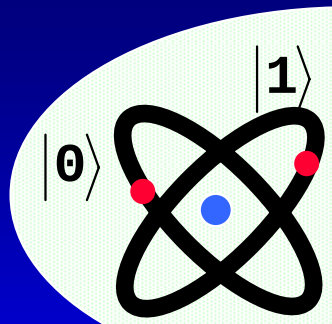
量子理論に基づく セキュリティプロトコル

北陸先端科学技術大学院大学
情報科学研究科
双紙正和

内容

- 電子社会の安心性要件
- 量子計算
- 量子セキュリティプロトコル
- まとめ

電子社会の安心性要件



量子計算

・量子コイン投げ
・量子秘密分散

知的財産保護

・耐タンパ
ソフトウェア

モバイルエージェント保護

アクセス制御

ユーザプライバシの保護

・匿名通信

DoS攻撃対策

・IPトレースバック
・フィルタリング

物理系としてのコンピュータ

- Moore の法則
  - チップの集積密度は、1年半ごとにほぼ2倍
- R. Keyes の推定
  - 2020年ごろには、1ビットあたり1個の原子
- エネルギー効率
  - 莫大な熱量の発生

“Information is Physical”

- 計算および計算機の構成に、量子論的効果を考えざるを得ない
- 量子力学に基づいた、新たな計算のパラダイム

計算の物理学 (Physics of Computation)

- R. Landauer and C. H. Bennett
  (IBM Thomas J. Watson Research Center)
- C. Mead (Caltech Research Group)

量子力学

- 基本原理： 粒子-波動の二重性
  - 原子のような小さな物理系は、離散的エネルギーをとる
  - 量子力学的波は、重ね合わせることができる
- 不確定性原理

量子チューリング機械

- R. Feynman (1982年)
  - 「(古典的)チューリング機械は、ある種の量子現象を指数的速度低下を起こさずには模倣できない」
- **D. Deutsch (1985年)**
  - **最初の真の量子チューリング機械を提案**

Deutsch の量子チューリング機械

- チューリング機械の読み、書き、シフト操作を、量子力学的相互作用によって実現
- テープに、「0」「1」の重ね合わせを同時に書き込むことができる

量子並列化の能力

多数の入力を同時に符号化し、一つの（古典的）計算を行う時間で、すべての入力に対する計算を行うことが可能

Shor のアルゴリズム（1994年）

- 量子チューリング機械を利用すると、因数分解問題と離散対数問題が非常に小さな誤り確率で高速に解ける
  - 現在の公開鍵暗号系に対する大きな脅威となりうる

量子コンピュータ研究の活発化

量子計算の一般原理

- はじめに　ー　原理？公理？
- 状態ベクトル
- 発展
- 重ねあわせ原理
- 測定
- 多粒子系

はじめに　ー　原理？公理？

- 「…次のような質問をしようとする人がいるかもしれない。『どうしてそんなことになるのか。法則の背後に隠されているからくりは何なのか』と。法則の背後のからくりなどを発見した人は、これまでにひとりもいない。」

  R. Feynman

- “Beginning students of quantum mechanics, when first exposed to these rules, are often told not to ask ‘Why?’”

  J. Preskill

内積空間H

- 複素数体C上のベクトル空間H
- 内積$\langle \cdot | \cdot \rangle$が定義される
- ノルム　$\|\psi\| = \sqrt{\langle \psi | \psi \rangle}$
- ヒルベルト空間

状態ベクトル - qubit

- 状態ベクトル‥量子系の状態を表す，ヒルベルト空間におけるベクトル
  - 0でない任意の複素数cに対して，状態ベクトルψとcψは同一状態を表す
    ↓
    通常，単位ベクトルを想定する
- Diracの記法
  - $|\psi\rangle$‥「ケット」ベクトル（列ベクトル）
  - $\langle\psi|$‥「ブラ」ベクトル（$|\psi\rangle$の共役転置）
  - $\langle\psi|\phi\rangle$‥ $|\psi\rangle$と$|\phi\rangle$の内積

発展

- 閉じた量子系の発展は、ユニタリ変換によって記述される:

$$|\psi'\rangle = U|\psi\rangle$$

- $|\psi\rangle$ … 時刻t1 の状態ベクトル
- $|\psi'\rangle$ … 時刻t2 の状態ベクトル
- U … t1とt2のみに依存するユニタリ変換

重ねあわせ原理

$|0\rangle$, $|1\rangle$をqubitの正規直交基底とする．このとき，この状態空間における任意の状態ベクトルは，

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$$

とおける．ここで，$|\alpha|^2 + |\beta|^2 = 1$, $\langle\psi|\psi\rangle = 1$, であり，$|\alpha|^2$, $|\beta|^2$ の確率でそれぞれ$|0\rangle$,$|1\rangle$が観測される

量子測定- 一般測定 -

- 量子系の測定は、測定演算子の集合 $\{M_m\}$ によって表現される。

$$p(m) = \langle \psi | M_m^\dagger M_m | \psi \rangle$$ …測定によりmを得る確率

$$\frac{M_m |\psi\rangle}{\sqrt{\langle \psi | M_m^\dagger M_m | \psi \rangle}}$$ …測定後のシステムの状態

$$\sum_m M_m^\dagger M_m = I$$ …測定演算子が満たす関係

合成系

- 合成系の状態空間は、構成系の状態空間のテンソル積によって表現される。

$$|\psi_1\rangle \otimes |\psi_2\rangle \otimes \cdots \otimes |\psi_n\rangle$$

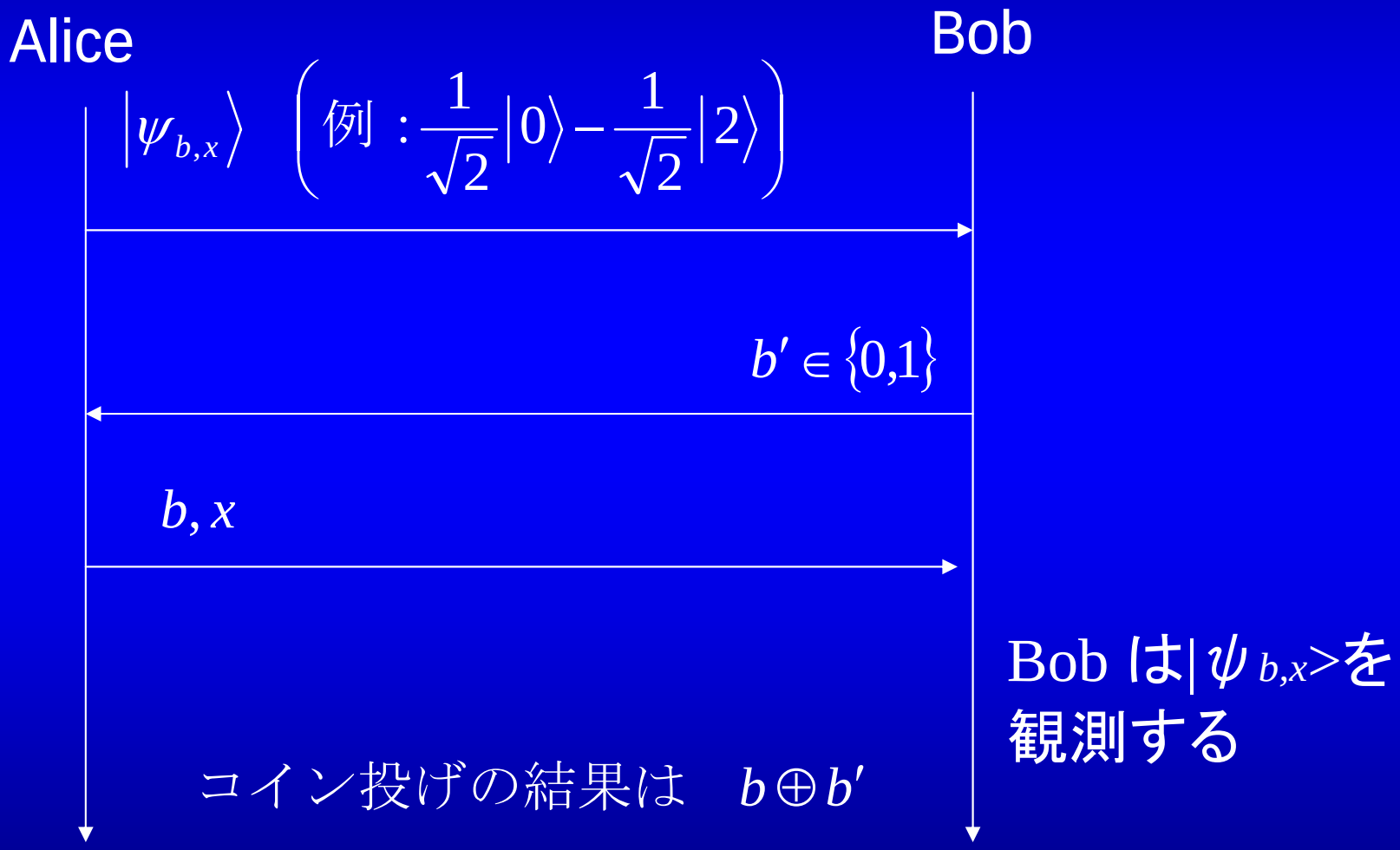
量子セキュリティプロトコル

- 量子コイン投げ
  - 二人のプレーヤー（不正を行う可能性がある）が、1ビットについて合意する
- 量子秘密分散法
  - ある定められたグループが集まると，秘密（量子）を復元できる

量子コイン投げ -- 状態の定義

$$|\psi_{b,x}\rangle = \begin{cases} \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle & \text{if } b=0, x=0 \\ \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle & \text{if } b=0, x=1 \\ \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|2\rangle & \text{if } b=1, x=0 \\ \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|2\rangle & \text{if } b=1, x=1 \end{cases}$$

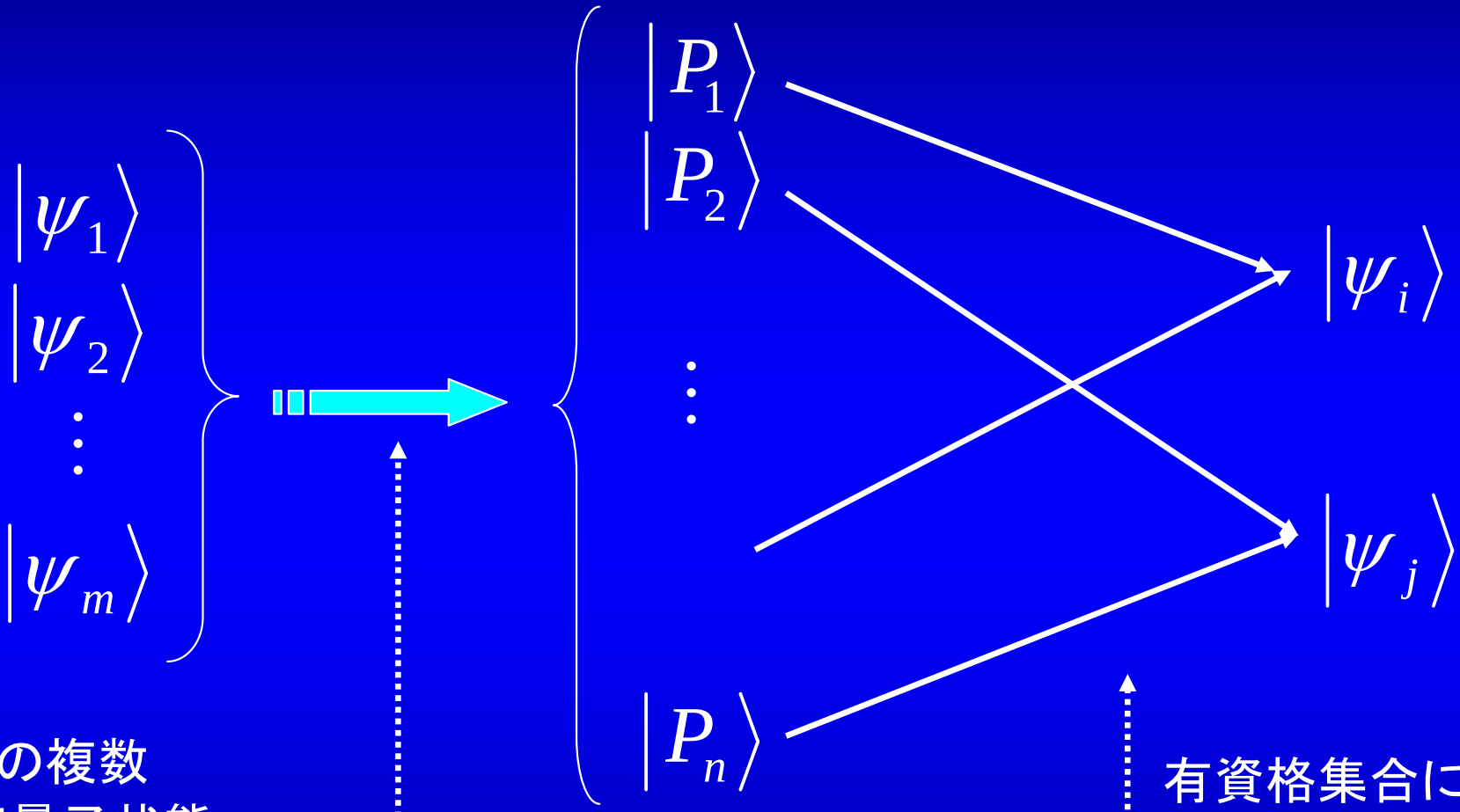
3状態量子コイン投げプロトコル



n 次元量子状態コイン投げプロトコル

- 3次元量子状態を，n次元量子状態に拡張（従来プロトコルの一般化）
- 一方のユーザの不正成功確率の偏り（バイアス）を犠牲にすることで，もう一方のユーザのバイアスを任意に小さくすることが可能となった

量子複数秘密分散法



m個の複数
秘密量子状態

量子操作
(秘密の分散)

n個の分散
情報(シェア)

有資格集合によって
復元された秘密

量子操作
(秘密の復元)

提案量子複数秘密分散法の成果

- Monotone Span Programs (MSP)を用いた一般的なアクセス構造をもつ量子複数秘密分散法を初めて提案
- 量子情報理論に基づき，量子複数秘密分散法が安全に構成されるために満たすべき条件を考察

多対多における量子秘密分散法

- それぞれ m 人，n 人からなる2つのグループ間において，それぞれ満場一致法の秘密分散を使って，同一の秘密を共有
- 特に，量子メモリを必要としない方式を提案

量子計算機は実現可能か？

- 量子通信は，100km程度の実証実験に成功
- 2001年，IBM が，7qubit 量子計算機を利用して，15=3×5の因数分解に成功
- 太田，國廣（電気通信大）
  - Shor のアルゴリズムを実行するための量子計算機のスペックについて詳細な評価．現実的な時間で因数分解するためには，1演算あたり50μ秒以下の処理速度で，1730個以上のqubit が必要

まとめ

- 近未来電子社会における安心性要件としての，量子セキュリティプロトコル
- 今後の方針
  - 量子複数秘密分散法の構成要件の研究（必要十分条件），具体的な構成法
  - 量子公開鍵暗号
  - 量子セキュリティモデル