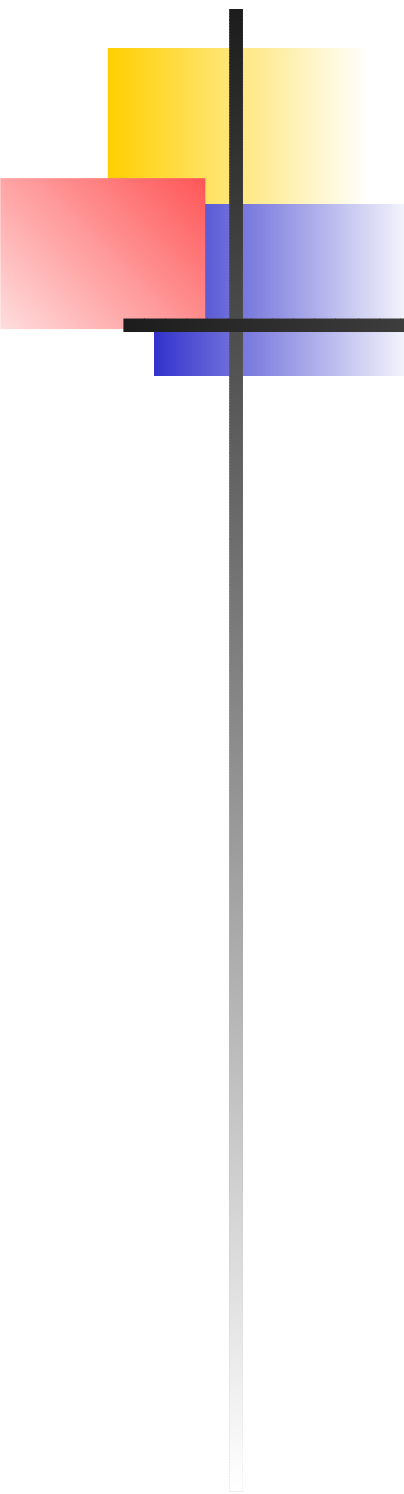




2008 年度 プロジェクト研究課題研究報告

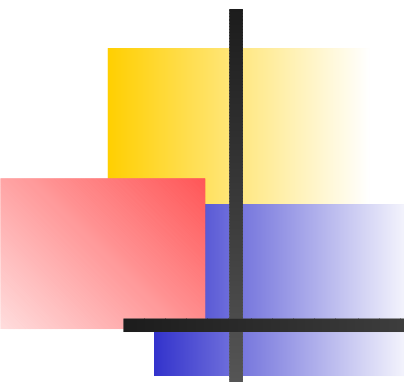
バーナム暗号に用いる
疑似乱数生成アルゴリズムの比較

2009 年 2 月 16 日

1090302 青野 裕太

高知工科大学 情報システム工学科

福本研究室



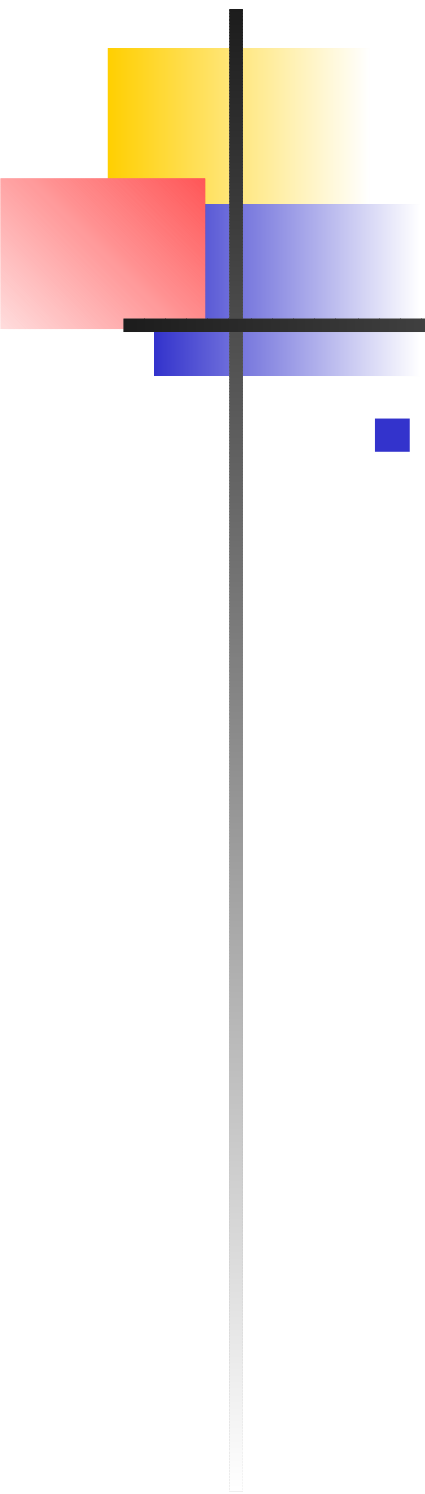
はじめに

■ 背景

- 真性乱数を鍵とした暗号方式
→ 安全な暗号の実現
- 真性乱数の生成の困難性
→ 疑似乱数の利用

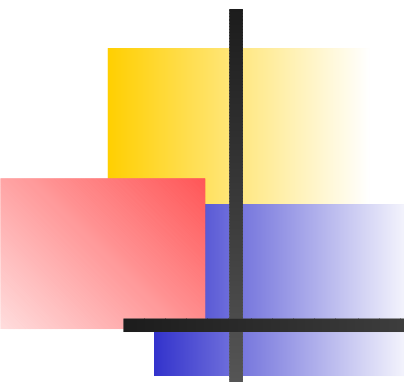
■ 目的

疑似乱数のランダム性の評価



疑似乱数のランダム性

- 評価尺度
 - バランス性
 - 周期性
 - 無相関性
 - 非線形性
 - 線形複雑度

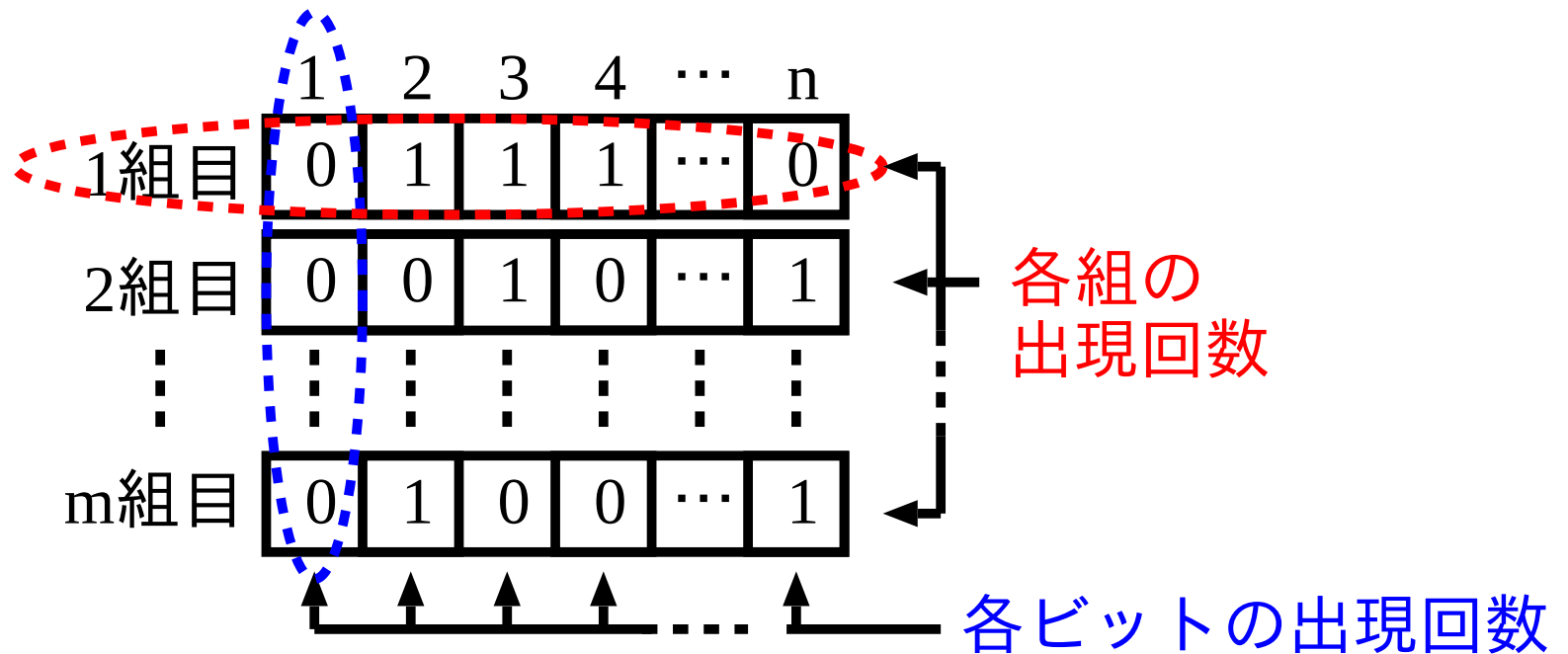


疑似乱数

- 生成アルゴリズム
 - 線形合同法 (LCG)
 - 線形帰還シフトレジスタ (LFSR)
 - メルセンヌ・ツイスタ (MT)
 - XorShift
- 2 値乱数

バランス性の比較方法

■ 各組と各ビットの出現頻度



■ 設定

ビット長 n : 1024, 生成組数 m : 2000

バランス性の比較結果

■ 1 の平均出現頻度の割合

	各ビット	各組
真性乱数	0.50000	0.50000
LCG	0.50072	0.50072
LFSR	0.50069	0.50069
MT	0.50017	0.50017
XorShift	0.50079	0.50079

- 疑似乱数では偏りが生じる
→ バランス性はない



バランス性の比較結果

- 短いビット長の場合
→ バランス性を持つ可能性

	割合	誤差の確率
真性乱数	0.50000	0
LCG	0.50072	0.00072

ビット長により誤差が確率論的に出る場合と
出ない場合に分かれる



まとめ

- バランス性の観点から比較
 - 偏りがあることを確認
→ バランス性はない
 - 短いビット長の場合
→ バランス性を持つ可能性
- 今後の課題
 - バランス性以外の評価尺度