# Rapport de thèse : Intrication dans les réseaux d'information quantique.

Anne Marin.
LTCI, Telecom-ParisTech, Paris, France

Directeur de thèse : Damian Markham, Telecom-ParisTech
Gilles Zémor, University of Bordeaux-1

Nov 2009 - Avr 2011

Durant la première année et demi de ma thèse, j'ai travaillé sur la théorie de l'information quantique à travers l'étude de la cryptographie et de la théorie des codes quantique. Toutefois cette approche théorique garde à l'esprit un point de vue réaliste sur les possibilités expérimentales actuelles. Au cours de cette période, j'ai également eu l'occasion de participer à une école d'été à Montréal, extrèmement bénéfique tant du point de vue des cours pointus en théorie de l'information quantique que de l'opportunité d'y rencontrer les acteurs contemporains en la matière. J'ai aussi travaillé, en plus de l'équipe IQ de Telecom-Paristech à laquelle j'appartiens, et de ses nombreux visiteurs, en collaboration avec l'université de Bordeaux-1 et avec le LIG de Grenoble ; une partie du travail résultant fut présenté lors d'une session Poster au premier colloque GDR-IQFA de Nice en mars dernier, et est soumis en ce moment même à la conférence QCrypt de Zurich.

L'intrication est une propriété spécifique à l'information quantique et est au coeur des ressources potentielles pour transmettre et coder de l'information quantique. Néanmoins, nous sommes loin d'en connaitre toutes les conséquences. En outre, l'information quantique est appliquée à de plus en plus de protocoles cryptographiques, tel le partage de secret qui constitue la première grande partie d'étude de ma thèse. Pour cela nous utilisons des « états-graphes »qui sont des états intriqués, parmis les plus simples à implémenter et les plus largement étudiés, du fait de leur structure simple. Basé sur le précédent travail [2], [3], [4], nous pouvons explorer plusieurs domaines : la théorie des codes afin d'identifier et de classer les schémas (im)possibles de partage de secret en fonction de leurs paramètres, la théorie des graphes afin de caractériser les « flow »d'information correspondants dans un graphe, et les protocoles de cryptographie afin d'imaginer de nouvelles applications pouvant elles-mêmes impliquer de nouvelles propriétés.

## 1 Recherche

### 1.1 Cadre de travail

Le partage de secret est un protocole de cryptographie qui consiste à encoder un secret $s$ dans un message de longueur $n$ et de partager ce message entre $n$ joueurs. On représente formellement la phase d'encodage et de partage par l'action d'un « dealer ». Le schéma de paramètre $(n, k, k')$ est valide lorsque :

1. $p \geq k$ joueurs peuvent retrouver $s$. (Ensemble autorisé).
2. $p \leq k'$ joueurs ne peuvent obtenir aucune information sur $s$. (Ensemble non autorisé)

De plus, le schéma est dit parfait lorsque $k' = k-1$. A titre d'exemple on peut citer le schéma de Shamir, premier protocole de partage de secret ( [1]).
Dans la version quantique du problème, la situation reste fondamentalement la même. On distingue, en se référant à [2], trois types de protocoles "graduels" (CC, CQ, QQ). Le secret est classique dans les

deux premiers cas, quantique dans le troisième. Dans tous les cas, le dealer encode le secret dans un état-graphe, que l'on peut définir ainsi :
Un état-graphe est tout d'abord un registre de **qudits**. On nomme qudit l'unité de base de mesure d'un signal quantique, c'est-à-dire un vecteur unitaire d'un espace de Hilbert de dimension $q$ sur $\mathbb{C}$. On parle de **qubit** lorsque $q = 2$.
Un état-graphe de longueur $n$ est l'unique (à une phase prés) état quantique stabilisé par $n$ opérateurs de Pauli $K_i$ mutuellement indépendants et commutatifs. Ces stabilisateurs sont décrits à partir d'un graphe $G$ à $n$ sommets et vérifient :

$$K_i = X_i \bigotimes_{j \in N(i)} Z_j^{\omega g(i,j)} \ \forall\, i=1,\dots,n, \quad \text{où} \quad \begin{array}{l} \omega g(i,j) \text{ est le poids de l'arête } \{i,j\} \text{ à valeur dans un corps fini à} \\ q \text{ élements.} \\ N(i) \text{ est le voisinnage de l'arête i.} \end{array}$$

Pour chaque protocole, le dealer envoie un qudit à chacun des $n$ joueurs, ensuite :

- Dans le protocole CC, il mesure son qudit dans la base $Z$. La structure d'accés dans le graphe assure la validité du schéma.
- Dans le protocole CQ, il choisit aléatoirement la base dans laquelle il mesure son qudit. Le schéma est valide s'il existe $q$ bases ortogonales dans laquelle la structure d'accés est vérifiée. Ces $q$ bases correspondent à $q$ opérations de complémentation locale du graphe initial. En répétant la procédure et en ajoutant une phase de distillation, nous faisons en fait une distribution de clef quantique entre le dealer et les $n$ joueurs (généralisation du protocole Ekert91).
- Dans le protocole QQ, le dealer téléporte son qudit à l'ensemble autorisé. Ceci requiert une structure d'accés valide dans $q+1$ complémentations locales du graphe initial. De plus, nous utilisons le fait qu'un état-graphe valide pour ce protocole est nécessairement un code MDS quantique (voir [5]). C'est pourquoi nous travaillons en dimension supérieure. En effet, le travail relatif à la conjecture MDS implique des bornes sur la longueur du code, étant donnée sa dimension et la dimension de l'espace. Par exemple, avec des qubits, on ne peut pas réaliser de protocole QQ parfait avec plus de cinq joueurs.

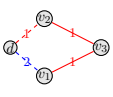
## 1.2 Nouveaux résultats

- Le premier résultat est la généralisation en dimension supérieure de la structure d'accés à l'information (c'est-à-dire au secret) dans un graphe.
  **Theorem 1.** *$B \subset V$ est un ensemble autorisé s'il existe $X \subset B$ et $(v_{x_1}, \dots, v_{x_{|X|}}) \in F_q^{*|X|}$, tel que*

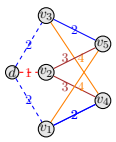
$$X \cup \mathit{NonZero}_{(v_{x_1},\dots,v_{x_{|X|}})}(X) \subset B$$
$$\sum_{\beta \in \mathbb{F}_q^*} \sum_{\alpha \in \mathbb{F}_q} \alpha\beta |N_\alpha(d) \cap X_{|\beta}| \neq 0 \mod q$$

- Nous avons transcrit les codes de Reed Solomon décrits dans [5], [6] en graphes de Reed Solomon. Il était connu que ces codes pouvaient être utilisé pour le protocole QQ, nous avons montré de plus que cette famille, comme tout code MDS, peut aussi être utilisée pour le protocole CQ. Nous pouvons réaliser des schémas parfaits de partages de secret avec cette famille de graphes. En effet, on peut vérifier que le théorème 1 est vérifié dans $q+1$ complémentations locales de chacun de ces graphes.

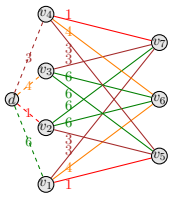
Exemples :



$(3,2)_3$



$(5,3)_5$



$(7,4)_7$

- Après avoir listé les codes MDS de dimension 1 connus sur des espaces de dimension 2, 3, 4, 5 et 7, nous avons essayer de trouver de nouveaux schémas en utilisant la recherche (quasiment) exhaustive de graphes, au moins en dimension 3. Le résultat des programmes a montré qu'il n'existait pas de schéma $(7,4)_3$ bien que celui-ci paraissait être un bon candidat après le $(5,3)_2$. C'est toujours une question ouverte à savoir si un tel schéma existe sur $\mathbb{F}_4$ ou $\mathbb{F}_5$. (sur $\mathbb{F}_7$ on peut construire

un graphe de Reed Solomon). La principale difficulté de la recherche exhaustive étant bien sûr la compléxité du problème. (Il y a $q^{\frac{n(n-1)}{2}}$ graphes à $n$ sommets sur $\mathbb{F}_q$).

### 1.3 Discussion

La caractérisation de la transmission d'information dans un graphe, combinée aux contraintes liées à la théorie des codes, nous permettent d'avoir une meilleure compréhension de la structure d'accés générale, et donc une meilleure caractérisation des trois protocoles de partage de secret, de leurs relations entre eux, et de leur sécurité. Au delà de la recherche de nouveaux (concrets et donc directement implémentables dans la mesure du possible) graphes en petites dimensions, une autre idée intéressante (apparue dans [7]) est de combiner le codage classique et quantique, afin d'améliorer le nombre de schémas possibles ; c'est l'objet d'une collaboration en cours avec l'équipe d'information quantique du LIG de Grenoble. Enfin, nous travaillons aussi à utiliser les états-graphes dans un autre protocole cryptographique : « the blind computation ».

## 2 Activités

- Travail en collaboration avec Gilles Zémor à l'université de Bordeaux-1. 27-29 Janv 2010.
- SMS 2010-Advanced School in Quantum Information Processing and Quantum Cryptography à Montréal. 21 Juin - 2 Juil 2010.
- Invitée dans l'équipe d'information quantique du LIG de Grenoble. 29 Nov - 3 Dec 2010.
- Présentation d'un Poster au GDR-IQFA Colloquium de Nice. 23-25 Mars 2011.
- Encadrement de TP de programmation (Language C and Système d'exploitation). Premier semestre 2010-2011.
- (en cours) Soumission d'un article à la conférence QCRYPT de Zürich. 12-16 Sept 2011.

## Références

[1] SHAMIR A., *How to share a secret*, Communications of the ACM, 22, 612–613 (1979).

[2] MARKHAM Damian, SANDERS Barry, *Graph State for Quantum Secret Sharing* .

[3] KEET A, FORTESCUE B, SANDERS B, MARKHAM D, *Quantum secret sharing with qudit graph states*.

[4] KASHEFI E, MARKHAM D, MHALLA M, PERDRIX S, *Information flow in Secret Sharing Protocols*.

[5] CLEVE R, GOTTESMAN D, LO HK, *How to share a quantum secret*.

[6] AHARONOV D, BEN-OR M, *Fault-tolerant quantum computation with constant error*.

[7] BROADBENT A,CHOUHA P, TAPP A, *The GHZ state in secret sharing and entanglement simulation.*