量子計算と量子暗号

京都大学　基礎物理学研究所
准教授　森前智行
（１５分）

YITP
YUKAWA INSTITUTE FOR THEORETICAL PHYSICS

量子計算の歴史

1981: ファインマンが量子シミレーターのアイデアを提唱（量子計算はまだ４１歳！）

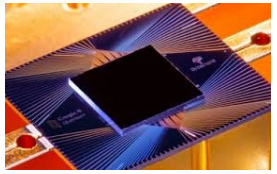
1992: ドイチ・ジョサのアルゴリズム（古典より高速な初めての例）

専門家の注目を集める

1994: ショアの素因数分解アルゴリズム（初めての有用な例）

第一次量子情報ブーム（ERATO、シンガポールCQT）

2009年あたり：国内は量子情報冬の時代（海外は違った）



2019: Google 50qubit マシン

第二次量子情報ブーム（Qleap、ムーンショット）

反省点

冬の時代のため、人材に年齢ギャップが
→５０代と２０代に少ししかいない

いきなり大規模プロジェクトをやっても参加できる専門家がいない
→海外は学生、若手、中堅、シニア各世代の専門家がまんべんなくそろった強力な布陣

理論研究は人が全てであり、育成に１０年かかる。

→流行り廃りにかかわらず、長期もしくはパーマネントポジションで薄くてもいいから長く安定にサポートするのが重要

私の研究テーマ

- 量子計算理論
- 量子暗号理論

5年間の（主要）業績

Physical Review Letters　２本（物理の著名学術誌）
Physical Review X　１本（物理の著名学術誌）
QIP　４本（量子情報のトップ国際会議）
Qcrypt　１本（量子暗号のトップ国際会議）
npj QI　１本（Natureの量子情報専門誌）IF=7.385
ITCS　１本（理論計算機科学のトップ国際会議）
CRYPTO　２本（暗号のトップ国際会議）
Eurocrypt １本（暗号のトップ国際会議）
Asiacrypt　２本（暗号の３大会議の一つ）

量子情報は学際的：伝統的な物理だけでは対処できない

→基礎物理学研究所はいちはやく独立した量子情報グループを作り、伝統的物理の枠を超えて、情報科学の分野でも国際的に顕著な業績を出している

→基礎物理学研究所は研究に注力できる環境をうまく作れており、非常にアクティブな研究活動が可能となっている

量子計算理論

量子計算は古典計算より速いのか？

VS

実はまだ完全には分かっていない

注：国内のメディアでよく見る某「実機」を用いて現実社会の組合せ最適化を解く話は量子計算とは何の関係もないので騙されないように！

→それらが高速であるという科学的根拠は全くない！（あるテーマが流行すると、「専門家」がわらわらと湧いてきて好き勝手なことを言い始めるので要注意！）

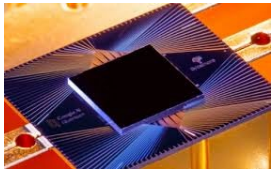
現状でいえること（量子超越性）

信頼できる仮定でないといけない（P≠NPなど）

もしある「仮定」が正しいなら、量子計算機はある「問題」を高速に解けるが、古典計算機では解けない

有用であることが望ましい（量子化学、TDAなど）

Googleの場合は？



仮定：XQUATH　ランダムに選ばれた量子回路が全て0を出す確率を2^{-n}よりも2^{-3n}高い精度で推定することは古典計算機では不可能である

問題：ランダムな量子回路をシミレートせよ

こんな微妙な仮定でしかもこんな役に立たない問題においてすら、量子超越性を示すのに世界中で皆苦労している。いわんや、現実社会の組み合わせ最適化や量子化学をや

そうはいっても、世界中で皆、ゴール（社会に役立つ量子計算機）に向けて研究を粛々と進めている

我々の貢献：

（１）今までで最も良い仮定（一方向性関数の存在）で量子超越性を証明

（２）TDAの高速量子計算アルゴリズム

（３）量子化学における（特定の）量子超越性

量子暗号

量子で暗号と聞くと。。。

普通の人がイメージするもの

（１）量子計算機で暗号が破れるんだよね（ショアのアルゴリズム）

（２）量子を使うと絶対安全な暗号ができるんだよね（ＱＫＤ）

間違いではないですが、全然それだけではありません！

量子暗号というのはもっといろいろなもの！

安全性には２種類ある

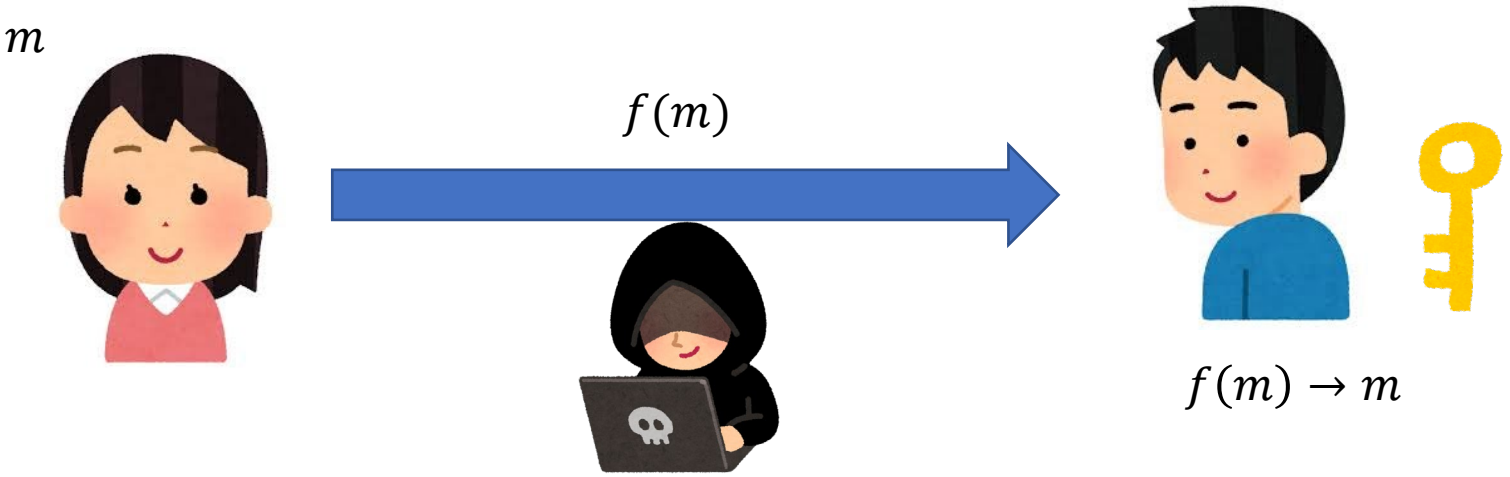
（１）情報理論的安全性

米国とソ連の大統領間のホットライン：鍵を厳重な警備のもと運ぶ

絶対安全。でもいろいろと制約が。。。

安全性には２種類ある

（２）計算量的安全性



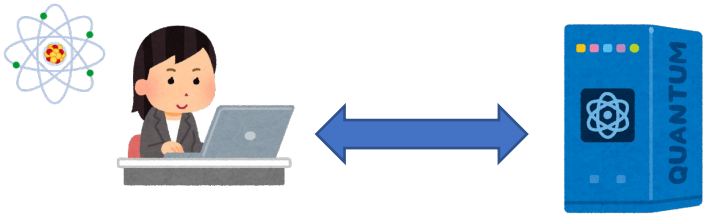
攻撃者の計算能力が制限されているなら安全

素因数分解はむつかしい、格子の問題がむつかしい、といった仮定を設ける

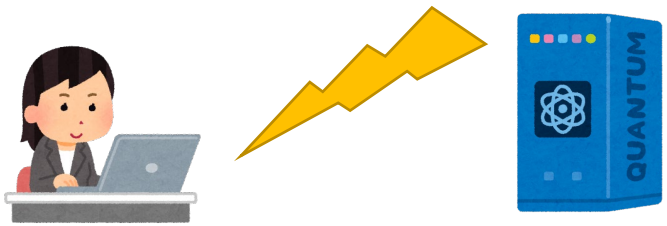
かなりいろいろなことができる！！

計算量的量子暗号

量子暗号プロトコル：量子を用いて情報理論的安全な暗号を実現



耐量子暗号：古典の暗号の量子的攻撃に対する安全性を研究する。



古典暗号

量子計算機による攻撃

ここ数年重要に
なってきている！

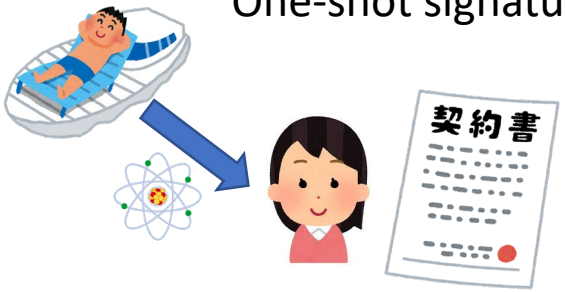
我々の貢献

（1）様々な新しい機能を持った暗号プロトコルの開発

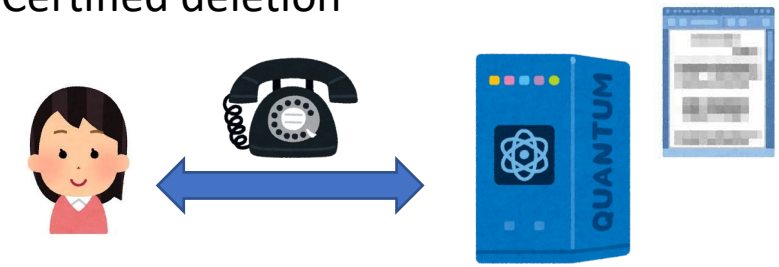
（2）計算量的量子暗号はより安全な仮定から構成できることを初めて証明

量子マネー

One-shot signature



Certified deletion



まとめ

- 基礎物理学研究所の量子情報グループでは、伝統的物理の枠を超えて学際的な分野で国際的に顕著な業績をあげてきている

- 理論研究は、流行に左右されない長く安定な人材へのサポートが重要