量子暗号について

Yuta Hiemori, Haru Yoshida
College of Physics, University of Tsukuba

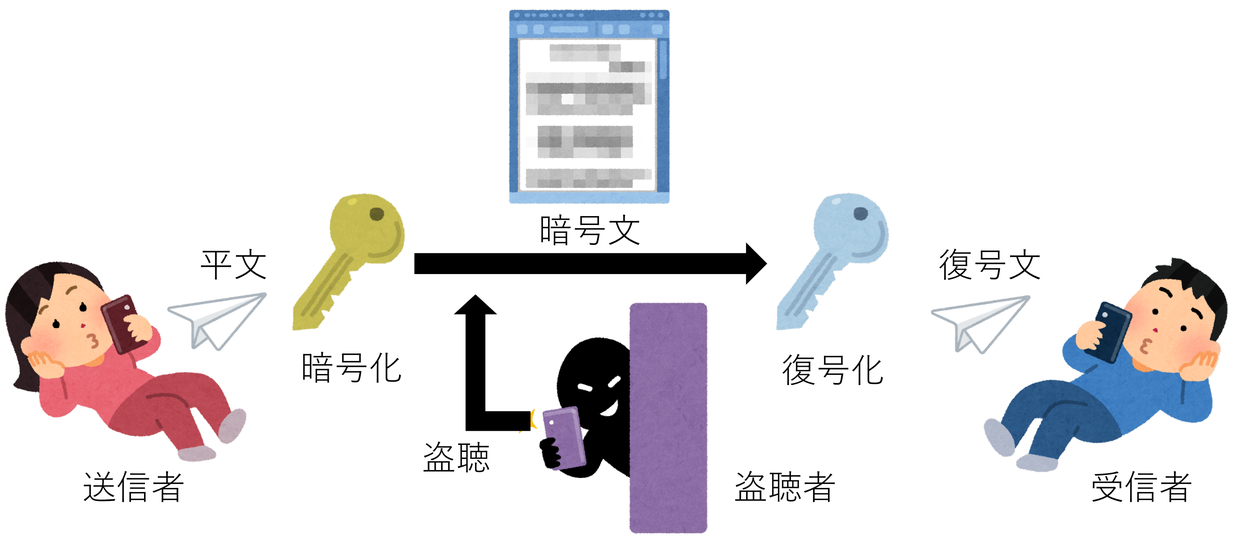
: 量子暗号とは何か理解するために最低限必要であると思われる箇所にこのクローバーのマークを添えてあります。ポスターをお読みになる際の参考としていただければ幸いです。

1. 暗号(Encryption) とは？

暗号 : 第3者に内容を見られることなく情報を伝達するために用いられる手法，またそのアルゴリズム。

用語の定義

- 平文　⇔　送りたい情報
- 暗号化 ⇔　第3者に分からないように平文を変換すること
- 暗号鍵 ⇔　暗号化に用いる特定の文字列
  （アルゴリズムに用いるナニカ。
  基本的には送信者と受信者で共有）
- 暗号文 ⇔　暗号化の施された平文
- 復号　⇔　暗号文を平文に直すこと



一般的な古典暗号の特徴

- 暗号化アルゴリズムは公開する
  : アルゴリズムの安全性の検討が可能
- **鍵の秘匿性保持**
  : 暗号鍵がバレた場合，新しい鍵を用意し直す
  : 鍵の安全な配送の確立
  （Kerckhoffs の原理）

Auguste Kerckhoffs

2. 有名な現代古典暗号: Vernam 暗号

Vernam 暗号 : 送信者と受信者の間で共通の鍵(乱数)を用意し，その鍵を用いて符号化した平文の排他的論理和を取ることで暗号化＆復号する。ただし，共通の鍵は他者には秘密にしなければならない（秘密鍵）。

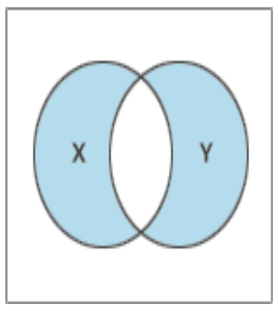
例 : 平文 : 110100　共通鍵 : 100101

1. 送る文と共通鍵の排他的論理和をとったものである暗号010001を送る。

2. 受信者は送られてきた暗号と共通鍵の排他的論理和をとって復号する。

排他的論理和の真理値表とベン図

X	Y	結果
0	0	0
0	1	1
1	0	1
1	1	0



➡ 平文 110100 が再び出てくる！

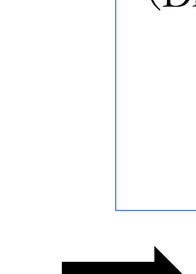
問題点 :

1. 共通の鍵を秘密に送ったりできるならば，
   最初からそのルートで送りたい文を送ればいいのでは？

2. 毎回共通鍵を変える必要があり，
   ランダムに決められなければならない。

3. 量子力学における測定(Measurement)

測定 (Measurement) :
量子力学を述べる上で欠かすことのできない重要な概念。
量子暗号においてもこの特性が重要な結果をもたらす



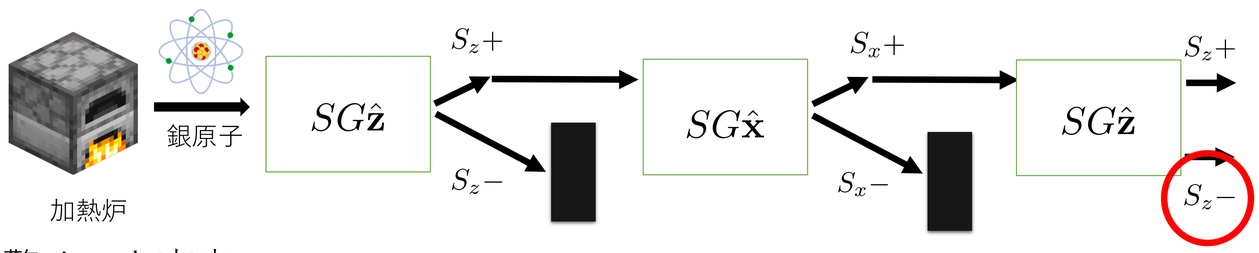
P.A.M Dirac

P.A.M Dirac

「測定された系はある1つの固有状態に確率的に飛び移る」

…ドウイウコト？

Stern–Gerlach の実験



驚くべき事実：
第1の装置で z 軸負方向のスピンの粒子を除いたにも関わらず，
第3の装置から出てきた粒子線には Sz ± 成分の両方が含まれている（!?）

（Dirac のことばに基づいて）与えられる解釈 :
**装置は「ある軸方向の測定」に対応し，
重ね合わせ状態にある粒子線は測定によって
その物理量の固有状態のいずれかへ
確率的に“飛び移る”！**

➡ この解釈によって，Stern–Gerlach の実験が説明可能！

第1の装置が「z 軸方向のスピンの測定」に対応。粒子線はこの物理量の固有状態z+ スピンと z- スピンの重ね合わせ状態にあって，この測定を受けることにより 1/2 の確率で z+ スピンと z- スピンの成分を持つ固有状態のいずれかに”飛び移る”んだ！

第2の装置では「x 軸方向のスピンの測定」を受け，x+ スピンと x- スピンの固有状態の重ね合わせで表されるz+のスピン状態の粒子線 は，1/2 の確率で x+ スピンと x- スピンの成分を持ついずれかの固有状態に”飛び移り”，装置から出てくるのよ。

第2の装置で「x 軸方向の測定」がされたことによって，z+ 固有状態は x+，x- 固有状態のいずれかに確率的に遷移して，z 軸方向に関する以前の情報は完全に無くなってしまったんだ！

第3の装置に飛び込む x+ 成分を持つ固有状態にある粒子線はz+，z- 固有状態の重ね合わせ状態。「z 軸方向の測定」を受けることで z+，z- 固有状態のいずれかに1/2の確率で遷移する。そのために，第3の装置では2つの成分が両方とも含まれているということになるのね。

…つまり量子力学における**測定**とは：

ある量子系に対し物理量の理想測定を行うと，その量子系はその物理量の固有状態のいずれかに確率的に”飛び移る”。
測定は一般に元の状態を保つとは限らない。
（測定をやり直すことはできない！）

「量子力学における測定」の理解を助けるもう一つの例として，放射線検出器（ラドン検出器）の実物を展示させていただいております。よろしければ是非そちらもご覧くださいませ。

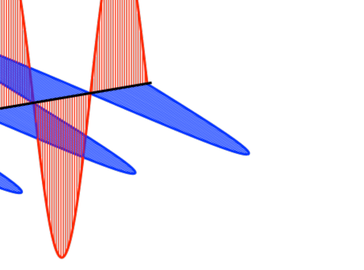
4. 量子鍵配送方式 : BB84 (Bennett Brassard 1984)

量子暗号(量子鍵配送方式):

- 暗号化に用いる暗号鍵を，量子力学を用いて配送する方式，そのアルゴリズム。
- 暗号化するために必要な鍵(乱数)を安全に送ることが目的であり，平文の暗号化およびその送受信が目的ではない。
- 鍵が安全に共有できれば，それを用いて既存の古典暗号で安全な通信が可能。

BB84 :

Charles Bennett と Gilles Brassard によって1984年に提案された、量子通信を利用する世界初の鍵配送プロトコル。



BB84 で用いるもの

1. 弱パルス光出力装置

・暗号鍵(乱数)をどう運搬？

➡ 光パルス

光を弱めていくと量子的な性質が出現！
エネルギー量子 $E = h\nu$ を光子1個あたりの単位として，1パルスあたり１つの光子が存在するようなパルスレーザーを光ファイバで送信する。

・光で符号 0, 1 をどう表現？

➡ 光の**“偏光の向き“** で定める。

光の偏光

光 :
電磁場を媒質として伝わる，横波の電磁波。
電場成分，磁場成分が互いに直交しつつ進行方向に対して垂直に振動。

http://physics.thick.jp/Experimental_Physics/Section1/1-4.html

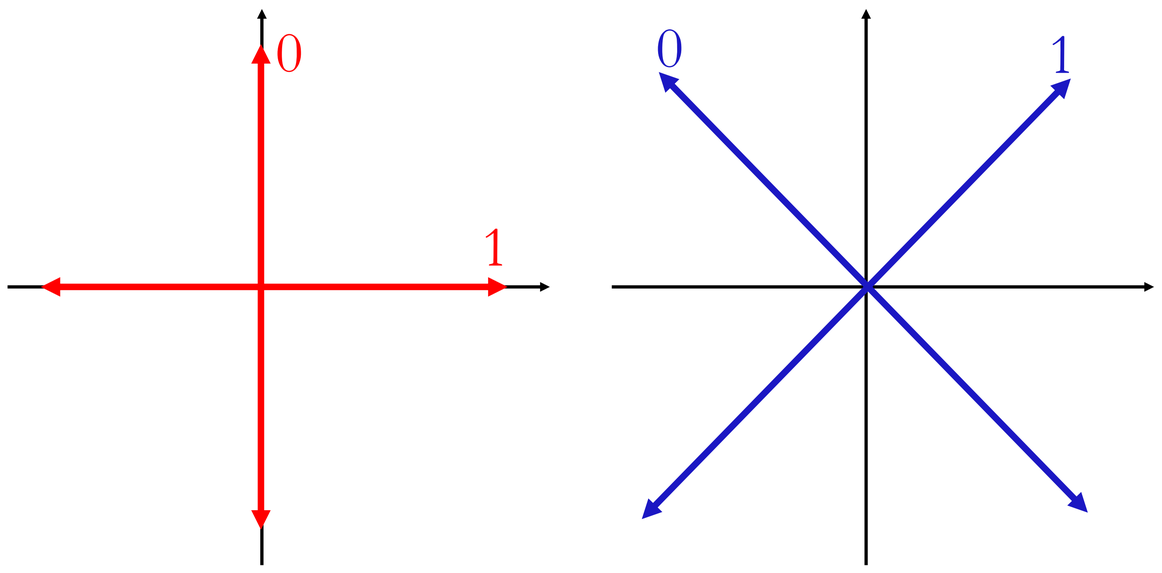
偏光 (Polarization) :
電場および磁場が特定の方向にのみ振動する光。

直線偏光
電場（および磁場）の振動方向が一定な偏光。

円偏光
電場（および磁場）の振動が伝播に伴って円を描く偏光。
右円偏光と左円偏光がある。

自然光など普通の光は無偏光。
光を偏光板(実物あります！)に通すと，偏光させることが可能。

進行方向を軸に 0°， 90° (45°, 135°)方向に電場が振動する光パルスに符号1, 0をそれぞれ割り振り，前者を A基底，後者を B基底 と呼ぶことにする；



任意の偏光状態は，A,Bいずれかの基底による**重ね合わせ**状態として表すことが可能。

(量子力学における**重ね合わせ**について詳しくは，
ポスター「ざっくり量子コンピュータ」(松本)を参照)

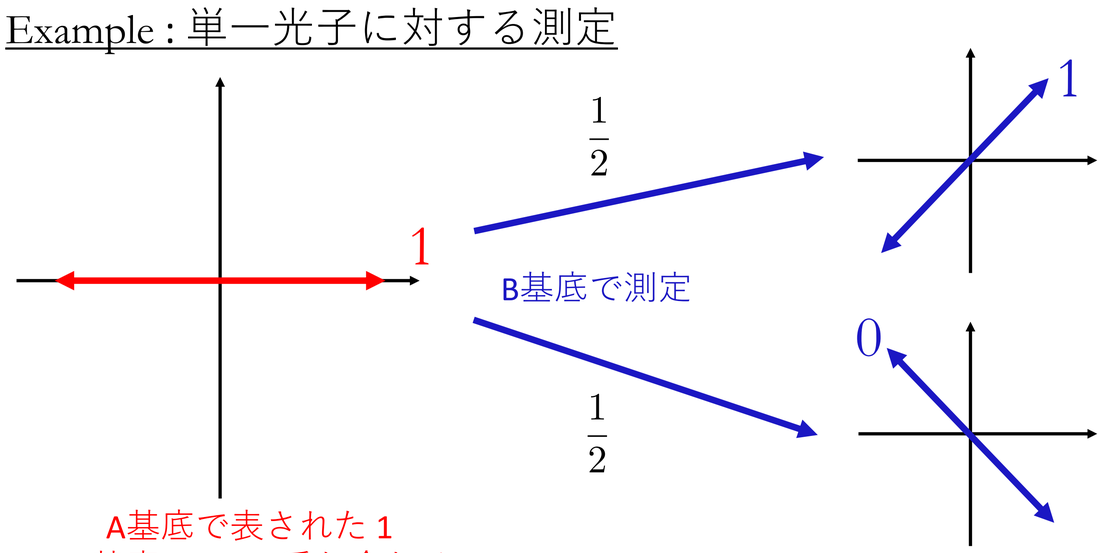
光を量子効果が現れる程度まで弱める

＋

スクランブルを行う

➡ ***盗聴行為の検出が可能！***

Example : 単一光子に対する測定



・別の基底で測定してしまった場合，
元の値に関わらず 0, 1 がランダムに得られる

・測定を行なった時点で光子の状態は変化しているので，
基底を変えて再度測定し直しても元の値を復元することは不可能

➡ 量子的性質のために測定によって同じ状態が保持できず，また測定をやり直すこともできない！

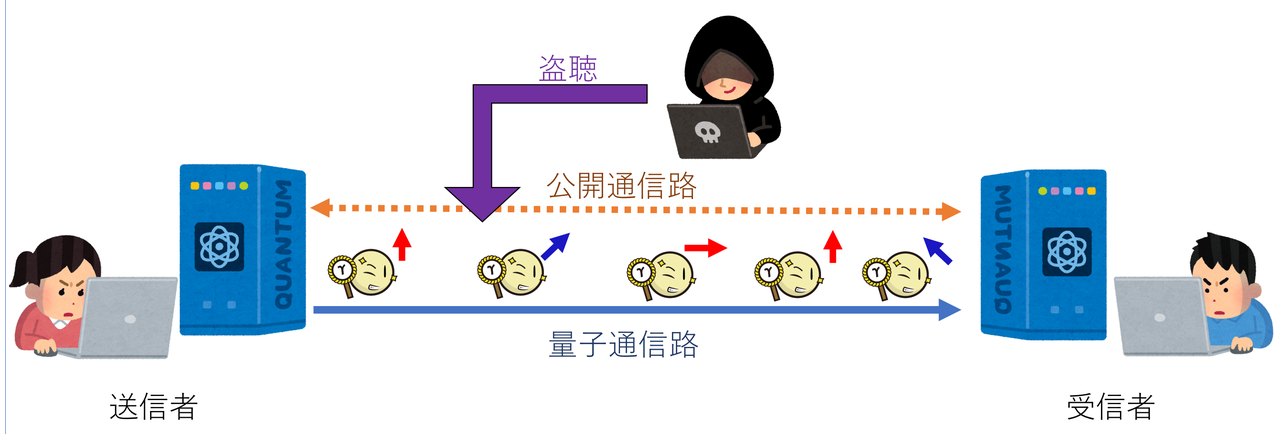
➡ **盗聴行為の定量的検出が原理的に可能**
（量子暗号の特筆すべき特徴！）

2. 量子通信路

乱数を光子に預けて送るための経路。
光ファイバがよく使われ，盗聴者はここに流れる光子を自由に盗聴可能。

3. 公開通信路

乱数本体ではなく，補助的な情報を送るための通路。
情報の伝達さえできれば何でもよく，インターネット(Twitter, LINE)や手紙，矢文でもよい。
盗聴者はこの経路を通る通信内容の傍受が可能だが，内容を書き換えることはできない（とする）。



Alice

送信者。乱数を生成し，個別の光パルスに A,B基底をランダムに選んで，量子通信路を通じて Bob へ送信する。

Bob

受信者。 Alice から送られてきた光パルスを，A,B基底のいずれかをランダムに選んで個々に測定する。

Eve

盗聴者。量子通信路を通る光パルスを自由に盗聴することができ，また公開通信路を渡って送受信される情報を傍受することもできる。
(通路や量子暗号装置におけるノイズもこれに包含。また，Eve は 最も単純な攻撃手法であるIntercept / Resend Attack をするものとする)

BB84 プロトコルの手順

(1) 量子通信:

1-1 Alice は乱数ビット列を生成して，各乱数ビットごとにA,B基底をランダムに選び，生成した光パルスを量子通信路を通じて Bob に送信。


Alice

Alice の作成した乱数ビット	1	1	1	0	0	1	0	0	1	0	1	1
Alice が選んだ偏光基底	B	A	A	B	A	B	A	A	A	B	B	A
偏光の向き	↗	→	→	↖	↑	↗	↑	↑	→	↖	↗	→

1-2 Bob は，A,B基底をパルスごとにランダムに選び，送られてきたパルスを測定する。

1-3 Bob の測定が全て終了したら，Alice と Bob は各光パルスに対してお互いが選択した基底全てを公開通信路を通じて公開。お互いの基底が一致したパルスの乱数ビットのみを残して，これを **生鍵** (raw key)とする。一致していないものは破棄し，以後使わない。

Alice が作成したビット列	1	1	1	0	0	1	0	0	1	0	1	1	…
Alice が選んだ偏光基底	B	A	A	B	A	B	A	A	A	B	B	A	…
偏光の向き	↗	→	→	↖	↑	↗	↑	↑	→	↖	↗	→	…
Eve が選んだ偏光基底	B	A	B	A	A	A	A	B	A	A	B	A	…
偏光の向き	↗	→	↖	↑	↑	↑	↑	↖	→	→	↗	→	…
Bob が選んだ偏光基底	B	B	A	B	A	A	A	B	A	B	B	B	…
Bob が得られた偏光の向き	↗	↖	↖	↑	↑	↑	↑	↖	→	→	↗	↖	…
Bob が得られたビット列	1	0	0	0	0	0	0	0	1	1	1	0	…
生鍵	○		○	○	○		○		○	○	○		…

1-4 生鍵ビットのうち， A 基底で一致しているものをまとめて **ふるい鍵** (sifted key) と呼び，B 基底で一致しているものをまとめて **サンプルビット** と呼ぶことにする。

Alice が選んだ偏光基底	B	A	A	B	A	B	A	A	A	B	B	A	…
Bob が選んだ偏光基底	B	B	A	B	A	A	A	B	A	B	B	B	…
Alice が作成したビット列	1	1	1	0	0	1	0	0	1	0	1	1	…
Bob が得られたビット列	1	0	0	0	0	0	0	0	1	1	1	0	…
生鍵	○		○	○	○		○		○	○	○		…
Alice のふるい鍵			1		0		0		1				…
Bob のふるい鍵			0		0		0		1				…
Alice のサンプルビット	1			0						0	1		…
Bob のサンプルビット	1			0						1	1		…

(2) 誤り率の算出:

Alice と Bob は，お互いが得たサンプルビットを公開し，その誤り率 p を算出する。この誤り率が高すぎる場合，プロトコルを中止して最初からやり直す。（**ここで盗聴検出が可能！**）

(3) 誤り訂正，秘匿性増強処理

3-1 Alice，Bob が持つふるい鍵の誤りをパリティチェックで訂正する。

パリティチェック

パリティチェック : ビット列を等分割し，公開通信路を用いて各ブロックごとにお互いのパリティ値を二分木探索で比較していき，最終的に誤りのあるビットを修正（除去）するアルゴリズム。

この訂正処理されたふるい鍵を，**訂正鍵** と呼ぶ。

3-2 訂正鍵に秘匿性増強処理を行い，**秘密鍵** を得る。

秘匿性増強処理 : 得られた訂正鍵を絶対強固なものとするために行われる処理を指し，ハッシュ関数を用いた操作がよく用いられる。

Hash 関数

暗号学的 Hash 関数　$\mathrm{hash}(\cdot)$

入力された任意の長さの文字列（メッセージ）に対して，固定長の文字列（ハッシュ値）を出力する関数。

- **原像計算困難性**

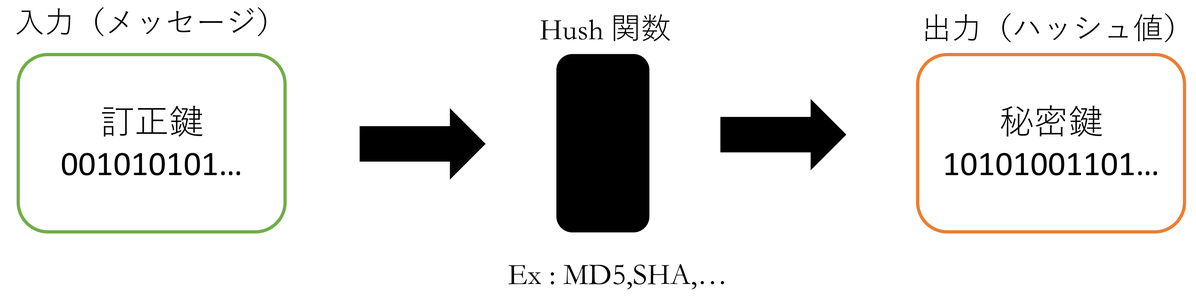
  ハッシュ値 h に対して，$h = \mathrm{hash}(m)$ となるメッセージ m を探すことが困難。

- **第2原像計算困難性（弱衝突耐性）**

  入力m_1が与えられ，$\mathrm{hash}(m_1) = \mathrm{hash}(m_2)$ となる$m_2(\neq m_1)$を探すことが困難。

- **強衝突耐性**

  $\mathrm{hash}(m_1) = \mathrm{hash}(m_2)$ となるような2つのメッセージ m_1 ,m_2を見つけ出すことが困難。



Alice は，どの Hush 関数を使うかを公開通信路を通じて Bob に伝達し，訂正鍵を Hush 関数に通して，秘密鍵を得る。

→ ***ワンタイムパッドとして使うことで絶対安全な秘密通信が達成！***

5. 量子暗号と古典暗号

…結局，量子暗号の何がすごいの？

① 盗聴検出が可能

秘密鍵運搬の際に量子的性質を持つ弱光パルスを符号に使用

量子力学における unique な性質「測定」から，

- **盗聴者の存在の推定**
- **盗聴のリアルタイム検出**

古典暗号では不可能であったことを可能に！

② 絶対的な安全性

暗号における「安全性」には，主に 2 つの観点が存在 :

- 計算量的安全性 : 暗号を解読するアルゴリズムの計算量に着目した暗号の安全性を表す指標。ある暗号を解読するためのアルゴリズムの計算量が，多項式時間$O(n^k)$ に収まらないような場合における安全性。

古典暗号の多くは，この計算量的安全性によって安全性が担保。

しかし
- 解読アルゴリズムの発見
- 計算機の演算能力向上

} 安全が破られてしまう危険性…

- 情報理論的安全性 : 暗号に対する攻撃に対する強度に着目した暗号の安全性を表す指標。ある暗号について，攻撃者の計算能力に依存しない秘匿性が証明できるような安全性。

量子暗号は，**自然の物理法則によって情報理論的安全性が証明！**

- **物理法則が正しい限り，確実にリアルタイム盗聴検出が可能**
- **安全性は計算機の進歩とは原理的に無縁で，いくら高性能な計算機を用いても解読されることは決してない**

参考文献など

[1] 量子情報と時空の物理 第2版，堀田昌寛(2019)
[2] かわいいフリー素材集 いらすとや
https://www.irasutoya.com
[3] HiggsTan
http://higgstan.com/particle-image/