COURS : Cryptographie
THÈME: La Cryptographie quantique
DATE : 09 Janvier 2026

II.3 AUTRES PROTOCOLES DE CRYPTOGRAPHIE QUANTIQUE

La cryptographie classique repose principalement sur la difficulté de certains calculs mathématiques. Cependant, avec l'émergence des ordinateurs quantiques, plusieurs de ces systèmes deviennent vulnérables. La cryptographie quantique propose une approche radicalement différente : elle s'appuie directement sur les lois de la mécanique quantique pour garantir la sécurité des communications. Après le protocole BB84, d'autres protocoles ont été proposés afin de renforcer la sécurité ou de s'adapter à des contraintes pratiques. Parmi eux, le protocole **E91**, proposé par **Artur Ekert** en 1991, occupe une place centrale.

II.3.1 Le Protocole E91 (Ekert, 1991) : Intrication + inégalités de Bell

Le protocole E91 repose sur un phénomène purement quantique appelé **intrication**. Deux particules intriquées forment un système unique : mesurer l'une influence instantanément l'autre, quelle que soit la distance qui les sépare. Dans ce protocole, une source génère des paires de particules intriquées.

- Alice reçoit une particule
- Bob reçoit l'autre

Ils effectuent ensuite des mesures indépendantes sur leurs particules.

II.3.1.1 Intrication : Son rôle dans la sécurité

L'état quantique utilisé dans E91 est généralement :

$$|\Psi\rangle = 1/\sqrt{2}\ (|00\rangle + |11\rangle)$$

Cela signifie que :

- si Alice mesure **0**, Bob mesure **0**
- si Alice mesure **1**, Bob mesure **1**

Ces corrélations ne peuvent pas être expliquées par la physique classique. Toute tentative d'interception par un espion perturbe l'état quantique et détruit ces corrélations. Ainsi, l'écoute devient **détectable**.

II.3.1.2 Inégalités de Bell

La sécurité du protocole **E91** est formellement démontrée grâce aux **inégalités de Bell**, notamment l'inégalité **CHSH** :

$$\mathbf{S=|E(a,b)-E(a,b')+E(a',b)+E(a',b')|}$$

- En physique classique : $\mathbf{S \leq 2}$
- En mécanique quantique : $\mathbf{S=2\sqrt{2}}$

Lorsque la valeur mesurée dépasse 2, cela prouve la présence d'intrication et garantit qu'aucun espion n'a intercepté la communication.

II.3.1.3 Démonstration par simulation

Pour illustrer ce principe, une simulation a été réalisée à l'aide de **Qiskit**.

Le circuit quantique utilisé comprend :

- une porte **Hadamard** pour créer une superposition
- une porte **CNOT** pour générer l'intrication
- une mesure finale des deux qubits

```python
from qiskit import QuantumCircuit
from qiskit.primitives import StatevectorSampler
import matplotlib.pyplot as plt

# 1. Création du circuit (intrication E91)
qc = QuantumCircuit(2)
qc.h(0)           # Hadamard
qc.cx(0, 1)       # CNOT → intrication
qc.measure_all()  # Mesure (registre 'meas' créé automatiquement)

# 2. Exécution locale avec le sampler V2
sampler = StatevectorSampler()
job = sampler.run([qc])  # V2 → liste de circuits

# 3. Récupération des résultats
result = job.result()

# Accès aux résultats du premier circuit
counts = result[0].data.meas.get_counts()

print("Résultats de la simulation :")
print(counts)

# 4. Affichage du circuit
print("\nCircuit quantique :")
print(qc.draw())
```

```
Résultats de la simulation :
{'00': 537, '11': 487}

Circuit quantique :
     ┌───┐     ┌─┐
q_0: ┤ H ├──■──┤M├──
     └───┘┌─┴─┐└╥┘┌─┐
q_1: ─────┤ X ├─╫─┤M├
          └───┘ ║ └╥┘
meas: 2/════════╩══╩═
                0  1
```

Les résultats obtenus montrent une forte corrélation entre les deux qubits, avec une majorité des états **00** et **11**, ce qui confirme la création d'un état intriqué.

Cette démonstration ne prouve pas à elle seule la sécurité complète du protocole, mais elle valide sa **brique fondamentale** : l'intrication quantique.

II.3.2 CV-QKD : Cryptographie quantique à variables continues

La **CV-QKD** est une approche de la cryptographie quantique qui utilise des variables continues de la lumière, comme l'amplitude et la phase, plutôt que des qubits discrets. Elle est particulièrement adaptée aux réseaux de fibres optiques actuels.

Alice encode l'information sur des **états cohérents** en modulant continûment les quadratures X et P du champ électromagnétique selon une loi gaussienne. Bob mesure ces quadratures à l'aide de techniques d'optique classique, comme la détection homodyne.

II.3.2.1 Différence avec les protocoles discrets

Contrairement à BB84 ou E91, la CV-QKD ne repose pas sur des bits quantiques, mais sur des distributions statistiques continues. L'information est portée par la variance du signal et non par des états discrets.

II.3.2.2 Sécurité du protocole

La sécurité repose sur le **bruit quantique**. Toute tentative d'interception introduit un **bruit excédentaire** dans le signal.

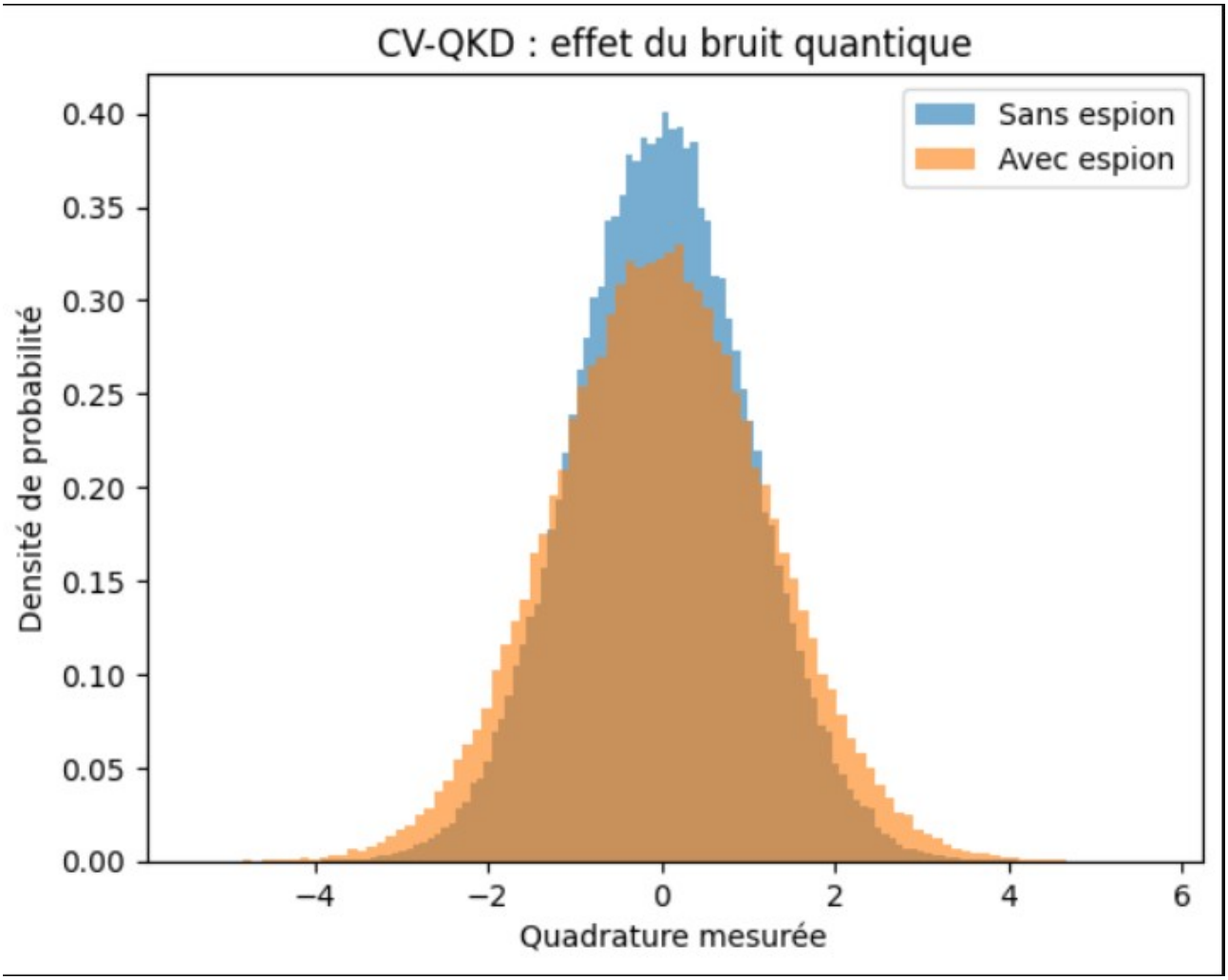
La relation fondamentale est : **Vmesuré = Vsignal + Vbruit**

Si le bruit mesuré dépasse la valeur théorique attendue, alors la communication est considérée comme compromise.

II.3.2.3 Démonstration par simulation

Une simulation montre que, sans espion, les valeurs mesurées par Bob suivent une distribution gaussienne étroite. En présence d'un espion, la distribution s'élargit, ce qui correspond à une augmentation mesurable de la variance. Cela illustre que l'écoute est **statistiquement détectable**.

```python
import numpy as np
import matplotlib.pyplot as plt

# Paramètres
N = 100000
V_signal = 1.0       # variance idéale
V_eve = 0.5          # bruit ajouté par un espion

# Cas 1 : canal sécurisé
alice = np.random.normal(0, np.sqrt(V_signal), N)
# Bob sans espion : bruit quantique naturel
bob_secure = alice + np.random.normal(0, 0.1, N)

# Cas 2 : espion présent->bruit excessif
bob_eve = alice + np.random.normal(0, np.sqrt(V_eve), N)

# Tracés/Comparaison des distributions reçues
plt.hist(bob_secure, bins=100, density=True, alpha=0.6, label="Sans espion")
plt.hist(bob_eve, bins=100, density=True, alpha=0.6, label="Avec espion")

plt.title("CV-QKD : effet du bruit quantique")
plt.xlabel("Quadrature mesurée")
plt.ylabel("Densité de probabilité")
plt.legend()
plt.show()
```


CV-QKD : effet du bruit quantique
Sans espion
Avec espion
Densité de probabilité
0.40
0.35
0.30
0.25
0.20
0.15
0.10
0.05
0.00
−4
−2
0
2
4
6
Quadrature mesurée