

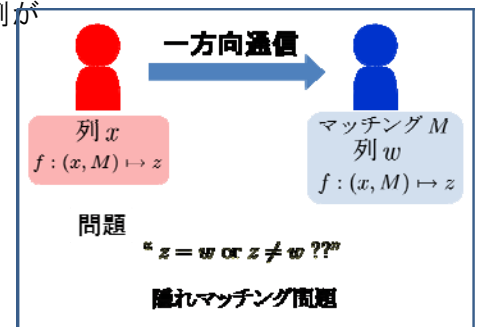
タイトル

隠れマッチング問題の通信計算量と暗号への応用

Communication complexity for the Hidden Matching Problem and applications to cryptography

概要

素因数分解問題のように、古典計算に対して量子計算が強力となる例があることはよく知られているが、通信においても古典通信に対して量子通信が有用な問題がある。その一つの例として、隠れマッチング問題を扱う。この問題に対して、古典通信と量子通信で通信計算量のギャップが大きいことを紹介する。また、この結果が暗号の通信においてプライバシー増幅や鍵拡張へと適用できることを紹介する。



URL

産業界への展開例・適用分野

量子通信、暗号

研究者

	氏名	専攻	研究室	役職 (学年)
展示担当者	照山順一	通信情報システム	岩間研究室	修士2年