2001/4/26 @虎ノ門パストラル

総合科学技術会議情報通信プロジェクト第1回会合説明資料

量子情報処理

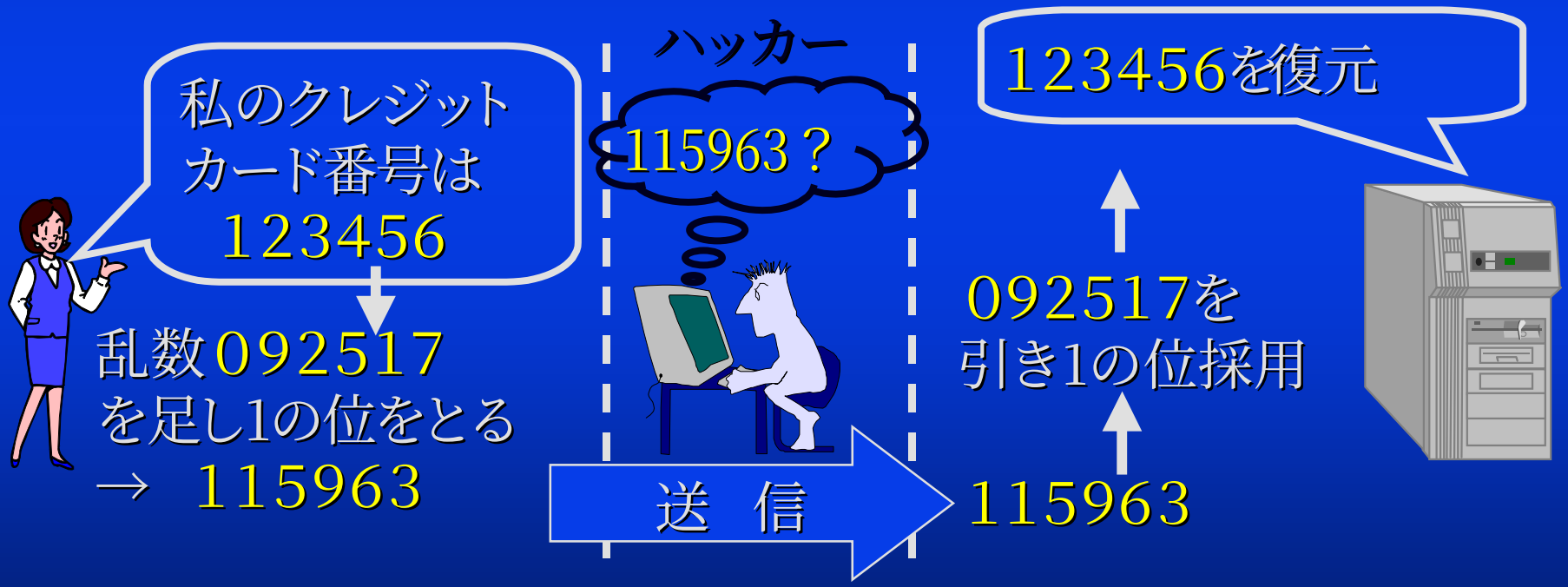
ー 量子コンピューティング・量子暗号ー

井元信之

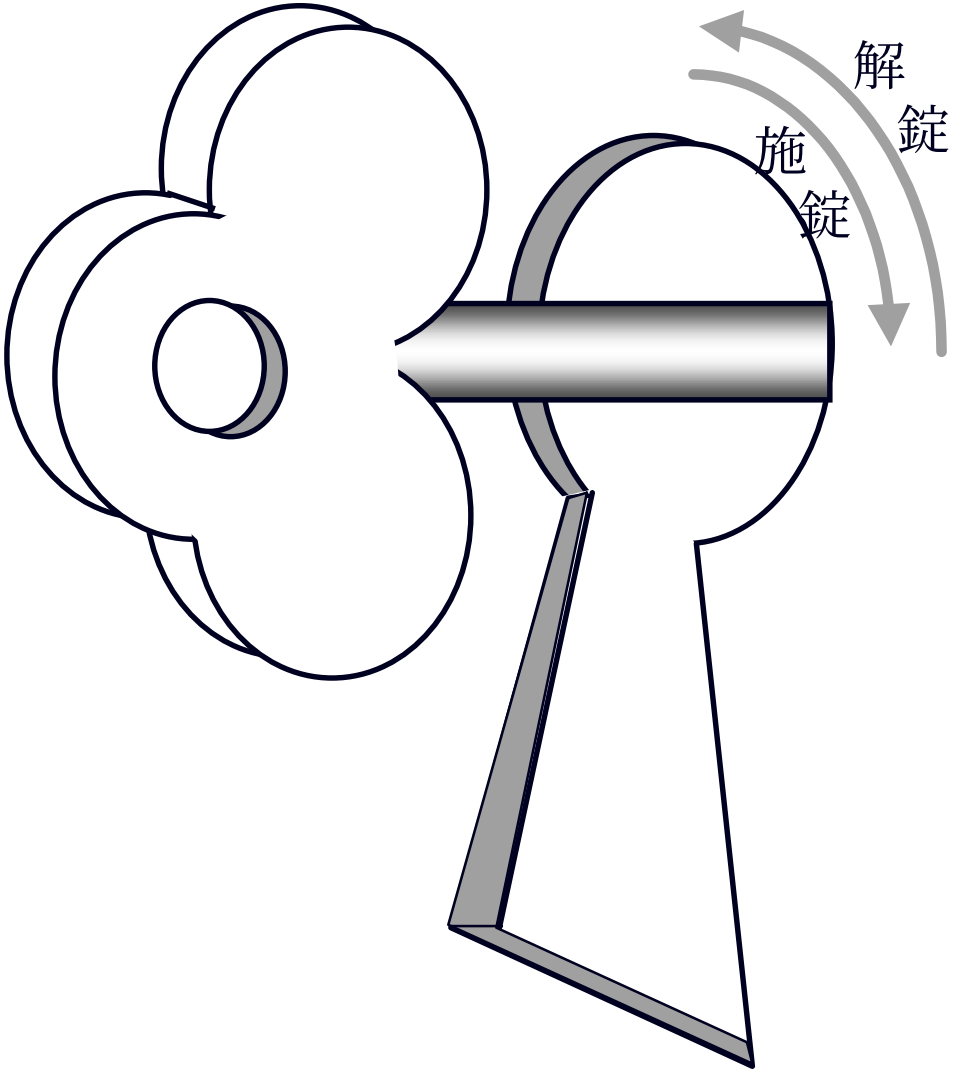
総合研究大学院大学
(東京大学大学院工学系研究科客員)

通信のプライバシー　→　暗号で実現

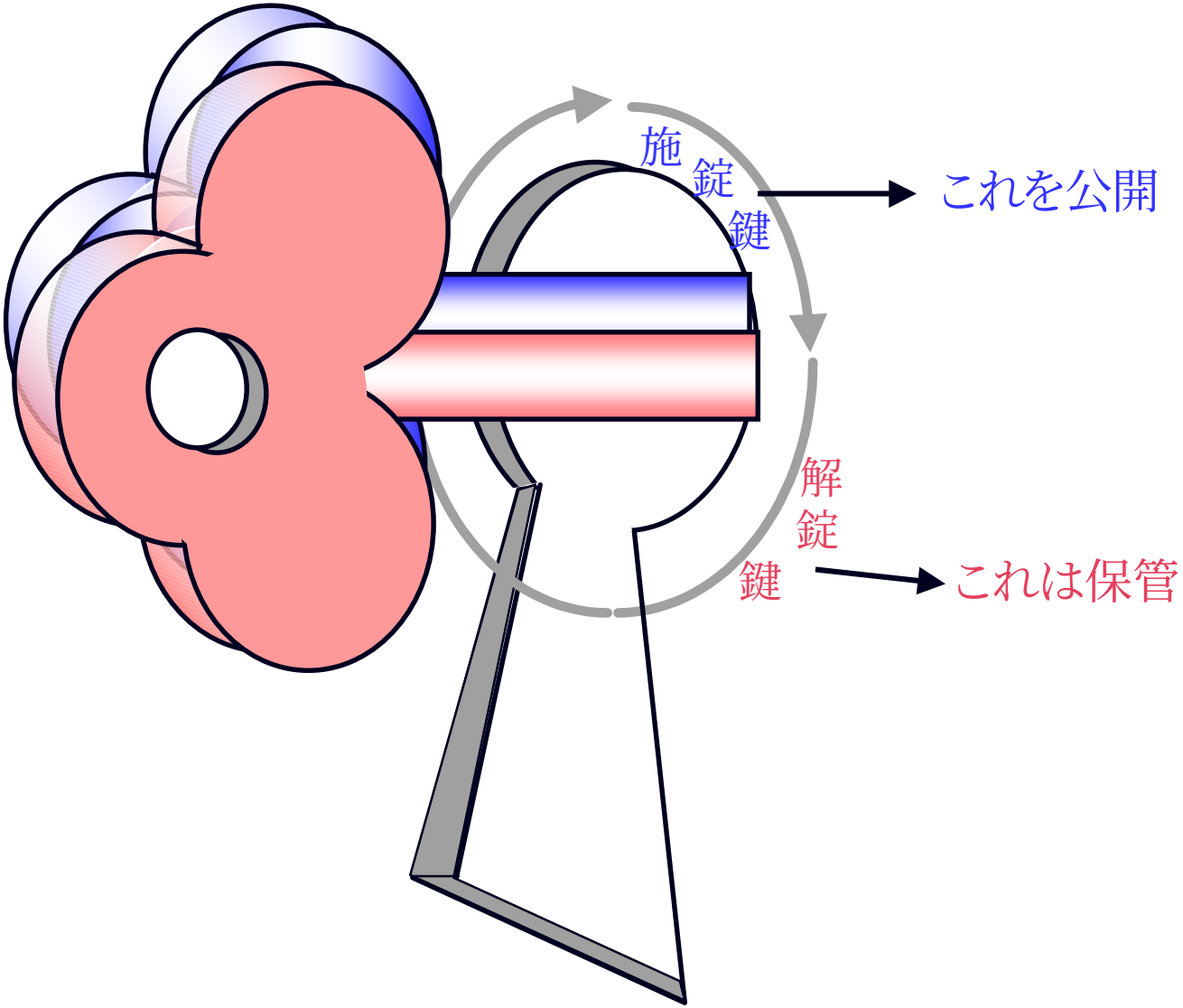
暗号とは？



1つ鍵(双方向鍵)→共通鍵暗号方式



2つ鍵(一方向鍵)→公開鍵方式



かけ算と素因数分解(一方向鍵の例)

かけ算：11 × 41 × 73 × 101 × 137 × 271 × 3541 × 9091 × 27961 × 1676321 × 5964848061

＝ 11111111111111111111111111111111111111

素因数分解：2で割れるか？ (No)
3で割れるか？ (No)
5で割れるか？ (No)
・・・・・・・・
11で割れるか？ (Yes)
・・・・・・・・
41で割れるか？ (Yes)
・・・・・・・・
5964848061で割れるか？ (Yes. 計算終了)

暗号の種類
(量子暗号以前に)

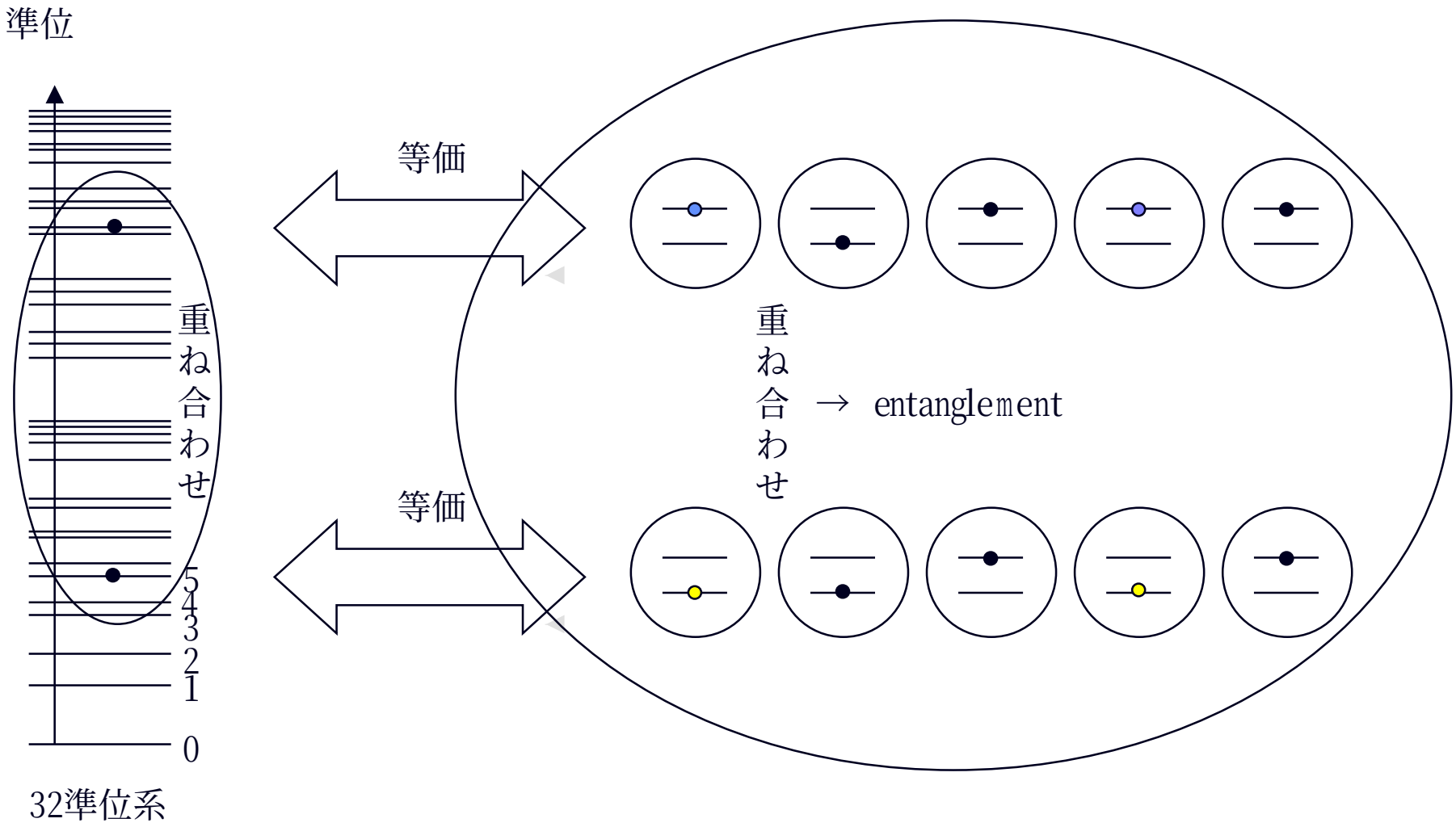
共通鍵暗号
(秘密鍵暗号)
(非公開鍵暗号)

- One-Time-Pad：使い捨て鍵方式
  究極の安全性！
  (ただし安全な鍵配送ができるなら)
  → 量子暗号 (量子信号に基づく鍵配送)
- 同じ鍵を何回も使う方式 (安全でない)

公開鍵暗号 ——

RSA暗号等：計算機数学に基づく暗号
安全神話が危ない！

重ね合わせを折り畳む → entanglement



例：重なっている一つ一つの状態の係数変換

Task：

すべての状態ベクトルの重ね合わせ状態

$$X_0 + X_1 + X_{10} + X_{11} + X_{100} + \cdots + X_{11\cdots11}$$

を

$$X_0 - X_1 + X_{10} - X_{11} + X_{100} - \cdots - X_{11\cdots11}$$

に変換せよ。

(1) 愚かなやり方

0 から 11･･･11 まで全ての i をscan。

奇数なら $X_i \to X_i$ とし、偶数なら $X_i \to -X_i$ として

重ね合わせる。

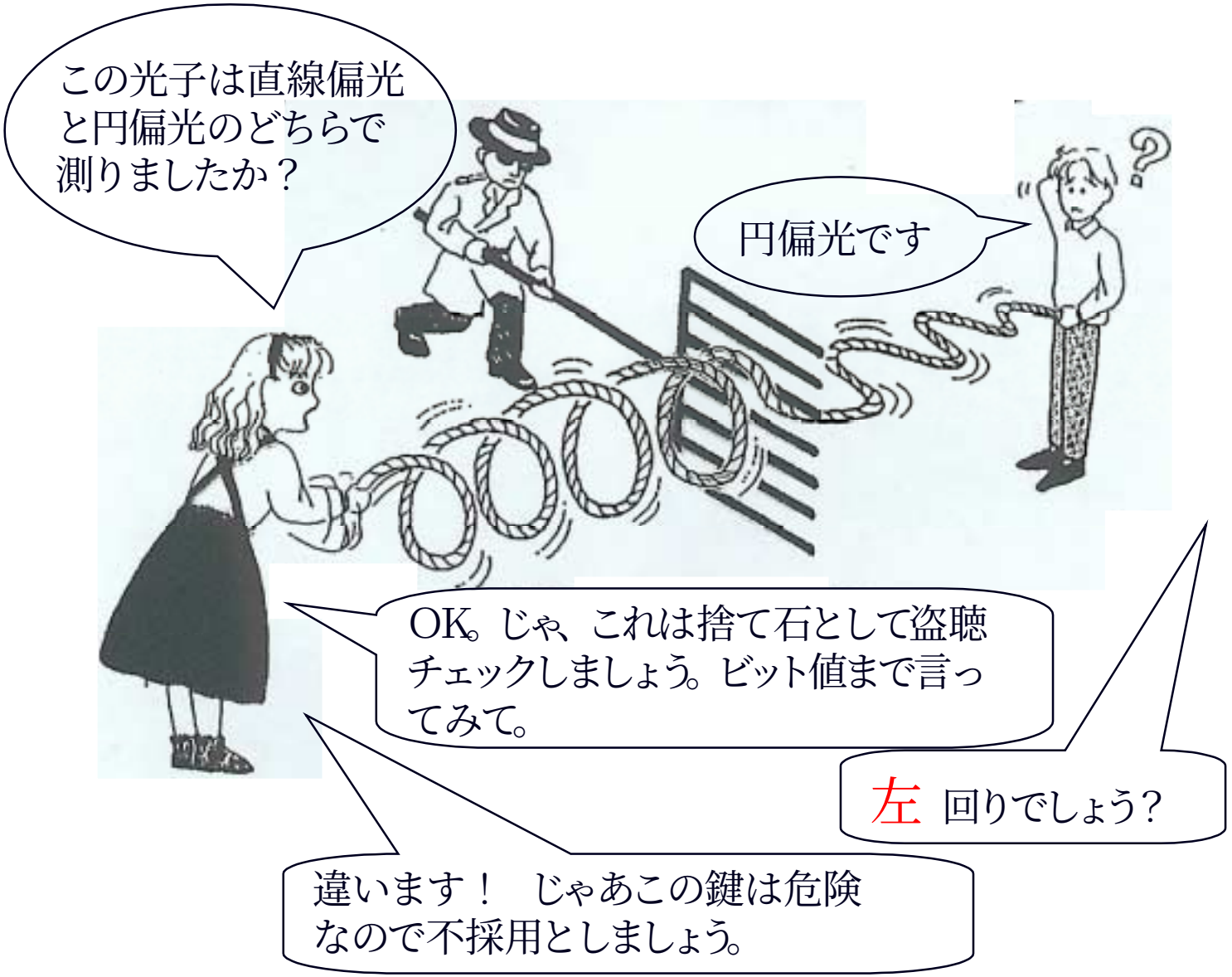
(2) 賢いやり方

右端の量子ビット一つだけ着目。

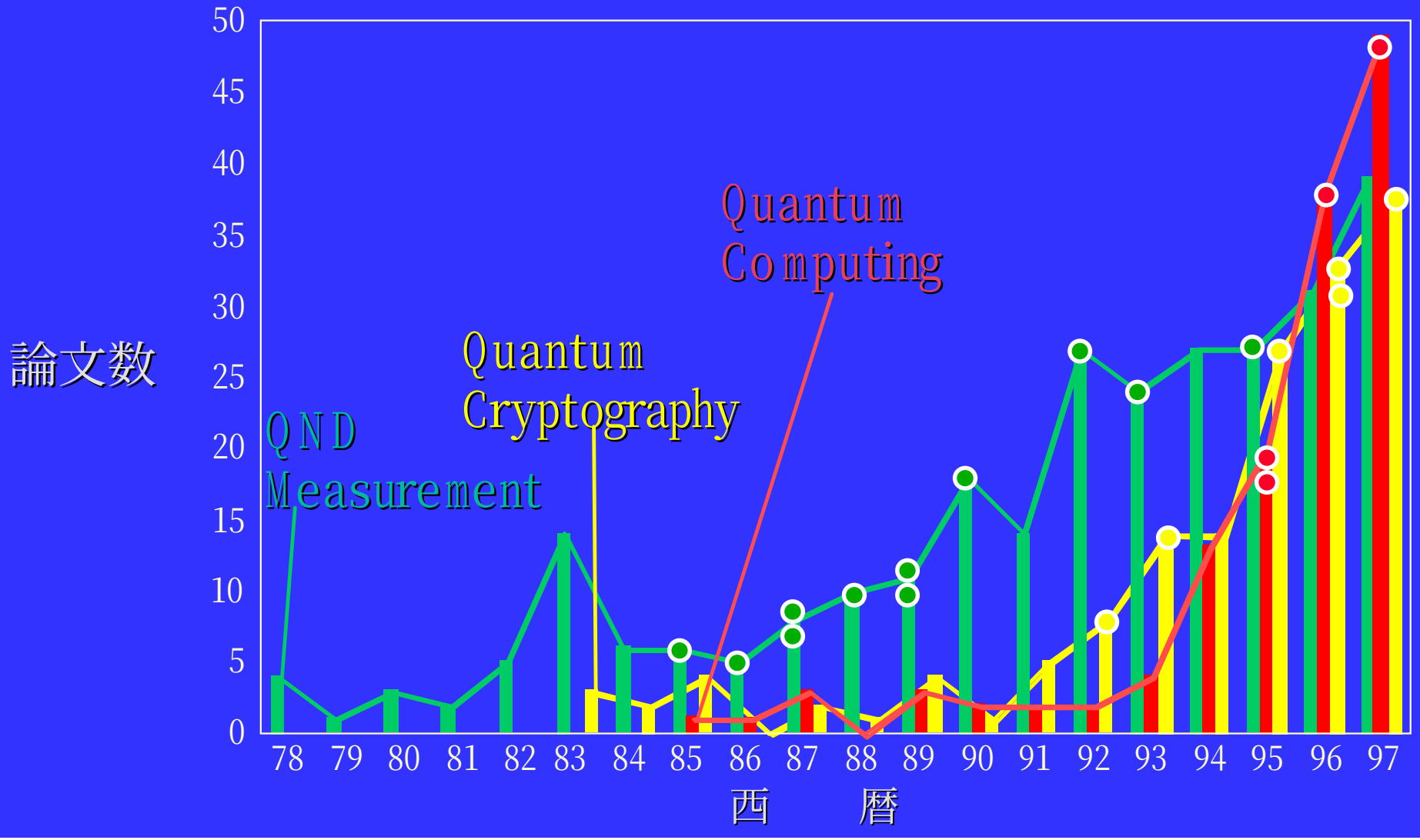
それが 0 なら $X_i \to X_i$ とし、1 なら $X_i \to -X_i$ として

重ね合わせる。

量子暗号：不確定性原理による盗聴行為の発見



論文数の推移


論文数
50
45
40
35
30
25
20
15
10
5
0
QND
Measurement
Quantum
Cryptography
Quantum
Computing
78 79 80 81 82 83 84 85 86 87 88 89 90 91 92 93 94 95 96 97
西　暦

現状・展望

◇ 量子コンピューティング
- 理論主体、実用化は当分先
- 種々のハードで少数qubit実験開始
- どの形態が本命と決める段階にない

◇ 量子暗号
- 形態は光通信。実験主体(基礎・実用)。実現近い。
  - 光ファイバー(1.5μ帯)
    専用通信／大衆通信。課題：フォトンカウンター
  - 空間伝送(0.8μ帯)
    衛星通信／地上通信。課題：安定性・損失
- US/EU、重要視

◇ その他の量子情報処理
- 理論研究開始。