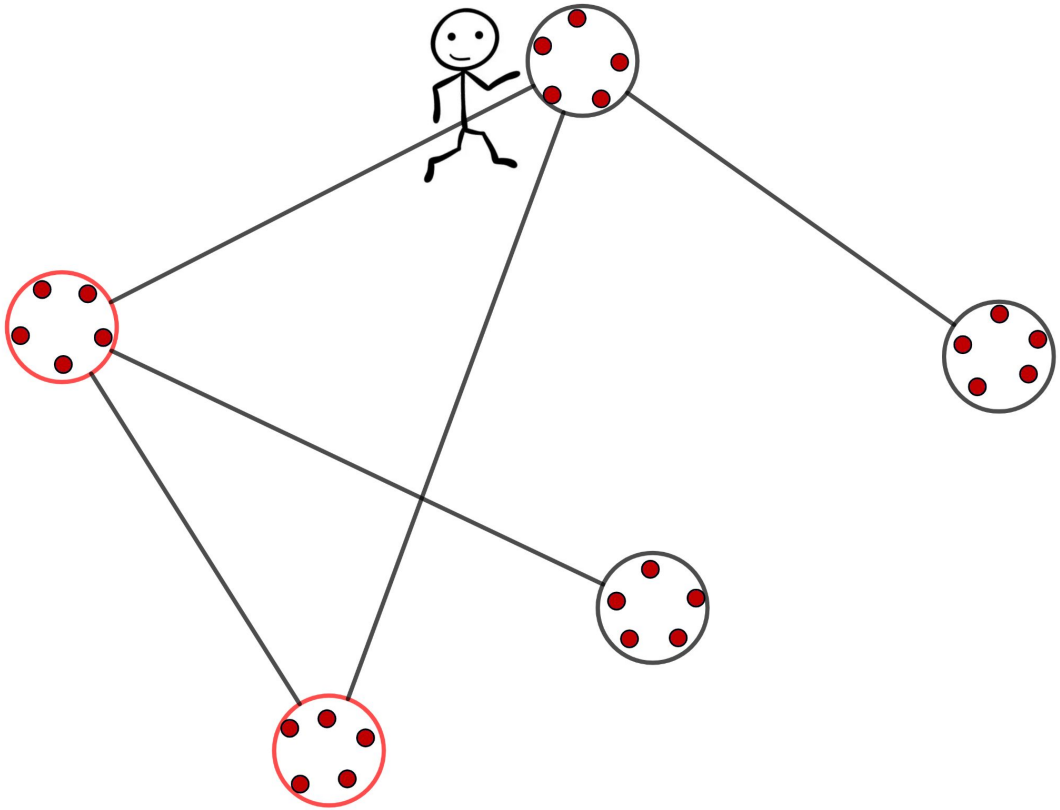


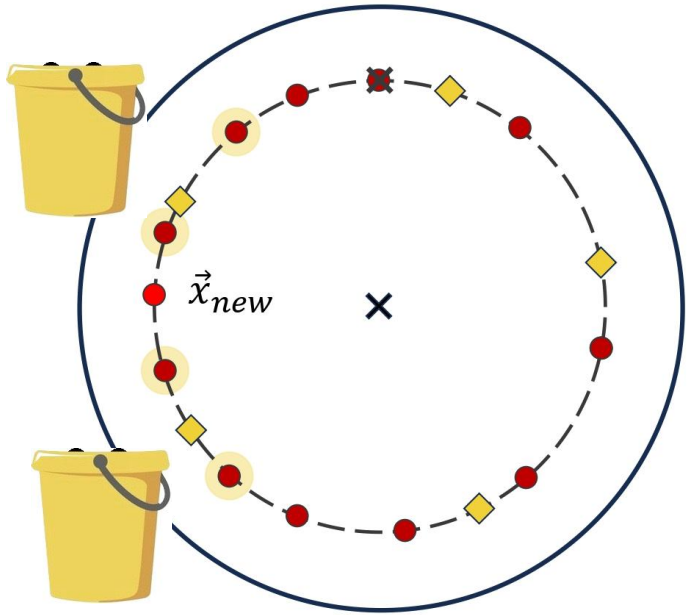
Objectif : Trouver 2 points proches dans 



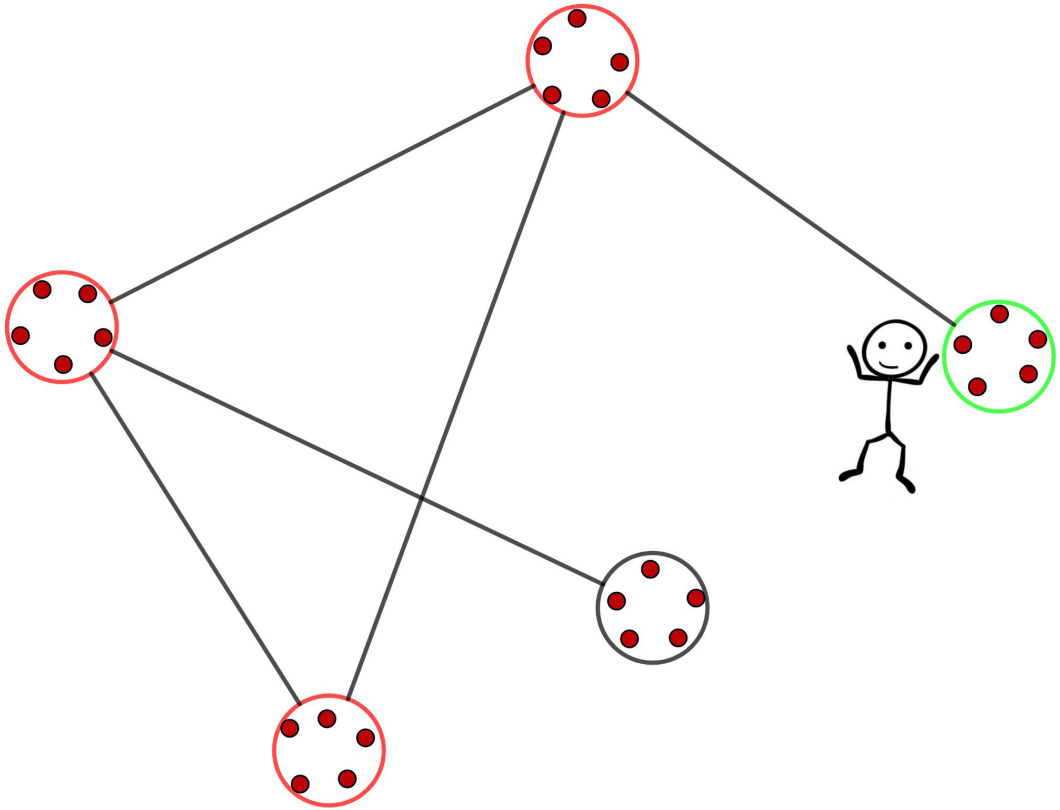


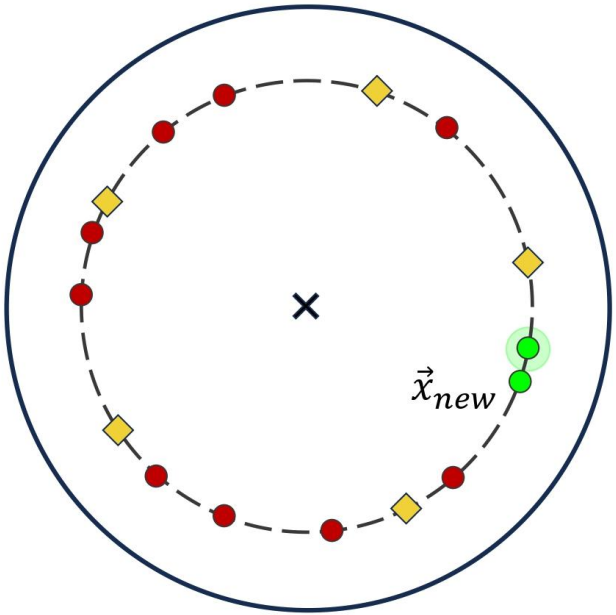
Objectif : Trouver 2 points proches dans 



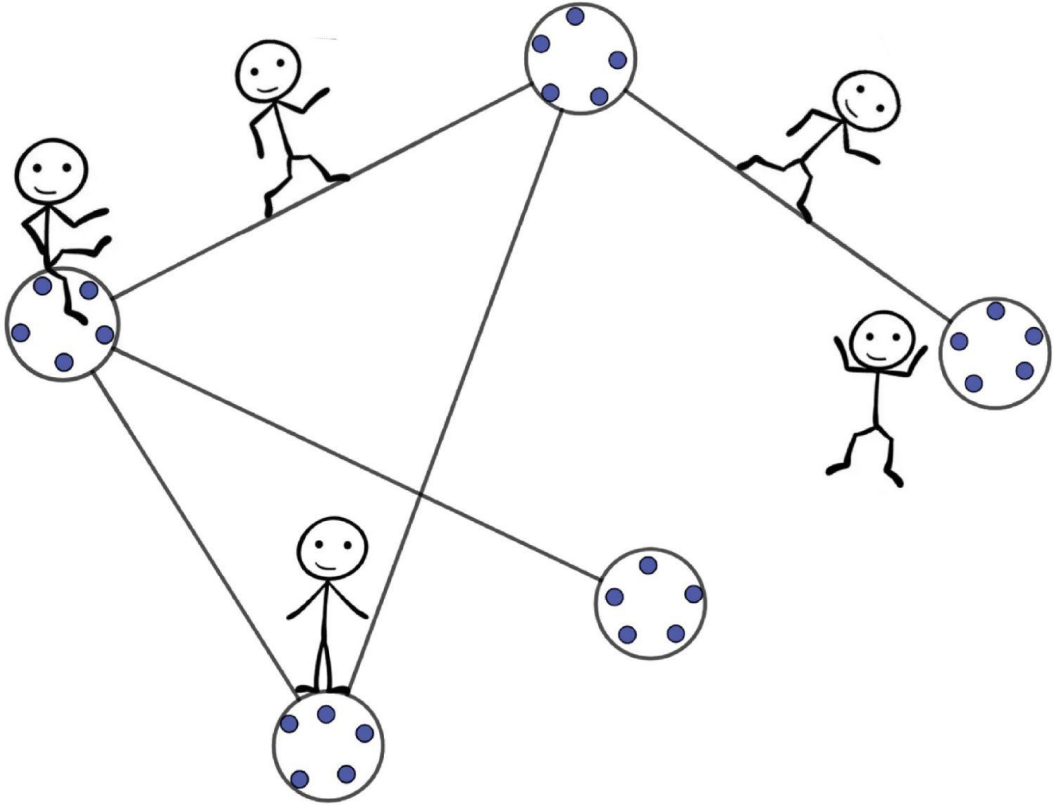


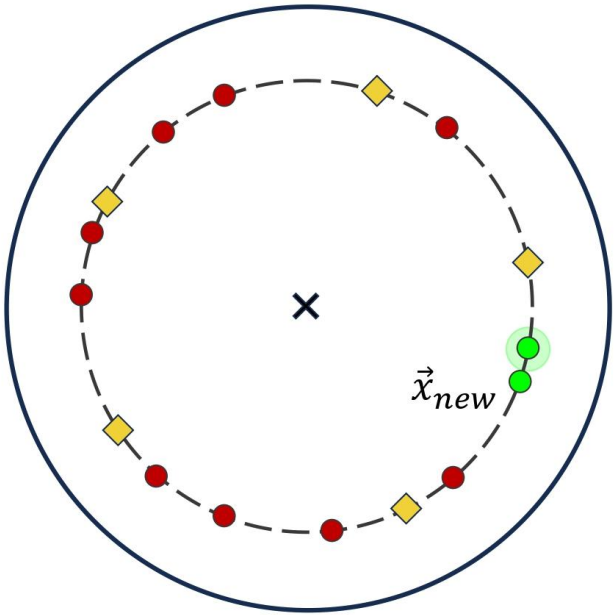
Objectif : Trouver 2 points proches dans 





Objectif : Trouver 2 points proches dans 





Attaques connues contre les lattices

d = 500	Classique	Quantique
Sans filtrage	10^{62}	10^{47}
Avec filtrage 	10^{44}	10^{40}
Marche quantique 		10^{38}

Attaques connues contre les lattices

d = 500	Classique	Quantique
Sans filtrage	10^{62}	10^{47}
Avec filtrage 	10^{44}	10^{40}
Marche quantique 		10^{38}

$< 10^{39}$

Cryptanalyse quantique des lattices

Dr. Johanna Loyer