量子コミットメントスキームの束縛性に関する調査

Survey on the binding property of quantum commitment schemes

弓濱まどか・システム分科会・情報セキュリティ大学院大学

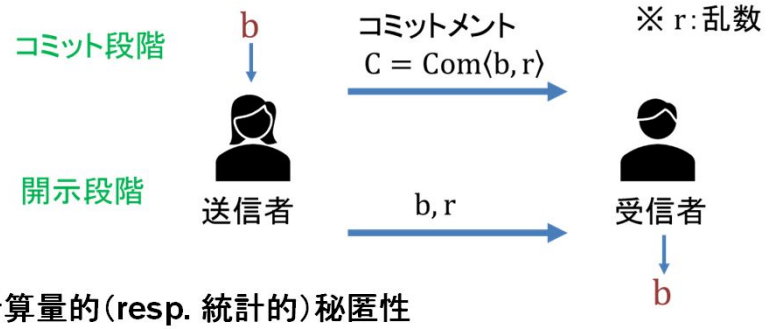
1. 背景・目的

近年、量子計算機開発の発展に伴い、送受信者が量子計算機を用いて計算・通信を行う量子計算機暗号に関する研究が進められている。暗号の重要な構成要素であるコミットメントスキームについては、量子特有の性質から古典的束縛性の定義が量子の世界では成り立たず、様々な束縛性の提案がなされてきた。

そこで、様々な束縛性定義の関係性について整理することを目標に調査を行った。

2. コミットメントスキームの定義

内容を明かさずにビットbを約束するもの。



・計算量的（resp. 統計的）秘匿性

多項式時間の（resp.無限の）計算能力を持つ悪意のある受信者は、コミットメントCを開封する前にその内容bを知ることができない。

・統計的（resp. 計算量的）束縛性

無限の（resp. 多項式時間の）計算能力を持つ悪意のある送信者は、コミットメントCを送信した後で、その内容bを別の内容b'(≠ b)に開示することはできない。

3. 各種束縛とその関係性

・正直束縛　$\left\|(Q_1|0\rangle\langle 0|Q_1^{\dagger})^{CR} U^{RZ}\left((Q_0|0\rangle)^{CR}|\psi\rangle^{Z}\right)\right\| < \epsilon$

・和束縛　$p_0 + p_1 < 1 + negl(n)$

・AQY−統計的束縛　$\mathrm{TD}\left(\mathrm{RealExpt}_n^{S^*}, \mathrm{IdealExpt}_n^{S^*,\mathrm{E}}\right) \leq \varepsilon(n)$

調査の結果、統計的束縛な標準的量子コミットメントスキームに関して、正直束縛、和束縛、AQY−統計的束縛は等価であることが分かった。

4. 量子コミットメントスキームの構成一覧

構成名	仮定	安全性	論文
純粋化DMSスキーム	量子安全な一方向性関数	統計的秘匿、計算量的正直束縛	Yan22
圧縮NOVYスキーム	量子安全な一方向性関数	統計的秘匿、計算量的正直束縛	Yan22
圧縮Naorスキーム	量子安全な擬似乱数生成器	計算量的秘匿、統計的束縛	Yan22
MYスキーム	擬似ランダム量子状態生成器	計算量的秘匿、統計的和束縛	MY22
AQYスキーム	擬似ランダム関数的量子状態生成器	計算量的秘匿、AQY-統計的束縛	AQY22
HMYスキーム	擬似ランダム量子状態生成器	統計的秘匿、計算量的和束縛	HMY23

量子安全な一方向性関数と擬似ランダム量子状態生成器のそれぞれを仮定とした、計算量的秘匿で統計的束縛なスキームと統計的秘匿で計算量的束縛なスキームがあることが分かった。