自由エネルギーは暗号化できるか？ – 計算量制限熱力学の可能性

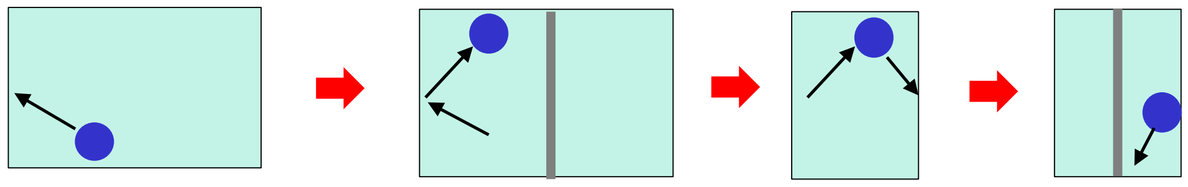
伊庭　幸人　　モデリング研究系　教授

物理系のエネルギーや運動量は，観測者の知識や能力に依存しないという意味で
客観的な存在であるが，エントロピーや自由エネルギーのような量はどうだろうか

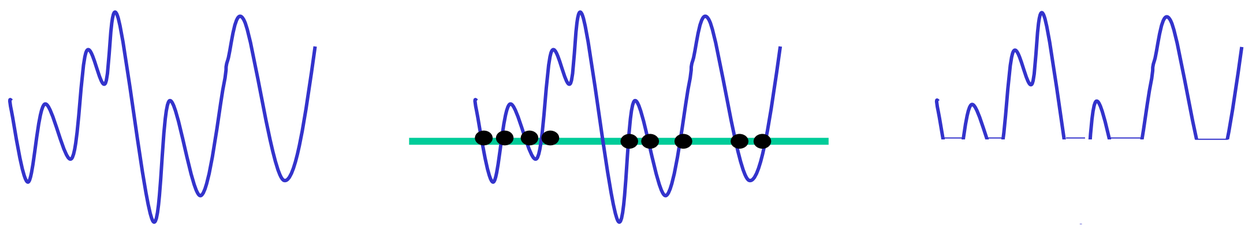
観測者が利用できる計算資源に制限を設けた場合，暗号論的疑似乱数を利用することで
等温サイクルで系から抽出できるエネルギーの上限が「鍵」の有無で異なる状況が作れる？

マックスウェルの悪魔の仲間たち（復習）

シラードのエンジン：　分子が左右のどちらにいるか常に既知なら，仕事ゼロで圧縮できる➔再膨張



熱雑音を整流：　いつ電流がゼロになるか常に既知なら，仕事ゼロで一方向きの電流が取りだせる



実際にはできない理由

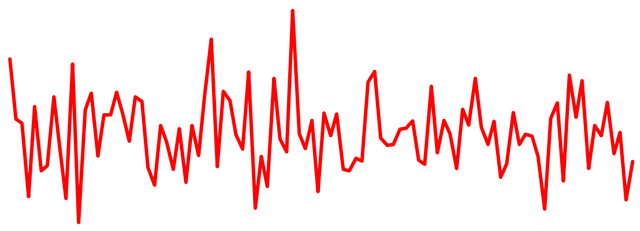
状態が既知でない
➔ 観測で系が乱される
（ガボール，ブリルアン）

装置の記憶の消去が必須
➔ 熱が発生してしまう
（ベネット，ランダウアー）

※現在は後者の見方が有力

もし疑似乱数で作られた状態だったら？

例）熱雑音と区別がつかないように
疑似乱数でシミュレートされた
波形を物理的に作って送る
（電波，光，音など媒体は任意）



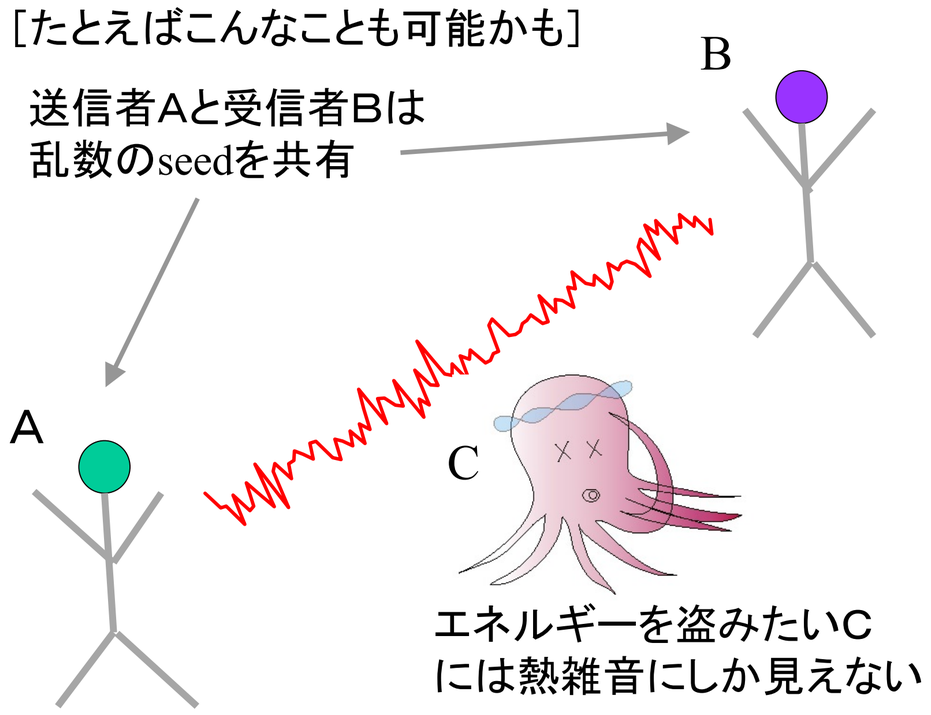
乱数の種を知っていれば観測なしですべてを予測できる
➔ 上のような手順を利用して多くのエネルギーを取りだせる

⇕

乱数の種を知らない人には本物の熱雑音と区別できない
➔ 熱雑音としての限界までしかエネルギーを取りだせない

［たとえばこんなことも可能かも］

送信者Aと受信者Bは
乱数のseedを共有



エネルギーを盗みたいC
には熱雑音にしか見えない

暗号論的疑似乱数の利用

［問題点］　普通の疑似乱数（たとえばM系列，乗算合同法）は
出力からseedが簡単に推測できてしまうのでダメ

➔「暗号用疑似乱数」を使う：具体例は右参照

公開鍵暗号と同様の仮定，たとえば
「大きい数の素因数分解や離散対数の計算は困難」
のもとで生成系列の予測困難性が証明されている

Blum-Micali

$x_j = g^{x_{j-1}} \bmod p$　　（p:大きな素数）

Blum-Blum-Shub

$x_j = \left(x_{j-1}\right)^2 \bmod N$

（$N = pq : p, q$はmod 4で3に合同な素数）

「一方向性置換」を利用　可逆だが，逆方向の計算量が大

疑似乱数の発生の計算で発熱する!?

［問題点］　乱数の種を知っていても必然的に計算過程で熱が発生する なら，種を知らないのと同じに？

「一方向性置換は〈可逆計算機〉で発熱なしに計算できるか」

・そもそも可逆計算で一方向性置換が計算できるなら
逆回しすれば同じ計算量で暗号が解けてしまう!?
・実は可逆計算では「ごみビット」がたまる → 消去すると発熱
・「鍵」を知っていて逆関数が少ない計算量で計算できる → 発熱せずに消去できる

可逆計算機の要素：フレドキン・ゲート
(X1,X2,X3) → (Y1,Y2,Y3)

Y3＝0: Y1＝X1,Y2＝X2, Y3＝X3
Y3＝1: Y1＝X2,Y2＝X1, Y3＝X3

C. H. Bennett (1989) SIAM J. COMP 18,766-776
H. F. Chau, H.-K. Lo (1996) One-way Functions In Reversible Computations, https://arxiv.org/abs/quant-ph/9506012

問題は解決できそうだが，理論的に構成されているが現存しない「可逆計算機」を仮定しなければならなくなった