Table of contents

Cryptographie Quantique & Post-Quantique - Support de révision oral

1. Le Problème : L'Apocalypse Cryptographique Quantique

Imaginez : Tous les cadenas du monde deviennent soudainement transparents. C'est ce qui pourrait arriver avec l'avènement des ordinateurs quantiques pour notre cryptographie actuelle.

Le danger concret : L'algorithme de **Shor** sur un ordinateur quantique peut casser : - RSA (basé sur la factorisation) - Diffie-Hellman (basé sur les logarithmes discrets) - ECC (courbes elliptiques)

> ❗ Important
>
> **Concept Clé : Menace existentielle** Un ordinateur quantique suffisamment puissant rendrait **obsolète toute la cryptographie asymétrique** actuelle, menaçant HTTPS, banques, communications sécurisées...

```
flowchart TD
    A[Ordinateur quantique<br/>suffisamment puissant] --> B[Algorithme de Shor]
    B --> C[Casse RSA, ECC, DH]
    C --> D[Internet actuel<br/>devient vulnérable]

    style D fill:#ffcccc
```

2. Qubit vs Bit : La Différence Fondamentale

Le Bit Classique : Un Interrupteur

- **État** : 0 **OU** 1
- **Comportement** : Déterministe
- **Visualisation** : Comme un interrupteur ON/OFF

Le Qubit Quantique : Une Sphère de Possibilités

- **État** : 0 **ET** 1 simultanément (superposition)
- **Comportement** : Probabiliste jusqu'à la mesure
- **Visualisation** : Comme une sphère de Bloch (flèche pouvant pointer n'importe où)

```
flowchart LR
    A[Bit classique] --> B[0 ou 1<br/>Comme un interrupteur]
    C[Qubit quantique] --> D[Superposition 0 et 1<br/>Comme une sphère de possibilités]

    style B fill:#e6f3ff
    style D fill:#e6ffe6
```

L'Intrication : La Magie Quantique

Phénomène contre-intuitif : Deux qubits intriqués restent connectés quelle que soit la distance. Mesurer l'un affecte instantanément l'autre.

Conséquence pratique : n qubits peuvent représenter 2 états simultanément → **parallélisme quantique**.

3. Pourquoi Nos Cryptosystèmes Sont en Danger

Le Cauchemar de Shor

Problème classique difficile : Factoriser 2048 bits prendrait des milliers d'années avec les meilleurs algorithmes classiques.

Solution quantique : L'algorithme de Shor résout ce problème en **temps polynomial** sur un ordinateur quantique.

> ⚠ Warning
>
> **Piège à éviter : Ne pas confondre les menaces** - **Shor** menace l'**asymétrique** (RSA, ECC, DH) → **apocalyptique** - **Grover** menace le **symétrique** (AES) → gérable en doublant la taille des clés

Le Calendrier de la Menace

1. **Aujourd'hui** : Ordinateurs quantiques très limités (NISQ era)
2. **Prochaines années** : Avancées progressives
3. **"Harvest now, decrypt later"** : On capture déjà des données chiffrées pour les déchiffrer plus tard

4. La Solution : La Cryptographie Post-Quantique

L'Idée Générale

Trouver des problèmes mathématiques **difficiles même pour les ordinateurs quantiques**.

Les 5 Familles de Solutions

```
flowchart TD
    A[Cryptographie Post-Quantique] --> B[Réseaux<br/>ex: Kyber]
    A --> C[Codes correcteurs<br/>ex: McEliece]
    A --> D[Multivarié<br/>équations polynomiales]
    A --> E[Hash-based<br/>ex: SPHINCS+]
    A --> F[Isogénies<br/>courbes elliptiques]

    style B fill:#ccffcc
```

Pourquoi Kyber (Réseaux) a Gagné ?

Le NIST a choisi Kyber car : **Équilibre** sécurité/performance
Clés raisonnables (1-2KB vs 1MB pour McEliece)
Opérations efficaces
Bien étudié depuis 20+ ans

5. L'Intuition derrière Kyber : Apprendre avec des Erreurs

L'Analogie du Professeur Distrait

Imaginez un professeur qui donne des équations pour trouver un secret **s**, mais qui **ajoute de petites erreurs** à chaque résultat.

Sans erreurs (facile) :

```
3s = 12  → s = 4
2s = 8   → s = 4
```

Avec erreurs (difficile) :

```
3s = 12 + 1  = 13
2s = 8 - 2   = 6
```

Trouver `s` devient très difficile !

La Formulation Mathématique

Kyber utilise **Module-Learning With Errors (MLWE)** : - Secrets et erreurs sont des **polynômes** avec petits coefficients - Opérations modulo `q` et modulo `X  + 1` - Problème : distinguer `(A, As + e)` d'aléatoire

> Tip
>
> **Astuce mnémotechnique :** - **LWE** = Learning With Errors (erreurs dans Z) - **MLWE** = Module-LWE (erreurs dans des modules sur anneaux de polynômes)

6. Comment Fonctionne Kyber-KEM (Schéma Simplifié)

Les Trois Personnages

- **Alice** veut envoyer un secret à Bob
- **Bob** génère une paire de clés
- **Eve** l'attaquant quantique

Les 3 Étapes

```
sequenceDiagram
    participant B as Bob
    participant A as Alice
    participant E as Eve (quantique)

    Note over B: 1. KeyGen
    B->>B: Génère (sk, pk)
    B->>A: Envoie pk

    Note over A: 2. Encapsulation
    A->>A: Calcule chiffré + clé
    A->>B: Envoie chiffré
```

```
    Note over B: 3. Decapsulation
    B->>B: Utilise sk pour retrouver la clé

    Note over E: Même avec un ordinateur quantique,<br/>Eve ne peut pas casser MLWE
```

L'Idée Clé de Sécurité

Même si Eve intercepte `pk = (A, t = As + e)`, elle ne peut pas trouver `s` car : 1. `A` est aléatoire public 2. `e` est une petite erreur secrète 3. Sans `s`, impossible de déchiffrer

7. La Crypto-Agilité : Préparer la Transition

Pourquoi C'est Essentiel ?

On ne sait pas **quand** les ordinateurs quantiques arriveront, ni **quel** algorithme post-quantique survivra aux analyses.

Solution : Construire des systèmes qui peuvent **changer d'algorithme** facilement.

L'Approche Hybride Recommandée

Ne pas remplacer, mais combiner :

```
Clé = RSA-2048 + Kyber-768
```

Avantage : Cassé seulement si **les deux** sont cassés.

> **Note**
>
> **Recommandation NIST :** Transition en 3 phases : 1. **Hybride** (classique + post-quantique) 2. **Évaluation** (surveillance des attaques) 3. **Transition complète** (si nécessaire)

8. Les Défis Pratiques de Kyber

Les Bonnes Nouvelles

- **Performances** : presque aussi rapide que RSA
- **Tailles** : clés 1-2KB, chiffrés ~1KB
- **Standardisation** : NIST, IETF en cours

Les Défis

1. **Nouveauté** : moins de 10 ans d'analyse vs 40+ pour RSA
2. **Implémentation** : attaques par canaux auxiliaires possibles
3. **Probabilité d'échec** : très faible mais non nulle (contrairement à RSA)
4. **Migration** : mettre à jour toute l'infrastructure Internet

Comparaison des Tailles

Algorithme	Taille clé publique	Taille signature	Sécurité
RSA-2048	256 bytes	256 bytes	Classique
Kyber-768	1184 bytes	1088 bytes	Post-quantique Niveau 3

9. Exemple Jouet : Comprendre avec des Petits Nombres

Notre Monde Miniature

- `n = 4` (polynômes de degré < 4)
- `q = 17` (coefficients modulo 17)
- Secret `s = [1, 0, -1, 1]` (petits coefficients)

La Magie des Polynômes Circulants

Opération modulo `X + 1` : `X = -1`, `X = -X`, etc.

Exemple :

`(1 + X) * (1 - X) = 1 - X²`
`Car X * (-X) = -X² et X = -1`

Pourquoi C'est Sûr Même en Miniature ?

Même avec nos petits nombres, résoudre MLWE reste difficile. Dans la vraie vie : - `n = 256` ou `512` - `q` 2^{32} - Matrices de polynômes, pas juste scalaires

10. Fiche de Révision Express

> **!** Important
>
> **En 30 secondes pour l'oral :**
>
> 1. **Problème** : Ordinateurs quantiques cassent RSA/ECC avec Shor
> 2. **Solution** : Cryptographie post-quantique basée sur problèmes difficiles même quantiques
> 3. **Kyber** : Algorithme gagnant du NIST, basé sur MLWE (réseaux)
> 4. **Sécurité** : Distinguer (A, As+e) d'aléatoire est difficile
> 5. **Transition** : Crypto-agilité + approche hybride
> 6. **Statut** : Standardisation en cours, migration massive à venir

11. Pour l'Oral : L'Histoire à Raconter

"Imaginez que toutes les serrures de Paris deviennent transparentes. C'est ce que ferait un ordinateur quantique à notre Internet. Heureusement, des mathématiciens ont trouvé des problèmes si complexes que même les ordinateurs quantiques peinent : comme deviner un secret dans des équations pleines de petites erreurs. C'est la base de Kyber, le futur standard de sécurité post-quantique choisi par le NIST."

12. Questions Fréquentes à l'Examen

Q : "Pourquoi RSA est vulnérable au quantique mais pas AES ?" R : "Shor utilise la transformée de Fourier quantique pour trouver des périodes, ce qui casse la factorisation. Grover donne seulement une racine carrée d'accélération pour la recherche, donc doubler la taille de clé AES suffit."

Q : "Quand doit-on migrer vers le post-quantique ?" R : "Maintenant ! À cause du 'harvest now, decrypt later'. Les données sensibles à longue durée de vie (secrets d'État, biométrie) sont déjà en danger."

Q : "Kyber est-il parfait ?" R : "Non, c'est un compromis. Ses clés sont plus grosses que RSA, c'est un nouvel algorithme moins analysé, mais c'est le meilleur équilibre trouvé à ce jour."

13. Le Mot de la Fin

La cryptographie post-quantique n'est pas de la science-fiction. C'est une **nécessité pratique** qui demande une **transition planifiée**. Kyber représente le début de cette nouvelle ère, mais

la vigilance reste de mise : l'histoire de la cryptographie nous apprend que **seul le temps révèle les vraies faiblesses**.

En résumé : Nous vivons une révolution cryptographique aussi importante que le passage du DES à l'AES. Comprendre Kyber, c'est comprendre comment nous protégerons nos données dans le monde quantique à venir.