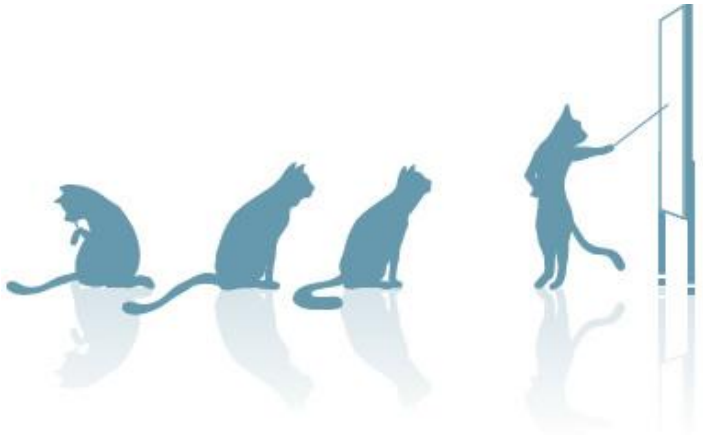
量子と暗号

平野琢也[1,2]
[1]学習院大学理学部物理学科
[2]ImPACT 革新的研究開発プログラム
「量子人工脳を量子ネットワークでつなぐ高度知識社会基盤の実現」
http://www.jst.go.jp/impact/hp_yamamoto/index.html



ImPACT Program　量子人工脳を量子ネットワークでつなぐ高度知識社会基盤の実現

ImPACT Program Manager

山本　喜久　*Yoshihisa YAMAMOTO*

1978年　東京大学大学院博士課程修了（工学博士）
1978～1992年　NTT（現在　R&Dフェロー）
1992年～2014年　スタンフォード大学 教授（現在　名誉教授）
2003年～2014年　国立情報学研究所 教授
2013年～2014年　理化学研究所 グループディレクター
2014年～ImPACT ﾌﾟﾛｸﾞﾗﾑ･ﾏﾈｰｼﾞｬｰ

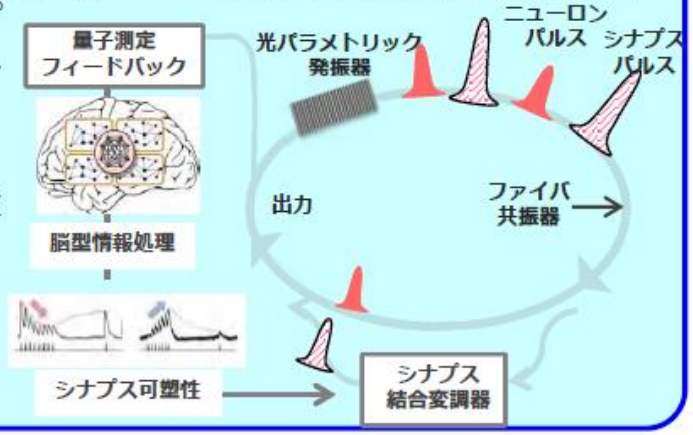
量子情報通信技術の研究グループをNTT基礎研究所内に設立し、以後30年以上にわたって、世界の量子情報通信研究の最先端を切り拓く。日本国内および米国内の大型国家プロジェクトを多数指揮。2009～2014年内閣府・最先端研究開発支援（FIRST）プログラム中心研究者。

＜研究開発プログラムの概要＞

脳型情報処理を量子コンピュータに取り込んだ量子人工脳を開発し、これを絶対に盗聴を許さない量子セキュアネットワークで結んだ高度知識社会の基盤を確立する。

＜非連続イノベーションのポイント＞

ファイバリング・パラメトリック発振器に同時に生成される1～100万の光パルスをニューロンと見立て、これらを量子測定フィードバック回路で相互結合し、大規模シナプスネットワークを実現し、組み合わせ最適化問題を高速で解くイジングマシーンとする。



＜期待される産業や社会へのインパクト＞

将来のデータセンターやロボット・衛星に搭載可能な革新的な量子人工脳が誕生し、その恩恵を安全性脅威に怯えることなく享受できる高度情報社会の基盤技術を確立する。

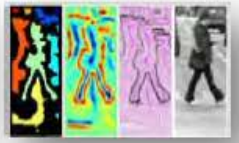
量子人工脳・量子シミュレーションの研究開発

背景

組み合わせ最適化問題は、現代社会の様々な分野で現われる重要な問題であるが、現代コンピュータでは効率よく解くことのできないNP困難クラスに属している。


創薬・生命科学

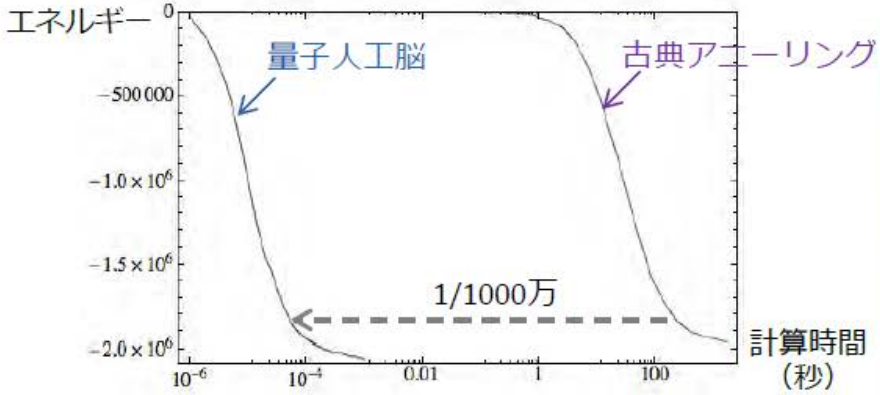

無線通信


機械学習


ソーシャル・ネットワーク

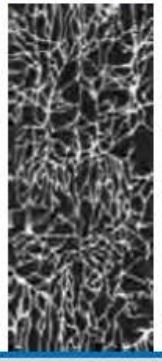
インパクト

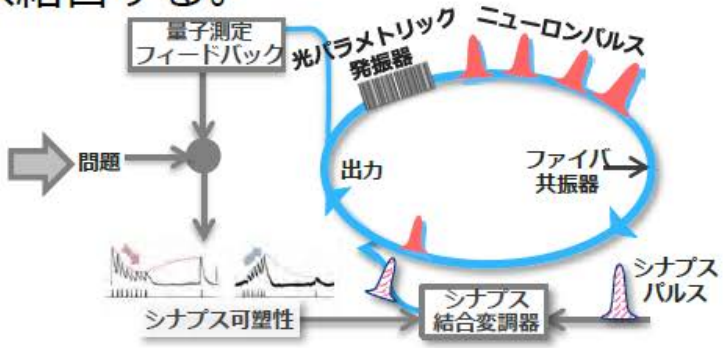
NP困難MAX-CUT問題（ノード数20,000の完全グラフ）を現代コンピュータ（古典アニーリング）と比べ、1/1000万の時間で解けることを計算機実験で確認した。



アイデア

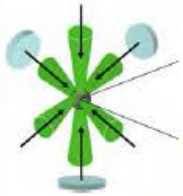
パラメトリック発振器に同時に発生される多重光パルス1つ1つをニューロンとみたて、これを量子測定フィードバック回路でシナプス結合する。

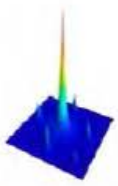


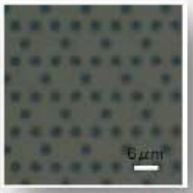


古典イジングモデルから量子スピンモデルへ

材料研究者のインスピレーションに頼らない新機能物質探索を可能にする。


冷却原子





励起子ポラリトン


超伝導量子回路

量子セキュアネットワークの研究開発

背景

現代暗号はその安全性が盗聴者の計算能力に依存しているため、常に改訂や更新が必要である。また、複雑なアルゴリズムで信号処理をするため遅延が避けられず、ネットワークの相互接続も困難である。

漏えいが致命的となる情報

- 個人の医療情報、遺伝子情報、犯罪履歴
- 国家安全保障

アイデア

異なる通信システムを跨ぐシームレスな暗号通信を実現

暗号方式の大幅な簡素化

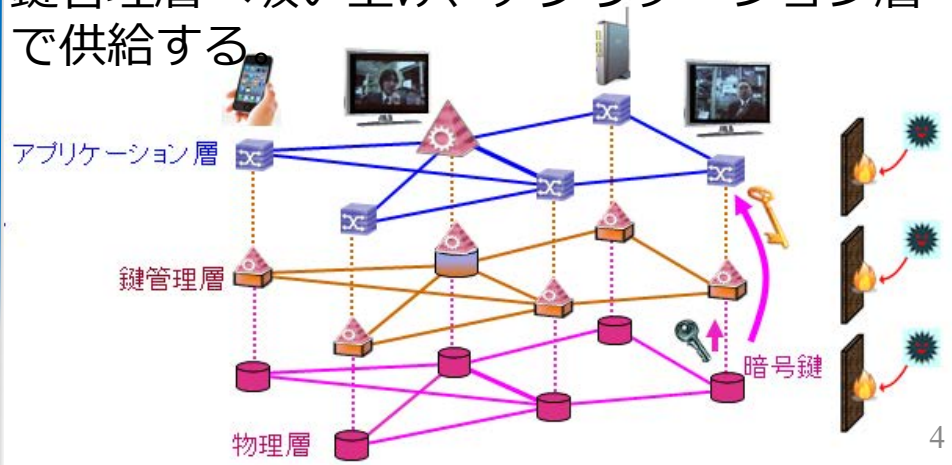
暗号化
平分と鍵の単純な足し算
$C = X \oplus K$

Decoy BB-84方式 対 RR-DPS方式

	Decoy-BB84方式	RR-DPS方式
原理	読まれたら気付く 不確定性原理	そもそも読まれない 波束の収縮
回線の雑音 (ビット誤り率)	～11%まで許容	～35%まで許容
最低限必要な通信量	～1,000,000ビット	～1,000ビット
変調方式	位相・振幅変調を併用	位相変調のみ
復調方式	固定遅延	可変遅延
光源の品質管理	多くのパラメータを保証する必要あり	単一のパラメータを保証するだけでよい
現状	実用化段階	研究段階

ネットワークアーキテクチャー

物理層の量子鍵配送で生成された安全鍵を鍵管理層へ吸い上げ、アプリケーション層で供給する。



量子情報処理とは

量子力学の基本的な原理や効果を直接利用した
情報処理、通信技術

例　量子コンピュータ、量子暗号、量子テレポーテーション

“Information is physical” ---Rolf Landauer
→ 情報は物質により担われており、情報の処理は
物理法則（＝量子力学）を基盤とすべし

既存の技術に比べて格段に優れた処理を実現可能

例 ・既存の技術では，宇宙の年齢よりも長い計算時間が必要な
問題を有限の時間で解く
・絶対に安全な通信

量子と暗号：本日の予定

1．はじめに

ImPACTの紹介

量子力学は面白くて不思議な法則で，未来技術の鍵．

2．量子情報科学入門

量子と暗号の関係とは？量子コンピュータとImPACT

3．量子論入門

干渉，粒子性と波動性 （DVD、討論）

4．量子暗号とは

量子暗号の説明

量子暗号デモ実験

5．質疑など

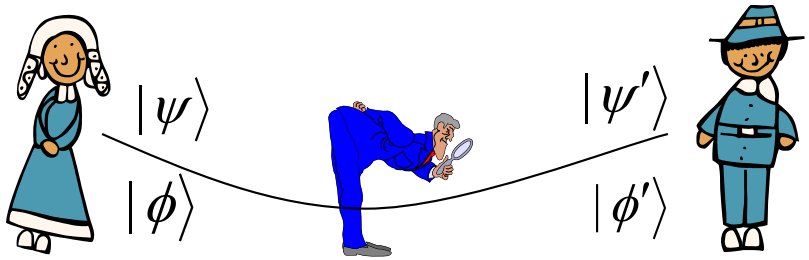
量子暗号とは

量子暗号：量子力学の原理を利用して安全な通信を実現する

↓

測定対象について何らかの情報を得た場合，
測定対象の状態は変化してしまう

第3者による盗聴
→検出可能



量子鍵配送(Quantum Key Distribution)の目的

空間的に離れた2つの地点で同じランダムなビット列を共有する
（秘密鍵）

秘密鍵をどのように使うのか？

Alice

送りたい信号
001010011

秘密鍵
100111010

暗号化
101101001

XOR	0	1
0	0	1
1	1	0

Bob

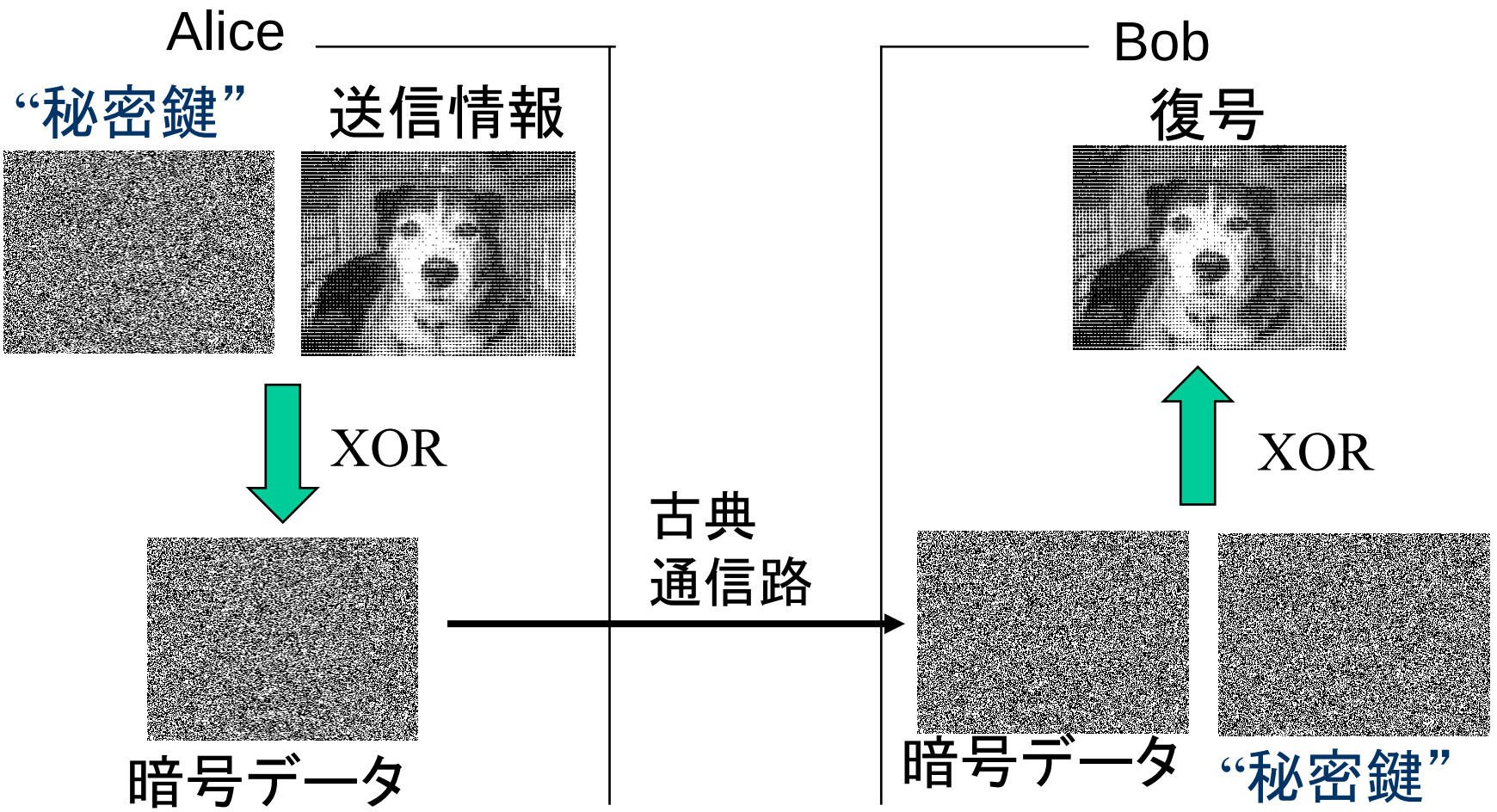
XORにより
001010011

秘密鍵
100111010

受け取った信号
101101001

ワンタイムパッド暗号ー情報理論的に安全
送りたい情報と同じ長さの秘密鍵を使う

秘密鍵を使った安全な通信



まとめ

量子の世界

　　日常的な常識の通用しない不思議な世界

　　先端技術分野では量子の世界が目前に

　　量子の原理を利用することで優れた情報処理が可能

光の粒子性と波動性

　　たった1個の光子もヤングの干渉を起こす

量子暗号：絶対安全な通信

　　単一光子の偏光を使うBB84プロトコルを紹介

・物理は皆さんが思っているより広くて自由

・様々な分野が融合して，新しい可能性が生まれている