令和４年７月７日

自然法則に裏打ちされた実用的乱数実現へ

―日々の買い物もより安全に―

鶴丸豊広　　三菱電機株式会社 情報技術総合研究所
佐々木寿彦　東京大学大学院 工学系研究科 物理工学専攻
筒井 泉　　高エネルギー加速器研究機構 素粒子原子核研究所

講演内容

I. はじめに：量子性とパリティ対称性 …… 10分

今回の研究の核心となる２つの物理的性質　　筒井 泉

II. 今回の研究とその成果…… 30分

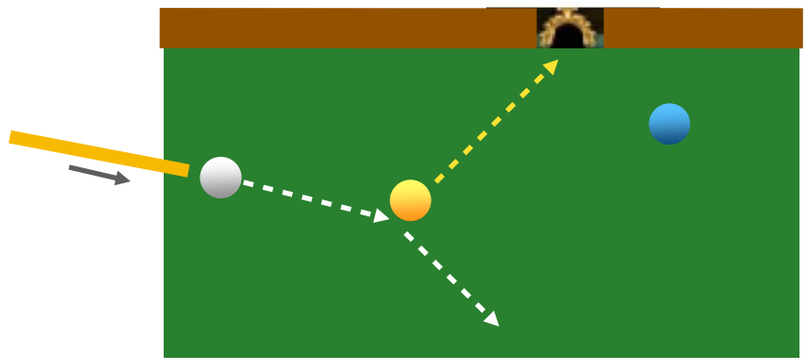
乱数とその生成方法、放射線乱数の安全性とその証明　　佐々木寿彦

I. はじめに：量子性とパリティ対称性

量子物理の世界と古典物理の世界の決定的な違い

- 古典物理（我々に身近なマクロな世界）

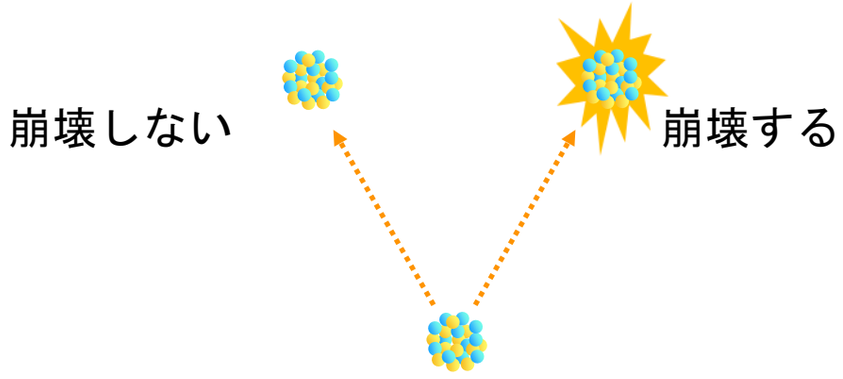
→ 原因（初期状態）から結果が一意に定まる: 決定論的



ビリヤード球の運動

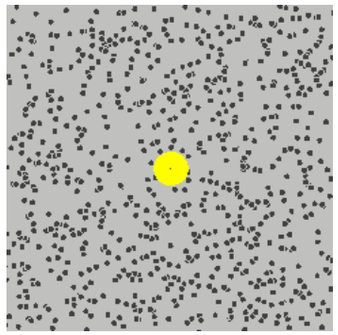
- 量子物理（素粒子や原子などのミクロな世界）

→ 原因（初期状態）は同じでも結果は一意に定まらず、どれになるかはランダムに決まる: 確率的



量子現象のランダム性は本質的（原理的）

古典的な（マクロの）現象でも、気体分子の運動や熱雑音など、一見、確率的に見えるものがあるが、それらは実際上、原因（初期状態）を厳密に決められないことによるものであり、本質的（原理的）なものではない



ブラウン運動：古典的な（擬似）ランダム性

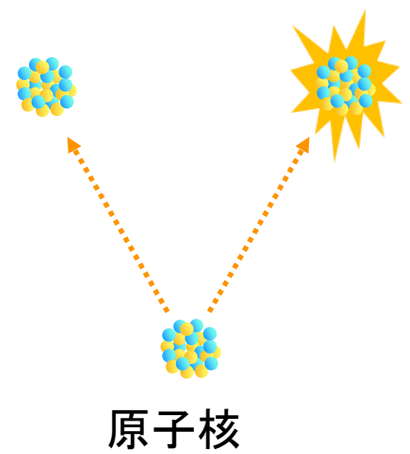
http://weelookang.blogspot.com/2010/06/ejs-open-source-brownian-motion-gas.html

一方、量子現象のランダム性が本質的なものであることは、想定される決定因子の存在が検証実験（ベル不等式の検証）により否定されていることから実証

量子現象にはそれを確定させる原因が存在しない

→本質的にランダム

原子核は崩壊の有無を定める決定要素（情報）を持たない →



原子核

素粒子・原子核を支配する原理的な対称性

- ローレンツ対称性（時空の回転や並行移動の下での対称性）

  エネルギーや運動量の保存、角運動量保存はこの対称性の結果

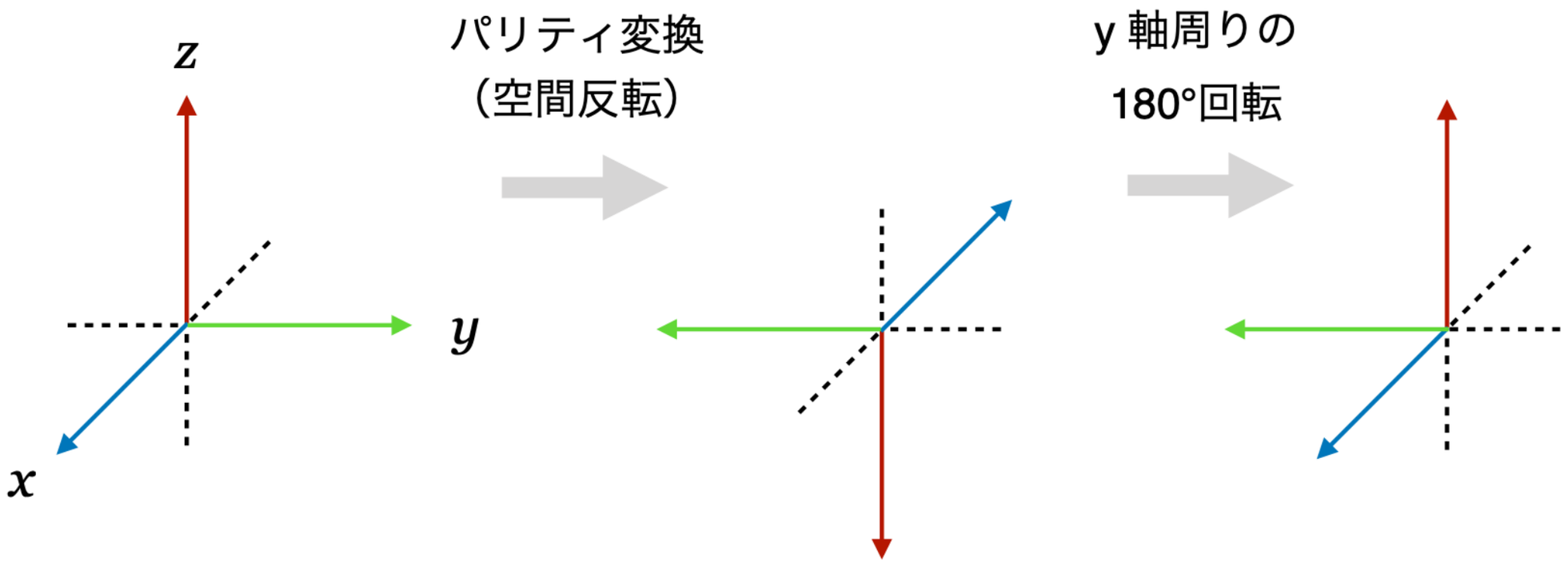
- CPT対称性（CPT変換の組み合わせの下での対称性）

荷電共役	パリティ	時間反転
粒子・反粒子の入れ替え	空間反転（鏡映）	時間の向きの反転

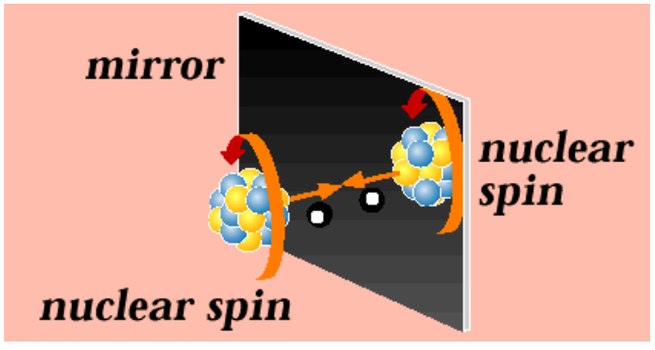
これらの変換の下で自然界の物理現象を支配する４つの基本的な相互作用（電磁力、強い力、弱い力、重力）は不変

→ 自然界の物理現象を規定する最も基本的な性質

パリティ対称性



パリティ変換は回転と組み合わせると鏡に映した鏡映の変換になる



https://www2.lbl.gov/abc/ wallchart/guide.html

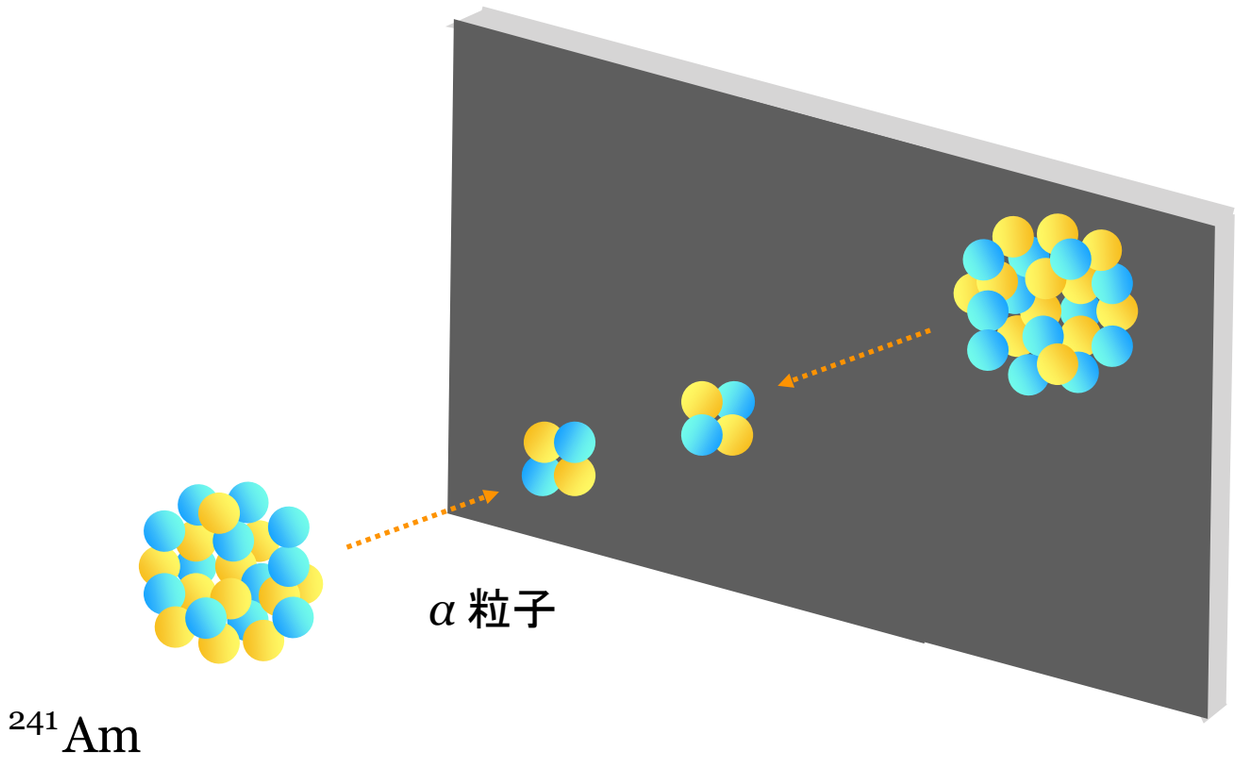
鏡映ペアの現象の起こる確率に差異

原子核の崩壊現象のうち、弱い相互作用が支配するベータ崩壊（電子とニュートリノを放出して別の原子核に変わる現象）ではパリティ対称性が破れている

（理論的に予言したLeeとYangにノーベル賞：1957）

パリティ対称性

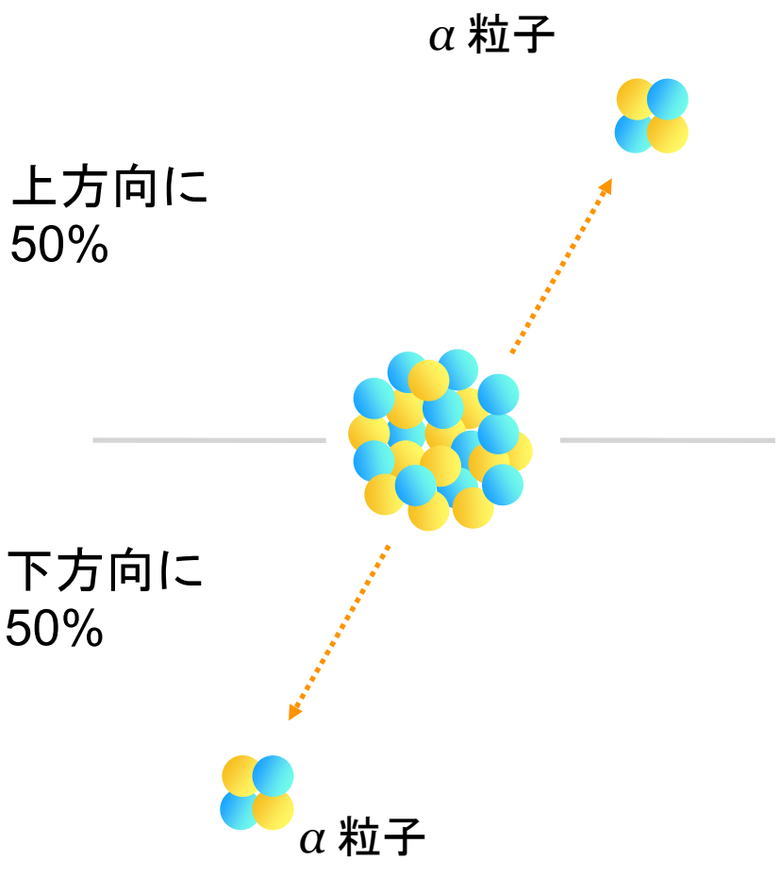
一方、強い相互作用（と電磁相互作用）が支配するアルファ崩壊（ヘリウム原子核を放出して別の原子核に変化する現象）ではパリティ対称性が保たれている（基本的相互作用の性質）



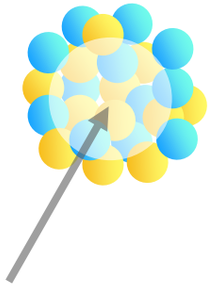
鏡映ペアの現象の確率は等しい

パリティ対称性

パリティ対称性 → ヘリウム原子核（α 粒子）は、上下（又は左右など）方向に等しい確率で放出



核崩壊は量子現象なので、どちらの方向に放出されるかは本質的にランダムで予め決まっていない



崩壊前の原子核の内部には、α 粒子の放出方向の決定要素（情報）は存在しない

→ 乱数生成に用いた際の安全性

自然法則に裏打ちされた
実用的乱数実現へ
―日々の買い物もより安全に―

鶴丸豊広[1], 佐々木寿彦[2], 筒井泉[3]

1: 三菱電機株式会社 情報技術総合研究所

2:東京大学大学院工学系研究科物理工学専攻

3:高エネルギー加速器研究機構（KEK） 素粒子原子核研究所

概要

- 背景: 乱数について
- 放射線乱数生成器について
- 放射線乱数生成器の安全性について
- まとめ

乱数について

- 乱数とは直感的には、ランダムな数字の列のこと。
  - 例: 01101010001011101111111...
- 乱数の応用先
  - あらゆる暗号アルゴリズムに不可欠
    - CPUに乱数源が標準装備されている
    - 例: ネットショッピングにおける、通信の暗号化や認証の実行に利用される
  - 数値計算(確率的アルゴリズム)にも使う
    - 例: モンテカルロ法による積分計算

乱数が問題になることはあるのか？

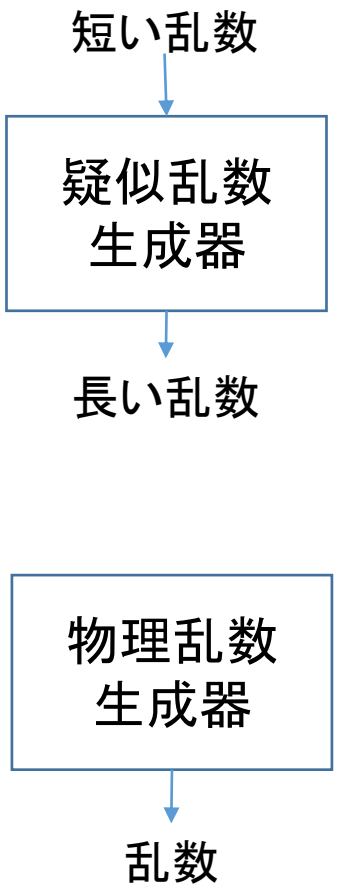
- 暗号アルゴリズムにおいては
  - 予測可能な乱数だと、暗号が解読可能になってしまう
- 数値計算(確率的アルゴリズム)に使う
  - 乱数が特定の周期性をもっていたりすると、本来であればほとんど出現しないはずの誤った結果が高い確率で出力されるようになる

乱数生成器
(Random Number Generator, RNG)

- 乱数生成器(RNG) ＝「（決められた範囲の）数 r を繰り返し出力する装置」
  - 例: 乱数 r は長さnのビット列($r \in \{0,1\}^n$)で, 各値は確率2^{-n}で起こる
- RNGの達成すべき性質:
  - ランダム性: rはどれも同じ確率で出現する
  - (暗号用途なら)秘匿性: rの値は所有者以外と相関がない

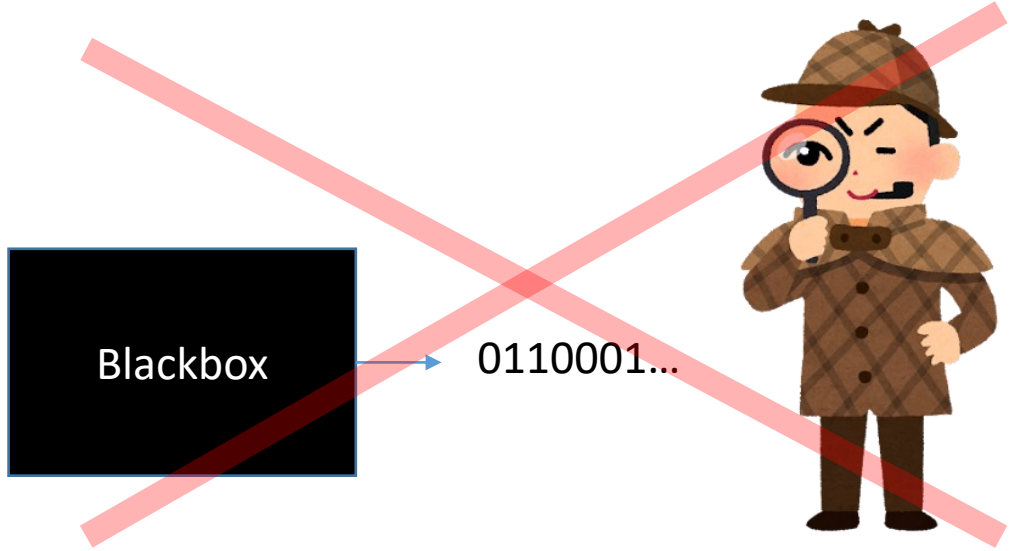
乱数生成器(RNG)の種類

- 世間ですでに使われている方式：
  - 疑似乱数生成器(PRNG)
    - 短い乱数（シード）をもとに，長い，一見乱数に見える数列を出力する乱数に見えるだけで，真の意味では乱数ではない
    - 例: メルセンヌ・ツイスタ、ChaCha20
  - (古典)物理乱数生成器
    - 実用的にはシードの生成に使うことが多い
    - 基本的に複雑だったり制御が難しい物理現象を使う
    - 例：電気抵抗の熱雑音によるもの、発振回路を用いるもの



乱数生成器(RNG)の課題

- RNGが良いものか出力を見るだけだと保証できない
- RNGの出力を見るテストの方法自体はある
  - 乱数テストに通らない -> 悪い乱数
  - 乱数テストに通った -> 悪いと断言できないが、良いかもわからない
    - 疑似乱数生成器でも乱数テストに通るように設計される



乱数生成器(RNG)の課題

- RNGが良いかは中身を見る必要がある
  - 古典物理の範囲内だと中身をみても原理的には判断が難しい
    - 因果律の世界(秘匿性の否定)
    - そもそも何を確認したらランダム性や秘匿性があるのかわからない
  - 実際上は、最初からランダム性や秘匿性が内在していると”仮定”してしまう。
    - 物理的性質から導出しているわけではない。
    - 物理的過程は出力値の範囲の増幅に使われるだけで、ランダム性や秘匿性を増幅しているわけではない。

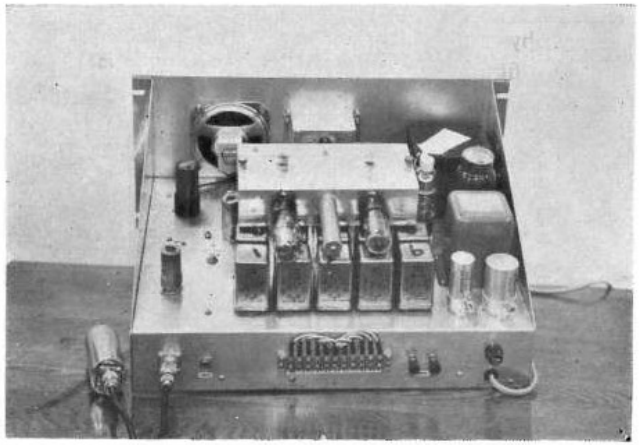
？？？

RNGの
中身

0110001…

量子乱数生成器

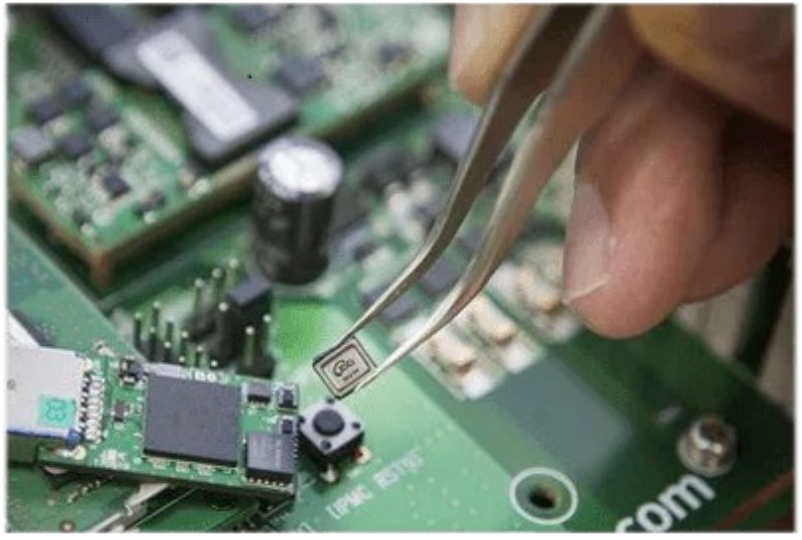
- 量子現象を使った乱数生成器
- 例
  - 光を使った量子乱数(1990年くらいからある)
    - (1光子レベルの)微弱光を使ったもの
    - 強い光を使ったもの
  - 放射線乱数(1950年くらいからある)
    - この1950年くらいというのは日本人の仕事(Isida, Ikeda (1956))
    - 放射線の検出を信号とする
  - 量子情報で扱われる系なら大抵乱数生成に使える。

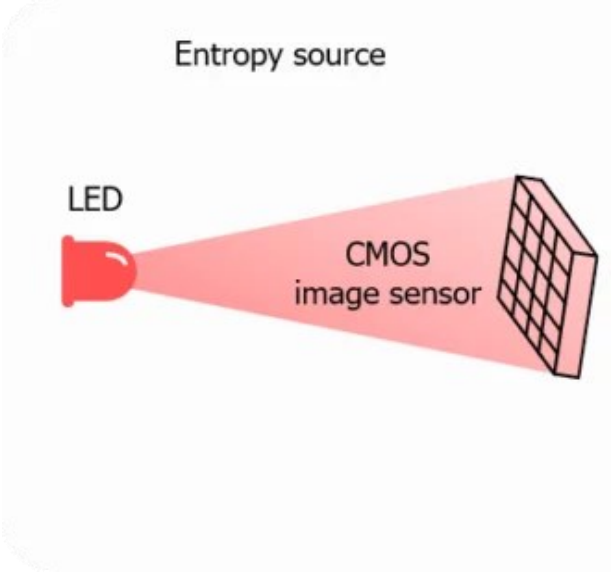


The back view of R–N generator and G-M tube (the left side)

Isida, Ikeda, Proceedings of the Institude of Statistical Mathematics **4**, 119 (1956)

(強い)光を使う乱数生成器の例





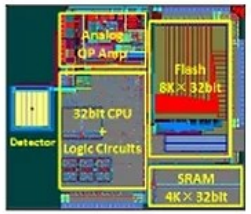
ID Quantique社製
Quantis QRNG Chip
Quantis QRNG PCIe & USB Legacy

韓国製スマートフォンで搭載モデルが発売された。（2020年5月）

Model	IDQ250C2	IDQ6MC1	IDQ20MC1
QRNG CORE			
Compliant to the Standard NIST 800-90A/B/C	✓ (B)	✓	✓
Certified AEC-Q100		✓	
Size	2.5 x 2.5 x 0.84 mm	4.2 x 5 x 1.1 mm	4.2 x 5 x 1.1 mm
RNG Data Output	N/A	1.47 Mbps (@ SPI Interface)	4.90 Mbps
Quantum Entropy Source	250 Kbps (typical)	5.88 Mbps (@ SPI Interface)	19.64 Mbps

https://www.idquantique.com/random-number-generation/products/

放射線乱数生成器の例

	QNT100	QNT500	QNT1000
写真/チップレイアウト			
機　能	ランダムパルス発生器	ランダムパルス発生器	真正乱数生成器
電源電圧	4.5～5.5V	2.7～3.6V	2.7～3.6V
乱数生成速度	10～80cps	10～80cps	2.56kbps（typ）
消費電流	12mA	1.8mA	TBD
動作温度範囲	−40℃～+85℃	−40℃～+85℃	−40℃～+85℃
チップサイズ	― ―	1.15x1.34mm	3.68x3.04mm
パッケージサイズ	5.0x5.0x1.4mm（4端子）	5.0x5.0x1.4mm（4端子）	7.0x7.0x0.76mm（QFN48）
特　長	情報機器に組込んで乱数や識別符号の生成などへの応用ができます。宇宙空間や車載用途などの過酷な環境での利用も可能です	QNT100のアルファ粒子検出器と パルス出力回路を集積化したワンチップICです	ランダムパルス発生器とCPU、Flashメモリを集積したLSIで認証、ID管理、暗号 鍵作成などの高度なセキュリ ティ管理に応用できます

Quantaglion社製
QNT Series

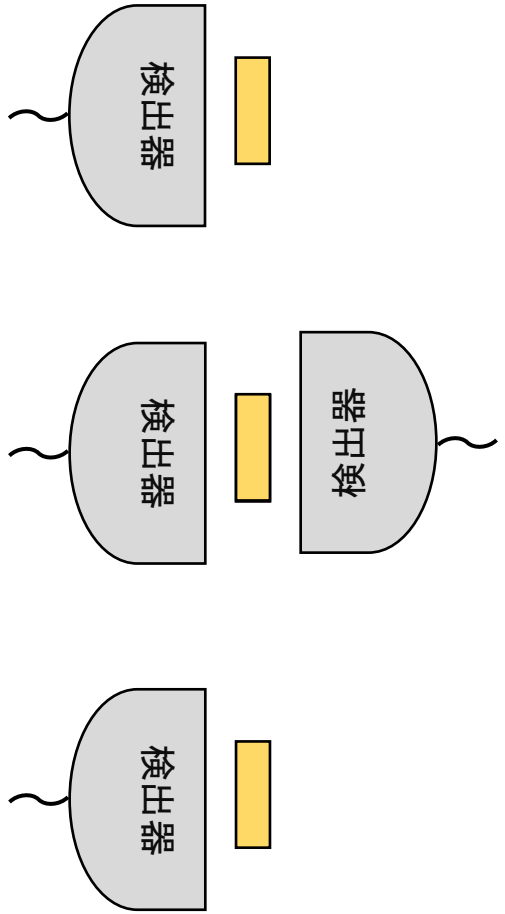
https://www.quantaglion.com/application

量子乱数生成器の動機

- ランダム性や秘匿性を最初から仮定せずに、物理的性質から導出する
  - 量子乱数生成器すべてがそうではない(むしろ少数派)
  - 安全性(ランダム性+秘匿性)は ε-security という共通基準が存在する
- 量子論でなぜそれができるか
  - 直感: 実際の物理現象は古典物理的(決定論的)でないことを保証できる。
    - 例: Bell の不等式の破れの検証実験

放射線乱数生成器

- 旧来型I: 検出タイミング型
  - 原子核の崩壊が指数減衰するというモデル
  - 秘匿性は最初から仮定している。
- 旧来型II: 検出方向型
  - 放射線の放出方向がランダムであることを使う。
  - 検出器を複数使う。
  - 秘匿性は最初から仮定している。
- 今回の話
  - パリティ対称性のある放射線源を使う。
  - 基本構成だと検出器は1つ。
  - ランダム性と秘匿性は導出される。



放射線を使った乱数生成器

- 正規ユーザによる乱数生成:
  - ステップ1: 放射線源からくる放射線をN回検出し,
    検出のタイミング $\vec{i}$ を記録する.

正規ユーザ

時間枠	1	2	3	4	5	6
検出の有無	有	無	有	無	無	有

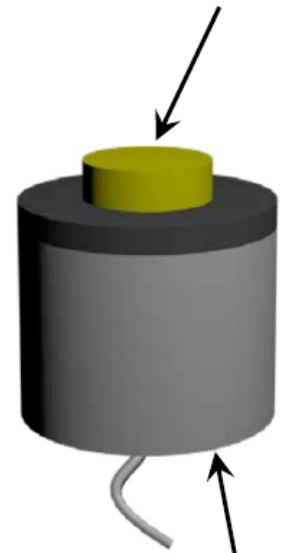
検出タイミング $\vec{i} = (1,\ 3,\ 6)$

  - ステップ2: 検出のタイミング $\vec{i}$ に乱数抽出 (ランダム行列演算)の
    操作を施し, 乱数 r を得る.

- 想定される脅威: 盗聴者が事前に放射線源に細工.
  (例:固定パターン, 量子もつれ)

盗聴者

放射線源
(盗聴者が細工できる)



検出器
(盗聴者が細工できない)

放射線RNGの安全性の根拠
＝ パリティ対称性（空間反転対称性）

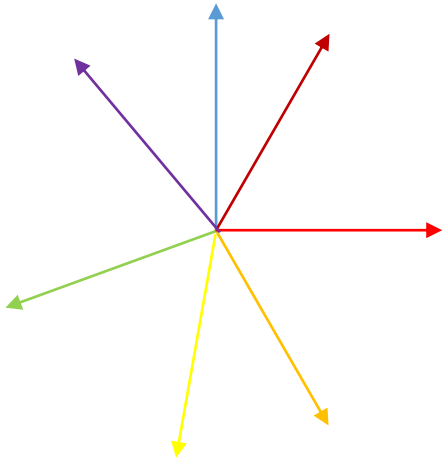
- 空間反転（パリティ変換）P
  ＝ 空間座標 x, y, z を，原点を中心にして反転する操作
  $$P\colon (x, y, z) \mapsto (-x, -y, -z)$$

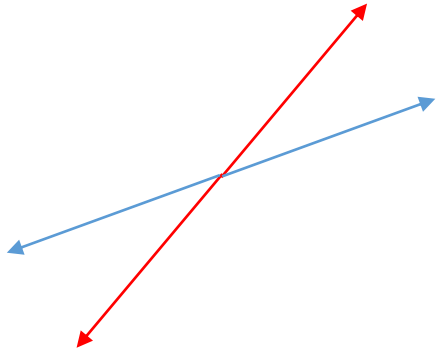
- ある種の核種の放射線は，パリティ変換Pのもとで不変である†
  - 例：アメリシウム(^{241}Am)から放出されるα線

†正確には：
- ある種の原子核崩壊で放出される放射線の量子状態が，パリティ不変である
- 例えば，α崩壊，γ崩壊はパリティ不変である（電磁相互作用，強い相互作用）
- 一方で，β崩壊はパリティ不変でない（弱い相互作用）

パリティ対称性

- パリティ対称かどうかは放射の分布だけを直接みてもわからない。
  - 左(パリティ対称ではない): それぞれの崩壊は方向が決まっているが、それぞれが別々の方向にいくために放射が球対称にみえる。
  - 右(パリティ対称): それぞれの崩壊の方向には偏りがあるが、それぞれの崩壊で反対向きにも同じ確率で飛んでいく。



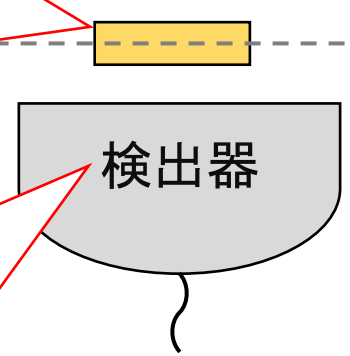


理想的な場合の安全性証明

- 基本アイディアを説明するために，理想的な状況を考える

放射線源：
- 各タイムビンで，粒子が必ず放出されるとは限らない
- 放出されても、1粒子とは限らない

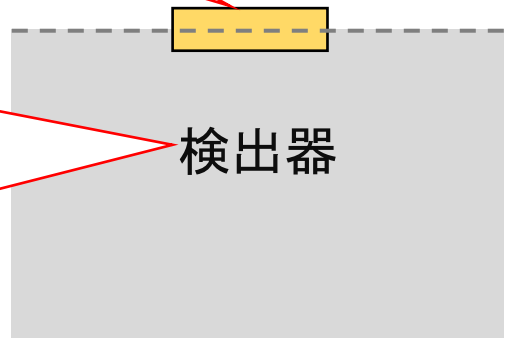
検出器：
- 検出効率は1でもないし方向によってばらつきもある
- 暗計数（誤検出）は存在する



理想化

放射線源：
- 各タイムビンで必ず1粒子を放出

検出器：
- 理想的な性能
  - 検出効率＝ 1
  - 暗計数（誤検出）＝ 0
- 半球を完全に覆う



放射線乱数の秘匿性の保証 ⇐ パリティ対称性

正規ユーザ

検出結果をもとに乱数 r を生成

盗聴者

空間反転により検出器$D^{\uparrow}, D^{\downarrow}$は入れ替わるが、放射線がパリティ対称性を持つので、盗聴者にはどちらで検出されたか分からない

放射線源：
理想的には各時間枠で上下どちらかに1粒子を放出

検出器：
理想的には完全な検出性能（効率1，暗計数0，角度欠損なし）

放射線源

検出器 D

検出器 $D^{\uparrow}$

検出器 $D^{\downarrow}$

検出器 $D^{\downarrow}$

検出器 $D^{\uparrow}$

等価

空間反転

放射線は上下の「重ね合わせ」状態になっていてパリティ対称性を持つ

放射線はパリティ対称性を持つので、空間反転しても変わらない

議論

- いつでも大丈夫なのか?
  - 仮定がやぶれなければ。
- 今までの物理乱数はダメだったのか?
  - 秘匿性の仮定を信じられるならそれでもよい。検証はできないが。
- 検品のやりやすさの問題
  - RNGチップは買ってくるものなので、検証のやりやすさ(≒構造の単純さ)は重要
- 放射線源のパリティ対称性はどの程度わかっているのか?
  - 原理的には直接検証可能だが、実際的には間接検証しかしていない
- これに置き換わる?
  - ハード部分はそのままで、ソフト部分の改良だけでよく、実装しやすい
  - 実際上は、セキュリティの向上とコストや組み込みやすさとの兼ね合い

まとめ

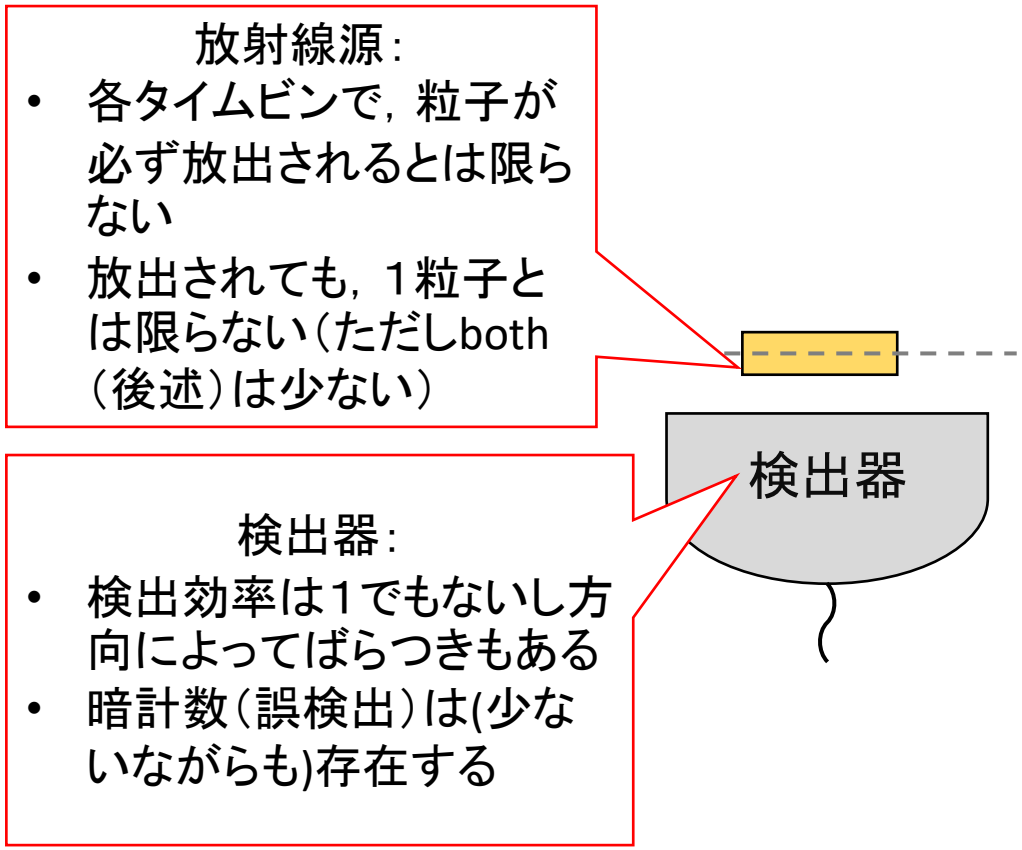
- 乱数生成器(random number generator , RNG)は暗号、計算に不可欠な要素であり，すでに様々な方式が知られている。
- 中でも放射線を用いたもの（放射線RNG）は長い歴史を持つ。
  しかしその安全性は単に仮定されるもので、示されたことはなかった。
- 今回の論文では物理的性質から放射線RNGの安全性を証明した。
  - 特に放射線源のパリティ対称性（空間反転対称性）を利用することが重要
  - ^{241}Amなど，α崩壊する核種は，パリティ対称性をもつ放射線を放出する

現実的な場合の安全性証明

…理想的な話をやめて，現実に戻る

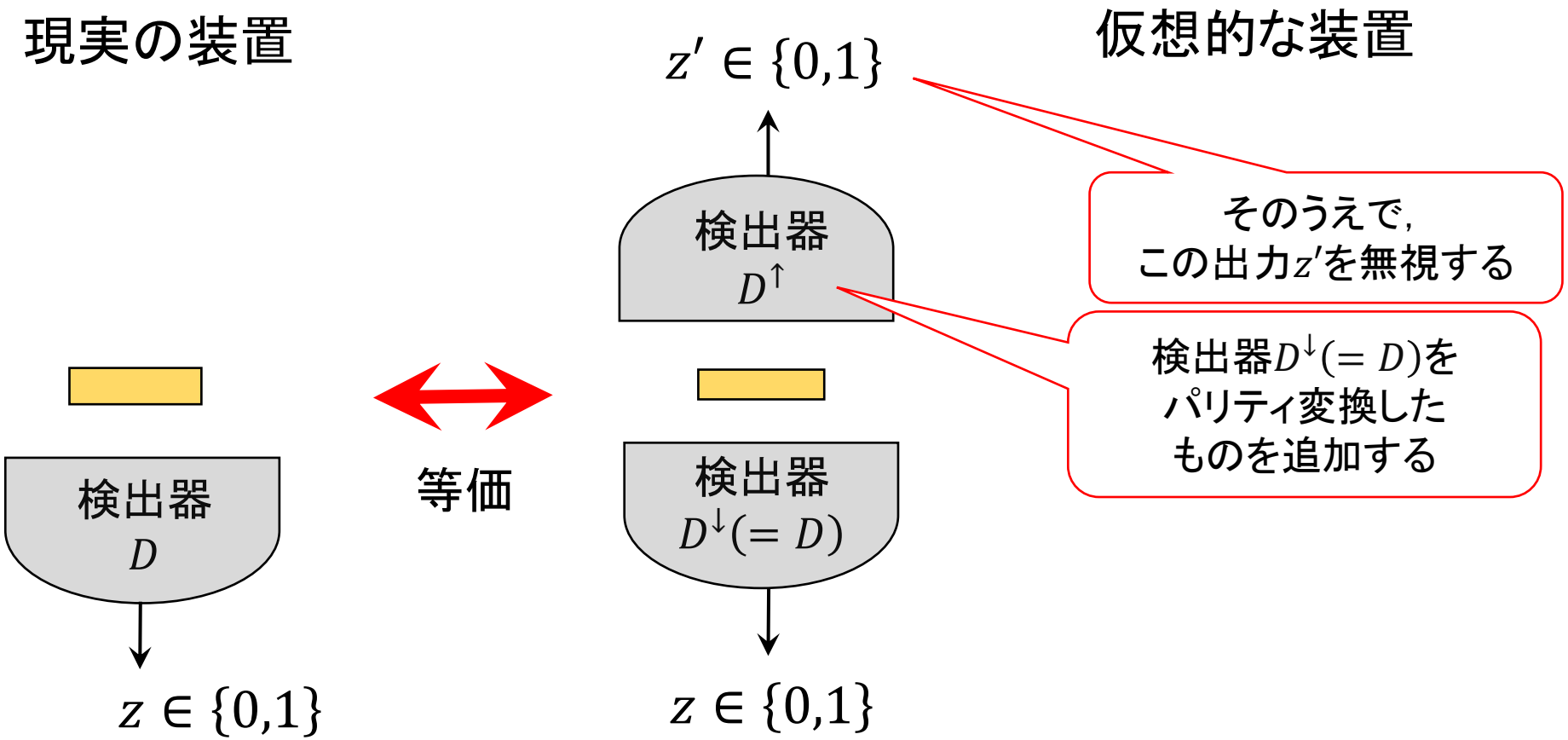
現実の放射線乱数生成器

- 現実には様々な要素が入り込む



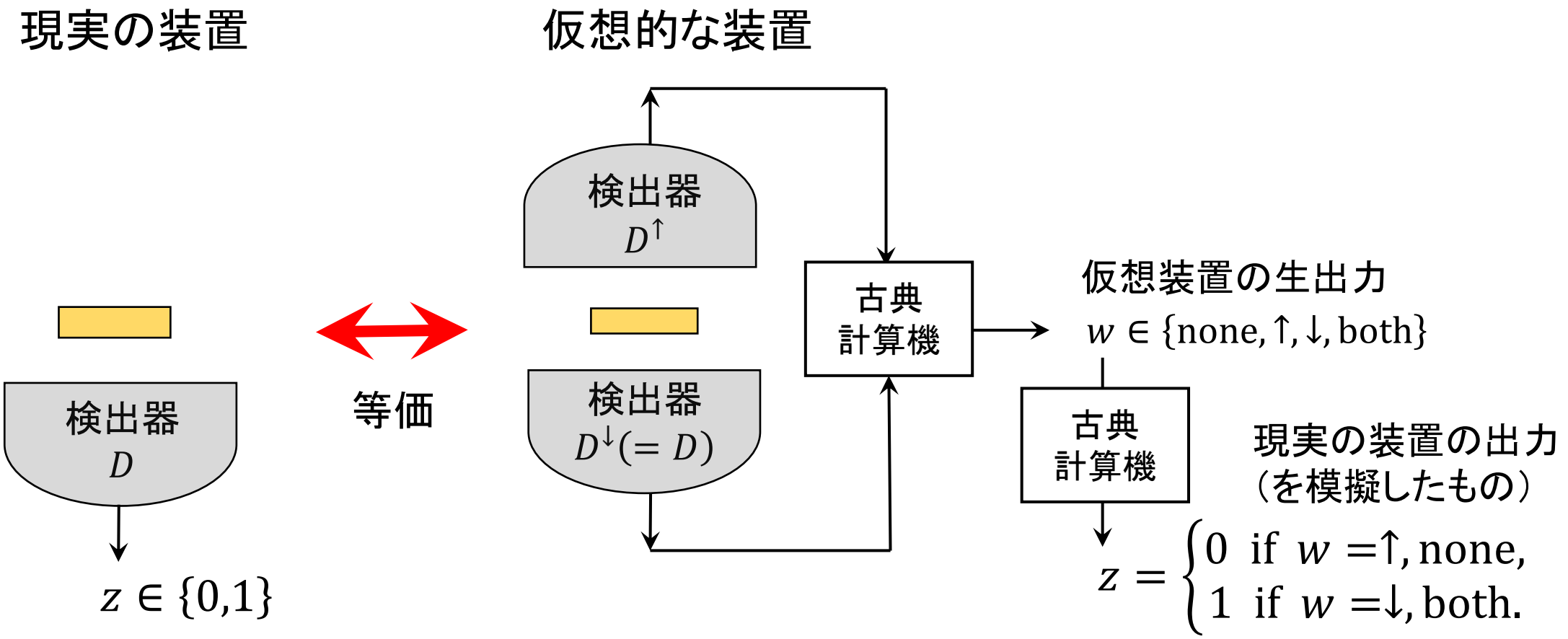
現実的な場合の安全性証明

- パリティ変換の効果が分かりやすい状況に書き換えていく



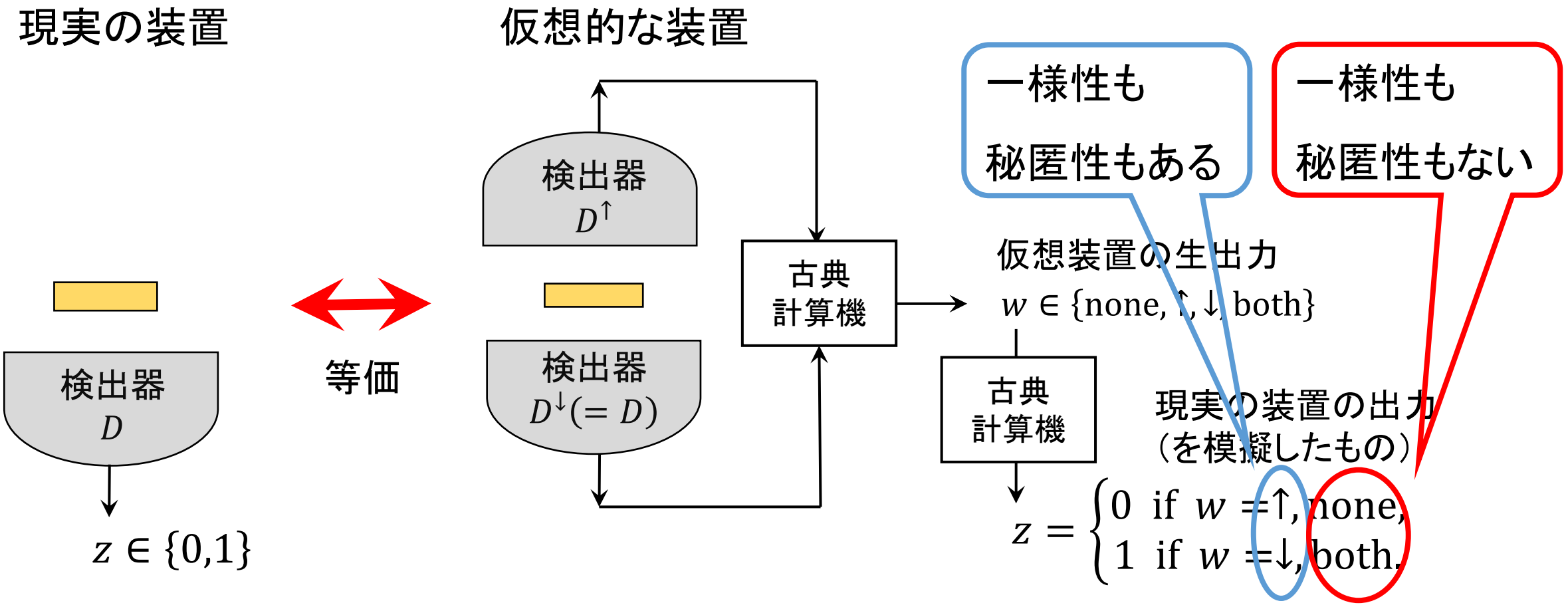
現実的な場合の安全性証明

- パリティ変換の効果が分かりやすい状況に書き換えていく



現実的な場合の安全性証明

- パリティ変換の効果が分かりやすい状況に書き換えていく



現実的な場合の安全性証明

- パリティ変換の効果が分かりやすい状況に書き換えていく