光の不思議な性質を用いた盗聴不可能な暗号

（まとめ資料）

玉木　潔

富山大学工学部
知能情報コース

暗号って何？

一言でいうと、情報を隠すためのテクニック

通信における暗号の例

送信者

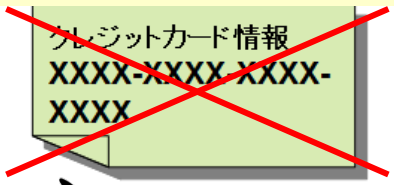
クレジットカード情報
XXXX-XXXX-XXXX-XXXX

正規受信者

クレジットカード情報
XXXX-XXXX-XXXX-XXXX

送信者の目標

正規受信者にはクレジットカードの番号を伝えたいけれど、盗聴者には隠したい



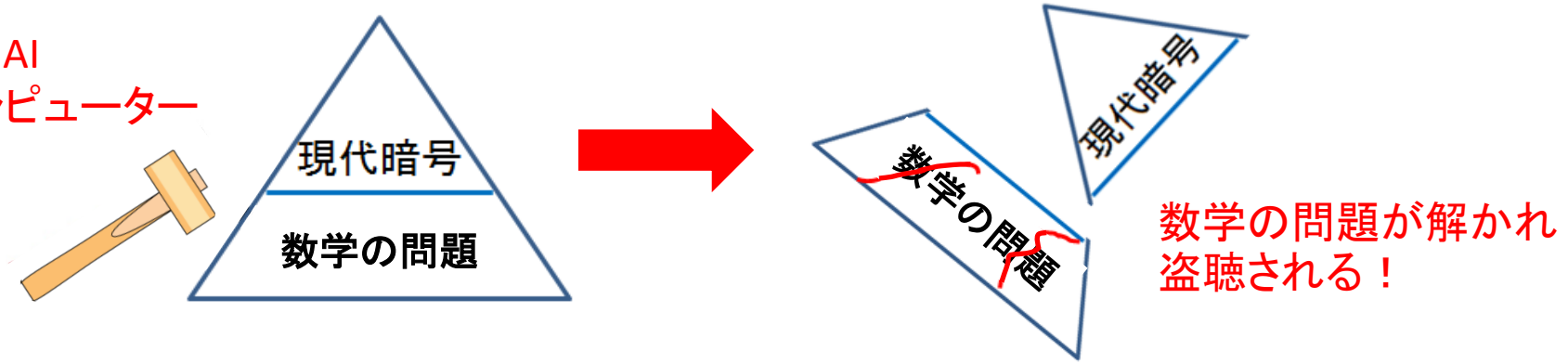
盗聴者

現在主流の暗号（現代暗号）の安全性
⇒ 数学の問題を解く難しさを利用

数学の問題

- ✓ 量子コンピューターなどの速い計算機によって解かれる危険性がある！
- ✓ 賢い人やAIが解くことができない、という保証はどこにもない！

賢い人、AI
量子コンピューター



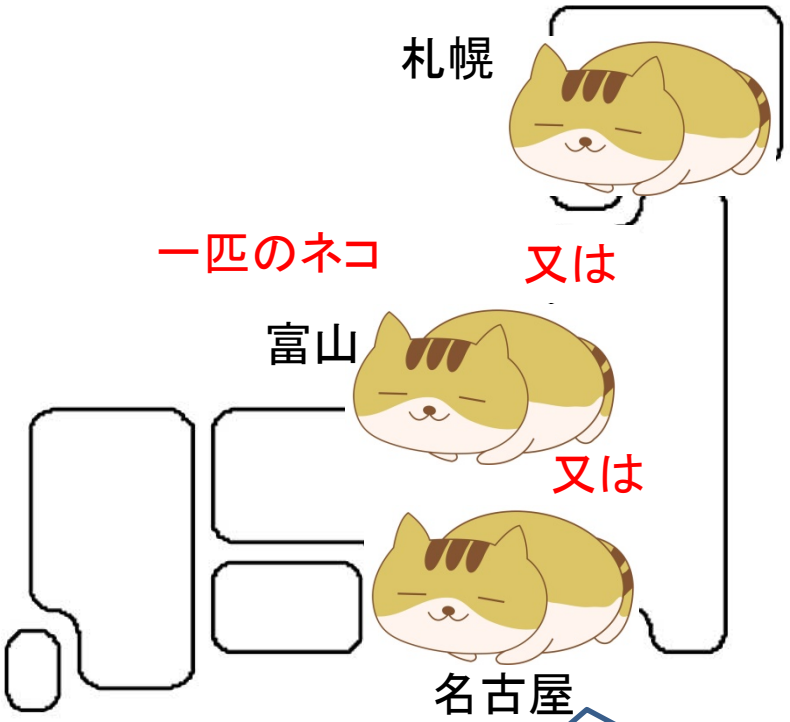
数学の問題が解かれ
盗聴される！

数学の問題に基づく暗号は、賢い人、AI、高性能なコンピューターなどによって盗聴される恐れが常にある

数学の問題ではなく、微小な物（光の粒等）がもつ不思議な性質に情報を守ってもらおう！

⇒　量子暗号

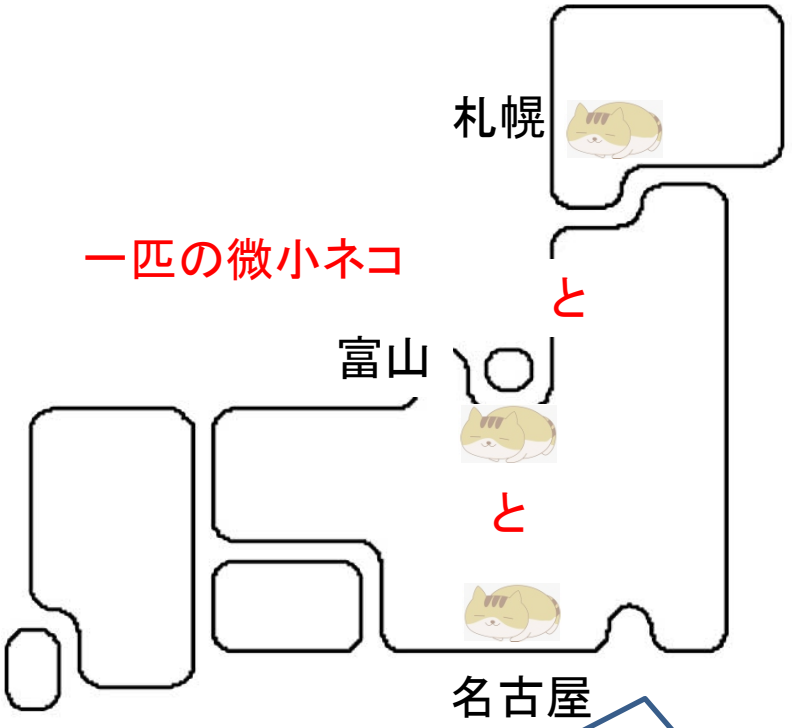
私達の常識



私は名古屋か札幌か富山にいます

微小な物の不思議な世界

イメージ図



私は名古屋と札幌と富山に同時にいます

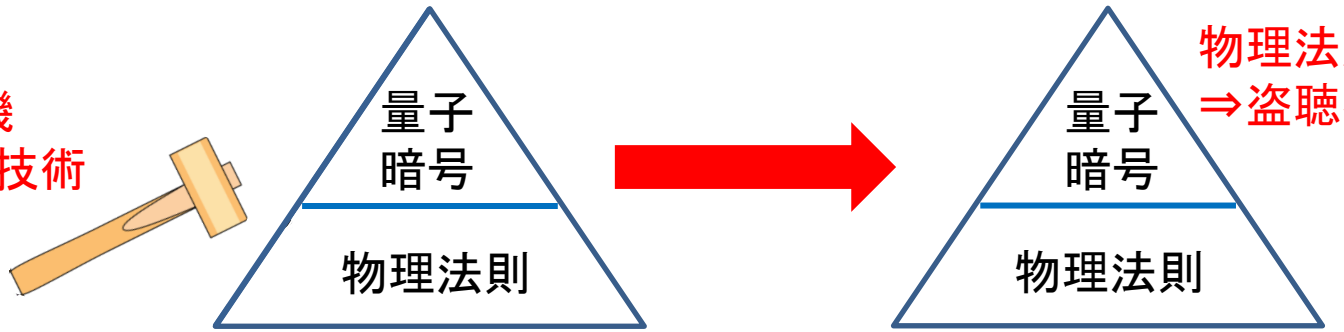
- ✓ 微小な物は**複数個所に同時に存在できる！**
- ✓ また、微小な物に書き込まれた情報は一般に**コピーができない！**

微小な物（光の粒）の性質が盗聴を防ぐ量子暗号！

量子暗号専用装置が必要

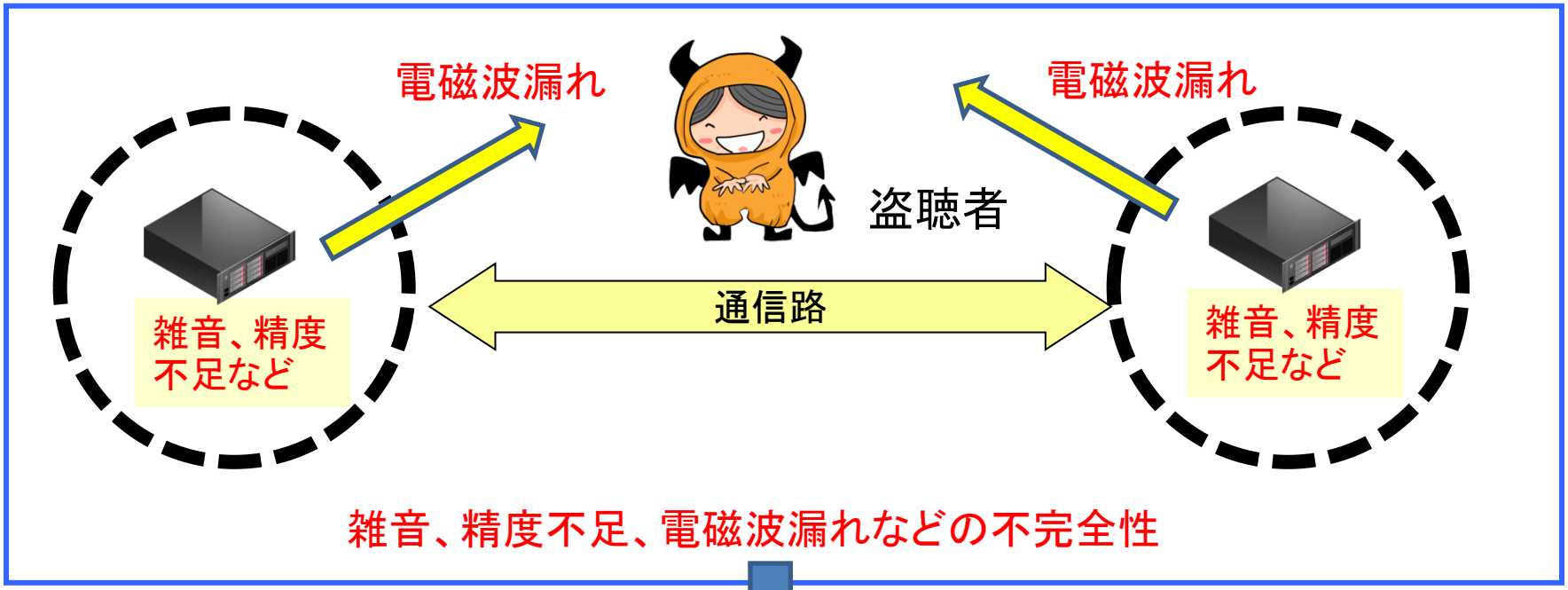
盗聴するには、光の粒の性質を変える必要あり（不可能）
⇒ 盗聴不可能！

賢い人,AI
量子計算機
1万年後の技術



物理法則は崩れない
⇒盗聴不可能！

実際の量子暗号装置



安全性が脅かされる！

装置の不完全性を利用した盗聴を防ぐ研究が盛んに行われています

量子暗号ネットワークの敷設例

米国

大規模量子暗号ネットワーク（主にワシントン・オハイオ州都間 ）

中国

大規模量子暗号ネットワーク（主に北京・上海間）

英国

複数都市間(ケンブリッジ、サウサンプトン、ブリストルなど)

EU

量子暗号の産業化を目指す

日本

東京QKDネットワーク（主に小金井・大手町間）