# 小芦研究室

## （量子情報　理論）　量子通信、量子コンピュータ、量子インターネット、基礎論…

### *量子情報の面白さ：基礎と応用が密接に関連　　例えば…*

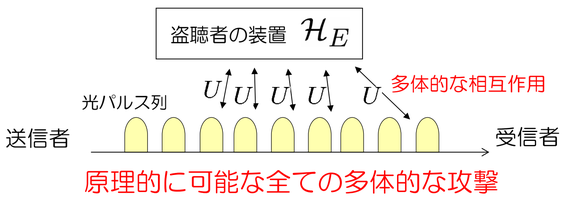
#### 量子暗号

BennettとBrassardによる提案（1984年）

- ハイゼンベルクの不確定性原理を利用

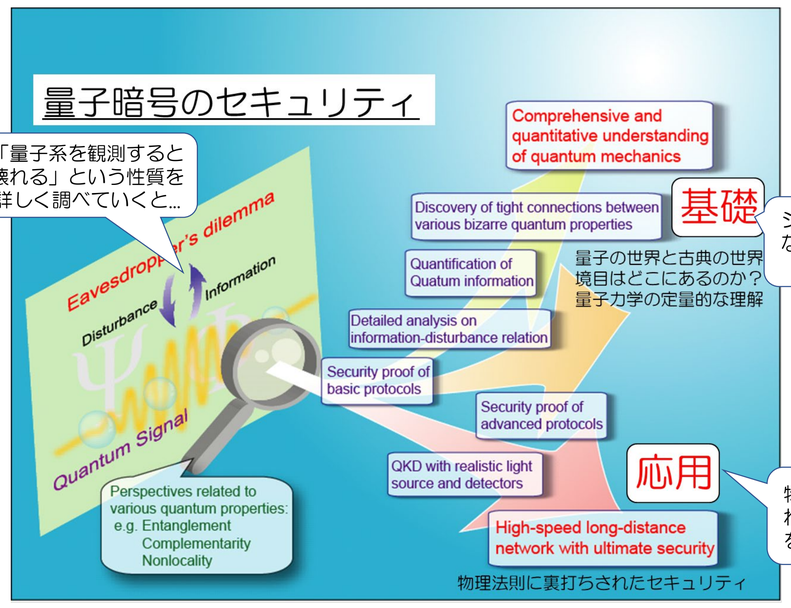
「観測すると壊れる」


「盗聴者に読まれたことがあとでチェックすればわかる」




原理的に可能な全ての多体的な攻撃

直接計算しようとしても、歯が立たない。そこで…




量子力学のいろいろな性質を総動員して考察する。
（エンタングルメント、相補性、非局所性など）

シャノン理論の量子版などの根源的な問題が明らかに。

物理法則によって守られた高いセキュリティをもつ暗号通信の実現

量子情報の大きさとは？

古典情報　　シャノンの理論（情報理論の礎）

$\{p_i, i\}$　　ABCDBCDBCABCDBC….

確率　文字

$H(\{p_i\}) \equiv -\sum_i p_i \log_2 p_i$ bits Shannon(1948)

この信号を保存するのに最低限必要なメモリの大きさ

量子情報の場合は？

$\{p_i, \rho_i\}$　この信号を保存するのに必要十分な量子メモリの大きさは？

量子状態

$\rho \equiv \sum_i p_i \rho_i$

$S(\rho) \equiv -\mathrm{Tr}[\rho \log_2 \rho]$

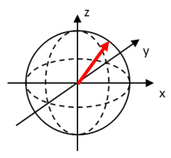
$\rho = \bigoplus_l p^{(l)} \sigma^{(l)} \otimes \tau^{(l)}$

$S(\rho) = H(\{p^{(l)}\}) + \sum_l p^{(l)} S(\sigma^{(l)}) + \sum_l p^{(l)} S(\tau^{(l)})$

必要な古典メモリ(bits)　必要な量子メモリ(qubits)　保存の必要なし

一見、無関係に思える量子暗号のセキュリティの研究の副産物として、この公式が発見された。

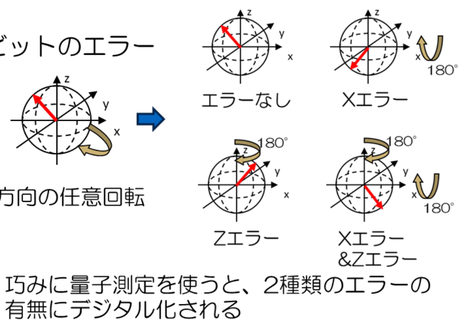
### 量子誤り訂正



見ると変化する ⟶ 壊れやすい

状態は連続的 ⟶ アナログエラーって訂正できない？

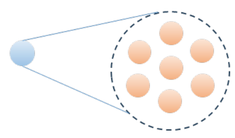
量子ビットのエラー




任意方向の任意回転

巧みに量子測定を使うと、2種類のエラーの有無にデジタル化される

量子誤り訂正符号 [Shor, Stean]



1量子ビットの情報を7量子ビットに載せる（Steane符号）

- 大規模量子コンピュータに必須の仕組み～
- 量子暗号のセキュリティ証明にも使われる

### ムーンショット目標６

MOONSHOT RESEARCH & DEVELOPMENT PROGRAM

https://www.jst.go.jp/moonshot/program/goal6/

ムーンショット目標６

**2050年までに、経済・産業・安全保障を飛躍的に発展させる誤り耐性型汎用量子コンピュータを実現**

理論研究のプロジェクトを担当

目標6 研究開発プロジェクト

**誤り耐性型量子コンピュータにおける理論・ソフトウェアの研究開発**

プロジェクトマネージャー(PM)　小芦 雅斗
東京大学 大学院工学系研究科　教授

**概要**

量子情報、アーキテクチャおよび物理系の研究者を結集し、量子ビットの設計、誤り耐性方式の実装、効率的に計算を実行するためのコンパイラや言語までを包含した協調設計モデルを構築します。それにより、2050年には、大規模な量子コンピュータの実現を目指します。

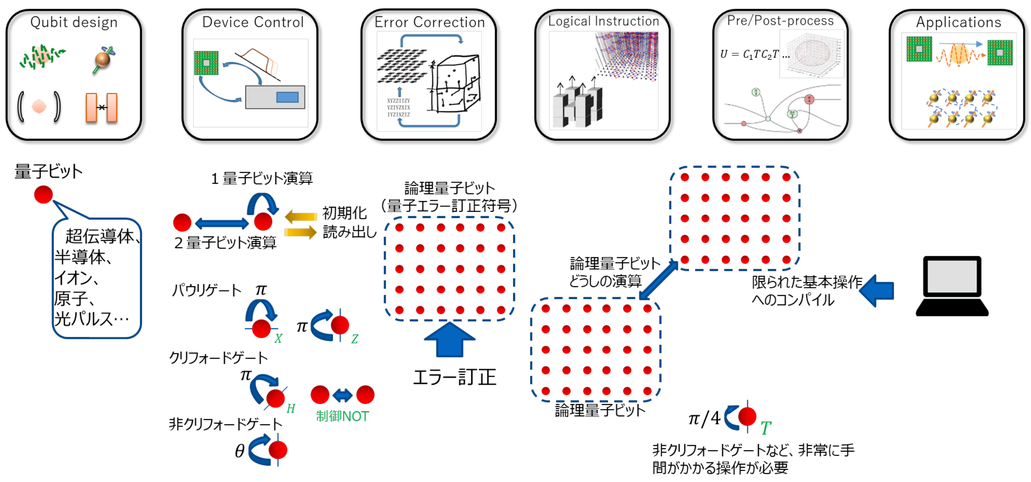
**研究開発機関**

大阪大学、沖縄科学技術大学院大学、京都大学、慶應義塾大学、産業技術総合研究所、情報・システム研究機構、筑波大学、電気通信大学、東京医科歯科大学、東京大学、日本電信電話株式会社、理化学研究所

### 誤り耐性量子計算（FTQC）

Fault-Tolerant Quantum Computation

・ エラーを随時訂正しながら計算を進める仕組み




### 量子アルゴリズム　～物性・化学の高速・高精度なシミュレーション～

**量子多体系の問題**

- 時間発展(ダイナミクス)　$|\psi\rangle \to e^{-iHt}|\psi\rangle$
- 熱平衡状態　$\rho_\beta \propto e^{-\beta H}$
- 固有値/固有状態　$H|\phi_n\rangle = E_n|\phi_n\rangle$

⟶ 低温物理（磁性,超伝導 etc）　化学反応

量子計算が従来の古典計算機より

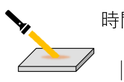
多項式的 or 指数的な計算時間の改善

指数的な計算メモリの改善

の可能性！！

R. Feynman (1981) from wikipedia

**当研究室の成果**　K. Mizuta, K. Fujii, QIP 2023 / K. Mizuta, K. Fujii, Quantum 7, 962 (2023)



時間依存系の最適な量子アルゴリズム

$|\psi\rangle \to \mathcal{T}\exp\left(-i\int_0^t \mathrm{d}t' H(t')\right)|\psi\rangle$

時間周期系・準周期系

最適な計算コスト　$\alpha t + \omega t \log(1/\varepsilon)$　≅ 理論限界

**高速・高精度な量子計算に向けた課題**

理論上最も良い計算コストを持つ量子アルゴリズムの構築

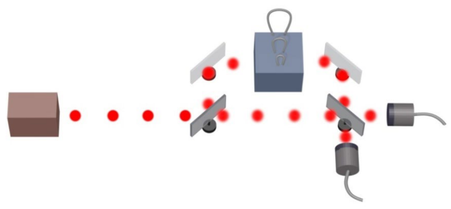
• Trotter 分解　・ユニタリ線型結合　・量子特異値変換

“量子多体系(物性物理)の知見”

・Lieb-Robinson 限界
・時間周期系
・量子開放系

### *量子情報には、まだまだ知らないことが眠っている！*

#### 全く新しい原理に基づく量子暗号



（従来）
「盗聴者に読まれたことがあとでチェックすればわかる」

「そもそも盗聴者がほとんど読めない」
不確定性原理は無関係

LETTER

doi:10.1038/nature13303

**Practical quantum key distribution protocol without monitoring signal disturbance**

Toshihiko Sasaki[1], Yoshihisa Yamamoto[2,3] & Masato Koashi[1]

Sasaki, Yamamoto, Koashi, Nature **509**, 475 (2014).
Takesue, Sasaki, Tamaki, Koashi, Nature Photonics **9**, 827 (2015).

どうやら量子力学には、我々が３０年気が付かなかった情報の隠し場所があるらしい・・・

### *大学院生も第一線で活躍！*

欧州のグループが
「量子暗号の通信距離を数百キロ長くするアイデア」をNature誌に発表
でも肝心の「セキュリティ」がどうなのかは不明

世界中の大御所がセキュリティ証明を競うお祭り状態

当時M1の学生が無謀にもこれに挑戦、見事に解決！

nature COMMUNICATIONS

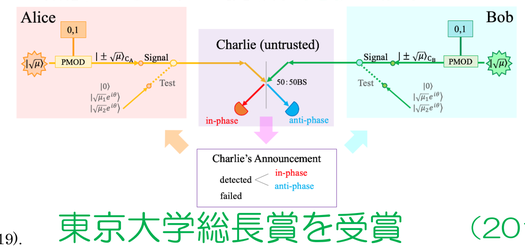
ARTICLE

https://doi.org/10.1038/s41467-019-11008-z OPEN

**Repeaterless quantum key distribution with efficient finite-key analysis overcoming the rate-distance limit**

Kento Maeda[1,2], Toshihiko Sasaki[1] & Masato Koashi[1,2]

Maeda, Sasaki, Koashi, Nature Communications **10**, 3140 (2019).




東京大学総長賞を受賞　（2019年度）

2021年度にも博士学生が総長賞を受賞