北海道大学

2030年エレクトロニクスの旅

－旅2　量子が守る情報－

2011年10月18日

北海道大学工学部　情報エレクトロニクス学科
電子情報コース
情報科学研究科情報エレクトロニクス専攻
光エレクトロニクス研究室

富田　章久

20世紀を代表する科学的発見は？

ボーア

- ボーアモデル
- 相補性原理
- コペンハーゲン解釈

アインシュタイン

- 光量子仮説
- ボーズ-アインシュタイン凝縮
- EPR相関
- 「神はサイコロを振らない」

クロード　シャノン

通信の数学的理論
- 信号源符号化
- 通信路符号化

秘匿系での通信理論
- ワンタイムパッド

ハイゼンベルク

- 行列力学
- 不確定原理

シュレディンガー

- 波動力学
- 「猫」

情報理論

量子力学

量子情報科学

現代社会の要求と量子情報科学

量子情報ってなに？

なんで量子情報？　量子情報は何ができる？

量子暗号

(1) 現代暗号の安全性の限界

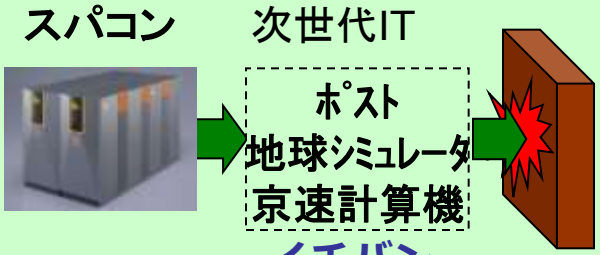
技術の進歩による解読の危険性
(例：量子コンピュータができると
今の公開鍵暗号系は崩壊・・)

(2)高まるセキュリティ要求

今のコンピュータ技術を仮定しない
安全性
－ その保証(理論的証明!!)

量子計算

(1) 現モデルの原理的限界



(2) 超高速計算への要求

・環境、気象、分子設計（製薬）、
セキュリティ・・

(悪）例：　公開鍵暗号破り

今そこにある
限界の打破

夢の実現へ

こんなことがニュースになるかも・・？

ニュートップ

2030年10月18日

インターネットバンキングをハッキング

SSL通信を解読：量子コンピュータは暗号系を崩壊させるか

[札幌発]北海道大学は10月17日情報科学研究科情報エレクトロニクス専攻（**工学部電子情報コース**）光エレクトロニクス研究室の大学院生が同研究室で開発した**量子コンピュータ**の性能テスト中に誤ってインターネット上で行われている通信を傍受，取引内容やパスワード等を保護していた**暗号**を解読していたと発表した．解読した内容は既に破棄されているため，実質的な損害は与えていないとしている．

なお，解読されたのは＊＊国のオンラインバンキング通信で日本の銀行では既に**量子暗号**による秘匿通信に切り替えられているため直接の影響は受けないが，・・・

誰にでも隠し事がある～暗号は何のため？

Everybody 's got something to hide except me and my monkey　(J. Lennon)

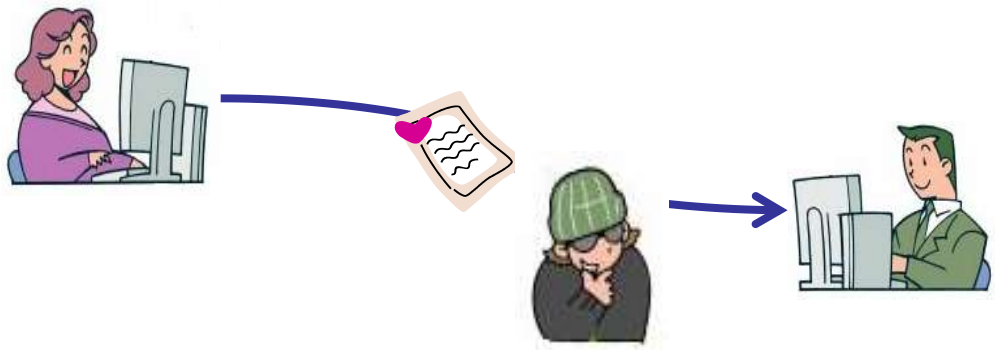
キャッシュカードの暗証番号
クレジットカードの暗証番号
＊＊サイトのパスワード
預金通帳と印鑑をしまってある場所

＃＃からのメール
○○先生の講義で代返頼んだこと

なかったことにしたいことは隠滅すればよい（できれば）
今後も**使いたい**情報で他人に知られてはいけないことを守る

秘密が通信回線を通ることが増えている
盗聴されていないか；**改ざん**されていないか；**相手**は本人か？

あなたの通信は盗聴されているかもしれない



現在の技術では光ファイバから漏れる光を検出できる

光は急に曲がらない

注意：写真の装置はファイバ保守のための
テスターで，盗聴器ではありません

RSA暗号：インターネットなどでも使われている暗号

準備

1. ランダムな素数p,qを選ぶ
   例：3,5（本当は大きくないといけない）
2. $N=pq$；$L=\mathbf{LCM}(p-1,q-1)$を求める.
   例：$N=15$；$L=4$
3. 公開鍵(e,N)を作る．eはLと素な正数
   例：$(7,15)$
4. 秘密鍵dを作る．$ed=Lk+1$　（kは任意の正数）
   例：$d=3(k=5)$

LCMとは最小公倍数のこと

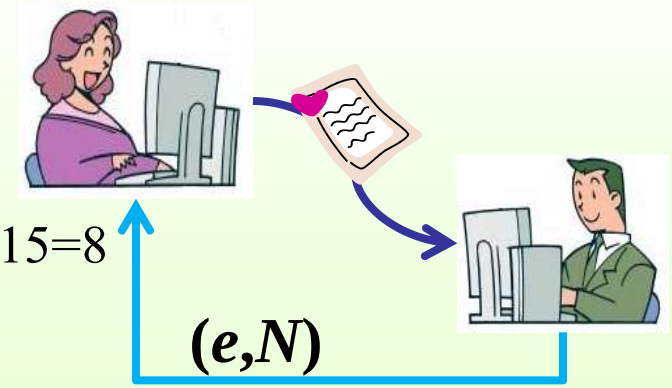
$a \bmod b$ とはaをbで割った余り．
例：$8 \bmod 3=2$
$(8\div3=2$ あまり$2)$

任意の数$M<N$について
$M^L \bmod N=1$　だから
$M^{1+Lk} \bmod N= M \bmod N$

暗号化

$\underline{\boldsymbol{C=M^e \bmod N}}$

例：$M=2$
$C=2^7 \bmod 15=8$



復号化

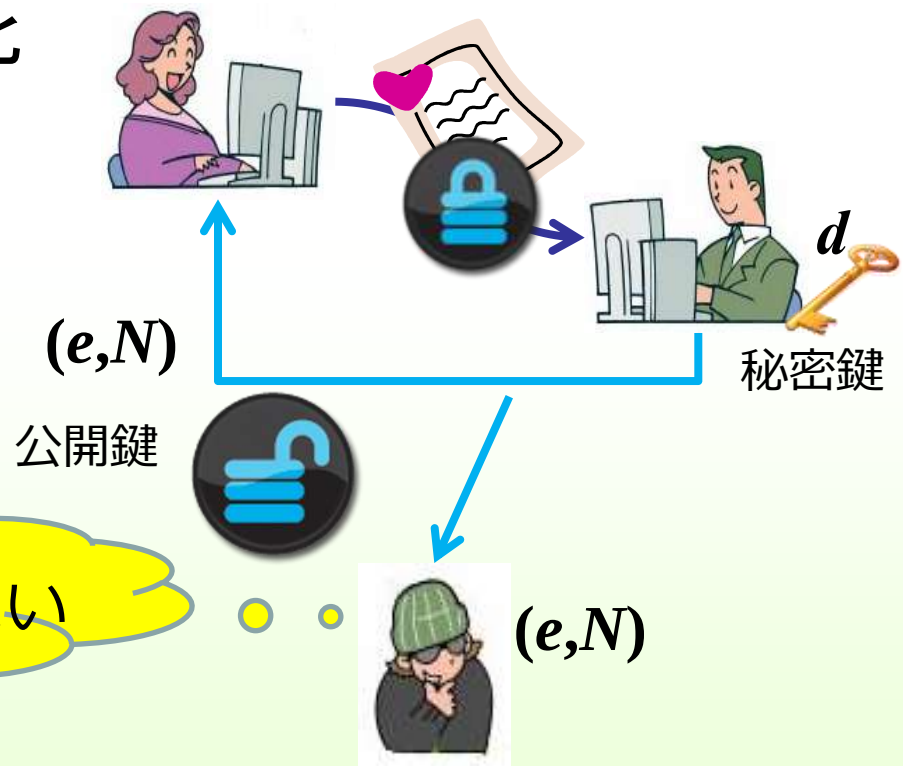
$\underline{\boldsymbol{M=C^d \bmod N}}$

ただし，$(M^e)^d \bmod N$
$= M^{1+Lk} \bmod N$

例：$C=8$　　$M=8^3 \bmod 15=2$

いろいろ数学が面倒そうだが，要するに

1. 受信者が公開鍵(e,N)を作る：$N=pq$と適当なe
2. 秘密鍵を作る：$ed=Lk+1$ただし，$L=\mathbf{LCM}(p-1,q-1)$
3. 公開鍵を送信者に送る
4. 送信者は公開鍵で暗号化
5. 暗号文を送る
6. 受信者は秘密鍵で復号



$(p.q)$かLがわかればよい

素因数分解

素因数分解の難しさ

できますか？

１５＝□×□

これは？

９１＝□×□

じゃあ，これは？

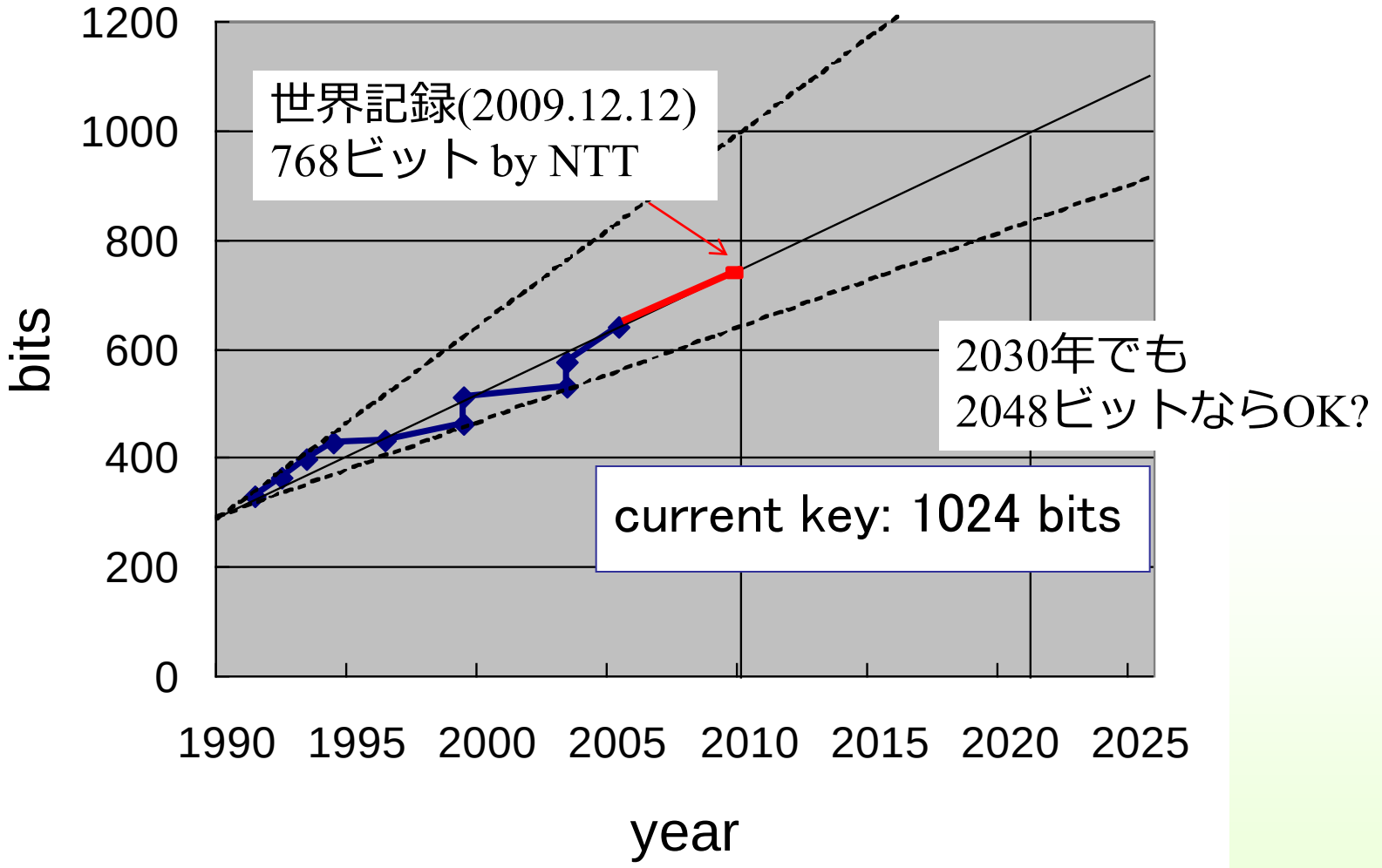
４,４６６,７００,４３３,６７０,４２１,７８１

＝□×□

計算量～$\exp[(\log n)^{1/2} \log(\log n))^{1/2}]$：準指数的

現在1024ビット＝10進で約300桁

RSAチャレンジ
RSA社が賞金を出した素因数分解のコンテスト



ビット数が増えるとより安全．でも計算コストがかかる

解けない暗号なんて

“… and it may well be doubted whether human ingenuity can construct an enigma of the kind which human ingenuity may not, by proper application, resolve. "
エドガー・アラン・ポー　黄金虫より

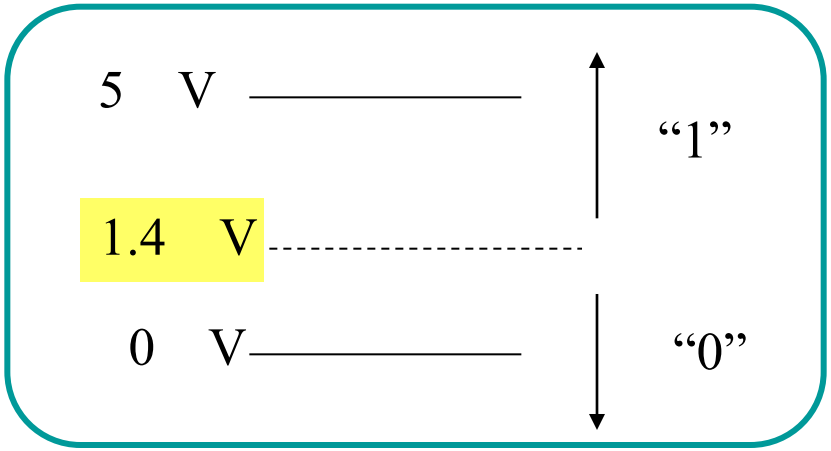
"What one man can invent another can discover," said Holmes.
アーサー・コナン・ドイル　踊る人形より

RSAが破れるとき

- 抜け穴の発見（RSAの困難≠素因数分解の困難）
- 素因数分解の効率的な解法の発見
- 計算機の驚異的な発達
- **量子コンピュータ**の実現

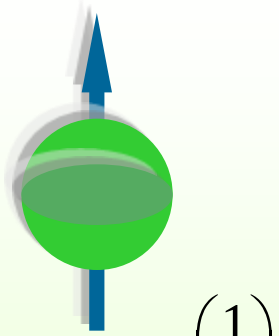
量子力学的状態

- 2準位で考えよう
  - 古典ビット: [0,1]

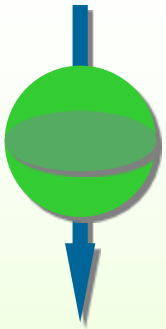


  - 量子ビット(キュービット qbit, qubit) : [|0>,|1>]
    スピン、偏光、電荷(の有無)、基底状態−励起状態、・・

量子状態は（長さ1の）ベクトルだ！



“|0>” $\begin{pmatrix}1\\0\end{pmatrix}$



“|1>” $\begin{pmatrix}0\\1\end{pmatrix}$

重ね合わせ

“$\alpha|0>+\beta|1>$” $\begin{pmatrix}\alpha\\\beta\end{pmatrix} = \alpha\begin{pmatrix}1\\0\end{pmatrix} + \beta\begin{pmatrix}0\\1\end{pmatrix}$

0と1の両方の成分を持つ

量子コンピュータが速い理由

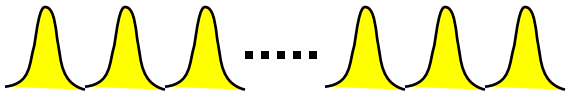
2^N 個

$x_0 + x_1 + x_2 + x_3 + x_4 + x_5 + x_6 + x_7$

000 001 010 011 100 101 110 111

量子ビットN個

$\begin{pmatrix}1\\1\end{pmatrix}\begin{pmatrix}1\\1\end{pmatrix}\begin{pmatrix}1\\1\end{pmatrix}$



重ね合わせ

一括処理
（超並列性）

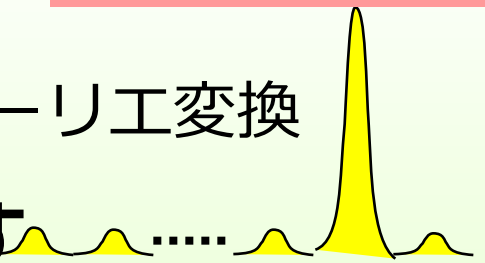
$$|\psi\rangle = \left(\frac{|0\rangle+|1\rangle}{\sqrt{2}}\right)\left(\frac{|0\rangle+|1\rangle}{\sqrt{2}}\right)\left(\frac{|0\rangle+|1\rangle}{\sqrt{2}}\right)$$

$$= \frac{1}{\sqrt{8}}\left(|000\rangle+|001\rangle+|010\rangle+|011\rangle+|100\rangle+|101\rangle+|110\rangle+|111\rangle\right)$$

$f(|\psi\rangle)$ ⟺ $f(x_1), f(x_2), \cdots, f(x_8)$

量子力学的干渉
量子力学的もつれ

例：量子フーリエ変換



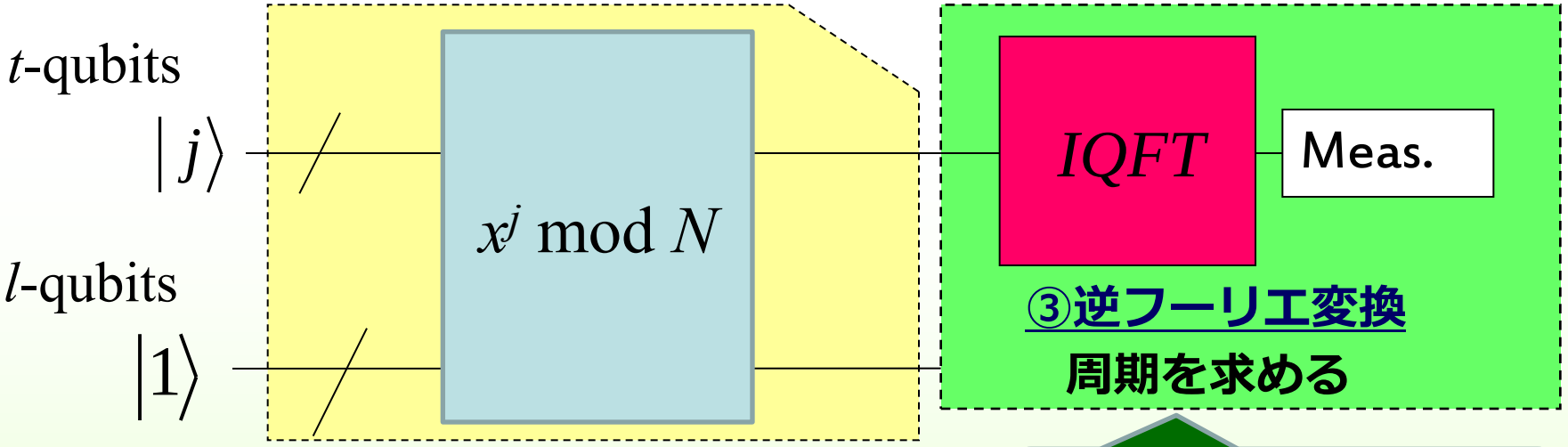
解となる状態を取り出す

・答のレジスタ

RSA暗号を破る量子コンピュータ

- 秘密鍵は　$ed=Lk+1$で計算するのでLがわかればよい
- $M^{Lk} \bmod N = 1$なので適当な数xについて$x^j \bmod N$を計算するとLごとに$x^a \bmod N = 1$になるaが現れる：つまり周期Lの関数

①tビットの全ての数を表わす重ね合わせ

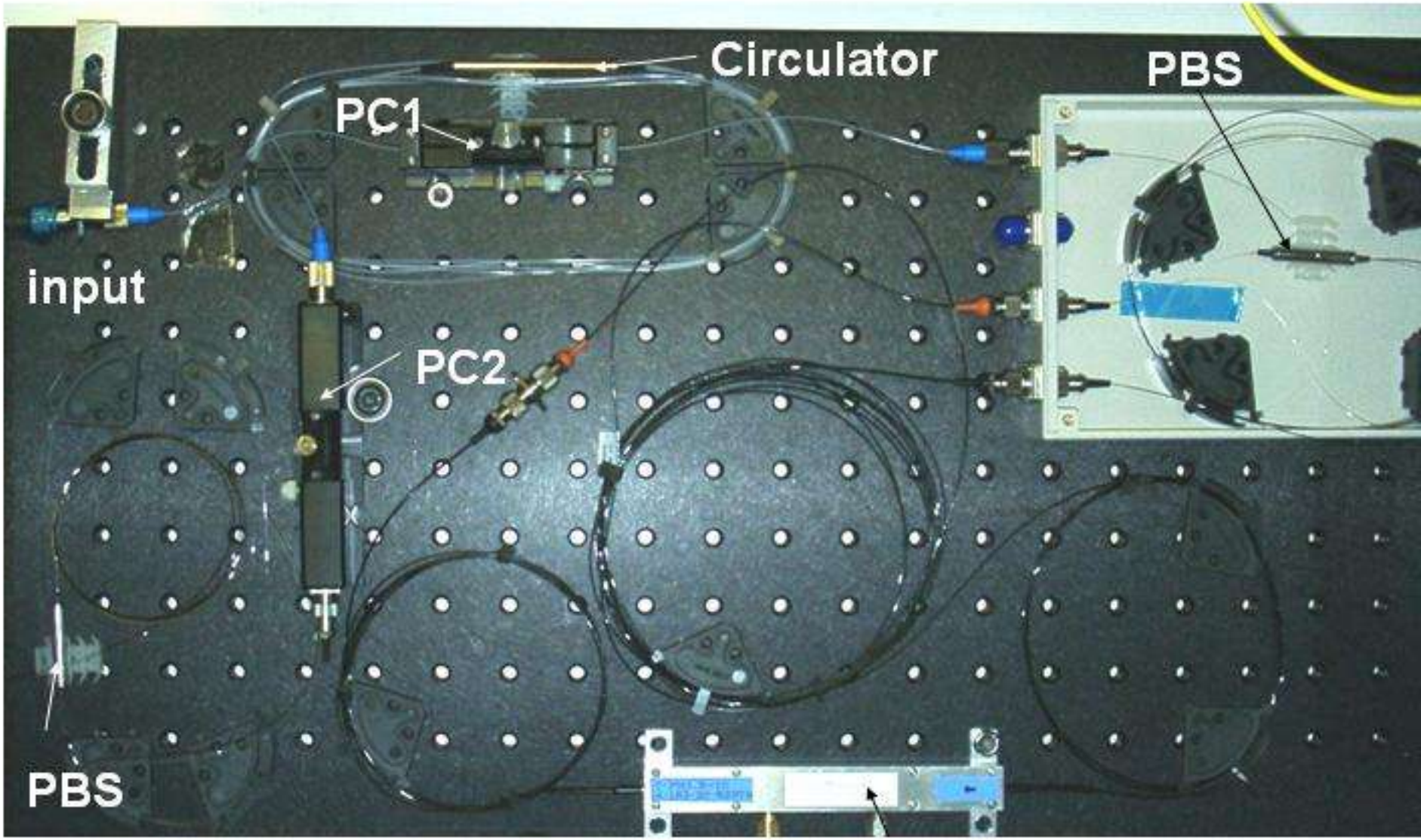


② 関数 $f_{x,N}(a)=x^a \bmod N$ を超並列計算

実はもうできている

こっちは難しい

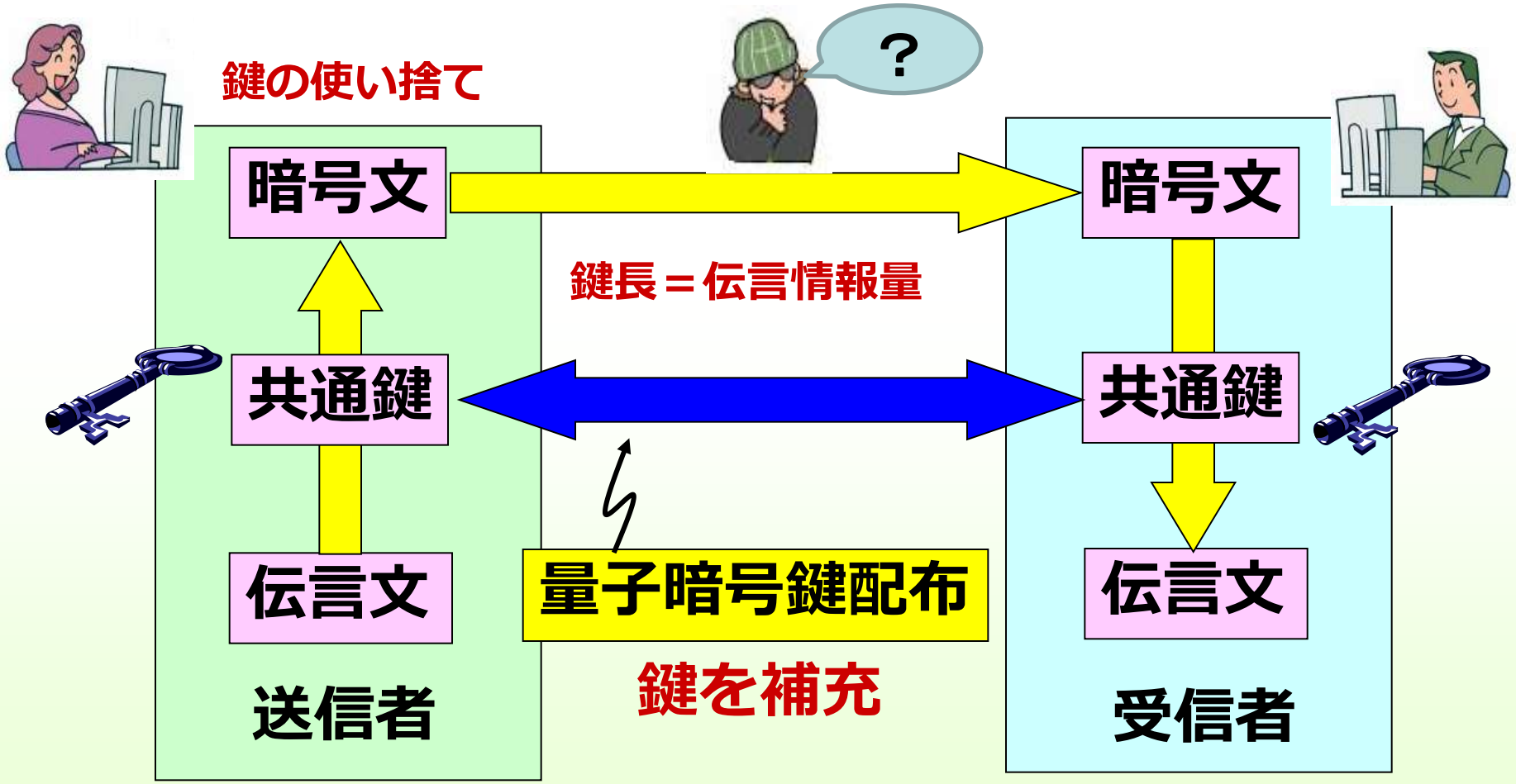
光通信デバイスで構成した量子フーリエ変換回路



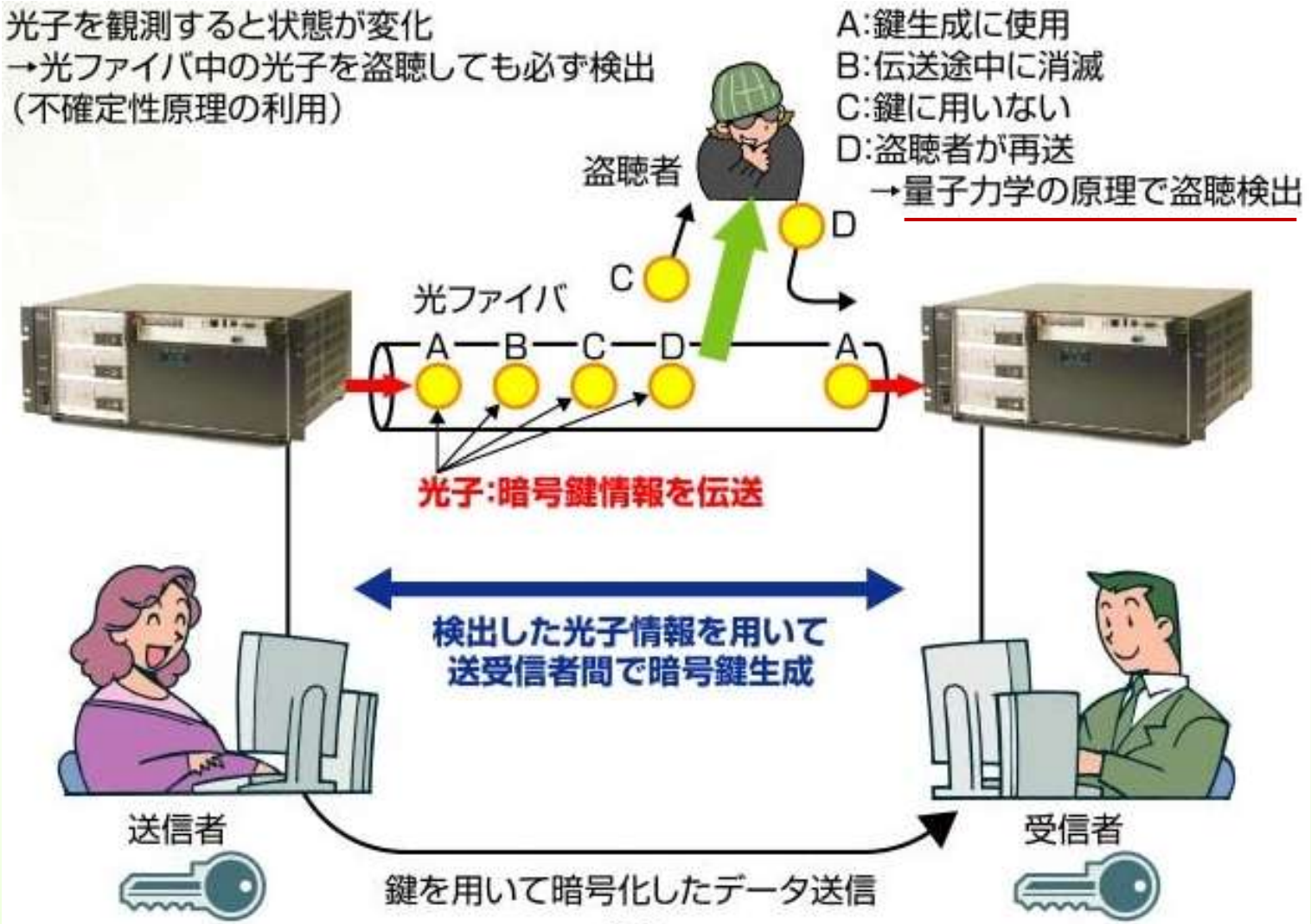
解けない暗号は存在する

ワンタイムパッド＝使い捨て鍵

無条件安全（無限の計算能力があっても解けない）が証明済



量子暗号鍵配付（QKD）



暗号鍵（乱数）を共有

※このイラストはNEC製です

量子暗号にとって重要な量子ビットの性質

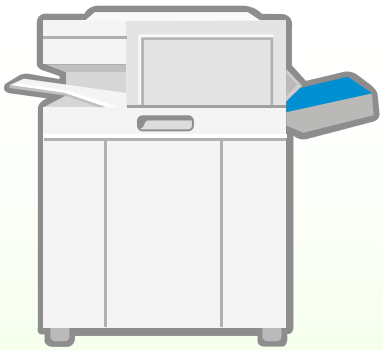
コピーできない

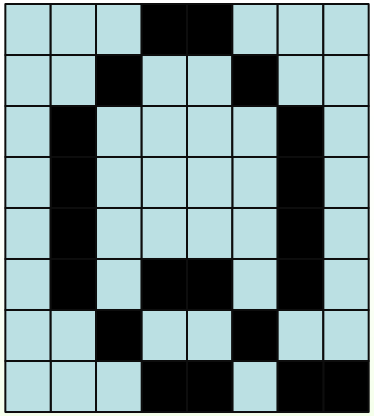
1回の測定では状態がわからない

} 同じこと

{あるか，ないか}

古典のばあい





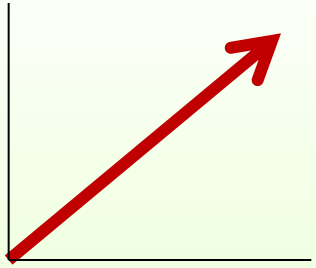
f(1,1)=0, f(1,2)=0,
f(1,3)=0, f(1,4)=1,…

測定して転写する

量子のばあい

状態はベクトル

向きが縦または横とか知っていれば1回の測定で分かるが・・・

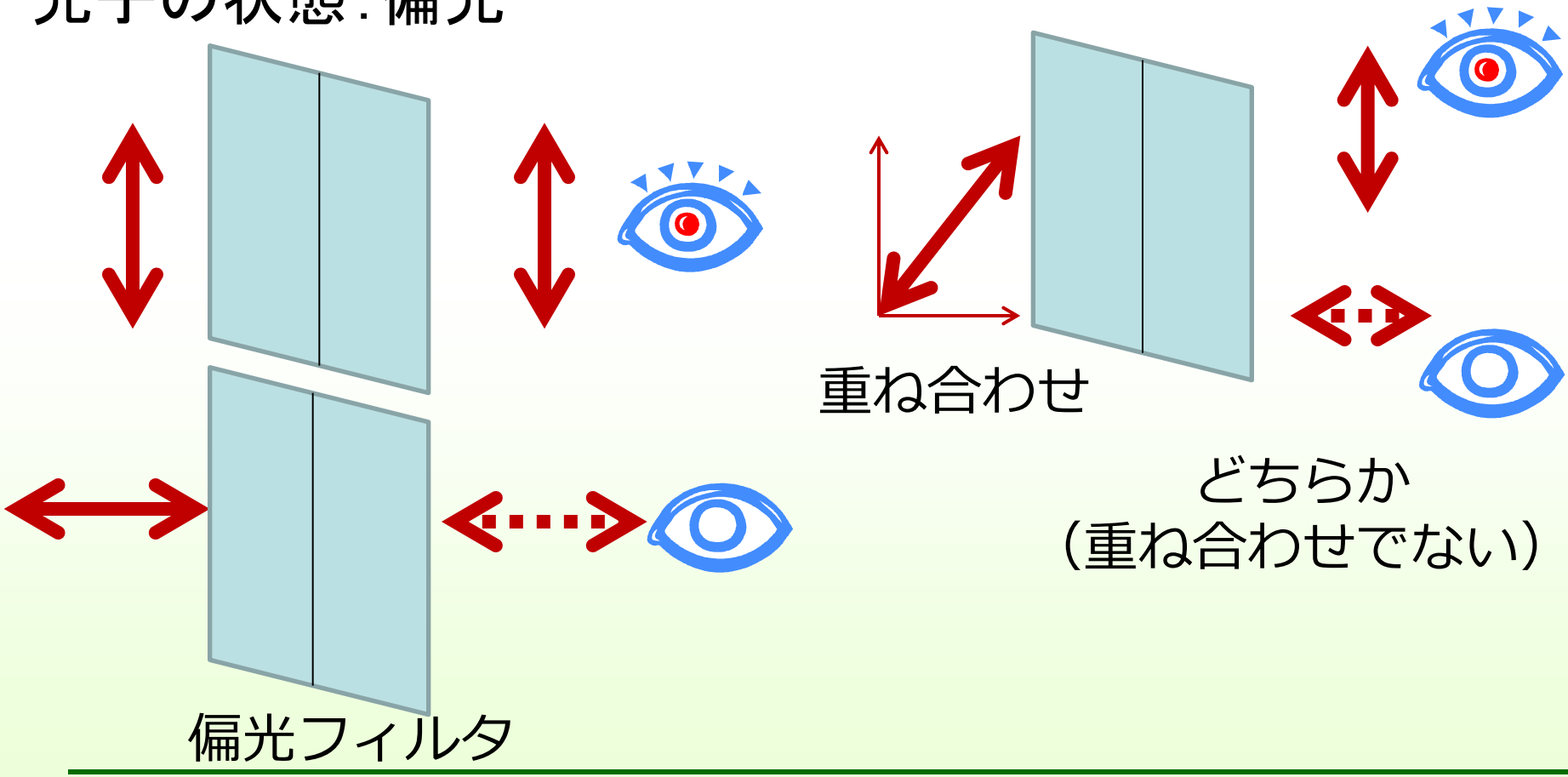


成分が決まらないので転写不能

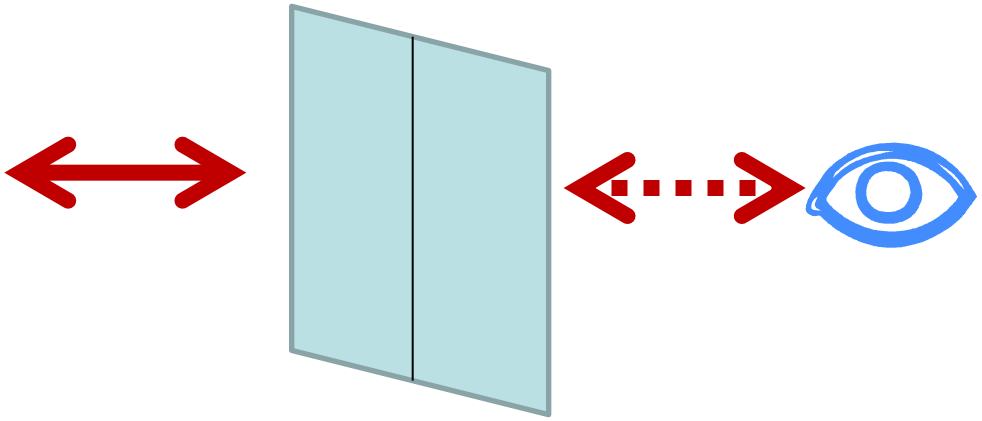
さらに悪いことに,

測定すると状態が変わってしまう

光子の状態：偏光



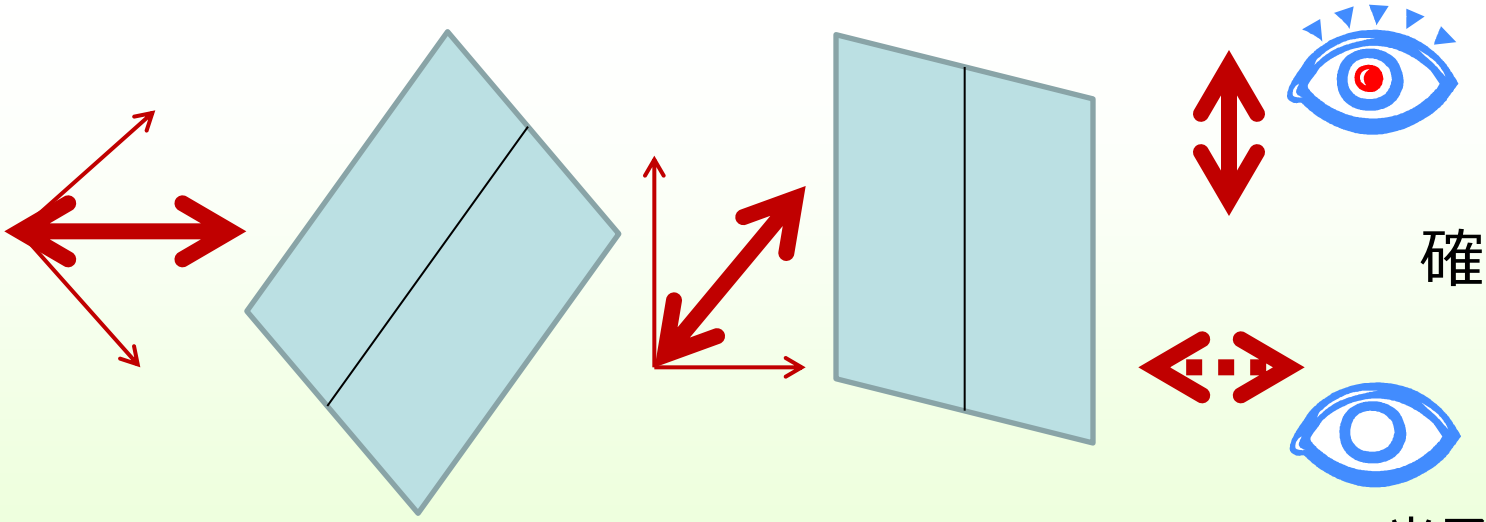
従って，こんなことも起きる



光子が来ない

偏光フィルタ

光子が来た！



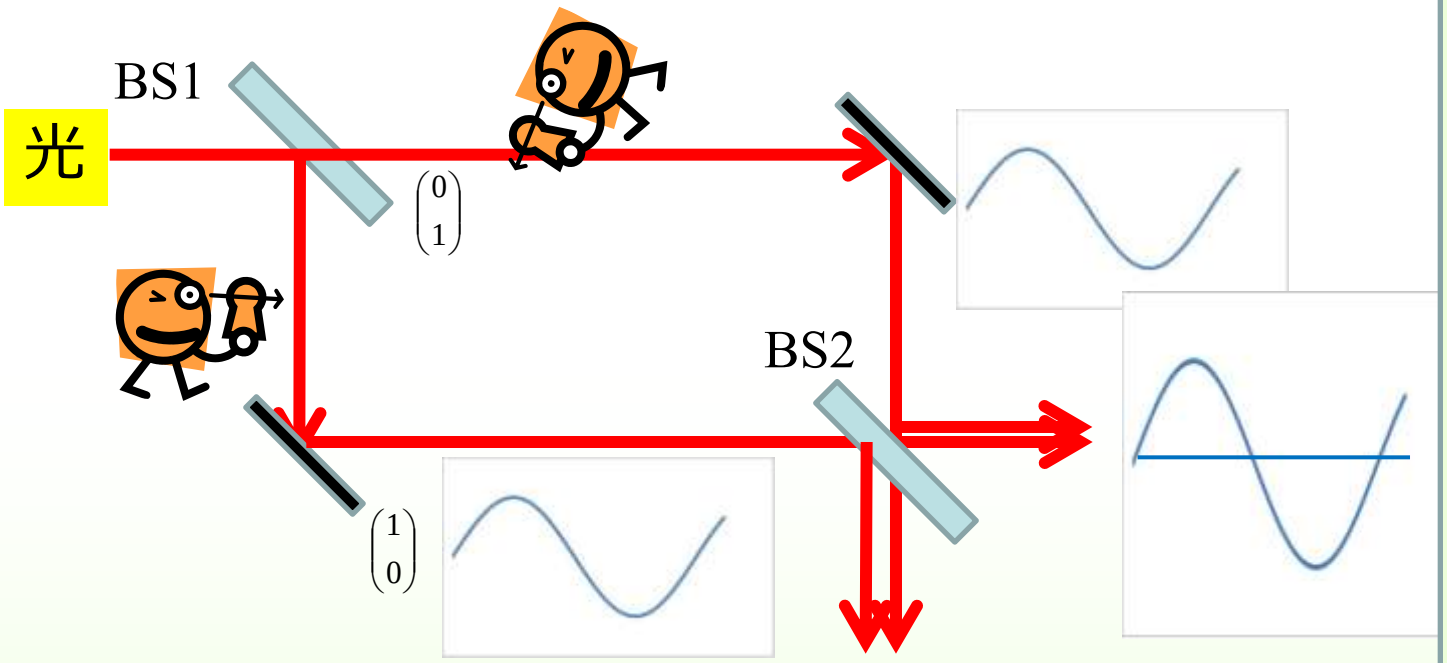
確率 1/2

光子が来ない

干渉現象

2つ以上の波の強めあい・弱めあい

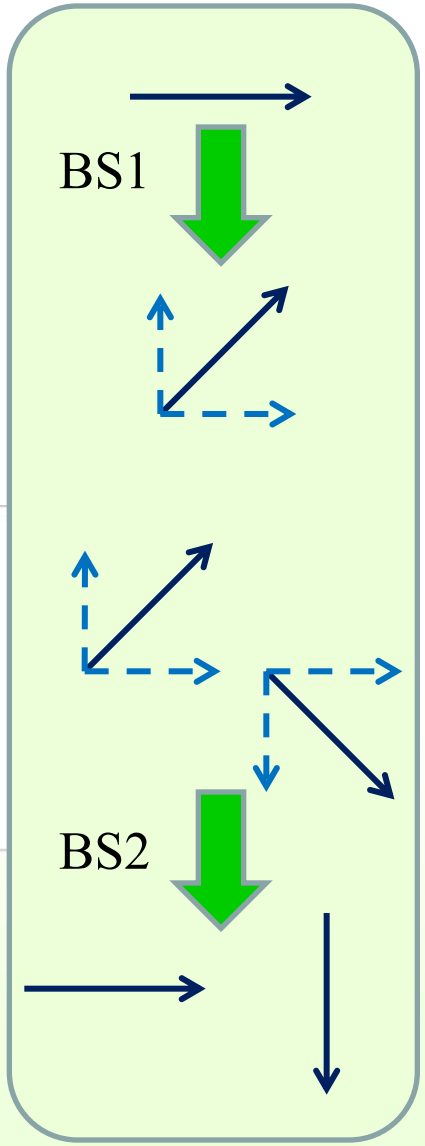
波同士の区別がつかないこと



経路を調べると干渉が消える

=ベクトル的な性質（重ね合わせがこわれる）

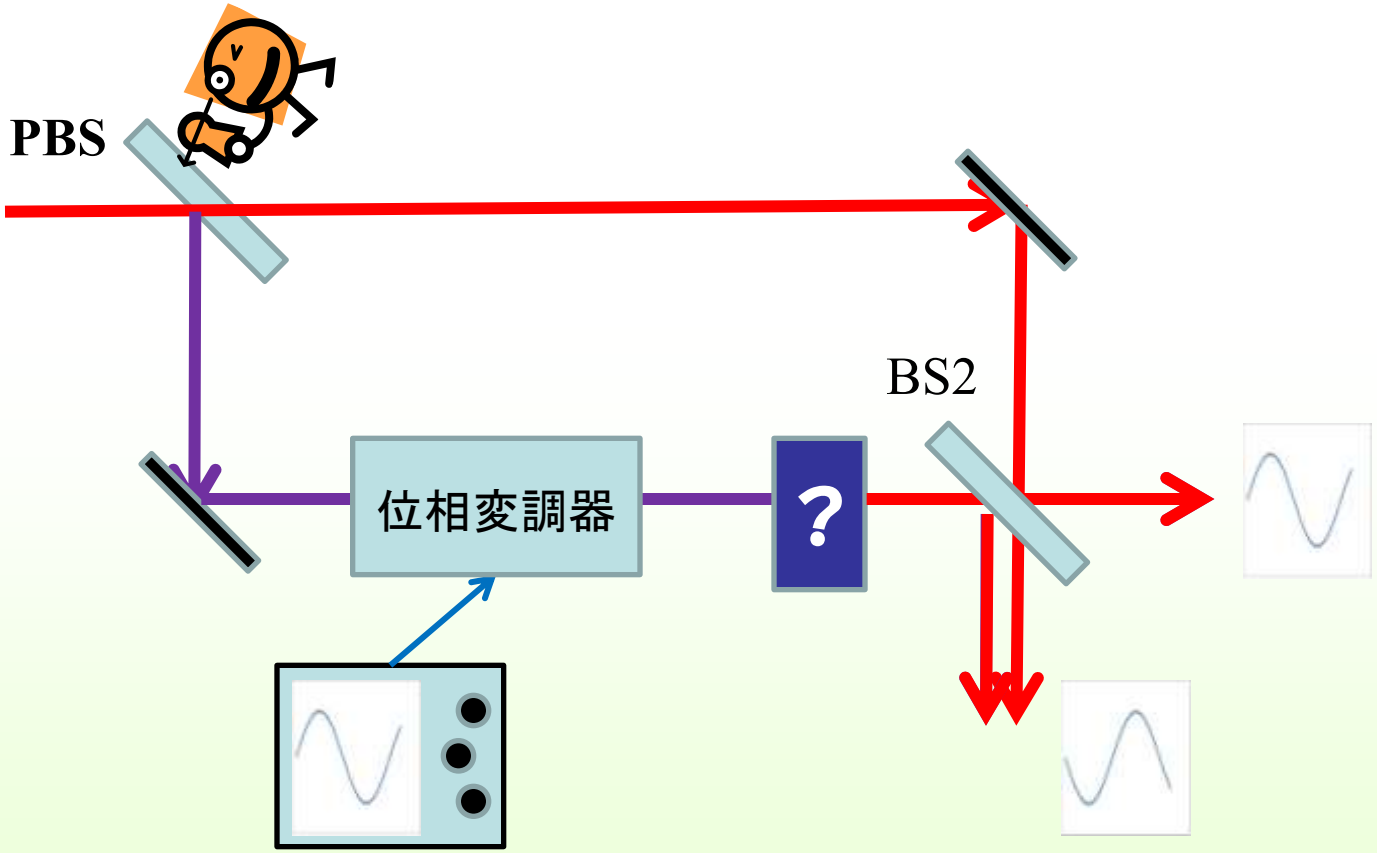
ベクトルで考えると



量子消しゴム（デモンストレーション）

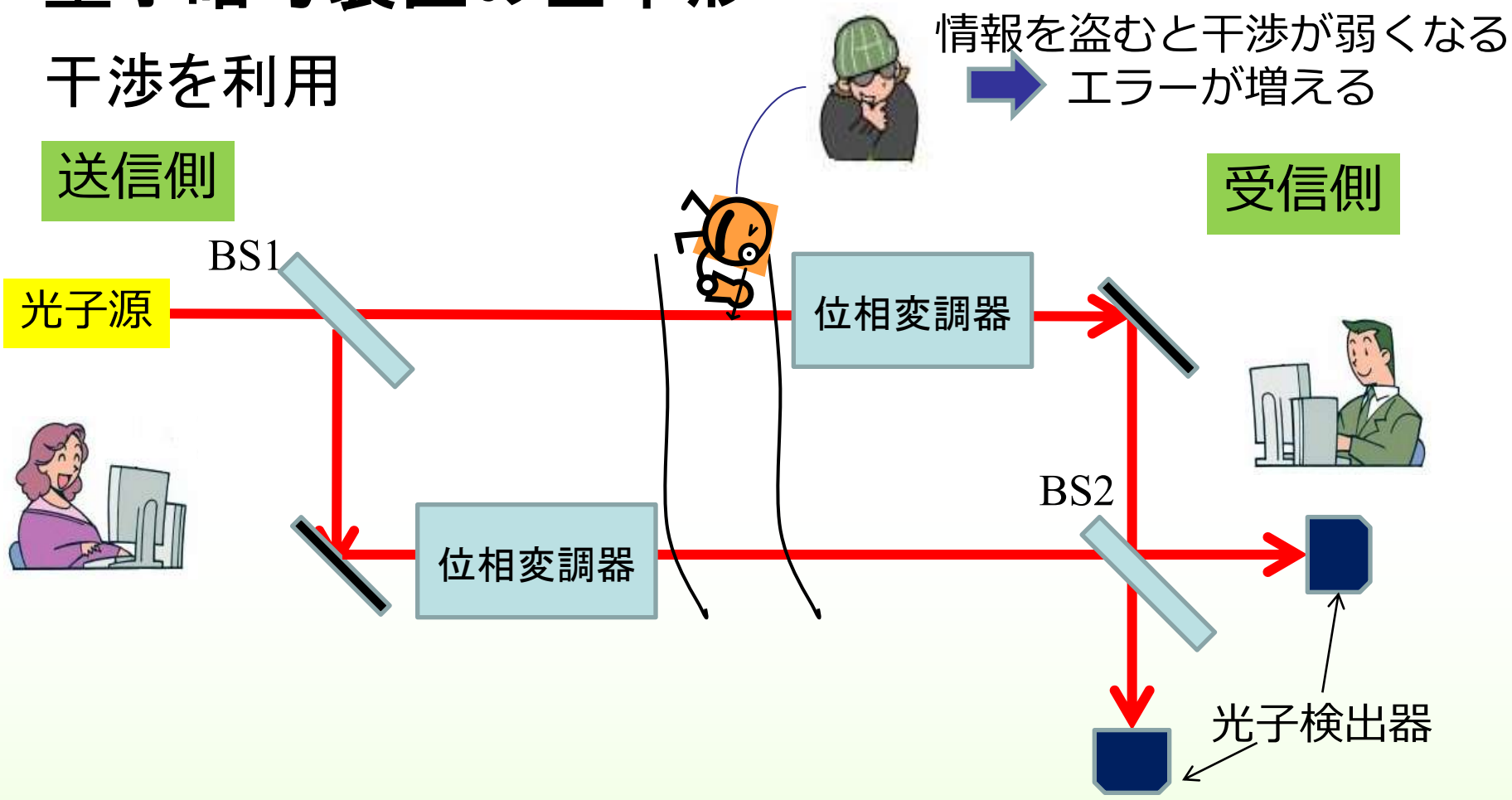
経路を調べる（＝情報を得る）と干渉が消える

では，情報を消すと？　干渉が戻るか



量子暗号装置の基本形

干渉を利用



送受信したビットの一部を照合してエラー率を求める
盗聴された情報量の上限が求められる ➡ 情報を消去（鍵蒸留）

鍵蒸留（秘匿性増強）

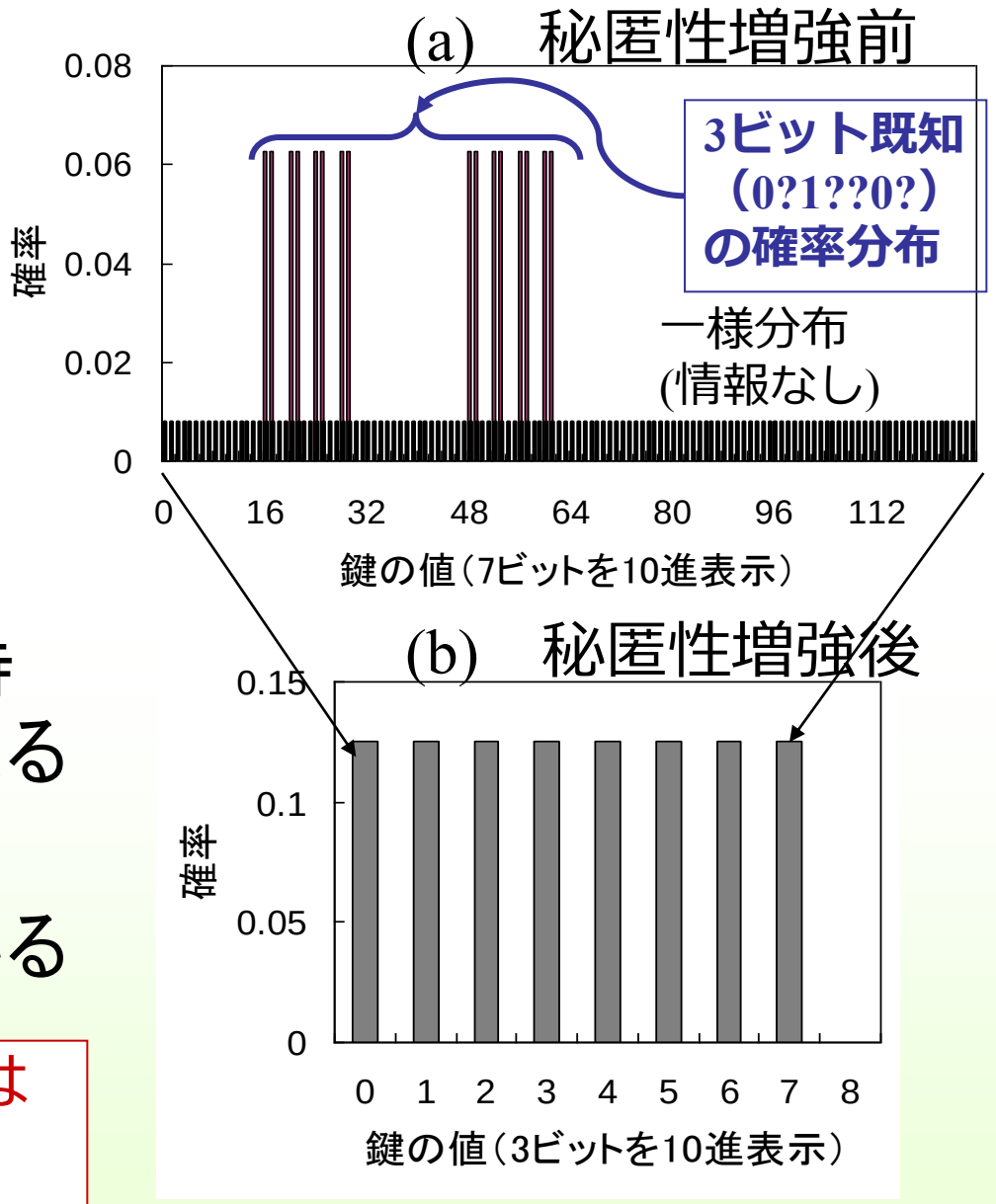
Nビットの鍵に対して，
盗聴情報量の上限Wが
わかっているとき

N-W-sビットの鍵を
ランダムに選び出す

最終鍵について盗聴者が持つ情報量を2^{-s}以下に抑えることができる

N-W-s<0　なら盗聴されている

盗聴情報量を見積れるのは
量子のおかげ



高速量子暗号装置

実際につくられている.

50kmファイバ伝送後1Mbpsの鍵生成能力
（テレビ電話を暗号化可能）

量子暗号装置全体

鍵蒸留基板

量子通信基板

NICTプロジェクトでNECが試作した量子暗号装置

東京QKDネットワーク

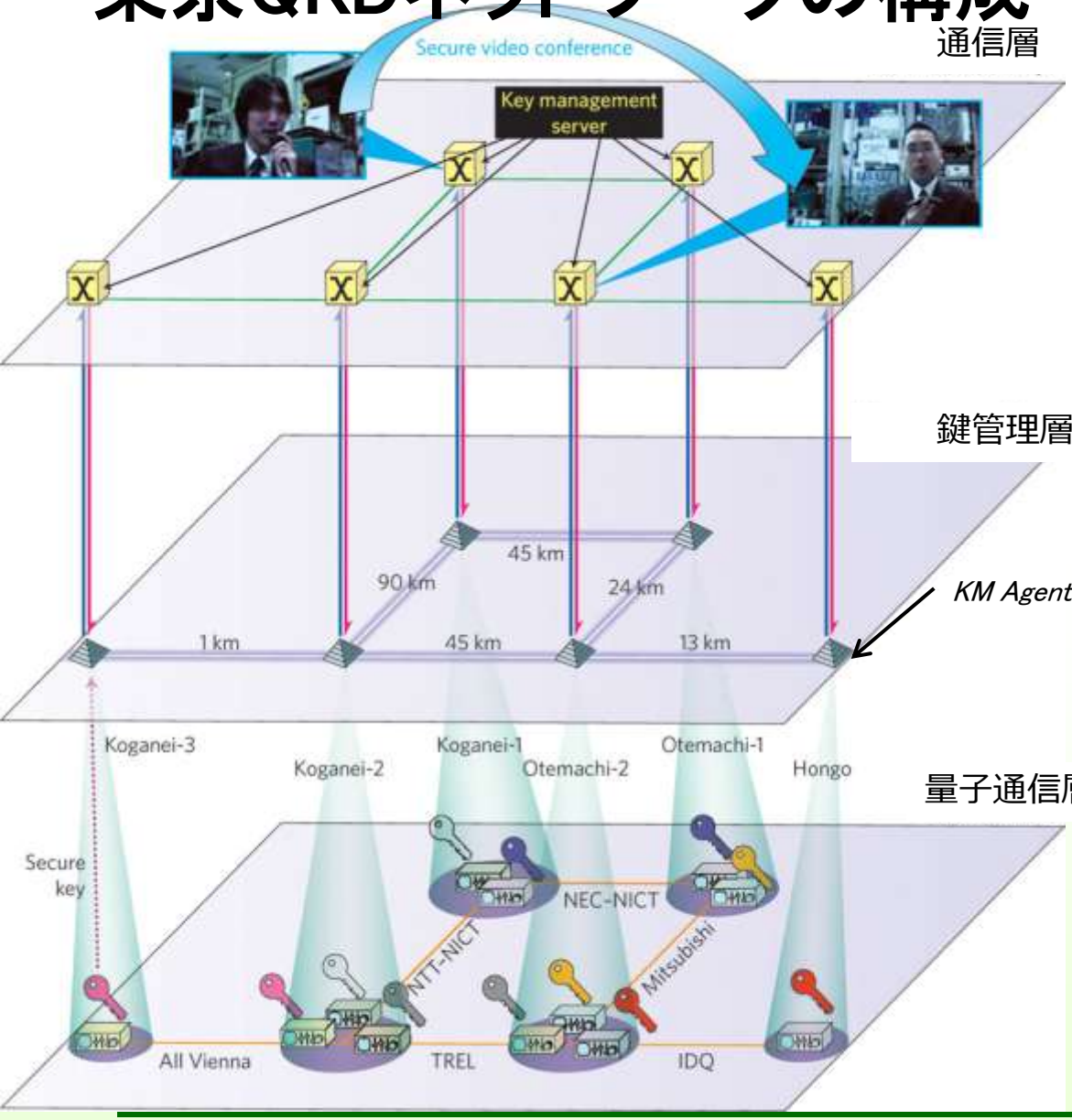
- 2010年10月18日稼働
- 日本初の量子暗号ネットワーク

  本郷ー大手町ー小金井を6つのリンクで結ぶ

  NICT, NEC, 三菱電機, NTTとヨーロッパ研究機関・企業（英, 瑞西, 墺太利）も参加
- テレビ会議のライブデモンストレーション（世界最高速の量子鍵生成）

  盗聴検知・経路変更
- 鍵管理・ネットワーク監視機能

東京QKDネットワークの構成



通信層

（アプリケーション）

secure communication with distributed key

鍵管理層

Monitor and Distribution of secure key

KM Agent and KM server

- KMA: collect-distribute-store
- KMS: monitor-supervise

量子通信層

key generation (point-to-point)

interface between Q-KM is designed to keep compatibility with SECOQC

量子暗号の実用化を阻む(？)もの

- **技術的な課題**
  - 現実の（不完全性を持つ）装置での安全性の保証
  - 伝送距離
  - 鍵生成速度
  - 鍵配付以外の機能
  - 値段・使いやすさ

- **社会的/心理的な課題**
  - 今の方法でいいじゃない
  - 標準化されてないと・・・
  - 「量子」なんて分かんないし，信用できない
  - 完璧な秘匿性が実現できると悪用されない？

量子暗号のこれから

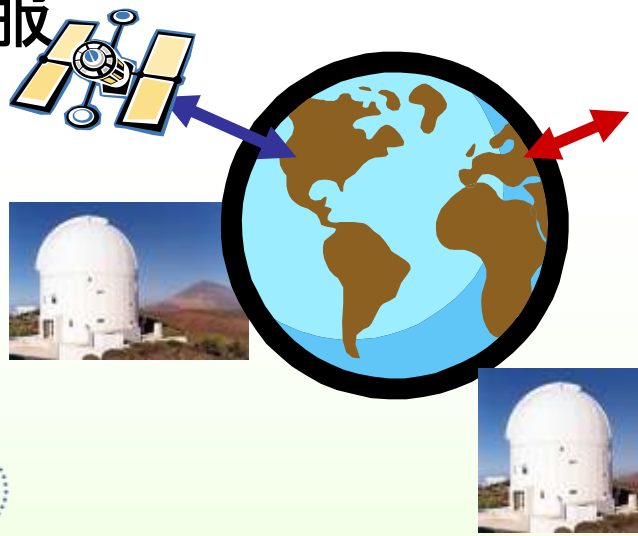
セキュアネットワークの実現＝実用化への課題解決

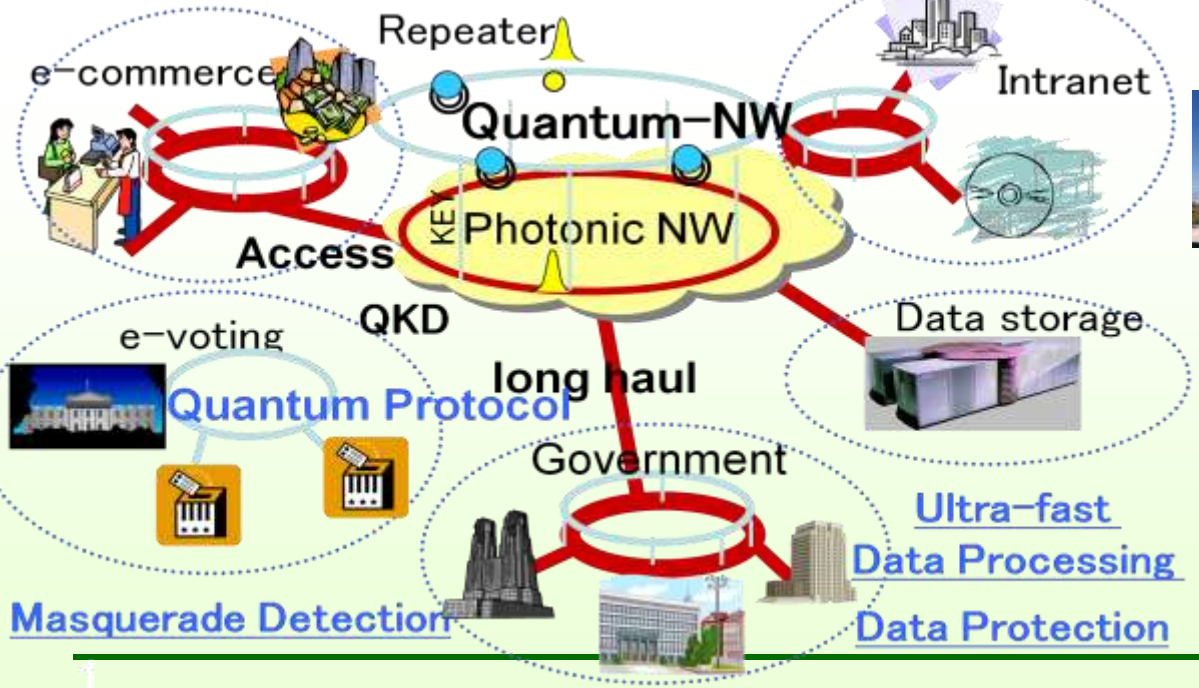
NICT　研究プロジェクトが始動 (2011～2016.3)

NEC, NTT, 三菱電機, 東芝,

北大, 東北大, 東工大, 国立情報学研究所

衛星利用量子暗号通信＝距離の克服





もっと量子の不思議

量子もつれ（エンタングルメント）

離れた場所にある原子が相関を持つ

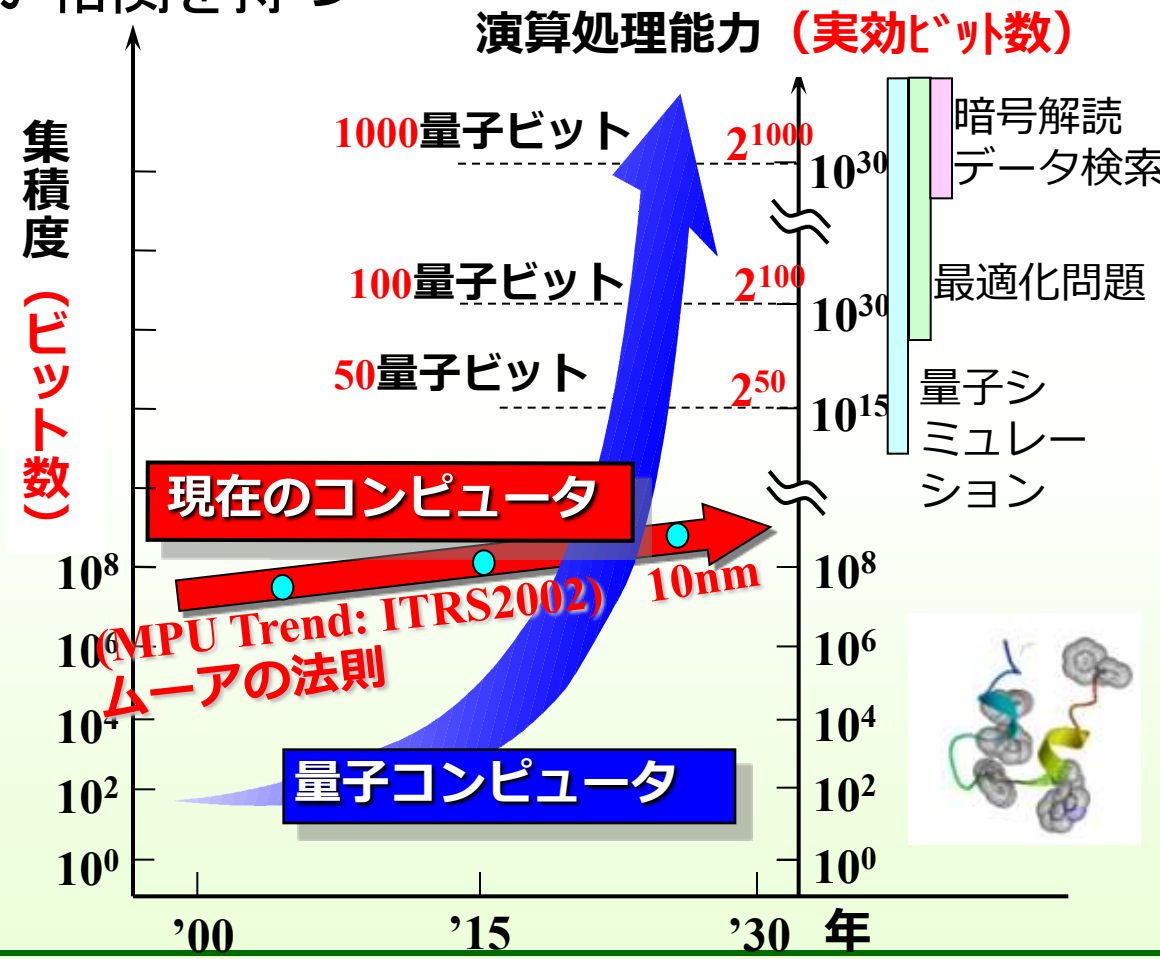
テレパシー？？

量子テレポーテーション

精密測定

そしてもちろん，

量子コンピュータ！



もっと知りたいひとは・・・

研究室（量子情報）HP

http://www.eng.hokudai.ac.jp/labo/hikari/qit/index.html

電子メール

tomita@ist.hokudai.ac.jp

研究室

情報科学研究科棟　5F （5-02室）

tel. (011)706-6521