Informatique quantique IFT6155

Authentification de données quantiques

En cryptologie classique une tache importante est l'authentification de donnée. Cette tache permet de s'assurer que des données, par exemple un message ou de l'information stockée n'ont pas été modifié. Dans le monde classique, l'authentification est un problème bien connu et des solutions élégantes, efficaces et peu coûteuses existent. Nous allons voir comment il est possible de faire de même pour des donnés quantiques.

Les résultats contenus dans ce chapitre proviennent de l'article suivant.

Howard Barnum, Claude Crépeau, Daniel Gottesman,
Adam Smith et Alain Tapp
Authentication of Quantum Messages
FOCS 2002

Code correcteur (détecteur)

Nous nous intéressons seulement à la détection d'erreur. Un code détecteur d'erreur est associé à une opération unitaire de la forme:

$$U : \mathcal{H}_M \otimes \mathcal{H}_S \to \mathcal{H}_C$$

- $\mathcal{H}_M = \mathcal{H}_2^{\otimes m}$ l'espace d'états.
- $\mathcal{H}_S = \mathcal{H}_2^{\otimes s}$ le syndrome d'erreur.
- $\mathcal{H}_C = \mathcal{H}_2^{\otimes (m+s)}$ l'espace de code.

On encode $|\psi\rangle \in \mathcal{H}_M$ par $U|\psi\rangle \otimes |0\rangle$. Soit $|x\rangle \in \mathcal{H}_M$ un état de base; alors $U|x\rangle$ est un mot de code.

Pour vérifier qu'il n'y a pas d'erreur, on mesure le syndrome.

Détection d'erreur

Soit $\{E_x\}$ la base d'erreur canonique.

$$E_x = \sigma_{x_1} \otimes \sigma_{x_2} \otimes \cdots \otimes \sigma_{x_n}$$

Une famille de détection d'erreur $\{Q_k\}$ pour $k \in K$ de parametre ϵ est telle que

$$\forall x \neq 0, |\{k|E_x \text{ donne syndrome 0 avec } Q_k\}| \leq \epsilon |K|$$

Pour n'importe quelle erreur $E_x \neq E_0$ avec un choix aléatoire de k, la probabilité de détecter l'erreur est $1 - \epsilon$.

Théorème Il existe une famille de détection d'erreur $\{Q_k\}$ qui encode m qubits dans $m + t$ qubits tel que

$$\epsilon \simeq \frac{2m}{t2^t}.$$

Test de pureté

Alice et Bob croient partager $|\Phi^+\rangle^{\otimes n}$ et voudraient le vérifier. Il sont prêts à sacrifier quelques paires.

Un protocole de *test de pureté* avec paramètre ϵ est un operateur T (LOCC) qui, partant de $2(m+t)$ qubits, produit $2m+1$ qubits tel que:

- $T(|\Phi^+\rangle^{\otimes(m+t)}) = |\Phi^+\rangle^{\otimes m} \otimes |\text{accept}\rangle$.

- Soit P le sous-espace engendré par $|\psi\rangle^{\otimes m} \otimes |\text{accept}\rangle$ avec $\left\langle\psi|\Phi^+\right\rangle^{\otimes(m+t)} = 0$;
  alors pour tout ρ , $\text{Tr}(PT(\rho)) \leq \epsilon$.

Détection d'erreur et test de pureté

Une technique simple pour effectuer un test de pureté est d'utiliser une famille de détection d'erreur $\{Q_k\}$ avec paramètre ϵ.

- Alice et Bob partagent $|\Phi^+\rangle^{\otimes(m+t)}$.
- Alice et Bob choisissent $k \in_R K$.
- Alice mesure le syndrome s_A de son état.
- Bob mesure le syndrome s_B de son état.
- Alice et Bob vérifient que $s_A = s_B$.
- Alice et Bob décodent et obtiennent $|\Phi^+\rangle^{\otimes m}$.

Détection d'erreur et test de pureté

Theoreme Si $\{Q_k\}$ est une famille de codes détecteurs d'erreur avec paramètre ϵ, alors T tel que décrit précédement est un test de pureté avec paramètre ϵ.

Authentification de données classiques

M: ensemble de messages

K: ensemble de clefs

C: ensemble de messages authentifiés

A, B: algorithmes classiques polynomiaux

$$\begin{aligned} A &: K \times M \to C \\ B &: K \times C \to M \times \{\text{valide, invalide}\} \end{aligned}$$

Complétude:

$$\forall m, k : B_k(A_k(m)) = \langle m, \text{valide} \rangle$$

Validité:

$$\forall m' : \text{Prob}_k\{B_k(E(A_k(m))) = \langle m', \text{valide} \rangle\} \leq \epsilon$$

Wegman et Carter

Fonctions de hachage universelles fortes

Taille des clefs pour un message de taille n:

$$4(t + \log\log n)\log n$$

avec

$$\epsilon = 2^{-t+2}$$

Borne inférieure:

$$\Omega(t + \log n - \log t)$$

Authentification de données quantiques

$\mathcal{H}_M$: espace des messages, n qubits
K: ensemble de clefs classiques
$\mathcal{H}_C$: espace des message authentifiés, $n+t$ qubits
A, B: algorithmes quantiques polynomiaux

$$\begin{aligned} \mathcal{A} &: K \otimes \mathcal{H}_M \to \mathcal{H}_C \\ \mathcal{B} &: K \otimes \mathcal{H}_C \to \mathcal{H}_M \otimes \{|\text{valide}\rangle,\ |\text{invalide}\rangle\} \end{aligned}$$

Complétude:

$$\forall |\psi\rangle, k : B_k(A_k(|\psi\rangle)) = |\psi\rangle \otimes |\text{valide}\rangle$$

Validité:

$$\rho = \frac{1}{|K|} \sum_{k \in K} B_k(E(A_k(|\psi\rangle)))$$

$$P = (I - |\psi\rangle\langle\psi|) \otimes |\text{valide}\rangle\langle\text{valide}|$$

$$\forall E, |\psi\rangle, \text{Tr}(\rho P) \leq \epsilon$$

Protocole interactif

Toute communication classique est authentifiée.

1. $\mathcal{A}$ et $\mathcal{B}$ choisissent une famille de codes $\{Q_k\}$.
2. $\mathcal{A}$ crée $|\Phi^+\rangle^{\otimes n}$ et envoie la moitié de chaque paire à $\mathcal{B}$.
3. $\mathcal{B}$ annonce qu'il a recu n qubits.
4. $\mathcal{A}$ choisit $k \in_R K$ et l'annonce à $\mathcal{B}$.
5. $\mathcal{A}$ et $\mathcal{B}$ mesurent le syndrome de Q_k. $\mathcal{A}$ annonce son résultat à $\mathcal{B}$ qui le compare au sien. En cas d'erreur $\mathcal{B}$ avorte le protocole.
6. $\mathcal{A}$ et $\mathcal{B}$ décodent leurs n qubits. (Ils obtiennent l'état $|\Phi^+\rangle^{\otimes m}$).
7. $\mathcal{A}$ utilise $|\Phi^+\rangle^{\otimes m}$ pour téléporter ρ à $\mathcal{B}$.

Protocole intermédiaire I

1. $\mathcal{A}$ et $\mathcal{B}$ choisissent une famille de codes $\{Q_k\}$
2. $\mathcal{A}$ crée $|\Phi^+\rangle^{\otimes n}$, choisit $k \in_R \mathcal{K}$ et mesure le syndrome y du code Q_k sur ses qubits. $\mathcal{A}$ décode m qubits avec le code Q_k. $\mathcal{A}$ effectue sa partie de la téléportation de l'etat ρ sans annoncer x (les $2m$ bits classiques). $\mathcal{A}$ envoie les n qubits non touchés à $\mathcal{B}$.
3. $\mathcal{B}$ annonce qu'il a recu les n qubits σ'.
4. $\mathcal{A}$ annonce k et y à $\mathcal{B}$.
5. $\mathcal{B}$ mesure le syndrome y' de Q_k sur ρ. Si $y' \neq y$, $\mathcal{B}$ rejette l'état. $\mathcal{B}$ décode les n qubits avec Q_k.
6. $\mathcal{A}$ révèle x à $\mathcal{B}$, qui termine la téléportation et obtient $\rho' \simeq \rho$.

Protocole intermédiaire II

1. $\mathcal{A}$ et $\mathcal{B}$ choisissent une famille de codes $\{Q_k\}$
2. $\mathcal{A}$ choisit $x \in_R \{0,1\}^{2n}$, encrypte ρ avec x et obtient τ. $\mathcal{A}$ choisit $k \in_R \mathcal{K}$ et un syndrome y et encode τ avec Q_k et y. $\mathcal{A}$ envoie le résultat à $\mathcal{B}$.
3. $\mathcal{B}$ annonce qu'il a recu σ'.
4. $\mathcal{A}$ annonce k, x, et y à $\mathcal{B}$.
5. $\mathcal{B}$ mesure le syndrome y' du code Q_k. Si $y \neq y'$, $\mathcal{B}$ rejette l'état. $\mathcal{B}$ décode ρ' avec Q_k et y, et produit τ'. $\mathcal{B}$ décrypte τ' avec x et obtient $\rho' \simeq \rho$.

Protocole non interactif

1. Préparation: $\mathcal{A}$ et $\mathcal{B}$ s'entendent sur une famille de codes de purification $\{Q_k\}$ et des clefs privées aléatoires k, x, et y.

2. $\mathcal{A}$ encrypte ρ et obtient τ en utilisant x comme clef. $\mathcal{A}$ encode τ avec le code Q_k ayant pour syndrome y, et produit σ qu'elle envoie a $\mathcal{B}$.

3. $\mathcal{B}$ recoit σ' et mesure le syndrome y' de Q_k. Si $y \neq y'$ $\mathcal{B}$ rejette l'état recu. $\mathcal{B}$ décode σ' avec Q_k et obtient τ', qu'il décrypte en utilisant x et finalement obtient $\rho' \simeq \rho$.

Conclusion

Théorème: Soit s un parramètre de sécurité. Il existe un protocole non interactif permettant l'authentification d'un message de m qubits utilisant une clefs secrète de $2(m+s)+1$ bits et la transmission de $m+s$ qubits ayant pour paramètre de validité $\epsilon = \frac{2(m+s)}{s(2^s-1)}$.