# Cryptographie dans un monde quantique

# CryptiQ

anr agence nationale de la recherche

**Appel : AAPG**

**Année : 2018**

**Instrument : JCJC**

**Contact : C. Chevalier**


**COORDINATEUR : Céline Chevalier**

**PARTENAIRES : Paris-Panthéon-Assas Université**

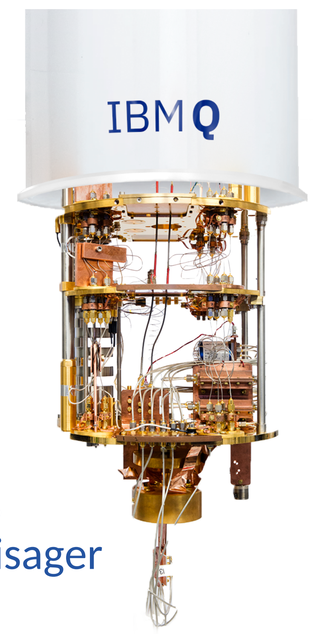


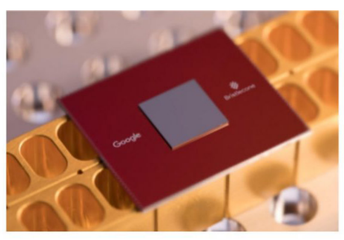
**Résumé :**

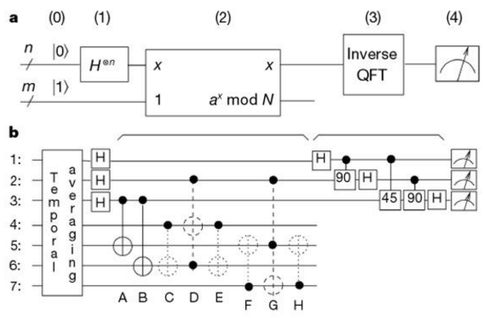
**L'objectif du projet CryptiQ est d'anticiper les changements majeurs liés à l'avènement de la communication quantique (et, à plus long terme, du calcul quantique), pour continuer à garantir la sécurité des schémas cryptographiques classiques exécutés dans un tel environnement.**


## CONTEXTE ET OBJECTIFS

Le respect de la vie privée et la confidentialité des données numériques sur le long terme est un enjeu majeur.
L'intention du NIST de standardiser des protocoles cryptographiques post-quantiques, ainsi que les différentes annonces d'IBM et Google, révèlent la nécessité d'envisager l'existence à plus ou moins long terme d'un attaquant muni d'un ordinateur quantique, qui pourrait anéantir la sécurité de schémas à clef publique très utilisés, en cassant les hypothèses calculatoires sous-jacentes à l'aide d'algorithmes spécifiques (ci-contre l'algorithme de Shor, d'après Nature 414883).



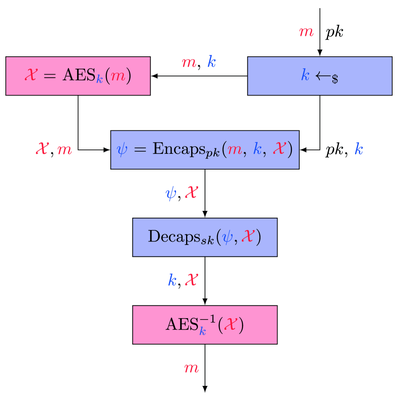





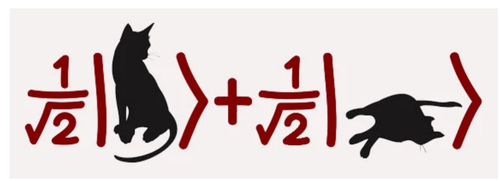

En parallèle, les technologies de communication quantique commencent à devenir concrètement accessibles et pourraient améliorer l'efficacité et la sécurité de certains protocoles cryptographiques.

## MÉTHODOLOGIE ET RÉSULTATS

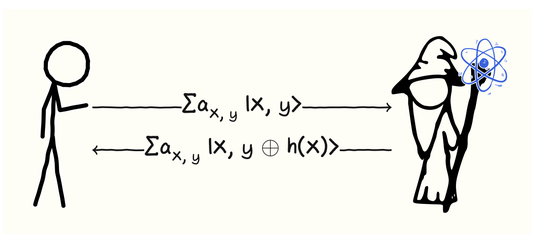
Le projet s'attache dans un premier temps à l'étude de primitives cryptographiques dites post-quantiques (c'est-à-dire classiques mais basées sur des hypothèses résistant à un potentiel ordinateur quantique).
Une étude comparative a ainsi été réalisée sur les candidats à la compétition du NIST pour le chiffrement (ci-contre une représentation schématique du paradigme KEM-DEM utilisé).




Des constructions de protocoles post-quantiques plus complexes ont ensuite été proposées, par exemple un schéma d'*oblivious transfer* qui a fait l'objet d'une publication scientifique à la conférence de sécurité informatique ARES 2019. D'autres travaux sont en cours en partenariat avec Thales et concernent par exemple des signatures de groupe, des accréditations anonymes et de l'échange de clefs authentifié.
La principale problématique du projet consiste ensuite à considérer les nouveaux moyens donnés à l'adversaire avec l'arrivée des modes de communication quantique (attaques par superposition, ci-contre) et à les modéliser de façon adéquate. Ces résultats ont fait l'objet d'une publication scientifique (ProvSec 2020 et DCC 2022) et une autre soumission est en cours.




Il s'agit également d'adapter les techniques traditionnelles de preuve (ci-contre une interaction illustrant le modèle de l'oracle aléatoire quantique).




Ceci a une incidence sur les constructions et leur efficacité pratique en modifiant les outils utilisés et la manière de les combiner.
Le jeu de sécurité IND-CCA pour les schémas de chiffrement classiques a par exemple été étendu pour prendre en compte des requêtes quantiques (Qcrypt 2020 et travaux en cours).

## VALORISATION ET PERSPECTIVES

Les travaux réalisés dans le cadre du projet CryptiQ permettent d'améliorer la confiance dans les moyens de sécurisation des données dans le cloud sur le long terme, même dans le cas de l'arrivée de l'ordinateur quantique dans les prochaines décennies.

PANTHÉON-ASSAS UNIVERSITÉ PARIS

CryptiQ