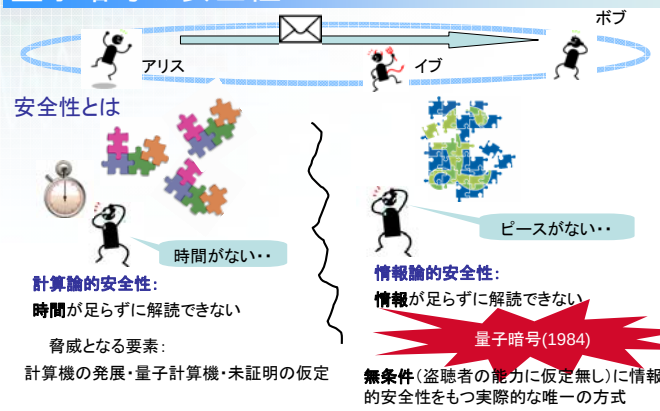
量子論理におけるコピー不可能性定理

宮寺 隆之
（独）産業技術総合研究所
情報セキュリティ研究センター　物理解析研究チーム

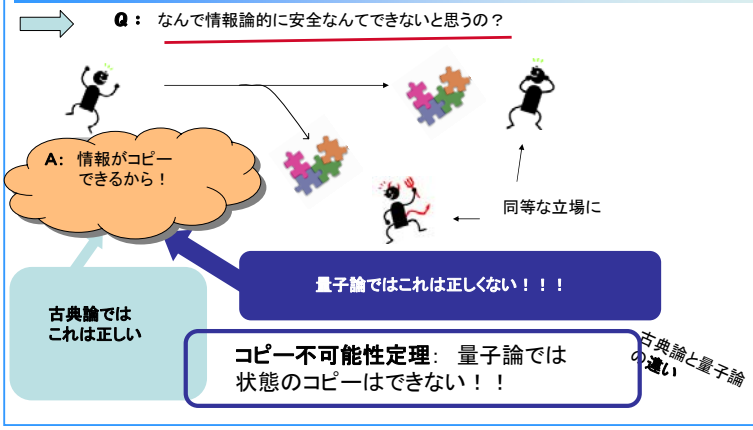
量子暗号の安全性



脅威となる要素:
計算機の発展・量子計算機・未証明の仮定

無条件（盗聴者の能力に仮定無し）に情報論的安全性をもつ実際的な唯一の方式

何で情報論的に安全なんてことができるの？



コピー不可能性定理の起源を探る

コピー不可能性定理の深化

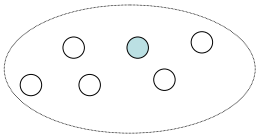
情報量的表現 ⇒ 情報撹乱定理 etc.
— 量子暗号の安全性証明へ適用

一般化？ この定理の根本的な起源は？
— これは「量子論特有」の定理なのか？

量子論を含む広い枠組みでのコピー不可能性定理の研究

確率論をベースにした枠組み ＝ 一般確率論 (convex approach)
‥‥ Barnum et al.
質問のなす代数をベースにした枠組み ＝ 量子論理 (quantum logics)

古典論理



全ての観測量は同時測定可能
本質的に荒い観測か細かい観測かの差だけ

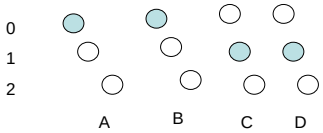
“最も細かい観測量”の値をPhase spaceとすれば‥‥
- 他の観測量はPhase spaceの分割に相当
- 結果は部分集合に対応

部分集合の為す代数
＝ Boole代数

量子論理

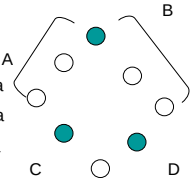
同時測定不可能な観測量が存在！

A, B, C,D: 同時測定できない観測量
（それぞれ三つの値を取るとする）



一つ一つの観測量＝部分集合
測定結果は更にその部分集合

Moreover
If A takes 0, then B takes 0 and vice versa
If A takes 2, then C takes 0 and vice versa
If C takes 2 then D takes 2 and vice versa
If D takes 0 then B takes 2 and vice versa



Pasting of subsets (Boolean algebras)
＝ orthoalgebra

主定理

L: partially ordered set (A,B ∈ L)

i) A+B=B+A (if l.h.s. is defined: A⊥B)
ii) (A+B)+C=A+(B+C) (if l.h.s. is defined)
iii) For all A there exists a unique A’ s.t. A+A’=1
iv) A+A is defined => A=0
v) A∧B exists
vi) A∧B=0 ⇔ A+B is defined

Orthoalgebra ⇔ i) ii) iii) iv)
Ortholattice (量子力学) ⇔ i) ii) iii) iv) v)
Boolean algebra ⇔ i) ii) iii) iv) v) vi)

合成系＝テンソル積で定義

主定理
Orthoalgebra L について以下は同値
A) コピー操作を許す
= 以下のmorphismが存在

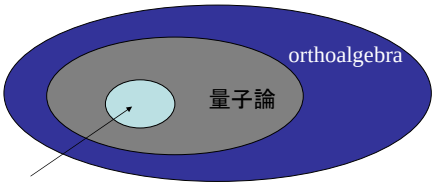
$$\phi: \quad L \otimes L \to L$$
$$\phi(A \otimes 1) = \phi(1 \otimes A) = A$$

B) LはBoole代数である

Heisenberg描像で考えている

T.Miyadera and H. Imai, “No-cloning theorem on Quantum Logics”, Journal of Mathematical Physics **50**, 102107 (2009).
なお、もっと広いEffect algebraでも類似した結果が成り立つ

まとめ



古典論＝Boole代数＝コピー可能

コピー不可能性定理は古典論でなければ必ず成り立つ

- 量子論の次の理論（！）でも‥‥
- 同時測定不可能な観測量があるような有効理論で記述される系でも‥‥

情報論的安全性をもつ鍵分配ができる可能性