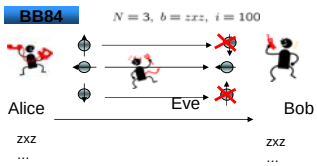
量子コルモゴロフ複雑性と量子鍵分配

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　＝　量子鍵分配

BB84量子鍵分配プロトコル　(Bennett, Brassard 1984)

1. AliceがNビットの乱数をN個の量子ビットに載せて送る
   (1) 各量子ビット毎に{＋,×}基底をランダムに選び
   (2) Nビットを対応する基底に1ビットずつエンコード
2. Bobは各量子ビット毎にランダムに{＋,×}基底を選び測定する
3. エラー率を公開通信路でチェック　→　エラー訂正
4. 秘匿性増強を行う　→　最終鍵☺



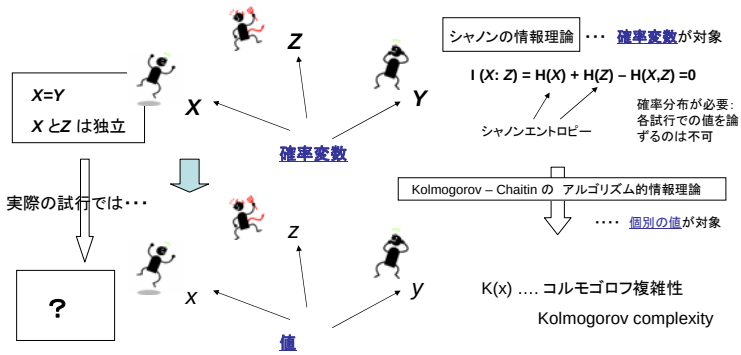
Eveの情報撹取は正規ユーザ間のデータ間に誤りを生じさせる（情報撹乱定理 [MI1]）

$$I(A:E|b) \le H(A \oplus B|b)$$

情報論的安全性！

AliceとBobはEveの存在を検知できる！

情報論的安全性？

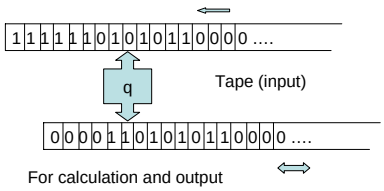


量子コルモゴロフ複雑性

1960年代：Kolmogorov, Chaitin:（古典）コルモゴロフ複雑性

K(x) = x を記述するために必要な最小の文字数
= x を出力するための最小プログラム長

Turing machine (1936)



量子Turing machine
(1985: Deutsch)

量子コルモゴロフ複雑性(2001:Vitanyi)

K(ψ) = 量子状態 ψ を出力するための最小古典プログラム長

K(ψ)はShannon (von Neumann) エントロピー のように「良い」性質をもつ

★ コルモゴロフ複雑性の値は万能Turing machineの選び方に（本質的には）依らない

$$K_U(x) \le K_T(x) + Const.$$

シミュレートされるTuring machineを指定する数(xに依らない)

★ 任意の数列 x のコルモゴロフ複雑性は、その長さ l(x) が与えられたならばl(x) 以下

$$K(x|l(x)) \le l(x) + c$$

プログラム：「 x をプリントせよ」

★ K(x) が小さい　⇔　x にパターンがある

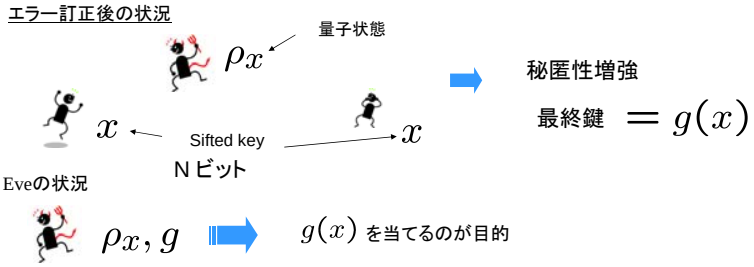
$$K(\underbrace{000\cdots00}_{N}|N) = C$$

プログラム：「0をN回プリントせよ」

x はランダム　⇔　$K(x|l(x)) \ge l(x)$

安全性

エラー訂正後の状況



Eveの状況

$K(g(x)|\rho_x, g)$　＝　最終鍵のEveにとっての複雑さ
＝最終鍵を正確に得るためにはEveは更にどのくらいの情報（プログラム）が必要か

Eveにとっては最終鍵がランダム　＝「本質的」に $K(g(x)|\rho_x, g) \ge l(g(x))$

安全性証明

M=l(g(x)) =N(1-h(2p))　最終鍵長

$$\forall_{\epsilon, p,}$$

$$\Pr(K(f(x)|\rho^{E}_{x,b,T,z_T,z'_T}, f, b, T, z_T, z'_T) \le M - \delta N - c \wedge |z_T \oplus z'_T| < Np) \le 2^{-\delta N} + 3\epsilon^{-\frac{\epsilon^2}{4}N}$$

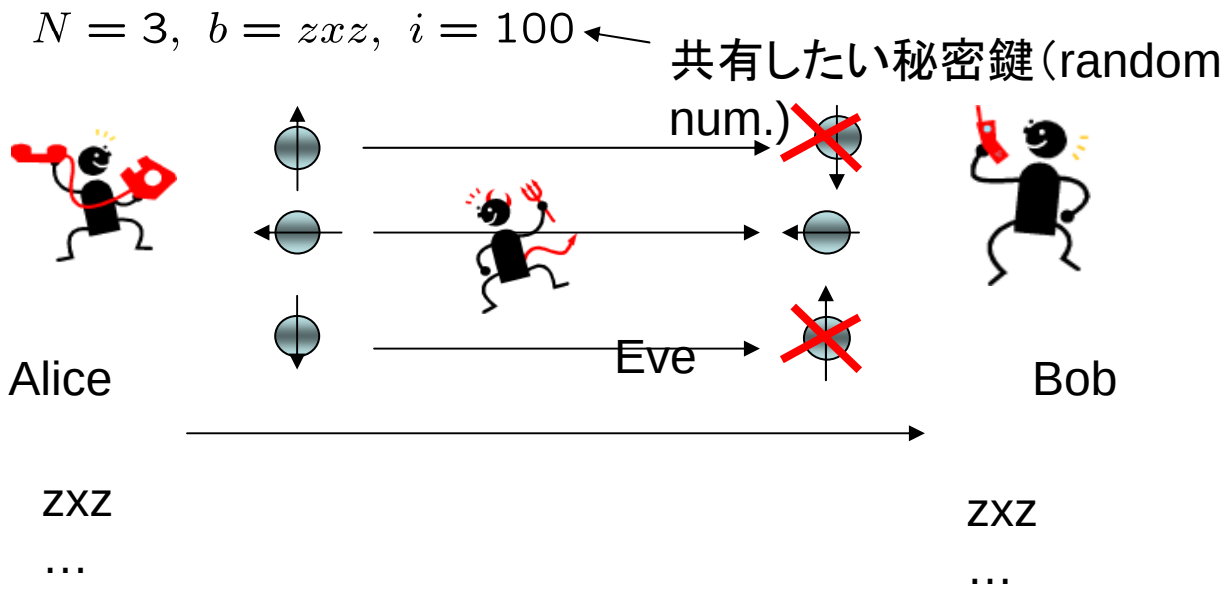
$K(g(x)|\rho_x, g) < l(g(x))$　最終鍵がEveにとってランダムでないという確率は
Nについて指数関数的に少ない！

Reference:
T.Miyadera and H. Imai, Quantum Kolmogorov Complexity and Quantum Key Distribution, Physical Review A 79, 012324 (2009)

量子コルモゴロフ複雑性と量子鍵分配

物理解析研究チーム
宮寺隆之

BB84量子鍵分配プロトコル
Bennett-Brassard 1984



無条件に

情報論的な安全性

をもつ暗号方式

＝ 盗聴者の能力に仮定をおかず

＝ **情報**が足りない！

$$I(A:E|b) \leq H(A \oplus B|\bar{b})$$

盗聴者の得る情報

正規ユーザ間のデータの不一致

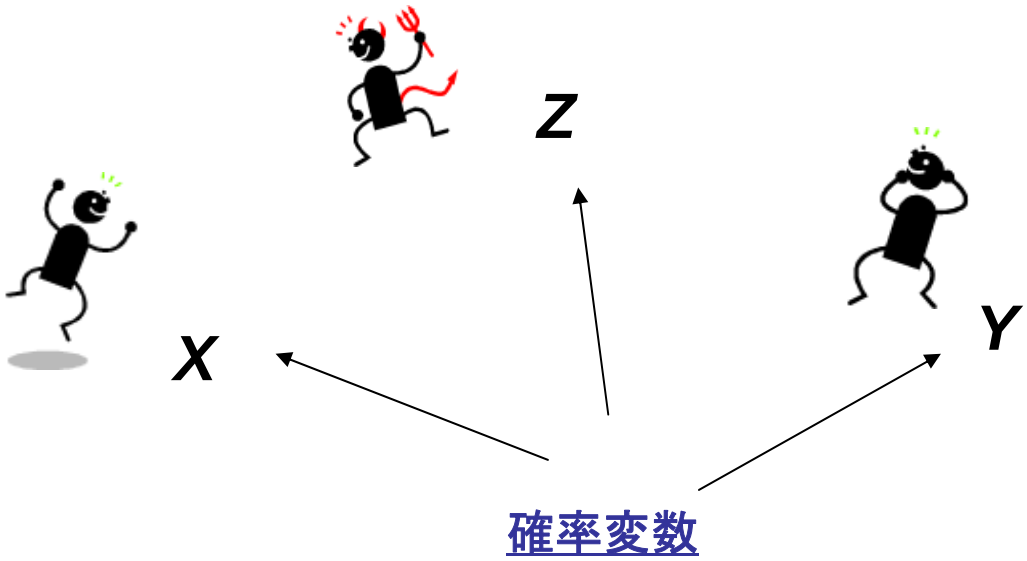
情報理論的安全性

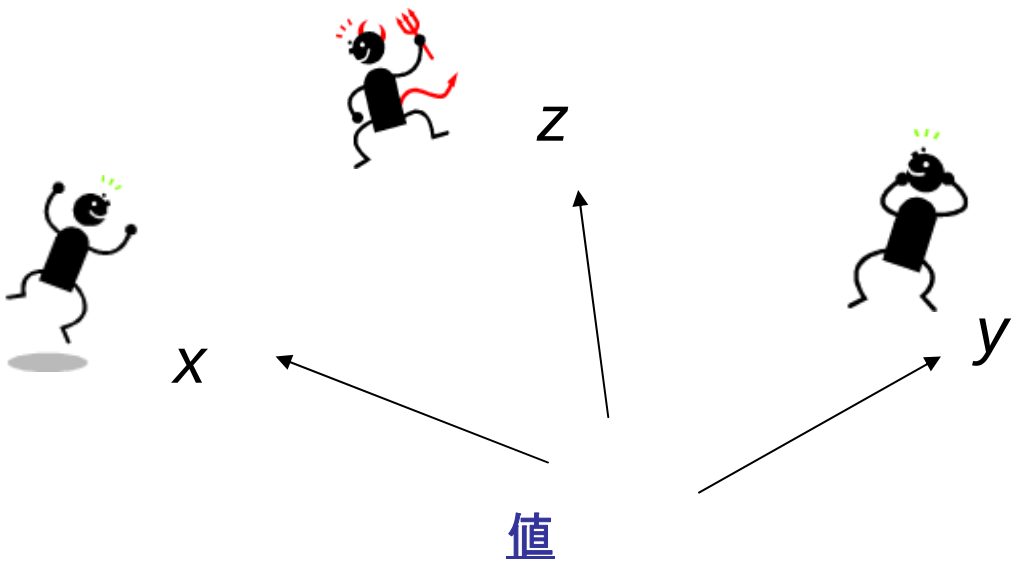
$X=Y$

X とZ は独立

実際の試行では・・・

?





Shannonの情報理論 ・・・ 確率変数が対象

$$I(X:Z) = H(X) + H(Z) - H(X,Z) = 0$$

確率分布が必要：各試行での値を論ずるのは不可

シャノンエントロピー

Kolmogorov – Chaitin の Algorithmic Information theory

・・・・ 個別の値が対象

K(x) …. Kolmogorov Complexity

Kolmogorov Complexity を用いて安全性を定義し、BB84量子鍵分配プロトコルが実際にその安全性を満たすことを示す

アルゴリズム的情報理論 (Kolmogorov, Chaitin 1965,1966)

= 確率変数なしの情報理論

= 個々のデータに対する情報理論

Key notion = アルゴリズム的ランダムネス

アルゴリズム的情報理論

x 01列

$K(x)$ Kolmogorov 複雑性

$K(x|y)$ 条件付Kolmogorov複雑性

シャノンの情報理論

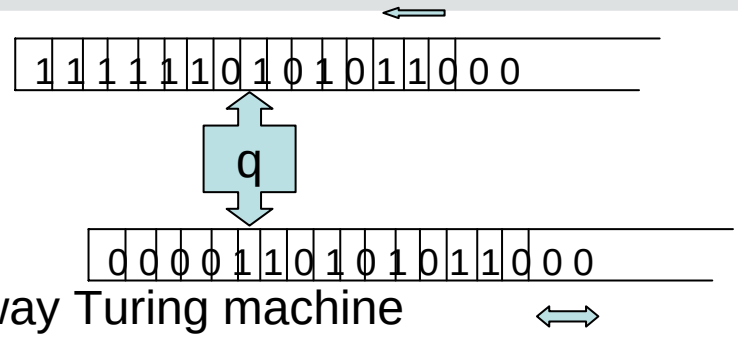
X 確率変数

$H(X)$: エントロピー

$H(X|Y)$ 条件付エントロピー

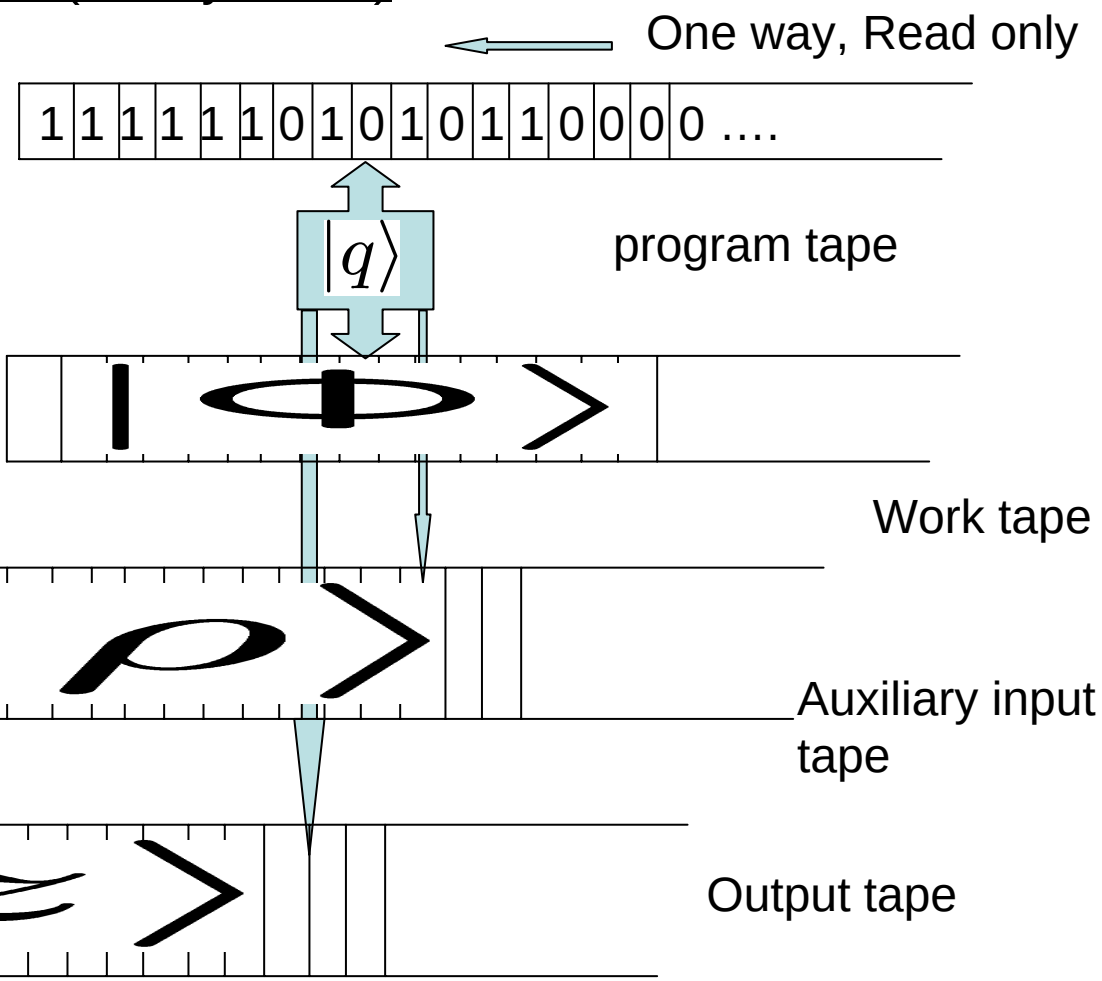
$K(x)$ = x を記述するために必用な文字数

= x を出力する最小プログラム長



One-way Turing machine ⟺

量子 Kolmogorov 複雑性 (Vitanyi 2001)



Quantum Turing Machine *U*

$$K(|x\rangle|\rho) = \min_{m}\{l(m) - \log|\langle z|x\rangle|^2|\ U(m|\rho) = |z\rangle\}$$

プログラムは古典

プログラム長

Approximation term

詳しくはポスターで