

目 次

第 1 章	2 進法の世界における確率法則	1
1.1	2 進法での演算規則	1
1.2	2 進法での確率法則	3
第 2 章	乱数を用いた暗号化送信における統計的問題	6
2.1	送信と統計的表現	6
2.2	仮説検定について	9
2.3	乱数の扱いと送信の表現	17
第 3 章	暗号化送信に用いる乱数の統計的検定	21
3.1	乱数性と統計的検定法	21
3.2	NIST による一組みの乱数性の統計的検定方法	22
3.2.1	NIST による一組みの統計的検定方法の紹介	22
3.2.2	統計学的に検討を要するいくつかの点	37
3.3	Non-overlapping Template Matching Test とその一つの改善策の提案	38
3.3.1	パターン (テンプレート)	39
3.3.2	テンプレートの出現個数の数え方	42
3.3.3	テンプレートの定め方	44
3.3.4	出現個数の経験分布関数の作成	45
3.3.5	帰無仮説 SNH のもとでの出現個数の確率分布関数	46
3.3.6	テンプレートの出現個数の分布による帰無仮説 SNH の検定統計量の構成	57
3.3.7	Template Matching Test の改善策の試み (統計学的観点からの改善策の試み)	59

3.4 検討と試み	71
3.4.1 暗号化送信に用いる乱数と統計的解読可能性	71
3.4.2 暗号化送信に用いる乱数の検定について	79
3.4.3 乱数の検定に用いる標本の大きさについて	87
第4章 二つの0・1数列の和による乱数性の向上	95
4.1 一様性からのずれ	95
4.2 独立性からのずれ	97
参考文献	101
索引	103