Cryptographie et calcul quantique

Serge Chaumette

serge.chaumette@labri.fr

Image source : http://i3.kym-cdn.com/photos/images/original/000/605/748/58f.jpg

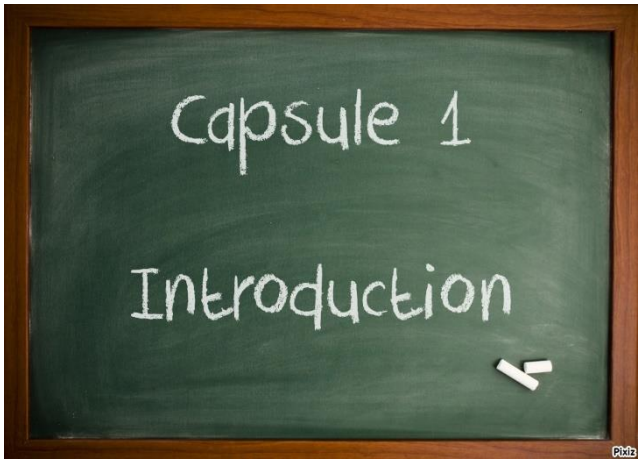
Serge Chaumette, serge.chaumette@labri.fr

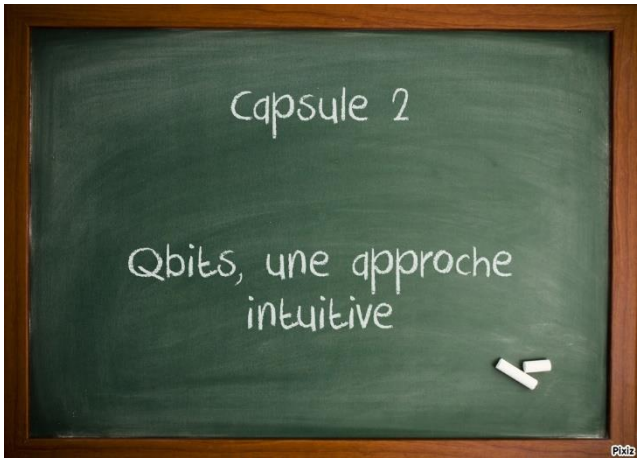
Ref : 0011@2023-nov-20@09h32-CET@sc ; Author : Serge Chaumette

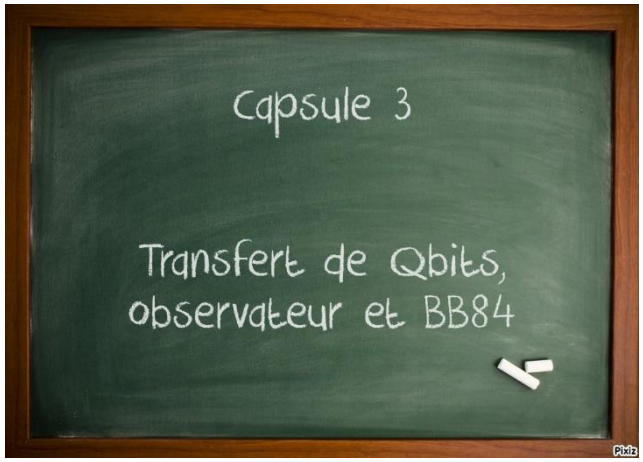
université de BORDEAUX

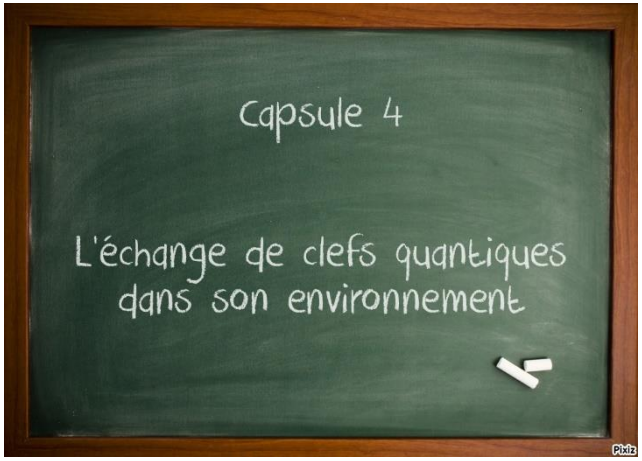
LABORATOIRE BORDELAIS DE RECHERCHE EN INFORMATIQUE LaBRI

Organisation









Serge Chaumette, serge.chaumette@labri.fr

Ref : 0011@2023-nov-20@09h32-CET@sc ; Author : Serge Chaumette

Cryptographie et calcul quantique

Serge Chaumette

serge.chaumette@labri.fr

Image source : http://i3.kym-cdn.com/photos/images/original/000/605/748/58f.jpg

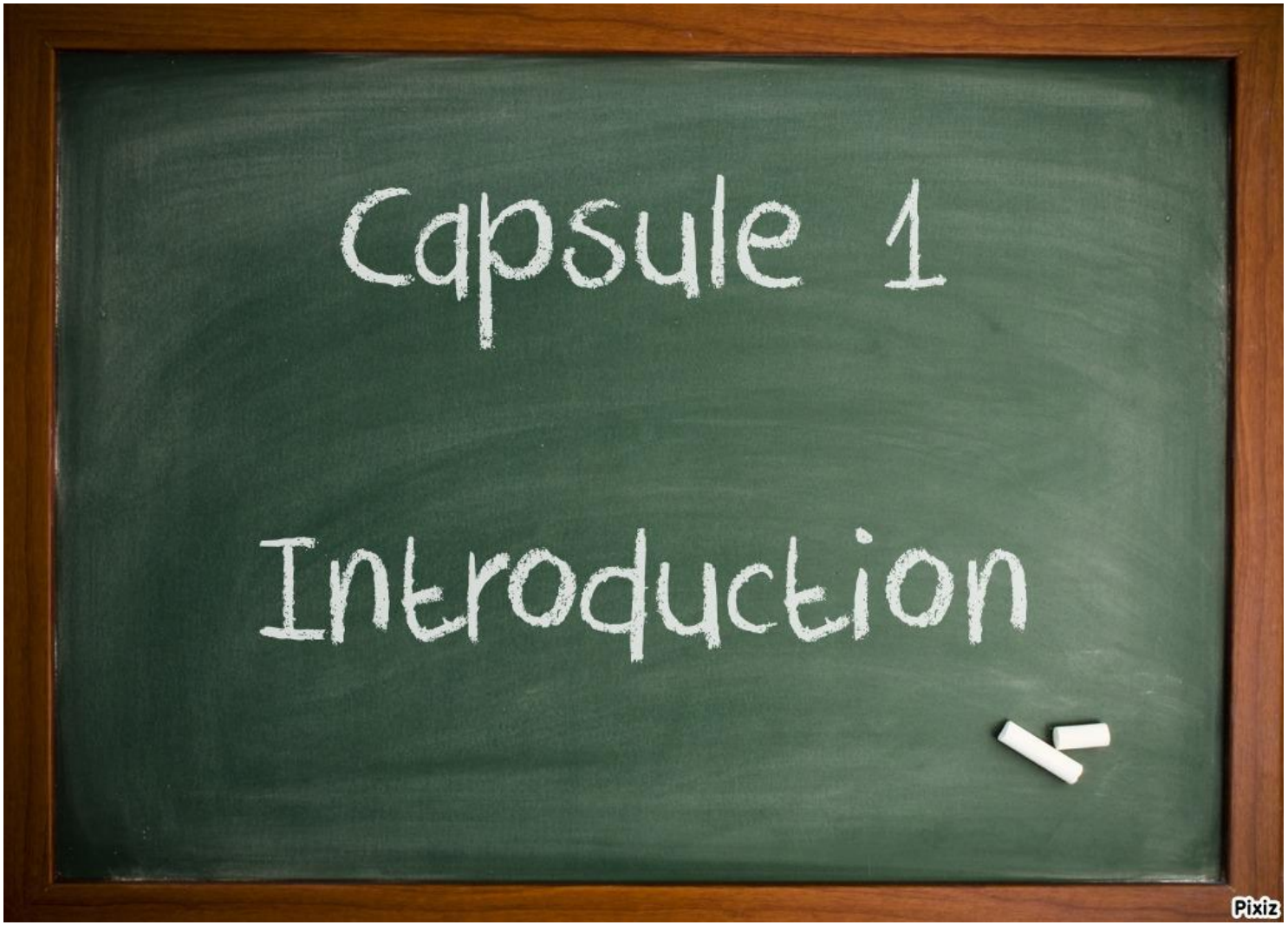
Serge Chaumette, serge.chaumette@labri.fr

Ref : 0011@2023-nov-20@09h32-CET@sc ; Author : Serge Chaumette

université de BORDEAUX

LABORATOIRE BORDELAIS DE RECHERCHE EN INFORMATIQUE LaBRI

Cryptographie et calcul quantique



Serge Chaumette, serge.chaumette@labri.fr

Ref : 0011@2023-nov-20@09h32-CET@sc ; Author : Serge Chaumette

Idée clef

- Quand on parle de cryptographie quantique on parle avant tout d'échange de clefs

- La cryptographie quantique repose sur un principe de physique quantique qui fait que la capacité à « casser » un protocole sécurisé ne dépend pas de la puissance de calcul de l'attaquant

Serge Chaumette, serge.chaumette@labri.fr

Ref : 0011@2023-nov-20@09h32-CET@sc ; Author : Serge Chaumette

Historique des attaques en environnement non quantique

Les algorithmes de chiffrement cassés

Arnaud Jacques
4 Octobre 2004,
mis à jour en Septembre 2014
SecuriteInfo.com

https://www.securiteinfo.com/cryptographie/cracked.shtml

Serge Chaumette, serge.chaumette@labri.fr

Mise en garde

- La quantique n'est pas la panacée !

> *« Le réseau informatique d'un acteur économique est désormais la principale porte d'entrée pour l'accès à l'information. Sa sécurité peut s'avérer vitale pour l'établissement.* ***Mais celle-ci se mesure à l'aune de son maillon le plus faible.*** *Chacun à son poste doit donc être pleinement mobilisé. »*
>
> PREMIER MINISTRE, DÉLÉGATION INTERMINISTÉRIELLE À L'INTELLIGENCE ÉCONOMIQUE, avril 2014

- Parmi les maillons faibles, on retrouve souvent :
  - L'humain
  - Le sans fil
  - Etc.

Serge Chaumette, serge.chaumette@labri.fr

Ref : 0011@2023-nov-20@09h32-CET@sc ; Author : Serge Chaumette

Mise en garde (suite)

La sécurité économique au quotidien en 28 fiches thématiques

Ministère de l'économie, des finances et de la relance

https://www.entreprises.gouv.fr/fr/securite-economique/la-securite-economique-28-fiches-thematiques

Serge Chaumette, serge.chaumette@labri.fr

Une bonne technologie ne suffit pas

Quantum Cryptography: As Awesome As It Is Pointless

Bruce Schneier
Wired
October 16, 2008

https://www.wired.com/2008/10/quantum-cryptography-as-awesome-as-it-is-pointless/

Serge Chaumette, serge.chaumette@labri.fr

Expérimentations

SECOQC

08.10.2008

QKD Network Demonstration and conference

The **first live demonstration** of a **working quantum key distribution (QKD) network** took place in Vienna on Oct 6, 2008 in the framework of the **SECOQC Demonstration and International Conference**. Eight QKD-links were combined in a novel quantum-back-bone network physically deployed within a typical metropolitan area network to connect different company sites from SIEMENS Austria. Typical applications for QKD, to secure data traffic from telephony and video conferencing, were included in the demonstration.

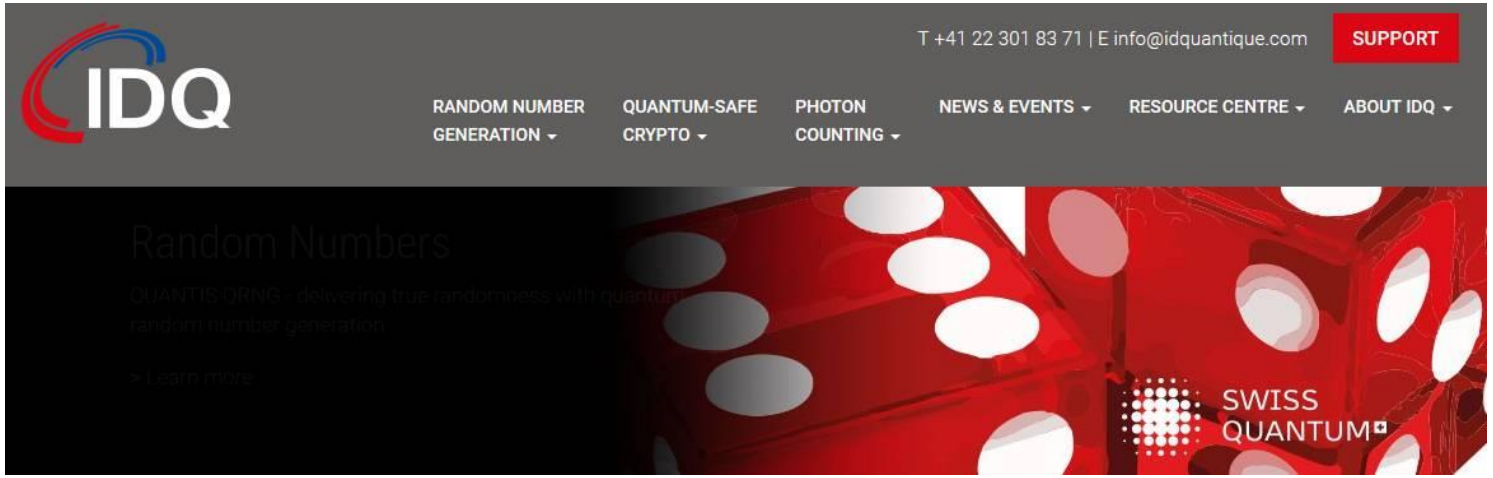
Source : http://www.secoqc.net/

Serge Chaumette, serge.chaumette@labri.fr

Ref : 0011@2023-nov-20@09h32-CET@sc ; Author : Serge Chaumette

Mais des produits existent

Exemple :



http://www.idquantique.com/

Serge Chaumette, serge.chaumette@labri.fr

Informatique quantique

- Le principe de base est la mesure de polarisation d'un photon
  - inconnue avant mesure
  - établie une fois mesurée

- Il est donc dans un ensemble d'états simultanés

Serge Chaumette, serge.chaumette@labri.fr

Deux aspects

Le calcul

- La cryptographie. C'est :
  - le chiffrement
  - la gestion de clefs. C'est là que la quantique intervient, pas sur le chiffrement (au moins pour l'instant).

Serge Chaumette, serge.chaumette@labri.fr

Un exemple théorique pour le calcul

- Manipuler toutes les images noir et blanc possibles
  - Chaque pixel est stocké sous la forme d'un qbit (*quantum bit*) qui peut être à la fois noir et blanc
  - Appliquer une opération à une telle image a pour effet de l'appliquer à toutes les images possibles à la fois

Serge Chaumette, serge.chaumette@labri.fr

Ref : 0011@2023-nov-20@09h32-CET@sc ; Author : Serge Chaumette

Quelques algorithmes

- Algorithme de Shor
  - Factorisation d'entiers – 1994

- Algorithme de Grover
  - Recherche – 1996

Serge Chaumette, serge.chaumette@labri.fr

Ref : 0011@2023-nov-20@09h32-CET@sc ; Author : Serge Chaumette

Cryptographie et calcul quantique

Serge Chaumette

serge.chaumette@labri.fr

Image source : http://i3.kym-cdn.com/photos/images/original/000/605/748/58f.jpg

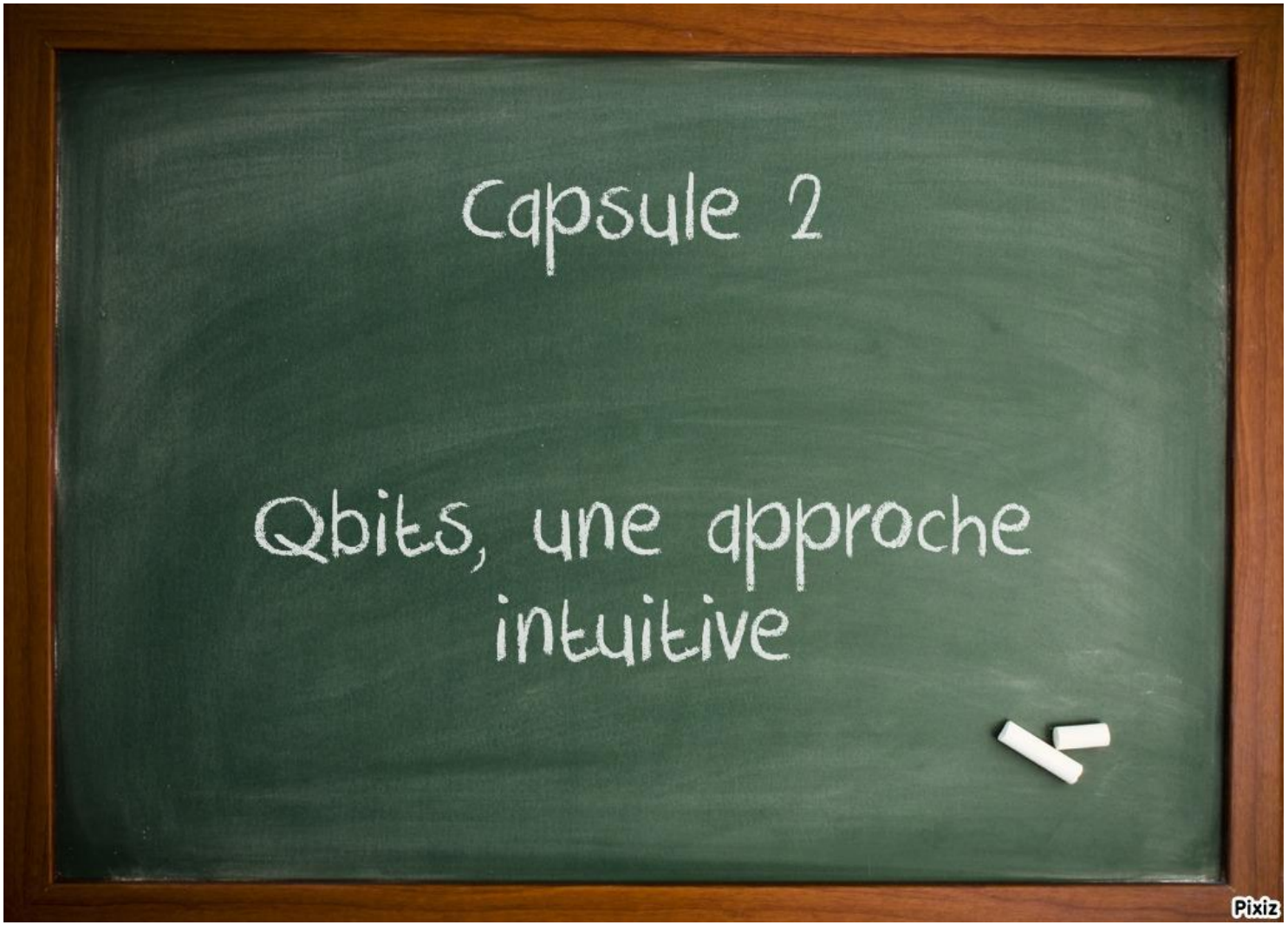
Serge Chaumette, serge.chaumette@labri.fr

Ref : 0011@2023-nov-20@09h32-CET@sc ; Author : Serge Chaumette

université de BORDEAUX

LABORATOIRE BORDELAIS DE RECHERCHE EN INFORMATIQUE LaBRI

Cryptographie et calcul quantique



Serge Chaumette, serge.chaumette@labri.fr

Ref : 0011@2023-nov-20@09h32-CET@sc ; Author : Serge Chaumette

Principe de base

- Un qbit :
  - Il peut être dans deux états à la fois
  - L'observer fixe un des deux états avec une probabilité de 50 % pour chacun de ces deux états possibles

- Intuition : une balle rouge ou verte. Une fois observée, cette balle est dans un état stable (toujours rouge ou toujours verte).

Serge Chaumette, serge.chaumette@labri.fr

Ref : 0011@2023-nov-20@09h32-CET@sc ; Author : Serge Chaumette

Préparation et lecture d'un qbit

- Un qbit est créé avec une certaine valeur (0 ou 1) et une certaine polarisation
- Si on le lit avec la même polarisation on obtient la valeur donnée lors de sa création (0 ou 1)
- Si on le lit avec la mauvaise polarisation ont lit 0 ou 1 de manière statistiquement équiprobable. Lors de toute nouvelle lecture on observe la même valeur que lors de la première lecture.

Serge Chaumette, serge.chaumette@labri.fr

Ref : 0011@2023-nov-20@09h32-CET@sc ; Author : Serge Chaumette

Succès/échec de la lecture

- Quand on a accès à un qbit, on ne sait rien de sa polarisation. On peut donc le lire avec
  - la bonne polarisation : 1 chance sur 2
  - la mauvaise polarisation : 1 chance sur 2

p(observer bonne valeur) =
p(bonne polarisation) + ½ p(mauvaise polarisation) = 75%

p(observer mauvaise valeur) =
½ p(mauvaise polarisation) = 25%

Serge Chaumette, serge.chaumette@labri.fr

Exemple

Pour 100 qbits générés aléatoirement en termes de valeurs et de polarisation

→ 50 valant 0, avec 25 dans chaque polarisation

→ 50 valant 1, avec 25 dans chaque polarisation

Décodage

- 1 chance sur 2 de décoder avec la bonne polarisation
  → ceux-là sont décodés correctement (50)
- 1 chance sur 2 de décoder avec la mauvaise polarisation
  → la moitié de ceux-là sont décodés correctement (25)

Au total 75 sont décodés correctement

Serge Chaumette, serge.chaumette@labri.fr

Ref : 0011@2023-nov-20@09h32-CET@sc ; Author : Serge Chaumette

Copie impossible

- Lors d'une lecture, comme on ne sait rien, on crée un noveau qbit avec la même valeur et on polarize aléatoirement

- Si on observe un 0
  - On crée un 0 avec une certaine polarization

    75 % de lecture correcte * ½ de recreation avec la bonne polarization

    37,5 % de succès de la copie
  - Idem si on observe un 1

Serge Chaumette, serge.chaumette@labri.fr

Une approche intuitive

Introduction à l'information quantique

Alexandre Blais (2002)

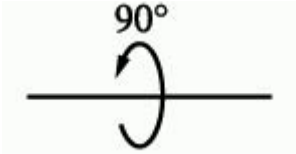
Équipe de Recherche en Physique de l'Information Quantique, Sherbrooke, Canada

~~http://epiq.physique.usherbrooke.ca/?section=intro~~

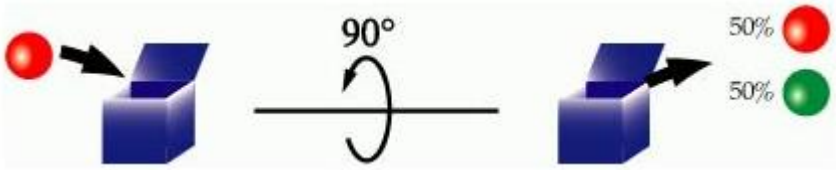
Serge Chaumette, serge.chaumette@labri.fr

Operations sur les qbits

- Création de superposition d'états

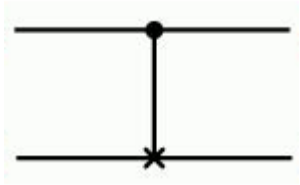


- Basculement, déphasage

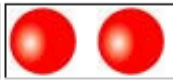
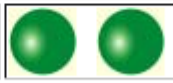


Serge Chaumette, serge.chaumette@labri.fr

Porte cnot



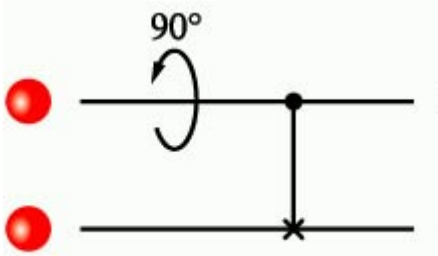
CNOT :Table de Vérité

Entrée	Sortie
	
	
	
	

Serge Chaumette, serge.chaumette@labri.fr

Ref : 0011@2023-nov-20@09h32-CET@sc ; Author : Serge Chaumette

Enchevêtrement



Serge Chaumette, serge.chaumette@labri.fr

Cryptographie et calcul quantique

Serge Chaumette

serge.chaumette@labri.fr

Image source : http://i3.kym-cdn.com/photos/images/original/000/605/748/58f.jpg

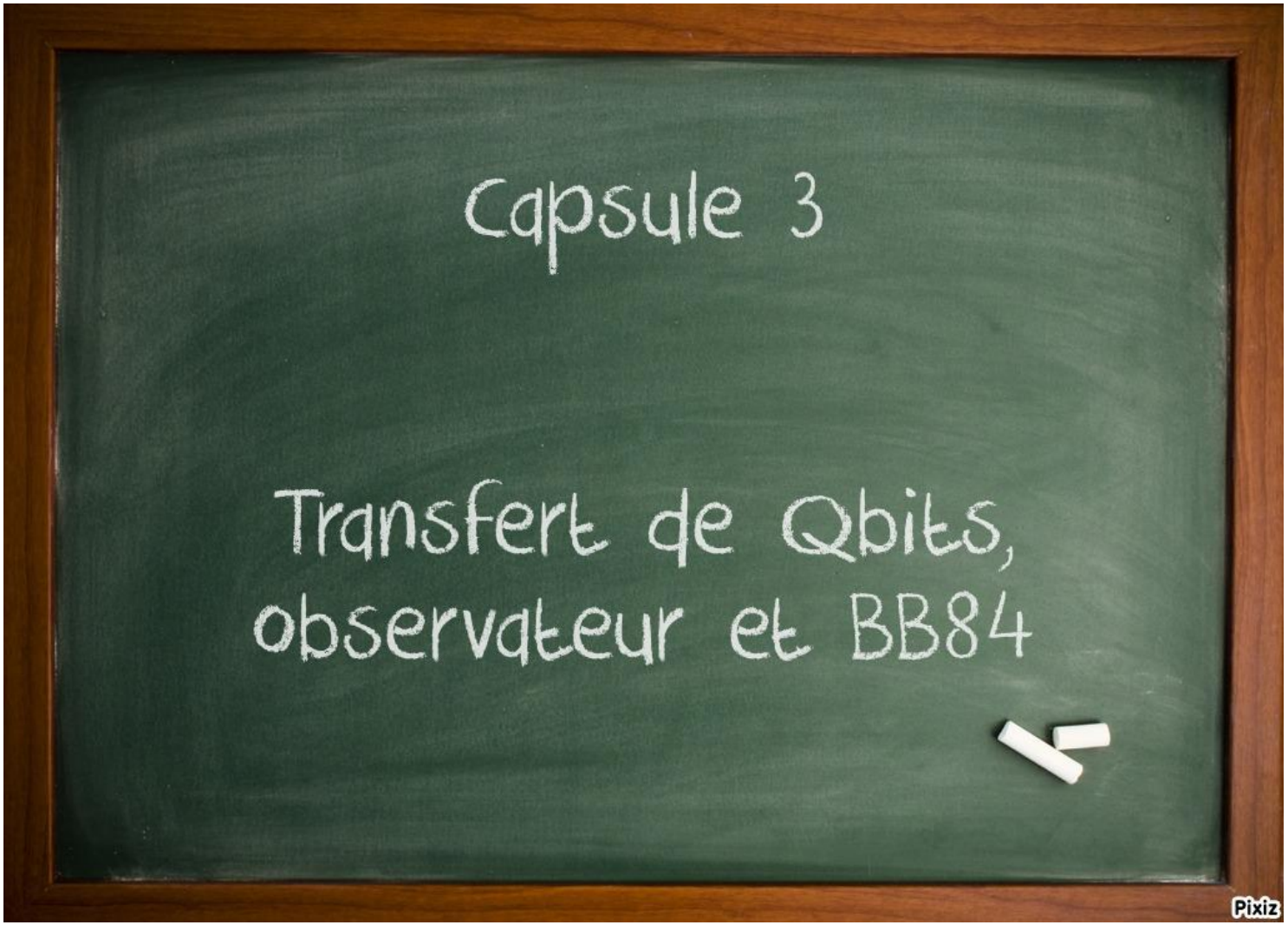
Serge Chaumette, serge.chaumette@labri.fr

Ref : 0011@2023-nov-20@09h32-CET@sc ; Author : Serge Chaumette

université de BORDEAUX

LABORATOIRE BORDELAIS DE RECHERCHE EN INFORMATIQUE LaBRI

Cryptographie et calcul quantique



Serge Chaumette, serge.chaumette@labri.fr

Ref : 0011@2023-nov-20@09h32-CET@sc ; Author : Serge Chaumette

Cryptographie quantique

- Il ne s'agit pas de chiffrer mais de transmettre une clef

- Principe
  - si on observe/mesure on perturbe
  - on ne sait pas si ce que l'on observe est la bonne chose ou pas
  - on vérifie à la fin par retransmission publique

Serge Chaumette, serge.chaumette@labri.fr

Mise en œuvre

Quand Bob reçoit de Alice

- Si bon choix de polarisation ➔ bon décodage = 100 % de succès
- Si mauvais choix de polarisation ➔ 1 chance / 2 = 50 % de succès

Donc en moyenne : 50 % de bon choix et 50 % de mauvais choix donc 50% + 50% de 50% de bons décodages

Bilan :

- 75 % bien décodés
- 25 % mal décodés

Serge Chaumette, serge.chaumette@labri.fr

Ref : 0011@2023-nov-20@09h32-CET@sc ; Author : Serge Chaumette

Si un observateur (Eve) est présent

- Si on transmet 100 rouges
  - 75 décodés par Eve comme rouges
    - 75*75% décodés par Bob comme rouges = 56,25
    - 75*25% décodés par Bob comme verts = 23,75
  - 25 décodés par Eve comme verts
    - 25*25% décodés par Bob comme rouges = 6,25
    - 25*75% décodés pat Bob comme verts = 18,75
  - Soit 62,5 décodés comme rouges par Bob en présence d'un observateur, contre 75% sinon

Serge Chaumette, serge.chaumette@labri.fr

Ref : 0011@2023-nov-20@09h32-CET@sc ; Author : Serge Chaumette

Articles de référence

- BB84 protocol: Charles H. Bennett and Gilles Brassard (1984)

- E91 protocol: Artur Ekert (1991)
  - Basé sur l'enchevetrement quantique

Serge Chaumette, serge.chaumette@labri.fr

Le protocole BB84

Quantum cryptography: Public key distribution and coin tossing

Charles H. Bennett, Gilles Brassard, 1984

~~http://researcher.watson.ibm.com/researcher/files/us-bennetc/BB84highest.pdf~~

Serge Chaumette, serge.chaumette@labri.fr

Le protocole BB84

https://www.youtube.com/watch?app=desktop&v=OITZ24i5wX4

Serge Chaumette, serge.chaumette@labri.fr

Cryptographie et calcul quantique

Serge Chaumette

serge.chaumette@labri.fr

Image source : http://i3.kym-cdn.com/photos/images/original/000/605/748/58f.jpg

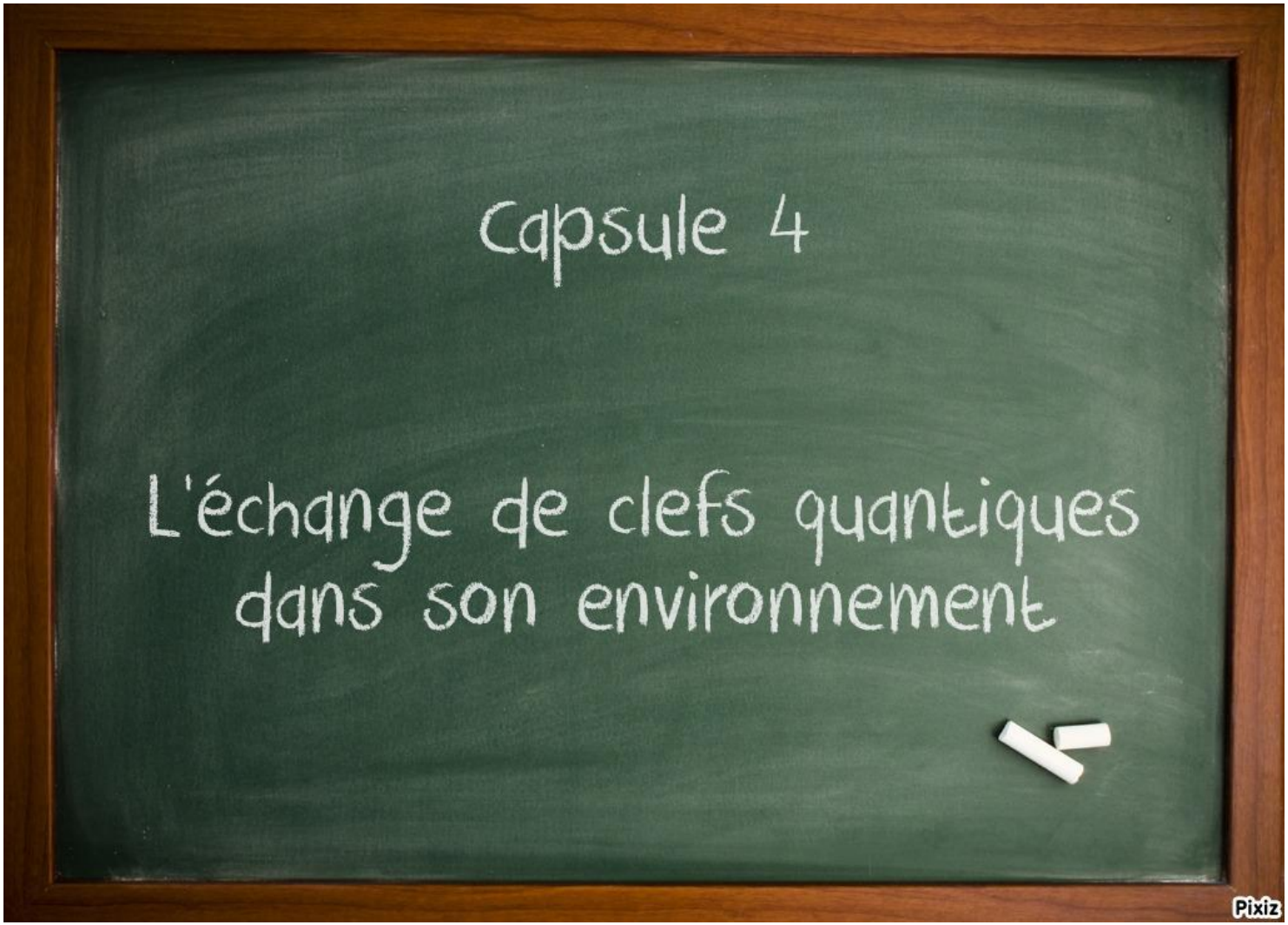
Serge Chaumette, serge.chaumette@labri.fr

Ref : 0011@2023-nov-20@09h32-CET@sc ; Author : Serge Chaumette

université de BORDEAUX

LABORATOIRE BORDELAIS DE RECHERCHE EN INFORMATIQUE LaBRI

Cryptographie et calcul quantique



Serge Chaumette, serge.chaumette@labri.fr

Attaques classiques

- Man-in-the-middle
- Photon number splitting attack
- Déni de service
- Cheval de Troie

  Trojan-horse attacks threaten the security of practical quantum cryptography
  Nitin Jain, Elena Anisimova, Imran Khan, Vadim Makarov, Christoph Marquardt, Gerd Leuchs
  https://arxiv.org/abs/1406.5813

- …

Serge Chaumette, serge.chaumette@labri.fr

Un satellite quantique lancé par la Chine

Le 17 Aout 2016

Liaisons chiffrées : la Chine lance un satellite quantique

Le satellite quantique Micius a été lancé hier par la Chine depuis son pas de tir situé dans la province du Gansu. (crédit : CCTV)

Le satellite quantique Quess lancé hier par la Chine a une mission de deux ans pour mettre en place des communications chiffrées inviolables.

Avec le lancement du Quess (Quantum Experiments at Space Scale), réalisé hier depuis la Mongolie, la Chine a annoncé mettre sur orbite le premier satellite « quantique » destiné à pouvoir mettre en place des communications indéchiffrables dans le cadre d'une mission de deux ans. Egalement baptisé Micius (du nom d'un philosophe et scientifique chinois né au 5ème siècle avant JC), l'équipement héberge une technologie de chiffrement à très haut niveau de sécurité qui distribuera des clés de chiffrement quantique entre les stations relais en Chine et en Europe.

Source : https://www.lemondeinformatique.fr/actualites/lire-liaisons-chiffrees-la-chine-lance-un-satellite-quantique-65650.html

Serge Chaumette, serge.chaumette@labri.fr

Un satellite quantique lancé par la Chine

- Espace : la Chine lance le 1er satellite quantique, une percée technologique majeure
  https://www.youtube.com/watch?v=GuM3byypcTU

- China launches world's first quantum satellite successfully
  https://www.youtube.com/watch?v=XjHosmTOyUE

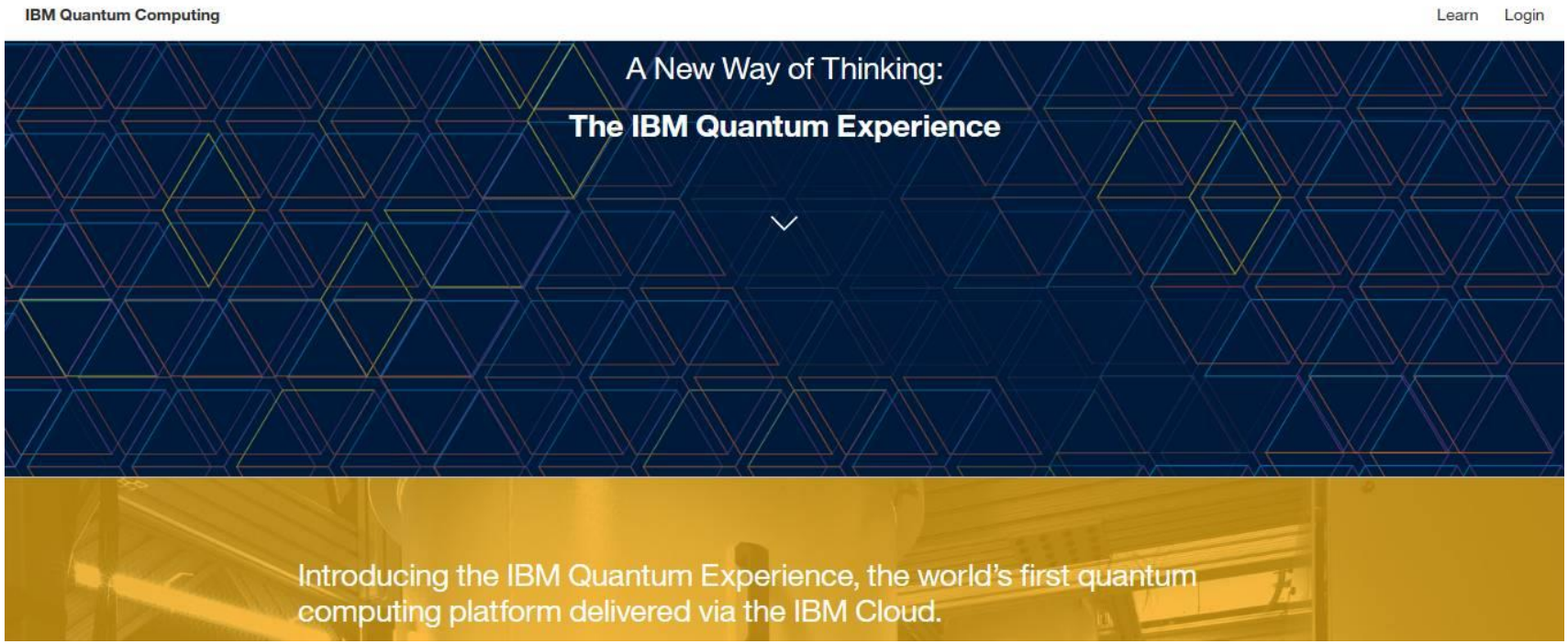
- Dialogue— Quantum Satellite Launch
  https://www.youtube.com/watch?v=sIfAYAgxVy4

- How does China's quantum satellite work?
  https://www.youtube.com/watch?v=qj22gj6vNX4

Serge Chaumette, serge.chaumette@labri.fr

Ref : 0011@2023-nov-20@09h32-CET@sc ; Author : Serge Chaumette

The IBM Quantum Experience



http://www.research.ibm.com/quantum/
https://www.ibm.com/quantum-computing/technology/experience
https://quantum-computing.ibm.com/login

Serge Chaumette, serge.chaumette@labri.fr

Ref : 0011@2023-nov-20@09h32-CET@sc ; Author : Serge Chaumette